Business Communications Manager (BCM)

BCM 3.6 Security Guide

Issue 1.2
09 June 2004

Table of Contents

1 Purpose and Audience

The importance of security continues to grow as the number of cyber-attacks increases year-to-year resulting in greater disruptions and potential revenue loss. Security issues need to be treated seriously and dealt with appropriately. A comprehensive end-to-end network security solution is required to address this growing threat.

This document provides an overview of security considerations, features and solutions for the BCM 3.6 release. The goal is to equip Nortel Networks partners, lead customers, Sales and System Engineers with the information required to answer questions regarding data network and system security.

Security can be viewed from two perspectives: the security services offered by the platform, and the security of the platform itself. In the case of the former, what services does the platform offer to help implement a secure data network? In the case of the latter, how difficult is it for someone to compromise the security of the platform itself and what has been done to harden the platform's security related settings? Both these areas are addressed in this security guide.

This document describes the BCM security services as well as the system security that is available in the BCM 3.6 GA release. It is not the intent of this document to provide an in-depth discussion of the various security-related topics introduced. The reference section provides some sources of additional information. This document is also not the primary configuration guide for the various BCM security services; please refer to the BCM configuration manuals for detailed instructions. The BCM configuration manuals contain security notes which are designated using a Padlock Icon. Each security note indicates a point of system security where a default configuration value should be changed or where the administrator needs to make a decision about the level of security required for their BCM platform. Additional security related information is also available through the context sensitive help in the OAM interface.

2 What is Security?

Security for servers and data networks means protecting information and information systems against manipulation, mistakes and destructive attacks. Security and risk management are interrelated. Risk management is used to determine what needs to be protected, how to safeguard it, and determine who is the threat. An assessment weighs the cost of protecting the information or system against the potential loss if security is compromised. IT Security has the following aspects, but not all of these need to be present for effective security. The appropriate strategy should consider the information and systems being protected, as well as the risk analysis. The remaining chapters in this document will present the capabilities available on the BCM to address these issues.

2.1 Physical Security

The physical security of an IT infrastructure is central to any security strategy. Someone with easy access to a server that contains protected information can compromise a system by disconnecting it or causing physical damage thus rendering it unusable. Large companies with servers and data networks have a secure server room, wiring closet or other either closed or restricted and monitored area to protect their infrastructure. This is the recommended placement location for the BCM.

One approach to mitigating the threat of physical security is to make a system “headless” by removing the keyboard, monitor and mouse. This configuration makes a physical security breach less likely in some situations. The BCM is a “headless” configuration that also does not include a floppy drive and a CD ROM drive minimizing the threat of foreign software executing on the platform.

2.2 Authentication, Authorization and Auditing

Authentication and authorization mechanisms are used to restrict access so that only authorized individuals can view or control certain information. Most servers and data networks have usernames and passwords that grant different levels of access to individuals. Resources have Access Control Lists (ACLs) assigned to them that grant access only to select individuals or groups and an audit trail can be used to record access attempts or changes made to the control settings. In the following chapters, solutions using user privilege settings, password protection and system hardening on the BCM will be presented to demonstrate authentication, authorization and auditing.

2.3 Data Integrity and Confidentiality

Data integrity means that the information being read has not been altered from its original form. Data integrity violations can be ‘in-place’, that is, the file or resource on the server is changed or replaced with a forgery or ‘in-transit’, while it is being sent across the network. To achieve data integrity, both in-place and in-transit data integrity must be addressed. Data confidentiality requires that the information sent across a data network is encrypted to prevent access of sensitive information. In the following chapters, solutions using SSL, SSH, VPN, encryption, password protection and system hardening on the BCM will be presented to demonstrate data integrity and confidentiality.

2.4 Data and Service Availability

Data availability denotes that data is present when it is required. Often it is easier for a malicious attacker to delete or refuse access to data than to alter or forge the data. The attacker can remove files from a local server, or breach a network and deny service by either blocking the information, or making the server unable to send it or respond to a valid service request. In the next chapters, solutions employing firewall configurations and system hardening on the BCM will demonstrate approaches to dealing with data availability and Denial of Service (DoS) threats.

3 BCM System Security – Secure right out of the box

The default BCM platform system security settings are set at a level which balances the need to adequately secure the BCM while maintaining compatibility with current supported client PC platforms and satisfying customer support needs. Some security settings are configurable in order to accommodate customer specific environments and needs for stronger or weaker security settings.

The list of Unified Manager configurable security settings in release 3.6 include:

- setting the authentication type,
- configuring lockout and password policy,
- enabling and disabling SSL web access,
- enabling and disabling modem access,
- configuring option to clear the page file on shutdown,
- setting SMB signing level for client and server,
- setting Domain Secure Channel signing and encryption options,
- setting web encryption level,
- configuring the dial back feature,
- uploading site specific SSL certificate

Unified Manager also allows you to view the list of applied Windows/NT hotfixes.

The BCM also provides security logging that captures an audit trail for login attempts, logoffs and changes such as policy settings.

Note that the default settings for the password length and complexity level on upgraded BCMs do not automatically get set to the BCM 3.6 configuration so that existing accounts and passwords on older releases can be preserved after the upgrade to release 3.6. See section 5.2.1 BCM 3.6 Upgrades - Password Policy Settings for further details.

