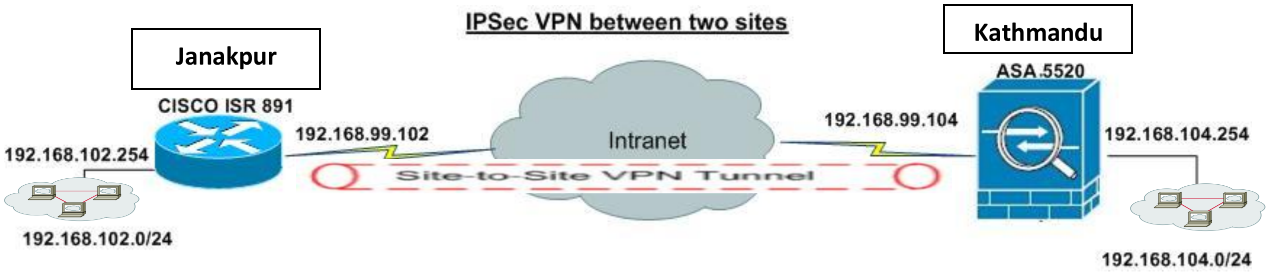
An Example of IPSec VPN between two sites:



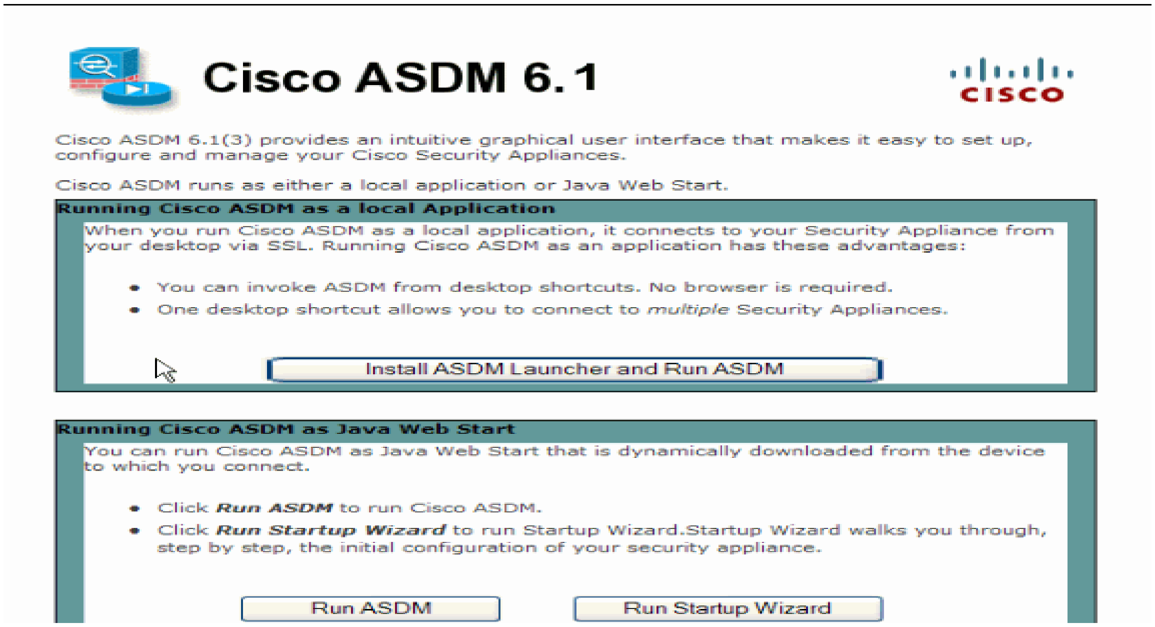
Cisco ISR 891 Configuration:

```
Hostname ISR-891

Username  cisco  privilege 15 secret 0 Password@123

Crypto  isakmp  policy  12

Encryption  3des

Hash  sha

Authentication  pre-share

Group   2

Lifetime  3600

Exit


Crypto  isakmp key  0 cisco123 address   192.168.99.104

Crypto ipsec transform-set   set-70  esp-3des  esp-sha-hmac

Mode tunnel

Exit


Crypto  ipsec  security-association  lifetime  seconds  1800

Access-list  111 permit   ip  192.168.102.0  0.0.0.255  192.168.104.0  0.0.0.25

Crypto  map connect-to-asa  80  ipsec-isakmp

Set  peer  192.168.99.104

Match  address  111

Set  transform-set set-70

Exit
```

```
Interface  GigabitEthernet 0
Ip address  192.168.99.102  255.255.255.0
Crypto  map  connect-to-asa
No  shutdown
Exit

Interface VALN 1
Ip  address  192.168.102.0  255.255.255.0
No  shutdown
Exit

Ip   route  192.168.104.0  255.255.255.0  192.168.99.104

….end
```

Cisco ASA 5520 Configuration:

1.Open your browser and enter **https://<IP_Address of the interface of ASA that has been configured for ASDM Access>** to access the ASDM on the ASA.



Cisco ASDM 6.1

Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or Java Web Start.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

Running Cisco ASDM as Java Web Start

You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device to which you connect.

