CORE® 5

CORE Enterprise®
on a WAN

Vitech

Copyright 1992 - 2007 Vitech Corporation.
All Rights Reserved

Copyright © 2006-2007 Vitech Corporation. All rights reserved.

No part of this document may be reproduced in any form, including, but not limited to, photocopying, translating into another language, or storage in a data retrieval system, without prior written consent of Vitech Corporation.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7013.

Vitech Corporation
2070 Chain Bridge Road, Suite 100
Vienna, Virginia 22182-2536
703.883.2270 FAX: 703.883.1860
Customer Support: support@vitechcorp.com
www.vitechcorp.com

CORE® is a registered trademark of Vitech Corporation.

Other product names mentioned herein are used for identification purposes only, and may be trademarks of their respective companies.

Publication Date: September 2007

Table of Contents

List of Figures

This document describes how to use CORE Enterprise 5 in a WAN (wide-area network) environment, including necessary configuration of the CORE Enterprise server and clients, configuration of domain name servers, and configuration of network firewalls and routers separating the server and clients.

Alternative Approaches

Rather than configuring firewalls and routers to natively support CORE Enterprise, it may be possible to leverage existing network capabilities.

Virtual Private Network (VPN)

If the CORE Enterprise clients and server are on a common virtual private network (VPN) bridged by the firewalls between them, then no special configuration may be required. However, the firewalls should forward all traffic to the VPN, and firewall rules should not be applied to the VPN. In addition to simplifying configuration of CORE Enterprise on a WAN, a VPN is also desirable because it provides end-to-end encryption of all CORE data.

Terminal Services

Windows Terminal Services and some other products can allow CORE Enterprise users who are remote from the CORE Enterprise server to run their clients on server but see the user interface on their own computers. Vitech cannot support this approach, but, if Terminal Services is already used in your organization, you may be able to leverage it. Using CORE Enterprise via Terminal Services may require considerable resources on the server and may consume a moderate amount of network bandwidth, but performance will be better over high-latency links, especially for performing exports, generating reports, and running simulations.

General Notes

The following should be observed throughout these instructions:

Restricted Port Numbers

While the IP ports used for CORE Enterprise network communications are configurable, you should avoid using lower-numbered ports, many of which are already used by Windows operating systems. Using them in CORE may result in a resource conflict that could cause CORE Enterprise and/or your operating systems to malfunction. Also avoid using ports required by other software on your network or any commonly used ports.

IP Services Database

The mapping of IP service names to port numbers and protocols is defined in a simple text file named “services”. Several ports used by CORE Enterprise are configured via this file. Because some ISP software installs its own version of the file, a computer may have several of them in different locations. When modifying this mapping, it is best to find and modify all of them. The default location is %SystemRoot%\system32\drivers \etc\services. The actual current location is specified in the Windows registry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters \DataBasePath.)

Network License Manager (NLM) Notes

The following facts may simplify configuring your network to support CORE Enterprise:

Alternative License Mechanisms

The Network License Manager (NLM) allows a pool of licenses to be shared by all users with access to a common network. However, there are three alternatives to using the NLM for licensing. The preferred way to license CORE Enterprise is the “Enterprise” license mechanism, which is built into the CORE Enterprise client and server software and requires no additional network configuration. However, the Enterprise license mechanism can only license CORE Enterprise, whereas the Network License Manager can serve a mix of Enterprise and Workstation licenses. The “node-locked” license mechanism locks one of your client licenses directly to the client computer. The disadvantage is that it cannot be shared by multiple installations on different computers. There is also a “floppy key” mechanism which can be shared by multiple installations but requires a license diskette to be in the floppy drive of the computer running the software. Different users of the same CORE Enterprise server can employ a mix of license mechanisms.

Network License Manager (NLM) 4.3

NLM 4.3 uses the UDP protocol. If an NLM 4.3 client terminates abnormally, there may be a delay (90 minutes, by default) before the license is released. The NetTerm utility may be used to manually release an unused token. NetTerm can release tokens checked out by the computer where it is running. If NetTerm is running on the NLM server, it can release any token.

Network License Manager Location

If the Network License Manager is used, it is often installed on the same computer as the CORE Enterprise Server software. However, the NLM is a separate product and can be installed on a separate host from the CORE Enterprise server. (A client can obtain a license from an NLM on one computer and use it to log into a CORE Enterprise server on another computer.) If possible, the NLM should be installed on the same LAN as the clients.