3.1 Closed System

The BCM is a communications platform and a closed system that is tuned to the specific performance requirements of a converged communications server. Since no additional software is installed onto a BCM by an end user, it is ***protected from many common types of malware (viruses and Trojan horses)*** that embed themselves in the software that get installed on other open systems. The software that is shipped with the BCM has been pre-scanned for malware. **Note that the installation of any additional software onto the BCM violates the Nortel Networks support agreement and may adversely affect the functionality, security, and performance of the BCM.**

3.2 Passwords

All of the administration interfaces for the BCM are protected by a username and a password or PIN. Whether connecting locally through the serial port, or remotely through SSH, Telnet, Unified Manager or NCM, usernames and passwords are required to gain access to the system. Each logon attempt is recorded in the NT System event log. In the case of BCM client applications, a userid and password is required to logon or a PIN entry is needed for a telephony interface. It is critical that the ***BCM system administrator change each default password or PIN immediately after system initialization*** to ensure that public, documented userid/passwords and PINs cannot be used to access the BCM.

Some of the default passwords that should be changed include Unified Manager default administration accounts, PINs for the IP set, companion and DECT sets, Call Pilot administration, Telephony hospitality feature (desk and room condition passwords), call log and hunt group monitoring password, Call Centre administration, and the SNMP community string.

The BCM platform provides a configurable password policy and lockout mechanisms to assist the system administrator to enforce compliancy to the password settings and control unauthorized system logon attempts. The lockout mechanism is an effective mechanism against password cracking programs.

The password and account policy settings are configurable through the User Manager Interface in Unified Manager.

The BCM platform password policy settings control:

- Minimum Password Length -> 8 Characters (default) (range is 1-8 characters)
- Password complexity -> 3 different types of characters (default) (range 0-3 types); a character type can be a lower case, upper case, numeric or special character.

The BCM platform account lockout policy settings control:

- Lockout policy -> Enabled (default) (range enabled/disabled)
- Account lockout count -> 50 Invalid logon attempts (default) (range is 1-999 attempts)
- Lockout account for -> 30 Minutes (default) (range is 1-99999 minutes)
- Reset account lockout count after -> 30 Minutes (default) (range is 1-99999 minutes or -1 forever)

The NCM management application enforces password validation based on a password complexity of 3 and a password length of 8 characters for all the BCMs it manages, irrespective of software release or modified settings on any particular BCM.

If a VNC session is required for support personnel, not only is the logon password protected, but also VNC access is restricted until an access code is first obtained from Nortel Networks to enable VNC. The VNC access code is host specific and changes daily.

3.3 Authentication Protocols

A secure authentication protocol is required to validate a user's credentials during the logon process. The security of the protocol ensures that the authentication is not spoofed with forged data.

The system administrator can control the authentication protocol used on the BCM through a configuration option in the Unified Manager Security window. The lowest levels (level 0 and 1) maintain compatibility with Win9x (95/98/Me) client PCs allowing them to logon to the BCM. Level 1 is the default value but the authentication protocol level can be set more secure if Win9x compatibility is not required. LM authentication is weak, allowing an attacker to use readily available tools to try and crack passwords. NTLM is significantly better than LM and NTLMv2 provides further encryption strength and improved session security.

The BCM platform authentication protocol settings include:

- Level 0 - Send LM response and NTLM response; never use NTLMv2 session security
- Level 1 - Use NTLMv2 session security if negotiated or LM, NTLM (default)
- Level 2 - Send NTLM authentication only
- Level 3 - Send NTLMv2 authentication only
- Level 4 - DC refuses LM authentication, NTLMv2 response only

3.4 Account Privileges

The key to a secure system is ensuring that users have only the level of access required to perform their function. Every user does not require, nor should be granted full administrator access to the BCM. Access rights within Unified Manager and Win/NT are controlled through predefined account groups. ***The Unified Manager interface provides the ability to create user accounts with specific system access rights.*** A user account can be added into any of the default user groups or added into a new custom user group. Group membership provides read-only default access.

A user account can be configured to be a member of multiple user groups; as a result, the Unified Manager GUI access rights are incrementally added.

Dial-in access permission is controlled in Unified Manager through membership to the DialupUserGroup. To remove dial-in access permissions from a user account, the user must be removed from the DialupUserGroup in Unified Manager. Modem dial back access is also configured individually for each user account and provides important access security (see section 4.6 Modem Security).

Only administrator accounts have the ability to access the BCM through interactive logins. SSH and Telnet access through the network or through the serial console is restricted to user accounts that are members of the Administration group since this interface is used only for administration purposes.

3.5 File Privileges

To enhance the degree of security, the ***default permission on all files and folder on the Windows NT portion of the BCM have been replaced*** with more restrictive permissions intended to tighten overall system security. The access permissions to various registry entries have also been made more restrictive.

Drive shares have also been disabled by default since they pose a significant security concern. If drive shares need to be re-enabled for file access, they can be re-enabled through the Unified Manager Maintenance pages. It is advisable to disable them once the drive access is complete. The FTP server on the BCM is disabled by default and anonymous FTP access is not allowed. There is no TFTP server on the BCM in order to eliminate the associated potential vulnerabilities.

3.6 Windows NT Domain

The BCM can participate in a limited manner in a Windows domain. Although participation in a domain can be convenient from the point of view of user management and administration, such as for Call Detail Recording (CDR), it can also be a potential security problem. ***If a domain account elsewhere in the network becomes compromised, it can result in unauthorized access to the BCM***.

