>THIS IS THE WAY

>THIS IS NORTEL™

Secure Remote Access Technical Solution Guide

Enabling Application, IP Telephony and Multimedia Access for Teleworkers and Road Warriors

Enterprise Solution Engineering
Document Date: January 2006
Document Version: 1.0

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

Trademarks

Nortel, the Nortel logo, the Globemark, Unified Networks, PASSPORT, BayStack, Nortel Application Switch, Nortel Business Communications Manager, Nortel Communication Server, Nortel IP Softphone, Nortel Multimedia Communication Server, Nortel Multimedia PC Client, Nortel Multimedia Web Client, Nortel Threat Protection System, Nortel VPN Gateway, and Nortel VPN Router are trademarks of Nortel.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

All other trademarks are the property of their respective owners.

Disclaimer

This engineering document contains the best information available at the time of publication in terms of supporting the application and engineering of Nortel products in the customer environment. They are solely for the use by Nortel customers and meant as a guide for network engineers and planners from a network engineering perspective. All information is subject to interpretation based on internal Nortel test methodologies, which were used to derive the various capacity and equipment performance criteria and should be reviewed with Nortel engineering primes prior to implementation in a live environment.

Abstract

This guide is intended to define the recommended designs and best practices for a Secure Remote Access Solution. The document provides an overview of the best design practices to implement a network capable of providing access to business applications, including web applications, client-server applications, and IP Telephony and multimedia services to teleworkers and road warriors.

The intended audience for this Solution Guide is Nortel sales teams, Partner sales teams and end customers. All of these groups can benefit from understanding the common design practices and recommended components for a Secure Remote Access Solution.

Revision control

No	Date	Version	Revised by	Remarks
1	10/19/05	0.1	B. Black	Initial Draft
2	11/18/05	0.2	B. Black	Best Practices and Other Updates
3	11/28/05	0.3	B. Black	Edits based on initial feedback
4	11/29/05	0.4	B. Black	Review-Ready Draft
5	01/27/06	1.0	B. Black	Final

Acknowledgements

Gerardo Flores – Enterprise Solution Engineering

Shangli Lu – Enterprise Solution Engineering

Table of contents

1. Overview

Today’s enterprise network must support a growing number of mobile workers who require access to a broad range of information and applications. These workers include full-time teleworkers who use remote access as the primary connection to the network and services. There is also a growing number of occasional teleworkers. Another key user category is the road warrior, who improves productivity by engaging customers and business partners out of the office but must stay connected. As organizations recognize the benefits of IP Telephony and multimedia solutions, including intelligent call routing, network presence, application integration, and network convergence, they demand that these benefits be available beyond the traditional boundaries of the enterprise network. This Technical Solution Guide provides a prescription for meeting this requirement while providing the network and information security that must accompany such a solution.

This guide provides a list of best practices for Secure Remote Access that reduce security exposure and lower cost of operation. It provides information about solution design, deployment, and network integration to maximize the benefits to your organization.

1.1 Scope of solution

This document describes the infrastructure components required to design a Secure Remote Access solution. This document highlights the Nortel recommended designs and best practices for implementing a converged solution. While it is impossible to include every design scenario, this document discusses the most prevalent situations encountered within the enterprise. The following highlights the components covered within these designs:

Virtual Private Network Gateway:

Nortel VPN Gateway 3050
Nortel VPN Gateway 3070
Nortel VPN Router 221/251

Server load balancing for resiliency and scalability:

Nortel Application Switch 2424
Nortel Application Switch 3408

Intrusion detection and prevention (optional but recommended):

Nortel Threat Protection System

Communication Servers and Clients:

Nortel Multimedia Communication Server 5100
Nortel Communication Server 1000
Nortel Business Communications Manager 50/200/400
Nortel Multimedia PC Client
Nortel Multimedia Web Client
Nortel IP Softphone 2050

2. Secure Remote Access best practices

Following best practices in designing and deploying a remote access solution lowers cost of ownership and dramatically lowers the risk of common security incidents, such as unauthorized access, theft of information, hacking, denial of service and propagation of threats such as worms and viruses. Nortel solutions fully support these best practices.

2.1 Keep it simple!

Complexity is the enemy of security and should be avoided in a Secure Remote Access design. Determine which set of applications each group of users needs. This application set will be small for most users, and typically includes:

- Web access to e-mail
- Access to a common web portal (News and Frequently Accessed Information)
- Phone directory
- IP Telephony and multimedia
- Web access to voice mail, such as Nortel CallPilot
- Employee tools such as expense vouchering/purchasing/timesheets
- Key line-of-business applications based on employee role

The number of unique roles or groups of users is also typically small and might not directly map to the concept of organizational departments. For many deployments, providing access to less than a dozen key applications maximizes the benefit of remote access while allowing strict access control and tracking.

2.2 User authentication

The first step in granting access is user authentication: establishing that a remote user has the appropriate credentials to connect to the network.

Use a network-based external authentication system that is common to your network and application environment. Users should not have different sets of IDs and passwords for remote access. A common authentication system simplifies user management and authorization control, as well as providing a framework for single sign-on or reduced sign-on capability.

When possible, use a two-factor authentication system that implements a one-time-password (OTP) scheme. These systems are compatible with existing authentication systems and prevent unauthorized access based on password guessing or theft. Two-factor authentication schemes are a key requirement when allowing access from public devices, such as shared PCs and Internet kiosks. You can also restrict remote access to less sensitive applications if users do not present two-factor-based credentials.

When two-factor authentication is not used, prevent password guessing by requiring passwords that are at least eight characters long and use a mix of letters, numbers, and punctuation. Set these passwords to expire at regular intervals, and prohibit reuse of the past five passwords.

Employ a preauthentication scan of the client system to detect crimeware or malware, such as keyloggers, to prevent theft of access credentials.

Employ a mechanism for Password Guess Lockout to disable an account upon successive failed logon attempts. You can do this through configuration of your network-based authentication system. The mechanism must be tied to a process that alerts system administrators of failed logon attempts and requires follow-up with appropriate action.

Define a procedure to reset expired or locked-out passwords that requires providing additional private information that is only known to valid users.

2.3 Client admission, compliance, and remediation

In addition to user authentication, check the security policy compliance of endpoints, such as PCs, laptops, and other devices connecting to your network, before they are admitted. Establish a minimal set of criteria that includes:

Antivirus protection and signature updates

Personal firewall to protect PCs while connecting through the Internet

Antispyware to detect and remove software that collects personal information

Required operating system type, version, and service pack level

You can also use this minimal set of requirements to distinguish managed devices from shared PCs such as Internet kiosks and home computers. In the case of non-compliance, you can deny access or provide access to a minimal set of controlled web applications based on the security sensitivity of your environment. You may also wish to provide a remediation portal for non-compliant devices with access to software updates, patches, and other tools.

2.4 Establish authorization based on user and network context

Employ the security concept of least privilege – only allow access to the minimal set of applications and network subnets required for each group of remote access users. In general, remote access users do not need full IP access to all parts of your network, including desktop subnets and all application servers. Use per-group access controls as a baseline for limiting access. Augment this baseline with additional rules to allow or deny access based on:

Authentication strength (client-certificate use, simple password or OTP/two-factor)

Device type (managed or non-managed/shared)

Source IP address (applicable for home-based teleworkers with static IP assignments)

Results of endpoint compliance scanning

Access type (such as web-only access or full IP access through virtual network adaptors)

2.5 Inspect and track remote access user activity

After users are granted access, it is critical to continually monitor and log activity. Check endpoint compliance periodically to determine if rogue software successfully disabled security software during a session.

Ensure that key security and information access related events are logged to a centralized event manager, such as a syslog server or security event/incident collector. Examples of items to track include:

Successful and failed logon attempts, including source address and username

Session start and stop times

IP assignment of private addresses with correlation to username

Access control violations

Endpoint compliance-check violations

When providing web-based access, the VPN Gateway will proxy all information requests through a single, common internal IP address. In this case, configure the gateway to embed user information such as the username in HTTP headers to allow per-user tracking through internal IDS and web application servers.

Ensure that the topology you use for remote access deployment allows security inspection of non-encrypted traffic. This requires placing internal firewalls and intrusion detection and prevention (IDP) systems on the trusted side of the VPN Gateway so that remote user traffic can be inspected and blocked accordingly.

2.6 Protect information and network access

There are a number of techniques you can employ to ensure that information and network access are protected, even in the case of forgetful or careless end users. Examples include:

Enable idle timeouts to close a remote access session after a period of inactivity. This limits unauthorized access if a user walks away from an active session.

