AUTHORIZED DOCUMENTATION

SSL VPN Server Guide

Novell® Access Manager

3.1 SP1

March 17, 2010

www.novell.com

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 deliverable 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.
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

The Novell® Access Manager SSL VPN uses encryption and other security mechanisms to ensure that the data cannot be intercepted and only authorized users have access to the network. Users can access SSL VPN services from any Web browser. This guide has the following information:

Audience

This guide is intended for Access Manager administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

- Extensible Markup Language (XML)
- Simple Object Access Protocol (SOAP)
- Security Assertion Markup Language (SAML)
- Public Key Infrastructure (PKI) digital signature concepts and Internet security
- Secure Socket Layer/Transport Layer Security (SSL/TSL)
- Hypertext Transfer Protocol (HTTP and HTTPS)
- Uniform Resource Identifiers (URIs)
- Domain Name System (DNS)
- Web Services Description Language (WSDL)

Feedback

We want to hear your comments and suggestions about this guide 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 Documentation Feedback (http://www.novell.com/documentation/feedback.html) at www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell Access Manager SSL VPN Server Guide*, visit the Novell Access Manager Documentation Web site (http://www.novell.com/documentation/novellaccessmanager).

Additional Documentation

- *Novell Access Manager 3.1 SP1 Installation Guide*
- *Novell Access Manager 3.1 SP1 Setup Guide*

- *Novell Access Manager 3.1 SP1 Quick Starts*
- *Novell Access Manager 3.1 SSL VPN User Guide*

For information about the other Access Manager devices and features, see the following:

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.

Overview of SSL VPN

The Novell® Access Manager SSL VPN uses Secure Sockets Layer (SSL) as the underlying security protocol for network transmissions. It uses encryption and other security mechanisms to ensure that the data cannot be intercepted and only authorized users have access to the network. Users can access SSL VPN services from any Web browser.

This section has the following information:

SSL VPN Features

1

Novell® SSL VPN comes with a number of key features that make the product secure, easy to access, and reliable.

Browser-Based End User Access

Novell SSL VPN has browser-based end user access that does not require users to preinstall any components on their machines. Users can access the SSL VPN services from any Web browser, from their personal computers, laptop, or from an Internet kiosk.

When users access SSL VPN through the Web browser, they are prompted to authenticate. On successful authentication, a Java* applet or an ActiveX* control is delivered to the client, depending on the browser. This establishes a secure tunnel between the user's machine and the SSL VPN server.

Support on Linux, Macintosh, and Windows

The SSL VPN client is supported on Linux, Macintosh*, and Windows* environments. For a complete list of operating software and browsers that are supported by SSL VPN, see "Client Machine Requirements" in the *Novell Access Manager 3.1 SSL VPN User Guide*.

Support on 64-Bit Clients

Enterprise mode SSL VPN can be installed on 64-bit client configurations.

High and Low Bandwidth Versions

Novell SSL VPN comes in high and low bandwidth versions. The default low bandwidth SSL VPN server is restricted to 249 simultaneous user connections and a transfer rate of 44 Mbits per second because of export restrictions.

If the export law permits, you can install the high bandwidth SSL VPN RPM to get the high bandwidth capabilities, because that version does not have connection and performance restrictions. You can order the high bandwidth SSL VPN key at no extra cost. It is also essential to have the high bandwidth SSL VPN if you want to cluster the SSL VPN servers.

For more information on how to order and install the high bandwidth SSL VPN, and to upgrade the high bandwidth version to the latest build, see Section 4.5, "Installing the RPM Containing Key For High Bandwidth SSL VPN," on page 41.

Traditional and ESP-Enabled Installation

You can install SSL VPN in two ways.

- As an ESP-enabled SSL VPN, which is installed with the Identity Server and the Administration console.
- As a Traditional SSL VPN, which is installed with the Identity Server, Administration Console, and the Access Gateway.

For more information on these methods, see Chapter 2, “Traditional and ESP-Enabled SSL VPNs,” on page 19.

Enterprise and Kiosk Modes for End User Access

The Novell SSL VPN uses both clientless and thin-client access methods. The clientless method is called the Kiosk mode SSL VPN and the thin-client method is called the Enterprise mode SSL VPN.

In Enterprise mode, all applications, including those on the desktop and the toolbar, are enabled for SSL, regardless of whether they were opened before or after connecting to SSL VPN. In this mode, a thin client is installed on the user’s workstation, and the IP Forwarding feature is enabled by default. For more information on Enterprise mode, see Section 3.1, “Enterprise Mode,” on page 23

In Kiosk mode, only a limited set of applications enabled for SSL VPN. In Kiosk mode, applications that were opened before the SSL VPN connection was established are not enabled for SSL. For more information on Kiosk mode, see Section 3.2, “Kiosk Mode,” on page 25.

As SSL VPN server administrators, you can decide which users can connect in Enterprise mode and which users can connect in Kiosk mode, depending on the role of the user. Or you can let the client decide the mode in which the SSL VPN connection is made. For more information on how to do this, see Chapter 15, “Configuring How Users Connect to SSL VPN,” on page 101. Enterprise mode is available to a user who has the administrator right in a Windows workstation or a `root` user privilege on Linux or Macintosh workstations, and if the user does not have administrator rights or `root` user privileges for that workstation, the SSL VPN connection is made in Kiosk mode.

Customized Home and Exit Pages for End Users

The home page and the exit page of SSL VPN can be customized to suit the needs of different customers. For more information, see Section 15.5, “Customizing SSL VPN User Interface,” on page 104.

Clustering SSL VPN Servers

The SSL VPN servers can be clustered to provide load balancing and fault tolerance, When you form a cluster of SSL VPN servers, all members of a cluster should belong to only one type of SSL VPN and they should all be running the high bandwidth SSL VPN. For example, all the members of a cluster should belong to either the ESP-enabled SSL VPN or the traditional SSL VPN. For more information on SSL VPN clustering, see Part IV, “Clustering the High Bandwidth SSL VPN Servers,” on page 121.

End-Point Security Checks

The Novell SSL VPN has a set of policies that can be configured to protect your network and applications from clients that are using insufficient security restraints and also to restrict the traffic based on the role of the client.

You can configure a client integrity check policy to run a check on the client workstations before establishing a tunnel to SSL VPN server. This check ensures that the users have specified software installed and running in their systems. Each client is associated with a security level, depending on the assessment of the client integrity check and the relevant traffic policies are assigned. For more information on configuring end-point security, see Chapter 14, “Configuring End-Point Security and Access Policies for SSL VPN,” on page 89.

Ability to Order Rules

If you have configured more than one rule for a user's role, the rule that is placed first is applied first. Novell SSL VPN allows you to change the order of rules by dragging and dropping them, based on their priority. For more information on rule ordering in SSL VPN, see Section 14.3.2, "Rule Ordering," on page 99.

Ability to Import and Export Policies

Novell SSL VPN allows you to export the existing configuration into an XML file through the Administration Console. You can reimport this configuration later. This is a very useful feature when you upgrade your servers from one version to another. For more information, see Section 14.3.3, "Exporting and Importing Traffic Policies," on page 100

Desktop Cleanup Feature

When a user accesses the protected resource from outside by using SSL VPN, it also means that the sites that the user visited are stored in the browser history, or some sensitive information is stored in the cache or cookies. This is a potential security threat if it is not properly dealt with. The Novell SSL VPN client comes with the desktop cleanup feature, so the user has the option to delete all the browser history, cache, cookies, and files from the system, before logging out of the SSL VPN connection.

If the user uses Firefox* to connect to SSL VPN, the browsing data that was stored after the SSL VPN connection was made is deleted. In Internet Explorer*, all the browser data is deleted including the data that was stored before the SSL VPN session was established.

Sandbox Feature

When you connect to SSL VPN in either Kiosk mode or Enterprise mode, a folder named VPN-SANDBOX is created on your desktops can manually copy any files that you download from your corporate network or any other files into this folder. This folder is automatically deleted along with its contents when the user logs out of the SSL VPN connection. For more information on the sandbox feature of SSL VPN, see "Sandbox Feature" in the *Novell Access Manager 3.1 SSL VPN User Guide*.

Custom Login Policy

When custom login policy is configured, SSL VPN redirects the custom login requests to different URLs based on the policy. This is a very useful feature if users want to access applications such as those on the Citrix* application servers. For more information on how to configure a custom login policy, see Section 15.4, "Configuring a Custom Login Policy for SSL VPN," on page 103.

Traditional and ESP-Enabled SSL VPNs

2

The Novell® SSL VPN can be deployed as either an ESP-enabled SSL VPN or a Traditional SSL VPN.

When SSL VPN is deployed without the Access Gateway, an Embedded Service Provider (ESP) component is installed along with the SSL VPN server. This deployment requires the Identity Server and the Administration server to also be installed. This type of deployment is called an ESP-enabled Novell SSL VPN.

When SSL VPN is deployed with the Access Gateway, it is called a Traditional Novell SSL VPN. In this type of installation, SSL VPN is deployed with the Identity Server, Administration Console, and the Linux Access Gateway components of Novell Access Manager.

2.1 ESP-Enabled Novell SSL VPN

In ESP-enabled Novell SSL VPN, the process involved in establishing a secure connection between a client machine and the different components of Novell Access Manager is as follows:

1. The user specifies the following URL to access the SSL VPN server:

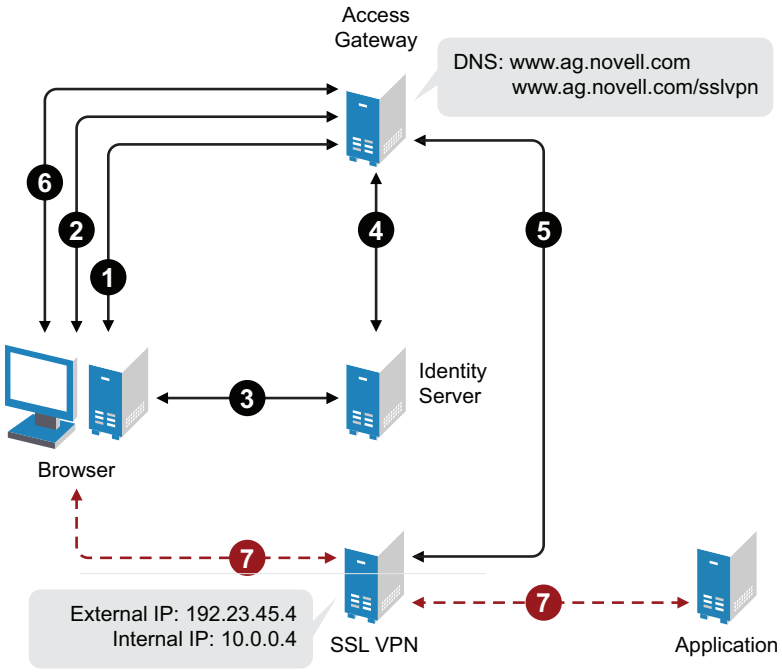
   https://<*www.sslvpn.novell.com*>/sslvpn/login

   <*www.sslvpn.novell.com*> is the DNS name of the SSL VPN server, and /sslvpn/login is the path of the SSL VPN server.
2. The SSL VPN redirects the browser to the Identity Server for authentication.
3. After successful authentication, the Identity Server redirects the browser back to SSL VPN.
4. The Identity Server propagates the session information to the SSL VPN server through the Embedded Service Provider.
5. The SSL VPN server injects the SSL VPN policy for that user into the SSL VPN servlet. The SSL VPN servlet processes the parameters and sends the policy information back to the server.
6. The SSL VPN checks if the client machine has sufficient security restraints. For more information on client integrity checks, see Chapter 14.1, “Configuring Policies to Check the Integrity of Client Machine,” on page 90.
7. When the user accesses the applications behind the protected network, the connection goes through the secure tunnel formed with the SSL VPN server.
8. The browser stays open throughout the SSL VPN connection to allow the keep-alive packets.
9. When the user clicks the logout button to close the SSL VPN session, all the client components are automatically uninstalled from the workstation.

2.2 Traditional Novell SSL VPN

The following figure shows the Novell Access Manager components and the process involved in establishing a secure connection between a client machine and traditional Novell SSL VPN server. In this type of deployment, the Linux Access Gateway accelerates and protects the SSL VPN server.

Figure 2-1 *Traditional Novell SSL VPN*



1. The user specifies the following URL to access the SSL VPN server:

   https://<*www.ag.novell.com*>/sslvpn/login

   <*www.ag.novell.com*> is the DNS name of the Access Gateway that accelerates the SSL VPN server, and /sslvpn/login is the path of the SSL VPN server.
2. The Access Gateway redirects the user to the Identity Server for authentication, because the URL is configured as a protected resource.
3. The Identity Server authenticates the user's identity.
4. The Identity Server propagates the session information to the Access Gateway through the Embedded Service Provider.
5. The Access Gateway injects the SSL VPN policy for that user into the SSL VPN servlet. The SSL VPN servlet processes the parameters and sends the policy information back to the Access Gateway.
6. The SSL VPN checks if the client machine has sufficient security restraints. For more information on client integrity checks, see Chapter 14.1, "Configuring Policies to Check the Integrity of Client Machine," on page 90.

7. One of the following actions takes place depending on the mode of SSL VPN connection:
   - In Enterprise mode, a tunnel interface is created and is bound with the tunnel IP address assigned by the SSL VPN server. A secure tunnel is established between the client machine and the SSL VPN server and the routing table is updated with the protected network configuration.
   - In Kiosk mode, a secure tunnel is established between the client machine and the SSL VPN server and the protected network configuration is pushed to the client.
8. When the user accesses the applications behind the protected network, the connection goes through the secure tunnel formed with the SSL VPN server and not through the Access Gateway.
9. Keep the browser open throughout the SSL VPN connection to allow the keep-alive packets to go through the Access Gateway.
10. When the user clicks the logout button to close the SSL VPN session, all the client components are automatically uninstalled from the workstation.

2.3 High and Low Bandwidth SSL VPNs

Novell SSL VPN comes in high and low bandwidth versions.

Low Bandwidth Version: The default SSL VPN server is a low bandwidth version. It is restricted to 249 simultaneous user connections and a transfer rate of 44 Mbits per second because of export restrictions.

High Bandwidth Version: The high bandwidth version does not have the connection and performance restrictions. It is also essential to have the high bandwidth SSL VPN installed if you want to cluster the SSL VPN servers.

If the export law permits, you can order the high bandwidth SSL VPN RPM to get the high bandwidth capabilities at no extra cost. After the export controls have been satisfied, the order will be fulfilled. You can install the high bandwidth SSL VPN RPM on both the traditional Novell SSL VPN server and on the ESP-enabled Novell SSL VPN server.

Your regular Novell sales channel can determine if the export law allows you to order the high bandwidth version at no extra cost.

For more information on how to order and install the high bandwidth SSL VPN, and to upgrade the high bandwidth version to the latest build, see Section 4.5, “Installing the RPM Containing Key For High Bandwidth SSL VPN,” on page 41.

SSL VPN Client Modes

3

Novell SSL VPN has two client modes, Enterprise mode and Kiosk mode. In Enterprise mode, which is available for users who have administrative privileges, all applications are enabled for SSL VPN. In Kiosk mode, only a limited set of applications are enabled for SSL VPN.

Enterprise mode is available to a user who has the administrator right in a Windows workstation or a `root` user privilege on Linux or Macintosh workstations. If the user does not have administrator rights or `root` user privileges for that workstation, the SSL VPN connection is made in Kiosk mode.

For more information on the client platforms and setups tested by Novell, see Access Manager 3.1 Support Pack 1 SSLVPN integration testing report (http://www.novell.com/support/viewContent.do?externalId=7004342&sliceId=1).

3.1 Enterprise Mode

In Enterprise mode, all applications, including those on the desktop and the toolbar, are enabled for SSL, regardless of whether they were opened before or after connecting to SSL VPN. In this approach, a thin client is installed on the user’s workstation. In Enterprise mode, the IP Forwarding feature is enabled by default.

Enterprise mode is recommended for devices that are managed by an organization, such as a laptop provided by the organization for its employees. Enterprise mode supports the following:

- Protocols such as TCP, UDP, ICMP, and NetBIOS.
- Applications that open TCP connections on both sides, such as VoIP and FTP.
- Enterprise applications such as CRM and SAP*.
- Applications such as Windows File Sharing systems, the Novell Client™, and Novell SecureLogin.

You can configure a user to connect only in Enterprise mode, depending on the role of the user. For more information, see Section 15.1, “Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode,” on page 101.

NOTE: If you have configured a user to connect in Enterprise mode only and that user does not meet the prerequisites, then, the SSL VPN connection fails with an appropriate error message if using the applet-based Web browser, or a blank screen if an ActiveX-based Web browser is used.

This section has the following information:

3.1.1 Prerequisites

A user can access SSL VPN in Enterprise mode if the user is:

- An administrator or a `root` user of the machine. or a Super user or an Administrator user in Windows Vista* user.
- A non-admin or a non-`root` user who knows the credentials of the administrator or `root` user, or a standard user in Windows Vista.
- The SSL VPN client components are preinstalled on the user's machine.

3.1.2 User Scenarios

This section has the following information:

- "Scenario 1: User Is the Admin or Root User of the Machine" on page 24
- "Scenario 2: User Is the Non-Admin or Non-Root User of Machine and Knows the Admin or Root Credentials" on page 24
- "Scenario 3: The User Is a Non-Admin or Non-Root User, but the Client Components are Preinstalled on the Machine" on page 25

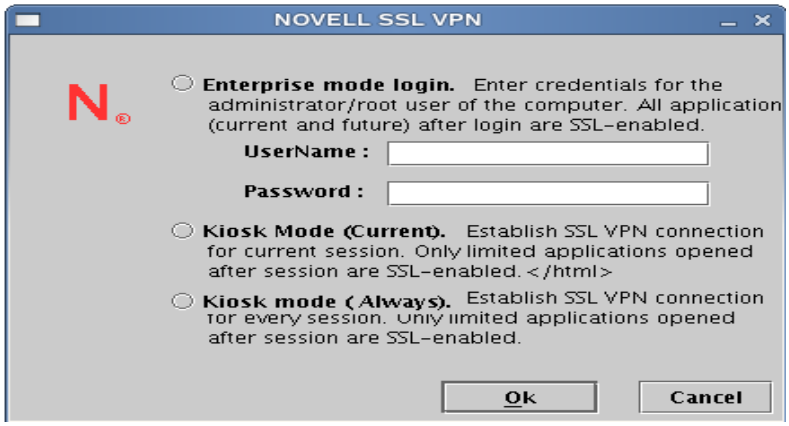
Scenario 1: User Is the Admin or Root User of the Machine

When the user is an administrator or a `root` user of the machine, the tool identifies the user as the admin or `root` user and Enterprise mode is enabled by default after the user specifies the credentials in the Access Manager page. An admin or a `root` user can connect to SSL VPN only in Enterprise mode unless the system administrator configures the user to connect in Kiosk mode only. For more information on how to configure users for Kiosk mode only, see Section 15.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 101.

Scenario 2: User Is the Non-Admin or Non-Root User of Machine and Knows the Admin or Root Credentials

A non-admin or a non-`root` user can access SSL VPN in Enterprise mode if the user knows the administrator or `root` user credentials. When a non-admin or a non-`root` user connects to SSL VPN, the user is prompted to specify the credentials on the Access Manager page. The tool identifies that the credentials supplied are those of the non-admin or a non-`root` user and displays the following dialog box.

Figure 3-1 *SSL VPN dialog box*



The user must specify the username and password of the administrator or the `root` user of the machine in the dialog box, then click *OK* to enable Enterprise mode.

Enterprise mode is enabled by default in the subsequent sessions and the user is not prompted again for the administrator or `root` username and password.

Non-admin or non-`root` users who have connected to SSL VPN in Enterprise mode can connect to SSL VPN in Kiosk mode on the same machine. For more information, see "Switching from Enterprise Mode to Kiosk Mode" in the *Novell Access Manager 3.1 SSL VPN User Guide*.

NOTE: Users cannot switch from one mode to another if you have configured them to connect in one mode only.

Scenario 3: The User Is a Non-Admin or Non-Root User, but the Client Components are Preinstalled on the Machine

If a non-admin or a non-`root` user wants to install SSL VPN in Enterprise mode, you can preinstall the SSL VPN client components on the user's machine. For more information, see Chapter 6, "Preinstalling the SSL VPN Client Components," on page 53. When non-admin or non-`root` users access the client components from a workstation that has the SSL VPN client components preinstalled, the users are not prompted to enter the credentials of the admin user or `root` user.

The users are connected to SSL VPN in Enterprise mode after they specify their credentials on the Access Manager login page.

3.2 Kiosk Mode

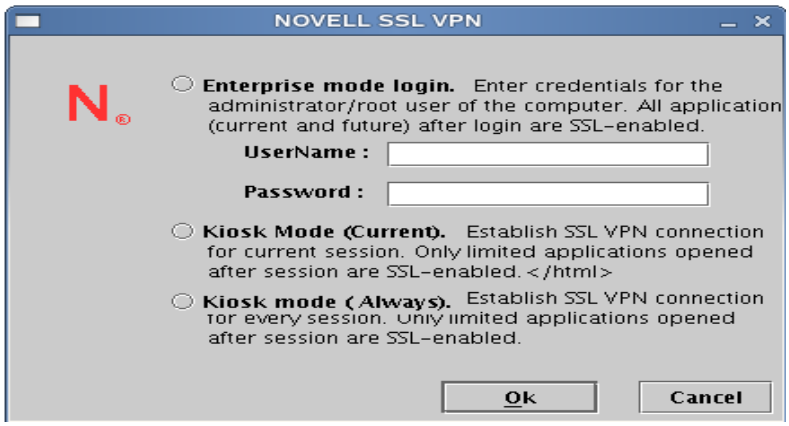
In Kiosk mode, only a limited set of applications are enabled for SSL VPN. A non-admin user, a non-`root` user, or a standard user in Windows Vista can connect to SSL VPN in Kiosk mode if he or she does not have administrator access. In Kiosk mode, applications that were opened before the SSL VPN connection was established are not SSL-enabled.

Kiosk mode supports TCP and UDP applications only. This mode is better suited for machines that are not managed by an organization, such as home computers and computers in Web browsing kiosks.

You can configure a user to connect in Kiosk mode only. When you have done so, a user is connected to SSL VPN in Kiosk mode after the user provides credentials in the Novell Access Manager login page. For more information, see Section 15.1, “Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode,” on page 101.

If you have left the mode selection to the client and when a user logs in to the SSL VPN client as a non-admin or non-`root` user, the following dialog box is displayed:

Figure 3-2 *SSL VPN dialog box*



The user can do one of the following to load the Kiosk mode:

- Click *Ignore* to connect to SSL VPN in Kiosk mode for that particular session. The user is prompted again to provide the administrator or the root username and password during the next login.
- Click *Ignore Forever* to connect to SSL VPN in Kiosk mode in the current session, as well as in subsequent sessions.

A user who has clicked *Ignore Forever* can still connect to SSL VPN in Enterprise mode in the next session. For more information, see “Switching from Kiosk Mode to Enterprise Mode” in *Novell Access Manager 3.1 SSL VPN User Guide*.

NOTE: When a non-admin user uses Internet Explorer to establish an SSL VPN connection, the ActiveX download fails. This happens because ActiveX requires admin rights to download.This issue might also occur if you have upgraded from an older version. If a user wants to access SSL VPN with Internet Explorer, use the following URL:

https:<*DNS-Name*>/sslvpn/login?forcejre=true

For more information, see Section 15.3, “Configuring SSL VPN to Download the Java Applet on Internet Explorer,” on page 103.

