



## >THIS IS THE WAY

NORTEL PROVIDES ENTERPRISES A BLUEPRINT  
FOR SECURING IT INFRASTRUCTURE

>THIS IS NORTEL™

### Position Paper

#### Nortel Unified Security Framework for corporate and government security

The greater the reach and availability of the network, the greater its vulnerability to threats from within and outside the organization.

The new openness of networked communications introduces various ethical, financial and regulatory pressures to protect networks and enterprises from internal and external threats and attacks.

Every IT security professional should be up-to-date on the challenges to corporate and government security — and the latest recommendations to address those challenges.

#### Executive summary

Today's virtual enterprise<sup>1</sup> faces a security paradox. The ports and portals that welcome mobile users, customers and business partners into the trusted internal network also, if not appropriately secured, welcome uninvited users, viruses, worms and other threats.

Security breaches that threaten data privacy and protection are among the top three business issues identified by corporate chief information officers in a recent survey by market research firm, Gartner Inc., and for good reason.

Threats to wireless, wireline and enterprise networks through worms, viruses and unauthorized access are expected to cost U.S. business more than \$140 billion in 2004, according to the Federal Bureau of Investigation (FBI). The MyDoom email virus of January 2004, for example, quickly spread to computers in more than 200 countries, causing an estimated \$22.6 billion in damages in just three days. While costs of interrupted services and damage to a company's brand and reputation are key considerations for business, the broader risk of security breaches to government, institu-



A conceptual, physical, and procedural framework to secure the IT infrastructure, including clients, applications, communications services, the converged network and network management.

<sup>1</sup> The term enterprise refers to both corporate and government environments.

tional, medical and emergency services can go well beyond the financial to impact life and death situations.

With today's widespread reliance on communications as the global foundation for business and personal services, security has become a critical top priority for ensuring networks deliver trusted communications anywhere, anytime. The only effective network security strategy is one that permeates the enterprise, including people, processes and technology.

What are the requirements and vulnerabilities? What technology options and implementation choices are available? How do you protect the network at all levels?

Nortel, a global leader in secure converged networking and applications, offers proven solutions to satisfy end-to-end network security requirements. Security is one of the six elements of Nortel's Architecture for the Converged Enterprise (ACE), and is built into every element of ACE to protect enterprise resources from internal and external threats. The Unified Security Framework provides a conceptual, physical and procedural

framework for enterprise network security. It serves as an important reference guide for IT professionals responsible for designing and implementing secure networks.

This comprehensive framework addresses the pressing concerns facing IT security specialists, and offers encouraging news about the depth and breadth of options available for securing critical network, user, information and application resources.

#### **The Unified Security Framework is realistic.**

It assumes that all components of an IT infrastructure are targets... that even internal users could be network threats... attacks are inevitable... network performance cannot be compromised by processing-intensive security measures... and IT budgets are constrained.

#### **The Unified Security Framework acknowledges the diversity of networked enterprises.**

It is not a one-size-fits-all prescription, but rather a framework of functionality that offers multiple implementation choices suitable for large and small

enterprises in all industries and at all levels of government — and for diverse application requirements within all enterprise types.

#### **The Unified Security Framework addresses the multi-level complexity of network threats.**

It provides answers on multiple levels — for instance, from a firewall guardian that blocks intruders at the enterprise perimeter to endpoint security that controls network access by authenticated users (with compliant devices)... from end-to-end encryption to shroud every packet in privacy to WLAN link encryption... from virtual private networks that span the global Internet to virtual LANs that segregate network management traffic from desktop users... from virus signature detection to rate limiting and intelligent traffic management.

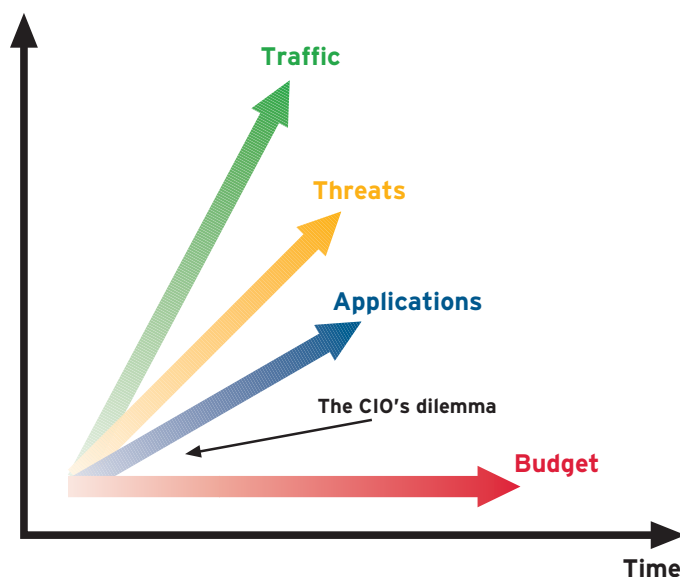
#### **The Unified Security Framework promotes a process, rather than an endpoint.**

