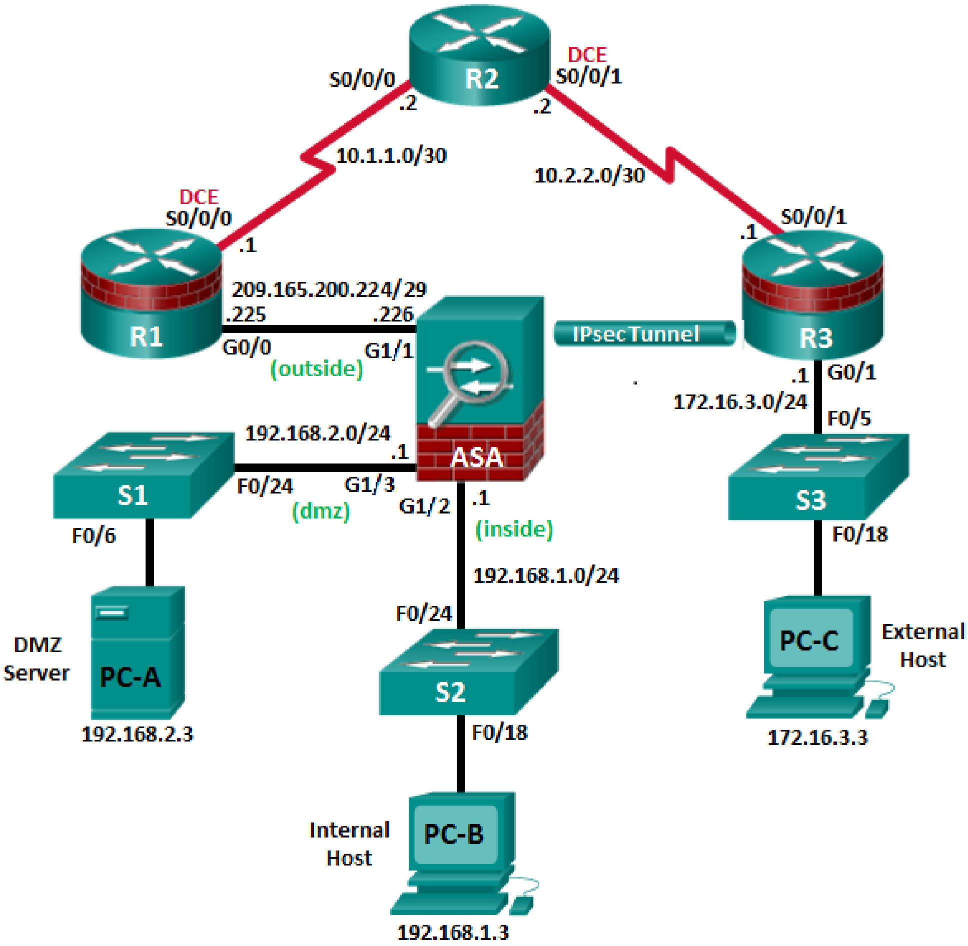
CCNA Security

Chapter 10 – Configure a Site-to-Site IPsec VPN between an ISR CLI and an ASA ASDM

This lab has been updated for use on NETLAB+

Topology



Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA G1/1
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	G1/2	192.168.1.1	255.255.255.0	NA	S2 Fa0/24
	G1/1	209.165.200.226	255.255.255.248	NA	R1 F0/0
	G1/3	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Basic Router/Switch/PC Configuration

- Configure basic settings for routers.
- Configure PC host IP settings.
- Verify connectivity.
- Save the basic running configuration for each router and switch.

Part 2: Accessing the ASA Console and ASDM

- Access the ASA console.
- Clear the previous ASA configuration settings.
- Bypass Setup mode.
- Use the CLI command script to configure the ASA.
- Verify HTTP ASDM access.

Part 3: Configuring the ISR as a Site-to-Site IPsec VPN Endpoint Using the CLI

- Configure basic VPN connection information settings.
- Specify IKE policy parameters.
- Configure a transform set.
- Specify traffic to protect.
- Review the summary of the configuration.
- Review the site-to-site VPN tunnel configuration.

Part 4: Configuring the ASA as a Site-to-Site IPsec VPN Endpoint Using ASDM

- Access ASDM.
- Review the ASDM Home screen.
- Start the VPN wizard.
- Configure peer device identification.
- Specify the traffic to protect.
- Configure authentication.
- Configure miscellaneous settings.
- Review the configuration summary and deliver the commands to the ASA.
- Verify the ASDM VPN connection profile.
- Test the VPN configuration from R3.
- Use ASDM monitoring to verify the tunnel.

Background/Scenario

In addition to acting as a remote access VPN concentrator, the ASA can provide site-to-site IPsec VPN tunneling. The tunnel can be configured between two ASAs or between an ASA and another IPsec VPN-capable device, such as an ISR, as is the case with this lab.

Your company has two locations connected to an ISP. R1 represents a customer-premise equipment (CPE) device managed by the ISP. R2 represents an intermediate Internet router. R3 connects users at the remote branch office to the ISP. The ASA is an edge security device that connects the internal corporate network and DMZ to the ISP while providing NAT services to inside hosts.

Management has asked you to provide a dedicated site-to-site IPsec VPN tunnel between the ISR router at the remote branch office and the ASA device at the corporate site. This tunnel will protect traffic between the branch office LAN and the corporate LAN, as it passes through the Internet. The site-to-site VPN does not require a VPN client on the remote or corporate site host computers. Traffic from either LAN to other Internet destinations is routed by the ISP and is not protected by the VPN tunnel. The VPN tunnel will pass through R1 and R2; both routers are not aware of the tunnel’s existence.

In Part 1 of this lab, you will configure the topology and non-ASA devices. In Part 2, you will prepare the ASA for ASDM access. In Part 3, you will use the CLI to configure the R3 ISR as a site-to-site IPsec VPN endpoint. In Part 4, you will configure the ASA as a site-to-site IPsec VPN endpoint using the ASDM VPN wizard.

Note: The router commands and output in this lab are from a Cisco 1941 router with Cisco IOS Release 15.4(3)M2 (with a Security Technology Package license). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5506 with an 8-port integrated router, running OS version 9.8(1), Adaptive Security Device Manager (ASDM) version 7.8(1), and comes with a Base license.

Part 1: Basic Router/Switch/PC Configuration

In Part 1, you will configure basic settings on the routers, such as interface IP addresses and static routing.

Note: Do not configure any ASA settings at this time.

Step 1: Configure R1 using the CLI script.

In this step, you will use the following CLI script to configure basic settings on R1. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

Note: Passwords in this task are set to a minimum of 10 characters and are relatively simple for the purposes of performing the lab. More complex passwords are recommended in a production network.

```
enable
config t
hostname R1
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/0
 ip address 209.165.200.225 255.255.255.248
 no shut
exit
int serial 0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
crypto key generate rsa general-keys modulus 1024
```

Step 2: Configure R2 using the CLI script.

In this step, you will use the following CLI script to configure basic settings on R2. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

```
enable
config t
hostname R2
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface serial 0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
exit
interface serial 0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 209.165.200.224 255.255.255.248 Serial0/0/0
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

Step 3: Configure R3 using the CLI script.

In this step, you will use the following CLI script to configure basic settings on R3. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

```
enable
config t
hostname R3
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/1
 ip address 172.16.3.1 255.255.255.0
 no shut
exit
int serial 0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP Addressing table.

Step 5: Verify connectivity.

Because the ASA is the focal point for the network zones, and it has not yet been configured, there will be no connectivity between devices that are connected to it. However, PC-C should be able to ping the R1 interface G0/0. From PC-C, ping the R1 G0/0 IP address (**209.165.200.225**). If these pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-C to R1 G0/0 and S0/0/0, you have demonstrated that static routing is configured and functioning correctly.

Save the **running configuration** for each router.

Part 2: Accessing the ASA Console and ASDM

Step 1: Clear the previous ASA configuration settings.

a. Use the **write erase** command to remove the **startup-config** file from flash memory.

