13.10.6 Network Appliance Facts

Network appliances are devices that are dedicated to providing certain network services. Common network appliances include:

- Switches
- Wireless access points
- Routers
- Firewalls
- Security threat management devices

These devices are unlike common network hosts in that they don't typically provide monitor, keyboard, or mouse connections. Instead, they are designed to be plugged directly into the network and then managed using a web-based interface from the system administrator's workstation.

Large organizations typically purchase separate appliances for each network function they require. However, this strategy can be quite expensive. To reduce costs, smaller organizations may choose to use an all-in-one device instead of purchasing separate network appliances. For example, an all-in-one security appliance combines many network security functions into a single device. All-in-one security appliances are also known as unified threat security devices or web security gateways. This type of device may be the best choice for:

- A small company without the budget to purchase individual components
- A small office without the physical space for individual components
- A remote office without a technician to manage individual security components

Security functions implemented within an all-in-one security appliance may include components such as:

- An endpoint management server to keep track of various devices, while ensuring their software is secure
- A network switch to provide internal network connectivity between hosts
- A router to connect network segments together
- An ISP interface for connecting the local network to the internet
- A firewall to filter network traffic
- A syslog server to store event messages
- A spam filter to block unwanted emails
- A web content filter to prevent employees from visiting inappropriate websites
- A malware inspection engine to prevent malware from entering the network
- An intrusion detection system (IDS) or intrusion prevention system (IPS) to detect hackers trying to break into systems on the network

    An IDS detects intrusion attempts and alerts the system administrator. An IPS detects intrusion attempts, notifies the administrator, and also tries to block the attempt.

While they are less expensive, all-in-one appliances have several drawbacks that you should consider before implementing one:

- All-in-one appliances perform many tasks adequately. However, they usually can't perform any one task extremely well. If high-performance is a concern, then using dedicated appliances might be more appropriate.
- All-in-one devices create a single point of failure. Because so many services are hosted by a single device, then all of the services are affected if that device goes down.
- All-in-one devices create a single attack vector that can be exploited by an attacker. Compromising the single device could potentially expose many aspects of the network.

Unified threat management (UTM) or unified security management (USM), is a network gateway defense solution for organizations. UTM is the evolution of the traditional firewall into an all-in-one device that can perform multiple security functions within one single system.