Installing and Deploying the SSL VPN Server

The Novell® SSL VPN can be installed as an ESP-enabled SSL VPN, or as a Traditional SSL VPN along with the Access Gateway. You can also install the high bandwidth version of SSL VPN if export laws permit.

If you already have SSL VPN servers installed, you can upgrade your servers to the Traditional SSL VPN. You cannot upgrade the 3.0 version of SSL VPN to the 3.1 version of ESP-enabled SSL VPN.

The following sections discuss different installation, upgrade, and uninstallation steps for SSL VPN:

Installing the SSL VPN Server

4

You can deploy SSL VPN either as a Traditional SSL VPN or as an ESP-enabled SSL VPN.

4.1 Prerequisites

The SSL VPN server requires the following software and hardware:

- ❑ 100 MB of disk space
- ❑ Network interface card
- ❑ SUSE®Linux Enterprise Server (SLES) 10 SP2 or SP3
- ❑ `gettext` package
- ❑ All ports used by SSL VPN must be opened. By default, SSL VPN uses TCP port 443 or 7777, and 7778.

  NOTE: Port 7778 is not required if UDP is selected on port 7777 or 443.
- ❑ You have root privileges.
- ❑ You have the following information:
  - IP address of the SSL VPN server
  - IP address of the Administration Console
- ❑ You have downloaded the relevant RPMs from the Novell® Download site or you have the install CD.

4.2 Limitations With 64-Bit Software

SSL VPN has the following limitations, if the client or the server is running the 64-bit platforms:

- ❑ No Kiosk Mode Support for 64-bit Clients
- ❑ In Enterprise mode, if the clients are running 64-bit operating software, they cannot use 64-bit browsers to establish the SSL VPN connection.

4.3 Installing ESP-Enabled SSL VPN

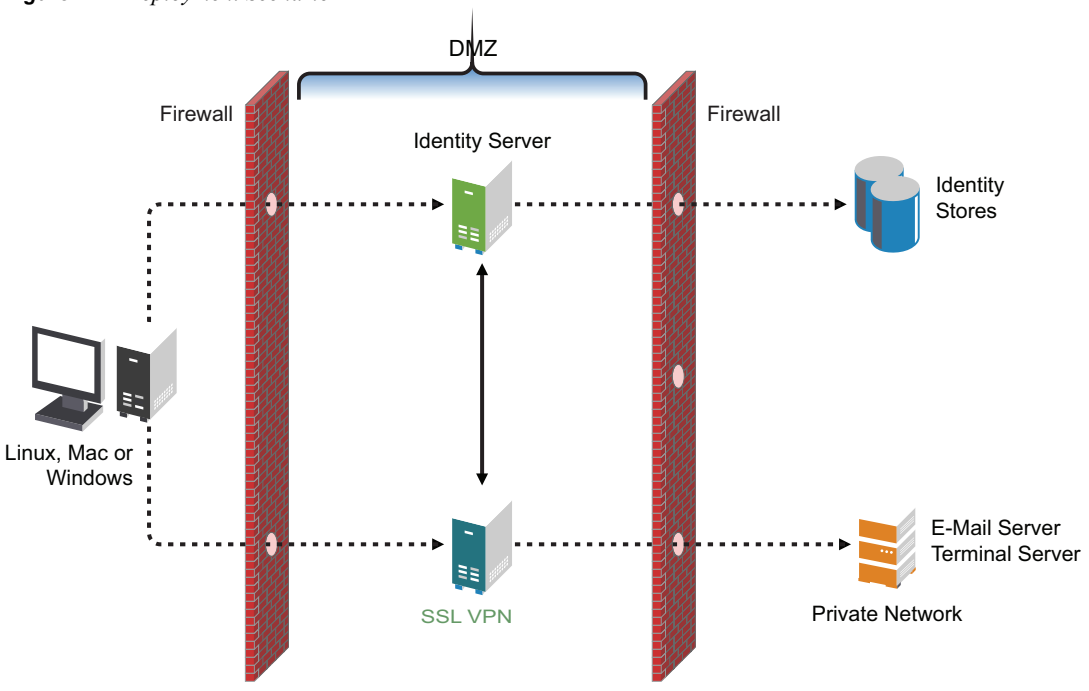
When SSL VPN is deployed without the Access Gateway, an Embedded Service Provider (ESP) component is installed along with the SSL VPN server. This requires the Identity Server and the Administration server to also be installed. This deployment is called an ESP-enabled Novell SSL VPN.

4.3.1 Deployment Scenarios

For installing the ESP-Enabled version of SSL VPN, you have the following deployment scenarios:

Deployment Scenario 1: Installing SSL VPN on a Separate Machine

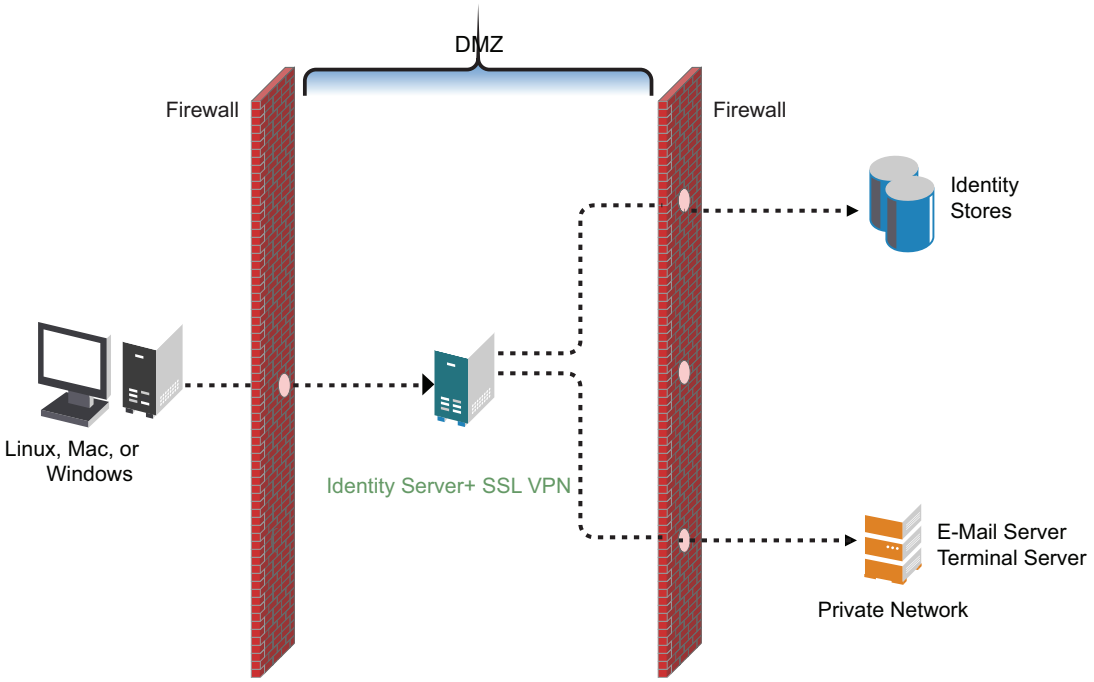
Figure 4-1 *Deployment Scenario 1*



This deployment scenario consists of a demilitarized zone, where the Identity Server and SSL VPN are deployed separately, without the Access Gateway. For installation instructions for this scenario, see Section 4.3.2, “Installing the ESP-Enabled SSL VPN,” on page 33.

Deployment Scenario 2: Installing SSL VPN and the Identity Server on the Same Machine

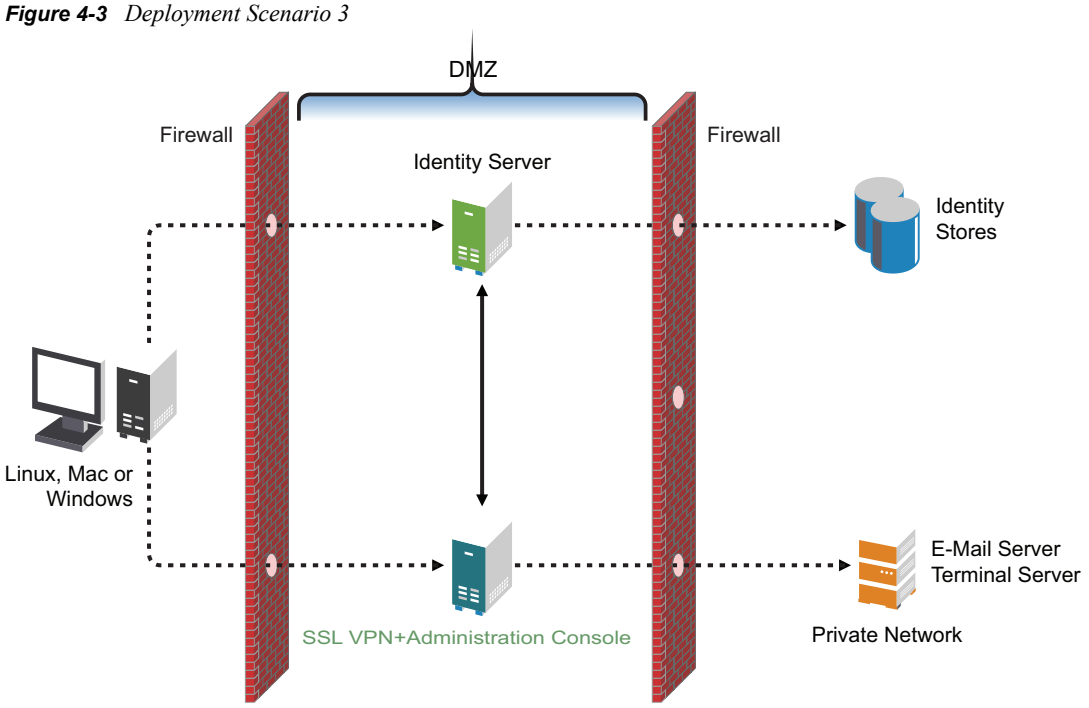
Figure 4-2 *Deployment Scenario 2*



This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on a single machine. The Access Gateway is deployed separately. For installation instructions for this scenario, see Section 4.3.2, “Installing the ESP-Enabled SSL VPN,” on page 33.

Deployment Scenario 3: Installing SSL VPN and the Administration Console on the Same Machine

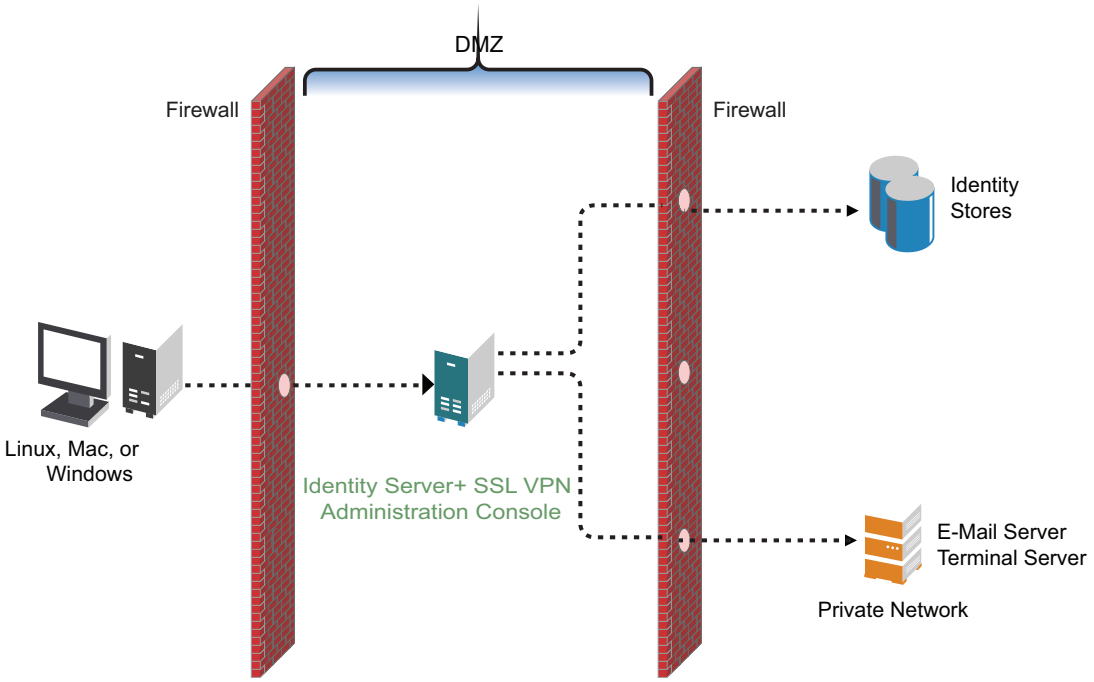
Figure 4-3 *Deployment Scenario 3*



This deployment scenario consists of a demilitarized zone where the SSL VPN, and Administration Console are on the same machine and the Linux Access Gateway and the Identity servers are deployed separately. For installation instructions for this scenario, see Section 4.3.2, “Installing the ESP-Enabled SSL VPN,” on page 33.

Deployment Scenario 4: Installing SSL VPN, the Administration Console and the Identity server on the Same Machine

Figure 4-4 *Deployment Scenario 4*



This deployment scenario consists of a demilitarized zone where the Identity Server, SSL VPN, and Administration Console are on the same machine and the Linux Access Gateway is deployed separately. For installation instructions for this scenario, see Section 4.3.2, “Installing the ESP-Enabled SSL VPN,” on page 33.

4.3.2 Installing the ESP-Enabled SSL VPN

The following installation steps are applicable to all the deployment scenarios for ESP-enabled SSL VPN. The individual scenarios are explained in Section 4.3.1, “Deployment Scenarios,” on page 30.

1. Do one of the following:
   - Insert the CD into the CD drive, then locate `install.sh`.
   - Untar the RPMs.
2. At a command prompt, enter the following install script command:

   ```
   ./install.sh
   ```

   You are prompted to select an installation.
3. Type 4 to install the ESP-Enabled SSL VPN, then press Enter.
4. Optional When you are prompted to replace the low bandwidth SSL VPN RPM with the high bandwidth RPM, replace it if the security law permits you to do so.

   For more information on the high bandwidth SSL VPN, see “High and Low Bandwidth Versions” on page 15. For more information on installing the high bandwidth SSL VPN, see Section 4.5, “Installing the RPM Containing Key For High Bandwidth SSL VPN,” on page 41.

5 Review and accept the License Agreement.

6 (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server when you are prompted to do so.

7 Specify the name of the administrator for the Administration Console.

8 Specify the administration password.

9 Confirm the password.

10 (Conditional) If you are installing the SSL VPN server on the same machine as the Administration Console, you are not prompted for the IP address of the Administration Console. If the Administration Console is on a different machine, provide the IP address when you are prompted for it.

11 Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.

The installation ends with the following message: `Installation complete.`

12 To verify the installation of the SSL VPN, continue with Section 4.7, "Verifying That Your SSL VPN Service Is Installed," on page 42.

4.4 Installing the Traditional Novell SSL VPN

When SSL VPN is deployed with the Access Gateway, it is called a Traditional Novell SSL VPN. In this type of installation, SSL VPN is deployed with the Identity Server, Administration Console, and the Linux Access Gateway components of Novell Access Manager.

You can install the Traditional Novell SSL VPN either with the Linux Access Gateway on the same machine or with the Identity Server, or you can install the Linux Access Gateway, Identity Server, and SSL VPN on three different machines.

The following sections describe the different deployment scenarios that are available for the traditional Novell SSL VPN and also documents the installation steps:

- Section 4.4.1, "Deployment Scenarios," on page 34
- Section 4.4.2, "Installing the Traditional Novell SSL VPN," on page 38

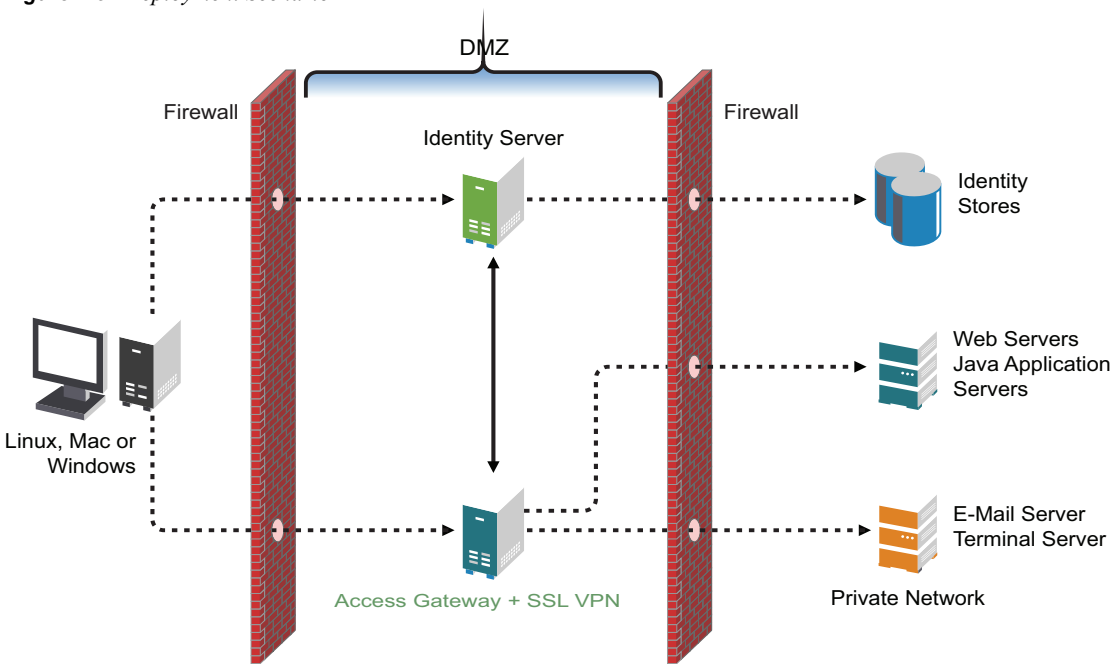
4.4.1 Deployment Scenarios

The Novell SSL VPN can interoperate with the Access Gateway in different ways. Some of the deployment scenarios are:

- "Deployment Scenario 1: Linux Access Gateway and SSL VPN on the Same Server" on page 35
- "Deployment Scenario 2: SSL VPN Server Installed on a Separate Machine" on page 35
- "Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server" on page 36
- "Deployment Scenario 4: Novell Administration Console and SSL VPN on the Same Server" on page 37
- "Deployment Scenario 5: Administration Console, Identity Server, and SSL VPN on the Same Server" on page 38

Deployment Scenario 1: Linux Access Gateway and SSL VPN on the Same Server

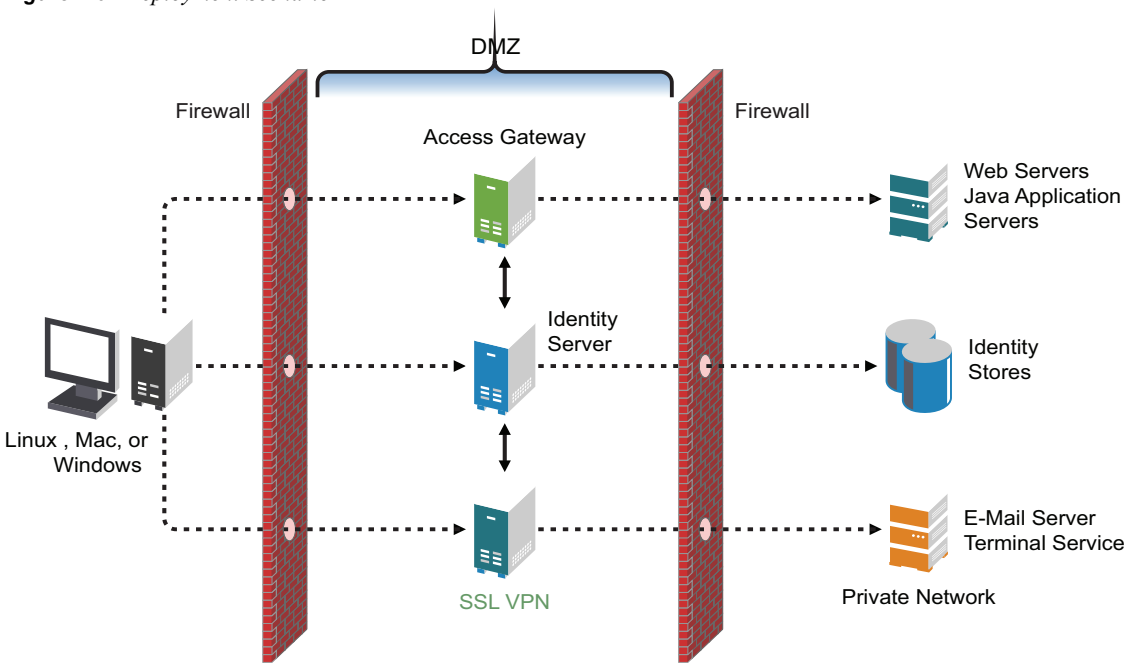
Figure 4-5 *Deployment Scenario 1*



This deployment scenario consists of a demilitarized zone where the Linux Access Gateway and SSL VPN are on the same server and the Identity Server is deployed separately. For installation instructions for this scenario, see "Installing SSL VPN with the Linux Access Gateway" on page 38.

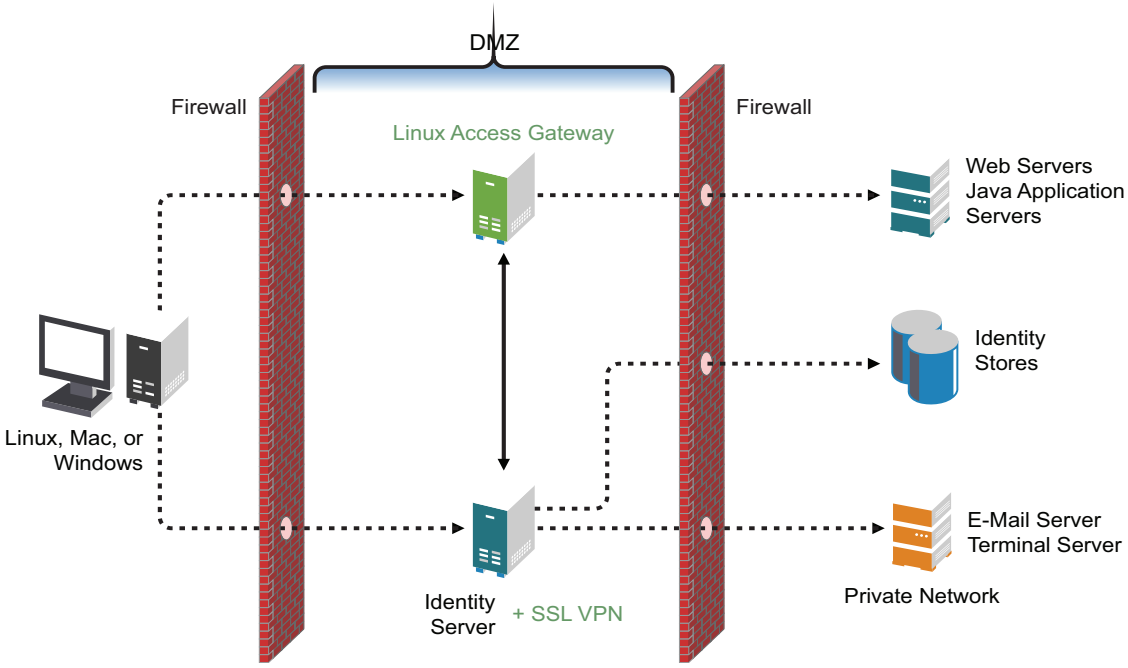
Deployment Scenario 2: SSL VPN Server Installed on a Separate Machine

Figure 4-6 *Deployment Scenario 2*



This deployment scenario consists of a demilitarized zone where the Access Gateway, Identity Server, and SSL VPN are deployed separately. For installation instructions for this scenario, see Section 4.4.2, “Installing the Traditional Novell SSL VPN,” on page 38.

