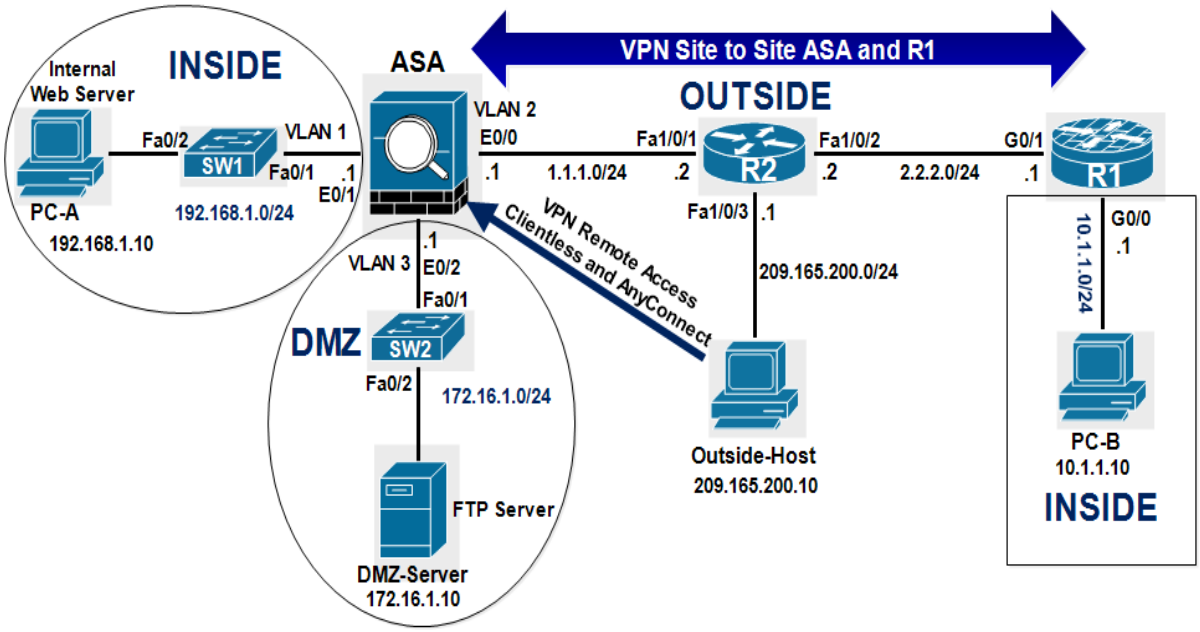
Cisco Security Practice Labs

Redouane MEDDANE

Table of Contents

Lab 1: VPNs Site to Site, Remote Access and ZBF



Part-1: Basic configuration of all routers and Cisco ASA:

On R1:

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shut
```

```
R1(config-if)#interface GigabitEthernet0/1
R1(config-if)# ip address 2.2.2.1 255.255.255.0
R1(config-if)#no shut
```

```
R1(config-if)#ip route 0.0.0.0 0.0.0.0 2.2.2.2
```

On R2:

```
R2(config)#interface FastEthernet1/0/1
R2(config-if)# no switchport
R2(config-if)# ip address 1.1.1.2 255.255.255.0
```

```
R2(config-if)#interface FastEthernet1/0/2
R2(config-if)# no switchport
R2(config-if)# ip address 2.2.2.2 255.255.255.0
```

```
R2(config-if)#interface FastEthernet1/0/3
R2(config-if)# no switchport
R2(config-if)# ip address 209.165.200.1 255.255.255.0
```

```
R2(config)#ip route 10.1.1.0 255.255.255.0 2.2.2.1
R2(config)#ip route 172.16.1.0 255.255.255.0 1.1.1.1
R2(config)#ip route 192.168.1.0 255.255.255.0 1.1.1.1
```

On ASA:

```
ciscoasa(config)# interface Vlan1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
ciscoasa(config-if)#interface Vlan2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 1.1.1.1 255.255.255.0
```

```
ciscoasa(config-if)#interface Vlan3
ciscoasa(config-if)#nameif DMZ
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0
```

```
ciscoasa(config-if)#int e0/0
ciscoasa(config-if)#switc mode access
ciscoasa(config-if)#switch acc vlan 2
ciscoasa(config-if)#int e0/1
ciscoasa(config-if)#switc mode access
ciscoasa(config-if)#switch acc vlan 1
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switc mode access
ciscoasa(config-if)#switch acc vlan 3
```

Configure a static default route for the ASA:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 1.1.1.2
```

Verify the vlan interfaces configuration:

```
ciscoasa# show run int vlan 1
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
ciscoasa#
ciscoasa# show run int vlan 2
!
interface Vlan2
nameif outside
security-level 0
ip address 1.1.1.1 255.255.255.0
ciscoasa#
ciscoasa# show run int vlan 3
!
interface Vlan3
nameif DMZ
security-level 50
ip address 172.16.1.1 255.255.255.0
ciscoasa#
```

Display the VLANs and port assignments on the ASA using the show switch vlan command:

```
ciscoasa(config)# show switch vlan
VLAN Name                            Status    Ports
---- ------------------------------- --------- -----------------------------
1    insideupEt0/1, Et0/3, Et0/4, Et0/5
                                               Et0/6, Et0/7
2    outsideupEt0/0
3    DMZupEt0/2
ciscoasa(config)#
```

Configure ASDM access to the ASA.
Allow HTTPS connections from any host on the inside network (192.168.1.0/24).

```
ciscoasa(config)# username admin password cisco
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
ciscoasa(config)# aaa authentication http console LOCAL
```

Part-2: Modify the default MPF application inspection global service policy

For application layer inspection, as well as other advanced options, the Cisco MPF is available on ASAs. Cisco MPF uses three configuration objects to define modular, object-oriented, and hierarchical policies:

1. **Class maps - Define a match criterion.**
2. **Policy maps - Associate actions to the match criteria.**
3. **Service policies - Attach the policy map to an interface, or globally to all interfaces of the appliance.**

Display the default MPF policy map that performs the inspection on inside-to-outside traffic. Only traffic that was initiated from the inside is allowed back in to the outside interface. Notice that the ICMP protocol is missing.

```
ciscoasa# show run | begin class
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512

policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

Add the inspection of ICMP traffic to the policy map list using the following commands:

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

You can use the fixup protocol icmp command to add inspection of ICMP traffic:

```
ciscoasa(config)# fixup protocol icmp
INFO: converting 'fixup protocol icmp ' to MPF commands
ciscoasa(config)#
```

Display the default MPF polich map to verify ICMP is now listed in the inspection rules.

```
ciscoasa(config-pmap-c)# show run policy-map
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
```

Part-3: Configure a Synchronized Time Source Using NTP

R1 will be the master NTP clock source for R2 and ASA.
1-Configure NTP authentication by defining the authentication key number 1 with md5 hashing, and a password of ntp-pass.
2-Configure the trusted key that will be used for authentication on R2.
3-Enable the NTP authentication feature on R2.
4-Configure R2 as the NTP master using the ntp master stratum-number command in global configuration mode. The stratum number indicates the distance from the original source. For this lab, use a stratum number of 4 on R1. When a device learns the time from an NTP source, its stratum number becomes one greater than the stratum number of its source.

On R1:

```
R1(config)#ntp master 4
R1(config)#ntp authenticate
R1(config)#ntp authentication-key 1 md5 ntp-pass
R1(config)#ntp trusted-key 1
```

Configure R2 and ASA as NTP clients:

On R2:

```
R2(config)#ntp authenticate
R2(config)#ntp server 2.2.2.1
R2(config)#ntp authentication-key 1 md5 ntp-pass
R2(config)#ntp trusted-key 1
```

On ASA:

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp server 1.1.1.2
ciscoasa(config)# ntp authentication-key 1 md5 ntp-pass
ciscoasa(config)# ntp trusted-key 1
```

Use the show ntp associations command to verify that R2 and ASA have made an association with R1. Use the show ntp status to verify that the clock is synchronized:

On R2:

```
R2#show ntp associ

address         ref clock     st  when  poll reach  delay  offset    disp
*~2.2.2.1          127.127.1.1       4    33    64    1     1.7    0.21  15875.
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R2#
```

```
R2#show ntp status
Clock is synchronized, stratum 5, reference is 2.2.2.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**18
reference time is DB6698DF.C42C0F69 (09:41:51.766 UTC Tue Aug 23 2016)
clock offset is 0.2111 msec, root delay is 1.72 msec
root dispersion is 15875.60 msec, peer dispersion is 15875.02 msec
R2#
```

On ASA:

```
ciscoasa# show ntp asso
address         ref clock     st  when  poll reach  delay  offset    disp
*~1.1.1.22.2.2.1           5   123   128  377     0.9   35.82    18.8
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
ciscoasa#
```

```
ciscoasa# show ntp status
Clock is synchronized, stratum 6, reference is 1.1.1.2
nominal freq is 99.9984 Hz, actual freq is 99.9974 Hz, precision is 2**6
reference time is db66b113.14934bb0 (11:25:07.080 UTC Tue Aug 23 2016)
clock offset is 35.8157 msec, root delay is 1.86 msec
root dispersion is 55.18 msec, peer dispersion is 18.75 msec
ciscoasa#
```

Part-4: Configure a Zone-Based Firewall on R1

Create the INSIDE and OUTSIDE security zones.

```
R1(config)#zone security INSIDE
R1(config)#zone security OUTSIDE
```

Create an inspect class-map to match the traffic to be allowed from the INSIDE zone to the OUTSIDE zone. Because we trust the INSIDE zone, we allow all the main protocols. Use the match-any keyword to instruct the router to use the OR Logic. Match for TCP, UDP, or ICMP packets:

```
R1(config)# class-map type inspect match-any INSIDE-TRAFFIC
R1(config-cmap)# match protocol tcp
R1(config-cmap)# match protocol udp
R1(config-cmap)# match protocol icmp
```

Create an inspect policy-map named IN-OUT-POLICY. Bind the INSIDE-TRAFFIC class-map to the policy-map. All packets matched by the INSIDE-TRAFFIC class-map will be inspected:

```
R1(config-cmap)#policy-map type inspect IN-OUT-POLICY
R1(config-pmap)#class type inspect INSIDE-TRAFFIC
R1(config-pmap-c)#inspect
```

Create a zone-pair called IN-TO-OUT that allows traffic initiated from the INSIDE network to the OUTSIDE network, in other words from the INSIDE zone to the OUTSIDE zone and apply the policy-map to the zone-pair:

```
R1(config)# zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
R1(config-sec-zone-pair)#service-policy type inspect IN-OUT-POLICY
```

Assign R1's G0/0 interface to the INSIDE security zone and the G0/1 interface to the OUTSIDE security zone:

```
R1(config)# interface g0/0
R1(config-if)# zone-member security INSIDE
R1(config)# interface g0/1
R1(config-if)# zone-member security OUTSIDE
```

Part-5: On ASA configure address translation using PAT for the inside network

The inside network requires PAT when routed to the outside interface, the hosts in the inside network share the same public IP address 1.1.1.1 which is the IP address of the outside interface. Network objects are used to configure all forms of NAT. A network object is created, and it is within this object that NAT is configured. The network object INSIDE-NET is used to translate the inside network addresses (192.168.1.0/24) to the global address of the outside ASA interface. This type of object configuration is called Auto-NAT.

```
ciscoasa(config)# object network INSIDE-NET
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

Part-6: Configure static NAT and ACL for the DMZ server

Configure a network object named DMZ-SRV and assign it the static IP address of the DMZ server (172.16.1.10). While in object definition mode, use the nat command to specify that this object is used to translate a DMZ address to an outside address using static NAT, and specify a public translated address of 1.1.1.10.

```
ciscoasa(config)# object network DMZ-SRV
ciscoasa(config-network-object)# host 172.16.1.10
ciscoasa(config-network-object)# nat (DMZ,outside) static 1.1.1.10
```

Verify the object networks:

```
ciscoasa# show run object
object network INSIDE-NET
subnet 192.168.1.0 255.255.255.0
object network DMZ-SRV
host 172.16.1.10
ciscoasa#
```

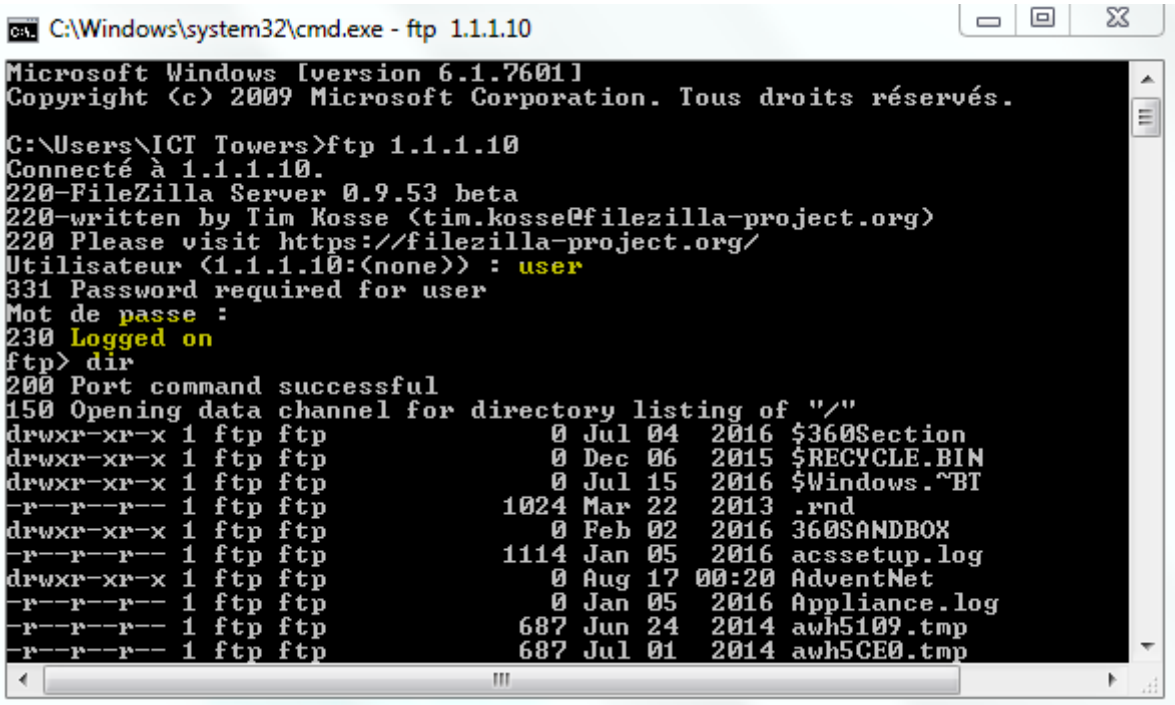
```
ciscoasa# show run nat
!
object network INSIDE-NET
nat (inside,outside) dynamic interface
object network DMZ-SRV
nat (DMZ,outside) static 1.1.1.10
ciscoasa#
```

Configure an ACL to allow access to the DMZ server from the Internet.
Configure a named access list (DMZ-ACL) that permits any IP protocol from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA outside interface in the IN direction.

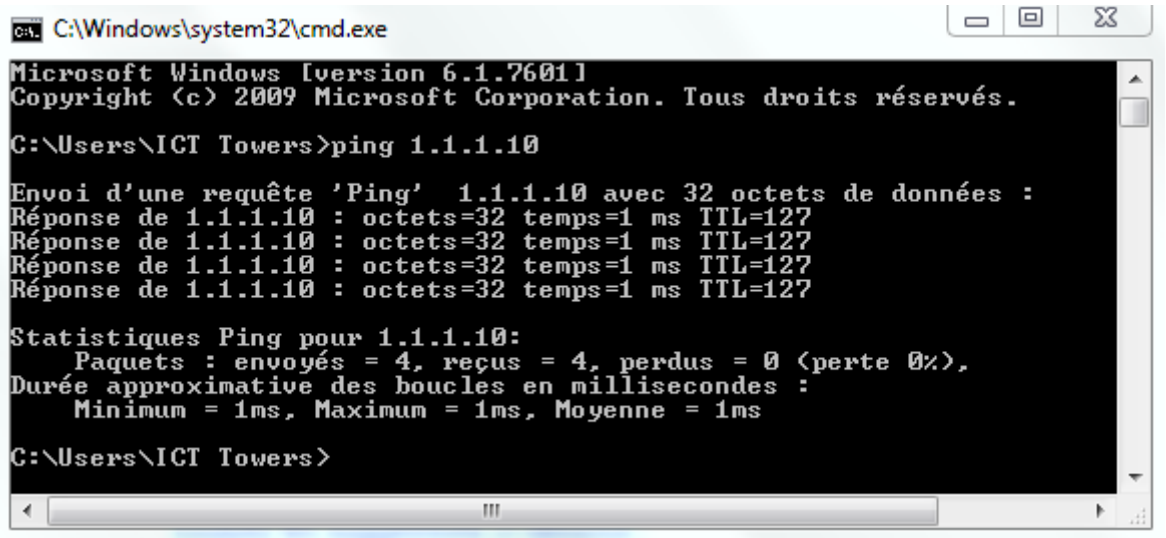
```
ciscoasa(config)# access-list DMZ-ACL ext perm icmp any host 172.16.1.10
ciscoasa(config)# access-list DMZ-ACL ext perm tcp any host 172.16.1.10eq ftp
ciscoasa(config)# access-list DMZ-ACL ext perm tcp any host 172.16.1.10eq ftp-data
ciscoasa(config)# access-group DMZ-ACL in interface outside
```

Test access to the DMZ server using FTP from the outside network.

From Outside Host access the FTP files located in the DMZ Server, the access should be successful:



From Outside Host, ping the IP address of the static NAT public server address (1.1.1.10). The pings should be successful.



Part-7: On R1 configure address translation using PAT for the inside network 10.1.1.0/24

The inside network requires PAT when routed to the outside interface, the hosts in the inside network share the same public IP address 2.2.2.1 which is the IP address of R1's G0/1 interface:

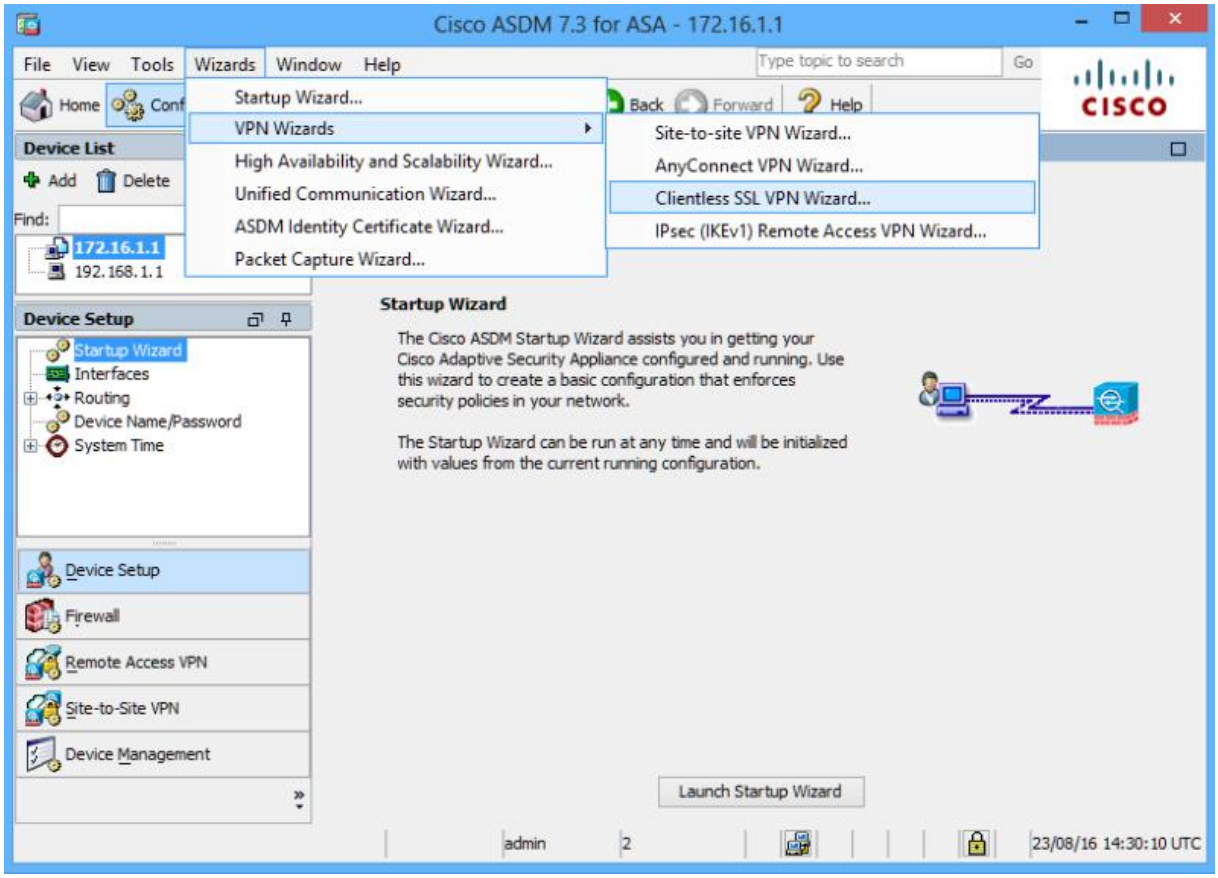
Note: Configure NAT exemption between the inside network of R1 (10.1.1.0/24) and the inside network of ASA (192.168.1.0/24) for VPN Site to Site purpose.

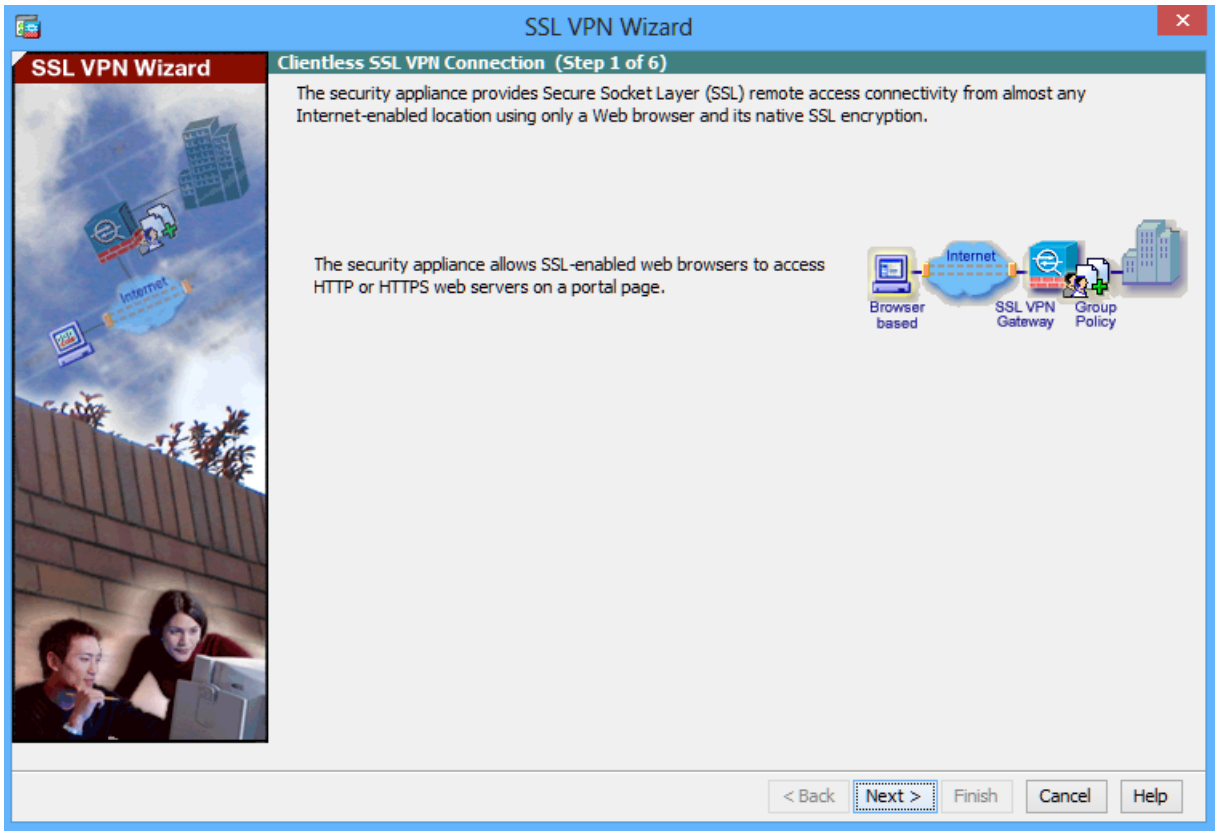
```
R1(config)#access-list 100 deny ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#access-list 100 permit ip 10.1.1.0 0.0.0.255 any
```

