

Securing your network

A three-tiered approach to better security **By James Gretta**

As networks and inter-networking become more complex, the need for more advanced and capable security practices is paramount in keeping information and resources secure from malicious activities.

There are many best practices available, including a three-tiered approach that utilizes a firewall, intrusion detection system and virus scanning to prevent, detect and quarantine/remove malicious activities and threats from internal networks.

Firewalls

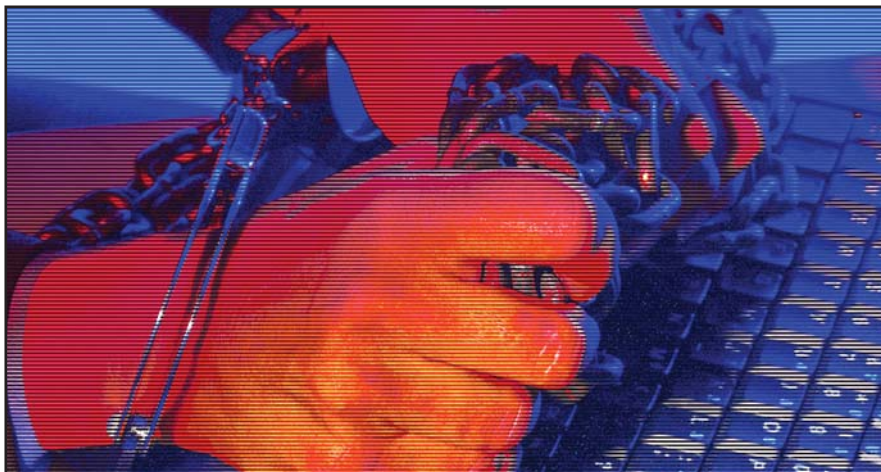
A firewall is the first line of defense in a comprehensive security solution. Firewalls inspect traffic and match it against a set of preconfigured rules. They can filter by source address, source port, destination address, destination port or any combination therein. Based upon these rule sets, the firewall either passes the traffic through to the internal network or blocks it entirely.

Firewalls come in a variety of flavors and from several manufacturers. Some are hardware or appliance-based; others are software-based and reside on high-end servers or workstations. Regardless of the platform an organization chooses to implement, the basic functionality is the same. Keeping current with technology, as well as maintaining and updating rules as new threats are exposed, will help increase your level of protection.

Intrusion Detection Systems

The Intrusion Detection System (IDS) is responsible for detecting paradoxical behavior based upon predetermined guidelines. There are two forms of IDS — host-based and network-based. The host-based IDS is software-based and is used to detect malicious activity on a single endpoint, whereas a network-based IDS is used to inspect and detect malicious activity within its network segment.

A host-based IDS may be a personal firewall or a software agent running on a local machine. A network-based IDS operates in promiscuous mode and has sensors that monitors packets moving across the network segment. The packets are compared



against various signatures and when suspicious activity is detected, alerts are sent to appropriate resources.

A combination of both systems should be implemented to detect the presence of malicious activity. There is one key point to remember when implementing host-based IDS — protect every host.

Antivirus software

The final and most important part of this layered approach is the antivirus software. Antivirus software is written specifically to combat harmful viruses and remove them from your computer.

Antivirus software utilizes updates to keep a current listing of known virus definition files. Maintaining a current virus definition file can be accomplished by manual or scheduled updates. The definition files are updated by supporting software vendors as new viruses, worms and other malicious files are discovered, and are typically posted on the vendor's Web site.

Antivirus software is reactive in nature and is only a small part of a comprehensive security solution.

There are emerging technologies such as Network Admission Control (NAC) that proactively protect networks from clients whose integrity is not yet established. The theory behind NAC is that when a network-capable device attempts to access the LAN, it is segregated from known good resources until it adheres to established security guidelines.

NAC-compliant software scans the host to determine if it is properly patched and updated. If a machine requires updates, it can be automatically redirected to the proper resources. Once the updates are installed, the new host will be given predetermined access. In the event that the machine cannot be properly updated, the host may be denied access, given restricted access or placed in a quarantined area. This is another method of taking a proactive approach to defending your network.

Due to the popularity of mobile computing, it is nearly impossible to ensure a network is 100 percent secure. Computers are often used in multiple locations and on multiple networks. This causes an inherent risk within SMB and corporate networks, but with a properly designed and implemented security solution, the effects can be minimized.

Protecting internal resources from external attacks by utilizing a firewall, monitoring network segments and hosts utilizing IDS for known malicious and suspicious activity, and implementing and enforcing antivirus protection policies, as well as keeping current with emerging technologies, are only a few steps you can take to secure your network.

JAMES GRETTA is a network integration engineer at TriLogic Corp., a solutions integration company focusing on IT infrastructure solutions. Gretta is a Cisco Certified Network Associate (CCNA). Reach him at (724) 745-0200 or jgretta@tri-logic.com

Experts **Technology** is brought to you by TriLogic Corp.