

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

"Building Secure FTP Policies with IBM z/OS Configuration Assistant"

Hands-on Lab Guide

(AT-TLS Exercises with Workshop X.509 Certificates)



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

Revision date -

Saturday, 21 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.

Table of Contents

Part 0: Lab Description (Configuring Policy Agent for AT-TLS and FTP).....	4
Part 1: Configuring an FTP TLS Policy with z/OS Configuration Assistant	6
Getting Started: The z/OS IBM Configuration Assistant on MVS1.....	6
Installing the files for ZOSn on the Mainframe.....	33
Part 2: Enabling the TCP/IP Stack for AT-TLS	41
Part 3: Testing the TCP/IP Stack and FTP with AT-TLS.....	49
End of AT-TLS FTP Lab.....	56

Part 0: Lab Description (Configuring Policy Agent for AT-TLS and FTP)

Each student ZOS (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 ZOS until you have finished building your own student TCP/IP stacks and procedures. You 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.

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. Please review the lab diagram above.

LEGEND for the TEAM Number:

TEAM_nx, where “n” represents your ZOS suffix and “x” represents your userid suffix. EXAMPLE: TEAM5₃ means ZOS5 and USERID of USER₃.

As the diagram above shows, you will configure a policy that allows you to be a Secure FTP Server on your MVS (MVS2, MVS3, MVS4, MVS5, MVS6, MVS7, MVS8, MVS9). You will become a Secure FTP Client on MVS1 in order to test your FTP Server AT-TLS policy.

You will use the z/OSMF IBM Network Configuration Assistant that is installed on **MVS1** to configure an AT-TLS policy for a Secure FTP Server. The FTP Server (FTPT) owns a Server Certificate that resides on a RACF Key ring named “ServerRing1.” The RACF Key ring also contains a copy of the Certificate Authority Certificate that has signed both the Server Certificate and the Client Certificate.

The RACF Key ring is owned by a userid named FTPD, although the FTPT server’s OMVS segment is associated with the userid named “TCPIP.” This fact has implications for how you define the Server Key Ring when you create your AT-TLS policy for this server

As the diagram shows, you will also configure a policy that allows you to be a Secure FTP Client on your MVS (MVS2, MVS3, MVS4, MVS5, MVS6, MVS7, MVS8, MVS9).

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

Concurrent with your configuration of a Secure FTP Server policy, you will configure a Secure FTP Client policy for the system depicted on the right-hand side of the diagram. You will use the z/OSMF IBM Configuration Assistant that is installed on MVS1 to configure this client policy. The policy will be valid for ANY client whose USERID is represented with a wildcard of "USER*".

Each Secure FTP Client owns its own Key ring named "LabClientRing." The LabClientRing contains a copy of the Client Certificate that your USERID owns, a copy of the private key belonging to your userid, and a copy of the Certificate Authority Certificate that has signed both the Client Certificate and the Server Certificate.

You will ftp the Secure FTP Server and the Secure FTP Client policies into the MVS assigned to you using the non-secured FTP server named **FTPCCL(1)**. You will initialize FTPT(1), the Secure FTP Server on your MVS. You will become a Secure FTP Client on MVS1 -- the control MVS-- in order to test your Secure FTP Server policy. When you are ready to test your Secure FTP Client, you will sign onto your MVS system and test your Secure FTP Client policy by ftp'ing to FTPT(1) on MVS1.

The lab is divided into several sections:

- ***Part 1: Configuring an FTP TLS Policy with z/OS Configuration Assistant.***
 - *You are creating policies for both Server and Client Authentication.*
 - *Your policy points to valid x.509 certificates that have already been built for you. (In a later lab, you create the certificates for testing.)*
- ***Part 2: Enabling the TCP/IP stack for AT-TLS.***
 - *Verifying RACF prerequisites for AT-TLS*
- ***Part 3: Testing Secure FTP with AT-TLS using clients and servers on MVS1 and your assigned MVS.***
 - *Testing with Instructor versions of FTP.DATA files*
 - *Testing with Student versions of FTP.DATA files*

Part 1: Configuring an FTP TLS Policy with z/OS Configuration Assistant

Getting Started: The z/OS IBM Configuration Assistant on MVS1

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.

1. Open a Web Browser window and go to URL:
https://192.168.20.81:443/zosmf

IBM z/OS Management Facility

LEARN MORE NEED HELP?

Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe.

z/OS USER ID

z/OS PASSWORD

LOG IN

Shopz
IBM Support

z Systems Redbooks
z/OSMF home Page

WCS Flashes and Techdocs
z/OS home Page

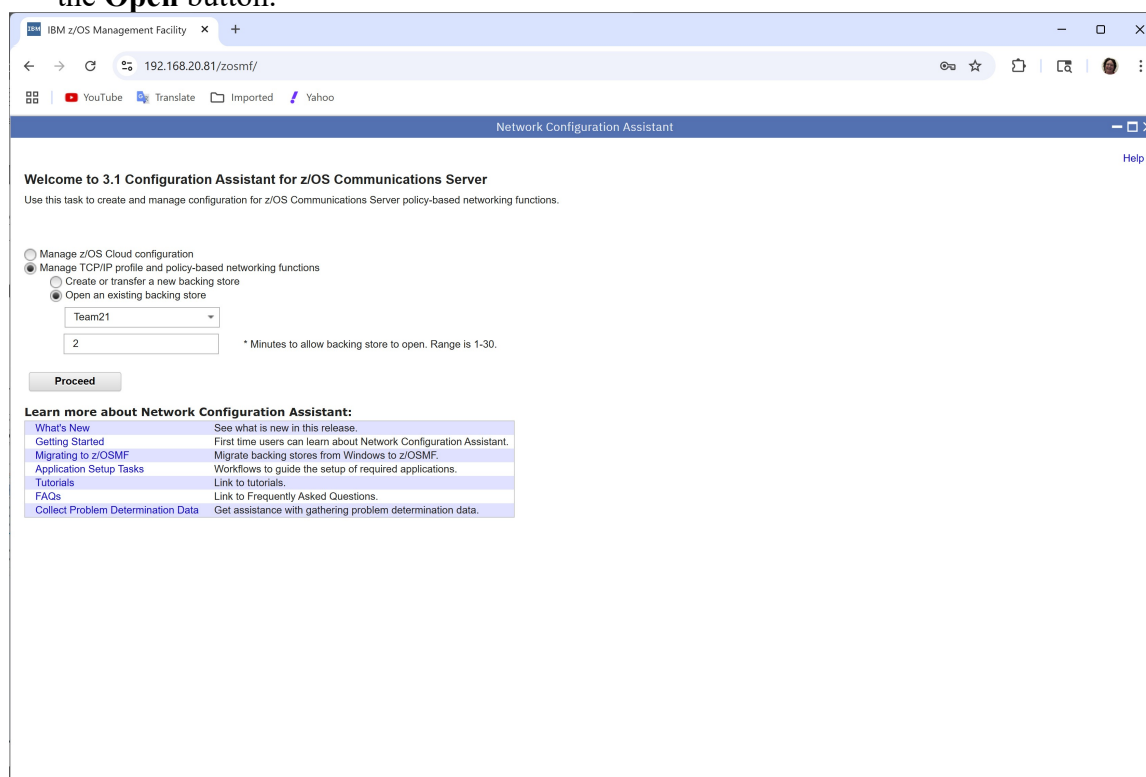
z/OS Knowledge Center

© Copyright IBM Corp. 2009.2020, Version 2.4

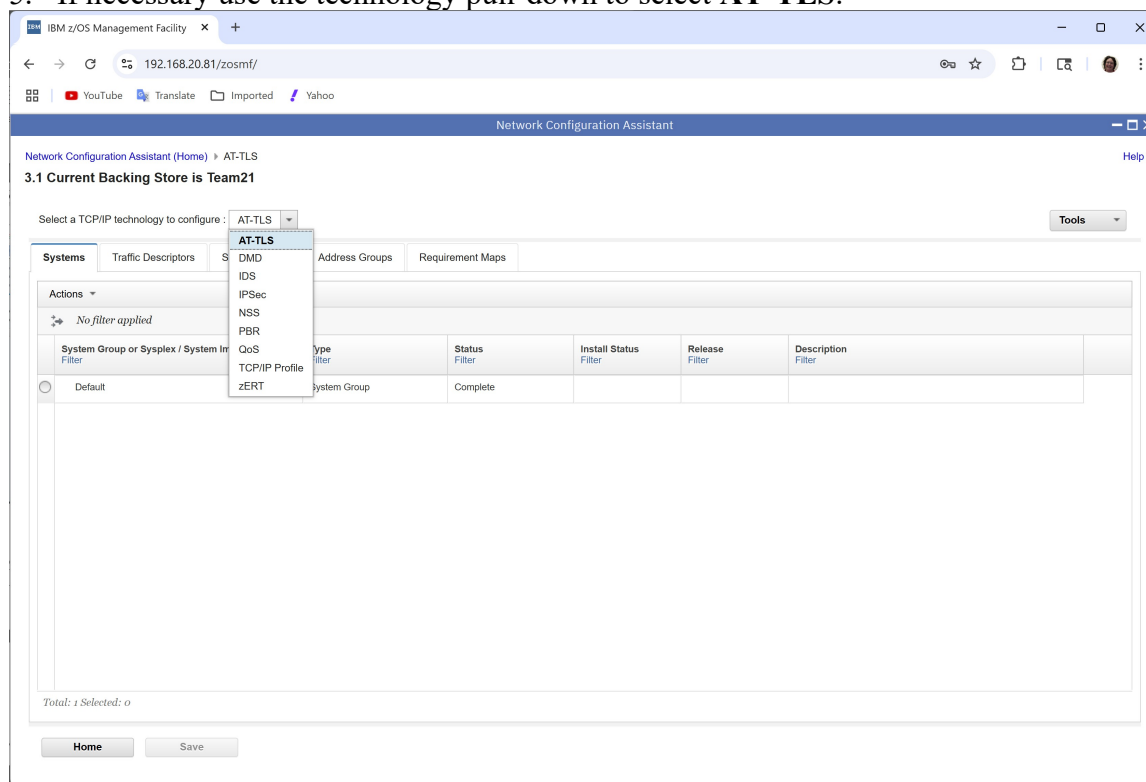
2. Logon using your Team Information Sheet to determine your z/OS User ID and password (the same ones as your TSO logon to your z/OS system).
3. Double click on the “**Network Configuration Assistant**”.

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.

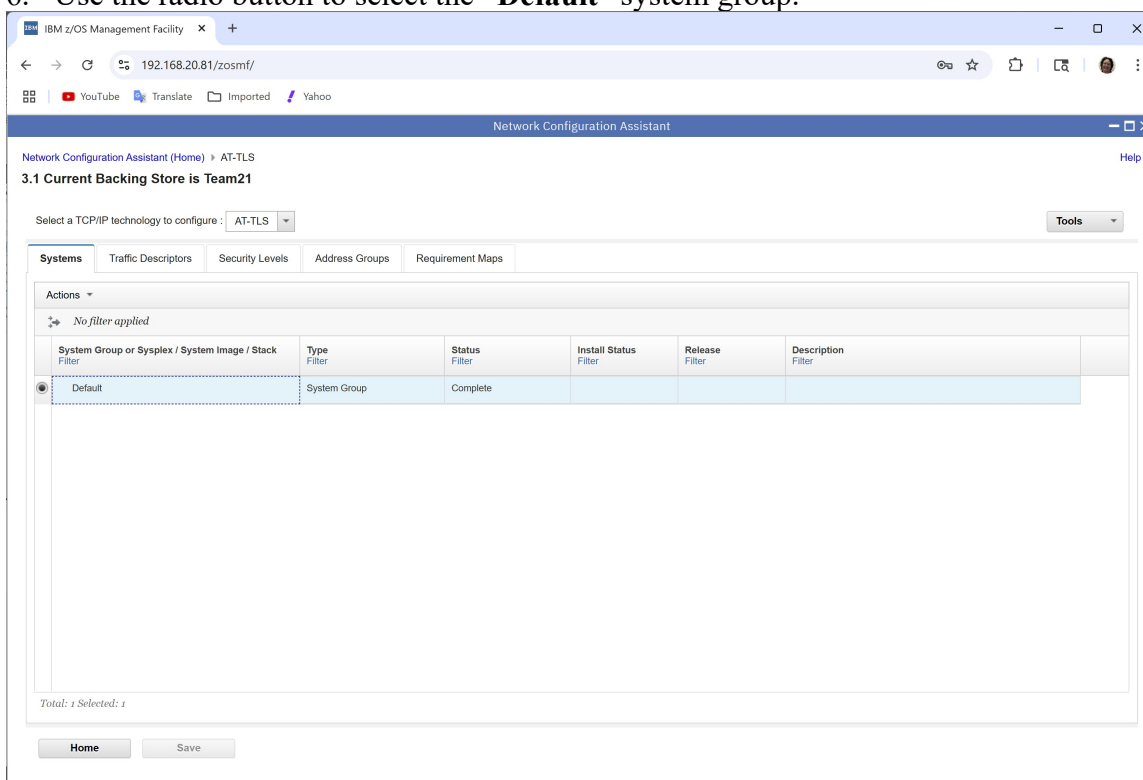


5. If necessary use the technology pull-down to select **AT-TLS**.



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

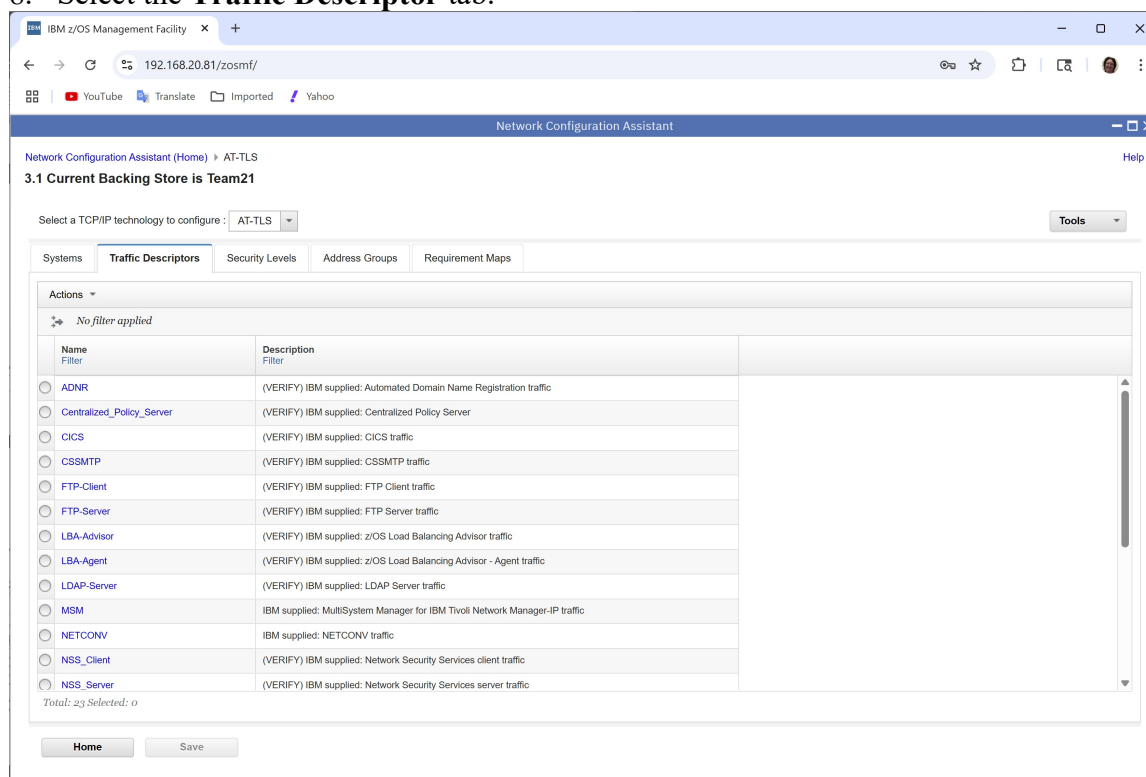
6. Use the radio button to select the “**Default**” system group.



