

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

"IPSec VPNs Using Preshared Key Authentication"

Hands-on Lab Guide

(IPSec Preshared Key Lab)



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

Revision date -

Tuesday, 24 May 2022

This edition applies to IBM z/OS Configuration Assistant running in z/OSMF on z/OS V2.4.

Attention:

Information in this document was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

Acknowledgements:

Many thanks to two members of the IBM Communications Server team in Raleigh who reviewed this document: Allen Bailey and Sara Hagggar.

Table of Contents

Part 0: Lab Description for Configuring Policy Agent for IP Filtering with IPSec VPNs 4	
Overview of this LAB: Building Dynamic Tunnels using IPSec with Preshared Key Mode	5
Part 1: IPSec Dynamic Tunnels (Preshared Key) for PINGs between Addresses	
192.168.20.109 and 192.168.20.9n/192.168.20.1ab	7
Worksheet: Collect the Information You Need to Configure a Dynamic Tunnel with Preshared Key Mode.....	7
Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1	8
Configure Connectivity Rule for Security Endpoints Using Preshared Key Mode.....	10
Sort the Connectivity Rules to the Correct Sequence	20
Send Your Configurations to Your ZOSn	22
Customize Pagent for the New VPN Rules on ZOSn.....	23
Part 2: Test your IPSec Dynamic Tunnel Policies	24
Testing PING Connections that use a Dynamic Tunnel Authenticated with Preshared Key Mode.....	24
End of IPSec VPN Preshared Mode LAB	33

Part 0: Lab Description for Configuring Policy Agent for IP Filtering with IPsec VPNs

Each student ZOSn (MVS) system has two TCP/IP stacks running in it. The basic TCPIP stack belonging to the instructors is named TCPIP1. The TN3270 procedure that has affinity to the instructor TCPIP1 is named TN3270. The FTP procedure that has affinity to TCPIP1 is named FTPCCL(1).

In our labs you use TCPIP1 for basic maintenance on ZOSn until you have finished building your own student TCP/IP stacks and procedures. You will telnet into TCPIP1 to reach ISPF and UNIX for building the procedures that should run together with the student TCP/IP stack.

The student TCP/IP stack is named TCPIPT. The students customize this stack and not the instructor “maintenance” stack. The students also customize any other procedures that are part of the security labs and that are to have affinity with TCPIPT.

You will configure policies for IPsec Filtering and for IPsec VPNs on your MVS node (ZOS2, ZOS3, ZOS4, ZOS5, ZOS6, ZOS7, ZOS8, ZOS9).

Overview of this LAB: Building Dynamic Tunnels using IPSec with Preshared Key Mode

You will use the z/OS IBM Configuration Assistant to configure IPSec policies. Preshared Key Mode uses x.509 certificates and a preshared key for establishing dynamic tunnel protocols with IKED. The IP identities are taken from the entries in the x.509 certificate.

The IKE Daemon owns a Certificate that resides on a RACF Key Ring named “IKEDnRING.” The RACF Key Ring also contains a copy of both of the Certificate Authority Certificates, one for each side of the connection. **All the required certificates for this lab, including all the student certificates, have already been created for you.**

Remember that you must also implement IKED for the Dynamic Tunnel protocols and that you must implement TRMD if you plan to enable logging and capture the log messages.

The Data and Security Endpoints (DE and SE) at ZOS1 are 192.168.20.109 (DVIPA). **The DE at ZOSn is 192.168.20.1ab (DVIPA). The SE at ZOSn is 192.168.20.9n (OSA).** Note how the Preshared key identity at each end of the VPNs is also different: ZOS1 uses “**USER@FQDN**” as its IP Identity and ZOSn uses “**FQDN**” as its IP identity. A traffic type of “PING” is being protected over this VPN that is established with Preshared Key Mode.

Note: Using a DE and an SE on a single node that are identified with different IP addresses as we do in this lab is not necessarily a good design, because it represents some challenges in exploiting the Configuration Assistant. Most customers would probably design with the VIPA as both the DE and the SE.

Since both the DE and the SE are on the same node at each end of the IPSec VPN, this is truly to be applied to “Local” traffic. The z/OS Configuration Assistant tool assumes the traffic is “Routed” because the SE and DE are different.

You would not normally be protecting PING traffic over a VPN; we are using ping just to illustrate how to establish a dynamic tunnel using preshared key, and we are illustrating how to create a policy with “Gateway” in the topology. In reality, you might be trying to protect a significant production application like Enterprise Extender, CICS, DB2, MQ, or WebSphere Application Server using an IPSec VPN. Please understand that we are using PING for this lab only for the sake of simplicity – not because you would ever need to encrypt pings.

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

The lab is divided into two sections:

- ***Part 1: Enable IPSec Dynamic Tunnels with Preshared Key Mode: Configure IPSec VPN policies for PINGs between Addresses 192.168.20.109 and 192.168.20.9n/192.168.20.1ab***
- ***Part 2: Test the IPSec VPN Policies***

Part 1: IPSec Dynamic Tunnels (Preshared Key) for PINGs between Addresses 192.168.20.109 and 192.168.20.9n/192.168.20.1ab

IMPORTANT: Screen captures are APPROXIMATE EXAMPLES of what you may see. Always follow the lab instructions for what to enter on the tool screens and ignore the entries in the EXAMPLE unless you are told to use those entries.

Worksheet: Collect the Information You Need to Configure a Dynamic Tunnel with Preshared Key Mode

1. What are the Data Endpoints?
 - a. Local Data Endpoint (LDE at your ZOSn): 192.168.20.
 - b. Remote Data Endpoint (RDE at ZOS1): 192.168.20.
2. What are the Security Endpoints?
 - a. Local Security Endpoint (LSE at your ZOSn): 192.168.20.
 - b. Remote Security Endpoint (RSE at ZOS1): 192.168.20.
3. What kind of IPSec Topology does **at ZOS1** need to configure for this connection?
 - a. **Host to Host?** (Yes or No) _____
 - b. **Host to Gateway?** (Yes or No) _____
 - c. **Gateway to Host?** (Yes or No) _____
 - d. **Gateway to Gateway?** (Yes or No) _____
4. What kind of IPSec Topology do you **at ZOSn** need to configure for this connection?
 - a. **Host to Host?** (Yes or No) _____
 - b. **Host to Gateway?** (Yes or No) _____
 - c. **Gateway to Host?** (Yes or No) _____
 - d. **Gateway to Gateway?** (Yes or No) _____
5. What is the ZOS1 IKE Identity?
 - a. **Certificate ALTNAME of IPADDR?** (Yes or No) _____
 - b. **Certificate ALTNAME of FQDN?** (Yes or No) _____
 - c. **Certificate ALTNAME of USER@FQDN?** (Yes or No) _____
 - d. **Certificate SUBJECT NAME of x.500 DN?** (Yes or No) _____
6. What is the ZOSn IKE Identity?
 - a. **Certificate ALTNAME of IPADDR?** (Yes or No) _____
 - b. **Certificate ALTNAME of FQDN?** (Yes or No) _____
 - c. **Certificate ALTNAME of USER@FQDN?** (Yes or No) _____
 - d. **Certificate SUBJECT NAME of x.500 DN?** (Yes or No) _____
7. What is the preshared key that will be used during Phase 1 negotiation?
 - a. **userlabs** (lower case)
8. Security Association (SA_{IKE}): What are the *Key Exchange Proposals* that the peer (MVS1) wishes you to use? (We have provided the responses here.)
 - a. **IETF's VPN~A, which means:**