3.7 Dual-OS

The BCM platform utilizes two separate operating systems. A real-time embedded OS runs on the MSC (Multi-Services Card) and provides the call server features of the BCM. Another embedded OS runs on the motherboard and provides advanced IP telephony features, data routing, OAM and application support. ***The advantage of a dual-OS approach is that it provides a robust platform for call server features that can withstand attacks and security breaches on the motherboard platform***. In fact, all traditional TDM calling features except voicemail function normally as long as the MSC has power on it.

3.8 NT Embedded

Microsoft Windows NT Embedded OS is a version of the NT server OS that can be configured to remove unneeded services and features from the system. In contrast, the services and features of the regular NT server can generally be switched off but not completely removed. The BCM includes only the features and services required to deliver communication services. As a result, ***a number of unnecessary subsystems are not present on the BCM***, thus eliminating any potential security risk associated with them. Default security settings can be adjusted through Unified Manager.

3.9 Telephony Security

Securing the telephone system includes ensuring that:

- Valuable telephony resources are used for their intended purpose by authorized users
- Information is kept private

- Only authorized personnel can change the system programming

All of these security areas are addressed by the telephony security capabilities provided by the BCM.

3.9.1 Toll Fraud

Toll fraud is the theft of services (ToS) by a hacker gaining access to the system or by tricking authorized personnel into making calls, which results in the company being billed.

The BCM's Direct Inward System Access (DISA) is password protected and controlled by a Class of Service (COS) that restricts access to system features and outside lines.

Call Detail Recording (CDR) is a capability that can be enabled so that system administrators can keep track of the incoming and outgoing calls. By monitoring calling patterns, it is often possible to ***identify fraudulent use of toll services***.

Telephone sets communicate with the network using a set of DTMF tones to indicate the dialed digits. A hand-held DTMF generator can be used to bypass the normal dialing process and make unauthorized long distance telephone calls. To prevent this, ***the BCM has a Nortel Networks patented feature that can be set to block the voice path to the network until the dialing restrictions have been passed***. This prevents someone from dialing restricted numbers, and ensures that the administrator retains control over access to long distance facilities.

3.9.2 Controlling Access to Toll Calls

Sets and Lines in the BCM can have dialing restrictions that specify the numbers that can be dialed and the long distance charges that users can incur. Access to specific lines can be assigned on a per set basis or selected through the dialing plan to ensure the correct lines are used for toll calls. Restrictions can also be based on the time of day and day of the week.

The Class of Service (COS) defines which BCM features, lines, and dialing restrictions are available when a call is placed within the system or remotely. It can be associated with a line, a set, or a Class of Service password. The Class of Service password allows users to temporarily override the restrictions associated with a specific phone or line with a personal set of restrictions.

3.9.2.1 Transfers to external numbers

Call Pilot auto attendant (CCR) can transfer callers externally if configured to do so. This would allow external callers to potentially perform toll fraud if the Call Pilot application was mis-configured or maliciously configured. ***To address this threat, restrictions can be placed against the Call Center/Call Pilot DN's not allowing unauthorized phone numbers to be called from Call Pilot. Call Center routing should be checked and the default passwords for Call Pilot should be changed.***

3.9.2.2 Outdial type for mailboxes

Call Pilot mailboxes have the ability to outdial to external numbers for Off-premise Message Notification when messages are left or for outbound transfer from a mailbox. Both of these options allow the user to configure external phone numbers for the Call Pilot to dial and therefore are susceptible to toll fraud. ***To address this threat, the mailbox defaults are set to none for outdial and dialling restrictions can be applied. If the outdial type configuration is not set to None, be aware that there is potential for unauthorized long-distance dialling unless outdialing restrictions are used.***

3.9.2.3 Auto-Login for Voice Mail

The Auto-Login feature allows subscribers to bypass entering their mailbox number and password. Subscribers with Auto-Login can dial the Call Pilot Messaging access number or enter the feature code in order to immediately be logged on to their mailbox. With physical access to a phone set, an individual can gain unauthorized voicemail access by pushing the voice mail key. ***The Auto-Login feature should not***

be used in insecure environments. The Auto-Login feature is disabled by default and should remain disabled.

3.9.2.4 Call Center routing

Through Call Center, routing steps can be configured to transfer to external phone numbers for CLID/DNIS, Overflow, Caller Input, and standard day/night routing. If these numbers are mis-configured or maliciously configured an external caller could potentially perform toll fraud. ***To address this threat, the configuration of Call Center routing should be verified and the passwords for Call Pilot should be changed. Restrictions should also be placed against the Call Center/Call Pilot DN's to avoid toll calls.***

3.9.3 Information Security

The BCM's Voice Mail system ensures user privacy by ***PIN protecting mailboxes***. To check for messages, a mailbox owner must enter their PIN. As a security measure, a mailbox owner can be required to periodically change their PINs.

The BCM can be programmed with system speed diallers for commonly dialled numbers. Some of these numbers may require access codes and passwords that are private. These ***speed dial entries can be programmed to not display the dialled number when used***.

The BCM supports Direct Inward Dialling (DID) so outside callers can reach specific sets without having to dial an extension or go through an operator. The system programming provides complete control over which sets are reachable and by which number. Some phones can remain private and reachable only from within the system or through an operator.

CDR data logs can be extracted from the BCM. This CDR data contains among other things, call activity data as well as digits collected after call set-up. This ***sensitive CDR data should be stored in a secure location and a secure transmission method should be used***. See section 3.9.6 Protecting Sensitive Data for further details.

