

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

"Configuring Policy IP Filters"

Hands-on Lab Guide

(Configuring IP Filters)



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

Revision date -

Monday, 23 June 2025

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

Attention:

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

Acknowledgements:

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

Table of Contents

Part 0: Lab Description for Configuring Policy Agent for IP Filters	5
Part 1: Configure Filter-Only Policies to Permit FTP and CICS to Addresses 192.168.20.10n.....	6
Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1	6
Configure Filter-Only Connectivity Rule for CICS and FTP	8
Use the Actions pull-down to select Rules... ..	8
Part 2: Configuring IPsec Filter-Only Policies to Permit Connections from the Workstations to Address 192.168.20.10n for FTP and TN3270	16
Part 3: Configuring IPsec Filter-Only Policies to Permit Basic IP Services among all IPv4 Addresses.....	19
Sort the Connectivity Rules in the Correct Sequence and Complete the Definitions...	23
Send Your Configuration to zOSn.....	24
End of IP Filter Configuration Lab	25

Part 0: Lab Description for Configuring Policy Agent for IP Filters

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

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

Your Lab Instructor has provided you with your TEAM name, your MVS system number, your USERID, and your PASSWORD.

You will implement and test IPSec Filter-Only policies for “permit” and “deny”. ***You require TRMD in order to capture any logging that you may wish to enable.***

- You will test PINGS from your workstation to verify that they are permitted to your MVSn system.
- You will test from your class workstation to verify that non-secured FTP administrator traffic to 192.168.20.10n works with the filters you have implemented.
- You will test with a TN3270 Secure client from your class workstation to verify that AT-TLS administrator traffic is permitted with your Secure TN3270T server.
- You will also test your existing FTP AT-TLS Client and Server between ZOS1 and ZOSn at addresses 192.168.20.10n to verify that these connections still succeed, despite the presence of IP Filtering. We require IP Filtering only for these connections because the traffic is already protected with AT-TLS.
- You will test PING between your MVSn and MVS1 at 192.168.20.101 to verify that your filters still permit this type of activity.

In a later lab you will implement IP Filtering that “Permits with IPSec.”

The lab is divided into several sections:

- *Part 1: Configuring IPSec Filter-Only Policies to Permit Connections between Address 192.168.20.10n and 192.168.20.101 for FTP and CICS*
 - *Note that we do not test CICS. We include it as one of the traffic types to provide the definition experience only.*
- *Part 2: Configuring IPSec Filter-Only Policies to Permit Connections from the Workstations to Address 192.168.20.10n for FTP and TN3270*
- *Part 3: Configuring IPSec Filter Only Policies to Permit Basic IP services between all IPv4 addresses.*

Part 1: Configure Filter-Only Policies to Permit FTP and CICS to Addresses 192.168.20.10n

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.
5. If you get a “Locked” message, click on **Proceed**.

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

6. Use the technology pull-down to select **IPsec**.
7. Use the radio button to select TCP/IP stack **TCPIPT**.

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) » IPsec". Below the title, it says "3.1 Current Backing Store is Team21". A dropdown menu labeled "Select a TCP/IP technology to configure:" shows "IPsec" selected. To the right of this dropdown is a "Tools" button. Below the dropdown, there are tabs for "Systems", "Traffic Descriptors", "Security Levels", "Address Groups", "Requirement Maps", and "Reusable Rules". The "Systems" tab is active. It shows a table with columns: "System Group or Sysplex / System Image / Stack", "Type", "Status", "Install Status", "Release", and "Description". The table has three rows: "Default" (System Group, Complete), "ZOS2" (System Image, Complete), and "TCPIPT" (Stack, Incomplete). The "TCPIPT" row is selected with a radio button. Below the table, it says "Total: 3 Selected: 1". At the bottom, there are "Home" and "Save" buttons.

Network Configuration Assistant (Home) » IPsec

3.1 Current Backing Store is Team21

Select a TCP/IP technology to configure : IPsec

Tools

Systems Traffic Descriptors Security Levels Address Groups Requirement Maps Reusable Rules

Actions

No filter applied

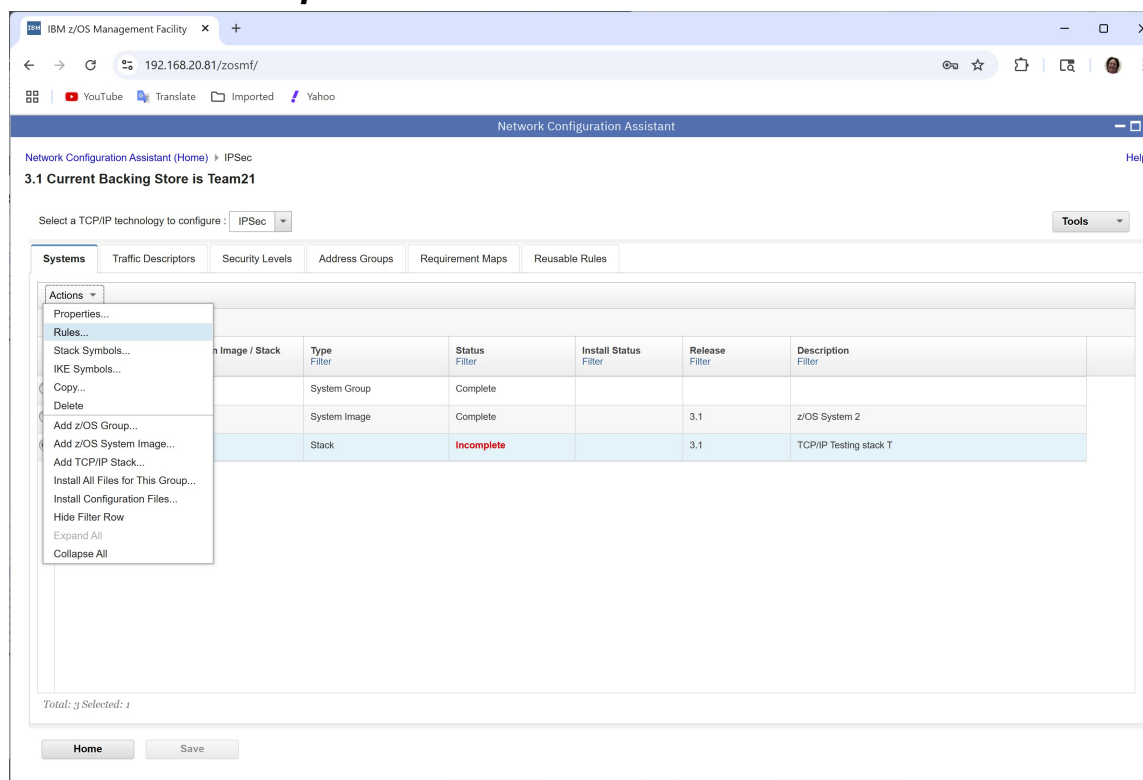
System Group or Sysplex / System Image / Stack	Type	Status	Install Status	Release	Description
Default	System Group	Complete			
ZOS2	System Image	Complete		3.1	z/OS System 2
TCPIPT	Stack	Incomplete		3.1	TCP/IP Testing stack T