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

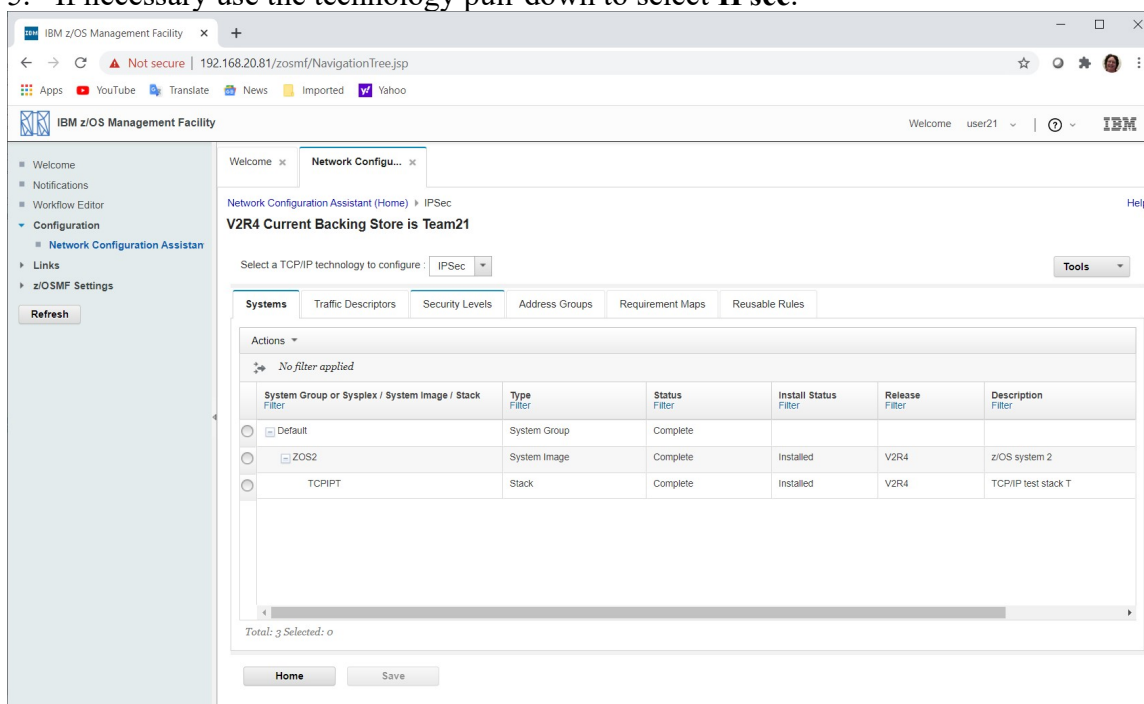
- i. **3DES**
 - ii. **SHA-1**
 - iii. **Diffie_Hellman Group 2 (DHGroup2)**
 - iv. **Lifetime of 1440 minutes (both min and max)**
9. Security Association (SA_{IPSec}): What are the *Data Offer Proposals* that the peer (MVS1) wishes you to use? (We have provided the responses here.)
 - a. **IETF's VPN~A, which means:**
 - i. **3DES**
 - ii. **SHA-1**
 - iii. **Diffie_Hellman Group 2 (DHGroup2)**
 - iv. **Lifetime of 1440 minutes (both min and max)**

Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1

1. Open a Web Browser window and go to URL:
<https://192.168.20.81:443/zosmf>
2. Logon using your Team Information Sheet to determine your z/OS User ID and password (the same ones as your TSO logon to your z/OS system).
3. Expand the “**Configuration**” section in the list on the left side of the page if it is not already expanded (“>” means it is not expanded and “V” means that it is already expanded), and click on “**Configuration Assistant**” which is the only option in the expanded section.
4. Use the pull-down if necessary to select your team's backing store file and click on the **Open** button.

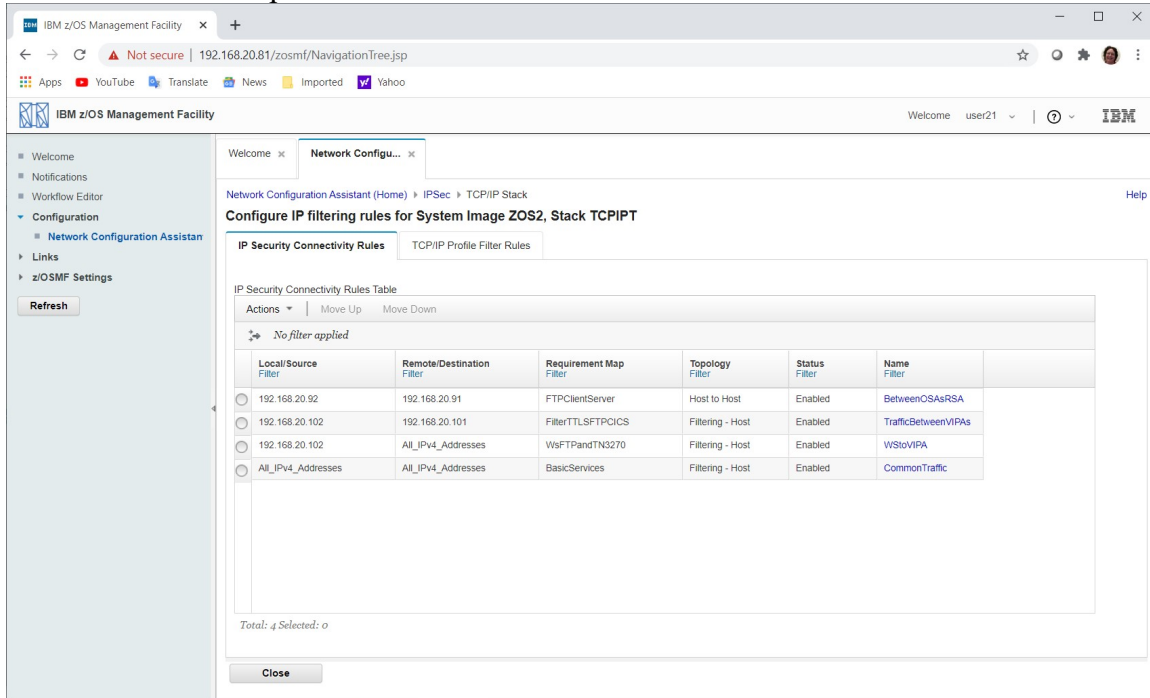
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

