

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

**"Examining Defense Manager Daemon (DMD)  
Hands-on Lab Guide**

**(DMD Lab)**



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

Revision date -

Monday, 6 June 2022

This edition applies to IBM z/OS Configuration Assistant running in z/OSMF 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 Defense Manager Daemon (DMD)..... 4

    Overview of this LAB: Defense Manager Daemon (DMD)..... 5

Part 1: Defense Manager Daemon (DMD) ..... 6

    Connect to the z/OS IBM Configuration Assistant in z/OSMF on ZOS1 ..... 6

    Create Defense Manager Daemon (DMD) Configuration File..... 7

    Install DMD Configuration File..... 9

    Test DMD ..... 11

End of DMD LAB ..... 14

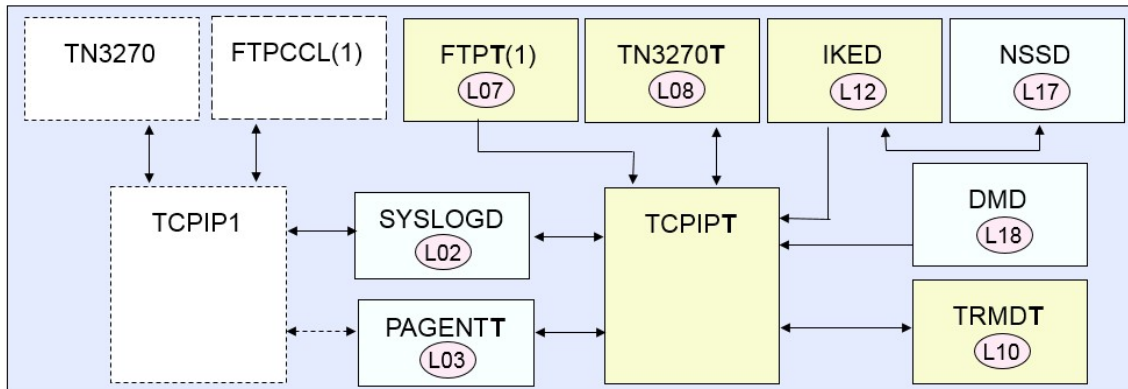
## **Part 0: Lab Description for Defense Manager Daemon (DMD)**

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).

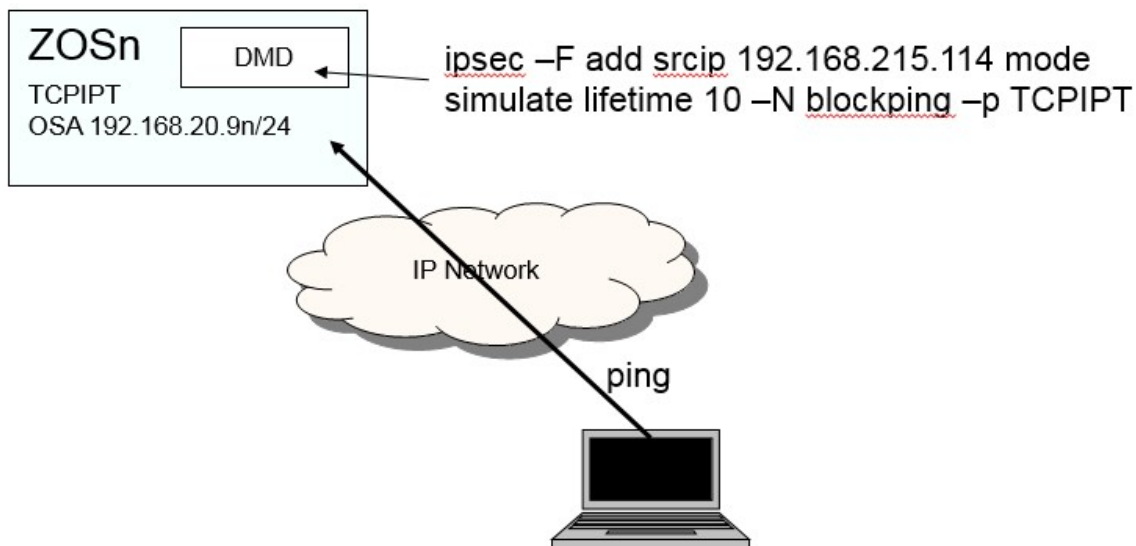
In our labs you use TCPIP1 for basic maintenance on ZOSn until you have finished building your own student TCP/IP stacks and procedures. You will telnet into TCPIP1 to reach ISPF and UNIX for building the procedures that should run together with the student TCP/IP stack.

