A GUIDE TO UNDERSTANDING

NETWORK SECURITY

DATA NETWORKS

INTERNATIONAL

1 fits your budget!

Everyone wants to secure their data from cyberattacks, but how do you go about reducing your vulnerabilities? Combining a variety of network security hardware, software, and security methods is the best way to protect your network from protentional threats.

What is Network Security?

Cisco Systems, a leader in the industry, defines Network Security as any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies.
- It targets a variety of threats.
- It stops them from entering or spreading on your network.
- Effective network security manages access to the network.

Not only should your security manage the access to the network, but it should be able to prevent a possible attack from spreading. With the internet being a necessity in today's world, taking the steps to ensure protection and minimize any down time is essential.

How does network security work?

Through combining multiple layers of defense at the edge and inside the network, a network security system provides an active line of protection. With several layers of security, authorized users can gain access while potential threats are blocked from private information. All network security solutions are implemented in accordance with the core principles of network security.

The Core Principals of Network Security

The core principles that work together to ensure network security are confidentiality, integrity, and availability. These are defined as:

- **Confidentiality:** Data is kept protected against threats and unauthorized access.

- **Integrity**: Data is kept accurate and trustworthy by preventing accidental or intentional alterations or deletion.
- **Availability**: Data is kept accessible to those who are authorized to have access.

Components of Network Security

For a complete security system, three components should be part of your design including hardware, software, and cloud security.

Hardware components include tangible equipment including servers and devices that perform an array of security operations within a network. Hardware components can be set up in two ways:

- Out of band: Operating as a separate entity from network traffic, out-of-line security appliances are tasked with monitoring traffic and raising alerts when they detect malicious data.
- In-line: A more popular option of the two, in-line hardware appliances are tasked with directly blocking data packets the moment they run into potential threats.

Security **software** components are installed on devices across the network, providing added detection capabilities and threat remediation. The far most common form of software network security components are antivirus applications.

Lastly, **cloud** services entail offloading the security infrastructure onto a cloud provider. The protection strategy is similar to in-line hardware appliances as all the network traffic goes through the cloud provider. While there, the traffic gets scanned for potential threats before either being blocked or allowed into the network.

The most protected networks should have a combination of components working at once. Using multilayered protection creates a web of safety nets to stop a threat if it manages to slip through the cracks of one component.

Layered Security

Layered security is a network security practice that combines multiple security controls to protect networks against threats. By using a layered security approach, a network has the greatest amount of coverage possible to address the wide variety of security threats that could infiltrate the network. A layered security approach also provides added opportunities for threat detection and response if a threat bypasses one of the security layers.

For example, to secure a house against outside intruders a homeowner may use a fence, locks on the doors, security cameras, and a guard dog. Each added layer of security increases the overall effectiveness of the defense strategy while simultaneously adding unique threat detection and prevention capabilities that complement and supplement the other security measures.

Types of Network Security, Methods, and Tools

Access Control & Authentication

Access control and authentication measures protect networks and data by validating user credentials and ensuring that those users are only permitted to access the data that is necessary for their role. Tools that aid access control and authentication include privileged access management (PAM), Identity as a Service (IaaS) providers, and network access control (NAC) solutions.

Access control and authentication solutions are also used to verify that valid users are accessing the network from secured endpoints. To verify, it performs a ‘health check’ that ensures the latest security updates and prerequisite software are installed on the endpoint device.

Anti-Virus & Anti-Malware

Anti-virus and anti-malware protect networks from malicious software that is used by threat actors to create a backdoor that they can use to further infiltrate the network. It’s important to note that while there are similarities between anti-virus and anti-malware programs, they are not exactly the same.

- **Anti-Virus:** Prevention-based, protects networks by proactively stopping endpoint devices from becoming infected.
- **Anti-Malware:** Treatment-based, protects networks by detecting and destroying malicious programs that have infiltrated the network.

As the nature of malicious software is continually evolving, implementing both network security options in conjunction is the best method for ensuring network security.

Application Security

Application security ensures that the software used throughout the network is secure. Application security is ensured by limiting the amount of software that is used, ensuring that software is kept up to date with the latest security patches and that applications developed for use in the network are appropriately hardened against potential exploits.

Behavioral Analytics

Behavioral analytics is an advanced threat detection method that compares historical network activity data to current events to detect anomalous behavior. An example of this would be if a user typically uses a given endpoint device to access a specific database somewhere between 3-4 times per day on average, an instance where that user instead uses a new endpoint device to access a different database several times would be flagged for review.

DDoS Prevention

Distributed denial-of-service (DDoS) attacks attempt to crash the network by overloading it with a large influx of incoming connection requests. DDoS prevention solutions analyze incoming requests to identify and filter out illegitimate traffic to maintain the network's accessibility for legitimate connections.