Enable session timeouts to limit the total session time allowed.

Use a cache wiper to remove any residual data left behind during a session.

Disable split tunneling. Split tunneling allows non-remote access traffic, such as web access to Internet sites, to bypass the VPN connection. If a connected PC is compromised and a hacker connects through a backdoor, the hacker will have access to internal resources during an active session. To limit the possibility of this type of attack, disable split tunneling. Note that this will not prevent reverse-connecting Trojan horses and backdoors unless the protocol ports used are blocked by your access control lists and DMZ security policies. Use endpoint security checking, including malware detection, to disallow connections from hosts infected with those threats.

2.7 Ensure remote access availability

Provide a resilient and highly available solution by using an active/active deployment with redundant VPN Gateways. Depending on the size of your network and criticality of remote access, you may wish to employ both local redundancy through clustering and geographical redundancy with a multisite VPN Gateway deployment.

2.8 Don’t forget people, process, and policy

These best practices are related to deployment options for a Virtual Private Network. Such a solution needs to reflect company policies and procedures, including:

Information security policy

Audit logging and data retention policy

Appropriate legislative compliance policies

In addition to the technology to support Secure Remote Access, it is critical to establish operating procedures and security policy elements specific to remote users and clients.

Education and training of end users also plays a key role in protecting information and securing access to the network.

3. Supported access modes

The VPN Gateway portfolio provides several different access modes. These access modes can be used concurrently by different users or groups. They can be served from the same public IP address or separated as desired. Each mode has advantages and disadvantages in terms of application support flexibility, compatibility, and security.

3.1 IPsec

IPsec delivers network level access to the intranet through a preinstalled software client that provides a virtual network adapter to the client operating system. All applications and protocols are supported, and the end user experience is comparable to that of a LAN connected user. Access controls configured on the VPN Gateway limit which subnets the client can access. Endpoint security for IPsec access is provided by an installed version of the TunnelGuard agent.

IPsec strengths include broad application support and the fact that it is a proven, time-tested technology for Secure Remote Access.

IPsec weaknesses include the fact that the client must be installed on each connecting device and the fact that some networks may block the protocol ports used by IPsec. This can be an issue for traveling employees that spend time in corporate intranets managed by external parties, such as customers or business partners.

3.2 SSL-VPN Clientless Mode

SSL-VPN Clientless Mode allows any web browser to be used as a VPN client. It provides access to a portal with links to web-based applications (see Figure 1 for a sample SSL-VPN portal).

The advantages of SSL-VPN Clientless Mode include ubiquitous access, including home PCs, Internet kiosks and shared or public PCs. No software installation is required. A Java Virtual Machine is required to provide endpoint compliance checking through an applet-based version of TunnelGuard. Another benefit of SSL-VPN Clientless Mode is that it provides a highly restricted access mode, with all web requests proxied by the VPN Gateway. This provides a high level of granular access control, including URL path checking on a per-group basis.

SSL-VPN Clientless Mode cannot provide access to non-web applications.

3.3 SSL-VPN Enhanced Clientless Mode

SSL-VPN Enhanced Clientless Mode extends the Clientless Mode through Java applets that enable client-server application communication. This mode provides access to many client-server applications, such as e-mail clients, including Microsoft Outlook, and remote access applications, such as Windows Terminal Server or Citrix.

SSL-VPN Enhanced Clientless Mode cannot provide access to complex applications that do not support Network Address Translation (NAT) or that use dynamic ports. An example of a complex application is Voice over IP (VoIP).

3.4 SSL-VPN NetDirect Mode

NetDirect Mode provides full network level access through a virtual adapter. A browser-based applet version of NetDirect is available, as well as a preinstalled client version. NetDirect was developed to provide IPsec-like access without the limitations of IPsec, such as the requirement for preinstallation and issues with NAT and firewall traversal. NetDirect supports any IP application and has an optimized FastPath mode for UDP-based traffic, such as the real-time protocol (RTP) used to carry VoIP traffic.

NetDirect has some specific browser and platform requirements, depending on the version of VPN Gateway software used. In addition, NetDirect may require the user to have Administrator rights on the client PC.

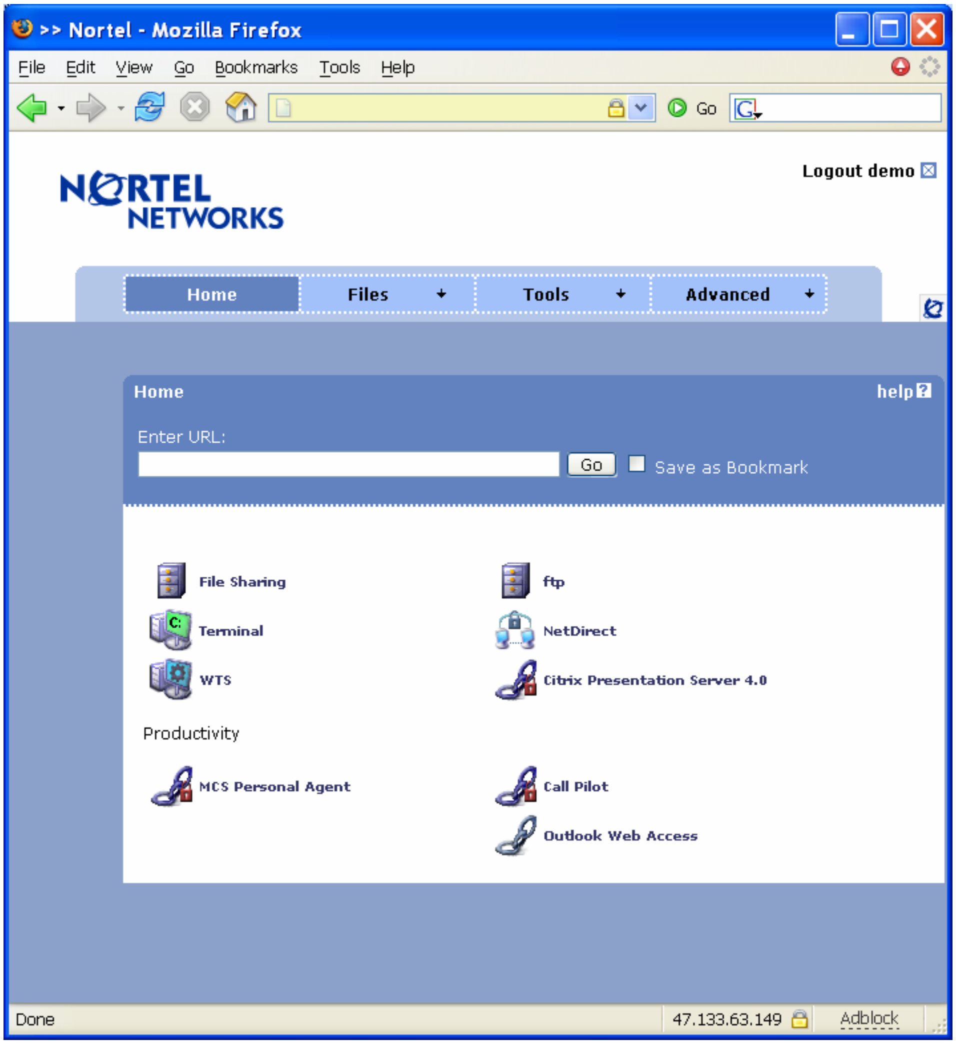

Figure 1: Sample SSL-VPN portal

4. Secure Remote Access design

This section addresses Secure Remote Access design in terms of security, resiliency, and considerations for both application access and IP Telephony access primarily through software IP Phone clients.

4.1 Secure Remote Access Solution topology

Figure 2 on page 13 depicts a basic topology for a non-resilient solution. Connecting clients can be anywhere on the global Internet. When using IPsec, clients launch a software client, which connects to the VPN Gateway after resolving the public domain name system (DNS) name. When using SSL-VPN, a browser is used to connect to the Gateway through a URL such as https://sslvpn.example.com. Although many scenarios are possible, a simple and time-tested configuration is to place the VPN Gateway behind an Internet-facing screening router or firewall. This router or firewall restricts access to the DMZ to application traffic based on protocol ports. You can choose to deploy one or more access modes.

4.1.1 Required DMZ access policies

Based on the access modes used, configure the following minimal rules to allow client traffic to connect to the VPN Gateway on the appropriate service addresses, also known as Virtual Internet Protocol addresses (VIP).