Server-Side Firewall Rules for Network License Manager 4.3

The following must be allowed by a server-side firewall to permit CORE Enterprise clients to obtain licenses from Network License Manager 4.3:

NLM Listening Port for CORE Enterprise client

Default port:	32000
Protocol:	UDP
Direction:	Inbound
Server configuration:	Customized NLM.Ini.Z file supplied by Vitech.
Client configuration:	Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech Corporation\CORE Enterprise\5.0\NLM\port.

NLM Reply Port for CORE Enterprise client

Default port:	32001
Protocol:	UDP
Direction:	Outbound
Server configuration:	Automatic
Client configuration:	Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech Corporation\CORE Enterprise\5.0\NLM\replyPort.

NLM Listening Port for NetTerm (Optional)

Default port:	32000
Protocol:	UDP
Direction:	Inbound
Server configuration:	Customized NLM.Ini.Z file supplied by Vitech.
Client configuration:	Options >> Network command on NetTerm console window or Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \cca\netterm\nlm_port.

NLM Reply Port for NetTerm (Optional)

Default port:	No default.
Protocol:	UDP
Direction:	Outbound
Server configuration:	Automatic
Client configuration:	Not configurable. NetTerm may not work if a server-side firewall restricts outbound UDP traffic (initiated by the server).

Server-Side Firewall Rules for CORE Enterprise

The following must be allowed by a server-side firewall to permit CORE Enterprise clients to access the server:

<u>CORE Enterprise Server NetLDI Listening Port (Required)</u>

Default port:	10085
Protocol:	TCP
Direction:	Inbound
Server configuration:	Specified during installation or as “CORE50NetLDI” in the services file. (See “IP Services Database” above.)
Client configuration:	Specified during installation or as “CORE50NetLDI” in the services file. (See “IP Services Database” above.)
Purpose:	Handles client logins.

Gem Listening Port (Required)

Default port: 10086
Protocol: TCP
Direction: Inbound
Server configuration: Specified during installation or manually as follows:

Must first stop and uninstall CORE50NetLDI service. At a command prompt, enter:

```
netldi delete CORE50NetLDI
```

Edit %CORE50Server%\InstallAids\CreateNetLDI.Bat. Replace “10086:10086” with desired port range. Run CreateNetLDI.Bat and start the service.
Client configuration: Automatic
Purpose: A “gem” process is an agent spawned on the CORE Enterprise application server for each client.

Broadcast Update Port (Optional)

Default Port: 32061
Protocol: UDP
Direction: Outbound
Server configuration: Specified during installation or as “CORE50Update” in the services file. (See “IP Services Database” above.) Must be unique for each CORE Enterprise server in the subnet.
Client configuration: Automatic
Purpose: The broadcast update mechanism is the most efficient way for the server to report repository changes to interested clients.

Backchannel Update Port (Optional)

Default Port: 32062
Protocol: UDP
Direction: Outbound
Server configuration: Specified during installation or as “CORE50Update2” in the services file. (See “IP Services Database” above.)
Client configuration: Automatic
Purpose: The backchannel update mechanism is the second most efficient way for the server to report repository changes to interested clients. If a client is unable to use either the broadcast or backchannel update mechanism, it reverts to “standard” mode, which requires no additional ports or configuration.

CORE2net Server NetLDI Listening Port (Optional)

Default port: 10087

Protocol: TCP

Direction: Outbound

Server configuration: Specified as “CORE2net50NetLDI” in the services file. (See “IP Services Database” above.)

Server-Side Firewall Rules for CORE2net

The following must be allowed by a server-side firewall to permit web clients to browse pages served by a CORE2net web server. CORE2net is usually installed on the same host as the CORE Enterprise server with which it is associated (during CORE2net installation). However, CORE2net is separately licensed and installed and may reside on a system that is remote from the CORE Enterprise server, in which case an additional port is required:

HTTP Listening Port (Required)

Default port: 80

Protocol: TCP

Direction: Inbound

Server configuration: Specified via Administrative Tools window in CORE Enterprise client software (using a client that logs in to the CORE Enterprise server associated with the CORE2net server).

Purpose: Handles requests from HTTP clients such as web browsers.

CORE Enterprise Server NetLDI Listening Port (Required)

Default port: 10085

Protocol: TCP

Direction: Outbound

Server configuration: Specified during installation or as “CORE50NetLDI” in the services file. (See “IP Services Database” above.) Must match CORE Enterprise server configuration.

Gem Listening Port (Required)

Default port: 10086 (depends on CORE Enterprise server configuration as described above)

Protocol: TCP

Direction: Outbound

Server configuration: Automatic

CORE2net Server NetLDI Listening Port

(Required if CORE2net server resides on different host from CORE Enterprise server)

Default port: 10087
Protocol: TCP
Direction: Inbound
Server configuration: Specified as "CORE2net50NetLDI" in the services file. (See "IP Services Database" above.)
Purpose: Listens for requests to start the CORE2net server. The requests are issued from the Administrative Tools window of the CORE Enterprise client software.

