FORCEPOINT
POWERED BY Raytheon

Whitepaper

Network Management and Operational Efficiency: How the Right NGFW Makes It Possible

THE NEW CYBERSECURITY BLUEPRINT

Contents

WHY DOES OPERATIONAL EFFICIENCY IN NETWORK MANAGEMENT MATTER?

According to Gartner, 80% of total IT costs occur after initial purchase. The significance of recurring operational costs is not always realized by organizations that are mainly focused on short-term investments.

Correct configuration is fundamental for network security. In the end, systems and technologies will not be robust if setup is incorrectly configured and contains critical security holes. Misconfiguration is, in fact, the result of human error, which is the leading factor in security failures. As much as 80% of unplanned outages are due to ill-planned changes made by administrators or developers. On top of security concerns, fixing issues causes extra work, which eats into profitability. Misconfiguration also leads to increasing network complexity and makes overall control and troubleshooting more challenging.

Network management systems play a critical role in avoiding human error and optimizing time and resources used in network operations. All of this has a direct impact on the perceived security level and recurring costs.

CUSTOMER NEEDS AND CHALLENGES

According to the global next-generation firewall (NGFW) study conducted by Forcepoint, most enterprises prefer to manage their network security themselves despite the clear trend towards outsourcing management to third parties. Security outsourcing is still considered risky, and enterprises themselves prefer to have network visibility, full control, and the independence to make their own decisions about changes.

Based on the survey, it is clear that management capabilities play an extremely important role in overall satisfaction with NGFW solutions. Manageability and centralized management tools in particular were flagged as important areas that enterprises are not happy with. The more distributed the network gets, the more essential remote management capabilities become.

Network/network operations and security teams are the primary decision makers when making NGFW purchase decisions. Solutions must fulfill requirements for both departments.

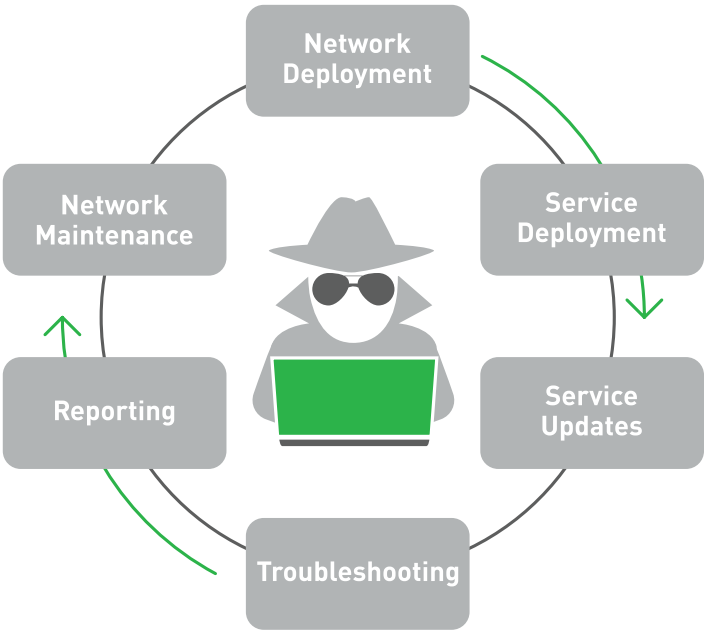
> **"The more distributed the network gets, the more essential remote management capabilities become."**

> **"Human error is the leading factor in security failures."**

Key Operational Tasks

If we look at the network security and management lifecycle, a proper management solution must provide tools for all major administrative phases and areas as shown in Figure 1.

FIGURE 1. Network Operation Lifecycle



Management tools must enable customers to rapidly react to network and business changes and provide constant control and visibility over the network. Based on customer interviews, the following tasks were highlighted as frequent administrative activities:

- Network deployment.
- Policy management.
- Network monitoring and troubleshooting.
- VPN management.
- Network maintenance.
- Flexible separation of administrative rights.