5. If necessary use the technology pull-down to select **IPsec**.



Configure Connectivity Rule for Security Endpoints Using Preshared Key Mode

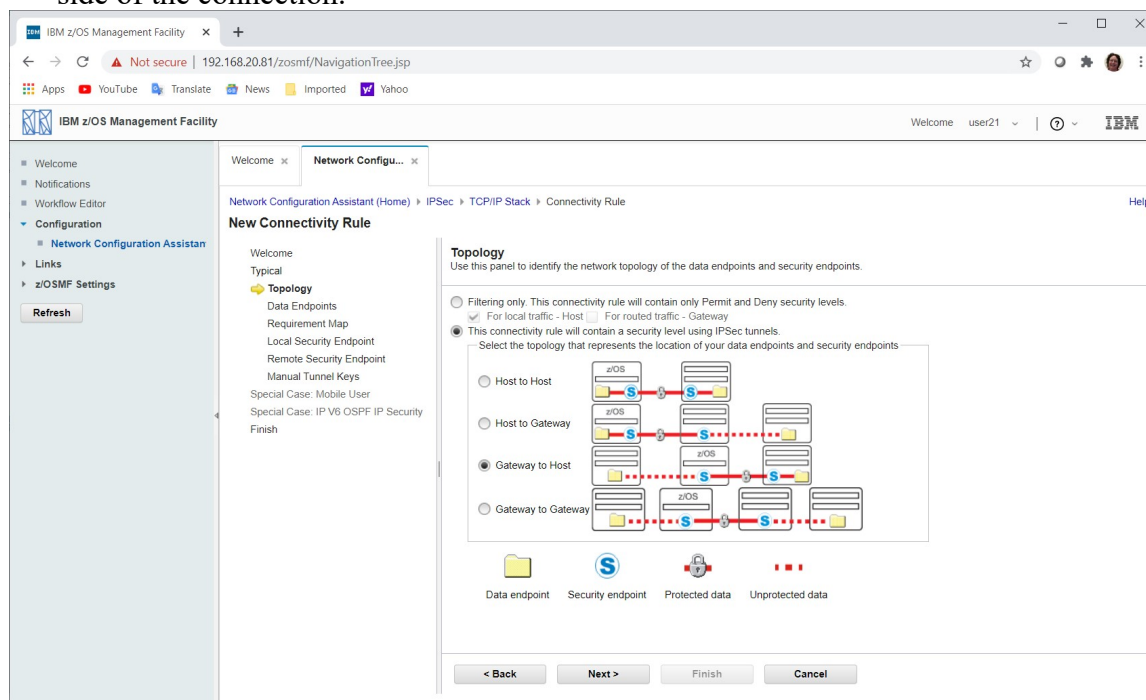
1. Use the radio button to select your TCP/IP stack **TCPIPT**.
2. Use the **Actions** pull-down to select **Rules...**



3. Use the Actions pull-down to select **New...**
4. Accept the default **Typical** connectivity type.
5. Click on the **Next** button.

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

6. Select **Gateway to Host** topology because the DE and SE are different on the student side of the connection.



7. Click on the **Next** button.

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

8. Name the Connectivity Rule: **TrafOSA2DVIPAPresh**.

IBM z/OS Management Facility

Welcome user21

Network Configuration Assistant (Home) > IPsec > TCP/IP Stack > Connectivity Rule

New Connectivity Rule

Welcome
Typical
✓ Topology
Data Endpoints
Requirement Map
Local Security Endpoint
Remote Security Endpoint
Manual Tunnel Keys
Special Case: Mobile User
Special Case: IP V6 OSPF IP Security
Finish

Data Endpoints

Use this panel to identify the data endpoints.
These are the IP addresses of the host endpoints of the traffic you want to protect.

Gateway to Host - Data Endpoints

* Connectivity rule name:
TrafOSA2DVIPAPresh

Source data endpoint:
☐ Address group:
All_IPv4_Addresses
☒ * IPv4 or IPv6 address, subnet, or range:
192.168.20.122
Examples: x.x.x.x.x.x.x.y.y.y, x.x.x.x.y.y.y.y
x.x, x.x.y.y.y, x.x.y.y

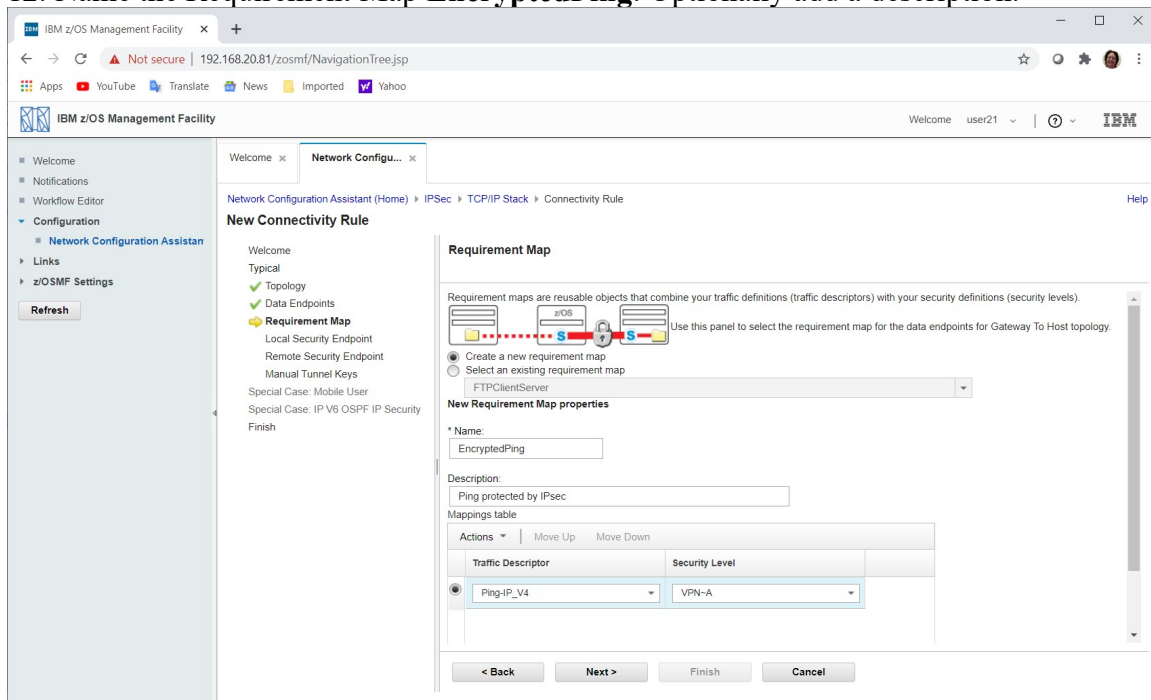
Destination data endpoint:
☐ Address group:
All_IPv4_Addresses
☒ * IPv4 or IPv6 address, subnet, or range:
192.168.20.121
Examples: x.x.x.x.x.x.x.y.y.y, x.x.x.x.y.y.y.y
x.x, x.x.y.y.y, x.x.y.y

< Back Next > Finish Cancel

9. In the **Source data endpoint** area leave the default **IPv4 or IPv6 address**, and fill in **192.168.20.1ab** (the DVIPA on ZOSn).
10. In the **Destination data endpoint** area leave the default **IPv4 or IPv6 address**, and fill in **192.168.20.109** (the DVIPA on ZOS1).
11. Click on **Next**.

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

12. Name the Requirement Map **EncryptedPing**. Optionally add a description.



13. Use the **Actions** pull-down to select **Add Row** if necessary.

14. Use the traffic descriptor pull-down in the top row to select **Ping-IP_V4**.

15. Use the security level pull-down in the top row to select **VPN~A**.

16. Select all other rows in turn and use the **Actions** pull-down to select **Remove Row**.

17. Click on **Next**.

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

18. Use the pull-down to select **Local identity type** of **Fully qualified domain name (FQDN)**.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The left sidebar contains a navigation tree with options like Welcome, Notifications, Workflow Editor, Configuration, Network Configuration Assistant, Links, and z/OSMF Settings. The main panel displays the 'New Connectivity Rule' wizard, specifically the 'Local Security Endpoint' step. The wizard includes a diagram of the network topology and a form for entering information about the IPsec local security endpoint. The 'Local identity type' is set to 'Fully qualified domain name (FQDN)', and the 'Local identity' is 'WSC.LABS.IBM.COM'. The 'Local security endpoint address' is '192.168.20.92'. The bottom of the panel has buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

19. Enter the **Local identity** of **WSC.LABS.IBM.COM**.

20. Enter the **Local security endpoint address** for the OSA of **192.168.20.9n**.

21. Click on **Next**.

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

22. Use the **Remote identity type** pull-down to select **User ID @ FQDN**.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The left sidebar contains a navigation tree with options like Welcome, Notifications, Workflow Editor, Configuration, Network Configuration Assistant, Links, and z/OSMF Settings. The main panel displays the 'New Connectivity Rule' wizard. The 'Remote Security Endpoint' step is active, showing a diagram of a z/OS system connected to a host. The 'Remote identity type' is set to 'User ID @ FQDN', and the 'Remote identity' is 'ZOS1@WSC.LABS.IBM.COM'. The authentication method is 'Shared key' with 'EBCDIC' encoding and the key 'userlabs'. The 'Additional IKEv2 options...' section is also visible.

