CISCO Academy

CCNA Security

Lab – Configure a Site-to-Site IPsec VPN Using ISR CLI and ASA 5505 ASDM (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



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

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
D1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
КI	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
DO	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
KZ	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
Do	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
кз	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA	S2 Fa0/24
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA	R1 F0/0
	VLAN 3 (E0/2)	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

IP Addressing Table

Objectives

Part 1: Basic Router/Switch/PC Configuration

- Cable the network and clear previous device settings, as shown in the topology.
- 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 this 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 5505 with an 8-port integrated switch, running OS version 9.2(3) and ASDM version 7.4(1) and comes with a Base license that allows a maximum of three VLANs.

Note: Before beginning, ensure that the routers and switches have been erased and have no startup configurations.

Instructor Note: Instructions for erasing switches and routers are provided in Chapter 0.0.0.0. Instructions for erasing the ASA, accessing the console, and accessing ASDM are provided in this lab.

Required Resources

• 1 ASA 5505 (OS version 9.2(3) and ASDM version 7.4(1) and Base license or comparable)

- 3 routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology package license)
- 3 switches (Cisco 2960 or comparable) (not required)
- 3 PCs (Windows 7 or Windows 8.1, with SSH Client software installed)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

Instructor Notes:

- This lab has four main parts. Part 1 and 2 can be performed separately but must be performed before
 parts 3 and 4. Part 2 prepares the ASA for ASDM access. Part 3 configures the R3 ISR as a site-to-site
 IPsec VPN endpoint using the CLI. Part 4 configures the opposite end of the tunnel on the ASA using
 ASDM. Parts 3 and 4 should be performed sequentially. Each part will use CLI and ASDM as required to
 verify the configuration.
- The main goal is to configure a site-to-site IPsec VPN between two sites using an ISR at one end of the tunnel and an ASA at the other end.
- The final running configs for all devices are found at the end of the lab.

Part 1: Basic Router/Switch/PC Configuration

In Part 1, 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. Ensure that the routers and switches have been erased and have no startup configurations.

Step 2: 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.

```
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 209.165.200.225 255.255.258.248
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 3: 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.

```
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 4: 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.

```
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 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.

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 2.

- a. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with no.
- 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 at the ASA global configuration mode prompt 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
1
interface Ethernet0/0
 switchport access vlan 2
no shut
1
interface Ethernet0/1
 switchport access vlan 1
no shut
I.
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
1
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.258.248
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
1
object network inside-net
 subnet 192.168.1.0 255.255.255.0
1
object network dmz-server
 host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
1
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
1
username admin01 password admin01pass
1
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
1
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 the 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
                Set the Diffie-Hellman group
  group
  hash
                Set hash algorithm for protection suite
              Set lifetime for ISAKMP security association
  lifetime
                 Negate a command or set its defaults
  no
```

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: 3600 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?

The IP address should be the ASA outside IP address of 209.165.200.226.

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	$\ensuremath{\texttt{IP}}$ 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

employs on the data packets sent through the IPsec tunnel. These algorithms include the encryption, encapsulation, authentication, and data integrity services that IPsec can apply.

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.

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?

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.

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.

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 <u>https://192.168.1.1</u>. After entering the <u>https://192.168.1.1</u> 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.

	- • ×
🗲 🕘 🥥 https://192.168.1.1/admin/pi 🔎 🕶 😵 Cer 🗟 🖒 🗙 🥥 Cisco ASDM 7.4(1) 🛛 🗙	6 🛠 😳
File Edit View Favorites Tools Help	
× Google ✓ 🖑 Search ▼ More >	🕨 Sign In 🔌 🕶
Cisco ASDM 7.4(1)	
Cisco ASDM 7.4(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 <i>multiple</i> security appliances. 	
Install ASDM Launcher	
Run Cisco ASDM as a Java Web Start application	
 Click <i>Run ASDM</i> to run Cisco ASDM. Click <i>Run Startup Wizard</i> 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 © 2006-2015 Cisco Systems, Inc. All rights reserved.	-

c. Log in as user admin01 with the password admin01pass.

📴 Cisco A	SDM-IDM Launcher v1.6(0)	- • •
	Cisco ASDM-IDM Launcher	ululu cisco
Enter usern	name and password for 192.168.1.1	
Username:	admin01	
Password:	•••••	
	Remember the username of the specified device on	this computer
	OK Close	
		👙 🔒

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.

