NORTEL

Position Paper

Layered Defense approach to network security

Protecting the enterprise network

Taking a Layered Defense approach to security is a key attribute of the Nortel Unified Security Framework and offers enterprise and government customers many options to implement a security architecture solution that is most effective for their own unique network and business security needs.

Overview

Merely one virus, the My Doom email virus, is estimated to have cost enterprises $22.6B (mi2g Intelligence Unit). These costs don't fully reflect the damage that negative publicity can cause an organization which has been attacked. The increasing sophistication of such viruses and worms — with payloads that could include Trojan horses which lie dormant and later use victim machines to launch other attacks — and the speed at which they are propagated are of great concern. The speed with which exploits to known vulnerabilities are released is also increasing. Additional avenues for threats come from new applications on networks, specifically given the growth in public Instant Messaging and Peer-to-Peer networks for file sharing.

Today's enterprises and governments are enjoying the many benefits of greater communications with fewer boundaries between them and their business partners, customers and remote employees. While there are many benefits, they can be outweighed by the various risks of doing business on public networks or open intranets. Organizations must still make the right business decisions to appropriately protect their assets, sensitive information (payroll, research and development, etc.) and their customers' privacy. With their increasing business on public networks and the mobility of

Table of Contents

An enterprise's need to communicate with its remote employees, business partners and customers should not be hampered by the threats public networks can harbor.

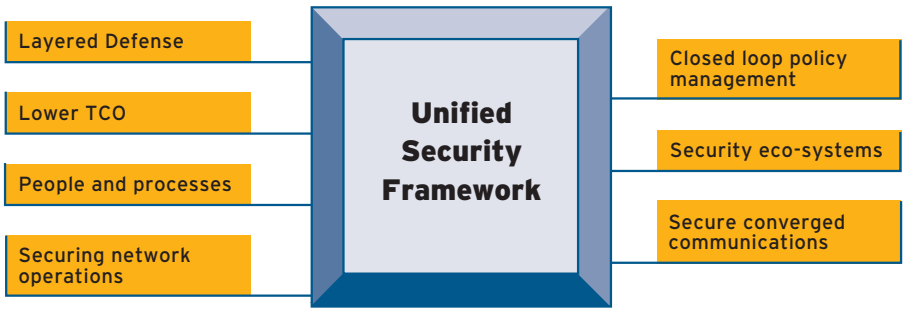
their workforce, enterprises are unfortunately more likely today than ever to be victims of worms, viruses, denial of service attacks, and online fraud or theft. A combination of developing and enforcing security policies that address the technical, business and human aspects of security, choosing the right security solutions and putting the appropriate processes in place will help enterprises face these challenges directly while meeting new compliance regulations. A properly designed and implemented security policy is an absolute requirement for all types of enterprises and should be a living document and process, which is enforced, implemented and updated to reflect the latest changes in the enterprise infrastructure and service requirements. Ultimately, a solid approach to network security not only ensures security of your network, but your overall network reliability, resiliency, business continuity and business productivity.

Nortel Layered Defense

Securing the network perimeter and prohibiting unauthorized access from within can prove to be a daunting challenge. Today's businesses must guarantee uninterrupted access to network resources and the applications they support; and a consistent quality of experience for real-time applications, such as IP telephony and unified communications services. Products must be designed with a high level of resiliency and security even under attack. Evolution of the enterprise and the way it does business, coupled with today's network threats, has reduced the effectiveness of traditional perimeter security. Nortel secures communications, information and applications anywhere, anytime. To that end, Nortel has devised a paradigm for enterprise network security which recognizes the need for flexible and extensible security with low management overhead. This paper describes Nortel's Layered Defense approach to network security. Layered Defense is a key attribute of the Nortel Unified Security Framework model[1] (Figure 1) and is designed to ensure there are no single points of security failure in a network. This is accomplished by using multiple approaches to security enforcement at multiple areas within a network. This approach is bolstered by leveraging open solutions that utilize security capabilities and products from best-of-breed security vendors. For example, Nortel has strategic alliances with leading security vendors such as Symantec™ and Check Point Software Technologies™, and leverages applications from various third-party partners through Nortel's Developer Program for Security. More detail on this program can be found at: *http://www.nortel.com/solutions/securenet/sec_partners.html*. With this open, standards-based approach, Nortel's security solutions provide security for the entire enterprise network — remote and local network users, data and multimedia, wired and wireless connections.