Effective security is not achieved through technology alone. This framework outlines measures for strong ongoing security policy management, reflecting both the technical as well as the human factors that impact the security of the network.

### **Today's security realities and the requirements for a Unified Security Framework**

CIOs across all industries and in government are driven to do more with less: fixed budgets while serving demands for more bandwidth, introducing more applications and having to deal with growing security threats. Whether on an operational basis or when developing forward-looking plans, they must face a number of security realities.

**Figure 1. CIO challenges**



### **Security is not optional and is not just about technology.**

Security breaches and unlawful access to confidential data can cost enterprises millions, but the security mandate goes beyond financial incentives. The governments of many countries are enacting regulations on network security and privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act in the United States, and the Data Protection Directive in the EU. Failure to comply with these regulations brings civil and criminal penalties, even prison terms. Vulnerabilities arise both from people and process failures (such as posting their passwords in public view, or slack policy enforcement) and technology failures (such as use of VPNs that lack remote endpoint security) — and combinations of all three. A security framework must allow enterprises to develop and enforce risk-optimized security policies across increasingly converged environments, which address process and technical considerations as well as regulatory mandates to protect data integrity and confidentiality.

### **The bad guys have good guns.**

Attackers have a broad repertoire of tools and techniques they can use to compromise a network. These include IP spoofing, network sniffers, bucket brigade attacks, denial-of-service attacks and masquerading. Worms can include Trojan horses which lie dormant and later use victim machines to launch other attacks. The increasing sophistication of attacks and the increasing speed at which they are propagated are major concerns. A security framework must deliver a range of protection mechanisms to thwart these attacks, which can be deployed as required to mitigate business risk, and to quickly respond to newly identified vulnerabilities.

### **It's not enough to guard the front gate.**

The typical enterprise “internal” trusted network is being extended to include supply chain partners, telecommuters, remote access users, Web users, application service providers, disaster recovery providers, and more. As a result, the avenues for security threats are expanding from the gateway to the Internet to multiple entry points including wireless LANs, and mobile devices of all sorts, including laptops, PDAs and cell phones. Every component of the IT infrastructure is susceptible to attacks. For example, PCs and IP phones, application and IP Telephony servers, routers and switches can be attacked from inside or outside the enterprise. In addition, disgruntled employees and others can misappropriate network resources for personal gain. A security framework must permeate the network end-to-end and enforce corporate policies on multiple levels — user, application and network — and at multiple points in the network using multiple approaches to threat detection and prevention.

### **Frisking everybody and everything takes time.**

Turning up the full complement of security features can slow Web servers and legacy routers to a crawl as they bog down with processing-intensive encryption, decryption, key management, deep packet filtering and more. Voice applications are particularly sensitive to delay and jitter. A security framework must deliver the Quality of Experience expected by users, by including purpose-built security solutions that use innovative acceleration technologies to minimize latency and maximize application throughput.

### **You're never totally secure.**

Security is not an end point, but rather a process including an evolving way of thinking about how to protect systems, networks, applications and resources. Corporations and government institutions need to continuously (re-)assess risk, identify the nature of new vulnerabilities, and determine how processes and technology need to evolve. Even with the best planning, **you will be attacked**; a sound philosophy is to recognize this reality and be ready to isolate the attack as quickly as possible. Therefore, network survivability dictates that the network must continue to operate — delivering business-critical services in a timely manner, even if parts of the network are quarantined or disabled due to an overt attack. A security framework must deliver continuous feedback and improvement, reflecting the latest industry knowledge and best practices, as well as define ways to minimize the impacts of attacks.