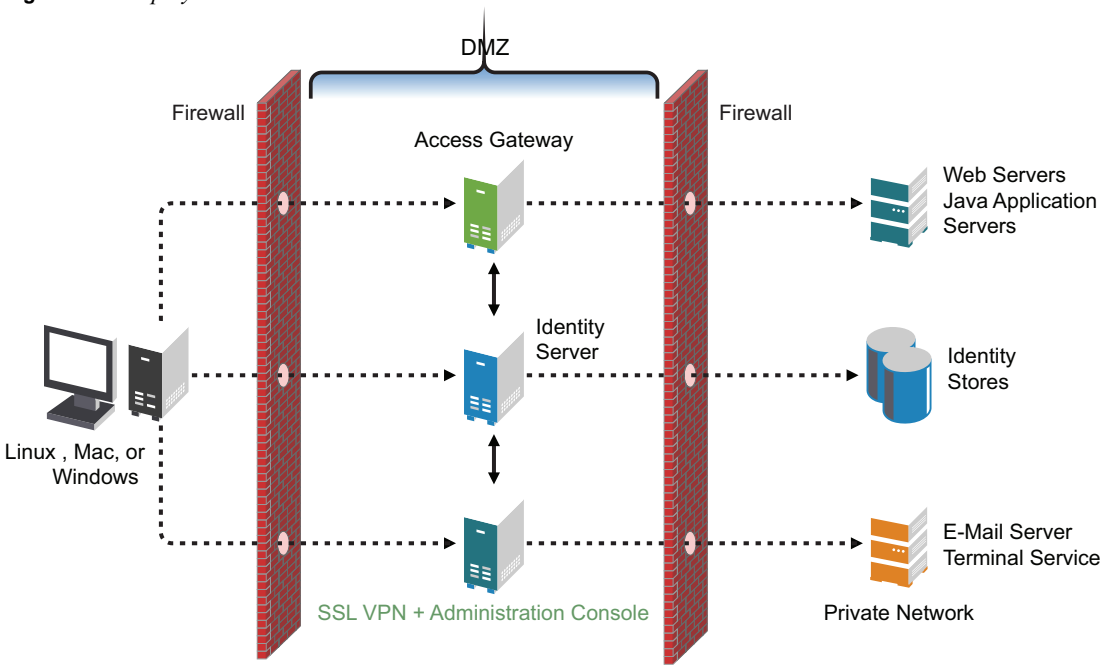
Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server



This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions for this scenario, see “Installing SSL VPN on a Separate Machine, on the Same Machine With the Identity Server, or with the Administration Console” on page 40.

Deployment Scenario 4: Novell Administration Console and SSL VPN on the Same Server

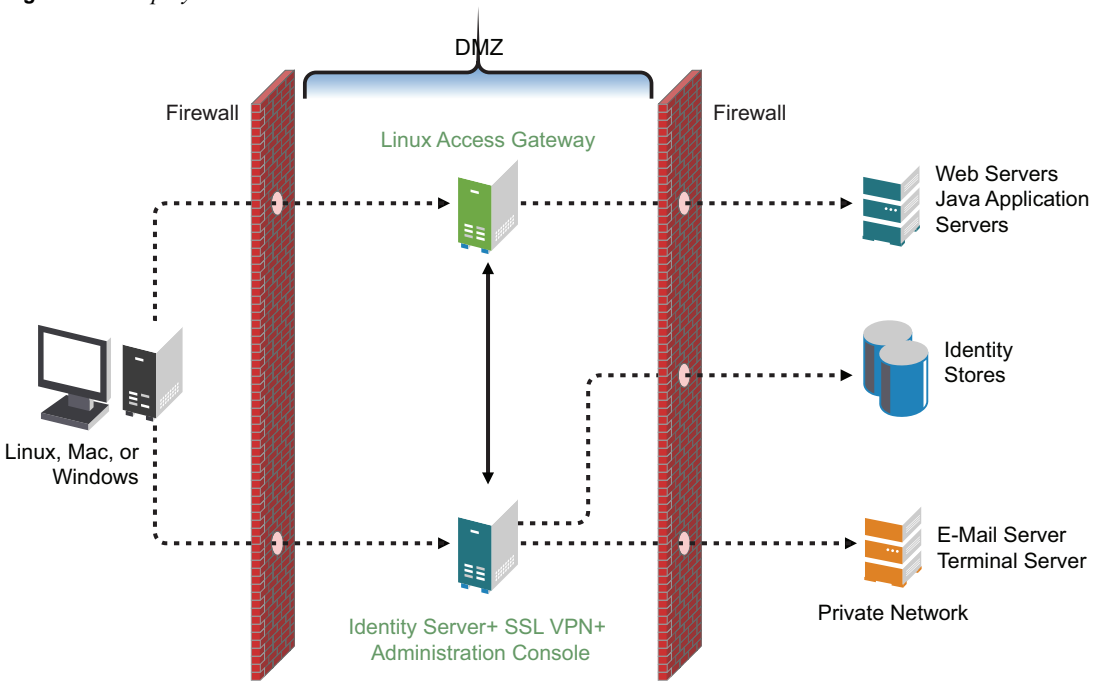
Figure 4-7 *Deployment Scenario 4*



This deployment scenario consists of a demilitarized zone where the Administration Console and SSL VPN are on one machine and the Access Gateway and Identity Server are deployed separately on different machines. For installation instructions for this scenario, see "Installing SSL VPN on a Separate Machine, on the Same Machine With the Identity Server, or with the Administration Console" on page 40.

Deployment Scenario 5: Administration Console, Identity Server, and SSL VPN on the Same Server

Figure 4-8 *Deployment Scenario 5*



This deployment scenario consists of a demilitarized zone where the Identity Server, Administration Console, and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions for this scenario, see "Installing SSL VPN on a Separate Machine, on the Same Machine With the Identity Server, or with the Administration Console" on page 40.

4.4.2 Installing the Traditional Novell SSL VPN

This section describes the installation procedures for different SSL VPN deployments:

- "Installing SSL VPN with the Linux Access Gateway" on page 38
- "Installing SSL VPN on a Separate Machine, on the Same Machine With the Identity Server, or with the Administration Console" on page 40
- "Re-Installing SSL VPN on the Linux Access Gateway" on page 40

Installing SSL VPN with the Linux Access Gateway

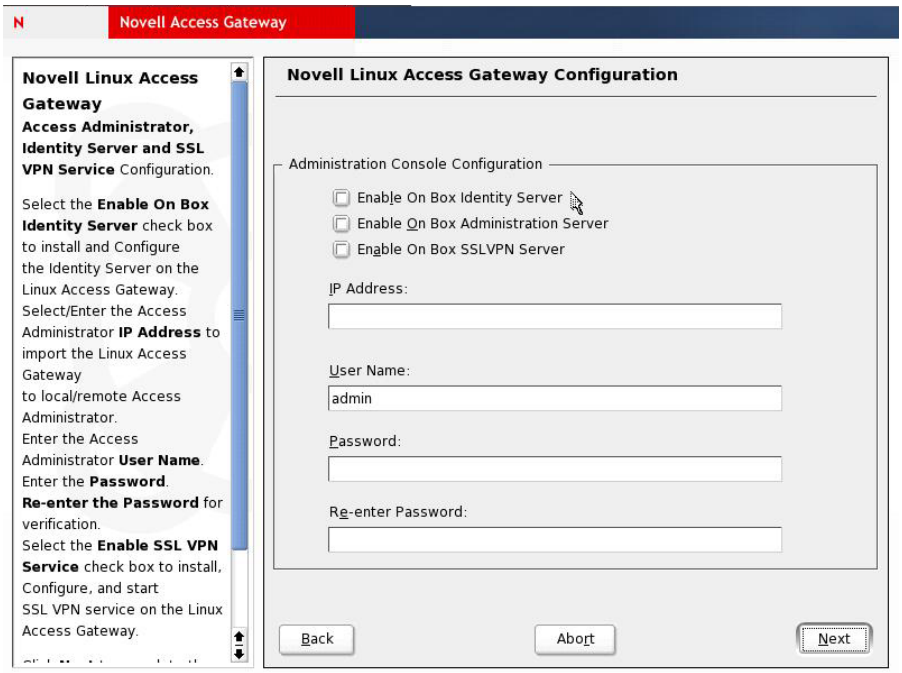
- "Standard Installation" on page 38
- "Advanced Installation" on page 39

Standard Installation

The standard installation process installs SSL VPN along with the Linux Access Gateway. This is the preferred method of installation.

For more information on a standard installation of the Linux Access Gateway, refer to "Using a Standard Linux Installation with the Default Settings" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

1. Start the standard installation of the Linux Access Gateway. For details, refer to "Using a Standard Linux Installation with the Default Settings" in the *Novell Access Manager 3.1 SP1 Installation Guide*.
2. In the Access Administrator Configuration section in the Novell Linux Access Gateway Configuration page, select the *Enable On Box SSL VPN Server* check box to install and configure SSL VPN on the Linux Access Gateway.



3. Follow the on-screen instructions to continue with the Linux Access Gateway installation.

Advanced Installation

For an advanced installation of Linux Access Gateway, use the following steps to install SSL VPN:

1. Start the advanced installation of the Linux Access Gateway. For details, refer to "Installing the Linux Access Gateway Appliance" in the *Novell Access Manager 3.1 SP1 Installation Guide*.
2. On the Access Administrator Configuration page, select *Enable On Box SSL VPN Server*. This installs SSL VPN along with the Linux Access Gateway.
3. Click *Accept*.

   The Installation Settings page is displayed. If the installation is successful, SSL VPN is displayed in the Software section.
4. Follow the on-screen instructions to continue with the Linux Access Gateway installation.

Installing SSL VPN on a Separate Machine, on the Same Machine With the Identity Server, or with the Administration Console

You can use an install script to install the traditional Novell SSL VPN on a separate machine with the Identity Server on the same machine, or on the same machine with the Administration Console or with the Identity Server and the Administration Console.

1. Do one of the following:
   - Insert the CD into the CD drive, then locate `install.sh`.
   - Untar the RPMs.
2. At a command prompt, enter the following install script command:

   ```
   ./install.sh
   ```

   You are prompted to select an installation.
3. Type 3 to install the ESP-Enabled SSL VPN, then press Enter.
4. (Optional) When you are prompted to replace the low bandwidth SSL VPN RPM with the high bandwidth RPM, replace it if the security law permits you to do so.

   For more information on the high bandwidth SSL VPN, see "High and Low Bandwidth Versions" on page 15. For more information on installing the high bandwidth SSL VPN, see Section 4.5, "Installing the RPM Containing Key For High Bandwidth SSL VPN," on page 41.
5. Review and accept the License Agreement.
6. (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server when you are prompted to do so.
7. Specify the name of the administrator for the Administration Console.
8. Specify the administration password.
9. Confirm the password.
10. Specify the IP address of the Administration Console.
11. Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.

    The installation ends with the following message: `Installation complete.`
12. To verify the installation of the SSL VPN, continue with Section 4.7, "Verifying That Your SSL VPN Service Is Installed," on page 42.

Re-Installing SSL VPN on the Linux Access Gateway

If you have deleted the SSL VPN server that was installed along with the Linux Access Gateway, follow the steps given below to re-install it:

1. Download and copy the Novell Access Manager `tar.gz` files to the Linux Access Gateway machine.

   For the actual filenames, see the Novell Access Manager Readme (http://www.novell.com/documentation/novellaccessmanager/readme/accessmanager_readme.html).
2. Unpack the `tar.gz` file by using the following command:

   ```
   tar -xzvf <filename>
   ```
3. At the command prompt, enter the following install script command:

   ```
   ./install.sh
   ```

4 You are prompted to select an installation.

5 When prompted to install the Novell SSL VPN Agent, press Enter.

6 Review and accept the License Agreement.

7 (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server when you are prompted to do so.

8 Specify the IP address of the Administration Console when prompted.

9 Specify the name of the administrator for the Administration Console.

10 Specify the administration password.

11 Confirm the password.

12 Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.

The installation ends with the following message: `Installation complete.`

13 To verify the installation of the Access Gateway, continue with Section 4.7, "Verifying That Your SSL VPN Service Is Installed," on page 42.

4.5 Installing the RPM Containing Key For High Bandwidth SSL VPN

With this release, customers who are eligible to install high bandwidth SSL VPN can install the RPM containing key for the high bandwidth SSL VPN after they get the export clearance. This key is installed only once. There is no need to upgrade the RPM every time the servlet and the server RPMs for SSL VPN are upgraded. In the previous releases, you needed to upgrade the high bandwidth RPMs every time the SSL VPN server and servlet RPMs were upgraded.

You must install the high bandwidth SSL VPN if you want to cluster the SSL VPN servers.

After you have ordered the high bandwidth version, log in to the Novell Customer Center (http://www.novell.com/center) and look for the link that allows you to download the RPM containing key for the high bandwidth version.

During SSL VPN installation, you are prompted to install the high bandwidth. (Step 4 on page 33 or Step 4 on page 40) If you have export clearance, use the steps in this procedure to install the RPM, then return to your installation of SSL VPN.

1 Download the following high bandwidth RPM:

```
novl-sslvpn-hb-key-3.1.0-0.noarch.rpm
```

2 Log in as `root`.

3 Enter the following command to stop all services:

```
/etc/init.d/novell-sslvpn stop
```

4 Enter the following command to install the RPM for the high bandwidth version of SSL VPN:

```
rpm -ivh novl-sslvpn-hb-key-3.1.0-0.noarch.rpm
```

5 Enter the following command to restart all SSL VPN services:

```
/etc/init.d/novell-sslvpn start
```

6 Enter the following command to check the status:

```
/etc/init.d/novell-sslvpn status
```

4.6 Uninstalling the RPM Containing Key For High Bandwidth SSL VPN

1 Log in as `root`.

2 Enter the following command to uninstall the RPM for the high bandwidth version of SSL VPN:

```
rpm -e novl-sslvpn-hb-key-3.1.0-0.noarch.rpm
```

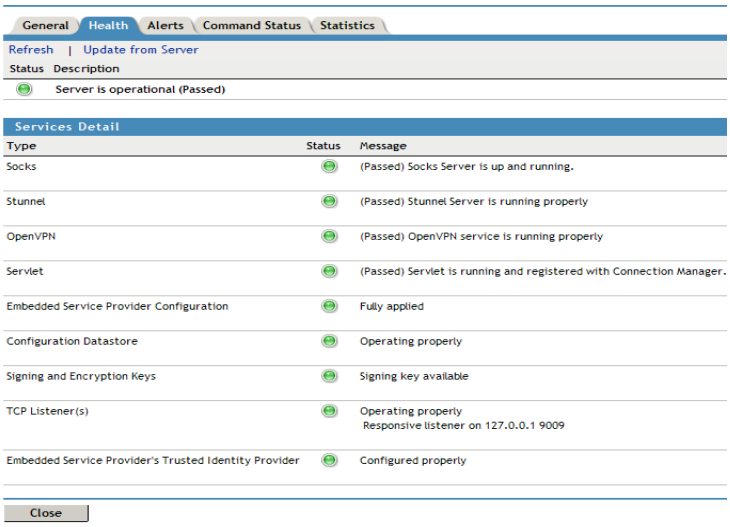
4.7 Verifying That Your SSL VPN Service Is Installed

You can check the status of the SSL VPN server in the Administration Console:

1 In the Administration Console, click *Devices* > *SSL VPNs*.

A list of SSL VPN servers appears, displaying their status.

2 Select a server, then click the *Health* icon to display the health of the SSL VPN server.



The initial health status of an ESP-enabled SSL VPN shows yellow because the trust relationship between the Identity server and the Embedded service provider is yet to be established. For more information on how to configure the trust relationship, see Chapter 9, “Configuring Authentication for ESP-Enabled Novell SSL VPN,” on page 67.

3 (Optional) Continue with Part III, “Configuring SSL VPN,” on page 65, if you have not already configured the SSL VPN server.

Upgrading SSL VPN Servers

5

Upgrade running time: about three minutes.

For this release, you can upgrade the Traditional Novell® SSL VPN 3.0 SP4 to Traditional Novell SSL VPN 3.1. You cannot upgrade the Traditional Novell SSL VPN from SP4 to the 3.1 version of ESP-enabled SSL VPN. After the upgrade, traffic policies that you configured for SSL VPN 3.0 are migrated to SSL VPN 3.1.

This section has the following information:

5.1 Prerequisites

Make sure that you have done the following before you proceed with the installation:

- ❑ If your server is running version of SSL VPN earlier than Novell SSL VPN 3.0 SP4, you must upgrade it first to SP4.
- ❑ Identify the way in which SSL VPN SP4 was installed. Download the relevant upgrade file from Novell (http://support.novell.com/patches.html) and extract the file. For the actual filename, see the Readme (http://www.novell.com/documentation/novellaccessmanager/index.html).
- ❑ Upgrade the Administration Console, Identity Server and Linux Access Gateway in the recommended sequence. For more information, see “Before Starting the Upgrade” and “Upgrading the SP4 SSL VPN Server” in the *Novell Access Manager 3.1 SP1 Installation Guide*.
- ❑ If you have installed high bandwidth SSL VPN, make sure you download and install the high bandwidth SSL VPN RPM. With this release, SSL VPN has a high bandwidth RPM that needs to be installed once to get its capabilities This RPM should be installed before upgrading the SSL VPN server. For information on how to install the high bandwidth SSL VPN RPM, see Section 4.5, “Installing the RPM Containing Key For High Bandwidth SSL VPN,” on page 41.

- The Access Manager Administration Console must be up and running before you begin upgrading SSL VPN servers. Do not perform any configuration tasks in the Administration Console during an SSL VPN Server upgrade.
- If the SSL VPN server was installed on a separate machine, refer to Section 5.3, "Upgrading SSL VPN Installed on a Separate Machine," on page 45. If the SSL VPN server was installed with the other Novell Access Manager components, the SSL VPN server is automatically upgraded along with the other component.

5.2 Upgrade Scenarios

The Table 5-1 on page 44 contains a list of upgrade scenarios available for SSL VPN along with the procedure to upgrade the server.

Table 5-1 *Upgrade Scenarios*

Serial Number	Installation Scenario	Upgrade Procedure
1	Traditional SSL VPN, Identity Server, and the Administration Console on the same machine; Linux Access Gateway on a separate machine	The SSL VPN 3.0 version cannot coexist with other Novell Access Manager components that are running the 3.1 version. When SSL VPN is installed along with the other Novell Access Manager component on the same machine, the SSL VPN server is automatically upgraded to 3.1. For more information, see "Upgrading the Identity Server" in the *Novell Access Manager 3.1 SP1 Installation Guide*.
2	Traditional SSL VPN, Identity Server, Linux Access Gateway, and Administration Console on separate machines	To upgrade the SSL VPN server that is installed on a separate machine, see Section 5.3, "Upgrading SSL VPN Installed on a Separate Machine," on page 45.
3	Traditional SSL VPN and the Identity server on the same machine; Administration Console and Linux Access Gateway on separate machines	When SSL VPN is installed along with the Identity Server on the same machine, the SSL VPN server is automatically upgraded to 3.1. For more information, see "Upgrading the Identity Server" in the *Novell Access Manager 3.1 SP1 Installation Guide*.
4	Traditional SSL VPN and the Administration Console on same machine, Identity Server, Linux Access Gateway on a separate machine	When SSL VPN is installed along with the Administration Console, on the same machine, the SSL VPN server is automatically upgraded to 3.1. For more information, see "Upgrading the Administration Console" in the *Novell Access Manager 3.1 SP1 Installation Guide*.
5	Traditional SSL VPN and the Linux Access Gateway on the same machine, Administration Console and Identity Server on separate machines	When SSL VPN is installed along with the Linux Access Gateway, on the same machine, the SSL VPN server is automatically upgraded to 3.1. For more information, see "Upgrading the Linux Access Gateway Appliance".

Serial Number	Installation Scenario	Upgrade Procedure
6	Move from Traditional Novell SSL VPN 3.0 to ESP-enabled SSL VPN 3.1	If you have installed the Traditional Novell SSL VPN server and want to move to the ESP-enabled SSL VPN, you cannot upgrade the server directly. You need to install the ESP-enabled SSL VPN on a separate machine and then import the traffic policies from the 3.0 Traditional SSL VPN into the 3.1 ESP-enabled SSL VPN. For more information, see Section 5.4, “Migrating a Traditional SSL VPN Server to the ESP-Enabled Version,” on page 46.
7	Upgrade traditional SSL VPN servers clustered in the 3.0 version by using config.txt or the server persistent method through Linux Access Gateway.	If you have configured a cluster of SSL VPN servers in 3.0 by using the `config.txt` file or though the Linux Access Gateway do one of the following: • If the `config.txt` file is used to cluster SSL VPN, all configuration details in the file are lost after you upgrade to 3.1. SSL VPN 3.1 does not support the using the `config.txt` file. After upgrading the server, you must reconfigure the SSL VPN cluster with the help of an L4 server. For more information, see Part IV, “Clustering the High Bandwidth SSL VPN Servers,” on page 121. • If you clustered SSL VPN by using the Linux Access Gateway, your cluster configuration continues to work. You also have an option to cluster SSL VPN with the help of an L4 server. For more information, see Part IV, “Clustering the High Bandwidth SSL VPN Servers,” on page 121

5.3 Upgrading SSL VPN Installed on a Separate Machine

To upgrade from Novell SSL VPN 3.0 SP4 to Novell SSL VPN 3.1:

1. Upgrade the Administration Console, Identity Server, and Linux Access Gateways before you proceed with upgrading the SSL VPN server.

   For upgrade information, see “Upgrading from Access Manager 3.0 SP4 to Access Manager 3.1 SP1” in the *Novell Access Manager 3.1 SP1 Installation Guide*.

2. Download the upgrade file from Novell (http://support.novell.com/patches.html) and extract the file.

   One of the extracted files contains the Administration Console, the Identity Server, and SSL VPN. For the actual filename, see the Readme (http://www.novell.com/documentation/novellaccessmanager31/index.html).

3. Unpack the `tar.gz` file by using the following command:

```
tar -xzvf <filename>
```

For this installation, you need to unpack the Identity Server `.tar.gz` file, which contains the SSL VPN files.

4. Log in as the `root` user.
5. Open the unpacked Identity Server file, and enter the following at the terminal window:

   ```
   ./install.sh
   ```

6. When prompted to install a product, type 3 to select SSL VPN, then press the Enter key.

   The system detects whether an SSL VPN Server is installed, and prompts you whether to upgrade.

7. Type *Y*, then press the Enter key.
8. Review and enter *Y* to accept the License Agreement.
9. (Conditional) If the SSL VPN machine has been configured with multiple IP address, select an IP address for the SSL VPN server when you are prompted to do so.
10. Press Enter to accept the current Administration Console IP address.
11. Specify the name of the administrator for the Administration Console.
12. Specify the administration password.
13. Confirm the password, then wait as the system installs the components. (This will take several minutes.)
14. View the files in the `/tmp/novell_access_manager` directory to verify the results of the upgrade process.

