



The Key to Uninterrupted Business: Multi-Layered Gateway Security

The Key to Uninterrupted Business: Multi-Layered Gateway Security

Contents

Executive summary	2
Challenges to ensuring uninterrupted business	2
The solution: comprehensive gateway security	3
Requirements for an effective gateway solution	4
Easy to manage	4
Multi-function	5
Effective network security	5
Proactive prevention	6
Best-in-class technologies	6
Protection against complex blended threats	6
Symantec™ Gateway Security 5600 Series: easy-to-manage, multi-function security appliances	7
Meeting requirements of strategic IT (CIO, VP, or Director of IT)	7
Meeting requirements of IT/network administrators and managers	7
Meeting requirements of the CEO and CFO	8
Only from Symantec – a trusted security partner	9

The Key to Uninterrupted Business: Multi-Layered Gateway Security

Executive summary

Faced with growing pressures to protect critical network environments and information and a growing number of remote user machines from increasingly complex threats, many small and midsize organizations have deployed firewall products in conjunction with antivirus software. Unfortunately, this approach does not provide adequate protection against blended threats such as Nimda, MyDoom, Klez, and Blaster that combine the characteristics of viruses, worms, Trojan Horses, and malicious code to propagate using multiple methods and to exploit application and network vulnerabilities.

Protecting networks from such threats requires a multi-layered approach to security at the network gateway, but many small and midsize organizations have been hesitant to deploy multiple layers of security due to concerns about procurement and management costs, complexity, and ongoing management requirements.

This paper describes the challenges that businesses face in ensuring uninterrupted business, why enterprises of all sizes need a multi-layered approach to security at the network gateway, and what to look for in a network gateway security solution. Finally the paper presents the Symantec Gateway Security 5600 Series—easy-to-manage, affordable, multi-function network security appliances from Symantec, the leader in Internet security.

Challenges to ensuring uninterrupted business

To ensure a competitive advantage, today's small and medium-sized businesses seek to control costs and realize process efficiencies throughout the organization. In order to accomplish this, they must provide employees, customers, partners, and contractors with unrestricted and reliable access to the corporate network and applications, no matter where these people are located. However, this open access adds another layer of complexity in securing the corporate network, as organizations are challenged to ensure that all users' actions are compliant with the organization's security policies. Non-compliance with policies increases the likelihood of vulnerabilities, and a successful attack that leverages these vulnerabilities could result in interrupted operations and a costly clean up.

Organizations find that to enable such openness, they need to invest in solutions that defend their network from a variety of security threats, including mischievous hackers and malicious email attachments, as well as blended threats and Zero Day attacks. Blended threats—such as MyDoom, SQL Slammer—combine the characteristics of viruses, worms, Trojan Horses, and malicious code to propagate via multiple methods and exploit known vulnerabilities. Such threats can disable the network and interrupt business, compromise business integrity,

The Key to Uninterrupted Business: Multi-Layered Gateway Security

and potentially lead to violations of laws and regulations, such as the Sarbanes-Oxley Act, and HIPAA, for example.

IT executives and administrators are challenged to address these issues while supporting a dynamic business environment – keeping up with the demands of the business is complicated by the need to simultaneously address security threats on an ongoing basis and in a proactive manner. Realizing that a firewall or antivirus product alone cannot protect against blended threats, many organizations try to piece together point products that address individual security functions, such as antivirus, firewall, antispam, and intrusion detection and protection, to name a few.

But attempting to combat today's threats with a multitude of individual, single-purpose products can be cost-prohibitive and difficult to deploy, update, and manage. In the end, these security products often go underutilized and poorly managed, which can result in security breaches. At the same time, the lack of integration between the various products can inadvertently create new security holes; products that are poorly integrated are inadequate, potentially leaving security holes in a perimeter. The problems are compounded for large and growing enterprises with multiple gateways and remote sites for which IT staff must deploy each security product whenever there is an addition to the network, such as a new remote site. The fact is, most small and midsize businesses lack the time, resources, and budget to deploy and properly manage a non-integrated security solution—and without significant, ongoing monitoring and management of the various technologies, such organizations risk costly security breaches.