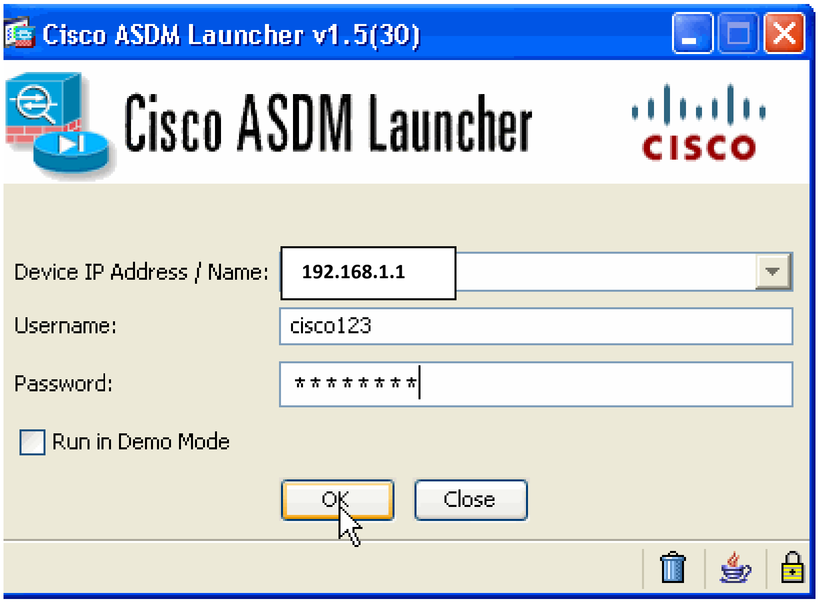
- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run Startup Wizard.Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

2. Click **Download ASDM Launcher and Start ASDM** in order to download the installer for the ASDM application.

3.Once the ASDM Launcher downloads, perform the steps directed by the prompts in order to install the software and run the Cisco ASDM Launcher.

4.Enter the IP address for the interface you configured with the **http** − command. Also, enter a username and password if you specified one.

This example uses *cisco123* for both the username and the password.



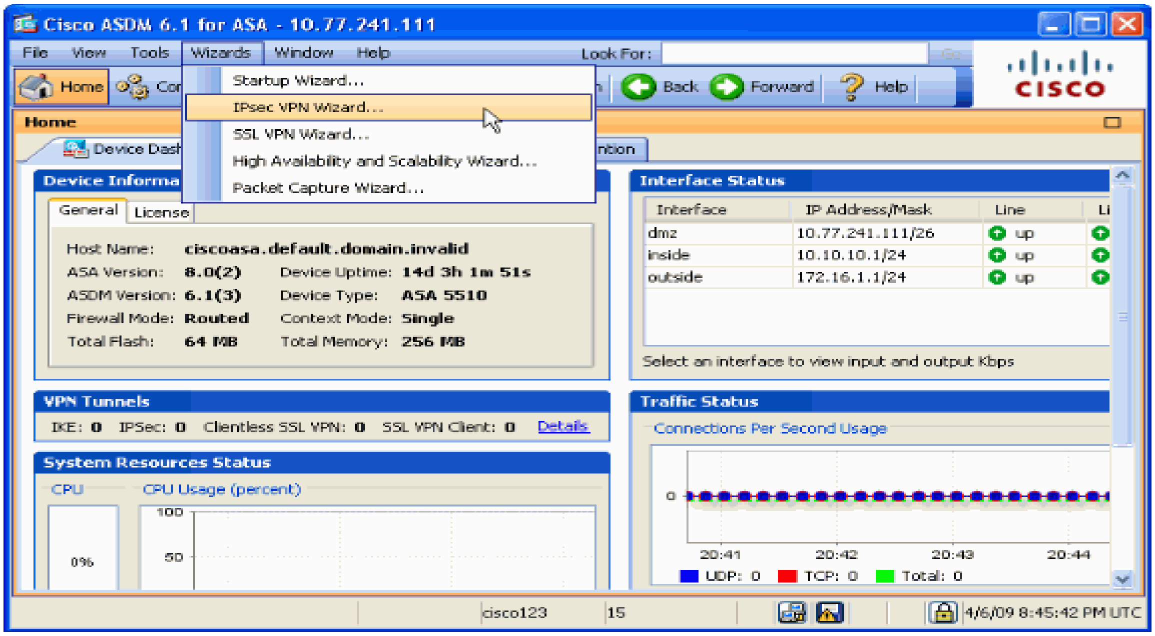
Device IP Address / Name: 192.168.1.1

Username: cisco123

Password: ********

□ Run in Demo Mode

5. Run the **IPsec VPN Wizard** once the ASDM application connects to the ASA.



Cisco ASDM 6.1 for ASA - 10.77.241.111

Device Information

Host Name:	ciscoasa.default.domain.invalid		
ASA Version:	8.0(2)	Device Uptime:	14d 3h 1m 51s
ASDM Version:	6.1(3)	Device Type:	ASA 5510
Firewall Mode:	Routed	Context Mode:	Single
Total Flash:	64 MB	Total Memory:	256 MB

Interface Status

Interface	IP Address/Mask	Line
dmz	10.77.241.111/26	up
inside	10.10.10.1/24	up
outside	172.16.1.1/24	up

