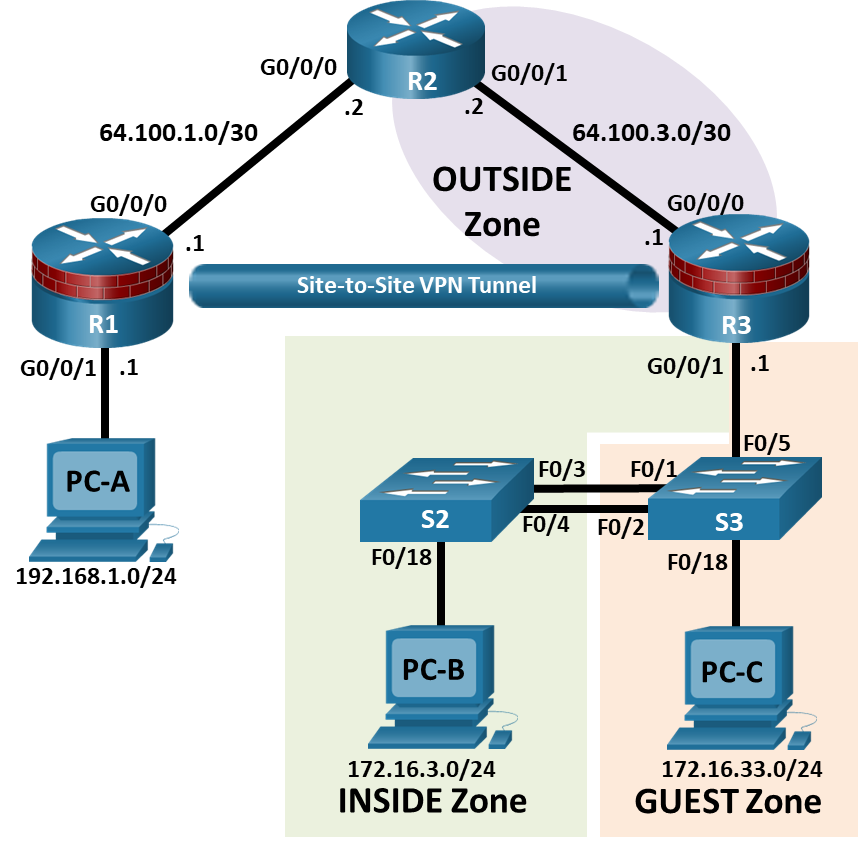
# Topology



# Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/0/0 | 64.100.1.1 | 255.255.255.252 | N/A |
| R1 | G0/0/1 | 192.168.1.0 | 255.255.255.0 | N/A |
| R2 | G0/0/0 | 64.100.1.2 | 255.255.255.252 | N/A |
| R2 | G0/0/1 | 64.100.3.2 | 255.255.255.252 | N/A |
| R3 | G0/0/0 | 64.100.3.1 | 255.255.255.252 | N/A |
| R3 | G0/0/1.3 | 172.16.3.1 | 255.255.255.0 | N/A |
| R3 | G0/0/1.33 | 172.16.33.1 | 255.255.255.0 | N/A |
| S2 | VLAN 3 | 172.16.3.2 | 255.255.255.0 | 172.16.3.1 |
| S3 | VLAN 3 | 172.16.3.3 | 255.255.255.0 | 172.16.3.1 |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 172.16.3.10 | 255.255.255.0 | 172.16.3.1 |
| PC-C | NIC | 172.16.33.10 | 255.255.255.0 | 172.16.33.1 |

Blank Line, No additional information

# Assessment Objectives

Part 1: Secure Layer 2 Switches (25 points, 25 minutes)

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

Part 3: Configure a Site-To-Site IPsec VPN (30 points, 30 minutes)

Part 4: Configure a Zone-Based Policy Firewall (30 points, 30 minutes)

# Scenario

### Configure the PCs.

Configure the IP address and default gateway for each PC according to the Addressing Table.