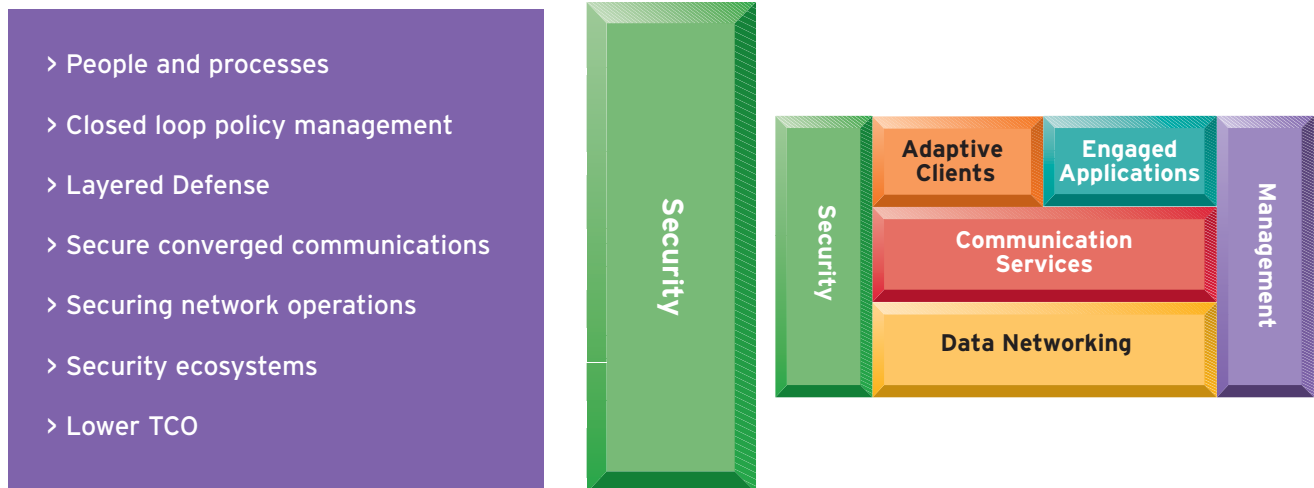
*What can security IT professionals do about the security given these realities?*

## **The Nortel Unified Security Framework**

The Nortel Unified Security Framework defines a conceptual, physical and procedural framework of best practices for end-to-end enterprise network security. At the heart of this comprehensive security framework are seven key attributes as identified in Figure 2 and discussed throughout this document.

1. **People and processes and technology alignment** meeting enterprise security objectives
2. **Closed-loop policy management**, including configuration of edge devices, enforcement of policies in the network, and verification of network functionality

**Figure 2. Attributes of the Nortel Unified Security Framework**



3. **Layered Defense** across the enterprise, providing endpoint security, perimeter security, communications security and core network security as well as many different approaches to enforcement ranging from access lists to behavior anomaly detection
4. **Secure converged communications** for IP Telephony and unified communications (which includes multimedia) by hardening clients, gateways and servers; by establishing multimedia zones and by leveraging layered network security
5. **Secure network operations**, by physically or logically partitioning network management from user traffic, and applying recommended security mechanisms to operational activities
6. **Security ecosystems**, leveraging standards and best-in-class security technologies, to allow extended security solutions through partnerships
7. **Lower TCO**, allowing increased security functionality to be delivered, while lowering the total cost of ownership of these solutions

The seven key attributes of the Unified Security Framework offer enterprises a security blueprint to use as they move towards convergence on the one hand and increasingly open environments on the other.

Nortel recognizes that each enterprise has unique business needs and networking environments. In general terms, some are relatively closed enterprises, using private lines between sites, with dial-up Internet access for selected users. Other more extended enterprises use IP virtual private networks (VPNs) and offer Internet access for most employees. Yet others are relatively open enterprises, which allow partners, suppliers and customers into the internal trusted network via the Internet. That means the “right” security strategy is neither a ‘one size fits all’ nor a static implementation. The Unified Security Framework allows enterprise security solutions to be tailored to the individual needs of enterprises.

#### **People and processes**

The Unified Security Framework calls for developing and enforcing security policies that address technical considerations, and business and human aspects of security. A properly designed and

implemented security policy is an absolute requirement for all types of enterprises and has to be owned by one group. It is a living document and process, which is enforced, implemented and updated to reflect the latest changes in the enterprise infrastructure and service requirements. The security policy clearly identifies the resources in the enterprise that are at risk and resulting threat mitigation methodologies, whether these are procedural or electronic. It defines which users or classes of users have access to which resources, and defines the use of audit trails to help identify and discover violations and the appropriate responses.

