



Securing the Simple Small Business Network

INSIDE

- > The network security challenge
- > Meeting the security challenge
- > Simplifying for small business: integrated, easy-to-use solutions
- > The preferred solution

Contents

Abstract	3
The network security challenge	3
Meeting the security challenge	4
Simplifying for the small business: integrated, easy-to-use solutions	5
The preferred solution	6
Enabling technologies	6
Key benefits	7
Key software features	7
Key hardware features	9
Conclusion	9

> **Abstract**

Like their larger counterparts, small businesses need to protect their internal networks from Internet threats. However, most small businesses have a simple network architecture, and ordinary corporate security solutions are more than they need. Of course, they'd like the high-quality protection big companies receive, but because it's expensive to buy and manage separate firewalls, routers, and antivirus products, they'd prefer a simpler, integrated solution. Small businesses also need a solution that's easy to deploy and manage, and they don't want the complications of working with multiple vendors.

As a result, many small businesses settle for small consumer firewall devices. These entry-level products provide some rudimentary protection, but not enough to fully defend their information assets. Fortunately, there are now security products designed specifically for small businesses with simple network needs. The best of these products combine the following features:

- A multi-function, integrated security gateway
- An Internet-sharing LAN switch with multiple 10/100 Ethernet ports
- A secure wireless LAN access point
- Reliability features including Internet connection redundancy and WAN failover
- Bandwidth aggregation and load balancing for higher Internet throughput
- Automated policy enforcement for other security products the business may already own
- Automated device updates
- All of the above in an affordable device that's easy to install, deploy, manage, and troubleshoot

Network security appliances combining all these features are becoming the small business security solution of choice.

> **The network security challenge**

One of the largest concerns with the evolution and continual expansion of the Internet is network security. Of course, preventing and stopping "hacker" attacks is a key part of the network security challenge. However, the challenge extends far beyond hacker defense. It also encompasses denial of service attacks, viruses, blended threats, and physical network protection. Another aspect of the challenge lies within the ever-evolving nature of Internet threats themselves. Because the technical details of most threats cannot be fully known in advance, security solutions must employ fast and reliable update technology to keep their threat detection capabilities up to date. Finally, having the intelligence or capabilities to detect a threat is only part of the equation. Stopping threats once they're identified is a completely different exercise all together. It quickly becomes evident that the network security challenge is wide-ranging, dealing with various threats on multiple levels and demanding an equally wide range of security measures in response.

> Meeting the security challenge

To meet the network security challenge, businesses typically employ multiple network hardware devices, including firewalls, hubs, routers, switches, repeaters, remote access services, and wireless access points (WAPs). Most business networks are rather complex, and they need all these devices to ensure proper routing and to provide fast and reliable network performance. On top of this, multiple software solutions—such as antivirus protection, intrusion detection (IDS), intrusion prevention (IPS), VPN concentrators, and content filtering (i.e., URL blocking)—ordinarily round out a network security solution.

Firewalls or security gateways provide network protection on several levels. The initial level of protection is a threshold point-of-entry test. When someone attempts to access a network with a firewall in place, the firewall asks this question: “Does the company’s security policy allow this type of traffic to traverse the gateway, enter the network, and communicate with protected machines?” If the answer is “Yes!” the traffic may pass through. While this gives access to desirable traffic, it also means a hidden threat could infect the network.

That’s where other network security technologies, like IDS, IPS, and antivirus software, come into play. These technologies help detect threats and prevent them from entering a network and causing havoc. IDS solutions detect the identity of a threat itself. Much like identifying an individual’s signature, IDS scans network packets for the “signatures” of known Internet threats. If it appears to be a threat, they block the threat and log an alert. To secure the private network one level further, businesses commonly deploy antivirus tools. Antivirus software protects against network viruses, worms, Trojan horses, and other threats. Some of these threats spread via email attachments or network file sharing, while others are hybrids, or blended threats, that use multiple methods of infiltration, proliferation, and destruction. The better these security layers work together, the stronger the overall network security. Therefore, interoperability among IDS, IPS, and client-level antivirus software is a valued aspect of an effective network security architecture.

