BLUE COAT

Security Empowers Business

7 QUESTIONS TO CONSIDER IN SECURING YOUR NEXT GENERATION DATA CENTER

WHITEPAPER

Virtualization and other next generation technologies are proving cost-effective, but with the expanded role of the network, network security requires some rethinking. The choices made for network security can impact ongoing operational costs, the uptime of security services, and the precision to control which users are using which applications. This paper considers those network security choices and their cost effectiveness in protecting the network, the data passed over that network, and therefore the organization's reputation.

Consolidated and virtualized data centers have become the norm for both traditional applications and evolving cloud-based applications. Securing these data centers, however, requires a broad set of protection - a simple perimeter defense is no longer adequate.

With more complex threats arising daily, setting and forgetting about network security is no longer an option. Not only must your network security solution stay in front of the escalating number of attacks and their increasing sophistication, but it must also support the demands for ever-higher network performance and continuous network availability. Additionally, given ongoing budget constraints, it is worthwhile to explore some considerations for cost-effective consolidation which could also improve performance and continuous availability of your network security.

As you rethink network security, consider the following:

1. **How flexible and scalable will your network security infrastructure be when capacity requirements change?**

   Will it allow for incremental and cost-effective expansion over time or will it require you to purchase additional or larger network security appliances to replace devices? Will additions require structural changes to the network that could impact network availability? Data center consolidation can exacerbate future throughput requirements, or at a minimum, temporarily impact throughput if it is necessary to move data to a new data center. Will you have the flexibility desired?

   This level of scalable performance is available today with the Crossbeam X-Series platform. It provides flexibility for incremental expansion since it scales linearly – each application module scales performance equally, whether it's the 1st or the 8th Application Processor Module (APM). The Crossbeam X-Series enables you to pay-as-you grow – adding performance as it is needed without the need of a forklift upgrade or re-architect the network.

2. **Will the network security solution support your business uptime goals?**

   Interruptions to firewall and other security appliances typically require manual efforts to rectify problems, potentially impacting business operations in the interim. When evaluating network security solutions, it is key to understand how different failures impact service availability. For example:

CONFIGURATION	IMPACT UPON A FAILURE	TASKS TO REMEDIATE AND RESTORE MAY INCLUDE:
ACTIVE: ACTIVE PAIR	Network Performance	1. Locate or obtain replacement device 2. Bring that device up to current patch level 3. Configure device for network 4. Make network changes to accommodate device
ACTIVE: STANDBY PAIR	Delay during transition; May require manual intervention	
IPS APPLICATION	No longer processes traffic (fails open-traffic flows without IPS inspection)	

   The effort to fully restore service should not be underestimated – it could be a full day of tasks and headaches before the replacement device can join the network. In contrast, the Crossbeam X-series enables redundant modules to instantaneously and automatically pick up the load of a failed module – without any interruption to the network and without needing to locate and service a replacement appliance. This Crossbeam Adaptive Self-Healing approach allows the most stringent service level requirements to be met without any network modifications or re-wiring to recover from a failure, thereby enabling 5 9's availability, or 7 9's availability with a dual box pairing.

FUNCTIONAL AREA	DESCRIPTION	IMPACT OF USING
PROXY FIREWALL	Terminates incoming requests, inspects them, and then reestablishes each connection	Ensures that no traffic enters without inspection – no leaking firewalls here!
IPS	Intrusion Prevention	Detects unknown, but suspicious requests
ANTI-VIRUS STRONG BOTNET ANTI-SPAM	Inspects for known malware and spam	Eliminates known threats from your incoming traffic
URL FILTERING	Utilizes SmartFilter, the leading web filtering software, to intelligently filter based on monitoring over 35 million blockable websites via Global Threat Intelligence	Prevents use of your network to access sites that could expose your organization.
DEEP APPLICATION CONTROL	Inspect and identify applications and application sub-functions	Know what traffic and applications are entering the network
IPSEC VPN	Create and manage VPNs	Confidentiality of data transmitted; Secure access
SUPPORT FOR COMPRESSED FILES	Scanning of compressed files	All types of traffic inspected
SUPPORT FOR SSL/SSH	SSL/SSH decruption to inspect encrypted traffic	All types of traffic inspected

