1. CCNA Security

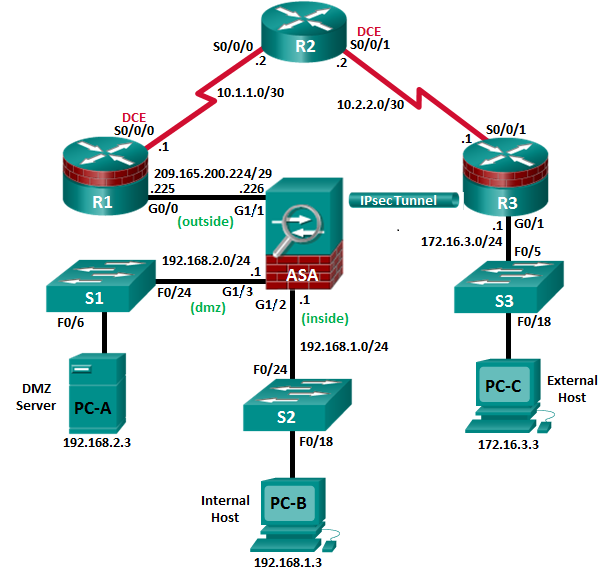
Chapter 10 – Configure a Site-to-Site IPsec VPN between an ISR CLI and an ASA ASDM (Instructor Version)

(ASA-5506 / Equiv)

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

|  |  |
| --- | --- |
|  | **This lab has been updated for use on NETLAB+.**  [www.netdevgroup.com](https://www.netdevgroup.com/) |

1. Topology



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

1. IP Addressing Table

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

1. Objectives

Part 1: Basic Router/Switch/PC Configuration

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

Part 2: Accessing the ASA Console and ASDM

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

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

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

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

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

1. Background/Scenario

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

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

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

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

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

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

**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.

**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.

1. Basic Router/Switch/PC Configuration

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

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

* + 1. Configure R1 using the CLI script.

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

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

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

enable

config t

hostname R1

security passwords min-length 10

enable algorithm-type scrypt secret cisco12345

username admin01 algorithm-type scrypt secret admin01pass

ip domain name ccnasecurity.com

line con 0

login local

exec-timeout 5 0

logging synchronous

exit

line vty 0 4

login local

transport input ssh

exec-timeout 5 0

logging synchronous

exit

interface gigabitethernet 0/0

ip address 209.165.200.225 255.255.255.248

no shut

exit

int serial 0/0/0

ip address 10.1.1.1 255.255.255.252

clock rate 2000000

no shut

exit

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

crypto key generate rsa general-keys modulus 1024

* + 1. Configure R2 using the CLI script.

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

enable

config t

hostname R2

security passwords min-length 10

enable algorithm-type scrypt secret cisco12345

username admin01 algorithm-type scrypt secret admin01pass

ip domain name ccnasecurity.com

line con 0

login local

exec-timeout 5 0

logging synchronous

exit

line vty 0 4

login local

transport input ssh

exec-timeout 5 0

logging synchronous

exit

interface serial 0/0/0

ip address 10.1.1.2 255.255.255.252

no shut

exit

interface serial 0/0/1

ip address 10.2.2.2 255.255.255.252

clock rate 2000000

no shut

exit

ip route 209.165.200.224 255.255.255.248 Serial0/0/0

ip route 172.16.3.0 255.255.255.0 Serial0/0/1

crypto key generate rsa general-keys modulus 1024

* + 1. Configure R3 using the CLI script.

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

enable

config t

hostname R3

security passwords min-length 10

enable algorithm-type scrypt secret cisco12345

username admin01 algorithm-type scrypt secret admin01pass

ip domain name ccnasecurity.com

line con 0

login local

exec-timeout 5 0

logging synchronous

exit

line vty 0 4

login local

transport input ssh

exec-timeout 5 0

logging synchronous

exit

interface gigabitethernet 0/1

ip address 172.16.3.1 255.255.255.0

no shut

exit

int serial 0/0/1

ip address 10.2.2.1 255.255.255.252

no shut

exit

ip route 0.0.0.0 0.0.0.0 Serial0/0/1

crypto key generate rsa general-keys modulus 1024

* + 1. 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.

* + 1. **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.

1. Accessing the ASA Console and ASDM
   * 1. Clear the previous ASA configuration settings.
        1. 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.

* + - 1. 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**.
    1. Bypass Setup mode.

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

* + - 1. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with **No**.
      2. Enter privileged EXEC mode with the **enable** command. The password should be kept blank (no password).
    1. 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.

* + - 1. 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.
      2. Enter global configuration mode. When prompted to enable anonymous call-home reporting, respond **no**.
      3. Copy and paste the Pre-VPN Configuration Script commands listed below to start configuring the SSL VPNs.
      4. Observe the messages as the commands are applied to ensure that there are no warnings or errors. If prompted to replace the RSA key pair, respond **yes**.

hostname CCNAS-ASA

domain-name ccnasecurity.com

enable password cisco12345

!

interface Gi1/1

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

no shut

!

interface gi1/2

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

no shut

!

interface gi1/3

nameif dmz

security-level 70

ip address 192.168.2.1 255.255.255.0

no shut

!

object network inside-net

subnet 192.168.1.0 255.255.255.0

!

object network dmz-server

host 192.168.2.3

!

access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3

!

object network inside-net

nat (inside,outside) dynamic interface

!

object network dmz-server

nat (dmz,outside) static 209.165.200.227

!

access-group OUTSIDE-DMZ in interface outside

!

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

!

username admin01 password admin01pass

!

aaa authentication ssh console LOCAL

aaa authentication http console LOCAL

!

http server enable

http 192.168.1.0 255.255.255.0 inside

ssh 192.168.1.0 255.255.255.0 inside

ssh timeout 10

!

class-map inspection\_default

match default-inspection-traffic

policy-map global\_policy

class inspection\_default

inspect icmp

!

crypto key generate rsa modulus 1024

* + - 1. 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.

1. 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.

* + 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.

* + 1. 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.
  + - 1. Verify that IKE is supported and enabled.

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

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

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

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

* + - 1. 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**

* + - 1. 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

* + 1. 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.

* + - 1. 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**

* + - 1. Verify the IKE policy with the **show crypto isakmp policy** command.