```
R1(config)#ip nat inside source list 100 interface g0/1 overload
R1(config)#int g0/0
R1(config-if)#ip nat inside
R1(config-if)#int g0/1
R1(config-if)#ip nat outside
```

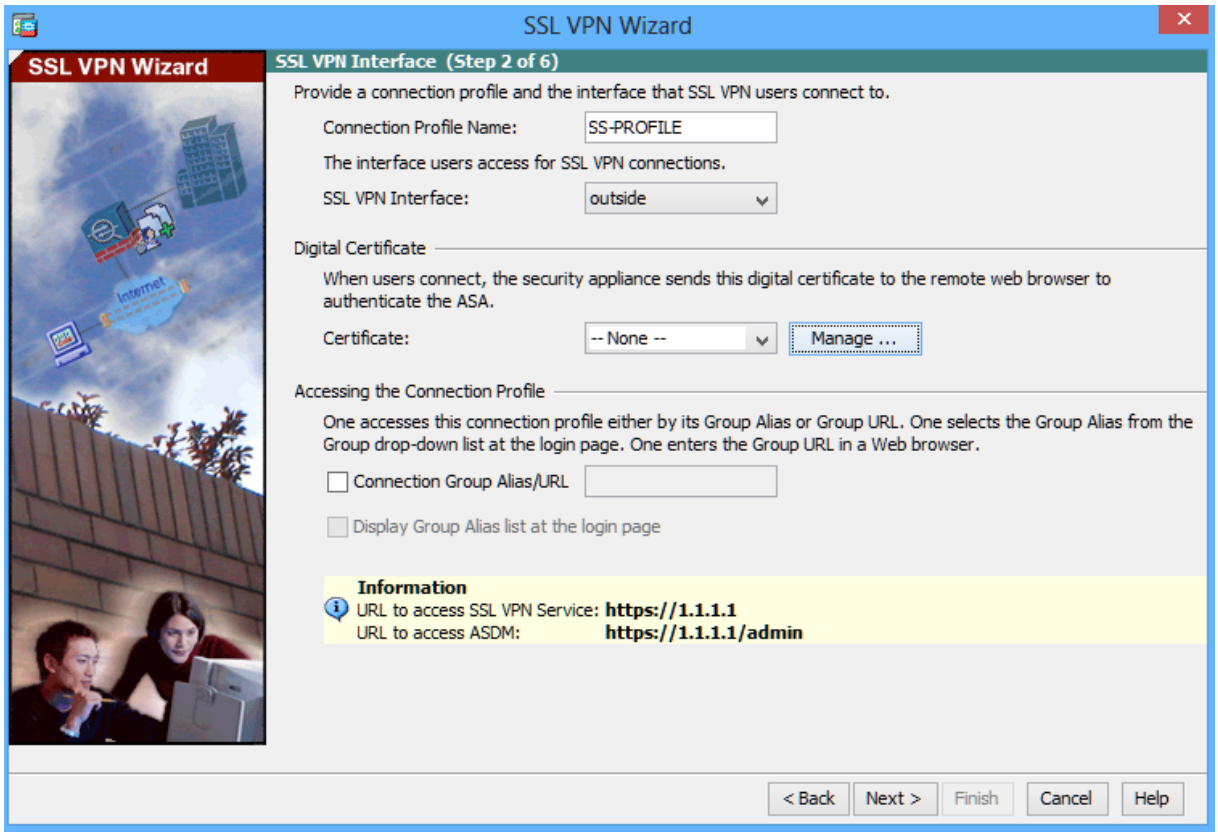
Part-8: Configure ASA Clientless SSL VPN Remote Access

Using ASDM: click Wizards > VPN Wizards > Clientless SSL VPN wizard. The SSL VPN wizard Clientless SSL VPN Connection screen displays.

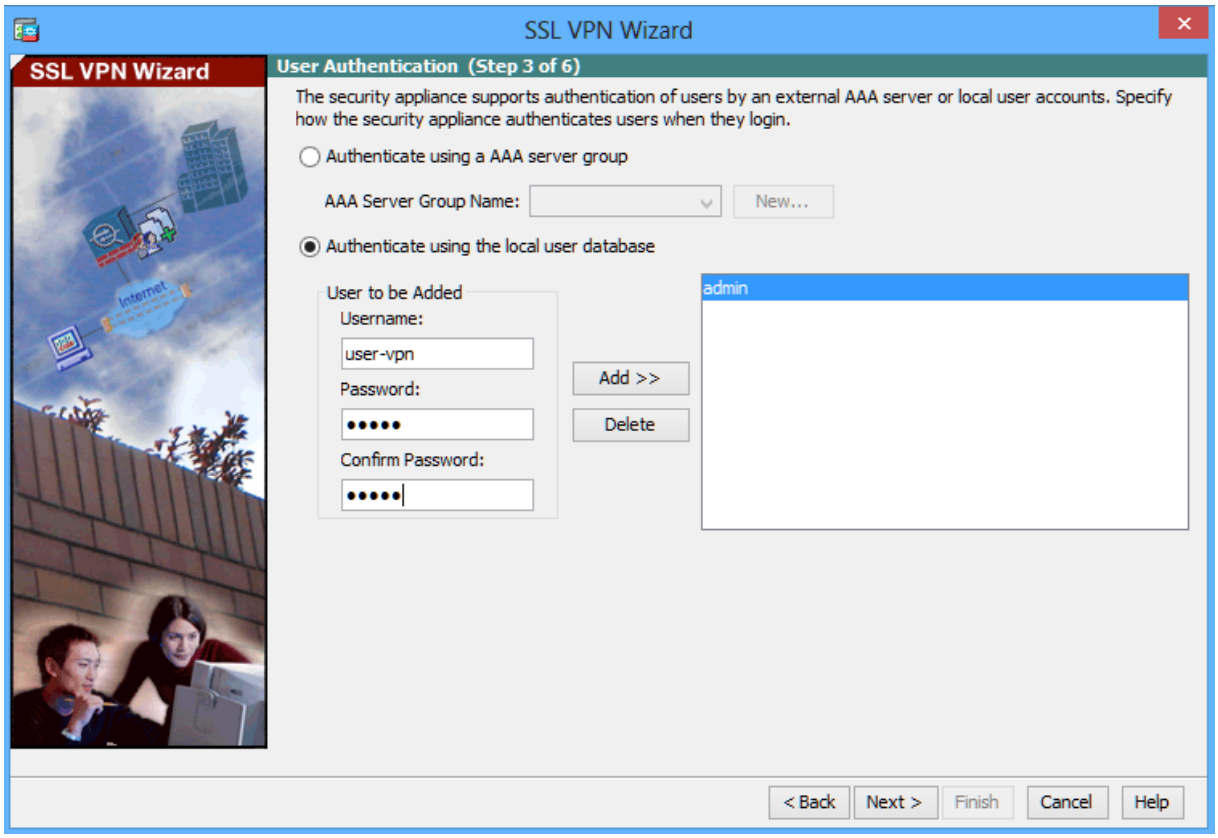


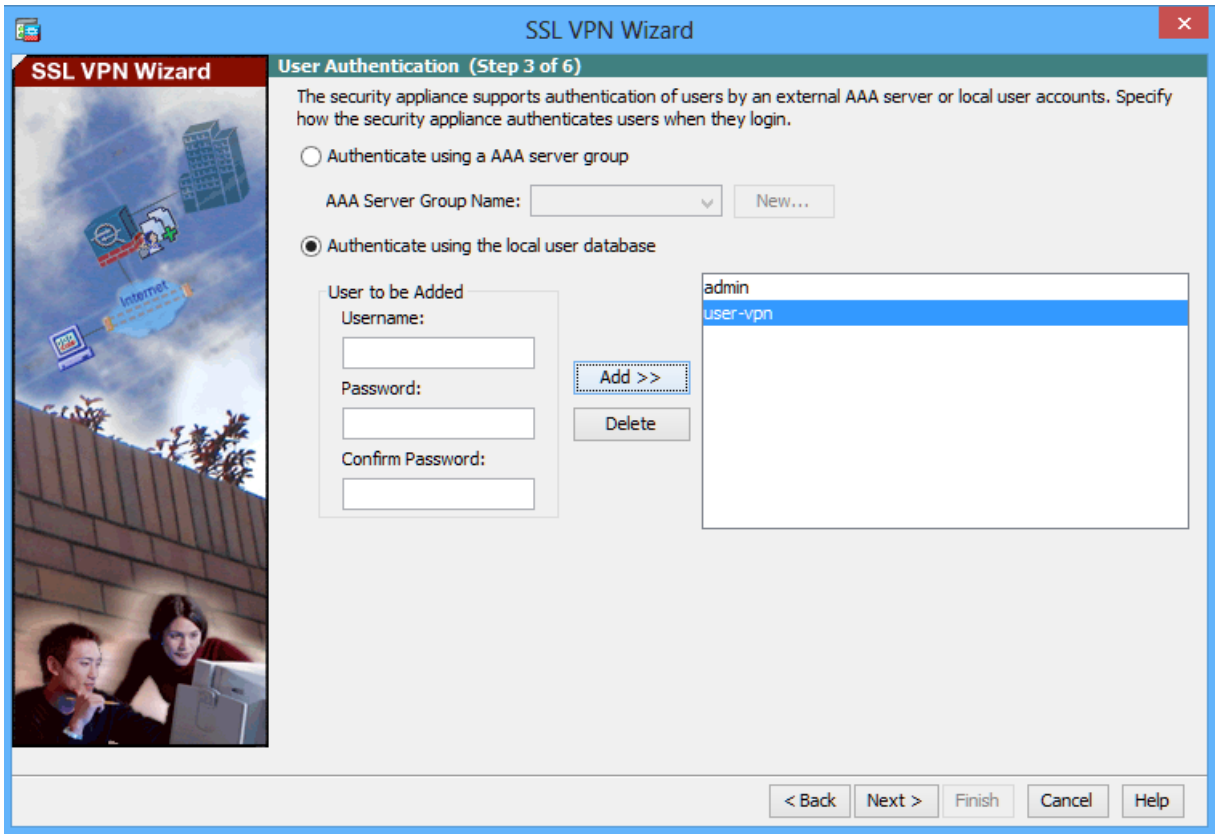


Configure the SSL VPN user interface.
On the SSL VPN Interface screen, configure SS-PROFILE as the Connection Profile Name and specify outside as the interface to which outside users will connect.

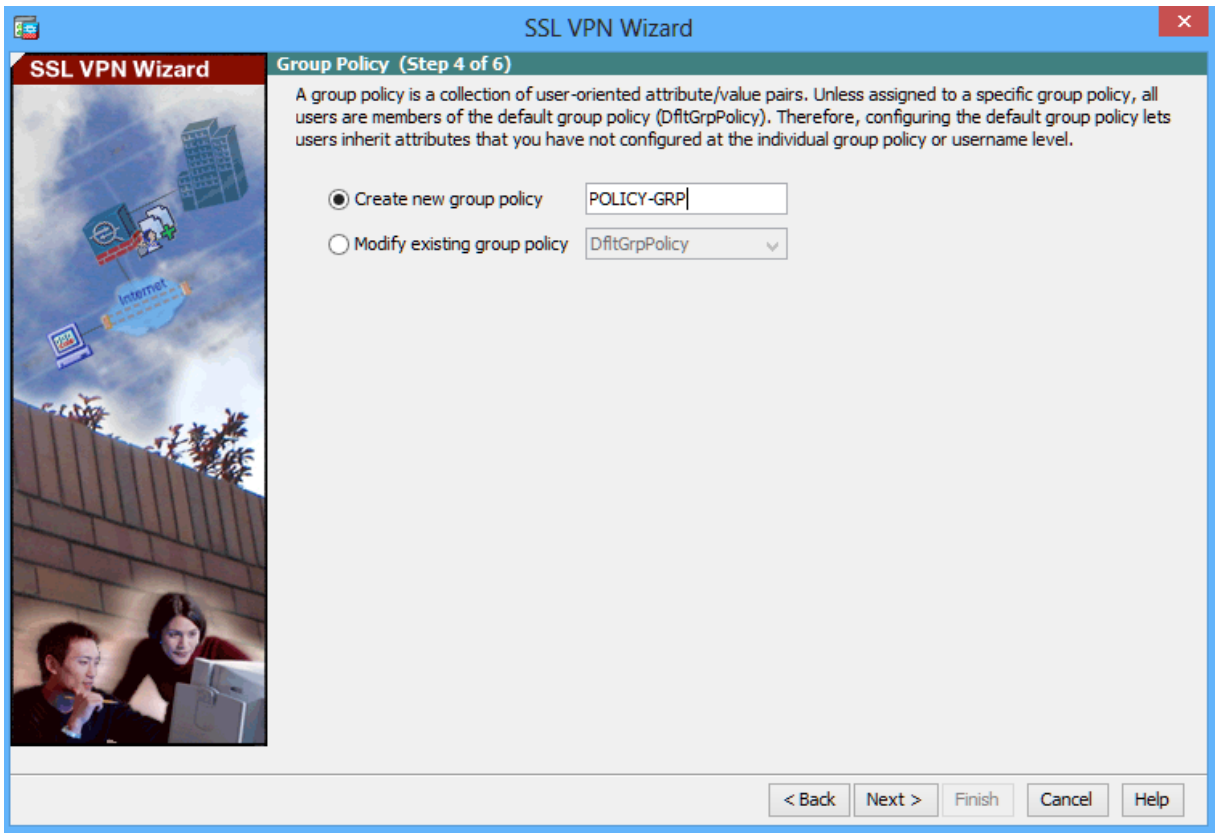


Configure AAA user authentication.
On the User Authentication screen, click Authenticate Using the Local User Database and enter the username user-vpn with a password of cisco. Click Add to create the new user.

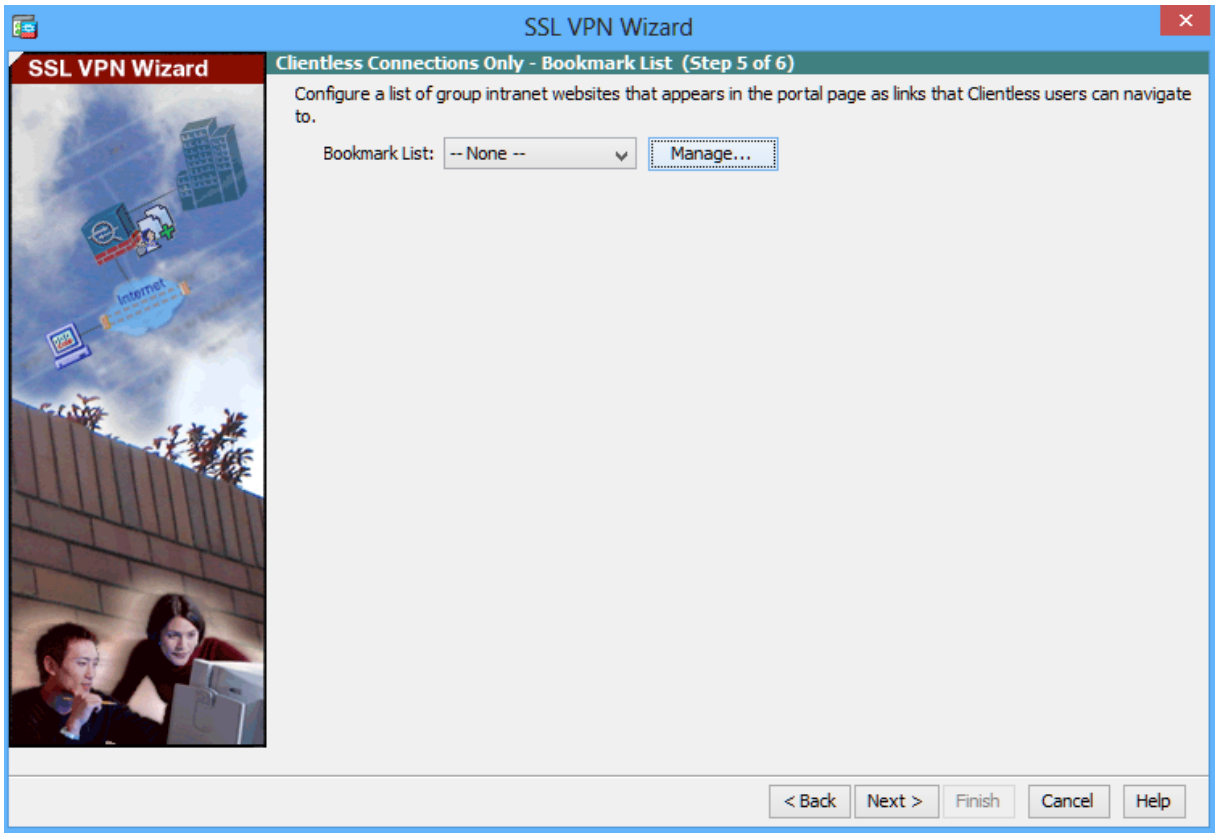




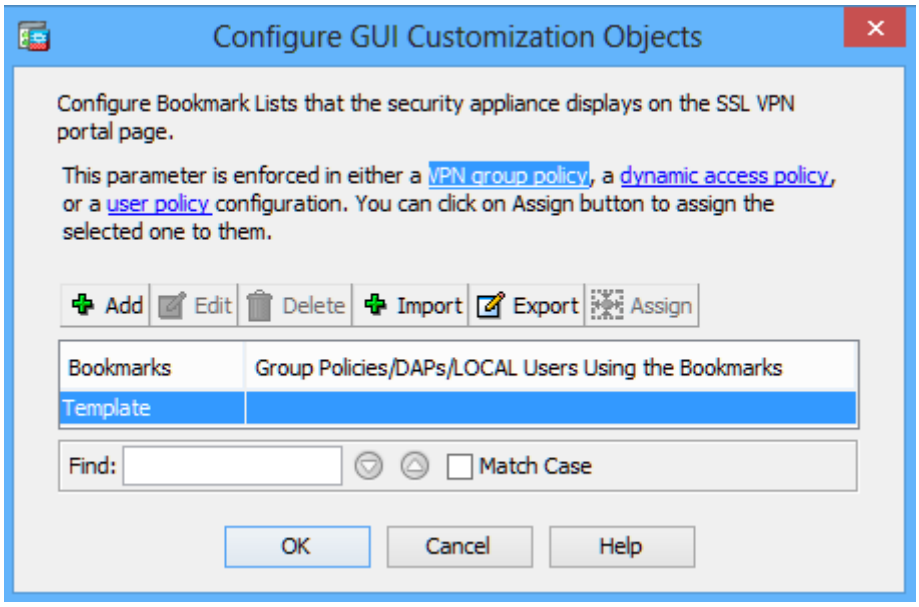
Configure the VPN group policy.
On the Group Policy screen, create a new group policy named POLICY-GRP.

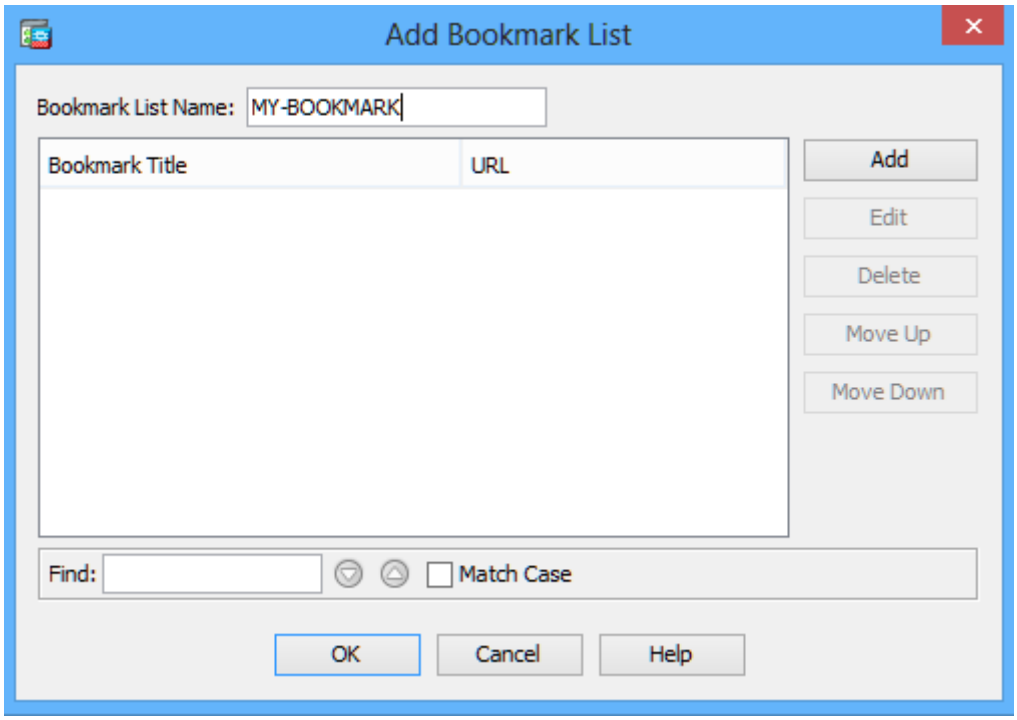


Configure the bookmark list.
From the Clientless Connections Only – Bookmark List screen, click Manage to create an HTTP server bookmark in the bookmark list.

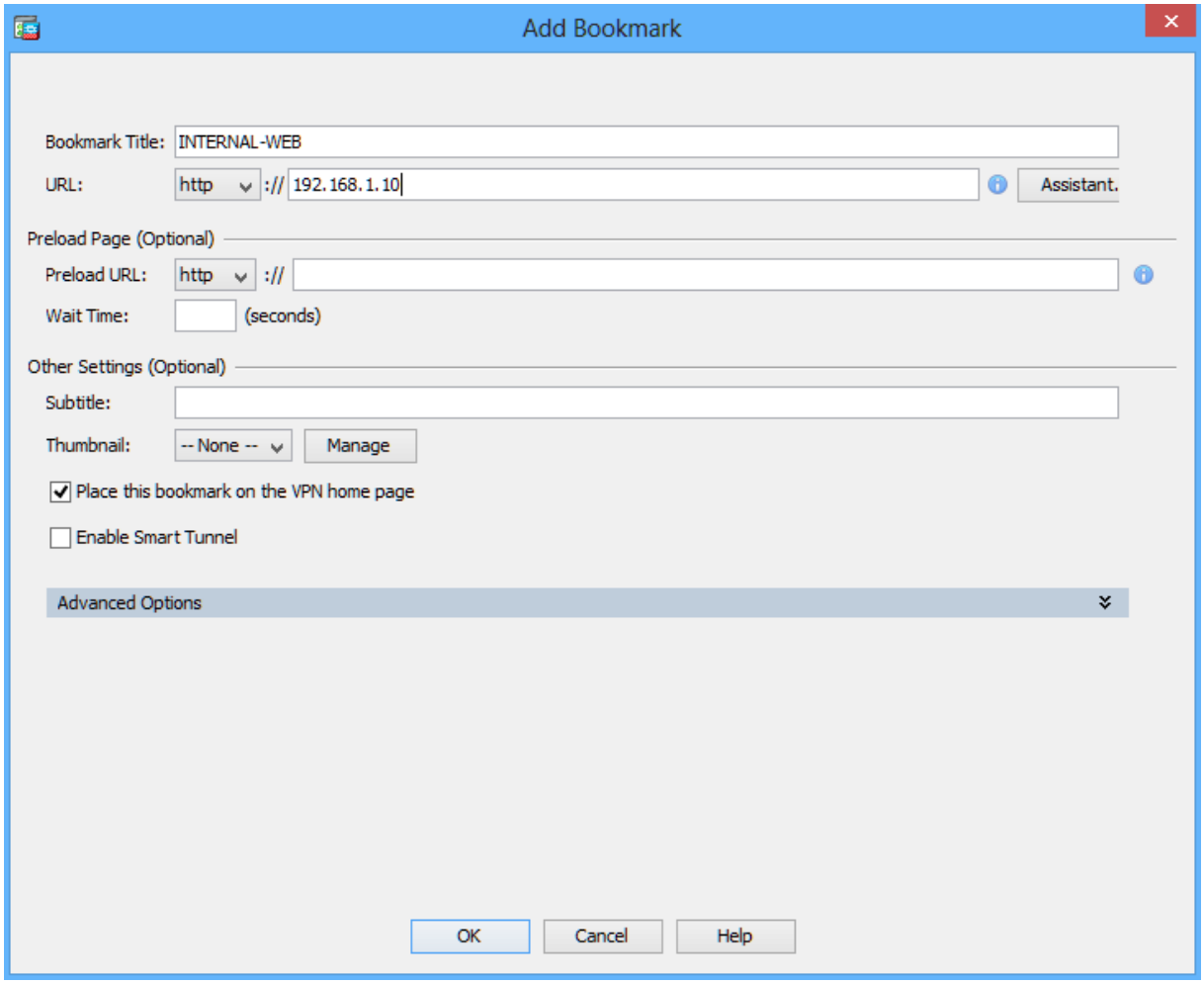


In the Configure GUI Customization Objects window, click Add to open the Add Bookmark List window. Name the list MY-BOOKMARK.

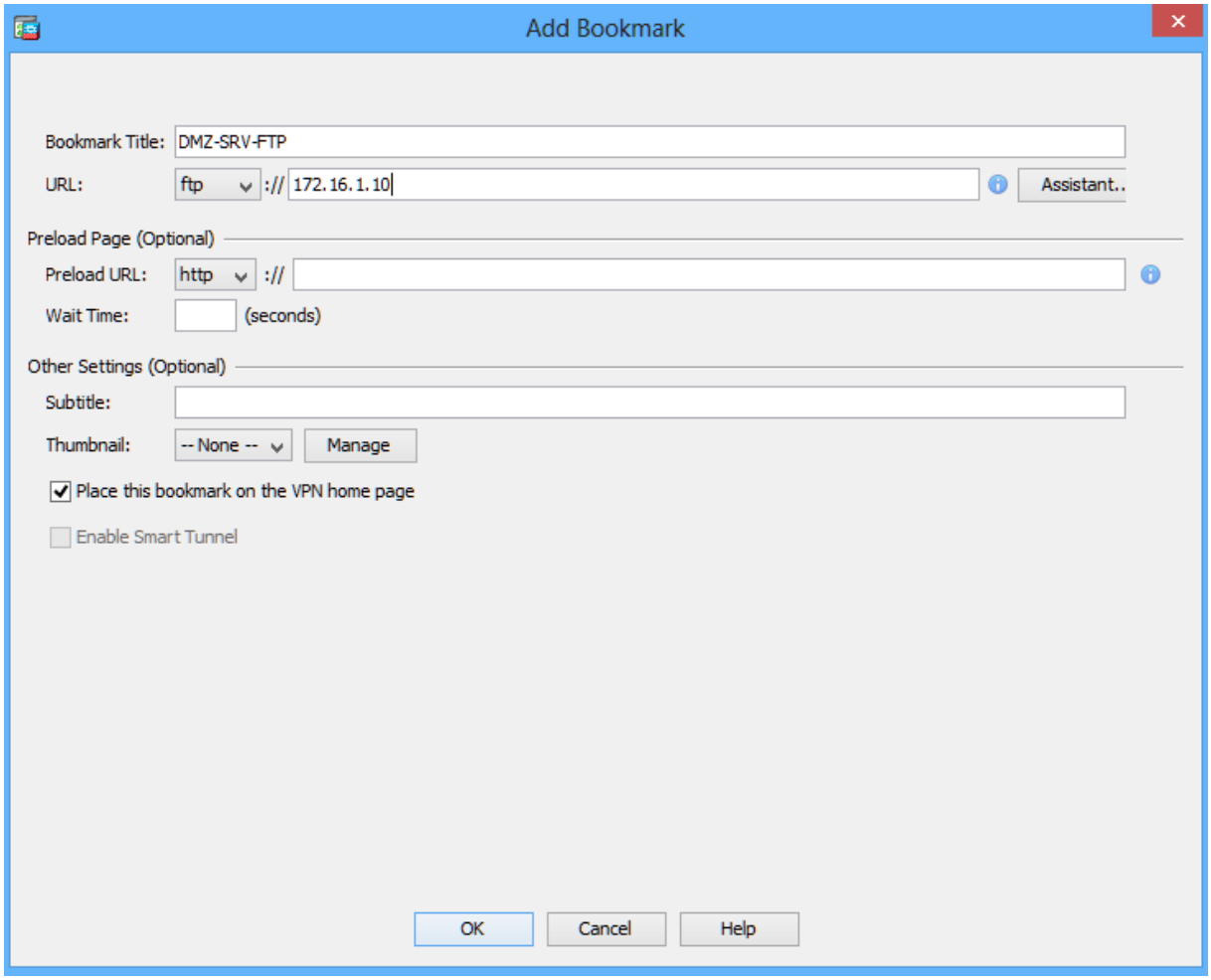


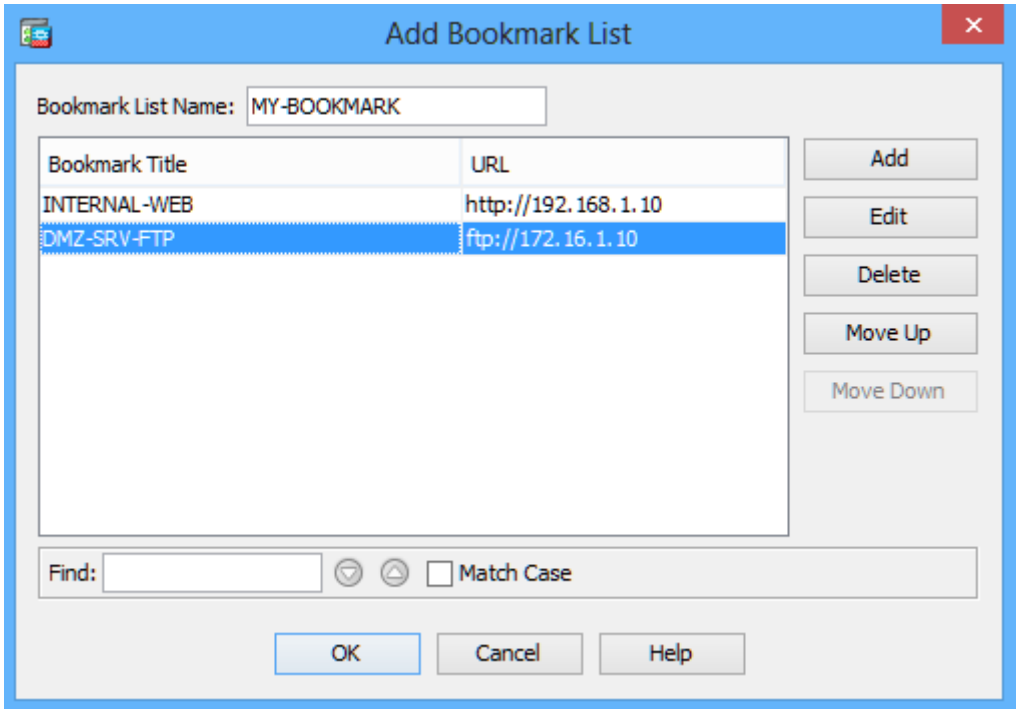


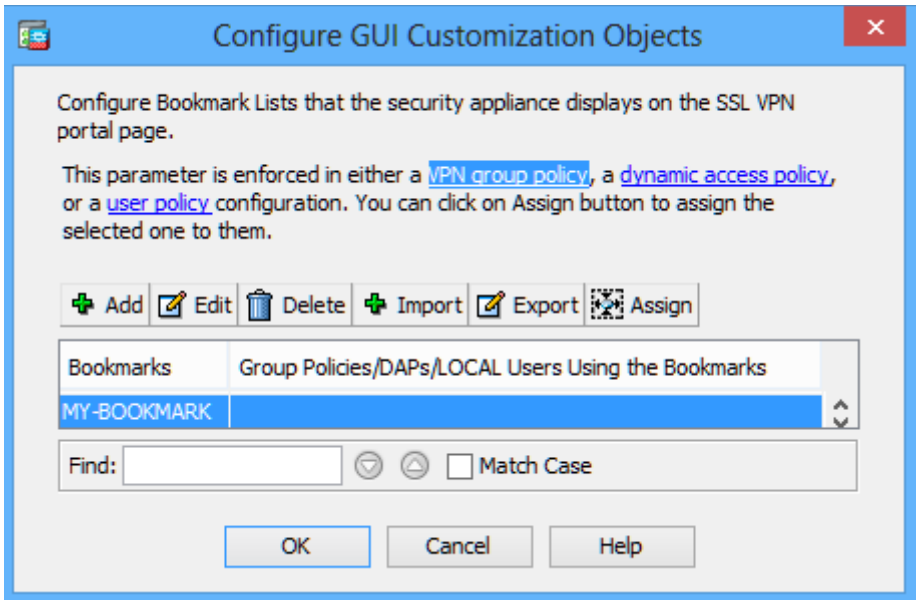
Add a new bookmark with INTERNAL-WEB as the Bookmark Title. Enter the server destination IP address of 192.168.1.10 as the URL.

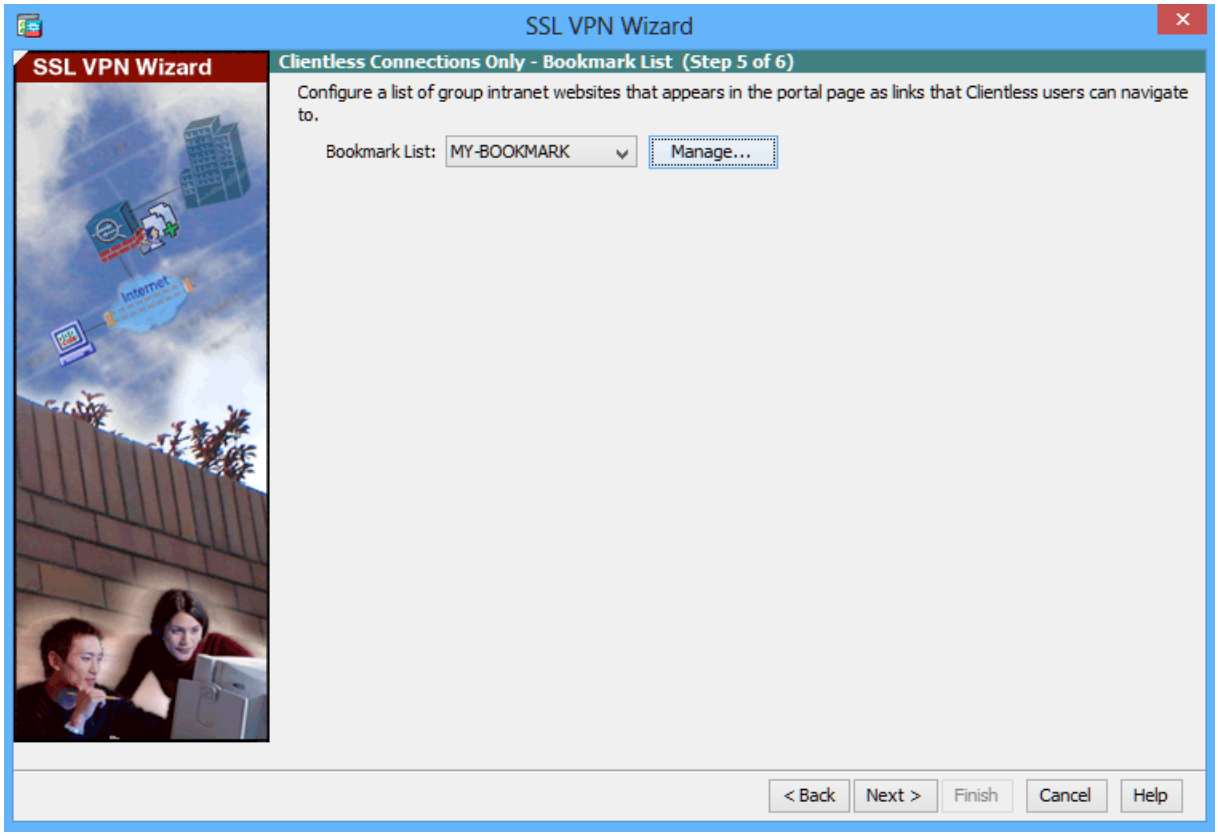


Add a new bookmark with DMZ-SRV-FTP as the Bookmark Title. Enter the server destination IP address of 172.16.1.10 as the URL.

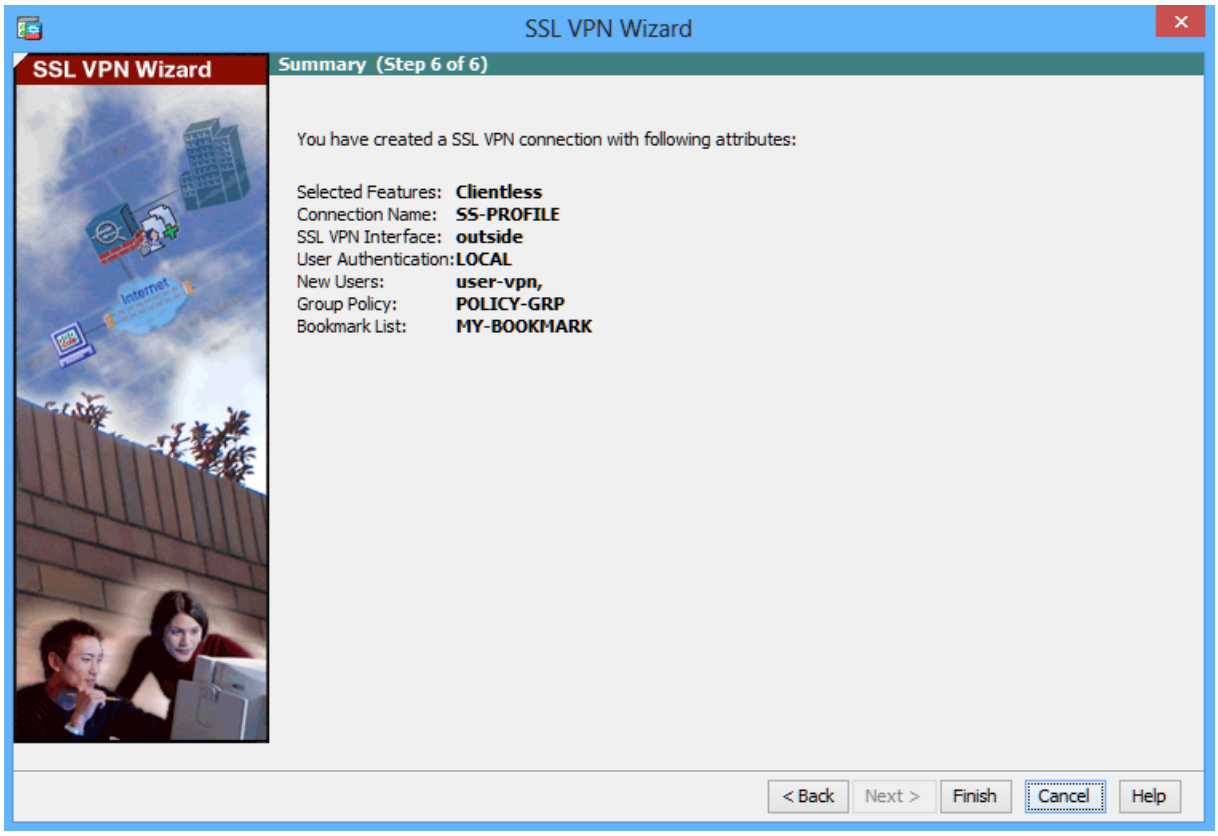


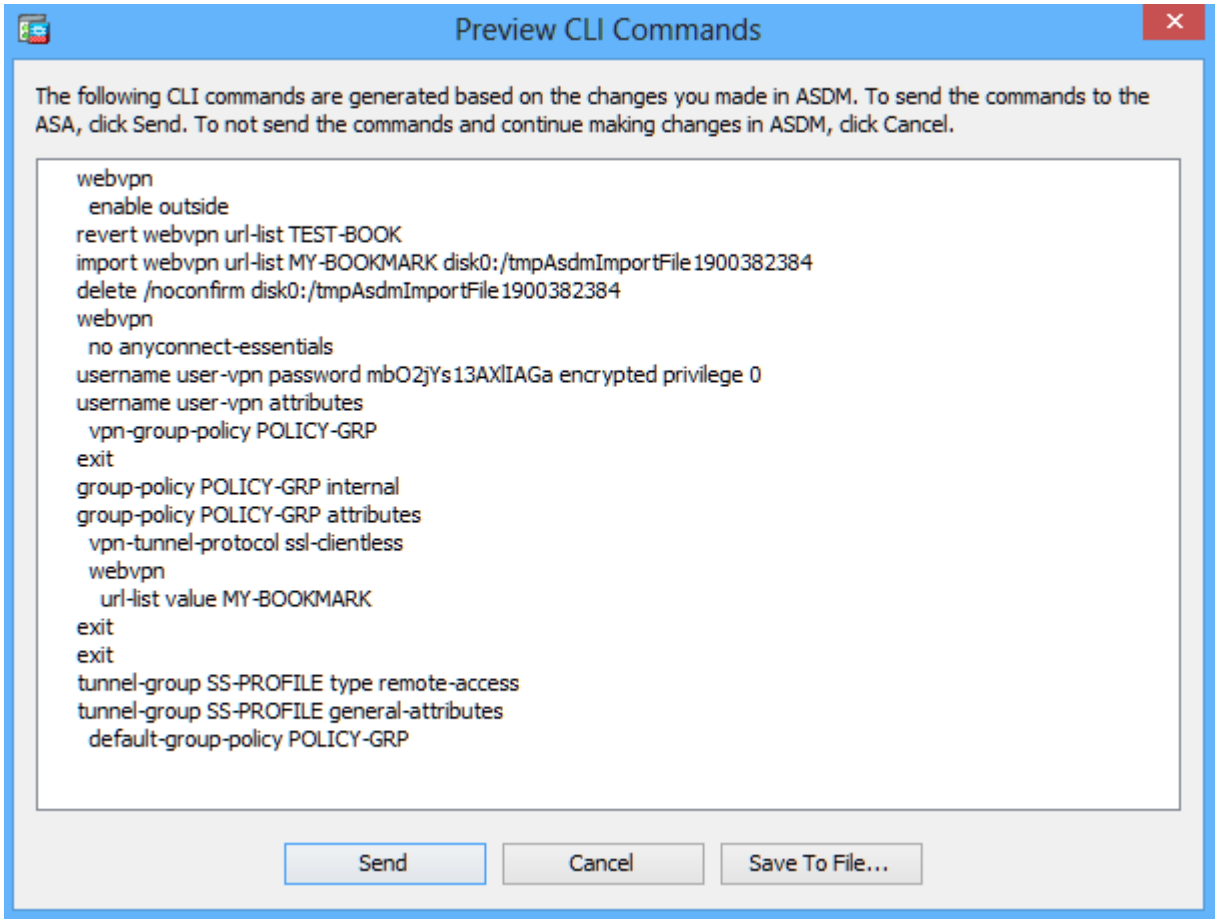






Click finish to complete the wizard and send the commands, and Apply to the ASA

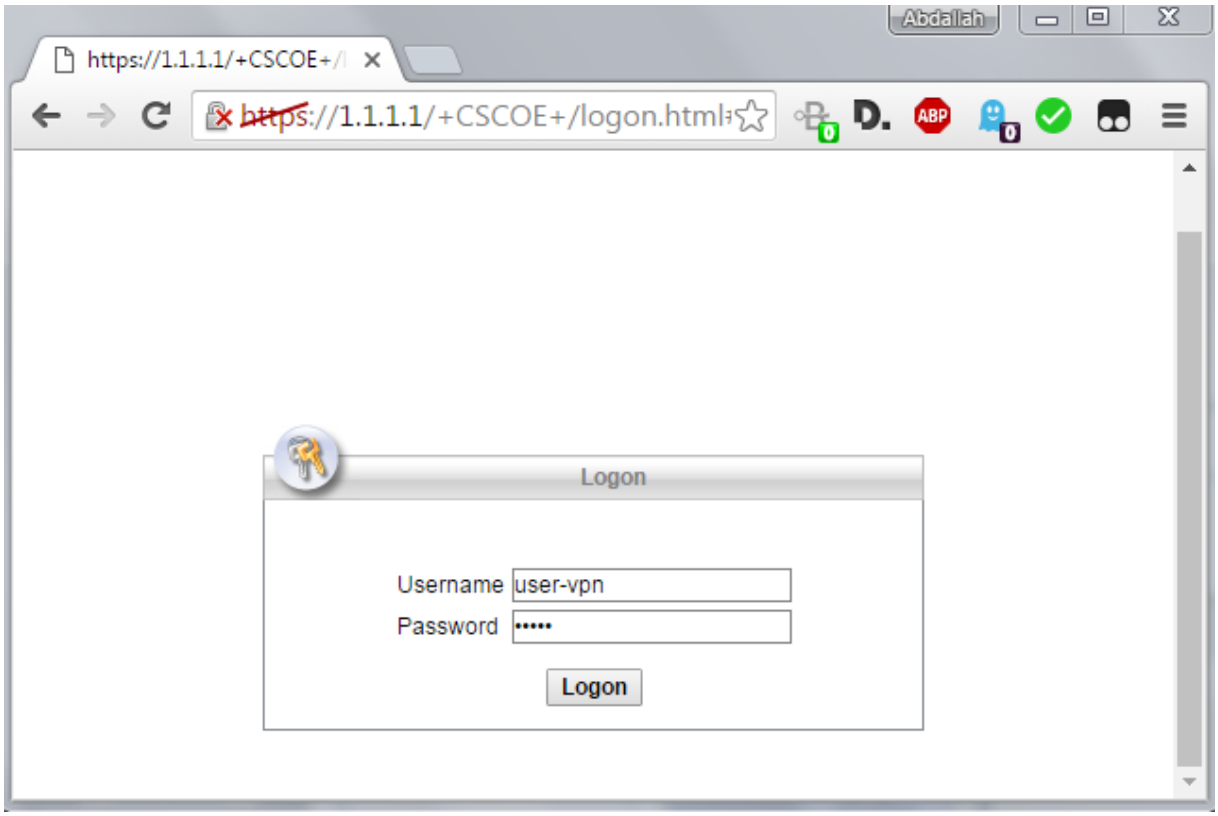




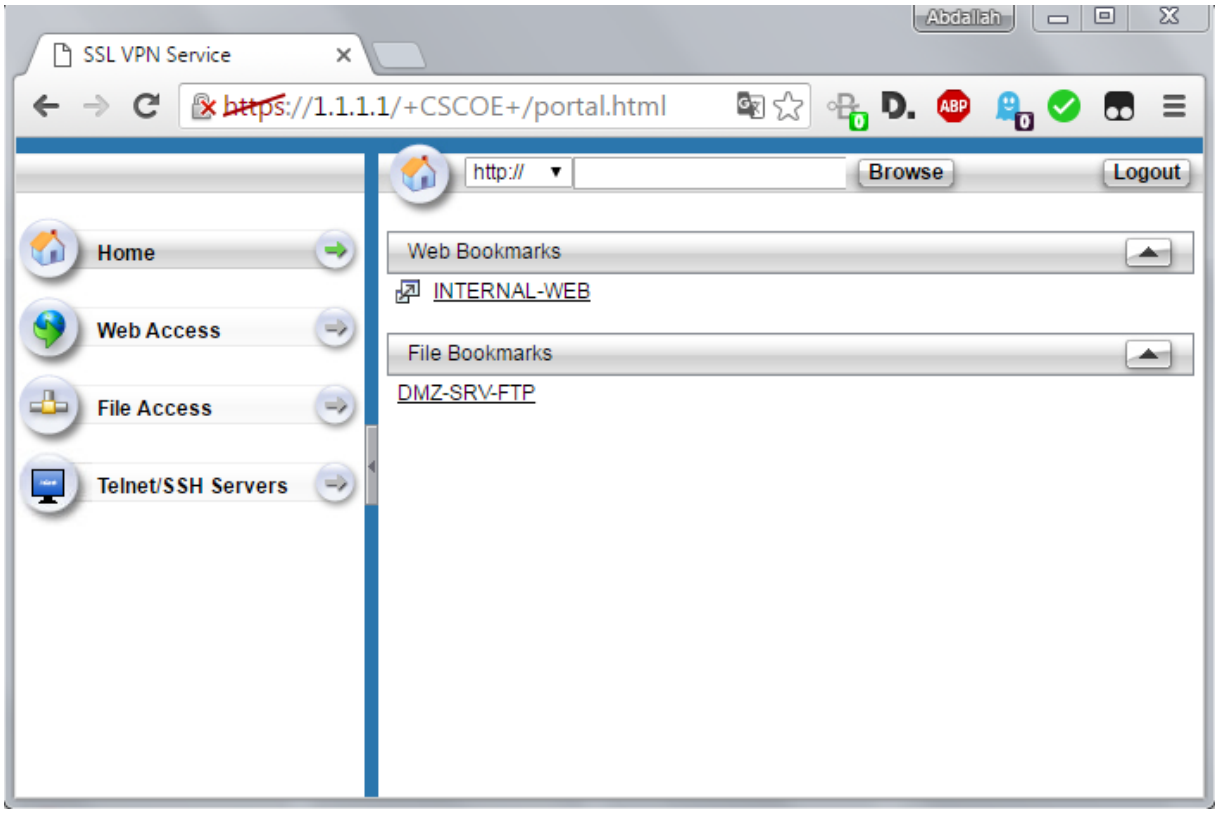
Verify VPN access from the remote host.

Open the browser on OUTSIDE-Host and enter the login URL for the SSL VPN into the address field (https://1.1.1.1). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA. Note: Accept security notification warnings.

The Login window should display. Enter the previously configured username user-vpn, enter the password cisco, and click Logon to continue.

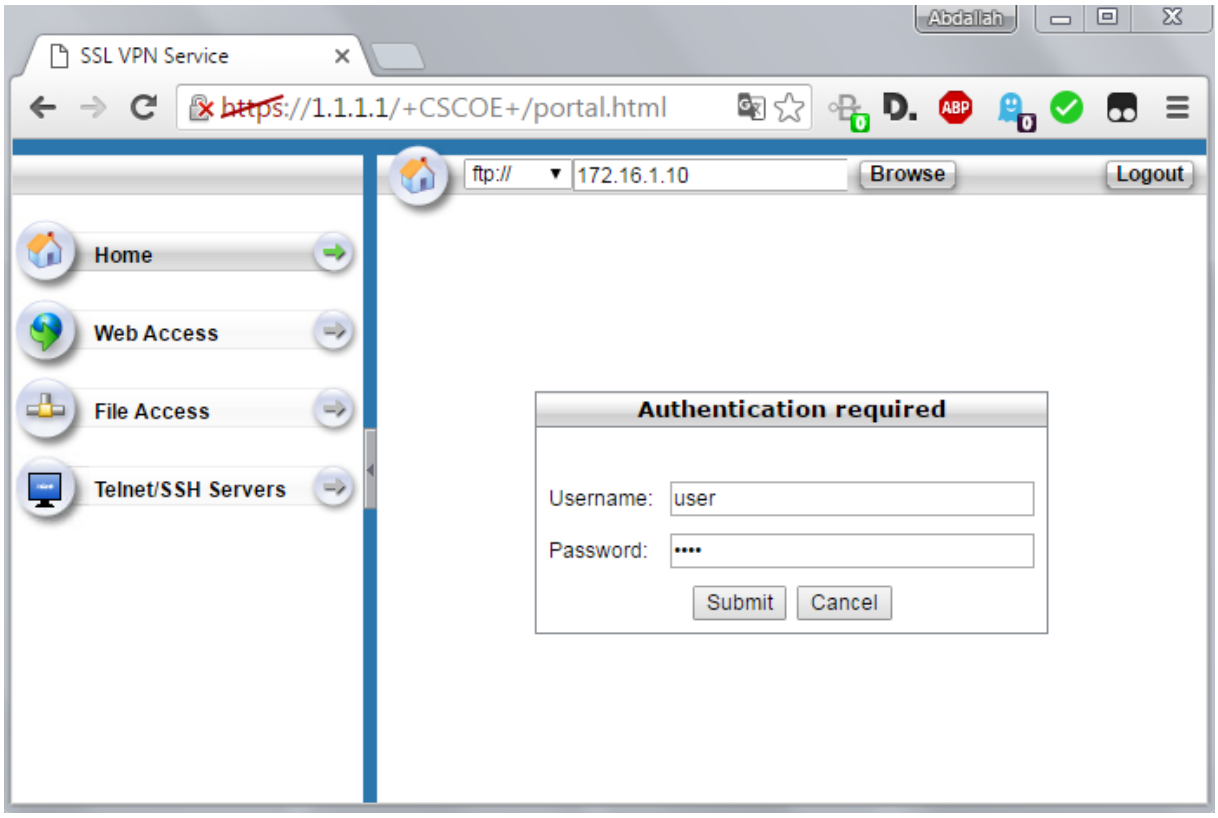


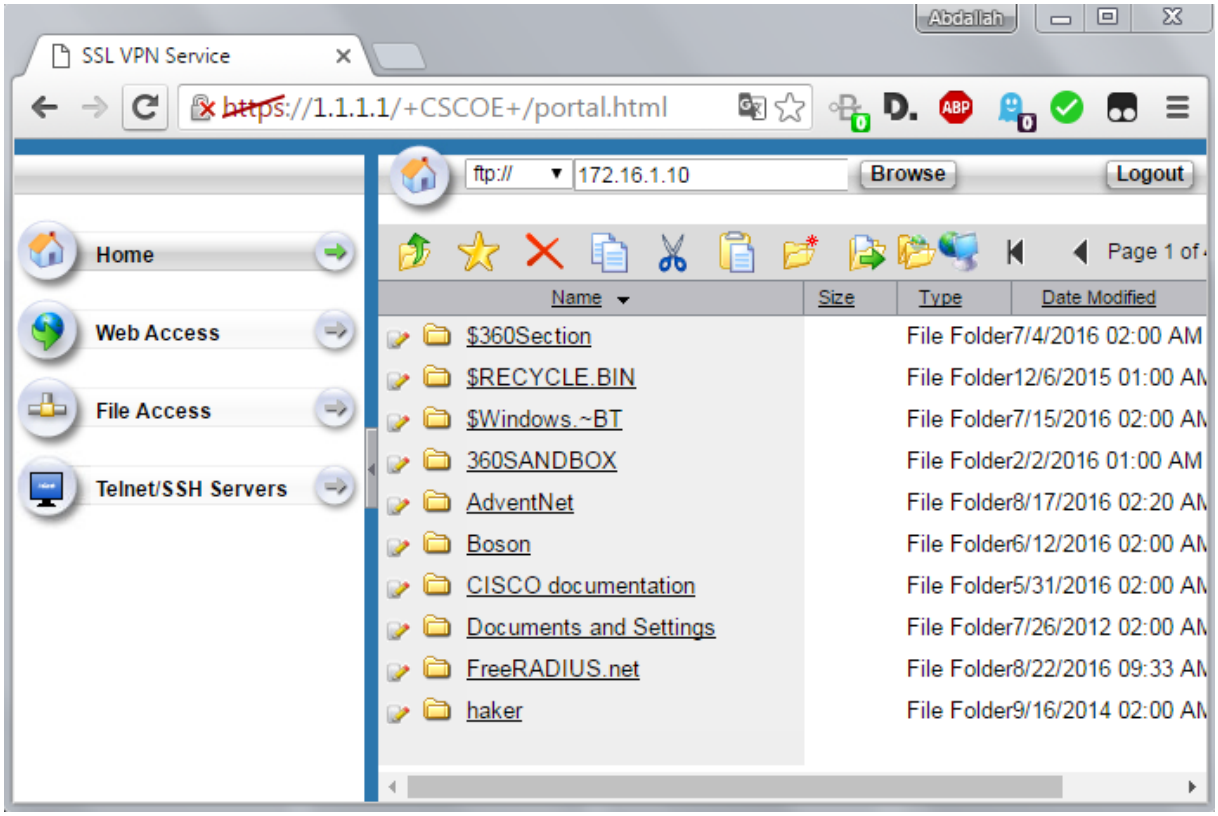
Access the web portal window.
After the user authenticates, the ASA SSL web portal webpage will be displayed. This webpage lists the bookmarks previously assigned to the profile.



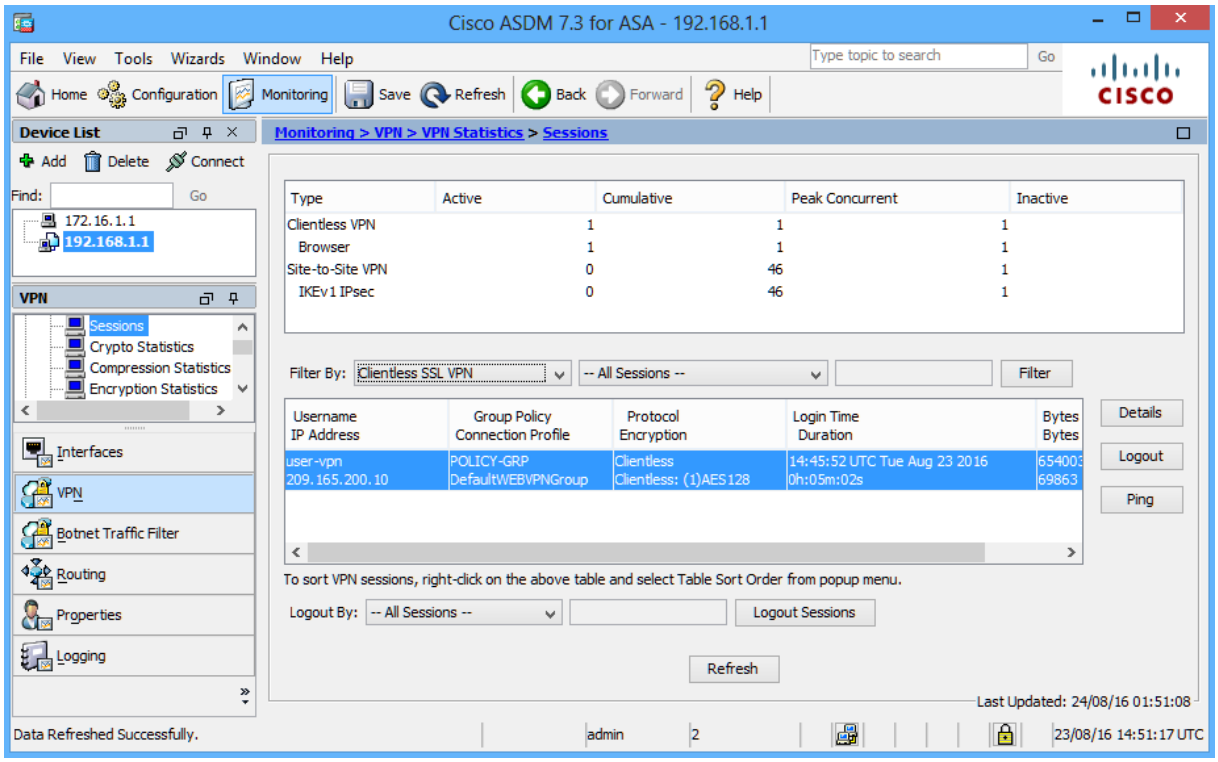
Access the Inside Web Server by clicking on INTERNAL-WEB bookmark, the web page is displayed:

Access the DMZ server by clicking on DMZ-SRV-FTP URL, the FTP server in DMZ needs authentication, the outside user can access the FTP server from the ASA portal.



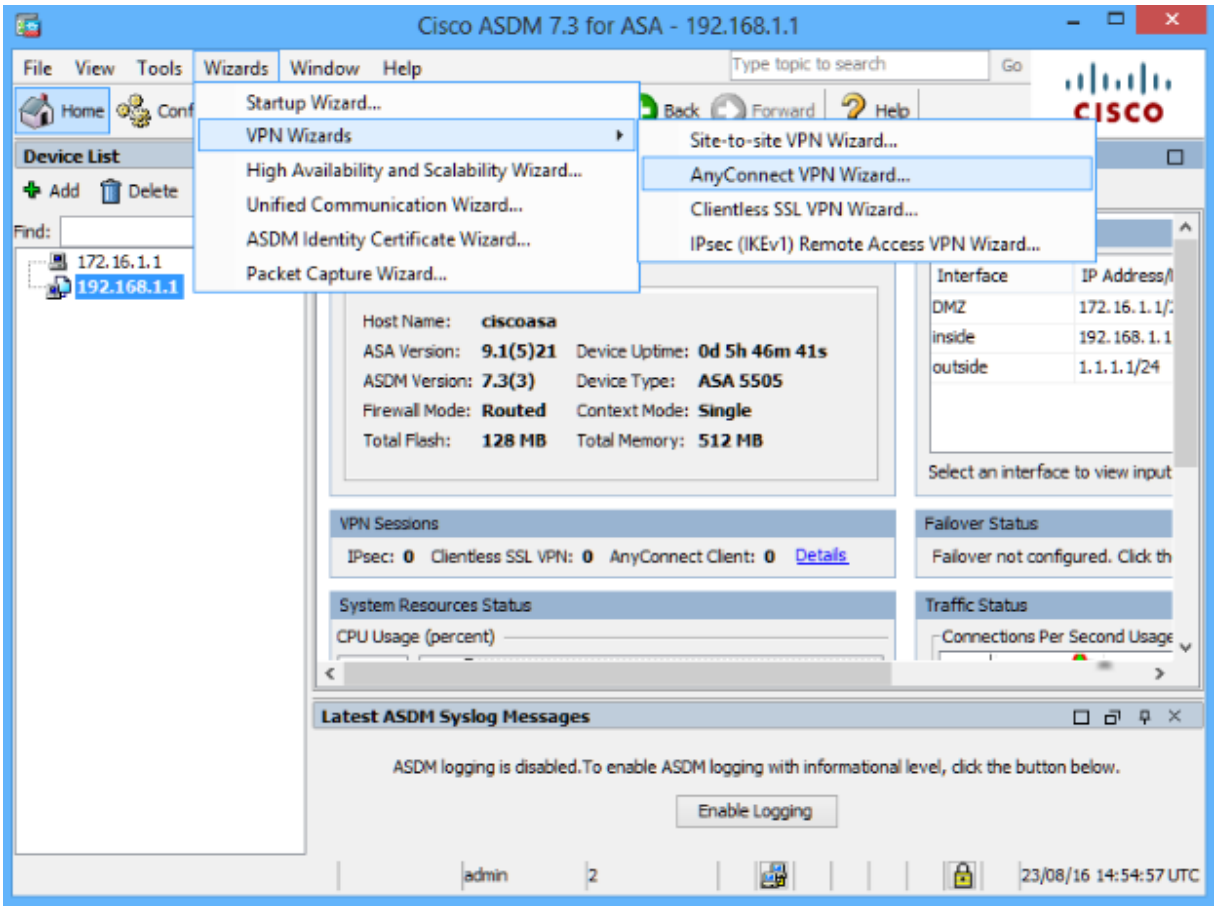


From ASDM, verify that the VPN Clientless is established from the IP address 209.165.200.10 of the Outside Host:

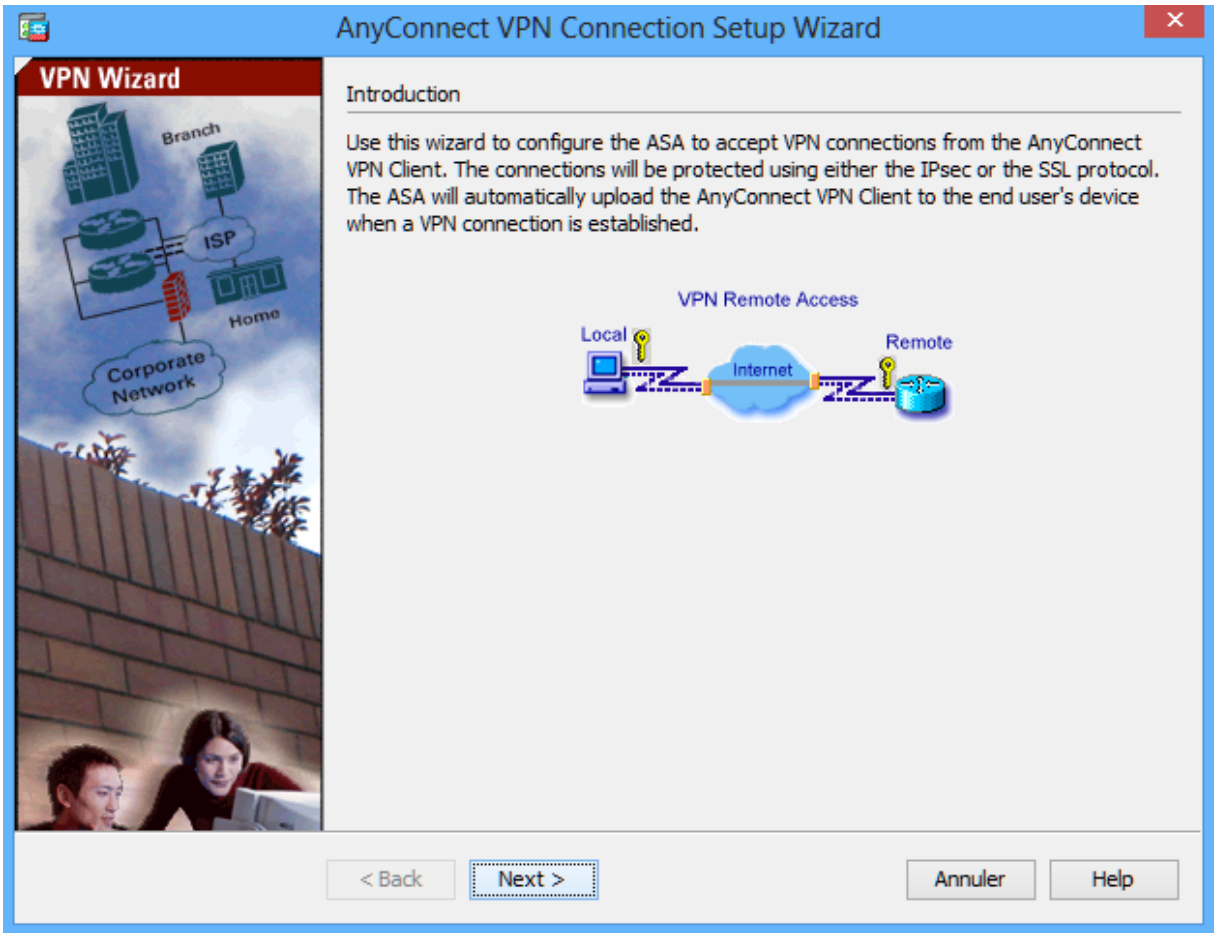

Cisco ASDM 7.3 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Add Delete Connect
Find:
Go
172.16.1.1
192.168.1.1
VPN
Sessions
Crypto Statistics
Compression Statistics
Encryption Statistics
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Monitoring > VPN > VPN Statistics > Sessions
Type Active Cumulative Peak Concurrent Inactive
Clientless VPN 1 1 1
Browser 1 1 1
Site-to-Site VPN 0 46 1
IKEv1 IPsec 0 46 1
Filter By: Clientless SSL VPN
-- All Sessions --
Filter
Username
IP Address
Group Policy
Connection Profile
Protocol
Encryption
Login Time
Duration
Bytes
Bytes
user-vpn
209.165.200.10
POLICY-GRP
DefaultWEBVPNGroup
Clientless
Clientless: (1)AES128
14:45:52 UTC Tue Aug 23 2016
0h:05m:02s
654003
69863
Details
Logout
Ping
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.
Logout By: -- All Sessions --
Logout Sessions
Refresh
Last Updated: 24/08/16 01:51:08
Data Refreshed Successfully.
admin
2
23/08/16 14:51:17 UTC

Part-9: Configure ASA AnyConnect SSL VPN Remote Access

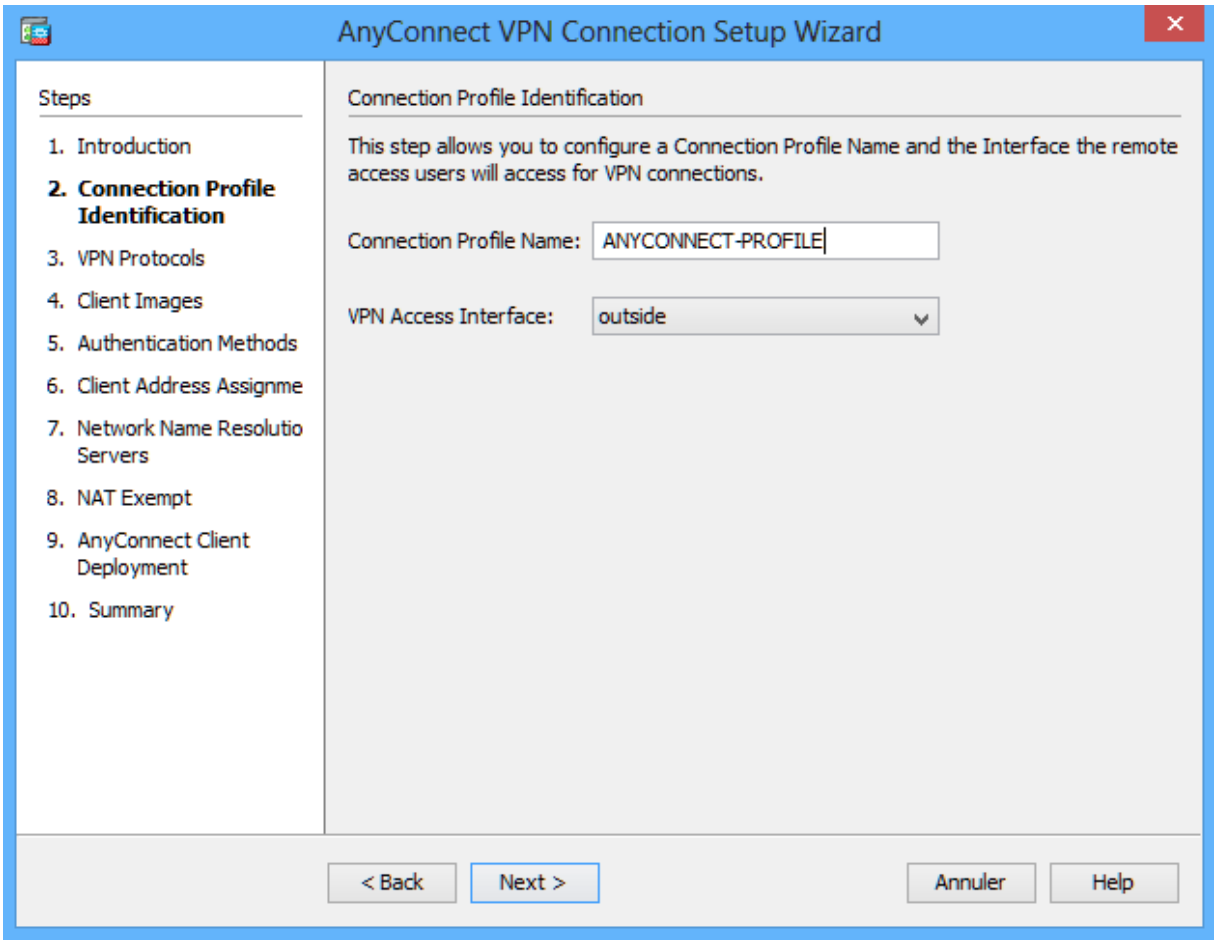
Start the VPN wizard.
On the ASDM main menu, click Wizards > VPN Wizards > AnyConnect VPN Wizard.



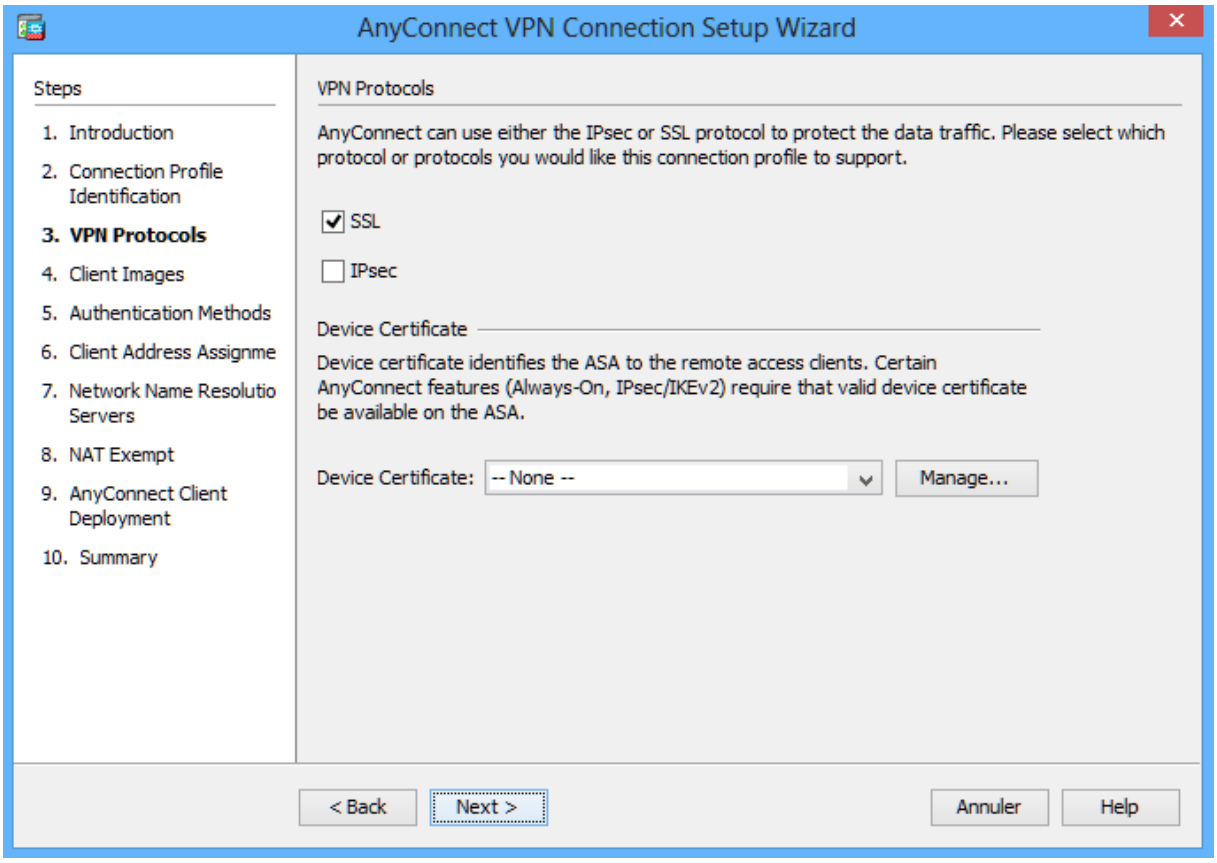
Review the on-screen text and topology diagram. Click Next to continue.



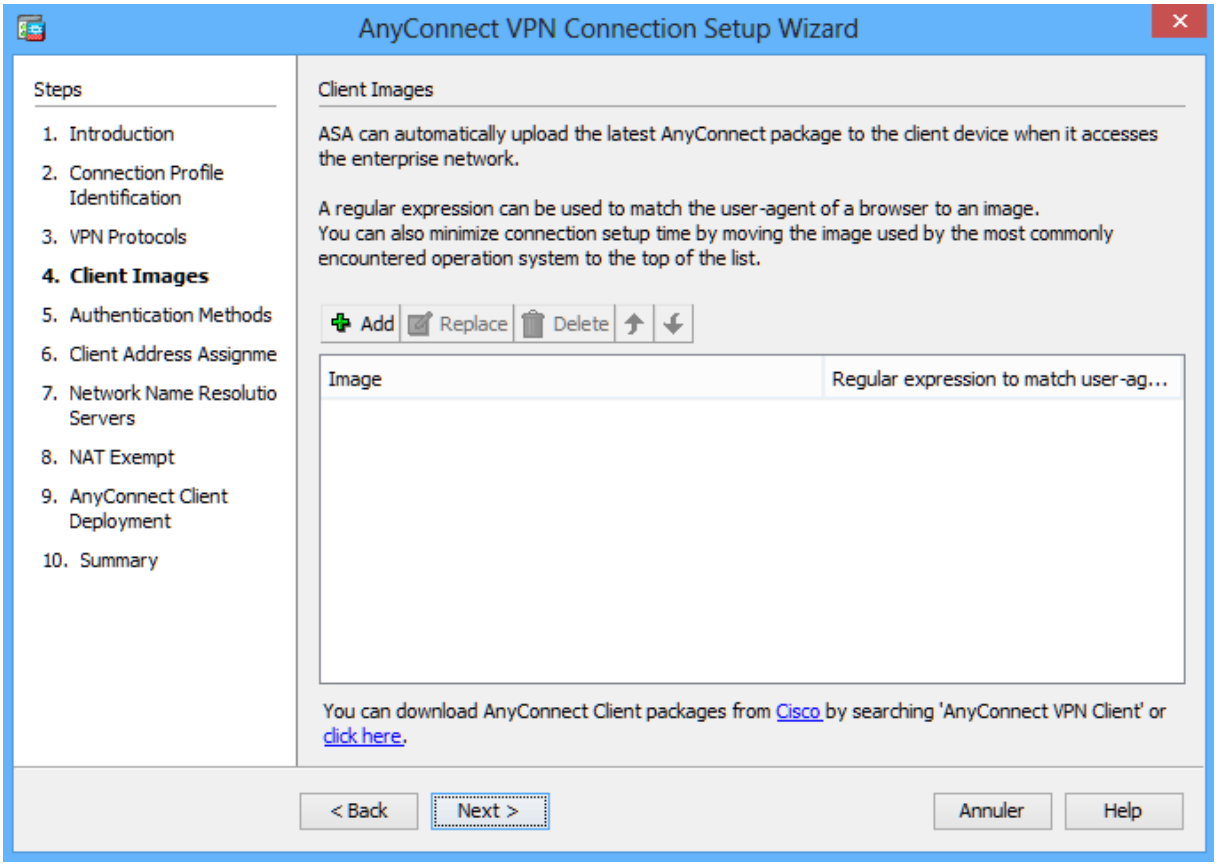
Configure the SSL VPN interface connection profile.
On the Connection Profile Identification screen, enter AnyConnect-PROFILE as the Connection Profile Name and specify the outside interface as the VPN Access Interface. Click Next to continue.



Specify the VPN encryption protocol.
On the VPN Protocols screen, uncheck the IPsec check box and leave the SSL check box checked. Do not specify a device certificate. Click Next to continue.

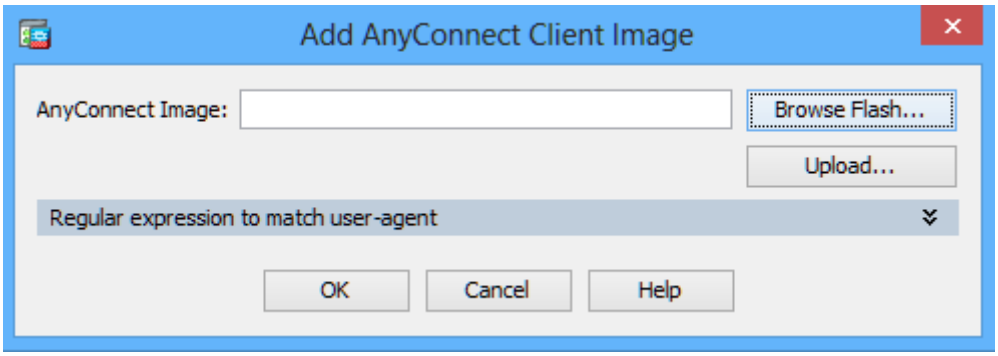


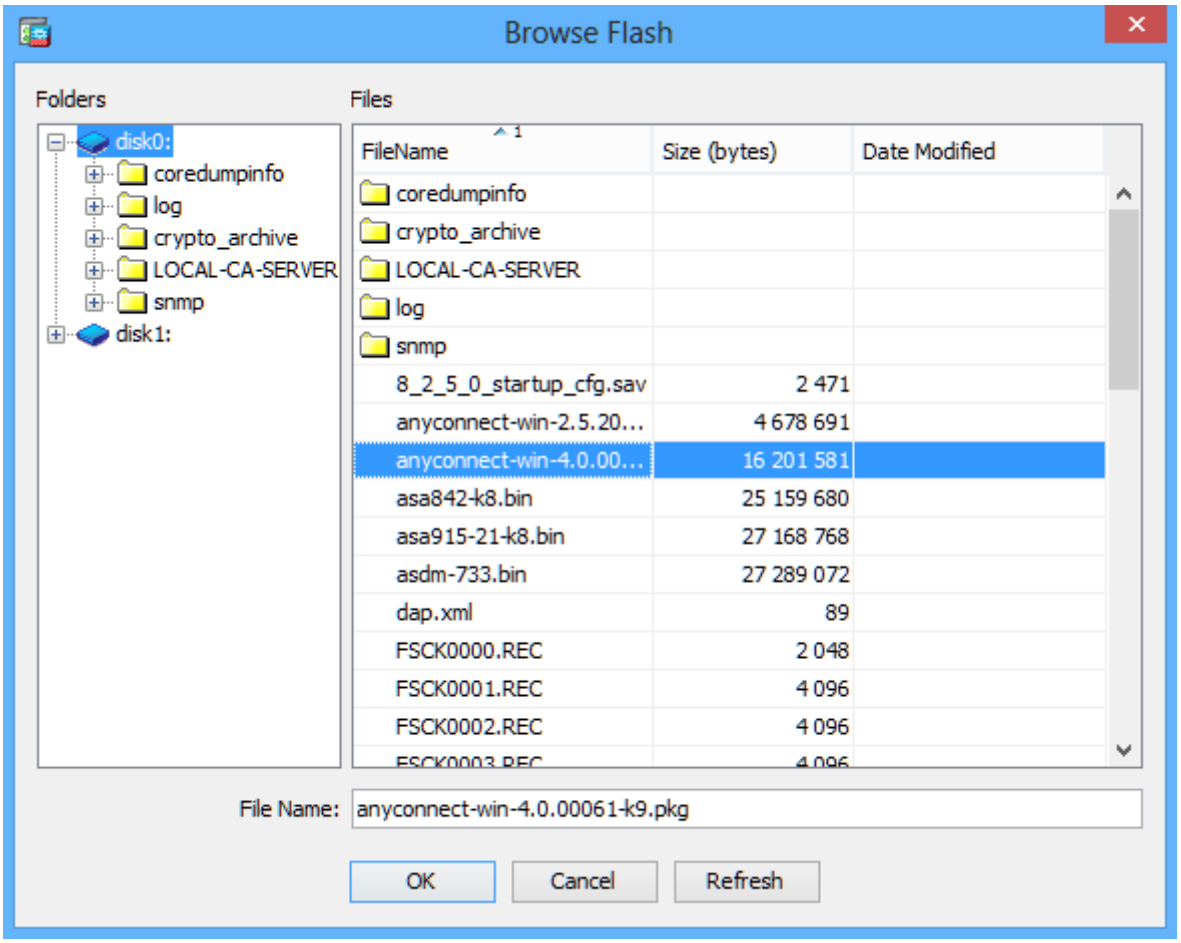
Specify the client image to upload to AnyConnect users.
On the Client Images screen, click Add to specify the AnyConnect client image filename.



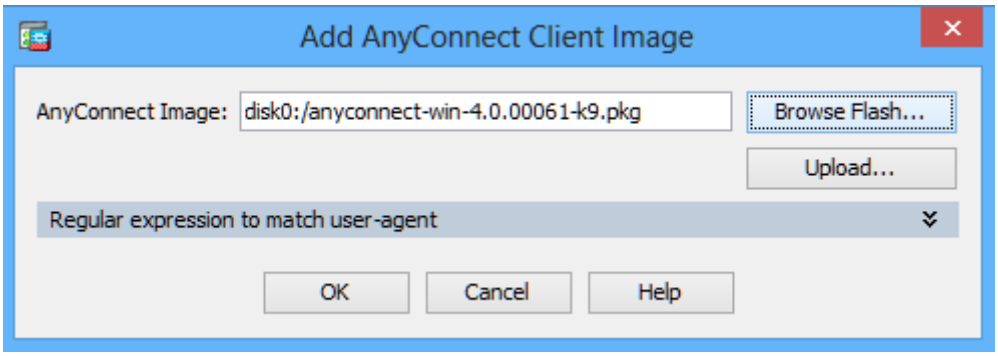
In the Add AnyConnect Client Image window, click Browse Flash.

In the Browse Flash window, select the AnyConnect package file for Windows (anyconnect-win-4.0.00061-k9.pkg, in the example). Click OK to return to the AnyConnect Client Image window.

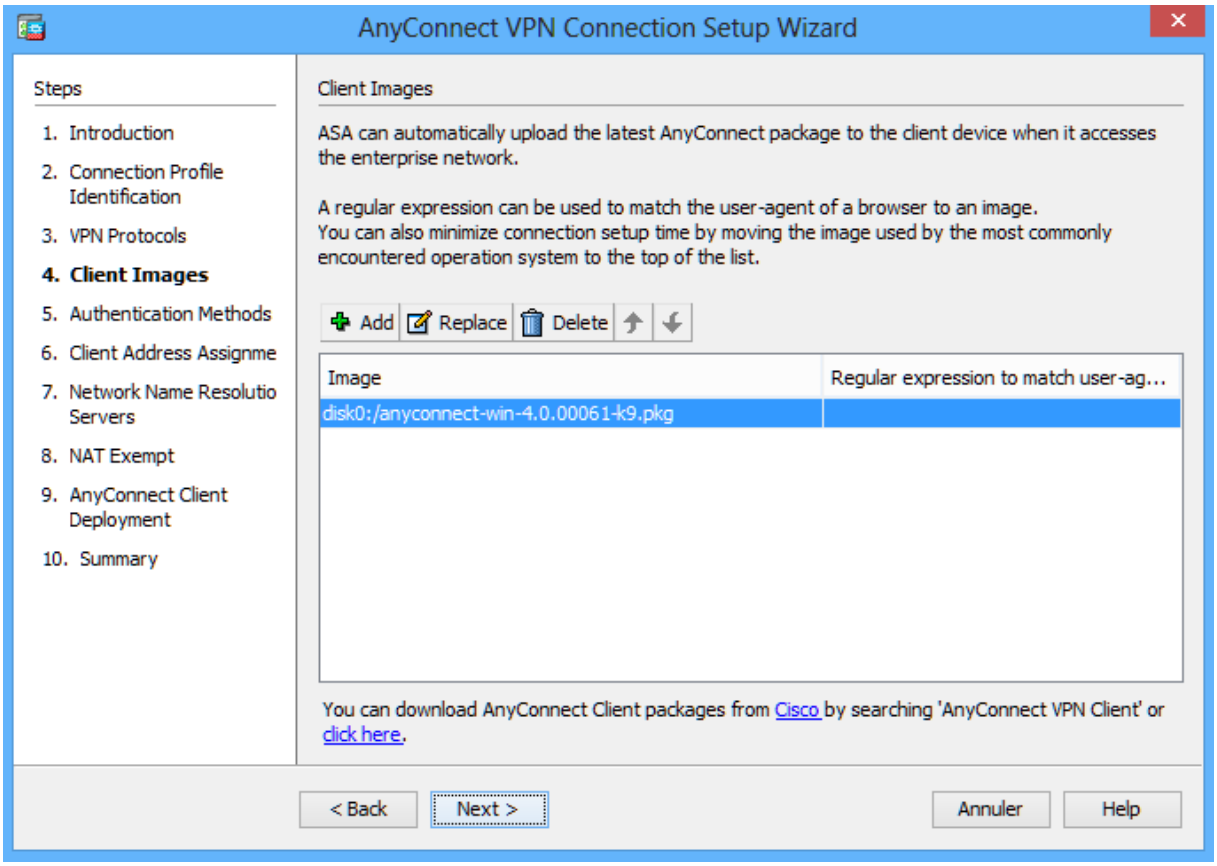




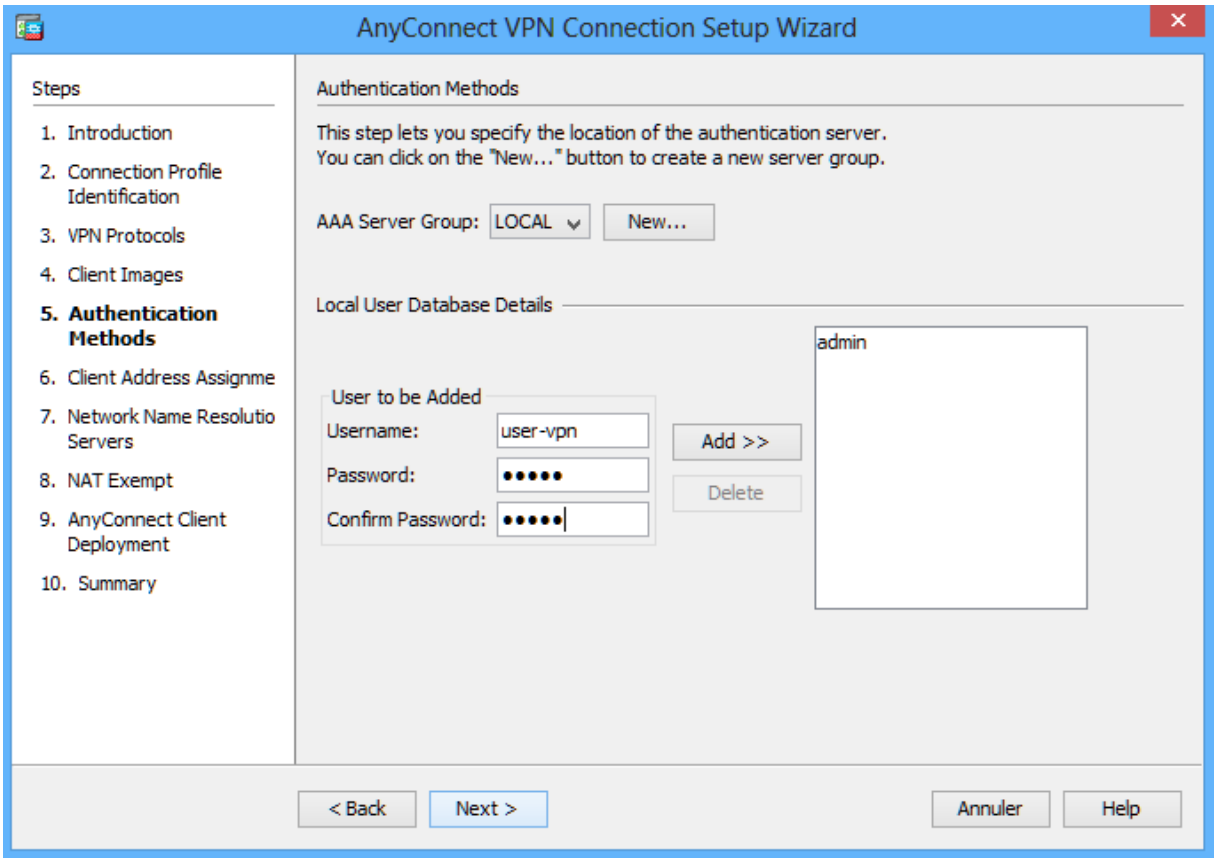
Click OK again to return to the Client Image window.

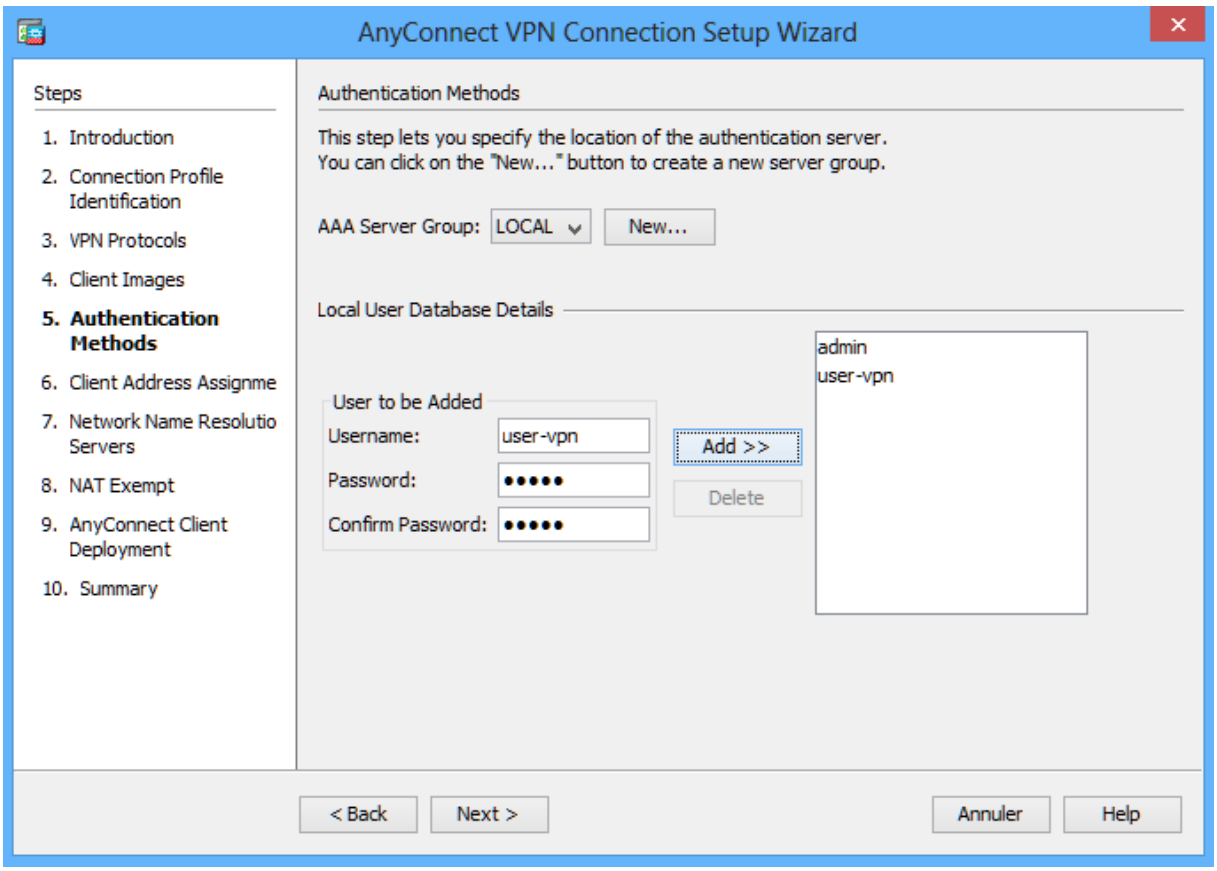


The selected image is now displayed on the Client Image window. Click Next to continue.