Configuration Configuration Action Configuration Configura	ward 💡 Help	Туре	e topic to search	Go	······································
Home					
Bevice Information	Interface Status				<u>^</u>
General License	Interface	IP Address/Mask	Line	Link	Kbps
	dmz	192.168.2.1/24	? n/a	🔂 up	n/a
Host Name: CCNAS-ASA	inside	192.168.1.1/24	? n/a	G up	n/a
ASA Version: 9.2(3) Device Uptime: 0d 0h 59m 53s	outside	209.165.200.226/29	? n/a	🖸 up	n/a
Total Flash: 128 MB Total Memory: 512 MB	Lost connection to	Firewall.			
VPN Sessions	Traffic Status				E
IPsec: Clientless SSL VPN: 0 AnyConnect Client: 0 Details	Connections Per	Second Usage			
System Resources Status CPU Usage (percent)	3 2- 1 0 UDP: 0	Lost connect	tion to Firewall. 14:59	15:00	15:01
n/a 14:57 14:58 14:59 15:00 15:01	- 'outside' Interfac	e Traffic Usage (Kbos)			
Memory Usage (MB)		e name obage (rapo)			
0MB 200 Lost connection to Firewall.		Lost connect	tion to Firewall.		-
Latest ASDM Syslog Messages					
ASDM logging is disabled. To enable ASDM	logging with information	onal level, dick the button be	low.		
Device configuration loaded successfully.	admin01	2			5/9/15 3:01:12 PM UTC

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.

📑 Site-to-site VPN Connectio	on Setup Wizard	×
VPN Wizard	Introduction	
Branch	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.	
ISP	Site-to-Site VPN	
Corporate Network		
	Here is a <u>video</u> on how to setup a site-to-site VPN connection.	
	< Back Next > Cancel Help	

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 (VLAN 2 E0/0). Click **Next** to continue.

🔄 Site-to-site VPN Connecti	on Setup Wizard
Steps	Peer Device Identification
1. Introduction	This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.
2. Peer Device Identification	Peer IP Address: 10.2.2.1
 Traffic to protect Security NAT Exempt Summary 	VPN Access Interface: outside
	< Back Next > Cancel Help

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. A message may display stating that the certificate information is being retrieved.

🔄 Site-to-site VPN Connectio	on Setup Wizard	
Steps	Traffic to protect	
1. Introduction	This step lets you i	dentify the local network and remote network between which the traffic is to be protected using IPsec encryption.
2. Peer Device Identificatio	Local Network:	inside-network/24
3. Traffic to protect	Remote Network:	172.15.3.0/24
5. NAT Exempt		
6. Summary		
	< Back Ne	kt > Cancel Help

Note: If the ASA does not respond, you may need to close the window and continue to the next step. If prompted to authenticate, log in again as **admin01** with the password **admin01pass**.

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.

🥫 Site-to-site VPN Connection	on Setup Wizard	×
Steps	Security	
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt 	This step lets you secure the selected traffic.	
6. Summary	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.	3
	< Back Next > Cancel Hel	p

Step 7: Configure miscellaneous settings.

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

on Setup Wizard	×
NAT Exempt	
This step allows you to exempt the local network addresses from network translation.	
Exempt ASA side host/network from address translation:	
	_
< Back Next > Cancel Help	
	on Setup Wizard NAT Exempt This step allows you to exempt the local network addresses from network translation. Image: The step allows you to exempt the local network addresses from network translation. Image: The step allows you to exempt the local network addresses from network translation. Image: The step allows you to exempt the local network addresses from network translation. Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the local network from address translation Image: The step allows you to exempt the step allows

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 (recommended). 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.

Branch	Here is the summary of the configuration.	
SET	Name	Value
Cost ISP	IKE Version Allowed	IKE version 1 and IKE version 2
	Authentication Method	
Home	IKE v1	Use pre-shared key
Corporate Network	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	
FLITTE THE	Perfect Forward Secrecy (PFS)	Disabled
	E 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
TH	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
PN Wizord	Network Address Translation	The protected traffic is not subjected to network address translation

Step 9: Verify the ASDM VPN connection profile.