As these activities can be considered routine tasks, it is paramount that management tools enable customers to execute these easily, accurately, and in a scalable manner.

TYPICAL MANAGEMENT SYSTEMS

In practice, all NGFW solutions on the market offer a centralized management system, which is generally considered a must-have. However, the real usability and robustness of management systems greatly differ between vendors. Some important points to consider when selecting between NGFW technologies are:

1. The available tools for essential tasks across the whole operational lifecycle.
2. The ability to streamline real-world operational workflows.
3. The scalability to support network growth.
4. The number of resources required to manage the network.
5. The system's long-term total cost of ownership (TCO).

The level of compliance with many key capabilities cannot be understood just from paperwork but requires testing, investigation, and familiarity with system architecture. Simple product demonstration is not enough to prove that a system is robust in real-world network operating conditions, so is essential to dig deeper into the real management capabilities of NGFW systems.

As mentioned previously, proper understanding of a management system's real capabilities can only be achieved by testing the system in tasks that are relevant to the customer. Based on testing the latest versions of competitive network security management solutions, we have outlined the common capabilities of typical NGFW management solutions (Table 1).

TABLE 1. Operational Tasks and Typical Management Solutions

KEY TASK	TYPICAL MANAGEMENT SOLUTIONS	IMPLICATIONS FOR THE NETWORK AND ADMINISTRATIONS
Network Deployment	• No automated deployment tools. • Lack of efficient group operations.	• Costly roll-out process requiring site visits and manual work. • Time-consuming deployment.
Policy Management	• Lengthy, unstructured policies. • Lack of granular rule counters and policy comparisons. • Extra licenses for complete policy management.	• Inefficient policy execution. • Lack of central control of policies. • Lack of clear visibility of policy relevance. • High TCO—difficult to budget.
Network Monitoring and Troubleshooting	• Lack of clear log visualizations. • Slow log responsiveness. • Extra licenses for deeper log navigation.	• Difficult to get a clear picture of network events. • Slow reaction to network security issues. • High TCO—difficult to budget.
VPN Management	• Labor-intensive configuration. • Lack of VPN link aggregation concepts over multiple ISPs.	• VPN network setup takes as much as 10 minutes per site. • No practical, fast resilience option for site-to-site VPN.
Network Maintenance	• No scheduled upgrade tools. • Not designed for large network maintenance.	• Remote engine upgrade takes time and resources. • High risk of human error. • Service disruptions in maintenance window.
Flexible Coordination of Administrative Rights	• One-to-one mapping between administrative and role only. • No efficient tools for MSPs to manage their customers within a single management system.	• Limited flexibility to combine administrators and rights in large organizations and MSPs. • High total cost—difficult to budget.

HOW FORCEPOINT NGFW TAKES NETWORK MANAGEMENT EFFICIENCY TO THE NEXT LEVEL

Many customers consider the criteria discussed earlier important for their businesses. Wouldn't it be nice if the management system were capable of the following?

1. Centralized coverage over all key operational tasks for the entire NGFW network.The ability to stream-line real-world operational workflows.
2. Optimize workflows to make operations fast and straightforward for the user.
3. Scale for management environments with thousands of NGFW or nodes.
4. Provide an easily controllable and understandable cost structure with no hidden costs.

Implementing proper tools that meet the real needs of network security administrators often requires thorough and long-term understanding about customer processes. In addition, when management tools are all built in rather than bolted on, navigating between functions and getting a holistic picture of the network is only possible when different functions "talk to each other."

The Forcepoint NGFW Security Management Center (SMC), which is part of Forcepoint NGFW , provides a single "pane of glass" for management tasks across the management lifecycle. The Forcepoint NGFW Security Management Center is developed in-house and has all tools built into one system—without the limitations and complexity of rigid blade-type architecture. From the beginning, the Forcepoint NGFW Security Management Center has been designed to scale for large networks and remain responsive despite network growth.

