Network Security—Increasing Threats Need Immediate Attention

The Internet, remote computing, wireless networks and increased mobility are significantly increasing the need for network security. All it takes for unprotected PCs or laptops to become infected with malware is opening one infected email, or making a single visit to an innocent looking but malicious website.

Unfortunately, when an infected PC connects to the corporate network, the malicious code can spread throughout the entire organization. Use of home computers, Internet cafes or devices not controlled or safeguarded by the organization compound this problem. Attackers are now capitalizing on this fact, and increasingly utilizing weak endpoints to launch their assaults against corporate networks and resources.

Furthermore, a number of laws and regulations now mandate that additional security measures such as encryption be put in place. Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, California Senate Bill 1386, Basel II and other regulations require that sensitive data be encrypted.

The sophisticated nature of today’s network security attacks and the recent IT security legislation cannot be ignored. Extreme Networks® helps organizations address these security challenges.

Extreme Networks Security Solutions

Extreme Networks provides organizations with cost-effective security solutions that give meaningful insight and unprecedented control. Unlike traditional security systems, solutions from Extreme Networks allow the network to participate in the overall security scheme by detecting events at the network level and then enforcing security policy across the whole network.

Solutions from Extreme Networks validate that devices connecting to the network are free from contamination and conform to the organization’s security policy before they are allowed access to the network. If a virus or worm outbreak does occur, products from Extreme Networks are designed to detect and remediate the threat before it can spread and cause extensive damage. Additionally, the network-based insight and control provided by Extreme Networks allows for advanced security functions, so traffic can be selectively and intelligently routed for encryption, decryption or inspection for attacks and malware.

Security features such as the CLEAR-Flow Security Rules Engine are built into switches from Extreme Networks. These capabilities, together with the Sentriant® family of security products provide powerful solutions to address the security challenges facing today’s organizations.

Open Networking Approach

Unlike self-centered networking products where security resources are proprietary and closed, Extreme Networks uses an open networking approach. This allows customers to use best-of-breed products and applications. Extreme Networks open networking approach integrates Extreme Networks solutions and third-party systems into a cohesive system. This provides insight and control that leverages the strengths of all products, and avoids the pitfalls of being locked into a single vendor solution.

Comprehensive Security

Extreme Networks security solutions utilize the network to detect security events and enforce policies. Deep analysis of suspicious traffic and devices are done by Virtualized Security Resources (VSRs) that effectively offer the analysis and mitigation services for the whole network.

ExtremeXOS®, the advanced operating system developed by Extreme Networks that allows open collaboration based on XML APIs, and CLEAR-Flow, a Security Rules Engine, are both features on Extreme Networks switches. These capabilities allow for virtualization of security resources on a network.

Advanced security functions allow network administrators to increase the reach of security coverage for the same budget compared to link-by-link protection using in-line appliances.
Most organizations have experienced the pain and financial impact of network compromises due to insecure endpoint devices connecting from within their own network. Preventing these security incidents requires more than shutting off ports or limiting physical access within a building. Effective access control requires a proactive approach to ensuring that all endpoint devices are properly secured and free of threats before they are granted access to internal network resources.

The Sentriant Family of Network Security Appliances from Extreme Networks

The Sentriant family of security products provides organizations with cost-effective, easy-to-deploy solutions to today’s tough network security challenges. These high-performance, highly scalable products verify that connecting devices are in compliance with security policy, detect and mitigate rapidly propagating network threats in seconds, and provide security enforcement across the wired and wireless network.

Sentriant AG200

The Sentriant AG200 protects the network by allowing access only to endpoint devices that are free from threats and meet IT security policies. Key features include:

- Advanced endpoint integrity testing that verifies each endpoint meets your organization’s security policy before allowing access
- Flexible deployment options support several enforcement schemes for easy integration without costly network upgrades
- Enterprise-class management and administration combines centralized system management with multi-user, role-based administration to minimize operational complexity

Sentriant NG300

Sentriant NG300 is a security appliance that secures the network interior against rapidly propagating threats, such as virus or worm storms. Sentriant NG300 uses behavior-based detection methods to identify even new threats for which no signatures exist at the time of the attack. Key features include:

- Defends against threats without interfering with network traffic or lowering network availability
- Delivers fast detection with a network of virtual decoys creating an early warning system that fires an alert when a virtual target is detected
- Protects IP Telephony devices from targeted attacks
- Isolates attackers and prevents them from communicating with the remainder of the network, allowing mission-critical data to continue to flow normally

ExtremeXOS

The ExtremeXOS operating system is a highly available, secure, open and extensible foundation for converged networks. Built-in security capabilities provide network access control integrated with end point integrity checking, and protection for the network control and management planes.

- Network login enforces authentication before granting access to the network via 802.1x, Web-based or MAC-based, and supports multiple supplicants on the same switch edge port, even in separate VLANs
- MAC Security allows the lockdown of a port to a given MAC address and limiting the number of MAC addresses on a port
- ExtremeXOS IP Security framework protects network infrastructure, network services such as DHCP and DNS and even host computers from spoofing and man-in-the-middle attacks
- ExtremeXOS provides secure management via SSH2/SCP2/SSL and SNMPv3 for authentication and protection