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

Gisco ASDM 7.4 for ASA - 192.168.1.1							
File View Tools Wizards Window	Help				Type topic to sea	rch (Go alaala
Home 🦓 Configuration 🔯 Monito	ring 🔚 Save 🥃	🔖 Refresh 🚺 Back 🔘 F	orward 🢡 Help				cisco
Site-to-Site VPN Group Polices Group Polices Group Polices Group Polices Group Advanced	Configuration >> Manage site-to Access Interfaces Enable interface Interface outside dmz inside	site-to-Site VPN > Connectors. Site VPN connections. Here is a se for IPsec access. Allow IKE v1 Access v allow IKE v1 Access v erface access lists for inbound VI	Allow IKE v2 Acce	a site-to-site VPN co	nnection.		
	Access lists from	m group policy and user policy a	ways apply to the traffi	c.			
	Access lists from Connection Profile Connection profile encrypted, and Add Z E Name In	m group policy and user policy a es	ways apply to the traffi to-site connection. It sp figure the mapping fror Remote Network	ic. Decifies what data tra In certificate to conne IKEv1 Enabled	affic is to be encrypte ection profile <u>here</u> . IKEv2 Enabled	d, how the data tra Group Policy	affic is to be
	Access lists fro Connection Profile Connection pro encrypted, and Add [2] E Name In 10.2.2.1 ou	m group policy and user policy a ss ofile identifies the peer of a site- d other parameters. You can cor- idit Delete Iterface Local Network tside	ways apply to the traffi to-site connection. It sp figure the mapping fror Remote Network 데 다 172.16.3.0/24	ic. Decifies what data train in certificate to conne IKEV 1 Enabled	offic is to be encrypte ction profile <u>here</u> . IKEv2 Enabled	d, how the data tra Group Policy GroupPolicy_10.	offic is to be
Device Setup Frewal Remote Access VPN	Access lists from	m group policy and user policy a es	ways apply to the traffi to-site connection. It sp figure the mapping fror Remote Network @ 172.16.3.0/24	ic. Decifies what data tra n certificate to conne IXEV 1 Enabled	affic is to be encrypte cition profile <u>here</u> , IKEv2 Enabled	d, how the data tra Group Policy GroupPolicy_10.	Affic is to be
Device Setup Device Setup Frewall Remote Access VPN Ste-to-Site VPN	Access lists from Connection Profile Connection profile encrypted, and Add 2 fe Name In 10.2.2.1 out	m group policy and user policy a es	ways apply to the traffi to-site connection. It sp figure the mapping fror Remote Network Remote Network IT2.16.3.0/24	c. n certificate to conne IKEV 1 Enabled	affic is to be encrypte sction profile <u>here</u> . IKEv2 Enabled	d, how the data tra Group Policy GroupPolicy_10.	NAT Exempt
Device Setup Device Setup Prewall Device Management Device Management	Access lists from Connection Profile Connection pro- encrypted, and Add 2 2 E Name In 10.2.2.1 out Find:	m group policy and user policy a es	ways apply to the traffi to-site connection. It sp figure the mapping from Remote Network Remote Network IT2.16.3.0/24	c. bedfes what data tra n certificate to conne IKEv 1 Enabled	affic is to be encrypte sction profile <u>here</u> . IKEv2 Enabled	d, how the data tra Group Policy GroupPolicy_10.	NAT Exempt

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.

Cisco ASDM 7.4 for ASA - 192.168.1.1						
File View Tools Wizards Window	Help			Type topic to sea	rch Go	ahaha
Home 🦓 Configuration 🔯 Monitorin	ng 🔲 Save 💽 Refresh	G Back	Forward 💡 Help			CISCO
vpn ਰਾਸ਼	Monitoring > VPN > VPN	<u>Statistics</u> > <u>Sessi</u>	ons			
VPN Statistics VPN Statistics Crypto Statistics Gobal IEC/Pare Statistics Gobal IEC/Pare Statistics VAN Mapping Sessions VAN Mapping Sessions VAN Mapping Sessions VAN Client VPN Connection Graphs VPN Sense Servers	Type Filter By: IPsec Site-to-Sit	Active te •	Cumulative	Peak Concurrent	Filter	
	Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes T3 Bytes R	¢	Details Logout Ping
Interfaces	To sort VPN sessions, right Logout By: — All Sessions	click on the above to	able and select Table Sort Orde	er from popup menu. jout Sessions		
*					Last Updated: !	5/11/15 1:26:07 PM
Data Refreshed Successfully.			admin01 2	📑 🔂	5/1	1/15 8:25:26 PM UTC

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.

📖 C:\Windows\system32\cmd.exe	
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	^ =
C:\Users\NetAcad>ping 172.16.3.3	
Pinging 172.16.3.3 with 32 bytes of data: Request timed out. Request timed out. Reply from 172.16.3.3: bytes=32 time=40ms ITL=127 Reply from 172.16.3.3: bytes=32 time=41ms ITL=127	
Ping statistics for 172.16.3.3: Packets: Sent = 4, Received = 2, Lost = 2 (50% loss), Approximate round trip times in milli-seconds: Minimum = 40ms, Maximum = 41ms, Average = 40ms	
C:\Users\NetAcad>	

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.

