

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

"Building Intrusion Detection (IDS) Policies with IBM z/OS Configuration Assistant"

Hands-on Lab Guide

(IDS Exercises with Policy Agent)



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

Revision date -

Tuesday, 24 May 2022

This edition applies to IBM z/OS Configuration Assistant running in z/OSMV on z/OS V2.4.

Attention:

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

Table of Contents

Part 0: Lab Description for Configuring Intrusion Detection Services for z/OS.....	4
Specific Lab Diagram for Intrusion Detection Services	5
Part 1: Configuring an IDS Policy with z/OS Configuration Assistant.....	6
Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1	6
IDS for z/OS: Step-by-Step	7
Part 2: Installing the IDS Policy on Your z/OS Image	18
Part 3: Testing the TCP/IP Stack and TN3270T for the IDS Policies	19
Configure Personal Communications to Connect to TN3270T	20
End of IDS Lab	23

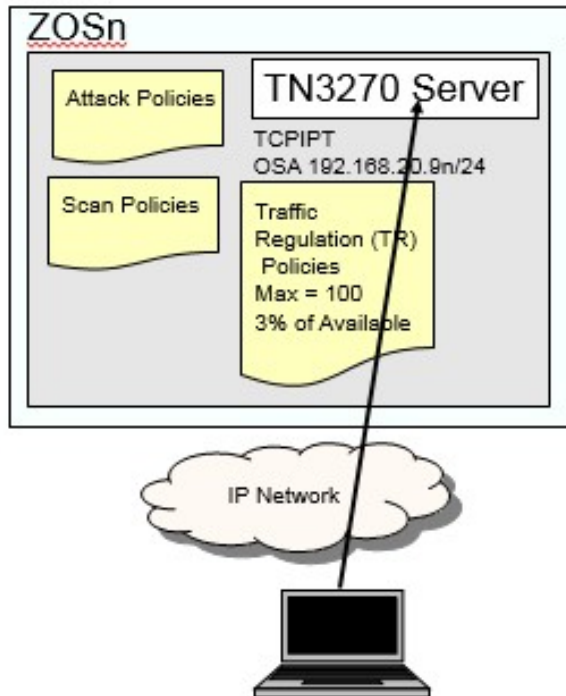
Part 0: Lab Description for Configuring Intrusion Detection Services for z/OS

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.

Specific Lab Diagram for Intrusion Detection Services



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.

As the diagram shows, you will configure an IDS policy that contains three types of rules:

1. ATTACK Rules
2. SCAN Rules
3. Traffic Regulation (TR) Rules

You will enable the ATTACK and SCAN rules.

You will also set up a TR Rule to permit only a total of 100 TN3270 connections. A single IP address is allowed to consume only 3% of the available connections. (A TR rule is implemented to prevent “hogging” of system resources: address spaces, CPU, etc.)

The lab is divided into several sections:

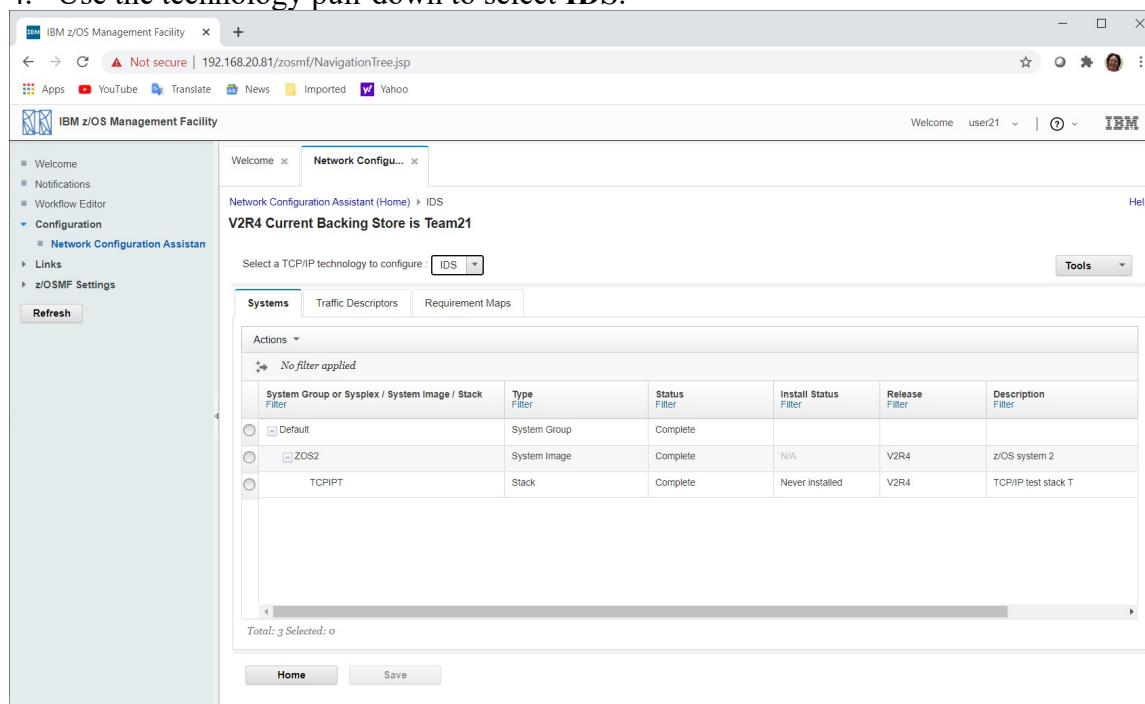
- **Part 1: Configuring an IDS Policy with z/OS Configuration Assistant.**
- **Part 2: Installing the IDS Policy into the TCPIPT stack.**
- **Part 3: Testing the TR policy for TN3270.**

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

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 technology pull-down to select **IDS**.

