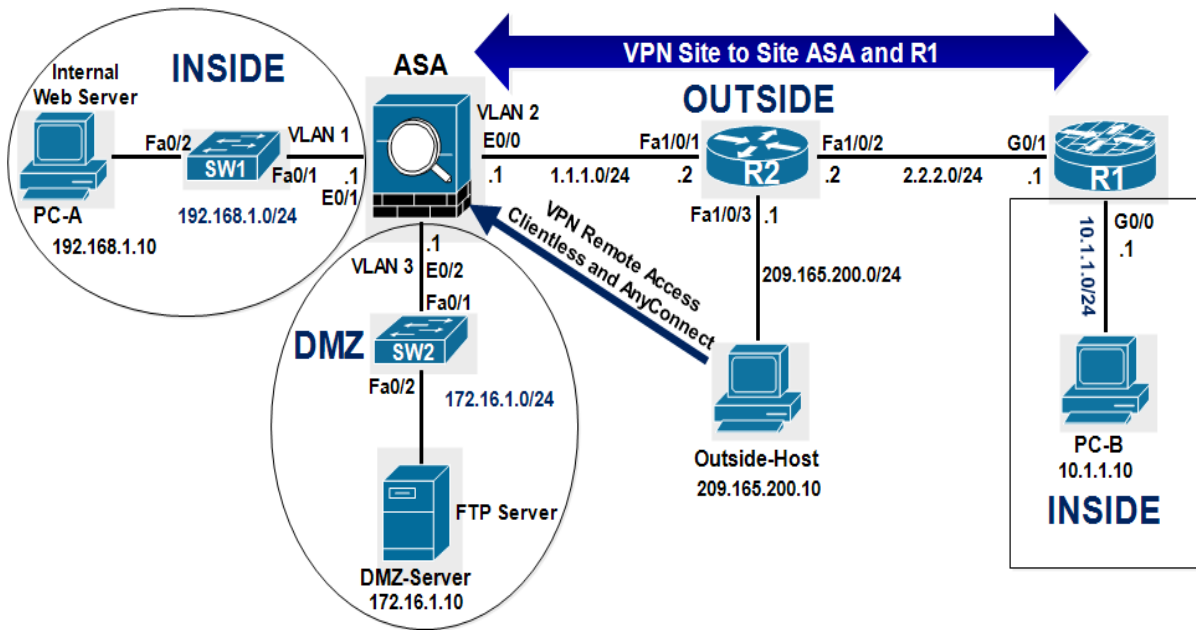


ASA Firewall, VPN Clientless, VPN AnyConnect, VPN Site to Site Zone-Based Firewall



By Redouane MEDDANE

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 (syncd), # master (unsyncd), + 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
*~1.1.1.2    2.2.2.1      5  123 128 377  0.9 35.82 18.8
 * master (syncd), # master (unsyncd), + 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#
```

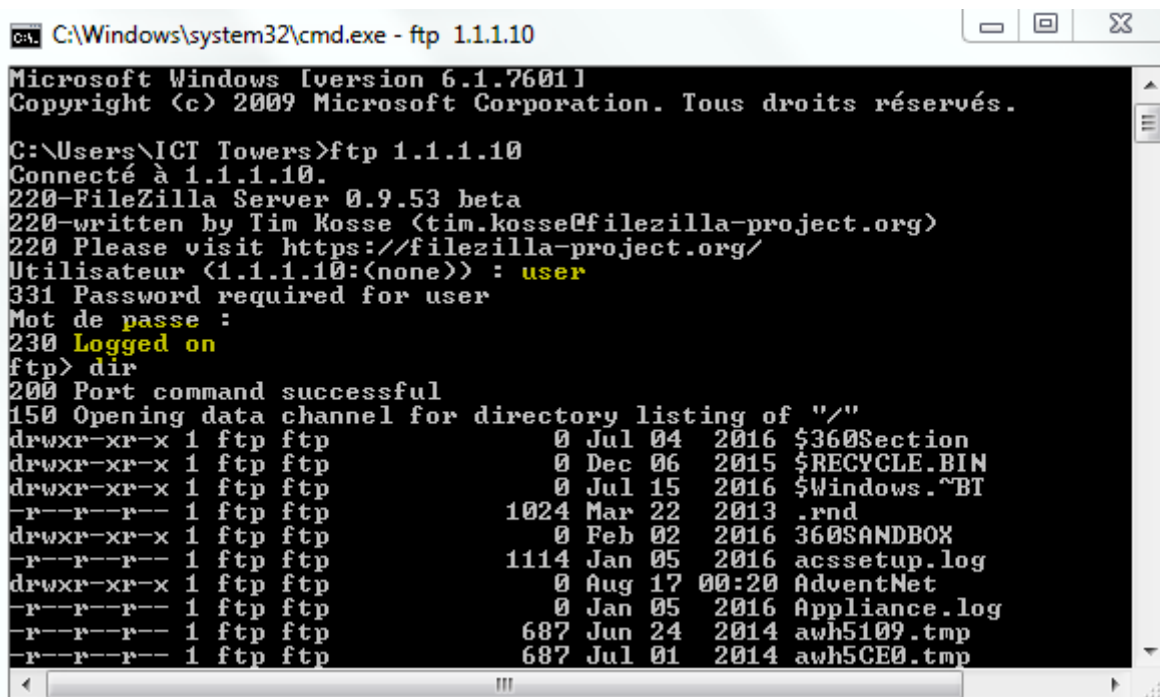
Configure an ACL to allow access to the DMZ server from the Internet.

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.

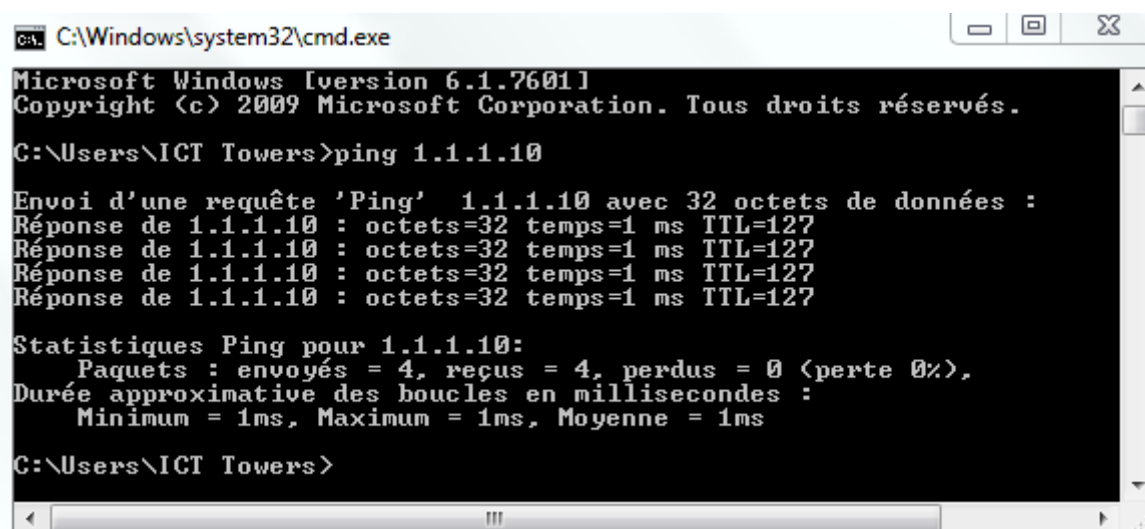
From Outside Host access the FTP files located in the DMZ Server, the access should be successful:



```
C:\Windows\system32\cmd.exe - ftp 1.1.1.10
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\ICT Towers>ftp 1.1.1.10
Connecté à 1.1.1.10.
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse <tim.kosse@filezilla-project.org>
220 Please visit https://filezilla-project.org/
Utilisateur (1.1.1.10:(none)) : user
331 Password required for user
Mot de passe :
230 Logged on
ftp> dir
200 Port command successful
150 Opening data channel for directory listing of "/"
drwxr-xr-x 1 ftp ftp          0 Jul 04 2016 $360Section
drwxr-xr-x 1 ftp ftp          0 Dec 06 2015 $RECYCLE.BIN
drwxr-xr-x 1 ftp ftp          0 Jul 15 2016 $Windows.~BT
-r--r--r-- 1 ftp ftp       1024 Mar 22 2013 .rnd
drwxr-xr-x 1 ftp ftp          0 Feb 02 2016 360SANDBOX
-r--r--r-- 1 ftp ftp       1114 Jan 05 2016 acssetup.log
drwxr-xr-x 1 ftp ftp          0 Aug 17 00:20 AdventNet
-r--r--r-- 1 ftp ftp          0 Jan 05 2016 Appliance.log
-r--r--r-- 1 ftp ftp         687 Jun 24 2014 awh5109.tmp
-r--r--r-- 1 ftp ftp         687 Jul 01 2014 awh5CE0.tmp
```

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



```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\ICT Towers>ping 1.1.1.10

Envoi d'une requête 'Ping' 1.1.1.10 avec 32 octets de données :
Réponse de 1.1.1.10 : octets=32 temps=1 ms TTL=127
Réponse de 1.1.1.10 : octets=32 temps=1 ms TTL=127
Réponse de 1.1.1.10 : octets=32 temps=1 ms TTL=127
Réponse de 1.1.1.10 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 1.1.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\ICT Towers>
```


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:

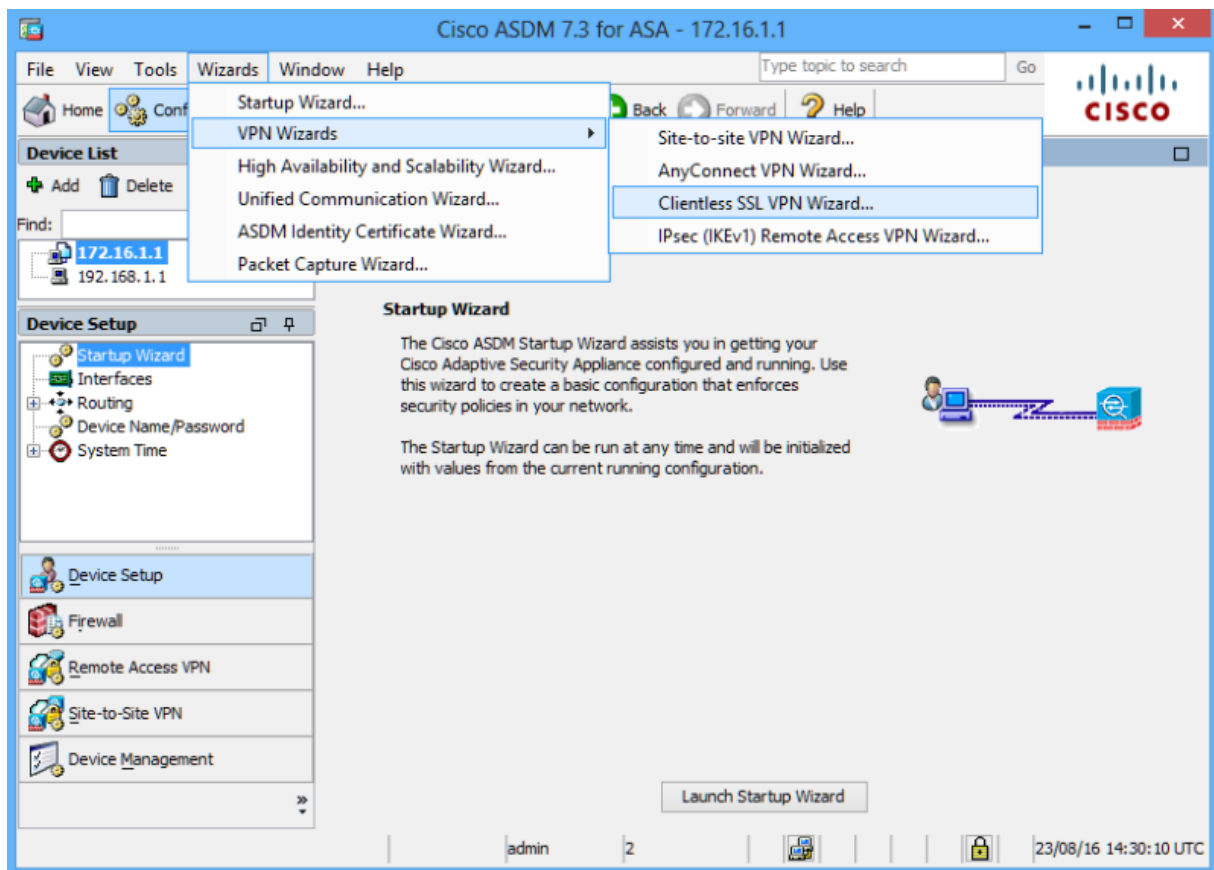
Note: Configure NAT exemption between the inside network of R1 (10.1.1.0/24) and the inside network of ASA (192.168.1.0/24) for VPN Site to Site purpose.

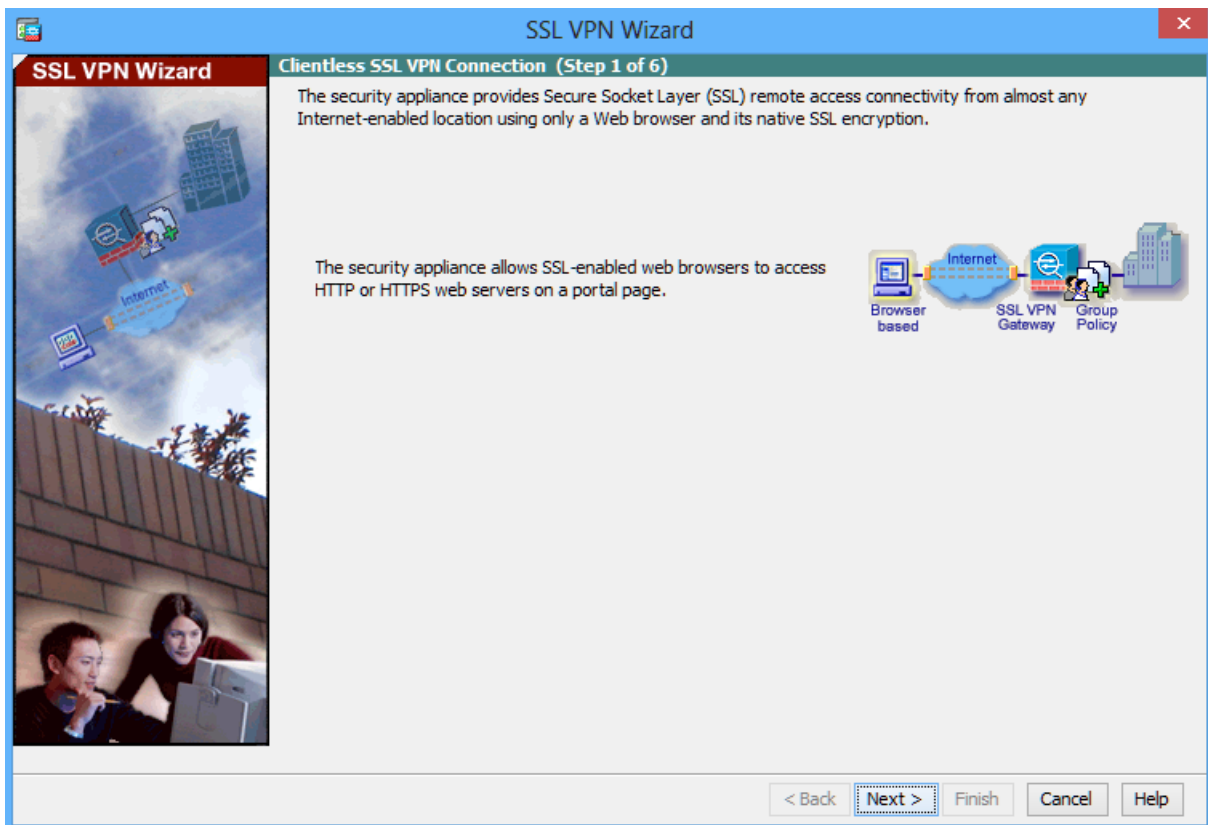
```
R1(config)#access-list 100 deny ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#access-list 100 permit ip 10.1.1.0 0.0.0.255 any
```

```
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

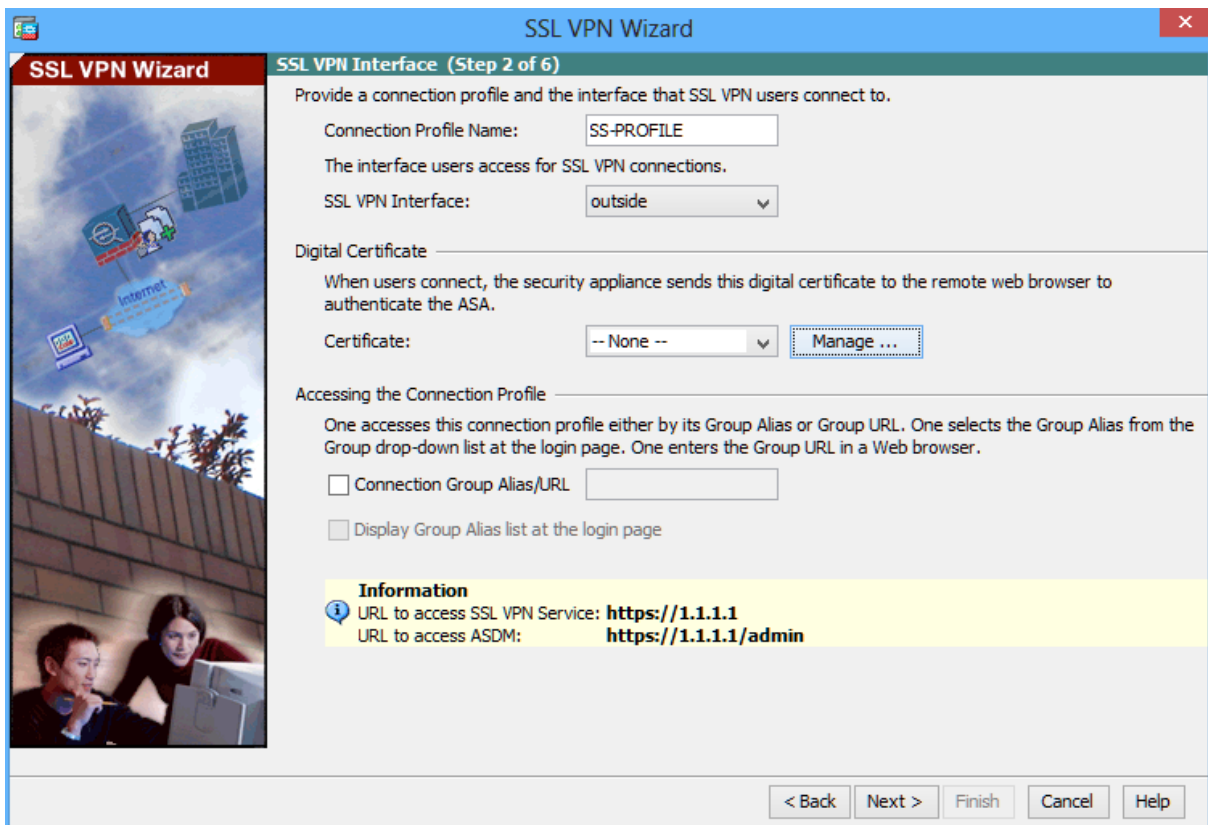
Using ASDM: click Wizards > VPN Wizards > Clientless SSL VPN wizard. The SSL VPN wizard Clientless SSL VPN Connection screen displays.





