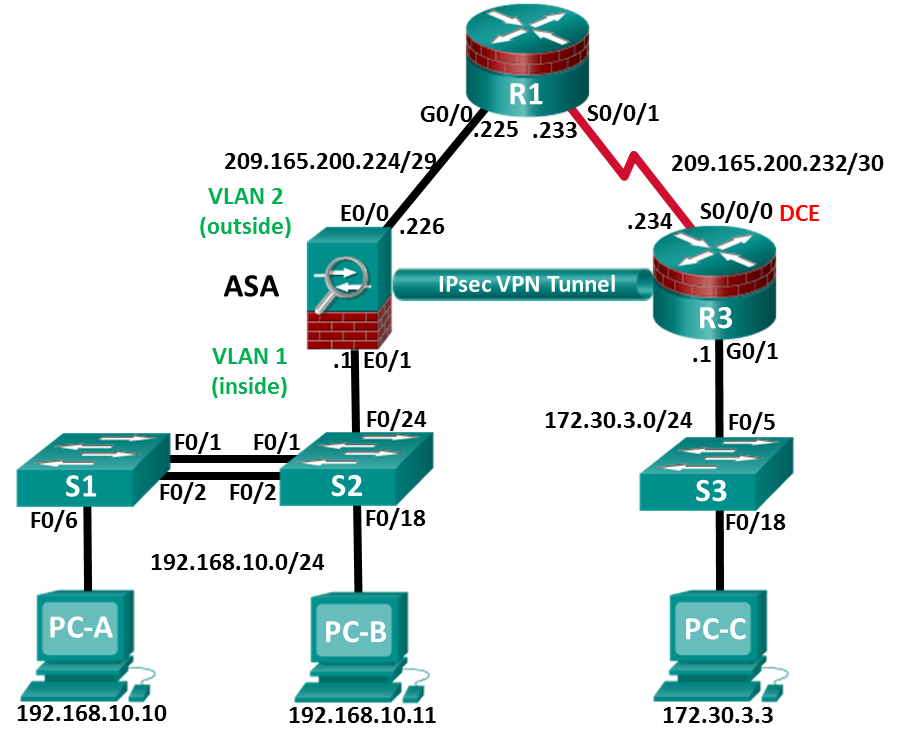
Skills Assessment Using ASA 5505 – Form B (Answer Key)

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

1. Topology



1. Assessment Objectives

Part 1: Verify Network Connectivity (1 points, 5 minutes)

Note: Basic configuration is completed by the instructor in preparation for the exam.

Part 2: Configure Secure Router Administrative Access (17 points, 15 minutes)

Part 3: Configure a Zone-Based Policy Firewall (14 points, 10 minutes)

Part 4: Secure Layer 2 Switches (22 points, 20 minutes)

Part 5: Configure ASA Basic Management and Firewall Settings (18 points, 15 minutes)

Part 6: Configure a Site-To-Site IPsec VPN (28 points, 25 minutes)

1. Scenario

This Skills Assessment (SA) is the final practical exam of student training for the CCNA Security course. The exam is divided into six parts. The parts should be completed sequentially and signed off by your instructor before moving on to the next part. In Part 1 you will verify that the basic device settings have been preconfigured by the instructor. In Part 2, you will secure a network router using the command-line interface (CLI) to configure various IOS features including AAA and SSH. In Part 3, you will configure zone-based policy firewall (ZPF) on an integrated service router (ISR) using the CLI. In Part 4, you will configure and secure Layer 2 switches using the CLI. In Part 5, you will configure the ASA management and firewall settings using the CLI. In Part 6, you will configure a site-to-site IPsec VPN between R3 and the ASA using the CLI and ASDM.

**Instructor Note**: The routers used in this SA are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in this SA. Refer to the Router Interface Summary table at the end of this SA for the correct interface identifiers.

**Instructor Note**: Sample scoring and estimated times for each exam are provided. These can be adjusted by the instructor as necessary to suit the testing environment. Total points for the exam are 100 and total time is estimated at 90 minutes. The instructor may elect to deduct points if excessive time is taken for a part of the assessment.

1. Required Resources

* 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
* 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 1 ASA 5505 (OS version 9.2(3) and ASDM version 7.4(1) and Base license or comparable)
* 3 PCs (Windows 7 with terminal emulation program, such as Tera Term)
* Console cable to configure the Cisco IOS devices via the console ports
* Ethernet and Serial cables as shown in the topology

1. Instructor Notes:

**Router Resource Requirements:**

**Note**: The following requirements are critical to successful completion of this SA.

**Instructor Note**: In the interest of time, the instructor should pre-configure the basic device settings. Basic configurations are provided below for R1 and R3. Static IP address settings have also been provided for the PC hosts.

R1 Startup Configuration

**hostname R1**

**no ip domain lookup**

**interface GigabitEthernet0/0**

**ip address 209.165.200.225 255.255.255.248**

**no shutdown**

**interface Serial0/0/1**

**ip address 209.165.200.233 255.255.255.252**

**no shutdown**

**ip route 172.30.3.0 255.255.255.0 209.165.200.234**

**ntp authentication-key 1 md5 NTPpassword**

**ntp trusted-key 1**

**ntp authenticate**

**ntp master 3**

**end**

R3 Startup Configuration

**hostname R3**

**no ip domain lookup**

**interface G0/1**

**ip address 172.30.3.1 255.255.255.0**

**no shut**

**int S0/0/0**

**ip address 209.165.200.234 255.255.255.252**

**no shutdown**

**ip route 0.0.0.0 0.0.0.0 209.165.200.233**

**end**

S1 Startup Configuration

**hostname S1**

**no ip domain lookup**

**spanning-tree vlan 1 root primary**

**interface range f0/3-5, f0/7-24, g0/1-2**

**shutdown**

**end**

S2 Startup Configuration

**hostname S2**

**no ip domain lookup**

**spanning-tree vlan 1 root secondary**

**end**

PC-A

IP Address: 192.168.10.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

PC-B

IP Address: 192.168.10.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

PC-C

IP Address: 172.30.3.3

Subnet Mask: 255.255.255.0

Default Gateway: 172.30.3.1

1. Verify Network Connectivity

**Total points: 17**

**Time: 15 minutes**

In the interest of time, your instructor has pre-configured basic settings on R1 and R3, and the static IP address information for the PC hosts in the topology. In Part 1, you will verify that PC-C can ping the G0/1 interface on R1.

|  |  |  |
| --- | --- | --- |
| Configuration Task | Specification | Points |
| Ping the G0/1 interface on R3 from PC-C. | See Topology for specific settings. | 1/2 |
| Ping the S0/0/1 interface on R1 from R3. | See Topology for specific settings. | 1/2 |

**Instructor Sign-Off Part 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 1**

**Note**: Do not proceed to Part 2 until your instructor has signed off on Part 1.

1. Configure Secure Router Administrative Access

**Total points: 17**

**Time: 15 minutes**

In Part 2, you will secure administrative access on router R3 using the CLI. Configuration tasks include the following:

| Configuration Item or Task | Specification | Points |
| --- | --- | --- |
| Set minimum password length. | Minimum Length: **10** characters | 1 |
| Assign and encrypt a privileged EXEC password. | Password: **cisco12345**  Encryption type: 9 (**scrypt**) | 1 |
| Add a user in the local database for administrator access | Username: **Admin01**  Privilege level: **15**  Encryption type: 9 (**scrypt**)  Password: **admin01pass** | 1 |
| Configure MOTD banner. | **Unauthorized Access is Prohibited!** | 1/2 |
| Disable HTTP server services. |  | 1/2 |
| Configure SSH. | Domain name: **ccnassecurity.com**  RSA Keys size: **1024**  Version: **2**  Timeout: **90** seconds  Authentication retries: **2** | 4 |
| Configure VTY lines to allow SSH access. | Allow only **SSH** access. | 1 |
| Configure AAA authentication and authorization settings. | Enable AAA  Use **local database** as default setting. | 2 |
| Configure NTP. | Authentication Key: **NTPpassword**  Encryption: **MD5**  Key: **1**  NTP Server: **209.165.200.233**  Configure for periodic calendar updates. | 4 |
| Configure syslog. | Enable timestamp service to log the date and time in milliseconds.  Send syslog messages to: **172.30.3.3**  Set message logging severity level: **Warnings** | 2 |

| Configuration Item or Task | Configuration Commands | Verification Commands |
| --- | --- | --- |
| Set minimum password length. | security passwords min-length 10 | show run | inc passwords |
| Assign and encrypt a privileged EXEC password. | enable algorithm-type scrypt secret cisco12345 | show run | inc enable  Verify encryption type 9. |
| Add a user in the local database for administrator access. | username Admin01 privilege 15 algorithm-type scrypt secret admin01pass | show run | include username  Verify Username, Privilege level, and encryption type. The password can be verified. |
| Configure MOTD banner. | banner motd $Unauthorized Access is Prohibited!$ | show run | inc banner |
| Disable HTTP server services. | no ip http server | show run | inc http |
| Configure SSH. | ip domain-name ccnasecurity.com  crypto key generate rsa general-keys modulus 1024  ip ssh version 2  ip ssh time-out 90  ip ssh authentication-retries 2 | show ip ssh |
| Configure VTY lines to allow SSH access. | line vty 0 4  transport input ssh  exit | show run | sec vty |
| Configure AAA authentication and authorization settings. | aaa new-model  aaa authentication login default local  aaa authorization exec default local | show run | inc aaa |
| Configure NTP. | ntp authentication-key 1 md5 NTPpassword  ntp authenticate  ntp server 209.165.200.233  ntp update-calendar | show ntp associations  show run | sec ntp |
| Configure syslog. | service timestamps log datetime msec  logging 172.30.3.3  logging trap warnings | show run | sec logging  show logging |

