

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

"Examining Network Security Services Daemon (NSSD) Hands-on Lab Guide

(NSSD 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.

Table of Contents

Part 0: Lab Description for <i>Network Security Services Daemon (NSSD) and Internet Key Exchange Version 2 (IKEv2)</i>	4
Overview of this LAB: NSSD and IKEv2	5
Part 1: Network Security Services Daemon (NSSD) and IKEv2 Definitions	6
Review ZOS1 NSSD RACF Definitions	6
Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1	9
Select IKEv2 for IPSec	10
Create IP Filter Policy for AT-TLS Connection	12
Create NSSD Configuration File	14
Create AT-TLS Policy	21
Part 2: Network Security Services Daemon (NSSD) and IKEv2 Testing	26
Check NSSD Definitions on ZOSn	26
FTP with IKEv1	26
Test NSSD and IKEv2	27
End of NSSD LAB	30

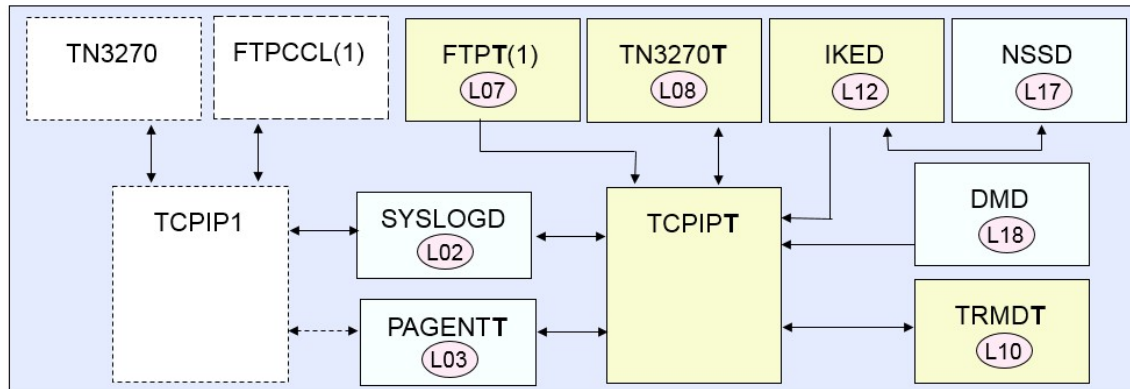
Part 0: Lab Description for *Network Security Services Daemon (NSSD) and Internet Key Exchange Version 2 (IKEv2)*

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.

Overview of this LAB: NSSD and IKEv2



- “Maintenance” TCP/IP stack (TCPIP1)
- “Student” TCP/IP stack (TCPIPT)
- Stack Specific
 - TN3270 (Lab L08)
 - FTP (Lab L07)
 - TRMD (Lab L10)
- Available to all TCP/IP Stacks
 - SYSLOGD (Lab L02)
 - PAGENT (Lab L03)
 - IKED (Lab L12)
 - NSSD (Lab L17)
 - DMD (Lab L18)

You will use the z/OS IBM Configuration Assistant tool to configure NSSD and IKED configuration files, change the previous IPsec policies to use IKEv2 protocol, and create AT-TLS policies for connections between the NSSD server and the NSS client IKED.

The NSSD Daemon owns a key ring and all the private certificates that reside on it. The RACF Key Ring is named “NSSDnRing.” The NSSD certificate used for AT-TLS Server Authentication is named “NSSDn at ZOSn”. The NSS Client IKED certificate used to identify itself to partner IKED servers is named “NSS Client at ZOSn”. The RACF Key Ring also contains a copy of both of the Certificate Authority Certificates, one for each side of the IKED to IKED connection. **All the required certificates for this lab, including all the student certificates, have already been created for you.**

You will use the previously create IPsec policies and FTP to test the NSSD and IKEv2 implementations.

The lab is divided into two sections:

- **Part 1: Network Security Services Daemon (NSSD) and IKEv2 Definitions**
- **Part 2: Network Security Services Daemon (NSSD) and IKEv2 Testing**

Part 1: Network Security Services Daemon (NSSD) and IKEv2 Definitions

Review ZOSn NSSD RACF Definitions

NSSD requires several RACF steps as outlined in the “IP Configuration Guide” manual. All the required RACF steps have been done for you in this class.

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 TSO Command input panel.
 - a. **=6**
4. NSSD uses AT-TLS for NSSD Client IKED connections.
5. View the RACF key ring.
 - a. **RACDCERT ID(NSSD) LISTRING(NSSDnRing)**
6. View the RACF server certificate for AT-TLS. We are only using Server side authentication; Client Authentication is not defined.
 - a. **RACDCERT ID(NSSD) LIST(LABEL('NSSDn at ZOSn'))**
7. View the RACF certificate that your IKED will use to identify itself to partners.
 - a. **RACDCERT ID(NSSD) LIST(LABEL('NSS Client at ZOSn'))**
8. View the RACF certificate of the Certificate Authority (CA) that signed your IKED certificate.
 - a. **RACDCERT CERTAUTH LIST(LABEL('MVSn LABS Certificate Authority'))**
9. Open the “IP Configuration Guide” manual to the “Network security services” chapter. The “Preparing to provide network security services” section details all the RACF definitions required for NSSD.
 - a. Note, samples are provided in the EZARACF member of SEZAINST.
10. All the RACF definitions have been done for you. You will issue Displays of all the RACF definitions as you review the steps in the manual.
11. “Step 1. Define and authorize the NSSD user ID.” in the manual.
 - a. **LISTUSER (NSSD) OMVS**
 - b. **RLIST STARTED NSSD.* STDATA**
12. “Step 2. Permit the NSSD user ID to SYS1.PARMLIB.” in the manual.
 - a. Skip this step because SYS1.PARMLIB is not protected on this class system.
13. “Step 3. Define key ring controls.” in the manual.
 - a. **RLIST FACILITY IRR.DIGTCERT.ADD**
 - b. **RLIST FACILITY IRR.DIGTCERT.ADDRING**
 - c. **RLIST FACILITY IRR.DIGTCERT.CONNECT**
 - d. **RLIST FACILITY IRR.DIGTCERT.GENCERTD**
 - e. **RLIST FACILITY IRR.DIGTCERT.GENREQ**
 - f. **RLIST FACILITY IRR.DIGTCERT.LIST**
 - g. **RLIST FACILITY IRR.DIGTCERT.LISTRING**