    These log files are all dated and time-stamped.

15. After you have upgraded the servers proceed with Section 5.6, "Updating Configuration Changes to the Upgraded Server," on page 49.

NOTE: Occasionally, the first SSL VPN user connection might fail after upgrading, especially if you have encountered any problems during the upgrade process. To work around this problem, we recommend that you initiate multiple SSL VPN connections after upgrading.

5.4 Migrating a Traditional SSL VPN Server to the ESP-Enabled Version

---

NOTE: Before you proceed with this configuration, refer to "Upgrading from Access Manager 3.0 SP4 to Access Manager 3.1 SP1" in the *Novell Access Manager 3.1 SP1 Installation Guide* to understand the prerequisites.

You cannot directly upgrade the traditional Novell SSL VPN from version 3.0 to version 3.1 of the ESP-enabled SSL VPN, but you cane export the traffic policies from the traditional 3.0 SSL VPN into the ESP-enabled 3.1 SSL VPN, which is installed on a separate machine.

- Section 5.4.1, "Upgrade Scenarios," on page 47
- Section 5.4.2, "Migrating Traffic Policies from Traditional SSL VPN to ESP- Enabled SSL VPN," on page 48

5.4.1 Upgrade Scenarios

The following table explains the various upgrade scenarios available when you want to upgrade from traditional SSL VPN to ESP-Enabled SSL VPN.

Table 5-2 *Upgrade Scenarios*

Serial Number	Installation Scenarios	Upgrade Procedure
1	Traditional SSL VPN, Identity Server, Linux Access Gateway, and Administration Console on separate machines	1. Upgrade the Administration Console and Identity Server in the recommended order. 2. Export the traffic policies of the Traditional SSL VPN 3.0 SP4 server that you want to migrate. 3. Install the ESP-enabled SSL VPN on a separate machine. 4. Import the traffic policies that you saved in Step 2 into the ESP-enabled SSL VPN 3.1 server. 5. Establish a trust relationship with the Identity Server. 6. Verify that the server is working.s 7. Delete the Traditional SSL VPN server from the Administration Console and uninstall it. For more information on migrating, see Section 5.4.2, “Migrating Traffic Policies from Traditional SSL VPN to ESP- Enabled SSL VPN,” on page 48.

Serial Number	Installation Scenarios	Upgrade Procedure
2	Traditional SSL VPN, Identity User-friendly Administration Console on the same machine; Linux Access Gateway on a separate machine	When SSL VPN is installed with any of the Novell Access Manager components, the Traditional SSL VPN server is automatically upgraded to 3.1. To migrate to the ESP-enabled version, do one of the following: ◆ Proceed with Step 2 in the upgrade procedure in Serial Number 1. ◆ Follow the steps given below: 1. Export the traffic policies of the Traditional SSL VPN server that you want to migrate. 2. Delete the Traditional SSL VPN server from the Administration Console and uninstall it. 3. Install the ESP-enabled SSL VPN on the same machine. 4. Import the traffic policies that you saved in Step 1. 5. Establish a trust relationship with the Identity Server. 6. Verify that the server is working. Proceed with Section 5.4.2, "Migrating Traffic Policies from Traditional SSL VPN to ESP-Enabled SSL VPN," on page 48.
3	Traditional SSL VPN and Identity Server on the same machine, Administration Console and Linux Access Gateway on separate machines	
4	Traditional SSL VPN, Administration Console on the same machine; Identity Server Linux Access Gateway on a separate machine	
5	Traditional SSL VPN and Linux Access Gateway on same machine; Administration Console and Identity Server on separate machines	You cannot migrate to the ESP-enabled version.

5.4.2 Migrating Traffic Policies from Traditional SSL VPN to ESP- Enabled SSL VPN

If you have not already upgraded the Administration Console from SP4 to 3.1, upgrade it. For more information, see "Upgrading the Administration Console" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

To migrate the traffic policies from the traditional SSL VPN version to the ESP-enabled SSL VPN version:

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*
2. Select *Traffic Policies* from the *Policies* section. The SSL VPN Traffic Policies page is displayed.
3. Select the Traditional SSL VPN 3.0 SP4 from which you want to import the traffic policies, then click *Export*.
4. Specify a filename for the XML document.

5 Specify a location to save the XML file.

6 Install the ESP-enabled 3.1 SSL VPN. For more information, see Section 4.3, “Installing ESP-Enabled SSL VPN,” on page 30.

7 Log in to the Administration Console into which you have imported the ESP-enabled SSL VPN, then click *Devices* > *SSL VPNs* > *Edit*.

8 Select *Traffic Policies* from the *Policies* section, then click *Import* in the traffic policies page.

9 Browse and select the XML file that contains the saved traffic policies.

NOTE: When the traffic policies are imported into the SSL VPN server, they might not retain their original order. To order the traffic rules, see Section 14.3.2, “Rule Ordering,” on page 99.

---

10 Select *Authentication Configuration* and establish a trust relationship with the Identity Server. For more information, see Chapter 9, “Configuring Authentication for ESP-Enabled Novell SSL VPN,” on page 67.

11 To save your modifications, click *OK*, then click *Update* on the Configuration page.

The health status of the SSL VPN server must display green.

12 Delete the traditional SSL VPN from the Administration Console, then uninstall it. For more information on uninstalling the SSL VPN server, see Chapter 7, “Uninstalling the SSL VPN Server,” on page 55.

5.5 Upgrading Clustered SSL VPN Servers

If you have clustered the SSL VPN servers in 3.0, upgrade the SSL VPN servers after you have upgraded the Administration Console, Identity Server, and the Linux Access Gateway. For more information on upgrading SSL VPN, see “Upgrading the SP4 SSL VPN Server”. After the upgrade:

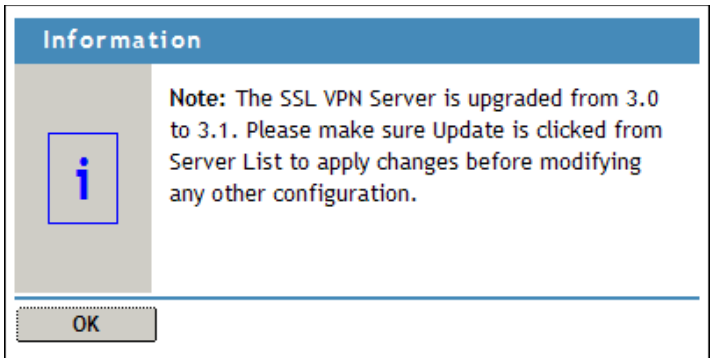
- If you have configured the SSL VPN clusters by using `config.txt`, then you must configure the SSL VPN cluster again by using the Administration Console. For more information, see Part IV, “Clustering the High Bandwidth SSL VPN Servers,” on page 121. You cannot make any configuration changes by using `config.txt` file in this release.
- If you have configured the cluster by using the Access Gateway:
  - Upgrade the servers in the recommended manner.
  - Configure the SSL VPN cluster with the help of an L4 server. For more information, see Part IV, “Clustering the High Bandwidth SSL VPN Servers,” on page 121.

5.6 Updating Configuration Changes to the Upgraded Server

After you have upgraded your SSL VPN server to the 3.1 version, you must follow the steps given below before you perform any configuration changes:

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

2 Click *OK* in the dialog box prompting you to update the servers.



3 Click *OK*, then click *Update* on the Configuration page to save modifications.

4 Define the security levels using the client integrity check policies and associate the traffic policies to the appropriate security level, before you allow any client connections.

For more information on assigning security levels to traffic policies, see Section 14.2, "Configuring Client Security Levels," on page 95. This is a mandatory activity before you proceed with any other configuration steps because, after upgrading the SSL VPN servers, all the traffic policies are associated to security level `None` by default. In such a scenario, all the traffic policies are pushed to the client, even if the client fails the client integrity check.

5 (Optional) If you configured SSL VPN to connect only in Kiosk mode, to download applet when a user uses Internet Explorer, or to enable SSL VPN to connect to Citrix servers by using `config.txt` and `web.xml` files, do the following:

- If you used the `config.txt` file to configure SSL VPN to connect only in Kiosk mode, configure SSL VPN again by using the Administration Console. For more information, see Section 15.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 101.
- If you have configured SSL VPN to download the applet when a user uses Internet Explorer, configure SSL VPN again by using the Administration Console. For more information, see Section 15.3, "Configuring SSL VPN to Download the Java Applet on Internet Explorer," on page 103.
- If you have configured custom login policies by using `web.xml`, reconfigure them again by using the Administration Console For more information, see Section 15.4, "Configuring a Custom Login Policy for SSL VPN," on page 103.

5.7 Configuration Changes to the SSL VPN Server Installed with the Linux Access Gateway

After you have upgraded the SSL VPN server installed along with the Linux Access Gateway, you must modify the existing path-based service accelerating the SSL VPN server as follows:

1 In the Administration Console, click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

2 In the *Proxy Service List* section, click the SSL VPN service that you have configured.

3 Select the *Webservers* tab. Click the Webserver IP address link from the *Webservers list* section.

4 Originally, the public IP address of SSL VPN was configured as the IP address of the Webserver. Change the IP address to 127.0.0.1, which is the loopback IP address.

5 Click *OK* when prompted to purge cache.

6 Click *OK*, then click *Update* on the Configuration page to save your modifications.

Preinstalling the SSL VPN Client Components

6

You can preinstall SSL VPN client components in the client machine, so that the users can access SSL VPN in Enterprise mode.

6.1 Installing Client Components for Linux

1. On the client machine, download the following RPM from the `/var/opt/novell/tomcat4/webapps/sslvpn/linux` directory:

   `novell-sslvpn-serv.tar.gz`

2. Enter the following command to untar the file:

   `tar -zxvf <filename>`

3. Enter the following command to install `novl-sslvpn-service-xxx-xx.i586.rpm`:

   `rpm -ivh <rpm_name>`

6.2 Installing Client Components for Macintosh

1. On the client machine, download the following package from the `/var/opt/novell/tomcat4/webapps/sslvpn/MacOS` directory:

   `novell-sslvpn-serv.tar.gz`

2. Enter the following command to untar the file:

   `tar -zxvf novell-sslvpn-serv.tar.gz`

3. Enter the following command to install the `novl-sslvpn-service.pkg` package extracted from the tar ball:

   `installer -pkg novl-sslvpn-service.pkg -target “/”`

6.3 Installing Client Components for Windows

1. On the client machine, download the following file from `/var/opt/novell/tomcat4/webapps/sslvpn/windows`:

   `novl-sslvpn-service-install.exe`

2. Run the `.exe` file to install the client components.

Uninstalling the SSL VPN Server 7

NOTE: If you have installed SSL VPN and the Linux Access Gateway on the same machine, you cannot uninstall the SSL VPN server.

Before you uninstall the SSL VPN server installed with the Identity Server, you must first remove it from the cluster configuration, then delete it from the Administration Console.

7.1 Deleting the Server from the Administration Console and from the Cluster

1. In the Administration Console, *Devices* > *Devices* > *SSL VPNs*.
2. Select the SSL VPN server that you want to uninstall.
3. (Optional) If the server is part of a cluster, select *Actions* > *Remove from Cluster*.
4. Update the cluster configuration.
5. Select the SSL VPN Server that you want to uninstall, then click *Actions* > *Delete*.

7.2 Uninstalling the Server

IMPORTANT: If you have installed the High-Bandwidth SSL VPN key, uninsall the key before proceeding to uninstall the SSL VPN server. For more informataion on uninstalling the high-bandwidth key, see Section 4.6, "Uninstalling the RPM Containing Key For High Bandwidth SSL VPN," on page 42.

1. Browse and locate the uninstall script `uninstall.sh`.

   The uninstall script is located in the root directory of the installation CD or in the installation directory.
2. At the command prompt, run the following command:

   ```
   ./uninstall.sh
   ```

   NOTE: If you want to run the uninstallation script directly from the CD, insert the CD, then run the command.
3. Do one of the following, depending on your installation type:
   - Enter 4 to uninstall the Traditional Novell® SSL VPN.
   - Enter 5 to uninstall the ESP-enabled Novell SSL VPN.

NOTE: If SSL VPN fails to uninstall gracefully, use option 6 to forcefully uninstall SSL VPN.

Deploying SSL VPN

8

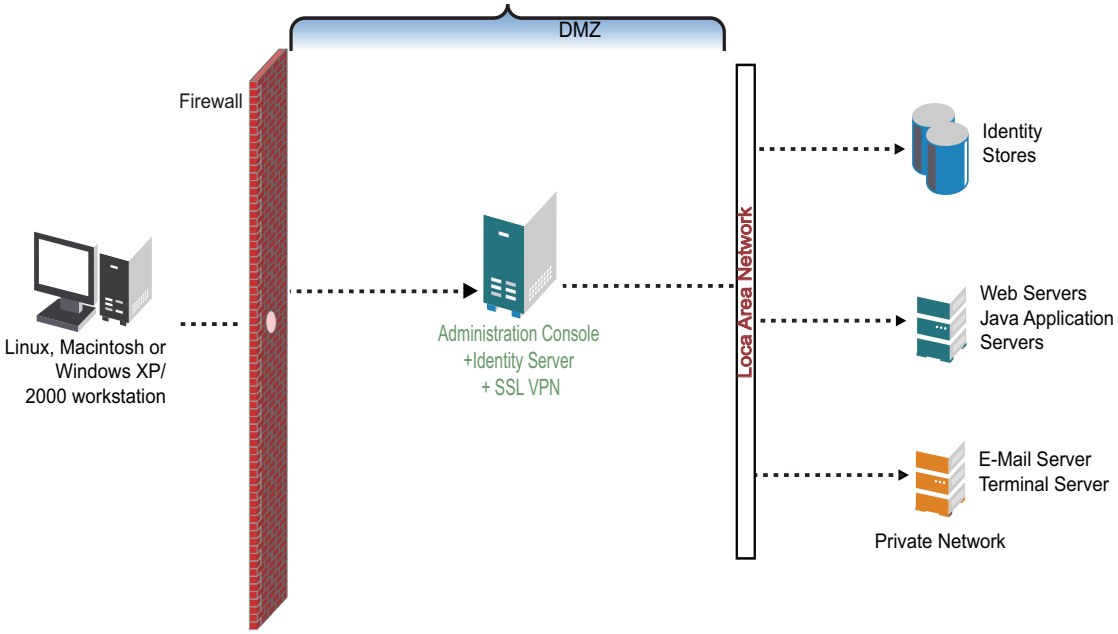
You can have several possible deployment scenarios, depending on whether you want to install the ESP-enabled Novell® SSL VPN or the traditional novell SSL VPN. Some of the possible deployment scenarios are:

- **Single Machine Installation of an ESP-Enabled SSL VPN:** In this deployment scenario, the Administration Console, the Identity Server, and the SSL VPN server are all installed on a single machine. For more information on this deployment scenario, see Section 8.1, “Installing ESP-Enabled SSL VPN on a Single Machine,” on page 57.
- **Clustering Single-Machine SSL VPNs:** In this deployment scenario, the ESP-enabled SSL VPN is installed on a single machine along with the Administration Console and the Identity Server and several such machines are clustered. For more information about this deployment scenario, see Section 8.2, “Deploying a Cluster of Single-Machine SSL VPNs,” on page 59.
- **Installing the Traditional Novell SSL VPN:** In this deployment scenario, SSL VPN is installed along with Linux Access Gateway, Administration Console, and Identity Server. You can install SSL VPN along with the Linux Access Gateway on the same machine, you can install it along with the Identity Server on the same machine, or you can install SSL VPN on a separate machine. For more information on this deployment scenario, see Section 8.3, “Deploying the Traditional Novell SSL VPN,” on page 62 and “Installing SSL VPN on a Separate Machine, on the Same Machine With the Identity Server, or with the Administration Console” on page 40.

8.1 Installing ESP-Enabled SSL VPN on a Single Machine

In a single-machine installation SSL VPN, the Identity Server, and the Administration Console are all installed on a single machine.

Figure 8-1 *ESP-Enabled SSL VPNs installed on a Single Machine*



The following sections explain the prerequisites and the procedures for single-machine installation:

- Section 8.1.1, “Prerequisites,” on page 58
- Section 8.1.2, “Deployment Procedure,” on page 59

8.1.1 Prerequisites

- ❑ For the hardware and software requirements, see Chapter 4.1, “Prerequisites,” on page 29.
- ❑ Public IP address.

  You might need up to three IP addresses, depending on your firewall settings. The SSL VPN server has following three listeners that communicate with the public network:

  - Tomcat Connector for authentication
  - Enterprise mode tunnel listener
  - Kiosk mode tunnel listener

  You need two public IP addresses, one for the Tomcat connector and one for the Kiosk mode tunnel, if your firewall setting allows only port 443 for secure communication and the Enterprise mode tunnel listens on UDP port 443. However, you need three public IP addresses if you require a TCP port for an Enterprise mode tunnel.
- ❑ One private IP address. This is the IP address of the interface that is connected to the private LAN.
- ❑ One public DNS name
- ❑ One X.509 certificate, if the locally generated certificate is not sufficient.

8.1.2 Deployment Procedure

To install the ESP-enabled Novell SSL VPN on a single machine:

1. Install the Administration Console.

   For more information on installing the Administration console, see "Installing the Access Manager Administration Console" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

2. Install the Identity Server and the SSL VPN server by using the `install.sh` script.

   For more information on installing the Identity Server, see "Deployment Scenario 2: Installing SSL VPN and the Identity Server on the Same Machine" on page 31.

3. Configure the Identity Server.

   For more information on configuring the Identity Server, see "Configuring an Identity Server"in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

4. Assign the Security certificate.

   For more information, see "Enabling SSL Communication" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

5. The SSL VPN server is auto-imported into the Administration Console after the installation.

   Establish a trust relationship between the Identity Server and the SSL VPN server.

   For more information, see Chapter 9, "Configuring Authentication for ESP-Enabled Novell SSL VPN," on page 67.

6. In the Administration Console, select *Devices* > *SSL VPNs*. The health status at this stage should be green, indicating that the SSL VPN server is properly imported into the Administration Console and a trust relationship between the Identity Sever and the SSL VPN server has been established.

7. Configure the Client Integrity check policies and other relevant configurations for SSL VPN.

   For more information on configuring the SSL VPN, see Part III, "Configuring SSL VPN," on page 65.

8.2 Deploying a Cluster of Single-Machine SSL VPNs

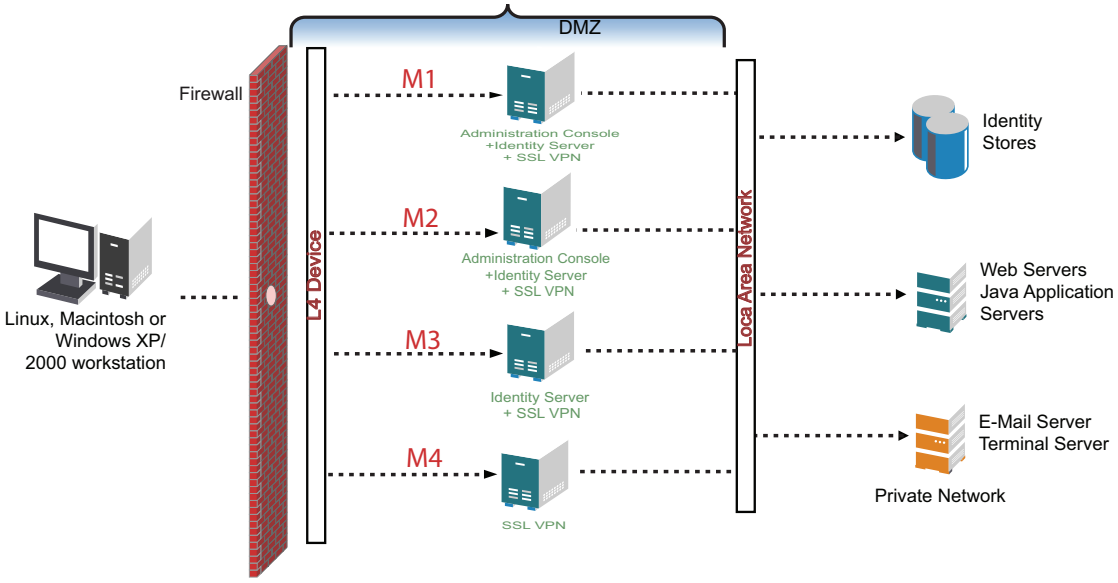
In a single-machine cluster of SSL VPNs, SSL VPN, the Identity Server, and the Administration Console are all installed on a single machine and several of these SSL VPNs are clustered. In this deployment scenario, the ESP-enabled Novell SSL VPN is used. You can deploy SSL VPN along with the Identity Server cluster or on a single Identity Server.

The following sections document the prerequisites and the procedure that are involved in configuring a cluster of single machine SSL VPNs:

8.2.1 Deployment Scenario

This sample deployment scenario consists of a cluster of four ESP-enabled Novell SSL VPNs. The following figure explains the setup:

Figure 8-2 *Cluster of ESP-enabled Novell SSL VPNs Installed on a Single Machine*



In this scenario, the M1 and M2 setup consists of the Administration Console, Identity Server, and the SSL VPN server installed on a single machine. M3 has the Identity Server and the SSL VPN server installed on a single machine, and M4 has only the SSL VPN server installed.

8.2.2 Prerequisites

The prerequisites for the above setup are:

- ❑ For the hardware and software requirements, see Chapter 4.1, “Prerequisites,” on page 29.
- ❑ One public DNS name for the L4 device.
- ❑ Three public IP addresses for the L4 device.
- ❑ Two listening IP addresses each for the four SSL VPN servers.

  NOTE: Two IP addresses are required if the UDP port is not opened in the firewall or if both Enterprise and Kiosk mode listen on the TCP port. You can also use the second IP address as the secondary IP address.

- ❑ Three private IP addresses.
- ❑ Security certificate.

8.2.3 Deployment Procedure

To install the ESP-enabled Novell SSL VPN on a single machine:

1 Install the Administration Console on M1.

For more information on installing the Administration Console, see "Installing the Access Manager Administration Console" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

2. Install the secondary Administration Console on M2.

   For more information on how to install the secondary Administration Console, see "Installing Secondary Versions of the Administration Console" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

3. Install the Identity Server and the SSL VPN server by using the `install.sh` script.

   For more information on installing the Identity Server, see "Deployment Scenario 2: Installing SSL VPN and the Identity Server on the Same Machine" on page 31.

4. Configure the Identity Server.

   For more information on configuring the Identity Server, see "Configuring an Identity Server" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*

5. Assign the security certificate.

   For more information, see "Enabling SSL Communication" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

6. Create a cluster of Identity Servers.

   For more information on how to create a cluster of Identity Servers, see "Creating a Cluster Configuration" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

7. Establish a trust relationship between the Identity Server and the SSL VPN server.

   For more information, see Chapter 9, "Configuring Authentication for ESP-Enabled Novell SSL VPN," on page 67.

8. Create a cluster of SSL VPNs on M1.

9. Install the Identity Server along with SSL VPN on M2.

   For more information on how to create the SSL VPN cluster, see Section 21.1, "Creating a Cluster of SSL VPN Servers," on page 125.