R3# **show crypto isakmp policy**

Global IKE policy

Protection suite of priority 10

encryption algorithm: Three key triple DES

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

* + 1. 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.

* + - 1. 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**

* + 1. Configure the IPsec transform set and lifetime.
       1. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. It is configured using the **crypto ipsec transform-set** *tag* global configuration command. Configure the transform set with the tag **ESP-TUNNEL**. Use **?** to see which parameters are available.

R3(config)# **crypto ipsec transform-set ESP-TUNNEL ?**

ah-md5-hmac AH-HMAC-MD5 transform

ah-sha-hmac AH-HMAC-SHA transform

ah-sha256-hmac AH-HMAC-SHA256 transform on R3

ah-sha384-hmac AH-HMAC-SHA384 transform

ah-sha512-hmac AH-HMAC-SHA512 transform

comp-lzs IP Compression using the LZS compression algorithm

esp-3des ESP transform using 3DES(EDE) cipher (168 bits)

esp-aes ESP transform using AES cipher

esp-des ESP transform using DES cipher (56 bits)

esp-gcm ESP transform using GCM cipher

esp-gmac ESP transform using GMAC cipher

esp-md5-hmac ESP transform using HMAC-MD5 auth

esp-null ESP transform w/o cipher

esp-seal ESP transform using SEAL cipher (160 bits)

esp-sha-hmac ESP transform using HMAC-SHA auth

esp-sha256-hmac ESP transform using HMAC-SHA256 auth

esp-sha384-hmac ESP transform using HMAC-SHA384 auth

esp-sha512-hmac ESP transform using HMAC-SHA512 auth

* + - 1. In our Site-to-site VPN with the ASA, we will use the two highlitghed parameters. Complete the command by entering the two highlighted parameters.

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

What is the function of the IPsec transform set?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The IPsec transform set specifies the cryptographic algorithms and functions (transforms) that a router 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.

* + 1. 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.

* + - 1. 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.

* + 1. 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.

* + - 1. Create the crypto map on R3, name it **S2S-MAP**, and use **10** as the sequence number. Use a type of **ipsec-isakmp**, which means IKE is used to establish IPsec security associations. A message displays after the command is issued.

R3(config)# **crypto map S2S-MAP 10 ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R3(config-crypto-map)#

* + - 1. 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**

* + - 1. 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**

* + - 1. 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

* + - 1. 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#

1. 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.

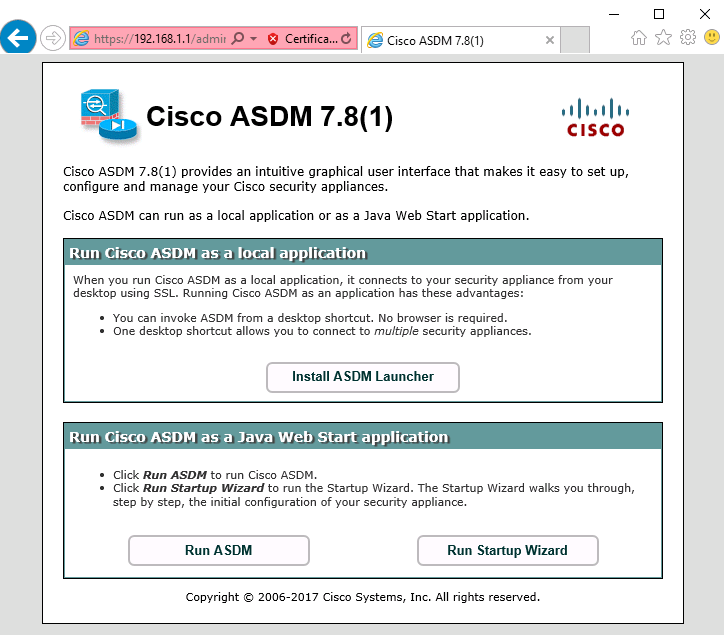
* + 1. Access ASDM.
       1. Open a browser on PC-B and test the HTTPS access to the ASA by entering <https://192.168.1.1>. After entering the <https://192.168.1.1> URL, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings.

**Note**: Specify the HTTPS protocol in the URL.

* + - 1. At the ASDM welcome page, click **Run ASDM**. The ASDM-IDM Launcher will display. Log in as user **admin01** with the password **admin01pass**.

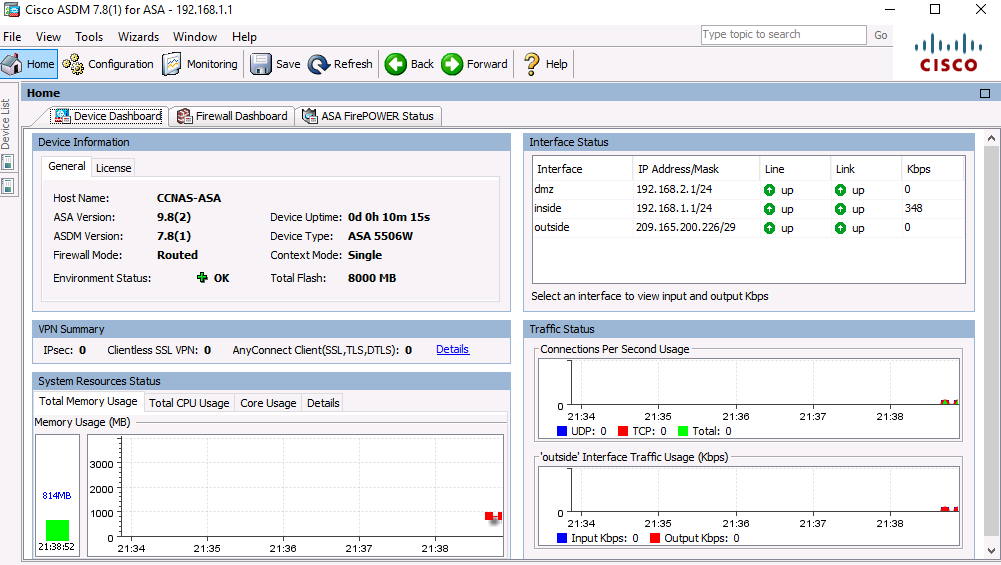
**Note:** You will need to accept all security messages and/or add the ASA IP address to the allowed list of IP addresses in Java.

