Examining the Dangers of Complexity in Network Security Environments

AlgoSec Survey Insights
Executive Summary

An online survey of 127 IT security professionals, with direct responsibility for managing their organizations’ network security environments, reveals that the complexity of multi-vendor environments correlates to more frequent system outages and security incidents. Surprisingly, most organizations still manage their environments manually—even large enterprises with hundreds of devices. Overall, the survey reveals a tremendous opportunity for security teams to reduce risk by simplifying and automating security management across their entire estates.

Key Highlights:

- **Complexity yields risk.** A majority of respondents in midsized and enterprise organizations (55.3%) reported a security breach, system outage, or both, due to complex policies.

- **Too many policies yields complexity.** “Too many policies to manage” is the leading challenge (43.7%) of managing multiple devices.

- **Too many vendors yields complexity.** The leading challenge of managing an environment with multiple vendors is “different expertise is required for each vendor” (49.6%).

- **Manual management is still the norm.** Nearly 75% of organizations manage their network security manually, even among the largest companies. 51.2% manage their devices manually through each vendor’s console. Another 23.6% manage their network security per device.

- **Consolidation would yield simplicity.** Half of our respondents believe that the greatest benefit of consolidating network security vendors would be simplified management. Among those who manage network security devices manually using vendor consoles, this number is nearly 60%.

About the Survey

The “Dangers of Network Security Complexity 2012” survey was conducted to study the impact of complexity in network security environments, based on the numbers of vendors, devices, and rules in the environment.

AlgoSec invited security professionals to participate from a global database representing companies of different sizes, in a broad range of industries, and with various levels of complexity. No AlgoSec customers or partners were invited.

All survey respondents indicated that they have direct responsibility for administering/managing their organization’s network security environment.

The respondents in the final analysis represent 29 countries on 6 continents, across a wide range of industries including financial services, technology, consumer goods, transportation, healthcare, and government sectors.
What is “Complexity”? 

For the purposes of this survey, we define a complex environment as one that has multiple vendors, many devices, and many firewall rules.

To analyze various levels of complexity, we surveyed security professionals in businesses of various sizes (Figure 1).

The data supports the assumption that a larger organization is likely to have a more complex network security environment. When we rank all the organizations we surveyed by numbers of vendors, devices and rules, 55.8% of Enterprise organizations are in the top half of the ranking, while only 11.8% of Midsize organizations and 4.2% (1 out of 23) of Small organizations are in the top half.

Vendors and Devices

An overwhelming majority, 94.4%, uses network devices from multiple vendors, and 57.1% have 4 or more vendors’ devices to manage (Figure 2). Nearly half have 50 or more devices (Figure 3).

As one might predict, a high number of devices correlates with a high number of vendors, but with some exceptions. In the group with less than 10 devices, 79.0% have relationships with three vendors or fewer. However, two of these respondents use 6-10 vendors, which equates to one or two devices per vendor.
At the other extreme, of the respondents with 250+ devices, 56.5% have six vendors or more, and 39.1% have more than 10. Yet, one respondent (in the educational sector) manages over 250 devices from one vendor.

Firewall Rules
41.8% of organizations of all sizes manage over 200 rules per firewall (Figure 4). The total number of firewall rules across the estate generally correlates to the size of the organization: all but three of the Small organizations have 1-1,000 rules, while all except one of the organizations with 10,000+ rules are Enterprise.

Impacts of Complexity
We asked, “Complex and/or conflicting security policies, such as firewall rule sets, router ACLs, IPS configurations, etc. have had what impact on security and system availability?” The responses are markedly different according to company size: Small organizations are much less likely to report a known negative impact. When we examine Midsize and Large organizations only, which are more likely to have complex networks, 55.3% report that complexity in security policies and configurations has created a known security breach, a system outage, or both (Figure 5).

Figure 4: 
Rules per Firewall
On average, how many rules are implemented on each firewall?

Figure 5:
Impact of Complex or Conflicting Security Policies, Midsize and Enterprise

Figure 5a: 
Impact, All Respondents (Small, Midsize, Enterprise)
We asked respondents, “How do you manage multiple devices/vendors on your network?” Surprisingly high numbers of the respondents, 74.8%, manage their networks manually, either using vendor consoles, or device by device (Figure 6).

Respondents who manage their network security manually (rather than through automation or outsourcing) are more likely to report that complexity “caused a system outage” (Figure 7).

They are also more likely to state that complexity “had no known impact” on security breaches or system outages. Since manual management is typically more error-prone than automated, we surmise that some security breaches might be going unnoticed in manually managed, complex environments.

Figure 6: How do you manage multiple devices/vendors on your network?