Total: 3 Selected: 1

Home Save

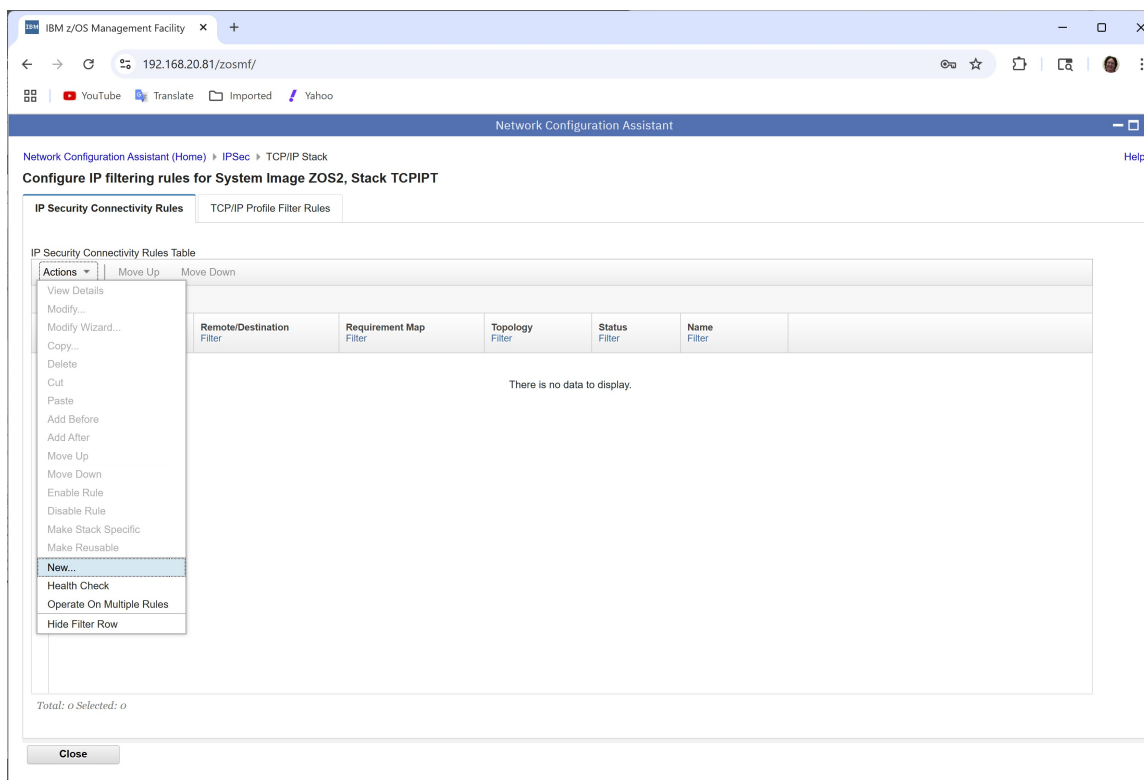
Configure Filter-Only Connectivity Rule for CICS and FTP

Use the Actions pull-down to select Rules...



1. Use the **Actions** pull-down to select **New...**

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

2. Accept the default **Typical** connectivity type.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant. 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) > IPsec > TCP/IP Stack > Connectivity Rule". The main heading is "New Connectivity Rule".

On the left, there is a sidebar with the following items:

- Welcome
- Welcome
- Typical
- Special Case: Mobile User
- Special Case: IP V6 OSPF IP Security
- Finish

The main content area is titled "Welcome" and says "Welcome to the connectivity rule wizard." Below this, there is a section "Indicate connectivity rule type" with three radio buttons:

- ☒ Typical
- ☐ Single reusable rule:
 - No reusable connectivity rules are defined
- ☐ Multiple reusable rules:
 - (Rule is not available for selection if it contains a symbol not defined for this stack.)

Below these options are two columns: "Available Data" and "Selected Data", each with a list box and a "Move" button. At the bottom of this section is a "Special case:" radio button with a dropdown menu showing "Mobile User".

Below the "Special case:" section, there is a paragraph explaining what a connectivity rule consists of:

A connectivity rule consists of the following:

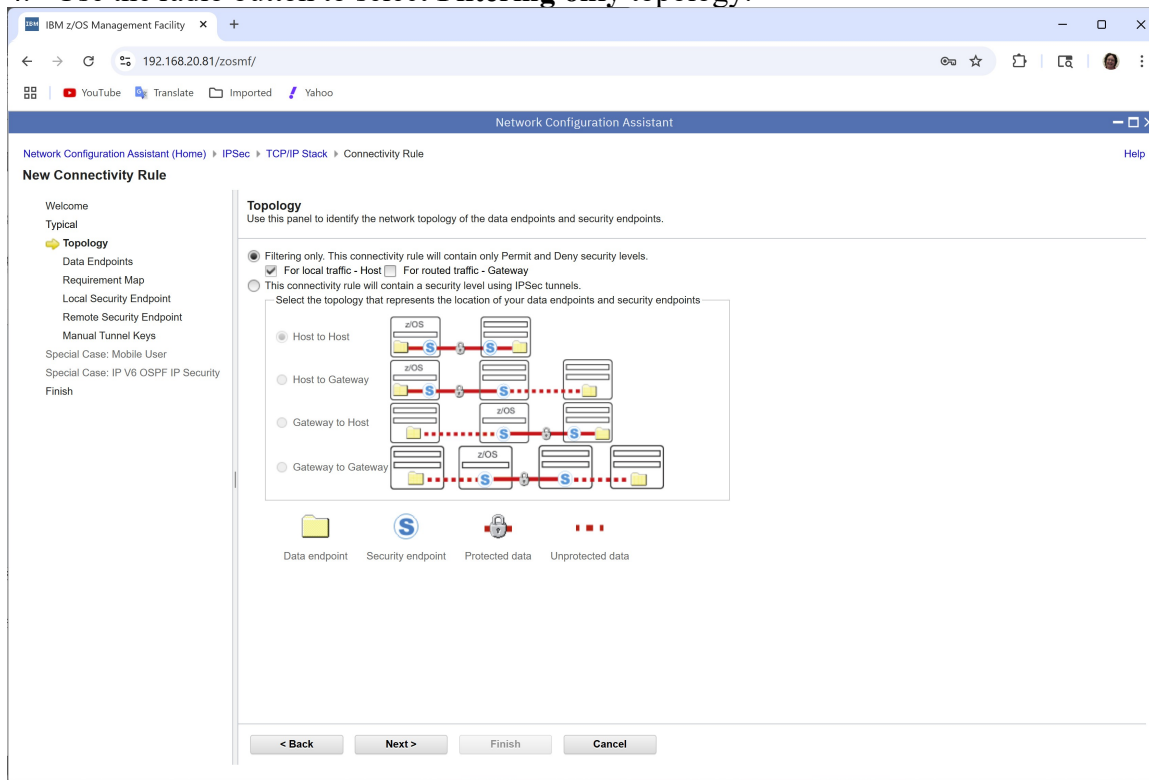
- Network topology - (only required when using IPsec tunnels)
- Data endpoints - may be single IP addresses or wildcarded
- A requirement map - which is a set of traffic descriptors mapped to security levels. This dictates behavior between the data endpoints.
- Security endpoints (if using IPsec tunnels in the selected requirement map) This indicates where IPsec tunnels begin and terminate.
- Additional information determined by your data endpoint and requirement map selections.

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

3. Click on the **Next** button.

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

4. Use the radio button to select **Filtering only** topology.



5. Notice how the default for **Filtering only** is to apply the filtering to **Local Traffic** – not routed traffic. We happen to be using this for local traffic but of course if you wanted a rule to apply to routed traffic you would just unselect local traffic here.
6. Click on the **Next** button.

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

7. Enter a Connectivity rule name of **TrafficBetweenVIPAs**.

The screenshot shows the 'Network Configuration Assistant' window. The breadcrumb trail is 'Network Configuration Assistant (Home) > IPSec > TCP/IP Stack > Connectivity Rule'. The left sidebar shows a tree view with 'Data Endpoints' selected. The main panel is titled 'Data Endpoints' and contains the following fields:

- * Connectivity rule name:** TrafficBetweenVIPAs
- Local data endpoint:**
 - ☐ Address group: All_IPv4_Addresses
 - ☒ * IPv4 or IPv6 address, subnet, or range: 192.168.20.101
 - Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y, x::x, x::x/yyy, x::x-y::y
 - ☐ Stack Symbol name: No stack symbol names are configured.
- Remote data endpoint:**
 - ☐ Address group: All_IPv4_Addresses
 - ☒ * IPv4 or IPv6 address, subnet, or range: 192.168.20.100
 - 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

At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

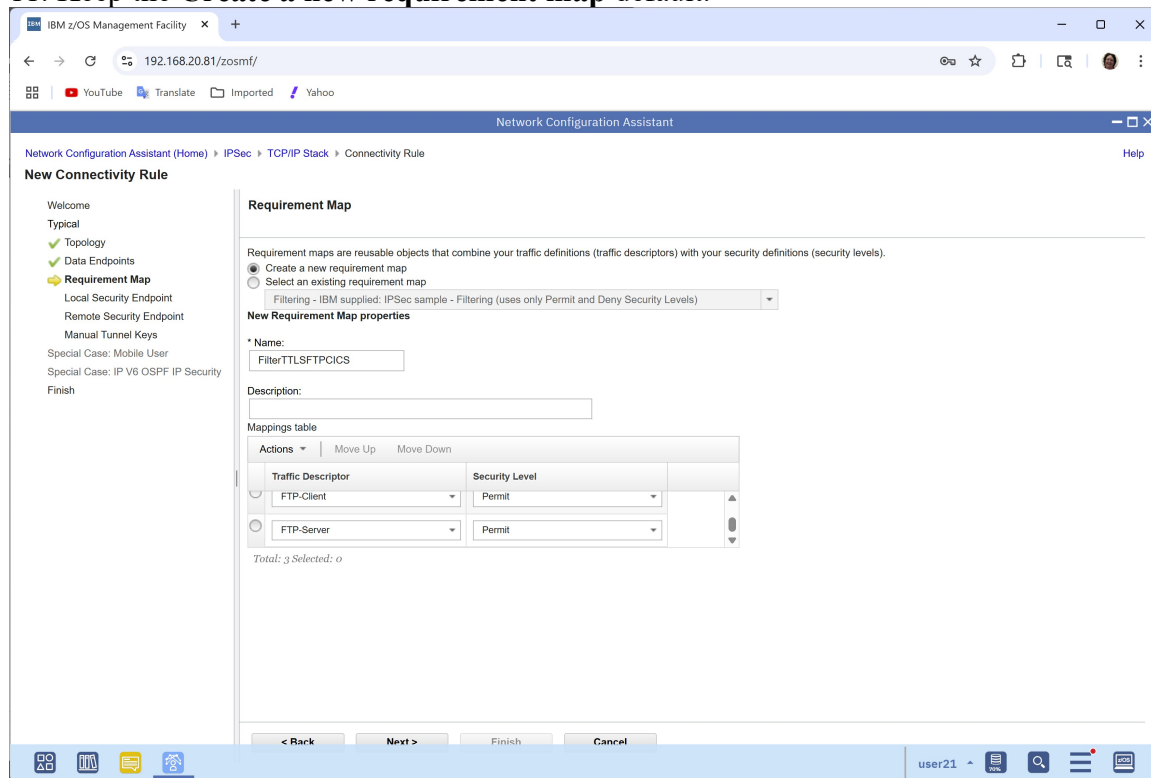
8. Enter Local data endpoint specific address **192.168.20.1ab** (your z/OS system).

9. Enter the Remote data endpoint specific address **192.168.20.100** (at ZOS1).

10. Click on **Next**.

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

11. Keep the **Create a new requirement map** default.

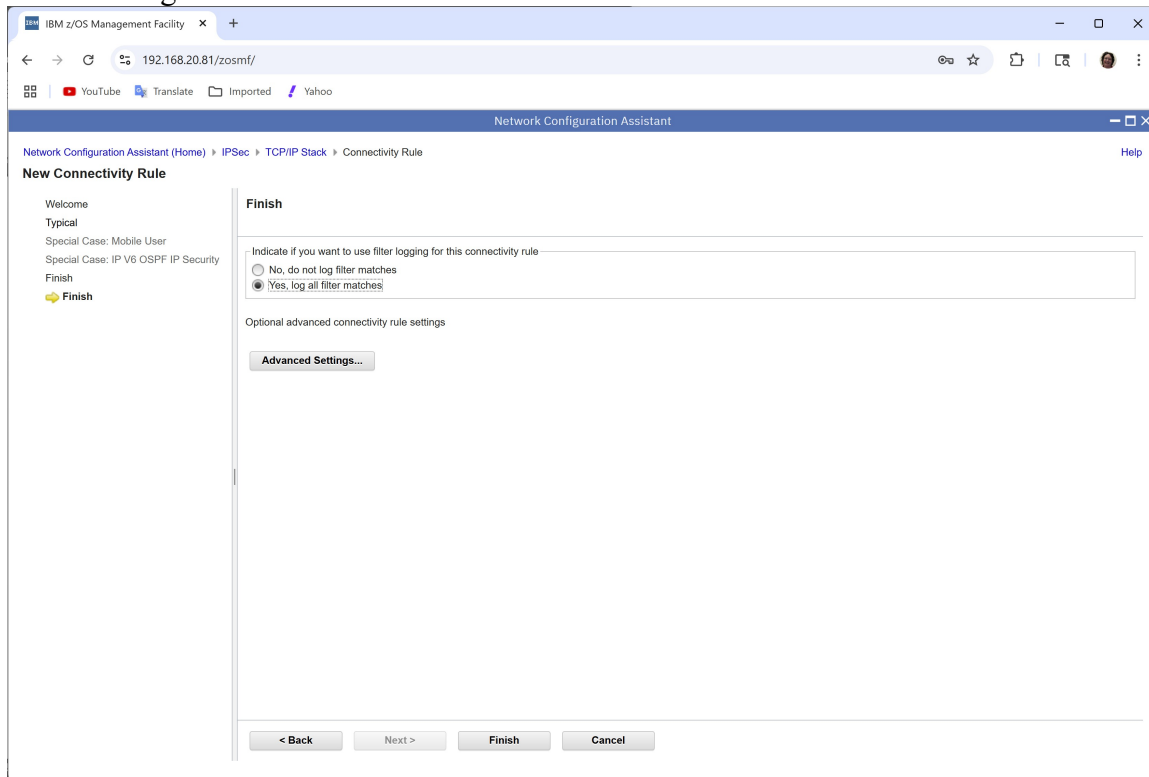


12. Enter a new Requirement Map Name of **FilterTTLSTPCICS**, and optionally add a description.
13. If necessary, use the **Actions** pull-down to select **Add Row**.
14. Use the pull-down for the traffic descriptor field in the **first** row to select **CICS**.
15. Use the pull-down for the traffic descriptor field in the **second** row to select **FTP-Client**.
16. Use the pull-down for the traffic descriptor field in the **third** row to select **FTP-Server**.
17. For each of those three rows:
 - a. Use the pull-down for the security level field to select **Permit**.
 - i. Note: Permit is for filters that do not require a VPN with encryption or authentication.
18. **If** there are any rows below the 3 that you just customized, use the radio button to select them and the **Actions** pull-down to select **Remove Row**.
 - a. Use scroll bar to view all rows if necessary.
19. Click on **Next**.
20. Why are we creating IP Filter rules for FTP between VIPAs when we have already implemented AT-TLS policies for this traffic?

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

21. Select **Yes, log all filter matches**.

- While testing you may want to match all filter matches, or ...
- If your security auditor requires logging for all filter matches, you may need to leave this value enabled. Otherwise, disable this value once you have completed testing.