10. Configure the Identity Server and assign it to the Identity Server cluster.

11. Configure SSL VPN and assign it to the SSL VPN server cluster.

12. Install the Identity Server along with SSL VPN on M3.

13. Configure the Identity Server and assign it to the Identity Server cluster.

14. Configure the SSL VPN server and assign it to the SSL VPN server cluster.

15. Install the SSL VPN server on M4.

    For more information on installing SSL VPN on a separate machine, see "Deployment Scenario 1: Installing SSL VPN on a Separate Machine" on page 30.

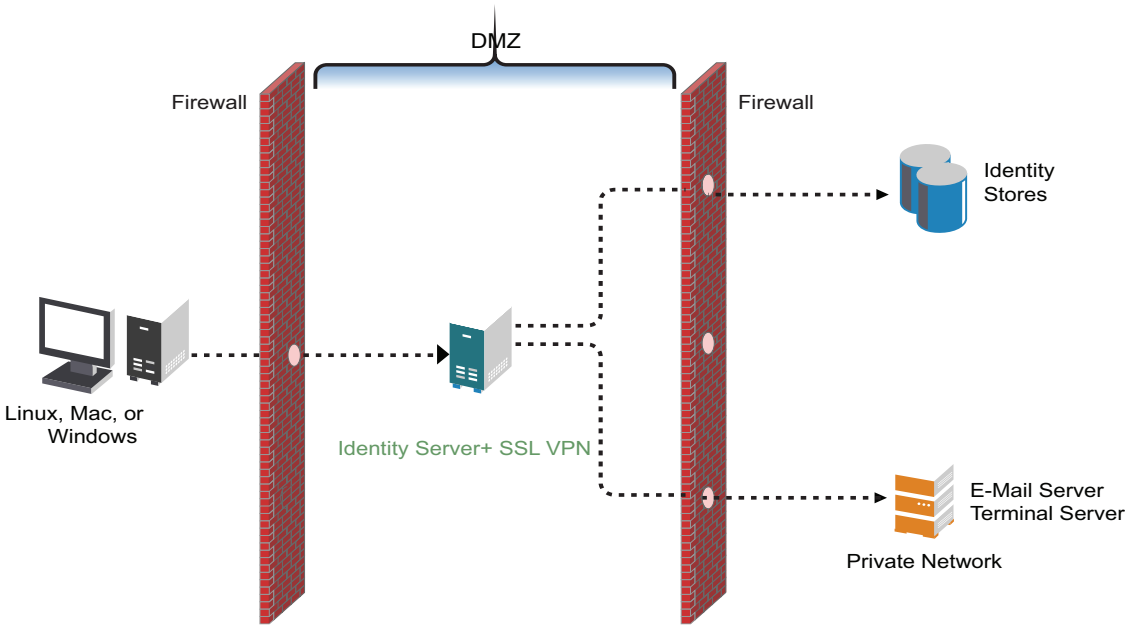
16. Configure the SSL VPN server and assign it to the SSL VPN server cluster.

17. Configure the Client Integrity check policies and other relevant configurations for the SSL VPN cluster.

    For more information on configuring SSL VPN, see Part III, "Configuring SSL VPN," on page 65.

8.3 Deploying the Traditional Novell SSL VPN

Figure 8-3 *Deployment Scenario for SSL VPN Enabled by the Access Gateway*



When you deploy the traditional Novell SSL VPN, you can install the SSL VPN along with the Identity Server on the same machine, you can install SSL VPN along with Linux Access Gateway on the same machine or you can install the Linux Access Gateway, Identity server and the SSL VPN server on different machines.

The following sections explain the prerequisites and the procedures for single machine installation:

- Section 8.3.1, “Prerequisites,” on page 62
- Section 8.3.2, “Deployment Procedure,” on page 62

8.3.1 Prerequisites

- ❑ For the hardware and software requirements, see Chapter 4.1, “Prerequisites,” on page 29.
- ❑ Public IP address. You need two IP addresses if the UDP port is not opened in the firewall or if both Enterprise and Kiosk mode listen on the TCP port. You can also use the second IP address as the secondary IP address.
- ❑ One private IP address.
- ❑ One public DNS name
- ❑ One security certificate.

8.3.2 Deployment Procedure

1 Install the Administration Console.

For more information on installing the Administration console, see “Installing the Access Manager Administration Console” in *Novell Access Manager 3.1 SP1 Installation Guide*.

2 Install the Identity Server.

For more information on installing the Identity Server, see "Installing the Novell Identity Server" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

3 Configure the Identity Server.

For more information on configuring the Identity Server, see "Configuring an Identity Server"in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

4 Assign the security certificate.

For more information, see "Enabling SSL Communication" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

5 Install the Linux Access Gateway server.

For more information, see "Installing the Linux Access Gateway Appliance" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

During the installation steps, make sure that you select *Enable SSL VPN Service,* to install SSL VPN along with the Linux Access Gateway.

The SSL VPN server is auto-imported into the Administration Console after the installation.

6 Configure the Linux Access Gateway to accelerate and protect the SSL VPN Server.

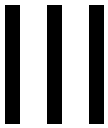
For more information, see Chapter 10, "Accelerating the Traditional Novell SSL VPN," on page 69.

7 In the Administration Console, select *Devices* > *SSL VPNs*. The health status at this stage should be green indicating that the SSL VPN server is properly imported into the Administration Console and a trust relationship between the Identity Sever and the SSL VPN server has been established.

8 Configure the Client Integrity check policies and other relevant configurations for SSL VPN.

For more information on configuring the SSL VPN, see Part III, "Configuring SSL VPN," on page 65.

Configuring SSL VPN



SSL VPN servers are auto-imported into the Administration Console during installation.You can use the SSL VPNs page in the Administration Console to view information about the current status of all SSL VPN servers and to configure the SSL VPN servers.

Before you proceed with the SSL VPN configuration, you must do the following:

- Install the SSL VPN server. For more information, see Part II, "Installing and Deploying the SSL VPN Server," on page 27
- Install the Linux Access Gateway, if you want to accelerate SSL VPN by using the Linux Access Gateway. For more information, see the *Novell Access Manager 3.1 SP1 Installation Guide*.
- Login to the Administration Console as the admin user. For more information, see "Logging In to the Administration Console" in the *Novell Access Manager 3.1 SP1 Installation Guide*.
- Create an Identity Server configuration. For more information, see "Configuring an Identity Server" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*
- If you have upgraded from SSL VPN 3.0 to SSL VPN 3.1, update changes to the SSL VPN servers before you proceed with any other configurations. For more information, see Section 5.6, "Updating Configuration Changes to the Upgraded Server," on page 49.
- Refer to *Chapter 8, "Deploying SSL VPN," on page 57* to know more about the deployment scenarios and the configurations that are relevant for your scenarios.

This section has the following information:

Configuring Authentication for ESP-Enabled Novell SSL VPN

9

If you installed the ESP-enabled Novell® SSL VPN, then an Embedded Service Provider component was installed along with the SSL VPN server during the installation. You must now configure the Embedded Service Provider in order to establish a trust relationship between the Identity Server and the Embedded Service Provider.

NOTE: If you have installed the traditional SSL VPN, refer to Chapter 10, "Accelerating the Traditional Novell SSL VPN," on page 69.

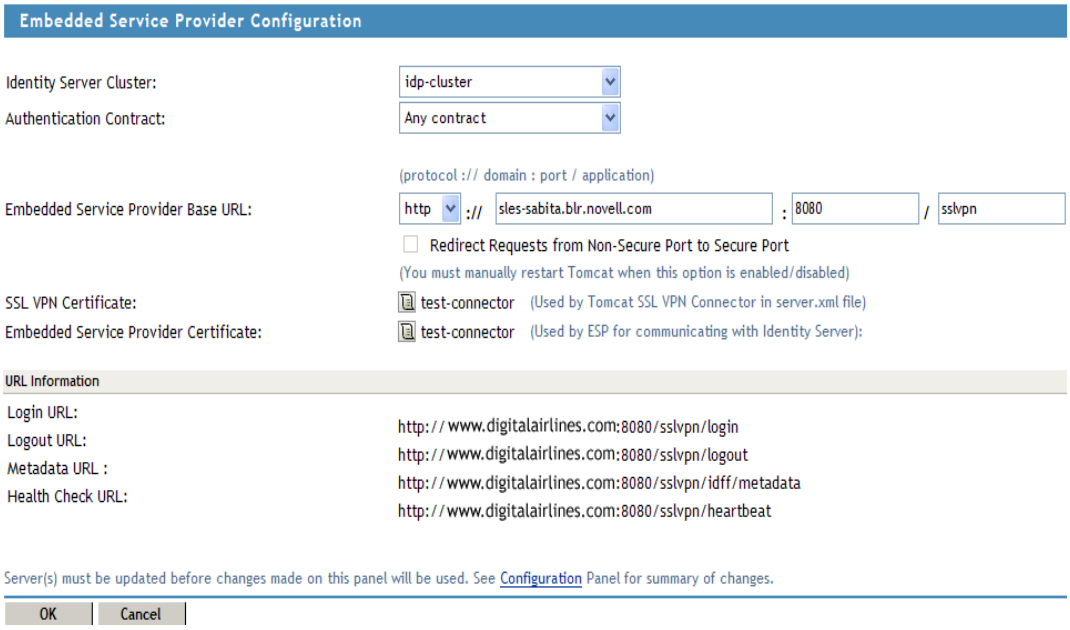
---

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

The Server configuration page is displayed.

2 Select *Authentication Configuration* from the *Basic Gateway Configuration* section.

The SSL VPN Embedded Service Provider Configuration page is displayed.



3 Fill in the following fields:

Identity Server Cluster: Specifies the Identity Server cluster that you want the Access Gateway to trust for authentication. Select the configuration you have assigned to the Identity Server.

Authentication Contract: Specifies the type of contract, which determines the information a user must supply for authentication. By default, you can select from the following authentication contracts:

- **Any Contract:** If the user has authenticated, allows any contract defined for the Identity Server to be valid, or if the user has not authenticated, prompts the user to authenticate using the default contract assigned to the Identity Server configuration.
- **Name/Password - Basic:** Specifies basic authentication over HTTP, using a standard login pop-up provided by the Web browser.
- **Name/Password - Form:** Specifies a form-based authentication over HTTP, using the Access Manager login form.
- **Secure Name/Password - Basic:** Specifies basic authentication over HTTPS, using a standard login pop-up provided by the Web browser.
- **Secure Name/Password - Form:** Specifies a form-based authentication over HTTPS, using the Access Manager login form.

Embedded Service Provider Base URL: The application path for the Embedded Service Provider. This URL has the following constituents:

- **Protocol:** Specifies the communication protocol. Specify HTTPS in order to run securely in SSL mode. Use HTTP only if you do not require security
- **Domain:** The DNS name used to access the SSL VPN server. Using an IP address is not recommended.
- **Port:** Specifies the port values for the protocol. The port is 8080 for HTTP or 8443 for HTTPS. If you want to use port 80 or 433, specify the port here, then configure the operating system to translate the port.

Application: Specifies the SSL VPN server application path.

Redirect Requests from Non-Secure Port to Secure Port: Specify this option to redirect the browsers to the secure port in order to establish an SSL connection. If this option is not selected, browsers that connect to the non-secure port are denied service.

SSL VPN Certificate: Configure a certificate for SSL. You can click the icon to select a certificate. If you have installed the Identity Server and the SSL VPN server on the same machine, then same certificate is used for both the services.

Embedded Service Provider Certificate: Configure a certificate for the Embedded Service Provider to communicate with the Identity Server. You can click the icon to select a certificate.

The following URLs are displayed when the Published DNS name is populated:

- **Login URL:** Displays the URL that you need to use for logging users in to the protected resources.
- **Logout URL:** Displays the URL that you need to use for logging users out of protected resources.
- **Metadata URL:** Displays the location of the metadata.
- **Health Check URL:** Displays the location of the health check.

4 Restart the Tomcat server when prompted.

5 To save your modifications, click *OK,* then click *Update* on the Configuration page.

6 Click *Update* on the Identity Server Configuration page.

7 (Optional) Proceed with Chapter 11, “Configuring the IP Address, Port, and NAT,” on page 75, if you have not already configured the SSL VPN server details.

Accelerating the Traditional Novell SSL VPN

10

NOTE: If you have installed the ESP-enabled Novell® SSL VPN, skip this section and make sure that you have completed Chapter 9, "Configuring Authentication for ESP-Enabled Novell SSL VPN," on page 67.

If you have installed the traditional Novell SSL VPN, this is a mandatory configuration in order to accelerate the SSL VPN server.

This section has the following information:

10.1 Configuring the Default Identity Injection Policy

The SSL VPN server requires a user credential profile consisting of the following elements:

- Username and password information
- A proxy session cookie
- The roles assigned to the current user for authentication information

Each element added to the custom header requires a name with an "X-" prefix. The name you enter is specific to the application using the custom header, and might be case sensitive. You need to obtain this information from the application before creating the custom header. The Access Gateway injects these headers into the SSL VPN server.

The SSL VPN server requires the following three headers:

- Authentication header containing the credential profile with a username and password
- Custom header containing a proxy session cookie element named X-SSLVPN-PROXY-SESSION-COOKIE
- Custom header containing roles for current user element, named X-SSLVPN-ROLE

You can configure Access Gateway to inject the client IP address as a custom header along with the other three headers. This custom header should be named X-SSLVPN-CLIENTIP. This enables logging of the client IP address for SSL VPN. This is an optional configuration and is not enabled by default. If it is not enabled, the SSL VPN server reports it to the Audit server as a connection accepted from `Unknown Host`.

To add this header to the SSL VPN policy:

1. In the Administration Console, click *Devices* > *Access Gateway*s > *Policies*.
2. (Conditional) If you have not created the SSL VPN default policy, click *Create SSL VPN Default*. Then click *Apply Changes*.

3 In the list of policies, click *SSLVPN Default* > 1.

4 In the *Actions* section, click *New*, then select *Inject into Custom Header*.

5 Fill in the following values:

Custom Header Name: Specify *X-SSLVPN-CLIENTIP*.

Value: Select *Client IP*.

6 Click *OK* twice.

7 Click *Apply Changes*.

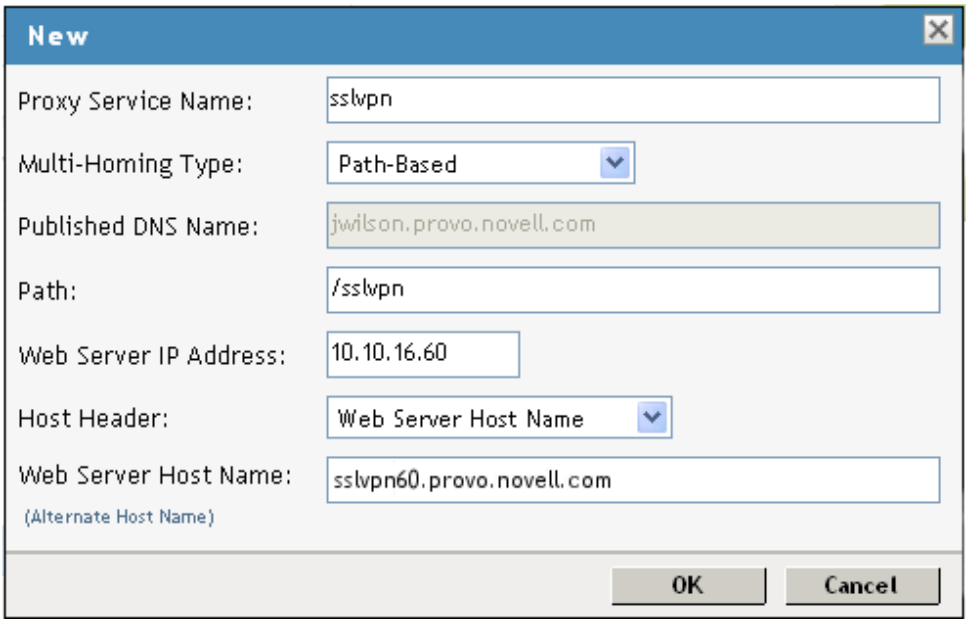
10.2 Injecting the SSL VPN Header

The example in this section explains how to accelerate SSL VPN server in a path-based multi-homing configuration.

Before you begin, make sure you have already created a proxy service and an authentication procedure. For more information on creating a proxy service and authentication procedure, see "Configuring a Reverse Proxy" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

1 In the Administration Console, click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

2 In the *Proxy Service List* section, click *New*.



3 Fill in the following fields:

Proxy Service Name: Specify a name for the proxy service.

Multi-Homing Type: Specify the method for finding a second resource on the reverse proxy. For this example configuration, *Path-Based* has been selected.

Published DNS Name: This field is populated by default with the published DNS name.

Path: Specify the path to the SSL VPN resource. This must be `/sslvpn`.

Web Server IP Address: Specify the public IP address of the SSL VPN server.

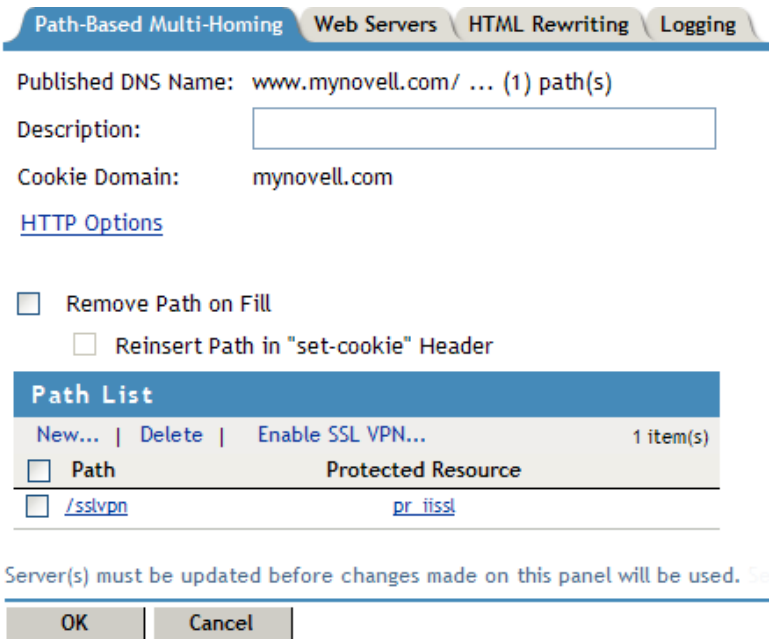
NOTE: If the SSL VPN server and the Linux Access Gateway are installed on the same machine, configure the loopback IP address 127.0.0.1 as the Web Server IP address. For more information on configuring the loopback IP address, see Section 17.1, "Understanding How SSL VPN Connects Through a Forward Proxy," on page 109.

Host Header: Select which hostname is forwarded to the Web server in the host header. If your SSL VPN server has a DNS name, select *Web Server Host Name*.

Web Server Host Name: Specify the DNS name of the SSL VPN server.

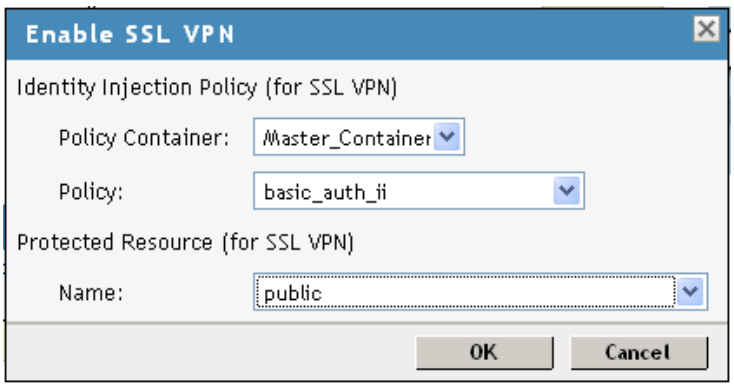
4 Click *OK*.

5 To configure the default Identity Injection policy and protected resources, click the newly added proxy service.



6 In the *Path List* section, make sure the *Path* is */sslvpn*.

7 In the *Path List* section, select the */sslvpn* check box, then click *Enable SSL VPN*. The Enable SSL VPN pop-up is displayed.



8 Fill in the following fields:

Policy Container: Select a policy container from the list.

Policy: Select *Create SSL VPN Default Policy* from the drop-down list. A policy pop-up appears. Click *Apply Changes* in the pop-up, then click *Close*.

The default SSL VPN policy injects both the username and password in the authentication header. If you do not want the password to be pushed to the authentication header, configure a policy with a username and a string constant. For more information on configuring policies, see "Creating Identity Injection Policies"in the *Novell Access Manager 3.1 SP1 Policy Management Guide*

You can also configure the SSL VPN policy to inject the client IP address, so that the IP address can then be included in log entries. For more information, see Section 10.1, "Configuring the Default Identity Injection Policy," on page 69.

Name: Select *Create SSL VPN Default Protected Resource* from the drop-down list.

9 Click *OK* to close the *Enable SSL VPN* pop-up.

10 Click the *Web Servers* tab.

11 Specify 8080 in the *Connect Port* field, then click *OK*.

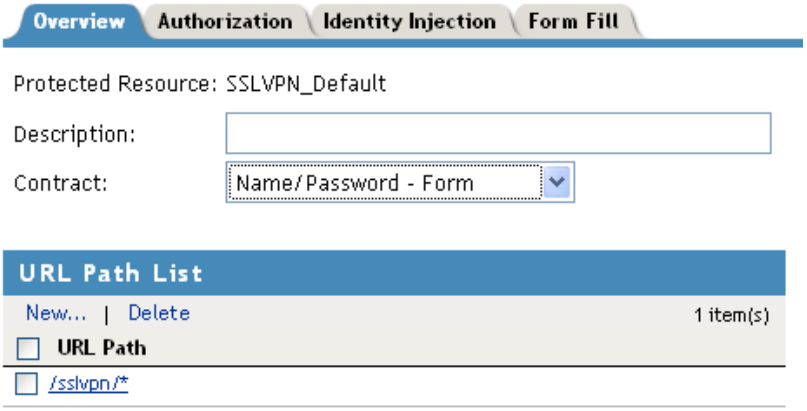
12 In the *Proxy Service List* section, click the name of the parent proxy service of the newly created SSL VPN proxy service. This host does not have a multi-homing value.

13 Select the *Protected Resources* tab.

14 Select *SSLVPN_Default* from *Protected Resources List*.

15 Select an authentication contract from the *Contract* drop-down list. Make sure you select *Name/Password - Form* as the authentication contract.

16 In the *URL Path List* section, ensure that the URL is */sslvpn/**.



IMPORTANT: Make sure that you configure the URL as given above. Any variation leads to the failure of SSL VPN service.

17 Click *Configuration Panel,* then click *OK*.

18 On the *Configuration* page, click *OK*.

19 On the Access Gateways page, click *Update*.

20 To update the Identity Server, click *Identity Servers* > *Update*.

21 Click *Close*.

22 (Optional) Proceed with Chapter 11, “Configuring the IP Address, Port, and NAT,” on page 75, if you have not already configured the SSL VPN server details.

Configuring the IP Address, Port, and NAT

11

The Gateway Configuration page displays the current configuration of the SSL VPN server, such as the external IP address if the SSL VPN server is behind NAT, the listening IP address, TCP encryption port, connection manager port, and the type of encryption used.

This section describes how to configure the IP addresses, port, subnet address and subnet mask, and protocol for SSL VPN.