**Note**: Before proceeding to Part 3, ask your instructor to verify R3’s configuration and functionality.

**Instructor Sign-Off Part 2: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 17**

1. Configure a Zone-Based Policy Firewall

**Total points: 14**

**Time: 10 minutes**

In Part 3, you will configure a zone-based policy firewall on R3 using the CLI. Configuration tasks include the following:

| Configuration Item or Task | Specification | Points |
| --- | --- | --- |
| Create security zone names. | Inside zone name: **INSIDE**  Outside zone name: **INTERNET** | 2 |
| Create an inspect class map. | Class map name: **INSIDE\_PROTOCOLS**  Inspection type: **match-any**  Protocols allowed: **tcp, udp, icmp** | 3 |
| Create an inspect policy map. | Policy map name: **INSIDE\_TO\_INTERNET**  Bind the class map to the policy map.  Matched packets should be inspected. | 3 |
| Create a zone pair. | Zone pair name: **IN\_TO\_OUT\_ZONE**  Source zone: **INSIDE**  Destination zone: **INTERNET** | 2 |
| Apply the policy map to the zone pair. | Zone pair name: **IN\_TO\_OUT\_ZONE**  Policy map name: **INSIDE\_TO\_INTERNET** | 2 |
| Assign interfaces to the proper security zones. | Interface G0/1: **INSIDE**  Interface S0/0/0: **INTERNET** | 2 |

| Configuration Item or Task | Configuration Commands | Verification Commands |
| --- | --- | --- |
| Create security zone names. | zone security INSIDE  zone security INTERNET | show run | section zone security |
| Create an inspect class map. | class-map type inspect match-any INSIDE\_PROTOCOLS  match protocol tcp  match protocol udp  match protocol icmp | show class-map type inspect |
| Create an inspect policy map. | policy-map type inspect INSIDE\_TO\_INTERNET  class type inspect INSIDE\_PROTOCOLS  inspect | show policy-map type inspect |
| Create a zone pair. | zone-pair security IN\_TO\_OUT\_ZONE source INSIDE destination INTERNET | show zone-pair security |
| Apply the policy map to the zone pair. | zone-pair security IN\_TO\_OUT\_ZONE  service-policy type inspect INSIDE\_TO\_INTERNET | show zone-pair security |
| Assign interfaces to the proper security zones. | interface g0/1  zone-member security INSIDE  interface s0/0/0  zone-member security INTERNET | show zone security |

Troubleshoot as necessary to correct any issues discovered.

**Note**: Before proceeding to Part 4, ask your instructor to verify your ZPF configuration and functionality.

**Instructor Sign-Off Part 2: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 14**

1. Secure Layer 2 Switches

**Total points: 22**

**Time: 20 minutes**

**Note**: Not all security features in this part of the exam will be configured on all switches. However, in a production network, all security feature will be configured on all switches. In the interest of time, the security features are configured on just S2, except where noted.

In Part 4, you will configure security settings on the indicated switch using the CLI. Configuration tasks include the following:

| Configuration Item or Task | Specification | Points |
| --- | --- | --- |
| Assign and encrypt a privileged EXEC password. | Switch: **S2**  Password: **cisco12345**.  Encryption type: 9 (**scrypt**) | 1/2 |
| Add a user in the local database for administrator access | Switch: **S2**  Username: **Admin01**  Privilege level: **15**  Encryption type: 9 (**scrypt**)  Password: **admin01pass** | 1 |
| Configure MOTD banner. | Switch: **S2**  Banner: **Unauthorized Access is Prohibited!** | 1/2 |
| Disable HTTP and HTTP secure server. | Switch: **S2** | 1 |
| Configure SSH. | Switch: **S2**  Domain name: **ccnassecurity.com**  RSA Keys size: **1024**  Version: **2**  Timeout: **90** seconds  Authentication retries: **2** | 2 |
| Configure VTY lines to allow SSH access. | Switch: **S2**  Allow **SSH** access only. | 1/2 |
| Configure AAA authentication and authorization settings. | Switch: **S2**  Enable **AAA**  Use **local database** as default setting | 2 |
| Create VLAN list. | Switches: **S1 &** **S2**  VLAN**: 2,** Name: **NewNative**  VLAN: **10**, Name: **LAN**  VLAN: **99**, Name: **Blackhole** | 1/2 |
| Configure trunk ports. | Switches: **S1 & S2**  Interfaces: **F0/1, F0/2**  Native VLAN: 2  Prevent DTP. | 2 |
| Disable trunking. | Switch: **S2**  Ports: **F0/18, F0/24**  VLAN assignment: **10** | 2 |
| Enable PortFast and BPDU guard. | Switch: **S2**  Ports: **F0/18, F0/24** | 2 |
| Configure basic port security. | Switch: **S2**  Port: **F0/18**  Maximum limit: **1**  Remember MAC Address  Violation Action: **Shutdown** | 3 |
| Disable unused ports on S2, and assign ports to VLAN 99. | Switch: **S2**  Ports: **F0/3-17, F0/19-23, G0/1-2** | 1 |
| Configure Loop guard. | Switch: **S2**  Loop guard: **Default** | 1 |
| Configure DHCP snooping. | Enable DHCP Snooping globally  Enable DHCP for VLAN: **10**  DHCP trusted interface: **F0/24** | 3 |

**NETLAB+ Note:** Use a Maximum limit of **2** when configuring basic port security. Otherwise, the hidden Control Switch will cause a violation to occur and the port will be shutdown.

