Making Everything Easier!™

SonicWALL Special Edition

Firewalls FOR DUMMIES®

Learn to:

- Protect networks from today's threat landscape
- Manage and control applications
- Use real-time visualization to adjust network policy
- Enable and protect remote workers

Peter H. Gregory,
CISA, CISSP, CRISC,
DRCE, CCSK

About SonicWALL

SonicWALL®, Inc. provides intelligent network security and data protection solutions that enable customers and partners — around the world — to dynamically secure, control, and scale their global networks. Built on a shared network of millions of global touch points, SonicWALL Dynamic Security begins by leveraging the SonicWALL Global Response Intelligent Defense (GRID) Network and the SonicWALL Threat Center that provide continuous communication, feedback, and analysis regarding the nature and changing behavior of threats worldwide.

Leveraging its patented* Reassembly-Free Deep Packet Inspection™ technology in combination with a high speed, multi-core parallel hardware architecture, SonicWALL enables simultaneous, multi-threat scanning and analysis at wire speed and provides the technical framework that allows the entire solution to scale for deployment in high bandwidth networks.

The SonicWALL family of firewalls tightly integrates intrusion prevention, malware protection, and application intelligence and control with real-time visualization. Solutions are available for the SMB through the Enterprise and are deployed in large campus environments, distributed enterprise settings, government, retail point-of-sale and healthcare segments, as well as through service providers.

For more information visit `www.sonicwall.com.`

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Firewalls FOR DUMMIES®

SONICWALL SPECIAL EDITION

by Peter H. Gregory,
CISA, CISSP, CRISC,
DRCE, CCSK

WILEY

John Wiley & Sons, Inc.

Firewalls For Dummies®, SonicWALL Special Edition

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Business Development Department in the U.S. at 317-572-3205. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-118-06194-7

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

WILEY

Table of Contents

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact `info@dummies.biz`. For details on licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Business Development Representative: Kimberley Schumacker

Custom Publishing Project Specialist: Michael Sullivan

Cartoons: Rich Tennant (`www.the5thwave.com`)

Composition Services

Sr. Project Coordinator: Kristie Rees

Layout and Graphics: Lavonne Roberts

Proofreader: Melanie Hoffman

Special Help from SonicWALL: Dori Legard, John Gordineer, Eric Crutchlow, Scott Grebe, Heather O'Reilly

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Introduction

With this book, you get "must have" information about next-generation firewalls to understand how they work and the threats they counter. If your organization has networks connected to the Internet, you need the information in this book if you want to protect your network from threats that continue to grow in their power and impact.

How This Book Is Organized

The main purpose of this book is to acquaint you with next-generation firewalls and how they protect your organization.

In **Chapter 1, Understanding Threats and the Role of Firewalls**, I explain today's threat landscape and how firewalls help to protect an organization against these threats.

Chapter 2, Examining Features in Today's Firewalls, is a review of the common features found in firewall products available today. Each feature is described in detail.

Then, in **Chapter 3, Uncovering Advanced Firewall Features**, I discuss more firewall features, primarily those found in advanced firewall products.

Next, **Chapter 4, Enabling and Protecting Remote Workers**, explains remote access and remote management technologies present in firewalls that protect remote workers, their communications with internal networks, and the internal networks themselves.

Finally in **Chapter 5: Ten Advantages of Next-Generation Firewalls,** I list ten things about next-generation firewalls that make you wonder how you ever got along without them.

Icons Used in This Book

Icons are used throughout this book to call attention to material worth noting in a special way. Here is a list of the icons along with a description of what each means:

REMEMBER

Some points bear repeating, and others bear remembering. When you see this icon, take special note of what you're about to read.

TECHNICAL STUFF

This icon indicates technical information that is probably most interesting to technology planners and architects.

TIP

If you see a Tip icon, pay attention — you're about to find out how to save some aggravation and time.

Where to Go from Here

Whether you've been managing firewalls for years or if firewalls are a new subject, there's something in this book for you. If you're just starting out with firewalls, I suggest you begin with Chapter 1 to understand today's network-borne threats and how firewalls protect networks from those threats.

If you're experienced with firewalls and you want to understand the newer features found in firewalls, jump to Chapters 2 and 3. If you're interested in telework and other remote access topics, Chapter 4 is where you want to go.

If you need a quick understanding of the advantages of next-generation firewalls, turn to Chapter 5 where you find the *For Dummies* tried and true ten reasons why next-generation firewalls are needed to protect organizations' networks.

Chapter 1

Understanding Threats and the Role of Firewalls

In This Chapter

- Learning about traditional and evolving threats
- Taking a look at modern firewalls

Threats: Not just hypothetical ideas, but real: malware, botnets, hackers, spam, and organized crime. They want to take control of your computers, steal your data, and use your systems to attack their next victim. A generation ago, firewalls were enough to protect against this. Today, alone, they hardly make a difference. Instead, a plethora of defenses are needed to repel the variety of attacks that are bombarding every corporate network.

Understanding the Threat Landscape

The Internet is the global marketplace of businesses, schools, and governments, the prime medium for personal and business communication, and the meeting place for personal and business networking. Practically everything that happens in the world happens on the Internet, or the Internet is used to communicate these events to others.

The Internet is also the medium of choice for organized crime throughout the world. Not only is the Internet the means for their communication, but also businesses, governments, and schools on the Internet are targets of organized crime for the purposes of next-generation profiteering through a variety of illegal activities, such as theft and fraud. For example, criminal organizations build botnets to take control of thousands of users' computers and use them to send spam, launch phishing schemes, and attack more systems.

Technology companies are driving innovation through the development of new web technologies like Web 2.0. But hackers are innovating too, with ever-improving tools and techniques for discovering and exploiting technical and human vulnerabilities to deface, defraud, and steal. The phrase "cat and mouse" comes to mind just now, but this phrase is too playful and childlike. Nation-states are getting into the game, too, by carrying out attacks to conduct espionage and to disrupt government and military networks (you can call this cyberwar).

Older but still potent threats

The original targets of hackers were computer operating systems. Designed in an era of mutual trust, the computer operating systems of the 80s and early 90s assumed that anyone on the network was vetted and trusted. But as organizations connected themselves to the Internet, unknown actors could now communicate, and some of them were there to bring harm to anyone vulnerable to it.

Early threat paradigms

Earlier generations of threats took the form of tools and techniques used to identify features in a computer's operating system that were

- **Active:** This refers to whether a potentially-vulnerable feature in an operating system is running.
- **Accessible:** This refers to whether a remote attacker is able to remotely access a potentially-vulnerable operating system's features.
- **Vulnerable:** If the operating system feature has some kind of a weakness, an attacker may be able to take advantage of this.
- **Exploitable:** By this I mean that any vulnerability in an operating system can be used by an attacker to cause the feature or the entire system to malfunction, or may give the attacker partial or complete control of the operating system.

While you may find many sexier and more valuable exploits today, the tools that intruders use to discover and exploit vulnerabilities still include all the basic operating system-level weaknesses. This is like saying an intruder who may try to find ways to break into your home with advanced lock picks still checks under the doormat for the key.

Responding to early types of threats

The types of threats that targeted weaknesses in operating systems could be effectively managed by working through a simple decision tree.

