

# SECURITY

## White Paper

### Security for service provider VoIP networks

*Industry solutions to address end-to-end network security requirements for mass deployment of voice over IP (VoIP)*

## Executive summary

Forward-thinking service providers are seeking to capitalize on the advantages of voice over IP (VoIP) services, but the real world is not a friendly place for VoIP networks. All components of a VoIP infrastructure are targets, even from internal threats. Attempted attacks are inevitable, so protections are imperative. Yet delay-sensitive voice traffic cannot be compromised by processing-intensive security measures.

Fortunately, there are pragmatic and proven answers to all these challenges. Security mechanisms can be implemented into service provider VoIP networks at multiple levels—protecting against these cyber-threats without adding undue latency to delay-sensitive voice traffic or complexity to user login procedures, network architecture, or network administration.

Singly and in combination, the security mechanisms described in this document contribute to an overall security architecture that protects the VoIP network from service disruption, theft of service, and privacy violations at multiple levels:

- **At the network segment level**, isolating critical elements of the solution wherever possible
- **At the traffic level**, to sustain integrity even if perimeter measures are compromised
- **At the element level**, whereby key telephony servers are hardened against attacks

Together, these measures enable service provider VoIP networks to be open and accessible for legitimate subscriber services, but not wide open for inappropriate or malicious uses.

Nortel Networks commitment to and active participation in various forums and working groups helps align our security strategy with our customers' needs, and drives interoperability across platforms and solutions. Nortel Networks is actively involved in security-related activities with such groups as the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU), the European Telecommunications Standards Institute (ETSI), Cablelabs' PacketCable, Committee T1, and the U.S. Department of Homeland Security.

Read on for more about how service providers can apply security mechanisms to VoIP networks, to enjoy all the advantages of this emerging revenue service while mitigating the risks.

## Voice over IP has grown up. It's time for carriers to *really* put it to work.

Voice over IP (VoIP) has come a long way since the first rudimentary applications provided erratic yet free phone calls over the unmanaged Internet.

For one, voice quality on controlled IP backbones and private networks can now emulate the public switched telephone network (PSTN). Newer voice codecs (coder/decoders) deliver PSTN-grade voice quality yet consume a fraction of the bandwidth required by traditional TDM networks. The technology is available today—the clients, softswitches, SIP proxies, media gateways, and application servers—to deliver complete Class 5 telephony services on a converged packet infrastructure more cost effectively than the PSTN.

The maturity of VoIP standards and quality of service (QoS) on IP networks opens up new possibilities for carrier applications:

- Running voice services over IP maximizes network efficiency, streamlines the network architecture, offers the potential to reduce capital and operating costs, and opens up new service opportunities.
- VoIP makes it easier and more economical to extend service to remote locations over cost-effective IP links.
- VoIP enables new multimedia service opportunities, such as Web-enabled multimedia conferencing, unified messaging, and PC-based call management.
- With multiple services available on a single customer link, service providers have lots of opportunities to bundle services.
- The IP infrastructure makes development and deployment of these services much faster than in traditional circuit-switched networks.

For all these advantages—and the opportunity to trim operating costs by more than 30 percent, according to Nortel Networks business case research—it's no surprise that all major carriers and many enterprises have implemented IP Telephony to some degree. These deployments will continue to grow as more and more networks converge. Danny Klein, Senior Analyst at the Yankee Group projects a compound annual growth rate of 58 percent as the global carrier VoIP equipment market grows from slightly over \$2 billion in 2003 to nearly \$13.8 billion in 2007.

## Is there a dark lining to this silver cloud?

VoIP offers compelling advantages, but it also presents a security paradox. The very openness and ubiquity that make IP networks such powerful business tools also make them a liability. The ports and portals that welcome legitimate subscribers into the service provider network also potentially welcome hackers and others who would misappropriate network resources for personal gain.

Nortel Networks Baseline Security Standards specify a set of capabilities to provide secure management across packet networks—and how to implement the capabilities. Security standards provide consistent functionality, reduce training costs, and accelerate the introduction of new security capabilities across the network.

