Novell BorderManager®

www.novell.com

3.8

VPN DEPLOYMENT FAQ

November 10, 2003

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell BorderManager 3.8 VPN Deployment FAQ

November 10, 2003

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

BorderManager is a registered trademark of Novell, Inc. in the United States and other countries.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

All third-party products are the property of their respective owners.

Contents

About This Guide

This documentation presents a list of typical scenarios that the user might face while deploying the Novell® BorderManager® (NBM) 3.8 VPN services. The details for all the installation and configuration steps are provided in the Novell BorderManager 3.8 Installation and Administration Guide. The overview and planning considerations for proxy and firewall are provided in the Novell BorderManager 3.8 Proxy and Firewall Overview and Planning Guide. Read this document as a supplement to the above these two documents.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Common Questions

This section covers some of the common questions while deploying Novell® BorderManager® VPN services.

Scenarios

This section details some of the common VPN services deployment scenarios.

Do I need to first upgrade the server or the clients?

On a server you need to upgrade the master first. You can upgrade the client at any time, whether the server is upgraded or not.

What if we have a mixture of NBM 3.7 and NBM 3.8 clients and servers in the network?

The master should always be NBM 3.8 and should be configured for both IKE and SKIP.

Steps to Deploy:

1. Make sure the master is on NBM 3.8 with IKE and SKIP configured.
2. An NBM 3.7 slave should be configured for SKIP.
3. An NBM 3.8 slave should be configured for both SKIP and IKE.

Testing Your Configuration:

1. Exchange packets between the master and the NBM 3.7 slave with SKIP.
2. Exchange packets among the NBM 3.7 slaves with SKIP enabled.
3. Exchange packets between the NBM 3.8 slave and the NBM 3.7 slave with SKIP enabled.
4. Exchange packets among the NBM 3.8 slaves with SKIP enabled.
5. Exchange packets between master and the NBM 3.8 slave with IKE enabled.

Can I use third-party servers in the network?

Yes, but you should have the same rules in the master NBM 3.8 and in the third-party server.

Steps to Deploy:

1. Configure the NBM network and then put the 3rd-Party server.

TIP: See third-party servers information on BorderManager Cool Solutions.

Can I use an LDAP server which is on a different machine?

Yes, but before using LDAP with VPN, make sure LDAP is working properly.

Steps to Deploy:

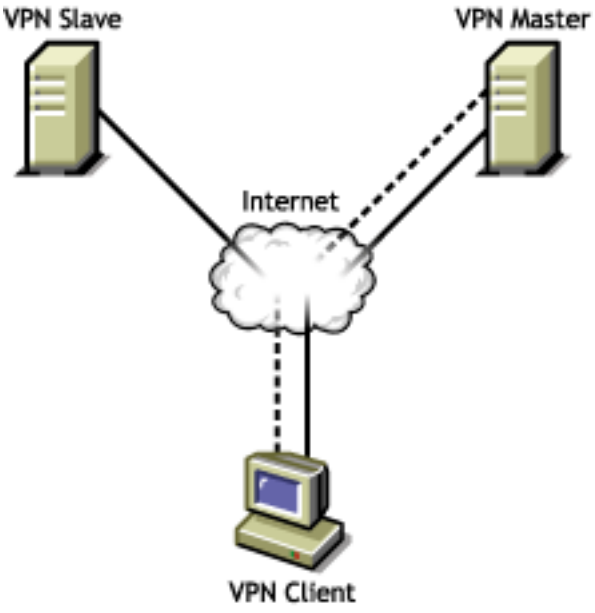
1. If you already have an LDAP server, collect the IP address and other details of the LDAP server and put them in the client-to-site details.

NOTE: No specific steps are needed if the server is on a different machine.

How do I deal with slow links across different sites?

By default, the VPN traffic rule encrypts all the packets going out of the client, and sends them to the VPN server. This adds unnecessary load to the tunnel, so you should use traffic rules to restrict the traffic.

Figure 1 Slow Links



Steps to Deploy:

1. Configure the client-to-site and site-to-site services.
2. In the client-to-site policy, add traffic rules to encrypt traffic only for particular protocol or network.
3. Add site-to-site protected network traffic rules with only protected networks as the destination.