DDoS attacks are either carried out through a distributed network of attackers that execute scripts to send a large volume of incoming requests to the network or through a widespread series of devices that have been compromised and converted into an orchestrated system known as a *botnet.*

Data Loss Prevention (DLP)

Data loss prevention (DLP) tools protect the data inside a network by preventing users from sharing sensitive or valuable information outside of the network and ensuring that data is not lost or misused. This can be accomplished by analyzing files that are sent via email, file transfers, and instant messages for data that is sensitive, such as personally identifiable information (PII).

Email Security

Email security measures protect networks from phishing attacks that attempt to trick users into clicking links to malicious websites or downloading seemingly innocent attachments that introduce malware into the network. Email security tools proactively fight phishing by identifying suspicious emails and filtering them out before they reach the user's inbox.

According to the 2019 Verizon Data Breach Investigations Report (DBIR), 94% of malware was discovered to have been delivered via email and 32% of data breaches involved phishing attacks. Email security tools complement anti-phishing training by reducing the volume of malicious emails that pass through the network and into the inboxes of users.

Endpoint Security

Endpoint security protects networks by ensuring that the devices that will be connected to the network are secured against potential threats. Endpoint security is achieved alongside network security by combining several other network security tools such as network access control, application security, and network monitoring.

An **endpoint device** is any piece of hardware that is connected to a local area network (LAN) or wide area network (WAN), such as workstations, laptops, smartphones, printers, and mobile kiosks.

Firewalls

Firewalls are hardware appliances and software programs that act as a barrier between incoming traffic and the network. The firewall compares data packets that are sent over the network to predefined policies and rules that indicate whether the data should be permitted into the network.

Mobile Device Security

Mobile device security centers around limiting the access that mobile devices have to the network and ensuring that the security vulnerabilities of mobile devices that are permitted on the network are monitored and managed.

Mobile device security measures include mobile device management (MDM) solutions that allow administrators to segment sensitive data on mobile devices, enforce data encryption, determine the applications that are permitted to be installed, locate lost or stolen devices, and remotely wipe sensitive data.

Network Monitoring & Detection Systems

Network monitoring & detection systems include a wide variety of applications that are designed to monitor incoming and outgoing network traffic and respond to anomalous or malicious network activity.

Examples of network monitoring & detection systems:

- **Intrusion Prevention Systems (IPS)** scan network traffic for suspicious activity such as policy violations to automatically block intrusion attempts.
- **Intrusion Detection Systems (IDS)** work similarly to IPS, with an emphasis on monitoring network packets and flagging suspicious activity for review.
- **Security Information and Event Management (SIEM)** provide a detailed overview of network events using a combination of host-based and network-based intrusion detection methods. SIEM systems provide administrators with valuable log data for investigating security incidents and flagging suspicious behavior.

Network Segmentation

Network segmentation is a common network security practice for reducing the ease of which network security threats can spread. Network segmentation involves classifying a larger network into multiple subnetworks, with each subnetwork being managed with its own unique access controls. Each subnetwork acts as its own unique network to improve monitoring capabilities, boost network performance, and enhance security.

Virtual Private Networks (VPN)

Virtual private networks provide secure remote access from a given endpoint into a network. A VPN encrypts all network traffic that goes through it to prevent the unauthorized analysis of data sent to and from the network. It is often used by off-site workers that need a secure connection to their company’s network, allowing them to access data and applications that are necessary for their role.

Web Security

Web security protects networks by proactively protecting endpoint devices against web-based threats. Web security technologies such as a web filter will use a database of known malicious or vulnerable websites to maintain a blacklist, block commonly exploited network ports, and prevent users from engaging in high-risk activities on the internet.

Web filtering solutions can be configured to only allow pre-authorized domains that are on the web filter’s whitelist. When a whitelist is used the web filter will block access to all websites that are not on the whitelist.

Web security products may also include capabilities for analyzing connection requests to a website and determining if the website meets the minimum-security requirements of the network before allowing users to access it.

Wireless Security

Wireless security measures protect the network against vulnerabilities that are unique to wireless connections. Wi-Fi networks openly broadcast connections to nearby devices, creating added opportunities for nearby threat actors to attempt to access the network. Wireless security is enhanced through methods such as encrypting data passed over wireless networks, filtering MAC addresses to restrict access, and privatizing the network SSID to avoid broadcasting the name of the network.

Conclusion

To safeguard your network, a customized system needs to be installed and managed. Using multi-layered prevention is the safest approach to ensure that your data is protected.

If you have more questions, a specialist will be happy to assist in creating a customized plan for your needs. Sales@DNI-LLC.com or by phone 973-383-3832

DATA NETWORKS
INTERNATIONAL
Now IT fits your budget!