### Load provided device configurations.

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

S2 Startup Configuration

enable

configure terminal

hostname S2

no ip domain lookup

interface vlan 3

ip add 172.16.3.2 255.255.255.0

no shutdown

ip default-gateway 172.16.3.1

end

S3 Startup Configuration

enable

configure terminal

hostname S3

no ip domain lookup

interface vlan 3

ip add 172.16.3.3 255.255.255.0

no shut

ip default-gateway 172.16.3.1

end

R1 Startup Configuration

enable

configure terminal

host R1

no ip domain lookup

interface GigabitEthernet0/0/0

description Link to R2

ip address 64.100.1.1 255.255.255.252

no shutdown

interface GigabitEthernet0/0/1

description Link to R1 LAN

ip address 192.168.1.1 255.255.255.0

no shutdown

router ospf 1

passive-interface GigabitEthernet0/0/1

network 64.100.1.0 0.0.0.3 area 0

network 192.168.1.0 0.0.0.255 area 0

end

R2 Startup Configuration

enable

configure terminal

hostname R2

no ip domain lookup

interface GigabitEthernet0/0/0

description Link to R1

ip address 64.100.1.2 255.255.255.252

no shutdown

interface GigabitEthernet0/0/1

description Link to R3

ip address 64.100.3.2 255.255.255.252

no shutdown

router ospf 1

network 64.100.1.0 0.0.0.3 area 0

network 64.100.3.0 0.0.0.3 area 0

username webuser privilege 15 algorithm-type scrypt secret webuserpass

ip http server

ip http secure-server

ip http authentication local

end

R3 Startup Configuration

enable

config terminal

hostname R3

no ip domain lookup

interface GigabitEthernet0/0/0

description Link to R2

ip address 64.100.3.1 255.255.255.252

no shutdown

interface GigabitEthernet0/0/1.3

description Link to VLAN 3

encapsulation dot1q 3

ip address 172.16.3.1 255.255.255.0

interface GigabitEthernet0/0/1.33

description Link to VLAN 33

encapsulation dot1q 33

ip address 172.16.33.1 255.255.255.0

interface GigabitEthernet0/0/1

no shutdown

router ospf 1

network 64.100.3.0 0.0.0.3 area 0

network 172.16.0.0 0.0.255.255 area 0

passive-interface g0/0/1

end

### Secure Layer 2 Switches.

**Note**: The security features in this part of the exam will be configured on switch S2 and S3. However, in a production network, all switches would be secured.

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

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Assign and encrypt the privileged EXEC password. | Switch: **S2**   * Password: **cisco12345** * Encryption type: **9** (**scrypt**) | 0.5 | blank |
| Add a user to the local database for administrator access | Switch: **S2**   * Username: a**dmin01** * Privilege level: **15** * Encryption type: **9** (**scrypt**) * Password: **admin01pass** | 0.5 | blank |
| Configure SSHv2. | Switch: **S2**   * Domain name: **netsec.com** * RSA Keys size: **1024** * Version: **2** * Timeout: **90** seconds * Authentication retries: **2** | 2 | blank |
| Configure the AAA authentication settings. | Switch: **S2**   * Enable AAA * Use **local database** as default setting. * Use case-sensitive local username authentication | 2 | blank |
| Enhanced Login settings | Switch: **S2**   * Block for **three** minutes after **four** failed attempts in **two**-minute period. | 1 | blank |
| Encrypt all passwords | Switch: **S2** | 0.5 | blank |
| Configure VTY lines to allow SSH access. | Switch: **S2**   * Allow **SSH** access only. | 0.5 | blank |
| Create the VLAN list. | Switches: **S2 &** **S3**   * VLAN**: 3,** Name: **INSIDE** * VLAN: **33**, Name: **GUEST** * VLAN: **99**, Name: **NULL** | 0.5 | blank |
| Configure trunk ports. | Interfaces:   * **S2: F0/3-4** * **S3: F0/1-F02 and F0/5**   Native VLAN: **99**  Disable DTP. | 2 | blank |
| Disable trunking. | Switch: **S2 & S3**   * Ports: **F0/18** | 1 | blank |
| VLAN Assignments | VLAN 3: **S2 F0/18**  VLAN 33: **S3 F0/18** | 1 | blank |
| Enable PortFast and BPDU guard. | Switch: **S2 & S3**  Ports: **F0/18** | 1 | blank |
| Configure basic port security. | Switch: **S2**   * Port: **F0/18** * Maximum limit: **1**   (NETLAB+ user: maximum limit: **2**)   * Remember MAC Address * Violation Action: **Shutdown** | 2 | blank |
| Disable unused ports on S2 and assign ports to VLAN 99. | Switch: **S2**   * Ports: **F0/1-2, F0/5-17, F0/19-24, G0/1-2** | 1 | blank |
| Configure Loop guard. | Switch: **S2**   * Loop guard: **Default** | 0.5 | blank |
|  | **Total** | **16** | **blank** |