The solution: comprehensive gateway security

These issues have created the need for an affordable and easy-to-manage multi-function network security appliance. For small to midsize organizations, multi-function security gateways are the best way to ensure uninterrupted business while protecting against today's blended threats.

These appliances tightly integrate a firewall with multiple layers of security technologies, including firewall, antispam, antivirus, VPN, intrusion detection, intrusion prevention, content filtering, spyware and adware detection, IPSec, and SSL VPN technologies, resulting in an easy-to-manage, comprehensive security solution in a single device. In addition to reducing deployment and administrative costs, these appliances offer the following benefits:

- **Improved security effectiveness and lower risk:** By providing the security layers required to protect against blended threats and by making it easier for IT staff to properly manage and fully utilize the various security technologies, multi-function security appliances can offer the most effective security available. This type of solution is also more likely to prevent a compromise by unknown threats, thereby reducing the costs associated with cleanup.

The Key to Uninterrupted Business: Multi-Layered Gateway Security

- **Easier installation, management, and maintenance:** Multi-function security appliances simplify the process of security management because IT staff need to deploy and monitor only one product to see what is entering and leaving through the Internet gateway. Because fewer people need to be involved in security monitoring and management, IT staff can address more urgent or strategic activities.
- **Lower total cost of securing infrastructure:** Multi-function security appliances enable IT staff to purchase, deploy, and manage one product instead of eight or nine individual products, lowering the total cost of securing the network. Equally important, in the event of a problem, organizations only need to work with a single vendor to resolve the issue—a real time saver. In addition, this type of solution offers a less expensive high availability configuration. To achieve high availability with single or dual purpose systems would require purchasing up to six pairs (12) of systems; with integrated security solutions, only one pair is needed.

A comprehensive gateway security solution of this type offers the best way for small to midsize organizations to protect against blended threats and offers significant benefits for corporations and IT departments with limited IT security staff and budgets.

Requirements for an effective gateway solution

There are a number of multi-function security appliances available on the market, each with a unique set of characteristics and capabilities. Most attempt to integrate products from different vendors into a single device. As a result, response to threats is slow or non-existent. And the lack of tight integration between the components can negatively impact an organization's overall security posture. A preferred multi-function security appliance will address these issues, as well as offer the following characteristics and capabilities:

- Easy to manage
- Multi-function
- Effective network security
- Proactive prevention
- Best-in-class technologies
- Protection against complex blended threats

Easy to manage

Because today's busy security administrators can barely find the time to address all the tactical aspects of their job, organizations must provide them the tools to ease the management of security solutions. A preferred gateway security solution will offer improved visibility and control

The Key to Uninterrupted Business: Multi-Layered Gateway Security

through centralized management, alerting, logging, and graphical reporting. This will enable employees to view all activity and trends across all security technologies at a glance.

Every organization has its own unique requirements when it comes to protecting its assets and proprietary information. With this in mind, the ideal solution should be configurable to meet the organization's security needs, while providing the flexibility to adjust to the changing business environment as required.

Some products offering integrated security technologies are not optimized to act as a single, holistic solution. Unless all the security technologies work seamlessly together, the administrative burden will not be reduced, and the protection afforded will be less than optimal.

Multi-function

To proactively identify and block both known and unknown attacks (zero-day) and worms, a multi-function gateway must integrate intelligent, full inspection firewall capabilities with a minimum of antivirus software and an intrusion protection system (IPS). Ideally, the solution will also incorporate clientless and IPSec VPN (to support remote connections) and anti-spam, content filtering, and adware and spyware detection (to prevent unwanted content). The better content filtering alternatives will offer a combination of list-based filtering and heuristic-based filtering. All the security functions must work together and communicate with each other to provide the best possible perimeter protection against sophisticated, blended threats. This is only possible when the technologies are integrated at the lowest levels, and cannot be achieved when integrating separate distinct products, such as through a combination of original equipment manufacturer (OEM) arrangements.

