z/OSMF Hands-On Lab : Choose your own, Parts I, II, and III

Lab Exercise:

Configuration Assistant for z/OS Communications Server

Session ID’s:

15604: Wednesday 10:00am

15815: Thursday 1:30pm

15814: Friday 11:15am

Estimated Lab Time: 30 minutes

Speaker Names: Kim Bailey and Lin Overby
Enterprise Networking Solutions Design and Strategy

Wednesday: 15604	Thursday:15815	Friday:15814

Abstract:

This hands-on lab will provide an opportunity to learn about using some of the functions and features of the Configuration Assistant in z/OSMF first hand.

This session is intended as a user experience session, and will be useful to systems programmers that focus on z/OS TCP/IP network administration that want to experience using the Configuration Assistant to create configuration for a Policy-based networking technology; or, for administrators that have been using the Configuration Assistant on Windows, are planning to migrate to z/OSMF and want to become familiar with the web interface.

As a reminder: With z/OS V2R1, the Configuration Assistant is no longer provided as a Window's download. Users must use the Configuration Assistant with z/OSMF.

The Configuration Assistant for z/OS Communications Server is a management application that helps users configure the Policy-based networking technologies of z/OS Communications Server:

- IP Security (IPSec)
  - IP Filter Rules
  - VPN Tunnels
- Network Security Services (NSS)
  - Required for IKEv2 for certificate services
  - Also used for remote security services with a DataPower appliance
- Defense Manager Daemon (DMD)
  - Setup to user IPSec defensive filters
- Application Transparent TLS (AT-TLS)
  - Support for the TLS/SSL protocol as an extension of the TCP/IP stack's TCP transport layer
- Intrusion Detection Services (IDS)
  - TCP/IP can detect signature events (ex: scans and attacks) that can cause misuse of system resources
- Policy-based Routing (PBR)
  - Configure TCP/IP to route traffic based upon criteria other than destination IP address
- Qualities of Service (QoS)
  - Provides settings to allow the TCP/IP stack to provide advanced controls for tuning the performance of the traffic it's servicing

The z/OS Management Facility (z/OSMF) provides a web-based, graphical interface with systems management applications that plug-in. These applications are targeted toward system programmers on z/OS. Configuration Assistant for z/OS Communications Server is one of the application plug-ins to z/OSMF.

This session is not intended to provide instruction or education for the following, and it assumes that users have some basic understanding of the TCP/IP networking technologies on z/OS. Other Share sessions may be more appropriate for a technology introduction or deep-dive.

- Understanding the Policy-based networking technologies (IPSecurity, NSS, DMD, AT-TLS, PBR, IDS, QoS)
- Setup up Policy-based networking environment (Policy Agent, IKE, NSS, Syslogd, etc)
- TCP/IP profile setup in support of IPSec or AT-TLS

Using the Configuration Assistant:

This lab helps you to become familiar with using the Configuration Assistant as a plug-in to z/OSMF

Lab Hints and Tips:

- Do not use the browser “back” button selection. Use the breadcrumbs!
- While using the Configuration Assistant, feel free to use the comprehensive helps and tutorials to learn more about the technology being configured.
- As with all the labs in this session, all the teams will be working with the same z/OSMF instance. Each team will be given a unique id to work with.
- Each team will have their own configuration backing store to save the configuration created during the session.

Configuration Assistant Lab

This lab provides one main task and one optional task.

Main Task: Helps you to briefly explore the technology perspectives and reusable resources, and then takes you through the creation of an IPSec filter rule and the generation of policy.

Optional Task: Once you complete the Main task, the optional task provides a quick exploration of the “Tools” menu.

Feel free to explore the technologies other than IPSec after you complete the session.

Exercise instructions:

Here are the steps you will perform in this lab:

__ 1. Logon to z/OSMF

__ a. Launch the Mozilla Firefox browser

__ b. Point Browser to z/OSMF – enter the following URL
https://mvs1.centers.ihost.com/zosmf/

__ c. Enter the User ID (SHARAnn) and password assigned to your workstation.

__ 2. Begin using the Configuration Assistant

__ a. Expand the Configuration Category in the Left Navigation Tree

__ b. Click on Configuration Assistant

__ 3. Open the configuration backing store for your session

__ a. Use the perspective selection to switch between each perspective

__ b. Create z/OS Images in the systems table

__ c. Create the TCP/IP stacks in the systems table

__ 4. Explore the IPSec (IP Security Perspective) Reusable Resources

__ a. Become familiar with the IPSec technology perspective reusable resources

__ b. Traffic Descriptors

__ c. Security Levels

__ d. Requirement Maps

__ e. Address Groups

__ 5. Define IPSec reusable resources for use in your Connectivity Rule (Filter Rule)

__ a. Create a Traffic Descriptor

__ b. Create a Requirement Map

__ c. Create an Address Group

__ d. Create a Connectivity Rule

__ 6. Generate and Install the policy configuration (for the Policy Agent)

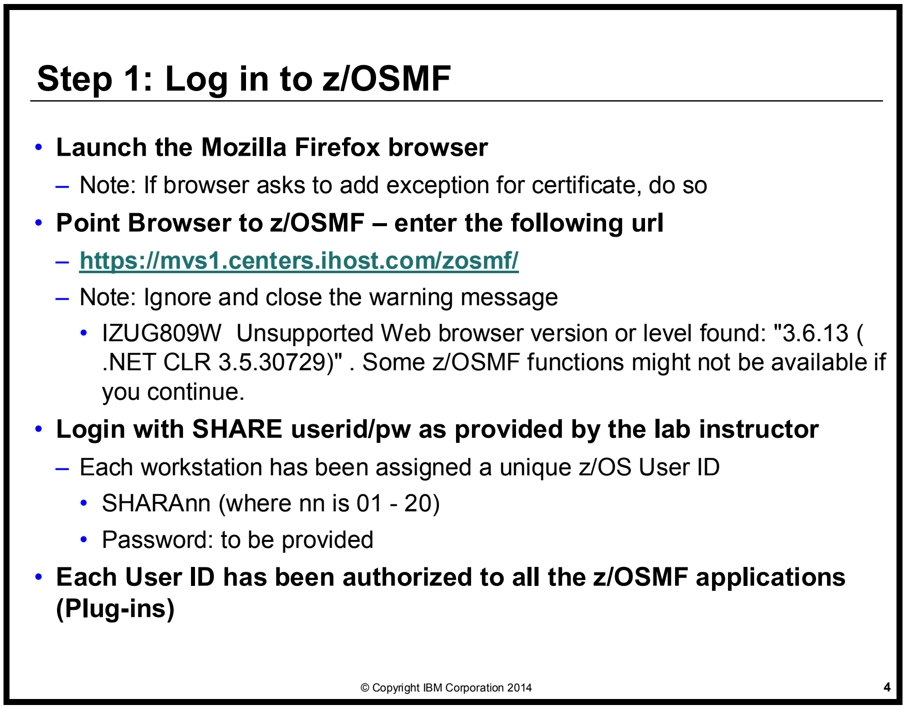
__ a. Select “**Install Configuration Files**”

__ b. View the generated policy

__ c. Perform the Install

Refer to Section 7 for the Optional Task of exploring the Tools button actions.

1. Logon to zOSMF

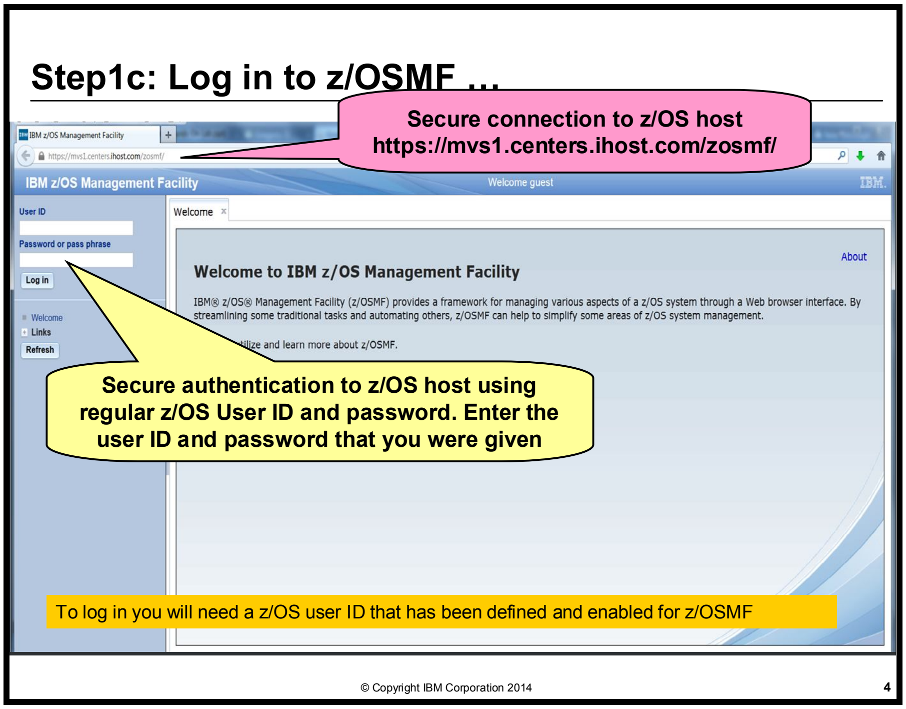


Step 1: Log in to z/OSMF

- **Launch the Mozilla Firefox browser**
  - Note: If browser asks to add exception for certificate, do so
- **Point Browser to z/OSMF – enter the following url**
  - https://mvs1.centers.ihost.com/zosmf/
  - Note: Ignore and close the warning message
    - IZUG809W Unsupported Web browser version or level found: "3.6.13 (.NET CLR 3.5.30729)" . Some z/OSMF functions might not be available if you continue.
- **Login with SHARE userid/pw as provided by the lab instructor**
  - Each workstation has been assigned a unique z/OS User ID
    - SHARAnn (where nn is 01 - 20)
    - Password: to be provided
- **Each User ID has been authorized to all the z/OSMF applications (Plug-ins)**

© Copyright IBM Corporation 2014 4

Note: All screen captures in the handout show the ID SHARA20, your browser will be slightly different to reflect the User ID that you were given.



Step1c: Log in to z/OSMF …

Secure connection to z/OS host https://mvs1.centers.ihost.com/zosmf/

IBM z/OS Management Facility
https://mvs1.centers.ihost.com/zosmf/
IBM z/OS Management Facility
Welcome guest
IBM.
User ID
Password or pass phrase
Log in
Welcome
Links
Refresh
Welcome
About

Welcome to IBM z/OS Management Facility

IBM® z/OS® Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

…tilize and learn more about z/OSMF.

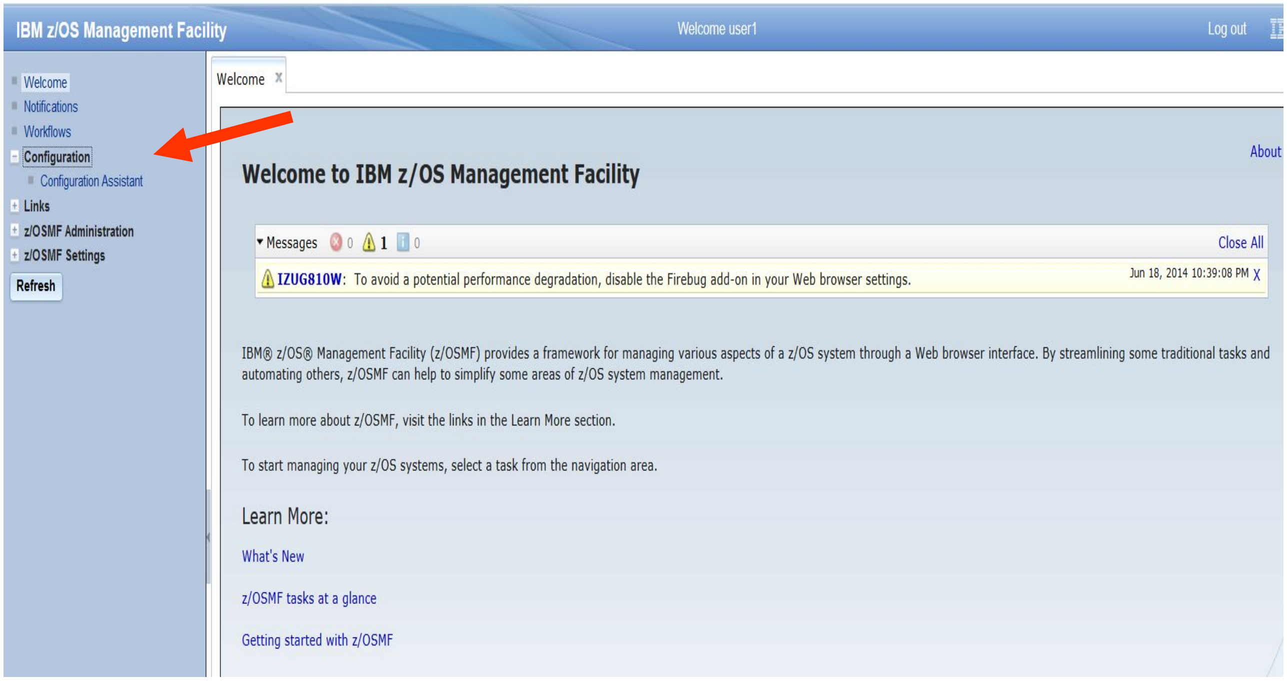
Secure authentication to z/OS host using regular z/OS User ID and password. Enter the user ID and password that you were given

To log in you will need a z/OS user ID that has been defined and enabled for z/OSMF

© Copyright IBM Corporation 2014 4

2. Begin Using the Configuration Assistant

Step 2a: Expand the Configuration Category in the Left Navigation Tree and Click on Configuration Assistant



Welcome to IBM z/OS Management Facility

IZUG810W: To avoid a potential performance degradation, disable the Firebug add-on in your Web browser settings. Jun 18, 2014 10:39:08 PM

IBM® z/OS® Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

To learn more about z/OSMF, visit the links in the Learn More section.

To start managing your z/OS systems, select a task from the navigation area.

Learn More:

What's New

z/OSMF tasks at a glance

Getting started with z/OSMF

Step 2b: Selecting and Opening the Configuration Backing Store

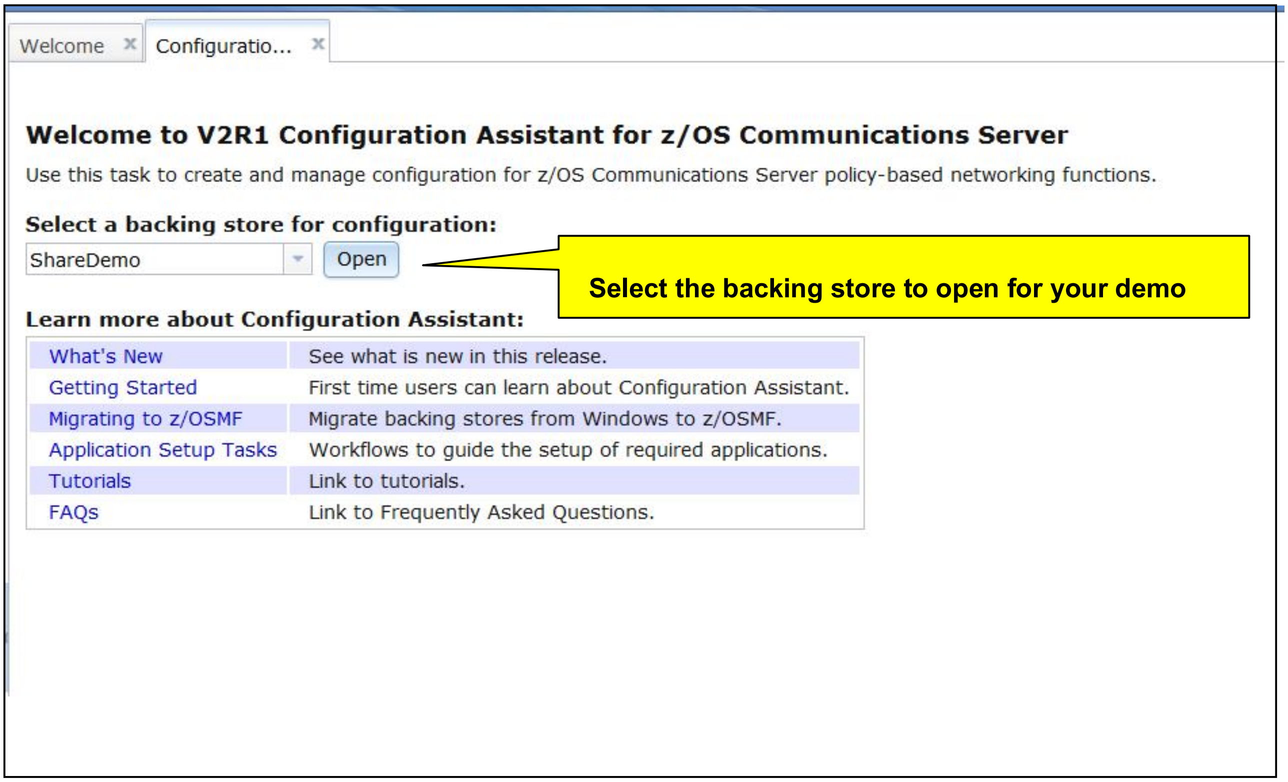
The next panel is the first panel that opens is the main panel of the Configuration Assistant. Here you will see drop-down selection box and an **Open** button.

Also shown is a table with a set of links. Feel free to click on the links and view What's New (in this release), Getting Starting (new users), etc.

Use the selection box to select your configuration backing store for the session which is the name of your user Id and the day of this lab (however in this document the backing store is called ShareDemo), for example, if your user id is SHARA01 and this is the lab session on Wednesday, then your backing store will be SHARA01_WEDNESDAY. Please only open **your** backing store. You will work with your backing store during your session with the Configuration Assistant.

The configuration backing store contains representations of the z/OS system images and TCP/IP stacks along with the configuration resources defined to those stacks that you define during your session.

Click on "**Open**" to begin configuring your TCP/IP stacks with the policy-based networking technologies.



Welcome to V2R1 Configuration Assistant for z/OS Communications Server

Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

Select a backing store for configuration:

ShareDemo

Select the backing store to open for your demo

Learn more about Configuration Assistant:

What's New	See what is new in this release.
Getting Started	First time users can learn about Configuration Assistant.
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Application Setup Tasks	Workflows to guide the setup of required applications.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.

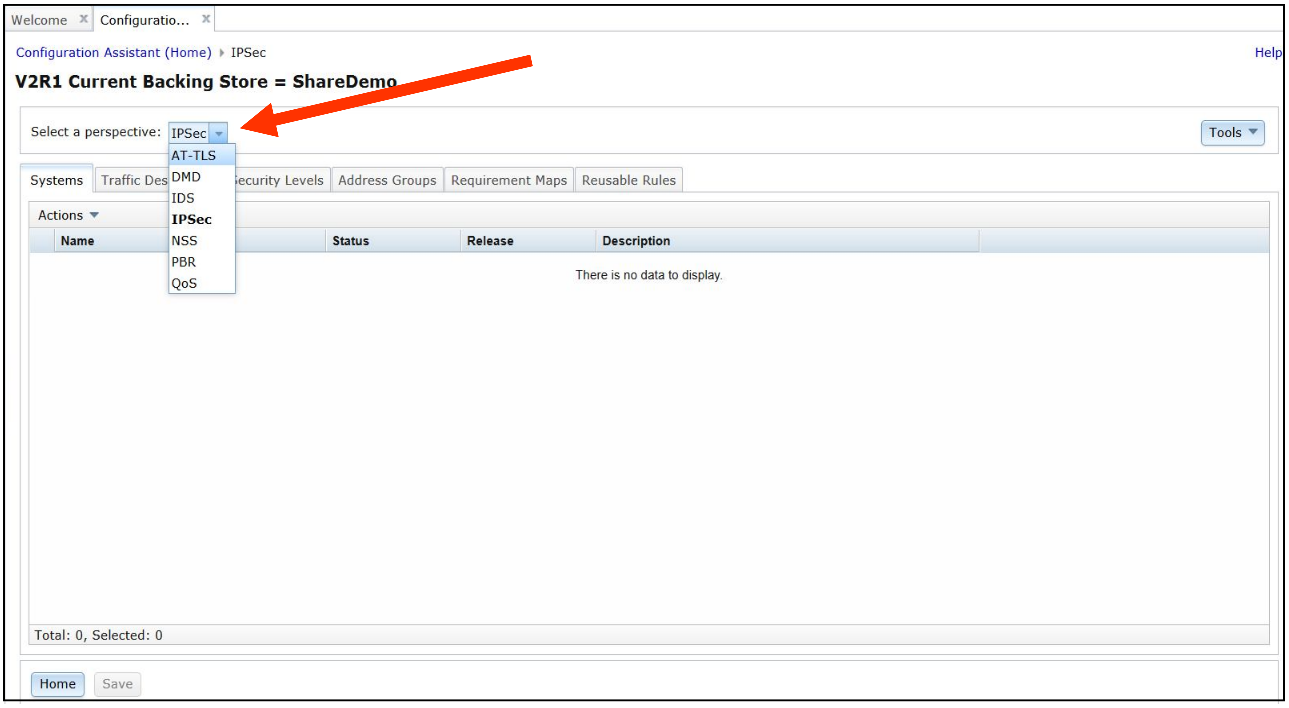
3. Become Familiar with the TCP/IP Technologies you can Configure with the Configuration Assistant

The Configuration Assistant presents each TCP/IP technology in a “Perspective”, which provides the following:

- A separate view for configuring each of the policy-based networking technologies: IPSec (IP Security), AT-TLS (Application Transparent TLS), IDS (Intrusion Detection Services), PBR (Policy-based Routing), DMD (Defense Manager Daemon), NSS (Network Security Services).
- The systems table where the images and stacks to be configured are displayed is a key feature in each technology perspective. The system table spans all technology perspectives.

Step 3a: Switching between perspectives

When the backing store is opened, if it is a new backing store, the default perspective is **IPSec**; otherwise, it is the last perspective being configured when the backing store was saved. Take some time to switch between technology perspectives and come back to **IPSec**.



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

There is no data to display.

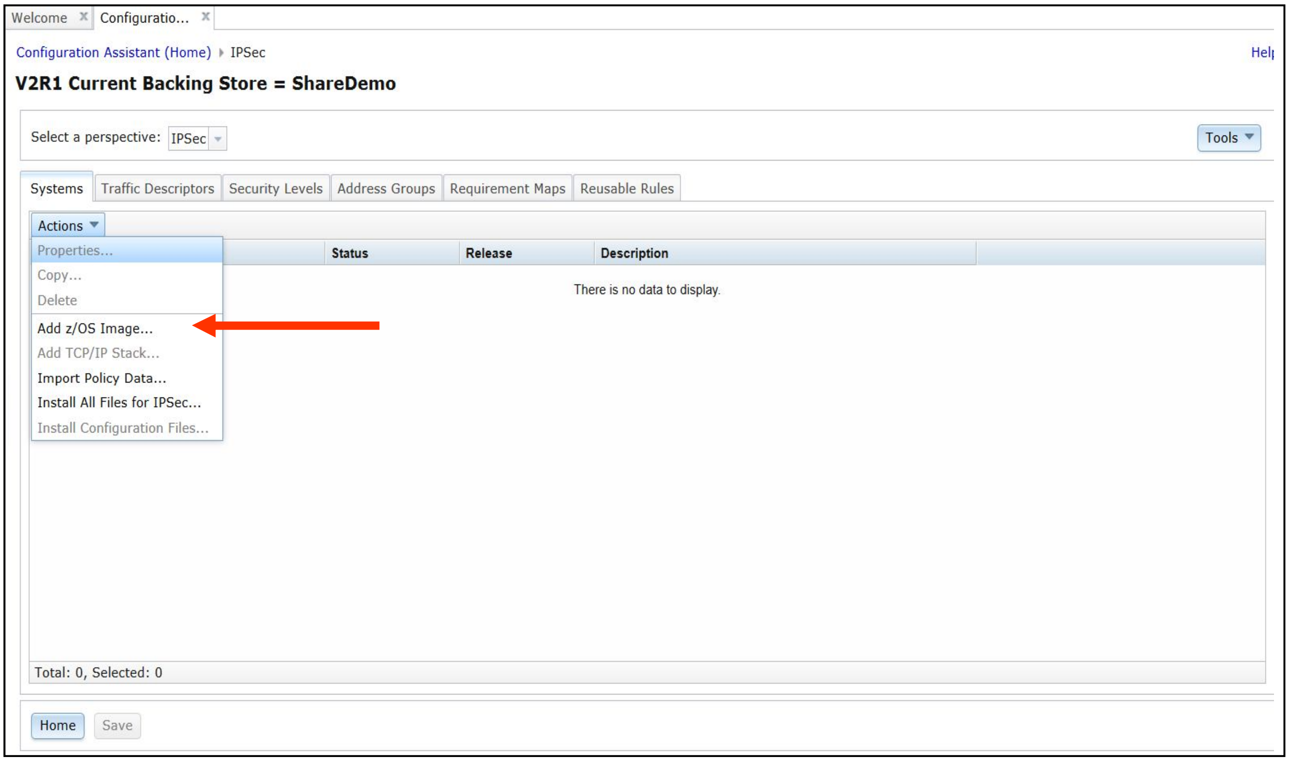
Total: 0, Selected: 0

Step 3b: Create z/OS System Images and TCP/IP Stacks in the systems table

Add the z/OS system images and TCP/IP stacks that you want to configure to the systems table. The same systems table spans all technology perspectives.

Use the table "**Actions**" menu and select "**Add a z/OS Image**".

This lab requires only one z/OS Image and Stack, but feel free to add more to practice.



