Compliments of Avaya, Juniper Networks & Extreme Networks®

AVAYA

# Converged Network Security

FOR DUMMIES®

Avaya Custom Edition

Protect your IP network from threats and misuse

A Reference for the Rest of Us!®

Peter H. Gregory, CISA, CISSP

What is the challenge with converged network security? Finding the right partners to deliver a secure, reliable, converged voice and data network infrastructure — without limiting your flexibility to grow your business and extend the reach of your network — is the key.

Converged network security isn't something to be added after the fact — the need to protect your mission-critical communications systems and business applications should be considered from the very start of your converged network planning. At the same time, it's not enough to simply protect your network from external threats. With more and more employees using laptops and IP Softphones, converged network security has to enable protection of these assets from within the network as well — without limiting the ability of these employees to work remotely when necessary.

Avaya has partnered with two of the market leaders for converged networks, Juniper Networks and Extreme Networks, to bring best-in-class security solutions to converged voice and data networks. Avaya Global Services provides expert advice on security design and implementations for small businesses to world-wide enterprises.

Explore the possibilities at
**www.avaya.com**.

AVAYA

extreme networks

Juniper® NETWORKS

# Converged Network Security

FOR

# DUMMIES®

AVAYA CUSTOM EDITION

**by Peter H. Gregory, CISA, CISSP**


Wiley Publishing, Inc.

**Converged Network Security For Dummies®, Avaya Custom Edition**

Published by
**Wiley Publishing, Inc.**
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com



ISBN: 978-0-470-12098-9

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at www.dummies.com/register/. For information on a custom Dummies book for your business or organization, or information about 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:** Jan Sims

**Business Development Representative:** Jacqueline Smith

**Editorial Manager:** Rev Mengle

***Composition Services***

**Project Coordinator:** Kristie Rees

**Layout and Graphics:** Erin Zeltner

**Proofreaders:** Laura Albert, Brian H. Walls

***Special Help:*** Jon Alperin

---

**Publishing and Editorial for Technology Dummies**

**Richard Swadley,** Vice President and Executive Group Publisher

**Andy Cummings,** Vice President and Publisher

**Mary Bednarek,** Executive Acquisitions Director

**Mary C. Corder,** Editorial Director

**Publishing for Consumer Dummies**

**Diane Graves Steele,** Vice President and Publisher

**Joyce Pepple,** Acquisitions Director

**Composition Services**

**Gerry Fahey,** Vice President of Production Services

**Debbie Stailey,** Director of Composition Services

## Avaya Acknowledgments

This book would not have been complete without the assistance and expertise of Craig Adams and Tim Bardzil of Extreme Networks, and Shrikant Latkar of Juniper Networks.

# Contents at a Glance

# Introduction

Competitive businesses today need competitive security — and it's a team effort. What is your role in your organization? Are you responsible for network architecture, policy, security, and strategy? Then this book can help you understand how to secure your converged network.

If you're a network practitioner, this book introduces you to the security technologies and practices you will likely be setting up and performing in a converged network environment. If you're in management, you can gain an appreciation for what others in the organization need to think about in order to ensure the security and success of your converged network.

Don't forget to check out the Avaya Limited Edition of *VoIP Security For Dummies* for additional insight into how Avaya IP telephony relies and builds upon the security environment of the underlying converged network. You can request a copy from Avaya's Web site at `www.avaya.com`.

## Understanding Network Security Inside-Out

Getting a grip on security in today's converged network environment can seem like a daunting and abstract exercise. But the steps you take are actually similar to those for basic home security: When you think of providing security and protection for your family and possessions, first you typically create a layer of security that surrounds your house and family — you put locks on doors and windows, set alarms to notify you of intruders, and perhaps even contract with a security firm to respond in case intruders manage to get in. And when your family is traveling outside the home, you may provide them with mobile phones so that they can stay in touch with other family members in case of emergencies.

In many ways, this level of externally oriented security is what Avaya's partnership with Juniper Networks brings to the table — Network Access Control, firewalls, intrusion detection and prevention systems, and Virtual Private Networks (VPNs) all create a level of security that protects the converged network of enterprises from external threats.

But if you have young children, you may also think of child-proofing inside the house — putting locks on cabinets to keep children away from chemicals and other dangerous items, covering electrical outlets to make sure that they aren't sticking their fingers in them, and so on. And perhaps you lock your expensive home electronics behind cabinet doors to keep little ones from storing their grilled cheese sandwiches in the DVD player. You also teach children not to open the door to strangers. This is a case of protecting against internal threats and mishaps.

This variety of security from within is where Avaya's partnership with Extreme Networks brings extra security value. Virtual LANs (VLANs) help protect network resources by logically separating different types of traffic from impact by other activities. Extreme Networks also uses industry-standard protocols such as 802.1x and LLDP-MED, as well as host integrity checking, to validate the permissions of devices to connect to and use the resources of the network. It can also provide powerful switch-based capabilities that can detect anomalous behavior and identify potentially damaging network traffic for further evaluation.

Finally, just as your entire family can often end up with a cold or virus that is sweeping through your child's elementary school, so viruses and security threats can bypass the externally facing firewalls of your enterprise. With 60 to 70 percent of virus and security threats coming from inadvertent actions of remote workers who bring their laptops back and forth between work, home, and public access points, the need to protect the network, communication systems, and other mission-critical business applications and systems from within is as important as protecting them from overt malicious hacking. As recently as October 2006, Apple computer admitted that a small number of their iPOD music devices were inadvertently shipped with a PC virus that could infect laptops that they are attached to. No matter how good your network firewall is, you are still vulnerable to a wide variety of attacks from within.

Ready to automatically lock doors as people come and go, childproof the cabinets, and get a flu vaccine? That's what converged network security is all about.

# How This Book Is Organized

The primary purpose of this book is to highlight the strategic role that Avaya's two strategic partners, Juniper Networks and Extreme Networks, plus Avaya's own Global Services professional services, play in the realization of Avaya's vision and leadership in converged voice and data networks.

## Chapter 1: The Importance of Securing Converged Networks

Chapter 1 makes the pitch for securing converged networks. Besides securing your VoIP hardware, you need to protect all your assets, including mission-critical applications and servers, such as Customer Service, Unified Communications and Web conferencing solutions, and so on. This chapter is not only about what, but how.

## Chapter 2: Jumping Juniper Networks: Improving Security for All

Chapter 2 describes how Juniper Networks, one of Avaya's strategic partners, contributes to the security of converged networks through its product offerings.

## Chapter 3: Extreme Improvements for Network Security

Chapter 3 shows how Avaya's strategic partner, Extreme Networks, contributes to converged network security.

### Chapter 4: Plans, Policies, and Avaya Security Services

Chapter 4 showcases Avaya Global Services and their security services as another strategic partner for assessing security and developing policy, architecture, and design for your enterprise network.

## 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 each:


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


This icon indicates technical information that is probably most interesting to IT professionals.


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

## Where to Go from Here

Regardless of where you are in your converged network plan, never lose sight of the big picture: Avaya is the converged networks expert and has strategic vision and leadership in intelligent communications, converged networks, and security. Companies that go with Avaya enjoy all the benefits of Avaya's knowledge, experience, and strategic partnerships with Juniper Networks and Extreme Networks. Discover for yourself why Avaya is the undisputed leader in delivering intelligent communications solutions.

# Chapter 1

# The Importance of Securing Converged Networks

### *In This Chapter*

- Understanding security in converged networks
- Protecting networks and devices in converged networks

Just look around . . . it seems as though *everything* that businesses are doing these days involves the Internet. And I don't just mean fancy Web sites with online ordering, but even the lackluster back-office things: the plumbing, the basement storage room, and the loading dock — the unsexy stuff is online. I'll bet even the coffee pot has an IP address.

Consider this phenomenon from another angle. Everything (coffee pot included) is about TCP/IP. It's not just in the computer center any more — it's everywhere! The sheer ubiquity of TCP/IP technology (and from now on I'll just say IP but I mean the same thing) is making it more important than before.