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.**

SSL VPN Wizard User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

Authenticate using a AAA server group

AAA Server Group Name:

Authenticate using the local user database

User to be Added

Username:

Password:

Confirm Password:

admin

< Back Next > Finish Cancel Help

SSL VPN Wizard User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

Authenticate using a AAA server group

AAA Server Group Name:

Authenticate using the local user database

User to be Added

Username:

Password:

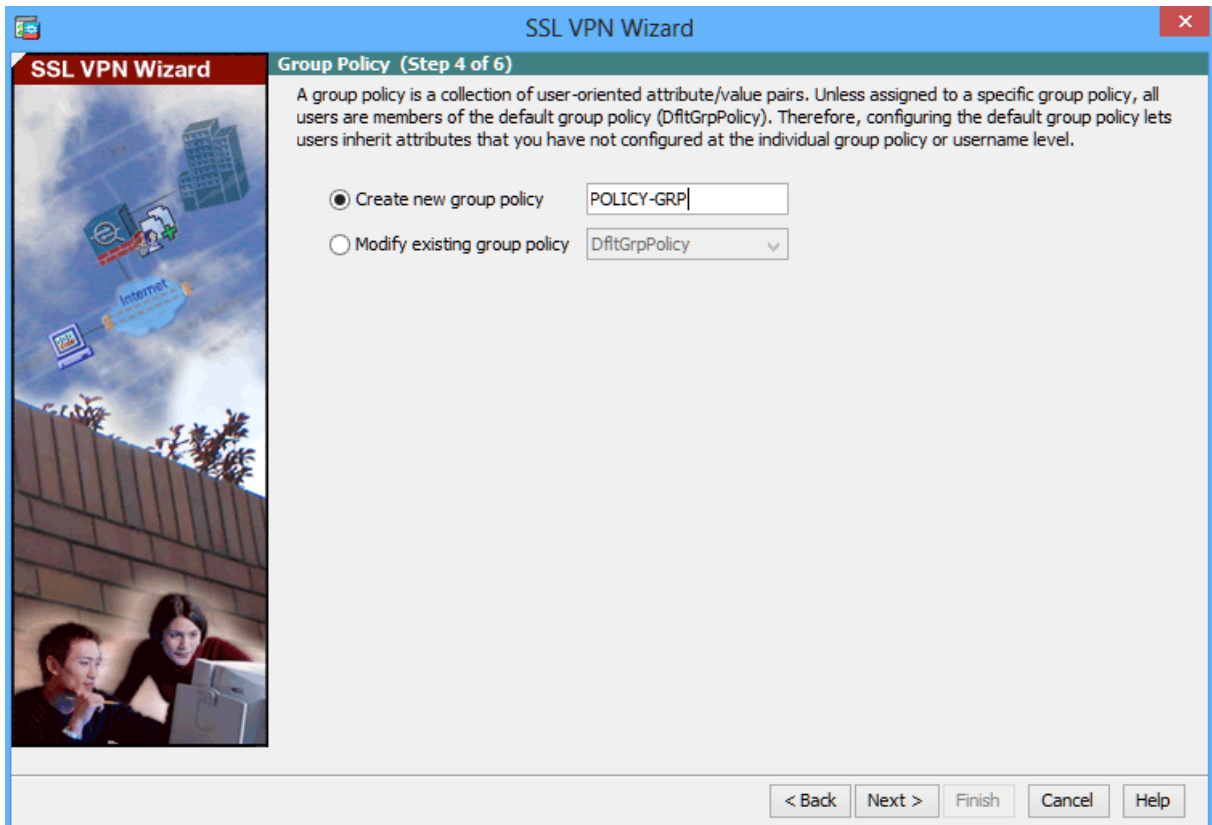
Confirm Password:

admin
user-vpn

< Back Next > Finish Cancel Help

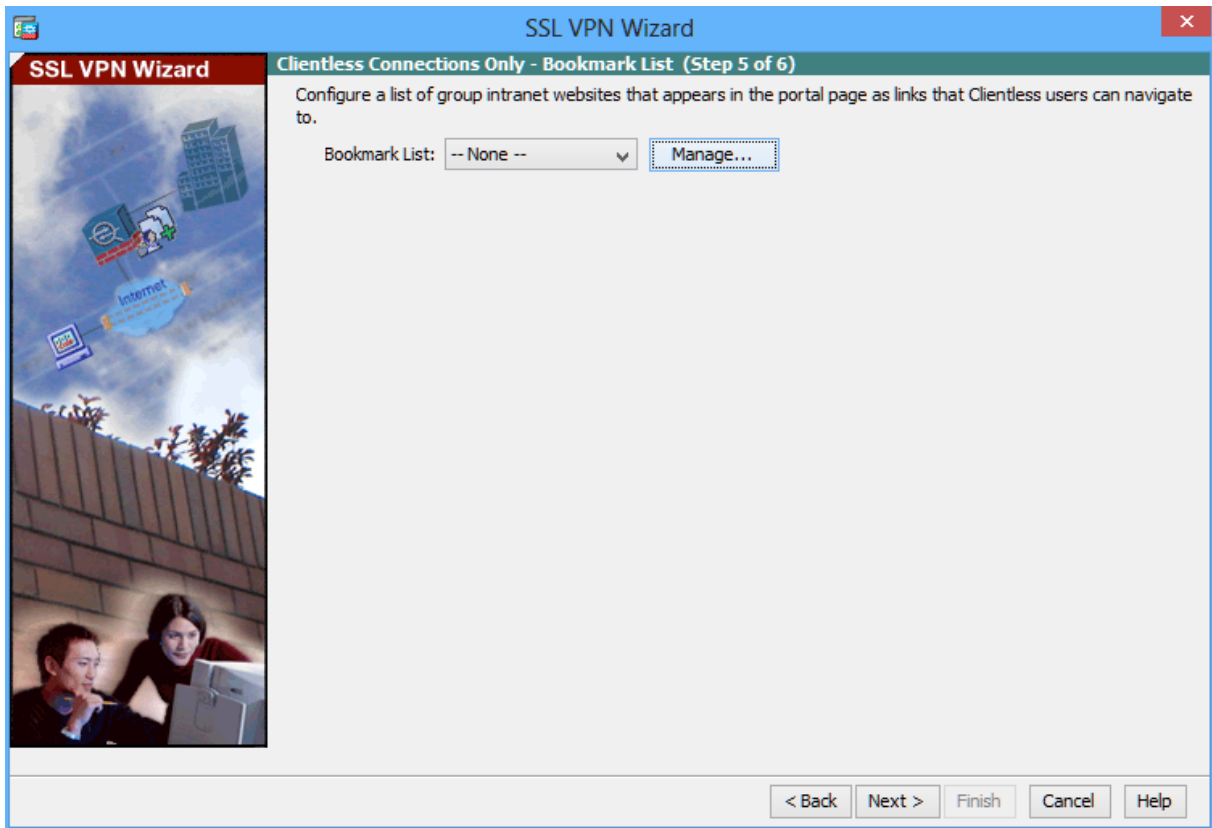
Configure the VPN group policy.

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

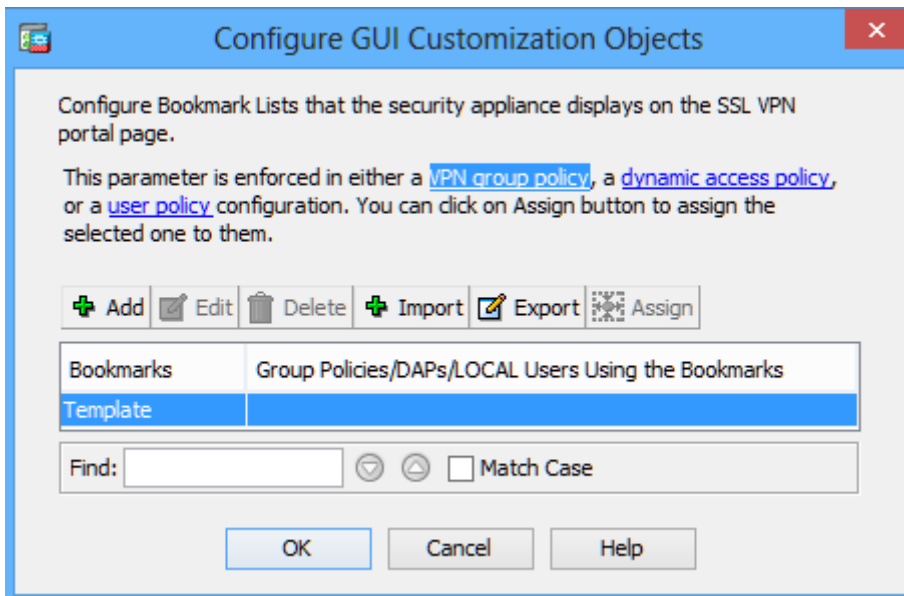


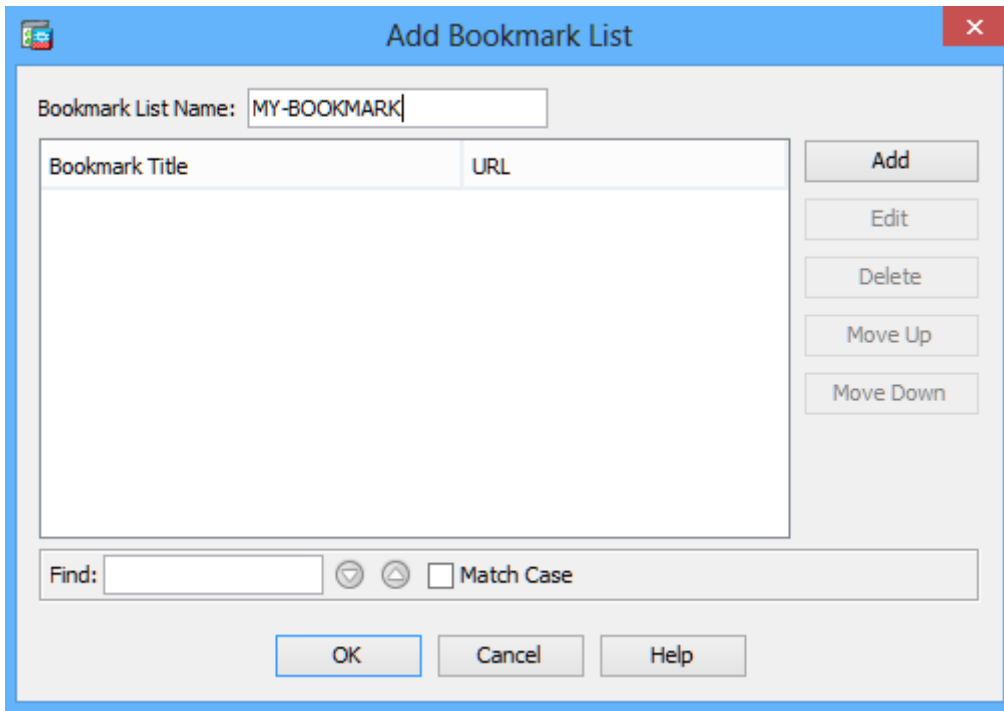
Configure the bookmark list.

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

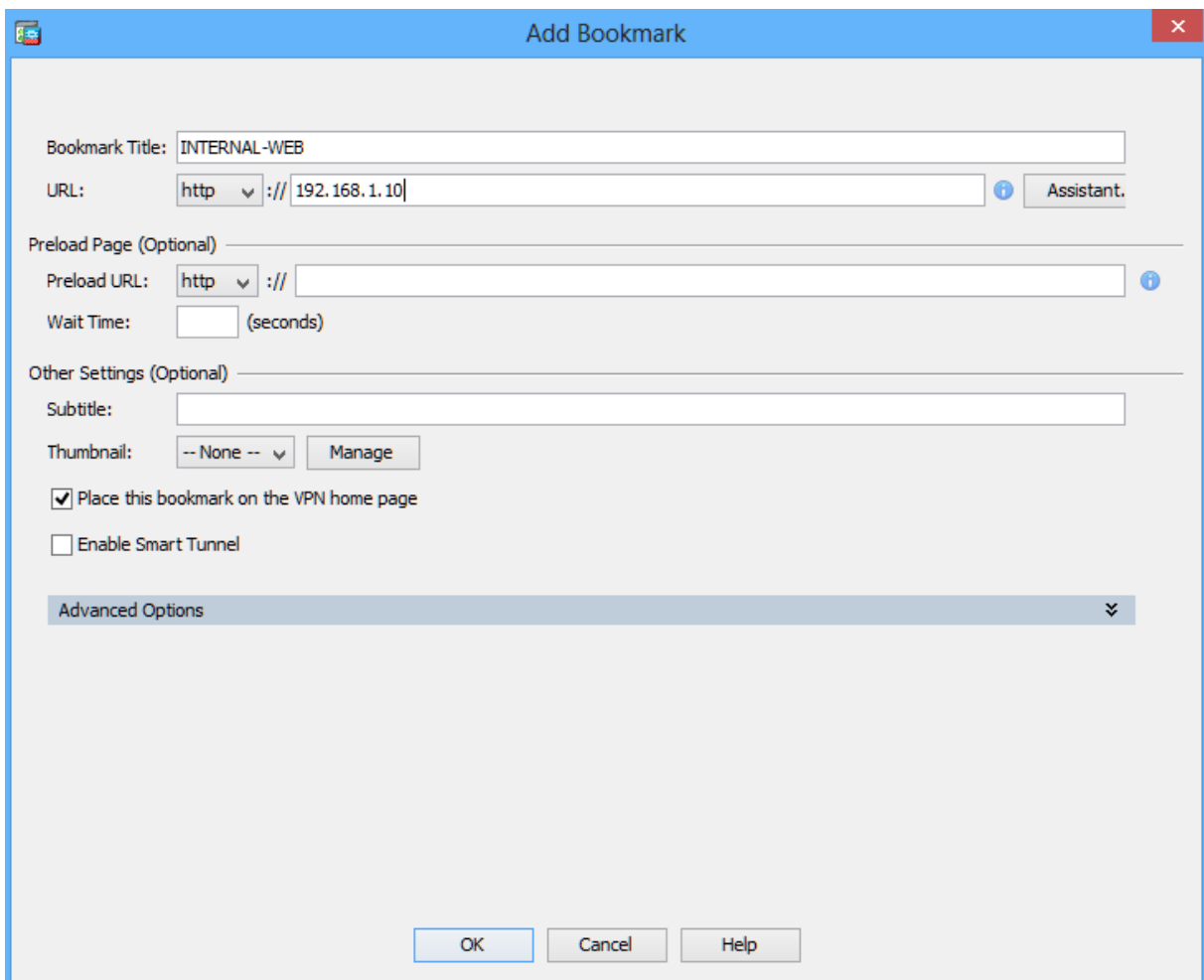


In the Configure GUI Customization Objects window, click Add to open the Add Bookmark List window. Name the list MY-BOOKMARK.





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.

Add Bookmark

Bookmark Title:

URL: :// Assistant..

Preload Page (Optional)

Preload URL: ://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail: Manage

Place this bookmark on the VPN home page

Enable Smart Tunnel

OK Cancel Help

Add Bookmark List

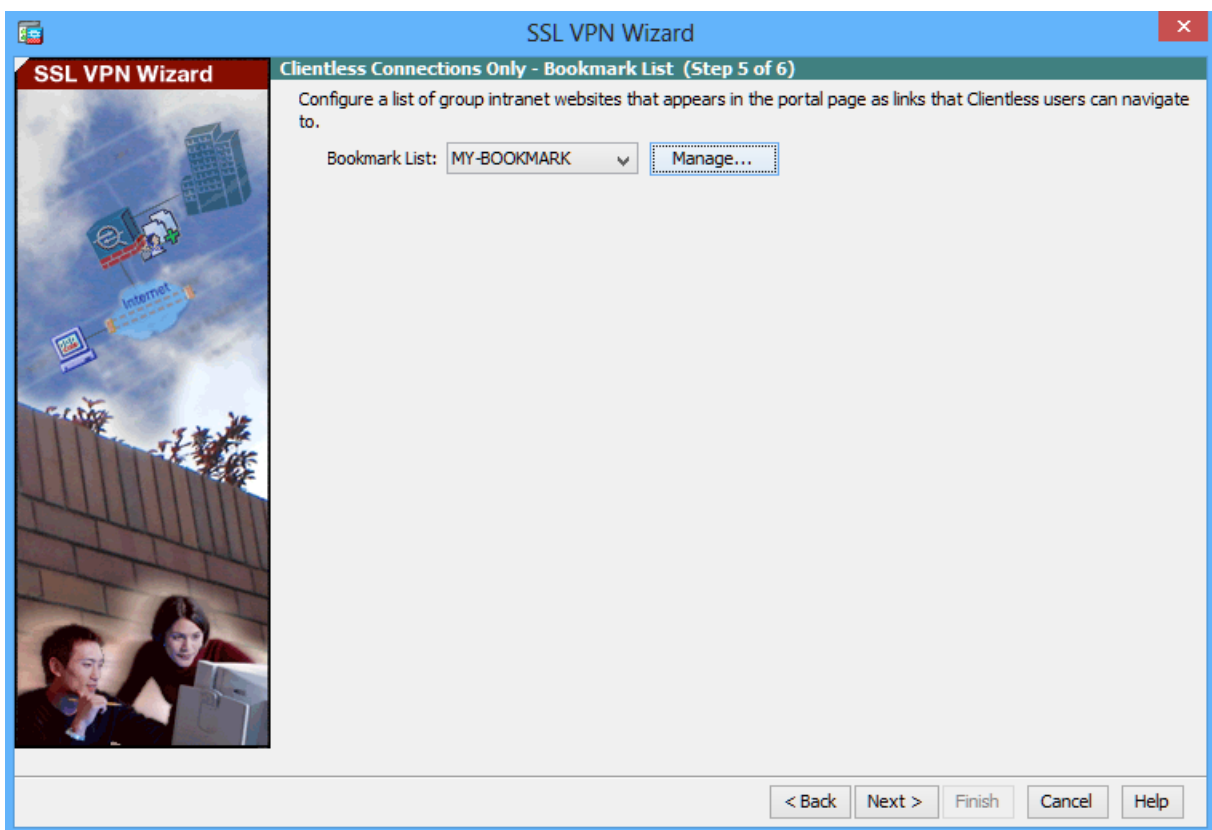
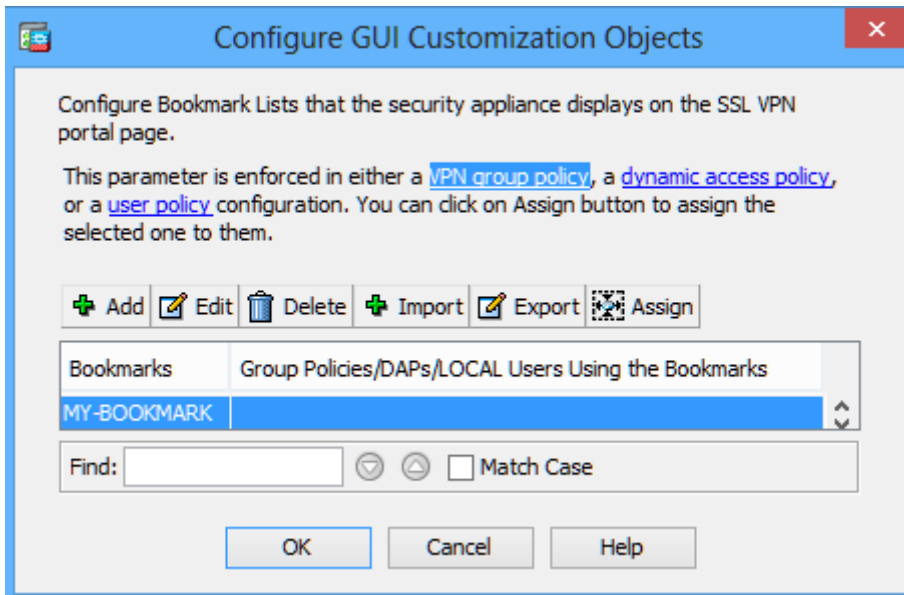
Bookmark List Name:

Bookmark Title	URL
INTERNAL-WEB	http://192.168.1.10
DMZ-SRV-FTP	ftp://172.16.1.10

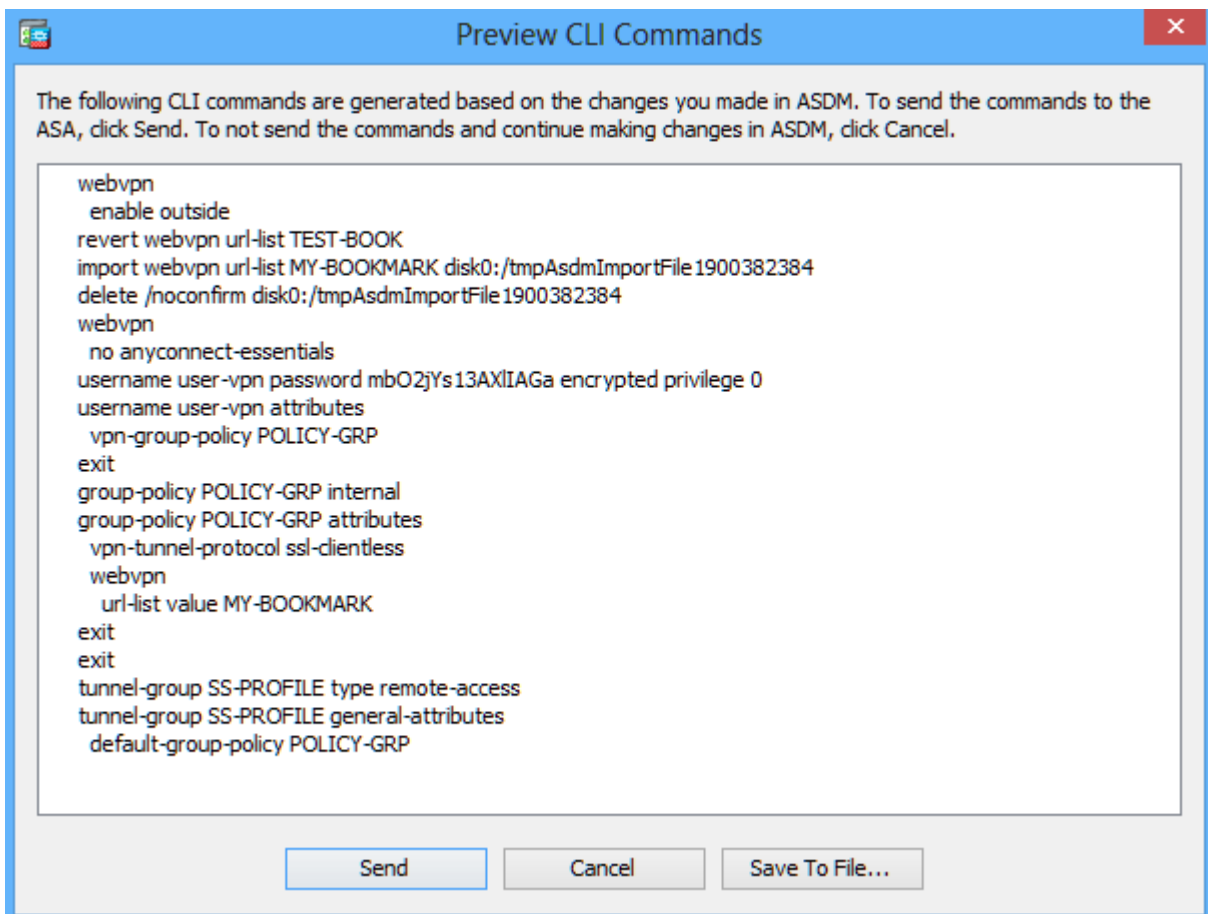
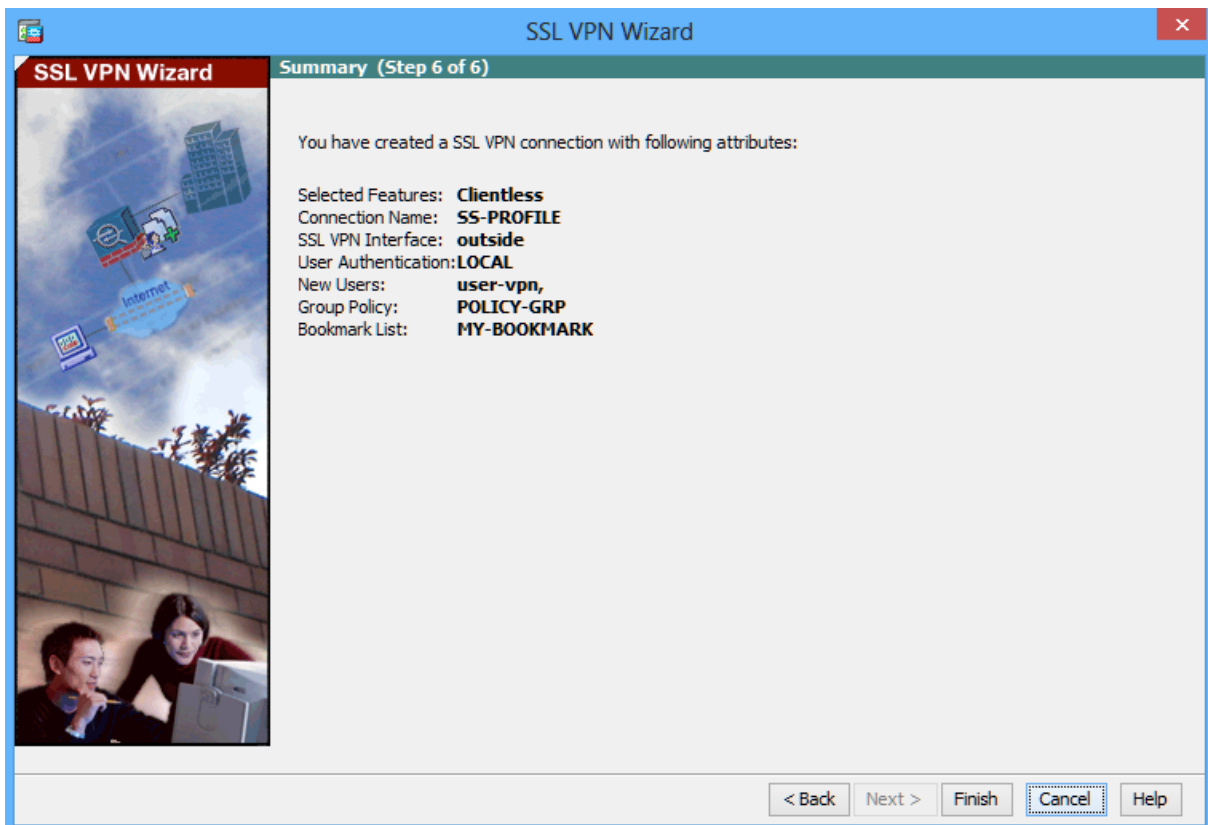
Add
Edit
Delete
Move Up
Move Down