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

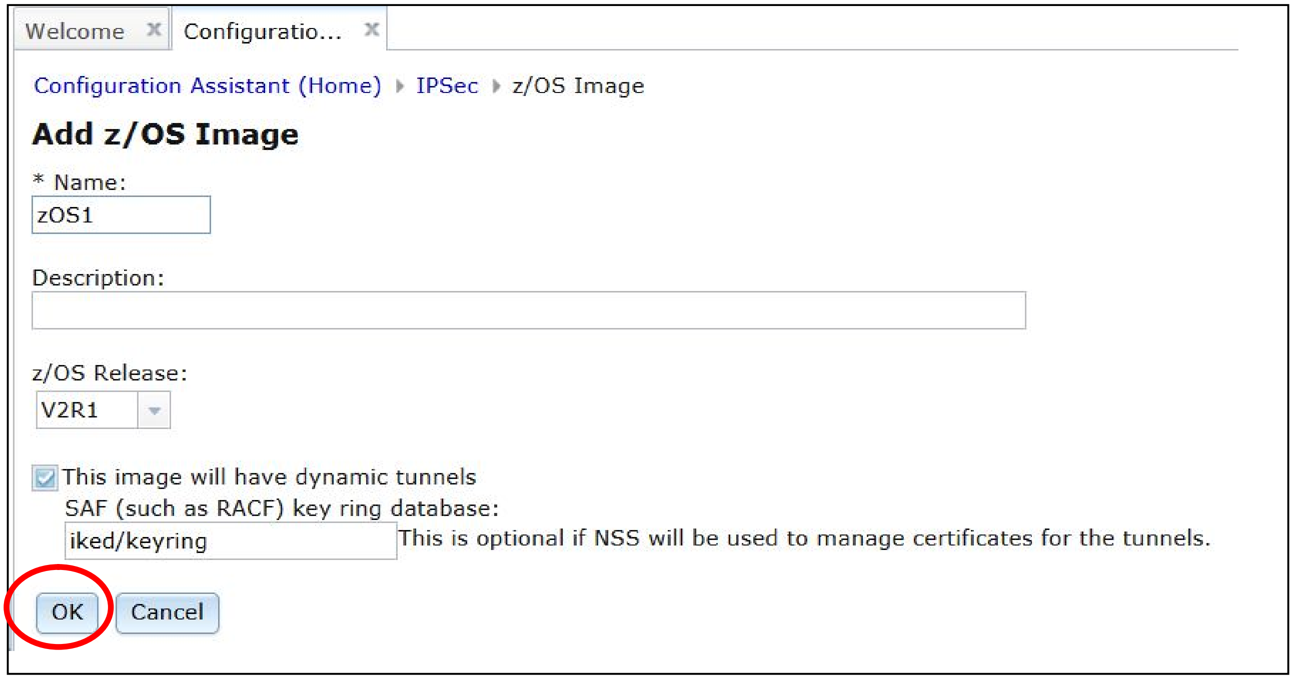
There is no data to display.

Total: 0, Selected: 0

Fill in the panel to define the z/OS system image. Use the panel Help link to learn more about the properties of the image. You can choose your own names; however, it may be more difficult to track since the examples will not match.

Select the “**Ok**” button to complete the image.

A popup dialog will appear to ask if a stack should be created, select the “**Proceed**” button.



Add z/OS Image

* Name: zOS1

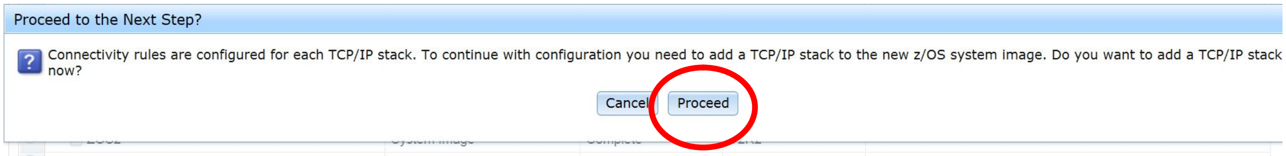
Description:

z/OS Release: V2R1

☑ This image will have dynamic tunnels

SAF (such as RACF) key ring database: iked/keyring This is optional if NSS will be used to manage certificates for the tunnels.

Popup dialog asking to create the stack. Select “**Proceed**”.



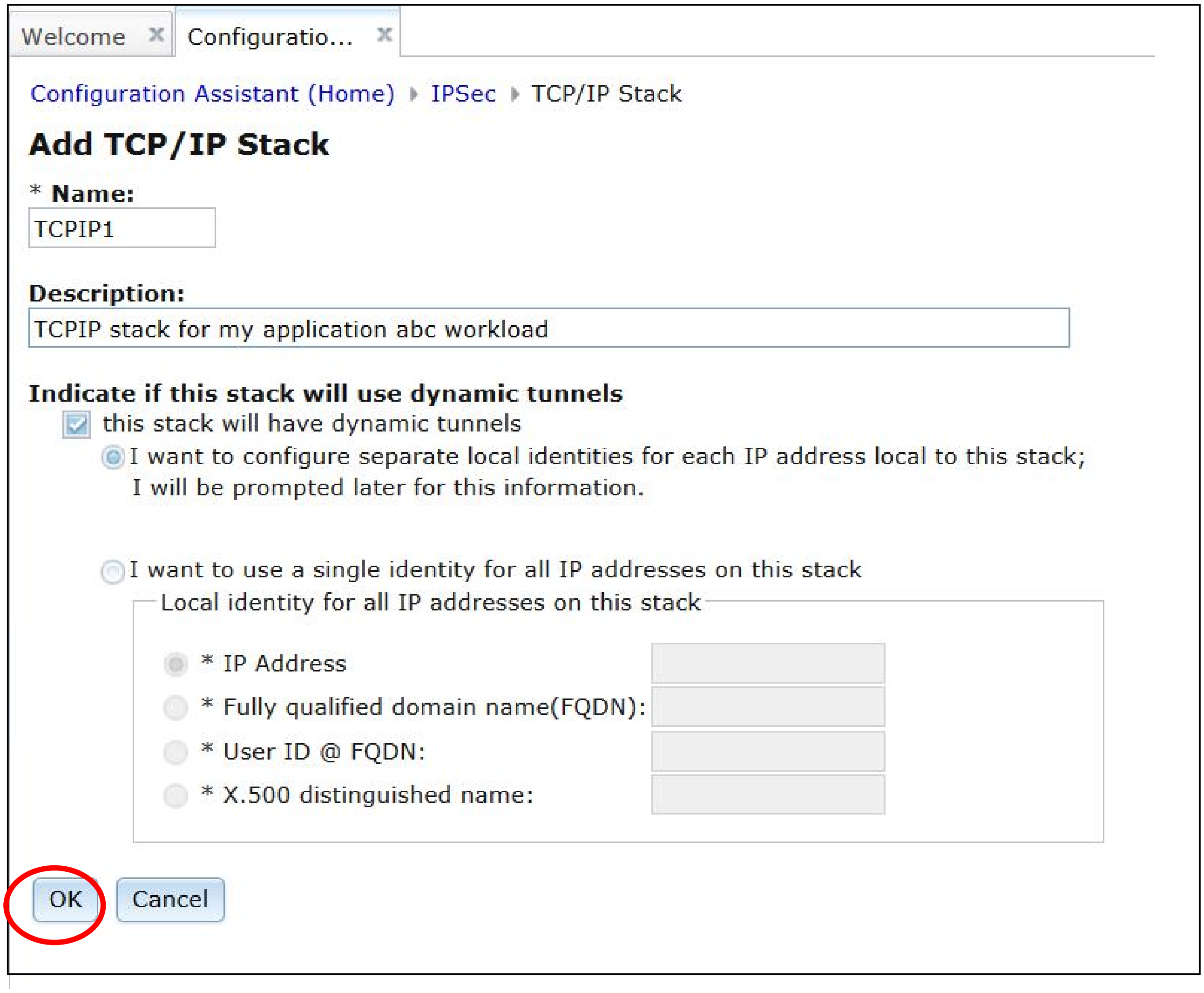
Proceed to the Next Step?

Connectivity rules are configured for each TCP/IP stack. To continue with configuration you need to add a TCP/IP stack to the new z/OS system image. Do you want to add a TCP/IP stack now?

Step3c: Create the TCP/IP stack

Fill in the properties of the TCP/IP stack for image ZOS1 and select the “**Ok**” button.

You will see another dialog asking to begin configuring the stack with IPSec rules, select the “**Cancel**” button.



Add TCP/IP Stack

* **Name:** TCPIP1

Description: TCPIP stack for my application abc workload

Indicate if this stack will use dynamic tunnels

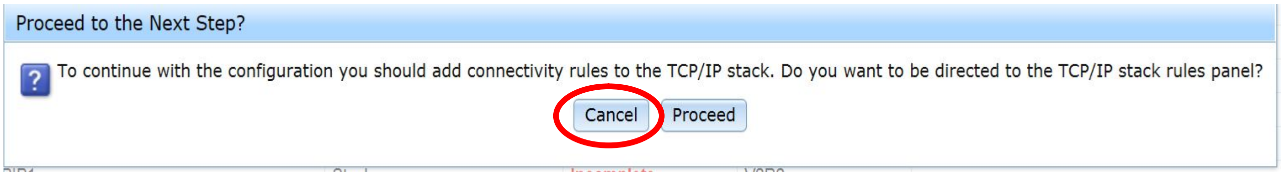
☑ this stack will have dynamic tunnels

● I want to configure separate local identities for each IP address local to this stack; I will be prompted later for this information.

○ I want to use a single identity for all IP addresses on this stack

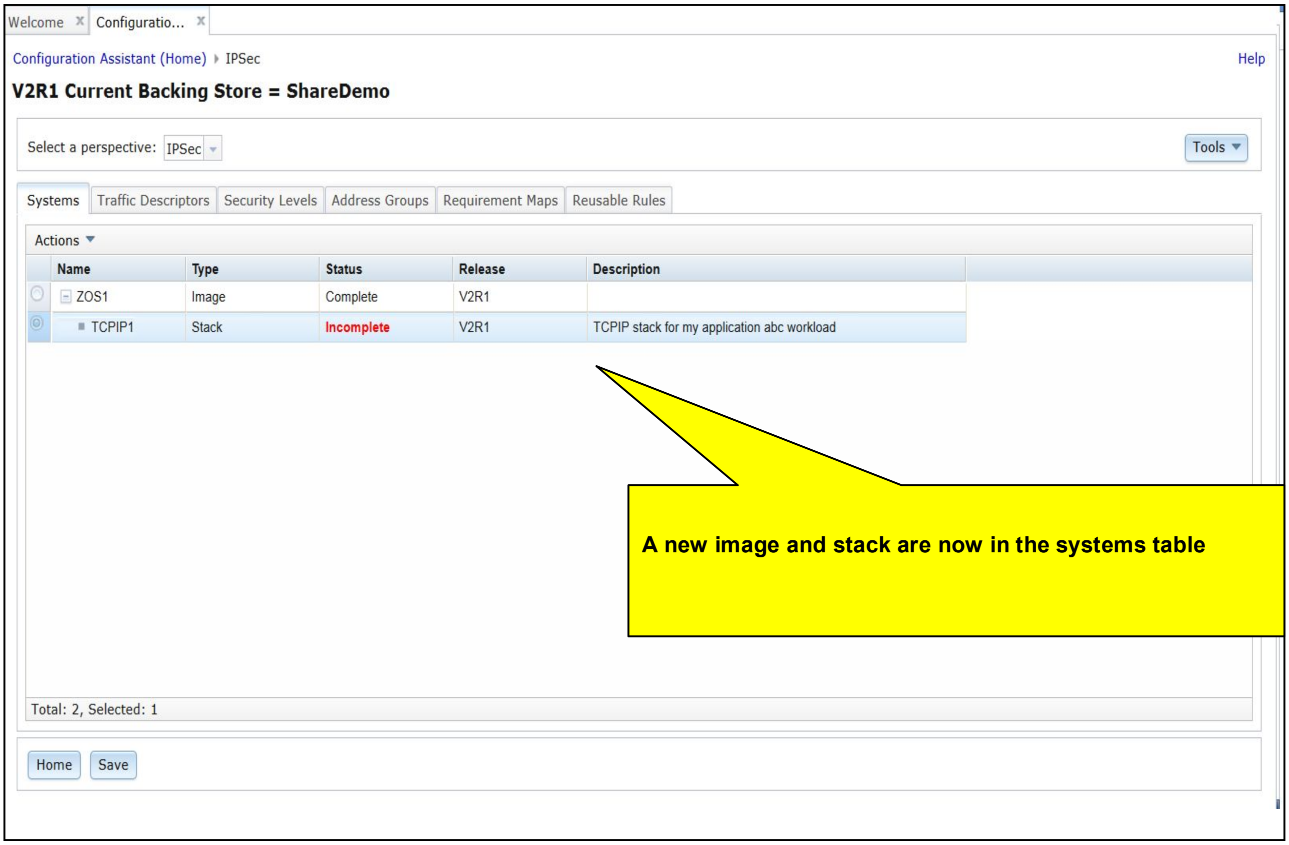
Local identity for all IP addresses on this stack

● * IP Address
○ * Fully qualified domain name(FQDN):
○ * User ID @ FQDN:
○ * X.500 distinguished name:


Proceed to the Next Step?

To continue with the configuration you should add connectivity rules to the TCP/IP stack. Do you want to be directed to the TCP/IP stack rules panel?

You will be sent back to the systems table where a new z/OS system image and TCP/IP stack are displayed.



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

Name	Type	Status	Release	Description
ZOS1	Image	Complete	V2R1	
TCPIP1	Stack	Incomplete	V2R1	TCPIP stack for my application abc workload

Total: 2, Selected: 1

A new image and stack are now in the systems table

4. IPSec Reusable Resources

Step 4a. Learn about reusable resources, specifically those for IPSec

Now that you've created the TCP/IP stacks you want configure, the next step is to create your IPSec connectivity rules. But first, it's important to understand the **reusable resources** the Configuration Assistant provides to help you with creating your rules.

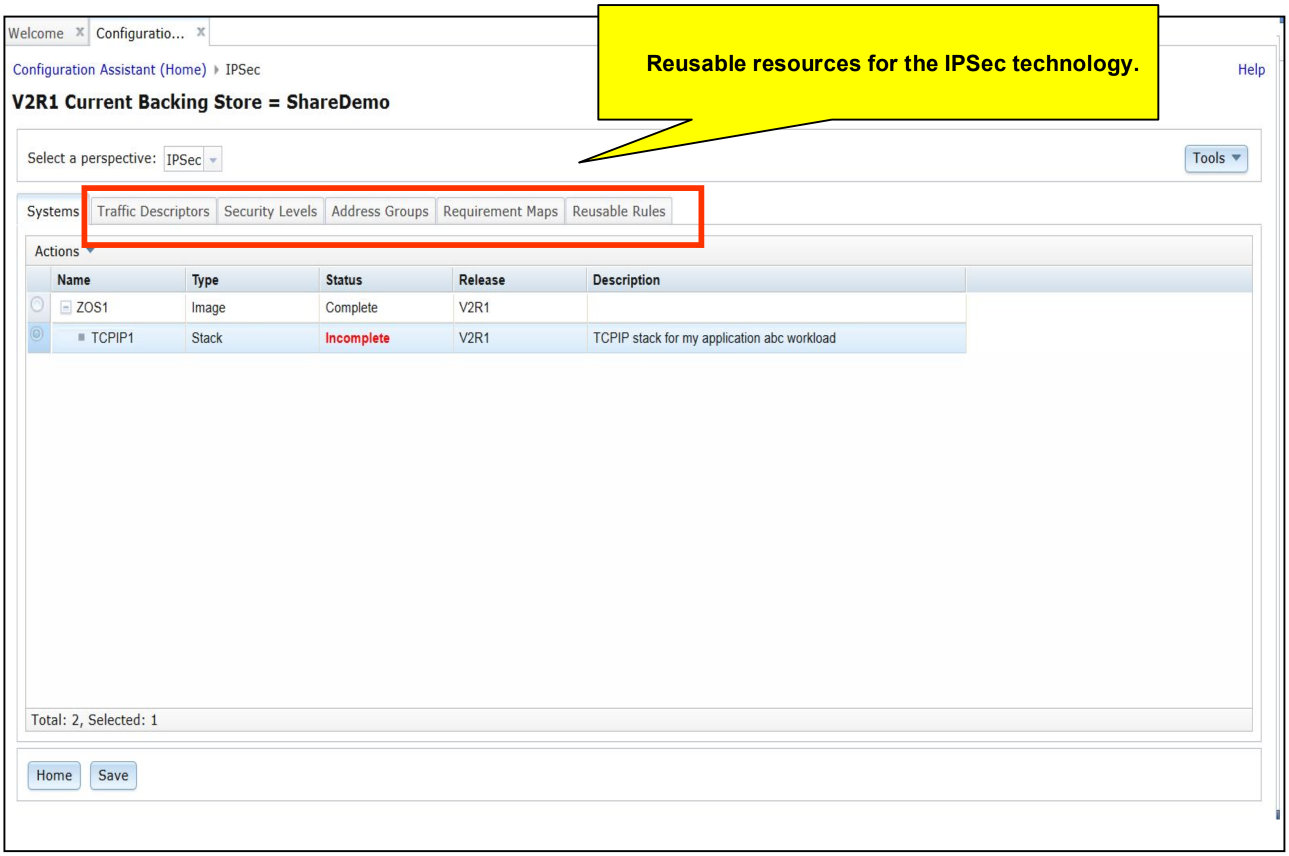
Reusable resources help define the properties of your rules, and the value they provide is that they can be reused in rules for a single stack or across stacks. Each policy-based technology has its own set of reusable resources, and they are not shared across technologies.

For technology perspectives that have **reusable resources**, the Configuration Assistant presents these as tabs within the perspective beside the Systems table. This session will focus only on the **IPSec** reusable resources, but when complete, feel free to explore the other technologies.

The **IPSec** technology perspective has five types of reusable resources:

Reusable Resource Type	Description
Traffic Descriptors	Define the traffic you want to protect, using properties such as the TCP/IP port and jobname.
Security Levels	• For VPN tunnels, define the authentication and encryption methods used to protect the traffic. • For basic filer rules, the security level is permit or deny.
Requirement Maps	Compound resource used to map one or more Traffic Descriptors to a Security Level. (What is protected and how)
Address Groups	Defines the IP Addresses or subnets that are the endpoints of the communication for connectivity rules.
Reusable (Connectivity) Rules	Define the rule once and reuse it across multiple stacks.

- Click on the tabs for each reusable resource.
- As reusable resources are created, they are added to a table. Each type of reusable resource has its own table. All reusable resources, except Reusable Rules, have predefined resources (IBM-provided) created.



Reusable resources for the IPSec technology.

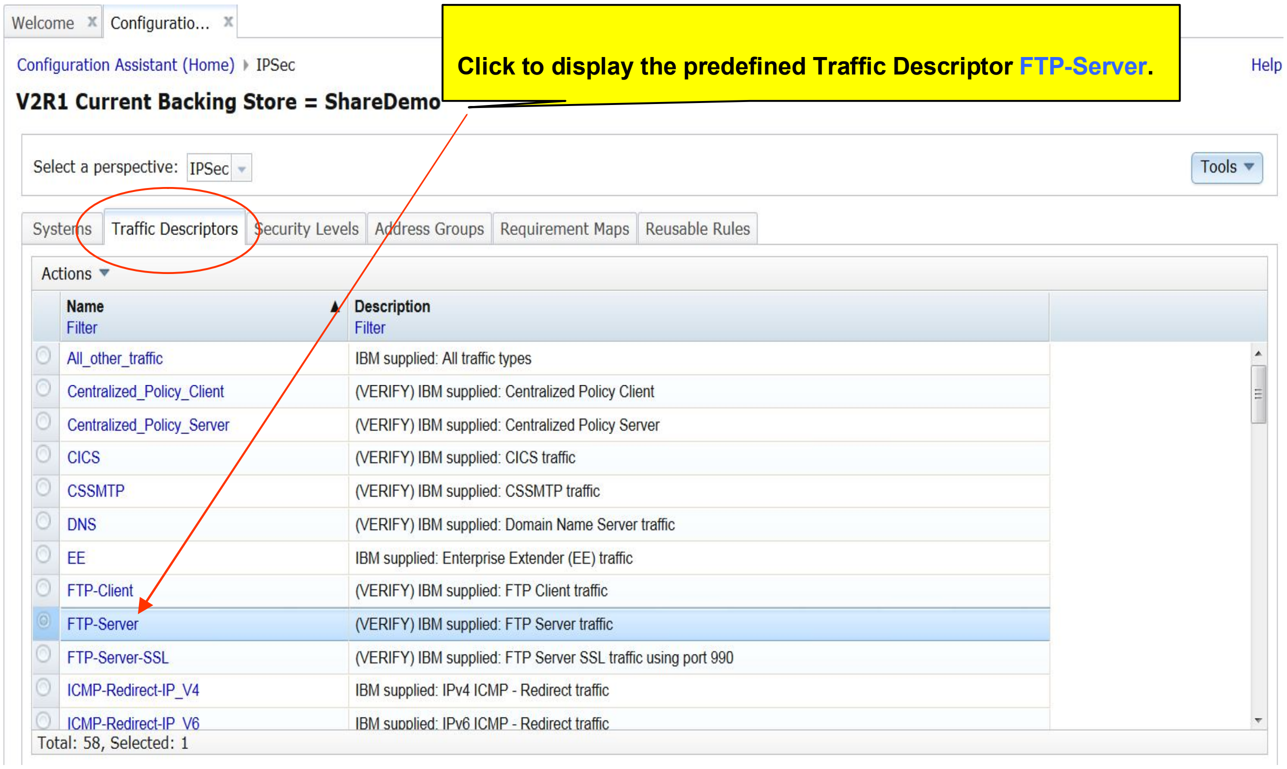
V2R1 Current Backing Store = ShareDemo

Name	Type	Status	Release	Description
ZOS1	Image	Complete	V2R1	
TCPIP1	Stack	Incomplete	V2R1	TCPIP stack for my application abc workload

Total: 2, Selected: 1

Step 4b: View Predefined Traffic Descriptors

- Click on the "**Traffic Descriptors**" tab
- Select the Traffic Descriptor "FTP-Server" and click on the link. The default action is Modify. (Alternatively, select the button for "FTP-Server" and use the table **Actions** menu to **Modify**.)
    - Notice the Description of "**FTP-Server**" and other Traffic Descriptors shows **(VERIFY).** This indicates that IBM has provided this Traffic Descriptor, and and it should be verified to determine if it should be modified.
- Select the table Actions menu and issue the "**View Details**"



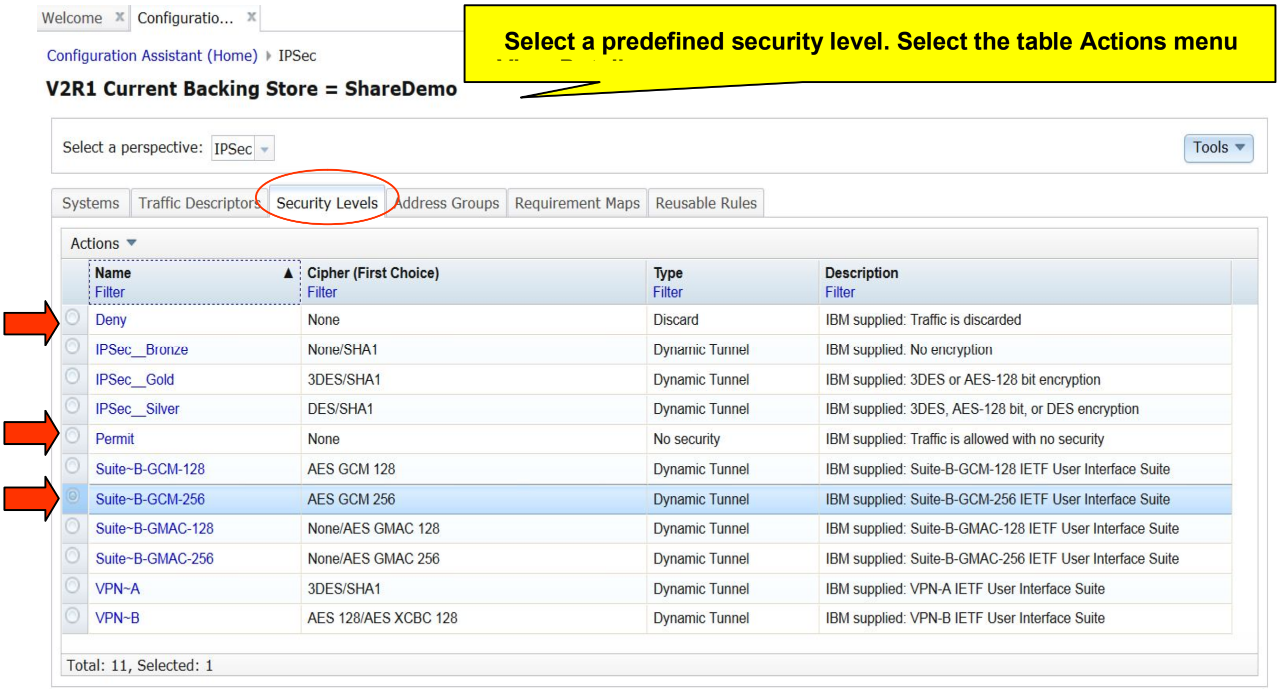
Click to display the predefined Traffic Descriptor FTP-Server.

	Name Filter	Description Filter
○	All_other_traffic	IBM supplied: All traffic types
○	Centralized_Policy_Client	(VERIFY) IBM supplied: Centralized Policy Client
○	Centralized_Policy_Server	(VERIFY) IBM supplied: Centralized Policy Server
○	CICS	(VERIFY) IBM supplied: CICS traffic
○	CSSMTP	(VERIFY) IBM supplied: CSSMTP traffic
○	DNS	(VERIFY) IBM supplied: Domain Name Server traffic
○	EE	IBM supplied: Enterprise Extender (EE) traffic
○	FTP-Client	(VERIFY) IBM supplied: FTP Client traffic
●	FTP-Server	(VERIFY) IBM supplied: FTP Server traffic
○	FTP-Server-SSL	(VERIFY) IBM supplied: FTP Server SSL traffic using port 990
○	ICMP-Redirect-IP_V4	IBM supplied: IPv4 ICMP - Redirect traffic
○	ICMP-Redirect-IP_V6	IBM supplied: IPv6 ICMP - Redirect traffic

Total: 58, Selected: 1

Step 4c: View Predefined Security Levels

- Click on the "**Security Levels**" tab
- Select one the Security Levels pointed to below with the "red arrows". Select the table **Actions** menu "**View Details**" option to view the details of the security level. Do this for each of the security levels pointed to with the red arrows.
  - Notice that the predefined security levels can't be modified, but they can be copied.


