Extending Networks

Learned:

- Firewalls are crucial for network security. They block incoming packets which helps to prevent attacks such as DDos from reaching a web server.

- A VPN is best for transferring secure data across the network by using encryption and masking the IP address to another location.

- Different VPN technologies such as PPP and PPTP encrypt data so that information can be sent securely across networks.

- IPsec provides strong encryption on a VPN making it harder for data to be exposed or stolen on the network.

Port Forwarding

Port forwarding is an important component in connecting applications and services to the internet. Without port forwarding, applications and services such as web servers are only available to devices within the same direct network. If the administrator wanted the website to be accessible to the public by using the internet, then they would have to implement port forwarding. Firewalls determine if traffic can travel across those ports even if ports are open by port forwarding. A router is used to configure port forwarding.

Firewalls

A firewall is a device within a network responsible for determining what traffic is allowed to enter and exit. An administrator can configure a firewall to permit or deny traffic from entering or exiting a network based on where the traffic is coming from, where it is going, what port it is for, and what protocol it is using (TCP, UDP, or both). Firewalls perform packet inspection to determine the answers to these questions. Firewalls come in all shapes and sizes, from dedicated hardware in large networks to residential routers or software such as Snort.

Stateful firewalls use the entire information from a connection rather than inspecting individual packets. They determine device behavior based on the whole connection. **Stateless** firewalls use a static set of rules to check individual packets. They are less smart, use fewer resources, and only follow the rules defined within them. Stateless firewalls are effective when receiving large amounts of traffic from a set of hosts, such as during a DDoS attack. Firewalls fall under the **networking and transport layers** of the OSI model.

VPN (Virtual Private Network)

A VPN allows devices on separate networks to communicate securely by creating a dedicated path over the internet (known as a **tunnel**). Devices within this tunnel form their own private network. Only devices within the same network can communicate directly, but a VPN allows two offices to be connected. VPNs allow networks in different geographical locations to be connected, provide **privacy** by encrypting data, and offer **anonymity** by protecting users from tracking by ISPs or intermediaries.

VPN Technologies: PPP is used by PPTP for authentication and encryption and requires a private key and certificate to match. **PPTP** allows PPP data to leave a network, is easy to set up, but weakly encrypted. **IPsec** encrypts data using the IP framework, is harder to set up, but has strong encryption and is widely supported.

Layer 3 Switches & VLANs

Layer 3 switches are more sophisticated than layer 2 switches. They send **frames** to devices like layer 2 switches but can also **route packets** using IP like a router. **VLAN (Virtual Local Area Network)** allows specific devices to be virtually split up. Devices can share resources like the Internet but are treated separately. This separation provides **security** and controls how devices communicate with each other.