Avaya has been on the leading edge of this revolution by developing communications technology — especially Voice over IP (VoIP) that uses beefed-up enterprise data networks, doing away with the large and largely inefficient and costly voice networks. But Avaya isn't alone; strategic converged network technology partners Juniper Networks and Extreme Networks have been right there on the cutting edge developing the enabling and protective technologies that give Avaya products and services even more punch.

# Arrival of Converged Networks

Circuit-switched networks are soooo 20th century. They're expensive, underutilized, and definitely *not* cool. When was the last time you read about a killer app that ran on a circuit-switched *phone* network? Thought so.

Success in business today is all about IP. Avaya and their partners Juniper Networks and Extreme Networks have been working their fingers to the bone on a big mission: getting voice and other communications technologies *off* the voice network and *onto* the data network. This new network is still a data network, but it carries more than just your data, it carries your voice. Or put another way, your voice *is* data!

The new voice-plus-data network is called a *converged network*. The applications are converged, the protocols are converged, and even the wiring is converged. The single, multi-technology converged network carries all kinds of communications. A converged network is an IP network with the same technology at its core that runs the Internet. But converged networks carry not just computer-to-computer traffic, but also voice and other time- and delay-sensitive traffic, too, such as telephony, video and streaming media.

In addition to laptops and servers, many cool new devices are found on converged networks, such as *IP phones*. Although in appearance just like office phones seen everywhere, IP phones are *data network devices*. They plug into Ethernet networks just like computers and printers do. To the average user, IP phones are just like office phones, but to the IT manager and the CIO, they are network devices. And to the CFO and CEO, they are saving the organization lots of money by reducing communications costs. (Maybe they thought of this because we kept plugging laptops into the phone jack and vice-versa.)

# Protection of Converged Networks and Devices

So if you thought that data networks were important (they are!), when you put your phone system on your converged

network, the network becomes more important than ever. The network's reliability and freedom from jitter (you coffee drinkers will be happy to note) is not negotiable. Anyone who remembers the early days of digital cell phones remembers the clipping and other bizarre effects that digital transmission had on voice. That just won't fly on converged networks today.

Not only is performance more vital, but so is security. Threats don't originate *only* on the Internet, to be repelled by the firewall and antivirus software. That's the old school of security. Threats exist *within* the network as well — from sick laptops to mobile user carelessness. A new approach for security is called for — scalable, holistic security that protects the very fabric of the network.

There's more at stake if the converged network is compromised. In a converged network environment, if you take the network away, you might as well turn off the power. In fact, if you're using Power over Ethernet (PoE) devices, turning off the network *is* the same as turning off the power!

## VoIP-related complexities and challenges

Adding voice to the enterprise network has many advantages for an enterprise, but it also makes protecting the network more complicated:

- All network devices must operate with *minimum latency* in order to assure the quality of performance-sensitive services such as VoIP and streaming media.
- All security devices must be specifically aware of VoIP and other multimedia technologies so that they can continue to offer robust protection while not getting in the way of these services.

Existing security issues — Denial of Service (DoS), worms, viruses, spam and so on — that plague servers that run e-mail, Web sites and other applications, now also plague the VoIP systems.

## Evolving protection techniques to answer new threats

Not so long ago, if you had a firewall, you were pretty well set for network security. Firewalls were the only means necessary to protect data networks from fairly simple threats, which were unsophisticated and easily brushed aside. When there was little for troublemakers to do but vandalize the Web site, firewalls were all you needed. But as the *value* of business data on the Internet increases, the threats are growing in sophistication as they try to pry into business data for fun and profit.

Malware (viruses, worms, and Trojan horses) have more attitude and impact than they used to, and insider threats are more potent than before. And by insider threats, we mean both the malicious kind and the accidental variety: The classic example is a laptop or other mobile device that becomes infected with a worm or virus while it is on the Internet in an unprotected location, then brought back into the network where it is free to infect other systems.

To meet these threats, network design techniques and new security capabilities are available to protect business networks, including:

- **Firewalls:** Like a moat encircling the castle, the original network protector remains the mainstay of perimeter network protection. They permit data traffic of known types to specific servers and devices such as Web servers, e-mail servers, and VoIP gateways, while rejecting all other intrusive traffic.

  The perimeter isn't just between the enterprise and the rest of the world. Juniper Networks firewalls can also be used to protect internal assets by creating security zones for internal traffic and then applying the same sorts of policies as they would to external traffic, such as between brokers and research analyst organizations in a financial institution. See Chapter 2 for more discussion on zone architectures.

- **Intrusion detection and intrusion prevention systems:** These devices perform a more careful examination of network traffic than firewalls do. As the name suggests, IDS and IPS devices detect intrusions — whether it's a hacker probing your network or a virus using your network to

spread by scanning network traffic for specific signatures or anomalous traffic patterns. Intrusion *detection* systems generate alarms to notify network personnel that something is amiss, whereas intrusion *prevention* systems can actually stop the progress of an attack by dropping the offending traffic much like a firewall.

- **Unified access control (UAC) and Network access control (NAC):** This newest technique helps to ensure that all connections to the network conform to the policies set by the organization. UAC/NAC is used to authenticate and verify devices that connect to the enterprise network, devices such as PCs and IP phones. The two protocols in use are 802.1x and *Link Layer Discovery Protocol (LLDP).* Each is concerned with verifying both that the devices are authorized to connect to the network and also that such devices are healthy and present no threat to the organization.

  A good UAC/NAC solution does four things:

  - Makes sure the device or user is who they claim to be.
  - Makes sure the device or user is authorized to use the network.
  - Makes sure the device is healthy and presents no threat to the organization or the network.
  - Quickly reacts to threats and disconnects rogue systems from the network in real-time. This responsiveness to constantly changing business needs is a part of Extreme Networks *engaged network* and Juniper Networks UAC solutions.

- **Network partitioning:** Enterprise networks can be divided into zones based upon business needs. This is accomplished with VLANs and firewalls, used together or separately. Network partitioning is an effective way to safely deliver high-quality services to a variety of devices and users, such as IP phones and employees. You can even enable visitors to use your network to reach the Internet and back into their own corporate networks, without giving them access to any of your own business systems or applications.

- **MAC and IP Security:** Sometimes called *wire level* control and security, IP security protects the traffic and systems that control the network, such as Domain Name Service (DNS) servers or Avaya Communication Manager

> software. This protection minimizes exposure to Denial of Service (DoS) attacks, spoofing, and so-called 'man in the middle' attacks, whether they originate outside the network or within it.

One way to think about IP security is that the network has two major layers: the *Routing/Firewall layer*, which connects LANs together and to the outside world, and the *LAN Layer*, which connects end user devices to corporate resources like DHCP servers, DNS servers, databases, applications and, of course, communications systems and applications. Within this LAN layer are edge switches, typically 24 or 48 ports that support PCs and IP phones, and aggregation switches that connect edge switches to the other resources and router/firewalls. Security at this layer ensures that no one can plug a rogue laptop into the network and try to steal information or services from other users.


All devices in a converged network communicate using the TCP/IP network protocol, and to a great extent they all participate in the great realm of threats and vulnerabilities.

# Understanding threats in today's business environment

IP communications has facilitated capabilities unimagined in the past, such as employees' ability to work from remote locations such as homes, WiFi hotspots, hotels, conference venues, and even airplanes, buses and trains.

This is where the big-I Internet comes into play, as an untrusted network, over which business communications and information will be exchanged with a remote worker or branch office. It's never enough to just send data across the network — you need to *protect* it somehow, using means that reflect an intelligent architecture and good use of resources.

## Remote access

Remote access is the mechanism that provides the "just like in the office" connectivity to all of the resources that are normally available to you when you are actually in the office. With remote access you can get to these resources from anywhere in the world, so it's understandably in demand. Understandably,

also, remote access is vulnerable to threats and can place the entire converged network at risk. Any entry point into a network by legitimate users can be targeted by others too, or simply accidentally put sensitive data at risk. (Read any stories in the news lately about a misplaced or stolen laptop? Besides putting whatever files that are on the laptop at risk, such mobile devices may provide easy entry to top-secret confidential files elsewhere in the network.)

