



White Paper

Nortel Secure Unified Communications

Table of Contents	
Introduction	1
Nortel Secure Unified Communications Solution	2
Removing security as an obstacle	2
Key tenets of the Nortel security strategy	2
A layered security strategy	2
A layered approach to security ...	3
Five steps to comprehensive enterprise network security ...	3
Step 1. Protect the internal network infrastructure	4
Step 2. Protect client and server platforms	5
Step 3. Protect the integrity of multimedia traffic	5
Step 4. Secure remote access from branch offices and mobile workers	6
Step 5. Protect the integrity of network management systems	6
Closing thoughts	8

Introduction

Today's hyperconnected enterprise faces a security paradox. The very openness and ubiquity that makes IP networking such a powerful business enabler can also expose it to a significant threat. The ports and portals that welcome remote sites, mobile users, customers, and business partners into the trusted internal network are also welcoming to those who may compromise the network's security.

Security breaches—and the business disruptions they cause—represent a key concern of Chief Information Officers (CIOs). Enterprises relied on intranets primarily for email and file exchange, and they used the Internet as their Web storefront. With unified communications, since IP networks are being entrusted to carry the essential functions of conducting business—customer contact centers, voice, unified



messaging, conferencing, and more—there's a heightened requirement for protecting and securing those networks.

Nortel offers a comprehensive network security strategy that permeates the end-to-end architecture and enforces corporate policies on multiple levels and at multiple network points. The Nortel Communication Server 1000, when deployed together with a data network infrastructure, provides a secure unified communications solution that protects the network from internal and external threats, enhances reliability and reduces total cost of ownership, compared to traditional approaches.

This document describes how the Nortel Communications Server 1000 can ensure that the voice network is safe for your business. It describes best practices that can be applied to protect the voice network from attacks

Nortel Secure Unified Communications Solution

Now that IP networks offer the robustness and quality of service that voice service requires, enterprises have been quick to capitalize on the benefits of unified communications. Converging voice and data over IP maximizes network efficiency, streamlines the architecture, reduces capital and operating costs, and opens up new service opportunities.

The IP-based multimedia architecture makes it easy to extend service to remote sites and home offices over cost-effective IP links, and makes it easy to deploy, reconfigure (add/move/change) and repair service. VoIP enables rich, new multimedia services, such as Web-enabled multimedia contact centers, unified messaging, presence and remote PC-based call management.

However, there are factors that need to be considered in deploying a VoIP solution. As the lines blur between internal and external resources the network reaches more audiences and touch points,

carries more mission-critical services, and adds more distributed servers and intelligent client. It also becomes increasingly vulnerable to security threats.

The typical enterprise internal network extends to supply chain partners, telecommuters, remote access users, Web users, application service providers, disaster recovery providers and more. That means that the network may also be more accessible to hackers, cyber-thieves, disgruntled employees, and others who would misappropriate network resources. Worse yet, although estimates vary on what percentage of security breaches are internal, most sources consider that figure to be over 50%.

Organizations have been understandably concerned about securing this new multimedia environment, in which proprietary company information flows across shared facilities, public places, open airwaves and unknown users. It's clear that security must be a key focus in any VoIP deployment.

Removing security as an obstacle

Security for IP multimedia networks should be achievable, affordable and manageable. Confidentiality, integrity, and authentication of critical multimedia resources must be ensured while maintaining service continuity, feature richness, performance and availability. Security features should be transparent to the user, standard-based, simple to administer, uniform across products and cost-effective. Finally, security should be implemented consistently across the solution.

Nortel is delivering on that promise with a Secure Unified Communications Solution that:

- Protects the integrity of network infrastructure and communications by preventing unauthorized access
- Increases network reliability by preventing disruptions from attacks on user services, network hardware or network management systems

- Prevents theft of intellectual property and abuse of resources from eavesdropping and toll fraud

This security solution melds best-of-breed technologies and industry best practices into a solution that permeates every aspect of the enterprise network—from client devices to network access points and services.