Nortel has over 100 years of experience building reliable, secure communication

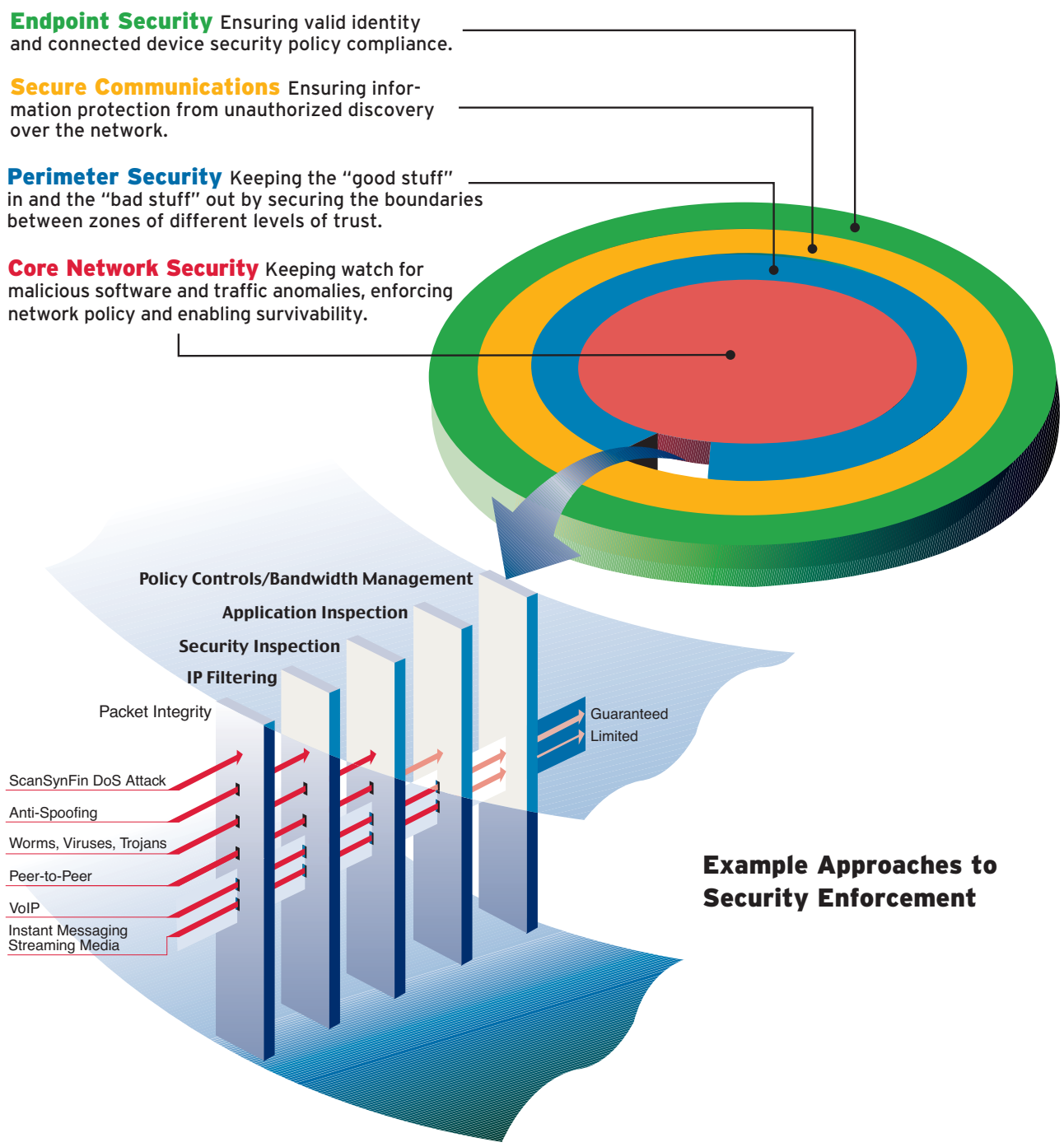
Figure 1. Unified Security Framework



A Layered Defense uses multiple approaches to security enforcement at multiple areas within a network. This approach removes single points of security failure in order to secure enterprise information assets.

[1] Unified Security Framework position paper, document number NN104120

Figure 2. Layered Defense — multiple approaches to security enforcement at multiple areas within a network

