1. CCNA Security

Lab - Configure AnyConnect Remote Access SSL VPN Using ASA 5506-X ASDM

1. Topology

The image displays the topolgy with 3 routers, 3 switches, 3 PCs, and 1 ASA.

R1 G0/0 connects to ASA G1/1
ASA G1/2 connects to S2 F0/24
S2 F0/18 connects to PC-B
ASA G1/3 connects to S1 F0/24
S0/6 connects to PC-A
R1 S0/0/0 connects to R2 S0/0/0
R2 s0/0/1 connects to R3 S0/0/1
R3 G0/1 connects to S3 F0/5
S3 F0/18 connects to PC-C

**Note**: ISR G1 devices use FastEthernet interfaces instead of GigabitEthernet 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 |
| R1 | 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 |
| R2 | 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 |
| R3 | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| ASA | G1/1 (outside) | 209.165.200.226 | 255.255.255.248 | NA | R1 G0/0 |
| ASA | G1/2 (inside) | 192.168.1.1 | 255.255.255.0 | NA | S2 F0/24 |
| ASA | G1/3 (dmz) | 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: Configure Basic Device Settings

* 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: Access the ASA Console and ASDM

* Access the ASA console.
* Clear the previous ASA configuration settings.
* Bypass Setup mode.
* Configure the ASA by using the CLI script.
* Access ASDM.

Part 3: Configure AnyConnect Client SSL VPN Remote Access Using ASDM

* Start the VPN wizard.
* Specify the VPN encryption protocol.
* Specify the client image to upload to AnyConnect users.
* Configure AAA local authentication.
* Configure the client address assignment.
* Configure the network name resolution.
* Exempt address translation for VPN traffic.
* Review the AnyConnect client deployment details.
* Review the Summary screen and apply the configuration to the ASA.

Part 4: Connect to an AnyConnect SSL VPN

* Verify the AnyConnect client profile.
* Log in from the remote host.
* Perform platform detection (if required).
* Perform an automatic installation of the AnyConnect VPN Client (if required).
* Manually install the AnyConnect VPN Client (if required).
* Confirm VPN connectivity.

1. Background/Scenario

In addition to stateful firewall and other security features, the ASA can provide both site-to-site and remote access VPN functionality. The ASA provides two main deployment modes that are found in Cisco SSL remote access VPN solutions:

* **Clientless SSL VPN -** A clientless, browser-based VPN that lets users establish a secure, remote-access VPN tunnel to the ASA and use a web browser and built-in SSL to protect VPN traffic. After authentication, users are presented with a portal page and can access specific, predefined internal resources from the portal.
* **Client-Based SSL VPN -** A client-based VPN that provides full-tunnel SSL VPN connection, but requires a VPN client application to be installed on the remote host. After authentication, users can access any internal resource as if they were physically on the local network. The ASA supports both SSL and IPsec client-based VPNs.

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 ASDM VPNwizard to configure an AnyConnect client-based SSL remote access VPN. In Part 4 you will establish a connection and verify connectivity.

Your company has two locations connected to an ISP. R1 represents a 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 VPN access to teleworkers using the ASA as a VPN concentrator. They want you to test the client-based model using SSL and the Cisco AnyConnect client.

**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-X with an 8-port integrated switch, running OS version 9.10(1), Adaptive Security Device Manager (ASDM) version 7.10(1), and comes with a Base license that allows a maximum of five VLANs.

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

1. **Required Resources**

* 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
* 3 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE7 or comparable) (not required)
* 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1) and Base license or comparable)
* 3 PCs (Windows, SSH Client and Java version compatible with installed ASDM version)
* Serial and Ethernet cables, as shown in the topology
* Console cables to configure Cisco networking devices

1. Configure Basic Device Settings

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.

* + 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.

* + 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.

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.

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.

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.

The ASA is the focal point for the network zones, and it has not yet been configured. Therefore, 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.

* + 1. Save the basic running configuration for each router and switch.

1. Access 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 not go into Setup mode, repeat Step 2.

* + - 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 at the ASA global configuration mode prompt to start configuring the SSL VPNs.

