Your Location: Home / News & Events / News Releases

Events

Media Resources

Related Information:

Corporate Information

Enterprise Solutions

Top News

# News Release

December 7, 2004

## Enhanced Enterprise Security Solutions Deliver Nortel Vision of Trusted Communications

*New Products, Partners Provide Secure Access Anywhere, Anytime on Any Device*

SANTA CLARA, Calif. – Nortel* [NYSE/TSX: NT] has enhanced its portfolio of security solutions by introducing new remote access security solutions and threat protection capabilities designed to improve access security for remote workers and to instantly detect and shut down threats from anywhere within a customer's network.

These solutions are part of Nortel's continuing drive to deliver on its vision to secure and protect the world's most critical information by providing reliable and secure trusted communications capabilities for voice, data, multimedia and video across multiple devices.

Customers around the globe are already realizing the benefits of Nortel's approach to reliable and secure, trusted communications. These include BT Retail in the UK; National Air Traffic Services, the UK's leading air traffic services company; Coca Cola Icecek of Turkey; Spanish financial institution Caixa Catalunya; and in the United States, Coppin State University, Baltimore, Md.; ProMedica Health System, Toledo, Ohio; and St. Luke's Hospital & Health Network in Pennsylvania.

Nortel has also introduced a Developer Program for Security targeted at simplifying customer deployments by bringing together industry-leading security vendors with solutions tailored to provide comprehensive network security on a Nortel-based infrastructure. The program will support customers with cooperation from security companies such as Sygate Technologies, Inc.

and Concord Communications Inc. and complements existing security relationships with Check Point Software Ltd., Sourcefire and Symantec. Nortel also announced today an alliance with Symantec focused on providing next-generation network security capabilities to enterprises and service providers.

"Enterprises require network solutions to protect their infrastructure not only from end-users that may inadvertently compromise security from remote-access based threats but also from threats carried in the network that require immediate isolation and containment," said Zeus Kerravala, vice president, enterprise infrastructure, The Yankee Group.

"By addressing both aspects in tandem, companies can avail themselves of the most comprehensive measures to protect the entire infrastructure, whether in a hosted, managed model from service providers or whether they deploy their own networks," Kerravala said. "Without addressing threats from internal and external sources, regardless of whether those threats are malicious or accidental, enterprises risk adopting a security posture based on false assumptions that effectively lock the front door while leaving the back door wide open."

"Nortel recognizes that the network is constantly evolving, and maintaining a strong defense is complex and often costly," said Malcolm Collins, president, Enterprise Networks, Nortel. "Our enhanced security portfolio is a key component of our Virtual Enterprise vision, where any worker can access networks remotely as safely and securely as if they were sitting at their desks in an office."

"Achieving that vision requires deploying a layered defense consisting of secure remote access, network perimeter security, and end-point security to protect enterprises from security threats," Collins said. "To this end, Nortel is working closely with its channel partners and other leading vendors in the security market to build a coalition that ensures we are offering our customers the best security solution that meets all of their needs for reliable and secure trusted communications."

Secure and Flexible Universal Remote Access is at the heart of the enhancement of Nortel's VPN (Virtual Private Network) Gateway 3070, a new high-end SSL and IPSec VPN platform designed for large enterprise and managed VPN service provider deployments. In addition, Nortel is integrating IPSec VPN functionality into the VPN Gateway 3050 platform.

Coca-Cola Icecek (CCI), the authorised bottling partner of the Coca-Cola Company in Turkey, has successfully deployed Nortel VPN Router (formerly known as Contivity* Secure IP Services Gateway) to provide the routing, VPN, firewall, bandwidth management, encryption, authentication and data integrity for secure connectivity for CCI's 90 dealers across Turkey.

“The Nortel VPN Router connects CCI offices, dealers and mobile users over the Internet with the same security and control found in private networks,” said İhsan Ercan, group manager, CCI Business Systems Group. “The Nortel VPN Router offers our remote users the ability to transfer the working environment of their offices to the location where they are working, allowing them to rapidly access all their related data and applications over a secure network and giving them access to key sales information, resulting in higher employee productivity and increased employee satisfaction.”

"The flexibility of having both IPsec and SSL VPN capabilities on a common platform is not only convenient, but it is an absolute requirement to support our mixed user population, various locations and wide range of application access requirements,” said Matthew M. Woodruff, system engineer, St. Luke’s Hospital & Health Network. “Our doctors and healthcare staff are able to get secure remote access to critical patient information regardless of how or where they access the hospital network. This ability to rapidly share knowledge, securely, in real-time helps St. Luke's improve patient care, meet regulatory security requirements, and lower the cost and complexity of providing remote access. The result is our ability to offer world-class healthcare without compromise."