File View Tools Wizards Window Help Type topic to search Go Image: Home Image: Home </th <th>(). CO</th>	(). CO
WIN Image: Configuration Image: Configura	00
VPN D Monitoring > VPN > VPN Statistics > Sessions Image: Second Statistics Image: Second Statistics Image: Second Statistics	
B VPN Statistics	
Constructions	
Compression Statistics Site-to-Site VPN 1 1 1	
Encryption Statistics DKEv1 IPsec 1 1 1	
Groud Interprets Statistics Protocol Statistics	
Easy VPN Clent	
P VPN Connection Graphs Filter By: [IPsec Site +o-Site +] - All Sessions +] Filter	
Connection Profile Protocol Login Time Bytes Tx Det	ails
IP Address Encryption Duration Bytes Rx	
10.2.2.1 DRFv11Pace D22246 UTC Tue May 12 2015 3382 L09 10.2.2.1 DRFv11 (130265 DPacet (13.3.0h)0980496 1704	JUL
Per	g
La Interfaces	
City VPN	
A Control of the second	
A set of the set of th	
Coport of the second and the second	
Logging Refresh	
Last Updated: 5/12/15 1:3	3:48 PM
Data Refreshed Successfully.	6 PM UTC

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

Cisco ASDM 7.4 for ASA - 192.168.1.1						
File View Tools Wizards Window H	Help				Type topic to search	Go
Home 🦓 Configuration 🔯 Monitoring	Save 🔇 Refresh	G Back 🔘 Forwa	rd 🧖 Help		<u></u>	CISCO
VPN 🗗 🕂	Monitoring > VPN > VPN St	atistics > Encryption	Statistics			
VPN Statistics Sessions Crypto Statistics Godal Technological Statistics Godal Technological Statistics Global Technological Statistics Protocol Statistics Vortuge Statistics	Encryption Statistics Each row represents one Show Statistics For:	encryption algorithm ty	ies 🔹 🔻	Percent		
Cleantlace SSL VPN	End ypdon Algona in		Jessions	Percenta	iye oor	
Easy VPN Client	DES			0	0%	
VPN Connection Graphs	3DES			2	100%	
WSA Sessions	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%	
Interfaces		Re	fresh		lai	st Undated: 5/12/15 1:29:13 PM
· · · · ·						ac opulateu: 3/12/13 1:25:13 PM -
Data Refreshed Successfully.			admin01	2	🚔 📐	5/12/15 8:28:56 PM UTC

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

Tisco ASDM 7.4 for ASA - 192.168.1.1			- • •
File View Tools Wizards Window He	lp	Type topic to search Go	. dealer
Home 🦓 Configuration 🔯 Monitoring	🔚 Save 🔇 Refresh 🔇 Back 🕥 Forward 🤗 Help		CISCO
VPN 🗗 🕂 👖	onitoring > VPN > VPN Statistics > Crypto Statistics		
PPN Statistics Sessions Google Statistics Google Statistics Google Statistics Google Statistics Google Statistics Protocol Statistics Protocol Statistics Web Materia Compared	rypto Statistics Each row represents one crypto statistic. Show Statistics For:	Value	
Cientless SSL VPN	Second and the requests	22	
Easy VPN Client	Encapsulate packet requests	33	
VPN Connection Graphs	Decrypt packet requests	32	
	Decapsulate packet requests	32	
	HMAC calculation requests	49	
	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	1	
	Encapsulate packet requests	1	
	Decrypt packet requests	1	
	Decapsulate packet requests	1	
	HMAC calculation requests	15	
	SA creation requests	1 +	
VPN_			
	Refresh		
Properties			
×		Last Updated:	5/12/15 1:30:16 PM
Data Refreshed Successfully.	admin01	2 😹 🗖 5	/12/15 8:29:16 PM UTC

Reflection

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

When a large number of hosts exist at a remote office and traffic between the office and a central site needs

to be protected. 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 is protected.

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.