3.9.3.1 IP Set Security

IP sets on an IP network are potentially vulnerable to unauthorized access if not properly configured. This vulnerability could potentially allow someone to register an IP client and make fraudulent calls on a BCM. IP clients are keycode protected, therefore as long as no licenses are enabled, sets cannot be registered. By default there are no IP client licenses installed. If additional or spare IP client keycodes are available on a BCM, extra precaution should be taken around registration settings. The first time an IP client is configured on a BCM, it must be registered to the system so that its hardware ID can be mapped to a DN in the BCM. The mapping of the hardware ID to a DN is the protection mechanism against someone taking any IP client and connecting it to the BCM. To add an IP client, the registration process must be enabled. By default, the registration process is disabled. ***For added security, it is highly recommended that registration for IP clients remain disabled unless a new phone is to be added.***

During the registration process of IP clients, there is a password that protects against unwanted IP clients registering. The password can be an alphanumeric value of up to 10 characters. Because the password is entered through the telephone, only numeric values can actually be used. ***This default password should be changed during initial system installation.*** For additional security, a firewall could be used during the registration process to protect the BCM from unwanted IP clients. By allowing only the IP addresses of the configured IP sets and blocking all others from using UDP port 7000, this protects the BCM from unwanted IP client connections.

3.9.3.2 Companion handset security

Wireless Companion sets require security practices similar to IP sets. The security threat is that someone could register a Companion handset and make fraudulent calls on the BCM. The Companion sets require a keycode for every handset that is registered to a BCM. By default there are no Companion keycodes

installed. If additional or spare Companion keycodes are available, extra precaution should be taken around registration settings. The first time a Companion handset is configured on a BCM, it must be registered to the system so that its hardware ID can be mapped to a DN in the BCM. The mapping of the hardware ID to a DN is the protection mechanism against someone taking any Companion handset and connecting it to the BCM. To add a Companion handset, the registration process must be turned on. By default, the registration is enabled. ***For added security, it is highly recommended that registration for Companion be disabled unless a new handset is to be added.***

During the registration process of Companion handsets, there is a password that protects against unwanted wireless handsets registering. The password can be an alphanumeric value of up to 6 characters. Because the password is entered through the telephone, only numeric values can actually be used. ***This default password should be changed during initial system installation.***

3.9.3.3 802.11b wireless handset security

IP Wireless handsets based on IEEE 802.11b and H.323 require security practices similar to Companion sets. Before the handset is allowed access to the network, an ESS ID code must be entered on the handset to identify the access point. The handset also requires a PIN entry before it can register with the BCM and be utilized. The topic of Wireless (WLAN) security is outside the scope of this document[1].

3.9.3.4 DECT handset security

Wireless DECT handsets require security practices similar to Companion sets. Ensure that ***mobile recording is turned off*** when not required. This can be accomplished using the DECT Maintenance Console or through the use of a DECT Wizard. The ***default mobile recording password and installer passwords should also be changed*** using the Maintenance Console.

3.9.4 System Administration

The BCM lets individual users configure a number of settings on their phones. The degree to which a user can program the phone is controlled through the ***system administration set lock feature***, which provides full, partial, and none levels. Access to telephony configuration is via Unified Manager which is password protected. The BCM also provides limited access to telephony programming through set based admin.

3.9.5 Wiretapping and Eavesdropping

Each Business Series Telephone (BST) is connected directly to a Media Bay Module on the BCM using a dedicated loop and Time Compression Multiplexing (TCM). This makes it ***very difficult to physically tap the wire***. The BCM controls which phones have access to which lines, so users cannot indiscriminately eavesdrop on private calls.

The BCM uses a Function Messaging Protocol (FUMP) to set up calls between sets and lines. During call set-up, it is often necessary to provide access codes and passwords and transmit these to the network. In the BCM, ***FUMP is not accessible on TCM loops***, so it is not possible to monitor FUMP messaging to acquire access codes and passwords.

IP connected telephones, such as the i2004 and i2050 softphone, transmit digits and voice unencrypted over the IP network. Anyone with direct access to the IP network carrying the voice stream can eavesdrop on the conversation using a packet sniffer. Although this is similar to the security level offered by public cell phone service, it is more restrictive because access is restricted to specific IP subnets. IP communication from one BCM to another can be protected from packet sniffing using trunk-to-trunk VPN connections. The risk of packet sniffing on IP communication from an IP set to the BCM can be reduced by using private segments, leased private corporate WANs or segmented VLANs.

[1] Refer to http://www.nortelnetworks.com/solutions/security/doclib.html for additional information on this subject.

BCM Wireless solutions such as DECT and Companion transmit digits and voice unencrypted over the airwaves. The security and privacy offered by these wireless solutions is equivalent to public cell phones. The BCM also offers IP Wireless Terminals based on IEEE 802.11b and H.323. ***IEEE 802.11b systems can employ WEP and Kerberos encryption to enhance the security of this wireless solution***.

3.9.6 Protecting Sensitive Data

Sensitive data such as passwords and call records should be protected through encryption. There are various capabilities provided by the BCM for protecting sensitive data. A VPN tunnel is a powerful, general purpose method of encrypting all data transmission that goes through the tunnel. Up to 16 IPSec client tunnel connections can be made to the BCM. See section 4.5 VPN for further details.

The CDR data contains sensitive telephony data which is transmitted to servers for collection. The data should be transmitted securely to ensure data confidentiality. For the CDR Pull method, the data is sent through a secure SSL interface. For the DCOM (real-time) interface method, the data is encrypted within the DCOM protocol but this DCOM encryption is not available on Win9x client OSs, only Win/NT, 2000 and XP. There is no secure data transmission for the CDR Push method which utilizes standard FTP.