   Note: The **erase startup-config** IOS command is not supported on the ASA.

b. Use the **reload** command to restart the ASA. This causes the ASA to display in CLI Setup mode. If you see the **System config has been modified. Save? [Y]es/[N]o:** message, type **N**, and press **Enter**.

Step 2: Bypass Setup mode.

When the ASA completes the reload process, it should detect that the startup configuration file is missing and go into Setup mode. If it does go into Setup mode, repeat Step 1.

a. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with **No**.

b. Enter privileged EXEC mode with the **enable** command. The password should be kept blank (no password).

Step 3: Configure the ASA by using the CLI script.

In this step, you will use a CLI script to configure basic settings, the firewall, and the DMZ.

a. Use the **show run** command to confirm that there is no previous configuration in the ASA other than the defaults that the ASA automatically inserts.

b. Enter global configuration mode. When prompted to enable anonymous call-home reporting, respond **no**.

c. Copy and paste the Pre-VPN Configuration Script commands listed below to start configuring the SSL VPNs.

d. Observe the messages as the commands are applied to ensure that there are no warnings or errors. If prompted to replace the RSA key pair, respond **yes**.

```
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password cisco12345
!
interface Gi1/1
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
 no shut
!
interface gi1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shut
!
interface gi1/3
nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
 no shut
!
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
object network dmz-server
 host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
!
object network inside-net
 nat (inside,outside) dynamic interface
!
object network dmz-server
 nat (dmz,outside) static 209.165.200.227
!
access-group OUTSIDE-DMZ in interface outside
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
username admin01 password admin01pass
!
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
!
http server enable
http 192.168.1.0 255.255.255.0 inside
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 10
!
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
   inspect icmp
!
crypto key generate rsa modulus 1024
```

e. At the privileged EXEC mode prompt, issue the **write mem** (or **copy run start**) command to save the running configuration to the startup configuration and the RSA keys to non-volatile memory.

Part 3: Configuring the ISR as a Site-to-Site IPsec VPN Endpoint Using the CLI

In Part 3 of this lab, you will configure R3 as an IPsec VPN endpoint for the tunnel between R3 and the ASA. R1 and R2 are unaware of the tunnel.

Step 1: Verify connectivity from the R3 LAN to the ASA.

In this step, you will verify that PC-C on the R3 LAN can ping the ASA outside interface.

Ping the ASA IP address of **209.165.200.226** from PC-C.

```
PC-C:\> ping 209.165.200.226
```

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Step 2: Enable IKE policies on R3.

IPsec is an open framework that allows for the exchange of security protocols as new technologies and encryption algorithms are developed.

There are two central configuration elements in the implementation of an IPsec VPN:

- Implement Internet Key Exchange (IKE) parameters.
- Implement IPsec parameters.

a. Verify that IKE is supported and enabled.

IKE Phase 1 defines the key exchange method used to pass and validate IKE policies between peers. In IKE Phase 2, the peers exchange and match IPsec policies for the authentication and encryption of data traffic.

IKE must be enabled for IPsec to function. IKE is enabled, by default, on IOS images with cryptographic feature sets. If it is disabled, you can enable it with the **crypto isakmp enable** command. Use this command to verify that the router IOS supports IKE and that it is enabled.

```
R3(config)# crypto isakmp enable
```

Note: If you cannot execute this command on the router, you must upgrade to an IOS image that includes the Cisco cryptographic services.

b. Establish an ISAKMP policy and view the available options.

To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms, and the hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later.

Issue the **crypto isakmp** *policy number* global configuration mode command on R1 for policy 10.

```
R1(config)# crypto isakmp policy 10
```

c. View the various IKE parameters available using Cisco IOS help by typing a question mark (**?**).

```
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Step 3: Configure ISAKMP policy parameters on R3.

The encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, which ensures that the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was sent and signed by the remote peer. The Diffie-Hellman group is used to create a secret key shared by the peers that has not been sent across the network.

a. Configure an ISAKMP policy with a priority of **10**. Use **pre-shared key** as the authentication type, **3des** for the encryption algorithm, **sha** as the hash algorithm, and the Diffie-Hellman group **2** key exchange.

   Note: Older versions of Cisco IOS do not support AES 256 encryption and SHA as a hash algorithm. Substitute whatever encryption and hashing algorithm your router supports. Ensure that the same changes are made on R3 in order to be in sync.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 2
R3(config-isakmp)# end
```

b. Verify the IKE policy with the **show crypto isakmp policy** command.

```
R3# show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
      encryption algorithm:   Three key triple DES
      hash algorithm:         Secure Hash Standard
      authentication method:  Pre-Shared Key
      Diffie-Hellman group:   #2 (1024 bit)
      lifetime:         86400 seconds, no volume limit
```

Step 4: Configure pre-shared keys.

Because pre-shared keys are used as the authentication method in the IKE policy, a key must be configured on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration mode **crypto isakmp key** *key-string* **address** *ip-address* command is used to enter a pre-shared key. Use the IP address of the remote peer. The IP address is the remote interface that the peer would use to route traffic to the local router.

Which IP address should you use to configure the IKE peer, given the topology diagram and IP addressing table?

____

____

____

a. Each IP address that is used to configure the IKE peers is also referred to as the IP address of the remote VPN endpoint. Configure the pre-shared key of **SECRET-KEY** on R3. Production networks should use a complex key. This command points to the remote ASA outside IP address.

```
R3(config)# crypto isakmp key SECRET-KEY address 209.165.200.226
```

Step 5: Configure the IPsec transform set and lifetime.

a. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. It is configured using the **crypto ipsec transform-set** *tag* global configuration command. Configure the transform set with the tag **ESP-TUNNEL**. Use **?** to see which parameters are available.

```
R3(config)# crypto ipsec transform-set ESP-TUNNEL ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform on R3
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
```

b. In our Site-to-site VPN with the ASA, we will use the two highlitghed parameters. Complete the command by entering the two highlighted parameters.

```
R3(config)# crypto ipsec transform-set ESP-TUNNEL esp-3des esp-sha-hmac
```

What is the function of the IPsec transform set?

____

____

____

____

Step 6: Define interesting traffic.

To make use of the IPsec encryption with the VPN, it is necessary to define extended access lists to tell the router which traffic to encrypt. A packet that is permitted by an access list used for defining IPsec traffic is encrypted if the IPsec session is configured correctly. A packet that is denied by one of these access lists is not dropped. The packet is sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which means the default action is to not encrypt traffic. If there is no IPsec security association correctly configured, no traffic is encrypted and traffic is forwarded unencrypted.

In this scenario, from the perspective of R3, the traffic you want to encrypt is traffic going from R3's Ethernet LAN to the ASA inside LAN or vice versa from the perspective of the ASA.

a. Configure the IPsec VPN interesting traffic ACL on R3.

```
R3(config)# ip access-list extended VPN-ACL
R3(config-ext-nacl)# remark Link to the CCNAS-ASA
R3(config-ext-nacl)# permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config-ext-nacl)# exit
```

Does IPsec evaluate whether the access lists are mirrored as a requirement to negotiate its security association?

____

____

____

Step 7: Create and apply a crypto map.

A crypto map associates traffic that matches an access list to a peer and various IKE and IPsec settings. After the crypto map is created, it can be applied to one or more interfaces. The interfaces that it is applied to should be the interfaces facing the IPsec peer.

To create a crypto map, use the **crypto map** *name sequence-num type* global configuration command to enter crypto map configuration mode for that sequence number. Multiple crypto map statements can belong to the same crypto map and are evaluated in ascending numerical order.

a. Create the crypto map on R3, name it **S2S-MAP**, and use **10** as the sequence number. Use a type of **ipsec-isakmp**, which means IKE is used to establish IPsec security associations. A message displays after the command is issued.

```
R3(config)# crypto map S2S-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
R3(config-crypto-map)#
```

b. Use the **match address** *access-list* command to specify which access list defines which traffic to encrypt.

```
R3(config-crypto-map)# match address VPN-ACL
```

c. Setting a peer IP or hostname is required. Set it to the ASA remote VPN endpoint interface using the following command.

```
R3(config-crypto-map)# set peer 209.165.200.226
```

d. Use the **set transform-set** *tag* command to hard code the transform set to be used with this peer.

```
R3(config-crypto-map)# set transform-set ESP-TUNNEL
R3(config-crypto-map)# exit
```

e. Apply the crypto map to interfaces.