23. Fill in the **Remote identity** of **ZOS1@WSC.LABS.IBM.COM**.

24. Select authentication of **Shared key** and **EBCDIC** and fill in the Key value of **userlabs** (lower case).

25. Click on **Next**.

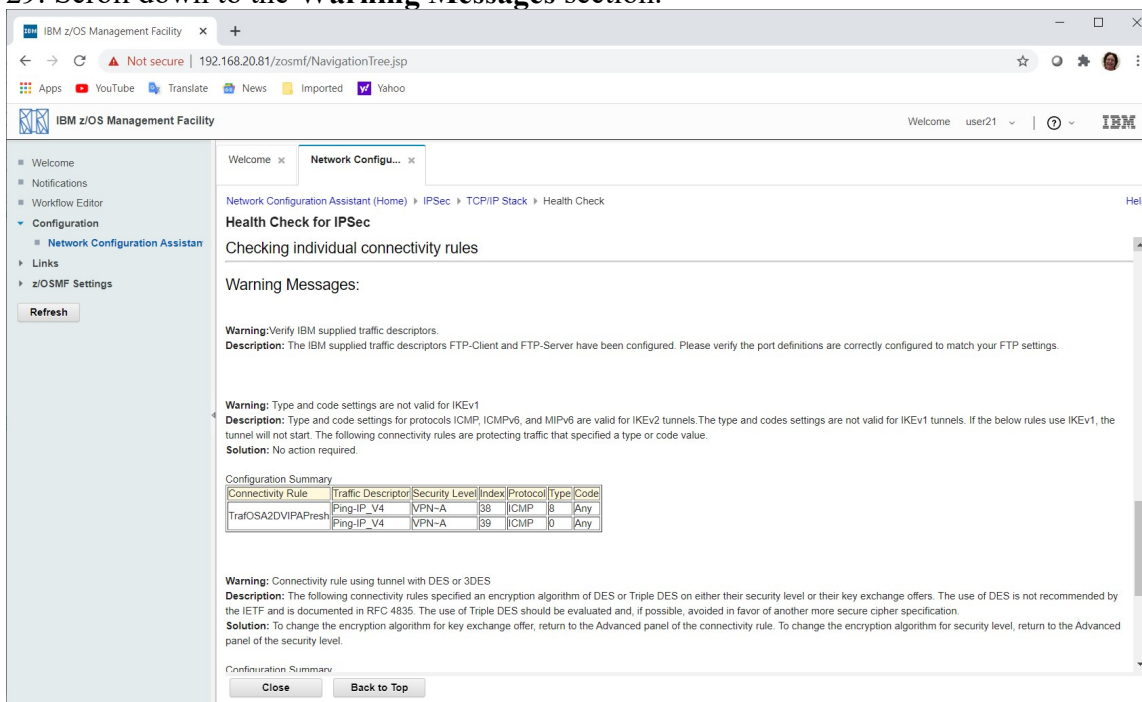
26. Select “**Yes, log all filter matches.**”

27. Click on **Finish**.

28. Use **Actions** pull-down to select **Health Check**.

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

29. Scroll down to the **Warning Messages** section.



The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (Network Configu...) interface. The left sidebar contains navigation links: Welcome, Notifications, Workflow Editor, Configuration (selected), Network Configuration Assistant (selected), Links, and z/OSMF Settings. The main content area displays the 'Health Check for IPsec' results, specifically the 'Warning Messages' section. It includes a 'Warning' about traffic descriptors, a 'Description' about port definitions, and another 'Warning' about IKEv1 settings. A 'Configuration Summary' table is also present.

Connectivity Rule	Traffic Descriptor	Security Level	Index	Protocol	Type	Code
Ping-IP_V4	VPN-A	38	ICMP	8	Any	
TrafOSA2DVIPAPres	Ping-IP_V4	VPN-A	39	ICMP	0	Any

30. Note the Warning: Type and code settings are not valid for IKEv1.

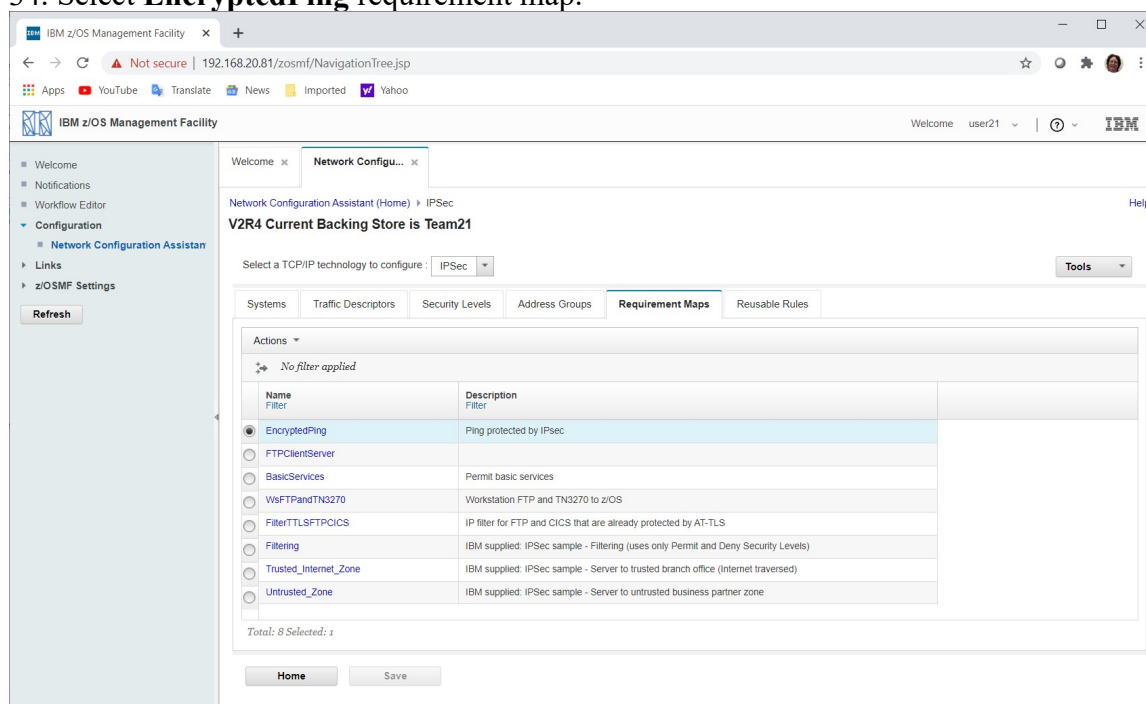
31. **Close** the Health Check panel.

32. **Close** the Rules panel.

33. Select the **Requirement Maps** tab.

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

34. Select **EncryptedPing** requirement map.




35. Use **Actions** pull-down to select **Modify...**

36. Use the traffic descriptor pull-down to change **Ping-IP_V4** to **All_other_traffic**.
 - a. Since this is the only rule with these endpoints we don't mind if it applies to all traffic, including ping.



Modify Requirement Map



The requirement map you are changing may be referenced in at least one connectivity rule.

