White Paper

McAfee®

Consolidate Network Security to Reduce Cost and Maximise Enterprise Protection

Table of Contents

Security Consolidation 3
Application identification and control 3
User identification and control 3
Intrusion prevention 3
Denial-of-service protection 3
Web application protection 3
Network behavioural analysis 4
Network access control 4
Approaches for Network Security Consolidation 4
Cost and Security Considerations 4
Hardware and software license capital expenditure 4
Firewall rule-set migration costs 5
Policy and process modifications 5
Potential for increased security coverage 5
Summary 6

Security Consolidation

An organisation's network security infrastructure has typically been built from discrete blocks of security technologies. Starting with the network firewall providing perimeter access control, today's network security often comprises a complex, difficult-to-manage amalgam of anywhere between five and 50 different technologies.

With advances in technology, you are presented with the opportunity to consolidate many of these security components into fewer platforms. This consolidation can reap many benefits:

- Reduced need for hardware devices unlocks the potential for significant capital expenditure savings
- Consolidation of management platforms reduces the operational overhead of network security
- Consolidation of management platforms also provides an integrated view into your security posture, giving your organisation better control and hence better security
- With fewer platforms to manage, your staff will be freed from maintaining security and can use their time to work on managing risk much more effectively

There are multiple options when considering network security consolidation—too many to cover fully in this white paper—so let's look at the most common scenario faced by most organisations:

Key Consolidation Capabilities

Deploy advanced threat detection and prevention technologies to supplement the access control provided by your existing firewall estate.

Let's take a look at technology capabilities to consider in the context of network security consolidation.

Application identification and control

With so many enterprise applications now web-enabled, the traditional firewall has neither visibility nor control over how these are accessed. Many remote desktop, peer-to-peer, file-sharing, and other similar high-risk applications will tunnel over any open port they can find, leaving your organisation incapable of securing your environment. Application identification and control peels back the layers and exposes the true application inside network traffic, allowing you to regain the control necessary to effectively secure the environment.

Many exploits try to benefit from the lax security in social networking sites by concealing their payloads within trendy applets. With application identification and control, you can allow access to the beneficial elements of sites like Facebook, but minimise the risk of compromised applications within each site.

User identification and control

Fine-grained control allows comprehensive enforcement of policy based on business needs. Instead of policies matched just to IP address, port, or protocol, you can now associate a user, their role, and their authorised set of applications. This tight control not only provides better security, but also makes policies much easier to define and implement.

Intrusion prevention

Intrusion prevention provides organisations with the ability to automatically detect and block an attack in progress, thereby preventing the exploit and keeping you secure.

Denial-of-service protection

A denial-of-service (DoS) attack is one of the most disruptive threats facing organisations today, often resulting in key services not being available for days or weeks. The business impact of a DoS attack can be significant. By building in DoS protection as part of your consolidation project, the potential impact of such an event can be contained and often fully mitigated, keeping your business up and running.

Web application protection

Web applications have become the heartbeat of many organisations, typically representing the core business applications for internal staff and customer interactions. Building on top of intrusion prevention capabilities, dedicated web application security technologies can protect your key assets from becoming the target of attacks.

Network behavioural analysis

Advanced persistent threats (APTs), by their very nature, are particularly difficult to identify and block with traditional security technologies. By utilising network behavioural analysis, organisations can look for the markers associated with APTs, identify a security breach, and prevent the loss of sensitive company assets.

Network behavioural analysis also allows the security organisation to collect information from parts of the network where it is simply not practical or cost effective to deploy security technologies. This wider visibility is essential for obtaining a complete view of threats throughout the organisation.

Network access control

Many security threats bypass robust perimeter security by connecting directly to the internal network. Infected visitor and contractor machines are the most common examples of this type of threat. Using network access control to extend the perimeter controls to internal devices, you can ensure that you maintain the integrity of your systems without security becoming a burden on the users.

Approaches for Network Security Consolidation

We will look at the following three approaches to achieve consolidation:

- Upgrading your existing network firewall to a next-generation firewall from the same vendor. For this case, we will use Check Point Software Technologies, the most widely deployed network firewall, as the example.
- Swapping out your existing network firewall for a next-generation firewall from a different vendor. In this case, we will use Palo Alto Networks as the example.
- Supplementing the existing network firewall with a stand-alone intrusion prevention system (IPS) platform. We will use McAfee Network Security Platform, the leader in the Gartner Magic Quadrant, as the example in this case.

Cost and Security Considerations

To compare and contrast these options, let's look at the key cost aspects of the consolidation, as well as the potential for increased security.

Hardware and software license capital expenditure

Check Point	Palo Alto	McAfee
€€€	€€	€€

Check Point represents the option with the highest capital cost outlay for consolidation. Existing Check Point customers will find that their current firewall hardware will not support the next-generation firewall feature set; therefore, a fork-lift upgrade will be necessary. Customers migrating to Check Point will have the exact same requirement to purchase hardware.