3. **What level of protection will your Firewall provide?**

   Security products vary in their effectiveness against threats depending upon the vector – application, file, web, email, or network. To achieve the highest level of assurance, security products across these vectors should be integrated, which can require substantial effort. McAfee, however, has designed it's Firewall Enterprise to include a broad set of security services that can operate in an integrated high performance manner on a Crossbeam X-series platform:

4. **How beneficial would it be to further consolidate your security services?**

   With the pressure to maximize resources and fulfill cost constraints, larger data centers have become the norm. The concentration of computing, storage, and networking in consolidated or next generation data centers increases the criticality of network availability and adequate performance. Consolidating all security services onto a single platform, like the Crossbeam X-series, affords you the opportunity to add additional security inspections to the traffic flow very cost-effectively. As more security services are used, the greater potential impact on network performance, making the performance capability of the network security platform critical. For example, the McAfee Firewall Enterprise can be used with other best-in-class security applications, such as those from Check Point, Sourcefire, and Imperva – protecting against many critical threats vectors simultaneously on a single platform.

5. **How quickly will your firewall rules and security policies become outdated?**

   A static set of firewall rules is not sufficient in today's perpetually morphing threat environment. Security capabilities should be driven by up-to-the-minute information for reputation-based filtering. One way to stay up to date on threats is incorporated into the McAfee Firewall Enterprise via McAfee's Global Threat Intelligence (GTI). GTI is a comprehensive, real-time, cloud-based threat intelligence service that enables McAfee security products to detect and track unknown and emerging cyberthreats. GTI collects data from more than a hundred million sensors, and correlates that with information from McAfee Labs, McAfee TrustedSource and Geo-location technology, providing the McAfee Firewall Enterprise with up-to-date threat information. And best, it can be enabled on a per rule basis and is not restricted to NAT (Network Address Translation).

6. **How adaptable will your network security be when you need to restructure your network the next time?**

   Since the shift from physical servers to multiple virtual machines enables application workloads to be agile, applications can potentially move transparently from one physical server to another as user access peaks and subsides. Handling these peaks requires agile security for the intra-server traffic. One advantage of the Crossbeam platform, as a "network-in-a-box", is its adaptability to control the flow and sequence different security applications. Flows across different segments of the network can be adjusted without any network reconfigurations or re-wiring. This flow processing provides

BLUE COAT

Security Empowers Business

the flexibility to adapt and consolidate network security applications as needed, handling security holistically and effectively rather than bolting it on the side of your network infrastructure and distorting your network topology to do what you need to do.

7. **How easy will it be to manage?**

   To reduce the impact of network outages, it's highly advantageous to have automated management capabilities. You need to centrally manage which users can access what applications. Having an easy mechanism to identify, set up, and manage the particular users and their access to particular portions of different applications reduces OpEx both initially and also over the long-term. Having those security policies centralized across the organization also brings significant operational efficiencies, including the right click integration between McAfee ePolicy Orchestrator and the McAfee Firewall Enterprise, along with proven endpoint protection and a mature migration tool to move from existing legacy firewalls.

   Energy efficiency also impacts operational costs, so if many security functions can be consolidated into a single highly energy efficient box, significant cost savings can be realized over time. The Crossbeam X-series is saving some customers up to 96% on their CO2 emissions and energy costs, and cutting operating expenses in half.

Summary

However consolidated your network security infrastructure is today, further virtualization and adoption of cloud-based applications presents an opportunity to reduce operational expense and risk if you rethink your network security. The Crossbeam X-series offers advantages for high performance and high availability, which the McAfee Firewall Enterprise on Crossbeam leverages. As a high assurance Next Generation Firewall, the McAfee Firewall Enterprise on Crossbeam creates the most secure, resilient and integrated network security solution available to defend critical corporate and organizational environments from burgeoning threats.

BLUE COAT

Security Empowers Business

v.WP-7QUESTIONS-TO-CONSIDER-IN-SECURING-YOUR-NEXT-GENERATION-DATA-CENTER-EN-v2b-0413

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000