When a vulnerable operating system service was identified, there were four basic choices:

- Turn it off
- Block vulnerable systems and ports with a firewall
- Patch or configure to make safe
- Pray for the best

At this time, it was usually easy to determine whether a service needed to be accessible from the Internet. If so, then it needed to be patched or configured to be safe. If Internet access was not required, then a firewall was used to block access from the Internet. If the service wasn't needed at all, it could be turned off.

All of this talk about features and services and blocking with firewalls requires a little more talk about the technology in play here. Operating system features and services are uniquely identified with something called a port number. Servers are each assigned a unique IP address. Stateful packet inspection firewalls, which you discover more about in this chapter, block or permit messages based on their source and destination IP address and the port number.

Make no mistake: These older threats are just as dangerous as the latest exploits. If left exposed, an intruder may be able to steal or alter data, and take partial or complete control of the target system.

Current and evolving threats

The early paradigm of blocking individual services with firewalls was effective, for a time. But the next type of threat was more difficult to deal with. When intruders discovered that many organizations were blocking all but essential services, intruders developed a new strategy: attack systems via the services still present on servers.

New threats in detail

Through the 1990s, many organizations built web servers for publicity, customer information, and e-commerce purposes. Intruders began to experiment with web servers and quickly found that they could send packets to webservers and trick those servers into doing any of several actions:

- Logging on without having to provide credentials
- Displaying sensitive application data
- Permitting intruder to "deface" the website's content
- Causing the server to malfunction, so legitimate users are unable to access it
- Giving complete control of a server to intruders

If this wasn't bad enough, another important fact about these types of exploits is that firewalls do nothing to stop them! Here is why: By their nature, firewalls permit all IP addresses on the Internet to access a web server. But firewalls didn't examine the *contents* of packets being sent to web servers.

REMEMBER

Stateful packet inspection firewalls only examine the source and destination IP addresses, and the destination port number of incoming packets. These types of firewalls didn't look any further into any incoming packet.

This problem was big for website operators, and for a time, no easy solution existed. Website operators had to become skilled at being able to block all kinds of malicious content that firewalls (and antivirus) weren't designed to inspect and block.

More critical services exposed

As the 1990s have given way to the 2000s, organizations put up other critical services on their networks, and in many cases they have made these services available to the Internet. These services include the following:

- Voice Over IP (VoIP)
- Remote Access via virtual private network (VPN)
- Customer relationship management (CRM), online order taking, and credit card processing on the Internet
- Expansion of telework

Like web servers, these other services are vulnerable to attack because firewalls weren't designed to examine the data being sent to them.

Looking at the Types of Firewalls

Like nearly every kind of information technology, the development of firewalls has brought about steady improvement in terms of features, reliability, and capacity. In this section I describe the earliest firewalls right up to the most sophisticated products available today.

Understanding the purpose of firewalls

The role of a firewall is to examine a network packet and make a pass/no-pass decision on the packet based on its characteristics — kind of like a security guard at a building entrance who checks the identification of personnel coming and going, and who controls who may come and who may go. In basic terms, firewalls do this.

A *firewall* is like a checkpoint at a border crossing. A firewall is strategically placed at the boundary between two networks, just like a physical checkpoint is placed at the boundary between two countries, or at the border of a military base, for example. At the network boundary, the firewall examines incoming and outgoing network packets and examines a few basic properties of these packets: source IP address, destination IP address, and destination port number. The firewall consults a list of allowed messages (called the *access control list,* or ACL), and either lets the packet pass through, or blocks it.

If a firewall allows a packet to pass through, the firewall simply transmits the packet to the other side. If the packet doesn't comply with policy, it's not allowed to advance to its destination. This is shown in Figure 1-1.

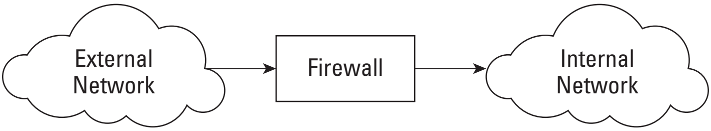


Figure 1-1: A firewall's location in a network.

Early types of firewalls

The earliest firewalls were programs that ran on Unix computer systems. These first firewalls were basic *packet filters,* making basic pass/no-pass decisions on each incoming packet based on its source and destination IP address and port number. There was nothing sophisticated about these firewalls — they were configured by editing rudimentary text files, and they had little in the way of logging.

In the early 1990s, router manufacturers realized that firewalls were important in the burgeoning Internet, and began to include packet filtering capabilities into their products. Standalone firewall products also began to emerge later in the decade.

As technology advanced, firewalls began to be "aware" of complicated protocols, such as FTP, by examining the contents of certain messages in order to track the facts about particular sessions. Firewalls did this so they would permit these complex sessions to pass unimpeded through the firewall while effectively blocking disallowed communication. While still basically a packet filter, this next improvement in firewalls had the intelligence to permit complex protocols such as FTP to pass through them.

Over time, firewalls were also improved to make administration easier (generally through graphical interfaces instead of command lines), and logging was improved so that administrators could monitor activities on the firewall such as failed and successful communication through the firewall.

Firewall technologies

Firewalls use several techniques to protect networks and systems. This section describes those techniques, in roughly the order that they have been developed over the years.

Proxy firewalls

A proxy is a server or device that acts as a gateway between two systems or networks. A firewall that acts as a proxy filters packets like a packet filter firewall, but it also performs another role: A proxy server sits in the middle of a connection between two servers and acts as a two-way intermediary.

For example, client system A wishes to communicate to server B. The communication path between A and B goes through a proxy firewall. When client A sends a message to server B, the proxy firewall receives the message. Next, the proxy firewall examines the message and compares the message's characteristics to see whether it should be permitted to pass through. If the packet is permitted, the proxy firewall transmits a packet to server B on behalf of client A.

When server B receives the message from client A, B acts as though the true origination point of the message is the proxy firewall. Likewise, when client A receives responses from server B, A believes that the proxy firewall is actually B. This is also like two people speaking through a language interpreter, where each person thinks the interpreter is actually the other party with whom they're speaking.

WARNING!

Because of the way they work, proxy firewalls generally suffer performance-wise, primarily through increased network latency (the time it takes for packets to reach their destinations).

Stateful packet inspection firewalls

Stateful packet inspection firewalls are distinguished from simple packet filter firewalls in this way: Packet filter firewalls are unaware of the details of complex TCP/IP protocols, but instead just make pass/block decisions on packets solely on the basis of their source and destination IP addresses and port numbers.

Stateful packet inspection firewalls, on the other hand, are familiar with the details of both simple and complex TCP/IP protocols such as file transfer protocol (FTP) and remote procedure call (RPC). Here are some examples of how a stateful packet inspection firewall decides whether packets are permitted to pass through it:

- Client A sends a domain name system (DNS) query through a firewall to domain server B. The firewall tracks the DNS query message. When the DNS server responds, the firewall permits the reply to pass back to Client A.
- Mail server A is transferring messages to mail server B. Servers A and B initially communicate on SMTP (simple mail transport protocol) port 25, but in the initial session negotiation, servers A and B randomly choose two high numbered (greater than 1024) port numbers through which to transmit messages. A stateful packet inspection firewall will monitor the initial session negotiation and permit the servers to communicate on those specific high numbered ports for the session.
- Client A establishes a file transfer protocol (FTP) session with FTP server B. Like SMTP in the earlier example, the two systems initially communicate on FTP port 21 (called the control channel) and negotiate high numbered ports. Then, when one system begins a file transfer session, they establish a separate file transfer channel on FTP port 20, and negotiate a separate pair of high numbered ports. A stateful packet inspection firewall keeps track of all of this and permits the control channel and data transfer channels to proceed.