Details on these standards can be found at: <http://www.nortelnetworks.com/solutions/securenet/snf/index.html>

## Extending VoIP across network boundaries

If carriers and their customers are to realize the full benefits of VoIP, they must be able to directly connect networks together, packet to packet, without converting to TDM (time division multiplexing). Direct packet interconnect improves service quality while lowering complexity and costs—but it raises some new issues. How does traffic traverse the stringent border protections that protect VoIP networks, such as firewalls and network address translation?

Here's where VoIP border control comes in. VoIP border control devices supervise the signaling and media streams entering or exiting your VoIP network—and satisfy critical requirements for security, service assurance, interoperability, and IP address translation in directly connecting VoIP networks.

Download our 10-page, illustrated white paper that discusses the functions of VoIP border control, the approaches being taken by major softswitch vendors and others, and which strategy might be most suitable for your VoIP interconnect needs.

*Eliminating Boundaries*—Nortel Networks Publication  
Number NN107880-041404

<http://www.nortelnetworks.com/products/01/succession/cs/softswitch/collateral/nn107880-041404.pdf>

When you start talking security, VoIP frequently gets a bad rap. “I see VoIP and SIP vulnerability as a huge problem,” Jim Louderback wrote in *eWEEK* (May 12, 2004). “Without a robust security infrastructure, Internet-based voice traffic is vulnerable to all kinds of monkey business.”

Just ask the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI). Their 2001 survey of more than 500 information security professionals showed that almost one-third of them (primarily large corporations and government agencies), had detected computer security breaches within the previous year. Half of them reported financial losses from the computer break-ins, and those who were willing and able to tally the cost reported losses of more than \$123 million.

*eWEEK*'s editor of VoIP & Telephony, Ellen Muraskin, contends that VoIP can be as secure as you want to make it—just as secure as traditional voice, with the right mechanisms in place (eWeek, May 14, 2004). “When voice is sent as IP-encapsulated data, it relies on the same firewalls, intrusion detection systems, VPN technology, authentication, and partition safeguards as data networks, and is as secure as that data.”

## What are the risks?

Attackers have three primary objectives when seeking to compromise a network: disruption of service, theft of service, and violation of privacy. They have a broad repertoire of tools and techniques they can use to achieve these aims. With their various tools of the trade, attackers can launch multi-level attacks to access the network—creating an access hole to intrude upon the network, and then using secondary attacks to exploit other parts of the network. Here's a sampling of hackers' favorite techniques:

- Attackers can take advantage of weak user authentication and authorization tools, improper allocation of hidden space, shared privileges among applications, or even sloppy employee habits to gain **unauthorized access** to network resources.
- They can disable a trusted host and assume its identity, a threat known as **IP spoofing** or **session hijacking**.
- Using sophisticated new **network sniffers** that can decode data from plain text packets across all layers of the OSI model, hackers can steal user names and passwords, and use that information to launch deeper attacks.
- **Denial of Service (DoS) attacks** flood a network with illegitimate requests and thereby prevent legitimate users from accessing their service.
- In **bucket brigade attacks**, also known as “man-in-the-middle” assaults, the attacker intercepts messages in a public key exchange between a server and a client, retransmits the messages substituting their public key, and in the process tricks the original entities/users into thinking they are communicating with each other.
- **Back door entries** to access network resources can be accidentally or intentionally opened by users and procedural oversights.
- **Masquerading** enables a hacker to pose as a subscriber to illicitly get services, or to pose as a valid administrator or engineer to access the network, often to elevate user privileges.

The good news is that security mechanisms can be implemented into carrier VoIP networks at multiple levels—protecting against these threats without adding undue complexity to user login procedures, network architecture, or network administration.

## The evolution of IP security

In olden times, an IP network was protected like a medieval castle—a walled domain surrounded by a moat. Security relied on sustaining a private domain and restricting access to authorized internal users only. In this enterprise model, intruders were kept in check by access controls; business partners and customers were excluded from the network altogether; and hacking from internal workstations was presumed to be unlikely or trivial.

This innocent model of perimeter security is obsolete even for enterprises, who now must openly grant network access to suppliers, partners, customers, and others. And of course, that model wouldn't have been relevant in the first place for service providers, who by default must invite “untrusted” outsiders into their networks.