14. "Step 4. Give the user ID of the administrator that will manage the NSS server's key ring appropriate access to manage the key ring." in the manual.
 - a. **RLIST FACILITY IRR.DIGTCERT.ADD AUTHUSER**
 - b. **RLIST FACILITY IRR.DIGTCERT.ADDRING AUTHUSER**
 - c. **RLIST FACILITY IRR.DIGTCERT.CONNECT AUTHUSER**
 - d. **RLIST FACILITY IRR.DIGTCERT.GENCERTD AUTHUSER**
 - e. **RLIST FACILITY IRR.DIGTCERT.GENREQ AUTHUSER**
 - f. **RLIST FACILITY IRR.DIGTCERT.LIST AUTHUSER**
 - g. **RLIST FACILITY IRR.DIGTCERT.LISTRING AUTHUSER**
15. "Step 5. Optionally, permit the NSS server to the BPX.DAEMON FACILITY class profile." in the manual.
 - a. Skip this step because NSSD is defined with UID 0, superuser authority.
16. "Step 6. Enable the secured signon function.
 - a. **RLIST PTKTDATA NSSD**
17. "Step 7. Define SERVAUTH profiles to authorize NSS clients to network security services." and "a. Define a SAF user ID representing an NSS client to the external security manager." in the manual.
 - a. **LISTUSER (IKED) OMVS**
 - b. **RLIST STARTED IKED.* STDATA**
18. "Step 7.b. If you choose to define an NSSD profile in the APPL class with UACC(NONE), issue the following command to authorize each SAF user ID to the NSSD application." in the manual.
 - a. Skip this step because NSSD is not defined to the APPL Class.
19. "Step 7.c. Authorize the user ID associated with an NSS client for each of the network security services it will use." in the manual.
 - a. **RLIST SERVAUTH EZB.NSS.*.IKED1.IPSEC.CERT AUTHUSER**
 - b. **RLIST SERVAUTH EZB.NSS.*.IKED2.IPSEC.CERT AUTHUSER**
 - c. **RLIST SERVAUTH EZB.NSS.*.IKED3.IPSEC.CERT AUTHUSER**
 - d. **Etc.**
 - e. **RLIST SERVAUTH EZB.NSS.*.IKED1.IPSEC.NETMGMT AUTHUSER**
 - f. **RLIST SERVAUTH EZB.NSS.*.IKED2.IPSEC.NETMGMT AUTHUSER**
 - g. **RLIST SERVAUTH EZB.NSS.*.IKED3.IPSEC.NETMGMT AUTHUSER**
 - h. **Etc.**
20. "Step 7.d. Create a SERVAUTH resource profile for each NSS IPsec client certificate added to the NSS server's key ring, and give each NSS IPsec client's user ID access to the profiles created for its own certificates." in the manual.
 - a. **RLIST SERVAUTH EZB.NSSCERT.*.NSS\$CLIENT\$AT\$ZOS1.HOST AUTHUSER**
 - b. **RLIST SERVAUTH EZB.NSSCERT.*.NSS\$CLIENT\$AT\$ZOS2.HOST AUTHUSER**
 - c. **RLIST SERVAUTH EZB.NSSCERT.*.NSS\$CLIENT\$AT\$ZOS3.HOST AUTHUSER**
 - d. **Etc.**
21. "Step 7.e. Create a SERVAUTH resource profile for each certificate authority (CA) certificate that could be used by an NSS IPsec client, and give the NSS client's user ID access to the profiles." in the manual.
 - a. **RLIST SERVAUTH EZB.NSSCERT.*.MVS1\$LABS\$CERTIFICATE\$AUTHORITY.CERTAUTH AUTHUSER**
 - b. **RLIST SERVAUTH EZB.NSSCERT.*.MVS2\$LABS\$CERTIFICATE\$AUTHORITY.CERTAUTH AUTHUSER**
 - c. **RLIST SERVAUTH EZB.NSSCERT.*.MVS3\$LABS\$CERTIFICATE\$AUTHORITY.CERTAUTH AUTHUSER**
 - d. **Etc.**