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

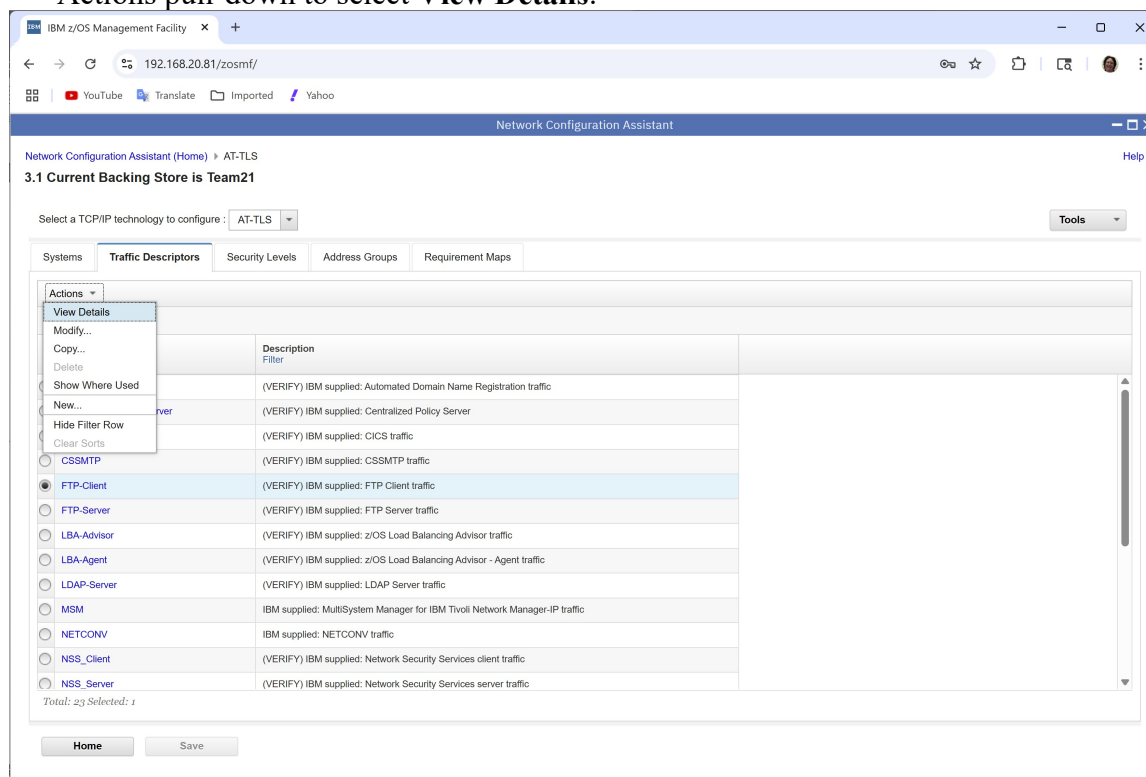
7. Before you can create a Connectivity Rule you need to create a Traffic Descriptor and a Security Level.

8. Select the **Traffic Descriptor** tab.



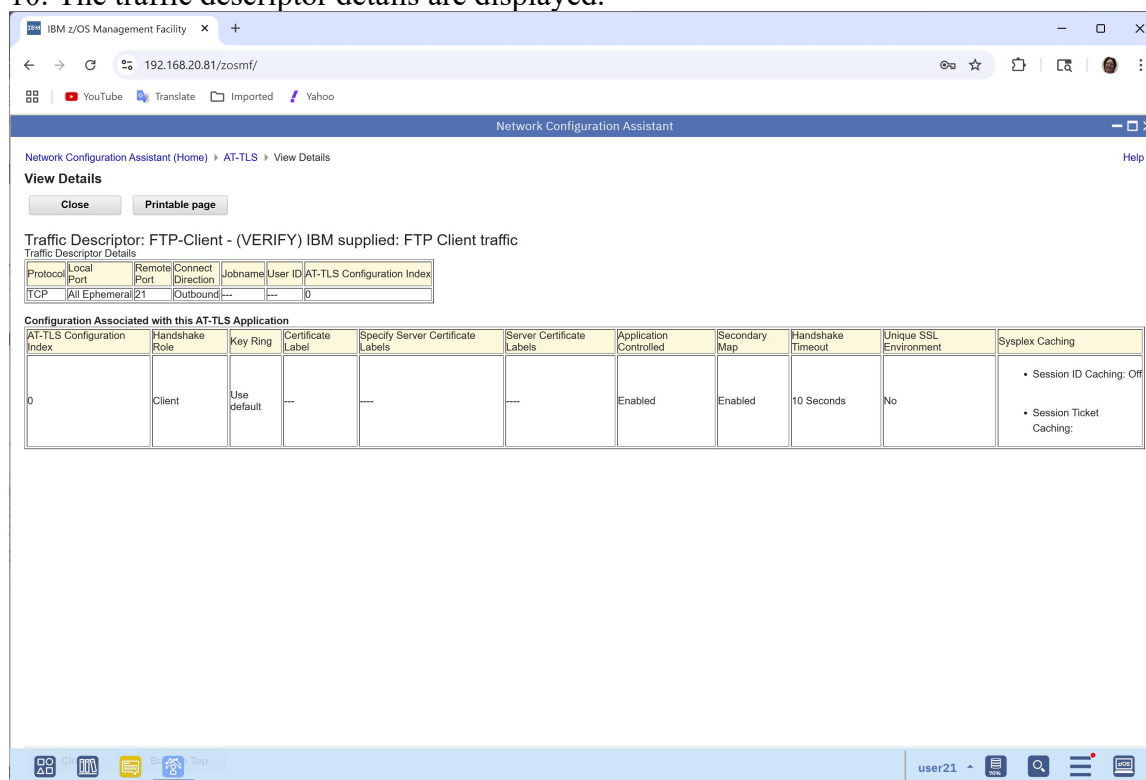
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

9. Use the radio button to select the sample FTP-Client traffic descriptor and use the Actions pull-down to select **View Details**.



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

10. The traffic descriptor details are displayed.



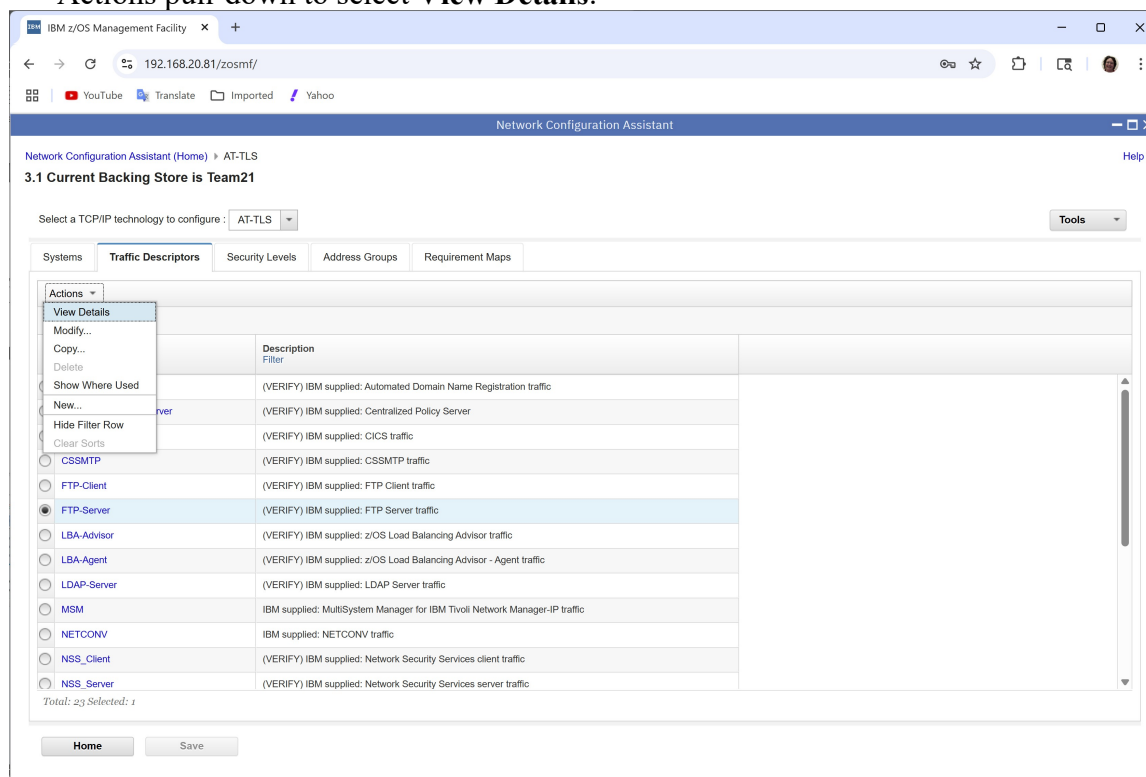
11. Notice the follow items:

- Key ring is default.
 - You need a different key ring defined.
- Outbound traffic (Connect Direction) is to remote port 21.
- Handshake Role is Client.
- The client User ID is not defined.
 - There are many different user IDs on each MVS that need separate client certificates.
- This rule does not completely suit your needs so you will need to create your own FTP Client traffic descriptor.

12. Use the **Close** button to close the View panel when you are finished reviewing the information.

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

13. Use the radio button to select the sample FTP-Server traffic descriptor and use the Actions pull-down to select **View Details**.



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

14. The traffic descriptor details are displayed.

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 main content area is titled 'View Details' and shows the 'Traffic Descriptor: FTP-Server - (VERIFY) IBM supplied: FTP Server traffic'. Below this, there is a table for 'Traffic Descriptor Details' and a table for 'Configuration Associated with this AT-TLS Application'.

Protocol	Local Port	Remote Port	Connect Direction	Jobname	User ID	AT-TLS Configuration Index
TCP	21	All Ephemeral	Inbound	---	---	0

AT-TLS Configuration Index	Handshake Role	Key Ring	Certificate Label	Specify Server Certificate Labels	Server Certificate Labels	Application Controlled	Secondary Map	Handshake Timeout	Unique SSL Environment	Sysplex Caching
0	Server	Use default	---	----	----	Enabled	Enabled	10 Seconds	No	<ul style="list-style-type: none">• Session ID Caching: Off• Session Ticket Caching:

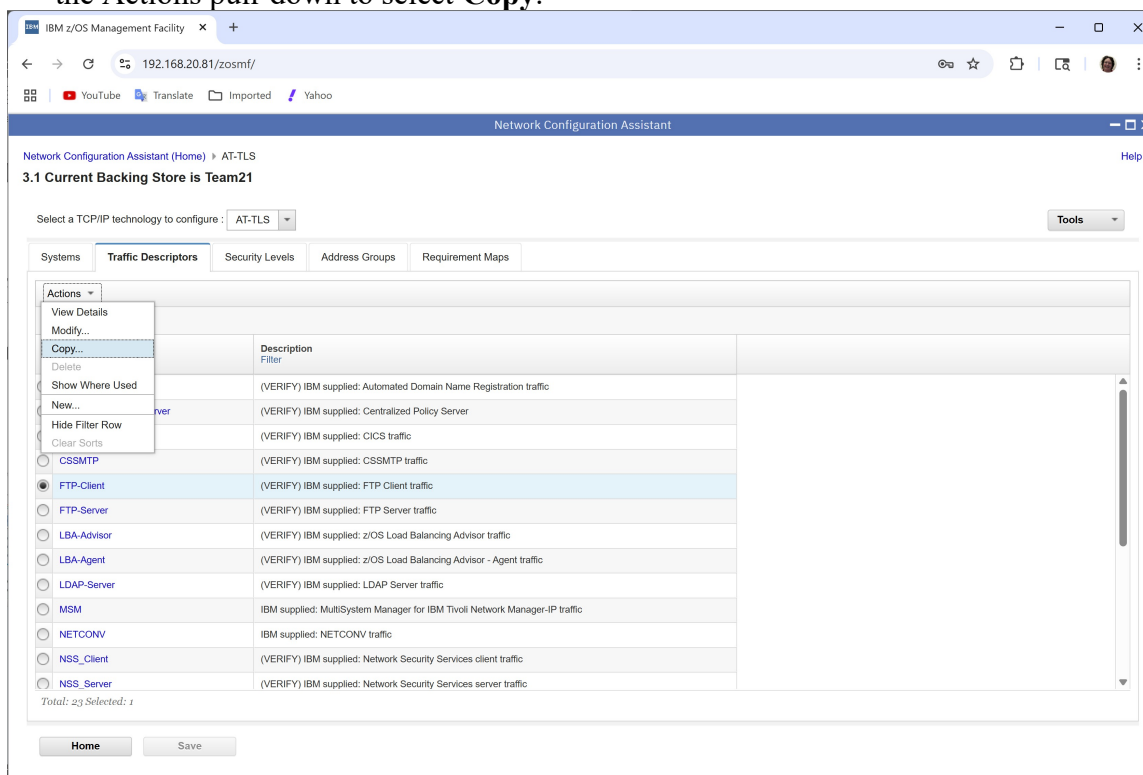
15. Notice the following items:

- Key ring is default.
- Inbound traffic is to local port 21.
- Handshake Role is Server.
 - You need Handshake Role of Server with Client Authentication Required.
- This rule does not completely suit your needs so you will need to create your own FTP Server traffic rule.

16. Use the **Close** button to close the View panel when you are finished reviewing the information.

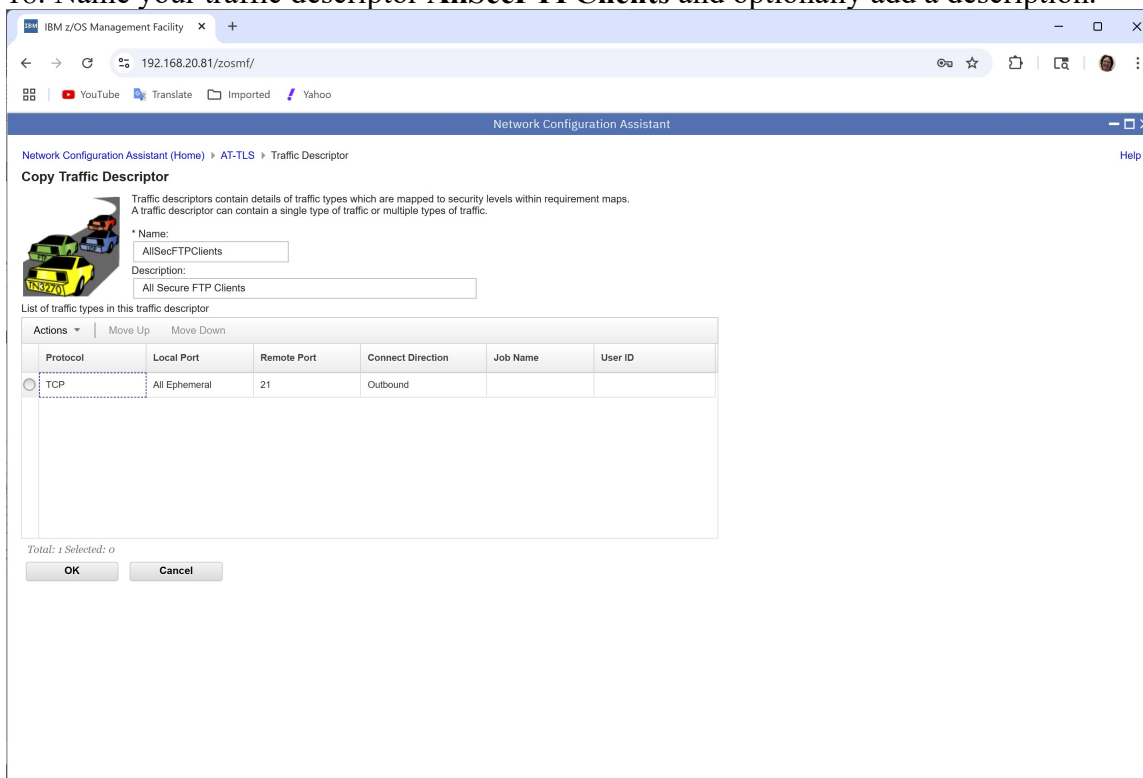
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

17. Use the radio button to select the sample FTP-Client traffic descriptor again and use the Actions pull-down to select **Copy**.



