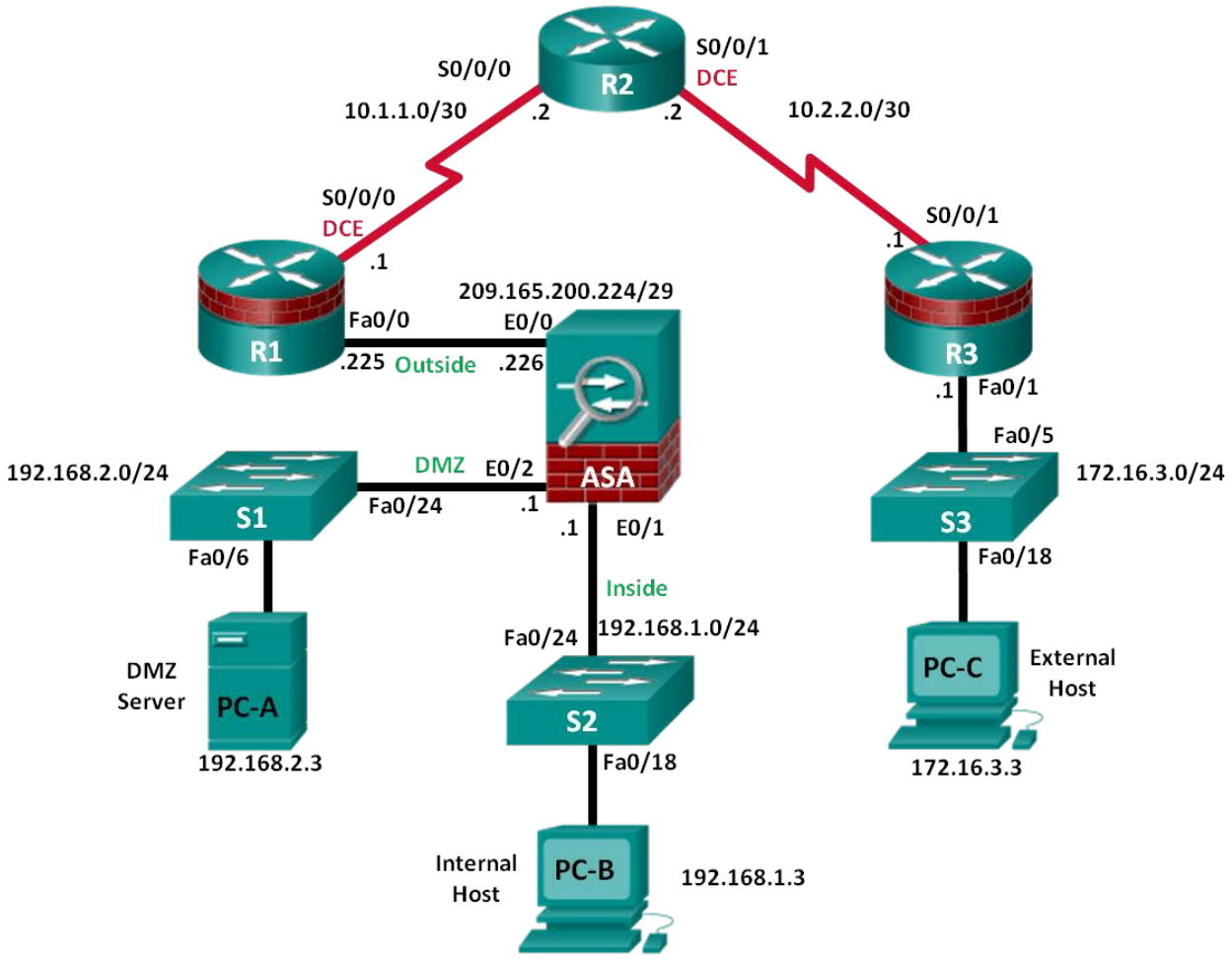
CCNA Security

Lab - Configuring a Site-to-Site IPsec VPN on ISR and ASA 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	Fa0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
	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	Fa0/1	172.16.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	E0/0 (outside)	209.165.200.226	255.255.255.248	NA	R1 Fa0/0
	E0/1 (inside)	192.168.1.1	255.255.255.0	NA	S2 Fa0/24
	E0/2 (dmz)	192.168.2.1	255.255.255.0	NA	S1 Fa0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 Fa0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 Fa0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 Fa0/18

Objectives

Part 1: Basic Router/Switch/PC Configuration

- Cable the network as shown in the topology.
- Configure hostnames, interface IP addresses for routers, switches and PCs.
- Configure static routing, including default routes, between R1, R2 and R3.
- Verify connectivity between hosts, switches and routers.

Part 2: Basic ASA Configuration

- Access the ASA console.
- Clear previous configuration settings.
- Configure basic settings.

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

- Configure basic VPN connection information settings.
- Configure IKE policy parameters.
- Configure a transform set.
- Define traffic to protect.
- Verify the VPN configuration on R3.

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

- Identify peer device and access interface.
- Configure IKE policy parameters.
- Configure a transform set.

- Specify traffic to protect.
- Configure static address translation for VPN support on ASA
- Verify VPN functionality.
- Monitor the VPN connection and traffic.

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. Router R1 represents a CPE device managed by the ISP. Router R2 represents an intermediate Internet router. Router R3 connects users at the remote branch office to the ISP. The ASA is an edge CPE 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, which are not aware of its existence.

In Part 1 of the lab you will configure the topology and non-ASA devices. In Part 2 you will prepare the ASA. In Part 3 you will configure the R3 ISR and the ASA as a Site-to-Site IPsec VPN endpoints.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 1841 with Cisco IOS Release 15.1(4)M8 Advanced IP Services image or comparable)
- 3 Switches (Cisco 2960 or comparable)
- 1 ASA 5505 (OS version 8.4(2) and Base license or comparable)
- 3 PCs (Windows Vista or Windows 7 with CCP 2.5, PuTTy SSH client)
- Serial and Ethernet cables as shown in the topology
- Console cables to configure the Cisco networking devices

Part 1: Basic Router/Switch/PC Configuration

In Part 1 of this lab, you will set up the network topology and 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: Cable the network and clear previous device settings.

Attach the devices shown in the topology diagram and cable as necessary. Make sure that the routers and switches have been erased and have no startup configurations.

Step 2: Configure basic settings for routers and switches.

a. Configure host names as shown in the topology for each router.

b. Configure router interface IP addresses as shown in the IP Addressing Table.

c. Configure a clock rate for routers with a DCE serial cable attached to their serial interface. Router R1 is shown here as an example.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. Configure the host name for the switches. Other than host name, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0

R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

b. Configure a static route from R2 to the R1 Fa0/0 subnet (connected to ASA interface E0/0) and a static route from R2 to the R3 LAN.

```
R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

Step 4: Configure the enable and VTY passwords on R3.

On R3, set the enable password to **class** and the console and VTY passwords to **cisco**. Configure these settings on R1 and R2. R3 is shown here as an example.

```
R3(config)# enable secret class

R3(config)# line vty 0 4
R3(config-line)# password cisco
R3(config-line)# login

R3(config)# line con 0
R3(config-line)# password cisco
R3(config-line)# login
```

Step 5: 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 6: Verify connectivity.

From PC-C, ping the R1 Fa0/0 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-C to R1 Fa0/0 you have demonstrated that static routing is configured and functioning correctly.

Step7: Save the basic running configuration for each router and switch.

Part 2: Basic ASA Configuration

Step 1: Access the ASA console.

a. Accessing the ASA via the console port is the same as with a Cisco router or switch. Connect to the ASA Console port with a rollover cable.

b. Use a terminal emulation program such as TeraTerm or HyperTerminal to access the CLI, and use the serial port settings of 9600 baud, eight data bits, no parity, one stop bit, and no flow control.

c. If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.

d. Enter privileged mode with the **enable** command and password (if set). By default the password is blank so you can just press **Enter**. If the password has been changed to that specified in this lab, the password will be **class**. In addition, the hostname and prompt will be **CCNAS-ASA>**, as shown here. The default ASA hostname and prompt is **ciscoasa>**.