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 G1/2

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

no shutdown

interface G1/1

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

no shutdown

interface G1/3

nameif dmz

security-level 70

ip address 192.168.2.1 255.255.255.0

no shutdown

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 telnet console LOCAL

aaa authentication ssh console LOCAL

aaa authentication http console LOCAL

http server enable

http 192.168.1.0 255.255.255.0 inside

ssh 192.168.1.0 255.255.255.0 inside

telnet 192.168.1.0 255.255.255.0 inside

telnet timeout 10

ssh timeout 10

class-map inspection\_default

match default-inspection-traffic

policy-map 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. Access ASDM.
       1. On PC-B, start ASDM using the ASDM application or by using a browser and connecting to **https://192.168.1.1** and then choosing **Run ASDM**.

Please refer to the previous lab for more detailed instructions.

**Note**: If one of the choices is **Install Java Web Start**, you will need to input <https://192.168.1.1/admin/public/startup.jnlp> in a browser if you do not want to install the Launcher.

* + - 1. After the ASDM Launcher starts, log in as user **admin01** with password **admin01pass**.

1. Configure AnyConnect SSL VPN Remote Access Using ASDM
   * 1. Start the VPN wizard.
        1. On the ASDM main menu, click **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**. Review the on-screen text and topology diagram.
        2. Click **Next** to continue and open the Connection Profile Identification window.
     2. Configure the SSL VPN interface connection profile.
        1. On the Connection Profile Identificationscreen, enter **AnyConnect-SSL-VPN** as the Connection Profile Name and specify the **outside** interface as the VPN Access Interface.
        2. Click **Next** to continue and open the VPN Protocols window.
     3. Specify the VPN encryption protocol.
        1. In this lab, we are not creating an IPsec VPN. Therefore, uncheck the **IPsec** check box and leave the **SSL** check box checked. Do not specify a device certificate.
        2. Click **Next** to continue to open the Client Images window.
     4. Specify the client image to upload to AnyConnect users.
        1. We need to make the Windows version of AnyConnect downloadable to connecting users. Click **Add** to open the Add AnyConnect Client Image window to specify the AnyConnect client image filename.
        2. Click **Browse Flash** andselect the AnyConnect package file for Windows. The image file name begins with **anyconnect-win-xxx.pkg**. In our example, the image filename is **anyconnect-win-4.6.04054-webdeploy-k9.pkg**.
        3. Click **OK** to return to the AnyConnect Client Image window.
        4. Click **OK** again to return to the Client Image window.
        5. The selected image is now displayed in the Client Images window.
        6. Click **Next** to continue to open the Authentication Methodswindow.
     5. Configure AAA local authentication.
        1. The corporate policy for remote administrative access is to authenticate administrative users against the local user database. Therefore, ensure that the AAA Server Group is specified as **LOCAL**.
        2. Enter a new user named **REMOTE-USER** with the password **cisco12345**.
        3. Click **Add**.
        4. Click **Next** to continue and open the SAML Configuration window. Security Assertion Markup Language (SAML) is an XML based open standard data format for exchanging authentication and authorization data. We are not enabling SAML in this lab, therefore leave settings to their default.
        5. Click **Next** to open the Client Address Assignmentwindow.
     6. Configure the client address assignment.

AnyConnect clients connecting remotely must be assigned an IP address from an IP address pool. There are no address pools by default. Therefore, a pool must first be created.

* + - 1. Click **New** to open the Add IPv4 Pool window to create an IPv4 address pool.
      2. Assign the pool the name **Remote-Pool** with a starting IP address of **192.168.1.100**, an ending IP address of **192.168.1.125**, and a subnet mask of **255.255.255.0**.
      3. Click **OK** to return to the Client Address Assignment window, which now displays the newly created remote user IP address pool.
      4. Click **Next** to continue and open the Network Name Resolution Servers window.
    1. Configure the network name resolution.
       1. Enter the IP address of a DNS server (**192.168.2.3**). Leave the current domain name as **ccnasecurity.com**.
       2. Click **Next** to continue to open the NAT Exempt window.
    2. Exempt address translation for VPN traffic.
       1. Remote user traffic should not use NAT. Therefore, click the **Exempt VPN traffic from network address translation** check box. Do not change the default entries for the Inside Interface (**inside**) and the Local Network (**any4**).
       2. Click **Next** to continue to open the AnyConnect Client Deploymentwindow.
    3. Review the AnyConnect client deployment details.
       1. This informational screen describes two AnyConnect connection options. Click **Next** to continue and open the Summary window.
    4. Review the Summary screen and apply the configuration to the ASA.
       1. On the Summary screen, review the configuration description. Use the Back button to make any changes.
       2. Click **Finish** to commit the configuration to the ASA. After the configuration is delivered to the ASA, ASDM displays the AnyConnect Connection Profiles window.

