Secure Wireless Networking for Small Business

INSIDE

> Abstract
> Introduction
> History of Wireless Security
> Importance of Two-way Authentication
> Symantec's Solution for Wireless Security
> Wireless LAN Security Recommendations
Contents

Abstract .............................................................. 3
Introduction .......................................................... 3
History of Wireless Security ........................................ 4
Importance of Two-way Authentication .......................... 6
Symantec’s Solution for Wireless Security ....................... 8
  Isolating wireless networks ................................... 10
  Securing a single-access point wireless network .......... 10
  Securing a multiple access point wireless network ..... 12
Wireless LAN Security Recommendations .................... 15
Abstract

This paper explains the wireless security problem and offers a viable solution to secure a business wireless network with a product that:

- Allows companies to avoid the wireless security “standards” bandwagon that even industry experts find hard to follow.
- Extends to wireless networks a field-tested, high-grade security technology that's already used widely for ensuring data confidentiality and integrity on wired Internet connections.
- Protects your investment by ensuring compatibility with existing and future technologies. Because this solution is not tied to specific wireless standards, there will be no need for new hardware or software when new standards emerge.

Introduction

Wireless networking offers clear benefits for businesses large and small. It saves time and money when deploying a local area network by eliminating wires, plugs, switches, and construction (such as drilling holes in walls). It also liberates your work force by allowing them to go mobile even within an office building, doing away with “plugging in” for meetings and presentations. Workers are free to group together wherever they need to accomplish tasks efficiently, without worrying about network connectivity.

Industries such as healthcare have mobile tasks that are tailor-made for wireless technology. Medical staff can use wireless handheld devices to send patient information to the main database from anywhere in a hospital, enabling them to update the information wherever the patient goes and eliminating handwritten charts. Another popular wireless application, the “hotspot” (wireless access point), offers Internet access in public locations for users on the go. It's hard to find a major airport without a hotspot these days.

For the typical business, wireless networking promises more than just cost savings. The same employees that would be using wireless at work are deploying wireless at their homes in record numbers. Two years ago, the sales of wireless residential Internet appliances exploded in comparison to sales of wired appliances, and the numbers have only grown in favor of wireless. So the general public has a growing familiarity with wireless and likes using the technology. This dovetails into the increase in teleworkers and the mobile workforce to make wireless very attractive as a networking technology for businesses.

Wireless networking does, however, have unique security issues. The same technology that frees workers from having to be plugged into the network also creates the possibility of accidental or intentional intrusions into your business network.
History of Wireless Security

Back in 1999, wireless networking started its growth with the publication by the IEEE (Institute of Electrical and Electronics Engineers) of the first commercially viable wireless standards, 802.11b and 802.11a. It wasn’t long before 802.11b products started appearing on retail shelves. (802.11a was delayed because of its complexity to implement.) Another organization, the Wi-Fi (Wireless Fidelity) Alliance, emerged as the guarantor of wireless compatibility among products using the 802.11 standards. The new higher-speed 802.11g standard was released in 2003 by the IEEE, completing the trio of common wireless networking protocols supported by vendor access points (APs) today.

However, the explosive growth in wireless networking has been tempered—especially in large organizations—by widely known problems with security. Indeed, wireless deployments have yet to flourish in business because of security fears. Those deployments that have been implemented are not always sanctioned; they may instead consist of an employee plugging an unapproved AP onto the network for greater networking convenience.

It’s not hard to comprehend the fears of network administrators when you examine the nature of wireless operations and the history of wireless security. With wireless networking, everything you send and receive is broadcast over the air and can be received by every wireless receiver within range. Wireless signals can travel through walls, and the range of even the most inexpensive APs has improved greatly as wireless technology has evolved. As a result, parking outside an office building with a wireless-enabled portable computer can yield quite a bit of data without anyone being aware of the network penetration. Of course, this type of vulnerability was accounted for when the first commercial wireless networking standards were published. Unfortunately, it wasn’t accounted for effectively.

The initial security standard for wireless dates back to a 1997 publication by the IEEE called Wired Equivalent Privacy (WEP). WEP’s intention was to prevent unauthorized users from reading wireless data packets between the client and the AP by encrypting the traffic. WEP was not meant as a complete security protocol, and the first weakness in WEP can be observed in its design: It does not contain a method for user authentication. WEP keys are commonly shared among all wireless users accessing the network. So both John Doe and Sue Smith can connect wirelessly, and because both share the same WEP key, the administrator has no method of knowing who’s connected. If Sue Smith is fired, the WEP keys must be immediately changed for all of the APs in the office. WEP is therefore not an easily scalable or maintainable security policy.

