

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

Student Datasets, Unix Files, and Certificates



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

MVS Datasets	4
**** Lab L01 SYS1.CS.TCPPARMS(TNnA) ****...	4
**** Lab L01 SYS1.CS.TCPPARMS(DATnA) ****...	6
**** Lab L01 SYS1.CS.TCPPARMS(TCPnA) ****...	6
**** Lab L01 USER.CS.TCPPARMS(TNnA) ****...	10
**** Lab L01 USER.CS.TCPPARMS(DATnA) ****...	12
**** Lab L01 USER.CS.TCPPARMS(TCPnA) ****...	12
**** Lab L02 SYS1.PROCLIB(TCPIPT) ****...	16
**** Lab L02 SYS1.PROCLIB(SYSLOGDC) ****...	16
**** Lab L03 SYS1.PROCLIB(PAGENTT) ****...	17
**** Lab L05 USER.CS.SOURCE(GBGCACnx) ****...	18
**** Lab L05 USER.CS.SOURCE(GBGCASnx) ****...	19
**** Lab L05 USER.CS.SOURCE(GBGCLInx) ****...	20
**** Lab L05 USER.CS.SOURCE(GBGSRVnx) ****...	20
**** Lab L05 USER.CS.SOURCE(GBGRGCnx) ****...	21
**** Lab L05 USER.CS.SOURCE(GBGRGSnx) ****...	21
**** Lab L05 SYS1.PROCLIB(SPECUSER) ****...	22
**** Lab L07 USER.CS.TCPPARMS(TLSOFFnx) ****...	23
**** Lab L07 USER.CS.TCPPARMS(TLSONnx) ****...	23
**** Lab L07 USER.CS.TCPPARMS(FTPSECnx) ****...	23
**** Lab L07 USER.CS.TCPPARMS(FTPCLSnx) ****...	47
**** Lab L07 SYS1.PROCLIB(FTPT) ****...	64
**** Lab L08 USER.CS.TCPPARMS(TNnATTLS) ****...	64
**** Lab L08 SYS1.PROCLIB(TN3270T) ****...	68
**** Lab L10 SYS1.PROCLIB(TRMDT) ****...	68
**** Lab L11 USER.CS.TCPPARMS(TCPnAIPS) ****...	70
**** Lab L11 SYS1.PROCLIB(IKED) ****...	75
**** Lab L16 SYS1.PROCLIB(NSSD) ****...	75
**** Lab L17 SYS1.PROCLIB(DMD) ****...	76
Unix Files.....	78
**** Lab L02 /etc/syslog.conf ****...	78
**** Lab L02 /etc/rc ****...	83
**** Lab L12 /etc/security/iked.conf ****...	85
**** Lab L16 /etc/security/iked.conf ****...	87
**** Lab L16 /etc/security/nssd.conf ****...	90
**** Lab L17 /etc/securty/dmd.conf ****...	90
Instructor Certificate Jobs	91
**** L07 CA Certificate for FTP Server and Client ****...	91
**** L07 FTP Server Certificate ****...	91
**** L07 FTP Client Usernx Certificate ****...	92
**** L07 FTP Server Key Ring ****...	92
**** L07 FTP Client Key Ring ****...	92
**** L07 FTP Client USERnx Key Ring ****...	94
**** L12 CA Certificate for IKED on MVSn ****...	94
**** L12 CA Certificate for IKED on MVSn ****...	94

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

***** L12 IKED Certificate ***** 95
***** L12 IKED Key Ring on MVS1 ***** 95
***** L12 IKED Key Ring on MVSn ***** 96
Certificate Displays.....	97
***** L07 CA Certificate for FTP Server and Client ***** 97
***** L07 FTP Server Certificate ***** 98
***** L07 FTP Client Usernx Certificate ***** 99
***** L07 FTP Server Key Ring ***** 100
***** L07 FTP Client Key Ring ***** 100
***** L07 FTP Client Usernx Key Ring ***** 101
***** L08 CA Certificate for TN3270 Server ***** 101
***** L08 CA Certificate for TN3270 Client Usernx ***** 102
***** L08 TN3270 Server Certificate ***** 102
***** L08 TN3270 Client Usernx Certificate ***** 103
***** L08 TN3270 Server Key Ring ***** 103
***** L08 TN3270 Client Usernx Key Ring ***** 104
***** L12 CA Certificate for IKED on MVS1 ***** 104
***** L12 CA Certificate for IKED on MVSn ***** 105
***** L12 IKED Certificate *****	.. 105
***** L12 IKED Key Ring on MVS1 ***** 106
***** L12 IKED Key Ring on MVSn ***** 106

MVS Datasets

```
*****
**** Lab L01 SYS1.CS.TCPPARMS(TNnA) ****
*****
;      STUDENT VERSION
; TN3270 profile for the CS Workshops
; =====
; =====
; Change:                               By Whom?   When?
; =====
; Created profile for TN3270 proc by copying   GJD       08/08/2008
;   from PRTNCCL1
; Added TCPIPJOBNAME of TCPIPT to TELNETGLOB.   GJD       08/08/2008
; =====
;
TelnetGlobals
;
;   CodePage ISO8859-1 IBM-1047   ; Linemode ASCII, EBCDIC code pages
;
; Format TELNETDEVICE Devicetype TN3270logmode,TN3270Elogmode
TELNETDEVICE 3278-2-E NSX32702,D4C32XX3      ; 24 lines, dynamic
TELNETDEVICE 3278-2   D4B32782,D4C32XX3      ; 24 lines, dynamic
TELNETDEVICE 3279-2-E NSX32702,D4C32XX3      ; 24 lines, dynamic
TELNETDEVICE 3279-2   D4B32782,D4C32XX3      ; 24 lines, dynamic
TELNETDEVICE 3278-3-E NSX32703,D4C32XX3      ; 32 lines, dynamic
TELNETDEVICE 3278-3   D4B32783,D4C32XX3      ; 32 lines, dynamic
TELNETDEVICE 3279-3-E NSX32703,D4C32XX3      ; 32 lines, dynamic
TELNETDEVICE 3279-3   D4B32783,D4C32XX3      ; 32 lines, dynamic
TELNETDEVICE 3278-4-E NSX32704,D4C32XX3      ; 48 lines, dynamic
TELNETDEVICE 3279-4-E NSX32704,D4C32XX3      ; 48 lines, dynamic
TELNETDEVICE 3278-5-E NSX32705,D4C32XX3      ; 132 columns, dynamic
TELNETDEVICE 3279-5-E NSX32705,D4C32XX3      ; 132 columns, dynamic
TELNETDEVICE LINEMODE INTERACT
TELNETDEVICE IBM-DYNAMIC      ,D4C32XX3      ; dynamic user specifies
;
TCPIPJOBNAME TCPIPT
EndTelnetGlobals
;
; -----
; Configure Telnet
; -----
;
; TELNETPARMS: Configure the Telnet Server
; - TN3270(E) server port 23 options
;
TelnetParms
  Port 23                               ; Port number 23 (std.)
  CodePage ISO8859-1 IBM-1047   ; Linemode ASCII, EBCDIC code pages
  Inactive 0                       ; Let connections stay around
  LUSESSIONPEND      ; On termination of a Telnet server connection,
                      ; the user will revert to the DEFAULTAPPL
                      ; instead of having the connection dropped
```

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

```
                ; instead of having the connection dropped

MSG07                ; Sends a USS error message to the client if an
                    ; error occurs during session establishment
                    ; instead of dropping the connection

PrtInactive 0                ; Let connections stay around
TimeMark 4500
ScanInterval 900
SNAEXT
TN3270E
TKOGENLURECON 10 KEEPONTMRESET SAMEIPADDR
EndTelnetParms
;
; BEGINVTAM: Defines the VTAM parameters required for the Telnet
server.
;
BeginVTAM
    Port 23
    ; Define the LUs to be used for general users.
    DEFAULTTLUS
        TCPSna00..TCPSna20
    ENDDEFAULTLUS
    LINEMODEAPPL TSO ; Send all line-mode terminals directly to TSO.
    ALLOWAPPL TSO* DISCONNECTABLE ; Allow all users access to TSO
                                ; applications.
                                ; TSO is multiple applications all beginning with TSO,
                                ; so use the * to get them all. If a session is closed,
                                ; disconnect the user rather than log off the user.

    ALLOWAPPL CNM* DISCONNECTABLE ;NetView
    ALLOWAPPL NPM* DISCONNECTABLE ;NPM

    ALLOWAPPL F00* DISCONNECTABLE
    ; Map Telnet sessions to display the USSMSG10 from USSTAB USSAPC

    USSTCP TCPRAP&CL1
EndVTAM
```

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

***** **Lab L01 SYS1.CS.TCPPARMS(DATnA)** *****

```
; STUDENT VERSION
TCPIPjobname TCPIPT
HostName MVSS&CL1.T
Lookup LOCAL DNS
; End of file.
```

***** **Lab L01 SYS1.CS.TCPPARMS(TCPnA)** *****

```
;
; PROFILE.TCPIP for the CS Networking WORKSHOP (STUDENT VERSION)
; =====
; =====
; General TCP/IP address space configuration
; =====
;
; GLOBALCONFIG: Provides settings for the entire TCP/IP stack
;
GLOBALCONFIG TCPIPSTATISTICS
;
; IPCONFIG: Provides settings for the IP layer of TCP/IP.
;
IPCONFIG DATAGRAMFWD SYSPLEXROUTING IGNOREREDIRECT
SOURCEVIPA MULTIPATH PATHMTUDISCOVERY TTL 64 DEVRETRYDUR 90
IGNOREREDIRECT ARPTO 1200
IPCONFIG DYNAMICXCF 10.1.1.&CL1 255.255.255.0 2
;
; SOMAXCONN: Specifies maximum length for the connection request queue
; created by the socket call listen().
;
SOMAXCONN 1000
;
;
; TCPCONFIG: Provides settings for the TCP layer of TCP/IP.
; RESTRICTLOWPORTS limits access to ports below 1024
; to APF authorized or superuser applications.
;
TCPCONFIG TCPSENDBFRSIZE 32K TCPRCVBUFRSIZE 32K TCPMAXRCVBFRSIZE 256K
TCPCONFIG RESTRICTLOWPORTS FINWAIT2Time 600 INTerval 120
TCPCONFIG SENDGARBAGE FALSE TCPTIMEstamp DELAYACKS
TCPCONFIG TTLS
;
;
; UDPCONFIG: Provides settings for the UDP layer of TCP/IP
; RESTRICTLOWPORTS limits access to ports below 1024
; to APF authorized or superuser applications.
;
UDPCONFIG RESTRICTLOWPORTS
;
```

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

```
; SRCIP allows the substitution of the source IP address on a
; jobname specific basis for client applications which specify
; inaddr_any for the source IP address. This may be done when
; an application issues an explicit bind() call with inaddr_any
; or when it bypasses issuing an explicit bind() call and
; issues a connect().
;
; =====
; Hardware definitions
; =====
; DEVICE: Defines name (and sometimes device number) for various types
;   of network devices for IPv4 only
; LINK: Defines a network interface to be associated with a particular
;   device. For IPv4 only.
; INTERFACE: Defines an IPv6 interface.
;
DEVICE GIG1F MPCIPA SECROUTER AUTORESTART
LINK LGIG1F IPAQENET GIG1F
; -----
; Virtual device definitions
; -----
;
; DEVICE and LINK for Virtual Devices (VIPA):
;
    DEVICE VDEV1 VIRTUAL 0
    LINK VLINK1 VIRTUAL 0 VDEV1
;
VIPADYNAMIC
    VIPADefINE MOVEABLE IMMEDIATE 255.255.255.240 192.168.20.11y
    VIPABACKUP 100 MOVEABLE IMMEDIATE 255.255.255.240 192.168.20.12z
;    VIPARANGE DEFINE 255.255.255.192 201.2.10.192
ENDVIPADYNAMIC
;
; =====
; HOME addresses
; =====
;
; HOME: Provides the list of home IP addresses and associated link
; names
;
    HOME
    192.168.20.10n VLINK1
    192.168.20.9n LGIG1F
;
; PRIMARYINTERFACE: Specifies which link is designated as the default
; local host for use by the GETHOSTID() function.
;
; =====
; Routing configuration
; =====
; -----
; Static routing
; -----
;
; BEGINRoutes: Defines static routes to the IP route table.
;
BEGINRoutes
```

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

```
;
; Direct Routes - Routes that are directly connected to my interfaces.
;   Destination Subnet Mask      First Hop      Link Name Packet Size
;
;ROUTE 9.82.128.1  HOST              =              OSATR      MTU 4096
;
;   ROUTE 192.168.20.0/24          =              LGIG1F      MTU 1492
;
; Indirect Routes - Routes that are reachable through routers on my
;                   network.
;
;   Destination Subnet Mask      First Hop      Link Name Packet Size
;
; Default Route - All packets to an unknown destination are routed
;                 through this route.
;
;   Destination Subnet Mask      First Hop      Link Name Packet Size
;
ROUTE DEFAULT                  192.168.20.1  LGIG1F      MTU 1492
ENDRoutes
;
; -----
; Dynamic routing
; -----
;
; =====
; Application configuration
; =====
;
; AUTOLOG: Supplies TCPIP with the procedure names to start and the
; timeout value to use for a hung procedure during AUTOLOG.
;
; PORT: Reserves a port for specified job names
PORT
    7 UDP MISCSERV                ; Miscellaneous Server - echo
    7 TCP MISCSERV                ; Miscellaneous Server - echo
    9 UDP MISCSERV                ; Miscellaneous Server - discard
    9 TCP MISCSERV                ; Miscellaneous Server - discard
    19 UDP MISCSERV               ; Miscellaneous Server - chargen
    19 TCP MISCSERV               ; Miscellaneous Server - chargen
    20 TCP * NOAUTOLOG            ; FTP Server Data Connection
; 21 TCP FTPSERVE                 ; FTP Server
; 21 TCP FTPT111                  ; FTP Server Control Connection
    22 TCP OMVS                   ; SSHD
    21 TCP *                      ; FTP Server Control Connection
; 23 TCP INTCLIEN                 ; Telnet 3270 Server
; 23 TCP TN3270&CL1.A             ; Telnet 3270 Server
    23 TCP TN3270T                ; Telnet 3270 Server for CS Networking
    25 TCP SMTP                   ; SMTP Server
    53 TCP NAMED                  ; Domain Name Server
    53 UDP NAMED                  ; Domain Name Server
    111 TCP PORTMAP               ; Portmap Server (SUN 3.9)
    111 UDP PORTMAP               ; Portmap Server (SUN 3.9)
    135 UDP LLBD                  ; NCS Location Broker
    161 UDP OSNMPD                ; SNMP Agent
    162 UDP SNMPQE                ; SNMP Query Engine
    512 TCP RXSERVE               ; Remote Execution Server
```

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

```
514 TCP RXSERVE          ; Remote Execution Server
515 TCP LPSERVE          ; LPD Server
520 UDP *                ; OROUTED Server
580 UDP NCPROUT          ; NCPROUTE Server
750 TCP MVSKERB          ; Kerberos
;   PORTRANGE 5000 6000 TCP * SAF RANGE1
;
; SACONFIG: Configures the TCP/IP SNMP subagent
;
; -----
; Configure Network Access Control
; -----
;
; -----
; Configure IPSECURITY default filter rules
; -----
;
; Example IPSEC default filter rule. This rule permits
; outbound TCP traffic from local IP address 1.1.1.1 port 23 to
; remote IP address 2.2.2.2. The same rule also permits
; inbound TCP traffic from remote IP address 2.2.2.2 to local
; IP address 1.1.1.1 port 23.
;
; =====
; Diagnostic data statements (ITRACE, PKTTRACE, SMFCONFIG, SMFPARMS)
; =====
;
; =====
; Other statements
; =====
;
; DELETE: Removes an ATMARPSV, ATMLIS, ATMPVC, device, link, port or
; portrange. This statement is typically done via an copy file, not
; in an initial profile.
;
; STOP: Stops a device. If used, this statement is typically put in
; an obey file, not in an initial profile.
;
; INCLUDE: Causes another data set that contains profile configuration
; statements to be included at this point.
;
; START: Starts a device or interface that is currently stopped.
;
; -----
;
START GIG1F
```

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

***** **Lab L01 USER.CS.TCPPARMS(TNnA)** *****

```
; STUDENT VERSION
; TN3270 profile for the CS Workshops
; =====
;
TelnetGlobals
;
; CodePage ISO8859-1 IBM-1047 ; Linemode ASCII, EBCDIC code pages
;
; Format TELNETDEVICE Devicetype TN3270logmode,TN3270Elogmode
TELNETDEVICE 3278-2-E NSX32702,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3278-2 D4B32782,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3279-2-E NSX32702,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3279-2 D4B32782,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3278-3-E NSX32703,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3278-3 D4B32783,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3279-3-E NSX32703,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3279-3 D4B32783,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3278-4-E NSX32704,D4C32XX3 ; 48 lines, dynamic
TELNETDEVICE 3279-4-E NSX32704,D4C32XX3 ; 48 lines, dynamic
TELNETDEVICE 3278-5-E NSX32705,D4C32XX3 ; 132 columns, dynamic
TELNETDEVICE 3279-5-E NSX32705,D4C32XX3 ; 132 columns, dynamic
TELNETDEVICE LINEMODE INTERACT
TELNETDEVICE IBM-DYNAMIC ,D4C32XX3 ; dynamic user specifies
;
TCPIPJOBNAME TCPIPT
EndTelnetGlobals
;
; -----
; Configure Telnet
; -----
;
; TELNETPARMS: Configure the Telnet Server
; - TN3270(E) server port 23 options
;
TelnetParms
Port 23 ; Port number 23 (std.)
CodePage ISO8859-1 IBM-1047 ; Linemode ASCII, EBCDIC code pages
Inactive 0 ; Let connections stay around
LUSESSIONPEND ; On termination of a Telnet server connection,
; the user will revert to the DEFAULTAPPL
; instead of having the connection dropped
; instead of having the connection dropped

MSG07 ; Sends a USS error message to the client if an
; error occurs during session establishment
; instead of dropping the connection

PrtInactive 0 ; Let connections stay around
TimeMark 4500
ScanInterval 900
; SMFinit std
; SMFterm std
```

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

```
SNAEXT
TN3270E
TKOGENLURECON 10 KEEPONTMRESET SAMEIPADDR
EndTelnetParms
;
; TelnetParms
;   Secureport 992 Keyring HFS /tmp/telnet.kdb
; EndTelnetParms
;
; BEGINVTAM: Defines the VTAM parameters required for the Telnet
; server.
;
BeginVTAM
  Port 23
  ; Define the LUs to be used for general users.
  DEFAULTTLUS
    TCPSna00..TCPSna20
  ENDDEFAULTTLUS

  LINEMODEAPPL TSO  ; Send all line-mode terminals directly to TSO.

  ALLOWAPPL TSO* DISCONNECTABLE ; Allow all users access to TSO
    ; applications.
    ; TSO is multiple applications all beginning with TSO,
    ; so use the * to get them all.  If a session is closed,
    ; disconnect the user rather than log off the user.

  ALLOWAPPL CNM*  DISCONNECTABLE      ;NetView
  ALLOWAPPL NPM*  DISCONNECTABLE      ;NPM

  ALLOWAPPL F00*  DISCONNECTABLE

  ;   Map Telnet sessions to display the USSMSG10 from USSTAB USSAPC

  USSTCP TCPRAP&CL1

  ;   Map Telnet sessions from the SNA1 link to display the USSMSG10
  ;   screen from USS table USSCBA.

EndVTAM
```

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

**** *Lab L01 USER.CS.TCPPARMS(DATnA)* ****

```
; STUDENT VERSION
TCPIPjobname TCPIPT
HostName MVSS&CL1.T
Lookup LOCAL DNS
; End of file.
```

**** *Lab L01 USER.CS.TCPPARMS(TCPnA)* ****

```
;
; PROFILE.TCPIP for the CS Networking WORKSHOP (STUDENT VERSION)
; =====
; General TCP/IP address space configuration
; =====
;
; GLOBALCONFIG: Provides settings for the entire TCP/IP stack
;
GLOBALCONFIG TCPIPSTATISTICS
;
; IPCONFIG: Provides settings for the IP layer of TCP/IP.
;
IPCONFIG DATAGRAMFWD SYSPLEXROUTING IGNOREREDIRECT
SOURCEVIPA MULTIPATH PATHMTUDISCOVERY TTL 64 DEVRETRYDUR 90
IGNOREREDIRECT ARPTO 1200
IPCONFIG DYNAMICXCF 10.1.1.&CL1 255.255.255.0 2
;
; SOMAXCONN: Specifies maximum length for the connection request queue
; created by the socket call listen().
;
SOMAXCONN 1000
;
;
; TCPCONFIG: Provides settings for the TCP layer of TCP/IP.
; RESTRICTLOWPORTS limits access to ports below 1024
; to APF authorized or superuser applications.
;
TCPCONFIG TCPSENBFRSIZE 32K TCPCVBUFRSIZE 32K TCPMAXRCVBUFRSIZE 256K
TCPCONFIG RESTRICTLOWPORTS FINWAIT2Time 600 INTerval 120
TCPCONFIG SENDGARBAGE FALSE TCPTIMEstamp DELAYACKS
TCPCONFIG TTLS
;
; UDPCONFIG: Provides settings for the UDP layer of TCP/IP
; RESTRICTLOWPORTS limits access to ports below 1024
; to APF authorized or superuser applications.
;
UDPCONFIG RESTRICTLOWPORTS
;
; SRCIP allows the substitution of the source IP address on a
; jobname specific basis for client applications which specify
```

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

```
; inaddr_any for the source IP address. This may be done when
; an application issues an explicit bind() call with inaddr_any
; or when it bypasses issuing an explicit bind() call and
; issues a connect().
;
; =====
; Hardware definitions
; =====
; DEVICE: Defines name (and sometimes device number) for various types
;   of network devices for IPv4 only
; LINK: Defines a network interface to be associated with a particular
;   device. For IPv4 only.
; INTERFACE: Defines an IPv6 interface.
;
; OSA Definitions
;
; Gigabit Ethernet connected to CISCO 6513 Switch:
; Layer3 on MVS and Linux Systems in 192.168.20.0/24 network
; Layer2 on Linux Systems in 10.168.20.0/24 network
;GbE --- CHPID 1F -----
;
DEVICE GIG1F  MPCIPA SECROUTER AUTORESTART
LINK LGIG1F   IPAQENET GIG1F
; -----
; Virtual device definitions
; -----
;
; DEVICE and LINK for Virtual Devices (VIPA):
;
    DEVICE  VDEV1    VIRTUAL  0
    LINK    VLINK1   VIRTUAL  0  VDEV1
;
VIPADYNAMIC
    VIPADefine      MOVEABLE IMMEDIATE  255.255.255.240  192.168.20.11y
    VIPABACKUP 100  MOVEABLE IMMEDIATE  255.255.255.240  192.168.20.12z
;    VIPARANGE DEFINE 255.255.255.192 201.2.10.192
ENDVIPADYNAMIC
;
; =====
; HOME addresses
; =====
;
; HOME: Provides the list of home IP addresses and associated link
; names
;
    HOME
    192.168.20.10n VLINK1
    192.168.20.9n  LGIG1F
;
; PRIMARYINTERFACE: Specifies which link is designated as the default
;   local host for use by the GETHOSTID() function.
;
; =====
; Routing configuration
; =====
; -----
; Static routing
```

