White Paper

Next-Generation Availability and Scalability

The role it plays in economic recovery

Table of Contents

Executive Summary

Network availability and performance have always been critical to enterprise performance, but never as important as it is today. As companies emerge from a recessionary economic climate, they are under increased pressure to meet growing network and business demands with exceptionally lean resources. At the same time, these companies are fighting for business and can't risk the negative impact of a down network or a network that can't keep pace with growing business demands. Regardless of the size and type of company, the cost of downtime can be devastating.

Whether a result of Internet downtime, organized security attacks, natural disasters, or human error, a down or under-performing network generates long-term brand damage, low customer satisfaction, and lost revenue. For companies trying to emerge from the recession ahead of the game, this can single-handedly change the outcome.

As the dependencies on the network are increasing, so are the costs and complexities of network connectivity and network infrastructures. The more complex the network, the more difficult it is to manage and the more prone it is to downtime. According to the Ponemon Institute, 33% of misconfigurations on network equipment are caused by human error leading to network downtime.[1] Even worse, this could lead to a security breach. As a result, many IT leaders are looking for new ways to cost effectively ensure high availability and scalability without jeopardizing profits or compliance.

Recently, a new approach has made its way into forward-thinking organizations that are discovering how to significantly reduce the costs, complexities, and downtime risks. This approach is called next-generation availability and scalability.

This approach, to be discussed further in this paper, goes far beyond system redundancy and load balancing. It encompasses high-availability technologies built into network security solutions. This approach eliminates additional bolt-on solutions and added costs typically required to achieve the level of network performance needed in today's environments.

Network Connectivity: The Roadblocks

In today's 24/7/365 world, virtually every type and size of organization depends on constant network connectivity. Organizations can lose revenue due to downtime. Whether it's internally among employees or externally with customers and partners, organizations expect to be connected anytime, anywhere—in fact, their business models depend upon this.

However, ensuring dependable connectivity is becoming increasingly difficult. To understand the issues, let's review the changes and pressures that IT departments are facing:

- *Economic pressures to cut costs*—IT leaders have always been faced with the challenges of doing more with less (less staff, less budget, and fewer resources), but the pressures have been further magnified in today's uncertain economic climate.
- *Network sprawl*—For many years, mission-critical applications resided on mainframes in a data center. The move to distributed computing environments in the 1980s took many critical systems off the monolithic, yet reliable mainframe and placed them on less reliable hardware. To compensate for outages, redundancy became a standard in network architectures. Disks, network equipment, processors, network cards, and even the servers themselves were doubled up to ensure that a failure would simply transfer the work to backup systems resulting in network sprawl. The result? Today's network infrastructure is complex, costly, and lacking in agility.
- *Increasing web-based and cloud applications*—Over time, software applications have become increasingly web-based. Web technologies and cloud services are deployed to enable employees, customers, partners, contractors, and consultants to be more productive. The implementation of these technologies continues to fuel organizations' dependence on the Internet. At the same time, many organizations have discovered that even dedicated lines, such as multiprotocol label switching (MPLS) networks, are not immune to outages. Anything unexpected, from a backhoe that hits fiber at a nearby construction site to a natural disaster, can disrupt connectivity.
- *More stringent compliance requirements*—With an increased focus on regulatory requirements, auditors are looking for these controls to ensure an organization's compliance with Sarbanes-Oxley, the Payment Card Industry Data Security Standard (PCI-DSS), Federal Information Security Management Act (FISMA), DoD Information Assurance Certification, Accreditation Process (DIACAP), HIPAA (The Health Insurance Portability and Accountability Act), ISO27002:2013 (Information security standard), and other requirements. If an outage occurs in the systems that support the business processes and workflows, the possibility of noncompliance and fines increases dramatically.

- *Truly distributed networks*—With the evolution of the mobile workforce, remote users can access networks from literally anywhere in the world. Organizations are challenged with managing not only their headquarters, but also scaling out to semi-trusted locations, such as branch offices and to even less-trusted networks for remote and mobile users. Each new network layer has unique connectivity challenges, adding more cost and complexity.
- *Demands for new technologies*—Today's organizations have deployed technologies, like voice over IP (VoIP) and video conferencing, as a way to gain operational efficiency and competitive advantage. Moving all communications to the data network sets challenges for scalability and service quality.
- *Virtualization risks*—A recent Forrester survey reported that approximately 15% of virtualization deployment projects have no interested in implementing virtualization-aware security technologies. Typically, the operations team will argue that nothing has really changed—they already have the skills and processes to secure workloads, operation systems, and the hardware underneath. While true, this argument ignores the security threats and potential downtime when there's an attack to the new layer of software in the form of a hypervisor and virtual machine in these virtual networks. Unfortunately, most products don't have built-in high availability to ensure that virtual networks never go down.

The result? IT leaders are struggling to maintain complex, redundant, and costly networks. Furthermore, they are seeking new ways to trim costs in equipment, communications, and resources and still ensure the highest levels of connectivity.

A Better Approach

What companies need today is network technology that features built-in network availability and scalability technology. Rather than add to network complexity by purchasing separate solutions to achieve this functionality, not to mention the added costs of managing them, source solutions that simplify network security while boosting overall performance.

