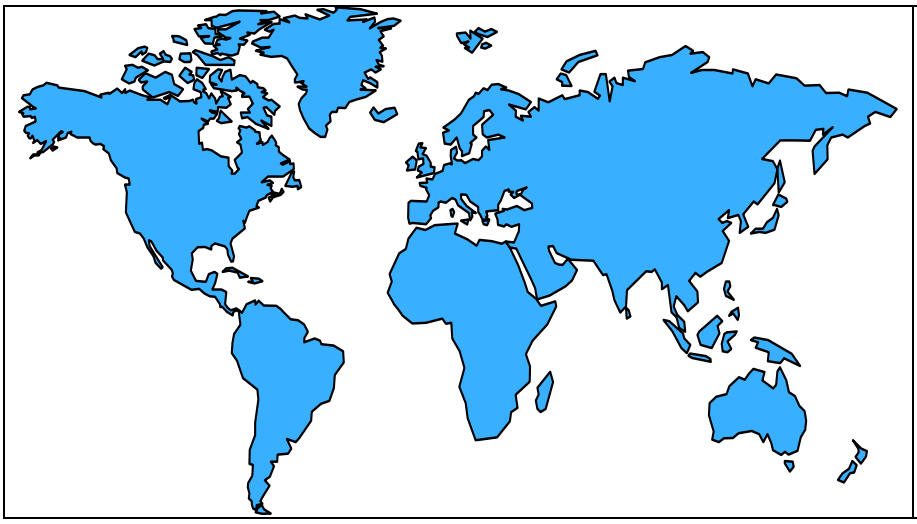
" z/OSMF Configuration Assistant for z/OS Communications Server" Hands-on Lab - Part 1 of 2

Part 1: IPsec Rule
Part 2: AT-TLS Rule

SHARE 16947

Hands-on Lab Guide



Revision date - Friday, 27 February 2015

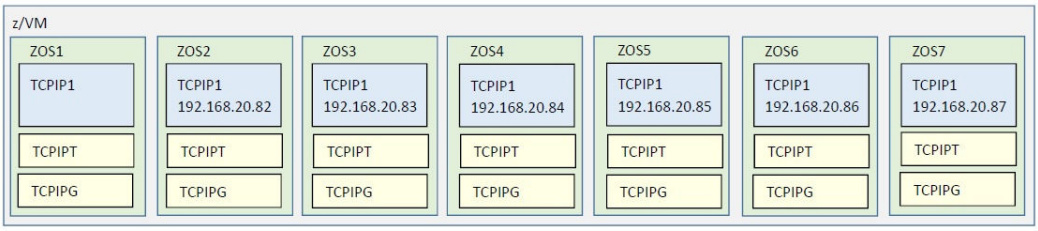
This edition applies to IBM z/OS Configuration Assistant V2R1 running in zOSMF on a z/OS V2.1 platform.
Attention:
Information in this document was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

Table of Contents

Introduction: Lab Description

z/OS Systems

There are 8 z/OS systems running as guests under a single z/VM system.



Each student ZOS (MVS) system has three TCP/IP stacks running in it: TCPIP***1***, TCPIP***T***, and TCPIP***G***.

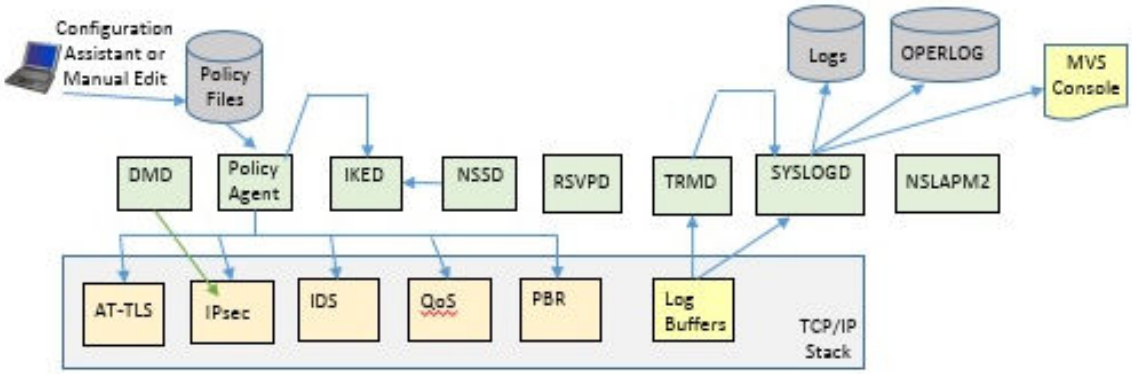
The basic TCPIP stack is used for access only and not testing and is named TCPIP***1***. The TN3270 procedure that has affinity to the access TCPIP***1*** is named TN3270. The FTP procedure that has affinity to TCPIP***1*** is named FTPCCL(1).

In our labs you use TCPIP***1*** for basic maintenance on your MVS***n*** 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 test stack.

There are six **"Student z/OS (MVS) systems"** that you will be working on: MVS***2***-MVS***7***. The student TCP/IP stacks on these systems are named TCPIP***T*** and TCPIP***G***. The students customize a test 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 TCPIP***T*** and TCPIP***G***.

Policy Agent Environment

There are lots of different elements in the Policy Agent (PAGENT) environment. The Configuration Assistant for z/OS can simplify the creation of this environment.

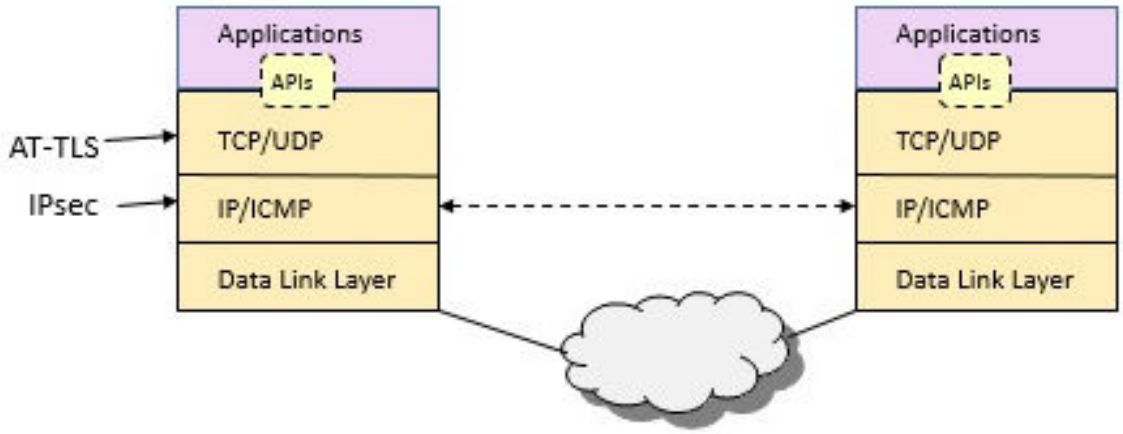


This lab does not have time to go into all the different parts of the z/OS Communications Server Policy Agent environment listed above. For more information please refer to the standard manuals and Redbooks.

- IP Configuration Guide, SC27-3650
- IP Configuration Reference, SC27-3651
- Redbook IBM z/OS V2R1 CS TCP/IP Implementation Vol 4: Security and Policy-Based Networking, SG24-8099

IPsec Lab

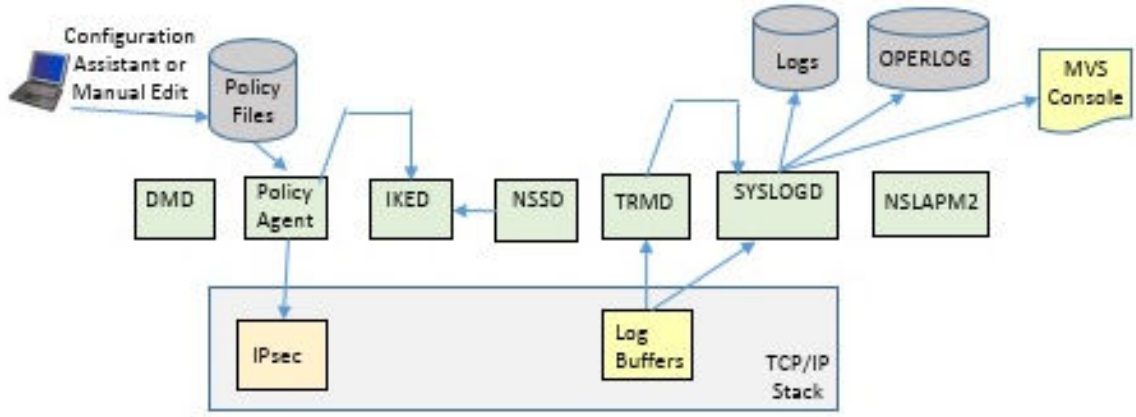
IPsec may be used to encrypt traffic between two hosts.



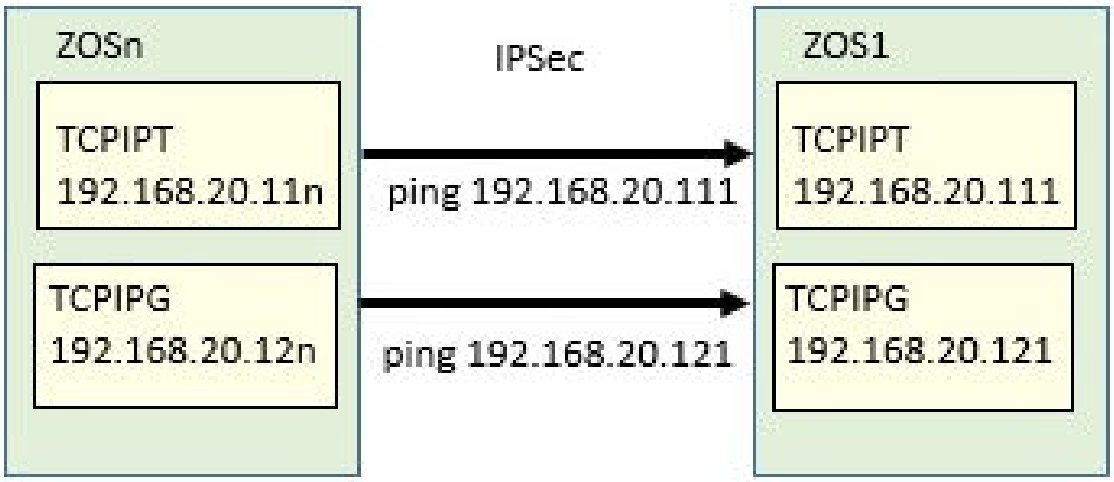
IPsec requires X.509 Certificates and Key Rings.