Access mode	Protocol/ports allowed to reach VIPs
SSL-VPN Clientless (web applications) SSL-VPN Enhanced Clientless (web and client server applications)	TCP 443
SSL-VPN NetDirect SSL-VPN NetDirect FastPath (optional)	TCP 443 UDP 5000, 5001 (optional)
IPsec	UDP 500 (IKE) IP Protocol 50 (IPsec ESP) UDP 10001 (Recommended port for NAT traversal)

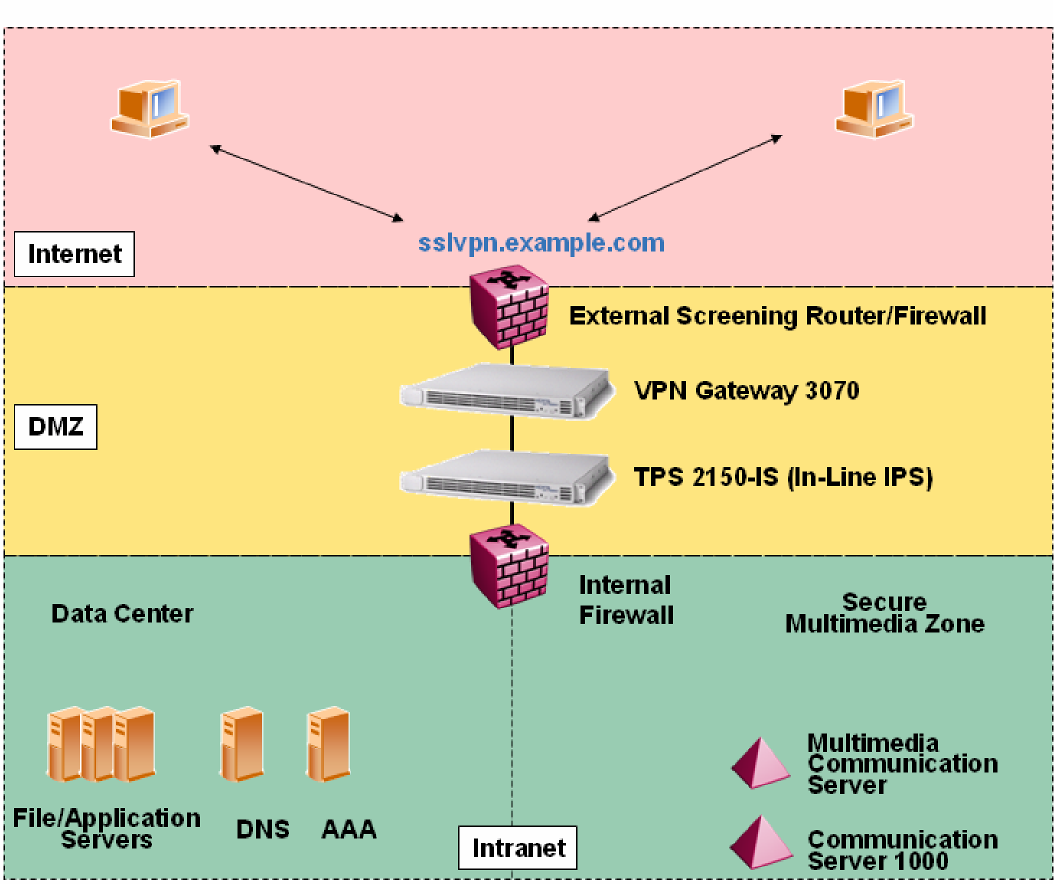

Figure 2: Secure Remote Access Solution topology

4.1.2 Required internal firewall policies

The VPN Gateway must have restricted access to intranet resources through the DMZ internal firewall. The security policy on this DMZ internal firewall is completely dependent on the applications and services provided by the remote access solution. Access to DNS and Authentication, Authorization, and Accounting (AAA) servers must be configured to provide name resolution and end-user authentication services to the VPN Gateway. In general, you should only configure access from the VPN Gateway trusted interface IP address to specific application servers. The exception is that when using NetDirect, you must assign a block of internal network addresses for use by NetDirect clients. Packets from NetDirect clients are forwarded on the trusted interface of the VPN Gateway and must access intranet resources through the DMZ internal firewall.

When NetDirect is used to provide IP Telephony services, the NetDirect pool of addresses may need to reach IP telephones or PCs within the Local or Wide Area Network to support peer-to-peer media connections using the RTP protocol, which runs over UDP. Use internal firewall policies to restrict which protocols and ports can access these internal zones. The RTP protocol typically uses a UDP source port greater than 1023 and a range of UDP destination ports between 40 000 and 60 000.

4.1.3 Threat Protection System (intrusion prevention) integration

Although not strictly required, Nortel strongly recommends the use of an intrusion detection/prevention system as an additional security layer in remote access solution designs. In the case of compromised or infected endpoints, an in-line intrusion prevention system (IPS) can detect and block known threats and act as a second line of defense to block unauthorized traffic. Place the IDS/IPS sensor on the trusted side of the VPN Gateway so that visibility to clear-text (non-encrypted) traffic is possible. Figure 2 shows the Nortel TPS 2150-IS in-line intrusion sensor configured in the path between the trusted interface of the VPN Gateway and the DMZ internal firewall.

Design recommendation: Deploy IDS/IDP sensors on the trusted side of the VPN Gateway to allow security inspection of clear-text traffic and provide visibility to threats from connecting remote access clients.

4.2 Network design

This section addresses network design including Security, Application Access, IP Telephony/Multimedia, Network Management and client considerations.

4.2.1 Security

This section addresses specific security recommendations and considerations beyond those discussed in section 4.1.1, related to DMZ policies and network topology.

4.2.1.1 Authentication

The choice of authentication method is often dictated by existing network directory and application infrastructure. Supported options include local, RADIUS, LDAP (including Microsoft Active Directory), NTLM, SiteMinder, RSA ClearTrust, RSA SecurID or Client SSL Certificate. Ideally, your IT infrastructure will have a single authoritative authentication source and you can base VPN authentication on this same system. Require strong two-factor authentication if VPN clients will connect from non-managed or shared client devices.

In addition to the product documentation, you can find a number of Technical Tip guides related to authentication, including RADIUS, LDAP, NTLM and certificate-based AAA, at the Nortel customer support portal at www.nortel.com/cs in the VPN Gateway 3050 documentation area.

Design Recommendation: Use a network-based authentication system that is also used by your IT infrastructure. Require strong two-factor authentication for VPN clients connecting from non-managed or shared client devices.

4.2.1.1.1 Single sign-on

Users connect to the VPN to access applications. Often these applications implement their own authentication and authorization mechanism. To simplify user access and reduce the need for multiple, redundant logons, the SSL-VPN provides a variety of single-sign-on capabilities. For web-based and file-sharing applications, you can configure the VPN portal links to automatically provide reusable credentials to internal applications. You can do this for applications that support:

HTML form-based logon, such as Microsoft Outlook Web Access

Standard HTTP authentication

Authentication through custom HTTP headers

You must restrict the use of single-sign-on (SSO) and credential passing to known application servers and domains to prevent non-approved systems from presenting a web authentication request and acquiring user credentials. Therefore, only identify approved applications as authorized SSO domains in the SSL-VPN configuration.

Design Recommendation: Use single-sign-on capabilities but restrict servers and domains to which the VPN Gateway passes credentials, to prevent password stealing from non-approved hosts.

When using token-based two-factor authentication systems that use a one-time password, the credentials cannot be reused for applications that also require OTP authentication. In this case, the solution supports several interworking options with third-party products that can insert a cookie in the browser with an encrypted authentication token after the OTP VPN logon step. This cookie is then inspected by the compatible applications to allow access. This solution combines the benefits of OTP/two-factor authentication with web-based single sign-on. Supported third-party products include Computer Associates SiteMinder and RSA ClearTrust.

You can also combine OTP/two-factor VPN logon with standard username/password reusable credentials for intranet application single sign-on. In this case, use the Secondary Authentication option to allow the user to provide both OTP and reusable credentials at VPN logon.

4.2.1.2 Authorization

The authorization process determines which specific resources can be accessed by an authenticated user.

4.2.1.2.1 Group model

The group model is fundamental to authorizing user access to intranet resources. During the authentication process, a user is associated with one or more groups. Each group is associated with unique:

Portal links to applications and file-sharing directories

Access control lists, including destination subnet addresses, HTTP URL paths, and destination hostnames

TunnelGuard endpoint compliance policies

IP pool addresses for IPsec and NetDirect clients

Permitted access modes (IPsec, SSL)

Session and idle timeout values

If a user belongs to more than one group, the group settings are logically joined so that the user sees all appropriate portal links and has access to all appropriate resources for the set of groups.