The Unified Security Framework allows security policies to be translated into technical security mechanisms to be used by the policy management system and deployed across the IT infrastructure.

#### **Closed-loop policy management**

Policy management addresses the full realm of security components — firewalls, intrusion detection systems, access lists and filters, authentication techniques, and more — along with a system-wide view of network environments, including IP Telephony and data center, wired and wireless campus, remote office and teleworker environments.

Closed-loop policy management includes configuration management of network devices, enforcement of policies in the network, and verification of network functionality via audit trails. Verification and audit trails close the loop on policy management, and result in updates to the policy to reflect corrective actions. Policy management operates at a granular

level to address each element of the end-to-end security system, while providing centralized control and accountability. Centralization ensures that security parameters are set consistently across multiple nodes, and that multiple policies for different administrative domains together reflect enterprise-wide policy and inter-domain consistency.

### Layered Defense

According to Gartner<sup>2</sup>, “Enterprises that rely only on proxy or stateful packet inspection will experience successful application-layer attacks at twice the rate of enterprises that use leading deep-packet inspection approaches.”<sup>2</sup> For protection against a broad range of security threats, multiple layers of network security are necessary (see also Figure 3).

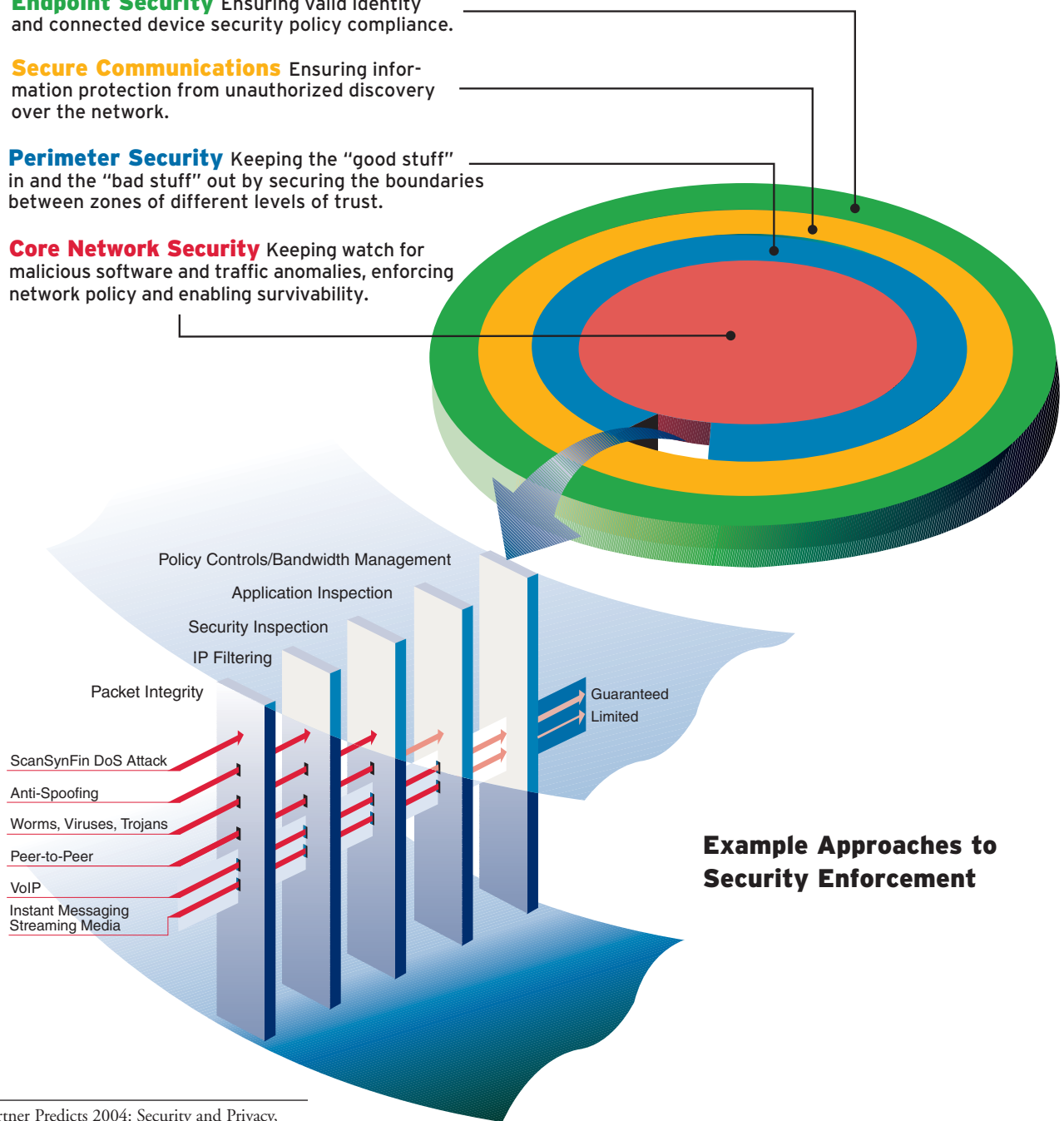
**Figure 3. Functional elements of a Layered Defense approach to network security**

