



Application Brief

**Nortel Networks**

# Securing the converged enterprise branch—Secure routing for voice and data with BCM and Contivity

The integration of Nortel Networks SRT into Business Communications Manager and Contivity gives customers a highly converged, secure, and low-cost access solution for enterprise branch networking.

The Business Communication Manager (BCM) is an IP-optimized data and telephony solution that has rich voice functionality and supports Web-enabled communications. It provides an unparalleled match of convergence voice and data for a unified IP internetworking solution. The BCM is a single platform that delivers both TDM-based and IP-based telephony, a full complement of applications such as Internet access, voice messaging, and call center capabilities, as well as Web-based system management.

**NORTEL**  
NETWORKS™

The Contivity\* Secure IP Services Gateways are purpose-built secure access routing devices designed to secure transmission of IP traffic via a Virtual Private Network (VPN/IPsec) tunnel. Contivity offers highly flexible and scalable solutions that provide secure remote access for individual remote (PC) clients, teleworkers, and small branches along with large-scale secure VPN aggregation at enterprise central locations.

Deployed together as a branch solution that both leverage Nortel Networks Secure Routing Technology, BCM and Contivity can cost-effectively and securely provide a total solution that addresses the critical requirements of enterprise branch voice and data networking.

**This combined solution provides enterprises the following benefits:**

- Low-cost converged enterprise branch deployments (one device at CPE)
- Secure dynamic branch office routing via Nortel Networks Secure Routing Technology (SRT)
- High performance and scalable enterprise VPN branch networking
- Secure remote access for SOHO, teleworkers, and mobile employees

There are two primary network design scenarios that leverage the synergy between the BCM and Contivity solutions:

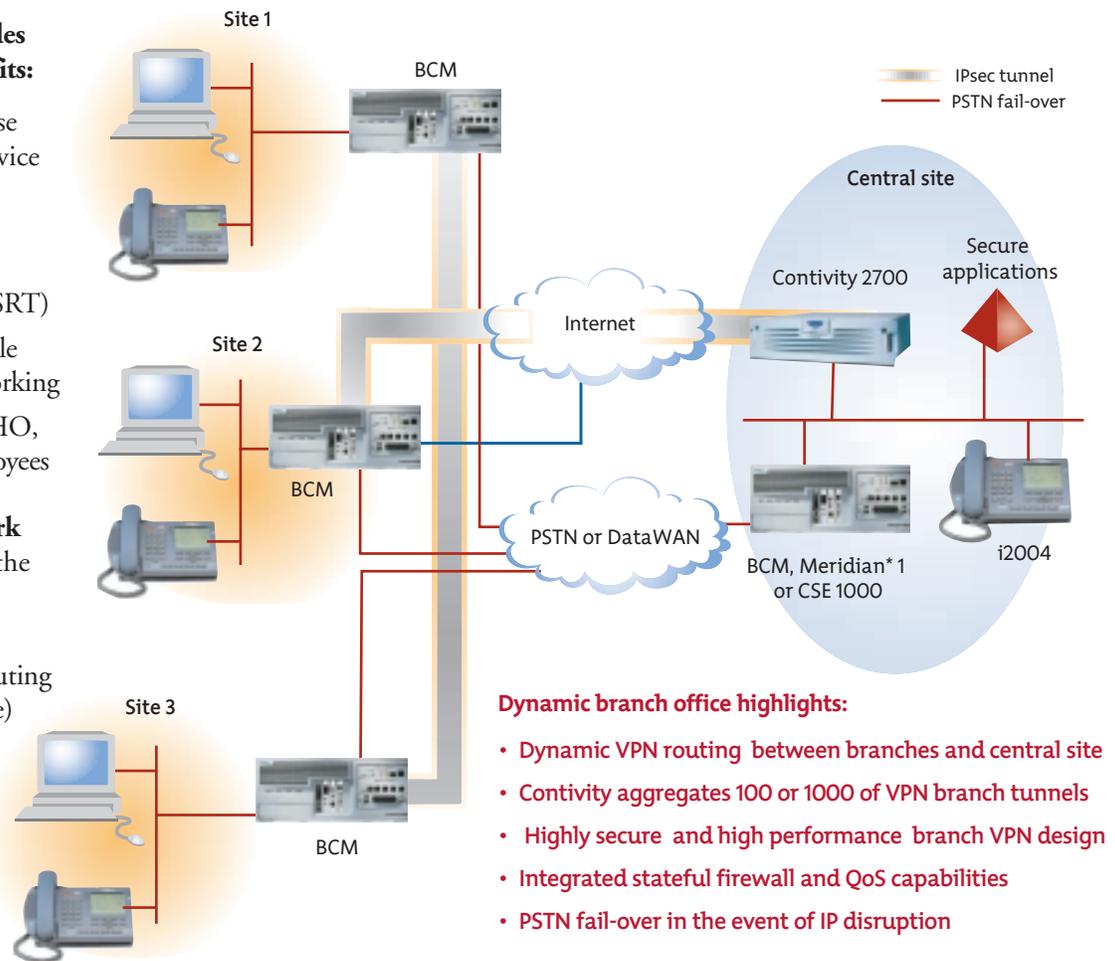
- Secure branch office VPN routing (branch-to-branch/central site)
- Remote access VPN for teleworkers/SOHO and mobile employees

In this first example (Figure 1), a customer with a number of converged BCM branch locations can turn on the secure dynamic routing aspect of SRT via a key-coded enabled VPN IPsec option to provide secure dynamic routing back to a central site Contivity Gateway. The central site Contivity can then aggregate and scale hundreds or thousands of secure BCM branch office VPN tunnels.