22. “Step 7.f. Create a SERVAUTH resource profile for each certificate that an NSS XMLAppliance client could retrieve and give the user ID of the NSS XMLAppliance client access to the appropriate profiles.” in the manual.
 - a. Skip this step because we are not implementing XMLAppliance support.
23. “Step 7.g. Create a SERVAUTH resource profile for the private key of each certificate to which an NSS XMLAppliance client requires access and give the user ID of the NSS XMLAppliance client access to the profiles.” in the manual.
 - a. Skip this step because we are not implementing XMLAppliance support.
24. “Step 7.h. Create the following SERVAUTH profiles to enable users to remotely monitor (IPSEC.DISPLAY) or manage (IPSEC.CONTROL) NSS clients.” in the manual.
 - a. `RLIST SERVAUTH EZB.NETMGMT.*.IKED1.IPSEC.DISPLAY AUTHUSER`
 - b. `RLIST SERVAUTH EZB.NETMGMT.*.IKED2.IPSEC.DISPLAY AUTHUSER`
 - c. `RLIST SERVAUTH EZB.NETMGMT.*.IKED3.IPSEC.DISPLAY AUTHUSER`
 - d. `Etc.`
 - e. `RLIST SERVAUTH EZB.NETMGMT.*.IKED1.IPSEC.CONTROL AUTHUSER`
 - f. `RLIST SERVAUTH EZB.NETMGMT.*.IKED2.IPSEC.CONTROL AUTHUSER`
 - g. `RLIST SERVAUTH EZB.NETMGMT.*.IKED3.IPSEC.CONTROL AUTHUSER`
 - h. `Etc.`
25. “Step 8. If you are using the NSS XMLAppliance private key service with ICSF-protected private keys, authorize the NSS server to the Integrated Cryptographic Service Facility (ICSF).” in the manual.
 - a. Skip this step because we are not implementing XMLAppliance support.
26. “Step 9. If XMLAppliance clients using the SAF access service are using certificates for access checks, enable RACF certificate name filtering.” in the manual.
 - a. Skip this step because we are not implementing XMLAppliance support.
27. “Step 10. The NSSD uses ICSF callable services for ECDSA digital signature support.” in the manual.
 - a. Skip this step because we are not going to use ECDSA support.

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.

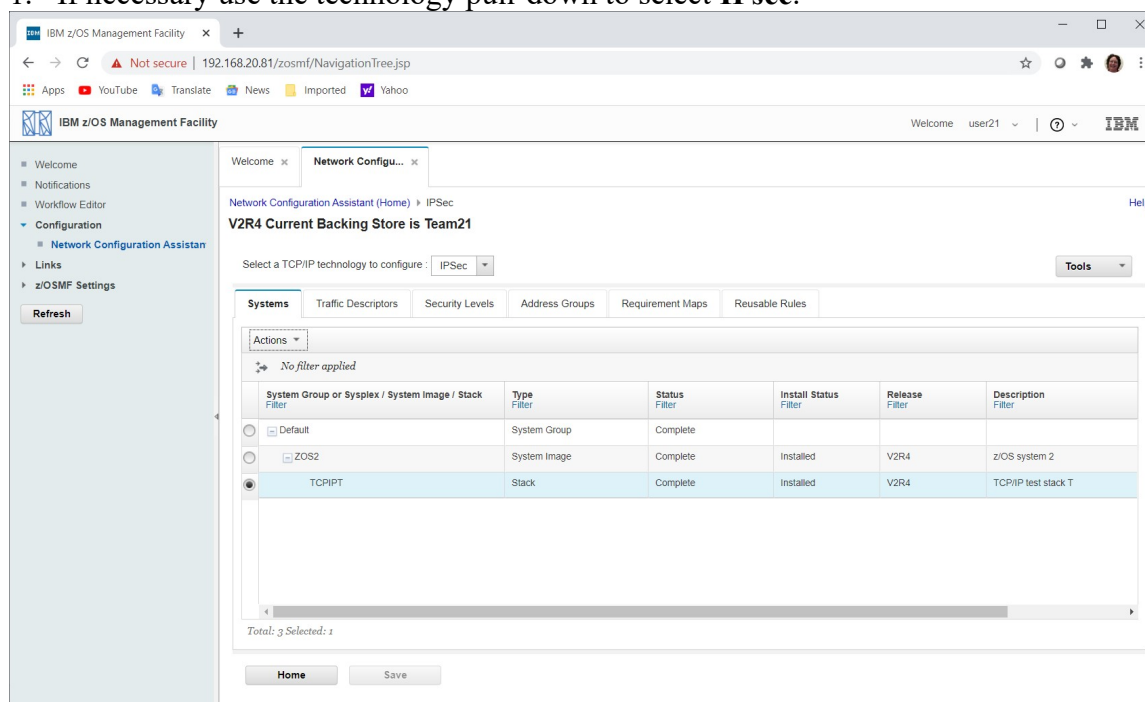
Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1