Server-Side Network Address Translation (NAT)

There are two kinds of network address translation (NAT): *dynamic* and *one-to-one*.

Firewall Configuration for Server-Side NAT

If a server-side firewall (or router) supports one-to-one NAT, then the device should assign the CORE Enterprise server, Network License Manager (NLM), and/or CORE2net server unique NAT public addresses. If the firewall or router must employ dynamic NAT (or sufficient public addresses are not available), then it must forward the CORE Enterprise Server NetLDI listening port and the gem listening port to the CORE Enterprise server, the NLM listening port to the Network License Manager, and the CORE2net Server NetLDI listening port and the HTTP listening port to the CORE2net server.

DNS Configuration for Server-Side NAT

A symbolic name should be registered for the CORE Enterprise server in DNS (Domain Name Service) servers both inside and outside the firewall or router. The DNS server inside the firewall or router should map the name to the server's actual IP address on its local network. The DNS server outside the firewall or router should map the same name to the server's NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address.

CORE Enterprise Server Configuration for Server-Side NAT

If no DNS is available inside the firewall or router to map the CORE Enterprise server's symbolic name (as established above) to its private IP address, then the same effect can be achieved by adding the mapping to the "hosts" file on the server. The hosts file is located in the same folder as the "IP Services Database" file (described above).

Client Configuration for Server-Side NAT

If no DNS is available outside the firewall or router to map the CORE Enterprise server's symbolic name (as established above) to its NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address, then the same effect can be achieved by adding the mapping to the "hosts" file on the client. The hosts file is located in the same folder as the "IP Services Database" file (described above).

When prompted for the IP address of the CORE Enterprise server during client installation, specify the server's symbolic name (as established above). If the client is already installed, set the value in the Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE\Vitech Corporation\CORE Enterprise\5.0 \Database\serverName.

If clients are still unable to log in to the CORE Enterprise server using DNS servers and/or hosts files as described above, then, when prompted for the IP address of the CORE Enterprise server during client installation, specify the CORE Enterprise server's NAT public address in dotted-decimal form (if the firewall or router uses one-to-one NAT) or the firewall's or router's WAN address. If the client is already installed, set the value in the Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE\Vitech Corporation\CORE Enterprise\5.0\Database\serverName. Add the following string value in the Windows registry: HKEY_LOCAL_MACHINE\SOFTWARE\Vitech Corporation \CORE Enterprise\5.0\Database\gemServerName. Set it to the actual private IP address of the CORE Enterprise server as it is known on its local network.

When prompted for the IP address of the Network License Manager during client installation, specify the NLM host's NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address. If the client is already installed, set the value in the Windows registry at HKEY_LOCAL_MACHINE \SOFTWARE\Vitech Corporation\CORE Enterprise\5.0\NLM\server.

CORE2net Configuration for NAT

No special steps are required if the CORE2net server software runs on the same host as the CORE Enterprise server. If the CORE2net server is separate from the CORE Enterprise server, then special configuration is required only if network address translation is performed by a device between them on the network.

If NAT is performed on the side of the CORE2net server, then, when you specify the IP address of the CORE2net server via the Administrative Tools window in the CORE Enterprise client software, use the CORE2net server's NAT public address (if the firewall or router uses one-to-one NAT) or the firewall's or router's WAN address.

Note that a web browser attempting to access CORE2net may need to specify a different address, depending on its network path to the CORE2net server.

If NAT is performed on the side of the CORE Enterprise server, then, if no DNS is available outside the firewall or router to map the CORE Enterprise server’s symbolic name (as established above) to its NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall’s or router’s WAN address, then the same effect can be achieved by adding the mapping to the “hosts” file on the CORE2net server. The hosts file is located in the same folder as the “IP Services Database” file (described above).

When prompted for the IP address of the CORE Enterprise server during CORE2net server installation, specify the CORE Enterprise server’s symbolic name (as established above). If the CORE2net server is already installed, set the value in the Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE\Vitech Corporation\CORE2net Communication Server\5.0 \Database\serverName.

If the CORE2net server still fails on startup using DNS servers and/or hosts files as described above, then, when prompted for the IP address of the CORE Enterprise server during CORE2net server installation, specify the CORE Enterprise server’s NAT public address in dotted-decimal form (if the firewall or router uses one-to-one NAT) or the firewall’s or router’s WAN address. If the CORE2net server is already installed, set the value in the Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE\Vitech Corporation\CORE2net Communication Server\5.0\Database\serverName. Add the following string value in the Windows registry: HKEY_LOCAL_MACHINE \SOFTWARE\Vitech Corporation\CORE2net Communication Server\5.0\Database \gemServerName. Set it to the actual private IP address of the CORE Enterprise server as it is known on its local network.