Prior to making this change you may want to see which connectivity rules are referencing this requirement map. Click OK to show where used. Click Proceed to proceed with the Modify; otherwise, click Cancel.

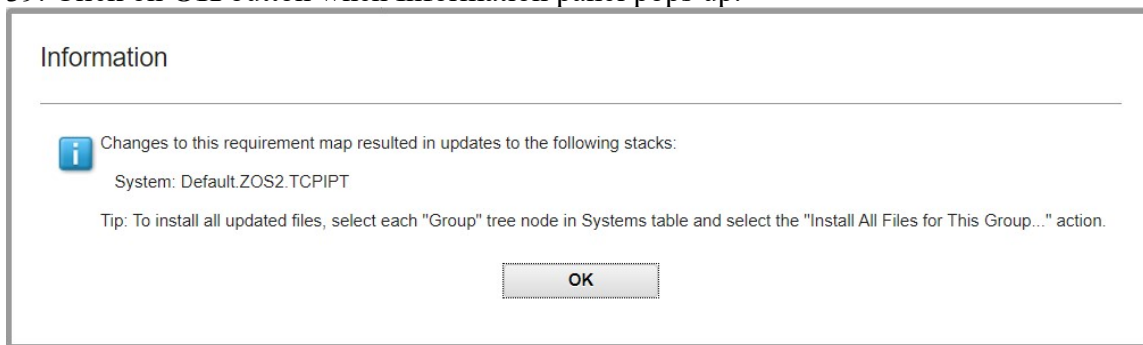
OK

Cancel

Proceed

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

39. Click on **OK** button when Information panel pops up.



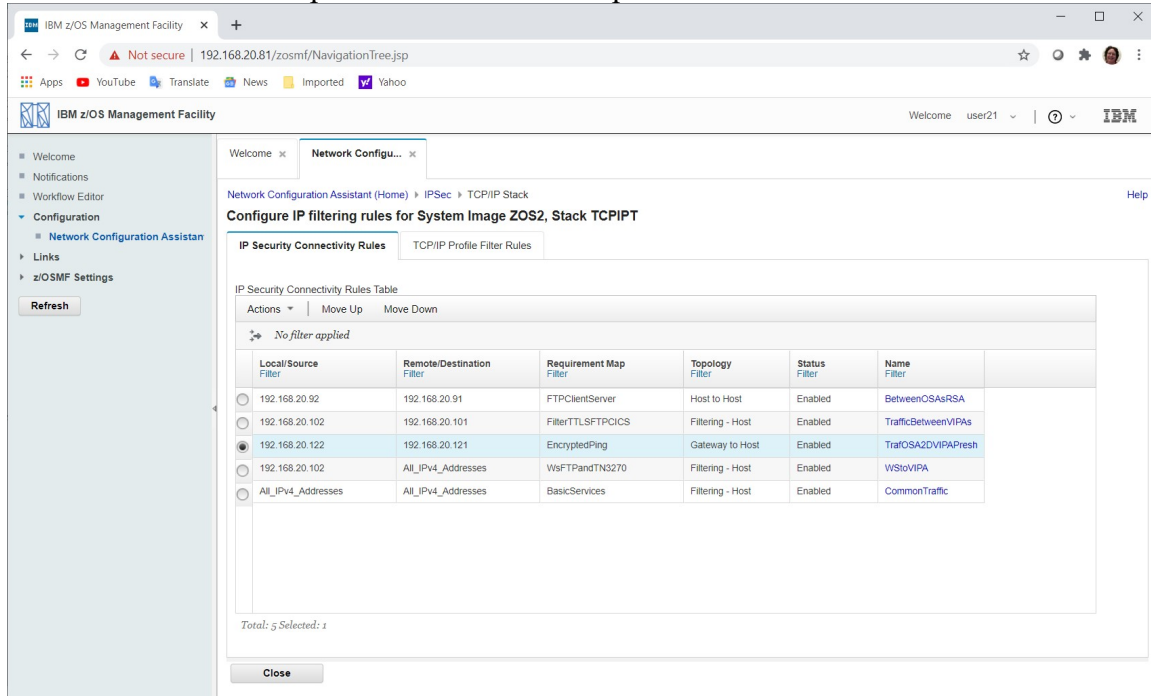
40. Click on **Save, OK**.

41. Click on **Systems** tab.

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

Sort the Connectivity Rules to the Correct Sequence

1. Return to the Rules panel. Use the **Actions** pull-down to select **Rules...**

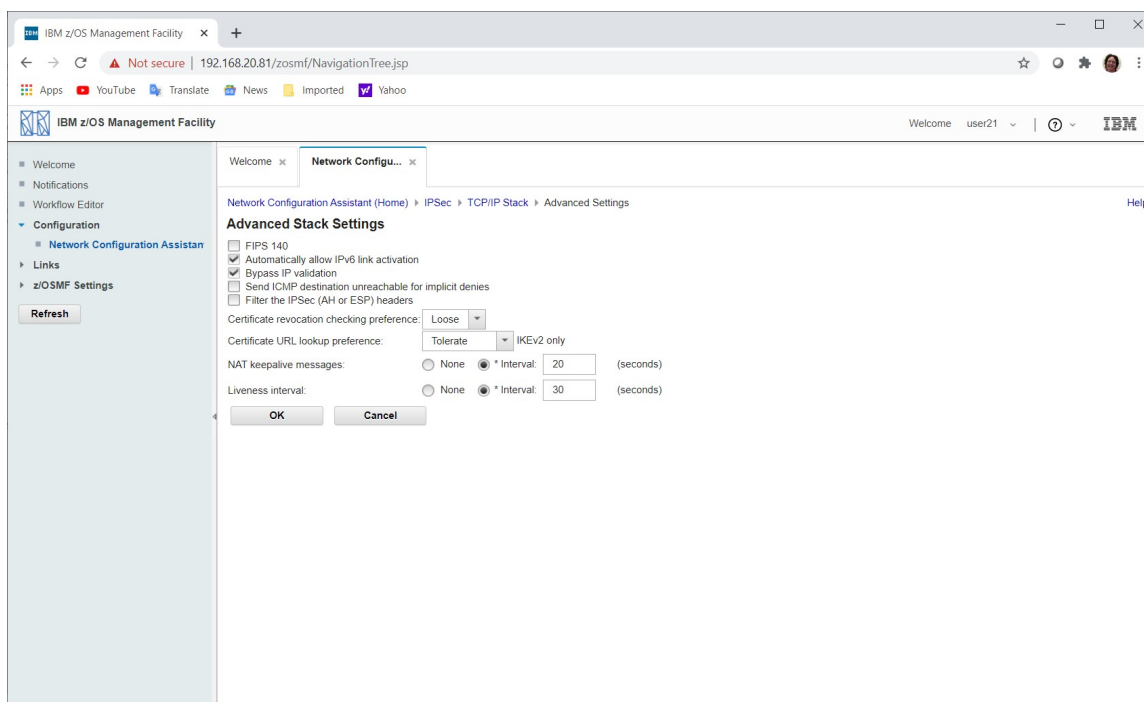


The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (Home) > IPsec > TCP/IP Stack. The main panel is titled "Configure IP filtering rules for System Image ZOS2, Stack TCPIPT". It displays the "IP Security Connectivity Rules" tab. Below the tab, there is a table titled "IP Security Connectivity Rules Table". The table has columns: Local/Source Filter, Remote/Destination Filter, Requirement Map Filter, Topology Filter, Status Filter, and Name Filter. The table contains five rows of rules. The third row, "192.168.20.122" to "192.168.20.121" with requirement "EncryptedPing", is selected. Below the table, it says "Total: 5 Selected: 1". There are "Move Up" and "Move Down" buttons above the table, and a "Close" button at the bottom.