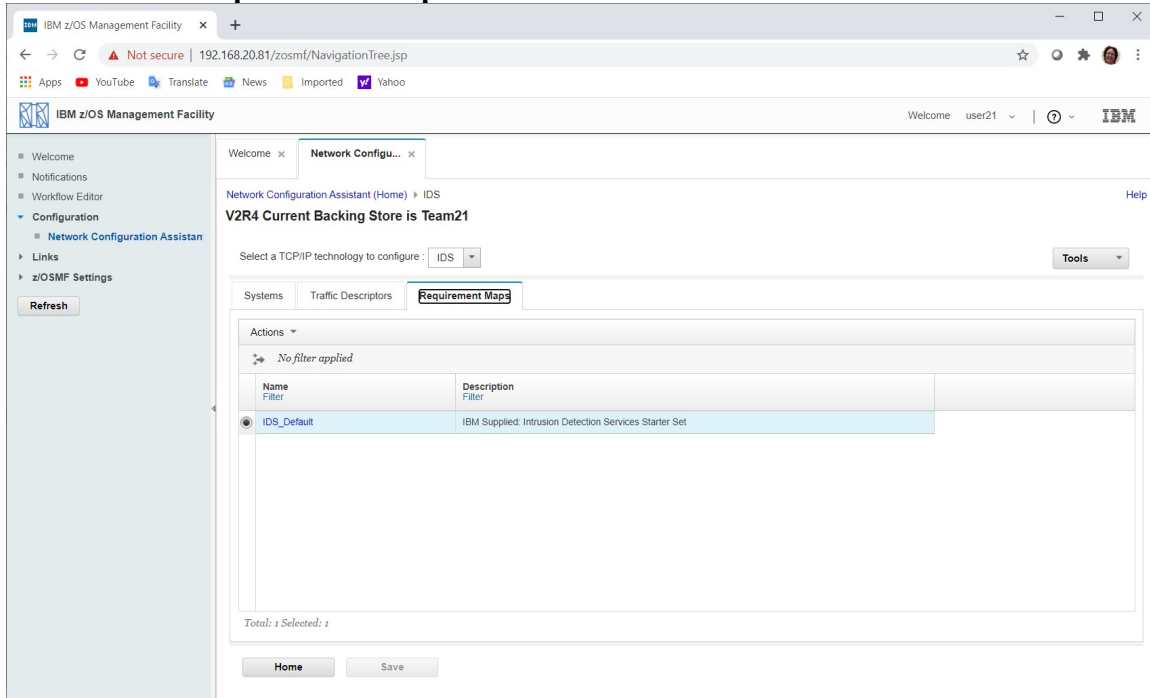


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

IDS for z/OS: Step-by-Step

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

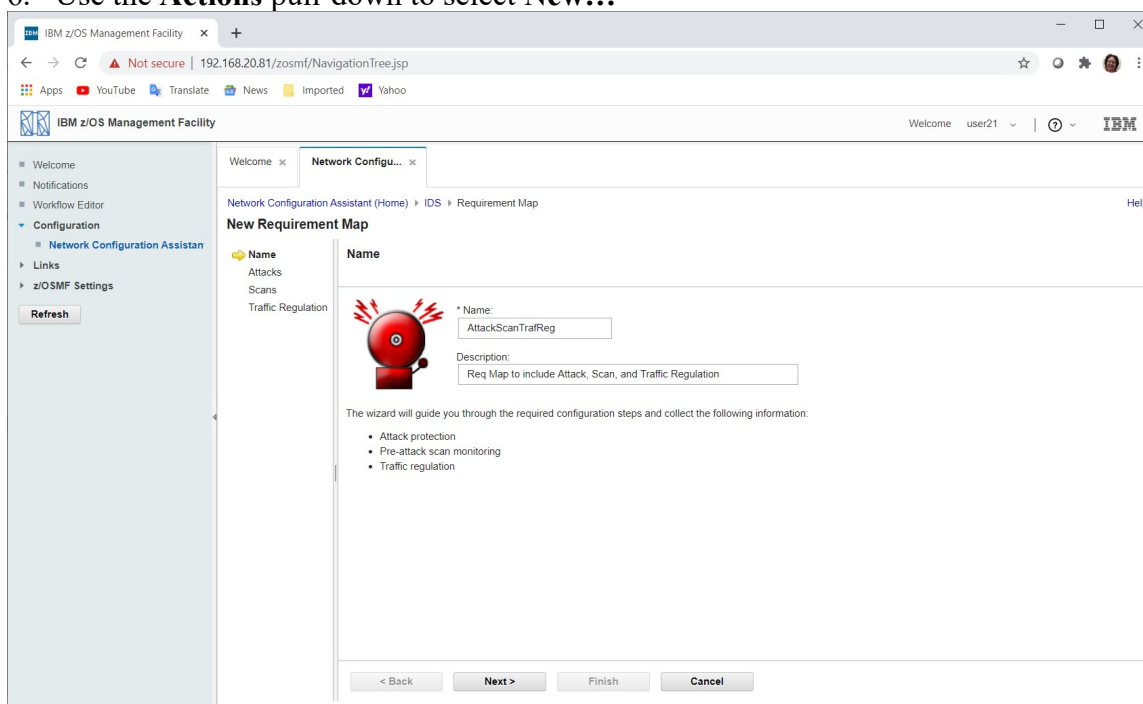
1. Select the **Requirement Maps** tab.



2. Notice there is a default IDS policy provided in the tool.
3. Use the **Actions** pull-down to select **View Details**.
4. Review the default IDS policy. It contains Attack policies but no Scan or Traffic Regulation policies. This default might be a good starting point for your site though.
 - a. There are other samples in “flat file” format in the unix TCP/IP sample directory, /usr/lpp/tcpip/samples, on z/OS.
5. When you are finished reviewing the default, use the **Close** button.

