Best Ways to Secure Your Network

Are you looking for better ways to secure your network? Being proactive and keeping a secure network can potentially save you from experiencing the dreaded, "crashed network." Sadly, many hackers assume your network is not defended; so, all networks are at risk of acquiring worms and hackers. Let's explore two vulnerable computer network areas: the endpoint and the perimeter.

What is the endpoint? "In computer science, in discussions of communications protocols, an endpoint is the name for the entity on one end of a transport layer connection" (Wikipedia). The (communication) endpoint is the communication channel between your computer and the computer connected on the other end. For example, if you are subscribing to an online newsletter and only want to receive automated email correspondence on a certain subject, you can expect to receive a subset of messages from the website you subscribed to. Computer network communication protocols work by a set of communication rules to ensure reliable interchange of data over imperfect communication channels. In order for data to successfully flow between two end points, transport layers are required: "In computing and telecommunications, the transport layer is the second highest layer in the four and five layer TCP/IP reference models, where it responds to service requests from the application layer and issues service requests to the network layer. It is also the name of layer four of the seven layer OSI model, where it responds to service requests from the session layer and issues service requests to the network layer" (Wikipedia). Therefore, the transport layer takes care of transferring data between hosts (or computers) and ensures data flow reliability within networks. The transport layer also controls and error recovery by making sure the data gets to the intended destination point. Centralized monitoring and event correlation systems which allow multiple end points to be used at the same time within a network necessitate a powerful multifunction network security appliance.

Both hardware appliances and software applications work in conjunction. The phrase, "perimeter based security" describes "the technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters" (Texas State Library and Archive Commission). Perimeters are typically protected with software applications. With software programs, you can monitor, block, and destroy spam, viruses, worms, and Trojans too.

Installation of the right security network-technology platforms are the key to secure networks. Genesis Global is a global provider for Cisco's Adaptive Security Appliances and PIX Firewall Appliances. Used Cisco PIX-525-R-BUN and ASA-SSM-AIP-10-K9 are excellent multi-user appliances at filtering all threats, at all gateways, in all directions—and is affordable! To get all the facts, call Genesis Global's Sales Accounts Managers at 1-800-908-9665 (or email sales@genesisglobalinc.com). Come visit us at: www.genesisglobalinc.com.

About Genesis Global's Author:

Debbie Jensen, an expert writer for business and technology for Genesis Global, has a Bachelor's Degree in Visual Communication (Multimedia). With her twenty year history of creative expressions and formalized study of Information Technology of digital print/web design and development, she is now publishing articles about networking for Genesis Global.