NORTEL

Solution Brief

Nortel Business Communications Manager Security

The Nortel Business Communications Manager is a full-featured convergence system that provides a rich array of data services that meet the requirements for small- to medium-sized sites. Local and wide area networking, Internet access, IP telephony... these data services and more can be securely delivered without adding external equipment.

Convergence. Converging voice and data services in one platform offers several important advantages, such as lower network cost of ownership, tight integration between voice and data networking features, and greater reliability and ease of management, compared to solutions that rely on multiple components.

Security. Extensive, multi-layered security enables Business Communications Manager platforms to withstand network attacks from the Internet or from within the organization, such as computer worms, viruses, online fraud and other cyber-attacks. Security provisions reflecting the desired security policy enforcement protect applications and multimedia communications — starting with full security management and extending all the way to end-user devices and desktops for total end-to-end integrity.

Designed to be secure in both public and private networks, Business Communications Manager leads competitors by offering such enhanced features as:

- Support for extensive security policies
- Encryption of all operations, administration and maintenance communications
- Comprehensive security audit trail, including tracking of configuration changes
- Acceptance only of digitally signed software updates

In a hostile world, Business Communications Manager establishes a protected business environment, even as your "internal" network extends far outside the building or campus to reach mobile and remote users, business partners and customers.

Full-featured IP router — built right in

Nortel Business Communications Manager 200 and 400 platforms come with a built-in IP router that supports industry-standard routing protocols and a broad range of data services. The smaller Business Communications Manager 50 platform offers the integrated broadband router as an option — either Ethernet or ADSL — for Internet access or branch networking.

Nortel is an industry leader in security expertise and best-in class product solutions.

Robust, reliable and secure data services — all in one box

Here's a sampling of the data services and capabilities you can get from your Business Communications Manager system:

Create secure networks over the public Internet. Virtual private networks (VPNs) enable you to enjoy secure connectivity with branch offices, business partners and remote users far beyond the reach of private networks. VPNs carry the private data traffic on a logical connection — a secure, encrypted "tunnel" over a public network.

Protect the confidentiality of data in transit. Business Communications Manager platforms use industry-standard IPSec protocols to protect Internet communications through encryption, authentication, confidentiality, data integrity, anti-replay protection and protection against traffic flow analysis. Communications to and from the Web can also be protected by the widely used Secure Sockets Layer (SSL) protocol, which provides data encryption, server authentication, message integrity and optional client authentication. Management communications are encrypted with Secure Shell (SSH), SSL and HTTPs protocols.

Extend secure access to mobile users and telecommuters. Remote users simply install IPSec client software on their laptops, or use a small IPSec device such as a Nortel Business Secure Router 222 — and they can then securely connect to the Business Communications Manager network and access its voice and data resources. Users can work from anywhere, while satisfying even stringent government security requirements.

Prevent hackers and viruses from entering your business. A built-in firewall provides a perimeter defense to guard your internal network, computers and employees from unauthorized access, such as Trojan horse attacks or hackers trying to "spoof" their way in by pretending to be legitimate users.

The advanced firewall with "stateful packet filtering" can grant or deny network access based on time of day, application, IP address, port range and other attributes. Ultra-granular control enables Web or data traffic to be restricted while still letting IP telephony calls pass through.

Protect the core platform itself. Digital signatures and enhanced tamper detection features ensure that only trusted sources are used for software upgrades. The Linux operating system has been hardened with strong access controls that restrict access to the operating system and file system. Security diagnostics and self-test capabilities facilitate system integration and enhance product support. An alarm system immediately alerts administrators to any potentially important security issue.

Establish stringent security best practices within the business. For example, data users and administrators log in with passwords that can be centrally maintained and regularly changed. The system locks out access after someone makes several failed attempts to login, ends a session when a user leaves a workstation idle for too long and closes unused accounts after a designated time.

Maintain a detailed audit trail. User and administrator activity — even password changes — are encrypted for confidentiality and tracked in a secure audit log. Audit log records can be archived off-box for extended, persistent storage.

Prioritize your most important data services. Some data services, such as IP telephony, are sensitive to even the slightest delay, while others, such as email or fax, can receive secondary treatment if necessary. Business Communications Manager platforms accommodate these differences with quality of service (QoS) capabilities that recognize and prioritize voice traffic for fastest treatment, even if you are using an external router.

