Network Security

All topics:

* Describe the security threats facing modern network infrastructures.
* Secure Cisco devices.
* Secure the network infrastructure.
* Implement AAA on Cisco routers using a local router database and external AAA servers.
* Mitigate threats to Cisco routers and networks using access control lists (ACLs).
* Implement secure network design, management, and reporting.
* Implement the Cisco IOS firewall feature set.
* Mitigate common Layer 2 attacks.
* Implement a site-to-site VPN.
* Implement a remote access VPN.

Networks as Target

Network security relates directly to an organization's business continuity. Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people’s privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety.

**Vectors of Network Attacks**

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.

An internal user, such as an employee, can accidentally or intentionally:

* Steal and copy confidential data to removable media, email, messaging software, and other media.
* Compromise internal servers or network infrastructure devices.
* Disconnect a critical network connection and cause a network outage.
* Connect an infected USB drive into a corporate computer system.

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

Data loss, or data exfiltration, is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. The data loss can result in:

* Brand damage and loss of reputation
* Loss of competitive advantage
* Loss of customers
* Loss of revenue
* Litigation/legal action that results in fines and civil penalties.
* Significant cost and effort to notify affected parties and recover from the breach.

Various Data Loss Prevention (DLP) controls must be implemented that combine strategic, operational, and tactical measures.