- Automate through centralized management: 13.4%
- Outsource: 11.8%
- Manually manage through each vendor’s console: 51.2%
- Manually manage each device/technology: 23.6%

Figure 7: Impact of complexity, companies who manage multiple vendors/devices manually (compare to Figure 5)

- Caused a security incident: 6.7%
- Caused a system outage: 30.0%
- Caused both a security incident and a system outage: 6.7%
- Had no known impact on security/system availability: 56.7%

SHARE THIS RESEARCH:
Challenges of Complexity

**Figure 8:** What is the greatest challenge of working with multiple security devices in your network?

- Too many policies to manage: 43.7%
- Too many management consoles: 27.0%
- Audit preparation is too time-consuming: 13.5%
- Different departments responsible for different devices: 15.9%

**Figure 9:** What is the greatest challenge of working with multiple security vendors on your network?

- Different expertise required for each vendor: 49.6%
- Complexity of the audit process: 17.3%
- Conflicting policies create security gaps: 10.2%
- Lack of interoperability: 22.8%

**Number of Devices**

43.7% of all respondents state that the leading challenge of managing multiple devices is that there are too many policies to manage (Figure 8). Another 27.0% state that having to use too many management consoles is their top challenge. Both these responses indicate that the sheer volume of policies and devices adds difficulty to network security management.

**Number of Vendors**

Nearly half, 49.6%, of respondents state that the greatest challenge of working with multiple vendors is that different expertise is required for each vendor (Figure 9).

When these responses are grouped by the number of vendors supported, “different expertise” remains the top challenge across all groups, and increases in prominence as the number of vendors increases. Of the respondents who work with more than 10 vendors, 71.4% cited the need for different expertise as the top challenge.
Complexity and Next-Generation Firewalls (NGFWs)

This survey validates the findings on NGFWs in our previous study, “The State of Network Security 2012: Attitudes and Opinions,” which found that while 84.0% of respondents report feeling more secure with NGFWs, 76.0% report the NGFWs add more work to their firewall management processes. In this study, 45.7% of respondents use NGFWs and of this group we see notable differences in the responses, relative to the overall survey:

- **“Too many policies” is a greater challenge.** 48.3% of NGFW users state that “Too many policies to manage” is the greatest challenge of managing multiple devices, compared to 43.7% in the total survey (Figure 8).

- **“Conflicting policies” is a lesser challenge.** 6.9% of NGFW users report that “Conflicting policies create a security gap” is the greatest challenge of working with multiple vendors, compared to 10.2% in the overall survey (Figure 9).

Together, these differences reinforce the finding that NGFWs are effective at closing security gaps, while adding to the overall complexity of the security environment.

**Benefits of Consolidating Vendors**

We asked the security professionals in our survey what the greatest benefit of consolidating vendors would be, and they overwhelmingly state that simplified management would be the most positive result (Figure 10).

When we isolate those organizations who manage network security policy manually through each vendor’s console, the “Simplified management” and “Standardization of expertise” groups are much larger. These respondents are less concerned with integration, support required, and costs (Figure 10a).

It is clear that multi-vendor environments add to the complexity, overhead, and skills required to maintain a secure environment.
Conclusions

The landscape of network security is only becoming more complex and difficult to manage, as security threats become more sophisticated and as new technologies are adopted. Next-generation firewalls and other new technologies can reduce risk, but at a potential cost of complexity and overhead. Security professionals face an increasing challenge to keep their networks safe, affordable, and manageable.

The good news is that opportunities for simplifying network security do exist. Most markedly, a vast majority of companies of all sizes have the opportunity to automate their manual processes.

With too many policies, too many management consoles, and too much of a range of expertise required to keep the network secure, security professionals know that consolidating vendors would simplify their operations. And simplifying operations means tighter, more effective security.

More is not better when it comes to devices and vendors in a network security environment. When the environment grows so complex that policies are harder to manage and available personnel can’t handle the load, then bigger and better technology doesn’t mitigate risk—it creates risk. Security professionals who manage these complex environments have a new responsibility to simplify, in order to keep their digital assets safe.

For further reading, see “The State of Network Security 2012: Attitudes and Opinions,” available from AlgoSec.
About AlgoSec

AlgoSec is the market leader in network security policy management. AlgoSec enables security and operations teams to intelligently automate the policy management of firewalls, routers, VPNs, proxies and related security devices, improving operational efficiency, ensuring compliance and reducing risk.

More than 900 of the world’s leading enterprises, MSSPs, auditors and consultancies rely on AlgoSec Security Management Suite for unmatched automation of firewall operations, auditing and compliance, risk analysis and the security change workflow.

AlgoSec is committed to the success of every single customer, and offers the industry's only money-back guarantee.

For more information, visit www.AlgoSec.com.