Step 10: Save the basic running configuration for all three routers.

a. Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Step 11: Save the configuration on R1 and R3 for later restoration.

Use HyperTerminal or another means such as copy and paste to save the R1 and R3 running configurations from Part 1 of this lab and edit them so that they can be used to restore the routers in Part 3 of the lab to configure the VPN with SDM.

Note: When editing the captured running config text, remove all occurrences of "- - More - -." Remove any commands that are not related to the items you configured in Part 1 of the lab, such as the Cisco IOS version number, no service pad, and so on. Many commands are entered automatically by the Cisco IOS software. Also replace the encrypted passwords with the correct ones specified previously and be sure to use the **no shutdown** command for interfaces that need to be enabled.

Part 2: Configure a Site-to-Site VPN with Cisco IOS

In Part 2 of this lab, you configure an IPsec VPN tunnel between R1 and R3 that passes through R2. You will configure R1 and R3 using the Cisco IOS CLI. You then review and test the resulting configuration.

Task 1: Configure IPsec VPN Settings on R1 and R3

Step 1: Verify connectivity from the R1 LAN to the R3 LAN.

In this task, you verify that with no tunnel in place, the PC-A on the R1 LAN can ping the PC-C on R3 LAN.

a. From PC-A, ping the PC-C IP address of 192.168.3.3.

```
PC-A:\>ping 192.168.3.3
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Enable IKE policies on R1 and R3.

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 for some reason, you can enable it with the command **crypto isakmp enable**. Use this command to verify that the router IOS supports IKE and that it is enabled.

```
R1(config)#crypto isakmp enable

R3(config)#crypto isakmp enable
```

Note: If you cannot execute this command on the router, you need to upgrade the IOS image to one with a feature set 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* configuration 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 R1 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.

a. Configure an authentication type of pre-shared keys. Use AES 256 encryption, SHA as your hash algorithm, and Diffie-Hellman group 5 key exchange for this IKE policy.

b. Give the policy a life time of 3600 seconds (one hour). Configure the same policy on R3. 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. Be sure the same changes are made on the other VPN endpoint so that they are in sync.

Note: You should be at the R1(config-isakmp)# at this point. The **crypto isakmp policy 10** command is repeated below for clarity.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#end

R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption aes 256
```

```
R3(config-isakmp)#hash sha
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#end
```

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

```
R1#show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
   encryption algorithm: AES - Advanced Encryption Standard (256 bit
   keys).
   hash algorithm:            Secure Hash Standard
   authentication method:     Pre-Shared Key
   Diffie-Hellman group:      #5 (1536 bit)
   lifetime:                  3600 seconds, no volume limit
```

Step 4: Configure pre-shared keys.

a. Because pre-shared keys are used as the authentication method in the IKE policy, configure a key on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration command **crypto isakmp key** *key-string* **address** *address* 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?

_____

_____

b. 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 R1 using the following command. Production networks should use a complex key. This command points to the remote peer R3 S0/0/1 IP address.

```
R1(config)#crypto isakmp key cisco123 address 10.2.2.1
```

c. The command for R3 points to the R1 S0/0/0 IP address. Configure the pre-shared key on router R1 using the following command.

```
R3(config)#crypto isakmp key cisco123 address 10.1.1.1
```

Step 5: 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* parameters. Use **?** to see which parameters are available.

```
R1(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 R1 and R3, create a transform set with tag 50 and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

```
R1(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#exit

R3(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

c. What is the function of the IPsec transform set?

_____

_____

d. You can also change the IPsec security association life times from the default of 3600 seconds or 4,608,000 kilobytes, whichever comes first. On R1 and R3, set the IPsec security association life time to 30 minutes, or 1800 seconds.

```
R1(config)#crypto ipsec security-association lifetime seconds 1800

R3(config)#crypto ipsec security-association lifetime seconds 1800
```

Step 6: Define interesting traffic.

a. 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.

b. In this scenario, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

c. Configure the IPsec VPN interesting traffic ACL on R1.

```
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

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

```
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

e. 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 ones facing the IPsec peer.

a. To create a crypto map, use the global configuration command **crypto map** *name sequence-num type* to enter the 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 the crypto map configuration mode on R1. Use a type of ipsec-isakmp, which means IKE is used to establish IPsec security associations.

b. Create the crypto map on R1, name it CMAP, and use 10 as the sequence number. A message will display after the command is issued.

```
R1(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.
```

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

```
R1(config-crypto-map)#match address 101
```