**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.

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| 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 SSHv2.  (Switch: **S2** only) | ip domain-name netsec.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 the AAA authentication settings. | aaa new-model  aaa authentication login default local-case | show run | inc aaa |
| Enhanced Login settings | login block-for 180 attempts 4 within 120 | show login |
| Encrypt all passwords | service password-encryption | show run | incl password-e |
| Configure VTY lines to allow SSH access.  (Switch: **S2** only) | line vty 0 15  transport input ssh  exit | show run | section vty |
| Create VLAN list.  (Switches: **S2** & **S3**) | vlan 3  name INSIDE  vlan 33  name GUEST  vlan 99  name NULL  exit | show vlan |
| Configure trunk ports.  (Switches: **S2** & **S3**) | **Switch S2:**  interface range f0/3-4  switchport mode trunk  switchport trunk native vlan 99  switchport nonegotiate  **Switch S3:**  interface range f0/1-2, f0/5  switchport mode trunk  switchport trunk native vlan 99  switchport nonegotiate | show run | beg interface |
| Disable trunking. (Switches: **S2** & **S3**) | **Switch S2:**  interface f0/18  switchport mode access  switchport access vlan 3  **Switch S3:**  interface f0/18  switchport mode access  switchport access vlan 33 | show run interface f0/18 |
| Enable PortFast and BPDU guard.  (Switch: **S2** & **S3**) | **Switch S2:**  interface f0/18  spanning-tree portfast  spanning-tree bpduguard enable  **Switch S3:**  interface f0/18  spanning-tree portfast  spanning-tree bpduguard enable | show run interface f0/18 |
| 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 f0/18 |
| Disable unused ports on S2 and assign ports to VLAN 99.  (Switch: **S2 only)** | interface range f0/1-2, f0/5-17, f0/19-24, g0/1-2  switchport mode access  switchport access vlan 99  shutdown | show ip interface brief  (Determine whether interfaces are administratively down.) |
| Configure Loop guard globally.  (Switch: **S2 only)** | spanning-tree loopguard default | show spanning-tree summary  (Determine whether Loopguard Default is enabled.) |

Troubleshoot as necessary to correct any issues discovered.

### Verify Network Connectivity.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Task | Specification | Pts | Earned |
| Verify connectivity between PC-C and PC-B |  | 0.5 | Blank |
| From PC-B and PC-C, SSH into S2 | SSH should be successful. | 0.5 | Blank |
|  | **Total** | **1** | **blank** |

Instructor Sign-Off Part 1:

Type your answers here.

Points for Part 1: (Total points 25)

Type your answers here.

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

## Configure Secure Router Access

**Total points: 15**

**Time: 15 minutes**

In Part 2, you will secure administrative access on router R3. You will also configure OSPF routing protocol authentication between routers R2 and R3.

### Configure secure router administrative access.

In this step, you will secure administrative access on R3.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Set minimum password length. | Minimum Length: **10** characters | 0.5 | blank |
| Assign and encrypt a privileged EXEC password. | Password: **cisco12345**  Encryption type: **9** (**scrypt**) | 0.5 | blank |
| Add a user in the local database for administrator access | Username: **admin01**  Privilege level: **15**  Encryption type: **9** (**scrypt**)  Password: **admin01pass** | 1 | blank |
| Configure SSH. | Domain name: **netsec.com**  RSA Keys size: **1024**  Version: **2**  Timeout: **90** seconds  Authentication retries: **2** | 1 | blank |
| Configure the AAA authentication settings. | Enable AAA  Use **local database** as default setting.  Use case-sensitive local username authentication | 2 | blank |
| Enhanced Login settings | Block for **three** minutes after **four** failed attempts in **two**-minute period. | 1 | blank |
| Encrypt all passwords |  | 0.5 | blank |
| Configure VTY lines to allow SSH access only | Allow only **SSH** access. | 0.5 | blank |
| Verify SSH access to R3 from PCs | SSH should be successful. | 1 | blank |
|  | **Total** | **8** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| 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 SSH. | ip domain-name netsec.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 the AAA authentication settings. | aaa new-model  aaa authentication login default local-case | show run | inc aaa |
| Enhanced Login settings | login block-for 180 attempts 4 within 120 | show login |
| Encrypt all passwords | service password-encryption | show run | incl password-e |
| Configure VTY lines to allow SSH access | line vty 0 4  transport input ssh  exit | show run | sec vty |