Find: Match Case

OK Cancel Help



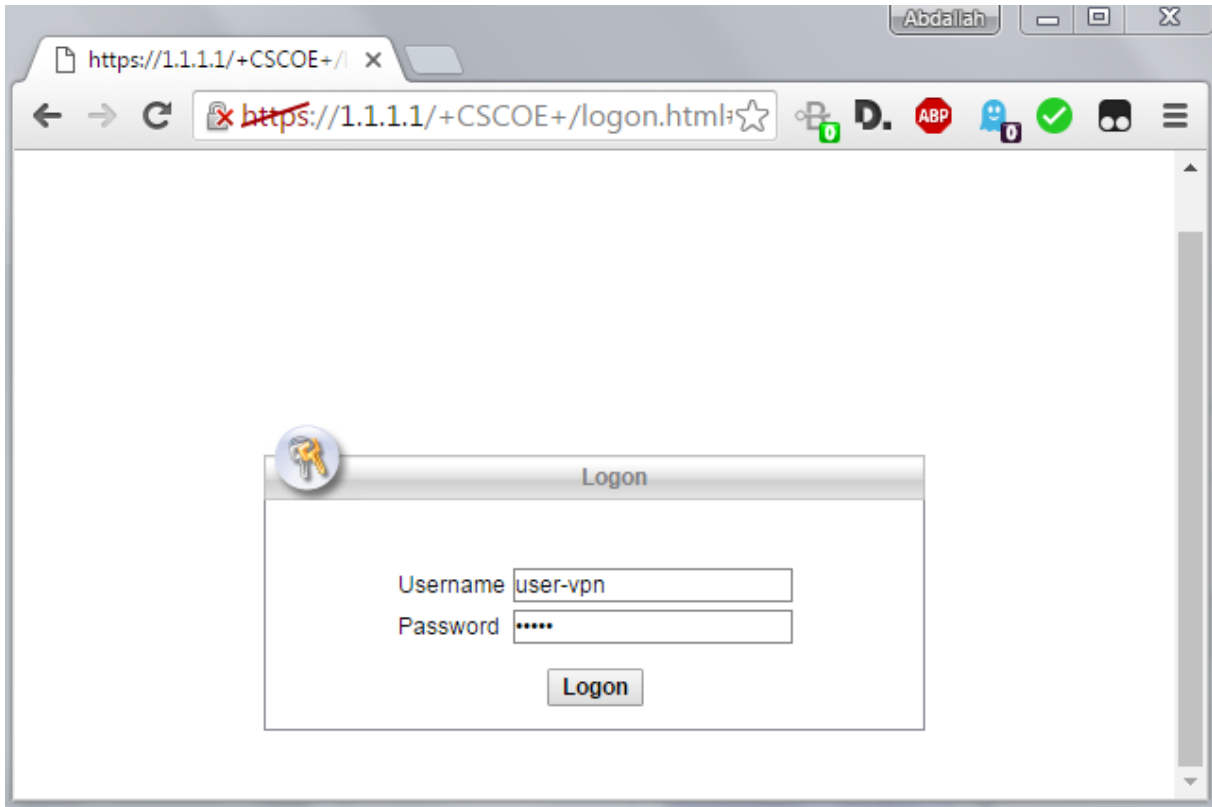
Click finish to complete the wizard and send the commands, and Apply to the ASA



Verify VPN access from the remote host.

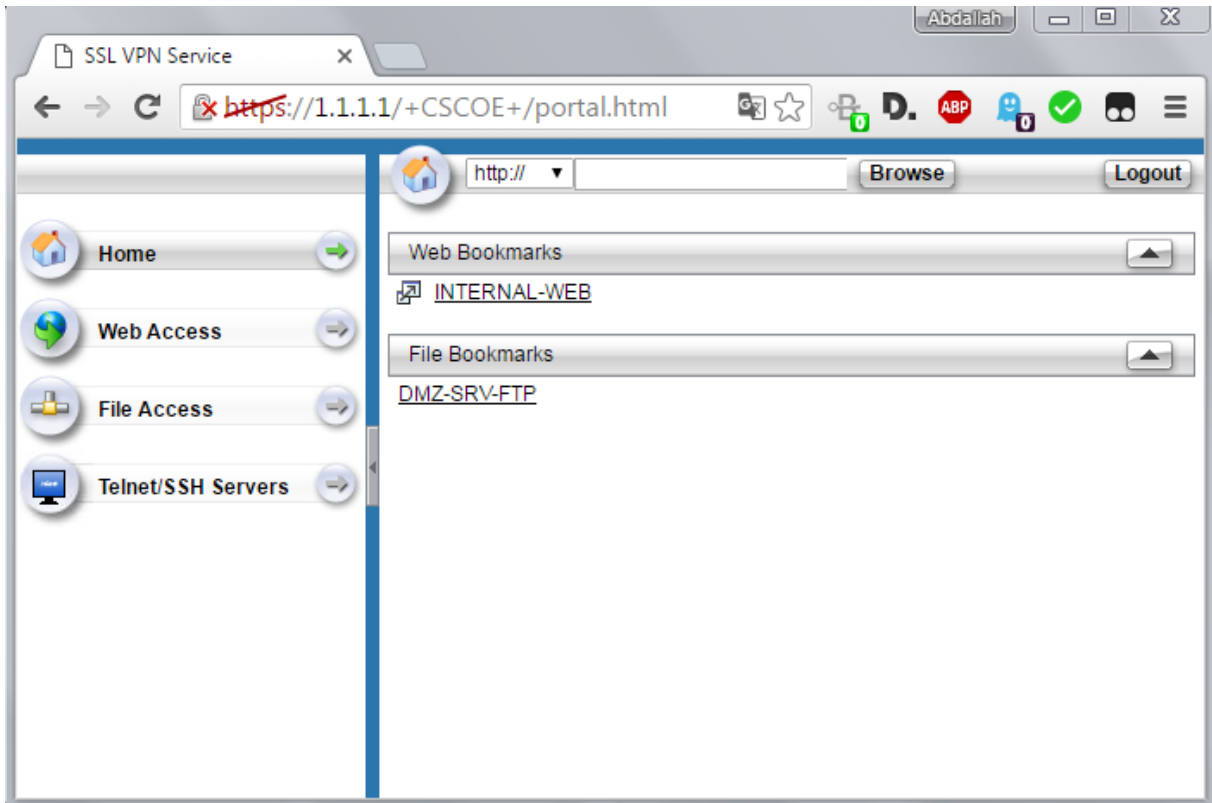
Open the browser on OUTSIDE-Host and enter the login URL for the SSL VPN into the address field (<https://1.1.1.1>). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA. Note: Accept security notification warnings.

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.

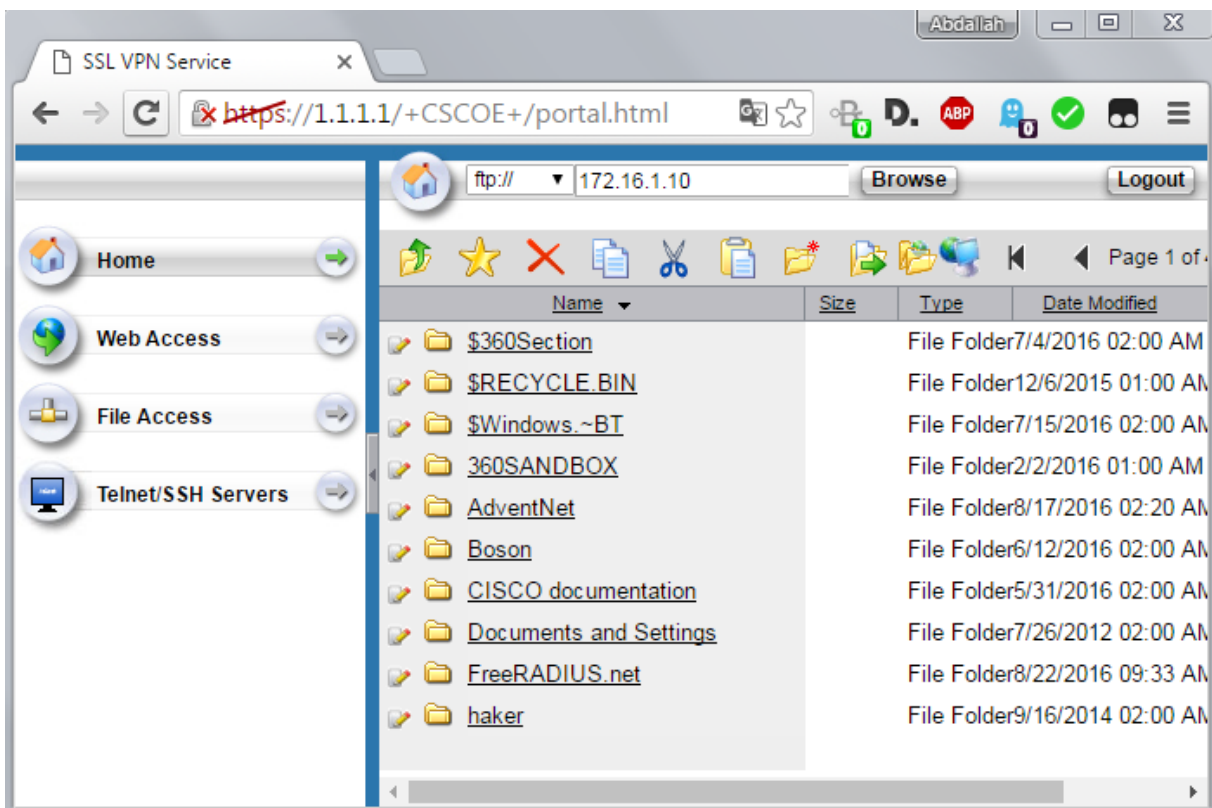
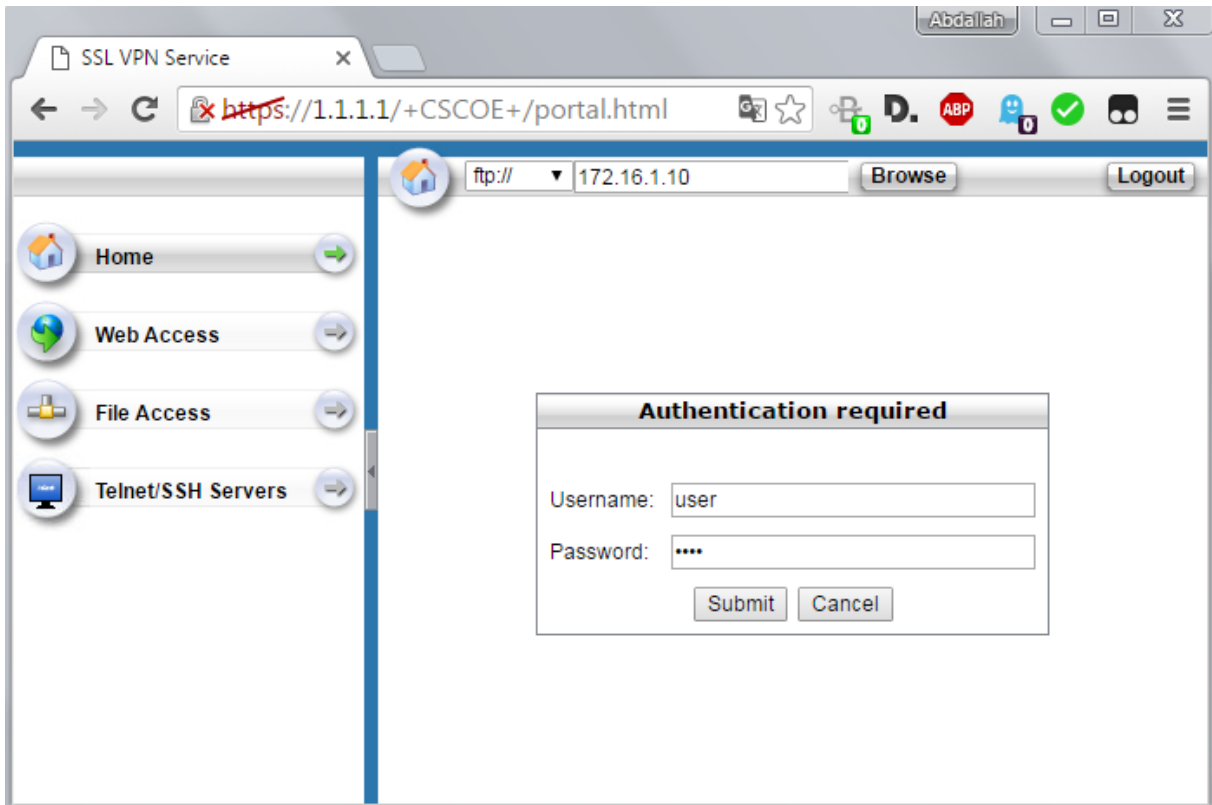
After the user authenticates, the ASA SSL web portal webpage will be displayed. This webpage lists the bookmarks previously assigned to the profile.



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

Home Configuration Monitoring Save Refresh Back Forward Help

Device List: 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	Details
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	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

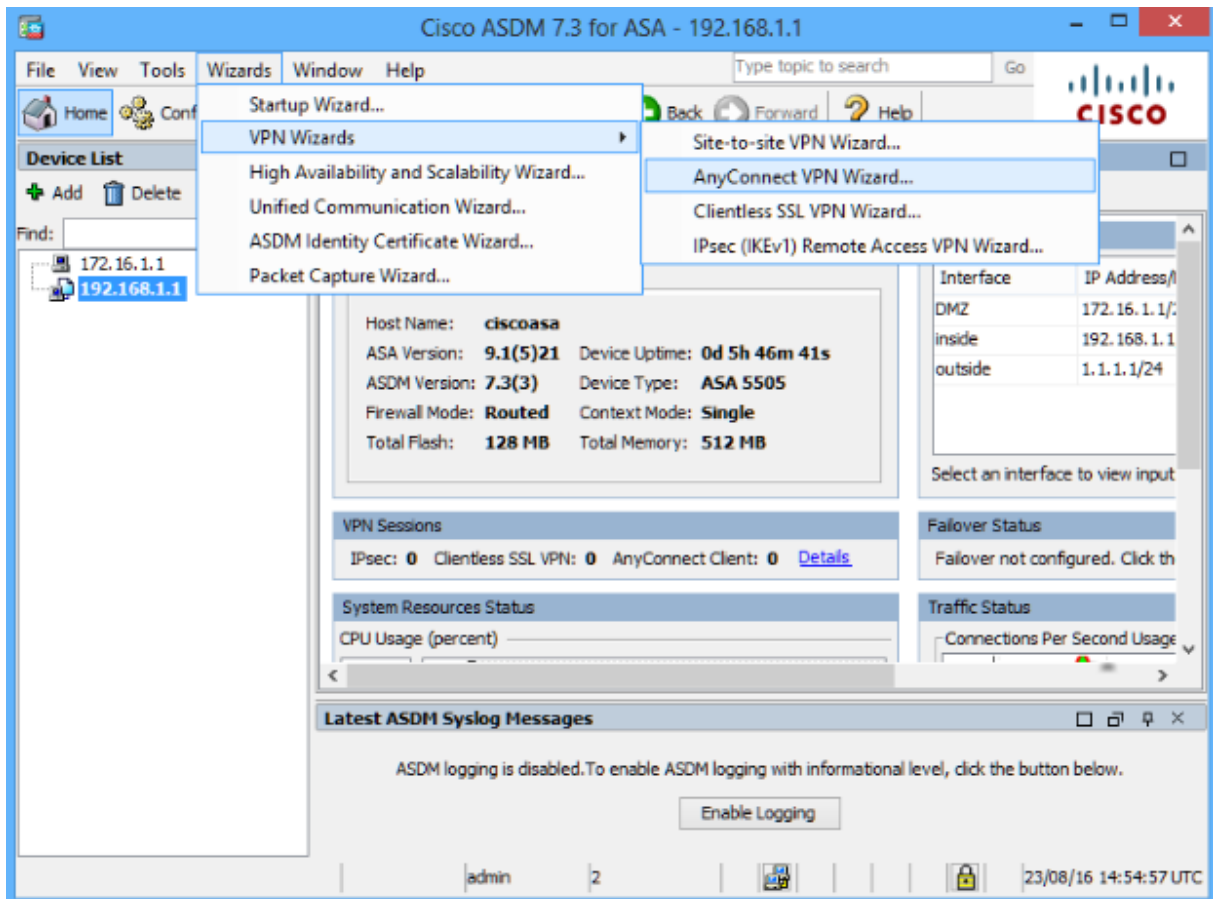
Last Updated: 24/08/16 01:51:08

Data Refreshed Successfully. admin 2 23/08/16 14:51:17 UTC

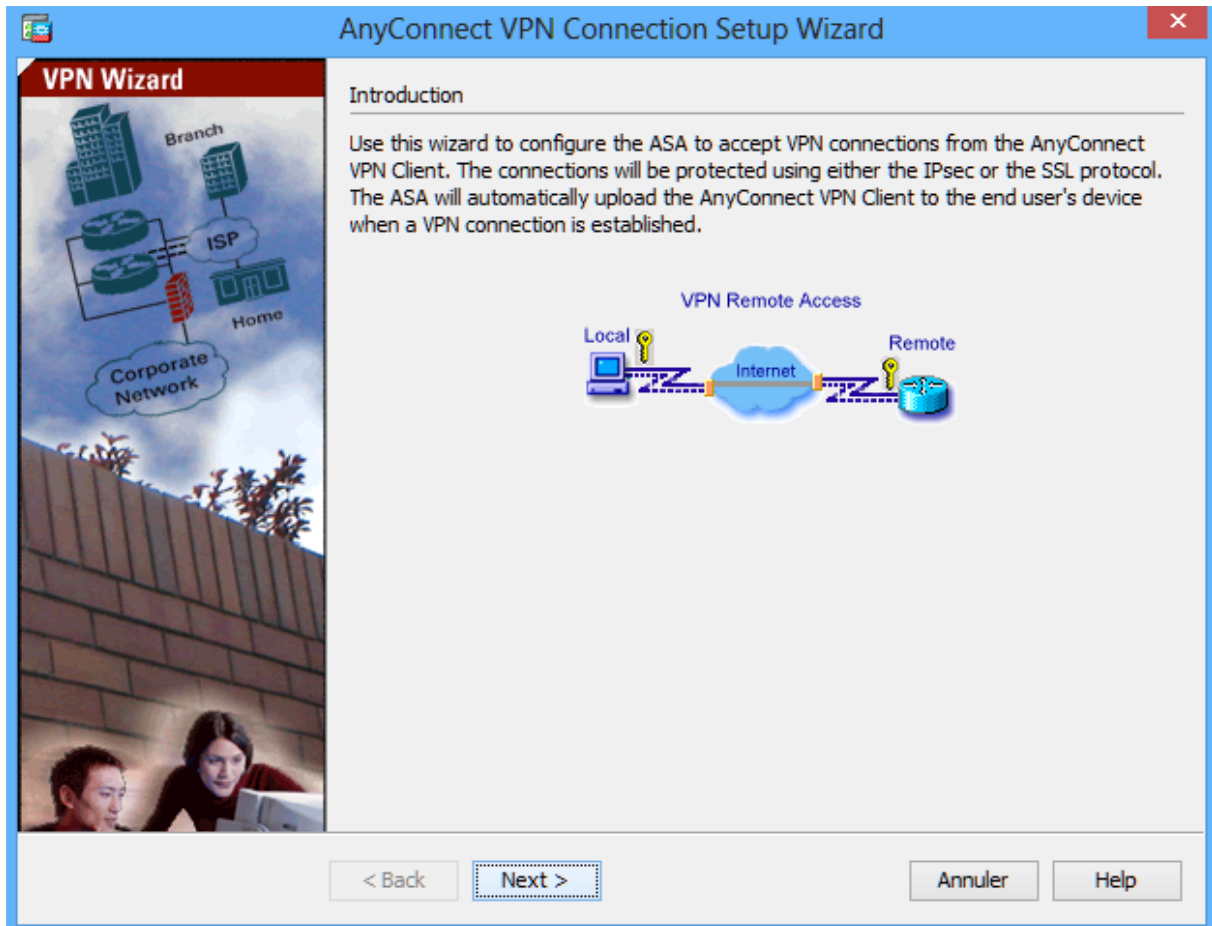
Part-9: Configure ASA AnyConnect SSL VPN Remote Access

Start the VPN wizard.