Conserve valuable bandwidth by avoiding unnecessary network traffic. For instance, frequently-visited Web pages, such as the business home page, can be cached on the local system and updated automatically — thereby eliminating the need to go back through the Internet every time this page is requested. An internal Domain Name System (DNS) function remembers the

Full security management

- Active protection – detection, blocking and repair
- Cost-effective support for multi-vendor solutions
- Policy-based, central solutions for easy provisioning and audit
- Comprehensive reports for ongoing security analysis and follow-up

IP address of previously accessed Web pages, so the system does not re-visit the Internet for a URL-to-IP conversion.

Increase security and flexibility in IP addressing. Network Address Translation (NAT) converts internal IP addresses into your public IP address and vice versa. By hiding your private IP addresses from the world, NAT provides an extra layer of security. NAT can also be used to share static addresses across a group of users who need exclusive, but temporary, use of a static IP address. Since static IP addresses can be costly, this can translate into hard cash savings for your company.

A Dynamic Host Control Protocol (DHCP) function within the Business Communications Manager platform automatically issues IP addresses as needed. In addition to its value for sharing IP addresses through NAT, DHCP enables mobile users to simply walk into a wireless IP hot spot, and their IP telephony-equipped laptop is automatically ready to make and receive calls.

Connect to the Internet and intranet through one link. A single physical interface can support up to five IP addresses for internal and external communications, each with its own filters and policies. For instance, on one wide area network (WAN) link, you could set up:

- An Internet connection that limits inbound traffic, so users could browse the Web for legitimate research but not download huge music or video files
- Another private virtual connection that permits free flow of traffic on your company's internal network
- A third connection for remotely managing the Business Communications Manager unit over the Web, yet thwarting hackers by permitting no internal routing from this virtual connection

Data services made affordable, achievable and secure

Your Business Communications Manager system with embedded router makes an attractive package for small sites wishing to become Internet-capable, medium-sized sites that formerly couldn't be included in the corporate WAN because the cost was too high, and managed service providers who want the convenience of bundling voice and data in a single, easy-to-manage platform.

Robust security features safeguard the confidentiality and integrity of network resources and allow access only by authorized users and administrators. Security policies are implemented, enforced and adapted to block real-time threats. With adaptive defense, your business, its applications, data and users are protected from zero-day events.

Discover for yourself the advantages of secure converged voice and data services on Business Communications Manager platforms. For more information, contact your local reseller or visit us on the Web at: *www.nortel.com/bcm*.

Business Communications Manager security features at a glance

Layered security in the platform

- Hardened, robust platform for integrity and security
- Full audit trail of login and configuration change activity
- Full alarm and log management capabilities
- Security diagnostics and self-test
- Vulnerability resolution infrastructure
  - Dedicated Nortel Security Advisory Task Force
  - New threats constantly monitored and expediently addressed
- Robust Linux operating system

Access management security

- Stringent password and session management
  - Password policy and management via Business Element Manager and telephone
  - Password aging, history and change notification
  - Lockout policy and management via Business Element Manager and telephone
- Account policy and management with account expiry
- Privilege assignment and management with logon messages
  - Access to system resources and services restricted according to privilege level
  - Predefined and configurable, multi-level privilege groups and permissions
- Certificate management
- Centralized authentication and authorization using RADIUS client
  - Central management of accounts for multiple network elements
  - Fallback to secondary RADIUS server
  - Optional local authentication available

Interface security

- Modem control management and PPP security
- Remote network access and telephone administrative interface
- IPSec virtual private networks (VPNs), VPN client support
  - Site-to-site VPN capabilities
  - Client-side VPNs for remote/mobile users
  - SSH and SSL for secure communications
- Firewall management
  - Stateful firewall
  - Content filtering by IP address, URL keyword, Web feature
  - Resistance to denial-of-service (DoS) attacks
- Network address translation (NAT) management
- SNMP access security (SNMPv3)
- Encrypted communications: SSL/SSH, HTTPs for management traffic

Telephony security

- Toll fraud protection — Passwords, activity logging, dialing restrictions
- Information security — PIN-protected voice mail, hidden speed dial numbers, encrypted transmission of call detail record (CDR) log data
- Handset security — Only sets activated by keycode can be used

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. Our next-generation technologies, for both service providers and enterprises, span access and core networks, support multimedia and business-critical applications, and help eliminate today's barriers to efficiency, speed and performance by simplifying networks and connecting people with information. 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.

NN111340-082806

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