Novell BorderManager®

3.9

April 05, 2007

www.novell.com

VIRTUAL PRIVATE NETWORK DEPLOYMENT FREQUENTLY ASKED QUESTIONS

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on theNovell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide

Novell® BorderManager® 3.9 includes premier firewall and VPN technologies that safeguard your network and help you build a secure identity management solution. With the powerful directory-integrated features in Novell BorderManager, you can monitor users' Internet activities and control their remote access to corporate resources.

This documentation provides answers to some of the common questions you might encounter while using the Novell BorderManager 3.9 Virtual Private Network (VPN) services.

This documentation includes the following sections:

Audience

This audience for this documentation are experienced network administrators. This document is also userful for end-users who have VPN client installed on their computers.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to Novell Feedback Web site (http://www.novell.com/documentation/feedback.html) and provide your comments.

Documentation Updates

For most recent version of the *Virtual Private Network FAQ*, visit the Novell Documentation Web site. (http://www.novell.com/documentation/nbm39/index.html)

Additional Documentation

It is recommended that you read this document as a supplement to the following other related documentation of Novell BorderManager 3.9:

- *Novell BorderManager 3.9 Administration Guide*
- *Novell BorderManager 3.9 Installation Guide*
- *Novell BorderManager 3.9 Proxy and Firewall Overview and Planning Guide*
- *Novell BorderManager 3.9 Troubleshooting Guide*
- *Novell BorderManager 3.9 Virtual Private Network Client Installation Guide*

Documentation Conventions

In Novell 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.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Common Questions on VPN Services

1

This section provides answers to some common question that you might encounter while deploying or working with Novell BorderManager VPN services.

- Do I first upgrade the master server, or upgrade the slave server?
- What if we have a mixture of Novell BorderManager 3.8 and Novell BorderManager 3.9 servers in the network?
- Can I use a third-party server in the network?
- Can I use an LDAP server which is on a different machine?
- How do I deal with slow links across different sites?
- What if I have a large number of users in a third-party server and want to configure client-to-site service?
- What if a client is connected to the ISP through dial-up with dynamic NAT at the ISP?
- How can I restrict the users to access only some of my internal networks based on their access level for VPN client-to-site?
- How do I upgrade the existing Novell BorderManager 3.8 servers to the latest version?
- Can all the VPN servers be on the same eDirectory tree?
- What if the VPN servers are in different eDirectory trees?
- Can I configure both client-to-site and site-to-site on the same machine?
- Can eDirectory support two or more VPN services simultaneously?
- Can corporate resources be securely accessed using Novell BorderManager. Also, can resources among branch offices be shared securely?

1.1 Do I first upgrade the master server, or upgrade the slave server?

First, upgrade the master on the server.

You can upgrade the client at any time, irrespective of whether the server is upgraded or not.

1.2 What if we have a mixture of Novell BorderManager 3.8 and Novell BorderManager 3.9 servers in the network?

The master should always be Novell BorderManager 3.9, and should be configured for both certificate and pre-shared key methods of authentication.

Deployment

To deploy the servers:

1. Configure the Novell BorderManager 3.9 slave with certificate method of authentication.
2. Configure the Novell BorderManager 3.9 slave with both certificate and pre-shared key methods of authentication.

Testing your Configuration

1. Exchange packets between the master and the Novell BorderManager 3.8 with the certificate method of authentication enabled.
2. Exchange the packets among the Novell BorderManager 3.8 slaves with the certificate method of authentication enabled.
3. Exchange packets between the Novell BorderManager 3.9 slave and the Novell BorderManager 3.8 slave with certificate method of authentication enabled.
4. Exchange packets among the Novell BorderManager 3.9 salves with the certificate method of authentication enabled.
5. Exacting packets between the master and the Novell BorderManager 3.9 slave with the pre-shared key method of authentication enabled.

1.3 Can I use a third-party server in the network?

Yes. You can use a third-party server in the network.

To deploy, configure the Novell BorderManager network and then, configure the third-party server.

For more information on third-party servers, see the Novell Cool Solutions Web site. (http://www.novell.com/coolsolutions/)

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

Yes. You can use an LDAP server which is on a different machine. However, before using LDAP with VPN, ensure that LDAP is working properly.

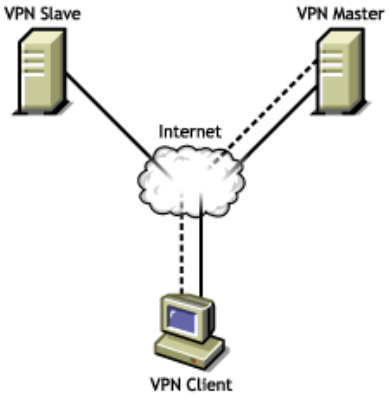
To deploy, collect the IP address and other details of your LDAP server and provide them in the client-to-site details.

1.5 How do I deal with slow links across different sites?

Use traffic rules to restrict the traffic.

By default, the VPN traffic rule encrypts all the packets going out for the client and sends them to the VPN server. This adds unnecessary load to the tunnel.

Figure 1-1 *Slow Links*



Deployment

Do the following to deploy:

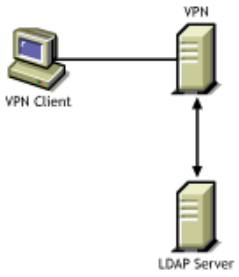
1. Configure the client-to-site and site-to-site services.
2. In the client-to-site policy, add traffic rules to encrypt traffic only for particular protocol or network.
3. Add site-to-site protected network traffic rules with only protected networks as the destination.