Device Configs

ASA 5505 Config

```
CCNAS-ASA# show run
: Saved
:
: Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
:
ASA Version 9.2(3)
```

```
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password 9D8jmmmgkfNZLETh encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
1
interface Ethernet0/2
switchport access vlan 3
1
interface Ethernet0/3
shutdown
!
interface Ethernet0/4
shutdown
1
interface Ethernet0/5
shutdown
!
interface Ethernet0/6
shutdown
!
interface Ethernet0/7
shutdown
1
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 1 ftp mode passive dns server-group DefaultDNS domain-name ccnasecurity.com object network inside-net subnet 192.168.1.0 255.255.255.0 object network dmz-server host 192.168.2.3 object network NETWORK OBJ 172.16.3.0 24 subnet 172.16.3.0 255.255.255.0 object network NETWORK OBJ 192.168.1.0 24 subnet 192.168.1.0 255.255.255.0 access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3 access-list outside cryptomap extended permit ip 192.168.1.0 255.255.255.0 172.16.3.0 255.255.255.0 pager lines 24 mtu inside 1500 mtu outside 1500 mtu dmz 1500 icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected 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 no-proxy-arp route-lookup 1 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 timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 dynamic-access-policy-record DfltAccessPolicy user-identity default-domain LOCAL 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 no snmp-server location no snmp-server contact crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport crypto ipsec ikev2 ipsec-proposal DES protocol esp encryption des protocol esp integrity sha-1 md5 crypto ipsec ikev2 ipsec-proposal 3DES protocol esp encryption 3des protocol esp integrity sha-1 md5 crypto ipsec ikev2 ipsec-proposal AES protocol esp encryption aes protocol esp integrity sha-1 md5 crypto ipsec ikev2 ipsec-proposal AES192 protocol esp encryption aes-192 protocol esp integrity sha-1 md5 crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-1 md5

```
crypto ipsec security-association pmtu-aging infinite
crypto map outside map 1 match address outside cryptomap
crypto map outside map 1 set peer 10.2.2.1
crypto map outside map 1 set ikev1 transform-set 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
crypto map outside map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside map interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
encryption aes-256
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption aes-192
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 30
encryption 3des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 40
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 20
authentication rsa-sig
```

encryption aes-256 hash sha group 2 lifetime 86400 crypto ikev1 policy 30 authentication pre-share encryption aes-256 hash sha group 2 lifetime 86400 crypto ikev1 policy 40 authentication crack encryption aes-192 hash sha group 2 lifetime 86400 crypto ikev1 policy 50 authentication rsa-sig encryption aes-192 hash sha group 2 lifetime 86400 crypto ikev1 policy 60 authentication pre-share encryption aes-192 hash sha group 2 lifetime 86400 crypto ikev1 policy 70 authentication crack encryption aes hash sha group 2 lifetime 86400 crypto ikev1 policy 80 authentication rsa-sig encryption aes hash sha group 2 lifetime 86400 crypto ikev1 policy 90 authentication pre-share encryption aes hash sha group 2 lifetime 86400 crypto ikev1 policy 100 authentication crack encryption 3des

hash sha group 2 lifetime 86400 crypto ikev1 policy 110 authentication rsa-sig encryption 3des hash sha group 2 lifetime 86400 crypto ikev1 policy 120 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 crypto ikev1 policy 130 authentication crack encryption des hash sha group 2 lifetime 86400 crypto ikev1 policy 140 authentication rsa-sig encryption des hash sha group 2 lifetime 86400 crypto ikev1 policy 150 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto ikev1 policy 65535 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 telnet 192.168.1.0 255.255.255.0 inside telnet timeout 10 ssh stricthostkeycheck ssh 192.168.1.0 255.255.255.0 inside ssh timeout 10 ssh key-exchange group dh-group1-sha1 console timeout 0

threat-detection basic-threat threat-detection statistics access-list

```
no threat-detection statistics tcp-intercept
group-policy GroupPolicy 10.2.2.1 internal
group-policy GroupPolicy 10.2.2.1 attributes
vpn-tunnel-protocol ikev1 ikev2
username admin01 password UsMZmktANM6Z2Y9I encrypted
tunnel-group 10.2.2.1 type ipsec-121
tunnel-group 10.2.2.1 general-attributes
default-group-policy GroupPolicy 10.2.2.1
tunnel-group 10.2.2.1 ipsec-attributes
ikev1 pre-shared-key *****
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
1
class-map inspection default
match default-inspection-traffic
!
policy-map type inspect dns preset dns map
parameters
 message-length maximum client auto
message-length maximum 512
policy-map global policy
class inspection default
 inspect dns preset dns map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
  inspect ip-options
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
  inspect icmp
1
service-policy global policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
 destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
 destination transport-method http
```

subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:8d83dd856f98a0f1e574fba6c6bfc478 : end

Router R1