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

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

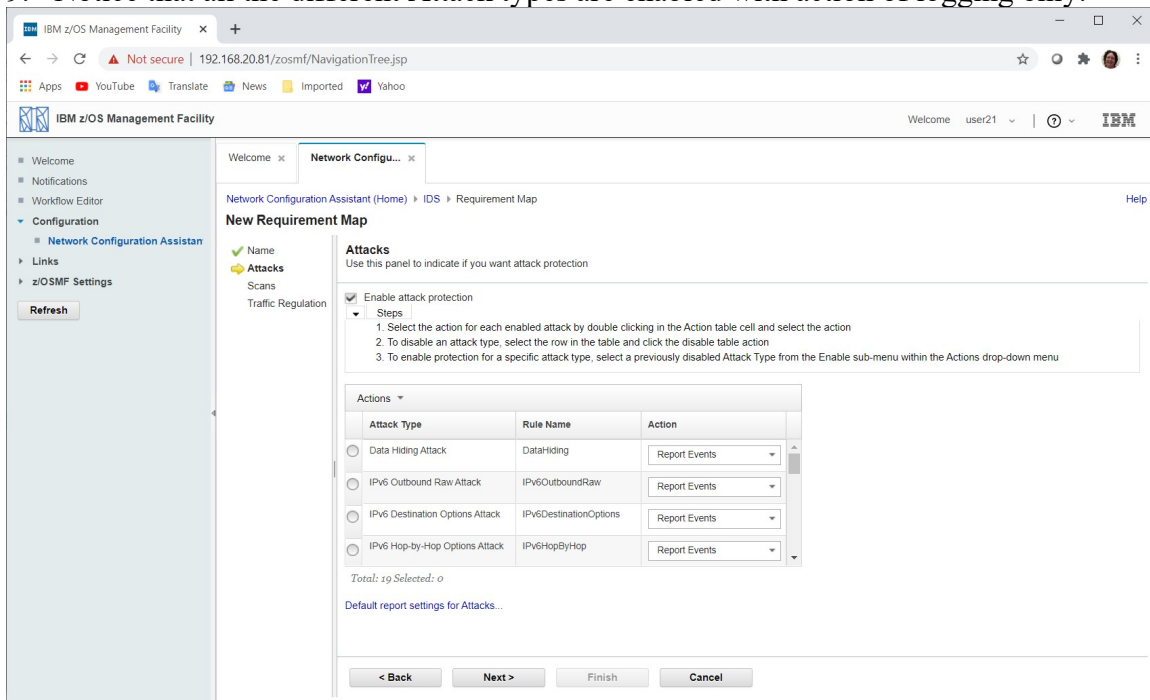


7. Name the Requirement Map **AttackScanTraffReg** and optionally add a description.

8. Click on the **Next** button.

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

9. Notice that all the different Attack types are enabled with action of logging only.



10. Expand the **Steps** arrow for further directions.

11. Click on the **Default report settings for Attacks...** link.

12. Review the default logging. When you are finished reviewing the options, click on the **Cancel** button.

13. Click on the **Next** button.

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

14. Click on the check box to **Enable scan**.

IBM z/OS Management Facility

Welcome user21

Network Configuration Assistant (Home) - IDS - Requirement Map

New Requirement Map

Scans

Use this panel to indicate if you want to monitor for preattack scans

☒ Enable scan

☐ Steps

1. To enable a scan for a particular traffic descriptor, select from the 'Enable' action sub-menu items

2. Select the monitor level for each enabled scan

3. To disable scan protection for a traffic descriptor, select the row in the enabled scans table and click the 'Disable' action

Enabled Traffic Descriptor	Rule Name	Sensitivity
<input type="radio"/> All_Well-Known_TCP	All_Well-Known_TCP	Medium
<input type="radio"/> All_Well-Known_UDP	All_Well-Known_UDP	Medium
<input type="radio"/> ICMP	ICMP	High

Total: 3 Selected: 0

Default report settings for Scans...

Modify Fast and Slow Scan Settings...