Select an interface to view input and output Kbps

VPN Tunnels

IKE: 0 IPSec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0

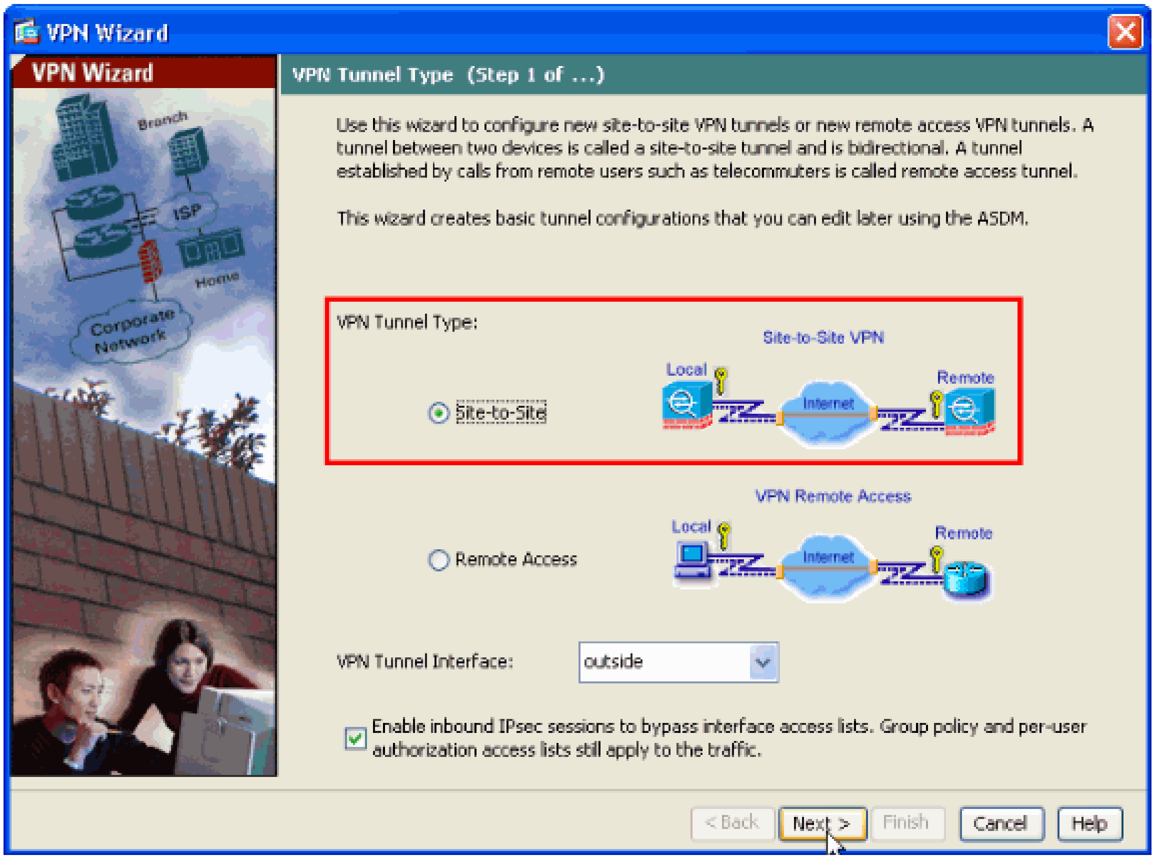
System Resources Status

Traffic Status

UDP: 0 TCP: 0 Total: 0

cisco123 15 4/6/09 8:45:42 PM UTC

6. Choose **Site−to−Site** for the IPsec VPN Tunnel Type, and click **Next**.



VPN Wizard

VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

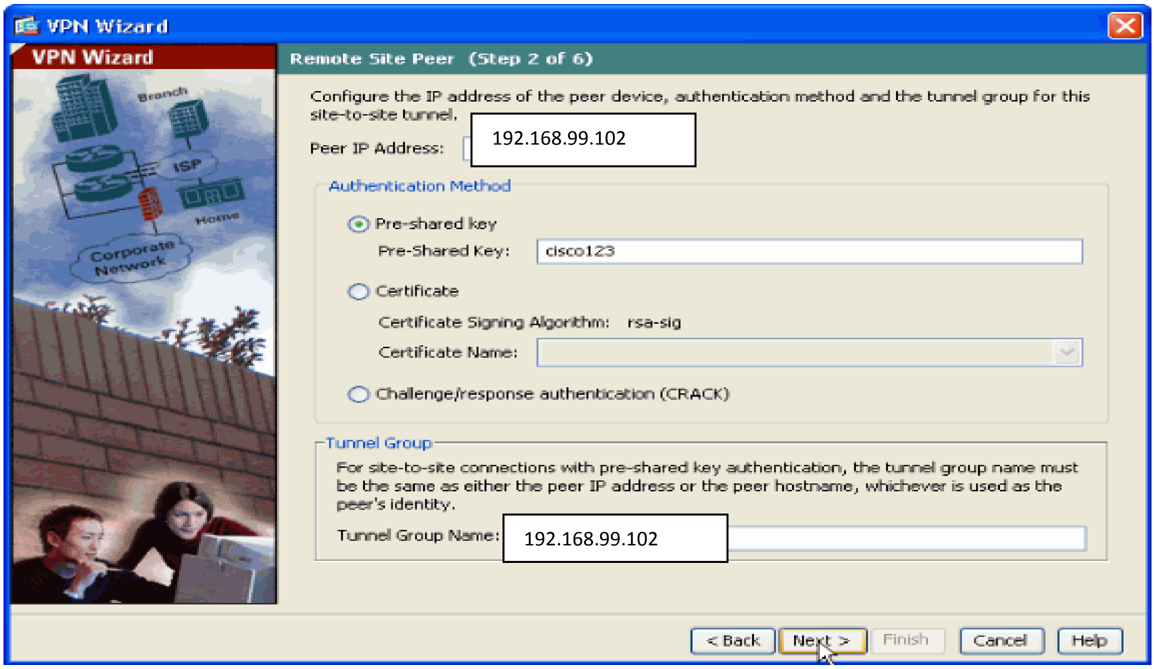
● Site-to-Site

○ Remote Access

VPN Tunnel Interface: outside

☑ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

7. Specify the outside IP address of the remote peer. Enter the authentication information to use, which is the pre–shared key in this example. The pre–shared key used in this example is *key123*. The Tunnel Group Name will be your outside IP address by default if you configure L2L VPN. Click **Next**.



Remote Site Peer (Step 2 of 6)

Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel.