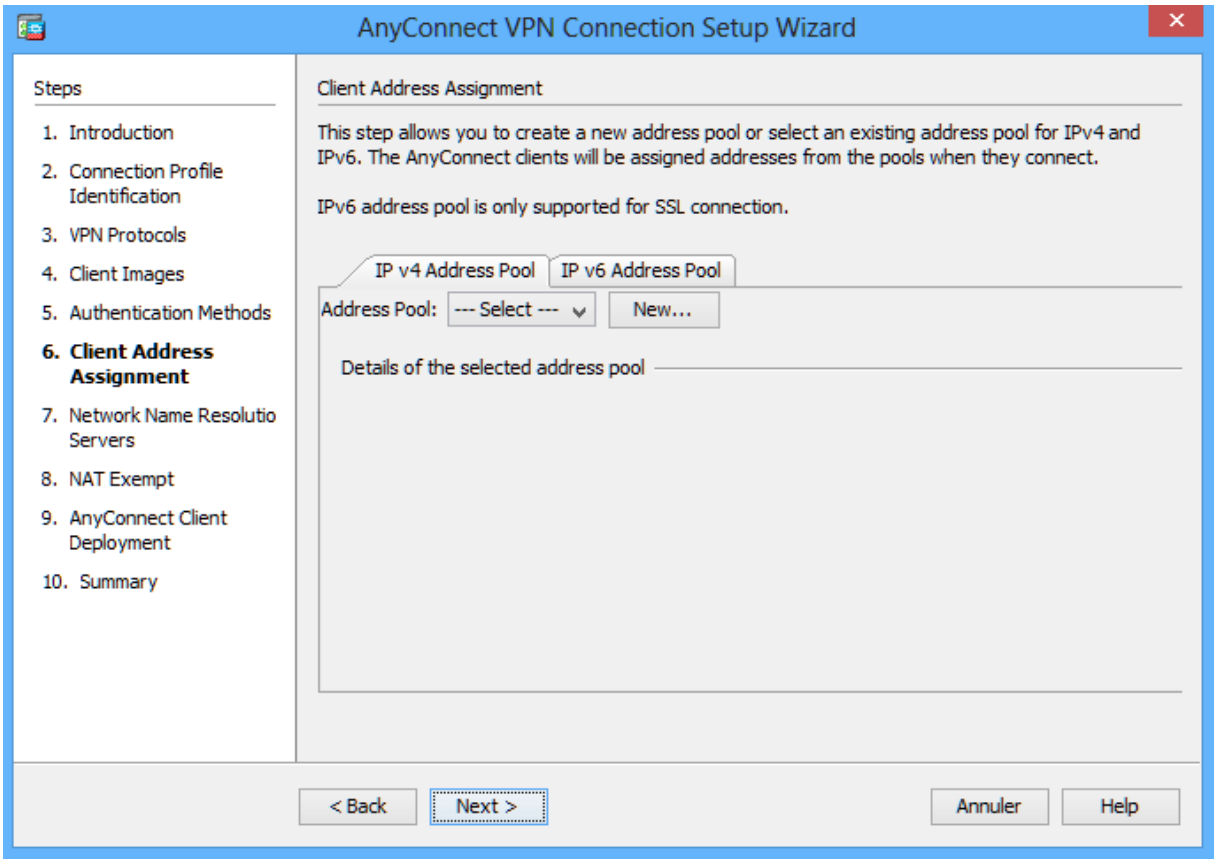


Configure AAA local authentication.
On the Authentication Methods screen, ensure that the AAA Server Group is specified as LOCAL.
Enter a new user named user-vpn with the password cisco. Click Add.

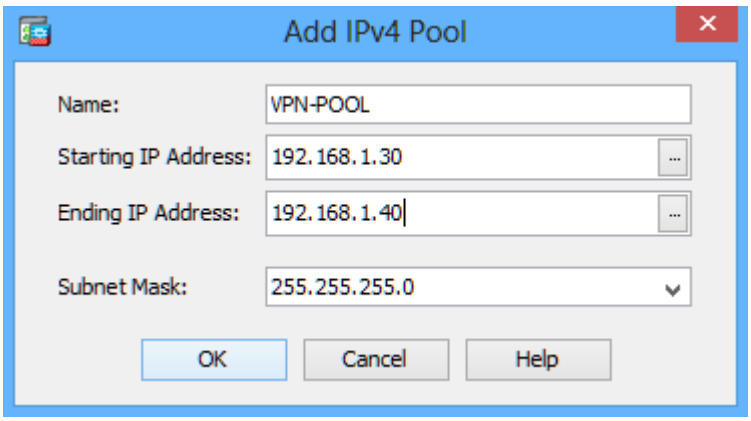




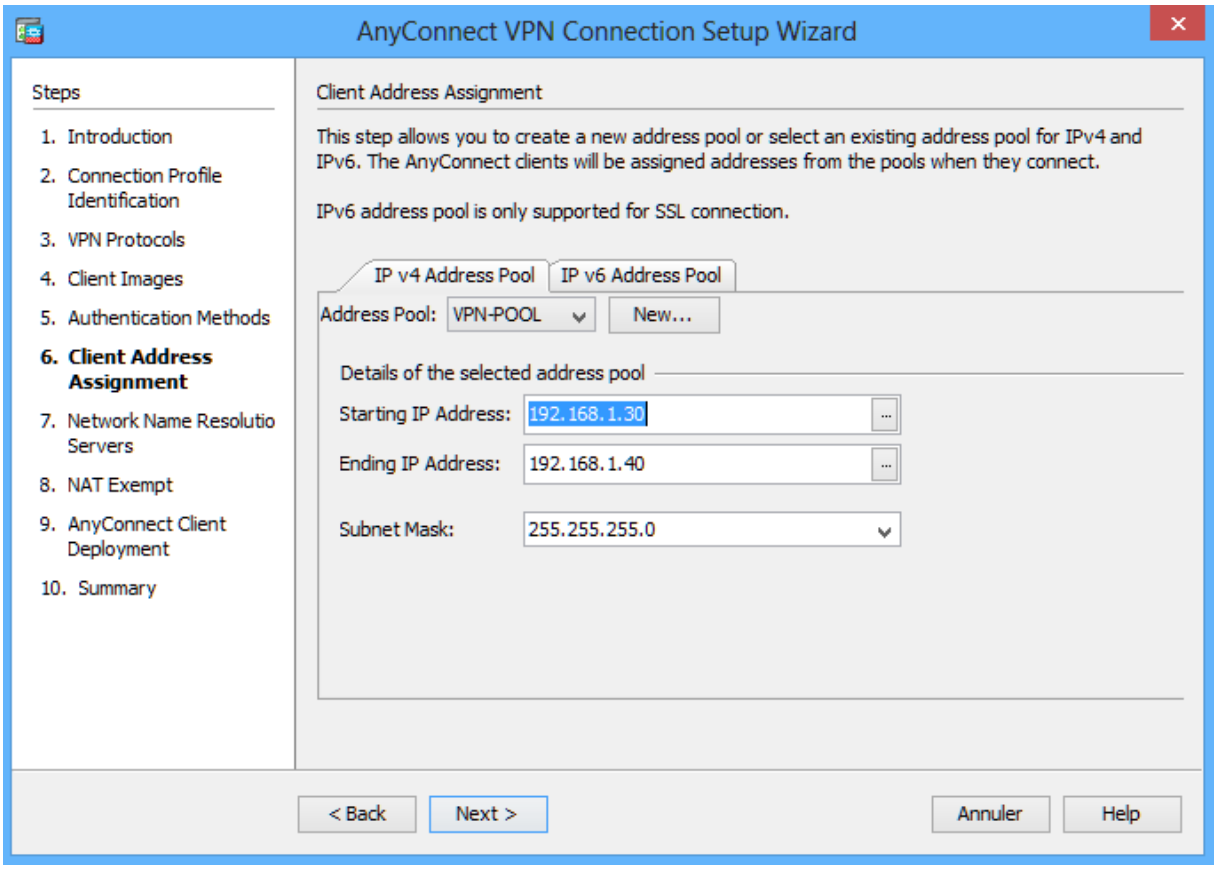
Configure the client address assignment.
In the Client Address Assignment window, click New to create an IPv4 address pool.



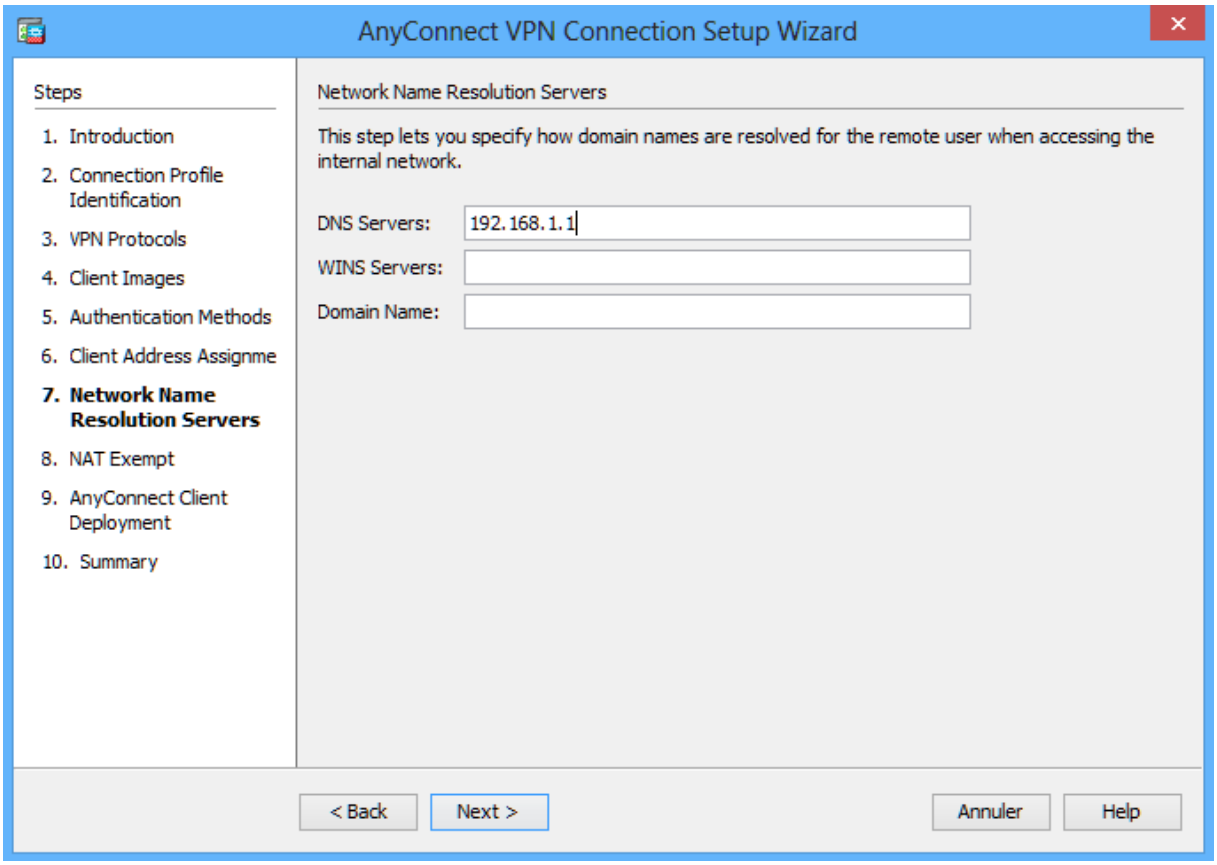
In the Add IPv4 Pool window, name the pool Remote-Pool with a starting IP address of 192.168.1.30, an ending IP address of 192.168.1.40, and a subnet mask of 255.255.255.0. Click OK to return to the Client Address Assignment window, which now displays the newly created remote user IP address pool.



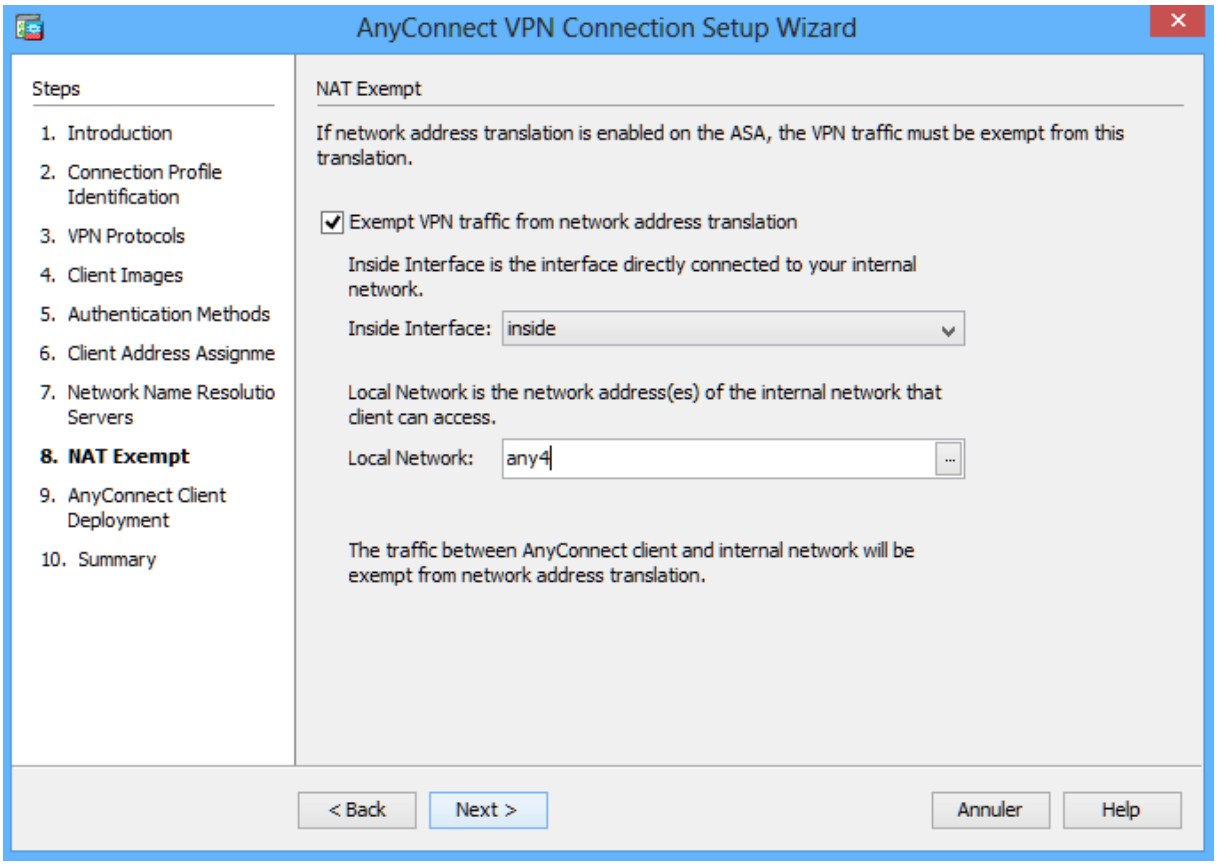
The Client Address Assignment window now displays the newly created remote user IP address pool. Click Next to continue.



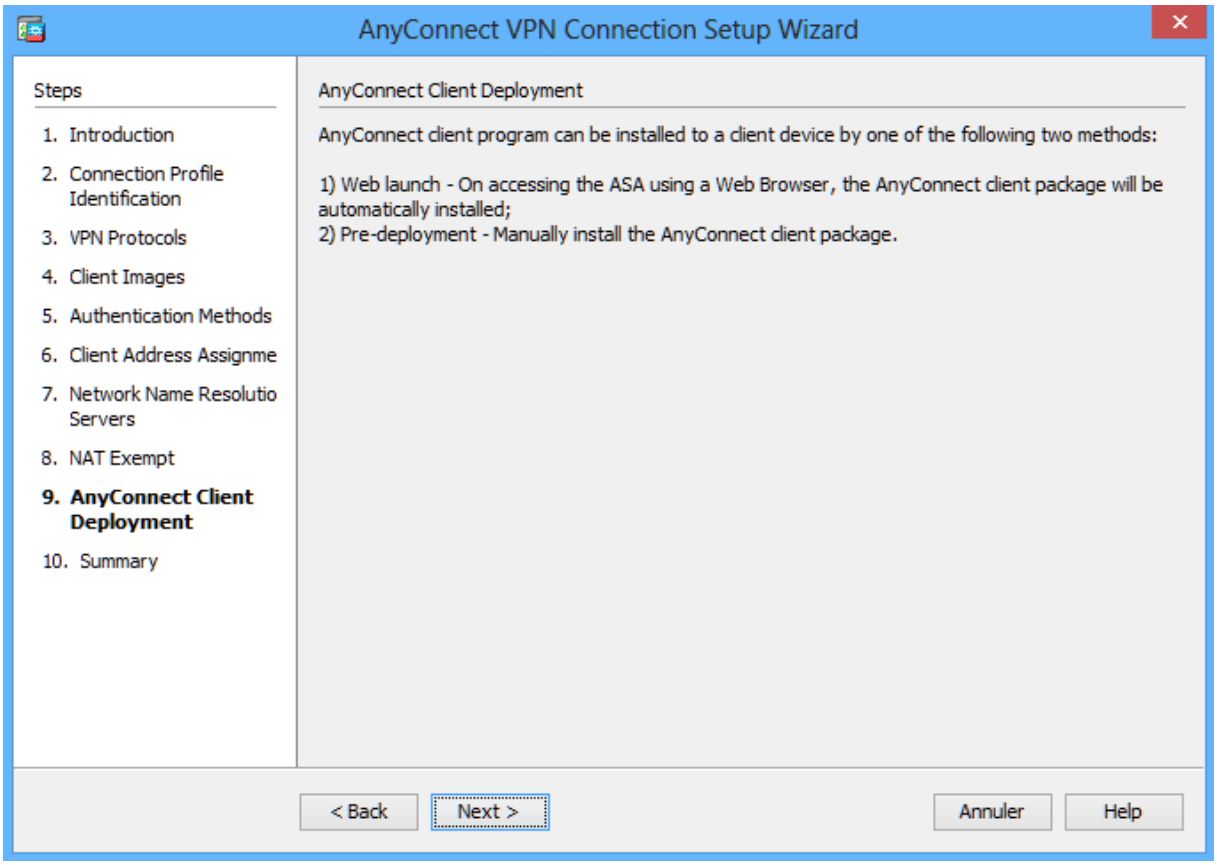
Configure the network name resolution.
On the Network Name Resolution Servers screen, enter the IP address of a DNS server (192.168.1.1). Click Next to continue.



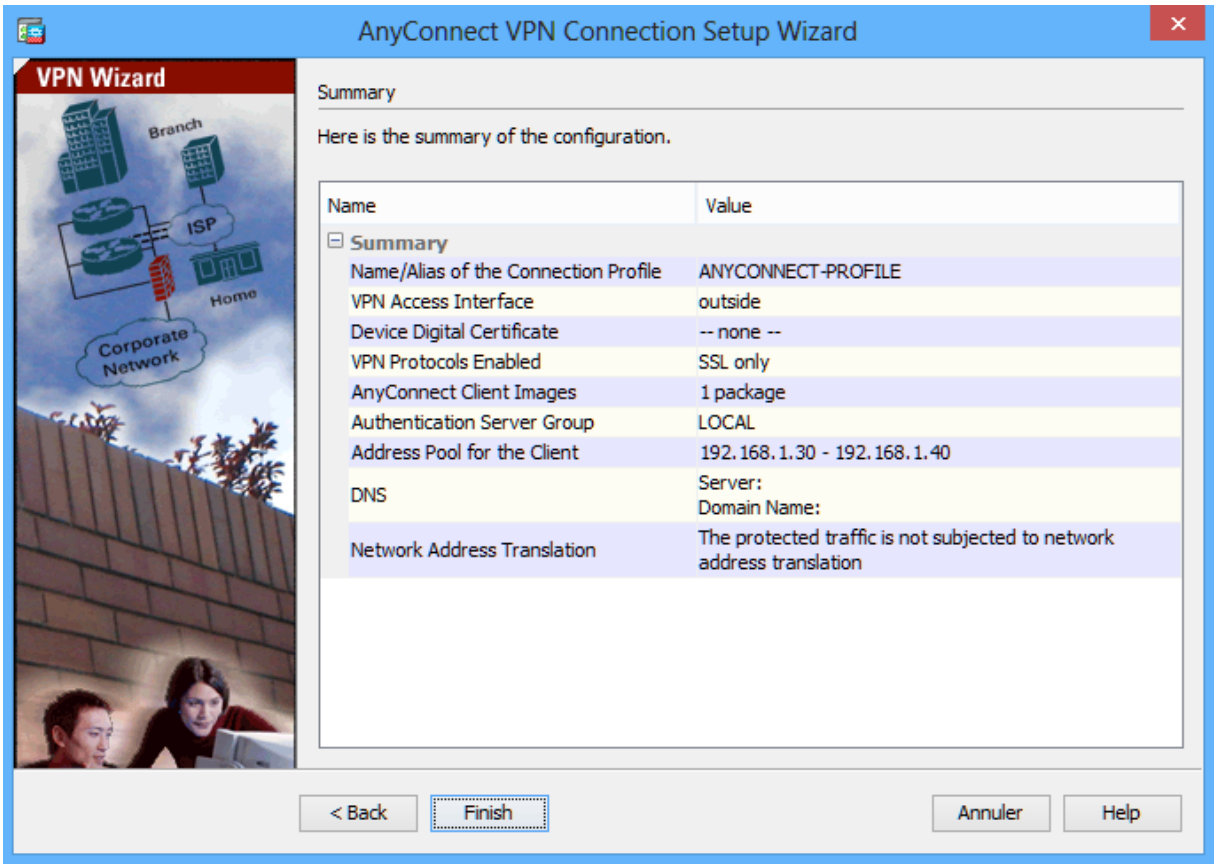
Exempt address translation for VPN traffic.
On the NAT Exempt screen, click the Exempt VPN traffic from network address translation check box. Do not change the default entries for the Inside Interface (inside) and the Local Network (any4). Click Next to continue.

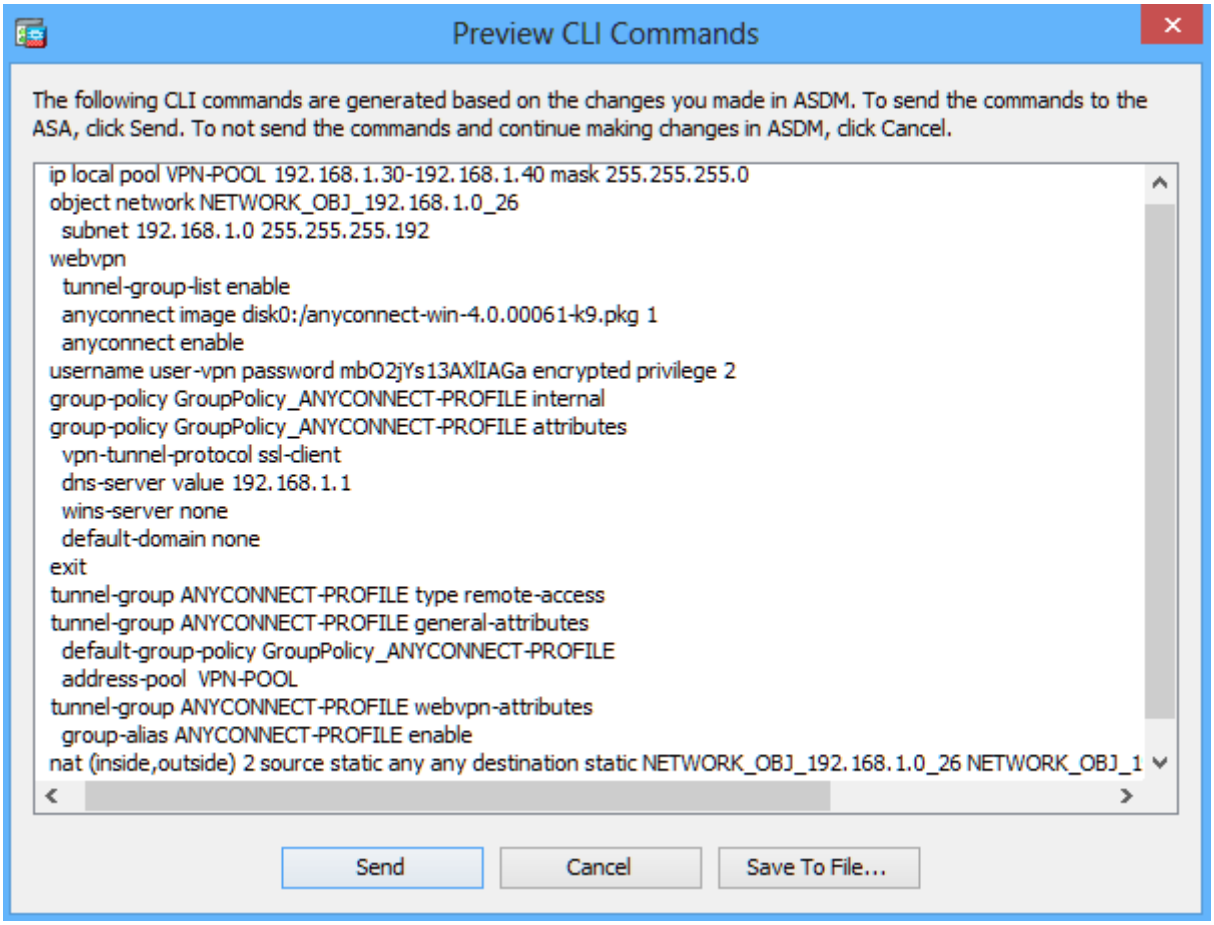


Review the AnyConnect client deployment details.
On the AnyConnect Client Deployment screen, read the text describing the options, and then click Next to continue.



Review the Summary screen and apply the configuration to the ASA.
On the Summary screen, review the configuration, click Finish, and send commands to ASA.

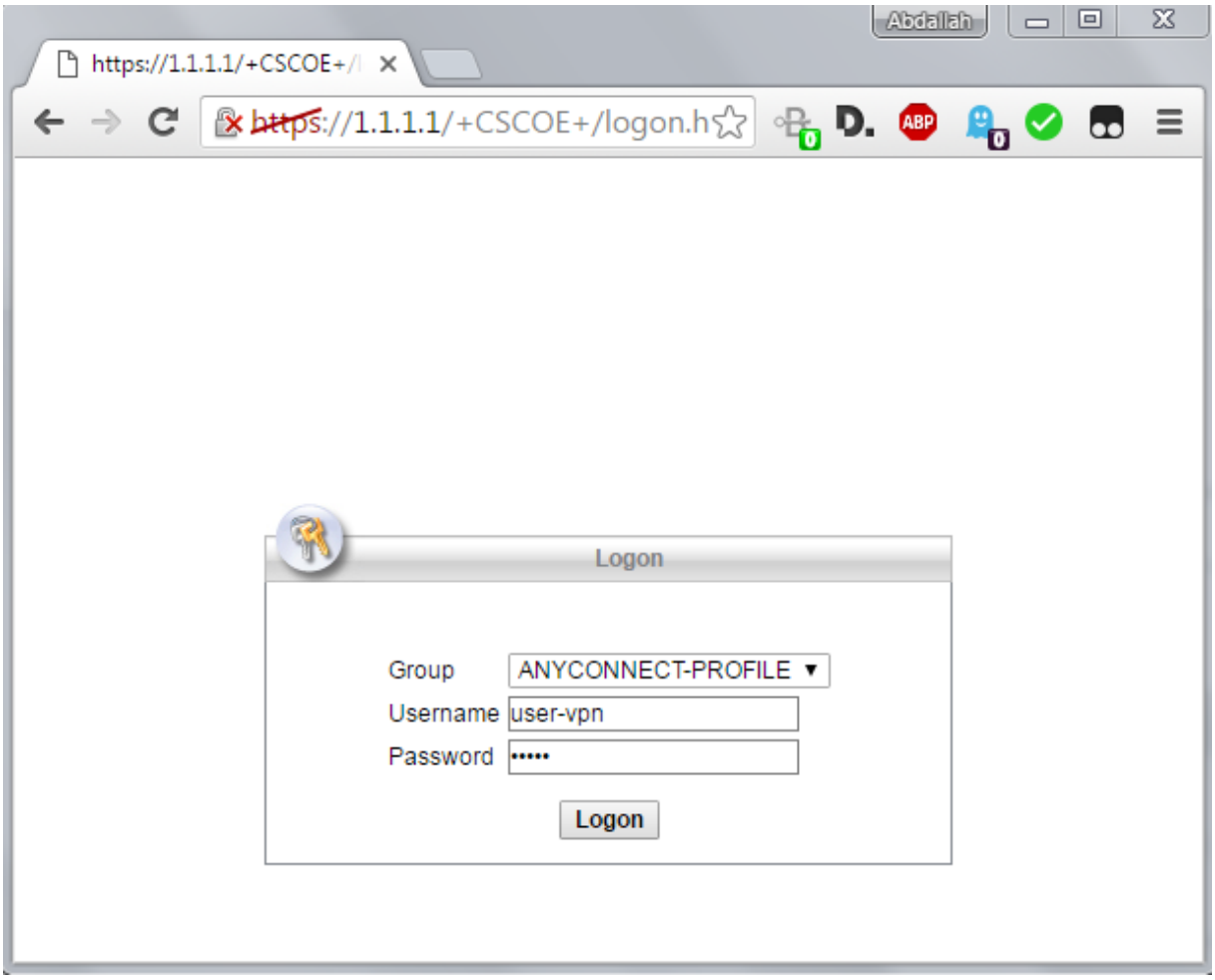




Log in from the Outside Host.

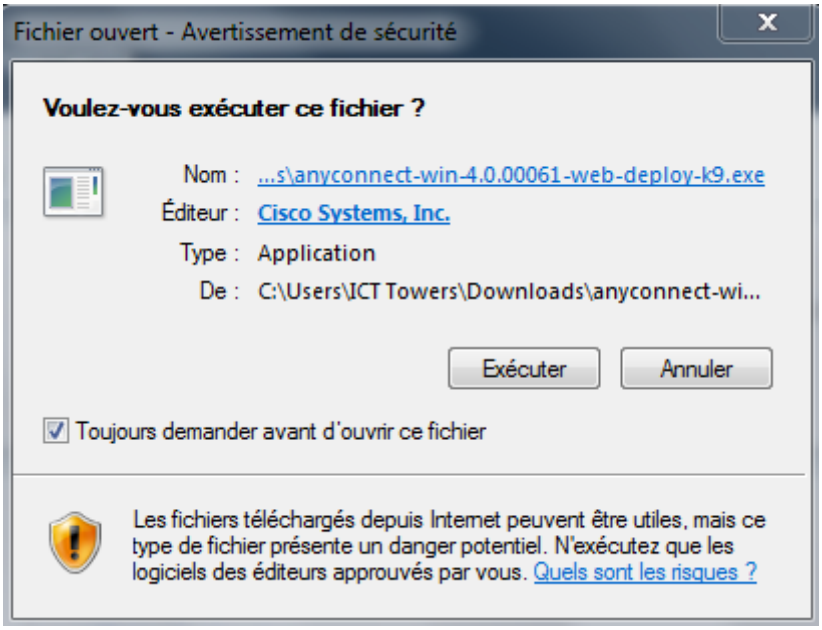
Initially, you will establish a clientless SSL VPN connection to the ASA in order to download the AnyConnect client software. Open a web browser on Outside Host. In the address field of the browser, enter https://1.1.1.1 for the SSL VPN. SSL is required to connect to the ASA, therefore, use secure HTTP (HTTPS).

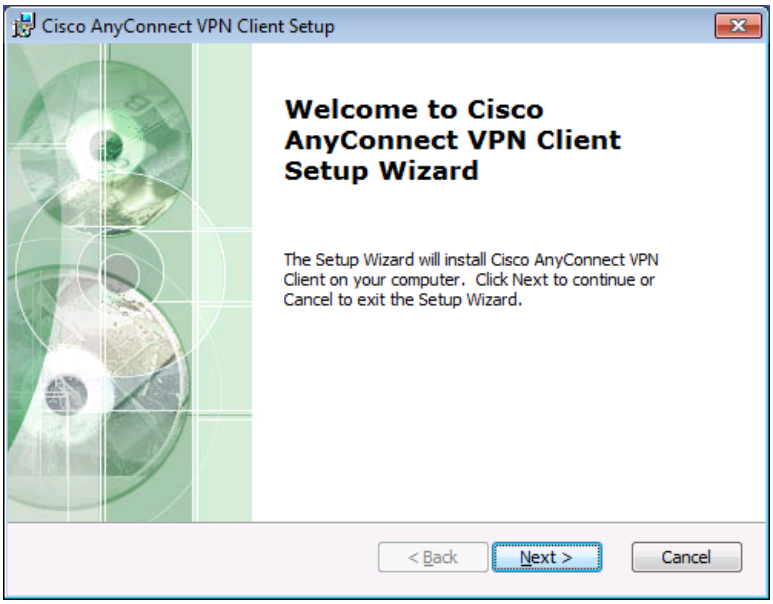
Enter the previously created username user-vpn with the password cisco. Click Logon to continue.



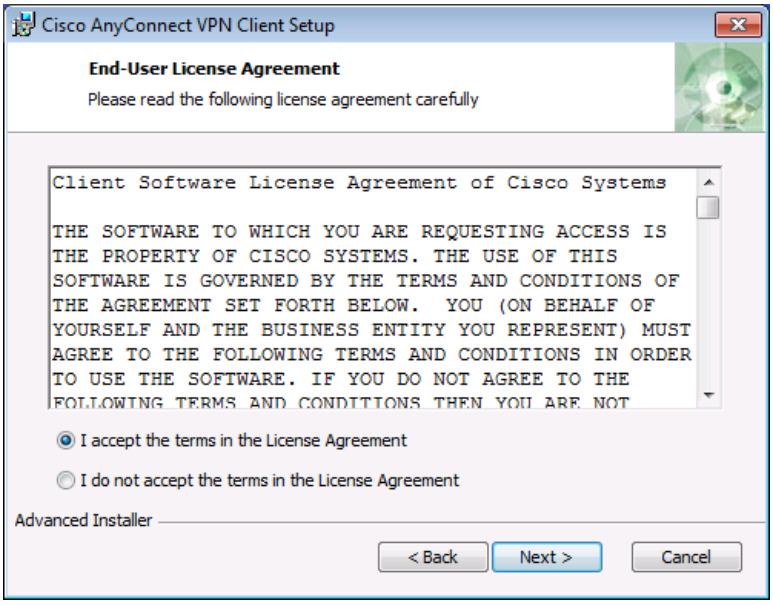
Install the AnyConnect VPN Client (if required).
On the Manual Installation screen, click AnyConnect VPN

After the download is complete, the Cisco AnyConnect VPN Client Setup starts. Click Next to continue.

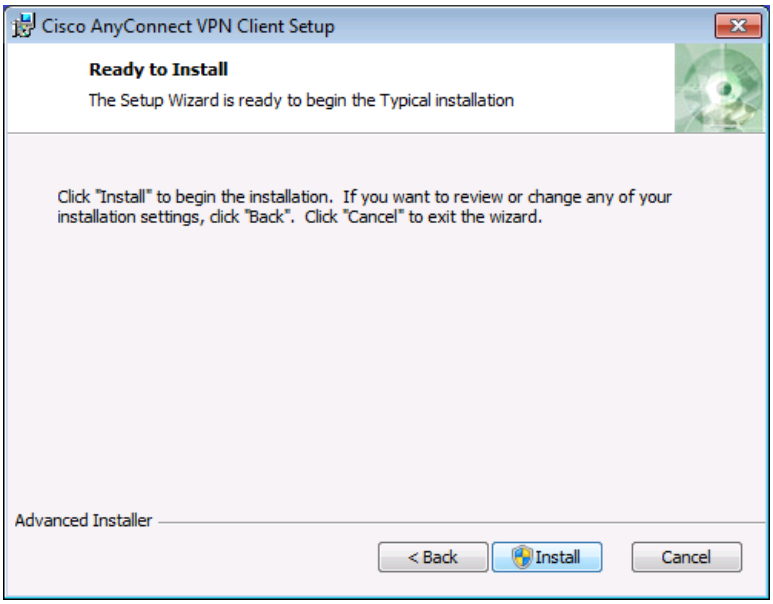




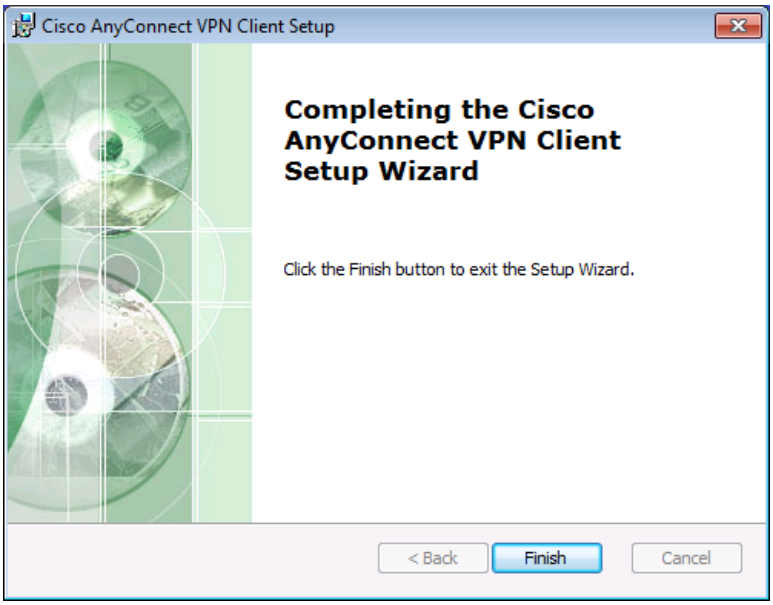
Read the End-User License Agreement. Select I accept the terms in the License Agreement and click Next to continue.



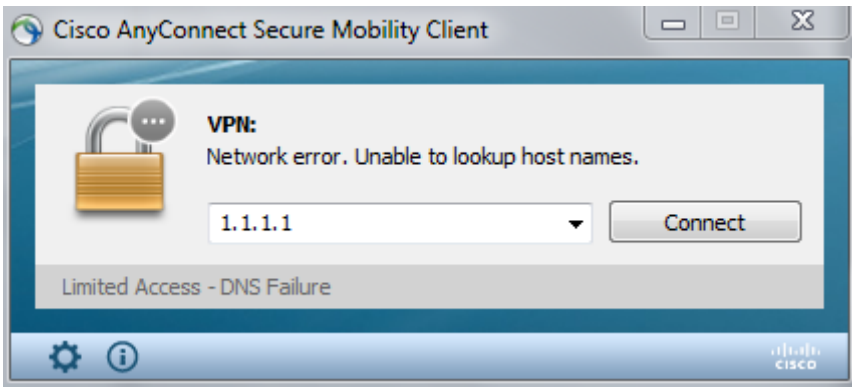
The Ready to Install window is displayed. Click Install to continue.



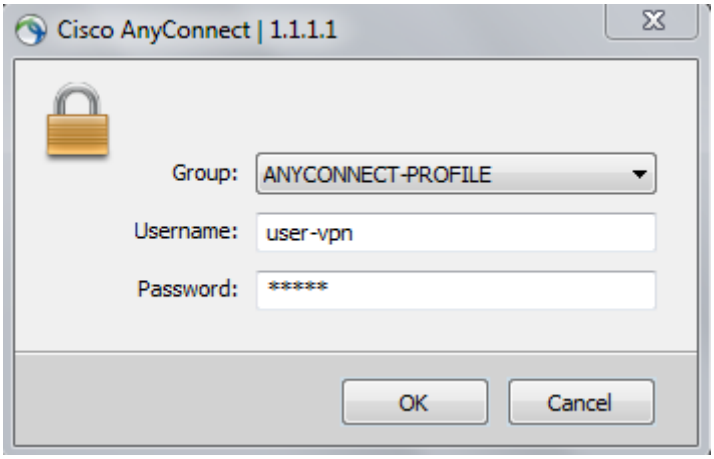
Click Finish to complete the installation.



Establish an AnyConnect SSL VPN Connection.
When prompted to enter the secure gateway address, enter 1.1.1.1 in the Connect field, and click Connect.



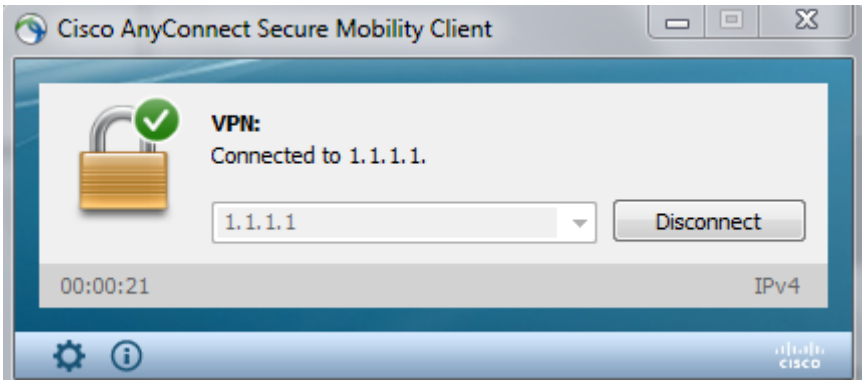
When prompted, enter user-vpn for the username and cisco as the password.



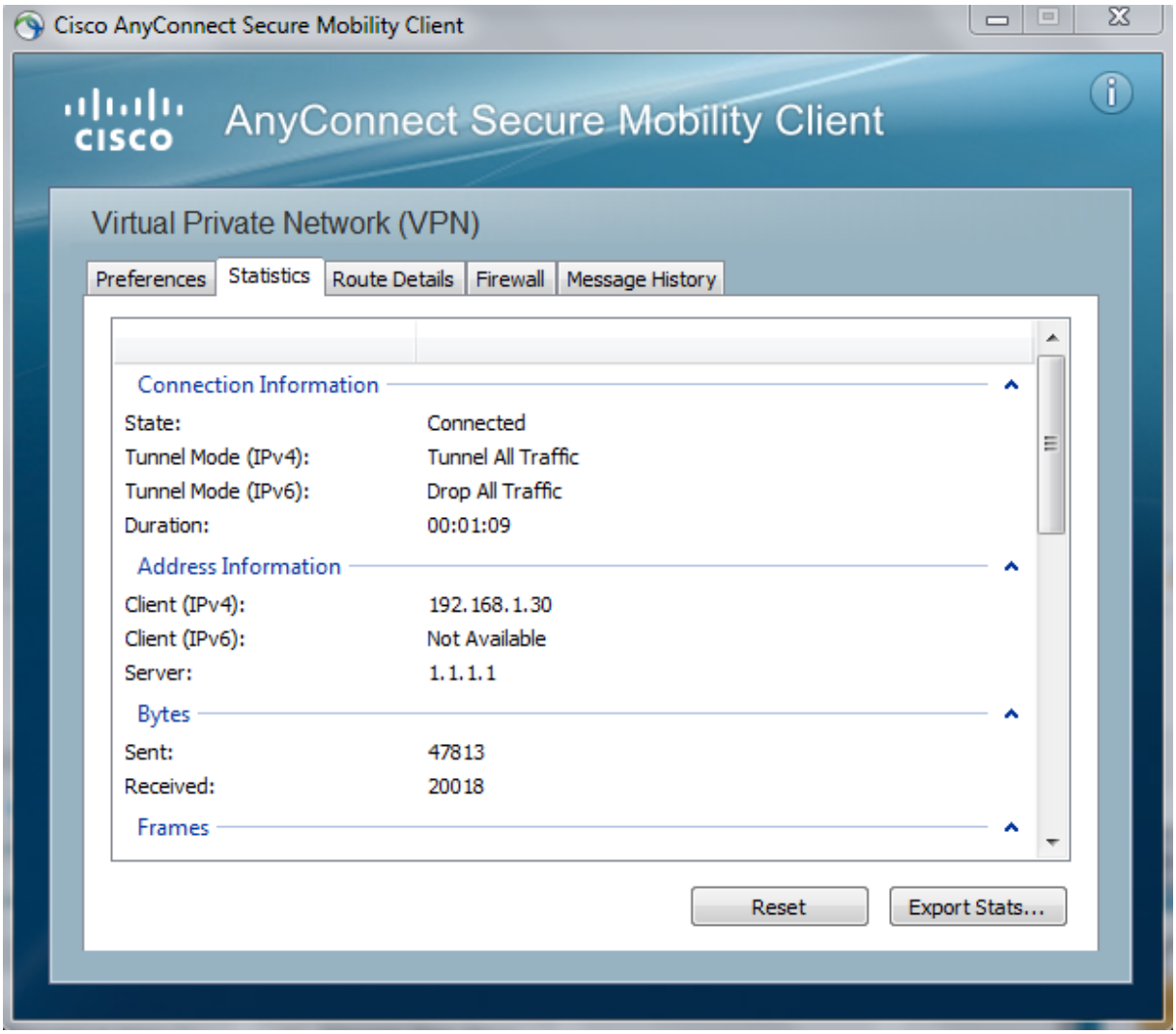
You should see this:

When the full tunnel SSL VPN connection is established, an icon will appear in the system tray that signifies that the client has successfully connected to the SSL VPN network.

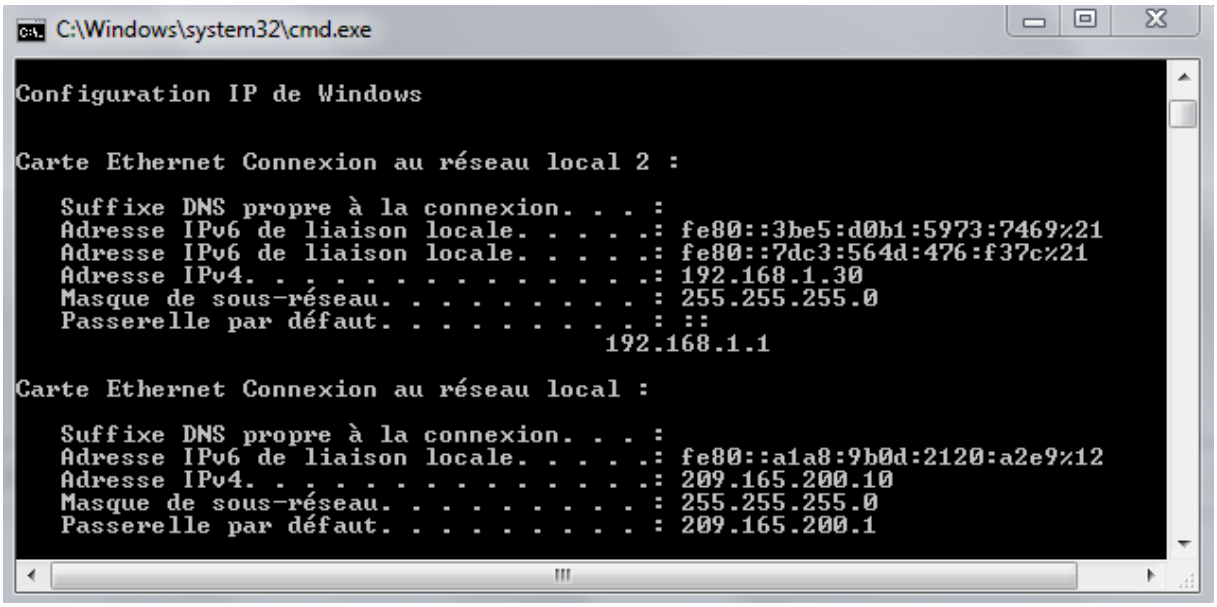
Click the gear icon at the bottom left corner of the Cisco AnyConnect Secure Mobility client window.



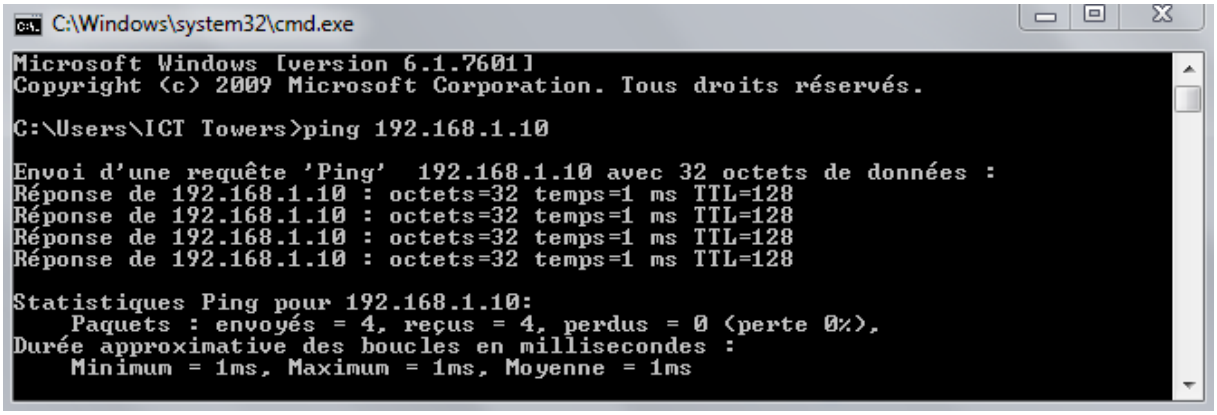
Use the scroll bar on the right side of the Virtual Private Network (VPN) – Statistics tab for additional connection information.
Note: The inside IP address that is assigned to the Outside Host is 192.168.1.30 which is selected from the VPN pool 192.168.1.30-40.



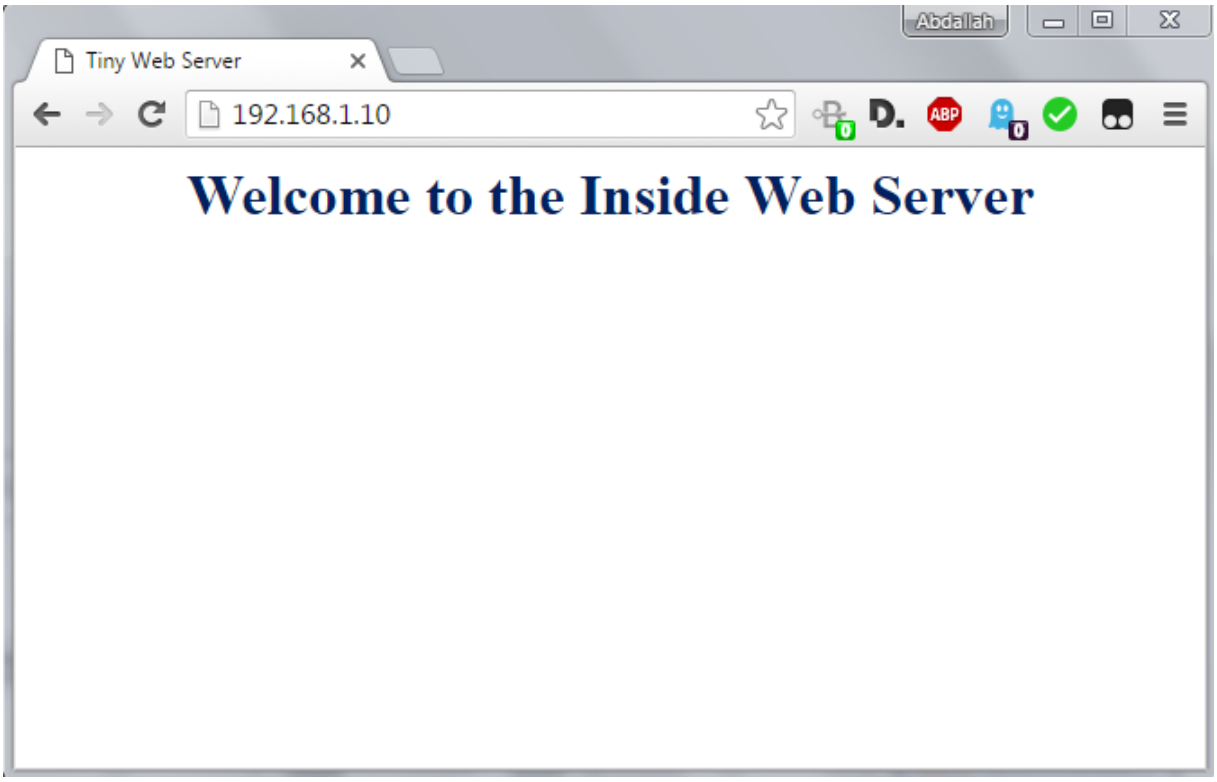
From a command prompt on the Outside Host, verify the IP addressing by using the ipconfig command. Notice that there are two IP addresses listed. One is for the Outside Host local IP address (209.165.200.10) and the other is the IP address assigned to the SSL VPN tunnel (192.168.1.30).



From Outside Host, ping PC-A (192.168.1.10) to verify connectivity.

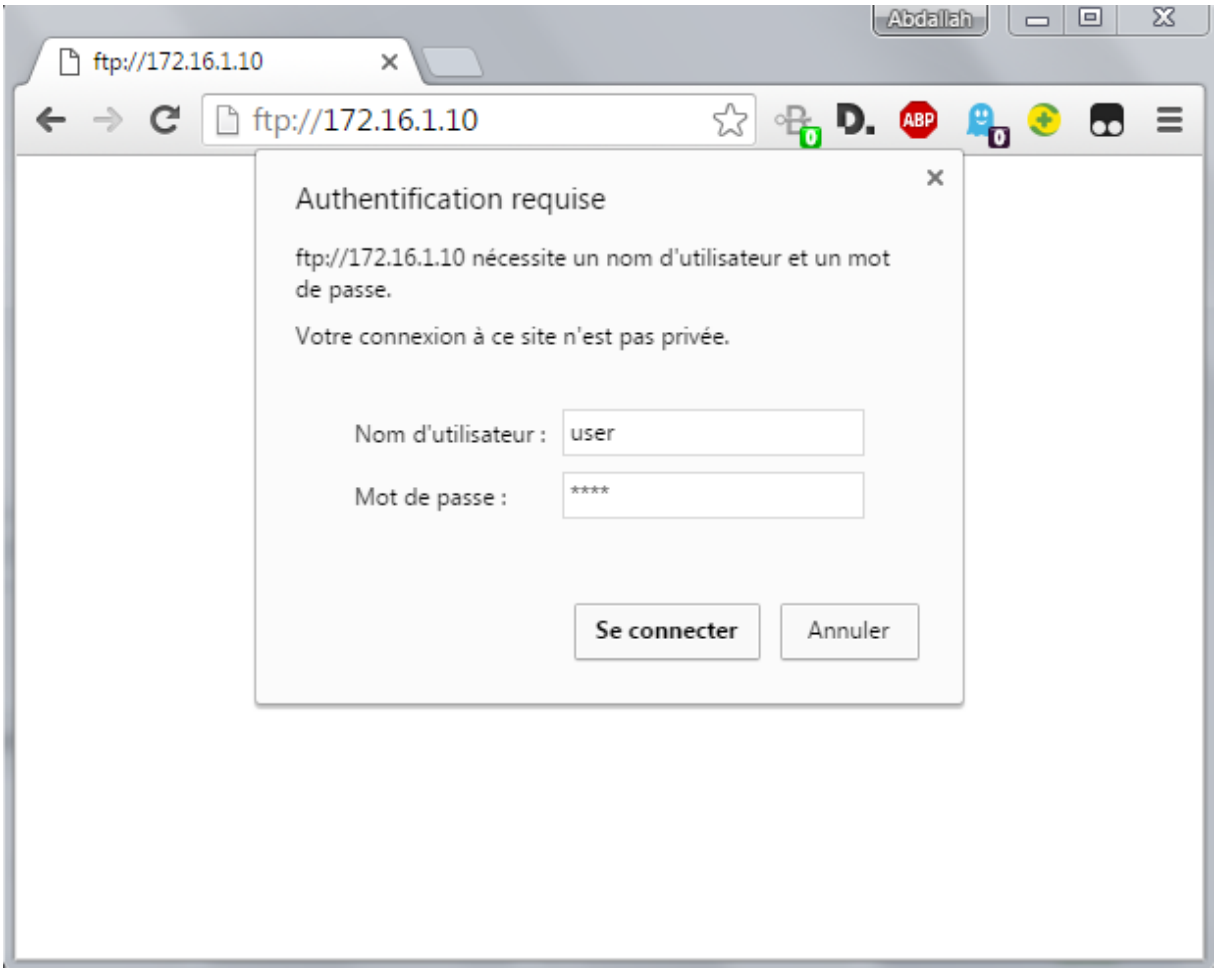


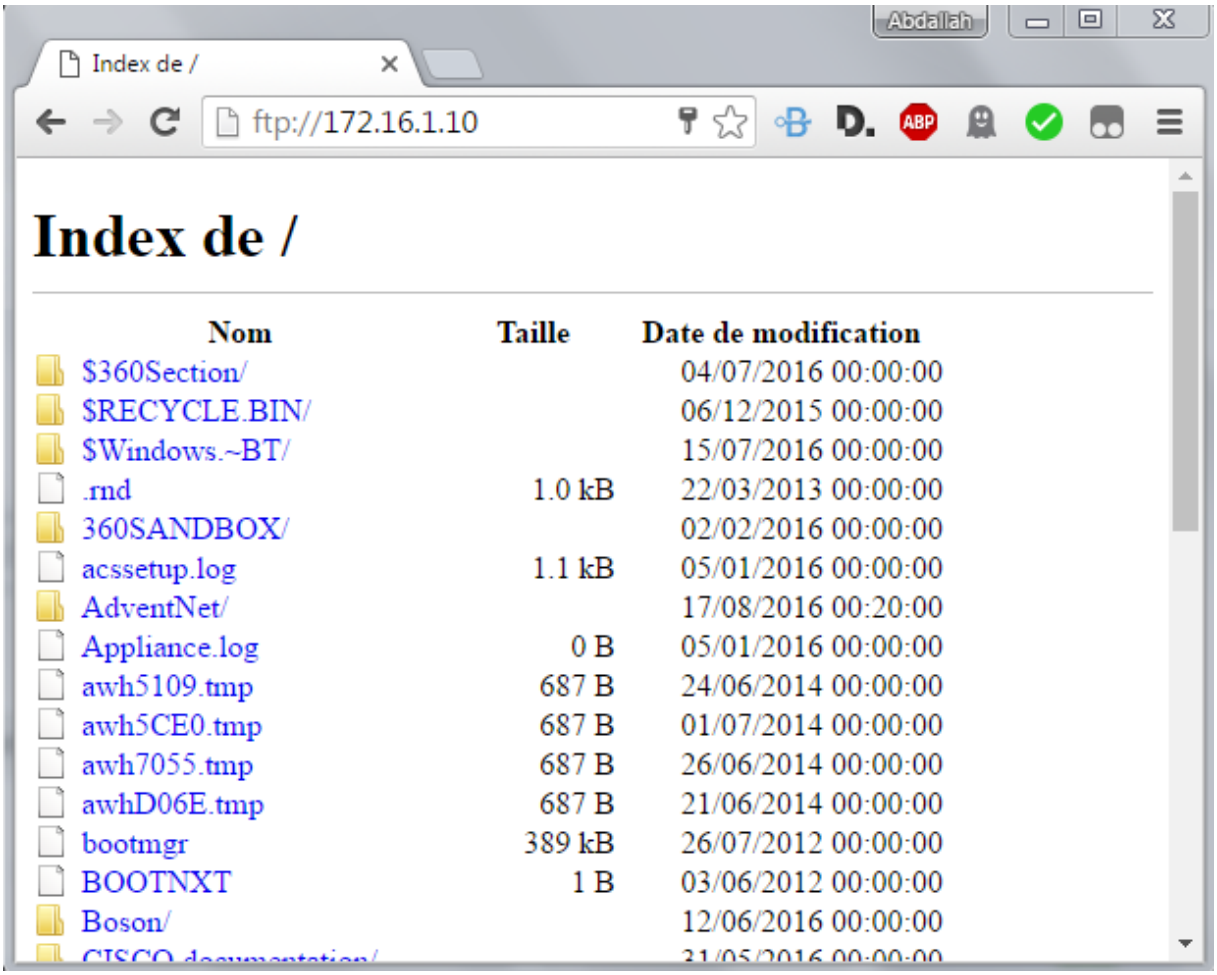
From Outside Host, open web browser and access the internal web site (http://192.168.1.10), the web page should be displayed successfully:



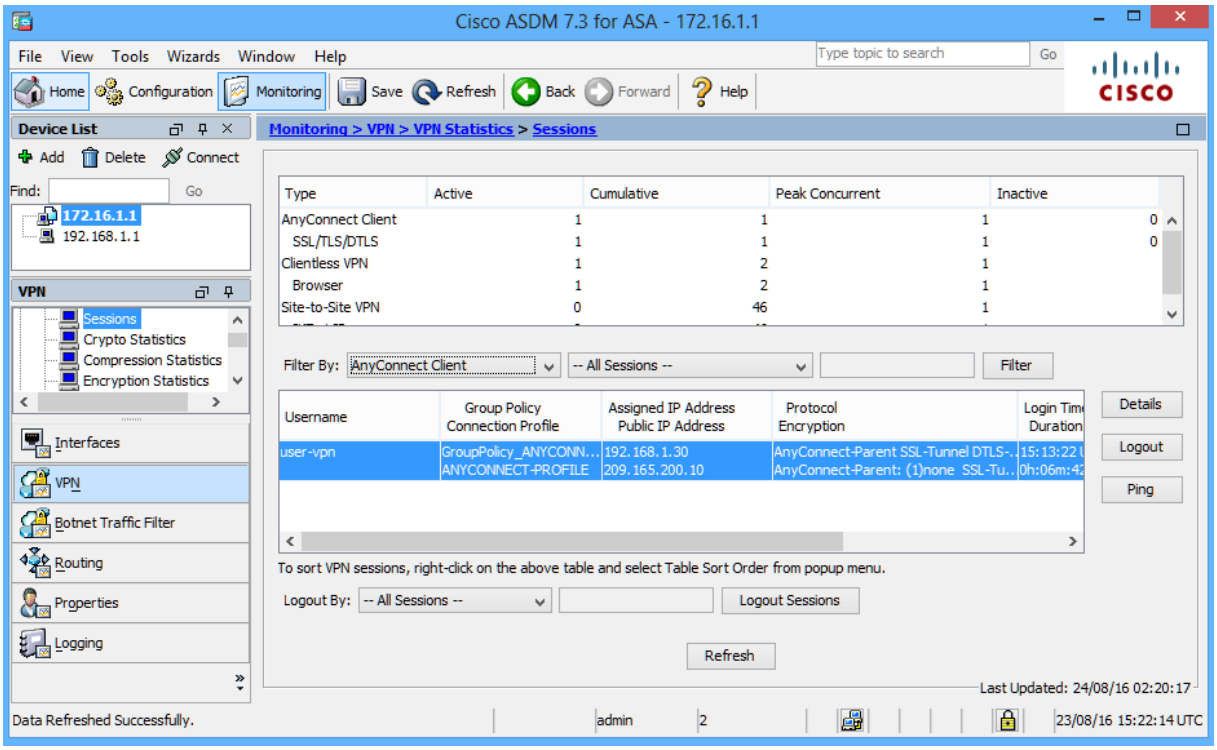
From Outside Host, ping DMZ-SERVER (172.16.1.10) to verify connectivity.

From Outside Host, open web browser and access the FTP Files located in the DMZ-SERVER (ftp://172.16.1.10), The access of the FTP Files requites authentication, enter the username user and the password cisco, the Outside Host should be able to view the FTP Files:


Abdallah
ftp://172.16.1.10
ftp://172.16.1.10
Authentification requise
ftp://172.16.1.10 nécessite un nom d'utilisateur et un mot de passe.
Votre connexion à ce site n'est pas privée.
Nom d'utilisateur :
user
Mot de passe :
****
Se connecter
Annuler



On the ASDM menu bar, click Monitoring and then select VPN > VPN Statistics > Sessions. Click the Filter By pull-down list and select AnyConnect Client. You should see the VPN user session logged in from Outside Host with IP address 209.165.200.10 which has been assigned an inside network IP address of 192.168.1.30 by the ASA.



Part-10: Configure the Site-to-Site IPsec VPN Tunnel between R1 and ASA

On R1:

Configure the ISAKMP policy parameters.
Create an ISAKMP policy with a priority number of 1.
Use the following parameters:

Authentication: pre-shared key
Encryption: AES
Hash algorithm: SHA
Diffie-Helman: group 2

