5.3.3 Security Zone Facts

Security *zones* are portions of the network or system that have specific security concerns or requirements. All devices with the same zone have the same security access and security protection needs. These zones are often separated by a traffic control device, such as a firewall or a router, that filters incoming and outbound traffic. For example, you can define a zone that includes all hosts on your private network protected from the internet. You can also define a zone within your network for controlled access to specific servers that hold sensitive information.

The following table lists types of networks found in your security zones:

Network Type	Description
Wireless	A wirelessly broadcasted network is used on most internal networks, usually in the intranet zone, so that internal users do not require a physical connection.
Guest	A guest network at an organization often grants only internet access for guest users, but also has some type of firewall to regulate that access. There could be limited internal resources made available on a guest network. Normally, it is just a way for guests to access the internet without being allowed on the intranet or internal network.
Honeynet	A *honeynet* is a special zone or network created to trap potential attackers. Honeynets have vulnerabilities that lure attacks so that you can track their actions. Honeypots can generate extremely useful security information.
Ad Hoc	An *ad hoc* network is a decentralized network that allows connections without a traditional base station or router. It allows users to connect two or more devices directly to each other for a specific purpose.

The following table lists common zones:

Zone	Description
Intranet	An *intranet* is a private network (LAN) that employs internet information services for internal use only. For example, your company network might include web servers and email servers that are used by company employees.
Internet	The *internet* is a public network that includes all publicly available web servers, FTP servers, and other services. The internet is public because access is largely open to everyone.
Extranet	An *extranet* is a privately-controlled network distinct from but located between the internet and a private LAN. An extranet is often used to grant resource access to business partners, suppliers, and even customers outside of the organization.
Demilitarized Zone	A *demilitarized zone* (DMZ) is a network that contains publicly accessible resources. The DMZ is located between the private network and an untrusted network (such as the internet) and is protected by a firewall. A *bastion host* is *a* server that is exposed to attacks by untrusted networks. It can be placed inside the DMZ or exposed on the public network.