**Endpoint Security** Ensuring valid identity and connected device security policy compliance.

**Secure Communications** Ensuring information protection from unauthorized discovery over the network.

**Perimeter Security** Keeping the “good stuff” in and the “bad stuff” out by securing the boundaries between zones of different levels of trust.

**Core Network Security** Keeping watch for malicious software and traffic anomalies, enforcing network policy and enabling survivability.



<sup>2</sup> Gartner Predicts 2004: Security and Privacy, 20 November 2003.

- › Endpoint security, whether local or remote and whether wired and wireless, ensures that only authenticated users and compliant devices can connect to the network and that these are authorized to access certain application and networking resources (all based on the enterprise security policy).
- › Secure communications provide link level or end-to-end encryption for signaling and/or payload as appropriate.
- › Network perimeter security protects application resources by ensuring that only legitimate traffic is permitted between trusted domains (whether physical or logical), these being defined organizationally (e.g., finance, HR) or functionally (e.g., data center, multimedia zone) following the enterprise security policy.
- › Core network security protects the overall IT infrastructure from malicious attack, ensuring that any threats that transgress perimeter or endpoint security are eliminated and that network operation, particularly for mission-critical communications, is maintained even under attack.

This illustrates Nortel's belief in implementing security in a similar way to which we have built highly reliable networks, by removing single points of failure. This philosophy ensures that security implementations are both secure and resilient. If a primary layer of security is breached, the secondary layer (or tertiary, etc.) is in place to thwart the attack. While these layers can represent specific areas within a network, they can also represent multiple approaches to security enforcement. For example, approaches can be based on simple traffic rules in a firewall, vulnerability pattern matching, anomalous behavior discovery, priority application attack protection, etc. By placing different forms of security at different layers or places in the network, overall security is

increased: threats that may pass one layer can be caught by another layer.

The power of the Layered Defense is that industry-defined security functions are leveraged in a structured fashion, tightening security overall. Finer-grained security and policy enforcement can be deployed the closer one gets to critical resources. To ensure survivability under attack, network services are organized into essential and non-essential services and mechanisms defined to quickly isolate attacks, allowing essential services to continue to be provided. The most effective approaches combine multiple resistance, identification and recovery strategies in an adaptable manner that responds to changing network conditions. For example, Layered Defense allows the enterprise to:

- › Quickly disable ports that are implicated in an attack
- › Segregate network servers and domains to limit the impact of an attack
- › Quickly recover from a successful system breach through backup/restore
- › Provide redundancy so backup resources are available if necessary
- › Protect and prioritize critical traffic and applications

### Secure converged communications

Unified networks can carry voice, data and video — each with their unique performance requirements and security considerations. When and where to protect this traffic is a major consideration, and is a key element of any enterprise security policy. Unified communications (which includes IP Telephony and real-time multimedia) represents a particularly important class of application. The IP networking infrastructure that supports unified communications must be secure from a data perspective and engineered to meet the

stringent latency and reliability requirements of multimedia. Security must be holistic and span the entire telephony environment, including IP Telephony clients and servers, application servers and related multimedia services (such as multimedia conferencing and contact centers), and traditional PBXs.

Segregation of traffic is an important tool for securing converged communications. VLANs (Virtual LANs) segregate voice users into their own private local area networks. Cross-traffic from other VLAN segments is strictly controlled or prohibited. Virtual private networks (VPNs) secure communications to and from the enterprise by creating encrypted 'tunnels' across the Internet using IPSec and SSL as appropriate. VPNs enable secure mobility — secure access to authorized remote users and business partners — without requiring dedicated connections, anytime and from any location or device.

