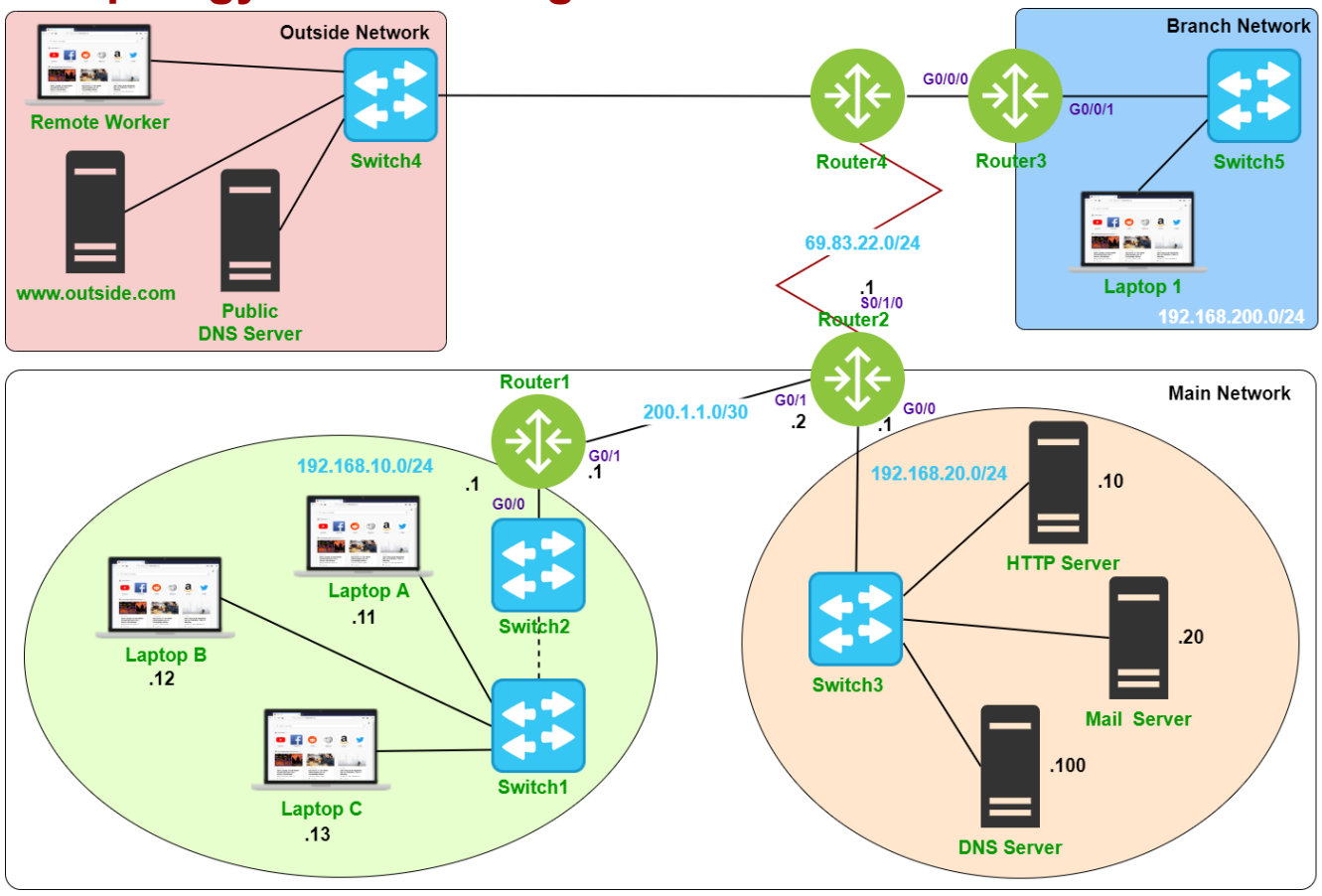
Lab 9 – Firewalls

Lab Topology and Learning Goal



Firewalls protect the network by analyzing and filtering unwanted traffic based on pre-defined rules. Cisco supports two families of firewalls on Integrated Service Router (ISR) Gen 2 devices, Context-Based Access Control (CABC) and Zone-Based Policy firewalls. In this lab, we will look at both technologies.

Lab Instructions and Required Resources

- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 9 – Firewalls.pkz**
- Take Lab Quiz: **Lab 9 - Requires Respondus LockDown Browser**

Lab 9 – Firewalls

Configure Context-Based Access Control (CABC)

Cisco Context-Based Access Control operates based on the idea that networks generally have a safe area "inside" the firewall, and everything "outside" is untrusted. CBAC provides firewall features by inspecting traffic flowing from the inside of the network to the outside and dynamically allows responses to the traffic to return to the inside network. We will configure CBAC on the network edge of the Branch office.

Test Network Connectivity Before Configuring Firewall

From **Laptop A**, test network connectivity to the **Web Server** (**192.168.20.10**), the **Remote Worker** laptop (**100.40.66.11**), and the **Laptop 1** (**192.168.200.10**); troubleshoot as necessary.

From **Laptop 1**, test network connectivity to the **Web Server** (**192.168.20.10**), the **Remote Worker** laptop (**100.40.66.11**), and the **Laptop A** (**192.168.10.11**); troubleshoot as necessary.

From the **Remote Worker** laptop, test network connectivity to **Laptop A** (**192.168.10.11**), the **Web Server** (**192.168.20.10**), and the **Laptop 1** (**192.168.200.10**); troubleshoot, as necessary.