Stateful packet inspection firewalls represent an advancement in firewall technology by making it easier to configure the firewall for complex protocols without compromising security (by permitting all high numbered ports to pass through). But other than session negotiation, packet filters and stateful inspection firewalls pay no attention to the contents of the data passing through.

Deep packet inspection firewalls

The next big jump in firewall technology is known as the *deep packet inspection firewall,* so named because this type of firewall examines more than just the packet's header (source and destination IP addresses and ports), but also examines the contents of data being transferred through the firewall.

The purpose of deep packet inspection (DPI) is to enable a firewall to make more intelligent decisions about whether incoming packets should be transmitted through to their destinations. DPI on a firewall must determine the type of data being examined and then make intelligent decisions about the types of scanning to perform on it. For instance, the packet could be JavaScript, a portion of a file transfer through CIFS, or a spreadsheet document attached to an e-mail message.

WARNING!

Some DPI firewalls inspect only a part of a file, assuming that malware usually occupies the very beginning or the very end of a file or packet. Sometimes known as streaming DPI, it isn't necessary to assemble the entire file before starting to scan it. The disadvantage is that hackers who discover how streaming DPI engines work can easily craft malware to escape detection. Also, a firewall that includes DPI doesn't necessarily inspect all network protocols. Be sure to check which protocols are supported so you can determine a firewall's suitability.

Another version of DPI was developed by SonicWALL called Reassembly-Free Deep Packet Inspection™ (RFDPI). I discuss this in Chapter 2.

Some examples of additional inspection that DPI firewalls can perform include

- **Antimalware:** A firewall can perform antivirus and antispyware examinations on packets to block any viruses or other malware.
- **Application attacks:** A firewall can block a wide variety of attacks against web applications including SQL injection, script injection, cross-site scripting, cross-frame script, and cross-site request forgery.
- **Intrusion prevention:** A DPI firewall can, through the recognition of signatures and behavior, recognize and block

attempted network intrusions. This is similar to the function of standalone intrusion prevention systems (IPS).

- **Protocol non-compliance:** A firewall can examine packets and make pass/no-pass decisions based on packet characteristics:
  - **SSH:** The firewall can block older versions of the secure shell (SSH) protocol.
  - **SSL:** The firewall can block older versions of SSL, or it can block SSL connections using older, weaker ciphers.
  - **SMTP:** A firewall can block ordinary SMTP (simple mail transfer protocol) and permit only newer SMTP-over-SSL.
- **Antispam:** A firewall can inspect e-mail messages and block spam messages.

Deep packet inspection techniques are being developed regularly. Modern firewalls will be able to incorporate advancements in DPI through periodic updates from manufacturers.

Current firewalls

Firewalls available today are far more advanced than at any time in the past. Two types of modern firewalls are:

- **Unified Threat Management (UTM):** This is the all-in-one firewall for the small to medium business. This single appliance provides multiple firewall functions which can include deep packet inspection (DPI), antivirus, antispam, content filtering, intrusion prevention (IPS), application control, and virtual private network (VPN).
- **Next-Generation Firewall (NGFW):** This is a firewall for the mid to large enterprise that incorporates application control, intrusion prevention (IPS), and deep packet inspection (DPI). The main differentiator is that NGFWs can also provide important visualization into what's happening on the network as well as deep packet inspection for SSL encrypted traffic.

The features listed here are explored in more detail in Chapter 2.

Chapter 2

Examining Features in Today's Firewalls

In This Chapter

- Understanding access control lists and why they're still important
- Knowing why firewalls decrypt and re-encrypt SSL traffic
- Seeing why logging is so important on today's firewalls

This chapter explores the features in today's modern firewalls in detail. Firewalls do a lot more than filter packets based on IP address and port number. Today they block intrusions, viruses, and spam; filter dangerous (and time wasting) Internet websites, manage VPN connections, and intelligently observe and control application traffic. They do a lot more than filter packets using access control lists. These are definitely *not* your father's firewalls.

Access Rules

The access control lists (ACLs) found in the earliest firewalls are present in modern firewalls. It is still important to block and permit network traffic to and from specific IP addresses, networks, and ports. The foundation of a firewall that's effectively protecting the organization starts with a well-built set of rules.

Access control lists contain individual entries that typically specify the following:

- Source IP or network address
- Source port

- Destination IP or network address
- Destination port
- Permit or deny

An ACL will usually have many such individual entries, possibly several dozen, including a special "include all" or "deny all" rule. When considered together, the ACL will usually resemble one of the following two rules:

- Deny all network packets except for the following that are explicitly allowed.
- Allow all network packets except for the following that are explicitly denied.

Security professionals tend to prefer the "deny all except . . . " approach, because it requires the administrator to specify which network packets should be permitted.

Intrusion Prevention (IPS)

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) used to be network components that were separate from other devices. Today, they're built into many firewalls.

IDSs have given way to IPSs. An IPS has all the features of an IDS but can also block suspected attacks instead of merely reporting them. IPSs work by examining the details of each packet on the network, and then blocking the packet or permitting it to proceed based on evaluation results.

It's a natural fit to have a firewall with a built-in IPS. Both a firewall and an IPS are made to examine network packets and then make decisions on whether each packet should be able to proceed to its destination. Firewall and IPS functions are complementary, because each is using a different set of logic to make the pass/no-pass decision.

Organizations typically take a slow approach to implementing an IPS. This helps to reduce the possibility that the IPS will block network traffic that should be allowed to pass through the network and therefore avoid embarrassing outages.

An IPS works a lot like an antivirus program: an IPS compares the contents of network packets with a list of known "signatures" on file that represent unwanted packets. An IPS can also block or permit a network packet based on its behavior, much like the "heuristic" capabilities of an antivirus program. IPS and antivirus also periodically update their signature file to be up-to-date with new types of attacks.

Reassembly-Free Deep Packet Inspection

Today's firewalls are packing in a lot of features into a single product. However, all these features can result in increased time for packets to get through the firewall because of all of the examination by IPS, antivirus, antispam, ACLs, and so on.

Reassembly-free deep packet inspection (RFDPI) improves performance by having each network packet examined only once by a single integrated scanning engine that checks for all of the various threats in a single pass. An incoming file of any size can be examined without having to load it all into the firewall's memory. All the data of every packet is inspected without having to buffer a file, so file size isn't a factor. Because malware must be delivered in its entirety to be a threat, if a piece of malware is split across multiple packets, the RFDPI process can detect this hack and still block the remaining packets. SonicWALL has five patents on this process (U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723).

Multi-function firewalls without this feature will spend considerably more time performing multiple inspections of each incoming packet — one for each function on the firewall. This results in reduced performance and increased latency.

When you're shopping for a next-generation firewall, be sure to check performance claims. A firewall with RFDPI is going to give better performance than one without it.

Antivirus and Antispyware

Many of today's firewalls include virus scanning. This can greatly improve an organization's "defense in depth" by having another set of eyes examining incoming (and outgoing) traffic for malware. And because a firewall is at the organization's network boundary, viruses and other spyware and malware are stopped at the boundary, safely away from e-mail servers, file servers, and end-user workstations.