Note: The SAs are not established until the crypto map has been activated by interesting traffic. The router generates a notification that crypto is now on.

Apply the crypto maps to the R3 Serial 0/0/1 interface.

```
R3(config)# interface Serial0/0/1
R3(config-if)# crypto map S2S-MAP
R3(config-if)# end
R3#
```

```
*Mar  9 06:23:03.863: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3#
```

Part 4: Configuring the ASA as a Site-to-Site IPsec VPN Endpoint Using ASDM

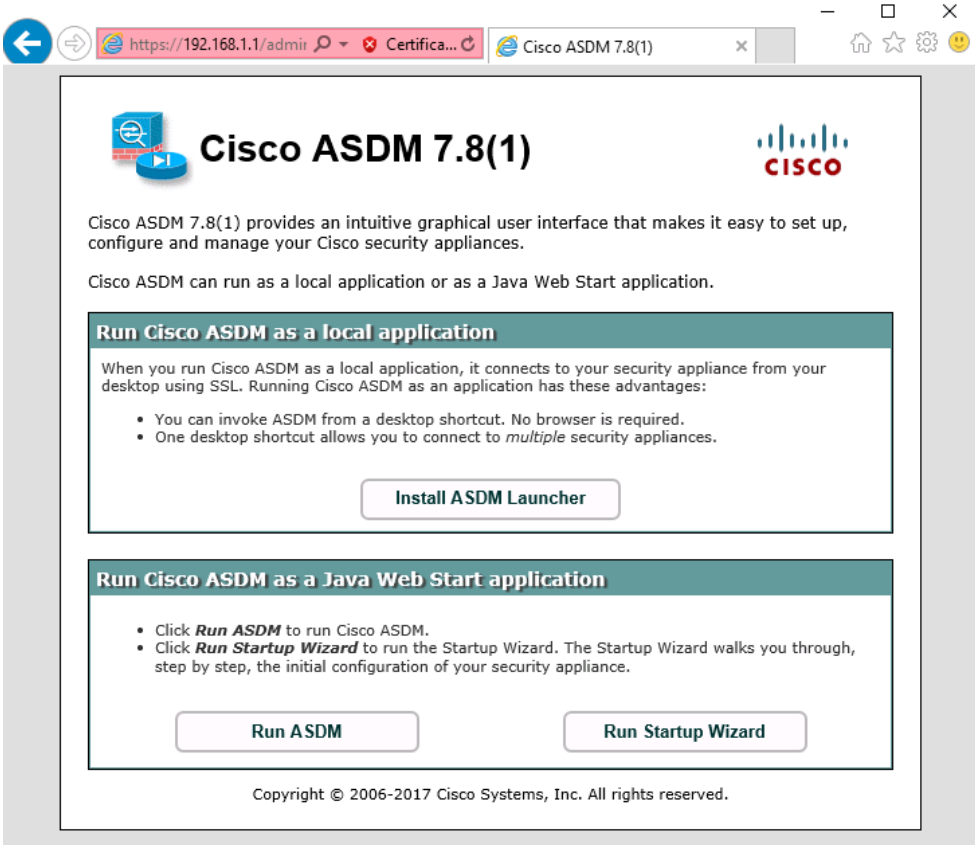
In Part 4 of this lab, you will configure the ASA as an IPsec VPN tunnel endpoint. The tunnel between the ASA and R3 passes through R1 and R2.

Step 1: Access ASDM.

a. Open a browser on PC-B and test the HTTPS access to the ASA by entering https://192.168.1.1. After entering the https://192.168.1.1 URL, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings.

   Note: Specify the HTTPS protocol in the URL.

b. At the ASDM welcome page, click **Run ASDM**. The ASDM-IDM Launcher will display. Log in as user **admin01** with the password **admin01pass**.



Cisco ASDM 7.8(1)

Cisco ASDM 7.8(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

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

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Install ASDM Launcher

Run Cisco ASDM as a Java Web Start application

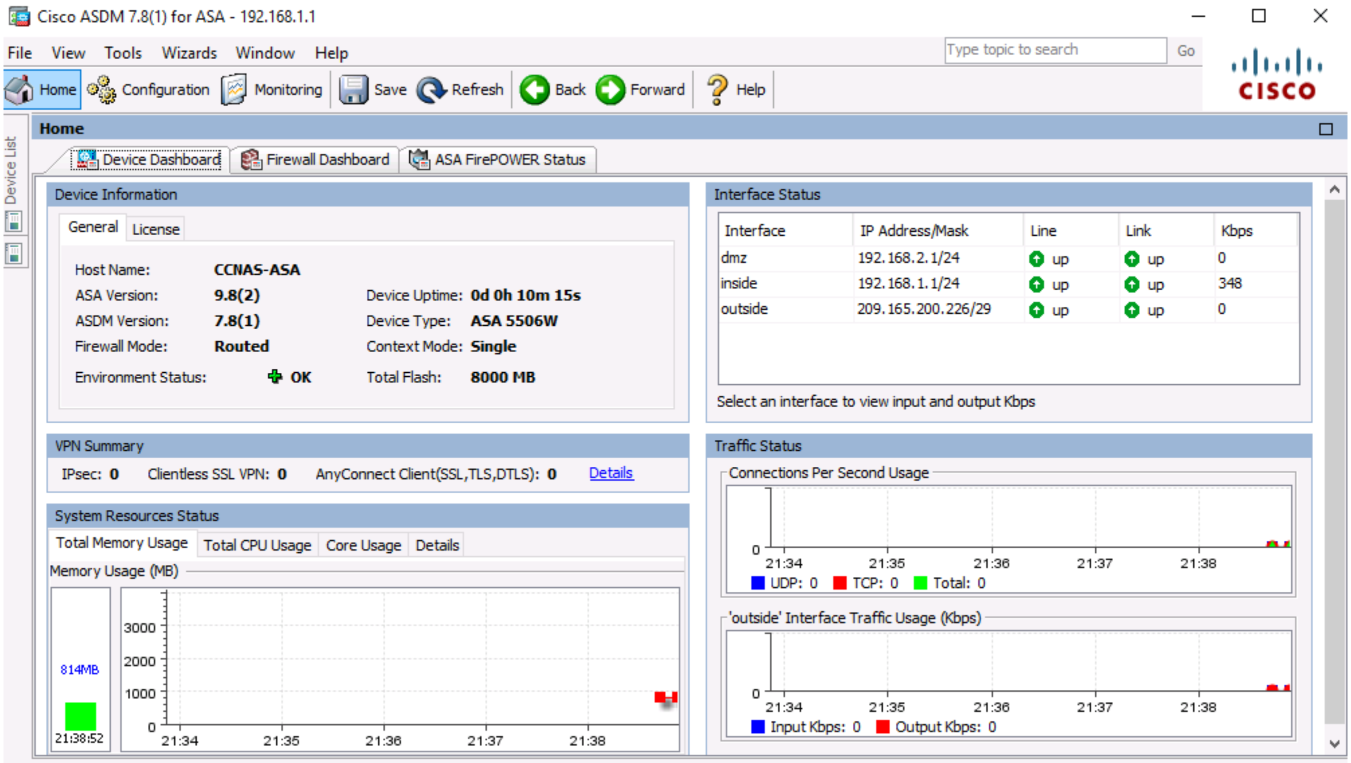
- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

Run ASDM   Run Startup Wizard

Copyright © 2006-2017 Cisco Systems, Inc. All rights reserved.

Step 2: Review the ASDM Home screen.

The Home screen displays and shows the current ASA device configuration and traffic flow statistics. Note the inside, outside, and dmz interfaces that were configured in Part 2 of this lab.