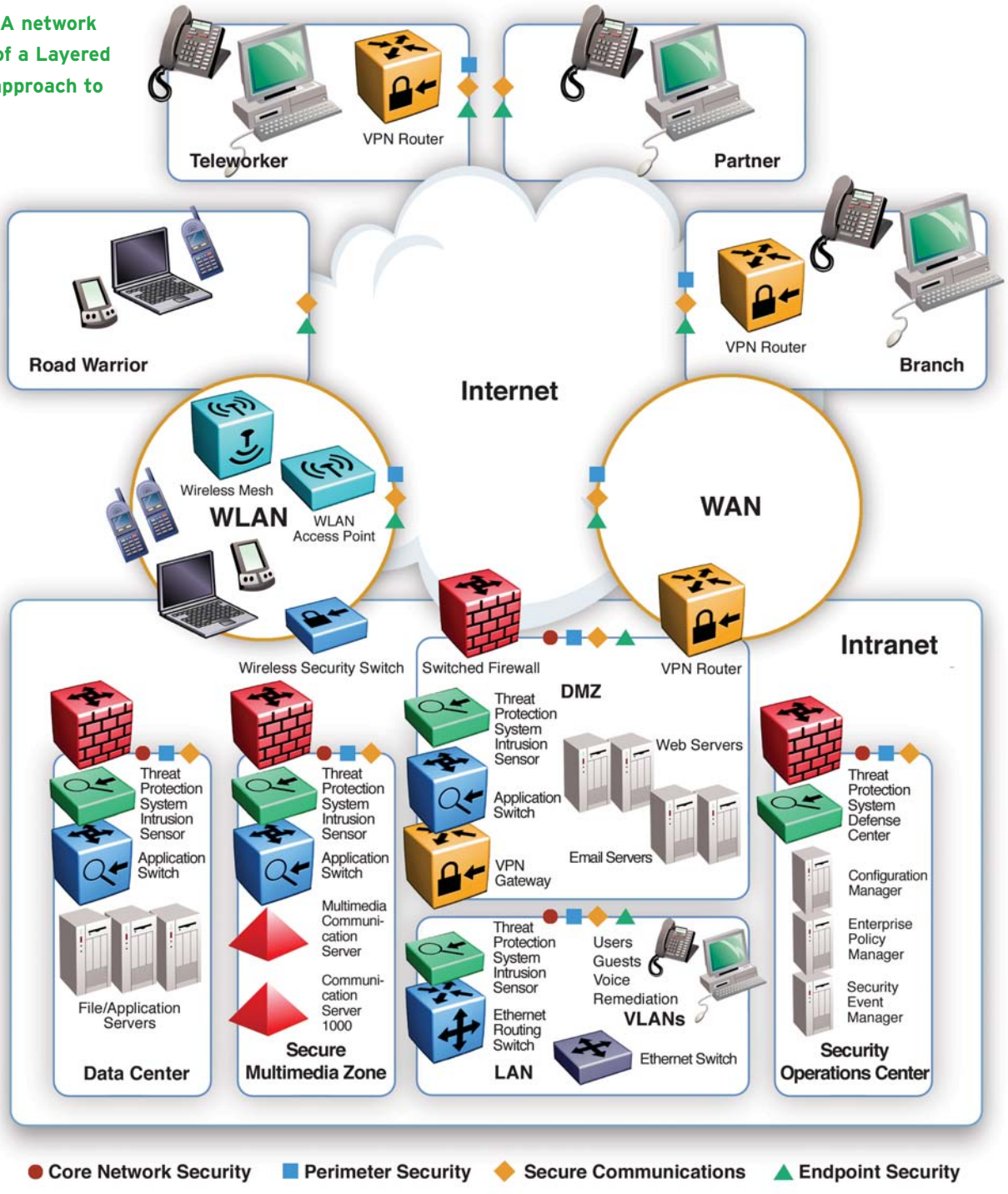


systems. Leveraging this highly available network experience led Nortel to develop the Layered Defense approach to network security. For protection against contemporary network security vulnerabilities and future threats, multiple approaches to security enforcement at multiple areas within a network are required. Deploying security solutions at remote endpoints and desktops, the network and department perimeter down to the core network (Figure 2), while also using multiple approaches to security such as filters for signatures and keywords for common attacks, encryption, stateful firewall inspection of known protocols, anti-virus and intrusion protection software are examples of necessary components. According to Gartner, "[Organizations] that rely only on proxy or stateful packet inspection will experience successful application-layer attacks at twice the rate of [organizations] that use leading deep-packet-inspection approaches."[2]

[2] Gartner Predicts 2004: Security and Privacy, 20 November 2003

Nortel's Layered Defense approach, announced in September 2002 as an attribute of the Unified Security Framework, provides a number of security technology and process options to effectively secure against today's and tomorrow's network threats. This paper builds on the architecture of the Unified Security Framework to explain specific technology and product solutions within Nortel's Enterprise portfolio that can enable an enterprise or government Layered Defense security posture. With security solutions that presume a multi-vendor network, customers can pick and choose which Nortel solutions they want to leverage in a heterogeneous environment. Based on open, standards-based solutions, this approach enables easy integration and simplified operations that reduce the overall network security total cost of ownership. The following sections of this paper describe Nortel security technology and products (Figure 3) in the context of broad functional security solution components such as **Endpoint Security, Perimeter Security, Core Network Security, Secure Communications and Security Management & Platform Security** that make up Nortel's Layered Defense approach.

Figure 3. A network example of a Layered Defense approach to security



Endpoint security — Blocking threats at the source

As employees, business partners and customers make more use of the enterprise network to meet their business objectives, enterprises need more control of the endpoints that are used to access the network. Because so many threats are from internal users on the network, this must include wired and wireless endpoints within the network as well as those at remote endpoints, where there is less control over the user's device. The Nortel Secure Network Access Solution solves these issues by checking to ensure the latest anti-virus or firewall applications, definitions or software patches are installed and running on any and all devices before users are authorized to access the network. The Nortel Secure Network Access Solution is device agnostic, and implements consistent, intelligent, user-based policy management across the enterprise network, providing proactive, continuous traffic analysis for any possible security attacks. The following sections describe the components of this solution.

Internal endpoint security — *802.1x and device authentication*

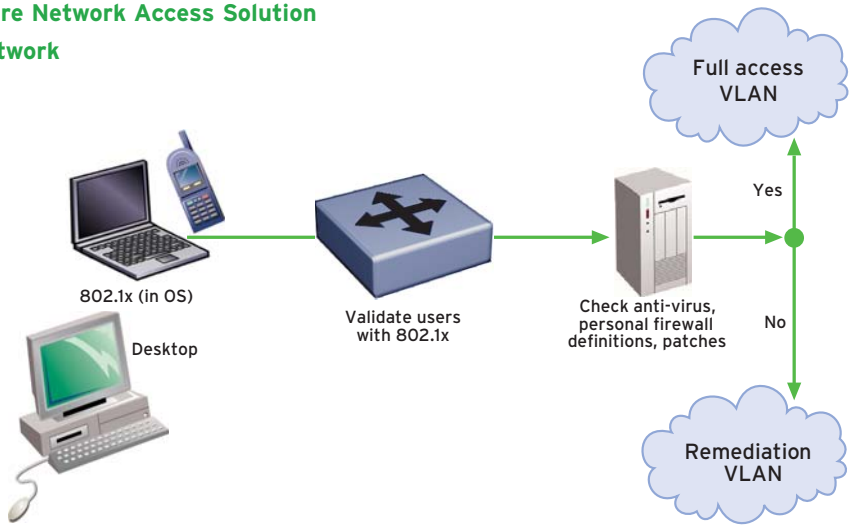
For protecting internal devices connecting to the network, Nortel's Ethernet Switch (formerly known as BayStack*) and Ethernet Routing Switch (formerly known as Passport*) portfolios support 802.1x/EAP authentication verifying someone connecting inside the network is in fact a legitimate user. The switches go one step further and can interoperate with third-party vendor solutions to check the endpoint security posture — virus and firewall definitions — and ensure compliance with organization security policies. Non-compliant systems attempting authentication to the switches are blocked and placed in a remediation VLAN. Updates can be pushed to the internal user's device and users can then subsequently re-attempt to join the network (Figure 4). Nortel Ethernet Switches and Ethernet Routing Switches also support Media Access Control (MAC) address filtering as an added form of access control.

Wireless Local Area Network (WLAN) — specific protections

Nortel's WLAN solutions provide a number of additional security capabilities to ensure security for wireless network segments. The latest industry security standards such as Wi-Fi Protected Access (WPA) and WPA2 provide strong wireless user authentication and Layer 2 encryption mechanisms using 802.1x, Temporal Key Integrity Protocol (TKIP) and CCMP. To reduce the incremental processing burden on backend authentication servers, the WLAN solution incorporates a unique 802.1x acceleration feature. The WLAN Security Switch offloads the key generation and management processing for EAP-TLS, PEAP and MD5 implementations to improve performance. User authentication can also be enforced with a Web-based AAA approach in which new users are directed to a captive portal for authentication before they can get a network IP address. During authentication, the WLAN establishes a unique user identity which is used to define specific policies including Layer 3/4 access privileges, VLAN and subnet assignments, and even time-of-day, week and location-based access restrictions. The associated mobility architecture helps ensure that these policies are enforced regardless of where the user roams.

Unauthorized rogue access points can present a significant security threat if they do not comply with enterprise security policy. The WLAN system will

Figure 4. Nortel Secure Network Access Solution at work inside the network



identify, classify and map the location of rogue APs, send an alarm to the administrator, and then initiate an orchestrated containment attack from neighboring legitimate APs to contain the threat. Similarly, the system will identify jamming, flooding and RF-based DoS attacks and alert administrators of the type of attack and map the location of originating source.

Remote endpoint security

In external remote environments where there is less control over where and how the end-user device is used (e.g., for personal e-mail systems, Instant Messaging and Peer-to-Peer file sharing), processes to check for viruses and other threats once a device connects to the network environment are even more critical than ever before. This protects the organization from mobile employees and business partners who may not be aware of the extent of such threats. The Nortel Secure Network Access Solution leverages a feature called Tunnel Guard for its VPN router and VPN gateway solutions to validate the security posture of an endpoint device, including the status of executables, software versions and operating system, before accepting or rejecting the endpoint VPN connection to the network. This solution can be implemented without the need for maintaining a software agent on the endpoint device, enabling partner and employee device interrogation without the costs associated with client management. Tunnel Guard additionally provides an open API that third-party software vendors can use to perform more detailed self checking and automatic software updates on the remote endpoint. Symantec™ is an example of a vendor that interfaces with this API.

Policy-based user provisioning

Policy-based networking takes a step beyond 802.1x/EAP authentication into the network. It is designed to ensure that users or a group of users (e.g., all employees of a financial department) have access to *only* those services authorized and marries that authorization to individual user-based security policies based on individual, departmental or corporate policies. Nortel's Enterprise Policy Manager (formerly known as Optivity* Policy Services) supports the network infrastructure that performs 802.1x authentication against RADIUS and other authentication, authorization and accounting (AAA) repositories to authenticate the user, grant access to specific authorized applications and provide real-time policy-provisioning capabilities across Nortel's devices on the network to mitigate the swift penetration of a virus or worm.

