NETWORK SECURITY

Network Security Network security is the authorization to access data controlled by a network administrator.

The security system starts with authentication, commonly with a username and a password, with the password being the one factor in authentication. A second factor, such as an ATM card or mobile phone increases this security. Security can be further enhanced when three-factors are required for authentication, such as a fingerprint or retinal scan.

A firewall determines access to data by a user and prevents misuse.

Antivirus software further refines the network's security by checking for and inhibiting potentially harmful viruses, computer worms or Trojans.

Managed Firewalls A firewall is a computer system that enforces your rules for controlling access between two networks. Typically, this would be between your system and the internet. The firewall executes an access control plan, i.e. what can go out and what can come into your system.

Threats from the internet are real and continue to grow. Malicious programs pose real threats to your business as well as your client's data and privacy. As the attacks get more numerous and potentially more harmful the firewalls become ever more sophisticated. Continually monitoring the firewall and analyzing the data from it is critical to staying ahead of the next big threat.

Many business owners have determined that these attacks on their system pose a real risk to their business, but spending the time necessary to stay on top of it them or the cost of employing someone to do so, is not realistic.

For companies that lack adequate IT resources, a Managed firewall service may be appropriate. The managed firewall provider will provide the experts available to help you in the planning stage for your business specific needs. They then program the firewall to perform to your specifications. Your team of experts continues to monitor your system, deploying upgrades and patches to stay current. You have backup and recovery options. They are up to date on best practices to help you develop your plans for effective access management. This can be a cost effective option for many businesses.

IDS/IPS (Intrusion Detection Systems and Intrusion Prevention Systems)
As the names imply, the detection system is that part of your network security that monitors your system for malicious activity. It will log the information and attempt to stop it. It then reports on the activities.

The prevention system works together with the detection system monitoring your network for suspicious activity based upon your protocol. It then sends warnings or blocks intrusions, including blocking future incoming packets from a suspect source.

A variety of systems exist to meet needs, such as, Network-based IPS, Wireless IPS, Host-based IPS, along with Network Behavior Analysis systems. Each works by targeting specific types of data or by positioning at different points in the data stream to identify potential threats.

The firewall and its protectors, the IDS and IPS, monitor both potential incoming and outgoing threats. Internal threats from unhappy employees, the curious or outside contractors continue to pose serious vulnerabilities. The type of data received from your system will provide data needed analyze and isolate these potential internal threats, as well as those being posed from the outside.

Whichever system you use, or likely a combination of systems, when the inevitable intrusion occurs, the visibility which you receive as a result of reporting from your IDS and IPS systems, will give you the information needed to be proactive in controlling the intrusion. Without visibility, you don't know what the problem is and you can't control it.

Network Forensic Appliances

Network forensics is the process of capturing information that moves over a network and making sense of it by the use of forensics. A network forensics appliance is a device that automates this process. A group of network forensics products are sometimes referred to as Network Forensic Analysis Tools (NFATs).

Just like the police forensics team at a crime site, network forensics is the process of capturing, recording and analyzing information related to events within a computer network. Some systems catch all data for analysis which requires a large amount of storage. Other programs selectively sample data quickly, determining what should be stored for further analysis at a later time (batched). These programs require fast processors to ensure the system's business requirements can be maintained.

While Firewalls and IDS systems offer threat protection, the Network Forensic Appliances offer memory, the stored data, for uncovering the source of security breaches and can fill in the gaps. Network Forensic Appliances are the latest in security for your network and work well in combination with IDS/IPS systems by taking a more in depth look at data reported by the other systems. This is helpful in isolating individual problems and general trends.

Other Network Security Services:

Vulnerability Assessments and IT Controls

Penetration Testing

Social Engineering

Application Security Assessment and Code Review

Incident Response Service

SOME OF OUR NETWORK SECURITY PARTNERS:

CISCO

NIKSUN

NETSCOUT

WILDPACKETS - OmniPeek

McAFEE

FLUKE NETWORKS – TruView

SONICWALL

RIVERBED

ALLIED INFOSECURITY

…and more!

Speak to a
Network Security
Consultant