

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

**"Configuring, Implementing, and Testing IPsec VPNs"**

**Hands-on Lab Guide**

**(IPsec VPN Lab)**



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

Revision date -

Monday, 23 June 2025

This edition applies to IBM z/OS Configuration Assistant running in z/OSMF on z/OS V3.1.

**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	
Review of IP Filtering (“permit” & “deny”) that You Defined in a Previous Lab.....	4
Overview of this LAB: Building Dynamic Tunnels using IPsec with RSA Signature Mode .....	5
Part 1: IPsec Dynamic Tunnels (RSA Signature Mode) for FTP between Addresses 192.168.20.91 and 192.168.20.9n.....	5
Worksheet: Collect the Information You Need to Configure a Dynamic Tunnel with RSA Signature Mode .....	6
Examine the certificate contents at your ZOSn and at ZOS1 .....	7
Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1 .....	7
Configure IPsec Dynamic Tunnels (RSA Signature Mode) .....	9
Sort the Connectivity Rules to the Correct Sequence .....	16
Send Your Configurations to Your ZOSn .....	18
Customize Pagent for the New VPN Rules on ZOSn.....	22
Configure IKE Daemon and Update SYSLOGD on ZOSn.....	23
Part 2: Test your IPsec Dynamic Tunnel Policies.....	24
Testing FTP Connections that use a Dynamic Tunnel Authenticated with RSA Mode .....	24
End of IPsec VPN LAB .....	31

## 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 FTPCCLn.

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).

### ***Review of IP Filtering (“permit” & “deny”) that You Defined in a Previous Lab***

In a previous lab, you built filters that permitted and denied traffic to addresses 192.168.20.100-192.168.20.108. These filters stay in place during this lab, but we will build an additional filter that invoke “permit with IPsec.” **The new filter in this lab will invoke authentication, data integrity checking, and encryption over dynamic tunnels.**

Your Lab Instructor has provided you with your TEAM name, your MVS system number, your USERID, and your PASSWORD. If you do not yet have this information, please advise the Instructor.

## **Overview of this LAB: Building Dynamic Tunnels using IPSec with RSA Signature Mode**

The Data Endpoint (DE) and Security Endpoints (SE) at ZOS1 are represented with the same IP address: 192.168.20.91. The DE and the SE at your MVS, ZOSn, are also identical to each other: both the DE and the SE are 192.168.20.9n.

From the perspective of ZOS1, this is a “Host-to-Host” configuration; from the perspective of ZOSn, this is also a “Host-to-Host” configuration.

*TRMD is required in order to capture any logging that you may wish to enable. IKED is required in order to establish Dynamic Tunnels. (Manual tunnels do not require IKED.)*

A traffic type of “FTP” is being protected over this VPN that is established with RSA Signature Mode.

We have already implemented FTP connectivity between the two MVS systems with AT-TLS, but the AT-TLS protection extended only to addresses 192.168.20.1ab and 192.168.20.100. ***Now we want to protect FTPs between addresses 192.168.20.9n and 192.168.20.91 by using IPSec.***

You will use the z/OS IBM Configuration Assistant to configure IPSec policies. RSA Signature Mode uses x.509 certificates for authentication and for establishing dynamic tunnel protocols with IKED. The IP identities are taken from the entries in the x.509 certificate; we will use the ***IP Address identity to authenticate the two IKED peers.***

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.**

*The lab is divided into two sections:*

- ***Part 1: Enable IPSec VPN Dynamic Tunnels with RSA Signature Mode:***  
***Configure IPSec VPN policies for FTPs between 192.168.20.91 and 192.168.20.9n***
- ***Part 2: Test the IPSec VPN Policies***

## **Part 1: IPSec Dynamic Tunnels (RSA Signature Mode) for FTP between Addresses 192.168.20.91 and 192.168.20.9n**

***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 RSA Signature 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 is represented?
  - 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. How is the LSE to identify itself during the Phase 1 security negotiations?
  - 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) \_\_\_\_\_
5. How is the RSE to identify itself during the Phase 1 security negotiations?
  - 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. Who owns the IKED Key ring and what is the name of the IKED Key ring that contains the appropriate x.509 certificates?
  - a. \_\_\_\_\_ / \_\_\_\_\_
7. Security Association (SA<sub>IKED</sub>): The Key Exchange Proposals that the peer (MVS1) wishes you to use (configured on MVS1):
  - a. **VPN~A** which means (example only, later releases may be different):
    - i. **3DES** with ESP
    - ii. **SHA-1**
    - iii. Diffie\_Hellman Group 2 (**DHGroup2**)
    - iv. **Lifetime of 1440** minutes (both min and max)
8. Security Association (SA<sub>IPSec</sub>): The Data Offer Proposals that the peer (MVS1) wishes you to use (configured on MVS1):
  - a. **VPN~A** which means (example only, later releases may be different):
    - i. **3DES** with ESP
    - ii. **SHA-1**
    - iii. Diffie\_Hellman Group 2 (**DHGroup2**)
    - iv. **Lifetime of 1440** minutes (both min and max)