People accessing VoIP resources by using either a VoIP phone or softphone need to know their communications are secured. VoIP phones use IPSec VPNs to encrypt traffic from the phone to the PBX (phone switch). The VoIP phone establishes a *VPN tunnel* to one of the head end firewalls to get connected to the corporate network without fear of interference or eavesdroppers.

Softphone users accessing corporate resources need to be authenticated, and checked to ensure that the PC from which they are logging in is not compromised or introducing worms, viruses, or Trojans into the network. This is where technology such as Juniper Networks SSL VPN (clientless access) becomes really important, delivering the performance required for VoIP applications and also ensuring end-point integrity.


Avaya's VPNRemote for 4600 Series software VPN client is built directly into the Avaya IP telephone itself. This enhancement enables you to plug in the Avaya IP phone and use it seamlessly with any broadband Internet connection, such as your home DSL or cable modem connection. You can then experience the same IP telephone features — as if you were using the phone in the office — simply by plugging the phone into your home network.

### *External access*

Remote access is more than just access to the enterprise network for employees, but also access to enterprise applications by others, including suppliers, partners, and customers. Such access provides competitive advantage by streamlining the order and fulfillment of goods and services. But when access to key enterprise applications is provided to users outside of the organization, the risk of security incidents rises proportionally. That, together with the arrival of IP-based voice communications, makes network security a matter of vital importance.

### Internal access

More than half of corporate virus problems originate from within the enterprises network, through employees who inadvertently pass around infected files, USB drives, or by connecting their laptops to their unsecured home networks to work on that important proposal over the weekend. With more mobile employees in a company, the threat of picking up a virus from a laptop that moves back and forth between the office, home, hotels and open WiFi hotspots grows, and UAC/NAC becomes very important.

Protecting the inside of the corporate network is where Extreme Networks' Sentriant Appliance and Juniper Networks UAC and IPS/IDS (what Juniper Networks calls "IDP") solutions can watch network traffic patterns and mitigate the effects of viruses and malicious traffic. Extreme Networks' Sentriant AG also helps to ensure that devices on the network adhere to pre-defined security access policies.

## Partnering for Better Protection

Companies on the cutting edge of converged networking need comprehensive security solutions, not piecemeal approaches. Technologies based on open standards and market-leading products and technologies that can meet the changing network demands of today's enterprise environments give the best value. Avaya's strategic relationships with Juniper Networks and Extreme Networks advances telecommunications and converged network capabilities, making Avaya the front-runner in today's new offerings.

Juniper Networks and Extreme Networks provide state of the art protection against the increasing array of threats, protecting converged networks from internal and external risks.

Avaya's Global Security Consulting Services is your consulting partner whether you need risk assessment, policy development, or network and security architecture — all delivered by seasoned experts, who know Avaya and other brands of network hardware and software.

Chapters 2 and 3 describe Juniper Networks' and Extreme Networks' security approaches and solutions that may just knock your socks off! Chapter 4 aims to *wow!* you with Avaya's security consulting services.

# Chapter 2

# Jumping Juniper Networks: Improving Converged Network Security for All

### *In This Chapter*

- Security for office-based users
- Security for road warriors
- Security for remote workers
- Access control
- Deployment scenarios

Juniper Networks is changing the way people look at securing their converged networks.

Organizations are coming to rely upon their converged enterprise networks for both voice *and* data based communications. Certainly converged networks reduce costs and introduce a multitude of business opportunities, yet converged networks can potentially introduce additional security risks, unless they are designed and deployed properly.

I emphasize *designed properly* — you need to line up strategic partners such as Avaya and Juniper Networks at the start of your converged network project, not after the ribbon-cutting ceremony when someone asks, "Oh, by the way, where's the security?"

Juniper Networks provides an impressive array of converged network infrastructure products, including top-quality leading-edge routing platforms, firewalls, intrusion prevention, application acceleration, and access control solutions. When you're designing the architecture and security of your new or existing converged network, you can look to Juniper Networks products to help build as well as secure the network. This chapter describes Juniper Networks' security solutions that protect converged networks and their services.

# Juniper Networks' Security Solutions

Juniper Networks has the full spectrum of best-in-class security technology for converged networks. This section takes you through each part of the Juniper Networks portfolio, starting with firewalls, IPSec and SSL VPN, intrusion detection and prevention (IDP), and access control. Your tour begins here; follow me please.

## Firewalls and IPSec VPN

Juniper Networks has a nice range of appliances that provide firewall and IPSec VPN capabilities for use in enterprise, branch office, or teleworker setups.

- Secure Services Gateway (SSG) Family.
- NetScreen Firewall/VPN appliances and systems.
- Integrated Security Gateways (ISGs).

Every Juniper Networks firewall and IPSec VPN appliance includes an application layer gateway (ALG). Juniper Networks' ALG improves the security of IP telephony by providing deep-packet inspection of H.323, SIP, SCCP, and MGCP traffic. The ALG dynamically opens pinholes to permit approved IP phone calls through the firewall. All these systems are high-performance devices and provide highly available, low-latency transport for VoIP traffic.

## Intrusion detection and prevention (IDP)

Juniper Networks' state-of-the-art IDP protects networks at both the application and network layers. Juniper Networks' IDP does a lot more in one appliance than several other vendors do separately. Some of the features found in Juniper Networks' IDP include:

- **Day Zero attack prevention:** Juniper Networks' IDP stops worms, Trojans, spyware, key loggers, and other malware dead in their tracks.
- **DoS attack mitigation:** Juniper Networks' IDP products understand over 60 application-level protocols, including SIP and H.323, thereby preventing unauthorized incoming or outgoing phone calls and toll fraud.
- **Rogue server detection:** Juniper Networks' IDP can detect rogue servers on the network, giving network administrators visibility into rogue servers and how they are being used.

## SSL VPN secure remote access

SSL VPNs provide secure remote access without the need for separate client-side VPN software. Juniper Networks offers SSL-based VPN on a wide variety of remote access appliances for every size of organization.

These devices are high-performance devices that ensure that latency and jitter-sensitive applications like VoIP are able to function as expected in this environment. Juniper Networks uses dual mode transport to ensure that the user gets the best connection possible in any environment. This includes trying different types of tunnels (IPSec, SSL) for the best performance and security. Best of all, it's transparent to the user.

Juniper Networks' SSL VPNs are certified to work with Avaya IP telephony products such as IP soft phone and IP agents.

## Network Access Control

Juniper Networks supports several network-based authentication protocols and standards to ensure that only authorized devices and users may connect to the enterprise network. Enterprises have long recognized that unauthorized devices can introduce malware into the organization, thereby threatening the availability of network-based services. Also, unauthorized devices may be an intruder's effort to eavesdrop on network traffic or attempt to access protected information, in either case an attempt to steal information from the organization from the inside.

Juniper Networks has the following means in place to enforce network-level access control:

- **Juniper Networks' UAC** (Unified Access Control) solution supports TNC (Trusted Network Connect), a suite of open standards for network access control developed by the Trusted Computing Group. The TNC specifications are designed to help network administrators solve the difficult task of enforcing security policies for network access in heterogeneous networks with an increasingly diverse mix of devices and software.
- **802.1X authentication,** coupled with Juniper Networks Steel Belted RADIUS (SBR) for placing IP phones and other devices on appropriate VLANs.

Coupled with the Extreme Networks switch that supports LLDP (Link Layer Discovery Protocol), Juniper Networks is able to provide a very comprehensive solution.

## Unified management

A lot of good it would do to implement all of these great security capabilities if there were no consolidated view of it. Consequently, Juniper Networks offers best-in-class centralized management of its security appliances and products that provide comprehensive views of security events, configurations, and performance.

# Security Deployment Scenarios

An easy way to understand how Juniper Networks protects converged networks is to take a deep dive into three common scenarios: office-based users, road warriors, and teleworkers.

