

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

"Implementing and Testing IP Filters in z/OS"

Hands-on Lab Guide

(Operating with IP Filters)



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 4

Part 1: Customize Pagent and TCP/IP Configuration on ZOSn for Default Stack Filters
and Policy Filters 5

Part 2: Test the IP Filter-only Policies: Profile vs. Policy Rules 7

 Part 2A: Testing the PROFILE Filter Rules 7

 Test your administrative access connections defined in the Profile IPSECRule and
 verify that they succeed: 9

 Part 2B: Test your Policy Agent Filter rules..... 10

End of IPFilter Lab 13

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 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).

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.

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.
- OPTIONAL: 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: Customize PAGENT and TCP/IP For IPSECURITY, Default Profile Filters, and Policy Filters**
- **Part 2: Test the Default Profile Filters and then the Policy Filters**

Part 1: Customize Pagent and TCP/IP Configuration on ZOSn for Default Stack Filters and Policy Filters

1. Using a PCOMM session, logon to Telnet at the **ZOSn** TCPIP1 stack using your userid **USERnx**.
 - a. Connect to **192.168.20.8n**
 - b. **TSO USERnx**
 - c. **<password>**
2. Go into the ISPF Primary Menu.
 - a. Enter **PDF**
3. Go to the OpenEdition/MVS selection screen.
 - a. Enter **O**
4. Invoke the OpenMVS POSIX Shell (OMVS).
 - a. Enter **4**
5. Switch to SuperUser mode.
 - a. Enter **su** on the Command line on the bottom of the window.
6. Edit the Pagent Configuration file you created in a previous lab.
 - a. **oedit pagentt.conf**
7. Add an IPsecConfig statement in the appropriate place in the file:
 - a. **IPsecConfig /u/usernx/TMnx_IPFilter.policy**
 - i. *IPsecConfig (IP Filter and IPsec VPN) policy file statement does not use FLUSH and PURGE.*
 - b. Save your changes to the file using **PF3** to exit from the file.
8. Return to the ISPF panel from the UNIX shell.
 - a. **Exit** (to exit SuperUser mode)
 - b. **Exit** (to exit the shell)
 - c. **Enter**
 - d. **PF3** (to exit the ISPF panels for OMVS)
9. Edit the PROFILE.TCPIP that will be used for IP Filtering and for IPsec VPNs.
 - a. Enter **=3.4**
 - b. At the Data Set List Utility Screen:
 - i. Enter **'USER.CS.TCPPARMS'**
 - ii. Press **Enter**
 - iii. Place an **"E"** next to the dataset to edit the contents.
10. Edit the profile **TCPnAIPS**.
 - a. Enter an **"S"** to the left of the **TCPnAIPS** member to select it for editing.

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

11. Note that TTLS is already enabled for you.
12. Add a source IP (SRCIP) statement for the connections to the MVS1 systems. (We ask you to do this just so that you can see how to influence the Source IP Addresses of connection requests without having to specify the Source IP Addresses in the connection request itself.)
 - a. Uncomment the SRCIP/ENDSRCIP section in the file:
SRCIP
DESTINATION 192.168.20.91 192.168.20.9n
DESTINATION 192.168.20.100 192.168.20.1ab
DESTINATION 192.168.20.109 192.168.20.1ab
DESTINATION 192.168.20.118 192.168.20.1ab
DESTINATION 10.1.1.0/24 10.1.1.n
ENDSRCIP
13. Note that IPCONFIG IPSECURITY is commented out. This is required for IP Filtering and IPsec both.
 - a. Uncomment the **IPCONFIG IPSECURITY** statement.
14. Note the commented out **IPSEC/ENDIPSEC** section in the file.
15. Create the **SYSDEFAULT** Rules that protect the stack until Policy Agent installs the **PAGENT** rules for IPSEC that you have coded.
 - a. Add the following lines:
IPSEC LOGENABLE LOGIMPLICIT
IPSECRULE * * NOLOG PROTOCOL OSPF
IPSECRULE * * NOLOG PROTOCOL 2
IPSECRULE * * LOG PROTOCOL TCP SRCPORT * DESTPORT 4159
IPSECRULE * 192.168.0.0/16 LOG PROTOCOL *
ENDIPSEC
 - b. IPSECRULE is documented in the IP Configuration Reference if there are any questions.
 - c. The last IPSECRULE allows administrative access from any terminal in this network **until** PAGENT policies for IPsec are installed in the TCP/IP stack.
16. Save and File the member:
 - a. **PF3**
17. Enter **PF3** three times to return to the Data Set Utility List panel.