### ***Examine the certificate contents at your ZOSn and at ZOS1***

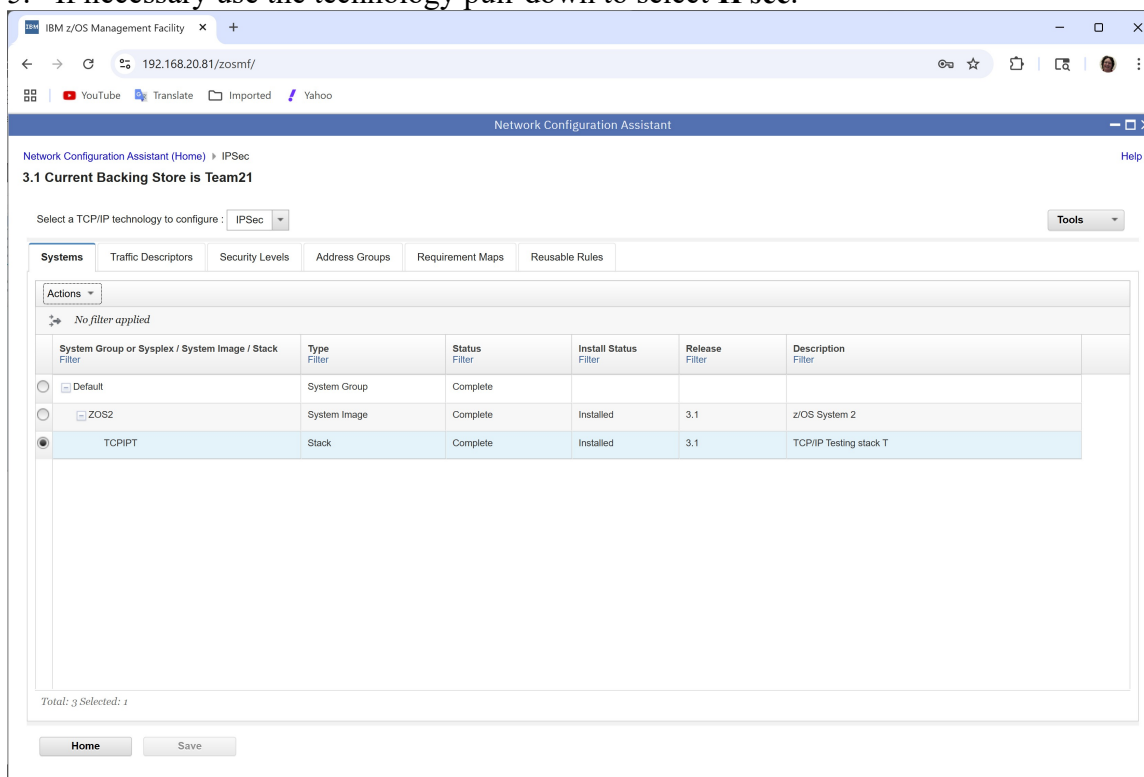
1. Log onto ZOSn and proceed to the ISPF Command Shell:
  - a. **ISPF 6**
2. At the Command Shell, enter the commands to view the contents of the IKED Key ring (IKEDnRING) to determine the label of the IKED procedure's certificate on your MVS:
  - a. **RACDCERT ID(IKED) LISTRING(\*)**
  - b. What is the Personal Certificate label from the correct IKED ring for our lab?
    - i. \_\_\_\_\_
3. At the Command Shell, enter the command to view the contents of the IKED Certificate that is required to negotiate a Dynamic Tunnel with RSA Signature Mode authentication:
  - a. **RACDCERT ID(IKED) LIST(LABEL('IKEDn at ZOSn'))**
4. Write down here the ALTNAME value that your IKED must present to the peer for RSA Signature Mode authentication:
  - a. **IP 192.168.20.** \_\_\_\_\_
5. Enter the commands to view the contents of the IKED1RING to determine the label of the IKED procedure's certificate at MVS1:
  - a. **RACDCERT ID(IKED) LISTRING(\*)**
  - b. What is the Certificate label that IKED at MVS1 will use in our lab?
    - i. \_\_\_\_\_
6. Enter the command to view the contents of the IKED Certificate that is required to negotiate a Dynamic Tunnel with RSA Signature Mode authentication:
  - a. **RACDCERT ID(IKED) LIST(LABEL('IKED1 at ZOS1'))**
7. Write down here the ALTNAME value that ZOS1's IKED must present to the peer for RSA Signature Mode authentication:
  - a. **IP 192.168.20.** \_\_\_\_\_

### ***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.

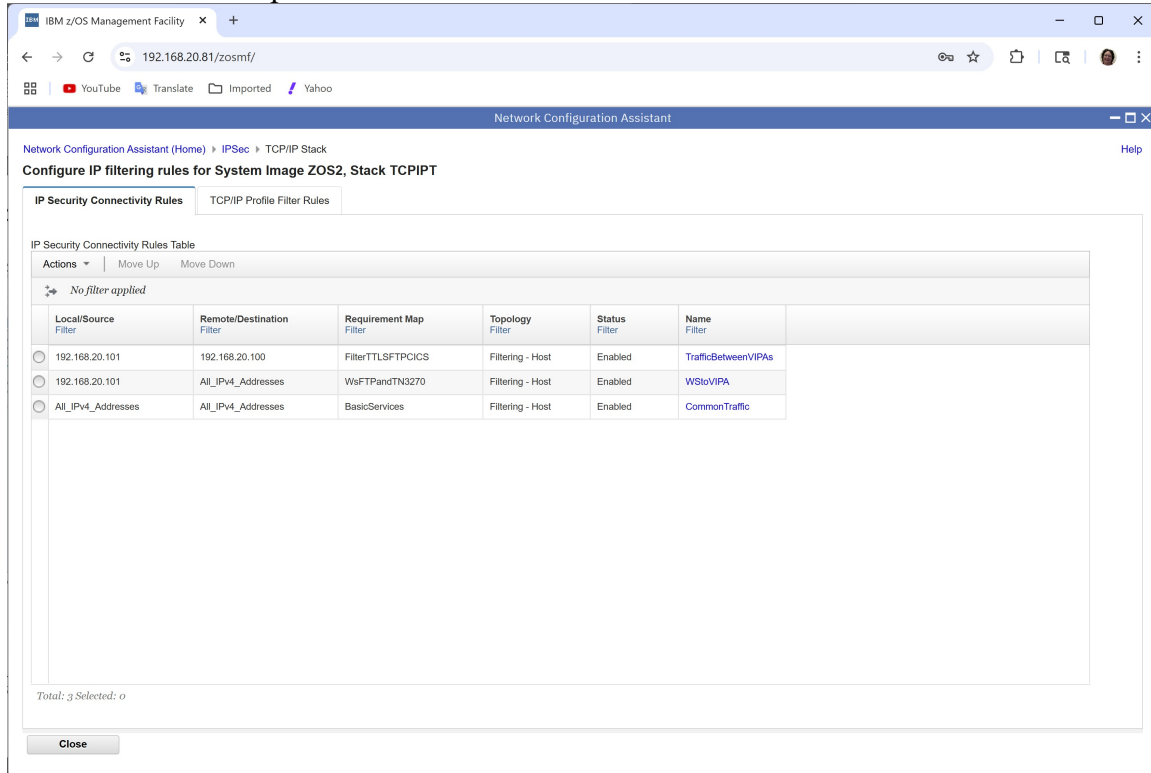
## Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

4. Use the pull-down if necessary to select your team's backing store file and click on the **Open** button.
5. If necessary use the technology pull-down to select **IPsec**.



## Configure IPsec Dynamic Tunnels (RSA Signature Mode)

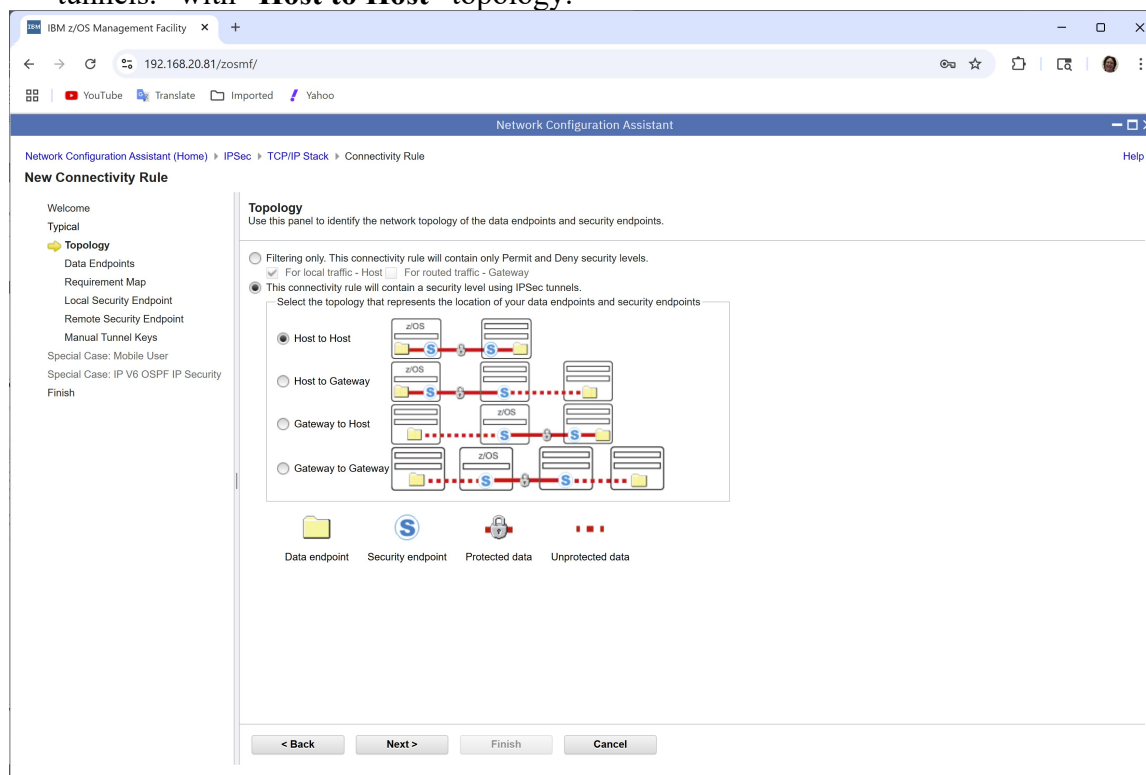
1. If necessary use the radio button to select your TCP/IP stack **TCPIPT**.
2. Use the **Actions** pull-down to select **Rules...**