### Configure OSPF authentication on R2 and R3.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Configure key chain using SHA256 hashing | Routers: **R2** & **R3**   * Key chain name: **NetSec** * Key number**: 10** * Key string: **NetSecOSPF** * Authentication algorithm: **hmac-sha-sha256** | 4 | blank |
| Apply the assigned the key chain to the appropriate interfaces |  | 2 | blank |
|  | **Total** | **6** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands |
| Configure key chain using SHA256 hashing | key chain NetSec  key 10  key-string NetSecOSPF  cryptographic-algorithm hmac-sha-256 | show run | section key |
| Apply the assigned the key chain to the appropriate interfaces | **Router R2:**  interface g0/0/1  ip ospf authentication key-chain NetSec  **Router R3:**  interface g0/0/0  ip ospf authentication key-chain NetSec | **Router R2:**  show ip ospf interface g0/0/1  **Router R3:**  show ip ospf interface g0/0/0 |

### Verify connectivity.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Task | Specification | Pts | Earned |
| Verify connectivity between PC-A and PC-B |  | 0.5 | Blank |
| Verify connectivity between PC-A and PC-C |  | 0.5 | Blank |
|  | **Total** | **1** | **blank** |

**Instructor Sign-Off Part 2:**

Type your answers here.

**Points for Part 2: (Total points 15)**

Type your answers here.

**Note**: Do not proceed to Part 3 until your instructor has signed off on Part 2.

## Configure a Site-to-Site VPN (30 points, 30 minutes)

**Total points: 30 points**

**Time: 30 minutes**

In this part, you will configure a Site-to-Site IPsec VPN between the routers R1 and R3. You will use the CLI to configure R1 and repeat the procedure for R3.

### Configure Site-to-Site VPN on R1 using CLI. (14 points, 15 minutes)

Configuration parameters include the following:

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Create an ISAKMP policy. | ISAKMP Policy Priority: **1**  Authentication type: **pre-share**  Encryption: **aes 256**  Hash algorithm: **sha**  Diffie-Hellman Group Key Exchange: **24** | 5 | blank |
| Configure the pre-shared key. | Preshare key: **ciscopreshare**  Address:**64.100.3.1** | 2 | blank |
| Configure the IPsec transform set. | Tag: **TRNSFRM-SET**  Cipher: **aes 256**  Hash function: **ESP-SHA-HMAC** | 2 | blank |
| Define interesting traffic. | ACL: **VPN-TRAFFIC**  Source Network: **192.168.1.0 /24**  Destination Network: **172.16.30 /24** | 1 | blank |
| Create a crypto map. | Crypto map name: **CMAP**  Sequence number: **1**  Type: **ipsec-isakmp**  ACL to match: **VPN-TRAFFIC**  Peer: **64.100.3.1**  Pfs type: **group24**  Transform-set: **TRNSFRM-SET** | 3 | blank |
| Apply crypto map to the interface. | Interface: **G0/0/0**  Crypto map name: **CMAP** | 1 | blank |
|  | **Total** | **14** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands |
| Create an ISAKMP policy. | crypto isakmp policy 1  authentication pre-share  encryption aes 256  hash sha  group 24 | show crypto isakmp policy |
| Configure the pre-shared key. | crypto isakmp key ciscopreshare address 64.100.3.1 | show run | include crypto |
| Configure the IPsec transform set. | crypto ipsec transform-set TRNSFRM-SET esp-aes 256 esp-sha-hmac | show run | include crypto |
| Define interesting traffic. | ip access-list extended VPN-TRAFFIC  permit ip 192.168.1.0 0.0.0.255 172.16.3.0 0.0.0.255 | show access-list |
| Create a crypto map. | crypto map CMAP 1 ipsec-isakmp  match address VPN-TRAFFIC  set transform-set TRNSFRM-SET  set peer 64.100.3.1  set pfs group24 | show crypto map |
| Apply crypto map to interface. | interface g0/0/0  crypto map CMAP | show crypto map  show run interface g0/0/0 |