Part 2: Test the IP Filter-only Policies: Profile vs. Policy Rules

You are going to test two types of Filters:

- Part 2A: The **Default Profile filters** coded with the IPSECRules inside the TCP/IP Profile
 - These rules permit you to PING, FTP, and TELNET from your workstation to both addresses in your stack: **192.168.20.9n and 192.168.20.1ab.**
 - **Exception:** If you test with Telnet and AT-TLS, then only the connection to **192.168.20.1ab** should succeed, because the AT-TLS policy was built for only this address.
- Part 2B: The **Policy Filter Rules** that you created with the z/OS Configuration Assistant
 - These rules permit you to PING to both addresses in your stack: **192.168.20.9n and 192.168.20.1ab.**
 - They permit you to connect via TN3270 only to **192.168.20.1ab.**
 - **They** permit you to FTP to **192.168.20.100** from **192.168.20.1ab** using AT-TLS protocols.

Part 2A: Testing the PROFILE Filter Rules

1. Go to the OpenEdition/MVS environment:
 - a. **TSO OMVS**
2. Display the IP Filters (“su” may be required):
 - a. **ipsec -f display -p TCPIPT > ipsec_disabled**
3. Why are you permitted to execute the “ipsec” command?
 - a. Because my userid or my group was permitted to the SERVAUTH class named:
4. Display the contents of the file named ipsec_disabled

 - a. **obrowse ipsec_disabled**
 - i. Note that IPsec has not been enabled.
EZD0861I Stack TCPIPT is not configured for IPSECURITY
 - b. Use **PF3** to exit out of obrowse.
5. Return to MVS so that you can implement the TCPIPT stack with the new profile that enables IPSECURITY:
 - a. If you were in SU mode, then Enter **Exit** (to exit from SuperUser mode)
 - b. Enter **Exit** (to exit from the omvs UNIX shell)
 - c. **Enter**
6. Go to the SDSF log.
 - a. Enter **=D.LOG**
7. Display active tasks:
 - a. **/D A,L**
8. Stop the TCP/IP Stack.

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

- a. **/P TCPIPT**
 - b. Note the FTP job, FTPT1, stops as well.
9. After TCPIPT stops, restart the TCP/IP Stack with the new IPsec profile.
 - a. **/S TCPIPT,CS=USER,PROF=TCPnAIPS**
10. Start your secure FTP Server.
 - a. **/S FTPT,CS=USER,FDAT=FTPSECnx**
11. Start the TRMDT procedure in order to capture IP Filtering messages in SYSLOGD:
 - a. **/S TRMDT**
12. Display active tasks:
 - a. **/D A,L**
13. The following procedures should be running on your MVS:
 - a. **TCPIP1**
 - b. **FTPCCL(1)**
 - c. **TN3270**
 - d. **TCPIPT** (started with profile TCPnAIPS)
 - i. Includes AT-TLS functionality
 - ii. Includes IPSecurity
 - e. **FTPT(1)**
 - f. **TN3270T**
 - g. **TRMDT(1)**
 - h. **PAGENTT**
 - i. (Technically we do not need PAGENTT to test the PROFILE rules, but we are also running AT-TLS for FTP and optionally for TN3270, which requires that we have PAGENTT enabled.)
14. Enter the OMVS environment again:
 - a. **TSO OMVS**
 - i. You may need to enter Superuser mode again:
su
15. Display the IP Filters:
 - a. **ipsec -f display -p TCPIPT > ipsec_defaults**
 - b. **obrowse ipsec_defaults**
 - c. What are the two types of rules that you see?
 - i. **SYSDEFAULT**_____
 - ii. **SYSDEFAULT**_____
 - d. Note that any policies defined in the TCP/IP profile with the IPSECR statements and the Implicit System Default Deny All rule are now loaded.
 - i. FilterName: **SYSDEFAULTRULE.1 – SYSDEFAULTRULE.4**
 - 1) The “Sysdefaultrules” rules were built from your IPSECRule statements.
 - 2) A single IPSECRule statement produces both outbound and inbound rules.
 - ii. FilterName: **SYSDEFAULTDENYRULE**
 - 1) By default there is ALWAYS a SYSDEFAULTDENYRULE pair for outbound and inbound.
 - iii. Use **PF3** to exit out of obrowse.