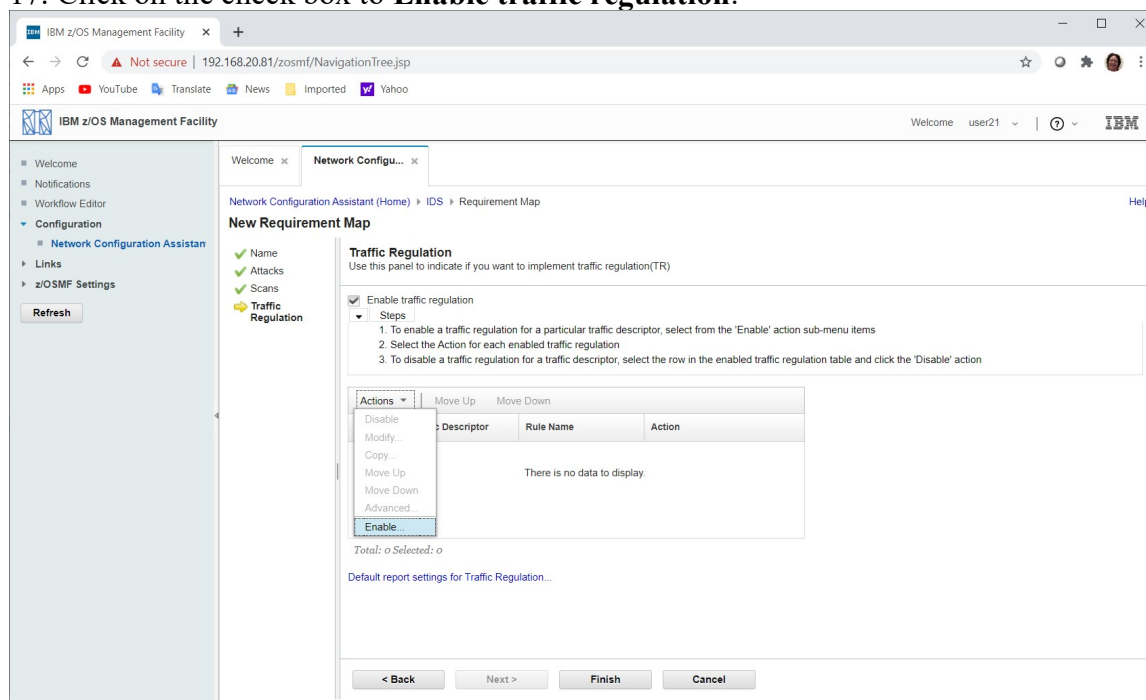
< Back Next > Finish Cancel

15. Expand the **Steps** arrow for further directions.

16. Accept the default Scan settings by clicking on the **Next** button.

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

17. Click on the check box to **Enable traffic regulation**.



18. Expand the **Steps** arrow for further directions.

19. Use the **Actions** pull-down to select **Enable**.

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

20. Enter Traffic Regulation Name **TN3270Limit**.

The screenshot shows the IBM z/OS Management Facility interface. The left sidebar contains a navigation tree with 'Configuration' expanded, showing 'Network Configuration Assistant' and 'z/OSMF Settings'. The main panel displays the 'Network Configuration Assistant (Home)' with a breadcrumb trail: 'IDS > Requirement Map > Traffic Regulation Details'. A 'New Traffic Regulation Details' dialog box is open, titled 'Network Configu...'. It contains the following fields:

- * Name: TN3270-Server
- * Traffic Descriptor: TN3270-Server
- Action: Limit and Report
- *Enter parameters for TCP traffic:
 - *Max number of connections: 100 (0-65535)
 - *Limit each host to the following percentage of the available connections: 3
 - Limit scope: Each socket

Buttons for 'OK' and 'Cancel' are at the bottom.

21. Use the Traffic Descriptor pull-down to select **TN3270-Server**.

22. Enter parameters for TCP traffic:

- Max number of connections **100**
- Limit each host to the following percentage of the available connections **3**
- Leave the default Limit scope “Each socket”

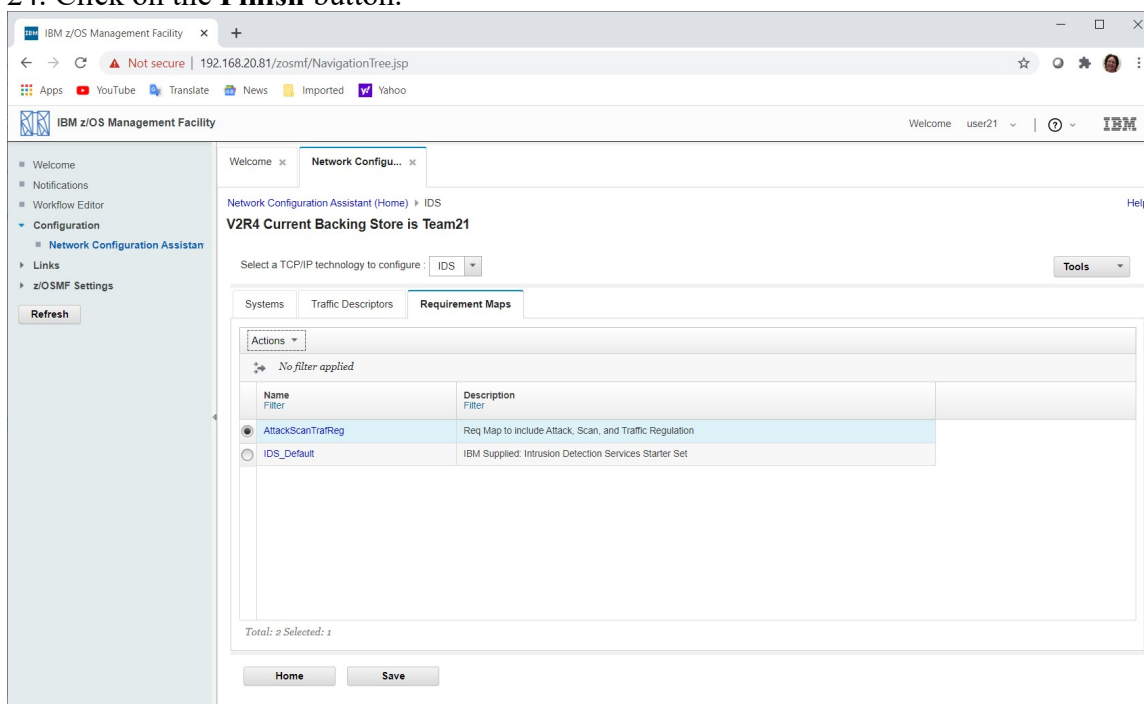
23. Click on the **OK** button.

The screenshot shows the IBM z/OS Management Facility interface. The left sidebar is the same as in the previous screenshot. The main panel displays the 'Network Configuration Assistant (Home)' with a breadcrumb trail: 'IDS > Requirement Map'. A 'New Requirement Map' dialog box is open, titled 'Network Configu...'. It contains the following sections:

- Checklist:** Name, Attacks, Scans, and Traffic Regulation (highlighted with a yellow icon).
- Traffic Regulation:** Use this panel to indicate if you want to implement traffic regulation(TR).
 - ☒ Enable traffic regulation
 - Steps:
 - To enable a traffic regulation for a particular traffic descriptor, select from the 'Enable' action sub-menu items
 - Select the Action for each enabled traffic regulation
 - To disable a traffic regulation for a traffic descriptor, select the row in the enabled traffic regulation table and click the 'Disable' action
- Table:** A table with columns 'Enabled Traffic Descriptor', 'Rule Name', and 'Action'. It contains one row: TN3270-Server, TN3270-Server, and Limit and Report.
- Buttons:** < Back, Next >, Finish, and Cancel.

