

KEEPING SECURITY SIMPLE, MANAGEABLE, AND EFFECTIVE

MOST FIREWALL MISCONFIGURATIONS THAT LEAD TO BREACHES ARE FROM HUMAN ERROR DUE TO CUMBERSOME OR COMPLEX MANAGEMENT CONSOLES

OPERATIONAL EFFICIENCY NEEDS MEASUREMENT METRICS. SINCE THESE PERFORMANCE EVALUATION TOOLS DIDN'T EXIST, WE CREATED THEM

THE KISSME CHALLENGE

Network security grows more complex every year with enterprises launching bolder applications with broader reach, facing more threats, adopting new devices, and implementing new security tools to protect it all. With so many sites to oversee, appliance settings, updates to install, and threats to protect against, keeping IT security simple, manageable, and effective (**KISSME**) begins, and ends, with efficient security management.

According to Gartner, "more than 95% of firewall breaches are caused by firewall misconfigurations, not firewall flaws"¹. Cumbersome or complex management consoles greatly increase the likelihood of human error. If you have five or six management platforms—with each requiring different software to configure, monitor, and update, the likelihood of making a mistake is much higher.

Every security vendor claims to have a simple management console, but how do we actually measure this simplicity? When it comes to ease of use, it is clear not all consoles are created equal. Operational efficiency needs clear metrics. Since there is no uniform performance evaluation tool available, we created a measurement system based on several key factors. Our research team selected four representative areas of security management—routine tasks that a security team commonly faces - and evaluated how these four vendors deal with managing them: Check Point Software Technologies, Palo Alto Networks, Fortinet, and Cisco. (You can watch some examples on this YouTube page: <http://tiny.cc/KISSME>.)

FOUR CHALLENGES THAT MEASURE SIMPLICITY

Security Function	Check Point	Palo Alto	Fortinet	Cisco
Challenge 1: How Many Consoles Does It Take?	1 console	3 console	3 console	3 console
Challenge 2: A day in the Life of an IT Admin	Fastest time. Validates and monitor policies.	3x more time. Little to no insight.	1.5x more time. Little to no insight.	2x more time. Little to no insight.
Challenge 3: Scaling for Growth	✓	✗	✓	✗
Challenge 4: Ease of Visibility	1 location	2 locations	5 locations	5 locations in 2 consoles

¹ Source: "Q&A: Is It More Secure to Use Firewalls from Two Different Vendors?" Gartner 2010

**COMPLEXITY TRANSLATES
DIRECTLY INTO HEADCOUNT—
DIRECTLY IMPACTING
OPERATIONAL COST AND RISK**

**THE MORE COMPLEX A SYSTEM
IS TO MANAGE, THE HIGHER
THE POSSIBILITY FOR
MISTAKES THAT EXPOSE YOUR
BUSINESS TO RISK AND
LOSSES**

**DIFFERENT SECURITY ZONES
SHOULD NOT BE MANAGED BY
DIFFERENT MANAGEMENT
CONSOLES**

We determined four common tasks or "challenges" that network administrators routinely manage and listed them in the table shown above. Then we ran through the list with each vendor and tallied the differences between the experiences. The first challenge was basic: we wanted to see how many software management applications each vendor uses to execute routine security tasks. In the second challenge, we evaluated how long it took to create a new security policy. The third challenge looked at how easily each vendor platform scales to support business growth. Finally, we looked at how each vendor helps visualize risk and monitor security events.

These four challenges all ask: How simple, manageable and easy is each vendor's product to use in daily operation? Complexity translates directly into headcount—directly impacting operational cost and risk. The more complex a system is to manage, the higher the possibility for mistakes that expose your business to risk and losses.

As you read through the challenges, reflect on these questions and evaluate your team's needs. How many times does your own team execute these exact same tasks every month? If you save five, ten, or even five hundred minutes per month in execution time across these challenge tasks, what would that mean to your productivity and overall business security?