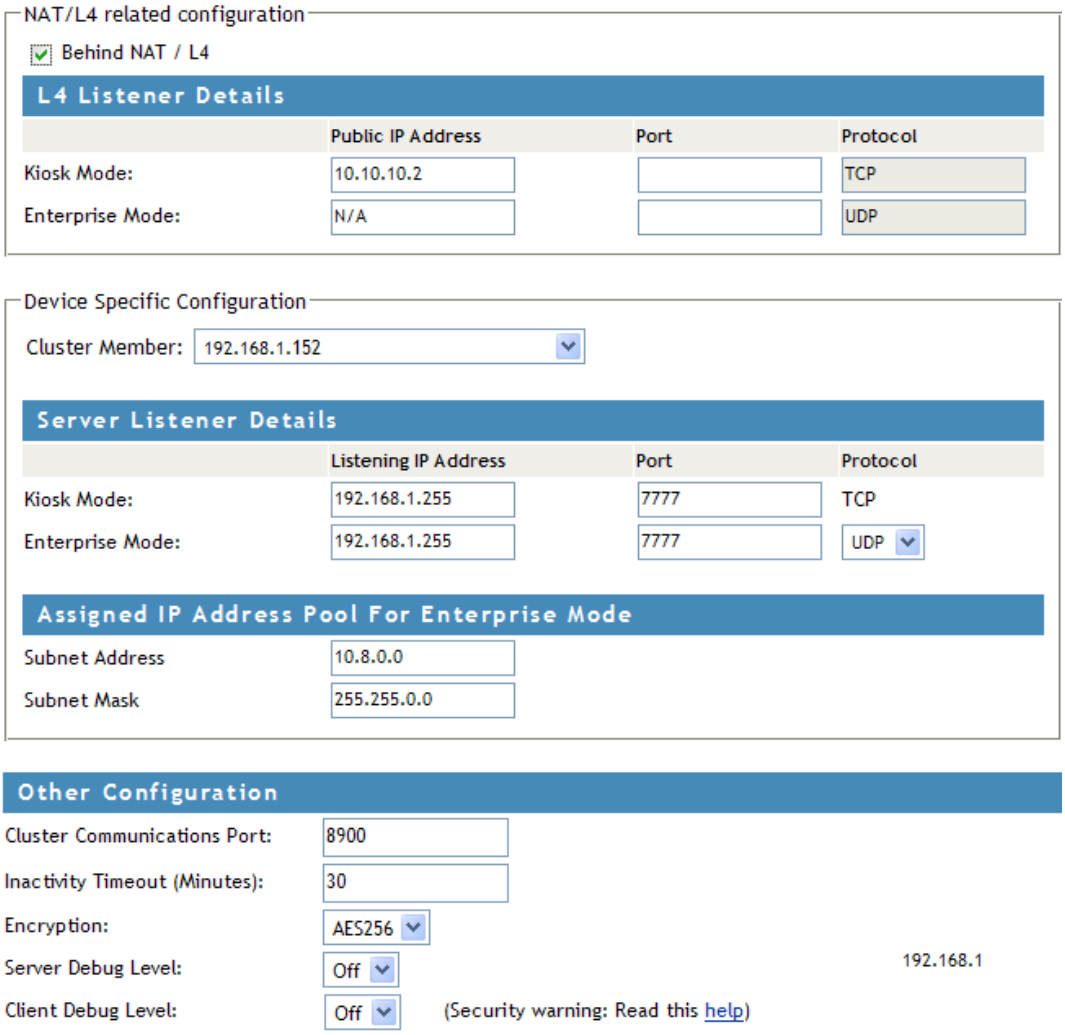
11.1 Configuring the SSL VPN Gateway Behind NAT or L4

To configure SSL VPN behind NAT (Network Address Translation) or by using an L4 server:

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

   The Server configuration page is displayed.
2. Select *Basic Configuration* from the *Gateway Configuration* section.

   The SSL VPN Basic Configuration page is displayed.



3 Specify the following NAT/L4 configuration as follows:

Behind NAT/L4: Select the check box to specify that the SSL VPN Gateway is behind NAT.

Public IP Address: This field is enabled when the *Behind NAT* check box is selected. Specify the public IP address (that is, the address exposed to the Internet user) that translates into the SSL VPN Gateway IP address. This is the IP address where the external user on the Internet must be able to access the SSL VPN server.

Port: Specify a port number for Kiosk mode as well as for Enterprise mode when the SSL VPN server is behind an L4 or a NAT.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN server is behind an L4 or a NAT. The protocol is TCP for Kiosk mode and UDP for Enterprise mode.

4 Specify the device-specific configuration as follows:

Cluster Member: Select the cluster member from a list of IP addresses.

Listening IP Address: Specify the IP address that the SSL VPN listens on.

Port: Specify a port number for Kiosk mode as well as for Enterprise mode when the SSL VPN server is behind an L4 or a NAT. Make sure that the port you specify here is free.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN server is behind an L4 or a NAT. The protocol is TCP for Kiosk mode, but it can either be TCP or UDP for Enterprise mode.

5 Specify the following information to configure the assigned IP address pool for Enterprise mode:

Subnet Address: Specify the IP address of the subnet pool where SSL VPN assigns the IP address to each client in Enterprise mode. For this assigned IP address pool to work properly, you must configure the routing table and source NAT. For more information, see Chapter 12, "Configuring Route and Source NAT for Enterprise Mode," on page 81.

Subnet Mask: Specify the subnet mask for Enterprise mode.

The values specified in the *Subnet Address* and *Subnet Mask* fields determine the IP addresses that are assigned to the clients. Make sure that the assigned IP address and the IP address of the client do not match.

6 Specify the other configuration as follows:

Cluster Communications Port: Specify the port that is used for communication between the cluster members.

Inactivity Timeout (Minutes): You can configure the time in minutes. If no data exchange takes place during the stipulated time, the connection is closed so that the resources are freed to allow additional incoming connections. The inactivity timeout period can be one minute to 1800 minutes. The default inactive timeout period is 30 minutes.

Encryption: Select the type of encryption. It can be either AES128 or AES 256.

Enterprise Mode Compression: Specify if you want to enable compression in Enterprise mode in order to reduce the time taken to establish connection.

Server Debug Level: Set this option to *On* if you want to get more debug information from the server. This option is set to *Off* by default.

Client Debug Level: Set this option to *On* if you want to get more debug information from the client side. This option is set to *Off* by default.

7 To save your modifications, click *OK,* then click *Update* on the Configuration page.

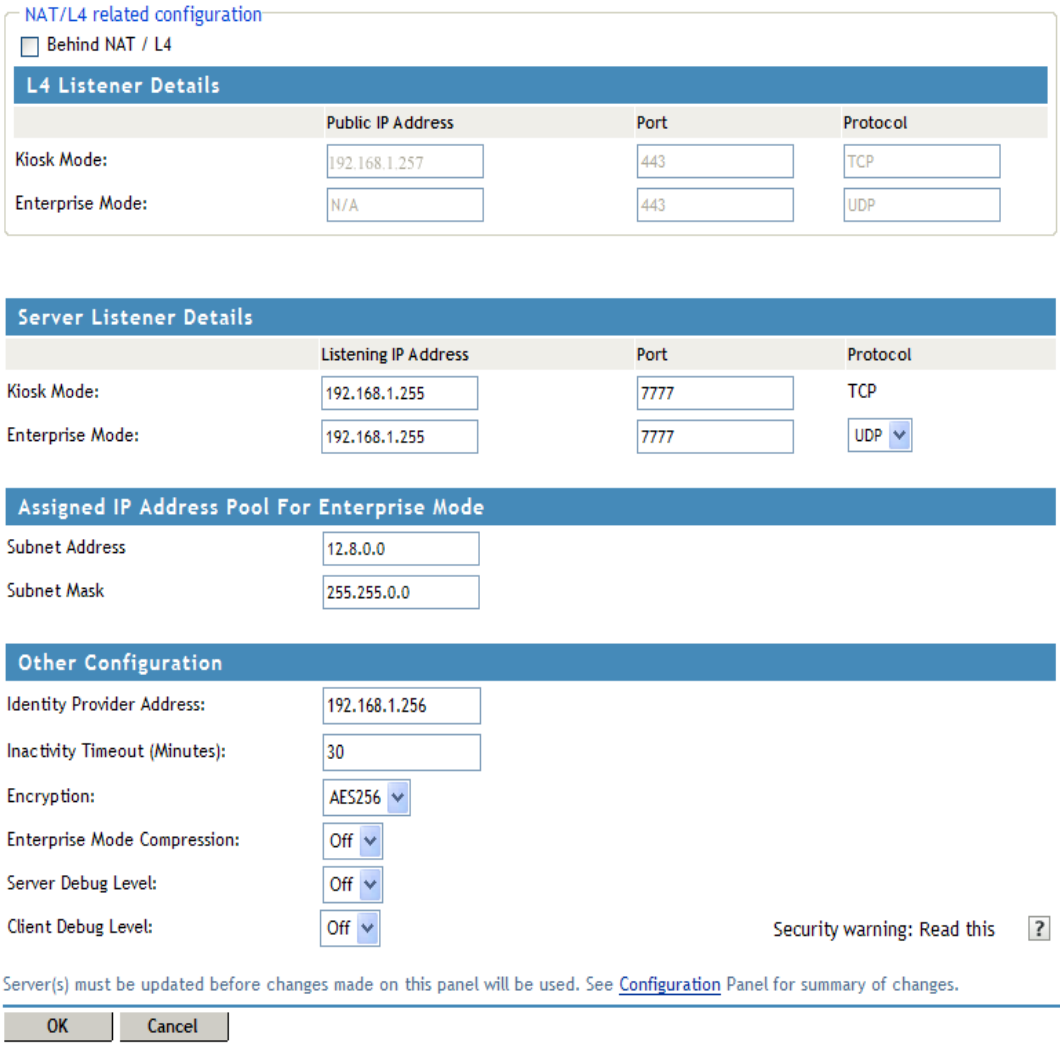
11.2 Configuring the SSL VPN Gateway Without NAT or L4

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

The Server configuration page is displayed.

2 Select *Basic Configuration* from the *Gateway Configuration* section.

The SSL VPN Gateway Basic Configuration page is displayed.



3 Specify the device-specific configuration as follows:

Cluster Member: Select the cluster member from a list of IP addresses.

Listening IP Address: Specify the IP address that the SSL VPN listens on.

Port: Specify a port number for Kiosk mode as well as for Enterprise mode when the SSL VPN server is behind an L4 or a NAT. Make sure that the port you specify here is free.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN server is behind an L4 or a NAT. The protocol is TCP for Kiosk mode, but it can either be TCP or UDP for Enterprise mode.

4 Specify the following information to configure the assigned IP address pool for Enterprise mode:

Subnet Address: Specify the IP address of the subnet pool where SSL VPN assigns the IP address to each client in Enterprise mode. For this assigned IP address pool to work properly, you must configure the routing table and source NAT. For more information, see Chapter 12, “Configuring Route and Source NAT for Enterprise Mode,” on page 81.

Subnet Mask: Specify the subnet mask for Enterprise mode.

The values specified in the *Subnet Address* and *Subnet Mask* fields determine the IP addresses that are assigned to the clients. Make sure that the assigned IP address and the IP address of the client do not match.

5 Specify the other configuration as follows:

Cluster Communications Port: Specify the port that is used for communication between the cluster members.

Inactivity Timeout (Minutes): You can configure the time in minutes. If no data exchange takes place during the stipulated time, the connection is closed so that the resources are freed to allow additional incoming connections. The inactivity timeout period can be one minute to 1800 minutes. The default inactive timeout period is 30 minutes.

Encryption: Select the type of encryption. It can be either AES128 or AES 256.

Server Debug Level: Set this option to *On* if you want to get more debug information from the server. This option is set to *Off* by default.

Client Debug Level: Set this option to *On* if you want to get more debug information from the client side. This option is set to *Off* by default.

6 To save your modifications, click *OK,* then click *Update* on the Configuration page.

Configuring Route and Source NAT for Enterprise Mode

12

In Enterprise mode, SSL VPN assigns IP addresses to each client from subnet specified in the configuration. For more information on configuring IP address, see Chapter 11, “Configuring the IP Address, Port, and NAT,” on page 75. The values specified in the *OpenVPN Subnet Address* and *OpenVPN Subnet Mask* fields determine the IP addresses that are assigned to the clients. Make sure that the assigned IP address and the IP address of the client do not match.

The packets from these clients reach the application server with the IP address of the client as the source address. The response packets need to be routed back to the SSL VPN server, which sends them on to the clients. You can solve this routing problem in one of the following ways:

12.1 Configuring the OpenVPN Subnet in Routing Tables

If you have a gateway for your network between the application server and the SSL VPN server, you can configure the gateway to send the dynamically assigned IP addresses from the OpenVPN address pool to the SSL VPN server. This is the best routing approach because most applications, including ActiveFTP and TFTP, can work in this type of environment. To establish this type of routing, you need to add a static route to your network’s routing infrastructure so that traffic to the OpenVPN subnet pool of addresses is sent via the SSL VPN gateway.

12.2 Configuring Source NAT for SSL VPN

You can configure the source NAT (SNAT) for SSL VPN Enterprise mode to change the dynamically assigned client addresses to the address of the SSL VPN server before sending them to the application server. The application server can then use the source address in the packets to send them back to the SSL VPN server, which can then reassign the client address and send the packets on to the client. This is the best approach if you are using SSL VPN for TCP and UDP applications. Other applications, such as ActiveFTP and TFTP, cannot work in this type of environment.

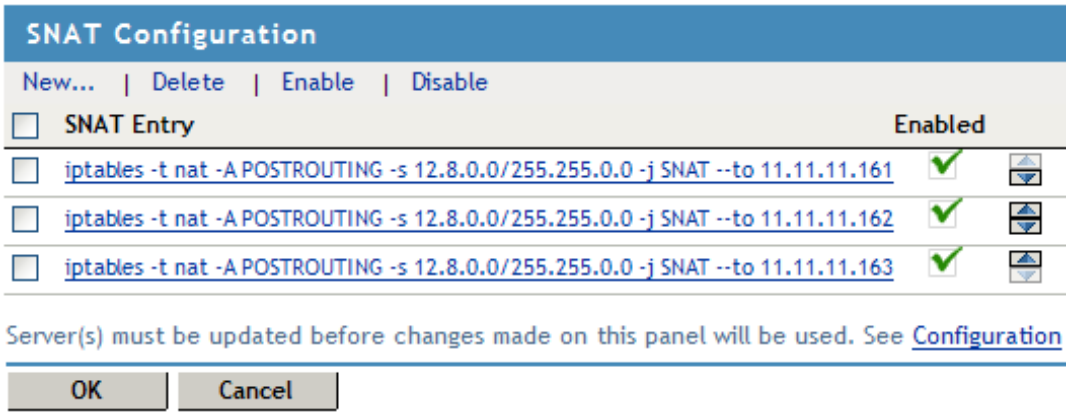
To establish this type of routing, you need to create an entry in the iptables rule on the SSL VPN server.

12.2.1 Configuring SNAT for Enterprise Mode

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

   The Server configuration page is displayed.
2. Select *Advanced Configuration* from the *Gateway Configuration* section.

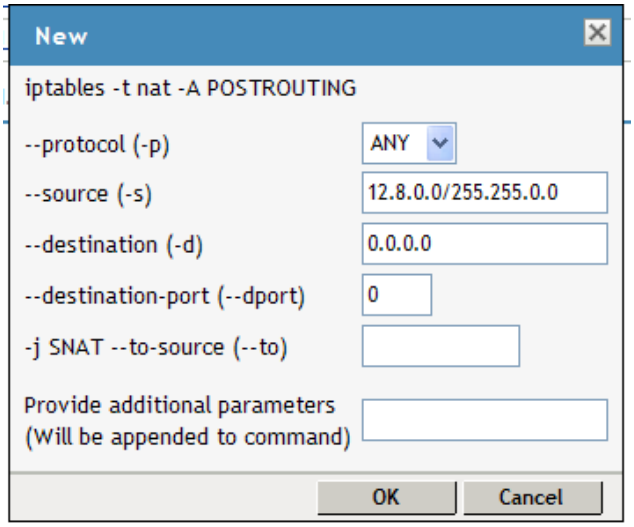
The SSL VPN Advanced Configuration page is displayed.



3 If the SSL VPN server is a member of a cluster, the *Cluster Member* option is displayed. The SNAT Entry configuration is specific to different cluster members. Select the IP address of the cluster member for which you want to configure the SNAT entry.

4 To configure a new SNAT entry click *New*.

The New dialog box opens.



5 Specify the information in the following format:

--protocol (-p): This is an optional parameter. To specify a protocol, select a protocol from the list. The protocol can be ANY, UDP, TCP or ICMP. By default, the ANY option is selected.

--source (-s): Specifies the IP address of the subnet pool where SSL VPN assigns the IP address to each client in Enterprise mode.

NOTE: This field is populated by the Enterprise mode IP address by default. But, you can edit the value in this field if you want to use this field to add iptables SNAT entries for other cases in Kiosk mode such as for full tunneling.

--destination (-d): This is an optional parameter. You can either specify the host IP address or the destination IP address or specify the IP address and the network mask combination in the following format:

<destination>/<SubnetMask>

The Network mask should be in the dotted decimal format only.

--destination-port (--dport): This is an optional parameter. You can specify the destination port.

-j SNAT --to-source (--to): This is a mandatory parameter. Specify a valid IP address of SSL VPN server.

Provide additional parameters (Will be appended to command): You can add any other parameters depending on your requirements. But, these parameters will not be validated.

Click *OK*.

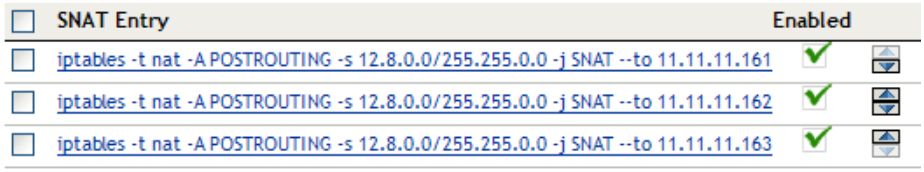
The new SNAT entry is displayed in the following format:

```
iptables -t nat -A POSTROUTING -p <Any> s <openVPNSubnetIP> -d
<destinationIP> --dport <destinationPort> -j SNAT --to <privateIPSSLVPN>
<additional parameters>
```

6 To save your modifications, click *OK,* then click *Update* on the Configuration page.

12.2.2 Ordering SNAT Entries

You can configure SNAT rules for a user's role. However, the SNAT entries are process based on their order. If you want to change the order of the rules based on their priority, you can click the up or down arrows to move them up or down respectively.



Configuring DNS Servers and Certificates

13

Some configurations are common to both the ESP-enabled Novell® SSL VPN and SSL VPN protected by the Access Gateway:

13.1 Configuring DNS Servers

The DNS servers configured here are pushed to the client from the SSL VPN server during the connection.

You can configure DNS servers for Enterprise mode through the Administration Console. The DNS servers can be configured for Kiosk mode either during the installation if you are installing Linux Access Gateway and SSL VPN on the same machine, or by using YaST after the installation.

13.1.1 Configuring DNS Servers for Enterprise Mode

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

   The Server configuration page is displayed.

2. Select *DNS Server List* from the *Basic Gateway Configuration* section.

   The DNS server list page is displayed.

3. To configure a DNS server, click *New* in the *DNS server* section, specify the IP address of the server, then click *OK*.
4. To configure a domain, click *New* in the *Domains* section, specify the domain name, then click *OK*.

5 To delete a DNS server or a domain, select the check box next to the field and click *Delete* in the section.

6 To save your modifications, click *OK,* then click *Update* on the Configuration page.

13.1.2 Configuring DNS Servers for Kiosk Mode

The DNS servers can be configured for Kiosk mode either during installation or by using YaST The configuration procedure is dependent on whether you have installed SSL VPN and the Linux Access Gateway on the same machine or on separate machines.

NOTE: You must configure the DNS server for both Kiosk mode and Enterprise mode. For information on configuring DNS servers for Enterprise mode, see Section 13.1.1, "Configuring DNS Servers for Enterprise Mode," on page 85.

Configuring DNS Servers During Installation

If you are installing SSL VPN and the Linux Access Gateway on the same machine, you can configure DNS Servers during the Linux Access Gateway installation. For more information, see "Installing the Linux Access Gateway Appliance" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

Configuring DNS Servers After the Installation

If you are installing SSL VPN and the Linux Access Gateway on separate machines, you can configure DNS servers in the `/etc/resolv.conf` file by using YaST as follows:

1 In YaST, select *Network Devices* > *Network Cards*, then press Enter.

2 Select *Change*, then press Enter.

3 Select *Edit*, then press Enter.

4 Select *Hostname and Name Servers*, then press Enter.

5 Specify the IP addresses of the DNS servers that you want to add.

6 Specify the domain names.

7 Click *OK*.

Verify that the DNS servers and domain names are added to the `/etc/resolv.conf` file.

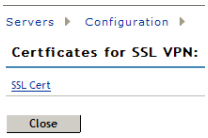
13.2 Configuring Certificate Settings

Access Manager components and agents can access the keystore to retrieve certificates, keys, and trusted roots as needed.

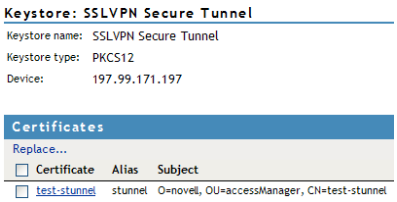
Before you proceed with this section, make sure you have already created a certificate. For more information on creating certificates, see "Security and Certificate Management"*Novell Access Manager 3.1 SP1 Administration Console Guide*.

NOTE: Make sure that SSL VPN certificate names contain only alphanumeric characters, space, underscore (_), hyphen (-), the at symbol @, and the dot (.).

1. In the Administration Console, select *Devices* > *SSL VPN* > *Edit*.
2. Select *SSL VPN Certificates* from the *Security settings* section. The Certificates for SSL VPN page is displayed.



3. Click *SSL Cert*. The Keystore: SSL VPN Secure Tunnel page is displayed.



Certificates in the SSL VPN STunnel are used by SSL VPN services for encryption. This page contains the following information:

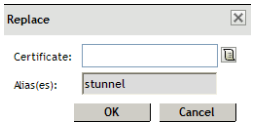
Keystore name: Specifies the name of the keystore to which the certificate belongs.

Keystore type: Specifies the type of keystore. It can be Java, PEM, or PKCS12.

Device: Specifies the IP address of the SSL VPN device.

NOTE: Every imported SSL VPN device has a default certificate.

4. To replace the default certificate, click *Replace*. The Replace dialog box is displayed.



Fill in the following fields:

Certificates: Click the *Select Certificate* icon to browse and select the certificate that you want to associate with SSL VPN.

Alias(es): You can provide an alternate name for the certificate you are importing.

5. Click *OK* to save changes.
6. To save your modifications, click *OK,* then click *Update* on the Configuration page.

Configuring End-Point Security and Access Policies for SSL VPN

14

Novell® SSL VPN has a set of client integrity check policies to protect your network and applications from clients that are using insufficient security restraints. SSL VPN also allows you to configure traffic policies to control access to resources based on the role of the client, and allows you to configure the client to access the resources either in Kiosk mode only or in Enterprise mode only.

You can configure a client integrity check policy to run on the client workstations before establishing a tunnel to the SSL VPN gateway. This check ensures that the users have specified software installed and running in their systems. You can also configure different levels of security and assign them to traffic policies.