But WEP’s main problem is that it turned out to be much weaker than expected in doing its primary job of encrypting data. Readers of this document are likely already aware of the media coverage surrounding WEP’s encryption weaknesses. The initial vulnerabilities were first published in March 2000, and larger holes were found in October of the same year. Easy-to-use hacker tools such as AirSnort and WEPCrack were quickly developed. These tools enable anyone with a laptop to capture wireless transmissions, then later break the WEP encryption and decode the data from the transmissions.
WEP’s weaknesses stem from the algorithms it uses to encrypt packets. It also has minimal data integrity (a simple CRC algorithm). So a hacker can modify the decrypted packets, change information in them, then re-encrypt them and forward the data without the network administrator ever knowing about the interception. A frightening example of this lack of guaranteed integrity is that of a hacker intercepting and changing a $100 transaction to $10,000 on the fly. Because of these problems, it became abundantly clear that, while better than no encryption, WEP was did not provide enough protection for businesses and could expose a company to legal liability issues and massive losses.

As a result of WEP’s weaknesses, standards bodies accelerated their plans for release of the next version of wireless security. In particular, the IEEE was working on a new suite of security standards for wireless called 802.11i. Because businesses were anxious to have more robust wireless security while 802.11i was still being drafted, a subset of the upcoming standard was created by the Wi-Fi Alliance as a stopgap solution. This encryption method, called Wi-Fi Protected Access (WPA), was to become the next standard for wireless security, representing a significant improvement over WEP.

WPA took the primary pieces of 802.11i and added a few features:

- Temporal Key Integrity Protocol (TKIP), a better method of encryption that uses constantly changing keys
- 802.1x, the standard for network port access
- Extensible Authentication Protocol (EAP) for secure user authentication
- Message integrity check (MIC), offering better data integrity to prevent modification of packets

WPA offers two operating modes: WPA-Personal and WPA-Enterprise. The Personal mode (intended for homes and small offices that don’t have network servers) uses only a pre-shared key (PSK) stored in the access point itself; there is no user authentication. The Enterprise mode adds user authentication (whose absence from WEP was a major drawback to that standard). In Enterprise mode, the AP off-loads the authentication to a company’s existing authentication server, such as a RADIUS server. Clients typically send a username and password to authenticate in this mode.

With WPA’s improved methods of encryption and data integrity, many vendors thought it had solved the wireless security issue and began implementing it in their new wireless devices. (Wireless equipment using older WEP-based hardware typically cannot perform WPA security and must either be upgraded to support WPA or replaced with WPA-compliant equipment.) But as we’ll see in the next section, WPA still contains at least one major vulnerability.

As for 802.11i, it’s currently past the draft stage and has been renamed WPA2. 802.11i now contains even more security features than originally planned, and there’s no guarantee that vendor equipment that supports WPA will support WPA2. One can see how all of this recent “standards” development turmoil would make any business nervous about investing in current wireless security technologies.
> **Importance of Two-way Authentication**

The main security problem with WPA (and its originating 802.11i standard) is its one-way authentication. In order to authenticate, a client has to send credentials that prove who they are. However, there’s no way of confirming that the entity to whom they’re sending their credentials is in fact the intended access point.

The weakness of one-way authentication lies at the core of how the IEEE 802.1x authentication standard works in WPA. 802.1x describes a framework for transmitting credentials and then, if the authentication has been successful, opening a path for network traffic to pass.

Here’s a typical scenario for connecting to a company’s wireless network using WPA in Enterprise Mode:

1. The wireless user sends his or her username and password to the local wireless access point (using the 802.1x framework).
2. The AP creates a temporary connection to the user, and at the same time, forwards the user’s credentials to the company’s RADIUS server.
3. The RADIUS server authenticates the user’s credentials and replies to the AP with a “match” or “no match” response. If the user’s credentials match the server’s list of authorized users, the temporary connection becomes an established data connection and network traffic can pass. If no match is found, the AP informs the user that the username and/or password is incorrect and closes the temporary connection.

Notice that at no time in this transaction is the access point required to prove that it’s the correct AP for the user to connect to.