CHALLENGE 1. HOW MANY CONSOLES DOES IT TAKE?

The Management Console Challenge

Let us assume you have a fairly typical network with five basic elements: (1) a Next Generation Firewall (NGFW) protecting your applications, running on (2) a set of virtual machines in a data center and (3) protected by both endpoint and threat management systems. You also have to (4) secure email and web content, as well as meet requirements to (5) collect forensics and show compliance. How many software management consoles does it take to manage all this?

The answer is three—if you are using Palo Alto Networks or Fortinet. With Cisco, the answer could actually be four. Using Check Point however, the answer is ONE.

Challenge 1 Results

Each vendor handles the five routine security tasks mentioned above differently:

Palo Alto Networks

Palo Alto Networks requires three different security management platforms to manage their security solutions. Palo Alto Networks Panorama for central gateway management, Traps for endpoint management, and GlobalProtect for mobile security management. Palo Alto Networks allows management of security policies locally from their gateways, or centrally from Panorama. The lack of coordination between the two, however, creates potential for policy conflicts that let malware in without administrators knowing.

CHECK POINT BUILT ITS SECURITY ARCHITECTURE FROM THE GROUND UP TO BE MANAGED FROM A SINGLE PLATFORM-ONE INTEGRATED PANE OF GLASS TO CONFIGURE, MONITOR AND MANAGE NETWORKS OF VIRTUALLY ANY SIZE

Fortinet

Fortinet requires three different security management platforms: FortiManager handles central gateway management, FortiAnalyzer collects forensics, and a separate VMX Service Manager handles the VMWare NSX virtual server security environment. As with Palo Alto Networks, Fortinet manages security policies either locally from a FortiGate gateway or centrally from FortiManager, creating the potential for policy conflict undetectable by administrators.

Cisco

Cisco uses four different platforms to manage the same services: Cisco ASDM/CMS manages the firewall and VPN, FireSIGHT manages the Next Generation Firewall, Secure Content Manager manages the email and web content filtering, and Cloud Web Security manages mobile remote access. Management of an 'ASA with Firepower' gateway requires two different consoles for a single device.

Check Point

Check Point built its security architecture from the beginning to be managed from a single platform; one integrated pane of glass configures, monitors, and manages networks of virtually any size. Policy management, content management, endpoint management, forensics, event analysis (SIEM), and compliance all integrate to create a unified ecosystem for increased network and threat visibility across the organization. Management of one console is easier, more cost effective, and much less prone to conflict and errors. The Check Point R80 console manages all functions using a unified set of policies.

How You Got There

You may have added multiple layers of security to your network over time, so now your security team must handle the complexities of managing and configuring each of them. **Different security zones should not be managed by different management consoles.** Monitoring and adjusting settings for every section of your network with a separate console can cause mistakes to quickly add up.

One single pane of glass for integrated security management is at the heart of our KISSME principle. This integrated platform allows collaboration of management duties and tools for comprehensive visibility, consistent security deployment, and increased efficiency.

IF PERFORMING A TASK TOOK 30 STEPS AND 6 MINUTES USING ONE VENDOR, AND ANOTHER HALF AS LONG, WHICH WOULD YOU CHOOSE?

THE FEWER NUMBER OF DISCRETE STEPS, THE LOWER THE WORKLOAD, DIRECTLY LOWERING LABOR COSTS

FEWER STEPS RESULT IN FEWER OPPORTUNITIES FOR MISTAKES

Security Function	Check Point	Palo Alto	Fortinet	Cisco
Police Management	R80 Security Manager	Panorama	FortiManager	Cisco Security Manager (CSM) + FirePower Management
Forensics			FortiAnalyzer	
Remote Access & Endpoint Security		GlobalProtect Mobile Security Manager	FortiManager	Cisco Security Manager (CSM)
		Traps		Cisco Cloud Web Security
Data Center Security (VMware NSX)		Panorama	FortiGate-VMX Manager	N/A
Email/Web Content Security			FortiManager	Secure Content Manager
SIEM (Event Analysis)		N/A	N/A	N/A
Best Practices (Compliance)		N/A	N/A	N/A

CHALLENGE 2. A DAY IN THE LIFE (OF AN IT ADMINISTRATOR)

The Typical Day Challenge

The design of the management console greatly affects how easy, or difficult, it is to complete a typical set of routine administrator tasks. If performing a task took 30 steps and 6 minutes with one vendor, and half as long using another, which option would you choose?

