# 5.1.3 Security Zone Facts

This lesson covers the following topics:

- Security zones
- Security zone networks
- Common security zones

## Security Zones

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.

## Security Zone Networks

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 so that internal users do not require a physical connection to a router or switch. |
| Guest | A guest network at an organization often grants internet access only for guest users, but it 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 network created to trap potential attackers. Honeynets have vulnerabilities that lure attacks so that you can track their actions and protect your real network. Honeynets 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. |

## Common Security Zones

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 the intranet 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. |
| Wireless | A wireless zone is a broadcasted network connection used within an organization. Users don't need a physical connection to a network port to connect to the intranet or internal resources. Instead they use a wireless connection on their device to connect to a wireless access point. |
| 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.<br><br>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. |