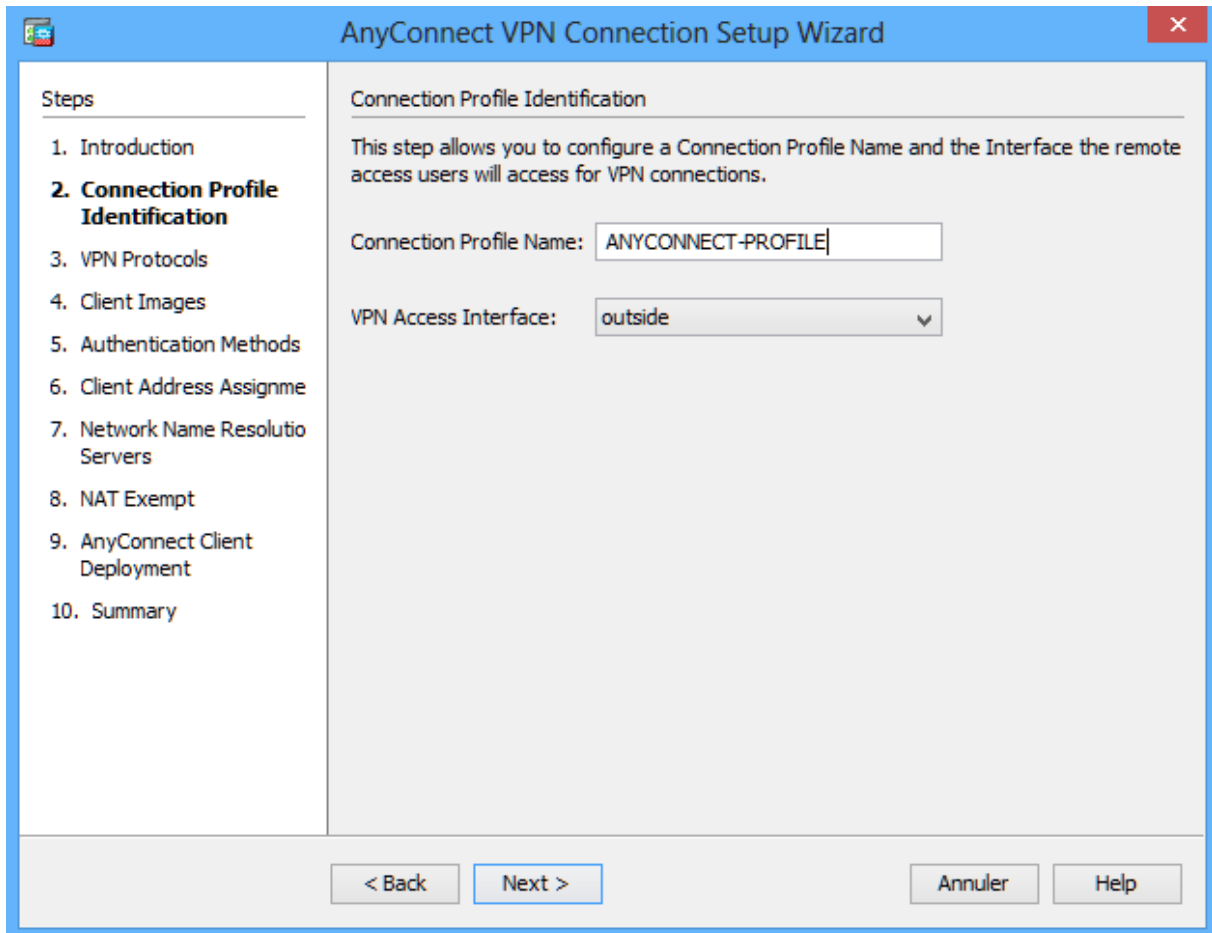
On the ASDM main menu, click Wizards > VPN Wizards > AnyConnect VPN Wizard.



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

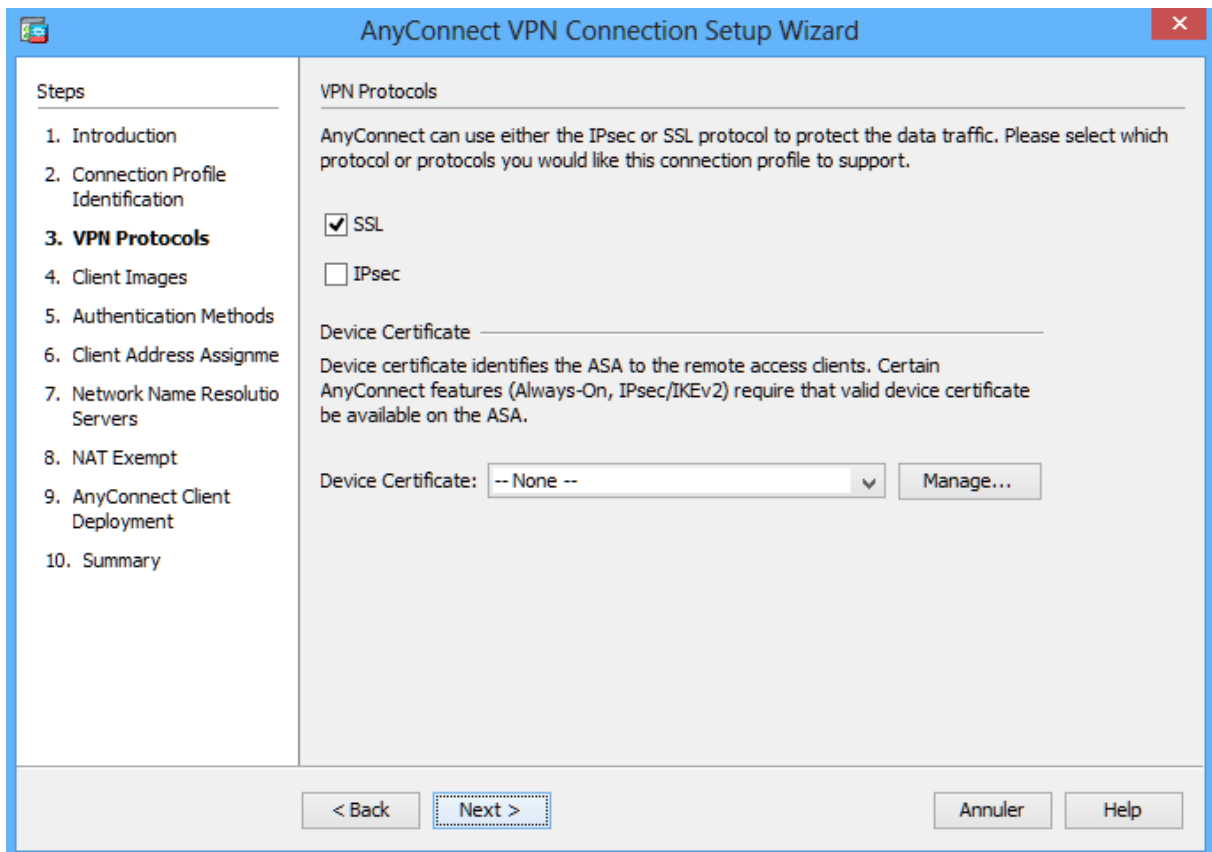


Configure the SSL VPN interface connection profile.
On the Connection Profile Identification screen, enter **AnyConnect-PROFILE** as the Connection Profile Name and specify the outside interface as the VPN Access Interface. Click Next to continue.

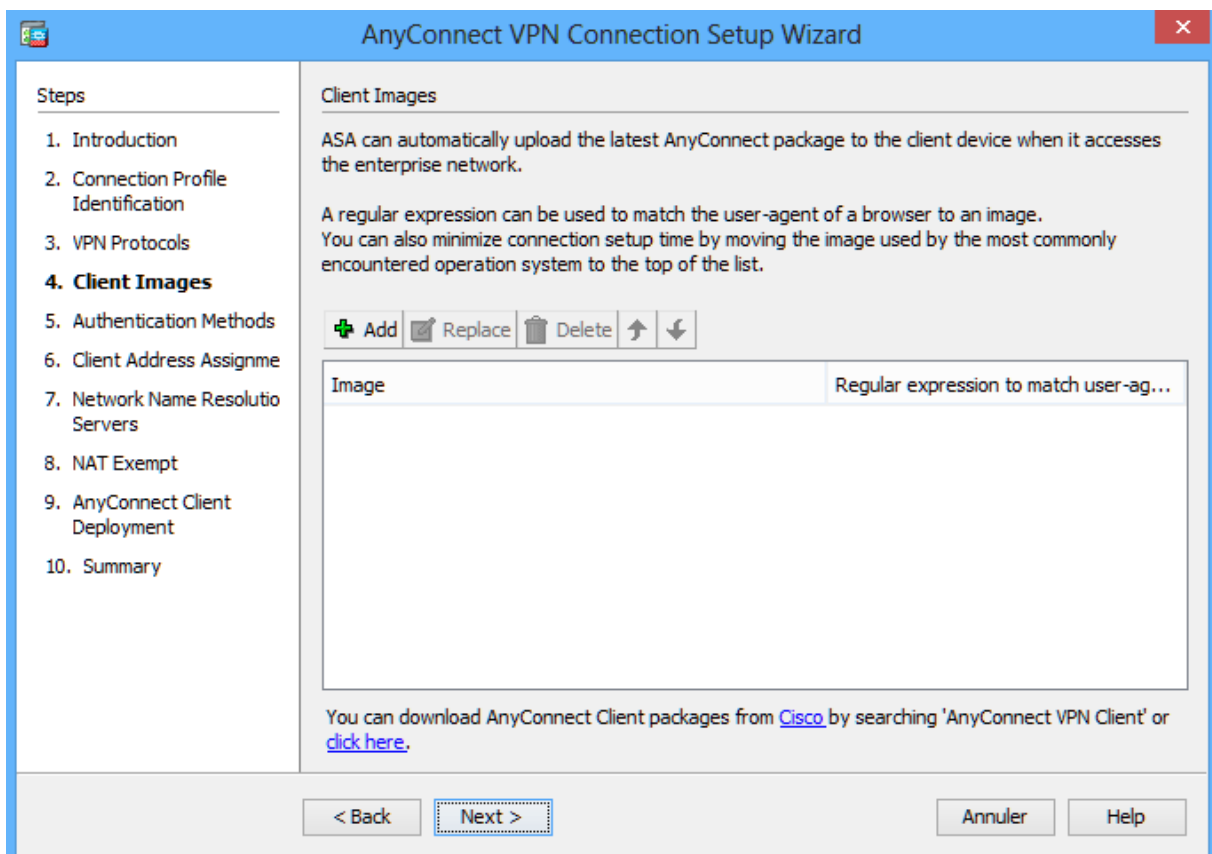


Specify the VPN encryption protocol.

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.

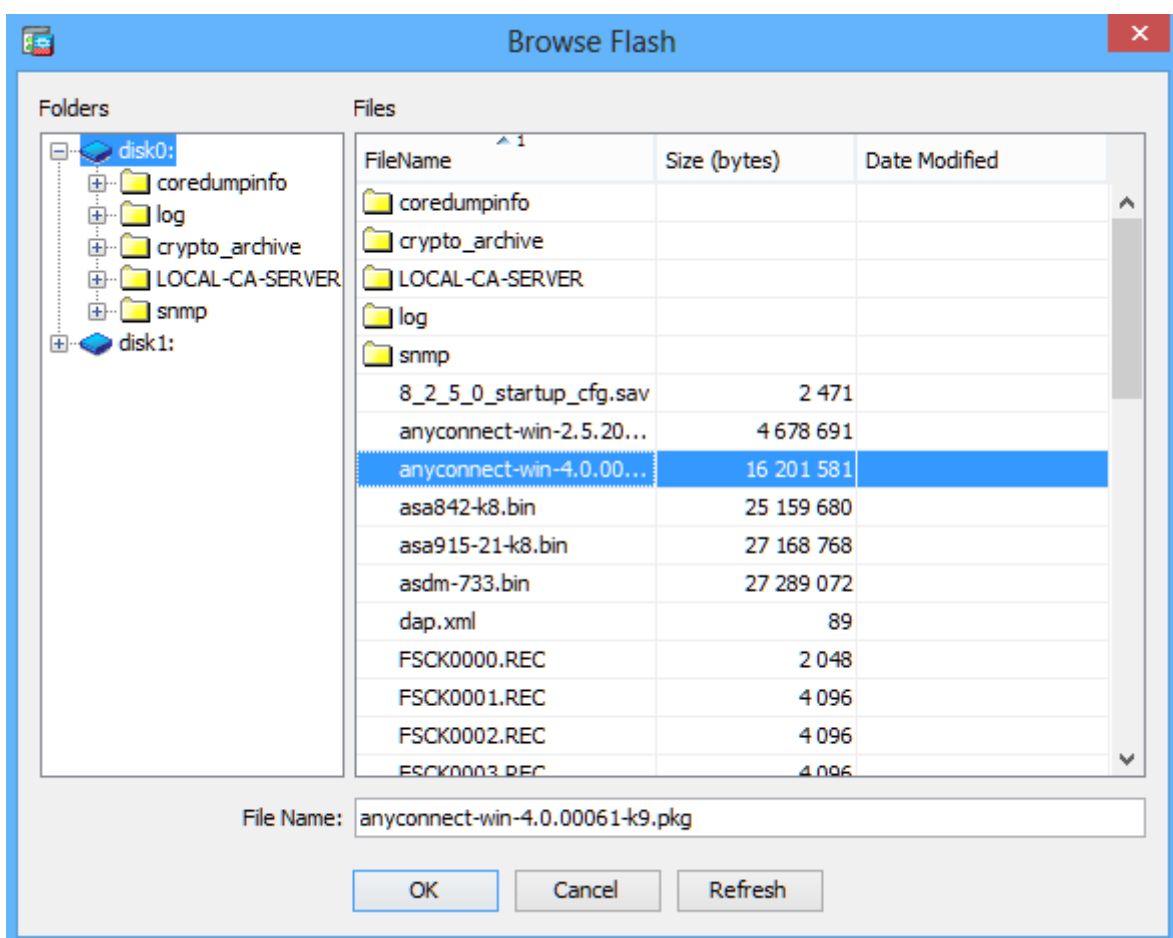
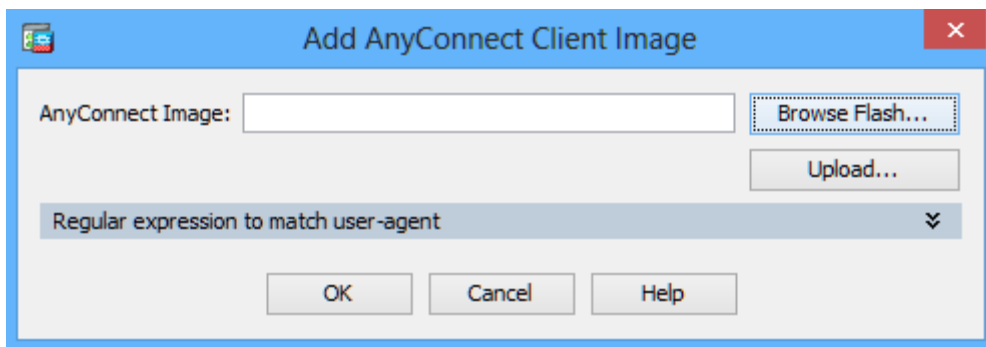


**Specify the client image to upload to AnyConnect users.
On the Client Images screen, click Add to specify the AnyConnect client image filename.**

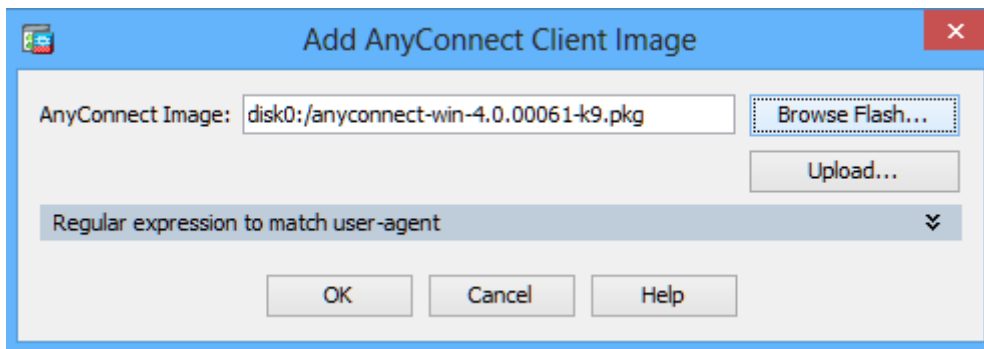


In the Add AnyConnect Client Image window, click Browse Flash.

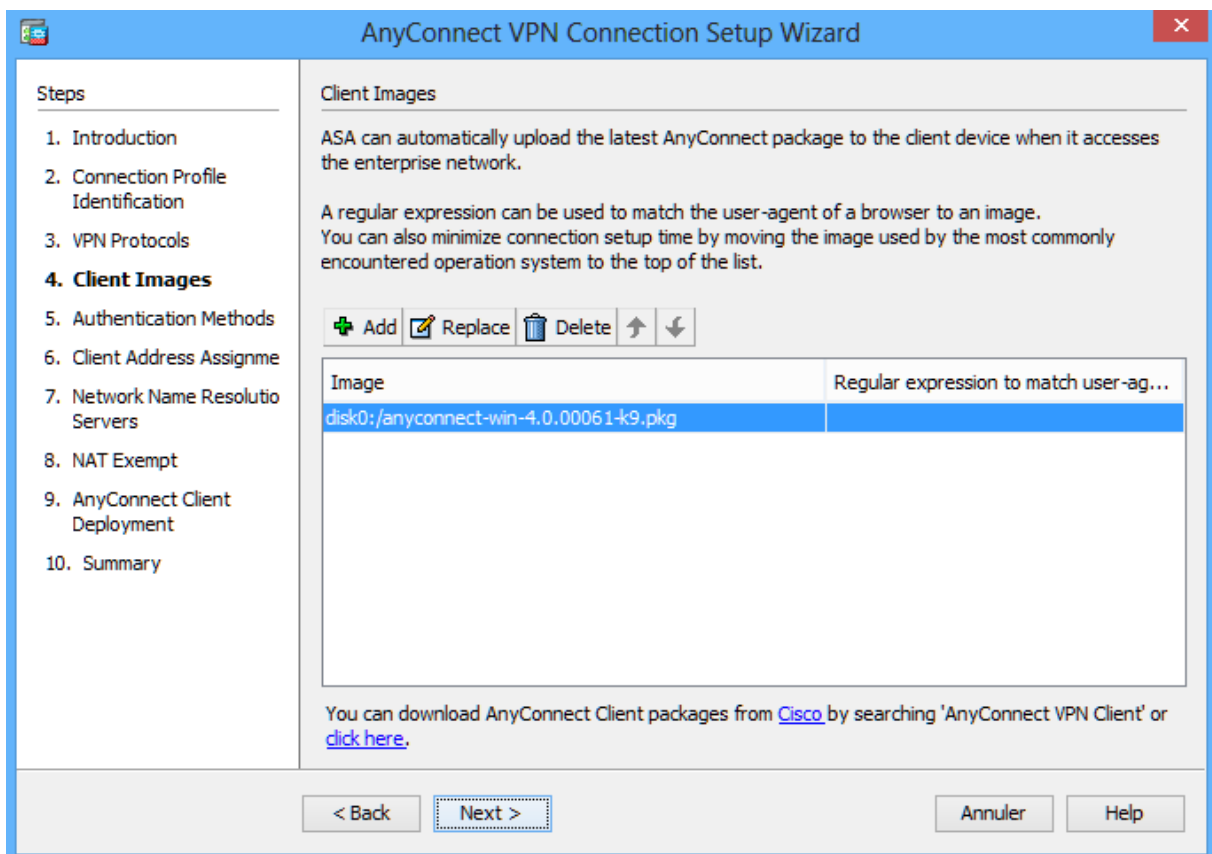
In the Browse Flash window, select the AnyConnect package file for Windows (anyconnect-win-4.0.00061-k9.pkg, in the example). Click OK to return to the AnyConnect Client Image window.



Click OK again to return to the Client Image window.



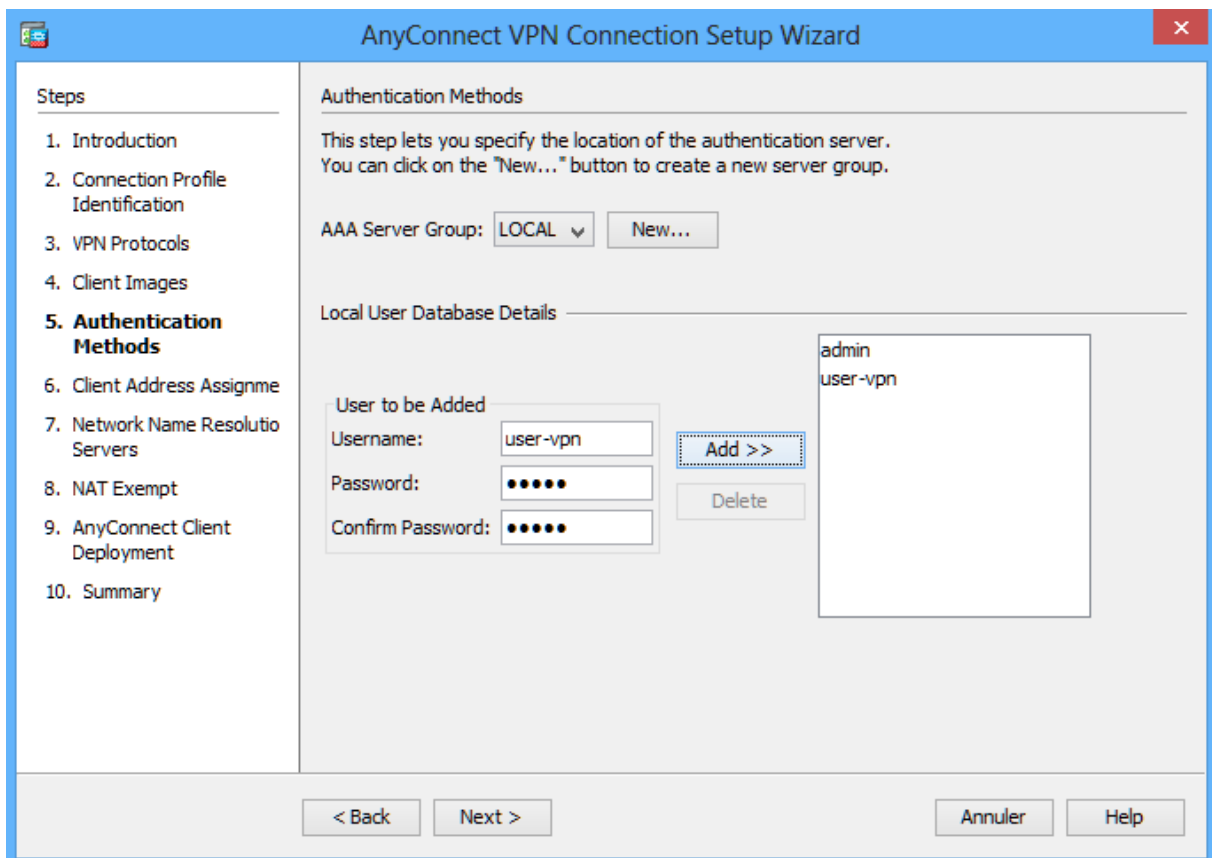
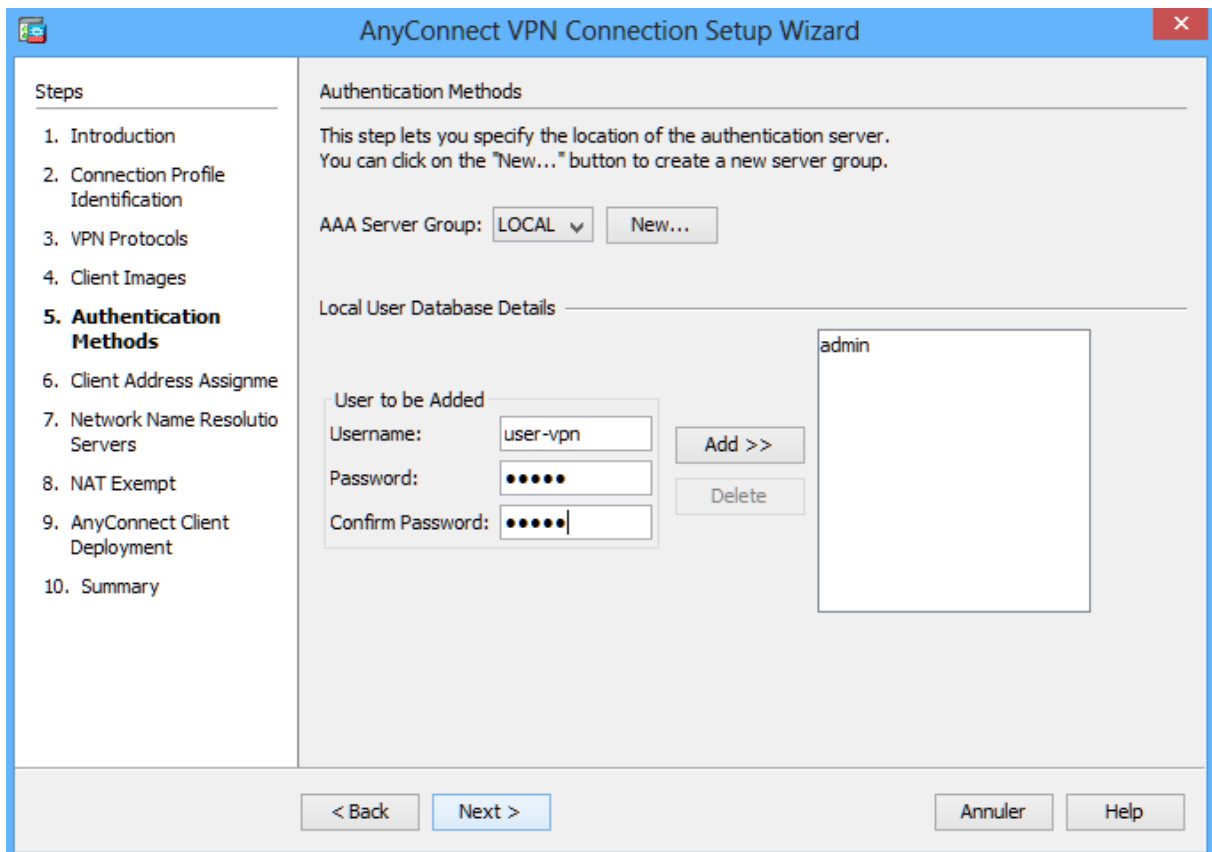
The selected image is now displayed on the Client Image window. Click Next to continue.