3. Note the Connectivity Rules pointing to the addresses **192.168.20.1ab**. Look at the **Topology** column where you notice that these rules represent **Filtering-Host** rules for your ZOSn.
  - a. We could modify these rules to convert them to an IPsec VPN topology, but, instead we will create new connectivity rules.
  - b. 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. Accept the default “This connectivity rule will contain a security level using IPSec tunnels.” with “**Host to Host**” topology.



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

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

### 8. Give the new rule the name **BetweenOSAsRSA**.

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

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

#### 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.

Host to Host - Data Endpoints

\* Connectivity rule name:  
BetweenOSAsRSA

Local data endpoint

Address group:  
All\_IPv4\_Addresses

\* IPv4 or IPv6 address, subnet, or range:  
192.168.20.92

Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y  
x:x, x:x/yyy, x:x-y:y

Stack Symbol name:  
No stack symbol names are configured.

Remote data endpoint

Address group:  
All\_IPv4\_Addresses

\* IPv4 or IPv6 address, subnet, or range:  
192.168.20.91

Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y  
x:x, x:x/yyy, x:x-y:y

< Back Next > Finish Cancel

### 9. Identify the specific addresses for the Local Data Endpoint and the Remote Data Endpoint.

- Local data endpoint **192.168.20.9n**
- Remote data endpoint **192.168.20.91**
- Press **Next**.

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

## 10. Keep the **Create a new requirement map** default.

The screenshot shows the 'Network Configuration Assistant' window. The left sidebar lists navigation options: Welcome, Typical, Topology, Data Endpoints, **Requirement Map** (selected), Local Security Endpoint, Remote Security Endpoint, Manual Tunnel Keys, Special Case: Mobile User, Special Case: IP V6 OSPF IP Security, and Finish. The main area is titled 'Requirement Map' and contains the following elements:

- A diagram showing traffic flow between z/OS and a host.
- Text: 'Requirement maps are reusable objects that combine your traffic definitions (traffic descriptors) with your security definitions (security levels). Use this panel to select the requirement map for the data endpoints for Host To Host topology.'
- Radio buttons: ☒ Create a new requirement map, ☐ Select an existing requirement map.
- A dropdown menu showing 'BasicServices'.
- Section: 'New Requirement Map properties'.
- Field: '\* Name: FTPClientServer'.
- Field: 'Description: FTP protected by IPsec'.
- Section: 'Mappings table'.
- A table with columns 'Traffic Descriptor' and 'Security Level'.
- Buttons: '< Back', 'Next >', 'Finish', 'Cancel'.

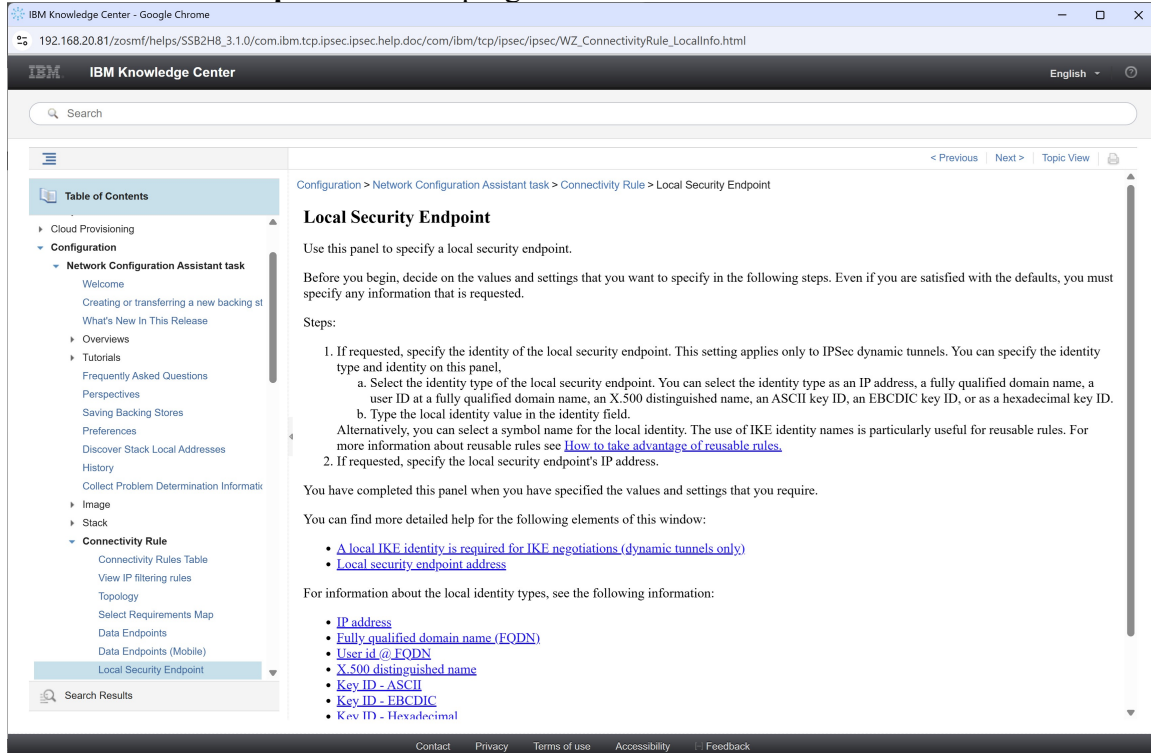
Traffic Descriptor	Security Level
FTP-Client	VPN-A
FTP-Server	VPN-A

Total: 2 Selected: 1

11. Name the Requirement Map **FTPClientServer** and optionally add a description.
12. If necessary use the **Actions** pull-down to select **Add Row**.
13. Use the pull-down for the traffic descriptor field in each row in turn to select:
  - a. **FTP-Client**
  - b. **FTP-Server**
14. For each of those rows:
  - a. Use the pull-down for the security level field to select **VPN~A**.
15. **If** there are any rows below the ones that you just customized, use the radio button to select them and the **Actions** pull-down to select **Remove Row**.
16. Click on **Next**.