1. Connect to an AnyConnect SSL VPN
   * 1. Log in from the remote host.
        1. Initially, you will establish a clientless SSL VPN connection to the ASA to download the AnyConnect client software. Open a web browser on PC-C. In the address field of the browser, enter **https://209.165.200.226** for the SSL VPN. SSL is required to connect to the ASA, therefore, use secure HTTP (HTTPS).
        2. Enter the previously created username **REMOTE-USER** with the password **cisco12345**.
        3. Click **Login** to continue and open the AnyConnect Secure Mobility Client Download window.

**Note**: The ASA may request confirmation that this is a trusted site. If requested, click **Yes** to proceed.

**Note**: If you were unable to log in, use the CLI to verify that the user REMOTE-USER is configured. If it is still not working, enter the command **username REMOTE-USER password cisco12345** in the CLI.

* + 1. Install the AnyConnect VPN Client.
       1. The AnyConnect Secure Mobility Client will detect your platform and if Java is installed. Next it stops at the Download option for you to select the image client. Click **AnyConnect VPN** to continue.
       2. Download the AnyConnect Secure Mobility Client by following the on-screen instructions.
       3. Install the AnyConnect client by following the on-screen instructions.
       4. When the AnyConnect VPN client has been installed, start the **Cisco AnyConnect VPN Client**.
       5. When prompted to enter the secure gateway address, enter **209.165.200.226** in the Connect to field, and click **Connect**.

If the message **Untrusted Server Blocked!** is displayed, click **Change Setting...**. Unselect the **Block connections to untrusted server** checkbox and close the window to continue and attempt to connect again. Click **Connect Anyway** to use the untrusted server certificate.

* + - 1. When prompted, enter **REMOTE-USER** for the username and **cisco12345** as the password.
    1. Confirm VPN connectivity.

When the full tunnel SSL VPN connection is established, an icon will appear in the system tray that signifies that the client has successfully connected to the SSL VPN network.

* + - 1. Display connection statistics and information by double-clicking the **AnyConnect** icon in the system tray. You will be able to disconnect the SSN VPN session from here. **Do Not** click **Disconnect** at this time. Click the **gear icon** at the bottom left corner of the Cisco AnyConnect Secure Mobility client window.
      2. Use the scroll bar on the right side of the Virtual Private Network (VPN) – Statistics tab for additional connection information.

**Note**: The inside IP address that is assigned to the client from the VPN pool is 192.168.1.100-125.

* + - 1. From a command prompt on the remote host PC-C, verify the IP addressing by using the **ipconfig** command. Notice that there are two IP addresses listed. One is for the PC-C remote host local IP address (172.16.3.3) and the other is the IP address assigned to the SSL VPN tunnel (192.168.1.100).
      2. From remote host PC-C, ping PC-B (**192.168.1.3**) to verify connectivity.
    1. Use the ASDM Monitor to view the AnyConnect remote user session.

**Note:** Future SSL VPN sessions can be launched through the web portal or through the installed Cisco AnyConnect SSL VPN client. While the remote user at PC-C is still logged in using the AnyConnect client, you can view the session statistics by using the ASDM monitor.

* + - 1. On the ASDM menu bar, click **Monitoring** and then select **VPN** > **VPN Statistics** > **Sessions**.
      2. Click the **Filter By** pull-down list and select **AnyConnect Client**. You should see the **VPN-User** session logged in from PC-C, which has been assigned an inside network IP address of 192.168.1.100 by the ASA.

**Note**: You may need to click **Refresh** to display the remote user session.

1. Reflection
   1. Describe at least two benefits of client–based vs. clientless VPNs?

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

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

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

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

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

* 1. Describe at least one difference between using SSL compared to IPsec for remote access tunnel encryption?

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

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

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

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

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

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 (Fa0/1) | 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. | | | | |