Design recommendation: Map your VPN users into a small set of groups and use those groups to control network access and portal application links.

4.2.1.2.2 Access control

The Nortel VPN Gateway allows fine-grained control of which intranet resources can be accessed by users. The following basic objects can be defined:

Access control object	Attributes
Network reference	A collection of IP subnets and IP host addresses
Network reference for web portal modes	DNS hostname
Service reference	TCP/UDP ports
Application reference for web portal modes	URL path , FTP directories, SMB directories

4.2.1.2.3 Extended profiles

Extended profiles allow refinement of access control based on a real-time context associated with the user. Access can be extended or restricted from the base access control list (ACL) based on:

Authentication strength (client-certificate use, simple password or OTP/two-factor)

Device type (managed or non-managed/shared)

Source IP address (applicable for home-based teleworkers with static IP assignments)

Results of endpoint compliance scanning

Access type (such as web-only access or full IP access through virtual network adaptors)

4.2.1.3 Endpoint compliance

The ongoing threat of worms, Trojan horses, and viruses presents a challenge for secure remote access. The value of Internet-based Virtual Private Networks is the ubiquity of access. The fact that clients must use the Internet implies that they are subject to the risk of infection and hacking. In addition, mobile devices such as laptops can be used for non-corporate Internet browsing prior to connecting to the VPN, presenting an opportunity for infection and subsequent worm propagation into the intranet.

Endpoint compliance through TunnelGuard requires the scanning devices, prior to allowing network admission, to ensure that a minimal set of security standards are met. These security standards can include:

Antivirus protection and signature updates: By checking that these are up-to-date and active, you can ensure that a basic layer of protection is in place to prevent viruses from being propagated from the connecting host. Current antivirus suites also do a good job of detecting and blocking known worms and Trojan horses, which can spread and infect PCs without user intervention (such as opening an e-mail attachment).

Personal firewall to protect PCs while connecting through the Internet: Install personal firewalls, running and configured to block attempts to connect to network services, such as file-shares or remote control tools, when a client PC is on the Internet.

Required operating system type, version and service pack level: Checking for baseline client operating system type, version, and service pack level assures compatibility and prevents older, potentially vulnerable systems from connecting. You can also check for specific patches when known vulnerabilities have been addressed by software patches. If you are using third-party software compliance and software management tools, you can check that they are installed and active.

If any of the compliance checks fail, based on the user role and risk factors you can:

disconnect the user immediately

provide limited access to a restricted set of applications

provide access to a remediation portal to correct security software and operating system compliance issues

You can deploy TunnelGuard for SSL-VPN users through a clientless agent that runs in the browser during network connection. IPsec users require the TunnelGuard agent installed on the client PC in addition to the VPN Client software.

Design recommendation: All remote access users must be running the minimal set of host security software and operating system patches. Antivirus and personal firewall software are a must. Use TunnelGuard to enforce remote system endpoint compliance prior to network admission.

4.2.1.4 Audit and accounting

Use network-based logging of user and administrative actions to:

Provide an authoritative audit trail of administrative access and all configuration changes

Provide a record of all successful and failed user access attempts

Provide a record of all sessions, including start/stop times

Provide a record of all access attempts that violate access controls; for example, attempts to access applications or network resources that a user is not authorized to access

4.2.1.4.1 Logs

The primary network-based logging mechanism is syslog. In general, all authentication requests and resulting actions should be logged to a network-based syslog server. For troubleshooting purposes, the VPN Gateway supports a traffic log facility that can log all web-based access to URLs and file shares. The traffic log logs all access requests, not just access violations. This facility can generate a large amount of log information and reduce system capacity, so use it only as needed or when strict access logging is required.

See Appendix C of the *VPN Gateway User's Guide* for a complete list of supported syslog messages.

For more information on syslog and traffic log, see the “Syslog and Traffic Log” Technical Tip at the Nortel customer support portal (www.nortel.com/cs) in the VPN Gateway 3050 documentation area.

4.2.1.4.2 Accounting

The supported accounting mechanism is RADIUS accounting. Start and stop records are recorded for each user session.

4.2.1.5 VPN Gateway clustering

The Nortel VPN Gateway provides built-in support for clustering multiple Gateways. Up to 255 devices can participate in a cluster. The benefits of clustering include:

Higher availability (active/active resiliency)

Higher scale (higher throughput, more concurrent user sessions)

Single system management (a cluster of Gateways is managed as a single system in terms of configuration and software management)

No requirement for load-balancing switches

Each Gateway in a cluster hosts a unique VIP address for each VPN domain configured. You can use round robin DNS to distribute clients across the cluster members. If a cluster member fails, the VIP addresses associated with the failed unit are migrated to a healthy unit and continue to operate. This provides a simple and effective way to scale the solution and avoids typical issues with round robin DNS strategies, such as directing users to failed gateways, as all DNS entries resolve to an in-service gateway unless *all* gateways are unavailable.

4.2.1.6 Application Switch load-balancing

For higher-scale resiliency, you can integrate the VPN Gateway with the Nortel Application Switch portfolio to actively load-balance requests. This provides a solution with a single VIP per VPN domain, intelligent user load-balancing, and advanced service health-checking to direct traffic to available gateways.

Figure 3 on page 19 depicts such an active/active high-availability (HA) topology utilizing dual Nortel Application Switch 3408 switches to provide a highly scalable solution with no single point of failure. Such a solution can easily scale to 50,000 or more active users. Note that all VPN Gateways are active and use backup network connections to the non-primary Application Switch. These connections are not shown in the diagram but ensure that even in the case of a switch failure, all VPN Gateways have network connectivity and remain operational.

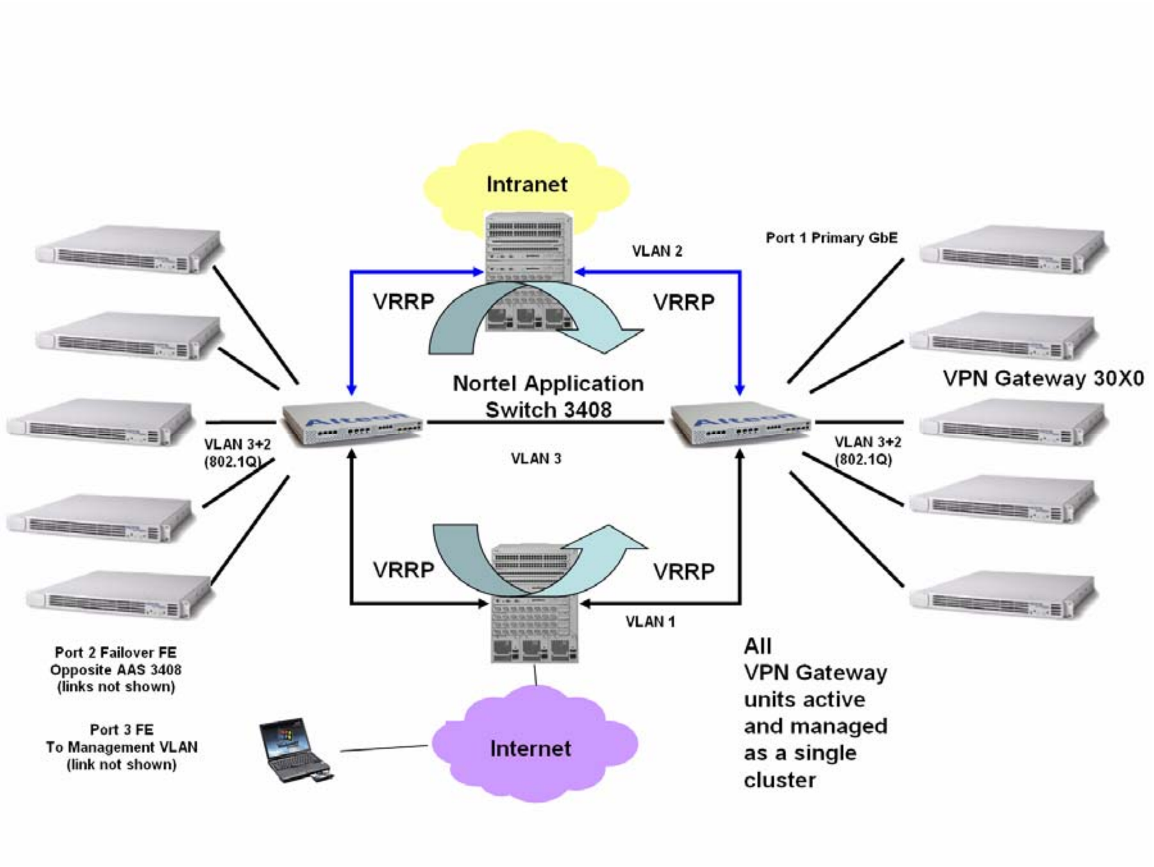
Intranet
VLAN 2
Port 1 Primary GbE
VRRP
VRRP
Nortel Application Switch 3408
VPN Gateway 30X0
VLAN 3+2 (802.1Q)
VLAN 3
VLAN 3+2 (802.1Q)
VRRP
VRRP
VLAN 1
Port 2 Failover FE Opposite AAS 3408 (links not shown)
Port 3 FE To Management VLAN (link not shown)
Internet
All VPN Gateway units active and managed as a single cluster

Figure 3: Active/active HA solution

See the *VPN Gateway BBI Application Guide* or *CLI Application Guide* for configuration information about DNS round robin integration, clustering, and Nortel Application Switch integration.