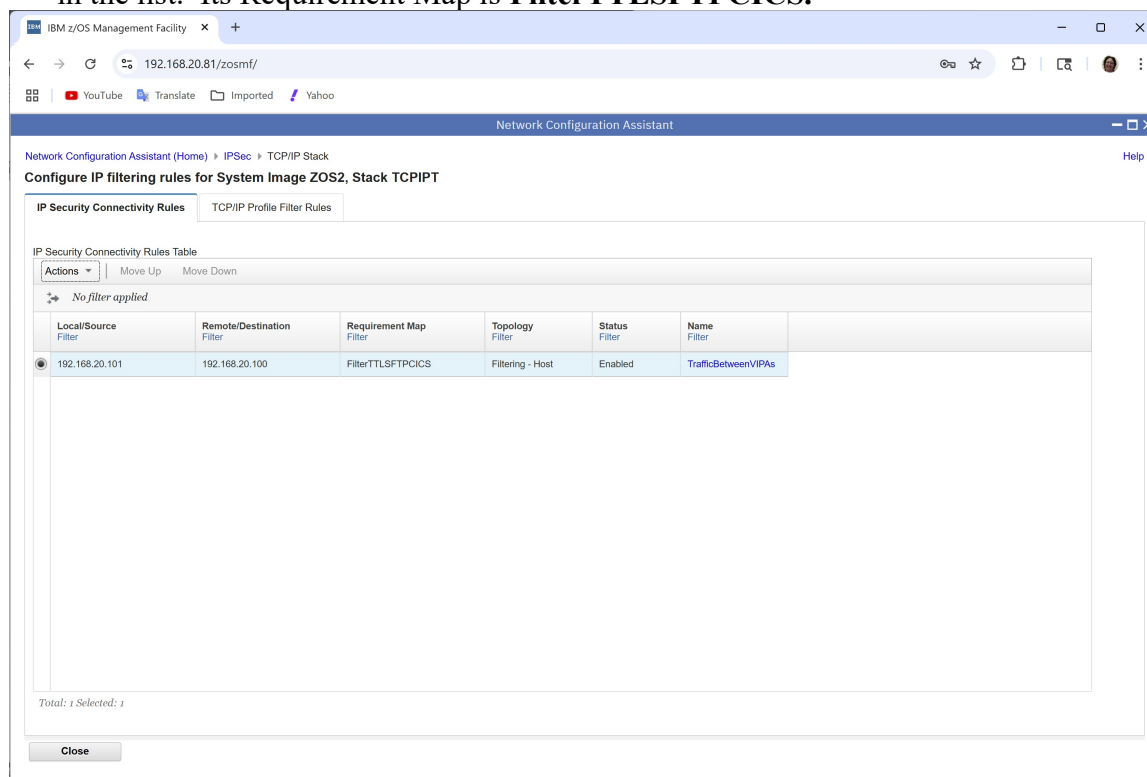


22. Feel free to check the **Advanced Settings**, clicking on **OK** after you are done.

23. Click on **Finish**.

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

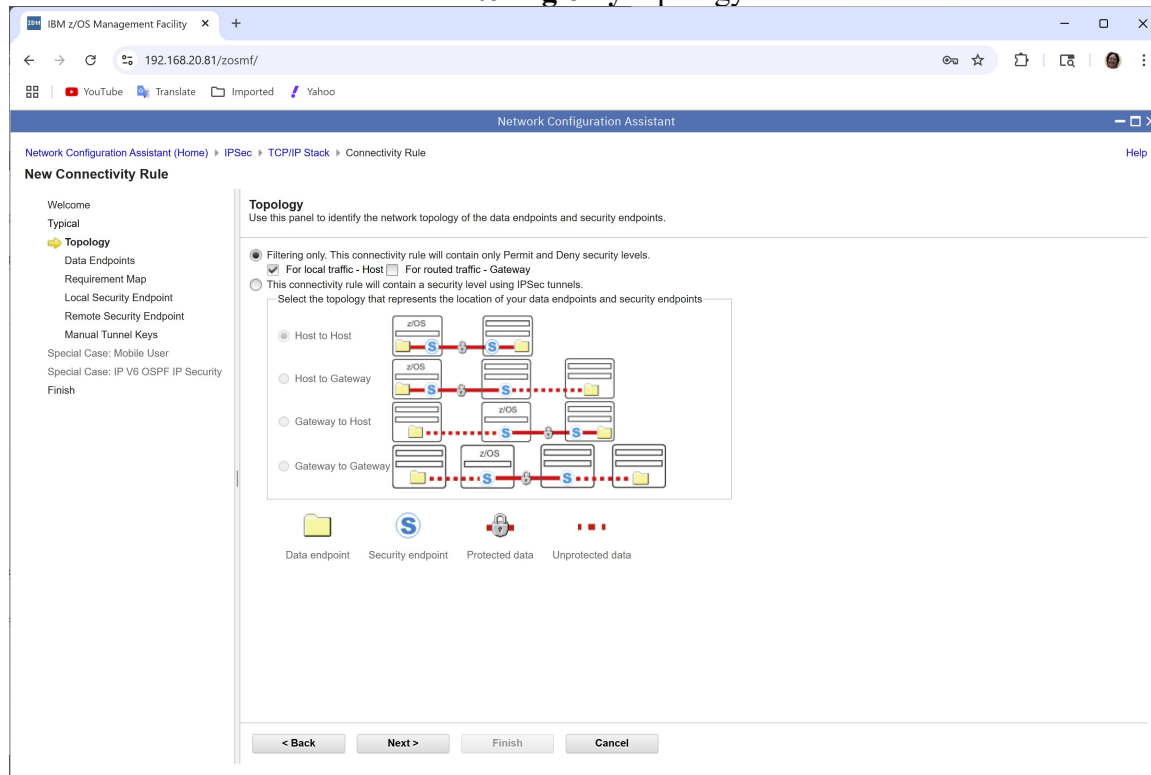
24. The Connectivity Rule that you just created, **TrafficBetweenVIPAs**, now appears in the list. Its Requirement Map is **FilterTTLSTPCICS**.



25. At this point you have created a rule to permit CICS and FTP Client/Server traffic to and from the ZOSn address of 192.168.20.10n. **Permit** is sufficient because this traffic will be encrypted with AT-TLS and does not require “double encryption” which is what you would achieve if you had created an IPsec VPN rule.

Part 2: Configuring IPSec Filter-Only Policies to Permit Connections from the Workstations to Address 192.168.20.10n for FTP and TN3270