Test your administrative access connections defined in the Profile IPSECRule and verify that they succeed:

1. As an administrator, **Ping** and **FTP** without security *from your workstation* to the ZOSn addresses permitted in the stack's IPSECRules. Open a Command Prompt window and issue the following commands:
 - a. **ftp 192.168.20.1ab**
 - b. **ftp 192.168.20.9n**
 - c. **ping 192.168.20.1ab**
 - d. **ping 192.168.20.9n**
 - e. Why do all of these connections succeed?
 - i. Because the stack's IPSECRules permitted access to all ZOSn addresses regardless of the protocol or the port numbers.
IPSECRULE * 192.168.0.0/16 LOG PROTOCOL *
 - ii. Because the FTP Server was set up with AT-TLS to allow security but not to require security; therefore your session which was not using AT-TLS security could still succeed.
2. You will next test your access to TN3270. You must have completed the AT-TLS TN3270 lab for these steps to work. If you did not successfully complete the AT-TLS TN3270 lab then skip this step.
 - a. Logon to your own TN3270T at ZOSn system from your workstation emulator **AT-TLS** connection using the **VIPA 192.168.20.1ab** address (which is protected by AT-TLS)
 - i. This should **SUCCEED** because you added a Profile filter-only administrative policy with IPSECR to permit connection between workstations in **192.168.0.0/16** and z/OS.
 - b. Next change the address of your TN3270T connection to **192.168.20.9n**.
 - i. Why does this connection fail?

 - ii. The TN3270 server port is set up as a secure port only with no negotiation. Plus, the AT-TLS policy applies only to z/OS addresses in the range 192.168.20.101-192.168.20.107. Therefore, this connection is rejected because it is requesting TLS to a non-permitted IP address over this secure port.

Part 2B: Test your Policy Agent Filter rules

1. Return to OMVS and switch to superuser mode if it is not already set:
 - a. **su**
 2. Copy your version of the Pagent Configuration file into the /etc/PAGT1 directory.
 - a. **cp pagentt.conf /etc/PAGT1/**
 3. Exit from OMVS:
 - a. **exit** twice
 - b. **Enter**
 4. Go to the SDSF log.
 - a. Enter **=D.LOG**
 5. Update the running Policy Agent with the new rules:
 - a. **/F PAGENTT,UPDATE**
 - b. Note that IPSEC now appears in the response.
 6. Return to OMVS and display the *Pagent Policy* IP Filter rules with “ipsec”:
 - a. **TSO OMVS**
 - b. **su**
 - c. **ipsec -f display -p TCPIPT > ipsec_policyfilter**
 - d. **obrowse ipsec_policyfilter**
 - i. There are **no** *SYSDEFAULTRULES*. They have now been replaced by the policies defined in the IPsec Pagent policy file.
 - ii. Note that **the Implicit System Default Deny All** rules are still at the bottom of the list although they is now called:
 - 1) **DenyAllRule_Generated_____Inbnd [or Outbnd]**
 - iii. Use **PF3** to exit out of obrowse.
 - e. NOTE: Until you stop the TCP/IP stack or reload the Default rules, these rules will stay in place to protect the stack. Even if you stop Policy Agent, the rules will not be flushed from the stack.
 7. Reload the Default Rules (the IPSECRule Profile Rules):
 - a. **ipsec -f default -p TCPIPT**
 - i. A useful command to temporarily switch between the IPsec policy sources.
 - ii. Note the messages:

```
# ipsec -f default -p TCPIPT
CS V2R4 ipsec Stack Name: TCPIPT Sun Jan 24 09:45:32 2021
Primary: Filter      Function: Default
Stack Profile filters now in effect
```
 8. Which policies are in effect? Stack Profile or Stack Policy?
-
9. Display the rules:
 - a. **ipsec -f display -p TCPIPT > ipsec_stackfilter**
 - b. **obrowse ipsec_stackfilter**
 - i. Observe how you now can see the *SYSDEFAULTRULES* and the *SYSDEFAULTDENY* rules again.
 10. You have already tested the Profile filter rules and know that:
 - a. *Pings to both 192.168.20.9n and 192.168.20.1ab succeed.*
 - b. *FTPs to both 192.168.20.9n and 192.168.20.1ab succeed.*