Welcome
Configuratio...
Configuration Assistant (Home) ▸ IPSec
Select a predefined security level. Select the table Actions menu
Select a perspective: IPSec
Tools
Systems
Traffic Descriptors
Security Levels
Address Groups
Requirement Maps
Reusable Rules
Actions

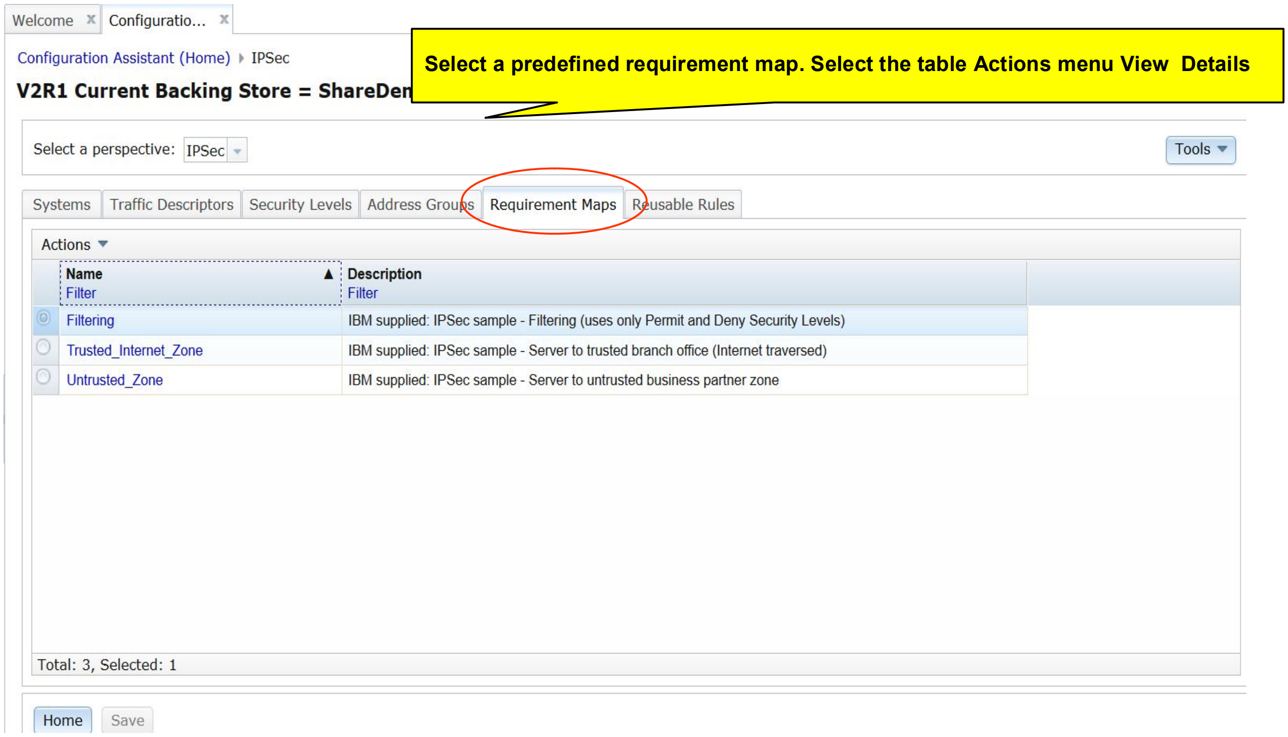
V2R1 Current Backing Store = ShareDemo

	Name	Cipher (First Choice)	Type	Description
○	Deny	None	Discard	IBM supplied: Traffic is discarded
○	IPSec__Bronze	None/SHA1	Dynamic Tunnel	IBM supplied: No encryption
○	IPSec__Gold	3DES/SHA1	Dynamic Tunnel	IBM supplied: 3DES or AES-128 bit encryption
○	IPSec__Silver	DES/SHA1	Dynamic Tunnel	IBM supplied: 3DES, AES-128 bit, or DES encryption
○	Permit	None	No security	IBM supplied: Traffic is allowed with no security
○	Suite~B-GCM-128	AES GCM 128	Dynamic Tunnel	IBM supplied: Suite-B-GCM-128 IETF User Interface Suite
●	Suite~B-GCM-256	AES GCM 256	Dynamic Tunnel	IBM supplied: Suite-B-GCM-256 IETF User Interface Suite
○	Suite~B-GMAC-128	None/AES GMAC 128	Dynamic Tunnel	IBM supplied: Suite-B-GMAC-128 IETF User Interface Suite
○	Suite~B-GMAC-256	None/AES GMAC 256	Dynamic Tunnel	IBM supplied: Suite-B-GMAC-256 IETF User Interface Suite
○	VPN~A	3DES/SHA1	Dynamic Tunnel	IBM supplied: VPN-A IETF User Interface Suite
○	VPN~B	AES 128/AES XCBC 128	Dynamic Tunnel	IBM supplied: VPN-B IETF User Interface Suite

Total: 11, Selected: 1

Step 4d: View Requirement Maps

- Click on the "**Requirement Maps**" tab
- Select the Filtering Requirement Map. Select the table **Actions** menu "View Details" option to view the details of the requirement maps. Then select the Trusted_Internet_Zone requirement map.
  - Notice that the predefined requirement maps can't be modified, but they can be copied!
  - Notice how the Requirement Maps contain predefined traffic descriptors and security levels.



Select a predefined requirement map. Select the table Actions menu View Details

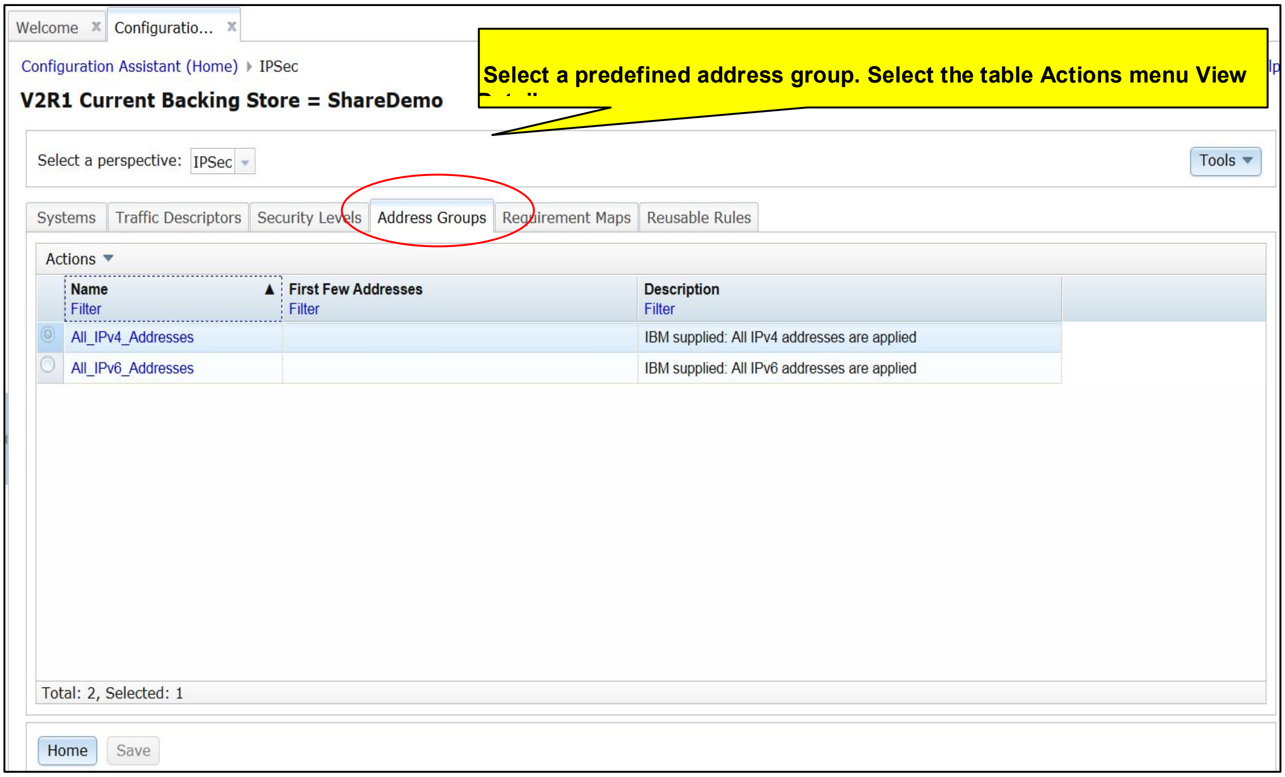
	Name Filter	Description Filter
●	Filtering	IBM supplied: IPSec sample - Filtering (uses only Permit and Deny Security Levels)
○	Trusted_Internet_Zone	IBM supplied: IPSec sample - Server to trusted branch office (Internet traversed)
○	Untrusted_Zone	IBM supplied: IPSec sample - Server to untrusted business partner zone

Total: 3, Selected: 1

.

Step 4e: View Address Groups

- Click on the "**Address Groups**" tab
- Select the predefined address group All_IPv4_Addresses, . Select the table **Actions** menu "**View Details**" option to view the details of the address group.



Welcome
Configuratio...
Configuration Assistant (Home) ▸ IPSec
V2R1 Current Backing Store = ShareDemo
Select a predefined address group. Select the table Actions menu View
Select a perspective: IPSec
Tools
Systems
Traffic Descriptors
Security Levels
Address Groups
Requirement Maps
Reusable Rules
Actions
Home
Save

	Name Filter	First Few Addresses Filter	Description Filter
●	All_IPv4_Addresses		IBM supplied: All IPv4 addresses are applied
○	All_IPv6_Addresses		IBM supplied: All IPv6 addresses are applied

Total: 2, Selected: 1

5. Define Reusable Resources for use in Connectivity Rules

Now that reusable resources have become more familiar, you will create some so they can be used in Connectivity Rules.

- In the IPSec technology, users can configure two basic types of Connectivity Rules, IP Filters and IP Tunnels. To determine the type of rule needed, first think about the systems and applications you want to protect and how you want to protect them. For example, consider (Note: These only provide one aspect in each case; however, there are certainly others to consider).:

IP Filtering:

- Do you want to ensure that only traffic that you “Permit” is able to enter or leave your system and all other traffic should not be serviced (“Denied”)?   If so, you'll want to create some filter rules.

IP Tunnels:

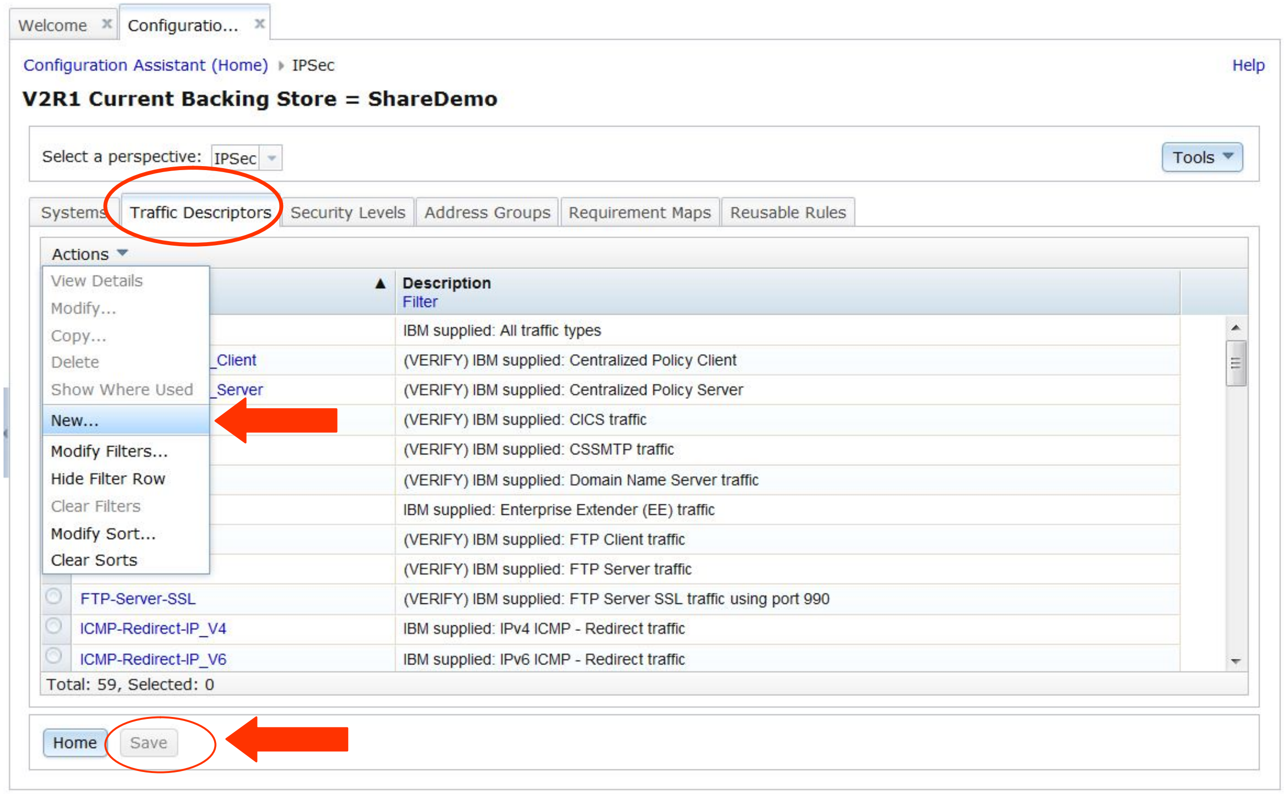
- Do you want to have secure communications to another system(s)? For example, you recently acquired a new business having two systems that require communication with your z/OS systems. You're not sure about all of the types of traffic that will flow, but some of it will be sensitive, so you decide to use IPSec VPN dynamic tunnels to secure the data using encryption.

The tasks under IPSec for this lab session will focus on the IP Filtering and create a filter rule to allow access to a test application “Testtool” in your enterprise, but only from the test systems **(“Permit**” the test systems). The Testtool application uses the **TCP** protocol and **listens on port 100** and the test systems are in subnet 201.100.10.0/29. Two administrator from systems 9.100.2.2 and 9.100.2.3 can also access the application.

Disclaimer: This IP filter rule created in this lab is a simplistic example used only for the purpose of demonstrating how to create a rule in the Configuration Assistant. No real-world application of this specific example is intended.

Step 5a: First, create the Traffic Descriptor

- From the table **Actions** menu, select **New** to create a new traffic descriptor
- One important feature to note is the **Save** button. Notice that it is “grayed”. This is because changes to the configuration have not yet been made. Once a resource, such as a traffic descriptor is created, the **Save** button will become active.
  - If the **Save** button is gray, that means that you haven’t created any resources to save. Once you do, the **Save** button is active. Then after the button is pushed, it becomes gray again.
  - Users are encouraged to save changes periodically throughout the session (keep in mind this is a web-based connection!). Saving your backing store actually writes the changes to disk.

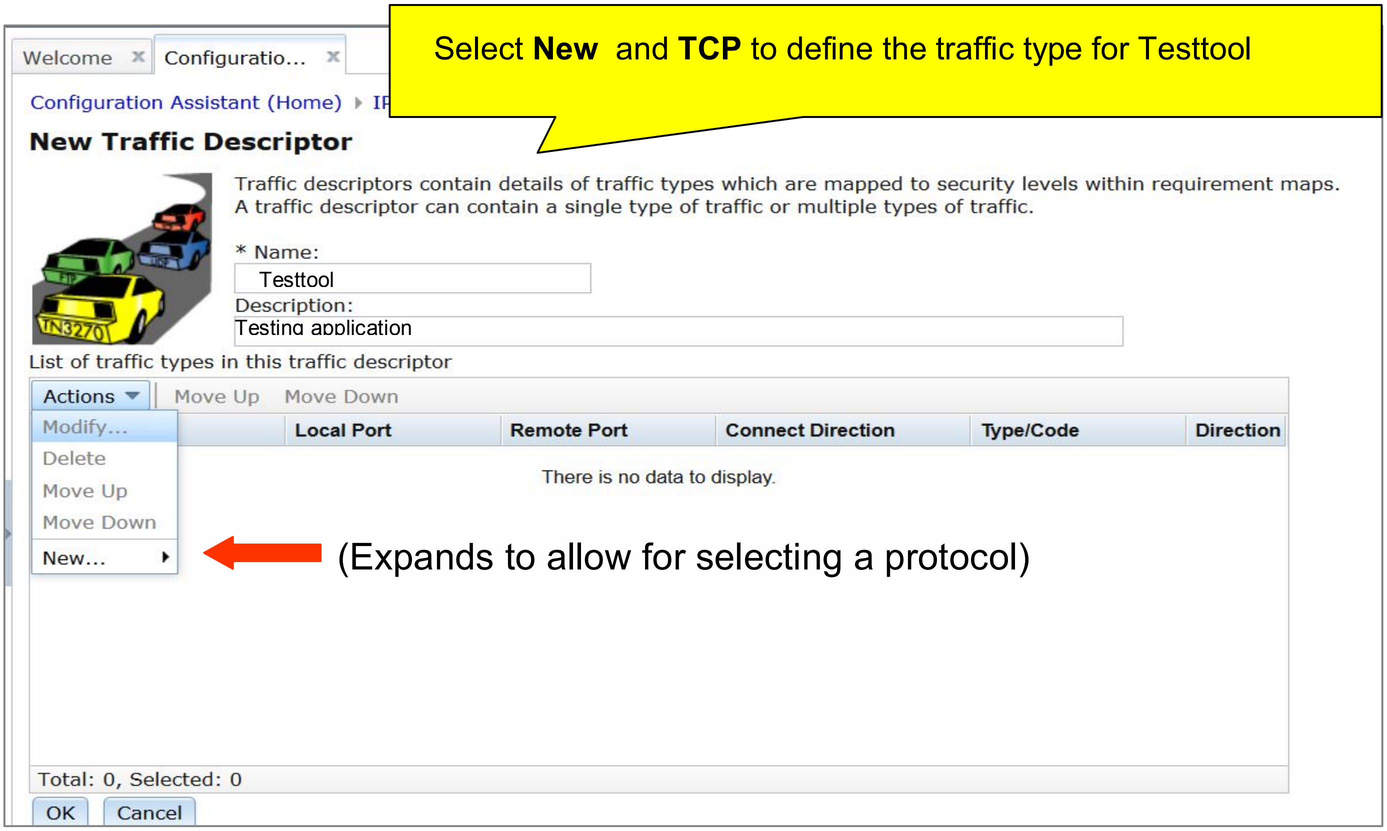


V2R1 Current Backing Store = ShareDemo

	Description Filter
	IBM supplied: All traffic types
_Client	(VERIFY) IBM supplied: Centralized Policy Client
_Server	(VERIFY) IBM supplied: Centralized Policy Server
	(VERIFY) IBM supplied: CICS traffic
	(VERIFY) IBM supplied: CSSMTP traffic
	(VERIFY) IBM supplied: Domain Name Server traffic
	IBM supplied: Enterprise Extender (EE) traffic
	(VERIFY) IBM supplied: FTP Client traffic
	(VERIFY) IBM supplied: FTP Server traffic
○ FTP-Server-SSL	(VERIFY) IBM supplied: FTP Server SSL traffic using port 990
○ ICMP-Redirect-IP_V4	IBM supplied: IPv4 ICMP - Redirect traffic
○ ICMP-Redirect-IP_V6	IBM supplied: IPv6 ICMP - Redirect traffic

Total: 59, Selected: 0

A traffic descriptor can contain more than one type of traffic that you want to pair with a security level. Select **New** to define the traffic type for Testtool.



Select **New** and **TCP** to define the traffic type for Testtool

New Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps. A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name: Testtool

Description: Testing application

List of traffic types in this traffic descriptor

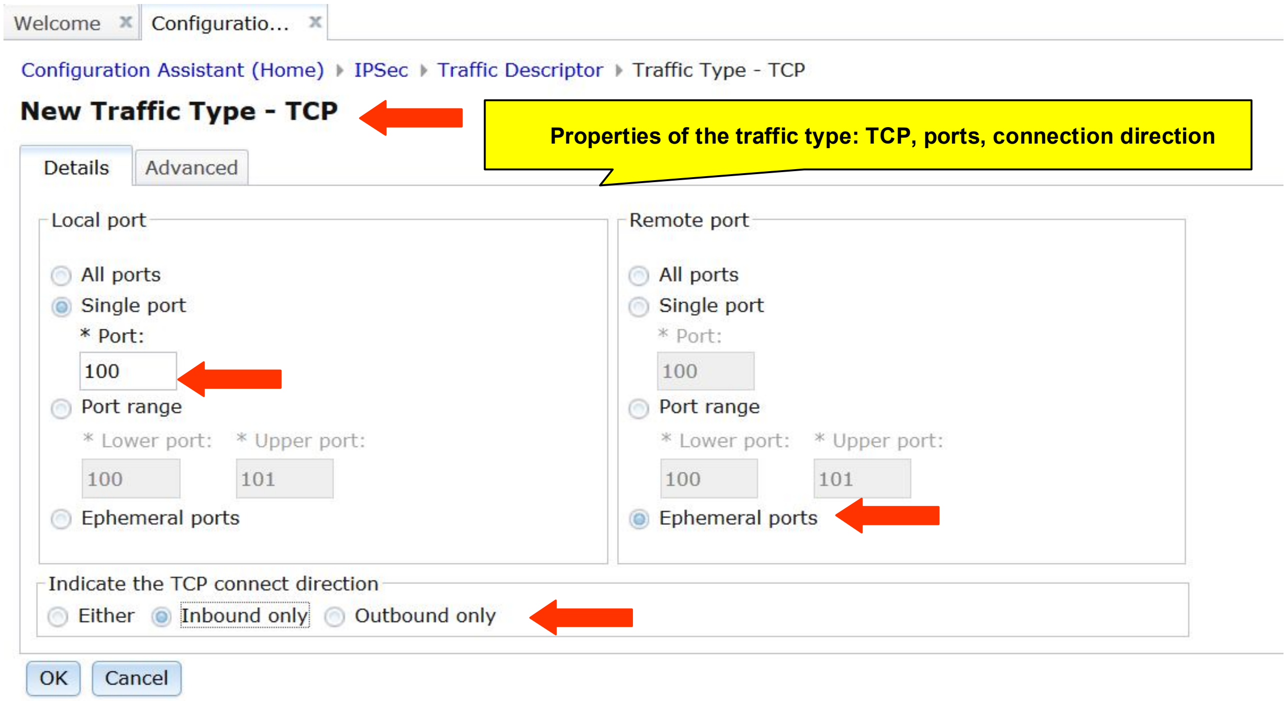
	Local Port	Remote Port	Connect Direction	Type/Code	Direction

There is no data to display.

(Expands to allow for selecting a protocol)

Total: 0, Selected: 0

Testtool is a server application that uses the **TCP protocol** and **listens on port 100**, so it receives connections from clients (connection direction is inbound). Fill in the properties and click “**Ok**”.



Welcome ✕ Configuratio... ✕

Configuration Assistant (Home) ▸ IPSec ▸ Traffic Descriptor ▸ Traffic Type - TCP

New Traffic Type - TCP

Properties of the traffic type: TCP, ports, connection direction

Details | Advanced

Local port

○ All ports
● Single port
* Port: 100
○ Port range
* Lower port: 100 * Upper port: 101
○ Ephemeral ports

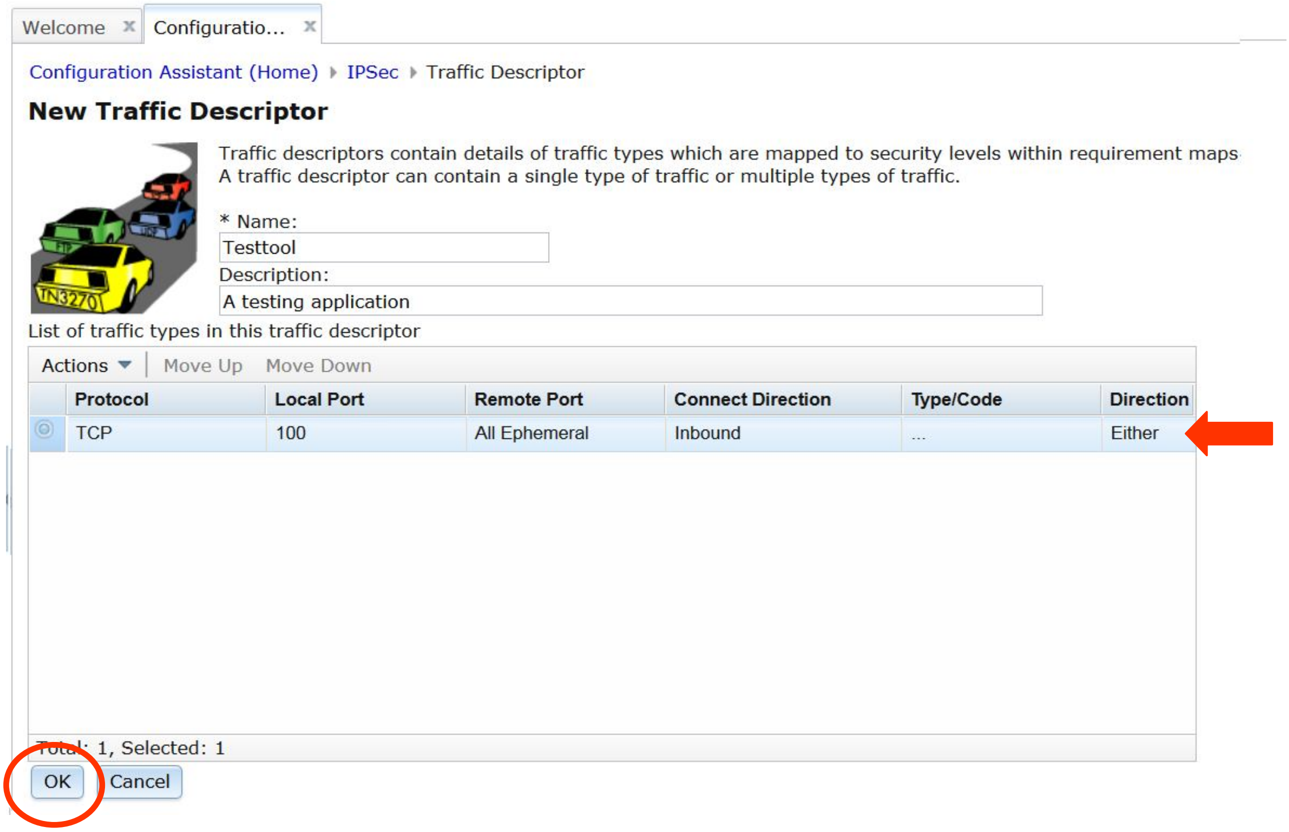
Remote port

○ All ports
○ Single port
* Port: 100
○ Port range
* Lower port: 100 * Upper port: 101
● Ephemeral ports

Indicate the TCP connect direction

○ Either ● Inbound only ○ Outbound only

The traffic type for Testtool has been created, so click “**Ok**” to complete the traffic descriptor. In this example the traffic descriptor only contains one traffic type, but a traffic descriptor can contain more than one traffic type.



New Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps. A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name: Testtool

Description: A testing application

List of traffic types in this traffic descriptor

	Protocol	Local Port	Remote Port	Connect Direction	Type/Code	Direction
●	TCP	100	All Ephemeral	Inbound	...	Either

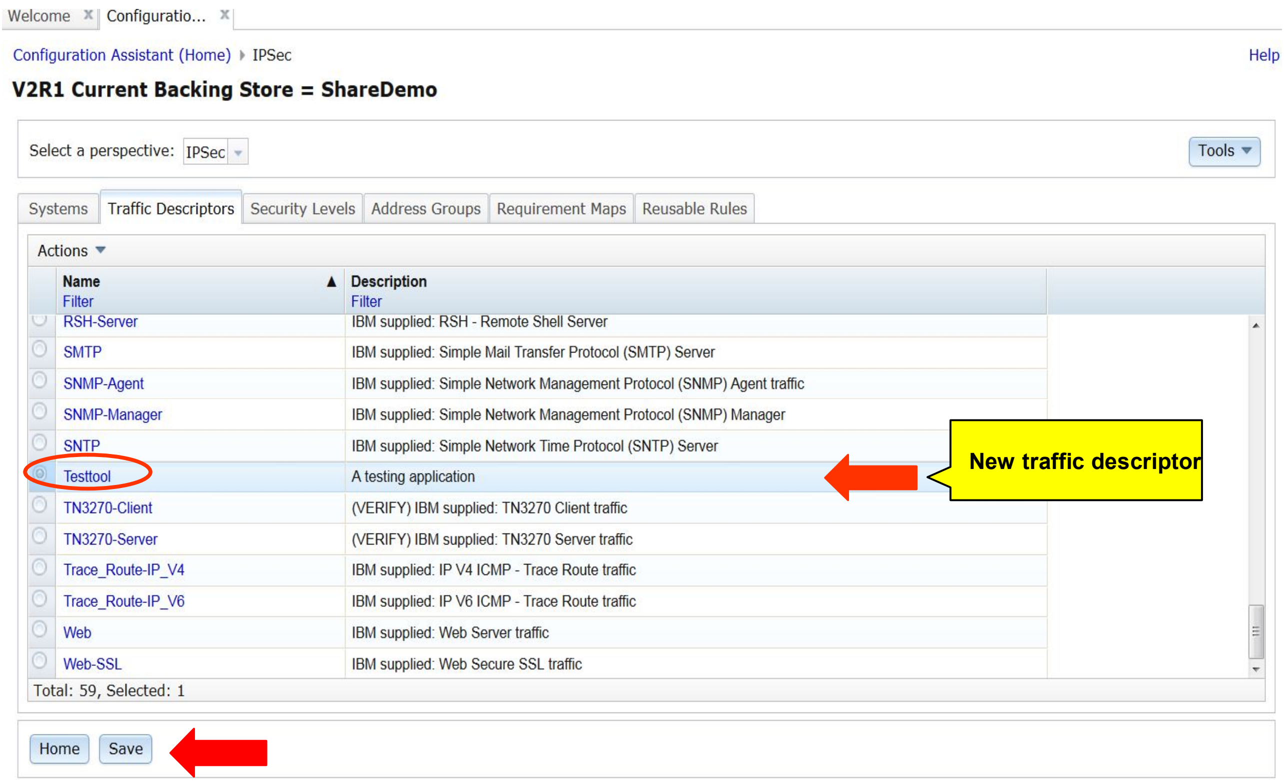
Total: 1, Selected: 1

Congratulations a new traffic descriptor has been created!

You will be positioned at the newly created resource.

Now that a resource has been created, notice the **Save** button is active.

Click “**Save**”



V2R1 Current Backing Store = ShareDemo

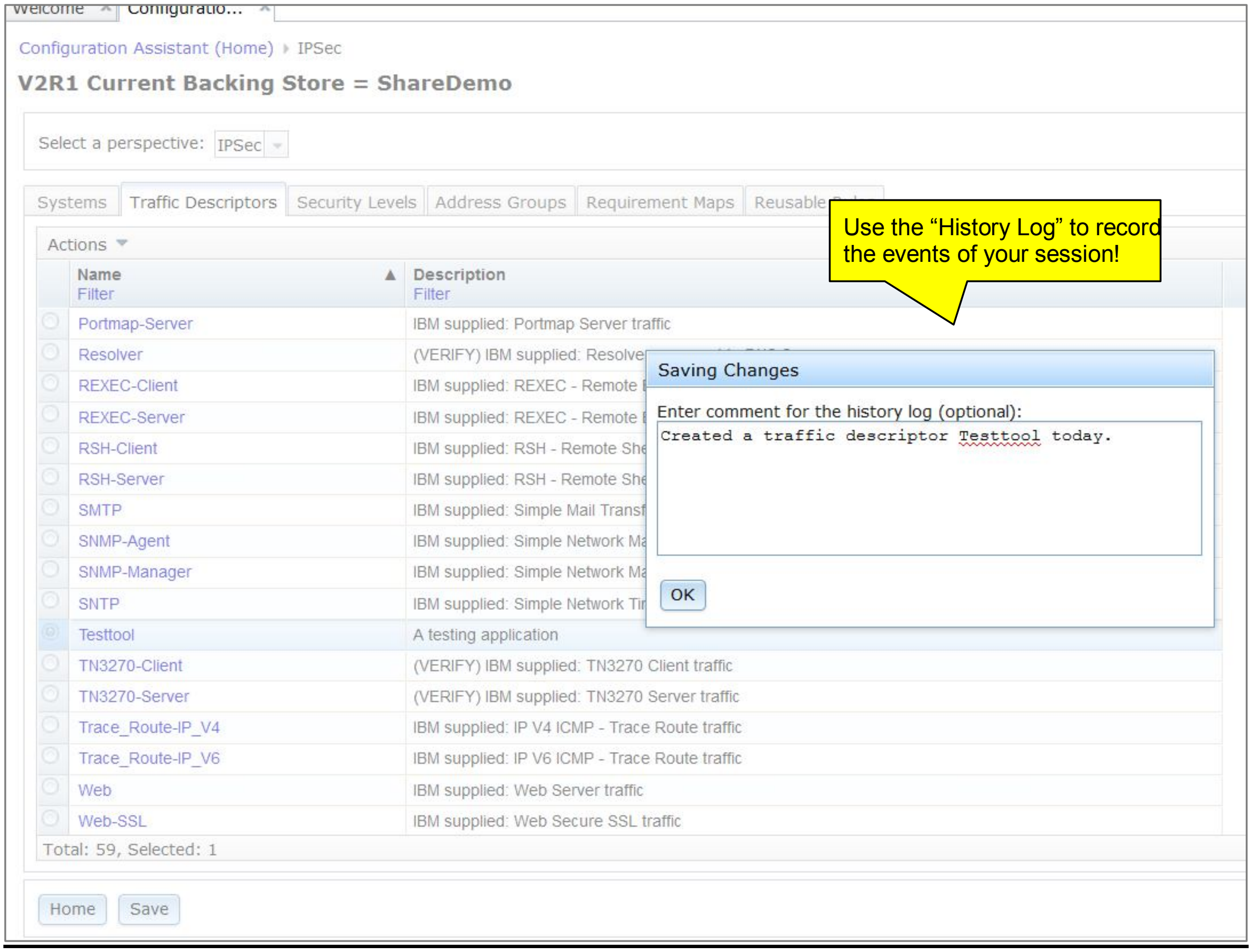
Select a perspective: IPSec

	Name ▲ Filter	Description Filter
○	RSH-Server	IBM supplied: RSH - Remote Shell Server
○	SMTP	IBM supplied: Simple Mail Transfer Protocol (SMTP) Server
○	SNMP-Agent	IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic
○	SNMP-Manager	IBM supplied: Simple Network Management Protocol (SNMP) Manager
○	SNTP	IBM supplied: Simple Network Time Protocol (SNTP) Server
●	Testtool	A testing application
○	TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
○	TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
○	Trace_Route-IP_V4	IBM supplied: IP V4 ICMP - Trace Route traffic
○	Trace_Route-IP_V6	IBM supplied: IP V6 ICMP - Trace Route traffic
○	Web	IBM supplied: Web Server traffic
○	Web-SSL	IBM supplied: Web Secure SSL traffic

Total: 59, Selected: 1

New traffic descriptor

Notice that after clicking “**Save**”, you will be prompted to record in the “History Log”. This is optional, although the Config Assistant will record all saves automatically.



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

Use the “History Log” to record the events of your session!

Name	Description
Portmap-Server	IBM supplied: Portmap Server traffic
Resolver	(VERIFY) IBM supplied: Resolve
REXEC-Client	IBM supplied: REXEC - Remote
REXEC-Server	IBM supplied: REXEC - Remote
RSH-Client	IBM supplied: RSH - Remote She
RSH-Server	IBM supplied: RSH - Remote She
SMTP	IBM supplied: Simple Mail Transf
SNMP-Agent	IBM supplied: Simple Network Ma
SNMP-Manager	IBM supplied: Simple Network Ma
SNTP	IBM supplied: Simple Network Ti
Testtool	A testing application
TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
Trace_Route-IP_V4	IBM supplied: IP V4 ICMP - Trace Route traffic
Trace_Route-IP_V6	IBM supplied: IP V6 ICMP - Trace Route traffic
Web	IBM supplied: Web Server traffic
Web-SSL	IBM supplied: Web Secure SSL traffic

Total: 59, Selected: 1

Saving Changes

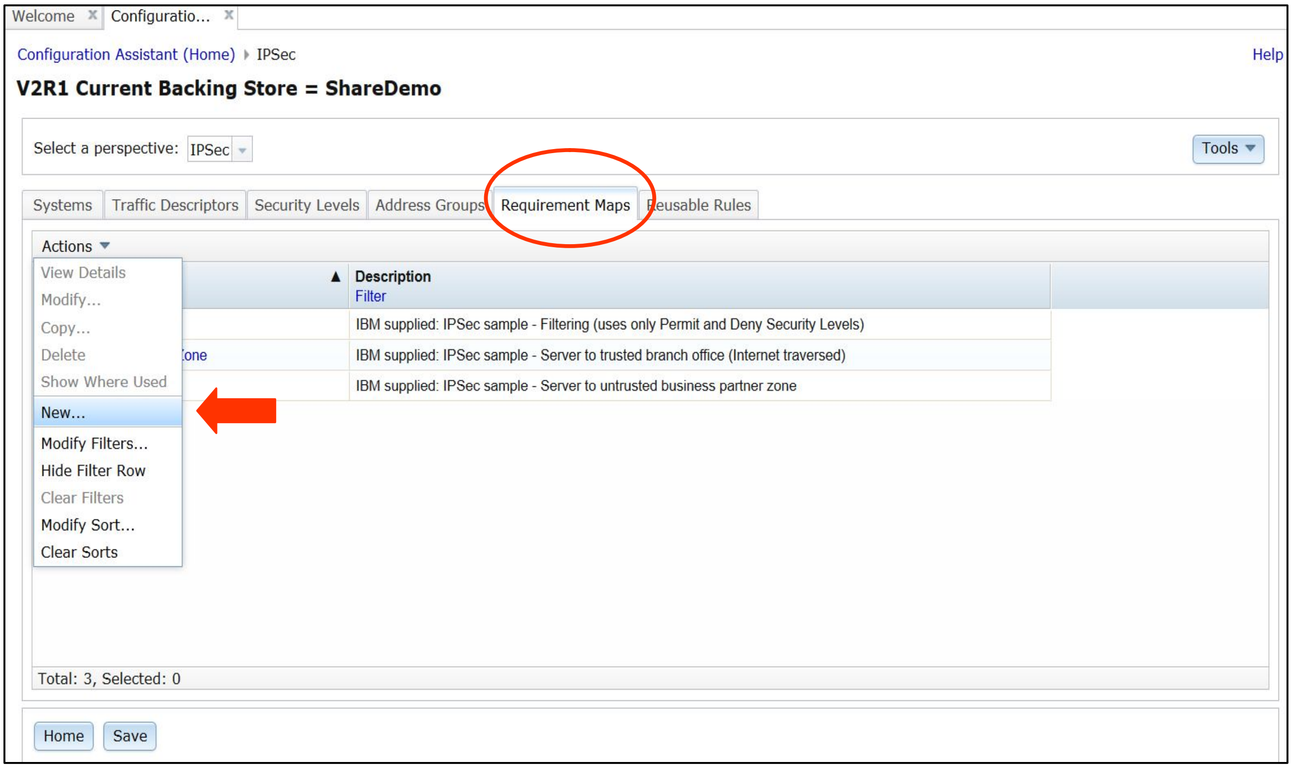
Enter comment for the history log (optional):

```
Created a traffic descriptor Testtool today.
```

Step 5b: Create the Requirement Map

Since we’re creating a filter rule to “**Permit**” and “**Deny**” access to the Testtool application, we’ll use those predefined **Security levels**. This means that next we’ll create our requirement map.

- ○ Remember that a requirement map maps the traffic descriptor to a security level.
- ○ Select the Requirement Maps tab and use the table **Actions** menu to select **New**.



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

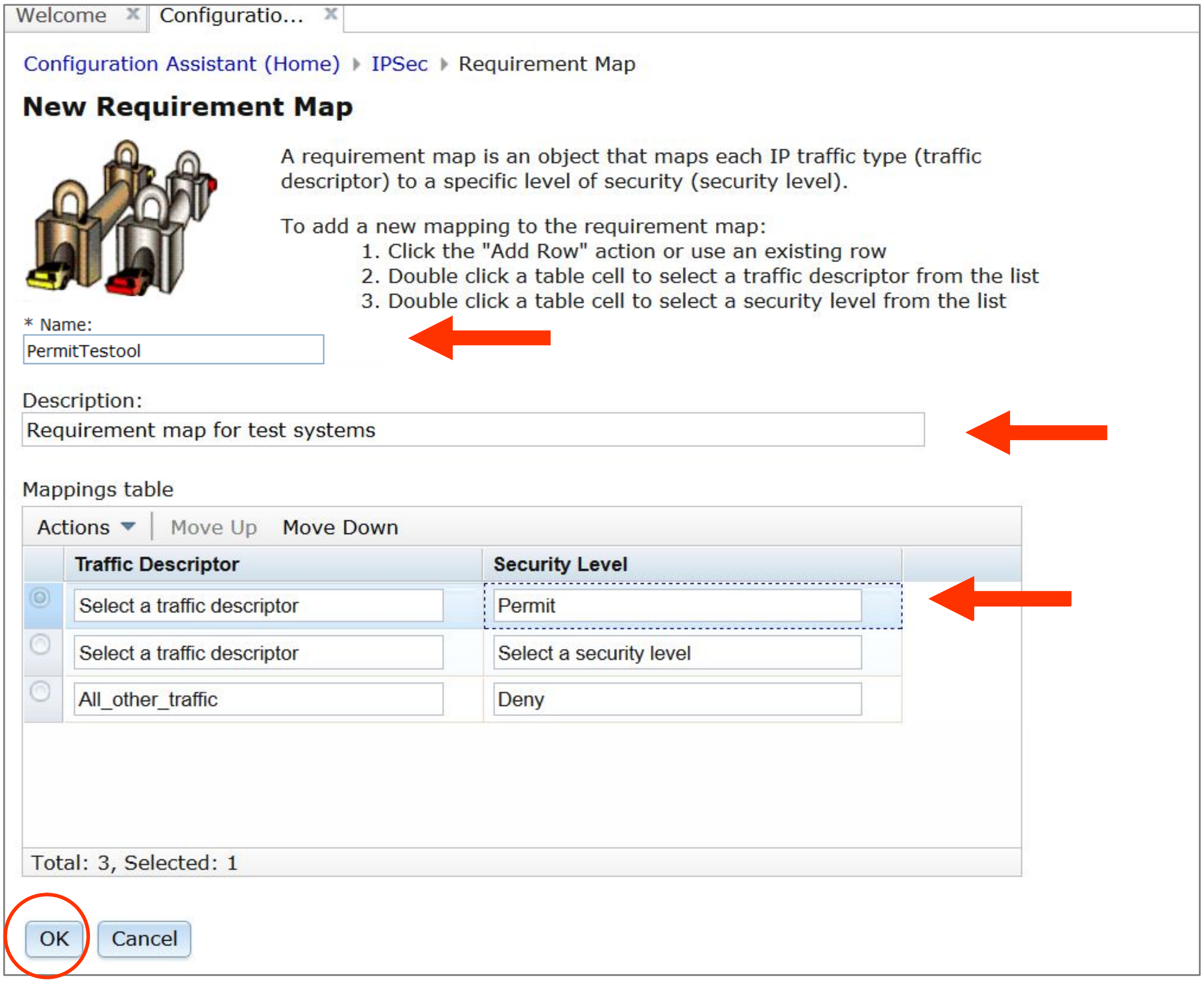
▲	Description Filter
	IBM supplied: IPSec sample - Filtering (uses only Permit and Deny Security Levels)
one	IBM supplied: IPSec sample - Server to trusted branch office (Internet traversed)
	IBM supplied: IPSec sample - Server to untrusted business partner zone

Total: 3, Selected: 0

Fill-in the properties of the Requirement Map. Select on the **Traffic Descriptor** in editable table an click. A list of the traffic descriptors will be show (see next panel figure). Select **Testtool.** Click on the **Security Level** and select **Permit**.

Notice the "**Deny**" for **All_Other_Traffic.** This will deny all other traffic for the connectivity rule.

Hint: You'll need to "double click" in the rows of the editable table.



Configuration Assistant (Home) ▸ IPSec ▸ Requirement Map

New Requirement Map

A requirement map is an object that maps each IP traffic type (traffic descriptor) to a specific level of security (security level).

To add a new mapping to the requirement map:

1. Click the "Add Row" action or use an existing row
2. Double click a table cell to select a traffic descriptor from the list
3. Double click a table cell to select a security level from the list

* Name: PermitTestool

Description: Requirement map for test systems

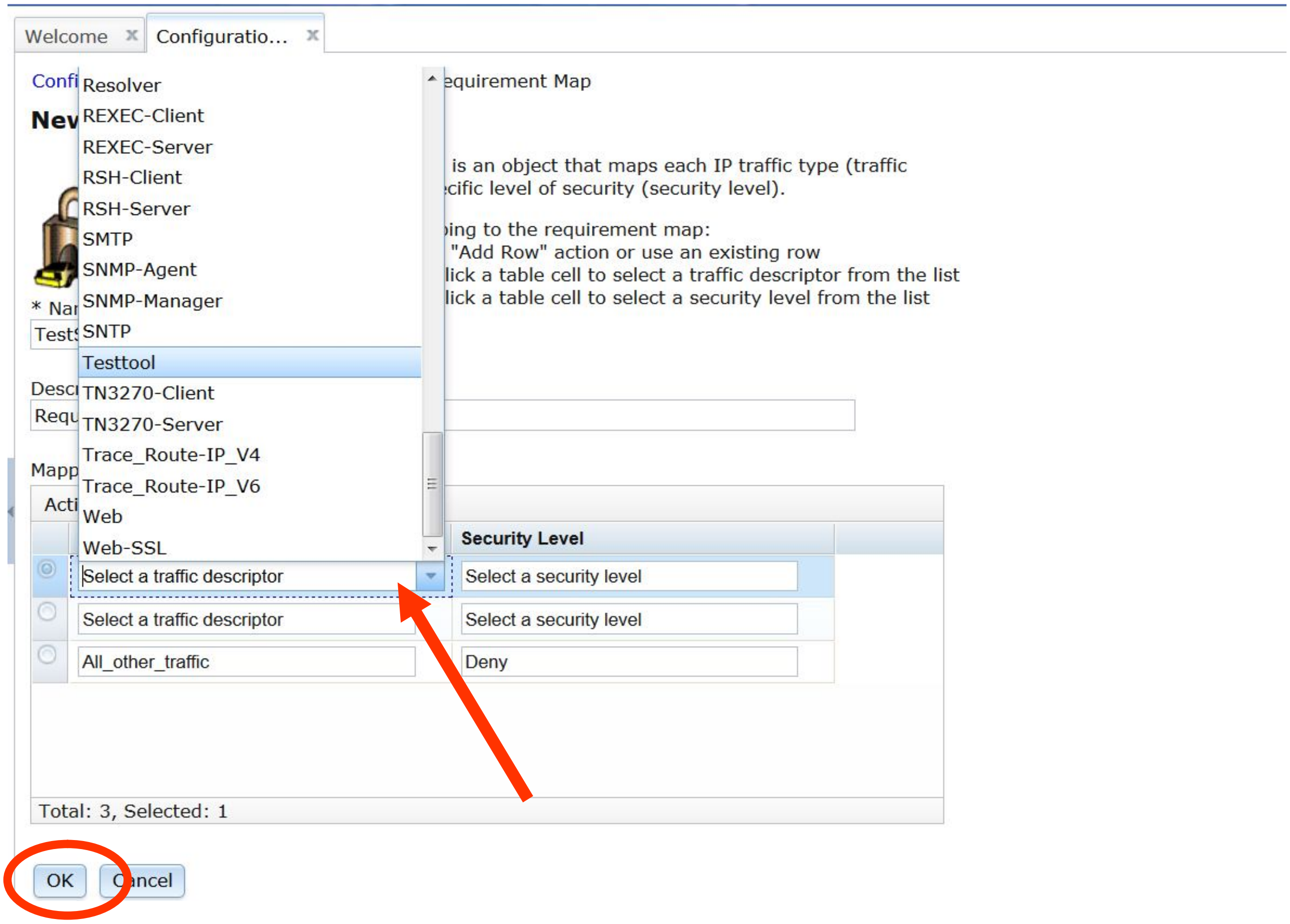
Mappings table

	Traffic Descriptor	Security Level
●	Select a traffic descriptor	Permit
○	Select a traffic descriptor	Select a security level
○	All_other_traffic	Deny

Total: 3, Selected: 1

Add the traffic descriptor **Testtool**.

Click "**Ok**"



equirement Map

is an object that maps each IP traffic type (traffic
cific level of security (security level).

ing to the requirement map:
"Add Row" action or use an existing row
lick a table cell to select a traffic descriptor from the list
lick a table cell to select a security level from the list

* Nar
Test

Desc
Requ

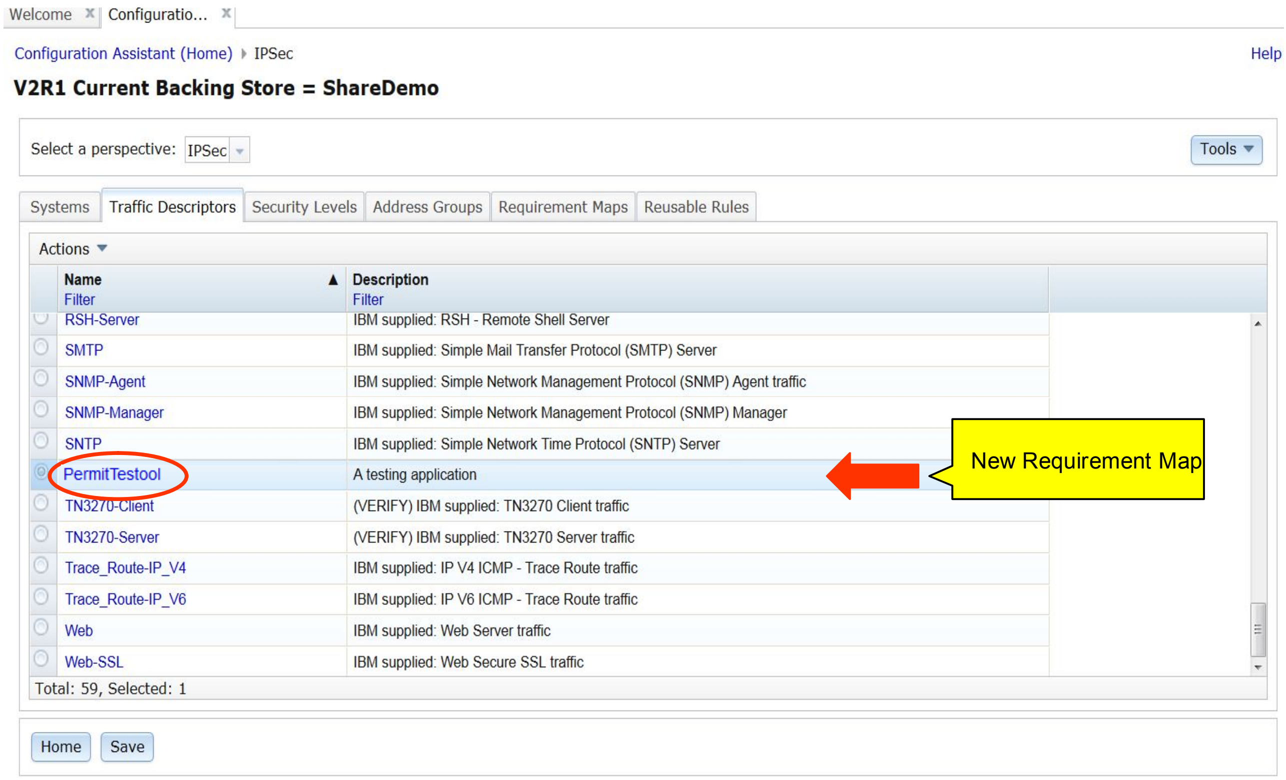
Mapp

Acti

		Security Level
●	Select a traffic descriptor	Select a security level
○	Select a traffic descriptor	Select a security level
○	All_other_traffic	Deny

Total: 3, Selected: 1

Congratulations a new Requirement Map has been created!



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

	Name ▲ Filter	Description Filter
○	RSH-Server	IBM supplied: RSH - Remote Shell Server
○	SMTP	IBM supplied: Simple Mail Transfer Protocol (SMTP) Server
○	SNMP-Agent	IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic
○	SNMP-Manager	IBM supplied: Simple Network Management Protocol (SNMP) Manager
○	SNTP	IBM supplied: Simple Network Time Protocol (SNTP) Server
●	PermitTestool	A testing application
○	TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
○	TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
○	Trace_Route-IP_V4	IBM supplied: IP V4 ICMP - Trace Route traffic
○	Trace_Route-IP_V6	IBM supplied: IP V6 ICMP - Trace Route traffic
○	Web	IBM supplied: Web Server traffic
○	Web-SSL	IBM supplied: Web Secure SSL traffic

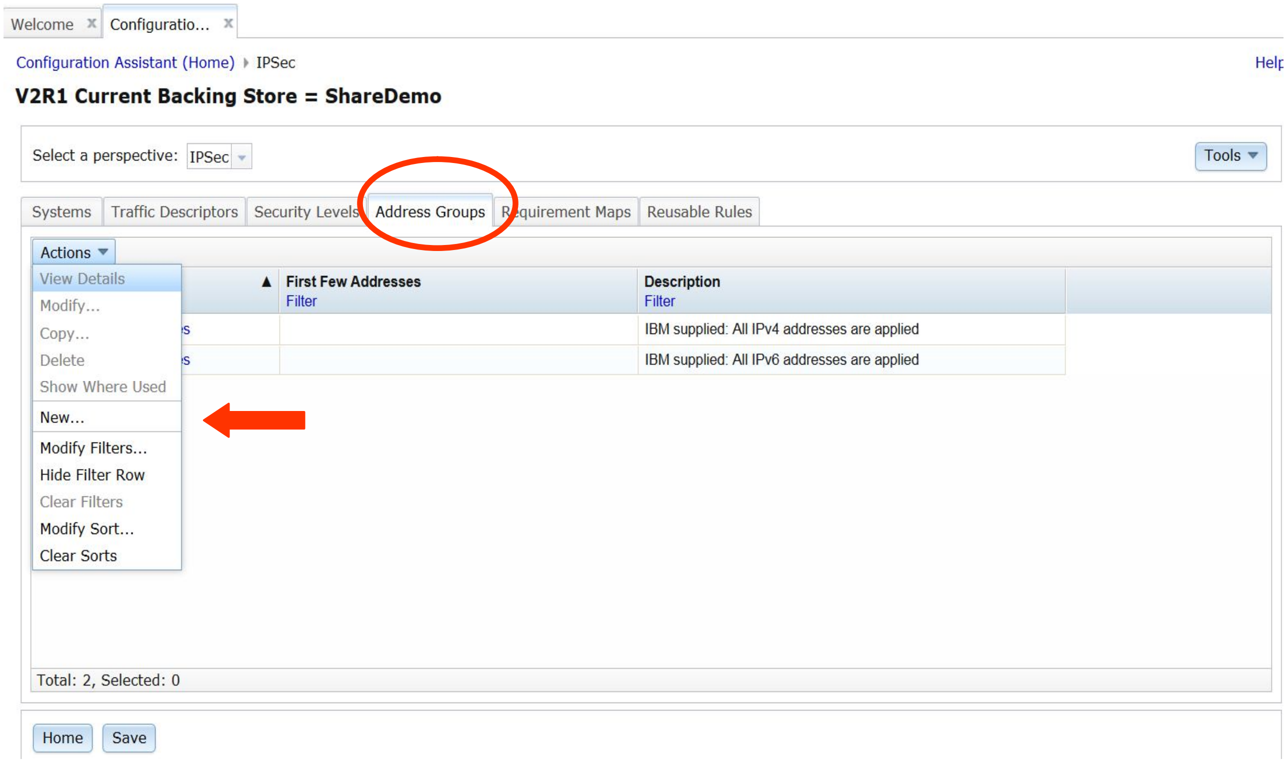
Total: 59, Selected: 1

Step 5c: Create an Address Group

An address group allows for defining the IP addresses and subnets that define the endpoints for the connectivity rule when protecting your Testtool application.