```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 2
```

Configure the pre-shared key of cisco123 and point it to the ASA's outside interface IP address 1.1.1.1:

```
R1(config)#crypto isakmp key cisco123 address 1.1.1.1
```

Configure the IPsec transform set
Create a transform set with tag TRNSFRM-SET and use an ESP transform with an AES 256 cipher with ESP and the SHA hash function:

```
R1(config)#crypto ipsec transform-set TRNSFRM-SET esp-aes esp-sha-hmac
```

Define interesting traffic.
Configure the IPsec VPN interesting traffic ACL. Use extended access list number 101. The source network should be R1's LAN (10.1.1.0/24), and the destination network should be the ASA's LAN (192.168.1.0/24):

```
R1(config)#access-list 101 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Create and apply a crypto map.

Create the crypto map on R1, name it CMAP, and use 1 as the sequence number.
Use the match address command to specify which access list defines which traffic to encrypt, the ACL should be 101.
Set the peer address to the ASA's remote VPN endpoint interface IP address (1.1.1.1).
Set the transform set to TRNSFRM-SET.

```
R1(config)#crypto map CMAP 1 ipsec-isakmp
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set peer 1.1.1.1
R1(config-crypto-map)#set transform-set TRNSFRM-SET
```

Apply the crypto map to R1's g0/1 interface:

```
R1(config)# interface g0/1
R1(config-if)# crypto map CMAP
```

Task 1 : Configure Site-to-Site VPN on ASA using CLI

On ASA configure NAT exemption:

```
ciscoasa(config)#object network LOCAL-NET
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#object network REMOTE-NET
ciscoasa(config-network-object)#subnet 10.1.1.0 255.255.255.0
```

```
ciscoasa(config)#nat (inside,outside) source static LOCAL-NET LOCAL-NET
destination static REMOTE-NET REMOTE-NET
```

Configure the ISAKMP policy parameters.
Create an ISAKMP policy with a priority number of 10.
Use the following parameters:

Authentication: pre-shared key
Encryption: AES
Hash algorithm: SHA
Diffie-Helman: group 2

```
ciscoasa(config)# cryp isakmp policy 10
ciscoasa(config-ikev1-policy)# auth pre-share
ciscoasa(config-ikev1-policy)# encry aes
ciscoasa(config-ikev1-policy)# hash sha
```

```
ciscoasa(config-ikev1-policy)# group 2
```

Enable ISAKMP on the outside interface and Configure the IPsec VPN interesting traffic ACL. Use extended access list named VPN-ACL. The source network should be the ASA's LAN (192.168.1.0/24), and the destination network should be the R1's LAN (10.1.1.0/24):

```
ciscoasa(config)#crypto isakmp enable outside
ciscoasa(config)#access-list VPN-ACL per ip 192.168.1.0 255.255.255.0 10.1.1.0
255.255.255.0
```

Configure the Tunnel Group (LAN-to-LAN Connection Profile)

For a LAN-to-LAN tunnel, use the tunnel-group 2.2.2.1 type ipsec-l2l command to define the connection profile type ipsec-l2l.
In order to configure the ISAKMP preshared key, enter the tunnel-group ipsec-attributes configuration mode using the tunnel-group 2.2.2.1 ipsec-attribute command, 2.2.2.1 is R1's G0/1 interface, and configure the pre-shared key of cisco123:

```
ciscoasa(config)#tunnel-group 2.2.2.1 type ipsec-l2l
ciscoasa(config)#tunnel-group 2.2.2.1 ipsec-attribute
ciscoasa(config-tunnel-ipsec)#pre-shared-key cisco123
```

Configure the IPsec Transform Set
Create a transform set named TEST and use an ESP transform with an AES 256 cipher with ESP and the SHA hash function:

```
ciscoasa(config)# crypto ipsec transform-set TEST esp-aes esp-sha-hmac
```

Configure a Crypto Map and Apply it to an Interface
crypto map defines an IPSec policy to be negotiated in the IPSec SA with R1 and should includes:

The ACL VPN-ACL that identifies the packets that the IPSec connection protects.
Peer address pointed to to the R1's remote VPN endpoint interface IP address (2.2.2.1).
The IPsec transform set named TEST.

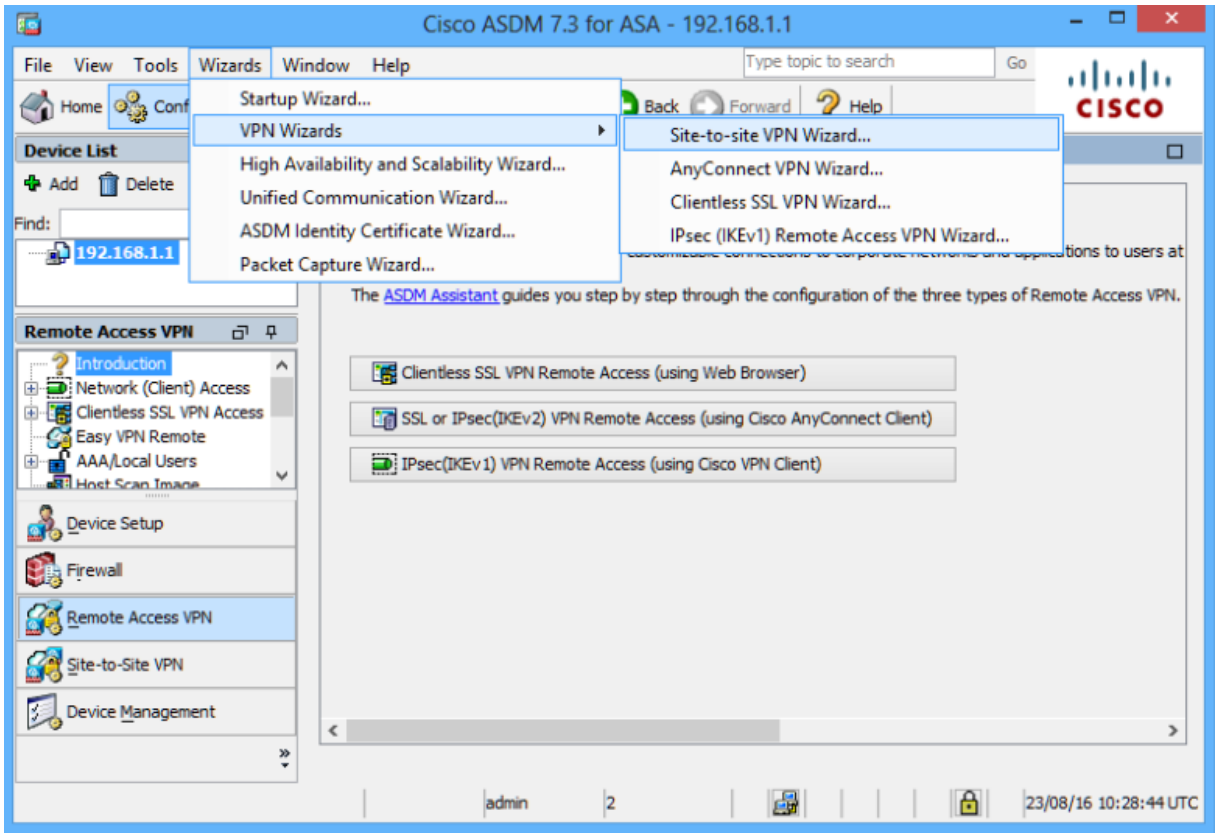
```
ciscoasa(config)# crypto map CRYPTO-MAP 1 match address VPN-ACL
ciscoasa(config)# crypto map CRYPTO-MAP 1 set peer 2.2.2.1
ciscoasa(config)# crypto map CRYPTO-MAP 1 set transform-set TEST
```

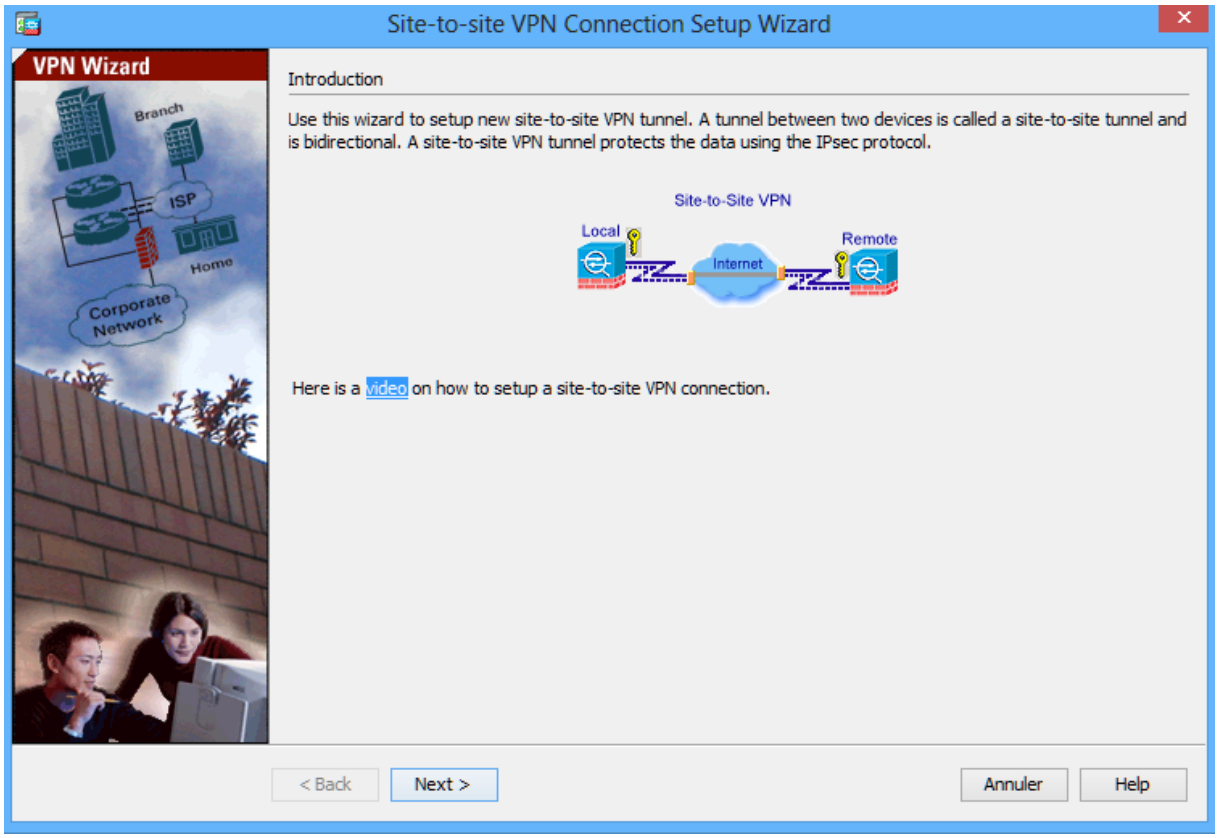
Apply the crypto map to the ASA's outside interface:

```
ciscoasa(config)# crypto map CRYPTO-MAP interface outside
```

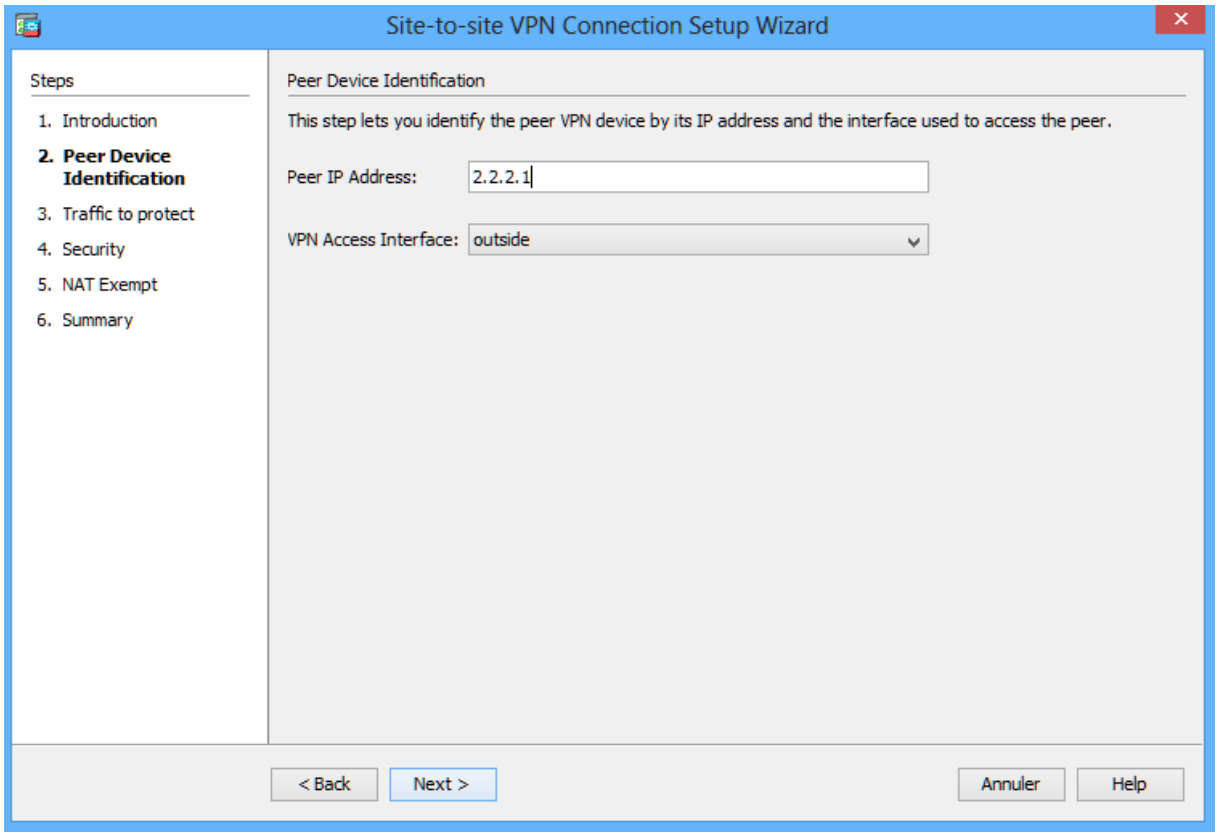
Task 2: Configure Site-to-Site VPN on ASA using ASDM

Using ASDM. Use the Site-to-Site VPN Wizard to configure the ASA for IPsec site-to-site VPN.

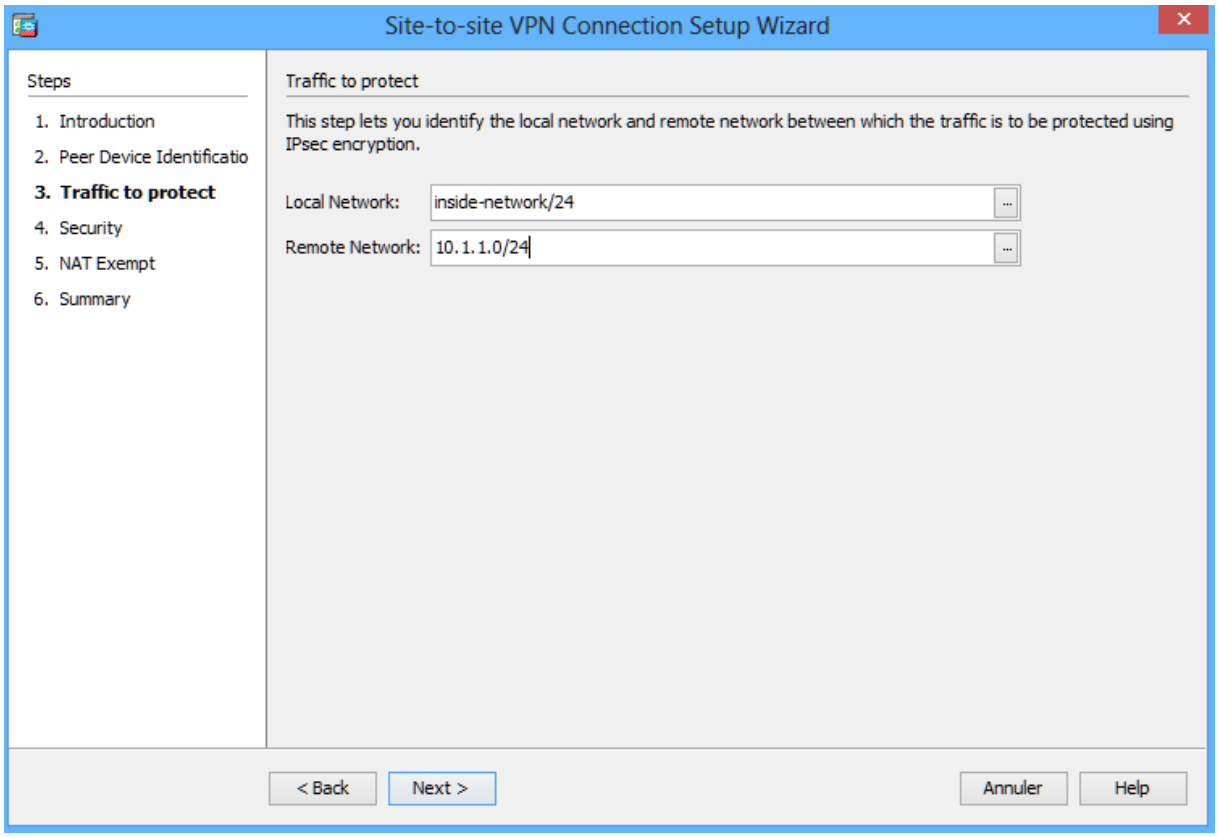




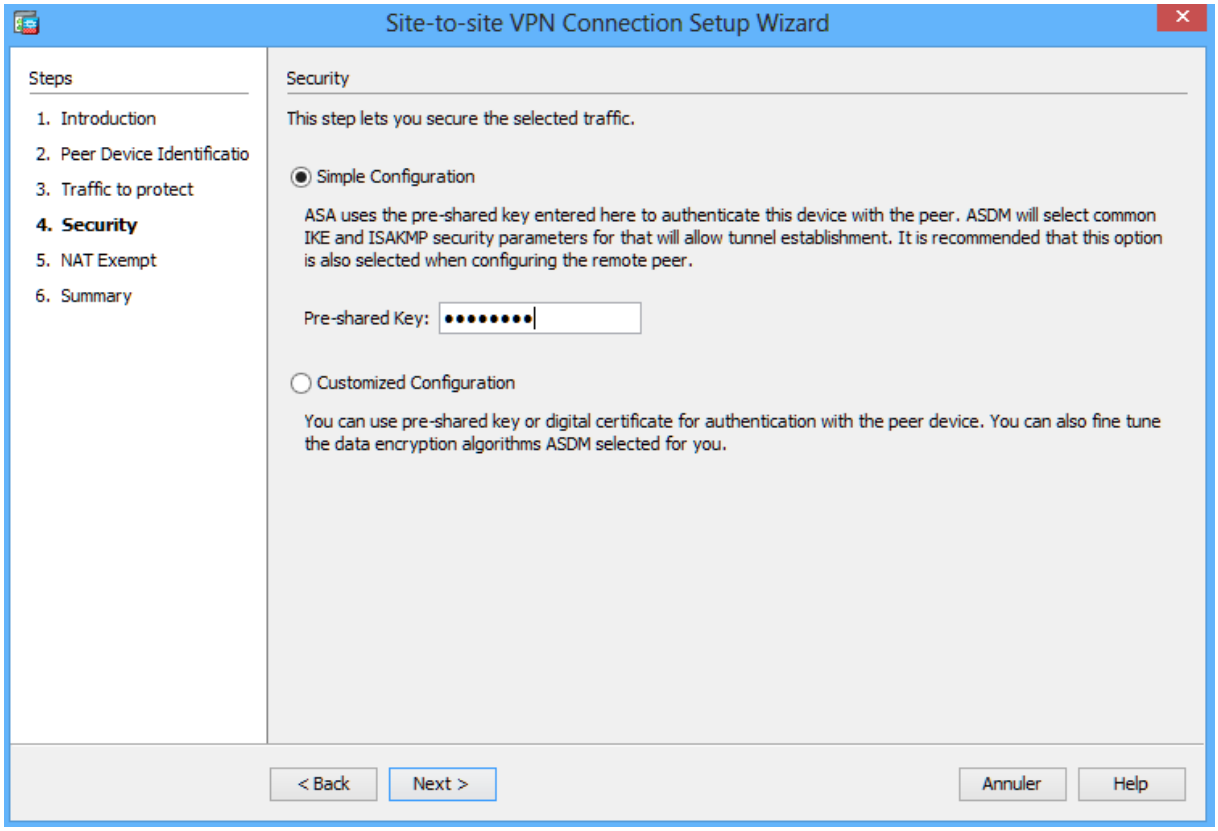
Set the Peer IP Address to R1's G0/1 IP address (2.2.2.1). Verify that outside is selected for the VPN Access Interface.