The BCM provides SSH support as a secure alternative to Telnet which is used for some OAM activity.

The BCM provides SSL support in order to secure http access. BCM client applications and some Unified Manager screens utilize SSL encryption. The Unified Manager transmits the logon userid and password in encrypted format. To secure the configuration screens in Unified Manager, a VPN tunnel should be used.

4 BCM Security Services – Securing your network

The BCM platform provides key security services to help customers implement a secure data network. Selection of which BCM services to utilize depends on each customer's security policy, risk assessment and requirements.

4.1 Firewall

The BCM comes equipped with a ***full-featured, stateful firewall*** that offers significant protection to both the BCM and the network behind it. When enabled, the BCM firewall allows the setting of filter criteria for both incoming and outgoing data traffic on port ranges, source and destination IP addresses, and protocols. No external firewall device is required to protect a private data network from unauthorized access. The firewall service is a very useful security first line of defense. The BCM firewall, sometimes referred to as a ***stealth firewall***, drops blocked packets and the sender is not aware of the rejection since there is no acknowledgement sent.

4.2 SSH

The BCM supports the Secure Shell (SSH) protocol as a secure alternative to the Telnet interface. SSH is an industry standard (IETF) protocol that provides a secure means of logging into another server (BCM) over a network. The SSH protocol authenticates identities and encrypts data communication resulting in confidentiality, on-the-wire tamper detection as well as IP spoofing protection.

The SSH protocol supports the following encryption algorithms: AES (Rijndael) (128 /192 / 256-bit keys), 3DES (168-bit key), Twofish (128 /192 / 256-bit keys), Blowfish (128-bit key), Arcfour (128-bit key), CAST128 (128-bit key) and DES (supported as a fallback). SSH also supports the following hash and public-key algorithms: MD5, SHA1, DSA, RSA, and Diffie-Hellman.

The BCM provides a SSH client for user's convenience. The open source **PuTTY** client can be downloaded from the BCM client download page however other SSH client applications are compatible. The Telnet service can be re-enabled through the Unified Manager and can co-exist with the SSH server if it is required. For further details, refer to section 5.8 Telnet Service.

4.3 SSL

The BCM supports the Secure Socket Layer (SSL) protocol which protects the http interface. SSL is related to the industry standard (IETF) protocol TLS (Transport Layer Security). The SSL protocol provides encryption on top of the TCP/IP layer for application layer protocols. SSL allows client and server applications to establish a secure, encrypted connection. The SSL protocol provides an end-user the ability to authenticate the server's (BCM) identity using the SSL handshake protocol. Public-key cryptography techniques are used to check that the server's certificate are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs. After this phase, an encrypted SSL connection (40, 56, or 128 bit) is established between the BCM and the client PC. The data is encrypted by the sender and decrypted by the receiver. The encryption provides confidentiality and detection of on-the-wire tampering. A 128 bit encryption is approximately $3x10^{26}$ stronger than 40 bit encryption.

Redirection from http to https (SSL) ensures all access is through https and old http bookmarks are gracefully managed. The BCM URL is: https://<IP address>. The default SSL port 443 is used.

SSL web access can be disabled in the Unified Manager through a configuration option if standard http access is required but this introduces the security risk associated with unencrypted communication.

SSL certificate management is provided through the Unified Manager Maintenance Tool interface which provides a Certificate and Private Key capability to end customers who want to install **their own certificate** to eliminate the site authentication security warning present with the default certificate. The

default self-signed certificate enables SSL encryption but cannot address site authentication. The certificate upload capability validates that the public and private keys are paired.

4.4 NAT

The Network Address Translation (NAT) can be enabled to ***effectively hide a network of computers behind a BCM***. NAT on the BCM works like standard NAT devices with optional additional default rules and settings to accommodate IP clients. After enabling NAT on an interface of the BCM, computers who talk with the interface do not know about any of the other interfaces on the BCM. The IP addresses of the other interfaces and any computers behind those interfaces are translated by the NAT service into the single address of the interface that has NAT enabled. Outsiders see only a single server and cannot communicate directly with any of the other computers behind the BCM, only indirectly through NAT.

4.5 VPN

The BCM's Virtual Private Network component can be used by client applications to initiate up to ***16 IPSec or 64 Microsoft PPTP encrypted tunnels*** between a BCM 3.6 system and:

- A BCM administration desktop computer running the Contivity VPN client (IPSec) software
- Another BCM 3.6 (for branch-to-branch tunnelling)
- A Nortel Networks Contivity Extranet Switch (excepting CES 100 and 400)
- A Nortel Networks Shasta 5000 Broadband Service Node.

The VPN IPSec tunnels can be used at the same time as the BCM NAT and firewall. The PPTP tunnels do not support NAT, firewall, and QoS settings but NAT, firewall filter and QoS rules for the end points of the PPTP tunnel can be set.

The IPSec protocol is a standard based solution for providing privacy, integrity, and authenticity for the transmission of sensitive information over the Internet. The BCM's IPSec software supports both ESP and AH protocols with various levels of encryption (56 and 40-bit) DES and Triple DES data encryption as well as authentication with MD5 (128-bit hash) or SHA1 (160-bit hash). Various combinations of these settings is possible, the most secure setting is 3DES with 160-bit SHA1.

The PPTP tunnel authentication can be set to enhanced encryption with CHAP (for encrypted authentication) or MS-CHAP (Microsoft only data encryption). The data encryption uses 40-bit RC4 encryption.