Key tenets of the Nortel security strategy

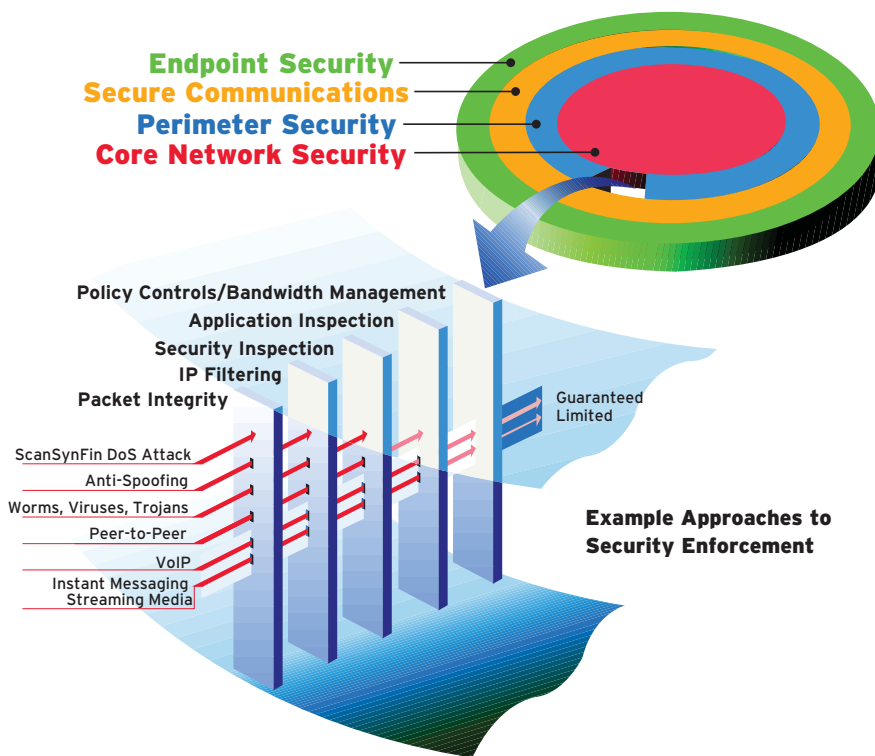
The Nortel Secure Unified Communications Solution is based on several fundamental principles. Security measures must:

- Be intrinsic in the design of all system components and features
- Be layered, with multiple controls and protections at multiple network levels
- Comply with the latest industry standards, certifications and best practices
- Leverage appropriate technology from best-in-breed partners
- Be continually and proactively enhanced to address emerging threats

Nortel offers a full array of security solutions for enterprise and service provider applications, from high-performance national backbones to business LANs. Design features built into the equipment enable components to protect themselves and report security aberrations to network management systems. In addition to security features within network components, Nortel offers security products that protect multiple network elements and entire networks.

A layered security strategy

A layered defense approach to network security applies multiple security approaches at multiple network levels—much like protecting your property with sentries and gates at several places.



The approach applies multiple enforcement tactics—such as authentication, encryption, packet filtering and signature-based inspection—at multiple network zones— such as access endpoint, network perimeter, network core and transport links.

With a layered approach, it minimizes the possibility that a single point of failure could compromise overall security. If a primary layer of security is breached, the secondary or tertiary layer of defense is there to thwart the attack.

A layered approach to security

The graphic above shows a cross section of the security layers with several enforcement approaches in action. This layered approach applies directly to a VoIP solution as follows:

The core network layer protection includes the devices that monitor for unwanted behavior or traffic patterns, and respond – this would include Intrusion Detection and Prevention Systems. The network protection approach could also apply policies that

authorize devices onto the network (such as the 802.1x protocol) as well as ensuring that DoS-like traffic could be detected and shut down, and prevent devices from IP address spoofing.

Protection around the communications layer would include the ability to encrypt your voice traffic with SRTP (Secure Real-Time Transport Protocol), and signaling traffic with UNIStim or TLS (Transport Layer Security) encryption. OAM security could be enforced through the strict use of SSH/SSL (Secure Shell/Secure Socket Layer) for OAM (Operations, Administration and Maintenance) access and IPsec connectivity between your VoIP components.

Perimeter security, as applied to VoIP solutions would infer that the voice network be segregated wherever possible, so that unwanted traffic between the voice and data network is constrained. Soft clients present a greater challenge however, Nortel’s IP hard phones can be easily isolated from the data network through the use of VLAN technology. Only OAM traffic, which can be secured over SSH/SSL, can be allowed

from the general telephony LAN where the IP Phones reside. The VoIP perimeter can be further protected through the use of firewalls and access control lists, and VLAN tagging if data access is provided through the IP Phone clients.