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

```
; -----
;
; BEGINRoutes: Defines static routes to the IP route table.
;
BEGINRoutes
;
; Direct Routes - Routes that are directly connected to my interfaces.
;
;      Destination Subnet Mask      First Hop      Link Name Packet Size
;
ROUTE 192.168.20.0/24                =                LGIG1F      MTU 1492
;
; Indirect Routes - Routes that are reachable through routers on my
;                  network.
;
;      Destination Subnet Mask      First Hop      Link Name Packet Size
;
; Default Route - All packets to an unknown destination are routed
;                  through this route.
;
;      Destination Subnet Mask      First Hop      Link Name Packet Size
;
ROUTE DEFAULT                        192.168.20.1  LGIG1F      MTU 1492
ENDRoutes
;
; -----
; Dynamic routing
; -----
;
; =====
; Application configuration
; =====
;
; AUTOLOG: Supplies TCPIP with the procedure names to start and the
; timeout value to use for a hung procedure during AUTOLOG.
;
;
; PORT: Reserves a port for specified job names
PORT
    7 UDP MISCSERV          ; Miscellaneous Server - echo
    7 TCP MISCSERV          ; Miscellaneous Server - echo
    9 UDP MISCSERV          ; Miscellaneous Server - discard
    9 TCP MISCSERV          ; Miscellaneous Server - discard
    19 UDP MISCSERV         ; Miscellaneous Server - chargen
    19 TCP MISCSERV         ; Miscellaneous Server - chargen
    20 TCP * NOAUTOLOG      ; FTP Server Data Connection
; 21 TCP FTPSERVE          ; FTP Server
; 21 TCP FTPT111           ; FTP Server Control Connection
    22 TCP OMVS             ; SSHD
    21 TCP *               ; FTP Server Control Connection
; 23 TCP INTCLIEN          ; Telnet 3270 Server
; 23 TCP TN3270&CL1.A      ; Telnet 3270 Server
    23 TCP TN3270T          ; Telnet 3270 Server for CS Networking
    25 TCP SMTP             ; SMTP Server
    53 TCP NAMED            ; Domain Name Server
    53 UDP NAMED            ; Domain Name Server
    111 TCP PORTMAP         ; Portmap Server (SUN 3.9)
```

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

```
111 UDP PORTMAP          ; Portmap Server (SUN 3.9)
135 UDP LLBD             ; NCS Location Broker
161 UDP OSNMPD           ; SNMP Agent
162 UDP SNMPQE           ; SNMP Query Engine
512 TCP RXSERVE          ; Remote Execution Server
514 TCP RXSERVE          ; Remote Execution Server
515 TCP LPSERVE          ; LPD Server
520 UDP *                ; OROUTED Server
580 UDP NCPROUT          ; NCPROUTE Server
750 TCP MVSKERB          ; Kerberos
;   PORTRANGE 5000 6000 TCP * SAF RANGE1
;
; SACONFIG: Configures the TCP/IP SNMP subagent
;
; -----
; Configure Network Access Control
; -----
;
; -----
; Configure IPSECURITY default filter rules
; -----
;
; Example IPSEC default filter rule. This rule permits
; outbound TCP traffic from local IP address 1.1.1.1 port 23 to
; remote IP address 2.2.2.2. The same rule also permits
; inbound TCP traffic from remote IP address 2.2.2.2 to local
; IP address 1.1.1.1 port 23.
;
; =====
; Diagnostic data statements (ITRACE, PKTTRACE, SMFCONFIG, SMFPARMS)
; =====
;
; =====
; Other statements
; =====
;
; DELETE: Removes an ATMARPSV, ATMLIS, ATMPVC, device, link, port or
; portrange. This statement is typically done via an copy file, not
; in an initial profile.
;
; STOP: Stops a device. If used, this statement is typically put in
; an obey file, not in an initial profile.
;
; INCLUDE: Causes another data set that contains profile configuration
; statements to be included at this point.
;
; START: Starts a device or interface that is currently stopped.
;
; -----
;
START GIG1F
```

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

**** Lab L02 SYS1.PROCLIB(TCPIPT) ****

```
//TCPIPT PROC PARMS='CTRACE(CTIEZB00)',PROF=TCP&CL1.A,DATA=DAT&CL1.A,
//      CS=SYS1
//*      CS=USER
//TCPIP EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//      PARM='&PARMS'
//*      PARM='&MODULE,ERRFILE(SYSERR),HEAP(512),&PARMS'
//*TEPLIB DD DSN=SYS1.TCPIP.SEZATCP,DISP=SHR
//*      DD DSN=SYS1.TCPIP.SEZALINK,DISP=SHR
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSOUT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSERROR DD SYSOUT=*
//SYSMDUMP DD SYSOUT=*
//SYSERR DD SYSOUT=*
//SYSDEBUG DD SYSOUT=*
//PROFILE DD DSN=&CS..CS.TCPPARMS(&PROF),DISP=SHR
//SYSTCPD DD DSN=&CS..CS.TCPPARMS(&DATA),DISP=SHR
```

**** Lab L02 SYS1.PROCLIB(SYSLOGDC) ****

```
//SYSLOGDC PROC
//*****
//*      Descriptive Name:          SYSLOGD Start Procedure          *
//*                                                                           *
//*      File Name:                  tcpip.SEZAINST(EZASYSLG)         *
//*                                  tcpip.SEZAINST(SYSLOGD)           *
//*                                                                           *
//*      SMP/E Distribution Name:     EZASYSLG                        *
//*                                                                           *
//*      Licensed Materials - Property of IBM                        *
//*      "Restricted Materials of IBM"                                *
//*      5694-A01                                                      *
//*      (C) Copyright IBM Corp. 1992, 2006                          *
//*      Status = CSV1R8                                               *
//*                                                                           *
//*      Note:                                                          *
//*      The SYSLOGD Daemon can read its configuration file from either a *
//*      PDS or the HFS. The procedure defaults to the HFS.           *
//*      If you are running the IVP for SYSLOGD or if you simply prefer *
//*      to use a PDS to store your configuration file,                 *
//*      either delete or comment the CONFHFS DD card                  *
//*      then uncomment the CONFPDS DD card and specify the data set and *
//*      member name.                                                  *
//*                                                                           *
//*      If you would like to run two instances of syslogd, make a second *
//*      copy of this proc and replace -i with -n in the second instance. *
//*      The instance using -n will process only log messages received *
//*      over the well-known syslogd port via UDP. One instance must    *
```

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

```
/* use -i and the other must use -n in order to run two instances. *
/*
/* The -c command-line option specifies that syslogd should create *
/* any log files or directories which do not already exist. *
/*
/* The -i command-line option specifies that syslogd should not *
/* process log messages sent to the well-known syslog port via UDP. *
/******
//CONFHFS EXEC PGM=SYSLOGD,REGION=4096K,TIME=NOLIMIT,PARM='/-c -i'
/*CONFPS EXEC PGM=SYSLOGD,REGION=4096K,TIME=NOLIMIT,
/* PARM='/-c -i -f //'TCPIVP.TCPPARMS(SYSLOG)''
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
```

***** Lab L03 SYS1.PROCLIB(PAGENTT) *****

```
//PAGENTT PROC
/*
/* IBM Communications Server for z/OS
/* SMP/E distribution name: EZAPAGSP
/*
/* 5694-A01 Copyright IBM Corp. 1998, 2007
/* Licensed Materials - Property of IBM
/* "Restricted Materials of IBM"
/* Status = CSV1R9
/*
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
// PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-c /
// etc/PAGT1/pagentt.conf -l SYSLOGD'
/* etc/pagent.conf'
/*
/* Example of passing parameters to the program (parameters must
/* extend to column 71 and be continued in column 16):
/* PARM='ENVAR("_CEE_ENVFILE=DD:STDENV")/-c /etc/pagent3.conf -l
/* SYSLOGD'
/*
/* Provide environment variables to run with the desired
/* configuration. As an example, the data set or file specified by
/* STDENV could contain:
/*
/* PAGENT_CONFIG_FILE=/etc/pagent2.conf
/* PAGENT_LOG_FILE=/tmp/pagent2.log
/* LIBPATH=/usr/lib
/* TZ=EST5EDT4
/*
/* For information on the above environment variables, refer to the
/* IP Configuration Reference. Other environment variables can also
/* be specified via STDENV.
/*
/*STDENV DD DUMMY
/* Sample MVS data set containing environment variables:
```

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

```
//*STDENV DD DSN=TCPIP.PAGENT.ENV(PAGENT),DISP=SHR
/* Sample HFS file containing environment variables:
//STDENV DD PATH='/etc/PAGT1/pagentt.env',PATHOPTS=(ORDONLY)
/*
/* Output written to stdout and stderr goes to the data set or
/* file specified with SYSPRINT or SYSOUT, respectively. But
/* normally, PAGENT doesn't write output to stdout or stderr.
/* Instead, output is written to the log file, which is specified
/* by the -c startup option, the PAGENT_LOG_FILE environment
/* variable, or the default of /tmp/pagent.log. For severe
/* startup errors, such as incorrect startup options specified,
/* or being unable to open the log file, log output is instead
/* written to the syslog daemon, and help text is written to
/* stdout.
/*
/*
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
/*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)

*****

**** Lab L05 USER.CS.SOURCE(GBGCACnx) ****

*****
CA Certificate for TN3270 Client
//GBGCACnx JOB MSGCLASS=X,NOTIFY=&SYSUID
//GBGCACnx EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
/* Create Certificate Authority for This Installation *
/* THIS CA SIGNS THE CLIENT CERTIFICATES *
/* CHANGE ALL "--" Characters to your team number *
/* CHANGE THE ALTNAME IP ADDR FOR THE CA 91 through 95 *
/* START CERTIFICATE VALIDITY TODAY; END IT IN 6 MONTHS *
//*****
//*****
/* USERIDs, HFS Datasets, UNIX directories created with *
/* (JOB ADDUSER) *
/* Certificates were created with JOB GBGCA, GBGFTP, GBGCLI *
/* (JOBS GBGCA, GBGFTP, GBGCLI) *
/* At this system, certificates were connected to appropri. keyring *
/* (JOB GBGRNGCL and GBGRNGSR) *
/* At this system, certificates were exported to a dataset *
/* (JOB GBGEXP12) *
/* Export CA certificate for LABS with DER (no private key) *
/* Export USER Certificates for FTP Clients to PKCS12, incl. Key *
/* FTP These files to other z/OS Systems *
/* FTP with BINARY, RECFM=VB, LRECL=84, BLOCKSIZE=27998 *
/* Connect there the same certificate to the appropriate keyring *
/* (JOBS GBGRNGCL and GBGRNGSR) *
//*****
//*****
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT CERTAUTH GENCERT -
SUBJECTSDN (O('GBG')) -
CN('GBGCACnx.LABS.IBM.COM') -
```

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

```
                C('US'))
ALTNAME (IP(192.168.20.9n)
          DOMAIN('GBG.LABS.IBM.COM')
          EMAIL('ZOSC@GBG.LABS.IBM.COM'))
NOTBEFORE (DATE(2013-03-13))
NOTAFTER (DATE(2013-09-13))
KEYUSAGE (CERTSIGN)
SIZE(1024)
WITHLABEL('GBGCACnx LABS Client CA')
setropts raclist(DIGTCERT) refresh
racdcert CERTAUTH list(label('GBGCACnx LABS Client CA'))
/*
```

**** Lab L05 USER.CS.SOURCE(GBGCASnx) ****

```
CA Certificate for TN3270 Server
//GBGCASnx JOB MSGCLASS=X,NOTIFY=&SYSUID
//GBGCASnx EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
//*      Create Certificate Authority for This Installation      *
//*      THIS CA SIGNS THE SERVER CERTIFICATES                  *
//*      CHANGE ALL "21" Characters to your team Suffix         *
//*      CHANGE THE ALTNAME IP ADDR 4TH OCTET TO 101 through 107 *
//*      START CERTIFICATE VALIDITY TODAY; END IN 6 MONTHS      *
//*****
//*****
//*      USERIDs, HFS Datasets, UNIX directories created with   *
//*      (JOB ADDUSER)                                           *
//*      Certificates were created with JOB GBGCA, GBGFTP, GBGCLI *
//*      (JOBS GBGCA, GBGFTP, GBGCLI)                            *
//*      At this system, certificates were connected to appropri. keyring *
//*      (JOB GBGRNGCL and GBGRNGSR)                             *
//*      At this system, certificates were exported to a dataset *
//*      (JOB GBGEXP12)                                           *
//*      Export CA certificate for LABS with DER (no private key) *
//*      Export USER Certificates for FTP Clients to PKCS12, incl. Key *
//*      FTP These files to other z/OS Systems                  *
//*      FTP with BINARY, RECFM=VB, LRECL=84, BLOCKSIZE=27998   *
//*      Connect there the same certificate to the appropriate keyring *
//*      (JOBS GBGRNGCnx and GBGRNGSnx)                         *
//*****
//*****
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT  CERTAUTH  GENCERT
                SUBJECTSDN (O('GBG')
                            CN('GBGCASnx.LABS.IBM.COM')
                            C('US'))
                ALTNAME (IP(192.168.20.10n)
                          DOMAIN('GBG.LABS.IBM.COM')
                          EMAIL('ZOSC@GBG.LABS.IBM.COM'))
                NOTBEFORE (DATE(2013-03-13))
                NOTAFTER (DATE(2013-09-13))
                KEYUSAGE (CERTSIGN)
```

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

```
        SIZE(1024)
        WITHLABEL('GBGCASnx LABS Server CA')
setropts raclist(DIGTCERT) refresh
racdcert CERTAUTH list(label('GBGCASnx LABS Server CA'))
/*
```

***** Lab L05 USER.CS.SOURCE(GBGCLInx) *****

```
TN3270 Client Certificate
//GBGCLInx JOB MSGCLASS=X,NOTIFY=&SYSUID
//GBGCLInx EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
//*****
//* Create Individual Personal Certificate for USERnx and MVSn *
//* "nx" is the TEAM Suffix; MVS-, where "-" is the MVS Suffix *
//* START CERTIFICATE VALIDITY TODAY; END IT IN 6 MONTHS *
//*****
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(USERnx) GENCERT
        SUBJECTSDN (O('IBM')
                    CN('USERnx.GBG.LABS.IBM.COM')
                    C('US'))
        ALTNAME (EMAIL('USERnx@GBG.LABS.IBM.COM'))
        NOTBEFORE (DATE(2013-03-13))
        NOTAFTER (DATE(2013-09-13))
        WITHLABEL('USERnx on MVSn')
        SIZE(1024)
        SIGNWITH(CERTAUTH
                Label('GBGCACnx LABS Client CA'))
setropts raclist(DIGTCERT) refresh
racdcert ID(USERnx) list(label('USERnx on MVSn'))
/*
```

***** Lab L05 USER.CS.SOURCE(GBGSRVnx) *****

```
TN3270 Server Certificate
//GBGSRVnx JOB MSGCLASS=X,NOTIFY=&SYSUID
//GBGSRVnx EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
//* Create Server Certificate for a Server owned by TN3270 *
//* "nx" is the TEAM Suffix; MVS-, where "-" is the MVS Suffix *
//* START CERTIFICATE VALIDITY TODAY; END IT IN 6 MONTHS *
//*****
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(TN3270) GENCERT
        SUBJECTSDN (O('IBM')
                    CN('TN3270.GBG.LABS.IBM.COM')
                    C('US'))
        ALTNAME (EMAIL('TN3270@GBG.LABS.IBM.COM'))
```

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

```
NOTBEFORE (DATE (2013-03-13)) -
NOTAFTER (DATE (2013-09-13)) -
WITHLABEL ('TN3270 on MVSn') -
SIZE (1024) -
SIGNWITH (CERTAUTH -
    Label ('GBGCASnx LABS Server CA'))
setropts raclist (DIGTCERT) refresh
racdcert ID (TN3270) list (label ('TN3270 on MVSn'))
/*
```

**** Lab L05 USER.CS.SOURCE(GBGRGCnx) ****

```
TN3270 Client Key Ring
//GBGRGCnx JOB MSGCLASS=X,NOTIFY=&SYSUID
//GBGRGCnx EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
/* Create Keyring for Client *
/* Substitute Your Team Suffix for the characters "nx" *
/* Substitute Your MVS Suffix where you see "MVS-" *
/* Include Client Certificate and Private Keys *
/* Include Clients' Signing CA Certificate *
/* Include Server's Signing CA Certificate *
/* NOTE: Different signing CA for Client and Server here *
//*****
//*****includes private key*****
//*****
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID (USERnx) ADDRING (USERnxRing)
RACDCERT ID (USERnx) CONNECT (ID (USERnx) LABEL ('USERnx on MVSn') -
    RING (USERnxRing) USAGE (PERSONAL) DEFAULT) -
RACDCERT ID (USERnx) CONNECT (CERTAUTH -
    LABEL ('GBGCACnx LABS Client CA') -
    RING (USERnxRing) USAGE (CERTAUTH)) -
RACDCERT ID (USERnx) CONNECT (CERTAUTH -
    LABEL ('GBGCASnx LABS Server CA') -
    RING (USERnxRing) USAGE (CERTAUTH)) -
setropts generic (DIGTCERT) refresh
setropts raclist (DIGTCERT) refresh
racdcert ID (USERnx) listring (USERnxRing)
/*
```

**** Lab L05 USER.CS.SOURCE(GBGRGSnx) ****

```
TN3270 Server Key Ring
//GBGRGSnx JOB MSGCLASS=X,NOTIFY=&SYSUID
//GBGRGSnx EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
/* Substitute Your Team Suffix for the characters "nx" *
/* Substitute Your MVS Suffix where you see "MVS-" *
/* Substitute Your MVS Suffix for the character "-" *
```

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

```
//*      Create Keyring for Server with TN3270 as Keyring Owner      *
//*      Include Server Certificates and Private Keys                *
//*      Include Server Certificates and Private Keys                *
//*      Include Clients' Signing CA Certificate                     *
//*      Include Server's Signing CA Certificate                     *
//*      NOTE: Different CAs for Client and CA in this case         *
//*****
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TN3270) ADDRING(MyServernRing)
RACDCERT ID(TN3270) CONNECT(ID(TN3270) LABEL('TN3270 on MVSn') -
RING(MyServernRing) USAGE(PERSONAL) DEFAULT)
RACDCERT ID(TN3270) CONNECT(CERTAUTH -
LABEL('GBGCACnx LABS Client CA') -
RING(MyServernRing) USAGE(CERTAUTH))
RACDCERT ID(TN3270) CONNECT(CERTAUTH -
LABEL('GBGCASnx LABS Server CA') -
RING(MyServernRing) USAGE(CERTAUTH))
setropts generic(DIGTCERT) refresh
setropts raclist(DIGTCERT) refresh
racdcert ID(TN3270) listring(MyServernRing)
/*
```

***** Lab L05 SYS1.PROCLIB(SPECUSER) *****

```
//SPECUSER PROC
//*      JOB MSGCLASS=X,NOTIFY=&SYSUID
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *****
//*
//* Will permit the students without SPECIAL AUTHORITY to execute **
//* SETROPTS Commands themselves. **
//* Job is associated with a userid (TEACH1) that has SPECIAL Author.**
//* Following steps run to enable this PROC **
//* RDEFINE STARTED SPECUSE*.* STDATA(USER(TEACH1)) **
//* SETROPTS RACLIST(STARTED) REFRESH **
//* SETROPTS GENERIC(STARTED) REFRESH **
//* **
//* The member named SETROPTS contains these two lines: **
//*      setropts raclist(DIGTCERT) refresh **
//*      setropts generic(DIGTCERT) refresh **
//* **
//* Created by GJD on September 19, 2012 **
//* **
//*****
//RACFSETR EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DISP=SHR,DSN=SYS1.PROCLIB(SETROPTS)
//* setropts raclist(DIGTCERT) refresh
//* setropts generic(DIGTCERT) refresh
//*
```

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

**** Lab L07 USER.CS.TCPPARMS(TLSOFFnx) ****

```
*****
;  REPLACE THE "?" MARKS WITH THE APPROPRIATE VALUES TO DISABLE AT-TLS
TCPCONFIG NOTTLS      ; OBEY FILE      FOR AT-TLS LAB
*****
```

**** Lab L07 USER.CS.TCPPARMS(TLSONnx) ****

```
*****
;  REPLACE THE "?" MARKS WITH THE APPROPRIATE VALUES TO ENABLE AT-TLS
TCPCONFIG TTLS        ; OBEY FILE      FOR AT-TLS LAB
*****
```

**** Lab L07 USER.CS.TCPPARMS(FTPSECnx) ****

```
*****
;*****
;
;  Name of File:          tcpip.SEZAINST(FTPDATA)
;
;  Descriptive Name:      FTP.DATA   (for the FTP Server)
;
;  SMP/E Distribution Name:  EZAFTPAS
;
;  Copyright:             Licensed Materials - Property of IBM
;
;                          "Restricted Materials of IBM"
;
;                          5694-A01
;
;                          Copyright IBM Corp. 1977, 2012
;
;                          US Government Users Restricted Rights -
;                          Use, duplication or disclosure restricted by
;                          GSA ADP Schedule Contract with IBM Corp.
;
;  Status:                CSV1R13
;
;  This FTP.DATA file is used to specify default file and disk
;  parameters used by the FTP server.
;
;  Note: For an example of an FTP.DATA file for the FTP client,
;  see the FTCDATA example.
;
;  Syntax Rules for the FTP.DATA Configuration File:
;
;  (a) All characters to the right of and including a ; will be
;      treated as a comment.
;
;  (b) Blanks and <end-of-line> are used to delimit tokens.
;
;  (c) The format for each statement is:
;
;      parameter value
;
;*****
```

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

```
;
; The FTP.DATA options are grouped into the following groups in
; this sample FTP server FTP.DATA configuration data set:
;
; 1. Basic configuration options
; 2. Anonymous support options
; 3. Attack Prevention options
; 4. Welcome banners, login messages, and directory information
;    files
; 5. z/OS Unix file options
; 6. Default attributes for MVS data set creation
; 7. MVS data set transfer options
; 8. Codepage conversion options
; 9. Jes interface options
; 10. DB2 (SQL) interface options
; 11. SMF recording options
; 12. Security options
; 13. Timers and intervals
; 14. Debug (trace) and activity logging options
; 15. Additional advanced options
;
; For options that have a pre-selected set of values, a (D)
; indicates
; the default value for the option.
;
; Options that can be changed via SITE commands are identified
; with an (S).
;
;*****

; -----
;
; 1. Basic server configuration options
;
; -----
;SUPPRESSIGNOREWARNINGS  FALSE      ; Suppress message EZYFT47I
;                                ; while processing remaining
;                                ; statements in this FTP.DATA
;                                ; TRUE - Yes
;                                ; FALSE (D) - No. EZYFT47I is
;                                ; issued to warn of ignored
;                                ; statements

FILETYPE                  SEQ          ; (S) Server mode of operation
;                                ; SEQ = transfer data sets or
;                                ;    files (D)
;                                ; JES = submit jobs or retrieve
;                                ;    JES output
;                                ; SQL = submit queries to DB2

STARTDIRECTORY            MVS          ; Initial resource type access
;                                ; MVS = MVS data sets (D)
;                                ; HFS = z/OS Unix files

; -----
```

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

```
;
; 2. Anonymous support
;
; -----

;ANONYMOUS          GUEST/xxxxxxx      ; Allow anonymous login
;                                     ; Use user ID GUEST and
;                                     ; xxxxxxxx as password
;                                     ; SURROGATE can be used as
;                                     ; password

ANONYMOUSLEVEL      1                  ; Enable R10 Anonymous support
;                                     ; 1 = CS OS/390 V2R5 level (D)
;                                     ; 2 = APAR PQ28980 level
;                                     ; 3 = CS OS/390 V2R10 level

;                                     ; The following options in the
;                                     ; anonymous section of this sample
;                                     ; FTP.DATA only apply to
;                                     ; ANONYMOUSLEVEL 3 - if you have
;                                     ; configured a lower level, these
;                                     ; options will not be in effect.

;EMAILADDRCHECK      NO                 ; EmailAddrCheck for Anonymous
;                                     ; NO          = No check (D)
;                                     ; WARNING      = Issue warning message
;                                     ; FAIL          = Fail login request

;ANONYMOUSHFSFILEMODE 000               ; If an anonymous user is allowed
;                                     ; to create new files, these files
;                                     ; will be created with these
;                                     ; permission bits. The anonymous
;                                     ; user is not allowed to use a
;                                     ; SITE CHMOD command.
;                                     ; Default value is 000.

;ANONYMOUSHFSDIRMODE  333               ; If an anonymous user is allowed
;                                     ; to create new directories, these
;                                     ; directories will be created with
;                                     ; these permission bits. The
;                                     ; anonymous user is not allowed to
;                                     ; use a SITE CHMOD command.
;                                     ; Default value is 333 -wx-wx-wx

;ANONYMOUSFILEACCESS  HFS               ; Is the anonymous user allowed
;                                     ; to access MVS data sets or z/OS
;                                     ; Unix files or both.
;                                     ; HFS          = z/OS Unix files only (D)
;                                     ; MVS          = MVS data sets only
;                                     ; BOTH         = z/OS Unix files and MVS
;                                     ;              data sets

;ANONYMOUSFILETYPESEQ TRUE              ; Is the anonymous user allowed
;                                     ; to use filetype=seq?
;                                     ; TRUE         = Yes (D)
;                                     ; FALSE        = No
```