| Configuration Item or Task | Configuration Commands | Verification Commands |
| --- | --- | --- |
| Assign and encrypt a privileged EXEC password. (Switch: **S2 only)** | enable algorithm-type scrypt secret cisco12345 | show run | inc enable  Verify encryption type 9. |
| Add a user in the local database for administrator access.  (Switch: **S2 only)** | username Admin01 privilege 15 algorithm-type scrypt secret admin01pass | show run | include username  Verify username, privilege level, and encryption type. The password can be verified. |
| Configure MOTD banner.  (Switch: **S2 only)** | banner motd $Unauthorized Access is Prohibited!$ | show run | inc banner |
| Disable HTTP and HTTP secure server.  (Switch: **S2 only)** | no ip http server  no ip http secure-server | show run | inc http |
| Configure SSH.  (Switch: **S2 only)** | ip domain-name ccnasecurity.com  crypto key generate rsa general-keys modulus 1024  ip ssh version 2  ip ssh time-out 90  ip ssh authentication-retries 2 | show ip ssh |
| Configure VTY lines to allow SSH access.  (Switch: **S2 only)** | line vty 0 15  transport input ssh  exit | show run | sec vty |
| Configure AAA authentication and authorization settings.  (Switch: **S2 only)** | aaa new-model  aaa authentication login default local  aaa authorization exec default local | show run | inc aaa |
| Create VLAN list.  (Switch: **S1 & S2**) | vlan 2  name NewNative  vlan 10  name LAN  vlan 99  name Blackhole  exit | show vlan |
| Configure trunk ports.  (Switch: **S1 & S2**) | interface range f0/1-2  switchport mode trunk  switchport trunk native vlan 2  switchport nonegotiate | show run | beg interface |
| Disable trunking.  (Switch: **S2 only)** | interface ran f0/18, f0/24  switchport mode access  switchport access vlan 10 | show run interface f0/18  show run interface f0/24 |
| Enable PortFast and BPDU guard.  (Switch: **S2 only)** | interface ran f0/18, f0/24  spanning-tree portfast  spanning-tree bpduguard enable | show run interface f0/18  show run interface f0/24 |
| Configure basic port security.  (Switch: **S2 only)** | Interface f0/18  switchport port-security  switchport port-security maximum 1  switchport port-security mac-address sticky  switchport port-security violation shutdown | show port-security interface fa0/18 |
| Disable unused ports on S2, and assign ports to VLAN 99.  (Switch: **S2 only)** | interface range f0/3-17, f0/19-23, g0/1-2  switchport mode access  switchport access vlan 99  shutdown | show ip interface brief  (Determine whether interfaces are administratively down.) |
| Configure Loop guard.  (Switch: **S2 only)** | spanning-tree loopguard default | show spanning-tree summary  (Determine whether Loopguard Default is enabled.) |
| Configure DHCP snooping.  (Switch: **S2 only)** | ip dhcp snooping  ip dhcp snooping vlan 10  int f0/24  ip dhcp snooping trust  end | show ip dhcp snooping |

Troubleshoot as necessary to correct any issues discovered.

**Note**: Before proceeding to Part 5, ask your instructor to verify your switch configuration and functionality.

**Instructor Sign-Off Part 4: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 22**

1. Configure ASA Basic Management and Firewall Settings

**Total points: 18**

**Time: 15 minutes**

**Note:** By default, the privileged EXEC password is blank. Press **Enter** at the password prompt.

In Part 5, you will configure the ASA’s basic setting and firewall using the CLI. Configuration tasks include the following:

| Configuration Item or Task | Specification | Points |
| --- | --- | --- |
| Configure the ASA hostname. | Name: **CCNAS-ASA** | 1/2 |
| Configure the domain name. | Domain Name: **ccnasecurity.com** | 1/2 |
| Configure the privileged EXEC password. | Password: **cisco12345** | 1/2 |
| Add a user to the local database for administrator console access. | User: **Admin01**  Password: **admin01pass** | 1/2 |
| Configure AAA to use the local database for SSH user authentication for console access. |  | 1 |
| Configure VLAN 1. | VLAN: **1**  Name: **inside**  IP address: **192.168.10.1**  Subnet Mask: **255.255.255.0**  Security Level: **100** | 2 |
| Configure VLAN 2. | VLAN: **2**  Name: **outside**  IP address: **209.165.200.226**  Subnet Mask: **255.255.255.248**  Security Level: **0**  Activate the VLAN | 3 |
| Assign VLANs to interfaces and activate each interface. | VLAN 1 interface: **E0/1**  VLAN 2 interface: **E0/0** | 2 |
| Generate an RSA key pair to support the SSH connections. | Key: **RSA**  Modulus size: **1024** | 1 |
| Configure ASA to accept SSH connections from hosts on the inside LAN. | Inside Network: **192.168.10.0/24**  Timeout: **10** minutes  Version: **2** | 1 |
| Configure the default route. | Default route IP address: **209.165.200.225** | 1 |
| Configure ASDM access to the ASA. | Enable HTTPS server services.  Enable HTTPS on the inside network. | 2 |
| Create a network object to identify internal addresses for PAT. Bind interfaces dynamically by using the interface address as the mapped IP. | Object name: **INSIDE-NET**  Subnet: **192.168.10.0/24**  Interfaces: **inside, outside** | 2 |
| Modify the default global policy to allow returning ICMP traffic through the firewall. | Policy-map: **global\_policy**  Class: **inspection\_default**  Inspect: **icmp** | 1 |