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

24. Click on the **Finish** button.

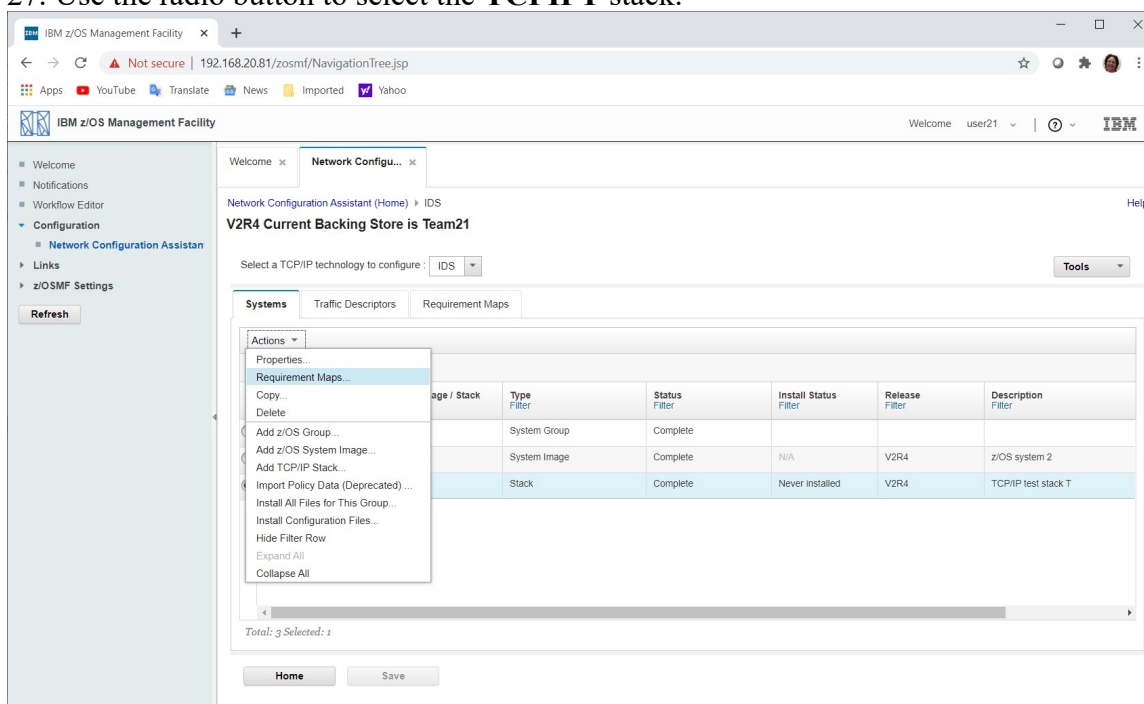


25. Click on the **Save** button, optionally enter a comment, and click on the **OK** button.

26. Select the **Systems** tab.

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

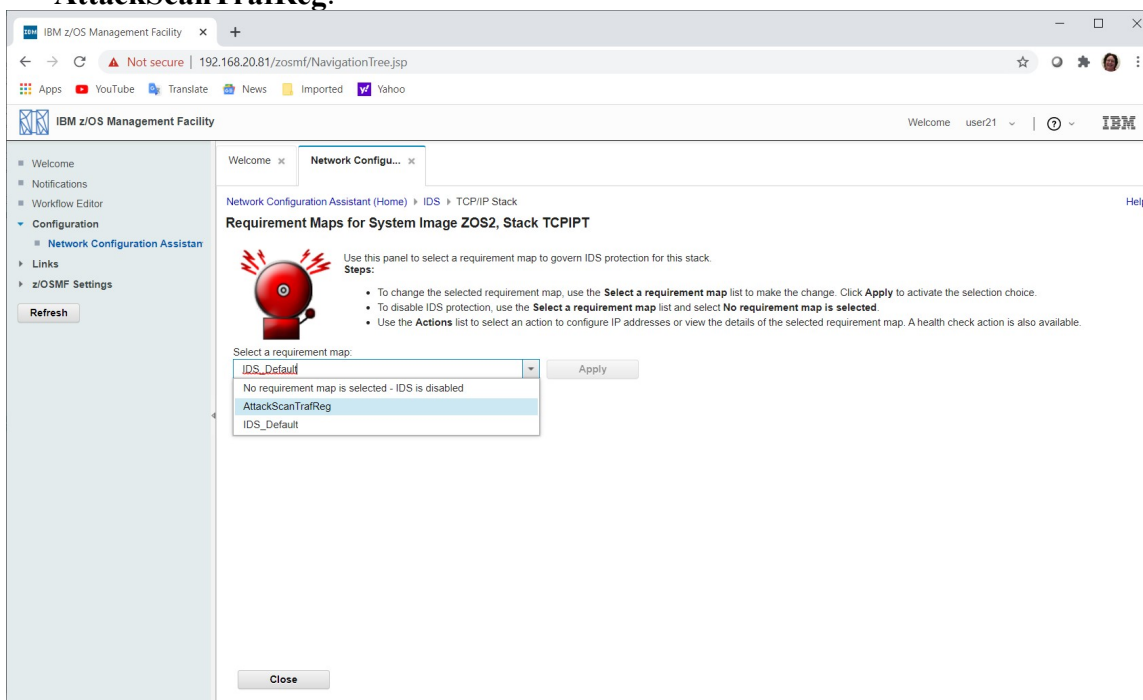
27. Use the radio button to select the **TCPIPT** stack.