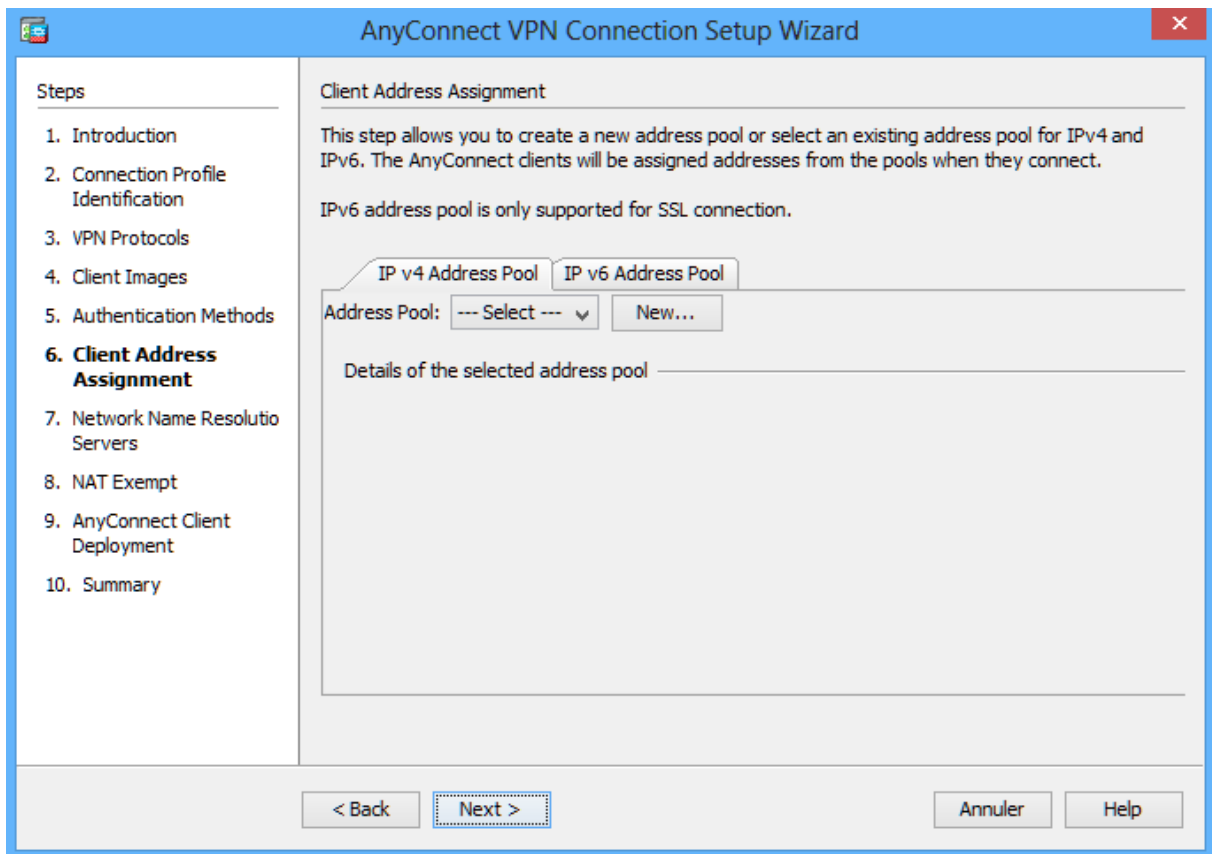
Configure AAA local authentication.

On the Authentication Methods screen, ensure that the AAA Server Group is specified as LOCAL.

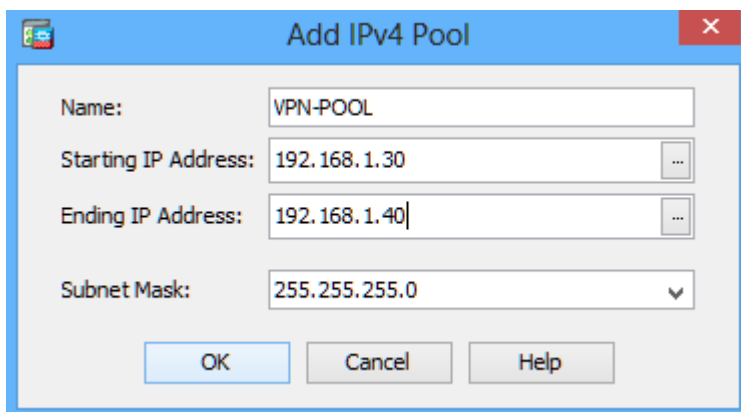
Enter a new user named user-vpn with the password cisco. Click Add.



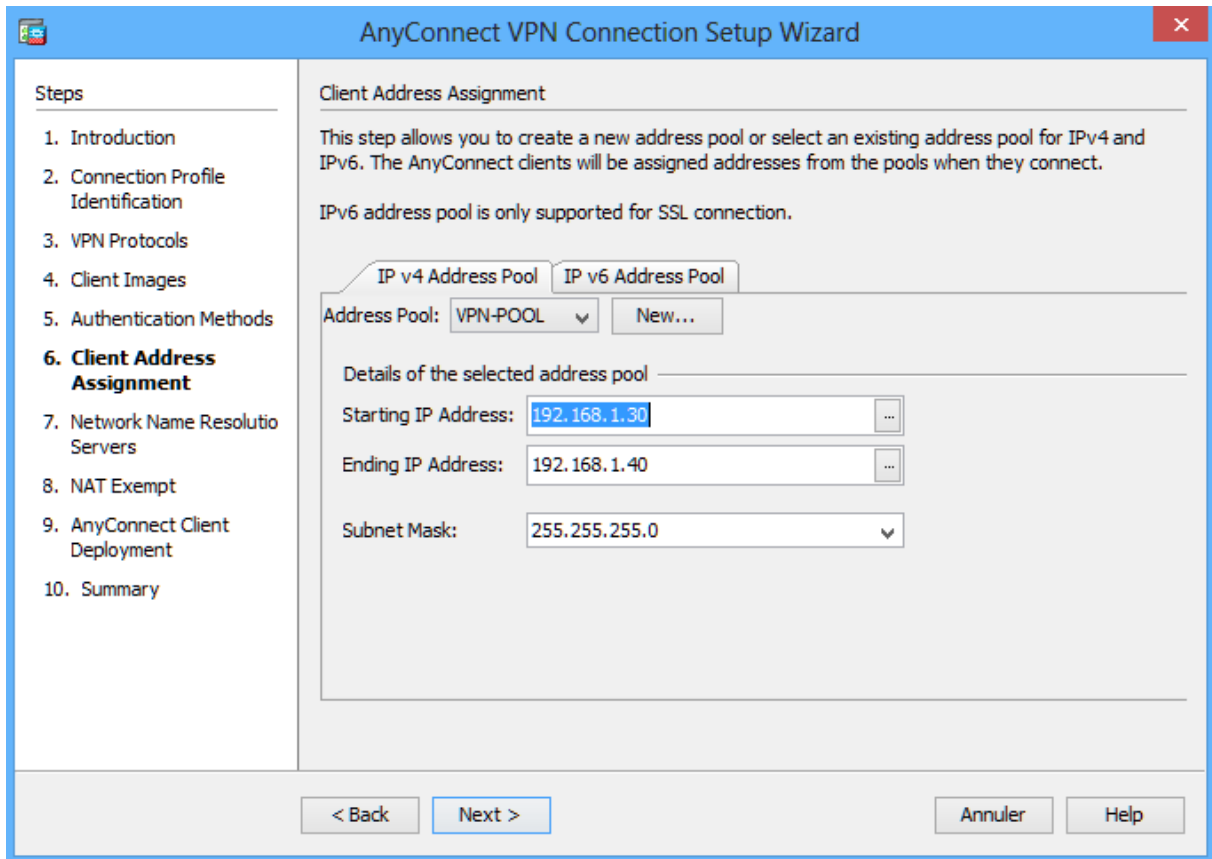
Configure the client address assignment.
In the Client Address Assignment window, click New to create an IPv4 address pool.



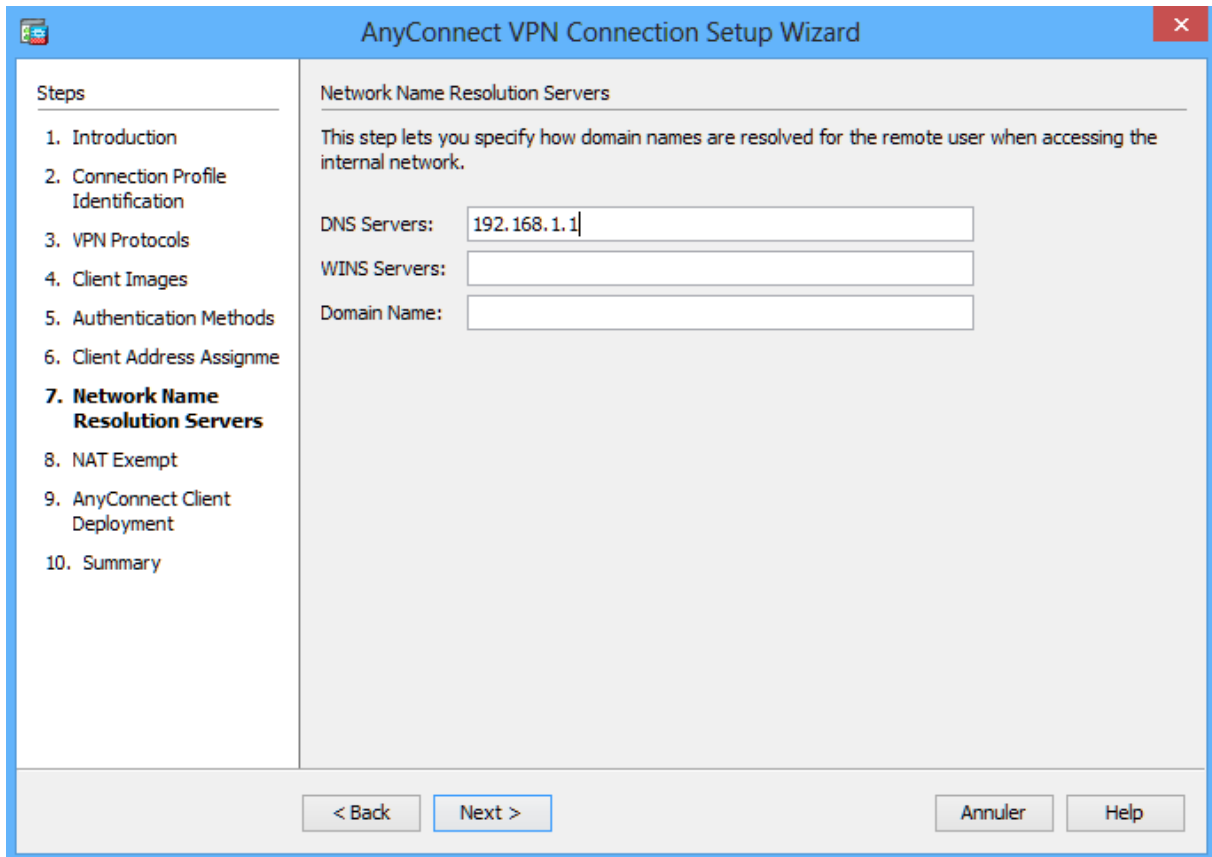
In the Add IPv4 Pool window, name the pool Remote-Pool with a starting IP address of 192.168.1.30, an ending IP address of 192.168.1.40, and a subnet mask of 255.255.255.0. Click OK to return to the Client Address Assignment window, which now displays the newly created remote user IP address pool.



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

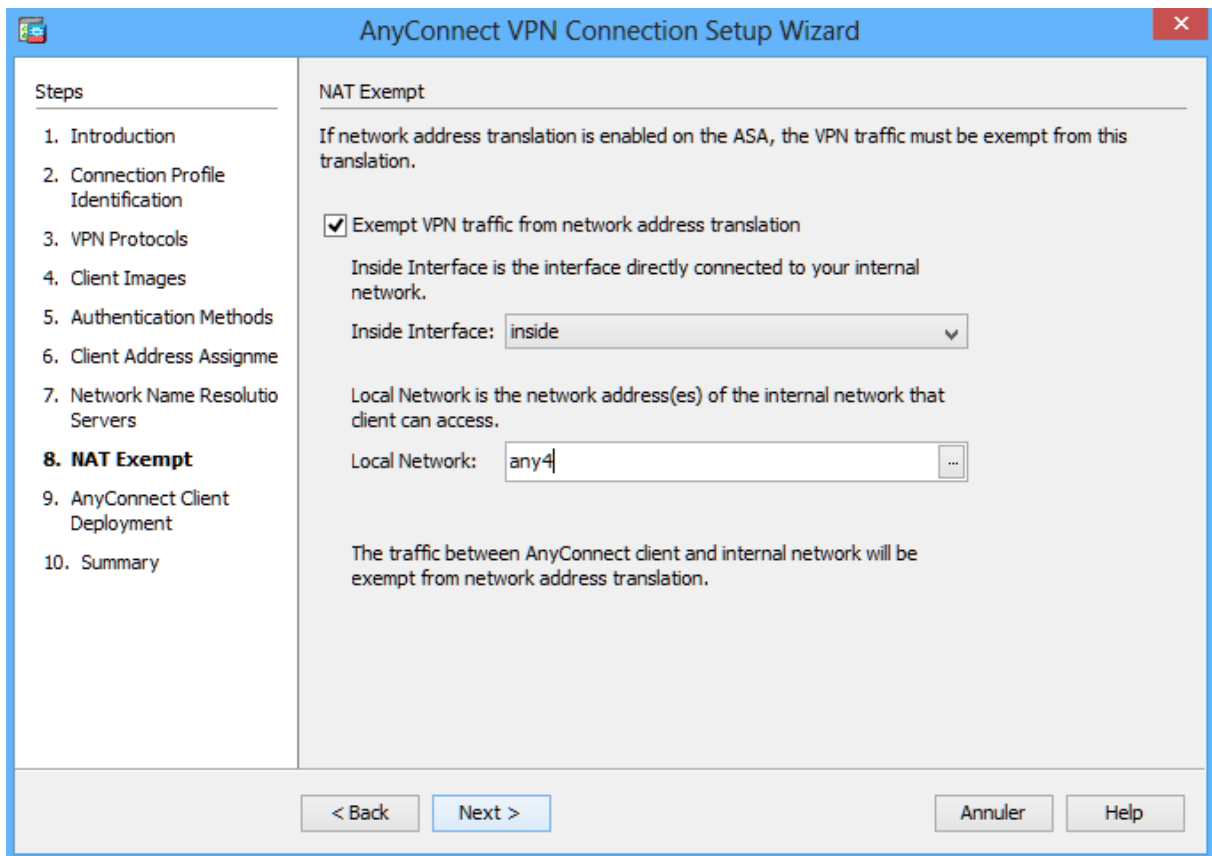


Configure the network name resolution.
On the Network Name Resolution Servers screen, enter the IP address of a DNS server (192.168.1.1). Click Next to continue.

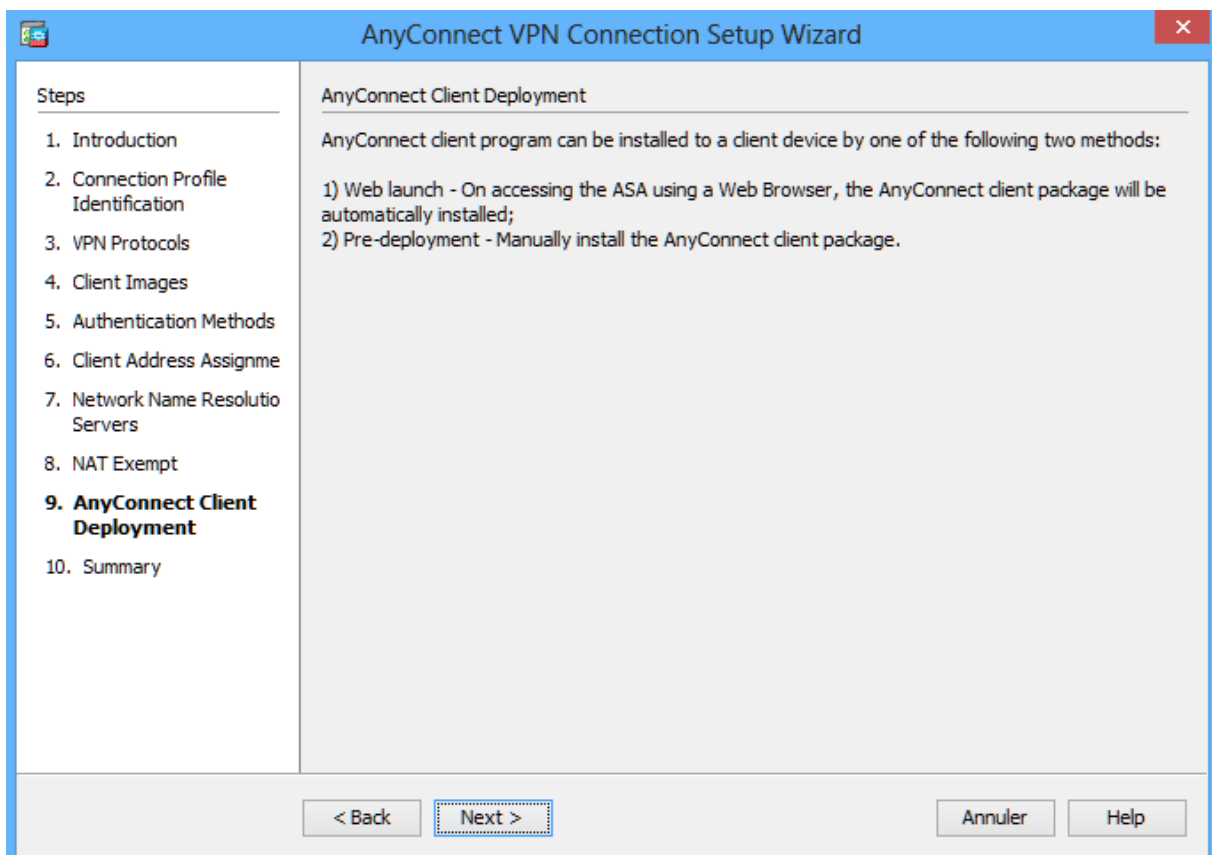


Exempt address translation for VPN traffic.

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.