| Configuration Item or Task | Configuration Commands | Verification Commands | |
| --- | --- | --- | --- |
| Configure the ASA hostname. | hostname CCNAS-ASA | (Look at command prompt to verify CCNAS-ASA name.) |
| Configure the domain name. | domain-name ccnasecurity.com | show run domain |
| Configure the privileged EXEC password. | enable password cisco12345 | show run enable |
| Add a user to the local database for administrator console access. | username Admin01 password admin01pass | show run username |
| Configure AAA to use the local database for SSH user authentication and for console access. | aaa authentication ssh console LOCAL | show run aaa |
| Configure VLAN 1. | interface vlan 1  nameif inside  ip add 192.168.10.1 255.255.255.0  security-level 100 | show run interface vlan 1 |
| Configure VLAN 2. | int vlan 2  nameif outside  ip add 209.165.200.226 255.255.255.248  security-level 0  no shutdown | show run interface vlan 2 |
| Assign VLANs to interfaces and activate each interface. | interface e0/1  switchport access vlan 1  no shutdown  interface e0/0  switchport access vlan 2  no shutdown | show switch vlan |
| Generate an RSA key pair to support the SSH connections. | crypto key generate rsa modulus 1024 | show crypto key mypubkey rsa |
| Configure ASA to accept SSH connections from hosts on the inside LAN. | ssh 192.168.10.0 255.255.255.0 inside  ssh timeout 10  ssh version 2 | show ssh |
| Configure the default route. | route outside 0.0.0.0 0.0.0.0 209.165.200.225 | show route  (Look for quad-zero static route.) |
| Configure ASDM access to the ASA. | http server enable  http 192.168.10.0 255.255.255.0 inside | show run http |
| Create a network object to identify internal addresses for PAT. Bind the interfaces dynamically by using the interface address as the mapped IP. | object network INSIDE-NET  subnet 192.168.10.0 255.255.255.0  nat (inside,outside) dynamic interface | show nat  show run object |
| Modify the default global policy to allow returning ICMP traffic through the firewall. | policy-map global\_policy  class inspection\_default  inspect icmp | show run policy-map |

Troubleshoot as necessary to correct any issues discovered.

**Note**: Before proceeding to Part 6, ask your instructor to verify your ASA configuration and functionality.

**Instructor Sign-Off Part 5: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 18**

1. Configure a Site-to-Site VPN

**Total points: 28**

**Time: 25 minutes**

In Part 6, you will configure a Site-to-Site IPsec VPN between R3 and the ASA. You will use the CLI to configure R3 and use ASDM to configure the ASA.

* 1. Configure Site-to-Site VPN on R3 using CLI.

Configuration parameters include the following:

| Configuration Item or Task | Specification | Points |
| --- | --- | --- |
| Enable IKE. | Note: ISAKMP is enabled by default. | 1 |
| Create an ISAKMP policy. | ISAKMP Policy Priority: **1**  Authentication type: **pre-share**  Encryption: **3des**  Hash algorithm: **sha**  Diffie-Hellman Group Key Exchange: **2** | 5 |
| Configure the pre-shared key. | Preshare key: **ciscopreshare**  Address: **209.165.200.226** | 2 |
| Configure the IPsec transform set. | Tag: **TRNSFRM-SET**  ESP transform: **ESP\_3DES**  Hash function: **ESP\_SHA\_HMAC** | 3 |
| Define interesting traffic. | ACL: **101**  Source Network: **172.30.3.0 0.0.0.255**  Destination Network: **192.168.10.0 0.0.0.255** | 1 |
| Create a crypto map. | Crypto map name: **CMAP**  Sequence number: **1**  Type: **ipsec-isakmp**  ACL to match: **101**  Peer: **209.165.200.226**  Transform-set: **TRNSFRM-SET** | 5 |
| Apply crypto map to the interface. | Interface: **S0/0/0**  Crypto map name: **CMAP** | 1 |

| Configuration Item or Task | Configuration Commands | Verification Commands | |
| --- | --- | --- | --- |
| Enable IKE. | crypto isakmp enable | show run | include crypto |
| Create an ISAKMP policy. | crypto isakmp policy 1  authentication pre-share  encryption 3des  hash sha  group 2 | show crypto isakmp policy |
| Configure the pre-shared key. | crypto isakmp key ciscopreshare address 209.165.200.226 | show run | include crypto |
| Configure the IPsec transform set. | crypto ipsec transform-set TRNSFRM-SET esp-3des esp-sha-hmac | show run | include crypto |
| Define interesting traffic. | access-list 101 permit ip 172.30.3.0 0.0.0.255 192.168.10.0 0.0.0.255 | show run | inc access-list |
| Create a crypto map. | crypto map CMAP 1 ipsec-isakmp  match address 101  set transform-set TRNSFRM-SET  set peer 209.165.200.226 | show crypto map |
| Apply crypto map to interface. | interface s0/0/0  crypto map CMAP | show crypto map  show run interface s0/0/0 |