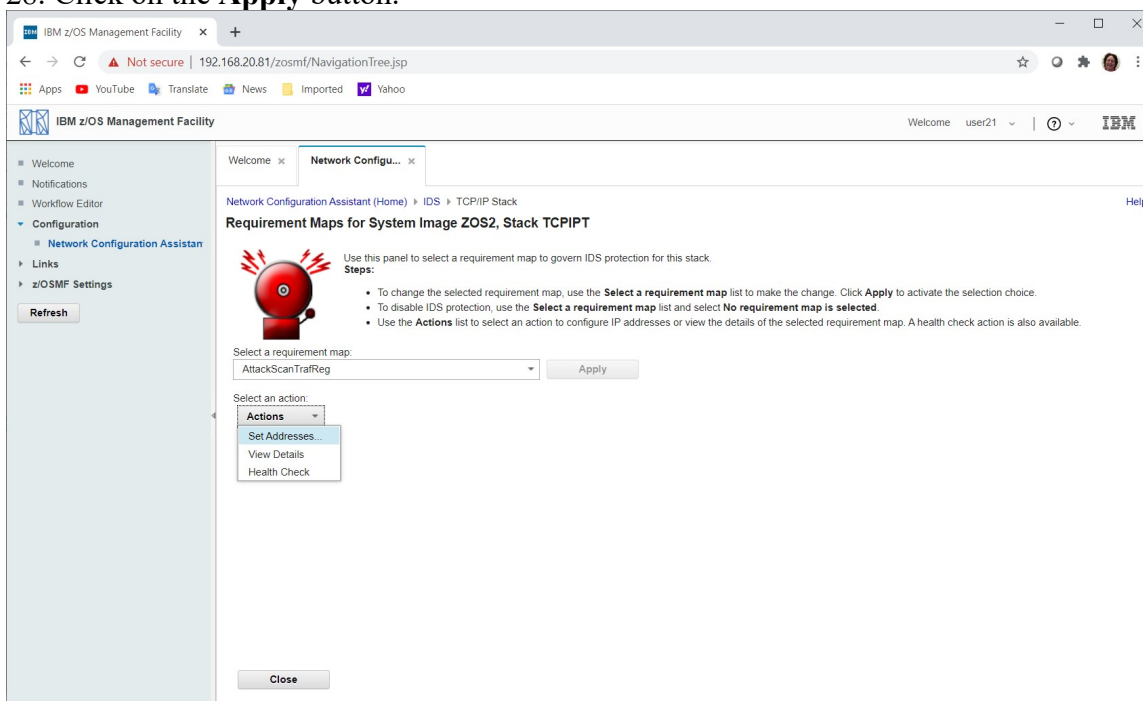
28. Use the Actions pull-down to select **Requirement Maps...**

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

29. Use the requirement map pull-down to select the one you just created, **AttackScanTraReg**.



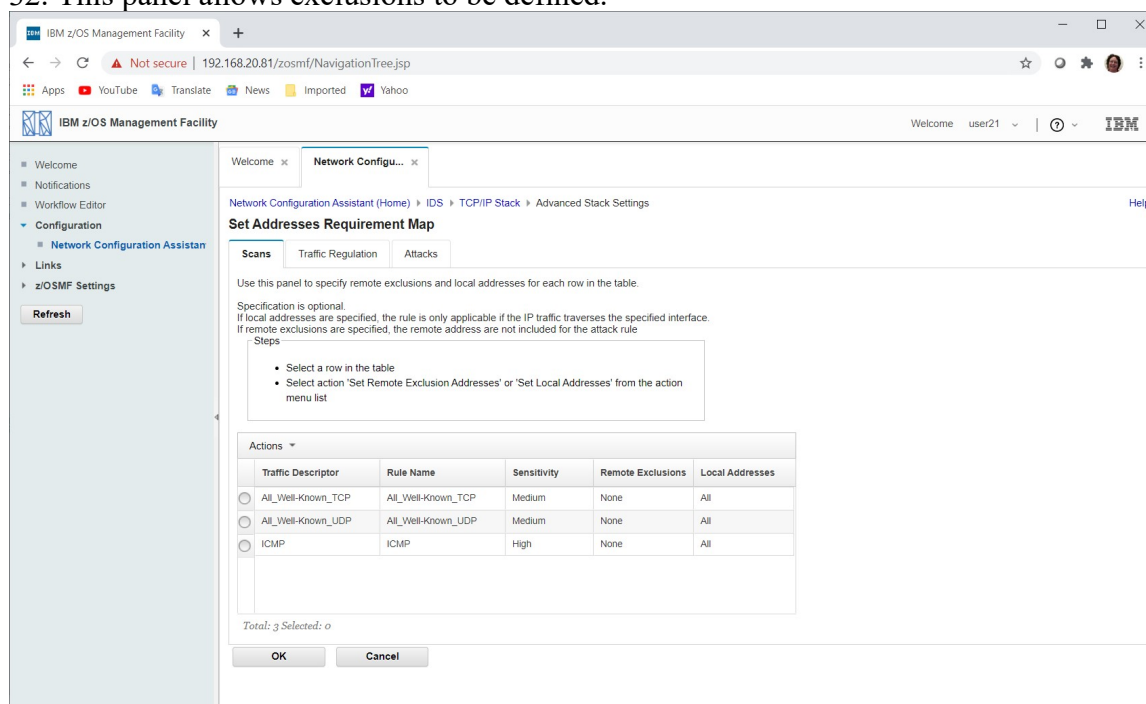
28. Click on the **Apply** button.