The final layer of defense, the endpoint security, can be enforced by requiring hardening of customer components that need access to the VoIP segments, by Nortel’s hardening policies on our system components and by closing down unneeded access and by restricting use of insecure protocols and shells at the endpoints. The endpoint security must include mechanisms to control access to the devices. Password control policies must be enforced so that passwords are changed regularly to strong passwords.

Five steps to comprehensive enterprise network security

By applying the following five step plan, enterprises can:

1. **Protect the internal network infrastructure** with network segregation, firewalls, intrusion-detection systems (IDS) and virtual LANs (VLANs).
2. **Protect client devices and servers** with mechanisms that thwart viruses, intruders and denial-of-service (DoS) attacks, while remaining resilient under attack. Enforce policies to ensure that the devices are protected.
3. **Protect the integrity of multimedia services** by safeguarding both the signaling traffic and media traffic.
4. **Extend security to remote and mobile workers** by ensuring that only authorized users can access the network, and encrypting their communications for privacy.
5. **Protect the integrity of management systems** through encryption, administrator access control and activity logging.

Let’s take a closer look at the key defense mechanisms Nortel applies for each of these areas.

Step 1. Protect the internal network infrastructure

The risks

Networks are vulnerable to a broad variety of attacks, such as spoofing, ARP table overflow, DHCP (Dynamic Host Control Protocol) starvation, rogue DHCP, VLAN (Virtual LAN) hopping, private VLAN proxy and spanning tree abuse.

The key defense mechanisms

Network Segregation prevents unnecessary or unwanted traffic from traversing into areas that might cause problems. By segregating the management traffic on its own VLAN together with host authentication and other methods outlined below, we minimize the probability that there is unwanted access to the telephony servers. As well, the best practices for network configuration would be to segregate the voice traffic from the data traffic, by isolating IP phones to specific subnets, which minimizes the possibility of attacks on phones and to the servers that handle these phones. IP softphones are a special case where a PC device must be allowed access to the voice network, and may bring other potential security threats that must be protected against using similar mechanisms to those applied in the data network. For PC devices that are connected through IP phones, VLAN tagging is available to ensure that the data traffic takes a separate VLAN from the voice traffic.

Firewalls examine network traffic passing through them and block packets that don't meet predefined criteria. Only traffic that is typical and expected can get through. An advanced firewall with "stateful packet filtering" can grant or deny network access based on time of day, application, IP address, port range and other attributes. Ultra-granular control enables Web or data traffic to be restricted while still letting IP telephony calls pass through.

Virtual LANs (VLANs) segregate different areas of the same network, for example, separating a company's client record servers from its public Web servers or separating IP phones from PCs and softphones (PCs equipped to perform like IP phones). VLANs control the propagation of traffic between network components, creating a logical separation even where there is no physical separation. Please note that the Nortel implementation of VLANs on its Ethernet switching platforms is secure and has no possible vulnerability to VLAN hopping that other network equipment vendors have been subjected to.

Network-based Intrusion Detection and Prevention Systems (IDS/IPS) can be deployed at strategic locations within the enterprise network to monitor network traffic and watch for signs of attack or misuse. In the case of IPS, the systems can also work to automatically block threats and attacks.

Network access control provides a method for authenticating and controlling access to network resources—especially critical for areas where you don't have physical control over network ports. Alternatives that could be used include 802.1x port-based authentication or use of the Nortel Secure Network Access Solution (SNA).

- **Nortel Secure Multimedia Controller 2450** is an application firewall that sits between communications system components and the enterprise network, protecting a "Secure Multimedia Zone." This device protects against internal and external threats using packet filtering and stateful packet inspection on appropriate protocols, and a rate-limiting function guards against denial-of-service attacks. The SMC 2450 also provides the ability to encrypt the UNISlim signaling, protecting attackers from intercepting and relaying UNISlim signaling information.

- **Nortel Ethernet Routing Switch Family** provides the Ethernet infrastructure that supports the VoIP and multimedia solutions required for the enterprise. The Ethernet Routing Switch products protect against internal and external threats using packet filtering and VLAN segregation of all network traffic entering and leaving the Communication Server 1000. Nortel Ethernet Routing Switch 4500 and 5500 allow the administrator to enforce anti-spoofing policies at the network layer. Anti-spoofing features on the Ethernet Routing Switch 5500 include DHCP Snooping, IP Source guard, and dynamic ARP inspection. Nortel's Ethernet Routing Switch 8600 can be used at the core to do reverse path checking which also ensures network security by not allowing IP spoofing of any connected network elements.

