›THIS IS **THE WAY**

NORTEL STOPS VIRUSES AND WORMS AT THE SOURCE

›THIS IS NORTEL™

Solution Brief

Nortel Secure Network Access

Reducing risk through endpoint security

Failing to secure the endpoint computing devices in your network costs the corporate enterprise in excess of $50 million[1] per year. During the first six months of 2004, 4,496[2] new viruses and worms were discovered, causing millions of damage to systems and lost productivity costs for the enterprise.

Organizations are continually bombarded with new viruses, worms and vulnerabilities in the technologies employed in business systems. The malicious software trend is expected to get worse, not better, over the foreseeable future. Failing to keep systems patched and current vulnerabilities managed increases the opportunities for successful attacks. Despite the plethora of patch management solutions, research suggests many organizations are still not current with vendor recommended patches. The sheer volume of devices to manage exacerbates the problem, including asset management and deciding which devices are corporate assets, which belong to non-employees such as contractors and ensuring all devices comply with the enterprise's security standards.

These factors increase the risk exposure footprint for the enterprise. Consequently, organizations must utilize a layered defense approach to network security to combat these increasing threats. A layered defense posture provides more than one layer of protection from any given attack method, thereby increasing the enterprise's control and mitigation capabilities. The mitigation and control of these issues is within our grasp and applicable to every enterprise, regardless of business focus or size.

Solutions

A key element described in the Nortel Layered Defense[1] posture is endpoint security, starting with the computing devices used by the user community. Spending time securing these devices is integral to the defensive posture as most enterprises have far more users than servers. Critical to managing these systems are security policies specifying the precise configurations required by the enterprise for holistic management and control. Security policies require specific components including anti-virus software, up-to-date definitions, personal firewall software and the unique configurations for the enterprise such as disallowing certain network applications on the device.

Controlling what devices are permitted to connect to the network provides significant protection. Does an enterprise really know what is connected to their network? Enterprise-provided systems, employees' personal devices, contractors, consultants and vendor

[1] Read about the Nortel Layered Defense in the paper entitled Layered Defense approach to network security, document number NN108120.

[2] Symantec Internet Security Threat Report, Sept. 2004

support personnel all have devices which may be connected at any given time. Solutions like port authentication as provided by IEEE standard 802.1x provide the ability for the enterprise to allow only authorized systems network connectivity. Limiting network access to only authorized systems is essential; however, even authorized systems can become infected with a virus.

Automated enforcement of configuration and security policies complete the defensive posture. Using solutions to evaluate the configuration of the authorized system increases control and risk mitigation level. If the system meets the criteria established in the security policy, it is authorized and connected to the network. Any system failing to meet the policy can be directed to the appropriate systems where patches, required software and configurations can be made.

Adding these components to your layered defense posture increases your control, reduces the risk of unauthorized or authorized but uncompliant systems from connecting to your network, infecting other systems or stealing your organization's information assets.