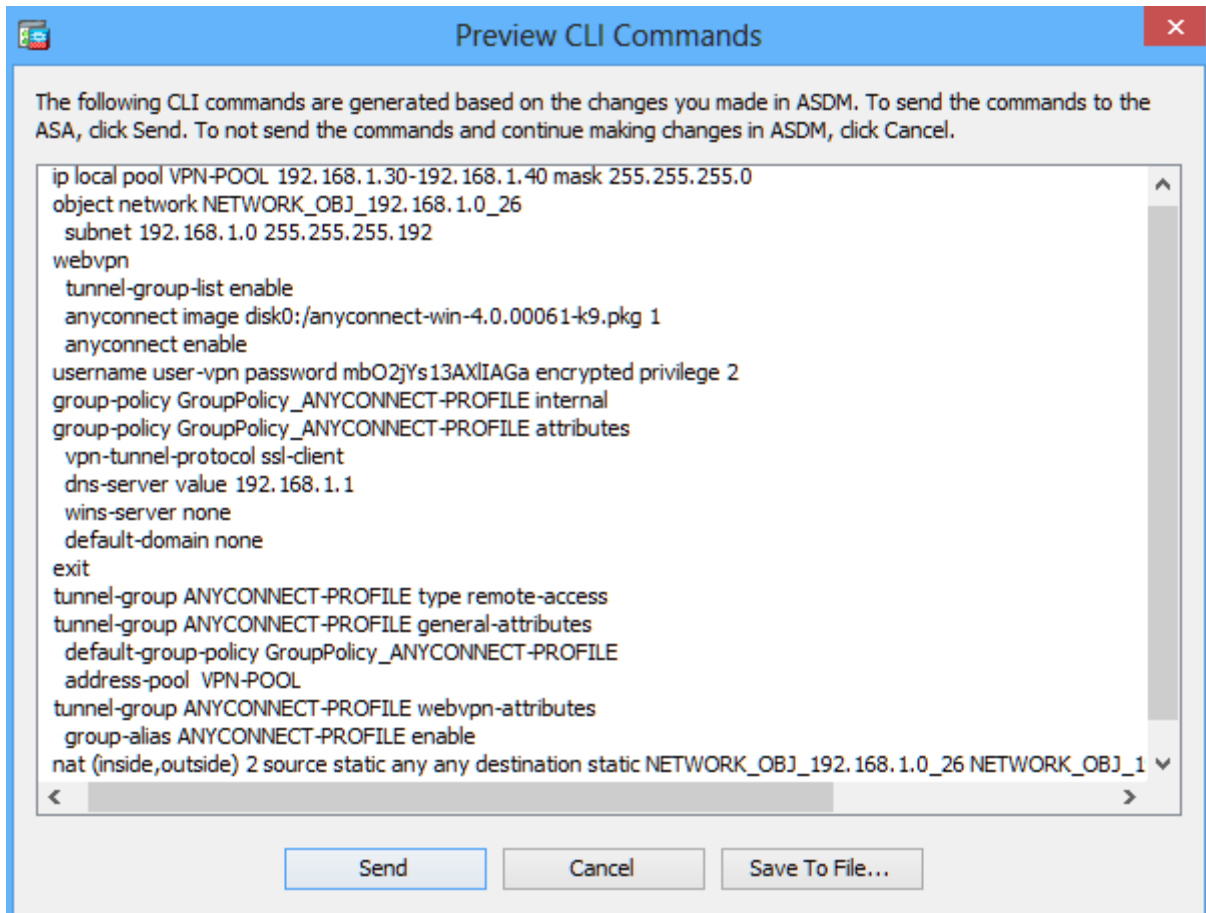
Review the Summary screen and apply the configuration to the ASA.
On the Summary screen, review the configuration, click Finish, and send commands to ASA.

Summary

Here is the summary of the configuration.

Name	Value
<input type="checkbox"/> Summary	
Name/Alias of the Connection Profile	ANYCONNECT-PROFILE
VPN Access Interface	outside
Device Digital Certificate	-- none --
VPN Protocols Enabled	SSL only
AnyConnect Client Images	1 package
Authentication Server Group	LOCAL
Address Pool for the Client	192.168.1.30 - 192.168.1.40
DNS	Server: Domain Name:
Network Address Translation	The protected traffic is not subjected to network address translation

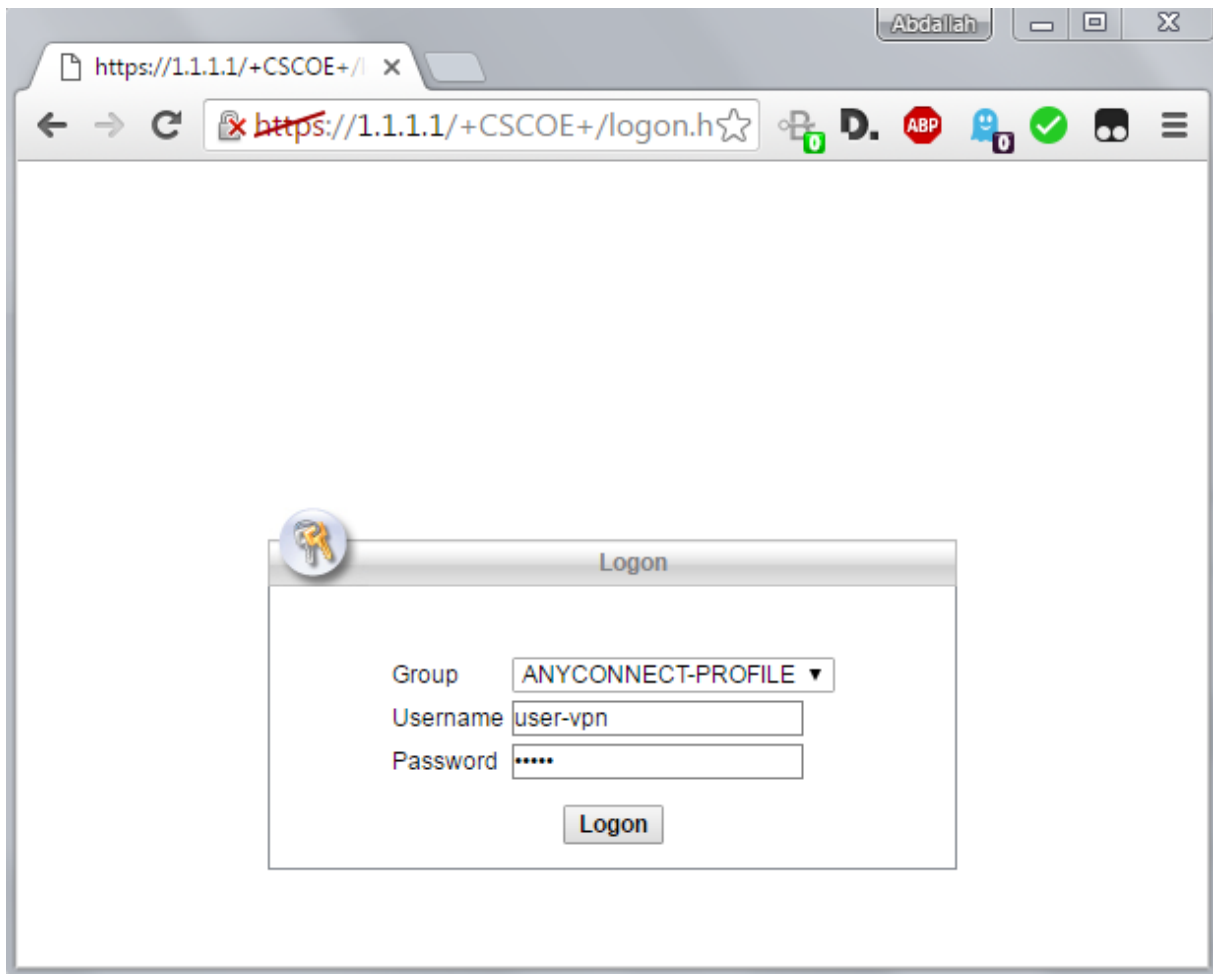
< Back Finish Annuler Help



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).

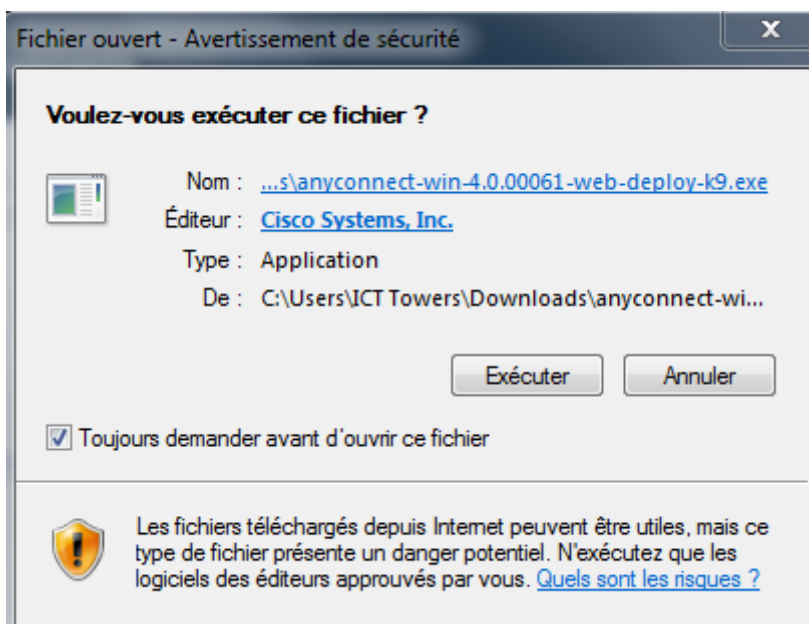
Enter the previously created username `user-vpn` with the password `cisco`. Click Logon to continue.

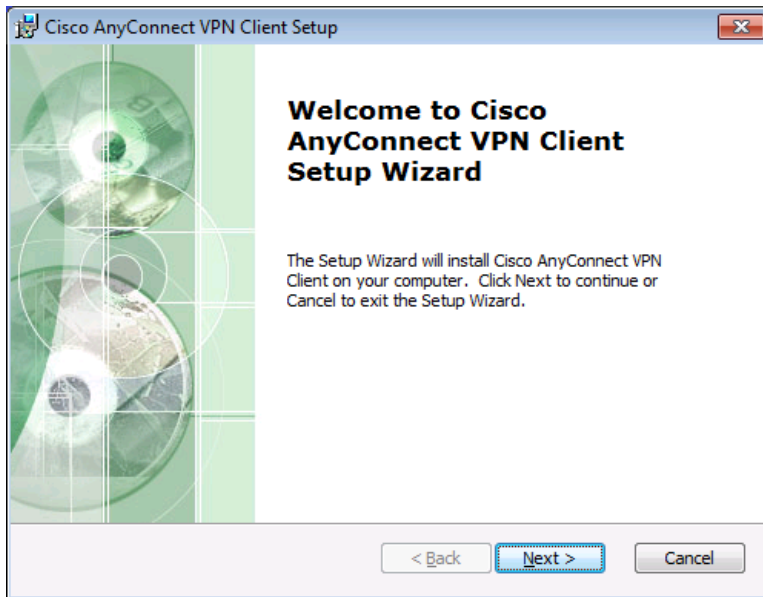


Install the AnyConnect VPN Client (if required).
On the Manual Installation screen, click AnyConnect VPN

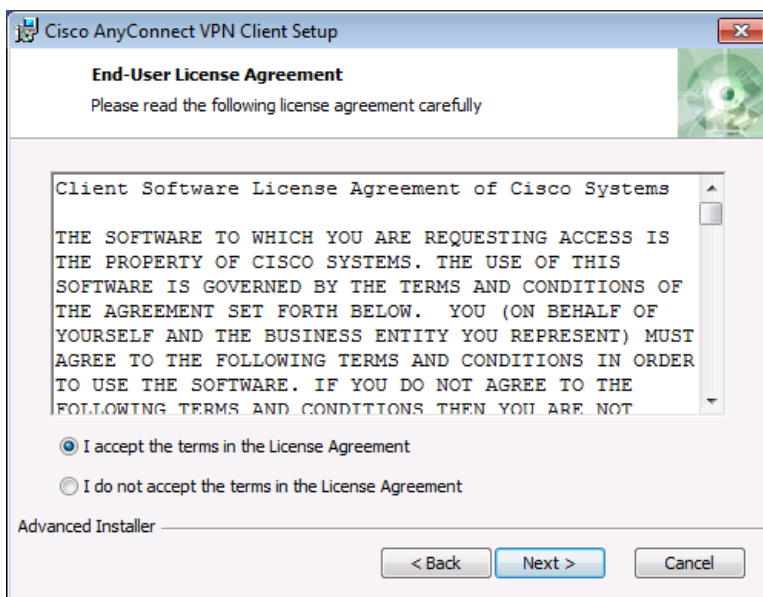


After the download is complete, the Cisco AnyConnect VPN Client Setup starts. Click Next to continue.

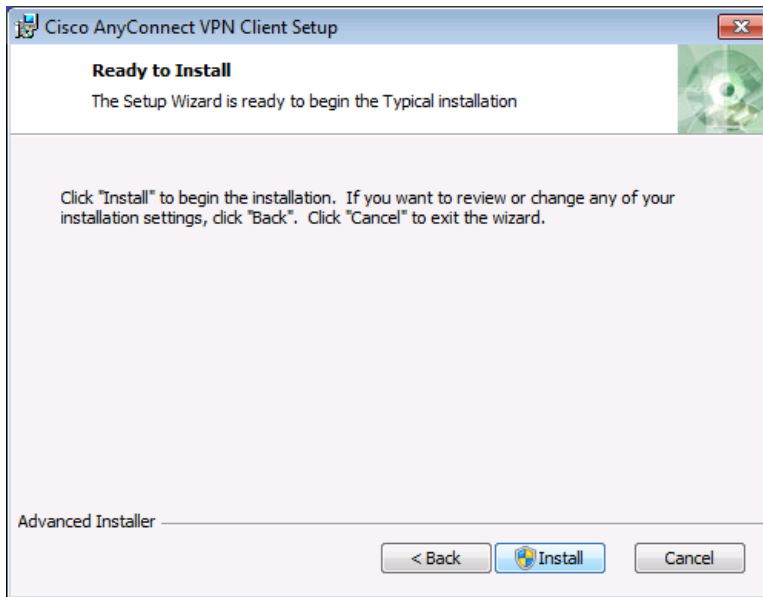




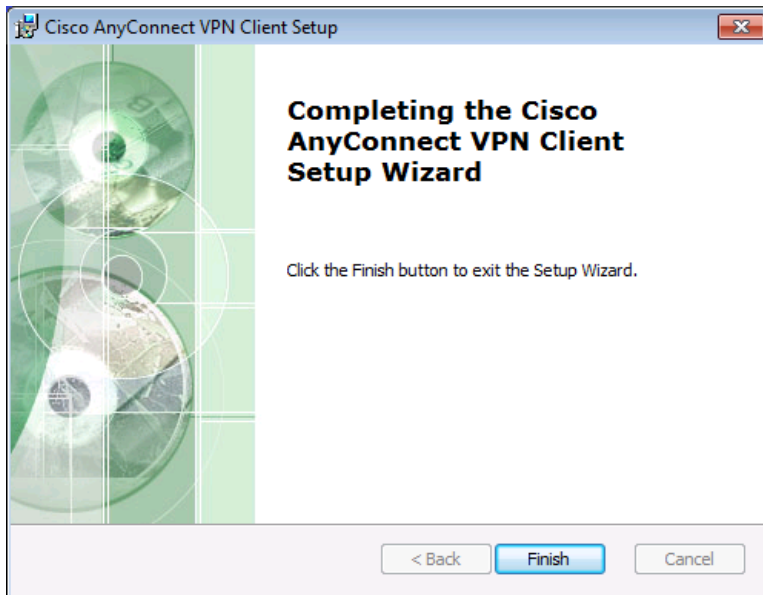
Read the End-User License Agreement. Select I accept the terms in the License Agreement and click Next to continue.



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

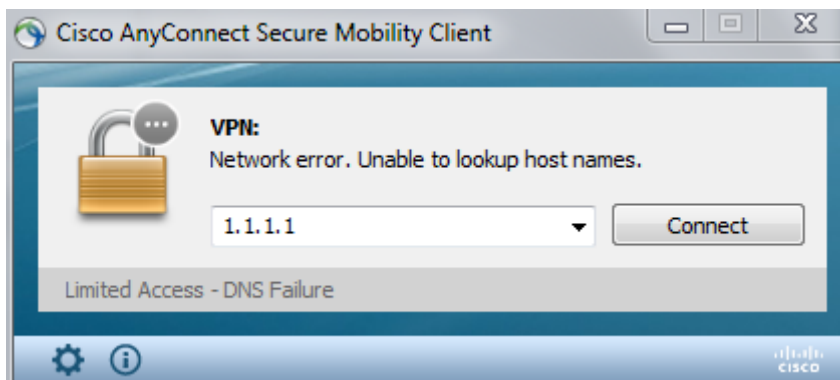


Click Finish to complete the installation.

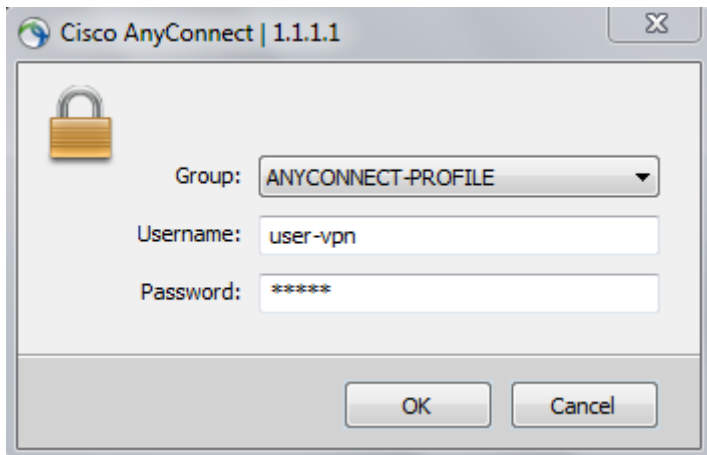


Establish an AnyConnect SSL VPN Connection.

When prompted to enter the secure gateway address, enter 1.1.1.1 in the Connect field, and click Connect.



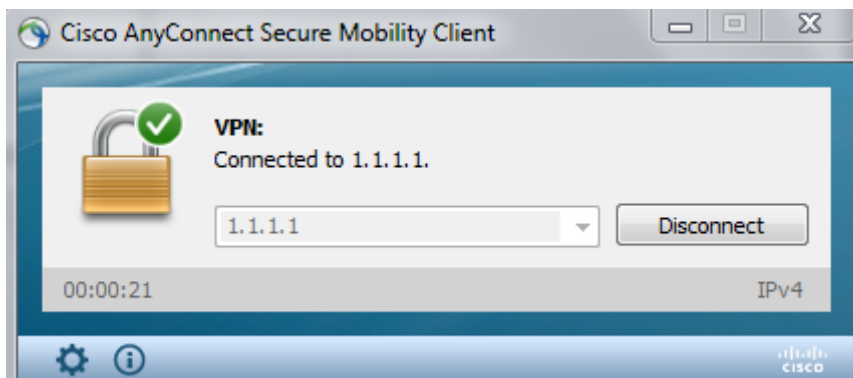
When prompted, enter user-vpn for the username and cisco as the password.



You should see this:

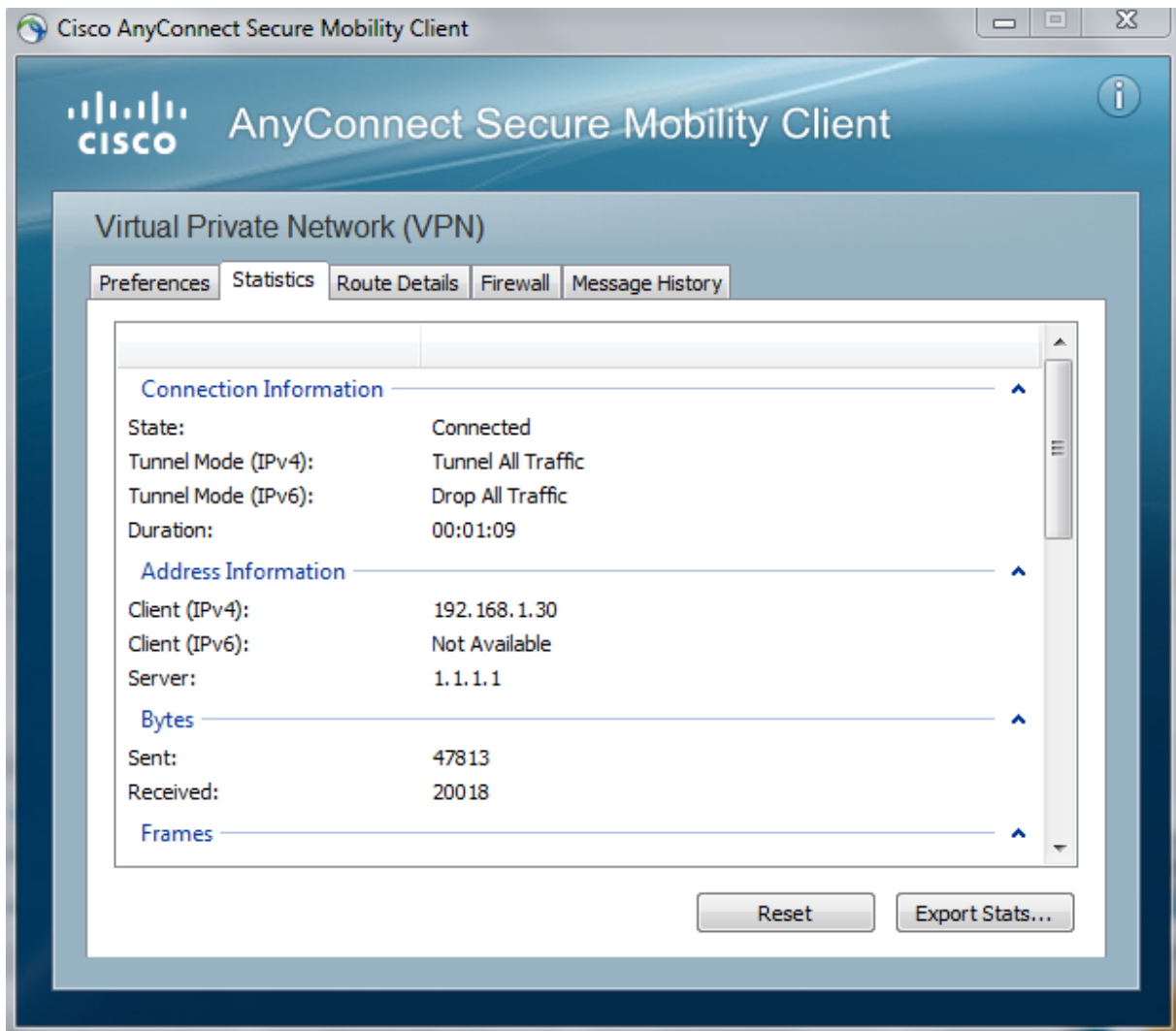
When the full tunnel SSL VPN connection is established, an icon will appear in the system tray that signifies that the client has successfully connected to the SSL VPN network.