- **Nortel Switched Firewall** is an application firewall that sits between communications system components and the enterprise network. This firewall protects the components of the voice network from internal and external threats using stateful packet inspection on signaling and network-management traffic. The Switched Firewall supports the Nortel VoIP portfolio and provides virtually jitter-free performance.

- **Nortel Threat Protection System (TPS)** can be added to the user network or the core network that surrounds it. The Threat Protection System provides early detection and protection against known threats as well as "day zero" protection from new attacks that have gotten through the perimeter or originated inside the enterprise. With Real-Time Network Awareness (RNA) technology to profile assets on the network, the TPS provides endpoint intelligence to determine the impact of threats.

The Threat Protection System can recognize a DoS attack occurring, and either shut off network access to the offending PC, block traffic from a

specific port, or limit the traffic, slowing the requests to a harmless level. Since the TPS supports remediation across the enterprise, it can automatically block attacks using the Nortel Switched Firewall, Application Switch, Secure Network Access Switch and VPN Gateway as enforcement points in the network.

- **Nortel Secure Network Access** continuously scans all network endpoints, ensuring that only those devices with the latest security patches and approved configurations can connect to the network. Any non-compliant endpoint is connected to a “remediation LAN,” where users are instructed to download appropriate software patches and make necessary configuration changes to comply with corporate security policies and be allowed back onto the user LAN.

Step 2. Protect client and server platforms

The risks

The overall security of a communication system depends in part, on the strength of client devices and network and application servers. The platforms themselves must be able to thwart viruses, intruders and denial-of-service (DoS) attacks, while remaining resilient under attack. For example, a device could pretend to be a phone and send millions of requests per second to the server. The server or a security gateway must be able to recognize which messages are valid and ignore invalid messages.

The key defense mechanisms

Operating system hardening improves resistance to attacks, such as allowing only certain ports to be active. Linux, Solaris, Windows and Real-Time operating systems used in multimedia networks can all be hardened for security. In the Telephony Manager (TM), a guideline is available for hardening the Microsoft operating system upon which TM is running.

Note: Nortel compiles and configures the VxWorks operating system, which enables us to turn off all OS services not required by the Communication Server 1000 applications. For example, Nortel does not enable IP routing in VxWorks, which ensures that unauthorized system traversal between ELAN and TLAN is not possible. Additional security capabilities have also been added to the OS by Nortel in order to further increase security, such as: an audit trail to report OS activities to determine root cause, a watch dog process minimizes impact of potential DoS attacks, and enhanced memory management optimizes memory allocation to minimize impact of potential system attack. Each release also receives a thorough security threat testing prior to being released. Testing is done under load and adverse conditions (including system failure and restart and testing with memory management tools) and security vulnerability testing is performed using industry accepted practices.

Host-based ‘malware’ protection

protects IP softphones against malicious software designed to damage or disrupt computing systems, such as viruses, worms and Trojan horses.

Host-based intrusion-detection systems (IDS) audit and analyze system events to watch for signs of attack or misuse. Host-based IDS can be integrated into many different network components.

Load and patch delivery management ensures the authenticity and integrity of software upgrades and fixes. This precaution is especially critical when downloading firmware to IP clients across insecure networks. Trusted software delivery methods ensure that you are downloading only approved software that is actually from Nortel. This capability is being delivered in the 3.0 version of UNISStim phone software.

Enforcement of Password Protection. Communication Server 1000 can be set up to apply internal mechanisms that ensure password policies are being applied, such as password complexity and password aging.

Step 3. Protect the integrity of multimedia traffic.

The risks

Every organization has a responsibility to protect the non-public customer/client data that it possesses. The network must be protected from eavesdroppers and attackers who are looking for confidential communications or wanting to wreak havoc with the signaling that runs the network.

New regulatory pressures increase the importance of this responsibility. For example, all but the smallest health plans must comply with Health Insurance Portability and Accountability Act (HIPAA) rules designed to safeguard the integrity and confidentiality of patient data. The Gramm-Leach-Bliley Act invokes similar requirements for financial services firms.