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

```
;ANONYMOUSFILETYPEJES FALSE          ; Is the anonymous user allowed
;                                     ; to use filetype=jes?
; TRUE = Yes
; FALSE = No (D)
;
;ANONYMOUSFILETYPESQL FALSE          ; Is the anonymous user allowed
;                                     ; to use filetype=sql?
; TRUE = Yes
; FALSE = No (D)
;
; -----
;
; 3. Attack Prevention options
;
; Prevents unwanted use of the FTP server or access to information
; the user should not see
;
; -----

DEBUGONSITE          FALSE          ; Are users allowed to issue the
;                                     ; SITE DEBUG command?
; TRUE = Yes
; FALSE = No (D)

DUMPSITE             FALSE          ; Are users allowed to issue the
;                                     ; SITE DUMP command?
; TRUE = Yes
; FALSE = No (D)

;PORTCOMMAND          ACCEPT          ; Should PORT commands be
;                                     ; accepted?
; ACCEPT = Yes (D)
; REJECT = No

;PORTCOMMANDPORT      UNRESTRICTED    ; UNRESTRICTED (D) = accept PORT
;                                     ; commands with all
;                                     ; PORT numbers
; NOLOWPORTS = reject PORT
;                                     ; commands with PORT
;                                     ; numbers less than
;                                     ; 1024.

;PORTCOMMANDIPADDR    UNRESTRICTED    ; UNRESTRICTED (D) = accept PORT
;                                     ; commands with all
;                                     ; IP addresses
; NOREDIRECT = reject PORT
;                                     ; commands
;                                     ; with IP addresses
;                                     ; other than the
;                                     ; client that sent
;                                     ; the
;                                     ; PORT command

ACCESSERRORMSG      FALSE          ; Detailed Access Error Replies
; TRUE = Send detailed access
; error
; replies to the client
```

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

```

; FALSE (D) = Do not send detailed
;           access error replies
;           to the client

REPLYSECURITYLEVEL 0      ; 0 (D) - No restriction are
;           placed
;           on information in FTP
;           replies
; 1 - No IP addresses, hostnames,
;           port numbers, or server
;           system level are included in
;           FTP replies

PASSIVEDATACONN  UNRESTRICTED ; UNRESTRICTED (D) - server allows
;           passive data connections
;           from any IP address.
; NOREDIRECT - server will verify
;           correct client IP address
;           before establishing data
;           connection

; -----
;
; 4. Welcome banner, login message, and directory information files
;
; The welcome banner is displayed at connection.
; Login message is displayed after successful login.
; Info files and data sets are displayed when CD'ing to the path.
;
; -----

;BANNER           /etc/ftpbanner      ; File-path for welcome banner -
;                                           ; both anonymous and real user

;ANONYMOUSLOGINMSG /etc/ftpanonlogin ; File-path for login message
;                                           ; for anonymous user

;LOGINMSG         /etc/ftplogin       ; File-path for login message
;                                           ; for real user

;ANONYMOUSMVSINFO README             ; Anonymous MVS info file LLQ

;MVSINFO          README             ; Real user MVS info file LLQ

;ANONYMOUSHFSINFO readme*            ; Anonymous z/OS Unix info
;                                           ; file-mask login

;HFSINFO          readme*            ; Real user z/OS Unix info
;                                           ; file-mask

;ADMINEMAILADDR   user@host.my.net    ; FTP administrator email address.
;                                           ; The substitution value for the
;                                           ; %E magic cookie in banner,
;                                           ; login, and info files.

; -----
;
```

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

; 5. z/OS Unix file options

;

; -----

UMASK	027	; (S) Octal UMASK to restrict setting ; of permission bits when creating ; new z/OS Unix files ; Default value is 027.
LISTSUBDIR	TRUE	; Should wildcard searches span ; subdirectories? ; TRUE (D) - Yes ; FALSE - No
;DBSUB	FALSE	; (S) Specifies whether the data ; should ; be substituted if untranslatable ; character is detected ; TRUE = Use substitution char ; FALSE = Terminate transfer (D) ;
;EXTENSIONS	MDTM	; Enable MDTM FTP command ; support. ; Default is disabled.
;EXTENSIONS	REST_STREAM	; Enable stream restart ; support. ; Default is disabled. ; EXTENSIONS SIZE must be enabled ; also.
;EXTENSIONS	SIZE	; Enable SIZE FTP command ; support. ; Default is disabled. ; NB: Enabling this support ; may have a negative effect ; on performance.
;UNIXFILETYPE	FILE	; (S) Unix System Services file type ; FILE (D) - Treat files as ; regular ; Unix files ; FIFO - Treat files as Unix named ; pipes
;FIFOOPENTIME	60	; (S) FIFO open timeout in seconds ; when ; opening a Unix named pipe. ; Default value is 60 seconds. ; Valid range is 1 through 86400.
;FIFOIOTIME	20	; (S) FIFO timeout for I/O to or from ; a ; Unix named pipe ; Default value is 20 seconds. ; Valid range is 1 through 86400.

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

```

; -----
;
; 6. Default attributes for MVS data set creation attributes
;
; -----

    BLKSIZE          6144          ; (S) New data set allocation
;BLKSIZE            6233          ; (S) New data set allocation
                                ; blocksize
                                ; Default is 6233
                                ; Range is from 0 to 32760

;DATACLASS          SMSDATA       ; (S) SMS data class name
                                ; There is no default

;MGMTCLASS           SMSMGNT       ; (S) SMS mgmtclass name
                                ; There is no default

;STORCLASS           SMSSTOR       ; (S) SMS storclass name
                                ; There is no default

;DCBDSN             MODEL.DCB     ; (S) New data set allocation
                                ; model dcb name - must be a
                                ; fully-qualified data set name
                                ; There is no default

    DIRECTORY        15           ; (S) Number of directory blocks in
;DIRECTORY           27           ; (S) Number of directory blocks in
                                ; new PDS/PDSE data sets.
                                ; Default value is 27.
                                ; Range is from 1 to 16777215.

;DSNTYPE             SYSTEM        ; (S) New data set allocation DSNTYPE
                                ; for physical sequential data
                                ; sets
                                ; BASIC = allocate basic format
                                ;      data set
                                ; LARGE = allocate large format
                                ;      data set
                                ; SYSTEM = use system default (D)

    LRECL            128           ; (S) New data set allocation lrecl.
;LRECL              256           ; (S) New data set allocation lrecl.
                                ; Default value is 256.
                                ; Valid range 0 through 32760.

PDSTYPE              ; (S) no value - allocate MVS
                    ;   directories according to the
                    ;   system default (PDS or PDSE)
                    ; PDS - allocate MVS
                    ;   directories as a PDS
                    ; PDSE - allocate MVS directories
                    ;   as a PDSE

    PRIMARY          5            ; (S) New data set allocation
;PRIMARY            1            ; (S) New data set allocation

```

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

		; primary space units according ; to the value of SPACETYPE. ; Default value is 1. ; Valid range 1 through 16777215.
RECFM	FB	; (S) New data set allocation
;RECFM	VB	; (S) New data set allocation ; record format. ; Default value is VB. ; Value may be specified as certain ; combinations of: ; A - ASA print control ; B - Blocked ; F - Fixed length records ; M - Machine print control ; S - Spanned (V) or Standard (F) ; U - Undefined record length ; V - Variable length records
RETPD		; (S) New data set retention ; period in days. ; Blank = no retention period (D) ; 0 = expire today ; Valid range 0 through 9999. ; NB: Note the difference between ; a blank value and a value ; of zero.
SECONDARY	2	; (S) New data set allocation
;SECONDARY	1	; (S) New data set allocation ; secondary space units according ; to the value of SPACETYPE. ; Default value is 1. ; Valid range 1 through 16777215.
SPACETYPE	CYLINDER	; (S) New data set allocation
;SPACETYPE	TRACK	; (S) New data set allocation ; space type. ; TRACK (D) ; BLOCK ; CYLINDER
UCOUNT		; (S) Sets the unit count for an ; allocation. ; If this option is not specified ; or is specified with a value of ; blank, the unit count attribute ; is not used on an allocation (D) ; Valid range is 1 through 59 or ; the character P for parallel ; mount requests
UNITNAME	3390	; (S) New data set allocation unit
;UNITNAME	SYSDA	; (S) New data set allocation unit ; name. ; There is no default.

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

```

VCOUNT          59          ; (S) Volume count for an
                           ; allocation.
                           ; Valid range is 1 through 255.
                           ; Default value is 59.

;VOLUME          WRKLB1,WRKLB2 ; (S) Volume serial number(s) to
                           ; use for allocating a data set.
                           ; Specify either a single volser
                           ; or a list of volsers
                           ; separated with commas

;EATTR          SYSTEM      ; (S) New data set allocation EATTR
                           ; specifies whether new data sets
                           ; can have extended attributes and
                           ; whether the data sets can reside
                           ; in the EAS.
                           ; NO = no extended attributes
                           ; OPT = yes if volume supports
                           ; them
                           ; SYSTEM = use system default (D)

; -----
;
; 7. MVS data set transfer options
;
; -----

ASATRANS          FALSE      ; (S) Conversion of ASA print
                           ; control characters
                           ; TRUE  = Use C conversion
                           ; FALSE = Do not convert (D)

AUTOMOUNT          TRUE      ; (S) Automatic mount of unmounted
                           ; DASD volumes
                           ; TRUE  = Mount volumes (D)
                           ; FALSE = Do not mount volumes

AUTORECALL          TRUE      ; (S) Automatic recall of
                           ; migrated data sets
                           ; TRUE  = Recall them (D)
                           ; FALSE = Do not recall them

AUTOTAPEMOUNT      TRUE      ; Automatic mount of unmounted
                           ; tape volumes
                           ; TRUE  = Mount volumes (D)
                           ; FALSE = Do not mount volumes

BUFNO              5         ; (S) Specify number of access
                           ; method buffers
                           ; Valid range is from 1 through
                           ; 35 - default value is 5

CONDDISP           CATLG     ; (S) Disposition of a new data set
                           ; when transfer ends prematurely
                           ; CATLG  = Keep and catalog (D)
                           ; DELETE = Delete data set
                           ; Note this option applies to z/OS

```

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

```

; Unix files also

DIRECTORYMODE      FALSE      ; (S) Specifies how to view the MVS
; data set structure:
; FALSE (D) = All qualifiers below
;          CWD are treated as
;          entries in the directory
; TRUE  = Qualifiers immediately
;          below the CWD are
;          treated
;          as entries in the
;          directory

ISPFSTATS          FALSE      ; (S) TRUE = create/update PDS
;          statistics
; FALSE (D) = does not create /
;          update PDS statistics

MIGRATEVOL          MIGRAT     ; (S) Migration volume volser to
; identify migrated data sets
; under control of non-HSM
; storage management products.
; Default value is MIGRAT.

;MVSURLKEY          MVSDS      ; URL identifier for references
; to MVS data sets - example:
; ftp://host/MVSDS/'USER1.DS1'
; MVSDS is the identifier that
; is used by the WebSphere server.
; There is no default value.

QUOTESOVERRIDE      TRUE      ; (S) How to treat quotes at the
; beginning or surrounding file
; names.
; TRUE  = Override current working
;          directory (D)
; FALSE = Treat quotes as part of
;          file name

RDW                  FALSE     ; (S) Specify whether Record
; Descriptor Words (RDWs) are
; discarded or retained.
; TRUE  = Retain RDWs and transfer
;          as part of data
; FALSE = Discard RDWs when
;          transferring data (D)

;READVB             LE        ; (S) Specifies whether variable
; length
; MVS data sets are read using LE
; or BSAM (low level I/O)
; BSAM  = Use BSAM
; LE    = Use LE              (D)
;

;TAPEREADSTREAM      FALSE     ; (S) Whether use a more efficient
; read path (read as stream) for

```

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

```

; reading tape data sets.
; TRUE  - Yes
; The more efficient path is used.
; Do not use this option to
; retrieve tape data sets that:
; - are ASA
; - are fixed format if you also
;   set TRAILINGBLANKS TRUE
; - contains <nl> characters that
;   require translation for
;   transfer
; FALSE - No (D)

TRAILINGBLANKS    FALSE      ; (S) How to handle trailing blanks
; in fixed format data sets during
; text transfers.
; TRUE  = Retain trailing blanks
;        (include in transfer)
; FALSE = Strip off trailing
;        blanks (D)

TRUNCATE          FALSE      ; (S) Used in conjunction with
; WRAPRECORD to specify what to do
; if no new-line is encountered
; before reaching the MVS data set
; record length limit as defined
; by LRECL when transferring data
; to MVS. This parameter only has
; meaning if WRAPRECORD is false.
; TRUE (D) = allow truncation and
; continue with the file transfer
; FALSE = fail the file transfer
; instead of truncating

WRAPRECORD        FALSE      ; (S) Specify what to do if no new-
; line
; is encountered before reaching
; the MVS data set record length
; limit as defined by LRECL when
; transferring data to MVS.
; TRUE  = Wrap data to new record
; FALSE (D) = Defer to the

TRUNCATE          ; setting to determine if the
; record is truncated or the
; file
; transfer fails

WRTAPEFASTIO      FALSE      ; (S) How should the server write
; ASCII stream mode to tapes?
; TRUE = Use BSAM I/O routines
; FALSE (D) = Use LE Run Time
; library fwrite

; -----
;
; 8. Text codepage conversion options
```

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

```
;
; -----

;CCXLATE          envqual          ; Control connection translate
; specification.  If CTRLCONN is
; also specified, CCXLATE is
; ignored.
; The specified value is used to
; construct the name of an
; environment variable:
; _FTPLATE_envqual and use the
; assigned value as a reference to
; a translate table data set.

;CTRLCONN          7BIT              ; (S) ASCII code page for
; control connection.
; 7BIT is the default if CTRLCONN
; is not specified AND no TCPXLBIN
; translation table data set
; found.
; Can be specified as any iconv
; supported ASCII codepage, such
; as IBM-850

;EXTDBSCHINESE     TRUE              ; (S) Specifies whether to use
; extended
; double byte range for Simplified
; Chinese or the old range.
; TRUE = (D) Use extended range
;       1st byte x'81' - x'FE'
;       2nd byte x'40' - x'FE'
; FALSE= Uses the range of
;       1st byte x'8C' - x'FE'
;       2nd byte x'A1' - x'FE'

;EXTENSIONS        UTF8              ; Enable RFC 2640 support.
; Default is disabled.
; Control connection starts as
; 7bit ASCII and switches to UTF-8
; encoding when LANG command
; received.  CCXLATE and CTRLCONN
; are ignored.

;ENCODING           SBCS              ; (S) Specifies whether multi-byte or
; single-byte data conversion is
; to be performed on ASCII data
; transfers.
; MBCS   = Use multi-byte
; SBCS   = Use single-byte          (D)
;

;MBDATACONN        (IBM-1388,IBM-5488) ; (S) Specifies the conversion table
; names for the data connection
; when ENCODING has a value of
; MBCS. The names are the file
; system codepage name and the
; network transfer codepage name.
```

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

```
;MBSSENDEOL          CRLF          ; (S) When translating multi-byte data
                                ; to ASCII:
                                ; CRLF = (D) Append a carriage
                                ;       return (x'0D') and line
                                ;       feed (x'0A') to each line
                                ;       of text. This is the
                                ;       default and the standard
                                ;       line terminator defined
                                ;       by
                                ;       RFC 959. The z/OS server
                                ;       and client can receive
                                ;       ASCII data only in this
                                ;       format.
                                ; CR   = Append a carriage return
                                ;       (x'0D') only to each line
                                ;       of text.
                                ; LF   = Append a line feed
                                ;       (x'0A')
                                ;       only to each line of
                                ;       text.
                                ; NONE = Do not append a line
                                ;       terminator to any line of
                                ;       text.

;MBREQUIRELASTEOL TRUE          ; (S) Specifies whether the last
                                ; record of an incoming multibyte
                                ; transfer is required to have
                                ; an EOL sequence.
                                ; TRUE  A missing EOL on the last
                                ; record received is treated as an
                                ; error (D)
                                ; FALSE A missing EOL on the last
                                ; record received is ignored

;REMOVEINBEOF FALSE             ; (S) Remove final UNIX EOF from
                                ; inbound ASCII transfers
                                ; TRUE   Final UNIX EOF is removed
                                ; FALSE  Final UNIX EOF is NOT
                                ; removed (D)

;SBDATACONN (IBM-1047,IBM-850)   ; (S) file system/network transfer
                                ; code pages for data connection.
                                ; Either a fully-qualified MVS
                                ; data set name or z/OS Unix file
                                ; name built with the CONVXLAT
                                ; utility -
                                ;       HLQ.MY.TRANS.DATASET
                                ;       /u/user1/my.trans.file
                                ; Or a file system codepage name
                                ; followed by a network transfer
                                ; codepage name according to iconv
                                ; supported codepages - for
                                ; example
                                ;       (IBM-1047,IBM-850)
                                ; If the SYSFTSX DD-name is
```

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

```

; present
; it will override SBADATACONN.
; If neither SYSFTSX nor
; SBADATACONN are present, std.
; search order for a default
; translation table data set will
; be used.

;SBSENDEOL          CRLF          ; (S) When translating single-byte
; data to ASCII :
; CRLF = (D) Append a carriage
;       return (x'0D') and line
;       feed (x'0A') to each line
;       of text. This is the
;       default and the standard
;       line terminator defined
; by
;       RFC 959. The z/OS server
;       and client can receive
;       ASCII data only in this
;       format.
; CR   = Append a carriage return
;       (x'0D') only to each line
;       of text.
; LF   = Append a line feed
;       (x'0A')
;       only to each line of
;       text.
; NONE = Do not append a line
;       terminator to any line of
;       text.

;SBSUB              FALSE         ; (S) Specifies whether the data
; should
; be substituted if untranslatable
; character is detected
; TRUE  = Use substitution char
; FALSE = Terminate transfer (D)
;

;SBSUBCHAR          SPACE         ; (S) Specifies the substitution char
; for single-byte transfers.
; nn    = n is a hexadecimal.
; SPACE = x'40' when target code
;       set is an EBCDIC, or
;       x'20' when target code
;       set is ASCII. (D)

;XLATE              envqual       ; (S) Data connection translate
; specification. If SBADATACONN is
; also specified, XLATE is
; ignored.
; The specified value is used to
; construct the name of an
; environmen variable:
; _FTPXLATE_envqual and use the
; assigned value as a reference to

```

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

```

; a translate table data set.

;UCSHOSTCS          code_set      ; (S) Specify the EBCDIC code set
;                                     ; to be used for data conversion
;                                     ; to or from UCS-2.
;                                     ; If UCSHOSTCS is not specified,
;                                     ; the current EBCDIC codepage
;                                     ; for the data connection is used.

UCSSUB              FALSE         ; (S) Specify whether UCS-2 to EBCDIC
;                                     ; conversion should use the EBCDIC
;                                     ; substitution character or
;                                     ; cause the data transfer to be
;                                     ; terminated if a UCS-2 character
;                                     ; cannot be converted to a
;                                     ; character in the target EBCDIC
;                                     ; code set
;                                     ; TRUE  = Use substitution char
;                                     ; FALSE = Terminate transfer (D)

UCSTRUNC            FALSE         ; (S) Specify whether the transfer
;                                     ; of Unicode data should be
;                                     ; aborted if truncation
;                                     ; occurs at the MVS host
;                                     ; TRUE  = Truncation allowed
;                                     ; FALSE = Terminate transfer (D)

;UNICODEFILESYSTEMBOM ASIS        ; (S) When storing UNICODE files,
;                                     ; specifies whether to store a
;                                     ; Byte Order Mark (BOM) as the
;                                     ; first character of the file.

;                                     ; ASIS   = (D) Store a BOM if one
;                                     ;         was transmitted with the file
;                                     ;         as the first character.
;                                     ; ALWAYS = Always store a BOM as
;                                     ;         the first character of the
;                                     ;         file
;                                     ; NEVER  = Never store a BOM as
;                                     ;         the first character of the
;                                     ;         file
;                                     ;         regardless of whether a BOM
;                                     ;         was
;                                     ;         was sent. Although a BOM can
;                                     ;         appear anywhere within the
;                                     ;         file, only a BOM sent as the
;                                     ;         first file character is
;                                     ;         affected by this setting.

; -----
;
; 9. JES interface options
;
; -----

JESLRECL            80            ; (S) Lrecl of jobs submitted to JES.
;                                     ; Default value is 80.
;                                     ; Valid range from 1 through 254.
```

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

```
JESPUTGETTO      600      ; Number of seconds in JesPutGet
                    ; state (number of seconds server
                    ; will wait between submitting a
                    ; job and retrieving its output.
                    ; Default value is 600 seconds.
                    ; Valid range 0 through 86400.

JESRECFM          F      ; (S) Recfm of jobs submitted to JES.
                    ; F = Fixed length (D)
                    ; V = Variable length (use only
                    ;       with JES3 systems)
                    ; * = Use record format specified
                    ;       on the RECFM statement

JESINTERFACELEVEL 1      ; Functional level of the JES
                    ; interface
                    ; 1 = Interface works as it did
                    ;       prior to OS/390 V2R10 (D)
                    ; 2 = Interface works according
                    ;       to the enhanced support
                    ;       in OS/390 V2R10

JESGETBYDSN      FALSE   ; (S) Describes how the server file
                    ; is retrieved when FILETYPE=JES
                    ; and JESINTERFACELEVEL=2
                    ; FALSE = Works as prior to z/OS
                    ;       VR10 - the server reads the
                    ;       file from the z/OS host,
                    ;       submits it to JES, waits for
                    ;       it to complete, and
                    ;       retrieves
                    ;       it's output
                    ; TRUE = a file retrieved in the
                    ;       format of JOBxxx.datasetname
                    ;       retrieves the job's spool
                    ;       file by JES spool data set
                    ;       name

JESENTRYLIMIT     200     ; (S) Maximum number of JES entries
                    ; to include in DIR listings while
                    ; in JES mode (LEVEL 2)
                    ; Default value is 200.
                    ; Valid range is 1 through 1024.

JESTRAILINGBLANKS TRUE    ; (S) How to handle trailing blanks
                    ; for
                    ; JES spool file transfers.
                    ; TRUE  = Retain trailing blanks
                    ;       (include in transfer) (D)
                    ; FALSE = Strip off trailing
                    ;       blanks

; -----
;
; 10. DB2 (SQL) interface options
```

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

```
;
; -----

DB2                DB2                ; (S) DB2 subsystem name
                                   ; The default name is DB2

DB2PLAN            EZAFTPMQ           ; DB2 plan name for FTP Server
                                   ; The default name is EZAFTPMQ

SPREAD             FALSE              ; (S) SQL spreadsheet output format
                                   ; TRUE  = Spreadsheet format
                                   ; FALSE = Not spreadsheet
                                   ;          format (D)

SQLCOL             NAMES              ; (S) SQL output headings
                                   ; NAMES  = Use column names (D)
                                   ; LABELS = Use column labels
                                   ; ANY    = Use label if defined,
                                   ;          else use name

; -----
;
; 11. SMF recording options
;
; -----

;*****
; Start of SMF settings for type 118 records
;*****
;SMF                STD                ; SMF 118 type records use
                                   ; standard
                                   ; subtypes
                                   ; Specify either SMF STD - or
                                   ; individual subtypes below for
                                   ; SMF type 118 records
                                   ; (The values used in this sample
                                   ; for the individual subtypes are
                                   ; the standard values - the values
                                   ; that will be used if you specify
                                   ; SMF STD).

SMFAPPE            70                 ; SMF record subtype for the
                                   ; APPEND subcommand
                                   ; for SMF type 118 records

;SMFDEL            71                 ; SMF record subtype for the
                                   ; DELETE subcommand
                                   ; for SMF type 118 records

;SMFLOGN           72                 ; SMF record subtype when
                                   ; recording logon failures
                                   ; for SMF type 118 records

;SMFREN            73                 ; SMF record subtype for the
                                   ; RENAME subcommand
                                   ; for SMF type 118 records
```