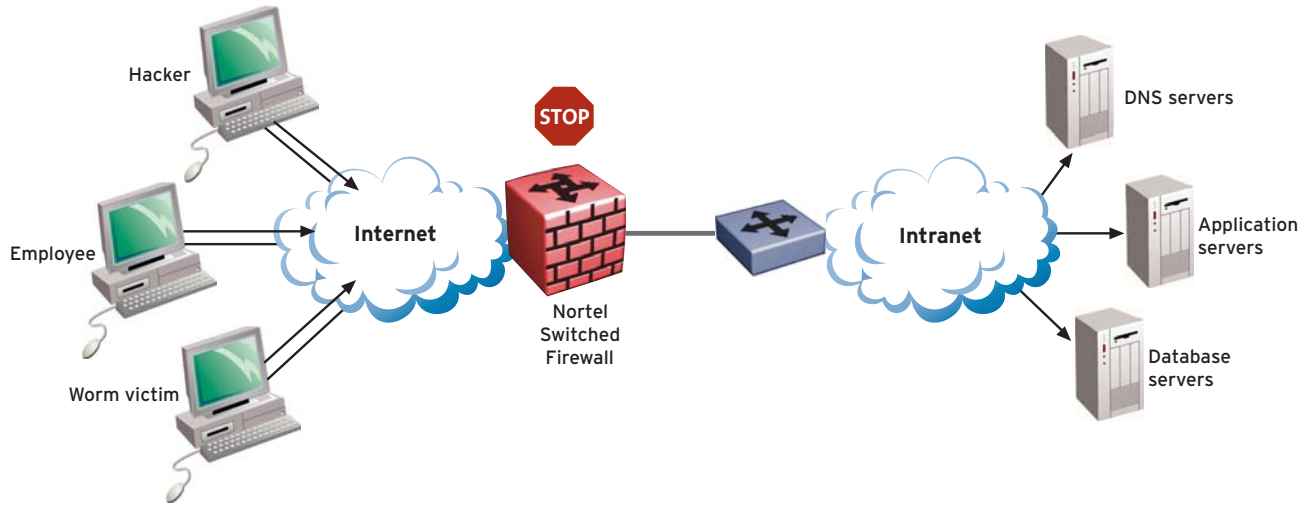
Securing the perimeter

Nortel provides a number of options for protecting the perimeter — be it an internal perimeter around departments, secure multimedia zones to protect multimedia and IP Telephony call servers, or at the external edge of the network. VLANs are an important Layer 2 mechanism to define internal perimeters. No matter what your business need, Nortel perimeter security products are designed to ensure you can effectively and efficiently secure boundaries between network zones of differing levels of trust, enabling your business to ensure your information assets are protected without minimizing business agility.

Firewalls

Firewall technologies have advanced from traditional packet filters to more sophisticated, state-aware, packet filtering firewalls. Today's next-generation firewalls, such as the Nortel Switched Firewall (formerly known as Alteon* Switched Firewall), perform deep-packet inspection to detect and block attacks that directly target applications and data using the packet payload. Deep-packet

Figure 5. Perimeter protection from threats (DoS, virus, worms, etc.)



inspection, Layer 4-7 content filtering and DoS protection within the operating system of the Nortel Switched Firewall (Figure 5), along with the complementary Layer 2-7 security enabled by the Check Point™ NG Application Intelligence engine, provide multiple layers of multi-gigabit protection at the perimeter. For additional perimeter protection, the Nortel Switched Firewall can load balance multiple groups of intrusion sensors. The integration of Nortel's switch-accelerated platform with Check Point Next Generation software provides perimeter protection without relinquishing application performance, incorporating deep packet inspection with a Denial of Service signature database which identifies the most popular attacks: Teardrop, Smurf, Ping of Death, SQL Slammer, LAND, etc.[3] Designed specifically for the support of real-time applications such as VoIP and multimedia, the Nortel Switched Firewall provides protection while maintaining user quality of experience. The Nortel Switched Firewall can also leverage the five 9's reliability of the Ethernet Routing Switch 8600, which can support up to four firewalls on its Service Delivery Module.

Nortel VPN Routers (formerly known as Contivity*) include a full-featured stateful inspection firewall that provides gateway and branch office firewall protections in a single platform with state-of-the-art VPN capability. This ensures that encrypted traffic is also firewall-inspected. Firewall user authentication in the VPN Routers goes one step further in providing fine-grained access to network resources based on user, whether over a tunneled or non-tunneled connection.

Nortel WLAN Security Switches feature Layer 3/4 traffic filters but also extend these access control policies to include time-of-day, day-of-week and location-based restrictions. Additionally, specific authentication and encryption types can be enforced on a per-user basis where failure to comply results in denied access.

Nortel Ethernet Switches provide policies which can direct application-specific (e.g., IP Telephony) traffic to a firewall, and separate it from the data traffic through the network. The switches can do this while also providing the QoS necessary for delay-sensitive traffic, such as voice, to ensure the highest priority on the network. IP filters and access control lists (ACLs) can also be used as additional granular enforcement tools to protect against unauthorized access.

Network killer and intelligent traffic management protection

Nortel Application Switches (formerly known as Alteon Application Switches) can provide perimeter security protections for network killer attacks (e.g., high volume DoS, virus and worm attacks) in addition to application delivery capabilities (e.g., load balancing, bandwidth management). This makes it the perfect component of a solution for providing perimeter protection around a set of high-value latency-sensitive application servers (e.g., VoIP, SIP multimedia, ERP, CRM, etc.) or a data center. This placement also provides protection against internally originated threats. The primary perimeter security capabilities of the Application Switch are Denial of Service/virus/worm attack signature recognition and blocking as well as application (P2P, mail, ERP, SAP, etc.) monitoring, policing and blocking. The Application Switch supports thousands of filters as well as delayed binding which acts as a proxy to the Web servers until TCP packets are ensured against SYN floods[4]. To protect against application abuse (by legitimate or illegitimate users) and its impact on the reliability of the network, Application Switches can place users in a penalty box if they initiate sessions above a predefined limit. Access to the application is restricted for a predefined time and only granted once the session level drops below the limit. These types of post-authentication quarantines are an effective mechanism in a Layered Defense approach to security.

