



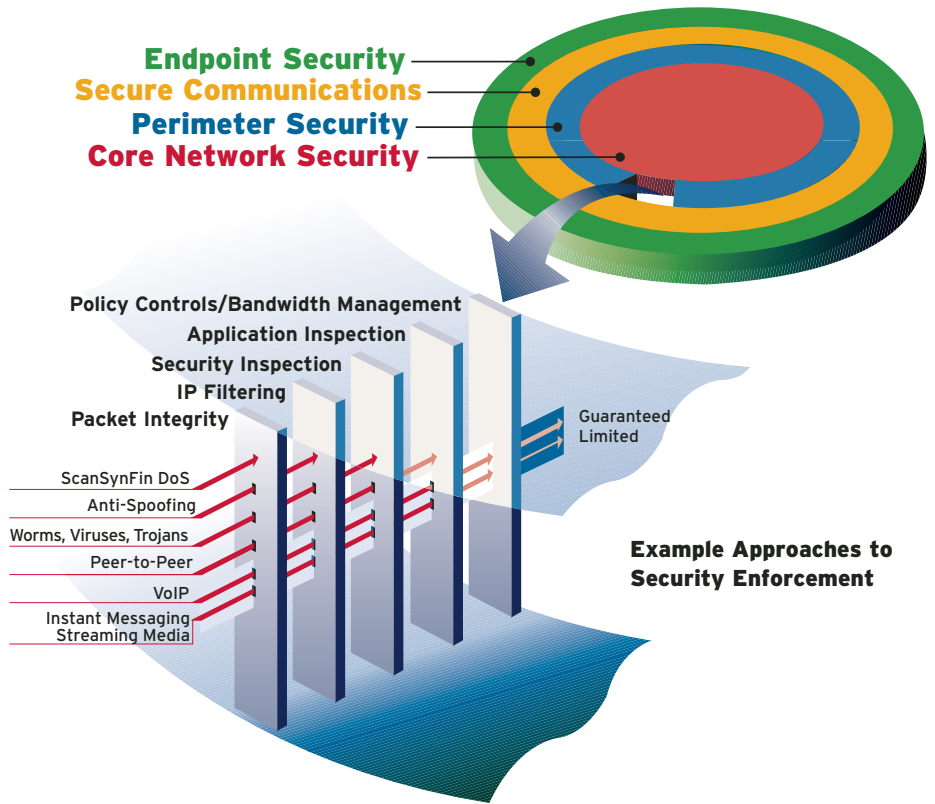
# NORTEL

## Solutions Overview

### Secure Multimedia

#### Layered Defense

Nortel's approach to securing communications is known as a Layered Defense. This approach is used to secure not only data communications, but also voice and multimedia applications. A Layered Defense consists of four parts. *Endpoint Security* ensures valid identity and connected device security policy compliance. *Secure Communications* ensures information protection from unauthorized discovery over the network. *Perimeter Security* keeps the "good stuff" in and the "bad stuff" out by securing the boundaries between zones of different levels of trust. And finally, *Core Network Security* keeps watch for malicious software and traffic anomalies, enforcing network policy and enabling survivability.