Design recommendation: For remote access environments with large numbers of users, high traffic volumes, or those that support critical applications, employ an active/active topology, including VPN Gateway clustering and dual Application Switches. When designing highly resilient VPN solutions, the network infrastructure, including DNS and AAA services, must also be designed using high-availability architectures.

4.2.2 Application access

4.2.2.1 Clientless Mode

When possible, use Clientless Mode for providing application access. Clientless Mode is simple and provides a high degree of access control, down to the individual file-share directory and web URL path level. Clientless Mode can also provide application-level auditing and logging of every object requested, if such detail is needed.

Clientless Mode requires web-based applications (examples include Microsoft Outlook Web Access and Lotus iNotes). Many enterprise-class applications have web front ends or interface options.

Another benefit of Clientless Mode is that it supports a wide range of client platforms and has minimal dependencies, as no additional ActiveX or Java applets are required.

Design recommendation: When possible, use Clientless Mode for application access.

4.2.2.2 Enhanced Clientless Mode for client/server

Enhanced Clientless Mode uses Java applets to enable client/server communication. These applets are automatically launched by preconfigured portal links on the SSL-VPN. The following enhanced clientless features are provided:

4.2.2.2.1 Port forwarder

The port-forwarder applet can redirect UDP/TCP client connections through an encrypted tunnel to the VPN Gateway, where they are then proxied to the actual application server. Multiple ports can be forwarded at the same time, and no client reconfiguration is necessary as the client name resolution mechanisms are used to direct the client application to resolve a local address for the application server hostname. Furthermore, the port-forwarder applet can automatically launch the required client application when the port forwarder applet is initialized. This function can be used to launch a native e-mail client, such as Outlook.

Several predefined link types are available for applications, including Windows Terminal Services, Microsoft Outlook, Windows Drive Mapping, and SMTP/POP/IMAP-based e-mail clients. You can define custom port-forwarder links for additional application support.

4.2.2.2.2 Citrix applet

You can enable the Citrix support applet in the SSL-VPN portal to provide seamless support for secure Citrix application delivery. This applet supports all Citrix client types, including Java, ActiveX (Web Client), and Program Neighborhood, and provides the following benefits:

No changes required on Citrix Server

No per-server configuration required on VPN portal

Supports complex environments, including large Citrix Server Farms

Support for NFuse and web interface web application portals, including single sign-on from VPN logon to application access

4.2.2.2.3 Terminal applet

The terminal applet provides a built-in Java terminal emulator that supports connecting to hosts through telnet and Secure Shell (SSH).

4.2.2.2.4 HTTP proxy applet

In some cases, complex web applications cannot be supported directly by the HTML/JavaScript rewriter in the SSL-VPN portal. In those cases, you can use an HTTP proxy applet to allow the web browser to connect to a Java-based proxy, which tunnels all requests to the VPN Gateway and bypasses HTML/JavaScript rewriting.

4.2.2.3 NetDirect

NetDirect is the required SSL-VPN mode for supporting complex applications such as IP Telephony. The NetDirect client can be launched automatically when the portal is displayed, or it can be manually launched by the user. If VoIP applications are used only occasionally, Nortel recommends that you allow the user to launch NetDirect only when needed.

4.2.2.3.1 Split tunneling

The split tunneling feature for IPsec and NetDirect access modes allows only intranet traffic to use the VPN and Internet traffic to be forwarded directly without forwarding through the VPN Gateway. As a general recommendation, disable split tunneling to reduce the risk of compromised remote access clients allowing unauthorized access to the intranet. If an IP Phone is controlled by the MCS Client as part of a home office or small office configuration, you can use inverse split tunneling to direct all traffic through the VPN Gateway, except a specified local subnet used for IP communication between the MCS Client and the IP Phone.

4.2.3 IP Telephony and multimedia

4.2.3.1 Considerations for IP Telephony

No configuration or software changes are required on IP Telephony or multimedia platforms to support remote access clients. The remote clients connecting through IPsec or NetDirect appear as standard IP soft clients connecting through the pool address ranges.

Ideally, keep the Communication Servers relatively close to the VPN Gateway within the network. For example, if you have a large network spanning a continent, collocating the VPN Gateway with the Communication Servers reduces the latency for VoIP traffic and avoids longer round trips, which can impact voice quality.

4.2.3.2 VPN Router 200 Series and small office/home office (SOHO) IP set solution

The VPN Router 221 and 251 models provide a solution for environments such as small offices and home offices where there is a need for continuous access to the enterprise network and a requirement to support IP Phones. This solution, as depicted in Figure 4, supports PC and IP Phone access, and there is no PC requirement for the operation of the IP Phone. Multiple IP Phones can be supported behind a single DSL or Cable Modem broadband connection, and full connectivity to the VoIP and data infrastructure is provided. This solution is currently compatible with the Nortel Communication Server 1000 Release 4.0.

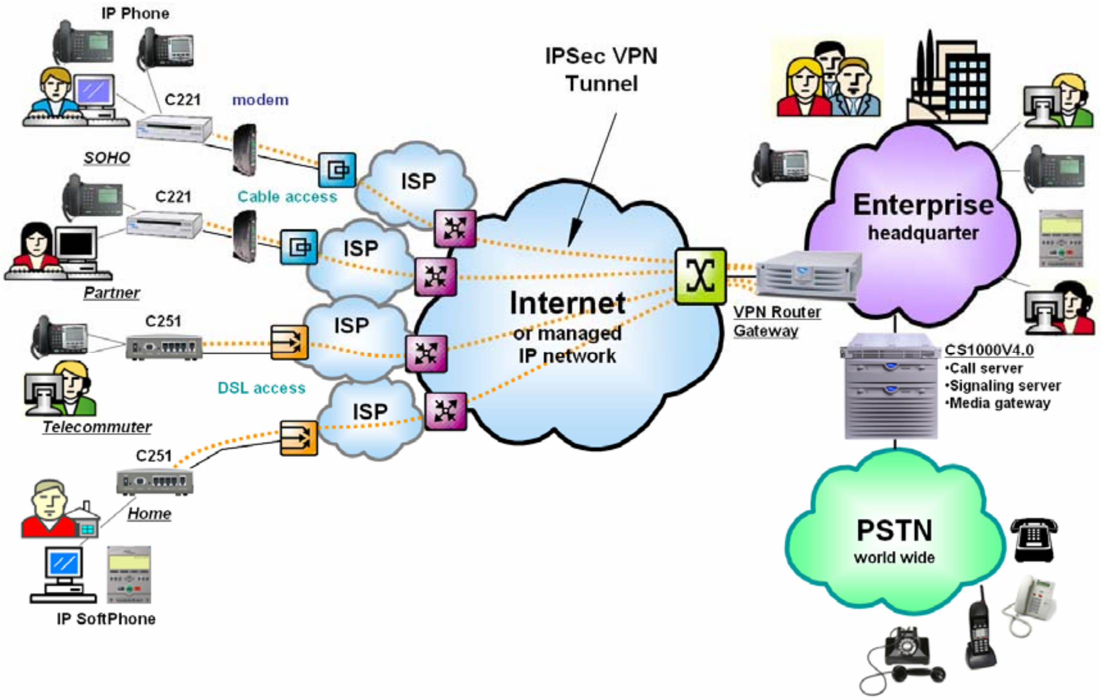

Figure 4: Small office/home office VPN Router 221/251 solution

For complete information about this solution, see the *CS 1000-C200 VoIP Solution and Configuration Guide* in the VPN Router 200 Series section of the Nortel customer support portal at www.nortel.com/cs.