To mitigate risks from Instant Messaging and Peer-to-Peer applications as well as underlying copyright concerns, enterprises can either minimize (rate limit/shape) the use of such applications or deny their use altogether. Nortel Application Switches offer Peer-to-Peer application filtering to provide network administrators complete control for this traffic. Although these applications use dynamic port allocations, the deep packet inspection capability of the switch can identify the traffic content and completely block it, rate limit or shape it. Ultimately, for reliability, resiliency and business continuity, real-time deep packet inspection to mitigate many of today's threats is best done by switch-based architectures such as that used by the Nortel Application Switch.

Virtual Local Area Networks

Virtual Local Area Networking (VLAN) enables for the isolation and separation of network traffic and is supported in many Nortel products, including the Ethernet Switches, Ethernet Routing Switches and Wireless Access Points. For example, the internal architecture of the Ethernet Routing Switch 8600 allows users to build secure port and tag-based VLANs. When port-based VLANs are

[3] Switched Firewall Product Brief, document number NN110161

[4] Application Layer Security whitepaper, document number NN105560

configured, each VLAN is completely separate from the others (broadcast domain). Its unique hardware architecture (distributed ASICs with local decision) analyzes each packet independently of the preceding ones. This approach allows complete traffic isolation. Allowing the user to discard untagged traffic on tagged ports or tagged traffic on untagged ports guarantees that this traffic is completely discarded — even if a tagged port receives traffic with a VLAN tag that identifies a VLAN from another "customer" configured on the box.

Core network security — Keeping watch for malicious activity and enforcing policy

Continually monitoring the network for malicious activity is key to ensuring that if an attack slips through other layers of security (e.g., endpoint, perimeter, deep packet inspection, signature matching, etc.) that your network will detect it and take appropriate action to block the attack and ensure survivability. This is of great concern with internally generated attacks or infections that may have unwittingly been released into the network by an otherwise innocent user. A great example is an Instant Message (IM)-delivered virus. With an early warning system, the network can identify the signs of such a virus once in the core of the network, define an effective mitigation tactic and push out a policy to enforcement points in the network to filter out the unwanted traffic. This protects the network and ensures survivability even during an attack.

A key goal of security in the core is to minimize the disruption of network resources and applications due to an attack (DoS, worms, virus, etc.). As part of the Layered Defense approach to security, the reliability of security solutions an enterprise chooses should be considered to ensure the highest level of uptime. Nortel has long been designing products with the highest reliability for carrier environments, and brings high availability and reliability to the full suite of enterprise products to ensure the survivability of the network even under attack.

The Nortel Threat Protection System (TPS) provides full intrusion detection capabilities including anomaly detection, and when paired with the Nortel Switched Firewall as a policy enforcement point, provides full active threat protection. The Threat Protection System works by placing intrusion sensors throughout the network. By utilizing the data they gather, the TPS then identifies threats and applies a policy to all Nortel Switched Firewalls to mitigate the attack. The TPS can detect known threats via deep packet inspection, can detect unknown threats via anomaly scanning (protection from zero-day attacks) and can eliminate the expense of false alarms with a flexible rule set and administrative structure.

The Nortel Application Switch, through its Intelligent Traffic Management feature, can provide an early warning of attacks in the core network and based on its policy structure enable intrusion protection through sophisticated filtering, rate limiting and shaping.

The Ethernet Routing Switch 8600 supports optional modules that can play a key role in core network security policy enforcement. The Service Delivery Module enables the Ethernet Routing Switch to support up to four Nortel Switched Firewalls. Given the Ethernet Routing Switch 8600's typical placement in the core of the network, it is positioned well to support the Threat Protection System. An optional Web Switching Module provides additional DoS, filtering and application abuse protections.

The Nortel Enterprise Policy Manager plays a role in core network security by providing real-time policy-provisioning capabilities across Nortel's devices (Ethernet Routing Switches, VPN Routers, etc.) on the network to mitigate the swift penetration of a virus or worm that is identified by the Threat Protection System, Application Switch or manually.

The enterprise's need to communicate with its remote employees, business partners and customers should not be hampered by the threats to public networks.

Secure communications — Protecting information in transit

Protecting corporate and government information from unauthorized discovery, eavesdropping or misappropriation while it transits across hostile networks is an important element of the Layered Defense approach to security. Having made secure connectivity available to more than 100 million users worldwide, enterprises have several options within the Nortel portfolio to secure their traffic leaving or arriving their network. Offering multiple methodologies enables Nortel customers to choose the exact solution that meets their organization's security need while minimizing TCO. While VPN is the primary approach to securing communications, VLANs can be used in conjunction with VPNs to enhance security. Coupled with the endpoint protections mentioned earlier, VPN and VLAN-enabled user devices are also checked before being allowed to join any network.