Effective network security

An effective network security appliance must address all types of network security threats and requirements. A preferred gateway will include a firewall with robust security features for protection at different points within the network. In addition, it will offer networking support such as VLAN and VPN to enable a variety of connection requirements. In order to help address a common source of vulnerabilities and related compromises in company networks, the solution should include endpoint security features that ensure users are protected with active and up-to-date client security, such as antivirus.

To support a dynamic and growing business, the gateway should come with integrated high availability and load balancing that scales to thousands of nodes. And because each organization has its unique requirements, the appliance should offer flexible licensing and configuration

The Key to Uninterrupted Business: Multi-Layered Gateway Security

options so organizations can buy the functionality they want today for the number of network devices they need to protect. Solutions should not force customers to buy more than they need.

Proactive prevention

Gone are the days when organizations can afford to react to security threats—instead, organizations must be proactive by staying abreast of threats and thwart them before they infiltrate the network. If the appliance features intelligent coordination of layered technologies, it can provide proactive zero-day vulnerability prevention. The ideal gateway security solution should also deliver automatic security updates to ensure that businesses are protected 24x7. Ideally, a multi-function security appliance is also backed up with coordinated responses and global insight to help protect against the widest possible range of network-based threats. Organizations need the expertise of a global security response team with global monitoring capabilities in order to respond to and prevent new threats, as well as to obtain real-time product updates to limit the effect of threats.

Best-in-class technologies

Some multi-function appliances combine unproven technologies from a variety of vendors, but organizations should look for a combination of tightly integrated best-in-class technologies. These should include multiple antivirus technologies to provide both traditional, definition-based virus detection and heuristic detection for identifying new or unknown viruses. The appliance should also combine vulnerability and exploit signature-based intrusion detection capabilities to identify new and unknown threats and stop attacks before they enter the network.

Spam protection should not only defend against real-time spam attacks, but also proactively identify first-time spam, while preventing false positives. And the firewall should combine the features of all major types of firewalls - simple packet, stateful, application layer, and deep packet inspection—to ensure the greatest degree of protection available today.

Only with multiple best-in-class technologies tightly integrated to work together seamlessly will an appliance provide the most effective network security against today's complex threats.

Protection against complex blended threats

Today's organizations are faced with dynamic threats that pose serious damage to business operations. These threats are not only evolving rapidly, making it difficult to respond, but they are increasingly being introduced by employees using mobile devices. Organizations need a gateway security solution that prevents threats based on multiple, complex attack vectors, and that can halt the propagation of vulnerabilities introduced by onsite and mobile users.

The Key to Uninterrupted Business: Multi-Layered Gateway Security

Symantec™ Gateway Security 5600 Series: easy-to-manage, multi-function security appliances

The Symantec™ Gateway Security 5600 Series (SGS 5600 Series) – a third-generation family of integrated security appliances – addresses all of these requirements to deliver optimal security, adaptability, visibility, and control. As a highly-available Unified Threat Management solution, the appliance meets the requirements of both IT and business constituents, as explained below.

Meeting requirements of strategic IT (CIO, VP, or Director of IT)

To address the concerns of those responsible for the resiliency of an organization's network, the SGS 5600 Series ensures a continuous and available secure network infrastructure for mission-critical business communication. It does so by offering the highest level of blended threat protection through multi-function security technology from Symantec, the world leader in Internet security. And by limiting malicious code outbreaks from impacting network resources and preventing loss of confidential critical data, it also reduces the total cost of securing the network infrastructure. With fewer outbreaks and infiltrations to attend to, the organization spends less on response and cleanups. Furthermore, the solution helps address an organization's compliance pressures by securing the corporate network infrastructure and offering control over inbound and outbound traffic.