Peer IP Address: 192.168.99.102

Authentication Method

● Pre-shared key

Pre-Shared Key: cisco123

○ Certificate

Certificate Signing Algorithm: rsa-sig

Certificate Name:

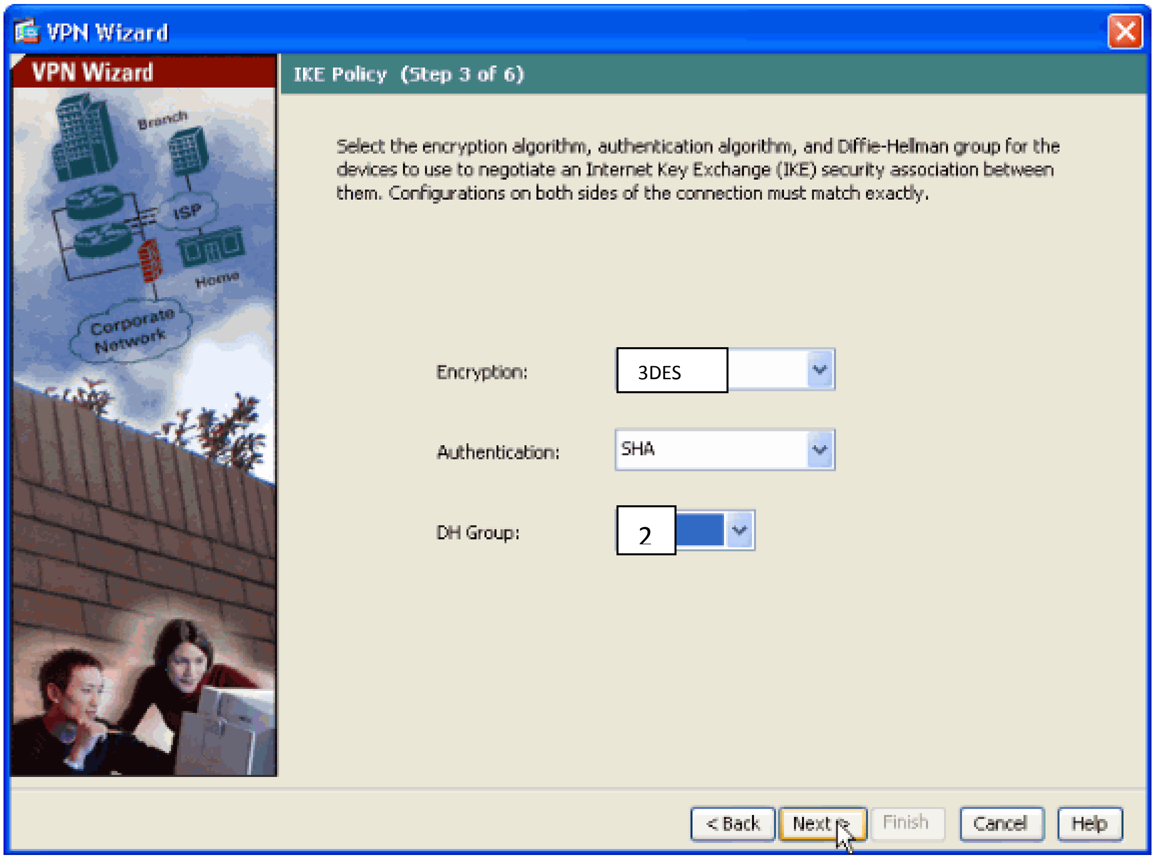
○ Challenge/response authentication (CRACK)

Tunnel Group

For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.

Tunnel Group Name: 192.168.99.102

8. Specify the attributes to use for IKE, also known as Phase 1. These attributes must be the same on both the ASA and the IOS Router. Click **Next**.



IKE Policy (Step 3 of 6)

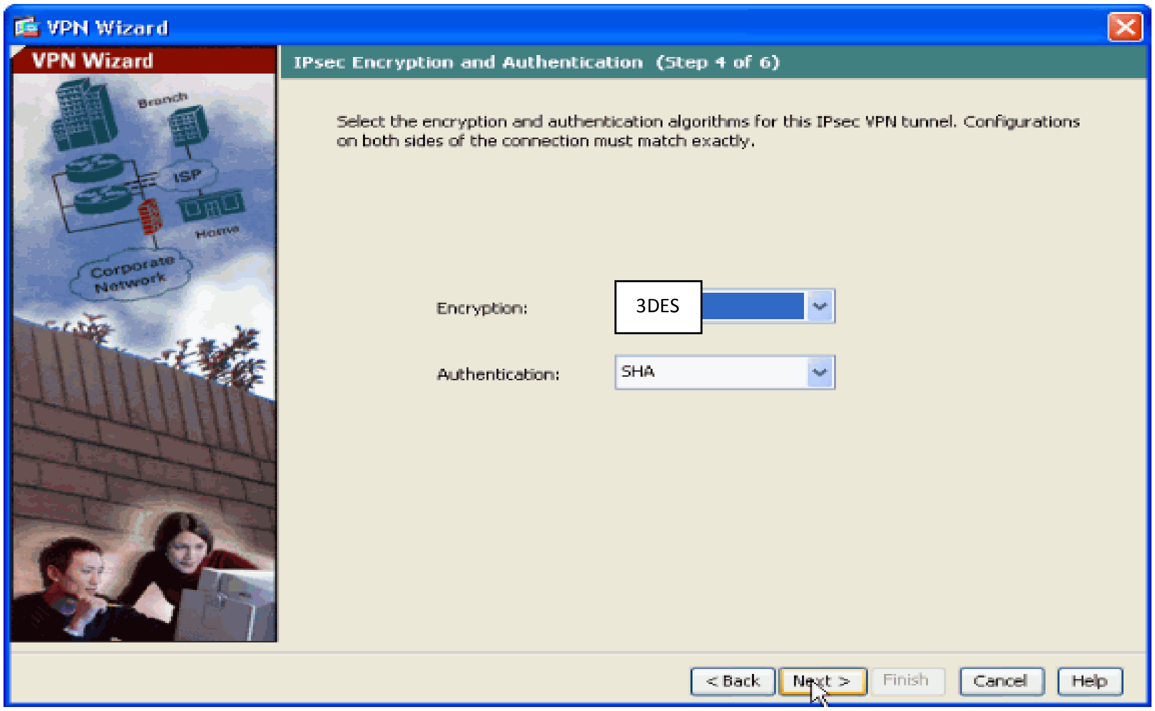
Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