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.

## Overview of this LAB: Defense Manager Daemon (DMD)



- “Maintenance” TCP/IP stack (TCPIP1)
- “Student” TCP/IP stack (TCPIPT)
- Stack Specific
  - TN3270 (Lab L08)
  - FTP (Lab L07)
  - TRMD (Lab L10)
- Available to all TCP/IP Stacks
  - SYSLOGD (Lab L02)
  - PAGENT (Lab L03)
  - IKED (Lab L12)
  - NSSD (Lab L17)
  - DMD (Lab L18)



You will use the z/OS IBM Configuration Assistant tool to create a DMD configuration file. You will install it into your ZOSn system, start the DMD, load an IP filter with the ipsec command, and test it.

*The lab only has a single section:*

- **Part 1: Defense Manager Daemon (DMD)**

## Part 1: Defense Manager Daemon (DMD)

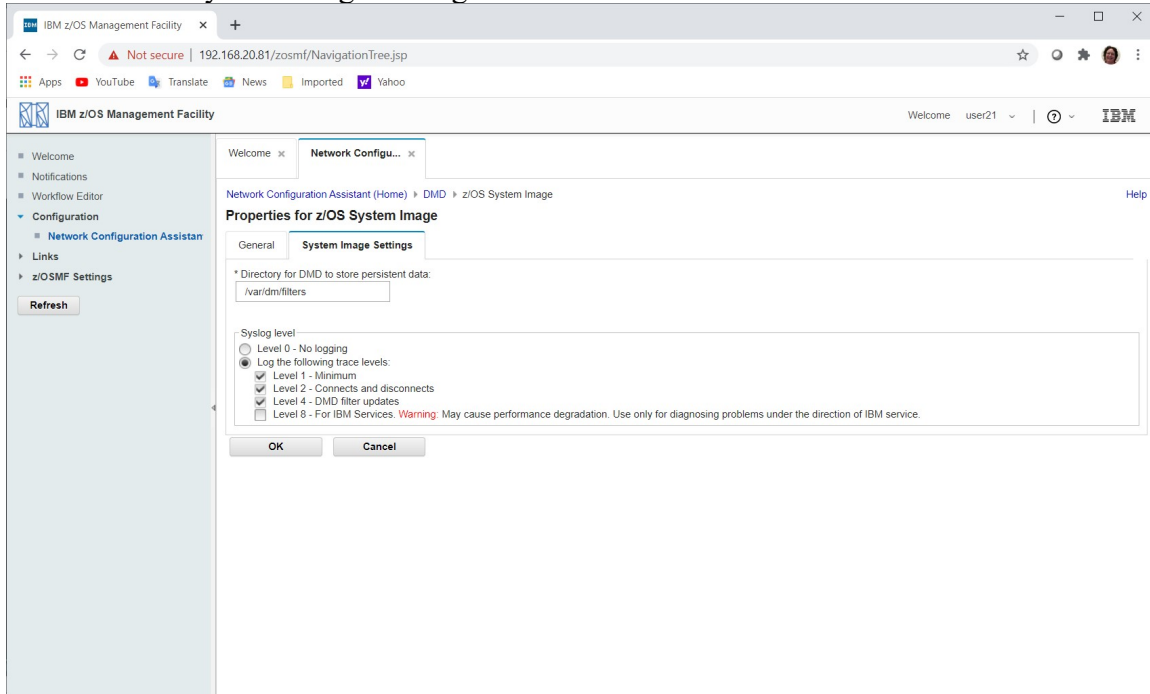
***IMPORTANT: Screen captures are APPROXIMATE EXAMPLES of what you may see. Always follow the lab instructions for what to enter on the tool screens and ignore the entries in the EXAMPLE unless you are told to use those entries.***