The fewer number of discrete steps, the lower the workload. This directly reduces labor costs, and more importantly, lowers risk. One single breach could cost your company millions of dollars and weeks to clean up. Less programming steps means fewer opportunities for costly mistakes.

We chose several routine tasks that security administrators have to complete on a regular basis and examined the performance of each vendor in this regard. The tasks we picked are: (1) Create a Next Generation Firewall rule with users, applications, data type, and rule expiry; (2) Create a sub-policy allowing granular administrator access only to this policy segment; (3) Verify that the new policy rule is valid across the network and compliant with security regulations and standards; (4) Monitor rule usage and track changes.

Each security offering performed these tasks very differently. Some offered all of the features while others did not. Some required a few mouse clicks to activate a feature while others required several dozen to accomplish the same task.

IN PALO ALTO NETWORKS, ISSUING A NEW FIREWALL POLICY REQUIRES 70 MOUSE CLICKS AND NEARLY FOUR MINUTES TO COMPLETE, ALMOST THREE TIMES MORE STEPS THAN CHECK POINT

FORTINET DOES NOT HAVE POLICY VERIFICATION BUILT INTO THE FORTIGATE SECURITY POLICY, AND NO ERRORS DISPLAY IF AN ADMINISTRATOR MISCONFIGURES A LOCAL FORTIGATE POLICY

Every administrator will tell you the simpler it is, the more they like it. Here is how each vendor performed on the series of typical tasks: (You can watch some examples on this YouTube page: <http://tiny.cc/KISSME>.)

Challenge 2 Results

Palo Alto Networks

- **Creating a firewall policy:** Issuing a new firewall policy requires nearly four minutes to complete, almost three times more steps than Check Point.
- **Policy segmentation:** Palo Alto Networks' policy lacks admin granularity and control for management operations within the security policy (e.g. inline/ordered policies with at-rule level permissions)
- **Verifying a firewall policy:** Palo Alto Networks verifies policy validity during installation, but cannot continuously monitor the policy at the time of policy creation. Verification of real-time policy compliance requires a third-party solution.
- **Monitoring rule usage and changes:** Palo Alto Networks' gateways show rule usage in the ACC (Application Control Center) only by traffic volume. Unlike Check Point, they cannot show rule utilization per session, rule change history, or log related rules in the security policy.

Fortinet

- **Creating a firewall policy:** Coming in second at approximately 20% longer than Check Point, Fortinet required over two minutes for configuring a policy rule.
- **Policy segmentation:** Fortinet's policy lacks admin granularity and control for management operations within the security policy (e.g. inline/ordered policies with at-rule level permissions)
- **Verifying a firewall policy:** Fortinet does not have policy verification built into in the Fortigate security policy (policy verification only available in FortiManager). No errors display if an administrator misconfigures a local Fortigate policy—meaning the administrator won't know until it is too late. Verification of real-time policy compliance requires a third-party solution.
- **Monitoring rule usage and changes:** Fortinet has very basic hit count data on its local Fortigate gateways. It can only show traffic volume processed by each rule and redirect policy rules to matching logs in the log view window. As this is only a local Fortigate feature, there is no global view of policy and rule utilization across multiple devices and policies.

