Subnetting and CIDR

Earlier in this course, you learned about network segmentation, a security technique that divides networks into sections. A private network can be segmented to protect portions of the network from the internet, which is an unsecured global network.

For example, you learned about the uncontrolled zone, the controlled zone, the demilitarized zone, and the restricted zone. Feel free to review the video about security zones for a refresher on how network segmentation can be used to add a layer of security to your organization's network operations. Creating security zones is one example of a networking strategy called subnetting.

Overview of subnetting

Subnetting is the subdivision of a network into logical groups called subnets. It works like a network inside a network. Subnetting divides up a network address range into smaller subnets within the network. These smaller subnets form based on the IP addresses and network mask of the devices on the network. Subnetting creates a network of devices to function as their own network. This makes the network more efficient and can also be used to create security zones. If devices on the same subnet communicate with each other, the switch changes the transmissions to stay on the same subnet, improving speed and efficiency of the communications.

Classless Inter-Domain Routing notation for subnetting

Classless Inter-Domain Routing (CIDR) is a method of assigning subnet masks to IP addresses to create a subnet. Classless addressing replaces classful addressing. Classful addressing was used in the 1980s as a system of grouping IP addresses into classes (Class A to Class E). Each class included a limited number of IP addresses, which were depleted as the number of devices connecting to the internet outgrew the classful range in the 1990s. Classless CIDR addressing expanded the number of available IPv4 addresses.

CIDR allows cybersecurity professionals to segment classful networks into smaller chunks. CIDR IP addresses are formatted like IPv4 addresses, but they include a slash ("/") followed by a number at the end of the address, This extra number is called the IP network prefix. For example, a regular IPv4 address uses the 198.51.100.0 format, whereas a CIDR IP address would include the IP network prefix at the end of the address, 198.51.100.0/24. This CIDR address encompasses all IP addresses between 198.51.100.0 and 198.51.100.255. The system of CIDR addressing reduces the number of entries in routing tables and provides more available IP addresses within networks. You can try converting CIDR to IPv4 addresses and vice versa through an online conversion tool, like IPAddressGuide, for practice and to better understand this concept.

Note: You may learn more about CIDR during your career, but it won't be covered in any additional depth in this certificate program. For now, you only need a basic understanding of this concept.

Security benefits of subnetting

Subnetting allows network professionals and analysts to create a network within their own network without requesting another network IP address from their internet service provider. This process uses network bandwidth more efficiently and improves network performance. Subnetting is one component of creating isolated subnetworks through physical isolation, routing configuration, and firewalls.

Key takeaways

Subnetting is a common security strategy used by organizations. Subnetting allows organizations to create smaller networks within their private network. This improves the efficiency of the network and can be used to create security zones.