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

- c. *Telnetts with TLS to only 192.168.20.1ab succeed when you are running with Telnet profile of TNnATTLS.)*
- d. *Therefore you need not test this part again.*
- 11. Reload the Policy Agent Filter Rules:
 - a. **PF3**
 - b. **ipsec -f reload -p TCPIPT**
 - i. Note the messages:
ipsec -f reload -p TCPIPT
CS V2R1 ipsec Stack Name: TCPIPT Tue Mar 24 15:42:55 2015
Primary: Filter Function: Reload
Stack Policy filters now in effect
- 12. Which policies are in effect? Stack Profile or Stack Policy?
- 13. Display the Pagent Policies that you just reloaded:
 - a. **ipsec -f display -p TCPIPT > ipsec_policyfilter1**
 - b. **obrowse ipsec_policyfilter1**
 - c. Notice the policies are loaded again.
 - d. **PF3**
- 14. Verify that your AT-TLS FTP session from MVSn to MVS1 still works with the filters you have in place. Therefore, from TSO or OMVS:
 - a. **ftp -r TLS -p TCPIPT -f "'/USER.CS.TCPPARMS(FTPCLS*nx*)'" 192.168.20.100**
 - i. Because of the SRCIP block in the TCP/IP stack, you may omit the source IP specification on the command.
 - b. Use **quit** to exit from the FTP connection.
- 15. Next test your access to TN3270. You must have completed the AT-TLS TN3270 lab for these steps to work. If you did not successfully complete the AT-TLS TN3270 lab then skip this step.
 - a. Logon to your own TN3270T at ZOSn system from your workstation emulator AT-TLS connection using the **VIPA 192.168.20.1ab** address (which is protected by AT-TLS)
 - b. This should ***SUCCEED*** for two reasons:
 - i. You added a Policy Agent filter-only policy to permit connections to TN3270 and FTP at the VIPA address 192.168.20.1ab only from the "world".
 - ii. You created a TTLS policy to permit TN3270 connections to VIPA address 192.168.20.10n.
- 16. From your workstation: **Ping 192.168.20.9n**
 - a. Note: The pings will ***SUCCEED*** because MVSn is configured to permit PINGS from workstations to all IP addresses.
- 17. From your workstation: **Ping 192.168.20.1ab**
 - a. Note: The pings will ***SUCCEED*** because MVSn is configured to permit PINGS from workstations to all IP addresses.
- 18. From your ZOSn system, ping the Control ZOS1 (MVS1) system:
 - a. From OMVS on your ZOSn:
 - i. **ping -p TCPIPT 192.168.20.91**
 - ii. **ping -p TCPIPT 192.168.20.100**

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

- b. or from TSO:
 - i. **ping 192.168.20.91 (TCP TCPIPT**
 - ii. **ping 192.168.20.100 (TCP TCPIPT**
 - c. NOTE: The pings will **SUCCEED** because you coded filter policies to permit PINGS to/from any IP address.
 - i. NOTE: Recall that you coded your TCP/IP stack with a SRCIP/ENDSRCIP block, which is why you did not have to include the source IP addresses on these ping commands from the ZOSn system.
 - ii. If you didn't have the SRCIP/ENDSRCIP statement in the profile you would have needed to include the source IP address as well.
 - 1) **OMVS ping -p TCPIPT -s 192.168.20.1ab 192.168.20.100 or**
 - 2) **TSO PING 192.168.20.100 (SRCIP 192.168.20.1ab TCP TCPIPT**
19. Use the pasearch command to display the filter policies:
- a. **pasearch -p TCPIPT -v f > mypasearch_filter1**
 - b. What is the name of the SERVAUTH class that permitted you to execute the "pasearch" command"?
-
- c. **obrowse mypasearch_filter1**
 - d. The TrafficBetweenVIPAs policy that you created allows all traffic between the class guest VIPA 192.168.20.10n addresses.
 - e. When you finish reviewing the output issue **PF3**.
20. View the syslogd information following the directions from the previous lab.
- a. **obrowse /var/CSLOG/syslogall.log**
 - b. You may review your policy matches generated when the traffic matched a policy that you created.
21. Return to the MVS console and stop the running PAGENTT procedure:
- a. **/P PAGENTT**
22. Return to OMVS to determine whether the IPSec policies have been removed from the running TCP/IP stack:
- a. **TSO OMVS**
 - b. **su**
 - c. **pasearch -p TCPIPT -v f > mypasearch_filter2**
 - i. You will see an error, because pasearch cannot be executed without a running Policy Agent:
 - 1) **EZZ8436I pasearch Command: Connection Error 30**
23. We coded **FLUSH** (executed at PAGENT startup) and **PURGE** (executed at PAGENT shutdown) on our Policy Definitions and so the QoS and the AT-TLS policies will have been deleted from the running IP Stack. Check to see if the IP Filters have been deleted:
- a. **ipsec -f display -p TCPIPT > ipsec_policyfilter2**
 - b. **obrowse ipsec_policyfilter2**
24. Which filters have been left in the running TCP/IP stack?
- a. The Default Stack Filters? Yes? or No?
 - b. The Policy Filters? Yes? or No?
25. Return to the MVS console

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

- a. **Exit** twice
- b. **Enter**
- 26. Return to the MVS log
 - a. **D.LOG**
- 27. Start Policy Agent
 - a. **/S PAGENTT**

End of IPFilter Lab

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