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

17. Determine how the Local Security Endpoint panel should be filled in:
- Press the **Help** link in the top right corner.



18. Select one of the following items from the Help panel and read the explanation
- “A local IKE identity is required ....” or “Local security endpoint address”.
    - This help panel does not tell you that the IKE identity or Local security endpoint must be one of the fields – possibly an ALTNAME field -- in the x.509 certificate when you are using RSA Signature Mode. ***It expects you to know the IPSec protocol when responding to this question.***
  - Close the HELP panel.

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

19. Accept the default (or update if needed) Local identity type of **IP Address** and Local identity of **192.168.20.9n**.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The browser address bar displays `192.168.20.81/zosmf/`. The NCA window has a title bar "Network Configuration Assistant" and a breadcrumb trail: "Network Configuration Assistant (Home) > IPsec > TCP/IP Stack > Connectivity Rule".

On the left, a "New Connectivity Rule" sidebar lists several steps: Welcome, Typical, Topology, Data Endpoints, Requirement Map, **Local Security Endpoint** (highlighted with a yellow star), Remote Security Endpoint, Manual Tunnel Keys, Special Case: Mobile User, Special Case: IP V6 OSPF IP Security, and Finish.

The main panel is titled "Local Security Endpoint". It contains a diagram of two z/OS systems connected by a red line with a lock icon. Below the diagram, a text box states: "A local IKE identity is required for IKE negotiations (used for dynamic tunnels only)".

There are two radio button options:

- ☒ Local identity type: IP Address (selected). Below this, a text field labeled "\* Local identity:" contains the value "192.168.20.92".
- ☐ Select symbol: No IKE identity symbols are configured for this stack. (disabled)

At the bottom of the panel are four buttons: "< Back", "Next >", "Finish", and "Cancel".

20. Click on the **Next** button.

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

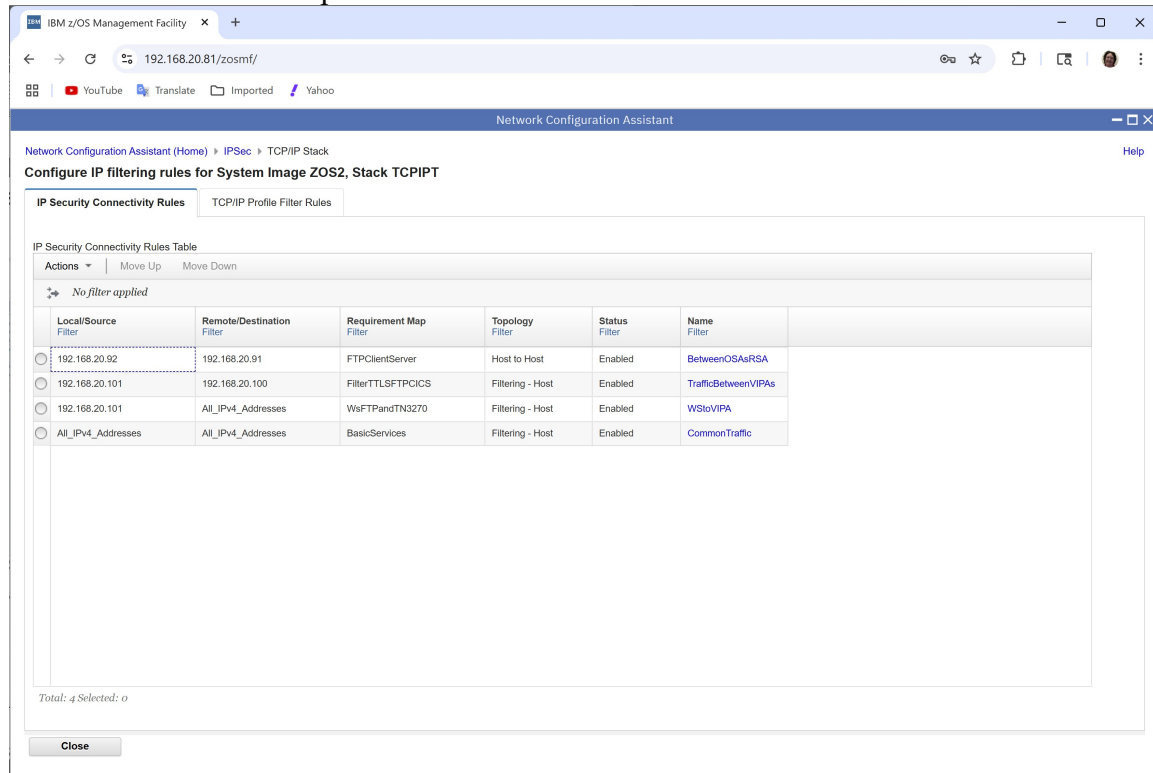
21. Accept the default (or update if needed) Remote identity type of **IP Address** and Remote identity of **192.168.20.91**.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant interface. The browser address bar displays '192.168.20.81/zosmf/'. The page title is 'Network Configuration Assistant'. The breadcrumb navigation shows 'Network Configuration Assistant (Home) > IPsec > TCP/IP Stack > Connectivity Rule'. The main heading is 'New Connectivity Rule'. On the left, a sidebar lists steps: Welcome, Typical, Topology, Data Endpoints, Requirement Map, Local Security Endpoint, Remote Security Endpoint (highlighted), Manual Tunnel Keys, Special Case: Mobile User, Special Case: IP V6 OSPF IP Security, and Finish. The 'Remote Security Endpoint' section contains a diagram of two hosts connected by a line with a lock icon. Below the diagram, text states: 'Use this panel to enter information about the IPsec remote security endpoint for Host To Host topology. A remote IKE identity is required for IKE negotiations (used for dynamic tunnels only)'. The 'Remote identity type' is set to 'IP Address' in a dropdown menu. The 'Remote identity' field contains '192.168.20.91'. Under 'Indicate how to authenticate the IKE peers (used for dynamic tunnels only)', the 'Digital signature' radio button is selected. The 'Shared key' section has radio buttons for 'EBCDIC', 'ASCII', and 'Hexadecimal', with 'EBCDIC' selected. A 'Key' field is present but empty. At the bottom, there is an 'Additional IKEv2 options...' link and four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

22. Accept the default IKE peers' authentication method of **Digital signature**.  
23. Click on the **Next** button.  
24. Use the radio button to select **Yes, log all filter matches**.  
25. Click on the **Finish** button.  
26. Use the Actions pull-down to select **Health Check**.  
    a. Review results for anomalies and then close the window.  
27. Click on **Close**.  
28. Click on **Save**.