IMPORTANT: If the traffic rules are not added, all the traffic passes through the VPN tunnel.

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

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

Figure 1-2 *Large number of users*



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.

IMPORTANT: If the full distinguished name of the LDAP entity (user or group) is not provided, the authentication does not succeed.

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

Configure the Windows machines to have dial-up.

The dial-up connection can be made in two ways:

- Dialup and connect to the VPN server.
- Use the dial-up client embedded in the VPN client.

Figure 1-3 *Dynamic NAT*

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

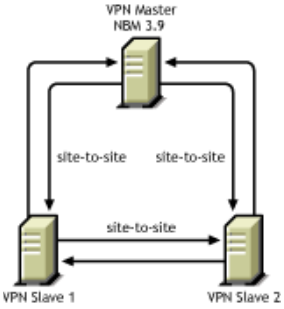
Novell BorderManager 3.9 provides various parameters through which you can restrict access to internal networks.

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

1.9 How do I upgrade the existing Novell BorderManager 3.8 servers to the latest version?

First, upgrade the master VPN server and then, upgrade the other VPN servers.

Figure 1-4 *Upgrading existing servers*



To deploy, ensure that the minimum requirements to install Novell BorderManager 3.9 are met.

For the minimum requirements, see "System Requirements" in the *Novell BorderManager 3.9 Installation Guide.*

1. Complete the installation by choosing to install VPN and other components that you want to install.
2. Run `VPNCFG` on the Novell BorderManager 3.9 machine.
3. If the client-to-site and site-to-site services are enabled before the upgrade, enable authentication rule for the pre-shared key method of authentication for the new VPN client-to-site object.

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

Testing your Configuration

Do the following to test your configuration:

1. After the configuration is complete, 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 Novell BorderManager 3.9 server. The login should now be successful and the tunnel should now be established.

1.10 Can all the VPN servers be on the same eDirectory tree?

eDirectory™ synchronization does not happen if any of the tunnels do not come up properly. It is recommended that you do not bring up the VPN services as soon as you install Novell BorderManager.

Deployment

Do the following to deploy:

1. Install and configure Novell BorderManager on all the servers.

   NOTE: 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. Start the VPN services on all the machines after the synchronization is complete.

To test your configuration, verify the VPN servers status from the Novell Remote Manager and make sure all the servers are in up-to-date.

IMPORTANT: If the eDirectory synchronization fails, VPN network does not come up. It affects other services too.

1.11 What if the VPN servers are in different eDirectory trees?

Install eDirectory separately and configure the servers for VPN.

1.12 Can I configure both client-to-site and site-to-site on the same machine?

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

1.13 Can eDirectory support two or more VPN services simultaneously?

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

1.14 Can corporate resources be securely accessed using Novell BorderManager. Also, can resources among branch offices be shared securely?

- If an 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 or cross check eDirectory.

IMPORTANT: 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.

Network Address Translation Issues

2

This section details some of the Network Address Translation (NAT) related VPN services deployment scenarios.

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

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

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

Figure 2-1 *Novell BorderManager 3.8 without NAT*

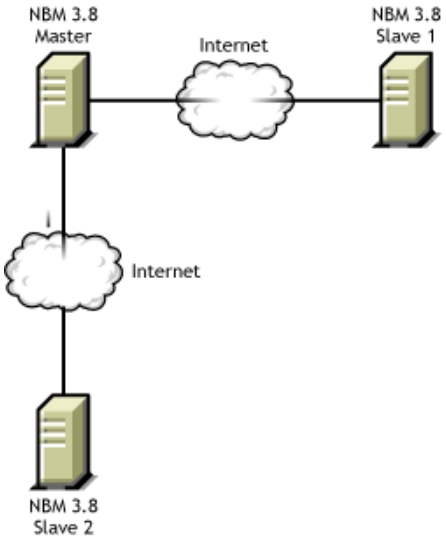
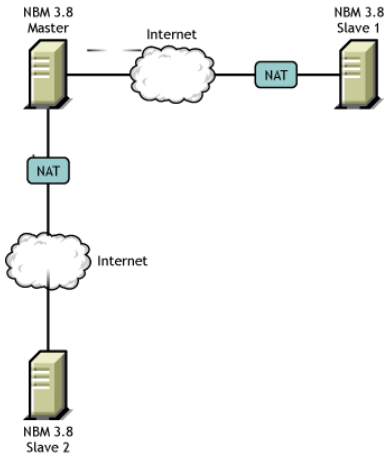


Figure 2-2 *Novell BorderManager 3.9 VPN with NAT*



Deployment

1. Upgrade all the Novell BorderManager 3.8 servers to Novell BorderManager 3.9 servers.
2. Configure the Novell BorderManager 3.9 servers and ensure that they are working properly.
3. Configure the Static NAT and put the Novell BorderManager 3.9 servers behind the NAT boxes.

2.2 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.

Deployment

1. Before configuring the VPN services on the Novell BorderManager 3.8 machine, ensure that Static NAT is working.
2. Configure the VPN services on the Novell BorderManager 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.

2.3 How do I move the existing VPN servers behind NAT?

You should have Novell BorderManager 3.9 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 Novell BorderManager 3.9, or move a VPN slave server behind NAT.

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

Deployment

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.