Cisco ASDM 7.8(1) 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
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
General License
Interface Status
VPN Summary
System Resources Status
Total Memory Usage Total CPU Usage Core Usage Details
Memory Usage (MB)
814MB
21:38:52
3000
2000
1000
0
21:34 21:35 21:36 21:37 21:38
Traffic Status
Connections Per Second Usage
'outside' Interface Traffic Usage (Kbps)

Host Name: CCNAS-ASA
ASA Version: 9.8(2)
ASDM Version: 7.8(1)
Firewall Mode: Routed
Environment Status: ✚ OK
Device Uptime: 0d 0h 10m 15s
Device Type: ASA 5506W
Context Mode: Single
Total Flash: 8000 MB

Interface	IP Address/Mask	Line	Link	Kbps
dmz	192.168.2.1/24	up	up	0
inside	192.168.1.1/24	up	up	348
outside	209.165.200.226/29	up	up	0

Select an interface to view input and output Kbps

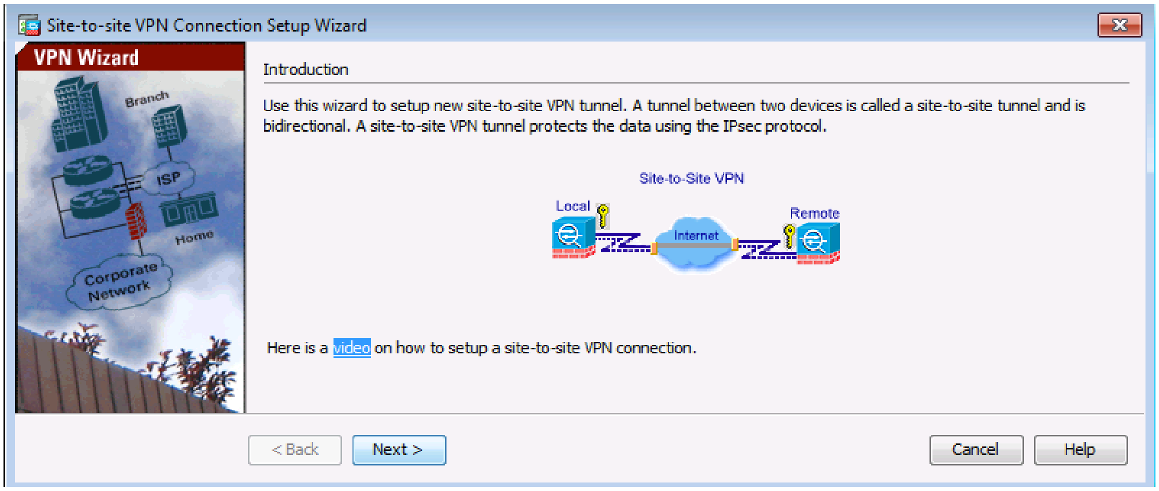
IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0 Details

UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

Step 3: Start the VPN wizard.

a. On the ASDM main menu, click **Wizards** > **VPN Wizards** > **Site-to-Site VPN Wizard** to open the Site-to-Site VPN Connection Setup Wizard Introduction window.



Introduction

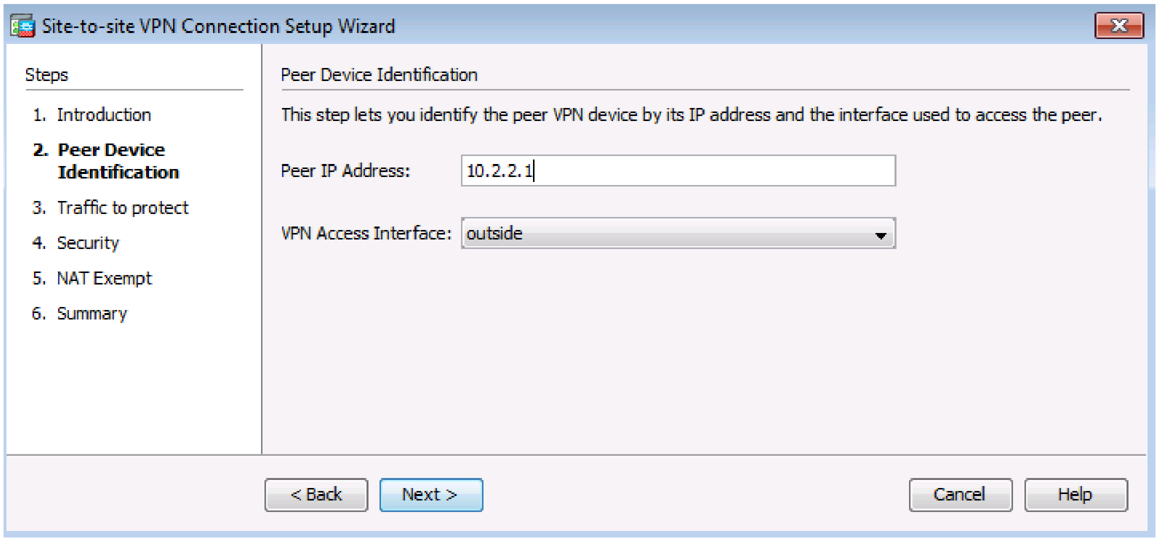
Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

Here is a video on how to setup a site-to-site VPN connection.

b. Review the on-screen text and topology diagram and click **Next** to continue.

Step 4: Configure peer device identification.

In the Peer Device Identification window, enter the IP address of the R3 Serial0/0/1 interface (**10.2.2.1**) as the Peer IP Address. Leave the default VPN Access Interface set to **outside**. The VPN tunnel will be between R3 S0/0/1 and the ASA outside interface (Gi1/1). Click **Next** to continue.



Peer Device Identification

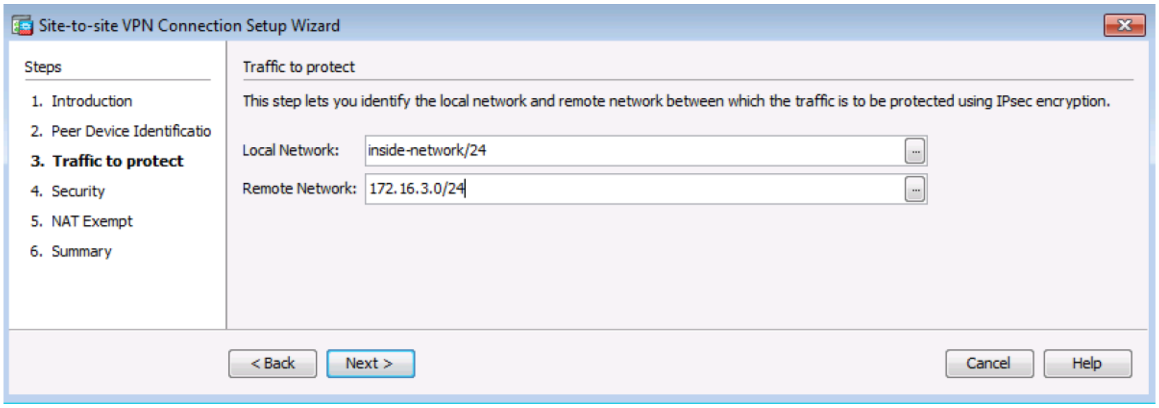
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 10.2.2.1

VPN Access Interface: outside

Step 5: Specify the traffic to protect.

In the Traffic to protect window, enter **inside-network/24** (192.168.1.0/24) as the Local Network and type**172.16.3.0/24** to add the R3 LAN as the Remote Network. Click **Next** to continue.