### Configure Site-to-Site VPN on R3 using CLI. (12 points, 10 minutes)

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Create an ISAKMP policy. | ISAKMP Policy Priority: **1**  Authentication type: **pre-share**  Encryption: **aes 256**  Hash algorithm: **sha**  Diffie-Hellman Group Key Exchange: **24** | 4 | blank |
| Configure the pre-shared key. | Preshare key: **ciscopreshare**  Address:**64.100.1.1** | 2 | blank |
| Configure the IPsec transform set. | Tag: **TRNSFRM-SET**  ESP transform: **R3-R1**  Cipher: **aes 256**  Hash function: **ESP-SHA-HMAC** | 2 | blank |
| Define interesting traffic. | ACL: **VPN-TRAFFIC**  Source Network: **172.16.3.0 /24**  Destination Network: **192.168.1.0 /24** | 1 | blank |
| Create a crypto map. | Crypto map name: **CMAP**  Sequence number: **1**  Type: **ipsec-isakmp**  ACL to match: **VPN-TRAFFIC**  Peer: **64.100.1.1**  Pfs type: **group24**  Transform-set: **TRNSFRM-SET** | 2 | blank |
| Apply crypto map to the interface. | Interface: **G0/0/0**  Crypto map name: **CMAP** | 1 | Blank |
|  | **Total** | **12** | blank |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands | |
| Create an ISAKMP policy. | crypto isakmp policy 1  authentication pre-share  encryption aes 256  hash sha  group 24 | show crypto isakmp policy |
| Configure the pre-shared key. | crypto isakmp key ciscopreshare address 64.100.1.1 | show run | include crypto |
| Configure the IPsec transform set. | crypto ipsec transform-set TRNSFRM-SET esp-aes 256 esp-sha-hmac | show run | include crypto |
| Define interesting traffic. | ip access-list extended VPN-TRAFFIC  permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255 | show access-list |
| Create a crypto map. | crypto map CMAP 1 ipsec-isakmp  match address VPN-TRAFFIC  set transform-set TRNSFRM-SET  set peer 64.100.1.1  set pfs group24 | show crypto map |
| Apply crypto map to interface. | Interface g0/0/0  crypto map CMAP | show crypto map  show run interface g0/0/0 |

### Verify VPN Connection.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Task | Specification | Pts | Earned |
| Verify VPN connectivity between PC-A and PC-B | Use the correct commands to demonstrate the packet route | 1 | Blank |
| Verify **NO** VPN connectivity between PC-A and PC-C | Use the correct commands to demonstrate the packet route | 1 | Blank |
| Verify VPN operation |  | 2 | blank |
|  | **Total** | **4** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands |
| Verify VPN connectivity between PC-A and PC-B | PC-A> tracert 172.16.3.10 | The tracepath from PC-A to PC-B:  192.168.1.1 > 64.100.3.1 > 172.16.3.10 |
| Verify **NO** VPN connectivity between PC-A and PC-C | PC-A> tracert 172.16.33.10 | The path from PC-A to PC-C goes thru R2, not thru the VPN tunnel |
| Verify the VPN operation. |  | show crypto isakmp sa  show crypto ipsec sa |

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

Instructor Sign-Off Part 3:

Type your answers here.

Points for Part 3: (Total points 27):

Type your answers here.

**Note**: Do not proceed to Part 4 until your instructor has signed off on Part 3.

## Configure a Zone-Based Policy Firewall (30 points, 30 minutes)

**Total points: 30 points**

**Time: 30 minutes**

In this part, you will configure a zone-based policy firewall on R3.

* Computers in the R3 INSIDE network are considered *trusted* and are allowed to initiate any type of traffic (TCP, UDP or ICMP based traffic).
* Computers in the R3 GUEST network are considered *untrusted* and are allowed to initiate only web traffic (HTTP or HTTPS) to the OUTSIDE.
* No traffic initiated from the OUTSIDE, except VPN connection, should be allowed into the INSIDE networks.

### Configure ZPF for INSIDE to OUTSIDE (14 points, 12 minutes)

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Create the security zones. | Inside zone name: **INSIDE**  Outside zone name: **OUTSIDE** | 2 | blank |
| Create an inspect class map. | Class map name: **INSIDE-PROTOCOLS**  Inspection type: **match-any**  Protocols allowed: **tcp,udp,icmp** | 3 | blank |
| Create an inspect policy map. | Policy map name: **INSIDE-TO-OUTSIDE-PM**  Bind the class map to the policy map.  Matched packets should be inspected. | 3 | blank |
| Create a zone pair. | Zone pair name: **INSIDE-TO-OUTSIDE-ZP**  Source zone: **INSIDE**  Destination zone: **OUTSIDE** | 3 | blank |
| Apply the policy map to the zone pair. | Zone pair name: **INSIDE-TO-OUTSIDE-ZP**  Policy map name: **INSIDE-TO-OUTSIDE-PM** | 2 | blank |
| Assign interfaces to the proper security zones. | Interface G0/0/1.3: **INSIDE**  Interface G0/0/0: **OUTSIDE** | 2 | blank |
|  | **Total** | **15** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands |
| Create security zone names. | zone security INSIDE  zone security OUTSIDE | show 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 inspectINSIDE-TO-OUTSIDE-PM  class type inspect INSIDE-PROTOCOLS  inspect | show policy-map type inspect |
| Create a zone pair. | zone-pair security INSIDE-TO-OUTSIDE-ZP source INSIDE destination OUTSIDE | show zone-pair security |
| Apply the policy map to the zone pair. | service-policy type inspect INSIDE-TO-OUTSIDE-PM | show zone-pair security |
| Assign interfaces to the proper security zones. | interface g0/0/1.3  zone-member security INSIDE  interface g0/0/0  zone-member security OUTSIDE | show zone security  or  show policy-map type inspect zone-pair |

Troubleshoot as necessary to correct any issues discovered.