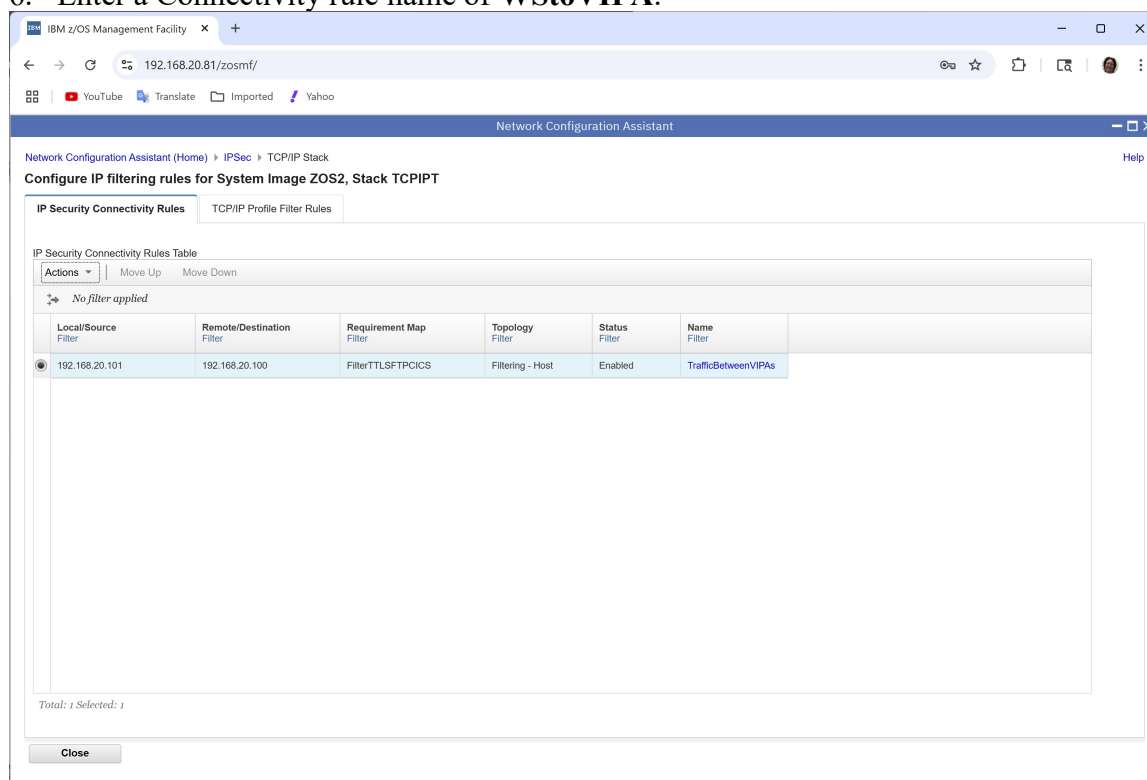
1. Use the **Actions** pull-down to select **New...**
2. Again, accept the default **Typical** connectivity type.
3. Click on the **Next** button.
4. Use the radio button to select **Filtering only** topology.



5. Click on the **Next** button.

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

6. Enter a Connectivity rule name of **WStoVIPA**.



7. Enter Local data endpoint specific address **192.168.20.1ab** (your z/OS system).
8. For Remote data endpoint select **Address Group: All_IPv4_Addresses**.
 - a. Any remote IPv4 address should be allowed to reach this VIPA under this rule.
9. Click on **Next**.

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

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

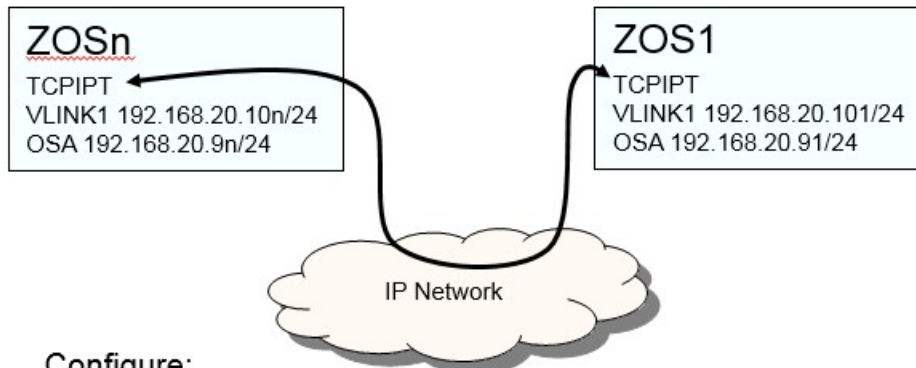
The screenshot shows the 'Network Configuration Assistant' window. The left sidebar has a tree view with 'Requirement Map' selected. The main area is titled 'New Requirement Map' and contains the following fields and controls:

- Requirement Map** section:
 - Requirement maps are reusable objects that combine your traffic definitions (traffic descriptors) with your security definitions (security levels).
 - Radio buttons: ☒ Create a new requirement map, ☐ Select an existing requirement map.
 - Filter: TSLFPCICS (dropdown menu).
- New Requirement Map properties** section:
 - * Name: WsFTPandTN3270 (text field).
 - Description: (empty text field).
- Mappings table** section:
 - Buttons: Actions (dropdown), Move Up, Move Down.
 - Table with 2 columns: Traffic Descriptor, Security Level.
 - Row 1: FTP-Server, Permit.
 - Row 2: TN3270-Server, Permit.
 - Footer: Total: 2 Selected: 1.
- Navigation buttons at the bottom: < Back, Next >, Finish, Cancel.

11. Enter a new Requirement Map Name of **WsFTPandTN3270**, and optionally add a description.
12. If necessary use the **Actions** pull-down to select **Add Row**.
13. Use the pull-down for the traffic descriptor field in the **first** row to select **FTP-Server**.
14. Use the pull-down for the traffic descriptor field in the **second** row to select **TN3270-Server**.
15. For each of those two rows:
 - a. Use the pull-down for the security level field to select **Permit**.
 - i. Note: Permit is for filters that do not require a VPN with encryption or authentication.
16. **If** there are any rows below the 2 that you just customized, use the radio button to select them and the **Actions** pull-down to select **Remove Row**.
17. Click on **Next**.
18. Select **Yes, log all filter matches**.
19. Click on **Finish**.
20. At this point you have created a rule to permit TN3270 and FTP traffic from your workstation (or any other IPv4 address) to the ZOSn address of 192.168.20.10n.

Part 3: Configuring IPSec Filter-Only Policies to Permit Basic IP Services among all IPv4 Addresses

1. Before you generate the configuration files, it is important to add a new Requirement Map to permit the basic services in the environment (such as PING, Resolver, DNS, and OMPROUTE traffic).