Enhanced Proactive Network Infrastructure Security is the key capability of the new Nortel Threat Protection System. The Nortel Threat Protection System combines world-class capabilities for detecting threats to the network and quickly adapts to eliminate them, allowing customers to shut down suspicious activity from anywhere within their network. In addition, working with CheckPoint, the Nortel Ethernet Routing Switch 8600 (formerly known as the Passport* 8600) now includes a Service Delivery Module for distributing resilient firewall capabilities as needed throughout the network.

"Security is of critical importance to Coppin State,” said Ahmed El-Haggan, vice president of information technology, chief information officer and professor of computer science at Coppin State University. “Computer virus and worm problems can cause unnecessary expense and disruption.”

“With the Nortel Threat Protection System, we have easily detected known and zero-day threats to avoid the associated problems they cause,” El-Haggan said. “In addition, we have an extra layer of protection that helps us to detect and block attacks before our students, faculty, or staff are impacted. Nortel’s layered defense strategy has helped us build a trusted network at Coppin.”

The solution is augmented with Nortel Application Switch (formerly known as Alteon* Application Switch) Intelligent Traffic Management (ITM), which continuously monitors network traffic for known threat signatures. Should such signatures, like those for worms or viruses, be matched, the application switch can immediately isolate that traffic and remove it from the network. Through a partnership with Concord Communications, the ITM solution also includes enhanced statistics gathering and reporting capabilities made possible via Concord Communications' eHealth Lite.

"It's vital that our healthcare practitioners and administrative staff have access to Internet resources that enhance hospital operations and patient care, but we needed to be sure those legitimate uses were not crowded out by recreational uses or security attacks," said Bruce Meyer, senior network engineer, ProMedica Health System. "Intelligent Application Traffic Management on our Nortel Application Switches gives us the visibility and control we need to manage Internet traffic for optimum user experience and bandwidth efficiency,"

Enhanced Endpoint Security is made possible with improved Nortel VPN Tunnel Guard for SSL VPNs. Nortel has continued its leadership position as first to deliver VPN remote access security policy enforcement by extending support to SSL VPN remote access as well as IPSec VPNs. VPN Tunnel Guard provides a comprehensive security solution capable of enforcing security policies on all VPN endpoints, allowing administrators to define endpoint security policies on Nortel VPN gateways and ensure all users or devices connecting to the VPN gateway are inspected for compliance.

Users can be denied access or have access restricted based on their security status, thus preventing the end-user PC from becoming a vehicle for viruses or other unwanted intrusions into the secure enterprise network through the VPN tunnel. Tunnel Guard allows end-users to receive automatic updates to ensure that every device connecting to the network is compliant with current security policies, including antivirus, patch and other subscription-styled update releases.

In addition, the Nortel Ethernet Routing Switch 8300 (formerly known as Passport 8300) offers an enhanced authentication capability enabled with Extensible Authentication Protocol, which allows multiple means of end-user authentication, including passwords, token-based challenge and response as well as Public Key Infrastructure certificate exchange.

The Security Expert Advantage Program, a North American initiative, is part of Nortel's award-winning Partner Advantage enterprise channel program that trains and accredits reseller partners in Nortel's security solutions. For participants, accreditation under the program establishes competitive advantage from a price, competency, awareness, and support perspective.

"Nortel provides the specialized security training and support necessary to ensure customers receive the most effective security implementations," said

Bart Graf, principal, Integration Partners Incorporated. “Customers that want a real security solution know that they can trust us to implement and support it.”

The EMEA Nortel Partner Program helps channel partners in Europe, the Middle East and Africa to adapt to the changing marketplace by building brand equity, and by positioning them to deliver end-to-end converged networking solutions and services. Nortel has introduced enhanced designations within the Program for those partners excelling in technical capability and promoting early adoption of technology – Innovator, Global Customer Leader and Convergence Leader. As a Security Innovator Partner, resellers offer high quality security solutions during the early phases of Nortel new product rollout to help promote the early adoption of new technology into the marketplace. Recently, Applinet was appointed Security Innovator Partner in the UK.