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

18. Name your traffic descriptor **AllSecFTPClients** and optionally add a description.



The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant interface. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor". The main heading is "Copy Traffic Descriptor". Below this, there is a text box for "Name:" containing "AllSecFTPClients" and a text box for "Description:" containing "All Secure FTP Clients". To the left of the text boxes is a small graphic of a yellow car. Below the text boxes is a table titled "List of traffic types in this traffic descriptor". The table has columns: Protocol, Local Port, Remote Port, Connect Direction, Job Name, and User ID. The first row is selected, showing Protocol TCP, Local Port All Ephemeral, Remote Port 21, and Connect Direction Outbound. At the bottom of the table, it says "Total: 1 Selected: 0". There are "OK" and "Cancel" buttons at the bottom of the page.

Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor

Copy Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps. A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name: AllSecFTPClients

Description: All Secure FTP Clients

List of traffic types in this traffic descriptor

Protocol	Local Port	Remote Port	Connect Direction	Job Name	User ID
<input checked="" type="radio"/> TCP	All Ephemeral	21	Outbound		

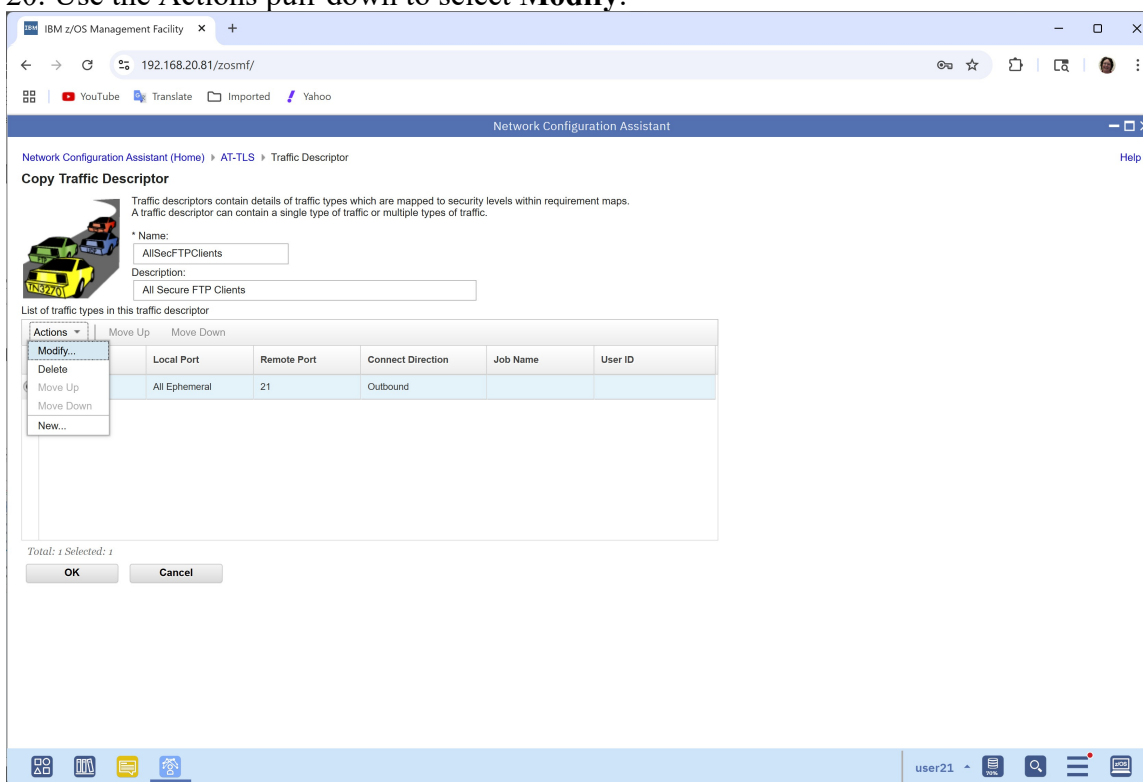
Total: 1 Selected: 0

OK Cancel

19. Use the radio button to select the only traffic type listed (Protocol TCP, Local Port All Ephemeral, Remote Port 21, Connection Direction Outbound).

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

20. Use the Actions pull-down to select **Modify**.



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

21. Specify the user ID as **USER***.

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/. The NCA window title is "Network Configuration Assistant". The breadcrumb navigation shows "Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor > Traffic Type - TCP". The main title is "Modify Traffic Type - TCP". The "Details" tab is selected, showing "Local port" and "Remote port" settings. The "Local port" section has radio buttons for "All ports", "Single port", and "Port range". The "Single port" option is selected, with the port number "100" entered. The "Remote port" section has radio buttons for "All ports", "Single port", and "Port range". The "Single port" option is selected, with the port number "21" entered. Below the port settings, there is a section for "Indicate the TCP connect direction" with radio buttons for "Either", "Inbound only", and "Outbound only". The "Outbound only" option is selected. There is a "Jobname:" field and a "User ID:" field with the value "USER*" entered. At the bottom, there is a section for "AT-TLS Handshake Role" with radio buttons for "Server" and "Client". The "Client" option is selected. The text "Client authentication role is set in the security level." is displayed below. At the bottom of the window, there are "OK" and "Cancel" buttons. The system tray at the bottom right shows the user "user21" and various system icons.

22. Technically this step is not necessary. We introduce it so that you may see that you can even create rules by filtering on USERID and not only on IP Address. This feature permits more rule granularity if such a strict rule is required.

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

23. Select the **KeyRing** tab.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant web interface. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant". The breadcrumb navigation shows "Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor > Traffic Type - TCP". The main heading is "Modify Traffic Type - TCP". There are three tabs: "Details", "KeyRing", and "Advanced". The "KeyRing" tab is selected. The page instructs the user to "Specify the key ring database to use for the traffic type specified on the Details tab." There are two main options: "Use the key ring database defined for the z/OS system image." and "Use a Simple name (as in a SAF product or in PKCS #11 Token format):". The "Use a Simple name" option is selected, and the "Key ring:" field is empty. Below this, there are three sub-options: "Use this z/OS UNIX file system key database:", "* Key database stash file:", and "* Key database password:". The "Use this z/OS UNIX file system key database:" option is selected, and the "* Key database stash file:" field is empty. There is also a "Certificate Label:" field which is empty. At the bottom, there is a checkbox "Specified server certificate labels to be used by server to accommodate clients with different types of public keys." which is unchecked. Below this is an "Actions" section with a "Certificate Label" field and a list of radio buttons.

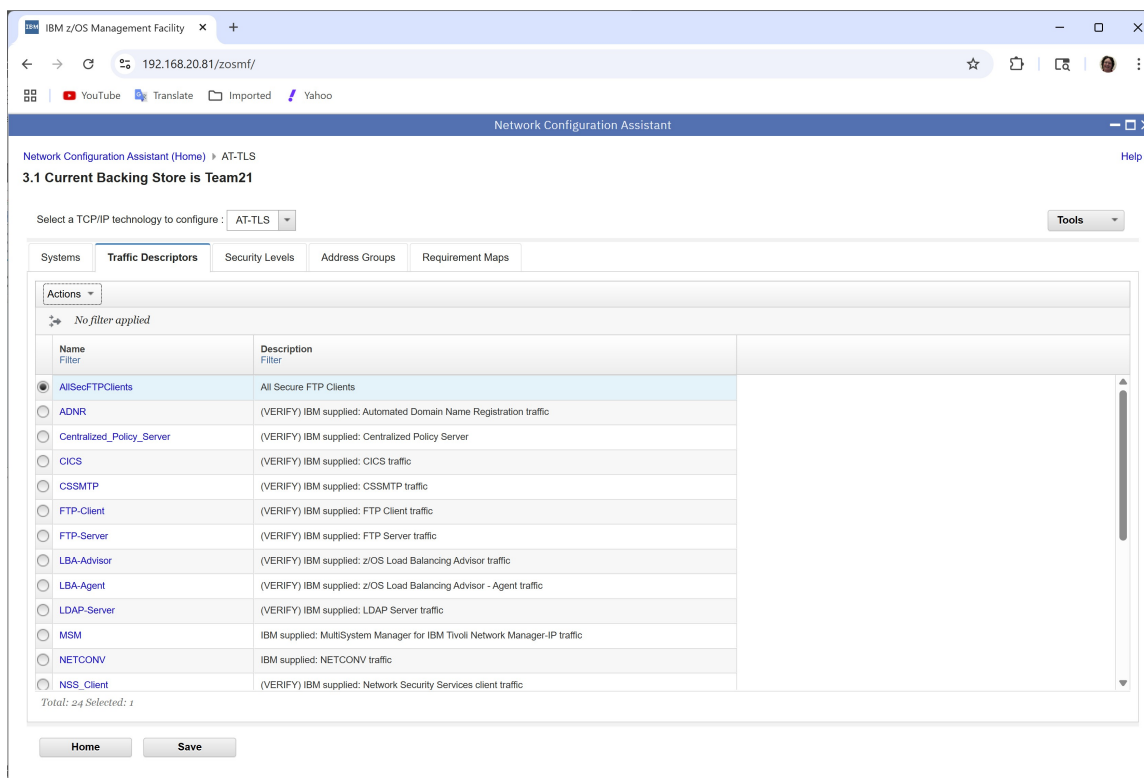
24. Select “Use a Simple name” and enter key ring name **LabClientRing**.

The screenshot shows the same IBM z/OS Management Facility Network Configuration Assistant web interface as in the previous screenshot. The "KeyRing" tab is still selected. The "Use a Simple name" option is still selected. The "Key ring:" field now contains the text "LabClientRing". The other options and fields remain the same as in the previous screenshot.

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

25. On z/OS user IDs, data set names, and RACF command keywords are not case sensitive but unix commands, unix file names, unix paths, certificate labels, and key rings are all case sensitive!!!
26. Note that you did not specify the owner of the LabClientRing.
27. When the key ring owner is not specified, the user ID requesting a certificate from the key ring is assumed to be the key ring owner.
 - a. In this case you each own your own key ring with your own certificate.
USER21/LabClientRing has default cert with label "USER21 on ANY ZOS"
USER31/LabClientRing has default cert with label "USER31 on ANY ZOS"
USER41/LabClientRing has default cert with label "USER41 on ANY ZOS"
USER51/LabClientRing has default cert with label "USER51 on ANY ZOS"
USER61/LabClientRing has default cert with label "USER61 on ANY ZOS"
USER71/LabClientRing has default cert with label "USER71 on ANY ZOS"
USER81/LabClientRing has default cert with label "USER81 on ANY ZOS"
USER91/LabClientRing has default cert with label "USER91 on ANY ZOS"
28. To use a certificate, you must be the owner of the certificate, but you do not need to be the key ring owner.
 - a. Review the following comments but **DO NOT ADD A LABEL name** in your policy!
 - b. When USER1 is the owner of keyring USER1Ring and their certificate with label "USER1 on ANY ZOS" is the default on the keyring, they specify the key ring as:
USER1Ring
 - c. When USER1 is the owner of keyring USER1Ring and their certificate with label "USER1 on ANY ZOS" is not the default on the keyring, they specify the key ring as:
USER1Ring (and they also have to specify the label "USER1 on ANY ZOS") (Note the certificate label field on the bottom of the panel.)
 - d. When USER99 owns keyring USERSRing and USER1's certificate with label "USER1 on ANY ZOS" is the default on the keyring, then USER1 must specify the key ring as:
USER99/USERSRing
 - e. When USER99 owns keyring USERSRing and USER1's certificate with label "USER1 on ANY ZOS" is not default on the keyring, then USER1 must specify the key ring as:
USER99/USERSRing (and they also have to specify the label "USER1 on ANY ZOS")
29. Feel free to examine the Advanced tab but leave all the defaults specified.
30. When you are finished select the **OK** button at the bottom of the page twice.

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



31. Select **Save**, optionally add a description, and click on **OK**.

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

32. Select the Security Levels tab.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The 'Security Levels' tab is selected. The 'Actions' dropdown menu is open, showing options like 'View Details', 'Modify...', 'Copy...', 'Delete', 'Show Where Used', 'New...', 'Hide Filter Row', and 'Clear Sorts'. The table below lists various security levels with their respective cipher choices and descriptions.

Name Filter	Cipher (First Choice) Filter	Type Filter	Description Filter
<input type="radio"/> Permit	None	No security	IBM supplied: Traffic is allowed with no security
<input type="radio"/> Default_NISTCiphers_z9	0x0067 - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z9 compliance
<input type="radio"/> Default_NISTCiphers_z10	0x006B - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z10 compliance
<input type="radio"/> Default_NISTCiphers_z196zEC12	0x006B - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z196 zEC12 compliance with client authorization
<input type="radio"/> Default_NISTCiphers_z196zEC12	0x006B - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z196 zEC12 compliance
<input type="radio"/> Default_Ciphers	0x0035 - TLS_RSA_WITH_AES_256_CBC_SHA	AT-TLS	IBM supplied: 3DES, AES-256 bit, AES-128 bit encryption
<input type="radio"/> AT-TLS_PlatinumClientAuth	0x0035 - TLS_RSA_WITH_AES_256_CBC_SHA	AT-TLS	IBM supplied: AES-256 bit encryption with client authentication
<input type="radio"/> AT-TLS_Platinum_with_TLS1.3	2019 Suggested	AT-TLS	IBM Supplied: Platinum with TLS1.3
<input type="radio"/> AT-TLS_Platinum_only_TLS1.3	2019 Suggested	AT-TLS	IBM Supplied: TLS1.3 only
<input type="radio"/> AT-TLS_Platinum_with_TLS1.2	2019 Suggested	AT-TLS	IBM Supplied: Platinum with TLS1.2
<input type="radio"/> AT-TLS_Platinum	0x0035 - TLS_RSA_WITH_AES_256_CBC_SHA	AT-TLS	IBM supplied: AES-256 bit encryption

Total: 14 Selected: 0

33. Select the AT-TLS__Gold security level and use Actions to view it.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The 'Security Levels' tab is selected. The 'Actions' dropdown menu is open, showing options like 'View Details', 'Modify...', 'Copy...', 'Delete', 'Show Where Used', 'New...', 'Hide Filter Row', and 'Clear Sorts'. The table below lists various security levels with their respective cipher choices and descriptions. The 'AT-TLS__Gold' security level is selected.