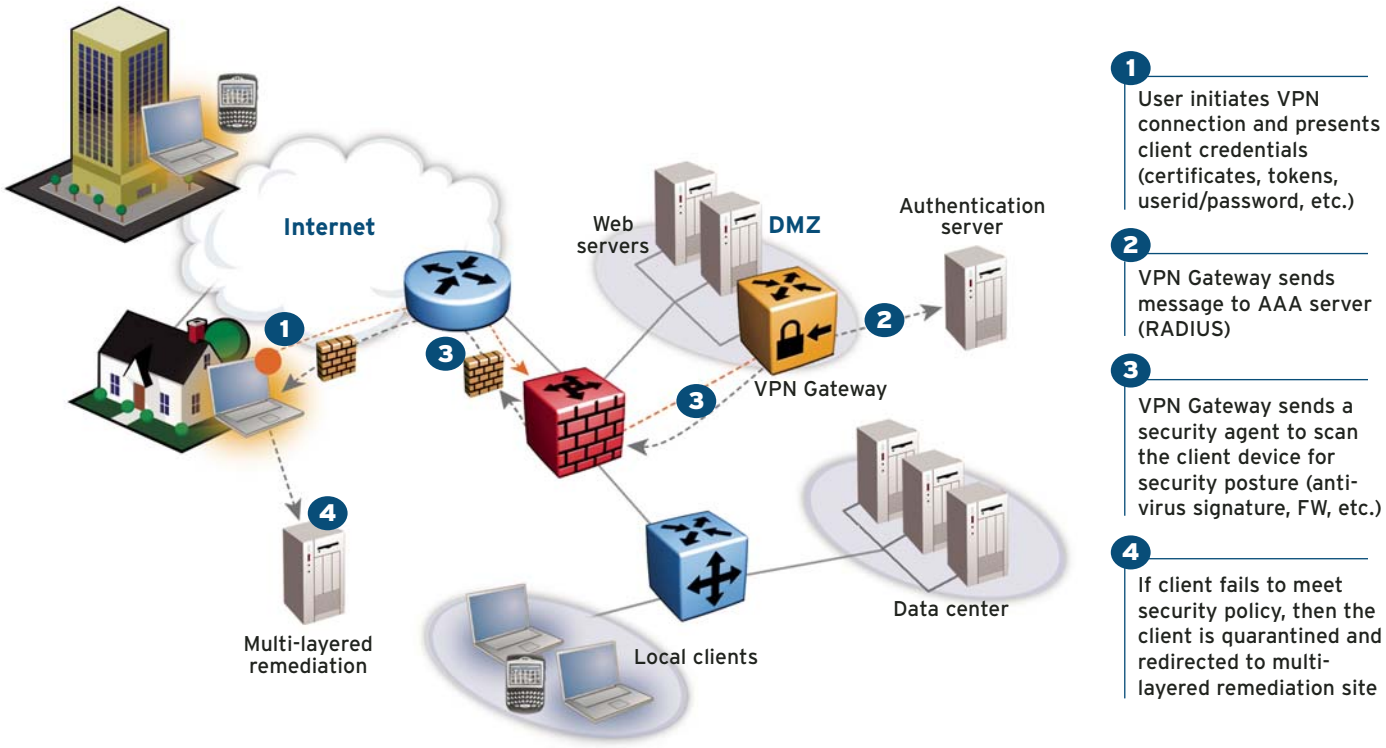
Nortel's answer

Nortel understands security means understanding networks. We are the leading vendor with strategies for traditional and emerging voice technologies. Nortel's comprehensive security strategy results in high-performance security products built on a culture of reliability and best-of-breed partnerships. Nortel's standards-based solutions provide lower integration challenges and increased interoperability with other network equipment.

Nortel understands the need for cohesive management of endpoint configuration and provides solutions addressing these industry concerns. To that end, Nortel offers the Secure Network Access Solution (NSNA). Providing information gathering and response capability into the network is essential. Being able to determine the configuration of the endpoint and allowing or denying access can decrease your exposure to malicious activity.

Nortel Ethernet and Ethernet Routing Switches (formerly known as BayStack* and Passport*) are IEEE 802.1x enabled, providing the capability to enforce 802.1x authentication on devices supporting it. Other methods are available for restricting access to authorized systems, including MAC address filtering. These services prevent unauthorized devices from connecting to the network, which can limit exposure to viruses, worms, malicious attacks, sniffers and rogue wireless access points. IT administrators can't always keep their remote users free of viruses, but they can keep them from infecting the network. With NSNA, featuring our Tunnel Guard technology, enterprises can reap the economic benefits of virtual private networking with much lower levels of security exposure. Nortel was the first VPN provider offering this technology for remote users. Nortel Secure Network Access supports both IPSec and SSL VPN using a client for IPSec and clientless