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

```

;SMFRETR          74          ; SMF record subtype for the
                           ; RETR subcommand
                           ; for SMF type 118 records

;SMFSTOR          75          ; SMF record subtype for the
                           ; STOR and STOU subcommands
                           ; for SMF type 118 records

;SMFEXIT          ; Load SMF user exit FTPSMFEX
                           ; Please note that there are no
                           ; parameters. If SMFEXIT is not
                           ; specified, no exit will be
                           ; loaded.

;SMFJES           ; SMF recording when filetype=jes
                           ; Please note that there are no
                           ; parameters. If SMFJES is not
                           ; specified, SMF recording while
                           ; in filetype=jes mode will not be
                           ; done for type 118 records

;SMFSQL           ; SMF recording when filetype=sql
                           ; Please note that there are no
                           ; parameters. If SMFSQL is not
                           ; specified, SMF recording while
                           ; in filetype=sql mode will not be
                           ; done for type 118 records

;*****
; End of SMF settings for type 118 records
;*****

;*****
; Start of SMF settings for type 119 records
;*****
;SMF              TYPE119

;SMFAPPE          TYPE119    ; SMF record subtype for the
                           ; APPEND subcommand
                           ; for SMF type 119 records

;SMFDEL           TYPE119    ; SMF record subtype for the
                           ; DELETE subcommand
                           ; for SMF type 119 records

;SMFLOGN          TYPE119    ; SMF record subtype when
                           ; recording logon failures
                           ; for SMF type 119 records

;SMFREN           TYPE119    ; SMF record subtype for the
                           ; RENAME subcommand
                           ; for SMF type 119 records

;SMFRETR          TYPE119    ; SMF record subtype for the
                           ; RETR subcommand
                           ; for SMF type 119 records

```

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

```

;SMFSTOR          TYPE119          ; SMF record subtype for the
                                   ; STOR and STOU subcommands
                                   ; for SMF type 119 records

;SMFJES           TYPE119          ; If SMFJES TYPE119 is not
                                   ; specified, SMF recording while
                                   ; in filetype=jes mode will not be
                                   ; done for type 119 records

;SMFSQL           TYPE119          ; If SMFSQL TYPE119 is not
                                   ; specified, SMF recording while
                                   ; in filetype=sql mode will not be
                                   ; done for type 119 records
;*****
; End of SMF settings for type 119 records
;*****

; -----
;
; 12. Security options
;
; -----

;EXTENSIONS       AUTH_GSSAPI      ; Enable Kerberos authentication
                                   ; Default is disabled.

EXTENSIONS        AUTH_TLS         ; Enable TLS authentication
;EXTENSIONS       AUTH_TLS         ; Enable TLS authentication
                                   ; Default is disabled.

SECURE_FTP        ALLOWED          ; Authentication indicator
;SECURE_FTP       ALLOWED          ; Authentication indicator
                                   ; ALLOWED          (D)
                                   ; REQUIRED

TLSMECHANISM      ATTLS
;
;
SECURE_LOGIN      REQUIRED          ; Authorization level indicator
;SECURE_LOGIN     NO_CLIENT_AUTH   ; Authorization level indicator
                                   ; for TLS
                                   ; NO_CLIENT_AUTH (D)
                                   ; REQUIRED
                                   ; VERIFY_USER

SECURE_PASSWORD   REQUIRED          ; REQUIRED (D) - User must enter
;SECURE_PASSWORD  REQUIRED          ; REQUIRED (D) - User must enter
                                   ; password
                                   ; OPTIONAL - User does not have to
                                   ; enter a password
                                   ; This setting has meaning only
                                   ; for TLS when implementing client
                                   ; certificate authentication

;SECURE_PASSWORD_KERBEROS  REQUIRED ; REQUIRED (D) - User must enter
                                   ; password
                                   ; OPTIONAL - User does not have to

```

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

```

;          enter a password
; This setting has meaning only
; for Kerberos

SECURE_CTRLCONN  PRIVATE          ; Minimum level of security for
;SECURE_CTRLCONN  CLEAR              ; Minimum level of security for
;                                     ; the control connection
; CLEAR              (D)
; SAFE
; PRIVATE

SECURE_DATACONN  CLEAR           ; Minimum level of security for
;SECURE_DATACONN  CLEAR              ; Minimum level of security for
;                                     ; the data connection
; NEVER
; CLEAR              (D)
; SAFE
; PRIVATE

;SECURE_PBSZ      16384              ; Kerberos maximum size of the
;                                     ; encoded data blocks
;                                     ; Default value is 16384
;                                     ; Valid range is 512 through 32768

; Name of a ciphersuite that can be passed to the partner during
; the TLS handshake. None, some, or all of the following may be
; specified. The number to the far right is the cipherspec id
; that corresponds to the ciphersuite's name.
;CIPHERSUITE      SSL_NULL_MD5       ; 01
;CIPHERSUITE      SSL_NULL_SHA       ; 02
;CIPHERSUITE      SSL_RC4_MD5_EX     ; 03
;CIPHERSUITE      SSL_RC4_MD5        ; 04
;CIPHERSUITE      SSL_RC4_SHA        ; 05
;CIPHERSUITE      SSL_RC2_MD5_EX     ; 06
;CIPHERSUITE      SSL_DES_SHA        ; 09
;CIPHERSUITE      SSL_3DES_SHA       ; 0A
;CIPHERSUITE      SSL_AES_128_SHA    ; 2F
;CIPHERSUITE      SSL_AES_256_SHA    ; 35

;KEYRING          name              ; Name of the keyring for TLS
;                                     ; It can be the name of a z/OS
;                                     ; Unix
;                                     ; file (name starts with /) or
;                                     ; a resource name in the security
;                                     ; product (e.g., RACF)

;TLSTIMEOUT       100               ; Maximum time limit between full
;                                     ; TLS handshakes to protect data
;                                     ; connections
;                                     ; Default value is 100 seconds.
;                                     ; Valid range is 0 through 86400

TLSRFCLEVEL      RFC4217         ; (S) Specify what level of RFC
;TLSRFCLEVEL      DRAFT              ; (S) Specify what level of RFC
;                                     ; 4217,
;                                     ; On Securing FTP with TLS, is
;                                     ; supported.
;                                     ; DRAFT      (D) Internet Draft

```

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

```

; level
; RFC4217          RFC level

;SECUREIMPLICITZOS TRUE          ; Specify when the FTP server
; expects the security handshake
; to occur.
; TRUE (D)  FTP server expects
; security handshake to occur
; after
; it sends the reply 220.
; FALSE  FTP server expects
; the security handshake before
; it sends the reply 220.

;VERIFYUSER          FALSE      ; TRUE Verify user has at least
; READ access to the FTP server's
; port profile when logging in,
; regardless of whether TLS level
; 3
; client authentication
; configured.
; FALSE (D) Verify user has at
; least READ access to the FTP
; server's port profile only when
; TLS level 3 authentication is
; configured.

;PASSPHRASE          TRUE       ; TRUE(D) - Password phrases
; are allowed to log in FTP
; FALSE - Password phrases
; are not allowed to log in
; FTP

; -----
;
; 13. Timers and intervals
;
; -----

CHKPTINT          0          ; (S) Specify the checkpoint interval
; in number of records.
; NB: checkpointing only works
; with datatype EBCDIC and block
; or compressed transfer mode.
; 0 = no checkpoints (D)

;DATAKEEPLIVE      0          ; (S) Keepalive packets are sent
; after the data connection is
; idle for the specified number
; of seconds.
; 0 (D)
; 0 = use keepalive interval
; configured in the PROFILE.TCPIP
; for passive mode and no
; keepalive
; packets for active mode
; Valid range is 60 - 86400
```

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

```
DATATIMEOUT      300      ; Data transfer timeout value in
                        ; seconds
                        ; Default is 300 seconds
                        ; 0 = do not timeout
                        ; Valid range is 1 - 86400 seconds

DCONNTIME        120      ; Length of time in seconds that
                        ; data connections will be closed
                        ; after a data transfer
                        ; Default is 120 seconds
                        ; 0 = do not timeout
                        ; Valid range is 15 - 86400
                        ; seconds

;DSWAITTIME      0        ; (S) The approximate number of
                        ; minutes ftp waits when trying
                        ; to access an MVS data set.
                        ; 0 (D)
                        ; 0 = do not wait for the data set
                        ; Valid range is 0 - 14400

;DSWAITTIMEREPLY  60      ; (S) The interval for repeating reply
                        ; 125-Data set access will be
                        ; retried at one minute
                        ; intervals - <number> attempts
                        ; remaining while the server is
                        ; waiting for access to a data
                        ; set.
                        ; Default is 60 seconds
                        ; Valid range is 15 - 60

FTPKEEPALIVE     0        ; Keepalive packets are sent after
                        ; the control connection is idle
                        ; for the specified number of
                        ; seconds
                        ; Default is 0 seconds
                        ; 0 = do not send keepalive
                        ; packets
                        ; Valid range is 60 - 86400

INACTIVE        0        ; The time in seconds a control
;INACTIVE        300      ; The time in seconds a control
                        ; connection is allowed to stay
                        ; inactive before it is closed by
                        ; the server.
                        ; Default value is 300 seconds.
                        ; Valid range is 1 - 86400
                        ; A value of zero disables the
                        ; inactivity timer check.

; -----
;
; 14. Debug (trace) and activity logging options
;
; -----
```

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

```

;DEBUG          ALL          ; (S)  activate all traces
;DEBUG          BAS          ; (S)  active basic traces
;              ;           ;           (marked with an *)
;DEBUG          FLO          ; (S)  function flow
;DEBUG          CMD          ; (S)* command trace
;DEBUG          PAR          ; (S)  parser details
;DEBUG          INT          ; (S)* program initialization and
;              ;           ;           termination
;DEBUG          ACC          ; (S)  access control (logging in)
;DEBUG          UTL          ; (S)  utility functions
;DEBUG          FSC(1)       ; (S)* file services
;DEBUG          SOC(1)       ; (S)* socket services
;DEBUG          JES          ; (S)  special JES processing
;DEBUG          SQL          ; (S)  special SQL processing
;DEBUG          SEC          ;           security processing
;DEBUG          SEC          ;           security processing
;DEBUG          USERID(USER1) ; collect traces only for this
;              ;           ;           user id
;DEBUG          IPADDR(X.X.X.X) ; collect traces only for this
;              ;           ;           IP address

;TRACE          ; Enable tracing to SYSLOGD
;              ; Please note that there are no
;              ; parameters. (Same as DEBUG BAS

FTPLOGGING      FALSE       ; Log activity for non-anonymous
;              ;           ;           users
;              ; TRUE  = log activity
;              ; TRUENODNS = log activity but no
;              ;           ;           DNS lookups
;              ; FALSE = do not log activity (D)

ANONYMOUSFTPLOGGING FALSE   ; Log activity for anonymous users
;              ; TRUE  = log activity
;              ; FALSE = do not log activity (D)

; -----
;
; 15. Additional advanced options
;
; -----

CHKCONFIDENCE   FALSE       ; (S) FALSE = (D) Do not perform
;              ;           ;           confidence checks of
;              ;           ;           data transfers.
;              ; TRUE  = Check and report on
;              ;           ;           the confidence in the
;              ;           ;           successful completion of
;              ;           ;           a data transfer. The FTP
;              ;           ;           server logs message
;              ;           ;           EZYFS86I after each file
;              ;           ;           transfer to report the
;              ;           ;           confidence level when
;              ;           ;           FTPLOGGING is set to
;              ;           ;           TRUE.

;DEST           USER14@MVSL ; (S) NJE destination of files that

```

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

```

; are stored on this FTP server.
; There is no default. If the
; option is specified, files are
; sent to the specified
; destination
; instead of being stored on the
; FTP server.

;LISTLEVEL          0          ; (S) The format of the LIST reply
; 0 = PDS, PDSE and HFS data sets
; are displayed with a DSORG
; value of PO in LIST reply.
; 1 = PDS data sets are displayed
; with a DSORG value of PO, PDSE
; data sets are displayed with
; a DSORG value of PO-E, and HFS
; data sets are displayed with a
; DSORG value of HFS in LIST
; reply.

;NONSWAPD           FALSE      ; FALSE (D) - Do not set the FTP
; daemon nonswappable
; TRUE - Set the FTP daemon
; nonswappable

;PASSIVEDATAPORTS   (low_port,high_port) ; Assign a range of ports to be
; used for passive data ports
; lowest valid port = 1024
; highest valid port = 65535
; There are no default values.

;REPLY226           FALSE      ; FALSE (D) - Reply 250 when
; server has choice of
; 250 or 226
; TRUE - Reply 226 when
; server has choice of
; 250 or 226

;RESTPUT            TRUE       ; (S) Will the server support a
; restart
; operation.
; TRUE (D) - Restart is supported
; fopen() issued with SEEK
; FALSE = Restart is not supported
; fopen issued with NOSEEK
```

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

**** *Lab L07 USER.CS.TCPPARMS(FTPCLSnx)* ****

```
;*****
;
;   Name of File:                SEZAINST(FTCDATA)
;
;   Descriptive Name:           FTP.DATA   (for FTP Client)
;
;   SMP/E Distribution Name:    EZAFTPAC
;
;   Copyright:      Licensed Materials - Property of IBM
;
;                   "Restricted Materials of IBM"
;
;                   5694-A01
;
;                   Copyright IBM Corp. 1977, 2012
;
;                   US Government Users Restricted Rights -
;                   Use, duplication or disclosure restricted by
;                   GSA ADP Schedule Contract with IBM Corp.
;
;   Status:      CSV1R13
;
;
;   This FTP.DATA file is used to specify default file and disk
;   parameters used by the FTP client.
;
;   Note: For an example of an FTP.DATA file for the FTP server,
;   see the FTPSDATA example.
;
;   Syntax Rules for the FTP.DATA Configuration File:
;
;   (a) All characters to the right of and including a ; will be
;       treated as a comment.
;
;   (b) Blanks and <end-of-line> are used to delimit tokens.
;
;   (c) The format for each statement is:
;
;       parameter value
;
;
;   The FTP.DATA options are grouped into the following groups in
;   this sample FTP client FTP.DATA configuration data set:
;
;   1. Basic configuration options
;   2. Unix System Services file options
;   3. Default attributes for MVS data set creation
;   4. MVS data set transfer options
;   5. Code page conversion options
;   6. DB2 (SQL) interface options
;   7. Security options
```

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

```
; 8. Timers *
; 9. Return codes *
; 10. Checkpoint / Restart options *
; 11. Socks server access *
; 12. Debug (trace) options *
; 13. Additional advanced options *
; *
; For options that have a pre-selected set of values, a (D) *
; indicates *
; the default value for the option. *
; *
; Options that can be changed via LOCSITE subcommands are *
; identified *
; with an (S). *
; *
;*****

; -----
;
; 1. Basic FTP client configuration options
;
; -----

;SUPPRESSIGNOREWARNINGS FALSE ; Suppress message EZYFT47I
;                               ; while processing remaining
;                               ; statements in this FTP.DATA
;                               ; TRUE - Yes
;                               ; FALSE (D) - No. EZYFT47I is
;                               ; issued to warn of ignored
;                               ; statements

FILETYPE          SEQ          ; (S) Client mode of operation
;                               ; SEQ = transfer data sets or
;                               ; files (D)
;                               ; SQL = submit queries to DB2

;SEQNUMSUPPORT FALSE          ; Support sequence numbers when input
;                               ; read from //INPUT DD file
;                               ; FALSE = (D) Do not support
;                               ; sequence numbers.
;                               ; EZYFS33I issued if
;                               ; sequence numbers
;                               ; detected
;                               ; TRUE = Support sequence numbers

; -----
;
; 2. Unix System Services file options
;
; -----

UMASK              027         ; (S) Octal UMASK to restrict setting
;                               ; of permission bits when creating
;                               ; new z/OS Unix files and named
;                               ; pipes.
;                               ; Default value is 027.
```

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

```

LISTSUBDIR      TRUE          ; Should wildcard searches span
                                ; subdirectories?
                                ; TRUE (D) - Yes
                                ; FALSE - No

;UNIXFILETYPE   FILE          ; (S) Unix System Services file type
                                ; FILE (D) - Treat files as
                                ; regular
                                ; Unix files
                                ; FIFO - Treat files as Unix named
                                ; pipes

;FIFOOPENTIME   60            ; (S) FIFO open timeout in seconds
                                ; when
                                ; opening a Unix named pipe.
                                ; Default value is 60 seconds.
                                ; Valid range is 1 through 86400.

;FIFOIOTIME     20            ; (S) FIFO timeout for I/O to or from
                                ; a
                                ; Unix named pipe
                                ; Default value is 20 seconds.
                                ; Valid range is 1 through 86400.

; -----
;
;
; 3. Default MVS data set creation attributes
;
; -----

BLKSIZE         6144          ; (S) New data set allocation block
;BLKSIZE        6233          ; (S) New data set allocation block
                                ; size
                                ; Default is 6233
                                ; Valid range is 0 to 32760

;DATACLASS      SMSDATA       ; (S) SMS data class name
                                ; There is no default

;MGMTCLASS      SMSMGNT       ; (S) SMS mgmtclass name
                                ; There is no default

;STORCLASS      SMSSTOR       ; (S) SMS storclass name
                                ; There is no default

;DCBDSN         MODEL.DCB     ; (S) New data set allocation
                                ; model DCB name - must be a
                                ; fully qualified data set name
                                ; There is no default

DIRECTORY       15            ; (S) Number of directory blocks in
;DIRECTORY       27            ; (S) Number of directory blocks in
                                ; new PDS/PDSE data sets.
                                ; Default value is 27.
                                ; Range is from 1 to 16777215.

```

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

;DSNTYPE	SYSTEM	; (S) New data set allocation DSNTYPE ; for physical sequential data ; sets ; BASIC = allocate basic format ; data set ; LARGE = allocate large format ; data set ; SYSTEM = use system default (D)
 LRECL ;LRECL	 128 256	 ; (S) New data set allocation LRECL. ; (S) New data set allocation LRECL. ; Default value is 256. ; Valid range 0 through 32760.
 PDSTYPE		 ; (S) no value - allocate MVS ; directories according to the ; system default (PDS or PDSE) ; PDS - allocate MVS ; directories as a PDS ; PDSE - allocate MVS directories ; as a PDSE
 PRIMARY ;PRIMARY	 5 1	 ; (S) New data set allocation ; (S) New data set allocation ; primary space units according ; to the value of SPACETYPE. ; Default value is 1. ; Valid range 1 through 16777215.
 RECFM ;RECFM	 FB VB	 ; (S) New data set allocation ; (S) New data set allocation ; record format. ; Default value is VB. ; Value may be specified as ; certain ; combinations of: ; A - ASA print control ; B - Blocked ; F - Fixed length records ; M - Machine print control ; S - Spanned (V) or Standard (F) ; U - Undefined record length ; V - Variable length records
 RETPD		 ; (S) New data set retention ; period in days. ; Blank = no retention period (D) ; 0 = expire today ; Valid range 0 through 9999. ; NB: Note the difference between ; a blank value and a value ; of zero.
 SECONDARY ;SECONDARY	 2 1	 ; (S) New data set allocation ; (S) New data set allocation

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

```

; secondary space units according
; to the value of SPACETYPE.
; Default value is 1.
; Valid range 1 through 16777215.

SPACETYPE          CYLINDER          ; (S) New data set allocation
;SPACETYPE         TRACK              ; (S) New data set allocation
;                                     ; space type.
;                                     ; TRACK (D)
;                                     ; BLOCK
;                                     ; CYLINDER

UCOUNT             ; (S) Sets the unit count for an
;                 ; allocation.
;                 ; If this option is not specified
;                 ; or is specified with a value of
;                 ; blank, the unit count attribute
;                 ; is not used on an allocation (D)
;                 ; Valid range is 1 through 59 or
;                 ; the character P for parallel
;                 ; mount requests

UNITNAME           3390              ; (S) New data set allocation unit
;UNITNAME          SYSDA             ; (S) New data set allocation unit
;                                     ; name.
;                                     ; There is no default.

VCOUNT             59                ; (S) Volume count for an
;                                     ; allocation.
;                                     ; Valid range is 1 through 255.
;                                     ; Default value is 59.

;VOLUME            WRKLB1,WRKLB2     ; (S) Volume serial number(s) to
;                                     ; use for allocating a data set.
;                                     ; Specify either a single VOLSER
;                                     ; or a list of VOLSERS
;                                     ; separated with commas

;EATTR             SYSTEM            ; (S) New data set allocation EATTR
;                                     ; specifies whether new data sets
;                                     ; can have extended attributes and
;                                     ; whether the data sets can reside
;                                     ; in the EAS.
;                                     ; NO = no extended attributes
;                                     ; OPT = yes if volume supports
;                                     ; them
;                                     ; SYSTEM = use system default (D)

; -----
;
; 4. MVS data set transfer options
;
; -----

ASATRANS           FALSE             ; (S) Conversion of ASA print
;                                     ; control characters
;                                     ; TRUE  = Use C conversion

```

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

		; FALSE = Do not convert (D)
AUTOMOUNT	TRUE	; (S) Automatic mount of unmounted ; DASD volumes ; TRUE = Mount volumes (D) ; FALSE = Do not mount volumes
AUTORECALL	TRUE	; (S) Automatic recall of ; migrated data sets ; TRUE = Recall them (D) ; FALSE = Do not recall them
AUTOTAPEMOUNT	FALSE	; Automatic mount of unmounted ; tape volumes ; TRUE = Mount volumes ; FALSE = Do not mount volumes (D)
BUFNO	5	; (S) Specify number of access ; method buffers ; Valid range is from 1 through ; 35 - default value is 5
CONDDISP	CATLG	; (S) Disposition of a new data set ; when transfer ends prematurely ; CATLG = Keep and catalog (D) ; DELETE = Delete data set ; This option applies to z/OS Unix ; files also
DIRECTORYMODE	FALSE	; (S) Specifies how to view the MVS ; data set structure: ; FALSE = (D) All qualifiers below ; LCWD are treated as ; entries in the directory ; TRUE = Qualifiers immediately ; below the LCWD are ; treated as entries in ; the ; directory
ISPFSTATS	FALSE	; (S) TRUE = create/update PDS ; statistics ; FALSE = (D) does not create / ; update PDS statistics
MIGRATEVOL	MIGRAT	; (S) Migration volume VOLSER to ; identify migrated data sets ; under control of non-HSM ; storage management products. ; Default value is MIGRAT.
QUOTESOVERRIDE	TRUE	; (S) How to treat quotes at the ; beginning or surrounding file ; names. ; TRUE = Override current working ; directory (D) ; FALSE = Treat quotes as part of

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

```

;          file name

RDW          FALSE      ; (S) Specify whether Record
                        ; Descriptor Words (RDWs) are
                        ; discarded or retained.
                        ; TRUE  = Retain RDWs and transfer
                        ;        as part of data
                        ; FALSE = Discard RDWs when
                        ;        transferring data (D)

;READVB      LE         ; (S) Specifies whether variable
                        ; length
                        ; MVS data sets are read using LE
                        ; or BSAM (low level I/O)
                        ; BSAM  = Use BSAM
                        ; LE    = Use LE              (D)
;

TRAILINGBLANKS  FALSE   ; (S) How to handle trailing blanks
                        ; in fixed format data sets during
                        ; text transfers.
                        ; TRUE  = Retain trailing blanks
                        ;        (include in transfer)
                        ; FALSE = Strip off trailing
                        ;        blanks (D)

TRUNCATE        FALSE   ; (S) Used in conjunction with
                        ; WRAPRECORD to specify what to do
                        ; if no new-line is encountered
                        ; before reaching the MVS data set
                        ; record length limit as defined
                        ; by LRECL when transferring data
                        ; to MVS. This parameter only has
                        ; meaning if WRAPRECORD is false.
                        ; TRUE (D) = allow truncation and
                        ; continue with the file transfer
                        ; FALSE = fail the file
                        ; transfer instead of truncating

WRAPRECORD      FALSE   ; (S) Specify what to do if no new-
                        ; line
                        ; is encountered before reaching
                        ; the MVS data set record length
                        ; limit as defined by LRECL when
                        ; transferring data to MVS.
                        ; TRUE  = Wrap data to new record
                        ; FALSE = Truncate data (D)

WRTAPEFASTIO    FALSE   ; (S) How should the server write
                        ; ASCII stream mode to tapes?
                        ; TRUE  = Use BSAM I/O routines
                        ; FALSE (D) = Use LE Run Time
                        ; library fwrite

; -----
;
; 5. Text code page conversion options

