Secureworks®

WHITE PAPER

Three Stages of Firewall Management Maturity

By Leo Kershteyn

Firewalls are a fundamental element of any organization's network defense. But relying on just the base configuration provided by the manufacturer will not effectively secure your network.

Achieving the most utility from your firewall investment requires work. Various elements of an organization's firewall investment require constant management in order to maximize effectiveness. From auditing and remediating out-of-date or conflicting policies to keeping up with vulnerabilities and OS releases, creating VPN tunnels, and troubleshooting vendor hardware and functionality, organizations often struggle to maintain optimized firewalls. The "set-it-and-forget-it" approach simply does not work.

Secureworks has identified three stages of firewall management maturity, and by partnering with an experienced cybersecurity company, organizations can get the most out of their firewall investment.

Stage 1: Basic Firewall Management

Organizations need in-house expertise to manage their firewalls, and resources need to be available after hours and on weekends (security events are not limited to business hours). Not just any type of expertise will do, as being an expert on one firewall brand does not translate into expertise on another brand. As networks grow, so does the requirement for deep and broad expertise on how different components of the security infrastructure work together to keep the network secure. Rather than a generalized approach to managing security, having a team of experts with deep knowledge in their respective domains is most effective.

Firewall functionality spans most of the OSI spectrum. Therefore, basic firewall management includes not only basic device management such as changes, patches and upgrades, but also the regular review of rules, auditing policies against established best practices, and security event monitoring.

Additionally, firewalls produce large volumes of log data. A company's security staff must find a way to detect valid security events, correlate them to attack vectors, and then know how to apply what they see to mitigate possible vulnerabilities and infiltrations. Without a Security Information Manager (SIM) or involvement from a managed security service provider, the network administrator staff becomes increasingly responsible for analyzing and remediating security events, a burden that expands exponentially as network usage grows.

Stage 2: Next-Generation Firewall Management

With the advent of the next-generation firewall, IPS functionality traditionally found in a standalone device is integrated into the firewall. Depending on the vendor, that integration can be as streamlined as an IPS being a feature selected with a click of a mouse, or as imprecise as having a separate management console, separate log streams, and the functionality of a separate software appliance on the same hardware as the firewall. Integration with cloud sandboxes, endpoint detection solutions and threat intelligence feeds from vendors and third parties requires constant tuning of next generation firewalls, making effective management even more intricate and challenging to do with in-house expertise.

Additional time is required to audit the policies, review the rules and identify security threats from the mountain of log data. This further strains in-house resources, to say nothing of the issue of around-the-clock coverage.

An experienced cybersecurity company understands the intricacies of next-generation firewall management. By their nature, next-generation firewalls are more complex than traditional firewalls. Security experts can execute change management, upgrades and patches, rule reviews and policy audits, and make sure an organization's next-generation firewall technology discovers threats beyond the port and protocol layers.

Integration with cloud sandboxes, endpoint detection solutions and threat intelligence feeds from vendors and third parties requires constant tuning of next generation firewalls, making effective management even more intricate and challenging to do with in-house expertise.

Stage 3: Advanced Firewall Management

Some next-generation firewalls have the advantage of advanced capabilities that further bolster an organization's security posture. Adding third-party threat intelligence feeds to next-generation firewalls such as those developed by Cisco, Palo Alto and Juniper, greatly amplifies the ability for firewall technology to catch more threats before they impact an organization's devices and data.

This is where partnering with an experienced cybersecurity company – one possessing visibility into the ever-changing global threat landscape – can pay huge dividends by bolstering the blocking capability of an organization's firewall. A reputable third party that can develop research-driven IPS signatures (such as signatures developed by The Secureworks Counter Threat Unit™ (CTU™) Research Team) and database lists of malicious IP addresses and domain names to augment those provided by the vendor (such as the Secureworks Attacker Database). Seamlessly providing those to an organization's next-generation firewall technology lends tremendous value.

Other Considerations

Managing firewall technology is not easy. It can be laborious, confusing, and drains valuable time from an organization's IT and security staff. An organization with adequate staff to accomplish effective management today will always struggle to retain that staff, as well as scale around-the-clock, or cover any deficiencies should in-house resources move to a new position or leave the company.

Some organizations are hesitant to hand over the keys to their entire firewall environment to an outside company. An experienced cybersecurity company that offers co-management eases those concerns. The co-managed approach provides organizations with the ability to retain ownership and administration rights to the extent they prefer.

Firewalls remain a fundamental part of any organization's security posture. But for many companies, the day-to-day effort required to get the highest positive impact from their firewall investment is an ongoing challenge. The right experienced cybersecurity company can provide reliable partnership to maximize the resource and cost investment in this pillar of information security.

This is where partnering with an experienced cybersecurity company – one possessing visibility into the ever-changing global threat landscape – can pay huge dividends by bolstering the blocking capability of an organization's firewall.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp