Benefits of Network Security

Network Security is vital in protecting client data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats. A well designed network security solution reduces overhead expenses and safeguards organizations from costly losses that occur from a data breach or other security incident. Ensuring legitimate access to systems, applications and data enables business operations and delivery of services and products to customers.

Types of Network Security Protections

Firewall

Firewalls control incoming and outgoing traffic on networks, with predetermined security rules. Firewalls keep out unfriendly traffic and is a necessary part of daily computing. Network Security relies heavily on Firewalls, and especially Next Generation Firewalls, which focus on blocking malware and application-layer attacks.

Network Segmentation

Network segmentation defines boundaries between network segments where assets within the group have a common function, risk or role within an organization. For instance, the perimeter gateway segments a company network from the Internet. Potential threats outside the network are prevented, ensuring that an organization’s sensitive data remains inside. Organizations can go further by defining additional internal boundaries within their network, which can provide improved security and access control.

What is Access Control?

Access control defines the people or groups and the devices that have access to network applications and systems thereby denying unsanctioned access, and maybe threats. Integrations with Identity and Access Management (IAM) products can strongly identify the user and Role-based Access Control (RBAC) policies ensure the person and device are authorized access to the asset.

Zero Trust Remote Access VPN

Remote access VPN provides remote and secure access to a company network to individual hosts or clients, such as telecommuters, mobile users, and extranet consumers. Each host typically has VPN client software loaded or uses a web-based client. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint compliance scanning, and encryption of all transmitted data.

Zero Trust Network Access (ZTNA)

The zero trust security model states that a user should only have the access and permissions that they require to fulfill their role. This is a very different approach from that provided by traditional security solutions, like VPNs, that grant a user full access to the target network. Zero trust network access (ZTNA) also known as software-defined perimeter (SDP) solutions permits granular access to an organization's applications from users who require that access to perform their duties.

Email Security

Email security refers to any processes, products, and services designed to protect your email accounts and email content safe from external threats. Most email service providers have built-in email security features designed to keep you secure, but these may not be enough to stop cybercriminals from accessing your information.

Data Loss Prevention (DLP)

Data loss prevention (DLP) is a cybersecurity methodology that combines technology and best practices to prevent the exposure of sensitive information outside of an organization, especially regulated data such as personally identifiable information (PII) and compliance related data: HIPAA, SOX, PCI DSS, etc.

Intrusion Prevention Systems (IPS)

IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and exploits of known vulnerabilities. A vulnerability is a weakness for instance in a software system and an exploit is an attack that leverages that vulnerability to gain control of that system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to quickly block these attacks.

Sandboxing

Sandboxing is a cybersecurity practice where you run code or open files in a safe, isolated environment on a host machine that mimics end-user operating environments. Sandboxing observes the files or code as they are opened and looks for malicious behavior to prevent threats from getting on the network. For example malware in files such as PDF, Microsoft Word, Excel and PowerPoint can be safely detected and blocked before the files reach an unsuspecting end user.

Hyperscale Network Security

Hyperscale is the ability of an architecture to scale appropriately, as increased demand is added to the system. This solution includes rapid deployment and scaling up or down to meet changes in network security demands. By tightly integrating networking and compute resources in a software-defined system, it is possible to fully utilize all hardware resources available in a clustering solution.

Cloud Network Security

Applications and workloads are no longer exclusively hosted on-premises in a local data center. Protecting the modern data center requires greater flexibility and innovation to keep pace with the migration of application workloads to the cloud. Software-defined Networking (SDN) and Software-defined Wide Area Network (SD-WAN) solutions enable network security solutions in private, public, hybrid and cloud-hosted Firewall-as-a-Service (FWaaS) deployments.

Robust Network Security Will Protect Against

- **Virus**: A virus is a malicious, downloadable file that can lay dormant that replicates itself by changing other computer programs with its own code. Once it spreads those files are infected and can spread from one computer to another, and/or corrupt or destroy network data.
- **Worms**: Can slow down computer networks by eating up bandwidth as well as the slow the efficiency of your computer to process data. A worm is a standalone malware that can propagate and work independently of other files, where a virus needs a host program to spread.
- **Trojan**: A trojan is a backdoor program that creates an entryway for malicious users to access the computer system by using what looks like a real program, but quickly turns out to be harmful. A trojan virus can delete files, activate other malware hidden on your computer network, such as a virus and steal valuable data.
- **Spyware**: Much like its name, spyware is a computer virus that gathers information about a person or organization without their express knowledge and may send the information gathered to a third party without the consumer's consent.
- **Adware**: Can redirect your search requests to advertising websites and collect marketing data about you in the process so that customized advertisements will be displayed based on your search and buying history.
- **Ransomware**: This is a type of trojan cyberware that is designed to gain money from the person or organization's computer on which it is installed by encrypting data so that it is unusable, blocking access to the user's system.