## Sort the Connectivity Rules to the Correct Sequence

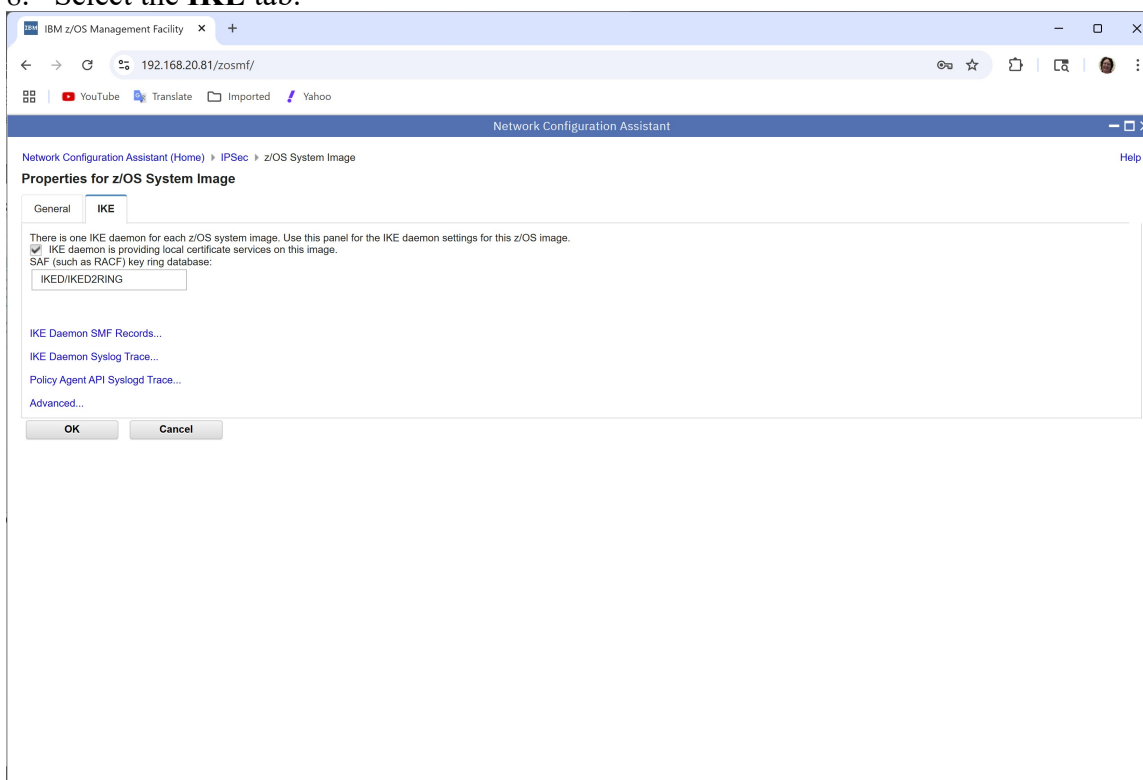
1. Return to the Connectivity Rules view.
  - a. Use the **Actions** pull-down to select **Rules...**



2. The IP addresses in a packet are compared with the IP addresses of the data endpoints of the connectivity rules in the order in which those rules appear in the table.
3. **Make sure the most Discrete or Unique rule is found first**, after which more general rules follow. The correct sequence should be similar to what you see here. (The first two rules depicted can be in any order since they are equally unique. The last two in the visual must be in the sequence depicted.) If the sequence is not correct,
  - a. Highlight one rule at a time.
  - b. Click on the **Move Up** or **Move Down** button until the sequence is correct.
4. Use the Actions pull-down to select **Health Check** to check for any configuration errors.
  - a. **Close** the Health Check help panel after you have reviewed it.
5. Click on **Close** and **Save**, optionally add a comment, and click on the **OK** button.
6. Use the radio button to select your z/OS image **ZOSn**.
7. Use the Actions pull-down to select **Properties...**

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

### 8. Select the **IKE** tab.



### 9. Fill in the owner and name of the IKED key ring for your ZOS system:

- a. **IKED/IKEDnRING**

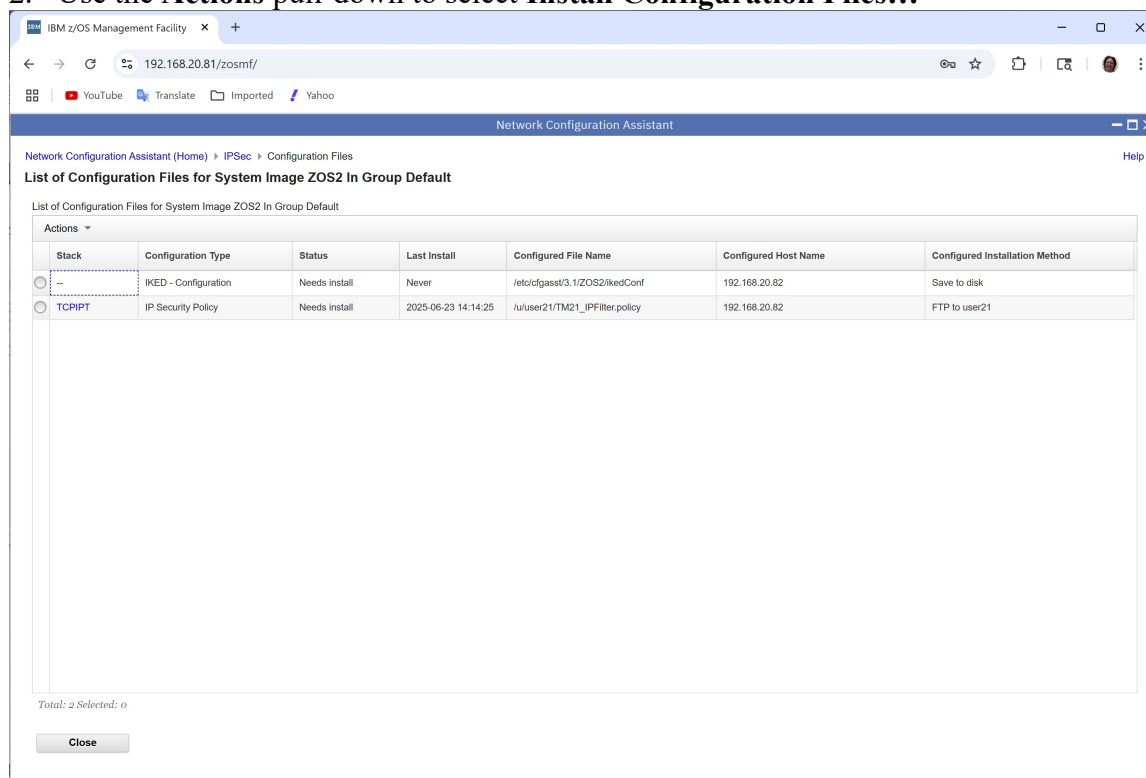
### 10. Review the other links and when you are finished:

- a. **OK**
- b. **Save**
- c. **OK**

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

## Send Your Configurations to Your ZOSn

1. Now send the policy configuration you just created up to your **ZOSn** system.
2. Use the **Actions** pull-down to select **Install Configuration Files...**