```
CCNAS-ASA> enable
Password: class (or press Enter if none set)
```

Step 2: Clear the previous ASA configuration settings.

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

```
CCNAS-ASA# write erase
Erase configuration in flash memory? [confirm]
[OK]
CCNAS-ASA#
```

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

b. Use the **reload** command to restart the ASA. This will cause the ASA to come up in CLI Setup mode. If you see the message `System config has been modified. Save? [Y]es/[N]o:`, respond with "N".

```
CCNAS-ASA# reload
Proceed with reload? [confirm] <Enter>
CCNAS-ASA#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45
<output omitted>
```

Step 3: Bypass Setup Mode.

When the ASA completes the reload process, it should detect that the **startup-config** file is missing and go into Setup mode. If it does not come up in this mode, repeat Step 2.

a. When prompted to pre-configure the firewall through interactive prompts (Setup mode), respond with "**no**".

```
Pre-configure Firewall now through interactive prompts [yes]? no
```

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

Step 4: Use the CLI script to configure the ASA.

In this step you will use the modified running-config from Lab 10E to preconfigure basic settings, the firewall and DMZ.

a. Ensure that there is no previous configuration in the ASA, other than the defaults that the ASA automatically inserts, using the **show run** command.

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

```
ciscoasa> enable
Password: <Enter>

ciscoasa# conf t
ciscoasa(config)#
```

c. Copy and paste the **Pre-VPN Configuration Script** commands listed below at the ASA global config mode prompt to bring it to the point where you can 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 keypair, respond "**yes**".

e. After script commands have been applied, 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.

Pre-VPN ASA Configuration Script:

```
hostname CCNAS-ASA
!
domain-name ccnasecurity.com
!
enable password class
passwd cisco
!
interface Ethernet0/0
 switchport access vlan 2
 no shut
!
interface Ethernet0/1
 switchport access vlan 1
 no shut
!
interface Ethernet0/2
 switchport access vlan 3
 no shut
```

```
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
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 admin password cisco123
!
aaa authentication telnet console LOCAL
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
telnet 192.168.1.0 255.255.255.0 inside
```

```
telnet timeout 10
ssh timeout 10
!
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 icmp
!
prompt hostname context
no call-home reporting anonymous
!
crypto key generate rsa modulus 1024
```

Part 3: Configuring the ISR and the ASA as a Site-to-Site IPsec VPN Endpoint

Review and test the resulting configuration.

Configure IPsec VPN Settings on ASA and R3.

Verify connectivity from the ASA LAN to the R3 LAN.

In this task, you will verify that with no tunnel in place, the PC-B on the ASA LAN can ping the PC-C on R3 LAN.

From PC-B, ping the PC-C IP address of **172.16.3.3**.

```
PC-B:\> ping 172.16.3.3
```

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

Enable IKE policies on R3 and ASA.

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

There are two central configuration elements to 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.

```
CCNAS-ASA(config)# crypto isakmp enable outside
```

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

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

b. Establish an Internet Security Association and Key Management Protocol (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 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 R3 for policy 10.

```
R3(config)# crypto isakmp policy 10
```

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

```
R3(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
```

Configure ISAKMP policy parameters on ASA and R3.

Your choice of an encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, ensuring that the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was, indeed, 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.

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 Diffie-Hellman group **2** key exchange. Give the policy a lifetime of **3600** seconds (one hour).

