Glossary terms from module 2

Terms and definitions from Course 3, Module 2

Address Resolution Protocol (ARP): A network protocol used to determine the MAC address of the next router or device on the path

Cloud-based firewalls: Software firewalls that are hosted by the cloud service provider

Controlled zone: A subnet that protects the internal network from the uncontrolled zone

Domain Name System (DNS): A networking protocol that translates internet domain names into IP addresses

Encapsulation: A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets

Firewall: A network security device that monitors traffic to or from your network

Forward proxy server: A server that regulates and restricts a person’s access to the internet

Hypertext Transfer Protocol (HTTP): An application layer protocol that provides a method of communication between clients and website servers

Hypertext Transfer Protocol Secure (HTTPS): A network protocol that provides a secure method of communication between clients and servers

IEEE 802.11 (Wi-Fi): A set of standards that define communication for wireless LANs

Network protocols: A set of rules used by two or more devices on a network to describe the order of delivery of data and the structure of data

Network segmentation: A security technique that divides the network into segments

Port filtering: A firewall function that blocks or allows certain port numbers to limit unwanted communication

Proxy server: A server that fulfills the requests of its clients by forwarding them to other servers

Reverse proxy server: A server that regulates and restricts the internet's access to an internal server

Secure File Transfer Protocol (SFTP): A secure protocol used to transfer files from one device to another over a network

Secure shell (SSH): A security protocol used to create a shell with a remote system

Security zone: A segment of a company's network that protects the internal network from the internet

Simple Network Management Protocol (SNMP): A network protocol used for monitoring and managing devices on a network

Stateful: A class of firewall that keeps track of information passing through it and proactively filters out threats

Stateless: A class of firewall that operates based on predefined rules and does not keep track of information from data packets

Subnetting: The subdivision of a network into logical groups called subnets

Transmission Control Protocol (TCP): An internet communication protocol that allows two devices to form a connection and stream data

Uncontrolled zone: The portion of the network outside the organization

Virtual private network (VPN): A network security service that changes your public IP address and masks your virtual location so that you can keep your data private when you are using a public network like the internet

Wi-Fi Protected Access (WPA): A wireless security protocol for devices to connect to the internet