- IPsec Authentication for both hosts.
  - Local HostA
    - HostA Certificate
    - HostA Private Key
    - HostA CA Certificate
    - HostB CA Certificate
  - Remote HostB
    - HostB Certificate
    - HostB Private Key
    - HostB CA Certificate
    - HostA CA Certificate

Policy Agent reads in the policy files and installs them into the TCP/IP stack. It is the TCP/IP stack that enforces the policies.



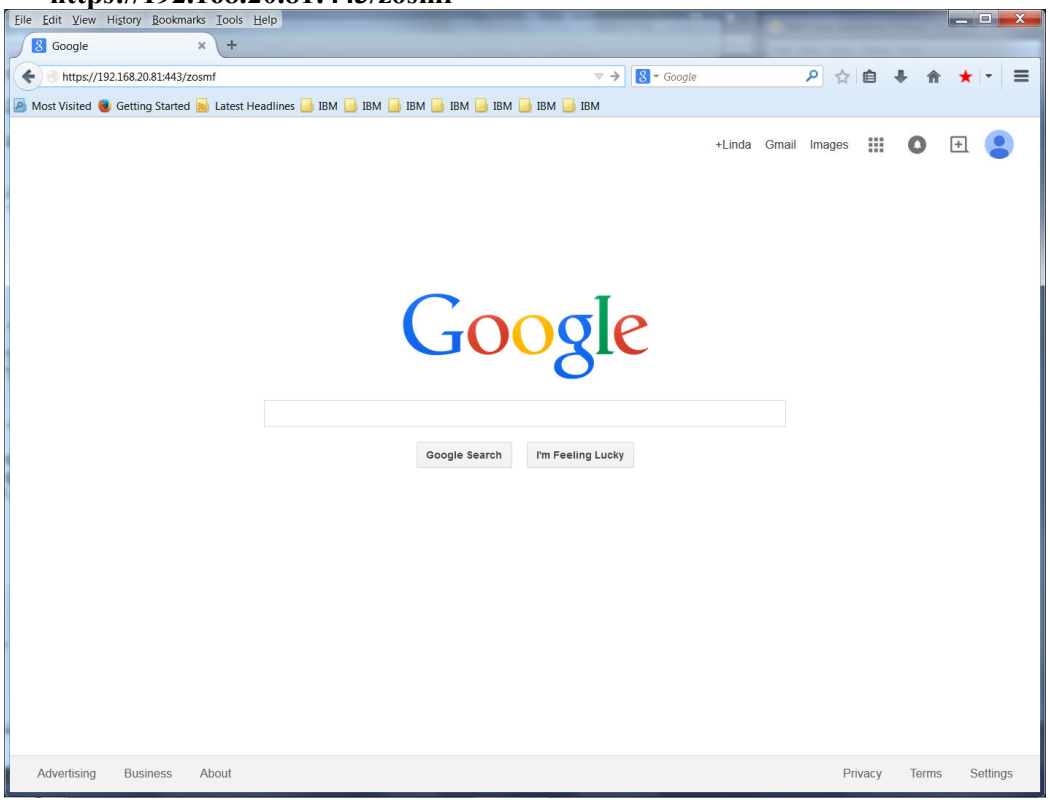
In this lab you will test IPsec using Ping.



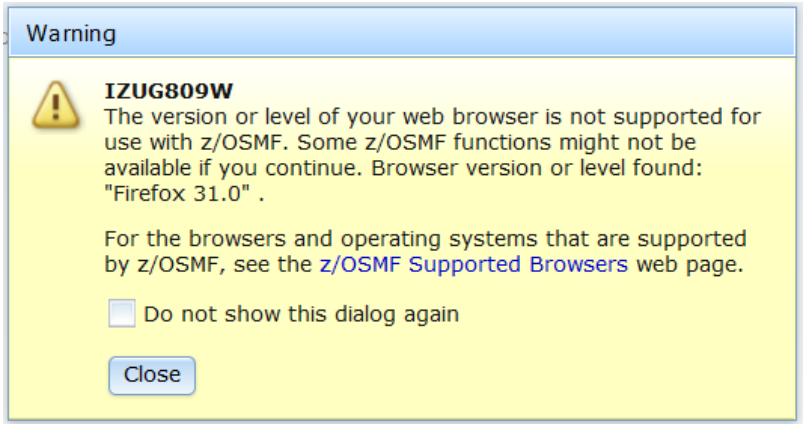
Scenario 1: Use zOSMF on ZOS1 for the First Time

If you already connected to zOSMF for a previous lab, then skip this Scenario and proceed to Scenario 2, otherwise proceed through this section.

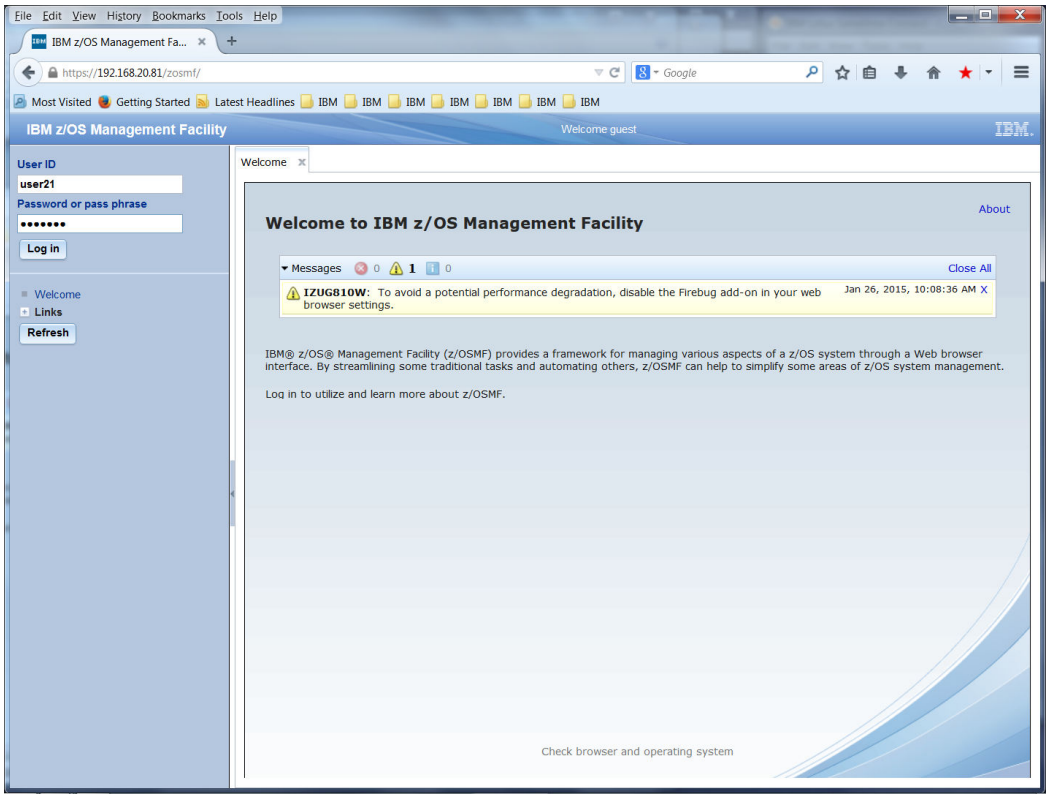
1. Open a Web Browser window and go to URL:
   https://192.168.20.81:443/zosmf



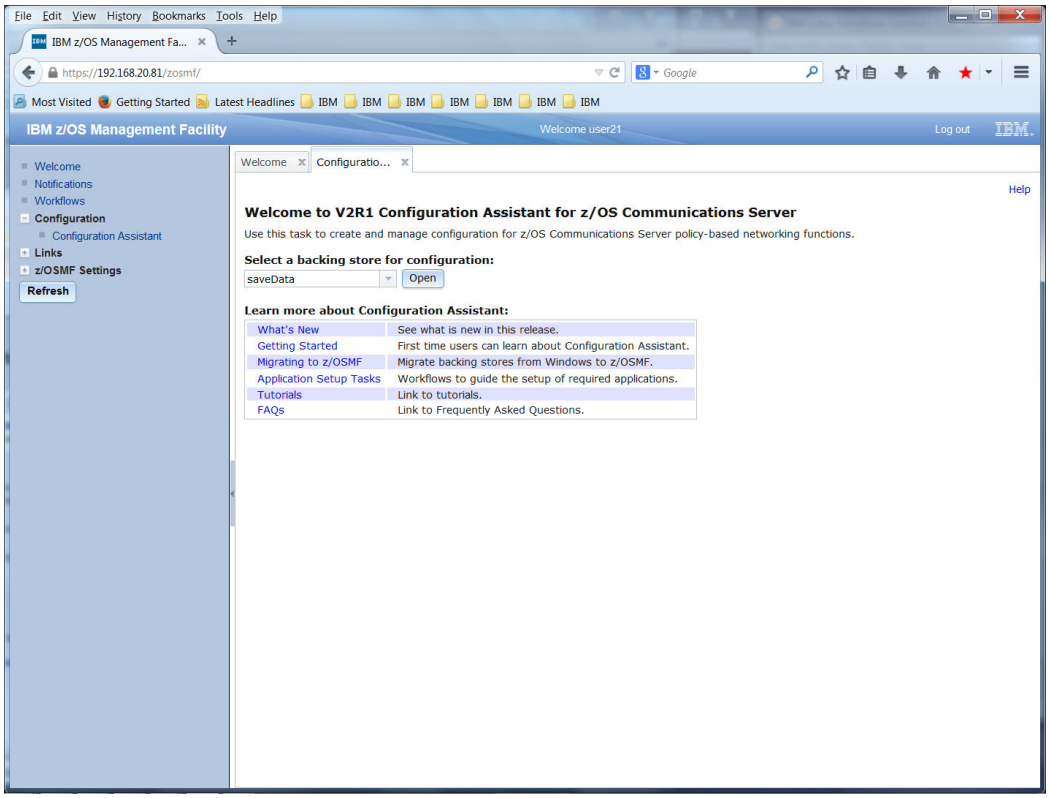
2. If a pop-up appears with warning IZUG809W warning "The version or level of your web browser is not supported for use with z/OSMF." Just ignore it and click on **Close** button.



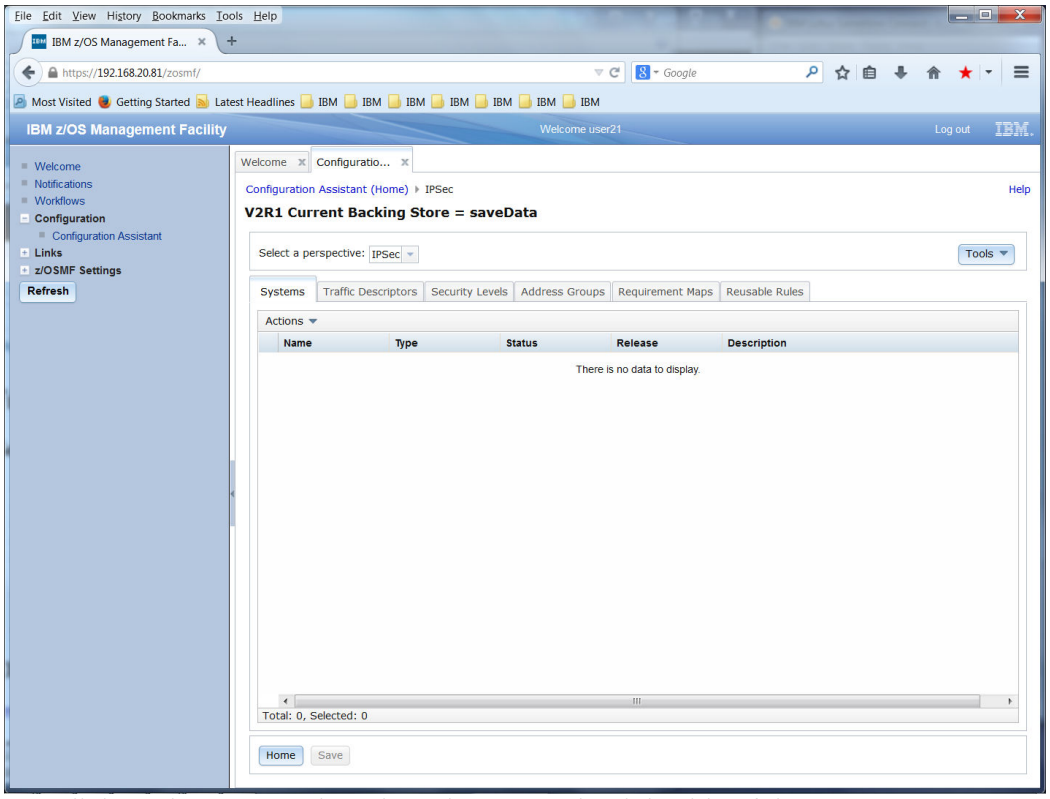
3. Logon using your Team Information Sheet to determine your z/OS User ID and password.



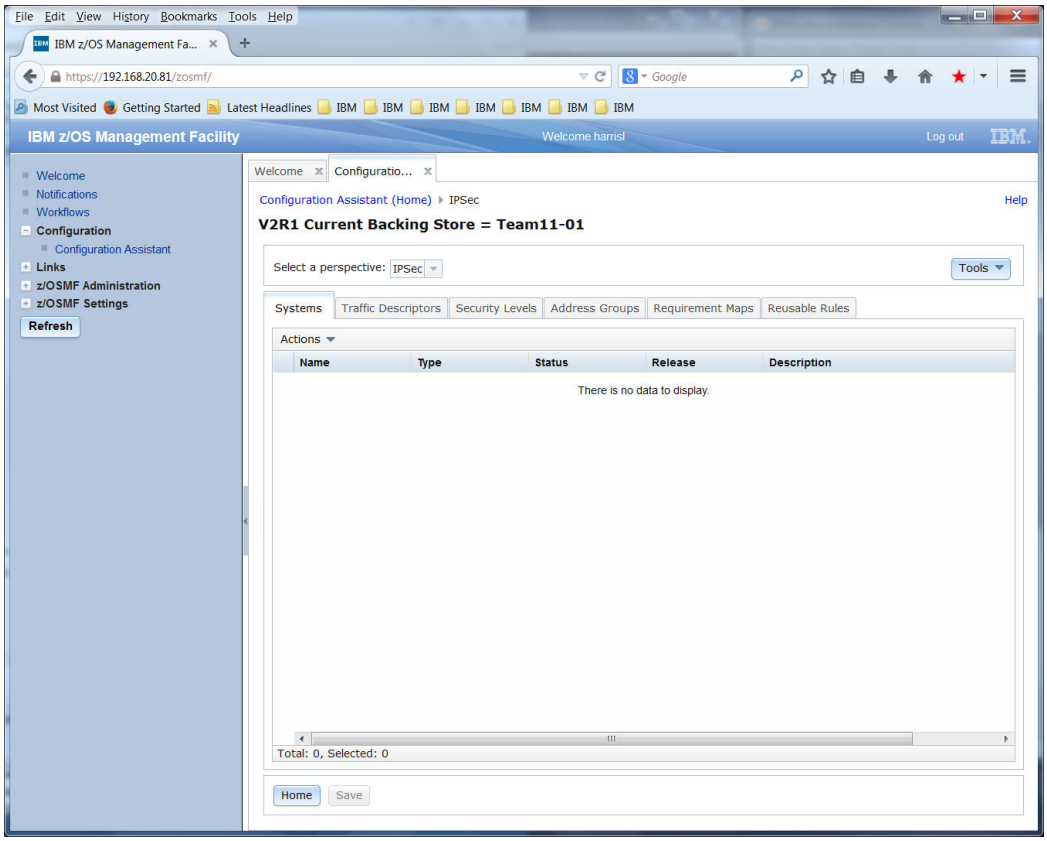
4. You should be presented with the "Welcome to IBM z/OS Management Facility" panel.
5. Feel free to click on the numerous links to learn more about zOSMF. There three links under the heading "Learn More:" at the bottom of the page, and there are several links in the left area of the page including the link to the current "Welcome" page. Since all these links, except "Configuration", pertain to zOSMF rather than the "z/OS Configuration Assistant for Communications Server" the lab instructor is not able to answer any question about them.
6. When you are finished exploring the page, 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 "–" means that it is already expanded), and click on "**Configuration Assistant**" which is the only option in the expanded section.



7. Feel free to click on the "Help" link in the top right corner of the page. This type of help is available as you navigate through the Configuration Assistant panels. When you are finished exploring the Help section you may close this page using the "X" in the top right corner to return to the "Welcome" page.
8. Feel free to click on each of the links under "Learn more about Configuration Assistant:" to view other Help sections. When you are finished exploring each one you may close the page using the X in the top right corner.
   a) What's New
   b) Getting Started
   c) Migrating to z/OSMF
   d) Application Setup Tasks
   e) Tutorials
   f) FAQs
9. Configurations created by the Configuration Assistant tool are saved as Backing Store files. These files are binary files that are only usable by a Configuration Assistant tool.
   a) If necessary use the drop-down beside the "Select a backing store for configuration" field to select Backing Store file "saveData".
   b) Click on the **Open** button.



10. Click on the "**Tools**" drop down button on the right side of the page.
11. Feel free to check out the "History", "Preferences", and "Log level" sections, using the "Close" and "Cancel" to return to the above page. Then Click on the "**Manage Backing Stores**" link from the drop down.
    a) Manage Backing Stores
    b) History – shows the history of save actions for the current Backing Store file
    c) Preferences – allows customization of save options
    d) Log level – allows customization of log level options (see Help for more details)
12. Click on the "**Actions**" drop down button and then select "**Save As…**"
13. Fill in "File name" of your team name:
    a) Team21
    b) Team22
    c) Team31
    d) Team32
    e) Team41
    f) Team42
    g) Team51
    h) Team52
    i) Team61
    j) Team62
    k) Team71
    l) Team72
    m) Team201
    n) Team201
    o) Team301
    p) Team302
    q) Team401
    r) Team402
    s) Team501
    t) Team502
    u) Team601
    v) Team602
    w) Team701
    x) Team702
14. Optionally fill in a comment and click on the **OK** button.
15. If you are presented with a pop-up window "You are now working on backing store file: Team21-01", then click on the **OK** button.
16. Click on the **Close** button to return to the configuration panel.



17. You have already seen the options available with the "Tools" drop-down on the right side of the screen.
18. There are multiple tabs available for configuration:
    a) Systems – Configure z/OS images, TCP/IP stack, and start wizard for Connectivity rules.
    b) Traffic Descriptors – Define types of traffic (i.e. FTP Server traffic).
    c) Security Levels – Define security to be applied to traffic.
    d) Address Groups – IP addresses may be defined as a single IP Address, an IP subnet, a range of IP addresses, or an IP Address Group.
    e) Requirement Maps – Associate Security Levels to Traffic Descriptors.
    f) Reusable Rules – Define reusable Connectivity Rules.
19. Notice that the "Perspective" displayed is the "IPSec" perspective. Use the pull-down beside IPSec to see the different perspectives available for configuration:
    a) AT-TLS – Application Transparent – Transport Layer Security is the z/OS TLS standard protocol support available in the TCP/IP stack that can provide encryption to remote hosts with TLS support.
    b) DMD – Defence Manager Daemon provides the capability to dynamically (via the ipsec command) add IP Filter rules for a specified time frame.
    c) IDS – Intrusion Detection Services provides TCP/IP stack protection against Scans, Attacks, and also allows connection limits to be defined.
    d) IPSec – is the standard protocol support in the TCP/IP stack that can provide encryption to remote hosts with IPSec support.
    e) NSS – Network Security Server provides support to remote IKED (Internet Key Exchange Daemon) for central certificate storage, support to remote DataPower devices for certificate retrieval, and IKEv2 support.
    f) PBR – Policy Based Routing provides the capability for choosing network routes depending upon traffic types.