The key defense mechanisms

Encryption of signaling traffic prevents illicit monitoring or tampering of the signaling that directs network operations, such as call setup and routing, service performance, event recording, billing, etc.

- **UNISStim** (Unified Networks IP Stimulus Protocol) is used for signaling between IP clients and Nortel communication servers. The Secure Multimedia Controller 2450 encrypts this signaling traffic using UNISStim Security (USEC).
- For **Session Initiation Protocol (SIP)**, a digest mechanism provides message authentication and replay protection. Transport Layer Security (TLS) encrypts SIP signaling traffic in accordance with IETF recommendations.

- **Other signaling protocols** are used to signal between network elements, such as between the call server and signaling server. Even though this traffic stays within the enterprise LAN, it is secured by IPsec or TLS encryption.
- **Protect Nortel IP Phones** by disabling the gratuitous ARP (Address Resolution Protocol) on the phones – this prevents attackers from attempting to poison the ARP cache.

Encryption of media traffic (the actual content of communications between users) prevents eavesdropping into private matters, whether the communication is voice, video or instant messaging (IM).

- **Voice streams** use the Secure Real-Time Transport Protocol (SRTP), an IETF standard for real time media traffic. Media endpoints may be configured to use media security on a “best effort”, or “always on” basis.
- **Encryption of OAM** (Management) traffic protects the Communication Server 1000 devices from attacks from users wishing to attack via maintenance points on the Communication Server 1000 system.
- **OAM Access for the Communication Server 1000** can be achieved via rlogin, telnet or SSH. The Communication Server 1000 allows the rlogin and telnet access to be shut down when the secure access is used. As well, web access to the Communication Server 1000 Element Manager can be restricted to strictly SSL-encrypted connectivity.

Full switching of traffic on the Nortel Ethernet Routing Switches limits the ability of a user to see the traffic of their neighbor’s PC or IP phone. The routing switch ignores gratuitous ARP signals and other tricks that end devices can use to confuse a LAN switch into “leaking” packets onto other ports. For maximum security, you can prevent RTP traffic from traversing broadcast segments, such as WiFi or Ethernet hubs—or require encryption for such traffic.

Step 4. Secure remote access from branch offices and mobile workers.

The risks

One of the chief merits of IP multimedia communications is the ability to connect from anywhere, while your network services and features follow you. Branch offices, teleworkers, road warriors and business partners can be brought into the network environment, so geographic location becomes irrelevant. However, remote access from insecure locations presents additional challenges. How do you guarantee user identity and shield privacy for remote communications that cross public networks?

The key defense mechanisms

Virtual private networks (VPNs) enable secure connectivity with branch offices, business partners and remote users far beyond the reach of private networks. VPNs, typically based on the IPsec protocol, carry the confidential data traffic on a logical connection — a secure, encrypted “tunnel” over a public network.

Nortel’s award-winning VPN technology is optimized not only for data application, but also for voice and multimedia communications. Through the Nortel VPN Router, the IPsec VPN client provides access for corporate client devices. The VPN Gateway provides SSL VPN access which doesn’t require client software on the access device. As a result, SSL VPN is best suited for guests, partners, and customers and employees using unmanaged devices or public kiosks. VPN Gateway SSL ON Demand Protection provides an enhanced level of security by ensuring that confidential information is not stored on unmanaged PCs and preventing unauthorized printing or saving of information to attached storage or flash memory devices.

For either type of connection—IPsec or SSL—Nortel Tunnel Guard technology ensures that the endpoints comply with corporate security policies. That is, the client device must have the appropriate operating system updates, application and software patches, approved software, virus/firewall protection and configuration.

VPN technology can also be used to secure remote management interfaces, reducing the risk that someone could tamper with branch office equipment that is managed from a central office.

Step 5. Protect the integrity of network management systems.

The risks

An intruder who gains access to the network management system could not only disrupt network management but also disable security provisions. If users can access remote monitoring, port mirroring or other LAN switch troubleshooting functions, they could copy other users’ traffic. Even legitimate administrators should only have access to the functions they need, and you need to be able to track who has done what.