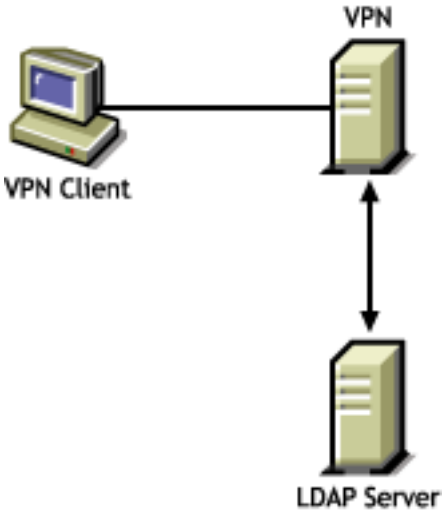
If Non-mandatory Steps are Missed:

If traffic rules are not added, all the traffic will pass through the VPN tunnel.

What if I have a very large number of users in a third-party directory server and want to configure client-to-site?

Configure the users at a server (such as LDAP) to have the fully distinguished name, and arrange them in groups.

Figure 2 Large number of users



Steps to Deploy:

1. Add the TRO of the LDAP server in the trusted root of the VPN server.
2. Add the group entries or user entries for which access is to be allowed.

If Non-mandatory Steps are Missed:

If the fully distinguished name of the LDAP entity (user or group) is not provided, the authentication will not succeed.

What if a client is connected to the ISP through dial-up with dynamic NAT at the ISP?

The dial-up connection can be made in two ways: Either dialup and connect to the VPN server, or use the dial-up client embedded in the VPN client.

Figure 3 Dynamic NAT

Steps to Deploy:

1. Configure the Windows machines to have dial-up.

How can I restrict the users to access only some of my internal networks based on their access level for VPN client-to-site?

Our Recommendation:

NBM provides various parameters through which this can be restricted.

Steps to Deploy:

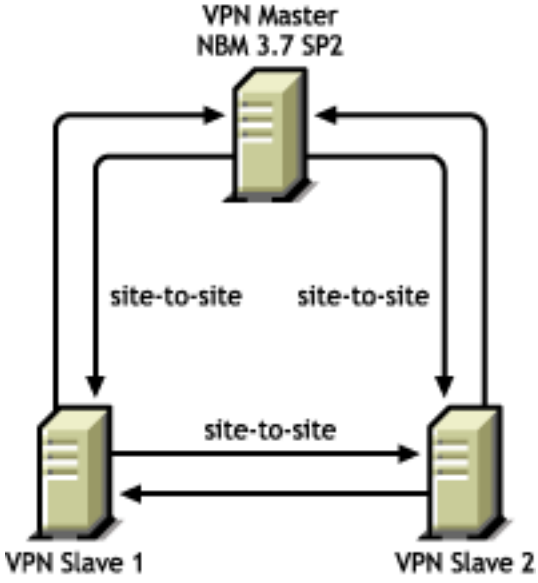
1. Add a traffic rule on top of the deny rule to encrypt the traffic only for those internal networks to which traffic has to be allowed.

TIP: The article that discusses these restrictions will be available in the November AppNotes.

How to upgrade the existing NBM servers to the latest version?

Upgrade the master VPN server first and then upgrade the other VPN servers.

Figure 4 Upgrading Existing Servers



Steps to Deploy:

1. Create a copy of the system related files like netinfo.cfg and resolv.cfg.
2. Note down the existing VPN configuration on the server. Also note whether client-to-site and site-to-site are enabled or not.
3. Make sure that the minimum requirements to install NBM 3.8 are met.
4. Start the NBM install and in the VPN schema extension screen choose to migrate the existing configuration in the future.
5. Complete the installation by choosing to install VPN and whichever other components you want to install.
6. Run VPNCFG on the NBM 3.8 machine.
7. If client-to-site and site-to-site are enabled before the upgrade, enable authentication rule for whichever authentication mechanism you want in the new VPN client-to-site object. For site-

to-site, install all the keys once again with all the slaves. Add the members configuration using NWAdmin.

