Justin Sterlacci  
Internetworking  
Professor Cannistra  
April 16th, 2023

**Lab 9 Lab Report**

**Lab Description:**   
Set up Access Control lists in a network to prevent or allow certain communications.

**Topography:**  
Diagram, schematic

Description automatically generated  
  
Syntax:

CLI Command Description Mode of Cisco OIS

|  |  |  |
| --- | --- | --- |
| ping | Used to ping ip addresses from a PC. You can ping other PC’s or switches with this. | Windows CMD |
| Logging synchronous | Forces error messages to be on its own line, rather than interrupt a line that you’re typing on. | Console Line |
| Enable | Enter Privileged Mode | User Mode |
| Conf t | Enter Global Configurator Mode | Privileged Mode |
| Line con 0 | Enter the Console Line | Global Configurator Mode |
| Hostname | Used to name a switch or PC | Privileged Mode |
| Password | Used to set a password | Privileged Mode |
| Login | Used to require the password to utilize User Mode | Global Configurator Mode |
| Enable password | Used to set an unencrypted Privileged Password | Global Configurator Mode |
| Show ip interface brief (sh ip int brief) | Displays a brief list of all interfaces | Privileged Mode |
| vtp domain INETLAB | Renames the VTP domain from NULL to INETLAB | Global Configurator Mode |
| Vtp password cisco | Set a password within the VTP Domain | Global Configurator Mode |
| Vtp mode server/client | Sets the vtp mode between server or client, in the case of this lab. | Global Configurator Mode |
| Switchport mode access | Changes the mode of a switchport to access mode | Line configuration Mode (within a vlan) |
| Switchport trunk encapsulation dot1q | Sets up the switch to switch connect to use IEEE 802.1Q encapsulation | Within a vlan with a multi-Connection switch |
| Switchport mode trunk | Sets the mode for the switchport to trunk | Within a vlan |
| Spanning-tree vlan xx root primary | Setting up a spanning tree within a vlan, and setting it to root primary | Privileged mode |
| Encapsulation dot1q xx | Sets up a VLAN in IEEE 802.1Q within a router | ROUTER Line Configuration Mode(within a sub interface) |
| Ip route (ip) (SM) (ip) | Sets up a static IP Route | Interface Mode |
| Router rip | Sets the Router into RIP mode | Global Configuration |
| Version 2 | Sets the RIP version to version 2 | Global Configuration |
| Network (ip address) | Sets the Network for RIPv2 networking | Global Configuration |
| Ipv6 router ospf 1 | Sets the router to have OSPFv3 enabled | Global Configuration |
| Passive-interface (interface) | Will set the selected interface as a passive interface in OSPFv3 | Router Line Configuration mode |
| Ipv6 ospf 1 area 0 | Sets the passive interface in area 0 | Interface Configuration |
| access-list # permit/deny (protocol) ip wildcard ip wildcard eq (port) | Sets up an extended access list to allow or deny the flow of a packet depending on the protocol and destination it is getting sent to | Global Configuration Mode |
| int x  ip access-group [1-99] [in | out] | Sets up the flow for the specified port when it comes to access groups | Interface Mode |

**Test Cases:**

Test Case 1: Verify that PC1 and PC2 can reach the HTTP-Server

1. Configure the ACL to allow traffic from PC1’s or PC2’s IP address  
2. Send a packet from PC1 or PC2 to the HTTP-Server  
3. Verify that the packet is received, and communication occurs.

Test Case 2: Verify that PC3 and PC4 can reach the HTTPS-Server  
1. Configure the ACL to allow traffic from PC3s or PC4s IP address  
2. Send a packet from PC3 or PC4 to the HTTPS-Server  
3. Verify that the packet is received, and communication occurs.

Test case 3: Verify that all Corporate PC’s can access the DMZ-HTTP-Server via HTTPS  
1. Configure the ACL to allow traffic from any of the Corporate PCs IP addresses  
2. Send a packet from any of the corporate PCs to the DMZ-HTTP-Server  
3. Verify that the packet is received, and communication occurs.

Test Case 4: Verify that all Corporate PCs can “ping” the ISP interface connected to the Edge Router  
1. Configure the ACL to allow traffic from any of the Corporate PCs IP addresses  
2. Send a packet from any of the Corporate PCs to the ISP interface connected to the Edge router, which is int g0/0 in this case.  
3. Verify that the packet is received, and communication occurs.

**Verification:**A)  
Text

Description automatically generatedPing from PC1 to HTTPS-Server

Text

Description automatically generated with medium confidencePing from PC1 to PC4  
Text

Description automatically generatedPing from PC1 to DMZ-HTTP-Server

B)   
Text

Description automatically generatedEdge Router’s IP Route table

C)  
Text, table

Description automatically generatedEdge Router’s Access List after implementation

D)  
Test Case 1:   
Graphical user interface, text, application, Word

Description automatically generatedPC1 before Test Case  
Graphical user interface, text, application, email

Description automatically generatedPC1 after Test Case

Test case 2:   
Graphical user interface, text, application

Description automatically generatedPC3 before Test Case  
Graphical user interface, text, application, email

Description automatically generatedPC3 after Test Case

Test Case 3:  
Graphical user interface, text, application, email

Description automatically generatedPC2 before Test Case  
Graphical user interface, text, application, email

Description automatically generatedPC2 after Test Case

Test Case 4:  
Graphical user interface, text, application

Description automatically generatedPC4 before Test Case  
Text

Description automatically generatedPC4 after Test Case

**Conclusion:**This lab’s initial set up was quite easy due to the partially completed network being configured, however I struggled to implement the Access Lists, since at first it allowed all packets to travel through regardless of me setting it to deny all other packets that wasn’t specified, then I had an issue where it didn’t allow any packets to get sent at all. What fixed this was making sure I didn’t set anything on int g0/1 and int g0/2 with ip access-group 100 [in | out]. When I set this, it allowed the proper communication with the PCs to the HTTP and HTTPS server, as well as allowing the Corporate PCs to ping the ISP interface connected to the Edge Router. The only thing left unresolved is allowing all the Corporate PCs to access the DMZ-EMAIL-Server. I believe I set the proper access list commands; however, I am unsure how to set up the email function on both the PC and the DMZ-EMAIL-Server.