Configure:

Between MVS_n any IP address and any other IP address

DNS

ICMP Time Exceeded

ICMP Unreachable

OMPROUTE

Path MTU Discovery

Ping

Resolver

Trace Route

2. Use the **Actions** pull-down to select **New...**
3. Again, accept the default **Typical** connectivity type.
4. Click on the **Next** button.
5. Use the radio button to select **Filtering only** topology.
6. Click on the **Next** button.

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

7. Enter a Connectivity rule name of **CommonTraffic**.

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

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

New Connectivity Rule

Welcome

Typical

✓ Topology

✚ Data Endpoints

Requirement Map

Local Security Endpoint

Remote Security Endpoint

Manual Tunnel Keys

Special Case: Mobile User

Special Case: IP V6 OSPF IP Security

Finish

Data Endpoints

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

* Connectivity rule name:
CommonTraffic

Local data endpoint

☒ Address group:
All_IPv4_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:
Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x:x, x:x/yyy, x:x-y:y

☐ Stack Symbol name:
No stack symbol names are configured.

Remote data endpoint

☒ Address group:
All_IPv4_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:
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

8. For Local and Remote data endpoint select **Address Group: All_IPv4_Addresses**.

9. Click on **Next**.

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

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

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

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

New Connectivity Rule

Welcome

Typical

✓ Topology

✓ Data Endpoints

✚ **Requirement Map**

Local Security Endpoint

Remote Security Endpoint

Manual Tunnel Keys

Special Case: Mobile User

Special Case: IP V6 OSPF IP Security

Finish

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

WsFTPandTN3270

New Requirement Map properties

* Name: BasicServices

Description:

Mappings table

Actions	Traffic Descriptor	Security Level
<input type="radio"/>	Resolver	Permit
<input type="radio"/>	Trace_Route-IP_V4	Permit

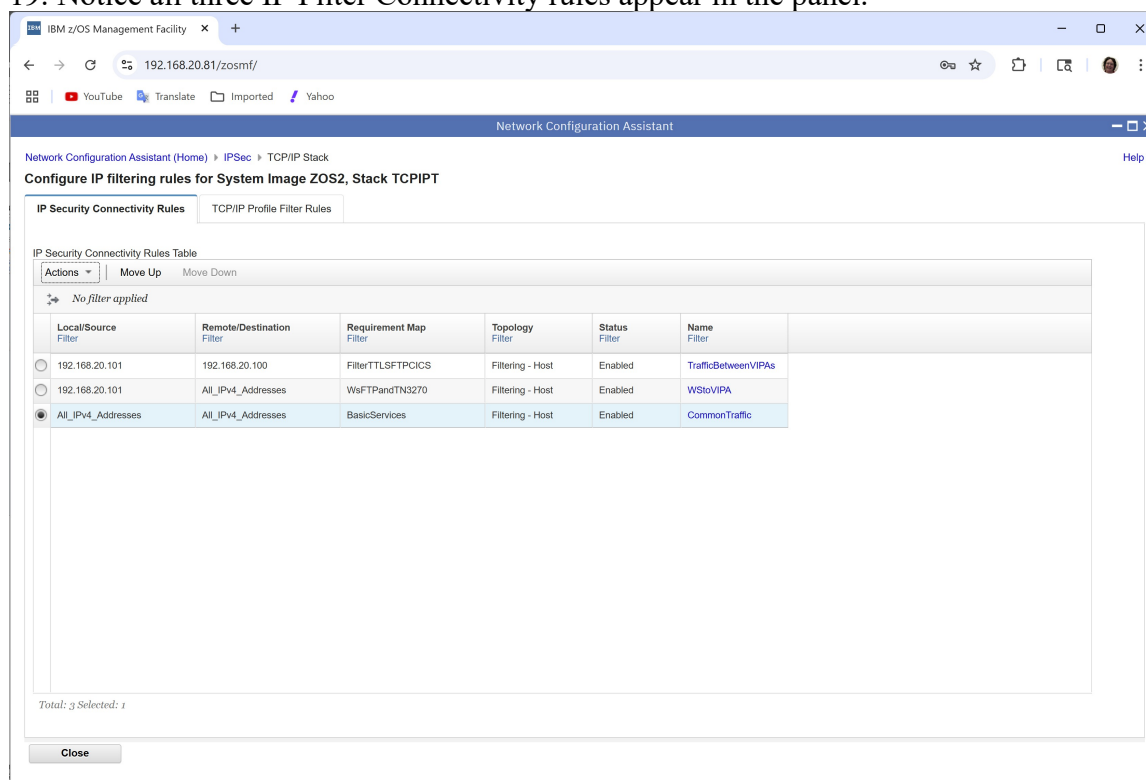
Total: 8 Selected: 0

< Back Next > Finish Cancel

11. Enter a new Requirement Map Name of **BasicServices**, and optionally add a description.
12. If necessary use the **Actions** pull-down to select **Add Row**.
13. Use the pull-down for the traffic descriptor field in each row in turn to select:
 - a. **DNS**.
 - b. **ICMP-Time_Exceeded-IP_V4**
 - c. **ICMP-Unreachable-IP_V4**
 - d. **OMPROUTE-IP_V4**
 - e. **Path_MTU_DiscoveryIP_V4**
 - f. **PingIP_V4**
 - g. **Resolver**
 - h. **Trace_Route-IP_V4**
14. For each of those rows:
 - a. Use the pull-down for the security level field to select **Permit**.
15. **If** there are any rows below the ones that you just customized, use the radio button to select them and the **Actions** pull-down to select **Remove Row**.
16. Click on **Next**.
17. Select **Yes, log all filter matches**.
18. Click on **Finish**.

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

19. Notice all three IP Filter Connectivity rules appear in the panel.



Sort the Connectivity Rules in the Correct Sequence and Complete the Definitions

1. The IP addresses in a packet are compared with the IP addresses of the data endpoints of the connectivity rules **in the order in which those rules appear in the table**.
2. Verify that the most Discrete or most Unique rule is found first, after which more general rules follow. The correct sequence should be as depicted in the previous screen shot. If it is not:
 - a. Select one rule at a time.
 - b. Use the **Actions** pull-down to select the **Move Up** or **Move Down** until the sequence is correct.
3. Use the Actions pull-down to select **Health Check** to check for any configuration errors.