Client-Side Firewall Rules for Network License Manager 4.3

The following must be allowed by a client-side firewall to permit CORE Enterprise clients to obtain licenses from Network License Manager (NLM) 2.0 or 4.3:

NLM Listening Port for CORE Enterprise client

Default port: 32000
Protocol: UDP
Direction: Outbound
Client configuration: Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech Corporation\CORE Enterprise\5.0\NLM\port. Must match server configuration.

NLM Reply Port for CORE Enterprise client

Default port: 32001
Protocol: UDP
Direction: Inbound
Client configuration: Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech Corporation\CORE Enterprise\5.0\NLM\replyPort.

NetTerm (Optional)

NetTerm will not work with a client-side firewall.

Client-Side Firewall Rules for CORE Enterprise

The following must be allowed by a client-side firewall to permit CORE Enterprise clients to access the server:

<u>NetLDI Listening Port (Required)</u>

Default port:	10085
Protocol:	TCP
Direction:	Outbound
Client configuration:	Specified during installation or as “CORE50NetLDI” in the services file. (See “IP Services Database” above.) Must match server configuration.

<u>Gem Listening Port (Required)</u>

Default port:	10086 (depends on server configuration as described above)
Protocol:	TCP
Direction:	Outbound
Client configuration:	Automatic

<u>Broadcast Update Port (Optional)</u>

Default Port:	32061 (depends on server configuration as described above)
Protocol:	UDP
Direction:	Inbound
Client configuration:	Automatic

<u>Backchannel Update Port (Optional)</u>

Default Port:	32062 (depends on server configuration as described above)
Protocol:	UDP
Direction:	Inbound
Client configuration:	Automatic

API Login Port (Optional)

Default Port: 32002
Protocol: TCP
Direction: Inbound
Client configuration: Specified via Administrative Tools window in CORE Enterprise client software. (Must be matched by any application written to use CORE Applications Programming Interface against this client.)
Purpose: Listens for connections from programs written to use CORE API.

API Data Ports (Optional)

Default Ports: 32003-32050
Protocol: TCP
Direction: Inbound
Client configuration: Specified via Administrative Tools window in CORE Enterprise client software.
Purpose: Handle requests from programs in active CORE API sessions.

Client-Side Network Address Translation (NAT)

There are two kinds of network address translation (NAT): *dynamic* and *one-to-one*.

Firewall Configuration for Client-Side NAT

Special configuration is required if client-side network address translation is applied to a client that needs to obtain a Network License Manager (NLM) 4.3 license, that desires the efficiency of the "broadcast" or "backchannel" update modes, or which will be used as a CORE API server. If the client-side firewall (or router) supports one-to-one NAT, then the device should assign each CORE Enterprise client a unique NAT public address. If the firewall or router must employ dynamic NAT (or sufficient public addresses are not available), and if only a single client is located behind it, then it must forward the inbound ports listed above to the CORE Enterprise client.

If multiple clients are behind the firewall or router, and if it must employ dynamic NAT (or sufficient public addresses are not available), then at most one of the clients will be able to use broadcast update mode, and at most one of the clients will be able to use backchannel update mode. (The broadcast update port can be forwarded to one and the backchannel port to the other.) The remaining clients will automatically revert to "standard" update mode, which is less efficient. Each client requiring an NLM 4.3 license should be assigned a different NLM reply port. Each client which will act as a CORE API server should be assigned a different API login port and a distinct range of API data ports. The firewall or router should forward the appropriate ports to the respective clients.

Client Configuration for Client-Side NAT

If multiple CORE Enterprise clients are behind a client-side firewall (or router), and if it must employ dynamic NAT (or sufficient public addresses are not available), then it must forward a unique set of inbound ports to each client (as described above). A client's assigned Network License Manager 4.3 reply port can be specified in the Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE\Vitech Corporation \CORE Enterprise\5.0\NLM\replyPort. If a client will act as a CORE API server, its assigned API login and data ports can be specified via the Administrative Tools window in the CORE Enterprise client software.

NetTerm

NetTerm will not work with client-side NAT.