For branch-to-branch VPN connections, the VPN encrypts not only the traffic between BCM systems, but can also tunnel the traffic of PCs and other devices on the data network behind the BCM, so they can also securely communicate with each other across the WAN or LAN. Using the BCM Contivity VPN client software, secure administration of the BCM platform from any location is possible without requiring additional hardware. With these VPN features, ***data can safely traverse the insecure public Internet***, while maintaining Data Integrity and Data Confidentiality.[2] The Contivity VPN Client can be downloaded via the Contivity Software download web interface (version 4.60_15).

4.6 Modem Security

Modem access can be restricted by disabling the modem interface using the V.90 Dial-Up interface in the Unified Manager as well as controlling Dial-In Access privileges by restricting group membership in the Dialup User Group.

[2] The BCM's VPN software is based on the Nortel Networks award winning Contivity switch that was awarded best VPN switch by 2002 Infosec, and was Network Computing 2002 Editor's choice. (http://www.infosecuritymag.com/2002/mar/excellencewinners032002.shtml)

A modem dial-back capability provides increased security for dial-in management support. The BCM's modem dial-back capability provides a two factor security. After the dial-in user provides logon credentials which are authenticated, the BCM disconnects the session and then initiates a call back to the preconfigured telephone number associated with the user. The dial-back feature utilizes the call back capabilities within Win/NT. The modem dial-back is an option that can be enabled or disabled for any given userid.

4.7 Data Recovery

In rare occasions, such as an unauthorized login, if a system becomes compromised and corrupted, it is important to have configuration data backups to restore a system to a known, functioning state. The ***BCM provides a full-featured and versatile Backup and Restore Utility*** (BRU), which should be used on a regular basis whenever making configuration changes. For customers with larger BCM networks, the use of the ***Network Configuration Manager*** (NCM) to manage, control and automate functions such as backup and restore, common file distribution and patching is recommended. For more information about NCM, please consult the NCM Application Brief available on the Partner Information Center, PIC.

During a BRU backup operation, sensitive data (CDR data, Vmail) is transmitted to the backup server. To protect data confidentiality, RC4 encryption is used to implement BRU data encryption. The data encryption provides data confidentiality both on-the-wire and protects against unauthorized access to the backup file on the storage server.

In cases where the extent of software or data corruption on the BCM's functional hard disk drive renders the BCM unusable, a re-image of the BCM's hard disk drive to an original factory image may be required. The ***BCM Imaging Tool (BIT)*** application is available to perform this type of data recovery. After re-imaging the BCM's hard disk drive, an un-corrupted back-up of user data may be restored, or the BCM can be manually re-configured. Please refer to BCM Imaging Tool User Guide for further details.

4.8 Virus Scanning Software

Virus scanning software is used on the BCM software loads before they are distributed to customers. The BCM does not embed any virus-scanning software on the platform because of the performance impact these types of applications may have on the BCM's real-time operation and the ensuing requirement for network access for frequent virus data file updates. A hardened server is well protected from viruses since the hardening measures provide a good barrier to virus infections. Proper system configuration and user practices are an effective virus defense. In order for anti-virus software to intercept and prevent a virus infection, the virus specific data files must be available and installed prior to exposure, which may not be achievable. However, if desired, it is possible to run the virus-scanning software remotely when the BCM hard drives are mounted. Refer to section 7 Virus Scanning on BCM for further details.

4.9 Intrusion Detection System (IDS)

No host-based IDS network security software is embedded on the BCM because this technology typically results in many false positive results that require much attention and administration to clear. IDS applications also require regular updating of data files containing documented attack signatures. The embedded firewall on the BCM provides considerable data network security; however customers can deploy a network IDS system (external to the BCM) if they feel the need is warranted.

5 Addressing Potential Attacks

Platform Security is all about protecting the system from attacks. Most attacks take the form of: “probe, scan, account compromise, file system compromise, packet sniffer, denial of service, exploitation of trust, [and] malicious code”[3]. Each of these aspects will be discussed in detail to review how the BCM protects against potential attacks.

5.1 Probe / Scan

Probes and scans are used to gather information about a platform. Depending on which services have been enabled, a great amount of detail about a server can be discovered with simple scans. Once this information is determined, tools that exploit known holes in a particular server may be used. ***Enabling the BCM’s firewall helps protect both the BCM and the data network behind it from malicious probes and scans***. The firewall rejects data communication on any ports that have not been enabled.

The default ***drive shares on the BCM have been disabled***. Note that*: the shared resources: IPC$ and NortelDT$ need to remain configured.* The NortelDT is used to provide access to retrieving Nortel Networks client applications and the IPC share is used for RPC system level communication. Null session queries and access are also restricted through operating system settings.

5.2 Account Compromise

Cracking tools, programs or social engineering may be used to obtain an account password and gain access into a system. ***A practical way to protect against account compromise is to have an effective password policy in place where secure passwords are used***. Passwords should be changed on a regular basis; especially all default passwords must be changed. The account lockout capability is also an effective deterrent to account compromise attacks.