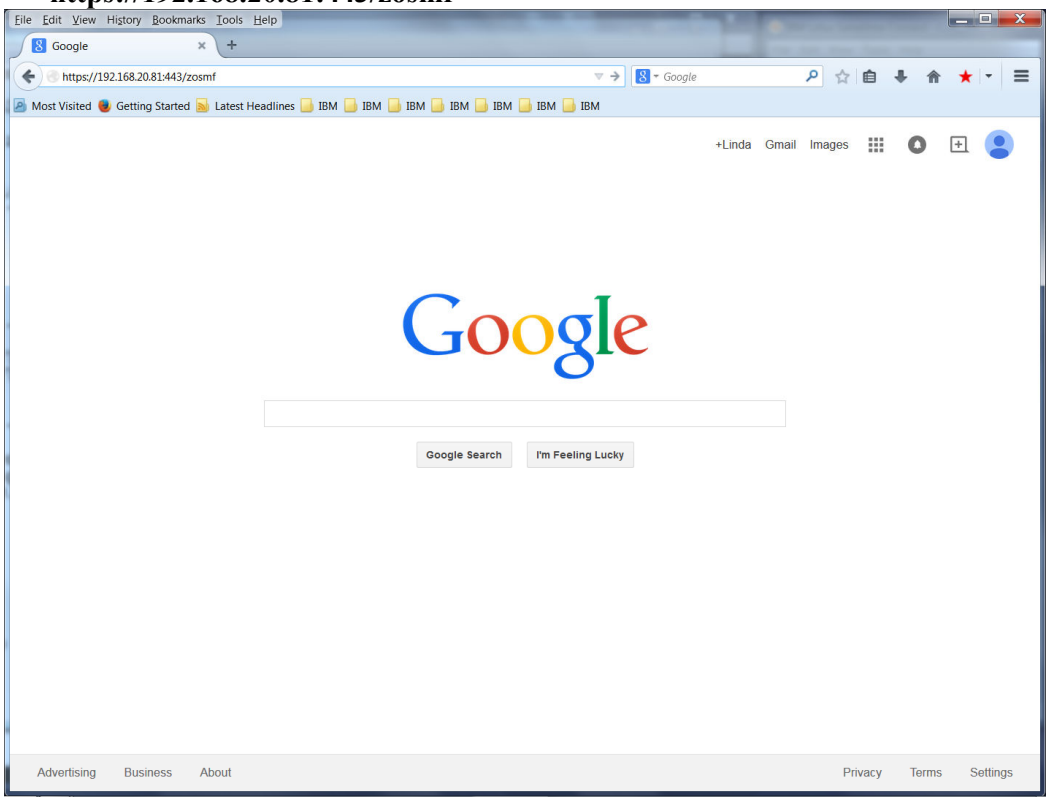
   g) QoS – Quality of Service provides different priority through the network depending upon the traffic types, and may be used to block traffic.
20. Staying on the "**IPSec**" perspective and the "**Systems**" tab, click on the "**Actions**" pull-down.
21. Select "**Add z/OS Image…**"
22. Enter a z/OS Image Name of your z/OS name:
    a) ZOS2
    b) ZOS3
    c) ZOS4
    d) ZOS5
    e) ZOS6
    f) ZOS7
23. Optionally add a description (i.e. z/OS image 2).
24. Our systems are running z/OS V2.1 so leave the default setting for z/OS Release, V2R1.
25. This image will have dynamic tunnels so enter SAF key ring database:
    a) **IKED/IKED2RING** for ZOS2
    b) **IKED/IKED3RING** for ZOS3
    c) **IKED/IKED4RING** for ZOS4
    d) **IKED/IKED5RING** for ZOS5
    e) **IKED/IKED6RING** for ZOS6
    f) **IKED/IKED7RING** for ZOS7
26. Click on the **OK** button.
27. You should be presented with a pop-up window "Proceed to the Next Step?" asking about creating a TCP/IP stack for the z/OS image.
    a) Click on the **Proceed** button.
28. Enter the TCP/IP Stack Name of **TCPIPT** or **TCPIPG**.
29. Optionally add a description (i.e. TCP/IP stack T).
30. Since you will create an IPsec tunnel in this lab leave the default indicating that this stack will be used for dynamic tunnels.
31. Click on the radio button beside "**I want to use a single identity for all IP addresses on this stack**".
32. Enter the IP Address of your 192.168.20.0 VIPA address:
    a) **192.168.20.112** for Team21 and Team22
    b) **192.168.20.113** for Team31 and Team32
    c) **192.168.20.114** for Team41 and Team42
    d) **192.168.20.115** for Team51 and Team52
    e) **192.168.20.116** for Team61 and Team62
    f) **192.168.20.117** for Team71 and Team72
    g) **192.168.20.122** for Team201 and Team202
    h) **192.168.20.123** for Team301 and Team302
    i) **192.168.20.124** for Team401 and Team402
    j) **192.168.20.125** for Team501 and Team502
    k) **192.168.20.126** for Team601 and Team602
    l) **192.168.20.127** for Team701 and Team702
33. You should be presented with a pop-up window "Proceed to the Next Step?" asking if you want to be directed to the TCP/IP stack rules panel.
    a) Click on the **Proceed** button.
34. You should be presented with a pop-up window "Proceed to the Next Step?" asking if you want to start a wizard to create a connectivity rule.
    a) Click on the **Proceed** button.

35. Skip Scenario 2 and continue with Scenario 3.

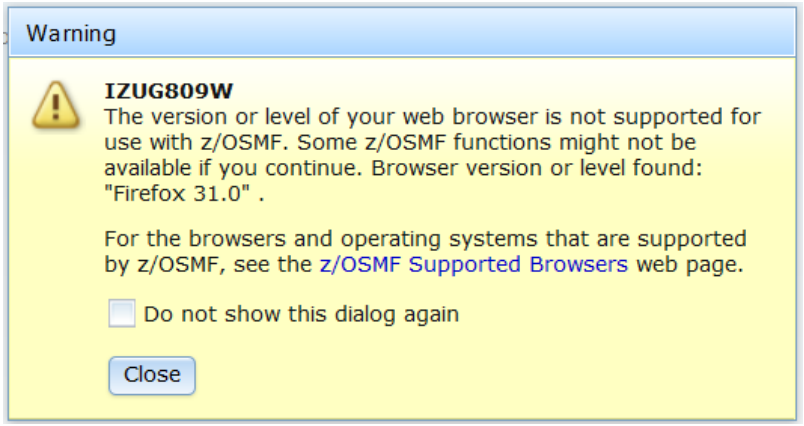
Scenario 2: Use zOSMF on ZOS1 Again

Complete this Scenario if you already connected to zOSMF for a previous lab.

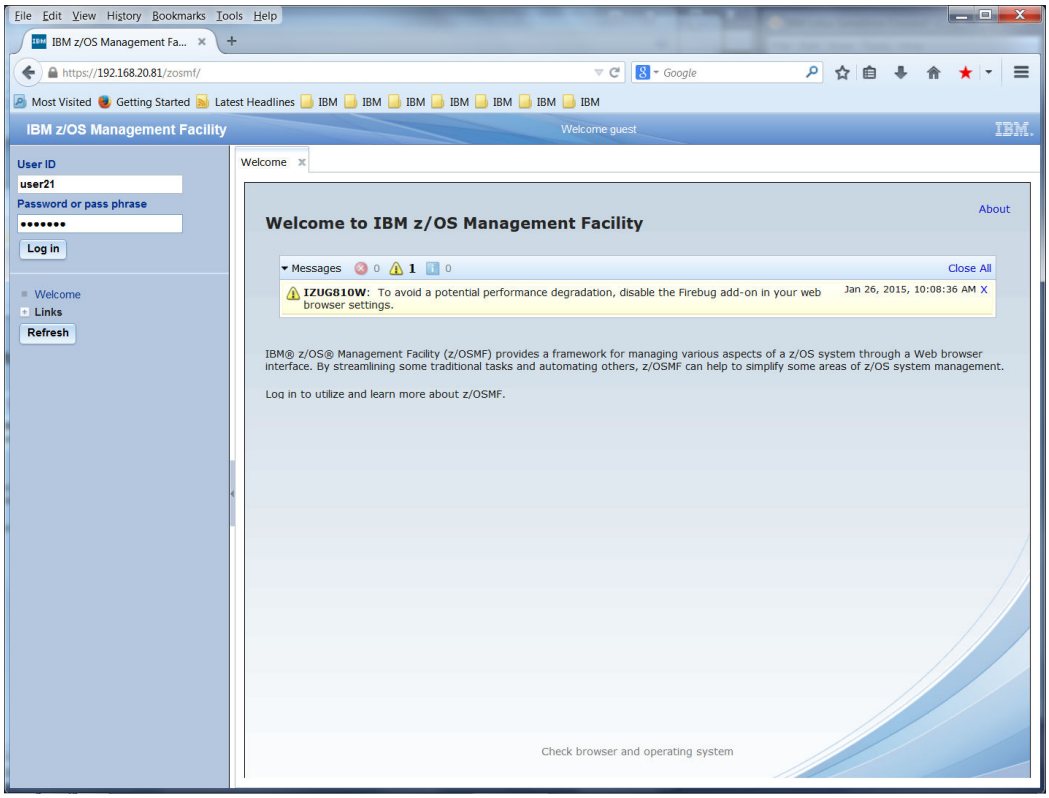
1. Open a Web Browser window and go to URL:
   https://192.168.20.81:443/zosmf



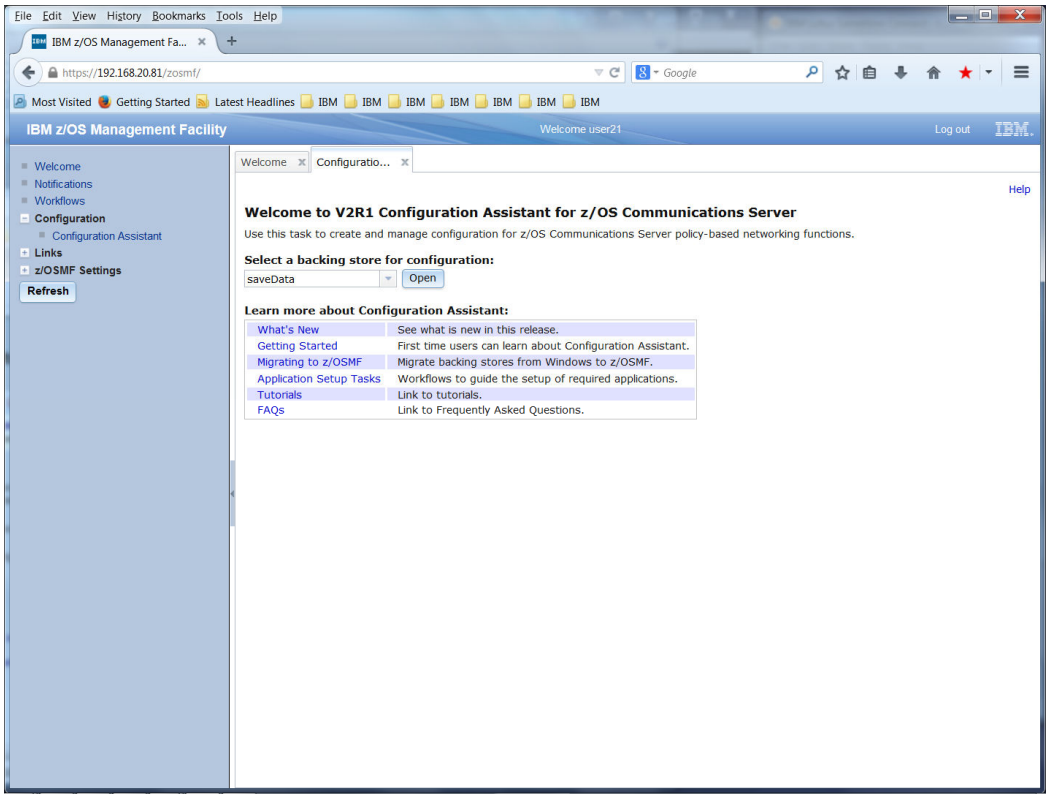
2. If a pop-up appears with warning IZUG809W warning "The version or level of your web browser is not supported for use with z/OSMF." Just ignore it and click on **Close** button.