* 1. Configure Site-to-Site VPN on ASA using ASDM

Use a browser on PC-B to establish an ASDM session to the ASA. When the session is established, use the **Site-to-Site VPN Wizard** to configure the ASA for IPsec Site-to-Site VPN. Configuration parameters include the following:

| Configuration Item or Task | Specification | Points |
| --- | --- | --- |
| Use a browser on PC-B, connect to the ASA, and run ASDM. | Connection: **HTTPS**  IP Address: **192.168.10.1**  Username: **Admin01**  Password: **admin01pass**  **Note:** You will need to accept all security messages. | 2 |
| Use the Site-to-site VPN Wizard to configure the site-to-site VPN settings on the ASA. | Peer IP Address: **209.165.200.234**  VPN Access Interface: **outside**  Local Network: **inside-network/24**  Remote Network: **172.30.3.0/24**  Pre-shared Key: **ciscopreshare**  Exempt ASA side/host network from NAT: **Enable** | 5 |
| Ping PC-B from PC-C. | This should generate interesting traffic and start site-to-site VPN. | 1/2 |
| Ping PC-C from PC-B. |  | 1/2 |
| Display the ISAKMP and IPsec SAs on R3. | show crypto isakmp sa  show crypto ipsec sa  (Look for an active session.) | 1 |
| Verify that a site-to-site session has been established using ASDM from PC-B. | ASDM **Monitoring**  **VPN** tab  Filter by: **IPsec Site-to-Site** | 1 |

Troubleshoot as necessary to correct any issues discovered.

**Instructor Note**: Have the student ping PC-B to demonstrate that PC-C has established an SSL VPN connection to the ASA. The student should also be able to use ASDM on PC-B to display the established VPN session.

**Instructor Sign-Off Part 6: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Points: \_\_\_\_\_\_\_\_\_ of 28**

1. Router Interface Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 (S0/0/1) |
| 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. Router R1 (Initial Configuration)

R1#sh run

Building configuration...

Current configuration : 1582 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

no aaa new-model

memory-size iomem 15

!

no ip domain lookup

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

redundancy

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 209.165.200.225 255.255.255.248

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

ip address 209.165.200.233 255.255.255.252

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 172.30.3.0 255.255.255.0 209.165.200.234

ip route 192.168.10.0 255.255.255.0 209.165.200.226

!

control-plane

!

line con 0

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

login

transport input none

!

scheduler allocate 20000 1000

ntp authentication-key 1 md5 153C3F3C142B38373F3C2726 7

ntp authenticate

ntp trusted-key 1

ntp master 3

!

end

1. Router R3 (After completion of Part 3)

R3#show run

Building configuration...

Current configuration : 2438 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9 $9$KNLoNKx4jYzt8k$wz88KSBb5KMY9121/qkhOTiXkV0XCothrCZLB1lbyko

!

aaa new-model

!

aaa authentication login default local

aaa authorization exec default local

!

aaa session-id common

memory-size iomem 15

!

no ip domain lookup

ip domain name ccnasecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

username Admin01 privilege 15 secret 9 $9$kbOeb3f5lka0rU$hLnVWpzbOBfZWFY1qX4xngsVwQPTojqeJGnujbcIllI

!

redundancy

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

class-map type inspect match-any INSIDE\_PROTOCOLS

match protocol tcp

match protocol udp

match protocol icmp

!

policy-map type inspect INSIDE\_TO\_INTERNET

class type inspect INSIDE\_PROTOCOLS

inspect

class class-default

drop

!

zone security INSIDE

zone security INTERNET

zone-pair security IN\_TO\_OUT\_ZONE source INSIDE destination INTERNET

service-policy type inspect INSIDE\_TO\_INTERNET

!

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 172.30.3.1 255.255.255.0

zone-member security INSIDE

duplex auto

speed auto

!

interface Serial0/0/0

ip address 209.165.200.234 255.255.255.252

zone-member security INTERNET

clock rate 125000

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 209.165.200.233

!

logging trap warnings

logging host 172.30.3.3

!

control-plane

!

banner motd ^CUnauthorized Access is Prohibited!^C

!

line con 0

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

transport input ssh

!

scheduler allocate 20000 1000

ntp authentication-key 1 md5 153C3F3C142B38373F3C2726 7

ntp authenticate

ntp update-calendar

ntp server 209.165.200.233

!

**end**

Switch S1 (After completion of Part 4)

S1# **show run**

hostname S1

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

spanning-tree vlan 1 priority 24576

!

interface FastEthernet0/1

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/2

switchport mode trunk

switchport nonegotiate

!

end

Switch S2 (After completion of Part 4)

S2# **show run**

Building configuration...

Current configuration : 2599 bytes

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S2

!

boot-start-marker

boot-end-marker

!

enable secret 9 $9$6E0RH.UQ3Nt221$fSKp.he411vh54DhobJk678MmZzj3sHxY3JMX/QdcTE

!

username Admin01 privilege 15 secret 9 $9$ELG3vxsMl43KNo$V3AYoDX3ogPeDL2FWjpeM9R.2/Sek8UY65l6OcqxK3E

aaa new-model

!

aaa authentication login default local

aaa authorization exec default local

!

aaa session-id common

system mtu routing 1500

!

ip dhcp snooping vlan 10

ip dhcp snooping

no ip domain-lookup

ip domain-name ccnasecurity.com

!

spanning-tree mode pvst

spanning-tree loopguard default

spanning-tree extend system-id

spanning-tree vlan 1 priority 28672

!

vlan internal allocation policy ascending

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

interface FastEthernet0/1

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/2

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/3

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/5

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/6

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/7

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/8

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/10

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/11

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 10

switchport mode access

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0050.56be.dca4

switchport port-security

spanning-tree portfast

spanning-tree bpduguard enable

!