Local/Source Filter	Remote/Destination Filter	Requirement Map Filter	Topology Filter	Status Filter	Name Filter
192.168.20.92	192.168.20.91	FTPClietServer	Host to Host	Enabled	BetweenOSAsRSA
192.168.20.102	192.168.20.101	FilterTTLSTPCICS	Filtering - Host	Enabled	TrafficBetweenVIPAs
192.168.20.122	192.168.20.121	EncryptedPing	Gateway to Host	Enabled	TrafOSA2DVIPAPresh
192.168.20.102	All_IPv4_Addresses	WsFTPandTN3270	Filtering - Host	Enabled	WSIoVIPA
All_IPv4_Addresses	All_IPv4_Addresses	BasicServices	Filtering - Host	Enabled	CommonTraffic

2. Select the rule you just create, **TrafOSA2DVIPAPreshare**.
3. Use the **Move Up** to move the rule above the two more general rules, **WorkstationtoVIPA** and **CommonTraffic**.
4. **Close, Save, OK**.
5. Use the **Actions** pull-down to select **Properties...**
6. Select the **Stack Settings** tab.
7. Select the **Advanced...** link.

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



8. Review the default values on this screen.
 - a. We identified our remote partner as ZOS1@WSC.LABS.IBM.COM. Therefore we need not validate the IP address of the remote peer against the IP Identity of the peer.
 - i. Use the Help panel to read about this option. After reviewing the Help panel information, exit from the panel.
9. Select **Bypass IP validation**.
10. Select **OK, OK, Save, OK**.

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

Send Your Configurations to Your ZOSn

1. Use **Actions** pull-down to select **Install Configuration Files...** and **Install**.
2. Your new policy file should be displayed. It contains the policies you created previously for RSA Mode encryption as well as your new policies for Preshared Key Mode encryption.
3. Use the **Actions** pull-down to select **Install...**

IBM z/OS Management Facility

Welcome user21

Network Configuration Assistant (Home) > IPsec > Configuration Files > Install

Install File for Default.ZOS2.TCPIPT

* Install file name:
/u/user21/TM21_IPSecVPN_wPreshare.policy

Installation method
☐ Save to disk
☒ FTP

FTP information
* Host name: 192.168.20.82
* Port number: 21
User ID: USER21 ☒ Save User ID
* Password: ***** ☒ Save Password
☐ Use TLS/SSL
Guideline: If Application Transparent TLS (AT-TLS) is being used to protect FTP connections between this z/OSMF server and the target z/OS system, clear this check box.
☐ Create the directories if they do not exist
Data transfer mode
☒ Default ☐ Passive ☐ Active
☐ Propagate this FTP configuration to all files on this image
Comment for the configuration file prologue (optional)

Selecting the GO button may do an automatic save of backing store before the install, based on your preference setting.

Go Close View FTP Log

4. Change the Install file name to **/u/usernx/TMnx_IPSecVPN_wPreshare.policy**.
5. Click on **Go, OK, OK, Close, Close**.

Customize Pagent for the New VPN Rules on ZOSn

1. Using a PCOMM session, logon to Telnet at the **ZOSn** TCPIP1 stack using your userid **USERnx**.
 - a. Connect to **192.168.20.8n**
 - b. **TSO USERnx** and enter password
2. Go into the ISPF Primary Menu.
 - a. Enter **ISPF**
3. Go to the OpenEdition/MVS selection screen.
 - a. Enter **O**
4. Invoke the OpenMVS POSIX Shell (OMVS).
 - a. Enter **4**
5. Edit the Policy file you just created and sent from the Configuration tool.
 - a. **su**
 - b. **oedit TMnx_IPSecVPN_wPreshare.policy**
 - c. *The Configuration Assistant tool makes the assumption that all Gateway configurations are for routed packets and not local packets.*
 - d. Currently the file looks like this:

```
IpService           All_other_traffic
{
  Protocol           All
  Direction           BiDirectional
  Routing            Routed
}
```
 - e. Edit this entry to look like this:

```
IpService           All_other_traffic
{
  Protocol           All
  Direction           BiDirectional
  Routing            Local
}
```
 - c. Save your changes to the file using **PF3** to exit from the file.
 - d. *If you neglect to make this change, your ICMP requests will time out.*
6. Edit the Pagent Configuration file you created in a previous lab.
 - a. **oedit pagentt.conf**.
7. **Comment out the previous IPSecConfig Statement.**
8. Add an IPSecConfig statement in the appropriate place in the file:
 - a. **IPSecConfig /u/usernx/TMnx_IPSecVPN_wPreshare.policy**
 - i. Filter and VPN Policies do not use “FLUSH” and “PURGE”.
9. Save your changes to the file using **PF3** to exit from the file.
10. Copy your config file to the production location.
 - a. **cp pagentt.conf /etc/PAGT1/**
11. **exit, exit, Enter, =D.LOG, /F PAGENTT,UPDATE.**

Part 2: Test your IPSec Dynamic Tunnel Policies

Testing PING Connections that use a Dynamic Tunnel Authenticated with Preshared Key Mode

1. Run a **Traffic Test command** to see whether traffic should be allowed to flow over an IKE tunnel built with Pre-Shared Key Mode:
 - a. **TSO OMVS**
 - b. **su**
 - c. **ipsec -p TCPIPT -t 192.168.20.1ab 192.168.20.109 udp 500 500 out**
 - d. *Observe how the values tell you that you have a Policy Rule for this tunnel and that you also have a DenyAll Rule that was automatically generated.*

Sample:

```
# ipsec -p TCPIPT -t 192.168.20.122 192.168.20.121 udp 500 500 out
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 1 13:08:34 2015
Primary: IP Traffic Test Function: Display Format: Detail
Source: Stack Policy Scope: n/a TotAvail: 2
TestData: 192.168.20.122 192.168.20.121 udp 500 500 out
Defensive Mode: Inactive
```

```
FilterName: TrafOSA2DVIPAPreshe~8
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: TrafOSA2DVIPAPreshe~7
VpnActionName: VPN~A~6
TunnelID: Y0
Type: Dynamic Anchor
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Outbound
OnDemand: Yes
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: All
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: Rule
SourceAddress: 192.168.20.122
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: n/a
SourcePortRange: n/a
SourcePortGranularity: n/a
```

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

```

DestAddress:                192.168.20.121
DestAddressPrefix:          n/a
DestAddressRange:           n/a
DestAddressGranularity:     Packet
DestPort:                   n/a
DestPortRange:              n/a
DestPortGranularity:        n/a
OrigRmtConnPort:            n/a
RmtIDPayload:               n/a
RmtUdpEncapPort:            n/a
CreateTime:                 2015/04/01 11:47:25
UpdateTime:                 2015/04/01 12:17:16
DiscardAction:              Silent
MIPv6Type:                  n/a
MIPv6TypeGranularity:       n/a
TypeRange:                  n/a
CodeRange:                  n/a
RemoteIdentityType:         n/a
RemoteIdentity:             n/a
FragmentsOnly:              No
FilterMatches:              0
LifetimeExpires:            n/a
AssociatedStackCount:       n/a
*****
FilterName:                  DenyAllRule_Generated_____Outbnd
FilterNameExtension:         n/a
GroupName:                   n/a
LocalStartActionName:        n/a
VpnActionName:               n/a
TunnelID:                    0x00
Type:                        Generic
DefensiveType:               n/a
State:                       Active
Action:                      Deny
Scope:                       Both
Direction:                   Outbound
OnDemand:                    n/a
SecurityClass:               0
Logging:                     None
LogLimit:                    n/a
Protocol:                    All
ICMPType:                    n/a
ICMPTypeGranularity:         n/a
ICMPCode:                    n/a
ICMPCodeGranularity:         n/a
OSPFType:                    n/a
TCPQualifier:                n/a
ProtocolGranularity:         n/a
SourceAddress:               0.0.0.0
SourceAddressPrefix:         0
SourceAddressRange:          n/a
SourceAddressGranularity:    n/a
SourcePort:                  n/a
SourcePortRange:             n/a
SourcePortGranularity:       n/a
DestAddress:                 0.0.0.0
DestAddressPrefix:           0