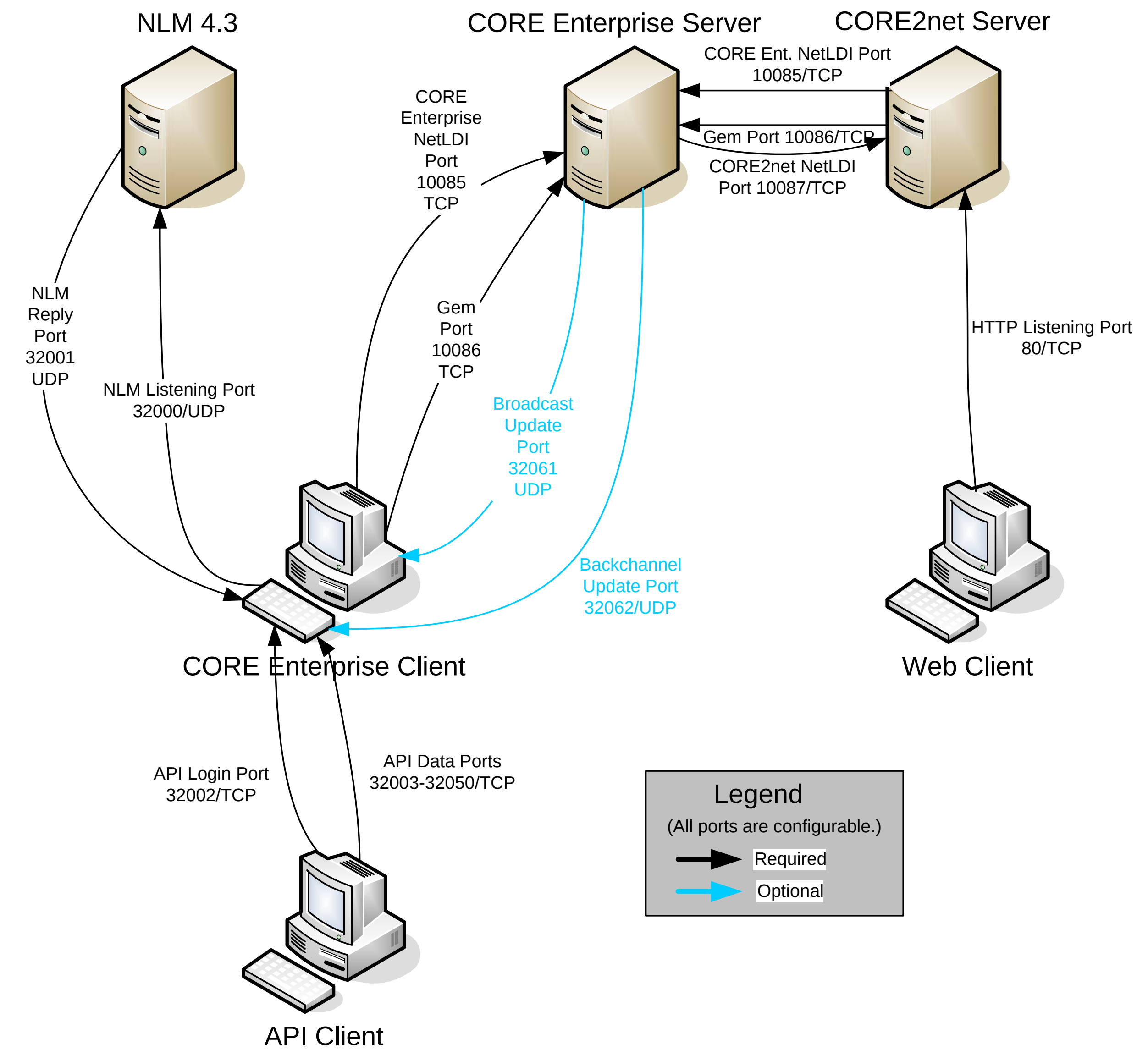
NLM 4.3
CORE Enterprise Server
CORE2net Server
CORE Ent. NetLDI Port 10085/TCP
Gem Port 10086/TCP
CORE2net NetLDI Port 10087/TCP
CORE Enterprise NetLDI Port 10085 TCP
Gem Port 10086 TCP
Broadcast Update Port 32061 UDP
Backchannel Update Port 32062/UDP
NLM Reply Port 32001 UDP
NLM Listening Port 32000/UDP
HTTP Listening Port 80/TCP
CORE Enterprise Client
Web Client
API Login Port 32002/TCP
API Data Ports 32003-32050/TCP
API Client
Legend
(All ports are configurable.)
Required
Optional

Figure 1 - Network Diagram

Vitech Corporation
2070 Chain Bridge Road, Suite 100
Vienna, Virginia 22182-2536
703.883.2270 FAX: 703.883.1860
Customer Support: support@vitechcorp.com
www.vitechcorp.com