Apart from threat protection, businesses also need to be sure their Internet connections are always up and running. Internet connection redundancy provides continuous connectivity in the event of a network outage or ISP hiccup. In business, time is paramount, and with Internet redundancy in place, businesses can be certain their invoices will be transferred successfully and on time, that Web servers will receive and process transactions without interruption, and that important emails will be sent and received without delay.

Virtual private networks (VPNs) have also become a core part of most network security plans. As more and more employees connect to business networks from home and the road, the need for secure remote network connections becomes increasingly important. With a VPN client, remote users can use public Internet connections (like a home office DSL line) to establish secure tunnels with corporate networks. VPN solutions use authentication and access control to secure these tunnels, and those with IPsec capabilities enable data encryption and verification as well.

Finally, more and more businesses are clamoring for a secure wireless solution. Many laptop devices now include wireless LAN (WLAN) transceivers at no extra charge. Most businesses are

eager to use these wireless capabilities, but they're afraid of the security risks inherent in the technology. Therefore, ensuring data integrity and data confidentiality over a wireless connection has become a much desired, but often elusive security concern. Businesses that find a way to meet their wireless security concerns, to keep wireless connections in conformance with their IT security policies, will be free to take advantage of all the conveniences and cost savings WLANs offer.

Wireless security, VPNs, Internet connection redundancy, antivirus software, IDS, IPS, firewalls, and multiple network devices: it's a daunting and confusing list for small business owners with a simple network and few resources. But, there is an alternative.

> **Simplifying for the small business: integrated, easy-to-use solutions**

The conventional approach to network security is quite complicated, often involving numerous technologies, devices, and vendors. Unfortunately, that approach isn't workable for most small businesses. Multiple hardware devices and software tools consume many man-hours of work, requiring a complex security infrastructure and multiple administrative positions. These are costs small businesses don't have the resources to bear.

In an ideal world, small businesses would have around-the-clock network security support from an experienced, fully-staffed IT team. In reality, small business owners face 24/7 confusion and worry about their networks. Confronted with the same threats as large enterprises, many small business owners are the IT team and shoulder the full burden of protecting their proprietary information and customer data. That sets up a special challenge for small business network security. Fortunately, there's an answer to that challenge: To protect the simple small business network, security providers must combine multiple network security technologies in one affordable, easy-to-use solution.

The first step is integration. Combining firewall security, Internet redundancy, secure wireless connectivity, secure VPN, IDS, IPS, and antivirus protection in one solution not only lowers purchase costs, but it eliminates the long-term expense of maintaining an overcomplicated, multiple-device solution. But integration alone isn't enough. Hand-in-hand with integration, comes interoperability. Each integrated component must work seamlessly with the others. Moreover, to be deployed successfully, it is essential that network security appliances work flawlessly with market-leading routers and other third-party security technologies. Without interoperability, securing any size business is not manageable or cost effective.

This integrated, interoperable solution must also be easy to install, manage, and maintain. Intuitive installation wizards and management interfaces go a long way toward reducing the complexity of network security management. In fact, for an integrated, multi-feature solution, an easy-to-use interface is essential. If small businesses aren't comfortable with their security management interface, they won't be comfortable with the security itself.

While small businesses need a simpler, consolidated solution, they don't want to sacrifice performance. Network performance (and the cost of performance) is a priority for the small business. They

need an appliance that offers performance-enhancement features like high-speed processing and VPN encryption acceleration, both of which facilitate faster throughput for more users. Conversely, they don't want a security solution that's going to slow down their network and frustrate employees.

Here's the bottom line. Most small businesses have simple networks but complex security needs; they have serious performance requirements but limited resources. So, small businesses need a solution that minimizes costs but maximizes protection and performance. In other words, they need an affordable, low-maintenance appliance that combines robust performance with a comprehensive set of security features.