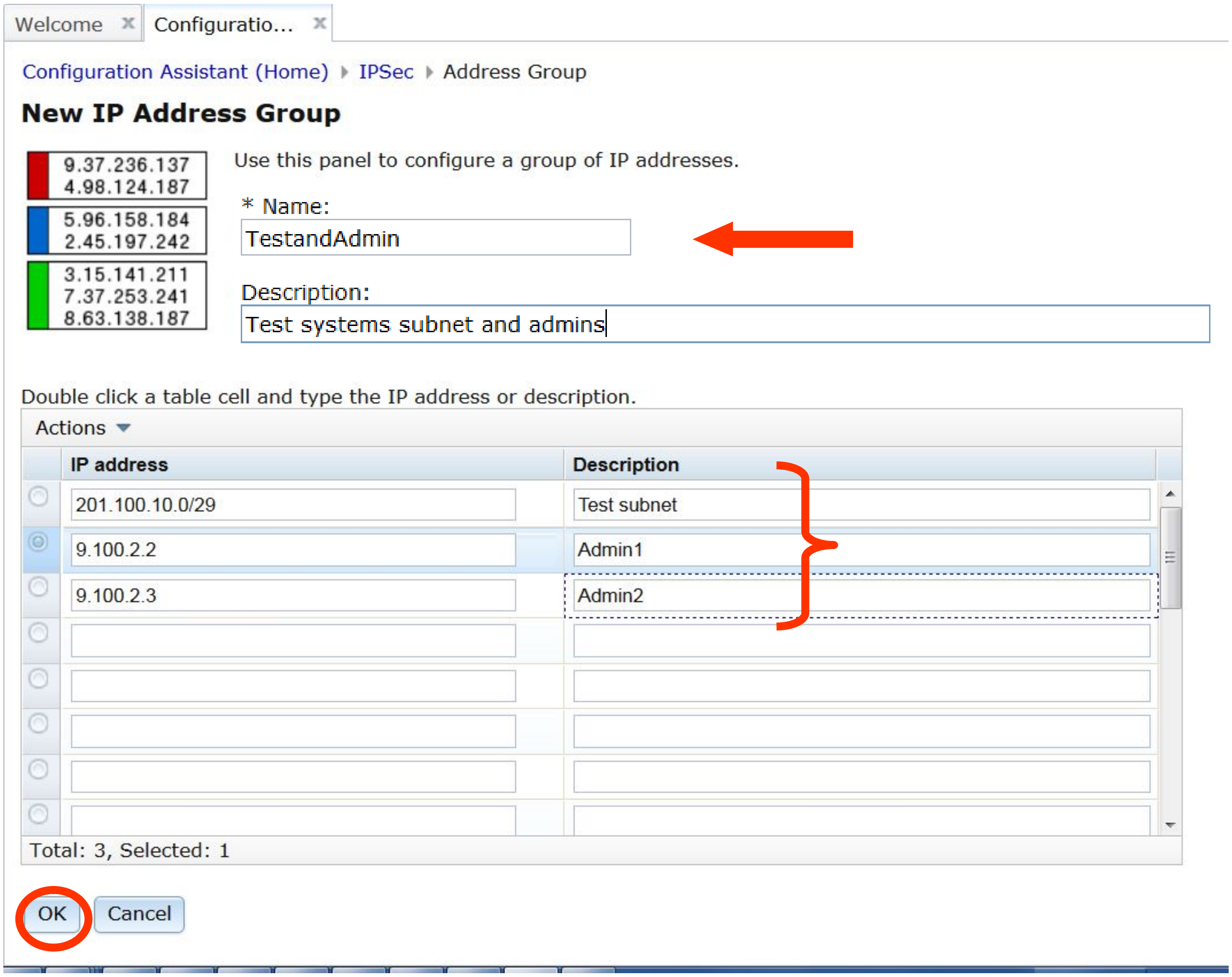
Select the **Address Groups** reusable resource tab. Use the table **Actions** menu and select **"New"** to begin creating an address group.

Recall that we need to permit the test systems and administrator to access Testtool. This is subnet 201.100.10.0/29 and IP addresses 9.100.2.2 and 9.100.2.3.



Add the following to the editable table: 201.100.10.0/29, and IP addresses 9.100.2.2 and 9.100.2.3.

Click “Ok”



Configuration Assistant (Home) ▸ IPSec ▸ Address Group

New IP Address Group

🟥 9.37.236.137 4.98.124.187
🟦 5.96.158.184 2.45.197.242
🟩 3.15.141.211 7.37.253.241 8.63.138.187

Use this panel to configure a group of IP addresses.

* Name: TestandAdmin

Description: Test systems subnet and admins

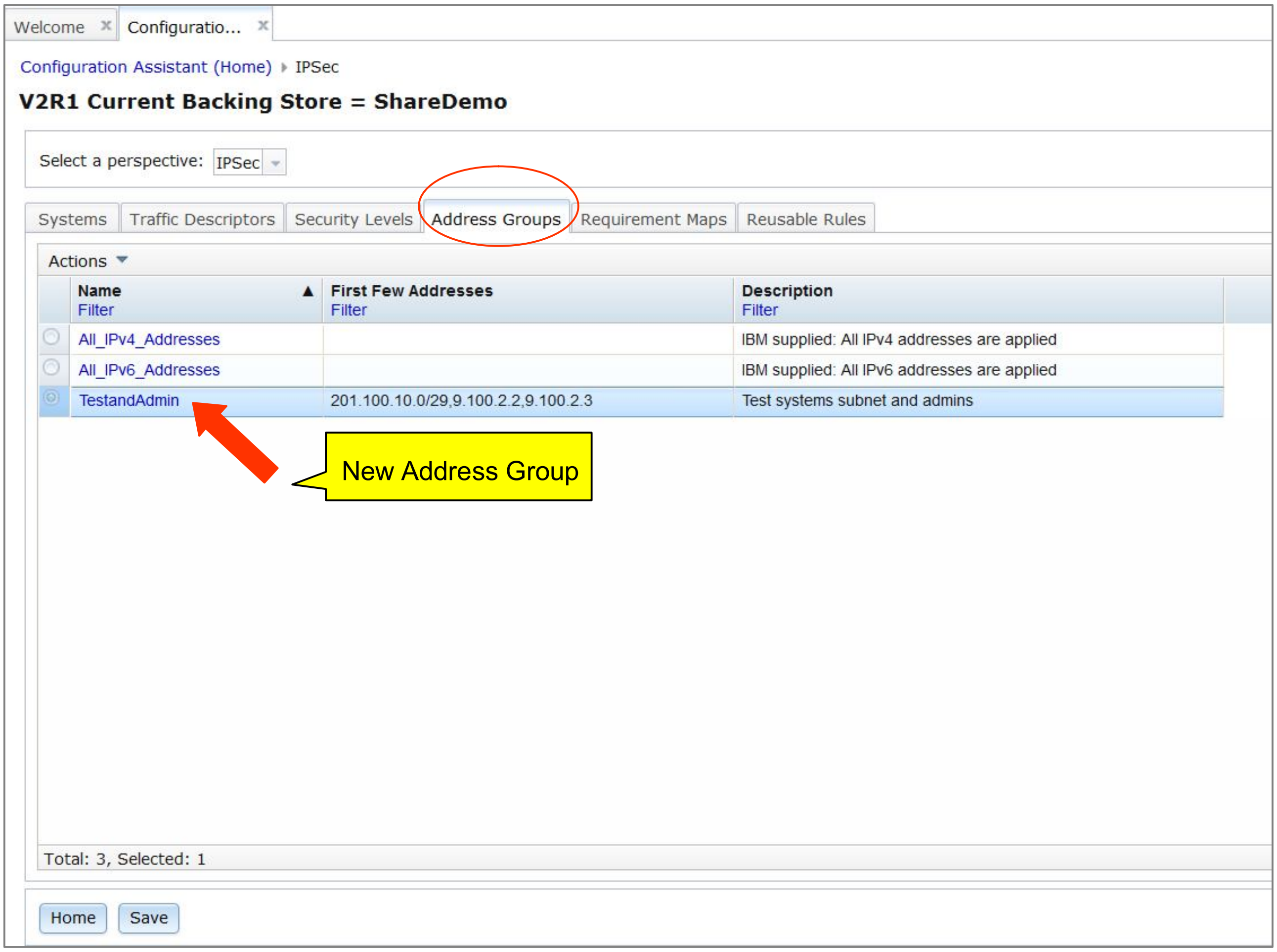
Double click a table cell and type the IP address or description.

Actions ▾

	IP address	Description
○	201.100.10.0/29	Test subnet
●	9.100.2.2	Admin1
○	9.100.2.3	Admin2
○		
○		
○		
○		
○		

Total: 3, Selected: 1

Congratulations a new address group, “**TestandAdmin**” has been created!



V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

	Name Filter	First Few Addresses Filter	Description Filter
○	All_IPv4_Addresses		IBM supplied: All IPv4 addresses are applied
○	All_IPv6_Addresses		IBM supplied: All IPv6 addresses are applied
●	TestandAdmin	201.100.10.0/29,9.100.2.2,9.100.2.3	Test systems subnet and admins

Total: 3, Selected: 1

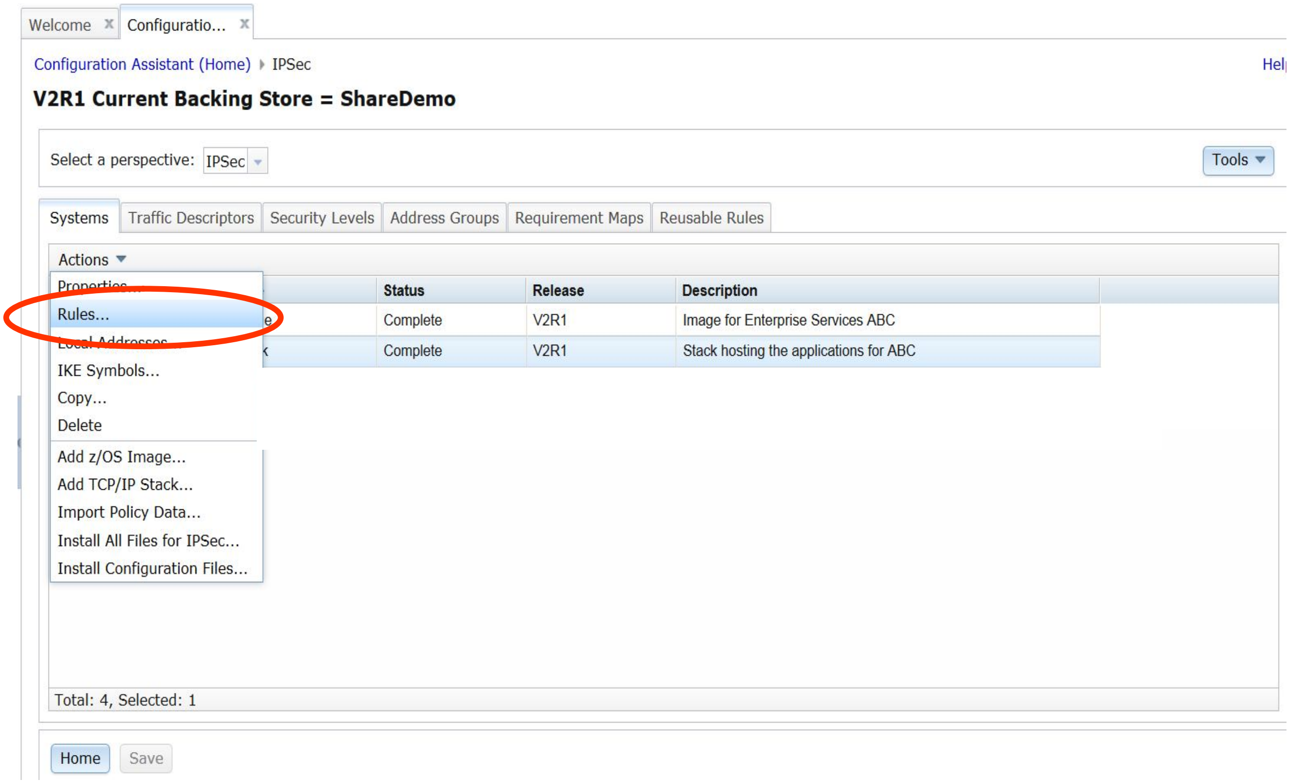
Now that reusable resources have been created (traffic descriptors, address groups, and requirement maps) , these will become the components of the connectivity rule.

Reusable resources don’t actually result in any TCP/IP policy configuration!   It is only when the connectivity rule is created that configuration can be generated for the stack.

Step 5d: Create a **Connectivity Rule** for the Testtool application

First, from the Systems table, select the TCP/IP stack. Then, select **“Rules…”** from the **Actions** menu to begin configuring this stack with IPSec connectivity rules.

A wizard will assist with creating the rule.



Configuration Assistant (Home) ▸ IPSec

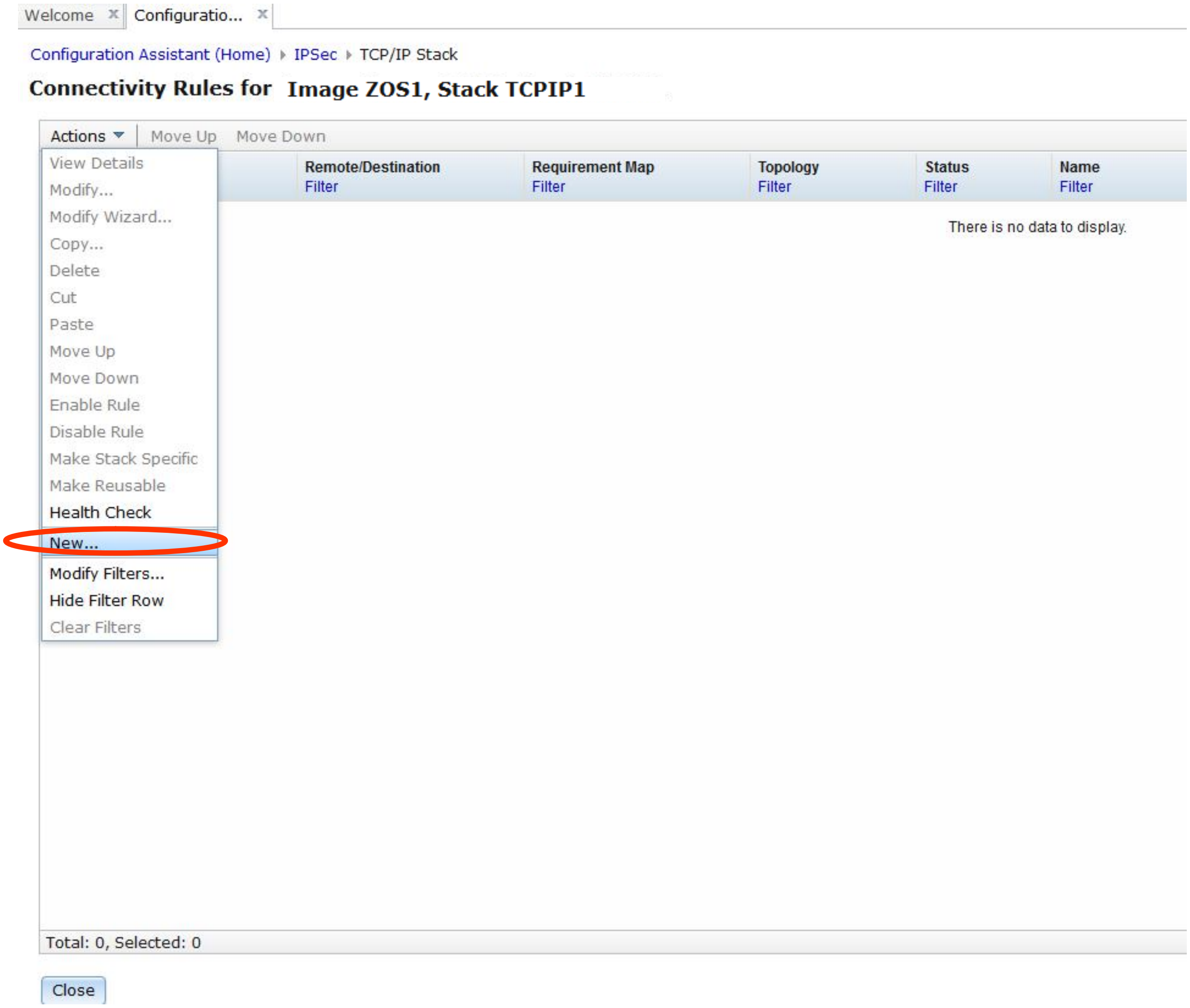
V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

	Status	Release	Description
e	Complete	V2R1	Image for Enterprise Services ABC
k	Complete	V2R1	Stack hosting the applications for ABC

Total: 4, Selected: 1

Click “New” to begin creating a connectivity rule



Connectivity Rules for Image ZOS1, Stack TCPIP1

Remote/Destination	Requirement Map	Topology	Status	Name
Filter	Filter	Filter	Filter	Filter

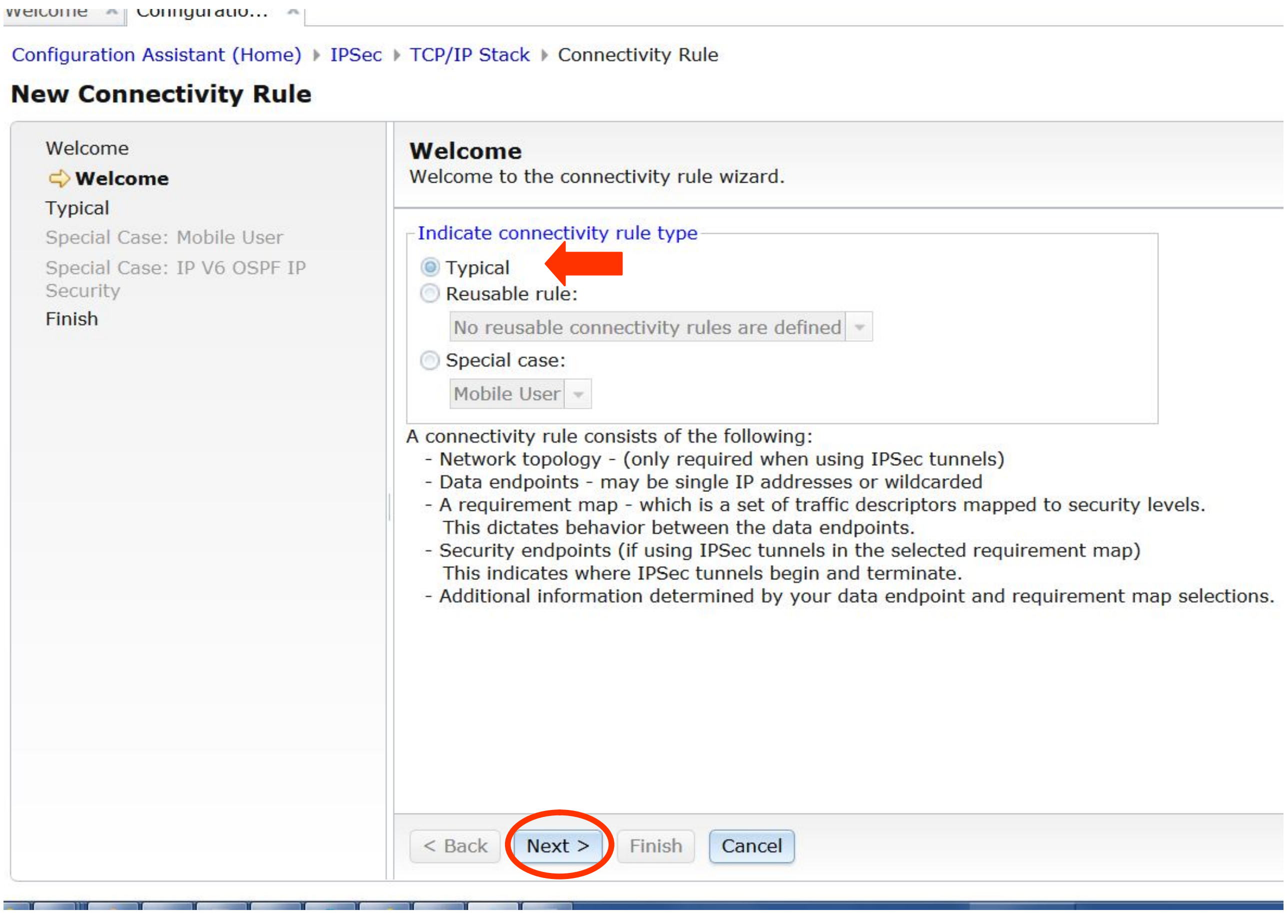
There is no data to display.

Total: 0, Selected: 0

Several types of connectivity rules are supported for IP Security, but the “**Typical**” rule allows for configuring basic filter rules and tunnels.

Use the radio button to select **“Typical”**.

Click “**Next**”



Configuration Assistant (Home) ▸ IPSec ▸ TCP/IP Stack ▸ Connectivity Rule
Welcome
Welcome
Typical
Special Case: Mobile User
Special Case: IP V6 OSPF IP Security
Finish
< Back
Next >
Finish
Cancel

New Connectivity Rule

Welcome

Welcome to the connectivity rule wizard.

Indicate connectivity rule type

● Typical

○ Reusable rule: No reusable connectivity rules are defined

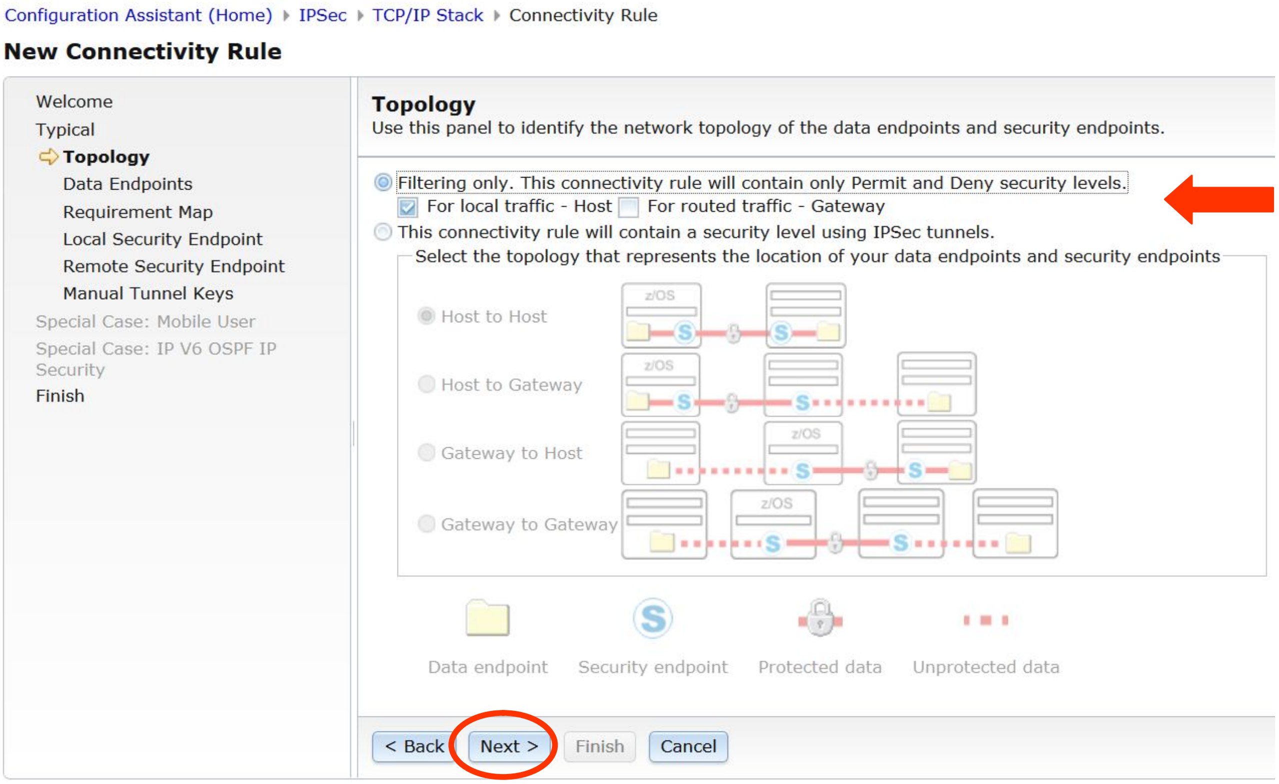
○ Special case: Mobile User

A connectivity rule consists of the following:

- Network topology - (only required when using IPSec tunnels)
- Data endpoints - may be single IP addresses or wildcarded
- A requirement map - which is a set of traffic descriptors mapped to security levels. This dictates behavior between the data endpoints.
- Security endpoints (if using IPSec tunnels in the selected requirement map) This indicates where IPSec tunnels begin and terminate.
- Additional information determined by your data endpoint and requirement map selections.

The rule to protect Testool is a basic filtering rule, so use the radio button to select **"Filtering only".** We're only concerned about **local traffic** since Testtool runs on this stack, so ensure **local traffic** is checked.

Click "**Next**"



Configuration Assistant (Home) ▸ IPSec ▸ TCP/IP Stack ▸ Connectivity Rule

New Connectivity Rule

- Welcome
- Typical
- ⇨ **Topology**
  - Data Endpoints
  - Requirement Map
  - Local Security Endpoint
  - Remote Security Endpoint
  - Manual Tunnel Keys
- Special Case: Mobile User
- Special Case: IP V6 OSPF IP Security
- Finish

Topology

Use this panel to identify the network topology of the data endpoints and security endpoints.

● Filtering only. This connectivity rule will contain only Permit and Deny security levels.

☑ For local traffic - Host □ For routed traffic - Gateway

○ This connectivity rule will contain a security level using IPSec tunnels.