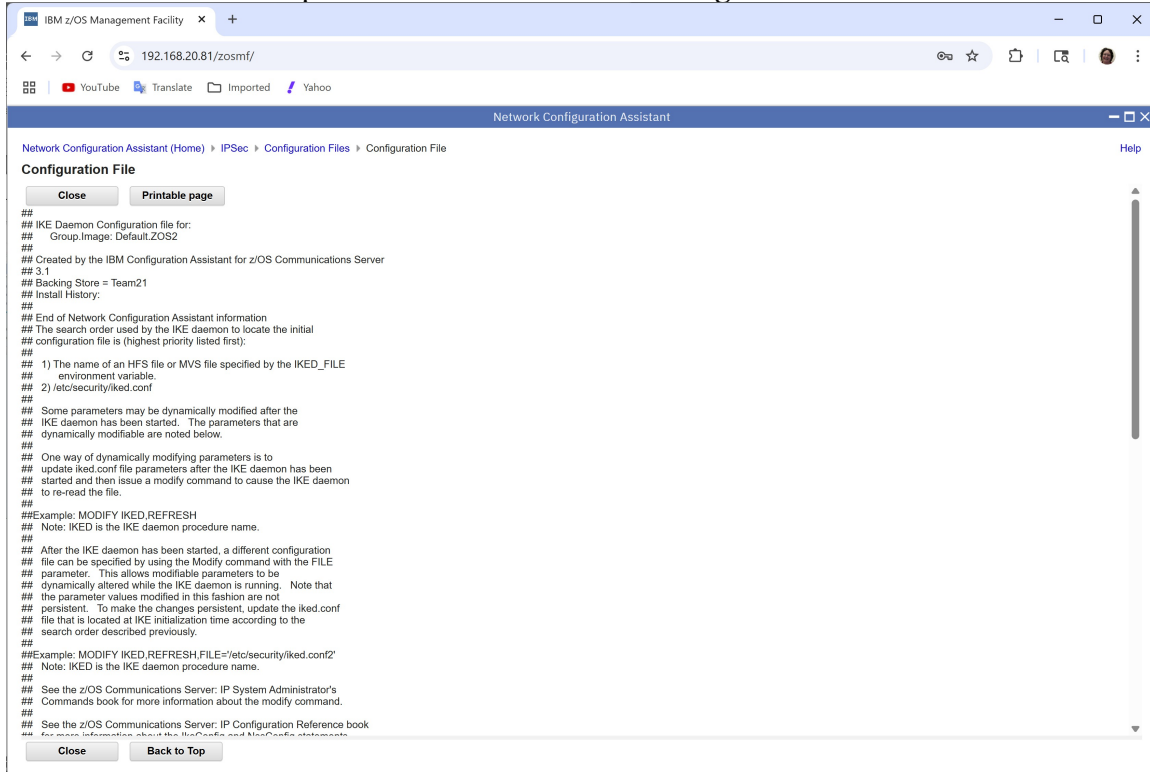


3. The following files should be listed:
  - a. **IKED – Configuration** (IKE Daemon Configuration)
  - b. **TCPIPT - IP Security Policy** (IPSec Policy file)

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

## 4. First, select **IKED - Configuration**

### a. Use the Actions pull-down to select **Show Configuration File...**



### b. Review the settings for logging.

### c. Review the settings for the IKED Key ring.

### d. **Close** the view of the file when you are finished reviewing it.

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

### 5. Use the Actions pull-down to select **Install...**

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

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

Help

**Install File for Default.ZOS2**

\* Install file name:

/u/user21/iked.conf

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

6. Change the Install file name to **/u/user`nx`/iked.conf**
7. Select FTP transfer. You may have some customization from a previous lab that you may continue to use:
  - a. Host name **192.168.20.8`n`**
  - b. User ID **user`nx`**
  - c. <password>
8. Optionally add a comment.
9. Click on **Go**
10. Click on **OK** twice.
11. Click on **Close**.
12. Use the radio button to select **TCPIPT – IP Security Policy**.

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

### 13. Use the **Actions** pull-down to select **Install...**

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

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

Help

**Install File for Default.ZOS2.TCPIPT**

\* Install file name:

/u/user21/TM21\_IPSecVPN.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

user21

14. Install file name **/u/usernx/TMnx\_IPSecVPN.policy**

15. Host name **192.168.20.8n**

16. User ID **usernx**

17. Password **<password>**

18. Click on **Go**, **OK** twice, **Close** twice.

## ***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 Pagent Configuration file you created in a previous lab.
  - a. **su**
  - b. **oedit pagentt.conf**
6. **Comment out the previous IPSecConfig Statement.**
7. Add an IPSecConfig statement in the appropriate place in the file:
  - a. **IPSecConfig /u/usernx/TMnx\_IPSecVPN.policy**
    - i. Filter and VPN Policies do not use “FLUSH” and “PURGE”.
8. Save your changes to the file using **PF3** to exit from the file.

## **Configure IKE Daemon and Update SYSLOGD on ZOSn**

1. Increase the IKED and the PAGENT PAPI logging levels by editing the IKED configuration file (**oedit iked.conf**) in your own subdirectory and adding the following two lines in the file:
    - a. **IkeSyslogLevel 127**
    - b. **PagentSyslogLevel 127**
      - i. *If you later forget to reset these values to “1” and “0” after testing, you will continue to generate huge amounts of output.*
      - ii. *After IKED has been started you do not need to recycle it to change the log levels. Change the values in the configuration file and then issue the **/F IKED,REFRESH** command to pick up the new log levels.*
  2. Identify the name of the IKED key ring that you will be using:
- 
3. Save and exit the file with **PF3**.
  4. Switch to SuperUser mode if not already set.
    - a. Enter **su** on the Command line on the bottom of the window.
  5. Copy your version of the IKED Configuration file into the /etc/security directory.
    - a. **cp iked.conf /etc/security/**
  6. Edit your copy of the syslogd Configuration file.
    - a. **oedit syslogt.conf**
  7. Find the statement to cause separate IKE logging. Uncomment the following line:
    - a. **local4.\* /var/CSLOG/ipsec.log**
  8. Find the statement that prevents double logging. Uncomment the following line:
    - a. **local4.none;\*. \* /var/CSLOG/syslogall.log**
  9. Comment out the previous logging statement:  
**# \*. \* /var/CSLOG/syslogall.log**
  10. Close and save the syslogt.conf file with **PF3**.
  11. Replace the running copy of the syslogd configuration file.
    - a. **cp syslogt.conf /etc/syslog.conf**
  12. Exit OMVS and pick up the new SyslogD configuration:
    - a. **exit, exit, Enter, =D.LOG, /F SYSLOGDC,RESTART**
  13. Start your IKE Daemon, which *points to the default /etc/security/iked.conf*.
    - a. **/S IKED**