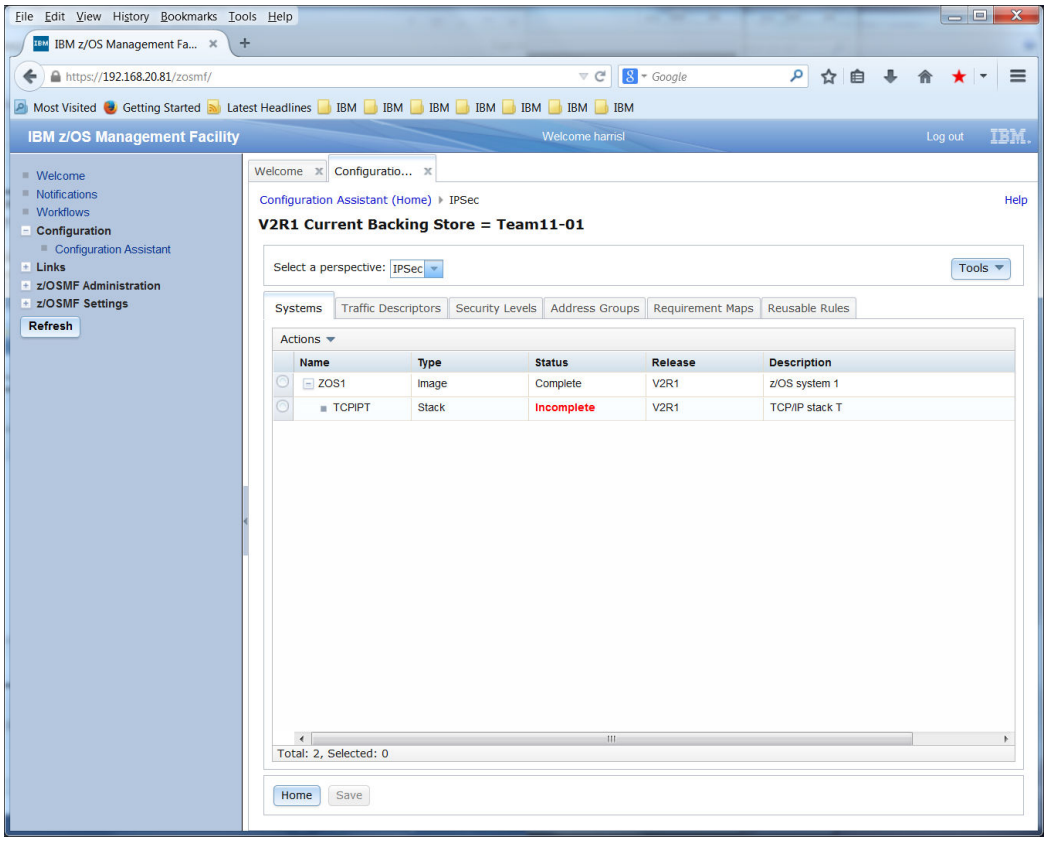
3. Logon using your Team Information Sheet to determine your z/OS User ID and password.



4. You should be presented with the "Welcome to IBM z/OS Management Facility" panel.
5. 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 "–" means that it is already expanded), and click on "**Configuration Assistant**" which is the only option in the expanded section.



6. Configurations created by the Configuration Assistant tool are saved as Backing Store files. These files are binary files that are only usable by a Configuration Assistant tool.
   a) Select your last Backing Store file.
   b) Click on the **Open** button.



7. If necessary use the drop-down to select the **IPSec** perspective.
8. Click on the radio button beside your z/OS image name.
9. Click on the "**Actions**" pull-down.
10. Select "**Properties…**"
11. Select the **IKE** tab.
12. If not already filled in, enter SAF key ring database:
    a) **IKED/IKED2RING** for ZOS2
    b) **IKED/IKED3RING** for ZOS3
    c) **IKED/IKED4RING** for ZOS4
    d) **IKED/IKED5RING** for ZOS5
    e) **IKED/IKED6RING** for ZOS6
    f) **IKED/IKED7RING** for ZOS7
13. Click on the **OK** button.
14. Click on the radio button beside TCP/IP stack TCPIPT or TCPIPG.
15. Click on the "**Actions**" pull-down.
16. Select "**Properties…**"
17. Select the **Local Identity** tab.
18. Click on the radio button beside "**I want to use a single identity for all IP addresses on this stack**".
19. Enter the IP Address of your 192.168.20.0 VIPA address:
    a) **192.168.20.112** for Team21 and Team22
    b) **192.168.20.113** for Team31 and Team32
    c) **192.168.20.114** for Team41 and Team42
    d) **192.168.20.115** for Team51 and Team52
    e) **192.168.20.116** for Team61 and Team62
    f) **192.168.20.117** for Team71 and Team72
    g) **192.168.20.122** for Team201 and Team202

h) **192.168.20.123** for Team301 and Team302
i) **192.168.20.124** for Team401 and Team402
j) **192.168.20.125** for Team501 and Team502
k) **192.168.20.126** for Team601 and Team602
l) **192.168.20.127** for Team701 and Team702

20. Select the **Stack Setting** tab.
21. Click on the radio button beside **IKEv2**.
22. Click on **OK** button.
23. Click on the "**Actions**" pull-down.
24. Select "**Rules…**"
25. Click on the "**Actions**" pull-down.
26. Select "**New…**"

Scenario 3: Configure IPsec Rules

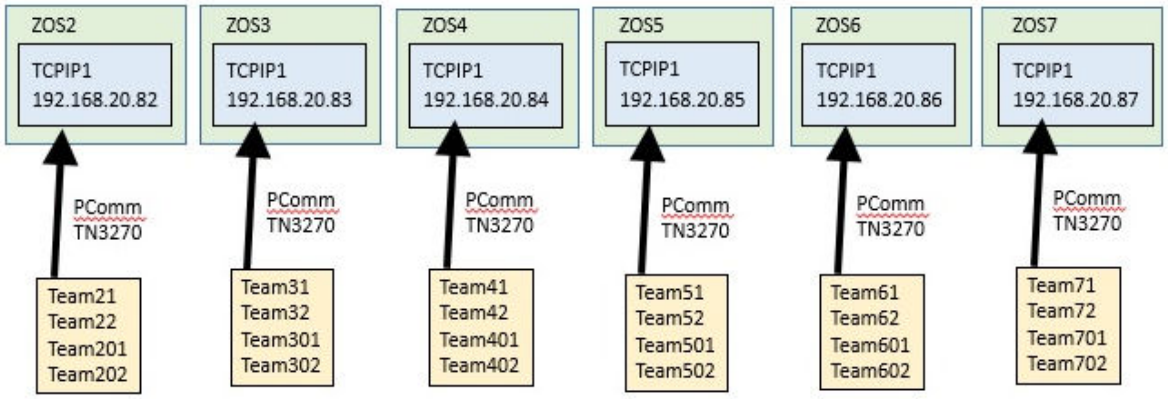
1. Click the **Next** button to accept the default connectivity rule type of Typical.
2. Click on the radio button next to "**Filtering only**" to create an IP Filter rule for the IDS lab. Leave the default "For local traffic" selected.
3. Click on the **Next** button.
4. Enter a Connectivity rule name (i.e. **PermitTN3270**).
5. Optionally add a description.
6. Enter Local and Remote data endpoint IP address range:
   192.168.20.91-192.168.20.107
7. Click on the **Next** button.
8. Leave "Create a new requirement map" selected.
9. Enter a Requirement Map name (i.e. **TN3270Clear**).
10. Optionally add a description.
11. If necessary (if there are no rows available) use the "Actions" pull-down to select **Add Row**.
12. In the top row double click the area where the field says "Select a traffic descriptor" until a pull-down arrow appears.
    a) Use the pull-down to select **TN3270-Server**.
13. Double click the area where the field says "Select a security level" until a pull-down arrow appears.
    a) Use the pull-down to select **Permit**.
14. Use the radio button to select each of the extra rows in turn and use the "Actions" pull-down to select **Remove Row**.
15. Click on the **Next** button.
16. Use the radio button to select "**Yes, log all filter matches**".
17. Click on the **Finish** button.
18. Use the "Actions" pull-down to select "**New…**"
19. Click the **Next** button to accept the default connectivity rule type of Typical.
20. Click the **Next** button to accept the default IPSec tunnels with Host to Host topology.
21. Enter a Connectivity rule name:
    a) **PingT2toT1** for Team21 and Team22
    b) **PingT3toT1** for Team31 and Team32
    c) **PingT4toT1** for Team41 and Team42
    d) **PingT5toT1** for Team51 and Team52
    e) **PingT6toT1** for Team61 and Team62
    f) **PingT7toT1** for Team71 and Team72
    g) **PingG2toG1** for Team201 and Team202
    h) **PingG3toG1** for Team301 and Team302
    i) **PingG4toG1** for Team401 and Team402
    j) **PingG5toG1** for Team501 and Team502
    k) **PingG6toG1** for Team601 and Team602
    l) **PingG7toG1** for Team701 and Team702
22. Optionally add a description.
23. Enter Local data endpoint IP address:
    a) 192.168.20.112 for Team21 and Team22
    b) 192.168.20.113 for Team31 and Team32
    c) 192.168.20.114 for Team41 and Team42
    d) 192.168.20.115 for Team51 and Team52

   e) 192.168.20.116 for Team61 and Team62
   f) 192.168.20.117 for Team71 and Team72
   g) 192.168.20.122 for Team201 and Team202
   h) 192.168.20.123 for Team301 and Team302
   i) 192.168.20.124 for Team401 and Team402
   j) 192.168.20.125 for Team501 and Team502
   k) 192.168.20.126 for Team601 and Team602
   l) 192.168.20.127 for Team701 and Team702
24. Enter Remote data endpoint IP address:
   a) 192.168.20.111 for TCPIPT
   b) 192.168.20.121 for TCPIPG
25. Under "Indicate how to authenticate the IKE peers":
   a) Select the radio button beside "Shared key".
   b) Leave "EBCDIC" selected.
   c) Fill in Key **IPsec Share Lab**
26. Click on the **Next** button.
27. Leave "Create a new requirement map" selected.
28. Enter a Requirement Map name (i.e. **EncryptPing**).
29. Optionally add a description.
30. If necessary (if there are no rows available) use the "Actions" pull-down to select **Add Row**.
31. In the top row double click the area where the field says "Select a traffic descriptor" until a pull-down arrow appears.
   a) Use the pull-down to select **ICMP~IPv4**.
32. Double click the area where the field says "Select a security level" until a pull-down arrow appears.
   a) Use the pull-down to select **VPN~A**.
33. Use the radio button to select each of the extra rows in turn and use the "Action" pull-down to select **Remove Row**.
34. Click on the **Next** button.
35. Use the radio button to select "**Yes, log all filter matches**".
36. Click on the **Finish** button.
37. Click on the **Close** button.
38. Click on the **Save** button.
39. Optionally enter comments and click on **OK** button.