4.2.4 Network management

The primary element management solution for the VPN Gateway is the browser based interface (BBI) or command line interface (CLI). Both support secure encrypted connections through HTTPS or SSH, and these should be used instead of clear-text protocols. To provide accurate administrative access control and auditing, use a network-based authentication system such as RADIUS for administrative access rather than local administrative accounts. Configure an administrative Access Control List to limit which hosts and subnets can connect to the management interfaces. When possible, employ a separate management VLAN and interface. Use SNMPv3 for network-based performance management and fault reporting.

As with all network security products, follow a process to track software patches and upgrades. The Nortel support portal at www.nortel.com/cs provides a My Alerts feature for timely information about patches and updates.

4.2.5 Converged applications and clients

The Secure Remote Access Solution described and detailed in the preceding sections provides the infrastructure for the media-rich clients. The infrastructure is a means, and the applications and clients are the end. The ability to provide a secure, resilient, and high performing infrastructure is key to enhancing productivity and the end-user experience. As applications and services converge onto a single infrastructure, it is critical to ensure resiliency and quality of service from end to end – the network is now mission critical to the enterprise.

There are many clients and applications that can now take advantage of the Secure Remote Access Solution. These include:

- IP Telephony
- IP Softphone 2050
- IP Phones (see SOHO solution is section 4.2.3.2)
- Multimedia Communication Server (MCS)
- Unified Messaging, including Nortel CallPilot

The following sections provide a brief overview of the solutions available.

4.2.5.1 Small IP Telephony platforms – Business Communications Manager

The Nortel Business Communications Manager 50/200/400 is an integrated communications platform for both multisite enterprises and single-site small to medium businesses. Each delivers a highly reliable, innovative, converged voice/data solution that enables a business to save money by streamlining costs, and to make money by increasing revenues, expanding market reach, and improving customer service. The BCM delivers PBX functionality along with no-compromise voice mail and auto attendant features. Combined with its robust quality of service (QoS) routing capability, it provides a single cost-effective solution for both data and voice needs. As businesses grow, the BCM functionality can be extended with a simple key code to deliver business-critical applications that positively impact the bottom line. The BCM provides enterprise-level telephony and data services, all in an easily managed platform. From one platform, a business can cost-effectively extend its communication capabilities. The Nortel Business Communications Manager system's built-in routing capabilities and data services such as firewall, web caching, and network address translation (NAT) enable a business to connect its LAN to the Internet quickly, reliably, and securely. The Nortel Business Communications Manager also offers an extensive range of communications applications – call center, unified messaging, VPN, auto attendant, wireless telephony – all accessed by simply entering a key code.

Nortel BCM 50

Nortel BCM 200

Nortel BCM 400

The top differentiators of the BCM 50/200/400 include:

- Comprehensive solutions that are easily implemented
- Choice of either IP-enabled or pure IP solutions
- Investment protection, because businesses may migrate without investing in completely new infrastructures
- The delivery of value-added applications, such as multimedia call center, IP Telephony, voice and data networking, Virtual Private Networks (VPN), unified messaging, and mobility
- Redundancy options, including power, fans, and hard drive, which automatically detect failures and switch over seamlessly without any loss of service

4.2.5.2 Enterprise IP Telephony platforms

The Nortel Enterprise IP Telephony offering is comprised of the Nortel Communication Server (CS) 1000 portfolio of fully featured IP-distributed communications systems that deliver the benefits of network convergence along with collaborative communications for today's increasingly "virtual" enterprise environment. The Communication Server 1000 portfolio includes the CS 1000S, 1000M and 1000E platforms, along with a variety of IP Communications Gateways and IP Remote Gateways. The innovative Nortel Remote Gateway Portfolio allows the enterprise to extend communications services to teleworkers and branch offices. With the wide variety of solutions, customers can choose the solution that best fits their needs based on branch office size, feature requirements, environment, and budget.

The Communication Server 1000 platform operates on Nortel CS 1000 Software. It offers a robust set of telephony features coupled with new SIP-based functionality that provides a fully integrated multimedia solution. System administration is performed using Optivity Telephony Manager along with Element Managers.

- Nortel Communication Server 1000 portfolio
  - Communication Server 1000 Software
  - Communication Server 1000S
  - Communication Server 1000E
  - Communication Server 1000M Chassis/1000M Cabinet/1000M Single-Group (SG)/1000M Multi-Group (MG)
- CS 1000 Element Manager
- Nortel Media Gateway 1000 portfolio
  - Media Gateway 1000S
  - Media Gateway 1000E
  - Media Gateway 1000T

- Nortel Remote Media Gateway portfolio
    - Media Gateway 1000B
    - Survivable Remote Gateway portfolio
    - Survivable Remote Gateway 50 (built on BCM 50 platform)
    - Survivable Remote Gateway 1.0 (built on BCM 200 and BCM 400 platforms)
    - Remote Gateway 9100 Series
    - Remote Gateway 9115
    - Remote Gateway 9150
- Nortel Optivity Telephony Manager (OTM)

4.2.5.2.1 Nortel Communication Server 1000

The Nortel Communication Server 1000 portfolio is an Enterprise IP Telephony solution supporting a flexible mix of phones, applications and PSTN gateways connected over a converged network. Telephones supported include IP Phones, digital TDM phones, analog TDM phones, DECT cordless and 802.11 wireless LAN phones, as well as software phones on PCs and PDAs. The Communication Server 1000 contains all the business telephony features and services developed for the market leading Nortel Meridian 1 PBX, plus new innovative features for IP convergence. It supports business applications for personal productivity, team productivity, mobility, customer service and management control. The Communication Server 1000 also provides advanced networking services to other Nortel and non-Nortel equipment using industry standards to protect customer investments and to keep total cost of ownership among the lowest in the industry.

Key areas of the Communication 1000 portfolio include:

- Distributed architecture over converged network
- Software built upon the highly reliable, feature-rich Meridian PBX feature set
- Full application portfolio support – Nortel and Developer Partner Program compatible applications
- Multiple built-in reliability mechanisms – no single point of failure, robust operating systems per call server (100 000 in a centrally managed network)
- Highly scalable – from 1000 to 15 000 IP clients per call server (100,000 in a centrally managed network)
- Centralized management control and dialing plan for 100 000 IP clients
- Centralized and networked business communication services
- IP telephony service overlay that works on any open standards-based data network
- Optional support for campus and geographic redundancy with CS 1000E

4.2.5.2.1.1 Nortel Communication Server 1000S

The Communication Server 1000S is a fully distributed IP Telephony solution with all of the features and capabilities of a PBX, designed primarily to support Nortel IP Phones, but with support for analog and digital phones as well.

- Scalable – supporting up to 1000 IP clients per call server
- Distributed Call Server and Gateways

- Redundant Gatekeepers, Gateways and Client Proxies
- WAN Gateway survivability
- Uses Media Gateway 1000S (up to four per system) to provide local access to TDM devices such as RAN/Music, Conference/Tones, analog/digital lines and analog/digital trunks.
- Seamless network integration, simplified management, greater flexibility in deployment, and reduced support costs

4.2.5.2.1.2 Nortel Communication Server 1000E

For enterprises that want to deploy a full IP PBX architecture supporting a large number of users, the Communication Server 1000E can be deployed either at a single location or distributed throughout a QoS managed IP network. The Communication Server 1000E introduces a redundant call processor configuration.

- Scalable – supporting up to 15 000 IP clients per Call Server
- Redundant Call Servers, Gatekeepers, Gateways and Client Proxies
- Campus mirroring – known as split core, allows active and inactive Call Servers of the system to be physically separated up to 25 miles (40 km) across a campus using a high-speed link
- Geographic redundancy – allows for a redundant CS 1000 system to be deployed at a remote location over any distance through the WAN to take over call processing if the primary system fails or is the subject of a major disaster
- Uses Media Gateway 1000E (up to 30 per system) to provide local access to TDM devices, to support Analog/Digital lines and to support Analog Trunks
- Uses Media Gateway 1000T to provide digital trunk PSTN access

4.2.5.2.1.3 Nortel Communication Server 1000M

The Communication Server 1000M transforms a Nortel Meridian 1 PBX into an IP PBX. Equipped with Signaling Servers and running on Communication Server 1000 software, the Communication Server 1000M functionally is no different than that of a CS 1000S/E. It is available in the following configurations:

- Communication Server 1000M – Cabinet/Chassis (11C Cabinet/Chassis)
- Communication Server 1000M – Half-Group (51C)
- Communication Server 1000M – Single Group (61C)
- Communication Server 1000M – Multi-Group (81C)

The Communication Server 1000M supports:

- Scalable up to 15 000 IP clients per call server and 16 000 digital or analog clients
- Redundant Centralized Call Processor and Gateways
- Distributed Remote Gateways • Integrated Media Gateways for trunk and line application interfaces
- Provides investment protection and allows for migration to IP Telephony

4.2.5.2.2 Nortel Communication Server 1000 Element Management

CS 1000 Series system management is performed using the Nortel Optivity Telephony Manager along with Element Manager. Element Manager is a simple, user-friendly web-based interface that supports a broad range of system management tasks, including:

- Configuration and maintenance of IP Peer and IP Telephony features
- Configuration and maintenance of traditional routes and trunks
- Configuration and maintenance of numbering plans
- Configuration of Call Server data blocks
- Maintenance commands, system status inquiries, backup and restore functions
- Software download, patch download and activation

Element Manager resides on the Signaling Server and can be accessed directly through a web browser or through Optivity Telephony Manager. The Optivity Telephony Manager System Navigator includes integrated links to each network system and its respective instances of Element Manager.