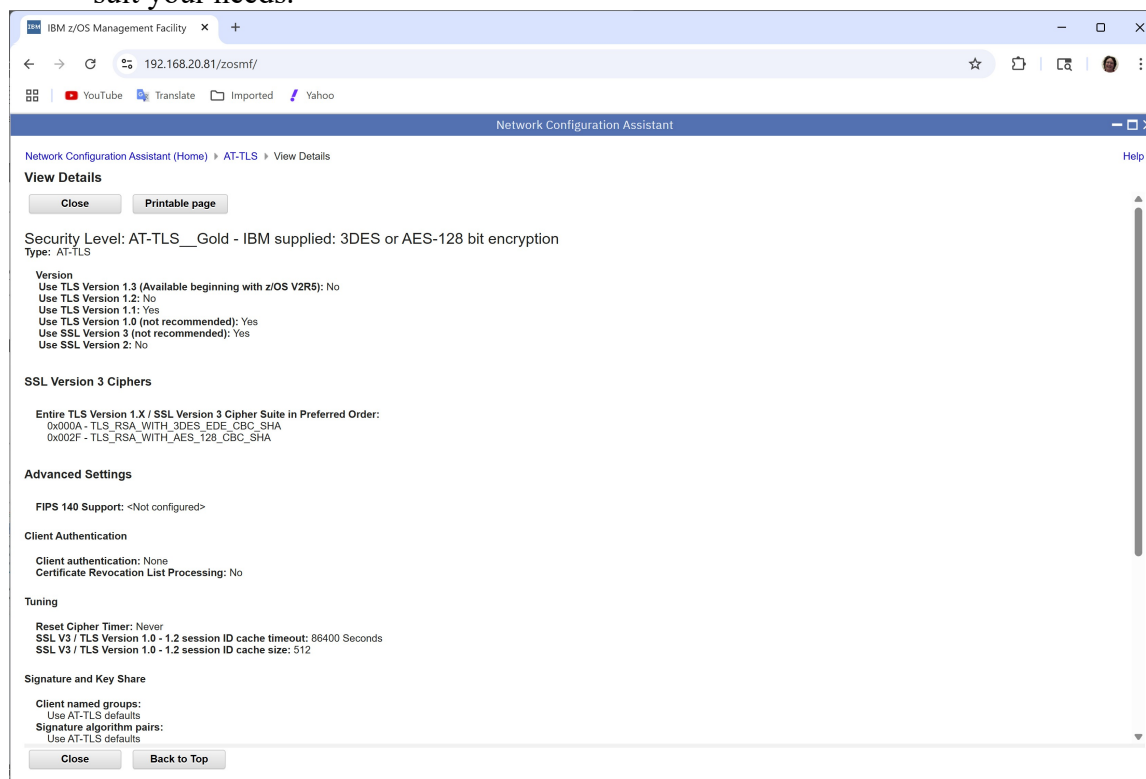
Name Filter	Cipher (First Choice) Filter	Type Filter	Description Filter
<input type="radio"/> Permit	None	No security	IBM supplied: Traffic is allowed with no security
<input type="radio"/> Default_NISTCiphers_z9	0x0067 - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z9 compliance
<input type="radio"/> Default_NISTCiphers_z10	0x006B - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z10 compliance
<input type="radio"/> Default_NISTCiphers_z196zEC12	0x006B - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z196 zEC12 compliance with client authorization
<input type="radio"/> Default_NISTCiphers_z196zEC12	0x006B - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z196 zEC12 compliance
<input type="radio"/> Default_Ciphers	0x0035 - TLS_RSA_WITH_AES_256_CBC_SHA	AT-TLS	IBM supplied: 3DES, AES-256 bit, AES-128 bit encryption
<input type="radio"/> AT-TLS_PlatinumClientAuth	0x0035 - TLS_RSA_WITH_AES_256_CBC_SHA	AT-TLS	IBM supplied: AES-256 bit encryption with client authentication
<input type="radio"/> AT-TLS_Platinum_with_TLS1.3	2019 Suggested	AT-TLS	IBM Supplied: Platinum with TLS1.3
<input type="radio"/> AT-TLS_Platinum_only_TLS1.3	2019 Suggested	AT-TLS	IBM Supplied: TLS1.3 only
<input type="radio"/> AT-TLS_Platinum_with_TLS1.2	2019 Suggested	AT-TLS	IBM Supplied: Platinum with TLS1.2
<input type="radio"/> AT-TLS_Platinum	0x0035 - TLS_RSA_WITH_AES_256_CBC_SHA	AT-TLS	IBM supplied: AES-256 bit encryption
<input checked="" type="radio"/> AT-TLS__Gold	0x000A - TLS_RSA_WITH_3DES_EDE_CBC_SHA	AT-TLS	IBM supplied: 3DES or AES-128 bit encryption
<input type="radio"/> AT-TLS__Silver	0x0009 - TLS_RSA_WITH_DES_CBC_SHA	AT-TLS	IBM supplied: 3DES, AES-128 bit, or DES encryption
<input type="radio"/> AT-TLS__Bronze	0x0002 - TLS_RSA_WITH_NULL_SHA	AT-TLS	IBM supplied: No encryption

Total: 14 Selected: 1

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

34. Note Client authentication is set to None.

- a. Your FTP Server needs to request Client Authentication so this default does not suit your needs.



35. When you are finished reviewing this Security Level use the **Close** button.

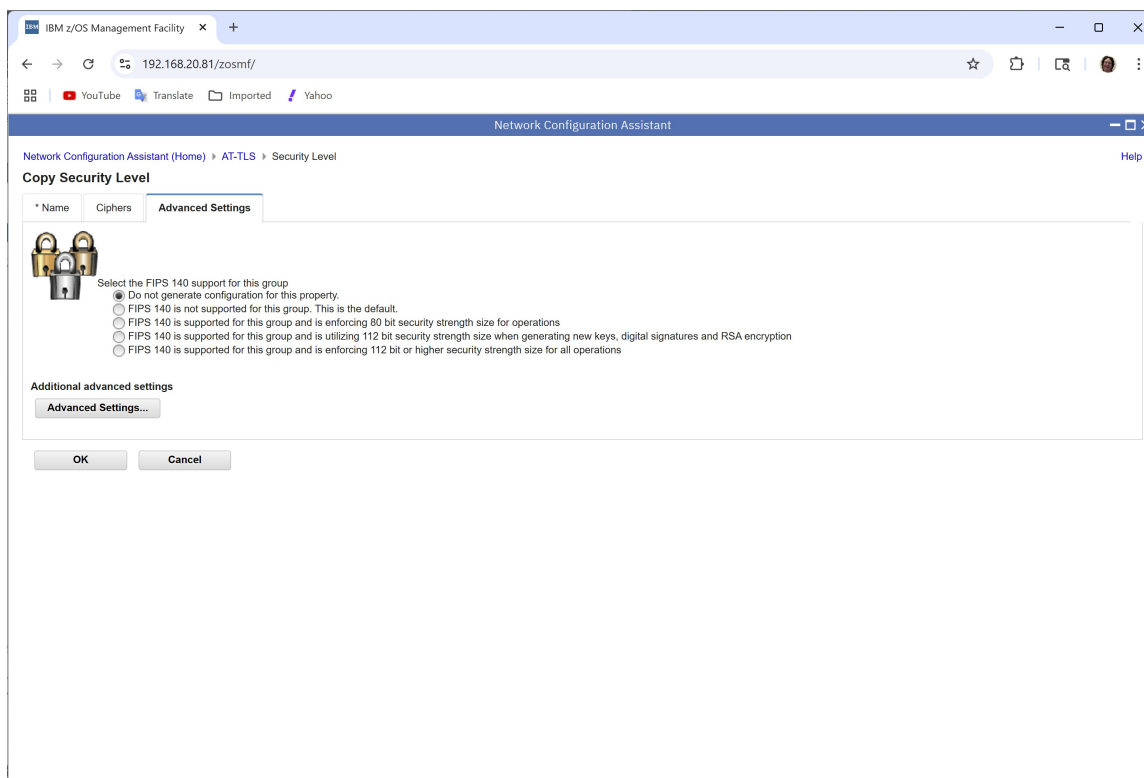
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

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

The screenshot shows a web browser window with the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant". The breadcrumb navigation shows "Network Configuration Assistant (Home) > AT-TLS > Security Level". The main heading is "Copy Security Level". There are three tabs: "Name", "Ciphers", and "Advanced Settings". The "Name" tab is active. It contains a lock icon, a text field for "Name" with the value "ATTLSGoldwClientAuth", and a text field for "Description" with the value "AT-TLS Encryption with Client Authentication". Below these fields is a section titled "Version choices" with five radio button options: "TLS V1.3", "TLS V1.2" (which is selected), "TLS V1.1", "TLS V1.0 (not recommended)", and "SSL V3 (not recommended)". At the bottom of the dialog are "OK" and "Cancel" buttons.

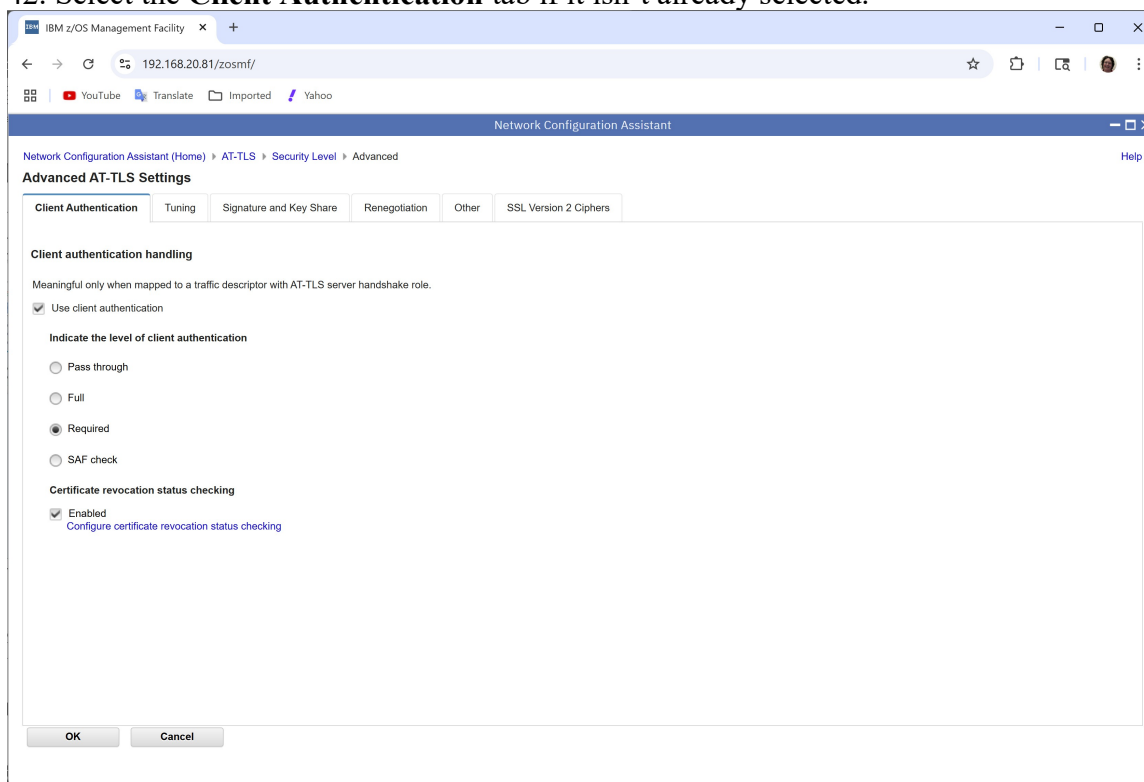
37. Name your copy **ATTLSGoldwClientAuth** and optionally add a description.
38. Select **TLS V1.2** and keep **TLS V1.1** selected as well. Unselect the other version choices.
39. Feel free to review the Ciphers tab but leave all the defaults selected.
40. When you are finished reviewing the Ciphers tab, select the **Advanced Settings** tab.

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



41. Select the **Advanced Settings** button.

42. Select the **Client Authentication** tab if it isn't already selected.



43. Select **Use client authentication**.

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

- a. This means that the Server will require Client Authentication during the TLS protocol negotiation and will only establish a secured connection if the client sends a Client Certificate to the server.

44. Click on **OK** twice.

45. Select **Save**, optionally add a description, and click on **OK**.

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

46. Click on the **Systems** tab.

47. If necessary, use the technology pull-down to select AT-TLS.

48. If necessary, use the radio button to select the “Default” system group.

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

Network Configuration Assistant (Home) > AT-TLS

3.1 Current Backing Store is Team21

Select a TCP/IP technology to configure: AT-TLS

Tools

Systems Traffic Descriptors Security Levels Address Groups Requirement Maps

Actions

No filter applied

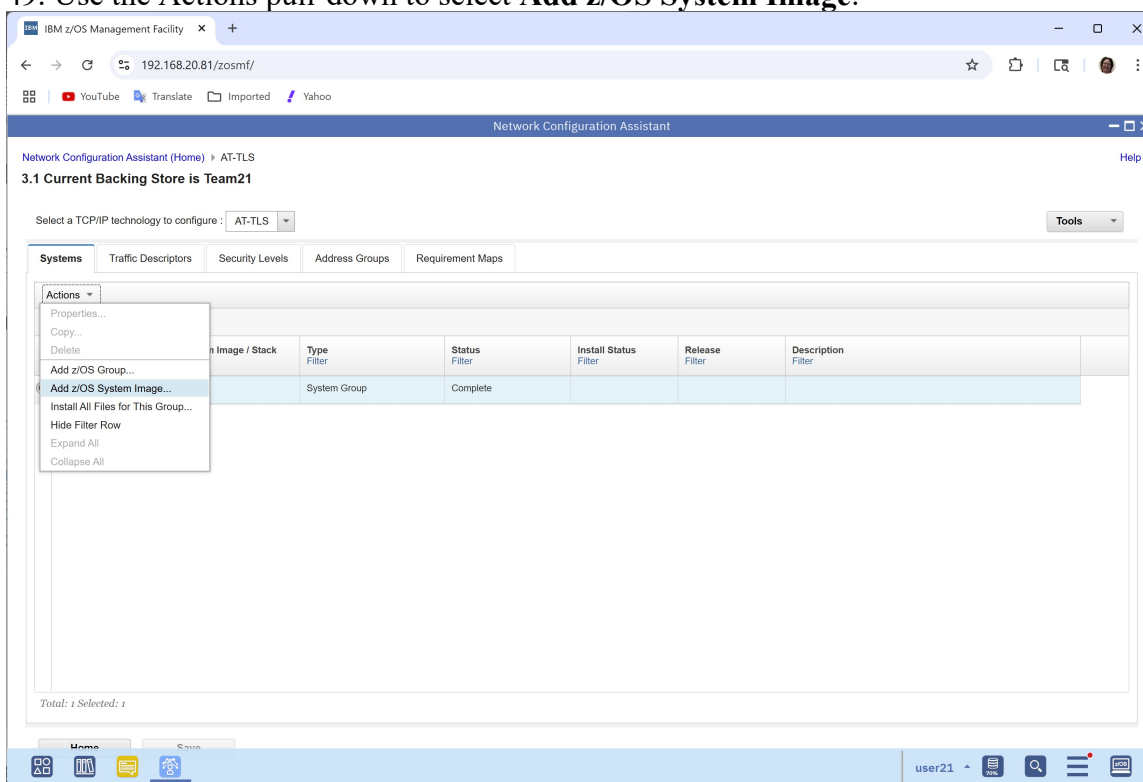
System Group or Sysplex / System Image / Stack	Type	Status	Install Status	Release	Description
Default	System Group	Complete			