While IPSec provides cryptographic protection at the network layer (OSI Layer 3), Web traffic uses Secure Sockets Layer (SSL) to secure communications at the transport layer (Layer 4) and offers the added benefit of not requiring the support of client software. Nortel is a leader in offering support for both VPN technologies in a single platform. Nortel VPN platforms ensure users do not pay a penalty in scaling, performance or TCO to receive the benefits of unified secure access (SSL and IPSec).

- Nortel VPN Gateway offers unified secure remote access (SSL and IPSec) for a wide range of uses from traditional remote access applications (mail, etc.) to Web-based access, extranets, portals and externalizing intranet Web applications/resources. Native applications normally supported only in an IPSec environment can be seamlessly supported by the VPN Gateway through SSL VPN. Added SSL endpoint protections such as automatic timeout for walkaway situations at kiosks and dynamic access policies to limit application access based on the employee's location provide enhanced use and security.
- Nortel VPN Router is a portfolio of award-winning, market-leading unified access VPN platforms that can address site-to-site environments ranging from small office/home office (SOHO), branch offices to large enterprise and government data centers. In addition, the Nortel VPN Router supports remote access and endpoint protection, and includes an integrated firewall. Using the exclusive Nortel Secure Routing Technology (SRT), VPN Routers enable dynamic routing to be leveraged inside site-to-site tunnels. This minimizes the administration costs/headaches of maintaining static routes and enhances user quality of experience by allowing the best path to be selected for each type of data and destination.
- Nortel Application Switch, with integrated SSL, provides SSL VPN remote access support with additional application security protections, and the benefits of full application delivery and load balancing capabilities (Layer 2-7 support).
- WLAN Security Switches can support wireless security standards such as WPA/WPA2 for security, or they can forward PPTP, SSL and IPSec tunneling to a VPN Gateway for secure communications across wireless LANs. These mechanisms can even be combined to provide the ultimate level of security. And to ensure the mobility benefits of WLAN are not mitigated by the need for secure communications, WLAN Security Switches support seamless secure roaming across IP subnets while maintaining the VPN tunnels. The Nortel WLAN can generate multiple "virtual" WLANs from a single infrastructure to isolate traffic and deliver unique service profiles to different user classes.
- The Services Edge Router 5500 platform provides support for large enterprise or VPN service provider employee or customer secure remote access requirements that can reach up to 50,000 IPSec tunnels.
- SSL acceleration to enhance the performance and capacity of secure communications is provided in the Nortel VPN Gateway, Nortel VPN Router (SSL VPN 1000 Module enabled), as well as SSL-optimized Nortel Application Switches and through an optional SSL acceleration blade on the Nortel Ethernet Routing Switch 8600.

Security management and platform security

A security solution can easily become too costly and not very beneficial if you can't effectively manage it. Effective management requires configuration, policy and event management components. Nortel provides answers to all these management areas.

Incorrectly configured devices can be a key weakness in a network's security posture. The configuration of several devices on large enterprise multi-vendor networks can present many problems and be very costly. Nortel partners with Opsware Inc. to offer complete multi-vendor network configuration control that tracks, regulates and automates all configuration and software changes across multi-vendor network devices. In addition, the solution enables IT governance initiatives, automates delivery and

enforcement of network change control processes, and provides automated management of security and compliance best practices.

The Nortel Enterprise Policy Manager (EPM) provides centralized, policy-based provisioning to reduce management complexity and operational cost as well as network admission control that protects network resources and controls denial of service attacks. The ability of the network to quickly respond to threats before patches are available or virus updates are released is critical. While being able to leverage the user-based policy provisioning of the Enterprise Policy Manager for an individual user or group of users, enterprises can also construct static policies that would apply to the entire enterprise network to push security policies to various devices. This ensures the enterprise has a "quick reaction" capability as they learn of new threats, without relying on individual security policy updates per device. By using protocol type or port to identify the malicious traffic, policies can be pushed either temporarily or permanently to prevent the traffic from hitting supported devices. EPM's strength is in its ability to push filters real-time to numerous devices on the network — very important as enterprises risk the systemic and swiftly-spreading threats posed by today's vulnerabilities.

Security Event Management acts to collect, normalize, correlate and prioritize reports of security policy violations throughout the network and IT infrastructure. Examples of such violations include traffic filter and firewall rule violations, repeated unsuccessful login attempts, anomalous traffic patterns and network intrusion alerts. Gaining a network-wide view of security events provides the basis for security operations, audit compliance, incident detection, investigation and response. Security Event Management also provides a further layer of defense to provide early warning of potential misconfiguration of security enforcement devices within the network. Nortel's partner, GuardedNet, complements our security solutions with a comprehensive, centralized security event management and incident response system.

A key aspect of the Layered Defense approach is to leverage the security that is part of the products themselves. We refer to this as platform security. Nortel products are designed with security capabilities embedded into every product, solution and network blueprint. Secure development also involves our supply management group and the evaluation of the security capabilities of our third-party suppliers. Nortel works to hold our suppliers to high levels of security "maturity" through our supply management engagement process. Nortel's Vulnerability Assessment and Management Program (VAMP) leverages industry-leading vulnerability scanning tools to ensure that Nortel products are tested against known vulnerabilities before being shipped to customers.