## Part 2: Test your IPSec Dynamic Tunnel Policies

## Testing FTP Connections that use a Dynamic Tunnel Authenticated with RSA Mode

1. Display the parameters for the running IKE Daemon:
  - a. **/F IKED,DISPLAY**
    - i. Verify the name of the key ring.

```
F IKED,DISPLAY  
EZD1158I DISPLAY IKE CONFIGURATION 736  
DISPLAY IKE configuration parameters:  
Values loaded from /etc/security/iked.conf  
IkeSyslogLevel = 127  
PagentSyslogLevel = 127  
SMF119 = NONE  
Keyring = IKED/IKED2RING <<<<<<<<<<  
IkeRetries = 6  
IkeInitWait = 2  
FIPS140 = no  
Echo = no  
PagentWait = 0  
NssWaitLimit = 60  
NssWaitRetries = 3  
IKE configuration contains no SupportedCertAuth labels.  
IKE configuration contains no NetworkSecurityServer info.  
IKE configuration contains no NetworkSecurityServerBackup info.  
IKE configuration contains no NssStackConfig definitions.
```
2. Copy your version of the Pagent Configuration file.
  - a. Go to OMVS: **TSO OMVS**
  - b. Enter **su** to change into super user mode.
  - c. **cp pagentt.conf /etc/PAGT1/.**
3. Return to Log and Load your new policies.
  - a. **/S PAGENTT** (if PAGENT is down)  
or  
b. **/F PAGENTT,UPDATE** (if PAGENT is already up)
4. Return to OMVS to verify you are actually running the Stack Policy Rules:
  - a. Enter the UNIX environment:
    - i. **TSO OMVS**
  - b. Enter the command to show the first 12 lines of output from the Filter Display command that you learned earlier:
    - i. **ipsec -f dis -p TCPIPT | head -n 12**
  - c. What type of policies for IPsec have been loaded?
    - i. The **Stack Profile Rules** or the **Stack Policy Rules?** (Circle the correct answer.)
  - d. If the display did not show the Policy Rules loaded, execute the command to reload the policy rules:
    - i. **ipsec -f reload -p TCPIPT**

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

5. Execute the **Traffic Test command** to locate and display active filter rules that match particular data traffic patterns for **inbound** traffic:

- ipsec -p TCPIPT -t 192.168.20.91 192.168.20.9n udp 500 500 in 0**
- 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 192.168.20.91 192.168.20.92 udp 500 500 in 0
```

```
CS 3.1 ipsec Stack Name: TCPIPT Mon Jun 23 16:18:39 2025
Primary: IP Traffic Test Function: Display Format:
Detail
Source: Stack Policy Scope: n/a TotAvail: 2
TestData: 192.168.20.91 192.168.20.92 udp 500 500 in 0
Defensive Mode: Inactive
```

```
FilterName: BetweenOSAsRSA~6
FilterNameExtension: 2
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: 0x00
Type: Generic
DefensiveType: n/a
State: Active
Action: Permit
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: n/a
Protocol: UDP (17)
ICMPType: n/a
ICMPTypeGranularity: n/a
ICMPCode: n/a
ICMPCodeGranularity: n/a
OSPFType: n/a
TCPQualifier: n/a
ProtocolGranularity: n/a
SourceAddress: 192.168.20.91
SourceAddressPrefix: n/a
SourceAddressRange: n/a
SourceAddressGranularity: n/a
SourcePort: 500
SourcePortRange: n/a
SourcePortGranularity: n/a
DestAddress: 192.168.20.92
DestAddressPrefix: n/a
DestAddressRange: n/a
DestAddressGranularity: n/a
DestPort: 500
DestPortRange: n/a
DestPortGranularity: n/a
OrigRmtConnPort: n/a
RmtIDPayload: n/a
```

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

```
RmtUdpEncapPort:      n/a
CreateTime:           2025/06/23 16:16:38
UpdateTime:           2025/06/23 16:16:38
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
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:            2025/06/23 11:23:42
```

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

```
UpdateTime:                2025/06/23 16:16:38
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

6. Execute the **Traffic Test command** to locate and display active filter rules that match particular data traffic patterns for **outbound** traffic:
  - a. **ipsec -p TCPIPT -t 192.168.20.9n 192.168.20.91 udp 500 500 out**  
*Observe how the output tells you that you have a **Policy Rule** for this type of traffic and that you also have a **DenyAll** Rule that was automatically generated.*
7. Things should be looking good, and so test your non-AT-TLS secured FTP Client by connecting from ZOSn to ZOS1 at **192.168.20.91**:
  - a. From your OMVS:
    - i. **ftp -p TCPIPT -s 192.168.20.9n 192.168.20.91**
  - b. Or From your TSO:
    - i. **ftp 192.168.20.91 (TCP TCPIPT**
    - ii. **or ftp -s 192.168.20.9n 192.168.20.91 (TCP TCPIPT**
  - c. The connection should **succeed**.
    - i. NOTE: You are protecting this FTP connection only with IPsec; there is no need for AT-TLS here.
8. Test your ATTLS-secured FTP Client by connecting from your ZOSn to ZOS1 at 192.168.20.101.
  - a. From your OMVS:  
**ftp -r tls -p TCPIPT -f "'/USER.CS.TCPPARMS(FTPCLSnx)'"**  
**192.168.20.100**
  - b. Or From your TSO:  
**ftp -r TLS -p TCPIPT -f "'/USER.CS.TCPPARMS(FTPCLSnx)'"**  
**192.168.20.100**
  - c. The connection should also still **succeed**.
9. You are protecting this type of connection with AT-TLS and the IPsec filters are merely permitting the connection. 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.*
  - c. Note in your display the IKE Tunnel ID. Dynamic Data Traffic Tunnels are always associated with their Parent IKE Tunnel ID.

```
$ ipsec -p tcpipt -k display
CS V2R1 ipsec Stack Name: TCPIPT Thu Mar 26 15:46:47 2015
Primary:  IKE tunnel      Function: Display      Format:  Detail
Source:   IKED            Scope:      Current      TotAvail: n/a
TunnelID:                               K1
```

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

```

Generation: 1
IKEVersion: 1.0
KeyExchangeRuleName: BetweenOSAsRSA~5
KeyExchangeActionName: BetweenOSAsRSA
LocalEndPoint: 192.168.20.92 <<<<<<<<<<<<
LocalIDType: ID_IPV4_ADDR <<<<<<<<<<<<
LocalID: 192.168.20.92 <<<<<<<<<<<<
RemoteEndPoint: 192.168.20.91 <<<<<<<<<<<<
RemoteIDType: ID_IPV4_ADDR <<<<<<<<<<<<
RemoteID: 192.168.20.91 <<<<<<<<<<<<
ExchangeMode: Main
State: DONE
AuthenticationAlgorithm: HMAC-SHA1 <<<<<<<<<<<<
EncryptionAlgorithm: 3DES-CBC <<<<<<<<<<<<
KeyLength: n/a
PseudoRandomFunction: HMAC-SHA1
DiffieHellmanGroup: 2
LocalAuthenticationMethod: RsaSignature <<<<<<<<<<<<
RemoteAuthenticationMethod: RsaSignature <<<<<<<<<<<<
InitiatorCookie: 0x235E465096534E8E
ResponderCookie: 0x329AE55F47221663
Lifesize: OK
CurrentByteCount: 616b
Lifetime: 1440m
LifetimeRefresh: 2015/03/27 15:10:33
LifetimeExpires: 2015/03/27 15:21:55
ReauthInterval: 1440m
ReauthTime: 2015/03/27 15:10:33
Role: Initiator
AssociatedDynamicTunnels: 1 <<<<<<<<<<<<
NATTSupportLevel: None
NATInFrntLclScEndPnt: No
NATInFrntRmtScEndPnt: No
zOSCanInitiatePIA: Yes
AllowNat: No
RmtNAPTDetected: No
RmtUdpEncapPort: n/a
*****