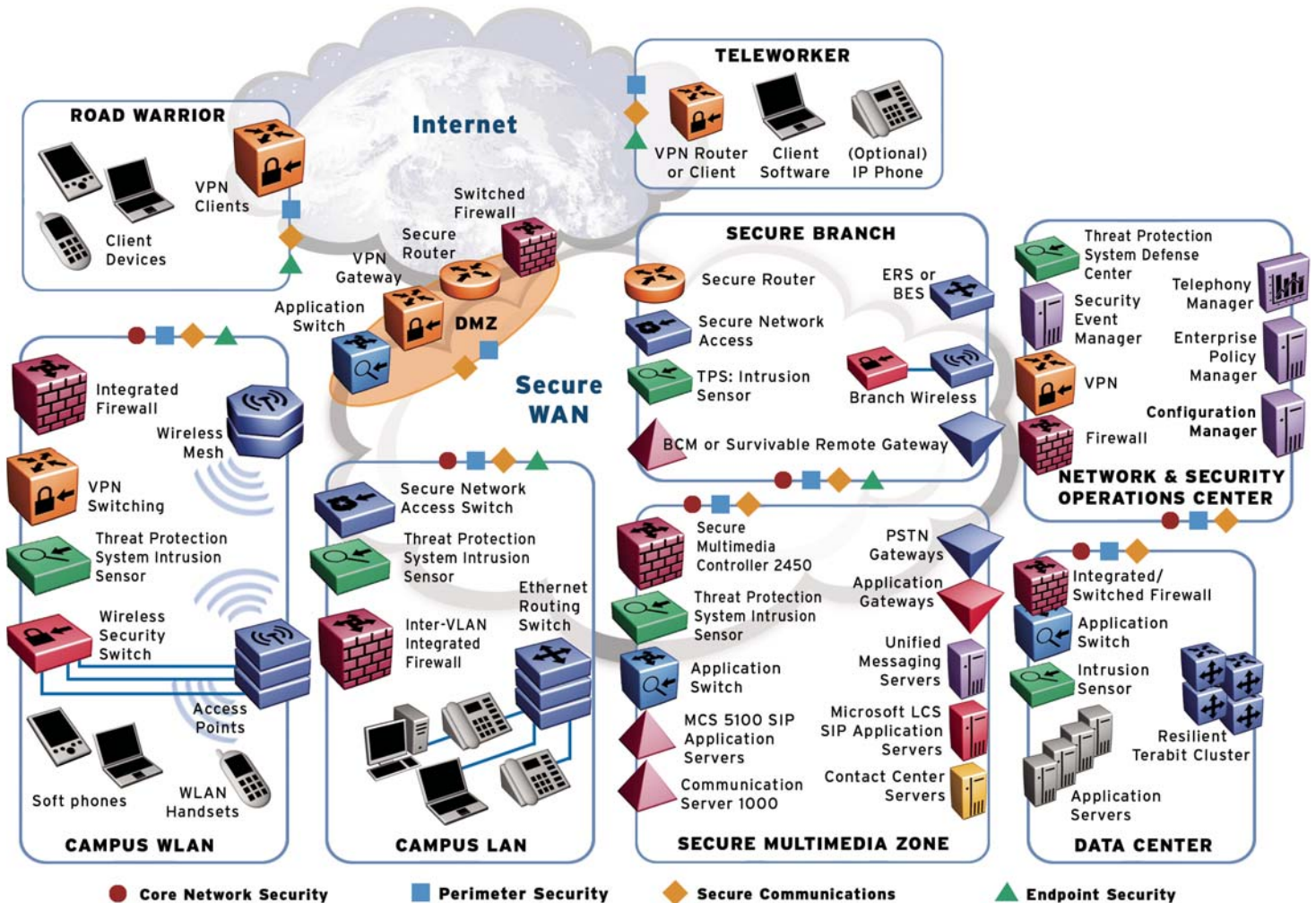


## Secure Multimedia Zone

Multimedia and IP Telephony servers reside in a secure multimedia zone, with Secure Multimedia Controllers (SMCs) providing a virtual “moat” around your servers, keeping them safe from denial-of-service (DoS) and other attacks. The SMC blocks unauthorized endpoints from accessing your communication servers. VoIP signaling is secured with a 128-bit AES encryption algorithm to

secure communications between the endpoints and the Secure Multimedia Zone, helping prevent any interception and manipulation of the control signaling of your IP Telephony system. Secure VoIP signaling also provides peer entity authentication, allowing endpoints to verify signaling information came from a valid server in the Secure Multimedia Zone, and helping prevent impostor servers from misleading phones. Threat Protection System

Intrusion Sensors keep an eye out for suspicious activities or malicious traffic from an intruder. Nortel Application Switch with SIP load-balancing can seamlessly redirect clients to an alternate location if the primary Secure Multimedia Zone becomes unavailable, while multiple PSTN gateways can accept calls from multiple PSTN trunk locations. All operating systems, including realtime operating systems used in servers, are hardened with a



variety of techniques designed to ensure that all non-used components are removed. Anti-virus security software is installed on any servers running non-embedded operating systems. Applications and platforms are hardened, with multiple access levels for both user services and management ports. Applications such as conferencing have integrated security features, such as reporting the identity of conference participants to chairpersons. Application gateways such as Application Gateway 1000, WLAN Application Gateway 2246 and the BlackBerry Enterprise Server all provide secure access to data center applications from IP Telephony client devices.