That's why Nortel Networks regards multi-level, comprehensive network security as a fundamental requirement of any network architecture solution—and particularly critical for service provider VoIP networks. As a result, we have created our carrier VoIP products around a holistic security strategy based on these key precepts:

- IP Telephony can be at least as secure, and potentially more secure, than traditional telephony and IP data networks—overcoming the challenges of keeping latency at acceptable levels for voice.
- Security provisions shall permeate the network architecture at multiple levels, built into the very DNA of the network and integrated into network products.
- Standalone security devices will be available as interim solutions, to provide deployment choice, and to integrate unsecured third-party products.
- Our active participation in shaping industry standards—and support for emerging standards in our VoIP products—will facilitate openness and third-party interoperability.

The following sections describe some available solutions and best practices for protecting service provider VoIP networks, with an example of how this strategy has been implemented with Nortel Networks carrier VoIP solutions.

## Security protections at three primary levels

Traditional public voice networks physically separate voice/data (bearer) traffic from management traffic and from control/signaling. Today's service provider IP networks can logically separate bearer traffic from management traffic from signaling traffic, while providing stringent access control, user authentication, and encryption.

This logical isolation and protection of network segments, devices, and users is accomplished through a variety of different mechanisms, such as firewalls, authentication, encryption, proxy servers, network address translation (NAT), and more. (Descriptions of these security mechanisms are found in the appendix to this document, "Primary security mechanisms to protect VoIP networks.")

Singly and in combination, these various security mechanisms contribute to an overall security architecture that protects the VoIP network from service disruption, theft of service, and privacy violations at three key levels:

- **Network segment level**—Network segmentation isolates critical elements of the solution, wherever possible, using such mechanisms as packet filters, firewalls, routing restrictions, and traffic segregation.
- **Traffic level**—Traffic security and peer-entity authentication sustains the integrity of the network even if perimeter measures are compromised, using such measures as encryption and secure protocols on management, call control signaling, and media planes.
- **Element level**—Key telephony servers are protected through platform hardening, separation of management functions from service-critical functions, and tight access control and user authentication, authorization, and accounting.

When security mechanisms are implemented at multiple levels in this framework, each security level builds upon the capabilities of the layer below and provides finer-grained security the closer you get to critical network resources.

*An effective security architecture melds security mechanisms at multiple levels to protect network activities that have highly variable security requirements—from subscriber services to call control signaling to network operations.*

## Security mechanisms at the network level

### *Partition the network into isolated segments.*

The practice of creating private domains—castles surrounded by moats—is still an important way to protect a network, but now the real-world approach is to create something of a community of castles and moats, where legitimate traffic is allowed across guarded drawbridges, with caution but without delay.

Network segregation enables providers to balance the protection value of isolation with the necessity for interaction among network segments. A variety of mechanisms, such as packet filters, firewalls, routing restrictions through VLANs and VPNs, route export filtering, traffic segregation, and anti-spoofing measures work together to provide concentric circles of defense around key VoIP components.

In a secure service provider VoIP network, VLANs organize the service provider's architecture into discrete and logically separate areas for access/aggregation, services, call processing, media processing, and network operations. Each of those network segments naturally has different access needs, traffic types, and user authorizations, so segregating these functions protects them without impeding their usefulness.

Increased security can be achieved by further segregation using virtual separation of VoIP traffic into the service provider's core network using IP-VPNs or MPLS tunnels. Access to the IP core can be controlled by a dedicated firewall and proxies. Only valid VoIP protocols, RTP media streams, and corresponding OAM traffic would be allowed through. Firewalls and proxies throttle excessive or inappropriate traffic to thwart Denial of Service (DoS) attacks.

### *Provide secure access to the wild 'n woolly Internet.*

The ubiquity and anonymity of the Internet make it a fertile ground for cyber-attacks. As a result, service providers will need extra layers of isolation between Web access and VoIP network functions. The same mechanisms that protect VoIP traffic on managed IP networks apply here, but the provisions should be more stringent, coordinated on a secure service control platform.

- Firewalls filter traffic between the Web and an access/aggregation VLAN, and also between the access/aggregation VLAN and the LAN that hosts the service provider's VoIP elements.
- Media proxy servers transparently handle all incoming and outgoing traffic, preventing any direct routing of traffic between subscribers and the Web.