Total: 1 Selected: 1

Home Save

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

49. Use the Actions pull-down to select **Add z/OS System Image**.



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

50. Enter your z/OS System Image Name:

- a) ZOS2
- b) ZOS3
- c) ZOS4
- d) ZOS5
- e) ZOS6
- f) ZOS7
- g) ZOS8
- h) ZOS9

51. Optionally add a description (i.e. z/OS system 7).

52. Our systems are running z/OS V3.1 so leave the default setting for z/OS Release.

53. Change the default AT-TLS key ring to **FTPD/ServerRing1**

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

Network Configuration Assistant (Home) > AT-TLS > z/OS System Image

Add z/OS System Image

* Name:
ZOS2

Description:
z/OS System 2

z/OS Release:
3.1

Default AT-TLS key ring database

☒ Simple name (as in an SAF product or in PKCS #11 token format)

* Key ring:
FTPD/ServerRing1

☐ Key database is a z/OS UNIX file system file:

* Key database:

* Key database stash file:

or

* Key database password:

OK Cancel

user21

55. Click on the **OK** button.

56. You have created a z/OS system so you will be prompted to create a TCP/IP stack.
Click on the **Proceed** button.

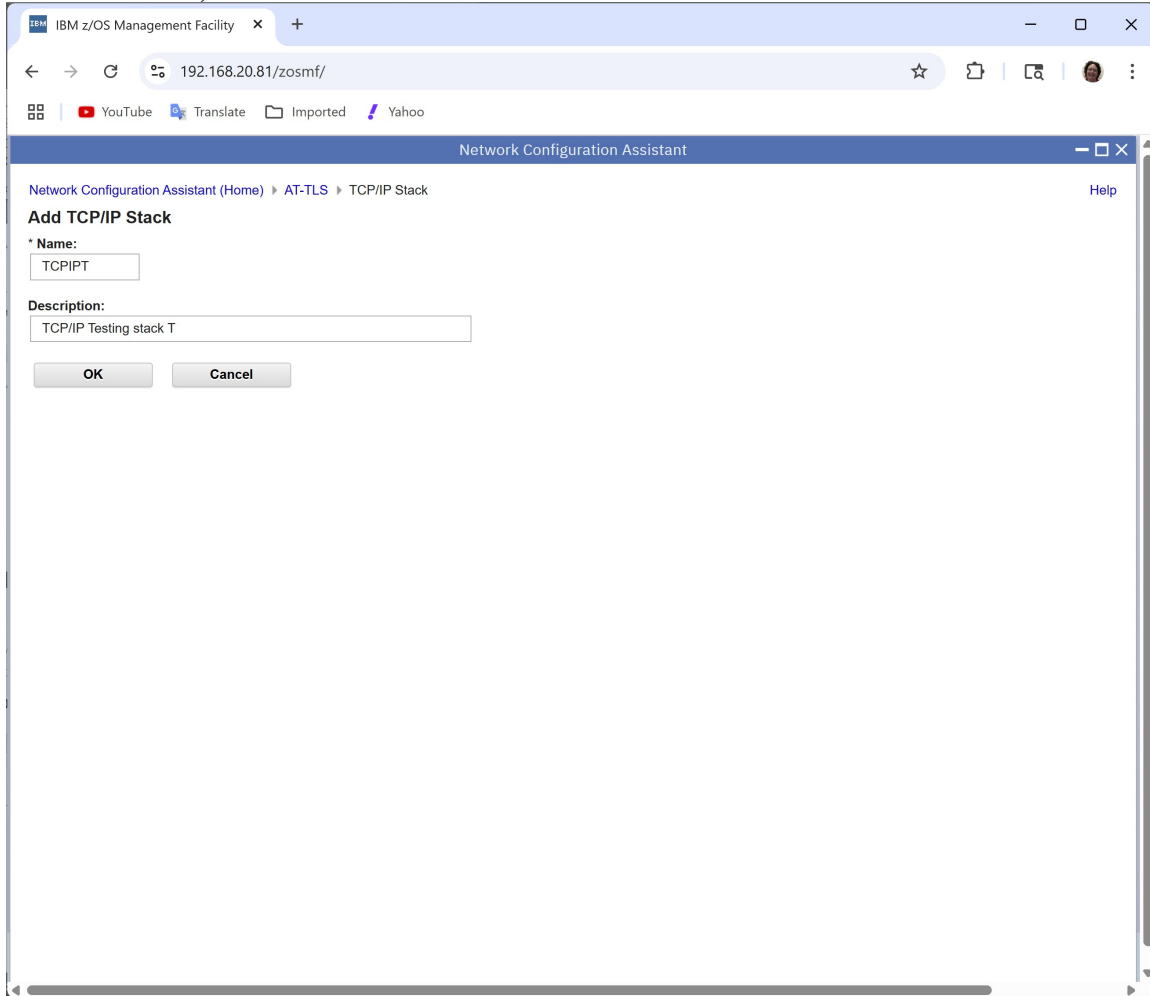
Proceed to the Next Step?

? Connectivity rules are configured for each TCP/IP stack. To continue with configuration you need to add a TCP/IP stack to the new z/OS system image. Do you want to add a TCP/IP stack now?

Cancel Proceed

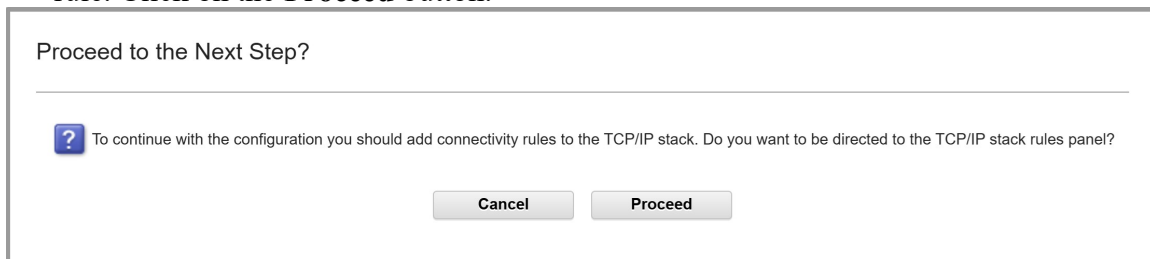
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

57. Enter the TCP/IP stack name of **TCPIPT**. Optionally add a description (ie. TCP/IP test stack T). Click on the **OK** button.



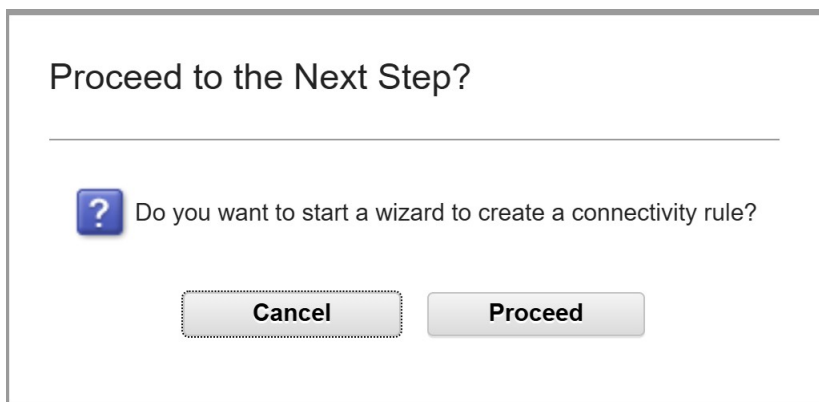
The screenshot shows a web browser window with the address bar displaying '192.168.20.81/zosmf/'. The browser's address bar includes navigation buttons (back, forward, refresh) and search, star, and print icons. Below the address bar are links for YouTube, Translate, Imported, and Yahoo. The main content area of the browser displays the 'Network Configuration Assistant' interface. The breadcrumb navigation shows 'Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack'. The title of the dialog is 'Add TCP/IP Stack'. It contains a field for '* Name:' with the value 'TCPIPT' and a field for 'Description:' with the value 'TCP/IP Testing stack T'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

58. You have created a TCP/IP stack so you will be prompted to create a connectivity rule. Click on the **Proceed** button.



The screenshot shows a confirmation dialog box with the title 'Proceed to the Next Step?'. Below the title is a horizontal line. Below the line is a question mark icon followed by the text: 'To continue with the configuration you should add connectivity rules to the TCP/IP stack. Do you want to be directed to the TCP/IP stack rules panel?'. At the bottom of the dialog are 'Cancel' and 'Proceed' buttons.

59. You will be prompted to use a wizard to create your connectivity rule. Click on the **Proceed** button.



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

AT-TLS Lab for FTP: Step-by-Step

Working with MVS Image ZOSn (FTP Server and Client Image)

1. Name your new Connectivity Rule **VIPAs2VIPAs**.

IBM z/OS Management Facility

192.168.20.81/zosmf/

Network Configuration Assistant

Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule

New Connectivity Rule

Data Endpoints

Requirement Map

Advanced Settings

* Connectivity rule name:

VIPAs2VIPAs

Select the address groups of the host endpoints of the traffic you want to protect.

Local data endpoint

Address group:

All_IPv4_Addresses

* IPv4 or IPv6 address, subnet, or range:

192.168.20.100-192.168.20.108

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

Remote data endpoint

Address group:

All_IPv4_Addresses

* IPv4 or IPv6 address, subnet, or range:

192.168.20.100-192.168.20.108

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

user21

2. For both the Local data endpoint and the Remote data endpoint select “IPv4 or IPv6 address, subnet, or range” and enter the address range **192.168.20.100-192.168.20.108**.
 - a. Note: The policy you are creating is a generic policy and can be used on several systems and not just your MVS because you are specifying a range as the source and destination IP addresses.
3. Press **Next** button.

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

4. Notice that you may create your own Requirement Map or use the sample the tool provides (AT-TLS_Sample...).
5. Since the sample does not meet your needs you will need to create a new one.

IBM z/OS Management Facility

192.168.20.81/zosmf/

Network Configuration Assistant

Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule

New Connectivity Rule

✓ Data Endpoints
➔ Requirement Map
Advanced Settings

Requirement Map

Requirement maps are reusable objects that combine your traffic definitions (traffic descriptors) with your security definitions (security levels).

☒ Create a new requirement map
☐ Select an existing requirement map

AT-TLS_Sample - IBM supplied: AT-TLS sample: CICS and TN3270

New Requirement Map properties

* Name:
SecFTPTrafNet

Description:
Secure FTP Traffic

Mappings table

Actions		Move Up	Move Down
Traffic Descriptor	Security Level		
<input type="radio"/> AllSecFTPClients	AT-TLS__Gold		
<input checked="" type="radio"/> FTP-Server	ATTLSGoldwClientAuth		

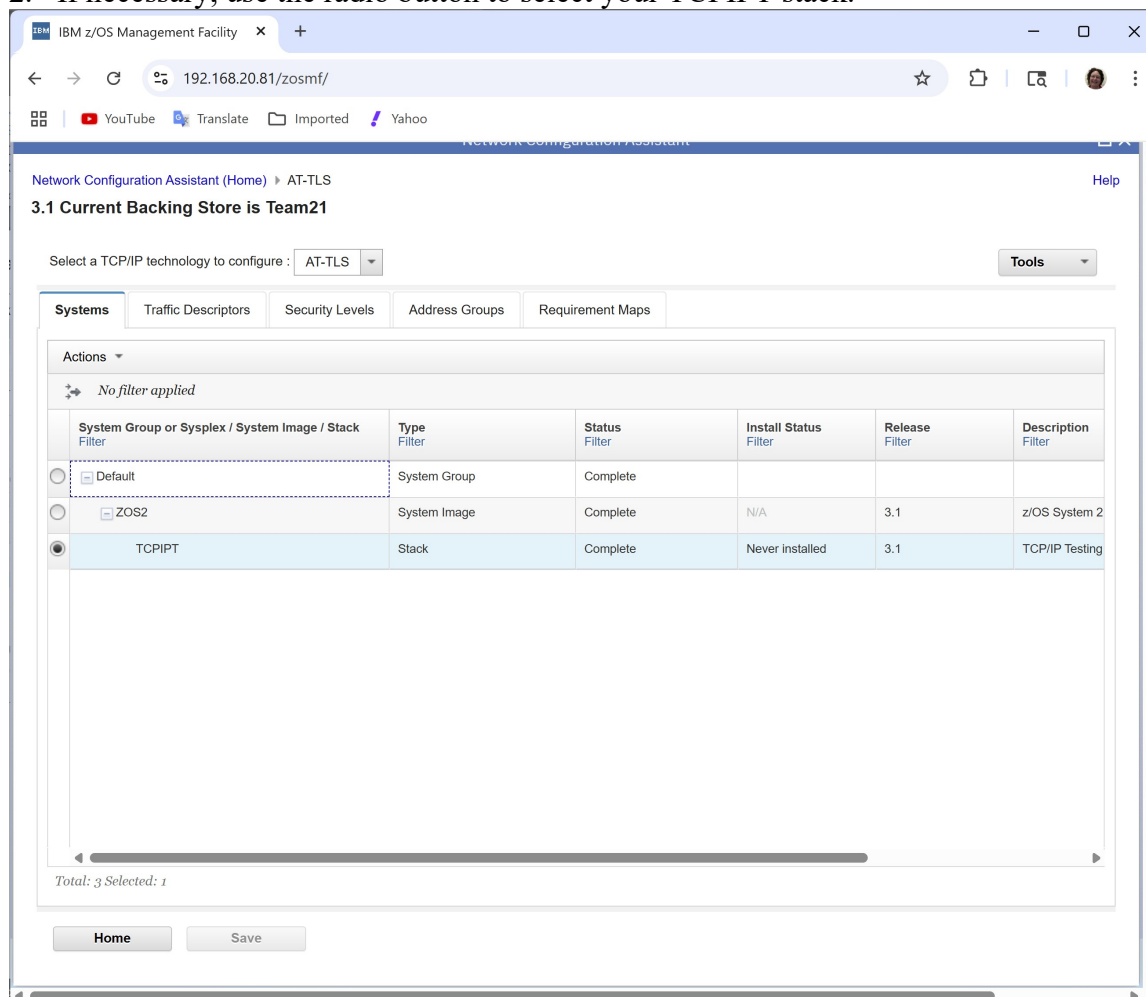
< Back Next > Finish Cancel

6. Name your new Requirement Map **SecFTPTrafNet** and optionally add a description.
7. Use the Traffic Descriptor pull-down in the first row to select the traffic descriptor that you created, **AllSecFTPClients**.
8. Use the Security Level pull-down in the first row to select security level **AT-TLS__Gold**.
9. Use the Traffic Descriptor pull-down in the second row to select traffic descriptor **FTP-Server**.
10. Use the Security Level pull-down in the second row to select the security level that you created, **ATTLSGoldwClientAuth**.
11. Use the radio button on any other rows one at a time to select them and use the **Actions** pull-down to select **Remove Row**.
12. Click on **Next** button.
13. Feel free to check out the Advanced Settings... but no changes are needed there.
14. Click on the **Finish** button.
15. Click on the **Close** button.
16. Select **Save**, optionally add a description, and click on **OK**.

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

Installing the files for ZOSn on the Mainframe

1. You should be at the Main Configuration panel.
2. If necessary, use the radio button to select your TCPIPT stack.



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

3. Use the **Actions** pull-down to select **Install Configuration Files**.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (AT-TLS) interface. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant (Home) > AT-TLS". The main heading is "3.1 Current Backing Store is Team21". Below this, there is a dropdown menu for "Select a TCP/IP technology to configure:" set to "AT-TLS". A "Tools" button is also visible.