5.2.1 BCM 3.6 Upgrades - Password Policy Settings

BCM platforms which have been upgraded to release 3.6 will not automatically have their password policy set to the defaults described in this document so that existing user accounts based on prior password policies are preserved during the upgrade process. ***It is the responsibility of the system administrator to increase the password policy and update the existing accounts with passwords that meet the new password complexity and length settings.***

5.3 Packet Sniffer

A packet sniffer is a software tool that can be used to pull traffic off a data network and view any unencrypted data, including administrator passwords. The packet sniffer decodes all the information in a network packet, which includes source and destination addresses, along with the actual data that is being sent. In its default configuration the BCM has minimal protection from packet sniffers, since none of the administrator tools use an entirely encrypted data stream. Although the Unified Manager GUI sends passwords in an encrypted format, other interfaces such as Telnet and the Call Pilot application do not and are therefore susceptible to sniffing.

To further protect against packet sniffing attacks, a VPN client connection to the BCM should be used to encrypt the data communication. All the application interfaces to the BCM are secured when they are tunnelled through the VPN component, even across the public Internet. No additional external switch is required to increase security.

If VPN client connections are not used, the risk of packet sniffing can be reduced by having administration take place either on private segments “behind” the BCM, or across leased private corporate WANs. On a

[3] http://www.cert.org/encyc_article/tocencyc.html

switched data network with segmented VLANs, the risk is also reduced since administrative access to the switch is required to sniff traffic destined for another device on the network. This approach is useful to mitigate the risk associated with IP set packet sniffing.

5.4 Denial of Service

A Denial-of-Service or DoS attack does not compromise the security of the server or network. There is no break-in, and confidential information is not obtained nor destroyed. Instead, a DoS attack causes a server or network to deny valid requests for service by exploiting deficiencies in its TCP/IP stack implementation or in other protocols. A DoS attack can clog the network with fake requests, or it can cause a server crash that makes the network unable to service valid requests. ***The use of the BCM firewall can help protect against many DoS attacks.***

5.4.1 Distributed Denial of Service

This is a special type of DoS attack that combines Malicious Code with a regular DoS attack. First a virus or worm is written to exploit a known hole in a particular type of server, and then code is added to trigger a DoS attack on a specific server. Sometimes the trigger will be a certain time on a certain date, while the more elaborate programs wait for an external trigger before attacking. Though it is extremely difficult to protect against certain types of DoS attacks, the ***BCM's OS hardening*** efforts have made the BCM more resistant to attacks that try to exploit known vulnerabilities.

5.5 Exploitation of Trust

Many computer systems have a trust relationship with other computer systems. In a trust relationship, logging onto one computer on a network provides access to many other computers without having to log onto them directly. This is how a Windows NT domain works. Be aware that configuring the BCM to participate in an NT domain can lead to a compromise if the domain is compromised. There is no protection from this type of attack. ***All trust relationships should be reviewed on a regular basis and an effective network password policy should be in place***. One reason for having the BCM participate in a domain is for ease of administration access to Call Detail Recording (CDR), but this is not a requirement.

5.6 Malicious Code

The three most common types of malicious programs are viruses, Trojan horses and worms. Viruses and Trojan horses are often hidden in a message or program. When the message is opened or the program is run, code executes and unleashes the virus, which spreads to other systems. Worms usually don't even require any sort of user intervention to initiate the process. Worms enter networks through known vulnerabilities in certain operating systems, and try to work their way into other systems.

The BCM is a closed system that does not support the installation of additional software, so the risk of a virus or Trojan horse infection is significantly reduced. Since worms don't require user intervention to get into a network, a properly configured **firewall on the BCM can be an effective protection**.

5.7 Social Engineering

Although it's not an attack as such, many security breaches take place through what is known as Social Engineering. This is when a hacker tries to trick an employee into revealing a username and password, usually by phoning and pretending to be someone else, such as a manager from another branch of the company[4]. Sometimes the security threat is low-tech, and the only way to ***guard against it is to educate employees***.

[4] http://www.sans.org/infosecFAQ/securitybasics/awareness.htm

5.8 Telnet Service

The telnet interface is an insecure interface and the BCM ***telnet service (tlntsvr) has been turned OFF by default.*** Instead, a secure SSH interface is enabled as a replacement alternative and a SSH client application called PuTTY is provided from the Unified Manager client download page.

5.9 Microsoft DCOM

The BCM's Unified Manager, CDR and LAN CTE application use Microsoft DCOM. There are known DoS attacks that can affect MS DCOM. If a public interface is used, ***enabling the firewall can protect against such attacks*** however, the settings must allow DCOM communication to continue to these applications. Specifying the source address in the settings may be advisable. The BCM's Windows NT embedded operating system is up to date with security hotfixes in this area.

5.10 Plaintext Passwords/PINS

When performing BCM management through interfaces such as Telnet, there is no encryption in their communication protocols and hence passwords are sent across the network in plain text. In an environment that requires encrypted management, a VPN client connection to the BCM should be used to ***secure a tunnel between the BCM and the management station.*** The use of an SSL interface encrypts the Unified Manager password but the Configuration Management menu is not encrypted.

5.11 SNMP security

The SNMP community string is analogous to a password for the public and private interface. The system ***administrator should change the default community string for both interfaces***. The community string should follow the same "strong password" policy as user accounts.

The default ***management list*** is set to 10.10.10.1 to disallow unauthorized public access from any IP address other than the one specified in the management list. The IP addresses of authorized SNMP management systems should be entered into the management list since an empty list allows any external system access to the SNMP interface.

6 Maintenance and Support Features

The following serviceability features and practices further enhance the overall BCM security solution.