Finally, mechanisms such as Transport Layer Security (TLS) and Secure Real Time Protocol (SRTP) are being introduced to provide end-to-end encryption of telephony and multimedia control traffic and of the media, respectively.

### Secure network operations

Because of the greater access authority and functional privileges granted to network management personnel, their access and activities must be carefully secured to protect network configuration, performance and survivability. Secure network management requires a holistic approach, rather than a specific security feature set on a network element. The Nortel Unified Security Framework defines nine critical areas to secure network operations:

- › **Secure activity logs** such as Syslog provide a verifiable audit trail of user or administrator activities and events generated by network devices.

## A security framework must allow enterprises to develop and enforce risk-optimized security policies across increasingly converged environments

- › **Network operator authentication** based on strong centralized administration and enforcement of passwords ensures that only authenticated operators gain access to management systems.
- › **Authorization for network operators** uses authenticated identity to determine the user's access privileges — what systems they can access, what functions they can perform.
- › **Encryption of network management traffic** protects the confidentiality and integrity of network management traffic — especially important with the growing use of in-band network management in an IP network environment.
- › **Secure remote access for operators** extends protections to operators and administrators who manage the network from a remote location using mechanisms such as SSL and IPSec.
- › **Firewalls and VLANs** partition the network to segregate management devices and traffic from other, less confidential systems such as public Web servers.
- › **Intrusion detection systems** in management servers defend against network intrusions by warning administrators of potential security incidents, such as a denial-of-service attack.
- › **Hardening operating systems** used for network management close potential security gaps in general-purpose operating systems and embedded real-time operating systems.
- › **Anti-virus protection** scans in-house and third-party software packages with virus-detection tools before incorporating the software into a product or network.

### Security ecosystems

The term 'ecosystem' is a common industry term. Nortel applies this term to a process whereby the business value of solutions can be expanded through partnerships leveraging open solutions and standards, and thus unleashing innovation. For the enterprise, implementing security ecosystems across their IT infrastructure brings with it multiple benefits: open interoperability leveraging best-in-class technologies; increased agility to changing environments avoiding vendor lock-in; and lower risk through Layered Defense architectures.

Nortel's unique position at the intersection between users and applications, and data networking, allows it to develop open ecosystems of developer partners to bring together extended solutions to enhance human experience, ignite global commerce and of course secure information. The security dimension is defined through the Unified Security Framework.

Nortel participates actively in ongoing security standards development within the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU), and the European Telecommunications Standards Institute (ETSI) for a broad range of security standards including WLAN security (802.11i), AES, IKEv2, TLS and SIP-TLS, and with certification authorities such as Common Criteria, FIPS140 and ICOSA.

Nortel partners with best-of-breed security application vendors to ensure seamless interoperability for multiple methods of authentication (hardware and software tokens, smartcards, biometrics),