31. Use the **Actions** pull-down to select **Set Addresses...**

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

32. This panel allows exclusions to be defined.



33. For this lab we will not define any exclusions.

34. Click on

- OK**
- Close**

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

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

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

37. Fill in the correct values to FTP the file to your z/OS image:

1. File `/u/usernx/TMnx_IDS.policy`
2. Host name `192.168.20.8n`
3. User ID `usernx`
4. Password `<password>`

IBM z/OS Management Facility

Welcome user21 | IBM

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

Install File for Default.ZOS2.TCPIPT

* Install file name:
/u/user21/TM21_IDS.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

38. Click on **Go**, **OK** twice, **Close** twice, and **Save**.

Part 2: Installing the IDS Policy on Your z/OS Image

In this part of the lab you

- Incorporate your IDS policy into the running Policy Agent.
 - Verify that TRMDT is running, since it is responsible for selecting IDS messages from the TCP/IP stack's address space to record in SYSLOGD.
 - Run some IDS reports using the *trmdstat* command for report generation.
1. LEGEND for the TEAM Number:
 - a. TEAMnx, where "n" represents your ZOS suffix and "x" represents your userid suffix.
 - i. EXAMPLE: TEAM53 means ZOS5 and USERID of USER3.
 2. Create a PCOMM session to connect to TN3270 at TCPIP1 on your assigned MVS system.
 - a. You should be telnetting into TCPIP1 your MVS system at **192.168.20.8n** (where "n" is the suffix of the MVS/ZOS system).
 3. When you see the Message 10 screen from the TN3270 server on TCPIP1, 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>**
 4. On the ISPF signon screen, provide the password you were given in class.
 - a. **<password>**
 - b. Press **ENTER**
 5. Go into SDSF to view the MVS log with:
 - a. **ISPF D.LOG**
 6. Verify that the following procedures are running by issuing the command **/D A,L** from the SDSF command line (don't use quotation marks):
 - 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 IDS with)
 - f. **PAGENTT** (this should be running with a student version of the /etc/PAGT1/pagentt.conf file if you have completed the Policy Agent lab.)
 - g. TRMDT (this should be running since the TRMDT lab.)
 7. If any of the procedures are not running, start them following the specific lab directions or the commands listed in the Lab Diagrams document.
 8. Move into the OMVS shell from the SDSF Command line in order to configure Policy Agent:
 - a. **TSO OMVS**
 9. Verify with the UNIX command *pwd* that your current directory is **/u/usernx/**.

Examples:

 - a. Userid **user22** is positioned in **/u/user22 on MVS2**
 - b. Userid **user33** is positioned in **/u/user33 on MVS3**

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

- c. Userid **user41** is positioned in **/u/user41 on MVS4**
 - d. Userid **user52** is positioned in **/u/user52 on MVS5**
 - e. **etc.**
10. Switch to SuperUser mode:
 - a. **su**
 11. Edit the pagentt.conf member that you created in an earlier lab:
 - a. **oedit pagentt.conf**
 12. Add the following line at the appropriate place in the file
 - a. **IDSConfig /u/usernx/TMnx_IDS.policy FLUSH PURGE** (where “usernx” is the name of your userid’s directory)
 - i. This is the file you uploaded in the workstation part of these labs.
 13. Close and File the new pagentt.conf file with a **PF3**.

Part 3: Testing the TCP/IP Stack and TN3270T for the IDS Policies

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**
 - b. **Enter**
4. Return to the SDSF log; if necessary re-enter this command:
 - a. **=D.LOG**
5. 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 IDS policy that you coded has been installed into TCPIPT.
6. Next enter the NETSTAT command to view the IDS policies installed in the TCPIPT stack:
 - a. **/D TCPIP,TCPIPT,N,IDS,SUMMARY**
 - b. Are IDS policies loaded for the TCPIPT stack? _____
 - c. Can you see that any connections have been rejected for Traffic Regulation?

 - d. As long as the IDS policies are loaded, return to the UNIX shell by issuing the command
 - i. **TSO OMVS**
7. Then issue the pasearch command (with “-i”) in order to see only the IDS policies that have been installed in the TCPIPT stack:
 - a. **pasearch -i > myidssearch**

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

8. Browse myidssearch and you see a consolidated list of the running IDS policies.
 - a. **obrowse myidssearch**
 - i. Look through the IDS policies. Note the TN3270-Server~1 policy.
 - ii. Use **PF3** to exit from the file you are browsing.
9. Browse the messages in SYSLOGD:
 - a. **su** if not already set.
 - b. **obrowse /var/CSLOG/syslogall.log**
 - c. Have you been attacked in any way yet?

 - i. Probably not. There is probably only a message there about the new IDS policy.
10. Move into the MVS environment again:
 - a. Exit out of UNIX.
 - b. **=D.LOG**
11. Now it is time to configure a TN3270 session that connects to your TN3270T.

Configure Personal Communications to Connect to TN3270T

1. Configure Personal Communications to connect to TN3270T – the Student TCP/IP stack.
 - a. Use PCOMM to configure a connection to **192.168.20.10n**.
 - i. **YOU MUST USE THE TCPIPT** telnet addresses with a final octet of **10n**.
 - ii. For ease in viewing the log, you may wish to make this a session with a large screen size. (27 x 132; 62 x 160)
 - iii. **NOTE:** If your system is running with a requirement for TN3270T SSL (TLS or AT-TLS), then configure this session to use security, or recycle TN3270T to start it with the instructor profile (/S TN3270T).
 - b. **Connect** this new PCOMM session to your ZOS system. **(Session 1)**
2. From this PCOMM TN3270 session, create 2 more connections like this:
 - a. From the **File** pulldown of the first session, select
 - i. **Run the Same**
 - b. Select **Run the Same** until you have 3 connections from the same terminal to your MVS.
 - i. Are the three connections successful? _____
 - ii. What percentage of the total available sessions do 3 connections represent?

 - iii. Is this percentage what you configured in your TR Policy? _____
3. Bring up a 4th connection to your TN3270T.
 - a. What happens? _____

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

b. Why did this happen with the 4th connection?