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

Select IKEv2 for IPsec

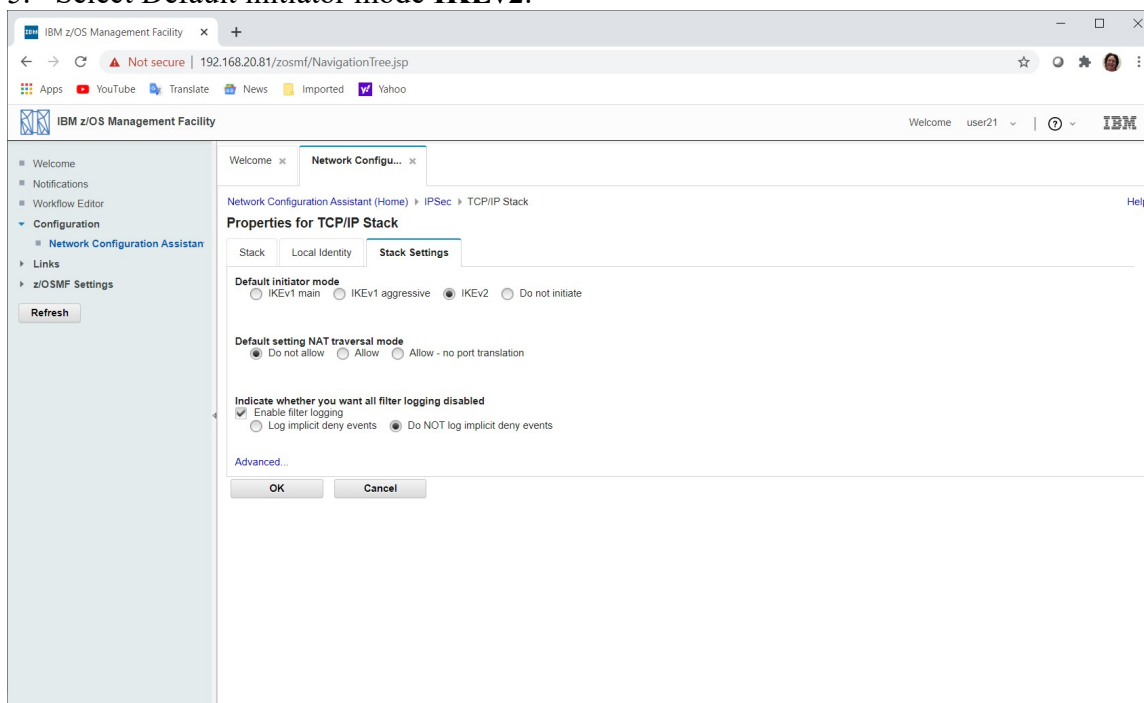
1. If necessary use the technology pull-down to select **IPsec**.



2. Use the radio button beside the **TCPIPT** stack under your **ZOSn** image.

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

3. Use the **Actions** pull-down to select **Properties...**
4. Select **Stack Settings** tab.
5. Select Default initiator mode **IKEv2**.



6. **OK.**

Create IP Filter Policy for AT-TLS Connection

The NSS Clients connect to the NSSD server using AT-TLS. First you will add to an existing IP Filter policy to “permit” the traffic, and then you will create the AT-TLS policy to protect the traffic.

1. If necessary use the technology pull-down to select **IPsec**.
2. Use the radio button beside the **TCPIPT** stack under your **ZOSn** image.
3. Use the **Actions** pull-down to select **Rules...**
4. Note there is already a rule, **CommonTraffic**, between **All_IPv4_Addresses** on both sides, that uses Requirement Map **BasicServices**. You just need to add the NSS traffic to that Requirement Map.
5. **Close**
6. Select the **Requirment Maps** tab.
7. Select the **BasicServices** Requirement Map.
8. Use the **Actions** pull-down to select **Modify...**
9. Use the **Actions** pull-down to select **Add Row...** twice.
10. Scroll to the bottom to locate the newly added rows.
 - a. Use the pull-down for the second to last Traffic Descriptor field to select **NSS_Client**.
 - b. Use the pull-down for the last Traffic Descriptor to select **NSS_Server**.
 - c. Use the Security Level pull-down for both rows to select **Permit**.
11. Click on **OK** button.
12. Click on **Proceed** button when Modify Requirement Map panel appears.
13. Click on **OK** button when the Information panel appears.
14. **Save, OK**.
15. Click on the **Systems** tab.

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

16. Use what you have learned previously to send your new policy file to your ZOSn image.

IBM z/OS Management Facility

Welcome user21 | ? IBM

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

Install File for Default.ZOS2.TCPIPT

* Install file name: /u/user21/TMZ1_IPSecVPN_wiKeyv2.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)

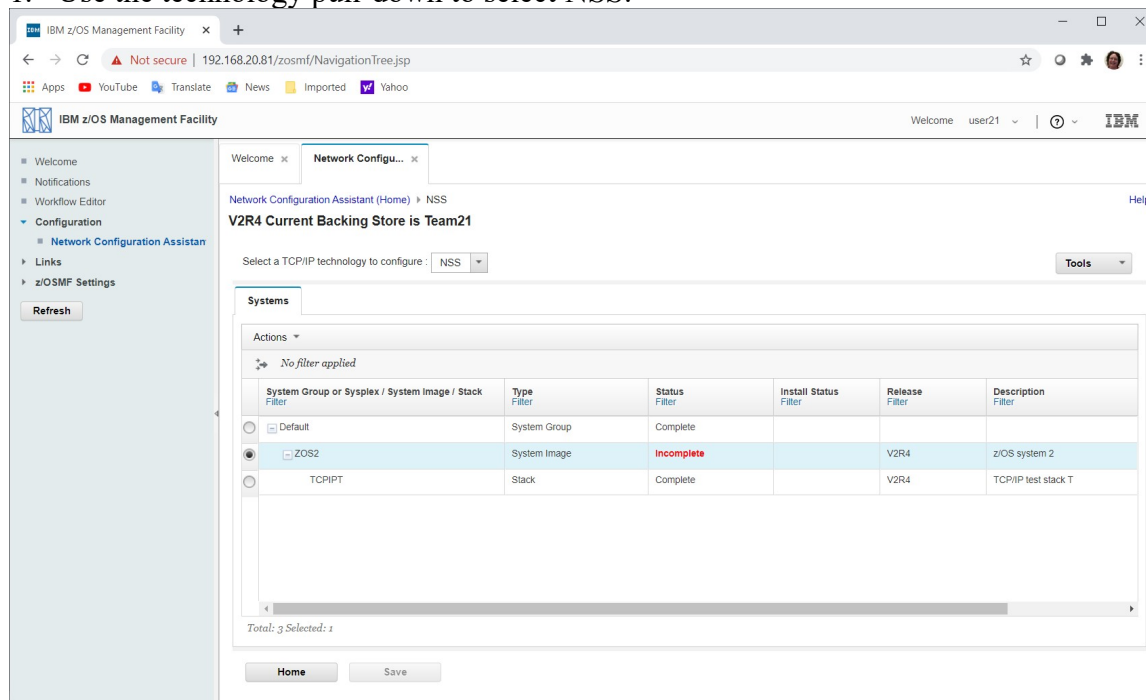
Selecting the GO button may do an automatic save of backing store before the install, based on your preference setting.