If the “*Run ASDM*” button via Java is not accessible, access your ASA via **https://<ip\_address>/admin/public/asdm.jnlp** to download the JNLP file and then open the file to continue using ASDM.

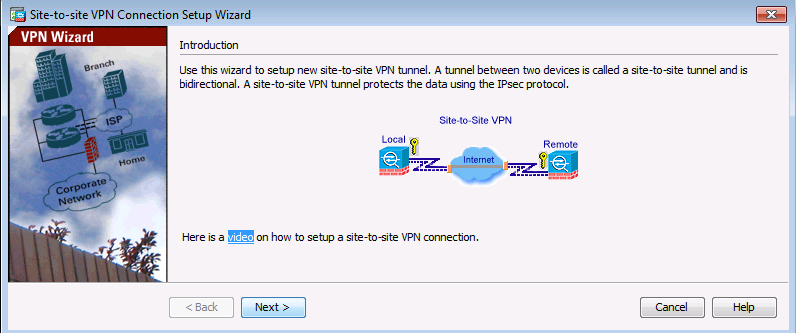


* + 1. Review the ASDM Home screen.

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.

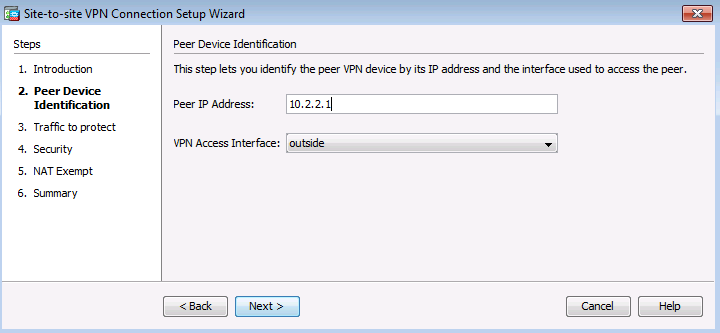


* + 1. Start the VPN wizard.
       1. On the ASDM main menu, click **Wizards** > **VPN Wizards** > **Site-to-Site VPN Wizard** to open the Site-to-Site VPN Connection Setup Wizard Introduction window.



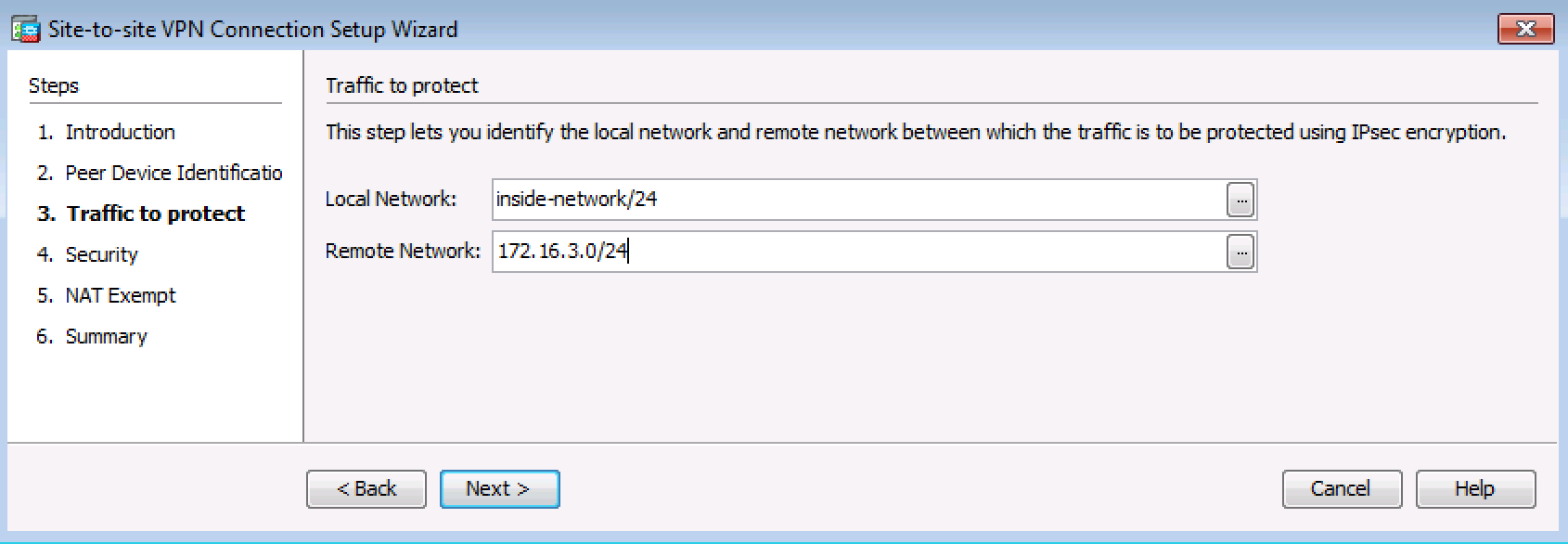
* + - 1. Review the on-screen text and topology diagram and click **Next** to continue.
    1. Configure peer device identification.

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



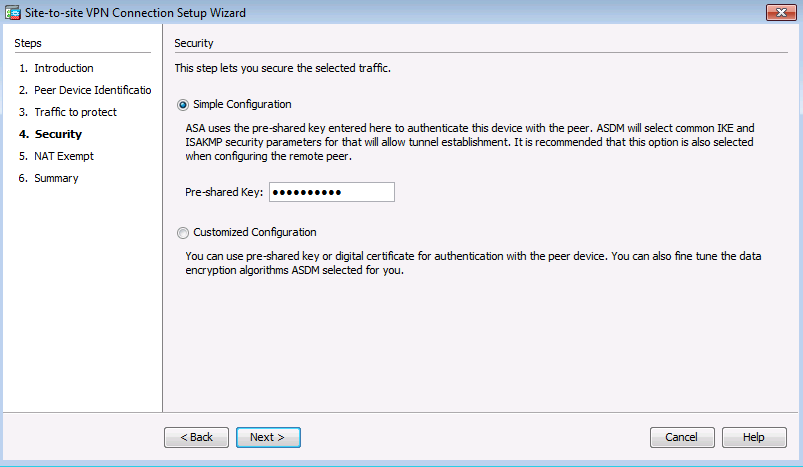
* + 1. Specify the traffic to protect.