Like most of these newer features, firewalls aren't going to be blindly scanning each incoming packet for the hundreds of thousands of known pieces of malware. Instead, next-generation firewalls are going to be smart about the types of packets to scan and how to scan them, so the firewall's performance isn't adversely affected. Firewalls with RFDPI are going to outperform those without it.

WARNING!

Because malware is so prevalent and potent, organizations using next-generation firewalls with antivirus and antispyware features should continue to rely on antivirus and antispyware programs on e-mail servers, file servers, and end-user workstations. This is necessary to have an effective defense in depth strategy against malware.

Antispam

Spam makes up 80 to 90 percent of all e-mail passing through the Internet. Besides being annoying, much of this spam contains malware in attached files or links to websites with malware that tries to install itself on victim computers. You can block spam on the

- **End-user system:** Blocking spam here removes it from a user's inbox, but the mail server and the internal network still have to process it.
- **E-mail server:** This is a handy place to detect and block spam. However, the problem with blocking spam here is that the e-mail server is subject to the burden of processing these unwanted messages before they're deleted.
- **Cloud service provider:** Here, all corporate incoming e-mail is routed to the cloud-based spam blocking service

provider, who filters out spam. While this process reduces network bandwidth, there's added risk because the spam service provider is now on the critical path for incoming e-mail, and the organization loses some control.

- **Antispam appliance:** This type of solution is becoming popular, because it removes spam before it reaches the corporate e-mail server. This dramatically reduces the volume of work that the e-mail server has to process.
- **Next-generation/UTM firewall:** Moving antispam to a firewall is another logical step in consolidating IT investment and improving performance. This type of firewall is already performing deep packet inspection, so why not let it perform your spam blocking?

While each of these methods has its pros and cons, organizations have moved to central control and blocking of spam, preferably before it reaches and overburdens e-mail servers.

REMEMBER

The main business driver for blocking spam used to be the conservation of network and staff bandwidth. Because so much spam contains malware or links users to sites with malware, risk reduction has become the new business driver for blocking spam.

Controlling Web Content

Web content filtering is a capability where organizations are able to control what websites employees are able to visit, and which are off-limits. Web content filtering systems are inline devices that intercept all requests from end-users' browsers. Each request is compared to the filtering device's list of policies. If the site is allowed, the device sends the request on to the website. If the site isn't allowed, the device displays a message to the end-user resembling the following:

> Access to this site (www.casino.com) has been blocked by the Company Name web filter. The reason that this site has been blocked is:
>
> Category: Gambling
>
> If you feel that this site should not be blocked, please contact the IT helpdesk at 800-555-2121.

Web content filtering systems are typically administered through the selection of categories (for example, weapons, violence, gambling, porn, and so on). If a category is selected, any site classified in that category is blocked. Web content filtering systems permit adding individual sites to the list of sites blocked and individual sites to be exempt from being blocked. Like other network security capabilities, web content filtering systems were once separate devices but are now included in next-generation firewalls.

Providing Remote Access: VPN

VPN, or virtual private network, is the primary way that organizations provide remote access to their internal networks. VPN permits a remotely located user to be able to access resources in the organization's network, through an encrypted tunnel. This tunnel is just a special network connection that's established when the user needs to be able to access systems or applications that are located in the organization's network.

Most VPN connections are encrypted with SSL or IPsec. These are two encryption and tunneling technologies that facilitate an experience that lets the user believe he's actually on the internal network. Discover more about remote access in Chapter 4.

In many organizations, VPN takes the form of a "VPN switch," a separate hardware system that is located just behind or beside the corporate firewall. But like other security functions, VPN is becoming a common feature in next-generation firewalls. This helps to simplify the network's architecture and simplifies administration by having one less network device to manage.

Application Intelligence and Control

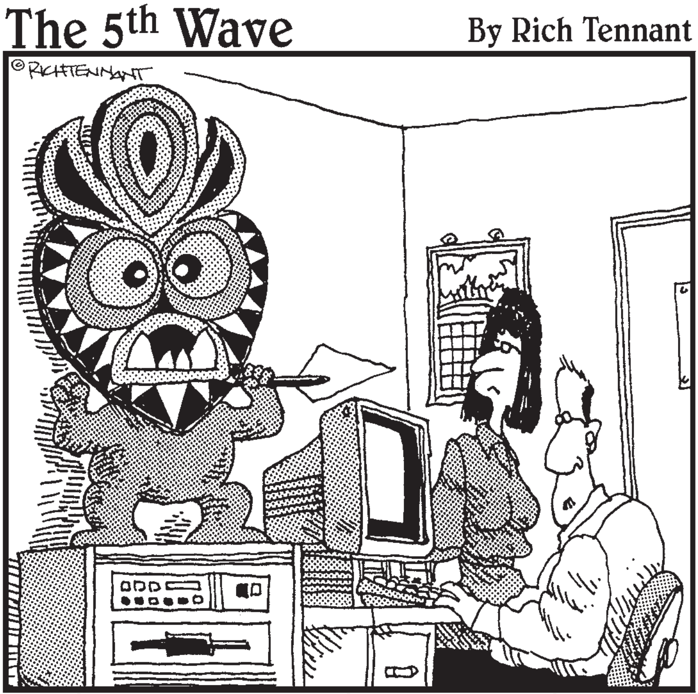
Leading next-generation firewalls are able to examine application-related traffic and act on those messages on an application basis instead of on a port number basis. A firewall that recognizes traffic as being related to a specific application can make better decisions about what to do with each packet as it flies through the network.

This level of granularity is important because most applications today are web applications, which all use port 80 or 443. Simply making pass-or-block decisions based on port number is insufficient for web applications. It's vital that a firewall recognize Oracle Financials traffic from Facebook traffic and make security decisions accordingly. Chapter 3 dives deeper into the benefits of application intelligence and control.

Logging and Alerting

A firewall is only as good as its ability to generate log entries and create actionable alerts. The firewall has to record what's going on. Firewalls have two main types of recordkeeping:

- **Firewall events:** These events occur on the firewall as it protects the enterprise from threats. Some of these events are
  - ACL violations: While many ACL rules are simply meant to keep intruders out, firewall administrators may be interested in a few of those rules and whether anyone tries to break them.
  - Blocked spam messages: Most messages are the same old boring stuff, but at least knowing how many were blocked in a day would be nice.
  - Blocked malware: It's always nice to know when malware filters are actually working.
  - Failed VPN logins: And successful logins too.
  - Web content filtering events: Don't you want to know who in your organization is trying to surf porn on the job?
- **Administrative events:** Whenever an administrator is carrying out her duties on the firewall, all the goings-on need to be recorded. These include configuration changes, software updates, adding or changing administrative users, and filter updates.



"So far it's saved us from Denial of Service attacks, as well as attacks from locust swarms, frogs, and zombies."

Chapter 3

Uncovering Advanced Firewall Features

In This Chapter

- Knowing why firewalls decrypt and re-encrypt SSL traffic
- Understanding the benefits of advanced application intelligence, control, and visualization
- Seeing how advanced features make firewalls even more valuable
- Understanding advanced reporting

This chapter discusses the advanced features found in today's next-generation firewalls. Today's firewalls also include several "standard" features (discussed in Chapter 2, as well). Here I go a little deeper into the topics.

Deep-Packet Inspection of Encrypted Network Traffic

Much of the sensitive traffic passing over the Internet, particularly Web traffic, is end-to-end encrypted with SSL. This means that intermediate devices like firewalls only see encrypted packets as they pass back and forth between endpoints.