Go Close View FTP Log

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

Create NSSD Configuration File

1. Use the technology pull-down to select NSS.



2. Use the radio button to select your z/OS image **ZOSn**.

3. Use the **Actions** pull-down to select **Properties...**

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

4. Click on the **Server** tab.

IBM z/OS Management Facility

Welcome user21

Network Configuration Assistant (Home) > NSS > z/OS System Image Default.ZOS2

Properties for z/OS System Image Default.ZOS2

Name: **Server** | IPsec client

☒ This system image will be an NSS server

* Port number to listen for NSS clients: 4159

* Key ring name for the client certificates: NSSD/NSSDnRing

☒ Permit and protect NSS traffic with AT-TLS

* AT-TLS key ring: NSSD/NSSD2Ring

* Server host name or IP address: 192.168.20.92

Server identity

☐ * IP Address

☐ * Fully qualified domain name(FQDN):

☒ * User ID @ FQDN: NSSD2@WSC.LABS.IBM.CO

☐ * X.500 distinguished name:

Advanced... Show Clients

OK Cancel

5. Select check box for **“This system image will be an NSS server”**.
6. Fill in Key ring name for the client certificates **NSSD/NSSDnRing**.
7. Fill in AT-TLS key ring **NSSD/NSSDnRing**.
 - a. You could use a different key ring for AT-TLS but you don’t have to.
8. Fill in Server host name or IP address **192.168.20.9n**.
9. Select Server identity **User ID @ FQDN**.
 - a. Fill in **NSSDn@WSC.LABS.IBM.COM**.

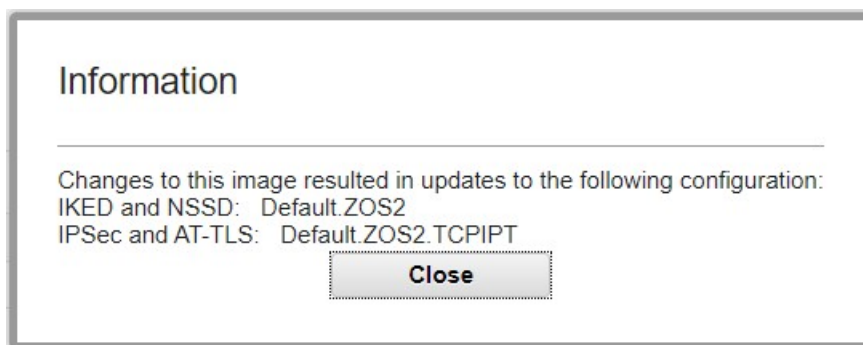
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

10. Select the **IPsec client** tab.

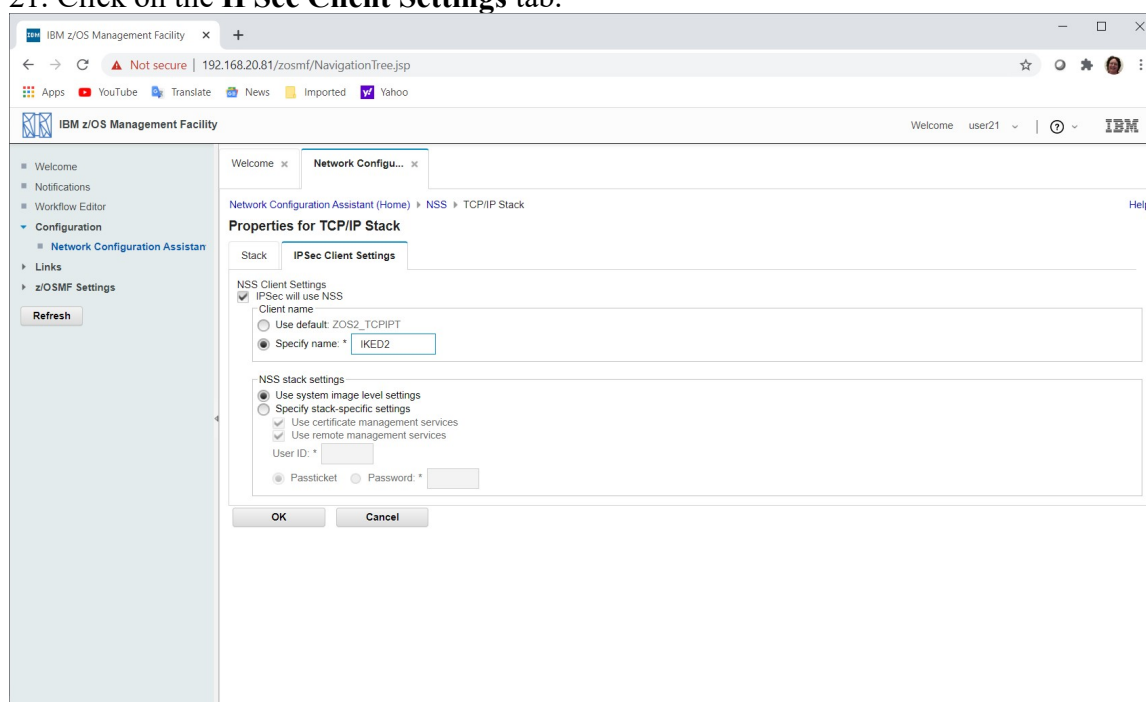
The screenshot shows the IBM z/OS Management Facility interface. The left sidebar contains a navigation menu with options like Welcome, Notifications, Workflow Editor, Configuration, Network Configuration Assistant, Links, and z/OSMF Settings. The main area displays the 'Network Configuration Assistant (Home)' with a breadcrumb trail: 'NSS > z/OS System Image'. The title is 'Properties for z/OS System Image Default.ZOS2'. There are three tabs: 'Name', 'Server', and 'IPSec client', with the 'IPSec client' tab selected. The configuration options include: a checked checkbox 'This system image will be an IPsec client of an NSS server'; 'Primary server' set to 'Default.ZOS2' and 'Backup server' set to 'Select a server from the list'; checked checkboxes for 'Use certificate management service' and 'Use remote management service'; 'User ID' set to 'IKED'; 'Select the login credential choice' with 'Use passticket' selected; a checked checkbox 'Permit and protect NSS traffic with AT-TLS'; and 'AT-TLS key ring' set to '*AUTH/*'. At the bottom are 'OK' and 'Cancel' buttons.