### Campus LAN

In the Campus LAN, Nortel Secure Network Access (NSNA) uses a variety of methods to authenticate devices wishing to join the network. IEEE 802.1X with EAP (Extensible Authentication Protocol) provides strong authentication for both PCs and Nortel IP Phones, while guest users can be authenticated via captive web portal interface, all helping to prevent unknown devices or users from gaining network access. Security policies are checked and enforced before endpoints are allowed to join the network, and based on the role of a user, devices are confined to a specific Virtual Local Area Network (VLAN) with a specific access control list (ACL). Users can only access network resources for which they are authorized — only finance employees on the finance VLAN can access payroll; only R&D engineers on the R&D VLAN can access product designs. IP Phones that are granted network access must further authenticate with a Secure Multimedia Controller before being allowed to access secure servers in the

Secure Multimedia Zone. Secure VoIP Signaling with 128-bit AES encryption prevents IP phones from being misled by internal PCs attempting to impersonate an IP Telephony server. AES encryption protects against man-in-the-middle attacks and interception or decoding of VoIP control signals. IP Phones can encrypt the voice path using standards-based Secure Real Time Protocol (SRTP), protecting conversations from being recorded, even by technicians with access to data infrastructure.

Internal attacks against the IP Telephony servers are blocked or rate-limited by the Secure Multimedia Controller. Traffic flood attacks are prevented from affecting more than one VLAN by integrated firewalls and access control lists (ACLs) controlling inter-VLAN traffic. The Threat Protection System can

detect attack traffic, isolate the source of the attack, remove the offenders from the network and notify administrators.

Other security policies are enforced by LAN switches in the wiring closets at the edge of the network. Quality of Service (QoS) marking (IEEE 802.1p at Ethernet Layer 2, DiffServ at IP Layer 3) can be policed and marked, helping prevent rogue endpoints from marking all of their traffic as high importance. QoS features can also prevent storms of data traffic from affecting voice performance. IP Phones and LAN switches all are designed to ignore gratuitous ARP (Address Resolution Protocol) requests, and LAN switches can prevent false DHCP servers on a user PC from misleading other end-user devices.

Security policies are checked and enforced before endpoints are allowed to join the network.



## Campus WLAN

The Campus Wireless LAN (WLAN) contains all of the features found in the Campus LAN, and adds additional wireless security features. Like the campus LAN, NSNA endpoint security can use 802.1X with EAP, captive web portal and other means to authenticate the identity of anyone attempting to join the network. The Wireless Security Switch maintains security while maintaining QoS for voice quality, and adds location awareness to the security capability. Location awareness can be critical to finding rogue access points and other unauthorized wireless devices. NSNA's Tunnel Guard feature can verify endpoint configuration, and disallow certain PC configurations such as ad-hoc/peer WLAN networking. Implementation of wireless multimedia standards helps to keep a high level of voice quality while maintaining a secure wireless environment. The centralized architecture of the WLAN Security Switch also helps ensure consistent security. Optional VPN clients in WLAN Handsets, PDAs and wireless laptops provide secure encryption of both voice and data delivered to the client.

## Secure branch

A secure branch includes many of the features of both the Secure Multimedia Zone and the Campus LAN. Threat Protection System's Intrusion Detection sensors keep an eye out for malicious traffic. Branch office-sized Wireless Security Switches maintain a secure wireless environment. NSNA maintains endpoint security and enforces security policies. Ethernet Routing Switches or Business Ethernet Switches provide LAN-based security. Secure Routers provide WAN connectivity, with integrated firewall, security policies, QoS and VPN encryption. Routers built into the Business Communications Manager and Survivable Remote Gateway provide WAN routing and security in a single, integrated device. Access to management interfaces of remote equipment can be secured by requiring VPN access with enforced password policies.

## Teleworkers and road warriors

Teleworkers and road warriors have a number of options for secure access. Nortel's VPN Gateway offers remote access utilizing both IPsec clients and SSL-clientless access. Tunnel Guard

provides endpoint validation, automatically enforcing an organization's security rules, even for those remote endpoints that are traditionally hard to keep an eye on. Home-based teleworkers can have the "full office" experience, with an IP Phone and PC operating together over a VPN. Road warriors have a wide range of secure communication choices, ranging from RIM BlackBerry devices to software clients such as the Dual Mode Mobile 3100, which provides both data and voice connectivity over both WLAN and cellular networks — all secured by VPN encryption.

## Data center

At the data center, integrated and/or switched firewalls protect access to servers and applications. Threat Protection System's intrusion sensors keep a constant eye out for suspicious traffic patterns. Servers can use redundant connections to a resilient terabit cluster, ensuring their constant availability to end users. Nortel Application Switches provide load balancing and SSL acceleration, helping ensure both performance and reliability of data applications. From a multimedia perspective, IP telephones, handsets and clients can access applications via

**A secure branch includes many of the features of both the Secure Multimedia Zone and the Campus LAN.**



gateways such as the Application Gateway 1000, WLAN Application Gateway 2246 and the BlackBerry Enterprise Server. Data applications requiring a human-like (VoiceXML) voice interface can be securely accessed via Nortel Media Processing Servers.