Scenario 4: Install IPsec Rules

1. Click on the "**Actions**" drop down button and then select "**Install All Files for IPSec…**"
2. Select your TCP/IP stack policy file:
   a) TCPIPT – IP Security Policy
   b) TCPIPG – IP Security Policy
3. Click on the "**Actions**" drop down button and then select "**Install**".
4. Fill in your userid's unix home directory and file name with your TCP/IP stack name:
   a) /u/user21/ZOS2_TCPIP**T**_IPSec.policy
   b) /u/user22/ZOS2_TCPIP**T**_IPSec.policy
   c) /u/user31/ZOS3_TCPIP**T**_IPSec.policy
   d) /u/user32/ZOS3_TCPIP**T**_IPSec.policy
   e) /u/user41/ZOS4_TCPIP**T**_IPSec.policy
   f) /u/user42/ZOS4_TCPIP**T**_IPSec.policy
   g) /u/user51/ZOS5_TCPIP**T**_IPSec.policy
   h) /u/user52/ZOS5_TCPIP**T**_IPSec.policy
   i) /u/user61/ZOS6_TCPIP**T**_IPSec.policy
   j) /u/user62/ZOS6_TCPIP**T**_IPSec.policy
   k) /u/user71/ZOS7_TCPIP**T**_IPSec.policy
   l) /u/user72/ZOS7_TCPIP**T**_IPSec.policy
   m) /u/user201/ZOS2_TCPIP**G**_IPSec.policy
   n) /u/user202/ZOS2_TCPIP**G**_IPSec.policy
   o) /u/user301/ZOS3_TCPIP**G**_IPSec.policy
   p) /u/user302/ZOS3_TCPIP**G**_IPSec.policy
   q) /u/user401/ZOS4_TCPIP**G**_IPSec.policy
   r) /u/user402/ZOS4_TCPIP**G**_IPSec.policy
   s) /u/user501/ZOS5_TCPIP**G**_IPSec.policy
   t) /u/user502/ZOS5_TCPIP**G**_IPSec.policy
   u) /u/user601/ZOS6_TCPIP**G**_IPSec.policy
   v) /u/user602/ZOS6_TCPIP**G**_IPSec.policy
   w) /u/user701/ZOS7_TCPIP**G**_IPSec.policy
   x) /u/user702/ZOS7_TCPIPG_IPSec.policy
5. Click the radio button beside **FTP** to select the installation method.
6. Enter your TCPIP1 IP address for the system Host name:
   a) 192.168.20.82 for ZOS2
   b) 192.168.20.83 for ZOS3
   c) 192.168.20.84 for ZOS4
   d) 192.168.20.85 for ZOS5
   e) 192.168.20.86 for ZOS6
   f) 192.168.20.87 for ZOS7
7. Fill in your userid and password.
8. Click on the **Go** button.
9. When the pop-up "The FTP file transfer was successful." appears click on the **OK** button.
10. Click on the **Close** button.
11. Optionally enter a comment and click on the **OK** button.
12. Click on the **Close** button.

Scenario 5: Test IPSec Policy on z/OS



1. On your Lab PC use PComm to logon to your z/OS system:
   a) 192.168.20.82 for ZOS2
   b) 192.168.20.83 for ZOS3
   c) 192.168.20.84 for ZOS4
   d) 192.168.20.85 for ZOS5
   e) 192.168.20.86 for ZOS6
   f) 192.168.20.87 for ZOS7
2. When you see the Message 10 screen from the TN3270 server, provide your userid 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** (the PComm **ENTER key** is the **Right Ctrl** key)
4. Move to the SDSF panel when you see the **READY** prompt:
   a) **ispf**
5. Move to the TSO command interface:
   a) **6**
6. View your IKED Key Ring:
   a) RACDCERT ID(IKED) LISTRING(IKED2RING)
   b) RACDCERT ID(IKED) LISTRING(IKED3RING)
   c) RACDCERT ID(IKED) LISTRING(IKED4RING)
   d) RACDCERT ID(IKED) LISTRING(IKED5RING)
   e) RACDCERT ID(IKED) LISTRING(IKED6RING)
   f) RACDCERT ID(IKED) LISTRING(IKED7RING)
7. View your IKED Certificate:
   a) RACDCERT ID(IKED) LIST(LABEL('IKEDS2 at ZOS2')
   b) RACDCERT ID(IKED) LIST(LABEL('IKEDS3 at ZOS3')
   c) RACDCERT ID(IKED) LIST(LABEL('IKEDS4 at ZOS4')
   d) RACDCERT ID(IKED) LIST(LABEL('IKEDS5 at ZOS5')
   e) RACDCERT ID(IKED) LIST(LABEL('IKEDS6 at ZOS6')
   f) RACDCERT ID(IKED) LIST(LABEL('IKEDS7 at ZOS7')
8. When you are finished reviewing the certificate information return to the main ISPF panel:
   a) **PF3**

9. Enter **O.4** (the letter "O") to go to the OMVS Unix environment. Remember the PComm ENTER key is the Right Ctrl key.
10. Enter **su** to change into Super User mode.
11. View the Main Pagent Configuration file:
    a) **obrowse /etc/PAGT1/pagentt.conf**
12. Notice that the Main Pagent Configuration file points to the two z/OS image files:
    a) /etc/PAGT1/pagent.tcpipt.conf for TCP/IP stack TCPIPT
    b) /etc/PAGT1/pagent.tcpipg.conf for TCP/IP stack TCPIPG
13. **PF3** to exit out of browse.
14. View an image file that has been provided for you in your home directory:
    a) **obrowse /u/user21/pagent.tcpipt.conf** for Team21
    b) **obrowse /u/user22/pagent.tcpipt.conf** for Team22
    c) **obrowse /u/user31/pagent.tcpipt.conf** for Team31
    d) **obrowse /u/user32/pagent.tcpipt.conf** for Team32
    e) **obrowse /u/user41/pagent.tcpipt.conf** for Team41
    f) **obrowse /u/user42/pagent.tcpipt.conf** for Team42
    g) **obrowse /u/user51/pagent.tcpipt.conf** for Team51
    h) **obrowse /u/user52/pagent.tcpipt.conf** for Team52
    i) **obrowse /u/user61/pagent.tcpipt.conf** for Team61
    j) **obrowse /u/user62/pagent.tcpipt.conf** for Team62
    k) **obrowse /u/user71/pagent.tcpipt.conf** for Team71
    l) **obrowse /u/user72/pagent.tcpipt.conf** for Team72
    m) **obrowse /u/user201/pagent.tcpipg.conf** for Team201
    n) **obrowse /u/user202/pagent.tcpipg.conf** for Team202
    o) **obrowse /u/user301/pagent.tcpipg.conf** for Team301
    p) **obrowse /u/user302/pagent.tcpipg.conf** for Team302
    q) **obrowse /u/user401/pagent.tcpipg.conf** for Team401
    r) **obrowse /u/user402/pagent.tcpipg.conf** for Team402
    s) **obrowse /u/user501/pagent.tcpipg.conf** for Team501
    t) **obrowse /u/user502/pagent.tcpipg.conf** for Team502
    u) **obrowse /u/user601/pagent.tcpipg.conf** for Team601
    v) **obrowse /u/user602/pagent.tcpipg.conf** for Team602
    w) **obrowse /u/user701/pagent.tcpipg.conf** for Team701
    x) **obrowse /u/user702/pagent.tcpipg.conf** for Team702
15. Notice the IPsec policy file that is defined:
    a) IPSecConfig /u/user21/ZOS2_TCPIPT_IPSec.policy FLUSH PURGE
    b) IPSecConfig /u/user22/ZOS2_TCPIPT_IPSec.policy FLUSH PURGE
    c) IPSecConfig /u/user31/ZOS3_TCPIPT_IPSec.policy FLUSH PURGE
    d) IPSecConfig /u/user32/ZOS3_TCPIPT_IPSec.policy FLUSH PURGE
    e) IPSecConfig /u/user41/ZOS4_TCPIPT_IPSec.policy FLUSH PURGE
    f) IPSecConfig /u/user42/ZOS4_TCPIPT_IPSec.policy FLUSH PURGE
    g) IPSecConfig /u/user51/ZOS5_TCPIPT_IPSec.policy FLUSH PURGE
    h) IPSecConfig /u/user52/ZOS5_TCPIPT_IPSec.policy FLUSH PURGE
    i) IPSecConfig /u/user61/ZOS6_TCPIPT_IPSec.policy FLUSH PURGE
    j) IPSecConfig /u/user62/ZOS6_TCPIPT_IPSec.policy FLUSH PURGE
    k) IPSecConfig /u/user71/ZOS7_TCPIPT_IPSec.policy FLUSH PURGE
    l) IPSecConfig /u/user72/ZOS7_TCPIPT_IPSec.policy FLUSH PURGE
    m) IPSecConfig /u/user201/ZOS2_TCPIPT_IPSec.policy FLUSH PURGE
    n) IPSecConfig /u/user202/ZOS2_TCPIPT_IPSec.policy FLUSH PURGE
    o) IPSecConfig /u/user301/ZOS3_TCPIPT_IPSec.policy FLUSH PURGE
    p) IPSecConfig /u/user302/ZOS3_TCPIPT_IPSec.policy FLUSH PURGE

q) IPSecConfig /u/user401/ZOS4_TCPIPT_IPSec.policy FLUSH PURGE
r) IPSecConfig /u/user402/ZOS4_TCPIPT_IPSec.policy FLUSH PURGE
s) IPSecConfig /u/user501/ZOS5_TCPIPT_IPSec.policy FLUSH PURGE
t) IPSecConfig /u/user502/ZOS5_TCPIPT_IPSec.policy FLUSH PURGE
u) IPSecConfig /u/user601/ZOS6_TCPIPT_IPSec.policy FLUSH PURGE
v) IPSecConfig /u/user602/ZOS6_TCPIPT_IPSec.policy FLUSH PURGE
w) IPSecConfig /u/user701/ZOS7_TCPIPT_IPSec.policy FLUSH PURGE
x) IPSecConfig /u/user702/ZOS7_TCPIPT_IPSec.policy FLUSH PURGE