Nortel also follows a number of procedures designed to ensure that our products are delivered securely, to the intended customer, with tamper resistance, deployed only on the platforms to which they were intended. This means that security is not only in Nortel's security products and those that enable security or partnering with best-of-breed security partners for a Layered Defense approach to security, but also building security into the products that implement IP Telephony, multimedia, WLANs, switching, network management and many others. Examples of this platform security in Nortel products include:

- Hardened operating systems loaded with only the necessary capabilities required to support full security functionality. By disabling unnecessary capabilities and services from an operating system, devices are less likely to be compromised through system weaknesses and unsupported features. As well, vulnerability assessments can be assured of testing the full suite of OS features.
- Highly reliable architectures minimize the disruption of device resources and applications due to component failure or attack on the device (DoS, worms, virus, etc.). Leveraging Nortel's heritage of providing resilient, 5 9's reliability, Nortel brings high availability and reliability to the full suite of enterprise products, including call servers, Layer 2-7 switching, VPNs, firewalls and server applications. Capabilities such as a device management shield against DoS or malformed packet attacks help ensure business continuity.
- Security of management traffic is a key requirement to ensure enterprise products are not compromised. Nortel devices support secure management capabilities such as secure shell (SSH), SNMPv3 and SSL.

A key component of ensuring platform security starts with the design process, but continues through the product lifecycle. Nortel is committed to continuing to monitor the security of devices once in the customer's network, communicating with customers about industry vulnerabilities and effective steps to take to maintain the overall security of the product in the customer's network. Beyond ensuring the products themselves are secure, products must also be securely deployed — moving from an issue of technology to that of human behavior and impact. Nortel works with our customers to help ensure that

products are deployed in a secure fashion, providing best practices against misconfigurations — for example, to ensure against network vulnerability.

To further help customers ensure secure deployment, Nortel's Global Services offer a full suite of security services such as Network Security Design and Planning, Security Audit and Assessments, Security Integration Planning as well as Compliancy and Regulatory Audits. In addition, Nortel can project manage and implement a security solution, provide ongoing technical support and software updates, and even provide security optimization, upgrade and migration support.

To ensure that our customers maintain an acceptable level of network security once our products are deployed, Nortel's Security Advisory Task Force works with industry organizations such as CERT to ensure quick reaction to new industry vulnerabilities that may impact Nortel products. This team works closely with Nortel product teams to evaluate the potential impact to Nortel products and, where warranted, to issue and communicate any patches necessary to customers as quickly as possible so customers know to respond to vulnerabilities. Sign up for Nortel security advisories at: *http://www.nortel.com/solutions/securenet/index.html*.

Today's businesses and governments are enjoying the many benefits of greater communications with fewer boundaries between them and their business partners, customers and remote employees.

Nortel on Nortel

Nortel's own network — one of the largest and most technically advanced enterprise networks in the world, connecting more than 280 locations across six continents — runs on products from Nortel's own portfolio. That's about 33 million minutes of voice calls, 1.1 petabytes of data traffic (including 19 million e-mails), and 100 live Web casts in a typical month — all on Nortel products. Leveraging the latest security available in Nortel's portfolio, Nortel's IS can use the Internet as a transport to reduce the costs and complexities associated with multiple network topologies and access methods while still protecting these critical network resources.

Currently, as an example of a Layered Defense approach, among its many solutions, Nortel's IS uses the Switched Firewall for its deep packet inspection, having prevented over 133 worms in the first month in the network, and with minimal latency, to protect our network IP Telephony and multimedia applications. Nortel Application Switches are used to provide redundancy to Session Initiation Protocol (SIP) servers to ensure high availability of our SIP applications and bandwidth management of Peer-to-Peer network applications. The Application Switches provide global multi-site and local redundancy of key servers, flexible packet inspection with packet offset, and pattern matching for UDP, ICMP, IP and TCP traffic, and to auto-learn and auto-update the latest attack signatures. Nortel Threat Protection System provides an early warning attack capability while VPN Gateways and VPN Routers are used to provide mobile employees with simple-to-use secure communications. Using best-of-breed security technologies available through Nortel's vendor partnerships, and security best practices including a strongly enforced and well-understood security policy, Nortel's IS enjoys a true end-to-end Layered Defense approach to security.

Summary

The organization's need to share information between employees, business partners and customers should not be hampered by threats to public networks or internally originated attacks. A Layered Defense is key to ensuring that an organization removes all single points of security failure and is able to fully leverage the benefits realized from state-of-the-art applications and networks. By building multiple approaches to security enforcement into all areas within a network, organizations are deploying a security infrastructure that is highly resilient against attacks while also providing the privacy capabilities needed to remain compliant with so many of today's new regulations.

Nortel has been building secure, reliable communications systems for over 100 years and has made secure connectivity available to more than 100 million users worldwide. Nortel's solutions are used by many of the world's largest stock exchanges, are embedded in the U.S. Dept. of Defense communications network, and are used by more than 80 percent of the top 100 U.S. banks. By taking a Layered Defense approach to network security, organizations can be well-positioned to defend their networks against today's threats and evolve to protect against tomorrow's threats while minimizing down time and maximizing productivity.

For more information on Nortel security solutions, please visit us on the Web at www.nortel.com/enterprisesecurity.

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

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

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.

NN108120-082707

NORTEL

BUSINESS MADE SIMPLE