CISCO REQUIRES TWO DIFFERENT POLICIES FOR MANAGEMENT OF CISCO ADAPTIVE SECURITY APPLIANCE (ASA) WHEN USED WITH FIREPOWER SERVICES

ADDING A NEW FIREWALL RULE TAKES 90 SECONDS WITH CHECK POINT AND THE LOWEST OVERALL LABOR TIME IN DAY-TO-DAY MANAGEMENT TASKS

CHECK POINT IS THE ONLY VENDOR TO SUPPORT POLICY CUSTOMIZATION AND ADMINISTRATIVE GRANULARITY IN THE FORM OF SUB-POLICIES AND LAYERS

Cisco

- **Creating a firewall policy:** Issuing a new firewall policy on Cisco gear using Cisco FireSIGHT Manager requires twice as much time as it does with Check Point.
- **Policy segmentation:** Cisco’s policy lacks the admin granularity and control for management operations within the security policy (e.g. inline/ordered policies with at-rule level permissions)
- **Verifying a firewall policy:** Cisco FireSIGHT and Check Point are the only management platforms providing verification mechanisms during policy installation and real-time validations during policy maintenance. Cisco verification of real-time policy compliance requires a third-party solution.
- **Monitoring rule usage and changes:** Cisco does not offer support in monitoring rule usage and changes.

Check Point

- **Creating a firewall policy:** Adding a new firewall rule takes 90 seconds—the lowest overall labor time amongst the four vendors.
- **Policy segmentation:** Check Point Management is the only vendor to support delegation and assignment of admin permissions per policy segment. Inline and ordered policies allow fine-tuning and control of admin duties and policy operations.
- **Verifying a firewall policy:** Check Point provides multi-layered policy checks accounting for human error and risks that could potentially lead to a security breach. Verifying and validating all policies and sub-policies is done continuously during operation. Check Point also offers real-time compliance checks and best practices security advisories for deeper understanding of the overall policy and gateway security status.
- **Monitoring rule usage and changes:** Check Point is the only vendor providing detailed information on session hit count, rule history, and integrated rule-related logs for every policy rule. Monitoring policy effectiveness and rule usage allows better policy optimization and maintenance. No other vendor provides this level of granularity for both policies and devices.

According to NSS labs’ Next Generation Firewall (NGFW) comparison testing², Check Point is the leading NGFW solution with the lowest management labor of security gateways.

Security Function	Check Point	Palo Alto	Fortinet	Cisco
Task 1: Add NGFW Policy	1:45 min	3:45 min	2:11 min	3:45 min
Task 2: Create a Sub-Policy	✓	✗	✗	✗
Task 3: Validate Policy	✓	✗	✓	✗
Task 4: Monitor Rule Usage and Changes	✓	Partial	Partial	✗

² Source: Next Generation Firewall Comparative Analysis—Management, NSS Labs 2013

**CHECK POINT IS THE ONLY
VENDOR TO PROVIDE
DETAILED INFORMATION ON
HIT COUNT, RULE HISTORY AND
INTEGRATED RULE-RELATED
LOGS FOR EVERY POLICY**

CHALLENGE 3: SCALING AND COLLABORATION

The Scaling and Collaboration Challenge

Whether your network consists of ten or ten thousand gateways in a single site or hundreds of locations around the globe, your security management must easily scale with your business. Scalability consists of the ability to (1) segment and separate admin duties based on location, business unit, and security functions, (2) load share management resources and tasks with the option for growth and scaling out, and (3) collaborate administrative duties without any collisions.

Failure to support all the above leads to excessive labor and increase in administration costs. There are several ways to deal with the demands of scalability. First, a solution must support logical separation or multi-tenancy between different security domains (domains are autonomous units—each can manage different policies, databases, and security functions). Secondly, it must support load sharing of management resources by utilizing function-specific dedicated servers to create a scalable ecosystem for policy administration, log collection, reporting, and event analysis. Thirdly, administrators must be able to collaborate and delegate security tasks, performing them on the same policy simultaneously without conflict.