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

```
R1(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
security-association Security association parameters
transform-set        Specify list of transform sets in priority order
```

e. Setting a peer IP or host name is required, so set it to R3's remote VPN endpoint interface using the following command.

```
R1(config-crypto-map)#set peer 10.2.2.1
```

f. Hard code the transform set to be used with this peer, using the **set transform-set** *tag* command. Set the perfect forwarding secrecy type using the **set pfs** *type* command, and also modify the default IPsec security association life time with the **set security-association lifetime seconds** *seconds* command.

```
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#exit
```

g. Create a mirrored matching crypto map on R3.

```
R3(config)#crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#exit
```

h. The last step is applying the maps to interfaces. Note that the security associations (SAs) will not be established until the crypto map has been activated by interesting traffic. The router will generate a notification that crypto is now on.

i. Apply the crypto maps to the appropriate interfaces on R1 and R3.

```
R1(config)#interface S0/0/0
R1(config-if)#crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)#end

R3(config)#interface S0/0/1
R3(config-if)#crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)#end
```

Task 2: Verify Site-to-Site IPsec VPN Configuration

Step 1: Verify the IPsec configuration on R1 and R3.

a. Previously, you used the **show crypto isakmp policy** command to show 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.

```
R1#show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },


R3#show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

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

```
R1#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.2.2.1
  Extended IP access list 101
  access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

  Current peer: 10.2.2.1
  Security association lifetime: 4608000 kilobytes/900 seconds
  PFS (Y/N): Y
  DH group:  group5
  Transform sets={
         50: { esp-256-aes esp-sha-hmac  } ,
        }
  Interfaces using crypto map MYMAP: Serial0/0/0

R3#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.1.1.1
  Extended IP access list 101
  access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

  Current peer: 10.1.1.1
  Security association lifetime: 4608000 kilobytes/900 seconds
  PFS (Y/N): Y
  DH group:  group5
  Transform sets={
```

```
        50: { esp-256-aes esp-sha-hmac  } ,
       }
  Interfaces using crypto map MYMAP: Serial0/0/1
```

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.

Task 3: Verify IPsec VPN Operation

Step 1: 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 will change.

```
R1#show crypto isakmp sa

dst   src   state       conn-id slot status
```

Step 2: Display IPsec security associations.

a. The **show crypto ipsec sa** command shows the unused SA between R1 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 R1 is shown here.

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 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.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     outbound ah sas:
     outbound pcp sas:
```

b. Why have no security associations (SAs) been negotiated?

_____

_____

Step 3: Generate some uninteresting test traffic and observe the results.

a. Ping from R1 to the R3 S0/0/1 interface IP address 10.2.2.1. Were the pings successful? _____

b. Issue the **show crypto isakmp sa** command. Was an SA created between R1 and R3? _____

c. Ping from R1 to the R3 Fa01 interface IP address 192.168.3.1. Were the pings successful? _____

d. Issue the **show crypto isakmp sa** command again. Was an SA created for these pings? Why or why not?

_____
_____
_____
_____

e. Issue the command **debug eigrp packets**. You should see EIGRP hello packets passing between R1 and R3.

```
R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
SIAQUERY, SIAREPLY)
R1#
*Jan 29 16:05:41.243: EIGRP: Received HELLO on Serial0/0/0 nbr 10.1.1.2
*Jan 29 16:05:41.243:   AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0 pe
erQ un/rely 0/0
*Jan 29 16:05:41.887: EIGRP: Sending HELLO on Serial0/0/0
*Jan 29 16:05:41.887:   AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
R1#
*Jan 29 16:05:43.143: EIGRP: Sending HELLO on FastEthernet0/1
*Jan 29 16:05:43.143:   AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
R1#
```

f. Turn off debugging with the **no debug eigrp packets** or **undebug all** command.

g. Issue the **show crypto isakmp sa** command again. Was an SA created between R1 and R3? Why or why not?

_____
_____

Step 4: Generate some interesting test traffic and observe the results.

a. Use an extended ping from R1 to the R3 Fa01 interface IP address 192.168.3.1. Extended ping allows you to control the source address of the packets. Respond as shown in the following example. Press enter to accept the defaults, except where a specific response is indicated.

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
```



```
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/92 ms
```

b. Issue the **show crypto isakmp sa** command again.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.2.1        10.1.1.1        QM_IDLE           1001    0 ACTIVE
```

c. Why was an SA created between R1 and R3 this time?

_____

_____

d. What are the endpoints of the IPsec VPN tunnel? _____

e. Ping from PC-A to PC-C. Were the pings successful? _____

f. Issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3? _____

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #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.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xC1DD058(203280472)

     inbound esp sas:
      spi: 0xDF57120F(3747025423)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:5, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC1DD058(203280472)
        transform: esp-256-aes esp-sha-hmac ,
```