You'll see that Juniper Networks can provide firewalls and VPN in all three of these portrayals, and in office-based environments we discuss several additional methods for protecting vital assets.

## Security for office-based users

Juniper Networks' product offerings protect all workers working out of any location — headquarters or campus, branch offices, home offices, or on the road. Most importantly, these products protect all converged network components such as IP PBXs, related converged application servers, and other applications such as e-mail, databases, and so on.


Availability of communications services such as telephone, voice-mail, and contact center apps is typically a 24/7 must-have for businesses. Converting these to IP-based technology exposes them to potential data network threats that must be nipped in the bud to ensure availability and integrity of these critical services.

### Firewalls/VPN

The leader in protecting converged networks, Juniper Networks Netscreen Firewalls are essential for defining and defending network boundaries between and within organizations.

Firewalls work by enforcing network access policy at the device and network service level. Policies specifically permit, or deny, IP communications using specific port numbers to and from endpoint networks or individual devices. Put another way, firewalls block or permit IP packets based only on the source address, destination address, and port number.

Juniper Networks' firewalls have application level gateways (ALGs) in them that dynamically open *pinholes* (really little holes, the packets have to squeeze through sideways) that are present only during specific voice calls. This provides network

protection that is head-and-shoulders above what the other firewall companies can do.


With Juniper Networks' firewalls you can also combine multiple firewalls into a single hardware device. This facilitates internal firewalling or partitioning that better protects networks from internal threats, kind of like bulkhead hatches in a submarine.

Juniper Networks' firewalls have IPSec VPN capabilities built in, eliminating the need for separate VPN appliances. The fewer power cords, the better.

Finally, Juniper Networks' firewalls are right at home in high-availability environments where you have multiple network entrances, front-end routers, and so on — you know, the full-mesh full-meal deal for ultra-high-demand environments. All of these features are critical for today's VoIP environments.

### Intrusion Detection and Prevention

When you plan and design your converged network, you *need* intrusion detection and prevention systems. Juniper Networks offers Intrusion Detection and Prevention (IDP) products that detect and block network-based security threats. Juniper Networks' IDP capabilities are available in dedicated hardware products, and can also be integrated into security gateways as well. Which way to implement IDP depends upon the network's architecture, performance, and security policies. You can put 'em anywhere and everywhere: at the edge, between zones, or wherever. And because they're integrated into Juniper Networks' other products, you need no additional power cords to trip over.


Juniper Networks' IDP solutions protect SIP, H.323, and H.225 services, as well as legacy and traditional network services such as Web and e-mail. It supports multiple methods of attack detection and prevention including stateful signatures, protocol anomalies, backdoor detection, traffic signatures, network honeypot, DoS detection, and so on. It can drop the number of attacks because it can be deployed inline or in sniffer mode. High-performance devices ensure minimal delays in VoIP traffic.

### Unified Access Control

Unified Access Control (UAC) represents an assortment of services that protect an enterprise network by permitting

only known, healthy devices to connect and communicate. UAC prevents unsafe devices such as unpatched "typhoid Mary" laptops from threatening the enterprise with viruses, worms, Trojans, and other digital crud.

UAC works by authenticating and permitting known devices such as laptops, hardphones, and softphones that connect to the network. UAC can also assert and enforce policies in conjunction with the Juniper Networks Netscreen firewall and SSG appliances, to ensure that devices get access to only pre-authorized network resources. No free rides! Further, UAC ensures that such devices have the right settings and characteristics such as anti-virus and device configuration. Think of it is as the automatic equivalent of "You must be *this tall* to use the network."

UAC prevents *inside* threats from disrupting network services inside the network. A common scenario that has played out in many enterprises is the employee's laptop computer that becomes infected with a worm or Trojan while connected to an unprotected network such as public WiFi access point. Then the employee brings the laptop into the enterprise, often bombarding the network with high-speed disruptive attacks that threaten the availability of critical services.

### DoS protection

Denial of Service (DoS) attacks have the potential for rendering any IP-based application or service unavailable for use. Increasingly, such attacks originate from hundreds or thousands of locations, making simple router or firewall filtering impractical and ineffective.

Juniper Networks' high-performance firewalls and IDP appliances ensure protection against DoS attacks by effectively absorbing even the highest volumes of attacks.

### Integrated Security Gateways

Juniper Networks' Integrated Security Gateways (ISGs) can be deployed in-line to protect key voice infrastructure from external attacks. These attacks include Denial of Service (DoS), worms, and Trojans. In addition to firewall capabilities, this product line integrates IDP functionality into the same device. These are data-center–class products designed for rugged enterprise-class service and reliability.

Because ISGs can be installed in-line, often this installation doesn't require an expensive change in the architecture of the enterprise network. Also, installation of the ISG is minimally disruptive because it requires only a couple of patch cord changes in the infrastructure. They're a network engineer's dream!


You can also integrate Juniper Networks' ISG with intrusion detection and prevention. You can plug an IDP blade into the Juniper Networks ISG 2000 and ISG 1000 to get the IDP functionality available in standalone appliances. The Juniper Networks ISG 2000 and ISG 1000 — with integrated, best-in-class IDP — stops worms, Trojans, spyware, malware, and other emerging attacks from penetrating and proliferating through the network.

### Application Layer Gateways

Juniper Networks' Application Layer Gateways (ALGs) provide specific protection for SIP and H.323 gateways. SIP and H.323, the centerpiece protocols for VoIP and other new-media applications, perform a lot of dynamic port activities, which pose a challenge for traditional firewalls. An ALG is needed to ensure maximum protection by permitting only active connections without holding open unused ports as firewalls do. Juniper Networks' ALGs run on all Juniper Networks firewall, VPN, and ISG devices.


Here's how they work: The H.323 and SIP ALGs *negotiate* layer 3 and 4 information, which means they listen to the control connection and dynamically open and close H.323 and SIP ports (also known as pinholes) through the firewall only for the duration of the call. This ability enables a higher level of security within the network because the ports that are needed remain open only for the duration of the call. When the call has ended, or is unexpectedly disconnected, the ports (pinholes) are closed. This system keeps the rest of the ports in deny (block) state, providing significantly tighter access control protection than a traditional firewall. Talk about smart!


For even greater access control protection, administrators can set a policy that blocks calls from certain parties or networks, or that allows calls only from specific partners at specific times. You might call that call blocking on steroids!

### *Zone-based architecture*

Another approach to protecting enterprise networks is to implement zone-based architecture. In a zone-based environment, the network is segregated into physical and logical zones based upon access needs, both within the enterprise and among branch offices, and also external entities such as partners and suppliers.

The security challenge is to segment the network, enabling communications with specific partners and customers, without permitting their access to the rest of the network.

## Establishing network security zones

Rather than running an old-school two-zone (internal, external/Internet) network, you can divide your entire organization into zones based upon business function. You can do this many ways, but here are just a few simple ideas that may help you to figure out what sort of a zone architecture is right for you:

- Separate office networks from data centers. From the perspective of the data center, you can treat the office network as an "external" network with less trust. This option aligns with many organizations that permit their users to install software on their own.
- Separate product development and test networks from the rest of the organization. This option allows for an added measure of control in both directions: You can keep the test environment pristine and free from interference, and you can contain development networks in case the programmers get a little out-of-control.
- Separate manufacturing or customer contact areas. These potentially sensitive areas may require protection not only from the outside world, but may have their own access control policies that are easily enforced through network zones.
- Separate business units. If your organization is large and has semi-autonomous infrastructure management, you can use zone-based architecture almost like boundaries separating the kingdoms within your federation.
- Use a separate extranet zone. If your organization has a lot of interaction with third parties, you can cordon them off in their own zone, where their activities are less prone to disrupt the rest of the enterprise.


There are almost as many ways to design a zone-based architecture as there are ways to arrange the furniture in your living room.

Juniper Networks' firewall and Integrated Security Gateway (ISG) solutions enable inter-zone and intra-zone access, which enables separation of converged network segments to ensure that access policies are applied.