Traffic to protect

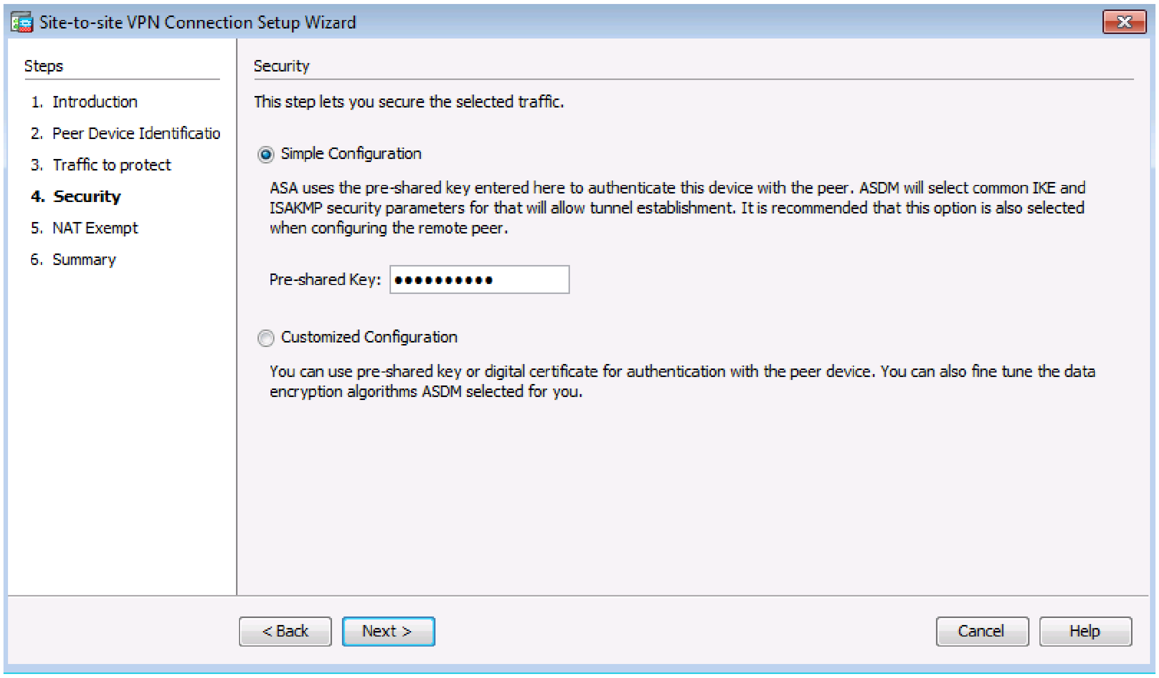
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

Local Network: inside-network/24

Remote Network: 172.16.3.0/24

Step 6: Configure authentication.

On the Security window, enter a pre-shared key of **SECRET-KEY**. You will not be using a device certificate. Click **Next** to continue.



Security

This step lets you secure the selected traffic.

● Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

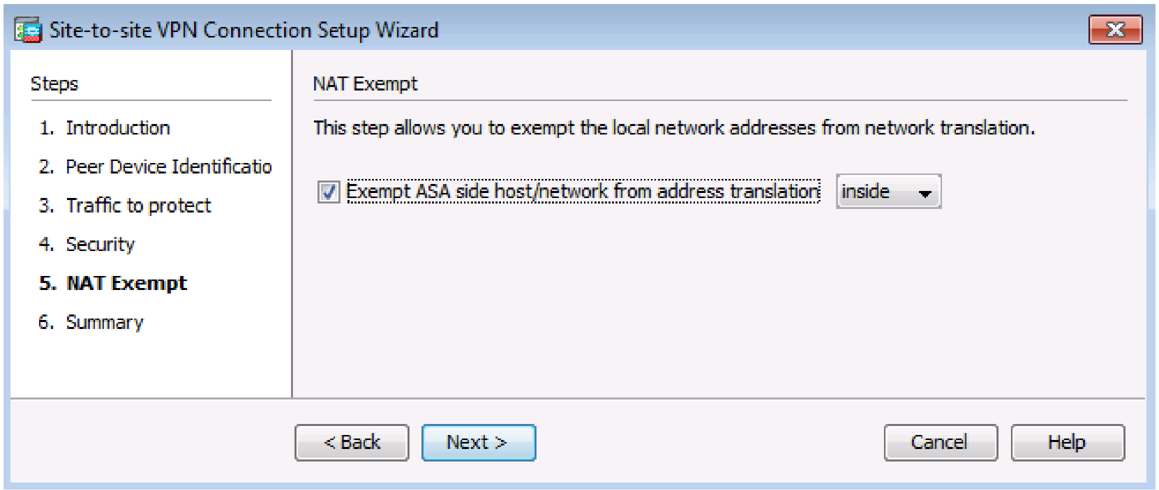
Pre-shared Key: ••••••••••

○ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

Step 7: Configure miscellaneous settings.

In the NAT Exempt window, click the **Exempt ASA** check box for the **inside** interface. Click **Next** to continue.



NAT Exempt

This step allows you to exempt the local network addresses from network translation.

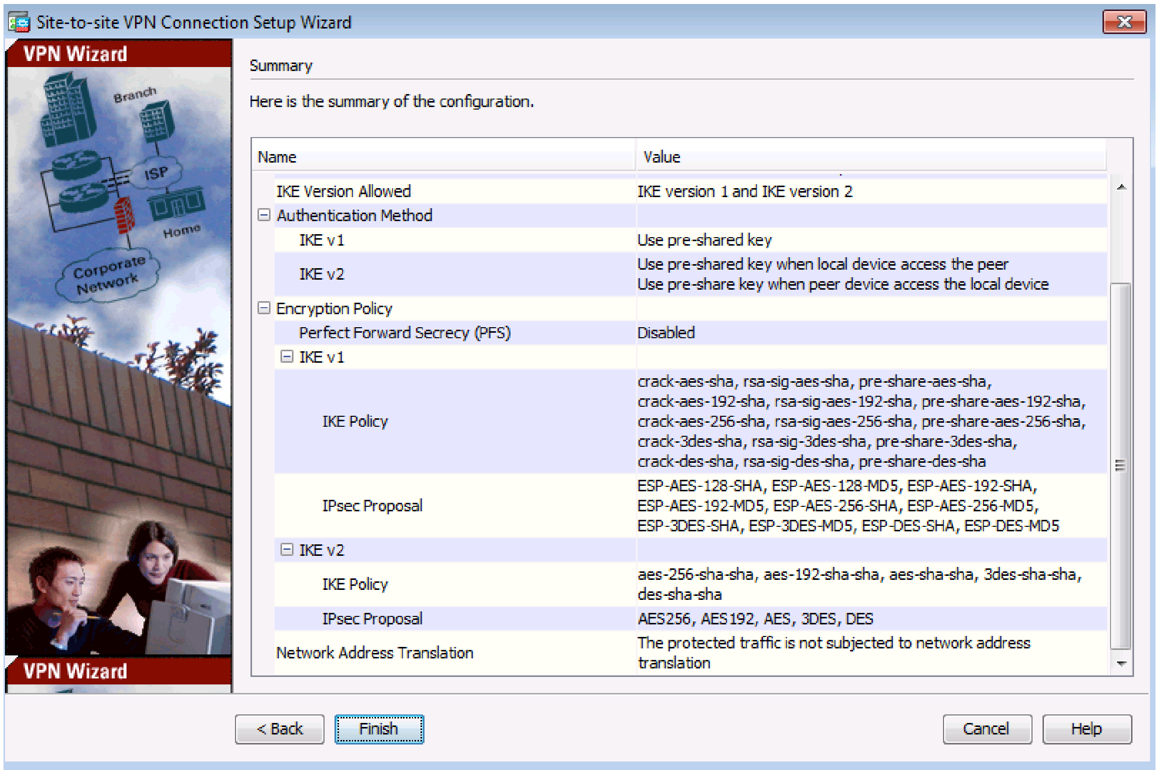
☑ Exempt ASA side host/network from address translation: inside

Step 8: Review the configuration summary and deliver the commands to the ASA.

The Summary page is displayed next. Verify that the information configured is correct. You can click **Back** to make changes, or click **Cancel** and restart the VPN wizard.

Click **Finish** to complete the process and deliver the commands to the ASA.

Note: If prompted to authenticate, log in again as **admin01** with the password **admin01pass**.