### Configure ZPF for GUEST to OUTSIDE (10 points, 8 minutes)

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Create the security zone. | GUEST zone name: **GUEST** | 1 | blank |
| Create an inspect class map. | Class map name: **GUEST-PROTOCOLS**  Inspection type: **match-any**  Protocols allowed: **http,https.dns** | 2 | blank |
| Create an inspect policy map. | Policy map name: **GUEST-TO-OUTSIDE-PM**  Bind the class map to the policy map.  Matched packets should be inspected. | 2 | blank |
| Create a zone pair. | Zone pair name: **GUEST-TO-OUTSIDE-ZP**  Source zone: **GUEST**  Destination zone: **OUTSIDE** | 2 | blank |
| Apply the policy map to the zone pair. | Zone pair name: **GUEST-TO-OUTSIDE-ZP**  Policy map name: **GUEST-TO-OUTSIDE-PM** | 2 | blank |
| Assign interfaces to the proper security zones. | Interface G0/0/1.33: **GUEST** | 1 | blank |
|  | **Total** | **10** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands |
| Create security zone names. | zone security GUEST | show run | section zone security |
| Create an inspect class map. | class-map type inspect match-any GUEST-PROTOCOLS  match protocol http  match protocol https  match protocol dns | show class-map type inspect |
| Create an inspect policy map. | policy-map type inspect **GUEST-TO-OUTSIDE-PM**  class type inspect GUEST-PROTOCOLS  inspect | show policy-map type inspect |
| Create a zone pair. | zone-pair security GUEST-TO-OUTSIDE-ZP source GUEST destination OUTSIDE | show zone-pair security |
| Apply the policy map to the zone pair. | service-policy type inspect GUEST-TO-OUTSIDE-PM | show zone-pair security |
| Assign interfaces to the proper security zones. | interface g0/0/1.33  zone-member security GUEST | show zone security |

### Configure ZPF for OUTSIDE to INSIDE (5 points, 7 minutes)

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item or Task | Specification | Pts | Earned |
| Create a named ACL to allow R1 VPN traffic through to VLAN 3 | Name: **REMOTE-TRAFFIC**  Source: **192.168.1.0 /24**  Destination: **172.16.3.0 /24** | 1 | Blank |
| Create an inspect class map. | Class map name: **OUTSIDE-TRAFFIC**  Inspection type: **match-all**  Access group allowed: **REMOTE-TRAFFIC** | 1 | Blank |
| Create an inspect policy map. | Policy map name: **OUTSIDE-TO-INSIDE-PM**  Bind the class map to the policy map.  Matched packets should be inspected. | 1 | Blank |
| Create a zone pair. | Zone pair name: **OUTSIDE-TO-INSIDE-ZP**  Source zone: **INSIDE**  Destination zone: **OUTSIDE** | 1 | Blank |
| Apply the policy map to the zone pair. | Zone pair name: **OUTSIDE-TO-INSIDE-ZP**  Policy map name: **OUTSIDE-TO-INSIDE-PM** | 1 | Blank |
|  | **Total** | **5** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

|  |  |  |
| --- | --- | --- |
| Configuration Item or Task | Configuration Commands | Verification Commands |
| Create ACL to allow R1 VPN traffic through | ip access-list extended REMOTE-TRAFFIC  permit ip 192.168.1.0 0.0.0.255 172.16.3.0 0.0.0.255 | show access-list REMOTE-TRAFFIC |
| Create an inspect class map. | class-map type inspect match-all OUTSIDE-TRAFFIC  match access-group name REMOTE-TRAFFIC | show class-map type inspect |
| Create an inspect policy map. | policy-map type inspect OUTSIDE-TO-INSIDE-PM  class type inspect OUTSIDE-TRAFFIC  inspect | show policy-map type inspect |
| Create a zone pair. | zone-pair security OUTSIDE-TO-INSIDE-ZP source OUTSIDE destination INSIDE | show zone-pair security |
| Apply the policy map to the zone pair. | service-policy type inspect OUTSIDE-TO-INSIDE-PM | show zone-pair security |

### Verify ZPF functionality.

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Task | Specification | Pts | Earned |
| Verify all PCs can access web browser on R2 |  | 1 | Blank |
| Verify VPN connection between PC-A and PC-B |  | 1 | Blank |
| Verify No OUTSIDE traffic into INSIDE zone, except via VPN |  | 1 | Blank |
|  | **Total** | **3** | **blank** |

Troubleshoot as necessary to correct any issues discovered.