### Eavesdropping prevention with VPN

Users of telephone networks have the expectation that their calls are private and not subject to eavesdropping (except, of course, for legal law enforcement wiretaps). Analog circuit-switched telephone networks are physically separate from data networks and are, for the most part, impervious from the same sorts of threats that are dogging the Internet.

So, one might assume that IP-based phones are less safe than their analog, circuit-switched counterparts because IP phones communicate over data networks, including the Internet.

In reality, IP phones and IP-based communications, even among different organizations (and even when using the Internet as the go-between) are every bit as safe. Designed with security in mind, Avaya phones and soft-phones employ encryption that protects conversations from eavesdropping. Organizations that connect their IP voice networks to one another can (and should!) use VPN technology to encrypt voice traffic as it traverses the Internet.

These encryption technologies make VoIP as safe as (and some would argue even *safer* than) traditional circuit-switched communications. If someone is able to intercept the actual packets in a VoIP conversation, even with a concerted effort it would be exceedingly difficult (and time consuming) to decrypt the conversation and learn what it contained.

Further, road warriors who use SSL VPN are also ensured of encrypted traffic flow from their laptop to the corporate HQ. I go into more detail on protection for road warriors in the following section.

## Juniper Networks supports Avaya's unique solutions

Juniper Networks brings unique and powerful technical advantages to Avaya's capabilities.

- Security features such as firewall, VPN, and other security services can be activated in the JUNOS operating system with a minimal level of impact to the throughput and processing power of the routing platform. This OS is available on all of Juniper Networks' J-series and M-series routing platforms.
- The Avaya IG550 Media Gateway was jointly developed by Avaya and Juniper Networks. This gateway can be installed in Juniper Networks' J-series J4350 and J6350 routers. It permits enterprises to deploy single high-performance platforms that offer firewall, VPN, routing, and IP telephony services all in one box.

These two examples illustrate how Juniper Networks' technical savvy works with Avaya's powerful innovations to put capabilities where they count: into your hands.

# Security for Road Warriors

A growing number of employees today work remotely or while on the road for business — and road warrior employees require the same level of protection as if they were in the office. Juniper Networks provides secure remote access with clientless VPN access through VPN appliances. These connectivity mechanisms work seamlessly with Avaya IP Softphones.

The two types of VPNs available are IPSec VPN and SSL VPN. In addition to IPSec and SSL VPNs, Juniper Networks offers additional encryption using DES, 3DES, and AES encryption, to prevent eavesdropping of data and voice communications between endpoints.

Juniper Networks provides clientless SSL VPN for client connections to enterprise Web and application servers. SSL VPN is the preferred technology of choice for remote connectivity; the advantage here is that Network Managers do not need to worry about maintaining additional client software on users' workstations. SSL VPN technology enables access to applications

including Avaya IP Softphone. This technology also ensures that users get access to network resources from any PC or kiosk (a public Web-connected terminal).

## Security for Teleworkers

Teleworkers work in and on enterprise applications *as though* they were physically on the premises, but they work at home or other locations. They require high-bandwidth access to network-intensive applications, and they need voice communication that is so highly integrated with the enterprise phone system that their location is all but irrelevant. Ten years ago this was a pipe dream, but it's routine for Avaya customers who want such service today.

Because teleworkers' communications often traverse the Internet, their endpoints must be protected from external attack, and their voice and data traffic must be protected from eavesdropping.

Juniper Networks' SSG appliances offer simple, integrated solutions that provide firewall, VPN, and other capabilities including anti-virus, anti-spam, anti-spyware, anti-adware, anti-phishing, Web filtering, and IPS functionality.

### VPN

A VPN connection is needed to protect the communications between the teleworker's workstation(s) and the enterprise, preventing eavesdropping and alteration of transmitted data and voice.

Depending upon what equipment and services are required, a teleworker may have a network-to-network IPSec VPN, where an appliance at the teleworker's location encrypts all traffic between it and a VPN server in the enterprise network, or the teleworker may use an SSL VPN. In either case, all communications between the teleworker's location and headquarters can be automatically and transparently encrypted.

Another common means for encrypting communications is to employ VPN capabilities on the teleworker's workstation and IP phone. A company can use either SSL or IPSec tunneling technologies.

Juniper Networks' branch office SSG (Secure Service Gateway) products offer full firewall and VPN along with UTM and IDP capabilities for teleworkers, including wireless routing capabilities. Avaya IP phones work with all of these VPN capabilities, often seamlessly.

### Firewall

A teleworker's environment needs to be protected against network-based threats that originate in the Internet and are directed towards the teleworker's systems and devices. Because the teleworker is not physically located in the enterprise, their equipment is not protected by the enterprise's firewall(s) and other protective means including IDP.

A Juniper Networks SSG (Secure Service Gateway) firewall appliance can protect all equipment — including workstations and IP phones — from all external threats aimed at the network, providing the same level of protection enjoyed in central enterprise networks.

## Deploying Juniper Networks Solutions

Companies have a lot of ways of putting together converged networks and can choose from a number of ways and means for securing them with solution from Juniper Networks. Working with Avaya, Juniper Networks can make implementation of your chosen path to converged network security a smooth one.

If your organization uses VoIP entirely within the enterprise, then you need to protect its VoIP and converged network infrastructure from common threats:

- **Zone-based security:** Protect the organization's hybrid or IP PBX from non-related traffic and general network threats such as worms and Trojans.
- **DoS protection:** The PBX needs protection from high-volume attacks that can occur internally or reach the PBX from internal and external sources.
- **Unified Access Control:** Protect critical resources and provide end point authentication.

## Corporate Profile: Juniper Networks

Juniper Networks has a cracker-jack development organization that builds purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper Networks to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at `www.juniper.net`.

If the enterprise has connected its VoIP capabilities with external entities, then you need additional protection, such as the following:

- **VPN tunnels:** Employees who require remote access for their IP phones will require IPSec or SSL VPNs so that their IP phones can communicate with the PBX.
- **Application layer gateways:** ALGs provide logical connectivity for VoIP networks residing in branch offices, remote locations, and other places.

In more complex architectures, a variety of choices and solutions are available to solve these same security issues.

# Chapter 3

# Extreme Improvements for Network Security

### *In This Chapter*

- Network access control
- Segmentation
- Threat mitigation

Extreme Networks has what it takes to protect an enterprise network from the inside-out. Extreme Networks builds advanced security features into its switches and routers, and offers some impressive security appliances that protect networks from disrupting security events.

As I explain in Chapter 1, security in a converged network is not just a perimeter challenge, solved with firewalls and IPS — it's also vital to protect the network from within. Security threats don't originate only outside the network, but within it as well. This is why Avaya chose Extreme Networks to be a strategic partner.

Extreme Networks has a rich portfolio of network infrastructure and security devices, ranging from 1U appliances to gigantic enterprise switches (read: lots of blinking lights). Extreme Networks' principal means for protecting networks are *network access control, network segmentation,* and *threat mitigation.*

## Network Access Control

In its product families, Extreme Networks includes powerful access control capabilities that protect your converged network from security and performance problems. By integrating

access control into the network, organizations can breathe a bit easier knowing every port is under their complete control.

Extreme Networks offers many access control options to meet a variety of needs for voice, data, and casual network access. In order to understand the available options, this section provides a brief introduction to access control concepts.

Network access control typically consists of two or three key phases, or steps:

1. The user or device needs to be identified or authenticated. This step might involve a user password, validation of a unique hardware address, or the exchange of other credentials.
2. The system can test the health and configuration of the device to determine whether it meets minimum security policies.
3. After the connection is approved, you may want to limit where the traffic can go and you may need to provide certain services (such as voice priority) to ensure security and performance. I cover that last step in the section "Network Segmentation," later in this chapter.


Extreme Networks uses the term *physical access* to mean the ability for end user devices to connect with and utilize systems and resources that are also connected to the enterprise network. These products don't necessarily prevent someone from physically and literally touching the network equipment and cabling.