Select the topology that represents the location of your data endpoints and security endpoints

○ Host to Host

○ Host to Gateway

○ Gateway to Host

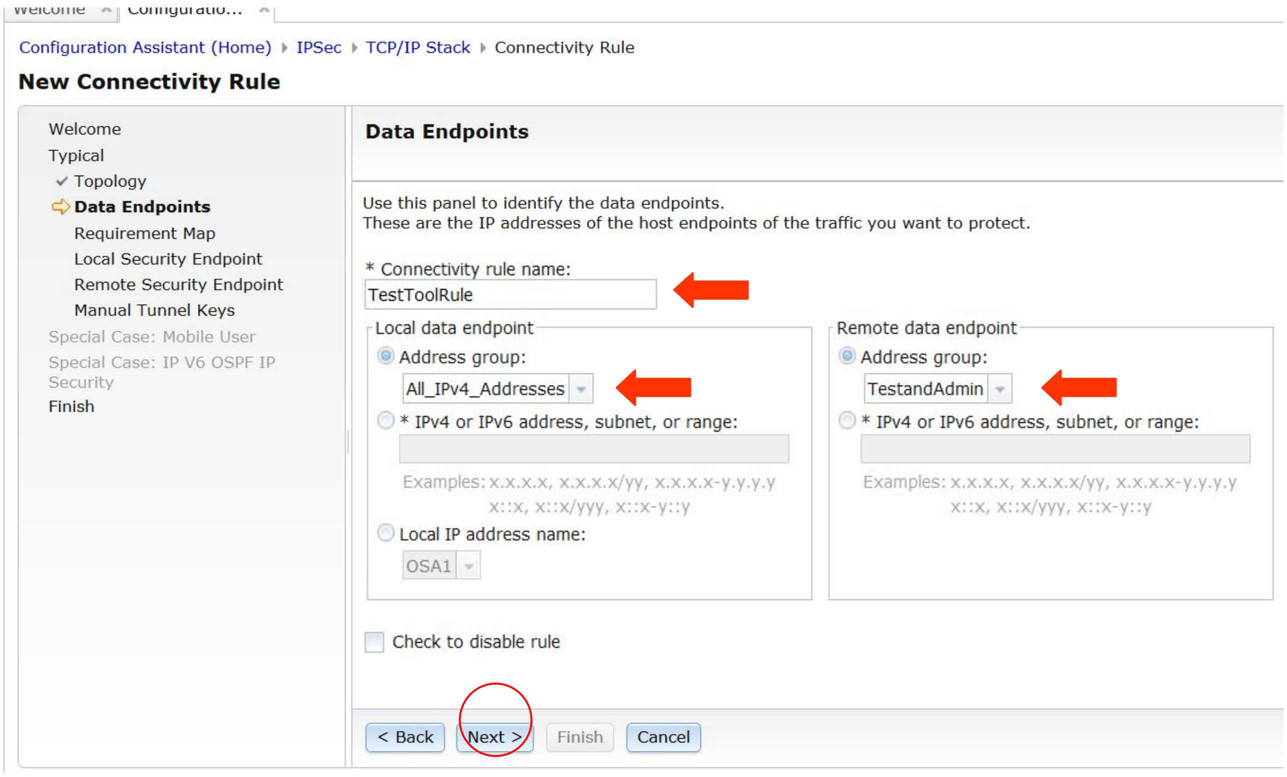
○ Gateway to Gateway

When creating the filter rule, the **local and remote data endpoints** refer to the IP addresses and/or networks that are the endpoints for communication. The **local data endpoint** refers to this stack.

Since our Testtool is a server application that issues a socket bind() to INAddr_Any (all IP addresses) and listens for incoming connections, we'll protect **All_IPv4_Addresses** for the **"Local data endpoint"** selection.

For the **"Remote data endpoint",** select the **TestandAdmin** address group that was created to ensure the intended users can access the Testtool application.

Click "**Next**"



Configuration Assistant (Home) ▸ IPSec ▸ TCP/IP Stack ▸ Connectivity Rule

New Connectivity Rule

Data Endpoints

Use this panel to identify the data endpoints.
These are the IP addresses of the host endpoints of the traffic you want to protect.

* Connectivity rule name: TestToolRule

Local data endpoint
● Address group: All_IPv4_Addresses
○ * IPv4 or IPv6 address, subnet, or range:
Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x::x, x::x/yyy, x::x-y::y
○ Local IP address name: OSA1

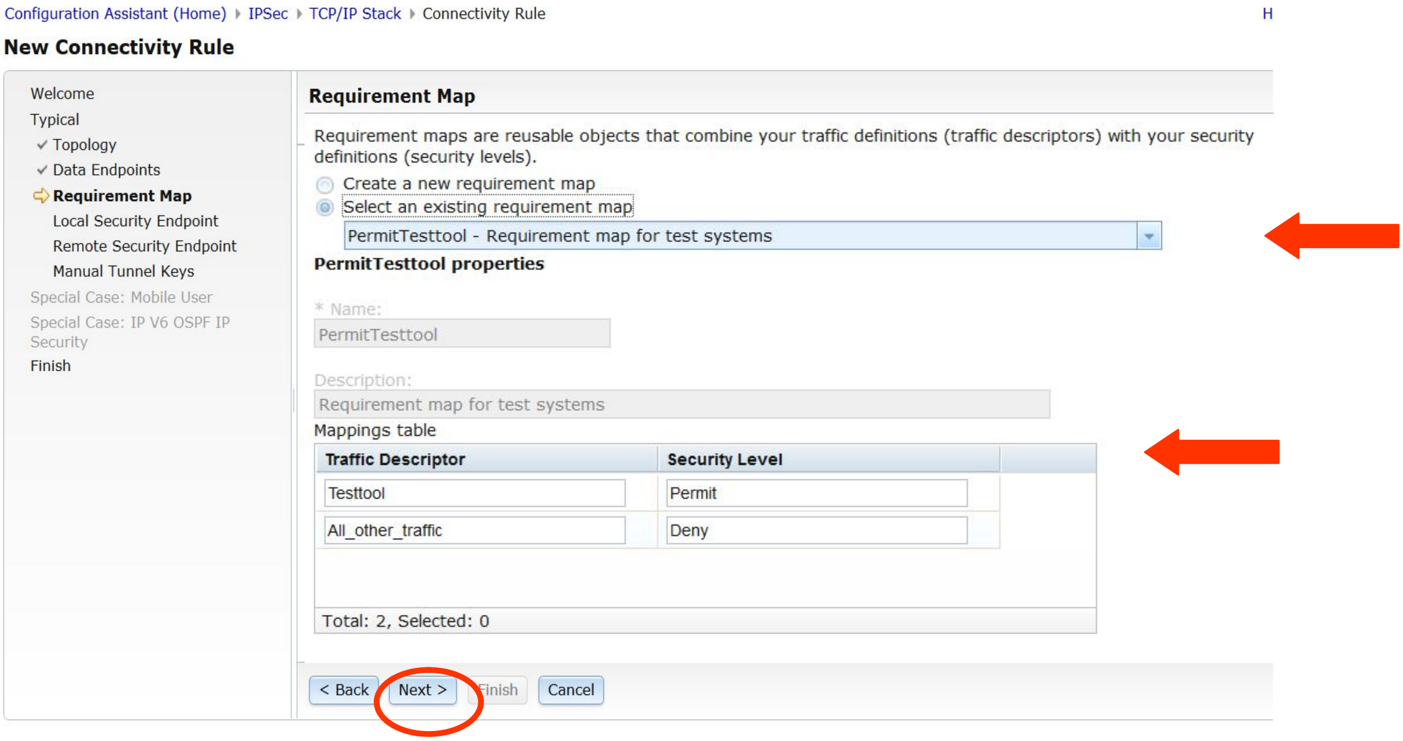
Remote data endpoint
● Address group: TestandAdmin
○ * IPv4 or IPv6 address, subnet, or range:
Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x::x, x::x/yyy, x::x-y::y

□ Check to disable rule

Now that the communication endpoints have been defined for the connectivity rule, next a requirement map is needed. A new requirement map can be created or one that is already existing can be used.

Select the requirement map, **PermitTestool,** that was just created. Once selected, the traffic descriptor(s) and security level that comprise PermitTesttool is shown.

Click "**Next**"



Configuration Assistant (Home) ▸ IPSec ▸ TCP/IP Stack ▸ Connectivity Rule

New Connectivity Rule

Requirement Map

Requirement maps are reusable objects that combine your traffic definitions (traffic descriptors) with your security definitions (security levels).

○ Create a new requirement map
● Select an existing requirement map

PermitTesttool - Requirement map for test systems

PermitTesttool properties

* Name: PermitTesttool

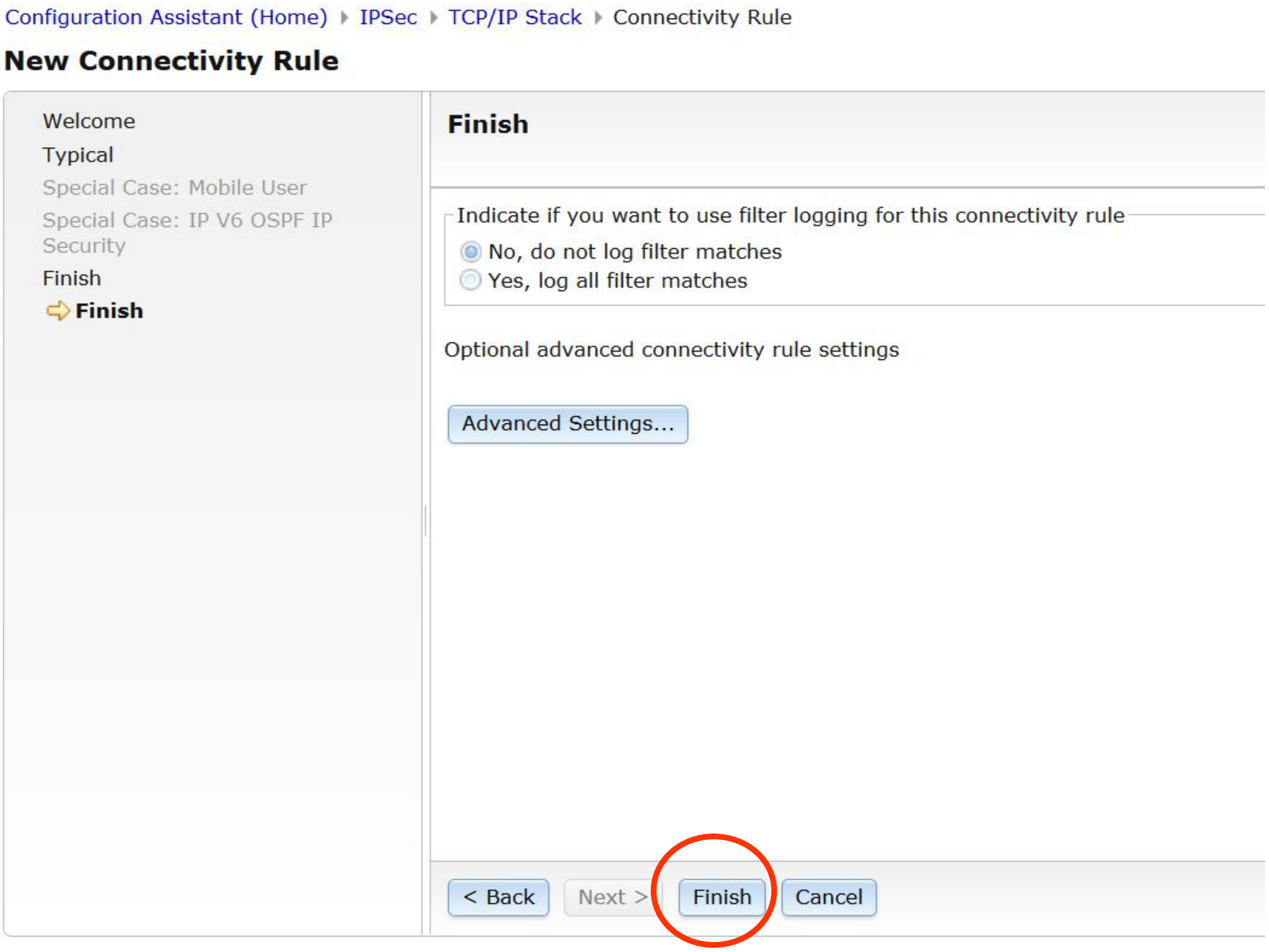
Description: Requirement map for test systems

Mappings table

Traffic Descriptor	Security Level
Testtool	Permit
All_other_traffic	Deny

Total: 2, Selected: 0

Select the **"Finish"** button to complete the connectivity rule.



Configuration Assistant (Home) ▸ IPSec ▸ TCP/IP Stack ▸ Connectivity Rule

New Connectivity Rule

Welcome
Typical
Special Case: Mobile User
Special Case: IP V6 OSPF IP Security
Finish
⇨ **Finish**

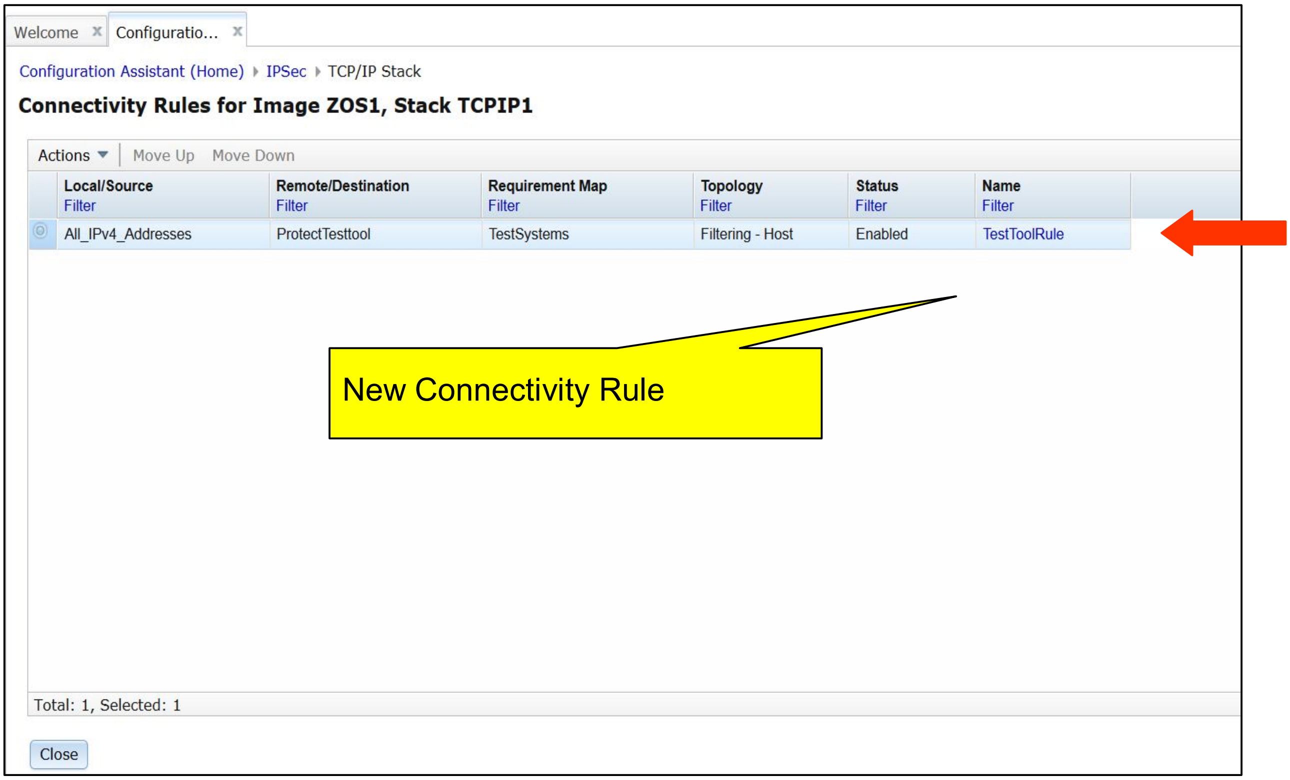
Finish

Indicate if you want to use filter logging for this connectivity rule

● No, do not log filter matches
○ Yes, log all filter matches

Optional advanced connectivity rule settings

Congratulations you have a new connectivity rule, **TestToolRule**, for Image ZOS1, TCP/IP stack TCPIP1!



Connectivity Rules for Image ZOS1, Stack TCPIP1

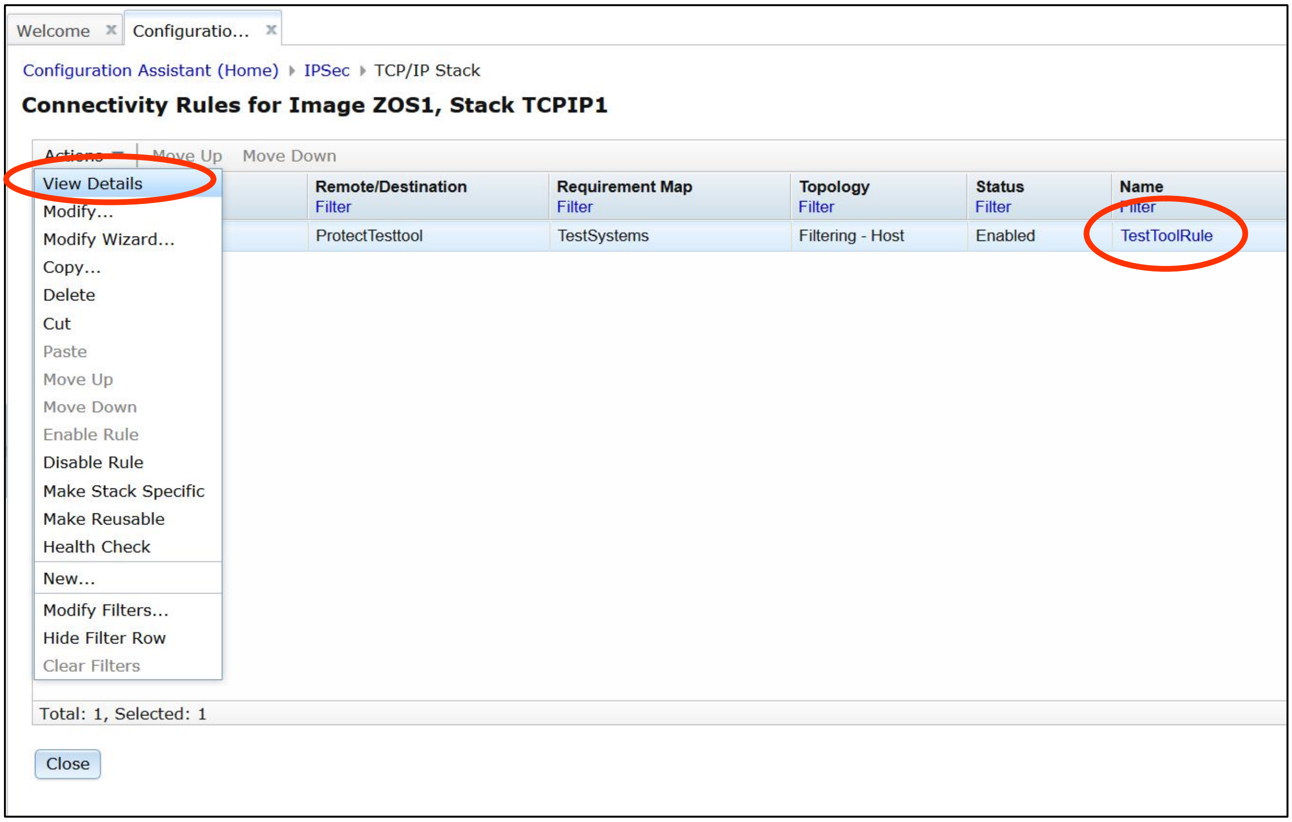
	Local/Source Filter	Remote/Destination Filter	Requirement Map Filter	Topology Filter	Status Filter	Name Filter
●	All_IPv4_Addresses	ProtectTesttool	TestSystems	Filtering - Host	Enabled	TestToolRule

Total: 1, Selected: 1

Now you can perform additional actions on the rule, such as:

- **View Details** to view the details of the rule
- Optionally, under the column "**Name**", click on the "TestToolRule" link. From here you can modify the rule or you can use the table **Actions** menu to modify.

When complete, click on the **"Close**" button and return to the view of the **Systems table.**



Configuration Assistant (Home) ▸ IPSec ▸ TCP/IP Stack

Connectivity Rules for Image ZOS1, Stack TCPIP1

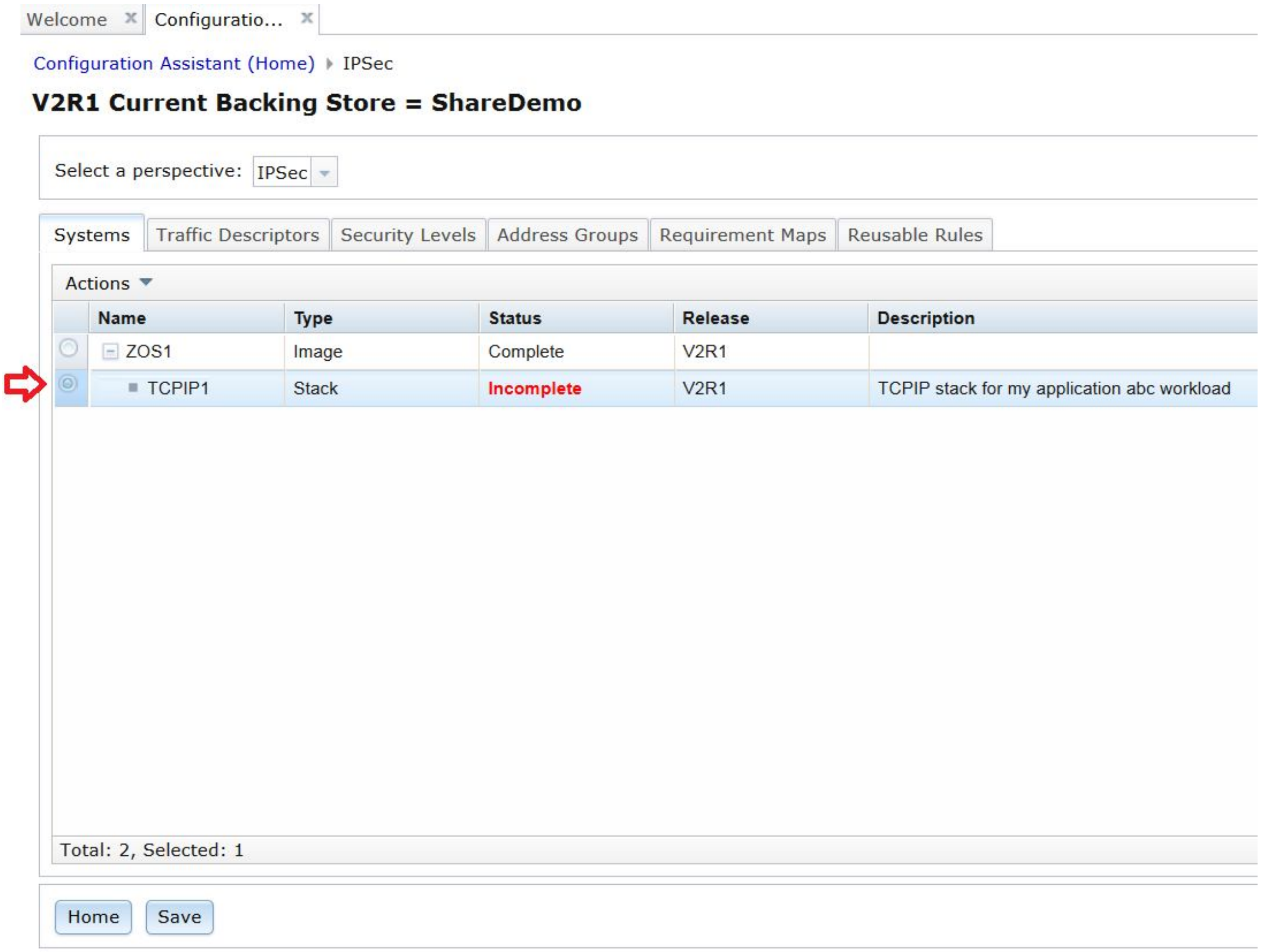
Remote/Destination Filter	Requirement Map Filter	Topology Filter	Status Filter	Name Filter
ProtectTesttool	TestSystems	Filtering - Host	Enabled	TestToolRule

Total: 1, Selected: 1

6. Generating and Installing the Configuration

Now that the rule is created, configuration must be generated and installed so that the Policy Agent (Pagent) can read the new configuration and install the new rule into the TCP/IP stack.

Select the TCP/IP stack, TCPIP1 and click on the **Actions** menu.



Configuration Assistant (Home) ▸ IPSec

V2R1 Current Backing Store = ShareDemo

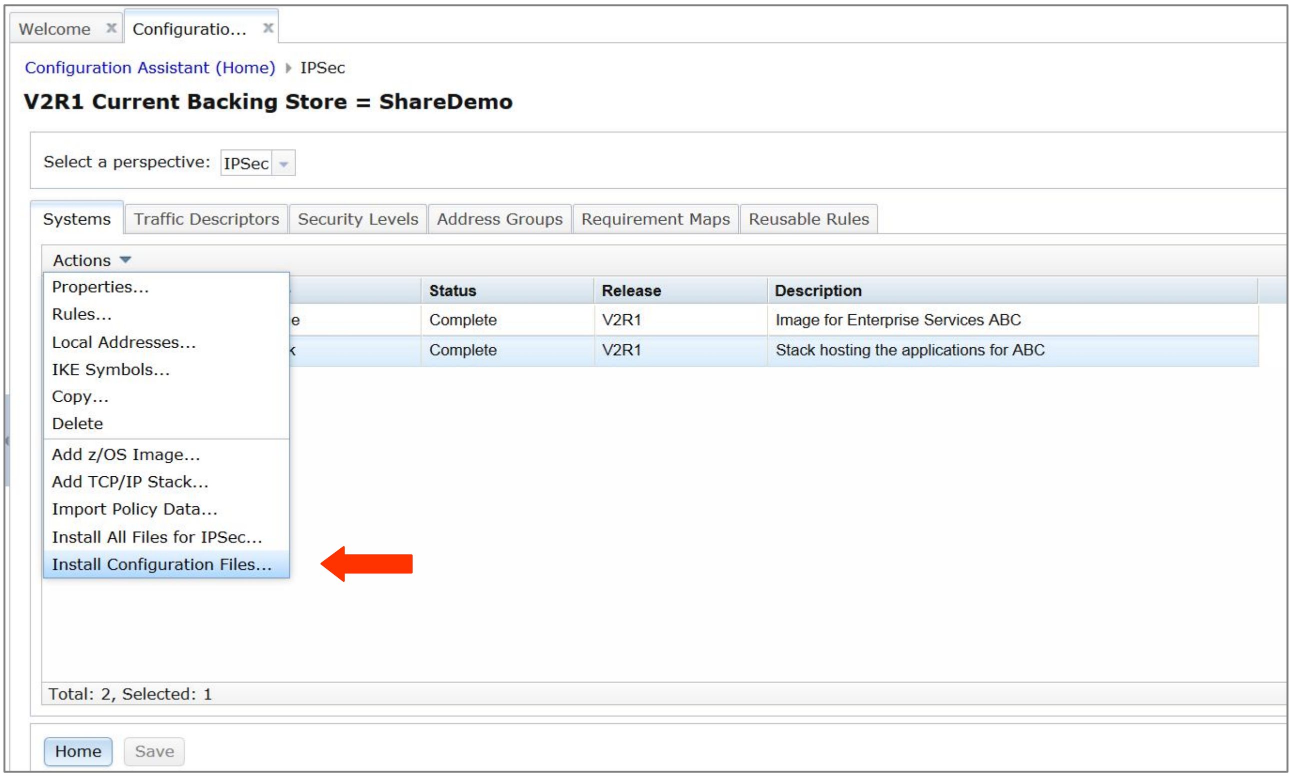
Select a perspective: IPSec

	Name	Type	Status	Release	Description
○	⊟ ZOS1	Image	Complete	V2R1	
◉	■ TCPIP1	Stack	Incomplete	V2R1	TCPIP stack for my application abc workload

Total: 2, Selected: 1

Step 6a: Select **"Install Configuration Files".**

With this action, the Configuration Assistant will generate the IPSec policy and prepare it for installation (saving to disk or FTP).