### **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.

## Create Defense Manager Daemon (DMD) Configuration File

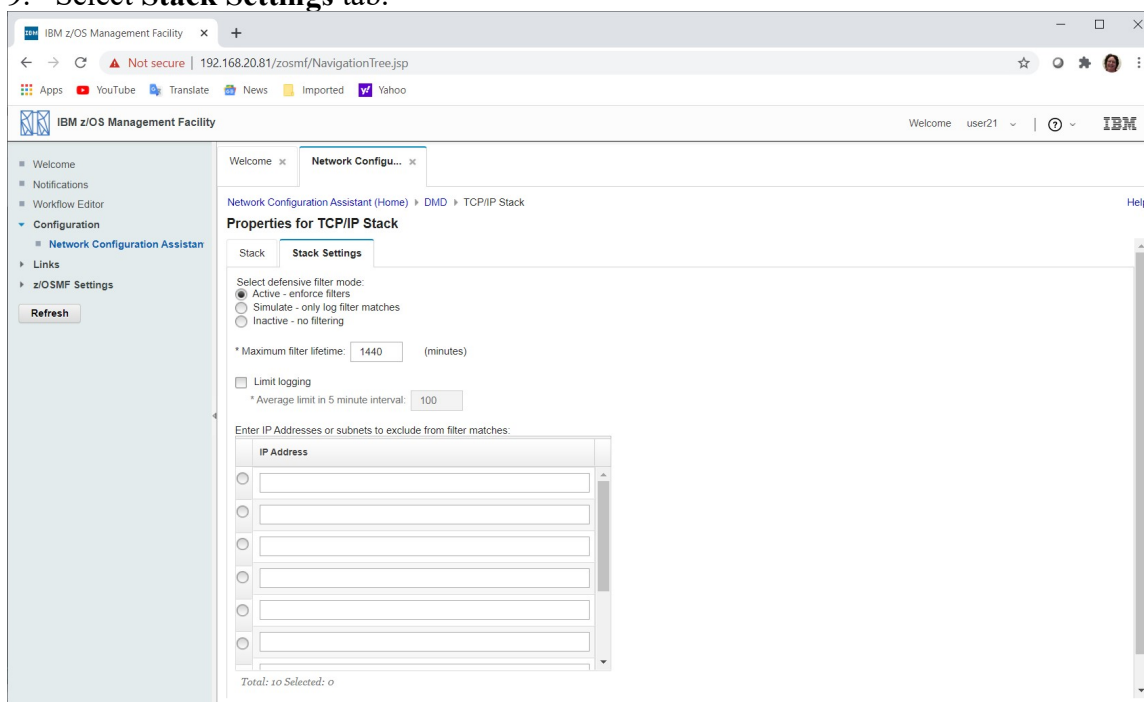
1. Use the technology pull-down to select **DMD**.
2. Use the radio button beside your **ZOSn** image.
3. Use the **Actions** pull-down to select **Properties...**
4. Select the System Image Settings tab.



5. DMD requires a directory location for persistent data. The default is /var/dm/filters and may have been created for you in this class.
6. **OK**
7. Use the radio button beside the **TCPIPT** stack under your **ZOSn** image.
8. Use the **Actions** pull-down to select **Properties...**