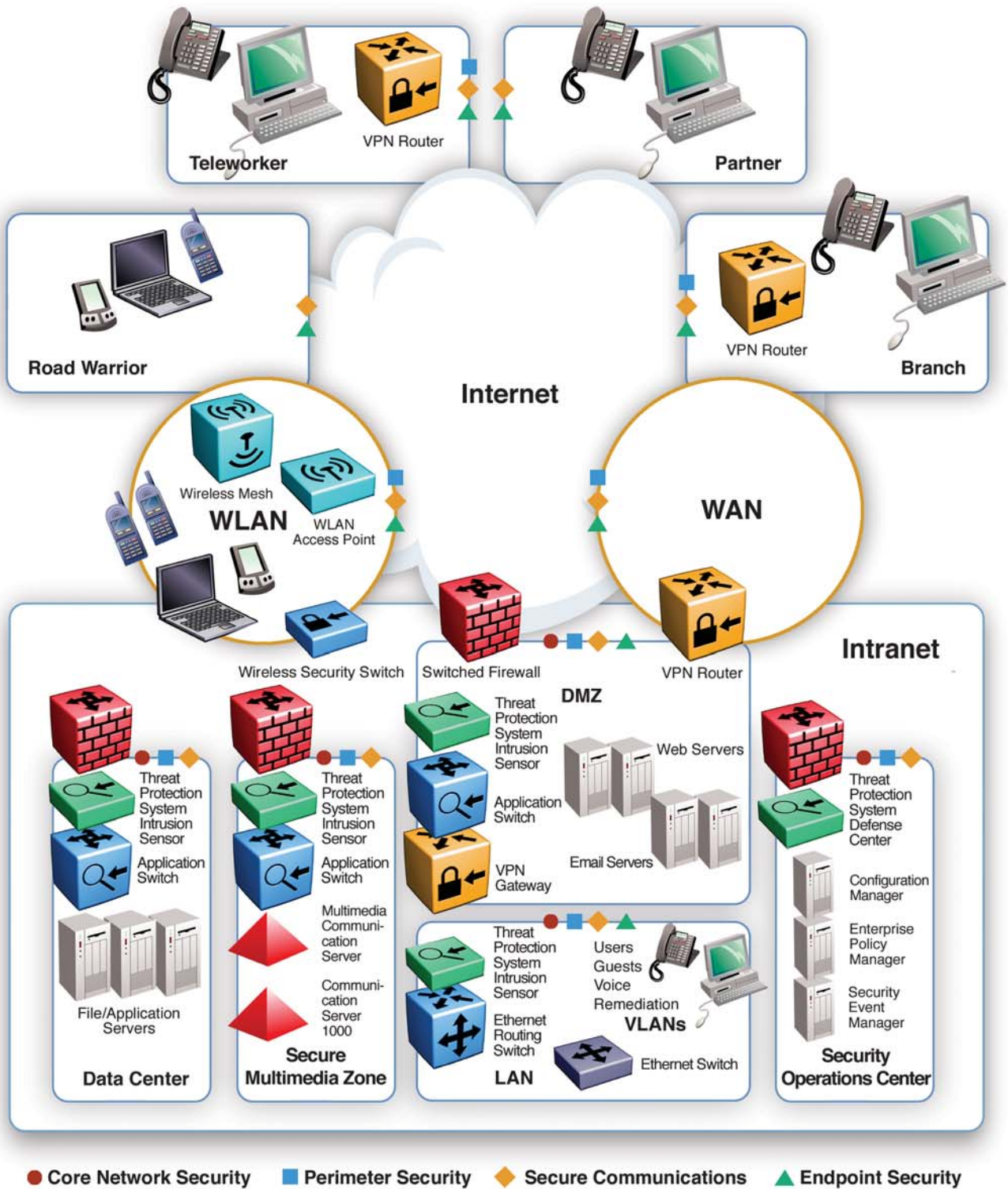
personal firewalls and anti-virus protection. For example, Nortel partners with Check Point™ on firewall technology, with DataPower™ on secure XML processing, with Guardednet™ on secure event management, with Sygate™ for endpoint security solutions for large enterprises, and with Symantec on next-generation security systems. Nortel also partners with service providers to enable them to offer best-in-class secure managed service solutions. For example, our VPN systems have been deployed by the majority of the world's leading service providers for their managed IP-VPN services.

### Lower TCO

IT executives have had to reassess the way they build, manage and use their information infrastructure. Convergence is seen as a strategic imperative, whether in the form of organizational convergence (e.g., one voice and data group), network convergence (i.e., one network), communications convergence (e.g., unified communications) and application convergence (e.g., bringing people and business processes closer together). This drives the opportunity of having one IT infrastructure to plan, build, make reliable, operate and protect, particularly in light of increasing security threats, not just from the Internet at large but from virtually any port in the network.

The Nortel Unified Security Framework recognizes that it is very important to architect network security to meet business objectives (as outlined in the enterprise security policy), while having the ability to deploy security functionality in the optimal way with an eye on mini-

Figure 4. A network example of Layered Defense network security



Nortel recognizes that each enterprise has unique business needs and networking environments.

mizing the impact on the TCO of the entire IT infrastructure. The keys to lower TCO include:

- › Layered Defense approach to network security, applied across functional elements (e.g., endpoint security, perimeter security, secure communications and core network security), leveraging multiple approaches to security enforcement, and targeting specific solutions (e.g., data center asset protection, remote access, unified communications) to ensure that security investments are optimized
- › A high degree of centralization to avoid the need to frequently upgrade edge devices
- › Network-based intelligence to minimize impacts on endpoints/client
- › Closed loop policy management systems, including comprehensive monitoring and configuration management to ensure optimal utilization of security capabilities

## The Nortel advantage

Nortel's experience in all network types — wired and wireless, voice and data, enterprise and carrier — and its technology strengths in hardware accelerated deep packet inspection and processing and in scalable and reliable multimedia networking uniquely position Nortel, with its partners, to deliver on the industry's need for ironclad, secure communications, anywhere, anytime and on any device. Towards this end, Nortel works with a number of international private and public sector organizations, to identify new threats and develop solutions on a cross-industry, worldwide basis.

