Network components, devices, and diagrams

In this section of the course, you will learn about network architecture.

Once you have a foundational understanding of network architecture, sometimes referred to as network design, you will learn about security vulnerabilities inherent in all networks and how malicious actors attempt to exploit them. In this reading, you will review network devices and connections and investigate a simple network diagram similar to those used every day by network security professionals. Essential tasks of a security analyst include setting up the tools, devices, and protocols used to observe and secure network traffic.

Devices on a network

Network devices are the devices that maintain information and services for users of a network. These devices connect over wired and wireless connections. After establishing a connection to the network, the devices send data packets. The data packets provide information about the source and the destination of the data.

A network diagram displaying how different devices are connected to an internal network

Devices and desktop computers

Most internet users are familiar with everyday devices, such as personal computers, laptops, mobile phones, and tablets. Each device and desktop computer has a unique MAC address and IP address, which identify it on the network, and a network interface that sends and receives data packets. These devices can connect to the network via a hard wire or a wireless connection.

Firewalls

A **firewall** is a network security device that monitors traffic to or from your network. Firewalls can also restrict specific incoming and outgoing network traffic. The organization configures the security rules. Firewalls often reside between the secured and controlled internal network and the untrusted network resources outside the organization, such as the internet.

Servers

Servers provide a service for other devices on the network. The devices that connect to a server are called clients. The following graphic outlines this model, which is called the client-server model. In this model, clients send requests to the server for information and services. The server performs the requests for the clients. Common examples include DNS servers that perform domain name lookups for internet sites, file servers that store and retrieve files from a database, and corporate mail servers that organize mail for a company.

A client server model showing three client devices sending requests and receiving responses from a database ser

Hubs and switches

Hubs and switches both direct traffic on a local network. A hub is a device that provides a common point of connection for all devices directly connected to it. Hubs additionally repeat all information out to all ports. From a security perspective, this makes hubs vulnerable to eavesdropping. For this reason, hubs are not used as often on modern networks; most organizations use switches instead. A switch forwards packets between devices directly connected to it. It maintains a MAC address table that matches MAC addresses of devices on the network to port numbers on the switch and forwards incoming data packets according to the destination MAC address.

Routers

Routers sit between networks and direct traffic, based on the IP address of the destination network. The IP address of the destination network is contained in the IP header. The router reads the header information and forwards the packet to the next router on the path to the destination. This continues until the packet reaches the destination network. Routers can also include a firewall feature that allows or blocks incoming traffic based on information in the transmission. This stops malicious traffic from entering the private network and damaging the local area network.

Modems and wireless access points

Modems

Modems usually interface with an internet service provider (ISP). ISPs provide internet connectivity via telephone lines or coaxial cables. Modems receive transmissions from the internet and translate them into digital signals that can be understood by the devices on the network. Usually, modems connect to a router that takes the decoded transmissions and sends them on to the local network.
Note: Enterprise networks used by large organizations to connect their users and devices often use other broadband technologies to handle high-volume traffic, instead of using a modem.

A modem converting data from the internet, connecting to a Wi-Fi router

Wireless access point

A wireless access point sends and receives digital signals over radio waves creating a wireless network. Devices with wireless adapters connect to the access point using Wi-Fi. Wi-Fi refers to a set of standards that are used by network devices to communicate wirelessly. Wireless access points and the devices connected to them use Wi-Fi protocols to send data through radio waves where they are sent to routers and switches and directed along the path to their final destination.

A wireless access point connected to wired and wireless devices on a network

Using network diagrams as a security analyst

Network diagrams allow network administrators and security personnel to imagine the architecture and design of their organization’s private network.
Network diagrams are topographical maps that show the devices on the network and how they connect. Network diagrams use small representative graphics to portray each network device and dotted lines to show how each device connects to the other. Security analysts use network diagrams to learn about network architecture and how to design networks.

A router connecting to two firewalls and creating two separate security zones

Key takeaways

In the client-server model, the client requests information and services from the server, and the server performs the requests for the clients. Network devices include routers, workstations, servers, hubs, switches, and modems. Security analysts use network diagrams to visualize network architecture.

Revision #1
Created 2023-06-27 01:07:29 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai