Virtual networks and privacy

This section of the course covered a lot of information about network operations. You reviewed the fundamentals of network architecture and communication and can now use this knowledge as you learn how to secure networks. Securing a private network requires maintaining the confidentiality of your data and restricting access to authorized users.

In this reading, you will review several network security topics previously covered in the course, including virtual private networks (VPNs), proxy servers, firewalls, tunnelling, and security zones. You'll continue to learn more about these concepts and how they relate to each other as you continue through the course.

Common network protocols

Network protocols are used to direct traffic to the correct device and service depending on the kind of communication being performed by the devices on the network. Protocols are the rules used by all network devices that provide a mutually agreed upon foundation for how to transfer data across a network.

There are three main categories of network protocols: communication protocols, management protocols, and security protocols.

1. Communication protocols are used to establish connections between servers. Examples include TCP, UDP, and Simple Mail Transfer Protocol (SMTP), which provides a framework for email communication.
2. Management protocols are used to troubleshoot network issues. One example is the Internet Control Message Protocol (ICMP).
3. Security protocols provide encryption for data in transit. Examples include IPSec and SSL/TLS.

Some other commonly used protocols are:

- HyperText Transfer Protocol (HTTP). HTTP is an application layer communication protocol. This allows the browser and the web server to communicate with one another.
- Domain Name System (DNS). DNS is an application layer protocol that translates, or maps, host names to IP addresses.
- Address Resolution Protocol (ARP). ARP is a network layer communication protocol that maps IP addresses to physical machines, or a MAC address recognized on the local area network.

Wi-Fi

This section of the course also introduced various wireless security protocols, including WEP, WPA, WPA2, and WPA3. WPA3 encrypts traffic with the Advanced Encryption Standard (AES) cipher as it travels from your device to the wireless access point. WPA2 and WPA3 offer two modes: personal and enterprise. Personal mode is best suited for home networks while enterprise mode is generally utilized for business networks and applications.

Network security tools and practices

Firewalls

Previously, you learned that firewalls are network virtual appliances (NVAs) or hardware devices that inspect and can filter network traffic before it's permitted to enter the private network. Traditional firewalls are configured with rules that tell it what types of data packets are allowed based on the port number and IP address of the data packet.

There are two main categories of firewalls.

- **Stateless:** A class of firewall that operates based on predefined rules and does not keep track of information from data packets
- **Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats. Unlike stateless firewalls, which require rules to be configured in two directions, a stateful firewall only requires a rule in one direction. This is because it uses a "state table" to track connections, so it can match return traffic to an existing session.

Next generation firewalls (NGFWs) are the most technologically advanced firewall protection. They exceed the security offered by stateful firewalls because they include deep packet inspection (a kind of packet sniffing that examines data packets and takes actions if threats exist) and intrusion prevention features that detect security threats and notify firewall administrators. NGFWs can inspect traffic at the application layer of the TCP/IP model and are typically application aware. Unlike traditional firewalls that block traffic based on IP address and ports, NGFWs rules can be configured to block or allow traffic based on the application. Some NGFWs have additional features like Malware Sandboxing, Network Anti-Virus, and URL and DNS Filtering.

Proxy servers

A proxy server is another way to add security to your private network. Proxy servers utilize network address translation (NAT) to serve as a barrier between clients on the network and external threats. Forward proxies handle queries from internal clients when they access resources external to the network. Reverse proxies function opposite of forward proxies; they handle requests from external systems to services on the internal network. Some proxy servers can also be configured with rules, like a firewall. For example, you can create filters to block websites identified as containing malware.

Virtual Private Networks (VPN)

A VPN is a service that encrypts data in transit and disguises your IP address. VPNs use a process called encapsulation. Encapsulation wraps your encrypted data in an unencrypted data packet, which allows your data to be sent across the public network while remaining anonymous. Enterprises and other organizations use VPNs to help protect communications from users' devices to corporate resources. Some of these resources include connecting to servers or virtual machines that host business applications. VPNs can also be used for personal use to increase personal privacy. They allow the user to access the internet without anyone being able to read their personal information or access their private IP address. Organizations

are increasingly using a combination of VPN and SD-WAN capabilities to secure their networks. A software-defined wide area network (SD-WAN) is a virtual WAN service that allows organizations to securely connect users to applications across multiple locations and over large geographical distances.

Key takeaways

There are three main categories of network protocols: communication, management, and security protocols. In this reading, you learned the fundamentals of firewalls, proxy servers, and VPNs. More organizations are implementing a cloud-based approach to network security by incorporating a combination of VPN and SD-WAN capabilities as a service.