Type your answers here.

# Router Interface Summary Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
| 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) |
| 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) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

Blank Line, No additional information

# Device Configs

## Router R1

R1# show run brief

Building configuration...

Current configuration : 1795 bytes

!

version 16.9

service timestamps debug datetime msec

service timestamps log datetime msec

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

!

hostname R1

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

no ip domain lookup

!

login on-success log

!

subscriber templating

multilink bundle-name authenticated

!

spanning-tree extend system-id

!

redundancy

mode none

!

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 24

crypto isakmp key ciscopreshare address 64.100.3.1

!

crypto ipsec transform-set TRNSFRM-SET esp-aes 256 esp-sha-hmac

mode tunnel

!

crypto map CMAP 1 ipsec-isakmp

set peer 64.100.3.1

set transform-set TRNSFRM-SET

set pfs group24

match address VPN-TRAFFIC

!

interface GigabitEthernet0/0/0

description Link to R2

ip address 64.100.1.1 255.255.255.252

negotiation auto

crypto map CMAP

!

interface GigabitEthernet0/0/1

description Link to R1 LAN

ip address 192.168.1.1 255.255.255.0

negotiation auto

!

interface Serial0/1/0

no ip address

!

interface Serial0/1/1

no ip address

!

router ospf 1

passive-interface GigabitEthernet0/0/1

network 64.100.1.0 0.0.0.3 area 0

network 192.168.1.0 0.255.255.255 area 0

!

ip forward-protocol nd

no ip http server

ip http secure-server

!

ip access-list extended VPN-TRAFFIC

permit ip 192.168.1.0 0.0.0.255 172.16.3.0 0.0.0.255

!

control-plane

!

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

!

end

## Router R2

R2# show run brief

Building configuration...

Current configuration : 1543 bytes

!

version 16.9

service timestamps debug datetime msec

service timestamps log datetime msec

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

!

hostname R2

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

no ip domain lookup

!

login on-success log

!

subscriber templating

!

multilink bundle-name authenticated

!

key chain NetSec

key 10

key-string NetSecOSPF

cryptographic-algorithm hmac-sha-256

!

spanning-tree extend system-id

!

username webuser privilege 15 secret 5 $1$t1x6$But2s0WOVK7oxozoIkMsX1

!

redundancy

mode none

!

interface GigabitEthernet0/0/0

description Link to R1

ip address 64.100.1.2 255.255.255.252

negotiation auto

!

interface GigabitEthernet0/0/1

description Link to R3

ip address 64.100.3.2 255.255.255.252

ip ospf authentication key-chain NetSec

negotiation auto

!

router ospf 1

network 64.100.1.0 0.0.0.3 area 0

network 64.100.3.0 0.0.0.3 area 0

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

control-plane

!

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

!

end

## Router R3

R3# show run brief

Building configuration...

Current configuration : 4195 bytes

!

version 16.9

service timestamps debug datetime msec

service timestamps log datetime msec

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

!

hostname R3

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9 $9$5d06ThFZdLHxBy$A56qWeaP9g6Znb3d2iImMN5KFH87FS4Ds4GMiaMocBQ

!

aaa new-model

!

aaa authentication login default local-case

!

aaa session-id common

!

no ip domain lookup

ip domain name netsec.com

!

login block-for 180 attempts 4 within 120

login on-success log

!

subscriber templating

!

multilink bundle-name authenticated

!

key chain NetSec

key 10

key-string 7 032A5E1F350A22637D393F

cryptographic-algorithm hmac-sha-256

!

spanning-tree extend system-id

!

username admin01 privilege 15 secret 9 $9$DeZoOK/8DhxDdi$EvM6XnDQxwyxKIqDWmeVv5q53jDflVihZ/z4u.o0O7c

!

redundancy

mode none

!

class-map type inspect match-all OUTSIDE-TRAFFIC

match access-group name REMOTE-TRAFFIC

class-map type inspect match-any GUEST-PROTOCOLS

match protocol http

match protocol https

match protocol dns

class-map type inspect match-any INSIDE-PROTOCOLS

match protocol tcp

match protocol udp

match protocol icmp

!