In this example, BCM could be the only CPE device deployed at the enterprise branch location or BCM could be deployed behind a dedicated (existing) IP access device. In either case, the customer can securely leverage the IP

network for flexible, low-cost networking for all voice and data traffic between all the locations. BCM-to-BCM traffic would be connected securely between point-to-point or meshed BCM connections. Hierarchical hub and spoke type traffic would flow from many BCM branches and be aggregated at the Contivity at the “central” site.

BCM can terminate 20 VPN tunnels. It makes sense to deploy a Contivity at any site (branch or central) that needs to aggregate more than 20 simultaneous IPsec VPN tunnels as a general design rule.



**Dynamic branch office highlights:**

- Dynamic VPN routing between branches and central site
- Contivity aggregates 100 or 1000 of VPN branch tunnels
- Highly secure and high performance branch VPN design
- Integrated stateful firewall and QoS capabilities
- PSTN fail-over in the event of IP disruption

**Figure 1. Dynamic branch office VPN routing**

For many small branch/SOHO type locations, a BCM solution may prove to be too large (Figure 2). However, these locations still can benefit from the secure converged voice/data BCM value proposition connected as an extension off the primary BCM. Deploying a low-cost Contivity platform at these smaller branch/SOHO sites allows these locations to participate as a “remote branch” off the primary BCM location, thereby providing the full set of IP and telephony features that the primary branch users enjoy.

Again, the secure access between the two locations is enabled by a seamless SRT (IPsec) dynamic routing connection. Contivity can serve as the primary SOHO IP access device connected either by a WAN (T-1, V.35) or behind a DSL modem (10/100, PPPoE) connection.

In addition to connecting these SOHO locations, the enterprise may need to provide secure access for remote and mobile users. The Contivity solution excels at addressing this type of secure remote access requirement. In this case, the remote users would simply be provided the Nortel Networks Contivity VPN IPsec client software for their PC/laptop—and all access to the branch BCM location would be fully authenticated and encrypted for absolute security.

Remote users can also take advantage of the Nortel Networks i2050 Internet softphone for secure voice and data communications over a single IP connection to flexibly address the mobility requirements of this population.