Testing Your Configuration:

Once the configuration is over:

1. Ping the slave servers from the master. It should ping with both the tunnel and server IP address.
2. Establish a client-to-site connection in the backward compatibility mode to the NBM 3.8 server. The login should be successful and the tunnel should get established.

Can all the VPN servers be on the same eDirectory Tree?

If any of the tunnels doesn't come up properly, the eDirectory synchronization would not have happened. So do not bring up the VPN services as soon as you install NBM.

Steps to Deploy:

1. Install and configure NBM on all the servers. Do not start the VPN services.
2. Add the members to the VPN master server.
3. Check the synchronization status of the eDirectory on all the services either using the ndsiMonitor or dstrace.
4. Once the synchronization is complete start the VPN services on all the machines.

Testing Your Configuration:

1. Check the VPN servers status from the Novell Remote Manager and make sure all the servers are in up-to-date.

If Non-mandatory Steps are Missed:

The eDirectory synchronizations will not happen because of which VPN network will not come up. It will affect other services also.

What if the VPN servers are in different eDirectory trees?

Steps to Deploy:

1. Install eDirectory separately and configure the servers for VPN.

Would like to configure both client-to-site and site-to-site on the same machine?

Steps to Deploy:

1. Configure a client-to-site and site-to-site and check for the connectivity from the client and other server.

Can eDirectory support two or more VPN services simultaneously?

It is better to keep the VPN networks and VPN masters in different containers.

Can corporate resources be securely accessed using NBM and can resources among branch offices be shared securely?

If the organization has certificates for all users they can use the certificate mode of authentication. Those organizations which have eDirectory users can use NMAS for authentication. Users from different places having users in LDAP in a central location can use the NMAS LDAP method. The services also allow you to granularize authentication policy to the individual user level and traffic rules for individual user as well as individual resource level.

Testing Your Configuration:

During configuration the updated information in the eDirectory can be verified. Once a service is configured we can open eDirectory for the service using iManager/ConsoleOne or cross check eDirectory.

If Non-Mandatory Steps are Missed:

Once the information in eDirectory is updated, make sure it is read by VPN modules. Use _vpn on the server console and see the different configured services.

Impact on Services:

Usage of encryption is according to the requirement of the organization. With slow links encryption helps only for specific services.

2 NAT

This section details some of the NAT related VPN services deployment scenarios

NAT-Related Scenarios

This section details some of the NAT related VPN services deployment scenarios.

Can I use NAT for both the master and the slaves?

Use only Static NAT and ensure that it is on a separate box than the VPN master or slave.