When evaluating different options to optimize their networks and save costs, consider the following key points:

- *Built-in versus bolt-on functionality*—Taking a close look at specific functionality and asking some basic questions will help uncover which solutions deliver the built-in functionality you need to ensure connectivity:
  - How is continuous uptime achieved? In most cases, you need to purchase another set of expensive redundant systems.
  - Does the solution offer instantaneous, transparent failover, or is your network at risk of going down for hours?
  - Can the solution cluster up to 16 nodes so that you can easily scale and increase the performance of your network? Most products can only cluster up to two or four nodes.
  - Does the solution offer active-active load balancing? Most solutions only offer active/passive functionality, so you don't get the full benefits optimizing traffic to accommodate current and future network requirements.
- *Flexibility and scalability*—The ability to choose the technologies that fit your environment and budget and still ensure the highest level of connectivity and security is critically important. A few key questions to consider include:
  - Can your company leverage any variety of connections, from MPLS to broadband Internet, and have the confidence of continuous uptime?
  - Can your current technologies easily scale to accommodate growth, remote networking, and the latest technologies?
- *Manageability*—Efficiently managing all of the components impacting connectivity from a single console is a critical component to any organization's ability to ensure continuous connectivity. A few key questions to ask include:
  - Can you manage virtual, physical, and hybrid solutions from a single management console? This is key when it comes to detecting, addressing, and remediating security threats that may undermine network availability and performance.
  - Can your administrators efficiently manage your network across multiple systems? Most products barely provide visibility into networks, let alone the tools administrators need to easily manage both physical and/or virtual environments.
  - Can deployments be done with minimal or no interruptions? In most cases, architecture and configuration changes must be done off-hours to minimize the impact on operations.

Conclusion

Network complexity has clearly made network costs and security a significant concern, especially as businesses recover from recent economic instability. However, as companies try to reduce network costs and boost security, they must put equal focus on network availability and scalability. A down network could very well be the costliest threat to your business.

McAfee Next Generation Firewall Availability and Scalability

McAfee maintains a rich history in integrating high availability and scalability functionality into its network security solutions. In fact, it's a fundamental part of what sets McAfee® network security solutions apart from others. McAfee Next Generation Firewall uses a unique built-in approach to optimizing network availability, scalability, and costs. Patented high availability technologies are built into all McAfee solutions, eliminating the need to purchase additional bolt-on solutions.

The elimination of additional network purchases isn't the only efficiency achieved through the unique McAfee approach. Our one-of-a-kind technologies and clustering mechanisms translate into zero downtime for today's networks. In other words, the network never fails on the McAfee watch—and there is never a need to take the system down for maintenance.

Through higher productivity, simplified management, and reduced costs, McAfee is transforming the way organizations secure their networks. McAfee Next Generation Firewall virtual and physical solutions include the following built-in technologies, each of which are redefining the standard for high availability and scalability:

- *McAfee Multi-Link™ technology*—Our technology eliminates network links as single points of failure and can provide seamless VPN failover across multiple circuits.

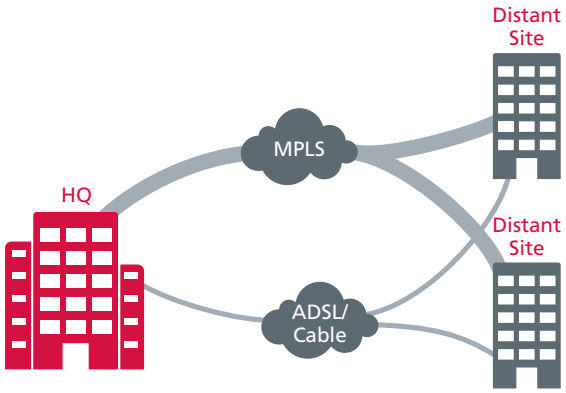

Figure 1. Removing the single point of failure in network connectivity with McAfee Multi-Link.

Regardless of the type of connections needed—DSL, leased lines, MPLS, mobile broadband, and even satellite—McAfee Multi-Link can load balance an unlimited number of circuits through a single appliance to ensure high availability, superior active/active performance, and optimization for VoIP and other emerging technologies. When multiple circuits are required for redundancy, McAfee Multi-Link also eliminates the cost and administration of BGP routers.

- *Clustering*—Ensures that systems protecting internal systems never go down. With the unique ability to cluster McAfee Next Generation Firewalls in a serial or parallel configuration, organizations can be assured that if one should fail, the other firewall in the configuration will automatically take over and monitor the traffic to keep the information flowing securely. With each McAfee Next Generation Firewall added to the cluster, inspection throughput performance increases significantly to ensure scalability for expanding organization
- *Drop-in active clustering*—Enables the unique clustering of up to 16 devices so organizations are assured the highest availability and scalability from the core to the edge of their networks without the need for expensive standby systems. With drop-in technology, clusters can be easily added into existing infrastructures without complex configuration requirements. When a three-node cluster is configured with a McAfee Multi-Link dual circuit, a five nines nearly fault-tolerant network can be achieved.
- *Dynamic server load balancing*—Distributes traffic between servers to balance the load efficiently and ensure that services are available when needed. User connections can be intelligently redistributed across server pools based on server availability. When configured with a two-node or three-node firewall cluster, maintenance can be done as needed during business hours with no downtime.
- *McAfee Security Management Center high availability*—Enables up to four standby management centers and real-time replication of repository data in the event of downtime, so network monitoring never stops.
- *VPN gateway redundancy*—Provides clustering of multiple links to ensure IPsec VPN connections are continuously available.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

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

[1] Young, Pescatore and Greg, John, August 12, 2008, *Q&A: Is It More Secure to Use Firewalls from Two Different Vendors*, G00146091, Inclusive—3. Retrieved August 12, 2008, from Gartner.

60962wp_ngfw-availability-scalability_0214_fnl_ETMG