Forcepoint NGFW and Forcepoint NGFW Security Management Center offer an optimal solution for enterprises, as they meet the needs of both network/network operations and security teams.

Table 2 outlines the key capabilities offered by the Forcepoint NGFW Security Management Center for improving operational efficiency and how it meets the combined needs of network and security administrators.

TABLE 2. Forcepoint Security Management Tools for Key Operational Tasks

KEY TASK	KEY FORCEPOINT CAPABILITIES	ADVANTAGE FOR OPERATIONAL EFFICIENCY	PRIMARY BUYER ORGANIZATION TEAM
Network Deployment	• Plug-and-play deployment tools. • Efficient group operations with multiple selections.	• No site visits and related costs. • Fast and automated network deployment for large and distributed roll-outs.	Network Administrator
Policy Management	• Hierarchical policies. • Re-use the same policy for many NGFWs with aliases. • Built-in rule counters and search. • Built-in policy validation and comparison tools.	• Short and simple policy structures. • Fast, accurate, and centrally controlled policy changes. • Efficient policy re-use across NGFWs. • Ability to keep policies relevant and remove idle rules. • No hidden costs.	Security Administrator
Network Monitoring and Troubleshooting	• Responsive log system. • Easy-to-use filtering and visualizations. • Direct links between logs, reports, and policies.	• Clear picture of network events and shortcuts between logs, policies, and reports. • Ability to focus on relevant logs and visualize the logs in an ad hoc manner. • Responsive log troubleshooting.	Network Administrator Security Administrator
VPN Management	• Support for configuring large VPN deployments efficiently. • Unique Forcepoint Multi-Link for resilient and flexible site-to-site connectivity.	• Rapid VPN network setup. • Ability to offer resilient and QoS aware site-to-site VPN across multiple ISPs and access technologies.	Network Administrator
Network Maintenance	• Scheduled tasks, including NGFW upgrades. • User-adjustable automated update and upgrade options. • In-service upgrades. • Automated log data management.	• Centrally controlled NGFW upgrades with the ability to precisely set time to execute, for example, per element. • Adjustable to required operational processes. • Unique cluster upgrades with no traffic disruption. • Tasks to automatically archive and delete logs.	Network Administrator
Flexible Coordination of Administrative Rights	• Granular customer roles. • Ability to mix roles, elements, and domains per administrator.	• Ability to optimize administrator tasks and change when needed. • Good fit for demanding large organizations and MSSPs.	Network Administrator Security Administrator

The Forcepoint NGFW Security Management Center is highly appreciated by Forcepoint NGFW customers, thanks to its centralized management capabilities. Customers also expressed that the Forcepoint NGFW Security Management Center enables administration teams to be small and efficient, regardless of the number of NGFWs or customers served.

Additionally, the simple Forcepoint NGFW Security Management Center license model facilitates transparent cost effectiveness as nearly all tools are inherently part of the basic product. This is critical when looking at a system's total lifecycle cost.

IS YOUR NEXT-GENERATION FIREWALL MAKING YOUR LIFE EASIER?

Management systems are vital to network security—and their lifecycle costs are high. Their importance grows with the tendency for networks to get more and more complex. Network management systems for NGFWs currently on the market are not all the same. They differ greatly in terms of how they support daily routine tasks, how well they automate workflows, how well they scale, and how they are licensed. With these challenges in mind, customers should take a closer look at their potential NGFW vendors and compare their management solutions.

Forcepoint NGFW Security Management Center has been designed for distributed enterprise networks that need simplicity, efficiency, and scalability for their daily routines. The efficiency of the Forcepoint NGFW Security Management Center consistently received high customer satisfaction ratings over the past 10 years.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[WHITEPAPER_NETWORK_MANAGEMENT_OPERATIONAL_EFFICIENCY_EN] 200035.021317