

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Lab Policy and Command Output



Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy Files.....	3
**** Lab L03 pagentt.env *****	3
**** Lab L03 pagentt.conf *****	3
**** Lab L07 TMnx_ATTLS_FTP.policy *****	53
**** Lab L08 TMnx_ATTLS_FTPandTN3270.policy *****	55
**** Lab L09 TMnx_IPFilter.policy *****	58
**** Lab L12 TMnx_IPSec_VPN.policy *****	69
**** Lab L14 TMnx_IDS.policy *****	83
**** Lab L15 TMnx_IPSecVPN_wPreshare.policy *****	98
**** Lab L16 TMnx_ATTLS_wNSS.policy *****	114
**** Lab L16 TMnx_IPSecVPN_wIKEv2.policy *****	120
**** MVS1 AT-TLS Policy *****	138
**** MVS1 IPSec Policy *****	143
pasearch Command Output.....	182
ipsec Command Output.....	319
Other Command Output.....	410
**** Lab L07 RACF List ServAuth EZB.INITSTACK *****	410

Policy Files

```
*****

**** Lab L03 pagentt.env ****

*****
PAGENT_CONFIG_FILE=/etc/PAGT1/pagentt.conf
PAGENT_LOG_FILE=/tmp/pagentt.log
LIBPATH=/usr/lib
TZ=EST5EDT4

*****

**** Lab L03 pagentt.conf ****

*****
# IBM Communications Server for z/OS
# SMP/E distribution path: /usr/lpp/tcpip/samples/IBM/EZAPAGCO
#
# Licensed Materials - Property of IBM
# Copyright IBM Corp. 1998, 2009
# 5694-A01
# Status = CSV1R11
#
# PAGENT policy configuration (this file)
# /usr/lpp/tcpip/samples/pagent.conf
#
# CommonIpSecConfig policy configuration
# /usr/lpp/tcpip/samples/pagent_CommonIPSec.conf
#
# IpSecConfig policy configuration
# /usr/lpp/tcpip/samples/pagent_IPSec.conf
#
# TLSConfig policy configuration
# /usr/lpp/tcpip/samples/pagent_TTLS.conf
#
# IDSCConfig policy configuration
# /usr/lpp/tcpip/samples/pagent_IDS.conf
#
# RoutingConfig policy configuration
# /usr/lpp/tcpip/samples/pagent_Routing.conf
#
# This file contains sample policy control statements for the Policy Agent
# which verifies and installs them down to the appropriate MVS
# TCP/IP stack. The search order used by the Policy Agent to locate
# the initial configuration file is (highest priority listed first):
#
# 1) HFS file or MVS data set specified by the -c startup option. The
# syntax for an HFS file is '/dir/file' and the syntax for an MVS
# data set is '//MVS.DATASET.NAME'.
# 2) HFS file or MVS data set specified with the PAGENT_CONFIG_FILE
# environment variable.
# 3) /etc/pagent.conf
#
#
# The following are general rules to be followed when defining policies:
#
# - Specify Policy Agent configuration files using code page IBM-1047
# for EBCDIC, unless the Codepage statement is configured.
# - Only one attribute and its values can be specified per line.
# - Text beyond the specified attribute and value is ignored.
# - Text beginning with the # character is a comment and is ignored,
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# unless documented otherwise.
# - Comments beginning with the # character in an LDAP server ldif
# configuration file might only be recognized as comments at the
# beginning of the file; therefore do not specify such comments
# elsewhere in the file, as they are interpreted as part of an
# attribute or attribute value.
# - For most range specifications, the ranges can be delimited by a
# colon (:), a dash (-), or a blank ( ), but these delimiters cannot
# be mixed within a single range specification. IP address ranges
# cannot use the colon or blank delimiter, unless stated otherwise.
# - See z/OS Communications Server: IPv6 Network and Application Design
# Guide for information about types of policies that support IPv6.
# - IPv6 policy is installed but is not enforceable in a stack that
# is not IPv6 enabled.
# - IPv6 addresses specified as IPv4-mapped or IPv4-compatible addresses
# are valid only for IP filter rules and for the Identity parameter on
# local and remote security end points.
# - The maximum decimal value for numeric values is 4294967295, unless
# otherwise noted.
# - Policy rule and action names are limited to 32 characters. If QoS
# and IDS LDAP statement names longer than 32 characters are specified,
# they are silently truncated. All other statements longer than 32
# characters cause an error message to be written to the log.
# - If a configuration file or LDAP configuration contains duplicate
# statement or object names, Policy Agent keeps the first or the last
# statement or object, as follows. The following are considered warnings,
# not errors.
#   - For IDS (LDAP) and QoS, Policy Agent keeps the first entry.
#   - For IDS (configuration file), IPSec, Routing, and AT-TLS, Policy
#     Agent keeps the last entry.
# - If a QoS or IDS statement or object is defined with the same name
# in both a configuration file and LDAP, Policy Agent keeps the first
# such statement or object that it reads. This is typically the statement
# or object in the configuration file, but as a result of timing
# constraints, it could also be the statement in LDAP. The last duplicate
# statement or object is discarded; this is considered an error.
# - Specify most attributes for configuration file statements only once
# per statement (exceptions are noted where appropriate). If you specify
# multiple attributes, no error or warning messages are written to the
# log, and the last instance of the attribute is used.
# - Attributes for policies defined on an LDAP server may be single- or
# multi-valued (meaning a single value or multiple values are allowed
# for that attribute). The Policy Agent detects multiple values for
# attributes that are defined as single valued, and treats the policy
# object as in error.
# - The policy version is specified by the configuration file statement
# name as follows:
#   - ServicePolicyRules and ServiceCategories statements specify version 1
#     policies.
#   - PolicyRule and PolicyAction statements specify version 2 policies.
#     Result: The policy version of LDAP-defined objects is determined
#     by the LDAP_SchemaVersion parameter on the ReadFromDirectory statement.
# For more information about policy version definitions, see z/OS
# Communications Server: IP Configuration Guide. For more information
# about policy version differences, see z/OS Communications Server: IP
# Diagnosis Guide.
# - Some configuration statements use an inline statement syntax. When a
# given statement is specified inline within another statement, only the
# inline statement name is shown in the syntax diagrams. However, the
# entire statement being inlined must be specified, including its own set
# of start and end braces ({} ) and all parameters.
# Tip: The name parameter on the statement name might or might not be
# optional, depending on the specific statement. In the following example,
# the IpFilterRule statement is included inline within the IpFilterGroup
# statement. A name is required on the IpFilterRule statement, for example,
# Rule1All-Permit, as follows:
# IpFilterGroup ZoneAll
# {
#   IpFilterRule Rule1All-Permit
#   {
#     IpSourceAddr All
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#      IpDestAddr All
#      IpServiceGroupRef Resolver
#      IpServiceRef PathMtuDiscovery
#      IpServiceGroupRef Ping-Outbound-Only
#      IpGenericFilterActionRef permit
#    }
#  }
# - For named inline statements where the name is optional, a nonpersistent
#   system name is created using the named portion of the statement name
#   with a unique identifier. This prevents reuse of the named inline
#   statement as a reference name.
# - Errors detected in a policy rule or action result in that policy
#   object being discarded.
# - For IPSec, Routing or AT-TLS policies, any errors detected during
#   parsing results in no new policies being installed. For all other
#   policy types, only the policy objects that contain errors are
#   discarded.
# - If a rule refers to an action that does not exist (or has been discarded
#   due to an error) then the rule is also discarded.
# - If a Routing action refers to Route Table that does not exist
#   (or has been discarded due to an error), the action is also
#   discarded.
#
# The following conventions are used in this configuration file:
#   p : choose one in the allowed parameter set
#   p+ : choose one or more in the allowed parameter set
#   B : integer value of a byte (i.e., 0 =< B =< 255)
#   b : bit string starting with left most bit (e.g., 101 is
#       equivalent 10100000 in a byte field)
#   i : integer value
#   s : a character string
#   a : IPv4 address in dotted-decimal format or
#       IPv6 address in colon-hex format
#   l : a distinguished name in directory format k=s,k=s...,
#       where k & s are strings
#   (R) : Required parameter
#   (C) : Conditionally required parameter (required if ...)
#   (O) : Optional parameter

# Codepage Statement
# Use the Codepage statement to specify the EBCDIC code page to be
# used for reading all configuration files and policy definition files.
# The default is IBM-1047. All statements read from the files are
# converted to the IBM-1047 code page from the specified code page.
#
# Result: If you specify a code page that is not one of the supported values,
# then Policy Agent issues a warning message to the log file and tries
# to read the configuration files using the IBM-1047 code page. It is
# possible that configuration errors will be detected in this case.
#
# statement format:
#   Codepage                s # Code page value.
# where:
#   s                        (R): One of the supported code
#                               page values:
#                               IBM-037
#                               IBM-273
#                               IBM-274
#                               IBM-275
#                               IBM-277
#                               IBM-278
#                               IBM-280
#                               IBM-281
#                               IBM-282
#                               IBM-284
#                               IBM-285
#                               IBM-297
#                               IBM-500
#                               IBM-871
#                               IBM-1047
#                               IBM-1140
```

```

IBM-1141
IBM-1142
IBM-1143
IBM-1144
IBM-1145
IBM-1146
IBM-1147
IBM-1148
IBM-1149

example: Codepage IBM-1141

LogLevel Statement
This statement specifies what type of log messages should be logged
into the Policy Agent log file. The default is log level 31. If
upon invocation of Pagent, the debug (-d) option is specified with
debug level 1, all log messages are logged.

statement format:
    LogLevel                                     i # Logging level.
where:
    i                                             (R): The sum of the following values
that
represent log levels:
LOGL_SYSERR      1
LOGL_OBJERR      2
LOGL_PROTERR     4
LOGL_WARNING     8
LOGL_EVENT      16
LOGL_ACTION      32
LOGL_INFO        64
LOGL_ACNTING    128
LOGL_TRACE       256

example: LogLevel 15 specifies four error types to be logged:
syserr, objerr, proterr, and warning.

LogLevel 31
LogLevel 511

TcpImage and PEPInstance Statements (synonyms)
This statement specifies an MVS TCP/IP image/stack and its associated
policy control file to be installed to that image. If policy control
file is not specified, following control statements (if any) in this
file will be installed to that image. If no TcpImage statement is
specified, all policies will be installed to the default TCP/IP image.
Parameter FLUSH or NOFLUSH (default) can be used to force flushing
(deletion) of all existing policy control data in the stack on
startup or when the configuration files change. The PURGE or NOPURGE
parameter controls whether or not policies are deleted from the stack
when Pagent is shut down. The time interval for checking for new,
changed, or deleted policies can be specified. The default is 1800
seconds (30 minutes).

statement format:
    TcpImage | PEPInstance      s1   s2   p   p   i # TCP/IP image specification
where:
    s1                           (R): (8 characters) is the name of t
VSV                               TCP/IP image.
    s2                           (O): Is the path of the policy contr
ile.                             If not specified, this file is
sed.                             (O): FLUSH | NOFLUSH, default is
NOFLUSH.                         (O): PURGE | NOPURGE, default is
NOPURGE.                         (O): File/LDAP modification check
interval in                     seconds. Default is 1800 (30
minutes).
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
# example: TcpImage TCPCS /tmp/TCPCS.policy FLUSH PURGE 600
# TcpImage TCPIPT FLUSH PURGE 600
#
# AutoMonitorApps Statement
#
# You can configure the Policy Agent to monitor and automatically start
# or restart a set of related applications. The following set of applications
# can be monitored:
#
# - Defense Manager daemon (DMD)
# - IKE daemon (IKED)
# - Network Security Server daemon (NSSD)
# - Syslog daemon (SYSLOGD)
# - Traffic Regulation Manager daemon (TRMD)
#
# Use the AutoMonitorParms statement to configure global parameters that
# control how the Policy Agent monitors and starts or restarts these applications.
#
# Use the AutoMonitorApps statement to configure what applications should
# be monitored, and to specify application-specific parameters.
#
# Results:
# - If you configure applications to be automatically started and restarted,
#   be aware of the following:
#   - If you start the Policy Agent after you've already started an application
#     to be monitored, Policy Agent starts monitoring the application if it was
#     originally started with the same job name that is configured to the Policy Agent.
#     If the application needs to be restarted later, it is restarted using the
#     cataloged procedure configured to the Policy Agent. This might not be the
#     same procedure that was originally used to start the application.
#   - If you start the Policy Agent after you've already started an application
#     to be monitored, but the application does not use the same job name that
#     is configured to the Policy Agent, then the Policy Agent is not able to
#     detect that the application is active. Policy Agent tries to start another
#     instance of the application, and this start will likely fail.
#
# Tip: If you configure applications to be monitored by the Policy Agent, ensure
# those applications are not running before starting the Policy Agent.
# However, you might need to start syslogd before starting the Policy Agent.
# If you start syslogd before starting the Policy Agent, ensure that Policy
# Agent is configured with the correct syslogd job name.
#
# - If this statement is removed, or one or more AppName parameters, or instances
#   of the TcpImageName parameter are removed, Policy Agent stops monitoring the
#   affected applications. You must stop or restart the applications if needed.
#
# - If one or more AppName parameters, or instances of the TcpImageName parameter
#   are added, Policy Agent starts the affected applications and begins monitoring
#   them.
#
# - If any of the parameters other than AppName or TcpImageName are added, removed,
#   or changed, Policy Agent stops and restarts the affected applications.
#
# statement format for applications without stack affinity:
#   AutoMonitorApps
#   {
#       AppName                p # Application name
#       {
#           ProcName            s # Cataloged procedure
#           Jobname              s # Job name
#           StartParms          s # Start options
#           EnvVar               s # Environment variable
#       }
#   }
#
# statement format for applications with stack affinity:
#   AutoMonitorApps
#   {
#       AppName                p # Application name
#       {
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#           TcpImageName                s # TCP/IP stack name
#           {
#           ProcName                    s # Cataloged procedure
#           Jobname                     s # Job name
#           StartParms                  s # Start options
#           EnvVar                      s # Environment variable
#           }
#           }
#           }
#
# where:
#       AppName                        (O): Specifies what applications
#                                     you want to monitor and
#                                     start and restart. Repeat this
#                                     parameter for each application.
#                                     The following applications are
#                                     supported:
#                                     - Defense Manager daemon (DMD)
#                                     - IKE daemon (IKED)
#                                     - Network security services daemon
#                                     - Syslog daemon (SYSLOGD)
#                                     - Traffic Regulation Manager daemon
#
#       (NSSD)
#
#       (TRMD)
#
#       TcpImageName                  (O): A string 1 - 8 characters in length
#                                     that specifies the TCP/IP images on
#                                     which
#                                     the application runs. Repeat this
#                                     parameter for each image.
#
#                                     Rules:
#                                     - This parameter is required and
#                                     only for applications that run a
#                                     separate instance for each TCP/IP
#
#                                     Currently, the only application
#                                     this is TRMD.
#                                     - You can specify a maximum of 8
#                                     TcpImageName parameters for a
#                                     AppName parameter.
#                                     - You must configure the specified
#                                     image on a TcpImage statement.
#
#                                     Results:
#                                     - In an single stack (INET)
#                                     the application runs on the
#                                     image.
#                                     - In a common INET (CINET)
#                                     you do not specify the TCP/IP
#                                     the application runs on the
#                                     image (resolver-supplied TCP/IP
#                                     TCP/IP job name). If the default
#                                     image cannot be determined, the
#                                     uses the name INET.
#                                     - If the TcpImage statement for the
#
#       valid
#
#       image.
#
#       that does
#
#       unique
#
#       given
#
#       TCP/IP
#
#       environment,
#
#       active TCP/IP
#
#       environment, if
#
#       image name,
#
#       default TCP/IP
#
#       user ID or
#
#       TCP/IP
#
#       Policy Agent
#
#       specified

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#                               TcpImageName is removed, Policy
Agent stops                     monitoring the application for
#                               image.
that TCP/IP
#
#                               (R): A string 1 - 8 characters in length
#                               ProcName
that                               specifies the name of a cataloged
#                               procedure
procedure                         that is used to start the
#                               sample procedure is included in
application. A                   SEZAINST(EZAPOLPR).
#
#                               Tip: You can use a single generic
#                               procedure for all configured
cataloged                        Parameters are passed to the start
#                               to identify the application name
applications.                    application-specific parameters.
#                               use a single procedure then all
procedure                        applications will run under the
#                               ID. If you want to use different
and                               for each application, specify
#                               procedure names for the
If you                           this parameter.
#                               Rule: The specified procedure must
started                          following JCL parameters:
#                               Variable  Description
same user                        -----
#                               PGM          Specifies the name  One
user IDs                        of the application
#                               program executable.
different
#                               -
applications using              -
#                               -
#                               -
contain the                      -
#                               -
#                               -
Value Passed                    -
#                               -
-----
#                               of the following
#                               supported application
#                               names:
#                               DMD
#                               IKED
#                               NSSD
#                               SYSLOGD
#                               TRMD
#                               Temporary file name
#                               generated by the Policy
#                               Agent.
#                               environment
#                               variables for the
#                               application.

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#
#
string specified
#
the StartParms
#
parameter on the
#
AutoMonitorApps
#
statement, or a null
#
string.
#
#           Jobname
#
name
#
#
#
#
the
#
parameter
#
value
#
parameter.
#
TcpImageName
#
required so
#
instance is unique.
#
#           StartParms
length that
#
the application.
#
on the PARM
#
statement, but without
#
#
#
#           EnvVar
length that
#
the application.
#
environment variable.
#
name and the value,
#
are some examples
#
#
#
for IKED,
#
#
IKED_FILE=/etc/iked.conf
#
configuration file
#
#
RESOLVER_CONFIG=/'SYS1.TCPPARMS(TCPDATA2)'
#
NSSD, code

```

PARMS Specifies start The parameters for the on application.

(O): A string 1 - 8 characters in length that specifies the run-time job for the application.

Rules:

- For applications that do not use TcpImageName parameter, this is optional. The default is the specified with the AppName
- For applications that use the parameter, this parameter is that the job name for each

(O): A string 1 - 45 characters in specifies the start parameters for Specify the parameters as you would parameter on the EXEC JCL using single quotes. For example:

StartParms -d 1

(O): A string 1 - 1024 characters in specifies environment variables for Repeat this parameter for each Specify the environment variable separated by an equal sign. Here of how this parameter can be used:

- To specify the configuration file code the following: EnvVar
- To specify the resolver for TRMD, code the following: EnvVar
- To specify the time zone for

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#                                     the following:
#                                     EnvVar    TZ=EST5EDT
#
# example:
#   AutoMonitorApps
#   {
#     AppName      IKED
#     {
#       Procname   POLPROC
#     }
#     AppName      TRMD
#     {
#       TcpImageName TCPIP1
#       {
#         Procname   POLPROC
#         Jobname    TRMD1
#       }
#       TcpImageName TCPIP3
#       {
#         Procname   POLPROC
#         Jobname    TRMD3
#       }
#     }
#   }
#
# AutoMonitorParms Statement
#   Use the AutoMonitorParms statement to configure the Policy Agent to monitor and
#   automatically start or restart a set of related applications. The following set
#   of applications can be monitored:
#
#   - Defense Manager daemon (DMD)
#   - IKE daemon (IKED)
#   - Network Security Server daemon (NSSD)
#   - Syslog daemon (SYSLOGD)
#   - Traffic Regulation Manager daemon (TRMD)
#
#   Use the AutoMonitorApps statement to configure what applications should be
#   monitored, and to specify application-specific parameters.
#
#   Use the AutoMonitorParms statement to configure global parameters that control
#   how the Policy Agent monitors and starts or restarts the configured applications.
#   If the default values for all parameters are acceptable, you do not need to use
#   this statement.
#
# Results:
#   - If this statement is removed, the default values are applied when the previously
#     specified MonitorInterval value expires.
#   - If this statement is added, the new values are applied when the previous
#     default MonitorInterval expires.
#   - If any changes are made to this statement, the new values are applied when
#     the previously specified MonitorInterval value expires.
#
# statement format:
#   AutoMonitorParms
#   {
#     MonitorInterval      i # Monitor interval
#     RetryLimitCount      i # Retry limit count
#     RetryLimitPeriod     i # Retry limit period
#   }
# where:
#   MonitorInterval      (0): Specifies the interval, in seconds,
#                           at which an application should be
#                           monitored if that application is
#                           still running. Valid values are in
#                           the range 1 - 1440. The default
#                           is 10 seconds.
#
#   RetryLimitCount      (0): Specifies the number of times
#                           Policy Agent should start or
restart

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

# an application within the time
period
# specified by the RetryLimitPeriod
# parameter. Valid values are in the
# range 1 - 99. The default is 5.
#
# Each time an application is
started,
# Policy Agent waits 1 minute for the
# application to start. If it does
not
# start, Policy Agent tries to start
it
# again until the limit specified
with
# this parameter is reached. If the
# application still has not started,
# Policy Agent stops monitoring the
# application until a MODIFY
MON, START
# command is issued for the
application.
# For example, if the application is
IKED,
# the MODIFY procname, MON, START, IKED
# command causes Policy Agent to
resume
# trying to start the application.
See
# the MODIFY Policy Agent topic in IP
# System Administrator's Commands for
# information about using MODIFY
commands
# to manage the monitored
applications.
#
# RetryLimitPeriod (0): Specifies the time interval, in
seconds,
# at which Policy Agent should try to
# start or restart an application.
See
# the RetryLimitCount parameter for
# more details. Valid values are in the
# range 1 - 1440. The default is 600 (10
minutes).
#
# example:
#   AutoMonitorParms
#   {
#     MonitorInterval    10
#     RetryLimitCount     5
#     RetryLimitPeriod   600
#   }
#
# ClientConnection Statement
# The Policy Agent acting as a policy server uses the ClientConnection
# statement to specify the listening port. The Policy Agent acting as a
# policy client uses this connection to retrieve remote policies.
#
# An error is flagged if both the ClientConnection and ServerConnection
# statements are configured on the same Policy Agent. The result is that
# there is no connection between the policy server and policy client.
#
# If the ClientConnection statement is removed, all connections to policy
# clients are disconnected.
#
# Updates to the ClientConnection statement are used only for new client
# connections to the policy server.
#

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# statement format:
# ClientConnection
# where:
# i
# connections
#
#
# that
#
#
# range
#
# is
#
#
# the
#
# connections
#
#
# port
#
# ServicesConnection
#
#
# example:
# ClientConnection 16310

# DynamicConfigPolicyLoad Statement
# The Policy Agent acting as a policy server uses the DynamicConfigPolicyLoad
# statement to obtain the file names of the configuration files to be retrieved by
# policy clients.
#
# The DynamicConfigPolicyLoad statement can appear only in the main configuration file.
#
# For each policy type the policy client files are read only after the policy
# client connects to the policy server. A DynamicConfigPolicyLoad statement (or
default
# values) is bound to a policy client for the life of that client, until one of the
following
# occurs:
#
# - The policy client disconnects from the policy server.
# - The connection between the policy server and the policy client ends.
# - The associated DynamicConfigPolicyLoad statement is removed.
#
# When a DynamicConfigPolicyLoad statement is removed, the policy clients that
# were using that statement change to use another statement, or default values.
#
# The policy client policies are removed from the policy server in the following cases:
#
# - The policy client disconnects from the policy server.
# - The connection between the policy server and the policy client ends.
# - The policy client requests that remote policies for a specific policy type be
unloaded
# from the policy server.
# - The associated DynamicConfigPolicyLoad statement is removed.
#
# To retrieve remote policies with the policy client, you must define security product
# authority in the SERVAUTH class for the policy client's user ID; the user ID is
defined
# on the Userid parameter on the PolicyServer statement. The ClientName parameter on
the
# PolicyServer statement is used as the image name. For more information, see the
general
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# policy agent configuration information in z/OS Communications Server: IP
Configuration
# Guide. Wildcard values are allowed in profile names. The following example shows the
# structure of the security product profile:
# EZB.PAGENT.sysname.image.ptype
#
# Multiple DynamicConfigPolicyLoad statements can appear in the main configuration
# file. The policy server maintains a list of these DynamicConfigPolicyLoad
# statements. When a policy client connects to the policy server, then the policy
# client name configured on the PolicyServer statement is matched to the clientname
# parameter. The names are case-sensitive with regard to matching. This clientname
# parameter can be a regular expression. The policy server matches these names in the
# following order:
# 1. A clientname parameter that has an exact match to the policy client name. The
policy
# client name must not contain any regular expression characters.
# 2. A regular expression clientname parameter that matches the policy client name. The
# longest matching regular expression is chosen. If multiple statements match with
the
# same length clientname parameter, the statement chosen is based on alphabetical
order.
# 3. If there is no matching clientname parameter or a matching clientname value does
not
# have a corresponding PolicyType parameter for this policy type, then the following
# default remote files are used:
# - Stack-specific remote files used for each policy type:
# - IDS - /etc/pagent_remote.ids
# - IPSec - /etc/pagent_remote.ipsec
# - QoS - /etc/pagent_remote.qos
# - Routing - /etc/pagent_remote.routing
# - AT-TLS - /etc/pagent_remote.ttls
# - For any default stack-specific remote file used, there is no corresponding
common
# configuration file.
# - If no matching clientname parameter is found, then the refresh interval is set
to
# 30 minutes.
#
# The PolicyLoad and CommonPolicyLoad parameters are optional; however, if neither the
# PolicyLoad parameter or the CommonPolicyLoad parameters are configured, this
# DynamicConfigPolicyLoad statement results in an error and the statement is discarded.
#
# statement format:
#     DynamicConfigPolicyLoad                s # Client name
#     {
#         PolicyType                        p # Policy type
#         {
#             CommonPolicyLoad              s # Common file name
#             PolicyLoad                    s # Image file name
#         }
#         RefreshInterval                  i # Refresh interval
#     }
#
# where:
#     s                                     (R): A string 1-511 characters in length
#                                           specifying the client name to be
#                                           matched to the policy client name.
#                                           If this is a regular expression,
#                                           the
#                                           string must consist of 1 - 511
#                                           characters.
#                                           Otherwise, it must consist of 1-24
#                                           characters.
#                                           This clientname parameter is used
#                                           to match the policy client name
#                                           when it connects to Policy Agent
#                                           to derive its policy files.
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
consist
#
simplest form
#
of
#
meaning. Such
#
z/OS
#
Configuration
#
#
usage.
#
#       PolicyType
configuration
#
type.
#
types
#
types
#
#
#
#
#
#
#       CommonPolicyLoad
policy
#
#
#
#
#
#
#
#
#       PolicyLoad
remote
#
#
#
#
#
#
#
#
specific
#
#
#
#
#
#
#       RefreshInterval
seconds)
#
changes
#
time of
```

The clientname parameter can also
of a regular expression. The
of regular expression is a string
characters without a special
a string matches only itself. See
Communications Server: IP
Reference for the allowable regular
expression characters and their

(O): Indicates additional policy
information for a specific policy
specific policy type. Multiple
can be specified. Valid policy
are:
- IDS
- IPSec
- QoS
- Routing
- TLS

(C): The path of the common remote
file to be used for the defined
policy type.

The CommonPolicyLoad parameter is
not supported for PolicyType QoS.

One or both of the CommonPolicyLoad
or PolicyLoad parameters must be
specified.

(C): The path of the stack-specific
policy file to be used for the
defined policy type.

If the PolicyLoad parameter is not
specified, then the associated
common remote policy file specified
on the CommonPolicyLoad parameter
is used.

The path name can contain a single
wildcard character (*). The policy
client name replaces the wildcard
position to obtain the stack-
remote policy file.

One or both of the CommonPolicyLoad
or PolicyLoad parameters must be
specified.

(O): Specifies the time interval (in
that lapses between checks for
to the creation or modification

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# the common and stack-specific
remote policy files. This attribute applies to
# configured policy types. In the
all cases, the update interval is
# - If a value is not specified, the
following is 1800 seconds (30 minutes).
# - If a value of 0 is specified, the
changed: value of 1800 seconds (30
# minutes) is used.
# rounded up to
# 300 seconds (5 minutes).
#
# example:
#   DynamicConfigPolicyLoad remote*
#   {
#     RefreshInterval      1800
#     PolicyType            IPSec
#     {
#       CommonPolicyLoad  /etc/pagent_remote.ipsec
#     }
#     PolicyType            TTLS
#     {
#       PolicyLoad        /etc/pagent_remote.ttls
#     }
#   }
#
# PolicyServer Statement
# The Policy Agent acting as a policy client uses the PolicyServer statement to
# determine what type of policies to retrieve from the policy server. This statement
# also specifies security information and processing information which is passed to
# the policy server.
#
# Connectivity to the policy server is needed for all images that specify the
# PolicyServer statement.
#
# The PolicyServer statement can appear only in an image configuration file (unless
# the main and image configuration files are the same file).
#
# If a ServerConnection statement is not configured in the main configuration file,
# then this statement is ignored.
#
# For a policy type, if remote policies are used, then the local policies of the same
# type are ignored.
#
# The policy client disconnects from the policy server when one of the following
# occurs:
# - The ServerConnection or PolicyServer statement is removed. The result is that
#   all remote policies are uninstalled. If local policies are configured, then they
#   are installed.
# - The PolicyServer statement is updated and all PolicyType parameters are removed.
#   The result is that the remote policies for the associated TCP/IP stack are
#   uninstalled.
#   If the local policies for the associated TCP/IP stack are configured, they are
#   installed.
#
# The policy client disconnects from and reconnects to the policy server when one of
# the following occurs:
# - The PolicyServer statement is updated and the client name, user identification or
#   authorization parameters have changed.
# - The connection between the policy server and the policy client ends.
#
# If a PolicyType parameter is removed, then the remote policies for this policy type
# are removed for the associated TCP/IP stack. If the local policies for this policy
# type are configured, they are installed.
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
# You must have defined security product authority in the SERVAUTH class for the policy
# client's user ID. The policy client's client name is used as the image name. For
details,
# see the general policy agent configuration information in z/OS Communications Server:
IP
# Configuration Guide. Wildcard values are allowed in profile names. The following
example
# shows the structure of the security product profile:
# EZB.PAGENT.sysname.image.ptype
#
# statement format:
#     PolicyServer
#     {
#         Userid                s # User ID
#         AuthBy                p s # Authorization type
#         ClientName            s # Client name
#         PolicyType            p # Policy type
#         {
#             FLUSH | NOFLUSH    s # Common file name
#             PURGE | NOPURGE    s # Image file name
#         }
#     }
#
# where:
#     Userid                (R): Specifies the policy client's user
server                        identification string. The policy
#                               uses this parameter to identify
which                          resources the client can access.
#                               ID is a string 1 - 8 alphanumeric
The user                      characters in length. The first
#                               cannot be a number. No special
#                               (@, $, #, *) are allowed.
character
#                               (R): Indicates which method the policy
characters                    uses for authentication of the user
#                               The options are Password and the
#                               secure PassTicket.
#                               - Password <string>
#                               This option causes the client to
send                            the configured password to the
#                               server for authentication. The
policy                          is 1 - 8 characters in length.
#                               - PassTicket
#                               The PassTicket option causes the
password                        to generate a one-time session
#                               the information about the secured
#                               function in z/OS Security Server
#                               Security Administrator's Guide.
client
#                               (O): A string 1-24 characters in length
key. See                      that
#                               specifies the client name
signon                        (PEPInstance name)
#                               for this policy client. This
RACF
#
#     ClientName
that
#
# (PEPInstance name)
#
client
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

# name is used by the policy server
to
# determine which configuration files
# to use to load the client's
policies
# and whether proper security
authorization
# is configured. See z/OS
Communications
# Server: IP Configuration Reference
# DynamicConfigPolicyLoad statement
for details
# about how this name is used to
select the remote
# configuration file names.
#
# If no client name is configured,
then
# the policy client generates this
# parameter based on the system's
host name
# and the associated TcpImage or
# PEPInstance statement image name.
#
# PolicyType (O): Indicates what policy types the
policy client retrieves from the policy server.
#
Multiple types can be specified. Valid
policy types
# are:
# - IDS
# - IPSec
# - QoS
# - Routing
# - TLS
#
# The additional set of braces are
# required only if the following
# parameters are specified.
#
# FLUSH | NOFLUSH (O): FLUSH or NOFLUSH value. These
# parameters are ignored for
PolicyType
# IPSec and Routing.
#
# PURGE | NOPURGE (O): PURGE or NOPURGE value. These
# parameters are ignored for
PolicyType
# IPSec and Routing.
#
# example:
# PolicyServer
# {
#     Userid USER10
#     AuthBy PassTicket
#     ClientName remote42
#     PolicyType IDS
#     {
#         FLUSH
#         PURGE
#     }
#     PolicyType Routing
# }

# ServerConnection Statement
# The Policy Agent acting as a policy client uses the ServerConnection statement to
# connect to the Policy Agent acting as a policy server. This statement includes
# security information and the location of the policy server. The policy client uses
# this connection to retrieve remote policies.
#

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# An error is flagged if both the ClientConnection and ServerConnection
# statements are configured on the same Policy Agent. As a result, there is
# no connection between the policy server and policy client.
#
# If a PolicyServer statement is not configured in any image configuration file,
# this statement is ignored, and no connections to the policy server exist.
#
# If any parameters on the ServerConnection statement are updated after a remote
# connection is established, the changed values take effect for new connections.
# The ServerConnectWait and ServerConnectRetries parameters take effect immediately
# for any connections that require retry processing.
#
# If the ServerConnection statement is deleted, all established remote connections
# are stopped. As a result, all remote policies are uninstalled. If configured,
# then the local policies are now installed.
#
# statement format:
#   ServerConnection
#   {
#       ServerHost           a|s # Primary host
#       ServerPort           i # Primary port
#       ServerHostBackup     a|s # Backup host
#       ServerPortBackup     i # Backup port
#       ServerConnectWait    i # Connect wait
#       ServerConnectRetries i # Connect retry
#       ServerSSL
#       {
#           ServerSSLKeyring      s # Keyring name
#           ServerSSLKeyringPassword s # Keyring password
#           ServerSSLKeyringStashFile s # Keyring stash file name
#           ServerSSLName         s # Label name
#           ServerSSLV3CipherSuites s # Cipher suites
#       }
#   }
#
# where:
#   ServerHost           (R): A string 1 - 512 characters in
length                    that specifies the name of the
#                           primary
#                           policy server host that contains
#                           policy definitions. Specify the
name                       as a hostname (for example,
#                           policyserver.mynetwork.com) or as
#                           an IP address (for example,
9.11.12.13).
#                           The IP address can be either IPv4
or                           IPv6.
#
#   ServerPort           (O): The policy server listening port
number.                    The policy client connects using
#                           this port
#                           number. The valid port values are
#                           in the
#                           range 1 - 65535. The default is
16310.
#
#   ServerHostBackup     (O): A string 1 - 512 characters in
length                    specifying the name of the backup
#                           policy server that contains policy
#                           definitions. The name can be
#                           as a hostname (for example,
#                           policyserver.mynetwork.com) or as
#                           an IP address (for example,
9.11.12.13).
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

<pre># or # server. # # ServerPortBackup # # # # in the # 16310. # # specified. # # ServerConnectWait 300) # between # # policy # seconds. # # ServerConnectWait value # ServerConnectRetries value # seconds that # connect with a # another # is configured). # ServerConnectWait value is # value is 3, then # # of 180 seconds # # # ServerConnectRetries 10) that # establish a # The default # # # ServerConnectWait value # ServerConnectRetries value # seconds that # connect with a # another # is configured). # ServerConnectWait value is # value is 3, then</pre>	<pre>The IP address can be either IPv4 IPv6. The default is no backup (O): The backup policy server listening port number. The policy client connects using this port number. The valid port values are range 1 - 65535. The default is This parameter is ignored if the ServerHostBackup parameter is not (O): Specifies the number of seconds (1- that the policy client waits connection attempts when trying to establish a connection with a server. The default value is 60 The product of the multiplied by the defines the maximum number of the policy client attempts to policy server before switching to policy server (if a backup server For example, if the 60 and the ServerConnectRetries the policy client waits a maximum for a successful connection. (O): Specifies the number of times (1- the policy client = attempts to connection with a policy server. value is 3 retries. The product of the multiplied by the defines the maximum number of the policy client attempts to policy server before switching to policy server (if a backup server For example, if the 60 and the ServerConnectRetries</pre>
---	---

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#                                     the policy client waits a maximum
of 180 seconds                       for a successful connection.
#
#                                     (O): Indicates that additional SSL
#                                     parameters follow.
#                                     This parameter is optional. If you
#                                     want to use a secure connection to the policy
#                                     server, specify this parameter and other SSL
#                                     parameters as needed.
#                                     (O): A string 1 - 1023 characters in
#                                     length specifying the name of the key ring
#                                     file created by gskkyman, or the ring name of
#                                     the SAF key ring. This key ring usually contains the
#                                     certificates of the trusted (by the client)
#                                     Certificate Authorities. The key ring can also
#                                     contain a public key and the associated
#                                     certificate (this is needed only when client
#                                     authentication is required).
#                                     This parameter is required if
#                                     ServerSSL is specified.
#                                     (O): A string 1 - 128 characters in
#                                     length that specifies the password for the key
#                                     database that protects the key ring file. It is
#                                     set when the key ring file is created with the
#                                     gskkyman tool. This parameter is optional. As an
#                                     alternative, you can specify the more secure
#                                     to use a ServerSSLKeyringStashFile parameter
#                                     the gskkyman key database that was created with
#                                     file parameter tool. The password and the stash
#                                     ring. are not required with a SAF key
#                                     #                                     (O): A string 1 - 1023 characters in
#                                     #                                     specifies the name of the key ring
#                                     #                                     The stash file is created when the
#                                     #                                     file is created with the gskkyman
#                                     #                                     the ServerSSLKeyringPassword
#                                     #                                     specified, then it is used instead
#                                     #                                     of this parameter. The password and the
#                                     #                                     stash file
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#                                     parameter are not required with a
SAF keyring.
#
#       ServerSSLName                 (O): A string 1 - 256 characters in
#                                     length specifying a case-sensitive
#                                     value that specifies the label
#                                     assigned when creating a private
#                                     key/certificate pair with gskkyman.
#                                     This is used when the client is
#                                     authenticated.
#
#       ServerSSLV3CipherSuites       (O): Specifies the SSL version 3 or TLS
#                                     version 1 cipher suites in order of
#                                     preference. If a
ServerSSLV3CipherSuites
#                                     parameter is specified more than
once,
#                                     the values are concatenated to
#                                     create
#                                     a single list of cipher suites. For
#                                     System SSL, the GSK_V3_CIPHER_SPECS
#                                     value is set to the concatenated
#                                     value.
#
#                                     The ciphers value is a string of
one or
#                                     more 2-hexadecimal character
#                                     that are SSL version 3 or AT-TLS
ciphers
#                                     1 ciphers, or a single cipher
#                                     The cipher string cannot have
version
#                                     each cipher. If duplicate ciphers,
constant.
#                                     first instance of the cipher is
#                                     all other instances you specify are
blanks between
#                                     The maximum number of ciphers is
#                                     255. For
#                                     the
#                                     description of
#                                     gsk_environment_open() call in z/OS
Sockets
#                                     Cryptographic Service System Secure
#                                     Layer Programming for a list of
valid cipher
#                                     suites.
#
#       example:
#       ServerConnection
#       {
#           ServerHost                 9.1.2.3
#           ServerPort                 16310
#           ServerHostBackup           policyserver.mynetwork.com
#           ServerPortBackup           16310
#           ServerConnectWait          60
#           ServerConnectRetries       3
#           ServerSSL
#           {
#               ServerSSLKeyring        /etc/client.kdb
#               ServerSSLKeyringStashFile /etc/client.sth
#               ServerSSLName           labell1
#               ServerSSLV3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
#               ServerSSLV3CipherSuites TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
#               ServerSSLV3CipherSuites TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
#               ServerSSLV3CipherSuites TLS_DHE_RSA_WITH_AES_256_CBC_SHA
#               ServerSSLV3CipherSuites TLS_DHE_DSS_WITH_AES_256_CBC_SHA
#               ServerSSLV3CipherSuites TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#           ServerSSLV3CipherSuites    TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
#       }
#   }

# ServicesConnection statement
#   The Policy Agent uses the ServicesConnection statement to specify the
#   listening port, listening TCP/IP image and security level for connections
#   to this Policy Agent. Applications that use this connection are known
#   as services requestors. One such services requestor is the IBM
#   Configuration Assistant for z/OS Communications Server, also known as
#   an import requestor that uses this connection to retrieve import policies.
#
#   The Policy Agent listens for TCP connections only on the specified or
#   defaulted TCP/IP image name.
#
#   If you remove the ServicesConnection statement, all services requestor
#   connections to this Policy Agent are disconnected.
#
#   Updates to the ServicesConnection statement are used only for new services
#   requestor connections to the Policy Agent.
#
#   If you change the port value, the Policy Agent listens for new TCP
#   connections using the updated value on the specified or defaulted TCP/IP
#   image name.
#
#   If you don't configure the ServicesConnection statement, or the image
#   name is not an active TCP/IP image, the Policy Agent does not listen on
#   any port for services requestor connections.
#
#   If you want to use default values for all parameters, you can specify
#   the ServicesConnection statement without a set of braces.
#
#   If you specify Security Secure, the Policy Agent generates an AT-TLS
#   policy similar to the following example and installs it at the lowest
#   priority (lower than any configured policies) into the specified or
#   defaulted TCP/IP image after any configured local or remote AT-TLS
#   policies have already been installed.
#
#   If you update any parameters that are used in the generated policy
#   (Port, Trace or Keyring parameters), the Policy Agent reinstalls the
#   generated policy.
#
#   If you update the ImageName parameter, the Policy Agent uninstalls the
#   generated policy from the previous TCP/IP image and installs it in the
#   new image.
#
#   If you change the Security parameter from Secure to Basic, the Policy
#   Agent uninstalls the generated AT-TLS policy from the specified or
#   defaulted TCP/IP image.
#
#   To restart the listen for services requestor connections and if required
#   to reinstall the generated AT-TLS policy, issue the MODIFY SRVLSTN command.
#   See Modify command--Policy Agent in z/OS Communications Server: IP System
#   Administrator's Guide for when you might use this command.
#
# statement format:
#     ServicesConnection
#     {
#         Port                i # Listening port
#         ImageName           s # Listening TCP/IP image
#         Security            p # Connection security type
#         Trace               i # Trace value for AT-TLS policy
#         Keyring             s # Keyring name
#     }
#
# where:
#     Port                    (0): Specifies the port that the Policy
#                               Agent listens on for TCP
connections
#                               from services requestors on the
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

#	specified or defaulted TCP/IP image
name.	
#	If you are using the IBM
Configuration	
#	Assistant for z/OS Communications
Server,	
#	this port must be same as the Host
#	Connection Port specification on
the	
#	Configuration Assistant Flat File
Import	
#	request panel for any import
requestor	
#	that connects to this Policy Agent.
#	
#	The valid port values are in the
range	
#	1 - 65535. The default port value
is 16311.	
#	
#	The port value cannot match the
port value	
#	configured on the ClientConnection
statement.	
#	
# ImageName	(O): A string 1 - 8 characters in length
that	
#	specifies the TCP/IP image name.
The Policy	
#	Agent listens for services
connections only	
#	on this TCP/IP image.
#	
#	In a single stack (INET)
environment, the	
#	Policy Agent uses the active TCP/IP
image	
#	to listen for services connection
requests.	
#	
#	In a common INET (CINET)
environment, if	
#	you don't specify the TCP/IP image
name,	
#	the Policy Agent uses the default
TCP/IP	
#	image (Resolver-supplied
TCPIPuserid or	
#	TCPIPjobname). If the default
TCP/IP	
#	image cannot be determined, the
Policy	
#	Agent uses the name "INET".
#	
#	If you specify an image name that
does	
#	not have a corresponding TcpImage
or	
#	PEPInstance statement, the Policy
Agent	
#	creates an internal TcpImage
statement	
#	to represent the specified TCP/IP
image.	
#	This means you can specify only 7
(instead	
#	of 8) TcpImage or PEPInstance
statements.	
#	
#	If you specify an image name that
is not	

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

<pre># listen # until # # # Security used for # # # # # the user # services # # # Policy # # # # installs an # or # # Configuration # # # # the # # # Trace tracing # The # # associated # is # as n. # written # traces # Communications # for # # # Keyring length # key # contains the # client) # #</pre>	<pre>active, the Policy Agent does not for services requestor connections the TCP/IP image becomes active. (O): Indicates the level of security the services requestor connection. - Basic The connection does not use SSL. If you specify Security Basic, ID and password provided by the requestor flows in the clear. - Secure The connection uses SSL and the Agent installs a generated AT-TLS policy to protect the connection. Policy Agent generates and AT-TLS policy into the specified defaulted TCP/IP image. See z/OS Communications Server: IP Reference for details about the generated policy. If you specify Security Secure, Keyring parameter is required. (O): Specifies the level of AT-TLS for the generated AT-TLS policy. valid values for n are in the range 0 - 255. The sum of the numbers with each level of tracing selected the value that should be specified If n is an odd number, errors are to joblog and all other configured are sent to syslogd. See z/OS Server: IP Configuration Reference details about the trace values. (C): A string 1 - 1023 characters in specifying the ring name of the SAF ring. This key ring usually certificates of the trusted (by the Certificate Authorities.</pre>
---	--

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# If Security is configured with
Secure, then this parameter is required.
#
# If you specify Security Basic, this
parameter is ignored.
#
# example:
#   ServicesConnection
#   {
#       Port 16311
#       ImageName TCPIP1
#       Security Secure
#       Trace 2
#       Keyring USERKEYRING
#   }

# CommonIDSConfig statement
# The CommonIDSConfig statement specifies the path of a IDS
# policy file that contains common IDS policy statements. These
# common statements can be referenced from a stack specific IDS
# policy file. To define a common set of policies for multiple
# stacks, the IDSConfig statement can specify the same
# file as the CommonIDSConfig statement.
#
# Stack specific IDS policies are defined in a stack IDS
# specific policy file. A stack specific IDS policy file is
# identified by a IDSConfig statement.
#
# The refresh interval for the CommonIDSConfig file is
# inherited from the main configuration file.
#
# The CommonIDSConfig statement may only appear in the main
# configuration file.
#
# If a CommonIDSConfig statement appears multiple times in the
# main configuration file the last occurrence of the statement
# will be used. If the CommonIDSConfig statement appears in an
# image configuration file it is ignored.
#
# The configuration information defined in the file identified with
# the CommonIDSConfig statement is prepended to the
# configuration information defined in files identified with the
# IDSConfig statement. This has the following consequences:
#
# - If no IDSConfig statements are specified, then the
#   CommonIDSConfig file is not parsed by Policy Agent. The
#   IDSConfig statement is required if IDS configuration files
#   for a given stack.
# - If multiple stacks are defined, the CommonIDSConfig file is
#   parsed for each stack, so any errors contained in the file are
#   reported multiple times.
#
# statement format:
#   CommonIDSConfig s1
# where:
#   s1 (R): The path of the common
#           IDS policy file to be
#           installed.
#
# example:
#   CommonIDSConfig /usr/lpp/tcpip/samples/pagent_IDS.conf

# IDSConfig Statements
# The IDSConfig statement specifies the path of a IDS
# policy file that contains stack specific IDS policy statements.
# The IDSConfig statement is required to define IDS policy
# for a given stack. To define a common set of policies for multiple
# stacks, the IDSConfig statement can be specified with no
# path name in each image configuration file.
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
# The refresh interval for the IDSEConfig file is inherited
# from the image configuration file containing the corresponding
# IDSEConfig statement.
#
# The IDSEConfig statement may only appear in an image
# configuration file. If a IDSEConfig statement appears
# multiple times in an image configuration file the last occurrence of
# the statement will be used. If the IDSEConfig statement
# appears in the main configuration file it is ignored
# (unless the main and image configuration files are the same file).
#
# statement format:
# IDSEConfig s1 p p
# where:
# s1 (O): The path of the stack
# specific IDS policy
# file to be installed.
# If no path name is
# specified, then the
# common IDS policy file
# specified on the
# CommonIDSEConfig
# statement is used.
# p (O): FLUSH | NOFLUSH,
# default value is
# obtained from the
# corresponding TcpImage or
# PEPInstance statement.
# p (O): PURGE | NOPURGE,
# default value is
# obtained from the
# corresponding TcpImage or
# PEPInstance statement.
#
# example:
# IDSEConfig /usr/lpp/tcpip/samples/pagent_IDSE.conf FLUSH PURGE
# IDSEConfig /u/user21/TM21_IDSE.policy FLUSH PURGE

# CommonIPSecConfig statement
# The CommonIPSecConfig statement specifies the path of an IPSec
# policy file that contains common IPSec policy statements. These
# common statements can be referenced from a stack specific IPSec
# policy file. To define a common set of policies for multiple
# stacks, the IPSecConfig statement can specify the same
# file as the CommonIPSecConfig statement.
#
# Stack specific IPSec policies are defined in a stack IPSec
# specific policy file. A stack specific IPSec policy file is
# identified by an IPSecConfig statement.
#
# The refresh interval for the CommonIPSecConfig file is
# inherited from the main configuration file.
#
# The CommonIPSecConfig statement may only appear in the main
# configuration file.
#
# If a CommonIPSecConfig statement appears multiple times in the
# main configuration file the last occurrence of the statement
# will be used. If the CommonIPSecConfig statement appears in an
# image configuration file it is ignored.
#
# The configuration information defined in the file identified with
# the CommonIPSecConfig statement is prepended to the
# configuration information defined in files identified with the
# IPSecConfig statement. This has the following consequences:
#
# - If no IPSecConfig statements are specified, then the
# CommonIPSecConfig file is not parsed by Policy Agent. The
# IPSecConfig statement is required to define IPSec policy for a
# given stack.
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# - If multiple stacks are defined, the CommonIpSecConfig file is
#   parsed for each stack, so any errors contained in the file are
#   reported multiple times.
#
# statement format:
#   CommonIPSecConfig    s1
# where:
#   s1                                (R): The path of the common
#                                       IPsec policy file to be
#                                       installed.
#
# example:
#   CommonIPSecConfig /usr/lpp/tcpip/samples/pagent_CommonIPSec.conf

# IPsecConfig Statements
# The IpSecConfig statement specifies the path of an IPsec
# policy file that contains stack specific IPsec policy statements.
# The IpSecConfig statement is required to define IPsec policy
# for a given stack. To define a common set of policies for multiple
# stacks, the IpSecConfig statement can be specified with no
# path name.
#
# The refresh interval for the IpSecConfig file is inherited
# from the image configuration file containing the corresponding
# IpSecConfig statement.
#
# The IpSecConfig statement may only appear in an image
# configuration file. If an IpSecConfig statement appears
# multiple times in an image configuration file the last occurrence of
# the statement will be used. If the IpSecConfig statement
# appears in the main configuration file it is ignored
# (unless the main and image configuration files are the same file).
#
# statement format:
#   IPsecConfig          s1
# where:
#   s1                                (O): The path of the stack
#                                       specific IPsec policy
#                                       file to be installed.
#                                       If no path name is
#                                       specified, then the
#                                       common IPsec policy file
#                                       specified on the
#                                       CommonIpSecConfig
#                                       statement is used.
#
# example:
#   IPsecConfig /usr/lpp/tcpip/samples/pagent_IPSec.conf
# IPsecConfig /u/user21/TM21_IPFilter.policy
# IPsecConfig /u/user21/TM21_IPSecVPN.policy
# IPsecConfig /u/user21/TM21_IPSecVPN_wPreshare.policy
# IPsecConfig /u/user21/TM21_IPSecVPN_wIKEv2.policy

# CommonRoutingConfig statement
#
# Use the CommonRoutingConfig statement to specify the path of a local
# Routing policy file that contains common Routing policy statements.
# These common statements can be referenced from a stack-specific
# Routing policy file. To define a common set of policies for multiple
# stacks, use the RoutingConfig statement to specify the same file as
# the CommonRoutingConfig statement.
#
# Stack-specific Routing policies are defined in a stack-specific
# Routing policy file. A stack-specific Routing policy file is
# identified by a RoutingConfig statement.
#
# The refresh interval for the CommonRoutingConfig file is inherited
# from the main configuration file.
#
# Restriction: The CommonRoutingConfig statement can appear only in the
# main configuration file.
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
# If a CommonRoutingConfig statement appears multiple times in the main
# configuration file, the last occurrence of the statement is used.
# If the CommonRoutingConfig statement appears in an image configuration
# file, it is ignored.
#
# The configuration information defined in the file identified with the
# CommonRoutingConfig statement is prepended to the configuration
# information defined in files identified with the RoutingConfig
# statement. This action has the following consequences:
#
# - If no RoutingConfig statements are specified, then the
#   CommonRoutingConfig file is not parsed by Policy Agent.
#
# Requirement: The RoutingConfig statement is required if Routing
# configuration files exist for a given stack.
# - If multiple stacks are defined, the CommonRoutingConfig file is
#   parsed for each stack; thus, any errors contained in the file are
#   reported multiple times.
#
# statement format:
#   CommonRoutingConfig    s1
# where:
#   s1                      (R):  The path of the common
#                                Routing policy file to be
#                                installed.
#
# example:
#   CommonRoutingConfig /usr/lpp/tcpip/samples/pagent_Routing.conf

# RoutingConfig Statements
# Use the RoutingConfig statement to specify the path of a local
# Routing policy file that contains stack-specific Routing policy
# statements.
#
# Requirement: The RoutingConfig statement is required to define
# Routing policy for a given stack.
#
# Results:
#   For the associated TCP/IP image on the policy client, if the
#   PolicyServer statement specifies remote Routing policies, then
#   the following occurs:
#   - If no local Routing policies are installed, then the
#     RoutingConfig statement is ignored.
#   - If local Routing policies are already installed, then this is
#     treated as if the RoutingConfig statement has been deleted.
#
# Specify the RoutingConfig statement with no path name in each image
# configuration file to define a common set of policies for multiple
# stacks.
#
# The refresh interval for the RoutingConfig file is inherited from
# the image configuration file containing the corresponding
# RoutingConfig statement.
#
# Restriction: The RoutingConfig statement can appear only in an image
# configuration file.
#
# If a RoutingConfig statement appears multiple times in an image
# configuration file, the last occurrence of the statement is used.
# If the RoutingConfig statement appears in the main configuration
# file, it is ignored (unless the main and image configuration files
# are the same file).
#
# statement format:
#   RoutingConfig    s1
# where:
#   s1                (O):  The path of the stack
#                           specific Routing policy
#                           file to be installed.
#                           If no path name is
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# specified, then the
# common Routing policy file
# specified on the
# CommonRoutingConfig
# statement is used.
#
# example:
#   RoutingConfig /usr/lpp/tcpip/samples/pagent_Routing.conf

# CommonTLSConfig statement
# The CommonTLSConfig statement specifies the path of a TLS
# policy file that contains common TLS policy statements. These
# common statements can be referenced from a stack specific TLS
# policy file. To define a common set of policies for multiple
# stacks, the TLSConfig statement can specify the same
# file as the CommonTLSConfig statement.
#
# Stack specific TLS policies are defined in a stack TLS
# specific policy file. A stack specific TLS policy file is
# identified by a TLSConfig statement.
#
# The refresh interval for the CommonTLSConfig file is
# inherited from the main configuration file.
#
# The CommonTLSConfig statement may only appear in the main
# configuration file.
#
# If a CommonTLSConfig statement appears multiple times in the
# main configuration file the last occurrence of the statement
# will be used. If the CommonTLSConfig statement appears in an
# image configuration file it is ignored.
#
# The configuration information defined in the file identified with
# the CommonTLSConfig statement is prepended to the
# configuration information defined in files identified with the
# TLSConfig statement. This has the following consequences:
#
# - If no TLSConfig statements are specified, then the
#   CommonTLSConfig file is not parsed by Policy Agent. The
#   TLSConfig statement is required to define TLS policy for a
#   given stack.
# - If multiple stacks are defined, the CommonTLSConfig file is
#   parsed for each stack, so any errors contained in the file are
#   reported multiple times.
#
# statement format:
#   CommonTLSConfig    s1
# where:
#   s1                                (R): The path of the common
#                                       TLS policy file to be
#                                       installed.
#
# example:
#   CommonTLSConfig /usr/lpp/tcpip/samples/pagent_TLS.conf

# TLSConfig Statements
# The TLSConfig statement specifies the path of a TLS
# policy file that contains stack specific TLS policy statements.
# The TLSConfig statement is required to define TLS policy
# for a given stack. To define a common set of policies for multiple
# stacks, the TLSConfig statement can be specified with no
# path name.
#
# The refresh interval for the TLSConfig file is inherited
# from the image configuration file containing the corresponding
# TLSConfig statement.
#
# The TLSConfig statement may only appear in an image
# configuration file. If a TLSConfig statement appears
# multiple times in an image configuration file the last occurrence of
# the statement will be used. If the TLSConfig statement
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# appears in the main configuration file it is ignored
# (unless the main and image configuration files are the same file).
#
# statement format:
#     TTLSConfig      s1      p      p
# where:
#     s1                                (O): The path of the stack
#                                         specific TTLS policy
#                                         file to be installed.
#                                         If no path name is
#                                         specified, then the
#                                         common TLS policy file
#                                         specified on the
#                                         CommonTTLSConfig
#                                         statement is used.
#     p                                (O): FLUSH | NOFLUSH,
#                                         default value is
#                                         obtained from the
#                                         corresponding TcpImage or
#                                         PEPInstance statement.
#     p                                (O): PURGE | NOPURGE,
#                                         default value is
#                                         obtained from the
#                                         corresponding TcpImage or
#                                         PEPInstance statement.
#
# example:
#     TTLSConfig /usr/lpp/tcpip/samples/pagent_TTLS.conf FLUSH PURGE
#     TTLSConfig /u/user21/TM21_ATTLS_FTPandTN3270.policy FLUSH PURGE
#     TTLSConfig /u/user21/TM21_ATTLS_wNSS.policy FLUSH PURGE

# QOSConfig Statement
# The QOSConfig statement specifies the path of a QoS
# policy file that contains stack specific QoS policy statements.
# The QOSConfig statement is optional. Two methods can be used
# to define QoS policy for a given stack:
#
# 1) Specify the QOSConfig statement in the image configuration
# file, and specify the QoS policy statements in the file
# specified on the QOSConfig statement.
#
# 2) Specify the QoS policy statements directly in the image
# configuration file, without specifying the QOSConfig
# statement.
#
# The refresh interval for the QOSConfig file is inherited
# from the image configuration file containing the corresponding
# QOSConfig statement.
#
# The QOSConfig statement may only appear in an image
# configuration file. If a QOSConfig statement appears
# multiple times in an image configuration file the last occurrence of
# the statement will be used. If the QOSConfig statement
# appears in the main configuration file it is ignored
# (unless the main and image configuration files are the same file).
#
# statement format:
#     QOSConfig      s1
# where:
#     s1                                (O): The path of the stack
#                                         specific QoS policy
#                                         file to be installed.
#
# example:
#     QOSConfig /u/user10/pagent_QoS.conf

# ReadFromDirectory Statement
# This statement initializes the LDAP client so that the rules will be
# downloaded from the LDAP server in addition to being read from this
# configuration file.
#
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

# statement format:
#   ReadFromDirectory
#   {
#       LDAP_Server                (a|s) # Name or IPv4 address of the
directory server.
#       LDAP_Port                  i # The port of the directory server.
#       LDAP_BackupServer          (a|s) # Name or IPv4 address of the
backup directory
#                                   # server.
#       LDAP_BackupPort            i # The port of the backup directory
server.
#       LDAP_DistinguishedName     l # LDAP logon id.
#       LDAP_Password              s # LDAP logon password.
#       LDAP_SSL                   # LDAP SSL security specification.
#       {
#           LDAP_SSLKeyringFile     s # SSL key ring file specification.
#           LDAP_SSLKeyringPassword s # Password to the key ring file.
#           LDAP_SSLName            s # Key ring label name.
#       }
#       LDAP_SessionPersistent     p # Should the LDAP session with the
server
#                                   # be kept open?
#       LDAP_ProtocolVersion        3 # LDAP protocol version.
#       LDAP_SchemaVersion          1|2|3 # Policy schema version.
#       Base                        l # The base to look up policies from
the server
#                                   # (for version 1 policies).
#       LDAP_SelectedTag            s # A tag to select policies for this
host
#                                   # (for version 1 policies).
#       LDAP_AbstractPolicy         p # Whether or no abstract policy
searching is
#                                   # supported by the LDAP server.
#       SearchPolicyBaseDN          l # The base to look up policies from
the server
#                                   # (for version 2 and up policies).
#       SearchPolicyKeyword          s # Search keyword for policy objects
#                                   # (for version 3 policies).
#       SearchPolicyGroupKeyWord     s # Search keyword for policy group
objects
#                                   # (for version 2 and up policies).
#       SearchPolicyRuleKeyWord      s # Search keyword for policy rule
objects
#                                   # (for version 2 and up policies).
#       PolicyRole                  s # Roles or role-combinations played
by this
#                                   # LDAP client (i.e. Policy Agent).
#   }
# where:
#       LDAP_Server                (O): LDAP_Server is the domain name or
the IPv4
#                                   address of the directory server.
#                                   does not specify this value, the
If the user
#                                   is the local host which is
#       LDAP_Port                  (O): LDAP_Port is the port on which the
default
#                                   directory server is running. If
#                                   does not specify this value, the
127.0.0.1.
#                                   LDAP port of 389 is used.
#       LDAP_BackupServer          (O): Domain name or IPv4 address of the
#                                   backup directory server. This is
used
#                                   when Pagent can't contact the
#                                   primary
primary

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

# server. Default is no backup
server.
#
# LDAP_BackupPort (O): The port on which the backup
directory server is running. Default is 389.
#
# LDAP_DistinguishedName (C): The Distinguished Name for userid
to be used when connecting to the LDAP
server. If this attribute is not
specified, anonymous userid is used for the
connect. If this attribute is specified,
LDAP_Password must also be
specified. Case sensitivity is determined by the
LDAP server.
#
# LDAP_Password (C): The password to be used when
connecting to the LDAP server. If this
attribute is specified. LDAP_DistinguishedName
must also be specified.
#
# LDAP_SSLKeyringFile (C): The name of the keyring file, which
contains the certificates trusted
by the client. The file may also contain
a public key and certificate. This
parameter is required if LDAP_SSL is
specified.
#
# LDAP_SSLKeyringPassword (O): The password of the keyring file.
The password is set using the gskkyman
tool.
#
# LDAP_SSLName (O): The label assigned to your private
key / certificate pair, created with the
gskkyman tool.
#
# LDAP_SessionPersistent (O): LDAP_SessionPersistent is YES|NO
that indicates if the session with the
LDAP server should be kept open or not,
for the purpose of querying for updates at
the interval specified on the TcpImage
statement. If this interval is small, the
value of keeping the session opened is
greater, to reduce the overhead of opening the
session for each query. The default is
NO.
#
# LDAP_ProtocolVersion (O): LDAP protocol version to be used.
Supported

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

<pre> # # # LDAP_SchemaVersion Version 1 is for # to CS # policy # Version 3 # V1R2. # # # Base the # policies # required # # # LDAP_SelectedTag which can # policies # value is not # by # This # version 1 # # # LDAP_AbstractPolicy Choose YES # are # for abstract # otherwise. # # searching the # objectClass=* # is YES. # # SearchPolicyBaseDN subtree under # defined # This parameter # and up. # the LDAP # # # SearchPolicyKeyword objects # allowed # used in </pre>	<pre> version is 3. Default is 3. (O): LDAP Policy schema version. policy schemas from releases prior for OS390 V2R10. Version 2 is for schemas for CS for OS390 V2R10. is for policy schemas as of OS390 Default is 3. (C): Base is the distinguished name of subtree in the directory where the are located. This parameter is with schema version 1. (O): LDAP_SelectedTag is any string be used to select a subset of the under the base tree. If this specified, the first name returned gethostname() is used as the tag. parameter is used in searching schema. (O): LDAP_AbstractPolicy is YES NO. for LDAP version 3 servers that capable of matching objectClass and auxiliary classes. Choose NO When YES is chosen, Pagent uses objectClass=ibm-policy when server. Otherwise, it uses (all object classes). The default (C): The distinguished name of the which to find policies that are with schema version 2 and up. is required with schema version 2 Case sensitivity is determined by server. (O): Keyword used to search for policy under the subtree. This is only with version 3 schema and it is </pre>
---	--

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

#	the initial search. Up to 8
instances of	
#	this attribute can be specified.
This value	
#	is matched against the
policyKeywords	
#	attribute in the policy rules.
Case	
#	sensitivity is determined by the
LDAP server.	
#	
# SearchPolicyGroupKeyWord	(O): Keyword used to search for policy
groups under	
#	the subtree (e.g., search
scoping). This is	
#	only allowed with version 2 and up
schema and	
#	it is used in the initial search.
Up to 8	
#	instances of this attribute can be
specified.	
#	This value is matched against the
#	policyGroupKeywords attribute in
the policy	
#	groups. Case sensitivity is
determined	
#	by the LDAP server.
#	
# SearchPolicyRuleKeyWord	(O): Keyword used to search for policy
rules under	
#	the subtree. This is only allowed
with	
#	version 2 and up schema and it is
used in the	
#	initial search. Up to 8 instances
of this	
#	attribute can be specified. This
value is	
#	matched against the
policyRuleKeywords	
#	attribute in the policy rules.
Case	
#	sensitivity is determined by the
LDAP server.	
#	
# PolicyRole	(O): Specifies a policy role or role-
combination	
#	(see below). Use this parameter
to filter	
#	the policy rules to be retrieved.
This	
#	parameter is only valid with
schema version	
#	3. This parameter can be repeated
as many	
#	times as necessary. Either a
single role or	
#	a set of roles, known as a role-
combination,	
#	may be specified. The roles may
be single	
#	words, or any strings containing
blanks or	
#	other special characters,
contained in	
#	double quotes. Role-combinations
are	
#	specified as follows. The first
role is	
#	specified the same way that a
single role is	

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# specified. Each additional role
in the role-combination is prefixed with
#
the characters "&&". For example:
# PolicyRole role1
# PolicyRole &&"quoted role 2"
# PolicyRole "quoted role 3"
# PolicyRole role4
# This parameter is used to filter
out policy rules that don't contain any of
# the specified roles or role-
# combinations, using the attribute ibm-policyRoles.
# For example, the set of roles specified above
# result in the retrieval of any policy rules
# that specify "role1&&quoted role 2" or
# "quoted role3" or "role4" in their
policyRoles values.
#
# Note: If the LDAP server being used is an z/OS LDAP server prior to Version 2 Release
10 then
# only one of the parameters SearchPolicyGroupKeyWord or SearchPolicyRuleKeyWord
may be used.
# If both parameters are used the LDAP server will not return any policy
information.
#
#
# example: ReadFromDirectory
# {
#     LDAP_Server 9.10.11.12
#     LDAP_Port 9000
#     LDAP_DistinguishedName cn=root, o=IBM, c=US
#     LDAP_Password secret
#     LDAP_ProtocolVersion 3
#     LDAP_SchemaVersion 3
#     SearchPolicyBaseDN cn=group5, o=IBM, c=US
# }

# PolicyPerfMonitorForSDR Statement
# This statement is used to enable/disable (without this statement, this
# function is turned off) the policy performance monitor function that
# assigns a QoS weight fraction to the monitored policy performance data and
# sends messages to the Sysplex Distributor (SD) routing component as the
# monitored data crosses its defined thresholds. SD uses this weight
# fraction to influence its routing decision on the incoming connection
# requests to appropriate hosts within a group that is responsible for
# processing the request. The QoS weight fraction is used by SD to reduce
# the availability factor that SD obtains from the Work Load Manager (WLM).
# For instance, assume the WLM weight (available processing capacity) is 64 and
# the QoS performance monitor detects a significant loss rate over the network
# from the corresponding node in the sysplex. Also assume that the QoS
# weight fraction is 50%: the resulting weight used in routing incoming
# connection requests to that node is now only 32 (64x0.5) instead of 64.
# This weight adjustment results in balancing the work load in the sysplex
# taking into account both the node processing capacity and the QoS
# performance over the network.
#
# Note that there must exist at least one policy rule definition that covers
# the application whose incoming connection request is being routed by SD.
# The policy rule(s) enables the collection of the performance data. This
# function only works with TCP since other IP transports contain data
# retransmission and error recovery. Also, if IDS TR policies
# exist that cover the application, and if a limit on the total connections
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# is defined, then when the total active connections for that application
# reaches the constrained state (i.e. 90% of the defined total), the QOS weight
# fraction will be set to 100%. This will divert incoming connection
# requests for the application away from the corresponding target node.
#
# statement format:
#     PolicyPerfMonitorForSDR      Enable/Disable # Default is Disable. If Enable,
#                                     # the following parameters can
#                                     # be specified.
#
#     {
#         SamplingInterval          i # How often to sample the policy
#                                     # performance information.
#         LossRatioAndWeightFr      i i # The first number is the unit
ratio of                                # retransmitted bytes (loss) over
#                                     # transmitted bytes; the second is
#                                     # the weight fraction to be
assigned.
#         LossMaxWeightFr          i # Maximum weight fraction to be
assigned.
#         TimeoutRatioAndWeightFr  i i # The first number is the unit
ratio of                                # the number of timeouts over
#                                     # total packets transmitted; the
second                                # is the weight fraction to be
#                                     #
assigned.
#         TimeoutMaxWeightFr       i # Maximum weight fraction to be
assigned.
#     }
# where:
#     SamplingInterval              (O): In units of seconds. Default is 60
seconds.
#     LossRatioAndWeightFr          (O): Loss (Retransmission) Ratio is in
units of                                tenths of a percent (1-1000) and
#                                     weight fraction is in percentage
the                                     (1-100%). Default is 10 and 10,
#                                     unit loss ratio corresponds to 10%
units
#                                     A weight fraction of 0 means to
meaning 1%
#                                     loss ratio factor in SD routing.
fraction.
#                                     (O): Weight fraction is added or
suppress
#                                     as the ratio exceeds the next unit
#                                     retreats to the lower unit. If
#                                     monitored loss ratio increases
#                                     the weight fraction exceeds the
#                                     only maximum weight fraction is
#                                     Default is 100, or 100%.
#     TimeoutRatioAndWeightFr      (O): Time out Ratio is also in units of
tenths of                                a percent and the weight fraction
#                                     percentage. Default is 10 and 20,
#                                     respectively. A weight fraction
#                                     of 0 means
#                                     to suppress timeout ratio factor
#                                     in SD
#                                     routing.
#     TimeoutMaxWeightFr           (O): Default is 100%.
#
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# example: PolicyPerfMonitorForSDR    Enable
#
#       {
#           SamplingInterval            120
#           LossRatioAndWeightFr       10 20
#           LossMaxWeightFr            100
#           TimeoutRatioAndWeightFr    5 50
#           TimeoutMaxWeightFr         100
#       }
#
# In this example, Pagent will send to SDR a message when the loss
# (retransmission) ratio begins to exceed 1% but not above 2%, with
# a weight fraction of 20% (this means that the WLM weight will be
# decreased by 20% before it is used as a measure to route incoming
# connection requests). When the loss (retransmission) ratio exceeds
# 2% but not above 3%, a message is sent with a weight fraction of 40%,
# and so on. When the loss exceeds 5%, a maximum weight fraction of 100%
# will be used. The same with the timeout ratio. When the timeout ratio
# exceeds 0.5% but not above 1%, a weight fraction of 50% is added to
# QoS fraction in the message sent to SD. And so on.

# PolicyPerformanceCollection Statement
# This statement is used to enable/disable the policy performance collection
# function. Without this statement, this function is turned off by default.
# When enabled, the Policy Agent collects performance data from the kernel
# and caches it. This performance data is then made available to user
# applications through the Policy API (PAPI). This data can also be
# optionally logged to a performance log file for offline performance
# analysis.
#
# statement format:
#       PolicyPerformanceCollection Enable/Disable # Default is Disable.
#       {
#           DataCollection                p+ # Specifies the type of performance
#                                           # data that needs to be collected.
#           MinimumSamplingInterval       i # The minimum time at which
performance                                     # data will be collected from the
kernel                                           # data will be collected from the
#           LogSamplingInterval           i # The time at which performance
data will                                       # be collected from the kernel and
#                                           # logged
logged                                       # into the performance log file.
#           PerformanceLogFile            s # Specifies the name of the file to
which                                           # performance data needs to be
logged.                                       #
#           NumberOfLogFiles              i # Specifies the number of
performance log                               # files to be maintained.
#           SizeOfLogFile                 i # Specifies the size of each log
file.                                         #
#       }
# where:
#       DataCollection                    (O): Specifies the type of performance
data that                                     will be collected. The values
#                                           could be
#                                           RULE or ACTION. Default is RULE.
#           MinimumSamplingInterval       (O): In seconds. Value ranges from 30 to
#                                           2147483647. Default is 30.
#           LogSamplingInterval           (C): In seconds. Value ranges from 30 to
#                                           2147483647. If LogSamplingInterval
is                                           specified then PerformanceLogFile
#                                           needs
#                                           to be specified.
#           PerformanceLogFile            (C): Specifies the name of the log file.
#                                           PerformanceLogFile needs to be
specified
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
# if LogSamplingInterval is
specified.
#      NumberOfLogFiles      (O): Ranges from 1 - 255. Default is 3.
#      SizeOfLogFile         (O): In kilobytes (Kb). Value ranges
from 1 -
#                               1000000Kb. Default is 300 Kb.
#
# example: PolicyPerformanceCollection  Enable
#          {
#              DataCollection            RULE ACTION
#              MinimumSamplingInterval  60
#              LogSamplingInterval      60
#              PerformanceLogFile       /tmp/perfdata.log
#          }
#
# In this example, Pagent will collect the performance data from the
# kernel every 60 seconds and will log the performance data to the
# performance log file (/tmp/perfdata.log) every 60 seconds.

# SetSubnetPrioTosMask Statement
# This statement defines the TOS/priority field in the IP header type of
# service byte. It is used by the TCP/IP stack to read the TOS value and
# assign appropriate service to the corresponding IP packets. If this
# statement is not specified, TCP/IP will use the system default TOS mask
# and priority levels for all interfaces currently defined for IPv4
# (RFC 791). Note that there is an alternate definition for the TOS
# byte referred to as the DS (Differentiated Services) byte, see RFC 2474
# for details. This statement can be used to support the DS byte format.
# statement format:
#     SetSubnetPrioTosMask
#     {
#         SubnetAddr             a # Subnet IP address.
#         SubnetTosMask          b # TOS mask to obtain priority
level.
#         PriorityTosMapping      B b B # Priority level, corresponding
TOS,
#                               # and optional user priority.
#     }
# where:
#     SubnetAddr                (O): Is the local subnet interface
address.
#                               Default is 0, meaning the mask is
the same
#                               for all interfaces.
#     SubnetTosMask             (R): The TOS mask (e.g., 11100000).
#     PriorityTosMapping        (O): This key can be repeated for each
priority
#                               level to Tos value mapping. For
example:
#                               PriorityTosMapping 0 0
#                               PriorityTosMapping 1 01000000
#
#                               The third parameter is the user
priority,
#                               which is also known as the VLAN
#                               and is an optional parameter.
#                               This allows the Virtual LAN (VLAN)
user
#                               priority to be set for those
devices
#                               that support tagging of VLAN
frames.
#
# CAUTION: The coding of the user priority (third parameter) will
# cause the frame to be sent out based on the IEEE 802.1Q
# specification which establishes a standard method for tagging
# Ethernet frames with VLAN priority and membership information.
# Specifically, VLAN priority tagged frame is used to convey packet
# priority to the switches, and has NULL for VLANID. A full VLAN
# tagged frame supported as of CS for z/OS V1R5 contains both the
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# priority and non-NULL VLANID. If you have switches in your
# network that DO NOT support the IEEE 802.1Q standard (either VLAN
# priority tagged frames or full VLAN tagged frames) or are not
# properly configured for this frame, the frame may be dropped by
# the switch.
#
# example: SetSubNetPrioTosMask
#
#         SubnetTosMask      11100000
#         PriorityTosMapping  1 1110000 7
#         PriorityTosMapping  1 1100000 6
#         PriorityTosMapping  2 1010000 5
#         PriorityTosMapping  2 1000000 4
#         PriorityTosMapping  3 0110000 3
#         PriorityTosMapping  3 0100000 2
#         PriorityTosMapping  4 0010000 1
#         PriorityTosMapping  4 0000000 0
#
#     }
#
SetSubNetPrioTosMask
{
    SubnetTosMask      11100000
    PriorityTosMapping  1 1110000
    PriorityTosMapping  1 1100000
    PriorityTosMapping  2 1010000
    PriorityTosMapping  2 1000000
    PriorityTosMapping  3 0110000
    PriorityTosMapping  3 0100000
    PriorityTosMapping  4 0010000
    PriorityTosMapping  4 0000000
}

# PolicyAction Statement
# This statement specifies the QoS that a flow of IP packets
# (e.g., from a TCP connection, or UDP data) should receive end-to-end
# as they traverse the network. In addition to QoS, this statement
# can also be used to specify Traffic Regulation Management action to
# be performed by TCP/IP for a target application specified in the
# policyRule.
#
# statement format:
#     policyAction          s # Policy action name.
#     {
#         PolicyScope        p # Type of action to be performed.
#         Permission         p # If packets belonging to this
#                               # action should be discarded
#                               # or allowed to proceed.
#         MaxRate            i # Maximum rate/throughput per TCP
#                               # connection allowed for traffic
#                               # in this action.
#         MinRate            i # Minimum rate/throughput per TCP
#                               # connection allowed for traffic
#                               # in this action.
#         MaxDelay           i # Maximum end-to-end delay time.
#                               # Result: MaxDelay parameter is no
#                               # longer supported and
#                               # will be ignored.
#         OutgoingTOS        b # TOS/DS value of outbound traffic
#                               # belonging to this action.
#         MaxConnections     i # Maximum number of end-to-end TCP
#                               # connections at any instance of
#                               # for this action.
#         OutboundInterface  a # Sysplex Distributor routing
#                               # The following are leaky bucket
#                               # conditioning parameters:
#         DiffServInProfileRate i # Token generation rate.
#         DiffServInProfilePeakRate i # Leaky bucket peak rate.
#         DiffServInProfileTokenBucket i # Burst size.
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#           DiffServInProfileMaxPacketSize           i # Peak rate max packet size.
#           DiffServOutProfileTransmittedTOSByte      b # TOS/DS for out-of-profile
#                                                     # traffic.
#           DiffServExcessTrafficTreatment            p # Treatment for out-of-profile
traffic.
#                                                     # The following are RSVP
parameters:
#           InboundScope                             p # Inbound QoS service type.
#           AverageConnectionRate                     i # Average new inbound connections
per
#                                                     # second.
#           ConnectionBurstSize                       i # Maximum number of new concurrent
#                                                     # inbound connections.
#           PeakConnectionRate                        i # Peak rate of inbound connection
#                                                     # token bucket conditioner.
#           AverageApplicationRate                     i # Average new application requests
#                                                     # per second.
#           AverageApplicationRequestRate              i # Synonym for
AverageApplicationRate.
#           ApplicationBurstSize                       i # Maximum number of new concurrent
#                                                     # application requests.
#           ApplicationRequestBurstSize                 i # Synonym for ApplicationBurstSize.
#           ApplicationPeakRate                       i # Peak rate of application request
#                                                     # token bucket conditioner.
#           ApplicationRequestPeakRate                 i # Synonym for ApplicationPeakRate.
#           PrioritizedQueue                          p # Order of processing inbound
#                                                     # connections.
#           InboundAcceptQueueID                      s # Identifier of accept queue
#                                                     # for inbound traffic.
#           FlowServiceType                           p # Type of RSVP reserved traffic.
#           MaxRatePerFlow                             i # Maximum rate a flow in this
service
#                                                     # category is allowed to reserve.
#           MaxTokenBucketPerFlow                     i # Maximum token bucket size per
flow.
#           MaxFlows                                  i # Maximum number of reserved flows.
#           SignalClient                             p # Enable RSVP for TCP/UDP
connection.
#           NumberOfAcceptQueues                      i # Number of accept queue
configuration
#                                                     # policy queues.
#           AcceptQueueIDandWeight                    s i # Identifier and weight for one of
the
#                                                     # accept queue configuration policy
#                                                     # queues.
#           DefaultAcceptQueueID                      s # Default accept queue identifier
for
#                                                     # accept queue configuration
policy.
#       }
#       where:
#           s
#
#           PolicyScope                               (R): Is the name of this policy action
#                                                     (up to 32 characters, truncated if
#                                                     longer).
#           (O): DataTraffic | RSVP | Both
#               Default is Both, which means both
#               DataTraffic and RSVP.
#           Permission                                (O): Allowed | Blocked, default is
Allowed.
#           MaxRate                                    (O): in Kbps (K bits per second),
default is
#               infinite.
#           MinRate                                    (O): In Kbps, default is zero.
#           MaxDelay                                    (O): Default is non-specified
(infinite).
#
#               # Result: MaxDelay parameter is no
#               # longer supported and
#               # will be ignored.
#           OutgoingTOS                                (O): Default is 0.
#           MaxConnections                            (O): Default is non-specified
(infinite).

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
# OutboundInterface (0): Sysplex Distributor routing
interfaces. Up to 32 instances of this
# attribute may be specified. If 0 is specified,
# then the SD routing component can use any
# available target server if the target
# servers identified with instances of this
# attribute are not available. Default is no
# policy control of Sysplex Distributor
# routing interfaces. Only IPv4 addresses
# can be specified.
# DiffServInProfileRate (C): In Kbps, specifies the mean rate
(token generating rate) of a token bucket
# traffic conditioner that enforces the rate
# of traffic that is mapped to the
# corresponding policy action by a policy rule. If
# the traffic exceeds this rate, it will
# be considered as out-of-profile and
# therefore will be treated with the action
# specified in DiffServExcessTrafficTreatment
# attribute. If this value is non-zero, but
# DiffServInProfileTokenBucket
# attribute is zero, then no token bucket traffic
# enforcement is performed.
# DiffServInProfilePeakRate (C): In Kbps, specifies the peak rate of
a token bucket traffic conditioner that
# enforces the peak rate of traffic that is
# mapped to the corresponding policy action by
# a policy rule. If the traffic
# exceeds this rate, it will be considered as out-
# of-profile and therefore will be treated with
# the DiffServExcessTrafficTreatment
# attribute. If this value is non-zero, but
# DiffServInProfileMaxPacketSize or
# DiffServInProfileRate attribute is
# zero, then no token bucket peak rate enforcement is
# performed. If this value is less than
# DiffServInProfileRate attribute, then no token bucket
# traffic or peak rate enforcement is performed.
#
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

# DiffServInProfileTokenBucket (C): In Kb, specifies the maximum burst
size of
#
# a token bucket traffic conditioner
# that enforces the burst of traffic
# that is mapped to the corresponding
# policy action by a policy rule. It
# is used together with the mean rate
# in generating tokens consumed by
outgoing
#
# traffic.
# DiffServInProfileMaxPacketSize (C): In Kb, specifies the maximum size
of an
#
# IP packet being enforced by a token
# bucket traffic conditioner. Note
# that due to blocking in S/390,
# multiple packets tend to be sent
# back to back and if maximum packet
# size is just big enough for one
# packet, violation of the peak rate
# (peak rate enforcement is based on
# the size of each individual packet)
# will result and violated packets
# will be sent with different TOS
value
#
# or dropped as a consequence. To
# accommodate this blocking, the
value
#
# of this attribute should be set in
# multiples of the maximum packet
size
#
# (e.g., equal to the token bucket
size).
# DiffServOutProfileTransmittedTOSByte (O): Specifies the TOS value to
#
# be used for out-of-profile traffic
# if the excess treatment specified
is
#
# to send them as best effort.
# DiffServExcessTrafficTreatment (O): Drop | BestEffort | Shape
#
# Specifies how a token bucket
# traffic conditioner should treat
# out-of-profile traffic. Two
options
#
# can be specified, either Drop or
# BestEffort. If treatment is to
send
#
# BestEffort, a different TOS value,
# if specified, will be used. If
# treatment is to Drop, depending on
# whether the traffic is UDP or TCP
# different mechanisms will be used
to
#
# handle Drop treatment:
#
# For UDP, traffic will actually be
# dropped.
#
# For TCP, Drop treatment is
simulated
#
# in that TCP congestion window is
# cut (just as the case when a
# packet is dropped) immediately
# but the violated packet will be
# sent. This is to avoid overhead
# associated with retransmission
# processing and also to reduce
# the traffic generated immediately
# without having to wait for a
# roundtrip time (i.e., standard TCP
# lost detection delay). Also, TCP
# connections that are mapped to the
# same policy (i.e., aggregation)
# will share the throughput equally
# among them.

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#           InboundScope                               (O): Connection | Application
#                                                     Identifies the type of inbound QoS
#                                                     service that the corresponding
policy
#                                                     action specifies. It can be either
#                                                     Application (for a named
application)
#                                                     or Connection (for general TCP
#                                                     connections). Based on the inbound
#                                                     scope, a set of corresponding
#                                                     parameters can be applied for the
#                                                     traffic that is mapped to the
policy
#                                                     action. This attribute is
extendable
#                                                     to other applications.
#           AverageConnectionRate                       (O): In Kbps, specifies the average
number
#                                                     of new requests (connections)
#                                                     admitted per second. If either the
#                                                     AverageConnectionRate or
#                                                     ConnectionBurstSize attribute is
#                                                     not in profile then the inbound
#                                                     connection will be <Drop>.
#           ConnectionBurstSize                         (O): In Kb, specifies the maximum
#                                                     number of new requests
#                                                     accepted concurrently. If either
#                                                     the AverageConnectionRate or
#                                                     ConnectionBurstSize attribute is
not
#                                                     in profile then the inbound
connection
#                                                     will be <Drop>.
#           PeakConnectionRate                         (O): In Kbps, specifies the peak rate of
a
#                                                     token bucket traffic conditioner
#                                                     that enforces the peak rate of
#                                                     traffic that is mapped to the
#                                                     corresponding inbound policy action
#                                                     by a policy rule. If the number
#                                                     of connections exceeds this rate,
it
#                                                     will be considered as out-of-
#                                                     profile
#                                                     and therefore will be treated is if
#                                                     the DiffServExcessTrafficTreatment
#                                                     attribute was set to <Drop>.
#           AverageApplicationRate
#           AverageApplicationRequestRate               (O): In Kbps, specifies the average
number
#                                                     of new application requests
#                                                     per second. If either the
#                                                     AverageApplicationRequestRate
#                                                     or ApplicationRequestBurstSize
#                                                     attribute is not in profile then
the
#                                                     inbound request will be <Drop>.
#           ApplicationBurstSize
#           ApplicationRequestBurstSize                 (O): In Kb, specifies the maximum number
of
#                                                     new application requests accepted
#                                                     concurrently. If either the
#                                                     AverageApplicationRequestRate or
#                                                     ApplicationRequestBurstSize
#                                                     attribute is not in profile then
#                                                     the inbound request will be <Drop>.
#           ApplicationPeakRate
#           ApplicationRequestPeakRate                 (O): In Kbps, specifies the peak rate of
a

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

# token bucket traffic conditioner
# that enforces the peak rate of
# traffic that is mapped to the
# corresponding inbound policy
# action by a policy rule. If
# the number of application
# requests exceeds this rate,
# it will be considered
# out-of-profile and the inbound
# application request will be
# <Drop>.
# PrioritizedQueue (O): 1 | 2 | 3 | 4
# Specifies the order the queue of
# the server processes incoming
# connections. If the incoming
# packet is within the profiles
# limits then each connection
# will be served by one of 3
# priorities.
# InboundAcceptQueueID (O): Identifies accept queue to use for
inbound traffic. Accept queue is
# configured with an accept queue configuration
# policy.
# FlowServiceType (O): ControlledLoad | Guaranteed,
# default is ControlledLoad. Guaranteed is
# considered greater than ControlledLoad. Use
# this attribute to limit the type of
# RSVP service requested by RSVP applications.
# MaxRatePerFlow (O): In Kbps, default is system defined
# limit the maximum. Use this attribute to
# applications mean rate requested by RSVP
# in the traffic specification
# (Tspec) or Guaranteed service Rspec.
# MaxTokenBucketPerFlow (O): In Kb, default is system defined
# maximum. Use this attribute to limit the
# token bucket depth requested by RSVP
# applications in the traffic specification (Tspec).
# MaxFlows (O): Default is non-specified
# (infinite).
# SignalClient (O): 0 (no signalling) | 1 (signalling)
# NumberOfAcceptQueues (O): 0 - 8. 0 requests the default
# accept queue configuration:
# ID Weight
# High 40%
# Med 30%
# Low 20%
# BestEffort 10%
# Values 1 - 8 define a number of
# accept queues, whose IDs and weights are
# defined with AcceptQueueIDandWeight
# parameter.
# AcceptQueueIDandWeight (O): 2 values: Identifier and weight as
# a percentage. This parameter is used when
# NumberOfAcceptQueues

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#
number of times
#
NumberOfAcceptQueues. The weights
#
up to 100%.
# DefaultAcceptQueueID (0): ID of accept queue to use when
provisioning
#
InboundAcceptQueueID.
#
NumberOfAcceptQueues is
#
specified with
#
AcceptQueueIDandWeight.

# The following are a set of default policyAction definitions based
# on the precedence field of the TOS byte in the IP header
# (refer to RFC 791 for detail). For network domains that support
# Differentiated Services (DS) definition (RFC 2474), the outgoing
# TOS (aka DS code points) value needs to be updated.
policyAction networkcontrol
{
    policyScope DataTraffic
    OutgoingTOS 11100000 # Precedence bits (first 3 bits)
}

policyAction internetwork # encapsulated network control
{
    policyScope DataTraffic
    OutgoingTOS 11000000 #
}

policyAction crit-realtime # realtime data
{
    policyScope DataTraffic
    OutgoingTOS 10100000 #
}

policyAction interactive1
{
    policyScope DataTraffic
    OutgoingTOS 10000000
}

policyAction interactive2
{
    policyScope DataTraffic
    OutgoingTOS 01100000
}

policyAction batch1
{
    policyScope DataTraffic
    OutgoingTOS 01000000
}

policyAction batch2
{
    policyScope DataTraffic
    OutgoingTOS 00100000
}

# policyRule statement
# This statement specifies characteristics of IP packets, that are used
# to match to a corresponding policyAction. In other words, it
# defines a set of IP packets that should receive a particular service.
#
# statement format:
# policyRule s # Policy rule name.
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

#      {
#          PolicyRulePriority          i # Priority of this policy rule.
#          ForLoadDistribution         p # Is the rule intended for load
#                                     # distribution?
#          SourceAddressRange         a1 a2 # Source IP address range.
#          DestinationAddressRange    a1 a2 # Destination IP address range.
#          SourcePortRange            i1 i2 # Source port range.
#          DestinationPortRange       i1 i2 # Destination port range.
#          ProtocolNumberRange        i1 i2 # Transport protocol id range to
which
#                                     # this policy rule applies.
#          ApplicationName             s # Local application/job name.
#          ApplicationData             s # Application data, used for Web
QoS.
#          ApplicationPriority         i # Application specified priority.
#          ServerDomainName           s # HTTP request URL domain name.
#          UserNameId                 s # User name requesting service.
#          UserQoSGroup               s # User group requesting service.
#          InboundInterface           a|s # Incoming interface for which
#                                     # this policy rule applies.
#          OutboundInterface          a|s # Outgoing interface for which
#                                     # this policy rule applies.
#          IncomingTOS                b # IncomingTOS value/mask.
#          AcceptQueueLocalApplicationName s # Accept queue configuration
#                                     # local application name.
#          AcceptQueueLocalIPAddressRange a1 a2 # Accept queue configuration
#                                     # local IP address range.
#          AcceptQueueLocalPortRange  i1 i2 # Accept queue configuration
#                                     # local port range.
#          ConditionTimeRange         s # Overall time range.
#          MonthOfYearMask            b # Months of year that this
#                                     # policy rule is active.
#          DayOfMonthMask             b # Days of month that this
#                                     # policy rule is active.
#          DayOfWeekMask             b # Days in a week that this
#                                     # policy rule is active.
#          TimeOfDayRange             s # Time of each day during which
#                                     # policy rule is active.
#          PolicyActionReference       s # Name of an action which this
policy
#                                     # rule uses.
#      }
#      where:
#          s
to 32
#          PolicyRulePriority
the order
#
others.
#
priority
#
maximum
#          ForLoadDistribution
for a
#
distributing
#
#
#
FALSE.
#          SourceAddressRange
default is 0
#
optional.
#
specified.
(R): Is the name of this policy rule (up
characters, truncated if longer).
(O): Priority of a rule, it determines
of rule evaluation relative to
Default is for Pagent to assign a
based on rule's specificity. The
value is 2000000000.
(O): Set to TRUE if the rule is intended
Sysplex Distributor (SD)
stack. Use this for rules to be
interpreted on the SD distributing
stack. Valid values are TRUE and
The default is FALSE.
(O): From a1 to a2 where a2 >= a1,
which is all inclusive. a2 is
IPv4 or IPv6 addresses can be

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

<pre># DestinationAddressRange default is 0 # optional. # specified. # SourcePortRange default is 0 # maximum value # DestinationPortRange default is 0 # maximum value # ProtocolNumberRange default is 0 # maximum value # ApplicationName application that # # # # # # # # # # # truncated). # ApplicationData # # # process. # assign # # # # # # the # # # # # truncated). # ApplicationPriority # # # # # # # # # #</pre>	<pre>(O): From a1 to a2 where a2 >= a1, which is all inclusive. a2 is IPv4 or IPv6 addresses can be (O): From i1 to i2 where i2 >= i1, which is all inclusive. The is 65535. i2 is optional. (O): From i1 to i2 where i2 >= i1, which is all inclusive. The is 65535. i2 is optional. (O): From i1 to i2 where i2 >= i1, which is all inclusive. The is 255. i2 is optional. (O): Specifies the name of the is executing in the S/390 (e.g., also referred to as job name). Application name is used when a predefined port number is not known for the application (e.g., applications that use dynamically assigned port numbers). Note that in S/390, application names are converted to upper case for comparison with job names. '*' can be used as a wildcard. The specified name is limited to 8 characters (longer names are silently (O): Attribute is used for content-based policy classification. This means the policy allows policy condition to include application data to be included in the evaluation It enables an application to different types of QoS treatments for different transactions (or streams of data) within a session. In S/390, only web URI (Universal Resource Identifier) is supported as application data and only when web application server activates Fast Response Cache Accelerator (FRCA) function. This parameter is limited to 128 characters (longer data are silently (O): Attribute is used for content-based policy classification. It allows an application to assign different priorities for different transactions (or streams of data) within a session. Valid values are as follows: 0 = Any application priority specified (default). 1 = EXPEDITED, 2 = HIGH, 3 = MEDIUM, 4 = LOW, 5 = BESTEFFORT.</pre>
---	--

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

<pre># ServerDomainName # request # # UserNameId # # UserQoSGroup that # # # InboundInterface Default # an IPv4 # be specified. # OutboundInterface Default # Either an IPv4 # be specified. # outbound # corresponding # traffic. This # policy # destined to or # node where # departs on # # IncomingTOS # value. n is # the TOS # # AcceptQueueLocalApplicationName queue # attribute cannot be # attributes, for # only be # configuration # # AcceptQueueLocalIPAddressRange queue # attribute cannot be # attributes, for # only be # configuration # # AcceptQueueLocalPortRange configuration # specified</pre>	<pre>(O): Attribute contains the name of the server specified in an HTTP URL. (O): Specifies the identity of the user that is requesting a service which is to be assigned a QoS level. (O): Attribute contains the QoS group is used to classify a user that is requesting a service. (O): Specifies a valid local interface. is all inbound interfaces. Either address or an interface name can (O): Specifies a valid local interface. is all outbound interfaces. address or an interface name can NOTE: if both local inbound and interfaces are specified, the rule won't be mapped to any is because S/390 implementation of is as a server where traffic is originates from, not as a routing traffic enters one interface and another. (O): bbbbbbbb-n First 8 bits are incoming TOS the number of significant bits in (1-8). (O): Local application name for accept configuration policy. This specified with provisioning example SourcePortRange. It can specified with other accept queue attributes. (O): Local IP address range for accept configuration policy. This specified with provisioning example SourcePortRange. It can specified with other accept queue attributes. (O): Local port range for accept queue policy. This attribute cannot be</pre>
--	--

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

<pre># example # specified with # attributes. # ConditionTimeRange # dates # # # # # nearest # # # # # # not # # - # # are # # MonthOfYearMask representing # all year. # DayOfMonthMask is # # DayOfWeekMask representing Sunday # 0111110 # all week. # TimeOfDayRange 25), # at 0 # Only hour # specified. # # 17:30-24 # after # 5:30PM to # # PolicyActionReference interactive # statement # attribute) to # different # rule</pre>	<pre>with provisioning attributes, for SourcePortRange. It can only be other accept queue configuration (O): yyyyymmddhhmmss:yyyyymmddhhmmss Specifies the range of calendar on which the corresponding policy rule is valid. where yyyy is year, mm is month, dd is date, hh is hour, mm is minute and ss is second. Seconds are rounded to the minute. Default is always. Out of bounds values are forced to be correct (for instance month 13 becomes January of the following year). Dates before the start of the Posix epoch (Jan/01/1970 00:00:00 UTC) are valid. The time is kept in the format of seconds since the epoch this value wraps early in the year 2038, so times after that not valid. (O): A mask of 12 0's and 1's January to December. Default is (O): A mask of 31 0's and 1's, default all month. (O): A mask of 7 0's and 1's through Saturday. For example, represents weekdays. Default is (O): A series of time intervals (up to separated by a comma. Time starts which is right after midnight. and minute are allowed to be Default is 24 hours. Example: TimeOfDayRange 0-8:30, means this policy is only active midnight to 8:30AM, and from midnight. (R): Example: policyActionReference Up to 4 instances of this can be specified (one name per associate this policy rule with actions. For instance, a policy</pre>
---	---

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
#                                     can reference two actions, one for
RSVP
#                                     and one for DataTraffic
(DiffServ).

# The following are a set of default policy rules defined
# for different traffic types including Enterprise Extender (EE),
# based on port numbers from the host side (390 server).
# This set is not exhaustive but only represents the majority of traffic
# in a typical network.
policyRule      routed      # ROUTED traffic
{
    protocolNumberRange 17
    SourcePortRange     520      # ROUTED port
    policyActionReference networkcontrol
}

policyRule      ospf        # OSPF link advertisement traffic
{
    protocolNumberRange 89      # OSPF protocol number
    policyActionReference networkcontrol
}

policyRule      tftpd       # TFTP traffic
{
    protocolNumberRange 17
    SourcePortRange     69      # TFTP port
    policyActionReference batch1
}

policyRule      ftpd        # FTP traffic
{
    protocolNumberRange 6
    SourcePortRange     20 21   # Both FTP control and data ports
    policyActionReference batch1
}

policyRule      telnetd     # telnet traffic
{
    protocolNumberRange 6
    SourcePortRange     23
    policyActionReference interactive1
}

policyRule      web-httpd   # web traffic
{
    protocolNumberRange 6
    SourcePortRange     80
    policyActionReference interactive2
}

policyRule      dns-udp     # domain name server udp traffic
{
    protocolNumberRange 17
    SourcePortRange     42
    policyActionReference interactive1
}

policyRule      dns-tcp     # domain name server tcp traffic
{
    protocolNumberRange 6
    SourcePortRange     42
    policyActionReference interactive1
}

policyRule      ntp         # NTP traffic
{
    protocolNumberRange 17
    SourcePortRange     123
    policyActionReference crit-realtime
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
policyRule          EE-xid
{
    protocolNumberRange 17
    SourcePortRange      12000
    policyActionReference internetwork
}

policyRule          EE-network
{
    protocolNumberRange 17
    SourcePortRange      12001
    policyActionReference internetwork
}

policyRule          EE-highpri
{
    protocolNumberRange 17
    SourcePortRange      12002
    policyActionReference interactive1
}

policyRule          EE-medpri
{
    protocolNumberRange 17
    SourcePortRange      12003
    policyActionReference batch1
}

policyRule          EE-lowpri
{
    protocolNumberRange 17
    SourcePortRange      12004
    policyActionReference batch2
}

# The following is a sample policy for enforcing Differentiated Services
# parameters that describe a token bucket mechanism. The action
# establishes a token bucket traffic conditioner with a mean rate of
# 512 kilobits per second and a burst size of 4 kilobytes. Any traffic
# that exceeds these specifications will be sent as best effort, with
# an accompanying TOS byte of '00000000'. Note that this is just an
# example: exact specifications depend on the characteristics of the
# sending application and the underlying network.
#
# PolicyRule                      DiffServ_Rule1
# {
#     DestinationAddressRange      211.40.100.0-211.40.100.255
#     SourcePortRange              20-21
#     PolicyActionReference         DiffServ_Action1
#     DayOfWeekMask                0111110
# }
#
# PolicyAction                    DiffServ_Action1
# {
#     PolicyScope                  DataTraffic
#     OutgoingTOS                 01000000
#     DiffServInProfileRate        512          # 512 Kbps
#     DiffServInProfileTokenBucket 64           # 64 Kbits
#     DiffServInProfilePeakRate    1500         # 1.5 Mbps
#     DiffServInProfileMaxPacketSize 120        # 120 Kbits
#     DiffServOutProfileTransmittedTOSByte 00000000
#     DiffServExcessTrafficTreatment BestEffort
# }
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

***** **Lab L07 TMnx_ATTLS_FTP.policy** *****

```
##
## AT-TLS Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS
Communications Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## End of Configuration Assistant information
TTLRule VIPAs2VIPAs~1
{
  LocalAddrSetRef      addr1
  RemoteAddrSetRef     addr1
  LocalPortRangeRef    portR1
  RemotePortRangeRef   portR2
  Userid               USER*
  Direction            Outbound
  Priority              255
  TTLGroupActionRef    gAct1
  TTLEnvironmentActionRef eAct1~AllSecFTPclients
  TLSConnectionActionRef cAct1~AllSecFTPclients
}
TTLRule VIPAs2VIPAs~2
{
  LocalAddrSetRef      addr1
  RemoteAddrSetRef     addr1
  LocalPortRangeRef    portR2
  RemotePortRangeRef   portR1
  Direction            Inbound
  Priority              254
  TTLGroupActionRef    gAct1
  TTLEnvironmentActionRef eAct2~FTP-Server
  TLSConnectionActionRef cAct2~FTP-Server
}
TTLGroupAction gAct1
{
  TTLEnabled          On
  Trace               2
}
TTLEnvironmentAction eAct1~AllSecFTPclients
{
  HandshakeRole       Client
  EnvironmentUserInstance 0
  TLSKeyringParmsRef  keyR1
}
TTLEnvironmentAction eAct2~FTP-Server
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

{
    HandshakeRole                ServerWithClientAuth
    EnvironmentUserInstance       0
    TTLSKeyringParmsRef           keyR~ZOS7
    TTLSGskAdvancedParmsRef       gskAdv1~ATTLSGoldwClientAuth
}
TTLSConnectionAction             cAct1~AllSecFTPClient
{
    HandshakeRole                Client
    TTLSCipherParmsRef           cipher1
    TTLSConnectionAdvancedParmsRef cAdv1~AllSecFTPClient
    CtraceClearText              Off
    Trace                        2
}
TTLSConnectionAction             cAct2~FTP-Server
{
    HandshakeRole                ServerWithClientAuth
    TTLSCipherParmsRef           cipher1
    TTLSConnectionAdvancedParmsRef cAdv2~FTP-Server
    CtraceClearText              Off
    Trace                        2
}
TTLSConnectionAdvancedParms      cAdv1~AllSecFTPClient
{
    SSLv3                        On
    TLSv1                        On
    TLSv1.1                      On
    ApplicationControlled         On
    SecondaryMap                  On
    TLSv1.2                      Off
}
TTLSConnectionAdvancedParms      cAdv2~FTP-Server
{
    SSLv3                        On
    TLSv1                        On
    TLSv1.1                      On
    ApplicationControlled         On
    SecondaryMap                  On
    TLSv1.2                      On
}
TTLSKeyringParms                 keyR1
{
    Keyring                      LabClientRing
}
TTLSKeyringParms                 keyR~ZOS7
{
    Keyring                      FTPD/ServerRing1
}
TTLSGskAdvancedParms             gskAdv1~ATTLSGoldwClientAuth
{
    TTLSGskHttpCdpParmsRef       gskHttp
}
TTLSCipherParms                  cipher1
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
V3CipherSuites          TLS_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites          TLS_RSA_WITH_AES_128_CBC_SHA
}
TTLSGskHttpCdpParms     gskHttp
{
  HTTPCDPENABLE          OFF
}
IpAddrSet               addr1
{
  Range                   192.168.20.101-192.168.20.107
}
PortRange               portR1
{
  Port                    1024-65535
}
PortRange               portR2
{
  Port                    21
}
```

**** *Lab L08 TMnx_ATTLS_FTPandTN3270.policy* ****

```
##
## AT-TLS Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## TLS default rules: TN3270-WS-to-Host (c)
## End TLS default rules
##
## End of Configuration Assistant information
TTLRule                VIPAs2VIPAs~1
{
  LocalAddrSetRef       addr1
  RemoteAddrSetRef      addr1
  LocalPortRangeRef     portR1
  RemotePortRangeRef    portR2
  Userid                USER*
  Direction             Outbound
  Priority               255
  TTLGroupActionRef     gAct1
  TTLEnvironmentActionRef eAct1~AllSecFTPclients
  TLSConnectionActionRef cAct1~AllSecFTPclients
}
TTLRule                VIPAs2VIPAs~2
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

LocalAddrSetRef          addr1
RemoteAddrSetRef          addr1
LocalPortRangeRef         portR2
RemotePortRangeRef         portR1
Direction                 Inbound
Priority                   254
TTLSTGroupActionRef        gAct1
TTLSEnvironmentActionRef   eAct2~FTP-Server
TTLSTConnectionActionRef   cAct2~FTP-Server
}
TTLSTRule                TN3270-WS-to-Host~3
{
  LocalAddrSetRef          addr1
  RemoteAddrSetRef          addr2
  LocalPortRangeRef         portR3
  RemotePortRangeRef         portR1
  Direction                 Inbound
  Priority                   253
  TTLSTGroupActionRef        gAct1
  TTLSEnvironmentActionRef   eAct3~TN3270DiffKeyring
  TTLSTConnectionActionRef   cAct3~TN3270DiffKeyring
}
TTLSTGroupAction          gAct1
{
  TTLSEnabled              On
  Trace                     2
}
TTLSEnvironmentAction     eAct1~AllSecFTPCLients
{
  HandshakeRole             Client
  EnvironmentUserInstance    0
  TTLSTKeyringParmsRef       keyR1
}
TTLSEnvironmentAction     eAct2~FTP-Server
{
  HandshakeRole             ServerWithClientAuth
  EnvironmentUserInstance    0
  TTLSTKeyringParmsRef       keyR~ZOS7
  TTLSTGskAdvancedParmsRef   gskAdv1~ATTLSGoldwClientAuth
}
TTLSEnvironmentAction    eAct3~TN3270DiffKeyring
{
  HandshakeRole             ServerWithClientAuth
  EnvironmentUserInstance    0
  TTLSTKeyringParmsRef       keyR3
  TTLSTGskAdvancedParmsRef   gskAdv1~ATTLSGoldwClientAuth
}
TTLSTConnectionAction     cAct1~AllSecFTPCLients
{
  HandshakeRole             Client
  TTLSTCipherParmsRef        cipher1
  TTLSTConnectionAdvancedParmsRef cAdv1~AllSecFTPCLients
  CtraceClearText            Off
  Trace                       2
}
TTLSTConnectionAction     cAct2~FTP-Server
{

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

HandshakeRole                ServerWithClientAuth
TTLSCipherParmsRef           cipher1
TTLSCConnectionAdvancedParmsRef cAdv2~FTP-Server
CtraceClearText              Off
Trace                        2
}
TTLSCConnectionAction      cAct3~TN3270DiffKeyring
{
    HandshakeRole           ServerWithClientAuth
    TTLSCipherParmsRef       cipher1
    TTLSCConnectionAdvancedParmsRef cAdv3~TN3270DiffKeyring
    CtraceClearText         Off
    Trace                   2
}
TTLSCConnectionAdvancedParms  cAdv1~AllSecFTPCLients
{
    SSLv3                    On
    TLSv1                    On
    TLSv1.1                  On
    ApplicationControlled    On
    SecondaryMap              On
    TLSv1.2                  Off
}
TTLSCConnectionAdvancedParms  cAdv2~FTP-Server
{
    SSLv3                    On
    TLSv1                    On
    TLSv1.1                  On
    ApplicationControlled    On
    SecondaryMap              On
    TLSv1.2                  On
}
TTLSCConnectionAdvancedParms cAdv3~TN3270DiffKeyring
{
    SSLv3                   On
    TLSv1                   On
    TLSv1.1                 On
    ApplicationControlled   On
    SecondaryMap            Off
    TLSv1.2                 On
}
TTLSCKeyringParms            keyR1
{
    Keyring                  LabClientRing
}
TTLSCKeyringParms            keyR~ZOS7
{
    Keyring                  FTPD/ServerRing1
}
TTLSCKeyringParms          keyR3
{
    Keyring                 TN3270/MyServer7Ring
}
TTLSCGskAdvancedParms        gskAdv1~ATTLSGoldwClientAuth
{
    TTLSCGskHttpCdpParmsRef  gskHttp
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
TTLSCipherParms          cipher1
{
  V3CipherSuites          TLS_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites          TLS_RSA_WITH_AES_128_CBC_SHA
}
TTLSGskHttpCdpParms      gskHttp
{
  HTTPCDPENABLE           OFF
}
IpAddrSet                addr1
{
  Range                   192.168.20.101-192.168.20.107
}
IpAddrSet                addr2
{
  Prefix                 192.168.0.0/16
}
PortRange                portR1
{
  Port                    1024-65535
}
PortRange                portR2
{
  Port                    21
}
PortRange                portR3
{
  Port                    23
}
*****
```

**** **Lab L09 TMnx_IPFilter.policy** ****

```
*****
##
## IPsec Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
## Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## End of Configuration Assistant information

IpGenericFilterAction    Permit__LogYes
{
  IpFilterAction          Permit
  IpFilterLogging         Yes
  DiscardAction           Silent
}

IpService                CICS
{
  Protocol                TCP
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortRange      3000
DestinationPortRange 1024 65535
Direction            BiDirectional InboundConnect
Routing              Local
}

IpService             FTP-Client
{
  Protocol            TCP
  SourcePortRange     1024 65535
  DestinationPortRange 21
  Direction            BiDirectional OutboundConnect
  Routing              Local
}

IpService             FTP-Client~1
{
  Protocol            TCP
  SourcePortRange     1024 65535
  DestinationPortRange 20
  Direction            BiDirectional InboundConnect
  Routing              Local
}

IpService             FTP-Client~2
{
  Protocol            TCP
  SourcePortRange     1024 65535
  DestinationPortRange 50000 50200
  Direction            BiDirectional OutboundConnect
  Routing              Local
}

IpService             FTP-Server
{
  Protocol            TCP
  SourcePortRange     21
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}

IpService             FTP-Server~3
{
  Protocol            TCP
  SourcePortRange     20
  DestinationPortRange 1024 65535
  Direction            BiDirectional OutboundConnect
  Routing              Local
}

IpService             FTP-Server~4
{
  Protocol            TCP
  SourcePortRange     50000 50200
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Routing                                Local
}

IpService                              TN3270-Server
{
  Protocol                             TCP
  SourcePortRange                      23
  DestinationPortRange                1024 65535
  Direction                           BiDirectional InboundConnect
  Routing                             Local
}

IpService                              DNS
{
  Protocol                             UDP
  SourcePortRange                      53
  DestinationPortRange                1024 65535
  Direction                           BiDirectional
  Routing                             Local
}

IpService                              DNS~5
{
  Protocol                             UDP
  SourcePortRange                      53
  DestinationPortRange                53
  Direction                           BiDirectional
  Routing                             Local
}

IpService                              DNS~6
{
  Protocol                             TCP
  SourcePortRange                      53
  DestinationPortRange                1024 65535
  Direction                           BiDirectional
  Routing                             Local
}

IpService                              DNS~7
{
  Protocol                             TCP
  SourcePortRange                      53
  DestinationPortRange                53
  Direction                           BiDirectional
  Routing                             Local
}

IpService                              ICMP-Time_Exceeded-IP_V4
{
  Protocol                             ICMP
  Type                                 11
  Code                                 Any
  Direction                           BiDirectional
  Routing                             Local
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                ICMP-Unreachable-IP_V4
{
  Protocol                               ICMP
  Type                                   3
  Code                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4
{
  Protocol                               OSPF
  Type                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4~8
{
  Protocol                               IGMP
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4~9
{
  Protocol                               UDP
  SourcePortRange                        520
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4~10
{
  Protocol                               UDP
  SourcePortRange                        1024 65535
  DestinationPortRange                  520
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4~11
{
  Protocol                               UDP
  SourcePortRange                        520
  DestinationPortRange                  520
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Path_MTU_Discovery-IP_V4
{
  Protocol                               ICMP
  Type                                   3
  Code                                   4
  Direction                             BiDirectional
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Routing                                     Local
}

IpService                                   Ping-IP_V4
{
  Protocol                                   ICMP
  Type                                       8
  Code                                       Any
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   Ping-IP_V4~12
{
  Protocol                                   ICMP
  Type                                       0
  Code                                       Any
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   Resolver
{
  Protocol                                   TCP
  SourcePortRange                           1024 65535
  DestinationPortRange                     53
  Direction                                 BiDirectional OutboundConnect
  Routing                                   Local
}

IpService                                   Resolver~13
{
  Protocol                                   UDP
  SourcePortRange                           1024 65535
  DestinationPortRange                     53
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   Trace_Route-IP_V4
{
  Protocol                                   ICMP
  Type                                       11
  Code                                       0
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   Trace_Route-IP_V4~14
{
  Protocol                                   ICMP
  Type                                       3
  Code                                       3
  Direction                                 BiDirectional
  Routing                                   Local
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpService                                Trace_Route-IP_V4~15
{
    Protocol                             ICMP
    Type                                 3
    Code                                 2
    Direction                           BiDirectional
    Routing                             Local
}

IpService                                Trace_Route-IP_V4~16
{
    Protocol                             UDP
    SourcePortRange                      1024 65535
    DestinationPortRange                 33435 33535
    Direction                           BiDirectional
    Routing                             Local
}
##
## Connectivity Rule TrafficBetweenVIPAs combines the following items:
##   Local data endpoint                TrafficBetweenVIPAs~ADR~1
##   Remote data endpoint               TrafficBetweenVIPAs~ADR~2
##   Topology                          Filtering - Host
##   Requirement Map
##     CICS                             => Permit
##     FTP-Client                       => Permit
##     FTP-Server                       => Permit

IpAddr                                   TrafficBetweenVIPAs~ADR~1
{
    Addr                                 192.168.20.107
}

IpAddr                                   TrafficBetweenVIPAs~ADR~2
{
    Addr                                 192.168.20.101
}

IpFilterRule                            TrafficBetweenVIPAs~3
{
    IpSourceAddrRef                     TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef                       TrafficBetweenVIPAs~ADR~2
    IpServiceRef                        CICS
    IpGenericFilterActionRef            Permit__LogYes
}

IpFilterRule                            TrafficBetweenVIPAs~4
{
    IpSourceAddrRef                     TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef                       TrafficBetweenVIPAs~ADR~2
    IpServiceRef                        FTP-Client
    IpGenericFilterActionRef            Permit__LogYes
}

IpFilterRule                            TrafficBetweenVIPAs~5
{
    IpSourceAddrRef                     TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef                       TrafficBetweenVIPAs~ADR~2

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpServiceRef      FTP-Client~1
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule          TrafficBetweenVIPAs~6
{
    IpSourceAddrRef    TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef      TrafficBetweenVIPAs~ADR~2
    IpServiceRef        FTP-Client~2
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule          TrafficBetweenVIPAs~7
{
    IpSourceAddrRef    TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef      TrafficBetweenVIPAs~ADR~2
    IpServiceRef        FTP-Server
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule          TrafficBetweenVIPAs~8
{
    IpSourceAddrRef    TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef      TrafficBetweenVIPAs~ADR~2
    IpServiceRef        FTP-Server~3
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule          TrafficBetweenVIPAs~9
{
    IpSourceAddrRef    TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef      TrafficBetweenVIPAs~ADR~2
    IpServiceRef        FTP-Server~4
    IpGenericFilterActionRef  Permit__LogYes
}
##
## Connectivity Rule WStoVIPA combines the following items:
##   Local data endpoint      WStoVIPA~ADR~1
##   Remote data endpoint     All4
##   Topology                 Filtering - Host
##   Requirement Map
##     FTP-Server              => Permit
##     TN3270-Server           => Permit

IpAddr                WStoVIPA~ADR~1
{
    Addr                192.168.20.107
}

IpFilterRule          WStoVIPA~2
{
    IpSourceAddrRef    WStoVIPA~ADR~1
    IpDestAddr         All4
    IpServiceRef        FTP-Server
    IpGenericFilterActionRef  Permit__LogYes
}

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                WStoVIPA~3
{
    IpSourceAddrRef                          WStoVIPA~ADR~1
    IpDestAddr                              All4
    IpServiceRef                            FTP-Server~3
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                WStoVIPA~4
{
    IpSourceAddrRef                          WStoVIPA~ADR~1
    IpDestAddr                              All4
    IpServiceRef                            FTP-Server~4
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                WStoVIPA~5
{
    IpSourceAddrRef                          WStoVIPA~ADR~1
    IpDestAddr                              All4
    IpServiceRef                            TN3270-Server
    IpGenericFilterActionRef                 Permit__LogYes
}
##
## Connectivity Rule CommonTraffic combines the following items:
##   Local data endpoint                    All4
##   Remote data endpoint                   All4
##   Topology                             Filtering - Host
##   Requirement Map
##     DNS                                 => Permit
##     ICMP-Time_Exceeded-IP_V4           => Permit
##     ICMP-Unreachable-IP_V4             => Permit
##     OMPROUTE-IP_V4                     => Permit
##     Path_MTU_Discovery-IP_V4           => Permit
##     Ping-IP_V4                         => Permit
##     Resolver                           => Permit
##     Trace_Route-IP_V4                  => Permit

IpFilterRule                                CommonTraffic~1
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            DNS
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~2
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            DNS~5
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~3
{
    IpSourceAddr                            All4

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    IpDestAddr          All4
    IpServiceRef         DNS~6
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~4
{
    IpSourceAddr        All4
    IpDestAddr          All4
    IpServiceRef         DNS~7
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~5
{
    IpSourceAddr        All4
    IpDestAddr          All4
    IpServiceRef         ICMP-Time_Exceeded-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~6
{
    IpSourceAddr        All4
    IpDestAddr          All4
    IpServiceRef         ICMP-Unreachable-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~7
{
    IpSourceAddr        All4
    IpDestAddr          All4
    IpServiceRef         OMPROUTE-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~8
{
    IpSourceAddr        All4
    IpDestAddr          All4
    IpServiceRef         OMPROUTE-IP_V4~8
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~9
{
    IpSourceAddr        All4
    IpDestAddr          All4
    IpServiceRef         OMPROUTE-IP_V4~9
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            CommonTraffic~10
{
    IpSourceAddr        All4
    IpDestAddr          All4
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpServiceRef      OMPROUTE-IP_V4~10
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~11
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      OMPROUTE-IP_V4~11
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~12
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Path_MTU_Discovery-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~13
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Ping-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~14
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Ping-IP_V4~12
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~15
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Resolver
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~16
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Resolver~13
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~17
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Trace_Route-IP_V4

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpGenericFilterActionRef    Permit__LogYes
}

IpFilterRule                  CommonTraffic~18
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              Trace_Route-IP_V4~14
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~19
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              Trace_Route-IP_V4~15
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~20
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              Trace_Route-IP_V4~16
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterPolicy
{
    PreDecap                  OFF
    FilterLogging              ON
    IpFilterLogImplicit        No
    AllowOnDemand              Yes
    ImplicitDiscardAction      Silent
    FIPS140                    No
    IpFilterRuleRef            TrafficBetweenVIPAs~3
    IpFilterRuleRef            TrafficBetweenVIPAs~4
    IpFilterRuleRef            TrafficBetweenVIPAs~5
    IpFilterRuleRef            TrafficBetweenVIPAs~6
    IpFilterRuleRef            TrafficBetweenVIPAs~7
    IpFilterRuleRef            TrafficBetweenVIPAs~8
    IpFilterRuleRef            TrafficBetweenVIPAs~9
    IpFilterRuleRef            WStoVIPA~2
    IpFilterRuleRef            WStoVIPA~3
    IpFilterRuleRef            WStoVIPA~4
    IpFilterRuleRef            WStoVIPA~5
    IpFilterRuleRef            CommonTraffic~1
    IpFilterRuleRef            CommonTraffic~2
    IpFilterRuleRef            CommonTraffic~3
    IpFilterRuleRef            CommonTraffic~4
    IpFilterRuleRef            CommonTraffic~5
    IpFilterRuleRef            CommonTraffic~6
    IpFilterRuleRef            CommonTraffic~7
    IpFilterRuleRef            CommonTraffic~8
    IpFilterRuleRef            CommonTraffic~9
    IpFilterRuleRef            CommonTraffic~10
    IpFilterRuleRef            CommonTraffic~11
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRuleRef      CommonTraffic~12
IpFilterRuleRef      CommonTraffic~13
IpFilterRuleRef      CommonTraffic~14
IpFilterRuleRef      CommonTraffic~15
IpFilterRuleRef      CommonTraffic~16
IpFilterRuleRef      CommonTraffic~17
IpFilterRuleRef      CommonTraffic~18
IpFilterRuleRef      CommonTraffic~19
IpFilterRuleRef      CommonTraffic~20
}
*****

**** Lab L12 TMnx_IPSec_VPN.policy ****
*****

##
## IPsec Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
## Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## End of Configuration Assistant information

## NOTE -- Generated IpGenericFilterAction Permit__LogYes
IpGenericFilterAction      Permit__LogYes
{
    IpFilterAction          Permit
    IpFilterLogging          Yes
    DiscardAction            Silent
}

IpGenericFilterAction      IPSec__LogYes
{
    IpFilterAction          IPSec
    IpFilterLogging          Yes
    DiscardAction            Silent
}

KeyExchangeOffer           VPN~A
{
    HowToEncrypt            AES_CBC KeyLength 128
    HowToAuthMsgs            SHA1
    HowToVerifyMsgs          HMAC_SHA1_96
    PseudoRandomFunction      HMAC_SHA1
    HowToAuthPeers            RsaSignature
    DHGroup                   Group2
    RefreshLifetimeProposed    1440
    RefreshLifetimeAccepted    1440 1440
    RefreshLifesizeProposed    None
    RefreshLifesizeAccepted    None
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpDataOffer                                VPN~A~R
{
    HowToEncap                               Transport
    HowToEncrypt                             3DES
    HowToAuth                                ESP Hmac_Sha1
    RefreshLifetimeProposed                   480
    RefreshLifetimeAccepted                   480 480
    RefreshLifesizeProposed                   None
    RefreshLifesizeAccepted                   None
}

## NOTE -- Generated IpService IKE~Gen
IpService                                   IKE~Gen
{
    Protocol                                  UDP
    SourcePortRange                          500
    DestinationPortRange                     500
    Direction                                BiDirectional
    Routing                                   Local
}

IpService                                   FTP-Client
{
    Protocol                                  TCP
    SourcePortRange                          1024 65535
    DestinationPortRange                     21
    Direction                                BiDirectional OutboundConnect
    Routing                                   Local
}

IpService                                   FTP-Client~1
{
    Protocol                                  TCP
    SourcePortRange                          1024 65535
    DestinationPortRange                     20
    Direction                                BiDirectional InboundConnect
    Routing                                   Local
}

IpService                                   FTP-Client~2
{
    Protocol                                  TCP
    SourcePortRange                          1024 65535
    DestinationPortRange                     50000 50200
    Direction                                BiDirectional OutboundConnect
    Routing                                   Local
}

IpService                                   FTP-Server
{
    Protocol                                  TCP
    SourcePortRange                          21
    DestinationPortRange                     1024 65535
    Direction                                BiDirectional InboundConnect
    Routing                                   Local
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                FTP-Server~3
{
  Protocol                               TCP
  SourcePortRange                        20
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional OutboundConnect
  Routing                               Local
}

IpService                                FTP-Server~4
{
  Protocol                               TCP
  SourcePortRange                        50000 50200
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional InboundConnect
  Routing                               Local
}

IpService                                CICS
{
  Protocol                               TCP
  SourcePortRange                        3000
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional InboundConnect
  Routing                               Local
}

IpService                                TN3270-Server
{
  Protocol                               TCP
  SourcePortRange                        23
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional InboundConnect
  Routing                               Local
}

IpService                                DNS
{
  Protocol                               UDP
  SourcePortRange                        53
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                DNS~5
{
  Protocol                               UDP
  SourcePortRange                        53
  DestinationPortRange                  53
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                DNS~6
{
  Protocol                               TCP
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortRange      53
DestinationPortRange 1024 65535
Direction            BiDirectional
Routing              Local
}

IpService             DNS~7
{
  Protocol            TCP
  SourcePortRange     53
  DestinationPortRange 53
  Direction            BiDirectional
  Routing              Local
}

IpService             ICMP-Time_Exceeded-IP_V4
{
  Protocol            ICMP
  Type                11
  Code                Any
  Direction            BiDirectional
  Routing              Local
}

IpService             ICMP-Unreachable-IP_V4
{
  Protocol            ICMP
  Type                3
  Code                Any
  Direction            BiDirectional
  Routing              Local
}

IpService             OMPROUTE-IP_V4
{
  Protocol            OSPF
  Type                Any
  Direction            BiDirectional
  Routing              Local
}

IpService             OMPROUTE-IP_V4~8
{
  Protocol            IGMP
  Direction            BiDirectional
  Routing              Local
}

IpService             OMPROUTE-IP_V4~9
{
  Protocol            UDP
  SourcePortRange     520
  DestinationPortRange 1024 65535
  Direction            BiDirectional
  Routing              Local
}
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                OMPROUTE-IP_V4~10
{
  Protocol                               UDP
  SourcePortRange                        1024 65535
  DestinationPortRange                  520
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4~11
{
  Protocol                               UDP
  SourcePortRange                        520
  DestinationPortRange                  520
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Path_MTU_Discovery-IP_V4
{
  Protocol                               ICMP
  Type                                   3
  Code                                   4
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Ping-IP_V4
{
  Protocol                               ICMP
  Type                                   8
  Code                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Ping-IP_V4~12
{
  Protocol                               ICMP
  Type                                   0
  Code                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Resolver
{
  Protocol                               TCP
  SourcePortRange                        1024 65535
  DestinationPortRange                  53
  Direction                             BiDirectional OutboundConnect
  Routing                               Local
}

IpService                                Resolver~13
{
  Protocol                               UDP
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

SourcePortRange      1024 65535
DestinationPortRange 53
Direction            BiDirectional
Routing              Local
}

IpService              Trace_Route-IP_V4
{
  Protocol            ICMP
  Type                11
  Code                0
  Direction            BiDirectional
  Routing              Local
}

IpService              Trace_Route-IP_V4~14
{
  Protocol            ICMP
  Type                3
  Code                3
  Direction            BiDirectional
  Routing              Local
}

IpService              Trace_Route-IP_V4~15
{
  Protocol            ICMP
  Type                3
  Code                2
  Direction            BiDirectional
  Routing              Local
}

IpService              Trace_Route-IP_V4~16
{
  Protocol            UDP
  SourcePortRange      1024 65535
  DestinationPortRange 33435 33535
  Direction            BiDirectional
  Routing              Local
}

IpDynVpnAction      VPN~A
{
  Initiation          Either
  VpnLife             1440
  InitiateWithPfs     Group2
  IpDataOfferRef      VPN~A~R
  AcceptablePfs       None
  AcceptablePfs       Group2
  PassthroughDF       Yes
  PassthroughDSCP     Yes
  HowToEncapIKEv2     Either
}
##
## Connectivity Rule BetweenOSAsRSA combines the following items:
##   Local data endpoint      BetweenOSAsRSA~ADR~1

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
## Remote data endpoint      BetweenOSAsRSA~ADR~2
## Topology                  Host to Host
## Requirement Map
##   FTP-Client              => VPN~A
##   FTP-Server              => VPN~A
```

```
IpAddr                      BetweenOSAsRSA~ADR~1
{
  Addr                      192.168.20.97
}
```

```
IpAddr                      BetweenOSAsRSA~ADR~2
{
  Addr                      192.168.20.91
}
```

```
LocalSecurityEndpoint       BetweenOSAsRSA~LSE~4
{
  Identity                  IpAddr 192.168.20.97
  LocationRef               BetweenOSAsRSA~ADR~1
}
```

```
RemoteSecurityEndpoint      BetweenOSAsRSA~RSE~3
{
  Identity                  IpAddr 192.168.20.91
  LocationRef               BetweenOSAsRSA~ADR~2
}
```

```
KeyExchangeRule             BetweenOSAsRSA~5
{
  LocalSecurityEndpointRef  BetweenOSAsRSA~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA~RSE~3
  KeyExchangeActionRef      BetweenOSAsRSA
}
```

```
KeyExchangeAction           BetweenOSAsRSA
{
  HowToRespondIKEv1         Either
  KeyExchangeOfferRef        VPN~A
  AllowNat                   No
  ReauthInterval             0
  ConstrainSource            192.168.20.97
  ConstrainDest              192.168.20.91
}
```

```
IpLocalStartAction          BetweenOSAsRSA~8
{
  AllowOnDemand              No
  LocalPortGranularity       Rule
  RemotePortGranularity      Rule
  ProtocolGranularity        Rule
  RemoteIpGranularity        Packet
  LocalIpGranularity         Packet
  IcmpCodeGranularity        Rule
  IcmpTypeGranularity        Rule
  IcmpV6CodeGranularity      Rule
  IcmpV6TypeGranularity      Rule
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
MipV6TypeGranularity      Rule
LocalSecurityEndpointRef   BetweenOSAsRSA~LSE~4
RemoteSecurityEndpointRef  BetweenOSAsRSA~RSE~3
}

## NOTE -- Generated IpFilterRule BetweenOSAsRSA~6
IpFilterRule               BetweenOSAsRSA~6
{
    IpSourceAddrRef         BetweenOSAsRSA~ADR~1
    IpDestAddrRef           BetweenOSAsRSA~ADR~2
    IpServiceRef            IKE~Gen
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule               BetweenOSAsRSA~7
{
    IpSourceAddrRef         BetweenOSAsRSA~ADR~1
    IpDestAddrRef           BetweenOSAsRSA~ADR~2
    IpServiceRef            FTP-Client
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef       VPN~A
}

IpFilterRule               BetweenOSAsRSA~9
{
    IpSourceAddrRef         BetweenOSAsRSA~ADR~1
    IpDestAddrRef           BetweenOSAsRSA~ADR~2
    IpServiceRef            FTP-Client~1
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef       VPN~A
    IpLocalStartActionRef   BetweenOSAsRSA~8
}

IpFilterRule               BetweenOSAsRSA~10
{
    IpSourceAddrRef         BetweenOSAsRSA~ADR~1
    IpDestAddrRef           BetweenOSAsRSA~ADR~2
    IpServiceRef            FTP-Client~2
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef       VPN~A
}