In the Traffic to protectwindow, 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.



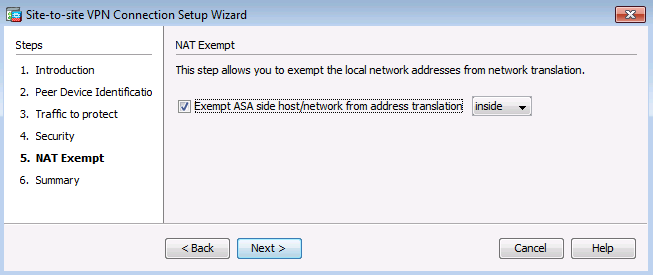
* + 1. Configure authentication.

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



* + 1. Configure miscellaneous settings.

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

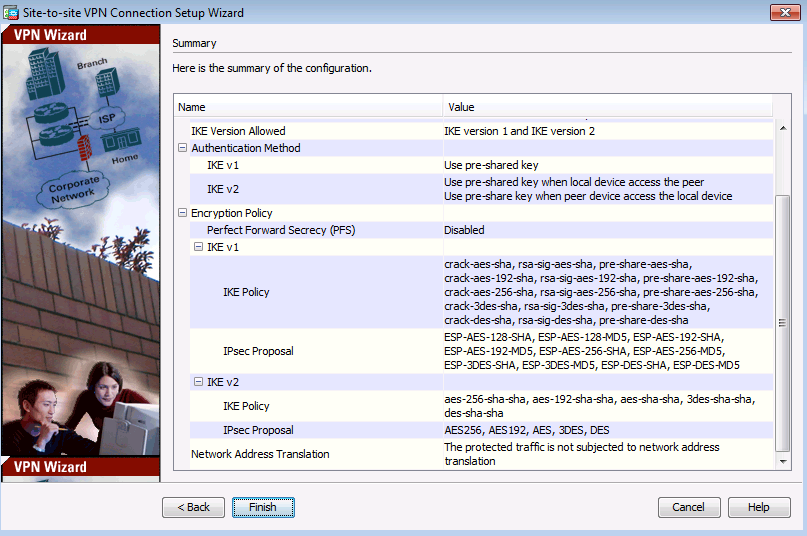


* + 1. Review the configuration summary and deliver the commands to the ASA.

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

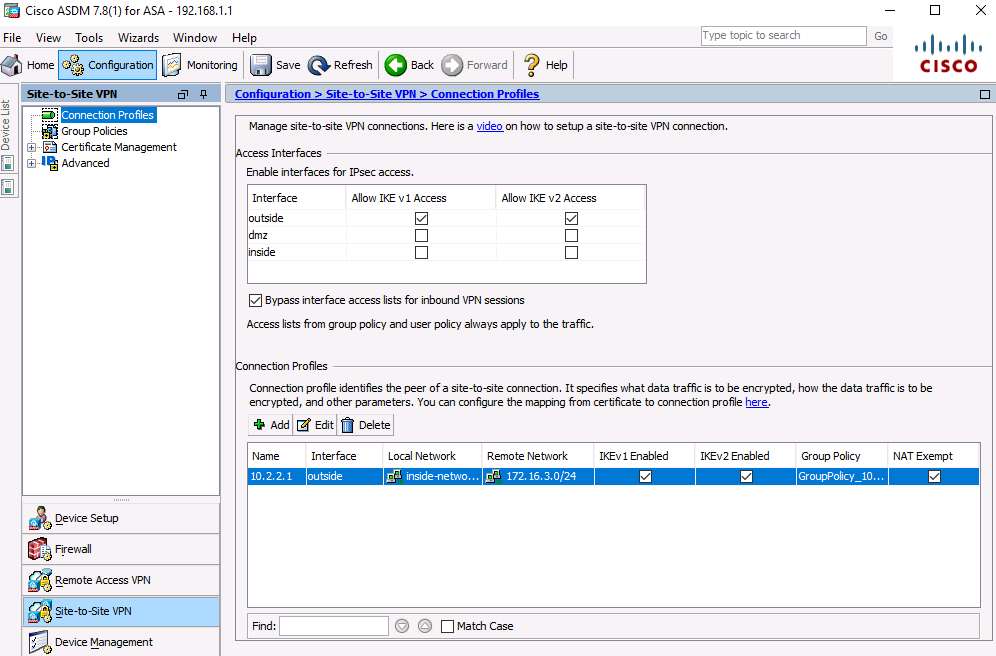
Click **Finish** to complete the process and deliver the commands to the ASA.

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



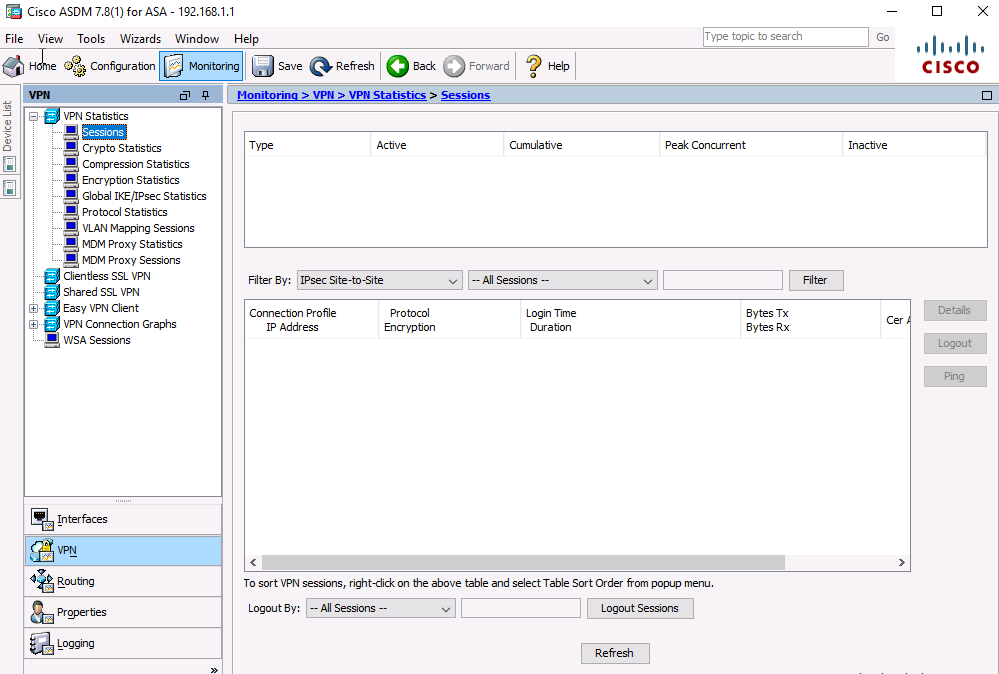
* + 1. Verify the ASDM VPN connection profile.