The "Systems" tab is selected, displaying a table with columns: "Image / Stack", "Type", "Status", "Install Status", "Release", and "Description". The table contains three rows:

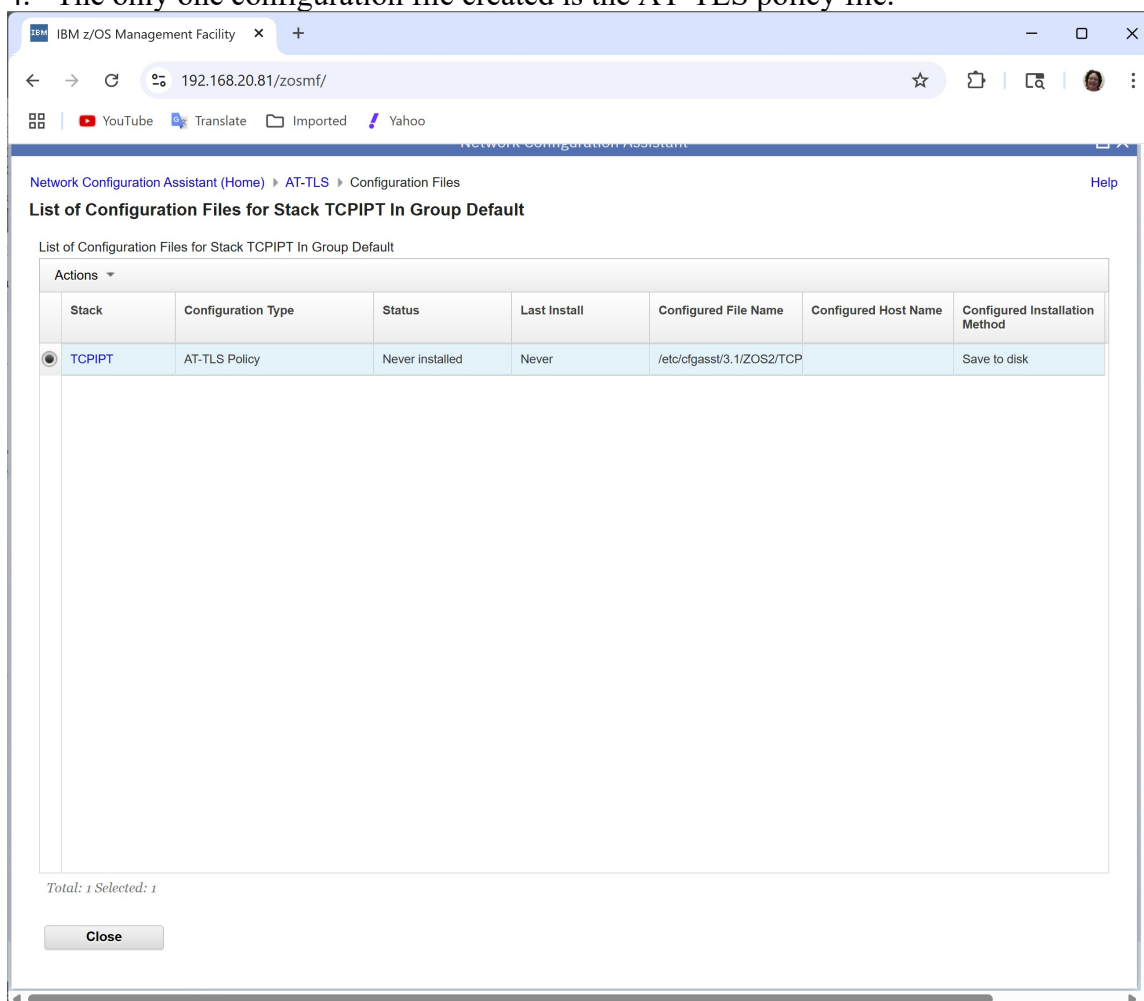
Image / Stack	Type	Status	Install Status	Release	Description
	System Group	Complete			
	System Image	Complete	N/A	3.1	z/OS System 2
	Stack	Complete	Never installed	3.1	TCP/IP Testing

An "Actions" menu is open over the table, showing options: Properties..., Rules..., Copy..., Delete, Add z/OS Group..., Add z/OS System Image..., Add TCP/IP Stack..., Install All Files for This Group..., **Install Configuration Files...** (highlighted), Hide Filter Row, Expand All, and Collapse All.

At the bottom of the table, it says "Total: 3 Selected: 1". Below the table are "Home" and "Save" buttons.

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

4. The only one configuration file created is the AT-TLS policy file.



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

5. Use the **Actions** pull-down to select **Configuration Summary...**

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant web interface. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant (Home) > AT-TLS > Configuration Files". The main heading is "List of Configuration Files for Stack TCPIPT In Group Default". Below this, there is a table with columns: Configuration Type, Status, Last Install, Configured File Name, Configured Host Name, and Configured Installation Method. The table contains one row with the following data: Configuration Type: policy, Status: Never installed, Last Install: Never, Configured File Name: /etc/cfgasst/3.1/ZOS2/TCP, Configured Host Name: , and Configured Installation Method: Save to disk. An "Actions" pull-down menu is open over the table, showing options: Show Configuration File..., Install..., Configure Install..., Install Multiple, Configuration Summary... (highlighted), and History. At the bottom of the table, it says "Total: 1 Selected: 1". A "Close" button is located at the bottom left of the interface.

Configuration Type	Status	Last Install	Configured File Name	Configured Host Name	Configured Installation Method
policy	Never installed	Never	/etc/cfgasst/3.1/ZOS2/TCP		Save to disk

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

6. This panel summarizes the configuration information in a format that can be helpful to the administrator and remote connection partners.

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/. The page title is "Configuration Summary for AT-TLS". Below the title are buttons for "Close" and "Printable page". The main content area is titled "Configuration Summary for AT-TLS Default.ZOS2.TCPIPT". It contains several paragraphs of text explaining the configuration and the tables that follow. The tables are: "Connectivity Rule: VIPAs2VIPAs" and "Security Level".

Connectivity Rule: VIPAs2VIPAs

- Stack: TCPIPT
- Local Data Endpoint: 192.168.20.100-192.168.20.108
- Remote Data Endpoint: 192.168.20.100-192.168.20.108

Traffic Type				Application Configuration				Security Level	
Local Port	Remote Port	Jobname	User ID	Connect Direction	Key Ring	Handshake Role	Application Controlled	Secondary Map	
1024-65535	21	---	USER*	Outbound	LabClientRing	Client	On	On	AT-TLS_Gold
21	1024-65535	---	---	Inbound	FTPD/ServerRing1	Server	On	On	ATTLSGoldwClientAuth

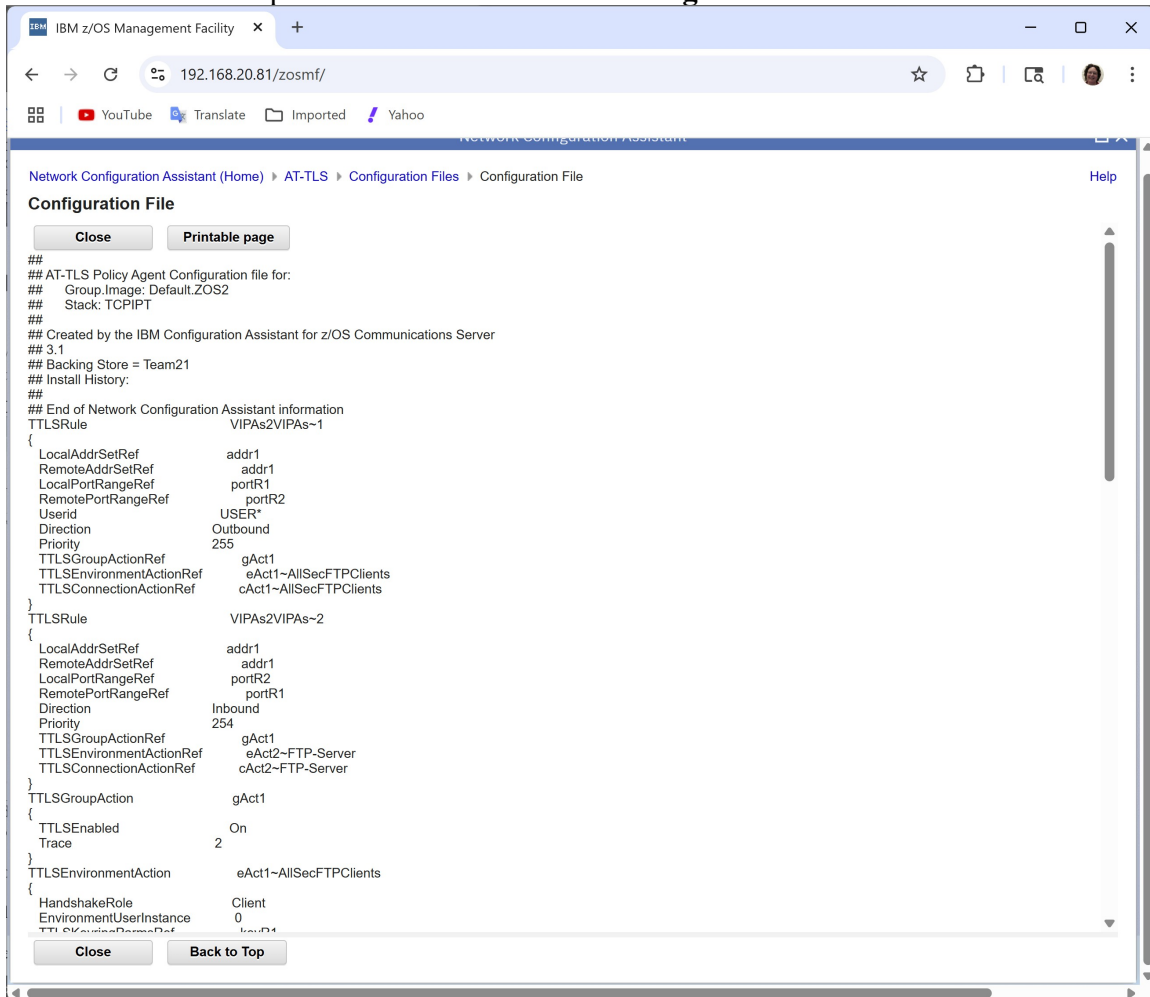
Security Level

Name	TLS Version 1/SSLv3	SSLv2	Client Auth Type

7. When you finish reviewing the panel use the **Close** button.

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

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



9. This is the policy file that you will next send (FTP) to your z/OS system to use.
10. You could have created this file manually, but you see how easy it was to create using the Configuration Assistant tool.
 - a. Can you imagine having to create this policy from scratch with all the syntactical idiosyncrasies?
 - b. Now you understand why it is useful to learn to build policies with the z/OS IBM Configuration Assistant.
11. When you finish reviewing the panel use the **Close** button.

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

12. 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) > AT-TLS > Configuration Files > Install

Install File for Default.ZOS2.TCPIPT

* Install file name:

/u/user21/TM21_ATTLS_FTP.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)

Sending AT-TLS FTP policy

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

13. Fill in:

- Select FTP to send the file using FTP.
- The path and file name **/u/user_{nx}/TM_{nx}_ATTLS_FTP.policy**.
- The IP address of the FTP Server (FTPCCL) **192.168.20.8_n**.
- The User ID **USER_{nx}**.
- The password.
- Optionally add a comment.
- Remember that “**n**” represents your ZOS suffix of **2 through 9**.
- Select the **Save User ID** and **Save Password**.
- Unselect **Use TLS/SSL**.
- You will get a pop up warning but just click on **OK**.

Information

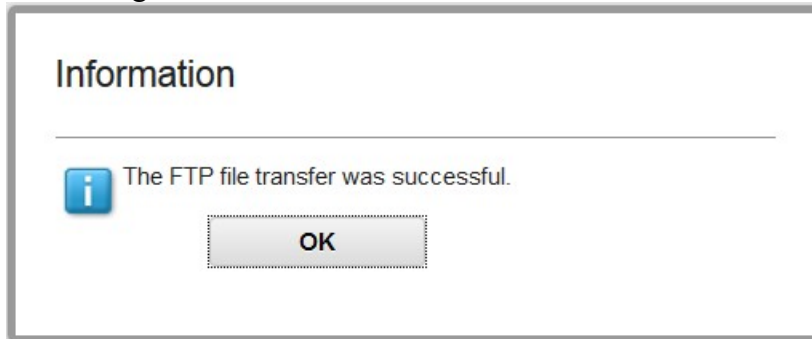
FTP connections used to install this configuration to the z/OS system will not be secured unless you are using Application Transparent TLS (AT-TLS) to secure them.

OK

14. Press the **Go** button to ftp the policy file to your z/OS platform.

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

- a. Optionally enter a comment for the history log.
 - b. Click on **OK**.
15. The transfer takes a little time but then you should receive a “successful” pop-up message.



15. Press **OK**.
16. **Close** the FTP window.
17. Click on **Close** to return to the AT-TLS Perspective.
18. **You are ready to test your policies on z/OS.**

Part 2: Enabling the TCP/IP Stack for AT-TLS

In this part of the lab you

- Create the definitions to enable the stack for AT-TLS.
- Create the FTP configuration members (called the “FTP.DATA” files) that allow your FTP client and server to invoke security with AT-TLS.

Remember that there are other steps to implementing PAGENT Security Definitions.

1. Design the secured environment that meets your needs
 - a. Network Diagram for the secure environment
 - b. SAF authorizations for the type of policy you are implementing
2. Implement SYSLOGD (already implemented)
3. Implement TRMD (not yet implemented; used for IDS and IKED)
4. Create the key ring populated with the appropriate certificates (already implemented)
5. Create the Policy Agent files and the Policy Agent (PAGENT) server environment (already implemented)
6. **Create the AT-TLS policy (just completed in Part 1 of current lab)**
7. Enable the TCP/IP stack for AT-TLS
8. Set up INITSTACK access control for the TCP/IP stack if implementing AT-TLS (must be verified)
9. Configure the FTP server and client configuration files (FTPDATA and FTPCDATA) to use AT-TLS
10. Test your policies

In this part of the lab you will install your AT-TLS policy into the running PAGENT environment on your MVS system and test it.