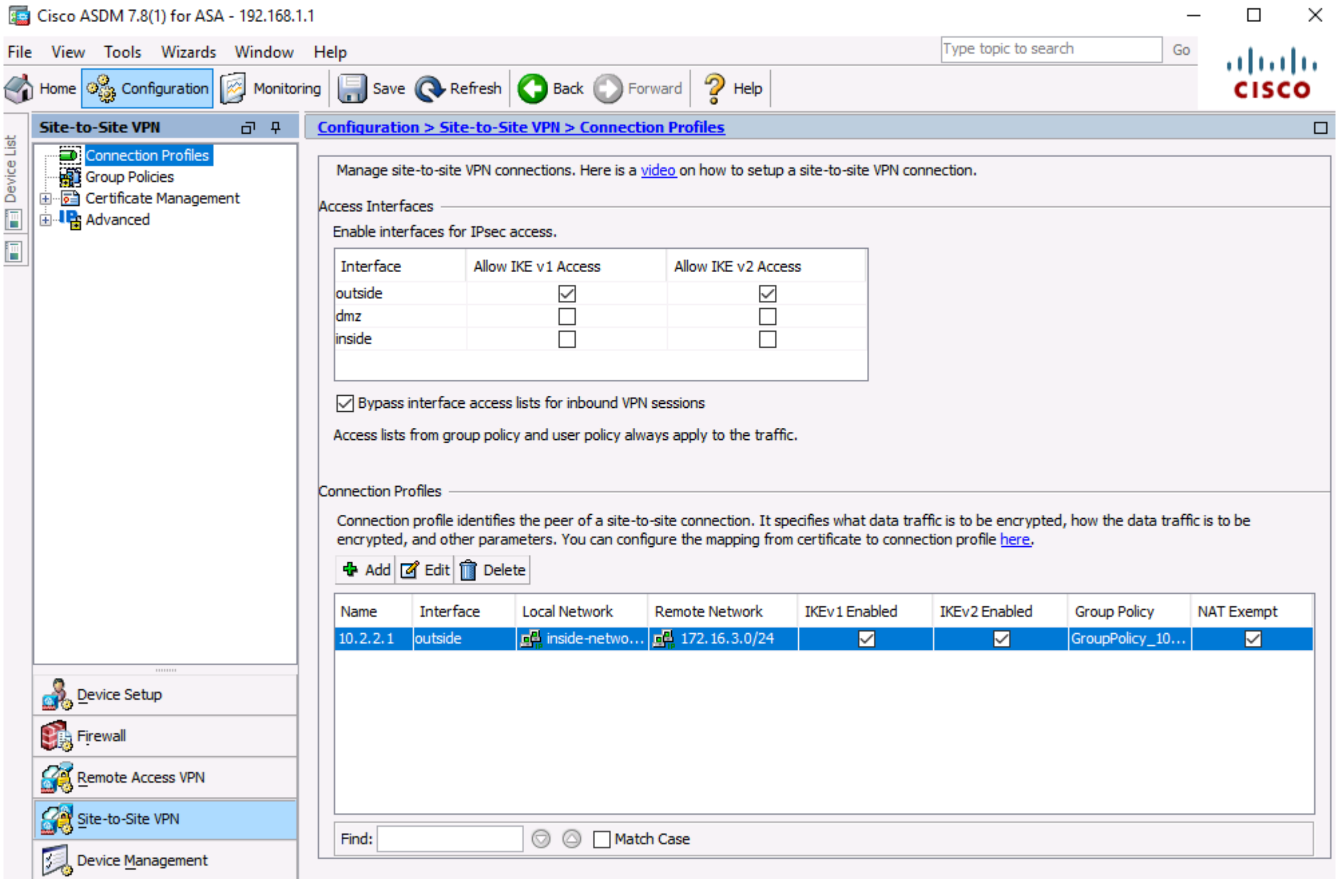
Summary

Here is the summary of the configuration.

Name	Value
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, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
⊟ IKE v2	
IKE Policy	aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Network Address Translation	The protected traffic is not subjected to network address translation

Step 9: Verify the ASDM VPN connection profile.

The ASDM **Configuration** > **Site-to-Site VPN** > **Connection Profiles** screen displays the settings you configured. From this window, the VPN configuration can be verified and edited.



Configuration > Site-to-Site VPN > Connection Profiles

Manage site-to-site VPN connections. Here is a video on how to setup a site-to-site VPN connection.

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	☑	☑
dmz	□	□
inside	□	□

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile here.

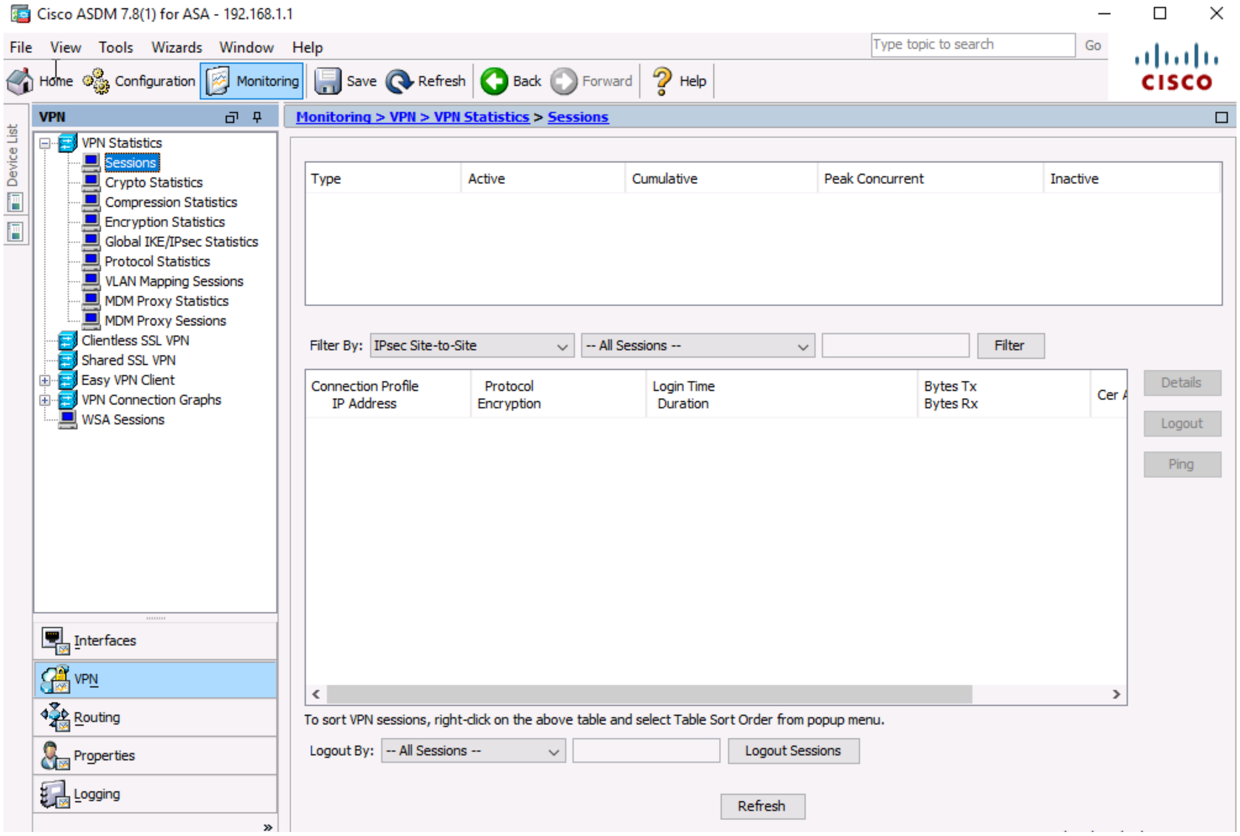
Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled	Group Policy	NAT Exempt
10.2.2.1	outside	inside-netwo...	172.16.3.0/24	☑	☑	GroupPolicy_10...	☑

Find: □ Match Case

Step 10: Use ASDM monitoring to verify the tunnel.

On the ASDM menu bar, click **Monitoring** > **VPN** from the panels at the lower left of the screen. Click **VPN Statistics** > **Sessions**. Notice how there is no active session. This is because the VPN tunnel has not been established.