## Authenticating users or devices

Authentication is the process of validating the identity of a device or user. This essential first step is necessary before a user or device is permitted to connect to — and communicate on — the network. Just plugging into the Ethernet wall jack doesn't mean you're connected automatically. If you can't get past Extreme Networks' authentication, you're out in the cold or placed into a guest access VLAN (sometimes called a *quarantine* or a *jail*). In a guest VLAN you can have access to mitigation resources or access to specified resources (and hopefully you can call for help). Network administrators have many options when using Extreme Networks solutions.


## 802.1X authentication and Avaya IP phones

Avaya IP phones and PCs connected to the phone's data port can be authenticated separately, receive different port profiles for QoS and security policies, and even communicate over different VLANs.

Ethernet switches can be configured in *single-supplicant* mode or *multi-supplicant* mode. In single-supplicant mode, only the IP phone can be authenticated with 802.1X. In multi-supplicant mode, a PC connected to an IP phone's Ethernet port is required to authenticate via 802.1X separately from the phone that it is attached to.

Extreme Networks uses several methods for authentication to the network; this section describes the key methods.

### 802.1x Authentication

This IEEE-based standard — often referred to as *dot one X* — is the foundation for highly secure access control. 802.1x allows the network to block access while it checks to make sure a connection is authorized. Avaya one-X phones (or other 802.1x-enabled devices) offer a secure way to verify identity that is nearly impossible to spoof. As an added benefit, these solutions easily integrate with existing corporate directory systems for simplified management and operations.

Extreme Networks takes 802.1x authentication a step further by supporting multiple devices or users on the same physical port. This capability is referred to as *multiple supplicant* and simply means that you can secure all the traffic on a single physical port — even if there is more than one device connected to that port. For example, if a computer is plugged into the Ethernet jack of an IP phone, and the IP phone is connected to the network, Extreme Networks' multiple supplicant capability makes sure to authenticate each device and treat the traffic from each device as a different virtual connection.


802.1x is an IEEE standard for port-based network access control. Devices that cannot authenticate to the network are barred from transmitting or receiving frames on the network.

### Local authentication

Extreme Networks switches support a switch-based local authentication, wherein user credentials are maintained directly in the switch hardware through an administrative user interface. This method is useful in smaller environments or as a fallback when 802.1x, RADIUS (Remote Authentication Dial-In User Service), or other external authentication authority is unavailable.

### MAC-based authentication

MAC-based authentication is supported in smaller environments with a limited number of nodes. MAC authentication works by comparing the MAC (hardware) address of the node or device that wishes to connect to the network with a table of permitted MAC addresses stored in memory.


Note that MAC addresses can be spoofed, so MAC-based authentication should not be the *only* means used to authenticate users, but instead as part of a larger security architecture.

### Web-based authentication

For casual access, the user can be presented with a Web-based authentication page that asks the user for a user id and password. The user id and password can be stored locally in the network switch, or the switch can reference a RADIUS, LDAP, Microsoft Active Directory, Sun ONE, or other similar server to confirm authentication.

### Guest access

Unauthorized users such as guests or partners can automatically be placed is a special guest VLAN providing limited network access. For example, you may choose to allow guests to access the Internet but not provide them with access to any internal network resources. A guest-access VLAN helps to keep the IT staff from having to create an account for each person attaching to the network when attending meetings at the company site.

## Discovering your needs automagically

After validating the identity of a user or device, you actually have to do quite a bit more during the authentication process.

The authentication phase is the best time to gather more information about the device or user — after all, you may want to limit or enhance the connection based on what you find out. For example, if the device is a phone, you may want to place that traffic into a virtual network that has a higher priority than other virtual networks. Or you may want to quarantine a laptop if its virus software isn't up to snuff.

Extreme Networks offers some powerful tools to detect more about a user or device, such as the *Link Layer Discovery Protocol (LLDP),* a vendor-neutral protocol that gives a network device a standardized way to proclaim its identity and capabilities to the network. Extreme Networks has adopted and implemented LLDP specifically for Avaya IP handsets, enabling the handsets to be identified, configured, and permitted to access the network, *automagically,* that is, automatically without end-user awareness or involvement.


LLDP is now a formal standard, IEEE 802.1AB-2005. The Multiple Endpoint Discovery (MED) extensions to LLDP have been adopted by the Telecommunications Industry Association as ANSI/TIA-1057. The MED extensions allow security policies to authenticate and treat a combined connection for an IP Phone and PC as *separate devices,* as though they had completely separate physical switch connections. This extra authentication keeps visitors or intruders from being able to access network resources by plugging unknown laptops or mobile devices into Ethernet connections on the back of IP Phones (or even trying to unplug the phone and using its existing network connection for new devices). Extreme Networks finds these stowaways and throws them overboard!


So when you need to add a phone for a visitor from another branch office, no problem: Simply plug in one of these self-announcing phones and it tells the network, "Hello, I'm here!" — and you have a secure end-point for your guest.


The network can still require *users* to authenticate themselves on the network prior to being able to use their IP handsets.

## Host integrity checking

*Host integrity checking* is an emerging technology that works to ensure that each device meets specific configuration requirements and conforms to local security policies. Like a doorman

who looks you over to make sure you're properly dressed for a fancy restaurant, host integrity checking looks over your computer to make sure it won't spoil the network manager's day by infecting the enterprise with some nasty worm or virus. Come to think of it, this could spoil the day for a lot of other people in the organization too.

The Extreme Networks Access Management solution, Sentriant AG, provides much-needed network *quarantine* capabilities, wherein devices such as *sick laptops* (that potentially threaten the integrity of the network) are not permitted to connect to corporate services until such devices conform to policies. If your laptop doesn't play well with others, Extreme Networks won't let it play on your network.


Users whose laptops don't meet site-specified requirements can be directed to a download page where they are required to download and install needed components before being permitted access to the network.

# Network Segmentation

For performance and security reasons, companies may need to logically separate voice and data networks from one another. It's not that they don't get along, but rather because their security and performance needs are different. Extreme Networks has several techniques available for accomplishing this goal.

## Virtual LANs

Extreme Networks' *VLAN* (Virtual LAN) implementation permits the separation of voice and data traffic on the network. This enables logically-separate networks to share the same physical network wiring, while maintaining logical separation needed to meet performance and security needs. This would be like putting all of your clothes in the same load of laundry, white clothes and colored clothes together, but having the washer and the soap treat each kind of clothes distinctly, so that everything turned out perfectly.


VLANs are logically-partitioned networks that exist on a single physical network. VLANs permit network architecture changes without having to change anything physical such as network wiring.


IEEE 802.1Q is the dominant standard for the definition and management of VLANs.

## Wire-speed encryption

Encryption is an even stronger technique for segregating traffic on a single physical network. When you want to protect traffic between two sites within a network, between two buildings on a campus, or even between two buildings across a WAN, encryption is essential. Yet encryption is often associated with performance degradation. Not so with Extreme Networks. With wire-speed encryption, sensitive network traffic is routed to an Extreme Networks Sentriant CE150 security appliance for gigabit speed, full-duplex encryption while less sensitive traffic flows directly to the network.


The Sentriant CE150 supports several forms of encryption, including AES: FIPS 197 (128, 192, 256 bit keys) and 3DES: ANSI X.952 (168 bit keys).

## Access control lists

Extreme Networks switches support robust, dynamic *access control lists* (ACLs). Extreme Networks products support ACLs at *wire speed* so that enterprises don't get penalized in performance for implementing numerous access lists. This versatile security measure gives you the power to control traffic based on application, IP addresses, ports, or pretty much anything else you see in the data packet's header. An enterprise can use ACLs to prevent unwanted traffic from being delivered to IP phones and other converged network equipment.

One interesting application for ACLs is the creation of *whitelists* (lists of permitted devices) that enable you to specify which phones or devices are permitted on a given LAN.

# Threat Mitigation

Remember, threats don't just originate "out there" on the Internet, but sometimes "in here" — as in from within the enterprise network. Infections and other trouble can originate inside the network, whether from a visitor's wireless PDA or even on trusted laptops if someone inadvertently opens an infected application from a USB key or MP3 player. Extreme

Networks has two remedies for this: IP security and Virtualized Security Resources. Extreme Networks' threat mitigation capabilities make an essential contribution to Extreme Networks' extraordinary performance under duress.