```
Building configuration...
```

```
Current configuration : 1713 bytes
1
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
1
security passwords min-length 10
enable secret 9 $9$xKxfXtYW7haqI.$gLUxyPBS.RKfwGx.5Nc/yaDEMxvUD9HmhyqDqqwRGWE
1
no aaa new-model
memory-size iomem 15
!
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
1
cts logging verbose
!
1
username admin01 secret 9
$9$5ShIv6PMmhCYYk$oCVgPgvKu80EKQWTWAj2CWyOkwyl2BHh1PlgxShL/8s
!
redundancy
1
interface Embedded-Service-Engine0/0
no ip address
shutdown
1
interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.248
```

duplex auto speed auto ! interface GigabitEthernet0/1 no ip address shutdown duplex auto speed auto ! interface Serial0/0/0 ip address 10.1.1.1 255.255.255.252 clock rate 2000000 ! interface Serial0/0/1 no ip address shutdown ! ip forward-protocol nd ! no ip http server no ip http secure-server 1 ip route 0.0.0.0 0.0.0.0 Serial0/0/0 ! control-plane 1 line con O exec-timeout 5 0 logging synchronous login local line aux 0 line 2 no activation-character no exec transport preferred none transport output pad telnet rlogin lapb-ta mop udptn v120 ssh stopbits 1 line vty 0 4 exec-timeout 5 0 logging synchronous login local transport input ssh 1 scheduler allocate 20000 1000 ! end

Router R2

R2# show run

```
Building configuration...
Current configuration : 1678 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
1
boot-start-marker
boot-end-marker
T.
security passwords min-length 10
enable secret 9 $9$Nb4BPAMsmT24y.$4bn2kyZCwulndKiaU14531zF4n3ge95hfoFIKrucvpI
Т
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
cts logging verbose
1
username admin01 secret 9
$9$6PSI5.sujsrgN.$LFz4TeeqS/1FtxvK23Le8jxUAY9sjeedVmyF/PA9sPo
!
redundancy
T.
interface Embedded-Service-Engine0/0
no ip address
interface Embedded-Service-Engine0/0
no ip address
shutdown
1
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
```

```
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
clock rate 2000000
1
ip forward-protocol nd
1
no ip http server
no ip http secure-server
1
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
ip route 209.165.200.224 255.255.255.248 Serial0/0/0
1
control-plane
1
line con O
exec-timeout 5 0
logging synchronous
login local
line aux O
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
exec-timeout 5 0
logging synchronous
login local
transport input telnet
1
scheduler allocate 20000 1000
end
```

Router R3

```
R3# show run
Building configuration...
```

```
Current configuration : 2120 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!
```

```
hostname R3
!
boot-start-marker
boot-end-marker
1
security passwords min-length 10
enable secret 9 $9$bkZXRtRQF6uqE.$MenFawyYEn642ALi3kGNBttfJxBOYk3fScLmuOFO9Tq
!
no aaa new-model
memory-size iomem 15
1
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
1
vtp domain TSHOOT
vtp mode transparent
username admin01 secret 9
$9$3qQ5keG1FNmNx.$YmVC/1GkYSErJRHSxRZ13xek9HBYHOASaKmQjYeHx36
!
redundancy
1
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
crypto isakmp key SECRET-KEY address 209.165.200.226
crypto ipsec transform-set ESP-TUNNEL esp-3des esp-sha-hmac
mode tunnel
1
crypto map S2S-MAP 10 ipsec-isakmp
set peer 209.165.200.226
set transform-set ESP-TUNNEL
match address VPN-ACL
1
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
```

! interface GigabitEthernet0/1 ip address 172.16.3.1 255.255.255.0 duplex auto speed auto 1 interface Serial0/0/0 no ip address shutdown clock rate 125000 1 interface Serial0/0/1 ip address 10.2.2.1 255.255.255.252 crypto map S2S-MAP ! ip forward-protocol nd ! no ip http server no ip http secure-server ! ip route 0.0.0.0 0.0.0.0 Serial0/0/1 1 ip access-list extended VPN-ACL permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255 1 control-plane ! line con O exec-timeout 5 0 logging synchronous login local line aux O line 2 no activation-character no exec transport preferred none transport output pad telnet rlogin lapb-ta mop udptn v120 ssh stopbits 1 line vty 0 4 exec-timeout 5 0 logging synchronous login local transport input ssh ! scheduler allocate 20000 1000 ! end

Switches S1, S2 and S3 – Use default configs, except for host name