Network Attack Mitigations

16.3.1

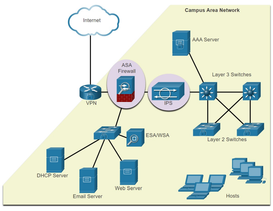
The Defense-in-Depth Approach

Now that you know more about how threat actors can break into networks, you need to understand what to do to prevent this unauthorized access. This topic details several actions you can take to make your network more secure.

To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach (also known as a layered approach) to security. This requires a combination of networking devices and services working in tandem.

Consider the network in the figure. There are several security devices and services that have been implemented to protect its users and assets against TCP/IP threats.

All network devices including the router and switches are also hardened by the combination locks on their respective icons. This indicates that they have been secured to prevent threat actors from gaining access and tampering with the devices.



Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats.

- **VPN** – A router is used to provide secure VPN services with corporate sites and remote access support for remote users using secure encrypted tunnels.
- **ASA Firewall** – This dedicated device provides stateful firewall services. It ensures that internal traffic can go out and come back, but external traffic cannot initiate connections to inside hosts.
- **IPS** – An intrusion prevention system (IPS) monitors incoming and outgoing traffic looking for malware, network attack signatures, and more. If it recognizes a threat, it can immediately stop it.
- **ESA/WSA** – The email security appliance (ESA) filters spam and suspicious emails. The web security appliance (WSA) filters known and suspicious internet traffic and provides reporting.
- **AAA Server** – This server contains a secure database of who is authorized to access and manage network devices. Network devices authenticate administrative users using this database.

16.3.2

Keep Backups

Backing up device configurations and data is one of the most effective ways of protecting against data loss. A data backup stores a copy of the information on a computer to removable backup media that can be kept in a safe place. Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy.

Backups should be performed on a regular basis as identified in the security policy. Data backups are usually stored offsite to protect the backup media if anything happens to the main facility. Windows hosts have a backup and restore utility. It is important for users to back up their data to another drive, or to a cloud-based storage provider.

The table shows backup considerations and their descriptions.

Consideration	Description
Frequency	• Perform backups on a regular basis as identified in the security policy. • Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files.
Validation	• Always validate backups to ensure the integrity of the data and validate the file restoration procedures.
Storage	• Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.
Security	• Backups should be protected using strong passwords. The password is required to restore the data.

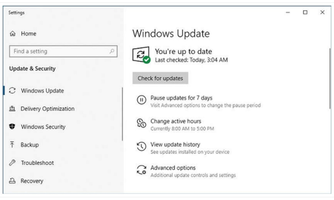
16.3.3

Upgrade, Update, and Patch

Keeping up to date with the latest developments can lead to a more effective defense against network attacks. As new malware is released, enterprises need to keep current with the latest versions of antivirus software.

The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. Administering numerous systems involves the creation of a standard software image (operating system and accredited applications that are authorized for use on client systems) that is deployed on new or upgraded systems. However, security requirements change, and already deployed systems may need to have updated security patches installed.

One solution to the management of critical security patches is to make sure all end systems automatically download updates, as shown for Windows 10 in the figure. Security patches are automatically downloaded and installed without user intervention.



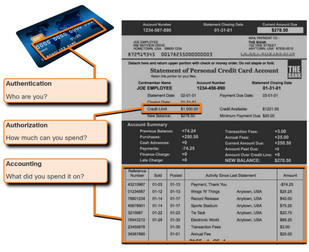
16.3.4

Authentication, Authorization, and Accounting

All network devices should be securely configured to provide only authorized individuals with access. Authentication, authorization, and accounting (AAA, or "triple A") network security services provide the primary framework to set up access control on network devices.

AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (accounting).

The concept of AAA is similar to the use of a credit card. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on, as shown in the figure.



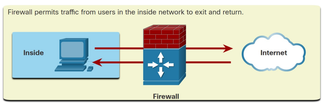
16.3.5

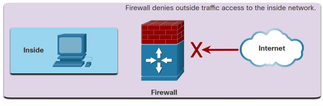
Firewalls

A firewall is one of the most effective security tools available for protecting users from external threats. A firewall protects computers and networks by preventing undesirable traffic from entering internal networks.

Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. For example, the top topology in the figure illustrates how the firewall enables traffic from an internal network host to exit the network and return to the inside network. The bottom topology illustrates how traffic initiated by the outside network (i.e., the internet) is denied access to the internal network.

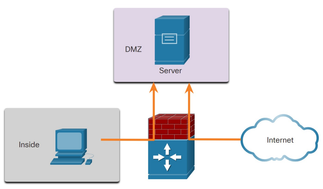
Firewall Operation





A firewall could allow outside users controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ), as shown in the figure. The DMZ enables a network administrator to apply specific policies for hosts connected to that network.

Firewall Topology with DMZ



16.3.6

Types of Firewalls

Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

- **Packet-filtering** – Prevents or allows access based on IP or MAC addresses.
- **Application filtering** – Prevents or allows access to specific application types based on port numbers.
- **URL filtering** – Prevents or allows access to websites based on specific URLs or keywords.
- **Stateful packet inspection (SPI)** – Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS).

16.3.7

Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets. Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules. Employees need to be trained on proper use of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

16.3.8

Check Your Understanding - Network Attack Mitigation

Check your understanding of network attack mitigation by choosing the BEST answer to the following questions.

1. Which device controls traffic between two or more networks to help prevent unauthorized access?
   - AAA Server
   - **firewall**
   - ESA/WSA
   - IPS
2. Which device is used by other network devices to authenticate and authorize management access?
   - **AAA Server**
   - firewall
   - ESA/WSA
   - IPS
3. Which backup policy consideration is concerned with using strong passwords to protect the backups and for restoring data?
   - frequency
   - storage
   - **security**
   - validation
4. This zone is used to house servers that should be accessible to outside users.
   - inside
   - outside
   - internet
   - **DMZ**
5. Which is appropriate for providing endpoint security?
   - a AAA server
   - **antivirus software**
   - a server-based firewall
   - an ESA/WSA

Check | Show Me | Reset