Configure CBAC on the Branch Router

Create an ACL to deny traffic originating from outside the network

```
Router3(config)# access-list 199 deny ip any any
```

Create an inspect list to inspect HTTP and ICMP traffic leaving the network

```
Router3(config)# ip inspect name CBAC http
Router3(config)# ip inspect name CBAC icmp
```

Apply CBAC to the Outside Interfaces

Apply the deny rule to the outside interface

```
Router3(config)# interface GigabitEthernet0/0/0
Router3(config-if)# ip access-group 199 in
Router3(config-if)# ip inspect CBAC out
Router3(config-if)# exit
```

All traffic leaving the network is inspected and an appropriate ACL is dynamically created to allow return traffic.

Lab 9 – Firewalls

Test the Results of the Firewall Rules on Network Traffic

From **Laptop 1**, test network connectivity to the **Web Server** (**192.168.20.10**), the **Remote Worker** laptop (**100.40.66.11**), and the **Laptop A** (**192.168.10.11**)

On **Laptop 1**, open the **Web Browser** and navigate to **www.fanshawe.ca**, does the page load?

Try navigating to **192.168.20.10**, does the page load now? Why is this so?

Use **Simulation Mode** to discover the reason.

Verify Firewall Configuration

View the ACL configuration
Router3# show access-list

View the active inspection sessions
Router3# show ip inspect sessions

Lab Challenge: Research how to properly use and format access control lists. Modify ACL 199 so Laptop 1 can access the web page by its domain name.

Use the ACL format:
access-list [ACL number] [action] [protocol] [source] [destination] [operator (port)]

Lab 9 – Firewalls

Configure Zone-Based Policy Firewall

Zone-Based Policy Firewalls move firewall design away from a safe inside and a dangerous outside of the network. With ZPF interfaces are assigned to a network zone, and a policy is applied to the zone. ZPF allows administrators more granular control over how traffic flows between zones. We will configure ZPF on the edge router of the Main Office.

Configure Network Security Zones

On Router2, create a security zone for all networks

```
Router2(config)# zone security LAN
Router2(config-sec-zone)# exit

Router2(config)# zone security EXTERNAL
Router2(config-sec-zone)# exit

Router2(config)# zone security DMZ
Router2(config-sec-zone)# exit
```

Assign Physical Interfaces to Network Security Zones

```
Router2(config)# interface GigabitEthernet0/0/1
Router2(config-if)# zone-member security LAN
Router2(config-if)# exit

Router2(config)# interface Serial0/1/0
Router2(config-if)# zone-member security EXTERNAL
Router2(config-if)# exit

Router2(config)# interface GigabitEthernet0/0/0
Router2(config-if)# zone-member security DMZ
Router2(config-if)# exit
```

Identify Internal Traffic

```
Router2(config)# access-list 195 permit ip 192.168.10.0 0.0.0.255 any
```

Configure a Class Map to Classify LAN traffic

```
Router2(config)# class-map type inspect match-all LANTraffic
Router2(config-cmap)# match access-group 195
Router2(config-cmap)# exit
```

Lab 9 – Firewalls

Create a Policy Map with Processing Instructions for Classified Traffic

Router2(config)# policy-map type inspect OUTBOUND
Router2(config-pmap)# class type inspect LANTraffic

Define an Action for Traffic Affected by the Policy

The available action items include Pass, Drop and Inspect
Router2(config-pmap-c)# inspect
Router2(config-pmap-c)# exit
Router2(config-pmap)# exit

Configure a Zone Pair

A Zone Pair ties two security zones together
Router2(config)# zone-pair security LAN2EXTERNAL source LAN destination EXTERNAL

Bind the policy map to the zone pair to enable inspection
Router2(config-sec-zone-pair)# service-policy type inspect OUTBOUND
Router2(config-sec-zone-pair)# exit

Test the Results of the Firewall Rules on Network Traffic

From **Laptop B**, test network connectivity to the **Web Server** (**192.168.20.10**) and the **Remote Worker** laptop (**100.40.66.11**); are these results expected?

On **Laptop B**, open the **Web Browser** and navigate to **www.outside.com**, does the page load?

Try navigating to **100.40.66.10**, does the page load now?

From the **Remote Worker** laptop, test network connectivity to **Laptop B** (**192.168.10.12**); all incoming connection requests should fail.

Configure the Firewall to Allow Communication to the DMZ

Configure a class map to classify incoming requests
Router2(config)# class-map type inspect match-any ExternalTraffic
Router2(config-cmap)# match protocol http
Router2(config-cmap)# exit

Lab 9 – Firewalls

Create a Policy Map with Processing Instructions for Classified Traffic

Router2(config)# policy-map type inspect INBOUND
Router2(config-pmap)# class type inspect ExternalTraffic

Define an Action for Traffic Affected by the Policy

The available action items include Pass, Drop and Inspect
Router2(config-pmap-c)# inspect
Router2(config-pmap-c)# exit
Router2(config-pmap)# exit

Configure a Zone Pair

A Zone Pair ties two security zones together
Router2(config)# zone-pair security EXTERNAL2DMZ source EXTERNAL destination DMZ

Bind the policy map to the zone pair to enable inspection
Router2(config-sec-zone-pair)# service-policy type inspect INBOUND
Router2(config-sec-zone-pair)# exit

Test the Results of the Firewall Rules on Network Traffic

From the **Remote Worker** laptop, test network connectivity to the **Web Server** (**192.168.20.10**); are these results expected?

Open the **Web Browser** and navigate to **192.168.20.10**, does the page load?

Verify Firewall Operation

Router2# show policy-map type inspect zone-pair sessions