6.1 Field Patches

The BCM software architecture ***supports the ability to apply field patches***. A patch tool is used to administer and apply these software fixes. This is an important capability that can be used to quickly deploy ***newly discovered security hotfixes to the NT embedded OS or any other application as deemed necessary by Nortel Networks***. For customers with larger BCM networks, the Network Configuration Manager can be used to automate the process of distributing and applying patches to a network of BCMs over an IP network. With NCM3.6, patch distribution and application can be scheduled for BCM 3.6, 3.5, 3.0.1 and 3.0 systems, thereby dramatically reducing the time required to deploy a patch to many BCMs.

The Unified Manager can be used to view the list of patches applied to a BCM system, including the list of applied Microsoft security hotfixes. This information is useful to confirm that the BCM system has the required patches applied.

6.2 Security Response Procedure

Nortel Networks security group plays an important active role in dealing with security threats. Nortel Networks is as a founding sponsor of the Internet Security Alliance (ISA) and has access to their Special Communications Database and Vulnerability Catalog. Nortel Networks receives notifications about current vulnerabilities, frequently before they are made public. Nortel Networks is obligated to not disclose to third parties any such pre-public information, but disseminates this information internally to product groups as required so that action can be taken and a response can be prepared.

Nortel Networks security group assesses each vulnerability notification received for potential impact on Nortel Networks products and solutions. If a product is affected, corrective actions are initiated, which include any or several of the following, as appropriate:

- Vendor Statement posted to the corresponding CERT web page (Advisory or Vulnerability Note) (http://www.cert.org/advisories/)
- Vendor Statement or technical bulletin approving application of a platform vendor's mitigation strategy or patch
- Technical bulletin detailing product-specific mitigation strategies, or
- Technical bulletin providing instructions on applying patches
- Software patch
- Upgrade load
- Correction on next scheduled maintenance release

A formal process ensures that Nortel Networks' level of response is appropriate to the severity of the vulnerability. The determining risk factors include the impact to customer networks, ease of exploitation, prevalence in installed base and whether or not exploits are known to exist and/or be underway. Similarly, customer communication strategies are invoked commensurate with the severity of the vulnerability. Nortel Networks avoids making public any detailed technical information which could be subverted maliciously against a customer network. Accordingly, most technical bulletins dealing with security vulnerability issues are available upon request only, from Technical Support or eService.

The BCM product security response procedure includes any or several of the following, as appropriate:

- Nortel Networks posting on CERT web page includes statement about BCM’s degree of vulnerability (http://www.cert.org/advisories/)

- BCM Product Advisory Alert is posted on to PIC web site and communication sent to partners (http://www.nortelnetworks.com/prd/picinfo/index.html)
- BCM Customer Support Bulletin issued
- Technical bulletin detailing product-specific mitigation strategies or instructions on applying patch is released along with the patch as required

A formal process ensures that the BCM product level response is appropriate to the severity of the vulnerability and considers of all the risk factors. Each software patch is carefully tested by the design group and a regression test is performed by the product verification team. The patch may then be released to Beta sites for further testing before being made generally available and distributed through the support organization. The deployment of GA patches for BCM security vulnerabilities are managed in the same manner as other BCM software patches.

6.3 Manufacturing Security

The manufacturing process of the BCM incorporates security practices designed to ensure the software is checksum authenticated and virus-free. All computers used during the manufacturing process are scanned for viruses and used in a closed and isolated environment.

6.4 Development Security

The development phase of the BCM makes use of a load build environment which is carefully managed so each release is built securely; two separate virus scanning software tools are run on the load build computers to facilitate a clean release.

7 Virus Scanning on BCM

7.1 Introduction

During the design and engineering phase of the BCM, two virus checking software packages are used to verify that the product is built in a secure environment. Since the BCM is a closed system, the BCM is significantly less susceptible to on-site virus infections than an average file or applications server.

Nevertheless, a ***virus scan can be performed on the mounted drives of the BCM*** if a virus has been detected within the corporate network and there is a need to verify all equipment as per business practices.

7.2 Requirements

Since the BCM is a closed, embedded system with precisely tuned performance, there are particular requirements that need to be adhered to during a virus scan. ***Do not install anti-virus software directly onto the BCM*** since doing this can adversely disrupt the integration of BCM applications and services, or cause some components to fail.

Virus scans on the BCM must be performed through remotely mapped drives. Select virus scanning software capable of scanning remotely mapped drives. The common anti-virus applications from Sophos, Norton and McAfee all have this capability. In addition, a Windows NT 4.0, Windows 2000 Professional or XP client PC is required to run the software. Virus scans should be performed during off-hours; this will minimize system resource impact.

7.3 Virus Detection

If a virus is detected during a remote scan of the BCM's hard drives, please ***do not attempt to remove any files yourself*** since this may adversely affect the operation of the BCM. Please ***contact your next level of support*** (distributor or Nortel Networks Technical Support) for assistance in dealing with the infected files.

Appendix A: Other Resources

These resources have useful information about computer and network security.

1. http://www.sans.org/ - Contains an extensive library of security-related papers and other resources.
2. http://www.cert.org/ - the authority on security threats. Excellent library of resources.
3. http://www.atstake.com/ - especially recommended is the “Research Labs” section.
4. http://www.cert.org/archive/html/analysis-method.html - Survivable Network Analysis.
5. http://www.boran.com/security/ - comprehensive resource.
6. http://www.symbol.com - Symbol NetVision IP Handset web site
7. http://developer.netscape.com/docs/manuals/security/sslin/index.html - Introduction to SSL
8. http://www.modssl.org/docs/2.8/ssl_intro.html - SSL description
9. http://www.ssh.com – SSH description