"UK organisations understand that, as the converged network becomes more and more central to their operations, ensuring network security is of increasing importance," said Darren Boyce, managing director, Applinet. "We are delighted to become a lead partner for Nortel in this area. Our close interworking with Nortel Technical Support and New Product Introduction teams through internship, combined with the other elements of the Innovator initiative and Nortel’s strong security portfolio, will allow us to bring a uniquely powerful security offering to the UK market."

The Developer Program for Security enables Nortel customers to leverage leading security vendors when implementing a secure network solution. Drawing from industry standards-compliant products that are interoperable with Nortel solutions, customers are backed up by working relationships with all of the participants, resulting in a total security solution.

Nortel helps enterprises control critical business processes by building standards-compliant, open security solutions that integrate into today's IT environment and adapt to tomorrow's security threats. Designed to protect multimedia communications and ensure user quality of experience, Nortel solutions actively respond to even unforeseen security threats by building resiliency and adaptability into every solution and network plan. The Nortel "security in the DNA" design philosophy protects the network at every touch point by building security measures into every new product, solution and network blueprint.

With today’s announcement, Nortel is introducing the first in a line of strategic security proof points that will follow in 2005. Nortel’s solutions deliver capabilities to secure computing, network, applications and end-user environments while maintaining unmatched reliability. Nortel helps governments, businesses and individuals stay ahead of threats, including hacker intrusion, worms and denial of service attacks, by protecting personal information and by delivering enhanced network management capabilities.

Nortel has made secure connectivity available to more than 100 million users worldwide.

## About Nortel

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. For the latest Nortel news, visit www.nortel.com/news.

*Certain information included in this press release is forward-looking and is subject to important risks and uncertainties. The results or events predicted in these statements may differ materially from actual results or events. Factors which could cause results or events to differ from current expectations include, among other things: the outcome of Nortel’s independent review and planned restatement or revisions of its previously announced or filed financial results; the resolution of the accounting issues announced on November 11, 2004, including the outcome of discussions with the United States Securities and Exchange Commission (SEC); the impact of the management changes announced on April 28, 2004 and August 19, 2004; the impact of the inability to meet Nortel’s filing obligations on support facilities and public debt obligations; any potential delisting or suspension of the Company’s or NNL’s securities; the adverse resolution of litigation, investigations, intellectual property disputes and similar matters; the sufficiency of Nortel’s restructuring activities, including the work plan announced on August 19, 2004 as updated on September 30, 2004, including the potential for higher actual costs to be incurred in connection with restructuring actions compared to the estimated costs of such actions; cautious or reduced spending by Nortel’s customers; fluctuations in Nortel’s operating results and general industry, economic and market conditions and growth rates; the communication by Nortel’s auditors of the existence of material weaknesses in internal controls; Nortel’s ability to recruit and retain qualified employees; fluctuations in Nortel’s cash flow, level of outstanding debt and current debt ratings; the use of cash collateral to support Nortel’s normal course business activities; the dependence on Nortel’s subsidiaries for funding; the impact of Nortel’s defined benefit plans and deferred tax assets on results of operations and Nortel’s cash flows; Nortel’s dependence on new product development and its ability to predict market demand for particular products; Nortel’s ability to integrate the operations and technologies of acquired businesses in an effective manner; the impact of rapid technological and market change; the impact of price and product competition; barriers to international growth and global economic conditions, particularly in emerging markets and including interest rate and currency exchange rate fluctuations; the impact of rationalization in the telecommunications industry; changes in regulation of the Internet; the impact of the credit risks of Nortel’s customers and the impact of customer financing and commitments; stock market volatility generally and as a result of acceleration of the settlement date or early settlement of Nortel’s purchase contracts; the impact of Nortel’s supply and outsourcing contracts that contain delivery and installation provisions, which, if not met, could result in the payment of substantial penalties or liquidated damages; and the future success of Nortel’s strategic alliances. For additional information with respect to certain of these and other factors, see the most recent Form 10-Q/A and Form 10-K/A filed by Nortel with the SEC. Unless otherwise required by applicable securities laws, Nortel disclaims any intention or obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.*

*Nortel, the Nortel logo, the Globemark, Contivity, Passport and Alteon are trademarks of Nortel Networks.

Use of the terms “partner” and “partnership” does not imply a legal partnership relationship between Nortel and any other party.

Contact for Press and Analysts:

Pat Cooper
Nortel
(425) 450-7523
pat.cooper@nortel.com

Giorgia Casnedi
Nortel
+44 1628 43 3117
casnedi@nortel.com

Additional Media & Analyst Contacts