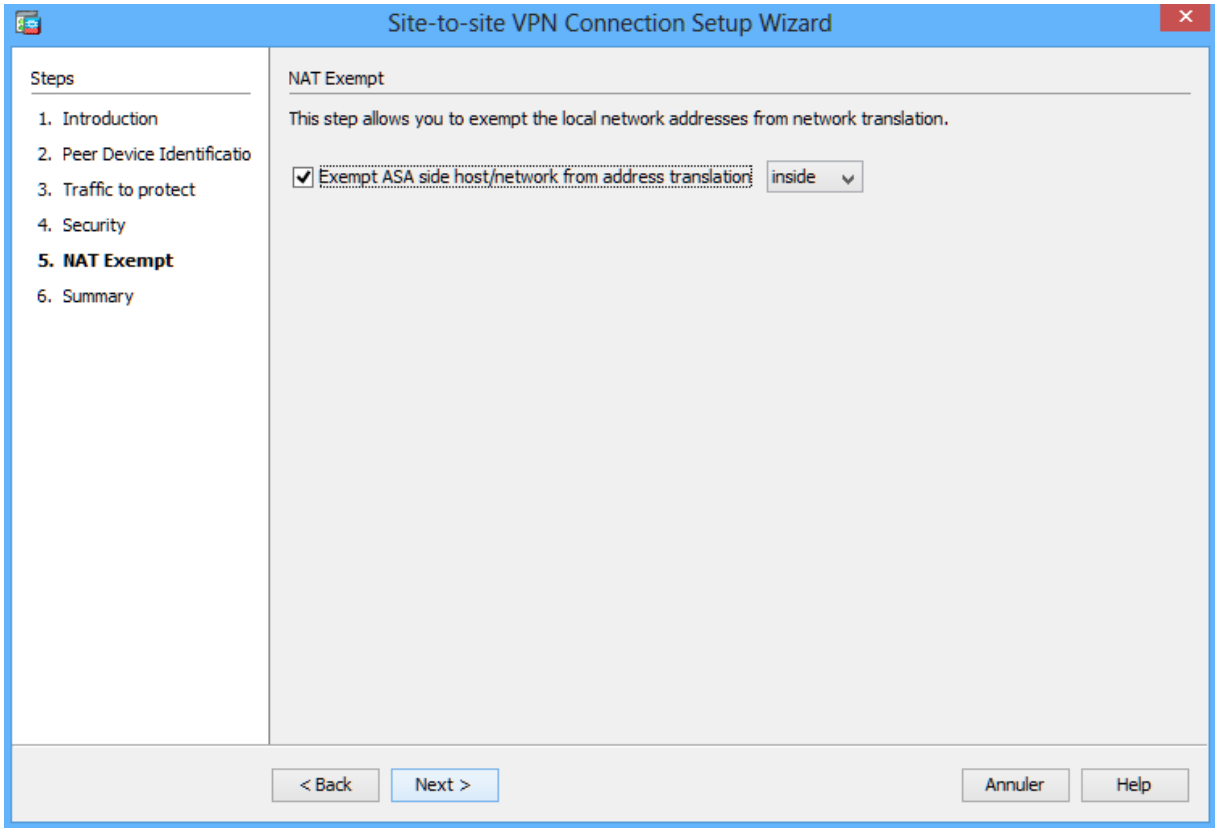
Identify the traffic to protect. Set the Local Network to inside-network/24 and the Remote Network to 172.16.3.0/24.



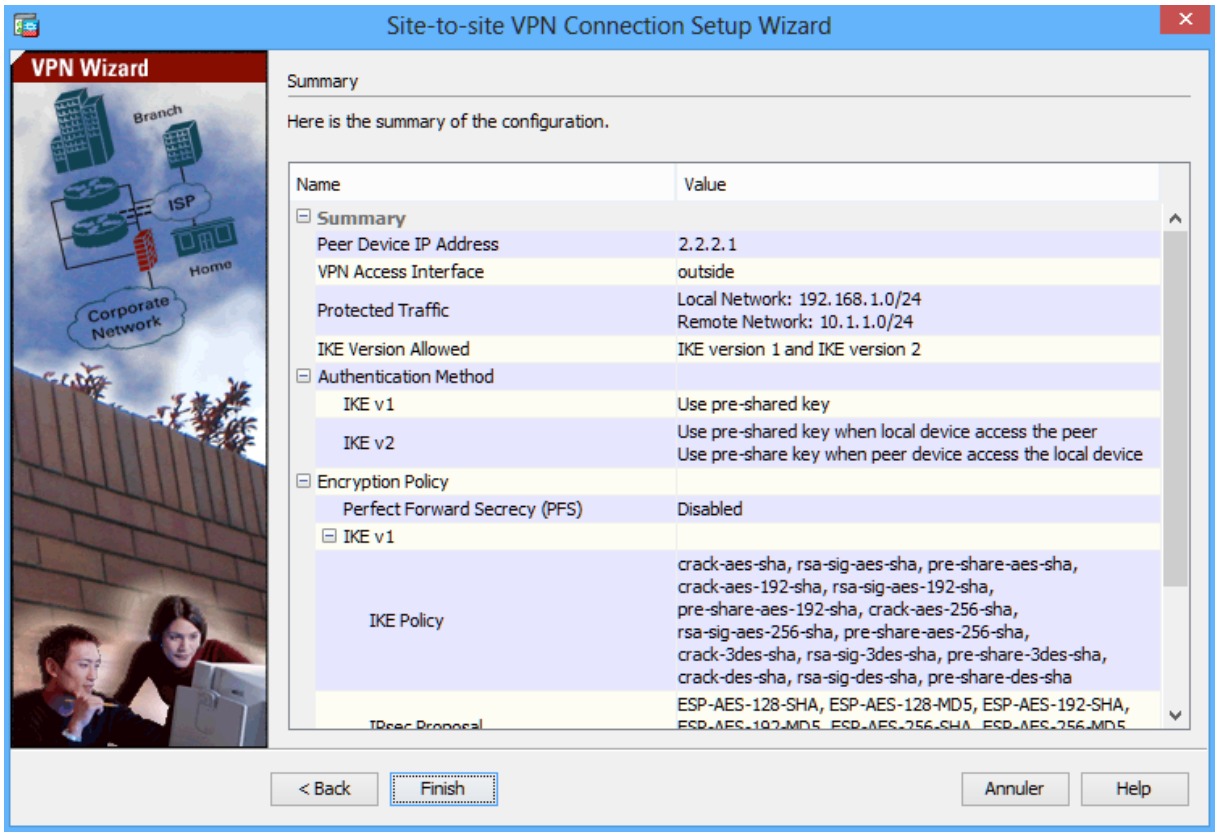
Configure the pre-shared key. Enter the Pre-shared Key of cisco123.

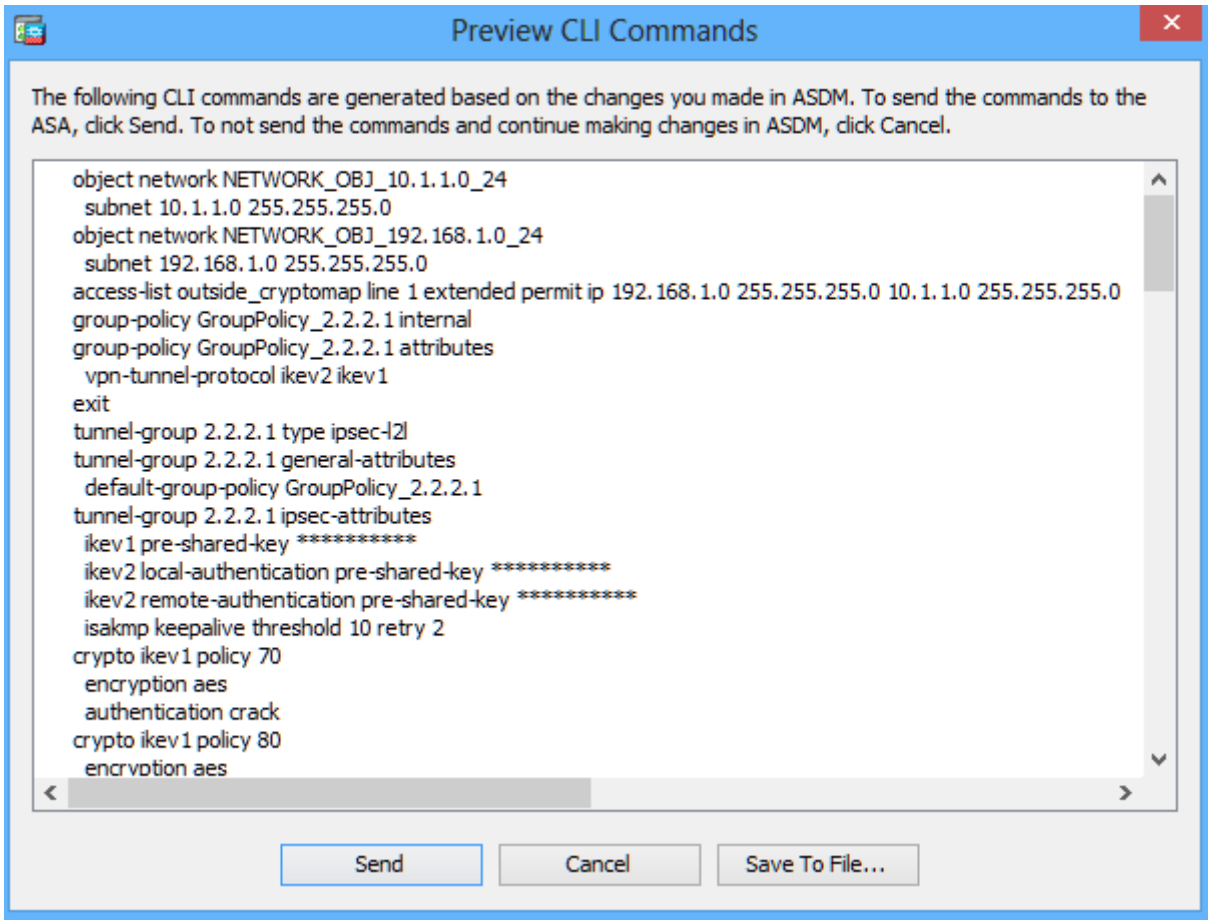


Enable NAT exemption. Check the Exempt ASA side host/network from address translation box and verify that the inside interface is selected.



Apply IPsec configuration to the ASA.
Click Finish to apply the site-to-site configuration and send the commands to the ASA.





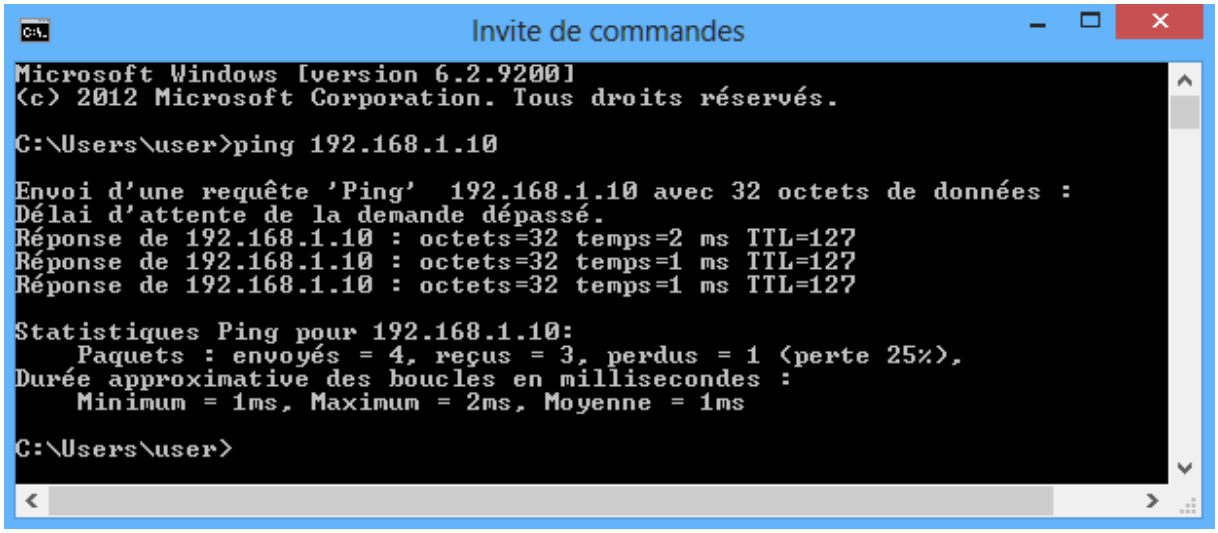
Verify the IPsec Association Security using the show crypto ipsec sa command, there are no packets encrypted/decrypted:

```
R1#show crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: CMAP, local addr 2.2.2.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 1.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

local crypto endpt.: 2.2.2.1, remote crypto endpt.: 1.1.1.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x0(0)
     PFS (Y/N): N, DH group: none
```

```
inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:
R1#
```

Let's test IPsec protected tunnel, from PC-B (10.1.1.10) ping the PC-A (192.168.1.10):

The ping is successfull as shown below:



Verify the ISAKMP policy, the association security for phase 1 is negociated successfully between R1 and ASA:

ISAKMP phase 1 on R1:

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
1.1.1.1         2.2.2.1         QM_IDLE           1014 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

ISAKMP phase 1 on ASA:

```
ciscoasa# show crypto isakmp sa

IKEv1 SAs:
```

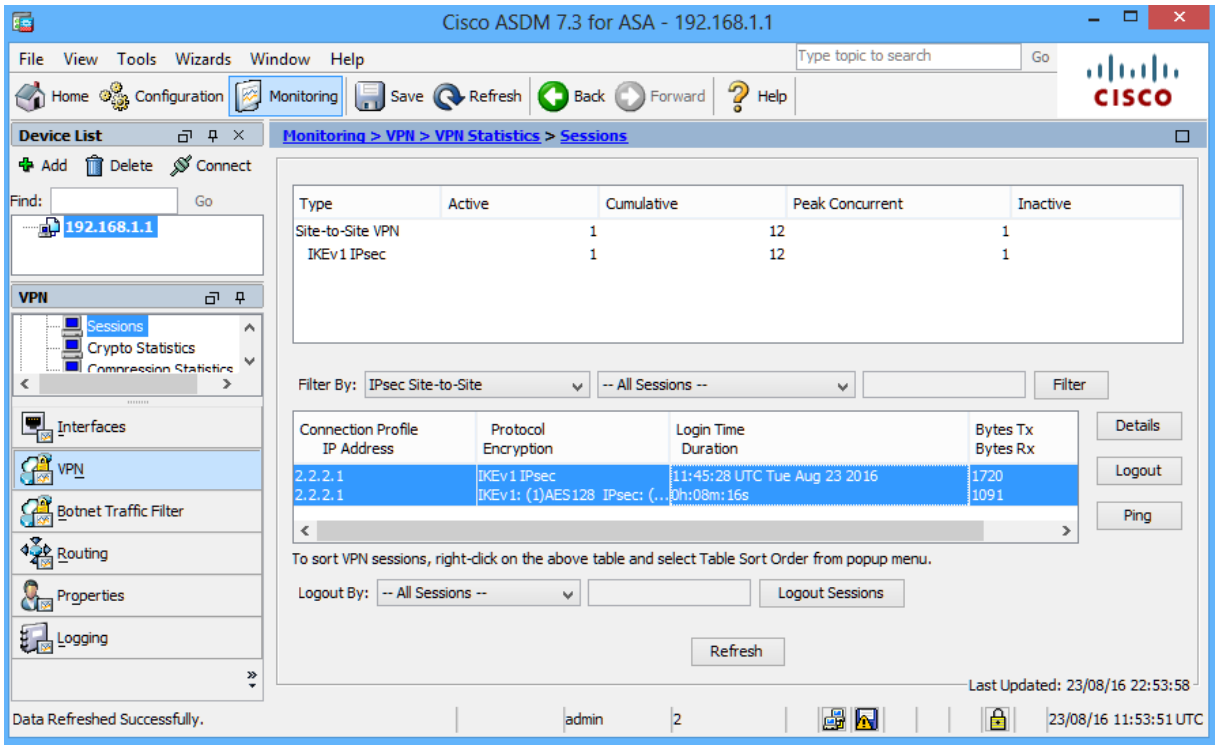
```
   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 2.2.2.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Verify the IPsec Association Security using the show crypto ipsec sa command once again, now the number of packets encrypted/decrypted is increased, since the first icmp packet is lost, three packets are encrypted/decrypted:

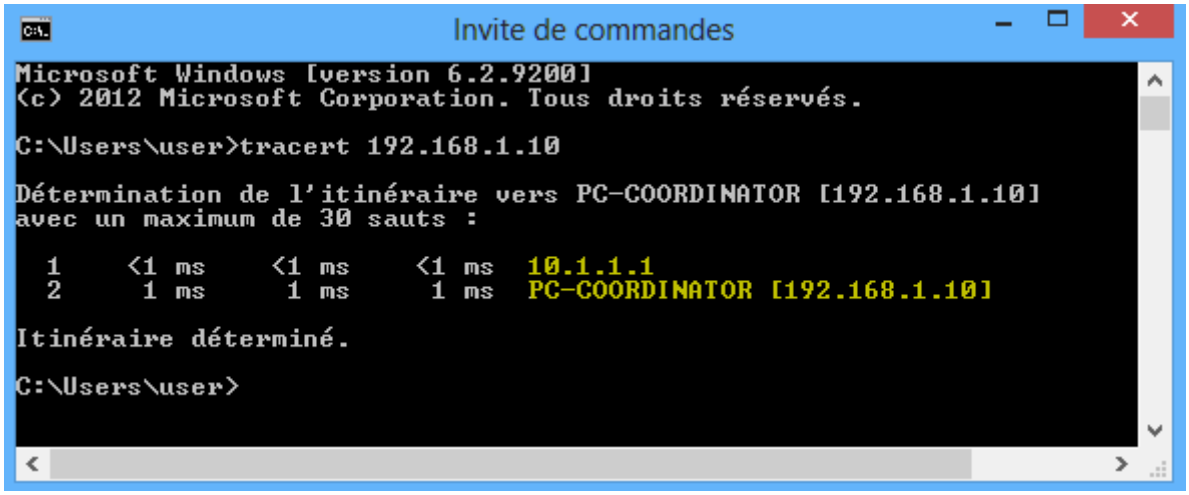
```
R1#show crypto ipsec sa | i local|remote|pkts
    Crypto map tag: CMAP, local addr 2.2.2.1
local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
local crypto endpt.: 2.2.2.1, remote crypto endpt.: 1.1.1.1
R1#
```

```
ciscoasa# show crypto ipsec sa | i local|remote|pkts
    Crypto map tag: outside_map, seq num: 1, local addr: 1.1.1.1
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 3, #pkts comp failed: 0, #pkts decomp failed: 0
local crypto endpt.: 1.1.1.1/0, remote crypto endpt.: 2.2.2.1/0
ciscoasa#
```

From ASDM , click the Monitoring>VPN menu. A connection profile IP address of 2.2.2.1 should be displayed in the middle of the screen. Click the Details button to see IKE and IPsec session details.:

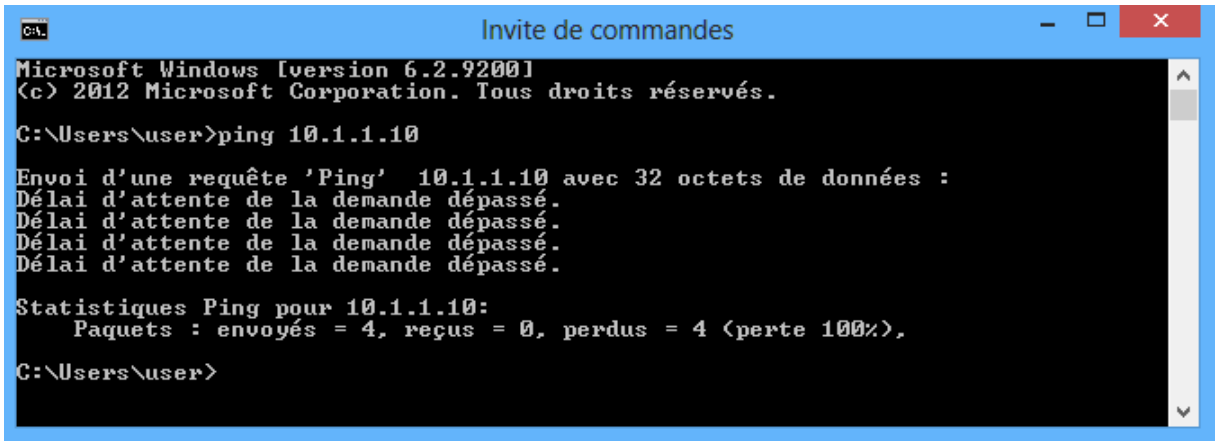


From PC-B, issue the command tracert 192.168.1.10. If the site-to-site VPN tunnel is working correctly, you will not see traffic being routed through R2 (2.2.2.2).



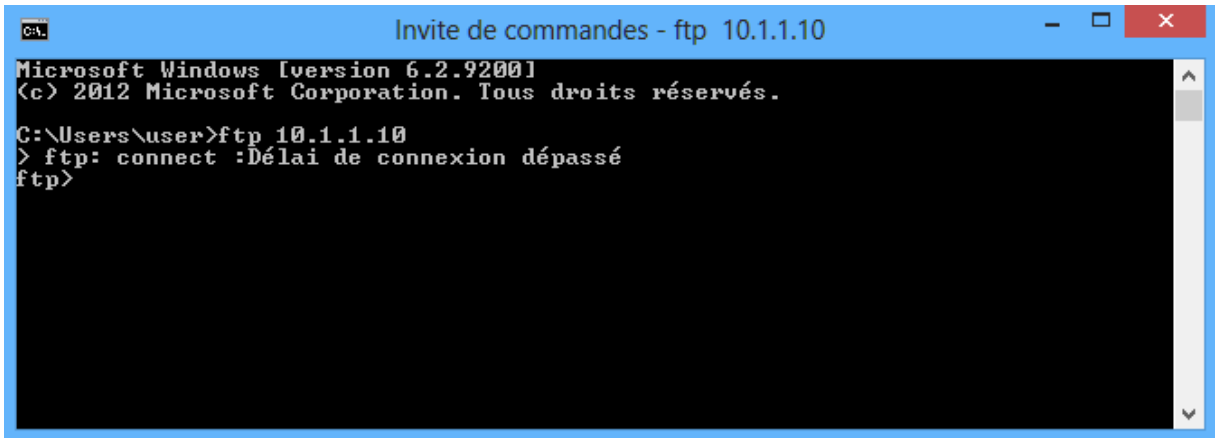
Part-11: Let's try ping from PC-A (192.168.1.10) to PC-B (10.1.1.10):

The ping fails, the PC-B cannot ping PC-A as shown below:



Let's do another test, on PC-B activate FTP Server and try to access FTP files from PC-A:

The PC-A cannot access the FTP files located on PC-B as shown below:



The reason behind this is that there is no zone pair that allows the traffic initiated from OUTSIDE zone to INSIDE zone.

Zone pairs apply policy enforcement to traffic flowing from one security zone to another. A zone pair must be defined for each direction in which traffic is allowed to be *initiated*. In this example , we have configured a zone par called "IN-TO-OUT" so that the INSIDE network can initiate UDP, TCP and ICMP traffic to the OUTSIDE, but no traffic may be initiated from the OUTSIDE to the INSIDE network. If there exists a requirement for traffic to be initiated from the OUTSIDE zone to the INSIDE zone, a second zone pair (in the opposite direction) must also be created.

Let's configure a second zone pair to inspect the FTP and ICMP traffic from OUTSIDE to INSIDE:

Create an numbered ACL 100 to match the FTP and ICMP traffic:

```
R1(config)#access-list 100 permit tcp any any eq ftp
R1(config)#access-list 100 permit tcp any any eq ftp-data
R1(config)#access-list 100 permit icmp any any
```

Create a class map called OUTSIDE-TRAFFIC and associate the previous ACL to identify the FTP and ICMP traffic:

```
R1(config)#class-map type inspect OUTSIDE-TRAFFIC
R1(config-cmap)#match access-group 100
```

Now configure a policy map called OUT-IN-POLICY, Bind the OUTSIDE-TRAFFIC class-map to the policy-map. All FTP and ICMP packets matched by the OUTSIDE-TRAFFIC class-map will be inspected:

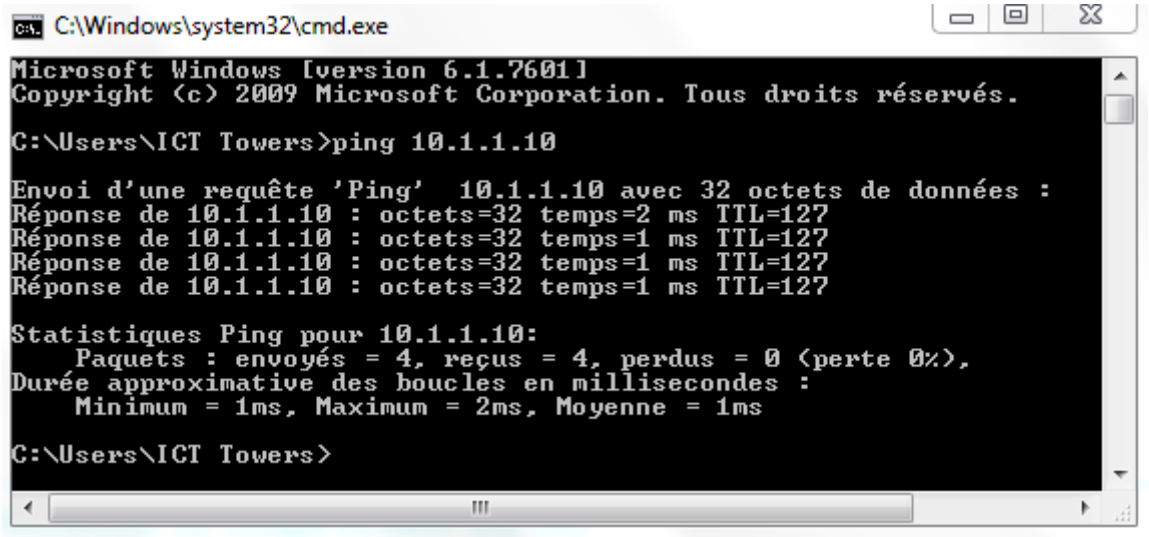
```
R1(config)#policy-map type inspect OUT-IN-POLICY
R1(config-pmap)#class OUTSIDE-TRAFFIC
R1(config-pmap-c)#inspect
```

Create a zone-pair called OUT-TO-IN that allows traffic initiated from the OUTSIDE network to the INSIDE network and apply the policy-map to the zone-pair:

```
R1(config)#zone-pair security OUT-TO-IN source OUTSIDE destination INSIDE
R1(config-sec-zone-pair)#service-policy type inspect OUT-IN-POLICY
```

Let's try ping once again from PC-A (192.168.1.10) to PC-B (10.1.1.10):

The ping is successfull:

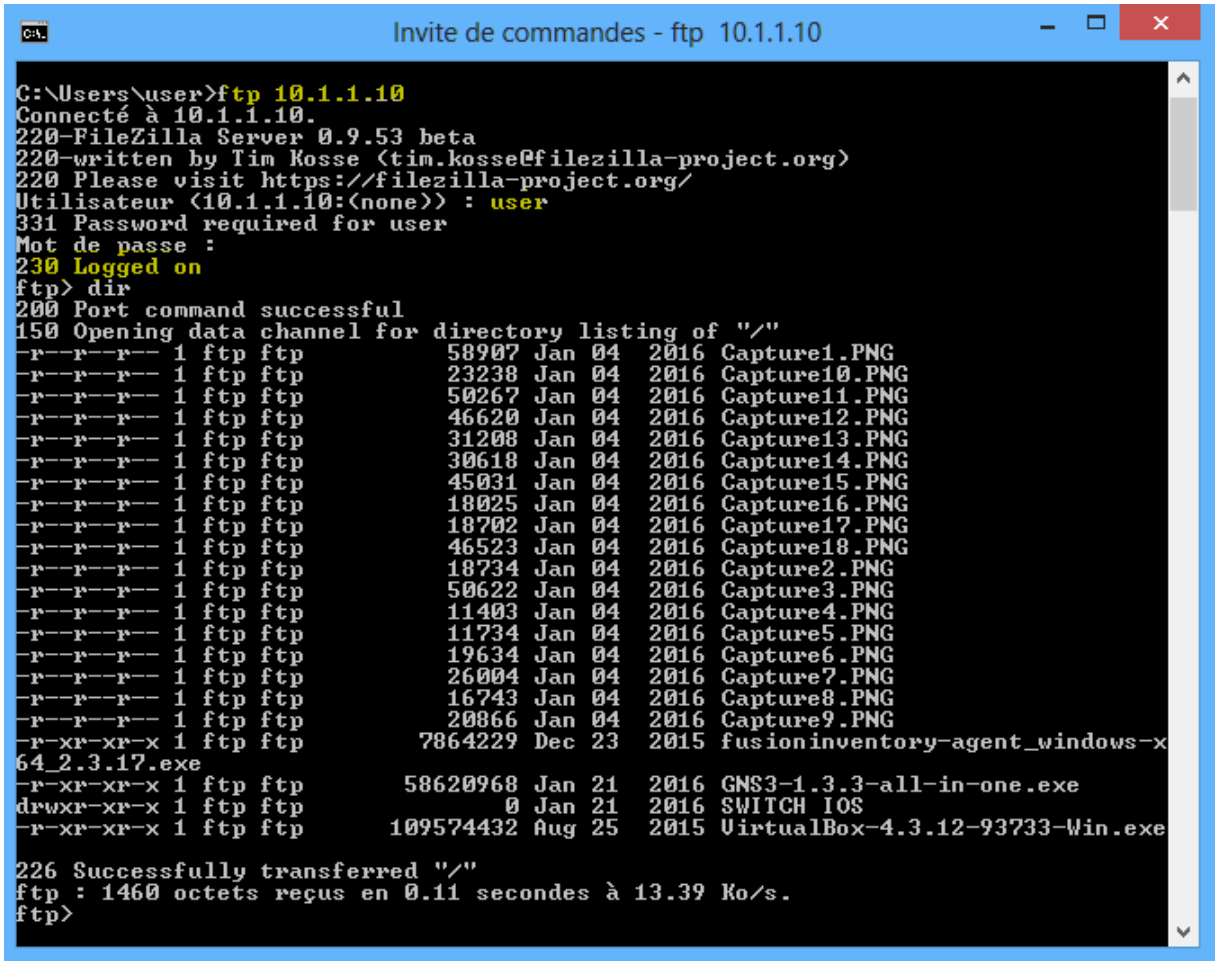


Verify the ZBF configuration by using show policy-map type inspect zone-pair OUT-TO-IN sessions command:

```
R1#show policy-map type inspect zone-pair OUT-TO-IN sessions

policy exists on zp OUT-TO-IN
Zone-pair: OUT-TO-IN

Service-policy inspect : OUT-IN-POLICY

    Class-map: OUTSIDE-TRAFFIC (match-all)
```

```
      Match: access-group 100

   Inspect

Number of Established Sessions = 1
Established Sessions
Session 2884F8E0 (192.168.1.10:8)=>(10.1.1.10:0) icmp SIS_OPEN
Created 00:00:03, Last heard 00:00:00
ECHO request
          Bytes sent (initiator:responder) [128:128]


    Class-map: class-default (match-any)
      Match: any
      Drop
        63 packets, 3236 bytes
R1#
```

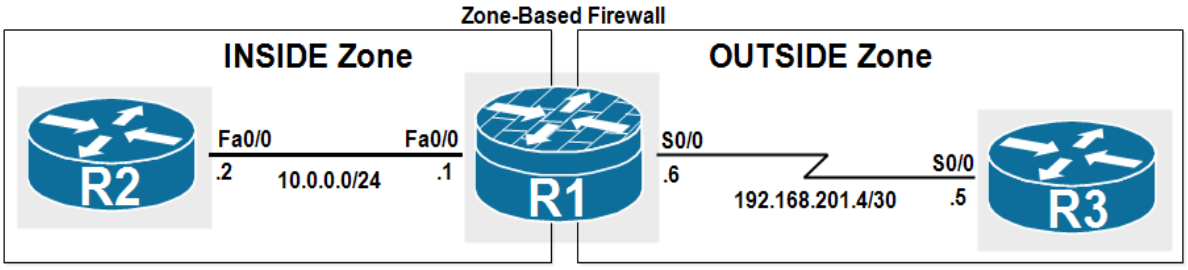
Let's try to access the FTP files located on PC-B:
The PC-A can access the FTP files:



Verify the ZBF configuration by using show policy-map type inspect zone-pair OUT-TO-IN sessions command:

```
R1#show policy-map type inspect zone-pair OUT-TO-IN sessions

policy exists on zp OUT-TO-IN
Zone-pair: OUT-TO-IN

Service-policy inspect : OUT-IN-POLICY

    Class-map: OUTSIDE-TRAFFIC (match-all)
      Match: access-group 100

   Inspect

Number of Established Sessions = 1
Established Sessions
Session 28851160 (192.168.1.10:27102)=>(10.1.1.10:21) tcpSIS_OPEN/TCP_ESTAB
Created 00:00:59, Last heard 00:00:52
          Bytes sent (initiator:responder) [55:308]


    Class-map: class-default (match-any)
      Match: any
      Drop
        63 packets, 3236 bytes
R1#
```

Lab 2: Zone-Based Firewall Scenario-1



R1 is configured with the Zone-Based Firewall:

Policy for the traffic from inside to outside:

Create a zones on R1, one dedicated to the inside hosts ,another zone dedicated to the outside hosts:

```
zone security Inside
 description Inside network
zone security Outside
 description Outside network
```

We will identify the traffic using class-map ,for example we want specify the traffic HTTP HTTPS ICMP and SSH are permitted to any destination on the Internet:

```
class-map type inspect match-any InternetTraffic
 match protocol http
 match protocol icmp
 match protocol https
 match protocol ssh
```

Match-any is the equivalent of OR Logic.
match-all is the equivalent of AND Logic,for example if we want identify a list of protocol toward a set of IP Addresses we must use the match-all keyword ,for example:

```
class-map type inspect match-any ServerInternet
 match protocol http
 match protocol https
!
class-map type inspect match-all INTERNET
 match class-map ServerInternet
 match access-group name Servers
!
ip access-list extended Servers
```

```
 permit ip any host 172.16.0.1
 permit ip any host 172.16.0.2
```

Notice the servers with the ip addresses 172.16.0.1 and 172.16.0.2 anywhere in the internet network.

After defining the traffic classes, we must take an action using policy-map:

Here we want:
-Inspect all traffic in class-map InternetTraffic.
-Drop and log all the other traffic.

```
policy-map type inspect InsideToOutside
 class type inspect InternetTraffic
  inspect
 class class-default
  drop log
```

The class class-default matches all traffic not identified in the class-map configured above

After configuring the policy-map ,we configure the zone-pair in order to tell to the router where to applay the policy, the zone-pair must match the policy-map configured above,in this case the traffic defined in the class-map must be inspected from the source inside to the destination outside:

```
zone-pair security InsideToOutside source Inside destination Outside
 service-policy type inspect InsideToOutside
```

Finally we assign the zone security to the interfaces (the interface facing the inside zone and the interface facing the outside to be member of these zones:

```
interface FastEthernet0/0
 zone-member security Inside
!
interface s0/0
 zone-member security Outside
```

Before verifying the Zone-Based Firewall let' verify the icmp http telnet traffic toward the outside:

Here the ping from R2 to R4 is successfully:

```
R2#ping 192.168.201.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/52/88 ms
R2#
```

The telnet from R2 to R4 works well:

```
R2#telnet 192.168.201.5
Trying 192.168.201.5 ... Open


User Access Verification

Username: admin
Password:
R4#
```

And the http traffic works well:

```
R2#telnet 192.168.201.5 80
Trying 192.168.201.5, 80 ... Open

^C
HTTP/1.1 400 Bad Request
Date: Fri, 01 Mar 2002 00:44:10 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 192.168.201.5 closed by foreign host]
R2#
```

Now we will configure the ZBF as written above:

We can ping from R2 to R4 because the ICMP traffic is defined in the class-map to be inspected:

```
R2#ping 192.168.201.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.5, timeout is 2 seconds:
!!!!!
R2#
```

The traffic telnet now is not allowed from R2 to R4 because telnet traffic matches the class class-default configured with drop action in the policy-map,notice below the log displayed on R1 which explain which traffic is initiated (the port 23) and The action taken and the zone-pair or the direction of the traffic :

```
R2#telnet 192.168.201.5
Trying 192.168.201.5 ...
% Connection timed out; remote host not responding
R2#
```

```
R1(config-if)#
*Mar  1 00:49:06.719: %FW-6-DROP_PKT: Dropping Other session 10.0.0.2:35563
192.168.201.5:23 on zone-pair InsideToOutside class class-default due to DROP
action found in policy-map with ip ident 27220
R1(config-if)#
*Mar  1 00:51:06.211: %FW-6-LOG_SUMMARY: 2 packets were dropped from
10.0.0.2:35563 => 192.168.201.5:23 (target:class)-(InsideToOutside:class-default)
*Mar  1 00:51:06.211: %FW-6-LOG_SUMMARY: 2 packets were dropped from
10.0.0.2:55928 => 192.168.201.5:23 (target:class)-(InsideToOutside:class-default)
R1(config-if)#
```

The http traffic is allowe for the same reason as the ICMP traffic:

```
R2#telnet 192.168.201.5 80

Trying 192.168.201.5, 80 ... Open

HTTP/1.1 400 Bad Request
Date: Fri, 01 Mar 2002 00:55:25 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 192.168.201.5 closed by foreign host]
R2#
```

Now if we want the router generates a line in the syslog for every session establishment and termination event.We can configure the audit-trail
First we configure the parametr-map type called audit ,then we turn on the audit-trail as follow:

```
parameter-map type inspect audit
 audit-trail on
```

we goes to the policy-map configured above InsideToOutside,we add the parameter-map named audit for the inspect action:

```
policy-map type inspect InsideToOutside
 class type inspect InternetTraffic
  inspect audit
```

We will ping from R2 to R4:

```
R2#ping 192.168.201.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.5, timeout is 2 seconds:
```

```
!!!!!
R2#
```

Notice the log message displayed on R1 after the ping ,the session establishment with the word start and the initiator which is here R2(10.0.0.2) and the responder ,R4 in this case with the ip address 192.168.201.5, also notice the termination event with the word Stop icmp :

```
R1#
*Mar  1 01:04:43.371: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-
(InsideToOutside:InternetTraffic):Start icmp session: initiator (10.0.0.2:8) --
responder (192.168.201.5:0)
R1#
*Mar  1 01:04:53.911: %FW-6-SESS_AUDIT_TRAIL: (target:class)-
(InsideToOutside:InternetTraffic):Stop icmp session: initiator (10.0.0.2:8) sent
360 bytes -- responder (192.168.201.5:0) sent 360 bytes
R1#
```

Protecting the router by using the zone self:

By default all the IP addresses configured on the router belong to the zone self, regardless of the zone memberships of theirinterfaces.And traffic to and from the self zone is allowed.

The requirement is
-No external access, only from ping (icmp echo).
-No access to the Internet from the router

First we create an extended access-list to permit the ICMP Echo:

```
ip access-list extended ICMPEcho
 permit icmp any any echo
```

We create a class-map called ping to identify the traffic ,here we will match the extended access-list called ICMPEcho:

```
class-map type inspect match-any ping
 match access-group name ICMPEcho
```

Then we create a policy-map to define the action inspect applied for the class-map to allow the icmp echo , and drop all other traffic with the drop action for class class-default :

```
policy-map type inspect OutsideToRouter
 class type inspect ping
  inspect
 class class-default
  drop log
```

Now we will create a zone-pair with the source Outside and the destionation self ,the router itself:

```
zone-pair security OutsideToRouter source Outside destination self
 service-policy type inspect OutsideToRouter.
```

Before configuring the policy ,let's verify the ping and telnet from R4 to R1 (outside to self zone):

both traffic ,icmp and telnet works well:

```
R4#ping 192.168.201.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/44 ms
R4#
R4#telnet 192.168.201.6
Trying 192.168.201.6 ... Open


User Access Verification

Password:
R1>ena
Password:
R1#
```

Now after configuring the policy to protect the router:

The ping is successfully because the icmp-echo is allow from outside zone to the self zone(the router itself):

```
R4#ping 192.168.201.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/23/44 ms
R2#
```

Now the telnet traffic is denied because the drop action for the class class-default(other traffic):

```
R4#telnet 192.168.201.6
Trying 192.168.201.6 ...
% Connection timed out; remote host not responding

R4#
```

Notice the log message displayed on R1:

```
R1(config-sec-zone-pair)#
*Mar  1 01:27:45.315: %FW-6-DROP_PKT: Dropping Other session 192.168.201.5:62815
192.168.201.6:23 on zone-pair OutsideToRouter class class-default due to DROP
action found in policy-map with ip ident 12442
R1(config-sec-zone-pair)#
```

If we want limit internal access from the inside zone to the self zone (for example ping SSH HTTP and HTTPS):

We create an access-list for all protocols we want allow :

```
ip access-list extended PROTOCOLS
 permit tcp any any eq 80
 permit tcp any any eq 443
 permit icmp any any echo
 permit tcp any any eq 22
```

We create a class-map to identify the traffic matching the access-list:

```
class-map type inspect match-any RouterProtocols
 match access-group name PROTOCOLS
```

The policy-map called InsideToRouter will match the class-map with an action of inspect ,the rest of traffic is dropped by default:

```
policy-map type inspect InsideToRouter
 class type inspect RouterProtocols
  inspect
 class class-default
```

We define the zone-pair for the direction of the traffic and applied the policy-map:

```
zone-pair security InsideToRouter source Inside destination self
 service-policy type inspect InsideToRouter
```

Before configuring the policy from inside to router ,let's verify the telnet and the ping:

The ping and the telnet works successfully:

```
R2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/50/84 ms
R2#
```

```
R2#telnet 10.0.0.1
```

```
Trying 10.0.0.1 ... Open


User Access Verification

Password:
R1>ena
Password:
R1#
```

Let's configure the policy from the inside zone to the router:

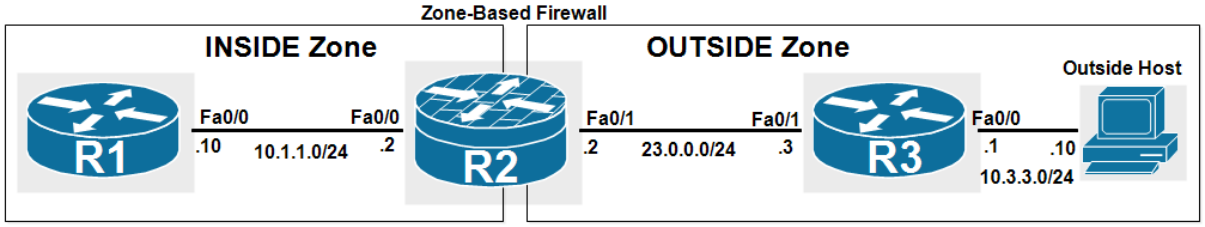
The ping from R2 to R1 is successfully as expected because the ICMP traffic is allowed under the policy-map InsideToRouter:

```
R2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/54/88 ms
R2#
```

As expected the telnet traffic from R2 to R1 is dropped because the telnet protocol is not included in the access-list configured under the class-map RouterProtocols ,because the telnet traffic does not match the class-map RouterProtocols the router matches the traffic with class class-default and apply the default action drop:

```
R2#telnet 10.0.0.1
Trying 10.0.0.1 ...
% Connection timed out; remote host not responding
R2#
```

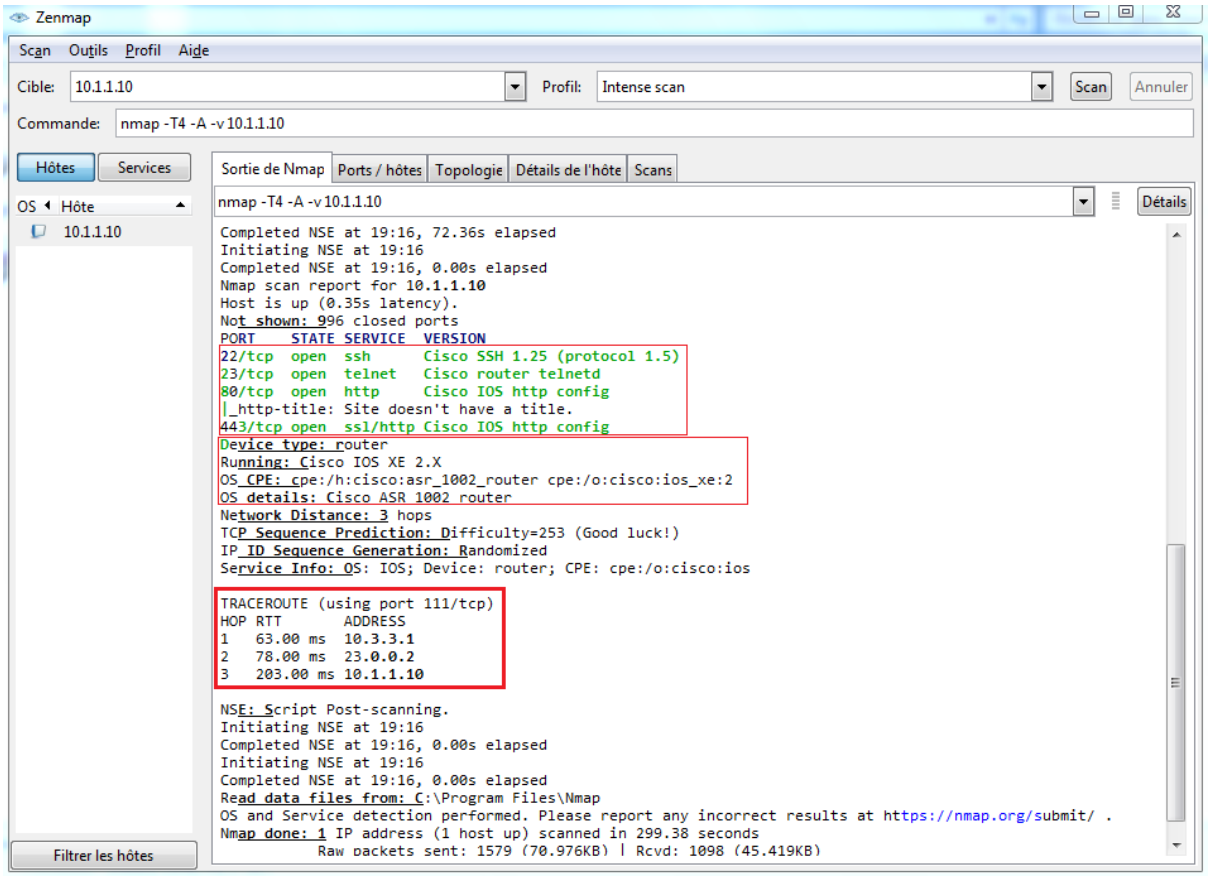
Lab 3: Zone-Based Firewall Scenario-2

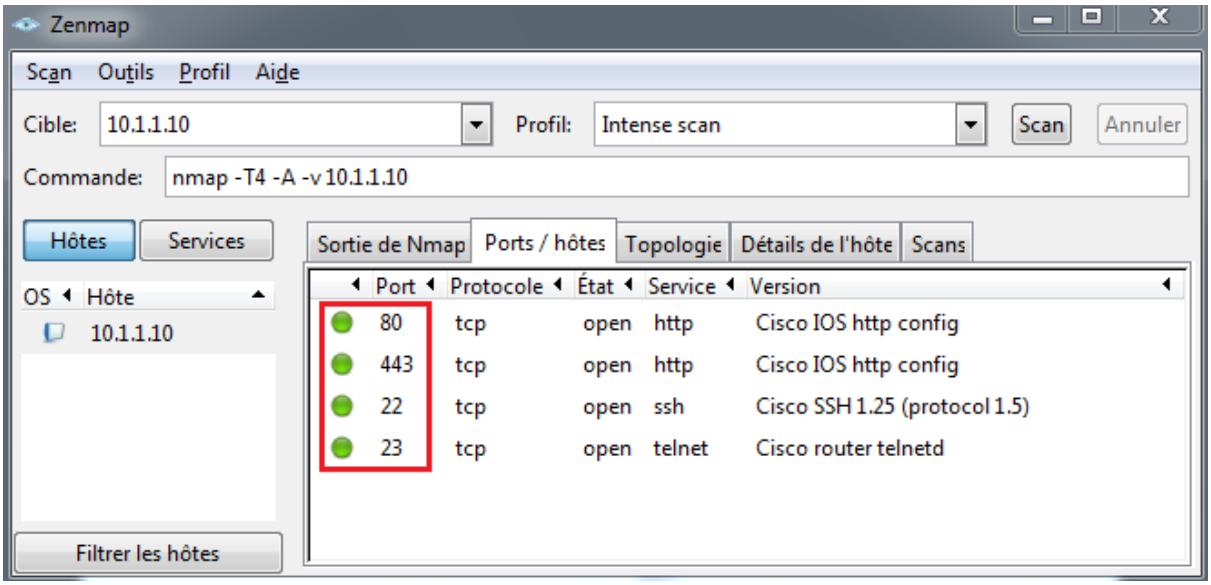


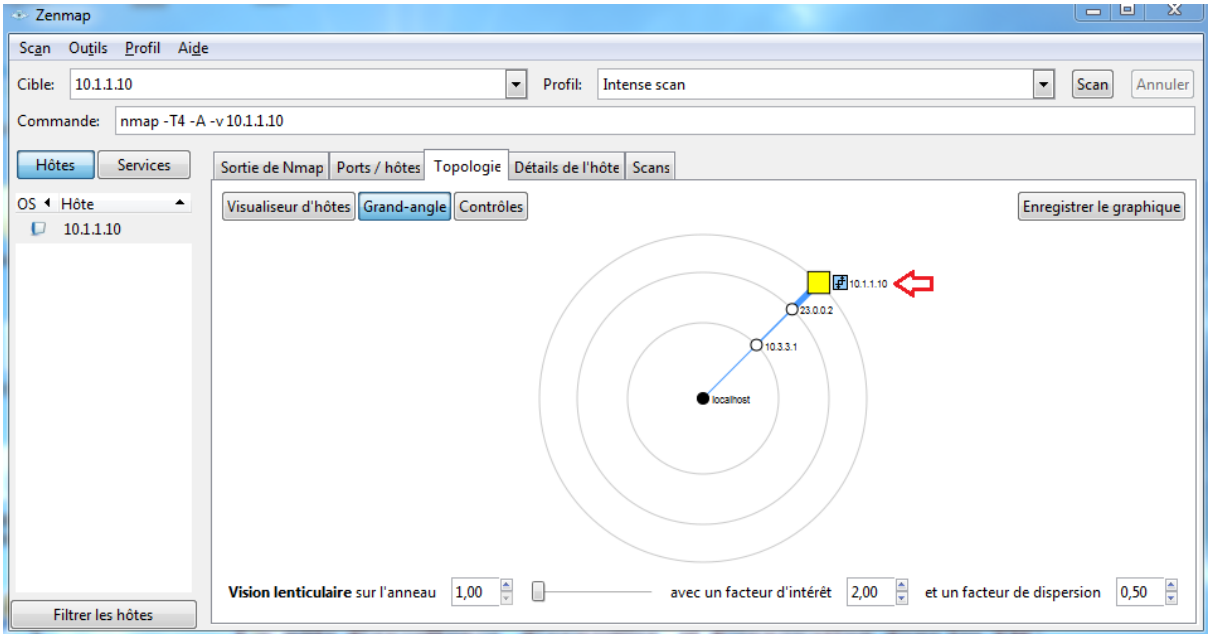
In the topology, the Outside Host is located in OUTSIDE, and the router R1 is located in the INSIDE network which is a private LAN that we should protect from intruders in the OUTSIDE.

On the PC located in the OUTSIDE, execute NMAP tool to scan the IP address 10.1.1.10 of R1:

As you can see, the intruder discovers four open ports: Telnet, SSH, HTTP and HTTPS, also it determines the distance of 3 hops toward the router R1 and the device model Cisco, so the intruder has free access to the router R1.







Cisco IOS Zone-Based Firewall configuration.

Requirements:

The router R2 should be configured as a Zone-Based Firewall to provide more protection against intruders that run scan port.

Task-1: Hosts in the inside zone with addresses in the 10.1.1.0/24 network can access any host in the OUTSIDE zone by using HTTP and ping (ICMP echo) protocols.

Hosts in the OUTSIDE zone can access the router R1 (10.1.1.10 using the HTTP and HTTPS protocols in the INSIDE zone.

Create a zone:

```
R2(config)#zone security INSIDE
R2(config-sec-zone)#zone security OUTSIDE
```

Assign interface to a zone:

```
R2(config)#interface f0/0
R2(config-if)#zone-member security INSIDE
R2(config)#interface f0/1
R2(config-if)#zone-member security OUTSIDE
```

Hosts in the inside zone with addresses in the 10.1.1.0/24 network can access any host in the OUTSIDE zone by using HTTP and ping (ICMP echo) protocols.

All other traffic between zone pairs is prohibited and should be dropped.

The IN-TO-OUT-ACL ACL describes the initial packets of HTTP and PING from 10.1.1.0/24 network.