16. **PF3** to exit out of browse.
17. If you did not previously complete the AT-TLS lab successfully you can use an AT-TLS policy file that has been provided to you.
    - cp /u/user21/TTLS.policy.test /u/user21/ZOS2_TCPIPT_TTLS.policy
    - cp /u/user22/TTLS.policy.test /u/user22/ZOS2_TCPIPT_TTLS.policy
    - cp /u/user31/TTLS.policy.test /u/user31/ZOS3_TCPIPT_TTLS.policy
    - cp /u/user32/TTLS.policy.test /u/user32/ZOS3_TCPIPT_TTLS.policy
    - cp /u/user41/TTLS.policy.test /u/user41/ZOS4_TCPIPT_TTLS.policy
    - cp /u/user42/TTLS.policy.test /u/user42/ZOS4_TCPIPT_TTLS.policy
    - cp /u/user51/TTLS.policy.test /u/user51/ZOS5_TCPIPT_TTLS.policy
    - cp /u/user52/TTLS.policy.test /u/user52/ZOS5_TCPIPT_TTLS.policy
    - cp /u/user61/TTLS.policy.test /u/user61/ZOS6_TCPIPT_TTLS.policy
    - cp /u/user62/TTLS.policy.test /u/user62/ZOS6_TCPIPT_TTLS.policy
    - cp /u/user71/TTLS.policy.test /u/user71/ZOS7_TCPIPT_TTLS.policy
    - cp /u/user72/TTLS.policy.test /u/user72/ZOS7_TCPIPT_TTLS.policy
    - cp /u/user201/TTLS.policy.test /u/user201/ZOS2_TCPIPG_TTLS.policy
    - cp /u/user202/TTLS.policy.test /u/user202/ZOS2_TCPIPG_TTLS.policy
    - cp /u/user301/TTLS.policy.test /u/user301/ZOS3_TCPIPG_TTLS.policy
    - cp /u/user302/TTLS.policy.test /u/user302/ZOS3_TCPIPG_TTLS.policy
    - cp /u/user401/TTLS.policy.test /u/user401/ZOS4_TCPIPG_TTLS.policy
    - cp /u/user402/TTLS.policy.test /u/user402/ZOS4_TCPIPG_TTLS.policy
    - cp /u/user501/TTLS.policy.test /u/user501/ZOS5_TCPIPG_TTLS.policy
    - cp /u/user502/TTLS.policy.test /u/user502/ZOS5_TCPIPG_TTLS.policy
    - cp /u/user601/TTLS.policy.test /u/user601/ZOS6_TCPIPG_TTLS.policy
    - cp /u/user602/TTLS.policy.test /u/user602/ZOS6_TCPIPG_TTLS.policy
    - cp /u/user701/TTLS.policy.test /u/user701/ZOS7_TCPIPG_TTLS.policy
    - cp /u/user702/TTLS.policy.test /u/user702/ZOS7_TCPIPG_TTLS.policy
18. **Warning!** In the next steps you must coordinate your testing with the other team that is using your TCP/IP stack, if there is another team.
19. These teams must coordinate testing:
    a) Team21 and Team22 both use TCPIPT on ZOS2
    b) Team31 and Team32 both use TCPIPT on ZOS3
    c) Team41 and Team42 both use TCPIPT on ZOS4
    d) Team51 and Team52 both use TCPIPT on ZOS5
    e) Team61 and Team62 both use TCPIPT on ZOS6
    f) Team71 and Team72 both use TCPIPT on ZOS7
    g) Team201 and Team202 both use TCPIPG on ZOS2
    h) Team301 and Team302 both use TCPIPG on ZOS3
    i) Team401 and Team402 both use TCPIPG on ZOS4
    j) Team501 and Team502 both use TCPIPG on ZOS5
    k) Team601 and Team602 both use TCPIPG on ZOS6

l) Team701 and Team702 both use TCPIPG on ZOS7

20. Copy your image file to directory /etc/PAGT1:
    a) **cp /u/user21/pagent.tcpipt.conf /etc/PAGT1/.**
    b) **cp /u/user22/pagent.tcpipt.conf /etc/PAGT1.**
    c) **cp /u/user31/pagent.tcpipt.conf /etc/PAGT1.**
    d) **cp /u/user32/pagent.tcpipt.conf /etc/PAGT1.**
    e) **cp /u/user41/pagent.tcpipt.conf /etc/PAGT1.**
    f) **cp /u/user42/pagent.tcpipt.conf /etc/PAGT1.**
    g) **cp /u/user51/pagent.tcpipt.conf /etc/PAGT1.**
    h) **cp /u/user52/pagent.tcpipt.conf /etc/PAGT1.**
    i) **cp /u/user61/pagent.tcpipt.conf /etc/PAGT1.**
    j) **cp /u/user62/pagent.tcpipt.conf /etc/PAGT1.**
    k) **cp /u/user71/pagent.tcpipt.conf /etc/PAGT1.**
    l) **cp /u/user72/pagent.tcpipt.conf /etc/PAGT1.**
    m) **cp /u/user201/pagent.tcpipg.conf /etc/PAGT1.**
    n) **cp /u/user202/pagent.tcpipg.conf /etc/PAGT1.**
    o) **cp /u/user301/pagent.tcpipg.conf /etc/PAGT1.**
    p) **cp /u/user302/pagent.tcpipg.conf /etc/PAGT1.**
    q) **cp /u/user401/pagent.tcpipg.conf /etc/PAGT1.**
    r) **cp /u/user402/pagent.tcpipg.conf /etc/PAGT1.**
    s) **cp /u/user501/pagent.tcpipg.conf /etc/PAGT1.**
    t) **cp /u/user502/pagent.tcpipg.conf /etc/PAGT1.**
    u) **cp /u/user601/pagent.tcpipg.conf /etc/PAGT1.**
    v) **cp /u/user602/pagent.tcpipg.conf /etc/PAGT1.**
    w) **cp /u/user701/pagent.tcpipg.conf /etc/PAGT1.**
    x) **cp /u/user702/pagent.tcpipg.conf /etc/PAGT1.**
21. Return to the ISPF panel by entering **exit** command twice (once to get out of su mode and once to get out of OMVS).
22. Policy Agent is also referred to as PAGENT because that is the default procedure name. In our lab the procedure name is PAGENTT. Please don't be confused by this. The same Policy Agent provides support for all three TCP/IP stacks: TCPIP1 (even though there are no policies defined for this stack), TCPIPT, and TCPIPG.
23. When Policy Agent is started or when a Modify, "F", command is issued, the Policy Agent will read in the defined policies and load them into the appropriate TCP/IP stack. It is the TCP/IP stack that enforces those policies.
24. **3.4** and press Enter
25. Dsname Level **SYS1.CS.TCPPARMS** and press Enter
26. **B** to the left of SYS1.CS.TCPPARMS and press Enter
27. **B** to the left of your PROFILE.TCPIP file and press Enter:
    a) TCPS25 for TCPIPT on ZOS2
    b) TCPS35 for TCPIPT on ZOS3
    c) TCPS45 for TCPIPT on ZOS4
    d) TCPS55 for TCPIPT on ZOS5
    e) TCPS65 for TCPIPT on ZOS6
    f) TCPS75 for TCPIPT on ZOS7
    m) TCPS26 for TCPIPG on ZOS2
    m) TCPS36 for TCPIPG on ZOS3
    m) TCPS46 for TCPIPG on ZOS4
    m) TCPS56 for TCPIPG on ZOS5
    m) TCPS66 for TCPIPG on ZOS6
    m) TCPS76 for TCPIPG on ZOS7
28. You should be viewing the PROFILE.TCPIP file for your TCP/IP stack. Notice the following:
    a) IPCONFIG IPSECURITY – required for IP Filtering and IPSec
    b) TCPCONFIG TTLS – required for AT-TLS
    c) **PF3** to exit when you are done reviewing the file.
29. Go to the ISPD Log:

a) **D.LOG**

30. Display your TCP/IP stack's configuration:
    a) **/D TCPIP,TCPIPT,NETSTAT,CONFIG**
    b) **/D TCPIP,TCPIPG,NETSTAT,CONIG**
31. Notice the following:
    a) **TTLS: YES** – a result of IPCONFIG IPSECURITY in the profile file
    b) **IPSECURITY: YES** – a result of TCPCONFIG TTLS in the profile file
32. **Warning!** In the next steps you must coordinate your testing with the other teams using the same Policy Agent as you are:
    a) Team21, Team22, Team201, and Team202 on ZOS2
    b) Team31, Team32, Team301, and Team302 on ZOS3
    c) Team41, Team42, Team401, and Team402 on ZOS4
    d) Team51, Team52, Team501, and Team502 on ZOS5
    e) Team61, Team62, Team601, and Team602 on ZOS6
    f) Team71, Team72, Team701, and Team702 on ZOS7
33. Cause the Policy Agent to reread its policy files:
    a) **/F PAGENTT,UPDATE**
34. Let the other Teams on the other TCP/IP stack know that you are done updating the Policy Agent. The Team on your same TCP/IP stack will still be impacted in the following steps.
    a) If you are using TCPIPT on system ZOSn then let the Teams using TCPIPG on system ZOSn know you are done updating the Policy Agent.
    b) If you are using TCPIPG on system ZOSn then let the Teams using TCPIPT on system ZOSn know you are done updating the Policy Agent.
35. Return to OMVS to test the AT-TLS policies:
    a) **=o.4**
36. Use Ping to test your IPSec definitions. **Note** you must issue the command several times (PF12 is the recall key) because the first time the command is issued the IPSec tunnel has not been built yet.
    a) ping –p TCPIP**T** 192.168.20.111
    b) ping –p TCPIP**G** 192.168.20.121
37. If your Ping was successful you should look at the messages in SyslogD.
    a) While you are in OMVS:
        i. **su**
        ii. **obrowse /var/syslogall.log**
    b) You have finished the lab and do not need to proceed any further.
        i. Remember to let the other Team that shares your TCP/IP stack know that you are done testing.
38. If the Ping fails you should continue with the rest of the lab.
39. You should do web searches on the errors you are getting.
    a) Look for errors in the SyslogD error log while you are in OMVS:
        i. **su**
        ii. **obrowse /var/syslogall.log**
    b) Look for errors in the console log (=D.LOG)
40. Back in OMVS, make sure you are in your own directory:
    a) **pwd**
    b) If you are not in your home directory then change to your directory:
        i. cd /u/user21
        ii. cd /u/user22
        iii. cd /u/user31
        iv. cd /u/user32
        xiii. cd /u/user201
        xiv. cd /u/user202
        xv. cd /u/user301
        xvi. cd /u/user302

v. cd /u/user41
vi. cd /u/user42
vii. cd /u/user51
viii. cd /u/user52
ix. cd /u/user61
x. cd /u/user62
xi. cd /u/user71
xii. cd /u/user72
xvii. cd /u/user401
xviii. cd /u/user402
xix. cd /u/user501
xx. cd /u/user502
xxi. cd /u/user601
xxii. cd /u/user602
xxiii. cd /u/user701
xxiv. cd /u/user702

