**VPN**

**Step 3: Identify interesting traffic on R1.**

Configure ACL 110 to identify the traffic from the LAN on **R1** to the LAN on **R3** as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the **R1** to **R3** LANs. All other traffic sourced from the LANs will not be encrypted. Because of the implicit **deny all**, there is no need to configure a **deny ip any any**statement.

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

**Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.**

Configure the **crypto ISAKMP policy 10**properties on **R1** along with the shared crypto key **vpnpa55**. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured.

**Note**: The highest DH group currently supported by Packet Tracer is group 5. In a production network, you would configure at least DH 24.

R1(config)# **crypto isakmp policy 10**

R1(config-isakmp)# **encryption aes 256**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 5**

R1(config-isakmp)# **exit**

R1(config)# **crypto isakmp key vpnpa55 address 10.2.2.2**

**Step 5: Configure the IKE Phase 2 IPsec policy on R1.**

a.     Create the transform-set VPN-SET to use **esp-aes and esp-sha-hmac**.

R1(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

b.     Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R1(config-crypto-map)# **description VPN connection to R3**

R1(config-crypto-map)# **set peer 10.2.2.2**

R1(config-crypto-map)# **set transform-set VPN-SET**

R1(config-crypto-map)# **match address 110**

R1(config-crypto-map)# **exit**

**Step 6: Configure the crypto map on the outgoing interface.**

Bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface.

R1(config)# **interface s0/0/0**

R1(config-if)# **crypto map VPN-MAP**

**Part 2: Configure IPsec Parameters on R3**

**Step 1: Enable the Security Technology package.**

a.     On **R3**, issue the **show version** command to verify that the Security Technology package license information has been enabled.

b.     If the Security Technology package has not been enabled, enable the package and reload **R3**.

**Step 2: Configure router R3 to support a site-to-site VPN with R1.**

Configure reciprocating parameters on **R3**. Configure ACL 110 identifying the traffic from the LAN on **R3** to the LAN on **R1** as interesting.

R3(config)# **access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255**

**Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.**

Configure the crypto ISAKMP policy 10 properties on **R3** along with the shared crypto key vpnpa55.

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

R3(config-isakmp)# **encryption aes 256**

R3(config-isakmp)# **authentication pre-share**

R3(config-isakmp)# **group 5**

R3(config-isakmp)# **exit**

R3(config)# **crypto isakmp key vpnpa55 address 10.1.1.2**

**Step 4: Configure the IKE Phase 2 IPsec policy on R3.**

a.     Create the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

R3(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

b.     Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

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

R3(config-crypto-map)# **description VPN connection to R1**

R3(config-crypto-map)# **set peer 10.1.1.2**

R3(config-crypto-map)# **set transform-set VPN-SET**

R3(config-crypto-map)# **match address 110**

R3(config-crypto-map)# **exit**

**Step 5: Configure the crypto map on the outgoing interface.**

Bind theVPN-MAP crypto map to the outgoing Serial 0/0/1 interface. **Note**: This is not graded.

R3(config)# **interface s0/0/1**

R3(config-if)# **crypto map VPN-MAP**

**Part 3: Verify the IPsec VPN**

**Step 1: Verify the tunnel prior to interesting traffic.**

Issue the **show crypto ipsec sa**command on **R1**. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.

**Step 2: Create interesting traffic.**

Ping PC-C from PC-A.

**Step 3: Verify the tunnel after interesting traffic.**

On **R1**, re-issue the **show crypto ipsec sa**command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

**Step 4: Create uninteresting traffic.**

Ping **PC-B** from **PC-A**. **Note**: Issuing a ping from router **R1** to **PC-C** or **R3** to **PC-A** is not interesting traffic.

**Step 5: Verify the tunnel.**

On **R1**, re-issue the **show crypto ipsec sa**command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.

**Step 6: Check results.**

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

-------------------------------------------------------------------------------------------------------------------------------------------

ASA

**interface g1/1**

NETSEC-ASA(config-if)# **nameif OUTSIDE**

NETSEC-ASA(config-if)# **ip address 209.165.200.226 255.255.255.248**

NETSEC-ASA(config-if)# **security-level 0**

NETSEC-ASA(config-if)# **no shutdown**

b.     Configure the G1/2 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100 and enable the interface.

NETSEC-ASA(config)# **interface g1/2**

NETSEC-ASA(config-if)# **nameif INSIDE**

NETSEC-ASA(config-if)# **ip address 192.168.1.1 255.255.255.0**

NETSEC-ASA(config-if)# **security-level 100**

NETSEC-ASA(config-if)# **no shutdown**

c.     Use the following verification commands to check your configurations:

1)     Use the **show interface ip brief** command to display the status for all ASA interfaces.

**Note**: This command is different from the IOS command **show ip interface brief**. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.

**Tip**: Most ASA **show** commands, including **ping**, **copy**, and others, can be issued from within any configuration mode prompt without the **do** command.

2)     Use the **show ip address** command to display the interface information.

### Step 5: Test connectivity to the ASA.

a.     You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fail, troubleshoot the configuration as necessary.

b.     From PC-B, ping the G1/1 (OUTSIDE) interface at IP address 209.165.200.226. You should not be able to ping this address.

## Part 3: Configure Routing, Address Translation, and Inspection Policy Using the CLI

### Step 1: Configure a static default route for the ASA.

Configure a default static route on the ASA OUTSIDE interface to enable the ASA to reach external networks.

a.     Create a “quad zero” default route using the **route** command, associate it with the ASA OUTSIDE interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort.