For example:

- › **Internet Security Alliance.** Nortel is a founding sponsor of this organization, 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.

- › **National Reliability and Interoperability Council (NRIC).** Part of the Homeland Security Working Group, the NRIC works to ensure the optimal reliability, interoperability, accessibility and interconnectivity of public telecommunications networks.
- › **The Telecommunications — Information Sharing and Analysis Center (Telecom-ISAC).** Nortel cooperates with this subgroup of the National Coordinating Center for Telecommunications (NCC), which gathers information on threats, outages, intrusions and anomalies; analyzes and sanitizes the information; disseminates the information in accord with sharing agreements; and alerts others in “near real time.”
- › **National Security Telecom Advisory Committee (NSTAC).** Nortel participates in the Network Security Information Exchange (NSIE) subcommittee of this group, driving the establishment of a common security baseline for enterprises and carriers to reduce customer operating expense and vendor R&D expense.
- › **Joint Group on Network and Information Security (NIS).** This is a European initiative formed by ETSI and the European Committee for Standardization. NIS helps coordinate effective use of security standards to establish trust on the Internet. Nortel chairs NIS.

In addition, Nortel maintains an internal cross-functional team — the Security Advisory Task Force (SATF) — that reports to the Chief Technology Officer

and addresses security vulnerabilities that could impact Nortel 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, SANS and ISA to ensure rapid awareness of new vulnerabilities. A process has been established to determine the level of risk of each potential vulnerability to Nortel customers, along with a risk mitigation plan, where required.

Nortel Security Solutions enable corporations and governments to confidently and confidentially leverage their IT infrastructures for competitive advantage (Figure 4). Nortel secures communications through seamless SSL and IPsec VPNs. Nortel secures the network perimeter through Advanced Firewall Technologies, protecting the network and applications from worms, Denial of Service attacks and other threats to network resources. Nortel secures network endpoints through the Nortel Secure Networks Access Solution that leverages both remote access Tunnel Guard protection and LAN-based 802.1x authentication. Nortel secures IP Telephony and unified communications by leveraging its heritage in telephony and its expertise in network security. Nortel WLAN security simplifies management and provides security to the total wireless LAN from a central point. Nortel's full portfolio of Homeland Security solutions provides real-time support in emergency situations and secures critical infrastructures.

In addition, Nortel partners with security services vendors with CISSP certification, and other security professionals, to provide security deployment assistance, security training, security assessments and regular security audits to validate the robustness of new security products and practices.

## Summary and call for action

As we become more dependent on a single, converged network, security is becoming increasingly critical to meeting business and IT objectives. The flexibility of the Unified Security Framework ensures corporations and governments can secure their networks, regardless of the nature of threats, size of network, or the enterprise business priorities. This approach to security combines strong policy management and enforcement, provides a choice of security solutions that are modular, flexible and scalable, and equips companies with the appro-

priate tools, policies and practices to effectively secure their IT infrastructures. Nortel's Unified Security Framework provides enterprises with a framework for considering all aspects of network security — the people, processes and technologies.

So where to next? If you have a security policy and organizational accountability, you're on the right track. As part of your ongoing security process, maybe it's time for a vulnerability assessment to highlight weak points in your layered security environment. If you're rolling out IP Telephony, then you need a plan

to ensure that this new converged environment is secure and continues to be. In fact, not all IP Telephony systems are designed with the same level of security in mind. In Nortel's Unified Security Framework, this plan should include telephones themselves and communication servers, establishing voice security zones and fully leveraging the underlying infrastructure. Nortel and its partners can help.

For more information on Nortel security solutions, please visit us on the Web at [www.nortel.com/enterprisesecurity](http://www.nortel.com/enterprisesecurity).

### In the United States:

Nortel  
35 Davis Drive  
Research Triangle Park, NC 27709 USA

### In Canada:

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

### In Asia Pacific:

Nortel  
Nortel Networks Centre  
1 Innovation Drive  
Macquarie University Research Park  
Macquarie Park NSW 2109 Australia  
Tel: +61 2 8870 5000

### In Greater China:

Nortel  
Sun Dong An Plaza  
138 Wang Fu Jing Street  
Beijing 100006, China  
Phone: (86) 10 6510 8000

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. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. 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.

This is the Way. This is Nortel, Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2005 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.