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

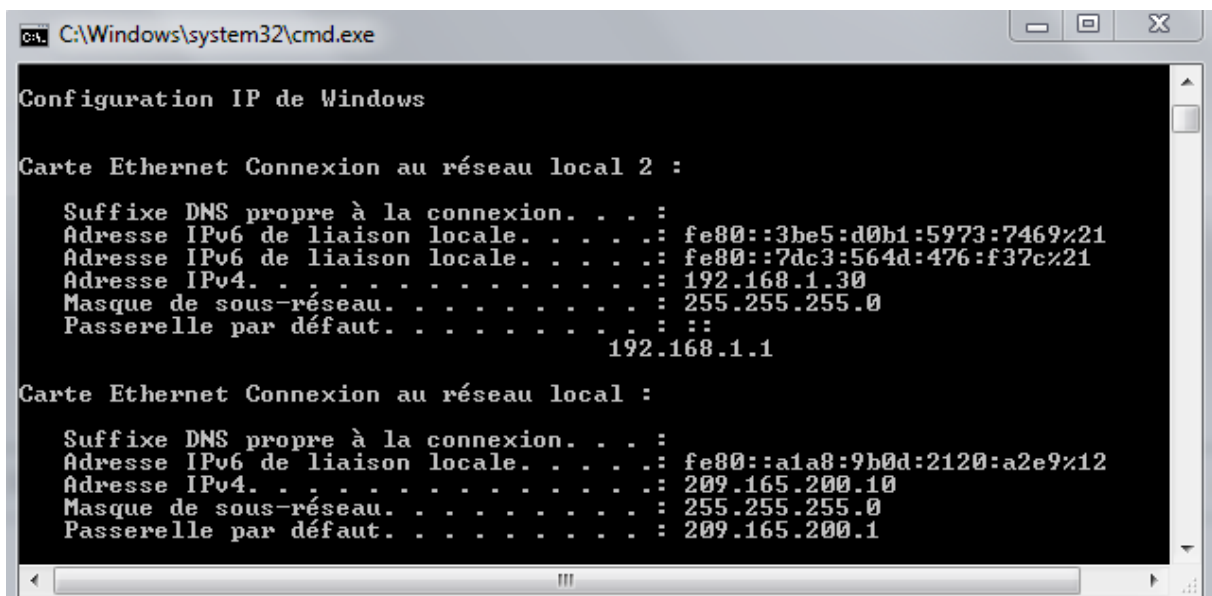


Use the scroll bar on the right side of the Virtual Private Network (VPN) – Statistics tab for additional connection information.

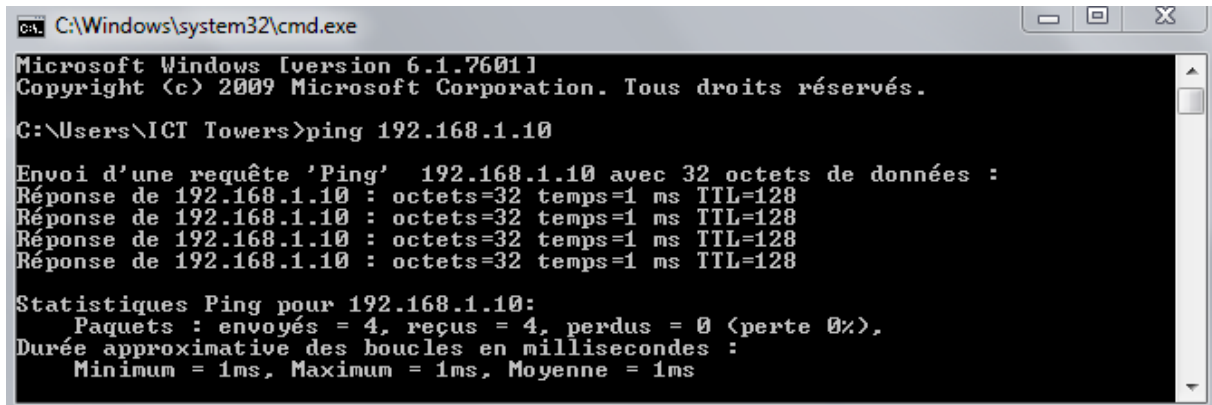
Note: The inside IP address that is assigned to the Outside Host is 192.168.1.30 which is selected from the VPN pool 192.168.1.30-40.



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.



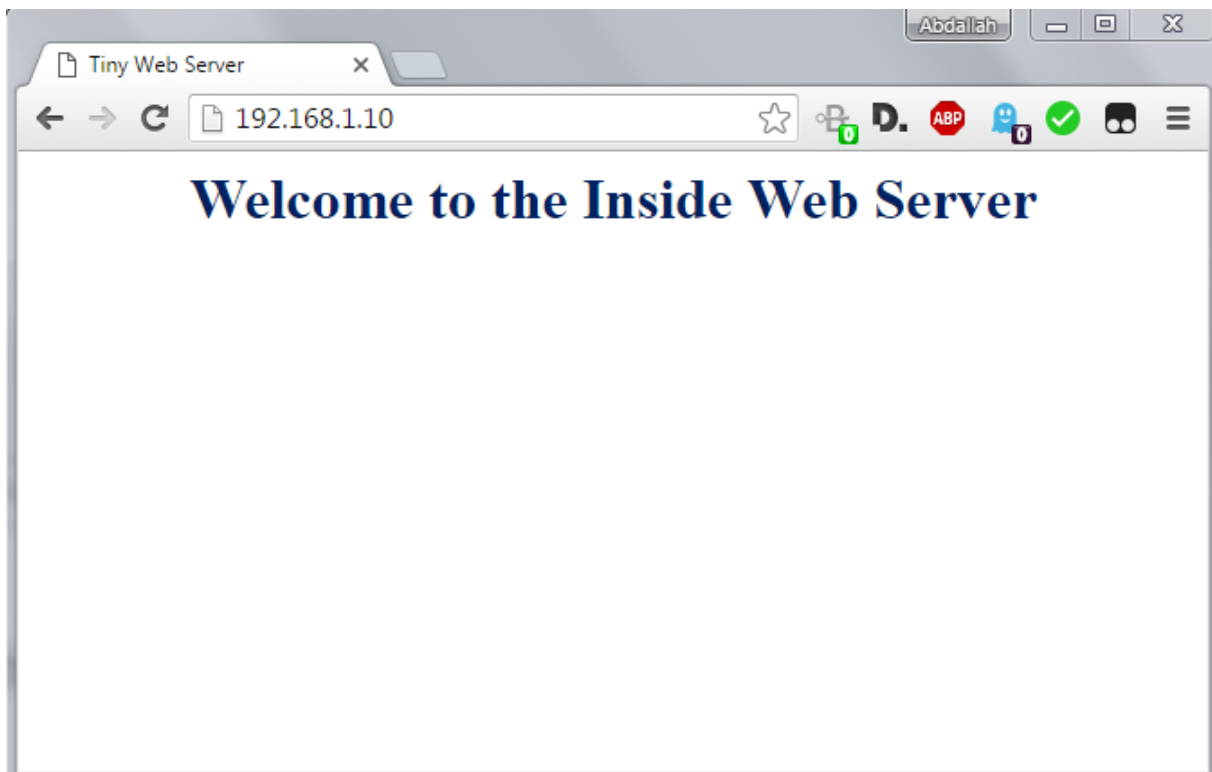
```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\ICT Towers>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

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



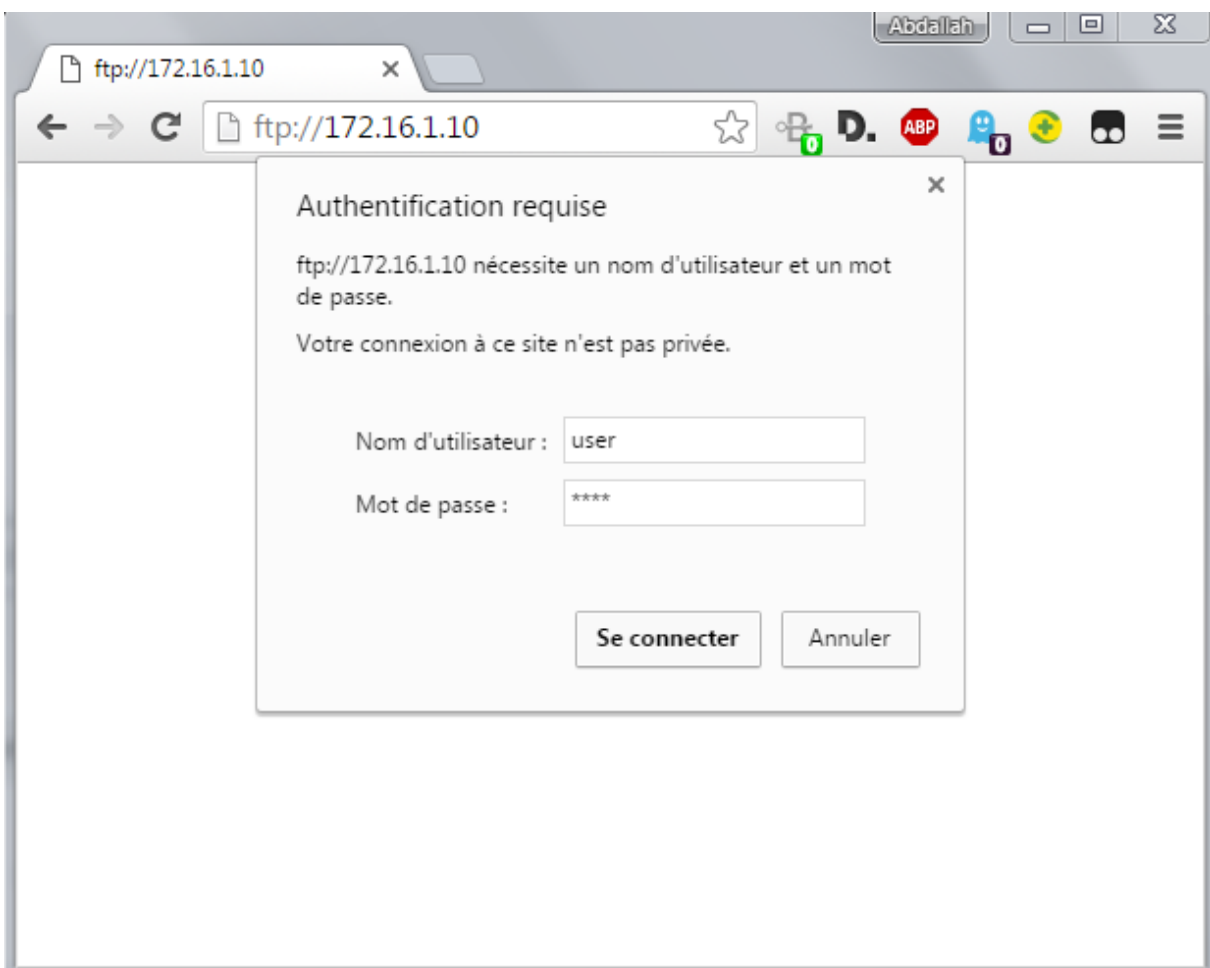
From Outside Host, ping DMZ-SERVER (172.16.1.10) to verify connectivity.

```
C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\ICT Towers>ping 172.16.1.10

Envoi d'une requête 'Ping' 172.16.1.10 avec 32 octets de données :
Réponse de 172.16.1.10 : octets=32 temps=2 ms TTL=128
Réponse de 172.16.1.10 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.1.10 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.1.10 : octets=32 temps=2 ms TTL=128

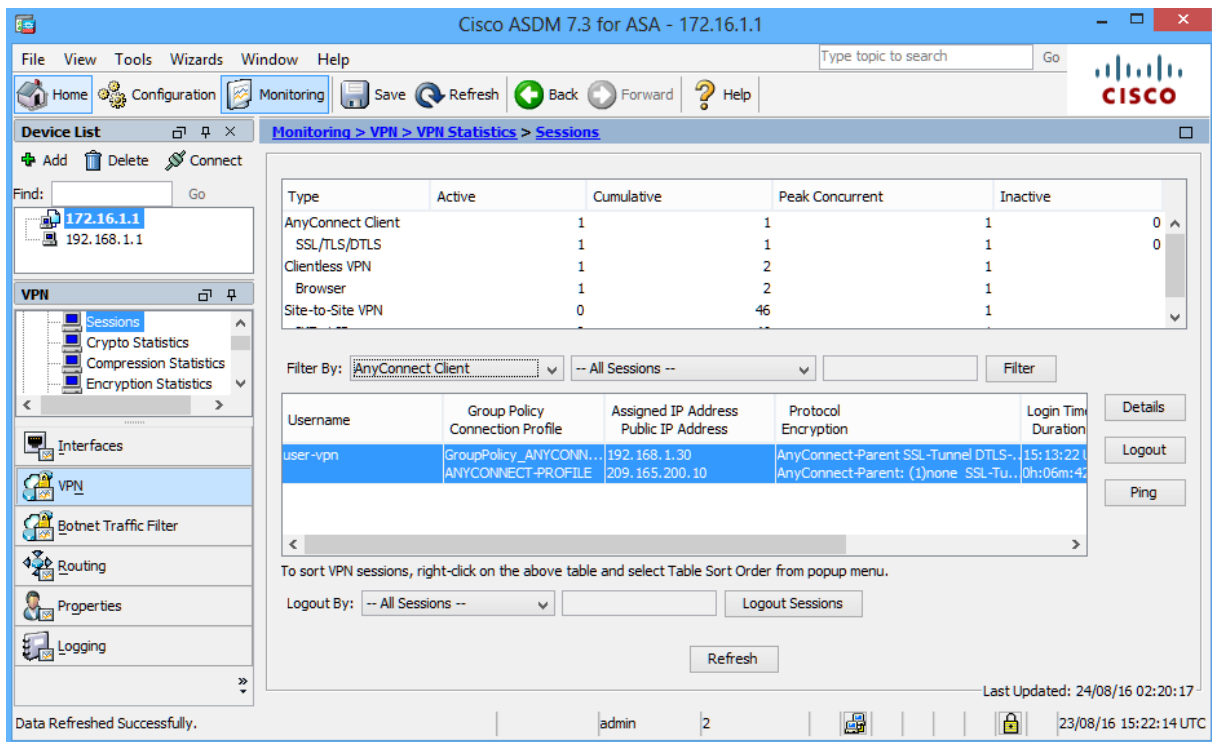
Statistiques Ping pour 172.16.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

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:





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 include:

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.

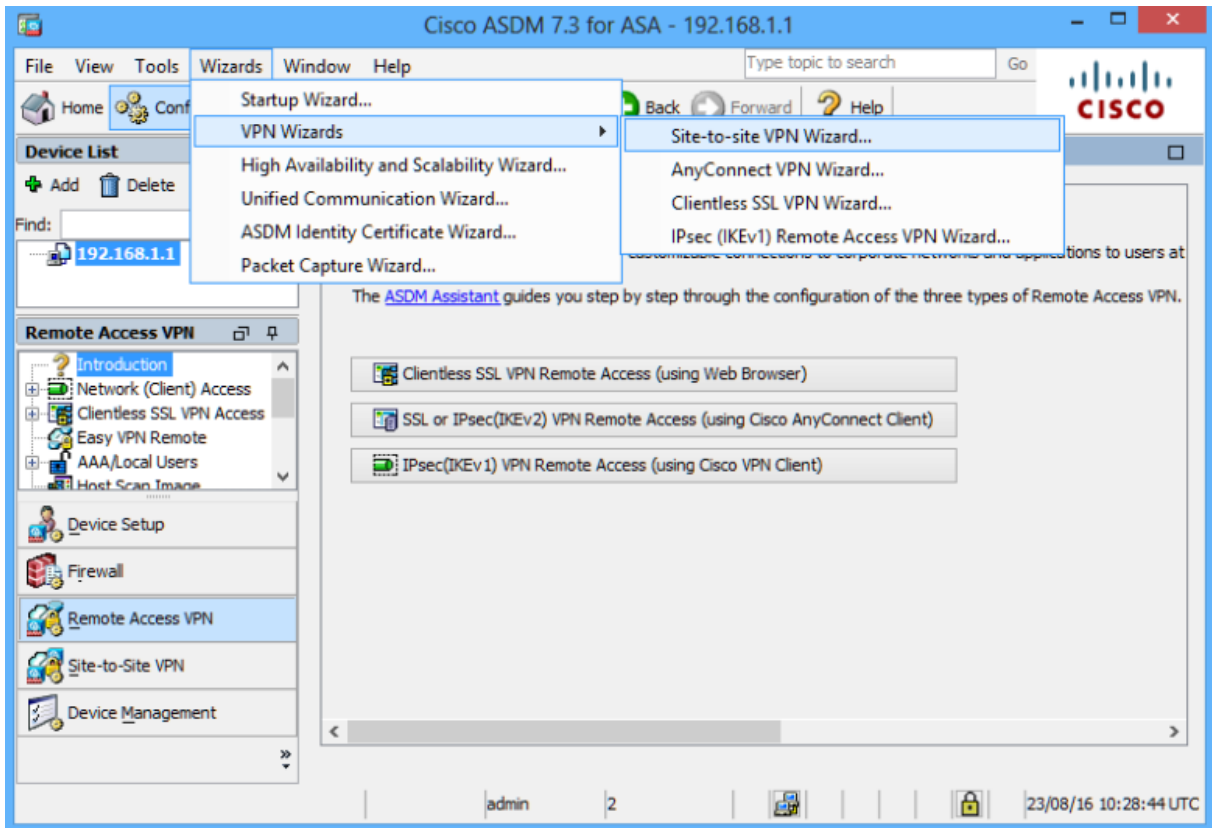
```
ciscoasa(config)# crypto map CRYPTO-MAP 1 match address VPN-ACL
ciscoasa(config)# crypto map CRYPTO-MAP 1 set peer 2.2.2.1
ciscoasa(config)# crypto map CRYPTO-MAP 1 set transform-set TEST
```

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

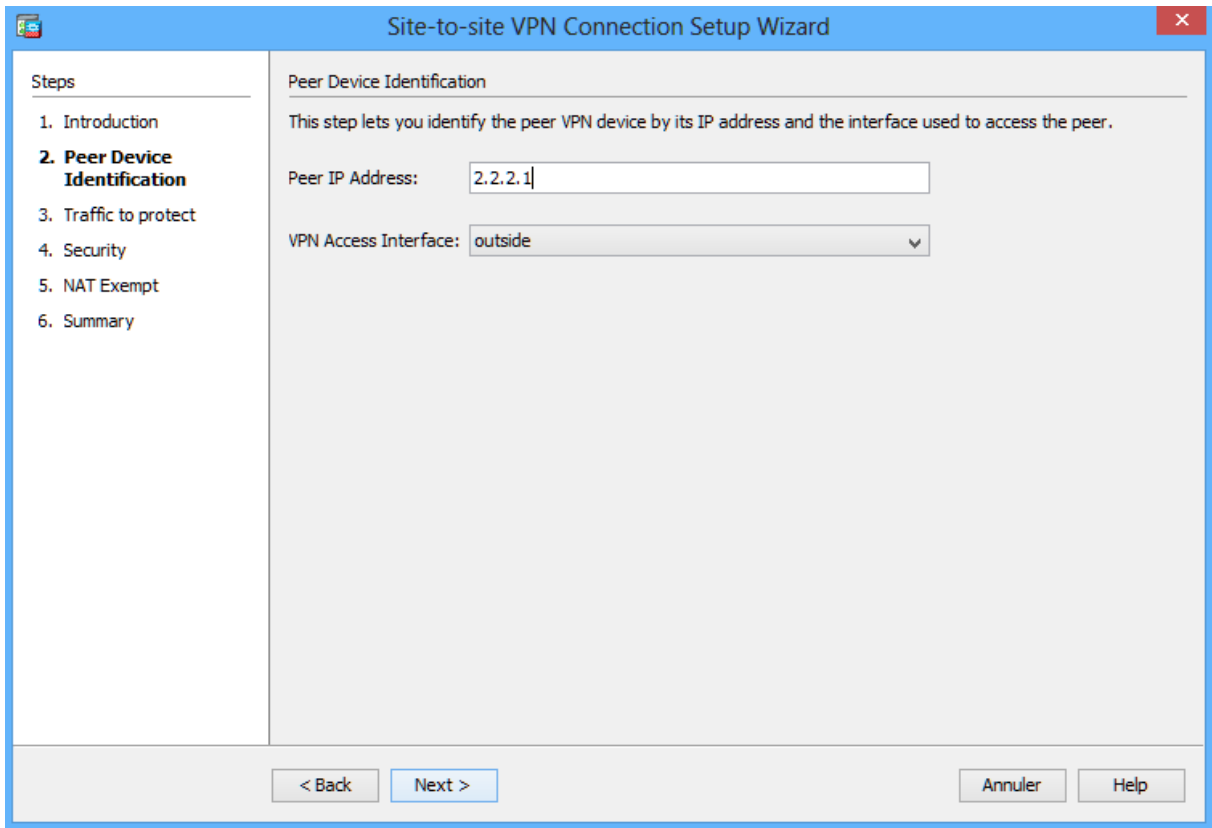
```
ciscoasa(config)# crypto map CRYPTO-MAP interface outside
```

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

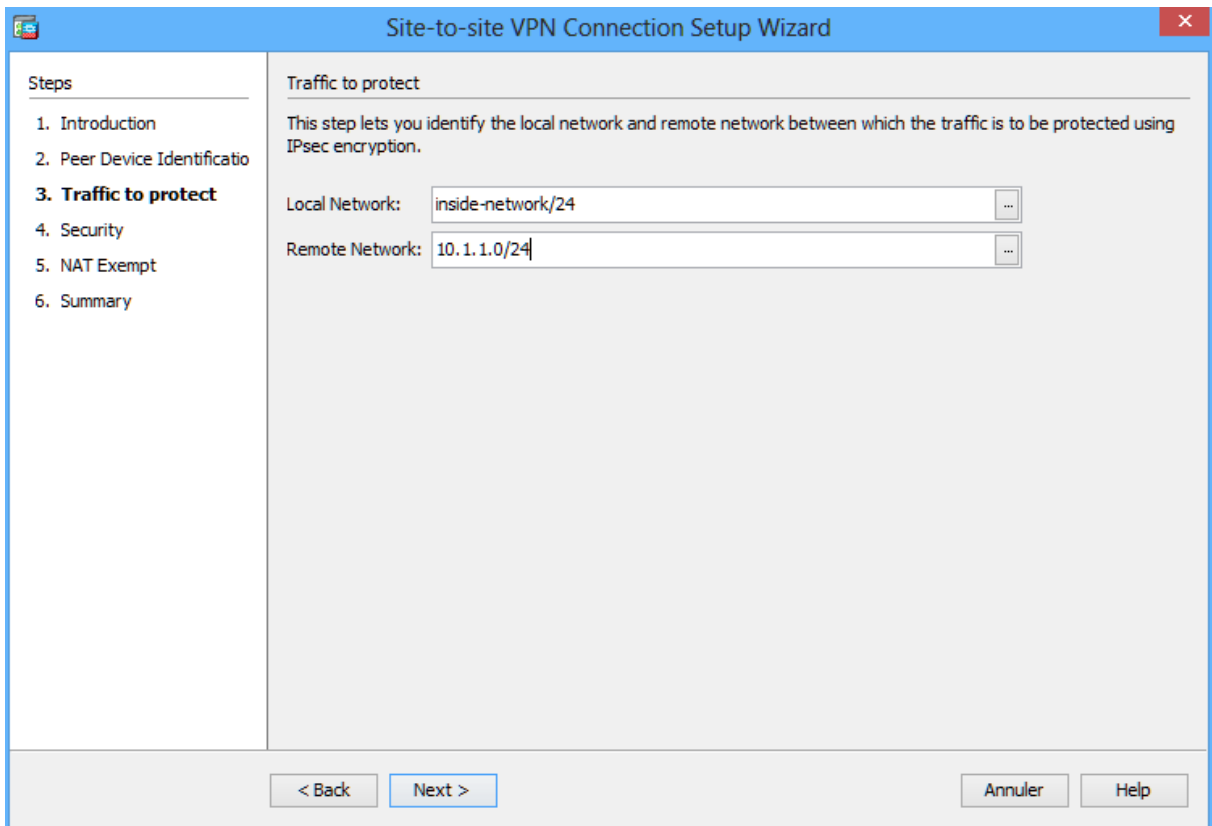
Using ASDM. Use the Site-to-Site VPN Wizard to configure the ASA for IPsec site-to-site VPN.