### **Network and security operations center**

Several methods and techniques are available to secure network and service management interfaces. Out-of-band management interfaces can be used to set up a separate network management LAN or VLAN. Access to this separate network can be further limited by Nortel Secure Network Access and/or by VPN access. This separate network can also be protected by firewalling. Threat Protection System's Defense Center receives information from various intrusion sensors, correlates the information and takes any necessary coordinated action to block malicious traffic on the user networks. Security Event Manager keeps an eye out on other security events reported on the network (such as repeated login attempts, or invalid SNMP access attempts). Telephony Manager keeps an eye out for suspicious voice traffic patterns, quickly reporting any potential toll-fraud events before they reach a crisis level. Multiple user permission levels control access to restricted applications and resources. Enterprise Policy Manager acts as a central storage point for all security policies enforced on the various networks (WLAN, LAN and VPN). Configuration Manager and other network management tools keep an eye on the current state of the network,

record any configuration changes and help administrators push out configuration changes to multiple networks quickly.

### **DMZ — demilitarized zone**

Strong perimeter security is provided by Switched Firewall, which maintains high throughput rates, even with complex stateful inspection. Secure access by remote users (both voice and data) is governed by VPN gateways, supporting both SSL and IPsec endpoints. WAN router connections are kept secure by the Nortel Secure Routers, which provide extensive security features while maintaining the high throughput necessary for realtime communications. Application switches can load balance, accelerate and provide failover for customer and partner access to public data applications, as well as provide load balancing, acceleration and failover for remote teleworkers and road warriors using VPN gateways.

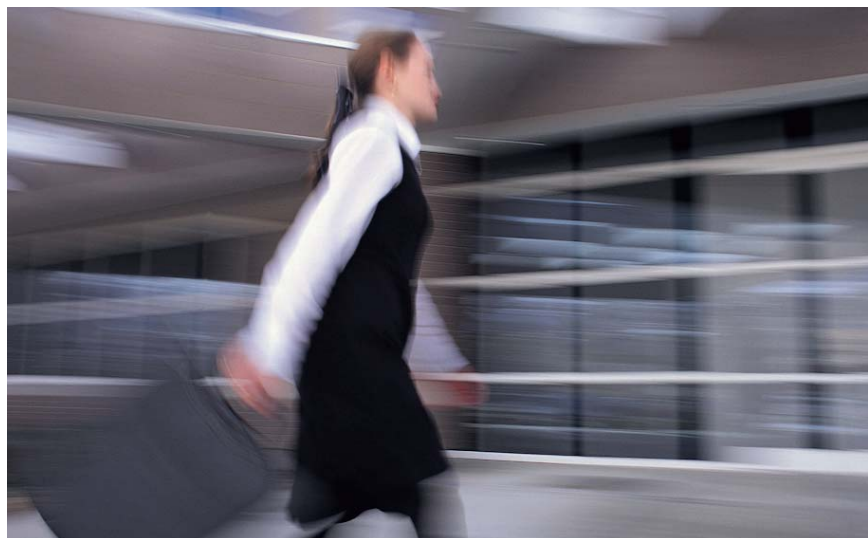
### **Security services**

Security services can provide a variety of help in rolling out Secure Multimedia and IP Telephony. Services are available

to help assist customers in designing and implementing their own systems, and help them with compliance checking, initial design and implementation — supplementing in-house expertise. Managed security service frees organizations from some of their security, allowing them to delegate it to a fully-staffed 24x7 security operations center that can monitor their network for them. Custom-designed security centers can also be set up to share the responsibility for security.

### **More information**

For more information, check the Nortel website ([www.nortel.com/securemultimedia](http://www.nortel.com/securemultimedia)). There, you will find additional information on securing your multimedia and IP Telephony systems, including a Frequently Asked Questions document. You may also wish to contact the security experts at your local Nortel office or authorized Nortel Channel Partner, who can discuss applying Nortel's Layered Defense strategy to your exact business communication requirements and existing systems.



**In the United States:**

Nortel  
35 Davis Drive  
Research Triangle Park, NC 27709 USA

**In Europe:**

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

**In Canada:**

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

**In Asia:**

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

**In Caribbean and Latin America:**

Nortel  
1500 Concorde Terrace  
Sunrise, FL 33323 USA

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Our next-generation technologies, for both service providers and enterprises, span access and core networks, support multimedia and business-critical applications, and help eliminate today's barriers to efficiency, speed and performance by simplifying networks and connecting people with information. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at [www.nortel.com](http://www.nortel.com).

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 © 2006 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.



> BUSINESS MADE **SIMPLE**