IpFilterRule               BetweenOSAsRSA~12
{
    IpSourceAddrRef         BetweenOSAsRSA~ADR~1
    IpDestAddrRef           BetweenOSAsRSA~ADR~2
    IpServiceRef            FTP-Server
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef       VPN~A
    IpLocalStartActionRef   BetweenOSAsRSA~8
}

IpFilterRule               BetweenOSAsRSA~13
{
    IpSourceAddrRef         BetweenOSAsRSA~ADR~1
    IpDestAddrRef           BetweenOSAsRSA~ADR~2
    IpServiceRef            FTP-Server~3
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
}

IpFilterRule                  BetweenOSAsRSA~15
{
    IpSourceAddrRef           BetweenOSAsRSA~ADR~1
    IpDestAddrRef             BetweenOSAsRSA~ADR~2
    IpServiceRef               FTP-Server~4
    IpGenericFilterActionRef   IpSec__LogYes
    IpDynVpnActionRef          VPN~A
    IpLocalStartActionRef      BetweenOSAsRSA~8
}
##
## Connectivity Rule TrafficBetweenVIPAs combines the following items:
##   Local data endpoint      TrafficBetweenVIPAs~ADR~1
##   Remote data endpoint     TrafficBetweenVIPAs~ADR~2
##   Topology                  Filtering - Host
##   Requirement Map
##     CICS                     => Permit
##     FTP-Client                => Permit
##     FTP-Server                => Permit

IpAddr                        TrafficBetweenVIPAs~ADR~1
{
    Addr                        192.168.20.107
}

IpAddr                        TrafficBetweenVIPAs~ADR~2
{
    Addr                        192.168.20.101
}

IpFilterRule                  TrafficBetweenVIPAs~3
{
    IpSourceAddrRef           TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef             TrafficBetweenVIPAs~ADR~2
    IpServiceRef               CICS
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  TrafficBetweenVIPAs~4
{
    IpSourceAddrRef           TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef             TrafficBetweenVIPAs~ADR~2
    IpServiceRef               FTP-Client
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  TrafficBetweenVIPAs~5
{
    IpSourceAddrRef           TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef             TrafficBetweenVIPAs~ADR~2
    IpServiceRef               FTP-Client~1
    IpGenericFilterActionRef   Permit__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                     TrafficBetweenVIPAs~6
{
  IpSourceAddrRef                               TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                                 TrafficBetweenVIPAs~ADR~2
  IpServiceRef                                  FTP-Client~2
  IpGenericFilterActionRef                      Permit__LogYes
}

IpFilterRule                                     TrafficBetweenVIPAs~7
{
  IpSourceAddrRef                               TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                                 TrafficBetweenVIPAs~ADR~2
  IpServiceRef                                  FTP-Server
  IpGenericFilterActionRef                      Permit__LogYes
}

IpFilterRule                                     TrafficBetweenVIPAs~8
{
  IpSourceAddrRef                               TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                                 TrafficBetweenVIPAs~ADR~2
  IpServiceRef                                  FTP-Server~3
  IpGenericFilterActionRef                      Permit__LogYes
}

IpFilterRule                                     TrafficBetweenVIPAs~9
{
  IpSourceAddrRef                               TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                                 TrafficBetweenVIPAs~ADR~2
  IpServiceRef                                  FTP-Server~4
  IpGenericFilterActionRef                      Permit__LogYes
}
##
## Connectivity Rule WStoVIPA combines the following items:
##   Local data endpoint      WStoVIPA~ADR~1
##   Remote data endpoint     All4
##   Topology                  Filtering - Host
##   Requirement Map
##     FTP-Server              => Permit
##     TN3270-Server           => Permit

IpAddr                                           WStoVIPA~ADR~1
{
  Addr                                           192.168.20.107
}

IpFilterRule                                     WStoVIPA~2
{
  IpSourceAddrRef                               WStoVIPA~ADR~1
  IpDestAddr                                     All4
  IpServiceRef                                  FTP-Server
  IpGenericFilterActionRef                      Permit__LogYes
}

IpFilterRule                                     WStoVIPA~3
{
  IpSourceAddrRef                               WStoVIPA~ADR~1
  IpDestAddr                                     All4

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    IpServiceRef          FTP-Server~3
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              WStoVIPa~4
{
    IpSourceAddrRef       WStoVIPa~ADR~1
    IpDestAddr            All4
    IpServiceRef          FTP-Server~4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              WStoVIPa~5
{
    IpSourceAddrRef       WStoVIPa~ADR~1
    IpDestAddr            All4
    IpServiceRef          TN3270-Server
    IpGenericFilterActionRef Permit__LogYes
}
##
## Connectivity Rule CommonTraffic combines the following items:
##   Local data endpoint      All4
##   Remote data endpoint     All4
##   Topology                 Filtering - Host
##   Requirement Map
##     DNS                    => Permit
##     ICMP-Time_Exceeded-IP_V4 => Permit
##     ICMP-Unreachable-IP_V4  => Permit
##     OMPROUTE-IP_V4         => Permit
##     Path_MTU_Discovery-IP_V4 => Permit
##     Ping-IP_V4             => Permit
##     Resolver               => Permit
##     Trace_Route-IP_V4      => Permit

IpFilterRule              CommonTraffic~1
{
    IpSourceAddr          All4
    IpDestAddr            All4
    IpServiceRef          DNS
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              CommonTraffic~2
{
    IpSourceAddr          All4
    IpDestAddr            All4
    IpServiceRef          DNS~5
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              CommonTraffic~3
{
    IpSourceAddr          All4
    IpDestAddr            All4
    IpServiceRef          DNS~6
    IpGenericFilterActionRef Permit__LogYes
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRule                                CommonTraffic~4
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             DNS~7
  IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~5
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             ICMP-Time_Exceeded-IP_V4
  IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~6
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             ICMP-Unreachable-IP_V4
  IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~7
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             OMPROUTE-IP_V4
  IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~8
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             OMPROUTE-IP_V4~8
  IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~9
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             OMPROUTE-IP_V4~9
  IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                CommonTraffic~10
{
  IpSourceAddr                             All4
  IpDestAddr                               All4
  IpServiceRef                             OMPROUTE-IP_V4~10
  IpGenericFilterActionRef                 Permit__LogYes
}
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                CommonTraffic~11
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            OMPROUTE-IP_V4~11
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~12
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Path_MTU_Discovery-IP_V4
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~13
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Ping-IP_V4
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~14
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Ping-IP_V4~12
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~15
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Resolver
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~16
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Resolver~13
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~17
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Trace_Route-IP_V4
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~18

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
{
  IpSourceAddr          All4
  IpDestAddr            All4
  IpServiceRef          Trace_Route-IP_V4~14
  IpGenericFilterActionRef Permit__LogYes
}
```

```
IpFilterRule            CommonTraffic~19
{
  IpSourceAddr          All4
  IpDestAddr            All4
  IpServiceRef          Trace_Route-IP_V4~15
  IpGenericFilterActionRef Permit__LogYes
}
```

```
IpFilterRule            CommonTraffic~20
{
  IpSourceAddr          All4
  IpDestAddr            All4
  IpServiceRef          Trace_Route-IP_V4~16
  IpGenericFilterActionRef Permit__LogYes
}
```

KeyExchangePolicy

```
{
  AllowNat              No
  NatKeepAliveInterval 20
  HowToInitiate         Main
  LivenessInterval      30
  BypassIpValidation     No
  CertificateURLLookupPreference Tolerate
  RevocationChecking     Loose
  KeyExchangeRuleRef    BetweenOSAsRSA~5
}
```

IpFilterPolicy

```
{
  PreDecap              OFF
  FilterLogging          ON
  IpFilterLogImplicit    No
  AllowOnDemand          Yes
  ImplicitDiscardAction  Silent
  FIPS140                No
  IpFilterRuleRef        BetweenOSAsRSA~6
  IpFilterRuleRef        BetweenOSAsRSA~7
  IpFilterRuleRef        BetweenOSAsRSA~9
  IpFilterRuleRef        BetweenOSAsRSA~10
  IpFilterRuleRef        BetweenOSAsRSA~12
  IpFilterRuleRef        BetweenOSAsRSA~13
  IpFilterRuleRef        BetweenOSAsRSA~15
  IpFilterRuleRef        TrafficBetweenVIPAs~3
  IpFilterRuleRef        TrafficBetweenVIPAs~4
  IpFilterRuleRef        TrafficBetweenVIPAs~5
  IpFilterRuleRef        TrafficBetweenVIPAs~6
  IpFilterRuleRef        TrafficBetweenVIPAs~7
  IpFilterRuleRef        TrafficBetweenVIPAs~8
  IpFilterRuleRef        TrafficBetweenVIPAs~9
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRuleRef      WStoVIPA~2
IpFilterRuleRef      WStoVIPA~3
IpFilterRuleRef      WStoVIPA~4
IpFilterRuleRef      WStoVIPA~5
IpFilterRuleRef      CommonTraffic~1
IpFilterRuleRef      CommonTraffic~2
IpFilterRuleRef      CommonTraffic~3
IpFilterRuleRef      CommonTraffic~4
IpFilterRuleRef      CommonTraffic~5
IpFilterRuleRef      CommonTraffic~6
IpFilterRuleRef      CommonTraffic~7
IpFilterRuleRef      CommonTraffic~8
IpFilterRuleRef      CommonTraffic~9
IpFilterRuleRef      CommonTraffic~10
IpFilterRuleRef      CommonTraffic~11
IpFilterRuleRef      CommonTraffic~12
IpFilterRuleRef      CommonTraffic~13
IpFilterRuleRef      CommonTraffic~14
IpFilterRuleRef      CommonTraffic~15
IpFilterRuleRef      CommonTraffic~16
IpFilterRuleRef      CommonTraffic~17
IpFilterRuleRef      CommonTraffic~18
IpFilterRuleRef      CommonTraffic~19
IpFilterRuleRef      CommonTraffic~20
}
```

**** Lab L14 TMnx_IDS.policy ****

```
##
## IDS Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
## Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## End of Configuration Assistant information
```

```
IDSRule              DataHiding
{
  ConditionType       Attack
  IDSAttackCondition
  {
    AttackType         DATA_HIDING
    OptionPadChk       Enable
    IcmpEmbedPktChk    Enable
  }
  IDSActionRef        DataHiding
}

IDSRule              IPv6OutboundRaw
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

ConditionType          Attack
IDSAttackCondition
{
    AttackType          OUTBOUND_RAW_IPv6
    ProtocolGroupRef    IpProtGroup~1
}
IDSActionRef           IPv6OutboundRaw
}

IDSRule                IPv6DestinationOptions
{
    ConditionType       Attack
    IDSAttackCondition
    {
        AttackType      RESTRICTED_IPV6_DST_OPTIONS
        RestrictedIpv6OptionGroupRef IpOptGroup~1
    }
    IDSActionRef         IPv6DestinationOptions
}

IDSRule                IPv6HopByHop
{
    ConditionType       Attack
    IDSAttackCondition
    {
        AttackType      RESTRICTED_IPV6_HOP_OPTIONS
        RestrictedIpv6OptionGroupRef IpOptGroup~2
    }
    IDSActionRef         IPv6HopByHop
}

IDSRule                IPv6NextHeader
{
    ConditionType       Attack
    IDSAttackCondition
    {
        AttackType      RESTRICTED_IPV6_NEXT_HDR
        IPv6NextHdrGroupRef IPv6NextHdrGroup~1
    }
    IDSActionRef         IPv6NextHeader
}

IDSRule                TcpQueueSize
{
    ConditionType       Attack
    IDSAttackCondition
    {
        AttackType      TCP_QUEUE_SIZE
        TcpQueueSize    Short
    }
    IDSActionRef         TcpQueueSize
}

IDSRule                GlobalTCPStall
{
    ConditionType       Attack
    IDSAttackCondition

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    {
        AttackType          GLOBAL_TCP_STALL
    }
    IDSActionRef            GlobalTCPStall
}

IDSRule                    Flood
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          FLOOD
        IfcFloodMinDiscard   1000
        IfcFloodPercentage   10
    }
    IDSActionRef            Flood
}

IDSRule                    Echo
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          PERPETUAL_ECHO
        LocalPortGroupRef    LocalEchoPortGroup~1
        RemotePortGroupRef   RemoteEchoPortGroup~1
    }
    IDSActionRef            Echo
}

IDSRule                    IPv4Protocol
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          RESTRICTED_IP_PROTOCOL
        ProtocolGroupRef     IpProtGroup~2
    }
    IDSActionRef            IPv4Protocol
}

IDSRule                    IPv4Option
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          RESTRICTED_IP_OPTIONS
        RestrictedIpOptionGroupRef IpOptGroup~3
    }
    IDSActionRef            IPv4Option
}

IDSRule                    ICMPRedirect
{
    ConditionType           Attack
    IDSAttackCondition
    {

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

        AttackType          ICMP_REDIRECT
    }
    IDSActionRef             ICMPRedirect
}

IDSRule                     MalformedPacket
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          MALFORMED_PACKET
    }
    IDSActionRef             MalformedPacket
}

IDSRule                     IPv4OutboundRaw
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          OUTBOUND_RAW
        ProtocolGroupRef    IpProtGroup~3
    }
    IDSActionRef             IPv4OutboundRaw
}

IDSRule                     Fragmentation
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          IP_FRAGMENT
    }
    IDSActionRef             Fragmentation
}

IDSRule                     EEMalformedPacket
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          EE_MALFORMED_PACKET
    }
    IDSActionRef             EEMalformedPacket
}

IDSRule                     EELDLCCheck
{
    ConditionType           Attack
    IDSAttackCondition
    {
        AttackType          EE_LDLC_CHECK
    }
    IDSActionRef             EELDLCCheck
}

IDSRule                     EEPortCheck

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

{
  ConditionType          Attack
  IDSAttackCondition
  {
    AttackType           EE_PORT_CHECK
  }
  IDSActionRef           EEPortCheck
}

IDSRule                  EEXIDFlood
{
  ConditionType          Attack
  IDSAttackCondition
  {
    AttackType           EE_XID_FLOOD
    EEXIDTimeOut         100
  }
  IDSActionRef           EEXIDFlood
}

IDSAction                DataHiding
{
  ActionType             Attack nodiscard
  IDSReportSet
  {
    TypeActions          LOG
    LoggingLevel         4
    TypeActions          STATISTICS
    StatType             Normal
    StatInterval         60
  }
}

IDSAction                IPv6OutboundRaw
{
  ActionType             Attack nodiscard
  IDSReportSet
  {
    TypeActions          LOG
    LoggingLevel         4
    TypeActions          STATISTICS
    StatType             Normal
    StatInterval         60
  }
}

IDSAction                IPv6DestinationOptions
{
  ActionType             Attack nodiscard
  IDSReportSet
  {
    TypeActions          LOG
    LoggingLevel         4
    TypeActions          STATISTICS
    StatType             Normal
    StatInterval         60
  }
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
}

IDSAction                                IPv6HopByHop
{
  ActionType                             Attack nodiscard
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IDSAction                                IPv6NextHeader
{
  ActionType                             Attack nodiscard
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IDSAction                                TcpQueueSize
{
  ActionType                             Attack noresetconn
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IDSAction                                GlobalTCPStall
{
  ActionType                             Attack noresetconn
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IDSAction                                Flood
{
  ActionType                             Attack discard
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IDSReportSet
{
    TypeActions          LOG
    LoggingLevel         4
    TypeActions          STATISTICS
    StatType             Normal
    StatInterval         60
}
}

IDSAction                Echo
{
    ActionType           Attack nodiscard
    IDSReportSet
    {
        TypeActions      LOG
        LoggingLevel     4
        TypeActions      STATISTICS
        StatType         Normal
        StatInterval     60
    }
}

IDSAction                IPv4Protocol
{
    ActionType           Attack nodiscard
    IDSReportSet
    {
        TypeActions      LOG
        LoggingLevel     4
        TypeActions      STATISTICS
        StatType         Normal
        StatInterval     60
    }
}

IDSAction                IPv4Option
{
    ActionType           Attack nodiscard
    IDSReportSet
    {
        TypeActions      LOG
        LoggingLevel     4
        TypeActions      STATISTICS
        StatType         Normal
        StatInterval     60
    }
}

IDSAction                ICMPRedirect
{
    ActionType           Attack nodiscard
    IDSReportSet
    {
        TypeActions      LOG
        LoggingLevel     4
        TypeActions      STATISTICS
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

        StatType          Normal
        StatInterval      60
    }
}

IDSAction          MalformedPacket
{
    ActionType        Attack discard
    IDSReportSet
    {
        TypeActions    LOG
        LoggingLevel    4
        TypeActions    STATISTICS
        StatType        Normal
        StatInterval    60
    }
}

IDSAction          IPv4OutboundRaw
{
    ActionType        Attack nodiscard
    IDSReportSet
    {
        TypeActions    LOG
        LoggingLevel    4
        TypeActions    STATISTICS
        StatType        Normal
        StatInterval    60
    }
}

IDSAction          Fragmentation
{
    ActionType        Attack nodiscard
    IDSReportSet
    {
        TypeActions    LOG
        LoggingLevel    4
        TypeActions    STATISTICS
        StatType        Normal
        StatInterval    60
    }
}

IDSAction          EEMalformedPacket
{
    ActionType        Attack nodiscard
    IDSReportSet
    {
        TypeActions    LOG
        LoggingLevel    4
        TypeActions    STATISTICS
        StatType        Normal
        StatInterval    60
    }
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IDSAction                                EELDLCCheck
{
  ActionType                             Attack nodiscard
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IDSAction                                EEPortCheck
{
  ActionType                             Attack nodiscard
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IDSAction                                EEXIDFlood
{
  ActionType                             Attack nodiscard
  IDSReportSet
  {
    TypeActions                          LOG
    LoggingLevel                         4
    TypeActions                          STATISTICS
    StatType                             Normal
    StatInterval                         60
  }
}

IpProtocolGroup                          IpProtGroup~1
{
  IpProtocolRangeRef                    IpProtRange~1
  IpProtocolRangeRef                    IpProtRange~2
  IpProtocolRangeRef                    IpProtRange~3
  IpProtocolRangeRef                    IpProtRange~4
}

IpProtocolGroup                          IpProtGroup~2
{
  IpProtocolRangeRef                    IpProtRange~5
  IpProtocolRangeRef                    IpProtRange~6
  IpProtocolRangeRef                    IpProtRange~7
  IpProtocolRangeRef                    IpProtRange~8
  IpProtocolRangeRef                    IpProtRange~9
  IpProtocolRangeRef                    IpProtRange~10
  IpProtocolRangeRef                    IpProtRange~11
  IpProtocolRangeRef                    IpProtRange~12
  IpProtocolRangeRef                    IpProtRange~13
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpProtocolGroup      IpProtGroup~3
{
    IpProtocolRangeRef  IpProtRange~14
    IpProtocolRangeRef  IpProtRange~15
    IpProtocolRangeRef  IpProtRange~16
    IpProtocolRangeRef  IpProtRange~17
}
IpProtocolRange      IpProtRange~1
{
    IpProtocol          0 16
}
IpProtocolRange      IpProtRange~2
{
    IpProtocol          18 57
}
IpProtocolRange      IpProtRange~3
{
    IpProtocol          59 88
}
IpProtocolRange      IpProtRange~4
{
    IpProtocol          90 255
}
IpProtocolRange      IpProtRange~5
{
    IpProtocol          0 0
}
IpProtocolRange      IpProtRange~6
{
    IpProtocol          3 3
}
IpProtocolRange      IpProtRange~7
{
    IpProtocol          5 5
}
IpProtocolRange      IpProtRange~8
{
    IpProtocol          7 16
}
IpProtocolRange      IpProtRange~9
{
    IpProtocol          18 45
}
IpProtocolRange      IpProtRange~10
{
    IpProtocol          48 49
}
IpProtocolRange      IpProtRange~11
{
    IpProtocol          52 88
}
IpProtocolRange      IpProtRange~12
{
    IpProtocol          90 93
}
IpProtocolRange      IpProtRange~13
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpProtocol          95 255
}
IpProtocolRange       IpProtRange~14
{
    IpProtocol          0 0
}
IpProtocolRange       IpProtRange~15
{
    IpProtocol          2 16
}
IpProtocolRange       IpProtRange~16
{
    IpProtocol          18 88
}
IpProtocolRange       IpProtRange~17
{
    IpProtocol          90 255
}
IpOptionGroup         IpOptGroup~1
{
    IpOptionRangeRef    IpOptRange~1
    IpOptionRangeRef    IpOptRange~2
    IpOptionRangeRef    IpOptRange~3
    IpOptionRangeRef    IpOptRange~4
    IpOptionRangeRef    IpOptRange~5
}
IpOptionGroup         IpOptGroup~2
{
    IpOptionRangeRef    IpOptRange~6
    IpOptionRangeRef    IpOptRange~7
    IpOptionRangeRef    IpOptRange~8
    IpOptionRangeRef    IpOptRange~9
    IpOptionRangeRef    IpOptRange~10
}
IpOptionGroup         IpOptGroup~3
{
    IpOptionRangeRef    IpOptRange~11
    IpOptionRangeRef    IpOptRange~12
    IpOptionRangeRef    IpOptRange~13
    IpOptionRangeRef    IpOptRange~14
    IpOptionRangeRef    IpOptRange~15
}
IpOptionRange         IpOptRange~1
{
    IpOption            2 3
}
IpOptionRange         IpOptRange~2
{
    IpOption            8 137
}
IpOptionRange         IpOptRange~3
{
    IpOption            139 193
}
IpOptionRange         IpOptRange~4
{
    IpOption            195 200

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}
IpOptionRange      IpOptRange~5
{
    IpOption        202 255
}
IpOptionRange      IpOptRange~6
{
    IpOption        2 3
}
IpOptionRange      IpOptRange~7
{
    IpOption        8 137
}
IpOptionRange      IpOptRange~8
{
    IpOption        139 193
}
IpOptionRange      IpOptRange~9
{
    IpOption        195 200
}
IpOptionRange      IpOptRange~10
{
    IpOption        202 255
}
IpOptionRange      IpOptRange~11
{
    IpOption        2 6
}
IpOptionRange      IpOptRange~12
{
    IpOption        8 67
}
IpOptionRange      IpOptRange~13
{
    IpOption        69 81
}
IpOptionRange      IpOptRange~14
{
    IpOption        83 147
}
IpOptionRange      IpOptRange~15
{
    IpOption        149 255
}
IPv6NextHdrGroup   IPv6NextHdrGroup~1
{
    IPv6NextHdrRangeRef  IPv6NextHdrRange~1
    IPv6NextHdrRangeRef  IPv6NextHdrRange~2
    IPv6NextHdrRangeRef  IPv6NextHdrRange~3
    IPv6NextHdrRangeRef  IPv6NextHdrRange~4
    IPv6NextHdrRangeRef  IPv6NextHdrRange~5
    IPv6NextHdrRangeRef  IPv6NextHdrRange~6
    IPv6NextHdrRangeRef  IPv6NextHdrRange~7
    IPv6NextHdrRangeRef  IPv6NextHdrRange~8
    IPv6NextHdrRangeRef  IPv6NextHdrRange~9
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IPv6NextHdrRange      IPv6NextHdrRange~1
{
  IPv6NextHdr          1  5
}
IPv6NextHdrRange      IPv6NextHdrRange~2
{
  IPv6NextHdr          7 16
}
IPv6NextHdrRange      IPv6NextHdrRange~3
{
  IPv6NextHdr          18 40
}
IPv6NextHdrRange      IPv6NextHdrRange~4
{
  IPv6NextHdr          42 42
}
IPv6NextHdrRange      IPv6NextHdrRange~5
{
  IPv6NextHdr          45 49
}
IPv6NextHdrRange      IPv6NextHdrRange~6
{
  IPv6NextHdr          52 57
}
IPv6NextHdrRange      IPv6NextHdrRange~7
{
  IPv6NextHdr          61 88
}
IPv6NextHdrRange      IPv6NextHdrRange~8
{
  IPv6NextHdr          90 134
}
IPv6NextHdrRange      IPv6NextHdrRange~9
{
  IPv6NextHdr          136 255
}
PortGroup              LocalEchoPortGroup~1
{
  PortRange
  {
    Port    7
  }
  PortRange
  {
    Port    13
  }
  PortRange
  {
    Port    17
  }
  PortRange
  {
    Port    19
  }
}
PortGroup              RemoteEchoPortGroup~1
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
PortRange
{
  Port 7
}
PortRange
{
  Port 13
}
PortRange
{
  Port 17
}
PortRange
{
  Port 19
}
}

IDSRule All_Well-Known_TCP~1
{
  Priority 65000
  ConditionType ScanEvent
  IDSScanEventCondition
  {
    Sensitivity MEDIUM
    Protocol TCP
    LocalPortRange 1-1023
  }
  IDSActionRef ScanAction
}

IDSRule All_Well-Known_UDP~1
{
  Priority 64990
  ConditionType ScanEvent
  IDSScanEventCondition
  {
    Sensitivity MEDIUM
    Protocol UDP
    LocalPortRange 1-1023
  }
  IDSActionRef ScanAction
}

IDSRule ICMP~1
{
  Priority 64980
  ConditionType ScanEvent
  IDSScanEventCondition
  {
    Sensitivity HIGH
    Protocol ICMP
  }
  IDSActionRef ScanAction
}

IDSRule ScanGlobal
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

{
  ConditionType          ScanGlobal
  IDSScanGlobalCondition
  {
    FSInterval           1
    FSThreshold           5
    SSInterval           120
    SSThreshold           10
  }
  IDSActionRef           ScanGlobalAction
}

IDSAction                ScanAction
{
  Actiontype             ScanEvent count
}

IDSAction                ScanGlobalAction
{
  ActionType             ScanGlobal
  IDSReportSet
  {
    TypeActions           LOG
    LogDetail             No
    LoggingLevel          4
  }
}

IDSRule                  TN3270-Server~1
{
  Priority                65000
  ConditionType           TR
  IDSTRCondition
  {
    LocalPortRange        23
    Protocol               TCP
    TRtcpTotalConnections  100
    TRtcpPercentage        3
    TRtcpLimitScope        PORT_INSTANCE
  }
  IDSActionRef            TN3270-Server
}

IDSAction                TN3270-Server
{
  ActionType             TR limit
  IDSReportSet
  {
    TypeActions           LOG
    LogDetail             No
    LoggingLevel          4
    TypeActions           STATISTICS
    StatType              Normal
    StatInterval          60
  }
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

***** **Lab L15 TMnx_IPSecVPN_wPreshare.policy** *****

```
##
## IPsec Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## End of Configuration Assistant information
```

```
## NOTE -- Generated IpGenericFilterAction Permit__LogYes
```

```
IpGenericFilterAction      Permit__LogYes
{
    IpFilterAction          Permit
    IpFilterLogging         Yes
    DiscardAction           Silent
}
```

```
IpGenericFilterAction      IpSec__LogYes
{
    IpFilterAction          IpSec
    IpFilterLogging         Yes
    DiscardAction           Silent
}
```

```
KeyExchangeOffer           VPN~A
{
    HowToEncrypt            AES_CBC KeyLength 128
    HowToAuthMsgs           SHA1
    HowToVerifyMsgs        HMAC_SHA1_96
    PseudoRandomFunction    HMAC_SHA1
    HowToAuthPeers          RsaSignature
    DHGroup                 Group2
    RefreshLifetimeProposed 1440
    RefreshLifetimeAccepted 1440 1440
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}
```

```
KeyExchangeOffer           VPN~A~5
{
    HowToEncrypt            AES_CBC KeyLength 128
    HowToAuthMsgs           SHA1
    HowToVerifyMsgs        HMAC_SHA1_96
    PseudoRandomFunction    HMAC_SHA1
    HowToAuthPeers          PresharedKey
    DHGroup                 Group2
    RefreshLifetimeProposed 1440
    RefreshLifetimeAccepted 1440 1440
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

RefreshLifesizeProposed      None
RefreshLifesizeAccepted     None
}

IpDataOffer                    VPN~A~R
{
    HowToEncap                  Transport
    HowToEncrypt                3DES
    HowToAuth                   ESP Hmac_Sha1
    RefreshLifetimeProposed     480
    RefreshLifetimeAccepted     480 480
    RefreshLifesizeProposed     None
    RefreshLifesizeAccepted     None
}

IpDataOffer                  VPN~A~N
{
    HowToEncap                  Tunnel
    HowToEncrypt                3DES
    HowToAuth                   ESP Hmac_Sha1
    RefreshLifetimeProposed     480
    RefreshLifetimeAccepted     480 480
    RefreshLifesizeProposed     None
    RefreshLifesizeAccepted     None
}

## NOTE -- Generated IpService IKE~Gen
IpService                      IKE~Gen
{
    Protocol                    UDP
    SourcePortRange             500
    DestinationPortRange       500
    Direction                   BiDirectional
    Routing                     Local
}

IpService                      FTP-Client
{
    Protocol                    TCP
    SourcePortRange             1024 65535
    DestinationPortRange       21
    Direction                   BiDirectional OutboundConnect
    Routing                     Local
}

IpService                      FTP-Client~1
{
    Protocol                    TCP
    SourcePortRange             1024 65535
    DestinationPortRange       20
    Direction                   BiDirectional InboundConnect
    Routing                     Local
}

IpService                      FTP-Client~2
{
    Protocol                    TCP

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortRange      1024 65535
DestinationPortRange 50000 50200
Direction            BiDirectional OutboundConnect
Routing              Local
}
```

```
IpService            FTP-Server
{
  Protocol            TCP
  SourcePortRange     21
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}
```

```
IpService            FTP-Server~3
{
  Protocol            TCP
  SourcePortRange     20
  DestinationPortRange 1024 65535
  Direction            BiDirectional OutboundConnect
  Routing              Local
}
```

```
IpService            FTP-Server~4
{
  Protocol            TCP
  SourcePortRange     50000 50200
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}
```

```
IpService            CICS
{
  Protocol            TCP
  SourcePortRange     3000
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}
```

```
IpService            All_other_traffic
{
  Protocol            All
  Direction            BiDirectional
  Routing              Routed
}
```

```
IpService            TN3270-Server
{
  Protocol            TCP
  SourcePortRange     23
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                DNS
{
  Protocol                               UDP
  SourcePortRange                        53
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                DNS~7
{
  Protocol                               UDP
  SourcePortRange                        53
  DestinationPortRange                  53
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                DNS~8
{
  Protocol                               TCP
  SourcePortRange                        53
  DestinationPortRange                  1024 65535
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                DNS~9
{
  Protocol                               TCP
  SourcePortRange                        53
  DestinationPortRange                  53
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                ICMP-Time_Exceeded-IP_V4
{
  Protocol                               ICMP
  Type                                  11
  Code                                  Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                ICMP-Unreachable-IP_V4
{
  Protocol                               ICMP
  Type                                  3
  Code                                  Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                OMPROUTE-IP_V4
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Protocol      OSPF
Type          Any
Direction    BiDirectional
Routing       Local
}

IpService     OMPROUTE-IP_V4~10
{
  Protocol    IGMP
  Direction   BiDirectional
  Routing      Local
}

IpService     OMPROUTE-IP_V4~11
{
  Protocol    UDP
  SourcePortRange 520
  DestinationPortRange 1024 65535
  Direction   BiDirectional
  Routing      Local
}

IpService     OMPROUTE-IP_V4~12
{
  Protocol    UDP
  SourcePortRange 1024 65535
  DestinationPortRange 520
  Direction   BiDirectional
  Routing      Local
}

IpService     OMPROUTE-IP_V4~13
{
  Protocol    UDP
  SourcePortRange 520
  DestinationPortRange 520
  Direction   BiDirectional
  Routing      Local
}

IpService     Path_MTU_Discovery-IP_V4
{
  Protocol    ICMP
  Type        3
  Code        4
  Direction   BiDirectional
  Routing      Local
}

IpService     Ping-IP_V4
{
  Protocol    ICMP
  Type        8
  Code        Any
  Direction   BiDirectional
  Routing      Local
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                Ping-IP_V4~14
{
  Protocol                               ICMP
  Type                                   0
  Code                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Resolver
{
  Protocol                               TCP
  SourcePortRange                        1024 65535
  DestinationPortRange                  53
  Direction                             BiDirectional OutboundConnect
  Routing                               Local
}

IpService                                Resolver~15
{
  Protocol                               UDP
  SourcePortRange                        1024 65535
  DestinationPortRange                  53
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Trace_Route-IP_V4
{
  Protocol                               ICMP
  Type                                   11
  Code                                   0
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Trace_Route-IP_V4~16
{
  Protocol                               ICMP
  Type                                   3
  Code                                   3
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Trace_Route-IP_V4~17
{
  Protocol                               ICMP
  Type                                   3
  Code                                   2
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Trace_Route-IP_V4~18
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Protocol                UDP
SourcePortRange         1024 65535
DestinationPortRange    33435 33535
Direction               BiDirectional
Routing                 Local
}

IpDynVpnAction           VPN~A
{
  Initiation             Either
  VpnLife                1440
  InitiateWithPfs        Group2
  IpDataOfferRef         VPN~A~R
  AcceptablePfs          None
  AcceptablePfs          Group2
  PassthroughDF          Yes
  PassthroughDSCP        Yes
  HowToEncapIkev2        Either
}

IpDynVpnAction          VPN~A~6
{
  Initiation            Either
  VpnLife               1440
  InitiateWithPfs       Group2
  IpDataOfferRef        VPN~A~N
  AcceptablePfs         None
  AcceptablePfs         Group2
  PassthroughDF         Yes
  PassthroughDSCP       Yes
  HowToEncapIkev2       Either
}
##
## Connectivity Rule BetweenOSAsRSA combines the following items:
##   Local data endpoint      BetweenOSAsRSA~ADR~1
##   Remote data endpoint    BetweenOSAsRSA~ADR~2
##   Topology                 Host to Host
##   Requirement Map
##     FTP-Client             => VPN~A
##     FTP-Server             => VPN~A

IpAddr                  BetweenOSAsRSA~ADR~1
{
  Addr                   192.168.20.97
}

IpAddr                  BetweenOSAsRSA~ADR~2
{
  Addr                   192.168.20.91
}

LocalSecurityEndpoint   BetweenOSAsRSA~LSE~4
{
  Identity               IpAddr 192.168.20.97
  LocationRef            BetweenOSAsRSA~ADR~1
}

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteSecurityEndpoint      BetweenOSAsRSA~RSE~3
{
  Identity                  IpAddr 192.168.20.91
  LocationRef               BetweenOSAsRSA~ADR~2
}
```

```
KeyExchangeRule            BetweenOSAsRSA~5
{
  LocalSecurityEndpointRef  BetweenOSAsRSA~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA~RSE~3
  KeyExchangeActionRef      BetweenOSAsRSA
}
```

```
KeyExchangeAction          BetweenOSAsRSA
{
  HowToRespondIKEv1        Either
  KeyExchangeOfferRef       VPN~A
  AllowNat                  No
  ReauthInterval            0
  ConstrainSource           192.168.20.97
  ConstrainDest             192.168.20.91
}
```

```
IpLocalStartAction         BetweenOSAsRSA~8
{
  AllowOnDemand             No
  LocalPortGranularity      Rule
  RemotePortGranularity     Rule
  ProtocolGranularity       Rule
  RemoteIpGranularity       Packet
  LocalIpGranularity        Packet
  IcmpCodeGranularity       Rule
  IcmpTypeGranularity       Rule
  IcmpV6CodeGranularity     Rule
  IcmpV6TypeGranularity     Rule
  MipV6TypeGranularity      Rule
  LocalSecurityEndpointRef  BetweenOSAsRSA~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA~RSE~3
}
```

NOTE -- Generated IpFilterRule BetweenOSAsRSA~6

```
IpFilterRule               BetweenOSAsRSA~6
{
  IpSourceAddrRef          BetweenOSAsRSA~ADR~1
  IpDestAddrRef            BetweenOSAsRSA~ADR~2
  IpServiceRef              IKE~Gen
  IpGenericFilterActionRef  Permit__LogYes
}
```

```
IpFilterRule               BetweenOSAsRSA~7
{
  IpSourceAddrRef          BetweenOSAsRSA~ADR~1
  IpDestAddrRef            BetweenOSAsRSA~ADR~2
  IpServiceRef              FTP-Client
  IpGenericFilterActionRef  IpSec__LogYes
  IpDynVpnActionRef        VPN~A
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                BetweenOSAsRSA~9
{
    IpSourceAddrRef                         BetweenOSAsRSA~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA~ADR~2
    IpServiceRef                             FTP-Client~1
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
    IpLocalStartActionRef                   BetweenOSAsRSA~8
}

IpFilterRule                                BetweenOSAsRSA~10
{
    IpSourceAddrRef                         BetweenOSAsRSA~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA~ADR~2
    IpServiceRef                             FTP-Client~2
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
}

IpFilterRule                                BetweenOSAsRSA~12
{
    IpSourceAddrRef                         BetweenOSAsRSA~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA~ADR~2
    IpServiceRef                             FTP-Server
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
    IpLocalStartActionRef                   BetweenOSAsRSA~8
}

IpFilterRule                                BetweenOSAsRSA~13
{
    IpSourceAddrRef                         BetweenOSAsRSA~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA~ADR~2
    IpServiceRef                             FTP-Server~3
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
}

IpFilterRule                                BetweenOSAsRSA~15
{
    IpSourceAddrRef                         BetweenOSAsRSA~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA~ADR~2
    IpServiceRef                             FTP-Server~4
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
    IpLocalStartActionRef                   BetweenOSAsRSA~8
}
##
## Connectivity Rule TrafficBetweenVIPAs combines the following items:
##   Local data endpoint                     TrafficBetweenVIPAs~ADR~1
##   Remote data endpoint                   TrafficBetweenVIPAs~ADR~2
##   Topology                               Filtering - Host
##   Requirement Map
##     CICS                                 => Permit
##     FTP-Client                           => Permit
##     FTP-Server                           => Permit

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpAddr                                TrafficBetweenVIPAs~ADR~1
{
  Addr                                192.168.20.107
}

IpAddr                                TrafficBetweenVIPAs~ADR~2
{
  Addr                                192.168.20.101
}

IpFilterRule                          TrafficBetweenVIPAs~3
{
  IpSourceAddrRef                    TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                      TrafficBetweenVIPAs~ADR~2
  IpServiceRef                      CICS
  IpGenericFilterActionRef          Permit__LogYes
}

IpFilterRule                          TrafficBetweenVIPAs~4
{
  IpSourceAddrRef                    TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                      TrafficBetweenVIPAs~ADR~2
  IpServiceRef                      FTP-Client
  IpGenericFilterActionRef          Permit__LogYes
}

IpFilterRule                          TrafficBetweenVIPAs~5
{
  IpSourceAddrRef                    TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                      TrafficBetweenVIPAs~ADR~2
  IpServiceRef                      FTP-Client~1
  IpGenericFilterActionRef          Permit__LogYes
}

IpFilterRule                          TrafficBetweenVIPAs~6
{
  IpSourceAddrRef                    TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                      TrafficBetweenVIPAs~ADR~2
  IpServiceRef                      FTP-Client~2
  IpGenericFilterActionRef          Permit__LogYes
}

IpFilterRule                          TrafficBetweenVIPAs~7
{
  IpSourceAddrRef                    TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                      TrafficBetweenVIPAs~ADR~2
  IpServiceRef                      FTP-Server
  IpGenericFilterActionRef          Permit__LogYes
}

IpFilterRule                          TrafficBetweenVIPAs~8
{
  IpSourceAddrRef                    TrafficBetweenVIPAs~ADR~1
  IpDestAddrRef                      TrafficBetweenVIPAs~ADR~2
  IpServiceRef                      FTP-Server~3
  IpGenericFilterActionRef          Permit__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}

IpFilterRule                                     TrafficBetweenVIPAs~9
{
    IpSourceAddrRef                             TrafficBetweenVIPAs~ADR~1
    IpDestAddrRef                               TrafficBetweenVIPAs~ADR~2
    IpServiceRef                                FTP-Server~4
    IpGenericFilterActionRef                     Permit__LogYes
}
##
## Connectivity Rule TrafOSA2DVIPAPresh combines the following items:
##   Local data endpoint                       TrafOSA2DVIPAPresh~ADR~1
##   Remote data endpoint                     TrafOSA2DVIPAPresh~ADR~2
##   Topology                                Gateway to Host
##   Requirement Map                         EncryptedPing
##   All_other_traffic                       => VPN~A

IpAddr                                           TrafOSA2DVIPAPresh~ADR~1
{
    Addr                                         192.168.20.127
}

IpAddr                                           TrafOSA2DVIPAPresh~ADR~2
{
    Addr                                         192.168.20.121
}

LocalSecurityEndpoint                           TrafOSA2DVIPAPresh~LSE~4
{
    Identity                                    Fqdn WSC.LABS.IBM.COM
    Location                                    192.168.20.97
}

RemoteSecurityEndpoint                         TrafOSA2DVIPAPresh~RSE~3
{
    Identity                                    UserAtFqdn ZOS1@WSC.LABS.IBM.COM
    LocationRef                                TrafOSA2DVIPAPresh~ADR~2
}

KeyExchangeRule                                TrafOSA2DVIPAPresh~5
{
    LocalSecurityEndpointRef                   TrafOSA2DVIPAPresh~LSE~4
    RemoteSecurityEndpointRef                 TrafOSA2DVIPAPresh~RSE~3
    KeyExchangeActionRef                     TrafOSA2DVIPAPresh
    SharedKey                                 Ebcdic "userlabs"
}

KeyExchangeAction                              TrafOSA2DVIPAPresh
{
    HowToRespondIKEv1                         Either
    KeyExchangeOfferRef                       VPN~A~5
    AllowNat                                   No
    ReauthInterval                            0
    ConstrainSource                           192.168.20.127
    ConstrainDest                             192.168.20.121
    HowToAuthMe                               PresharedKey
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpLocalStartAction                                TrafOSA2DVIPAPresh~7
{
    AllowOnDemand                                    Yes
    LocalPortGranularity                            Rule
    RemotePortGranularity                          Rule
    ProtocolGranularity                            Rule
    RemoteIpGranularity                            Packet
    LocalIpGranularity                             Packet
    IcmpCodeGranularity                            Rule
    IcmpTypeGranularity                            Rule
    IcmpV6CodeGranularity                          Rule
    IcmpV6TypeGranularity                          Rule
    MipV6TypeGranularity                           Rule
    LocalSecurityEndpointRef                       TrafOSA2DVIPAPresh~LSE~4
    RemoteSecurityEndpointRef                     TrafOSA2DVIPAPresh~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh~6
IpFilterRule                                       TrafOSA2DVIPAPresh~6
{
    IpSourceAddr                                    192.168.20.97
    IpDestAddrRef                                   TrafOSA2DVIPAPresh~ADR~2
    IpServiceRef                                    IKE~Gen
    IpGenericFilterActionRef                       Permit__LogYes
}

IpFilterRule                                       TrafOSA2DVIPAPresh~8
{
    IpSourceAddrRef                                 TrafOSA2DVIPAPresh~ADR~1
    IpDestAddrRef                                   TrafOSA2DVIPAPresh~ADR~2
    IpServiceRef                                    All_other_traffic
    IpGenericFilterActionRef                       IpSec__LogYes
    IpDynVpnActionRef                             VPN~A~6
    IpLocalStartActionRef                         TrafOSA2DVIPAPresh~7
}
##
## Connectivity Rule WStoVIPA combines the following items:
##   Local data endpoint      WStoVIPA~ADR~1
##   Remote data endpoint     All4
##   Topology                 Filtering - Host
##   Requirement Map
##     FTP-Server              => Permit
##     TN3270-Server           => Permit

IpAddr                                             WStoVIPA~ADR~1
{
    Addr                                             192.168.20.107
}

IpFilterRule                                       WStoVIPA~2
{
    IpSourceAddrRef                                 WStoVIPA~ADR~1
    IpDestAddr                                       All4
    IpServiceRef                                    FTP-Server
    IpGenericFilterActionRef                       Permit__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRule                                WStoVIPA~3
{
    IpSourceAddrRef                        WStoVIPA~ADR~1
    IpDestAddr                            All4
    IpServiceRef                          FTP-Server~3
    IpGenericFilterActionRef              Permit__LogYes
}

IpFilterRule                                WStoVIPA~4
{
    IpSourceAddrRef                        WStoVIPA~ADR~1
    IpDestAddr                            All4
    IpServiceRef                          FTP-Server~4
    IpGenericFilterActionRef              Permit__LogYes
}

IpFilterRule                                WStoVIPA~5
{
    IpSourceAddrRef                        WStoVIPA~ADR~1
    IpDestAddr                            All4
    IpServiceRef                          TN3270-Server
    IpGenericFilterActionRef              Permit__LogYes
}
##
## Connectivity Rule CommonTraffic combines the following items:
##   Local data endpoint                    All4
##   Remote data endpoint                  All4
##   Topology                             Filtering - Host
##   Requirement Map
##     DNS                                => Permit
##     ICMP-Time_Exceeded-IP_V4           => Permit
##     ICMP-Unreachable-IP_V4             => Permit
##     OMPROUTE-IP_V4                     => Permit
##     Path_MTU_Discovery-IP_V4           => Permit
##     Ping-IP_V4                         => Permit
##     Resolver                           => Permit
##     Trace_Route-IP_V4                  => Permit

IpFilterRule                                CommonTraffic~1
{
    IpSourceAddr                          All4
    IpDestAddr                            All4
    IpServiceRef                          DNS
    IpGenericFilterActionRef              Permit__LogYes
}

IpFilterRule                                CommonTraffic~2
{
    IpSourceAddr                          All4
    IpDestAddr                            All4
    IpServiceRef                          DNS~7
    IpGenericFilterActionRef              Permit__LogYes
}

IpFilterRule                                CommonTraffic~3
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       DNS~8
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~4
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       DNS~9
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~5
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       ICMP-Time_Exceeded-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~6
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       ICMP-Unreachable-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~7
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       OMPROUTE-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~8
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       OMPROUTE-IP_V4~10
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~9
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       OMPROUTE-IP_V4~11
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~10
{
    IpSourceAddr      All4
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    IpDestAddr      All4
    IpServiceRef    OMPROUTE-IP_V4~12
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~11
{
    IpSourceAddr   All4
    IpDestAddr     All4
    IpServiceRef   OMPROUTE-IP_V4~13
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~12
{
    IpSourceAddr   All4
    IpDestAddr     All4
    IpServiceRef   Path_MTU_Discovery-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~13
{
    IpSourceAddr   All4
    IpDestAddr     All4
    IpServiceRef   Ping-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~14
{
    IpSourceAddr   All4
    IpDestAddr     All4
    IpServiceRef   Ping-IP_V4~14
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~15
{
    IpSourceAddr   All4
    IpDestAddr     All4
    IpServiceRef   Resolver
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~16
{
    IpSourceAddr   All4
    IpDestAddr     All4
    IpServiceRef   Resolver~15
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      CommonTraffic~17
{
    IpSourceAddr   All4
    IpDestAddr     All4
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpServiceRef          Trace_Route-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              CommonTraffic~18
{
    IpSourceAddr          All4
    IpDestAddr            All4
    IpServiceRef          Trace_Route-IP_V4~16
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              CommonTraffic~19
{
    IpSourceAddr          All4
    IpDestAddr            All4
    IpServiceRef          Trace_Route-IP_V4~17
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              CommonTraffic~20
{
    IpSourceAddr          All4
    IpDestAddr            All4
    IpServiceRef          Trace_Route-IP_V4~18
    IpGenericFilterActionRef Permit__LogYes
}

KeyExchangePolicy
{
    AllowNat                No
    NatKeepAliveInterval    20
    HowToInitiate           Main
    LivenessInterval        30
    BypassIpValidation      Yes
    CertificateURLLookupPreference Tolerate
    RevocationChecking       Loose
    KeyExchangeRuleRef       BetweenOSAsRSA~5
    KeyExchangeRuleRef      TrafOSA2DVIPAPresh~5
}

IpFilterPolicy
{
    PreDecap                OFF
    FilterLogging            ON
    IpFilterLogImplicit      No
    AllowOnDemand            Yes
    ImplicitDiscardAction    Silent
    FIPS140                  No
    IpFilterRuleRef          BetweenOSAsRSA~6
    IpFilterRuleRef          BetweenOSAsRSA~7
    IpFilterRuleRef          BetweenOSAsRSA~9
    IpFilterRuleRef          BetweenOSAsRSA~10
    IpFilterRuleRef          BetweenOSAsRSA~12
    IpFilterRuleRef          BetweenOSAsRSA~13
    IpFilterRuleRef          BetweenOSAsRSA~15
    IpFilterRuleRef          TrafficBetweenVIPAs~3

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRuleRef      TrafficBetweenVIPAs~4
IpFilterRuleRef      TrafficBetweenVIPAs~5
IpFilterRuleRef      TrafficBetweenVIPAs~6
IpFilterRuleRef      TrafficBetweenVIPAs~7
IpFilterRuleRef      TrafficBetweenVIPAs~8
IpFilterRuleRef      TrafficBetweenVIPAs~9
IpFilterRuleRef      TrafOSA2DVIPAPresh~6
IpFilterRuleRef      TrafOSA2DVIPAPresh~8
IpFilterRuleRef      WStoVIPA~2
IpFilterRuleRef      WStoVIPA~3
IpFilterRuleRef      WStoVIPA~4
IpFilterRuleRef      WStoVIPA~5
IpFilterRuleRef      CommonTraffic~1
IpFilterRuleRef      CommonTraffic~2
IpFilterRuleRef      CommonTraffic~3
IpFilterRuleRef      CommonTraffic~4
IpFilterRuleRef      CommonTraffic~5
IpFilterRuleRef      CommonTraffic~6
IpFilterRuleRef      CommonTraffic~7
IpFilterRuleRef      CommonTraffic~8
IpFilterRuleRef      CommonTraffic~9
IpFilterRuleRef      CommonTraffic~10
IpFilterRuleRef      CommonTraffic~11
IpFilterRuleRef      CommonTraffic~12
IpFilterRuleRef      CommonTraffic~13
IpFilterRuleRef      CommonTraffic~14
IpFilterRuleRef      CommonTraffic~15
IpFilterRuleRef      CommonTraffic~16
IpFilterRuleRef      CommonTraffic~17
IpFilterRuleRef      CommonTraffic~18
IpFilterRuleRef      CommonTraffic~19
IpFilterRuleRef      CommonTraffic~20
}
```

**** **Lab L16 TMnx_ATTLS_wNSS.policy** ****

```
*****
##
## AT-TLS Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
Server
## Version 2 Release 3
## Backing Store = Team72
## Install History:
##
## TLS default rules: TN3270-WS-to-Host (c)
##                      NSS_Client-IKED (c)
##                      NSS_Server (c)
## End TLS default rules
##
## End of Configuration Assistant information
TTLSRule      VIPAs2VIPAs~1
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

LocalAddrSetRef      addr1
RemoteAddrSetRef      addr1
LocalPortRangeRef     portR1
RemotePortRangeRef    portR2
Userid                USER*
Direction             Outbound
Priority               255
TTLSGroupActionRef    gAct1
TTLSEnvironmentActionRef eAct1~AllSecFTPclients
TTLSCONNECTIONActionRef cAct1~AllSecFTPclients
}
TTLRule               VIPAs2VIPAs~2
{
  LocalAddrSetRef      addr1
  RemoteAddrSetRef      addr1
  LocalPortRangeRef     portR2
  RemotePortRangeRef    portR1
  Direction             Inbound
  Priority               254
  TTLSGroupActionRef    gAct1
  TTLSEnvironmentActionRef eAct2~FTP-Server
  TTLSCONNECTIONActionRef cAct2~FTP-Server
}
TTLRule               TN3270-WS-to-Host~3
{
  LocalAddrSetRef      addr1
  RemoteAddrSetRef      addr2
  LocalPortRangeRef     portR3
  RemotePortRangeRef    portR1
  Direction             Inbound
  Priority               253
  TTLSGroupActionRef    gAct1
  TTLSEnvironmentActionRef eAct3~TN3270DiffKeyring
  TTLSCONNECTIONActionRef cAct3~TN3270DiffKeyring
}
TTLRule             NSS_Client-IKED~4
{
  LocalAddr           ALL
  RemoteAddr          ALL
  LocalPortRangeRef    portR1
  RemotePortRangeRef  portR4
  Direction           Outbound
  Priority             252
  TTLSGroupActionRef   gAct1
  TTLSEnvironmentActionRef eAct4~NSS-Client
  TTLSCONNECTIONActionRef cAct4~NSS-Client
}
TTLRule             NSS_Server~5
{
  LocalAddr           ALL
  RemoteAddr          ALL
  LocalPortRangeRef    portR4
  RemotePortRangeRef  portR1
  Direction           Inbound
  Priority             251
  TTLSGroupActionRef   gAct1
  TTLSEnvironmentActionRef eAct5~NSSD

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

TTLSTConnectionActionRef      cAct5~NSSD
}
TTLSTGroupAction                gAct1
{
    TTLSEnabled                  On
    Trace                        2
}
TTLSTEnvironmentAction          eAct1~AllSecFTPCLients
{
    HandshakeRole                Client
    EnvironmentUserInstance       0
    TTLSTKeyringParmsRef         keyR1
}
TTLSTEnvironmentAction          eAct2~FTP-Server
{
    HandshakeRole                ServerWithClientAuth
    EnvironmentUserInstance       0
    TTLSTKeyringParmsRef         keyR~ZOS7
    TTLSTGskAdvancedParmsRef     gskAdv1~ATTLSGoldwClientAuth
}
TTLSTEnvironmentAction          eAct3~TN3270DiffKeyring
{
    HandshakeRole                ServerWithClientAuth
    EnvironmentUserInstance       0
    TTLSTKeyringParmsRef         keyR3
    TTLSTGskAdvancedParmsRef     gskAdv1~ATTLSGoldwClientAuth
}
TTLSTEnvironmentAction      eAct4~NSS-Client
{
    HandshakeRole            Client
    EnvironmentUserInstance   0
    TTLSTKeyringParmsRef     keyR4
}
TTLSTEnvironmentAction      eAct5~NSSD
{
    HandshakeRole            Server
    EnvironmentUserInstance   0
    TTLSTKeyringParmsRef     keyR5
}
TTLSTConnectionAction           cAct1~AllSecFTPCLients
{
    HandshakeRole                Client
    TTLSTCipherParmsRef          cipher1
    TTLSTConnectionAdvancedParmsRef cAdv1~AllSecFTPCLients
    CtraceClearText              Off
    Trace                        2
}
TTLSTConnectionAction           cAct2~FTP-Server
{
    HandshakeRole                ServerWithClientAuth
    TTLSTCipherParmsRef          cipher1
    TTLSTConnectionAdvancedParmsRef cAdv2~FTP-Server
    CtraceClearText              Off
    Trace                        2
}
TTLSTConnectionAction           cAct3~TN3270DiffKeyring
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

HandshakeRole          ServerWithClientAuth
TTLSCipherParmsRef     cipher1
TTLSCConnectionAdvancedParmsRef cAdv3~TN3270DiffKeyring
CtraceClearText        Off
Trace                  2
}
TTLSCConnectionAction      cAct4~NSS-Client
{
  HandshakeRole            Client
  TTLSCipherParmsRef       cipher2~Default_Ciphers
  TTLSCConnectionAdvancedParmsRef cAdv4~NSS-Client
  CtraceClearText         Off
  Trace                   2
}
TTLSCConnectionAction      cAct5~NSSD
{
  HandshakeRole            Server
  TTLSCipherParmsRef       cipher2~Default_Ciphers
  TTLSCConnectionAdvancedParmsRef cAdv5~NSSD
  CtraceClearText         Off
  Trace                   2
}
TTLSCConnectionAdvancedParms cAdv1~AllSecFTPCLients
{
  SSLv3                  On
  TLSv1                  On
  TLSv1.1                On
  ApplicationControlled  On
  SecondaryMap            On
  TLSv1.2                Off
}
TTLSCConnectionAdvancedParms cAdv2~FTP-Server
{
  SSLv3                  On
  TLSv1                  On
  TLSv1.1                On
  ApplicationControlled  On
  SecondaryMap            On
  TLSv1.2                On
}
TTLSCConnectionAdvancedParms cAdv3~TN3270DiffKeyring
{
  SSLv3                  On
  TLSv1                  On
  TLSv1.1                On
  ApplicationControlled  On
  SecondaryMap            Off
  TLSv1.2                On
}
TTLSCConnectionAdvancedParms cAdv4~NSS-Client
{
  SSLv3                  On
  TLSv1                  On
  TLSv1.1                On
  ApplicationControlled On
  SecondaryMap           Off
  TLSv1.2                Off
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}
TTLSTConnectionAdvancedParms      cAdv5~NSSD
{
    SSLv3                            On
    TLSv1                            On
    TLSv1.1                          On
    ApplicationControlled            On
    SecondaryMap                     Off
    TLSv1.2                          Off
}
TTLSTKeyringParms                  keyR1
{
    Keyring                          LabClientRing
}
TTLSTKeyringParms                  keyR~ZOS7
{
    Keyring                          FTPD/ServerRing1
}
TTLSTKeyringParms                  keyR3
{
    Keyring                          TN3270/MyServer7Ring
}
TTLSTKeyringParms                  keyR4
{
    Keyring                          *AUTH*/*
}
TTLSTKeyringParms                  keyR5
{
    Keyring                          NSSD/NSSD7Ring
}
TTLSTGskAdvancedParms              gskAdv1~ATTLSGoldwClientAuth
{
    TTLSTGskHttpCdpParmsRef          gskHttp
}
TTLSTCipherParms                  cipher1
{
    V3CipherSuites                    TLS_RSA_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                    TLS_RSA_WITH_AES_128_CBC_SHA
}
TTLSTCipherParms                  cipher2~Default_Ciphers
{
    V3CipherSuites                    TLS_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites                    TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites                    TLS_DH_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites                    TLS_DHE_DSS_WITH_AES_256_CBC_SHA
    V3CipherSuites                    TLS_DH_DSS_WITH_AES_256_CBC_SHA
    V3CipherSuites                    TLS_RSA_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                    TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                    TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                    TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                    TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                    TLS_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites                    TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites                    TLS_DH_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites                    TLS_DHE_DSS_WITH_AES_128_CBC_SHA
    V3CipherSuites                    TLS_DH_DSS_WITH_AES_128_CBC_SHA
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

TTLSGskHttpCdpParms      gskHttp
{
    HTTPCDPENABLE        OFF
}
IpAddrSet                addr1
{
    Range                192.168.20.101-192.168.20.107
}
IpAddrSet                addr2
{
    Prefix               192.168.0.0/16
}
PortRange                portR1
{
    Port                1024-65535
}
PortRange                portR2
{
    Port                21
}
PortRange                portR3
{
    Port                23
}
PortRange                portR4
{
    Port                4159
}

##
## CA generated policy statements for TTLSRule(s) in support of NSS
function.
##

TTLSGroupAction          NSS~TLS~ON
{
    TTLSEnabled          On
}
TTLSCipherParms         NSS~CIPHER~PARMS
{
    V3CipherSuites      TLS_RSA_WITH_3DES_EDE_CBC_SHA
}
TTLSEnvironmentAction   NSS~TLS~CLIENT~ENV
{
    HandShakeRole        Client
    TTLSCipherParmsRef   NSS~CIPHER~PARMS
    TTLSKeyRingParms
    {
        Keyring          *AUTH*/*
    }
}
## Rule from client to server ZOS7
TTLSRule                 NSS~TLS~CLIENT~1
{
    RemotePortRange      4159
    Direction            Outbound
    TTLSGroupActionRef    NSS~TLS~ON
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
TTLSEnvironmentActionRef  NSS~TLS~CLIENT~ENV
}
TTLSEnvironmentAction      NSS~TLS~SERVER~ENV
{
    HandShakeRole           Server
    TTLSCTCipherParmsRef    NSS~CIPHER~PARMS
    TTLSKeyRingParms
    {
        Keyring             NSSD/NSSD7Ring
    }
}
TTLRule                    NSS~TLS~SERVER
{
    LocalPortRange          4159
    Direction               Inbound
    TTLSGroupActionRef      NSS~TLS~ON
    TTLSEnvironmentActionRef NSS~TLS~SERVER~ENV
}
*****
```