The traffic policies are a set of rules and regulations, administered to regulate user access to the protected network resources based on the role of the user and the security level adhered to by the client machine. The policies ensure that certain actions take place when the user tries to establish an SSL VPN connection:

1. A client integrity check is performed on the client machine to determine if the client has the required firewall or antivirus installed on the machine. For more information on how to configure client integrity checks, see Section 14.1.3, “Configuring Applications for a Category,” on page 92. If the client fails the integrity check, one of the following actions occurs:
    a. If there is a traffic policy configured for that user’s role with the security level as none, the SSL VPN connection is established with minimal access to that client.
    b. If there is no traffic policy configured for that user’s role with the security level as none, the SSL VPN connection fails.
2. If the client passes the client integrity check, the level of security at the client machine is determined depending on the requirements for the different levels configured and the software installed in the client machine. For more information on how to configure security levels, see Section 14.2, “Configuring Client Security Levels,” on page 95.
3. If the client adheres to the accepted security level, then the SSL VPN connection is made and the secure tunnel is established between the SSL VPN client and server.

NOTE: ◆When the tunnel is up, if some changes are made to the Client Integrity Check policy, client policy or the traffic policy and the changes alter the security level of the client, you must restart the server to force the clients to reconnect with the new security level that applies to them.

◆When the tunnel is up, if the user installs a new software that enhances the security level of the client, the SSL VPN connection continues without the tunnel being disconnected. But if the security level of the client is changed to a lower level because the client deleted some of the CIC resources, the SSL VPN connection is disconnected. When the user logs in again, new policies applicable to the changed level are imposed on the user.

4. The user is then given access to different resources based on the traffic policies configured for the role of the user and the security levels adhered to by the user. For more information on how to configure traffic policies for different roles, see Section 14.3, "Configuring Traffic Policies," on page 97.

14.1 Configuring Policies to Check the Integrity of Client Machine

You can configure a client integrity check policy to verify if the prescribed software (such as firewall and antivirus software) is installed on the client machine. You can configure different policies for Windows, Linux, and Macintosh machines, then specify applications that must be present in the client machines in order to pass the client integrity check. To configure the client integrity check policy:

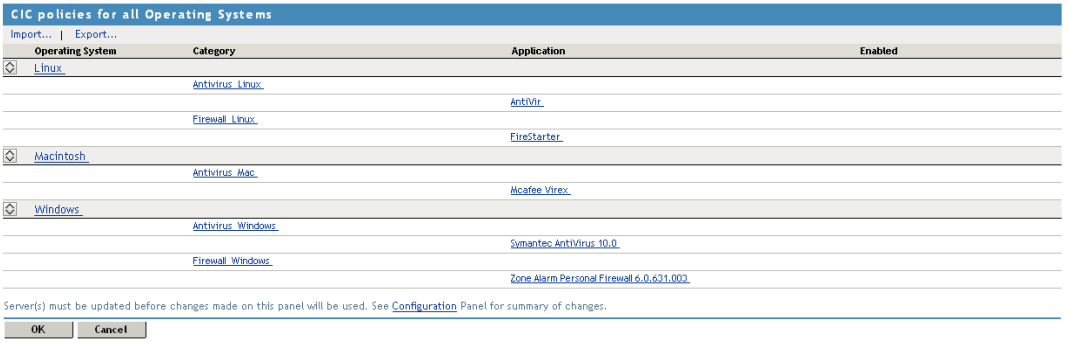
1. Select the operating system.
2. Configure the category.
3. Configure applications for a category.
4. Configure attributes for each of these applications.

A category that you have configured can be deleted only if it is not assigned to any of the security levels. This section has the following information:

14.1.1 Selecting the Operating System

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

2 Select *Client Integrity Check Policies* from the *Policies* section. The Client Integrity Check Policies page is displayed.



3 Select the operating system.

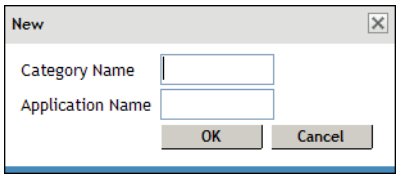
Next, you must configure a category of software that needs to be present in the client machine.

4 Continue with Section 14.1.2, “Configuring the Category,” on page 91.

14.1.2 Configuring the Category

A category is a group of similar software. For example, a firewall category can contain a list of firewalls such as the Windows firewall and ZoneAlarm* firewall. You can configure multiple software categories for a single client integrity check policy.

1 To add a new category, click *New*. The New dialog box is displayed.



2 Specify a name for category and a name for the application in the *Category Name* and the *Application Name* fields respectively, then click *OK*.

3 To enable the newly added category, select the category, then click *Enable*.

4 To disable a category that is already enabled, select the category, then click *Disable*.

5 To delete a category, select the category, then click *Delete*.

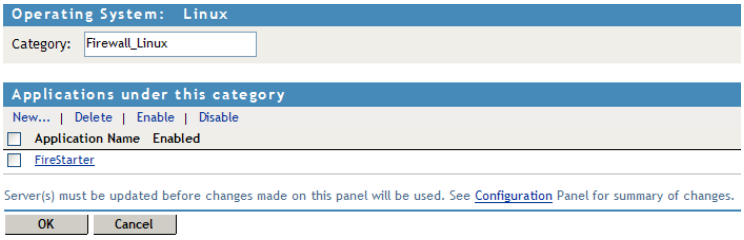
6 Click *OK* to save your modifications, then click *Update* on the Configuration page.

7 Continue with Section 14.1.3, “Configuring Applications for a Category,” on page 92.

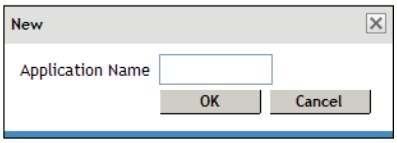
14.1.3 Configuring Applications for a Category

A category consists of group of applications. You can add more than one application under a category. A client workstation is checked for the presence of any one of the software items in the category.

1 To configure or add applications to a category, click the category. The Client Integrity Check - Category page is displayed.



2 To add a new application click *New*. The new dialog box is displayed.



3 Specify an application name, then click *OK*.

4 Select the newly added application, then click *Enable*.

5 To disable an application that is already enabled, select the application, then click *Disable*.

6 To delete an application, select the application, then click *Delete*.

7 Click *OK* to save your modifications, then click *Update* on the Configuration page.

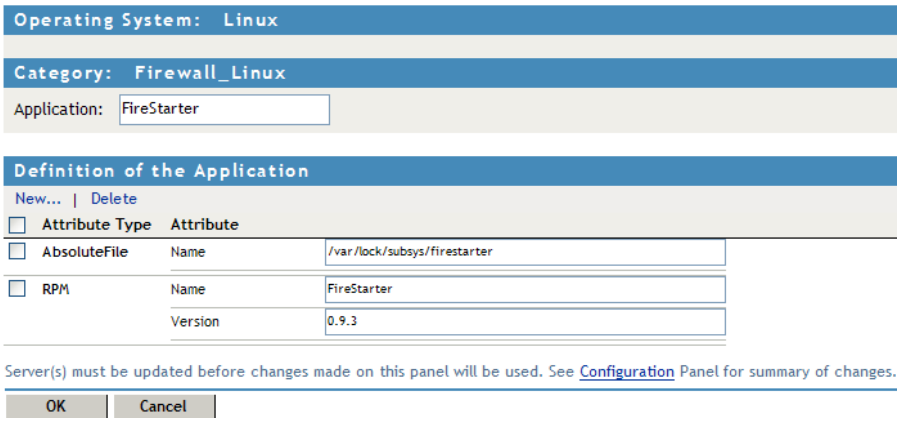
8 Continue with Section 14.1.4, “Configuring Attributes for an Application,” on page 92.

14.1.4 Configuring Attributes for an Application

After you have added an application to a category, you must configure the attributes to each of these applications. These attributes can be in the form of RPMs, processes, registry keys or executable files. The Client Integrity checks detects the presence of these attributes. For example, if you have specified in the client integrity check that

1 To add a new attribute, click *New*, specify an attribute name, then click *OK*.

2 Click the application to add application details and attributes. The Application Details and Attributes page is displayed.



3 Specify details for the attributes. The following table lists the attributes for applications on different operating systems:

Operating System	Attribute Type	Attribute Name
Linux	RPM	**Name:** Specify the name of the RPM that must be present in the client machine.
		Version: Specify the version of the RPM that must be present in the client machine.
	Process	**Name:** Specify the name of the process that must be present in the client machine.
		Owner: Specify the owner of the process.
	Absolute File	**Name:** Specify the name and absolute path of the file that must be present in the client machine.

Operating System	Attribute Type	Attribute Name
Windows	Process	**Name:** Specify the name of the executable file that must be present in the client machine. **Version:** Specify the version of software process that must be running in the client machine. **RegistryKey:** Specify the registry key name and absolute path. **RegistryKeyValue:** Specifies registry key value. The value data found in this key value should be the absolute path of the folder where the process file is present.
	RegistryKey	**Name:** Specify the name and absolute path of the registry key that must be present in the client machine. **Value Name:** Specify the name of the registry key value. **Value Data:** Specify a data for the registry key value. This data can be for registry type REG_BINARY, REG_DWORD, REG_DWORD_LITTLE_ENDIAN, REG_MULTI_SZ, or REG_SZ. The value for REG_DWORD and REG_DWORD_LITTLE_ENDIAN, is hexadecimal or decimal.The value of a REG_MULTI_SZ, REG_SZ can be a string value or, numeric or alphanumeric.And the value of REG_BINARY can be binary or hexadecimal. The Value name and Value data are separated by a comparison operator such as `=, >. <, <=, >=.` You must always use = with a string or with the registry type REG_BINARY. You can use any comparison operator with other registry types For example, if the Registry key name is specified as `RegKey` with a Value Name of `RegValue`, comparison operator of = and Value Data of `RegData`, then, the client integrity check process looks for the presence of `RegKey` with a value name `RegValue` = value data `RegData` in the client machine. If the registry is present with the specified values, then the client passes the client integrity check.
	Absolute File	**Name:** Specify the name and absolute path of the file that must be present in the client machine. **Version:** Specify the owner of the process.
	Service	**Name:** Specify the display name of the service. **Status:** Specify the status of the process in the client machine. The status of the process can be *Running* or *Stopped*.

Operating System	Attribute Type	Attribute Name
Macintosh	Package	**Name:** Specify the name of the software package that must be present in the client machine.
		Version Specify the version of the software package
	Process	**Name:** Specify the name of the executable file that must be present in the client machine.
		Owner: Specify the owner of the process.
	Absolute File	**Name:** Specify the name and absolute path of the file that must be present in the client machine.

4 To delete an attribute, select the attribute, then click *Delete*.

5 Click *OK* to save your modifications, then click *Update* on the Configuration page.

6 To continue with configuring a connection and traffic policy for a client, proceed with Section 14.2, “Configuring Client Security Levels,” on page 95.

14.1.5 Exporting and Importing Client Integrity Check Policies

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

2 Select *Client Integrity Check Policies* from the *Policies* section. The Client Integrity Check Policies page is displayed.

3 Select the policies that you want to export, then click *Export*.

4 Specify a filename for the XML document that saves the configuration.

5 Specify a location to save the XML file.

6 To import the exported XML file, select the server into which you want to import the client integrity check policies.

7 Click *Import* in the Client Integrity Check policies page.

8 Browse and select the XML file that contains the saved client integrity check policies.

9 To save your modifications, click *OK*, then click *Update* on the Configuration page.

14.2 Configuring Client Security Levels

You can configure SSL VPN server to send traffic on the SSL VPN tunnel based on the level of security configured at the client machine. You can decide the categories of software that you want to be present for each level. You can configure the following security levels:

- **Least Secure:** Specifies the minimum categories of software that must be present on a client machine for the client to be at the lowest secure level. When a client is at a least secure level, you can configure the traffic policies so that the client has access to limited set of resources.
- **Moderately Secure:** Specifies the categories of software that must be present on a client machine for the client to be at a moderately secure level. When a client is at a moderately secure level, you can configure the traffic policies accordingly.

- **Secure:** Specifies the software categories that must be present on a client machine for the client to be secure. When a client is at a secure, the traffic policies can be configured so that the client has access to all or most of the protected resources, depending on the role of the client.
- **None:** If a client does not have any of the software such as firewall or antivirus specified in the client integrity check policy, then the security level of that client is None. When a client is at this level, the SSL VPN connection is established, but the client is given access to only a minimal set of resources.

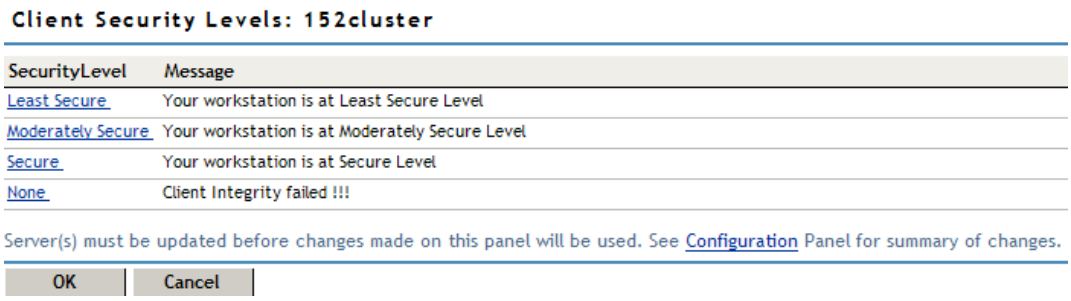
In some circumstances you cannot configure a custom security level of a client.

- If, during the client integrity check, a client is found to have a certain level of security, then all the policies under that level as well as the policies under the lower security levels are imposed on the client. For example, if the client passes the security level check as Moderately Secure, then all the policies for this level as well as policies for Least Secure and None are imposed on the client.
- If you change the requirements for a particular security level, the changes are applied only to new user connections. For example, a client that has established the SSL VPN connection is currently at the Secure level. You now add a new the requirement for the Secure level, so the client that is already connected at the Secure level now does not meet the requirements for the new Secure level. In this scenario, the client that is already connected continues to be connected to the server. The new policies are applicable only to new connections.

NOTE: If you want to impose the new policies for clients that are already connected, you must force the clients to reconnect by restarting the SSL VPN server.

To configure a client security level:

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Client Security Levels* from the *Policies* section. The Client Security Levels page is displayed.



The following security levels can be configured:

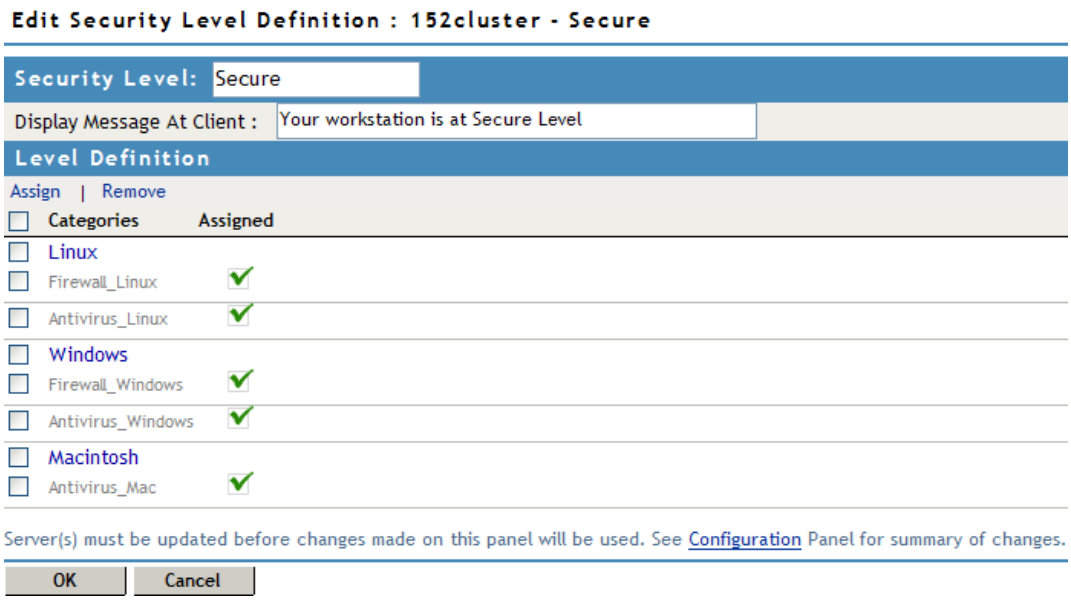
Least Secure: You can configure this level for a client that has met the minimal requirement for the client integrity check.

Moderately Secure: You can configure this level for a client that has met the moderate requirements for the client integrity check.

Secure: You can configure this level for a client that has met all the requirements for the client integrity check.

None: You can configure this level to provide minimal access to resources for a client, who that has failed the client integrity check.

3 Click a security level to configure. The Edit Security Level Definition page is displayed.



Any category that is not enabled in the Client Integrity Check policy appears as dimmed.

4 To assign a category for a level, select categories under each operation system, then click *Assign*.

5 To remove a category for a level, select the category, then click *Remove*.

6 To save your modifications, click *OK,* to save your modifications, then click *Update* on the Configuration page.

14.3 Configuring Traffic Policies

You can configure a maximum of 250 traffic rules per role, depending on the length of the policy name. If you have configured multiple traffic policies, the policies are prioritized based on the order of their creation.

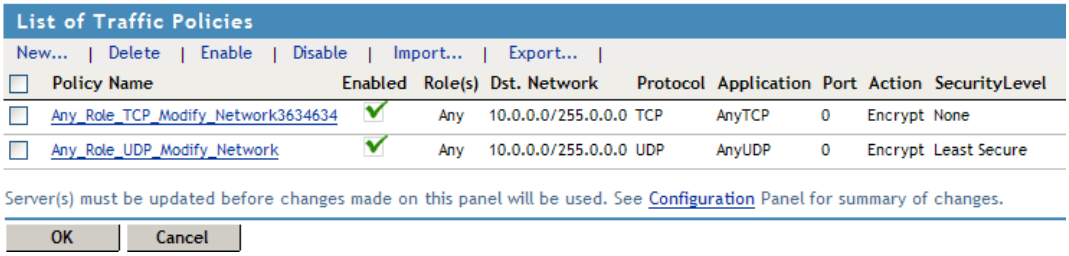
The roles for a user are created in the Identity Server. These roles are displayed in the traffic policies page by default. But SSL VPN traffic policies cannot be tightly coupled with the roles created for the Identity server. In scenarios such as a federated setup, where the role can be injected from another Identity Server, you can add or remove the user-configured roles, while creating the traffic policies.

14.3.1 Configuring Traffic Policies

You can configure a different set of traffic policies for different roles as follows:

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

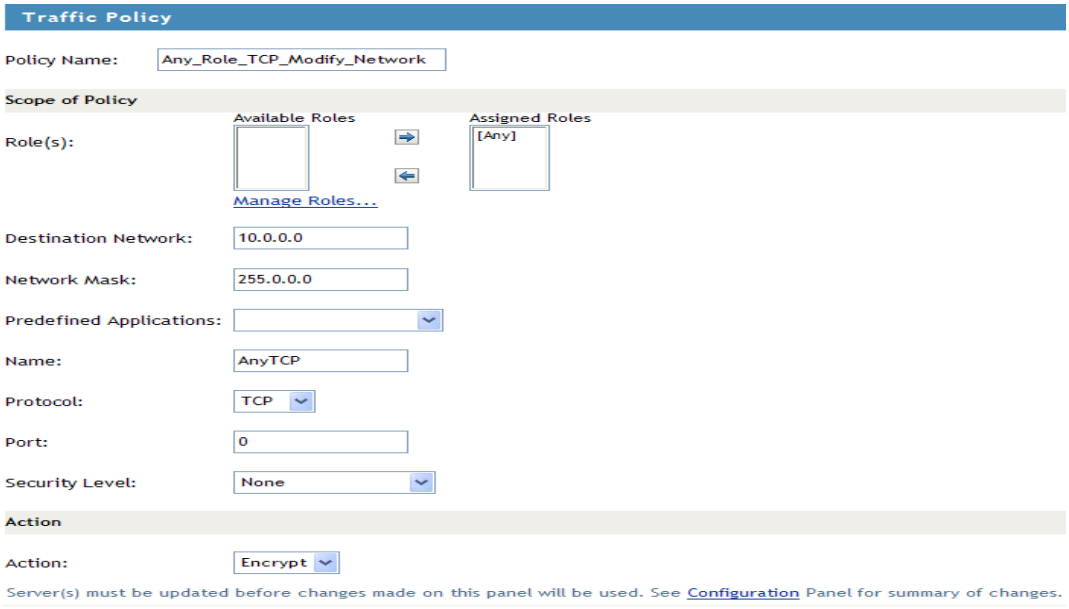
2 Select *Traffic Policies* from the *Policies* section. The SSL VPN Traffic Policies page is displayed.



3 Click *New*. The New dialog box is displayed.

4 Specify the traffic policy name in the *Traffic Policy Name* field, then click *OK*.

5 Click the newly added traffic policy. The Edit Traffic Policy page is displayed.

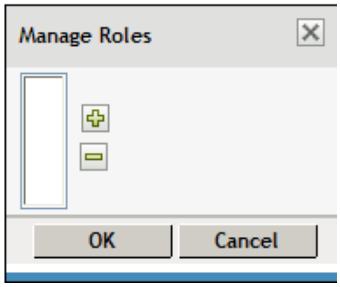


Fill in the following fields:

Policy Name: Displays the name that you have specified for the traffic policy.

Role (s): The role to which the traffic rule applies. If the role is created in the Identity Server, it is displayed in *Available Roles* by default. Select the role you want to assign the traffic policy to and click the forward arrow to send it to *Assigned Roles*. If you want to assign a traffic policy to multiple roles, press the Ctrl key when selecting the roles.

To assign a traffic policy to user-defined roles, click the *Manage Roles* button.



Click the *Add Role* icon to add the roles and click the *Remove selected roles* icon to delete the roles. Click *OK* to confirm your changes, or click *Cancel* to discard the changes.

The role is case-sensitive. If the role configured is `Employee` and the Identity Server sends a request for `employee`, the rule is not pushed to the client. You cannot change the role name after you have configured a traffic rule. If you do so, the changes are not reflected in the associated traffic rule.

Destination Network: Specify the host IP address or the destination IP address.

Network Mask: The network mask is displayed by default when you specify the destination address. However, you can edit the mask.

Predefined Application: Select a predefined application from the drop-down list.

Name: Specify a name for the application. This information is optional.

Protocol: Select a protocol from the drop-down list. You can select the protocol to be TCP, UDP, ICMP, or Any.

Port: Specify the port number on which the service is available. You can also specify a range of port numbers. You can specify a port range separated by a comma or a hyphen. For example 8, 10, 11-15.

NOTE: Specify 0 to allow all ports depending on the protocol.

Action: Specify if a service can be allowed or denied. Select *Encrypt* to allow the service in encrypted form. Select *Deny* if you do not want to allow the service.

Security Level: Specify the minimum level of security to be adhered to by the client machine in order to apply this traffic policy. For more information on how to configure security levels, see Section 14.2, “Configuring Client Security Levels,” on page 95.

6 To delete a traffic rule, select the rule, then click *Delete*.

7 To enable a traffic rule, select the rule, then click *Enable*.

8 To disable a traffic rule, select the rule, then click *Disable*.

9 To save your modifications, click *OK*, then click *Update* on the Configuration page.

14.3.2 Rule Ordering

You can configure multiple rules for a user’s role. However, for a user, traffic policies are applied based on the order of the traffic rules. For example, the policy of the first traffic rule is applied to the user first, followed by the second, and so on. If you want to order the rules based on their priority, you can drag and drop the rules in the order that you want them to be placed.