Some advanced firewalls have the ability to decrypt and re-encrypt SSL traffic that passes through them. Firewalls with this capability can perform various types of deep packet inspection, content filtering, and antivirus on these packets. Firewalls that can't do this will be blind to all SSL traffic. This would be a serious deficiency in any next-generation firewall. Deep packet inspection of SSL encrypted traffic is illustrated in Figure 3-1.

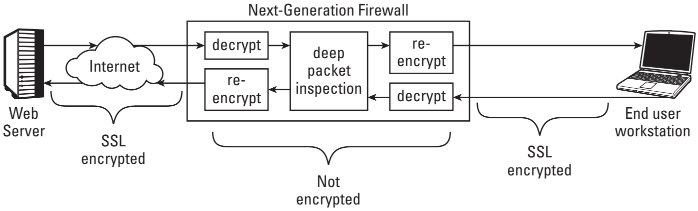


Figure 3-1: Deep packet inspection of SSL traffic.

Devices that perform decryption and re-encryption of SSL traffic usually have a "wildcard" SSL certificate. If not implemented properly, this can cause end-users to get SSL certificate errors on their Web browsers when they visit websites, because the SSL certificate in the security device doesn't match the site that the user is visiting.

Application Intelligence, Control, and Visualization

Advanced firewalls are aware of the details of traffic on the network at the application level. These details can be displayed visually, giving you a better idea of what's going on in the network.

Many advanced firewalls go further than this, by allowing control over the use of network resources at the application and user level. This means that firewalls can be used to control the amount of network resources that can be allocated to applications, users, and destinations. This goes way beyond the simple pass/no-pass rules of packet filter firewalls of the past.

Application intelligence

Today's advanced firewalls are application-aware. Not only are these firewalls cognizant of what traffic is traversing the firewall on what ports, but also

- What applications are running
- Who is using them
- What devices and programs those users are using

Advanced awareness gives administrators the ability to control the traffic that traverses the firewall by application instead of just by port number. This is important, especially with web applications that primarily run on ports 80 (HTTP) and 443 (HTTPS).

Awareness also gives administrators the ability to identify and control users (both individuals and groups of users) that use specific applications. Contrast this with older firewalls that had visibility only over IP addresses and IP address ranges.

Application control

Advanced firewalls give administrators control over the network traffic that flows through the firewall. The types of control available on today's advanced firewalls include the following:

- **Traffic flow by application:** Here, firewall administrators can determine the traffic flow for individual applications. This means that specific web applications (which nearly all run on ports 80 and 443) can be controlled.
- **Traffic flow by category of application:** Firewall administrators can control network traffic by categories of applications. If an organization has many applications, it can be logically organized into groups in an advanced firewall's configuration so it can more easily be controlled collectively instead of individually.
- **Traffic flow by user:** Administrators can control network traffic by individual user. Firewalls can be aware of users through integration with directory services, such as LDAP or Active Directory.
- **Traffic flow by groups of users:** Firewall administrators can logically create groups of users — for example, customer service, human resources, and executive.
- **Traffic flow by device type:** Firewall administrators can control traffic based on the type of system that end-users are using. Used together with network access control (NAC) technologies, organizations can effectively enforce policies that require the use of certain device types for application access.

- **Traffic flow by client software type:** Administrators can control traffic based on the browser and version that individual users are using to access web applications. This can help an organization to enforce the use of specific browsers while blocking those that aren't in policy.
- **Traffic flow by destination:** Administrators can control the flow of traffic based on its destination. For example, an advanced firewall can be made aware of botnets and other harmful traffic and block traffic to them.

Other configuration settings on an advanced firewall can then be used to control traffic based on these applications, users, and destinations.

The characteristics that the firewall administrator is able to impose on this network traffic are

- **Time of day traffic flow:** Administrators can determine what types of traffic are permitted to flow through the firewall at specific times of day. For instance, end-users may be permitted to access webmail at certain times of day (like on their lunch hour, or after hours).
- **Priority of traffic flow:** Administrators can prioritize critical enterprise applications and throttle back and even block the flow of other applications or users so they take fewer network resources. This can be used to ensure Quality of Service (QoS) for mission-critical applications. For example during peak periods, high-bandwidth sites like YouTube can be restricted.
- **Type of traffic:** Here, administrators can further control the types of traffic (types of files, specific URLs, or e-mail attachments, to name a few).

These types of controls are multi-dimensional. Administrators are able to control traffic flow for mission-critical and non-mission critical applications, prioritizing (or throttling) traffic at specific times per day and/or for specific users, classes of users, and traffic destinations.

Organizations aren't limited to managing only unencrypted application use. Reassembly-free deep packet inspection (RFDPI) can be used to examine and control application traffic encrypted with SSL.

Effective network access policy

Advanced firewalls that can be configured to control access to types of applications can help to effectively enforce company policy. For example, if an organization's security policy states that users shouldn't access file sharing sites (for example, LimeWire, BitTorrent), an advanced firewall can actually block this access, and also show which users are making access attempts. This solution is far more effective than having a policy without any means for actually enforcing it.

Application visualization

Today's advanced firewalls wouldn't be complete unless they also included advanced means for viewing the traffic that's flowing through the firewall. "A picture paints a thousand words," as the old saying goes, and graphical representations of firewall traffic can help administrators and management immediately understand what's happening on the firewall right now or over a span of time.

Dashboards

Understanding what's going on in a firewall starts with one or more high-level views. Today, these views are called "dashboards" because they include a broad array of valuable information. A typical application visualization dashboard can illustrate the portion of traffic used by various applications in an organization. Another can show network utilization of various applications over a period of time.

Detailed visualization

Understanding the traffic that's flowing through a firewall at the "dashboard" level is important, but often it's necessary to be able to "drill down" and get more detailed information about what's going on. Administrators and management are likely to want to know

- What users are using which applications over a period of time
- The bandwidth consumed by various groups of users

- Which URLs are being used most often
- To or from which countries is most of the traffic flowing

With detailed information, administrators and managers can view the utilization of application, system, and network resources. This helps them make further changes to the firewall configuration to fine-tune the allocation of resources.

Advanced firewalls include several ways to view the details of resource utilization, such as network bandwidth by user group or utilization by country.

The old saying, “If you can’t measure it, you can’t manage it,” fits the firewall management problem quite well. Be sure your firewall has a rich array of visual and numeric measurement capabilities that will enable you to manage traffic flow through your firewall.

Data Leakage Prevention

Organizations are concerned about the transmission of sensitive or proprietary information out of their networks. Organizations that manage high-value information need to identify and control opportunities for data leakage, including

- Webmail
- File sharing sites
- Social networking sites

Organizations are implementing data leakage prevention (DLP) systems. These systems are inline appliances that are positioned in the network near the firewall to examine all outbound (and perhaps inbound) traffic.