4. Examine the MVS log.

a. What message numbers do you see?

b. If you don't see these messages is probably because you do not have DEBUG CONN DETAIL defined in the TN3270 profile.

c. Example:

```
EZZ6034I TN3270T CONN 000004DE LU **N/A** ACCEPTED 23 481
IP..PORT: 192.168.215.97..59275
EZZ6034I TN3270T CONN 000004DE LU TCPS2A03 NEGOTIATED TN3270E 482
IP..PORT: 192.168.215.97..59275
EZZ6035I TN3270T DEBUG CONN DETAIL 483
IP..PORT: 192.168.215.97..59275
CONN: 000004DE LU: TCPS2A03 MOD: EZBTPGLU
RCODE: 3011-00 Application name is required.
PARM1: 00000000 PARM2: 00000000 PARM3: 00000000
EZZ6034I TN3270T CONN 000004E0 LU **N/A** ACCEPTED 23 484
IP..PORT: 192.168.215.97..59276
EZZ6035I TN3270T DEBUG CONN DETAIL 485
IP..PORT: 192.168.215.97..59276
CONN: 000004E0 LU: TCPS2A03 MOD: EZBTPTKO
RCODE: 1014-00 Takeover has started.
PARM1: 0000000A PARM2: 00000000 PARM3: TKOGENLURECON
EZZ6034I TN3270T CONN 000004E2 LU **N/A** ACCEPTED 23 486
IP..PORT: 192.168.215.97..59277
EZZ6035I TN3270T DEBUG CONN DETAIL 487
IP..PORT: 192.168.215.97..59277
CONN: 000004E2 LU: MOD: EZBTPGLU
RCODE: 3003-00 LUs are all in use.
PARM1: 00000000 PARM2: *DEFLUS* PARM3: 00000000
EZZ6034I TN3270T CONN 000004E2 LU TCPS2A04 NEGOTIATED TN3270E 488
IP..PORT: 192.168.215.97..59277
EZZ6035I TN3270T DEBUG CONN DETAIL 489
IP..PORT: 192.168.215.97..59277
CONN: 000004E2 LU: TCPS2A04 MOD: EZBTPGLU
RCODE: 3011-00 Application name is required.
PARM1: 00000000 PARM2: 00000000 PARM3: 00000000
EZZ6035I TN3270T DEBUG CONN DETAIL 490
IP..PORT: 192.168.215.97..59276
CONN: 000004E0 LU: TCPS2A03 MOD: EZBTDALU
RCODE: 1009-00 Takeover has failed.
PARM1: 00000000 PARM2: 00000000 PARM3: TKOGENLU
EZZ6034I TN3270T CONN 000004E0 LU TCPS2A05 NEGOTIATED TN3270E 491
IP..PORT: 192.168.215.97..59276
EZZ6035I TN3270T DEBUG CONN DETAIL 492
IP..PORT: 192.168.215.97..59276
CONN: 000004E0 LU: TCPS2A05 MOD: EZBTPGLU
RCODE: 3011-00 Application name is required.
PARM1: 00000000 PARM2: 00000000 PARM3: 00000000
```

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

5. Issue the command to check IDS statistics:
 - a. **/D TCPIP,TCPIPT,N,IDS,SUMMARY**
 - b. Can you see that any connections have been rejected for Traffic Regulation?

i. You should see evidence of connection rejection for TR.

6. Return to the UNIX environment to run some reports.
 - a. **TSO OMVS**
7. Browse through the help for the trmdstat command by entering the following:
 - a. **su**
 - b. **trmdstat**

8. View a report for TCPIPT with the following parameters:

a. **trmdstat -j TCPIPT /var/CSLOG/syslogall.log**

Example:

```
# trmdstat -j tcpipt /var/CSLOG/syslogall.log
trmdstat for z/OS CS V2R1  Fri Mar 27 10:45:21 2015
```

```
Command Entered      : trmdstat -j tcpipt /var/CSLOG/syslogall.log
Log Time Interval    : Mar 27 14:16:40 - Mar 27 14:27:40
Stack Time Interval  : Mar 27 14:16:26 - Mar 27 14:27:31
TRM Records Scanned : 23
```

TCP - Traffic Regulation

```
-----
Connections would have been refused :          0
Connections refused                  :          1

Constrained entry logged             :          0
Constrained exit logged              :          0
Constrained entry                    :          0
Constrained exit                     :          0

QOS exceptions logged                :          0
QOS exceptions made                  :          0
```

UDP - Traffic Regulation

```
-----
Constrained entry logged             :          0
Constrained exit logged              :          0
Constrained entry                    :          0
Constrained exit                     :          0
```

SCAN Detection

```
-----
Threshold exceeded                   :          0
Detection delayed                    :          0
Storage constrained entry            :          0
Storage constrained exit             :          0
```

ATTACK Detection

```
-----
Packet would have been discarded    :          0
Packet discarded                     :          0
```

FLOOD Detection

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

```
-----
Accept queue expanded           :          0
SYN flood start                 :          0
SYN flood end                   :          0
Interface flood start           :          0
Interface flood end             :          0
EE XID flood start              :          0
EE XID flood end                :          0
```

Global TCP Stall Detection

```
-----
Global TCP stall entry          :          0
Global TCP stall exit           :          0
Connections would have been reset :          0
Connections reset               :          0
```

TCP Queue Size Detection

```
-----
Send queue
  Constrained entry             :          0
  Constrained exit              :          0
  Connections reset             :          0
Receive queue
  Constrained entry             :          0
  Constrained exit              :          0
  Connections reset             :          0
Out-of-order queue
  Constrained entry             :          0
  Constrained exit              :          0
  Connections reset             :          0
```

9. View any other reports you like if trmdstat seems to be working.
10. Exit from UNIX.
11. Sign off of MVS and disconnect all the sessions you created to your MVS.
12. You have completed the IDS lab.
 - a. We do not test the ATTACK and the SCAN policies.

End of IDS Lab

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