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

## 9. Select **Stack Settings** tab.

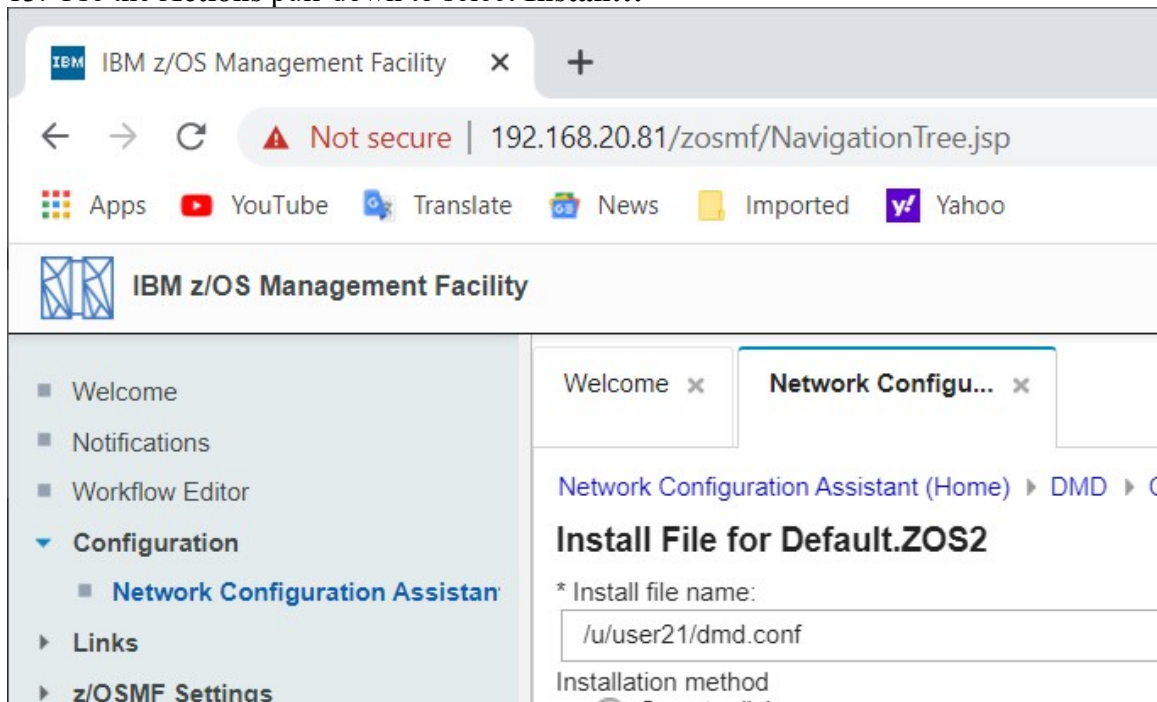


10. The default setting, Active, is to discard packets that match the Defensive IP Filter.

11. **OK**

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

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



14. Enter Install file name **/u/usernx/dmd.conf**.

15. **Go, OK, Close, OK, Close.**

## ***Install DMD Configuration File***

NSSD requires several RACF steps as outlined in the “IP Configuration Guide” manual. All the required RACF steps have been done for you in this class.

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** and enter password
2. Go into the ISPF Primary Menu.
  - a. Enter **ISPF**
3. Go to the TSO Command input panel.
  - a. **=6**
4. Display the user ID that is associated with the JCL Started Procedure.
  - a. **LISTUSER (DMD) OMVS**
  - b. **RLIST STARTED DMD.\* STDATA**
5. If SYS1.PARMLIB is being protected you must add a PERMIT for user ID DMD. We have not protected SYS1.PARMLIB on your test systems.
6. The ipsec command may be defined to RACF SERVAUTH Class.
  - a. Please see the manuals for further information.
7. Display the DMD JCL procedure.
  - a. **=3.4**

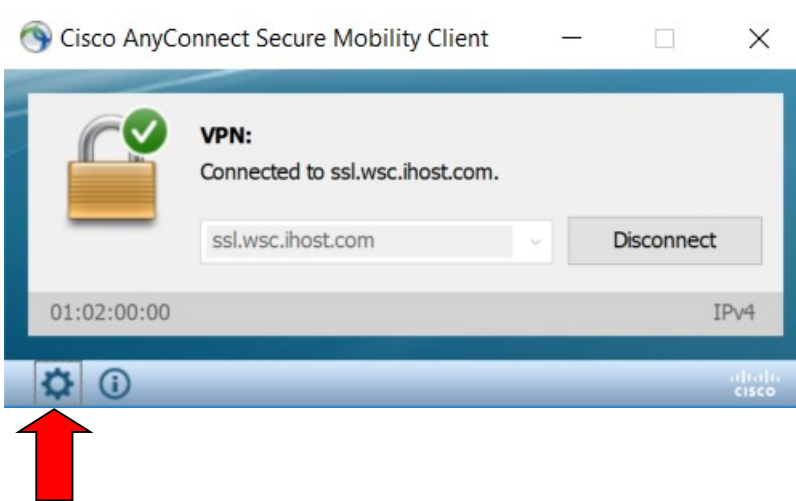
- b. **SYS1.PROCLIB**
  - c. View the file **DMD**.
  - d. The proc was copied from the TCPIP sample directory SEZAINST and was not customized at all.
8. Is an environment file specified in the DMD proc?
9. Is the DMD configuration file specified in the DMD proc?
10. What DMD configuration file will be used?
11. Exit viewing the DMD proc.
- a. **PF3**
12. Copy the DMD configuration file to the location in the server search order.
- a. **=O**
  - b. **4**
  - c. **su**
  - d. **cp dmd.conf /etc/security/dmd.conf**
13. Check for the directory location for persistent data.
- a. **cd /var/dm/filters**
  - b. If the above directory exists you can skip the next steps to create it.
  - c. **cd /var**
  - d. **mkdir dm**
  - e. **cd dm**
  - f. **mkdir filters**
14. Exit out of OMVS.
- a. **exit**
  - b. **exit**
  - c. **Enter**

## Test DMD

1. Start DMD.
  - a. =D.LOG
  - b. /S DMD
2. Look at the active programs listed in the bottom right corner of your computer screen. You will notice the icon for the Cisco AnyConnect Client that you are using for VPN access to the mainframe network. I have pointed it out below with a red arrow. Double click on the icon to find your PC's **Client Address** in the VPN network. You will use this IP address to create a Defensive IP Filter on your ZOSn.