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

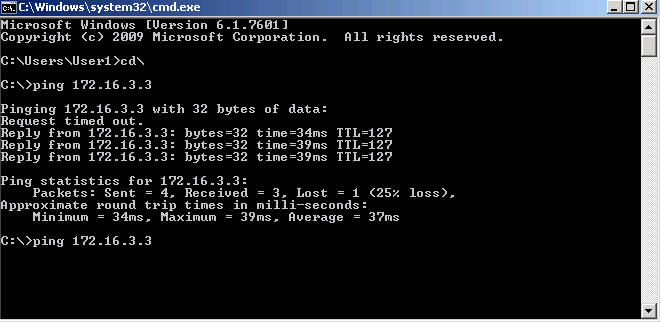


* + 1. Use ASDM monitoring to verify the tunnel.

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.

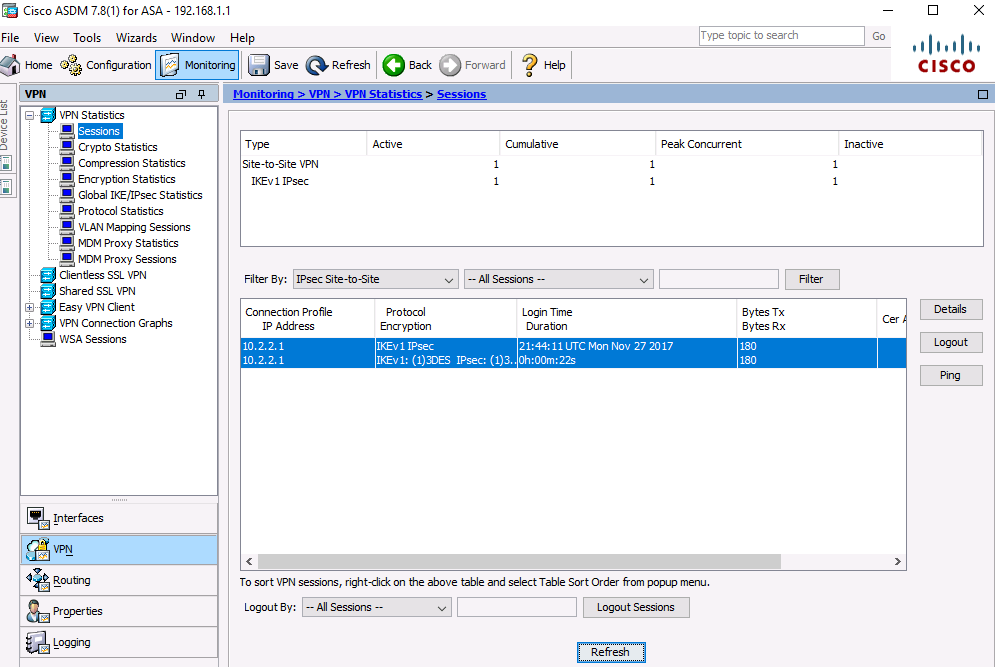


* + 1. Test the VPN configuration from PC-B.
       1. To establish the VPN tunnel, interesting traffic must be generated. From PC-B, ping PC-C.

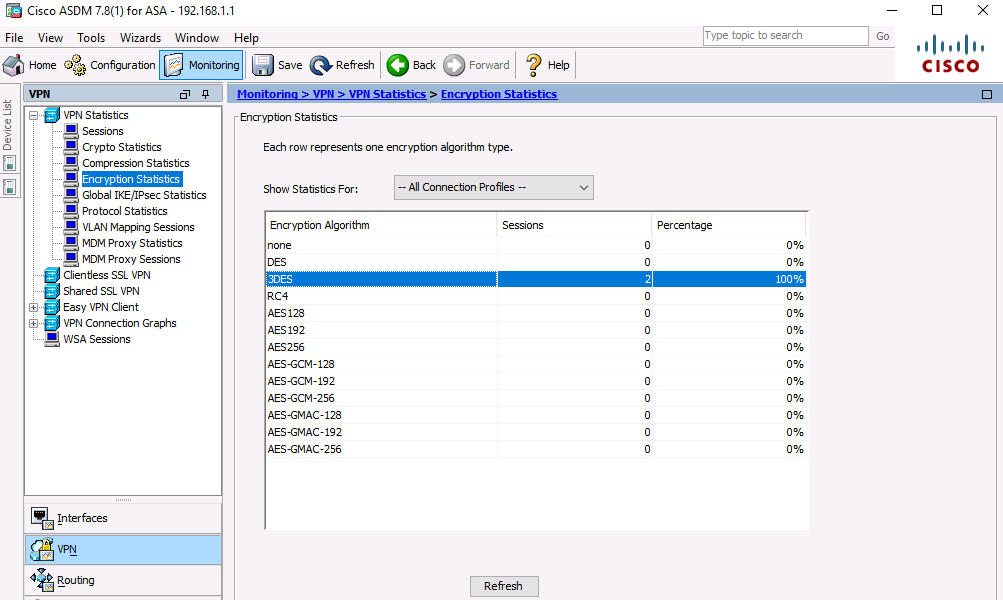


* + - 1. This generates interesting traffic. Notice how two pings failed before being successful. This is because the tunnel first had to be negotiated and established before the ICMP packets could be successful.
      2. The VPN information is now being displayed on the ASDM **Monitoring** > **VPN** > **VPN Statistics** > **Sessions** page.

