WatchGuard Sets New Standards for Network Security

New WatchGuard Fireware XTM OS Provides Extensive Array of New Security, Networking and Management Capabilities

WatchGuard Technologies, a global leader in extensible network security and connectivity solutions, today unveiled its new operating system for WatchGuard security appliances – WatchGuard Fireware XTM. With this new operating system, WatchGuard customers can extend the capabilities of their unified threat management (UTM) firewall appliances to include a bevy of new security features, networking capabilities and management functions. The new WatchGuard operating system, Fireware XTM, defends networks by adding innovative security features, including full HTTPS inspection, VoIP security, and IM and Peer-to-Peer (P2P) application blocking. Furthermore, Fireware XTM integrates new networking capabilities, including clustering, load-balancing and other networking features. Additionally, the new operating system also extends management capabilities by adding role-based access control (RBAC), centralized multi-box management and enhanced reporting functions. The combination of this makes Fireware XTM the most powerful operating system developed by WatchGuard needed for today's ever-growing threats and dynamic business environments. "WatchGuard's vision of extensible threat management means giving customers the ability to extend or add on to or augment their security foundation," said Eric Aarrestad, Vice President, Marketing at WatchGuard Technologies. "With Fireware XTM, businesses gain a new and formidable tool that keeps their networks, resources and sensitive data safe and highly secure." Fireware XTM – Superior Security for Today's Dynamic Business Environments HTTPS connections are often used for payment transactions on the Web, such as online banking, and for sensitive transactions in corporate information systems. Because HTTPS traffic is encrypted, it presents a blind spot to network administrators who are unable to "see" into these packets. This opens network doors to malware attacks and other pernicious threats, such as HTTPS cookie hijacking. With Fireware XTM, administrators can now effectively eliminate the HTTPS network threat vector. By way of WatchGuard's HTTPS proxy technology that intercepts, scans and rebuilds HTTPS data streams, administrators can now accurately audit, report and protect users from receiving dangerous file types. With a projected growth of 20.1 percent, VoIP is easily one of the fastest growing IT markets, which also makes it one of the most exposed threat vectors into corporate networks. Because of this, threats such as DoS attacks on VoIP networks, directory harvesting, and "vishing" attacks are rapidly increasing in popularity. Unlike some UTM solutions that merely provide network address translation to obscure a VoIP system, Fireware XTM provides application-level security for SIP and H.323 protocols. These security capabilities conceal business VoIP systems and concomitantly harden them to withstand directory harvesting attacks, input validation hacks (buffer overflows), and other major VoIP threats. Botnets – hijacked computers containing malware applications – are also major concerns and liabilities for today's businesses. Because many botnets use the same protocols used for legitimate business applications, such as instant messaging, administrators are faced with limited options – eliminate IM or risk botnet infection, loss of resources and control. With Fireware XTM administrators can enjoy having both the convenience of IM and protection from botnets. Fireware XTM provides application inspection as well as port and protocol identification to ensure application traffic is valid and safe. Additionally, the WatchGuard HTTPS inspection works in tandem with IM and P2P application blocking, which foils even those bots that use encryption in their attempt to evade detection. Fireware XTM – Extending Security and Networking Capabilities Users today demand that their networks provide non-stop, high-performance throughput. To help meet this need while providing extensible protection, Fireware XTM supports full appliance clustering so that organizations can meet high availability requirements, including active/active load balancing, seamless fail-over, full session synchronization and the ability to add high-security throughput capacity as their network grows. Because every network is unique and requires different capabilities, WatchGuard designed its new OS for maximum network flexibility. With Fireware XTM network administrators can use a WatchGuard firewall UTM appliance in a multitude of new ways. This includes support for transparent mode, HTTP redirection for support of caching proxy servers, multicast support over VPN tunnels, NAT over branch office VPN, and the ability to assign multiple VLANs on external interfaces. For workers in mobile environments who need to maintain secure VPN connectivity as they roam from access point to access point, Fireware XTM supports roaming while using mobile VPN with IPSEC. With this feature, VPN tunnels remain "alive" while users move among multiple APs or 3G connection points. This gives users a new level of freedom coupled with strong security. Fireware XTM – Making Security More Manageable Administrators will agree that information security is only as good as its management. Here, WatchGuard introduces new features that allow administrators to work they way that they prefer. With Fireware XTM administrators can now manage their appliances by a command line interface (CLI), a web GUI, or from the WatchGuard System Manager (WSM) console. Additionally, with CLI control, administrators can create and use their favorite scripting tools to automate common tasks, thus saving time and reducing errors. Further adding defense in depth and management control, Fireware XTM now supports RBAC (Role Based Access Control). This enables organizations to create and assign firewall/UTM management roles to specified administrators based on the best security practice and rule of "least privilege." In order to meet the latest regulatory requirements, administrators are challenged to standardize and automate the collection and management of firewall and device configurations. With WatchGuard System Manager, which is included with all Firebox X Core and Peak appliances, administrators can have complete, centralized multi-box management and control of WatchGuard appliances, including scheduling of software updates, configuration of data,

creation of policy procedures, and the ability to publish changes globally across all WatchGuard devices. Organizations need detailed reports for a variety of reasons, ranging from regulatory compliance and security incident troubleshooting, to monitor Web usage and billing requirements. WatchGuard System Manager now offers new audit reports driven by role-based access control records, customized report output and new filtering options so that administrators can quickly get the information most important to them. WatchGuard Fireware XTM – Pricing and Availability Fireware XTM is free for current WatchGuard LiveSecurity customers. It is supported on all WatchGuard e-Series families of Edge, Core and Peak firewall UTM appliances. Fireware XTM will be available within 45 days. About WatchGuard Technologies, Inc. Since 1996, WatchGuard Technologies, Inc. has been the advanced technology leader of network security solutions, providing mission-critical security to hundreds of thousands of businesses worldwide. The WatchGuard family of wired and wireless unified threat management appliances and WatchGuard SSL VPN remote access solutions provide extensible network security, unparalleled network visibility, management and control. WatchGuard products are backed by WatchGuard LiveSecurity Service, an innovative support, maintenance, and education program. WatchGuard is headquartered in Seattle and has offices serving North America, Europe, Asia Pacific, and Latin America. To learn more, visit http://www.watchguard.com/. # # #