## *Security principles in action*

### **A sample network segmentation strategy in Nortel Networks carrier VoIP architecture**

In a secure Nortel Networks carrier VoIP network, a Communication Server LAN (CS-LAN) is used to provide internal communications among network elements in the physically secure Communication Server complex. Redundant Passport 8600 Multiservice Switches segregate network layers by function and degree of protection required. The Passport 8600 Multiservice Switches also provide high-performance packet filtering to regulate traffic entering or leaving the CS-LAN.

The CS-LAN is segregated into several subnets, which are enforced with VLANs. For example, all call processing elements are contained in a call processing subnet, optional media components reside in a media subnet, and element management systems reside in an OAM&P subnet. Traffic between various subnets is strictly controlled by the Passport 8600 to create a full, logical separation and guard against unauthorized access.

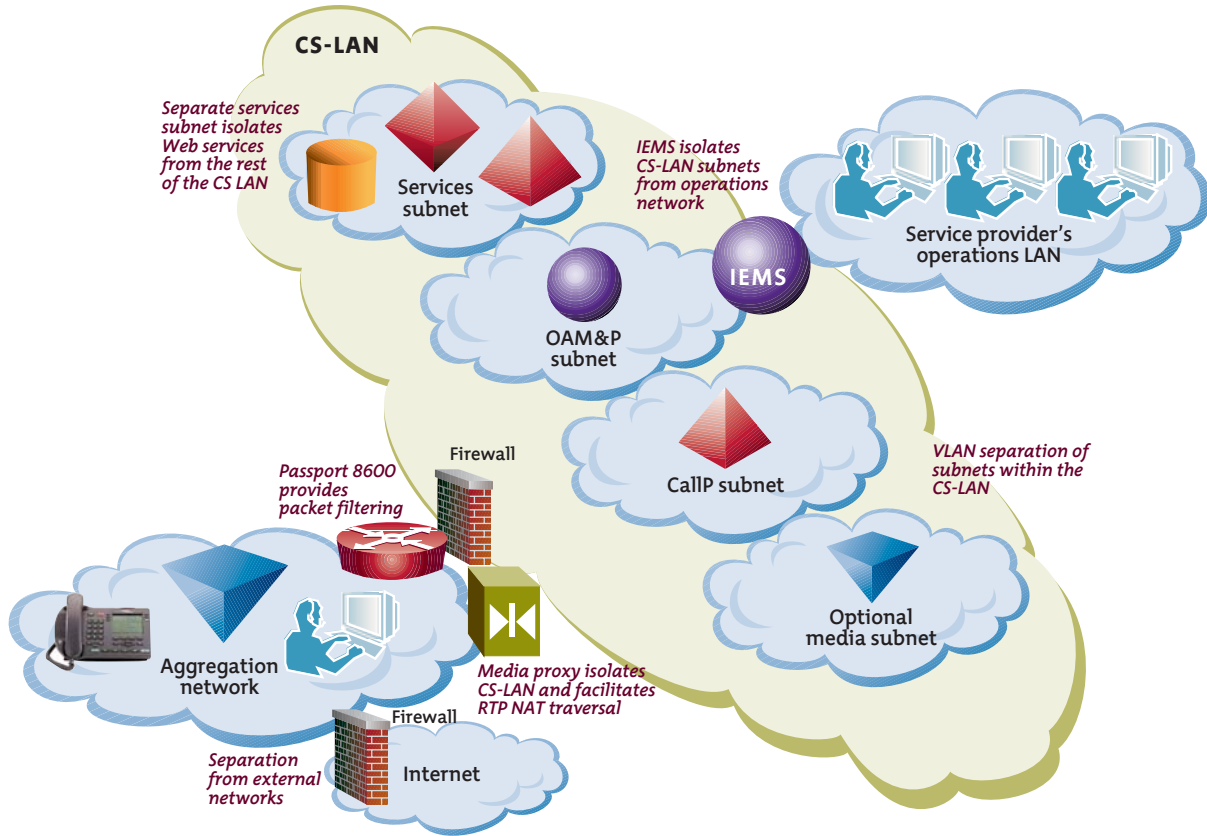
Only valid call signaling, media, and OAM traffic can reach the servers that process that traffic. Traffic among Succession VoIP components is isolated from traffic between external devices and Succession servers—a practice that limits the types of traffic to which key telephony servers are exposed, and minimizes the opportunity for attack.