```

```

1 entries selected
$

```

### 10. 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.*
- c. Note in your display how the Tunnel ID (e.g., Y2 and Y1) is associated with the Parent IKE Tunnel ID (K1).

```

$ ipsec -p tcpipt -y display
CS V2R1 ipsec Stack Name: TCPIPT Thu Mar 26 15:59:54 2015
Primary: Dynamic tunnel Function: Display Format: Detail
Source: Stack Scope: Current TotAvail: 1
TunnelID: Y2
Generation: 1
IKEVersion: 1.0
ParentIKETunnelID: K1

```

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

```

VpnActionName:          VPN~A
LocalDynVpnRule:        n/a
State:                  Active
HowToEncap:             Transport  <<<<<<<<<<<<
LocalEndPoint:          192.168.20.92  <<<<<<<<<<<<
RemoteEndPoint:         192.168.20.91  <<<<<<<<<<<<
LocalAddressBase:       192.168.20.92
LocalAddressPrefix:     n/a
LocalAddressRange:      n/a
RemoteAddressBase:      192.168.20.91
RemoteAddressPrefix:    n/a
RemoteAddressRange:     n/a
HowToAuth:              ESP
  AuthAlgorithm:         HMAC-SHA1  <<<<<<<<<<<<
  AuthInboundSpi:        3345891883 (0xC76E422B)  <<<<<<<
  AuthOutboundSpi:       910334912  (0x36429BC0)
HowToEncrypt:           3DES-CBC  <<<<<<<<<<<<
  KeyLength:             n/a
  EncryptInboundSpi:     3345891883 (0xC76E422B)  <<<<<<<
  EncryptOutboundSpi:    910334912  (0x36429BC0)
Protocol:               TCP (6)
LocalPort:              1025
LocalPortRange:         n/a
RemotePort:             21
RemotePortRange:        n/a
Type:                   n/a
TypeRange:              n/a
Code:                   n/a
CodeRange:              n/a
OutboundPackets:        9
OutboundBytes:          323
InboundPackets:         7
InboundBytes:           444
Lifesize:               0K
LifesizeRefresh:        0K
CurrentByteCount:       0b
LifetimeRefresh:        2015/03/26 23:16:19
LifetimeExpires:        2015/03/26 23:21:55
CurrentTime:            2015/03/26 15:59:54
VPNLifetimeExpires:     2015/03/27 15:21:55
NAT Traversal Topology:
  UdpEncapMode:          No
  LclNATDetected:        No
  RmtNATDetected:        No
  RmtNAPTDetected:       No
  RmtIsGw:               n/a
  RmtIsZOS:              n/a
  zOSCanInitP2SA:        n/a
  RmtUdpEncapPort:       n/a
  SrcNATOArcvd:          n/a
  DstNATOArcvd:          n/a
PassthroughDF:          n/a
PassthroughDSCP:        n/a
*****
1 entries selected
$

```

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

11. Open the SYSLOG Daemon log (ipsec.log) to look for IKE and IPsec messages:
  - a. **su**
  - b. **obrowse /var/CSLOG/ipsec.log**
  - c. Remember: The IKE information is now **ONLY** in the separate **ipsec.log** and not in the syslogall.log file because you specified “local4.none” on the second line below. If you had not done so, you would have been logging in two locations and consuming additional logging space.
    - i. local4.\* /var/CSLOG/ipsec.log
    - ii. local4.none;\*. \* /var/CSLOG/syslogall.log
12. Notice message ESD0990I The IKE daemon is set up to support RSA signature mode of authentication.
13. Find the section that starts with “Transform Payload” and fill in the blanks. If you don’t find a “Transform Payload” section in your log you can skip this section or increase your policy agent log level (max 511). Hint: To increase your policy agent log level you may refer to the class lecture.
  - a. Transform Payload
  - b. Next Payload: 0(NONE), Payload length: 0x24(36)
  - c. Transform Number: 0x1(1), Transform ID: 1(KEY\_IKE)
  - d. Attribute Type: 1(Encr Alg),
  - e. Attribute Length(fixed)=0x2(2) Value=0x5(5)
  - f. (\_\_\_\_\_)
  - g. Attribute Type: 2(Hash Alg),
  - h. Attribute Length(fixed)=0x2(2) Value=0x2(2)
  - i. (\_\_\_\_\_)
  - j. Attribute Type: 3(Auth Method),
  - k. Attribute Length(fixed)=0x2(2) Value=0x3(3)
  - l. (\_\_\_\_\_)
14. Find the section that starts with “Phase 1 tunnel ID...” and fill in the blanks:
  - a. Phase 1 tunnel ID : K0 Generation : 0
  - b. Stackname : TCPIPT
  - c. Local IKE ID info : ID\_IPV4\_ADDR 192.168.20.\_\_\_\_\_
  - d. Remote IKE ID info : ID\_IPV4\_ADDR 192.168.20.\_\_\_\_\_
  - e. Local IKE IP : 192.168.20.\_\_\_\_\_ port \_\_\_\_\_
  - f. Remote IKE IP : 192.168.20.\_\_\_\_\_ port \_\_\_\_\_
  - g. KeyExchangeRuleName : BetweenOSAsRSA~5
  - h. Icookie/Rcookie : x235E465096534E8E /  
x0000000000000000
  - i. IKE Version : 1
  - j. Pending phase 2 info:
  - k. Local IPsec upper-layer info : port \_\_\_\_\_
  - l. Remote IPsec upper-layer info : port \_\_\_\_\_
  - m. Local IPsec IP info : 192.168.20.\_\_\_\_\_
  - n. Remote IPsec IP info : 192.168.20.\_\_\_\_\_

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

15. Look for one of the “Certificate Request Payload” entries and examine the contents. You should recognize some of the fields. This is an example:  
**Certificate Request Payload:**  
**Next Payload:** 0(NONE), **Payload Length:** 0x44(68)  
**Certificate Encoding Type:** 4(X.509 Certificate - Signature)  
**Certificate Authority (length 0x3f(63) in bytes):**  
**Storage Dump Length = 63 bytes**  
**IKE CERTINFO : Matched certificate with label IKED2 at ZOS2**
16. Look for one of the “ID Payload” entries and examine the contents. You should recognize some of the fields. This is an example:  
**ID Payload**  
**Next Payload:** 6(Certificate), **Payload length:** 0xc(12)  
**ID type:** 1(IPV4), **Protocol:** 0, **Port = 0x0(0)**  
**ID:**  
**IP Address:** 192.168.20.92
17. Finally, notice there are “Message before decryption” sections followed by “Message after decryption” sections.
18. **OPTIONAL:** Test your FTP Server by connecting from ZOS1 to our ZOSn. That is: Logon to ZOS1 and FTP from there to your MVSn.
  - a. Logon to MVS1 with PComm session to MVS1 address 192.168.20.81.
  - b. From OMVS or TSO at ZOS1:  
**ftp -r TLS -f "///SYS1.CS.TCPPARMS(FTPCLSEC)" -p TCPIPT 192.168.20.10n**
19. This should work since you have allowed this connection at the IP layer and encrypted this traffic with AT-TLS.
20. After your test **PLEASE** be sure to log off of MVS1.
  - a. **Log off MVS1**
  - b. **Close MVS1 PComm session.**
  - a. **You MUST log off of MVS1 and close the PComm session to avoid accidentally making changes on MVS1!!!**
  - b. Click on the “X” in the top right of the PComm session window to close it.

## End of IPsec VPN LAB

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