DH Group: 2

9. Specify the attributes to use for IPsec, also known as Phase 2. These attributes must match on both the ASA and the IOS Router. Click **Next**.



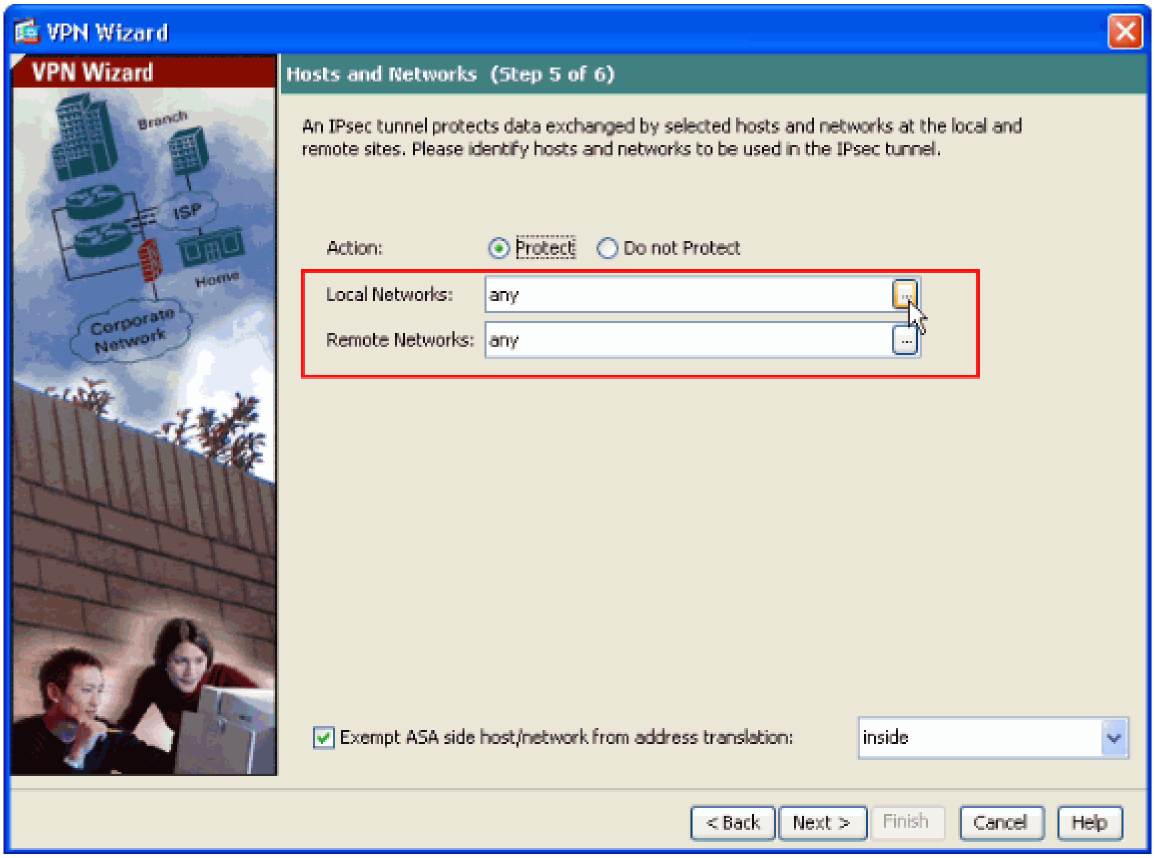
IPsec Encryption and Authentication (Step 4 of 6)

Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

10. Specify the hosts whose traffic should be allowed to pass through the VPN tunnel. In this step, you have to provide the Local Networks and Remote Networks for the VPN Tunnel. Click the button next to **Local Networks** as shown here to choose the local network address from the drop−down menu.



Hosts and Networks (Step 5 of 6)

An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.