Furthermore, certain types of traffic are regulated by proxies between the CS-LAN subnets. For example, all access to call processing (CallP) and media subnets from the network operations center (NOC) must be proxied by element management systems (EMSs) through secure, authenticated interfaces. In this manner, key call processing functions are protected even from internal threats.

Add physical security around CS-LAN interfaces—along with complementary security features, such as authentication, encryption, and stateful firewall capabilities at the demarcation points between remote VoIP POPs/aggregation networks and the core VoIP network—and this network architecture provides a solid level of security inside and outside the CS-LAN.

- Security features intrinsic to HTTP (Hyper-Text Transfer Protocol) and server authentication functions provide added protections.
- Secure user authentication, such as password/username login, coupled with device identification, protect against spoofing, aliasing, and other forms of unauthorized access.
- Platform and service hardening ensure that even if threats manage to pass through these other security provisions, their impact will be minimized and mitigated.
- Vulnerability testing ensures that hardened platforms and network configurations are resilient to external attacks.

Figure 1. How does CS-LAN protect the Succession solution?



## Security mechanisms at the traffic level

### *Make sure subscribers really are who they say they are.*

Sadly, subscribers must be assumed to be untrusted, from a service provider point of view. For authentication purposes, you can't rely on data that can be easily modified or tampered. You have to assume that subscribers may try to appropriate services wherever possible, network devices might not really be what they claim to be, and that many other attacks may come from networks that are not under your direct control.

The good news is that these risks can be effectively mitigated through various mechanisms, such as the following:

- Anti-spoofing packet filters in the network minimize IP address spoofing.
- Users can be positively identified using challenge-response-based SIP client authentication.
- Transport Layer Security (TLS) provides data encryption for SIP traffic.
- Strong authentication, protocol integrity, and confidentiality protect Centrex IP clients.
- IPSec call signalling authentication and integrity applied to other protocols.

### *Protect signaling and management traffic as it traverses the network.*

Since tampering with network traffic is common in IP networks, the call control signaling, OAM, and even RTP traffic that traverses potentially hostile networks must be protected. This security is provided through multiple mechanisms:

- Physical and logical segregation of network traffic, as described earlier
- Encryption using SSL or TLS for SIP, IPSec, or SSH (Secure SHell) authentication for other call signaling, and SRTP (Secure Real-time Transport Protocol) for RTP traffic

## Security mechanisms at the element level

### *Make sure that operations personnel really are who they say they are.*

Since network operators/administrators have access to sensitive network functions, they must be subject to the most stringent access controls. During authentication, users identify themselves to the network, using any number of methods, such as permanent or one-time passwords, biometric techniques, smart cards, and certificates—singly or in combination.

During authorization, the network determines the authenticated user's level of privileges (what systems they can access, what functions they can perform) based on their identity, as defined in policy. Access control techniques based on RADIUS (Remote Authentication Dial-In User Service) servers provide a fundamental level of access control. An additional LDAP (Lightweight Directory Access Protocol) server can provide more fine-grained access control if necessary. VPNs prevent unauthorized access to OAM functions from remote users.

In defining access privileges on all ports and devices, the concept of "least privilege" should be applied, granting access only as needed.

The system should perform session management per user after the user is authenticated—and use flexible configuration and policy enforcement with fine-grained rules, capable of dealing with specific objects. Unique accounts for each administrator should be used, with accountability for actions traceable to individuals, to provide for appropriate monitoring, accounting, and secure audit trails.

### *Isolate operations, administration, and management (OAM) functions.*

Network segregation—using any of the methods described earlier, including physical controls—isolates critical OAM functions from other network subnets. Element management systems (EMSs) create a demilitarized zone between an OAM subnet and the service provider's operations systems (OSs) and network operations center (NOC).