```

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

```
;
; -----

;CCTTRANS          dsn_qual          ; Control connection translate
;                  ; table data set qualifier.
;                  ; Used to search for
;                  ;   a) userid.dsn_qual.TCPXLBIN
;                  ;   b) hlq.dsn_qual.TCPXLBIN
;                  ; If CTRLCONN is specified, that
;                  ; value overrides CCTTRANS.

;CTRLCONN          7BIT              ; (S) ASCII code page for
;                  ; control connection.
;                  ; 7BIT is the default if CTRLCONN
;                  ; is not specified AND no TCPXLBIN
;                  ; translation table data set
;                  ; found.
;                  ; Can be specified as any iconv
;                  ; supported ASCII code page, such
;                  ; as IBM-850

;DBSUB             FALSE             ; (S) Specifies whether untranslatable
;                  ; data bytes should be replaced
;                  ; with substitution character in
;                  ; iconv() during data transfer.
;                  ; TRUE = Replace each
;                  ; untranslatable byte
;                  ; FALSE = Terminate transfer (D)
;                  ; when untranslatable bytes are
;                  ; detected

;ENCODING           SBCS             ; (S) Specifies whether multi-byte or
;                  ; single-byte data conversion is
;                  ; to be performed on ASCII data
;                  ; transfers.
;                  ; MBCS = Use multi-byte
;                  ; SBCS = Use single-byte      (D)
;

;EXTDBSCHINESE     TRUE              ; (S) Specifies whether to use
;                  ; extended
;                  ; double byte range for Simplified
;                  ; Chinese or the old range.
;                  ; TRUE = (D) Use the extended
;                  ; range
;                  ; 1st byte x'81' - x'FE'
;                  ; 2nd byte x'40' - x'FE'
;                  ; FALSE= Use the range of
;                  ; 1st byte x'8C' - x'FE'
;                  ; 2nd byte x'A1' - x'FE'

;EXTENSIONS        UTF8              ; Enable RFC 2640 support.
;                  ; Default is disabled.
;                  ; Control connection starts as
;                  ; 7bit ASCII and switches to UTF-8
;                  ; encoding when LANG command
;                  ; processed successfully. CCTTRANS
```

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

```

; and CTRLCONN are ignored.

;MBDATACONN    (IBM-1388,IBM-5488) ; (S) Specifies the conversion table
;              ; names for the data connection
;              ; when ENCODING has a value of
;              ; MBCS. The names are the file
;              ; system code page name and the
;              ; network transfer code page name.

;MBSENDEOL      CRLF                ; (S) When translating multi-byte data
;              ; to ASCII :
;              ; CRLF = (D) Append a carriage
;              ;       return (x'0D') and line
;              ;       feed (x'0A') to each line
;              ;       of text. This is the
;              ;       default and the standard
;              ;       line terminator defined
;              ;       by
;              ;       RFC 959. The z/OS server
;              ;       and client can receive
;              ;       ASCII data only in this
;              ;       format.
;              ; CR   = Append a carriage return
;              ;       (x'0D') only to each line
;              ;       of text.
;              ; LF   = Append a line feed
;              ;       (x'0A')
;              ;       only to each line of
;              ;       text.
;              ; NONE = Do not append a line
;              ;       terminator to any line of
;              ;       text.

;MBREQUIRELASTEOL TRUE            ; (S) Specifies whether the last
;              ; record of an incoming multibyte
;              ; transfer is required to have
;              ; an EOL sequence.
;              ; TRUE  A missing EOL on the last
;              ; record received is treated as an
;              ; error (D)
;              ; FALSE A missing EOL on the last
;              ; record received is ignored

;REMOVEINBEOF   FALSE              ; (S) Remove final UNIX EOF from
;              ; inbound ASCII transfers
;              ; TRUE  - final UNIX EOF is removed
;              ; FALSE - final UNIX EOF is not
;              ; removed (D)

;SBDATACONN     (IBM-1047,IBM-850) ; (S) file system/network transfer
;              ; code pages for data connection.
;              ; Either a fully-qualified MVS
;              ; data set name or z/OS Unix file
;              ; name built with the CONVXLAT ;
;              ; utility -
;              ;       HLQ.MY.TRANS.DATASET
;              ;       /u/user1/my.trans.file
```

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

```

; Or a file system code page name
; followed by a network transfer
; code page name according to
; iconv supported code pages -
; for example
;      (IBM-1047,IBM-850)
; If SBDATACONN is not present,
; std. search order for a default
; translation table data set will
; be used.

;SBSENDEOL          CRLF          ; (S) When translating single-byte
; data to ASCII :
; CRLF = (D) Append a carriage
;      return (x'0D') and line
;      feed (x'0A') to each line
;      of text. This is the
;      default and the standard
;      line terminator defined
;      by
;      RFC 959. The z/OS server
;      and client can receive
;      ASCII data only in this
;      format.
; CR   = Append a carriage return
;      (x'0D') only to each line
;      of text.
; LF   = Append a line feed
;      (x'0A')
;      only to each line of
;      text.
; NONE = Do not append a line
;      terminator to any line of
;      text.

;SBSUB              FALSE         ; (S) Specifies whether untranslatable
; data bytes should be replaced
; with SBSUBCHAR when detected
; during SBCS data transfer.
; TRUE  = Replace each
; untranslatable byte with
; SBSUBCHAR.
; FALSE = Terminate transfer (D)
; when untranslatable bytes are
; detected

;SBSUBCHAR          SPACE         ; (S) Specifies the substitution char
; for SBCS data transfer when
; SBSUB is TRUE.
; nn    = hexadecimal value from
;      0x'00' to 0x'FF'.
; SPACE = x'40' when target code
; set is EBCDIC, and
; x'20' when target code
; set is ASCII. (D)

;SBTRANS            dsn_qual      ; Data connection translate
```

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

```

; table data set qualifier.
; Used to search for
;   a) userid.dsn_qual.TCPXLBIN
;   b) hlq.dsn_qual.TCPXLBIN
; If SBDATACONN is specified, that
; value overrides SBTRANS

;UCSHOSTCS      code_set      ; (S) Specify the EBCDIC code set
; to be used for data conversion
; to or from UCS-2.
; If UCSHOSTCS is not specified,
; the current EBCDIC code page
; for the data connection is used.

UCSSUB          FALSE        ; (S) Specify whether UCS-2 to EBCDIC
; conversion should use the EBCDIC
; substitution character or
; cause the data transfer to be
; terminated if a UCS-2 character
; cannot be converted to a
; character in the target EBCDIC
; code set
; TRUE  = Use substitution char
; FALSE = Terminate transfer (D)

UCSTRUNC        FALSE        ; (S) Specify whether the transfer
; of UCS-2 data should be
; aborted if truncation
; occurs at the MVS host
; TRUE  = Truncation allowed
; FALSE = Terminate transfer (D)

;UNICODEFILESYSTEMBOM ASIS    ; (S) When storing UNICODE files,
; specifies whether to store a
; Byte Order Mark (BOM) as the
; first character of the file.

; ASIS    = (D) Store a BOM if one
; was transmitted with the file
; as the first character.
; ALWAYS = Always store a BOM as
; the first character of the
; file
; NEVER  = Never store a BOM as
; the first character of the
; file
; regardless of whether a BOM
; was
; was sent. Although a BOM can
; appear anywhere within the
; file, only a BOM sent as the
; first file character is
; affected by this setting.

; -----
;
; 6. DB2 (SQL) interface options
;
```

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

```
; -----
DB2                DB2                ; (S) DB2 subsystem name
                                   ; The default name is DB2

DB2PLAN            EZAFTPMQ           ; DB2 plan name for FTP client
                                   ; The default name is EZAFTPMQ

SPREAD             FALSE              ; (S) SQL spreadsheet output format
                                   ; TRUE  = Spreadsheet format
                                   ; FALSE = Not spreadsheet
                                   ;          format (D)

SQLCOL             NAMES              ; (S) SQL output headings
                                   ; NAMES  = Use column names (D)
                                   ; LABELS = Use column labels
                                   ; ANY    = Use label if defined,
                                   ;          else use name

; -----
;
; 7. Security options
;
; -----

SECURE_MECHANISM  TLS                ; Name of the security mechanism
;SECURE_MECHANISM  GSSAPI              ; Name of the security mechanism
                                   ; that the client uses when it
                                   ; sends an AUTH command to the
                                   ; server.
                                   ; GSSAPI = Kerberos support
                                   ; TLS    = TLS

SECURE_FTP       ALLOWED            ; Authentication indicator
;SECURE_FTP       ALLOWED              ; Authentication indicator
                                   ; ALLOWED      (D)
                                   ; REQUIRED

TLSMECHANISM    ATTLS
;
;
SECURE_CTRLCONN PRIVATE            ; Minimum level of security for
;SECURE_CTRLCONN  CLEAR               ; Minimum level of security for
                                   ; the control connection
                                   ; CLEAR      (D)
                                   ; SAFE
                                   ; PRIVATE

SECURE_DATACONN PRIVATE            ; Minimum level of security for
;SECURE_DATACONN  CLEAR               ; Minimum level of security for
                                   ; the data connection
                                   ; NEVER
                                   ; CLEAR      (D)
                                   ; SAFE
                                   ; PRIVATE

SECURE_HOSTNAME OPTIONAL          ; Authentication of hostname in
```

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

```

;SECURE_HOSTNAME    OPTIONAL                ; Authentication of hostname in
                                           ; the server certificate
                                           ; OPTIONAL (D)
                                           ; REQUIRED

;SECURE_PBSZ        16384                   ; Kerberos maximum size of the
                                           ; encoded data blocks
                                           ; Default value is 16384
                                           ; Valid range is 512 through 32768

; Name of a ciphersuite that can be passed to the partner during
; the TLS handshake. None, some, or all of the following may be
; specified. The number to the far right is the cipherspec id
; that corresponds to the ciphersuite's name.
;CIPHERSUITE        SSL_NULL_MD5            ; 01
;CIPHERSUITE        SSL_NULL_SHA            ; 02
;CIPHERSUITE        SSL_RC4_MD5_EX         ; 03
;CIPHERSUITE        SSL_RC4_MD5            ; 04
;CIPHERSUITE        SSL_RC4_SHA            ; 05
;CIPHERSUITE        SSL_RC2_MD5_EX         ; 06
;CIPHERSUITE        SSL_DES_SHA            ; 09
;CIPHERSUITE        SSL_3DES_SHA           ; 0A
;CIPHERSUITE        SSL_AES_128_SHA        ; 2F
;CIPHERSUITE        SSL_AES_256_SHA        ; 35

;KEYRING            name                    ; Name of the keyring for TLS
                                           ; It can be the name of a z/OS
                                           ; Unix
                                           ; file (name starts with /) or
                                           ; a resource name in the security
                                           ; product (e.g., RACF)

;TLSTIMEOUT         100                    ; Maximum time limit between full
                                           ; TLS handshakes to protect data
                                           ; connections
                                           ; Default value is 100 seconds.
                                           ; Valid range is 0 through 86400

;SECUREIMPLICITZOS  TRUE                   ; (S) Specify whether client will
                                           ; connect to a z/OS FTP server
                                           ; when connecting to the TLS port.
                                           ; TRUE (D)
                                           ; FALSE Use FALSE if server is
                                           ; not z/OS or when not connecting
                                           ; to the TLS port as specified by
                                           ; the TLSPOST statement.

;TLSPOST            990                    ; Specify which FTP port is
                                           ; implicitly secured with TLS
                                           ; 0 disable implicit security
                                           ; 990 (D) default value
                                           ; Valid range is 0 to 65534

TLSRFCLEVEL       RFC4217                ; (S) Specify what level of RFC
;TLSRFCLEVEL        DRAFT                  ; (S) Specify what level of RFC
                                           ; 4217,
                                           ; On Securing ; FTP with TLS, is

```

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

```

; supported
; DRAFT (D) Internet Draft level
; RFC4217 RFC level
; -----
;
; 8. Timers
;
; -----

CCONNTIME          30          ; Timeout value for successful
                               ; close of control connection.
                               ; Default value is 30 seconds.
                               ; Valid range is 15 through 86400.
                               ; 0 = do not timeout

DATACTIME          120         ; Timeout for send/receive data
                               ; operations.
                               ; Default value is 120 seconds.
                               ; Valid range is 15 through 86400.
                               ; 0 = do not timeout

;DATAKEEPLIVE      0           ; (S) Keepalive packets are sent
                               ; after the data connection is
                               ; idle for the specified number
                               ; of seconds on the data
                               ; connection.
                               ; 0 seconds (D)
                               ; 0 = use keepalive interval
                               ; configured in the PROFILE.TCPIP
                               ; for passive mode and no
                               ; keepalive
                               ; packets for active mode
                               ; Valid range is 60 - 86400

DCONNTIME          120         ; Timeout value for successful
                               ; close of data connection.
                               ; Default value is 120 seconds.
                               ; Valid range is 15 through 86400.
                               ; 0 = do not timeout

;DSWAITTIME        0           ; (S) The approximate number of
                               ; minutes ftp waits when trying
                               ; to access an MVS data set.
                               ; Default is 0 minutes
                               ; 0 (D)
                               ; Valid range is 0 - 14400

FTPKEEPLIVE        0           ; Keepalive packets are sent after
                               ; the control connection is
                               ; idle for the specified number
                               ; of seconds
                               ; Default is 0 seconds
                               ; 0 = do not send keepalive
                               ; packets
                               ; Valid range is 60 - 86400

INACTTIME          120         ; The time in seconds to wait for
```

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

```

; an expected response from the
; server.
; Default value is 120 seconds.
; Valid range is 15 through 86400.
; 0 = do not timeout

MYOPENTIME      60      ; Connection timeout value in
; seconds.
; Default value is 60 seconds.
; Valid range is 15 through 86400.
; 0 = do not timeout

PROGRESS        10      ; Time interval in seconds between
; progress updates for file
; transfers. Default is 10
; seconds
; Valid range is 10 through 86400,
; or 0 to request no updates.

; -----
;
; 9. Return codes
;
; -----

;CLIENTERRCODES      FALSE      ; Return code format
; TRUE - 2 digit error return code
; FALSE (D) - 5 digit XXYYY format
;   XX - FTP subcommand
;   YYY - server reply code
; EXTENDED - 4 digit XXYY format
;   XX - 2 digit error return
;   code
;   YY - FTP subcommand

;CLIENTEXIT          FALSE      ; Specify whether the FTP client
; exits with a nonzero MVS return
; code for certain FTP errors.
; TRUE          - Yes
; FALSE (D)      - No

LOGCLIENTERR         TRUE      ; Report errors with EZZ9830I msg?
;LOGCLIENTERR        FALSE      ; Report errors with EZZ9830I msg?
; TRUE          - Yes
; FALSE (D)      - No

; -----
;
; 10. Checkpoint / Restart options
;
; -----

CHKPTINT           0      ; (S) Specify the checkpoint interval
; in number of records.
; NB: checkpointing only works
; with datatype EBCDIC and block
; or compressed transfer mode.
```

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

```

; 0 = no checkpoints (D)

;CHKPTFLUSH      FALSE      ; (S) Whether flush checkpoint
;                  ; information from buffer to
;                  ; storage media as each record is
;                  ; written?
;                  ; TRUE      - Yes
;                  ; FALSE (D) - No

RESTGET          TRUE       ; (S) Should checkpointing occur
;                  ; during
;                  ; a GET operation?
;                  ; TRUE (D) - Yes
;                  ; FALSE    - No

CHKPTPREFIX      HOME      ; (S) Low level qualifier of
;                  ; checkpoint
;                  ; data set: FTP.CHECKPOINT
;                  ; HOME (D) - either TSO prefix or
;                  ;          UNIX local directory path
;                  ; USERID - login user ID
;                  ; LOCAL - current local directory

; -----
;
; 11. SOCKS server options
;
; -----

;SOCKSCONFIGFILE  /etc/socks.conf ; file path for SOCKS
;                  ; configuration
;                  ; file. The SOCKS configuration
;                  ; file specifies which FTP servers
;                  ; should be accessed via SOCKS.

; -----
;
; 12. Debug (trace) options
;
; -----

;DEBUG           TIME      ; time stamp client trace
;                  ; entries
;DEBUG           ALL       ; activate all traces
;DEBUG           BAS       ; active basic traces
;                  ; (marked with an *)
;DEBUG           FLO       ; function flow
;DEBUG           CMD       ; * command trace
;DEBUG           PAR       ; parser details
;DEBUG           INT       ; * program initialization and
;                  ; termination
;DEBUG           ACC       ; access control (logging in)
;DEBUG           SEC       ; security processing
;DEBUG           SEC       ; security processing
;DEBUG           UTL       ; utility functions
;DEBUG           FSC(1)    ; * file services
```

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

```

;DEBUG          SOC(1)          ; * socket services
;DEBUG          SQL             ;  special SQL processing

; -----
;
; 13. Additional advanced options
;
; -----

CHKCONFIDENCE   FALSE          ; (S) FALSE = (D) Do not perform
                                ;      confidence checks of
                                ;      data transfers.
                                ; TRUE  = Check and report on
                                ;      the confidence in the
                                ;      successful completion of
                                ;      a data transfer. The FTP
                                ;      client reports the level
                                ;      of confidence after each
                                ;      file transfer with the
                                ;      message EZA2108I.

;FWFRIENDLY     FALSE          ; (S) Use firewall friendly protocol
                                ; for starting data connections?
                                ; TRUE - Yes
                                ; FALSE (D) - NO

;EPSV4          FALSE          ; (S) Use NAT firewall friendly
                                ; protocol
                                ; for starting data connections?
                                ; TRUE - Yes
                                ; FALSE (D) - NO

;PASSIVEIGNOREADDR FALSE      ; (S) Specifies whether the FTP client
                                ; should ignore the IP address in
                                ; the FTP server PASV reply for
                                ; the data connection and use the
                                ; IP address that was used to log
                                ; into the FTP server.
                                ; TRUE - Ignore FTP Server PASV
                                ; reply IP address
                                ; FALSE (D) - Use FTP Server PASV
                                ; reply IP address

;NETRCLEVEL     1              ; When logging in, should the FTP
                                ; server's IP addr be converted to
                                ; a host name to use NETRC login
                                ; file?
                                ; 1 (D) - IP addr is not converted
                                ; 2      - IP addr is converted
                                ; 2      - IP addr is converted
;TRACEAPI       CONDITIONAL    ; When the FTP client is invoked
                                ; from the FTP Callable API, write
                                ; records to the API trace spool
                                ; data set based on this setting
                                ; CONDITIONAL (D)
                                ; Trace requests for which the
                                ; application has set the

```

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

```
; FCAI_TraceIt field to
; FCAI_TraceIt_Yes (1)
; ALL
; Trace all requests, regardless
; of the value in FCAI_TraceIt
; NONE
; Trace no requests, regardless
; of the value in FCAI_TraceIt
```

**** Lab L07 SYS1.PROCLIB(FTPT) ****

```
*****
//FTPT PROC MODULE='FTPD',CS=SYS1,DATA=DAT&CL1.A,FDAT=FTPSEC,PARMS=' '
//FTPD EXEC PGM=&MODULE,REGION=0M,TIME=NOLIMIT,
// PARM=('POSIX(ON) ALL31(ON) ',
// 'ENVAR("_BPXK_SETIBMOPT_TRANSPORT=TCPIPT"',
// '"_BPX_JOBNAME=TCPTFTP"',
// '"TZ=EST5EDT")/&PARMS')
//* CS=USER
//* CS=SYS1
//* FDAT=FTPDATA
//* FDAT=FTPSEC
//* FTPT PROC MODULE='FTPD',CS=SYS1,PARMS=' '
//* PARM=('POSIX(ON) ALL31(ON) ',
//* 'ENVAR("RESOLVER_CONFIG=//'"_BPX_JOBNAME=MYFTP")/'&PARMS')
//*
//* PARM=('POSIX(ON) ALL31(ON) ENVAR("_BPX_JOBNAME=MYFTP")/'&PARMS')
//*
//* PARM=('POSIX(ON) ALL31(ON) ENVAR("KRB5_SERVER_KEYTAB=1")/'&PARMS')
//*
//CEEDUMP DD SYSOUT=*
//SYSFTPD DD DISP=SHR,DSN=&CS..CS.TCPPARMS(&FDAT)
//SYSTCPD DD DISP=SHR,DSN=&CS..CS.TCPPARMS(&DATA)
```

**** Lab L08 USER.CS.TCPPARMS(TNnATTLS) ****

```
*****
; STUDENT VERSION for TTLS
; TN3270 profile for the CS Workshops
; =====
; ===== By Whom? When?
; Change: GJD 08/08/2008
; Created profile for TN3270 proc by copying
; from PRTNCCL1
; Added TCPIPJOBNAME of TCPIPT to TELNETGLOB. GJD 08/08/2008
; CHANGED TO TTLS . GJD 11/29/2009
; =====
;
; TelnetGlobals
;
```

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

```
CodePage ISO8859-1 IBM-1047 ; Linemode ASCII, EBCDIC code pages
;
; Format TELNETDEVICE Devicetype TN3270logmode,TN3270Elogmode
TELNETDEVICE 3278-2-E NSX32702,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3278-2 D4B32782,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3279-2-E NSX32702,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3279-2 D4B32782,D4C32XX3 ; 24 lines, dynamic
TELNETDEVICE 3278-3-E NSX32703,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3278-3 D4B32783,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3279-3-E NSX32703,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3279-3 D4B32783,D4C32XX3 ; 32 lines, dynamic
TELNETDEVICE 3278-4-E NSX32704,D4C32XX3 ; 48 lines, dynamic
TELNETDEVICE 3279-4-E NSX32704,D4C32XX3 ; 48 lines, dynamic
TELNETDEVICE 3278-5-E NSX32705,D4C32XX3 ; 132 columns, dynamic
TELNETDEVICE 3279-5-E NSX32705,D4C32XX3 ; 132 columns, dynamic
TELNETDEVICE LINEMODE INTERACT
TELNETDEVICE IBM-DYNAMIC ,D4C32XX3 ; dynamic user specifies
;
TCPIPJOBNAME TCPIPT
EndTelnetGlobals
;
; -----
; Configure Telnet
; -----
;
; TELNETPARMS: Configure the Telnet Server
;
; - TN3270(E) server port 23 options
;
TelnetParms
  TTLSPORT 23 ; Port number 23 is for AT-TLS
  CONNTYPE SECURE ; SSL/TLS/AT-TLS IS REQUIRED
; DEBUG CONN DETAIL
; EXPRESSLOGON
; RESTRICTAPPL CERTAUTH
; SECUREPORT
; KEYRING
; ENCRYPTION
; CLIENTAUTH
; CRLLDAPSERVER
; SSLV2 or NOSSLV2
; SSLTIMEOUT
CodePage ISO8859-1 IBM-1047 ; Linemode ASCII, EBCDIC code pages
Inactive 0 ; Let connections stay around
LUSESSIONPEND ; On termination of a Telnet server connection,
; the user will revert to the DEFAULTAPPL
; instead of having the connection dropped
; instead of having the connection dropped

MSG07 ; Sends a USS error message to the client if an
; error occurs during session establishment
; instead of dropping the connection

PrtInactive 0 ; Let connections stay around
TimeMark 4500
ScanInterval 900
; SMFinit std
```