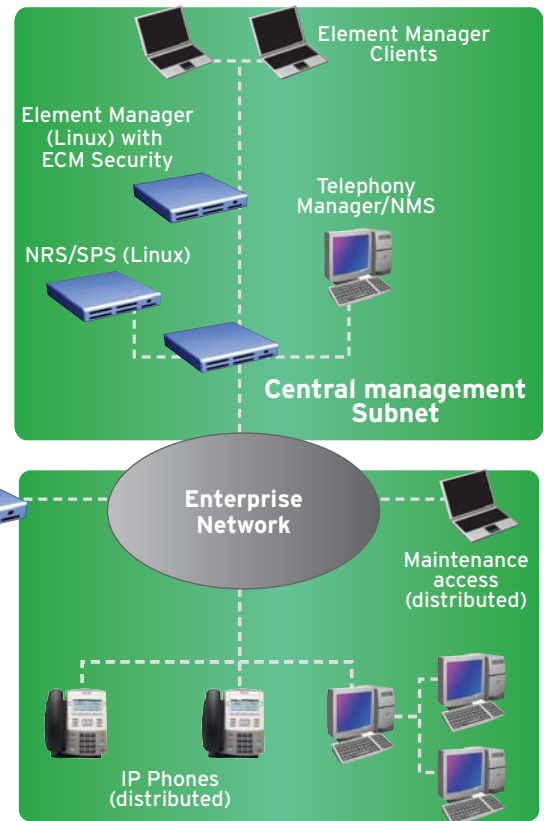
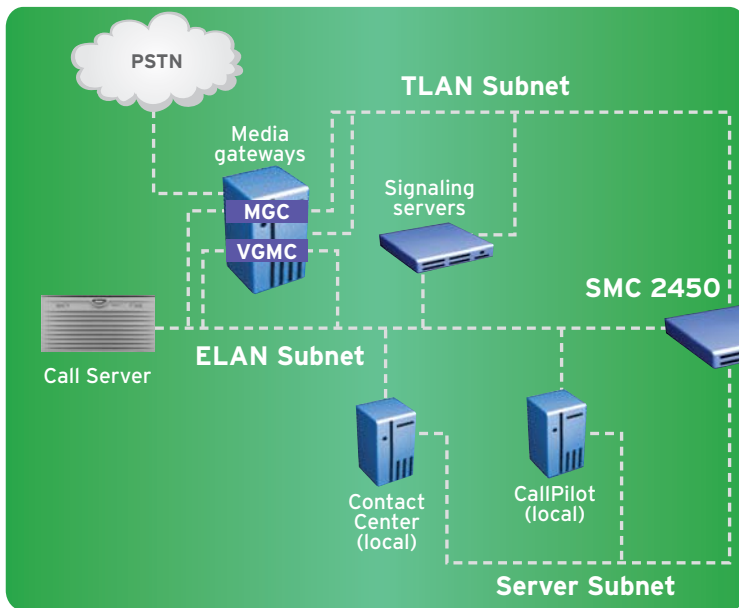
The key defense mechanisms

Authentication ensures that only authorized users can access management facilities. This is normally accomplished through the use of strong passwords that are centrally administered.

Access permissions define administrators’ roles and restrict the functions they can use. In this way, the security administrator can grant access privileges to only those users who are entrusted to the tasks they must perform.

System event logging records all system events, such as operational activity, errors and security activities. Secure billing records protect confidentiality and identify theft of service. Security

CS1000 Secure Deployment



logs and alarms provide notification and accountability. With detailed audit trails of system activity, administrators are aware of and can respond to issues that could compromise network integrity or user security.

Encryption of management traffic

prevents interception or eavesdropping, even within the secure environment. For example:

- Secure Sockets Layer (SSL) is the de-facto standard for securing the HyperText Transport Protocol (HTTP) that is used for Web-based management.
- IPsec secures communications between the Communication Server 1000 components, through the ISSS feature, which protects communications between the components through an IPsec tunnel.
- IPsec, SSL or Secure Shell (SSH) can be used to add security to such tools as Remote Desktop Connection, VNC or PCAnywhere, which are used to remotely control internal management stations from outside the enterprise network.

These industry-standard encryption protocols prevent unauthorized users or devices from hacking into management activities or pilfering sensitive information about the network or its security provisions.

Advantages of the Nortel Secure Unified Communications Solution

Together, the Five Steps and their respective defense mechanisms establish a highly secure enterprise network environment—one that reliably protects against known and emerging threats, without compromising quality of service or the user experience.