4.2.5.2.3 Nortel Media Gateway 1000

Distributed throughout the IP network, Nortel Media Gateway 1000 acts as a bridge between IP and traditional telephony networks (such as the PSTN) by housing various cards that perform line, trunk, and translation functions. The hardware for the entire Media Gateway 1000 portfolio has the same characteristics: four slots that can be used for media cards, analog and digital line cards, analog and digital trunk cards as well as various applications.

4.2.5.2.3.1 Nortel Media Gateway 1000S

The Media Gateway 1000S is used with the Communication Server 1000S to support PSTN trunks, analog/digital telephone resources, TDM application cards and Voice Gateway Media Cards. Each Media Gateway can support one Media Gateway Expander. The Media Gateway 1000S contains a gateway controller card (called SSC card) and four slots for flexible configurations of line, trunk, and application cards. The SSC card controls the interface and application cards and acts as a call processor in the survivable mode. The Call Server database is automatically synchronized onto this controller. Application cards provide interfaces to applications like CallPilot and Nortel Integrated Applications portfolio.

4.2.5.2.3.2 Nortel Media Gateway 1000E

The Media Gateway 1000E is used with the Communication Server 1000E to provide basic telephony media services – including tone detection and generation and conference – to phones. It operates under direct control of the Call Server and can support an optional Media Gateway 1000E Expander. The Media Gateway 1000E contains a gateway controller card (called SSC card) and four slots for IPE cards and Voice Gateway Media Cards. The Media Gateway 1000E supports CallPilot and Nortel Integrated applications. It also provides direct physical connections for digital and analog (500/2500-type) telephones as well as analog trunks for telephone and fax.

4.2.5.2.3.3 Nortel Media Gateway 1000T

The Media Gateway 1000T provides the Communication Servers 1000E/S with digital trunk and PRI access to the PSTN and to other PBX systems. The Media Gateway 1000T contains a gateway controller card (called SSC card) and four slots for IPE cards. It also supports an optional MG 1000T Expander. Unlike the MG 1000Es, the MG 1000T platform does not operate under the direct control of the CS 1000E Core Call Servers. Instead, the MG 1000T provides the primary processing for the MG 1000T platform. The MG 1000T Core SSC card controls the circuit cards in the MG 1000T Core and all cards in up to four MG 1000T Expansions. The MG 1000T supports Media Cards, Digital PSTN Interface Cards (E1, T1, ISDN), Analog Trunk Cards, Service Cards and DECT Mobility Cards.

4.2.5.2.4 Nortel Remote Gateway

Nortel offers a wide variety of remote gateway solutions that extend enterprise communications to teleworkers and remote offices. With Nortel Remote Gateway 9100 Series, the enterprise can extend 450-plus features and system resources to those working away from the main office, while leveraging the investment of a central corporate PBX. Using the Nortel Survivable Remote Gateways (Release 1.0) and Survivable Remote Gateway 50, an enterprise under network failure conditions has continued telephone services in a cost-effective manner for IP clients at even the smallest remote sites. Using Nortel Media Gateway 1000B, up to 400 users can be distributed across an IP WAN in a survivable environment that supports the same analog and digital line and trunk cards and phones as that of the main site.

4.2.5.2.4.1 Nortel Media Gateway 1000B

The Media Gateway 1000B allows larger groups of users to be distributed across an IP WAN to branch office sites with seamless feature and application transparency with a Communication Server 1000 at the main site. It supports up to 400 IP users and provides access to an array of PSTN trunk types as well as line interfaces located at the branch office. IP Phones at the branch office are managed from the main site. The survivability feature allows IP Phones that are centrally managed from the main site to fail over to survival mode, retaining all available features. Survival mode engages automatically if the IP WAN fails and reverts back when the IP WAN resumes normal operation.

4.2.5.2.4.2 Nortel Survivable Remote Gateway

The Nortel Survivable Remote Gateway (SRG) 1.0 (BCM 200) and SRG 1.0 (BCM 400) seamlessly extend the services and applications of a Nortel Communication Server 1000 Series system at a headquarters site to the smallest remote sites. In addition to the SRG 1.0 (BCM 200) and the SRG 1.0 (BCM 400), there is a mini model for the smaller branch office, known as the Nortel Survivable Remote Gateway (SRG) 50. Introduced with Communication Server 1000 Software Release 4.5, it is cost optimized for sites ranging from between 5 and 32 users.

While the Nortel SRG 1.0 platform is based on the market-leading small site IP Telephony solution and Nortel Business Communications Manager 200 and 400, the Nortel Survivable Remote Gateway 50 is based on the BCM 50. The SRG series has been designed to provide continued telephony services for IP clients under network failure conditions – and to do so in a very cost-effective manner at smaller locations.

The SRG portfolio is not only cost effective at smaller sites, but also provides highly reliable solutions that include the intelligence to drive Nortel IP terminals while providing IP routing capabilities and a suite of PSTN interfaces to enable local PSTN access. It is capable of addressing the needs of smaller branch offices ranging in size from 5 to up to 80 users.

4.2.5.2.4.3 Nortel Remote Gateway 9100 series

The award-winning Nortel Remote Gateway 9100 Series provides an ideal solution for extending cost-effective, high-quality communications to teleworkers and remote offices. The Nortel Remote Gateway 9115 extends the features and functions of a Nortel Meridian 1 PBX, Meridian SL-100, or Communication Server 1000 (CS 1000) system out to a single telephone at a small remote office or telecommuter home office, utilizing a standard IP-based network connection and an analog PSTN telephone line and a Nortel Meridian digital telephone. The Nortel Remote Gateway 9150 is a powerful option for extending these features and functions to remote branch offices using up to 32 Nortel Meridian digital telephones and a standard IP-based connection and PSTN circuit-switched telephone lines. With each Nortel Remote Gateway solution, the remote workers have full access to the corporate telephone network just as if working at the main corporate site. All of the 450-plus features and system resources enjoyed in the main office are available remotely, such as unified messaging, the corporate directory and corporate dialing plans, as well as features such as boss-secretary filtering, audio conferencing and automatic call distribution.

The Remote Gateway Series 9100 products are configured and maintained using the Remote Gateway 9100 Series Configuration Manager software, a Windows™-based application that is installed on a PC. It provides a simple Configuration Wizard for initial installation that prompts the user through obtaining the minimum information needed to get the remote site communicating with the main site.

4.2.5.3 IP Phones/IP Softphone 2050/Mobile Voice Client 2050

Nortel IP Phones are the portals to application access, supporting a comprehensive suite of telephony features from Nortel Communication Servers and application presentation for information exchange from network-based application gateways. Serving the needs of organizations of all sizes – from those with users who have basic communications requirements to those whose needs span high call volumes, multimedia presentation and mobility, Nortel has solutions for every worker. Nortel offers desktop solutions for the campus-based worker who prefers physical phone presence at the desktop along with a variety of wireless and soft-client solutions offering whenever and wherever real-time communications access for workers who are constantly on the go. With Nortel IP Telephony Clients, customers benefit from the latest in telecommunications technology while leveraging the reliability, quality, and cost effectiveness only Nortel can deliver.