```
R2(config)#ip access-list extended IN-TO-OUT-ACL
R2(config-ext-nacl)# permit tcp 10.1.1.0 0.0.0.255 any eq www
R2(config-ext-nacl)# permit icmp 10.1.1.0 0.0.0.255 any echo
```

The IN-TO-OUT-CLASS matches the configured ACL to classify these two applications into the same class.

```
R2(config)#class-map type inspect IN-TO-OUT-CLASS
R2(config-cmap)# match access-group name IN-TO-OUT-ACL
```

we want the router generates a line in the syslog for every session establishment and termination event. We can configure the audit-trail.
First we configure the parameter-map type called audit, then we turn on the audit-trail.

```
R2(config)#parameter-map type inspect audit
R2(config-profile)#audit-trail on
```

Use the policy-map type inspect command to create a named policy map (IN-TO-OUT-POLICY). In the policy map, use the class type inspect command to refer to a previously configured IN-TO-OUT-CLASS and specify the inspect action to permit and statefully inspect the class protocols (HTTP and ping).
Add the parameter-map named audit for the inspect action.

Create an optional reference to the class-default class using the class-class-default command. in the class class-default, tune the default drop action to also log denied traffic by specifying both actions (drop log) in the class-policy.

```
R2(config)#policy-map type inspect IN-TO-OUT-POLICY
R2(config-pmap)# class type inspect IN-TO-OUT-CLASS
R2(config-pmap-c)#  inspect audit
R2(config-pmap-c)# class class-default
```

```
R2(config-pmap-c)#  drop log
```

Apply the configured policy map.

Associate the IN-TO-OUT-POLICY with the IN-TO-OUT zone pair, the source is INSIDE zone and the destination is the OUTSIDE zone.

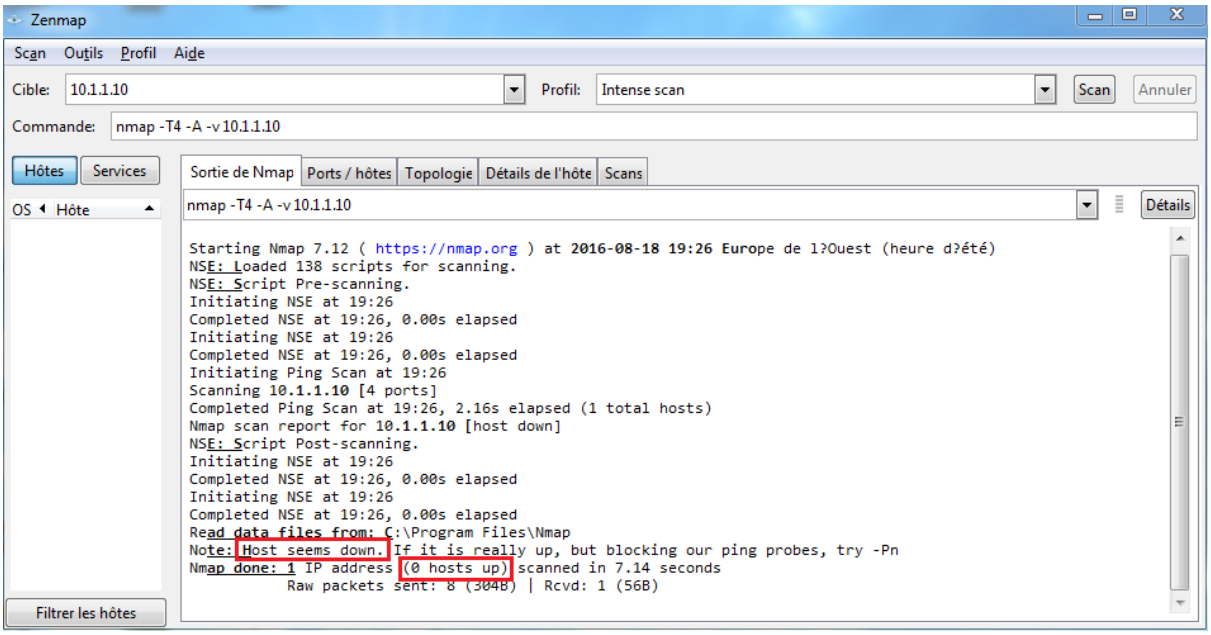
```
R2(config)#zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
R2(config-sec-zone-pair)#service-policy type inspect IN-TO-OUT-POLICY
```

Since the default interzone policy is to drop all traffic unless explicitly allowed, the HTTP and echo ICMP traffic coming from INSIDE to OUTSIDE is inspected and allowed.

Since there is no zone pair for the traffic initiated from OUTSIDE to INSIDE, the ZBF drops this traffic when coming from OUTSIDE.

On the Outside-Host execute the NMAP tool:

We can see that the Port Scan fails and no active host detected:



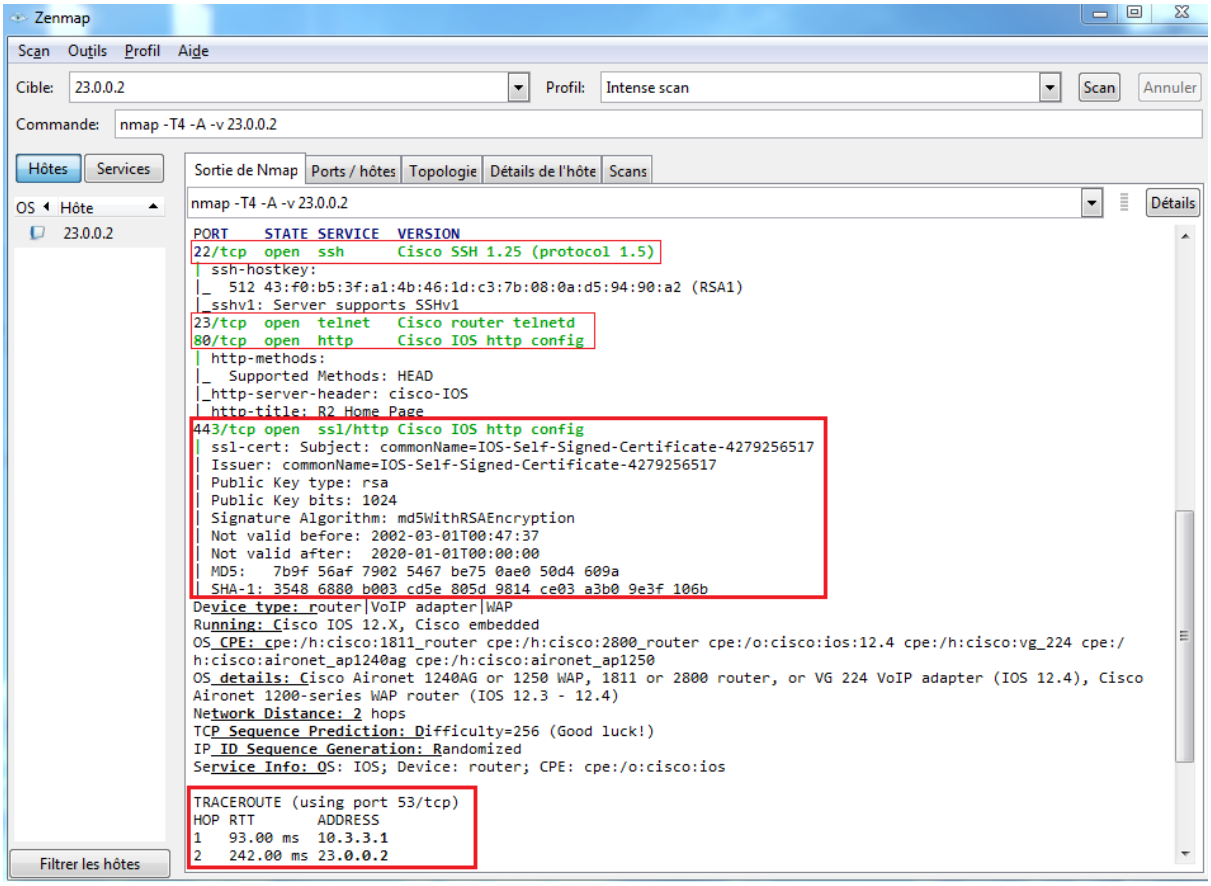
Task-2:

The firewall configuration has successfully protected inside hosts from outside attacks and limited the services the inside host can access on the outside.

However the router R2 itself remains vulnerable because the traffic to and from the router itself is not restricted by the interzone policy.

To verify, on the Outside Host execute a scan port by specifying the IP address 23.0.0.2 of R2:

We can see that the intruder can collect a lot information about R2, such the current open ports: Telnet, SSH, HTTP and HTTPS and especially the self-signed certificate informations.



Zone-Based Firewall offers a novel approach to this problem. The router itself can be defined as a separate security zone (with the predefined name self), and the incoming and outgoing sessions can be limited in the same way as the routed interzone traffic.

When configuring the self zone, considers these facts:

1-All IP addresses configured on the router belong to the zone self, regardless of the zone memberships of their interfaces.

2-Unless configured otherwise, traffic to and from the self zone is allowed.

3-The moment you use the self zone in a zone pair, the traffic between the self zone and the other zone in the zone pair is restricted in both directions. For example if we define a zone pair from inside to self, the router cannot originate any sessions toward the inside zone until we define a zone pair from self to inside.

4-Traffic between the router itself and the zones not mentioned in the combination with the self zone in a zone pair is not affected.

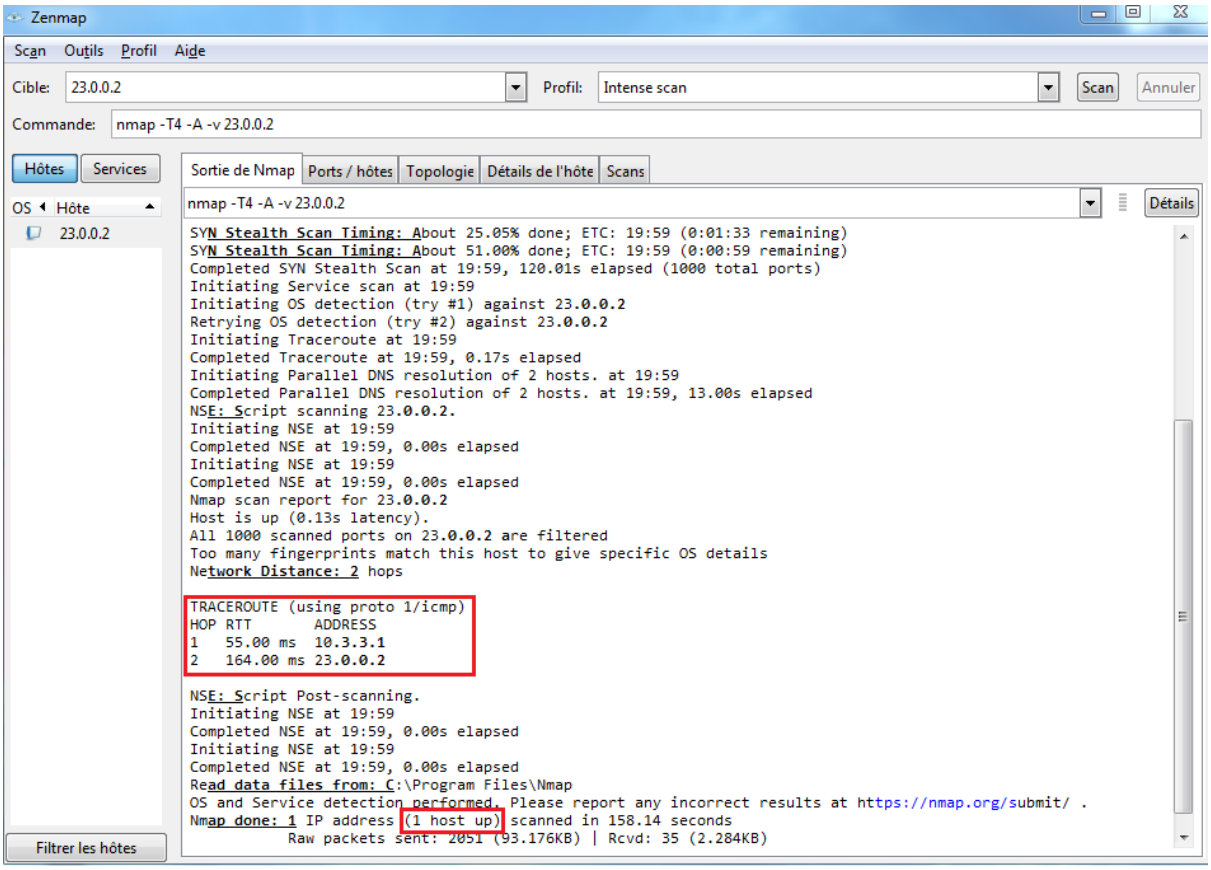
5-When configuring the restrictions for the inbound traffic, consider the necessary outbound traffic (including the routing and network management protocols). For example if you restrict inbound traffic from zone to the router itself, the routing could stop working on all interfaces belonging to that zone.

In this example we want restrict traffic from outside to R2 itself in order to prevent any potential attack from the Outside Host such the Port Scan.

Allow only the ping echo ICMP from the outside to R2 itself and drop all other traffic.

```
R2(config)#ip access-list ext ACL-SELF
R2(config-ext-nacl)#permit icmp any any echo

R2(config)#class-map type inspect match-any CLASS-SELF
R2(config-cmap)#match access-group name ACL-SELF

R2(config)#policy-map type inspect POLICY-SELF
R2(config-pmap)#class type inspect CLASS-SELF
R2(config-pmap-c)#inspect audit
R2(config-pmap-c)#class class-default
R2(config-pmap-c)#drop log

R2(config)#zone-pair security OUT-TO-SELF source OUTSIDE destination self
R2(config-sec-zone-pair)# service-policy type inspect POLICY-SELF
```

On the Outside Host, execute NMAP scan, we can see that the host cannot access the router at all and cannot see any open ports, akthrough it can still be pinged and issued a traceroute to see the number of hops (see the "1 host is up).



On R2, a message is displayed telling that a TCP session is dropped:

```
R2#
```

```
*Mar  1 01:02:43.291: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-
SELF:CLASS-SELF):Start icmp session: initiator (10.3.3.10:8) -- responder
(23.0.0.2:0)
R2#
*Mar  1 01:02:53.303: %FW-6-SESS_AUDIT_TRAIL: (target:class)-(OUT-TO-SELF:CLASS-
SELF):Stop icmp session: initiator (10.3.3.10:8) sent 0 bytes -- responder
(23.0.0.2:0) sent 0 bytes
R2#
*Mar  1 01:03:02.979: %FW-6-DROP_PKT: Dropping tcp session10.3.3.10:57593
23.0.0.2:5051 on zone-pair OUT-TO-SELF class class-default due to DROP action
found in policy-map with ip ident 17300
R2#
*Mar  1 01:03:33.307: %FW-6-DROP_PKT: Dropping tcp session10.3.3.10:57592
23.0.0.2:8600 on zone-pair OUT-TO-SELF class class-default due to DROP action
found in policy-map with ip ident 55666
R2#
*Mar  1 01:04:03.659: %FW-6-DROP_PKT: Dropping tcp session10.3.3.10:60904
23.0.0.2:1217 on zone-pair OUT-TO-SELF class class-default due to DROP action
found in policy-map with ip ident 4172
R2#
```

Verify the number of packets dropped by the policy map definded in the zone pair OUT-TO-SELF:

```
R2#show policy-map type inspect zone-pair sessions | beg  OUT-TO-SELF
Zone-pair: OUT-TO-SELF

  Service-policy inspect : POLICY-SELF

    Class-map: CLASS-SELF (match-any)
      Match: access-group name ACL-SELF
        4 packets, 272 bytes
        30 second rate 0 bps
      Inspect

Class-map: class-default (match-any)
      Match: any
Drop
4098 packets, 104944 bytes
R2#
```

Task-3:Hosts in the OUTSIDE zone can access the host in the inside (10.1.1.10) in the DMZ zone by using HTTP and HTTPS protocols.

All other traffic between zone pairs is prohibited and should be dropped.

The OUT-TO-IN-ACL ACL describes the initial packets of HTTP and HTTPS from outside network to inside.

```
R2(config)#ip access-list extended OUT-TO-IN-ACL
```

```
R2(config-ext-nacl)# permit tcp any host 10.1.1.10 eq 80
R2(config-ext-nacl)# permit tcp any host 10.1.1.10 eq 443
```

The OUT-TO-IN-CLASS matches the configured ACL to classify these two applications into the same class.

```
R2(config)#class-map type inspect OUT-TO-IN-CLASS
R2(config-cmap)# match access-group name OUT-TO-IN-ACL
```

Finally configure a policy map to control access between the OUTSIDE and INSIDE zones (OUT-TO-IN-POLICY). In the policy map use the class type inspectcommand to refer to a previously configured OUT-TO-IN-CLASS and specify the inspect action to statefully inspect the HTTP and HTTPS protocols. Assign the drop log actions to the class-default class on this policy map.

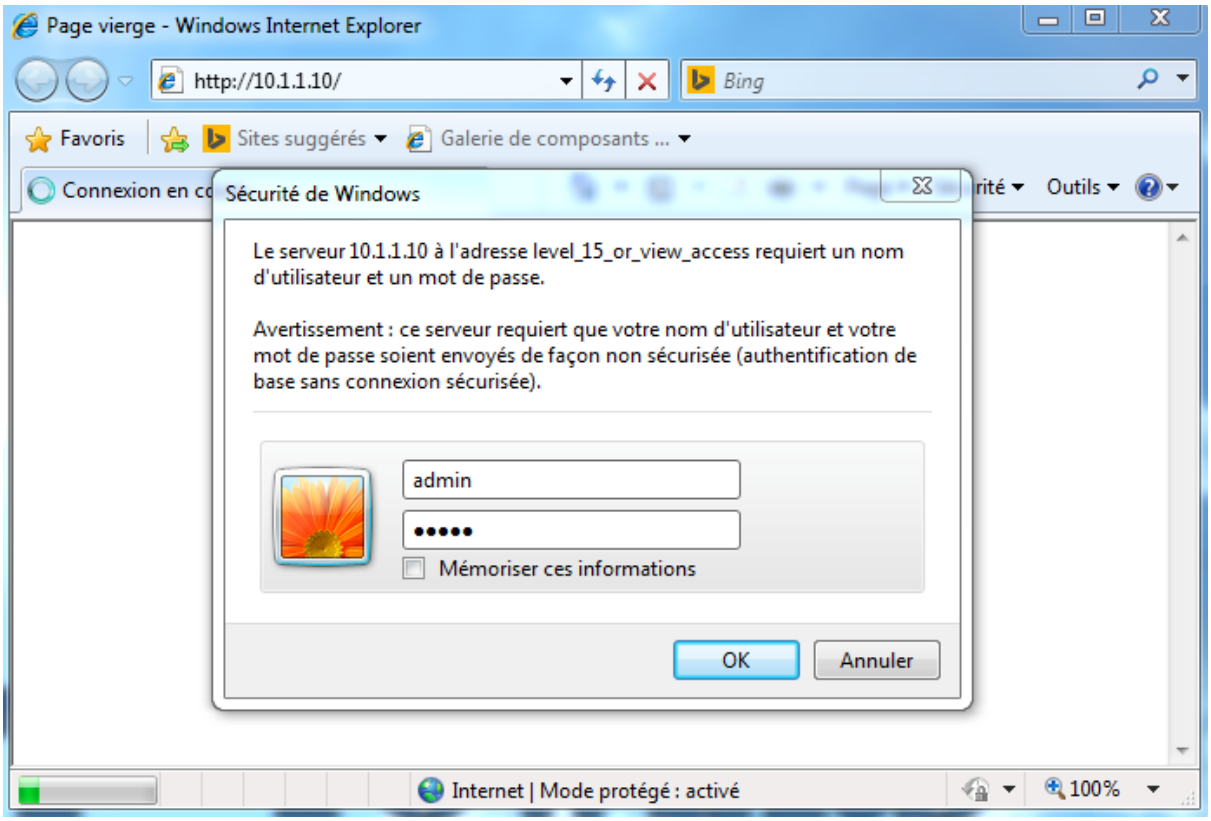
```
R2(config)#policy-map type inspect OUT-TO-IN-POLICY
R2(config-pmap)# class type inspect OUT-TO-IN-CLASS
R2(config-pmap-c)#  inspect audit
R2(config-pmap-c)# class class-default
R2(config-pmap-c)#  drop log
```

Apply the configured policy map.

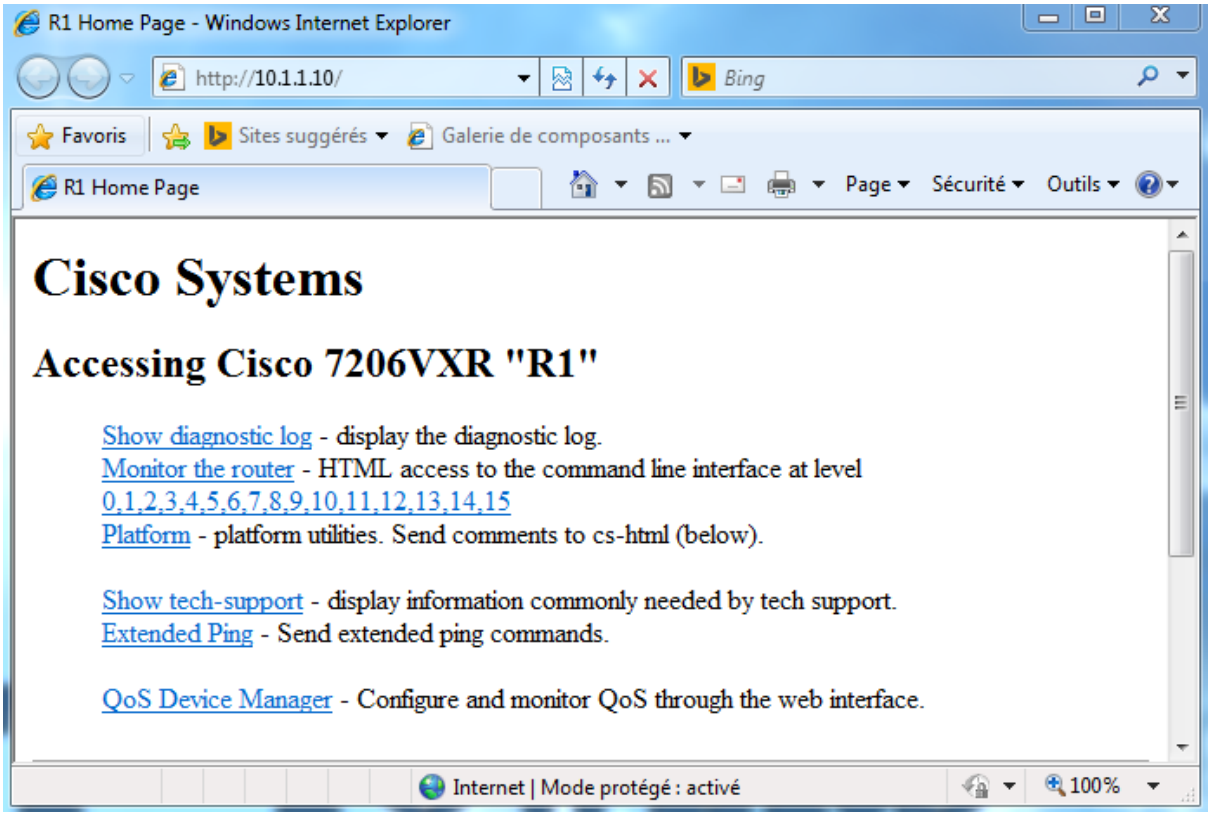
Associate the OUT-TO-IN-POLICY with the OUT-TO-IN zone pair, the source is OUTSIDE zone and the destination is the INSIDE zone.

```
R2(config)#zone-pair security OUT-TO-IN source OUTSIDE destination INSIDE
R2(config-sec-zone-pair)# service-policy type inspect OUT-TO-IN-POLICY
```

From the OUTSIDE Host, initiate an HTTP traffic using the web browser to access the router R1 in the inside.



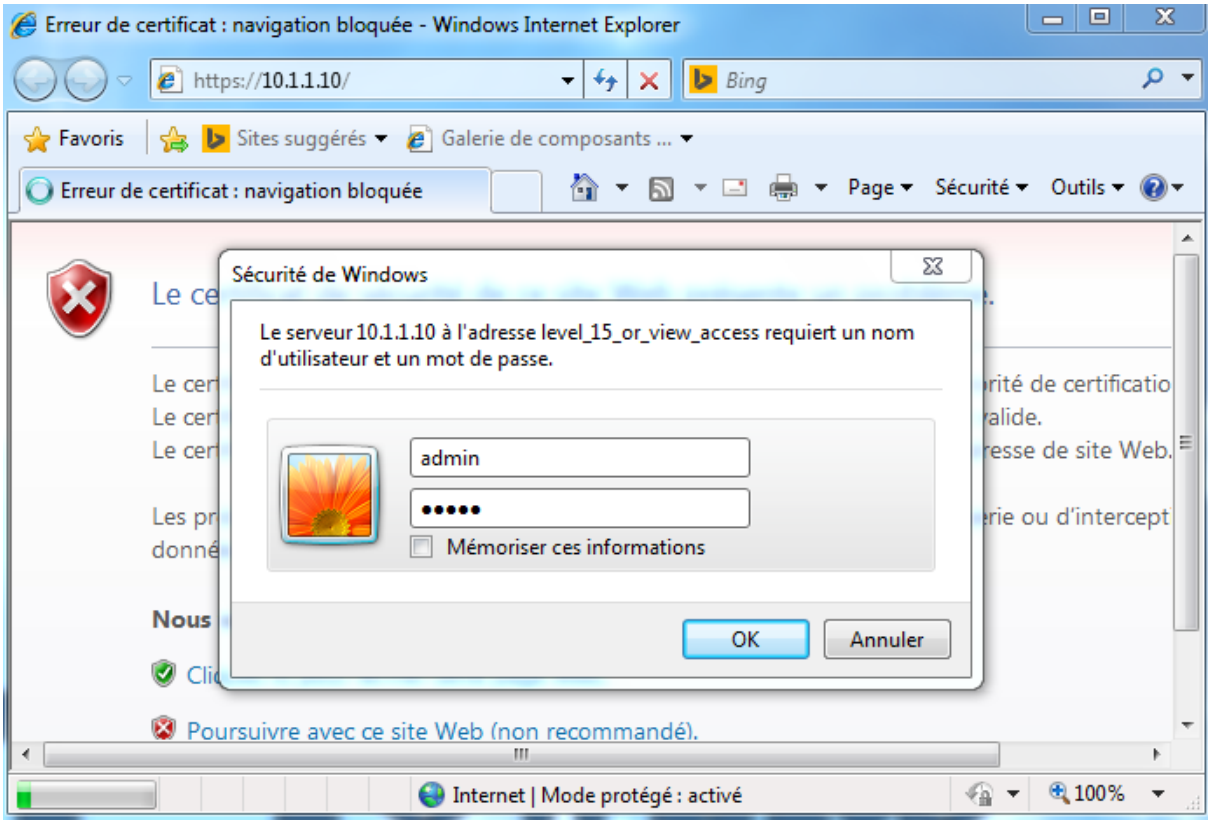
The access is successful.

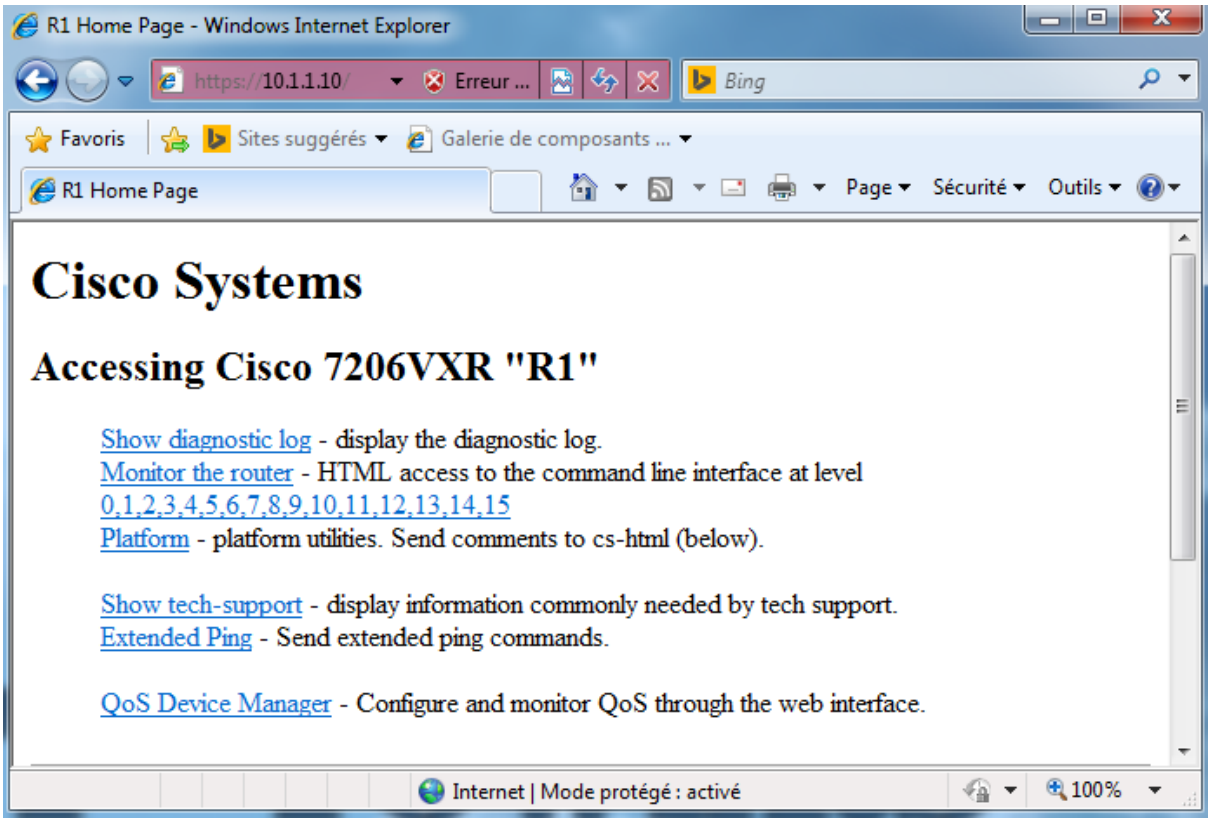


Return to router R2. Notice the log message displayed on R2, the HTTP session establishment with the word start and the initiator is the Outside Host (10.3.3.10) and the responder is R1 with IP address 10.1.1.10.

```
R2#
*Mar  1 00:38:36.559: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-IN:OUT-TO-IN-CLASS):Start http session: initiator (10.3.3.10:49216) -- responder (10.1.1.10:80)
R2#
*Mar  1 00:39:17.923: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-IN:OUT-TO-IN-CLASS):Start http session: initiator (10.3.3.10:49217) -- responder (10.1.1.10:80)
R2#
*Mar  1 00:39:19.427: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-IN:OUT-TO-IN-CLASS):Start http session: initiator (10.3.3.10:49218) -- responder (10.1.1.10:80)
R2#
```

From the OUTSIDE Host, initiate an HTTPS traffic using the web browser.

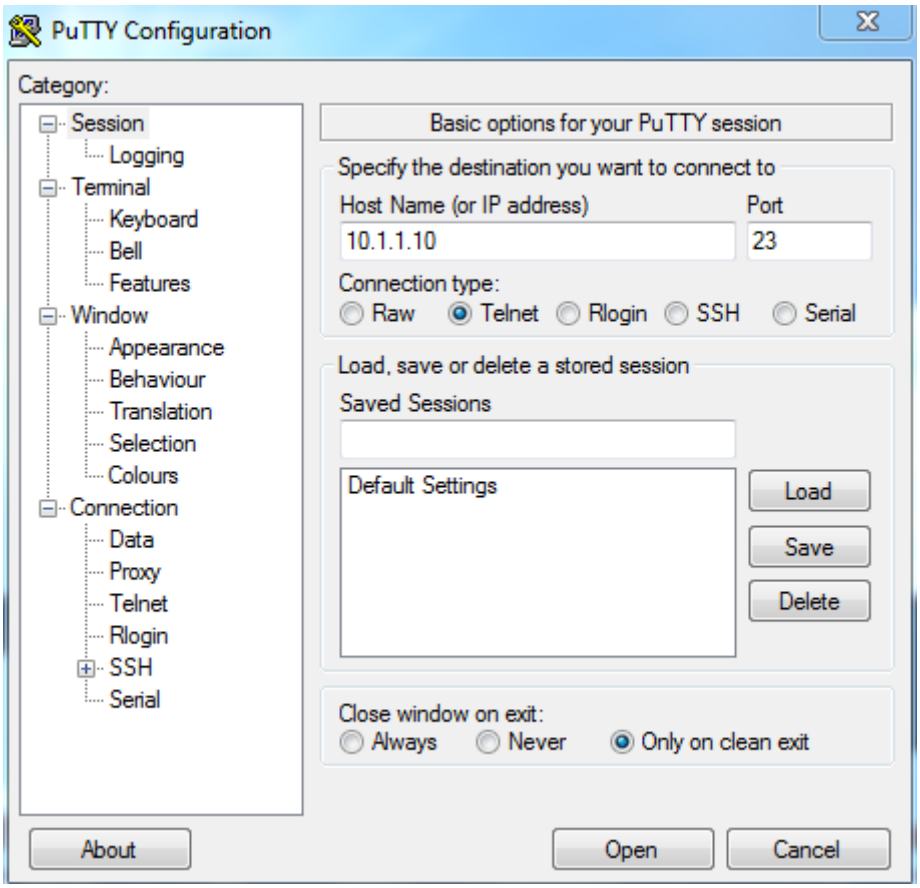




On R2, notice the HTTPS session establishment with the word start and the initiator is the Outside Host (10.3.3.10) and the responder is R1 with IP address10.1.1.10.

```
R2#
*Mar  1 00:41:50.915: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-IN:OUT-
TO-IN-CLASS):Start https session: initiator (10.3.3.10:49219) -- responder
(10.1.1.10:443)
R2#
*Mar  1 00:41:54.075: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-IN:OUT-
TO-IN-CLASS):Start https session: initiator (10.3.3.10:49220) -- responder
(10.1.1.10:443)
R2#
*Mar  1 00:41:55.555: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(OUT-TO-IN:OUT-
TO-IN-CLASS):Start https session: initiator (10.3.3.10:49221) -- responder
(10.1.1.10:443)
R2#
```

On the Outside Host, initiate a telnet traffic toward R1.



Now the telnet traffic is denied because the drop action for the class class-default (other traffic).

Notice the log message displayed on R1.

```
R2#
*Mar  1 00:44:36.727: %FW-6-DROP_PKT: Dropping Other session 10.3.3.10:49224
10.1.1.10:23 on zone-pair OUT-TO-IN class class-default due to DROP action
found in policy-map with ip ident 1261
R2#

R2#
*Mar  1 00:46:02.999: %FW-6-LOG_SUMMARY: 3 packets were dropped from
10.3.3.10:49224 => 10.1.1.10:23 (target:class)-(OUT-TO-IN:class-default)
R2#
```

Verify the zone pair session, in the OUT-TO-IN zone pair notice there are two packets dropped in the class-default:

```
R2#show policy-map type inspect zone-pair sessions
 Zone-pair: IN-TO-OUT

  Service-policy inspect : IN-TO-OUT-POLICY

    Class-map: IN-TO-OUT-CLASS (match-all)
```

```
      Match: access-group name IN-TO-OUT-ACL
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
Zone-pair: OUT-TO-IN

Service-policy inspect : OUT-TO-IN-POLICY

    Class-map: OUT-TO-IN-CLASS (match-all)
      Match: access-group name OUT-TO-IN-ACL
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop
2 packets, 64 bytes
R2#
```

Try to ping from R1 to Host in the outside zone, the ping is successfull because the ICMP echo traffic is defined in the class-map to be inspected.

```
R1#ping 10.3.3.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/142/168 ms
R1#
```

The router R2 displays a message and an ICMP session establishment with the initiator R1 (10.1.1.10) and the responder (10.3.3.10).

```
R2#
*Mar  1 00:04:42.487: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(IN-TO-OUT:IN-
TO-OUT-CLASS):Start icmp session: initiator (10.1.1.10:8) – responder
(10.3.3.10:0)
R2#
*Mar  1 00:04:53.187: %FW-6-SESS_AUDIT_TRAIL: (target:class)-(IN-TO-OUT:IN-TO-OUT-
CLASS):Stop icmp session: initiator (10.1.1.10:8) sent 360 bytes --responder
(10.3.3.10:0) sent 360 bytes
R2#
```

Verify the zone pair sessions, notice the ICMP sessions established between 10.1.1.10 and 10.3.3.10.

```
R2#show policy-map type inspect zone-pair sessions
Zone-pair: IN-TO-OUT
```

```
Service-policy inspect : IN-TO-OUT-POLICY

    Class-map: IN-TO-OUT-CLASS (match-all)
      Match: access-group name IN-TO-OUT-ACL
      Inspect
        Established Sessions
Session 6715FF84 (10.1.1.10:8)=>(10.3.3.10:0) icmp SIS_OPEN
          Created 00:00:05, Last heard 00:00:04
ECHO request
          Bytes sent (initiator:responder) [360:360]

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
 Zone-pair: OUT-TO-IN

  Service-policy inspect : OUT-TO-IN-POLICY

    Class-map: OUT-TO-IN-CLASS (match-all)
      Match: access-group name OUT-TO-IN-ACL
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
R2#
```

From R1 try to telnet to R3 (10.3.3.1). The telnet traffic is denied because the drop action for the class class-default (other traffic) defined in the IN-TO-OUT-POLICY policy map applied in the zone pair IN-TO-OUT. And R2 displays a message.

```
R1#telnet 10.3.3.1
Trying 10.3.3.1 ...
% Connection timed out; remote host not responding

R1#
```

```
R2#
*Mar  1 00:12:06.319: %FW-6-DROP_PKT: Dropping Other session 10.1.1.10:56712
10.3.3.1:23 on zone-pair IN-TO-OUT class class-default due to DROP action found in
policy-map with ip ident 28604
R2#
```

Verify the zone pair sessions, int the zone pair IN-TO-OUT, notice 2 packets are dropped in the class-default.

```
R2#show policy-map type inspect zone-pair sessions
Zone-pair: IN-TO-OUT
```

```
  Service-policy inspect : IN-TO-OUT-POLICY

    Class-map: IN-TO-OUT-CLASS (match-all)
      Match: access-group name IN-TO-OUT-ACL
      Inspect

Class-map: class-default (match-any)
      Match: any
      Drop
2 packets, 48 bytes
 Zone-pair: OUT-TO-IN

  Service-policy inspect : OUT-TO-IN-POLICY

    Class-map: OUT-TO-IN-CLASS (match-all)
      Match: access-group name OUT-TO-IN-ACL
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
R2#
```

Verify the configuration the Zone-Based Firewall:

First verify the configured zones and the interfaces assigned:

```
R2#show zone security
zone self
  Description: System defined zone


zone INSIDE
  Member Interfaces:
    FastEthernet0/0


zone OUTSIDE
  Member Interfaces:
    FastEthernet0/1


R2#
```

Verify the class-map that identifies the traffic:

```
R2#show class-map type inspect
 Class Map type inspect match-all IN-TO-OUT-CLASS (id 1)
   Match access-group name IN-TO-OUT-ACL
```

```
 Class Map type inspect match-all OUT-TO-IN-CLASS (id 2)
   Match access-group name OUT-TO-IN-ACL

R2#
```

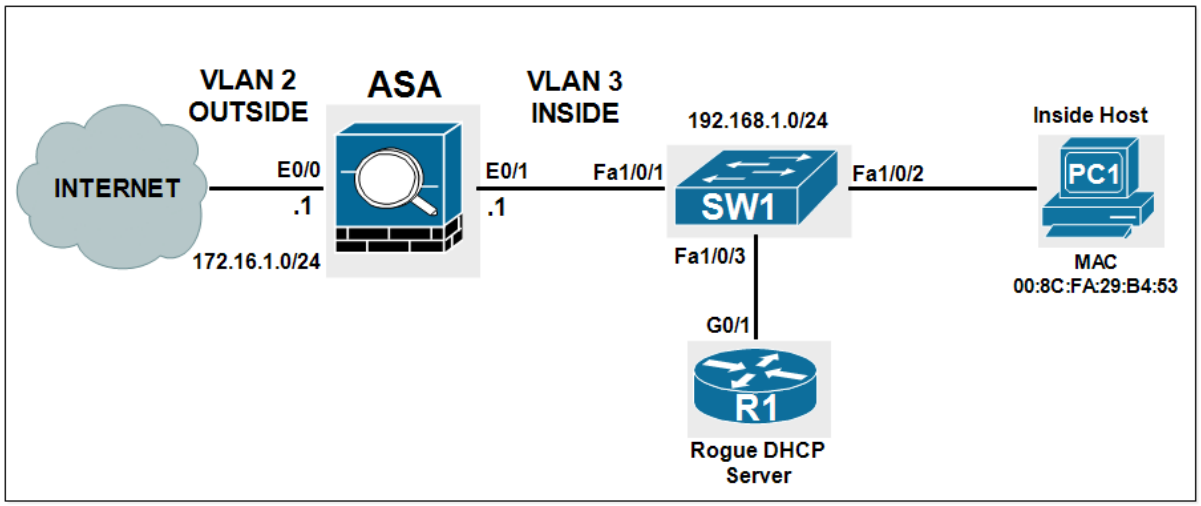
Verify the policy-map that takes an action:

```
R2#show policy-map type inspect
  Policy Map type inspect IN-TO-OUT-POLICY
    Class IN-TO-OUT-CLASS
      Inspect audit
    Class class-default
      Drop log

  Policy Map type inspect OUT-TO-IN-POLICY
    Class OUT-TO-IN-CLASS
      Inspect audit
    Class class-default
      Drop log

R2#
```

Verify the zone-pair and the direction to apply the corresponding policy-map:

```
R2#show zone-pair security
Zone-pair name IN-TO-OUT
Source-Zone INSIDE  Destination-Zone OUTSIDE
service-policy IN-TO-OUT-POLICY
Zone-pair name OUT-TO-IN
Source-Zone OUTSIDE  Destination-Zone INSIDE
service-policy OUT-TO-IN-POLICY

R2#
```

Lab 4: DHCP Snooping and ARP Inspection



Task-1:

On ASA, configure IP addressing and nameif settings on the vlan interfaces:

```
ciscoasa(config)#interface Vlan3
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
ciscoasa(config)#interface Vlan2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip add 172.16.1.1 255.255.255.0
```

Affect the physical interface to the appropriate vlan:

```
ciscoasa(config)#interface e0/0
ciscoasa(config-if)#switchport mode access
ciscoasa(config-if)#switchport access vlan 2
```

```
ciscoasa(config)#interface e0/1
ciscoasa(config-if)#switchport mode access
ciscoasa(config-if)#switchport access vlan 3
```

Verify the Vlan interfaces:

```
ciscoasa# show run int vlan 2
!
```

```
interface Vlan2
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0

ciscoasa# show run int vlan 3
!
interface Vlan3
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
ciscoasa#
```

The show switch vlan command is similaire to show vlan command of switch, it shows the ports and the associated VLAN:

```
ciscoasa# show switch vlan
VLAN Name                            Status    Ports
---- ------------------------------- --------- ----------------------------
1    -                               down      Et0/2, Et0/3, Et0/4, Et0/5
                                               Et0/6, Et0/7
2    outside                         up        Et0/0
3    inside                          up        Et0/1
ciscoasa#
```

On SW1, configure the ports fa1/0/1 and fa1/0/2 in VLAN 3, enable spanning-tree porfast to avoid the listening and learning states of STP:

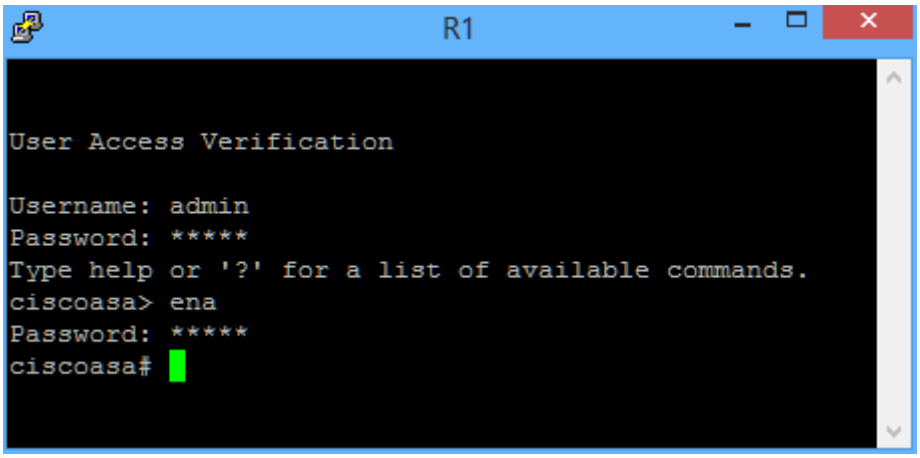
```
SW1(config)#interface range fa1/0/1-2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 3
SW1(config-if)# spanning-tree portfast
```

Task-2:

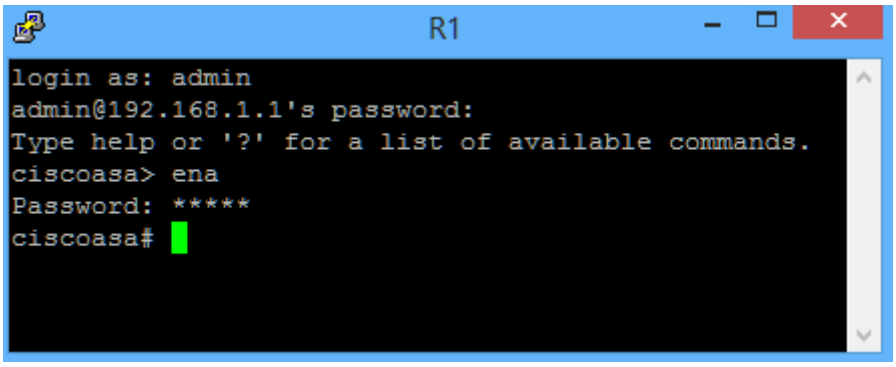
Configure the ASA to accept Telnet and SSH connections from a single host or a range of hosts on the inside network. Configure the ASA to allow Telnet and SSH connections from any host on the inside network 192.168.1.0/24, use the AAA local authentication:

```
ciscoasa(config)#username admin password cisco
ciscoasa(config)#telnet 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#aaa authentication telnet console LOCAL
ciscoasa(config)#aaa authentication ssh  console LOCAL
```

From the inside host, access the ASA using telnet:



From the inside host, access the ASA using SSH:



Task-3:

Configure HTTP and verify ASDM access to the ASA.

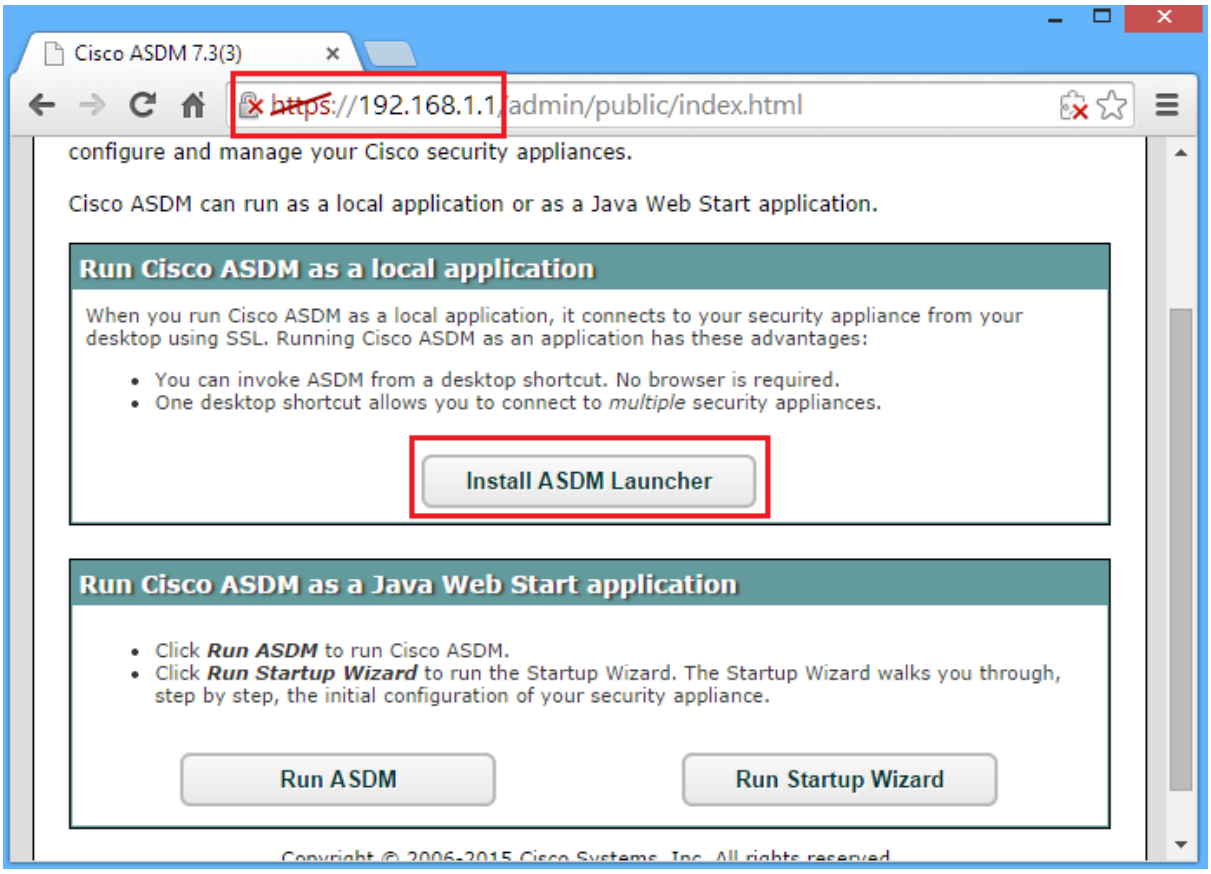
You can configure the ASA to accept HTTPS connections using the http command. This allows access to the ASA GUI (ASDM). Configure the ASA to allow HTTPS connections from any host on the inside network 192.168.1.0/24.