Types of sensitive data

A DLP system, when examining outgoing traffic, looks for patterns that suggest that outgoing data may be in any one or more of the following categories:

- **Account numbers:** Includes credit card numbers, bank account numbers, and other financial account numbers
- **Personal identification data:** Includes social security and social insurance numbers, passport numbers, driver's license numbers, home addresses, and medical information
- **Customer related information:** Includes nearly everything about customers, including contact information, sales history, contracts, and customer-owned data
- **Company proprietary information:** Includes M&A (mergers and acquisitions) information, company financials, prospect lists, internal memos, and source code

In advanced firewalls with DLP capabilities, organizations can configure the types and patterns of data that should be monitored for leakage. Plus, these data types and patterns can be prioritized by criticality. The criticality of data leakage events can be used to elicit different responses, including

- **Block and send an alert:** These high criticality events should not only be blocked, but also personnel in security management may need to be notified immediately so they may take appropriate action.
- **Block and record:** Events of slightly lower criticality may still need to be blocked, but they may not warrant interrupting management every time. Instead, these events can be managed when event logs are periodically reviewed.
- **Record but don't block:** Low criticality events may be worth recording, but they may not warrant blocking.

Data leakage reporting

In most organizations, the majority of DLP events doesn't result in real-time alerts but instead are logged for later review. Reporting in advanced firewalls should be rich and robust and include

- **Top leakage events:** Administrators and management need to understand the most significant leakage events that are occurring.

- **Most popular destinations:** It's important to know where sensitive data is going, whether it's personal webmail or file sharing sites.
- **Most frequent offenders:** It is important to know which users are most frequently sending sensitive data off-site.

Regular review of these and other DLP reports will help management to better understand the effectiveness of its DLP system and whether additional configuration changes are needed. For instance, there may be too many alerts of certain types, or too few of another. Also, the DLP system may be blocking legitimate network traffic.

REMEMBER

A network based DLP system is a vital part of an enterprise wide data leakage prevention strategy. Organizations may need to consider additional DLP controls including

- Scanning hard drives for sensitive documents
- Restricting or blocking the use of USB based storage
- Whole disk encryption for notebook computers
- Controls that limit the use of smartphones and other mobile devices

Management in Large Distributed Enterprises

Managing two or three firewalls is relatively easy. Managing dozens of firewalls in a larger organization is considerably more difficult. The primary challenge is the enforcement of consistency and uniformity of the configuration of multiple firewalls. Whenever an organization has multiple servers, routers, or firewalls, all of them should be managed the same way and have similar (or even identical) configurations.

Some of the forces that exacerbate this challenge include

- **Varying levels of expertise:** Some firewall administrators will be more skilled than others, resulting in differences in configuration styles.

- **Language differences:** Firewall administrators in different countries may have a greater or lesser understanding of technical documentation and company policy.
- **Remote office expediency:** It's a well known fact that people in remote offices will do things based on expediency as opposed to home-office personnel who'll do things more consistently.

Centralized firewall management helps solve this problem by providing a single interface that is used to manage multiple firewalls regardless of their location. This helps to make firewall configurations more consistent with each other and also helps firewall administrators to more effectively and efficiently manage greater numbers of firewalls.

Network Performance Management and Monitoring

Advanced firewalls provide improved reporting capabilities, showing the network resources consumed by various applications, users, and destinations. This helps management understand what traffic is on the network.

TIP

SonicWALL firewalls provide not only snapshot visualization (what's on the network *right now*) but also trending information in visual form that can help management understand the patterns and trends of network traffic over periods of time.

Enterprise monitoring

These reporting tools can permit an enterprise monitoring team to keep an eye on the firewalls' perspective on network traffic. Firewalls that have the capability of producing alarms when traffic thresholds are reached can alert operations personnel that there may be traffic on the network that warrants closer observation and maybe even intervention. This can help the organization to respond to security issues such as attacks, break-ins, or malware infections.

Periodic reviews

Coupled with formal management review processes, management can periodically examine traffic patterns on the network to get a better long-term understanding of network traffic, and which applications and users are consuming network resources.

Management should consider doing periodic reviews of alarms and alerts from the intrusion prevention system (IPS), data leakage prevention (DLP), antimalware, antispam, and packet filtering modules. Again, this helps management better understand long-term trends of security-related events on the network.

Advanced Reporting

Organizations with larger and more complex environments often need more flexibility and power in their reporting. While great on-box reporting has high value, some organizations need to be able to combine firewall reporting data with data from other sources. This means that advanced firewalls need to be able to export their reporting data into other systems.

I'm talking about more than exporting data into CVS files for import into spreadsheets. Instead, what is needed is an interface such as IPFIX/NetFlow with Extensions that is sent to external collectors for comprehensive long-term trending, forensic analysis, and threat analysis.

Chapter 4

Enabling and Protecting Remote Workers

In This Chapter

- Understanding the trends and risks of remote working
- Protecting the enterprise while allowing remote working

Remote workers — sometimes called teleworkers — work outside of the office most or all of the time. They can be in almost any role: sales, support, or any other job where workers just need a good Internet connection and a phone.

To make remote workers successful means giving them connectivity back to the organization's core internal network where they can access corporate e-mail, file servers, internal applications, internal phone systems, and voice-mail. Today's firewalls enforce and facilitate this connectivity — enabling remote access while protecting internal networks from intruders.

Understanding Trends in Remote Working

Advances in technology, the proliferation of broadband Internet connectivity, and new economic realities are increasing the incentives for employees and organizations to increase remote work. This section describes why remote working is increasingly common in organizations.

Telework and "work from anywhere"

More and more organizations are sending their employees home. No, they aren't terminating their workers, but instead they understand that with today's communications technologies, significant cost savings opportunities are available through the elimination of expensive office space and replacing it with relatively inexpensive voice and data communications capabilities.

Employees are appreciating this trend as well. They're free of the cost and time used in daily commutes, whether they drove, carpooled, or used public transportation. Teleworkers' commutes consist of walking from the bedroom to the kitchen to make breakfast, and then to the home office where they spend their workdays.

Outside sales personnel have enjoyed this lifestyle for years, but now they're being joined by workers in many other departments, whether they're software developers, systems engineers, staff attorneys, or accountants. Employees are enjoying the freedoms of telework in greater numbers, and employers benefit from the cost savings in the form of less office space to lease and manage.

Not everyone works in a home office. While many do, many others work from public hotspots and "hotel" cubes in offices.

REMEMBER

Remote workers will be effective only if they have the tools needed to stay in touch with their colleagues. Organizations can rest easy only when they know that the information used by their remote workers is adequately protected.

Mobile devices

Mobile devices, such as smartphones and tablet computers, are the new endpoint. Outselling laptop computers, mobile devices have rich connectivity and processing capabilities unknown even a few years ago.

Mobile devices are capable of connecting to the Internet at speeds unheard of even in the recent past. This makes it possible for remote workers, even those with only a cellular signal, to run bandwidth-hungry applications from practically anywhere.

Understanding the Risks of Remote Working

The typical remote worker is a teleworker who works in a home office or frequents public hot spots such as coffee houses. She has a laptop computer and some type of a smartphone or advanced mobile device.

While a teleworker can experience many cost benefits and quality-of-life advantages to remote working, some risks need to be considered. These risks fall into two major categories.

Physical security

WARNING!

A remote worker, whether working at home or at some other off-site location such as a hotspot, isn't protected with the same physical security controls that are found in many office locations, such as

- **Commercial grade locked buildings:** Typical office buildings, particularly "Class A" buildings, are constructed of materials that withstand break-ins and also natural threats such as floods and earthquakes. Workers and office equipment such as computers are safer from theft and damage in office buildings.
- **Key card systems:** Many office buildings incorporate some kind of a key card access system that controls which persons may enter a workspace. This reduces the risk of theft or damage to equipment including computers.
- **Video surveillance:** Some office buildings employ a video surveillance system, which acts as both a deterrent as well as a detective control by recording who comes and who goes.
- **Shredders:** Many office buildings have shredders or shred bins that ensure that all discarded printed materials are securely destroyed.