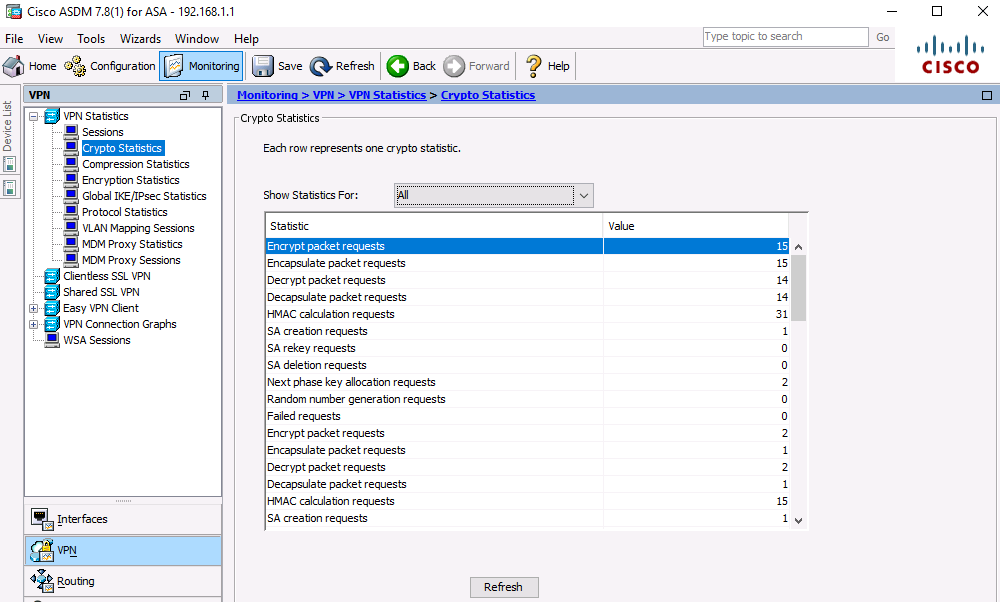
**Note**: You may need to click **Refresh** before the statistics will display.



* + - 1. Click **Encryption Statistics**. You should see one or more sessions using the 3DES encryption algorithm.



* + - 1. Click **Crypto Statistics**. You should see values for the number of packets encrypted and decrypted, security association (SA) requests, etc.



1. 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.