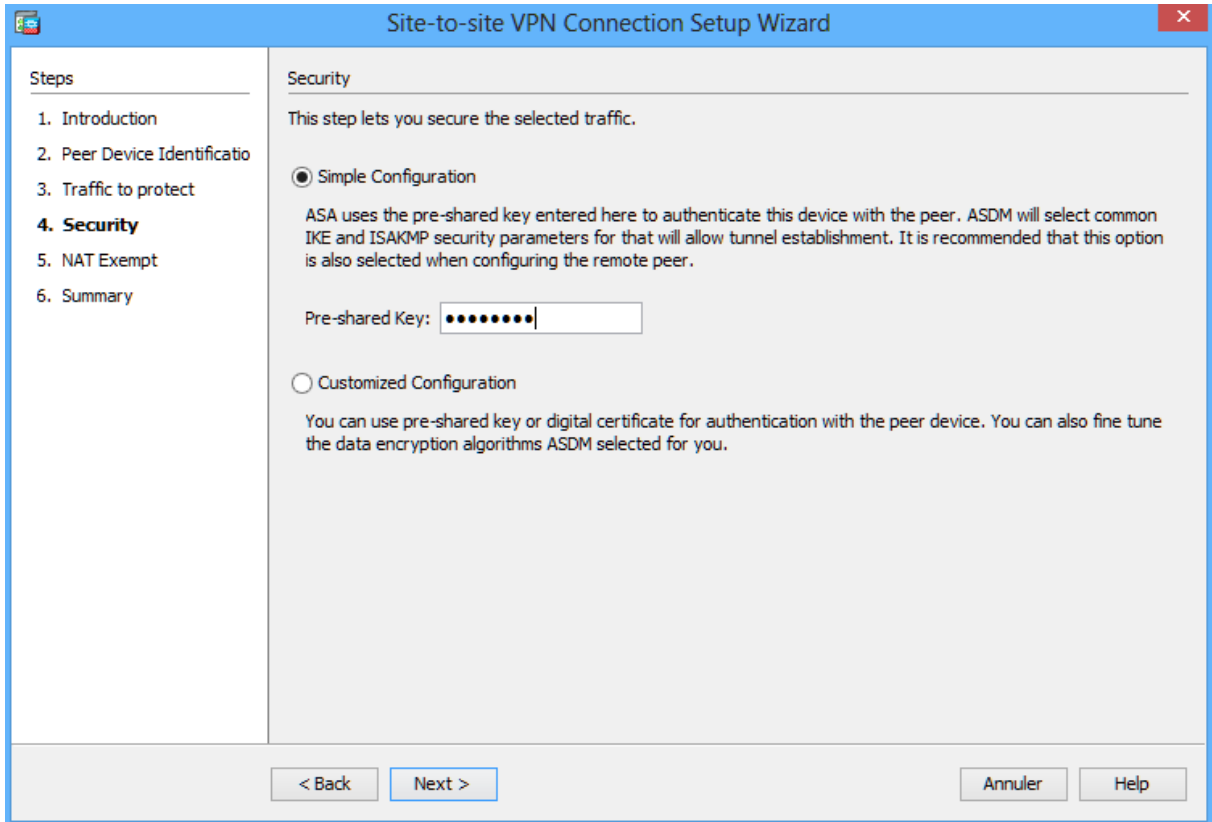
Set the Peer IP Address to R1's G0/1 IP address (2.2.2.1). Verify that outside is selected for the VPN Access Interface.



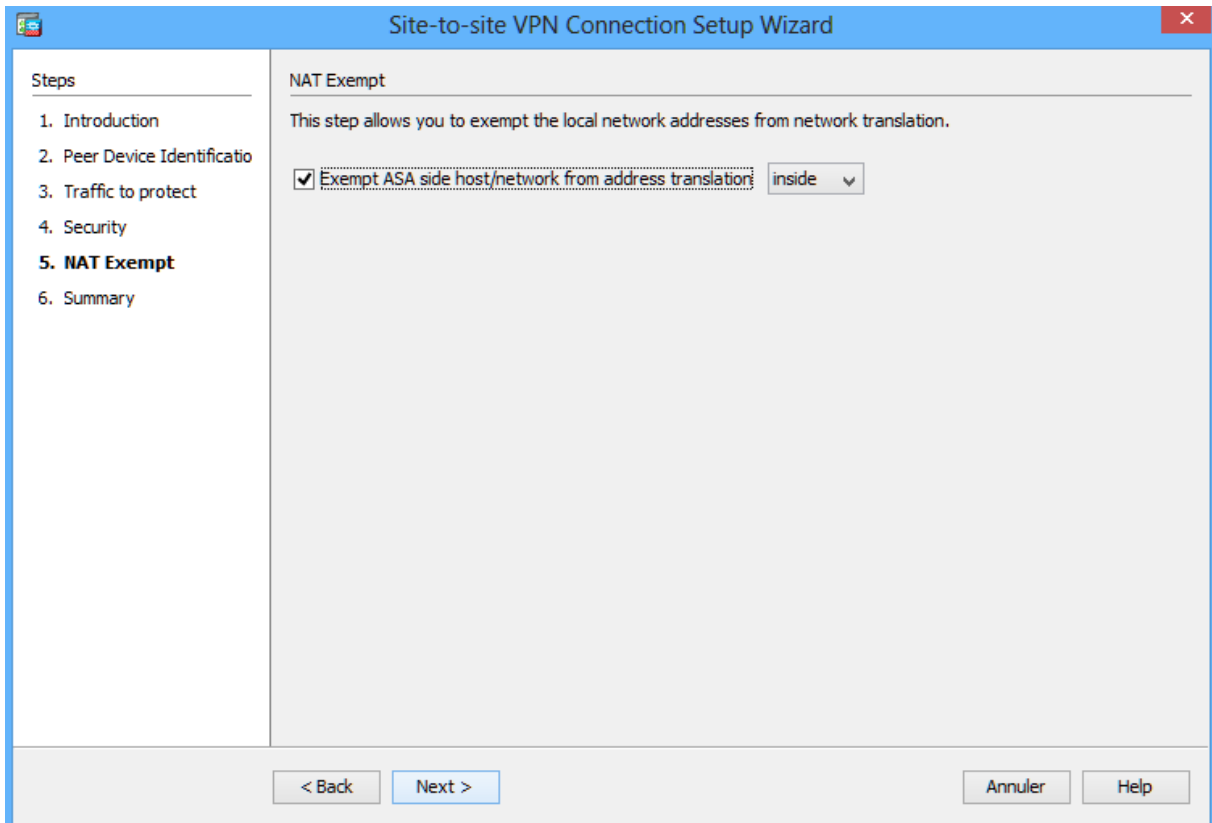
Identify the traffic to protect. Set the Local Network to inside-network/24 and the Remote Network to 172.16.3.0/24.



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.

Name	Value
Summary	
Peer Device IP Address	2.2.2.1
VPN Access Interface	outside
Protected Traffic	Local Network: 192.168.1.0/24 Remote Network: 10.1.1.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
IKE v1	
IKE Policy	crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-sha, crack-aes-256-sha, rsa-sig-aes-256-sha, pre-share-aes-256-sha, crack-3des-sha, rsa-sig-3des-sha, pre-share-3des-sha, crack-des-sha, rsa-sig-des-sha, pre-share-des-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5

At the bottom of the window, there are buttons for '< Back', 'Finish', 'Annuler', and 'Help'.

```

object network NETWORK_OBJ_10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_192.168.1.0_24
 subnet 192.168.1.0 255.255.255.0
access-list outside_cryptomap line 1 extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
group-policy GroupPolicy_2.2.2.1 internal
group-policy GroupPolicy_2.2.2.1 attributes
 vpn-tunnel-protocol ikev2 ikev1
exit
tunnel-group 2.2.2.1 type ipsec-l2l
tunnel-group 2.2.2.1 general-attributes
 default-group-policy GroupPolicy_2.2.2.1
tunnel-group 2.2.2.1 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
isakmp keepalive threshold 10 retry 2
crypto ikev1 policy 70
 encryption aes
 authentication crack
crypto ikev1 policy 80
 encryption aes
  
```

At the bottom of the window, there are buttons for 'Send', 'Cancel', and 'Save To File...'.

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 pcg sas:

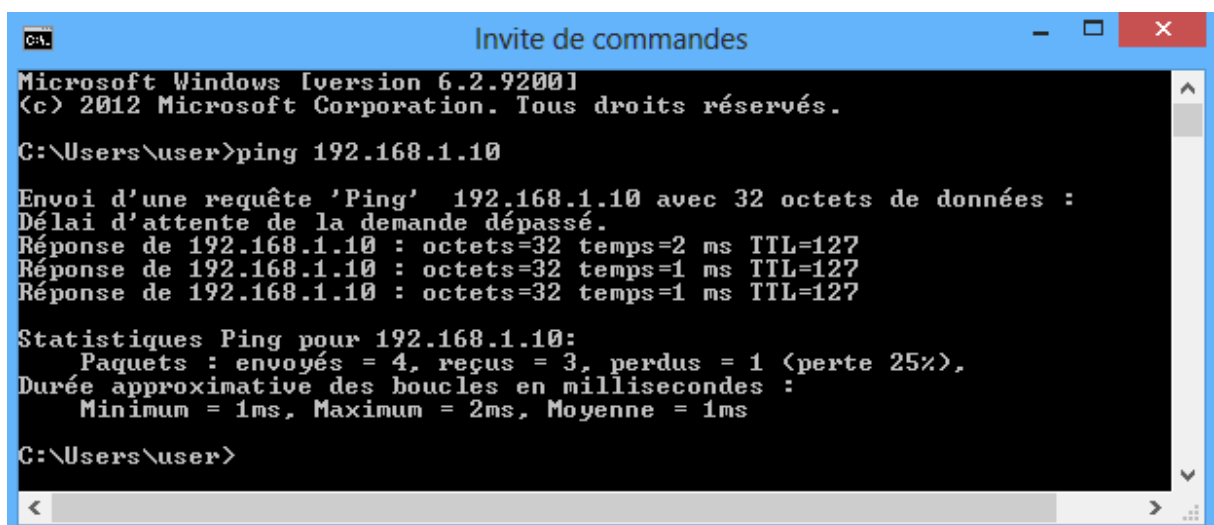
outbound esp sas:

outbound ah sas:

outbound pcg 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 successful as shown below:



```
Microsoft Windows [version 6.2.9200]
(c) 2012 Microsoft Corporation. Tous droits réservés.

C:\Users\user>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Réponse de 192.168.1.10 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\user>
```

Verify the ISAKMP policy, the association security for phase 1 is negotiated 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

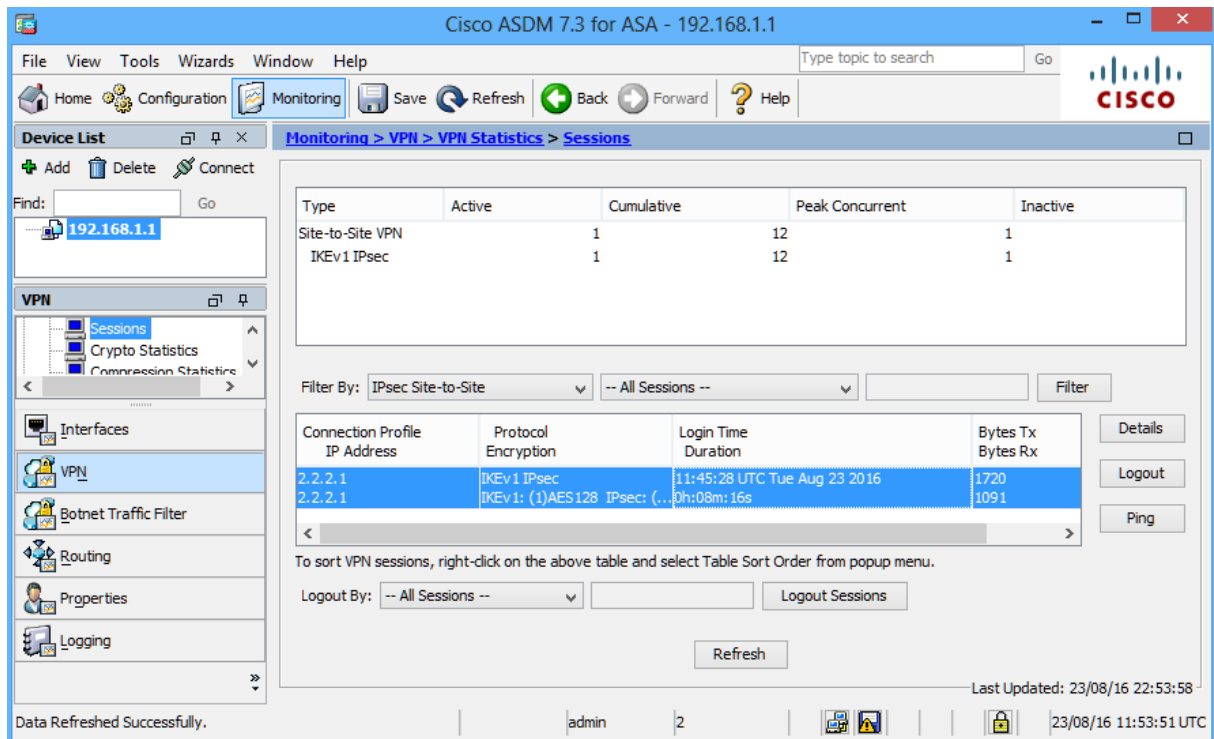
There are no IKEv2 SAs
ciscoasa#
```

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:

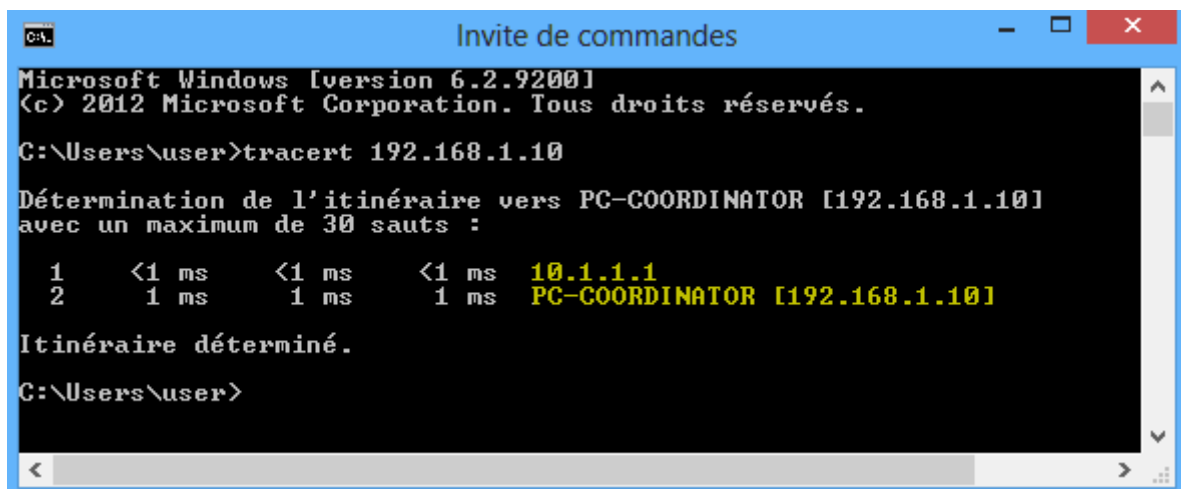
```
R1#show crypto ipsec sa | i local|remote|pkts
Crypto map tag: CMAP, local addr 2.2.2.1
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
#pkts decaps: 3, #pkts decrypt: 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:

```

C:\Users\user>ping 10.1.1.10

Microsoft Windows [version 6.2.9200]
(c) 2012 Microsoft Corporation. Tous droits réservés.

C:\Users\user>ping 10.1.1.10

Envoi d'une requête 'Ping' 10.1.1.10 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 10.1.1.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\user>

```

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:

```

C:\Users\user>ftp 10.1.1.10

Microsoft Windows [version 6.2.9200]
(c) 2012 Microsoft Corporation. Tous droits réservés.

C:\Users\user>ftp 10.1.1.10
> ftp: connect :Délai de connexion dépassé
ftp>

```

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 pair 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:

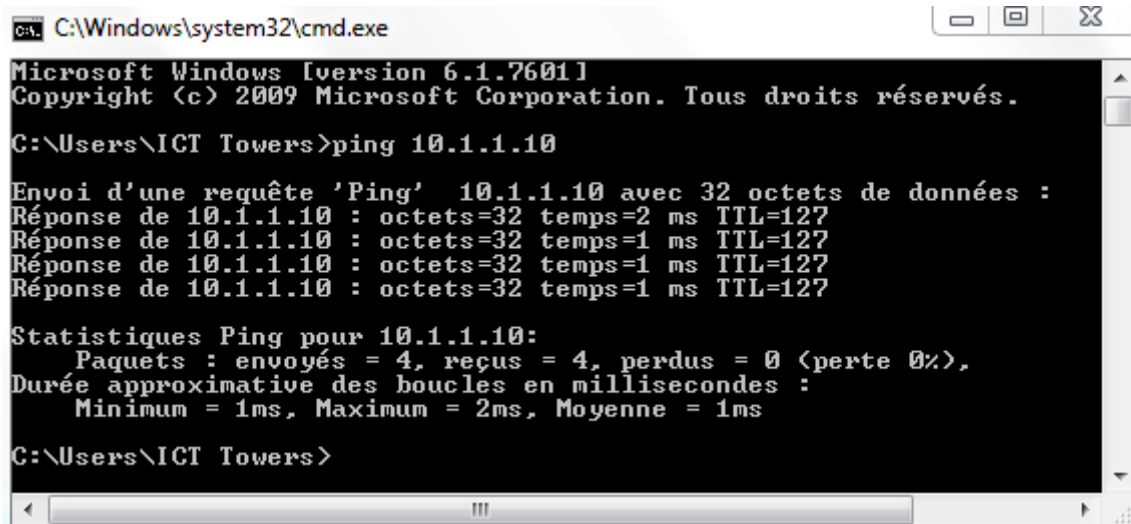
```
R1(config)#policy-map type inspect OUT-IN-POLICY
R1(config-pmap)#class OUTSIDE-TRAFFIC
R1(config-pmap-c)#inspect
```

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 successful:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\ICT Towers>ping 10.1.1.10

Envoi d'une requête 'Ping' 10.1.1.10 avec 32 octets de données :
Réponse de 10.1.1.10 : octets=32 temps=2 ms TTL=127
Réponse de 10.1.1.10 : octets=32 temps=1 ms TTL=127
Réponse de 10.1.1.10 : octets=32 temps=1 ms TTL=127
Réponse de 10.1.1.10 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 10.1.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\ICT Towers>
```

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:

```

C:\Users\user>ftp 10.1.1.10
Connecté à 10.1.1.10.
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse <tim.kosse@filezilla-project.org>
220 Please visit https://filezilla-project.org/
Utilisateur (10.1.1.10:(none)) : user
331 Password required for user
Mot de passe :
230 Logged on
ftp> dir
200 Port command successful
150 Opening data channel for directory listing of "/"
-r--r--r-- 1 ftp ftp      58907 Jan 04 2016 Capture1.PNG
-r--r--r-- 1 ftp ftp      23238 Jan 04 2016 Capture10.PNG
-r--r--r-- 1 ftp ftp      50267 Jan 04 2016 Capture11.PNG
-r--r--r-- 1 ftp ftp      46620 Jan 04 2016 Capture12.PNG
-r--r--r-- 1 ftp ftp      31208 Jan 04 2016 Capture13.PNG
-r--r--r-- 1 ftp ftp      30618 Jan 04 2016 Capture14.PNG
-r--r--r-- 1 ftp ftp      45031 Jan 04 2016 Capture15.PNG
-r--r--r-- 1 ftp ftp      18025 Jan 04 2016 Capture16.PNG
-r--r--r-- 1 ftp ftp      18702 Jan 04 2016 Capture17.PNG
-r--r--r-- 1 ftp ftp      46523 Jan 04 2016 Capture18.PNG
-r--r--r-- 1 ftp ftp      18734 Jan 04 2016 Capture2.PNG
-r--r--r-- 1 ftp ftp      50622 Jan 04 2016 Capture3.PNG
-r--r--r-- 1 ftp ftp      11403 Jan 04 2016 Capture4.PNG
-r--r--r-- 1 ftp ftp      11734 Jan 04 2016 Capture5.PNG
-r--r--r-- 1 ftp ftp      19634 Jan 04 2016 Capture6.PNG
-r--r--r-- 1 ftp ftp      26004 Jan 04 2016 Capture7.PNG
-r--r--r-- 1 ftp ftp      16743 Jan 04 2016 Capture8.PNG
-r--r--r-- 1 ftp ftp      20866 Jan 04 2016 Capture9.PNG
-r-xr-xr-x 1 ftp ftp      7864229 Dec 23 2015 fusioninventory-agent_windows-x
64_2.3.17.exe
-r-xr-xr-x 1 ftp ftp      58620968 Jan 21 2016 GNS3-1.3.3-all-in-one.exe
drwxr-xr-x 1 ftp ftp           0 Jan 21 2016 SWITCH IOS
-r-xr-xr-x 1 ftp ftp      109574432 Aug 25 2015 VirtualBox-4.3.12-93733-Win.exe
226 Successfully transferred "/"
ftp : 1460 octets reçus en 0.11 secondes à 13.39 Ko/s.
ftp>

```

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#