Network security

Remote workers are often exposed to more threats than workers located in corporate offices because the remotely connected worker isn't protected by corporate security controls and devices, such as a firewall or an IPS.

When a remote worker is connected via VPN to the corporate network, the remote worker *may* have one or more protections, but remote workers typically only launch their VPN when they have a specific need to access internal-only resources, and the rest of the time they turn off the VPN.

Figure 4-1 illustrates the typical VPN problem. The office connected user in this figure is protected from Internet-borne threats by the corporate firewall and other controls. The remote user is connected directly to the Internet and isn't protected by any of those controls. The VPN connected user connects directly to the internal network, bypassing controls protecting the internal network from possible threats present on the user's remote computer.

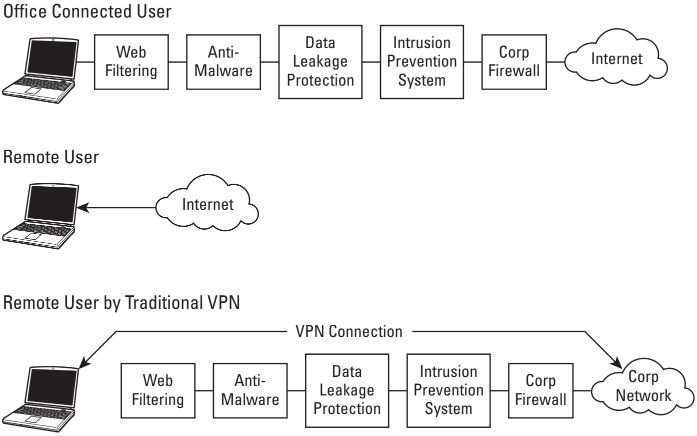


Figure 4-1: Local and remote worker security controls.

When a remote worker is connected to the Internet, he may be doing so over a less secured or unsecured wireless access point that could easily permit an eavesdropper to listen in on the remote user's network traffic and even hijack the user's sessions.

Enabling Remote Work Without Compromising Security

Countless numbers of organizations have suffered through security incidents where relatively unprotected endpoints became infected with malware that was then permitted to infiltrate the corporate network through trusted VPN connections. This section discusses the security controls available that effectively protect remote workers' systems and the enterprise network.

VPN remote access

Today's advanced firewalls have many features built-in, including VPN (virtual private network). This permits users who are away from the organization's office building(s) to be able to access internal network resources such as file servers, printers, and internal applications. VPN systems provide an "as though you were in the office" experience, via a special encrypted "tunnel" that encrypts this traffic so eavesdroppers can't view what remote users are doing. Advanced firewalls include enterprise-class features for VPN including

- **Integration with enterprise authentication:** Instead of using separate login credentials, VPN solutions permit users to use their LDAP (lightweight directory access protocol) or Active Directory user ID and password to log in to the VPN.
- **Integration with two-factor authentication:** Many organizations require that remote access users employ two-factor authentication — a user must use more than just a user ID and password to gain remote access to the internal network. Forms of two-factor authentication include security tokens, digital certificates, and biometric (for example, fingerprint and iris scan) readers.
- **Scalable and multi-site capabilities:** Some organizations may wish to implement multiple VPN "entry points" for their employees around the world. Instead of requiring workers worldwide to access one VPN point of entry, workers can automatically connect to the geographically nearest VPN entry point for more efficient connections.

- **Client and clientless capabilities:** Organizations may wish to implement VPN clients on some systems (for instance, mobile devices) while permitting others to connect using “clientless” connections, where remote users simply point their web browsers to a site to establish a remote connection.

Clean VPN

Many organizations install their VPN entry point *behind* the firewall, in effect placing remotely connecting PCs and other devices just as though they were in the office (this is consistent with the purpose of VPN — to give the end-user a “just like I’m in the office” experience). Most organizations do not use a firewall to control network communications between remote PCs and the internal network.

This approach assumes that the remote system is clean and trustworthy, despite the fact that the remote system is away from the physical protection of the organization’s building. Aside from other advanced features, such as those discussed in the next section, Securing remote access, it may not be wise to completely trust remote systems, but instead they should be firewalled. This is shown in Figure 4-2.

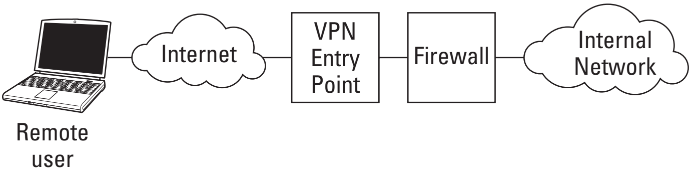


Figure 4-2: Firewalling remote access users.

TIP

Firewalling remote users is a part of most advanced firewalls. SonicWALL’s *Clean VPN* solution integrates firewall and VPN capabilities so remote users are subject to the same deep packet inspection and other security capabilities, ensuring complete protection of enterprise assets.

Securing remote access

Advanced remote access (VPN) systems include many security controls to ensure that a remote worker’s system can’t threaten the organization's internal network. These newer VPN systems interrogate every device that wishes to connect to the internal network to ensure that the remote device

- Has all required security configurations
- Is running the right version of antivirus and antispyware software
- Has a personal firewall that is properly configured
- Is a registered device known to the organization
- Has any required digital certificates onboard
- Has any required files onboard
- Is running any required programs or processes

Remote devices that lack these characteristics are connected to a "quarantine" network where any missing characteristics can be fixed — automatically, or through end-user prompting.

Secure remote access systems like this ensure that only compliant devices are permitted to connect to the network. This dramatically reduces the likelihood that an infected endpoint is able to spread an infection to the internal network.

Remote administration and control

Working remotely will only be successful if there is a viable way for the IT department to support remote workers and their workstations. Requiring remote users to come in to the office if they have a serious problem isn't feasible if the remote worker is more than a few miles away from the office — in many companies, remote workers may be hundreds of miles from the office, and the cost of travel may exceed even the replacement cost of their workstation.

Advanced remote access systems include capabilities for desktop support personnel to remotely access remote users' systems through their Internet connections. SonicWALL's own Virtual Assist tool permits a helpdesk technician to remotely view and even control (with the user's permission) a user's workstation.

Remote access to user workstations

Remote workers may, at times, be away from their home office (or wherever it is they hang out) and need to access their remote PC. SonicWALL has another tool called Virtual Office that permits a user to be able to connect back to their remote PC when it's connected to a SonicWALL VPN. This permits users to be able to access their files or even run applications on their remotely connected PC. This solution is more secure than any of those "go to my PC" tools.

Global management

In many IT shops today, the mantra heard in the hallways is "scalability." This means that small IT staffs need to be able to manage large numbers of devices and systems using tools to make these tasks easier, and to make those systems configured and managed more consistently.

IT administrators need to be able to manage multiple devices like VPN systems without having to log in to each one. For instance, if an administrator needs to make a configuration change on all of the organization's VPN switches, he or she should be able to make one configuration change and "apply" it to some or all VPN switches.

In addition to scalable configuration, administrators and management should be able to get global reporting capabilities from all VPN devices instead of having to go to each VPN device to get usage, configuration, and event reporting.