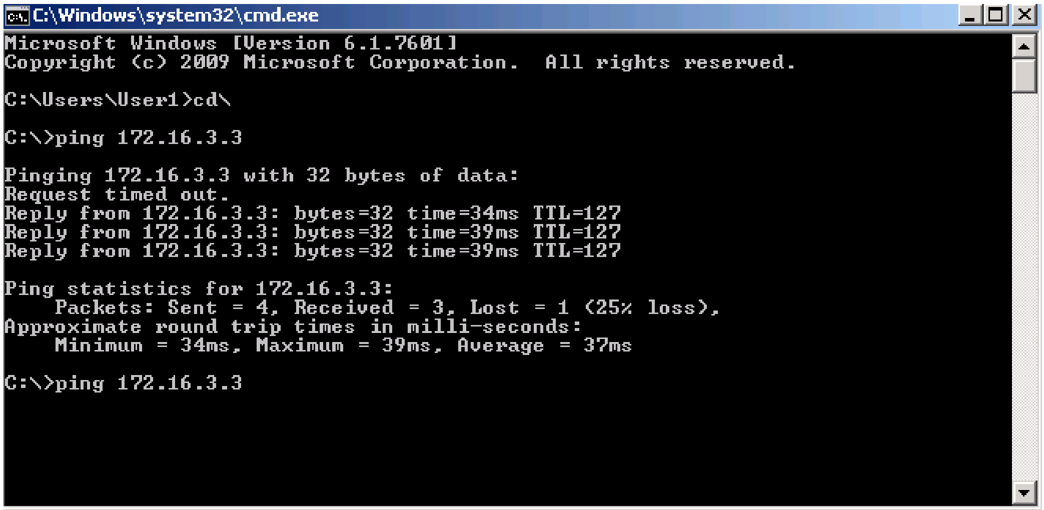
Filter By: IPsec Site-to-Site; -- All Sessions --

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Step 11: Test the VPN configuration from PC-B.

a. To establish the VPN tunnel, interesting traffic must be generated. From PC-B, ping PC-C.

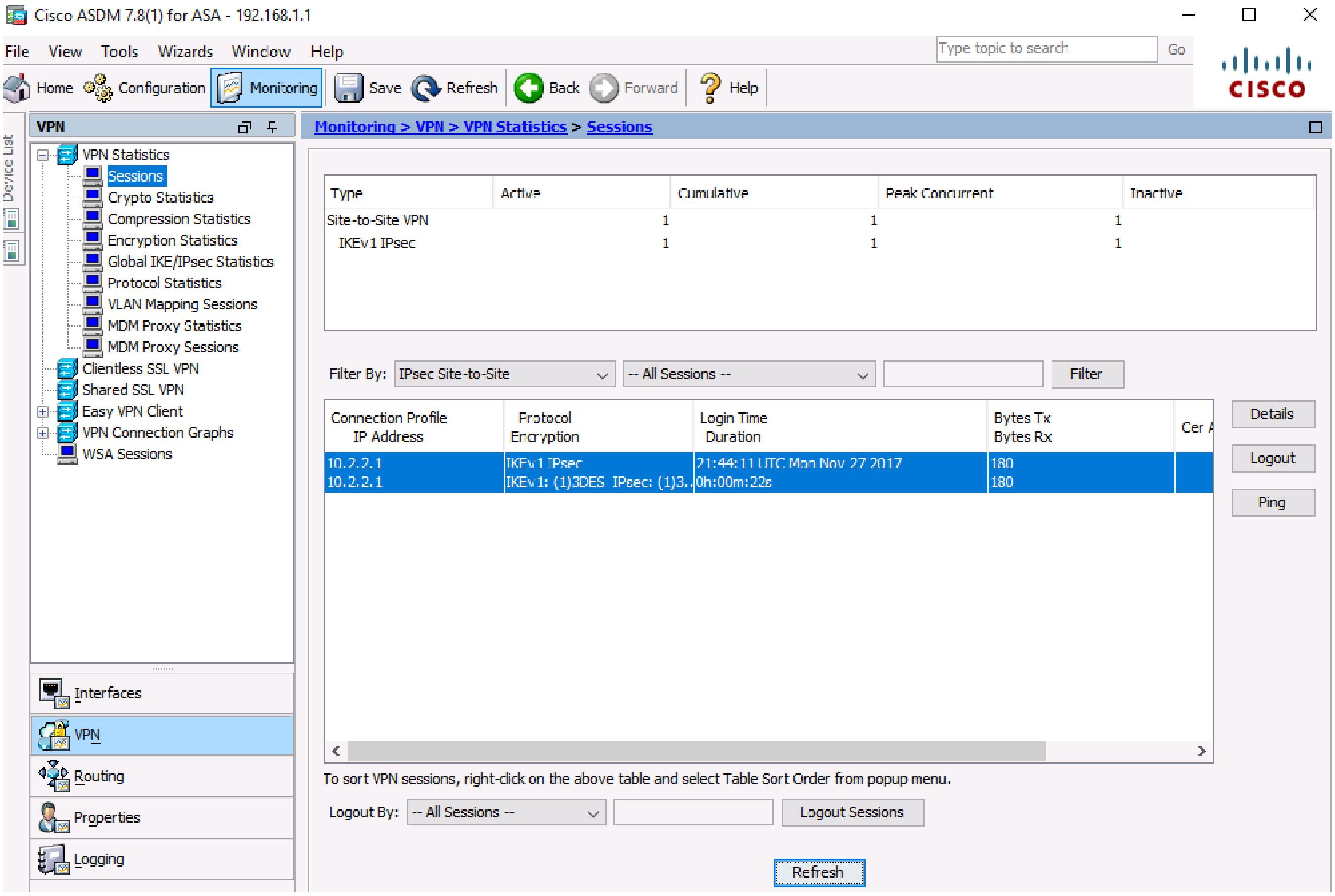


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User1>cd\

C:\>ping 172.16.3.3

Pinging 172.16.3.3 with 32 bytes of data:
Request timed out.
Reply from 172.16.3.3: bytes=32 time=34ms TTL=127
Reply from 172.16.3.3: bytes=32 time=39ms TTL=127
Reply from 172.16.3.3: bytes=32 time=39ms TTL=127

Ping statistics for 172.16.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 39ms, Average = 37ms