4.2.5.3.1 Nortel IP Softphone 2050

The Nortel IP Softphone 2050 provides access to the same services and capabilities as the Nortel IP Phones 2002 and 2004, but it uses the computer and audio resources of a standard PC or laptop. Supported by Nortel Business Communications Manager 50/200/400, Nortel Communication Server 1000, and hybrid Nortel Meridian 1 systems, the Nortel IP Softphone 2050 supports the following features:

- Easily twinned with any other set that the user may have in the office, providing a choice of how users answer or make calls
- Three slide-out feature trays (line/feature keys, dialpad or combination)
- Supports five special-purpose service keys and four interactive keys
- Message waiting indicator alerts users to new voice messages and incoming calls
- Supports direct headset connection through a PC USB port
- Enhanced USB Audio Kit provides a telephony optimized sound card to ensure superior audio quality
- Supports local directory imports. Reads Symantec ACT, Microsoft Outlook, and LDAP databases for seamless directory integration
- TAPI compliance for operation with other telephony applications

4.2.5.4 Multimedia Communication Server 5100

The Nortel Multimedia Communication Server (MCS) 5100 is the Nortel enterprise multimedia applications solution, providing innovative communications, real-time collaboration and productivity services for enterprise users. Nortel MCS 5100 uses open, industry standard hardware to evolve TDM as well as IP networks to highly collaborative, multimedia networks.

Nortel MCS 5100 is seamlessly deployed alongside an enterprise's current network infrastructure, enriching the enterprise user's communications experience and providing new SIP multimedia applications.

The Nortel MCS 5100 supports an impressive suite of integrated multimedia capabilities that allow users to enjoy a feature-rich multimedia experience. The following summarizes the key capabilities:

- Desktop video calling is delivered through coordinated video display on the PC screen and audio conversation through the hard or soft client. Low-cost desktop multipoint video conferencing extends video to all users.
- Presence – Notification is provided on the status of a watched user. When a user is on the phone, dynamic presence shows the person as on the phone, and when a user is away from their desk, the presence changes to inactive.
- Picture calling line ID – Incoming and outgoing communications present a picture of the originating caller on the PC screen along with CLID.
- Personal agent–Call screening – This user friendly html (web) interface provides a Find me/Follow me service, with call screening provisioning for communication personalization. Users define who, where, when, and how callers can reach them. Calls can be screened and routed based on who is calling (or groups), or on when calls are received (time of day, day of week). Calls can be directed to try multiple locations at once (office, cell phone and house), or to ring sequentially one after the other, or a combination. This solution set provides tremendous flexibility and control of the communication experience.
- Network-based incoming and outgoing call logs are kept for easy access and retrieval.
- Directory – Includes personal and global directories so that users can store information and use the directories for click-to-call capability.
- Click to Call – From the directory on the multimedia PC client, from the incoming/outgoing call logs, or from the Outlook contact or inbox.
- Mobility solution – The multimedia PC client can provide the primary voice service for users who are not in their office, or those who do not leverage existing voice infrastructures.
- Conferencing – Meet-me media conferencing delivers multimedia services such as visual notification to the conference chair of all participants entering or leaving the conference. Conferencing also supports file exchange, web push and cobrowse, and allows instant message chat for sidebar real-time communications. This solution set delivers a very impressive return on investment (ROI) over outsourced conference solutions, as well as improved functionality.
- Collaborative applications – The Nortel MCS 5100 provides a suite of applications such as instant messaging, web collaboration, IM Chat, file sharing, white boarding and web pushing. Video conferencing is another key application in today's collaborative environments, improving the effectiveness of distance conferencing.
- PDA support – Many MCS 5100 applications are supported on PDA devices such as the RIM Blackberry giving users extended use of presence, secure instant messaging, Click to Call and route management.

4.2.5.4.1 Nortel Multimedia Clients

Now you can talk, send instant messages, send and receive video, share text and images, and collaborate in real time, using a single Internet connection

from your PC and the Nortel Multimedia Clients. The Multimedia Client applications provide a wealth of powerful communications features, from traditional telephone service to advanced multimedia communications such as video calling, instant messaging, call screening, real-time call disposition, conferencing, file sharing, and white boarding. Advanced web communications include web collaboration, pushing web pages and cobrowsing the web with customers, coworkers, and associates.

The Multimedia Clients can be used to control communications over a PC headset or over the Nortel IP Phone 2004 or 2002, while becoming more productive and efficient and gaining greater control over daily communications. You can efficiently perform diverse communications tasks in a single session, bring the human touch of face-to-face contact to remote communications, and manage incoming and outgoing communications in new ways.

4.2.5.5 Unified Messaging

Nortel messaging solutions incorporate the latest technology and add web-based graphical user interfaces to bring feature-rich communications to the desktop or mobile device while making message management easy and effective. For any size enterprise, the Nortel Messaging portfolio of products provides unified, personalized messaging to both office and mobile or remote workers.

4.2.5.5.1 Nortel CallPilot

CallPilot is a unified messaging tool that brings together voice mail, e-mail, and fax to create a personalized, feature-rich communications and message management system. CallPilot incorporates the latest technology, including advanced speech activated messaging and email-by-phone, which enables access to messages using telephone user interface (TUI) through either voice commands or dual tone multi frequency (DTMF) tones from virtually anywhere. CallPilot builds on the customer-driven functionality of proven Nortel messaging products and adds web-based graphical user interfaces (GUI) to make system management easy and effective.

The CallPilot portfolio includes CallPilot 100/150 (current Software Release 3.5) for the Nortel Norstar Integrated Communications System, CallPilot Unified Messaging (current Software Release 3.0) for the Nortel Communication Server 1000 Series, and CallPilot as an integrated version for Business Communications Manager 50/200/400.

4.2.5.5.2 Nortel Hospitality Messaging Server 400

The Hospitality Messaging Server 400 (HMS 400) replaces the Meridian Mail HVS as the messaging solution for the hospitality industry. It is a global product with multilanguage support. The HMS 400 platform provides ample resources to add additional feature/capabilities in the future. It is scalable up to 7000 users with the choice of single server or multiserver configurations.

4.2.5.6 Wireless VoIP

Nortel WLAN Handsets 2210, 2211 and 2212 are mobile phones for workplaces with Nortel Communication Servers. Nortel WLAN Handsets reside on the wireless LAN with other wireless devices using direct sequence spread spectrum (DSSS) radio technology. They operate over an 802.11b wireless Ethernet LAN providing users a wireless voice over IP (VoIP) telephony extension, sending and receiving packets at up to 11 Mbps. Quality of service on the wireless LAN for IP Telephony is provided through the WLAN Telephony Manager 2245. The WLAN Application Gateway 2246 is an open application interface (OAI) that enables third-party software applications to communicate with the Nortel WLAN handsets. By seamlessly integrating with the infrastructure IP Telephony system, wireless telephone users are provided with high-quality mobile voice communications throughout the workplace. The wireless telephone gives users the freedom to roam throughout the workplace while providing all the features and functionality of an

IP desk phone. The Nortel WLAN IP Telephony Handset is one of the components of the Nortel WLAN IP Telephony Solution.

Refer to the Voice over Wireless LAN Technical Solution Guide for a detailed overview of the entire wireless LAN solution.

5. Secure Remote Access Solution summary

The Secure Remote Access Solution presented in this guide shows the components, features, and functionality available when implementing a Nortel solution. Nortel is uniquely positioned to provide a secure, resilient infrastructure capable of supporting a wide range of converged applications including data, multimedia, and voice applications. By taking a solutions approach to remote access to applications including IP Telephony and Multimedia, this guide highlights the best practices and puts forth design recommendations when implementing an end-to-end solution.

5.1 Performance and scalability

The performance and scalability of the Secure Remote Access Solution is a major competitive differentiator for Nortel. Several third-party test results were published, along with internal testing on the various components within the solution.

Tolly Nortel VPN Gateway 3070 SSL VPN Throughput, Scalability and Voice Quality Benchmark Evaluation: http://www.tolly.com/DocDetail.aspx?DocNumber=205113

Tolly White Paper – Building a World-Class VPN Solution to Meet Today's Needs—and Tomorrow's: http://www.tolly.com/DocDetail.aspx?DocNumber=205103

5.2 Interoperability with other products

The VPN Consortium has tested the Nortel VPN Gateway portfolio for a number of interoperability scenarios. More information is available at:

http://www.vpnc.org/testing.html

5.3 Security certifications

The Nortel VPN Gateway and VPN Router products have achieved ICSA certification. For more information, see:

VPN Gateway: https://newlabs.icsalabs.com/icsa/topic.php?tid=9379$9a95ffdd-2cb3ae1e$7a80-854ffdda

VPN Router: https://newlabs.icsalabs.com/icsa/product.php?tid=428c$4e933c47-c58cef17$5298-2f493ab2

Contact us

For product support and sales information, visit the Nortel web site at:

www.nortel.com

In North America, dial toll-free 1-800-4Nortel, outside North America dial 987-288-3700.