```

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

```
DestAddressRange:          n/a
DestAddressGranularity:    n/a
DestPort:                  n/a
DestPortRange:             n/a
DestPortGranularity:       n/a
OrigRmtConnPort:           n/a
RmtIDPayload:              n/a
RmtUdpEncapPort:           n/a
CreateTime:                2015/03/24 15:21:18
UpdateTime:                2015/03/31 17:57:16
DiscardAction:             Silent
MIPv6Type:                 n/a
MIPv6TypeGranularity:      n/a
TypeRange:                 n/a
CodeRange:                 n/a
RemoteIdentityType:        n/a
RemoteIdentity:            n/a
FragmentsOnly:            No
FilterMatches:             0
LifetimeExpires:           n/a
AssociatedStackCount:      n/a
*****
```

2 entries selected

#

2. Run a similar command to verify whether IKE traffic is allowed in the inbound direction:

a. **ipsec -p TCPIPT -t 192.168.20.109 192.168.20.1ab udp 500 500 in 0**

Sample:

```
# ipsec -p TCPIPT -t 192.168.20.121 192.168.20.122 udp 500 500 in 0
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 1 13:14:13 2015
Primary: IP Traffic Test Function: Display Format: Detail
Source: Stack Policy Scope: n/a TotAvail: 2
TestData: 192.168.20.121 192.168.20.122 udp 500 500 in 0
Defensive Mode: Inactive
```

```
FilterName:                TrafOSA2DVIPAPreshe~8
FilterNameExtension:       2
GroupName:                 n/a
LocalStartActionName:      TrafOSA2DVIPAPreshe~7
VpnActionName:             VPN~A~6
TunnelID:                  Y0
Type:                      Dynamic Anchor
DefensiveType:             n/a
State:                     Active
Action:                    Permit
Scope:                     Local
Direction:                 Inbound
OnDemand:                  Yes
SecurityClass:             0
Logging:                   All
LogLimit:                  n/a
Protocol:                  All
ICMPType:                  n/a
ICMPTypeGranularity:       n/a
```

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

```
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFTType: n/a
TCPQualifier: n/a
ProtocolGranularity: Rule
SourceAddress: 192.168.20.121
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: Packet
SourcePort: n/a
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 192.168.20.122
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: Packet
DestPort: n/a
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/04/01 11:47:25
UpdateTime: 2015/04/01 12:17:16
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
FilterName: DenyAllRule_Generated_____Inbnd
FilterNameExtension: n/a
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Deny
Scope: Both
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: None
LogLimit: n/a
Protocol: All
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
```

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

```
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 0.0.0.0
SourceAddressPrefix: 0
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: n/a
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 0.0.0.0
DestAddressPrefix: 0
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: n/a
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
RmtUdpEncapPort: n/a
CreateTime: 2015/03/24 15:21:18
UpdateTime: 2015/03/31 17:57:16
DiscardAction: Silent
MIPv6Type: n/a
MIPv6TypeGranularity: n/a
TypeRange: n/a
CodeRange: n/a
RemoteIdentityType: n/a
RemoteIdentity: n/a
FragmentsOnly: No
FilterMatches: 0
LifetimeExpires: n/a
AssociatedStackCount: n/a
*****
```

```
2 entries selected
#
```

3. Things should be looking good, and so you should test “Ping” from your ZOSn system to ZOS1 (MVS1).
 - a. From OMVS:
 - i. **ping -p TCPIPT -s 192.168.20.1ab 192.168.20.109**
 - b. or from TSO:
 - i. **ping 192.168.20.109 (TCP TCPIPT SRCIP 192.168.20.1ab**
 - c. The first ping may fail because the tunnel is being established “on-demand.” The subsequent pings should succeed.
4. Display the IKE tunnel that was built:
 - a. **ipsec -p TCPIPT -k display**
 - b. *Observe how the values in your IKE tunnel display correspond to the values you specified in the definitions.*

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

Sample:

```
# ipsec -p TCPIPT -k display
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 1 13:19:17 2015
Primary: IKE tunnel Function: Display Format: Detail
Source: IKED Scope: Current TotAvail: n/a
```

```
TunnelID: K1
Generation: 1
IKEVersion: 1.0
KeyExchangeRuleName: TrafOSA2DVIPAPreshe~4
KeyExchangeActionName: TrafOSA2DVIPAPreshe
LocalEndPoint: 192.168.20.92 <<<<<<<<<<<<
LocalIDType: ID_FQDN
LocalID: WSC.LABS.IBM.COM <<<<<<<<<<<<
RemoteEndPoint: 192.168.20.121 <<<<<<<<<<<<
RemoteIDType: ID_USER_FQDN
RemoteID: ZOS1@WSC.LABS.IBM.COM <<<<<<<<<<<<
ExchangeMode: Main
State: DONE
AuthenticationAlgorithm: HMAC-SHA1
EncryptionAlgorithm: 3DES-CBC <<<<<<<<<<<<
KeyLength: n/a
PseudoRandomFunction: HMAC-SHA1
DiffieHellmanGroup: 2
LocalAuthenticationMethod: PresharedKey <<<<<<<<<<<<
RemoteAuthenticationMethod: PresharedKey <<<<<<<<<<<<
InitiatorCookie: 0xC0DBE965B6AB4690
ResponderCookie: 0x092F690B07C69D9D
Lifesize: OK
CurrentByteCount: 616b
Lifetime: 480m
LifetimeRefresh: 2015/04/01 19:07:31
LifetimeExpires: 2015/04/01 19:18:06
ReauthInterval: 480m
ReauthTime: 2015/04/01 19:07:31
Role: Initiator
AssociatedDynamicTunnels: 1 <<<<<<<<<<<<
NATTSupportLevel: None
NATInFrntLclScEndPnt: No
NATInFrntRmtScEndPnt: No
zOSCanInitiatePlSA: Yes
AllowNat: No
RmtNAPTDetected: No
RmtUdpEncapPort: n/a
*****
```

```
1 entries selected
```

```
#
```

NOTE: You may also see the RSA tunnel that was created; it all depends on the sequence in which you tested the tunnels and the lifetime of the tunnels.