Configuration Assistant (Home) ▸ IPSec

V2R1 Current Backing Store = ShareDemo

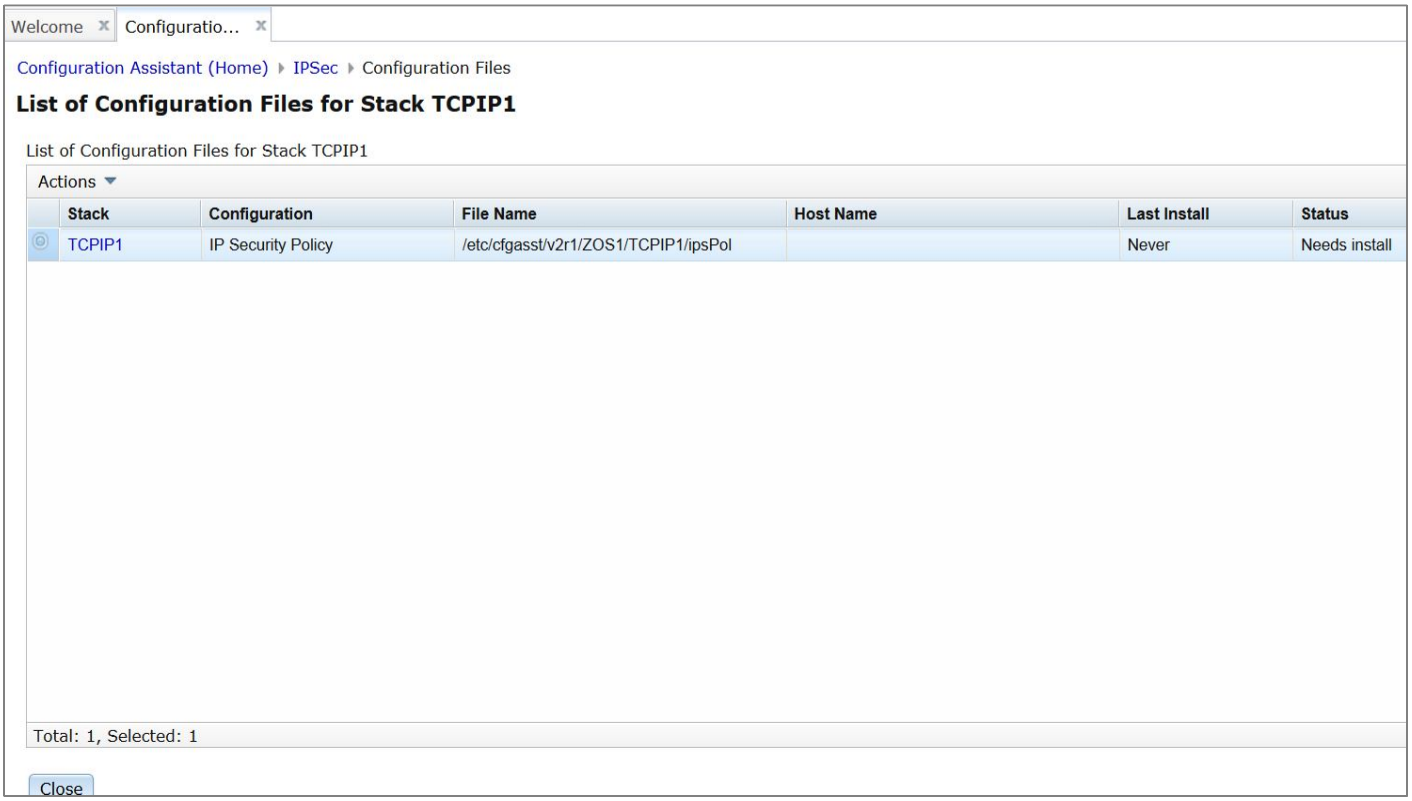
Select a perspective: IPSec

	Status	Release	Description
e	Complete	V2R1	Image for Enterprise Services ABC
k	Complete	V2R1	Stack hosting the applications for ABC

Total: 2, Selected: 1

The following displays the entry that represents the IPSec policy that will be generated for stack TCPIP1, and provides information about when the install (save to disk or FTP) for this policy has occurred (see the table columns).

Click on the entry TCPIP1 and the table **Actions** menu.


Welcome ×
Configuratio... ×
Configuration Assistant (Home) ▸ IPSec ▸ Configuration Files

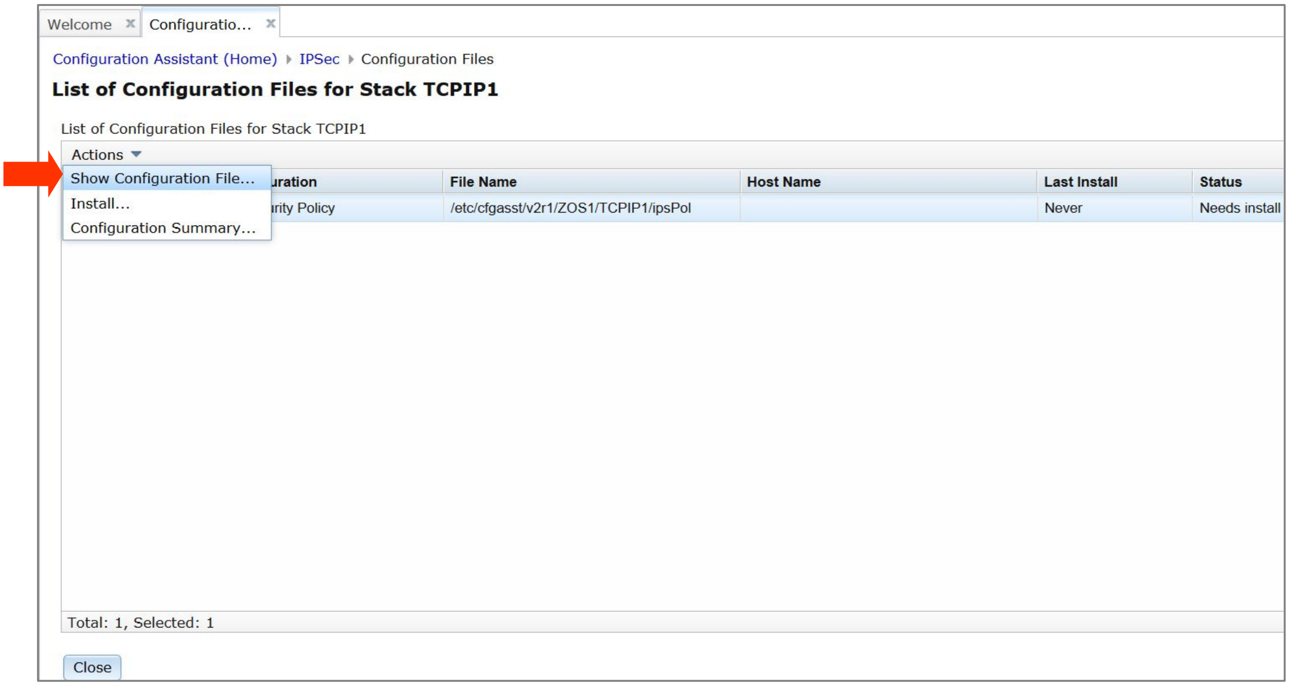
List of Configuration Files for Stack TCPIP1

List of Configuration Files for Stack TCPIP1

	Stack	Configuration	File Name	Host Name	Last Install	Status
●	TCPIP1	IP Security Policy	/etc/cfgasst/v2r1/ZOS1/TCPIP1/ipsPol		Never	Needs install

Total: 1, Selected: 1

Step 6b: Before clicking on install, view the policy configuration that will be generated if you are curious!



Welcome ✕
Configuratio... ✕
Configuration Assistant (Home) ▸ IPSec ▸ Configuration Files

List of Configuration Files for Stack TCPIP1

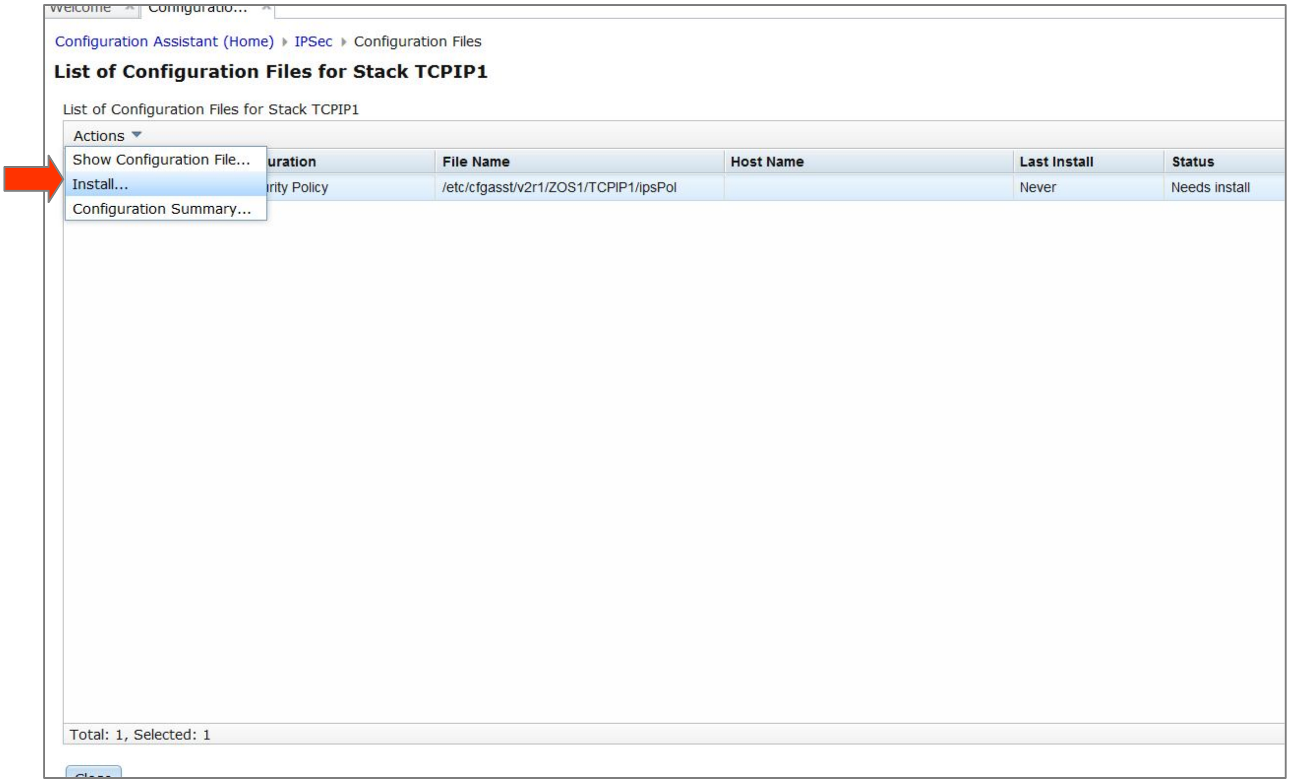
List of Configuration Files for Stack TCPIP1

Actions ▾
Show Configuration File...
Install...
Configuration Summary...

...uration	File Name	Host Name	Last Install	Status
...rity Policy	/etc/cfgasst/v2r1/ZOS1/TCPIP1/ipsPol		Never	Needs install

Total: 1, Selected: 1

Step 6c: Use the **Actions** menu to select **Install**



Configuration Assistant (Home) ▸ IPSec ▸ Configuration Files

List of Configuration Files for Stack TCPIP1

List of Configuration Files for Stack TCPIP1

...uration	File Name	Host Name	Last Install	Status
...rity Policy	/etc/cfgasst/v2r1/ZOS1/TCPIP1/ipsPol		Never	Needs install

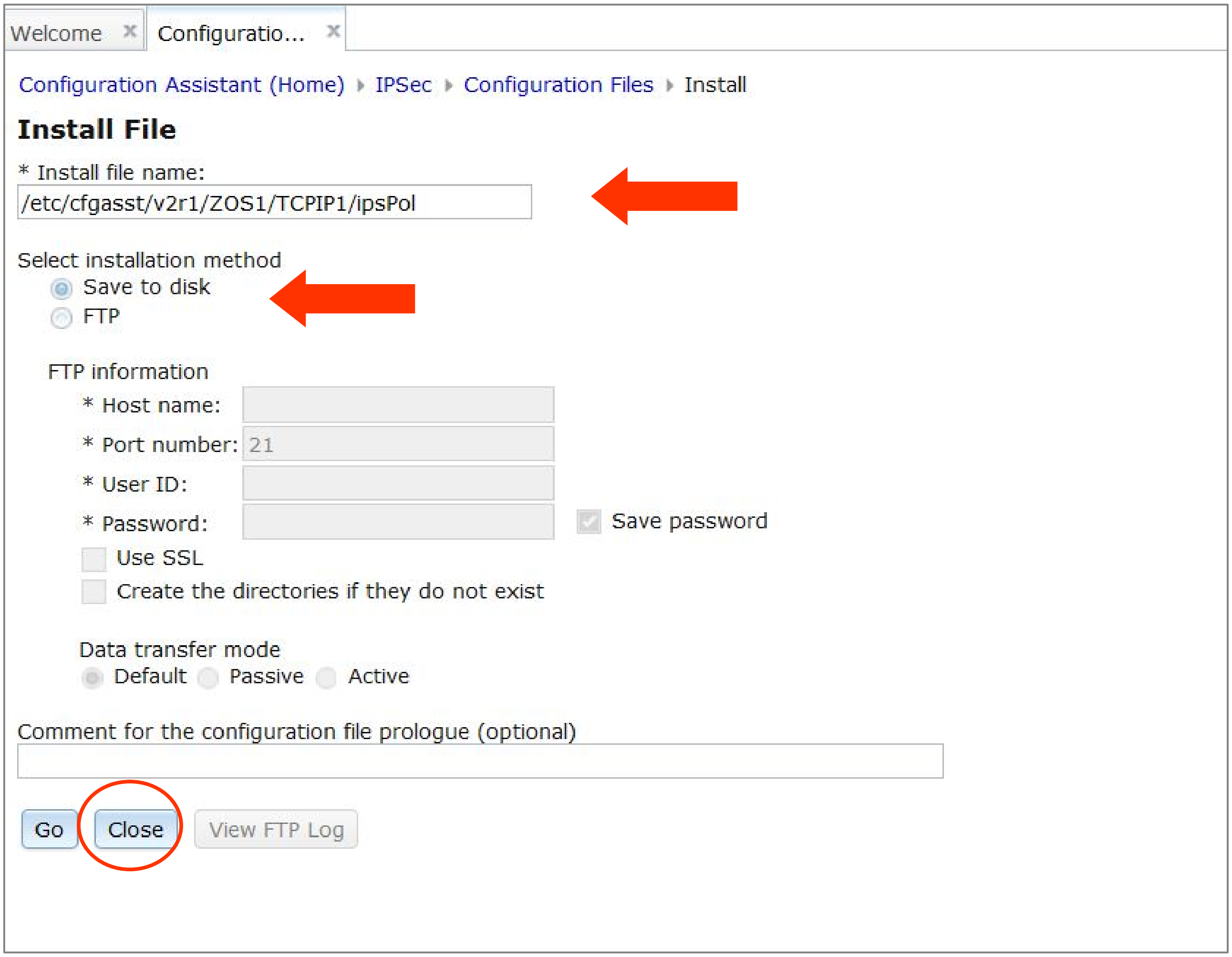
Total: 1, Selected: 1

The install panel is launched.

Install file name: The Install file name can be changed. Both Unix file names and MVS datasets are supported.

Installation method: Files may be saved locally or can be FTP'd to another system.

Note: Since this is a "demo" system, you won't be able to save the file, so just click **"Close"**


Welcome
Configuratio...
Configuration Assistant (Home) ▸ IPSec ▸ Configuration Files ▸ Install
Go
Close
View FTP Log

Install File

* Install file name: /etc/cfgasst/v2r1/ZOS1/TCPIP1/ipsPol

Select installation method

● Save to disk

○ FTP

FTP information

* Host name:

* Port number: 21

* User ID:

* Password:

☑ Save password

□ Use SSL

□ Create the directories if they do not exist

Data transfer mode

● Default ○ Passive ○ Active

Comment for the configuration file prologue (optional)

7. Optional Exercise

7.1 Exploring the "Tools" button

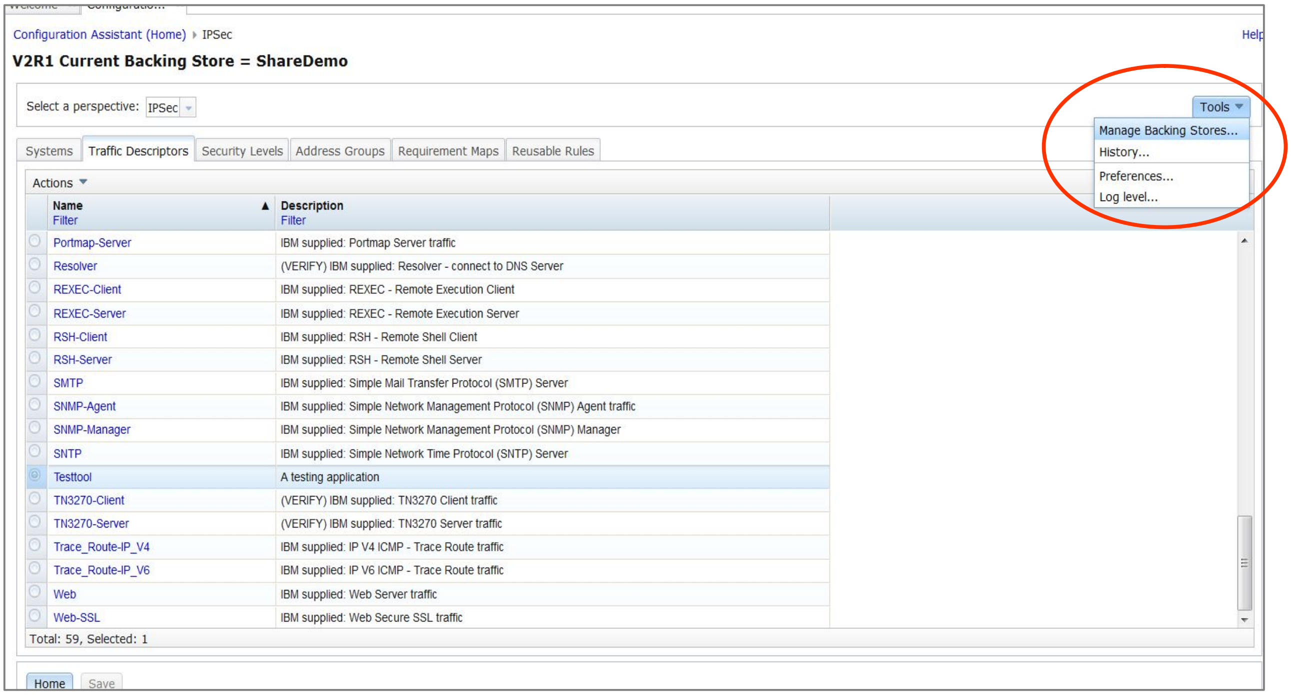
The tools button provides access to tasks that occur outside of the technology perspectives. These tasks relate to the Configuration Assistant as a whole and apply consistently across perspectives.

We'll take a quick look at all tasks except for **Log Level.** This is serviceability setting that you may be directed to change by IBM Service based upon the need for servicing the product.

Step 7.1a: Tools button

The **Tools** button is in the right corner of the panel for each technology perspective.

Click on the drop-down arrow on the button to display the Actions.



V2R1 Current Backing Store = ShareDemo

	Name Filter	Description Filter
○	Portmap-Server	IBM supplied: Portmap Server traffic
○	Resolver	(VERIFY) IBM supplied: Resolver - connect to DNS Server
○	REXEC-Client	IBM supplied: REXEC - Remote Execution Client
○	REXEC-Server	IBM supplied: REXEC - Remote Execution Server
○	RSH-Client	IBM supplied: RSH - Remote Shell Client
○	RSH-Server	IBM supplied: RSH - Remote Shell Server
○	SMTP	IBM supplied: Simple Mail Transfer Protocol (SMTP) Server
○	SNMP-Agent	IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic
○	SNMP-Manager	IBM supplied: Simple Network Management Protocol (SNMP) Manager
○	SNTP	IBM supplied: Simple Network Time Protocol (SNTP) Server
●	Testtool	A testing application
○	TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
○	TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
○	Trace_Route-IP_V4	IBM supplied: IP V4 ICMP - Trace Route traffic
○	Trace_Route-IP_V6	IBM supplied: IP V6 ICMP - Trace Route traffic
○	Web	IBM supplied: Web Server traffic
○	Web-SSL	IBM supplied: Web Secure SSL traffic

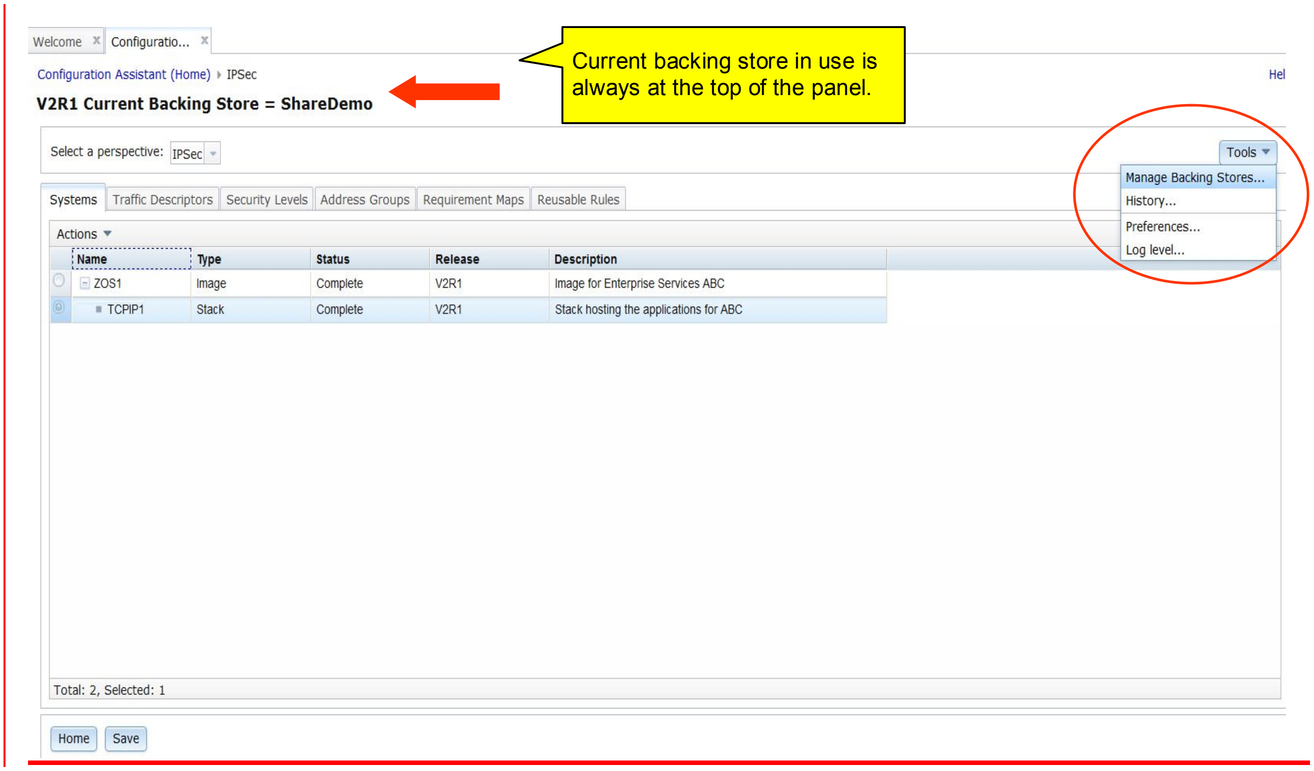
Total: 59, Selected: 1

Step 7.1b: Manage Backing Stores

The Manage Backing Stores task is new in z/OS V2R1. A new panel has been developed to assist with improved backing store management.

From each perspective, access the Tools drop-down menu on the right of the panel.

Click on "**Manage Backing Stores**"



Current backing store in use is always at the top of the panel.

Configuration Assistant (Home) ▸ IPSec

V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

	Name	Type	Status	Release	Description
○	⊟ ZOS1	Image	Complete	V2R1	Image for Enterprise Services ABC
●	▪ TCPIP1	Stack	Complete	V2R1	Stack hosting the applications for ABC

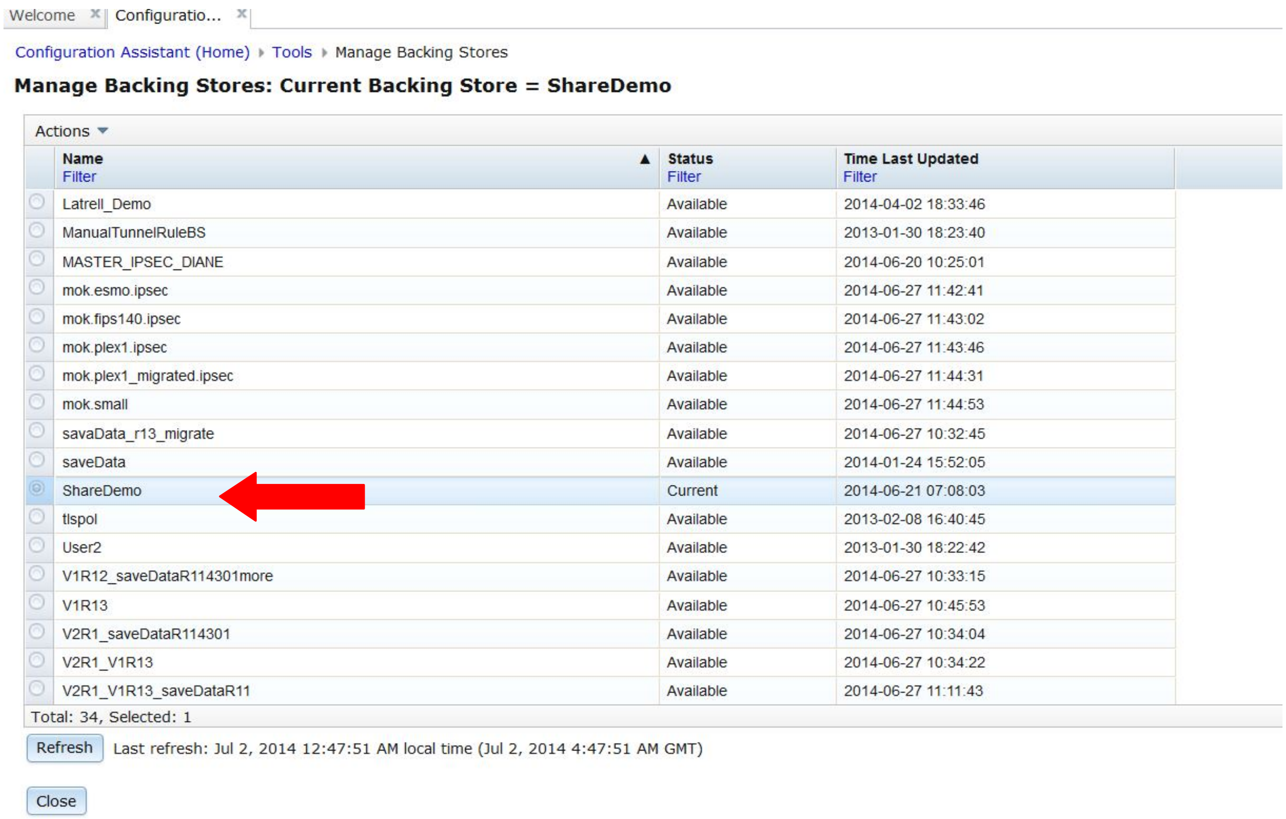
Total: 2, Selected: 1

Displays all of the backing stores.