Imagine a scenario in which a hacker parks a van outside of your office. He has brought along his own AP already configured with the name of your wireless network. (That name—known as the Extended Service Set ID or “ESSID”—is easily obtainable by monitoring your network’s traffic.) As far as your wireless clients are concerned, this rogue access point looks like one of your office APs. John Doe, your star employee with lots of important information on his laptop, forwards his credentials to the rogue AP, which authenticates him to start sending traffic. The hacker now has access to John’s laptop and all of his information (unless John is running a firewall program on the computer). He also has John’s wireless network authentication credentials.

The security concerns with one-way authentication should now be obvious, and they make this type of security unacceptable for business applications—especially considering federal regulations for guaranteeing the privacy of customer data. (Additional concerns with 802.1x are coming to light as well, although they are outside the scope of this document.) Vendors have taken notice of this vulnerability and are developing methods of overcoming the rogue access point problem. However, these countermeasures are proprietary to each vendor, are not always easy to deploy, can be costly, and may have their own vulnerabilities.

For wireless security to be effective, it needs mechanisms that provide the following capabilities:

- A way to authenticate both the user and the authenticator (the access point). Both parties have to know that the other entity is trusted and has the proper credentials. The method employed
for user authentication should be two-way and strong.

- Bulletproof data integrity to protect against someone modifying a data packet “in flight” and then resending it.
- Data encryption that is cost prohibitive to break.

A security solution that fulfills all of these needs would be perfect for wireless security—and such a solution is available today. It’s been the de facto enterprise network security standard for years, and has been adopted in growing numbers by smaller businesses to secure their networks.

This technology is IP security protocol virtual private networking (IPsec VPN), and it is very secure indeed. Unfortunately, it hasn’t been implemented widely for wireless yet, and the attempts that have been made so far have all had their drawbacks. There will be more discussion about those developments later in this paper.

First it’s important to understand that VPN technology encompasses a number of different security services. The particular VPN technology we’re focusing on is called an Internet Key Exchange (IKE) IPsec-based VPN, and it’s the most common and most secure commercial solution available. IKE IPsec is routinely used to provide secure communications for remote users who need to connect across the Internet back to their company’s internal network.

IKE is the part of an IPsec VPN that handles authentication. IKE IPsec is a mature security standard that implements two-way authentication for both users and network gateways. Its encryption standards for confidentiality and mechanisms for data integrity are considered virtually unbreakable when set to their strongest levels.

There are several methods to authenticate with IKE, one being a simplified type of user authentication that’s appropriate for small business implementations. This method uses a client ID (essentially a username) and a preshared key (PSK, which is like a password). Here’s an abbreviated explanation of how a user authenticates with IKE in this mode:

1. The user sends her client ID, then uses her PSK to create a strong encryption algorithm that’s applied to the outgoing authentication message.

2. In order to decrypt the authentication message, the access point must have a matching PSK for this user. User PSKs are only entered by network administrators into trusted APs.

3. After decrypting the message, the AP reads it and creates a reply. The AP then sends an encrypted reply to the user.

4. Upon receipt of the reply, the user decrypts it to make sure that she is communicating with a trusted access point. Only when this entire sequence has been completed is authentication successful.

Notice that at no time are the PSKs sent to the other party over the air (or wire), but both must have the same PSK to read each other’s messages, and both need to receive authenticated messages from the other party before further communication can take place.

Let’s see how the use of an IKE IPsec VPN would change our earlier data-theft scenario. The same hacker drives up in a van with a rogue AP. Employee Jane Jones—using VPN-based wireless security—sends her client ID, encrypts her authentication message with her PSK, and attempts to connect to the network. The rogue AP intercepts her message as before. However, without a matching PSK, the rogue AP cannot decrypt Jane’s message and thus cannot successfully reply to
prove that it is a trusted party. The hacker’s intrusion attempt is thwarted, and he drives away looking for someone using WPA instead.

IKE-based VPNS also offer a more traditional form of user authentication called Extended Authentication (xAuth) that is common in larger businesses. xAuth begins with the same client ID and PSK sequence. However, the resulting agreed-upon encryption is then used to start a new challenge/response sequence. This sequence is usually implemented via a central RADIUS server and requires usernames and passwords (not necessarily the same as the client ID and PSK) similar to the WPA example. But because the xAuth exchange is contained within the IKE authentication encryption, it is more secure than WPA.

