5.4.4 DMZ 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). A DMZ typically contains publicly-accessible resources, such as Web, FTP, or email servers. Creating a *demilitarized zone* (DMZ) is part of a layered security approach.

Be aware of the following DMZ facts:

- 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.
- Packet filters on the firewall allow traffic directed to the public resources inside the DMZ. Packet filters also prevent unauthorized traffic from reaching the private network.
- When designing the firewall packet filters, a common practice is to close all ports, opening only those ports necessary for accessing the public resources inside the DMZ.
- To allow access to private resources from the internet, use one of the following approaches:
  - Place a VPN server inside the DMZ. Require internet users to authenticate to the VPN server. Then allow communications from the VPN server to the private network. Only communications coming through the VPN server are allowed through the inner firewall.
  - Copy resources that are accessible to internet users to servers inside the DMZ. Even with authentication and authorization configured, this approach exposes those resources in the DMZ to internet attacks.
- Typically, firewalls allow traffic originating 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).

Only places servers in the DMZ that need to be there.

The following terms are related to DMZs.

Term	Definition
Bastion or Sacrificial Host	A *bastion host* is any host that is exposed to attack and that has been hardened (or fortified) against those attacks. The bastion host is sometimes referred to as a *sacrificial host* because it is assumed that it will be subject to attack. The term has been applied to the following types of devices: • A host that is exposed on the network and is not protected by a firewall device. • The device that provides the firewall service to the screened network behind it. Attacks must pass through the bastion host before they are allowed inside the screened subnet. • A honey pot device that is purposefully exposed to attack in order to distract attackers. The following actions should be taken to harden a bastion host: • Separate roles of bastion hosts by placing a single application on each server. • Fully patch your bastion host on the operating system and on applications. • Run current versions of anti-virus and anti-spyware software. • Include a personal firewall. • Uninstall any unnecessary applications or utilities. • Disable and lock down all unnecessary services and ports. • Tighten security on the registry and the user database. • Add IP filters. • Run lockdown facilities, such as IIS lock down and URLScan.
Screening Router	A *screening router* is the router that is most external to your network and closest to the internet. It uses access control lists (ACLs) to filter packets as a form of security. A firewall performing router functions is considered a screening router.
Dual-Homed Gateway	A *dual-homed gateway* is a firewall device that typically has three network interfaces: one connected to the Internet, one connected to the public subnet, and one connected to the private network. Gateways have to be logged on to, whereas routers pass traffic through without user authentication. IP forwarding is disabled on gateways, effectively blocking through traffic to the network.
Screened Host Gateway	A *screened host gateway* resides within the DMZ, requiring users to authenticate in order to access resources within the DMZ or the intranet.
Screened Subnet	A *screened subnet* uses two firewalls. The external firewall is connected to the internet and allows access to the public resources; the internal firewall connects the screened subnet to the private network. With a screened subnet, if the outer firewall is compromised, the inner firewall still protects the private network.