Notice the **Status** and **Time Last Updated** columns and that the backing store in use is "current".

- A status of "**Available**" indicates that the backing store is free for use. A status of **"Locked**" indicates the backing store is in use by another user.

Next click on the table **Actions** menu.


Welcome
Configuratio...
Configuration Assistant (Home) ▸ Tools ▸ Manage Backing Stores
Actions ▾
Refresh
Close

Manage Backing Stores: Current Backing Store = ShareDemo

	Name ▲ Filter	Status Filter	Time Last Updated Filter
○	Latrell_Demo	Available	2014-04-02 18:33:46
○	ManualTunnelRuleBS	Available	2013-01-30 18:23:40
○	MASTER_IPSEC_DIANE	Available	2014-06-20 10:25:01
○	mok.esmo.ipsec	Available	2014-06-27 11:42:41
○	mok.fips140.ipsec	Available	2014-06-27 11:43:02
○	mok.plex1.ipsec	Available	2014-06-27 11:43:46
○	mok.plex1_migrated.ipsec	Available	2014-06-27 11:44:31
○	mok.small	Available	2014-06-27 11:44:53
○	savaData_r13_migrate	Available	2014-06-27 10:32:45
○	saveData	Available	2014-01-24 15:52:05
●	ShareDemo	Current	2014-06-21 07:08:03
○	tlspol	Available	2013-02-08 16:40:45
○	User2	Available	2013-01-30 18:22:42
○	V1R12_saveDataR114301more	Available	2014-06-27 10:33:15
○	V1R13	Available	2014-06-27 10:45:53
○	V2R1_saveDataR114301	Available	2014-06-27 10:34:04
○	V2R1_V1R13	Available	2014-06-27 10:34:22
○	V2R1_V1R13_saveDataR11	Available	2014-06-27 11:11:43

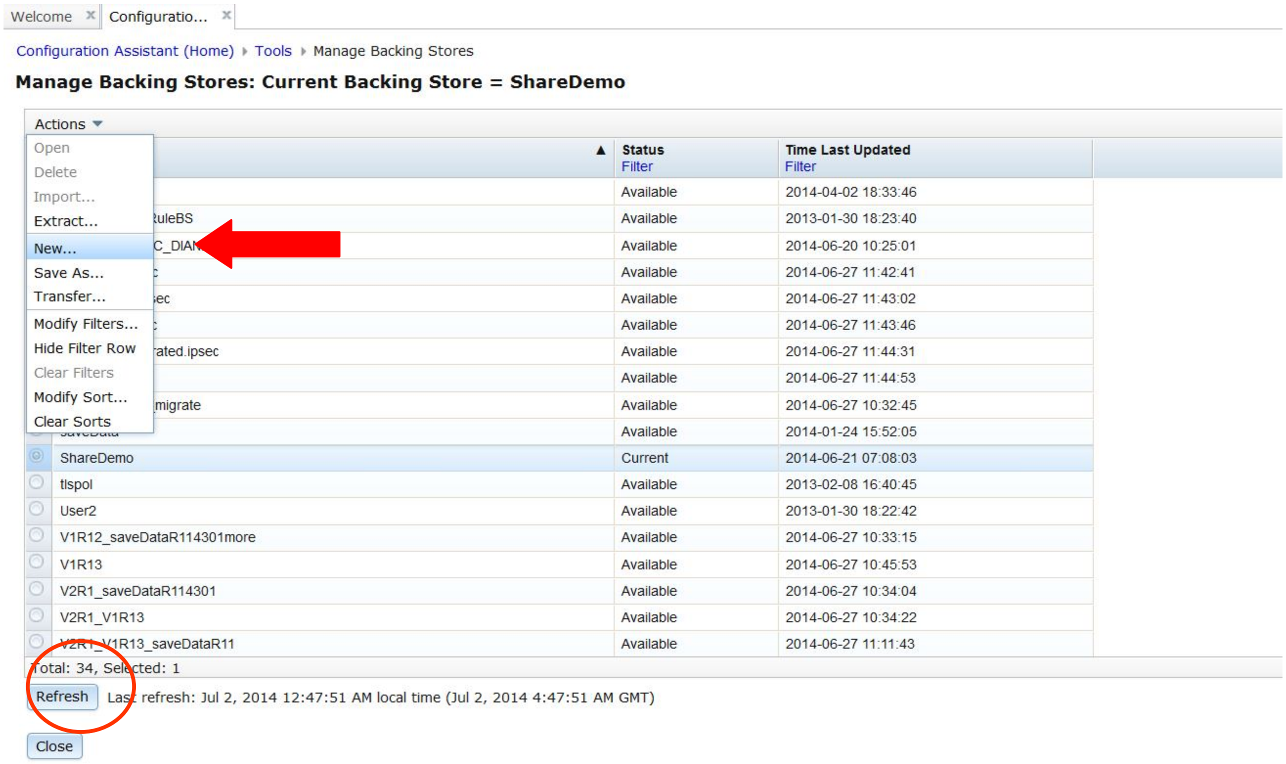
Total: 34, Selected: 1

Last refresh: Jul 2, 2014 12:47:51 AM local time (Jul 2, 2014 4:47:51 AM GMT)

View the tasks available from the Actions menu.

(Note: since this is a live system environment with other users, please don't complete any of the **Actions**. Thanks!)

Notice the **Refresh** button. You may want to refresh to update the list of backing stores to see if anything changed.



Manage Backing Stores: Current Backing Store = ShareDemo

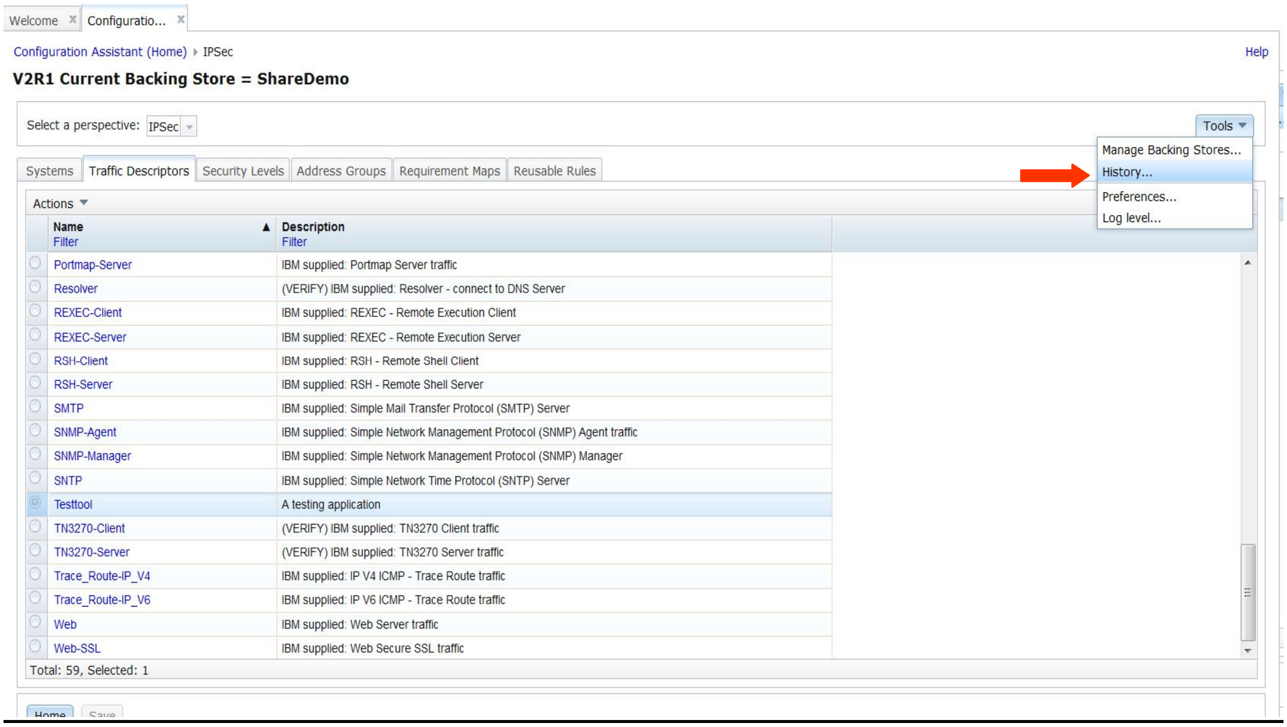
	▲	Status Filter	Time Last Updated Filter
		Available	2014-04-02 18:33:46
	RuleBS	Available	2013-01-30 18:23:40
	C_DIA	Available	2014-06-20 10:25:01
	c	Available	2014-06-27 11:42:41
	sec	Available	2014-06-27 11:43:02
	c	Available	2014-06-27 11:43:46
	rated.ipsec	Available	2014-06-27 11:44:31
		Available	2014-06-27 11:44:53
	migrate	Available	2014-06-27 10:32:45
	saveData	Available	2014-01-24 15:52:05
●	ShareDemo	Current	2014-06-21 07:08:03
○	tlspol	Available	2013-02-08 16:40:45
○	User2	Available	2013-01-30 18:22:42
○	V1R12_saveDataR114301more	Available	2014-06-27 10:33:15
○	V1R13	Available	2014-06-27 10:45:53
○	V2R1_saveDataR114301	Available	2014-06-27 10:34:04
○	V2R1_V1R13	Available	2014-06-27 10:34:22
○	V2R1_V1R13_saveDataR11	Available	2014-06-27 11:11:43

Total: 34, Selected: 1

Last refresh: Jul 2, 2014 12:47:51 AM local time (Jul 2, 2014 4:47:51 AM GMT)

Step 7.1c: History and Preferences

Click on “**History**”



Configuration Assistant (Home) ▸ IPSec

V2R1 Current Backing Store = ShareDemo

Select a perspective: IPSec

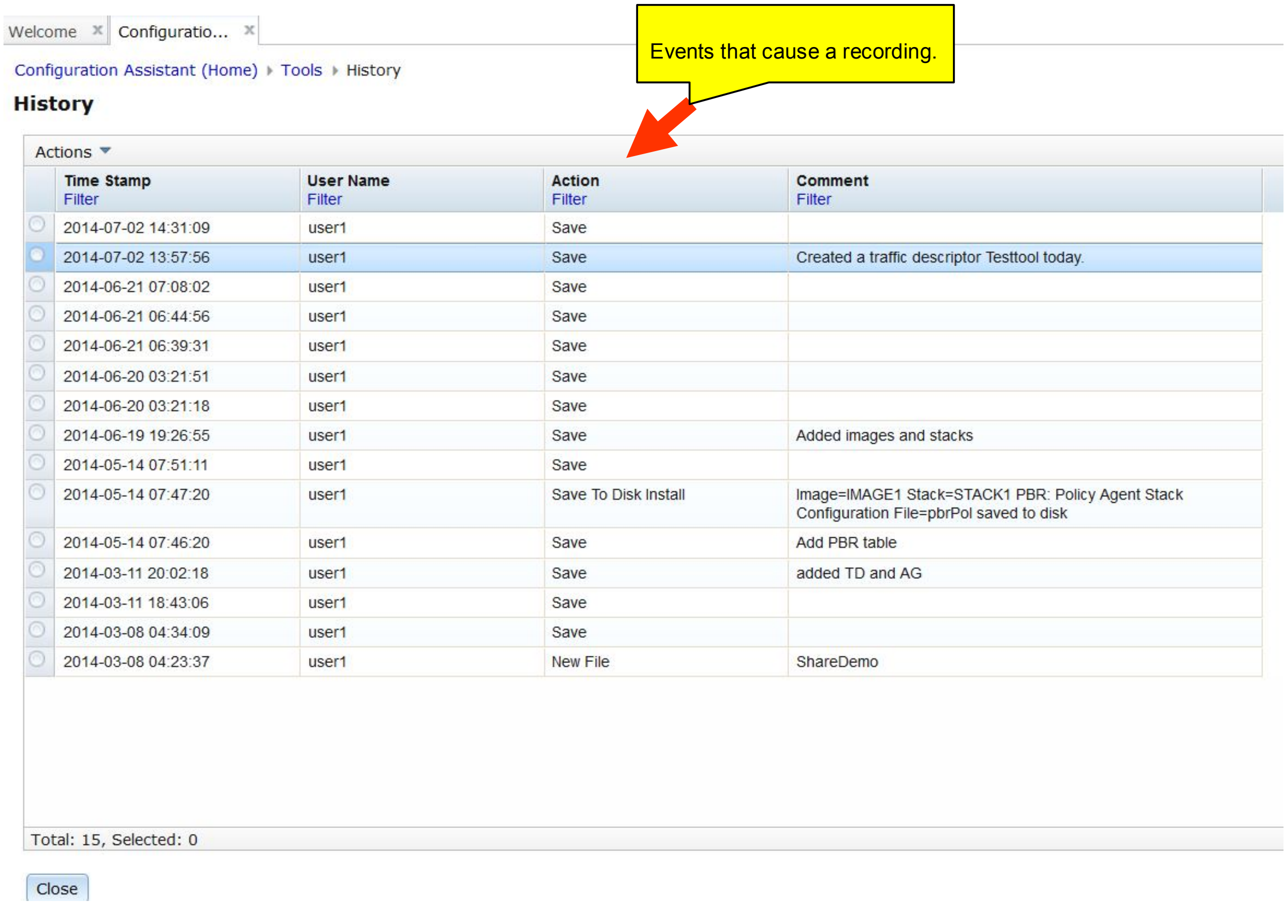
Name Filter	Description Filter
Portmap-Server	IBM supplied: Portmap Server traffic
Resolver	(VERIFY) IBM supplied: Resolver - connect to DNS Server
REXEC-Client	IBM supplied: REXEC - Remote Execution Client
REXEC-Server	IBM supplied: REXEC - Remote Execution Server
RSH-Client	IBM supplied: RSH - Remote Shell Client
RSH-Server	IBM supplied: RSH - Remote Shell Server
SMTP	IBM supplied: Simple Mail Transfer Protocol (SMTP) Server
SNMP-Agent	IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic
SNMP-Manager	IBM supplied: Simple Network Management Protocol (SNMP) Manager
SNTP	IBM supplied: Simple Network Time Protocol (SNTP) Server
Testtool	A testing application
TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
Trace_Route-IP_V4	IBM supplied: IP V4 ICMP - Trace Route traffic
Trace_Route-IP_V6	IBM supplied: IP V6 ICMP - Trace Route traffic
Web	IBM supplied: Web Server traffic
Web-SSL	IBM supplied: Web Secure SSL traffic

Total: 59, Selected: 1

The History selection takes you to the History Log. Here the events of your session are recorded. You can control whether you are prompted to comment for the event; however, the Configuration Assistant will automatically record certain events such as Saving the backing store or performing an **Install** automatically.

During your session certain events are important to record. Saves are important since this actually saves the resources you have created during your session to disk.

Notice that some events have no comment this is because the user did not comment, but the Config Assistant still recorded the event.



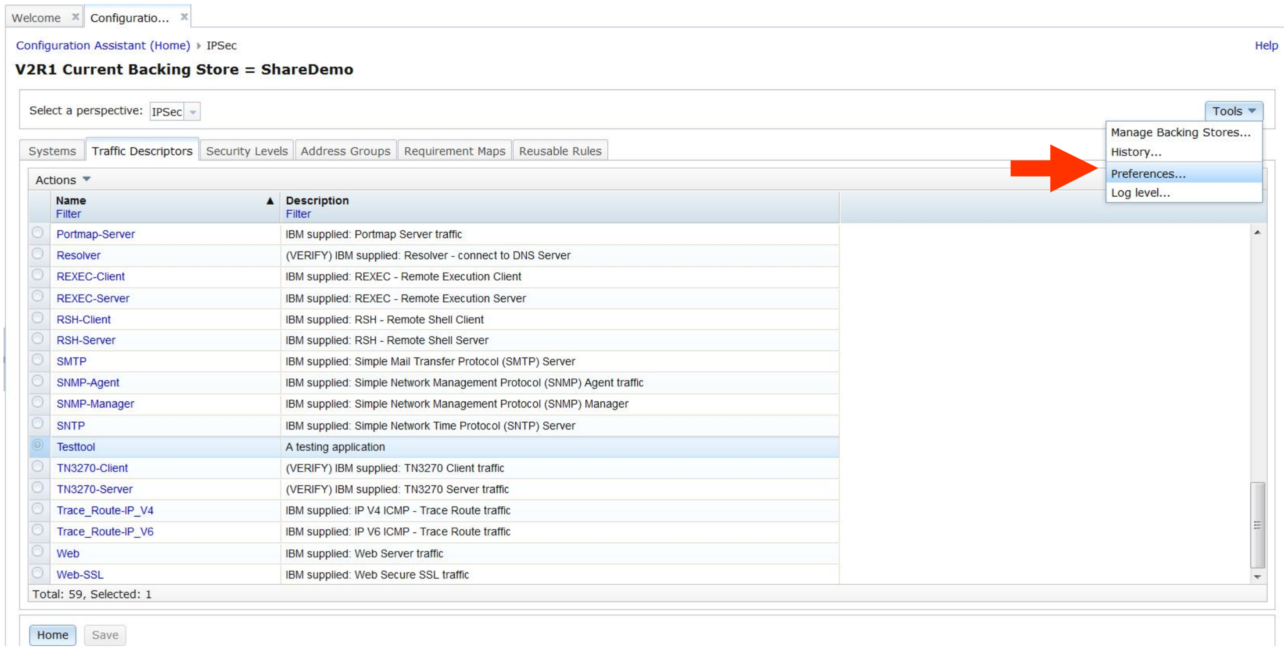
Events that cause a recording.

History

Time Stamp	User Name	Action	Comment
2014-07-02 14:31:09	user1	Save	
2014-07-02 13:57:56	user1	Save	Created a traffic descriptor Testtool today.
2014-06-21 07:08:02	user1	Save	
2014-06-21 06:44:56	user1	Save	
2014-06-21 06:39:31	user1	Save	
2014-06-20 03:21:51	user1	Save	
2014-06-20 03:21:18	user1	Save	
2014-06-19 19:26:55	user1	Save	Added images and stacks
2014-05-14 07:51:11	user1	Save	
2014-05-14 07:47:20	user1	Save To Disk Install	Image=IMAGE1 Stack=STACK1 PBR: Policy Agent Stack Configuration File=pbrPol saved to disk
2014-05-14 07:46:20	user1	Save	Add PBR table
2014-03-11 20:02:18	user1	Save	added TD and AG
2014-03-11 18:43:06	user1	Save	
2014-03-08 04:34:09	user1	Save	
2014-03-08 04:23:37	user1	New File	ShareDemo

Total: 15, Selected: 0

Next, select “Preferences”



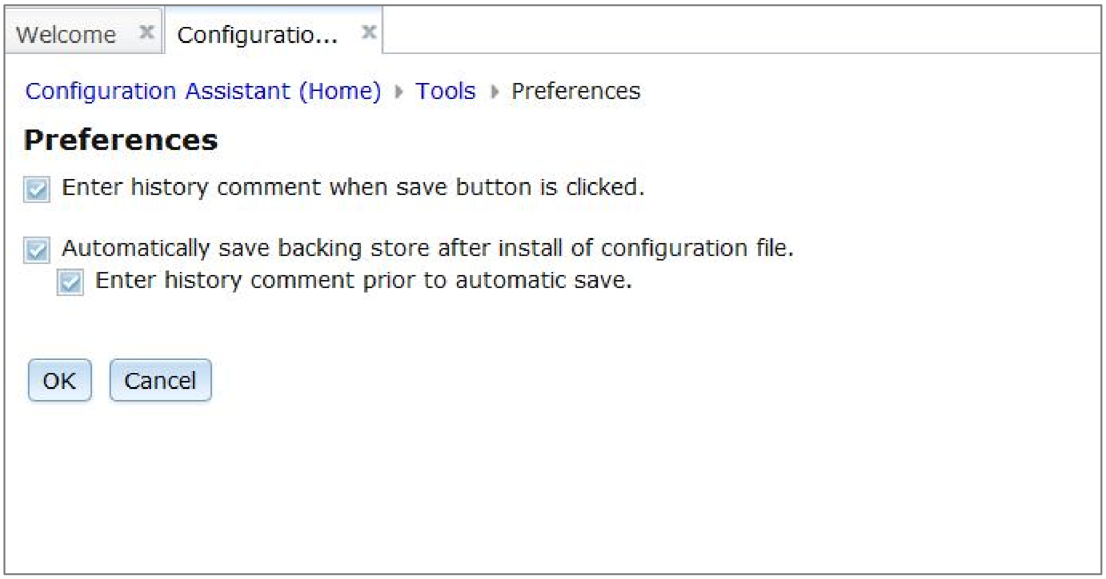
V2R1 Current Backing Store = ShareDemo

	Name Filter	Description Filter
○	Portmap-Server	IBM supplied: Portmap Server traffic
○	Resolver	(VERIFY) IBM supplied: Resolver - connect to DNS Server
○	REXEC-Client	IBM supplied: REXEC - Remote Execution Client
○	REXEC-Server	IBM supplied: REXEC - Remote Execution Server
○	RSH-Client	IBM supplied: RSH - Remote Shell Client
○	RSH-Server	IBM supplied: RSH - Remote Shell Server
○	SMTP	IBM supplied: Simple Mail Transfer Protocol (SMTP) Server
○	SNMP-Agent	IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic
○	SNMP-Manager	IBM supplied: Simple Network Management Protocol (SNMP) Manager
○	SNTP	IBM supplied: Simple Network Time Protocol (SNTP) Server
●	Testtool	A testing application
○	TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
○	TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
○	Trace_Route-IP_V4	IBM supplied: IP V4 ICMP - Trace Route traffic
○	Trace_Route-IP_V6	IBM supplied: IP V6 ICMP - Trace Route traffic
○	Web	IBM supplied: Web Server traffic
○	Web-SSL	IBM supplied: Web Secure SSL traffic

Total: 59, Selected: 1

Preferences allow you to control when you receive the prompt for recording a comment to the History Log. For example, if you don't want to enter comments then you may want to disable the comment settings.

Take a moment to view the options.



Preferences

☑ Enter history comment when save button is clicked.

☑ Automatically save backing store after install of configuration file.

☑ Enter history comment prior to automatic save.

End of exercise

This completes the prepared lab session tasks. Please feel free to explore other features of the Configuration Assistant.

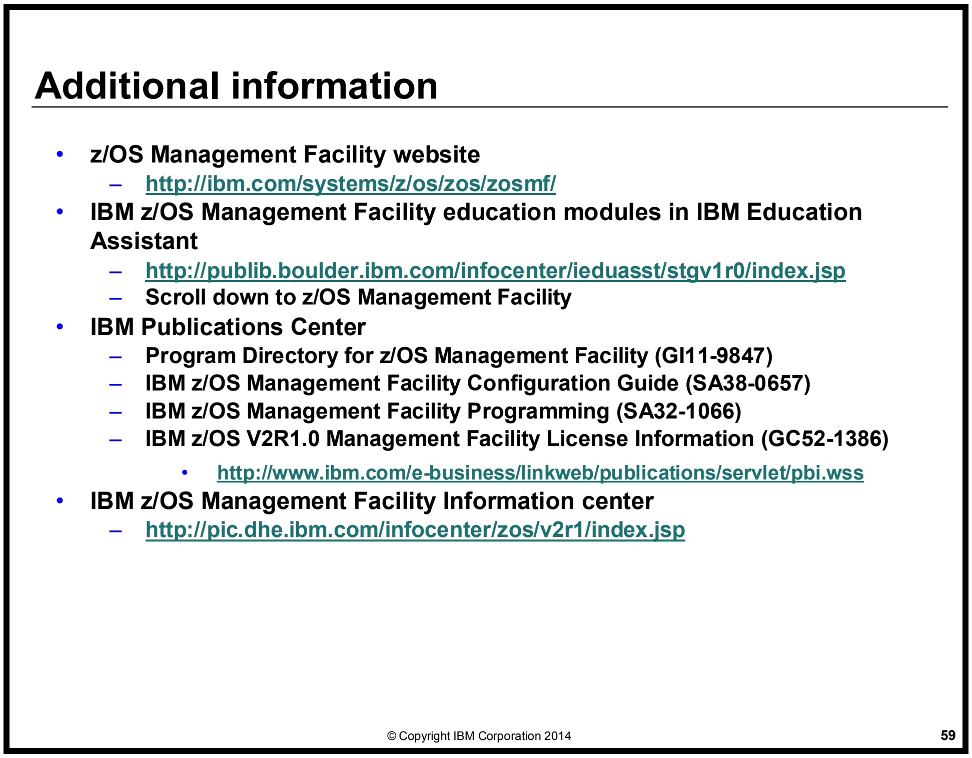
We are open to comments for improving the user experience provided by the Configuration Assistant.

Thank You

© Copyright IBM Corporation 2014

58

Additional Information



Additional information

- z/OS Management Facility website
  - http://ibm.com/systems/z/os/zos/zosmf/
- IBM z/OS Management Facility education modules in IBM Education Assistant
  - http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp
  - Scroll down to z/OS Management Facility
- IBM Publications Center
  - Program Directory for z/OS Management Facility (GI11-9847)
  - IBM z/OS Management Facility Configuration Guide (SA38-0657)
  - IBM z/OS Management Facility Programming (SA32-1066)
  - IBM z/OS V2R1.0 Management Facility License Information (GC52-1386)
    - http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss
- IBM z/OS Management Facility Information center
  - http://pic.dhe.ibm.com/infocenter/zos/v2r1/index.jsp