A truly scalable management system encompasses maximum operational efficiency, enhanced productivity, and easy management of thousands of objects, rules, and domains. In the following series of tasks, we tested the vendor tools available for security administrators to manage large scale deployments and distributed networks with multiple domains and complex policies.

IN LARGE SCALE ENVIRONMENTS WITH LARGE VOLUMES OF BUSINESS TRANSACTIONS, FAST DETECTION AND REACTION ARE CRITICAL

Challenge 3 Results

- Palo Alto Networks** has very limited operational efficiency. Unable to scale up to more than a single policy, its management does not offer separation of duties and multi-tenancy or separation of object database and logs. For full separation of administrators and policy management, a new Panorama management instance is needed. Administrative collaboration for simultaneous policy editing requires overriding other administrator changes or having each admin manually lock the database policy.
- Fortinet** offers a scalable solution using administrative domains with separation of objects database, policies, and logs—but only on the same FortiManager device. Administrative domains and logs are limited and cannot be shared between different FortiManager devices. Administrative collaboration is also very limited --there is no way to allow simultaneous policy modification without overriding other administrators' changes. Locking the policy manually by each administrator is possible, but is disabled by default.
- Cisco** management (FireSIGHT) offers very limited scalability with the ability to manage only 25 gateways. It does not offer multi-tenancy, or load sharing between management devices and functions. With no full separation of management duties, customers must purchase a new Cisco Management device for these capabilities. As with other vendors, simultaneous collaboration of administrators and the option to perform multiple tasks at the same time is not available.
- Check Point** management offers the best operational efficiency for policy management. The Multi-Domain Manager offers full separation of duties, allowing domains to be spun up in one click. A brand new domain launches with its own object database, policies, logs, admin roles, and even its own SmartConsole access. Horizontal scaling of domains across different servers in multiple locations facilitates load sharing and high availability. Global policies for firewall, IPS, and VPN allow fast deployment of policies and objects across multiple domains. In addition, only Check Point allows multiple administrators to modify the same security policy simultaneously, without any collision or conflicts.

Security Function	Check Point	Palo Alto	Fortinet	Cisco
Management Multi-Tenancy	✓	✗	✓	✗
Full Separation of Object Database, Policies and Logs	✓	✗	✓	✗
Global Policies Across Domains	✓	✗	✓	✗
Admin Concurrency and Collaboration	✓	✗	✗	✗

CHALLENGE 4: SIMPLE VISIBILITY AND MONITORING

The Visibility and Monitoring Challenge

Security administrators must know what is happening inside the organization at all times. They require visibility into the flow of data streaming in and out of the business operation—a complete picture of network traffic, applications, data flow, user identity, and security incidents.

In large-scale environments with large volumes of business transactions, fast detection and reaction is critical. Security management platforms must provide real-time monitoring, network traffic history status, system resource usage, and overall performance. How each vendor logs, analyzes, and monitors events within your organization is critical to your security effectiveness. How difficult is it for your administrators to find this data, and how quickly?

Challenge 4 Results

Palo Alto Networks

Palo Alto Networks console does not offer integrated advanced forensics nor event analysis tools. Although unified logging is supported for network traffic, Palo Alto log view doesn't show logs received from endpoints (Traps). Instead of simple Google-like contextual searching, log search with Palo Alto Networks requires complex filter expressions.

```
(receive_time in last-7-days) and (user.src eq 'John Smith') and (app eq dropbox) and (port.dst eq 8080)
```

Fortinet

With five different locations for logs, Fortinet requires specific queries and filters when searching for logs. The management console does not offer integrated advanced forensics and event analysis tools.

Cisco

The most cumbersome of the four and requiring specialized knowledge for searching, Cisco requires five places to look for logs across two different consoles. The console also does not offer integrated advanced forensics and event analysis tools.