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

```
; SMFterm std
SNAEXT
TN3270E
TKOGENLURECON 10 KEEPONTMRESET SAMEIPADDR
; WLMClusterName
;   TN3270E
; EndWLMClusterName
;

EndTelnetParms
;
; TelnetParms
;   Secureport 992 Keyring HFS /tmp/telnet.kdb
; EndTelnetParms
;
; BEGINVTAM: Defines the VTAM parameters required for the Telnet
; server.
;
BeginVTAM
Port 23
; Define the LUs to be used for general users.
DEFAULTLUS
  TCPSna00..TCPSna20
ENDDEFAULTLUS

; DEFAULTAPPL TSO ; Set the default application for all TN3270(E)
; Telnet sessions to TSO

LINEMODEAPPL TSO ; Send all line-mode terminals directly to TSO.

; ALLOWAPPL SAMON QSESSION ; SAMON appl does CLSDST Pass to next appl

ALLOWAPPL TSO* DISCONNECTABLE ; Allow all users access to TSO
; applications.
; TSO is multiple applications all beginning with TSO,
; so use the * to get them all. If a session is closed,
; disconnect the user rather than log off the user.

ALLOWAPPL CNM* DISCONNECTABLE ;NetView
ALLOWAPPL NPM* DISCONNECTABLE ;NPM

ALLOWAPPL F00* DISCONNECTABLE
; ALLOWAPPL F192* DISCONNECTABLE
; ALLOWAPPL F193* DISCONNECTABLE
; ALLOWAPPL * ; Allow all applications that have not been
; ; previously specified to be accessed.
; ALLOWAPPL * DISCONNECTABLE

; RESTRICTAPPL IMS ; Only 3 users can use IMS.
;   USER USER1 ; Allow user1 access.
;   LU TCPIMS01 ; Assign USER1 LU TCPIMS01.
;   USER USER2 ; Allow user2 access from the default LU pool.
;   USER USER3 ; Allow user3 access from 3 Telnet sessions,
; ; each with a different reserved LU.
;   LU TCPIMS31 LU TCPIMS32 LU TCPIMS33

; Map Telnet sessions to display the USSMSG10 from USSTAB USSAPC
```

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

```
USSTCP TCPRAP3
; USSTCP TCPRAP OSATRA10

;   Map Telnet sessions from the SNA1 link to display the USSMSG10
;   screen from USS table USSCBA.

; USSTCP USSCBA SNA1
; LUGROUP  LUGRP1
;         TCPM0001..TCPM0999
;         TCPM1001
; ENDLUGROUP

; LUGROUP  LUGRP2
;         TCPM2001  TCPM2003  TCPM2004
;         TCPM0AAA..TCPM0ZZZ
; ENDLUGROUP

; Define groups of host names
; HNGROUP  HNGRP1
;         TEST1.TCP.RALEIGH.IBM.COM
;         TEST2.TCP.RALEIGH.IBM.COM
;         *.*.RALEIGH.IBM.COM
; ENDHNGROUP

; HNGROUP  HNGRPALL
;         *.*.COM
; ENDHNGROUP

; Map LUs to groups for host names
; LUMAP  LUGRP1  HNGRP1
; LUMAP  LUGRP2  HNGRPALL
; LUMAP  TCPM5000  SPECIAL.TCP.RALEIGH.IBM.COM
EndVTAM
```

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

**** Lab L08 SYS1.PROCLIB(TN3270T) ****

```
//TN3270T PROC PARMS='CTTRACE (CTIEZBTN) ', PROF=TN&CL1.A, CS=SYS1,
//          DATA=DAT&CL1.A
//* CS=SYS1 ... OR ... CS=USER ... OR ... CS=CS
//*TN1A PROC PARMS='CTTRACE (CTIEZBTN) ', PROF=TN&CL1.A, CS=SYS1
//*TN32701A PROC PARMS='CTTRACE (CTIEZBTN) ', PROF=TN&CL1.A, CS=CS
//*
//* FUNCTION: START TN3270 TELNET SERVER
//* *****
//* START WITH CS=USER FOR STUDENTS; START WITH CS=SYS1 FOR INSTRUCTOR
//* *****
//* THE PARM= FIELD IS USED FOR CTTRACE SETUP ONLY
//* CTTRACE PARMLIB MEMBER MAY BE SPECIFIED AS OR TRC=XX SETUP
//* CTTRACE(MEMBER) OR TRC=XX, WHERE XX IS SUFFIX OF CTIEZBXX
//*
//TN3270 EXEC PGM=EZBTNINI, REGION=0M, TIME=1440,
//          PARM='&PARMS '
//*
//*STEPLIB DD          NEEDED IF C LIBRARIES NOT IN LINK LIST
//*
//SYSPRINT DD SYSOUT=*, DCB=(RECFM=VB, LRECL=132, BLKSIZE=136)
//SYSOUT DD SYSOUT=*, DCB=(RECFM=VB, LRECL=132, BLKSIZE=136)
//CEEDUMP DD SYSOUT=*, DCB=(RECFM=VB, LRECL=132, BLKSIZE=136)
//*
//* DATA SET CONTAINING TELNET CONFIGURATION PARAMETERS
//PROFILE DD DSN=&CS..CS.TCPPARMS (&PROF), DISP=SHR
//* DATA SET CONTAINING RESOLVER FOR THIS STACK
//SYSTCPD DD DSN=&CS..CS.TCPPARMS (&DATA), DISP=SHR
//*
```

**** Lab L10 SYS1.PROCLIB(TRMDT) ****

```
//TRMDT PROC DATA=DAT&CL1.A,
//      CS=SYS1
//* CS=USER
//*
//* IBM Communications Server for z/OS
//* SMP/E distribution name: EZATRMDP
//*
//* 5694-A01 (C) Copyright IBM Corp. 1996, 2005.
//* Licensed Materials - Property of IBM
//* "Restricted Materials of IBM"
//*
//* Status = CSV1R7
//*
//* Function: Sample procedure for running the Traffic
//*           Regulator Management Daemon (TRMD)
//*
//TRMD EXEC PGM=EZATRMD, REGION=4096K, TIME=NOLIMIT,
```

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

```
// PARM=('POSIX(ON) ALL31(ON) ',
// 'ENVAR("RESOLVER_CONFIG=/'&CS..CS.TCPPARMS(&DATA)'"') ',
// 'TZ=EST5EDT'/' )
// * 'TZ=EST'/' -d1')
// *
// *** Notes:
// *
// * - TRMD can also be invoked from the Unix System Services shell
// * as a shell command: trmd
// *
// * - The system link list concatenation must contain the TCP/IP
// * runtime libraries and the C runtime libraries. If they are
// * not in the link list concatenation, this procedure will need
// * to be changed to STEPLIB to them.
// *
// * - To pass parameters to TRMD, specify them after the final slash
// * on the PARM statement. For example:
// * // PARM=('POSIX(ON) ALL31(ON) /-d 1')
// * 'ENVAR("LIBPATH=/usr/lib")/' )
// *
// * - TRMD must find the TCP/IP job name with which it should be
// * associated. It uses the TCPIPJOBNAME value from the TCPIP.DATA
// * file. The TCPIP.DATA file used can be controlled by setting the
// * RESOLVER_CONFIG environment variable. See examples below.
// *
// *** Examples for specifying configuration data sets
// *
// * Example 1: TCPIP.DATA in partitioned data set
// *
// * // PARM=('POSIX(ON) ALL31(ON) ',
// * // 'ENVAR("RESOLVER_CONFIG=/'SYS1.TCPPARMS(TCPDATA)'"')/' )
// *
// * Example 2: TCPIP.DATA in HFS file
// *
// * // PARM=('POSIX(ON) ALL31(ON) ',
// * // 'ENVAR("RESOLVER_CONFIG=/etc/resolv.conf")/' )
// *
// * Example 3: Specification of data sets via STDENV DD statement
// *
// * // PARM=('POSIX(ON) ALL31(ON) ',
// * // 'ENVAR("_CEE_ENVFILE=DD:STDENV")/' )
// *
// * For this method, the STDENV DD statement below must be
// * changed to point to a data set containing settings for any
// * environment variables. For example, it can contain
// *
// * RESOLVER_CONFIG=/'SYS1.TCPPARMS(TCPDATA) '
// * LIBPATH=/usr/lib:
// *
// * The use of the STDENV DD statement works well when more than
// * one environment variable is specified, as there is a JCL limit
// * of 100 characters on the PARM= statement.
// * Note: Language Environment recommends
// * the record format of this file be variable.
// *
// STDENV DD DUMMY
// SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
```

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

```
//SYSIN      DD DUMMY
//SYSERR      DD SYSOUT=*
//SYSOUT      DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//CEEDUMP     DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

**** Lab L11 USER.CS.TCPPARMS(TCPnAIPS) ****

```
;
; PROFILE.TCPIP for the CS Networking WORKSHOP (STUDENT VERSION)
; =====
;   Change:                                By Whom?   When?
; =====
; Add STATIC VIPA                          GJD         08/18/08
; Add Dynamic VIPAs to coord. with PROFCS1  GJD         08/18/08
; Add DYNAMIC XCF to coord with PROFCS1    GJD         08/18/08
; Added IPSECURITY and SRCIP sections.     LLH         11/24/09
; =====
; =====
; General TCP/IP address space configuration
; =====
;
; GLOBALCONFIG: Provides settings for the entire TCP/IP stack
;
GLOBALCONFIG TCPIPSTATISTICS
;
; IPCONFIG: Provides settings for the IP layer of TCP/IP.
;
IPCONFIG DATAGRAMFWD SYSPLEXROUTING IGNOREREDIRECT
SOURCEVIPA MULTIPATH PATHMTUDISCOVERY TTL 64 DEVRETRYDUR 90
IGNOREREDIRECT ARPTO 1200
IPCONFIG DYNAMICXCF 10.1.1.&CL1 255.255.255.0 2
;
; =====
; Uncomment the line below to enable IP Filtering and IPsec
; IPCONFIG IPSECURITY
; =====
;
; SOMAXCONN: Specifies maximum length for the connection request queue
;   created by the socket call listen().
;
SOMAXCONN 1000
;
;
; TCPCONFIG: Provides settings for the TCP layer of TCP/IP.
;
;   RESTRICTLOWPORTS limits access to ports below 1024
;   to APF authorized or superuser applications.
;
TCPCONFIG TCPSENDBFRSIZE 32K TCPCVBUFRSIZE 32K TCPMAXRCVBUFRSIZE 256K
TCPCONFIG RESTRICTLOWPORTS FINWAIT2Time 600 INTerval 120
TCPCONFIG SENDGARBAGE FALSE TCPTIMEstamp DELAYACKS
TCPCONFIG TTLS
;
;
; UDPCONFIG: Provides settings for the UDP layer of TCP/IP
```

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

```
;          RESTRICTLOWPORTS limits access to ports below 1024
;          to APF authorized or superuser applications.
;
UDPCONFIG RESTRICTLOWPORTS
;
; SRCIP allows the substitution of the source IP address on a
; jobname specific basis for client applications which specify
; inaddr_any for the source IP address. This may be done when
; an application issues an explicit bind() call with inaddr_any
; or when it bypasses issuing an explicit bind() call and
; issues a connect().
;
;SRCIP
; JOBNAME USER15  9.43.242.5
; JOBNAME USER*   9.43.242.4
; JOBNAME USER15  2001::092B:F203
; JOBNAME JOB*    ETHER1
; JOBNAME *       9.43.242.3
;ENDSRCIP
;
; =====
; Uncomment the lines below to enable source routing to MVS1
SRCIP
  DESTINATION 192.168.20.91 192.168.20.9n
  DESTINATION 192.168.20.101 192.168.20.10n
  DESTINATION 192.168.20.121 192.168.20.12n
  DESTINATION 10.1.1.0/24 10.1.1.n
ENDSRCIP
; =====
;
; =====
; Hardware definitions
; =====
; DEVICE: Defines name (and sometimes device number) for various types
;   of network devices for IPv4 only
; LINK: Defines a network interface to be associated with a particular
;   device. For IPv4 only.
; INTERFACE: Defines an IPv6 interface.
;
; Gigabit Ethernet connected to CISCO 6513 Switch:
; Layer3 on MVS and Linux Systems in 192.168.20.0/24 network
; Layer2 on Linux Systems in 10.168.20.0/24 network
;GbE --- CHPID 1F -----
;
DEVICE GIG1F MPCIPA SECROUTER AUTORESTART
LINK LGIG1F IPAQENET GIG1F
; -----
; Virtual device definitions
; -----
;
; DEVICE and LINK for Virtual Devices (VIPA):
;
;   DEVICE VDEV1 VIRTUAL 0
;   LINK VLINK1 VIRTUAL 0 VDEV1
;
;
VIPADYNAMIC
```

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

```

VIPADefine      MOVEABLE IMMEDIATE 255.255.255.240 192.168.20.11y
VIPABackup 100  MOVEABLE IMMEDIATE 255.255.255.240 192.168.20.12n
;  VIPARange Define 255.255.255.192 201.2.10.192
ENDVIPADynamic
;
; =====
; HOME addresses
; =====
;
; HOME: Provides the list of home IP addresses and associated link
; names
;
HOME
192.168.20.10n VLink1
192.168.20.9n  LGIG1F
;
; PRIMARYInterface: Specifies which link is designated as the default
; local host for use by the GETHOSTID() function.
;
; =====
; Routing configuration
; =====
; -----
; Static routing
; -----
;
; BEGINRoutes: Defines static routes to the IP route table.
;
BEGINRoutes
;
; Direct Routes - Routes that are directly connected to my interfaces.
;
;      Destination Subnet Mask      First Hop      Link Name Packet Size
;
ROUTE 192.168.20.0/24              =              LGIG1F      MTU 1492
;
; Default Route - All packets to an unknown destination are routed
;                  through this route.
;
;      Destination Subnet Mask      First Hop      Link Name Packet Size
;
ROUTE DEFAULT                      192.168.20.1  LGIG1F      MTU 1492
ENDRoutes
;
; -----
; Dynamic routing
; -----
;
; =====
; Application configuration
; =====
;
; AUTOLOG: Supplies TCPIP with the procedure names to start and the
; timeout value to use for a hung procedure during AUTOLOG.
;
; AUTOLOG 5
;  FTPCCL                      ; FTP Server

```

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

```
; ENDAUTOLOG
;
;
; PORT: Reserves a port for specified job names
PORT
    7 UDP MISCSERV          ; Miscellaneous Server - echo
    7 TCP MISCSERV          ; Miscellaneous Server - echo
    9 UDP MISCSERV          ; Miscellaneous Server - discard
    9 TCP MISCSERV          ; Miscellaneous Server - discard
    19 UDP MISCSERV         ; Miscellaneous Server - chargen
    19 TCP MISCSERV         ; Miscellaneous Server - chargen
    20 TCP * NOAUTOLOG      ; FTP Server Data Connection
; 21 TCP FTPSERVE          ; FTP Server
; 21 TCP FTPT111           ; FTP Server Control Connection
    22 TCP OMVS             ; SSHD
    21 TCP *               ; FTP Server Control Connection
; 23 TCP INTCLIEN         ; Telnet 3270 Server
; 23 TCP TN3270&CL1.A      ; Telnet 3270 Server
    23 TCP TN3270T         ; Telnet 3270 Server for CS Networking
    25 TCP SMTP            ; SMTP Server
    53 TCP NAMED           ; Domain Name Server
    53 UDP NAMED           ; Domain Name Server
    111 TCP PORTMAP        ; Portmap Server (SUN 3.9)
    111 UDP PORTMAP        ; Portmap Server (SUN 3.9)
    135 UDP LLBD           ; NCS Location Broker
    161 UDP OSNMPD         ; SNMP Agent
    162 UDP SNMPQE         ; SNMP Query Engine
    512 TCP RXSERVE        ; Remote Execution Server
    514 TCP RXSERVE        ; Remote Execution Server
    515 TCP LPSERVE        ; LPD Server
    520 UDP OROUTED        ; OROUTED Server
    580 UDP NCPROUT        ; NCPROUTE Server
    750 TCP MVSKERB        ; Kerberos
;   PORTRANGE 5000 6000 TCP * SAF RANGE1
;
; SCONFIG: Configures the TCP/IP SNMP subagent
;
; SCONFIG ENABLED COMMUNITY fred AGENT 161
;
;
; -----
; Configure Network Access Control
; -----
; NETACCESS      INBOUND      OUTBOUND      ; check both ways
;   DEFAULTHOME      HOME      ; Optional Default local
;   DEFAULT          DEFZONE   ; Optional Default zone
;   192.168.0.0/16    CORPNET   ; Net address
;   192.168.113.19/32 HOST1    ; Specific host address
;   192.168.113.0     255.255.255.0 SUBNET1 ; Subnet address
;   192.168.112.0     255.255.248.0 SUBNET2 ; Subnet address
;   192.168.192.0/24  CAMPUS    ; Subnet address
;   192.168.214.0/24  CAMPUS    ; Subnet address
;   fe80::6:2900:1dc:21bc/128 HOST2    ; IPv6 specific host
; ENDNETACCESS
;
; -----
; Configure IPSECURITY default filter rules
```

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

```
; -----
;
; Example IPSEC default filter rule. This rule permits
; outbound TCP traffic from local IP address 1.1.1.1 port 23 to
; remote IP address 2.2.2.2. The same rule also permits
; inbound TCP traffic from remote IP address 2.2.2.2 to local
; IP address 1.1.1.1 port 23.
;
; IPSEC LOGDISABLE NOLOGIMPLICIT
; Rule SrcIp DestIp Log Prot SrcPort DestPort Secclass
; IPSECR 1.1.1.1 2.2.2.2 NOLOG PROTO TCP SRCPORT 23 DSTPORT *
; ENDIPSEC
;
IPSEC LOGENABLE LOGIMPLICIT
IPSECRULE * * NOLOG PROTOCOL OSPF
IPSECRULE * * NOLOG PROTOCOL 2
IPSECRULE * * LOG PROTOCOL TCP SRCPORT * DESTPORT 4159
IPSECRULE * 192.168.0.0/16 LOG PROTOCOL *
ENDIPSEC
;
; Example IPSEC default filter rule. This rule permits
; outbound TCP traffic from local IP address 1.1.1.1 port 23 to
; remote IP address 2.2.2.2. The same rule also permits
; inbound TCP traffic from remote IP address 2.2.2.2 to local
; IP address 1.1.1.1 port 23.
;
; IPSEC LOGDISABLE NOLOGIMPLICIT
; Rule SrcIp DestIp Log Prot SrcPort DestPort Secclass
; IPSECR 1.1.1.1 2.2.2.2 NOLOG PROTO TCP SRCPORT 23 DSTPORT *
; ENDIPSEC
;
; =====
; Diagnostic data statements (ITRACE, PKTTRACE, SMFCONFIG, SMFPARMS)
; =====
;
; =====
; Other statements
; =====
;
; DELETE: Removes an ATMARPSV, ATMLIS, ATMPVC, device, link, port or
; portrange. This statement is typically done via an copy file, not
; in an initial profile.
;
; STOP: Stops a device. If used, this statement is typically put in
; an obey file, not in an initial profile.
;
; INCLUDE: Causes another data set that contains profile configuration
; statements to be included at this point.
;
; START: Starts a device or interface that is currently stopped.
;
; -----
;
START GIG1F
```

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

***** **Lab L11 SYS1.PROCLIB(IKED)** *****

```
//IKED      PROC
//*
//* SAMPLE IKE DAEMON START PROCEDURE FOR:
//*      IMAGE: MVS1
//*
//* CREATED BY THE IBM CONFIGURATION ASSISTANT FOR Z/OS COMMUNICATIONS
//* SERVER
//* VERSION 1 RELEASE 10
//* DATE CREATED = MON NOV 23 22:01:43 EST 2009
//*
//* COPYRIGHT =  NONE
//*
//IKED      EXEC PGM=IKED,REGION=0K,TIME=NOLIMIT,
//          PARM='ENVAR("_CEE_ENVFILE=DD:STDENV")/'
//*
//* PROVIDE ENVIRONMENT VARIABLES TO RUN WITH THE DESIRED
//* CONFIGURATION.  AS AN EXAMPLE, THE DATA SET OR FILE SPECIFIED BY
//* STDENV COULD CONTAIN:
//*
//*      IKED_FILE=/ETC/SECURITY/IKED.CONF
//*      IKED_CTRACE_MEMBER=CTIIKE01
//*
//* FOR INFORMATION ON THE ABOVE ENVIRONMENT VARIABLES, REFER TO THE
//* Z/OS COMMUNICATIONS SERVER: IP CONFIGURATION REFERENCE.
//*
//STDENV    DD DUMMY
//* SAMPLE MVS DATA SET CONTAINING ENVIRONMENT VARIABLES:
//*STDENV    DD DSN=TCPIP.IKED.ENV(IKED),DISP=SHR
//* SAMPLE HFS FILE CONTAINING ENVIRONMENT VARIABLES:
//*STDENV    DD PATH='/ETC/SECURITY/IKED.ENV',PATHOPTS=(ORDONLY)
//*
//* OUTPUT WRITTEN TO STDOUT AND STDERR GOES TO THE DATA SET OR
//* FILE SPECIFIED WITH SYSPRINT OR SYSOUT, RESPECTIVELY.
//SYSPRINT  DD SYSOUT=*
//SYSOUT    DD SYSOUT=*
```

***** **Lab L16 SYS1.PROCLIB(NSSD)** *****

```
//NSSD PROC
//NSSD EXEC PGM=NSSD,REGION=0K,TIME=NOLIMIT,
// PARM='ENVAR("_CEE_ENVFILE_S=DD:STDENV")/'
//*
//* Provide environment variables to run with the desired
//* configuration. As an example, the data set or file specified by
//* STDENV could contain:
//*
//*      NSSD_FILE=/etc/security/nssd.conf
//*      NSSD_CTRACE_MEMBER=CTINSS01
//*      NSSD_CODEPAGE=IBM-1047
```

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

```
/*
/* If you want to include comments in the data set or
/* z/OS UNIX file, specify the _CEE_ENVFILE_COMMENT
/* environment variable as the first environment variable
/* in the data set or file. The value specified for
/* the _CEE_ENVFILE_COMMENT variable is the comment character.
/* For example, if you want to use the pound sign, #, as
/* the comment character, specify this as the first
/* statement:
/*     _CEE_ENVFILE_COMMENT=#
/*
/* For information on the above environment variables, refer to the
/* IP Configuration Reference.
/*
//STDENV DD DUMMY
/* Sample MVS data set containing environment variables:
/*STDENV DD DSN=TCPIP.NSSD.ENV(NSSD),DISP=SHR
/* Sample file containing environment variables:
/*STDENV DD PATH='/etc/security/nssd.env',PATHOPTS=(ORDONLY)
/*
/* Output written to stdout and stderr goes to the data set or
/* file specified with SYSPRINT or SYSOUT, respectively.
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
```

***** **Lab L17 SYS1.PROCLIB(DMD)** *****

```
//DMD PROC
/*
/* IBM Communications Server for z/OS
/* SMP/E distribution name: EZADMD
/*
/* 5650-ZOS Copyright IBM Corp. 2008, 2013
/* Licensed Materials - Property of IBM
/* Status = CSV2R1
/*
/*
//DMD EXEC PGM=DMD,REGION=0K,TIME=NOLIMIT,
// PARM='ENVAR("_CEE_ENVFILE_S=DD:STDENV")/'
/*
/* Provide environment variables to run with the desired
/* configuration. As an example, the data set or file specified by
/* STDENV could contain:
/*
/* DMD_FILE=/etc/security/dmd.conf
/* DMD_CTRACE_MEMBER=CTIDMD00
/* DMD_PIDFILE=/var/dm/dmd.pid
/* DMD_CODEPAGE=IBM-1047
/*
/* If you want to include comments in the data set or
/* z/OS UNIX file, specify the _CEE_ENVFILE_COMMENT
/* environment variable as the first environment variable
/* in the data set or file. The value specified for
/* the _CEE_ENVFILE_COMMENT variable is the comment character.
```

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

```
/* For example, if you want to use the pound sign, #, as
/* the comment character, specify this as the first
/* statement:
/*      _CEE_ENVFILE_COMMENT=#
/*
/* For information on the above environment variables, refer to the
/* IP Configuration Reference.
/*
/*STDENV DD DUMMY
/* Sample MVS data set containing environment variables:
/*STDENV DD DSN=TCPIP.DMD.ENV(DMD),DISP=SHR
/* Sample file containing environment variables:
/*STDENV DD PATH='/etc/security/dmd.env',PATHOPTS=(ORDONLY)
/*
/* Output written to stdout and stderr goes to the data set or
/* file specified with SYSPRINT or SYSOUT, respectively.
/*SYSPRINT DD SYSOUT=*
/*SYSOUT DD SYSOUT=*
```

Unix Files

***** **Lab L02 /etc/syslog.conf** *****