Chapter 5

Ten Advantages of Next-Generation Firewalls

In This Chapter

- Understanding how next-generation firewalls simplify threat management
- Seeing how a single UI makes configuration and event viewing easier
- Keeping your organization's bad news out of the headlines

Here, in the familiar *For Dummies* style, I present ten great advantages of next-generation firewalls. While this chapter isn't a substitute for the rest of this book, you've come to the right place for bulleted items and speaking points.

Consolidated Network Architecture

In order to adequately protect a network from today's threats, an organization would have to purchase all these devices:

- Firewall
- Intrusion prevention system (IPS)
- Data leakage prevention (DLP) system
- Antivirus system
- Antispyware system
- Spam filter
- Virtual private network (VPN) system (both SSL and/or IPSec)

- Web content filtering
- Network access control (NAC)

Buying these results in a complex network environment with several devices to manage, all from different vendors with their own support organizations is a vendor management nightmare.

Today's advanced firewalls have all capabilities built into a single hardware solution. This consumes less rack space, less power, offers simpler support, and eases vendor management. Not to mention fewer power cords!

Single Configuration for Management of All Threats

Blended and advanced persistent threats require that many different types of controls on different systems be in place, including firewalls, antimalware, web content filtering, intrusion prevention, and antispam. Effectively protecting the enterprise from threats is far more difficult when administrators are required to configure a lot of separate systems, often entering the same information over and over.

On a single next-generation firewall, all the configuration items for the network, applications, devices, and so on need to be entered only once. Later on when the network's architecture changes a little bit or when new applications are added, again there's just one place where configuration changes need to be made.

Single UI for Viewing and Managing Threat Events

Imagine, for a moment, that you're trying to view a threat event that is unfolding in your network. The threat may consist of an attacker (perhaps a rogue employee) who's sending messages containing links to sites containing malware to company employees to steal information or disrupt company operations.

On a typical piecemeal network, administrators look at log entries on several different devices:

- Firewalls
- Antivirus
- Web content filtering
- Intrusion prevention system
- Data leakage prevention system

Of course, this is assuming that the organization has all these systems in place. Anyway, the point here is that a threat event takes on many different forms, and organizations with next-generation firewalls are going to see these events on a single system instead of having to look in many different places.

Also, with security solutions integrated into one platform, administrators are more likely to even notice events like this. On separate systems, they may look like the noise that one sees in a typical day.

Improved Security Defense in Depth

The real threats that organizations face today can't be stopped with any one type of security system. It's not only just network-based attacks that organizations have to worry about, but also spam, malware, rogue websites, and eavesdropping that all threaten to disrupt operations or steal data.

Today's adversaries have an offense in depth that can only be met by a defense in depth solution. Today's next-generation firewalls are up to the challenge.

Improved Control Over Applications

Previous generation firewalls just block or pass packets based on IP address and port number. They don't have a clue about applications. Next-generation firewalls, on the other hand, not only recognize various applications (even web applications, which use ports 80 or 443), but also can control them in a number of ways, including

- **Control by category:** A highly secure organization can simply block games, social networking, or online gambling, which results in blocking access to those types of websites. This broad-brush control can help an organization to quickly control the types of applications that users are able to access. Sometimes even components within a category can be permitted or blocked at a granular level. For example, allow Facebook, but block games.
- **Bandwidth management:** Organizations can control which applications get higher or lower priority network bandwidth. Critical enterprise applications can be given higher priority while others get lower priority.
- **User access:** It's possible to determine which users — or groups of users — are able to access applications or groups of applications.
- **Destination control:** It's possible for organizations to control connectivity to applications from various external endpoints or geographies.

Easier to Manage Through Intuitive UIs

Next-generation firewalls are built around advanced administrative interfaces that make it easier to manage them. Point-and-click, drag-and-drop, hover, and other capabilities reduce the time needed to configure and manage firewalls.

Intuitive interfaces also mean that less training is required. Security engineers who understand the concepts of firewalls, antivirus, IPS, and DLP can simply log on to the firewall and configure as needed.

All the Enterprise's Network Security in One Place

Imagine a complex network environment with separate firewalls, intrusion prevention systems (IPS), data leakage prevention (DLP), web content filtering, spam blocking, and antimalware. Just keeping track of where all these devices are in the network, how the data flows through each from here to there, and understanding any interdependencies between them is going to be someone's full time job.

Contrast that with a next-generation firewall: one box, everything flows through it. Just a power cord, one cable in, and one cable out.

REMEMBER

Security professionals love simplicity. A simpler environment is easier to manage; the likelihood of mistakes is lower, and it's less likely that errors are overlooked.

A Single View of Enterprise Network Security

An organization with separate firewalls, web content filtering, data leakage prevention (DLP), intrusion prevention (IPS), antispam, VPN, and web content filtering is going to be spending a lot of time looking at many different screens.

And forget about event correlation, unless you do it manually.

Putting all these functions into a single next-generation firewall provides a single, comprehensive view of all your network security events.

Secure Wireless and Remote Access

A next-generation firewall has a built-in, easy-to-manage VPN system for secure remote access. The VPN system integrates with the enterprise directory management system (LDAP or Active Directory to name a few) for simple end-user management.

So, sure, the VPN system is easy to use and set up for end-users. But security benefits are also available to end-users at remote locations, including home offices, public hotspots, hotels, airports, customer sites, and so on. The primary benefits: All communications between the end-user and the central network are encrypted, so eavesdroppers on unsecured wireless networks can't intercept remote user communications.

Helps Keep You Out of the News

A next-generation firewall can help to keep you out of the news. I think you know what I mean, but if not, it's this: Many security break-ins happen — it seems like each week there's a new one. A next-generation firewall, with its defense-in-depth approach, if properly configured and managed, can help to avoid the unthinkable.

Every organization must do a few other very important things to effectively protect its data:

- Develop a mature, end-to-end security management system.
- Perform periodic risk assessments. Address and treat all identified risks.
- Solicit highly qualified external security audit firms to periodically conduct audits and security scans.
- Regularly train and educate management, technical workers, and end-users.

WARNING!

Never believe that you have security completely figured out. Properly done, it's never done, because adversaries are always coming up with new ways to get you.

Chat between Miranda and Ryan
31,031
VoIP
Q3 Results
SAAS Quick Viewer
Western Region
Northern Region
Q3 Results by region
PROFILE 2
STREAMING MEDIA
Now playing
wind power
solar
energy
oil and gas
renewable energy projection 2015

Control, manage, and protect your network easily and automatically!

It can be a real challenge for IT administrators to maximize the business value of web applications while minimizing the risk. Today's firewalls make the job easy with granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. This turns the traditional gateway firewall into something much more important: *a productivity optimization tool*.

- ***Shut threats out at the gateway* — detect and eliminate malware, intrusions, data leakage, and policy violations**
- ***Seize control of your applications* — prioritize bandwidth to mission-critical applications and restrict bandwidth for non-productive applications**
- ***Take command of your network* —manage configurations, view real-time monitoring metrics, and integrate policy and compliance reporting**
- ***Secure and enable your remote workforce* — extend easy-to-manage intrusion prevention and anti-malware to mobile employees and branch offices**

Open the book and find:

- **How today's threat landscape has changed**
- **How firewall technology has advanced**
- **How to prioritize critical applications while minimizing risk**
- **How to protect any user, anywhere**
- **How advanced firewalls improve employee productivity**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-06194-7
Not for resale