Network Security

1.8.1

Security Threats

You have, no doubt, heard or read news stories about a company network being breached, giving threat actors access to the personal information of thousands of customers. For this reason, network security is always going to be a top priority of administrators.

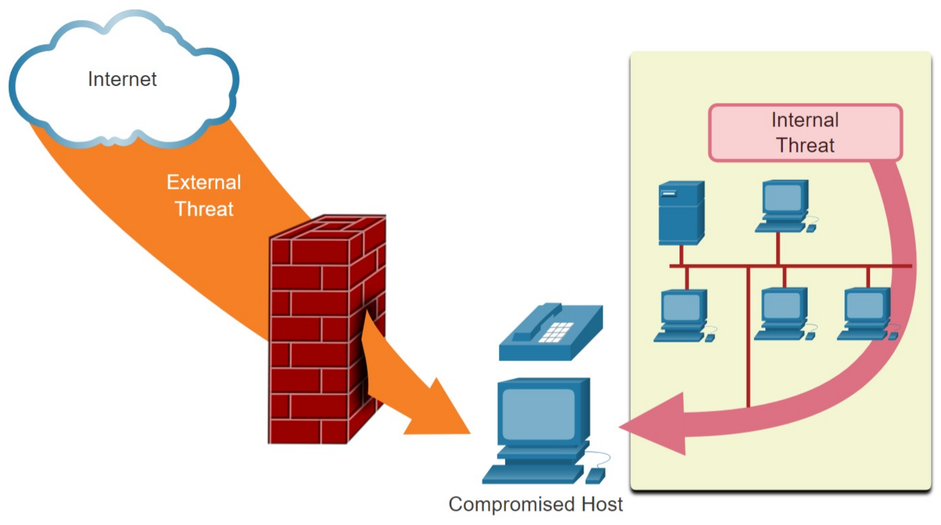
Network security is an integral part of computer networking, regardless of whether the network is in a home with a single connection to the internet or is a corporation with thousands of users. Network security must consider the environment, as well as the tools and requirements of the network. It must be able to secure data while still allowing for the quality of service that users expect of the network.

Securing a network involves protocols, technologies, devices, tools, and techniques in order to protect data and mitigate threats. Threat vectors may be external or internal. Many external network security threats today originate from the internet.

There are several common external threats to networks:

- **Viruses, worms, and Trojan horses** - These contain malicious software or code running on a user device.
- **Spyware and adware** - These are types of software which are installed on a user's device. The software then secretly collects information about the user.
- **Zero-day attacks** - Also called zero-hour attacks, these occur on the first day that a vulnerability becomes known.
- **Threat actor attacks** - A malicious person attacks user devices or network resources.
- **Denial of service attacks** - These attacks slow or crash applications and processes on a network device.
- **Data interception and theft** - This attack captures private information from an organization's network.
- **Identity theft** - This attack steals the login credentials of a user in order to access private data.

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats, as shown in the figure.



1.8.2

Security Solutions

No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others may succeed.

A home network security implementation is usually rather basic. Typically, you implement it on the end devices, as well as at the point of connection to the internet, and can even rely on contracted services from the ISP.

These are the basic security components for a home or small office network:

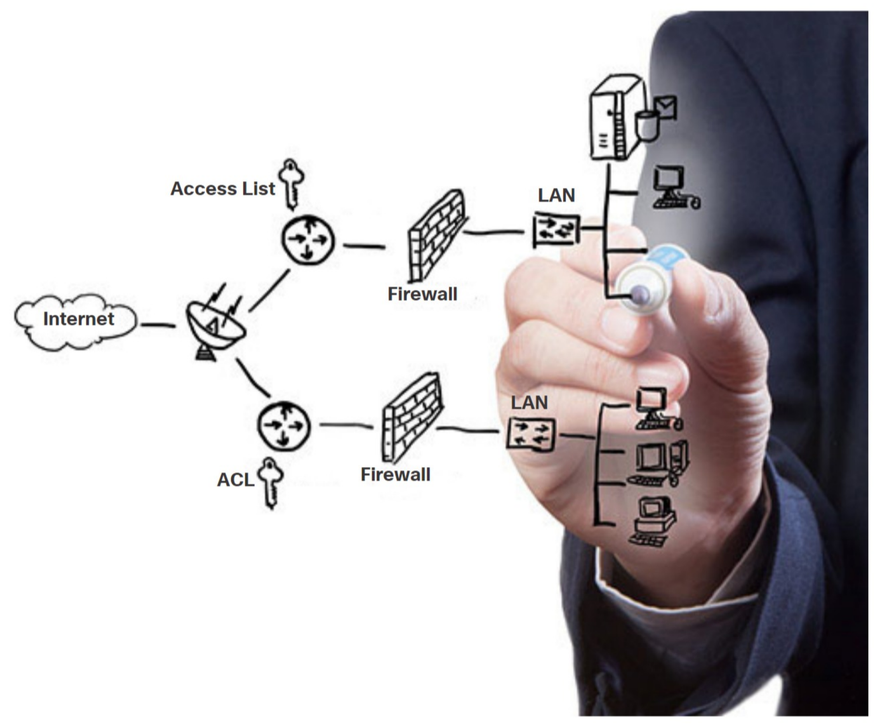
- **Antivirus and antispyware** - These applications help to protect end devices from becoming infected with malicious software.
- **Firewall filtering** - Firewall filtering blocks unauthorized access into and out of the network. This may include a host-based firewall system that prevents unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

In contrast, the network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security. Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

- **Dedicated firewall systems** - These provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
- **Access control lists (ACL)** - These further filter access and traffic forwarding based on IP addresses and applications.
- **Intrusion prevention systems (IPS)** - These identify fast-spreading threats, such as zero-day or zero-hour attacks.
- **Virtual private networks (VPN)** - These provide secure access into an organization for remote workers.

Network security requirements must consider the environment, as well as the various applications, and computing requirements. Both home and business environments must be able to secure their data while still allowing for the quality of service that users expect of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services.



1.8.3

Check Your Understanding - Network Security

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

1. Which attack slows down or crashes equipment and programs?
   - ( ) Firewall
   - ( ) Virus, worm, or Trojan horse
   - ( ) Zero-day or Zero-hour
   - ( ) Virtual Private Network (VPN)
   - (•) Denial of Service (DoS)
2. Which option creates a secure connection for remote workers?
   - ( ) Firewall
   - ( ) Virus, worm, or Trojan horse
   - ( ) Zero-day or Zero-hour
   - (•) Virtual Private Network (VPN)
   - ( ) Denial of Service (DoS)
3. Which option blocks unauthorized access to your network?
   - (•) Firewall
   - ( ) Virus, worm, or Trojan horse
   - ( ) Zero-day or Zero-hour
   - ( ) Virtual Private Network (VPN)
   - ( ) Denial of Service (DoS)
4. Which option describes a network attack that occurs on the first day that a vulnerability becomes known?
   - ( ) Firewall
   - ( ) Virus, worm, or Trojan horse
   - (•) Zero-day or Zero-hour
   - ( ) Virtual Private Network (VPN)
   - ( ) Denial of Service (DoS)
5. Which option describes malicious code running on user devices?
   - ( ) Firewall
   - (•) Virus, worm, or Trojan horse
   - ( ) Zero-day or Zero-hour
   - ( ) Virtual Private Network (VPN)
   - ( ) Denial of Service (DoS)

Check

Show Me

Reset