1. 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. | | | | |

1. Device Configs
2. ASA 5506 Config
3. CCNAS-ASA# show run
4. ikev1 policy 30 is superceded by identical policy 10
5. ikev1 policy 60 is superceded by identical policy 40
6. ikev1 policy 90 is superceded by identical policy 70
7. ikev1 policy 120 is superceded by identical policy 100
8. ikev1 policy 150 is superceded by identical policy 130
9. : Saved
10. :
11. : Serial Number: JAD2002064E
12. : Hardware: ASA5506W, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
13. :
14. ASA Version 9.8(2)
15. !
16. hostname CCNAS-ASA
17. domain-name ccnasecurity.com
18. enable password $sha512$5000$tFzC24wAT3W6daZEuK1Jqg==$8DdiB6Xy11f98NG5fkcQcQ== pbkdf2
19. xlate per-session deny tcp any4 any4
20. xlate per-session deny tcp any4 any6
21. xlate per-session deny tcp any6 any4
22. xlate per-session deny tcp any6 any6
23. xlate per-session deny udp any4 any4 eq domain
24. xlate per-session deny udp any4 any6 eq domain
25. xlate per-session deny udp any6 any4 eq domain
26. xlate per-session deny udp any6 any6 eq domain
27. names
28. !
29. interface GigabitEthernet1/1
30. nameif outside
31. security-level 0
32. ip address 209.165.200.226 255.255.255.248
33. !
34. interface GigabitEthernet1/2
35. nameif inside
36. security-level 100
37. ip address 192.168.1.1 255.255.255.0
38. !
39. interface GigabitEthernet1/3
40. nameif dmz
41. security-level 70
42. ip address 192.168.2.1 255.255.255.0
43. !
44. interface GigabitEthernet1/4
45. shutdown
46. no nameif
47. no security-level
48. no ip address
49. !
50. interface GigabitEthernet1/5
51. shutdown
52. no nameif
53. no security-level
54. no ip address
55. !
56. interface GigabitEthernet1/6
57. shutdown
58. no nameif
59. no security-level
60. no ip address
61. !
62. interface GigabitEthernet1/7
63. shutdown
64. no nameif
65. no security-level
66. no ip address
67. !
68. interface GigabitEthernet1/8
69. shutdown
70. no nameif
71. no security-level
72. no ip address
73. !
74. interface Management1/1
75. management-only
76. shutdown
77. no nameif
78. no security-level
79. no ip address
80. !
81. ftp mode passive
82. dns server-group DefaultDNS
83. domain-name ccnasecurity.com
84. object network inside-net
85. subnet 192.168.1.0 255.255.255.0
86. object network dmz-server
87. host 192.168.2.3
88. object network NETWORK\_OBJ\_172.16.3.0\_24
89. subnet 172.16.3.0 255.255.255.0
90. object network NETWORK\_OBJ\_192.168.1.0\_24
91. subnet 192.168.1.0 255.255.255.0
92. access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
93. access-list outside\_cryptomap extended permit ip 192.168.1.0 255.255.255.0 172.16.3.0 255.255.255.0
94. pager lines 24
95. mtu outside 1500
96. mtu inside 1500
97. mtu dmz 1500
98. icmp unreachable rate-limit 1 burst-size 1
99. no asdm history enable
100. arp timeout 14400
101. no arp permit-nonconnected
102. arp rate-limit 16384
103. 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
104. !
105. object network inside-net
106. nat (inside,outside) dynamic interface
107. object network dmz-server
108. nat (dmz,outside) static 209.165.200.227
109. access-group OUTSIDE-DMZ in interface outside
110. route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
111. timeout xlate 3:00:00
112. timeout pat-xlate 0:00:30
113. timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
114. timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
115. timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
116. timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
117. timeout tcp-proxy-reassembly 0:01:00
118. timeout floating-conn 0:00:00
119. timeout conn-holddown 0:00:15
120. timeout igp stale-route 0:01:10
121. user-identity default-domain LOCAL
122. aaa authentication ssh console LOCAL
123. aaa authentication http console LOCAL
124. aaa authentication login-history
125. http server enable
126. http 192.168.1.0 255.255.255.0 inside
127. no snmp-server location
128. no snmp-server contact
129. service sw-reset-button
130. crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
131. crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
132. crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
133. crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
134. crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
135. crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
136. crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
137. crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
138. crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
139. crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
140. crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
141. crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
142. crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
143. crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
144. crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
145. crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
146. crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
147. crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
148. crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
149. crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
150. crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
151. crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
152. crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
153. crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
154. crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
155. crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
156. crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
157. crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
158. crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
159. crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
160. crypto ipsec ikev2 ipsec-proposal DES
161. protocol esp encryption des
162. protocol esp integrity sha-1 md5
163. crypto ipsec ikev2 ipsec-proposal 3DES
164. protocol esp encryption 3des
165. protocol esp integrity sha-1 md5
166. crypto ipsec ikev2 ipsec-proposal AES
167. protocol esp encryption aes
168. protocol esp integrity sha-1 md5
169. crypto ipsec ikev2 ipsec-proposal AES192
170. protocol esp encryption aes-192
171. protocol esp integrity sha-1 md5
172. crypto ipsec ikev2 ipsec-proposal AES256
173. protocol esp encryption aes-256
174. protocol esp integrity sha-1 md5
175. crypto ipsec security-association pmtu-aging infinite
176. crypto map outside\_map 1 match address outside\_cryptomap
177. crypto map outside\_map 1 set peer 10.2.2.1
178. 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
179. crypto map outside\_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
180. crypto map outside\_map interface outside
181. crypto ca trustpool policy
182. crypto ikev2 policy 1
183. encryption aes-256
184. integrity sha
185. group 5 2
186. prf sha
187. lifetime seconds 86400
188. crypto ikev2 policy 10
189. encryption aes-192
190. integrity sha
191. group 5 2
192. prf sha
193. lifetime seconds 86400
194. crypto ikev2 policy 20
195. encryption aes
196. integrity sha
197. group 5 2
198. prf sha
199. lifetime seconds 86400
200. crypto ikev2 policy 30
201. encryption 3des
202. integrity sha
203. group 5 2
204. prf sha
205. lifetime seconds 86400
206. crypto ikev2 policy 40
207. encryption des
208. integrity sha
209. group 5 2
210. prf sha
211. lifetime seconds 86400
212. crypto ikev2 enable outside
213. crypto ikev1 enable outside
214. crypto ikev1 policy 10
215. authentication pre-share
216. encryption aes-256
217. hash sha
218. group 2
219. lifetime 86400
220. crypto ikev1 policy 20
221. authentication rsa-sig
222. encryption aes-256
223. hash sha
224. group 2
225. lifetime 86400
226. crypto ikev1 policy 40
227. authentication pre-share
228. encryption aes-192
229. hash sha
230. group 2
231. lifetime 86400
232. crypto ikev1 policy 50
233. authentication rsa-sig
234. encryption aes-192
235. hash sha
236. group 2
237. lifetime 86400
238. crypto ikev1 policy 70
239. authentication pre-share
240. encryption aes
241. hash sha
242. group 2
243. lifetime 86400
244. crypto ikev1 policy 80
245. authentication rsa-sig
246. encryption aes
247. hash sha
248. group 2
249. lifetime 86400
250. crypto ikev1 policy 100
251. authentication pre-share
252. encryption 3des
253. hash sha
254. group 2
255. lifetime 86400
256. crypto ikev1 policy 110
257. authentication rsa-sig
258. encryption 3des
259. hash sha
260. group 2
261. lifetime 86400
262. crypto ikev1 policy 130
263. authentication pre-share
264. encryption des
265. hash sha
266. group 2
267. lifetime 86400
268. crypto ikev1 policy 140
269. authentication rsa-sig
270. encryption des
271. hash sha
272. group 2
273. lifetime 86400
274. telnet timeout 5
275. ssh stricthostkeycheck
276. ssh 192.168.1.0 255.255.255.0 inside
277. ssh timeout 10
278. ssh key-exchange group dh-group1-sha1
279. console timeout 0
280. threat-detection basic-threat
281. threat-detection statistics access-list
282. no threat-detection statistics tcp-intercept
283. group-policy GroupPolicy\_10.2.2.1 internal
284. group-policy GroupPolicy\_10.2.2.1 attributes
285. vpn-tunnel-protocol ikev1 ikev2
286. dynamic-access-policy-record DfltAccessPolicy
287. username admin01 password $sha512$5000$5qojfU4A3sDU9RksGwuZ7g==$c8XssCbMaibBS0+G2JUkZA== pbkdf2
288. tunnel-group 10.2.2.1 type ipsec-l2l
289. tunnel-group 10.2.2.1 general-attributes
290. default-group-policy GroupPolicy\_10.2.2.1
291. tunnel-group 10.2.2.1 ipsec-attributes
292. ikev1 pre-shared-key \*\*\*\*\*
293. ikev2 remote-authentication pre-shared-key \*\*\*\*\*
294. ikev2 local-authentication pre-shared-key \*\*\*\*\*
295. !
296. class-map inspection\_default
297. match default-inspection-traffic
298. !
299. policy-map type inspect dns preset\_dns\_map
300. parameters
301. message-length maximum client auto
302. message-length maximum 512
303. no tcp-inspection
304. policy-map global\_policy
305. class inspection\_default
306. inspect ftp
307. inspect h323 h225
308. inspect h323 ras
309. inspect ip-options
310. inspect netbios
311. inspect rsh
312. inspect rtsp
313. inspect skinny
314. inspect esmtp
315. inspect sqlnet
316. inspect sunrpc
317. inspect tftp
318. inspect sip
319. inspect xdmcp
320. inspect dns preset\_dns\_map
321. inspect icmp
322. policy-map type inspect dns migrated\_dns\_map\_2
323. parameters
324. message-length maximum client auto
325. message-length maximum 512
326. no tcp-inspection
327. policy-map type inspect dns migrated\_dns\_map\_1
328. parameters
329. message-length maximum client auto
330. message-length maximum 512
331. no tcp-inspection
332. !
333. service-policy global\_policy global
334. prompt hostname context
335. no call-home reporting anonymous
336. call-home
337. profile CiscoTAC-1
338. no active
339. destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
340. destination address email callhome@cisco.com
341. destination transport-method http
342. subscribe-to-alert-group diagnostic
343. subscribe-to-alert-group environment
344. subscribe-to-alert-group inventory periodic monthly
345. subscribe-to-alert-group configuration periodic monthly
346. subscribe-to-alert-group telemetry periodic daily
347. Cryptochecksum:56ad1b55bc334a52b5bd7922f3f5635f
348. : end
349. Router R1
350. R1#show run
351. Building configuration...
352. Current configuration : 2116 bytes
353. !
354. ! Last configuration change at 20:24:02 UTC Tue Jan 6 2015
355. !
356. version 15.4
357. service timestamps debug datetime msec
358. service timestamps log datetime msec
359. no service password-encryption
360. !
361. hostname R1
362. !
363. boot-start-marker
364. boot-end-marker
365. !
366. security passwords min-length 10
367. enable secret 9 $9$f3iTKhnvYzZ9zE$32mfWqHTdRavcb2DaCCfzNbw6BQZep.o2/6h.anoS4Q
368. !
369. no aaa new-model
370. memory-size iomem 15
371. !
372. ip domain name ccnasecurity.com
373. ip cef
374. no ipv6 cef
375. !
376. multilink bundle-name authenticated
377. !
378. cts logging verbose
379. !
380. voice-card 0
381. !
382. license udi pid CISCO2911/K9 sn FTX1713ALKC
383. license accept end user agreement
384. license boot module c2900 technology-package securityk9
385. license boot module c2900 technology-package uck9
386. license boot module c2900 technology-package datak9
387. !
388. username admin01 secret 9 $9$Op9dtgqMnN0Fek$XV3H6tvQpkhoV1OB3qCyw.g7tlsp1ufLkClHqWvGj.M
389. !
390. redundancy
391. !
392. interface Embedded-Service-Engine0/0
393. no ip address
394. shutdown
395. !
396. interface GigabitEthernet0/0
397. ip address 209.165.200.225 255.255.255.248
398. duplex auto
399. speed auto
400. !
401. interface GigabitEthernet0/1
402. no ip address
403. shutdown
404. duplex auto
405. speed auto
406. !
407. interface GigabitEthernet0/2
408. no ip address
409. shutdown
410. duplex auto
411. speed auto
412. !
413. interface Serial0/0/0
414. ip address 10.1.1.1 255.255.255.252
415. clock rate 125000
416. !
417. interface Serial0/0/1
418. no ip address
419. shutdown
420. !
421. ip forward-protocol nd
422. !
423. no ip http server
424. no ip http secure-server
425. !
426. ip route 0.0.0.0 0.0.0.0 Serial0/0/0
427. !
428. control-plane
429. !
430. mgcp behavior rsip-range tgcp-only
431. mgcp behavior comedia-role none
432. mgcp behavior comedia-check-media-src disable
433. mgcp behavior comedia-sdp-force disable
434. !
435. mgcp profile default
436. !
437. gatekeeper
438. shutdown
439. !
440. line con 0
441. exec-timeout 5 0
442. logging synchronous
443. login local
444. line aux 0
445. line 2
446. no activation-character
447. no exec
448. transport preferred none
449. transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
450. stopbits 1
451. line vty 0 4
452. exec-timeout 5 0
453. logging synchronous
454. login local
455. transport input ssh
456. !
457. scheduler allocate 20000 1000
458. !
459. end
460. Router R2

R2#show run

Building configuration...

Current configuration : 2138 bytes

!

! Last configuration change at 16:25:53 UTC Thu Nov 30 2017

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9 $9$Fgj5CkIg/U4RTE$M8IrwcweLZv.v9jxX7I.LfElovp2ypeEkpP68gNNT.M

!

no aaa new-model

memory-size iomem 15

!

ip domain name ccnasecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

voice-card 0

!

license udi pid CISCO2911/K9 sn FTX1713ALJP

license boot module c2900 technology-package securityk9

license boot module c2900 technology-package uck9

license boot module c2900 technology-package datak9

!

username admin01 secret 9 $9$qJNNkYckfMXWvk$VNbxSdII9JE0JCr91Ved4RaV4jyWfPhNrX2wjKSBfKU

!

redundancy

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/2

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 125000

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

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

!

control-plane

!

mgcp behavior rsip-range tgcp-only

mgcp behavior comedia-role none

mgcp behavior comedia-check-media-src disable

mgcp behavior comedia-sdp-force disable

!

mgcp profile default

!

gatekeeper

shutdown

!

line con 0

exec-timeout 5 0

logging synchronous

login local

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output lat 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

1. Router R3

R3#show run

Building configuration...

Current configuration : 2614 bytes

!

! Last configuration change at 20:37:45 UTC Tue Jan 6 2015 by admin01

!

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

!

security passwords min-length 10

enable secret 9 $9$crXbcke/ZPxhl.$8TiTjASbeothAwTy/Q4w.U2ZM7GuBSbhu71ZwBYkeWE

!

no aaa new-model

memory-size iomem 15

!

ip domain name ccnasecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

voice-card 0

!

license udi pid CISCO2911/K9 sn FTX1713ALJV

license accept end user agreement

license boot module c2900 technology-package securityk9

license boot module c2900 technology-package uck9

license boot module c2900 technology-package datak9

!

vtp domain TSHOOT

vtp mode transparent

username admin01 secret 9 $9$EEYgCfdmSzmwRk$1oZUjSBjCs2SncJ6Aa/NfJo/OMf6LYAwT2htmfhPSiM

!

redundancy

!

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

!

crypto map S2S-MAP 10 ipsec-isakmp

set peer 209.165.200.226

set transform-set ESP-TUNNEL

match address VPN-ACL

!

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

!

interface GigabitEthernet0/2

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 125000

!

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

!

ip access-list extended VPN-ACL

remark Link to the CCNAS-ASA

permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255

!

control-plane

!

mgcp behavior rsip-range tgcp-only

mgcp behavior comedia-role none

mgcp behavior comedia-check-media-src disable

mgcp behavior comedia-sdp-force disable

!

mgcp profile default

!

gatekeeper

shutdown

!

line con 0

exec-timeout 5 0

logging synchronous

login local

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output lat 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

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