Figure 1. Nortel Secure Network Access — VPN endpoint protection



The IEEE 802.1x protocol is the standard providing access control services for both wired and wireless LANs. The protocol defines a method of authenticating and authorizing a device to connect to a given LAN based upon the Extensible Authentication Protocol (EAP). When a device connects to an 802.1x-protected network, the network requests the device authenticate and if successful connects the device to the network. Port level authentication blocks unauthorized computers from connecting to the network, prevents access from non-secured areas and is useful for preventing network-level attacks against critical network resources.

operation for SSL VPNs. Nortel Secure Network Access enables the administrator to define endpoint security policy on the VPN Gateway itself and ensures all users or devices connecting to the VPN Gateway are inspected for compliance to the policy. Users can be denied access or have access restricted based on compliance status.

Through Nortel's established relationships with leading security vendors like Sygate Technologies, our 802.1x-enabled switch products provide full control over the configuration requirements for every authorized system. The Sygate Secure Enterprise solution provides a personal firewall and agent-based technologies to ensure the system is compliant with the organization's security requirements. All elements of the system can be evaluated including the operating system, patches, anti-virus software, personal firewall status, registry settings and other system configuration components. Verifying compliance and blocking connections from non-compliant systems can guarantee 100 percent compliance with corporate policy 100 percent of the time.

The network edge is no longer where the corporate firewalls are. A paradigm shift over the last few years has pushed the network edge to where the user and their computing device are located. The road warrior establishing a connection to the corporate network from their hotel, the support engineer providing support to a customer or the sales representative demonstrating your latest product can have secure remote access to your network. Likewise, organizations are extending their firewall installations to include locations within the corporate network to increase protection for critical computing resources such as data centers and mission-critical applications. The versatile Nortel Ethernet Routing Switch platform provides high-speed switching and routing services over a wide range of network interfaces. Adding the Service Delivery Module to the Ethernet Routing Switch extends enterprise firewall protection to the data center, enabling a higher level of protection for the mission-critical systems and information.

Nortel provides secure access to your network using IPSec and SSL VPN technologies with the Nortel VPN Gateway and Nortel Application Switch (formerly known as Alteon* Application Switch) portfolios. Nortel has the product flexibility providing both IPSec and SSL VPN solutions to meet your connectivity needs. Regardless of where your employees are, Nortel VPN Router (formerly known as Contivity*) and VPN Gateway provide full, secured access to the resources and services they need including mobility services such as Voice over IP. Available on Nortel's VPN Gateway portfolio and Nortel VPN Router platforms, Nortel Secure Network Access helps to prevent the end-user PC from becoming a vehicle for viruses or other unwanted intrusions into the secure enterprise network through the VPN tunnel. When combined with Sygate Secure Enterprise, every system in your organization can be compliant with your security policy regardless of where they are and how they connect.

Nortel provides your next-generation network, capable of withstanding today's malicious software attacks. Nortel's solutions provide your network with the ability to deal with tomorrow's attacks by anticipating attacks before they occur. Full connectivity strategies, service delivery and network control provide your organization the capability of providing whatever level of access you need.

For Nortel, success is delivering technologies providing secure access to your information using security-compliant systems regardless of where you are and how you access the network. Your success is measured by increased employee productivity and lower network operations costs. Nortel's award-winning solutions provide your organization with the network intelligence required for success. That makes good business.

This is the way we reduce the impact of viruses, worms and other malicious software.

This is Nortel.

Viruses and worms are a major threat in today's computing landscape. Computer viruses were first seen more than 20 years ago and we can expect them and future variants to continue. Enterprise security managers understand the need for integrated and cohesive solutions — point products no longer meet the need. Instead, they look for interoperability between their network equipment and security software systems. Nortel allows the security and networking teams to leverage their existing environment in combination with our significant security portfolio.

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
Phone: 00800 8008 9009 or
+44 (0) 870-907-9009

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 enterprise and service provider 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**.

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

NN110300-062905

NORTEL