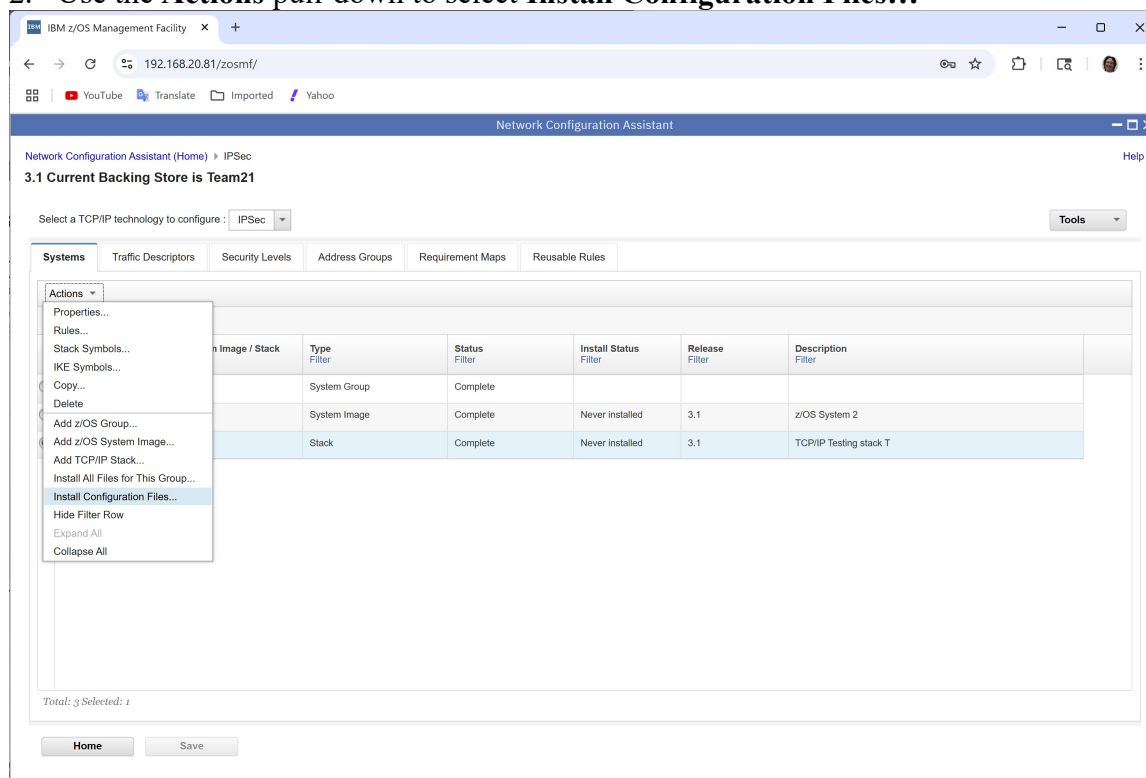
The screenshot shows the 'Network Configuration Assistant' window with the 'Health Check for IPSec' tab selected. Below the title bar, there are buttons for 'Close' and 'Printable page'. The main content area displays the 'Health Check: IPSec' results, including a table of IPSec connectivity rules. The table has columns for Connectivity Rule, Traffic Descriptor, IPSec Security Level, Index, Protocol, Local Port, Remote Port, Connect Direction, Type Code, Direction, Routing, and Security Class. The rules are listed in the order as defined, starting with CICS and ending with ICMP-Unreachable-IP_V4.

Connectivity Rule	Traffic Descriptor	IPSec Security Level	Index	Protocol	Local Port	Remote Port	Connect Direction	Type Code	Direction	Routing	Security Class ¹
TrafficBetweenVIPAs	FTP-Client	Permit	1	TCP	3000	1024-65535	Inbound	---	Either	Local	0
		Permit	2	TCP	1024-65535	21	Outbound	---	Either	Local	0
		Permit	3	TCP	1024-65535	20	Inbound	---	Either	Local	0
		Permit	4	TCP	1024-65535	50000-50200	Outbound	---	Either	Local	0
192.168.20.101 192.168.20.100 Filtering - Host	FTP-Server	Permit	5	TCP	21	1024-65535	Inbound	---	Either	Local	0
		Permit	6	TCP	20	1024-65535	Outbound	---	Either	Local	0
		Permit	7	TCP	50000-50200	1024-65535	Inbound	---	Either	Local	0
WStoVIPA	FTP-Server	Permit	8	TCP	21	1024-65535	Inbound	---	Either	Local	0
		Permit	9	TCP	20	1024-65535	Outbound	---	Either	Local	0
		Permit	10	TCP	50000-50200	1024-65535	Inbound	---	Either	Local	0
192.168.20.101 All_IPv4_Addresses Filtering - Host	TN3270-Server	Permit	11	TCP	23	1024-65535	Inbound	---	Either	Local	0
		Permit	12	UDP	53	1024-65535	Both	---	Either	Local	0
		Permit	13	UDP	53	53	Both	---	Either	Local	0
		Permit	14	TCP	53	1024-65535	Both	---	Either	Local	0
		Permit	15	TCP	53	53	Both	---	Either	Local	0
	ICMP-Time_Exceeded-IP_V4	Permit	16	ICMP	---	---	Both	11/ All	Either	Local	0
		Permit	17	ICMP	---	---	Both	3/ All	Either	Local	0

4. When you are finished viewing the Health Check results click on the **Close** button twice.
5. Click on the **Save** button.
6. Optionally enter a comment and click on the **OK** button.
7. You have finished this section of the lab.

Send Your Configuration to zOSn

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



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

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

4. Change the Install file name to /u/usernx/TMnx_IPFilter.policy

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

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

Install File for Default.ZOS2.TCPIPT

* Install file name:
/u/user21/TM21_IPFilter.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

5. Select installation method **FTP**.
6. Your FTP information should appear from a previous lab:
 - a. Host name 192.168.20.8n.
 - b. User ID usernx.
 - c. Password
7. Click on **Go**.
8. Click on **OK** button twice.
9. Click on the **Close** button twice.

End of IP Filter Configuration Lab

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

