



Product Bulletin

Convergence 101 Tutorial Series: Network Security

What is network security?

Network security is simply the process of ensuring the integrity of the network and protecting the voice, data and multimedia traffic that traverses it from malicious attacks and threats. As enterprises have expanded their use of the Internet Protocol (IP), the need for security has grown in lockstep. This is because the Internet was designed to share, not to protect. External attack from hackers internal and external to enterprises, application abuse, viruses, unauthorized access and interception of data en route are some of the potential threats. Network security helps ensure network integrity and data confidentiality and protect against these threats.

Why is security important to convergence?

Converged networks bring with them the advantages — and disadvantages — of always-on, connectionless networks. These benefits include potentially dangerous security problems associated with IP. Network security products and technologies protect against a variety of threats to the voice/data network:

- **Integrity**

- Unauthorized use of network bandwidth (e.g., peer-to-peer traffic)
- Electronic commerce fraud
- Toll fraud

- **Availability**

- Denial of Service (DoS) attacks, worms and viruses
- Disrupting critical application and voice call servers
- Hackers intercepting and terminating critical network resources

- **Confidentiality**

- VoIP Signaling attacks (e.g., caller ID theft and eavesdropping)
- Theft of subscriber information (e.g., credit card numbers, collection of personal information, etc.)
- Spyware and malware compromising integrity of the host (e.g., PCs, VoIP phones, etc.)

Key terms/elements

NAC — Network Access Control. NAC provides endpoint security by authenticating users and scanning connecting devices for approved applications before granting access to enterprise network resources.

IDS/IPS — Intrusion Detection System/Intrusion Prevention System. IDS/IPS monitors network activities for malicious or unwanted behavior and can react in real-time to block or prevent those activities.

VPN — Virtual Private Network. A VPN uses the public network to securely transfer information between remote locations. It maintains privacy across the public network through encryption and tunneling.

Encryption/decryption — A mathematical process of scrambling information before it enters a nonsecure area (such as the Internet) and descrambling it as it reaches a secure area (such as the corporate network) to ensure that even if someone intercepts the encrypted information, they would not be able to decipher it without the appropriate key.

IPsec — A standards-based framework providing secure transmission of information over unprotected IP networks,

such as the Internet. IPsec operates at the network layer, protecting and authenticating IP packets between participating devices, such as routers and gateways.

3DES — Data Encryption Standard is used for securing voice and data streams in IPsec VPNs. Devices supporting DES encrypt and decrypt data using a single key. 3DES applies three stages of encryption, using separate keys for each stage.

Firewall — A firewall is a network security device that protects a private network from unauthorized access — much like a security guard controlling access to a building by examining the credentials of individuals attempting to enter. A firewall makes these decisions based on the corporate security policies the firewall has been configured to enforce. Firewalls can also be deployed internally to filter traffic going to/coming from one or more segments of a corporate network and to deny/restrict access to unauthorized users.

DMZ — An acronym for “demilitarized zone”. In computer networks, a DMZ is a group of servers deployed between a company’s private network and the public network. The DMZ is directly accessible to the public network, but does not allow unauthorized access to the internal network resources, such as a server containing company data.

DoS/DDoS — A denial of service (DoS) attack or distributed DoS (DDoS) attack is an incident in which a user or organization is deprived of a resource they would normally expect to have because a hacker has overwhelmed the network with false requests.

SSL (Secure Sockets Layer) — A commonly used protocol designed to secure Web-based traffic traversing the Internet. Networking vendors have extended the use of SSL beyond eCommerce to include Web portals and clientless VPNs. To date, SSL applications have focused on data traffic, but Nortel will offer support for IP Telephony applications in the near future.

Portfolio components

Nortel VPN Routers

VPN Router provides dynamic routing and encryption of signaling and bearer traffic between branches and remote network users, using IPsec tunnels to guarantee the confidentiality and integrity of the payload. VPN Routers include a stateful inspection firewall to ensure perimeter security, provide support for voice signaling protocols, and can be used in IP Telephony multi-site and remote access deployments.

Nortel VPN Gateways

The VPN Gateway is a remote access security solution that extends the reach of enterprise applications and resources to remote users through browser-based VPN tunnels. By using SSL VPN capabilities, customers can simplify network administration by building a “secure remote management portal” that provides instant remote access to any management application from any available browser.

Nortel Secure Routers

Secure routers combine robust IP routing, flexible WAN connectivity and security in a single cost-effective device. Nortel Secure Routers are optimized to deliver the low-latency, high packet throughput required by IP telephony and multimedia applications, and

provide wire-speed performance even with advanced WAN services enabled.

Nortel Switched Firewall

The Switched Firewall provides multi-gigabit and low latency throughput perimeter security. Deep-packet inspection and application intelligence capabilities are provided by our partnership with Check Point, utilizing their industry-leading Firewall-1 technology. The firewall also protects VoIP environments that utilize Nortel Multimedia Communications (MCS) products to help prevent data attacks from affecting latency and jitter-sensitive voice traffic traversing the network. In addition, the Firewall provides the necessary support for H.323 and SIP voice signaling protocols.

Nortel Ethernet Routing Switch

The Nortel Ethernet Routing Switch 8600 is a core Ethernet switch found in the data center and multimedia zone where critical application, voice and multimedia servers are connected. The Service Delivery Module provides Layer 2-7 security by leveraging the same technology found in the Switched Firewall and Threat Protection System. With policies (based on port number, address, content, etc.), VoIP traffic can be directed to the firewall and then forwarded to VoIP call servers.

Nortel Application Switch

The Nortel Application Switch is a server load balancing switch. It provides Denial of Service (DoS) attack protection, bandwidth management and application rate-limiting using Intelligent Traffic Management (ITM). ITM can detect, rate limit, deny or shape all application traffic including peer-to-peer applications as well as network-based worms and viruses. Through our partnership

with Symantec, Intelligent Network Protection (INP) provides signature-based blocking for the top 100 viruses.

Nortel WLAN Security Switch

The WLAN Security Switch provides comprehensive security enforcement for wireless users in addition to unique security functions necessary to secure wireless environments. The WSS supports standards-based wireless security protocols including WEP/WPA/WPA2 and can integrate with existing AAA backend servers and/or Nortel's Secure Network Access switch. The WSS features a secure web portal and can enforce expiration times and location restrictions on an individual basis. The WSS can also integrate with AirDefense WIDPS systems for installations requiring the strongest security available.

Competitive advantages

Security acceleration — Our acceleration technologies enable performance and scalability, from ensuring end-to-end SSL encryption between client and server, to improving the performance of firewall security by offloading up to 90 percent of session processing to a switch-based accelerator.

Security in the DNA — We build our products from the ground up to be secure and take into account that we will be running real-time applications.

Layered Defense — Our Layered Defense Architecture ensures that there are no single points of security failure in the network. By building security into every new product and solution, we provide comprehensive security to protect networks from threats at the Endpoint, Secure Communications, Perimeter and Core Network Layers.

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.

Nortel, the Nortel logo, Nortel Business Made Simple and the Globemark are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2007 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. NN109243-100907

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
Phone: 00 800 8008 9009

In Asia:

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



BUSINESS MADE SIMPLE