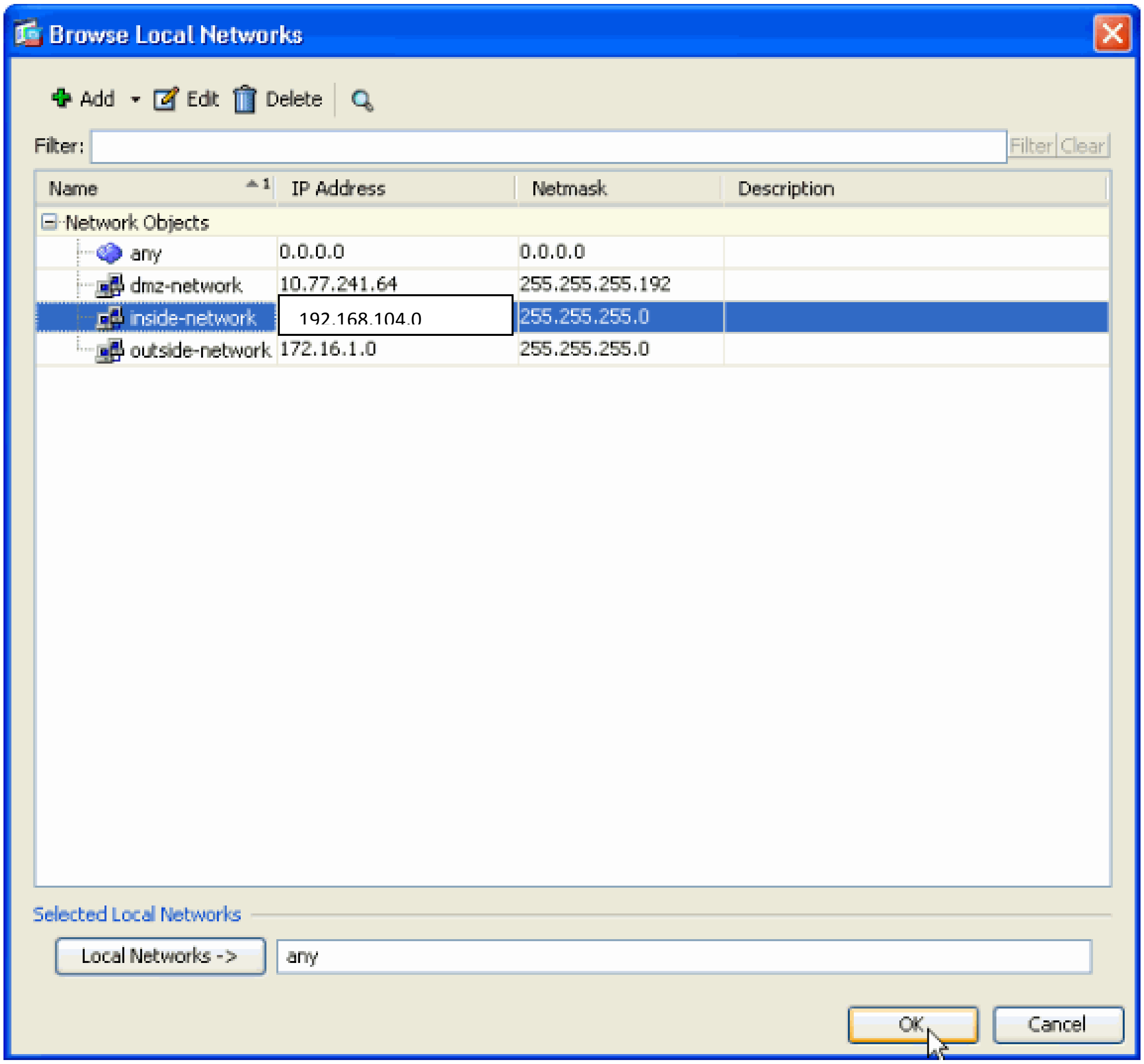
Action: ● Protect ○ Do not Protect

Local Networks: any

Remote Networks: any

☑ Exempt ASA side host/network from address translation: inside

11. Choose the **Local Network** address, and click **OK**.



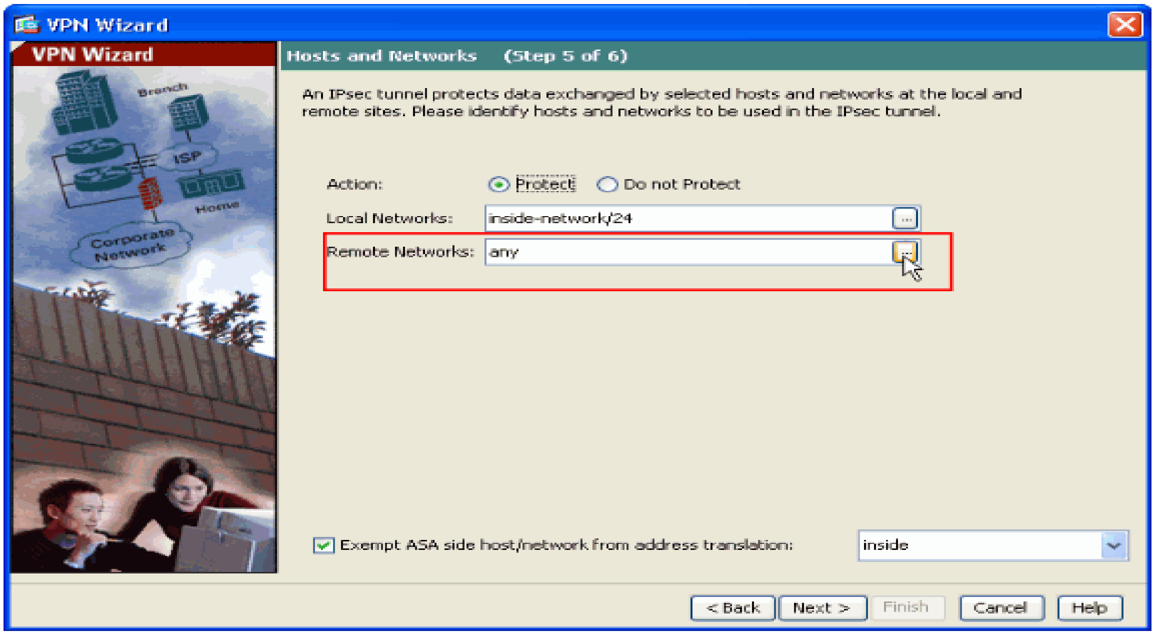
Filter:

Name	IP Address	Netmask	Description
Network Objects			
any	0.0.0.0	0.0.0.0	
dmz-network	10.77.241.64	255.255.255.192	
inside-network	192.168.104.0	255.255.255.0	
outside-network	172.16.1.0	255.255.255.0	

Selected Local Networks

Local Networks -> any

12. Click the button next to **Remote Networks** in order to choose the remote network address from the drop−down menu.



Hosts and Networks (Step 5 of 6)

An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.