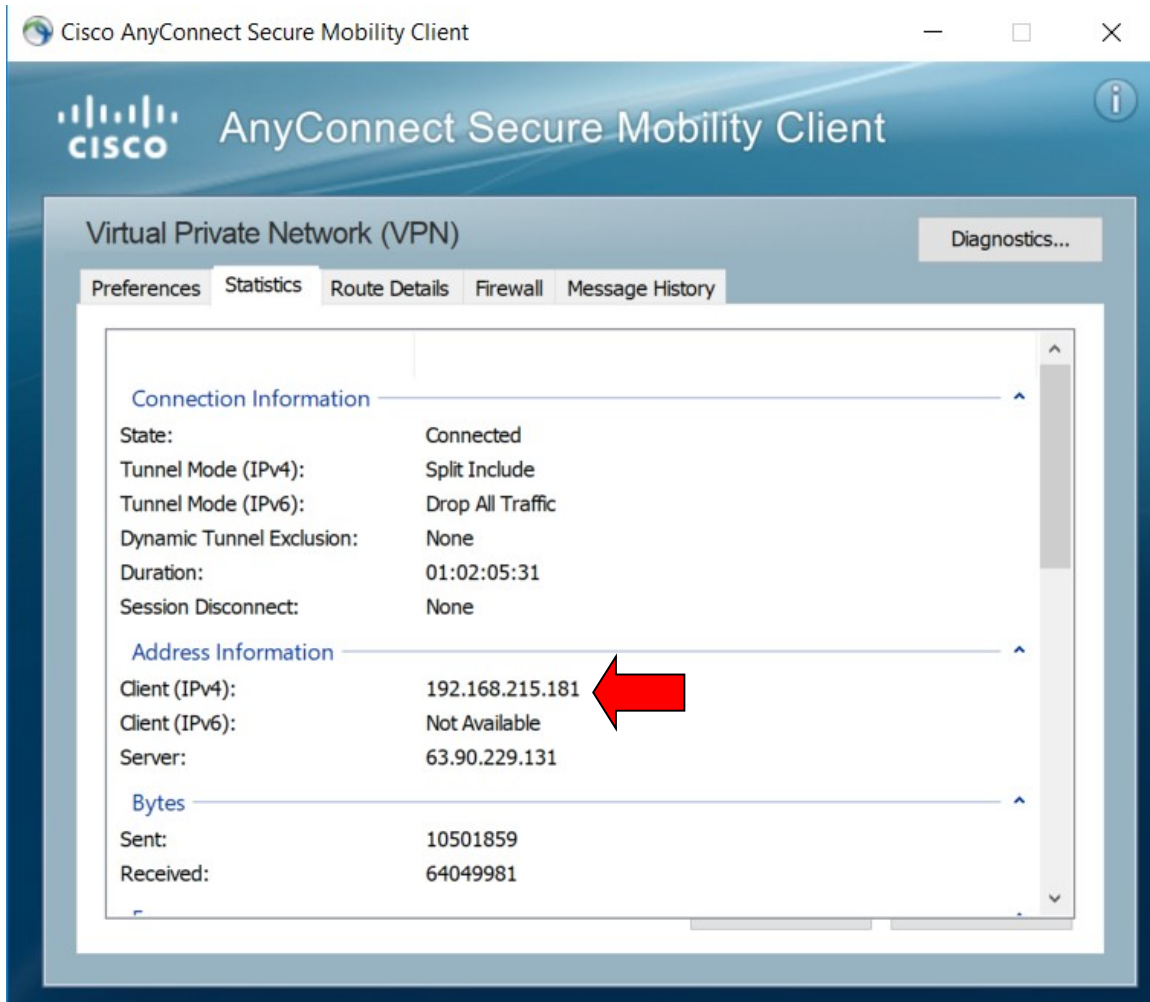


3. Click on the gear shaped icon on the Cisco AnyConnect client window. I have pointed it out below with a red arrow.



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

4. Get your local PC IP address in the 192.168.0.0/16 lab subnet from the Advanced window.



5. Open a Command Prompt window on your PC.
  - a. The location may vary but one possible location is:  
Start >>> All Programs >>> Accessories >>> Command Prompt
6. Ping your ZOSn TCPIPT system.
  - a. **ping 192.168.20.9n**
7. Return to your PComm session window.
8. Return to OMVS to enter Defensive IP Filter and test it.
  - a. **=O**
  - b. **4**
  - c. **su**
9. Enter Defensive IP Filter.
  - a. **ipsec -F add srcip 192.168.215.181 mode simulate lifetime 10 -N blockping -p TCPIPT**
    - i. where 192.168.215.181 is your Client Address that you retrieved from the Cisco AnyConnect client panel in the previous step.

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

10. Return to your Command Prompt window on your PC and enter the Ping again (Up arrow will retrieve your last command).
  - a. **ping 192.168.20.9n**
11. Return to your PComm session window.
  - a. **obrowse /var/CSLOG/ipsec.log** (if you have completed lab L12)
  - b. **obrowse /var/CSLOG/syslogall.log** (if you have NOT completed lab L12)
  - c. Near the bottom of the log you should find messages:
  - d. **EZD1722I** Packet would have been denied by defensive filter...
12. Exit out of obrowse.
  - a. **PF3**
13. Change the filter to discard packets.
  - a. **ipsec -F update mode block lifetime 10 -N blockping -p TCPIPT**
14. Return to your Command Prompt window on your PC and enter the Ping again (Up arrow will retrieve your last command).
  - a. **ping 192.168.20.9n**
  - b. Now you 'should' get message "Request timed out."
15. Return to your PComm session window.
  - a. **obrowse /var/CSLOG/ipsec.log**
  - b. Near the bottom of the log you should find messages:
  - c. **EZD1721I** Packet denied by defensive filter...
16. Exit out of obrowse.
  - a. **PF3**