interface FastEthernet0/19

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/21

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/22

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/23

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/24

switchport access vlan 10

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

ip dhcp snooping trust

!

interface GigabitEthernet0/1

switchport access vlan 99

switchport mode access

shutdown

!

interface GigabitEthernet0/2

switchport access vlan 99

switchport mode access

shutdown

!

interface Vlan1

no ip address

!

no ip http server

no ip http secure-server

!

banner motd ^CUnauthorized Access is Prohibited!^C

!

line con 0

line vty 0 4

transport input ssh

line vty 5 15

transport input ssh

!

end

ASA (Config after Part 5)

CCNAS-ASA# sh run

: Saved

:

: Serial Number: JMX15364087

: Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz

:

ASA Version 9.2(3)

!

hostname CCNAS-ASA

domain-name ccnasecurity.com

enable password 9D8jmmmgkfNZLETh encrypted

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

names

!

interface Ethernet0/0

switchport access vlan 2

!

interface Ethernet0/1

!

interface Ethernet0/2

shutdown

!

interface Ethernet0/3

shutdown

!

interface Ethernet0/4

shutdown

!

interface Ethernet0/5

shutdown

!

interface Ethernet0/6

shutdown

!

interface Ethernet0/7

shutdown

!

interface Vlan1

nameif inside

security-level 100

ip address 192.168.10.1 255.255.255.0

!

interface Vlan2

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

!

ftp mode passive

dns server-group DefaultDNS

domain-name ccnasecurity.com

object network INSIDE-NET

subnet 192.168.10.0 255.255.255.0

pager lines 24

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

!

object network INSIDE-NET

nat (inside,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

dynamic-access-policy-record DfltAccessPolicy

user-identity default-domain LOCAL

aaa authentication ssh console LOCAL

http server enable

http 192.168.10.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet timeout 5

ssh stricthostkeycheck

ssh 192.168.10.0 255.255.255.0 inside

ssh timeout 10

ssh version 2

ssh key-exchange group dh-group1-sha1

console timeout 0

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

username Admin01 password fQAK6Vi5QObtK4Ob encrypted

!

class-map inspection\_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

parameters

message-length maximum client auto

message-length maximum 512

policy-map global\_policy

class inspection\_default

inspect dns preset\_dns\_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect ip-options

inspect netbios

inspect rsh

inspect rtsp

inspect skinny

inspect esmtp

inspect sqlnet

inspect sunrpc

inspect tftp

inspect sip

inspect xdmcp

inspect icmp

!

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

call-home

profile CiscoTAC-1

no active

destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService

destination address email callhome@cisco.com

destination transport-method http

subscribe-to-alert-group diagnostic

subscribe-to-alert-group environment

subscribe-to-alert-group inventory periodic monthly

subscribe-to-alert-group configuration periodic monthly

subscribe-to-alert-group telemetry periodic daily

Cryptochecksum:98a5d8473709326520708d615104fa12

: end

R3 (Final Configuration)

R3# **show run**

Building configuration...

Current configuration : 2908 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9 $9$KNLoNKx4jYzt8k$wz88KSBb5KMY9121/qkhOTiXkV0XCothrCZLB1lbyko

!

aaa new-model

!

aaa authentication login default local

aaa authorization exec default local

!

aaa session-id common

memory-size iomem 15

!

no ip domain lookup

ip domain name ccnasecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

username Admin01 privilege 15 secret 9 $9$kbOeb3f5lka0rU$hLnVWpzbOBfZWFY1qX4xngsVwQPTojqeJGnujbcIllI

!

redundancy

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

class-map type inspect match-any INSIDE\_PROTOCOLS

match protocol tcp

match protocol udp

match protocol icmp

!

policy-map type inspect INSIDE\_TO\_INTERNET

class type inspect INSIDE\_PROTOCOLS

inspect

class class-default

drop

!

zone security INSIDE

zone security INTERNET

zone-pair security IN\_TO\_OUT\_ZONE source INSIDE destination INTERNET

service-policy type inspect INSIDE\_TO\_INTERNET

!

crypto isakmp policy 1

encr 3des

authentication pre-share

group 2

crypto isakmp key ciscopreshare address 209.165.200.226

!

crypto ipsec transform-set TRNSFRM-SET esp-3des esp-sha-hmac

mode tunnel

!

crypto map CMAP 1 ipsec-isakmp

set peer 209.165.200.226

set transform-set TRNSFRM-SET

match address 101

!