## IP and MAC security

When technologies like Ethernet and IP were first designed, the trust and integrity of the infrastructure services was a given. History has proven that to be a short-sighted assumption. In response, Extreme Networks has devised several methods that prevent an attacker from undermining IP command and control protocols and compromising the network. In each case, Extreme Networks beefs up well-known and open services that have been around for years:

- **Trusted DHCP:** Prevents untrusted or rogue DHCP servers from interfering with network operation.
- **Gratuitous ARP (Address Resolution Protocol) identification:** Prevents ARP cache poisoning that can disrupt network communication.
- **ARP validation:** Prevents ARP-based man-in-the-middle attacks.
- **Disabled ARP learning:** Also prevents ARP cache poisoning that disrupts network communications.
- **Source IP lockdown:** Prevents IP spoofing by rogue network nodes.
- **MAC limits:** Prevent unauthorized access and MAC address spoofing.

These methods prevent many types of malicious attacks from occurring on the network, including those which can interfere with, or permit eavesdropping on, VoIP services.

## Virtualized Security Resources

Extreme Networks' revolutionary Virtualized Security Resources (VSR) model mitigates threats across the organization by engaging the network to project advanced security capabilities across the infrastructure. As a result, you avoid excessive costs by enabling the network to share the security burden, and you eliminate availability risks by avoiding in-line

security approaches. You also enjoy lightening-fast responsiveness to emerging threats with a solution that quickly identifies, analyzes, and classifies new threats by using advanced techniques to confront specific types of attacks.

Virtualized Security Resources work by allowing specialized, dedicated security solutions to engage the network for detection and enforcement of security events. This approach frees up the security resource to focus on the more challenging tasks of analysis and decision-making.

Sentriant (see Figure 3-1) is an exciting example of how a VSR can extend protection across the entire network. Sentriant uses advanced analysis techniques to accurately identify rapidly-propagating attacks such as Day Zero attacks and rapidly spreading worms. Sentriant receives anomalies from CLEAR-Flow (Extreme Networks' hardware-based, switch-integrated instrumentation capability), makes on-the-spot decisions, and then tells the switch whether to permit the traffic to continue, quarantine it to a specific LAN, or shut down the port completely.

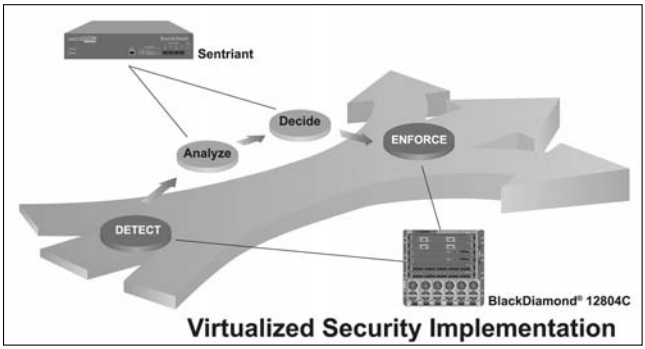



**Figure 3-1:** Sentriant is the key engine that starts Extreme Networks' intrusion detection capabilities.

# Deploying Extreme Networks Solutions

Because networks can be designed and deployed many ways, Extreme Networks has products that provide connectivity and security for all sorts of enterprises.

## Corporate Profile: Extreme Networks, Inc.

Extreme Networks designs, builds, and installs Ethernet infrastructure solutions that help solve the toughest business communications challenges. The company's commitment to open networking sets it apart from the alternatives by delivering meaningful insight and unprecedented control to applications and services. Extreme Networks believes openness is the best foundation for growth, freedom, flexibility, and choice. The company focuses on enterprises and service providers who demand high performance, converged networks that support voice, video and data over a wired and wireless infrastructure.

Organizations that use VoIP need to protect their converged network from security threats:

- **Network Access Control:** Secure authentication from Extreme Networks ensures that only known, trusted, healthy devices may connect to the enterprise network. LLDP permits Avaya handsets and softphones to authenticate to the network automatically.
- **Network Segmentation:** Extreme Networks' VLANs and Access Control lists ensure that latency-sensitive voice and video communications function well and unimpeded. Wire-speed encryption protects sensitive communications including voice and video.
- **Threat Mitigation:** IP address security and Virtualized Security Resources combine to deliver a network that's uniquely capable of mitigating attacks that threaten the network interior. Enhanced IP security features strengthen conventional services such as DHCP and ARP. As a result, you enjoy unparalleled network uptime and great performance under duress (of the network kind; if you are under pressure to get that status report done — sorry, you're on your own).

Extreme Networks has the network and security products and features that fit every type and size of organization.

# Chapter 4

# Plans, Policies, and Avaya Security Services

*In This Chapter*

- Protecting increasingly complex networks
- Dealing with the growing tide of regulation
- Recognizing that no network is an island

The way-cool advances in network technology are really a boon to businesses that use them. However, down at the nuts-and-bolts level, implementing and protecting these networks is getting harder. You need more than a man (or woman) with a badge; you need help from Avaya's Security Consulting Services.

## Understanding Avaya's Security Consulting Services

As you pile more complicated services such as VoIP onto your data networks, securing those networks is a lot more scientific than it used to be. Avaya Security Consulting Services helps you create and maintain secure network infrastructures for converged networks.

Unauthorized access to sensitive data and resources is an increasingly serious concern for today's businesses. Today, more information — and *more sensitive* information — is shared by greater numbers of people. Network security has become critical, often all the way to the boardroom level.

Avaya Global Services has expertise not just with voice and data networks, but also in converged technologies in multi-vendor network environments. Whether you're using IP-enabled PBX applications, IP Telephony, VoIP, Unified Messaging, or Customer Service applications, Avaya Global Services provides a solid platform of services that protect all your enterprise information and network assets.

Avaya's Security Consulting Services performs three primary services:

- **Security Assessment:** Avaya performs a comprehensive review of your current network security posture. This assessment helps identify the security vulnerabilities that exist, where they are, and how to fix them.
- **Security Policy Development:** Avaya helps develop a network security policy that will most effectively protect your assets and intellectual property with minimal disruption to your business operations.
- **Security Architecture & Design:** Avaya develops the blueprint for a successful security infrastructure implementation.

# Why You Need Avaya's Security Consulting Services

Today's semipermeable networks have more complex architectures, involve active and frequent communications with outside entities such as customers and suppliers, and are by their nature more difficult to protect. Many organizations don't have the expertise to go it alone. Avaya's Security Consulting Services understands these challenges and is prepared to meet them.

## New services introduce new vulnerabilities

As services are added to the enterprise network, the number of vulnerabilities increases proportionally, if not exponentially. The vulnerabilities increase further when these services

are made available to those who are physically outside of the organization: remote access, VoIP, web applications, and extranets all can make networks more vulnerable, unless they are properly secured.

Rather than focus on point solutions for protecting each new service, Avaya considers the big picture and develops holistic security solutions that protect your converged network and the vital services that it supports.

## Expertise

Gone are the days when building a network meant plugging all of the workstations and servers into big hubs, and implementing a router ACL or simple firewall for the Internet connection. Although the convergence of voice, data, and multimedia services is making overall business environments simpler, the networks themselves are becoming more complicated.

Avaya's Security Consulting Services engineers and architects have expertise with not only Avaya equipment but with all vendors' products.

## Regulation

In the 1990s in most industries, securing networks meant doing just enough to stay out of the newspaper headlines with news of the latest big security breach. Sure, even then, security was a good idea, but one fundamental change has occurred: *security is now the law*.


Another key change is that systems such as voice mail, IVRs, and IM applications, as well as recorded conversations in call centers, can become part of your corporate electronic record once recorded, and are therefore governed by many of these data security, protection, and retention policies.

For example, some of the more prominent data security regulations that you need to be aware of include:

- **GLBA (Gramm-Leach-Bliley Act)** requires all financial services companies to adequately protect their customers' private information from improper disclosure.

- **HIPAA (Health Insurance Portability and Accountability Act)**, in particular its Security Rule, requires all institutions that store or process medical information provide specific means for protecting that information.
- **Sarbanes-Oxley** requires a high degree of integrity in an organization's financial accounting applications and all supporting infrastructure.
- **PDD-63 (Presidential Decision Directive-63)** requires protection of national critical infrastructures such as telecommunications, utilities, banking and financial systems, and transportation.

I could list more, but you get the idea.

There are also a number of regulations imposed by organizations and industry groups, most notably the PCI DSS (Payment Card Industry Data Security Standard), which applies to all online merchants and other organizations that store or transmit credit card numbers, requires specific and comprehensive safeguards on credit card numbers and related information.

Many of these regulations require or imply the use of regular internal or external auditing, and/or the preparation of reports of compliance to relevant governing bodies.

Knowing how to be in compliance with these regulations requires considerable expertise. Using guidance from your organization's legal department, Avaya's. Security Consulting Services can help get your systems and networks into compliance.

## Even old technology is still important

If you carefully consider how to secure your network by configuring your firewalls, routers, IPS/IDS and network LAN switches, you're off to a good start. But in truth, you've really only scratched the surface when it comes to security planning.

Converged network security planning means also considering how to secure all the devices and applications that are connected to that network. You need to determine how to secure

systems at the operating system level, enable security and encryption features on wireless LAN access points, and encrypt VoIP traffic moving between IP phones and IP PBX systems. Then you may wonder: What about all the non-IP stuff still in the system?

Even though the world is moving towards end-to-end IP networks for all sorts of services, you probably still have connections to the public switched telephone network (PSTN) for long-distance services, and perhaps even inbound and toll-free lines that enable outsiders to access many of your communications systems, especially voice-mail systems, audio-conferencing bridges, and fax machines.

Just because you're migrating an old PBX system to a new IP telephony solution doesn't mean you can stop worrying about things like theft of service from unauthorized use of network bandwidth, toll fraud, and subscription fraud — in addition to threats of service disruption and privacy issues.

Avaya's consulting and systems integration experts look at your entire network, not just the data network elements, and can help you identify places where your communications applications may still be exposed to misuse and fraud, even if you've locked down the IP network. So, you don't have to worry that someone may use your audio bridge or Web conferencing system to plan parties with their friends — and on your dime.


Access to network services is more important than ever, and yet the network perimeter is becoming almost impossible to define. Intranets, extranets, VPNs and other remote access services blur the definition of a trusted user, and critical corporate data may be located on handhelds, laptops, thumbdrives, phone — anywhere.

# WE'RE AT THE HEART OF OVER A MILLION COMPANIES WORLDWIDE.

# IS YOURS NEXT?

Avaya is the world leader in IP Telephony, Mobility Solutions and Contact Centers.

But really, we're revolutionaries at heart.

Avaya not only delivers the reliability and robustness of voice—we embed it right at the heart of business.

Let us assess your network for VoIP readiness. Let us show you how embedded communications can transform your business.

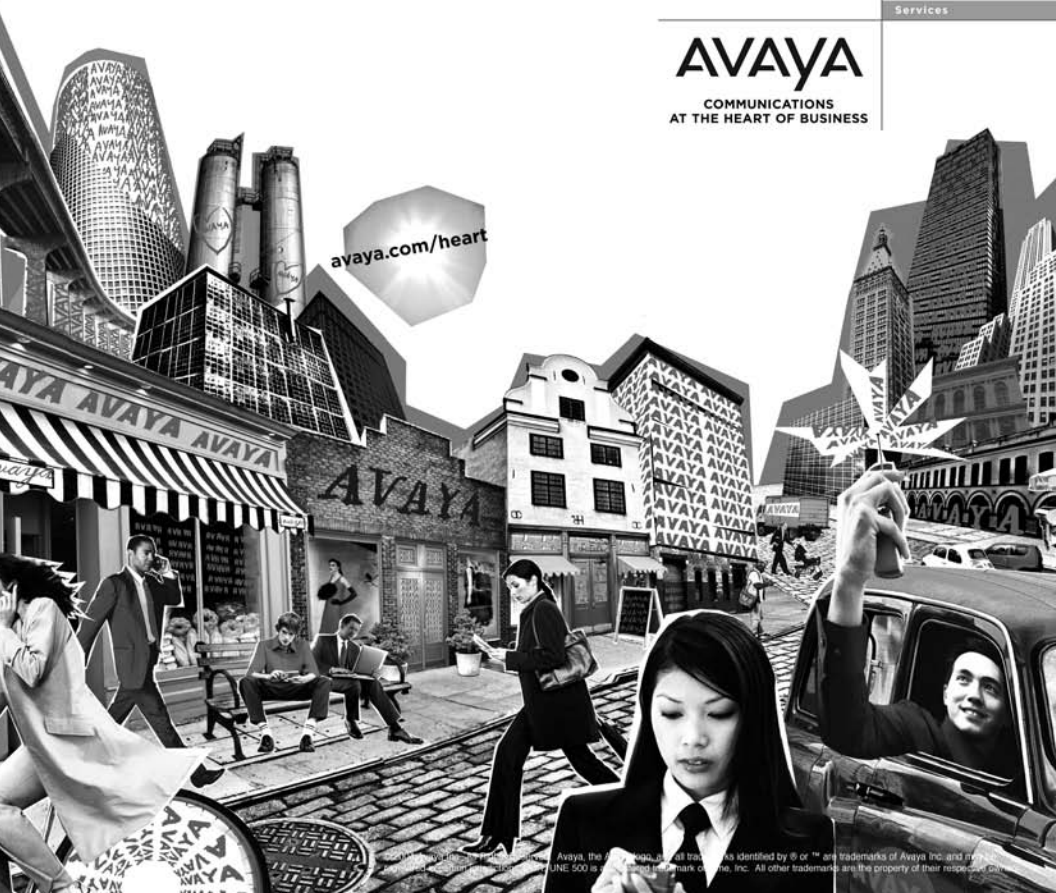
Go to avaya.com/heart for more possibilities.

Some may actually quicken your pulse.

IP Telephony
Contact Centers
Mobility
Services

AVAYA

COMMUNICATIONS
AT THE HEART OF BUSINESS



**Protect your mission-critical communications systems and networks from harm**

## Is your converged voice, video, and data network safe from threats, both internal and external?

This Avaya custom edition of *Converged Network Security For Dummies* shows you how to protect the communications and business application assets that you rely on to run your business. Find out how Avaya Strategic Alliance partners Juniper Networks and Extreme Networks provide multi-layered, industry-leading security infrastructures — and how Avaya Security Services can help you assess, deploy, and ultimately protect your networks. As an IT manager or decision-maker, you'll appreciate the way that these converged network security solutions protect your corporate assets and infrastructure not only from external threats but also from threats within the ever-more-mobile business environment.

And once you've secured your converged network, check out Avaya's limited edition of *VoIP Security For Dummies* for more hints on how to effectively secure your Avaya IP Telephony solutions. Available from www.avaya.com.

## Discover how to:

- ***Ensure that security spans the entire enterprise network***
- ***Use Juniper Networks and Extreme Networks comprehensive security solutions for converged networks***
- ***Extend remote access to employees without compromising security***
- ***Develop converged network security policies with Avaya Security Services***

THE DUMMIES WAY®

- *Explanations in plain English*
- *"Get in, get out" information*
- *Icons and other navigational aids*
- *Top ten lists*
- *A dash of humor and fun*

## Get smart! @www.dummies.com

- *Find listings of all our books*
- *Choose from many different subject categories*
- *Sign up for eTips at etips.dummies.com*

**ISBN:978-0-470-12098-9**
**Avaya Part #: SVC3359**
**Not resaleable**

BICENTENNIAL 1807 WILEY 2007 BICENTENNIAL

**For Dummies®**
A Branded Imprint of
WILEY