***** **Lab L16 TMnx_IPSecVPN_wlKEv2.policy** *****

```
##
## IPsec Policy Agent Configuration file for:
##   Image: ZOS7
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS Communications
Server
## Version 2 Release 3
## Backing Store = TTLab16
## Install History:
##
## End of Configuration Assistant information

## NOTE -- Generated IpGenericFilterAction Permit__LogYes
IpGenericFilterAction      Permit__LogYes
{
    IpFilterAction          Permit
    IpFilterLogging          Yes
    DiscardAction            Silent
}

IpGenericFilterAction      IpSec__LogYes
{
    IpFilterAction          IpSec
    IpFilterLogging          Yes
    DiscardAction            Silent
}

KeyExchangeOffer           VPN~A
{
    HowToEncrypt            AES_CBC KeyLength 128
    HowToAuthMsgs           SHA1
    HowToVerifyMsgs         HMAC_SHA1_96
    PseudoRandomFunction    HMAC_SHA1
}
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    HowToAuthPeers          RsaSignature
    DHGroup                 Group2
    RefreshLifetimeProposed 1440
    RefreshLifetimeAccepted 1440 1440
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}

KeyExchangeOffer           VPN~A~5
{
    HowToEncrypt           AES_CBC KeyLength 128
    HowToAuthMsgs          SHA1
    HowToVerifyMsgs        HMAC_SHA1_96
    PseudoRandomFunction   HMAC_SHA1
    HowToAuthPeers          PresharedKey
    DHGroup                 Group2
    RefreshLifetimeProposed 1440
    RefreshLifetimeAccepted 1440 1440
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}

IpDataOffer                VPN~A~R
{
    HowToEncap              Transport
    HowToEncrypt             3DES
    HowToAuth                ESP Hmac_Sha1
    RefreshLifetimeProposed  480
    RefreshLifetimeAccepted  480 480
    RefreshLifesizeProposed  None
    RefreshLifesizeAccepted  None
}

IpDataOffer                VPN~A~N
{
    HowToEncap              Tunnel
    HowToEncrypt             3DES
    HowToAuth                ESP Hmac_Sha1
    RefreshLifetimeProposed  480
    RefreshLifetimeAccepted  480 480
    RefreshLifesizeProposed  None
    RefreshLifesizeAccepted  None
}

## NOTE -- Generated IpService IKE~Gen
IpService                   IKE~Gen
{
    Protocol                 UDP
    SourcePortRange          500
    DestinationPortRange     500
    Direction                 BiDirectional
    Routing                   Local
}

IpService                   FTP-Client
{
    Protocol                 TCP

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortRange      1024 65535
DestinationPortRange 21
Direction            BiDirectional OutboundConnect
Routing              Local
}

IpService             FTP-Client~1
{
  Protocol            TCP
  SourcePortRange     1024 65535
  DestinationPortRange 20
  Direction            BiDirectional InboundConnect
  Routing              Local
}

IpService             FTP-Client~2
{
  Protocol            TCP
  SourcePortRange     1024 65535
  DestinationPortRange 50000 50200
  Direction            BiDirectional OutboundConnect
  Routing              Local
}

IpService             FTP-Server
{
  Protocol            TCP
  SourcePortRange     21
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}

IpService             FTP-Server~3
{
  Protocol            TCP
  SourcePortRange     20
  DestinationPortRange 1024 65535
  Direction            BiDirectional OutboundConnect
  Routing              Local
}

IpService             FTP-Server~4
{
  Protocol            TCP
  SourcePortRange     50000 50200
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
  Routing              Local
}

IpService             CICS
{
  Protocol            TCP
  SourcePortRange     3000
  DestinationPortRange 1024 65535
  Direction            BiDirectional InboundConnect
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Routing                                     Local
}

IpService                                   All_other_traffic
{
  Protocol                                   All
  Direction                                 BiDirectional
  Routing                                   Routed
}

IpService                                   TN3270-Server
{
  Protocol                                   TCP
  SourcePortRange                           23
  DestinationPortRange                      1024 65535
  Direction                                 BiDirectional InboundConnect
  Routing                                   Local
}

IpService                                   DNS
{
  Protocol                                   UDP
  SourcePortRange                           53
  DestinationPortRange                      1024 65535
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   DNS~7
{
  Protocol                                   UDP
  SourcePortRange                           53
  DestinationPortRange                      53
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   DNS~8
{
  Protocol                                   TCP
  SourcePortRange                           53
  DestinationPortRange                      1024 65535
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   DNS~9
{
  Protocol                                   TCP
  SourcePortRange                           53
  DestinationPortRange                      53
  Direction                                 BiDirectional
  Routing                                   Local
}

IpService                                   ICMP-Time_Exceeded-IP_V4
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Protocol      ICMP
Type          11
Code          Any
Direction     BiDirectional
Routing       Local
}

IpService     ICMP-Unreachable-IP_V4
{
  Protocol    ICMP
  Type        3
  Code        Any
  Direction   BiDirectional
  Routing     Local
}

IpService     OMPROUTE-IP_V4
{
  Protocol    OSPF
  Type        Any
  Direction   BiDirectional
  Routing     Local
}

IpService     OMPROUTE-IP_V4~10
{
  Protocol    IGMP
  Direction   BiDirectional
  Routing     Local
}

IpService     OMPROUTE-IP_V4~11
{
  Protocol    UDP
  SourcePortRange 520
  DestinationPortRange 1024 65535
  Direction   BiDirectional
  Routing     Local
}

IpService     OMPROUTE-IP_V4~12
{
  Protocol    UDP
  SourcePortRange 1024 65535
  DestinationPortRange 520
  Direction   BiDirectional
  Routing     Local
}

IpService     OMPROUTE-IP_V4~13
{
  Protocol    UDP
  SourcePortRange 520
  DestinationPortRange 520
  Direction   BiDirectional
  Routing     Local
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                Path_MTU_Discovery-IP_V4
{
  Protocol                               ICMP
  Type                                   3
  Code                                   4
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Ping-IP_V4
{
  Protocol                               ICMP
  Type                                   8
  Code                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Ping-IP_V4~14
{
  Protocol                               ICMP
  Type                                   0
  Code                                   Any
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Resolver
{
  Protocol                               TCP
  SourcePortRange                        1024 65535
  DestinationPortRange                  53
  Direction                             BiDirectional OutboundConnect
  Routing                               Local
}

IpService                                Resolver~15
{
  Protocol                               UDP
  SourcePortRange                        1024 65535
  DestinationPortRange                  53
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Trace_Route-IP_V4
{
  Protocol                               ICMP
  Type                                   11
  Code                                   0
  Direction                             BiDirectional
  Routing                               Local
}

IpService                                Trace_Route-IP_V4~16
{
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    Protocol          ICMP
    Type              3
    Code              3
    Direction         BiDirectional
    Routing            Local
}

IpService            Trace_Route-IP_V4~17
{
    Protocol          ICMP
    Type              3
    Code              2
    Direction         BiDirectional
    Routing            Local
}

IpService            Trace_Route-IP_V4~18
{
    Protocol          UDP
    SourcePortRange   1024 65535
    DestinationPortRange 33435 33535
    Direction         BiDirectional
    Routing            Local
}

IpService           NSS_Client
{
    Protocol          TCP
    SourcePortRange   1024 65535
    DestinationPortRange 4159
    Direction         BiDirectional OutboundConnect
    Routing           Local
}

IpService           NSS_Server
{
    Protocol          TCP
    SourcePortRange   4159
    DestinationPortRange 1024 65535
    Direction         BiDirectional InboundConnect
    Routing           Local
}

IpDynVpnAction       VPN~A
{
    Initiation        Either
    VpnLife            1440
    InitiateWithPfs    Group2
    IpDataOfferRef     VPN~A~R
    AcceptablePfs       None
    AcceptablePfs       Group2
    PassthroughDF       Yes
    PassthroughDSCP     Yes
    HowToEncapIKEv2     Either
}

IpDynVpnAction       VPN~A~6

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
{
  Initiation                Either
  VpnLife                   1440
  InitiateWithPfs           Group2
  IpDataOfferRef            VPN~A~N
  AcceptablePfs             None
  AcceptablePfs             Group2
  PassthroughDF             Yes
  PassthroughDSCP           Yes
  HowToEncapIKEv2           Either
}

## Filter rules to permit NSS traffic
IpGenericFilterAction      NssPermit~LogNo
{
  IpFilterAction           Permit
  IpFilterLogging         No
}

IpService                 NssSFor~ZOS7
{
  Protocol                 TCP
  SourcePortRange         4159
  DestinationPortRange    1024 65535
  Direction              BiDirectional InboundConnect
  Routing                 Local
}

IpFilterRule             NssTrafficIPv4
{
  IpSourceAddr           All4
  IpDestAddr             All4
  IpServiceRef           NssSFor~ZOS7
  IpGenericFilterActionRef NssPermit~LogNo
}

IpService                 NssPFor~ZOS7
{
  Protocol                 TCP
  SourcePortRange         1024 65535
  DestinationPortRange    4159
  Direction              BiDirectional
  Routing                 Local
}

IpFilterRule             NssTrafficIPv4~1
{
  IpSourceAddr           All4
  IpDestAddr             All4
  IpServiceRef           NssPFor~ZOS7
  IpGenericFilterActionRef NssPermit~LogNo
}

##
## Connectivity Rule BetweenOSAsRSA combines the following items:
##   Local data endpoint      BetweenOSAsRSA~ADR~1
##   Remote data endpoint     BetweenOSAsRSA~ADR~2
##   Topology                 Host to Host
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
## Requirement Map
##      FTP-Client          => VPN~A
##      FTP-Server          => VPN~A

IpAddress          BetweenOSAsRSA~ADR~1
{
  Addr              192.168.20.97
}

IpAddress          BetweenOSAsRSA~ADR~2
{
  Addr              192.168.20.91
}

LocalSecurityEndpoint  BetweenOSAsRSA~LSE~4
{
  Identity           IpAddr 192.168.20.97
  LocationRef         BetweenOSAsRSA~ADR~1
}

RemoteSecurityEndpoint  BetweenOSAsRSA~RSE~3
{
  Identity           IpAddr 192.168.20.91
  LocationRef         BetweenOSAsRSA~ADR~2
}

KeyExchangeRule       BetweenOSAsRSA~5
{
  LocalSecurityEndpointRef  BetweenOSAsRSA~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA~RSE~3
  KeyExchangeActionRef      BetweenOSAsRSA
}

KeyExchangeAction      BetweenOSAsRSA
{
  HowToRespondIKEv1      Either
  KeyExchangeOfferRef     VPN~A
  AllowNat                No
  ReauthInterval          0
  ConstrainSource          192.168.20.97
  ConstrainDest            192.168.20.91
}

IpLocalStartAction     BetweenOSAsRSA~8
{
  AllowOnDemand           No
  LocalPortGranularity    Rule
  RemotePortGranularity   Rule
  ProtocolGranularity     Rule
  RemoteIpGranularity     Packet
  LocalIpGranularity       Packet
  IcmpCodeGranularity     Rule
  IcmpTypeGranularity     Rule
  IcmpV6CodeGranularity   Rule
  IcmpV6TypeGranularity   Rule
  MipV6TypeGranularity    Rule
  LocalSecurityEndpointRef BetweenOSAsRSA~LSE~4
}
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteSecurityEndpointRef    BetweenOSAsRSA~RSE~3
}

## NOTE -- Generated IpFilterRule BetweenOSAsRSA~6
IpFilterRule                 BetweenOSAsRSA~6
{
    IpSourceAddrRef          BetweenOSAsRSA~ADR~1
    IpDestAddrRef            BetweenOSAsRSA~ADR~2
    IpServiceRef              IKE~Gen
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule                 BetweenOSAsRSA~7
{
    IpSourceAddrRef          BetweenOSAsRSA~ADR~1
    IpDestAddrRef            BetweenOSAsRSA~ADR~2
    IpServiceRef              FTP-Client
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
}

IpFilterRule                 BetweenOSAsRSA~9
{
    IpSourceAddrRef          BetweenOSAsRSA~ADR~1
    IpDestAddrRef            BetweenOSAsRSA~ADR~2
    IpServiceRef              FTP-Client~1
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
    IpLocalStartActionRef    BetweenOSAsRSA~8
}

IpFilterRule                 BetweenOSAsRSA~10
{
    IpSourceAddrRef          BetweenOSAsRSA~ADR~1
    IpDestAddrRef            BetweenOSAsRSA~ADR~2
    IpServiceRef              FTP-Client~2
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
}

IpFilterRule                 BetweenOSAsRSA~12
{
    IpSourceAddrRef          BetweenOSAsRSA~ADR~1
    IpDestAddrRef            BetweenOSAsRSA~ADR~2
    IpServiceRef              FTP-Server
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
    IpLocalStartActionRef    BetweenOSAsRSA~8
}

IpFilterRule                 BetweenOSAsRSA~13
{
    IpSourceAddrRef          BetweenOSAsRSA~ADR~1
    IpDestAddrRef            BetweenOSAsRSA~ADR~2
    IpServiceRef              FTP-Server~3
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}

IpFilterRule                                BetweenOSAsRSA~15
{
    IpSourceAddrRef                          BetweenOSAsRSA~ADR~1
    IpDestAddrRef                            BetweenOSAsRSA~ADR~2
    IpServiceRef                             FTP-Server~4
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
    IpLocalStartActionRef                   BetweenOSAsRSA~8
}
##
## Connectivity Rule TrafficBetweenVIPAs combines the following items:
##   Local data endpoint                    TrafficBetweenVIPAs~ADS~1
##   Remote data endpoint                   TrafficBetweenVIPAs~ADS~2
##   Topology                              Filtering - Host
##   Requirement Map
##     CICS                                => Permit
##     FTP-Client                         => Permit
##     FTP-Server                         => Permit

IpAddrSet                                  TrafficBetweenVIPAs~ADS~1
{
    Range                                    192.168.20.101-192.168.20.107
}

IpAddrSet                                  TrafficBetweenVIPAs~ADS~2
{
    Range                                    192.168.20.101-192.168.20.107
}

IpFilterRule                                TrafficBetweenVIPAs~3
{
    IpSourceAddrSetRef                      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef                       TrafficBetweenVIPAs~ADS~2
    IpServiceRef                           CICS
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                TrafficBetweenVIPAs~4
{
    IpSourceAddrSetRef                      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef                       TrafficBetweenVIPAs~ADS~2
    IpServiceRef                           FTP-Client
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                TrafficBetweenVIPAs~5
{
    IpSourceAddrSetRef                      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef                       TrafficBetweenVIPAs~ADS~2
    IpServiceRef                           FTP-Client~1
    IpGenericFilterActionRef                 Permit__LogYes
}

IpFilterRule                                TrafficBetweenVIPAs~6
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpSourceAddrSetRef      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef        TrafficBetweenVIPAs~ADS~2
    IpServiceRef            FTP-Client~2
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule                TrafficBetweenVIPAs~7
{
    IpSourceAddrSetRef      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef        TrafficBetweenVIPAs~ADS~2
    IpServiceRef            FTP-Server
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule                TrafficBetweenVIPAs~8
{
    IpSourceAddrSetRef      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef        TrafficBetweenVIPAs~ADS~2
    IpServiceRef            FTP-Server~3
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule                TrafficBetweenVIPAs~9
{
    IpSourceAddrSetRef      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef        TrafficBetweenVIPAs~ADS~2
    IpServiceRef            FTP-Server~4
    IpGenericFilterActionRef Permit__LogYes
}
##
## Connectivity Rule TrafOSA2DVIPAPresh combines the following items:
##   Local data endpoint      TrafOSA2DVIPAPresh~ADR~1
##   Remote data endpoint    TrafOSA2DVIPAPresh~ADR~2
##   Topology                 Gateway to Host
##   Requirement Map
##   All_other_traffic        => VPN~A

IpAddr                      TrafOSA2DVIPAPresh~ADR~1
{
    Addr                     192.168.20.127
}

IpAddr                      TrafOSA2DVIPAPresh~ADR~2
{
    Addr                     192.168.20.121
}

LocalSecurityEndpoint        TrafOSA2DVIPAPresh~LSE~4
{
    Identity                 Fqdn WSC.LABS.IBM.COM
    Location                 192.168.20.97
}

RemoteSecurityEndpoint       TrafOSA2DVIPAPresh~RSE~3
{
    Identity                 UserAtFqdn ZOS1@WSC.LABS.IBM.COM
    LocationRef              TrafOSA2DVIPAPresh~ADR~2
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}

KeyExchangeRule                                TrafOSA2DVIPAPresh~5
{
    LocalSecurityEndpointRef                    TrafOSA2DVIPAPresh~LSE~4
    RemoteSecurityEndpointRef                  TrafOSA2DVIPAPresh~RSE~3
    KeyExchangeActionRef                      TrafOSA2DVIPAPresh
    SharedKey                                Ebcdic "userlabs"
}

KeyExchangeAction                              TrafOSA2DVIPAPresh
{
    HowToRespondIKEv1                          Either
    KeyExchangeOfferRef                       VPN~A~5
    AllowNat                                  No
    ReauthInterval                            0
    ConstrainSource                           192.168.20.127
    ConstrainDest                             192.168.20.121
    HowToAuthMe                               PresharedKey
}

IpLocalStartAction                            TrafOSA2DVIPAPresh~7
{
    AllowOnDemand                             Yes
    LocalPortGranularity                      Rule
    RemotePortGranularity                     Rule
    ProtocolGranularity                       Rule
    RemoteIpGranularity                       Packet
    LocalIpGranularity                        Packet
    IcmpCodeGranularity                       Rule
    IcmpTypeGranularity                       Rule
    IcmpV6CodeGranularity                     Rule
    IcmpV6TypeGranularity                     Rule
    MipV6TypeGranularity                      Rule
    LocalSecurityEndpointRef                  TrafOSA2DVIPAPresh~LSE~4
    RemoteSecurityEndpointRef                  TrafOSA2DVIPAPresh~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh~6
IpFilterRule                                  TrafOSA2DVIPAPresh~6
{
    IpSourceAddr                             192.168.20.97
    IpDestAddrRef                            TrafOSA2DVIPAPresh~ADR~2
    IpServiceRef                             IKE~Gen
    IpGenericFilterActionRef                  Permit__LogYes
}

IpFilterRule                                  TrafOSA2DVIPAPresh~8
{
    IpSourceAddrRef                          TrafOSA2DVIPAPresh~ADR~1
    IpDestAddrRef                            TrafOSA2DVIPAPresh~ADR~2
    IpServiceRef                             All_other_traffic
    IpGenericFilterActionRef                  IpSec__LogYes
    IpDynVpnActionRef                        VPN~A~6
    IpLocalStartActionRef                    TrafOSA2DVIPAPresh~7
}
##

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
## Connectivity Rule WStoVIPA combines the following items:
##   Local data endpoint      WStoVIPA~ADS~1
##   Remote data endpoint     All4
##   Topology                  Filtering - Host
##   Requirement Map
##     FTP-Server              => Permit
##     TN3270-Server           => Permit

IpAddrSet                                WStoVIPA~ADS~1
{
  Range                                192.168.20.101-192.168.20.107
}

IpFilterRule                             WStoVIPA~2
{
  IpSourceAddrSetRef                 WStoVIPA~ADS~1
  IpDestAddr                         All4
  IpServiceRef                       FTP-Server
  IpGenericFilterActionRef           Permit__LogYes
}

IpFilterRule                             WStoVIPA~3
{
  IpSourceAddrSetRef                 WStoVIPA~ADS~1
  IpDestAddr                         All4
  IpServiceRef                       FTP-Server~3
  IpGenericFilterActionRef           Permit__LogYes
}

IpFilterRule                             WStoVIPA~4
{
  IpSourceAddrSetRef                 WStoVIPA~ADS~1
  IpDestAddr                         All4
  IpServiceRef                       FTP-Server~4
  IpGenericFilterActionRef           Permit__LogYes
}

IpFilterRule                             WStoVIPA~5
{
  IpSourceAddrSetRef                 WStoVIPA~ADS~1
  IpDestAddr                         All4
  IpServiceRef                       TN3270-Server
  IpGenericFilterActionRef           Permit__LogYes
}
##
## Connectivity Rule CommonTraffic combines the following items:
##   Local data endpoint      All4
##   Remote data endpoint     All4
##   Topology                  Filtering - Host
##   Requirement Map          BasicServices
##     DNS                     => Permit
##     ICMP-Time_Exceeded-IP_V4 => Permit
##     ICMP-Unreachable-IP_V4  => Permit
##     OMPROUTE-IP_V4          => Permit
##     Path_MTU_Discovery-IP_V4 => Permit
##     Ping-IP_V4              => Permit
##     Resolver                 => Permit
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
##      Trace_Route-IP_V4          => Permit
##      NSS_Client                 => Permit
##      NSS_Server                 => Permit

IpFilterRule                          CommonTraffic~1
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     DNS
    IpGenericFilterActionRef         Permit__LogYes
}

IpFilterRule                          CommonTraffic~2
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     DNS~7
    IpGenericFilterActionRef         Permit__LogYes
}

IpFilterRule                          CommonTraffic~3
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     DNS~8
    IpGenericFilterActionRef         Permit__LogYes
}

IpFilterRule                          CommonTraffic~4
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     DNS~9
    IpGenericFilterActionRef         Permit__LogYes
}

IpFilterRule                          CommonTraffic~5
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     ICMP-Time_Exceeded-IP_V4
    IpGenericFilterActionRef         Permit__LogYes
}

IpFilterRule                          CommonTraffic~6
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     ICMP-Unreachable-IP_V4
    IpGenericFilterActionRef         Permit__LogYes
}

IpFilterRule                          CommonTraffic~7
{
    IpSourceAddr                     All4
    IpDestAddr                      All4
    IpServiceRef                     OMPROUTE-IP_V4
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpGenericFilterActionRef    Permit__LogYes
}

IpFilterRule                  CommonTraffic~8
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              OMPROUTE-IP_V4~10
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~9
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              OMPROUTE-IP_V4~11
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~10
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              OMPROUTE-IP_V4~12
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~11
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              OMPROUTE-IP_V4~13
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~12
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              Path_MTU_Discovery-IP_V4
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~13
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              Ping-IP_V4
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                  CommonTraffic~14
{
    IpSourceAddr              All4
    IpDestAddr                All4
    IpServiceRef              Ping-IP_V4~14
    IpGenericFilterActionRef   Permit__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}

IpFilterRule                                CommonTraffic~15
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Resolver
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~16
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Resolver~15
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~17
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Trace_Route-IP_V4
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~18
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Trace_Route-IP_V4~16
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~19
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Trace_Route-IP_V4~17
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~20
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            Trace_Route-IP_V4~18
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~21
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            NSS_Client
    IpGenericFilterActionRef                Permit__LogYes
}

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule
{
    IpSourceAddr           All4
    IpDestAddr            All4
    IpServiceRef          NSS_Server
    IpGenericFilterActionRef Permit__LogYes
}

KeyExchangePolicy
{
    AllowNat                No
    NatKeepAliveInterval    20
    HowToInitiate          IKEv2
    LivenessInterval        30
    BypassIpValidation       Yes
    CertificateURLLookupPreference Tolerate
    RevocationChecking       Loose
    KeyExchangeRuleRef       BetweenOSAsRSA~5
    KeyExchangeRuleRef       TrafOSA2DVIPAPresh~5
}

IpFilterPolicy
{
    PreDecap                OFF
    FilterLogging            ON
    IpFilterLogImplicit      No
    AllowOnDemand            Yes
    ImplicitDiscardAction    Silent
    FIPS140                  No
    IpFilterRuleRef        NssTrafficIPv4
    IpFilterRuleRef        NssTrafficIPv4~1
    IpFilterRuleRef          BetweenOSAsRSA~6
    IpFilterRuleRef          BetweenOSAsRSA~7
    IpFilterRuleRef          BetweenOSAsRSA~9
    IpFilterRuleRef          BetweenOSAsRSA~10
    IpFilterRuleRef          BetweenOSAsRSA~12
    IpFilterRuleRef          BetweenOSAsRSA~13
    IpFilterRuleRef          BetweenOSAsRSA~15
    IpFilterRuleRef          TrafficBetweenVIPAs~3
    IpFilterRuleRef          TrafficBetweenVIPAs~4
    IpFilterRuleRef          TrafficBetweenVIPAs~5
    IpFilterRuleRef          TrafficBetweenVIPAs~6
    IpFilterRuleRef          TrafficBetweenVIPAs~7
    IpFilterRuleRef          TrafficBetweenVIPAs~8
    IpFilterRuleRef          TrafficBetweenVIPAs~9
    IpFilterRuleRef          TrafOSA2DVIPAPresh~6
    IpFilterRuleRef          TrafOSA2DVIPAPresh~8
    IpFilterRuleRef          WStoVIPA~2
    IpFilterRuleRef          WStoVIPA~3
    IpFilterRuleRef          WStoVIPA~4
    IpFilterRuleRef          WStoVIPA~5
    IpFilterRuleRef          CommonTraffic~1
    IpFilterRuleRef          CommonTraffic~2
    IpFilterRuleRef          CommonTraffic~3
    IpFilterRuleRef          CommonTraffic~4
    IpFilterRuleRef          CommonTraffic~5
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRuleRef      CommonTraffic~6
IpFilterRuleRef      CommonTraffic~7
IpFilterRuleRef      CommonTraffic~8
IpFilterRuleRef      CommonTraffic~9
IpFilterRuleRef      CommonTraffic~10
IpFilterRuleRef      CommonTraffic~11
IpFilterRuleRef      CommonTraffic~12
IpFilterRuleRef      CommonTraffic~13
IpFilterRuleRef      CommonTraffic~14
IpFilterRuleRef      CommonTraffic~15
IpFilterRuleRef      CommonTraffic~16
IpFilterRuleRef      CommonTraffic~17
IpFilterRuleRef      CommonTraffic~18
IpFilterRuleRef      CommonTraffic~19
IpFilterRuleRef      CommonTraffic~20
IpFilterRuleRef      CommonTraffic~21
IpFilterRuleRef      CommonTraffic~22
}
*****

**** MVS1 AT-TLS Policy ****
*****

##
## AT-TLS Policy Agent Configuration file for:
##   Image: ZOS1
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS
## Communications Server
## Version 2 Release 3
## Backing Store = TTLab12
## Install History:
##
## TLS default rules: NSS_Server (c)
##                      NSS_Client-IKED (c)
## End TLS default rules
##
## End of Configuration Assistant information
TTLRule      VIPAs2VIPAs~1
{
  LocalAddrSetRef      addr1
  RemoteAddrSetRef      addr1
  LocalPortRangeRef      portR1
  RemotePortRangeRef      portR2
  Userid      USER*
  Direction      Outbound
  Priority      255
  TTLGroupActionRef      gAct1
  TTLEnvironmentActionRef      eAct1~AllSecFTPclients
  TLSConnectionActionRef      cAct1~AllSecFTPclients
}
TTLRule      VIPAs2VIPAs~2
{
  LocalAddrSetRef      addr1
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

RemoteAddrSetRef      addr1
LocalPortRangeRef     portR2
RemotePortRangeRef    portR1
Direction             Inbound
Priority               254
TTLSTGroupActionRef   gAct1
TTLSEnvironmentActionRef eAct2~FTP-Server
TTLSTConnectionActionRef cAct2~FTP-Server
}
TTLSTRule              NSS_Server~3
{
  LocalAddr            ALL
  RemoteAddr           ALL
  LocalPortRangeRef    portR3
  RemotePortRangeRef   portR1
  Direction            Inbound
  Priority              253
  TTLSTGroupActionRef  gAct1
  TTLSEnvironmentActionRef eAct3~NSSD
  TTLSTConnectionActionRef cAct3~NSSD
}
TTLSTRule              NSS_Client-IKED~4
{
  LocalAddr            ALL
  RemoteAddr           ALL
  LocalPortRangeRef    portR1
  RemotePortRangeRef   portR3
  Direction            Outbound
  Priority              252
  TTLSTGroupActionRef  gAct1
  TTLSEnvironmentActionRef eAct4~NSS-Client
  TTLSTConnectionActionRef cAct4~NSS-Client
}
TTLSTGroupAction       gAct1
{
  TTLSEnabled          On
  Trace                2
}
TTLSEnvironmentAction  eAct1~AllSecFTPCLients
{
  HandshakeRole         Client
  EnvironmentUserInstance 0
  TTLSTKeyringParmsRef  keyR1
}
TTLSEnvironmentAction  eAct2~FTP-Server
{
  HandshakeRole         ServerWithClientAuth
  EnvironmentUserInstance 0
  TTLSTKeyringParmsRef  keyR~ZOS1
  TTLSTGskAdvancedParmsRef gskAdv1~ATTLSGoldwClientAuth
}
TTLSEnvironmentAction  eAct3~NSSD
{
  HandshakeRole         Server

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    EnvironmentUserInstance      0
    TTLSKeyringParmsRef         keyR3
}
TTLSEnvironmentAction          eAct4~NSS-Client
{
    HandshakeRole               Client
    EnvironmentUserInstance      0
    TTLSKeyringParmsRef         keyR4
}
TTLSTLSConnectionAction        cAct1~AllSecFTPCLients
{
    HandshakeRole               Client
    TTLS cipherParmsRef         cipher1
    TTLSConnectionAdvancedParmsRef cAdv1~AllSecFTPCLients
    CtraceClearText             Off
    Trace                       2
}
TTLSTLSConnectionAction        cAct2~FTP-Server
{
    HandshakeRole               ServerWithClientAuth
    TTLS cipherParmsRef         cipher1
    TTLSConnectionAdvancedParmsRef cAdv2~FTP-Server
    CtraceClearText             Off
    Trace                       2
}
TTLSTLSConnectionAction        cAct3~NSSD
{
    HandshakeRole               Server
    TTLS cipherParmsRef         cipher2~Default_Ciphers
    TTLSConnectionAdvancedParmsRef cAdv3~NSSD
    CtraceClearText             Off
    Trace                       2
}
TTLSTLSConnectionAction        cAct4~NSS-Client
{
    HandshakeRole               Client
    TTLS cipherParmsRef         cipher2~Default_Ciphers
    TTLSConnectionAdvancedParmsRef cAdv4~NSS-Client
    CtraceClearText             Off
    Trace                       2
}
TTLSTLSConnectionAdvancedParms cAdv1~AllSecFTPCLients
{
    SSLv3                       On
    TLSv1                       On
    TLSv1.1                     On
    ApplicationControlled        On
    SecondaryMap                 On
    TLSv1.2                     Off
}
TTLSTLSConnectionAdvancedParms cAdv2~FTP-Server
{
    SSLv3                       On
    TLSv1                       On

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    TLSv1.1                      On
    ApplicationControlled        On
    SecondaryMap                  On
    TLSv1.2                      On
}
TTLSTLSConnectionAdvancedParms  cAdv3~NSSD
{
    SSLv3                        On
    TLSv1                        On
    TLSv1.1                      On
    ApplicationControlled        On
    SecondaryMap                  Off
    TLSv1.2                      Off
}
TTLSTLSConnectionAdvancedParms  cAdv4~NSS-Client
{
    SSLv3                        On
    TLSv1                        On
    TLSv1.1                      On
    ApplicationControlled        On
    SecondaryMap                  Off
    TLSv1.2                      Off
}
TTLSTLSKeyringParms             keyR1
{
    Keyring                      LabClientRing
}
TTLSTLSKeyringParms             keyR~ZOS1
{
    Keyring                      FTPD/ServerRing1
}
TTLSTLSKeyringParms             keyR3
{
    Keyring                      NSSD/NSSD1Ring
}
TTLSTLSKeyringParms             keyR4
{
    Keyring                      *AUTH*/*
}
TTLSTLSGskAdvancedParms         gskAdv1~ATTLSGoldwClientAuth
{
    TTLSTLSGskHttpCdpParmsRef    gskHttp
}
TTLSTLSCipherParms              cipher1
{
    V3CipherSuites                TLS_RSA_WITH_3DES_EDE_CBC_SHA
    V3CipherSuites                TLS_RSA_WITH_AES_128_CBC_SHA
}
TTLSTLSCipherParms              cipher2~Default_Ciphers
{
    V3CipherSuites                TLS_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites                TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites                TLS_DH_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites                TLS_DHE_DSS_WITH_AES_256_CBC_SHA
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

V3CipherSuites      TLS_DH_DSS_WITH_AES_256_CBC_SHA
V3CipherSuites      TLS_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_DH_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_DH_DSS_WITH_AES_128_CBC_SHA
}
TTLSSGskHttpCdpParms gskHttp
{
    HTTPCDPENABLE      OFF
}
IpAddrSet            addr1
{
    Range              192.168.20.101-192.168.20.107
}
PortRange            portR1
{
    Port              1024-65535
}
PortRange            portR2
{
    Port              21
}
PortRange            portR3
{
    Port              4159
}

##
## CA generated policy statements for TLSRule(s) in support of NSS
function.
##

TTLSSGroupAction     NSS~TLS~ON
{
    TLSSEnabled       On
}
TTLSCipherParms      NSS~CIPHER~PARMS
{
    V3CipherSuites    TLS_RSA_WITH_3DES_EDE_CBC_SHA
}
TTLSEnvironmentAction NSS~TLS~CLIENT~ENV
{
    HandShakeRole      Client
    TLSCipherParmsRef  NSS~CIPHER~PARMS
    TLSKeyRingParms    {
        Keyring        *AUTH*/*
    }
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
}
## Rule from client to server ZOS1
TTLSSRule                                NSS~TLS~CLIENT~1
{
    RemotePortRange                      4159
    Direction                            Outbound
    TLSGroupActionRef                     NSS~TLS~ON
    TLSEnvironmentActionRef               NSS~TLS~CLIENT~ENV
}
TLSEnvironmentAction                     NSS~TLS~SERVER~ENV
{
    HandShakeRole                         Server
    TLSCipherParmsRef                     NSS~CIPHER~PARMS
    TLSKeyRingParms
    {
        Keyring                           NSSD/NSSD1Ring
    }
}
TTLSSRule                                NSS~TLS~SERVER
{
    LocalPortRange                        4159
    Direction                            Inbound
    TLSGroupActionRef                     NSS~TLS~ON
    TLSEnvironmentActionRef               NSS~TLS~SERVER~ENV
}
*****
```

**** **MVS1 IPsec Policy** ****

```
##
## IPsec Policy Agent Configuration file for:
##   Image: ZOS1
##   Stack: TCPIPT
##
## Created by the IBM Configuration Assistant for z/OS
Communications Server
## Version 2 Release 3
## Backing Store = TTLab15
## Install History:
##
## End of Configuration Assistant information

## NOTE -- Generated IpGenericFilterAction Permit__LogYes
IpGenericFilterAction                     Permit__LogYes
{
    IpFilterAction                       Permit
    IpFilterLogging                       Yes
    DiscardAction                         Silent
}

IpGenericFilterAction                     IpSec__LogYes
{
    IpFilterAction                       IpSec
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpFilterLogging      Yes
    DiscardAction        Silent
}

KeyExchangeOffer        VPN~A
{
    HowToEncrypt          AES_CBC KeyLength 128
    HowToAuthMsgs          SHA1
    HowToVerifyMsgs        HMAC_SHA1_96
    PseudoRandomFunction    HMAC_SHA1
    HowToAuthPeers          RsaSignature
    DHGroup                Group2
    RefreshLifetimeProposed 1440
    RefreshLifetimeAccepted 1440 1440
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}

KeyExchangeOffer        VPN~A~5
{
    HowToEncrypt          AES_CBC KeyLength 128
    HowToAuthMsgs          SHA1
    HowToVerifyMsgs        HMAC_SHA1_96
    PseudoRandomFunction    HMAC_SHA1
    HowToAuthPeers          PresharedKey
    DHGroup                Group2
    RefreshLifetimeProposed 1440
    RefreshLifetimeAccepted 1440 1440
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}

IpDataOffer             VPN~A~R
{
    HowToEncap            Transport
    HowToEncrypt          3DES
    HowToAuth              ESP Hmac_Sha1
    RefreshLifetimeProposed 480
    RefreshLifetimeAccepted 480 480
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}

IpDataOffer             VPN~A~N
{
    HowToEncap            Tunnel
    HowToEncrypt          3DES
    HowToAuth              ESP Hmac_Sha1
    RefreshLifetimeProposed 480
    RefreshLifetimeAccepted 480 480
    RefreshLifesizeProposed None
    RefreshLifesizeAccepted None
}

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
## NOTE -- Generated IpService IKE~Gen
IpService IKE~Gen
{
    Protocol UDP
    SourcePortRange 500
    DestinationPortRange 500
    Direction BiDirectional
    Routing Local
}

IpService FTP-Client
{
    Protocol TCP
    SourcePortRange 1024 65535
    DestinationPortRange 21
    Direction BiDirectional OutboundConnect
    Routing Local
}

IpService FTP-Client~1
{
    Protocol TCP
    SourcePortRange 1024 65535
    DestinationPortRange 20
    Direction BiDirectional InboundConnect
    Routing Local
}

IpService FTP-Client~2
{
    Protocol TCP
    SourcePortRange 1024 65535
    DestinationPortRange 50000 50200
    Direction BiDirectional OutboundConnect
    Routing Local
}

IpService FTP-Server
{
    Protocol TCP
    SourcePortRange 21
    DestinationPortRange 1024 65535
    Direction BiDirectional InboundConnect
    Routing Local
}

IpService FTP-Server~3
{
    Protocol TCP
    SourcePortRange 20
    DestinationPortRange 1024 65535
    Direction BiDirectional OutboundConnect
    Routing Local
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService      FTP-Server~4
{
  Protocol      TCP
  SourcePortRange 50000 50200
  DestinationPortRange 1024 65535
  Direction     BiDirectional InboundConnect
  Routing       Local
}
```

```
IpService      CICS
{
  Protocol      TCP
  SourcePortRange 3000
  DestinationPortRange 1024 65535
  Direction     BiDirectional InboundConnect
  Routing       Local
}
```

```
IpService      All_other_traffic
{
  Protocol      All
  Direction     BiDirectional
  Routing       Local
}
```

```
IpService      DNS
{
  Protocol      UDP
  SourcePortRange 53
  DestinationPortRange 1024 65535
  Direction     BiDirectional
  Routing       Local
}
```

```
IpService      DNS~7
{
  Protocol      UDP
  SourcePortRange 53
  DestinationPortRange 53
  Direction     BiDirectional
  Routing       Local
}
```

```
IpService      DNS~8
{
  Protocol      TCP
  SourcePortRange 53
  DestinationPortRange 1024 65535
  Direction     BiDirectional
  Routing       Local
}
```

```
IpService      DNS~9
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
{
  Protocol          TCP
  SourcePortRange   53
  DestinationPortRange 53
  Direction         BiDirectional
  Routing           Local
}

IpService           ICMP-Time_Exceeded-IP_V4
{
  Protocol          ICMP
  Type              11
  Code              Any
  Direction         BiDirectional
  Routing           Local
}

IpService           ICMP-Unreachable-IP_V4
{
  Protocol          ICMP
  Type              3
  Code              Any
  Direction         BiDirectional
  Routing           Local
}

IpService           OMPROUTE-IP_V4
{
  Protocol          OSPF
  Type              Any
  Direction         BiDirectional
  Routing           Local
}

IpService           OMPROUTE-IP_V4~10
{
  Protocol          IGMP
  Direction         BiDirectional
  Routing           Local
}

IpService           OMPROUTE-IP_V4~11
{
  Protocol          UDP
  SourcePortRange   520
  DestinationPortRange 1024 65535
  Direction         BiDirectional
  Routing           Local
}

IpService           OMPROUTE-IP_V4~12
{
  Protocol          UDP
  SourcePortRange   1024 65535
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    DestinationPortRange    520
    Direction               BiDirectional
    Routing                 Local
}

IpService                  OMPROUTE-IP_V4~13
{
    Protocol                UDP
    SourcePortRange         520
    DestinationPortRange    520
    Direction               BiDirectional
    Routing                 Local
}

IpService                  Path_MTU_Discovery-IP_V4
{
    Protocol                ICMP
    Type                    3
    Code                    4
    Direction               BiDirectional
    Routing                 Local
}

IpService                  Ping-IP_V4
{
    Protocol                ICMP
    Type                    8
    Code                    Any
    Direction               BiDirectional
    Routing                 Local
}

IpService                  Ping-IP_V4~14
{
    Protocol                ICMP
    Type                    0
    Code                    Any
    Direction               BiDirectional
    Routing                 Local
}

IpService                  Resolver
{
    Protocol                TCP
    SourcePortRange         1024 65535
    DestinationPortRange    53
    Direction               BiDirectional OutboundConnect
    Routing                 Local
}

IpService                  Resolver~15
{
    Protocol                UDP
    SourcePortRange         1024 65535
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    DestinationPortRange    53
    Direction               BiDirectional
    Routing                 Local
}

IpService                  Trace_Route-IP_V4
{
    Protocol               ICMP
    Type                   11
    Code                   0
    Direction              BiDirectional
    Routing                Local
}

IpService                  Trace_Route-IP_V4~16
{
    Protocol               ICMP
    Type                   3
    Code                   3
    Direction              BiDirectional
    Routing                Local
}

IpService                  Trace_Route-IP_V4~17
{
    Protocol               ICMP
    Type                   3
    Code                   2
    Direction              BiDirectional
    Routing                Local
}

IpService                  Trace_Route-IP_V4~18
{
    Protocol               UDP
    SourcePortRange        1024 65535
    DestinationPortRange   33435 33535
    Direction              BiDirectional
    Routing                Local
}

IpService                  NSS_Client
{
    Protocol               TCP
    SourcePortRange        1024 65535
    DestinationPortRange   4159
    Direction              BiDirectional OutboundConnect
    Routing                Local
}

IpService                  NSS_Server
{
    Protocol               TCP
    SourcePortRange        4159
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    DestinationPortRange      1024 65535
    Direction                  BiDirectional InboundConnect
    Routing                    Local
}

IpDynVpnAction                VPN~A
{
    Initiation                 Either
    VpnLife                    1440
    InitiateWithPfs            Group2
    IpDataOfferRef             VPN~A~R
    AcceptablePfs              None
    AcceptablePfs              Group2
    PassthroughDF              Yes
    PassthroughDSCP            Yes
    HowToEncapIkev2            Either
}

IpDynVpnAction                VPN~A~6
{
    Initiation                 Either
    VpnLife                    1440
    InitiateWithPfs            Group2
    IpDataOfferRef             VPN~A~N
    AcceptablePfs              None
    AcceptablePfs              Group2
    PassthroughDF              Yes
    PassthroughDSCP            Yes
    HowToEncapIkev2            Either
}

## Filter rules to permit NSS traffic
IpGenericFilterAction          NssPermit~LogNo
{
    IpFilterAction              Permit
    IpFilterLogging              No
}

IpService                      NssSFor~ZOS1
{
    Protocol                    TCP
    SourcePortRange              4159
    DestinationPortRange         1024 65535
    Direction                    BiDirectional InboundConnect
    Routing                      Local
}

IpFilterRule                   NssTrafficIPv4
{
    IpSourceAddr                 All4
    IpDestAddr                   All4
    IpServiceRef                 NssSFor~ZOS1
    IpGenericFilterActionRef      NssPermit~LogNo
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpService                                NssPFor~ZOS1
{
  Protocol                               TCP
  SourcePortRange                        1024 65535
  DestinationPortRange                  4159
  Direction                             BiDirectional
  Routing                               Local
}

IpFilterRule                             NssTrafficIPv4~1
{
  IpSourceAddr                           All4
  IpDestAddr                             All4
  IpServiceRef                           NssPFor~ZOS1
  IpGenericFilterActionRef               NssPermit~LogNo
}
##
## Connectivity Rule BetweenOSAsRSA2 combines the following items:
##   Local data endpoint                 BetweenOSAsRSA2~ADR~1
##   Remote data endpoint                 BetweenOSAsRSA2~ADR~2
##   Topology                             Host to Host
##   Requirement Map
##     FTP-Client                         => VPN~A
##     FTP-Server                         => VPN~A

IpAddr                                   BetweenOSAsRSA2~ADR~1
{
  Addr                                   192.168.20.91
}

IpAddr                                   BetweenOSAsRSA2~ADR~2
{
  Addr                                   192.168.20.92
}

LocalSecurityEndpoint                    BetweenOSAsRSA2~LSE~4
{
  Identity                               IpAddr 192.168.20.91
  LocationRef                             BetweenOSAsRSA2~ADR~1
}

RemoteSecurityEndpoint                    BetweenOSAsRSA2~RSE~3
{
  Identity                               IpAddr 192.168.20.92
  LocationRef                             BetweenOSAsRSA2~ADR~2
}

KeyExchangeRule                          BetweenOSAsRSA2~5
{
  LocalSecurityEndpointRef                BetweenOSAsRSA2~LSE~4
  RemoteSecurityEndpointRef                BetweenOSAsRSA2~RSE~3
  KeyExchangeActionRef                    BetweenOSAsRSA2
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

KeyExchangeAction          BetweenOSAsRSA2
{
    HowToRespondIKEv1      Either
    KeyExchangeOfferRef    VPN~A
    AllowNat                No
    ReauthInterval         0
    ConstrainSource        192.168.20.91
    ConstrainDest          192.168.20.92
}

IpLocalStartAction         BetweenOSAsRSA2~8
{
    AllowOnDemand          No
    LocalPortGranularity   Rule
    RemotePortGranularity  Rule
    ProtocolGranularity    Rule
    RemoteIpGranularity    Packet
    LocalIpGranularity     Packet
    IcmpCodeGranularity    Rule
    IcmpTypeGranularity    Rule
    IcmpV6CodeGranularity  Rule
    IcmpV6TypeGranularity  Rule
    MipV6TypeGranularity   Rule
    LocalSecurityEndpointRef BetweenOSAsRSA2~LSE~4
    RemoteSecurityEndpointRef BetweenOSAsRSA2~RSE~3
}

## NOTE -- Generated IpFilterRule BetweenOSAsRSA2~6
IpFilterRule               BetweenOSAsRSA2~6
{
    IpSourceAddrRef        BetweenOSAsRSA2~ADR~1
    IpDestAddrRef          BetweenOSAsRSA2~ADR~2
    IpServiceRef           IKE~Gen
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule               BetweenOSAsRSA2~7
{
    IpSourceAddrRef        BetweenOSAsRSA2~ADR~1
    IpDestAddrRef          BetweenOSAsRSA2~ADR~2
    IpServiceRef           FTP-Client
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef      VPN~A
}

IpFilterRule               BetweenOSAsRSA2~9
{
    IpSourceAddrRef        BetweenOSAsRSA2~ADR~1
    IpDestAddrRef          BetweenOSAsRSA2~ADR~2
    IpServiceRef           FTP-Client~1
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef      VPN~A
    IpLocalStartActionRef  BetweenOSAsRSA2~8
}

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
}

IpFilterRule                               BetweenOSAsRSA2~10
{
    IpSourceAddrRef                         BetweenOSAsRSA2~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA2~ADR~2
    IpServiceRef                             FTP-Client~2
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
}

IpFilterRule                               BetweenOSAsRSA2~12
{
    IpSourceAddrRef                         BetweenOSAsRSA2~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA2~ADR~2
    IpServiceRef                             FTP-Server
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
    IpLocalStartActionRef                   BetweenOSAsRSA2~8
}

IpFilterRule                               BetweenOSAsRSA2~13
{
    IpSourceAddrRef                         BetweenOSAsRSA2~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA2~ADR~2
    IpServiceRef                             FTP-Server~3
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
}

IpFilterRule                               BetweenOSAsRSA2~15
{
    IpSourceAddrRef                         BetweenOSAsRSA2~ADR~1
    IpDestAddrRef                           BetweenOSAsRSA2~ADR~2
    IpServiceRef                             FTP-Server~4
    IpGenericFilterActionRef                 IpSec__LogYes
    IpDynVpnActionRef                       VPN~A
    IpLocalStartActionRef                   BetweenOSAsRSA2~8
}
##
## Connectivity Rule BetweenOSAsRSA3 combines the following items:
##   Local data endpoint                     BetweenOSAsRSA3~ADR~1
##   Remote data endpoint                   BetweenOSAsRSA3~ADR~2
##   Topology                               Host to Host
##   Requirement Map
##     FTP-Client                           => VPN~A
##     FTP-Server                           => VPN~A

IpAddr                                      BetweenOSAsRSA3~ADR~1
{
    Addr                                    192.168.20.91
}

IpAddr                                      BetweenOSAsRSA3~ADR~2
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

{
  Addr                      192.168.20.93
}

LocalSecurityEndpoint      BetweenOSAsRSA3~LSE~4
{
  Identity                  IpAddr 192.168.20.91
  LocationRef               BetweenOSAsRSA3~ADR~1
}

RemoteSecurityEndpoint     BetweenOSAsRSA3~RSE~3
{
  Identity                  IpAddr 192.168.20.93
  LocationRef               BetweenOSAsRSA3~ADR~2
}

KeyExchangeRule            BetweenOSAsRSA3~5
{
  LocalSecurityEndpointRef  BetweenOSAsRSA3~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA3~RSE~3
  KeyExchangeActionRef      BetweenOSAsRSA3
}

KeyExchangeAction          BetweenOSAsRSA3
{
  HowToRespondIKEv1        Either
  KeyExchangeOfferRef       VPN~A
  AllowNat                  No
  ReauthInterval            0
  ConstrainSource           192.168.20.91
  ConstrainDest             192.168.20.93
}

IpLocalStartAction         BetweenOSAsRSA3~8
{
  AllowOnDemand             No
  LocalPortGranularity      Rule
  RemotePortGranularity     Rule
  ProtocolGranularity       Rule
  RemoteIpGranularity       Packet
  LocalIpGranularity        Packet
  IcmpCodeGranularity       Rule
  IcmpTypeGranularity       Rule
  IcmpV6CodeGranularity     Rule
  IcmpV6TypeGranularity     Rule
  MipV6TypeGranularity      Rule
  LocalSecurityEndpointRef  BetweenOSAsRSA3~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA3~RSE~3
}

## NOTE -- Generated IpFilterRule BetweenOSAsRSA3~6
IpFilterRule               BetweenOSAsRSA3~6
{
  IpSourceAddrRef           BetweenOSAsRSA3~ADR~1
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpDestAddrRef      BetweenOSAsRSA3~ADR~2
    IpServiceRef        IKE~Gen
    IpGenericFilterActionRef Permit__LogYes
}

```

```

IpFilterRule          BetweenOSAsRSA3~7
{
    IpSourceAddrRef    BetweenOSAsRSA3~ADR~1
    IpDestAddrRef      BetweenOSAsRSA3~ADR~2
    IpServiceRef        FTP-Client
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef   VPN~A
}

```

```

IpFilterRule          BetweenOSAsRSA3~9
{
    IpSourceAddrRef    BetweenOSAsRSA3~ADR~1
    IpDestAddrRef      BetweenOSAsRSA3~ADR~2
    IpServiceRef        FTP-Client~1
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef   VPN~A
    IpLocalStartActionRef BetweenOSAsRSA3~8
}

```

```

IpFilterRule          BetweenOSAsRSA3~10
{
    IpSourceAddrRef    BetweenOSAsRSA3~ADR~1
    IpDestAddrRef      BetweenOSAsRSA3~ADR~2
    IpServiceRef        FTP-Client~2
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef   VPN~A
}

```

```

IpFilterRule          BetweenOSAsRSA3~12
{
    IpSourceAddrRef    BetweenOSAsRSA3~ADR~1
    IpDestAddrRef      BetweenOSAsRSA3~ADR~2
    IpServiceRef        FTP-Server
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef   VPN~A
    IpLocalStartActionRef BetweenOSAsRSA3~8
}

```

```

IpFilterRule          BetweenOSAsRSA3~13
{
    IpSourceAddrRef    BetweenOSAsRSA3~ADR~1
    IpDestAddrRef      BetweenOSAsRSA3~ADR~2
    IpServiceRef        FTP-Server~3
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef   VPN~A
}

```

```

IpFilterRule          BetweenOSAsRSA3~15
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpSourceAddrRef      BetweenOSAsRSA3~ADR~1
IpDestAddrRef        BetweenOSAsRSA3~ADR~2
IpServiceRef         FTP-Server~4
IpGenericFilterActionRef  IpSec__LogYes
IpDynVpnActionRef    VPN~A
IpLocalStartActionRef BetweenOSAsRSA3~8
}
##
## Connectivity Rule BetweenOSAsRSA4 combines the following items:
##   Local data endpoint      BetweenOSAsRSA4~ADR~1
##   Remote data endpoint    BetweenOSAsRSA4~ADR~2
##   Topology                 Host to Host
##   Requirement Map
##     FTP-Client             => VPN~A
##     FTP-Server             => VPN~A

IpAddr               BetweenOSAsRSA4~ADR~1
{
  Addr               192.168.20.91
}

IpAddr               BetweenOSAsRSA4~ADR~2
{
  Addr               192.168.20.94
}

LocalSecurityEndpoint BetweenOSAsRSA4~LSE~4
{
  Identity           IpAddr 192.168.20.91
  LocationRef        BetweenOSAsRSA4~ADR~1
}

RemoteSecurityEndpoint BetweenOSAsRSA4~RSE~3
{
  Identity           IpAddr 192.168.20.94
  LocationRef        BetweenOSAsRSA4~ADR~2
}

KeyExchangeRule      BetweenOSAsRSA4~5
{
  LocalSecurityEndpointRef  BetweenOSAsRSA4~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA4~RSE~3
  KeyExchangeActionRef     BetweenOSAsRSA4
}

KeyExchangeAction     BetweenOSAsRSA4
{
  HowToRespondIKEv1     Either
  KeyExchangeOfferRef   VPN~A
  AllowNat              No
  ReauthInterval        0
  ConstrainSource       192.168.20.91
  ConstrainDest         192.168.20.94
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpLocalStartAction          BetweenOSAsRSA4~8
{
    AllowOnDemand            No
    LocalPortGranularity     Rule
    RemotePortGranularity    Rule
    ProtocolGranularity      Rule
    RemoteIpGranularity      Packet
    LocalIpGranularity       Packet
    IcmpCodeGranularity      Rule
    IcmpTypeGranularity      Rule
    IcmpV6CodeGranularity    Rule
    IcmpV6TypeGranularity    Rule
    MipV6TypeGranularity     Rule
    LocalSecurityEndpointRef BetweenOSAsRSA4~LSE~4
    RemoteSecurityEndpointRef BetweenOSAsRSA4~RSE~3
}

```

NOTE -- Generated IpFilterRule BetweenOSAsRSA4~6

```

IpFilterRule                BetweenOSAsRSA4~6
{
    IpSourceAddrRef          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef            BetweenOSAsRSA4~ADR~2
    IpServiceRef              IKE~Gen
    IpGenericFilterActionRef  Permit__LogYes
}

```

```

IpFilterRule                BetweenOSAsRSA4~7
{
    IpSourceAddrRef          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef            BetweenOSAsRSA4~ADR~2
    IpServiceRef              FTP-Client
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
}

```

```

IpFilterRule                BetweenOSAsRSA4~9
{
    IpSourceAddrRef          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef            BetweenOSAsRSA4~ADR~2
    IpServiceRef              FTP-Client~1
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
    IpLocalStartActionRef    BetweenOSAsRSA4~8
}

```

```

IpFilterRule                BetweenOSAsRSA4~10
{
    IpSourceAddrRef          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef            BetweenOSAsRSA4~ADR~2
    IpServiceRef              FTP-Client~2
    IpGenericFilterActionRef  IpSec__LogYes
    IpDynVpnActionRef        VPN~A
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                BetweenOSAsRSA4~12
{
    IpSourceAddrRef                          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef                            BetweenOSAsRSA4~ADR~2
    IpServiceRef                             FTP-Server
    IpGenericFilterActionRef                  IpSec__LogYes
    IpDynVpnActionRef                         VPN~A
    IpLocalStartActionRef                     BetweenOSAsRSA4~8
}

IpFilterRule                                BetweenOSAsRSA4~13
{
    IpSourceAddrRef                          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef                            BetweenOSAsRSA4~ADR~2
    IpServiceRef                             FTP-Server~3
    IpGenericFilterActionRef                  IpSec__LogYes
    IpDynVpnActionRef                         VPN~A
}

IpFilterRule                                BetweenOSAsRSA4~15
{
    IpSourceAddrRef                          BetweenOSAsRSA4~ADR~1
    IpDestAddrRef                            BetweenOSAsRSA4~ADR~2
    IpServiceRef                             FTP-Server~4
    IpGenericFilterActionRef                  IpSec__LogYes
    IpDynVpnActionRef                         VPN~A
    IpLocalStartActionRef                     BetweenOSAsRSA4~8
}
##
## Connectivity Rule BetweenOSAsRSA5 combines the following items:
##   Local data endpoint                      BetweenOSAsRSA5~ADR~1
##   Remote data endpoint                     BetweenOSAsRSA5~ADR~2
##   Topology                                Host to Host
##   Requirement Map
##     FTP-Client                            => VPN~A
##     FTP-Server                            => VPN~A

IpAddr                                       BetweenOSAsRSA5~ADR~1
{
    Addr                                     192.168.20.91
}

IpAddr                                       BetweenOSAsRSA5~ADR~2
{
    Addr                                     192.168.20.95
}

LocalSecurityEndpoint                       BetweenOSAsRSA5~LSE~4
{
    Identity                                IpAddr 192.168.20.91
    LocationRef                             BetweenOSAsRSA5~ADR~1
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteSecurityEndpoint      BetweenOSAsRSA5~RSE~3
{
  Identity                  IpAddr 192.168.20.95
  LocationRef               BetweenOSAsRSA5~ADR~2
}
```

```
KeyExchangeRule            BetweenOSAsRSA5~5
{
  LocalSecurityEndpointRef  BetweenOSAsRSA5~LSE~4
  RemoteSecurityEndpointRef BetweenOSAsRSA5~RSE~3
  KeyExchangeActionRef      BetweenOSAsRSA5
}
```

```
KeyExchangeAction          BetweenOSAsRSA5
{
  HowToRespondIKEv1        Either
  KeyExchangeOfferRef       VPN~A
  AllowNat                  No
  ReauthInterval            0
  ConstrainSource            192.168.20.91
  ConstrainDest              192.168.20.95
}
```

```
IpLocalStartAction          BetweenOSAsRSA5~8
{
  AllowOnDemand              No
  LocalPortGranularity        Rule
  RemotePortGranularity       Rule
  ProtocolGranularity         Rule
  RemoteIpGranularity         Packet
  LocalIpGranularity          Packet
  IcmpCodeGranularity         Rule
  IcmpTypeGranularity         Rule
  IcmpV6CodeGranularity       Rule
  IcmpV6TypeGranularity       Rule
  MipV6TypeGranularity        Rule
  LocalSecurityEndpointRef    BetweenOSAsRSA5~LSE~4
  RemoteSecurityEndpointRef   BetweenOSAsRSA5~RSE~3
}
```

NOTE -- Generated IpFilterRule BetweenOSAsRSA5~6

```
IpFilterRule                BetweenOSAsRSA5~6
{
  IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
  IpDestAddrRef              BetweenOSAsRSA5~ADR~2
  IpServiceRef                IKE~Gen
  IpGenericFilterActionRef    Permit__LogYes
}
```

```
IpFilterRule                BetweenOSAsRSA5~7
{
  IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
  IpDestAddrRef              BetweenOSAsRSA5~ADR~2
  IpServiceRef                FTP-Client
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
}

IpFilterRule                  BetweenOSAsRSA5~9
{
    IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
    IpDestAddrRef              BetweenOSAsRSA5~ADR~2
    IpServiceRef                FTP-Client~1
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
    IpLocalStartActionRef      BetweenOSAsRSA5~8
}

IpFilterRule                  BetweenOSAsRSA5~10
{
    IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
    IpDestAddrRef              BetweenOSAsRSA5~ADR~2
    IpServiceRef                FTP-Client~2
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
}

IpFilterRule                  BetweenOSAsRSA5~12
{
    IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
    IpDestAddrRef              BetweenOSAsRSA5~ADR~2
    IpServiceRef                FTP-Server
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
    IpLocalStartActionRef      BetweenOSAsRSA5~8
}

IpFilterRule                  BetweenOSAsRSA5~13
{
    IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
    IpDestAddrRef              BetweenOSAsRSA5~ADR~2
    IpServiceRef                FTP-Server~3
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
}

IpFilterRule                  BetweenOSAsRSA5~15
{
    IpSourceAddrRef            BetweenOSAsRSA5~ADR~1
    IpDestAddrRef              BetweenOSAsRSA5~ADR~2
    IpServiceRef                FTP-Server~4
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
    IpLocalStartActionRef      BetweenOSAsRSA5~8
}
##
## Connectivity Rule BetweenOSAsRSA6 combines the following items:
##   Local data endpoint          BetweenOSAsRSA6~ADR~1

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
## Remote data endpoint      BetweenOSAsRSA6~ADR~2
## Topology                  Host to Host
## Requirement Map
##   FTP-Client              => VPN~A
##   FTP-Server              => VPN~A

IpAddr                       BetweenOSAsRSA6~ADR~1
{
  Addr                       192.168.20.91
}

IpAddr                       BetweenOSAsRSA6~ADR~2
{
  Addr                       192.168.20.96
}

LocalSecurityEndpoint        BetweenOSAsRSA6~LSE~4
{
  Identity                   IpAddr 192.168.20.91
  LocationRef                BetweenOSAsRSA6~ADR~1
}

RemoteSecurityEndpoint       BetweenOSAsRSA6~RSE~3
{
  Identity                   IpAddr 192.168.20.96
  LocationRef                BetweenOSAsRSA6~ADR~2
}

KeyExchangeRule              BetweenOSAsRSA6~5
{
  LocalSecurityEndpointRef   BetweenOSAsRSA6~LSE~4
  RemoteSecurityEndpointRef  BetweenOSAsRSA6~RSE~3
  KeyExchangeActionRef       BetweenOSAsRSA6
}

KeyExchangeAction            BetweenOSAsRSA6
{
  HowToRespondIKEv1          Either
  KeyExchangeOfferRef         VPN~A
  AllowNat                    No
  ReauthInterval              0
  ConstrainSource              192.168.20.91
  ConstrainDest                192.168.20.96
}

IpLocalStartAction           BetweenOSAsRSA6~8
{
  AllowOnDemand               No
  LocalPortGranularity        Rule
  RemotePortGranularity       Rule
  ProtocolGranularity         Rule
  RemoteIpGranularity         Packet
  LocalIpGranularity           Packet
  IcmpCodeGranularity         Rule
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IcmpTypeGranularity      Rule
IcmpV6CodeGranularity    Rule
IcmpV6TypeGranularity    Rule
MipV6TypeGranularity     Rule
LocalSecurityEndpointRef  BetweenOSAsRSA6~LSE~4
RemoteSecurityEndpointRef BetweenOSAsRSA6~RSE~3
}
```

NOTE -- Generated IpFilterRule BetweenOSAsRSA6~6

```
IpFilterRule              BetweenOSAsRSA6~6
{
  IpSourceAddrRef          BetweenOSAsRSA6~ADR~1
  IpDestAddrRef            BetweenOSAsRSA6~ADR~2
  IpServiceRef             IKE~Gen
  IpGenericFilterActionRef Permit__LogYes
}
```

```
IpFilterRule              BetweenOSAsRSA6~7
{
  IpSourceAddrRef          BetweenOSAsRSA6~ADR~1
  IpDestAddrRef            BetweenOSAsRSA6~ADR~2
  IpServiceRef             FTP-Client
  IpGenericFilterActionRef IpSec__LogYes
  IpDynVpnActionRef        VPN~A
}
```

```
IpFilterRule              BetweenOSAsRSA6~9
{
  IpSourceAddrRef          BetweenOSAsRSA6~ADR~1
  IpDestAddrRef            BetweenOSAsRSA6~ADR~2
  IpServiceRef             FTP-Client~1
  IpGenericFilterActionRef IpSec__LogYes
  IpDynVpnActionRef        VPN~A
  IpLocalStartActionRef    BetweenOSAsRSA6~8
}
```

```
IpFilterRule              BetweenOSAsRSA6~10
{
  IpSourceAddrRef          BetweenOSAsRSA6~ADR~1
  IpDestAddrRef            BetweenOSAsRSA6~ADR~2
  IpServiceRef             FTP-Client~2
  IpGenericFilterActionRef IpSec__LogYes
  IpDynVpnActionRef        VPN~A
}
```

```
IpFilterRule              BetweenOSAsRSA6~12
{
  IpSourceAddrRef          BetweenOSAsRSA6~ADR~1
  IpDestAddrRef            BetweenOSAsRSA6~ADR~2
  IpServiceRef             FTP-Server
  IpGenericFilterActionRef IpSec__LogYes
  IpDynVpnActionRef        VPN~A
  IpLocalStartActionRef    BetweenOSAsRSA6~8
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                BetweenOSAsRSA6~13
{
    IpSourceAddrRef                        BetweenOSAsRSA6~ADR~1
    IpDestAddrRef                         BetweenOSAsRSA6~ADR~2
    IpServiceRef                          FTP-Server~3
    IpGenericFilterActionRef              IpSec__LogYes
    IpDynVpnActionRef                     VPN~A
}

IpFilterRule                                BetweenOSAsRSA6~15
{
    IpSourceAddrRef                        BetweenOSAsRSA6~ADR~1
    IpDestAddrRef                         BetweenOSAsRSA6~ADR~2
    IpServiceRef                          FTP-Server~4
    IpGenericFilterActionRef              IpSec__LogYes
    IpDynVpnActionRef                     VPN~A
    IpLocalStartActionRef                 BetweenOSAsRSA6~8
}
##
## Connectivity Rule BetweenOSAsRSA7 combines the following items:
##   Local data endpoint                   BetweenOSAsRSA7~ADR~1
##   Remote data endpoint                  BetweenOSAsRSA7~ADR~2
##   Topology                             Host to Host
##   Requirement Map
##     FTP-Client                         => VPN~A
##     FTP-Server                         => VPN~A

IpAddr                                       BetweenOSAsRSA7~ADR~1
{
    Addr                                   192.168.20.91
}

IpAddr                                       BetweenOSAsRSA7~ADR~2
{
    Addr                                   192.168.20.97
}

LocalSecurityEndpoint                       BetweenOSAsRSA7~LSE~4
{
    Identity                              IpAddr 192.168.20.91
    LocationRef                           BetweenOSAsRSA7~ADR~1
}

RemoteSecurityEndpoint                      BetweenOSAsRSA7~RSE~3
{
    Identity                              IpAddr 192.168.20.97
    LocationRef                           BetweenOSAsRSA7~ADR~2
}

KeyExchangeRule                            BetweenOSAsRSA7~5
{
    LocalSecurityEndpointRef              BetweenOSAsRSA7~LSE~4
    RemoteSecurityEndpointRef             BetweenOSAsRSA7~RSE~3
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    KeyExchangeActionRef      BetweenOSAsRSA7
}

KeyExchangeAction            BetweenOSAsRSA7
{
    HowToRespondIKEv1        Either
    KeyExchangeOfferRef      VPN~A
    AllowNat                  No
    ReauthInterval            0
    ConstrainSource           192.168.20.91
    ConstrainDest             192.168.20.97
}

IpLocalStartAction           BetweenOSAsRSA7~8
{
    AllowOnDemand             No
    LocalPortGranularity      Rule
    RemotePortGranularity     Rule
    ProtocolGranularity       Rule
    RemoteIpGranularity       Packet
    LocalIpGranularity        Packet
    IcmpCodeGranularity       Rule
    IcmpTypeGranularity       Rule
    IcmpV6CodeGranularity     Rule
    IcmpV6TypeGranularity     Rule
    MipV6TypeGranularity      Rule
    LocalSecurityEndpointRef   BetweenOSAsRSA7~LSE~4
    RemoteSecurityEndpointRef  BetweenOSAsRSA7~RSE~3
}

## NOTE -- Generated IpFilterRule BetweenOSAsRSA7~6
IpFilterRule                  BetweenOSAsRSA7~6
{
    IpSourceAddrRef           BetweenOSAsRSA7~ADR~1
    IpDestAddrRef             BetweenOSAsRSA7~ADR~2
    IpServiceRef               IKE~Gen
    IpGenericFilterActionRef    Permit__LogYes
}

IpFilterRule                  BetweenOSAsRSA7~7
{
    IpSourceAddrRef           BetweenOSAsRSA7~ADR~1
    IpDestAddrRef             BetweenOSAsRSA7~ADR~2
    IpServiceRef               FTP-Client
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A
}

IpFilterRule                  BetweenOSAsRSA7~9
{
    IpSourceAddrRef           BetweenOSAsRSA7~ADR~1
    IpDestAddrRef             BetweenOSAsRSA7~ADR~2
    IpServiceRef               FTP-Client~1
    IpGenericFilterActionRef    IpSec__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpDynVpnActionRef      VPN~A
    IpLocalStartActionRef  BetweenOSAsRSA7~8
}

IpFilterRule              BetweenOSAsRSA7~10
{
    IpSourceAddrRef       BetweenOSAsRSA7~ADR~1
    IpDestAddrRef         BetweenOSAsRSA7~ADR~2
    IpServiceRef           FTP-Client~2
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef      VPN~A
}

IpFilterRule              BetweenOSAsRSA7~12
{
    IpSourceAddrRef       BetweenOSAsRSA7~ADR~1
    IpDestAddrRef         BetweenOSAsRSA7~ADR~2
    IpServiceRef           FTP-Server
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef      VPN~A
    IpLocalStartActionRef  BetweenOSAsRSA7~8
}

IpFilterRule              BetweenOSAsRSA7~13
{
    IpSourceAddrRef       BetweenOSAsRSA7~ADR~1
    IpDestAddrRef         BetweenOSAsRSA7~ADR~2
    IpServiceRef           FTP-Server~3
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef      VPN~A
}

IpFilterRule              BetweenOSAsRSA7~15
{
    IpSourceAddrRef       BetweenOSAsRSA7~ADR~1
    IpDestAddrRef         BetweenOSAsRSA7~ADR~2
    IpServiceRef           FTP-Server~4
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef      VPN~A
    IpLocalStartActionRef  BetweenOSAsRSA7~8
}
##
## Connectivity Rule TrafficBetweenVIPAs combines the following
items:
##   Local data endpoint      TrafficBetweenVIPAs~ADS~1
##   Remote data endpoint    TrafficBetweenVIPAs~ADS~2
##   Topology                 Filtering - Host
##   Requirement Map
##       CICS                 => Permit
##       FTP-Client           => Permit
##       FTP-Server           => Permit

IpAddrSet                 TrafficBetweenVIPAs~ADS~1
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    Range                192.168.20.101-192.168.20.107
}

IpAddrSet                TrafficBetweenVIPAs~ADS~2
{
    Range                192.168.20.101-192.168.20.107
}

IpFilterRule              TrafficBetweenVIPAs~3
{
    IpSourceAddrSetRef    TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef      TrafficBetweenVIPAs~ADS~2
    IpServiceRef           CICS
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              TrafficBetweenVIPAs~4
{
    IpSourceAddrSetRef    TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef      TrafficBetweenVIPAs~ADS~2
    IpServiceRef           FTP-Client
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              TrafficBetweenVIPAs~5
{
    IpSourceAddrSetRef    TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef      TrafficBetweenVIPAs~ADS~2
    IpServiceRef           FTP-Client~1
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              TrafficBetweenVIPAs~6
{
    IpSourceAddrSetRef    TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef      TrafficBetweenVIPAs~ADS~2
    IpServiceRef           FTP-Client~2
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              TrafficBetweenVIPAs~7
{
    IpSourceAddrSetRef    TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef      TrafficBetweenVIPAs~ADS~2
    IpServiceRef           FTP-Server
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule              TrafficBetweenVIPAs~8
{
    IpSourceAddrSetRef    TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef      TrafficBetweenVIPAs~ADS~2
    IpServiceRef           FTP-Server~3
    IpGenericFilterActionRef Permit__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

}

IpFilterRule                                TrafficBetweenVIPAs~9
{
    IpSourceAddrSetRef                      TrafficBetweenVIPAs~ADS~1
    IpDestAddrSetRef                        TrafficBetweenVIPAs~ADS~2
    IpServiceRef                            FTP-Server~4
    IpGenericFilterActionRef                 Permit__LogYes
}
##
## Connectivity Rule TrafOSA2DVIPAPresh2 combines the following
## items:
##   Local data endpoint                    TrafOSA2DVIPAPresh2~ADR~1
##   Remote data endpoint                  TrafOSA2DVIPAPresh2~ADR~2
##   Topology                             Host to Gateway
##   Requirement Map
##   All_other_traffic                     => VPN~A

IpAddr                                      TrafOSA2DVIPAPresh2~ADR~1
{
    Addr                                    192.168.20.121
}

IpAddr                                      TrafOSA2DVIPAPresh2~ADR~2
{
    Addr                                    192.168.20.122
}

LocalSecurityEndpoint                      TrafOSA2DVIPAPresh2~LSE~4
{
    Identity                               UserAtFqdn ZOS1@WSC.LABS.IBM.COM
    LocationRef                            TrafOSA2DVIPAPresh2~ADR~1
}

RemoteSecurityEndpoint                     TrafOSA2DVIPAPresh2~RSE~3
{
    Identity                               Fqdn WSC.LABS.IBM.COM
    Location                               192.168.20.92
}

KeyExchangeRule                           TrafOSA2DVIPAPresh2~5
{
    LocalSecurityEndpointRef                TrafOSA2DVIPAPresh2~LSE~4
    RemoteSecurityEndpointRef                TrafOSA2DVIPAPresh2~RSE~3
    KeyExchangeActionRef                    TrafOSA2DVIPAPresh2
    SharedKey                               Ebcdic "userlabs"
}

KeyExchangeAction                          TrafOSA2DVIPAPresh2
{
    HowToRespondIKEv1                       Either
    KeyExchangeOfferRef                      VPN~A~5
    AllowNat                                 No
    ReauthInterval                           0
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
    ConstrainSource          192.168.20.121
    ConstrainDest            192.168.20.122
    HowToAuthMe              PresharedKey
}

IpLocalStartAction          TrafOSA2DVIPAPresh2~7
{
    AllowOnDemand            Yes
    LocalPortGranularity     Rule
    RemotePortGranularity    Rule
    ProtocolGranularity      Rule
    RemoteIpGranularity       Packet
    LocalIpGranularity        Packet
    IcmpCodeGranularity       Rule
    IcmpTypeGranularity       Rule
    IcmpV6CodeGranularity     Rule
    IcmpV6TypeGranularity     Rule
    MipV6TypeGranularity      Rule
    InitiateToLocation        IpAddr 192.168.20.92
    LocalSecurityEndpointRef   TrafOSA2DVIPAPresh2~LSE~4
    RemoteSecurityEndpointRef  TrafOSA2DVIPAPresh2~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh2~6
IpFilterRule                 TrafOSA2DVIPAPresh2~6
{
    IpSourceAddrRef           TrafOSA2DVIPAPresh2~ADR~1
    IpDestAddr                192.168.20.92
    IpServiceRef              IKE~Gen
    IpGenericFilterActionRef   Permit__LogYes
}

IpFilterRule                 TrafOSA2DVIPAPresh2~8
{
    IpSourceAddrRef           TrafOSA2DVIPAPresh2~ADR~1
    IpDestAddrRef             TrafOSA2DVIPAPresh2~ADR~2
    IpServiceRef              All_other_traffic
    IpGenericFilterActionRef   IpSec__LogYes
    IpDynVpnActionRef          VPN~A~6
    IpLocalStartActionRef     TrafOSA2DVIPAPresh2~7
}

##
## Connectivity Rule TrafOSA2DVIPAPresh3 combines the following
## items:
##   Local data endpoint      TrafOSA2DVIPAPresh3~ADR~1
##   Remote data endpoint     TrafOSA2DVIPAPresh3~ADR~2
##   Topology                 Host to Gateway
##   Requirement Map
##   All_other_traffic         => VPN~A

IpAddr                       TrafOSA2DVIPAPresh3~ADR~1
{
    Addr                      192.168.20.121
}
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpAddr                                     TrafOSA2DVIPAPresh3~ADR~2
{
  Addr                                     192.168.20.123
}

LocalSecurityEndpoint                     TrafOSA2DVIPAPresh3~LSE~4
{
  Identity                                UserAtFqdn  ZOS1@WSC.LABS.IBM.COM
  LocationRef                             TrafOSA2DVIPAPresh3~ADR~1
}

RemoteSecurityEndpoint                     TrafOSA2DVIPAPresh3~RSE~3
{
  Identity                                Fqdn  WSC.LABS.IBM.COM
  Location                                192.168.20.93
}

KeyExchangeRule                           TrafOSA2DVIPAPresh3~5
{
  LocalSecurityEndpointRef                 TrafOSA2DVIPAPresh3~LSE~4
  RemoteSecurityEndpointRef                 TrafOSA2DVIPAPresh3~RSE~3
  KeyExchangeActionRef                     TrafOSA2DVIPAPresh3
  SharedKey                                Ebcdic "userlabs"
}

KeyExchangeAction                         TrafOSA2DVIPAPresh3
{
  HowToRespondIKEv1                        Either
  KeyExchangeOfferRef                      VPN~A~5
  AllowNat                                  No
  ReauthInterval                           0
  ConstrainSource                           192.168.20.121
  ConstrainDest                             192.168.20.123
  HowToAuthMe                              PresharedKey
}

IpLocalStartAction                        TrafOSA2DVIPAPresh3~7
{
  AllowOnDemand                             Yes
  LocalPortGranularity                       Rule
  RemotePortGranularity                     Rule
  ProtocolGranularity                       Rule
  RemoteIpGranularity                       Packet
  LocalIpGranularity                         Packet
  IcmpCodeGranularity                       Rule
  IcmpTypeGranularity                       Rule
  IcmpV6CodeGranularity                     Rule
  IcmpV6TypeGranularity                     Rule
  MipV6TypeGranularity                       Rule
  InitiateToLocation                         IpAddr 192.168.20.93
  LocalSecurityEndpointRef                   TrafOSA2DVIPAPresh3~LSE~4
  RemoteSecurityEndpointRef                 TrafOSA2DVIPAPresh3~RSE~3
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh3~6
IpFilterRule      TrafOSA2DVIPAPresh3~6
{
    IpSourceAddrRef      TrafOSA2DVIPAPresh3~ADR~1
    IpDestAddr           192.168.20.93
    IpServiceRef          IKE~Gen
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule      TrafOSA2DVIPAPresh3~8
{
    IpSourceAddrRef      TrafOSA2DVIPAPresh3~ADR~1
    IpDestAddrRef        TrafOSA2DVIPAPresh3~ADR~2
    IpServiceRef          All_other_traffic
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef     VPN~A~6
    IpLocalStartActionRef TrafOSA2DVIPAPresh3~7
}
##
## Connectivity Rule TrafOSA2DVIPAPresh4 combines the following
items:
##   Local data endpoint      TrafOSA2DVIPAPresh4~ADR~1
##   Remote data endpoint     TrafOSA2DVIPAPresh4~ADR~2
##   Topology                 Host to Gateway
##   Requirement Map
##   All_other_traffic        => VPN~A

IpAddr            TrafOSA2DVIPAPresh4~ADR~1
{
    Addr            192.168.20.121
}

IpAddr            TrafOSA2DVIPAPresh4~ADR~2
{
    Addr            192.168.20.124
}

LocalSecurityEndpoint TrafOSA2DVIPAPresh4~LSE~4
{
    Identity         UserAtFqdn ZOS1@WSC.LABS.IBM.COM
    LocationRef       TrafOSA2DVIPAPresh4~ADR~1
}

RemoteSecurityEndpoint TrafOSA2DVIPAPresh4~RSE~3
{
    Identity         Fqdn WSC.LABS.IBM.COM
    Location          192.168.20.94
}

KeyExchangeRule    TrafOSA2DVIPAPresh4~5
{
    LocalSecurityEndpointRef TrafOSA2DVIPAPresh4~LSE~4
    RemoteSecurityEndpointRef TrafOSA2DVIPAPresh4~RSE~3
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    KeyExchangeActionRef      TrafOSA2DVIPAPresh4
    SharedKey                  Ebcdic "userlabs"
}

KeyExchangeAction            TrafOSA2DVIPAPresh4
{
    HowToRespondIKEv1         Either
    KeyExchangeOfferRef       VPN~A~5
    AllowNat                   No
    ReauthInterval            0
    ConstrainSource            192.168.20.121
    ConstrainDest              192.168.20.124
    HowToAuthMe                PresharedKey
}

IpLocalStartAction           TrafOSA2DVIPAPresh4~7
{
    AllowOnDemand              Yes
    LocalPortGranularity       Rule
    RemotePortGranularity      Rule
    ProtocolGranularity        Rule
    RemoteIpGranularity        Packet
    LocalIpGranularity          Packet
    IcmpCodeGranularity        Rule
    IcmpTypeGranularity        Rule
    IcmpV6CodeGranularity      Rule
    IcmpV6TypeGranularity      Rule
    MipV6TypeGranularity       Rule
    InitiateToLocation         IpAddr 192.168.20.94
    LocalSecurityEndpointRef    TrafOSA2DVIPAPresh4~LSE~4
    RemoteSecurityEndpointRef   TrafOSA2DVIPAPresh4~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh4~6
IpFilterRule                  TrafOSA2DVIPAPresh4~6
{
    IpSourceAddrRef            TrafOSA2DVIPAPresh4~ADR~1
    IpDestAddr                  192.168.20.94
    IpServiceRef                IKE~Gen
    IpGenericFilterActionRef    Permit__LogYes
}

IpFilterRule                  TrafOSA2DVIPAPresh4~8
{
    IpSourceAddrRef            TrafOSA2DVIPAPresh4~ADR~1
    IpDestAddrRef              TrafOSA2DVIPAPresh4~ADR~2
    IpServiceRef                All_other_traffic
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef           VPN~A~6
    IpLocalStartActionRef       TrafOSA2DVIPAPresh4~7
}

##
## Connectivity Rule TrafOSA2DVIPAPresh5 combines the following
items:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
##    Local data endpoint      TrafOSA2DVIPAPresh5~ADR~1
##    Remote data endpoint    TrafOSA2DVIPAPresh5~ADR~2
##    Topology                Host to Gateway
##    Requirement Map
##    All_other_traffic        => VPN~A

IpAddr                            TrafOSA2DVIPAPresh5~ADR~1
{
    Addr                          192.168.20.121
}

IpAddr                            TrafOSA2DVIPAPresh5~ADR~2
{
    Addr                          192.168.20.125
}

LocalSecurityEndpoint             TrafOSA2DVIPAPresh5~LSE~4
{
    Identity                      UserAtFqdn ZOS1@WSC.LABS.IBM.COM
    LocationRef                   TrafOSA2DVIPAPresh5~ADR~1
}

RemoteSecurityEndpoint            TrafOSA2DVIPAPresh5~RSE~3
{
    Identity                      Fqdn WSC.LABS.IBM.COM
    Location                      192.168.20.95
}

KeyExchangeRule                  TrafOSA2DVIPAPresh5~5
{
    LocalSecurityEndpointRef      TrafOSA2DVIPAPresh5~LSE~4
    RemoteSecurityEndpointRef     TrafOSA2DVIPAPresh5~RSE~3
    KeyExchangeActionRef          TrafOSA2DVIPAPresh5
    SharedKey                     Ebcdic "userlabs"
}

KeyExchangeAction                 TrafOSA2DVIPAPresh5
{
    HowToRespondIKEv1             Either
    KeyExchangeOfferRef           VPN~A~5
    AllowNat                      No
    ReauthInterval                0
    ConstrainSource               192.168.20.121
    ConstrainDest                 192.168.20.125
    HowToAuthMe                   PresharedKey
}

IpLocalStartAction               TrafOSA2DVIPAPresh5~7
{
    AllowOnDemand                 Yes
    LocalPortGranularity          Rule
    RemotePortGranularity         Rule
    ProtocolGranularity           Rule
    RemoteIpGranularity           Packet
}
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

LocalIpGranularity      Packet
IcmpCodeGranularity     Rule
IcmpTypeGranularity     Rule
IcmpV6CodeGranularity   Rule
IcmpV6TypeGranularity   Rule
MipV6TypeGranularity    Rule
InitiateToLocation      IpAddr 192.168.20.95
LocalSecurityEndpointRef TrafOSA2DVIPAPresh5~LSE~4
RemoteSecurityEndpointRef TrafOSA2DVIPAPresh5~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh5~6
IpFilterRule            TrafOSA2DVIPAPresh5~6
{
    IpSourceAddrRef      TrafOSA2DVIPAPresh5~ADR~1
    IpDestAddr           192.168.20.95
    IpServiceRef          IKE~Gen
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule            TrafOSA2DVIPAPresh5~8
{
    IpSourceAddrRef      TrafOSA2DVIPAPresh5~ADR~1
    IpDestAddrRef        TrafOSA2DVIPAPresh5~ADR~2
    IpServiceRef          All_other_traffic
    IpGenericFilterActionRef IpSec__LogYes
    IpDynVpnActionRef     VPN~A~6
    IpLocalStartActionRef TrafOSA2DVIPAPresh5~7
}
##
## Connectivity Rule TrafOSA2DVIPAPresh6 combines the following
items:
##   Local data endpoint      TrafOSA2DVIPAPresh6~ADR~1
##   Remote data endpoint     TrafOSA2DVIPAPresh6~ADR~2
##   Topology                 Host to Gateway
##   Requirement Map
##   All_other_traffic        => VPN~A

IpAddr                  TrafOSA2DVIPAPresh6~ADR~1
{
    Addr                  192.168.20.121
}

IpAddr                  TrafOSA2DVIPAPresh6~ADR~2
{
    Addr                  192.168.20.126
}

LocalSecurityEndpoint    TrafOSA2DVIPAPresh6~LSE~4
{
    Identity              UserAtFqdn ZOS1@WSC.LABS.IBM.COM
    LocationRef            TrafOSA2DVIPAPresh6~ADR~1
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

RemoteSecurityEndpoint      TrafOSA2DVIPAPresh6~RSE~3
{
  Identity                  Fqdn WSC.LABS.IBM.COM
  Location                  192.168.20.96
}

KeyExchangeRule             TrafOSA2DVIPAPresh6~5
{
  LocalSecurityEndpointRef  TrafOSA2DVIPAPresh6~LSE~4
  RemoteSecurityEndpointRef TrafOSA2DVIPAPresh6~RSE~3
  KeyExchangeActionRef      TrafOSA2DVIPAPresh6
  SharedKey                 Ebcdic "userlabs"
}

KeyExchangeAction           TrafOSA2DVIPAPresh6
{
  HowToRespondIKEv1        Either
  KeyExchangeOfferRef       VPN~A~5
  AllowNat                  No
  ReauthInterval            0
  ConstrainSource            192.168.20.121
  ConstrainDest              192.168.20.126
  HowToAuthMe                PresharedKey
}

IpLocalStartAction          TrafOSA2DVIPAPresh6~7
{
  AllowOnDemand              Yes
  LocalPortGranularity        Rule
  RemotePortGranularity       Rule
  ProtocolGranularity         Rule
  RemoteIpGranularity         Packet
  LocalIpGranularity          Packet
  IcmpCodeGranularity         Rule
  IcmpTypeGranularity         Rule
  IcmpV6CodeGranularity       Rule
  IcmpV6TypeGranularity       Rule
  MipV6TypeGranularity        Rule
  InitiateToLocation          IpAddr 192.168.20.96
  LocalSecurityEndpointRef    TrafOSA2DVIPAPresh6~LSE~4
  RemoteSecurityEndpointRef   TrafOSA2DVIPAPresh6~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh6~6
IpFilterRule                 TrafOSA2DVIPAPresh6~6
{
  IpSourceAddrRef            TrafOSA2DVIPAPresh6~ADR~1
  IpDestAddr                  192.168.20.96
  IpServiceRef                IKE~Gen
  IpGenericFilterActionRef    Permit__LogYes
}

IpFilterRule                 TrafOSA2DVIPAPresh6~8
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpSourceAddrRef      TrafOSA2DVIPAPresh6~ADR~1
IpDestAddrRef        TrafOSA2DVIPAPresh6~ADR~2
IpServiceRef         All_other_traffic
IpGenericFilterActionRef  IpSec__LogYes
IpDynVpnActionRef     VPN~A~6
IpLocalStartActionRef TrafOSA2DVIPAPresh6~7
}
##
## Connectivity Rule TrafOSA2DVIPAPresh7 combines the following
items:
##   Local data endpoint      TrafOSA2DVIPAPresh7~ADR~1
##   Remote data endpoint    TrafOSA2DVIPAPresh7~ADR~2
##   Topology                Host to Gateway
##   Requirement Map
##   All_other_traffic       => VPN~A

IpAddr               TrafOSA2DVIPAPresh7~ADR~1
{
  Addr               192.168.20.121
}

IpAddr               TrafOSA2DVIPAPresh7~ADR~2
{
  Addr               192.168.20.127
}

LocalSecurityEndpoint TrafOSA2DVIPAPresh7~LSE~4
{
  Identity           UserAtFqdn ZOS1@WSC.LABS.IBM.COM
  LocationRef        TrafOSA2DVIPAPresh7~ADR~1
}

RemoteSecurityEndpoint TrafOSA2DVIPAPresh7~RSE~3
{
  Identity           Fqdn WSC.LABS.IBM.COM
  Location            192.168.20.97
}

KeyExchangeRule      TrafOSA2DVIPAPresh7~5
{
  LocalSecurityEndpointRef TrafOSA2DVIPAPresh7~LSE~4
  RemoteSecurityEndpointRef TrafOSA2DVIPAPresh7~RSE~3
  KeyExchangeActionRef    TrafOSA2DVIPAPresh7
  SharedKey               Ebcdic "userlabs"
}

KeyExchangeAction     TrafOSA2DVIPAPresh7
{
  HowToRespondIKEv1      Either
  KeyExchangeOfferRef    VPN~A~5
  AllowNat               No
  ReauthInterval         0
  ConstrainSource        192.168.20.121
  ConstrainDest          192.168.20.127
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    HowToAuthMe                PresharedKey
}

IpLocalStartAction            TrafOSA2DVIPAPresh7~7
{
    AllowOnDemand              Yes
    LocalPortGranularity       Rule
    RemotePortGranularity      Rule
    ProtocolGranularity        Rule
    RemoteIpGranularity        Packet
    LocalIpGranularity         Packet
    IcmpCodeGranularity        Rule
    IcmpTypeGranularity        Rule
    IcmpV6CodeGranularity      Rule
    IcmpV6TypeGranularity      Rule
    MipV6TypeGranularity       Rule
    InitiateToLocation         IpAddr 192.168.20.97
    LocalSecurityEndpointRef    TrafOSA2DVIPAPresh7~LSE~4
    RemoteSecurityEndpointRef   TrafOSA2DVIPAPresh7~RSE~3
}

## NOTE -- Generated IpFilterRule TrafOSA2DVIPAPresh7~6
IpFilterRule                  TrafOSA2DVIPAPresh7~6
{
    IpSourceAddrRef            TrafOSA2DVIPAPresh7~ADR~1
    IpDestAddr                 192.168.20.97
    IpServiceRef               IKE~Gen
    IpGenericFilterActionRef    Permit__LogYes
}

IpFilterRule                  TrafOSA2DVIPAPresh7~8
{
    IpSourceAddrRef            TrafOSA2DVIPAPresh7~ADR~1
    IpDestAddrRef              TrafOSA2DVIPAPresh7~ADR~2
    IpServiceRef               All_other_traffic
    IpGenericFilterActionRef    IpSec__LogYes
    IpDynVpnActionRef          VPN~A~6
    IpLocalStartActionRef      TrafOSA2DVIPAPresh7~7
}

##
## Connectivity Rule CommonTraffic combines the following items:
##   Local data endpoint      All4
##   Remote data endpoint     All4
##   Topology                 Filtering - Host
##   Requirement Map         BasicServices
##   DNS                     => Permit
##   ICMP-Time_Exceeded-IP_V4 => Permit
##   ICMP-Unreachable-IP_V4  => Permit
##   OMPROUTE-IP_V4          => Permit
##   Path_MTU_Discovery-IP_V4 => Permit
##   Ping-IP_V4              => Permit
##   Resolver                 => Permit
##   Trace_Route-IP_V4       => Permit
##   NSS_Client               => Permit

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
##      NSS_Server      => Permit

IpFilterRule      CommonTraffic~1
{
    IpSourceAddr      All4
    IpDestAddr         All4
    IpServiceRef       DNS
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule      CommonTraffic~2
{
    IpSourceAddr      All4
    IpDestAddr         All4
    IpServiceRef       DNS~7
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule      CommonTraffic~3
{
    IpSourceAddr      All4
    IpDestAddr         All4
    IpServiceRef       DNS~8
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule      CommonTraffic~4
{
    IpSourceAddr      All4
    IpDestAddr         All4
    IpServiceRef       DNS~9
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule      CommonTraffic~5
{
    IpSourceAddr      All4
    IpDestAddr         All4
    IpServiceRef       ICMP-Time_Exceeded-IP_V4
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule      CommonTraffic~6
{
    IpSourceAddr      All4
    IpDestAddr         All4
    IpServiceRef       ICMP-Unreachable-IP_V4
    IpGenericFilterActionRef  Permit__LogYes
}

IpFilterRule      CommonTraffic~7
{
    IpSourceAddr      All4
    IpDestAddr         All4
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpServiceRef      OMPROUTE-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~8
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      OMPROUTE-IP_V4~10
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~9
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      OMPROUTE-IP_V4~11
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~10
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      OMPROUTE-IP_V4~12
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~11
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      OMPROUTE-IP_V4~13
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~12
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Path_MTU_Discovery-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~13
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef      Ping-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~14
{

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Ping-IP_V4~14
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~15
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Resolver
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~16
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Resolver~15
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~17
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Trace_Route-IP_V4
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~18
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Trace_Route-IP_V4~16
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~19
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Trace_Route-IP_V4~17
    IpGenericFilterActionRef Permit__LogYes
}

IpFilterRule          CommonTraffic~20
{
    IpSourceAddr      All4
    IpDestAddr        All4
    IpServiceRef       Trace_Route-IP_V4~18
    IpGenericFilterActionRef Permit__LogYes
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpFilterRule                                CommonTraffic~21
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            NSS_Client
    IpGenericFilterActionRef                Permit__LogYes
}

IpFilterRule                                CommonTraffic~22
{
    IpSourceAddr                            All4
    IpDestAddr                              All4
    IpServiceRef                            NSS_Server
    IpGenericFilterActionRef                Permit__LogYes
}

KeyExchangePolicy
{
    AllowNat                                No
    NatKeepAliveInterval                    20
    HowToInitiate                           IKEv2
    LivenessInterval                        30
    BypassIpValidation                      Yes
    CertificateURLLookupPreference          Tolerate
    RevocationChecking                      Loose
    KeyExchangeRuleRef                      BetweenOSAsRSA2~5
    KeyExchangeRuleRef                      BetweenOSAsRSA3~5
    KeyExchangeRuleRef                      BetweenOSAsRSA4~5
    KeyExchangeRuleRef                      BetweenOSAsRSA5~5
    KeyExchangeRuleRef                      BetweenOSAsRSA6~5
    KeyExchangeRuleRef                      BetweenOSAsRSA7~5
    KeyExchangeRuleRef                      TrafOSA2DVIPAPresh2~5
    KeyExchangeRuleRef                      TrafOSA2DVIPAPresh3~5
    KeyExchangeRuleRef                      TrafOSA2DVIPAPresh4~5
    KeyExchangeRuleRef                      TrafOSA2DVIPAPresh5~5
    KeyExchangeRuleRef                      TrafOSA2DVIPAPresh6~5
    KeyExchangeRuleRef                      TrafOSA2DVIPAPresh7~5
}

IpFilterPolicy
{
    PreDecap                                OFF
    FilterLogging                           ON
    IpFilterLogImplicit                     No
    AllowOnDemand                           Yes
    ImplicitDiscardAction                   Silent
    FIPS140                                No
    IpFilterRuleRef                         NssTrafficIPv4
    IpFilterRuleRef                         NssTrafficIPv4~1
    IpFilterRuleRef                         BetweenOSAsRSA2~6
    IpFilterRuleRef                         BetweenOSAsRSA2~7
    IpFilterRuleRef                         BetweenOSAsRSA2~9
    IpFilterRuleRef                         BetweenOSAsRSA2~10
    IpFilterRuleRef                         BetweenOSAsRSA2~12
}

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

IpFilterRuleRef	BetweenOSAsRSA2~13
IpFilterRuleRef	BetweenOSAsRSA2~15
IpFilterRuleRef	BetweenOSAsRSA3~6
IpFilterRuleRef	BetweenOSAsRSA3~7
IpFilterRuleRef	BetweenOSAsRSA3~9
IpFilterRuleRef	BetweenOSAsRSA3~10
IpFilterRuleRef	BetweenOSAsRSA3~12
IpFilterRuleRef	BetweenOSAsRSA3~13
IpFilterRuleRef	BetweenOSAsRSA3~15
IpFilterRuleRef	BetweenOSAsRSA4~6
IpFilterRuleRef	BetweenOSAsRSA4~7
IpFilterRuleRef	BetweenOSAsRSA4~9
IpFilterRuleRef	BetweenOSAsRSA4~10
IpFilterRuleRef	BetweenOSAsRSA4~12
IpFilterRuleRef	BetweenOSAsRSA4~13
IpFilterRuleRef	BetweenOSAsRSA4~15
IpFilterRuleRef	BetweenOSAsRSA5~6
IpFilterRuleRef	BetweenOSAsRSA5~7
IpFilterRuleRef	BetweenOSAsRSA5~9
IpFilterRuleRef	BetweenOSAsRSA5~10
IpFilterRuleRef	BetweenOSAsRSA5~12
IpFilterRuleRef	BetweenOSAsRSA5~13
IpFilterRuleRef	BetweenOSAsRSA5~15
IpFilterRuleRef	BetweenOSAsRSA6~6
IpFilterRuleRef	BetweenOSAsRSA6~7
IpFilterRuleRef	BetweenOSAsRSA6~9
IpFilterRuleRef	BetweenOSAsRSA6~10
IpFilterRuleRef	BetweenOSAsRSA6~12
IpFilterRuleRef	BetweenOSAsRSA6~13
IpFilterRuleRef	BetweenOSAsRSA6~15
IpFilterRuleRef	BetweenOSAsRSA7~6
IpFilterRuleRef	BetweenOSAsRSA7~7
IpFilterRuleRef	BetweenOSAsRSA7~9
IpFilterRuleRef	BetweenOSAsRSA7~10
IpFilterRuleRef	BetweenOSAsRSA7~12
IpFilterRuleRef	BetweenOSAsRSA7~13
IpFilterRuleRef	BetweenOSAsRSA7~15
IpFilterRuleRef	TrafficBetweenVIPAs~3
IpFilterRuleRef	TrafficBetweenVIPAs~4
IpFilterRuleRef	TrafficBetweenVIPAs~5
IpFilterRuleRef	TrafficBetweenVIPAs~6
IpFilterRuleRef	TrafficBetweenVIPAs~7
IpFilterRuleRef	TrafficBetweenVIPAs~8
IpFilterRuleRef	TrafficBetweenVIPAs~9
IpFilterRuleRef	TrafOSA2DVIPAPresh2~6
IpFilterRuleRef	TrafOSA2DVIPAPresh2~8
IpFilterRuleRef	TrafOSA2DVIPAPresh3~6
IpFilterRuleRef	TrafOSA2DVIPAPresh3~8
IpFilterRuleRef	TrafOSA2DVIPAPresh4~6
IpFilterRuleRef	TrafOSA2DVIPAPresh4~8
IpFilterRuleRef	TrafOSA2DVIPAPresh5~6
IpFilterRuleRef	TrafOSA2DVIPAPresh5~8
IpFilterRuleRef	TrafOSA2DVIPAPresh6~6
IpFilterRuleRef	TrafOSA2DVIPAPresh6~8

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilterRuleRef      TrafOSA2DVIPAPresh7~6
IpFilterRuleRef      TrafOSA2DVIPAPresh7~8
IpFilterRuleRef      CommonTraffic~1
IpFilterRuleRef      CommonTraffic~2
IpFilterRuleRef      CommonTraffic~3
IpFilterRuleRef      CommonTraffic~4
IpFilterRuleRef      CommonTraffic~5
IpFilterRuleRef      CommonTraffic~6
IpFilterRuleRef      CommonTraffic~7
IpFilterRuleRef      CommonTraffic~8
IpFilterRuleRef      CommonTraffic~9
IpFilterRuleRef      CommonTraffic~10
IpFilterRuleRef      CommonTraffic~11
IpFilterRuleRef      CommonTraffic~12
IpFilterRuleRef      CommonTraffic~13
IpFilterRuleRef      CommonTraffic~14
IpFilterRuleRef      CommonTraffic~15
IpFilterRuleRef      CommonTraffic~16
IpFilterRuleRef      CommonTraffic~17
IpFilterRuleRef      CommonTraffic~18
IpFilterRuleRef      CommonTraffic~19
IpFilterRuleRef      CommonTraffic~20
IpFilterRuleRef      CommonTraffic~21
IpFilterRuleRef      CommonTraffic~22
}
```

pasearch Command Output

TCP/IP pasearch CS V2R3

Date: 05/23/2018
QoS Instance Id: 1526855473
IDS Instance Id: 1526928819
IPSec Instance Id: 1526932888
TLS Instance Id: 1526947704

Image Name: TCPIPT

Time: 19:53:04

policyRule: dns-tcp

Rule Type: QoS

Version: 2

Weight: 3

Priority: 0

No. Policy Action: 1

policyAction: interactive1

ActionType: QOS

Action Sequence: 0

Time Periods:

Day of Month Mask:

First to Last: 11111111111111111111111111111111

Last to First: 11111111111111111111111111111111

Month of Yr Mask: 1111111111

Day of Week Mask: 111111 (Sunday - Saturday)

Start Date Time: None

End Date Time: None

Status: Active

ForLoadDist: False

Sequence Actions: Don't Care

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 6 ProtocolNumTo: 6
SourcePortFrom: 42 SourcePortTo: 42
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: interactive1
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 10000000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: dns-udp
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
policyAction: interactive1
ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 17 ProtocolNumTo: 17
SourcePortFrom: 42 SourcePortTo: 42
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: interactive1
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 10000000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: ftpd
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
policyAction: batch1
ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 6 ProtocolNumTo: 6
SourcePortFrom: 20 SourcePortTo: 21
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: batch1
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 01000000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: ntp
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
policyAction: crit-realtime
ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 17 ProtocolNumTo: 17
SourcePortFrom: 123 SourcePortTo: 123
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: crit-realtime
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 10100000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: routed
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
policyAction: networkcontrol
ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 17 ProtocolNumTo: 17
SourcePortFrom: 520 SourcePortTo: 520
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: networkcontrol
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 11100000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: telnetd
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
policyAction: interactive1
ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 17 ProtocolNumTo: 17
SourcePortFrom: 12002 SourcePortTo: 12002
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: interactive1
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 10000000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: EE-lowpri
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
policyAction: batch2
ActionType: QOS
Action Sequence: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Time Periods:

Day of Month Mask:

First to Last: 11111111111111111111111111111111

Last to First: 11111111111111111111111111111111

Month of Yr Mask: 111111111111

Day of Week Mask: 1111111 (Sunday - Saturday)

Start Date Time: None

End Date Time: None

Fr TimeOfDay: 00:00

To TimeOfDay: 24:00

Fr TimeOfDay UTC: 04:00

To TimeOfDay UTC: 04:00

TimeZone: Local

Net Condition Summary:

NegativeIndicator: Off

RouteCondition:

InInterface: All

OutInterface: All

IncomingTOS: 00000000

IncomingTOSMask: 0

HostCondition:

SourceIpFrom: All

SourceIpTo: All

DestIpFrom: All

DestIpTo: All

DestHostDomainName:

ApplicationCondition:

ProtocolNumFrom: 17

ProtocolNumTo: 17

SourcePortFrom: 12004

SourcePortTo: 12004

DestPortFrom: 0

DestPortTo: 0

ApplicationName:

ApplPriority: 0

ApplicationData:

Policy created: Sun May 20 18:31:13 2018

Policy updated: Sun May 20 18:31:13 2018

Qos Action: batch2

Version: 2

Status: Active

Scope: DataTraffic

OutgoingTOS: 00100000

Permission: Allowed

MaxRate: 0

MinRate: 0

MaxConn: 0

Routing Interfaces: 0

RSVP Attributes:

ServiceType: 0

MaxRatePerFlow: 0

MaxTokBuckPerFlw: 0

MaxFlows: 0

SignalClient: True

DiffServ Attributes:

InProfRate: 0

InProfPeakRate: 0

InProfTokBuck: 0

InProfMaxPackSz: 0

OutProfXmtTOSByte: 00000000

ExcessTrafficTr: BestEffort

Policy created: Sun May 20 18:31:13 2018

Policy updated: Sun May 20 18:31:13 2018

policyRule: EE-medpri

Rule Type: QoS

Version: 2

Status: Active

Weight: 3

ForLoadDist: False

Priority: 0

Sequence Actions: Don't Care

No. Policy Action: 1

policyAction: batch1

ActionType: QOS

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Action Sequence: 0

Time Periods:

Day of Month Mask:

First to Last: 11111111111111111111111111111111

Last to First: 11111111111111111111111111111111

Month of Yr Mask: 1111111111

Day of Week Mask: 1111111 (Sunday - Saturday)

Start Date Time: None

End Date Time: None

Fr TimeOfDay: 00:00 To TimeOfDay: 24:00

Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00

TimeZone: Local

Net Condition Summary: NegativeIndicator: Off

RouteCondition:

InInterface: All

OutInterface: All

IncomingTOS: 00000000 IncomingTOSMask: 0

HostCondition:

SourceIpFrom: All

SourceIpTo: All

DestIpFrom: All

DestIpTo: All

DestHostDomainName:

ApplicationCondition:

ProtocolNumFrom: 17 ProtocolNumTo: 17

SourcePortFrom: 12003 SourcePortTo: 12003

DestPortFrom: 0 DestPortTo: 0

ApplicationName: ApplPriority: 0

ApplicationData:

Policy created: Sun May 20 18:31:13 2018

Policy updated: Sun May 20 18:31:13 2018

Qos Action: batch1

Version: 2 Status: Active

Scope: DataTraffic OutgoingTOS: 01000000

Permission: Allowed

MaxRate: 0 MinRate: 0

MaxConn: 0

Routing Interfaces: 0

RSVP Attributes:

ServiceType: 0 MaxRatePerFlow: 0

MaxTokBuckPerFlw: 0 MaxFlows: 0

SignalClient: True

DiffServ Attributes:

InProfRate: 0 InProfPeakRate: 0

InProfTokBuck: 0 InProfMaxPackSz: 0

OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort

Policy created: Sun May 20 18:31:13 2018

Policy updated: Sun May 20 18:31:13 2018

policyRule: EE-network

Rule Type: QoS

Version: 2 Status: Active

Weight: 3 ForLoadDist: False

Priority: 0 Sequence Actions: Don't Care

No. Policy Action: 1

policyAction: internetwork

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off
RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 17 ProtocolNumTo: 17
SourcePortFrom: 12001 SourcePortTo: 12001
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: internetwork
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 11000000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: EE-xid
Rule Type: QoS
Version: 2 Status: Active
Weight: 3 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

policyAction: internetwork
ActionType: QOS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Net Condition Summary: NegativeIndicator: Off

RouteCondition:
InInterface: All
OutInterface: All
IncomingTOS: 00000000 IncomingTOSMask: 0
HostCondition:
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
DestHostDomainName:
ApplicationCondition:
ProtocolNumFrom: 17 ProtocolNumTo: 17
SourcePortFrom: 12000 SourcePortTo: 12000
DestPortFrom: 0 DestPortTo: 0
ApplicationName: ApplPriority: 0
ApplicationData:

Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

Qos Action: internetwork
Version: 2 Status: Active
Scope: DataTraffic OutgoingTOS: 11000000
Permission: Allowed
MaxRate: 0 MinRate: 0
MaxConn: 0
Routing Interfaces: 0
RSVP Attributes:
ServiceType: 0 MaxRatePerFlow: 0
MaxTokBuckPerFlw: 0 MaxFlows: 0
SignalClient: True
DiffServ Attributes:
InProfRate: 0 InProfPeakRate: 0
InProfTokBuck: 0 InProfMaxPackSz: 0
OutProfXmtTOSByte: 00000000 ExcessTrafficTr: BestEffort
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018

policyRule: ospf
Rule Type: QoS
Version: 2 Status: Active
Weight: 2 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
No. Policy Action:      1
policyAction:          networkcontrol
  ActionType:          QOS
  Action Sequence:     0
Time Periods:
  Day of Month Mask:
  First to Last:       11111111111111111111111111111111
  Last to First:       11111111111111111111111111111111
  Month of Yr Mask:     111111111111
  Day of Week Mask:     1111111  (Sunday - Saturday)
  Start Date Time:      None
  End Date Time:        None
  Fr TimeOfDay:         00:00           To TimeOfDay:         24:00
  Fr TimeOfDay UTC:     04:00           To TimeOfDay UTC:     04:00
  TimeZone:             Local
```

Net Condition Summary: NegativeIndicator: Off

```
RouteCondition:
  InInterface:      All
  OutInterface:     All
  IncomingTOS:      00000000      IncomingTOSMask: 0
```

```
HostCondition:
  SourceIpFrom:      All
  SourceIpTo:        All
  DestIpFrom:        All
  DestIpTo:          All
  DestHostDomainName:
```

```
ApplicationCondition:
  ProtocolNumFrom:      89          ProtocolNumTo:      89
  SourcePortFrom:       0          SourcePortTo:       0
  DestPortFrom:         0          DestPortTo:         0
  ApplicationName:
  ApplPriority:         0
  ApplicationData:
```

```
Policy created: Sun May 20 18:31:13 2018
Policy updated: Sun May 20 18:31:13 2018
```

Qos Action:	networkcontrol		
Version:	2	Status:	Active
Scope:	DataTraffic	OutgoingTOS:	11100000
Permission:	Allowed		
MaxRate:	0	MinRate:	0
MaxConn:	0		
Routing Interfaces:	0		
RSVP Attributes:			
ServiceType:	0	MaxRatePerFlow:	0
MaxTokBuckPerFlw:	0	MaxFlows:	0
SignalClient:	True		
DiffServ Attributes:			
InProfRate:	0	InProfPeakRate:	0
InProfTokBuck:	0	InProfMaxPackSz:	0
OutProfXmtTOSByte:	00000000	ExcessTrafficTr:	BestEffort
Policy created: Sun May 20 18:31:13 2018			
Policy updated: Sun May 20 18:31:13 2018			

```
policyRule:      All_Well-Known_TCP~1
  Rule Type:     IDS
  Version:       4                               Status:      Active
  Weight:        65100                           ForLoadDist:  False
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Priority:                65000                      Sequence Actions:    Don't Care
No. Policy Action:      1
IdsType:                policyIdsScanEvent
policyAction:           ScanAction
  ActionType:           IDS
  Action Sequence:      0
Time Periods:
  Day of Month Mask:
  First to Last:        11111111111111111111111111111111
  Last to First:        11111111111111111111111111111111
  Month of Yr Mask:     111111111111
  Day of Week Mask:     1111111  (Sunday - Saturday)
  Start Date Time:      None
  End Date Time:        None
  Fr TimeOfDay:         00:00                      To TimeOfDay:       24:00
  Fr TimeOfDay UTC:     04:00                      To TimeOfDay UTC:   04:00
  TimeZone:             Local
Ids Condition Summary:                                     NegativeIndicator: Off
ScanEvent Condition:
  Sensitivity:          Medium
  Protocol:             TCP    (6)
  LocalPortFrom:        1                      LocalPortTo:        1023
  LocalHostAddress:
    FromAddr:           All
    ToAddr:             All
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

```

```

Ids Action:      ScanAction
Version:         4                      Status:      Active
ScanEvent ActionType: Count
Policy created:  Mon May 21 14:53:39 2018
Policy updated:  Mon May 21 14:53:39 2018

```

```

policyRule:                TN3270-Server~1
  Rule Type:                IDS
  Version:                  4
  Weight:                   65100
  Priority:                  65000
  No. Policy Action:        1
  IdsType:                  policyIdsTR
  policyAction:              TN3270-Server
    ActionType:              IDS
    Action Sequence:         0
  Time Periods:
    Day of Month Mask:
      First to Last:         11111111111111111111111111111111
      Last to First:         11111111111111111111111111111111
    Month of Yr Mask:        111111111111
    Day of Week Mask:        1111111  (Sunday - Saturday)
    Start Date Time:         None
    End Date Time:           None
    Fr TimeOfDay:            00:00
    To TimeOfDay:            24:00
    Fr TimeOfDay UTC:        04:00
    To TimeOfDay UTC:        04:00
    TimeZone:                Local
  Ids Condition Summary:
    TR Condition:
      NegativeIndicator:      Off

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
LocalPortFrom:      23                      LocalPortTo:      23
LocalHostAddress:
  FromAddr:         All
  ToAddr:           All
Protocol:           TCP    (6)
TcpTotConnections:  100                      TcpPercentage:    3
TcpLimitScope:      PortInstance
UDPQueueSize:       Very Long
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:         TN3270-Server
Version:            4                      Status:           Active
TR ActionType:      Limit
TypeActions:        Statistics Log
StatType:           Normal                  StatInterval:     60
LogDetail:          No                      LoggingLevel:      4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:         All_Well-Known_UDP~1
Rule Type:          IDS
Version:            4                      Status:           Active
Weight:             65090                  ForLoadDist:      False
Priority:            64990                  Sequence Actions: Don't Care
No. Policy Action:  1
IdsType:            policyIdsScanEvent
policyAction:       ScanAction
ActionType:         IDS
Action Sequence:    0
Time Periods:
  Day of Month Mask:
  First to Last:    11111111111111111111111111111111
  Last to First:    11111111111111111111111111111111
  Month of Yr Mask:  111111111111
  Day of Week Mask:  1111111 (Sunday - Saturday)
  Start Date Time:  None
  End Date Time:    None
  Fr TimeOfDay:     00:00                  To TimeOfDay:     24:00
  Fr TimeOfDay UTC: 04:00                  To TimeOfDay UTC: 04:00
  TimeZone:         Local
Ids Condition Summary:
ScanEvent Condition:
  Sensitivity:      Medium
  Protocol:         UDP    (17)
  LocalPortFrom:    1                      LocalPortTo:      1023
  LocalHostAddress:
    FromAddr:       All
    ToAddr:         All
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:         ScanAction
Version:            4                      Status:           Active
ScanEvent ActionType: Count
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
policyRule:          ICMP~1
  Rule Type:         IDS
  Version:           4
  Weight:            65080
  Priority:           64980
  No. Policy Action: 1
  IdsType:           policyIdsScanEvent
  policyAction:       ScanAction
    ActionType:      IDS
    Action Sequence: 0
  Time Periods:
    Day of Month Mask:
      First to Last: 11111111111111111111111111111111
      Last to First: 11111111111111111111111111111111
    Month of Yr Mask: 111111111111
    Day of Week Mask: 1111111 (Sunday - Saturday)
    Start Date Time:  None
    End Date Time:    None
    Fr TimeOfDay:     00:00
    To TimeOfDay:     24:00
    Fr TimeOfDay UTC: 04:00
    To TimeOfDay UTC: 04:00
    TimeZone:         Local
  Ids Condition Summary:
    ScanEvent Condition:
      Sensitivity:     High
      Protocol:        ICMP (1)
      LocalPortFrom:   0
      LocalPortTo:     0
      LocalHostAddress:
        FromAddr:      All
        ToAddr:         All
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018
```

```
Ids Action:          ScanAction
  Version:            4
  ScanEvent ActionType: Count
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018
  Status:             Active
```

```
policyRule:          Echo
  Rule Type:         IDS
  Version:           4
  Weight:            3
  Priority:           0
  No. Policy Action: 1
  IdsType:           policyIdsAttack
  policyAction:       Echo
    ActionType:      IDS
    Action Sequence: 0
  Time Periods:
    Day of Month Mask:
      First to Last: 11111111111111111111111111111111
      Last to First: 11111111111111111111111111111111
    Month of Yr Mask: 111111111111
    Day of Week Mask: 1111111 (Sunday - Saturday)
    Start Date Time:  None
    End Date Time:    None
  Status:             Active
  ForLoadDist:        False
  Sequence Actions:   Don't Care
  ConditionListType:  CNF
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Fr TimeOfDay:      00:00          To TimeOfDay:      24:00
Fr TimeOfDay UTC:   04:00          To TimeOfDay UTC:   04:00
TimeZone:          Local
Ids Condition Summary:          NegativeIndicator: Off
Attack Condition:
  IdsAttackType:      PERPETUAL_ECHO
  LocalPortFrom:      7          LocalPortTo:      19
  RemotePortFrom:     7          RemotePortTo:     19
Condition Work Level:          0
  Group Number:       0          Cond Count:       1
  Ignore:             No
Ids Condition Work Summary:     NegativeIndicator: Off
Attack Condition:
  IdsAttackType:      PERPETUAL_ECHO
Condition Work Level:          1
  Group Number:       1          Cond Count:       5
  Ignore:             No
Ids Condition Work Summary:     NegativeIndicator: Off
Attack Condition:
  LocalPortFrom:      7          LocalPortTo:      19
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  LocalPortFrom:      7          LocalPortTo:      7
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  LocalPortFrom:      13         LocalPortTo:      13
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  LocalPortFrom:      17         LocalPortTo:      17
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  LocalPortFrom:      19         LocalPortTo:      19
Condition Work Level:          2
  Group Number:       2          Cond Count:       5
  Ignore:             No
Ids Condition Work Summary:     NegativeIndicator: Off
Attack Condition:
  RemotePortFrom:     7          RemotePortTo:     19
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  RemotePortFrom:     7          RemotePortTo:     7
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  RemotePortFrom:     13         RemotePortTo:     13
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  RemotePortFrom:     17         RemotePortTo:     17
Ids Condition Work:            NegativeIndicator: Off
Attack Condition:
  RemotePortFrom:     19         RemotePortTo:     19
Condition Work Level:          3
  Group Number:       6          Cond Count:       1
  Ignore:             No
Ids Condition Work Summary:     NegativeIndicator: Off
Attack Condition:
  IdsAttackType:      PERPETUAL_ECHO
Policy created: Mon May 21 14:53:39 2018

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy updated: Mon May 21 14:53:39 2018

Ids Action: Echo
Version: 4 Status: Active
Attack ActionType: NoDiscard
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: IPv4Option
Rule Type: IDS
Version: 4 Status: Active
Weight: 2 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IdsType: policyIdsAttack
policyAction: IPv4Option
ActionType: IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: RESTRICTED_IP_OPTIONS
IPOptionFrom: 2 IPOptionTo: 255
Condition Work Level: 0
Group Number: 0 Cond Count: 1
Ignore: No
Ids Condition Work Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: RESTRICTED_IP_OPTIONS
Condition Work Level: 1
Group Number: 5 Cond Count: 6
Ignore: No
Ids Condition Work Summary: NegativeIndicator: Off
Attack Condition:
IPOptionFrom: 2 IPOptionTo: 255
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPOptionFrom: 2 IPOptionTo: 6
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPOptionFrom: 8 IPOptionTo: 67
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPOptionFrom: 69 IPOptionTo: 81

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Ids Condition Work:                               NegativeIndicator: Off
  Attack Condition:
    IPOptionFrom:      83                        IPOptionTo:      147
Ids Condition Work:                               NegativeIndicator: Off
  Attack Condition:
    IPOptionFrom:      149                       IPOptionTo:      255
Condition Work Level:      2
  Group Number:      6                        Cond Count:      1
  Ignore:      No
Ids Condition Work Summary:                       NegativeIndicator: Off
  Attack Condition:
    IdsAttackType:      RESTRICTED_IP_OPTIONS
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:      IPv4Option
  Version:      4                        Status:      Active
  Attack ActionType:      NoDiscard
  TypeActions:      Statistics Log
  StatType:      Normal                StatInterval:      60
  LogDetail:      No                  LoggingLevel:      4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:      IPv4OutboundRaw
  Rule Type:      IDS
  Version:      4                        Status:      Active
  Weight:      2                        ForLoadDist:      False
  Priority:      0                      Sequence Actions:      Don't Care
  No. Policy Action:      1              ConditionListType:      CNF
  IdsType:      policyIdsAttack
  policyAction:      IPv4OutboundRaw
  ActionType:      IDS
  Action Sequence:      0
Time Periods:
  Day of Month Mask:
    First to Last:      11111111111111111111111111111111
    Last to First:      11111111111111111111111111111111
  Month of Yr Mask:      1111111111
  Day of Week Mask:      111111 (Sunday - Saturday)
  Start Date Time:      None
  End Date Time:      None
  Fr TimeOfDay:      00:00                To TimeOfDay:      24:00
  Fr TimeOfDay UTC:      04:00            To TimeOfDay UTC:      04:00
  TimeZone:      Local
Ids Condition Summary:                       NegativeIndicator: Off
  Attack Condition:
    IdsAttackType:      OUTBOUND_RAW
    ProtocolNumFrom:      0                ProtocolNumTo:      255
Condition Work Level:      0
  Group Number:      0                        Cond Count:      1
  Ignore:      No
Ids Condition Work Summary:                       NegativeIndicator: Off
  Attack Condition:
    IdsAttackType:      OUTBOUND_RAW
Condition Work Level:      1
  Group Number:      4                        Cond Count:      5

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Ignore:                No
Ids Condition Work Summary:      NegativeIndicator: Off
Attack Condition:
  ProtocolNumFrom:    0          ProtocolNumTo:    255
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  ProtocolNumFrom:    0          ProtocolNumTo:    0
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  ProtocolNumFrom:    2          ProtocolNumTo:    16
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  ProtocolNumFrom:    18         ProtocolNumTo:    88
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  ProtocolNumFrom:    90         ProtocolNumTo:    255
Condition Work Level:      2
  Group Number:        6          Cond Count:      1
Ignore:                No
Ids Condition Work Summary:      NegativeIndicator: Off
Attack Condition:
  IdsAttackType:      OUTBOUND_RAW
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:             IPv4OutboundRaw
Version:                4          Status:          Active
Attack ActionType:      NoDiscard
TypeActions:            Statistics Log
StatType:               Normal     StatInterval:   60
LogDetail:              No         LoggingLevel:   4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:             IPv4Protocol
Rule Type:              IDS
Version:                4          Status:          Active
Weight:                 2          ForLoadDist:    False
Priority:                0          Sequence Actions: Don't Care
No. Policy Action:      1          ConditionListType: CNF
IdsType:                policyIdsAttack
policyAction:            IPv4Protocol
ActionType:              IDS
Action Sequence:        0
Time Periods:
  Day of Month Mask:
    First to Last:      11111111111111111111111111111111
    Last to First:      11111111111111111111111111111111
  Month of Yr Mask:     1111111111
  Day of Week Mask:     1111111   (Sunday - Saturday)
  Start Date Time:      None
  End Date Time:        None
  Fr TimeOfDay:         00:00      To TimeOfDay:    24:00
  Fr TimeOfDay UTC:     04:00      To TimeOfDay UTC: 04:00
  TimeZone:             Local
Ids Condition Summary:      NegativeIndicator: Off
Attack Condition:

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IdsAttackType:      RESTRICTED_IP_PROTOCOL
    ProtocolNumFrom:    0                      ProtocolNumTo:      255
    Condition Work Level:      0
    Group Number:          0                      Cond Count:      1
    Ignore:                No

```

```

    Ids Condition Work Summary:      NegativeIndicator: Off

```

```

    Attack Condition:
    IdsAttackType:      RESTRICTED_IP_PROTOCOL
    Condition Work Level:      1
    Group Number:          4                      Cond Count:      10
    Ignore:                No

```

```

    Ids Condition Work Summary:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      0                      ProtocolNumTo:      255

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      0                      ProtocolNumTo:      0

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      3                      ProtocolNumTo:      3

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      5                      ProtocolNumTo:      5

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      7                      ProtocolNumTo:      16

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      18                     ProtocolNumTo:      45

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      48                     ProtocolNumTo:      49

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      52                     ProtocolNumTo:      88

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      90                     ProtocolNumTo:      93

```

```

    Ids Condition Work:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    ProtocolNumFrom:      95                     ProtocolNumTo:      255

```

```

    Condition Work Level:      2

```

```

    Group Number:          6                      Cond Count:      1

```

```

    Ignore:                No

```

```

    Ids Condition Work Summary:      NegativeIndicator: Off

```

```

    Attack Condition:

```

```

    IdsAttackType:      RESTRICTED_IP_PROTOCOL

```

```

    Policy created: Mon May 21 14:53:39 2018

```

```

    Policy updated: Mon May 21 14:53:39 2018

```

```

    Ids Action:          IPv4Protocol
    Version:             4                      Status:          Active
    Attack ActionType:    NoDiscard
    TypeActions:          Statistics Log
    StatType:             Normal                StatInterval:    60
    LogDetail:            No                    LoggingLevel:     4
    Policy created: Mon May 21 14:53:39 2018

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy updated: Mon May 21 14:53:39 2018

```
policyRule: IPv6DestinationOptions
Rule Type:  IDS
Version:    4                      Status:    Active
Weight:     2                      ForLoadDist: False
Priority:    0                      Sequence Actions: Don't Care
No. Policy Action: 1                ConditionListType: CNF
IdsType:    policyIdsAttack
policyAction: IPv6DestinationOptions
ActionType:  IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00                To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00            To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: RESTRICTED_IPV6_DST_OPTIONS
IPv6OptionFrom: 2                  IPv6OptionTo: 255
Condition Work Level: 0
Group Number: 0                    Cond Count: 1
Ignore: No
Ids Condition Work Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: RESTRICTED_IPV6_DST_OPTIONS
Condition Work Level: 1
Group Number: 5                    Cond Count: 6
Ignore: No
Ids Condition Work Summary: NegativeIndicator: Off
Attack Condition:
IPv6OptionFrom: 2                  IPv6OptionTo: 255
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPv6OptionFrom: 2                  IPv6OptionTo: 3
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPv6OptionFrom: 8                  IPv6OptionTo: 137
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPv6OptionFrom: 139                IPv6OptionTo: 193
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPv6OptionFrom: 195                IPv6OptionTo: 200
Ids Condition Work: NegativeIndicator: Off
Attack Condition:
IPv6OptionFrom: 202                IPv6OptionTo: 255
Condition Work Level: 2
Group Number: 6                    Cond Count: 1
Ignore: No
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Ids Condition Work Summary: NegativeIndicator: Off

Attack Condition:

IdsAttackType: RESTRICTED_IPV6_DST_OPTIONS

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

Ids Action: IPv6DestinationOptions

Version: 4 Status: Active

Attack ActionType: NoDiscard

TypeActions: Statistics Log

StatType: Normal StatInterval: 60

LogDetail: No LoggingLevel: 4

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

policyRule: IPv6HopByHop

Rule Type: IDS

Version: 4 Status: Active

Weight: 2 ForLoadDist: False

Priority: 0 Sequence Actions: Don't Care

No. Policy Action: 1 ConditionListType: CNF

IdsType: policyIdsAttack

policyAction: IPv6HopByHop

ActionType: IDS

Action Sequence: 0

Time Periods:

Day of Month Mask:

First to Last: 11111111111111111111111111111111

Last to First: 11111111111111111111111111111111

Month of Yr Mask: 1111111111

Day of Week Mask: 111111 (Sunday - Saturday)

Start Date Time: None

End Date Time: None

Fr TimeOfDay: 00:00 To TimeOfDay: 24:00

Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00

TimeZone: Local

Ids Condition Summary: NegativeIndicator: Off

Attack Condition:

IdsAttackType: RESTRICTED_IPV6_HOP_OPTIONS

IPv6OptionFrom: 2 IPv6OptionTo: 255

Condition Work Level: 0

Group Number: 0 Cond Count: 1

Ignore: No

Ids Condition Work Summary: NegativeIndicator: Off

Attack Condition:

IdsAttackType: RESTRICTED_IPV6_HOP_OPTIONS

Condition Work Level: 1

Group Number: 5 Cond Count: 6

Ignore: No

Ids Condition Work Summary: NegativeIndicator: Off

Attack Condition:

IPv6OptionFrom: 2 IPv6OptionTo: 255

Ids Condition Work: NegativeIndicator: Off

Attack Condition:

IPv6OptionFrom: 2 IPv6OptionTo: 3

Ids Condition Work: NegativeIndicator: Off

Attack Condition:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    IPv6OptionFrom:      8                      IPv6OptionTo:      137
    Ids Condition Work:   NegativeIndicator: Off
    Attack Condition:
    IPv6OptionFrom:      139                     IPv6OptionTo:      193
    Ids Condition Work:   NegativeIndicator: Off
    Attack Condition:
    IPv6OptionFrom:      195                     IPv6OptionTo:      200
    Ids Condition Work:   NegativeIndicator: Off
    Attack Condition:
    IPv6OptionFrom:      202                     IPv6OptionTo:      255
    Condition Work Level: 2
    Group Number:         6                      Cond Count:        1
    Ignore:               No
    Ids Condition Work Summary: NegativeIndicator: Off
    Attack Condition:
    IdsAttackType:        RESTRICTED_IPV6_HOP_OPTIONS
    Policy created: Mon May 21 14:53:39 2018
    Policy updated: Mon May 21 14:53:39 2018

    Ids Action:           IPv6HopByHop
    Version:              4                      Status:            Active
    Attack ActionType:    NoDiscard
    TypeActions:          Statistics Log
    StatType:             Normal                  StatInterval:      60
    LogDetail:            No                      LoggingLevel:       4
    Policy created: Mon May 21 14:53:39 2018
    Policy updated: Mon May 21 14:53:39 2018

policyRule:              IPv6NextHeader
    Rule Type:            IDS
    Version:              4                      Status:            Active
    Weight:               2                      ForLoadDist:       False
    Priority:              0                      Sequence Actions:  Don't Care
    No. Policy Action:    1                      ConditionListType: CNF
    IdsType:              policyIdsAttack
    policyAction:          IPv6NextHeader
    ActionType:           IDS
    Action Sequence:      0
    Time Periods:
    Day of Month Mask:
    First to Last:        11111111111111111111111111111111
    Last to First:        11111111111111111111111111111111
    Month of Yr Mask:     111111111111
    Day of Week Mask:     1111111 (Sunday - Saturday)
    Start Date Time:      None
    End Date Time:        None
    Fr TimeOfDay:         00:00                  To TimeOfDay:      24:00
    Fr TimeOfDay UTC:     04:00                  To TimeOfDay UTC:  04:00
    TimeZone:             Local
    Ids Condition Summary: NegativeIndicator: Off
    Attack Condition:
    IdsAttackType:        RESTRICTED_IPV6_NEXT_HDR
    IPv6NextHdrFrom:      1                      IPv6NextHdrTo:     255
    Condition Work Level: 0
    Group Number:         0                      Cond Count:        1
    Ignore:               No
    Ids Condition Work Summary: NegativeIndicator: Off

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Attack Condition:
  IdsAttackType:      RESTRICTED_IPV6_NEXT_HDR
Condition Work Level: 1
  Group Number:      4          Cond Count:      10
  Ignore:            No
Ids Condition Work Summary:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    1          IPv6NextHdrTo:    255
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    1          IPv6NextHdrTo:    5
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    7          IPv6NextHdrTo:    16
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    18         IPv6NextHdrTo:    40
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    42         IPv6NextHdrTo:    42
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    45         IPv6NextHdrTo:    49
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    52         IPv6NextHdrTo:    57
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    61         IPv6NextHdrTo:    88
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    90         IPv6NextHdrTo:    134
Ids Condition Work:      NegativeIndicator: Off
Attack Condition:
  IPv6NextHdrFrom:    136        IPv6NextHdrTo:    255
Condition Work Level:    2
  Group Number:      6          Cond Count:      1
  Ignore:            No
Ids Condition Work Summary:      NegativeIndicator: Off
Attack Condition:
  IdsAttackType:      RESTRICTED_IPV6_NEXT_HDR
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:            IPv6NextHeader
Version:               4          Status:            Active
Attack ActionType:    NoDiscard
TypeActions:          Statistics Log
StatType:             Normal      StatInterval:       60
LogDetail:            No          LoggingLevel:       4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:            IPv6OutboundRaw
Rule Type:             IDS
Version:               4          Status:            Active
Weight:                2          ForLoadDist:       False
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Priority:	0	Sequence Actions:	Don't Care
No. Policy Action:	1	ConditionListType:	CNF
IdsType:	policyIdsAttack		
policyAction:	IPv6OutboundRaw		
ActionType:	IDS		
Action Sequence:	0		
Time Periods:			
Day of Month Mask:			
First to Last:	11111111111111111111111111111111		
Last to First:	11111111111111111111111111111111		
Month of Yr Mask:	111111111111		
Day of Week Mask:	1111111 (Sunday - Saturday)		
Start Date Time:	None		
End Date Time:	None		
Fr TimeOfDay:	00:00	To TimeOfDay:	24:00
Fr TimeOfDay UTC:	04:00	To TimeOfDay UTC:	04:00
TimeZone:	Local		
Ids Condition Summary:		NegativeIndicator:	Off
Attack Condition:			
IdsAttackType:	OUTBOUND_RAW_IPV6		
ProtocolNumFrom:	0	ProtocolNumTo:	255
Condition Work Level:	0		
Group Number:	0	Cond Count:	1
Ignore:	No		
Ids Condition Work Summary:		NegativeIndicator:	Off
Attack Condition:			
IdsAttackType:	OUTBOUND_RAW_IPV6		
Condition Work Level:	1		
Group Number:	4	Cond Count:	5
Ignore:	No		
Ids Condition Work Summary:		NegativeIndicator:	Off
Attack Condition:			
ProtocolNumFrom:	0	ProtocolNumTo:	255
Ids Condition Work:		NegativeIndicator:	Off
Attack Condition:			
ProtocolNumFrom:	0	ProtocolNumTo:	16
Ids Condition Work:		NegativeIndicator:	Off
Attack Condition:			
ProtocolNumFrom:	18	ProtocolNumTo:	57
Ids Condition Work:		NegativeIndicator:	Off
Attack Condition:			
ProtocolNumFrom:	59	ProtocolNumTo:	88
Ids Condition Work:		NegativeIndicator:	Off
Attack Condition:			
ProtocolNumFrom:	90	ProtocolNumTo:	255
Condition Work Level:	2		
Group Number:	6	Cond Count:	1
Ignore:	No		
Ids Condition Work Summary:		NegativeIndicator:	Off
Attack Condition:			
IdsAttackType:	OUTBOUND_RAW_IPV6		
Policy created:	Mon May 21 14:53:39 2018		
Policy updated:	Mon May 21 14:53:39 2018		
Ids Action:	IPv6OutboundRaw		
Version:	4	Status:	Active
Attack ActionType:	NoDiscard		

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: DataHiding
Rule Type: IDS
Version: 4 Status: Active
Weight: 1 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsAttack
policyAction: DataHiding
ActionType: IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: DATA_HIDING
OptionPadChk: Enable IcmpEmbedPktChk: Enable
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action: DataHiding
Version: 4 Status: Active
Attack ActionType: NoDiscard
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: EELDLCCheck
Rule Type: IDS
Version: 4 Status: Active
Weight: 1 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsAttack
policyAction: EELDLCCheck
ActionType: IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Month of Yr Mask:      111111111111
Day of Week Mask:      1111111  (Sunday - Saturday)
Start Date Time:       None
End Date Time:         None
Fr TimeOfDay:          00:00      To TimeOfDay:          24:00
Fr TimeOfDay UTC:      04:00      To TimeOfDay UTC:      04:00
TimeZone:              Local
Ids Condition Summary:  NegativeIndicator: Off
Attack Condition:
  IdsAttackType:        EE_LDLC_CHECK
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

```

```

Ids Action:      EELDLCCheck
Version:         4                      Status:      Active
Attack ActionType: NoDiscard
TypeActions:     Statistics Log
StatType:        Normal                 StatInterval: 60
LogDetail:       No                     LoggingLevel:  4
Policy created:  Mon May 21 14:53:39 2018
Policy updated:  Mon May 21 14:53:39 2018

```

```

policyRule:      EEMalformedPacket
Rule Type:      IDS
Version:        4
Weight:         1
Priority:        0
No. Policy Action: 1
IdType:         policyIdsAttack
policyAction:   EEMalformedPacket
  ActionType:   IDS
  Action Sequence: 0
Time Periods:
  Day of Month Mask:
    First to Last: 11111111111111111111111111111111
    Last to First: 11111111111111111111111111111111
  Month of Yr Mask: 111111111111
  Day of Week Mask: 1111111 (Sunday - Saturday)
  Start Date Time: None
  End Date Time: None
  Fr TimeOfDay: 00:00
  To TimeOfDay: 24:00
  Fr TimeOfDay UTC: 04:00
  To TimeOfDay UTC: 04:00
  TimeZone: Local
Ids Condition Summary:
  Attack Condition:
    IdsAttackType: EE_MALFORMED_PACKET
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