Figure 5 NBM 3.7 without NAT

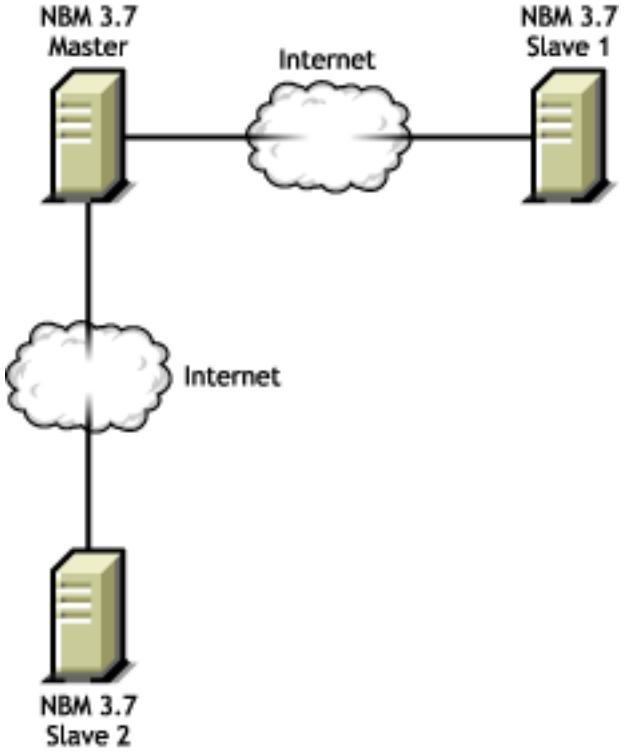
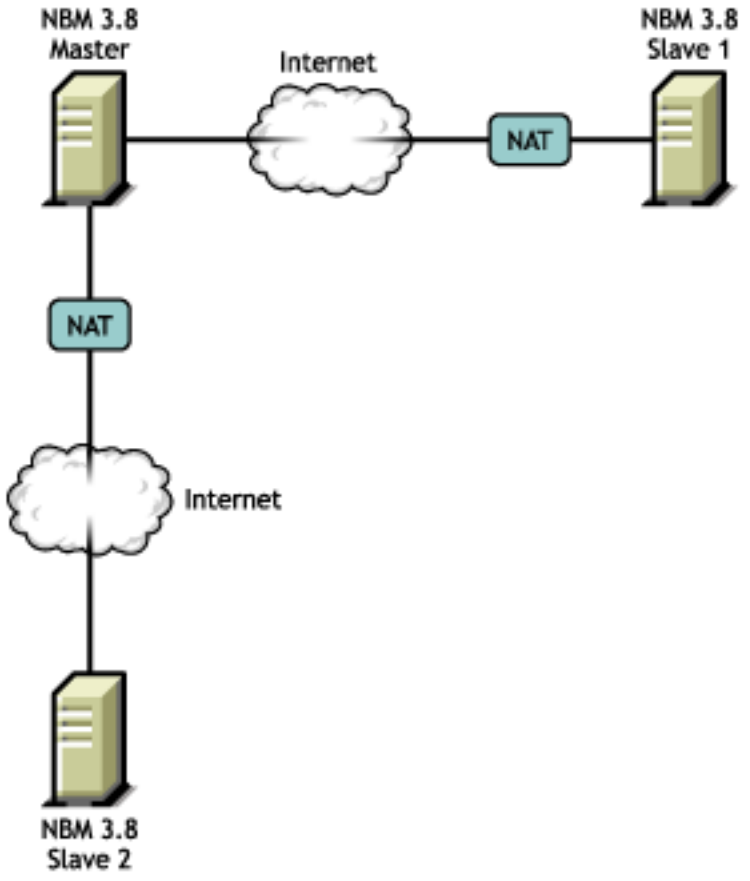


Figure 6 NBM 3.8 VPN with NAT



Steps to Deploy:

1. If you have any NBM 3.7 server in the network, you need to first upgrade all the NBM 3.7 servers to NBM 3.8 servers.
2. After that, configure the NBM 3.8 servers and ensure that they are working properly.
3. Configure the Static NAT and put the NBM 3.8 servers behind the NAT boxes.

Should I keep NAT and VPN on the same machine or on different machines?

You should always keep the NAT and VPN on separate machines.

Steps to Deploy:

1. Before configuring the VPN services on the NBM 3.8 machine, ensure that Static NAT is working.
2. Configure the VPN services on the NBM 3.8 machine with the public IP address on which the VPN service is to run.

Testing Your Configuration:

1. After configuring the Static NAT, ensure the traffic from the NAT to the VPN server is flowing properly.

What should I do to move existing VPN servers behind NAT?

You should have the NBM 3.8 as the VPN master server. If you are moving a server behind NAT make sure either any of the other master servers in the VPN network is upgraded to NBM 3.8, or move a VPN slave server behind NAT. Moving the VPN master server behind NAT has no issues.

We recommend that the VPN and NAT are on the different machines.

Steps to Deploy:

1. Configure a static NAT server by mapping the secondary IP address of the NAT server to the VPN server private IP address.
2. In the VPN server set the default route as the NAT server's private interface.
3. Reconfigure the VPN server configuration with the secondary IP address of the NAT server.
4. Ping the secondary IP address from the public machine. The traffic should get diverted to the VPN server.
5. If the VPN server moved is a VPN master server you need to create new keys by using vpncfg and should add other VPN members to this master server.

Testing Your Configuration:

1. Establish the VPN tunnel by pinging to the tunnel IP address.