Strong operator authentication and access control mechanisms, described earlier, prevent unauthorized access to sensitive OAM capabilities. VPNs prevent unauthorized access to OAM functions from remote users.

A firewall or proxy can authenticate and allow only legitimate protocols to pass through, so traffic from unauthorized sources can be quickly discarded without committing significant processing resources.

Encryption protects confidentiality, and traffic authentication/integrity controls protect the integrity of network management data traffic—especially important with the growing use of in-band network management. Encryption provides a high degree of protection from internal and external threats, because access is limited to the small group of administrators that have legitimate access to encryption keys.

### ***Empower telephony servers to protect themselves.***

Of course, key telephony and OAM servers are protected by multiple levels of network and traffic-level security, plus tight access control and user authentication, authorization, and accounting (AAA). In the rare event that a cyber-attack penetrates those many layers of security provisions, the network elements themselves must be hardened against harm, to the extent possible. This can be accomplished through administrative measures that are part of generally accepted IT best practices. For example:

- Close potential security gaps in general-purpose operating systems and embedded real-time operating systems. OS hardening should use the latest procedures and patches from the OS manufacturer.
- Disable nonessential services to prevent potential backdoor attacks and other vulnerabilities.
- Apply security patches, perform penetration and vulnerability testing at the solution level to identify any remaining security issues, and address them if they exist.
- Use anti-virus protection tools to scan all in-house and third-party software packages before implementing the software into a product or network. A rigorous, established process ensures that network software is virus-free, to the extent possible.

## **Nortel Networks and cross-industry security developments**

Nortel Networks actively participates in ongoing security standards development within the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU), the European Telecommunications Standards Institute (ETSI), Cablelabs' PacketCable ([www.packetcable.com](http://www.packetcable.com)), Committee T1 ([www.t1.org](http://www.t1.org)), and a number of other international private- and public-sector organizations that are defining standardized solutions to address security vulnerabilities.

Nortel Networks is a leader in this area, having led the creation of the ANSI T1.276 standard (defining security requirements for network management) which has been adopted by industry and incorporated into recommendations to the U.S. Department of Homeland Security.

Our commitment to various forums and working groups helps align our security strategy with customers' needs, and facilitates interoperability across platforms and solutions. Here's a representative sample of the industry groups in which Nortel Networks has an active presence and/or a leadership role.

- **Internet Security Alliance (ISA)**—Nortel Networks was a founding member of this organization, which was created to share information and lead thought on information security issues. It is a collaborative effort between the Carnegie Mellon University Software Engineering Institute (SEI)\*, the Carnegie Mellon CERT® Coordination Center (CERT/CC), and the Electronic Industries Alliance (EIA)—a federation of trade associations. The Internet Security Alliance represents the industry's interest before legislators and regulators, and creates a collaborative environment to identify and standardize best practices and solutions.

- **Alliance for Telecommunications Industry Solutions (ATIS)**—Nortel Networks is an active member of this group, which develops and promotes technical and operations standards for communications and related information technologies industry worldwide.
- **National Security Telecom Advisory Committee (NSTAC)**—Nortel Networks serves on this committee of industry leaders representing various elements of the telecommunications industry. The committee advises the Executive Branch of the U.S. Federal government regarding policy and enhancements to communications for national security and emergency preparedness.
- **The Telecommunications-Information Sharing and Analysis Center (Telecom-ISAC)**—Nortel Networks cooperates with this subgroup of the National Coordinating Center for Telecommunications (NCC), which gathers information on vulnerabilities, threats, intrusions, and anomalies from the telecommunications industry, government, and other sources. This working group then analyzes the shared data, with the goal of mitigating the impact of these conditions on the telecommunications infrastructure.

The Nortel Networks Security Advisory Task Force (SATF) addresses security vulnerabilities that could affect Nortel Networks products, as soon as these vulnerabilities are discovered. This internal task force has established relationships with key security vulnerability agencies in the industry such as CERT<sup>®</sup>/CC, the first computer security incident response team; SANS (SysAdmin, Audit, Network, Security) Institute; and ISA to ensure rapid awareness of potential vulnerabilities and risk mitigation plans.