1. LEGEND for the TEAM Number:
 - a. TEAMnx, where “n” represents your ZOS suffix and “x” represents your userid suffix.
 - b. EXAMPLE:
 - i. TEAM53 means ZOS5 and USERID of USER53.
2. Each team will create its own *pagent.conf* file. **HOWEVER, when it is time to test the PAGENT process, you must coordinate with the other teams that are signed onto your own ZOS system. (Only one PAGENT may run at a time on a single ZOS.)**
3. Create a PCOMM session to connect to TN3270 at TCPIP1 on your assigned MVS system.
 - a. You should be telnetting into TCPIP1 on some MVS system at **192.168.20.8n** (where “n” is the suffix of the MVS/ZOS system).
 - b. Team 11 telnets as User11 to TCPIP1 in MVS1 at **192.168.20.81**
 - c. Team 12 telnets as User12 to TCPIP1 in MVS1 at 192.168.20.81
 - d. Team 13 telnets as User13 to TCPIP1 in MVS1 at 192.168.20.81
 - e. Team 21 telnets as User21 to TCPIP1 in MVS2 at **192.168.20.82**
 - f. Team 22 telnets as User22 to TCPIP1 in MVS2 at 192.168.20.82
 - g. Team 23 telnets as User23 to TCPIP1 in MVS2 at 192.168.20.82

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

- h. Team 31 telnets as User31 to TCPIP1 in MVS3 at **192.168.20.83**
 - i. Team 32 telnets as User32 to TCPIP1 in MVS3 at 192.168.20.83
 - j. Team 33 telnets as User33 to TCPIP1 in MVS3 at 192.168.20.83
 - k. Team 41 telnets as User41 to TCPIP1 in MVS4 at **192.168.20.84**
 - l. Team 42 telnets as User42 to TCPIP1 in MVS4 at 192.168.20.84
 - m. Team 43 telnets as User43 to TCPIP1 in MVS4 at 192.168.20.84
 - n. Team 51 telnets as User51 to TCPIP1 in MVS5 at **192.168.20.85**
 - o. Team 52 telnets as User52 to TCPIP1 in MVS5 at 192.168.20.85
 - p. Team 53 telnets as User53 to TCPIP1 in MVS5 at 192.168.20.85
 - q. Team 61 telnets as User61 to TCPIP1 in MVS6 at **192.168.20.86**
 - r. Team 62 telnets as User62 to TCPIP1 in MVS6 at 192.168.20.86
 - s. Team 63 telnets as User63 to TCPIP1 in MVS6 at 192.168.20.86
 - t. Team 71 telnets as User71 to TCPIP1 in MVS7 at **192.168.20.87**
 - u. Team 72 telnets as User72 to TCPIP1 in MVS7 at 192.168.20.87
 - v. Team 73 telnets as User73 to TCPIP1 in MVS7 at 192.168.20.87
 - w. Team 81 telnets as User81 to TCPIP1 in MVS8 at **192.168.20.88**
 - x. Team 82 telnets as User82 to TCPIP1 in MVS8 at 192.168.20.88
 - y. Team 83 telnets as User83 to TCPIP1 in MVS8 at 192.168.20.88
 - z. Team 91 telnets as User91 to TCPIP1 in MVS9 at **192.168.20.89**
 - aa. Team 92 telnets as User92 to TCPIP1 in MVS9 at 192.168.20.89
 - bb. Team 93 telnets as User93 to TCPIP1 in MVS9 at 192.168.20.89
4. When you see the Message 10 screen from the TN3270 server, provide your userid with the logon command that has been built for this system. (The logon command is named "TSO", but it is a VTAM LOGON nevertheless.)
- a. **TSO <userid>**
5. On the ISPF signon screen, provide the password you were given in class.
- a. **<password>**
 - b. Press **ENTER**
6. Go into SDSF to view the MVS log with:
- a. **ISPF D.LOG**
7. Start the FTPT server using the instructor configuration files:
- a. **/S FTPT**
8. Determine which OMVS segment (OMVS User ID) is associated with the FTPT server:
- a. HINT: Look for the USER that is assigned to the started task.
 - b. IEF695I START FTPT WITH JOBNAME FTPT IS ASSIGNED TO USER _____, GROUP=OMVSGRP
9. Verify that the following procedures are running by issuing the command **/D A,L** from the SDSF command line:
- a. SYSLOGDC (SYSLOG Daemon for this MVS)
 - b. TCPIP1 (this is the stack you telnetted into)
 - c. TN3270 (this is the TN3270 proc associated with TCPIP1)
 - d. FTPCCL(1) (this is the FTP proc associated with TCPIP1 – without TLS)
 - e. **TCPIPT** (this is the stack that you will be testing AT-TLS with)
 - f. **PAGENTT** (this should be running with a student version of the /etc/pagentt.conf file if you have completed the Policy Agent lab)

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

10. Verify that the SERVAUTH resource “EZB.INITSTACK” authorizes your TCPIP stack to the INITSTACK function:
 - a. **=6** (to take you to the ISPF command shell screen)
 - b. **RLIST SERVAUTH EZB.INITSTACK.*.*** to view the resource in the SERVAUTH group.
11. What is your access to this SERVAUTH resource?
12. Many other resources for TCP/IP security exist in the SERVAUTH class.
 - a. REMEMBER: You must consult the IP Configuration Guide and view the samples in hlq.SEZAINST(EZARACF) for information on how to set up RACF authorizations for features and commands, like Policy Agent, the command *trmdstat*, and the command *ipsec*.
13. Examine the contents of the prebuilt key rings (ServerRing1 and LabClientRing) that you will be using.

NOTE: When you learn about X.509 certificates and key rings, you will see the significance of the “DEFAULT” certificate, of the certificate owner, and of the key ring owner.

 - a. **RACDCERT ID(FTPD) LISTRING(ServerRing1)**
 - i. Who owns the FTP Server Certificate with the label of “FTP on ANY ZOS”?
 - ii. Is it the DEFAULT certificate on the ring? _____
 - iii. The owner of the certificate MUST be the owner of the FTPT procedure. Is this the right owner? _____
 - iv. What is the other type of certificate on this ring?
 - b. **RACDCERT ID(USERnx) LISTRING(*)**
(to see all rings owned by YOU)
 - i. How many USER certificates are on “LabClientRing”? _____
 - ii. How many CERTAUTH certificates? _____
 - c. **RACDCERT ID(FTPD) LISTRING(*)**
(to see all rings owned by FTPD)
 - i. How many USER certificates are on “ClientRing1”? One or Multiple? _____
 - ii. How many of these are the DEFAULT certificate? _____
 - iii. How many CERTAUTH certificates on this ring? _____

NOTE: We do not use this ring in our class labs. You will also see other rings that are owned by FTPD, but we do not use all of these in this class.
14. Move to the MVS SDSF Console:
 - a. **PF3**
 - b. **D.LOG**
15. Verify that the TCPCONFIG statement has enabled TCPIPT for AT-TLS.
 - a. Check to see if TLS has been enabled or not:
 - i. **/D TCPIP,TCPIPT,NETSTAT,CONFIG**
 - 1) Look in the output for: **TTLS: YES or NO**
 - ii. If TTLS: NO is set, then enable it with the following command:
 - 1) **/V TCPIP,TCPIPT,OBEYFILE,SYS1.CS.TCPPARMS(TLSON)**

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

- 2) You may run out of room to enter the command on the Command Input line. If you enter forward slash "/" alone you will be taken to a screen with a larger input area. Or if you don't realize you will run out of room until you get to the end of the input area, you can enter a plus sign "+" in the last character position. This will also take you to the panel with a larger input area.
- b. Re-issue the command to see that TLS is enabled:
 - i. **/D TCPIP,TCPIPT,NETSTAT,CONFIG**
- 1) Look in the output for: **TTLS: YES**
16. Next view the messages from the running TCP/IP Stack's joblog:
 - a. **=D.DA**
 - b. Enter an "S" next to the line with 'TCPIPT' in it to view the joblog
 - i. **S TCPIPT** ("S" is for "select")
17. Browse through the lines that show that TTLS has been enabled for the stack, but there are no rules to exploit it. You may see it multiple times because PAGENT has retried to access rules due to the 600 seconds that were coded for the image:
 - a. **EZZ4249I TCPIPT INSTALLED TTLS POLICY HAS NO RULES**
18. Exit from the view of the job log with a **PF3**.
19. Return to the SDSF Console:
 - a. **=D.LOG**
20. Next disable AT-TLS using an OBEYFILE against the running TCP/IP procedure:
 - a. **/V TCPIP,TCPIPT,OBEYFILE,SYS1.CS.TCPPARMS(TLSOFF)**
 - i. As you just demonstrated, TLS can be enabled and disabled dynamically.
21. Build your own versions of the OBEYFILES to enable and disable AT-TLS.
 - a. **=3.4**
22. Position yourself in the Student Datasets by entering "USER.CS" in the "Dsname" field of the "Data Set List Utility" screen:
 - a. Dsname Level . . . **USER.CS**
 - b. Press **ENTER**.
23. Edit the contents of 'USER.CS.TCPPARMS' by placing an "E" next to this dataset name.
E
24. Edit the two files named **TLSONnx** and **TLSOFFnx** by selecting each in turn and then filling them in:
 - a. **S TLSONnx** – configure to enable TLS; follow instructions in the member
 - b. **S TLSOFFnx** – configure to disable TLS; follow instructions in the member
 - c. Hint: These settings are documented in the IP Configuration Reference and mentioned in the class lecture.
25. The instructors have copied the sample client FTP data file from **SYS1.TCPIP.SEZAINST(FTCDATA)** to your student dataset as **USER.CS.TCPPARMS(FTPCLSnx)**.
26. The instructors have also copied the sample server FTP data file from **SYS1.TCPIP.SEZAINST(FTPSATA)** to your student dataset as **USER.CS.TCPPARMS(FTPSECnx)**.
27. Select your Server's **FTPSECnx** Profile member next for editing.
 - a. "S" next to the member name.

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

28. Browse through all sections of the Server's FTP.DATA file.
 - a. This is the file that describes the operating characteristics of the FTP server environment.
29. Notice the default settings for the following parameters. These are not security settings but are settings that are often customized for FTP usage. For this lab the defaults are OK. All of these settings are documented in the IP Configuration Reference if you have any questions about them.
FILETYPE
BLKSIZE
DIRECTORY
LRECL
AUTOMOUNT
AUTORECALL
DIRECTORYMODE
RDW
30. There are other settings that we would like you to change for this lab. They are settings that are often customized for FTP usage. All these settings are documented in the IP Configuration Reference if you have any questions about them. Please make the following changes in the file:
PRIMARY 5
RECFM FB
SECONDARY 2
SPACETYPE CYLINDER
UNITNAME 3390
SMFAPPE 70
INACTIVE 0
31. Next, update the Security section to make the FTP Server an AT-TLS-aware and AT-TLS-controlling application. On the command line use the find command:
 - a. **F 'Security options'**
 - i. You may have to repeat the find with a **PF5** to locate the "Security Options" section.
32. Fill in the Server's security options to indicate the following options for Client Certificates, for TTLS, etc. Uncomment items that need to be uncommented. Add items that do not exist in the default file. Comment out items that need to be commented out now because they will be defined in policies. Consult your lecture notes or the IP Configuration Reference if you have forgotten why we are coding these options. (Order might be different in what you see.)

```
EXTENSIONS        AUTH_TLS
SECURE_FTP        ALLOWED
TLSMECHANISM      ATTLS
SECURE_LOGIN      REQUIRED
SECURE_PASSWORD   REQUIRED
SECURE_CTRLCONN   PRIVATE
SECURE_DATACONN   PRIVATE
;CIPHERSUITE      SSL_NULL_MD5
;CIPHERSUITE      SSL_NULL_SHA
;CIPHERSUITE      SSL_RC4_MD5_EX
;CIPHERSUITE      SSL_RC4_MD5
;CIPHERSUITE      SSL_RC4_SHA
;CIPHERSUITE      SSL_RC2_MD5_EX
;CIPHERSUITE      SSL_DES_SHA
```

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

```
;CIPHERSUITE    SSL_3DES_SHA
;CIPHERSUITE    SSL_AES_128_SHA
;CIPHERSUITE    SSL_AES_256_SHA
;KEYRING        name
TLSRFCLEVEL     RFC4217
```

- a. NOTE: You might want to uncomment one of the CIPHERSUITE statements in order to see the effect when the equivalent statement is already specified in the policy. (i.e., MSG EZYFT47I would be triggered.)

33. Move to the “debugging options” section of the file and include logging of client errors:

```
DEBUG SEC
```

34. File the FTPSEC~~nx~~ member with PF3.

- a. **PF3**

35. Select your Client’s FTPCLS~~nx~~ Profile member next for editing.

- a. Enter “S” next to the member name.

36. Browse through all sections of the Client’s FTP.DATA file.

- a. This is the file that describes the operating characteristics of the FTP client environment.

37. Notice the default settings for the following parameters. These are not security settings but are settings that are often customized for FTP usage. For this lab the defaults are OK. All of these settings are documented in the IP Configuration Reference if you have any questions about them.

```
FILETYPE
BLKSIZE
DIRECTORY
LRECL
AUTOMOUNT
AUTORECALL
DIRECTORYMODE
RDW
```

38. There are other settings that we would like you to change for this lab. They are settings that are often customized for FTP usage. All these settings are documented in the IP Configuration Reference if you have any questions about them. Please make the following changes in the file:

```
PRIMARY      5
RECFM        FB
SECONDARY    2
SPACETYPE    CYLINDER
UNITNAME     3390
```

39. Next, edit the Security section to make the FTP Client an AT-TLS-aware and AT-TLS-controlling application. First find the security options:

- a. **F ‘Security options’**

- i. You may have to repeat the find with a **PF5** to locate the “Security Options” section.

40. Fill in the Client security options to indicate the correct options for Client Certificates, for TTLS, etc. **Uncomment** (or even add) what is indicated. (Order might be different in what you see.)

```
SECURE_FTP      ALLOWED
SECURE_MECHANISM TLS
TLSMECHANISM    ATTLS
```

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

```
SECURE_CTRLCONN PRIVATE
SECURE_DATACONN PRIVATE
SECURE_HOSTNAME OPTIONAL
;CIPHERSUITE SSL_NULL_MD5
;CIPHERSUITE SSL_NULL_SHA
;CIPHERSUITE SSL_RC4_MD5_EX
;CIPHERSUITE SSL_RC4_MD5
;CIPHERSUITE SSL_RC4_SHA
;CIPHERSUITE SSL_RC2_MD5_EX
;CIPHERSUITE SSL_DES_SHA
;CIPHERSUITE SSL_3DES_SHA
;CIPHERSUITE SSL_AES_128_SHA
;CIPHERSUITE SSL_AES_256_SHA
;KEYRING name
TLSRFCLEVEL RFC4217
```

- a. NOTE: You might want to uncomment one of the CIPHERSUITE statements in order to see the effect when the equivalent statement is already specified in the policy. (I.e., MSG EZYFT47I would be triggered.)

41. Move to the “return codes” section of the file and include logging of client errors:

```
LOGCLIENTERR TRUE
```

42. Move to the “debugging options” section of the file and include logging of client errors:

```
DEBUG SEC
```

43. File the FTPCLSnx member with PF3.

- a. **PF3**

44. Exit the panel and go to the =3.4 view of datasets.

- a. Enter ‘**SYS1.PROCLIB**’ and view it.
b. Enter a “**B**” beside the **FTPT** member to view it.

45. Look at the **EXEC PGM=** lines and examine the Language Environment (LE) variables there.

- a. What does LE variable “_BPXK_SETIBMOPT_TRANSPORT=TCPIPT” do for the FTP procedure?

- b. What does TZ=EST5EDT do for the FTP procedure?

46. Look at the DD card for the SYSFTPD entry.

- a. What configuration dataset is this FTP server proc pointing to?

47. Close the member:

- a. **PF3**

48. Move into the OMVS shell from the ISPF Command line in order to configure Policy Agent:

- a. **TSO OMVS**

49. Verify with the UNIX command *pwd* that your current directory is /u/userx/.

Examples:

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

- a. Userid **user21** is positioned in **/u/user21 on MVS2**
 - b. Userid **user22** is positioned in **/u/user22 on MVS2**
 - c. Userid **user23** is positioned in **/u/user23 on MVS2**
 - d. Userid **user31** is positioned in **/u/user31 on MVS3**
 - e. Userid **user32** is positioned in **/u/user32 on MVS3**
 - f. Userid **user33** is positioned in **/u/user33 on MVS3**
 - g. **etc.**
50. Switch to SuperUser mode:
- a. **su**
51. Edit the pagentt.conf member that you created in an earlier lab:
- a. **oedit pagentt.conf**
52. Add the following line at the appropriate place in the file
- a. **TTLSSConfig /u/usernx/TMnx_ATTLS_FTP.policy FLUSH PURGE**
(where **nx** in “**usernx**” and “**TMnx**” is you team number)
 - i. This is the file you uploaded in the workstation part of these labs.
53. Close and File the new pagentt.conf file with a **PF3**.