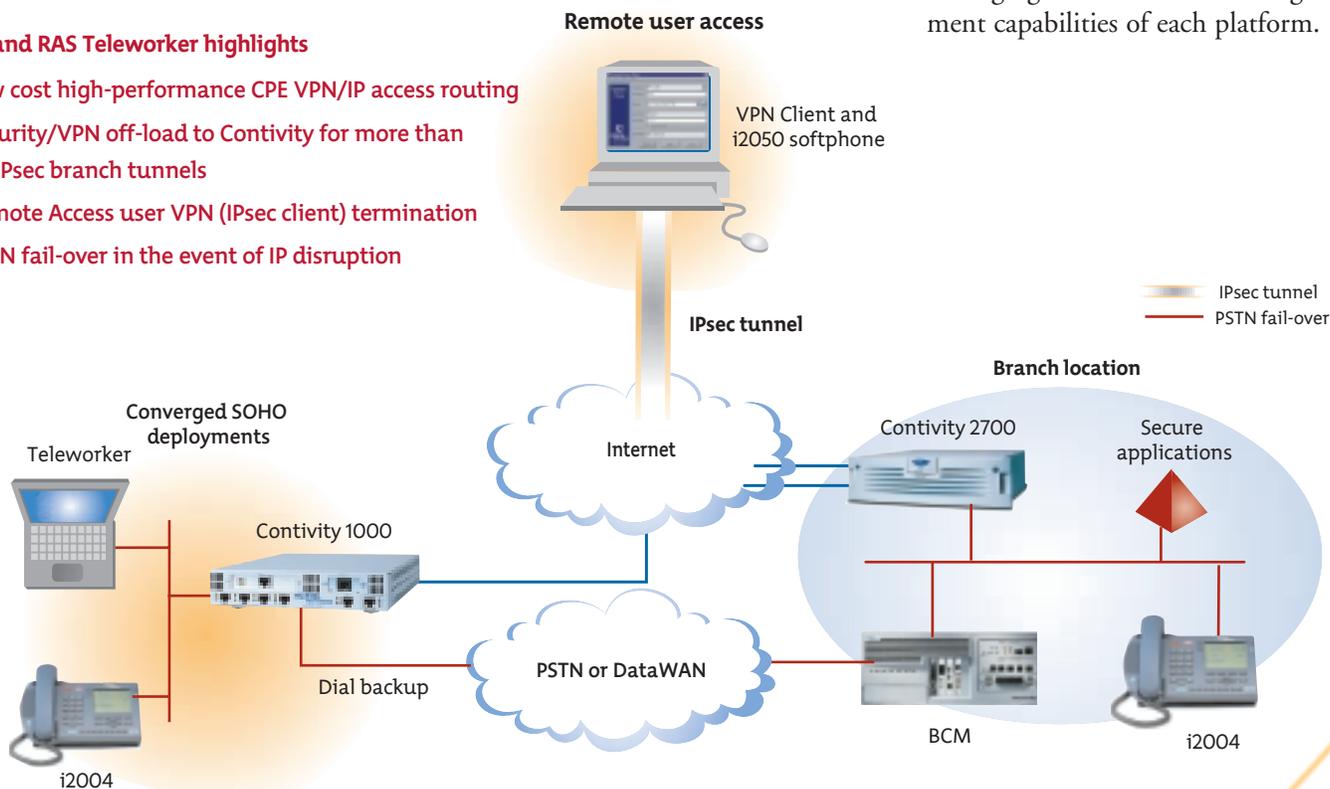
## The need for QoS

The interaction between BCM and Contivity does not stop at IPsec dynamic routing. Since voice traffic is sensitive to delay, it’s critical to prioritize VoIP over concurrent data traffic. BCM and Contivity’s open and standards-based Quality of Service (QoS) mechanisms are enabled to ensure the highest quality handling of voice traffic. This QoS interaction occurs within the secure IPsec tunnels that are established between the two endpoints.

The individual QoS capabilities of each platform act as a system to provide Expedited Forwarding of voice traffic by Classification and Marking the traffic (via Differentiated Services or DiffServ) along with shaping and policing of the traffic as it flows through the network. Fine grain control over users, devices, locations, and applications can also be enforced by leveraging the Bandwidth Management capabilities of each platform.

### VPN and RAS Teleworker highlights

- Low cost high-performance CPE VPN/IP access routing
- Security/VPN off-load to Contivity for more than 20 IPsec branch tunnels
- Remote Access user VPN (IPsec client) termination
- PSTN fail-over in the event of IP disruption



For designs that call for small-scale remote client access, BCM v3.0 also adds the ability to terminate up to 16 Contivity IPsec VPN client connections

Figure 2. VPN access for RAS and teleworkers

## Secure Routing Technology on Contivity and BCM

Secure Routing Technology (SRT) is a Nortel Networks architectural framework that addresses the dynamic routing and scaling requirements of deploying large-scale secure virtual private networks (VPNs).

As more and more enterprises move to deploy virtual private networks, it becomes critical to address the performance, scalability, and dynamic requirements of these networks in the same dynamic manner that traditional "clear text" IP-routed networks have benefited from in the past.

Most of the recently deployed enterprise branch VPN networks have been constrained by static branch configurations along with complex overlay protocols and administration that have limited the size and scale of these networks. These early designs have been typified by bolted-on IPsec encryption to existing multi-protocol routers with no real integration between dynamic routing and VPN/security.

Nortel Networks SRT overcomes these limitations by truly integrating dynamic IP routing capabilities within a secure VPN framework to allow extremely high levels of scalability, performance, and overall security when building large enterprise class virtual private networks.

SRT was first introduced on Contivity Secure IP Services Gateways and has just recently been extended to the Business Communications Manager (BCM) platform.

The benefit to Nortel Networks customers is that they can now deploy a combined solution in a fully interoperable manner that allows them to extend their convergence branch office network—dynamically, securely, and for very low total cost of ownership.



*Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Metro and Enterprise Networks, Wireless Networks, and Optical Long Haul Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the web at:*

**[www.nortelnetworks.com](http://www.nortelnetworks.com)**

**In the United States:**

Nortel Networks  
35 Davis Drive  
Research Triangle Park,  
North Carolina 27709  
USA

**In Canada:**

Nortel Networks  
8200 Dixie Road,  
Suite 100  
Brampton, Ontario L6T 5P6  
Canada

**In Caribbean and Latin America:**

Nortel Networks  
1500 Concorde Terrace  
Sunrise, FL 33323  
USA

**In Europe:**

Nortel Networks  
Maidenhead Office Park  
Westacott Way  
Maidenhead Berkshire SL6 3QH  
UK

**In Asia:**

Nortel Networks  
6/F Cityplaza 4,  
Taikooshing,  
12 Taikoo Wan Road,  
Hong Kong  
Tel:(852)21002888

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

GSA Schedule GS-35F-0140L  
1-888-GSA-NTEL

\*Nortel, Nortel Networks, and the Nortel Networks corporate logo, and Contivity are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2002 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

**NN101820-0902**