> **The preferred solution**

Designed especially for the small business, the Symantec™ Gateway Security 300 Series appliance is an easy-to-use, integrated network security solution. It provides stateful firewall inspection, plus five other multi-level security functions: IPsec VPN, intrusion detection, intrusion prevention, content filtering (i.e., URL blocking) and antivirus policy enforcement capabilities. In addition, the 300 Series offers fast, reliable network performance, ensuring continuous network connectivity and maximizing throughput for high-speed wired, wireless, and VPN-secured access points. A multi-function network security solution that's also low cost and easy to use, it will meet and exceed the demands of the average small business. The Symantec Gateway Security 300 Series appliance is the premier integrated security appliance for small businesses.

ENABLING TECHNOLOGIES

Symantec Gateway Security 300 Series appliances are designed for small businesses, yet they offer the power and advanced features found in enterprise-class security gateways. Their functions are tightly integrated for cooperative protection, and they require little additional licensing. Working together, the following technologies enable the appliance to meet the small business network security challenge:

- Integrated firewall, IPsec VPN, antivirus policy enforcement, intrusion detection, intrusion prevention, and content filtering technologies. All these security features are consolidated into one solution—a solution supported by a single security partner.
- A convenient Web-based management interface makes it easy to manage this multi-function security appliance either locally or remotely. It facilitates faster deployment, faster configuration, and hassle-free, enterprise-class administration, thus reducing management and maintenance costs.
- The appliance's antivirus policy enforcement feature automatically ensures that most Symantec AntiVirus clients accessing the gateway meet minimum security policies.
- All Symantec Gateway Security 300 Series models have secure wireless capability. They include a special wireless option slot that accepts the Symantec Gateway Security 802.11b/g WLAN Access Point Add-On. The WLAN upgrade is an integrated 802.11/b/g transceiver and antenna that activates wireless access point firmware upon installation and facilitates connectivity for other wireless-enabled devices. When used with wireless clients running Symantec Client VPN software, it also supports Symantec's integrated security for wireless LANs. To provide wider signal coverage, small businesses can deploy multiple 300 Series wireless access points, and a

roaming feature lets users move about with uninterrupted connectivity.

- Symantec's LiveUpdate™ technology, which is built into each 300 Series model, automatically keeps the appliance firmware current.

KEY BENEFITS

- Control all security issues from a single device located at the perimeter of the small business network.
- Stop intrusion attempts before they enter the network.
- Allow teleworkers, guests, and traveling employees to securely access the business LAN/WAN.
- Increase Internet throughput speeds and keep Internet connections up and running with dual WAN ports on select models.
- Minimize the cost of additional hubs with dual LAN ports on select models.
- Use low-cost broadband solutions (DSL, Cable) instead of costly T1 connections and still maintain full redundancy and load balancing.
- Allow clients to connect using a secure wireless VPN when onsite and a secure remote VPN connection from home—without buying additional licenses.
- Get up and running quickly and easily with a Web-based Setup wizard.

KEY SOFTWARE FEATURES

- **Less complex security functions and management** – Many vendors accommodate the small business market by repackaging the management interface of their high-end enterprise units in a low-performance appliance. These interfaces are designed for use by security engineers who understand specialized terminology, options, and parameter settings. Unfortunately, small businesses neither need, nor are they equipped to understand, these complex interfaces. That's why the Symantec 300 Series appliance offers only those functions that fit typical small business needs and that provide maximum protection by default.
- **Easy setup** – The startup wizard facilitates quick Internet connectivity for four common ISP connection types. To get connected, small businesses don't have to do much more than plug in the unit and run the wizard.
- **Broad local language support** – The administrator interface comes in any one of ten languages (released over time), including four double-byte languages: Japanese, Traditional Chinese, Simplified Chinese, and Korean. User interfaces, messages, and dialogs are fully localized, giving small business administrators the option to operate the appliance in the language they find most comfortable.
- **Simplified troubleshooting** – Troubleshooting tools—used with the guidance of Symantec Technical Support—facilitate quick diagnosis of common network connectivity problems.

