9.11.2 DLP Facts

Data loss prevention (DLP) is a system that attempts to detect and stop breaches of sensitive data within an organization. Sensitive data is monitored by the DLP system in four different states:

- While in use on endpoint systems
- While in motion as it is transmitted over the network
- While at rest on a storage medium
- While being transmitted to or from cloud-based systems

Accordingly, there are many ways in which DLP can be implemented. Be familiar with the following:

- *Network DLP* is a software or hardware solution that is typically installed near the network perimeter. It analyzes network traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.
- *Endpoint DLP* runs on end-user workstations and servers. Endpoint DLP is also referred to as a Chinese Wall solution. It could be something as simple as restricting the use of USB devices (USB blocking).
- *File-Level DLP* is used to identify sensitive files in a file system and then to embed the organization's security policy within the file so that it travels with the file when it is moved or copied.
- *Cloud DLP* is a software solution that is typically on cloud-based systems. It analyzes traffic to and from cloud systems in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

A related security system is unified threat management (UTM). A UTM can be implemented as a single network appliance or as a service on the network. UTMs are sometimes referred to as next-generation firewalls. UTMs provide multiple security features and services, including:

- Anti-malware
- Anti-spam
- Content filtering
- Web filtering
- Firewall
- Intrusion detection
- VPN