Authentication is just one of the advantages of VPN security. Its data integrity and encryption are extremely high-grade as well. The standards that make up VPN are mature and have withstood crypto-analysts’ attempts to break them over the years. So, there’s little chance of someone in the middle modifying a packet of data or reading its contents without your knowledge.

Because of VPN’s advantages, methods of implementing VPN-like solutions for wireless security have started appearing from a few vendors. Sometimes they don’t refer to it as VPN, but give it a trademarked name. These solutions typically require proprietary equipment to be installed specifically for the wireless network or to authenticate remote users, and also require software specifically developed for wireless security. Unfortunately, this proprietary equipment or software doesn’t perform other tasks needed for a small business network, so customers must buy additional equipment and integrate all the pieces themselves. And because of the proprietary nature of these products, there’s no guarantee of interoperability with other VPN equipment and standards. Finally, these solutions are usually not inexpensive.

But, as always, there is a better mousetrap on the horizon. As you’ll see in the following section, Symantec has greatly simplified the implementation of VPN for all network security uses and incorporated it seamlessly into wireless networks. Plus, Symantec’s product isn’t a “wireless-only” security solution; it’s part of an integrated, multilayered security solution that contains all the features a small business needs to create a local or extended network and to keep it safe. And, the best part: this solution is affordable.

> **Symantec’s Solution for Wireless Security**

Symantec has years of experience in providing security solutions for both consumers and businesses. The previous sections of this paper expressed our analysis of the issues and alternatives for providing enterprise-class wireless security. The following sections discuss specific affordable wireless LAN security solutions that offer a coherent strategy and the best current technologies.

Symantec has a range of gateways that perform many functions for a network, including market-leading VPN technology. For the purpose of example in this document, we’ll use our new line of entry-level integrated security appliances, the Symantec™ Gateway Security 300 Series. These appliances are designed for small businesses. They offer comprehensive security, a reliable Internet gateway, and a secure wireless LAN option in one affordable, easy-to-configure solution. The security functions in 300 Series appliances include firewall protection, virtual private networking, intrusion detection, intrusion prevention, antivirus policy enforcement, and content filtering. The
antivirus policy enforcement feature ensures that clients connecting have active and updated firewalls and antivirus software. The optional Symantec™ Gateway Security 802.11b/g Wireless Access Point Add-On turns a 300 Series appliance into a wireless LAN access point that features highly secure IPSec VPN connections.

Figure 1. A Symantec Gateway Security 300 Series appliance (front and back)

The 300 Series appliances are complemented by Symantec™ Client VPN software. Symantec’s VPN client is special in that it contains another piece needed for a proper security policy: an integrated personal firewall. Also, it interoperates with Symantec VPN gateways to receive its configuration automatically. Typically, IT staff configures the VPN client, but auto-configuration simplifies setup and deployment greatly, especially if a user ever needs to re-install or configure the VPN client himself or herself.

Figure 2. Symantec Client VPN software
ISOLATING WIRELESS NETWORKS

The optimum solution to wireless security is founded on the nature of a wireless network. Because wireless data is transmitted through walls and buildings and one cannot be sure of its origin point, all of the wireless network must be treated as an “untrusted” network and segregated from the rest of your network—just like the segregation you undoubtedly have between your network and the Internet. The device implementing wireless security must be able to differentiate between trusted and untrusted networks and enforce that segregation. Once this basic rule is followed, a wireless security policy can be implemented that operates the same as security policies for remote users connecting through the Internet.

Any users crossing an untrusted network to get to an internal network must be using VPN client software on their computers (laptops, home office desktops, or branch office workstations). The VPN client takes care of authentication and encryption of traffic with the internal network gateway. User credentials are the same whether the employee is away from the office or using a wireless connection in a meeting room. All users have unique PSKs and client IDs configured in their client computers. The VPN client ensures that wherever a user may be, data is encrypted and protected as soon as it leaves the computer. VPN clients encrypt at the IP (data packet) level, and are therefore compatible with all of a business’s current and future applications.

SECURING A SINGLE-ACCESS POINT WIRELESS NETWORK

Our wireless security scenarios based on 300 Series appliances will start with a simple single-AP deployment (Figure 3).

