



SOLUTION BRIEF

Three Pillars of Network Security Management

Best practices for central governance, risk management and compliance

Abstract

The new normal for business is hyper-distributed and mobile, with more reliance on cloud-based collaboration and remote work-at-home endpoints. This has created an explosion of exposure points. Adhering to best practices for network security management is more critical than ever. This brief examines three core pillars for network security management supported by the SonicWall Network Security Manager (NSM) solution.

Introduction

The ideal network security management solution would meet the needs of any organization, whether a small business, a distributed enterprise, or a managed security service provider (MSSP) with thousands of firewall devices under management across many locations. To do so, it must provide a holistic, unified approach, with a broad range of operational controls that can be easily licensed, adapted and scaled to meet these various use-case requirements. Best practices for a unified approach to network security management centers on three core pillars: central governance, risk management and compliance.

Central governance focuses on improving operational efficiencies and reducing overhead, while risk management and compliance concentrate on business value. These core objectives are interconnected, as each leverages a common set of information, processes and technologies. This helps enterprise security operations (SecOps) and MSSPs establish and deliver a strong, federated security defense,


and integrate response services into their security programs. The approach is grounded on the principle of simplifying and, in some cases, automating various task to achieve better security coordination and decision-making, while reducing the complexity, time and overhead of performing security operations and administration tasks.

Central Governance

In today's new paradigm of working offsite, you must be able to manage your entire security infrastructure from anywhere using a unified management console. To ease deployment, enhance user experience and reduce cost, an optimal solution would be available as software-as-a-service (SaaS), accessible on-demand via the cloud.

The management solution should leverage common management workflows and processes across the security ecosystem. This would include globally federating security policies with grouping and inheritance and synchronizing them across all managed firewalls. To minimize administrative overhead, it should simplify management tasks using automated security wizards. And to help stretch increasingly limited trained staff resources, and accommodate social distancing requirements, it should let you roll out firewalls remotely at scale using zero-touch technology, without the need for having dedicated technicians on site.

Best practices would leverage a cloud-based SaaS architecture so that network management can scale dynamically without increasing administrative overhead, whether for a small network or large distributed enterprise.



Particularly in MSSP environments, it should easily expand to support any number of tenants with each hosting thousands of managed firewalls.

Risk Management

To help contain network security risks, the solution must monitor active security applications and corresponding security resources, services and capabilities, globally and in real time. This lets SecOps ensure security measures are operational, in equilibrium with current network conditions, and harmonious with its security policies across the entire ecosystem. Moreover, it should regulate access and usage of networks, applications and data, and enforce consistent security across the enterprise using templates.

For higher security efficiency, the solution should also enhance communication and collaboration so key stakeholders can make rapid informed security policy decisions based on time-critical and consolidated threat information. It should enable the detection, isolation and correction of abnormal operations, and alert SecOps of security and operational issues.

Compliance

To comply with internal and external regulations, SecOps need to maintain consistent policies and procedures, along with corresponding analysis, testing and auditing. Not only must network security management services function properly and in a timely manner, they must also be consistent, measurable, and completely dependable under the scrutiny of an audit.

As a result, a network security management solution should integrate security orchestration, auditing, reporting and analytics capabilities into a single operator interface. It should equip SecOps teams with powerful but user-friendly set of controls for facilitating and accomplishing all vital network management tasks, while keeping the security ecosystem continuously running flawlessly and in compliance and good health.

A best-practice solution would enable SecOps to customize any combination of security auditable data to help address specific compliance regulations. And it should make internal and external auditors happy by automating scheduled security reports. It should let you mine analytics and conduct security event investigations, and easily exercise change management and audit processes.

SonicWall Network Security Management (NSM)

SonicWall Network Security Manager (NSM) gives you everything you need for central governance, risk management and compliance. It brings management, reporting and analytics of all firewalls into one place to centrally provision and synchronize all network security services in a single-pane-of-glass experience. This provides SecOps comprehensive visibility, granular control and capacity to govern the entire SonicWall network security operations with greater clarity, precision and speed. It accomplishes all this from a single function-packed interface that can be accessed from any location using any browser-enabled device.

NSM scales to any size organization and features functional integration for better efficiency and operational elasticity. Gain immediate access to workflow automation, zero-touch deployment, device templates and global policy engine. It enables SecOps to make informed decision and policy actions in response to any threat in real time, with detailed reporting and actionable analytics.

Because its design conforms with service level requirements for Security Operation Centers (SOCs), NSM supports your broader cyber defense strategy. Guided by business processes and a unified, auditable approach to security governance and compliance, NSM orchestrates and automates various tasks to promote better security coordination and corroboration all from one web-enabled app.

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.

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

Refer to our website for additional information.

www.sonicwall.com

SONICWALL®

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

SolutionBrief-ThreePillarsOfNetwork-US-VG-1966