```

```

Ids Action:      EEMalformedPacket
Version:         4                      Status:      Active
Attack ActionType: NoDiscard
TypeActions:     Statistics Log
StatType:        Normal                 StatInterval: 60
LogDetail:       No                     LoggingLevel:  4
Policy created:  Mon May 21 14:53:39 2018
Policy updated:  Mon May 21 14:53:39 2018

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
policyRule:          EEPortCheck
  Rule Type:         IDS
  Version:           4
  Weight:            1
  Priority:           0
  No. Policy Action: 1
  IdsType:           policyIdsAttack
  policyAction:      EEPortCheck
    ActionType:      IDS
    Action Sequence: 0
  Time Periods:
    Day of Month Mask:
      First to Last: 11111111111111111111111111111111
      Last to First: 11111111111111111111111111111111
    Month of Yr Mask: 111111111111
    Day of Week Mask: 1111111 (Sunday - Saturday)
    Start Date Time:  None
    End Date Time:    None
    Fr TimeOfDay:     00:00
    To TimeOfDay:     24:00
    Fr TimeOfDay UTC: 04:00
    To TimeOfDay UTC: 04:00
    TimeZone:         Local
  Ids Condition Summary:
    Attack Condition:
      IdsAttackType: EE_PORT_CHECK
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018
```

```
Ids Action:          EEPortCheck
  Version:            4
  Attack ActionType:  NoDiscard
  TypeActions:        Statistics Log
  StatType:           Normal
  LogDetail:          No
  StatInterval:       60
  LoggingLevel:       4
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018
```

```
policyRule:          EEXIDFlood
  Rule Type:         IDS
  Version:           4
  Weight:            1
  Priority:           0
  No. Policy Action: 1
  IdsType:           policyIdsAttack
  policyAction:      EEXIDFlood
    ActionType:      IDS
    Action Sequence: 0
  Time Periods:
    Day of Month Mask:
      First to Last: 11111111111111111111111111111111
      Last to First: 11111111111111111111111111111111
    Month of Yr Mask: 111111111111
    Day of Week Mask: 1111111 (Sunday - Saturday)
    Start Date Time:  None
    End Date Time:    None
    Fr TimeOfDay:     00:00
    To TimeOfDay:     24:00
    Fr TimeOfDay UTC: 04:00
    To TimeOfDay UTC: 04:00
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: EE_XID_FLOOD
EEXIDTimeout: 100
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action: EEXIDFlood
Version: 4 Status: Active
Attack ActionType: NoDiscard
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: Flood
Rule Type: IDS
Version: 4 Status: Active
Weight: 1 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsAttack
policyAction: Flood
ActionType: IDS
Action Sequence: 0

Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: FLOOD
IfcFloodPercent: 10 IfcFloodMinDisc: 1000
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action: Flood
Version: 4 Status: Active
Attack ActionType: Discard
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: Fragmentation
Rule Type: IDS
Version: 4 Status: Active

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Weight: 1 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsAttack
policyAction: Fragmentation
ActionType: IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 11111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
IdsAttackType: IP_FRAGMENT
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

```

```

Ids Action:      Fragmentation
Version:         4           Status:      Active
Attack ActionType: NoDiscard
TypeActions:     Statistics Log
StatType:        Normal      StatInterval: 60
LogDetail:       No          LoggingLevel: 4
Policy created:  Mon May 21 14:53:39 2018
Policy updated:  Mon May 21 14:53:39 2018

```

```

policyRule: GlobalTCPStall
  Rule Type: IDS
  Version: 4
  Weight: 1
  Priority: 0
  No. Policy Action: 1
  IdsType: policyIdsAttack
  policyAction: GlobalTCPStall
    ActionType: IDS
    Action Sequence: 0
  Time Periods:
    Day of Month Mask:
      First to Last: 11111111111111111111111111111111
      Last to First: 11111111111111111111111111111111
    Month of Yr Mask: 111111111111
    Day of Week Mask: 1111111 (Sunday - Saturday)
    Start Date Time: None
    End Date Time: None
    Fr TimeOfDay: 00:00
    To TimeOfDay: 24:00
    Fr TimeOfDay UTC: 04:00
    To TimeOfDay UTC: 04:00
    TimeZone: Local
  Ids Condition Summary: NegativeIndicator: Off
  Attack Condition:
    IdsAttackType: GLOBAL TCP STALL

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

Ids Action: GlobalTCPStall
Version: 4 Status: Active
Attack ActionType: NoResetConn
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: ICMPRedirect
Rule Type: IDS
Version: 4 Status: Active
Weight: 1 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsAttack
policyAction: ICMPRedirect
ActionType: IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
Attack Condition:
Ids Condition Summary: NegativeIndicator: Off
IdsAttackType: ICMP_REDIRECT
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action: ICMPRedirect
Version: 4 Status: Active
Attack ActionType: NoDiscard
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: MalformedPacket
Rule Type: IDS
Version: 4 Status: Active
Weight: 1 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsAttack
policyAction: MalformedPacket

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ActionType:          IDS
Action Sequence:     0
Time Periods:
  Day of Month Mask:
  First to Last:      11111111111111111111111111111111
  Last to First:      11111111111111111111111111111111
  Month of Yr Mask:    111111111111
  Day of Week Mask:    1111111  (Sunday - Saturday)
  Start Date Time:     None
  End Date Time:        None
  Fr TimeOfDay:         00:00          To TimeOfDay:         24:00
  Fr TimeOfDay UTC:     04:00          To TimeOfDay UTC:     04:00
  TimeZone:             Local
Ids Condition Summary:          NegativeIndicator: Off
Attack Condition:
  IdsAttackType:         MALFORMED_PACKET
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:             MalformedPacket
Version:                 4              Status:             Active
Attack ActionType:      Discard
TypeActions:             Statistics Log
StatType:                Normal          StatInterval:         60
LogDetail:               No              LoggingLevel:          4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:              TcpQueueSize
Rule Type:               IDS
Version:                  4              Status:             Active
Weight:                   1              ForLoadDist:         False
Priority:                  0              Sequence Actions:     Don't Care
No. Policy Action:        1
IdsType:                  policyIdsAttack
policyAction:             TcpQueueSize
  ActionType:             IDS
  Action Sequence:         0
Time Periods:
  Day of Month Mask:
  First to Last:          11111111111111111111111111111111
  Last to First:          11111111111111111111111111111111
  Month of Yr Mask:        111111111111
  Day of Week Mask:        1111111  (Sunday - Saturday)
  Start Date Time:         None
  End Date Time:           None
  Fr TimeOfDay:             00:00          To TimeOfDay:         24:00
  Fr TimeOfDay UTC:         04:00          To TimeOfDay UTC:     04:00
  TimeZone:                 Local
Ids Condition Summary:          NegativeIndicator: Off
Attack Condition:
  IdsAttackType:          TCP_QUEUE_SIZE
  TcpQueueSize:           Short
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action:              TcpQueueSize
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Version: 4 Status: Active
Attack ActionType: NoResetConn
TypeActions: Statistics Log
StatType: Normal StatInterval: 60
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: ScanGlobal
Rule Type: IDS
Version: 4 Status: Active
Weight: 0 ForLoadDist: False
Priority: 0 Sequence Actions: Don't Care
No. Policy Action: 1
IdsType: policyIdsScanGlobal
policyAction: ScanGlobalAction
ActionType: IDS
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
Ids Condition Summary: NegativeIndicator: Off
ScanGlobal Condition:
FastScanInterval: 1 FastScanThreshold: 5
SlowScanInterval: 120 SlowScanThreshold: 10
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

Ids Action: ScanGlobalAction
Version: 4 Status: Active
ScanGlobal ActionType
TypeActions: Log
LogDetail: No LoggingLevel: 4
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: BetweenOSAsRSA~6
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 144 ForLoadDist: False
Priority: 44 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Last to First:      11111111111111111111111111111111
Month of Yr Mask:   111111111111
Day of Week Mask:   1111111  (Sunday - Saturday)
Start Date Time:    None
End Date Time:      None
Fr TimeOfDay:       00:00          To TimeOfDay:      24:00
Fr TimeOfDay UTC:   04:00          To TimeOfDay UTC:   04:00
TimeZone:           Local
IpSec Condition Summary:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0          SecurityClass:      0
    FragmentsOnly: No
Condition Work Level:      0
  Group Number:      0          Cond Count:      2
  Ignore:            No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0          SecurityClass:      0
    FragmentsOnly: No
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
    FromAddr:      192.168.20.97
    ToAddr:        192.168.20.97
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0          SecurityClass:      0
    FragmentsOnly: No
Condition Work Level:      1
  Group Number:      1          Cond Count:      2
  Ignore:            No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0          SecurityClass:      0
    FragmentsOnly: No
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
    FromAddr:      192.168.20.91

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    ToAddr:                192.168.20.91
    Service Condition:
    Protocol:               0
    Direction:              0
    RouteType:              0
    FragmentsOnly:         No
    SecurityClass:          0
    Condition Work Level:   2
    Group Number:           3
    Cond Count:             2
    Ignore:                 No
    IpSec Condition Work Summary:
    NegativeIndicator:      Off
    IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
    Protocol:               0
    Direction:              0
    RouteType:              0
    FragmentsOnly:         No
    SecurityClass:          0
    IpSec Condition Work:
    NegativeIndicator:      Off
    IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
    Protocol:               UDP   (17)
    SrcPortFrom:            500
    SrcPortTo:              500
    DestPortFrom:           500
    DestPortTo:             500
    Direction:              Bidirectional
    RouteType:              Local
    SecurityClass:          0
    FragmentsOnly:         No
    Policy created: Mon May 21 14:53:39 2018
    Policy updated: Mon May 21 14:53:39 2018

    IpFilter Action:        Permit__LogYes
    Version:                3
    Status:                  Active
    Scope:                   GenericFilter
    ipFilterAction:          Permit
    IpFilterLogging:         Yes
    DiscardAction:           Silent
    Policy created: Mon May 21 14:53:39 2018
    Policy updated: Mon May 21 14:53:39 2018

    policyRule:              BetweenOSAsRSA~7
    Rule Type:               IpFilter
    Version:                 3
    Status:                   Active
    Weight:                  143
    ForLoadDist:             False
    Priority:                 43
    Sequence Actions:         Don't Care
    No. Policy Action:        2
    ConditionListType:        CNF
    IpSecType:               policyIpFilter
    policyAction:             IpSec__LogYes
    ActionType:              IpFilter GenericFilter
    Action Sequence:          0
    policyAction:             VPN~A
    ActionType:              IpFilter DynamicVpn
    Action Sequence:          0
    Time Periods:
    Day of Month Mask:
    First to Last:           11111111111111111111111111111111
    Last to First:           11111111111111111111111111111111

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local

IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No

IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No

IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: 192.168.20.97
ToAddr: 192.168.20.97
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 1
Group Number: 1 Cond Count: 2
Ignore: No

IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No

IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr: 192.168.20.91
ToAddr: 192.168.20.91

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
  SecurityClass:      0
Condition Work Level: 2
  Group Number:      3
  Cond Count:         2
  Ignore:            No
  NegativeIndicator:  Off
IpSec Condition Work Summary:
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:       0
      Direction:      0
      RouteType:      0
      FragmentsOnly:  No
      SecurityClass:   0
  NegativeIndicator:  Off
IpSec Condition Work:
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:       TCP (6)
      SrcPortFrom:    1024
      SrcPortTo:       65535
      DestPortFrom:    21
      DestPortTo:      21
      Direction:       Bidirectional
      RouteType:       Local
      OutboundConnect:
      SecurityClass:   0
      FragmentsOnly:  No
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      IpSec__LogYes
  Version:             3
  Status:               Active
  Scope:               GenericFilter
  ipFilterAction:      IPSec
  IpFilterLogging:      Yes
  DiscardAction:       Silent
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      VPN~A
  Version:             3
  Status:               Active
  Scope:               DynamicVpn
  Initiation:          Either
  VpnLife:              1440
  AcceptablePfs:       None
  AcceptablePfs:       Group2
  InitiateWithPfs:     Group2
  IpDataOfferNum:      1
  PassthroughDSCP:     Yes
  PassthroughDF:       Yes
  HowToEncapIKEv2:     Either
  IPDataOffer:         0
  HowToEncap:          Transport
  HowToEncrypt:         3DES
  KeyLength:            N/A
  HowToAuth:            ESP
  HowToAuthAlgr:        HMAC_SHA1
  RefLifeTmPropose:    480
  RefLifeTmAcptMin:    480
  RefLifeTmAcptMax:    480
  RefLifeSzPropose:    None
  RefLifeSzAccept :    None
  Policy created: Mon May 21 14:53:39 2018
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy updated: Mon May 21 14:53:39 2018

```
policyRule:          BetweenOSAsRSA~9
  Rule Type:         IpFilter
  Version:           3                      Status:           Active
  Weight:            142                   ForLoadDist:         False
  Priority:           42                   Sequence Actions:    Don't Care
  No. Policy Action: 3                      ConditionListType:   CNF
  IpSecType:         policyIpFilter
  policyAction:      IpSec__LogYes
    ActionType:      IpFilter GenericFilter
    Action Sequence: 0
  policyAction:      VPN~A
    ActionType:      IpFilter DynamicVpn
    Action Sequence: 0
  policyAction:      BetweenOSAsRSA~8
    ActionType:      IpFilter LocalStart
    Action Sequence: 0
Time Periods:
  Day of Month Mask: 11111111111111111111111111111111
  First to Last:     11111111111111111111111111111111
  Last to First:     11111111111111111111111111111111
  Month of Yr Mask:  111111111111
  Day of Week Mask:  1111111 (Sunday - Saturday)
  Start Date Time:   None
  End Date Time:     None
  Fr TimeOfDay:      00:00                To TimeOfDay:        24:00
  Fr TimeOfDay UTC:  04:00                To TimeOfDay UTC:    04:00
  TimeZone:          Local
IpSec Condition Summary:          NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0                SecurityClass:       0
      FragmentsOnly: No
  Condition Work Level:          0
    Group Number:      0                Cond Count:          2
    Ignore:            No
IpSec Condition Work Summary:     NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0                SecurityClass:       0
      FragmentsOnly: No
IpSec Condition Work:             NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:      192.168.20.97
      ToAddr:        192.168.20.97
    Destination Address:
    Service Condition:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Protocol:          0
Direction:        0
RouteType:        0          SecurityClass:      0
FragmentsOnly:    No
Condition Work Level: 1
Group Number:     1          Cond Count:       2
Ignore:           No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:         0
Direction:       0
RouteType:       0          SecurityClass:      0
FragmentsOnly:    No
IpSec Condition Work:        NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:        192.168.20.91
ToAddr:          192.168.20.91
Service Condition:
Protocol:         0
Direction:       0
RouteType:       0          SecurityClass:      0
FragmentsOnly:    No
Condition Work Level: 2
Group Number:     3          Cond Count:       2
Ignore:           No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:         0
Direction:       0
RouteType:       0          SecurityClass:      0
FragmentsOnly:    No
IpSec Condition Work:        NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:         TCP    (6)
SrcPortFrom:     1024          SrcPortTo:        65535
DestPortFrom:    20           DestPortTo:        20
Direction:       Bidirectional InboundConnect
RouteType:       Local        SecurityClass:      0
FragmentsOnly:    No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:   IpSec__LogYes
Version:          3          Status:           Active
Scope:           GenericFilter
ipFilterAction:   IPSec      IpFilterLogging:   Yes
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: VPN~A
Version: 3 Status: Active
Scope: DynamicVpn
Initiation: Either VpnLife: 1440
AcceptablePfs: None
AcceptablePfs: Group2
InitiateWithPfs: Group2 IpDataOfferNum: 1
PassthroughDSCP: Yes PassthroughDF: Yes
HowToEncapIKEv2: Either
IPDataOffer: 0
HowToEncap: Transport
HowToEncrypt: 3DES KeyLength: N/A
HowToAuth: ESP HowToAuthAlgr: HMAC_SHA1
RefLifeTmPropose: 480
RefLifeTmAcptMin: 480 RefLifeTmAcptMax: 480
RefLifeSzPropose: None
RefLifeSzAccept : None
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: BetweenOSAsRSA~8
Version: 3 Status: Active
Scope: LocalStart
AllowOnDemand: No LocalPortGran: Rule
RemotePortGran: Rule ProtocolGran: Rule
RemoteIpGran: Packet LocalIpGran: Packet
ICMPTypeGran: Rule ICMPCodeGran: Rule
ICMPv6TypeGran: Rule ICMPv6CodeGran: Rule
MIPv6TypeGran: Rule
LocalSecurityEndPoint:
Location:
FromAddr: 192.168.20.97
ToAddr: 192.168.20.97
Identity:
IpAddr:
FromAddr: 192.168.20.97
ToAddr: 192.168.20.97
RemoteSecurityEndPoint:
Location:
FromAddr: 192.168.20.91
ToAddr: 192.168.20.91
Identity:
IpAddr:
FromAddr: 192.168.20.91
ToAddr: 192.168.20.91
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: BetweenOSAsRSA~10
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 141 ForLoadDist: False
Priority: 41 Sequence Actions: Don't Care

```

No. Policy Action:      2                      ConditionListType: CNF
IpSecType:              policyIpFilter
policyAction:           IpSec__LogYes
  ActionType:           IpFilter GenericFilter
  Action Sequence:      0
policyAction:           VPN~A
  ActionType:           IpFilter DynamicVpn
  Action Sequence:      0
Time Periods:
  Day of Month Mask:
    First to Last:      11111111111111111111111111111111
    Last to First:      11111111111111111111111111111111
  Month of Yr Mask:     111111111111
  Day of Week Mask:     1111111  (Sunday - Saturday)
  Start Date Time:      None
  End Date Time:        None
  Fr TimeOfDay:         00:00                      To TimeOfDay:         24:00
  Fr TimeOfDay UTC:     04:00                      To TimeOfDay UTC:     04:00
  TimeZone:             Local
IpSec Condition Summary:                      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:           0
    Direction:          0
    RouteType:          0                      SecurityClass:        0
    FragmentsOnly:     No
Condition Work Level:      0
  Group Number:          0                      Cond Count:           2
  Ignore:                No
IpSec Condition Work Summary:                  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:           0
    Direction:          0
    RouteType:          0                      SecurityClass:        0
    FragmentsOnly:     No
IpSec Condition Work:                      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
    FromAddr:           192.168.20.97
    ToAddr:             192.168.20.97
  Destination Address:
  Service Condition:
    Protocol:           0
    Direction:          0
    RouteType:          0                      SecurityClass:        0
    FragmentsOnly:     No
Condition Work Level:      1
  Group Number:          1                      Cond Count:           2
  Ignore:                No
IpSec Condition Work Summary:                  NegativeIndicator: Off
IpFilterCondition:
  Source Address:

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr: 192.168.20.91
ToAddr: 192.168.20.91
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 2
Group Number: 3 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: TCP (6)
SrcPortFrom: 1024 SrcPortTo: 65535
DestPortFrom: 50000 DestPortTo: 50200
Direction: Bidirectional OutboundConnect
RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: IpSec__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: IPsec IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: VPN~A
Version: 3 Status: Active
Scope: DynamicVpn
Initiation: Either VpnLife: 1440
AcceptablePfs: None
AcceptablePfs: Group2

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

InitiateWithPfs:      Group2          IpDataOfferNum:      1
PassthroughDSCP:      Yes              PassthroughDF:       Yes
HowToEncapIKEv2:      Either
IPDataOffer:          0
  HowToEncap:          Transport
  HowToEncrypt:         3DES           KeyLength:           N/A
  HowToAuth:           ESP             HowToAuthAlgr:       HMAC_SHA1
  RefLifeTmPropose:    480
  RefLifeTmAcptMin:    480             RefLifeTmAcptMax:    480
  RefLifeSzPropose:    None
  RefLifeSzAccept :    None
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

```

```

policyRule:           BetweenOSAsRSA~12
Rule Type:            IpFilter
Version:              3              Status:                  Active
Weight:               140           ForLoadDist:             False
Priority:              40           Sequence Actions:        Don't Care
No. Policy Action:    3             ConditionListType:       CNF
IpSecType:            policyIpFilter
policyAction:          IpSec__LogYes
  ActionType:          IpFilter GenericFilter
  Action Sequence:     0
policyAction:          VPN~A
  ActionType:          IpFilter DynamicVpn
  Action Sequence:     0
policyAction:          BetweenOSAsRSA~8
  ActionType:          IpFilter LocalStart
  Action Sequence:     0
Time Periods:
  Day of Month Mask:
  First to Last:       11111111111111111111111111111111
  Last to First:       11111111111111111111111111111111
  Month of Yr Mask:    1111111111
  Day of Week Mask:    1111111 (Sunday - Saturday)
  Start Date Time:     None
  End Date Time:       None
  Fr TimeOfDay:        00:00        To TimeOfDay:           24:00
  Fr TimeOfDay UTC:    04:00        To TimeOfDay UTC:       04:00
  TimeZone:            Local
IpSec Condition Summary:           NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:          0
    Direction:         0
    RouteType:         0          SecurityClass:          0
    FragmentsOnly:     No
Condition Work Level:              0
  Group Number:          0          Cond Count:              2
  Ignore:                No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
    FromAddr:        192.168.20.97
    ToAddr:           192.168.20.97
  Destination Address:
  Service Condition:
    Protocol:         0
    Direction:        0
    RouteType:        0
    FragmentsOnly:     No
    SecurityClass:     0
Condition Work Level: 1
  Group Number:      1
  Ignore:             No
  Cond Count:         2
IpSec Condition Work Summary:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:         0
    Direction:        0
    RouteType:        0
    FragmentsOnly:     No
    SecurityClass:     0
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
    FromAddr:        192.168.20.91
    ToAddr:           192.168.20.91
  Service Condition:
    Protocol:         0
    Direction:        0
    RouteType:        0
    FragmentsOnly:     No
    SecurityClass:     0
Condition Work Level: 2
  Group Number:      3
  Ignore:             No
  Cond Count:         2
IpSec Condition Work Summary:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:         0
    Direction:        0
    RouteType:        0
    FragmentsOnly:     No
    SecurityClass:     0
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:         TCP    (6)
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

SrcPortFrom:	21	SrcPortTo:	21
DestPortFrom:	1024	DestPortTo:	65535
Direction:	Bidirectional	InboundConnect	
RouteType:	Local	SecurityClass:	0
FragmentsOnly:	No		
Policy created: Mon May 21 14:53:39 2018			
Policy updated: Mon May 21 14:53:39 2018			
IpFilter Action:	IpSec__LogYes		
Version:	3	Status:	Active
Scope:	GenericFilter		
ipFilterAction:	IPSec	IpFilterLogging:	Yes
DiscardAction:	Silent		
Policy created: Mon May 21 14:53:39 2018			
Policy updated: Mon May 21 14:53:39 2018			
IpFilter Action:	VPN~A		
Version:	3	Status:	Active
Scope:	DynamicVpn		
Initiation:	Either	VpnLife:	1440
AcceptablePfs:	None		
AcceptablePfs:	Group2		
InitiateWithPfs:	Group2	IpDataOfferNum:	1
PassthroughDSCP:	Yes	PassthroughDF:	Yes
HowToEncapIKEv2:	Either		
IPDataOffer:	0		
HowToEncap:	Transport		
HowToEncrypt:	3DES	KeyLength:	N/A
HowToAuth:	ESP	HowToAuthAlgr:	HMAC_SHA1
RefLifeTmPropose:	480		
RefLifeTmAcptMin:	480	RefLifeTmAcptMax:	480
RefLifeSzPropose:	None		
RefLifeSzAccept :	None		
Policy created: Mon May 21 14:53:39 2018			
Policy updated: Mon May 21 14:53:39 2018			
IpFilter Action:	BetweenOSAsRSA~8		
Version:	3	Status:	Active
Scope:	LocalStart		
AllowOnDemand:	No	LocalPortGran:	Rule
RemotePortGran:	Rule	ProtocolGran:	Rule
RemoteIpGran:	Packet	LocalIpGran:	Packet
ICMPTypeGran:	Rule	ICMPCodeGran:	Rule
ICMPv6TypeGran:	Rule	ICMPv6CodeGran:	Rule
MIPv6TypeGran:	Rule		
LocalSecurityEndPoint:			
Location:			
FromAddr:	192.168.20.97		
ToAddr:	192.168.20.97		
Identity:			
IpAddr:			
FromAddr:	192.168.20.97		
ToAddr:	192.168.20.97		
RemoteSecurityEndPoint:			
Location:			
FromAddr:	192.168.20.91		
ToAddr:	192.168.20.91		

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Identity:
 IpAddr:
 FromAddr: 192.168.20.91
 ToAddr: 192.168.20.91
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: BetweenOSAsRSA~13
 Rule Type: IpFilter
 Version: 3
 Weight: 139
 Priority: 39
 No. Policy Action: 2
 IpSecType: policyIpFilter
 policyAction: IpSec__LogYes
 ActionType: IpFilter GenericFilter
 Action Sequence: 0
 policyAction: VPN~A
 ActionType: IpFilter DynamicVpn
 Action Sequence: 0

Time Periods:
 Day of Month Mask:
 First to Last: 11111111111111111111111111111111
 Last to First: 11111111111111111111111111111111
 Month of Yr Mask: 1111111111
 Day of Week Mask: 1111111 (Sunday - Saturday)
 Start Date Time: None
 End Date Time: None
 Fr TimeOfDay: 00:00
 Fr TimeOfDay UTC: 04:00
 TimeZone: Local
 To TimeOfDay: 24:00
 To TimeOfDay UTC: 04:00

IpSec Condition Summary: NegativeIndicator: Off
 IpFilter Condition:
 Source Address:
 Destination Address:
 Service Condition:
 Protocol: 0
 Direction: 0
 RouteType: 0
 FragmentsOnly: No
 SecurityClass: 0

Condition Work Level: 0
 Group Number: 0
 Ignore: No
 Cond Count: 2

IpSec Condition Work Summary: NegativeIndicator: Off
 IpFilter Condition:
 Source Address:
 Destination Address:
 Service Condition:
 Protocol: 0
 Direction: 0
 RouteType: 0
 FragmentsOnly: No
 SecurityClass: 0

IpSec Condition Work: NegativeIndicator: Off
 IpFilter Condition:
 Source Address:
 FromAddr: 192.168.20.97
 ToAddr: 192.168.20.97

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
Condition Work Level:      1
  Group Number:    1
  Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
    SecurityClass: 0
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  FromAddr:      192.168.20.91
  ToAddr:        192.168.20.91
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
    SecurityClass: 0
Condition Work Level:      2
  Group Number:    3
  Ignore:          No
  Cond Count:      2
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
    SecurityClass: 0
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      TCP    (6)
    SrcPortFrom:   20
    SrcPortTo:     20
    DestPortFrom:  1024
    DestPortTo:    65535
    Direction:     Bidirectional
    RouteType:     Local
    FragmentsOnly: No
    OutboundConnect
    SecurityClass: 0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      IpSec__LogYes
Version:              3
Status:               Active
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Scope:                GenericFilter
ipFilterAction:        IPSec                IpFilterLogging:    Yes
DiscardAction:         Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:       VPN~A
Version:               3                    Status:            Active
Scope:                 DynamicVpn
Initiation:            Either                VpnLife:            1440
AcceptablePfs:         None
AcceptablePfs:         Group2
InitiateWithPfs:       Group2                IpDataOfferNum:     1
PassthroughDSCP:       Yes                    PassthroughDF:      Yes
HowToEncapIKEv2:       Either
IPDataOffer:           0
HowToEncap:            Transport
HowToEncrypt:          3DES                    KeyLength:           N/A
HowToAuth:             ESP                    HowToAuthAlgr:       HMAC_SHA1
RefLifeTmPropose:      480
RefLifeTmAcptMin:      480                    RefLifeTmAcptMax:    480
RefLifeSzPropose:      None
RefLifeSzAccept :      None
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:            BetweenOSAsRSA~15
Rule Type:             IpFilter
Version:               3                    Status:            Active
Weight:                138                  ForLoadDist:        False
Priority:               38                  Sequence Actions:    Don't Care
No. Policy Action:      3                    ConditionListType:   CNF
IpSecType:             policyIpFilter
policyAction:          IpSec__LogYes
ActionType:            IpFilter GenericFilter
Action Sequence:        0
policyAction:          VPN~A
ActionType:            IpFilter DynamicVpn
Action Sequence:        0
policyAction:          BetweenOSAsRSA~8
ActionType:            IpFilter LocalStart
Action Sequence:        0
Time Periods:
Day of Month Mask:
First to Last:         11111111111111111111111111111111
Last to First:         11111111111111111111111111111111
Month of Yr Mask:      111111111111
Day of Week Mask:      1111111 (Sunday - Saturday)
Start Date Time:       None
End Date Time:         None
Fr TimeOfDay:          00:00                To TimeOfDay:        24:00
Fr TimeOfDay UTC:      04:00                To TimeOfDay UTC:    04:00
TimeZone:              Local
IpSec Condition Summary:                NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
Condition Work Level:      0
  Group Number:       0
  Ignore:             No
IpSec Condition Work Summary:
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:       0
      Direction:      0
      RouteType:      0
      FragmentsOnly:  No
    SecurityClass:    0
  NegativeIndicator: Off
IpSec Condition Work:
  IpFilter Condition:
    Source Address:
      FromAddr:       192.168.20.97
      ToAddr:         192.168.20.97
    Destination Address:
    Service Condition:
      Protocol:       0
      Direction:      0
      RouteType:      0
      FragmentsOnly:  No
    SecurityClass:    0
  Condition Work Level:      1
    Group Number:       1
    Ignore:             No
  NegativeIndicator: Off
IpSec Condition Work Summary:
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:       0
      Direction:      0
      RouteType:      0
      FragmentsOnly:  No
    SecurityClass:    0
  NegativeIndicator: Off
IpSec Condition Work:
  IpFilter Condition:
    Source Address:
    Destination Address:
      FromAddr:       192.168.20.91
      ToAddr:         192.168.20.91
    Service Condition:
      Protocol:       0
      Direction:      0
      RouteType:      0
      FragmentsOnly:  No
    SecurityClass:    0
  Condition Work Level:      2
    Group Number:       3
    Ignore:             No
  NegativeIndicator: Off
IpSec Condition Work Summary:
  IpFilter Condition:
    Source Address:
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: TCP (6)
SrcPortFrom: 50000 SrcPortTo: 50200
DestPortFrom: 1024 DestPortTo: 65535
Direction: Bidirectional InboundConnect
RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: IpSec__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: IPsec IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: VPN~A
Version: 3 Status: Active
Scope: DynamicVpn
Initiation: Either VpnLife: 1440
AcceptablePfs: None
AcceptablePfs: Group2
InitiateWithPfs: Group2 IpDataOfferNum: 1
PassthroughDSCP: Yes PassthroughDF: Yes
HowToEncapIKEv2: Either
IPDataOffer: 0
HowToEncap: Transport
HowToEncrypt: 3DES KeyLength: N/A
HowToAuth: ESP HowToAuthAlgr: HMAC_SHA1
RefLifeTmPropose: 480
RefLifeTmAcptMin: 480 RefLifeTmAcptMax: 480
RefLifeSzPropose: None
RefLifeSzAccept : None
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: BetweenOSAsRSA~8
Version: 3 Status: Active
Scope: LocalStart
AllowOnDemand: No LocalPortGran: Rule
RemotePortGran: Rule ProtocolGran: Rule
RemoteIpGran: Packet LocalIpGran: Packet
ICMPTypeGran: Rule ICMPCodeGran: Rule
ICMPv6TypeGran: Rule ICMPv6CodeGran: Rule
MIPv6TypeGran: Rule

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
LocalSecurityEndPoint:
  Location:
    FromAddr:      192.168.20.97
    ToAddr:        192.168.20.97
  Identity:
    IpAddr:
      FromAddr:    192.168.20.97
      ToAddr:      192.168.20.97
RemoteSecurityEndPoint:
  Location:
    FromAddr:      192.168.20.91
    ToAddr:        192.168.20.91
  Identity:
    IpAddr:
      FromAddr:    192.168.20.91
      ToAddr:      192.168.20.91
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:      TrafficBetweenVIPAs~3
  Rule Type:      IpFilter
  Version:        3
  Weight:         137
  Priority:        37
  No. Policy Action: 1
  IpSecType:      policyIpFilter
  policyAction:    Permit__LogYes
  ActionType:     IpFilter GenericFilter
  Action Sequence: 0
  Time Periods:
    Day of Month Mask:
      First to Last: 11111111111111111111111111111111
      Last to First: 11111111111111111111111111111111
    Month of Yr Mask: 111111111111
    Day of Week Mask: 1111111 (Sunday - Saturday)
    Start Date Time:  None
    End Date Time:    None
    Fr TimeOfDay:     00:00
    To TimeOfDay:     24:00
    Fr TimeOfDay UTC: 04:00
    To TimeOfDay UTC: 04:00
    TimeZone:         Local
  IpSec Condition Summary:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol: 0
      Direction: 0
      RouteType: 0
      FragmentsOnly: No
      SecurityClass: 0
  Condition Work Level: 0
    Group Number: 0
    Ignore: No
    Cond Count: 2
  IpSec Condition Work Summary:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Protocol:          0
Direction:        0
RouteType:        0
FragmentsOnly:    No
SecurityClass:     0
IpSec Condition Work:
IpFilter Condition:
Source Address:
FromAddr:         192.168.20.107
ToAddr:           192.168.20.107
Destination Address:
Service Condition:
Protocol:         0
Direction:       0
RouteType:       0
FragmentsOnly:   No
SecurityClass:    0
Condition Work Level: 1
Group Number:    1
Cond Count:      2
Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:   No
SecurityClass:    0
NegativeIndicator: Off
IpSec Condition Work:
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:        192.168.20.101
ToAddr:          192.168.20.101
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:   No
SecurityClass:    0
Condition Work Level: 2
Group Number:    3
Cond Count:      2
Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:   No
SecurityClass:    0
NegativeIndicator: Off
IpSec Condition Work:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        TCP   (6)
SrcPortFrom:     3000
SrcPortTo:       3000
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

DestPortFrom: 1024 DestPortTo: 65535
Direction: Bidirectional InboundConnect
RouteType: Local SecurityClass: 0
FragmentsOnly: No

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: TrafficBetweenVIPAs~4
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 136 ForLoadDist: False
Priority: 36 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpSec Condition Work:                               NegativeIndicator: Off
IpFilter Condition:
  Source Address:
    FromAddr:      192.168.20.107
    ToAddr:        192.168.20.107
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
  Condition Work Level: 1
    Group Number: 1
    Ignore:       No
    Cond Count:   2
IpSec Condition Work Summary:                       NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
IpSec Condition Work:                               NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
    FromAddr:      192.168.20.101
    ToAddr:        192.168.20.101
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
  Condition Work Level: 2
    Group Number: 3
    Ignore:       No
    Cond Count:   2
IpSec Condition Work Summary:                       NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
IpSec Condition Work:                               NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      TCP (6)
    SrcPortFrom:   1024
    SrcPortTo:     65535
    DestPortFrom:  21
    DestPortTo:    21
    Direction:     Bidirectional
    RouteType:     Local
    OutboundConnect
    SecurityClass: 0
    FragmentsOnly: No
  
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: TrafficBetweenVIPAs~5
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 135 ForLoadDist: False
Priority: 35 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: 192.168.20.107

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ToAddr: 192.168.20.107
Destination Address:
Service Condition:
  Protocol: 0
  Direction: 0
  RouteType: 0
  FragmentsOnly: No
  SecurityClass: 0
Condition Work Level: 1
  Group Number: 1
  Ignore: No
  Cond Count: 2
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol: 0
    Direction: 0
    RouteType: 0
    FragmentsOnly: No
    SecurityClass: 0
  NegativeIndicator: Off
IpSec Condition Work:
  IpFilter Condition:
    Source Address:
    Destination Address:
    FromAddr: 192.168.20.101
    ToAddr: 192.168.20.101
    Service Condition:
      Protocol: 0
      Direction: 0
      RouteType: 0
      FragmentsOnly: No
      SecurityClass: 0
    Condition Work Level: 2
      Group Number: 3
      Ignore: No
      Cond Count: 2
    IpSec Condition Work Summary: NegativeIndicator: Off
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol: 0
        Direction: 0
        RouteType: 0
        FragmentsOnly: No
        SecurityClass: 0
      NegativeIndicator: Off
    IpSec Condition Work:
      IpFilter Condition:
        Source Address:
        Destination Address:
        Service Condition:
          Protocol: TCP (6)
          SrcPortFrom: 1024
          SrcPortTo: 65535
          DestPortFrom: 20
          DestPortTo: 20
          Direction: Bidirectional
          InboundConnect
          RouteType: Local
          SecurityClass: 0
          FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Version:          3                      Status:          Active
Scope:           GenericFilter
ipFilterAction:   Permit                  IpFilterLogging:   Yes
DiscardAction:    Silent
Policy created:   Mon May 21 14:53:39 2018
Policy updated:   Mon May 21 14:53:39 2018

policyRule:       TrafficBetweenVIPAs~6
Rule Type:        IpFilter
Version:          3                      Status:          Active
Weight:           134                    ForLoadDist:      False
Priority:          34                    Sequence Actions:  Don't Care
No. Policy Action: 1                      ConditionListType: CNF
IpSecType:        policyIpFilter
policyAction:     Permit__LogYes
ActionType:       IpFilter GenericFilter
Action Sequence:   0
Time Periods:
Day of Month Mask:
First to Last:    11111111111111111111111111111111
Last to First:    11111111111111111111111111111111
Month of Yr Mask:  11111111111
Day of Week Mask:  1111111 (Sunday - Saturday)
Start Date Time:   None
End Date Time:     None
Fr TimeOfDay:      00:00                  To TimeOfDay:      24:00
Fr TimeOfDay UTC:  04:00                  To TimeOfDay UTC:  04:00
TimeZone:          Local
IpSec Condition Summary:                   NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:     No
Condition Work Level: 0
Group Number:      0                      Cond Count:         2
Ignore:            No
IpSec Condition Work Summary:               NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:     No
IpSec Condition Work:                       NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr:          192.168.20.107
ToAddr:            192.168.20.107
Destination Address:
Service Condition:
Protocol:          0
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Direction:          0
RouteType:          0          SecurityClass:      0
FragmentsOnly:      No
Condition Work Level: 1
Group Number:       1          Cond Count:        2
Ignore:             No
IpSec Condition Work Summary:  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0          SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:           192.168.20.101
ToAddr:             192.168.20.101
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0          SecurityClass:      0
FragmentsOnly:      No
Condition Work Level: 2
Group Number:       3          Cond Count:        2
Ignore:             No
IpSec Condition Work Summary:  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0          SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           TCP    (6)
SrcPortFrom:        1024          SrcPortTo:          65535
DestPortFrom:        50000        DestPortTo:          50200
Direction:          Bidirectional OutboundConnect
RouteType:          Local          SecurityClass:      0
FragmentsOnly:      No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:     Permit__LogYes
Version:             3          Status:             Active
Scope:              GenericFilter
ipFilterAction:      Permit      IpFilterLogging:    Yes
DiscardAction:       Silent
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

```
policyRule: TrafficBetweenVIPAs~7
Rule Type:  IpFilter
Version:    3                               Status:    Active
Weight:     133                             ForLoadDist: False
Priority:    33                             Sequence Actions: Don't Care
No. Policy Action: 1                       ConditionListType: CNF
IpSecType:  policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00                      To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00                  To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0                      SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0                      Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0                      SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: 192.168.20.107
ToAddr: 192.168.20.107
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0                      SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 1
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Group Number:      1                      Cond Count:      2
Ignore:            No
IpSec Condition Work Summary:              NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:    No
IpSec Condition Work:                      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:          192.168.20.101
ToAddr:            192.168.20.101
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:    No
Condition Work Level:      2
Group Number:          3                      Cond Count:      2
Ignore:                No
IpSec Condition Work Summary:              NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:    No
IpSec Condition Work:                      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          TCP   (6)
SrcPortFrom:      21                      SrcPortTo:          21
DestPortFrom:     1024                    DestPortTo:         65535
Direction:        Bidirectional           InboundConnect
RouteType:        Local                    SecurityClass:      0
FragmentsOnly:    No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3                      Status:              Active
Scope:                GenericFilter
ipFilterAction:        Permit                IpFilterLogging:     Yes
DiscardAction:         Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:           TrafficBetweenVIPAs~8
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Rule Type:                IpFilter
Version:                  3
Weight:                   132
Priority:                  32
No. Policy Action:        1
IpSecType:                policyIpFilter
policyAction:             Permit__LogYes
  ActionType:             IpFilter GenericFilter
  Action Sequence:        0
Time Periods:
  Day of Month Mask:
    First to Last:        11111111111111111111111111111111
    Last to First:        11111111111111111111111111111111
  Month of Yr Mask:        111111111111
  Day of Week Mask:        1111111 (Sunday - Saturday)
  Start Date Time:        None
  End Date Time:          None
  Fr TimeOfDay:           00:00
  To TimeOfDay:           24:00
  Fr TimeOfDay UTC:       04:00
  To TimeOfDay UTC:       04:00
  TimeZone:               Local
IpSec Condition Summary:  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:            0
      Direction:           0
      RouteType:           0
      FragmentsOnly:       No
      SecurityClass:       0
    Condition Work Level:  0
      Group Number:        0
      Ignore:              No
      Cond Count:          2
IpSec Condition Work Summary: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:            0
      Direction:           0
      RouteType:           0
      FragmentsOnly:       No
      SecurityClass:       0
    Condition Work Level:  0
      Group Number:        0
      Ignore:              No
      Cond Count:          2
IpSec Condition Work:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:            192.168.20.107
      ToAddr:              192.168.20.107
    Destination Address:
    Service Condition:
      Protocol:            0
      Direction:           0
      RouteType:           0
      FragmentsOnly:       No
      SecurityClass:       0
    Condition Work Level:  1
      Group Number:        1
      Ignore:              No
      Cond Count:          2
IpSec Condition Work Summary: NegativeIndicator: Off
  IpFilter Condition:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Source Address:
Destination Address:
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
  SecurityClass:      0
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  FromAddr:          192.168.20.101
  ToAddr:             192.168.20.101
  Service Condition:
    Protocol:         0
    Direction:        0
    RouteType:        0
    FragmentsOnly:     No
    SecurityClass:     0
  Condition Work Level: 2
  Group Number:       3
  Ignore:             No
  Cond Count:         2
IpSec Condition Work Summary:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:         0
    Direction:        0
    RouteType:        0
    FragmentsOnly:     No
    SecurityClass:     0
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:         TCP   (6)
    SrcPortFrom:       20
    SrcPortTo:         20
    DestPortFrom:      1024
    DestPortTo:        65535
    Direction:         Bidirectional
    OutboundConnect:
    RouteType:         Local
    SecurityClass:     0
    FragmentsOnly:     No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3
Status:               Active
Scope:               GenericFilter
ipFilterAction:       Permit
IpFilterLogging:      Yes
DiscardAction:        Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:           TrafficBetweenVIPAs~9
Rule Type:            IpFilter
Version:              3
Status:               Active
Weight:               131
ForLoadDist:          False
Priority:              31
Sequence Actions:     Don't Care
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

No. Policy Action:      1                      ConditionListType: CNF
IpSecType:              policyIpFilter
policyAction:           Permit__LogYes
  ActionType:           IpFilter GenericFilter
  Action Sequence:      0
Time Periods:
  Day of Month Mask:
  First to Last:        11111111111111111111111111111111
  Last to First:        11111111111111111111111111111111
  Month of Yr Mask:      111111111111
  Day of Week Mask:      1111111  (Sunday - Saturday)
  Start Date Time:      None
  End Date Time:         None
  Fr TimeOfDay:          00:00          To TimeOfDay:          24:00
  Fr TimeOfDay UTC:      04:00          To TimeOfDay UTC:      04:00
  TimeZone:              Local
IpSec Condition Summary:                      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
      FragmentsOnly:     No
Condition Work Level:      0
  Group Number:          0          Cond Count:          2
  Ignore:                No
IpSec Condition Work Summary:                  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
      FragmentsOnly:     No
IpSec Condition Work:                          NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:          192.168.20.107
      ToAddr:            192.168.20.107
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
      FragmentsOnly:     No
Condition Work Level:      1
  Group Number:          1          Cond Count:          2
  Ignore:                No
IpSec Condition Work Summary:                  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Direction:          0
RouteType:          0          SecurityClass:      0
FragmentsOnly:     No
IpSec Condition Work:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:          192.168.20.101
ToAddr:            192.168.20.101
Service Condition:
Protocol:          0
Direction:        0
RouteType:        0          SecurityClass:      0
FragmentsOnly:     No
Condition Work Level:      2
Group Number:      3          Cond Count:      2
Ignore:            No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:        0
RouteType:        0          SecurityClass:      0
FragmentsOnly:     No
IpSec Condition Work:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          TCP   (6)
SrcPortFrom:      50000      SrcPortTo:      50200
DestPortFrom:     1024      DestPortTo:     65535
Direction:        Bidirectional  InboundConnect
RouteType:        Local      SecurityClass:      0
FragmentsOnly:     No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3          Status:              Active
Scope:                GenericFilter
ipFilterAction:        Permit      IpFilterLogging:      Yes
DiscardAction:         Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:           TrafOSA2DVIPAPresh~6
Rule Type:            IpFilter
Version:              3          Status:              Active
Weight:               130        ForLoadDist:         False
Priority:              30        Sequence Actions:    Don't Care
No. Policy Action:    1          ConditionListType:   CNF
IpSecType:            policyIpFilter
policyAction:          Permit__LogYes
ActionType:            IpFilter GenericFilter
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: 192.168.20.97
ToAddr: 192.168.20.97
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 1
Group Number: 1 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilter Condition:
Source Address:
Destination Address:
  FromAddr:      192.168.20.121
  ToAddr:        192.168.20.121
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
  SecurityClass: 0
Condition Work Level: 2
  Group Number: 3
  Ignore:       No
  Cond Count:   2
IpSec Condition Work Summary:
  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
  SecurityClass: 0
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      UDP (17)
  SrcPortFrom:   500
  DestPortFrom:  500
  SrcPortTo:     500
  DestPortTo:    500
  Direction:     Bidirectional
  RouteType:     Local
  FragmentsOnly: No
  SecurityClass: 0
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

IpFilter Action:      Permit__LogYes
Version:              3
Scope:                GenericFilter
ipFilterAction:       Permit
DiscardAction:        Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018
Status:               Active
IpFilterLogging:      Yes

policyRule:           TrafOSA2DVIPAPresh~8
Rule Type:            IpFilter
Version:              3
Weight:               129
Priority:              29
No. Policy Action:    3
IpSecType:            policyIpFilter
policyAction:         IpSec__LogYes
ActionType:           IpFilter GenericFilter
Action Sequence:      0
policyAction:         VPN~A~6
ActionType:           IpFilter DynamicVpn
Action Sequence:      0
Status:               Active
ForLoadDist:          False
Sequence Actions:     Don't Care
ConditionListType:    CNF
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
policyAction:      TrafOSA2DVIPAPresh~7
  ActionType:      IpFilter LocalStart
  Action Sequence:  0
Time Periods:
  Day of Month Mask:
  First to Last:    11111111111111111111111111111111
  Last to First:    11111111111111111111111111111111
  Month of Yr Mask:  111111111111
  Day of Week Mask:  1111111  (Sunday - Saturday)
  Start Date Time:   None
  End Date Time:      None
  Fr TimeOfDay:       00:00          To TimeOfDay:      24:00
  Fr TimeOfDay UTC:   04:00          To TimeOfDay UTC:   04:00
  TimeZone:           Local
IpSec Condition Summary:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0          SecurityClass:      0
      FragmentsOnly: No
  Condition Work Level:      0
    Group Number:      0          Cond Count:      2
    Ignore:            No
IpSec Condition Work Summary:  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0          SecurityClass:      0
      FragmentsOnly: No
IpSec Condition Work:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:      192.168.20.127
      ToAddr:        192.168.20.127
    Destination Address:
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0          SecurityClass:      0
      FragmentsOnly: No
  Condition Work Level:      1
    Group Number:      1          Cond Count:      2
    Ignore:            No
IpSec Condition Work Summary:  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0          SecurityClass:      0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    FragmentsOnly:      No
IpSec Condition Work:                                     NegativeIndicator: Off
IpFilter Condition:
    Source Address:
    Destination Address:
        FromAddr:      192.168.20.121
        ToAddr:        192.168.20.121
    Service Condition:
        Protocol:       0
        Direction:      0
        RouteType:      0
        FragmentsOnly:  No
    SecurityClass:      0
Condition Work Level:      2
    Group Number:         3
    Ignore:               No
    Cond Count:           2
IpSec Condition Work Summary:
IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
        Protocol:       0
        Direction:      0
        RouteType:      0
        FragmentsOnly:  No
    SecurityClass:      0
IpSec Condition Work:                                     NegativeIndicator: Off
IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
        Protocol:       All
        Direction:      Bidirectional
        RouteType:      Local
        FragmentsOnly:  No
    SecurityClass:      0
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

IpFilter Action:      IpSec__LogYes
Version:              3
Scope:                GenericFilter
ipFilterAction:       IPSec
DiscardAction:        Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018
IpFilterLogging:      Yes

IpFilter Action:      VPN~A~6
Version:              3
Scope:                DynamicVpn
Initiation:           Either
VpnLife:              1440
AcceptablePfs:        None
AcceptablePfs:        Group2
InitiateWithPfs:      Group2
IpDataOfferNum:       1
PassthroughDSCP:      Yes
PassthroughDF:        Yes
HowToEncapIKEv2:      Either
IPDataOffer:          0
HowToEncap:           Tunnel
HowToEncrypt:          3DES
KeyLength:             N/A
HowToAuth:            ESP
HowToAuthAlgr:        HMAC_SHA1

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

RefLifeTmPropose: 480
RefLifeTmAcptMin: 480 RefLifeTmAcptMax: 480
RefLifeSzPropose: None
RefLifeSzAccept : None
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

IpFilter Action: TrafOSA2DVIPAPresh~7
Version: 3 Status: Active
Scope: LocalStart
AllowOnDemand: Yes LocalPortGran: Rule
RemotePortGran: Rule ProtocolGran: Rule
RemoteIpGran: Packet LocalIpGran: Packet
ICMPTypeGran: Rule ICMPCodeGran: Rule
ICMPv6TypeGran: Rule ICMPv6CodeGran: Rule
MIPv6TypeGran: Rule
LocalSecurityEndPoint:
Location:
FromAddr: 192.168.20.97
ToAddr: 192.168.20.97
Identity:
Fqdn:
WSC.LABS.IBM.COM
RemoteSecurityEndPoint:
Location:
FromAddr: 192.168.20.121
ToAddr: 192.168.20.121
Identity:
UserAtFqdn:
ZOS1@WSC.LABS.IBM.COM
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

policyRule: WStoVIP~2
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 128 ForLoadDist: False
Priority: 28 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
Condition Work Level:      0
  Group Number:    0
  Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
  SecurityClass:      0
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  FromAddr:        192.168.20.107
  ToAddr:          192.168.20.107
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
  SecurityClass:      0
Condition Work Level:      1
  Group Number:    1
  Ignore:          No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
  SecurityClass:      0
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  FromAddr:        All4
  ToAddr:          All4
  Service Condition:
    Protocol:      0
    Direction:    0
    RouteType:    0
    FragmentsOnly: No
  SecurityClass:      0
Condition Work Level:      2
  Group Number:    3
  Ignore:          No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: TCP (6)
SrcPortFrom: 21 SrcPortTo: 21
DestPortFrom: 1024 DestPortTo: 65535
Direction: Bidirectional InboundConnect
RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: WStoVIPA~3
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 127 ForLoadDist: False
Priority: 27 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

RouteType: 0	SecurityClass: 0
FragmentsOnly: No	
Condition Work Level: 0	
Group Number: 0	Cond Count: 2
Ignore: No	
IpSec Condition Work Summary:	NegativeIndicator: Off
IpFilter Condition:	
Source Address:	
Destination Address:	
Service Condition:	
Protocol: 0	
Direction: 0	
RouteType: 0	SecurityClass: 0
FragmentsOnly: No	
IpSec Condition Work:	NegativeIndicator: Off
IpFilter Condition:	
Source Address:	
FromAddr: 192.168.20.107	
ToAddr: 192.168.20.107	
Destination Address:	
Service Condition:	
Protocol: 0	
Direction: 0	
RouteType: 0	SecurityClass: 0
FragmentsOnly: No	
Condition Work Level: 1	
Group Number: 1	Cond Count: 2
Ignore: No	
IpSec Condition Work Summary:	NegativeIndicator: Off
IpFilter Condition:	
Source Address:	
Destination Address:	
Service Condition:	
Protocol: 0	
Direction: 0	
RouteType: 0	SecurityClass: 0
FragmentsOnly: No	
IpSec Condition Work:	NegativeIndicator: Off
IpFilter Condition:	
Source Address:	
Destination Address:	
FromAddr: All4	
ToAddr: All4	
Service Condition:	
Protocol: 0	
Direction: 0	
RouteType: 0	SecurityClass: 0
FragmentsOnly: No	
Condition Work Level: 2	
Group Number: 3	Cond Count: 2
Ignore: No	
IpSec Condition Work Summary:	NegativeIndicator: Off
IpFilter Condition:	
Source Address:	
Destination Address:	
Service Condition:	
Protocol: 0	

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Direction:          0
RouteType:          0          SecurityClass:          0
FragmentsOnly:     No
IpSec Condition Work:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          TCP    (6)
SrcPortFrom:      20          SrcPortTo:          20
DestPortFrom:     1024       DestPortTo:          65535
Direction:        Bidirectional  OutboundConnect
RouteType:         Local        SecurityClass:          0
FragmentsOnly:     No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:     Permit__LogYes
Version:             3          Status:          Active
Scope:               GenericFilter
ipFilterAction:      Permit      IpFilterLogging:  Yes
DiscardAction:       Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:          WStoVIPA~4
Rule Type:           IpFilter
Version:             3          Status:          Active
Weight:              126       ForLoadDist:      False
Priority:             26       Sequence Actions: Don't Care
No. Policy Action:   1          ConditionListType: CNF
IpSecType:           policyIpFilter
policyAction:         Permit__LogYes
ActionType:          IpFilter GenericFilter
Action Sequence:     0
Time Periods:
Day of Month Mask:
First to Last:       11111111111111111111111111111111
Last to First:       11111111111111111111111111111111
Month of Yr Mask:    1111111111
Day of Week Mask:    1111111  (Sunday - Saturday)
Start Date Time:     None
End Date Time:       None
Fr TimeOfDay:        00:00      To TimeOfDay:      24:00
Fr TimeOfDay UTC:    04:00      To TimeOfDay UTC:  04:00
TimeZone:            Local
IpSec Condition Summary:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:            0
Direction:           0
RouteType:           0          SecurityClass:          0
FragmentsOnly:       No
Condition Work Level: 0
Group Number:        0          Cond Count:          2
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: 192.168.20.107
ToAddr: 192.168.20.107
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 1
Group Number: 1 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr: All4
ToAddr: All4
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 2
Group Number: 3 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: TCP (6)
SrcPortFrom: 50000 SrcPortTo: 50200
DestPortFrom: 1024 DestPortTo: 65535
Direction: Bidirectional InboundConnect
RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: WStoVIPA~5
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 125 ForLoadDist: False
Priority: 25 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
  Source Address:
    FromAddr:    192.168.20.107
    ToAddr:      192.168.20.107
  Destination Address:
  Service Condition:
    Protocol:    0
    Direction:  0
    RouteType:  0
    FragmentsOnly: No
Condition Work Level:      1
  Group Number:    1
  Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:    0
    Direction:  0
    RouteType:  0
    FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
  Source Address:
  Destination Address:
    FromAddr:    All4
    ToAddr:      All4
  Service Condition:
    Protocol:    0
    Direction:  0
    RouteType:  0
    FragmentsOnly: No
Condition Work Level:      2
  Group Number:    3
  Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:    0
    Direction:  0
    RouteType:  0
    FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
```

SecurityClass: 0

NegativeIndicator: Off

SecurityClass: 0

Cond Count: 2

NegativeIndicator: Off

SecurityClass: 0

NegativeIndicator: Off

SecurityClass: 0

Cond Count: 2

NegativeIndicator: Off

SecurityClass: 0

NegativeIndicator: Off

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Protocol: TCP (6)
SrcPortFrom: 23 SrcPortTo: 23
DestPortFrom: 1024 DestPortTo: 65535
Direction: Bidirectional InboundConnect
RouteType: Local SecurityClass: 0
FragmentsOnly: No

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~1
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 124 ForLoadDist: False
Priority: 24 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
IpSec Condition Work:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
FromAddr:	All4		
ToAddr:	All4		
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
Condition Work Level:	1		
Group Number:	1	Cond Count:	2
Ignore:	No		
IpSec Condition Work Summary:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
IpSec Condition Work:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
FromAddr:	All4		
ToAddr:	All4		
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
Condition Work Level:	2		
Group Number:	3	Cond Count:	2
Ignore:	No		
IpSec Condition Work Summary:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
IpSec Condition Work:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
Service Condition:			
Protocol:	UDP (17)		
SrcPortFrom:	53	SrcPortTo:	53
DestPortFrom:	1024	DestPortTo:	65535
Direction:	Bidirectional		

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~2
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 123 ForLoadDist: False
Priority: 23 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Source Address:
  FromAddr:      All4
  ToAddr:        All4
Destination Address:
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
  SecurityClass: 0
Condition Work Level: 1
  Group Number: 1
  Ignore:       No
  Cond Count:   2
IpSec Condition Work Summary:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
  NegativeIndicator: Off
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
    FromAddr:      All4
    ToAddr:        All4
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
  Condition Work Level: 2
    Group Number: 3
    Ignore:       No
    Cond Count:   2
IpSec Condition Work Summary:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      0
    Direction:     0
    RouteType:     0
    FragmentsOnly: No
    SecurityClass: 0
  NegativeIndicator: Off
IpSec Condition Work:
  NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:      UDP (17)
    SrcPortFrom:   53
    SrcPortTo:     53
    DestPortFrom:  53
    DestPortTo:    53
    Direction:     Bidirectional
    RouteType:     Local
    FragmentsOnly: No
    SecurityClass: 0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~3
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 122 ForLoadDist: False
Priority: 22 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: All4
ToAddr: All4
Destination Address:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
  SecurityClass:     0
Condition Work Level: 1
  Group Number:      1
  Cond Count:        2
  Ignore:            No
  NegativeIndicator: Off
IpSec Condition Work Summary:
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:       0
      Direction:      0
      RouteType:      0
      FragmentsOnly:  No
      SecurityClass:  0
      NegativeIndicator: Off
  IpSec Condition Work:
    IpFilter Condition:
      Source Address:
      Destination Address:
        FromAddr:      All4
        ToAddr:        All4
      Service Condition:
        Protocol:       0
        Direction:      0
        RouteType:      0
        FragmentsOnly:  No
        SecurityClass:  0
    Condition Work Level: 2
      Group Number:      3
      Cond Count:        2
      Ignore:            No
      NegativeIndicator: Off
    IpSec Condition Work Summary:
      IpFilter Condition:
        Source Address:
        Destination Address:
        Service Condition:
          Protocol:       0
          Direction:      0
          RouteType:      0
          FragmentsOnly:  No
          SecurityClass:  0
          NegativeIndicator: Off
      IpSec Condition Work:
        IpFilter Condition:
          Source Address:
          Destination Address:
          Service Condition:
            Protocol:      TCP    (6)
            SrcPortFrom:   53
            SrcPortTo:     53
            DestPortFrom:  1024
            DestPortTo:    65535
            Direction:     Bidirectional
            RouteType:     Local
            FragmentsOnly: No
            SecurityClass: 0
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3
Scope:                GenericFilter
Status:               Active
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~4
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 121 ForLoadDist: False
Priority: 21 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: All4
ToAddr: All4
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FragmentsOnly:      No
Condition Work Level:      1
Group Number:      1      Cond Count:      2
Ignore:      No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:      0
Direction:      0
RouteType:      0      SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:      All4
ToAddr:      All4
Service Condition:
Protocol:      0
Direction:      0
RouteType:      0      SecurityClass:      0
FragmentsOnly:      No
Condition Work Level:      2
Group Number:      3      Cond Count:      2
Ignore:      No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:      0
Direction:      0
RouteType:      0      SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:      TCP      (6)
SrcPortFrom:      53      SrcPortTo:      53
DestPortFrom:      53      DestPortTo:      53
Direction:      Bidirectional
RouteType:      Local      SecurityClass:      0
FragmentsOnly:      No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:      3      Status:      Active
Scope:      GenericFilter
ipFilterAction:      Permit      IpFilterLogging:      Yes
DiscardAction:      Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

policyRule:                CommonTraffic~5
  Rule Type:                IpFilter
  Version:                  3
  Weight:                   120
  Priority:                  20
  No. Policy Action:        1
  IpSecType:                policyIpFilter
  policyAction:              Permit__LogYes
  ActionType:                IpFilter GenericFilter
  Action Sequence:          0
  Time Periods:
    Day of Month Mask:
      First to Last:        11111111111111111111111111111111
      Last to First:        11111111111111111111111111111111
    Month of Yr Mask:        111111111111
    Day of Week Mask:        1111111 (Sunday - Saturday)
    Start Date Time:         None
    End Date Time:           None
    Fr TimeOfDay:            00:00
    To TimeOfDay:            24:00
    Fr TimeOfDay UTC:        04:00
    To TimeOfDay UTC:        04:00
    TimeZone:                Local
  IpSec Condition Summary:   NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:              0
      Direction:             0
      RouteType:             0
      FragmentsOnly:         No
    SecurityClass:           0
  Condition Work Level:      0
    Group Number:            0
    Ignore:                  No
    Cond Count:              2
  IpSec Condition Work Summary: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:              0
      Direction:             0
      RouteType:             0
      FragmentsOnly:         No
    SecurityClass:           0
  IpSec Condition Work:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:              All4
      ToAddr:                All4
    Destination Address:
    Service Condition:
      Protocol:              0
      Direction:             0
      RouteType:             0
      FragmentsOnly:         No
    SecurityClass:           0
  Condition Work Level:      1
    Group Number:            1
    Ignore:                  No
    Cond Count:              2

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

IpSec Condition Work Summary:           NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0
FragmentsOnly:      No
SecurityClass:      0
IpSec Condition Work:           NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:           All4
ToAddr:              All4
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0
FragmentsOnly:      No
SecurityClass:      0
Condition Work Level:           2
Group Number:        3
Ignore:              No
Cond Count:          2
IpSec Condition Work Summary:           NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0
FragmentsOnly:      No
SecurityClass:      0
IpSec Condition Work:           NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           ICMP (1)
TypeFrom:           11
Code:               Any
Direction:          Bidirectional
RouteType:          Local
FragmentsOnly:      No
TypeTo:              11
SecurityClass:      0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:           Permit__LogYes
Version:                   3
Scope:                     GenericFilter
Status:                    Active
ipFilterAction:            Permit
IpFilterLogging:           Yes
DiscardAction:             Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:                CommonTraffic~6
Rule Type:                 IpFilter
Version:                   3
Status:                    Active

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Weight: 119 ForLoadDist: False
Priority: 19 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
  ActionType: IpFilter GenericFilter
  Action Sequence: 0
Time Periods:
  Day of Month Mask:
  First to Last: 11111111111111111111111111111111
  Last to First: 11111111111111111111111111111111
  Month of Yr Mask: 111111111111
  Day of Week Mask: 111111 (Sunday - Saturday)
  Start Date Time: None
  End Date Time: None
  Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
  Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
  TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol: 0
      Direction: 0
      RouteType: 0 SecurityClass: 0
      FragmentsOnly: No
    Condition Work Level: 0
    Group Number: 0 Cond Count: 2
    Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol: 0
      Direction: 0
      RouteType: 0 SecurityClass: 0
      FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr: All4
      ToAddr: All4
    Destination Address:
    Service Condition:
      Protocol: 0
      Direction: 0
      RouteType: 0 SecurityClass: 0
      FragmentsOnly: No
    Condition Work Level: 1
    Group Number: 1 Cond Count: 2
    Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
  SecurityClass:      0
IpSec Condition Work:
  NegativeIndicator:  Off
  IpFilter Condition:
    Source Address:
    Destination Address:
      FromAddr:       All4
      ToAddr:         All4
    Service Condition:
      Protocol:        0
      Direction:       0
      RouteType:       0
      FragmentsOnly:   No
      SecurityClass:    0
    Condition Work Level: 2
      Group Number:    3
      Ignore:          No
      Cond Count:      2
    IpSec Condition Work Summary:
      NegativeIndicator: Off
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:      0
        Direction:     0
        RouteType:     0
        FragmentsOnly: No
        SecurityClass:  0
    IpSec Condition Work:
      NegativeIndicator: Off
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:      ICMP (1)
        TypeFrom:       3
        Code:           Any
        Direction:      Bidirectional
        RouteType:      Local
        FragmentsOnly:  No
        TypeTo:         3
        SecurityClass:  0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
  Version:            3
  Scope:              GenericFilter
  Status:              Active
  ipFilterAction:     Permit
  IpFilterLogging:     Yes
  DiscardAction:      Silent
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018

policyRule:           CommonTraffic~7
  Rule Type:          IpFilter
  Version:            3
  Weight:             118
  Priority:            18
  Status:              Active
  No. Policy Action:   1
  ForLoadDist:         False
  Sequence Actions:    Don't Care
  ConditionListType:   CNF
  IpSecType:          policyIpFilter
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
policyAction:          Permit__LogYes
  ActionType:          IpFilter GenericFilter
  Action Sequence:      0
Time Periods:
  Day of Month Mask:
  First to Last:        11111111111111111111111111111111
  Last to First:        11111111111111111111111111111111
  Month of Yr Mask:      111111111111
  Day of Week Mask:      1111111  (Sunday - Saturday)
  Start Date Time:       None
  End Date Time:          None
  Fr TimeOfDay:          00:00          To TimeOfDay:          24:00
  Fr TimeOfDay UTC:      04:00          To TimeOfDay UTC:      04:00
  TimeZone:              Local
IpSec Condition Summary:          NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
      FragmentsOnly:     No
  Condition Work Level:          0
    Group Number:         0          Cond Count:          2
    Ignore:               No
IpSec Condition Work Summary:     NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
      FragmentsOnly:     No
IpSec Condition Work:             NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:          All4
      ToAddr:            All4
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
      FragmentsOnly:     No
  Condition Work Level:          1
    Group Number:         1          Cond Count:          2
    Ignore:               No
IpSec Condition Work Summary:     NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0          SecurityClass:          0
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    FragmentsOnly:      No
IpSec Condition Work:                                     NegativeIndicator: Off
IpFilter Condition:
    Source Address:
    Destination Address:
        FromAddr:      All4
        ToAddr:        All4
    Service Condition:
        Protocol:       0
        Direction:      0
        RouteType:      0
        FragmentsOnly:  No
                                SecurityClass:      0
Condition Work Level:      2
    Group Number:          3
    Ignore:                No
                                Cond Count:          2
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
        Protocol:       0
        Direction:      0
        RouteType:      0
        FragmentsOnly:  No
                                SecurityClass:      0
IpSec Condition Work:                                     NegativeIndicator: Off
IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
        Protocol:       OSPF (89)
        Type:           Any
        Direction:      Bidirectional
        RouteType:      Local
        FragmentsOnly:  No
                                SecurityClass:      0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
    Version:           3
                                Status:              Active
    Scope:             GenericFilter
    ipFilterAction:    Permit
                                IpFilterLogging:      Yes
    DiscardAction:     Silent
    Policy created:    Mon May 21 14:53:39 2018
    Policy updated:    Mon May 21 14:53:39 2018

policyRule:           CommonTraffic~8
    Rule Type:         IpFilter
    Version:           3
                                Status:              Active
    Weight:            117
                                ForLoadDist:         False
    Priority:          17
                                Sequence Actions:     Don't Care
    No. Policy Action: 1
                                ConditionListType:    CNF
    IpSecType:         policyIpFilter
    policyAction:       Permit__LogYes
    ActionType:        IpFilter GenericFilter
    Action Sequence:    0
    Time Periods:
    Day of Month Mask:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

First to Last:      11111111111111111111111111111111
Last to First:     11111111111111111111111111111111
Month of Yr Mask:   111111111111
Day of Week Mask:   1111111   (Sunday - Saturday)
Start Date Time:    None
End Date Time:      None
Fr TimeOfDay:       00:00           To TimeOfDay:       24:00
Fr TimeOfDay UTC:   04:00           To TimeOfDay UTC:   04:00
TimeZone:          Local
IpSec Condition Summary:           NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:        0
    Direction:       0
    RouteType:       0           SecurityClass:        0
    FragmentsOnly:   No
Condition Work Level:      0
  Group Number:        0           Cond Count:        2
  Ignore:              No
IpSec Condition Work Summary:     NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:        0
    Direction:       0
    RouteType:       0           SecurityClass:        0
    FragmentsOnly:   No
IpSec Condition Work:           NegativeIndicator: Off
IpFilter Condition:
  Source Address:
    FromAddr:        All4
    ToAddr:          All4
  Destination Address:
  Service Condition:
    Protocol:        0
    Direction:       0
    RouteType:       0           SecurityClass:        0
    FragmentsOnly:   No
Condition Work Level:      1
  Group Number:        1           Cond Count:        2
  Ignore:              No
IpSec Condition Work Summary:     NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:        0
    Direction:       0
    RouteType:       0           SecurityClass:        0
    FragmentsOnly:   No
IpSec Condition Work:           NegativeIndicator: Off
IpFilter Condition:
  Source Address:
  Destination Address:

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    FromAddr:      All4
    ToAddr:        All4
    Service Condition:
      Protocol:      0
      Direction:     0
      RouteType:     0
      FragmentsOnly: No
      SecurityClass: 0
    Condition Work Level: 2
      Group Number: 3
      Ignore:       No
      Cond Count:   2
    IpSec Condition Work Summary:
      NegativeIndicator: Off
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:      0
        Direction:     0
        RouteType:     0
        FragmentsOnly: No
        SecurityClass: 0
    IpSec Condition Work:
      NegativeIndicator: Off
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:      IGMP (2)
        Direction:     Bidirectional
        RouteType:     Local
        FragmentsOnly: No
        SecurityClass: 0
    Policy created: Mon May 21 14:53:39 2018
    Policy updated: Mon May 21 14:53:39 2018

    IpFilter Action:      Permit__LogYes
    Version:              3
    Scope:                 GenericFilter
    Status:                Active
    ipFilterAction:        Permit
    IpFilterLogging:       Yes
    DiscardAction:         Silent
    Policy created: Mon May 21 14:53:39 2018
    Policy updated: Mon May 21 14:53:39 2018

    policyRule:           CommonTraffic~9
    Rule Type:            IpFilter
    Version:              3
    Weight:               116
    Priority:              16
    Status:               Active
    No. Policy Action:    1
    ForLoadDist:          False
    IpSecType:            policyIpFilter
    Sequence Actions:     Don't Care
    policyAction:         Permit__LogYes
    ConditionListType:    CNF
    ActionType:           IpFilter GenericFilter
    Action Sequence:      0
    Time Periods:
      Day of Month Mask:
        First to Last:    11111111111111111111111111111111
        Last to First:    11111111111111111111111111111111
        Month of Yr Mask: 111111111111
        Day of Week Mask: 1111111 (Sunday - Saturday)
        Start Date Time:  None
        End Date Time:    None

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Fr TimeOfDay:	00:00	To TimeOfDay:	24:00
Fr TimeOfDay UTC:	04:00	To TimeOfDay UTC:	04:00
TimeZone:	Local		
IpSec Condition Summary:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
Condition Work Level:	0		
Group Number:	0	Cond Count:	2
Ignore:	No		
IpSec Condition Work Summary:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
IpSec Condition Work:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
FromAddr:	All4		
ToAddr:	All4		
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
Condition Work Level:	1		
Group Number:	1	Cond Count:	2
Ignore:	No		
IpSec Condition Work Summary:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0
FragmentsOnly:	No		
IpSec Condition Work:		NegativeIndicator:	Off
IpFilter Condition:			
Source Address:			
Destination Address:			
FromAddr:	All4		
ToAddr:	All4		
Service Condition:			
Protocol:	0		
Direction:	0		
RouteType:	0	SecurityClass:	0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FragmentsOnly:      No
Condition Work Level:      2
Group Number:      3          Cond Count:      2
Ignore:      No
IpSec Condition Work Summary:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:      0
Direction:      0
RouteType:      0          SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:      UDP      (17)
SrcPortFrom:      520          SrcPortTo:      520
DestPortFrom:      1024        DestPortTo:      65535
Direction:      Bidirectional
RouteType:      Local          SecurityClass:      0
FragmentsOnly:      No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:      3          Status:      Active
Scope:      GenericFilter
ipFilterAction:      Permit      IpFilterLogging:      Yes
DiscardAction:      Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:      CommonTraffic~10
Rule Type:      IpFilter
Version:      3          Status:      Active
Weight:      115          ForLoadDist:      False
Priority:      15          Sequence Actions:      Don't Care
No. Policy Action:      1          ConditionListType:      CNF
IpSecType:      policyIpFilter
policyAction:      Permit__LogYes
ActionType:      IpFilter GenericFilter
Action Sequence:      0
Time Periods:
Day of Month Mask:
First to Last:      11111111111111111111111111111111
Last to First:      11111111111111111111111111111111
Month of Yr Mask:      111111111111
Day of Week Mask:      1111111      (Sunday - Saturday)
Start Date Time:      None
End Date Time:      None
Fr TimeOfDay:      00:00          To TimeOfDay:      24:00
Fr TimeOfDay UTC:      04:00        To TimeOfDay UTC:      04:00
TimeZone:      Local
IpSec Condition Summary:      NegativeIndicator: Off
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
Condition Work Level: 0
Group Number:    0
Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
Source Address:
  FromAddr:      All4
  ToAddr:        All4
Destination Address:
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
Condition Work Level: 1
Group Number:    1
Ignore:          No
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
Source Address:
Destination Address:
  FromAddr:      All4
  ToAddr:        All4
Service Condition:
  Protocol:      0
  Direction:     0
  RouteType:     0
  FragmentsOnly: No
Condition Work Level: 2
Group Number:    3
Ignore:          No
```