![Image of a simple one-AP configuration](image-url)

Figure 3. A simple one-AP configuration

The VPN Secured Wireless feature of Symantec Gateway Security 300 Series appliances is very easy to configure indeed. By adding the integrated high-speed wireless access point option, you can deploy the appliance in a small location without the need for additional access points.

After the appliance is set up, the administrator activates VPN security for the wireless LAN (WLAN). Once configured, the wireless interface on the 300 Series disallows any traffic other than authenticated VPN users from entering your network. The wireless network is now being treated as an untrusted network.

Figure 4 shows an actual screenshot of the 300 Series configuration interface. In addition to
enforcing VPN, 300 Series appliances can be configured to perform intrusion detection and intrusion prevention on traffic entering from the WLAN. In addition, WEP is supported for compatibility with existing deployments that do not use VPN.

![Configuration settings](image)

Figure 4. Setting the WLAN to allow VPN connections only

The next step is to configure the client users on the appliance. This is where the same VPN simplification that is implemented in the Symantec Client VPN software can be seen in the 300 Series. There are a couple of steps to this part of the configuration (Figure 5).

![Client configuration](image)

Figure 5a. A username and PSK are entered for each user. Up to 50 users can be entered on-box, and unlimited users with Extended Authentication (xAuth) using a RADIUS server.
First, the administrator enters the client IDs and PSKs for all users that will be authenticating. Once all entries are made, a single click on “Enable Tunnels on the WLAN/LAN” is all that’s needed. The appliance now uses VPN defaults and will automatically configure users’ VPN settings once they connect. Note in Figure 5 that enabling WAN side tunnels requires only another click of the mouse. No other settings need to be configured for users working from home or traveling.

After those two simple steps, you now have a wireless network that’s more secure than any of the current typical deployments. Plus, it has the versatility of securing workers’ connections whether they’re in the office, at home, or traveling. The same user credentials are used, and security is implemented at the IP level in each user’s computer. That ensures safe communications whether they’re using a wireless hotspot at an international airport or working at their office desk. The 300 Series automatically detects whether a user is local or remote and configures Symantec Client VPN appropriately when the user authenticates. Protection is also improved because each user now has a personal firewall installed (as part of the Symantec Client VPN software).

Remember that an important part of this solution is that it uses VPN standards and so is interoperable with your company’s existing infrastructure. For example, the 300 Series contains a RADIUS client that can use any RADIUS or RADIUS-interoperable authentication server—such as Microsoft Windows Active Directories, RSA SecurID, Passgo Defender, and so on—to authenticate users.

SECURING A MULTIPLE ACCESS POINT WIRELESS NETWORK

Not all wireless networks contain a single access point. Multiple APs are common in larger offices to expand wireless coverage throughout the facility. The Symantec Gateway Security 300 Series can secure these deployments as well, enabling users to stay in contact while roaming around the building or campus.

Keeping to the philosophy that wireless networks should always remain untrusted, you can set any LAN port on a Series 300 appliance to require VPN authentication by users coming into that port from insecure access points, as shown in Figure 6. (A 300 Series appliance has four to eight LAN
To keep wireless access points separate from the main network, they must be wired on their own segregated subnetwork, then connected to the main network at the main gateway’s LAN port (in this case, a 300 Series appliance). There are a couple of ways to implement security in a roaming scenario. The first is using the 300 Series to convert an existing AP infrastructure to use VPN for its security.

In Figure 7, all of the wireless access points are typical low-feature APs. Just as in the single-AP scenario shown in Figure 3, WLAN users still authenticate and establish their client VPN tunnels back to the main 360 unit. But in this multi-AP scenario, the users are free to roam from AP to AP while their tunnel to the 360 LAN switch remains established. They can therefore work without the interruption of needing to re-authenticate every time they leave the range of one access point and start interacting with a different one.
Notice that the access points are all on the untrusted ports, separated from the trusted network by the main 360 switch. This approach has the benefit of enabling a business to drop a 300 Series unit into their existing wireless network. But this is not the most secure method of implementing a wireless network with VPN technology. The one issue with this topology is that because insecure APs are being used, wireless clients are vulnerable to peer-to-peer attacks. This vulnerability can be exploited by a rogue computer using one of the insecure access points to attack a wireless user directly. Because this attack occurs peer-to-peer across the insecure AP, the 300 Series’ intrusion detection, intrusion protection, and VPN protection are bypassed. (Note that this is where the personal firewall that comes integrated with the Symantec Client VPN software gives a good measure of protection. Personal firewalls are an important piece of a complete security policy, and should be deployed to all client computers.)

