EXECUTIVE BRIEF

The Challenges of Network Security Management

Examining the hurdles to managing risk, operations and resources

Abstract

The rapid deployment of firewall and other security services across hyper-distributed networks, and the need for mobility in the "new normal" underscores the need for unified security management in companies of all sizes. This brief explores emerging trends, and examines network security challenges in the areas of risk management, security operations and resource allocation.

Introduction

Working-from-home, distributed networks, migration to the cloud, and a proliferation of apps and devices have resulted in an explosion of exposure points. Whether for a small business, distributed enterprise, or managed security service provider, the need to protect an 'anytime, anywhere business' is the new normal.

At the same time, threats are increasingly evasive. With undetected threats increasing 145 percent year-over-year[1], organizations can have no idea of what threats are being missed.

Moreover, IT organizations face rising costs, shrinking budgets, and a tighter pool of qualified staff.

Combined, these forces create significant network security challenges for IT to contain risk, manage operations and allocate resources.

Different Needs

All organizations need to understand and identify evolving threats. They all need insight into network activities, usage and

risk. They also all need to monitor, troubleshoot and resolve security and operational challenges. And they all must comply with strict internal security guidelines.

Small businesses, however, can have limited in-house technical resources. Managing security and optimizing performance can be overwhelming. While larger enterprises and service providers may have in-house SecOps staff, they can face even broader and more challenging concerns. They may need to scale deployment and management of security across complex distributed networks. They have concerns about security automation and change management, audit reporting and policy continuity.

Risk management

Organizations today understand things can go from normal one day to complete chaos in just a matter of seconds. Risk of being victim to targeted attacks persist for many organizations as news of network breaches and massive data exposure continue making headlines.

How do you know the extent to which your organization is at risk? Are there security gaps in your internal operations? What about your network users and the assets, websites and SaaS applications they use? And how do you decide to prioritize and address these risks?

Application and data traffic traverses the internet, remote campuses, branch offices, and perhaps even third-party vendors. Organizations can have insufficient visibility and control over unsafe network activities, traffic irregularities, unusual data access and movement, unpatched firmware, security events and system health.

Risks that go unmanaged can start something worse. A breach will slow a company's momentum and growth. Operations are disrupted as key personnel divert their focus away from key business priorities. Executives are compelled to put all their time towards damage control and public relations. The inability to recognize security risks inhibits security planning, policy decisions, and decisive actions.

Security operations

Firewalls themselves are also exposure points. Research from Gartner[2] suggests that 99 percent of firewall breaches are caused by firewall misconfigurations. As firewall rules are created, copied and amended, they can work against one another causing unwanted security and performance consequences. Misconfigurations and conflicting rules can make the network vulnerable to sophisticated threats, unauthorized access or intrusion.

Instead of tracking down security gaps and vulnerabilities, time might be better spent making sure that firewall configurations are not overly permissive and open backdoors to their infrastructures. Organizations need to validate and audit policies and configurations prior to rolling them out, and reverse them quickly if needed.

The movement toward larger, more complex multi-cloud networks supporting more applications and users forms a new digital workplace. As networks grow, managing security operations, optimizing performance, solving operational issues and ensuring security measures and control access for users, devices and applications continue to be complex challenges.

Organizations struggle to establish adequate internal security operations to comply with internal service level policies. These policies are designed protect businesses and their employees, reduce security risks, limit financial and legal liabilities.

In managing disparate firewall devices individually and manually, organizations often experience inconsistent policies and procedures. There is often little to no analysis, testing, auditing and approval process in place to ensure the company is executing the right firewall rules, at the right time, and in conformance to internal compliance requirements.

Resource allocation

A shortage of trained talent in the security industry has made staffing a serious concern. Many organizations, specifically SMBs, do not have adequate security talents and skill sets to proficiently maintain firewalls and solve serious security issues as they arise.

Even a single firewall requires regular planned maintenance, daily monitoring, policy reviews and administrations, and firmware upgrades. As networks scale and grow across distributed enterprises and multi-tenant provider networks, the burden on security staff multiplies exponentially.

Making matters worse, security operations staff can be burdened with managing and operating complex and fragmented firewall silos. Administrations are often complex, cumbersome and labor-intensive. Tasks and processes are generally unchecked, uncorroborated and non-compliant. This leads to a situation where small networks might accumulate dozens of firewall rules over many years while larger networks may have thousands.

Conclusion

A better way forward is needed. Smarter management tools are required for security teams to do their job effectively.

SonicWall Network Security Manager (NSM) gives you everything you need for comprehensive firewall management. It provides comprehensive visibility, granular control and capacity to govern the entire SonicWall network security operations with greater clarity, precision and speed. And it does it all from a single function-packed interface that can be accessed from any location using any web browser-enable device.

Learn more. Contact your SonicWall representative, or visit www.sonicwall.com/nsm.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

1 2020 SonicWall Cyber Threat Report
[2] Info Security

SONICWALL®

ExecutiveBrief-TheChallengeOfNSM-US-VG-1965