```
# Licensed Materials - Property of IBM
# 5694-A01
# (C) Copyright IBM Corp. 2007
# Status = CSV1R9
#
# /etc/syslog.conf - control output of syslogd
#
# The # sign begins a comment which extends to the end of the line.
#
# Blank lines are ignored.
#
# Rules in this file specify types of messages which syslogd will
# store, and where syslogd will store it.
#
# See IP Configuration Reference for detailed information about
# the syntax. These comments are meant to provide only a general
# overview.
#
# Four criteria can be used to select locally generated
# messages for processing:
#
# 1) user ID associated with application generating the message
#
# * can be specified for the user ID if the user ID is not
# important.
#
# 2) job name of application generating the message
#
# * can be specified for the job name if the job name is not
# important.
#
# 3) facility of the message, as specified by the application
#
# This is user, mail, news, uucp, daemon, auth, cron, lpr, or
# local0-local7. Consult the documentation for the application
# to determine which facility the application specifies.
#
# A special facility, mark, specifies that syslogd should log
# mark messages on a regular basis. These can be used to verify
# that syslogd was operational during a specific time interval.
#
# 4) priority of the message, as specified by the application
#
# This is emerg, panic, alert, crit, err, error, warn, warning,
# notice, info, or debug.
#
# A special priority, none, specifies that messages with the
# specified user ID, job name, or facility should not be
```

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

```
#      selected.
#
# These criteria are specified together as
#
#      userid.jobname.facility.priority
#
# or, if user ID and job name are both *, as
#
#      facility.priority
#
# This can be combined in a series as
#
#      userid.jobname.facility.priority;userid.jobname.facility.priority
#
# Three criteria can be used to select messages received over the
# network for processing:
#
# 1) IP address or hostname of the sender. The IP address may be in
#    IPv4 or IPv6 format or may be a hostname that resolves to an
#    IPv4 or IPv6 address. If an IP address is used, an optional prefix
#    length may be specified with the /x notation.
#
# 2) facility of the message. See the description of facility above.
# 3) priority of the message. See the description of priority above.
#
# These criteria can be specified together as
#
#      (ip_address).facility.priority
#
#      or
#
#      (hostname).facility.priority
#
# If the the IP address or hostname is not to be considered in
# selecting the
# rule, then omit it and specify just facility.priority
#
# The following rule will match locally generated messages or
# messages received over the network from any source IP address
# that have the specified facility and priority.
#
# facility.priority
#
# The criteria for selecting messages for processing are combined
# with a destination, which tells syslogd what to do with selected
# messages.
#
#      criteria      destination
#
# The destination can be a file, one or more user IDs, SMF, syslogd
# at a remote host, or all logged-in users, or the operlog log stream.
#
# If the destination is a file, it may be optionally followed by two
# options, -F and -D. -F should be followed by an octal number that
# indicates the permissions value to be used if syslogd must create
# the file. -D should be followed by an octal number that indicates
```

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

```
# the permissions value to be used if syslogd must create the
# directory to contain the file. These options are only effective
# if syslogd is started with the -c start option. See the
# Communications Server IP Configuration Reference for details.
#
# The following example stores messages with facility daemon or
# local1 in the file /directory/logfile.
#
#   daemon.*;local1.*    /directory/logfile
#
# The directory structure used in this sample configuration is
# expected to be created automatically by syslogd, with a new
# directory of log files for each day. This requires two types
# of configurations outside of the scope of this configuration
# file:
#
# 1) syslogd command-line option
#
#   The syslogd -c command-line option should be enabled, causing
#   syslogd to create log files and directories if they do not
#   already exist.
#
# 2) cron job
#
#   A cron job should be utilized to wake up syslogd at the
#   beginning of each day to switch to new log files in a new
#   directory. Here is the cron job definition:
#
#       1 0 * * * kill -HUP `cat /etc/syslog.pid`
#
#   This job should be defined for a user ID with UID zero so that
#   it has permissions to send the signal to syslogd.
#
#   See UNIX System Services Planning and UNIX System Services
#   Command Reference for more information about cron.
#
# A sample shell script is provided for removing log files which are
# a specified number of days old. It assumes the same directory
# structure which is used in this sample configuration.
#
# All example rules except for the last one are commented-out. Some
# or all of the example rules will need to be changed for your
# environment. Each example rule contains an explanation of changes
# which may be required.
#
#####
#
# Write all messages with priority crit or higher to the MVS operator
# console. See the UNIX System Services Planning manual for more
# information about the /dev/console special file.
#
# *.crit                /dev/console
#
#####
#
# Write all messages with facility of daemon and a priority of error
# or higher to the operlog log stream. The operlog facility must be
```

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

```
# active in order to be able to log messages to the operlog log
# stream.
#
# daemon.err /dev/operlog
#####
#
# Write all messages from syslogd itself to the file
# /var/log/YYYY/MM/DD/syslogd.log and to the system console.
#
# Notes:
#
# a) If syslogd is invoked as a started task or from a shell script
#     (e.g., /etc/rc) with job name SYSLOGD, the name of the
#     long-running syslogd job is SYSLOGD followed by a digit.
#
#     If syslogd runs with a different job name on your system, the
#     rule will have to be changed accordingly.
#
# b) During initialization, syslogd writes messages to
#     /dev/console. These rules cover messages during steady-
#     state.
#
# *.SYSLOGD*.*.* /var/log/%Y/%m/%d/syslogd
# *.SYSLOGD*.*.* /dev/console
#
#####
#
# Write all messages from inetd to the log file inetd and to the
# console.
#
# Notes:
#
# a) If inetd is invoked as a started task or from a shell script
#     (e.g., /etc/rc) with job name INETD, the name of the
#     long-running inetd job is INETD followed by a digit.
#
#     If inetd runs with a different job name on your system, the rule
#     will have to be changed accordingly.
#
# *.INETD*.*.* /var/log/%Y/%m/%d/inetd
# *.INETD*.*.* /dev/console
#
#####
#
# Write all messages with priority err or higher from applications
# which specify facility "daemon" to the log file daemon.
# Because we chose to log messages from syslogd and inetd separately,
# we'll filter out those messages from this rule using special
# priority none.
#
# Notes:
#
# a) In this example, SYSLOGD followed by some other character is the
#     job name of syslogd. If it is different on your system, change
#     the rule.
# b) In this example, INETD followed by some other character is the
#     job name of inetd. If it is different on your system, change the
```

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

```
# rule.
#
# daemon.err;*.SYSLOGD*.*.none;*.INETD*.*.none /var/log/%Y/%m/%d/daemon
#
#####
#
# Write all messages from applications which specify facility "auth"
# to the log file auth.
#
# auth.* /var/log/%Y/%m/%d/auth
#
#####
#
# Write all messages from applications which specify facility "mail"
# to the log file mail. Use file permissions of 640 octal if the file
# has to be created. Use permission of 770 octal if the directory has
# to be created. syslogd must be started with -c for these options
# to have any effect.
#
# mail.* /var/log/%Y/%m/%d/mail -F 640 -D 770
#
#####
#
# Write all messages with priority err and higher from otelnetd and
# other applications which specify facility "local1" to the log file
# local1.
#
# local1.err          /var/log/%Y/%m/%d/local1
#
#####
#
# Write all messages from otelnetd and other applications which
# specify facility "local1" when running as user SMITH to the log file
# local1.smith. This could be useful if, for example, otelnetd traces
# need to be collected for a problem which user SMITH is experiencing
# and you do not wish to collect otelnetd traces from all user IDs.
#
# Smith.*.local1.*    /var/log/%Y/%m/%d/local1.smith
#
#####
#
# Write all messages with priority err and higher to SMF. These will
# be stored in SMF record type 109. SMF must be active and
# configured to accept record type 109. The user ID associated with
# syslogd must have read access to BPX.SMF. See UNIX System Services
# Planning for more information about BPX.SMF.
#
# *.err              $SMF
#
#####
#
# Write all messages with priority crit and higher to the syslogd on
# host 192.168.1.9. The host may be specified by IPv4 address, by IPv6
# address, or by a name that resolves to an IPv4 or IPv6 address.
#
# *.crit             @192.168.1.9
#
```

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

```
#####  
#  
# Write all messages with priority crit and higher that arrive from  
# host 192.168.0.6 to the operlog log stream.  
#  
# (192.168.0.6).*.crit          /dev/operlog  
#  
#####  
#  
# Write all messages with priority crit and higher that arrive from  
# any host with IP address in the range 192.168.0.0 to 192.168.0.255  
# to the operlog log stream.  
#  
# (192.168.0.6/24).*.crit      /dev/operlog  
#  
#####  
#  
# Write all messages with priority err and higher to log file errors.  
#  
# THIS EXAMPLE STATEMENT IS UNCOMMENTED.  
#  
# *.err                        /var/log/%Y/%m/%d/errors  
# local4.*                    /var/CSLOG/ipsec.log  
# local4.none;*.              /var/CSLOG/syslogall.log  
# *.                           /var/CSLOG/syslogall.log  
#
```

***** **Lab L02 /etc/rc** *****

```
# Initialization shell script, pathname = /etc/rc
```

```
# Initial setup for z/OS UNIX
```

```
export _BPX_JOBNAME='ETCRC'
```

```
# Provide z/OS UNIX Startup Diagnostics
```

```
set -v -x
```

```
# Setup utmpx file
```

```
>/etc/utmpx
```

```
chmod 644 /etc/utmpx
```

```
# Reset all slave tty files
```

```
chmod 666 /dev/tty*
```

```
chown 0 /dev/tty*
```

```
# Allow only file owner to remove files from /tmp
```

```
chmod 1777 /tmp
```

```
# Allow only file owner to remove files from /var
```

```
chmod 1777 /var
```

```
# Allow only file owner to remove files from /dev
```

```
chmod 1755 /dev
```

```
# Setup write, talk, mesg utilities
```

```
# chgrp TTY    /bin/write
```

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

```
# chgrp TTY    /bin/mesg
# chgrp TTY    /bin/talk
# chmod 2755  /bin/write
# chmod 2755  /bin/mesg
# chmod 2755  /bin/talk
# Now performed when running FOMISCHO job
# Commented out in HOT6609

# Setup mailx utility
# No need to CHGRP /usr/mail directory
# No need to CHGRP mailx utility
# No need to CHMOD mailx to turn on SETGID

# Setup uucp utility
# chown uucp:uucpg /usr/lib/uucp
# chown uucp:uucpg /usr/lib/uucp/IBM
# chown uucp:uucpg /usr/spool/uucp
# chown uucp:uucpg /usr/spool/locks
# chown uucp:uucpg /usr/spool/uucppublic
# chown uucp:uucpg /usr/spool/uucp/.Xqtdir
# chown uucp:uucpg /usr/spool/uucp/.Sequence
# chown uucp:uucpg /usr/spool/uucp/.Status
# chown uucp:uucpg /bin/uucp
# chown uucp:uucpg /bin/uuname
# chown uucp:uucpg /bin/uustat
# chown uucp:uucpg /bin/uux
# chown uucp:uucpg /usr/lib/uucp/uucico
# chown uucp:uucpg /usr/lib/uucp/uuxqt
# chown uucp:uucpg /usr/lib/uucp/uucc
# chmod 4755 /bin/uucp
# chmod 4755 /bin/uuname
# chmod 4755 /bin/uustat
# chmod 4755 /bin/uux
# chmod 4754 /usr/lib/uucp/uucico
# chmod 4754 /usr/lib/uucp/uuxqt
# chmod 4754 /usr/lib/uucp/uucc
# Now performed when running FOMISCHO job
# Commented out in HOT6609

# Invoke vi recovery
#
#
# mkdir -m 777 /var/tmp
# export TMP_VI="/var/tmp"
mkdir -m 777 /etc/recover
/usr/lib/exrecover

# Create TERMINFO database
# tic /usr/share/lib/terminfo/ibm.ti
# tic /usr/share/lib/terminfo/dec.ti
# tic /usr/share/lib/terminfo/wyse.ti
# tic /usr/share/lib/terminfo/dtterm.ti
# commented tic out in HOT1180 - all TERMINFO files are shipped

# Start the INET daemon for remote login activity
_BPX_JOBNAME='INETD' /usr/sbin/inetd /etc/inetd.conf &
/usr/sbin/automount
```

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

```
#
# Start the SYSLOG daemon for logging UNIX activity (Method V2R10 plus)
# _BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf &
# _BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -c -i -u -f /etc/syslog.conf &
# _BPX_JOBNAME='SYSLOGDC' /usr/sbin/syslogd -c -i -u -f /etc/syslog.conf &
# /usr/sbin/syslogd -f /etc/syslog.conf &
#
# Start the INET daemon for remote login activity
# _BPX_JOBNAME='INETD' /usr/sbin/inetd /etc/inetd.conf &
#
# Start the DHCPD daemon for remote login activity
# _BPX_JOBNAME='DHCPTEST' /usr/lpp/tcpip/sbin/dhcpd -f /etc/dhcpd.conf &
# /usr/lpp/tcpip/sbin/dhcpd -f /etc/dhcpd.conf &
#
# Start the CRON daemon for automated, timed operations
# _BPX_JOBNAME='CRON' /usr/sbin/cron &
# /usr/sbin/cron &
# Start the AUTOMOUNT job
# _BPX_JOBNAME='AUTOMNT' /usr/sbin/automount &
# /usr/sbin/automount &
sleep 5
echo /etc/rc script executed, `date`
```

**** **Lab L12 /etc/security/iked.conf** ****

```
##
## IKE Daemon Configuration file for:
##   Image: ZOSn
##
## Created by the IBM Configuration Assistant for z/OS Communications
## Server
## Version 1 Release 13
## Backing Store = C:\IBM\zCSConfigAssist\V1R13\files\TMnx_IPSecVPN
## Install History:
## 2013-03-15 10:13:15 : usernx to 192.168.20.8n
##
## End of Configuration Assistant information
## The search order used by the IKE daemon to locate the initial
## configuration file is (highest priority listed first):
##
## 1) The name of an HFS file or MVS file specified by the IKED_FILE
##    environment variable.
## 2) /etc/security/iked.conf
##
## Some parameters may be dynamically modified after the
## IKE daemon has been started. The parameters that are
## dynamically modifiable are noted below.
##
## One way of dynamically modifying parameters is to
## update iked.conf file parameters after the IKE daemon has been
## started and then issue a modify command to cause the IKE daemon
## to re-read the file.
##
## Example: MODIFY IKED,REFRESH
```

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

```
## Note: IKED is the IKE daemon procedure name.
##
## After the IKE daemon has been started, a different configuration
## file can be specified by using the Modify command with the FILE
## parameter. This allows modifiable parameters to be
## dynamically altered while the IKE daemon is running. Note that
## the parameter values modified in this fashion are not
## persistent. To make the changes persistent, update the iked.conf
## file that is located at IKE initialization time according to the
## search order described previously.
##
## Example: MODIFY IKED,REFRESH,FILE='/etc/security/iked.conf2'
## Note: IKED is the IKE daemon procedure name.
##
## See the z/OS Communications Server: IP System Administrator's
## Commands book for more information about the modify command.
##
## See the z/OS Communications Server: IP Configuration Reference book
## for more information about the IkeConfig and NssConfig statements
## and their parameters.
IkeConfig
{
# IkeSyslogLevel      0-255                (dynamically modifiable)
# Specifies the level of logging to obtain from the IKE daemon.
# Default:           1
# IkeSyslogLevel      127
# PagentSyslogLevel  0-255                (dynamically modifiable)
# Specifies the level of logging to obtain from pagent through the PAPI
# Default:           0
# PagentSyslogLevel  127                (dynamically modifiable)

# Keyring              userid/ringname    (not dynamically modifiable)
# The owning userid and ringname used by the IKE server when performing
# RSA Signature Mode of authentication. The userid must be the userid
# of
# the process under which IKE will run.
KeyRing IKED/IKEDnRING

# IkeRetries           1-8                (dynamically modifiable)
# Specifies the number of times that an unanswered IKE negotiation
# message will be retransmitted before the negotiation is cancelled.
# Default:            6

# IkeInitWait          1-15              (dynamically modifiable)
# Specifies the number of seconds to wait before the
# first retransmission of an unanswered IKE message.
# Default:            2

# FIPS140             yes, no            (not dynamically modifiable)
# Specifies whether the IKE daemon should perform cryptographic
# operations by invoking cryptographic modules that are compliant with
# Federal Information Processing Standards (FIPS) publication 140-2's
# Level 1 security requirements.
# Default:            no

# Echo                 yes,no            (dynamically modifiable)
# Echoes all IKE daemon log messages to the job output file,
```

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

```
# specified by the IKEDOUT DD (JCL) statement.
# Default:          no

# PagentWait        0-9999          (not dynamically modifiable)
# The time limit in seconds to wait for connection to the policy agent.
# A value of 0 means retry forever.
# Default:          0

# SMF119    IKEAll,IKETunnel,DynTunnel,None (dynamically modifiable)
# Specifies the level of SMF logging.
# Default:          None

# SupportedCertAuth label          (dynamically modifiable)
# Specifies the label of a Certificate Authority(CA) certificate on the
# IKE server's keyring.  Use multiple instances of this keyword to
# specify
# multiple CA certificates.
}
```

***** **Lab L16 /etc/security/iked.conf** *****

```
##
## IKE Daemon Configuration file for:
##   Image: ZOS2
##
## Created by the IBM Configuration Assistant for z/OS Communications
## Server
## Version 2 Release 1
## Backing Store = Team11
## Install History:
## 2015-03-26 00:01:38 : user21 to 192.168.20.82
##
## End of Configuration Assistant information
## The search order used by the IKE daemon to locate the initial
## configuration file is (highest priority listed first):
##
## 1) The name of an HFS file or MVS file specified by the IKED_FILE
##    environment variable.
## 2) /etc/security/iked.conf
##
## Some parameters may be dynamically modified after the
## IKE daemon has been started.  The parameters that are
## dynamically modifiable are noted below.
##
## One way of dynamically modifying parameters is to
## update iked.conf file parameters after the IKE daemon has been
## started and then issue a modify command to cause the IKE daemon
## to re-read the file.
##
## Example: MODIFY IKED,REFRESH
## Note: IKED is the IKE daemon procedure name.
##
## After the IKE daemon has been started, a different configuration
## file can be specified by using the Modify command with the FILE
```

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

```
## parameter. This allows modifiable parameters to be
## dynamically altered while the IKE daemon is running. Note that
## the parameter values modified in this fashion are not
## persistent. To make the changes persistent, update the iked.conf
## file that is located at IKE initialization time according to the
## search order described previously.
##
## Example: MODIFY IKED,REFRESH,FILE='/etc/security/iked.conf2'
## Note: IKED is the IKE daemon procedure name.
##
## See the z/OS Communications Server: IP System Administrator's
## Commands book for more information about the modify command.
##
## See the z/OS Communications Server: IP Configuration Reference book
## for more information about the IkeConfig and NssConfig statements
## and their parameters.
IkeConfig
{
# IkeSyslogLevel      0-255              (dynamically modifiable)
# Specifies the level of logging to obtain from the IKE daemon.
# Default:            1

# PagentSyslogLevel 0-255              (dynamically modifiable)
# Specifies the level of logging to obtain from pagent through the PAPI
# Default:            0

# Keyring             userid/ringname   (not dynamically modifiable)
# The owning userid and ringname used by the IKE server when performing
# RSA Signature Mode of authentication. The userid must be the userid
# of
# the process under which IKE will run.
KeyRing IKED/IKED2RING

# IkeRetries          1-8              (dynamically modifiable)
# Specifies the number of times that an unanswered IKE negotiation
# message will be retransmitted before the negotiation is cancelled.
# Default:            6

# IkeInitWait         1-15            (dynamically modifiable)
# Specifies the number of seconds to wait before the
# first retransmission of an unanswered IKE message.
# Default:            2

# FIPS140             yes, no         (not dynamically modifiable)
# Specifies whether the IKE daemon should perform cryptographic
# operations by invoking cyptographic modules that are compliant with
# Federal Information Processing Standards (FIPS) publication 140-2's
# Level 1 security requirements.
# Default:            no

# Echo                yes,no          (dynamically modifiable)
# Echoes all IKE daemon log messages to the job output file,
# specified by the IKEDOUT DD (JCL) statement.
# Default:            no

# PagentWait          0-9999          (not dynamically modifiable)
# The time limit in seconds to wait for connection to the policy agent.
```

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

```
# A value of 0 means retry forever.
# Default:          0

# SMF119    IKEAll,IKETunnel,DynTunnel,None (dynamically modifiable)
# Specifies the level of SMF logging.
# Default:          None

# SupportedCertAuth label          (dynamically modifiable)
# Specifies the label of a Certificate Authority(CA) certificate on the
# IKE server's keyring. Use multiple instances of this keyword to
# specify
# multiple CA certificates.

NetworkSecurityServer      192.168.20.92 Port 4159 Identity UserAtFqdn
NSSD2@WSC.LABS.IBM.COM

# NssWaitLimit      1-300          (dynamically modifiable)
# Specifies the number of seconds that a Network Security client
# will wait between connection attempts when trying to establish a
# connection with a Network Security Server.
NssWaitLimit      60
}

# NssStackConfig    stackname      (dynamically modifiable)
# Used to configure a stack as a Network Security client.
NssStackConfig TCPIPT
{

# ClientName        clientname      (dynamically modifiable)
# Specifies the Network Security client name for the stack.
ClientName      IKED2

# ServiceType       Cert,RemoteMgmt (dynamically modifiable)
# Specifies the types of centralized services requested
# from the Network Security server.
ServiceType Cert

# ServiceType       Cert,RemoteMgmt (dynamically modifiable)
# Specifies the types of centralized services requested
# from the Network Security server.
ServiceType RemoteMgmt

# UserId            userid          (dynamically modifiable)
# Specifies the RACF userid that will be used to verify access
# for this stack to the services provided by the
# Network Security server.
UserId          IKED

# AuthBy            Password pw, Passticket (dynamically modifiable)
# Specifies the mechanism by which the Network Security server
# should authenticate the client TCPIP stack.
AuthBy          Passticket
}
```

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

**** **Lab L16 /etc/security/nssd.conf** ****

```
##
## NSS Daemon Configuration file for:
##   Image: ZOS2
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 1
## Backing Store = Team11
## Install History:
## 2015-04-27 16:07:46 : user21 to 192.168.20.82
## 2015-04-27 13:41:11 : user21 to 192.168.20.82
## 2015-04-25 00:36:05 : user21 to 192.168.20.82
## 2015-04-24 23:41:17 : user21 to 192.168.20.82
## 2015-04-24 18:14:51 : user21 to 192.168.20.82
##
## End of Configuration Assistant information
NssConfig
{
    Port          4159
    SyslogLevel 1
    KeyRing       NSSD/NSSD2Ring
}
```

**** **Lab L17 /etc/securiry/dmd.conf** ****

```
##
## Defense Manager Daemon Configuration file for:
##   Image: ZOS2
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 1
## Backing Store = Team11
## Install History:
## 2015-04-29 00:08:30 : user21 to 192.168.20.82
##
## End of Configuration Assistant information
DMConfig
{
    SyslogLevel 7
    DefensiveFilterDirectory /var/dm/filters
}

DmStackConfig TCPIPT
{
    Mode Active
    MaxLifetime 1440
    DefaultLogLimit 0
}
```

Instructor Certificate Jobs

***** *L07 CA Certificate for FTP Server and Client* *****

```
//FTPCACRT JOB MSGCLASS=X,NOTIFY=&SYSUID
//FTPCACRT EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT CERTAUTH GENCERT -
      SUBJECTSDN (O('MVS1') -
                  CN('WSCCA.LABS.IBM.COM') -
                  C('US')) -
      ALTNAME (IP(192.168.20.0) -
               DOMAIN('WSC.LABS.IBM.COM') -
               EMAIL('ZOS@WSC.LABS.IBM.COM')) -
      NOTBEFORE (DATE(2009/02/09)) -
      NOTAFTER (DATE(2029/02/09)) -
      KEYUSAGE (CERTSIGN) -
      SIZE(1024) -
      WITHLABEL('WSC LABS Certificate Authority')
SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** *L07 FTP Server Certificate* *****

```
//FTPSRCRT JOB MSGCLASS=X,NOTIFY=&SYSUID
//FTPSRCRT EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(TCPIP) GENCERT -
      SUBJECTSDN (O('IBM') -
                  CN('FTP.WSC.LABS.IBM.COM') -
                  C('US')) -
      ALTNAME (EMAIL('FTP@WSC.LABS.IBM.COM')) -
      NOTBEFORE (DATE(2009/02/09)) -
      NOTAFTER (DATE(2029/02/09)) -
      WITHLABEL('FTP on ANY ZOS') -
      SIZE(1024) -
      SIGNWITH(CERTAUTH -
               Label('WSC LABS Certificate Authority'))
SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

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

***** **L07 FTP Client Usernx Certificate** *****