41. You can test the environment to make sure it is setup correctly by testing with a working policy file that has been created for you.
    a) Rename your policy file to a different file name.
        - mv ZOS2_TCPIPT_IPSec.policy ZOS2_TCPIPT_IPSec.policy.failed
        - mv ZOS3_TCPIPT_IPSec.policy ZOS3_TCPIPT_IPSec.policy.failed
        - mv ZOS4_TCPIPT_IPSec.policy ZOS4_TCPIPT_IPSec.policy.failed
        - mv ZOS5_TCPIPT_IPSec.policy ZOS5_TCPIPT_IPSec.policy.failed
        - mv ZOS6_TCPIPT_IPSec.policy ZOS6_TCPIPT_IPSec.policy.failed
        - mv ZOS7_TCPIPT_IPSec.policy ZOS7_TCPIPT_IPSec.policy.failed
    b) Copy the one provided for you:
        - cp /u/user21/IPSec.policy.test /u/user21/ZOS2_TCPIPT_IPSec.policy
        - cp /u/user22/IPSec.policy.test /u/user22/ZOS2_TCPIPT_IPSec.policy
        - cp /u/user31/IPSec.policy.test /u/user31/ZOS3_TCPIPT_IPSec.policy
        - cp /u/user32/IPSec.policy.test /u/user32/ZOS3_TCPIPT_IPSec.policy
        - cp /u/user41/IPSec.policy.test /u/user41/ZOS4_TCPIPT_IPSec.policy
        - cp /u/user42/IPSec.policy.test /u/user42/ZOS4_TCPIPT_IPSec.policy
        - cp /u/user51/IPSec.policy.test /u/user51/ZOS5_TCPIPT_IPSec.policy
        - cp /u/user52/IPSec.policy.test /u/user52/ZOS5_TCPIPT_IPSec.policy
        - cp /u/user61/IPSec.policy.test /u/user61/ZOS6_TCPIPT_IPSec.policy
        - cp /u/user62/IPSec.policy.test /u/user62/ZOS6_TCPIPT_IPSec.policy
        - cp /u/user71/IPSec.policy.test /u/user71/ZOS7_TCPIPT_IPSec.policy
        - cp /u/user72/IPSec.policy.test /u/user72/ZOS7_TCPIPT_IPSec.policy
        - cp /u/user201/IPSec.policy.test /u/user201/ZOS2_TCPIPG_IPSec.policy
        - cp /u/user202/IPSec.policy.test /u/user202/ZOS2_TCPIPG_IPSec.policy
        - cp /u/user301/IPSec.policy.test /u/user301/ZOS3_TCPIPG_IPSec.policy
        - cp /u/user302/IPSec.policy.test /u/user302/ZOS3_TCPIPG_IPSec.policy
        - cp /u/user401/IPSec.policy.test /u/user401/ZOS4_TCPIPG_IPSec.policy
        - cp /u/user402/IPSec.policy.test /u/user402/ZOS4_TCPIPG_IPSec.policy
        - cp /u/user501/IPSec.policy.test /u/user501/ZOS5_TCPIPG_IPSec.policy
        - cp /u/user502/IPSec.policy.test /u/user502/ZOS5_TCPIPG_IPSec.policy
        - cp /u/user601/IPSec.policy.test /u/user601/ZOS6_TCPIPG_IPSec.policy
        - cp /u/user602/IPSec.policy.test /u/user602/ZOS6_TCPIPG_IPSec.policy
        - cp /u/user701/IPSec.policy.test /u/user701/ZOS7_TCPIPG_IPSec.policy
        - cp /u/user702/IPSec.policy.test /u/user702/ZOS7_TCPIPG_IPSec.policy
42. Use what you learned previously to test again.
43. Let the other Team that shares your TCP/IP stack know that you are done testing.

End of the Lab

Appendix: System Files

TCPIPT Proc

```
//TCPIPT PROC
PARMS='CTRACE(CTIEZB00)',PROF=TCP&CL1.A,DATA=DAT&CL1.A,
//    CS=SYS1
//*   CS=USER
//TCPIP  EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//    PARM='&PARMS'
//*           PARM='&MODULE,ERRFILE(SYSERR),HEAP(512),&PARMS'
//*TEPLIB  DD DSN=SYS1.TCPIP.SEZATCP,DISP=SHR
//*        DD DSN=SYS1.TCPIP.SEZALINK,DISP=SHR
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSERROR DD SYSOUT=*
//SYSMDUMP DD SYSOUT=*
//SYSERR   DD SYSOUT=*
//SYSDEBUG DD SYSOUT=*
//PROFILE  DD DSN=&CS..CS.TCPPARMS(&PROF),DISP=SHR
//SYSTCPD  DD DSN=&CS..CS.TCPPARMS(&DATA),DISP=SHR
```

TCPIPG Proc

```
//TCPIPG PROC
PARMS='CTRACE(CTIEZB00)',PROF=TCPS&CL1.3,DATA=DATAG,
//    CS=SYS1
//*   CS=USER
//TCPIP  EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//    PARM='&PARMS'
//*           PARM='&MODULE,ERRFILE(SYSERR),HEAP(512),&PARMS'
//*TEPLIB  DD DSN=SYS1.TCPIP.SEZATCP,DISP=SHR
//*        DD DSN=SYS1.TCPIP.SEZALINK,DISP=SHR
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSERROR DD SYSOUT=*
//SYSMDUMP DD SYSOUT=*
//SYSERR   DD SYSOUT=*
//SYSDEBUG DD SYSOUT=*
//PROFILE  DD DSN=&CS..CS.TCPPARMS(&PROF),DISP=SHR
//SYSTCPD  DD DSN=&CS..CS.TCPPARMS(&DATA),DISP=SHR
```

Pagent Main Configuration File

```
# CHANGE RECORD
# ================================================================
# Change for Winter Share 2015                LLH 02/22/15
# ================================================================
#
# LogLevel Statement
# LogLevel 31
# LogLevel 127
  LogLevel 511
#
# TcpImage and PEPInstance Statements (synonyms)
  TcpImage TCPIPT /etc/PAGT1/pagent.tcpipt.conf FLUSH PURGE 3600
  TcpImage TCPIPG /etc/PAGT1/pagent.tcpipg.conf FLUSH PURGE 3600
#
```

Pagent TCPIPT Image Configuration File

```
# CHANGE RECORD
# ================================================================
# Change for Winter Share 2015                LLH 02/22/15
#
================================================================
#
# IDSConfig Statements
  IDSConfig /u/user21/ZOS2_TCPIPT_IDS.policy FLUSH PURGE
#
# IPSecConfig Statements
  IPSecConfig /u/user11/ZOS2_TCPIPT_IPSec.policy
#
# RoutingConfig Statements
  RoutingConfig /u/user21/ZOS2_TCPIPT_Routing.policy
#
# TTLSConfig Statements
  TTLSConfig /u/user11/ZOS2_TCPIPT_TTLS.policy FLUSH PURGE
#
# QOSConfig Statement
  QOSConfig /u/user21/ZOS2_TCPIPT_QoS.policy
#
```

Pagent TCPIPG Image Configuration File

```
# CHANGE RECORD
# ================================================================
# Change for Winter Share 2015                LLH 02/22/15
#
================================================================
#
# IDSConfig Statements
  IDSConfig /u/user201/ZOS2_TCPIPG_IDS.policy FLUSH PURGE
```

```
#
# IPSecConfig Statements
 IPSecConfig /u/user201/ZOS2_TCPIPG_IPSec.policy
#
# RoutingConfig Statements
 RoutingConfig /u/user201/ZOS2_TCPIPG_Routing.policy
#
# TTLSConfig Statements
 TTLSConfig /u/user201/ZOS2_TCPIPG_TTLS.policy FLUSH PURGE
#
# QOSConfig Statement
 QOSConfig /u/user201/ZOS2_TCPIPG_QoS.policy
#
```

IKED Key Ring

```
Ring:
     >IKEDS2Ring<
Certificate Label Name              Cert Owner     USAGE      DEFAULT
---------------------------------   ------------   --------   -------
IKEDS2 at ZOS2                      ID(IKED)       PERSONAL     YES

MVS1 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO

MVS2 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO

MVS3 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO

MVS4 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO

MVS5 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO

MVS6 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO

MVS7 LABS Certificate Authority     CERTAUTH       CERTAUTH     NO
```

IKED Certificate

```
Label: IKED2 at ZOS2
Certificate ID: 2QTJ0sXEydLFxPJAgaNA6dbi8kBA
Status: TRUST
Start Date: 2015/02/26 00:00:00
End Date:   2030/12/30 23:59:59
Serial Number:
     >02<
Issuer's Name:
     >CN=MVS2CA.LABS.IBM.COM.O=MVS2 CA.C=US<
Subject's Name:
     >CN=IKED2.WSC.LABS.IBM.COM.O=IKED2 at ZOS2.C=US<
Subject's AltNames:
  IP: 192.168.20.92
  EMail: ZOS2 at WSC.LABS.IBM.COM
  Domain: WSC.LABS.IBM.COM
Signing Algorithm: sha1RSA
Key Type: RSA
```

```
Key Size: 1024
Private Key: YES
Ring Associations:
  Ring Owner: IKED
  Ring:
     >IKED2RING<
```