```
ciscoasa(config)#aaa authentication http console LOCAL
ciscoasa(config)#http server enable
ciscoasa(config)#http 192.168.1.0 255.255.255.0 inside
```

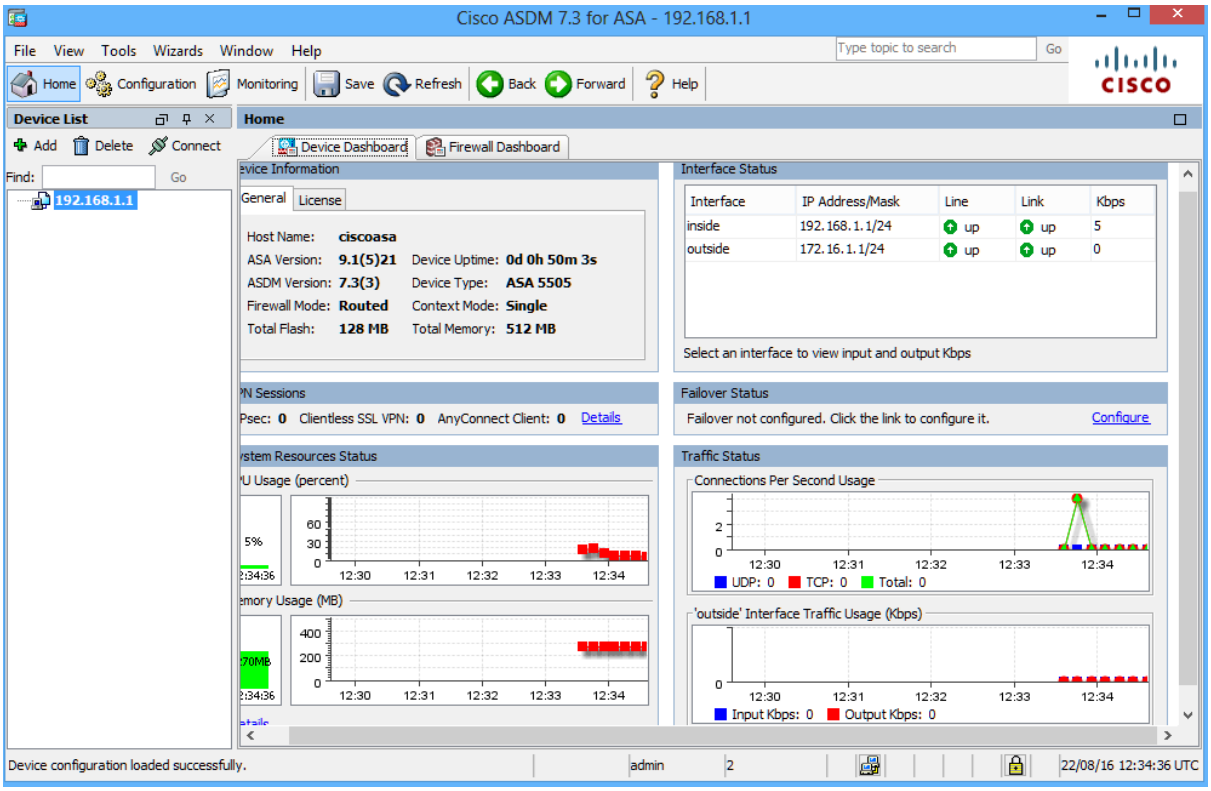
Locate the ASDM image in the ASA's Flash memory, otherwise download it using TFTP server and specify the location of the ASDM image, enter the following command:

```
ciscoasa(config)#asdm image disk0:/asdm-733.bin

ciscoasa# show flash: | i asdm
188  27289072    Feb 29 2016 09:23:16  asdm-733.bin
ciscoasa#
```

On the inside Host, open a web browser and enter the url: https://192.168.1.1, install ASDM Launcher:



Use the username and password configured previously:



Task-4:

Configure the ASA as a DHCP server to dynamically assign IP addresses for DHCP clients on the inside network.

Configure a DHCP address pool and enable it on the ASA inside interface. This is the range of addresses to be assigned to inside DHCP clients. Set the range from 192.168.1.5 through 192.168.1.36.

Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).

```
ciscoasa(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)# dhcpd enable inside
```

The inside Host receives the IP address 192.168.1.5 and the default gateway 192.168.1.1:

Use the show dhcpd binding to see the binding entry IP/MAC of the inside Host:

```
ciscoasa# show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

192.168.1.50100.8cfa.29b4.53            3135 seconds    Automatic
ciscoasa#
```

Configure the Switch to receive an IP address using DHCP for interface vlan 3:

```
SW1(config)#int vlan 3
SW1(config-if)#ip add dhcp
SW1(config-if)#
*Mar  1 02:51:52.107: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan3 assigned DHCPaddress
192.168.1.6, mask 255.255.255.0, hostname SW1

SW1(config-if)#
```

```
ciscoasa# show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

192.168.1.50100.8cfa.29b4.53            3491 seconds    Automatic
192.168.1.60063.6973.636f.2d30.           3514 seconds    Automatic
                 3032.312e.6437.3537.
                 2e37.6234.312d.566c.
                 33
ciscoasa#
```

Task-5:

Configure the Switch SW1 to provide security against DHCP rogue server. The ASA should be the only DHCP server. Configure DHCP Snooping, this feature when enabled on a switch, all ports will transition into "untrusted" state, the untrusted port will discard incoming DHCP Offers, ACK or NACK, which means that the port that the ASA is connected to should be in "trusted" state.

Enable DHCP Snooping globally and apply to a the Vlan 3, (we can apply DHCP Snooping to a range of Vlans), also disable option 82:

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 3
SW1(config)#no ip dhcp snooping information option
```

The following command on fa1/0/1 interface ensures that the ASA is the only DHCP server. So this is the only port allowed to receive, DHCPOFFER, DHCPACK, DHCPNACK and DHCPLEASEQUERY:

```
SW1(config)#int fa1/0/1
SW1(config-if)#ip dhcp snooping trust
```

When DHCP Snooping is enabled, the Switch eavesdrops on the conversation between the untrusted ports and the DHCP Server connected to the trusted port and builds database snooping, in this database only the IP and MAC address of the devices that are connected to untrusted ports are tracked, in this case the only the IP/MAC binding is for the inside Host PC1:

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------
--------
00:8C:FA:29:B4:53192.168.1.5      3393        dhcp-snooping3FastEthernet1/0/2
Total number of bindings: 1

SW1#
```

The show ip dhcp snooping command below displays that only fa1/0/1 interface of SW1 is in trusted state, there the host (ASA) connected to this port is the only host that can act as a DHCP Server:

```
SW1#show ip dhcp snooping | beg Trusted
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet1/0/1yes        yes             unlimited
  Custom circuit-ids:
SW1#
```

Let's test the DHCP snooping, configure the router R1 with the IP address 192.168.1.1 and as a DHCP server, R1 simulate a rogue server and it will attempt to spoof the legitimate DHCP server:

```
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config)#ip dhcp pool SPOOF-DHCP
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1
```

Configure the port fa1/0/3 of SW1 in Vlan 3, remember that this port is in untrusted state therefore it is not allowed toreceive, DHCPOFFER, DHCPACK:

```
SW1(config)#int fa1/0/3
SW1(config-if)# switchport access vlan 3
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
```

Enable DHCP debugging:

```
SW1#debug dhcp detail
```

```
DHCP client activity debugging is on (detailed)
SW1#
```

```
SW1(config)#int vlan 3
SW1(config-if)#ip add dhcp
```

We can see from the debugging that only the DHCPDISCOVER is processed:

```
SW1(config-if)#
*Mar  1 03:39:54.281: DHCP: DHCP client process started: 10
*Mar  1 03:39:54.281: RAC: Starting DHCP discover on Vlan3
*Mar  1 03:39:54.281: DHCP: Try 1 to acquire address for Vlan3
*Mar  1 03:39:54.281: DHCP: allocate request
*Mar  1 03:39:54.281: DHCP: zapping entry in DHC_PURGING state for Vl3
*Mar  1 03:39:54.281: DHCP: deleting entry 6132FE4 0.0.0.0 from list
*Mar  1 03:39:54.281: Temp IP addr: 0.0.0.0  for peer on Interface: Vlan3
*Mar  1 03:39:54.290: Temp  sub net mask: 0.0.0.0
*Mar  1 03:39:54.290:    DHCP Lease server: 0.0.0.0, state: 10 Purging
*Mar  1 03:39:54.290:    DHCP transaction id: 1196
*Mar  1 03:39:54.290:    Lease: 0 secs,  Renewal: 0 secs,  Rebind: 0 secs
*Mar  1 03:39:54.290:    Next timer fires after: 00:00:11
*Mar  1 03:39:54.290:    Retry count: 0   Client-ID: cisco-0021.d757.7b41-Vl3
*Mar  1 03:39:54.290:    Client-ID hex dump: 636973636F2D303032312E643735372E
*Mar  1 03:39:54.290:                        376234312D566C33
*Mar  1 03:39:54.290:    Hostname: SW1
*Mar  1 03:39:54.290: DHCP: new entry. add to queue
*Mar  1 03:39:54.290: DHCP: SDiscover attempt # 1 for entry:
*Mar  1 03:39:54.290: Temp IP addr: 0.0.0.0  for peer on Interface: Vlan3
*Mar  1 03:39:54.290: Temp  sub net mask: 0.0.0.0
*Mar  1 03:39:54.290:    DHCP Lease server: 0.0.0.0, state: 3 Selecting
*Mar  1 03:39:54.290:    DHCP transaction id: 1485
*Mar  1 03:39:54.290:    Lease: 0 secs,  Renewal: 0 secs,  Rebind: 0 secs
*Mar  1 03:39:54.290:    Next timer fires after: 00:00:04
*Mar  1 03:39:54.290:    Retry count: 1   Client-ID: cisco-0021.d757.7b41-Vl3
*Mar  1 03:39:54.290:    Client-ID hex dump: 636973636F2D303032312E643735372E
*Mar  1 03:39:54.290:                        376234312D566C33
*Mar  1 03:39:54.290:    Hostname: SW1
*Mar  1 03:39:54.290: DHCP: SDiscover: sending 290 byte length DHCP packet
*Mar  1 03:39:54.290: DHCP: SDiscover 290 bytes
*Mar  1 03:39:54.290:             B'cast on Vlan3 interface from 0.0.0.0
*Mar  1 03:39:57.897: DHCP: SDiscover attempt # 2 for entry:
*Mar  1 03:39:57.897: Temp IP addr: 0.0.0.0  for peer on Interface: Vlan3
*Mar  1 03:39:57.897: Temp  sub net mask: 0.0.0.0
*Mar  1 03:39:57.897:    DHCP Lease server: 0.0.0.0, state: 3 Selecting
*Mar  1 03:39:57.897:    DHCP transaction id: 1485
*Mar  1 03:39:57.897:    Lease: 0 secs,  Renewal: 0 secs,  Rebind: 0 secs
*Mar  1 03:39:57.897:    Next timer fires after: 00:00:04
*Mar  1 03:39:57.897:    Retry count: 2   Client-ID: cisco-0021.d757.7b41-Vl3
*Mar  1 03:39:57.897:    Client-ID hex dump: 636973636F2D303032312E643735372E
*Mar  1 03:39:57.897:                        376234312D566C33
*Mar  1 03:39:57.897:    Hostname: SW1
```

```
*Mar  1 03:39:57.897: DHCP: SDiscover: sending 290 byte length DHCP packet
*Mar  1 03:39:57.897: DHCP: SDiscover 290 bytes
*Mar  1 03:39:57.897:             B'cast on Vlan3 interface from 0.0.0.0
*Mar  1 03:40:01.923: DHCP: SDiscover attempt # 3 for entry:
*Mar  1 03:40:01.923: Temp IP addr: 0.0.0.0  for peer on Interface: Vlan3
*Mar  1 03:40:01.923: Temp  sub net mask: 0.0.0.0
*Mar  1 03:40:01.923:    DHCP Lease server: 0.0.0.0, state: 3 Selecting
*Mar  1 03:40:01.923:    DHCP transaction id: 1485
*Mar  1 03:40:01.923:    Lease: 0 secs,  Renewal: 0 secs,  Rebind: 0 secs
*Mar  1 03:40:01.923:    Next timer fires after: 00:00:04
*Mar  1 03:40:01.923:    Retry count: 3   Client-ID: cisco-0021.d757.7b41-Vl3
*Mar  1 03:40:01.923:    Client-ID hex dump: 636973636F2D303032312E643735372E
*Mar  1 03:40:01.923:                        376234312D566C33
*Mar  1 03:40:01.923:    Hostname: SW1
*Mar  1 03:40:01.923: DHCP: SDiscover: sending 290 byte length DHCP packet
*Mar  1 03:40:01.923: DHCP: SDiscover 290 bytes
*Mar  1 03:40:01.923:             B'cast on Vlan3 interface from 0.0.0.0
*Mar  1 03:40:05.950: DHCP: QScan: Timed out Selecting state
SW1(config-if)#
```

Task-6:

Configure SW1 based on the following policy:

1-SW1 must inspect all the ARP messages on untrusted interfaces in VLAN 100.

2-SW1 must intercept and verify that the IP to MAC binding matches an entry in the the DHCP snooping table.

3-SW1 must drop the ARP packets, if the IP-to-MAC binding does not match the entry in the DHCP snooping table.

Configure ARP inspection to inspect ARP messages, DAI inspects all ARP packets and compares the IP/MAC binding in the incoming packets against DHCP snooping database, if it matches, the packets are allowed, if it does not match, the packets are dropped:

Configure SW1 so that it drops the ARP packets, if the IP/MAC binding does not match the entry in the dynamic built table.

The dynamic built table is the DHCP snooping binding of SW1 as shown by the show ip dhcp snooping binding command, the IP/MAC (192.168.1.5/00:8C:FA:29:B4:53) is still present:

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------
--------
00:8C:FA:29:B4:53192.168.1.5      3543        dhcp-snooping   3
FastEthernet1/0/2
Total number of bindings: 1

SW1#
```

Enable ARP inspection for VLAN 3 and configure the port fa1/0/1 connected to the DHCP Server ASA as trust port:

```
SW1(config)#ip arp inspection vlan 3
SW1(config)#int fa1/0/1
SW1(config-if)#ip arp inspection trust
```

Verify the ARP Inspection:

```
SW1#show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
3     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    3     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    3              2              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    3              1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    3                   0                        0                      0
SW1#
```

The following commands display which port is trusted (Fa1/0/1) and which port is untrusted (Fa10/2):

```
SW1#show ip arp inspection interfaces fastEthernet 1/0/1

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
Fa1/0/1Trusted               None              N/A
SW1#
```

```
SW1#show ip arp inspection interfaces fastEthernet 1/0/2
```

```
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
Fa1/0/2Untrusted               15                1
SW1#
```

Let's test ARP Inspection, disconnect the PC-A and connect the router R1, then configure the G0/1 with the IP address 192.168.1.5, remember this IP address is already assigned to PC-A so an entry in the DHCP Snooping Database is present with MAC Address of PC-A:

```
R1(config)#int g0/1
R1(config-if)#ip add 192.168.1.5 255.255.255.0
R1(config-if)#no shutdown
```

Let's verify the MAC Address of R1, the MAC's R1 is 2c54.2d5c.60c1:

```
R1#show int g0/1 | i bia
  Hardware is CN Gigabit Ethernet, address is 2c54.2d5c.60c1 (bia 2c54.2d5c.60c1)
R1#
```

From R1 ping the ASA at the IP address 192.168.1.1, the ping fails:

```
R1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

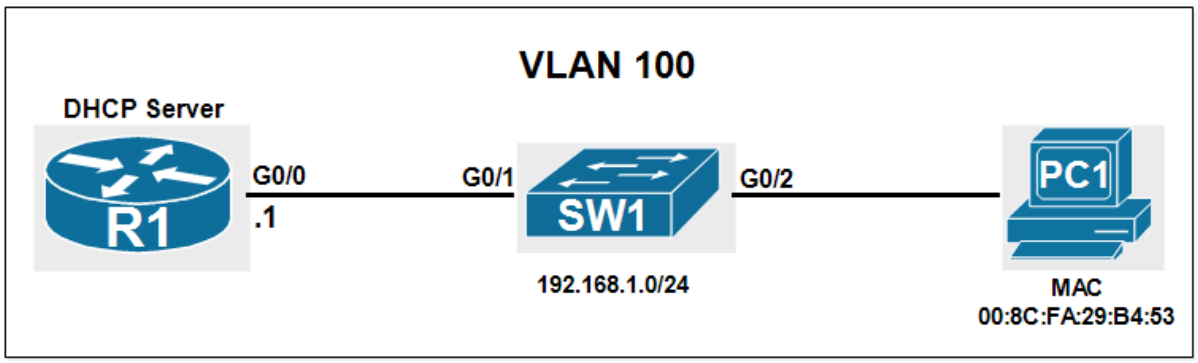
Since the MAC Address of R1 does not match an entry in the DHCP Snooping Database with the IP address 192.168.1.5, the SW1 displays the following output, the SW1 denies the ARP packet with source MAC Address 2c54.2d5c.60c1 because it does not match an entry in the DHCP snooping database table:

```
SW1#
*Mar  1 04:20:36.608: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Fa1/0/2, vlan 3.([2c54.2d5c.60c1/192.168.1.5/0000.0000.0000/192.168.1.1/04:20:36
UTC Mon Mar 1 1993])
*Mar  1 04:20:38.621: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Fa1/0/2, vlan 3.([2c54.2d5c.60c1/192.168.1.5/0000.0000.0000/192.168.1.1/04:20:38
UTC Mon Mar 1 1993])
*Mar  1 04:20:40.634: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Fa1/0/2, vlan 3.([2c54.2d5c.60c1/192.168.1.5/0000.0000.0000/192.168.1.1/04:20:40
UTC Mon Mar 1 1993])
*Mar  1 04:20:42.647: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Fa1/0/2, vlan 3.([2c54.2d5c.60c1/192.168.1.5/0000.0000.0000/192.168.1.1/04:20:42
UTC Mon Mar 1 1993])
*Mar  1 04:20:44.661: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Fa1/0/2, vlan 3.([2c54.2d5c.60c1/192.168.1.5/0000.0000.0000/192.168.1.1/04:20:44
UTC Mon Mar 1 1993])
SW1#
```

You can verify the Statistics of ARP Inspection using the show ip arp statistics to see the number of the packets dropped:

```
SW1#show ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
3             41             33             33              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    3             20              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    3                   0                        0                      0
SW1#
```

Lab 5: IP source guard



Task-1:

Configure R1 as DHCP server:

```
R1(config)#int g0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config)#ip dhcp pool TEST
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(config)#ip dhcp excluded-address 192.168.1.1
```

Configure the ports connected to R1 and PC1 in VLAN 100, enable spanning-tree porfast to avoid the listening and learning states of STP:

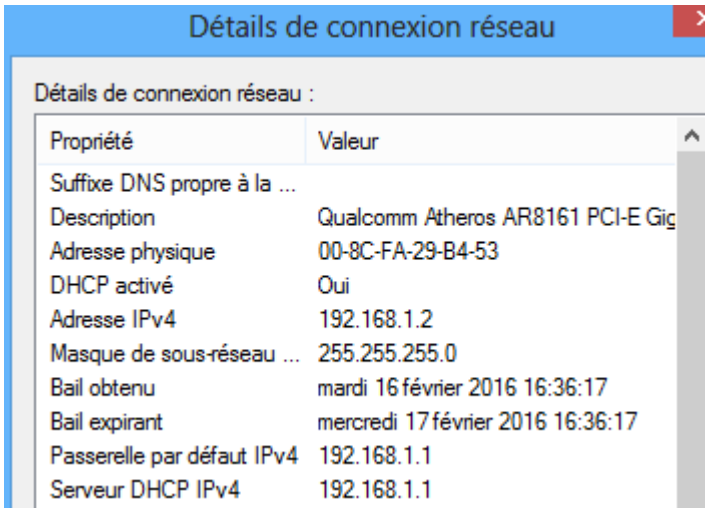
```
SW1(config-if)#interface GigabitEthernet0/1
SW1(config-if)# switchport access vlan 100
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
SW1(config)#interface GigabitEthernet0/2
SW1(config-if)# switchport access vlan 100
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
```

Task-2:

Enable DHCP snooping globally and for VLAN 100.
Configure the port g0/1 as a trusted port.

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 100
SW1(config)#
SW1(config)#int g0/1
SW1(config-if)# ip dhcp snoo trust
SW1(config)#no ip dhcp snooping information option
```

We can see below that R1 is allocating the IP address 192.168.1.2 to PC1:



On R1 use the show ip dhcp binding command to see the binding entry IP/MAC of the PC1:

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         0100.8cfa.29b4.53       Feb 17 2016 02:58 PM    Automatic
R1#
```

Since the PC2 receives the IP address 192.168.1.2 from the DHCP server R1, SW1 adds an entry IP/MAC in the DHCP snooping database table:

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------
--------
00:8C:FA:29:B4:53192.168.1.2      86289       dhcp-snooping100GigabitEthernet0/2
Total number of bindings: 1

SW1#
```

Task-3:

Configure the Switch SW1 so that when the source IP or MAC addresses of PC1 is changed, the traffic is dropped:

To perform this task we should configure IP source guard feature combined with port-security. IP source guard works with DHCP snooping, which means that the DHCP snooping must be enabled.

The IP source guard combined with port security means that the traffic is allowed when the source IP and MAC address matches an entry in the DHCP snooping binding database or a static IP source binding configured.

Let's enable IP source guard and port security on G0/2:

```
SW1(config)#int g0/2
SW1(config-if)#ip verify source port-security
SW1(config-if)#switchport port-security
```

And since the IP source guard is enabled, the Switch SW1 adds an entry in the source guard binding, in the Filter-type field, the "ip-mac" means that IP source Guard is configured with Port Security to prevent IP and MAC spoofing attacks:

```
SW1#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
Log
---------  -----------  -----------  ---------------  -----------------  ----   --
-
Gi0/2ip-mac       active       192.168.1.200:8C:FA:29:B4:53  100    disabled
SW1#
```

From PC1, ping the R1 IP address 192.168.1.1, the ping should be successfull:

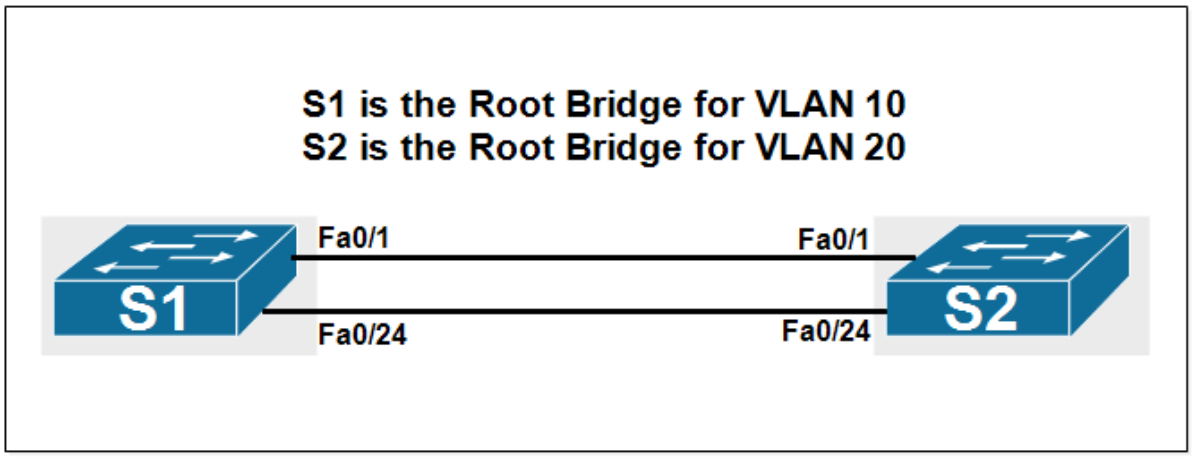
```
C:\Users\user>ping 192.168.1.1

Envoi d'une requête 'Ping'  192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\user>
```

Let's configure the PC1 with a static IP address 192.168.1.3:

Let's test the connectivity, the ping fails because the IP source Guard does not find an entry 00:8C:FA:29:B4:53/192.168.1.3 in the DHCP Snooping Database, 00:8C:FA:29:B4:53/192.168.1.2 is the valid entry. PC1 is trying to connect with a valid source MAC Address (or spoofed source MAC address) but with different source IP address. As a result the IP source Guard drops the packets coming from PC1 to prevent MAC spoofing attack:

```
C:\Users\user>ping 192.168.1.1

Envoi d'une requête 'Ping'  192.168.1.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\user>
```

Lab 6: Spanning-tree Loop Guard



Task-1:

Creates VLANs 10 and 20:

```
S1(config)#vlan 10
S1(config-vlan)#name TEST-10
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name TEST-20
```

```
S2(config)#vlan 10
S2(config-vlan)#name TEST-10
S2(config-vlan)#exit
S2(config)#vlan 20
S2(config-vlan)#name TEST-20
```

Task-2:

S1 should be the primary Root for VLAN 10 and the secondary Root for VLAN 20.
S2 should be the primary Root for VLAN 20 and the secondary Root for VLAN 10.

```
S1(config)#spanning-tree vlan 10 root primary
S1(config)#spanning-tree vlan 20 root secondary
```

```
S2(config)#spanning-tree vlan 20 root primary
S2(config)#spanning-tree vlan 10 root secondary
```

Use the The show spanning-tree vlan 10 and show spanning-tree vlan 20 commands to verify the port roles of S1, S1'fa0/24 is blocked for VLAN 20.

```
S1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     2c36.f82a.8b00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     2c36.f82a.8b00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Desg FWD 19        128.1    P2p
Fa0/24              Desg FWD 19        128.24   P2p


S1#
S1#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     2c36.f816.bc80
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     2c36.f82a.8b00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/24              Altn BLK 19        128.24   P2p


S1#
```

Task-3:

In STP, switches rely on continuous reception or transmission of BPDUs, depending on the port role. A designated port transmits BPDUs whereas a nondesignated port receives BPDUs. Bridging loops occur when a port erroneously transitions to forwarding state because it has stopped receiving BPDUs.

Ports with loop guard enabled do an additional check before transitioning to forwarding state. If a nondesignated port stops receiving BPDUs, the switch places the port into the STP loop-inconsistent blocking state.
If a switch receives a BPDU on a port in the loop-inconsistent STP state, the port transitions through STP states according to the received BPDU. As a result, recovery is automatic, and no manual intervention is necessary.

To stop receiving the BPDU frames on S1'fa0/24 we will enable the BPDU filter feature on S2'fa0/24:

```
S2(config-if)#int fa0/24
S2(config-if)#spanning-tree bpdufilter enable
```

This command tells to S2 to stop sending BPDU frames out the fa0/24 interface, because S1 does not receive the BPDU on the port fa0/24, it assumes the port designated port and puts this port in the Forwarding state creating a loop as shown by the show spanning-tree vlan 20 command.

```
S1#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     2c36.f816.bc80
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     2c36.f82a.8b00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/24              Desg FWD 19        128.24   P2p


S1#
```

With loop guard feature if BPDUs are not received on a non-designated port, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state.

Disable BDPU filter on S2 and enable loop guard on S1'fa0/24 as follow:

```
S2(config)#int fa0/24
S2(config-if)#spanning-tree bpdufilter disable
```

```
S1(config)#int fa0/24
S1(config-if)#spanning-tree guard loop
```

Enable BPDU filter once again to see loop guard operation:

```
S2(config)#int fa0/24
S2(config-if)#spanning-tree bpdufilter enable
```

After stopping the sending of the BPDU frames on S2'fa0/24 , the loop guard blocks the inconsistent port fa0/24 as shown by the show spanning-tree vlan 20 and show spanning-tree inconsistentports commands:

```
S1#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID     Priority    24596
              Address     2c36.f816.bc80
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28692  (priority 28672 sys-id-ext 20)
              Address     2c36.f82a.8b00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/24              Desg BKN*19        128.24   P2p *LOOP_Inc


S1#
```

```
S1#show spanning-tree inconsistentports

Name                 Interface               Inconsistency
-------------------- ----------------------- ------------------
VLAN0001             FastEthernet0/24        Loop Inconsistent
VLAN0020             FastEthernet0/24        Loop Inconsistent

Number of inconsistent ports (segments) in the system : 2

S1#
```

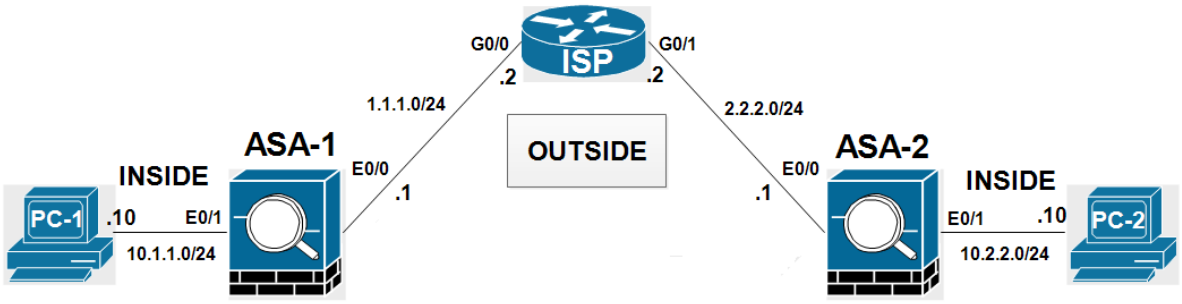
Disable the BDPU filter on S2'fa0/24 :

```
S2(config)#int fa0/24
S2(config-if)#spanning-tree bpdufilter disable
```

Now the port fa0/24 is assuming the normal blocking state after receiving the BPDUs:

```
S1#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     2c36.f816.bc80
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     2c36.f82a.8b00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/24              Altn BLK 19        128.24   P2p


S1#
```

Lab 7: Network Time Protocol NTP between ASA and IOS router



Configure IP addressing as illustrated in the topology:

On ASA-1:

```
ASA-1(config)#interface Vlan1
ASA-1(config-if)#nameif inside
ASA-1(config-if)#security-level 100
ASA-1(config-if)#ip address 10.1.1.1 255.255.255.0
```

```
ASA-1(config)#interface Vlan2
ASA-1(config-if)#nameif outside
ASA-1(config-if)#security-level 0
ASA-1(config-if)#ip address 1.1.1.1 255.255.255.0
```

```
ASA-1(config)#int e0/0
ASA-1(config-if)#switchport mode access
ASA-1(config-if)#switchport access vlan 2
```

```
ASA-1(config)#int e0/1
ASA-1(config-if)#switchport mode access
ASA-1(config-if)#switchport access vlan 1
```

On ASA-2:

```
ASA-2(config)#interface Vlan1
ASA-2(config-if)#nameif inside
ASA-2(config-if)#security-level 100
ASA-2(config-if)#ip address 10.2.2.1 255.255.255.0
```

```
ASA-2(config)#interface Vlan2
ASA-2(config-if)#nameif outside
ASA-2(config-if)#security-level 0
ASA-2(config-if)#ip address 2.2.2.1 255.255.255.0
```

```
ASA-2(config)#int e0/0
ASA-2(config-if)#switchport mode access
ASA-2(config-if)#switchport access vlan 2
```

```
ASA-2(config)#int e0/1
ASA-2(config-if)#switchport mode access
ASA-2(config-if)#switchport access vlan 1
```

Verification:

```
ASA-1# show run in vlan 1
!
interface Vlan1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
ASA-1#
ASA-1# show run in vlan 2
!
interface Vlan2
nameif outside
security-level 0
ip address 1.1.1.1 255.255.255.0
ASA-1#
```

```
ASA-2# show run int vlan 1
!
interface Vlan1
nameif inside
security-level 100
ip address 10.2.2.1 255.255.255.0
ASA-2#
ASA-2# show run int vlan 2
!
interface Vlan2
nameif outside
security-level 0
ip address 2.2.2.1 255.255.255.0
ASA-2#
```

Configure a static default route for internet access:

On ASA-1:

```
ASA-1(config)#route outside 0 0 1.1.1.2
```

On ASA-2:

```
ASA-2(config)#route outside 0 0 2.2.2.2
```

To ensure all devices in the network have the same time configure NTP server on ISP with a stratum of 4. The server should authenticate the clients ASA-1 and ASA-2 with a password of "cisco_ntp":

```
R1(config)#ntp authentication-key 1 md5 cisco_ntp
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
R1(config)#ntp master 4
```

Configure ASA-1 and ASA-2 as clients NTP:

```
ASA-1(config)# ntp authentication-key 1 md5 cisco_ntp
ASA-1(config)# ntp authenticate
ASA-1(config)# ntp trusted-key 1
ASA-1(config)# ntp server 1.1.1.2 key 1
```

```
ASA-2(config)# ntp authentication-key 1 md5 cisco_ntp
ASA-2(config)# ntp authenticate
ASA-2(config)# ntp trusted-key 1
ASA-2(config)# ntp server 1.1.1.2 key 1
```

Verification of NTP status using the show ntp status command and the show ntp associations command:

Note that R1 (the master) is synchronized with 127.127.7.1. This is an internaly created IP address of internal NTP server which instance has been created after issuing "ntp master" command:

```
ISP#show ntp status
Clock is synchronized, stratum 4, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is DB49AE2C.082FD8C4 (11:17:00.031 UTC Mon Aug 1 2016)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.28 msec, peer dispersion is 0.24 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 3 sec ago.
ISP#
```

```
ISP#show ntp associations

address         ref clock       st   when   poll reach  delay  offset   disp
*~127.127.1.1     .LOCL.           3      5     16   377  0.000   0.000  0.218
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
ISP#
```

Verify that ASA-1 and ASA-2 are assiociated with ISP:

On ASA-1:

```
ASA-1# show ntp associations
address         ref clock     st  when  poll reach  delay  offset    disp
*~1.1.1.2          127.127.1.1       4    35    64    7     0.7    4.22    17.9
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
ASA-1#
```

```
ASA-1# show ntp status
Clock is synchronized, stratum 5, reference is 1.1.1.2
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is db49aedd.194c29da (11:19:57.098 UTC Mon Aug 1 2016)
clock offset is 5.2097 msec, root delay is 0.63 msec
root dispersion is 23.38 msec, peer dispersion is 17.73 msec
ASA-1#
```

On ASA-2:

```
ASA-2# show ntp associations
address         ref clock     st  when  poll reach  delay  offset    disp
*~1.1.1.2          127.127.1.1       4    27    64   17     0.7  -11.19  1891.6
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
ASA-2#
```

```
ASA-2# show ntp status
Clock is synchronized, stratum 5, reference is 1.1.1.2
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is db49af0f.9395dea9 (11:20:47.576 UTC Mon Aug 1 2016)
clock offset is -11.1874 msec, root delay is 0.67 msec
root dispersion is 1903.27 msec, peer dispersion is 1891.62 msec
ASA-2#
```

ISP is the NTP master and ASA is synced with it. The asterisk in the show ntp associations command indicates that.
Address field contains an IP address of the NTP peer.
Ref clock field (reference clock) contains an IP address of reference clock of peer.
Note that stratum for this peer is 5 (every next NTP peer in the NTP path will results of increased stratum value).

Verify the time using the show clock:

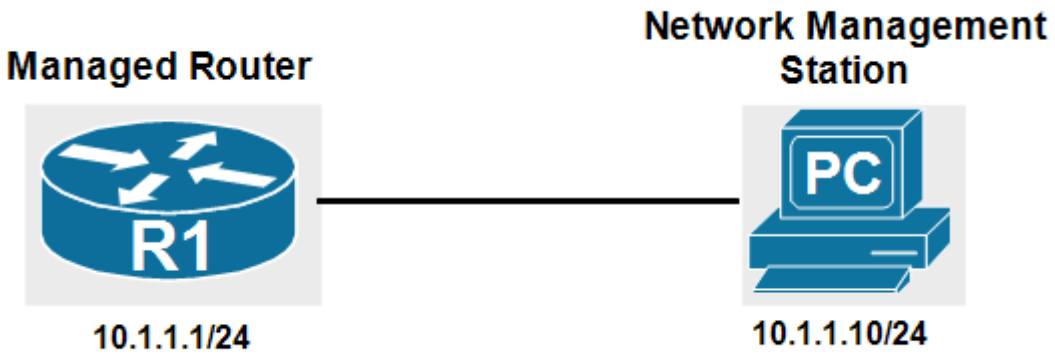
```
ISP#show clock
11:22:57.615 UTC Mon Aug 1 2016
ISP#
```

```
ASA-1# show clock
11:23:49.631 UTC Mon Aug 1 2016
ASA-1#
```

```
ASA-2# show clock
11:24:24.390 UTC Mon Aug 1 2016
```

```
ASA-2#
```

Lab 8: SNMPv3 on IOS Router



SNMP uses the concept of a Management Information Base (MIB). MIBs are databases of status configuration information that are stored in tree structures. A management system requests access to parts of the database by specifying the path that is taken from the root to the data's location. The MIB path is generally referred to as an OID or object ID.

View can be defined which limit which branches of tree are available for reading or writing by different SNMP management systems. Define an SNMP view named write-view which include access to all branches below 1.3.6.1.2.1.

Configure an SNMP version 3 group named GRP-SNMP with priv mode security that is provided write authorization as defined by the view named write-view.

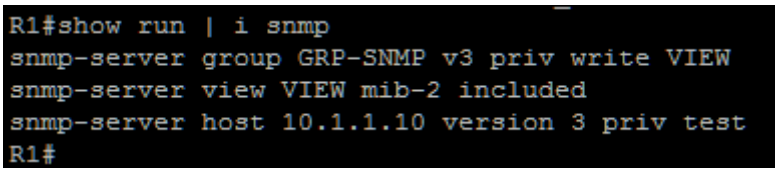
```
R1(config)#snmp-server view VIEW mib-2 included
R1(config)#snmp-server group GRP-SNMP v3 priv write VIEW
```

Configure an SNMPv3 user named test that is assigned to the group named GRP-SNMP. Configure SHA as the authentication algorithm using test as the shared key. Also configure 128-bit AES as the encryption algorithm using test-user as the shared encryption key.

Note a console message is displayed that you should indicates that you should wait.

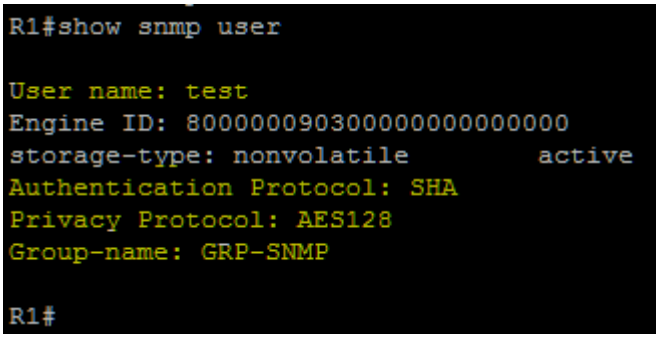
```
R1(config)#snmp-server user test GRP-SNMP v3 auth sha test priv aes 128 test-user
R1(config)#
Aug 17 10:08:53.439: Configuring snmpv3 USM user, persisting snmpEngineBoots.
Please Wait...

R1(config)#
```

Verify all the commands in the running configuration, note the snmp-server user command is not part of the running configuration.




```
R1#show run | i snmp
snmp-server group GRP-SNMP v3 priv write VIEW
snmp-server view VIEW mib-2 included
snmp-server host 10.1.1.10 version 3 priv test
R1#
```

Verify that the SNMP user war created using the show snmp user.

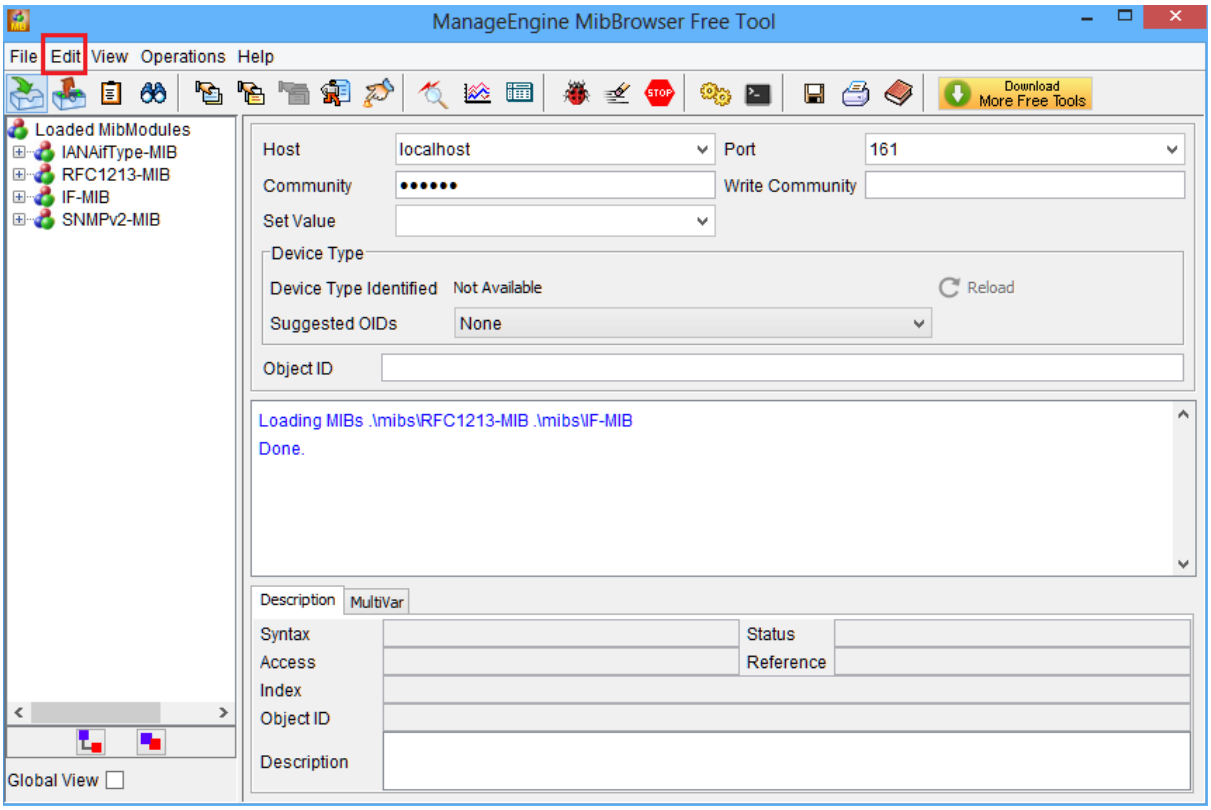



```
R1#show snmp user

User name: test
Engine ID: 800000090300000000000000
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: GRP-SNMP

R1#
```

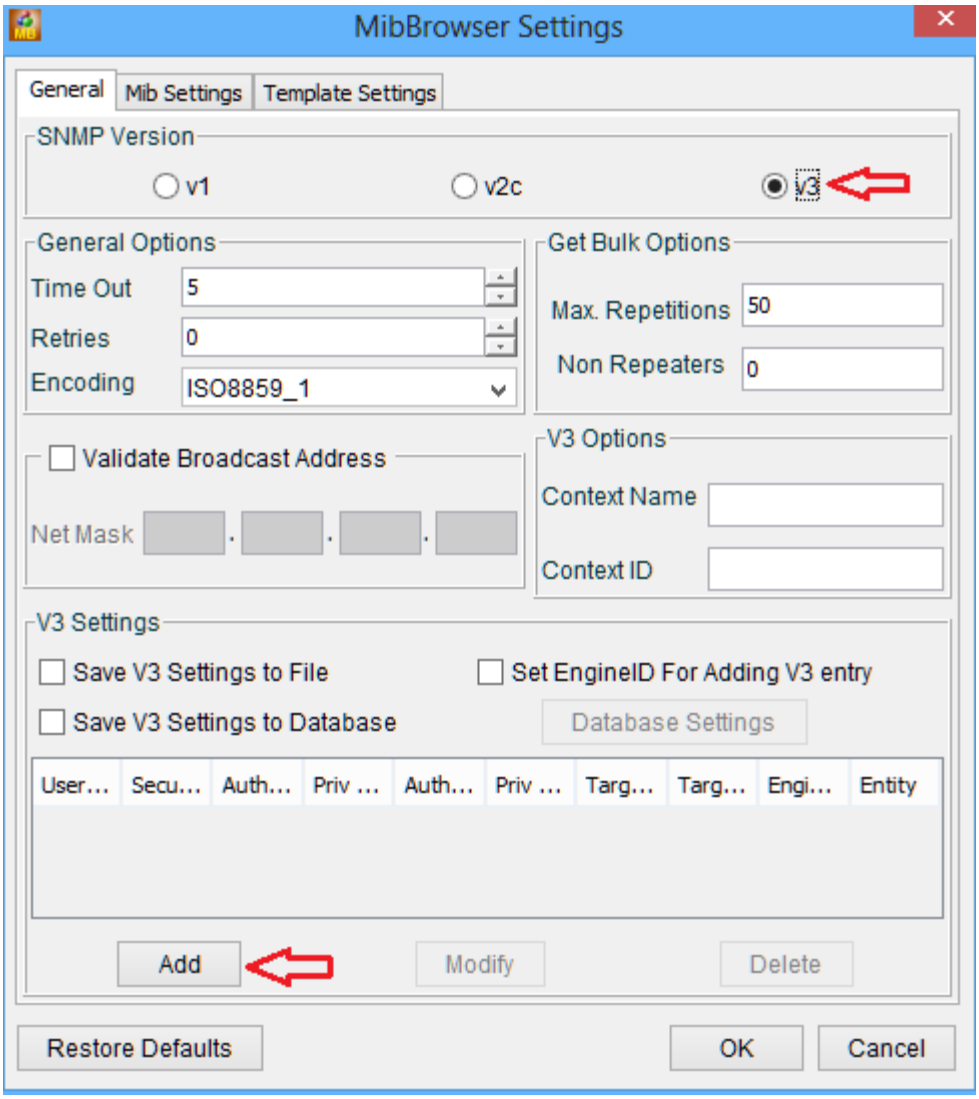
Configure the PC 10.1.1.10 as the destination of SNMP traps, specifiying that the algorithms and keys that are associated with the SNMP user test are to be used and enable the forwarding of traps to PC.

```
R1(config)#snmp-server host 10.1.1.10 traps version 3 priv test
R1(config)#snmp-server enable traps
```

Access the PC, launch Manage MibBrowser Tool. The tool must be configured to communicate with R1.
First edit Settings. The MibBrowser settings window opens.