```
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)# lifetime 3600
R3(config-isakmp)# end
```

Configure the same policy on ASA:

```
CCNAS-ASA(config)#  crypto isakmp enable outside
CCNAS-ASA(config)# crypto isakmp policy 10
CCNAS-ASA(config)# authentication pre-share
CCNAS-ASA(config)# encryption 3des
CCNAS-ASA(config)# hash sha
CCNAS-ASA(config)# group 2
CCNAS-ASA(config)# lifetime 3600
CCNAS-ASA(config)# end
```

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

```
R3# show crypto isakmp policy
CCNAS-ASA# show run crypto isakmp
```

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 address** command is used to enter a pre-shared key. Use the IP address of the remote peer, the remote interface that the peer would use to route traffic to the local router.

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

_____

_____

_____

The IP addresses should be R3 S0/0/1 IP address 10.2.2.1 and ASA E0/0 IP address 209.165.200.226. These are the addresses that are used to send normal traffic between R3 and ASA.

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 **cisco123** on router R3. Production networks should use a complex key. This command points to the remote peer ASA E0/0 IP address.

```
R3(config)# crypto isakmp key cisco123 address 209.165.200.226
```

b. Configure the pre-shared key of **cisco123** on router ASA. The command for ASA points to the R3 S0/0/1 IP address.

```
CCNAS-ASA(config)# tunnel-group 10.2.2.1 type ipsec-l2l

CCNAS-ASA(config)# tunnel-group 10.2.2.1 ipsec-attributes

CCNAS-ASA(config)# pre-shared-key cisco123
```

Configure the IPsec transform set and life times.

a. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. To create an IPsec transform set, use the **crypto ipsec transform-set tag** command. Use **?** to see which parameters are available.

```
R3(config)# crypto ipsec transform-set 50 ?
```

```
ah-md5-hmac   AH-HMAC-MD5 transform
ah-sha-hmac   AH-HMAC-SHA 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-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
```

b. On R3, create a transform set with tag **50** and use an Encapsulating Security Protocol (ESP) transform with an 3 DES cipher with ESP and the SHA hash function. The transform sets must match.

```
R3(config)# crypto ipsec transform-set 50 esp-3des esp-sha-hmac
R3(cfg-crypto-trans)# exit
```

Create a transform set on ASA:

```
CCNAS-ASA(config)# crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac
```

What is the function of the IPsec transform set?

_____

_____

_____

_____

The IPsec transform set specifies the cryptographic algorithms and functions (transforms) that a router employs on the actual data packets sent through the IPsec tunnel. These algorithms include the encryption, encapsulation, authentication, and data integrity services that IPsec can apply.

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, but sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which, in this case, 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 as unencrypted.

In this scenario, the traffic you want to encrypt is traffic going from ASA's Ethernet LAN (inside network) to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

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

```
R3(config)# access-list 101 permit ip 172.16.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

b. Configure the IPsec VPN interesting traffic ACL on ASA.

```
CCNAS-ASA(config)# access-list L2LACL extended permit ip 192.168.1.0
255.255.255.0 172.16.3.0 255.255.255.0
```

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

_____

_____

_____

Yes. IPsec does evaluate whether access lists are mirrored. IPsec does not form a security association if the peers do not have mirrored access lists to select interesting traffic.

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 ones facing the IPsec peer.

To create a crypto map, use **crypto map name sequence-num type** command in global configuration mode 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. Enter crypto map configuration mode on R3. Use a type of ipsec-isakmp, which means IKE is used to establish IPsec security associations.

a. Create the crypto map on R3, name it **CMAP**, and use **10** as the sequence number. A message displays after the command is issued.

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

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

```
R3(config-crypto-map)# match address 101
```

c. To view the list of possible **set** commands that you can do in a crypto map, use the help function.

```
R3(config-crypto-map)# set ?
  identity             Identity restriction.
  ip                   Interface Internet Protocol config commands
  isakmp-profile       Specify isakmp Profile
  nat                  Set NAT translation
  peer                 Allowed Encryption/Decryption peer.
  pfs                  Specify pfs settings
  reverse-route        Reverse Route Injection.
  security-association  Security association parameters
  transform-set        Specify list of transform sets in priority order
```

d. Setting a peer IP or hostname is required. Set it to R3's remote VPN endpoint interface using the following command.

