DMZ configurations

A DMZ is an area between the private network (intranet) and a public network (extranet) such as the Internet. A DMZ isn't a direct part of either network, but is instead an additional network between the two networks.

Computers in the DMZ are accessible to nodes on both the Internet and intranet. Typically, computers within the DMZ have limited access to nodes on the intranet. But, direct connections between the Internet and nodes on the internal network are blocked.

For example, you might put your company's mail server in a DMZ. Users on both the internal network and the Internet will need access to the mail server. The mail server might need to communicate with internal storage servers to save files and other data. But, Internet users shouldn't have access to your internal network.

You can set up a DMZ in several ways:

- Screened host
- Bastion host
- Three-homed firewall
- Back-to-back firewall
- Dead zone

Screened host

With a screened host, a router is used to filter all traffic to the private intranet but also to allow full access to the computer in the DMZ. The router is solely responsible for protecting the private network (see Exhibit 9-3). The IP address of the DMZ host is entered in the router configuration. This IP address is allowed full Internet access, but other computers on the network are protected behind the firewall provided by the router. The disadvantage of this setup is that sometimes a router firewall can fail and allow traffic through to the intranet.

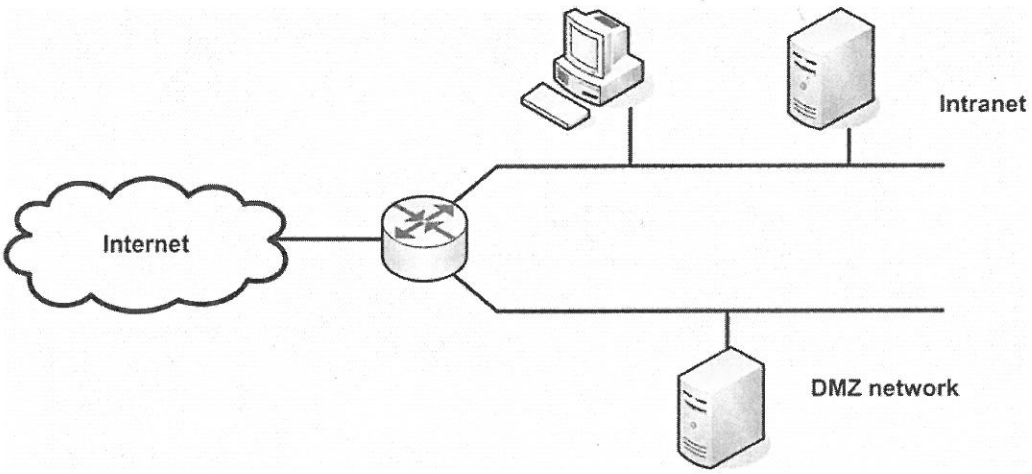

Exhibit 9-3: A screened host DMZ

In addition to using a router to protect a network, an administrator can also use subnets and subnet masks to protect the private network from a screened host. If the screened host is on one subnet and all other computers on the private intranet are on another subnet, if the screened host is penetrated, the intranet on another subnet is less likely to be compromised.