NETSEC-ASA(config)# **route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225**

b.     Issue the **show route** command to verify the static default route is in the ASA routing table.

c.     Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary.

### Step 2: Configure address translation using PAT and network objects.

a.     Create network object **INSIDE-NET** and assign attributes to it using the **subnet** and **nat** commands.

NETSEC-ASA(config)# **object network INSIDE-NET**

NETSEC-ASA(config-network-object)# **subnet 192.168.1.0 255.255.255.0**

NETSEC-ASA(config-network-object)# **nat (INSIDE,OUTSIDE) dynamic interface**

NETSEC-ASA(config-network-object)# **exit**

b.     The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run**command.

c.     From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail.

d.     Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, four were translated and four were not. The outgoing pings (echos) were translated and sent to the destination. The returning echo replies were blocked by the firewall policy.

## Part 4: Configure DHCP, AAA, and SSH

### Step 1: Configure the ASA as a DHCP server.

a.     Configure a DHCP address pool and enable it on the ASA INSIDE interface.

NETSEC-ASA(config)# **dhcpd address 192.168.1.5-192.168.1.36 INSIDE**

b.     (Optional) Specify the IP address of the DNS server to be given to clients.

NETSEC-ASA(config)# **dhcpd dns 209.165.201.2 interface INSIDE**

c.     Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (INSIDE).

NETSEC-ASA(config)# **dhcpd enable INSIDE**

d.     Change PC-B from a static IP address to a DHCP client and verify that it receives IP addressing information. Troubleshoot, as necessary to resolve any problems.

### Step 2: Configure AAA to use the local database for authentication.

a.     Define a local user named **admin** by entering the **username** command. Specify a password of **adminpa55**.

NETSEC-ASA(config)# **username admin password adminpa55**

b.     Configure AAA to use the local ASA database for SSH user authentication.

NETSEC-ASA(config)# **aaa authentication ssh console LOCAL**

### Step 3: Configure remote access to the ASA.

The ASA can be configured to accept connections from a single host or a range of hosts on the INSIDE or OUTSIDE network. In this step, hosts from the OUTSIDE network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network.

a.     Generate an RSA key pair, which is required to support SSH connections. Because the ASA device has RSA keys already in place, enter **no** when prompted to replace them.

NETSEC-ASA(config)# **crypto key generate rsa modulus 1024**

WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: **no**

ERROR: Failed to create new RSA keys named <Default-RSA-Key>

b.     Configure the ASA to allow SSH connections from any host on the INSIDE network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the OUTSIDE network. Set the SSH timeout to 10 minutes (the default is 5 minutes).

NETSEC-ASA(config)# **ssh 192.168.1.0 255.255.255.0 INSIDE**

NETSEC-ASA(config)# **ssh 172.16.3.3 255.255.255.255 OUTSIDE**

NETSEC-ASA(config)# **ssh timeout 10**

c.     Establish an SSH session from PC-C to the ASA (209.165.200.226). Troubleshoot if it is not successful.

C:\> **ssh -l admin 209.165.200.226**

d.     Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful.

C:\> **ssh -l admin 192.168.1.1**

## Part 5: Configure a DMZ, Static NAT, and ACLs

R1 G0/0 and the ASA OUTSIDE interface already use 209.165.200.225 and .226, respectively. You will use public address 209.165.200.227 and static NAT to provide address translation access to the server.

### Step 1: Configure the DMZ interface VLAN 3 on the ASA.

a.     Configure DMZ VLAN 3, which is where the public access web server will reside. Assign it IP address 192.168.2.1/24, name it **DMZ**, and assign it a security level of 70. Because the server does not need to initiate communication with the inside users, disable forwarding to interface VLAN 1.

NETSEC-ASA(config)# **interface g1/3**

NETSEC-ASA(config-if)# **ip address 192.168.2.1 255.255.255.0**

NETSEC-ASA(config-if)# **nameif DMZ**

INFO: Security level for "DMZ" set to 0 by default.

NETSEC-ASA(config-if)# **security-level 70**

NETSEC-ASA(config-if)# **no shutdown**

b.     Use the following verification commands to check your configurations:

Use the **show interface ip brief** command to display the status for the ASA interfaces.

Use the **show ip address** command to display the information for the ASA interfaces.

### Step 2: Configure static NAT to the DMZ server using a network object.

Configure a network object named **DMZ-SERVER** and assign it the static IP address of the DMZ server (192.168.2.3). While in object definition mode, use the **nat** command to specify that this object is used to translate a DMZ address to an OUTSIDE address using static NAT, and specify a public translated address of 209.165.200.227.

NETSEC-ASA(config)# **object network DMZ-SERVER**

NETSEC-ASA(config-network-object)# **host 192.168.2.3**

NETSEC-ASA(config-network-object)# **nat (DMZ,OUTSIDE) static 209.165.200.227**

NETSEC-ASA(config-network-object)# **exit**

### Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

Configure a named access list **OUTSIDE-DMZ** that permits the TCP protocol on port 80 from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA OUTSIDE interface in the “IN” direction.

NETSEC-ASA(config)# **access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3**

NETSEC-ASA(config)# **access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80**

NETSEC-ASA(config)# **access-group OUTSIDE-DMZ in interface OUTSIDE**

**Note**: Unlike IOS ACLs, the ASA ACL permit statement must permit access to the internal private DMZ address. External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.

### Step 4: Test access to the DMZ server.

From a web browser on PC-C, navigate to the DMZ server (209.165.200.227). Troubleshoot if it is not successful.

*End of document*

*end of document*