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

e. Hard code the transform set to be used with this peer, using the **set transform-set tag** command.

```
R3(config-crypto-map)# set transform-set 50
```

```
R3(config-crypto-map)# exit
```

f. Create a mirrored matching crypto map on ASA.

```
CCNAS-ASA(config)# crypto map TEST_MAP 10 match address L2LACL
CCNAS-ASA(config)# crypto map TEST_MAP 10 set peer 10.2.2.1
CCNAS-ASA(config)# crypto map TEST_MAP 10 set transform-set 3DES_SHA
CCNAS-ASA(config)# crypto map TEST_MAP 10 set reverse-route
```

The last step is applying the crypto map to interfaces.

Note: The security associations (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 appropriate interfaces on R3 and the ASA.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end

CCNAS-ASA(config)# crypto map TEST_MAP interface outside
```

Configure static address translation for VPN support on ASA

```
CCNAS-ASA(config)# object network NETWORK_OBJ_172.16.3.0_24
CCNAS-ASA(config)# subnet 172.16.3.0 255.255.255.0
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.0_24
CCNAS-ASA(config)# subnet 192.168.1.0 255.255.255.0

CCNAS-ASA(config)# nat (inside,outside) source static
NETWORK_OBJ_192.168.1.0_24 NETWORK_OBJ_192.168.1.0_24 destination static
NETWORK_OBJ_172.16.3.0_24 NETWORK_OBJ_172.16.3.0_24
```

Verify the Site-to-Site IPsec VPN Configuration.

Verify the IPsec configuration on R3 and ASA.

a. Previously, you used the **show crypto isakmp policy** command to display the configured ISAKMP policies on the router. Similarly, the **show crypto ipsec transform-set** command displays the configured IPsec policies in the form of the transform sets.

```
R3# show crypto ipsec transform-set
CCNAS-ASA# show run crypto ipsec
```

b. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R3# show crypto map

CCNAS-ASA# show run crypto map
```

Note: The output of these **show** commands does not change if interesting traffic goes across the connection. You test various types of traffic in the next task.

Verify the IPsec VPN Operation.

Step 2: Display isakmp security associations.

The **show crypto isakmp sa** command reveals that no IKE SAs exist yet. When interesting traffic is sent, this command output changes.

```
R3# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

Display IPsec security associations.

The **show crypto ipsec sa** command shows the unused SA between ASA and R3.

Note: The number of packets sent across and the lack of any security associations listed toward the bottom of the output. The output for R3 is shown here.

```
R3# show crypto ipsec sa
```

Why have no SAs been negotiated?

_____

_____

_____

Because no interesting traffic has been identified, IPsec has not begun to negotiate a security association over which it will encrypt traffic.

Generate some interesting test traffic and observe the results.

You can verify tunnel functionality by pinging from branch office PC-C to PC-B on the internal network. The pings should be successful.

Note: Without the tunnel in place and bypassing NAT, it would be impossible for PC-C on the external network to ping PC-B on the private internal network.

Step 3: Verify the tunnel.

Issue the show crypto isakmp sa command on R3 and ASA to view the security association created

```
CCNAS-ASA# show crypto isakmp sa
```

```
R3# show crypto isakmp sa
```

Issue the show crypto ipsec sa command. How many packets have been transformed between R3 and ASA?

```
R3# show crypto ipsec sa
```

You should see values for the number of packets encrypted and decrypted as well as security association (SA) requests, etc.

Reflection

1. What are some situations where a site-to-site IPsec VPN would be preferable as compared to a remote access SSL VPN?

   _____

   _____

   _____

   _____

   _____

   _____

   When a large number of hosts exists at a remote office and traffic between the office and a central site needs to be protected. Also, if it is desired to use IPsec for increased security as well as clientless access. One disadvantage of the site-to-site VPN is that traffic on the remote network (connecting host) is not protected, only the traffic between the site-to-site tunnel endpoints.

2. What are some situations where a remote access VPN would be preferable as compared to site-to-site VPN?

   _____

   _____

   _____

   _____

   _____

   _____

   When teleworkers and mobile workers are dispersed and it is desired to provide AnyConnect or clientless browser-based SSL VPN access from multiple locations.