```
//FTPCLCRT JOB MSGCLASS=X,NOTIFY=&SYSUID
//FTPCLCRT EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(USERnx) GENCERT -
      SUBJECTSDN (O('IBM') -
                  CN('USERnx.WSC.LABS.IBM.COM') -
                  C('US')) -
      ALTNAME (EMAIL('USERnx@WSC.LABS.IBM.COM')) -
      NOTBEFORE (DATE(2009/02/09)) -
      NOTAFTER (DATE(2029/02/09)) -
      WITHLABEL('USERnx on ANY ZOS') -
      SIZE(1024) -
      SIGNWITH(CERTAUTH -
               Label('WSC LABS Certificate Authority'))
      SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** **L07 FTP Server Key Ring** *****

```
//FTPSRRNG JOB MSGCLASS=X,NOTIFY=&SYSUID
//FTPSRRNG EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(FTPD) ADDRING(ServerRing1)
RACDCERT ID(FTPD) CONNECT(ID(TCPIP) LABEL('FTP on ANY ZOS') -
      RING(ServerRing1) USAGE(PERSONAL) DEFAULT) -
RACDCERT ID(FTPD) CONNECT(CERTAUTH -
      LABEL('WSC LABS Certificate Authority') -
      RING(ServerRing1) USAGE(CERTAUTH)) -
      SETROPTS GENERIC(DIGTCERT) REFRESH
      SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** **L07 FTP Client Key Ring** *****

```
//FTPCLRNG JOB MSGCLASS=X,NOTIFY=&SYSUID
//FTPCLRNG EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(FTPD) ADDRING(ClientRing1)
RACDCERT ID(FTPD) CONNECT(ID(USER1) LABEL('USER1 on ANY ZOS') -
      RING(ClientRing1) USAGE(PERSONAL) DEFAULT) -
RACDCERT ID(FTPD) CONNECT(ID(USER2) LABEL('USER2 on ANY ZOS') -
      RING(ClientRing1) USAGE(PERSONAL)) -
RACDCERT ID(FTPD) CONNECT(ID(USER3) LABEL('USER3 on ANY ZOS')) -
```

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

```

        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER4) LABEL('USER4 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER5) LABEL('USER5 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER6) LABEL('USER6 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER7) LABEL('USER7 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER11) LABEL('USER11 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER12) LABEL('USER12 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER13) LABEL('USER13 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER21) LABEL('USER21 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER22) LABEL('USER22 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER23) LABEL('USER23 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER31) LABEL('USER31 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER32) LABEL('USER32 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER33) LABEL('USER33 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER41) LABEL('USER41 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER42) LABEL('USER42 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER43) LABEL('USER43 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER51) LABEL('USER51 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER52) LABEL('USER52 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER53) LABEL('USER53 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER61) LABEL('USER61 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER62) LABEL('USER62 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER63) LABEL('USER63 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER71) LABEL('USER71 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER72) LABEL('USER72 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(ID(USER73) LABEL('USER73 on ANY ZOS')) -
        RING(ClientRing1) USAGE(PERSONAL))
RACDCERT ID(FTPD) CONNECT(CERTAUTH -
        LABEL('WSC LABS Certificate Authority') -
        RING(ClientRing1) USAGE(CERTAUTH))
        SETROPTS GENERIC(DIGTCERT) REFRESH
        SETROPTS RACLIST(DIGTCERT) REFRESH
/*

```

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

***** **L07 FTP Client USERnx Key Ring** *****

```
//FTPCURNJ JOB MSGCLASS=X,NOTIFY=&SYSUID
//FTPCURNJ EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(USERnx) ADDRING(LabClientRing)
RACDCERT ID(USERnx) CONNECT(ID(USERnx) -
    LABEL('USERnx on ANY ZOS') -
    RING(LabClientRing) USAGE(PERSONAL) DEFAULT)
RACDCERT ID(USERnx) CONNECT(CERTAUTH -
    LABEL('WSC LABS Certificate Authority') -
    RING(LabClientRing) USAGE(CERTAUTH))
    SETROPTS GENERIC(DIGTCERT) REFRESH
    SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** **L12 CA Certificate for IKED on MVSn** *****

```
//IKECACR1 JOB MSGCLASS=X,NOTIFY=&SYSUID
//IKECACR1 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT CERTAUTH GENCERT -
    SUBJECTSDN (O('MVS1') -
        CN('MVS1CA.LABS.IBM.COM') -
        C('US')) -
    ALTNAME (IP(192.168.20.0) -
        DOMAIN('WSC.LABS.IBM.COM') -
        EMAIL('ZOS@WSC.LABS.IBM.COM')) -
    NOTBEFORE(DATE(2011/01/01)) -
    NOTAFTER(DATE(2015/12/31)) -
    KEYUSAGE(CERTSIGN) -
    SIZE(1024) -
    WITHLABEL('MVS1LABS Certificate Authority')
    SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** **L12 CA Certificate for IKED on MVSn** *****

```
//IKECACRn JOB MSGCLASS=X,NOTIFY=&SYSUID
//IKECACRn EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT CERTAUTH GENCERT -
    SUBJECTSDN (O('MVSn') -
        CN('MVSnCA.LABS.IBM.COM')) -
```

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

```
                C('US'))
ALTNAME (IP(192.168.20.1)
        DOMAIN('WSC.LABS.IBM.COM')
        EMAIL('ZOS@WSC.LABS.IBM.COM'))
NOTBEFORE (DATE(2011/01/01))
NOTAFTER (DATE(2015/12/31))
KEYUSAGE (CERTSIGN)
SIZE(1024)
WITHLABEL('MVSn LABS Certificate Authority')
SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** **L12 IKED Certificate** *****

```
//IKESRCRn JOB MSGCLASS=X,NOTIFY=&SYSUID
//IKESRCRn EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(IKED) GENCERT
        SUBJECTSDN (O('IKEDn at ZOSn')
        CN('IKEDn.WSC.LABS.IBM.COM')
        C('US'))
        ALTNAME (IP(192.168.20.9n)
        DOMAIN('WSC.LABS.IBM.COM')
        EMAIL('ZOS@WSC.LABS.IBM.COM'))
        NOTBEFORE (DATE(2009/02/09))
        NOTAFTER (DATE(2029/02/09))
        WITHLABEL('IKEDn at ZOSn')
        SIZE(1024)
        SIGNWITH(CERTAUTH
        Label('WSC LABS Certificate Authority'))
SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** **L12 IKED Key Ring on MVS1** *****

```
//IKEDRNG1 JOB MSGCLASS=X,NOTIFY=&SYSUID
//IKEDRNG1 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(IKED) ADDRING(IKED1RING)
RACDCERT ID(IKED) CONNECT(ID(IKED) LABEL('IKED1 at ZOS1')
        RING(IKED1RING) USAGE(PERSONAL))
RACDCERT ID(IKED) CONNECT(CERTAUTH
        LABEL('MVS1 LABS Certificate Authority')
        RING(IKED1RING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH
        LABEL('MVS2 LABS Certificate Authority')
        RING(IKED1RING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH
        LABEL('MVS3 LABS Certificate Authority'))
```

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

```
        RING(IKED1RING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH                                -
        LABEL('MVS4 LABS Certificate Authority')                  -
        RING(IKED1RING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH                                -
        LABEL('MVS5 LABS Certificate Authority')                  -
        RING(IKED1RING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH                                -
        LABEL('MVS6 LABS Certificate Authority')                  -
        RING(IKED1RING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH                                -
        LABEL('MVS7 LABS Certificate Authority')                  -
        RING(IKED1RING) USAGE(CERTAUTH))
        SETROPTS GENERIC(DIGTCERT) REFRESH
        SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

***** *L12 IKED Key Ring on MVSn* *****

```
//IKEDRNGn JOB MSGCLASS=X,NOTIFY=&SYSUID
//IKEDRNGn EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(IKED) ADDRING(IKEDnRING)
RACDCERT ID(IKED) CONNECT(ID(IKED) LABEL('IKEDn at ZOSn')        -
        RING(IKEDnRING) USAGE(PERSONAL))
RACDCERT ID(IKED) CONNECT(CERTAUTH                                -
        LABEL('MVSn LABS Certificate Authority')                  -
        RING(IKEDnRING) USAGE(CERTAUTH))
RACDCERT ID(IKED) CONNECT(CERTAUTH                                -
        LABEL('MVS1 LABS Certificate Authority')                  -
        RING(IKEDnRING) USAGE(CERTAUTH))
        SETROPTS GENERIC(DIGTCERT) REFRESH
        SETROPTS RACLIST(DIGTCERT) REFRESH
/*
```

Certificate Displays

***** *L07 CA Certificate for FTP Server and Client* *****

```
racdcert CERTAUTH list(label('WSC LABS Certificate Authority'))
```

Digital certificate information for CERTAUTH:

```
Label: WSC LABS Certificate Authority
Certificate ID:
2QiJmZmDhZmjgebiw0DTwcLiQMOFmaOJhomDgaOFQMGko4iWmYmjQEBA
Status: TRUST
Start Date: 2009/02/09 00:00:00
End Date: 2029/02/09 23:59:59
Serial Number:
>008C<
Issuer's Name:
>CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
Subject's Name:
>CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
IP: 192.168.20.0
EMail: ZOS at WSC.LABS.IBM.COM
Domain: WSC.LABS.IBM.COM
Key Usage: CERTSIGN
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: FTPD
Ring:
>ClientRing1<
Ring Owner: FTPD
Ring:
>ServerRing1<
Ring Owner: USER11
Ring:
>LabClientRing<
Ring Owner: USER12
Ring:
>LabClientRing<
Ring Owner: USER13
Ring:
>LabClientRing<
Ring Owner: USER21
Ring:
>LabClientRing<
Ring Owner: USER22
Ring:
>LabClientRing<
Ring Owner: USER23
```

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

```
Ring:
  >LabClientRing<
Ring Owner: USER31
Ring:
  >LabClientRing<
Ring Owner: USER32
Ring:
  >LabClientRing<
Ring Owner: USER33
Ring:
  >LabClientRing<
Ring Owner: USER41
Ring:
  >LabClientRing<
Ring Owner: USER42
Ring:
  >LabClientRing<
Ring Owner: USER43
Ring:
  >LabClientRing<
Ring Owner: USER51
Ring:
  >LabClientRing<
Ring Owner: USER52
Ring:
  >LabClientRing<
Ring Owner: USER53
Ring:
  >LabClientRing<
Ring Owner: USER61
Ring:
  >LabClientRing<
Ring Owner: USER62
Ring:
  >LabClientRing<
Ring Owner: USER63
Ring:
  >LabClientRing<
Ring Owner: USER71
Ring:
  >LabClientRing<
Ring Owner: USER72
Ring:
  >LabClientRing<
Ring Owner: USER73
Ring:
  >LabClientRing<
```

***** **L07 FTP Server Certificate** *****

```
racdcert ID(TCPIP) list(label('FTP on ANY ZOS'))
```

Digital certificate information for user TCPIP:

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

Label: FTP on ANY ZOS
Certificate ID: 2QXjw9fJ18bj10CWlUDB1ehA6dbi
Status: TRUST
Start Date: 2009/02/09 00:00:00
End Date: 2020/02/09 23:59:59
Serial Number:
>36<
Issuer's Name:
>CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's Name:
>CN=FTP.WSC.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
Email: FTP at WSC.LABS.IBM.COM
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: FTPD
Ring:
>ServerRing1<

**** *L07 FTP Client Usernx Certificate* ****

racdcert ID(USERnx) list(label('USERnx on ANY ZOS'))

Digital certificate information for user USERnx:

Label: USERnx on ANY ZOS
Certificate ID: 2Qbk4sXZ8vHk4sXZ8vFAlpVAwdXoQOnW4kBA
Status: TRUST
Start Date: 2009/02/09 00:00:00
End Date: 2020/02/09 23:59:59
Serial Number:
>41<
Issuer's Name:
>CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's Name:
>CN=USERnx.WSC.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
Email: USERnx at WSC.LABS.IBM.COM
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: FTPD
Ring:
>ClientRing1<
Ring Owner: USERnx
Ring:
>LabClientRing<

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

***** L07 FTP Server Key Ring *****

```
racdcert ID(FTPD) listring(ServerRing1)
```

Digital ring information for user FTPD:

Ring:

>ServerRing1<

Certificate Label Name	Cert Owner	USAGE	DEFAULT
FTP on ANY ZOS	ID(TCPIP)	PERSONAL	YES
WSC LABS Certificate Authority	CERTAUTH	CERTAUTH	NO

***** L07 FTP Client Key Ring *****

```
racdcert ID(FTPD) listring(ClientRing1)
```

Digital ring information for user FTPD:

Ring:

>ClientRing1<

Certificate Label Name	Cert Owner	USAGE	DEFAULT
USER1 on ANY ZOS	ID(USER1)	PERSONAL	YES
USER2 on ANY ZOS	ID(USER2)	PERSONAL	NO
USER3 on ANY ZOS	ID(USER3)	PERSONAL	NO
USER4 on ANY ZOS	ID(USER4)	PERSONAL	NO
USER5 on ANY ZOS	ID(USER5)	PERSONAL	NO
USER6 on ANY ZOS	ID(USER6)	PERSONAL	NO
USER7 on ANY ZOS	ID(USER7)	PERSONAL	NO
USER11 on ANY ZOS	ID(USER11)	PERSONAL	NO
USER12 on ANY ZOS	ID(USER12)	PERSONAL	NO
USER13 on ANY ZOS	ID(USER13)	PERSONAL	NO
USER21 on ANY ZOS	ID(USER21)	PERSONAL	NO
USER22 on ANY ZOS	ID(USER22)	PERSONAL	NO
USER23 on ANY ZOS	ID(USER23)	PERSONAL	NO
USER31 on ANY ZOS	ID(USER31)	PERSONAL	NO
USER32 on ANY ZOS	ID(USER32)	PERSONAL	NO
USER33 on ANY ZOS	ID(USER33)	PERSONAL	NO
USER41 on ANY ZOS	ID(USER41)	PERSONAL	NO
USER42 on ANY ZOS	ID(USER42)	PERSONAL	NO
USER43 on ANY ZOS	ID(USER43)	PERSONAL	NO
USER51 on ANY ZOS	ID(USER51)	PERSONAL	NO
USER52 on ANY ZOS	ID(USER52)	PERSONAL	NO
USER53 on ANY ZOS	ID(USER53)	PERSONAL	NO
USER61 on ANY ZOS	ID(USER61)	PERSONAL	NO
USER62 on ANY ZOS	ID(USER62)	PERSONAL	NO
USER63 on ANY ZOS	ID(USER63)	PERSONAL	NO
USER71 on ANY ZOS	ID(USER71)	PERSONAL	NO
USER72 on ANY ZOS	ID(USER72)	PERSONAL	NO
USER73 on ANY ZOS	ID(USER73)	PERSONAL	NO
WSC LABS Certificate Authority	CERTAUTH	CERTAUTH	NO

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

***** L07 FTP Client Usernx Key Ring *****

```
racdcert ID(USERnx) listring(LabClientRing)
```

Digital ring information for user USERnx:

Ring:

Certificate Label Name	Cert Owner	USAGE	DEFAULT
USERnx on ANY ZOS	ID (USERnx)	PERSONAL	YES
WSC LABS Certificate Authority	CERTAUTH	CERTAUTH	NO

***** L08 CA Certificate for TN3270 Server *****

```
racdcert CERTAUTH list(label('GBGCASnx LABS Server CA'))
```

Digital certificate information for CERTAUTH:

```
Label: GBGCASnx LABS Server CA
Certificate ID: 2QiJmZmDhZmjgcfCx8PB4vLxQNPBwuJA4oWZpYWZQMPB
Status: TRUST      <=====Must have status TRUST
Start Date: 2013/03/13 00:00:00    <=====Must have valid date range
End Date:   2013/09/13 23:59:59    <=====Must have valid date range
Serial Number:
>00<
Issuer's Name:
>CN=GBGCASnx.LABS.IBM.COM.O=GBG.C=US<
Subject's Name:
>CN=GBGCASnx.LABS.IBM.COM.O=GBG.C=US<
Subject's AltNames:
IP: 192.168.20.10n
Email: ZOS at GBG.LABS.IBM.COM
Domain: GBG.LABS.IBM.COM
Key Usage: CERTSIGN
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: USERnx
Ring:
>USERnxRing<
Ring Owner: TN3270
Ring:
>MyServernRing<
```

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

***** **L08 CA Certificate for TN3270 Client Usernx** *****

```
racdcert CERTAUTH list(label('GBGCACnx LABS Client CA'))
```

Digital certificate information for CERTAUTH:

```
Label: GBGCACnx LABS Client CA
Certificate ID: 2QiJmZmDhZmjgcfCx8PBw/LxQNPBwuJAw5OJhZWjQMPB
Status: TRUST      <=====Must have status TRUST
Start Date: 2013/03/13 00:00:00    <=====Must have valid date range
End Date:   2013/09/13 23:59:59    <=====Must have valid date range
Serial Number:
    >00<
Issuer's Name:
    >CN=GBGCACnx.LABS.IBM.COM.O=GBG.C=US<
Subject's Name:
    >CN=GBGCACnx.LABS.IBM.COM.O=GBG.C=US<
Subject's AltNames:
    IP: 192.168.20.9n
    EMail: ZOSC at GBG.LABS.IBM.COM
    Domain: GBG.LABS.IBM.COM
Key Usage: CERTSIGN
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
    Ring Owner: USERnx
    Ring:
        >USERnxRing<
    Ring Owner: TN3270
    Ring:
        >MyServernRing<
```

***** **L08 TN3270 Server Certificate** *****

```
racdcert ID(TN3270) list(label('TN3270 on MVSn'))
```

Digital certificate information for user TN3270:

```
Label: TN3270 on MVSn
Certificate ID: 2Qbj1fPy9/Dj1fPy9/BAlpVA10Xi8kBA
Status: TRUST      <=====Must have status TRUST
Start Date: 2013/03/13 00:00:00    <=====Must have valid date range
End Date:   2013/09/13 23:59:59    <=====Must have valid date range
Serial Number:
    >01<
Issuer's Name:
    >CN=GBGCASnx.LABS.IBM.COM.O=GBG.C=US<
Subject's Name:
    >CN=TN3270.GBG.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
```

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

EMail: TN3270 at GBG.LABS.IBM.COM
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
 Ring Owner: TN3270
 Ring:
 >MyServernRing<

***** L08 TN3270 Client Usernx Certificate *****

racdcert ID(USERnx) list(label('USERnx on MVSn'))

Digital certificate information for user USERnx:

Label: USERnx on MVSn
Certificate ID: 2Qbk4sXZ8vHk4sXZ8vFAlpVA10Xi8kBA
Status: **TRUST** ←=====Must have status TRUST
Start Date: **2013/03/13 00:00:00** ←=====Must have valid date range
End Date: **2013/09/13 23:59:59** ←=====Must have valid date range
Serial Number:
 >01<
Issuer's Name:
 >CN=GBGCACnx.LABS.IBM.COM.O=GBG.C=US<
Subject's Name:
 >CN=USERnx.GBG.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
 Email: USERnx at GBG.LABS.IBM.COM
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
 Ring Owner: USERnx
 Ring:
 >USERnxRing<

***** L08 TN3270 Server Key Ring *****

racdcert ID(TN3270) listring(MyServernRing)

Digital ring information for user TN3270:

Ring:
 >MyServernRing<

Certificate Label Name	Cert Owner	USAGE	DEFAULT
TN3270 on MVSn	ID (TN3270)	PERSONAL	YES
GBGCACnx LABS Client CA	CERTAUTH	CERTAUTH	NO
GBGCASnx LABS Server CA	CERTAUTH	CERTAUTH	NO

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

***** **L08 TN3270 Client Usernx Key Ring** *****

racdcert ID(USERnx) listring(USERnxRing)

Digital ring information for user USERnx:

Ring:

Certificate Label Name	Cert Owner	USAGE	DEFAULT
USERnx on MVSn	ID (USERnx)	PERSONAL	YES
GBGCACnx LABS Client CA	CERTAUTH	CERTAUTH	NO
GBGCASnx LABS Server CA	CERTAUTH	CERTAUTH	NO

***** **L12 CA Certificate for IKED on MVS1** *****

racdcert CERTAUTH list(label('MVS1 LABS Certificate Authority'))

Digital certificate information for CERTAUTH:

Label: MVS1 LABS Certificate Authority
Certificate ID:
2QiJmZmDhZmjgdTl4vFA08HC4kDDhZmjiYaJg4GjhUDBpKOilpmJo6hA
Status: TRUST
Start Date: 2011/01/01 00:00:00
End Date: 2015/12/31 23:59:59
Serial Number:
>00<
Issuer's Name:
>CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
Subject's Name:
>CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
Key Usage: CERTSIGN
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: IKED
Ring:
>IKED1RING<
Ring Owner: IKED
Ring:
>IKED2RING<
Ring Owner: IKED
Ring:
>IKED3RING<
Ring Owner: IKED
Ring:
>IKED4RING<
Ring Owner: IKED
Ring:

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

```
>IKED5RING<
Ring Owner: IKED
Ring:
>IKED6RING<
Ring Owner: IKED
Ring:
>IKED7RING<
Ring Owner: TCPIP
Ring:
>Client_RING<
Ring Owner: FTPD
Ring:
>Server_RING<
Ring Owner: FTPD
Ring:
>Server_RING1<
```

***** **L12 CA Certificate for IKED on MVSn** *****

```
racdcert CERTAUTH list(label('MVSn LABS Certificate Authority'))
```

Digital certificate information for CERTAUTH:

```
Label: MVSn LABS Certificate Authority
Certificate ID:
2QiJmZmDhZmjgdTl4vJA08HC4kDDhZmjiYaJg4GjhUDBpKOIlpmJo6hA
Status: TRUST
Start Date: 2011/01/01 00:00:00
End Date: 2015/12/31 23:59:59
Serial Number:
>00<
Issuer's Name:
>CN=MVSnCA.LABS.IBM.COM.O=MVSn CA.C=US<
Subject's Name:
>CN=MVSnCA.LABS.IBM.COM.O=MVSn CA.C=US<
Key Usage: CERTSIGN
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: IKED
Ring:
>IKED1RING<
Ring Owner: IKED
Ring:
>IKEDnRING<
```

***** **L12 IKED Certificate** *****

```
racdcert ID(IKED) list(label('IKEDn at ZOSn'))
```

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

Digital certificate information for user IKED:

Label: IKEDn at ZOSn
Certificate ID: 2QTJ0sXEydLFxPFAgaNA6dbi8UBA
Status: TRUST
Start Date: 2011/01/01 00:00:00
End Date: 2015/12/31 23:59:59
Serial Number:
>01<
Issuer's Name:
>CN=MVSnCA.LABS.IBM.COM.O=MVSn CA.C=US<
Subject's Name:
>CN=IKEDn.WSC.LABS.IBM.COM.O=IKEDn at ZOSn.C=US<
Subject's AltNames:
IP: 192.168.20.9n
EMail: ZOS at WSC.LABS.IBM.COM
Domain: WSC.LABS.IBM.COM
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
Ring Owner: IKED
Ring:
>IKEDnRING<

***** **L12 IKED Key Ring on MVS1** *****

racdcert ID(IKED) listring(IKED1RING)

Digital ring information for user IKED:

Ring:
>IKED1RING<

Certificate Label Name	Cert Owner	USAGE	DEFAULT
IKED1 at ZOS1	ID (IKED)	PERSONAL	YES
MVS1 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS2 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS3 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS4 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS5 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS6 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS7 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO

***** **L12 IKED Key Ring on MVSn** *****

racdcert ID(IKED) listring(IKEDnRING)

Digital ring information for user IKED:

Ring:

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

>IKEDnRING<			
Certificate Label Name	Cert Owner	USAGE	DEFAULT
-----	-----	-----	-----
IKEDn at ZOSn	ID (IKED)	PERSONAL	YES
MVSn LABS Certificate Authority	CERTAUTH	CERTAUTH	NO
MVS1 LABS Certificate Authority	CERTAUTH	CERTAUTH	NO