policy-map type inspect OUTSIDE-TO-INSIDE-PM

class type inspect OUTSIDE-TRAFFIC

inspect

class class-default

policy-map type inspect INSIDE-TO-OUTSIDE-PM

class type inspect INSIDE-PROTOCOLS

inspect

class class-default

policy-map type inspect GUEST-TO-OUTSIDE-PM

class type inspect GUEST-PROTOCOLS

inspect

class class-default

!

zone security INSIDE

zone security OUTSIDE

zone security GUEST

zone-pair security GUEST-TO-OUTSIDE-ZP source GUEST destination OUTSIDE

service-policy type inspect GUEST-TO-OUTSIDE-PM

zone-pair security INSIDE-TO-OUTSIDE-ZP source INSIDE destination OUTSIDE

service-policy type inspect INSIDE-TO-OUTSIDE-PM

zone-pair security OUTSIDE-TO-INSIDE-ZP source OUTSIDE destination INSIDE

service-policy type inspect OUTSIDE-TO-INSIDE-PM

!

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 24

crypto isakmp key ciscopreshare address 64.100.1.1

!

crypto ipsec transform-set TRNSFRM-SET esp-aes 256 esp-sha-hmac

mode tunnel

!

crypto map CMAP 1 ipsec-isakmp

set peer 64.100.1.1

set transform-set TRNSFRM-SET

set pfs group24

match address VPN-TRAFFIC

!

interface GigabitEthernet0/0/0

description Link to R2

ip address 64.100.3.1 255.255.255.252

zone-member security OUTSIDE

ip ospf authentication key-chain NetSec

negotiation auto

crypto map CMAP

!

interface GigabitEthernet0/0/1

no ip address

negotiation auto

!

interface GigabitEthernet0/0/1.3

description Link to VLAN 3

encapsulation dot1Q 3

ip address 172.16.3.1 255.255.255.0

zone-member security INSIDE

!

interface GigabitEthernet0/0/1.33

description Link to VLAN 33

encapsulation dot1Q 33

ip address 172.16.33.1 255.255.255.0

zone-member security GUEST

!

router ospf 1

passive-interface GigabitEthernet0/0/1

network 64.100.3.0 0.0.0.3 area 0

network 172.16.0.0 0.0.255.255 area 0

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

ip access-list extended REMOTE-TRAFFIC

permit ip 192.168.1.0 0.0.0.255 172.16.3.0 0.0.0.255

ip access-list extended VPN-TRAFFIC

permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255

!

control-plane

!

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

transport input ssh

!

end

## Switch S2

S2# show run brief

Building configuration...

Current configuration : 3695 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S2

!

boot-start-marker

boot-end-marker

!

enable secret 9 $9$YayOy4FgblvfMJ$CZODl3OsdsFV/cCXv0SuVcXnrC4k7RhAb52T4wlgaNM

!

username admin01 privilege 15 secret 9 $9$C6qz0LLIjxwWh2$QhZnu4nwKyDdv3WgOpAG4yKjk7jaEZuIKX.EzZkDiU2

aaa new-model

aaa authentication login default local-case

!

aaa session-id common

system mtu routing 1500!

!

no ip domain-lookup

ip domain-name netsec.com

login block-for 180 attempts 4 within 120

!

spanning-tree mode rapid-pvst

spanning-tree loopguard default

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/2

switchport access vlan 99

switchport mode access

shutdown

!

interface FastEthernet0/3

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/4

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

!

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 3

switchport mode access

switchport port-security maximum 1

switchport port-security mac-address sticky 0050.569c.5f78

switchport port-security

spanning-tree portfast edge

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 99

switchport mode access

shutdown

!

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

shutdown

!

interface Vlan3

ip address 172.16.3.2 255.255.255.0

!

ip default-gateway 172.16.3.1

ip http server

ip http secure-server

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

line con 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

!

end

## Switch S3

S3# show run brief

Building configuration...

Current configuration : 4040 bytes

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service call-home

!

hostname S3

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

login on-success log

!

spanning-tree mode rapid-pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/2

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

switchport access vlan 33

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

no ip address

!

interface Vlan3

ip address 172.16.3.3 255.255.255.0

!

ip default-gateway 172.16.3.1

ip http server

ip http secure-server

!

line con 0

logging synchronous

stopbits 1

line vty 0 4

login

line vty 5 15

login

!

end

end of document