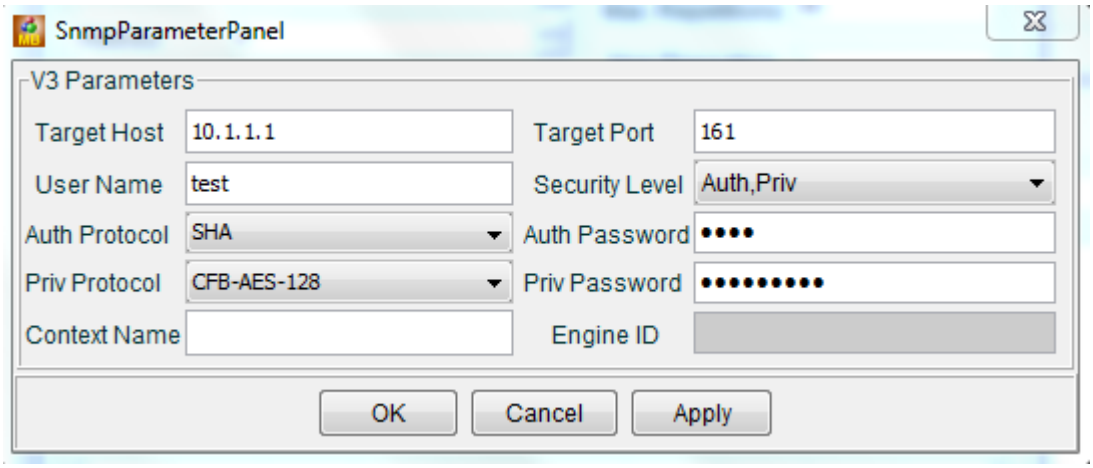


Select version 3 in the SNMP version field, and then click add below.
The SnmpParameterPanel window opens.

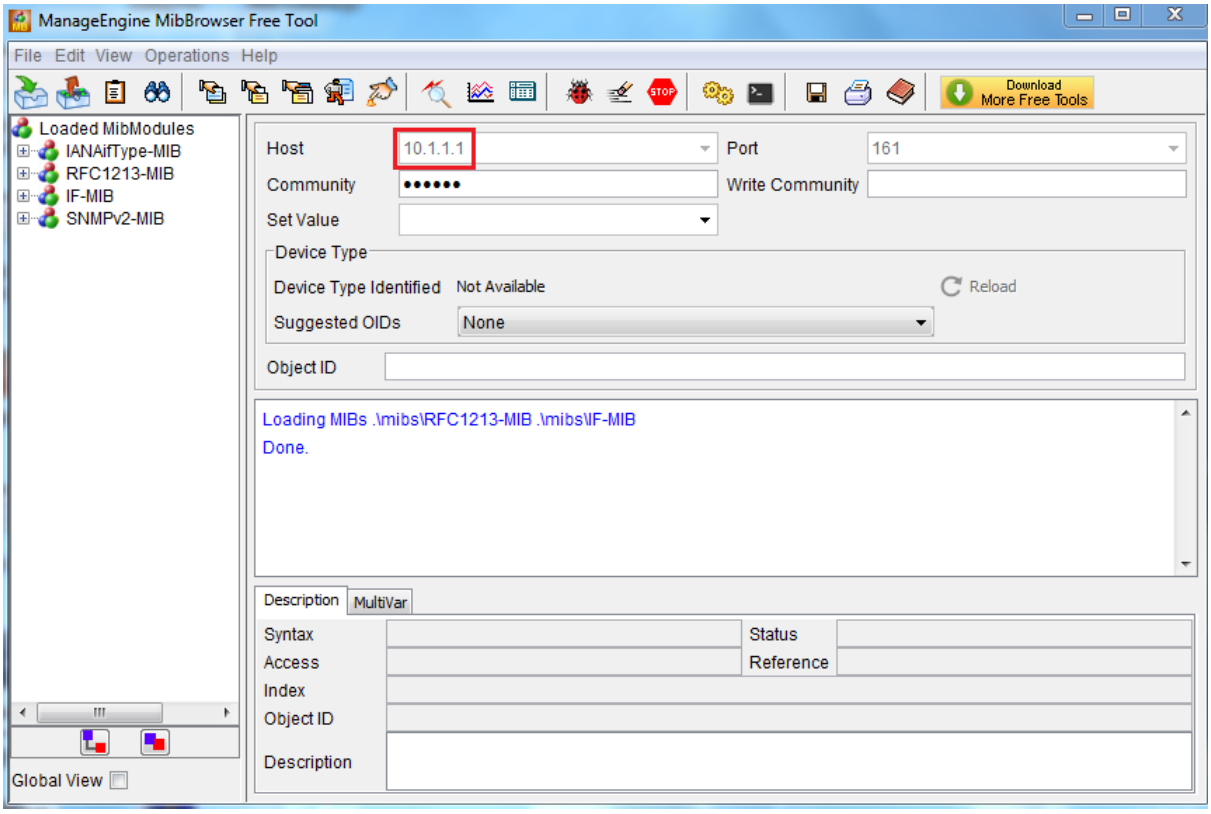


Fill in the fields as follow:

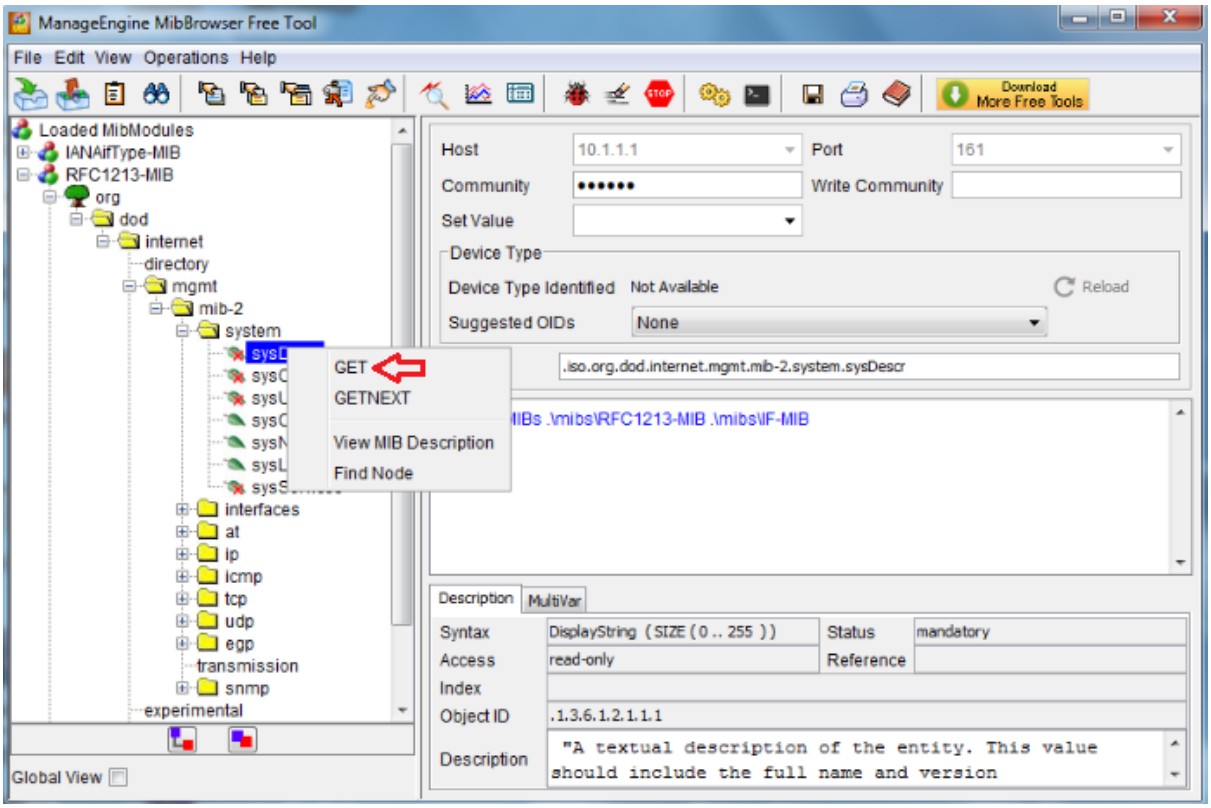
Target Host: **10.1.1.1**
Target Port: **161**
User Name: **user**
Security Level: **Auth, Priv**
Auth Protocol: **SHA**
Auth Password: **auth-pass**
Priv Protocol: **CFB-AES-128**
Priv Password: **priv-pass**



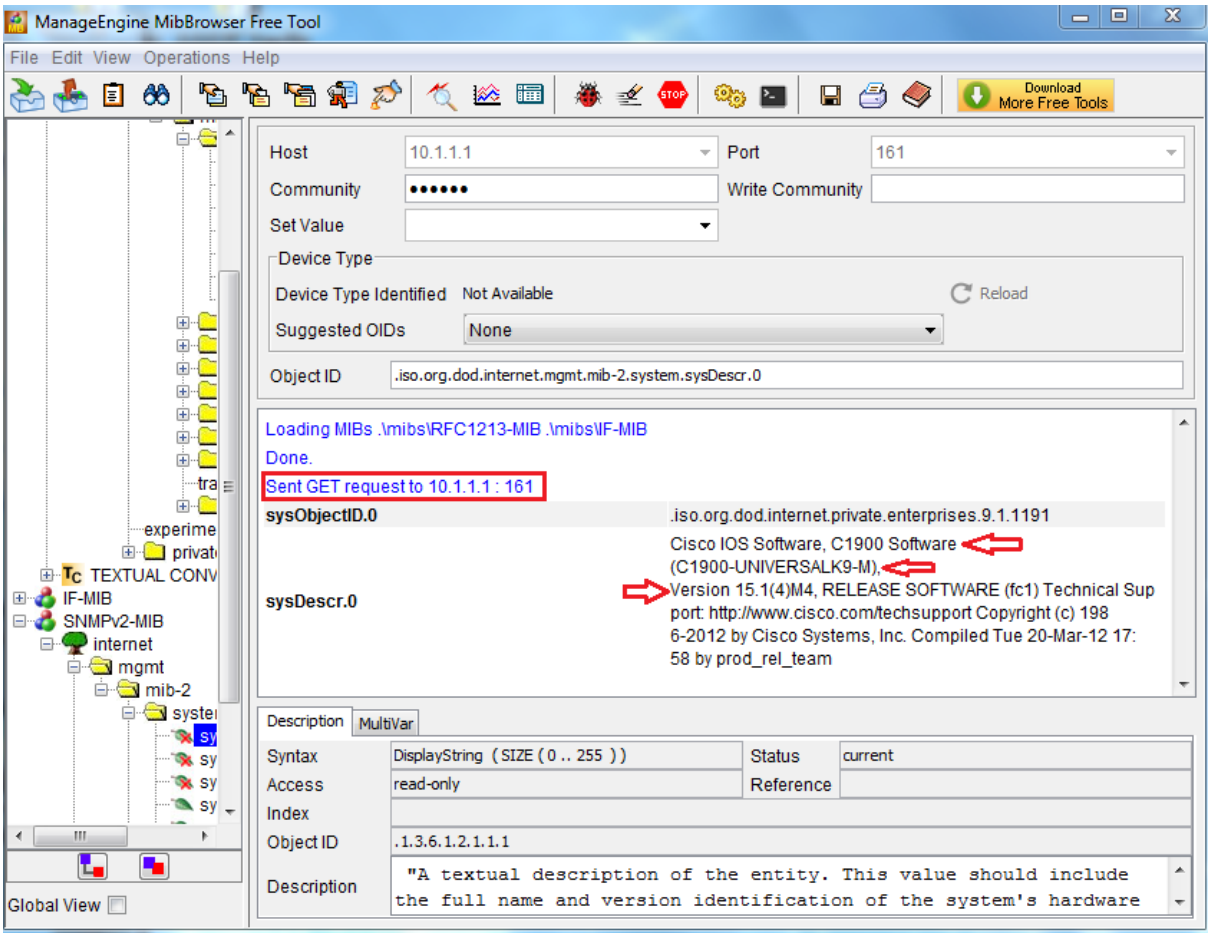
Click OK on the SnmpParameterPanel window. Click OK on the MibBrowser Settings window to return to the main application.



In the main window of the MibBrowser application, expand RFC1213-MIB org dod internet mgmt mib-2 system sysDser. Right-click on sysDser and click GET.

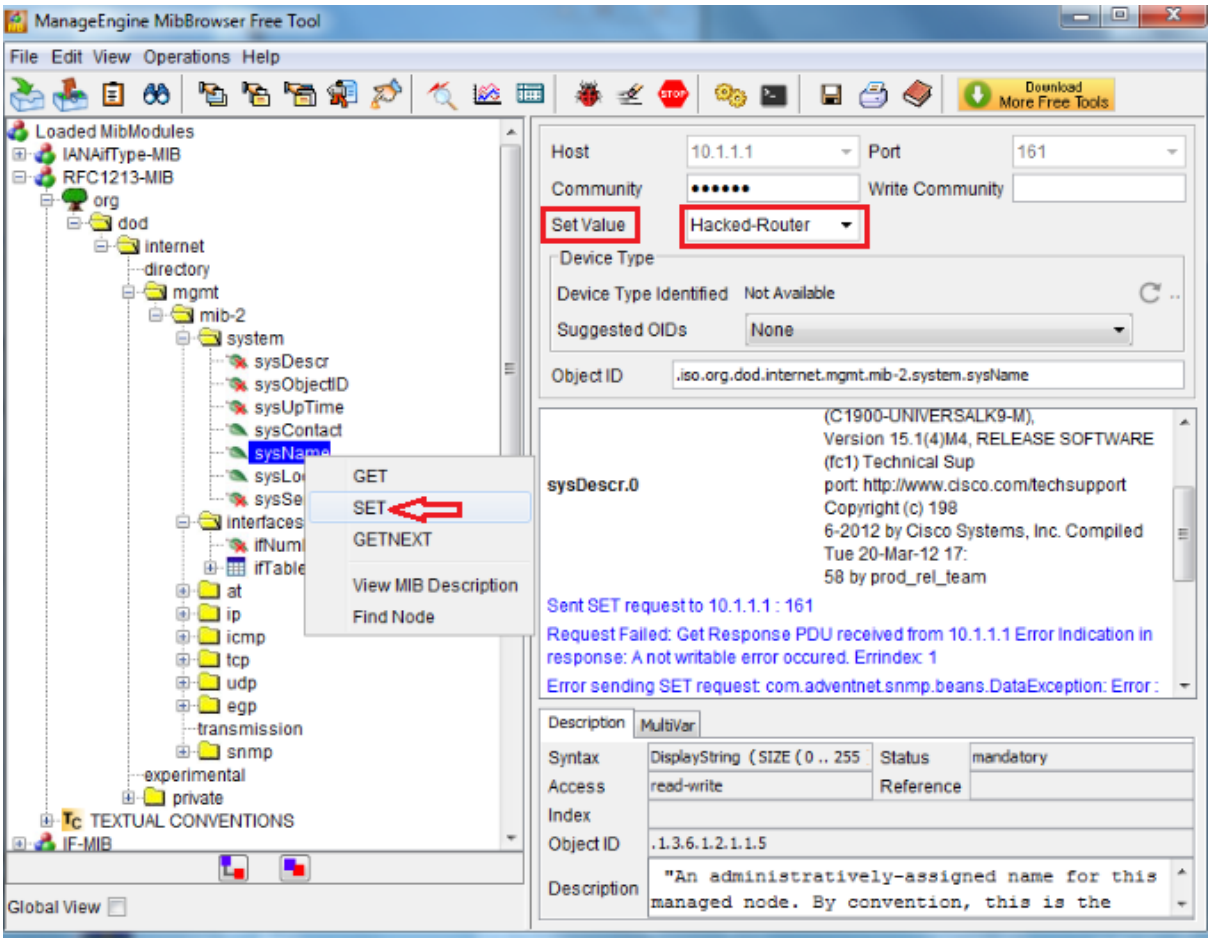


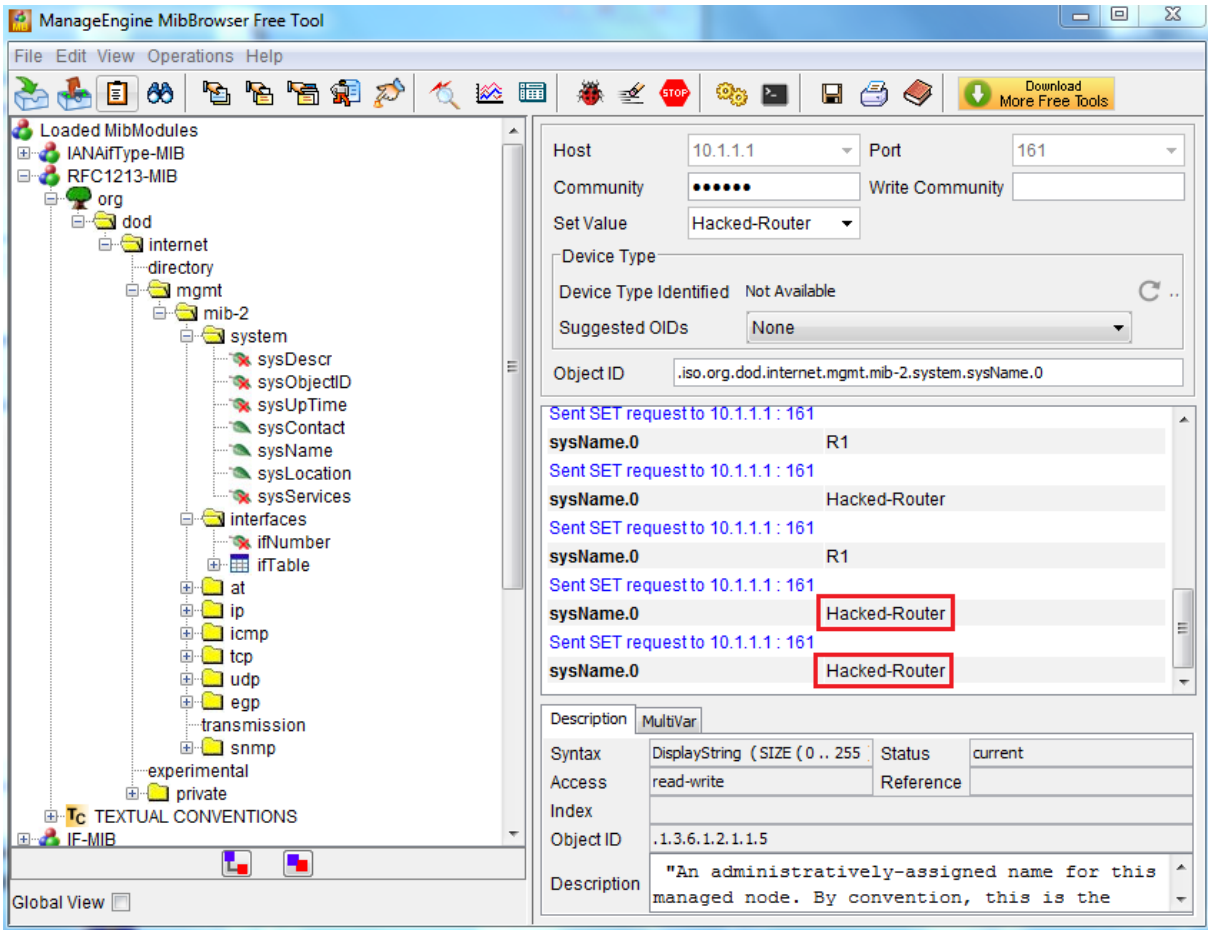
You should see that the value of sysDescr.0 contains a description of the operation system running on R1.



Verify that the write operations are also supported. Enter Hacked-router in the Set Value.

Righ-click sysName again, but select SET. A similar reponse appears in the results field showing the new setting for the sysName.


ManageEngine MibBrowser Free Tool
File Edit View Operations Help
Download More Free Tools
Loaded MibModules
IANAifType-MIB
RFC1213-MIB
org
dod
internet
directory
mgmt
mib-2
system
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLo
sysSe
interfaces
ifNum
ifTable
at
ip
icmp
tcp
udp
egp
transmission
snmp
experimental
private
TEXTUAL CONVENTIONS
IF-MIB
Global View
GET
SET
GETNEXT
View MIB Description
Find Node
Host 10.1.1.1 Port 161
Community ••••••
Write Community
Set Value
Hacked-Router
Device Type
Device Type Identified Not Available
Suggested OIDs None
Object ID .iso.org.dod.internet.mgmt.mib-2.system.sysName
sysDescr.0
(C1900-UNIVERSALK9-M),
Version 15.1(4)M4, RELEASE SOFTWARE
(fc1) Technical Sup
port: http://www.cisco.com/techsupport
Copyright (c) 198
6-2012 by Cisco Systems, Inc. Compiled
Tue 20-Mar-12 17:
58 by prod_rel_team
Sent SET request to 10.1.1.1 : 161
Request Failed: Get Response PDU received from 10.1.1.1 Error Indication in response: A not writable error occured. Errindex: 1
Error sending SET request: com.adventnet.snmp.beans.DataException: Error :
Description
MultiVar
Syntax DisplayString (SIZE (0 .. 255
Status mandatory
Access read-write
Reference
Index
Object ID .1.3.6.1.2.1.1.5
Description "An administratively-assigned name for this managed node. By convention, this is the



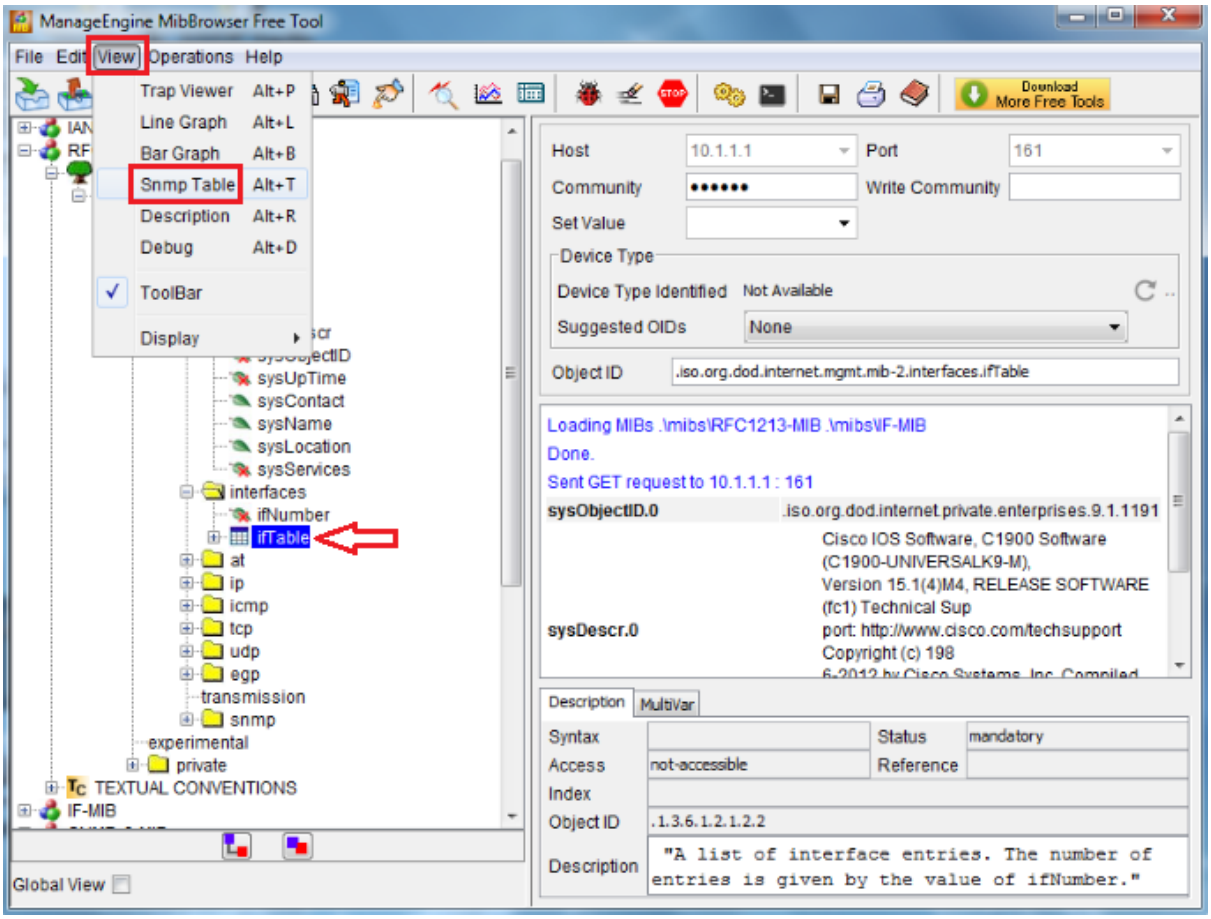
Return to the console of R1, you can see that now the hostname of the router is: Hacked-router.

```
R1#
Aug 17 10:43:08.795: %SYS-5-CONFIG_I: Configured from 10.1.1.10 by snmp
Hacked-Router#
Hacked-Router#
```

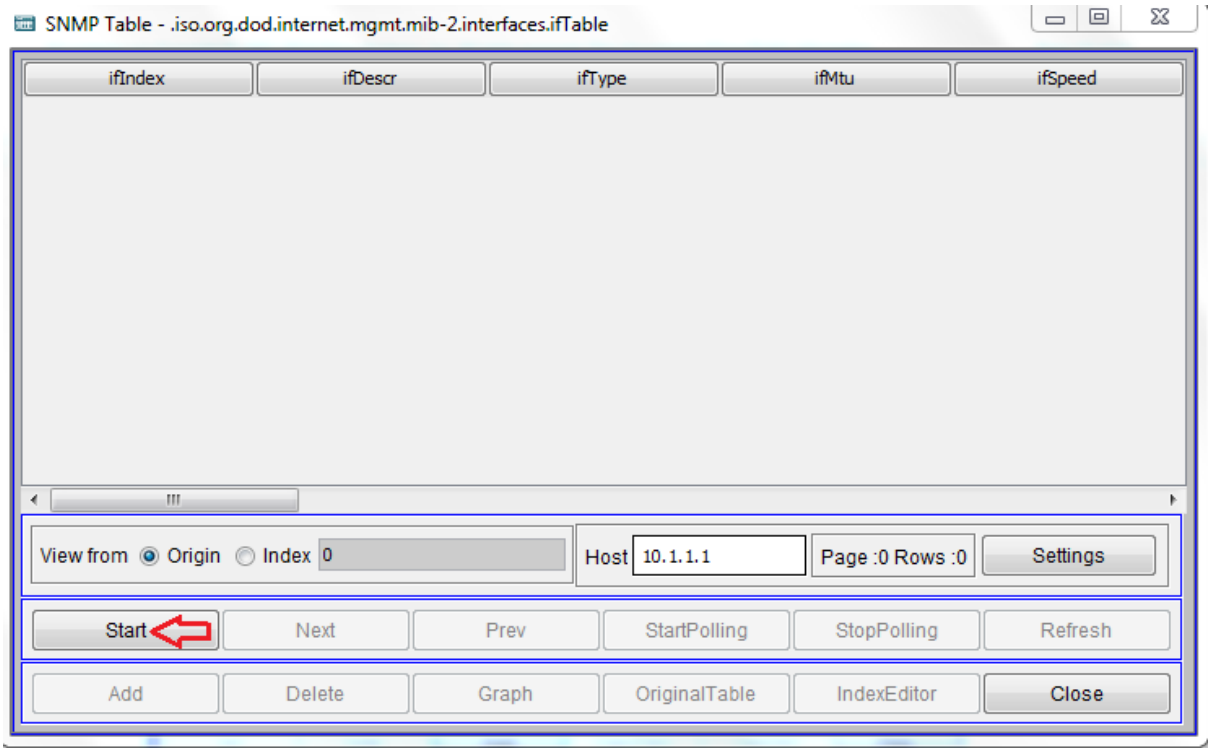
```
R1#
Aug 17 10:43:08.795: %SYS-5-CONFIG_I: Configured from 10.1.1.10 by snmp
Hacked-Router#
Hacked-Router#
```

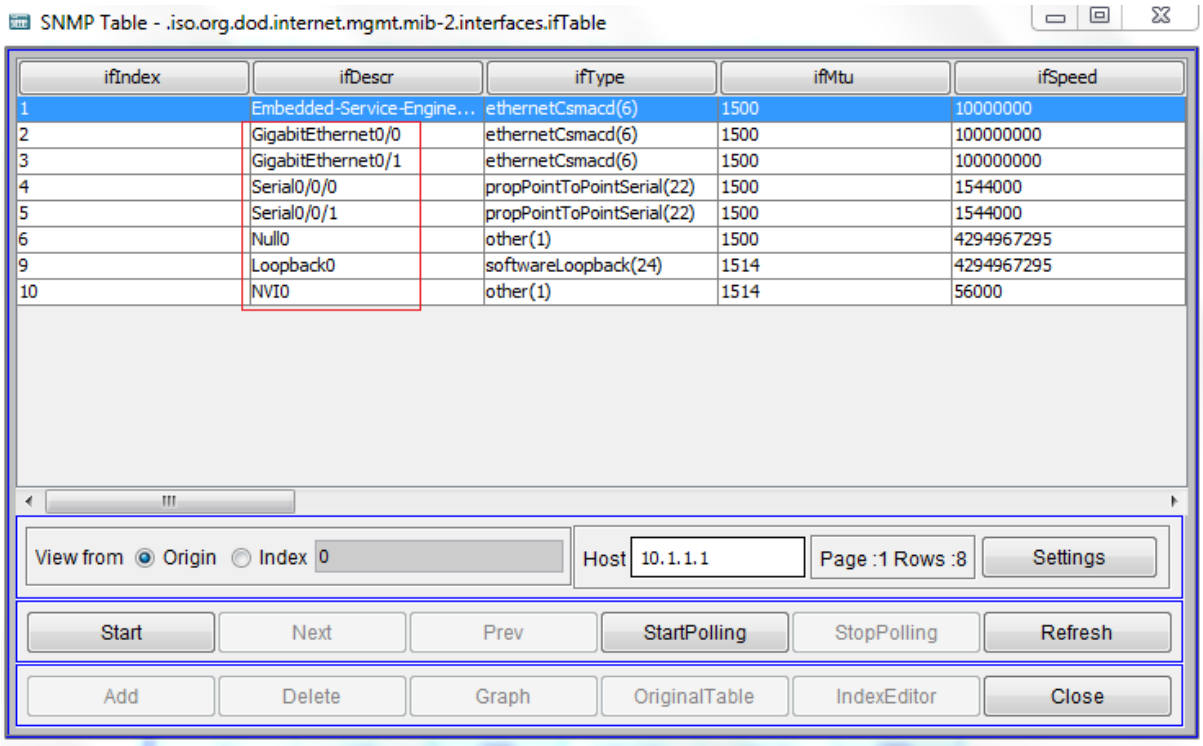
It is important to know that you have a write authority via SNMP just as privilege 15 from the device's command line. So it is very important to keep SNMP secured.

Select the ifTable entry and then on the file menu select View and Snmp Table, and a table will be built showing interface data from R1.



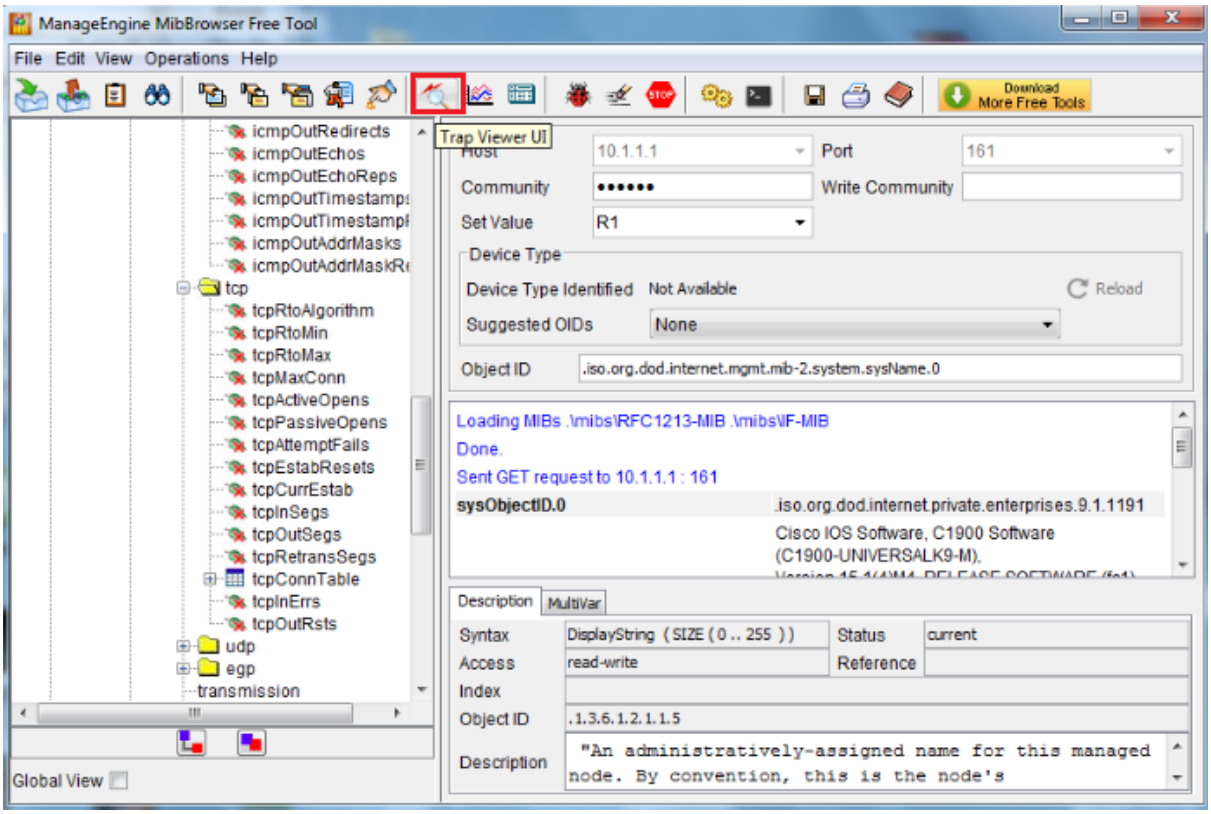
In the SNMP Table window, press Start and you should see interface information populated from R1.



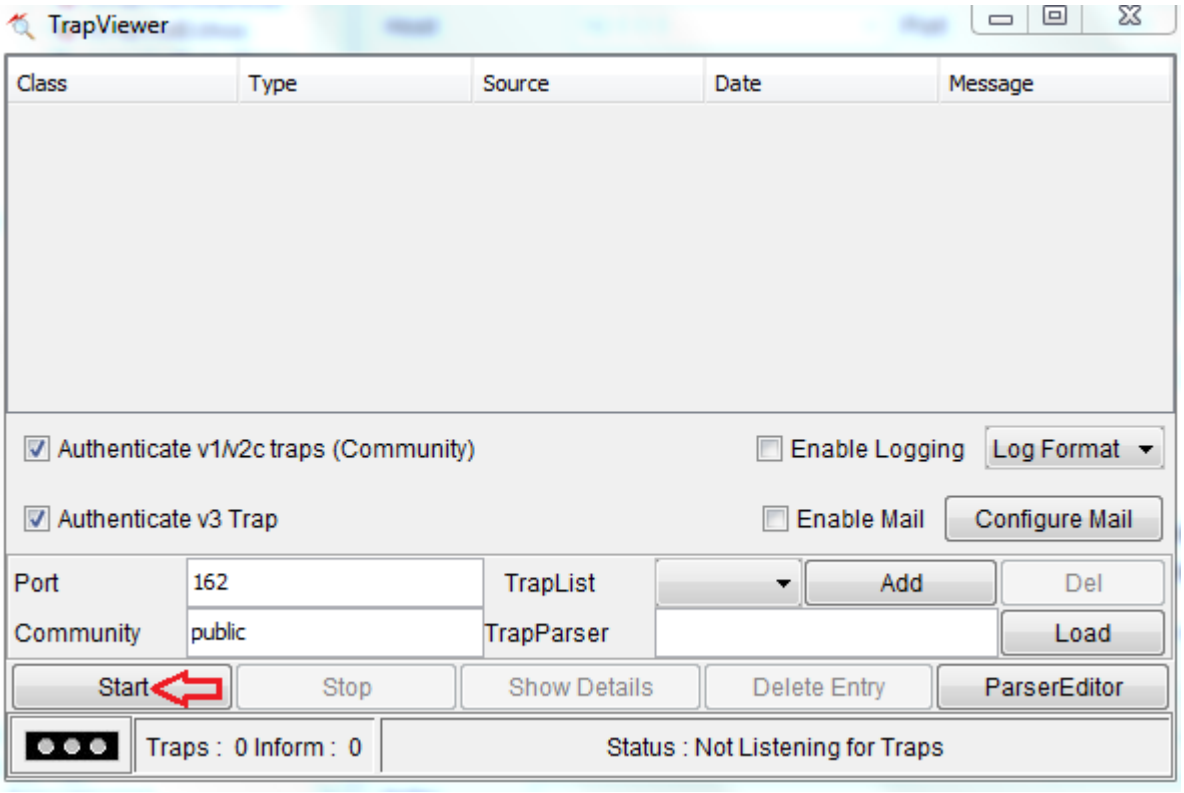


Now let's look at SNMPv3 traps.

Return to PC. In the MibBrowser click on the icone Trap Viewer as shown below.



Click start button.



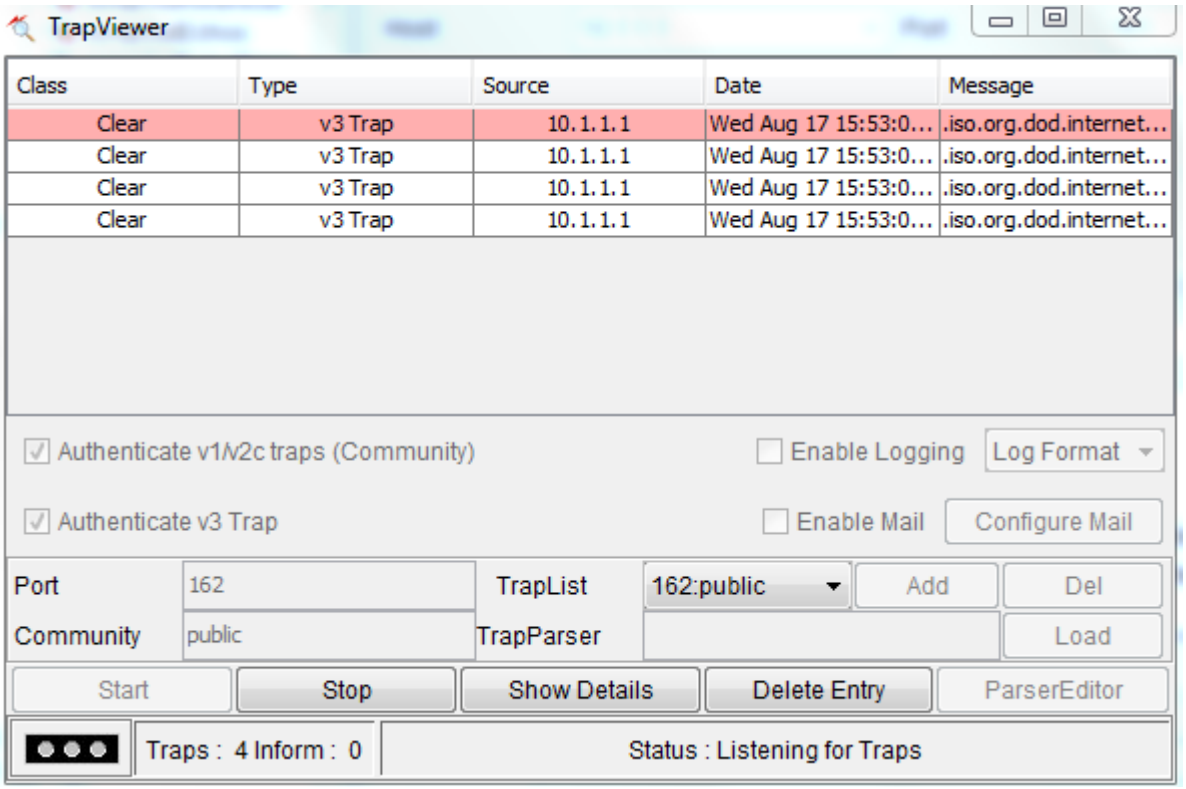
In the console of R1 enable the loopback interface.

```
R1#show ip int br | i Loo
Loopback0                  unassigned      YES unset  administratively down down
R1#
```

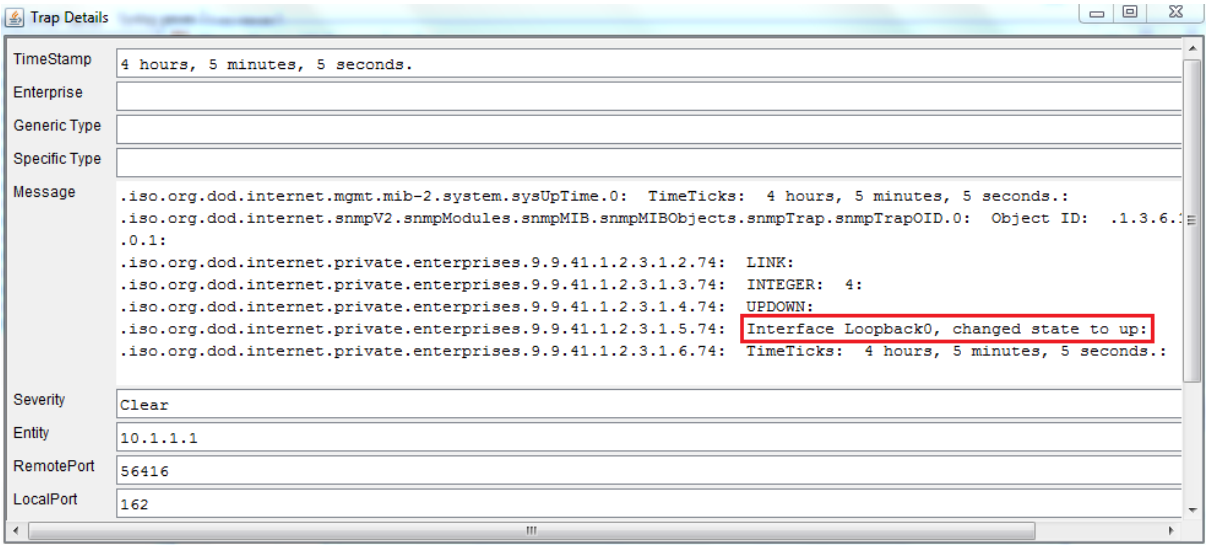

```
R1#show ip int br | i Loo
Loopback0                  unassigned      YES unset  administratively down down
R1#
```


```
R1(config)#int lo0
R1(config-if)#no shutdown
```

Return to PC, we can see that a traps are displayed in the TrapViewer window.



Click in the Show Details field, we can see the information of the trap about the loopback interface.



The CPU threshold Notification enables you to define rising and falling thresholds associated with CPU utilization using the process cpu threshold configuration command. The notifications are delivered via SNMP.

Let's configure the CPU threshold notification, choose a rising option with a threshold 1 percent.

```
R1(config)#process cpu threshold type total rising 2 interval 5
```

Verify the current CPU utilization using the show process CPU command.

```
R1#show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           8          36        222  0.00%  0.00%  0.00%   0 Chunk Manager
   2          48        2737         17  0.00%  0.01%  0.00%   0 Load Meter
   3        2432        1494       1627  0.00%  0.00%  0.05%   0 Exec
   4           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   5        9264        2085       4443  0.00%  0.05%  0.05%   0 Check heaps
   6           0           2          0  0.00%  0.00%  0.00%   0 Pool Manager
   7           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
   8           0           2          0  0.00%  0.00%  0.00%   0 Timers
   9           4         136         29  0.00%  0.00%  0.00%   0 WATCH_AFS
  10           0           1          0  0.00%  0.00%  0.00%   0 License Client N
  11           0           1          0  0.00%  0.00%  0.00%   0 Image License br
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  12       18184         229      79406  0.00%  0.10%  0.11%   0 Licensing Auto U
  13       11176       13663        817  0.00%  0.09%  0.06%   0 Environmental mo
  14           0        2738          0  0.00%  0.00%  0.00%   0 IPC Event Notifi
  15           0         229          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  16           0           1          0  0.00%  0.00%  0.00%   0 IPC Session Serv
  17           0           1          0  0.00%  0.00%  0.00%   0 IPC Zone Manager
  18           0       13377          0  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  19           8       13377          0  0.00%  0.00%  0.00%   0 IPC Deferred Por
  20           0           1          0  0.00%  0.00%  0.00%   0 IPC Process leve
  21           0           1          0  0.00%  0.00%  0.00%   0 IPC Seat Manager
  22           0         784          0  0.00%  0.00%  0.00%   0 IPC Check Queue
  23           0           1          0  0.00%  0.00%  0.00%   0 IPC Seat RX Cont

R1#
```


```
R1#show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           8          36        222  0.00%  0.00%  0.00%   0 Chunk Manager
   2          48        2737         17  0.00%  0.01%  0.00%   0 Load Meter
   3        2432        1494       1627  0.00%  0.00%  0.05%   0 Exec
   4           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   5        9264        2085       4443  0.00%  0.05%  0.05%   0 Check heaps
   6           0           2          0  0.00%  0.00%  0.00%   0 Pool Manager
   7           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
   8           0           2          0  0.00%  0.00%  0.00%   0 Timers
   9           4         136         29  0.00%  0.00%  0.00%   0 WATCH_AFS
  10           0           1          0  0.00%  0.00%  0.00%   0 License Client N
  11           0           1          0  0.00%  0.00%  0.00%   0 Image License br
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  12       18184         229      79406  0.00%  0.10%  0.11%   0 Licensing Auto U
  13       11176       13663        817  0.00%  0.09%  0.06%   0 Environmental mo
  14           0        2738          0  0.00%  0.00%  0.00%   0 IPC Event Notifi
  15           0         229          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  16           0           1          0  0.00%  0.00%  0.00%   0 IPC Session Serv
  17           0           1          0  0.00%  0.00%  0.00%   0 IPC Zone Manager
  18           0       13377          0  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  19           8       13377          0  0.00%  0.00%  0.00%   0 IPC Deferred Por
  20           0           1          0  0.00%  0.00%  0.00%   0 IPC Process leve
  21           0           1          0  0.00%  0.00%  0.00%   0 IPC Seat Manager
  22           0         784          0  0.00%  0.00%  0.00%   0 IPC Check Queue
  23           0           1          0  0.00%  0.00%  0.00%   0 IPC Seat RX Cont
```

```
R1#
```

Return to the PC, execute a ping 10.1.1.1 -t command.

In the console of R1, we can see a syslog message that indicates that CPU utilization rises the threshold configured.

```
R1#
Aug 17 13:34:14.267: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr): 2%/0%, Top 3 processes(Pid/Util):  12/1%, 13/0%, 65/0%
Aug 17 13:34:19.267: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr) 1%/0%.
Aug 17 13:35:14.267: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr): 2%/0%, Top 3 processes(Pid/Util):  12/1%, 13/0%, 65/0%
Aug 17 13:35:19.267: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr) 0%/0%.
Aug 17 13:36:14.267: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr): 2%/0%, Top 3 processes(Pid/Util):  12/1%, 13/0%, 65/0%
Aug 17 13:36:19.267: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr) 0%/0%.
R1#
```

```
R1#
Aug 17 13:34:14.267: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total
CPUUtilization(Total/Intr): 2%/0%, Top 3 processes(Pid/Util):  12/1%, 13/0%, 65/0%
Aug 17 13:34:19.267: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU
Utilization(Total/Intr) 1%/0%.
Aug 17 13:35:14.267: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total CPU
Utilization(Total/Intr): 2%/0%, Top 3 processes(Pid/Util):  12/1%, 13/0%, 65/0%
Aug 17 13:35:19.267: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU
Utilization(Total/Intr) 0%/0%.
Aug 17 13:36:14.267: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total CPU
Utilization(Total/Intr): 2%/0%, Top 3 processes(Pid/Util):  12/1%, 13/0%, 65/0%
Aug 17 13:36:19.267: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU
Utilization(Total/Intr) 0%/0%.
R1#
```

Verify the CPU utilization.

```
R1#show processes cpu
CPU utilization for five seconds: 3%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           8          36        222  0.00%  0.00%  0.00%   0 Chunk Manager
   2          88        2838         31  0.00%  0.01%  0.00%   0 Load Meter
   3        3220        5483        587  0.31%  0.21%  0.16%   0 Exec
   4           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   5        9624        2164       4447  0.39%  0.08%  0.06%   0 Check heaps
   6           0           2          0  0.00%  0.00%  0.00%   0 Pool Manager
   7           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
   8           0           2          0  0.00%  0.00%  0.00%   0 Timers
   9           4         139         28  0.00%  0.00%  0.00%   0 WATCH_AFS
  10           0           1          0  0.00%  0.00%  0.00%   0 License Client N
  11           0           1          0  0.00%  0.00%  0.00%   0 Image License br

R1#
```

```
R1#show processes cpu
CPU utilization for five seconds: 3%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           8          36        222  0.00%  0.00%  0.00%   0 Chunk Manager
   2          88        2838         31  0.00%  0.01%  0.00%   0 Load Meter
   3        3220        5483        587  0.31%  0.21%  0.16%   0 Exec
```

```
   4           0           1           0  0.00%  0.00%  0.00%   0 RO Notify Timers
   5        9624        2164        4447  0.39%  0.08%  0.06%   0 Check heaps
   6           0           2           0  0.00%  0.00%  0.00%   0 Pool Manager
   7           0           1           0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
   8           0           2           0  0.00%  0.00%  0.00%   0 Timers
   9           4         139          28  0.00%  0.00%  0.00%   0 WATCH_AFS
  10           0           1           0  0.00%  0.00%  0.00%   0 License Client N
  11           0           1           0  0.00%  0.00%  0.00%   0 Image License br

R1#
```

Return to PC. In the MibBrowser click on the icone Trap Viewer once again.

Click start and show details, we can see that a trap about the CPU utilization notification is displayed in the TrapViewer window.