17. Display all the Defensive IP Filters.
  - a. **ipsec -F display -p TCPIPT**
  - b. Example:

```
#ipsec -F display -p TCPIPT
```

```
CS V2R1 ipsec Stack Name: TCPIPT Wed Apr 29 09:58:29 2015
Primary: Defensive Filt Function: Display Format: Detail
Source: Stack Scope: n/a TotAvail: 95
Logging: n/a Predecap: n/a DVIPSec: n/a
NatKeepAlive: 20 FIPS140: n/a
Defensive Mode: Active
```

```
FilterName: blockping
FilterNameExtension: 1
GroupName: n/a
LocalStartActionName: n/a
VpnActionName: n/a
TunnelID: n/a
Type: Defensive
DefensiveType: Stack
State: Active
Action: Defensive Block
Scope: Local
Direction: Inbound
OnDemand: n/a
SecurityClass: 0
Logging: All
LogLimit: 0
Protocol: All
ICMPType: n/a
```

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

```
ICMPTypeGranularity:      n/a
ICMPCode:                 n/a
ICMPCodeGranularity:     n/a
OSPFType:                 n/a
TCPQualifier:             n/a
ProtocolGranularity:     n/a
SourceAddress:            192.168.215.114
SourceAddressPrefix:     n/a
SourceAddressRange:      n/a
SourceAddressGranularity: n/a
SourcePort:               n/a
SourcePortRange:         n/a
SourcePortGranularity:   n/a
DestAddress:              0.0.0.0
DestAddressPrefix:       0
DestAddressRange:        n/a
DestAddressGranularity:  n/a
DestPort:                 n/a
DestPortRange:           n/a
DestPortGranularity:     n/a
OrigRmtConnPort:         n/a
RmtIDPayload:             n/a
RmtUdpEncapPort:         n/a
CreateTime:               2015/04/29 09:55:42
UpdateTime:               2015/04/29 09:55:49
DiscardAction:            Silent
MIPv6Type:                n/a
MIPv6TypeGranularity:    n/a
TypeRange:                n/a
CodeRange:                n/a
RemoteIdentityType:      n/a
RemoteIdentity:           n/a
FragmentsOnly:           No
FilterMatches:            4
LifetimeExpires:         2015/04/29 10:05:49
AssociatedStackCount:     n/a
*****
1 entries selected
#
```

18. You may exit OMVS now.

- a. **exit**
- b. **exit**
- c. **Enter**

## End of DMD LAB

# 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