## Summary

Protection from external attacks, application abuse, viruses, unauthorized access, and interception or manipulation of voice, signaling, and management traffic... these are the issues troubling service providers as they move toward mass deployment of VoIP services.

Those concerns have workable answers. The security principles and mechanisms outlined in this document offer a framework for mitigating security concerns in a full range of VoIP network applications and architectures.

These security strategies address network threats at multiple levels—for instance, from a firewall guardian to block intruders at the front gate, to encryption to shroud every packet in privacy... from virtual LANs that segregate network management traffic from signaling and media-control traffic, to access control mechanisms that verify that each user and device is the genuine article.

With these security mechanisms, service providers can protect critical network resources, and confidently enjoy the advantages of VoIP as an extension of their secure service offerings.

Furthermore, end-to-end security in VoIP networks will be greatly simplified when IPv6 takes over the scene. The next generation of IP (version 6, or IPv6) leverages many IPv4 security mechanisms and also mitigates additional types of network attacks. IPv6 is expected to slowly replace IPv4, with the two existing side by side for many years. However, as with most protocols, IPv6 will mature slowly and must be introduced systematically and logically into the network. Nortel Networks is working closely with customers worldwide to determine the best strategy for introducing IPv6 into various regions and VoIP solutions.

For more information about security products, terms, standards, organizations, legislation, and certification, visit our security solutions Web site at <http://www.nortelnetworks.com/security>.

## Appendix

### Primary security mechanisms to protect VoIP networks

Here's a snapshot look at some of the key tools in the arsenal against cyber-attacks:

- **Firewalls**, such as Nortel Networks Alteon Switched Firewall, protect against unauthorized access by evaluating each packet against a security policy (the rules, conventions, and procedures governing communications into and out of a network) and accepting or denying admission accordingly.

Firewalls provide a perimeter defense to guard a network or its nodes against unauthorized users, such as those trying to “spoof” or pretend to be a legitimate network user. Firewalls may be deployed on a customer's premises or in a service provider's network—integrated with a virtual private network or as a stand-alone solution. Firewalls can be scaled to fit, for example, to satisfy the 1-Mbps connection requirements of broadband subscribers or the 1000-Mbps requirements of data center interconnection.

Firewalls don't have to be deployed at the edge of the service provider's network. They can be distributed at strategic points within the network, effectively segmenting the network into smaller areas, with filtering protection between those segments.

- **Network address translation (NAT)**, commonly implemented on firewalls, allows service providers to present a public IP address to the world and hide internal server addresses from public view. Converting external to internal addresses (and vice versa) can be performed in switch hardware, thereby enhancing the efficiency of routing, switching, and firewall functions.
- **VLANs (Virtual LANs)** provide basic network compartmentalization and segmentation, enabling various functions to be segregated in their own private local area networks, with cross-traffic from other VLAN segments strictly controlled or prohibited. The use of VLAN “tags” enables the segregation of traffic into specific groups such as OAM&P, call control, access aggregation, and Web services—separating their traffic without leakage between disparate functions.
- **Virtual Private Networks (VPNs)** enable yet another level of granularity in segregating and encrypting traffic. VPNs carry private network traffic on a logical connection—a secure “tunnel” over a shared or public network facility. As such, they're very good at safeguarding access to the critical core of your VoIP network.
- **Proxy servers** serve as intelligent intermediaries between domains, such as between the aggregation network and the service provider's core VoIP network, or between functional segments of the service provider's network. The media proxy (or media portal) provides a separation between two networks and only allows valid traffic to pass through. Isolation is achieved because there is no direct communication between one network segment and another; all media traffic must pass through the proxy.
- **Layer 3 switches**, such as Nortel Networks Passport 8600 Multiservice Switches, can help prevent denial of service (DoS) attacks by policing excessive or inappropriate traffic.
- **Encryption** protects the confidentiality of traffic, using agreed-upon algorithms to code and decode the communication. Encryption is especially important with the growing use of in-band network management. Encryption can be achieved through multiple techniques, some of which are described below.
  - **Secure Shell (SSH)** is used to log into a server over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over non-secure channels. It is intended as a replacement for telnet, rlogin, rsh, and rcp.
  - **Secure RTP (SRTP)** can be used to secure the media in the call, so even if an attacker had access to every packet, there is nothing they could do to decrypt it.
  - **IPSec** refers to a suite of IETF security protocols that protect IP communications through encryption, authentication, confidentiality, data integrity, anti-replay protection, and protection against traffic flow analysis. IPSec is an optional overlay for IPv4 and an integral component of IPv6.