Meeting requirements of IT/network administrators and managers

IT and Network administrators and managers can rest assured that the SGS 5600 Series provides proactive blended threat protection to keep the network up and running. In addition, the appliance helps organizations secure the network with ease by reducing the overhead required to install, manage, and maintain network security solutions, providing an easy-to-install appliance, centralized global management, and automatic and timely security updates using Symantec LiveUpdate.

Updates for virus definitions, IPS/IDS signatures, and URL lists for content filtering and antispam components are automatically downloaded and installed via LiveUpdate. These updates are provided by Symantec's industry-leading Global Security Response and DeepSight teams, which continuously monitor global network sensors around the clock, identify unusual activity, determine threat levels, and issue warnings and product updates as proactive measures against new threats.

Because the appliance combines all critical security functions and reduces the number of security devices needing to be managed or monitored, it alleviates the burden of network security administration. Network administrators can view logs, receive alerts, and correlate

The Key to Uninterrupted Business: Multi-Layered Gateway Security

security data from one management interface to gain a complete and real-time picture of network activity. All security technologies included in the appliance can be managed through a single console, resulting in increased administrator productivity, visibility, and control; simplified network security management; reduced remediation costs; and more efficient use of the various security technologies. Administrators can even configure different administrative roles with different levels of access and control.

Meeting Requirements of the CEO and CFO

With the most comprehensive solution from the world's leading security vendor in place, executive management can be confident of a continuous and available network infrastructure for mission-critical business communication. The combination of security and networking technologies provides the comprehensive and practical protection needed to effectively manage the widest possible range of network-based threats from a single device. And because all of these components are Symantec technologies, they are tightly integrated, providing organizations with maximum security effectiveness, while reducing the costs associated with acquiring and installing security products.

Just as importantly, this appliance provides the lowest total cost of ownership by proactively preventing business-crippling threats and malicious attacks, saving organizations from expensive downtime, costly cleanup efforts, and potential regulatory violations.

The Key to Uninterrupted Business: Multi-Layered Gateway Security

Only from Symantec – a trusted security partner

The Symantec Gateway Security 5600 Series is the industry's only third-generation integrated security appliance, offering proven, multi-layered network security in one, centrally managed appliance. It provides comprehensive protection unlike any other appliance available on the market and eases the deployment of multiple security technologies—all of which have been developed and integrated by Symantec, the world leader in Internet security. As a result, enterprises have a single source of support and accountability, further simplifying security management for today's small and midsize businesses.

By effectively securing the network and gateway infrastructure, the Symantec Gateway Security 5600 Series appliances help keep businesses up, running, and growing, no matter what happens. This gateway solution supports efforts to prevent and block blended threats at network layers, and leverages the Symantec Security Response infrastructure to ensure the latest threats are blocked and neutralized. With preventive technologies such as Intrusion Prevention with advanced Protocol Anomaly Detection, Full Application Inspection firewall, gateway antivirus, and content filtering, the appliances provide resiliency to the gateway and network infrastructure. In addition to multiple security functions, the appliance has available built-in high availability and load balancing features to prevent network downtime.

Symantec provides enterprise leadership with trustworthy technologies that integrate effectively and add greater stability to the overall environment. With multi-function network security solutions, Symantec helps organizations gain control of their network infrastructure, while helping reduce the overall total cost of ownership and infrastructure expenses associated with securing the network.

About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions.

Headquartered in Cupertino, California, Symantec has operations in 35 countries.

More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com

Symantec, the Symantec logo and pcAnywhere are registered trademarks of Symantec Corporation and/or its subsidiaries in the US and elsewhere. Windows, Active Directory and Microsoft are registered trademarks of Microsoft Corporation in the US and elsewhere. All other brands and products are trademarks of their respective holder/s. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. Copyright © 2005 Symantec Corporation. All rights reserved.
09/05 10479584