KEY HARDWARE FEATURES

- **High performance network functionality** – The appliance’s processor, switch chips, bus architecture, and memory provide enterprise-class performance that more than fulfills the needs of most small businesses.
- **Reliability**– The 300 Series was designed as an embedded system with all operating firmware included in the hardware’s chipset and no moving parts or fans. This eliminates the cost, complexity, failure rates, and thermal challenges of having rotating media on the device. As a result, all 300 Series models have Mean Time Between Failure rates in excess of 800,000 hours. That means small businesses won’t have to by a backup unit.
- **High Availability** – Every 300 Series model has built-in Internet connection redundancy. The appliance uses multiple techniques for WAN port failure detection and automatic failover to a backup connection. This feature protects against the most two prevalent network failures encountered by the small business: network congestion and WAN link failure.
- **Wireless LAN option slot** – The 300 Series is the ONLY entry-level security appliance to include an optional VPN-secured high-speed wireless LAN access point on all models. This feature offers the easy connectivity of a 802.11g/b WLAN without the security risks that have deterred many small businesses from using wireless connections.
- **Ergonomic design** – The 300 Series is simple to install and can be placed on any flat surface. All WAN, LAN, serial, and power connections are on the back of the appliance, while status LEDs on the front panel make monitoring easy.
- **Model 320**
 - Designed for small to medium businesses with at least one broadband Internet connection, this appliance includes:
 - Firewall
 - Antivirus policy enforcement
 - Intrusion detection
 - Intrusion prevention
 - IPsec VPN and enterprise-class performance
 - Content filtering
 - LiveUpdate
 - Internet sharing
- **Model 360/360R**
 - Designed for growing businesses who need to support more users and faster throughput, this appliance includes:
 - All the Model 320 features
 - Supports two high-speed WAN connections for failover and redundancy
 - Bandwidth aggregation and load balancing of two Internet connections for up to double the Internet throughput

> Conclusion

Securing the small business network can be a daunting task. However, the Symantec Gateway Security 300 Series provides the tools to meet that challenge. Here are three excellent reasons small business owners should purchase a 300 Series appliance today:

3. **Upgrade to integrated security without the complexity of a full-scale enterprise solution.** Although many small businesses already have a firewall/VPN device, it may be a consumer-grade unit that doesn't give them the protection they need. Viruses or other types of attacks may still cause significant disruptions to their network and Internet access:

The Symantec Gateway Security 300 Series is neither too simple nor too complex for the small business. It is the premier entry-level business security appliance with six integrated security functions: Firewall, IPsec VPN, antivirus policy enforcement, IDS, IPS, and content filtering. These functions were designed specifically for the small office environment, thus minimizing the unnecessary complexity of most "small business" appliances—appliances that are really just repackaged high-end solutions.

2. **Maximize your client antivirus software investment.** Small businesses know that viruses can enter their network in many ways, and therefore, they may have invested in client antivirus software for their users. However, viruses may still cause them significant problems because users either disable or don't update their antivirus clients. The Symantec Gateway Security 300 Series specifically addresses this problem. By integrating antivirus policy enforcement into the base appliance, it automates the tedious tasks of distributing updates as new virus definitions are available and keeping users' antivirus tools running at peak efficiency.
3. **Reduce management overhead and cost.** Even the smallest office may need multiple network functions, including Internet security, Ethernet LAN switching, routing, and wireless LAN connectivity. The Symantec Gateway Security 300 Series minimizes confusion and cost because it combines the following devices in one solution:
 - Integrated, six function, Internet security gateway
 - Internet-sharing, multi-port 10/100 LAN switch with routing functions
 - Secure wireless LAN access point add-on option
 - VPN gateway for remote users

If it's your task to protect a small business network against Internet attacks, don't spend another day struggling with an overcomplicated or underpowered solution. Get a Symantec Gateway Security 300 Series appliance today. It's the high-performance, integrated solution for the simple small business network.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF CLIENT, GATEWAY AND SERVER SECURITY SOLUTIONS FOR VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

**SYMANTEC CORPORATION
WORLD HEADQUARTERS**

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.**

**800 441 7234
408 517 8000**

www.symantec.com

**For Product Information
In the U.S., call toll-free
800 745 6054**

**Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers,
please visit our Web site.**