Part 3: Testing the TCP/IP Stack and FTP with AT-TLS

1. Copy your version of the pagentt.conf file into the /etc/PAGT1/ directory, thus overlaying the current running copy of the configuration file:
 - a. **cp pagentt.conf /etc/PAGT1/**
2. Exit from Superuser mode in the UNIX shell.
 - a. **exit**
3. Exit from the UNIX shell itself:
 - a. **exit**
4. Return to previous ISPF location:
 - a. **Enter**
5. Return to the SDSF log
 - a. **=D.LOG**
6. From the SDSF command line enable TLS, disable TLS, and view the running config to confirm that the obeyfiles have been correctly coded:
 - a. **/V TCPIP,TCPIPT,OBEYFILE,USER.CS.TCPPARMS(TLSONnx)**
 - b. **/D TCPIP,TCPIPT,NETSTAT,CONFIG**
 - c. **/V TCPIP,TCPIPT,O,USER.CS.TCPPARMS(TLSOFFnx)**
 - d. **/D TCPIP,TCPIPT,N,CONFIG**
7. Now that you have successfully tested your obeyfiles, issue the enablement one again because we really do want AT-TLS enabled at this point.
 - a. **/V TCPIP,TCPIPT,O,USER.CS.TCPPARMS(TLSONnx)**
 - b. **/D TCPIP,TCPIPT,N,CONFIG**
8. Start the Secure version of the FTP Server with affinity to TCPIPT and pointing to the Server's FTP.DATA file that you customized in an earlier step:
 - a. **/P FTPT1** (bring down FTPT server – UNIX forked address space -- if it is running)
 - b. **/S FTPT,CS=USER,FDAT=FTPSECnx**
9. Display which traces are running for the FTP Server:
 - a. **/F FTPT1,DEBUG=?**
 - b. Which traces are running? _____
10. Enable more tracing at the FTP Server:
 - a. **/F FTPT1,DEBUG=(ACC,BAS,SEC)**
 - i. NOTE: You had already enabled SECurity tracing in the **FTP.DATA** file. You needed to re-enter this option; otherwise the new trace options REPLACE the old ones.
 - ii. NOTE: Later ... not now ... you will disable the trace with **F FTPT1,DEBUG=(NONE)**
 - iii. FTP debug options are documented in the IP Configuration Reference manual.
11. Next enter the command to cause Policy Agent to re-read only the changed policies:
 - a. **/F PAGENTT,UPDATE**
 - b. With the resulting message (EZZ8771I) you should see that the TTLS policy that you coded has been installed into TCPIPT. You may find that PAGENT had already installed the new policy because changes to unix policy files are automatically picked up.

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

12. Move to the job log of the TCPIPT stack that the ATTLS policies have been loaded into:
 - a. Display active jobs
 - i. **DA**
 - b. Select the TCPIPT job
 - i. **S TCPIPT**
 - 1) Enter an “S” next to the line with ‘TCPIPT’ in it to view the joblog.
13. **Browse** through the lines issued by System SSL on behalf of the stack because AT-TLS has been enabled. (The messages will not appear if the AT-TLS policies have not been loaded.) (The SSL messages may be different due to version and release changes.)
 - System SSL: SHA-1 crypto assist is available
 - System SSL: SHA-224 crypto assist is available
 - System SSL: SHA-256 crypto assist is available
 - System SSL: SHA-384 crypto assist is not available
 - System SSL: SHA-512 crypto assist is not available
 - System SSL: DES crypto assist is available
 - System SSL: DES3 crypto assist is available
 - System SSL: AES 128-bit crypto assist is available
 - System SSL: AES 256-bit crypto assist is available
 - System SSL: AES-GCM crypto assist is available
 - System SSL: Cryptographic accelerator is not available
 - System SSL: Cryptographic coprocessor is not available
 - System SSL: Public key hardware support is not available
 - System SSL: ECC secure key support is not available.
 - System SSL: ICSF Secure key PKCS11 support is not available
 - System SSL: ICSF FMID is HCR77D1
 - a. NOTE: The System SSL Started Task allows you to display this information with a MODIFY command:
F GSKSRVR,DISPLAY CRYPTO
 - i. NOTE: If you want to display such output, you must start up the GSKSRVR task as documented in the SSL Programmer’s Guide. (***This procedure has not been customized on our systems.***)
14. Respond to these questions using the output from the display:
 - a. How many encryption and hashing algorithms have access to CPACF?
 - b. Note that AES 256-bit crypto assist is not available. This is not available until z15.
15. Return to the log and display the active applications.
 - a. **PF3**
 - b. **=D.LOG**
 - c. **/D A,L**
 - d. Has ICSF (Job name CSF) been enabled for this MVS image? _____

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

16. Next enter the NETSTAT command to view the TTLS policies installed in the TCPIPT stack:
 - a. **/D TCPIP,TCPIPT,NETSTAT,TTLS**
 - b. Do you see any TTLS sessions or connections yet? _____
 - c. Note that TTLS Group Actions are loaded and then return to the UNIX shell by issuing the command:
 - i. **TSO OMVS**
17. Switch to Superuser Mode:
 - a. **su**
18. Then issue the passearch command (with “-t”) in order to see only the TLS policies that have been installed in the TCPIPT stack:
 - a. **passearch -t > mypassearch**
19. Browse mypassearch and you see a consolidated list of the running policies.
 - a. **obrowse mypassearch**
 - i. Look for your AT-TLS policies and notice how your entries into the Configuration Assistant are now reflected in the displayed policies.
 - ii. Use **PF3** to exit from the file you are browsing.
20. Browse the messages from your FTP initialization.
 - a. **obrowse /var/CSLOG/syslogall.log**
 - b. If you left any items coded in FTP.DATA that are now coded in policies, like CIPHERSUITE you will see messages about those parameters being ignored in FTP.DATA (MSG EZYFT47I).
 - c. Browse through the log and when you are finish exit with **PF3**.
21. First you will test the FTP server at your MVS_n for TLS connections. Therefore you will be an FTP client at the Control MVS: MVS1. Follow these steps:
22. Create a PCOMM session to connect to TN3270 at TCPIP1 on the Control MVS1 system.
 - a. You should be telnetting into MVS1 (ZOS1) at **192.168.20.81**.
23. When you see the Message 10 screen from the TN3270 server, provide your User ID with the logon command that has been built for this system. (The logon command is named “TSO”, but it is a VTAM LOGON nevertheless.)
 - a. **TSO <userid>**
24. On the ISPF signon screen, provide the password you were given in class.
 - a. **<password>**
 - b. Press **ENTER**
25. Move to the Console of ZOS1:
 - a. **ISPF D.LOG**
26. Verify that TCPIPT, FTPT1, and PAGENTT are running:
 - a. At command line: **/D A,L**
 - i. Notice the applications that are running.
27. On the command line, move to Option 6 of ISPF:
 - a. **=6**
28. On the command line, enter the following FTP client command from the TCPIPT stack, request AT-TLS, point to the FTP Client Data File (which specifies AT-TLS security is allowed), and connect to the VIPA at your own MVS system:

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

```
FTP -r TLS -f '//SYS1.CS.TCPPARMS(FTPCLSEC)' -p  
TCPIPT -s 192.168.20.100 192.168.20.1ab
```

29. Whether or not the connection fails, re-execute the command. First exit FTP by entering **quit**. Then reissue the command with tracing (debugging= “-d”) enabled -- as follows:

```
FTP -r TLS -d -f '//SYS1.CS.TCPPARMS(FTPCLSEC)' -p  
TCPIPT -s 192.168.20.100 192.168.20.1ab
```

30. Examine the Client Connection Messages that you receive **before you login**.
- Note the messages about the AT-TLS policy for the client, VIPAs2VIPAs.
 - Note the >>> ftpAuthAttls message that appears.
 - Answer the following questions – the messages appear if you have coded DEBUG SEC in the client’s FTP data file:
 - What version of SSL or TLS has been negotiated? _____
 - What cipher was chosen? _____
 - Has FTP with AT-TLS been enabled for FIPS-140? _____
 - What is the meaning of this cipherspec 0A? (e.g., AES, or DES or 3DES, or something else?) _____
31. If the connection fails, investigate the MVS Console log, and the UNIX SYSLOG Daemon logs to find TTLS errors and to determine what the SSL Return Code is. You can interpret the SSL Return Codes using any of the following:
- The Internet pages found through search keywords “SSL Return Code”
 - The IP Diagnosis Manual (chapter on AT-TLS Return Codes)
 - The System SSL Programming Manual
32. When you get the connection to work, login to the FTP session.
- <username>**
 - <password>**
 - ENTER**
 - NOTE: You are using the Instructor version of the FTP Client DATA file because you are testing your FTP server with this command and not your own FTP client.
 - We have specified the following in the Client Data File to capture messages:
 - DEBUG SEC
 - LOGCLIENTERR TRUE
 - NOTE: On MVS1 we are collecting error messages for AT-TLS in /var/CSLOG/syslogall.log.
 - NOTE: If you encounter problems, you may want to raise the TRACE in the **TMnx_ATTLS_FTP.policy** file at YOUR OWN MVS to a value of **255** in order to examine the SSL error Return Codes. (Currently your policy logging is set at **only 2**.) Then REFRESH the procedure for PAGENTT, re-test, and look at the SYSLOG daemon log.
33. Issue the “dir” command to test the data connection.
- DIR**
34. Issue the command to view the connection status from the client perspective:
- LOCSTAT**
 - Find the security messages that prove this is a secure connection.
EZA2889I Authentication mechanism: TLS

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

EZA2890I Control connection protection: Private

EZA2891I Data connection protection: Private

35. Issue the command to view the connection status from the server perspective:
 - a. **STATUS**
 - i. Find the 211 response messages that prove this is a secure connection.
 - 211-Authentication type: TLS
 - 211-Control protection level: Private
 - 211-Data protection level: Private
36. While your FTP connection is still running, return to your MVS. Go to the console log at **MVS_n** and issue the command to see if TTL sessions are running:
 - a. **=D.LOG**
 - b. **/D TCPIP,TCPIPT,NETSTAT,TTLS**
 - c. Do you see a session count now? _____
37. Change back over to your MVS1 PComm session.
 - a. Log off the FTP session **on MVS1**:
 - b. **QUIT**
38. Enter ISPF command at MVS1 to view the Syslog Daemon log for messages about the client FTP connection:
 - a. **TSO OMVS**
 - b. **su**
 - c. **obrowse /var/CSLOG/syslogall.log**
39. After reviewing the syslogd file on MVS1, you have just completed testing the Secure FTP Server on your MVS_n system.
40. Back at your own MVS, browse the SYSLOG Daemon log to see if there are any messages about your FTP session.
 - a. **TSO OMVS**
 - b. **su**
 - c. **obrowse /var/CSLOG/syslogall.log**
41. Find a message that informs you that your FTP server at **MVS_n** requested a Client Certificate:
 - a. **FR2974 getUserIdAttls: Request certificate, size 958**
 - b. The FRxxxx message number may be different in your display depending upon z/OS release.
 - c. If the message does not appear the policy agent log level may not be set high enough to capture the message.
42. After examining the syslogd messages, enter the Option 6 of ISPF by executing the following command:
 - a. **PF3**
 - b. **exit**
 - c. **exit**
 - d. **Enter**
 - e. **= 6**
43. On the command line, enter the following FTP client command from the TCPIPT stack. Request AT-TLS, point to the FTP Client Data File (which specifies AT-TLS security is allowed), and connect to the VIPA at the "Control" MVS system (ZOS1):

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

```
FTP -r TLS -f '//USER.CS.TCPPARMS(FTPCLSnx)' " -p  
TCPIPT -s 192.168.20.1ab 192.168.20.100
```

- a. NOTE: We have specified the following in the Client Data File to capture messages:

```
DEBUG SEC  
LOGCLIENTERR TRUE
```

- b. We are collecting error messages for AT-TLS in /var/CSLOG/syslogall.log.
c. If you encounter problems, remember that you can raise the TRACE in the **TMnx_ATTLS_FTP.policy** file to a value of 255 in order to examine the SSL error Return Codes and messages. Then REFRESH the procedure for PAGENTT, re-test, and look at the SYSLOG daemon log.

44. Quit from the FTP connection and then reconnect with the debug option enabled:

```
FTP -r TLS -d -f '//USER.CS.TCPPARMS(FTPCLSnx)' "  
-p TCPIPT -s 192.168.20.1ab 192.168.20.100
```

45. **Prior to logging in**, examine the messages you receive about the connection.

- a. Is this an AT-TLS connection? _____
b. Is the connection "application-controlled" or not? _____
c. What version of SSL or TLS has been negotiated? _____
d. What cipher was chosen? _____
e. What is the meaning of this cipherspec? (e.g., AES, or DES or 3DES, or something else?) _____
f. Is **FIPS-140** enabled or not? _____

46. After logging in, issue the status command to determine the **FTP.DATA** values under which the MVS1 FTPT server is operating:

- a. **STAT**
b. Examine the messages having to do with the secured connection.
211-Authentication type: TLS
211-Control protection level: Private
211-Data protection level: Private
211-TLS security is supported at the RFC4217 level

47. Issue the local status command to determine the **FTP.DATA** values under which the MVS_n FTP client is operating:

- a. **LOCSTAT**
b. Examine the messages having to do with the secured connection.
EZA2889I Authentication mechanism: TLS
EZA2890I Control connection protection: Private
EZA2891I Data connection protection: Private

48. Issue the directory command to test the Data Connection for FTP:

- a. **DIR**

49. Exit from the FTP connection:

- a. **QUIT**

50. You have just completed testing the Secure FTP Client on your MVS system.

51. Edit the **TMnx_ATTLS_FTP.policy** file and raise the trace level from **2** to **255**.

Repeat the two FTP requests and then examine the log file again.

- a. **oedit TMnx_ATTLS_FTP.policy** and look for the **TRACE 2** setting for the FTP Server and FTP Client
i. Change the setting to **TRACE 255 for both the Server and Client**

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

- ii. File the policy with **PF3**.
- b. Exit from omvs:
 - i. **exit** twice
- 52. Return to the console at your MVS and issue the command to re-read the policy file to capture the new trace settings:
 - a. **=D.LOG**
 - b. **/F PAGENTT,UPDATE**
- 53. Return to **MVS1** and connect again as a client to the FTP server on your MVSn:
FTP -r TLS -f '//SYS1.CS.TCPPARMS(FTPCLSEC)' "
-p TCPIPT -s 192.168.20.100 192.168.20.1ab
- 54. Issue the **DIR** command a couple of times to test the Data Connection again:
 - a. **DIR**
 - b. **DIR**
 - c. **QUIT** (to leave the connection)
 - d. From your MVSn, test the client connection to MVS1 again:
FTP -r TLS -f '//USER.CS.TCPPARMS(FTPCLS*nx*)' " -p TCPIPT
-s 192.168.20.10n 192.168.20.101
- 55. **Log off MVS1.**
 - a. **PF3**
 - b. **exit**
 - c. **exit**
 - d. **Enter**
 - e. **PF3**
 - f. **PF3**
 - g. **LOGOFF**
- 56. **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.
- 57. Return to your MVS system.
- 58. Enter OMVS on your MVSn system to view the additional AT-TLS messages that have been generated for both the client and the server connections.
 - a. **TSO OMVS**
 - b. **su**
 - c. **obrowse /var/CSLOG/syslogall.log**
 - i. The messages show the contents of the AT-TLS negotiation flows including the offered cipher specs, the request for certificates, etc.
- 59. Once you have finished browsing these messages, exit the log and change the AT-TLS Log level back to 2 in the policy file.
 - a. **PF3** (to exit the log)
 - b. **oedit /u/usernx/TMnx_ATTLS_FTP.policy**
 - c. Change **TRACE 255** to **TRACE 2** that you previously edited.
- 60. Exit OMVS:
 - a. **exit** twice

End of AT-TLS FTP Lab