SecurityClass: 0

Cond Count: 2

NegativeIndicator: Off

SecurityClass: 0

NegativeIndicator: Off

SecurityClass: 0

Cond Count: 2

NegativeIndicator: Off

SecurityClass: 0

Cond Count: 2

NegativeIndicator: Off

SecurityClass: 0

Cond Count: 2

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

IpSec Condition Work Summary: NegativeIndicator: Off

IpFilter Condition:

Source Address:

Destination Address:

Service Condition:

Protocol: 0

Direction: 0

RouteType: 0

FragmentsOnly: No

SecurityClass: 0

IpSec Condition Work:

NegativeIndicator: Off

IpFilter Condition:

Source Address:

Destination Address:

Service Condition:

Protocol: UDP (17)

SrcPortFrom: 1024

SrcPortTo: 65535

DestPortFrom: 520

DestPortTo: 520

Direction: Bidirectional

RouteType: Local

SecurityClass: 0

FragmentsOnly: No

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes

Version: 3

Status: Active

Scope: GenericFilter

ipFilterAction: Permit

IpFilterLogging: Yes

DiscardAction: Silent

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~11

Rule Type: IpFilter

Version: 3

Status: Active

Weight: 114

ForLoadDist: False

Priority: 14

Sequence Actions: Don't Care

No. Policy Action: 1

ConditionListType: CNF

IpSecType: policyIpFilter

policyAction: Permit__LogYes

ActionType: IpFilter GenericFilter

Action Sequence: 0

Time Periods:

Day of Month Mask:

First to Last: 11111111111111111111111111111111

Last to First: 11111111111111111111111111111111

Month of Yr Mask: 1111111111

Day of Week Mask: 111111 (Sunday - Saturday)

Start Date Time: None

End Date Time: None

Fr TimeOfDay: 00:00

To TimeOfDay: 24:00

Fr TimeOfDay UTC: 04:00

To TimeOfDay UTC: 04:00

TimeZone: Local

IpSec Condition Summary:

NegativeIndicator: Off

IpFilter Condition:

Source Address:

Destination Address:

Service Condition:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Protocol:          0
Direction:        0
RouteType:        0
FragmentsOnly:    No
Condition Work Level: 0
Group Number:     0
Ignore:           No
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:         0
Direction:       0
RouteType:       0
FragmentsOnly:   No
SecurityClass:    0
IpSec Condition Work:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr:        All4
ToAddr:          All4
Destination Address:
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:  No
SecurityClass:   0
Condition Work Level: 1
Group Number:    1
Ignore:         No
IpSec Condition Work Summary:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:  No
SecurityClass:   0
IpSec Condition Work:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:        All4
ToAddr:          All4
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:  No
SecurityClass:   0
Condition Work Level: 2
Group Number:    3
Ignore:         No
IpSec Condition Work Summary:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Service Condition:
  Protocol:          0
  Direction:         0
  RouteType:         0
  FragmentsOnly:     No
  SecurityClass:      0
IpSec Condition Work:
  NegativeIndicator:  Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:       UDP    (17)
      SrcPortFrom:    520
      SrcPortTo:      520
      DestPortFrom:   520
      DestPortTo:     520
      Direction:      Bidirectional
      RouteType:      Local
      SecurityClass:   0
      FragmentsOnly:  No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
  Version:            3
  Status:              Active
  Scope:              GenericFilter
  ipFilterAction:     Permit
  IpFilterLogging:     Yes
  DiscardAction:      Silent
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018

policyRule:           CommonTraffic~12
  Rule Type:          IpFilter
  Version:            3
  Status:              Active
  Weight:             113
  ForLoadDist:        False
  Priority:            13
  Sequence Actions:    Don't Care
  No. Policy Action:   1
  ConditionListType:   CNF
  IpSecType:          policyIpFilter
  policyAction:        Permit__LogYes
  ActionType:          IpFilter GenericFilter
  Action Sequence:     0
  Time Periods:
    Day of Month Mask:
      First to Last:   11111111111111111111111111111111
      Last to First:   11111111111111111111111111111111
      Month of Yr Mask: 111111111111
      Day of Week Mask: 1111111 (Sunday - Saturday)
      Start Date Time: None
      End Date Time:    None
      Fr TimeOfDay:     00:00
      To TimeOfDay:     24:00
      Fr TimeOfDay UTC: 04:00
      To TimeOfDay UTC: 04:00
      TimeZone:         Local
  IpSec Condition Summary:
    NegativeIndicator:  Off
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:       0
        Direction:      0
        RouteType:      0
        SecurityClass:   0
        FragmentsOnly:  No
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Condition Work Level:      0
  Group Number:           0          Cond Count:           2
  Ignore:                 No
IpSec Condition Work Summary:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:           0
      Direction:          0
      RouteType:          0          SecurityClass:          0
      FragmentsOnly:      No
IpSec Condition Work:              NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:           All4
      ToAddr:             All4
    Destination Address:
    Service Condition:
      Protocol:           0
      Direction:          0
      RouteType:          0          SecurityClass:          0
      FragmentsOnly:      No
Condition Work Level:      1
  Group Number:           1          Cond Count:           2
  Ignore:                 No
IpSec Condition Work Summary:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:           0
      Direction:          0
      RouteType:          0          SecurityClass:          0
      FragmentsOnly:      No
IpSec Condition Work:              NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
      FromAddr:           All4
      ToAddr:             All4
    Service Condition:
      Protocol:           0
      Direction:          0
      RouteType:          0          SecurityClass:          0
      FragmentsOnly:      No
Condition Work Level:      2
  Group Number:           3          Cond Count:           2
  Ignore:                 No
IpSec Condition Work Summary:      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:           0
      Direction:          0
      RouteType:          0          SecurityClass:          0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FragmentsOnly:      No
IpSec Condition Work:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:            ICMP (1)
TypeFrom:            3           TypeTo:            3
CodeFrom:            4           CodeTo:            4
Direction:           Bidirectional
RouteType:           Local       SecurityClass:    0
FragmentsOnly:      No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3           Status:          Active
Scope:               GenericFilter
ipFilterAction:       Permit       IpFilterLogging:  Yes
DiscardAction:        Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:           CommonTraffic~13
Rule Type:            IpFilter
Version:              3           Status:          Active
Weight:              112          ForLoadDist:     False
Priority:             12          Sequence Actions: Don't Care
No. Policy Action:    1           ConditionListType: CNF
IpSecType:            policyIpFilter
policyAction:         Permit__LogYes
ActionType:           IpFilter GenericFilter
Action Sequence:      0
Time Periods:
Day of Month Mask:
First to Last:        11111111111111111111111111111111
Last to First:        11111111111111111111111111111111
Month of Yr Mask:      1111111111
Day of Week Mask:      111111    (Sunday - Saturday)
Start Date Time:       None
End Date Time:         None
Fr TimeOfDay:          00:00       To TimeOfDay:     24:00
Fr TimeOfDay UTC:      04:00       To TimeOfDay UTC: 04:00
TimeZone:              Local
IpSec Condition Summary:      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:              0
Direction:             0
RouteType:             0           SecurityClass:    0
FragmentsOnly:         No
Condition Work Level:   0
Group Number:          0           Cond Count:       2
Ignore:                 No
IpSec Condition Work Summary:      NegativeIndicator: Off
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
SecurityClass:      0
NegativeIndicator: Off

IpSec Condition Work:
IpFilter Condition:
Source Address:
  FromAddr:      All4
  ToAddr:        All4
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
SecurityClass:      0
Condition Work Level:      1
  Group Number:      1
  Ignore:            No
Cond Count:            2
IpSec Condition Work Summary:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
SecurityClass:      0
NegativeIndicator: Off

IpSec Condition Work:
IpFilter Condition:
Source Address:
Destination Address:
  FromAddr:      All4
  ToAddr:        All4
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
SecurityClass:      0
Condition Work Level:      2
  Group Number:      3
  Ignore:            No
Cond Count:            2
IpSec Condition Work Summary:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
SecurityClass:      0
NegativeIndicator: Off

IpSec Condition Work:
IpFilter Condition:
Source Address:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Destination Address:
Service Condition:
Protocol: ICMP (1)
TypeFrom: 8 TypeTo: 8
Code: Any
Direction: Bidirectional
RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~14
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 111 ForLoadDist: False
Priority: 11 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0

Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local

IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No

IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Protocol:          0
Direction:        0
RouteType:        0
FragmentsOnly:    No
SecurityClass:     0
IpSec Condition Work:
IpFilter Condition:
Source Address:
FromAddr:         All4
ToAddr:           All4
Destination Address:
Service Condition:
Protocol:         0
Direction:       0
RouteType:       0
FragmentsOnly:   No
SecurityClass:    0
Condition Work Level: 1
Group Number:    1
Ignore:          No
Cond Count:      2
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:   No
SecurityClass:   0
NegativeIndicator: Off
IpSec Condition Work:
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:        All4
ToAddr:          All4
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:   No
SecurityClass:   0
Condition Work Level: 2
Group Number:    3
Ignore:          No
Cond Count:      2
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        0
Direction:      0
RouteType:      0
FragmentsOnly:   No
SecurityClass:   0
NegativeIndicator: Off
IpSec Condition Work:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:        ICMP (1)
TypeFrom:        0
TypeTo:          0

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Code: Any
Direction: Bidirectional
RouteType: Local SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~15
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 110 ForLoadDist: False
Priority: 10 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

IpSec Condition Work: IpFilter Condition: Source Address: FromAddr: All4 ToAddr: All4 Destination Address: Service Condition: Protocol: 0 Direction: 0 RouteType: 0 FragmentsOnly: No Condition Work Level: 1 Group Number: 1 Ignore: No	NegativeIndicator: Off SecurityClass: 0 Cond Count: 2
IpSec Condition Work Summary: IpFilter Condition: Source Address: Destination Address: Service Condition: Protocol: 0 Direction: 0 RouteType: 0 FragmentsOnly: No	NegativeIndicator: Off SecurityClass: 0
IpSec Condition Work: IpFilter Condition: Source Address: Destination Address: FromAddr: All4 ToAddr: All4 Service Condition: Protocol: 0 Direction: 0 RouteType: 0 FragmentsOnly: No Condition Work Level: 2 Group Number: 3 Ignore: No	NegativeIndicator: Off SecurityClass: 0 Cond Count: 2
IpSec Condition Work Summary: IpFilter Condition: Source Address: Destination Address: Service Condition: Protocol: 0 Direction: 0 RouteType: 0 FragmentsOnly: No	NegativeIndicator: Off SecurityClass: 0
IpSec Condition Work: IpFilter Condition: Source Address: Destination Address: Service Condition: Protocol: TCP (6) SrcPortFrom: 1024 DestPortFrom: 53 Direction: Bidirectional RouteType: Local FragmentsOnly: No	NegativeIndicator: Off SrcPortTo: 65535 DestPortTo: 53 OutboundConnect SecurityClass: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

IpFilter Action: Permit__LogYes
Version: 3 Status: Active
Scope: GenericFilter
ipFilterAction: Permit IpFilterLogging: Yes
DiscardAction: Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule: CommonTraffic~16
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 109 ForLoadDist: False
Priority: 9 Sequence Actions: Don't Care
No. Policy Action: 1 ConditionListType: CNF
IpSecType: policyIpFilter
policyAction: Permit__LogYes
ActionType: IpFilter GenericFilter
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
Condition Work Level: 0
Group Number: 0 Cond Count: 2
Ignore: No
IpSec Condition Work Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol: 0
Direction: 0
RouteType: 0 SecurityClass: 0
FragmentsOnly: No
IpSec Condition Work: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: All4

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ToAddr:                All4
Destination Address:
Service Condition:
  Protocol:              0
  Direction:             0
  RouteType:             0
  FragmentsOnly:        No
  SecurityClass:         0
Condition Work Level:   1
  Group Number:          1
  Ignore:                No
  Cond Count:            2
IpSec Condition Work Summary:
  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:          0
      Direction:         0
      RouteType:         0
      FragmentsOnly:     No
      SecurityClass:     0
      NegativeIndicator: Off
    IpSec Condition Work:
      IpFilter Condition:
        Source Address:
        Destination Address:
        FromAddr:        All4
        ToAddr:          All4
        Service Condition:
          Protocol:       0
          Direction:      0
          RouteType:      0
          FragmentsOnly:  No
          SecurityClass:  0
        Condition Work Level: 2
          Group Number:    3
          Ignore:          No
          Cond Count:      2
        IpSec Condition Work Summary:
          NegativeIndicator: Off
        IpFilter Condition:
          Source Address:
          Destination Address:
          Service Condition:
            Protocol:      0
            Direction:     0
            RouteType:     0
            FragmentsOnly: No
            SecurityClass: 0
            NegativeIndicator: Off
        IpSec Condition Work:
          IpFilter Condition:
            Source Address:
            Destination Address:
            Service Condition:
              Protocol:      UDP (17)
              SrcPortFrom:   1024
              SrcPortTo:     65535
              DestPortFrom:  53
              DestPortTo:    53
              Direction:     Bidirectional
              RouteType:     Local
              FragmentsOnly: No
              SecurityClass: 0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:        Permit__LogYes
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Version:          3                      Status:          Active
Scope:           GenericFilter
ipFilterAction:   Permit                 IpFilterLogging:  Yes
DiscardAction:    Silent
Policy created:   Mon May 21 14:53:39 2018
Policy updated:   Mon May 21 14:53:39 2018

policyRule:       CommonTraffic~17
Rule Type:        IpFilter
Version:          3                      Status:          Active
Weight:           108                   ForLoadDist:      False
Priority:          8                     Sequence Actions:  Don't Care
No. Policy Action: 1                     ConditionListType: CNF
IpSecType:        policyIpFilter
policyAction:     Permit__LogYes
ActionType:       IpFilter GenericFilter
Action Sequence:  0
Time Periods:
Day of Month Mask:
First to Last:    11111111111111111111111111111111
Last to First:    11111111111111111111111111111111
Month of Yr Mask:  1111111111
Day of Week Mask:  1111111 (Sunday - Saturday)
Start Date Time:   None
End Date Time:     None
Fr TimeOfDay:      00:00                 To TimeOfDay:      24:00
Fr TimeOfDay UTC:  04:00                 To TimeOfDay UTC:  04:00
TimeZone:          Local
IpSec Condition Summary:                  NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                     SecurityClass:      0
FragmentsOnly:     No
Condition Work Level: 0
Group Number:      0                     Cond Count:         2
Ignore:            No
IpSec Condition Work Summary:              NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                     SecurityClass:      0
FragmentsOnly:     No
IpSec Condition Work:                      NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr:          All4
ToAddr:            All4
Destination Address:
Service Condition:
Protocol:          0

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Direction:          0
RouteType:          0
FragmentsOnly:      No
Condition Work Level: 1
Group Number:       1
Ignore:             No
IpSec Condition Work Summary:
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0
FragmentsOnly:      No
SecurityClass:      0
IpSec Condition Work:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:           All4
ToAddr:             All4
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0
FragmentsOnly:      No
SecurityClass:      0
Condition Work Level: 2
Group Number:       3
Ignore:             No
IpSec Condition Work Summary:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:          0
RouteType:          0
FragmentsOnly:      No
SecurityClass:      0
IpSec Condition Work:
NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           ICMP (1)
TypeFrom:           11
CodeFrom:           0
Direction:          Bidirectional
RouteType:          Local
FragmentsOnly:      No
TypeTo:             11
CodeTo:             0
SecurityClass:      0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:     Permit__LogYes
Version:             3
Scope:              GenericFilter
ipFilterAction:      Permit
DiscardAction:       Silent
Status:              Active
IpFilterLogging:     Yes

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy created: Mon May 21 14:53:39 2018

Policy updated: Mon May 21 14:53:39 2018

```
policyRule:          CommonTraffic~18
  Rule Type:          IpFilter
  Version:            3
  Weight:             107
  Priority:            7
  No. Policy Action:  1
  IpSecType:          policyIpFilter
  policyAction:        Permit__LogYes
  ActionType:         IpFilter GenericFilter
  Action Sequence:    0
  Time Periods:
    Day of Month Mask:
      First to Last:  11111111111111111111111111111111
      Last to First:  11111111111111111111111111111111
    Month of Yr Mask:  111111111111
    Day of Week Mask:  1111111 (Sunday - Saturday)
    Start Date Time:   None
    End Date Time:     None
    Fr TimeOfDay:      00:00
    To TimeOfDay:      24:00
    Fr TimeOfDay UTC:  04:00
    To TimeOfDay UTC:  04:00
    TimeZone:          Local
  IpSec Condition Summary:
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:      0
        Direction:     0
        RouteType:     0
        FragmentsOnly: No
      SecurityClass:    0
    Condition Work Level: 0
      Group Number:    0
      Ignore:          No
      Cond Count:      2
  IpSec Condition Work Summary:
    IpFilter Condition:
      Source Address:
      Destination Address:
      Service Condition:
        Protocol:      0
        Direction:     0
        RouteType:     0
        FragmentsOnly: No
      SecurityClass:    0
    IpSec Condition Work:
      IpFilter Condition:
        Source Address:
          FromAddr:     All4
          ToAddr:       All4
        Destination Address:
        Service Condition:
          Protocol:      0
          Direction:     0
          RouteType:     0
          FragmentsOnly: No
          SecurityClass: 0
      Condition Work Level: 1
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Group Number:      1                      Cond Count:      2
Ignore:            No
IpSec Condition Work Summary:              NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:    No
IpSec Condition Work:                      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:          All4
ToAddr:            All4
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:    No
Condition Work Level:      2
Group Number:      3                      Cond Count:      2
Ignore:            No
IpSec Condition Work Summary:              NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          0
Direction:         0
RouteType:         0                      SecurityClass:      0
FragmentsOnly:    No
IpSec Condition Work:                      NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:          ICMP (1)
TypeFrom:          3                      TypeTo:            3
CodeFrom:          3                      CodeTo:            3
Direction:         Bidirectional
RouteType:         Local                  SecurityClass:      0
FragmentsOnly:    No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3                      Status:            Active
Scope:                GenericFilter
ipFilterAction:       Permit                  IpFilterLogging:   Yes
DiscardAction:        Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018
```

policyRule: CommonTraffic~19

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Rule Type:                IpFilter
Version:                  3
Weight:                   106
Priority:                  6
No. Policy Action:        1
IpSecType:                policyIpFilter
policyAction:             Permit__LogYes
  ActionType:             IpFilter GenericFilter
  Action Sequence:        0
Time Periods:
  Day of Month Mask:
    First to Last:        11111111111111111111111111111111
    Last to First:        11111111111111111111111111111111
  Month of Yr Mask:        111111111111
  Day of Week Mask:        1111111 (Sunday - Saturday)
  Start Date Time:        None
  End Date Time:          None
  Fr TimeOfDay:           00:00
  To TimeOfDay:           24:00
  Fr TimeOfDay UTC:       04:00
  To TimeOfDay UTC:       04:00
  TimeZone:               Local
IpSec Condition Summary:   NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:            0
      Direction:           0
      RouteType:           0
      FragmentsOnly:       No
    SecurityClass:         0
  Condition Work Level:    0
    Group Number:          0
    Cond Count:            2
    Ignore:                No
IpSec Condition Work Summary: NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:            0
      Direction:           0
      RouteType:           0
      FragmentsOnly:       No
    SecurityClass:         0
  IpSec Condition Work:    NegativeIndicator: Off
    IpFilter Condition:
      Source Address:
        FromAddr:          All4
        ToAddr:            All4
      Destination Address:
      Service Condition:
        Protocol:          0
        Direction:         0
        RouteType:         0
        FragmentsOnly:     No
        SecurityClass:     0
      Condition Work Level: 1
        Group Number:      1
        Cond Count:        2
        Ignore:            No
    IpSec Condition Work Summary: NegativeIndicator: Off
      IpFilter Condition:

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Source Address:
Destination Address:
Service Condition:
  Protocol:      0
  Direction:    0
  RouteType:    0
  FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
  Source Address:
  Destination Address:
  FromAddr:      All4
  ToAddr:        All4
  Service Condition:
    Protocol:    0
    Direction:  0
    RouteType:  0
    FragmentsOnly: No
  Condition Work Level: 2
  Group Number:  3
  Ignore:        No
IpSec Condition Work Summary:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:    0
    Direction:  0
    RouteType:  0
    FragmentsOnly: No
IpSec Condition Work:
IpFilter Condition:
  Source Address:
  Destination Address:
  Service Condition:
    Protocol:    ICMP (1)
    TypeFrom:    3
    CodeFrom:    2
    Direction:   Bidirectional
    RouteType:   Local
    FragmentsOnly: No
    TypeTo:      3
    CodeTo:      2
    SecurityClass: 0
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3
Scope:                GenericFilter
ipFilterAction:        Permit
DiscardAction:         Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:           CommonTraffic~20
Rule Type:            IpFilter
Version:              3
Weight:               105
Priority:              5
Status:                Active
ForLoadDist:          False
Sequence Actions:     Don't Care
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

No. Policy Action:      1                      ConditionListType: CNF
IpSecType:             policyIpFilter
policyAction:          Permit__LogYes
  ActionType:          IpFilter GenericFilter
  Action Sequence:     0
Time Periods:
  Day of Month Mask:
  First to Last:       11111111111111111111111111111111
  Last to First:       11111111111111111111111111111111
  Month of Yr Mask:     111111111111
  Day of Week Mask:     1111111  (Sunday - Saturday)
  Start Date Time:     None
  End Date Time:        None
  Fr TimeOfDay:         00:00          To TimeOfDay:         24:00
  Fr TimeOfDay UTC:     04:00          To TimeOfDay UTC:     04:00
  TimeZone:             Local
IpSec Condition Summary:                      NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:         0
      Direction:        0
      RouteType:        0          SecurityClass:         0
      FragmentsOnly:    No
Condition Work Level:      0
  Group Number:           0          Cond Count:         2
  Ignore:                 No
IpSec Condition Work Summary:                  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:         0
      Direction:        0
      RouteType:        0          SecurityClass:         0
      FragmentsOnly:    No
IpSec Condition Work:                          NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
      FromAddr:         All4
      ToAddr:           All4
    Destination Address:
    Service Condition:
      Protocol:         0
      Direction:        0
      RouteType:        0          SecurityClass:         0
      FragmentsOnly:    No
Condition Work Level:      1
  Group Number:           1          Cond Count:         2
  Ignore:                 No
IpSec Condition Work Summary:                  NegativeIndicator: Off
  IpFilter Condition:
    Source Address:
    Destination Address:
    Service Condition:
      Protocol:         0

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Direction:          0
RouteType:          0          SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
FromAddr:           All4
ToAddr:             All4
Service Condition:
Protocol:           0
Direction:         0
RouteType:         0          SecurityClass:      0
FragmentsOnly:      No
Condition Work Level:      2
Group Number:        3          Cond Count:        2
Ignore:             No
IpSec Condition Work Summary:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           0
Direction:         0
RouteType:         0          SecurityClass:      0
FragmentsOnly:      No
IpSec Condition Work:          NegativeIndicator: Off
IpFilter Condition:
Source Address:
Destination Address:
Service Condition:
Protocol:           UDP   (17)
SrcPortFrom:        1024          SrcPortTo:        65535
DestPortFrom:        33435          DestPortTo:        33535
Direction:          Bidirectional
RouteType:          Local          SecurityClass:      0
FragmentsOnly:      No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

IpFilter Action:      Permit__LogYes
Version:              3          Status:          Active
Scope:               GenericFilter
ipFilterAction:       Permit          IpFilterLogging:  Yes
DiscardAction:        Silent
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

policyRule:           DenyAllRule_Generated_____Inbnd
Rule Type:            IpFilter
Version:              3          Status:          Active
Weight:               104          ForLoadDist:      False
Priority:              4          Sequence Actions: Don't Care
No. Policy Action:    0
IpSecType:            policyIpFilter
Time Periods:
Day of Month Mask:
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

First to Last:      11111111111111111111111111111111
Last to First:     11111111111111111111111111111111
Month of Yr Mask:   111111111111
Day of Week Mask:   1111111  (Sunday - Saturday)
Start Date Time:    None
End Date Time:      None
Fr TimeOfDay:       00:00           To TimeOfDay:      24:00
Fr TimeOfDay UTC:   04:00           To TimeOfDay UTC:   04:00
TimeZone:           Local
IPSec Condition Summary:           NegativeIndicator: Off
IpFilter Condition:
Source Address:
    FromAddr:       All4
    ToAddr:         All4
Destination Address:
    FromAddr:       All4
    ToAddr:         All4
Service Condition:
    Protocol:       All
    Direction:      Inbound
    RouteType:      Either           SecurityClass:      0
    FragmentsOnly:  No
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 14:53:39 2018

```

```
policyRule: DenyAllRule_Generated_____Outbnd
Rule Type: IpFilter
Version: 3 Status: Active
Weight: 103 ForLoadDist: False
Priority: 3 Sequence Actions: Don't Care
No. Policy Action: 0
IpSecType: policyIpFilter
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 111111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
IpSec Condition Summary: NegativeIndicator: Off
IpFilter Condition:
Source Address:
FromAddr: All4
ToAddr: All4
Destination Address:
FromAddr: All4
ToAddr: All4
Service Condition:
Protocol: All
Direction: Outbound
RouteType: Either SecurityClass: 0
FragmentsOnly: No
Policy created: Mon May 21 14:53:39 2018
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Policy updated: Mon May 21 14:53:39 2018

```
policyRule:          BetweenOSAsRSA~5
  Rule Type:          KeyExchange
  Version:            3                      Status:          Active
  Weight:             102                   ForLoadDist:        False
  Priority:            2                     Sequence Actions:    Don't Care
  No. Policy Action:   1
  IpSecType:          policyKeyExchange
  policyAction:        BetweenOSAsRSA
  ActionType:          KeyExchange
  Action Sequence:     0
  Time Periods:
    Day of Month Mask: 00000000000000000000000000000000
    Month of Yr Mask:  000000000000
    Day of Week Mask:  0000000 (Sunday - Saturday)
    Start Date Time:   None
    End Date Time:     None
    Fr TimeOfDay:       00:00                To TimeOfDay:        00:00
    Fr TimeOfDay UTC:   00:00                To TimeOfDay UTC:    00:00
    TimeZone:           Local
  IpSec Condition Summary:                    NegativeIndicator: Off
  KeyExchange Condition:
    LocalSecurityEndPoint:
      Location:
        FromAddr:      192.168.20.97
        ToAddr:        192.168.20.97
      Identity:
        IpAddr:
          FromAddr:     192.168.20.97
          ToAddr:       192.168.20.97
    RemoteSecurityEndPoint:
      Location:
        FromAddr:      192.168.20.91
        ToAddr:        192.168.20.91
      Identity:
        IpAddr:
          FromAddr:     192.168.20.91
          ToAddr:       192.168.20.91
  Policy created: Mon May 21 14:53:39 2018
  Policy updated: Mon May 21 14:53:39 2018
```

```
KeyExchange Action:  BetweenOSAsRSA
  Version:            3                      Status:          Active
  HowToInitiate:      Main                   HowToRespondIKEv1: Either
  AllowNat:           No                     FilterByIdentity:  No
  HowToAuthMe:        DigitalSignature       ReauthInterval:    0
  BypassIpValidation: Yes                    CertURLLookupPref: Tolerate
  RevocationChecking: Loose
  ConstrainSource:    0
    FromAddr:         192.168.20.97
    ToAddr:           192.168.20.97
  ConstrainDest:      0
    FromAddr:         192.168.20.91
    ToAddr:           192.168.20.91
  KeyExchangeOffer:   0
    HowToEncrypt:      AES_CBC                KeyLength:         128
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

HowToAuthPeers: RsaSignature DHGroup: Group2
HowToAuthMsgs: SHA1
HowToVerifyMsgs: HMAC_SHA1_96 PseudoRandomFunc: HMAC_SHA1
RefLifeTmPropose: 1440
RefLifeTmAcptMin: 1440 RefLifeTmAcptMax: 1440
RefLifeSzPropose: None
RefLifeSzAccept : None
Policy created: Mon May 21 14:53:39 2018
Policy updated: Mon May 21 20:08:24 2018

policyRule: TrafOSA2DVIPAPresh~5
 Rule Type: KeyExchange
 Version: 3 Status: Active
 Weight: 101 ForLoadDist: False
 Priority: 1 Sequence Actions: Don't Care
 No. Policy Action: 1
 IpSecType: policyKeyExchange
 policyAction: TrafOSA2DVIPAPresh
 ActionType: KeyExchange
 Action Sequence: 0
 Time Periods:
 Day of Month Mask: 00000000000000000000000000000000
 Month of Yr Mask: 000000000000
 Day of Week Mask: 0000000 (Sunday - Saturday)
 Start Date Time: None
 End Date Time: None
 Fr TimeOfDay: 00:00 To TimeOfDay: 00:00
 Fr TimeOfDay UTC: 00:00 To TimeOfDay UTC: 00:00
 TimeZone: Local
 IpSec Condition Summary: NegativeIndicator: Off
 KeyExchange Condition:
 LocalSecurityEndPoint:
 Location:
 FromAddr: 192.168.20.97
 ToAddr: 192.168.20.97
 Identity:
 Fqdn:
 WSC.LABS.IBM.COM
 RemoteSecurityEndPoint:
 Location:
 FromAddr: 192.168.20.121
 ToAddr: 192.168.20.121
 Identity:
 UserAtFqdn:
 ZOS1@WSC.LABS.IBM.COM
 Policy created: Mon May 21 20:08:24 2018
 Policy updated: Mon May 21 20:08:24 2018

KeyExchange Action: TrafOSA2DVIPAPresh
 Version: 3 Status: Active
 HowToInitiate: Main HowToRespondIKEv1: Either
 AllowNat: No FilterByIdentity: No
 HowToAuthMe: PresharedKey ReauthInterval: 0
 BypassIpValidation: Yes CertURLLookupPref: Tolerate
 RevocationChecking: Loose
 ConstrainSource: 0
 FromAddr: 192.168.20.127

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ToAddr: 192.168.20.127
ConstrainDest: 0
FromAddr: 192.168.20.121
ToAddr: 192.168.20.121
KeyExchangeOffer: 0
HowToEncrypt: AES_CBC KeyLength: 128
HowToAuthPeers: PresharedKey DHGroup: Group2
HowToAuthMsgs: SHA1
HowToVerifyMsgs: HMAC_SHA1_96 PseudoRandomFunc: HMAC_SHA1
RefLifeTmPropose: 1440
RefLifeTmAcptMin: 1440 RefLifeTmAcptMax: 1440
RefLifeSzPropose: None
RefLifeSzAccept : None
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

policyRule: VIPAs2VIPAs~1
Rule Type: TTLS
Version: 3 Status: Active
Weight: 255 ForLoadDist: False
Priority: 255 Sequence Actions: Don't Care
No. Policy Action: 3
policyAction: gAct1
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct1~AllSecFTPCLients
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct1~AllSecFTPCLients
ActionType: TTLS Connection
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
TTLS Condition Summary: NegativeIndicator: Off
Local Address:
FromAddr: 192.168.20.101
ToAddr: 192.168.20.107
Remote Address:
FromAddr: 192.168.20.101
ToAddr: 192.168.20.107
LocalPortFrom: 1024 LocalPortTo: 65535
RemotePortFrom: 21 RemotePortTo: 21
JobName: UserId: USER*
ServiceDirection: Outbound
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TTLS Action: gAct1
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Version: 3
Status: Active
Scope: Group
TTLS-enabled: On
CtraceClearText: Off
Trace: 2
FIPS140: Off
TTLSGroupAdvancedParms:
 SecondaryMap: Off
 SyslogFacility: Daemon
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TTLS Action: eAct1~AllSecFTPclients
Version: 3
Status: Active
Scope: Environment
HandshakeRole: Client
SuiteBProfile: Off
TTLSKeyringParms:
 Keyring: LabClientRing
TTLSEnvironmentAdvancedParms:
 SSLv2: Off
 SSLv3: Off
 TLSv1: On
 TLSv1.1: On
 TLSv1.2: Off
 ApplicationControlled: Off
 HandshakeTimeout: 10
 ClientAuthType: Required
 ResetCipherTimer: 0
 TruncatedHMAC: Off
 CertValidationMode: Any
 ServerMaxSSLFragment: Off
 ClientMaxSSLFragment: Off
 ServerHandshakeSNI: Off
 ClientHandshakeSNI: Off
 Renegotiation: Default
 RenegotiationIndicator: Optional
 RenegotiationCertCheck: Off
 3DesKeyCheck: Off
 ClientEDHGroupSize: Legacy
 ServerEDHGroupSize: Legacy
 PeerMinCertVersion: Any
 PeerMinDHKeySize: 1024
 PeerMinDsaKeySize: 1024
 PeerMinECCKeySize: 192
 PeerMinRsaKeySize: 1024
 ServerScsv: Off
TTLSGskAdvancedParms:
 TTLSGskHttpCdpParms:
 HttpCdpEnable: Off
 HttpCdpProxyServerPort: 80
 HttpCdpResponseTimeout: 15
 HttpCdpMaxResponseSize: 204800
 HttpCdpCacheSize: 32
 HttpCdpCacheEntryMaxsize: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TTLSGskOcspParms:
OcspAiaEnable: Off
OcspProxyServerPort: 80
OcspRetrieveViaGet: Off
OcspUrlPriority: On
OcspRequestSigalg:
0401 TLS_SIGALG_SHA256_WITH_RSA
OcspClientCacheSize: 256
OcspCliCacheEntryMaxsize: 0
OcspNonceGenEnable: Off
OcspNonceCheckEnable: Off
OcspNonceSize: 8
OcspResponseTimeout: 15
OcspMaxResponseSize: 20480
OcspServerStapling: Off
EnvironmentUserInstance: 0
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TTLS Action: cAct1~AllSecFTPCLients
Version: 3
Status: Active
Scope: Connection
HandshakeRole: Client
CtracedClearText: Off
Trace: 2
TTLSCConnectionAdvancedParms:
SecondaryMap: On
SSLv3: On
TLSv1: On
TLSv1.1: On
TLSv1.2: Off
ApplicationControlled: On
TTLSCipherParms:
v3CipherSuites:
000A TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F TLS_RSA_WITH_AES_128_CBC_SHA
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

policyRule: VIPAs2VIPAs~2
Rule Type: TTLS
Version: 3
Weight: 254
Priority: 254
No. Policy Action: 3
policyAction: gAct1
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct2~FTP-Server
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct2~FTP-Server
ActionType: TTLS Connection
Action Sequence: 0
Time Periods:
Day of Month Mask:

Status:	Active
ForLoadDist:	False
Sequence Actions:	Don't Care

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

First to Last:      11111111111111111111111111111111
Last to First:     11111111111111111111111111111111
Month of Yr Mask:   111111111111
Day of Week Mask:   1111111  (Sunday - Saturday)
Start Date Time:    None
End Date Time:      None
Fr TimeOfDay:       00:00                To TimeOfDay:      24:00
Fr TimeOfDay UTC:   04:00                To TimeOfDay UTC:  04:00
TimeZone:           Local
TTLS Condition Summary:      NegativeIndicator: Off
Local Address:
  FromAddr:         192.168.20.101
  ToAddr:           192.168.20.107
Remote Address:
  FromAddr:         192.168.20.101
  ToAddr:           192.168.20.107
LocalPortFrom:      21                   LocalPortTo:       21
RemotePortFrom:     1024                 RemotePortTo:      65535
JobName:            UserId:
ServiceDirection:   Inbound
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

```

```

TTLS Action:                                gAct1
  Version:                                    3
  Status:                                     Active
  Scope:                                      Group
  TTLS-enabled:                               On
  CtrClearText:                              Off
  Trace:                                     2
  FIPS140:                                   Off
  TTLSGroupAdvancedParms:
    SecondaryMap:                             Off
    SyslogFacility:                           Daemon
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

```

```

TTLS Action: eAct2~FTP-Server
Version: 3
Status: Active
Scope: Environment
HandshakeRole: ServerWithClientAuth
SuiteBProfile: Off
TTLSKeyringParms:
  Keyring: FTPD/ServerRing1
TTLSEnvironmentAdvancedParms:
  SSLv2: Off
  SSLv3: Off
  TLSv1: On
  TLSv1.1: On
  TLSv1.2: Off
  ApplicationControlled: Off
  HandshakeTimeout: 10
  ClientAuthType: Required
  ResetCipherTimer: 0
  TruncatedHMAC: Off
  CertValidationMode: Any

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

ServerMaxSSLFragment: Off
ClientMaxSSLFragment: Off
ServerHandshakeSNI: Off
ClientHandshakeSNI: Off
Renegotiation: Default
RenegotiationIndicator: Optional
RenegotiationCertCheck: Off
3DesKeyCheck: Off
ClientEDHGroupSize: Legacy
ServerEDHGroupSize: Legacy
PeerMinCertVersion: Any
PeerMinDHKeySize: 1024
PeerMinDsaKeySize: 1024
PeerMinECCKeySize: 192
PeerMinRsaKeySize: 1024
ServerScsv: Off

TTLSGskAdvancedParms:

TTLSGskHttpCdpParms:

HttpCdpEnable: Off
HttpCdpProxyServerPort: 80
HttpCdpResponseTimeout: 15
HttpCdpMaxResponseSize: 204800
HttpCdpCacheSize: 32
HttpCdpCacheEntryMaxsize: 0

TTLSGskOcspParms:

OcspAiaEnable: Off
OcspProxyServerPort: 80
OcspRetrieveViaGet: Off
OcspUrlPriority: On
OcspRequestSigalg:
 0401 TLS_SIGALG_SHA256_WITH_RSA
OcspClientCacheSize: 256
OcspCliCacheEntryMaxsize: 0
OcspNonceGenEnable: Off
OcspNonceCheckEnable: Off
OcspNonceSize: 8
OcspResponseTimeout: 15
OcspMaxResponseSize: 20480
OcspServerStapling: Off

EnvironmentUserInstance: 0

Policy created: Mon May 21 16:01:28 2018

Policy updated: Mon May 21 16:01:28 2018

TTLS Action: cAct2~FTP-Server
Version: 3
Status: Active
Scope: Connection
HandshakeRole: ServerWithClientAuth
CtracedClearText: Off
Trace: 2
TTLSConnectionAdvancedParms:
 SecondaryMap: On
 SSLv3: On
 TLSv1: On
 TLSv1.1: On
 TLSv1.2: On
 ApplicationControlled: On

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TTLSCipherParms:
v3CipherSuites:
000A TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F TLS_RSA_WITH_AES_128_CBC_SHA
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

policyRule: TN3270-WS-to-Host~3
Rule Type: TTLS
Version: 3 Status: Active
Weight: 253 ForLoadDist: False
Priority: 253 Sequence Actions: Don't Care
No. Policy Action: 3
policyAction: gAct1
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct3~TN3270DiffKeyring
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct3~TN3270DiffKeyring
ActionType: TTLS Connection
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
TTLS Condition Summary: NegativeIndicator: Off
Local Address:
FromAddr: 192.168.20.101
ToAddr: 192.168.20.107
Remote Address:
FromAddr: 192.168.0.0
Prefix: 16
LocalPortFrom: 23 LocalPortTo: 23
RemotePortFrom: 1024 RemotePortTo: 65535
JobName: UserId:
ServiceDirection: Inbound
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TTLS Action: gAct1
Version: 3
Status: Active
Scope: Group
TTLS Enabled: On
CtracedClearText: Off
Trace: 2
FIPS140: Off
TTLSGroupAdvancedParms:
SecondaryMap: Off

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

SyslogFacility: Daemon
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TLS Action: eAct3~TN3270DiffKeyring
Version: 3
Status: Active
Scope: Environment
HandshakeRole: ServerWithClientAuth
SuiteBProfile: Off
TTLSTKeyringParms:
Keyring: TN3270/MyServer7Ring
TTLSEnvironmentAdvancedParms:
SSLv2: Off
SSLv3: Off
TLSv1: On
TLSv1.1: On
TLSv1.2: Off
ApplicationControlled: Off
HandshakeTimeout: 10
ClientAuthType: Required
ResetCipherTimer: 0
TruncatedHMAC: Off
CertValidationMode: Any
ServerMaxSSLFragment: Off
ClientMaxSSLFragment: Off
ServerHandshakeSNI: Off
ClientHandshakeSNI: Off
Renegotiation: Default
RenegotiationIndicator: Optional
RenegotiationCertCheck: Off
3DesKeyCheck: Off
ClientEDHGroupSize: Legacy
ServerEDHGroupSize: Legacy
PeerMinCertVersion: Any
PeerMinDHKeySize: 1024
PeerMinDsaKeySize: 1024
PeerMinECCKeySize: 192
PeerMinRsaKeySize: 1024
ServerScsv: Off
TTLSTGskAdvancedParms:
TTLSTGskHttpCdpParms:
HttpCdpEnable: Off
HttpCdpProxyServerPort: 80
HttpCdpResponseTimeout: 15
HttpCdpMaxResponseSize: 204800
HttpCdpCacheSize: 32
HttpCdpCacheEntryMaxsize: 0
TTLSTGskOcspParms:
OcspAiaEnable: Off
OcspProxyServerPort: 80
OcspRetrieveViaGet: Off
OcspUrlPriority: On
OcspRequestSigalg:
0401 TLS_SIGALG_SHA256_WITH_RSA
OcspClientCacheSize: 256
OcspCliCacheEntryMaxsize: 0

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

OcspNonceGenEnable: Off
OcspNonceCheckEnable: Off
OcspNonceSize: 8
OcspResponseTimeout: 15
OcspMaxResponseSize: 20480
OcspServerStapling: Off
EnvironmentUserInstance: 0
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TTLS Action: cAct3~TN3270DiffKeyring
Version: 3
Status: Active
Scope: Connection
HandshakeRole: ServerWithClientAuth
CtracedClearText: Off
Trace: 2
TTLSConnectionAdvancedParms:
SecondaryMap: Off
SSLv3: On
TLSv1: On
TLSv1.1: On
TLSv1.2: On
ApplicationControlled: On
TTLSCipherParms:
v3CipherSuites:
000A TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F TLS_RSA_WITH_AES_128_CBC_SHA
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

policyRule: NSS_Client-IKED~4
Rule Type: TTLS
Version: 3
Weight: 252
Priority: 252
No. Policy Action: 3
Status: Active
ForLoadDist: False
Sequence Actions: Don't Care
policyAction: gAct1
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct4~NSS-Client
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct4~NSS-Client
ActionType: TTLS Connection
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00
Fr TimeOfDay UTC: 04:00
To TimeOfDay: 24:00
To TimeOfDay UTC: 04:00
TimeZone: Local

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TTLS Condition Summary: NegativeIndicator: Off
Local Address:
FromAddr: All
ToAddr: All
Remote Address:
FromAddr: All
ToAddr: All
LocalPortFrom: 1024 LocalPortTo: 65535
RemotePortFrom: 4159 RemotePortTo: 4159
JobName: UserId:
ServiceDirection: Outbound
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TTLS Action: gAct1
Version: 3
Status: Active
Scope: Group
TTLSEnabled: On
CtraceClearText: Off
Trace: 2
FIPS140: Off
TTLSGroupAdvancedParms:
SecondaryMap: Off
SyslogFacility: Daemon
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TTLS Action: eAct4~NSS-Client
Version: 3
Status: Active
Scope: Environment
HandshakeRole: Client
SuiteBProfile: Off
TTLSKeyringParms:
Keyring: *AUTH*/
TTLSEnvironmentAdvancedParms:
SSLv2: Off
SSLv3: Off
TLSv1: On
TLSv1.1: On
TLSv1.2: Off
ApplicationControlled: Off
HandshakeTimeout: 10
ClientAuthType: Required
ResetCipherTimer: 0
TruncatedHMAC: Off
CertValidationMode: Any
ServerMaxSSLFragment: Off
ClientMaxSSLFragment: Off
ServerHandshakeSNI: Off
ClientHandshakeSNI: Off
Renegotiation: Default
RenegotiationIndicator: Optional
RenegotiationCertCheck: Off
3DesKeyCheck: Off
ClientEDHGroupSize: Legacy

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

ServerEDHGroupSize: Legacy
PeerMinCertVersion: Any
PeerMinDHKeySize: 1024
PeerMinDsaKeySize: 1024
PeerMinECCKeySize: 192
PeerMinRsaKeySize: 1024
ServerScsv: Off

TTLSGskAdvancedParms:

TTLSGskHttpCdpParms:

HttpCdpEnable: Off
HttpCdpProxyServerPort: 80
HttpCdpResponseTimeout: 15
HttpCdpMaxResponseSize: 204800
HttpCdpCacheSize: 32
HttpCdpCacheEntryMaxsize: 0

TTLSGskOcspParms:

OcspAiaEnable: Off
OcspProxyServerPort: 80
OcspRetrieveViaGet: Off
OcspUrlPriority: On
OcspRequestSigalg:
 0401 TLS_SIGALG_SHA256_WITH_RSA
OcspClientCacheSize: 256
OcspCliCacheEntryMaxsize: 0
OcspNonceGenEnable: Off
OcspNonceCheckEnable: Off
OcspNonceSize: 8
OcspResponseTimeout: 15
OcspMaxResponseSize: 20480
OcspServerStapling: Off

EnvironmentUserInstance: 0

Policy created: Mon May 21 20:08:24 2018

Policy updated: Mon May 21 20:08:24 2018

TTLS Action: cAct4~NSS-Client

Version: 3
Status: Active
Scope: Connection
HandshakeRole: Client
CtracedClearText: Off
Trace: 2

TTLSConnectionAdvancedParms:

SecondaryMap: Off
SSLv3: On
TLSv1: On
TLSv1.1: On
TLSv1.2: Off
ApplicationControlled: On

TTLSCipherParms:

v3CipherSuites:

0035 TLS_RSA_WITH_AES_256_CBC_SHA
0039 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0037 TLS_DH_RSA_WITH_AES_256_CBC_SHA
0038 TLS_DHE_DSS_WITH_AES_256_CBC_SHA
0036 TLS_DH_DSS_WITH_AES_256_CBC_SHA
000A TLS_RSA_WITH_3DES_EDE_CBC_SHA
0016 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

0010 TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
0013 TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
000D TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
002F TLS_RSA_WITH_AES_128_CBC_SHA
0033 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
0031 TLS_DH_RSA_WITH_AES_128_CBC_SHA
0032 TLS_DHE_DSS_WITH_AES_128_CBC_SHA
0030 TLS_DH_DSS_WITH_AES_128_CBC_SHA
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

policyRule: NSS_Server~5
Rule Type: TTLS
Version: 3 Status: Active
Weight: 251 ForLoadDist: False
Priority: 251 Sequence Actions: Don't Care
No. Policy Action: 3
policyAction: gAct1
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct5~NSSD
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct5~NSSD
ActionType: TTLS Connection
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
TTLS Condition Summary: NegativeIndicator: Off
Local Address:
FromAddr: All
ToAddr: All
Remote Address:
FromAddr: All
ToAddr: All
LocalPortFrom: 4159 LocalPortTo: 4159
RemotePortFrom: 1024 RemotePortTo: 65535
JobName: UserId:
ServiceDirection: Inbound
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TTLS Action: gAct1
Version: 3
Status: Active
Scope: Group
TTLS Enabled: On
CtracedClearText: Off

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Trace: 2
FIPS140: Off
TLSGroupAdvancedParms:
 SecondaryMap: Off
 SyslogFacility: Daemon
Policy created: Mon May 21 16:01:28 2018
Policy updated: Mon May 21 16:01:28 2018

TLS Action: eAct5~NSSD
Version: 3
Status: Active
Scope: Environment
HandshakeRole: Server
SuiteBProfile: Off
TLSKeyringParms:
 Keyring: NSSD/NSSD7Ring
TLSEnvironmentAdvancedParms:
 SSLv2: Off
 SSLv3: Off
 TLSv1: On
 TLSv1.1: On
 TLSv1.2: Off
 ApplicationControlled: Off
 HandshakeTimeout: 10
 ClientAuthType: Required
 ResetCipherTimer: 0
 TruncatedHMAC: Off
 CertValidationMode: Any
 ServerMaxSSLFragment: Off
 ClientMaxSSLFragment: Off
 ServerHandshakeSNI: Off
 ClientHandshakeSNI: Off
 Renegotiation: Default
 RenegotiationIndicator: Optional
 RenegotiationCertCheck: Off
 3DesKeyCheck: Off
 ClientEDHGroupSize: Legacy
 ServerEDHGroupSize: Legacy
 PeerMinCertVersion: Any
 PeerMinDHKeySize: 1024
 PeerMinDsaKeySize: 1024
 PeerMinECCKeySize: 192
 PeerMinRsaKeySize: 1024
 ServerScsv: Off
TLSGskAdvancedParms:
 TLSGskHttpCdpParms:
 HttpCdpEnable: Off
 HttpCdpProxyServerPort: 80
 HttpCdpResponseTimeout: 15
 HttpCdpMaxResponseSize: 204800
 HttpCdpCacheSize: 32
 HttpCdpCacheEntryMaxsize: 0
 TLSGskOcspParms:
 OcspAiaEnable: Off
 OcspProxyServerPort: 80
 OcspRetrieveViaGet: Off
 OcspUrlPriority: On

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

OcspRequestSigalg:
0401 TLS_SIGALG_SHA256_WITH_RSA
OcspClientCacheSize: 256
OcspCliCacheEntryMaxsize: 0
OcspNonceGenEnable: Off
OcspNonceCheckEnable: Off
OcspNonceSize: 8
OcspResponseTimeout: 15
OcspMaxResponseSize: 20480
OcspServerStapling: Off
EnvironmentUserInstance: 0
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TTLS Action: cAct5~NSSD
Version: 3
Status: Active
Scope: Connection
HandshakeRole: Server
CtracedClearText: Off
Trace: 2
TTLSConnectionAdvancedParms:
SecondaryMap: Off
SSLv3: On
TLSv1: On
TLSv1.1: On
TLSv1.2: Off
ApplicationControlled: On
TTLSCipherParms:
v3CipherSuites:
0035 TLS_RSA_WITH_AES_256_CBC_SHA
0039 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0037 TLS_DH_RSA_WITH_AES_256_CBC_SHA
0038 TLS_DHE_DSS_WITH_AES_256_CBC_SHA
0036 TLS_DH_DSS_WITH_AES_256_CBC_SHA
000A TLS_RSA_WITH_3DES_EDE_CBC_SHA
0016 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
0010 TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
0013 TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
000D TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
002F TLS_RSA_WITH_AES_128_CBC_SHA
0033 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
0031 TLS_DH_RSA_WITH_AES_128_CBC_SHA
0032 TLS_DHE_DSS_WITH_AES_128_CBC_SHA
0030 TLS_DH_DSS_WITH_AES_128_CBC_SHA
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

policyRule: NSS~TLS~CLIENT~1
Rule Type: TTLS
Version: 3
Weight: 1
Priority: 1
No. Policy Action: 2
policyAction: NSS~TLS~ON
ActionType: TTLS Group
Action Sequence: 0
Status: Active
ForLoadDist: False
Sequence Actions: Don't Care

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

policyAction: NSS~TLS~CLIENT~ENV
ActionType: TTLS Environment
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
TTLS Condition Summary: NegativeIndicator: Off
Local Address:
FromAddr: All
ToAddr: All
Remote Address:
FromAddr: All
ToAddr: All
LocalPortFrom: 0 LocalPortTo: 0
RemotePortFrom: 4159 RemotePortTo: 4159
JobName: UserId:
ServiceDirection: Outbound
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TTLS Action: NSS~TLS~ON
Version: 3
Status: Active
Scope: Group
TTLSEnabled: On
CtraceClearText: Off
Trace: 2
FIPS140: Off
TTLSGroupAdvancedParms:
SecondaryMap: Off
SyslogFacility: Daemon
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TTLS Action: NSS~TLS~CLIENT~ENV
Version: 3
Status: Active
Scope: Environment
HandshakeRole: Client
SuiteBProfile: Off
TTLSKeyringParms:
Keyring: *AUTH*/
TTLSEnvironmentAdvancedParms:
SSLv2: Off
SSLv3: Off
TLSv1: On
TLSv1.1: On
TLSv1.2: Off
ApplicationControlled: Off

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
HandshakeTimeout:      10
ClientAuthType:        Required
ResetCipherTimer:      0
TruncatedHMAC:          Off
CertValidationMode:    Any
ServerMaxSSLFragment:  Off
ClientMaxSSLFragment:  Off
ServerHandshakeSNI:    Off
ClientHandshakeSNI:    Off
Renegotiation:         Default
RenegotiationIndicator: Optional
RenegotiationCertCheck: Off
3DesKeyCheck:          Off
ClientEDHGroupSize:    Legacy
ServerEDHGroupSize:    Legacy
PeerMinCertVersion:    Any
PeerMinDHKeySize:      1024
PeerMinDsaKeySize:     1024
PeerMinECCKeySize:     192
PeerMinRsaKeySize:     1024
ServerScsv:            Off
TTLSCipherParms:
  v3CipherSuites:
    000A  TLS_RSA_WITH_3DES_EDE_CBC_SHA
TTLSGskAdvancedParms:
  TTLSGskHttpCdpParms:
    HttpCdpEnable:      Off
    HttpCdpProxyServerPort: 80
    HttpCdpResponseTimeout: 15
    HttpCdpMaxResponseSize: 204800
    HttpCdpCacheSize:   32
    HttpCdpCacheEntryMaxsize: 0
  TTLSGskOcspParms:
    OcspAiaEnable:      Off
    OcspProxyServerPort: 80
    OcspRetrieveViaGet:  Off
    OcspUrlPriority:     On
    OcspRequestSigalg:
      0401  TLS_SIGALG_SHA256_WITH_RSA
    OcspClientCacheSize: 256
    OcspCliCacheEntryMaxsize: 0
    OcspNonceGenEnable:  Off
    OcspNonceCheckEnable: Off
    OcspNonceSize:      8
    OcspResponseTimeout: 15
    OcspMaxResponseSize: 20480
    OcspServerStapling:  Off
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018
```

```
policyRule:      NSS~TLS~SERVER
Rule Type:       TTLS
Version:         3
Weight:          1
Priority:         1
No. Policy Action: 2
policyAction:    NSS~TLS~ON
Status:          Active
ForLoadDist:     False
Sequence Actions: Don't Care
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

ActionType: TLS Group
Action Sequence: 0
policyAction: NSS~TLS~SERVER~ENV
ActionType: TLS Environment
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 1111111111
Day of Week Mask: 111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 04:00 To TimeOfDay UTC: 04:00
TimeZone: Local
TLS Condition Summary: NegativeIndicator: Off
Local Address:
FromAddr: All
ToAddr: All
Remote Address:
FromAddr: All
ToAddr: All
LocalPortFrom: 4159 LocalPortTo: 4159
RemotePortFrom: 0 RemotePortTo: 0
JobName: UserId:
ServiceDirection: Inbound
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TLS Action: NSS~TLS~ON
Version: 3
Status: Active
Scope: Group
TLSEnabled: On
CtraceClearText: Off
Trace: 2
FIPS140: Off
TLSSGroupAdvancedParms:
SecondaryMap: Off
SyslogFacility: Daemon
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018

TLS Action: NSS~TLS~SERVER~ENV
Version: 3
Status: Active
Scope: Environment
HandshakeRole: Server
SuiteBProfile: Off
TLSKeyringParms:
Keyring: NSSD/NSSD7Ring
TLSEnvironmentAdvancedParms:
SSLv2: Off
SSLv3: Off
TLSv1: On
TLSv1.1: On

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

    TLSv1.2:                               Off
    ApplicationControlled:                 Off
    HandshakeTimeout:                      10
    ClientAuthType:                        Required
    ResetCipherTimer:                      0
    TruncatedHMAC:                         Off
    CertValidationMode:                    Any
    ServerMaxSSLFragment:                  Off
    ClientMaxSSLFragment:                  Off
    ServerHandshakeSNI:                    Off
    ClientHandshakeSNI:                    Off
    Renegotiation:                         Default
    RenegotiationIndicator:                 Optional
    RenegotiationCertCheck:                Off
    3DesKeyCheck:                          Off
    ClientEDHGroupSize:                    Legacy
    ServerEDHGroupSize:                    Legacy
    PeerMinCertVersion:                    Any
    PeerMinDHKeySize:                      1024
    PeerMinDsaKeySize:                      1024
    PeerMinECCKeySize:                     192
    PeerMinRsaKeySize:                      1024
    ServerScsv:                            Off
TTLSCipherParms:
    v3CipherSuites:
        000A  TLS_RSA_WITH_3DES_EDE_CBC_SHA
TTLSGskAdvancedParms:
    TTLSGskHttpCdpParms:
        HttpCdpEnable:                     Off
        HttpCdpProxyServerPort:             80
        HttpCdpResponseTimeout:             15
        HttpCdpMaxResponseSize:             204800
        HttpCdpCacheSize:                   32
        HttpCdpCacheEntryMaxsize:           0
    TTLSGskOcspParms:
        OcspAiaEnable:                      Off
        OcspProxyServerPort:                80
        OcspRetrieveViaGet:                  Off
        OcspUrlPriority:                     On
        OcspRequestSigalg:
            0401  TLS_SIGALG_SHA256_WITH_RSA
        OcspClientCacheSize:                 256
        OcspCliCacheEntryMaxsize:            0
        OcspNonceGenEnable:                  Off
        OcspNonceCheckEnable:                Off
        OcspNonceSize:                       8
        OcspResponseTimeout:                 15
        OcspMaxResponseSize:                 20480
        OcspServerStapling:                  Off
Policy created: Mon May 21 20:08:24 2018
Policy updated: Mon May 21 20:08:24 2018
```