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 172.30.3.1 255.255.255.0

zone-member security INSIDE

duplex auto

speed auto

!

interface Serial0/0/0

ip address 209.165.200.234 255.255.255.252

zone-member security INTERNET

clock rate 125000

crypto map CMAP

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 209.165.200.233

!

logging trap warnings

logging host 172.30.3.3

!

access-list 101 permit ip 172.30.3.0 0.0.0.255 192.168.10.0 0.0.0.255

!

control-plane

!

banner motd ^CUnauthorized Access is Prohibited!^C

!

line con 0

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

transport input ssh

!

scheduler allocate 20000 1000

ntp authentication-key 1 md5 153C3F3C142B38373F3C2726 7

ntp authenticate

ntp update-calendar

ntp server 209.165.200.233

!

end

ASA (Final Configuration)

CCNAS-ASA# show run

: Saved

:

: Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz

:

ASA Version 9.2(3)

!

hostname CCNAS-ASA

domain-name ccnasecurity.com

enable password 9D8jmmmgkfNZLETh encrypted

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

passwd 2KFQnbNIdI.2KYOU encrypted

names

!

interface Ethernet0/0

switchport access vlan 2

!

interface Ethernet0/1

!

interface Ethernet0/2

shutdown

!

interface Ethernet0/3

shutdown

!

interface Ethernet0/4

shutdown

!

interface Ethernet0/5

shutdown

!

interface Ethernet0/6

shutdown

!

interface Ethernet0/7

shutdown

!

interface Vlan1

nameif inside

security-level 100

ip address 192.168.10.1 255.255.255.0

!

interface Vlan2

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

!

ftp mode passive

dns server-group DefaultDNS

domain-name ccnasecurity.com

object network INSIDE-NET

subnet 192.168.10.0 255.255.255.0

object network NETWORK\_OBJ\_172.30.3.0\_24

subnet 172.30.3.0 255.255.255.0

object network NETWORK\_OBJ\_192.168.10.0\_24

subnet 192.168.10.0 255.255.255.0

access-list outside\_cryptomap extended permit ip 192.168.10.0 255.255.255.0 172.30.3.0 255.255.255.0

pager lines 24

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

nat (inside,outside) source static NETWORK\_OBJ\_192.168.10.0\_24 NETWORK\_OBJ\_192.168.10.0\_24 destination static NETWORK\_OBJ\_172.30.3.0\_24 NETWORK\_OBJ\_172.30.3.0\_24 no-proxy-arp route-lookup

!

object network INSIDE-NET

nat (inside,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

dynamic-access-policy-record DfltAccessPolicy

user-identity default-domain LOCAL

aaa authentication ssh console LOCAL

http server enable

http 192.168.10.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport

crypto ipsec ikev2 ipsec-proposal DES

protocol esp encryption des

protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal 3DES

protocol esp encryption 3des

protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal AES

protocol esp encryption aes

protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal AES192

protocol esp encryption aes-192

protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal AES256

protocol esp encryption aes-256

protocol esp integrity sha-1 md5

crypto ipsec security-association pmtu-aging infinite

crypto map outside\_map 1 match address outside\_cryptomap

crypto map outside\_map 1 set peer 209.165.200.234

crypto map outside\_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

crypto map outside\_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES

crypto map outside\_map interface outside

crypto ca trustpool policy

crypto ikev2 policy 1

encryption aes-256

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 10

encryption aes-192

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 20

encryption aes

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 30

encryption 3des

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 40

encryption des

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 enable outside

crypto ikev1 enable outside

crypto ikev1 policy 10

authentication crack

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 20

authentication rsa-sig

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 30

authentication pre-share

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 40

authentication crack

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 50

authentication rsa-sig

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 60

authentication pre-share

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 70

authentication crack

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 80

authentication rsa-sig

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 90

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 100

authentication crack

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 110

authentication rsa-sig

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 120

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 130

authentication crack

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 140

authentication rsa-sig

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 150

authentication pre-share

encryption des

hash sha

group 2

lifetime 86400

telnet timeout 5

ssh stricthostkeycheck

ssh 192.168.10.0 255.255.255.0 inside

ssh timeout 10

ssh version 2

ssh key-exchange group dh-group1-sha1

console timeout 0

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

group-policy GroupPolicy\_209.165.200.234 internal

group-policy GroupPolicy\_209.165.200.234 attributes

vpn-tunnel-protocol ikev1 ikev2

username Admin01 password fQAK6Vi5QObtK4Ob encrypted

tunnel-group 209.165.200.234 type ipsec-l2l

tunnel-group 209.165.200.234 general-attributes

default-group-policy GroupPolicy\_209.165.200.234

tunnel-group 209.165.200.234 ipsec-attributes

ikev1 pre-shared-key \*\*\*\*\*

ikev2 remote-authentication pre-shared-key \*\*\*\*\*

ikev2 local-authentication pre-shared-key \*\*\*\*\*

!

class-map inspection\_default

match default-inspection-traffic

!

policy-map type inspect dns migrated\_dns\_map\_1

parameters

message-length maximum client auto

message-length maximum 512

policy-map global\_policy

class inspection\_default

inspect dns migrated\_dns\_map\_1

inspect ftp

inspect h323 h225

inspect h323 ras

inspect ip-options

inspect netbios

inspect rsh

inspect rtsp

inspect skinny

inspect esmtp

inspect sqlnet

inspect sunrpc

inspect tftp

inspect sip

inspect xdmcp

inspect icmp

!

service-policy global\_policy global

prompt hostname context

call-home reporting anonymous prompt 2

call-home

profile CiscoTAC-1

no active

destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService

destination address email callhome@cisco.com

destination transport-method http

subscribe-to-alert-group diagnostic

subscribe-to-alert-group environment

subscribe-to-alert-group inventory periodic monthly

subscribe-to-alert-group configuration periodic monthly

subscribe-to-alert-group telemetry periodic daily

Cryptochecksum:dc045167490d9cbf97a4c2a7fd9bc6b7

: end