General Information		
First Packet	2015-12-02 00:00:00	> 2009-07-16 13:00:31, < today at 4:30pm
Last Packet	2015-11-25 00:00:00	> 2009-07-16 13:00:31, < today at 4:30pm
Initiator User*	John Smith	jsmith
Networking		
Destination Port / ICMP Code*	8080	1-1024, 6000-6011, !80
Application		
Application Protocol*	Dropbox	HTTP

**FORTINET
REQUIRES 5 DIFFERENT
PLACES TO LOOK FOR LOGS,
AND SEARCHING LOGS IS DONE
USING COMPLEX FILTER
EXPRESSIONS**

**THE MOST CUMBERSOME OF
THE GROUP, CISCO REQUIRES
YOU TO LOOK FOR LOGS IN
FIVE PLACES ACROSS TWO
DIFFERENT CONSOLES**

CHECK POINT—LOOK IN ONLY ONE LOCATION TO MONITOR LOGS. SEARCH IS CONTEXTUAL, USING GOOGLE-LIKE SEARCH PARAMETERS FROM A SINGLE VIEW, MAKING FORENSICS SIMPLE AND FAST

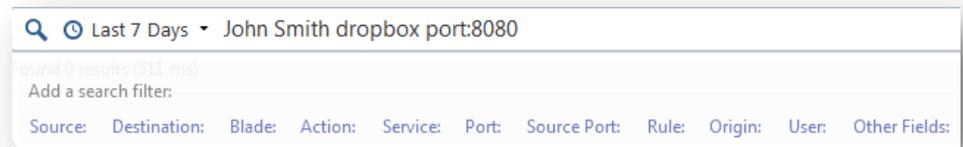
CHECK POINT PROVIDES A COMPLETE SUITE OF VISIBILITY AND FORENSICS OFFERINGS

SMARTLOG, SIMPLE SEARCH SINGLE LOG VIEW

SMARTEVENT, A SIEM EVENT MONITORING SYSTEM THAT DESCRIBES EVENTS USING ACTIONABLE SECURITY TERMINOLOGY

Check Point

With Check Point, you only need to look in one location to monitor logs and you can use contextual, Google-like search parameters for simple and fast forensics. Check Point also provides a complete suite of visibility and forensics offerings like SmartLog, a simple search single log view; SmartEvent, a SIEM event monitoring system describes events with actionable security terminology; and gateway monitoring with real-time history and intuitive statistics data. With logs integrated into the policy dashboard, you can access all associated logs for a rule with a single click. These integrated forensics features make management of complex security environments easier and faster, saving administrative time and lowering overall cost of ownership. Here is an example of the ease of searching and receiving results in reader-friendly format. All that the administrator needs to type is the user name, the application, and the port used:



Security Function	Check Point	Palo Alto	Fortinet	Cisco
Number of Log Views	1 view for everything	2 views	5 views	5 views in 2 different consoles
Contextual, Google-Like Log Search	✓	✗	✗	✗
Native SIEM with (Event analysis) with Actionable Security	✓	✗	✗	✗
Real-Time & History Gateway Monitoring	✓	Partial	Partial	Partial

SUMMARY

Network security is all about managing complexity and making it simple to access, configure, monitor, and scale security. Whether managing a few sites with hundreds of rules or complex architectures requiring auditing and compliance monitoring, you need the right tools and management architecture. One small mistake in the security policy can be catastrophic and expose the business to undesired risks. Your security administrators access the management console daily—and the more complex it is, the higher the chance for user error. Your security vendor should be keeping your IT security simple, manageable, and efficient. Take a close look at the challenges we have presented to see if you can find ways to be more efficient, organized, and effective in managing your security.

Based on the results of our analysis, Check Point Security Management (R80) is the industry's most integrated and robust platform for managing security at organizations large and small. Check Point is the only vendor in the industry to offer a fully integrated management architecture for your entire security system. Keep your IT security simple, manageable, and effective (KISSME). Manage it once. Manage it with high operational efficiency. Keep your business safe and lower your overall costs.

Visit <http://www.checkpoint.com/resources/r80/> for more information and to schedule a demonstration.