C:\>ping 172.16.3.3
```

b. This generates interesting traffic. Notice how two pings failed before being successful. This is because the tunnel first had to be negotiated and established before the ICMP packets could be successful.

c. The VPN information is now being displayed on the ASDM **Monitoring** > **VPN** > **VPN Statistics** > **Sessions** page.

Note: You may need to click **Refresh** before the statistics will display.



Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	1	1	
IKEv1 IPsec	1	1	1	

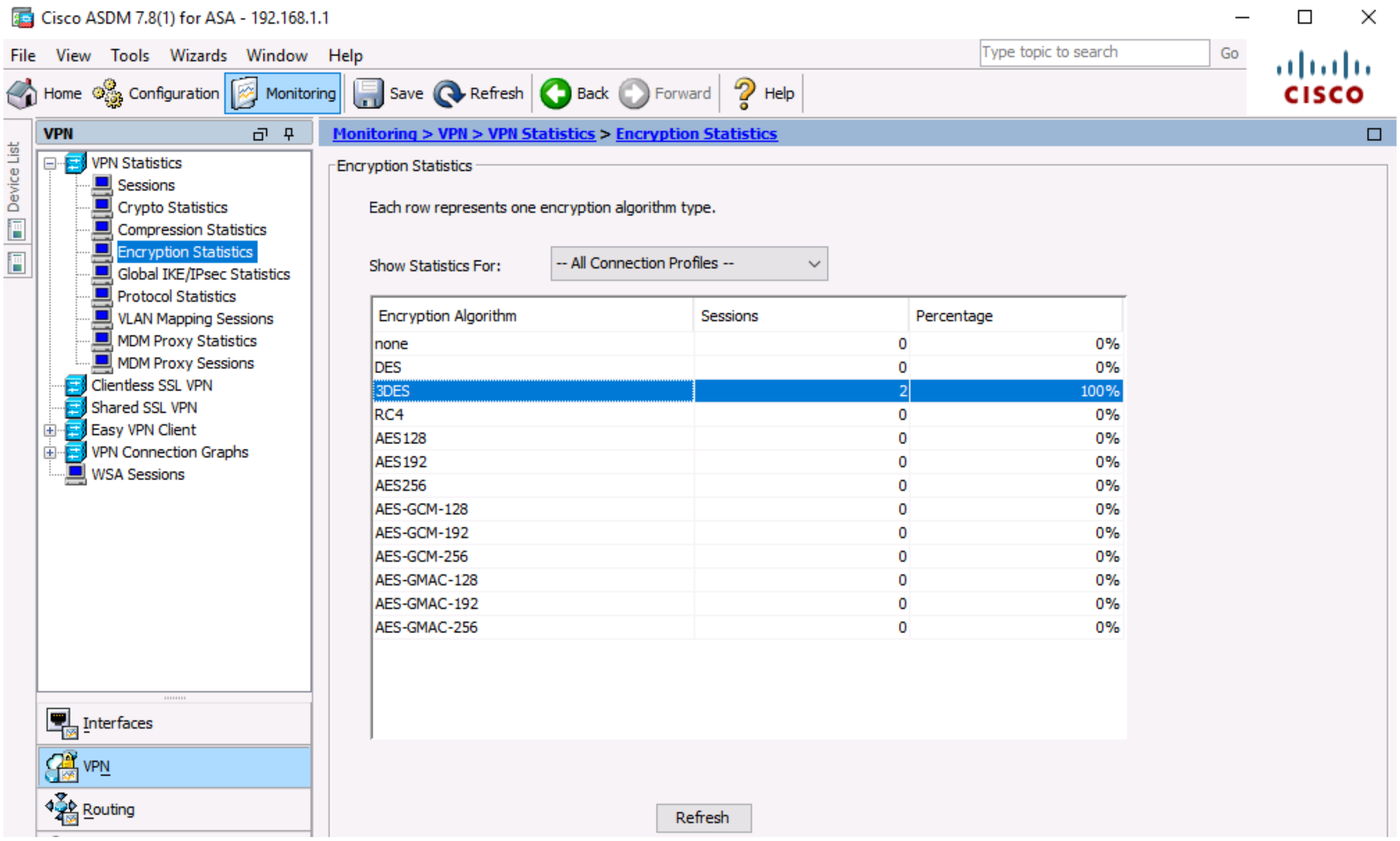
Filter By: IPsec Site-to-Site -- All Sessions --

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer
10.2.2.1 10.2.2.1	IKEv1 IPsec IKEv1: (1)3DES IPsec: (1)3..	21:44:11 UTC Mon Nov 27 2017 0h:00m:22s	180 180	

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

d. Click **Encryption Statistics**. You should see one or more sessions using the 3DES encryption algorithm.



Monitoring > VPN > VPN Statistics > Encryption Statistics

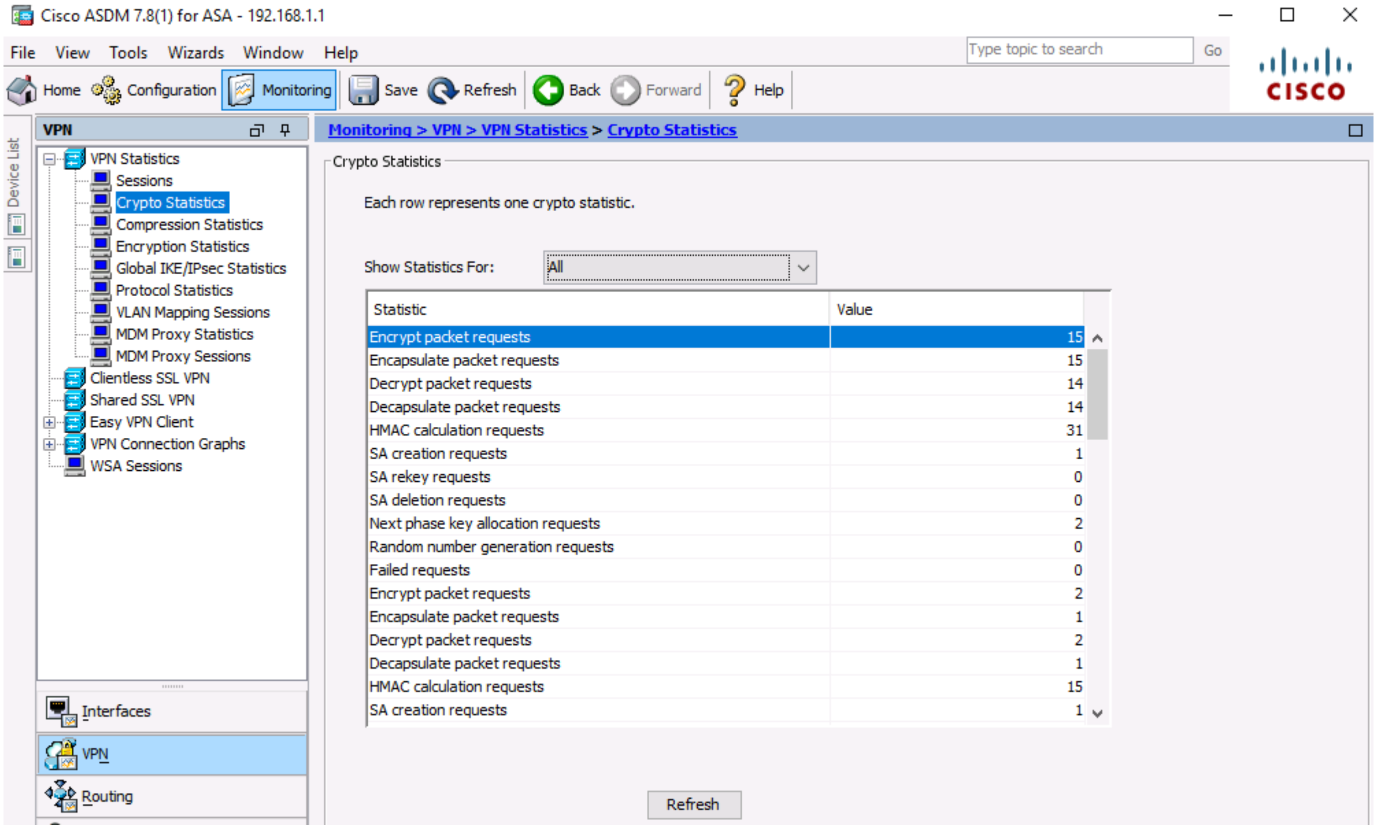
Encryption Statistics

Each row represents one encryption algorithm type.

Show Statistics For: -- All Connection Profiles --

Encryption Algorithm	Sessions	Percentage
none	0	0%
DES	0	0%
3DES	2	100%
RC4	0	0%
AES128	0	0%
AES192	0	0%
AES256	0	0%
AES-GCM-128	0	0%
AES-GCM-192	0	0%
AES-GCM-256	0	0%
AES-GMAC-128	0	0%
AES-GMAC-192	0	0%
AES-GMAC-256	0	0%

e. Click **Crypto Statistics**. You should see values for the number of packets encrypted and decrypted, security association (SA) requests, etc.



Monitoring > VPN > VPN Statistics > Crypto Statistics

Crypto Statistics

Each row represents one crypto statistic.

Show Statistics For: All

Statistic	Value
Encrypt packet requests	15
Encapsulate packet requests	15
Decrypt packet requests	14
Decapsulate packet requests	14
HMAC calculation requests	31
SA creation requests	1
SA rekey requests	0
SA deletion requests	0
Next phase key allocation requests	2
Random number generation requests	0
Failed requests	0
Encrypt packet requests	2
Encapsulate packet requests	1
Decrypt packet requests	2
Decapsulate packet requests	1
HMAC calculation requests	15
SA creation requests	1

Reflection

Describe a situation where a site-to-site IPsec VPN would be preferable over other VPN options.

____

____

____

____

____

____

____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.