Action: ● Protect ○ Do not Protect

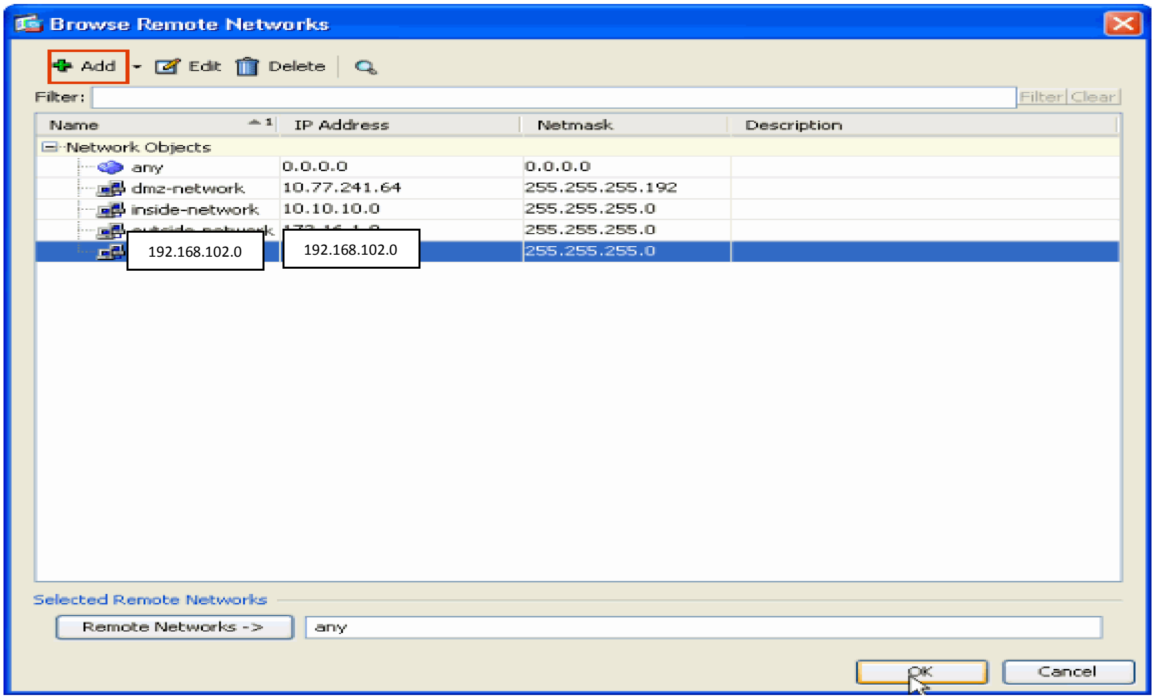
Local Networks: inside-network/24

Remote Networks: any

☑ Exempt ASA side host/network from address translation: inside

13. Choose the **Remote Network** address, and click **OK**.

Note: If you do not have the Remote Network in the list, then the network has to be added to the list. Click **Add** in order to do so.