ipsec Command Output

```
# ipsec -f display -p TCPIPT
CS V2R1 ipsec Stack Name: TCPIPT Thu May 14 13:03:28 2015
Primary: Filter Function: Display Format: Detail
Source: Stack Policy Scope: Current TotAvail: 94
Logging: On Predecap: Off DVIPSec: No
NatKeepAlive: 20 FIPS140: No
Defensive Mode: Active
```

```
FilterName: NssTrafficIPv4
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: None
LogLimit: n/a
Protocol: TCP(6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Inbound
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 4159
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/27 20:31:04
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

MIPv6TypeGranularity:      n/a
TypeRange:                  n/a
CodeRange:                  n/a
RemoteIdentityType:         n/a
RemoteIdentity:              n/a
FragmentsOnly:              No
FilterMatches:               0
LifetimeExpires:            n/a
AssociatedStackCount:        n/a
*****
FilterName:                  NssTrafficIPv4
FilterNameExtension:         2
GroupName:                   n/a
LocalStartActionName:        n/a
VpnActionName:               n/a
TunnelID:                    0x00
Type:                        Generic
DefensiveType:               n/a
State:                       Active
Action:                       Permit
Scope:                        Local
Direction:                   Inbound
OnDemand:                    n/a
SecurityClass:                0
Logging:                      None
LogLimit:                     n/a
Protocol:                     TCP (6)
ICMPType:                     n/a
ICMPTypeGranularity:          n/a
ICMPCode:                     n/a
ICMPCodeGranularity:          n/a
OSPFType:                     n/a
TCPQualifier:                 Connect Inbound
ProtocolGranularity:          n/a
SourceAddress:                0.0.0.0
SourceAddressPrefix:          0
SourceAddressRange:           n/a
SourceAddressGranularity:      n/a
SourcePort:                   1024
SourcePortRange:              65535
SourcePortGranularity:         n/a
DestAddress:                  0.0.0.0
DestAddressPrefix:            0
DestAddressRange:             n/a
DestAddressGranularity:        n/a
DestPort:                     4159
DestPortRange:                n/a
DestPortGranularity:           n/a
OrigRmtConnPort:              n/a
RmtIDPayload:                 n/a
RmtUdpEncapPort:              n/a
CreateTime:                   2015/04/27 20:31:04
UpdateTime:                   2015/04/27 20:31:04
DiscardAction:                 Silent
MIPv6Type:                    n/a
MIPv6TypeGranularity:          n/a
TypeRange:                    n/a

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: NssTrafficIPv4~1
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: None
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: None
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 4159
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/27 20:31:04
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:           0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:              NssTrafficIPv4~1
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                   Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                  None
LogLimit:                n/a
Protocol:                 TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            None
ProtocolGranularity:     n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              4159
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 1024
DestPortRange:           65535
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/27 20:31:04
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:                n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: BetweenOSAsRSA~6
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP (17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 192.168.20.92
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 500
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 192.168.20.91
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 500
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 23
LifetimeExpires: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
AssociatedStackCount:      n/a
*****
FilterName:                BetweenOSAsRSA~6
FilterNameExtension:      2
GroupName:                 n/a
LocalStartActionName:     n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  UDP (17)
ICMPType:                  n/a
ICMPTypeGranularity:      n/a
ICMPCode:                  n/a
ICMPCodeGranularity:      n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:       n/a
SourceAddress:             192.168.20.91
SourceAddressPrefix:       n/a
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                500
SourcePortRange:           n/a
SourcePortGranularity:     n/a
DestAddress:               192.168.20.92
DestAddressPrefix:         n/a
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  500
DestPortRange:             n/a
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:          n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             23
LifetimeExpires:           n/a
AssociatedStackCount:      n/a
*****
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

FilterName:                BetweenOSAsRSA~7
FilterNameExtension:       1
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             VPN~A
TunnelID:                  Y0
Type:                      Dynamic Anchor
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Outbound
OnDemand:                  Yes
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  TCP(6)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              Connect Outbound
ProtocolGranularity:       Rule
SourceAddress:             192.168.20.92
SourceAddressPrefix:       n/a
SourceAddressRange:        n/a
SourceAddressGranularity:  Packet
SourcePort:                1024
SourcePortRange:           65535
SourcePortGranularity:     Rule
DestAddress:               192.168.20.91
DestAddressPrefix:         n/a
DestAddressRange:          n/a
DestAddressGranularity:    Packet
DestPort:                  21
DestPortRange:             n/a
DestPortGranularity:       Rule
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:          n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:              Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:             No
FilterMatches:              57
LifetimeExpires:           n/a
AssociatedStackCount:       n/a
*****
FilterName:                BetweenOSAsRSA~7
FilterNameExtension:       2

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: VPN~A
TunnelID: Y0
Type: Dynamic Anchor
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: Yes
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP(6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: Rule
SourceAddress: 192.168.20.91
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: 21
SourcePortRange: n/a
SourcePortGranularity: Rule
DestAddress: 192.168.20.92
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: Packet
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: Rule
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 44
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: BetweenOSAsRSA~9
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: BetweenOSAsRSA~8
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

VpnActionName:      VPN~A
TunnelID:           Y0
Type:               Dynamic Anchor
DefensiveType:      n/a
State:              Active
Action:              Permit
Scope:              Local
Direction:          Outbound
OnDemand:           No
SecurityClass:      0
Logging:             All
LogLimit:           n/a
Protocol:            TCP(6)
ICMPType:           n/a
ICMPTypeGranularity: n/a
ICMPCode:           n/a
ICMPCodeGranularity: n/a
OSPFType:           n/a
TCPQualifier:        Connect Inbound
ProtocolGranularity: Rule
SourceAddress:       192.168.20.92
SourceAddressPrefix: n/a
SourceAddressRange:  n/a
SourceAddressGranularity: Packet
SourcePort:          1024
SourcePortRange:     65535
SourcePortGranularity: Rule
DestAddress:         192.168.20.91
DestAddressPrefix:   n/a
DestAddressRange:    n/a
DestAddressGranularity: Packet
DestPort:            20
DestPortRange:       n/a
DestPortGranularity: Rule
OrigRmtConnPort:     n/a
RmtIDPayload:        n/a
RmtUdpEncapPort:     n/a
CreateTime:          2015/04/21 21:08:43
UpdateTime:          2015/04/27 20:31:04
DiscardAction:        Silent
MIPv6Type:           n/a
MIPv6TypeGranularity: n/a
TypeRange:           n/a
CodeRange:           n/a
RemoteIdentityType:  n/a
RemoteIdentity:      n/a
FragmentsOnly:       No
FilterMatches:        0
LifetimeExpires:     n/a
AssociatedStackCount: n/a
*****
FilterName:           BetweenOSAsRSA~9
FilterNameExtension:  2
GroupName:            n/a
LocalStartActionName: BetweenOSAsRSA~8
VpnActionName:        VPN~A
TunnelID:             Y0

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Type: Dynamic Anchor
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: No
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP(6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Inbound
ProtocolGranularity: Rule
SourceAddress: 192.168.20.91
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: 20
SourcePortRange: n/a
SourcePortGranularity: Rule
DestAddress: 192.168.20.92
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: Packet
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: Rule
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: BetweenOSAsRSA~10
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: VPN~A
TunnelID: Y0
Type: Dynamic Anchor
DefensiveType: n/a

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: Yes
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: Rule
SourceAddress: 192.168.20.92
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: Rule
DestAddress: 192.168.20.91
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: Packet
DestPort: 50000
DestPortRange: 50200
DestPortGranularity: Rule
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: BetweenOSAsRSA~10
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: VPN~A
TunnelID: Y0
Type: Dynamic Anchor
DefensiveType: n/a
State: Active
Action: Permit
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Scope: Local
Direction: Inbound
OnDemand: Yes
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: Rule
SourceAddress: 192.168.20.91
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: 50000
SourcePortRange: 50200
SourcePortGranularity: Rule
DestAddress: 192.168.20.92
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: Packet
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: Rule
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: BetweenOSAsRSA~12
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: BetweenOSAsRSA~8
VpnActionName: VPN~A
TunnelID: Y0
Type: Dynamic Anchor
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
OnDemand:                No
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 TCP(6)
ICMPType:                 n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:             Connect Inbound
ProtocolGranularity:     Rule
SourceAddress:            192.168.20.92
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: Packet
SourcePort:               21
SourcePortRange:         n/a
SourcePortGranularity:   Rule
DestAddress:              192.168.20.91
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  Packet
DestPort:                 1024
DestPortRange:           65535
DestPortGranularity:     Rule
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:    n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:      n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               BetweenOSAsRSA~12
FilterNameExtension:      2
GroupName:                n/a
LocalStartActionName:     BetweenOSAsRSA~8
VpnActionName:            VPN~A
TunnelID:                 Y0
Type:                     Dynamic Anchor
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Inbound
OnDemand:                 No
SecurityClass:            0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Inbound
ProtocolGranularity: Rule
SourceAddress: 192.168.20.91
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: Rule
DestAddress: 192.168.20.92
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: Packet
DestPort: 21
DestPortRange: n/a
DestPortGranularity: Rule
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: BetweenOSAsRSA~13
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: VPN~A
TunnelID: Y0
Type: Dynamic Anchor
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: Yes
SecurityClass: 0
Logging: All
LogLimit: n/a

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Protocol:                TCP (6)
ICMPType:                n/a
ICMPTypeGranularity:    n/a
ICMPCode:                n/a
ICMPCodeGranularity:    n/a
OSPFType:                n/a
TCPQualifier:            Connect Outbound
ProtocolGranularity:    Rule
SourceAddress:            192.168.20.92
SourceAddressPrefix:    n/a
SourceAddressRange:      n/a
SourceAddressGranularity: Packet
SourcePort:              20
SourcePortRange:         n/a
SourcePortGranularity:   Rule
DestAddress:              192.168.20.91
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  Packet
DestPort:                 1024
DestPortRange:           65535
DestPortGranularity:     Rule
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:   n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:    n/a
*****
FilterName:               BetweenOSAsRSA~13
FilterNameExtension:      2
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            VPN~A
TunnelID:                 Y0
Type:                     Dynamic Anchor
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Inbound
OnDemand:                 Yes
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 TCP (6)
ICMPType:                 n/a

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ICMPTypeGranularity:    n/a
ICMPCode:               n/a
ICMPCodeGranularity:   n/a
OSPFTYPE:               n/a
TCPQualifier:           Connect Outbound
ProtocolGranularity:    Rule
SourceAddress:          192.168.20.91
SourceAddressPrefix:    n/a
SourceAddressRange:     n/a
SourceAddressGranularity: Packet
SourcePort:             1024
SourcePortRange:        65535
SourcePortGranularity:  Rule
DestAddress:            192.168.20.92
DestAddressPrefix:      n/a
DestAddressRange:       n/a
DestAddressGranularity: Packet
DestPort:               20
DestPortRange:          n/a
DestPortGranularity:    Rule
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:          No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:   n/a
*****
FilterName:              BetweenOSAsRSA~15
FilterNameExtension:     1
GroupName:               n/a
LocalStartActionName:    BetweenOSAsRSA~8
VpnActionName:           VPN~A
TunnelID:                Y0
Type:                    Dynamic Anchor
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Outbound
OnDemand:                No
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                 TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ICMPCodeGranularity:      n/a
OSPFTYPE:                 n/a
TCPQualifier:             Connect Inbound
ProtocolGranularity:      Rule
SourceAddress:            192.168.20.92
SourceAddressPrefix:      n/a
SourceAddressRange:       n/a
SourceAddressGranularity: Packet
SourcePort:               50000
SourcePortRange:          50200
SourcePortGranularity:    Rule
DestAddress:              192.168.20.91
DestAddressPrefix:        n/a
DestAddressRange:         n/a
DestAddressGranularity:   Packet
DestPort:                 1024
DestPortRange:            65535
DestPortGranularity:      Rule
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
FilterName:                BetweenOSAsRSA~15
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:      BetweenOSAsRSA~8
VpnActionName:             VPN~A
TunnelID:                  Y0
Type:                      Dynamic Anchor
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  No
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  TCP (6)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFTYPE:                  n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TCPQualifier:	Connect Inbound
ProtocolGranularity:	Rule
SourceAddress:	192.168.20.91
SourceAddressPrefix:	n/a
SourceAddressRange:	n/a
SourceAddressGranularity:	Packet
SourcePort:	1024
SourcePortRange:	65535
SourcePortGranularity:	Rule
DestAddress:	192.168.20.92
DestAddressPrefix:	n/a
DestAddressRange:	n/a
DestAddressGranularity:	Packet
DestPort:	50000
DestPortRange:	50200
DestPortGranularity:	Rule
OrigRmtConnPort:	n/a
RmtIDPayload:	n/a
RmtUdpEncapPort:	n/a
CreateTime:	2015/04/21 21:08:43
UpdateTime:	2015/04/27 20:31:04
DiscardAction:	Silent
MIPv6Type:	n/a
MIPv6TypeGranularity:	n/a
TypeRange:	n/a
CodeRange:	n/a
RemoteIdentityType:	n/a
RemoteIdentity:	n/a
FragmentsOnly:	No
FilterMatches:	0
LifetimeExpires:	n/a
AssociatedStackCount:	n/a

FilterName:	TrafficBetweenVIPAs~3
FilterNameExtension:	1
GroupName:	n/a
LocalStartActionName:	n/a
VpnActionName:	n/a
TunnelID:	0x00
Type:	Generic
DefensiveType:	n/a
State:	Active
Action:	Permit
Scope:	Local
Direction:	Outbound
OnDemand:	n/a
SecurityClass:	0
Logging:	All
LogLimit:	n/a
Protocol:	TCP(6)
ICMPType:	n/a
ICMPTypeGranularity:	n/a
ICMPCode:	n/a
ICMPCodeGranularity:	n/a
OSPFType:	n/a
TCPQualifier:	Connect Inbound
ProtocolGranularity:	n/a

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourceAddress:          192.168.20.102
SourceAddressPrefix:    n/a
SourceAddressRange:     n/a
SourceAddressGranularity: n/a
SourcePort:             3000
SourcePortRange:        n/a
SourcePortGranularity:  n/a
DestAddress:            192.168.20.101
DestAddressPrefix:      n/a
DestAddressRange:       n/a
DestAddressGranularity: n/a
DestPort:               1024
DestPortRange:          65535
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:         No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:              TrafficBetweenVIPAs~3
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:              Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:           192.168.20.101
SourceAddressPrefix:     n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              1024
SourcePortRange:         65535
SourcePortGranularity:   n/a
DestAddress:             192.168.20.102
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                3000
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               TrafficBetweenVIPAs~4
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                Outbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  TCP (6)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              Connect Outbound
ProtocolGranularity:       n/a
SourceAddress:             192.168.20.102
SourceAddressPrefix:       n/a
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 192.168.20.101
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 21
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: TrafficBetweenVIPAs~4
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: n/a
SourceAddress: 192.168.20.101
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 21
SourcePortRange: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortGranularity:    n/a
DestAddress:              192.168.20.102
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                1024
DestPortRange:           65535
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:        n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:    n/a
*****
FilterName:              TrafficBetweenVIPAs~5
FilterNameExtension:     1
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Outbound
OnDemand:                n/a
SecurityClass:           0
Logging:                  All
LogLimit:                n/a
Protocol:                 TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:            192.168.20.102
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              1024
SourcePortRange:         65535
SourcePortGranularity:   n/a
DestAddress:              192.168.20.101
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestAddressPrefix:      n/a
DestAddressRange:       n/a
DestAddressGranularity: n/a
DestPort:               20
DestPortRange:          n/a
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:          No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:              TrafficBetweenVIPAs~5
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                  All
LogLimit:                 n/a
Protocol:                 TCP(6)
ICMPType:                 n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:           192.168.20.101
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              20
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             192.168.20.102
DestAddressPrefix:       n/a
DestAddressRange:        n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestAddressGranularity:    n/a
DestPort:                  1024
DestPortRange:             65535
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:           n/a
AssociatedStackCount:       n/a
*****
FilterName:                TrafficBetweenVIPAs~6
FilterNameExtension:       1
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Outbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  TCP(6)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              Connect Outbound
ProtocolGranularity:       n/a
SourceAddress:              192.168.20.102
SourceAddressPrefix:       n/a
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                1024
SourcePortRange:           65535
SourcePortGranularity:     n/a
DestAddress:               192.168.20.101
DestAddressPrefix:         n/a
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  50000
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestPortRange:          50200
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:          No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:             TrafficBetweenVIPAs~6
FilterNameExtension:     2
GroupName:              n/a
LocalStartActionName:    n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:              Inbound
OnDemand:               n/a
SecurityClass:          0
Logging:                 All
LogLimit:                n/a
Protocol:                TCP (6)
ICMPType:               n/a
ICMPTypeGranularity:    n/a
ICMPCode:                n/a
ICMPCodeGranularity:    n/a
OSPFType:               n/a
TCPQualifier:            Connect Outbound
ProtocolGranularity:     n/a
SourceAddress:           192.168.20.101
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              50000
SourcePortRange:         50200
SourcePortGranularity:   n/a
DestAddress:             192.168.20.102
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                1024
DestPortRange:           65535
DestPortGranularity:     n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
OrigRmtConnPort:      n/a
RmtIDPayload:         n/a
RmtUdpEncapPort:      n/a
CreateTime:           2015/04/21 21:08:43
UpdateTime:           2015/04/27 20:31:04
DiscardAction:        Silent
MIPv6Type:            n/a
MIPv6TypeGranularity: n/a
TypeRange:            n/a
CodeRange:            n/a
RemoteIdentityType:   n/a
RemoteIdentity:       n/a
FragmentsOnly:        No
FilterMatches:         0
LifetimeExpires:      n/a
AssociatedStackCount:  n/a
*****
FilterName:           TrafficBetweenVIPAs~7
FilterNameExtension:  1
GroupName:            n/a
LocalStartActionName: n/a
VpnActionName:        n/a
TunnelID:             0x00
Type:                 Generic
DefensiveType:        n/a
State:                Active
Action:               Permit
Scope:                Local
Direction:            Outbound
OnDemand:             n/a
SecurityClass:        0
Logging:              All
LogLimit:             n/a
Protocol:              TCP(6)
ICMPType:             n/a
ICMPTypeGranularity:  n/a
ICMPCode:             n/a
ICMPCodeGranularity:  n/a
OSPFType:             n/a
TCPQualifier:         Connect Inbound
ProtocolGranularity:   n/a
SourceAddress:         192.168.20.102
SourceAddressPrefix:   n/a
SourceAddressRange:    n/a
SourceAddressGranularity: n/a
SourcePort:           21
SourcePortRange:       n/a
SourcePortGranularity: n/a
DestAddress:          192.168.20.101
DestAddressPrefix:     n/a
DestAddressRange:      n/a
DestAddressGranularity: n/a
DestPort:             1024
DestPortRange:         65535
DestPortGranularity:   n/a
OrigRmtConnPort:      n/a
RmtIDPayload:         n/a
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RmtUdpEncapPort:      n/a
CreateTime:           2015/04/21 21:08:43
UpdateTime:           2015/04/27 20:31:04
DiscardAction:        Silent
MIPv6Type:            n/a
MIPv6TypeGranularity: n/a
TypeRange:            n/a
CodeRange:            n/a
RemoteIdentityType:   n/a
RemoteIdentity:       n/a
FragmentsOnly:        No
FilterMatches:         0
LifetimeExpires:      n/a
AssociatedStackCount:  n/a
*****
FilterName:            TrafficBetweenVIPAs~7
FilterNameExtension:   2
GroupName:             n/a
LocalStartActionName:  n/a
VpnActionName:         n/a
TunnelID:              0x00
Type:                  Generic
DefensiveType:         n/a
State:                 Active
Action:                 Permit
Scope:                 Local
Direction:             Inbound
OnDemand:              n/a
SecurityClass:         0
Logging:               All
LogLimit:              n/a
Protocol:              TCP(6)
ICMPType:              n/a
ICMPTypeGranularity:   n/a
ICMPCode:              n/a
ICMPCodeGranularity:   n/a
OSPFType:              n/a
TCPQualifier:          Connect Inbound
ProtocolGranularity:    n/a
SourceAddress:          192.168.20.101
SourceAddressPrefix:    n/a
SourceAddressRange:     n/a
SourceAddressGranularity: n/a
SourcePort:            1024
SourcePortRange:        65535
SourcePortGranularity:  n/a
DestAddress:            192.168.20.102
DestAddressPrefix:      n/a
DestAddressRange:       n/a
DestAddressGranularity: n/a
DestPort:               21
DestPortRange:          n/a
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:             n/a
FragmentsOnly:             No
FilterMatches:              0
LifetimeExpires:           n/a
AssociatedStackCount:       n/a
*****
FilterName:                 TrafficBetweenVIPAs~8
FilterNameExtension:        1
GroupName:                  n/a
LocalStartActionName:       n/a
VpnActionName:              n/a
TunnelID:                   0x00
Type:                       Generic
DefensiveType:              n/a
State:                       Active
Action:                      Permit
Scope:                       Local
Direction:                  Outbound
OnDemand:                   n/a
SecurityClass:              0
Logging:                     All
LogLimit:                   n/a
Protocol:                   TCP(6)
ICMPType:                   n/a
ICMPTypeGranularity:        n/a
ICMPCode:                   n/a
ICMPCodeGranularity:        n/a
OSPFType:                   n/a
TCPQualifier:               Connect Outbound
ProtocolGranularity:        n/a
SourceAddress:              192.168.20.102
SourceAddressPrefix:        n/a
SourceAddressRange:         n/a
SourceAddressGranularity:   n/a
SourcePort:                 20
SourcePortRange:            n/a
SourcePortGranularity:      n/a
DestAddress:                192.168.20.101
DestAddressPrefix:          n/a
DestAddressRange:           n/a
DestAddressGranularity:     n/a
DestPort:                   1024
DestPortRange:              65535
DestPortGranularity:        n/a
OrigRmtConnPort:            n/a
RmtIDPayload:               n/a
RmtUdpEncapPort:            n/a
CreateTime:                 2015/04/21 21:08:43
UpdateTime:                 2015/04/27 20:31:04
DiscardAction:              Silent
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: TrafficBetweenVIPAs~8
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: n/a
SourceAddress: 192.168.20.101
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 192.168.20.102
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 20
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:          n/a
AssociatedStackCount:     n/a
*****
FilterName:               TrafficBetweenVIPAs~9
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                  TCP(6)
ICMPType:                 n/a
ICMPTypeGranularity:      n/a
ICMPCode:                 n/a
ICMPCodeGranularity:      n/a
OSPFType:                 n/a
TCPQualifier:             Connect Inbound
ProtocolGranularity:      n/a
SourceAddress:            192.168.20.102
SourceAddressPrefix:      n/a
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               50000
SourcePortRange:          50200
SourcePortGranularity:    n/a
DestAddress:              192.168.20.101
DestAddressPrefix:        n/a
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 1024
DestPortRange:            65535
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:         n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:    n/a
*****
FilterName:              TrafficBetweenVIPAs~9
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                 TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:           192.168.20.101
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              1024
SourcePortRange:         65535
SourcePortGranularity:   n/a
DestAddress:             192.168.20.102
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                50000
DestPortRange:           50200
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:                n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FragmentsOnly:          No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:             TrafOSA2DVIPAPreshe~6
FilterNameExtension:     1
GroupName:              n/a
LocalStartActionName:    n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                  Active
Action:                  Permit
Scope:                  Local
Direction:              Outbound
OnDemand:               n/a
SecurityClass:          0
Logging:                 All
LogLimit:               n/a
Protocol:                UDP (17)
ICMPType:               n/a
ICMPTypeGranularity:    n/a
ICMPCode:               n/a
ICMPCodeGranularity:    n/a
OSPFType:               n/a
TCPQualifier:           n/a
ProtocolGranularity:    n/a
SourceAddress:           192.168.20.92
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              500
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             192.168.20.121
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                500
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:          0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
LifetimeExpires:          n/a
AssociatedStackCount:     n/a
*****
FilterName:              TrafOSA2DVIPAPreshe~6
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                   Generic
DefensiveType:           n/a
State:                  Active
Action:                 Permit
Scope:                 Local
Direction:             Inbound
OnDemand:              n/a
SecurityClass:          0
Logging:               All
LogLimit:              n/a
Protocol:              UDP (17)
ICMPType:              n/a
ICMPTypeGranularity:   n/a
ICMPCode:              n/a
ICMPCodeGranularity:   n/a
OSPFType:              n/a
TCPQualifier:          n/a
ProtocolGranularity:    n/a
SourceAddress:          192.168.20.121
SourceAddressPrefix:    n/a
SourceAddressRange:     n/a
SourceAddressGranularity: n/a
SourcePort:            500
SourcePortRange:        n/a
SourcePortGranularity:  n/a
DestAddress:            192.168.20.92
DestAddressPrefix:      n/a
DestAddressRange:       n/a
DestAddressGranularity: n/a
DestPort:              500
DestPortRange:          n/a
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:         No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
*****
FilterName:                      TrafOSA2DVIPAPreshe~8
FilterNameExtension:             1
GroupName:                       n/a
LocalStartActionName:           TrafOSA2DVIPAPreshe~7
VpnActionName:                  VPN~A~6
TunnelID:                       Y0
Type:                           Dynamic Anchor
DefensiveType:                  n/a
State:                           Active
Action:                         Permit
Scope:                          Routed
Direction:                      Outbound
OnDemand:                       Yes
SecurityClass:                   0
Logging:                         All
LogLimit:                       n/a
Protocol:                       All
ICMPType:                       n/a
ICMPTypeGranularity:            n/a
ICMPCode:                       n/a
ICMPCodeGranularity:            n/a
OSPFType:                       n/a
TCPQualifier:                   n/a
ProtocolGranularity:            Rule
SourceAddress:                   192.168.20.122
SourceAddressPrefix:            n/a
SourceAddressRange:             n/a
SourceAddressGranularity:       Packet
SourcePort:                     n/a
SourcePortRange:                n/a
SourcePortGranularity:          n/a
DestAddress:                     192.168.20.121
DestAddressPrefix:              n/a
DestAddressRange:               n/a
DestAddressGranularity:         Packet
DestPort:                       n/a
DestPortRange:                  n/a
DestPortGranularity:            n/a
OrigRmtConnPort:                n/a
RmtIDPayload:                   n/a
RmtUdpEncapPort:                n/a
CreateTime:                     2015/04/21 21:08:43
UpdateTime:                     2015/04/27 20:31:04
DiscardAction:                   Silent
MIPv6Type:                      n/a
MIPv6TypeGranularity:           n/a
TypeRange:                      n/a
CodeRange:                      n/a
RemoteIdentityType:             n/a
RemoteIdentity:                 n/a
FragmentsOnly:                  No
FilterMatches:                   0
LifetimeExpires:                 n/a
AssociatedStackCount:            n/a
*****
FilterName:                      TrafOSA2DVIPAPreshe~8
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FilterNameExtension:      2
GroupName:                n/a
LocalStartActionName:    TrafOSA2DVIPAPreshe~7
VpnActionName:           VPN~A~6
TunnelID:                Y0
Type:                    Dynamic Anchor
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Routed
Direction:               Inbound
OnDemand:                Yes
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                All
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            n/a
ProtocolGranularity:     Rule
SourceAddress:            192.168.20.121
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: Packet
SourcePort:              n/a
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             192.168.20.122
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  Packet
DestPort:                n/a
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:              WorkstationtoVIPA~2
FilterNameExtension:     1
GroupName:               n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                   Permit
Scope:                   Local
Direction:               Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 TCP(6)
ICMPType:                 n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:             Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:            192.168.20.102
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:               21
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 1024
DestPortRange:           65535
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:         n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:    n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:            No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:                WorkstationtoVIPA~2
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              1024
SourcePortRange:         65535
SourcePortGranularity:   n/a
DestAddress:             192.168.20.102
DestAddressPrefix:       n/a
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                21
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:       n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               WorkstationtoVIP~3
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DefensiveType:      n/a
State:              Active
Action:             Permit
Scope:              Local
Direction:          Outbound
OnDemand:           n/a
SecurityClass:      0
Logging:            All
LogLimit:           n/a
Protocol:           TCP (6)
ICMPType:           n/a
ICMPTypeGranularity: n/a
ICMPCode:           n/a
ICMPCodeGranularity: n/a
OSPFType:           n/a
TCPQualifier:       Connect Outbound
ProtocolGranularity: n/a
SourceAddress:       192.168.20.102
SourceAddressPrefix: n/a
SourceAddressRange:  n/a
SourceAddressGranularity: n/a
SourcePort:         20
SourcePortRange:    n/a
SourcePortGranularity: n/a
DestAddress:         0.0.0.0
DestAddressPrefix:   0
DestAddressRange:    n/a
DestAddressGranularity: n/a
DestPort:           1024
DestPortRange:       65535
DestPortGranularity: n/a
OrigRmtConnPort:     n/a
RmtIDPayload:        n/a
RmtUdpEncapPort:     n/a
CreateTime:          2015/04/21 21:08:43
UpdateTime:          2015/04/27 20:31:04
DiscardAction:       Silent
MIPv6Type:           n/a
MIPv6TypeGranularity: n/a
TypeRange:           n/a
CodeRange:           n/a
RemoteIdentityType:  n/a
RemoteIdentity:       n/a
FragmentsOnly:       No
FilterMatches:        0
LifetimeExpires:     n/a
AssociatedStackCount: n/a
*****
FilterName:          WorkstationtoVIPa~3
FilterNameExtension: 2
GroupName:           n/a
LocalStartActionName: n/a
VpnActionName:        n/a
TunnelID:            0x00
Type:                Generic
DefensiveType:       n/a
State:               Active
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 192.168.20.102
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 20
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: WorkstationtoVIP~4
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Direction:	Outbound
OnDemand:	n/a
SecurityClass:	0
Logging:	All
LogLimit:	n/a
Protocol:	TCP(6)
ICMPType:	n/a
ICMPTypeGranularity:	n/a
ICMPCode:	n/a
ICMPCodeGranularity:	n/a
OSPFType:	n/a
TCPQualifier:	Connect Inbound
ProtocolGranularity:	n/a
SourceAddress:	192.168.20.102
SourceAddressPrefix:	n/a
SourceAddressRange:	n/a
SourceAddressGranularity:	n/a
SourcePort:	50000
SourcePortRange:	50200
SourcePortGranularity:	n/a
DestAddress:	0.0.0.0
DestAddressPrefix:	0
DestAddressRange:	n/a
DestAddressGranularity:	n/a
DestPort:	1024
DestPortRange:	65535
DestPortGranularity:	n/a
OrigRmtConnPort:	n/a
RmtIDPayload:	n/a
RmtUdpEncapPort:	n/a
CreateTime:	2015/04/21 21:08:43
UpdateTime:	2015/04/27 20:31:04
DiscardAction:	Silent
MIPv6Type:	n/a
MIPv6TypeGranularity:	n/a
TypeRange:	n/a
CodeRange:	n/a
RemoteIdentityType:	n/a
RemoteIdentity:	n/a
FragmentsOnly:	No
FilterMatches:	0
LifetimeExpires:	n/a
AssociatedStackCount:	n/a

FilterName:	WorkstationtoVIPA~4
FilterNameExtension:	2
GroupName:	n/a
LocalStartActionName:	n/a
VpnActionName:	n/a
TunnelID:	0x00
Type:	Generic
DefensiveType:	n/a
State:	Active
Action:	Permit
Scope:	Local
Direction:	Inbound
OnDemand:	n/a

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Inbound
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 192.168.20.102
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 50000
DestPortRange: 50200
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: WorkstationtoVIPA~5
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

LogLimit:                n/a
Protocol:                TCP (6)
ICMPType:                n/a
ICMPTypeGranularity:    n/a
ICMPCode:                n/a
ICMPCodeGranularity:    n/a
OSPFTYPE:                n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:    n/a
SourceAddress:            192.168.20.102
SourceAddressPrefix:    n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              23
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                1024
DestPortRange:           65535
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:        n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:                n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:    n/a
*****
FilterName:               WorkstationtoVIPA~5
FilterNameExtension:      2
GroupName:                n/a
LocalStartActionName:    n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Inbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 TCP (6)

```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Inbound
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 192.168.20.102
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 23
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: WorkstationtoVIPa~6
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFTYPE: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: n/a
SourceAddress: 192.168.20.102
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 4159
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/27 20:31:04
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: WorkstationtoVIPA~6
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

OSPFType: n/a
TCPQualifier: Connect Outbound
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 4159
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 192.168.20.102
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/27 20:31:04
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: WorkstationtoVIPA~7
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP(6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: Connect Inbound

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ProtocolGranularity:      n/a
SourceAddress:            192.168.20.102
SourceAddressPrefix:      n/a
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               4159
SourcePortRange:          n/a
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 1024
DestPortRange:            65535
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/27 20:31:04
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
FilterName:                WorkstationtoVIPA~7
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  TCP(6)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              Connect Inbound
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourceAddressPrefix:      0
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               1024
SourcePortRange:          65535
SourcePortGranularity:    n/a
DestAddress:              192.168.20.102
DestAddressPrefix:        n/a
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 4159
DestPortRange:            n/a
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/27 20:31:04
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:            No
FilterMatches:            0
LifetimeExpires:          n/a
AssociatedStackCount:     n/a
*****
FilterName:                CommonTraffic~1
FilterNameExtension:       1
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Outbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  UDP (17)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:        n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourceAddressGranularity:  n/a
SourcePort:                53
SourcePortRange:           n/a
SourcePortGranularity:     n/a
DestAddress:               0.0.0.0
DestAddressPrefix:         0
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  1024
DestPortRange:             65535
DestPortGranularity:        n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:           n/a
AssociatedStackCount:       n/a
*****
FilterName:                CommonTraffic~1
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  UDP (17)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:        n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:   n/a
SourcePort:                1024
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortRange:          65535
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 53
DestPortRange:            n/a
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:            No
FilterMatches:            0
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
FilterName:                CommonTraffic~2
FilterNameExtension:       1
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Outbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  UDP (17)
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
ICMPCode:                  n/a
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:        0
SourceAddressRange:        n/a
SourceAddressGranularity:   n/a
SourcePort:                53
SourcePortRange:           n/a
SourcePortGranularity:     n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 53
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~2
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP(17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 53
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestAddressRange:      n/a
DestAddressGranularity: n/a
DestPort:              53
DestPortRange:         n/a
DestPortGranularity:   n/a
OrigRmtConnPort:       n/a
RmtIDPayload:          n/a
RmtUdpEncapPort:       n/a
CreateTime:            2015/04/21 21:08:43
UpdateTime:            2015/04/27 20:31:04
DiscardAction:         Silent
MIPv6Type:             n/a
MIPv6TypeGranularity:  n/a
TypeRange:             n/a
CodeRange:             n/a
RemoteIdentityType:    n/a
RemoteIdentity:        n/a
FragmentsOnly:        No
FilterMatches:         0
LifetimeExpires:       n/a
AssociatedStackCount:   n/a
*****
FilterName:            CommonTraffic~3
FilterNameExtension:   1
GroupName:             n/a
LocalStartActionName:  n/a
VpnActionName:         n/a
TunnelID:              0x00
Type:                  Generic
DefensiveType:         n/a
State:                 Active
Action:                Permit
Scope:                 Local
Direction:             Outbound
OnDemand:              n/a
SecurityClass:         0
Logging:               All
LogLimit:              n/a
Protocol:              TCP (6)
ICMPType:              n/a
ICMPTypeGranularity:   n/a
ICMPCode:              n/a
ICMPCodeGranularity:   n/a
OSPFType:              n/a
TCPQualifier:          None
ProtocolGranularity:   n/a
SourceAddress:         0.0.0.0
SourceAddressPrefix:   0
SourceAddressRange:    n/a
SourceAddressGranularity: n/a
SourcePort:            53
SourcePortRange:       n/a
SourcePortGranularity: n/a
DestAddress:           0.0.0.0
DestAddressPrefix:     0
DestAddressRange:      n/a
DestAddressGranularity: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~3
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP (6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: None
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 53
DestPortRange: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestPortGranularity:      n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               CommonTraffic~4
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 TCP (6)
ICMPType:                 n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:             None
ProtocolGranularity:      n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:      0
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               53
SourcePortRange:         n/a
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 53
DestPortRange:            n/a
DestPortGranularity:      n/a
OrigRmtConnPort:         n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~4
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: TCP(6)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: None
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 53
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 53
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:            No
FilterMatches:            0
LifetimeExpires:          n/a
AssociatedStackCount:     n/a
*****
FilterName:                CommonTraffic~5
FilterNameExtension:       1
GroupName:                 n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:            n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Outbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  ICMP(1)
ICMPType:                  11
ICMPTypeGranularity:      n/a
ICMPCode:                  All
ICMPCodeGranularity:      n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                n/a
SourcePortRange:           n/a
SourcePortGranularity:     n/a
DestAddress:               0.0.0.0
DestAddressPrefix:         0
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  n/a
DestPortRange:             n/a
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:         No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:   n/a
*****
FilterName:             CommonTraffic~5
FilterNameExtension:    2
GroupName:              n/a
LocalStartActionName:   n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                  Active
Action:                 Permit
Scope:                  Local
Direction:              Inbound
OnDemand:               n/a
SecurityClass:          0
Logging:                All
LogLimit:               n/a
Protocol:                ICMP(1)
ICMPType:               11
ICMPTypeGranularity:    n/a
ICMPCode:               All
ICMPCodeGranularity:    n/a
OSPFType:               n/a
TCPQualifier:           n/a
ProtocolGranularity:    n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              n/a
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                n/a
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               CommonTraffic~6
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                  ICMP (1)
ICMPType:                 3
ICMPTypeGranularity:      n/a
ICMPCode:                 All
ICMPCodeGranularity:      n/a
OSPFType:                 n/a
TCPQualifier:             n/a
ProtocolGranularity:      n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                n/a
SourcePortRange:          n/a
SourcePortGranularity:     n/a
DestAddress:               0.0.0.0
DestAddressPrefix:         0
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  n/a
DestPortRange:             n/a
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:              Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~6
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: ICMP(1)
ICMPType: 3
ICMPTypeGranularity: n/a
ICMPCode: All
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: n/a
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: n/a
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:    n/a
*****
FilterName:              CommonTraffic~7
FilterNameExtension:     1
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                   Permit
Scope:                   Local
Direction:               Outbound
OnDemand:                n/a
SecurityClass:           0
Logging:                  All
LogLimit:                 n/a
Protocol:                 OSPF(89)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                All
TCPQualifier:            n/a
ProtocolGranularity:     n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              n/a
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 n/a
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:          No
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~7
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: OSPF(89)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: All
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: n/a
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: n/a
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
AssociatedStackCount:      n/a
*****
FilterName:               CommonTraffic~8
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 IGMP (2)
ICMPType:                 n/a
ICMPTypeGranularity:      n/a
ICMPCode:                 n/a
ICMPCodeGranularity:      n/a
OSPFType:                 n/a
TCPQualifier:             n/a
ProtocolGranularity:      n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:      0
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               n/a
SourcePortRange:          n/a
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 n/a
DestPortRange:            n/a
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FilterName: CommonTraffic~8
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: IGMP (2)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFTYPE: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: n/a
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: n/a
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~9
FilterNameExtension: 1
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP(17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 520
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a

FilterName: CommonTraffic~9
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
VpnActionName:      n/a
TunnelID:           0x00
Type:               Generic
DefensiveType:      n/a
State:              Active
Action:             Permit
Scope:              Local
Direction:          Inbound
OnDemand:           n/a
SecurityClass:      0
Logging:            All
LogLimit:           n/a
Protocol:           UDP (17)
ICMPType:           n/a
ICMPTypeGranularity: n/a
ICMPCode:           n/a
ICMPCodeGranularity: n/a
OSPFType:           n/a
TCPQualifier:       n/a
ProtocolGranularity: n/a
SourceAddress:      0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort:         1024
SourcePortRange:    65535
SourcePortGranularity: n/a
DestAddress:        0.0.0.0
DestAddressPrefix:  0
DestAddressRange:   n/a
DestAddressGranularity: n/a
DestPort:           520
DestPortRange:      n/a
DestPortGranularity: n/a
OrigRmtConnPort:    n/a
RmtIDPayload:       n/a
RmtUdpEncapPort:    n/a
CreateTime:         2015/04/21 21:08:43
UpdateTime:         2015/04/27 20:31:04
DiscardAction:       Silent
MIPv6Type:          n/a
MIPv6TypeGranularity: n/a
TypeRange:          n/a
CodeRange:          n/a
RemoteIdentityType: n/a
RemoteIdentity:     n/a
FragmentsOnly:      No
FilterMatches:       0
LifetimeExpires:     n/a
AssociatedStackCount: n/a
*****
FilterName:          CommonTraffic~10
FilterNameExtension: 1
GroupName:           n/a
LocalStartActionName: n/a
VpnActionName:       n/a
TunnelID:            0x00
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Type:	Generic
DefensiveType:	n/a
State:	Active
Action:	Permit
Scope:	Local
Direction:	Outbound
OnDemand:	n/a
SecurityClass:	0
Logging:	All
LogLimit:	n/a
Protocol:	UDP (17)
ICMPType:	n/a
ICMPTypeGranularity:	n/a
ICMPCode:	n/a
ICMPCodeGranularity:	n/a
OSPFTType:	n/a
TCPQualifier:	n/a
ProtocolGranularity:	n/a
SourceAddress:	0.0.0.0
SourceAddressPrefix:	0
SourceAddressRange:	n/a
SourceAddressGranularity:	n/a
SourcePort:	1024
SourcePortRange:	65535
SourcePortGranularity:	n/a
DestAddress:	0.0.0.0
DestAddressPrefix:	0
DestAddressRange:	n/a
DestAddressGranularity:	n/a
DestPort:	520
DestPortRange:	n/a
DestPortGranularity:	n/a
OrigRmtConnPort:	n/a
RmtIDPayload:	n/a
RmtUdpEncapPort:	n/a
CreateTime:	2015/04/21 21:08:43
UpdateTime:	2015/04/27 20:31:04
DiscardAction:	Silent
MIPv6Type:	n/a
MIPv6TypeGranularity:	n/a
TypeRange:	n/a
CodeRange:	n/a
RemoteIdentityType:	n/a
RemoteIdentity:	n/a
FragmentsOnly:	No
FilterMatches:	0
LifetimeExpires:	n/a
AssociatedStackCount:	n/a

FilterName:	CommonTraffic~10
FilterNameExtension:	2
GroupName:	n/a
LocalStartActionName:	n/a
VpnActionName:	n/a
TunnelID:	0x00
Type:	Generic
DefensiveType:	n/a

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP (17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFTType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 520
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~11
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Scope:                                Local
Direction:                            Outbound
OnDemand:                              n/a
SecurityClass:                          0
Logging:                                All
LogLimit:                               n/a
Protocol:                               UDP (17)
ICMPType:                               n/a
ICMPTypeGranularity:                    n/a
ICMPCode:                               n/a
ICMPCodeGranularity:                    n/a
OSPFType:                               n/a
TCPQualifier:                           n/a
ProtocolGranularity:                     n/a
SourceAddress:                           0.0.0.0
SourceAddressPrefix:                     0
SourceAddressRange:                       n/a
SourceAddressGranularity:                 n/a
SourcePort:                              520
SourcePortRange:                          n/a
SourcePortGranularity:                    n/a
DestAddress:                             0.0.0.0
DestAddressPrefix:                       0
DestAddressRange:                         n/a
DestAddressGranularity:                   n/a
DestPort:                                520
DestPortRange:                            n/a
DestPortGranularity:                      n/a
OrigRmtConnPort:                          n/a
RmtIDPayload:                             n/a
RmtUdpEncapPort:                          n/a
CreateTime:                              2015/04/21 21:08:43
UpdateTime:                              2015/04/27 20:31:04
DiscardAction:                            Silent
MIPv6Type:                               n/a
MIPv6TypeGranularity:                     n/a
TypeRange:                               n/a
CodeRange:                               n/a
RemoteIdentityType:                       n/a
RemoteIdentity:                           n/a
FragmentsOnly:                           No
FilterMatches:                            0
LifetimeExpires:                          n/a
AssociatedStackCount:                     n/a
*****
FilterName:                              CommonTraffic~11
FilterNameExtension:                       2
GroupName:                                n/a
LocalStartActionName:                      n/a
VpnActionName:                             n/a
TunnelID:                                  0x00
Type:                                       Generic
DefensiveType:                             n/a
State:                                     Active
Action:                                    Permit
Scope:                                     Local
Direction:                                Inbound

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP (17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 520
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 520
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~12
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Logging:	All
LogLimit:	n/a
Protocol:	ICMP(1)
ICMPType:	3
ICMPTypeGranularity:	n/a
ICMPCode:	4
ICMPCodeGranularity:	n/a
OSPFType:	n/a
TCPQualifier:	n/a
ProtocolGranularity:	n/a
SourceAddress:	0.0.0.0
SourceAddressPrefix:	0
SourceAddressRange:	n/a
SourceAddressGranularity:	n/a
SourcePort:	n/a
SourcePortRange:	n/a
SourcePortGranularity:	n/a
DestAddress:	0.0.0.0
DestAddressPrefix:	0
DestAddressRange:	n/a
DestAddressGranularity:	n/a
DestPort:	n/a
DestPortRange:	n/a
DestPortGranularity:	n/a
OrigRmtConnPort:	n/a
RmtIDPayload:	n/a
RmtUdpEncapPort:	n/a
CreateTime:	2015/04/21 21:08:43
UpdateTime:	2015/04/27 20:31:04
DiscardAction:	Silent
MIPv6Type:	n/a
MIPv6TypeGranularity:	n/a
TypeRange:	n/a
CodeRange:	n/a
RemoteIdentityType:	n/a
RemoteIdentity:	n/a
FragmentsOnly:	No
FilterMatches:	0
LifetimeExpires:	n/a
AssociatedStackCount:	n/a

FilterName:	CommonTraffic~12
FilterNameExtension:	2
GroupName:	n/a
LocalStartActionName:	n/a
VpnActionName:	n/a
TunnelID:	0x00
Type:	Generic
DefensiveType:	n/a
State:	Active
Action:	Permit
Scope:	Local
Direction:	Inbound
OnDemand:	n/a
SecurityClass:	0
Logging:	All
LogLimit:	n/a

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

Protocol:                ICMP (1)
ICMPType:                3
ICMPTypeGranularity:    n/a
ICMPCode:                4
ICMPCodeGranularity:    n/a
OSPFType:                n/a
TCPQualifier:            n/a
ProtocolGranularity:    n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:    0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              n/a
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 n/a
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               CommonTraffic~13
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                   All
LogLimit:                 n/a
Protocol:                 ICMP (1)
ICMPType:                 8

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ICMPTypeGranularity:    n/a
ICMPCode:               All
ICMPCodeGranularity:   n/a
OSPFTYPE:              n/a
TCPQualifier:          n/a
ProtocolGranularity:   n/a
SourceAddress:         0.0.0.0
SourceAddressPrefix:   0
SourceAddressRange:    n/a
SourceAddressGranularity: n/a
SourcePort:            n/a
SourcePortRange:       n/a
SourcePortGranularity: n/a
DestAddress:           0.0.0.0
DestAddressPrefix:     0
DestAddressRange:      n/a
DestAddressGranularity: n/a
DestPort:              n/a
DestPortRange:         n/a
DestPortGranularity:   n/a
OrigRmtConnPort:       n/a
RmtIDPayload:          n/a
RmtUdpEncapPort:       n/a
CreateTime:            2015/04/21 21:08:43
UpdateTime:            2015/04/27 20:31:04
DiscardAction:         Silent
MIPv6Type:             n/a
MIPv6TypeGranularity:  n/a
TypeRange:             n/a
CodeRange:             n/a
RemoteIdentityType:    n/a
RemoteIdentity:        n/a
FragmentsOnly:         No
FilterMatches:         0
LifetimeExpires:       n/a
AssociatedStackCount:  n/a
*****
FilterName:            CommonTraffic~13
FilterNameExtension:   2
GroupName:             n/a
LocalStartActionName:  n/a
VpnActionName:         n/a
TunnelID:              0x00
Type:                  Generic
DefensiveType:         n/a
State:                 Active
Action:                 Permit
Scope:                 Local
Direction:             Inbound
OnDemand:              n/a
SecurityClass:         0
Logging:                All
LogLimit:              n/a
Protocol:               ICMP(1)
ICMPType:              8
ICMPTypeGranularity:   n/a
ICMPCode:              All
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
ICMPCodeGranularity:      n/a
OSPFTYPE:                 n/a
TCPQualifier:             n/a
ProtocolGranularity:      n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:      0
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:              n/a
SourcePortRange:         n/a
SourcePortGranularity:    n/a
DestAddress:             0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:   n/a
DestPort:               n/a
DestPortRange:          n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:           16
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               CommonTraffic~14
FilterNameExtension:      1
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Outbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 ICMP(1)
ICMPType:                 0
ICMPTypeGranularity:     n/a
ICMPCode:                 All
ICMPCodeGranularity:     n/a
OSPFTYPE:                 n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

TCPQualifier:	n/a
ProtocolGranularity:	n/a
SourceAddress:	0.0.0.0
SourceAddressPrefix:	0
SourceAddressRange:	n/a
SourceAddressGranularity:	n/a
SourcePort:	n/a
SourcePortRange:	n/a
SourcePortGranularity:	n/a
DestAddress:	0.0.0.0
DestAddressPrefix:	0
DestAddressRange:	n/a
DestAddressGranularity:	n/a
DestPort:	n/a
DestPortRange:	n/a
DestPortGranularity:	n/a
OrigRmtConnPort:	n/a
RmtIDPayload:	n/a
RmtUdpEncapPort:	n/a
CreateTime:	2015/04/21 21:08:43
UpdateTime:	2015/04/27 20:31:04
DiscardAction:	Silent
MIPv6Type:	n/a
MIPv6TypeGranularity:	n/a
TypeRange:	n/a
CodeRange:	n/a
RemoteIdentityType:	n/a
RemoteIdentity:	n/a
FragmentsOnly:	No
FilterMatches:	16
LifetimeExpires:	n/a
AssociatedStackCount:	n/a

FilterName:	CommonTraffic~14
FilterNameExtension:	2
GroupName:	n/a
LocalStartActionName:	n/a
VpnActionName:	n/a
TunnelID:	0x00
Type:	Generic
DefensiveType:	n/a
State:	Active
Action:	Permit
Scope:	Local
Direction:	Inbound
OnDemand:	n/a
SecurityClass:	0
Logging:	All
LogLimit:	n/a
Protocol:	ICMP(1)
ICMPType:	0
ICMPTypeGranularity:	n/a
ICMPCode:	All
ICMPCodeGranularity:	n/a
OSPFType:	n/a
TCPQualifier:	n/a
ProtocolGranularity:	n/a

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourceAddress:          0.0.0.0
SourceAddressPrefix:    0
SourceAddressRange:     n/a
SourceAddressGranularity: n/a
SourcePort:             n/a
SourcePortRange:        n/a
SourcePortGranularity:  n/a
DestAddress:            0.0.0.0
DestAddressPrefix:      0
DestAddressRange:       n/a
DestAddressGranularity: n/a
DestPort:               n/a
DestPortRange:          n/a
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:         No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:   n/a
*****
FilterName:             CommonTraffic~15
FilterNameExtension:    1
GroupName:              n/a
LocalStartActionName:   n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:              Outbound
OnDemand:               n/a
SecurityClass:          0
Logging:                 All
LogLimit:               n/a
Protocol:                TCP(6)
ICMPType:               n/a
ICMPTypeGranularity:    n/a
ICMPCode:               n/a
ICMPCodeGranularity:    n/a
OSPFType:               n/a
TCPQualifier:           Connect Outbound
ProtocolGranularity:     n/a
SourceAddress:          0.0.0.0
SourceAddressPrefix:    0
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              1024
SourcePortRange:         65535
SourcePortGranularity:   n/a
DestAddress:             0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                53
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:              CommonTraffic~15
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                TCP (6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Outbound
ProtocolGranularity:     n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePort: 53
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 1024
DestPortRange: 65535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~16
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP (17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 53
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:        n/a
CreateTime:              2015/04/21 21:08:43
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:    n/a
*****
FilterName:               CommonTraffic~16
FilterNameExtension:     2
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                  All
LogLimit:                n/a
Protocol:                 UDP (17)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            n/a
ProtocolGranularity:     n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              53
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestAddressPrefix:      0
DestAddressRange:       n/a
DestAddressGranularity: n/a
DestPort:               1024
DestPortRange:          65535
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:          No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:             CommonTraffic~17
FilterNameExtension:    1
GroupName:              n/a
LocalStartActionName:   n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                  Active
Action:                 Permit
Scope:                  Local
Direction:              Outbound
OnDemand:               n/a
SecurityClass:          0
Logging:                All
LogLimit:               n/a
Protocol:               ICMP(1)
ICMPType:               11
ICMPTypeGranularity:    n/a
ICMPCode:               0
ICMPCodeGranularity:    n/a
OSPFType:               n/a
TCPQualifier:           n/a
ProtocolGranularity:    n/a
SourceAddress:          0.0.0.0
SourceAddressPrefix:    0
SourceAddressRange:     n/a
SourceAddressGranularity: n/a
SourcePort:             n/a
SourcePortRange:        n/a
SourcePortGranularity:  n/a
DestAddress:            0.0.0.0
DestAddressPrefix:      0
DestAddressRange:       n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestAddressGranularity:    n/a
DestPort:                  n/a
DestPortRange:             n/a
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:          n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:     n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:       n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
FilterName:                CommonTraffic~17
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  ICMP(1)
ICMPType:                  11
ICMPTypeGranularity:      n/a
ICMPCode:                  0
ICMPCodeGranularity:      n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                n/a
SourcePortRange:          n/a
SourcePortGranularity:     n/a
DestAddress:               0.0.0.0
DestAddressPrefix:         0
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
DestPortRange:          n/a
DestPortGranularity:    n/a
OrigRmtConnPort:        n/a
RmtIDPayload:           n/a
RmtUdpEncapPort:        n/a
CreateTime:             2015/04/21 21:08:43
UpdateTime:             2015/04/27 20:31:04
DiscardAction:          Silent
MIPv6Type:              n/a
MIPv6TypeGranularity:   n/a
TypeRange:              n/a
CodeRange:              n/a
RemoteIdentityType:     n/a
RemoteIdentity:         n/a
FragmentsOnly:         No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:             CommonTraffic~18
FilterNameExtension:    1
GroupName:              n/a
LocalStartActionName:   n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                  Active
Action:                  Permit
Scope:                  Local
Direction:              Outbound
OnDemand:               n/a
SecurityClass:          0
Logging:                 All
LogLimit:               n/a
Protocol:                ICMP(1)
ICMPType:               3
ICMPTypeGranularity:    n/a
ICMPCode:               3
ICMPCodeGranularity:    n/a
OSPFType:               n/a
TCPQualifier:           n/a
ProtocolGranularity:     n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              n/a
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                n/a
DestPortRange:           n/a
DestPortGranularity:     n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
OrigRmtConnPort:      n/a
RmtIDPayload:         n/a
RmtUdpEncapPort:      n/a
CreateTime:           2015/04/21 21:08:43
UpdateTime:            2015/04/27 20:31:04
DiscardAction:         Silent
MIPv6Type:            n/a
MIPv6TypeGranularity: n/a
TypeRange:            n/a
CodeRange:            n/a
RemoteIdentityType:   n/a
RemoteIdentity:        n/a
FragmentsOnly:        No
FilterMatches:         0
LifetimeExpires:      n/a
AssociatedStackCount:  n/a
*****
FilterName:            CommonTraffic~18
FilterNameExtension:   2
GroupName:            n/a
LocalStartActionName: n/a
VpnActionName:         n/a
TunnelID:              0x00
Type:                  Generic
DefensiveType:         n/a
State:                 Active
Action:                Permit
Scope:                 Local
Direction:             Inbound
OnDemand:              n/a
SecurityClass:         0
Logging:               All
LogLimit:              n/a
Protocol:              ICMP(1)
ICMPType:              3
ICMPTypeGranularity:  n/a
ICMPCode:              3
ICMPCodeGranularity:  n/a
OSPFType:              n/a
TCPQualifier:          n/a
ProtocolGranularity:   n/a
SourceAddress:         0.0.0.0
SourceAddressPrefix:   0
SourceAddressRange:    n/a
SourceAddressGranularity: n/a
SourcePort:            n/a
SourcePortRange:       n/a
SourcePortGranularity: n/a
DestAddress:           0.0.0.0
DestAddressPrefix:     0
DestAddressRange:      n/a
DestAddressGranularity: n/a
DestPort:              n/a
DestPortRange:         n/a
DestPortGranularity:   n/a
OrigRmtConnPort:      n/a
RmtIDPayload:         n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RmtUdpEncapPort:      n/a
CreateTime:           2015/04/21 21:08:43
UpdateTime:           2015/04/27 20:31:04
DiscardAction:        Silent
MIPv6Type:            n/a
MIPv6TypeGranularity: n/a
TypeRange:            n/a
CodeRange:            n/a
RemoteIdentityType:   n/a
RemoteIdentity:       n/a
FragmentsOnly:        No
FilterMatches:         0
LifetimeExpires:      n/a
AssociatedStackCount:  n/a
*****
FilterName:           CommonTraffic~19
FilterNameExtension:  1
GroupName:            n/a
LocalStartActionName: n/a
VpnActionName:        n/a
TunnelID:             0x00
Type:                 Generic
DefensiveType:        n/a
State:                Active
Action:               Permit
Scope:               Local
Direction:            Outbound
OnDemand:             n/a
SecurityClass:        0
Logging:              All
LogLimit:             n/a
Protocol:             ICMP(1)
ICMPType:             3
ICMPTypeGranularity:  n/a
ICMPCode:             2
ICMPCodeGranularity:  n/a
OSPFType:             n/a
TCPQualifier:         n/a
ProtocolGranularity:  n/a
SourceAddress:         0.0.0.0
SourceAddressPrefix:  0
SourceAddressRange:   n/a
SourceAddressGranularity: n/a
SourcePort:           n/a
SourcePortRange:      n/a
SourcePortGranularity: n/a
DestAddress:          0.0.0.0
DestAddressPrefix:    0
DestAddressRange:     n/a
DestAddressGranularity: n/a
DestPort:             n/a
DestPortRange:        n/a
DestPortGranularity:  n/a
OrigRmtConnPort:      n/a
RmtIDPayload:         n/a
RmtUdpEncapPort:      n/a
CreateTime:           2015/04/21 21:08:43
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:           n/a
AssociatedStackCount:      n/a
*****
FilterName:                CommonTraffic~19
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  ICMP(1)
ICMPType:                  3
ICMPTypeGranularity:       n/a
ICMPCode:                  2
ICMPCodeGranularity:       n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                n/a
SourcePortRange:           n/a
SourcePortGranularity:     n/a
DestAddress:               0.0.0.0
DestAddressPrefix:         0
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  n/a
DestPortRange:             n/a
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: CommonTraffic~20
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP (17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 1024
SourcePortRange: 65535
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 33435
DestPortRange: 33535
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/21 21:08:43
UpdateTime: 2015/04/27 20:31:04
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```

TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
*****
FilterName:               CommonTraffic~20
FilterNameExtension:      2
GroupName:                n/a
LocalStartActionName:     n/a
VpnActionName:            n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                   Permit
Scope:                    Local
Direction:                Inbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  All
LogLimit:                 n/a
Protocol:                 UDP (17)
ICMPType:                 n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:             n/a
ProtocolGranularity:      n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:      0
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               33435
SourcePortRange:          33535
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 1024
DestPortRange:            65535
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:         n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a

```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:          No
FilterMatches:           0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:              CommonTraffic~21
FilterNameExtension:     1
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                   Permit
Scope:                   Local
Direction:               Outbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                 TCP(6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Outbound
ProtocolGranularity:     n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              1024
SourcePortRange:         65535
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 4159
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/27 20:31:04
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:                n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FragmentsOnly:          No
FilterMatches:          0
LifetimeExpires:        n/a
AssociatedStackCount:    n/a
*****
FilterName:             CommonTraffic~21
FilterNameExtension:     2
GroupName:              n/a
LocalStartActionName:    n/a
VpnActionName:          n/a
TunnelID:               0x00
Type:                   Generic
DefensiveType:          n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Inbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                TCP (6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Outbound
ProtocolGranularity:     n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              4159
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                1024
DestPortRange:           65535
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/27 20:31:04
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:          No
FilterMatches:          0
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
LifetimeExpires:          n/a
AssociatedStackCount:     n/a
*****
FilterName:              CommonTraffic~22
FilterNameExtension:     1
GroupName:               n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                0x00
Type:                    Generic
DefensiveType:           n/a
State:                   Active
Action:                  Permit
Scope:                   Local
Direction:               Outbound
OnDemand:                n/a
SecurityClass:           0
Logging:                 All
LogLimit:                n/a
Protocol:                TCP (6)
ICMPType:                n/a
ICMPTypeGranularity:     n/a
ICMPCode:                n/a
ICMPCodeGranularity:     n/a
OSPFType:                n/a
TCPQualifier:            Connect Inbound
ProtocolGranularity:     n/a
SourceAddress:           0.0.0.0
SourceAddressPrefix:     0
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:              4159
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:             0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                1024
DestPortRange:           65535
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:            n/a
RmtUdpEncapPort:         n/a
CreateTime:              2015/04/27 20:31:04
UpdateTime:              2015/04/27 20:31:04
DiscardAction:           Silent
MIPv6Type:               n/a
MIPv6TypeGranularity:    n/a
TypeRange:               n/a
CodeRange:               n/a
RemoteIdentityType:      n/a
RemoteIdentity:          n/a
FragmentsOnly:           No
FilterMatches:           0
LifetimeExpires:         n/a
AssociatedStackCount:     n/a
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
*****
FilterName:                CommonTraffic~22
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:     n/a
VpnActionName:             n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:            n/a
State:                    Active
Action:                    Permit
Scope:                     Local
Direction:                Inbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                   All
LogLimit:                 n/a
Protocol:                  TCP (6)
ICMPType:                 n/a
ICMPTypeGranularity:      n/a
ICMPCode:                 n/a
ICMPCodeGranularity:      n/a
OSPFType:                 n/a
TCPQualifier:              Connect Inbound
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:               1024
SourcePortRange:          65535
SourcePortGranularity:     n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 4159
DestPortRange:            n/a
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/27 20:31:04
UpdateTime:               2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
FilterName:                DenyAllRule_Generated_____Inbnd
```

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
FilterNameExtension:      n/a
GroupName:                n/a
LocalStartActionName:    n/a
VpnActionName:           n/a
TunnelID:                 0x00
Type:                     Generic
DefensiveType:           n/a
State:                    Active
Action:                   Deny
Scope:                    Both
Direction:                Inbound
OnDemand:                 n/a
SecurityClass:            0
Logging:                  None
LogLimit:                 n/a
Protocol:                 All
ICMPType:                 n/a
ICMPTypeGranularity:     n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:             n/a
ProtocolGranularity:     n/a
SourceAddress:            0.0.0.0
SourceAddressPrefix:      0
SourceAddressRange:       n/a
SourceAddressGranularity: n/a
SourcePort:               n/a
SourcePortRange:          n/a
SourcePortGranularity:    n/a
DestAddress:              0.0.0.0
DestAddressPrefix:        0
DestAddressRange:         n/a
DestAddressGranularity:   n/a
DestPort:                 n/a
DestPortRange:            n/a
DestPortGranularity:      n/a
OrigRmtConnPort:          n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:          n/a
CreateTime:               2015/04/21 21:08:43
UpdateTime:               2015/04/27 20:31:04
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:     n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:       n/a
RemoteIdentity:           n/a
FragmentsOnly:            No
FilterMatches:             9
LifetimeExpires:          n/a
AssociatedStackCount:      n/a
*****
FilterName:                DenyAllRule_Generated_____Outbnd
FilterNameExtension:       n/a
GroupName:                 n/a
```


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

```
LocalStartActionName:      n/a
VpnActionName:             n/a
TunnelID:                  0x00
Type:                      Generic
DefensiveType:            n/a
State:                     Active
Action:                    Deny
Scope:                     Both
Direction:                 Outbound
OnDemand:                  n/a
SecurityClass:             0
Logging:                   None
LogLimit:                  n/a
Protocol:                  All
ICMPType:                  n/a
ICMPTypeGranularity:      n/a
ICMPCode:                  n/a
ICMPCodeGranularity:      n/a
OSPFType:                  n/a
TCPQualifier:              n/a
ProtocolGranularity:       n/a
SourceAddress:             0.0.0.0
SourceAddressPrefix:       0
SourceAddressRange:        n/a
SourceAddressGranularity:  n/a
SourcePort:                n/a
SourcePortRange:           n/a
SourcePortGranularity:     n/a
DestAddress:               0.0.0.0
DestAddressPrefix:         0
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  n/a
DestPortRange:             n/a
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/04/21 21:08:43
UpdateTime:                2015/04/27 20:31:04
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:             No
FilterMatches:             0
LifetimeExpires:           n/a
AssociatedStackCount:       n/a
*****
```

94 entries selected

Other Command Output

**** Lab L07 RACF List ServAuth EZB.INITSTACK ****

rlist servauth ezb.initstack.*.* authuser

CLASS NAME

SERVAUTH EZB.INITSTACK.*.* (G)

LEVEL	OWNER	UNIVERSAL ACCESS	YOUR ACCESS	WARNING
-------	-------	------------------	-------------	---------

-----	-----	-----	-----	-----
-------	-------	-------	-------	-------

00	SYS1	NONE	READ	NO
----	------	------	------	----

INSTALLATION DATA

NONE

APPLICATION DATA

NONE

SECLEVEL

NO SECLEVEL

CATEGORIES

NO CATEGORIES

SECLABEL

NO SECLABEL

AUDITING

FAILURES (READ)

NOTIFY

NO USER TO BE NOTIFIED

USER	ACCESS
------	--------

----	-----
------	-------

JC	ALTER
----	-------

TCPIP	READ
-------	------

TN3270	READ
--------	------

CCLNV	READ
-------	------

GDENTE	ALTER
--------	-------

USER	READ
------	------

SYS1	READ
------	------

IKED	READ
------	------

OMVSKERN	READ
----------	------

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

ID	ACCESS	CLASS	ENTITY NAME
*	READ	PROGRAM	PAGENT
*	READ	PROGRAM	EZAPAGEN
USER	READ	PROGRAM	PAGENT
SYS1	READ	PROGRAM	PAGENT
USER	READ	PROGRAM	EZAPAGEN
SYS1	READ	PROGRAM	EZAPAGEN

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