Independent third-party tests* show that enabling the next-generation security features has a major negative impact on the hardware performance. Given that the performance of a Check Point platform can be as little as 25 percent of the data sheet rating, Check Point customers must select hardware that is significantly oversized or face the risk of the firewall becoming a bottleneck in the network. This will add significant cost to the solution, making it more expensive than both Palo Alto Networks or McAfee solutions.

Hardware costs for both Palo Alto Networks and McAfee are equivalent for products with comparable specifications.

* NSS IPS Group Test Q4 2010: Check Point submitted a product rated on the data sheet as 10 Gbps IPS throughout. Testing revealed that when exposed to real-life network traffic, the product was only able to achieve 2.5 Gbps, or just 25 percent of the data sheet rating.

Firewall rule-set migration costs

Check Point	Palo Alto	McAfee
n/a or €€€	€€€	n/a

To realise the advantages of a combined firewall and IPS platform, organisations will have to replace their existing firewall deployment. This will require extensive work to migrate the existing firewall rule-set to the new firewall product. Despite the availability of migration tools, this process requires extensive manual tuning and testing to ensure an error-free deployment. For example, a customer with 50 firewalls can expect migrations to cost in the region of tens of thousands of dollars and projects to exceed one year for deployment.

For existing Check Point deployment, the addition of next-generation feature will not require any form of firewall rule-set migration—the existing management platform already holds the policy. For organisations migrating to either the Check Point or Palo Alto Networks platform, however, a complex and time-consuming rule-set migration will be required.

For organisations choosing to supplement their existing network firewall with the McAfee product, the existing firewall will remain untouched, thereby avoiding this complex, time-consuming, and expensive step. The single biggest benefit (cost avoidance aside) is that the advantage of having the additional security can be realised much more quickly, giving the project team success more quickly. For organisations under regulatory or compliance pressures, this shorter project cycle can mean the difference between success and failure.

Policy and process modifications

Check Point	Palo Alto	McAfee
€€ or €€€	€€€	€€

In all cases, the addition of next-generation security capability will require that your current security policies and process be adapted to include these new technologies. However, the degree of adaption effort varies considerably, depending upon your chosen path of consolidation.

In the case of upgrading an existing Check Point deployment to the latest next-generation security features, the changes required to processes are limited to the new technologies added. This goes equally for the McAfee option, as existing security technologies are not impacted.

In the case of a company migrating to either Check Point or Palo Alto Networks, existing security processes will need to be reviewed and rewritten to take both the new technologies into account and the new products associated with the existing security deployment.

Potential for increased security coverage

All three consolidation options offer the basic security enhancements often considered essential: application identification and control; user identification and control; and intrusion prevention.

The table below highlights the potential for increased security.

	Security Element	Check Point	Palo Alto Networks	McAfee
↑ Increasing Security	Network Access Control	Partial	No	Yes
	Network Behavioural Analysis	No	No	Yes
	Web Application Protection	Partial	No	Yes
	Denial-of-Service Protection	No	Partial	Yes
		CONSOLIDATION CEILING		↑
	Intrusion Prevention	Yes	Yes	Yes
	User Identification and Control	Yes	Yes	Yes
	Application Identification and Control	Yes	Yes	Yes
	Firewall and VPN	Yes	Yes	Use Existing

In the case of Check Point and Palo Alto Networks, this is the limit of the potential; in effect, an enterprise would be reaching a consolidation ceiling with either of these vendors. Organisations wishing to realise additional security benefits using these two vendors will need to create additional projects for the selection and acquisition of more security products. This will, in turn, require additional spend, staff time, and management overhead, eroding any consolidation benefit.

The McAfee option allows organisations to continue to enhance security using the products already deployed in the four key areas highlighted above: denial-of-service protection, web application protection, network behavioural analysis, and network access control.

	Check Point	Palo Alto Networks	McAfee
Benefits:			
Potential for Increased Security	Limited	Limited	Very High
Costs:			
Capital Expenditure	€€€	€€	€€
Rule-Set Migration	€€€ or n/a	€€€	n/a
Policy and Process Modification	€€	€€€	€€

Summary

There is no doubt that network security consolidation can deliver cost and security benefits and should be a key part of any organisation's strategy. However, there are also many hidden costs associated with re-engineering your security infrastructure that may erode some, if not all, of the potential savings.

Many of these hidden costs arise from the time and effort associated with the fork-lift upgrade necessary to change your current network firewall to support next-generation capabilities. By leaving this entrenched technology in place and supplementing with the McAfee Network Security Platform, organisations like yours can realise greater consolidation benefits whilst minimising project costs and disruption to your production environment. For more information about McAfee Network Security Platform, visit www.mcafee.com/nsp.

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com