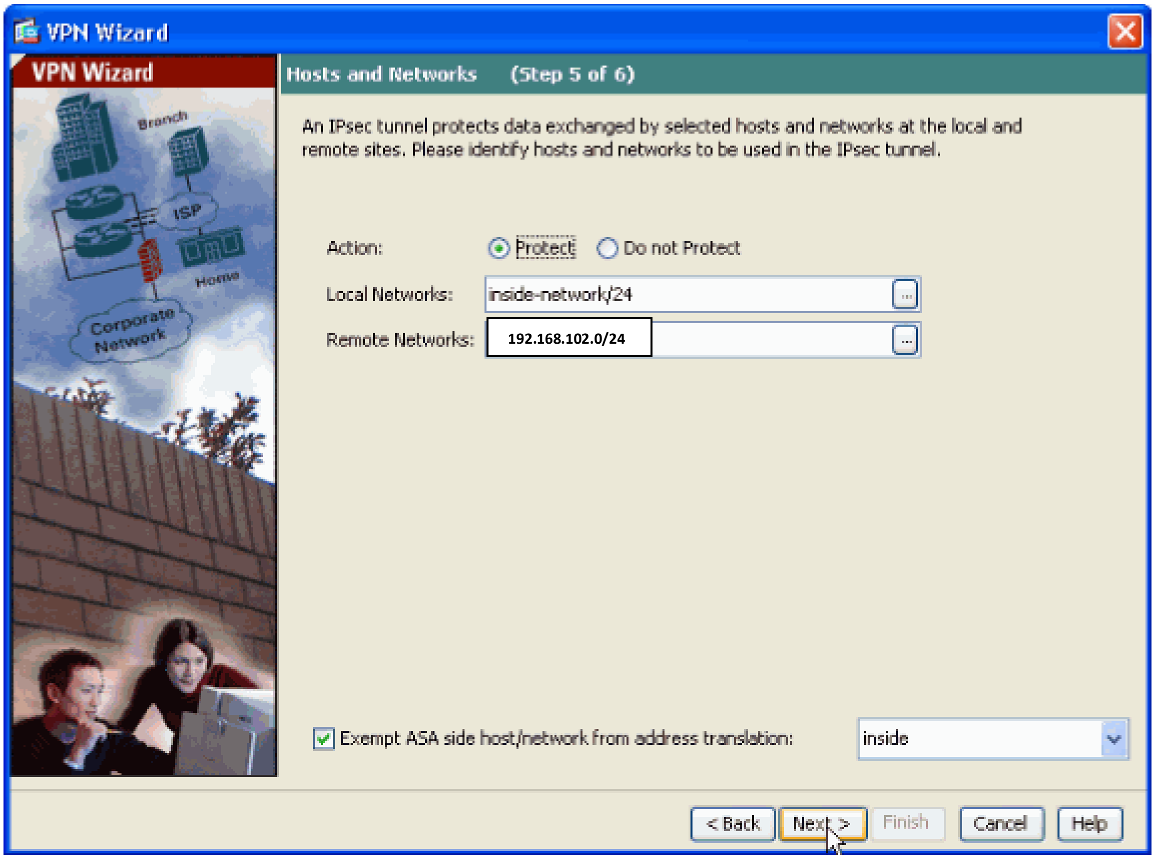


Name	IP Address	Netmask	Description
Network Objects			
any	0.0.0.0	0.0.0.0	
dmz-network	10.77.241.64	255.255.255.192	
inside-network	10.10.10.0	255.255.255.0	
outside-network	172.16.1.0	255.255.255.0	
192.168.102.0	192.168.102.0	255.255.255.0	

Selected Remote Networks

Remote Networks -> any

14. Check the **Exempt ASA side host/network from address translation** checkbox in order to prevent the tunnel traffic from undergoing Network Address Translation. Click **Next**.



Hosts and Networks (Step 5 of 6)

An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.

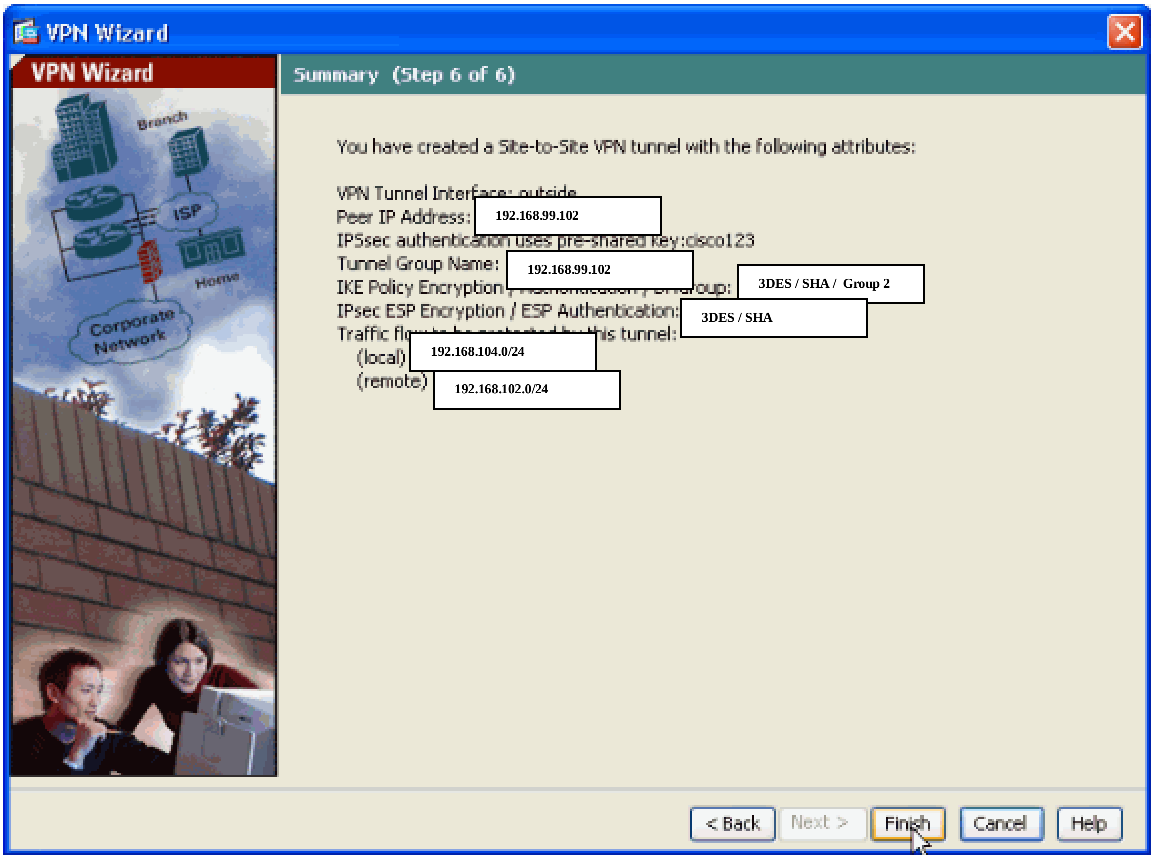
Action: ● Protect ○ Do not Protect

Local Networks: inside-network/24

Remote Networks: 192.168.102.0/24

☑ Exempt ASA side host/network from address translation: inside

15. The attributes defined by the VPN Wizard are displayed in this summary. Double check the configuration and click **Finish** when you are satisfied that the settings are correct.



Summary (Step 6 of 6)

You have created a Site-to-Site VPN tunnel with the following attributes:

VPN Tunnel Interface: outside
Peer IP Address: 192.168.99.102
IPSsec authentication uses pre-shared key:cisco123
Tunnel Group Name: 192.168.99.102
IKE Policy Encryption / Authentication / DH Group: 3DES / SHA / Group 2
IPsec ESP Encryption / ESP Authentication: 3DES / SHA
Traffic flow to be protected by this tunnel:
(local) 192.168.104.0/24
(remote) 192.168.102.0/24

->The End <-

Prepared by **Md. Nurain Akram**
nurain.akram@gmail.com