8.3.8 Firewall Design and Configuration Facts

A *demilitarized zone* (DMZ) is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the internet).

- Create a DMZ by performing the following:
  - Configure two firewall devices, one connected to the public network and one connected to the private network.
  - Configure a single device with three network cards, one connected to the public network, one connected to the private network, and one connected to the screened subnet.
  - Configure a single device with two network cards, one connected to the public network and another connected to a private subnet containing hosts that are accessible from the private network. Configure proxy ARP so the public interface of the firewall device responds to ARP requests for the public IP address of the device.
- Publicly accessible resources (servers) are placed inside the screened subnet. Examples of publicly accessible resources include web, FTP, or email servers.
- Packet filters on the outer firewall allow traffic directed to the public resources inside the DMZ. Packet filters on the inner firewall prevent unauthorized traffic from reaching the private network.
- If the firewall managing traffic into the DMZ fails, only the servers in the DMZ are subject to compromise. The LAN is protected by default.
- When designing the outer firewall packet filters, a common practice is to close all ports and open only the ports necessary for accessing the public resources inside the DMZ.
- Typically, firewalls allow traffic that originates in the secured internal network into the DMZ and through to the internet. Traffic that originates in the DMZ (low-security area) or the internet (no-security area) should not be allowed access to the intranet (high-security area).

Do not place any server in the DMZ that doesn't have to be there.

Firewall Types

There are two types of firewalls:

- A *routed firewall*, is also a Layer 3 router. In fact, many hardware routers include firewall functionality. Transmitting data through this type of firewall counts as a router hop. A routed firewall usually supports multiple interfaces, each connected to a different network segment.
- A *transparent firewall*, also called a *virtual firewall*, operates at Layer 2 and is not seen as a router hop by connected devices. Both the internal and external interfaces on a transparent firewall connect to the same network segment. Because it is not a router, you can easily introduce a transparent firewall into an existing network.

Access Control List (ACL)

Access control lists (ACLs) are rules firewalls use to manage incoming or outgoing traffic. You should be familiar with the following ACL characteristics:

- ACLs describe the traffic type that will be controlled.
- ACL entries:
  - Describe traffic characteristics.
  - Identify permitted and denied traffic.
  - Can describe a specific traffic type, allow all traffic, or restrict all traffic.
- An ACL usually contains an implicit **deny any** entry at the end of the list.
- Each ACL applies only to a specific protocol.
- Each router interface can have up to two ACLs for each protocol, one for incoming traffic and one for outgoing traffic.
- When an ACL is applied to an interface, it identifies whether the list restricts incoming or outgoing traffic.
- Each ACL can be applied to more than one interface. However, each interface can have only one incoming list and one outgoing list.
- ACLs can be used to log traffic that matches the list statements.

Many hardware routers, such as those from Cisco, also provide a packet filtering firewall. These devices are frequently used to fill both network roles (router and firewall) at the same time.

When you create an ACL on a Cisco device, a **deny any** statement is automatically added at the end of the list (this statement does not appear in the list itself). For a list to allow any traffic, it must have at least one permit statement that either permits a specific traffic type or permits all traffic not specifically restricted.

There are two general types of access lists used on Cisco devices:

Access List Type	Characteristics
Standard ACL	Standard ACLs: - Can filter only on source host name or host IP address.

	- Should be placed as close to the destination as possible. - Use the following number ranges: - 1–99 - 1300–1999
Extended ACL	Extended ACLs: - Can filter by: - Source IP protocol (IP, TCP, UDP, and so on) - Source host name or host IP address - Source or destination socket number - Destination host name or host IP address - Precedence or TOS values - Should be placed as close to the source as possible. - Use the following number ranges: - 100–199 - 2000–2699