11. Select the check box beside **This image will be an IPsec client of an NSS server.**
12. Use the Primary server pull-down for **Select a server from the list.**
 - a. Select your **ZOSn** server which is the only NSS server in the list.
13. Select **Use certificate management service** and **Use remote management service.**
 - a. Certificate Management Service allows you to manage certificates for NSS Client IKED servers.
 - b. Remote Management Service allows you to manage IPsec connections to NSS Client IKED servers via ipsec commands to the NSSD server.
14. Enter the User ID associated with the NSS Client IKED server which is **IKED**.
15. Select **Use passticket** for login credential choice.
 - a. For additional information about using a PassTicket, see z/OS Security Server RACF Security Administrator's Guide.
16. Since we are implementing AT-TLS with Server Authentication only we do not need a client key ring and can instead use a virtual key ring ***AUTH/***
17. Click on the **OK** button.

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

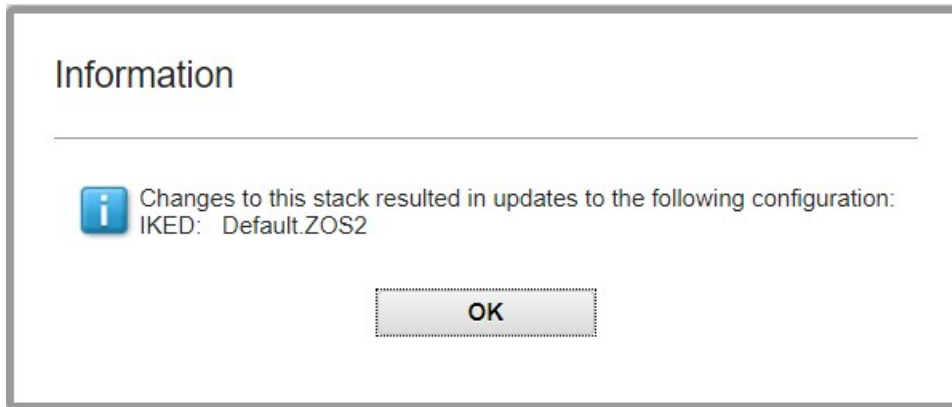


18. Click on **Close** button.
19. Select the **TCPIPT** stack under your **ZOSn** image.
20. Use the **Actions** pull-down to select **Properties...**
21. Click on the **IPSec Client Settings** tab.



22. Use the radio button to select **Specify name** and enter your systems Client name **IKEDn**.
23. **OK**

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



24. **OK, Save, OK.**
25. Use the radio button to select the your ZOSn image.
26. Use the **Actions** pull-down to select **Install Configuration Files...**
27. Select your team (ZOSn) **IKED – Configuration** and use the **Actions** pull-down to select **Install...**

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

28. Fill in the Install file name `/u/usernx/iked-nss-client.conf`.

IBM z/OS Management Facility

Welcome user21

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

Install File for Default.ZOS2

* Install file name:

Installation method
☒ FTP

FTP information

* Host name:

* Port number:

User ID: ☒ 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.

29. Go, OK, OK, Close.

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

30. Select **NSSD – Configuration** and use the **Actions** pull-down to select **Install...**

31. Fill in the Install file name **/u/usernx/nssd.conf**.

IBM z/OS Management Facility

Welcome user21 | ? IBM

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

Install File for Default.ZOS2

* Install file name: /u/user21/nssd.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

32. Go, OK, OK, Close, Close.

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

Create AT-TLS Policy

1. Move to the **AT-TLS** technology.
2. Select your **TCPIPT** stack under your **ZOSn** image.
3. Use the **Actions** pull-down to select **Rules...**
4. Select the **Default_NSS_Server**.
5. Use the **Actions** pull-down to select **Copy...**

IBM z/OS Management Facility

Welcome user21

Network Configuration Assistant (Home) > AT-TLS > TCPIPT Stack > Connectivity Rule

Copy Connectivity Rule

Default AT-TLS key ring database

* Rule name: ☒ Enable rule [Restore Defaults](#)

Traffic Role Key Ring Data Endpoints Security Level Advanced

Use this panel to specify the traffic settings.

* Application name:

Local Port: ☐ All ports ☐ All ephemeral ports ☒ Ports: Separate multiple ports with a comma

Remote Port: ☐ All ports ☒ All ephemeral ports ☐ Ports: Separate multiple ports with a comma

Indicate the TCP connect direction: ☐ Either ☒ Inbound only ☐ Outbound only

Specify jobname and user ID: Jobname: User ID:

OK Cancel

6. Select the check box beside **Enable rule**.
7. Change the Rule name to **NSS_Server**.
8. Enter Application name **NSSD**.

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

9. Select the **Key Ring** tab.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NSA) interface. The browser address bar indicates the URL is 192.168.20.81/zosmf/NavigationTree.jsp. The left sidebar contains a navigation menu with options: Welcome, Notifications, Workflow Editor, Configuration (selected), Network Configuration Assistant (selected), Links, and z/OSMF Settings. The main content area is titled 'Copy Connectivity Rule' and shows the 'Key Ring' tab selected. The 'Rule name' is 'NSS_Server' and the 'Enable rule' checkbox is checked. The 'Key Ring' tab is active, showing a section for 'Default AT-TLS key ring database'. The 'Simple name' radio button is selected, and the 'Key ring' field contains 'NSSD/NSSD2Ring'. The 'Key database is a z/OS UNIX file system file' radio button is also selected, with the 'Key database' field empty. The 'Certificate label' field is empty. A note at the bottom states: 'Specified server certificate labels to be used by server to accommodate clients with different types of public keys. The certificates are available beginning with V2R3.'

10. Use the radio button to select **Simple name** and enter key ring name **NSSD/NSSDnRing**.

11. OK.

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

12. Select the **Default_NSS_Client-IKED**.

13. Use the **Actions** pull-down to select **Copy...**

The screenshot shows the IBM z/OS Management Facility interface. The left sidebar contains navigation links: Welcome, Notifications, Workflow Editor, Configuration (selected), Network Configuration Assistant, Links, and z/OSMF Settings. The main content area is titled 'Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule'. Below this, the 'Copy Connectivity Rule' dialog is open. It features a 'Default AT-TLS key ring database' section with a text input for 'Rule name' set to 'NSS_Client-IKED' and a checked 'Enable rule' checkbox. Below this is a tabbed interface with 'Traffic' selected. The 'Traffic' tab contains instructions to specify traffic settings, an 'Application name' input set to 'NSS-Client', and sections for 'Local Port' and 'Remote Port'. Both sections have radio buttons for 'All ports', 'All ephemeral ports', and 'Ports'. The 'Ports' option is selected in both, with input fields showing '*' and '4159'. There are also checkboxes for 'Indicate the TCP connect direction' (Inbound only, Outbound only) and 'Specify jobname and user ID' (Jobname, User ID). At the bottom are 'OK' and 'Cancel' buttons.

14. Select the check box beside **Enable rule**.

15. Change the Rule name to **NSS_Client-IKED**.

16. Enter Application name **NSS-Client**.

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

17. Select the **Key Ring** tab.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The browser address bar shows the URL 192.168.20.81/zosmf/NavigationTree.jsp. The left sidebar contains a navigation menu with options: Welcome, Notifications, Workflow Editor, Configuration (selected), Network Configuration Assistant (selected), Links, and z/OSMF Settings. The main content area is titled 'Copy Connectivity Rule' and shows the 'Key Ring' tab selected. The 'Rule name' is 'NSS_Client-IKED' and the 'Enable rule' checkbox is checked. The 'Key Ring' tab is active, showing a section for specifying the key ring database and certificate label. The 'Default AT-TLS key ring database' section has two radio buttons: 'Use the key ring database defined for the z/OS system image' (selected) and 'Simple name (as in an SAF product or in PKCS #11 token format)'. The 'Key ring' field is set to '*AUTH/*'. Below this, there are fields for 'Key database', 'Key database stash file', and 'Key database password'. The 'Certificate label' field is empty. A note at the bottom states: 'Specified server certificate labels to be used by server to accommodate clients with different types of public keys. The certificates are available beginning with V2R3.'

18. Use the radio button to select **Simple name** and enter key ring name ***AUTH/***

19. **OK, Close, Save, OK.**

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

20. Use what you have learned previously to send your new policy file to your ZOSn image. Don't update pagentt.conf yet.

IBM z/OS Management Facility

Welcome user21 | ? IBM

Network Configuration Assistant (Home) > AT-TLS > Configuration Files > Install

Install File for Default.ZOS2.TCPIPT

* Install file name: /u/user21/TM21_ATTLS_wNSS.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

Part 2: Network Security Services Daemon (NSSD) and IKEv2 Testing

Check NSSD Definitions 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. Display the NSSD JCL procedure.
 - a. **=3.4**
 - b. **SYS1.PROCLIB**
 - c. View the file **NSSD**.
 - d. The proc was copied from the TCPIP sample directory SEZAINST and was not customized at all.
4. Is an environment file specified in the NSSD proc?
5. Is the NSSD configuration file specified in the NSSD proc?
6. What NSSD configuration file will be used?
7. Exit viewing the NSSD proc.
 - a. **PF3**

FTP with IKEv1

1. Go to TSO command panel.
 - a. **=6**
2. Test FTP with IKEv1.
 - a. **ftp -p TCPIPT -s 192.168.20.9n 192.168.20.91**
3. Login and then quit if you'd like or use Esc and quit.
4. View the syslogd log file.
 - a. **=O**
 - b. **4** (for OMVS)
 - c. **su**
 - d. **obrowse /var/CSLOG/ipsec.log**
5. Go to the bottom of the file and search for the previous IKE version message.
 - a. **F EZD1775I prev**
 - i. EZD1775I IKE version 1.0 security association...
6. Exit out of syslogd log file.
 - a. **PF3**

