Lab Part 3 – ZPF on Network Design

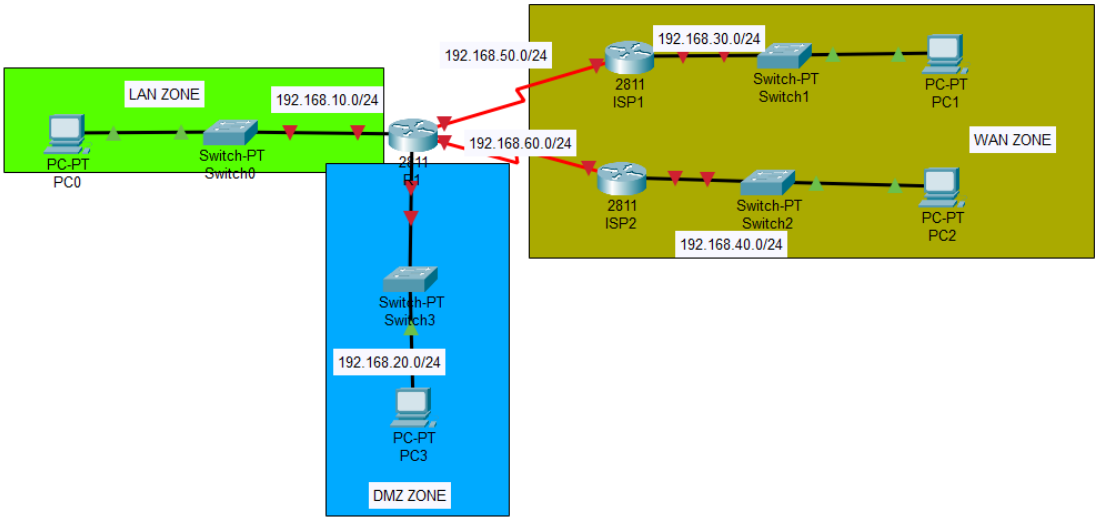
Overview:

Zone-Based Policy Firewall is the most advanced method of a stateful firewall available on Cisco IOS routers. The idea behind ZPF is that we don't assign access-lists to interfaces, but we will create different zones. Interfaces will be assigned to the different zones, and security policies will be assigned to traffic between zones. The network is divided into different security zones based on criteria such as trust levels, locations, or functions. Common zones might include "inside" (trusted internal network), "outside" (untrusted external network such as the internet), "DMZ" (demilitarized zone for servers accessible from the internet), and so on. Security policies are then defined based on the traffic flow between these zones. These policies specify what types of traffic are allowed or denied between different zones. In summary, zone-based firewalls are an effective approach to network security, particularly in environments where there are diverse security requirements and traffic patterns. They offer enhanced visibility and control over network traffic while helping to mitigate security risks.

Task 1: Configure ZPF

Consider this small network that has a LAN, DMZ, and WAN with two ISPs. The security policy for this network is as follows:

- Traffic from the LAN is allowed to the WAN but only to HTTP and HTTPS servers.
- Traffic from the LAN is allowed to the DMZ unrestricted.
- Traffic from the DMZ is not allowed to the LAN.
- Traffic from the DMZ is allowed to the WAN but only for the DNS and HTTP servers.
- Traffic from the WAN is allowed to the LAN but only to an FTP server.



Using the Cisco packet tracer, perform the following requirements:

- Implement this network with the IP addressing provided. The Packet tracer file is provided, you need to add IP addresses.
- Configure basic device settings on the router and switch such as hostnames, console password, enable password, banner messages, disable IP domain lookup.
- Configure Zone-Based Policy Firewall (ZPF) to achieve the security policy mentioned earlier.
- Test and Verifying Network Communication, ensure everything configured is working as expected by providing adequate screenshots.