5. Display the **Dynamic Tunnel** over which the data flows:
 - a. **ipsec -p TCPIPT -y display**
 - b. *Observe how the values in your Dynamic tunnel display correspond to the values you specified in the definitions.*

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

Sample:

```
# ipsec -p TCPIPT -y display
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 1 14:13:28 2015
Primary: Dynamic tunnel Function: Display Format: Detail
Source: Stack Scope: Current TotAvail: 1
```

```
TunnelID: Y3
Generation: 1
IKEVersion: 1.0
ParentIKETunnelID: K1
VpnActionName: VPN~A~6
LocalDynVpnRule: n/a
State: Active
HowToEncap: Tunnel
LocalEndPoint: 192.168.20.92 <<<<<<<<<<
RemoteEndPoint: 192.168.20.121 <<<<<<<<<<
LocalAddressBase: 192.168.20.122 <<<<<<<<<<
LocalAddressPrefix: n/a
LocalAddressRange: n/a
RemoteAddressBase: 192.168.20.121 <<<<<<<<<<
RemoteAddressPrefix: n/a
RemoteAddressRange: n/a
HowToAuth: ESP
AuthAlgorithm: HMAC-SHA1
AuthInboundSpi: 89648649 (0x 557EE09)
AuthOutboundSpi: 27422129 (0x 1A26DB1)
HowToEncrypt: 3DES-CBC
KeyLength: n/a
EncryptInboundSpi: 89648649 (0x 557EE09)
EncryptOutboundSpi: 27422129 (0x 1A26DB1)
Protocol: ALL(0)
LocalPort: n/a
LocalPortRange: n/a
RemotePort: n/a
RemotePortRange: n/a
Type: n/a
TypeRange: n/a
Code: n/a
CodeRange: n/a
OutboundPackets: 3
OutboundBytes: 852
InboundPackets: 3
InboundBytes: 852
Lifesize: 0K
LifesizeRefresh: 0K
CurrentByteCount: 0b
LifetimeRefresh: 2015/04/01 22:03:20
LifetimeExpires: 2015/04/01 22:07:41
CurrentTime: 2015/04/01 14:13:28
VPNLifeExpires: 2015/04/02 14:07:41
NAT Traversal Topology:
UdpEncapMode: No
LclNATDetected: No
RmtNATDetected: No
RmtNAPTDetected: No
```

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

```
RmtIsGw: n/a
RmtIsZOS: n/a
zOSCanInitP2SA: n/a
RmtUdpEncapPort: n/a
SrcNATOARcvd: n/a
DstNATOARcvd: n/a
PassthroughDF: Yes
PassthroughDSCP: Yes
*****
1 entries selected
#
```

6. Browse the ipsec.log.

a. obrowse /var/CSLOG/ipsec.log

Sending message:

Source Address: 192.168.20.92 Port: 500

Destination Address: 192.168.20.121 Port: 500

Dump of packet:

Storage Dump Length = 88 bytes

```
(000000) 000000: 732DC70B D3A6E51F 00000000 00000000
(000016) 000010: 01100200 00000000 00000058 0000003C
(000032) 000020: 00000001 00000001 00000030 01010001
(000048) 000030: 00000028 01010000 80010007 80020002
(000064) 000040: 80030001 80040002 800B0001 000C0004
(000080) 000050: 00015180 800E0080
```

...

Transform Payload

Next Payload: 0(NONE), Payload length: 0x28(40)

Transform Number: 0x1(1), Transform ID: 1(KEY_IKE)

Attribute Type: 1(**Encr Alg**),

Attribute Length(fixed)=0x2(2) Value=0x7(7)

(**AES-CBC**)

Attribute Type: 2(**Hash Alg**),

Attribute Length(fixed)=0x2(2) Value=0x2(2)

(**SHA1**)

Attribute Type: 3(**Auth Method**),

Attribute Length(fixed)=0x2(2) Value=0x1(1)

(**PresharedKey**)

Attribute Type: 4(Group Desc),

Attribute Length(fixed)=0x2(2) Value=0x2(2)

(1024 bit MODP)

Attribute Type: 11(Life Type),

Attribute Length(fixed)=0x2(2) Value=0x1(1)

(seconds)

Attribute Type: 12(Life Duration),

length: 0x4(4)

Value: 0x15180(86400)

Attribute Type: 14(Key Length),

Attribute Length(fixed)=0x2(2) Value=0x80(128)

*** SA Context Information ***

Phase 1 tunnel ID : K0 Generation : 0

Stackname : TCPIPT

Local IKE ID info : ID_FQDN WSC.LABS.IBM.COM

Remote IKE ID info : ID_USER_FQDN ZOS1@WSC.LABS.IBM.COM

Local IKE IP : 192.168.20.92 port 500

Remote IKE IP : 192.168.20.121 port 500

KeyExchangeRuleName : TrafOSA2DVIPAPresh~5

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

```
Icookie/Rcookie : x732DC70BD3A6E51F / x0000000000000000
IKE Version : 1
Pending phase 2 info:
Local IPSec upper-layer info : N/A N/A
Remote IPSec upper-layer info : N/A N/A
Local IPSec IP info : 192.168.20.122
Remote IPSec IP info : 192.168.20.121
Protocol : ALL(0)
...
```

7. Find the Transform Payload section of messages:
 - a. Which Encryption Algorithm (“Encr Alg”) is being proposed?

 - b. Which Hashing Algorithm (“Hash Alg”) is being proposed?

 - c. Which Authentication Method (“Auth Method”) is being proposed?

8. Provide the Security Endpoint Information -- IKE Authentication and IP Address information -- from the following messages:
 - a. Local IKE ID info : ID_FQDN _____
 - b. Remote IKE ID info : ID_USER_FQDN _____
 - c. Local IKE IP : 192.168.20._____ Port : _____
 - d. Remote IKE IP : 192.168.20._____ Port : _____
9. Provide the Data Endpoint Information from the following messages:
 - a. Local IPSec IP info : 192.168.20._____
 - b. Remote IPSec IP info : 192.168.20._____
10. Look for the “Encrypted Payload”
 - a. Observe how there are both an encrypted message and the decrypted message. *Do NOT be alarmed – this is not the actual data payload which does not display as decrypted.*
11. Close (**PF3**) the view of the log.
12. At your ZOSn OMVS console display the policy information from OMVS:
 - a. To display all IPSec policies
 - i. **pasearch -p TCPIPT -v a > ipsecout**
 - ii. **obrowse ipsecout**
 - iii. Browse through some IPSec rules in the output.
 - iv. Note how the Configuration Assistant tool creates many rules with the tilde number appended (ie. TrafOSA2DVIPAPresh~6). The Configuration Assistant tool creates multiple rules in this “modular” way to make each piece reusable.
 - v. When you are finished reviewing the policy configuration, use **PF3** to exit obrowse.
 - b. Alternatively subsets of the information may be displayed separately:
 - i. **pasearch -p TCPIPT -v f** displays the filter policies only.
 - ii. **pasearch -p TCPIPT -v k** displays the IKE policies only.
 - iii. **pasearch -p TCPIPT -v l** displays Local Dynamic VPN policies only.
 - iv. The pasearch parameters are all documented in the “IP System Administrator’s Commands” manual.

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

13. If you have time, practice deactivating IKE Tunnel and Dynamic Tunnel. (Issue the ping again if the tunnel goes down before you get the deactivate command issued.)
- Use the display IKE Tunnel or Dynamic Tunnel command to find the tunnel ID.
 - `ipsec -p TCPIPT -k display`
 - `ipsec -p TCPIPT -y display`
 - Issue the deactivate command.
 - `ipsec -p TCPIPT -k deactivate -a K2`
 - `ipsec -p TCPIPT -y deactivate -a Y2`

Samples:

```
# ipsec -p TCPIPT -y deactivate -a Y2
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 1 19:37:35 2015
Primary: Dynamic tunnel Function: Deactivate
```

Tunnel ID	LocalDynVpnRuleName	Status
Y2	<unknown>	Deactivating

```
#
# ipsec -p TCPIPT -k deactivate -a K1
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 1 19:51:42 2015
Primary: IKE tunnel Function: Deactivate
```

Tunnel ID	Status
K1	Deactivating

```
#
```

End of IPsec VPN Preshared Mode LAB

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