Peer-to-peer attacks may or may not be an acceptable risk depending upon a company’s security policy. If they aren’t acceptable to your organization, the following enhancement can help protect against them.

Figure 8 shows the recommended deployment topology for the most secure VPN wireless deployment—one that is not vulnerable to peer-to-peer attacks. In this topology, the wireless access points used for the roaming environment are all Symantec Gateway Security 300 Series appliances set to allow only VPN traffic on their wireless interfaces.
Figure 8. Topology of a VPN-secured WLAN with perimeter enforcement

In this configuration, VPN-secured wireless protection is extended to the network perimeter. Because VPN is being enforced at each access point in the roaming network, a rogue computer cannot access other wireless users without first authenticating with the main 360 unit, so peer-to-peer attacks are not possible. In this scenario, the main unit has its LAN ports set to SGS Access Point Secured mode (see Figure 6), allowing management and monitoring of the secondary 300 Series APs used by roaming users. Note that the VPN client tunnels are still terminating at the main 360 unit’s LAN switch, not at the roaming units. As before, this design enables a wireless user to roam freely from AP to AP while the client tunnel remains established at the main unit, but now with additional protection against peer-to-peer attacks. All Symantec Gateway Security 300 Series models can be wireless enabled and implemented as either main or secondary APs.

> **Wireless LAN Security Recommendations**

To summarize, Symantec recommends a pragmatic strategy for securing wireless networks: Use proven security technologies and techniques that are widely accepted for providing high-grade security, and follow the four steps listed below.

**STEP 1: SEGMENT YOUR WLAN**

Because wireless technology opens your internal network to additional threats, be sure to isolate wireless access points from your wired network. Separation and segmentation improve WLAN attack containment and minimize risk to your intranet.

**STEP 2: USE EXISTING VPN MECHANISMS**

As explained previously, use IKE-based IPsec virtual private networks. They have the most secure commercially available encryption technology to provide WLAN data confidentiality, data integrity, and user authentication.

**STEP 3: DEPLOY INTEGRATED GATEWAY SECURITY AT THE WLAN ACCESS POINT**

Because the best security posture is to treat your wireless network with the same distrust as you would the Internet, you should deploy gateway security mechanisms wherever wireless LANs connect to your internal network. The new comprehensive firewall appliances that have multiple integrated security functions and an integrated wireless access point offer the most effective and
efficient way of providing adequate protection. These devices provide maximum protection by integrating firewall, VPN, antivirus, intrusion detection, intrusion prevention, and content filtering capabilities in one unit.

STEP 4: SECURE WIRELESS CLIENTS

Remember that a laptop with a wireless transceiver is vulnerable to threats within its transmission range. An attacker who commandeers a client endpoint can use the secured tunnel to gain access into your internal network and compromise the corporate security posture. Symantec recommends three different levels of securing the wireless client:

- Deploy a personal firewall at each client.
- Use policy-based management to ensure that users don’t disable the firewall or let it get out of date.
- Enforce VPN at the access point level to prevent peer-to-peer attacks.

By implementing those four recommendations, your businesses can secure its wireless network easily and at low cost using proven technology. Additionally, teleworkers and traveling workers will be able to use the same credentials to secure their communications when remotely accessing the office network, so they’ll have the same user experience as when they’re on the internal network.

The maturity of IPsec VPNs also assures that your investment in wireless security, as part of a complete security policy, is not wasted. The same cannot be said for other new wireless security “standards” that are becoming available. There is no guarantee that hardware or OS support will be available for the next wireless security “standard” incarnation, or whether a major vulnerability will be discovered. Investments in entire infrastructures can be lost.

The use of VPN can also be freely applied to wired networks in locations with low physical security, such as branch offices open to the general public. VPN is also useful for open LAN ports at a main site where someone might “inadvertently” plug an access point onto your network.

The implementation of a secure wireless network described in this document uses models from Symantec’s entry-level integrated security appliance product line. High-end Symantec integrated appliances are also available, and support the same concepts.

FOR MORE INFORMATION

For more information on the complete line of Symantec Gateway Security appliances, visit www.symantec.com.

You may also wish to view the following information:

www.ieee.org. Institute of Electrical and Electronics Engineers site.
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