Test NSSD and IKEv2

1. Edit `/u/usernx/pagentt.conf`
2. Change IPSec policy to the file name that you gave your file when you sent it to z/OS from the tool, ie. `/u/usernx/TMnx_IPSecVPN_wIKEv2.policy`
3. Change AT-TLS policy to the file name that you gave your file when you sent it to z/OS, ie. `/u/usernx/TMnx_ATTLS_wNSS.policy`
4. Copy configuration files to usage locations.
 - a. `cp pagentt.conf /etc/PAGT1/pagentt.conf`
 - b. `cp iked-nss-client.conf /etc/security/iked.conf`
 - c. `cp nssd.conf /etc/security/nssd.conf`
5. Exit out of OMVS.
 - a. `exit,exit, Enter.`
6. Go to log and take down IKED.
 - a. `=D.LOG`
 - b. `/P IKED`
7. Pick up your new policy file.
 - a. `/F PAGENTT,UPDATE`
8. Bring up NSSD and IKED.
 - a. `/S NSSD`
 - b. `/S IKED`
9. Go to TSO command panel.
 - a. `=6`
10. Test FTP with IKEv1.
 - a. `ftp -p TCPIPT -s 192.168.20.9n 192.168.20.91`
11. Login to this FTP session and leave it up.
12. Bring up another PComm session to your ZOSn system. You may click on File and then Run the same. Login using a different user ID on your ZOS (`usern1`, `usern2`, or `usern3`).
13. View the syslogd log file.
 - a. `ISPF`
 - b. `=O`
 - c. `4` (for OMVS)
 - d. `su`
 - e. `obrowse /var/CSLOG/ipsec.log`
14. Go to the bottom of the file and search for the previous IKE version message.
 - a. `F EZD1775I prev`
 - i. `EZD1775I IKE version 2.0 security association...`
15. Exit out of syslogd log file.
 - a. `PF3`
16. Display your NSS Client currently connected to your NSSD server.
 - a. `nssctl -d`
 - b. Example:
`# nssctl -d`
`CS V2R1 nssctl SystemName: MVS2 Mon Apr 27 21:57:10 2015`

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

```
Function: Display      NSSClientName: n/a
ClientName:           IKED2
ClientAPIVersion:     4
StackName:           TCPIPT
SystemName:           MVS2
ClientIPAddress:      192.168.20.102
ClientPort:           4913
ServerIPAddress:      192.168.20.92
ServerPort:           4159
UserID:               IKED
ConnectState:         connected
TimeConnected:        2015/04/27 21:55:02
TimeOfLastMessageFromClient: 2015/04/27 21:55:23
Discipline:           IPSec
CertificateServiceSelected: Yes
CertificateServiceEnabled: Yes
RemoteManagementSelected: Yes
RemoteManagementEnabled: Yes
*****
```

1 entries selected

#

17. Another way to display client.

a. **ipsec -x display -z IKEDn**

b. Example:

```
# ipsec -x display -z IKED2
CS V2R1 ipsec NSS Client Name: IKED2 Mon Apr 27 20:49:00 2015
Primary: NSS Server Function: Display Format: Detail
Source: Server Scope: n/a TotAvail: 1
SystemName: MVS2
ClientName:           IKED2
ClientAPIVersion:     4
StackName:           TCPIPT
SystemName:           MVS2
ClientIPAddress:      192.168.20.102
ClientPort:           4910
ServerIPAddress:      192.168.20.92
ServerPort:           4159
UserID:               IKED
RemoteManagementSelected: Yes
RemoteManagementEnabled: Yes
CertificateServicesSelected: Yes
CertificateServicesEnabled: Yes
ConnectState:         connected
TimeConnected:        2015/04/27 20:31:26
TimeOfLastMessageFromClient: 2015/04/27 20:32:08
*****
```

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

1 entries selected

#

18. Display the active IPsec VPN tunnel.

a. **ipsec -y display -z IKEDn**

b. Example:

```
# ipsec -y display -z IKED2
```

```
CS V2R1 ipsec NSS Client Name: IKED2 Mon Apr 27 21:19:55 2015
```

```
Primary: Dynamic tunnel Function: Display Format: Detail
```

```
Source: Stack Scope: Current TotAvail: 1
```

```
TunnelID: Y2
```

```
Generation: 1
```

```
IKEVersion: 2.0
```

```
ParentIKETunnelID: K1
```

```
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: 66288408 (0x 3F37B18)
```

```
AuthOutboundSpi: 586633325 (0x22F7506D)
```

```
HowToEncrypt: 3DES-CBC
```

```
KeyLength: n/a
```

```
EncryptInboundSpi: 66288408 (0x 3F37B18)
```

```
EncryptOutboundSpi: 586633325 (0x22F7506D)
```

```
Protocol: TCP(6)
```

```
LocalPort: 1024
```

```
LocalPortRange: 65535
```

```
RemotePort: 21
```

```
RemotePortRange: n/a
```

```
Type: n/a
```

```
TypeRange: n/a
```

```
Code: n/a
```

```
CodeRange: n/a
```

```
OutboundPackets: 45
```

```
OutboundBytes: 1631
```

```
InboundPackets: 34
```

```
InboundBytes: 2266
```

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

Lifeseize: 0K
LifeseizeRefresh: 0K
CurrentByteCount: 0b
LifetimeRefresh: 2015/04/28 04:17:59
LifetimeExpires: 2015/04/28 04:32:08
CurrentTime: 2015/04/27 21:19:55
VPNLifeExpires: 2015/04/28 20:32:08
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
#

19. You may logoff both PComm sessions.

End of NSSD LAB

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

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

