

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

"Configuring TRMD for Security Policies in z/OS"

Hands-on Lab Guide for TRMD

(TRMD Exercises)



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.

Table of Contents

PART 0: INTRODUCTION TO TRMD LAB..... - 4 -
 Traffic Regulation Management Daemon (TRMD) - 5 -

PART 1: THE TRMD SAMPLE PROCEDURE IN Z/OS - 5 -

PART 2: THE TRMDT CUSTOMIZED PROCEDURE FOR LABS..... - 7 -
 END OF TRMD LAB- 7 -

Part 0: Introduction to TRMD Lab

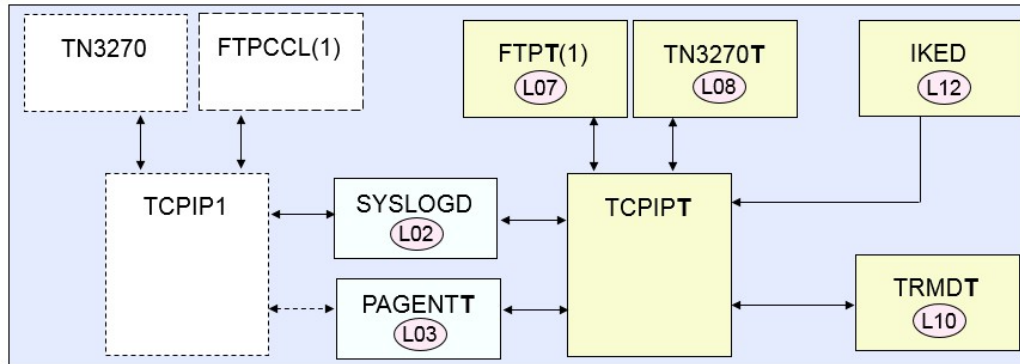
Each student ZOS (MVS) system has two TCP/IP stacks running in it. The basic TCPIP stack belonging to the instructors is named TCPIP1. The TN3270 procedure that has affinity to the instructor TCPIP1 is named TN3270. The FTP procedure that has affinity to TCPIP1 is named FTPCCL(1).

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.

Traffic Regulation Management Daemon (TRMD)



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

As the diagram above shows, your z/OS system (ZOSn or MVSn) should run with a UNIX Traffic Regulation Management Daemon. TRMD reads messages from the running TCP/IP stack and sends them to SYSLOG Daemon. The messages can be used for problem determination on behalf of IDS and IPSec processes. For IDS, the messages can also be used to create reports with the *trmdstat* command. You do not have to configure this daemon in our lab, but we want you to examine what has been built for you.

The lab contains only two sections:

- *Part 1: Examining the TRMD Procedure provided in the TCP/IP samples library on z/OS*
- *Part 2: Examining the running TRMDT procedure to see how we have modified it for the lab classes.*

Part 1: The TRMD Sample Procedure in z/OS

1. Telnet into your MVS system (ZOSn) at 192.168.20.8n.
2. 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>**
3. On the ISPF signon screen, provide the password you were given in class.
 - a. **<password>**
 - b. Press **ENTER**
4. At the READY prompt, enter the ISPF display screen with
 - a. **ISPF 3.4**

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

5. Enter the following Dataset name (DSNAME):
 - a. **SYS1.TCPIP.SEZAINST**
6. Place a “B” for “browse” next to the dataset name on the next panel:
 - a. **B**
7. Press ENTER to display the contents of the IBM TCPIP Samples Dataset.
 - a. **ENTER**
8. From the command line, enter the following command to view the contents of the TRMD sample procedure:
 - a. **S TRMD** (“S” is for “select” in this case)
9. Answer the following questions about the procedure:
 - a. Does the procedure point to a REAL or a DUMMY standard environment file?
 - b. If you run this procedure “as is”, how does TRMD know the following? (Use the IPCONFIG Guide or your class notes or your own experience to respond.)
 - i. How does it know which TCP/IP Stack it is to be associated with?

 - ii. How does it know the TIMEZONE variable it is to use for the messages printed to the log?

10. Use **PF3 (F3)** to exit the view of the TRMD sample procedure.
11. Next look at the contents of **SYS1.TCPIP.SEZAINST(EZARACF)**
 - a. **S EZARACF**
12. From the command line find the TRMD section for the RACF commands that should be executed to authorize TRMD:
 - a. **F TRMD**
13. Browse through these definitions.
 - a. NOTE: They have already been executed for our class procedure.
14. Exit the EZARACF member and the SEZAINST dataset.
 - a. **PF3 (F3)** three times

Part 2: The TRMDT Customized Procedure for Labs

1. View our customized version of the TRMD procedure.
 - a. Specify a dataset name of 'SYS1.PROCLIB' (without quotation marks) and press **ENTER**.
 - b. On the DSLIST screen place a **B** (for browse) next to the dataset.
 - c. View the contents of the TRMDT procedure by entering 'S TRMDT' (without quotation marks) on the command line.
2. Answer the following questions for our customization of the TRMDT procedure:
 - a. Does the procedure include a pointer to the symbolic name of the Language Environment file? (" _CEE_ENVFILE=)
 - b. How does the procedure point to the TCP/IP stack it is to be associated with?
 - c. How does the procedure indicate the timestamp to be associated with the logging time of the messages?
3. Exit from the view of our customized TRMDT procedure.
 - a. **PF3 (F3)** three times
4. For our labs you will use our customized version of the TRMDT procedure because we are using only one PROCLIB to which students have no WRITE access.

End of TRMD Lab

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