Protect against prevailing security threats. With Nortel security technologies, enterprises can confidently:

- Prevent unauthorized clients and endpoints from accessing the IP network and VoIP or multimedia services with the layered defense of the Nortel Secure Unified Communications Solution.

- Prevent attacks from occurring on the user LAN and affecting VoIP and unified communications with the Nortel Threat Protection System.
- Prevent unauthorized clients and endpoints from accessing the IP network with the Nortel Secure Network Access Solution.
- Prevent manipulation of IP phones with hardening, strong authentication, tamper-proofing and centralized password management.
- Prevent man-in-the-middle attacks and impostor servers or client by applying industry standard authentication and encryption.
- Prevent denial-of-service attacks from flooding the network with illegitimate requests that would crowd out legitimate users.
- Secure communications to branch offices, remote teleworkers and road warriors thanks to user authentication and award-winning VPN technology.

Sustain the quality of the user experience. When security features are overlaid on users' phones, there's no effect on feature functionality. No impact to end users.

On some other security platforms, encryption can cause a system to require an hour or more to reboot. In contrast, the Nortel Secure Multimedia Controller reboots in minutes, even with the full complement of encryption turned on.

Reduce total cost of ownership. Nortel open architecture solutions are standards-compliant and take advantage of strategic partnerships—a strategy that provides best-of-breed technology while minimizing integration cost. We work to provide fully integrated security products/solutions that are agnostic to the primary network architecture. The result is better operational efficiency, integration simplicity and rapid adaptation to emerging security threats.

Security in the real world

Nortel security solutions have been proven in some of the world's most demanding environments, including high-security national defense organizations, and state and local police organizations.

Select models of Nortel's VPN Router have achieved FIPS and Common Criteria certification. Nortel is the first networking vendor to provide an end-to-end VoIP solution certified by the U.S. Defense Department Joint Interoperability Test Command (JITC).

Bring it all together with Nortel Global Services

To help customers deploy a Secure Unified Communications Solution, Nortel's Global Services and select partners offer a full range of security services. Services include:

- Network security design and planning
- Security audits and assessments
- Security integration planning
- Compliancy and regulatory audits
- Project management and implementation of security solutions
- Ongoing technical support and software updates
- Security optimization, upgrade and migration support
- Managed services to help you get your security infrastructure up and running quickly

Closing thoughts

Enterprises are wise to capitalize on the productivity, performance and personalization advantages of IP multimedia communications. The greater the reach and availability of the network, the greater its vulnerability to threats from within and outside the organization.

Nortel's Secure Unified Communications Solution enables organizations to deploy VoIP and multimedia applications while meeting or exceeding their requirements to protect information, infrastructure and services. The layered defense approach prevents theft of intellectual property, abuse of resources and disruption of services due to network attacks.

Nortel security solutions are VoIP-aware, and our VoIP solutions are security-aware, providing strong security at low total cost of ownership, without compromising user quality of experience. In fact, security is in the very DNA of the Nortel enterprise network.

Find out more about Nortel Unified Communications solutions. Contact your regional Nortel representative or visit us on the Web at www.nortel.com/uc.

Nortel is a recognized leader in delivering communications capabilities that make the promise of Business Made Simple a reality for our customers. Our next-generation technologies, for both service provider and enterprise networks, support multimedia and business-critical applications. Nortel's technologies are designed to help eliminate today's barriers to efficiency, speed and performance by simplifying networks and connecting people to the information they need, when they need it. Nortel does business in more than 150 countries around the world. For more information, visit Nortel on the Web at www.nortel.com. For the latest Nortel news, visit www.nortel.com/news.

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

Nortel, the Nortel logo, Nortel Business Made Simple and the Globemark are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2008 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.

NN123481-022608

In the United States:

Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:

Nortel
195 The West Mall
Toronto, Ontario M9C 5K1 Canada

In Caribbean and Latin America:

Nortel
1500 Concorde Terrace
Sunrise, FL 33323 USA

In Europe:

Nortel
Maidenhead Office Park, Westacott Way
Maidenhead Berkshire SL6 3QH UK
Phone: 00 800 8008 9009

In Asia:

Nortel
United Square
101 Thomson Road
Singapore 307591
Phone: (65) 6287 2877



BUSINESS MADE SIMPLE