- *Secure Sockets Layer (SSL)* protocol is widely used to protect communications to and from the World Wide Web. Originally developed by Netscape Communications Corporation, SSL is built into most browsers and Web servers to provide data encryption, server authentication, message integrity, and optional client authentication.
  - *Transport Layer Security (TLS)* is an Internet Engineering Task Force (IETF) standard that merges SSL and other protocols. TLS enhances SSL with more secure data encryption and is supplanting SSL as a major standard for securing Web/http traffic and VoIP protocols such as SIP.
- **Authentication** determines that users are who they say they are, and links them to authorization rules that determine where they can go in the network and what they can do once they get there. Authentication also determines that devices are genuine. For example, two call servers could authenticate each other to ensure that neither one is actually a hacker's PC masquerading as a call server.
    - Single-factor authentication requires only one proof point, such as the originating address.
    - Two-factor authentication (stronger but slower) requires both something the user has (such as device address or biometric scan) with something the user knows (such as password or SecurID code).  
Subscribers will accept two-stage login for one-time registration of their IP phones, but not every time they want to make a simple phone call. This more stringent level of authentication should also be used for network operators to gain access to management systems.

Centralized administration of passwords enables enforcement of password strength and removes the need for local storage of passwords on the network elements. Nortel Networks Integrated EMS (Element Management System) offers centralized account management for authentication, authorization and security logging, as well as single sign-on for graphical element management applications.
  - **RADIUS** provides important authentication, authorization, and accounting functions. RADIUS is the basic mechanism of choice for automating centralized authentication within Nortel Networks products.
  - **Secure activity logs** provide a verifiable audit trail of user or administrator activities and events generated by network devices. Syslog is the most common mechanism used by equipment vendors; Syslog works with third-party log analyzer systems to analyze security incidents and long-term trends.
  - **Intrusion detection, anti-virus, and content filtering tools** provide essential protections for VoIP network elements. Intrusion Detection System (IDS) software identifies traffic patterns that indicate the presence of unauthorized users. Anti-virus software detects and defuses potential cyber-attacks. Content filtering software restricts the type of data that can be accessed or distributed.

Together, these and other measures enable service provider VoIP networks to be open and accessible for legitimate uses, but not wide open for inappropriate or malicious uses.

**In the United States:**

Nortel Networks  
35 Davis Drive, Research Triangle Park, NC 27709

**In Canada:**

Nortel Networks  
8200 Dixie Road, Suite 100, Brampton, Ontario L6T 5P6

**In Caribbean and Latin America:**

Nortel Networks  
1500 Concorde Terrace, Sunrise, FL 33323 USA

**In Europe:**

Nortel Networks  
Maidenhead Office Park, Westacott Way, Maidenhead Berkshire SL6 3QH UK

**In Asia:**

Nortel Networks  
Level 5, 495 Victoria Avenue, Chatswood, NSW 2067, Australia

**In Greater China:**

Nortel Networks  
Sun Dong An Plaza, 138 Wang Fu Jing Street, Beijing 100006, China

*Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the web at:*

**[www.nortelnetworks.com](http://www.nortelnetworks.com)**

For more information, contact your Nortel Networks representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

**LEGAL NOTICE: This document is for informational purposes only and does not constitute advice. The information contained herein is provided "as is" without any representation or warranty of any kind and any reliance upon this document shall be at your own risk. Nortel Networks shall in no event be responsible for any damages of any nature (including lost profits, revenue, or data), whether in contract, tort, negligence or otherwise, arising from use of or reliance upon the information contained herein.**

\*Nortel Networks, the Nortel Networks logo, the globemark design, Alteon, Passport, and Succession are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2004 Nortel Networks. All rights reserved. Information in this document is subject to change without notice.



**NORTEL  
NETWORKS**

**BUSINESS WITHOUT BOUNDARIES**