Network Security Components

Routers transfer network connections at Layer 3 of the OSI reference model, where more routing features become available, for example, packets. Routers are configurable to handle more complex routing tasks. They support security by guiding traffic down preferred routes rather than routes that might not be as logically or physically secure. An attacker can trick a router into altering the pathway of transmission, sending network traffic across a segment where a hacker has positioned a "sniffer." A sniffer is a packet analyzer, just like those used by security personnel. To avoid this situation, you can use authentication to exchange routing data. Routers bridge internal and external connections alike, but switches primarily serve internal functions. Routers have greater exposure to external attacks and attackers.

Switches transfer network connections usually at Layer 2 of the OSI reference model, the lowest level of logical traffic flow. They also allow you to segment a network. You can limit who may access each segment and the kind of traffic that will be allowed to reach each segment. In addition, because network traffic flows through a switch, you can monitor the activity of the switch and watch for errors and malicious traffic. Switches are reachable only from the inside. Redirection attacks are possible in both routers and switches.

A *dual-homed host* is a firewall that uses two separate network interfaces. It filters internal traffic separately and casually on one interface and external traffic separately and carefully on another interface. It creates disconnect between end users and external users.

Network tunneling encapsulates data for secure transport. It encapsulates confidential messages for transport. However, it may encapsulate unauthorized transmissions as well.

Wireless Security Considerations

- Attackers can leverage weaknesses specific to wireless.
- Radio signals reach more people than network ports.
- Accidental and malicious associations are a concern.
- Ad hoc or peer-to-peer associations are problematic.
- Weak security standards can expose sensitive data.

Wireless Security Countermeasures

- Use Wi-Fi-Protected Access (WPA).
- Disable Service Set Identifier (SSID) beaconing.
- Use strong authentication and cryptography to maintain integrity.
- Include Remote Authentication Dial-In User Service (RADIUS) authentication in enterprises.
- Use radio frequency (RF) shielding to keep signals within buildings.
- Ask for smartcards and tokens for authentication.