14.3.3 Exporting and Importing Traffic Policies

You can export the traffic policies that you have created and save them on your local machine as an XML file. This file can be imported when you want to copy the policies into a new setup or into an existing setup, for example, if you want to add to or duplicate the traffic policies. This feature is also useful when you want to reinstall a setup.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Traffic Policies* from the *Policies* section. The SSL VPN Traffic Policies page is displayed.
3. Select the policies that you want to export, then click *Export*.
4. Specify a filename for the XML document that saves the configuration.
5. Specify a location to save the XML file.
6. To import the exported XML file, select the server into which you want to import the traffic policies.
7. Click *Import* in the traffic policies page.
8. Browse and select the XML file that contains the saved traffic policies.
9. To save your modifications, click *OK*, then click *Update* on the Configuration page.

Configuring How Users Connect to SSL VPN

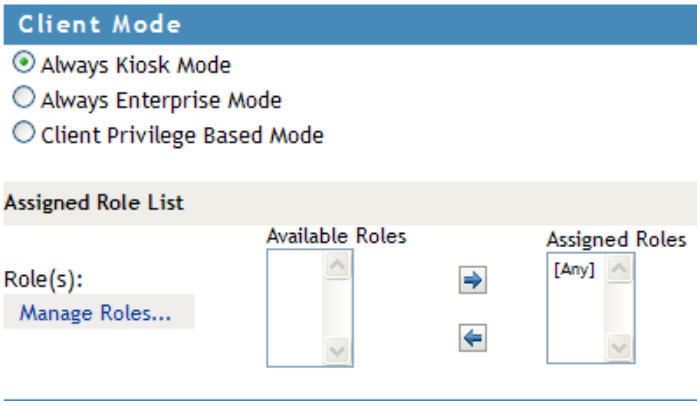
15

You can configure SSL VPN so that a client can be forced to connect in either Kiosk mode only or Enterprise mode only, depending on the role of a client. You can also configure SSL VPN to let the client select the SSL VPN mode based on the client privileges, or you can configure SSL VPN to download the applet client when the Internet Explorer browser is used to establish the SSL VPN connection.

15.1 Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode

You can configure client policies to user roles so that they can connect only in Enterprise mode or only in Kiosk mode.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Client Policies* from the policies section.
3. The Client Policies page is displayed.



Select one of the following options:

Always Kiosk Mode: Select this option to force SSL VPN users to connect in Kiosk mode only, depending on the role of the user.

Always Enterprise Mode: Select this option to force SSL VPN users to connect in Enterprise mode only, depending on the role of the user.

Client Privilege Based Mode: Select this option to allow users to connect in either Enterprise mode or Kiosk mode, depending on their privileges. If you do not select any client modes for roles, the roles are by default configured for the *Client Privilege Based Mode* option.

NOTE: You cannot configure some roles to connect in *Always Kiosk Mode* and other roles to connect in *Always Enterprise Mode.* The two modes are mutually exclusive. However, if you configure some roles for one of these two modes, and do not configure some other roles for any mode, then such role are by default configured for the *Client Privilege Based Mode*.

For example, you cannot configure the Sales role for the *Always Kiosk Mode* and the Finance role for the *Always Enterprise Mode.* However, if you configure the Sales role for either *Always Kiosk Mode* or *Always Enterprise Mode* and do not configure the Finance role for any mode, the Finance role is by default configured for the *Client Privilege Based Mode*.

---

4 To configure the role for which the Client policy should be applicable, specify the following information:

Role (s): The role to which the client policy applies. If the role is created in the Identity Server, it is displayed in *Available Roles* by default.

The role is case-sensitive. If the role configured is `Employee` and the Identity Server sends a request for `employee`, the rule is not pushed to the client.

Manage Roles: To assign a client policy to user-defined roles, click the *Manage Roles* button. Click the *Add Role* icon to add roles or click the *Remove selected role* icon to delete roles. Click *OK* to confirm your changes, or click *Cancel* to discard them.

Available Roles: Select the role for which you want to assign the client policy and click the forward arrow to send it to *Assigned Roles*. If you want to assign a client policy to multiple roles, press the Ctrl key when selecting the roles.

Assign Roles: Lists the roles for which a client policy is assigned.

If some roles are not explicitly configured for a mode, they are assigned to the Client Privileged Mode by default.

5 To save your modifications, click *OK*, then click *Update* on the Configuration page.

15.2 Allowing Users to Select the SSL VPN Mode

To configure the users to connect in either Enterprise mode or Kiosk mode, depending on their privileges, you assign them to the *Client Privilege Based Mode* option.

1 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.

2 Select *Client Policies* from the policies section.

3 The Client Policies page is displayed. Select the *Client Privilege Based Mode* option to allow users to select the SSL VPN connection mode. If the client has admin privileges, it can connect in Enterprise mode; otherwise, it can connect in Kiosk mode.

4 To save your modifications, click *OK*, then click *Update* on the Configuration page.

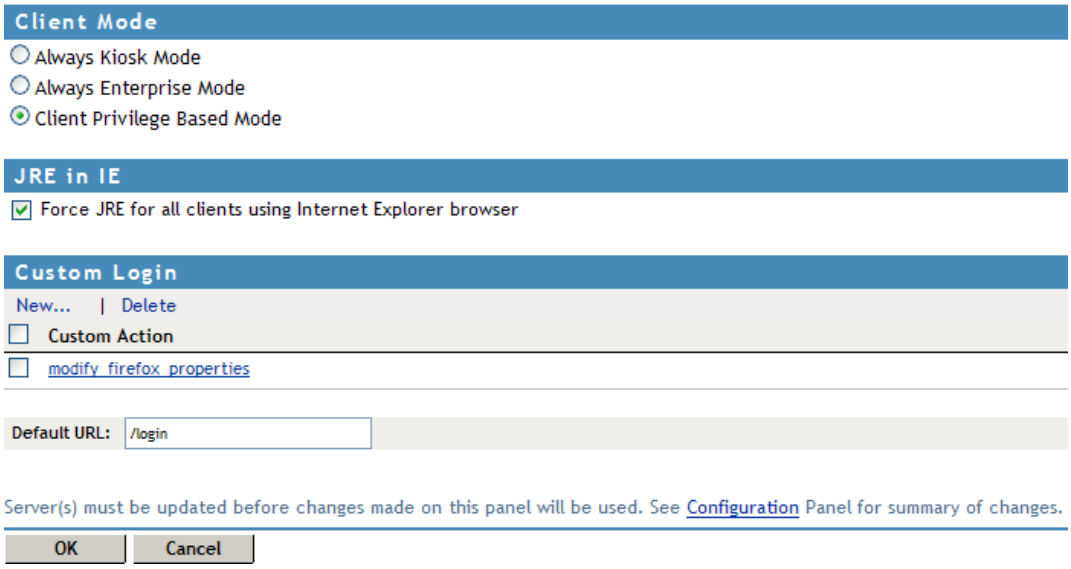
If you do not configure any client modes for roles, then the roles are by default configured for the *Client Privilege Based Mode* option.

15.3 Configuring SSL VPN to Download the Java Applet on Internet Explorer

The SSL VPN client components are downloaded on the client machine through a Java applet or through ActiveX, depending on the browsers they use. The Internet Explorer browser uses the ActiveX control by default to download the SSL VPN client components. However, some Windows clients do not allow ActiveX controls to run in the Internet Explorer.

In such scenarios, the you can force the Windows client to load Java applet instead of ActiveX controls.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Client Policies* from the policies section.



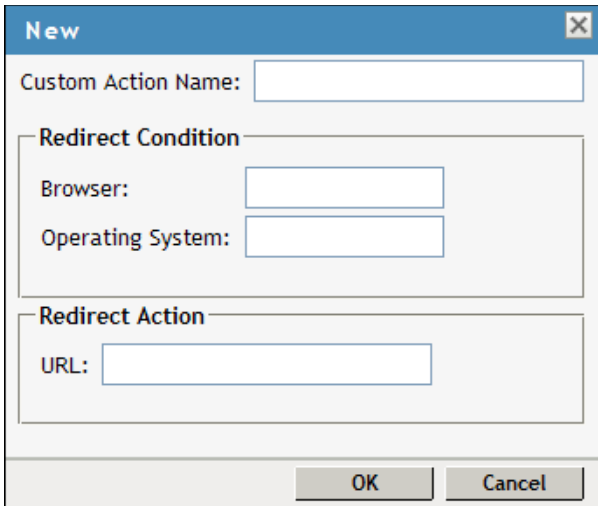
3. Select *Force JRE for all Clients Using Internet Browser*.
4. To save your modifications, click *OK*, then click *Update* on the Configuration page.

15.4 Configuring a Custom Login Policy for SSL VPN

When you configure a custom login policy for SSL VPN, the SSL VPN server redirects the login requests to different URLs based on the policy configured.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Client Policies* from the policies section.
3. Click *New* in the *Custom Login* section.

   The New dialog box is displayed.



4 Specify the following information:

Custom Action Name: Specify a name for the custom login policy.

Redirect Condition: Specify the redirect condition in terms of the browser and the operating system. The conditions configured for the workstation platform and the browser platform are verified against the user agent HTTP header of the browser. For an example of a custom-login policy configured for Citrix clients, see Section 18.3, “Configuring a Custom Login Policy for Citrix Clients,” on page 112.

- The browser can be Firefox, Safari*, Internet Explorer, or any other. You can specify more than one browser, separated by a comma.
- The operating software can be Windows, Linux, Macintosh, or Any. When you configure this attribute to Any, the custom-login policy becomes platform independent.

Redirect URL: Specify the URL to which a user is redirected if the redirection conditions match.

5 Click *OK*.

6 Specify a URL as the default URL. The user is redirected to this URL if none of the conditions are met.

7 To save your modifications, click *OK*, then click *Update* on the Configuration page.

15.5 Customizing SSL VPN User Interface

You can customize the contents of the SSL VPN home page, exit page and the error messages, depending on your organization’s requirements. This section has the following information:

15.5.1 Customizing the Home Page and Exit Page

To customize the home page, modify the `/var/opt/novell/tomcat5/webapps/sslvpn/sslvpnclient.jsp` file.

The home page content is displayed within the tags.

To customize the Exit page, modify the /var/opt/novell/tomcat5/webapps/sslvpn/logout.jsp file.

15.5.2 Customizing Error Messages

To customize the error messages, do the following:

1. Browse and open the following file:

   var/opt/novell/tomcat5/webapps/sslvpn/Applet/properties/BrowserAgentMessages.properties

2. You can do one of the following:
   - Modify the existing error message.
   - Add a new error message
3. Save and close the file.

15.5.3 Modifying Help Pages for the Customized Error Messages

To modify help pages for the customized error messages, do the following:

1. Browse to /var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp/en/sslvpnclienthelp/xml/sslvpnclienthelp.
2. Open sslerror.html in an HTML editor.
3. You can do one of the following:
   - Modify the error messages leaving the error number unchanged. For example:

     You can modify AM.1001: Server is not Responding.

     To AM.1001: Unable to establish connection with the server.

     Here, even though the error message is changed, the error message remains the same.
   - Add new error messages
4. Save and close the file.

Configuring Full Tunneling

16

When you configure SSL VPN for full tunneling, all traffic to the protected network as well as the public network passes through the tunnel, thereby making the SSL VPN connection more secure. Any session management information between the client and the Identity server, Linux Access Gateway -- (for traditional SSL VPN), and the SSL VPN server is exchanged outside the SSL VPN tunnel. You can configure full tunneling for both Kiosk mode as well as Enterprise mode.

Novell® SSL VPN is configured for split tunneling by default. This means that only the traffic that is enabled to go through the protected network, such as items meant for the corporate network, goes through the VPN tunnel. Traffic to public networks does not go through the tunnel. However, if you want all traffic in the client machine to go through the tunnel, you must configure SSL VPN for full tunneling.

You must configure policies for both split tunneling and full tunneling in your organization in order to permit access to specific internal hosts as well as prevent a hacker from controlling the machine via a connection external to the tunnel. The split tunneling policies must be ordered at the top and the full tunneling policy must be placed as the last policy.

To configure a policy for full tunneling:

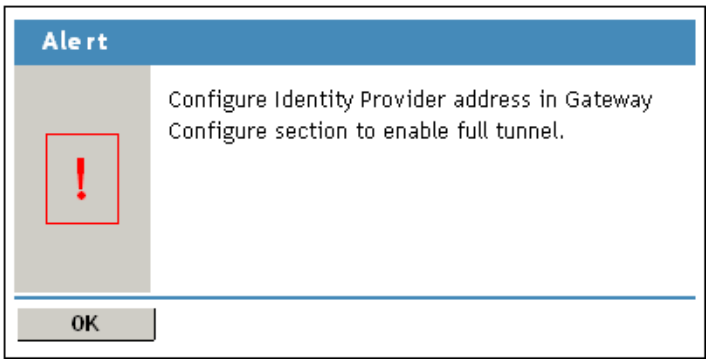
1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Create a new traffic policy. For more information on adding a new traffic policy, see Section 14.3, “Configuring Traffic Policies,” on page 97.
3. Click the newly added traffic policy. The Edit Traffic Policy page is displayed.
4. Configure the following fields:

   Destination Network: Specify 0.0.0.0 as the destination network IP address.

   Network Mask: Specify 0.0.0.0 as the network mask.

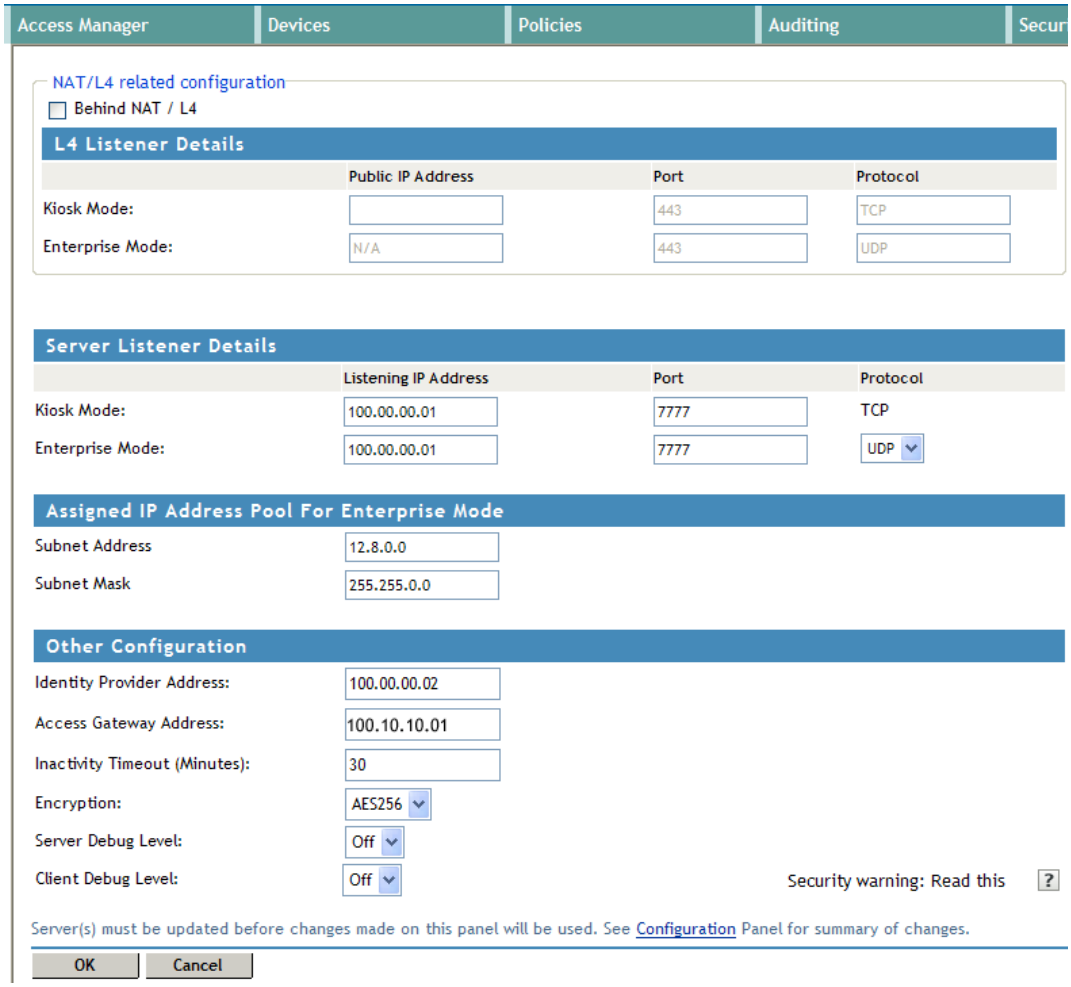
   Action: Select *Encrypt* to allow the service in encrypted form.

   Leave the default values in the other fields unchanged.
5. Click *OK* to save changes. You are prompted to configure the IP address or DNS name of the Identity Server, and the Linux Access Gateway if you have traditional SSL VPN.



6. Click *OK*.
7. Select *Gateway Configuration* from the *Basic Gateway Configuration* section.

The SSL VPN Gateway Basic Configuration page is displayed.



8 Specify the following information in the *Other Configuration* section:

Identity Provider Address: Specify the IP addresses or the DNS name of the Identity Server.

Access Gateway Address: Specify the IP address or DNS name of the Access Gateway if your server is accelerated by the Access Gateway. This field is not present if you have installed the ESP-enabled SSL VPN.

9 To save your modifications, click *OK*, then click *Update* on the Configuration page.

Configuring SSL VPN to Connect through a Forward Proxy

17

The Novell® SSL VPN can be configured to detect and connect through a forward proxy in both Kiosk as well as Enterprise modes after authenticating to the Identity server. To establish the SSL VPN connection through a forward proxy, you can either configure the browser or create a `proxy.conf` file in the user's home directory. You must also ensure that the SSL VPN server is listening on the TCP port and not on the UDP port.

NOTE: The SSL VPN client ignores the use of dynamic proxy configuration either by assigning a `proxy.pac` JavaScript* to the browser client or by using the WPAD protocol. In such a scenario, use the `proxy.conf` file. Fore more information on how to create a `proxy.conf` file, see Section 17.2, "Creating the proxy.conf File," on page 110.

This section has the following information:

17.1 Understanding How SSL VPN Connects Through a Forward Proxy

When a user initiates a connection to SSL VPN server through a browser, SSL VPN uses the following process to connect:

1. SSL VPN checks to see if the browser is configured to use a proxy.
2. If it is, SSL VPN checks for the `proxy.conf` file in the user's home directory.
3. If a proxy configuration file is present, the following occurs:
   a. SSL VPN checks for the format of the file. If the information provided in the file is not in the correct format, SSL VPN proceeds with Step 4.
   b. If the configuration information is in the correct format, SSL VPN reads the proxy information from the `proxy.conf` file, then proceeds with Step 6.
4. If the proxy configuration file is not present or if the information is not in the correct format, SSL VPN checks for proxy configuration information from the browser registry or profile.
5. If SSL VPN is unable to get the proxy configuration information either through the `proxy.conf` file or through the registry, it throws an error asking the user to edit the `proxy.conf` and tries to establish a direct connection.
6. SSL VPN reads the proxy configuration information and attempts to connect to the resource without the proxy. If this attempt fails, the SSL VPN connection is made through the forward proxy.

17.2 Creating the proxy.conf File

1. Create a text file and save it as `proxy.conf` in the following location:
   - `C:\Documents and Settings\<username>` in Windows.
   - `/home/<username>` in Linux.
   - `$home/` in Macintosh.
2. Specify the IP address and the port number of the forward proxy in the following format:

   `proxyHost=<IPaddress>:<port number>`

   For example: `proxyHost=172.10.0.0:8080`
3. (Optional) If the Basic authentication method is used for the forward proxy, SSL VPN can connect in Kiosk mode as well as Enterprise mode. To enable SSL VPN connection when authentication is enabled, specify the username and password of the forward proxy administrator in the following format:

   `proxyAuth=<username>:<password>`

   This is not a recommended method because you need to specify the credentials of the forward proxy in the configuration file and this might be a security vulnerability.
4. Save and close the file.

Configuring SSL VPN for Citrix Clients

18

You can configure a user to enable the single sign-on feature of Novell® Access Manager when accessing published Citrix Applications through SSL VPN. To enable single sign-on, you must configure a custom-login policy and protect the Citrix Application Server with the Access Gateway. If you are using the ESP-enabled Novell SSL VPN, you must install an Access Gateway in order to protect the Citrix server. The following sections discuss the configuration process:

18.1 Prerequisites

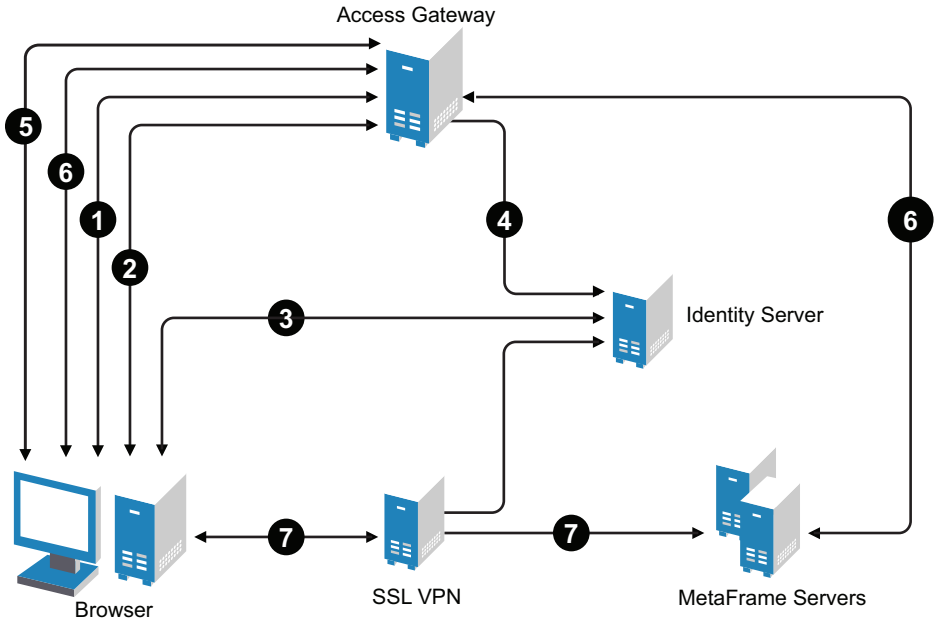
- ❑ NFuse* server
- ❑ MetaFrame* server
- ❑ Identity Server

  The MetaFrame server must be placed in the protected network. The SSL VPN server must use its private network interface adapter to communicate with the network interface of the MetaFrame server.
- ❑ Access Gateway
- ❑ SSL VPN configured to use the same Identity Server as the Access Gateway.
- ❑ Download the `test.js` file from the *Additional Resources* (http://www.novell.com/documentation/novellaccessmanager31/index.html) section on the Novell Documentation site and copy it to a Web server that is protected by the Linux Access Gateway.

18.2 How It Works

Access Manager can be configured to provide single sign-on for Citrix clients. Figure 18-1 illustrates this process for the Citrix Web client.

Figure 18-1 *Citrix Client Configuration*



1. The client specifies the public DNS name of the Access Gateway that accelerates the Web Interface login page of the Citrix MetaFrame Presentation Server.
2. The Access Gateway redirects the user to the Identity Server for authentication, because the URL is configured as a protected resource.
3. The Identity Server authenticates the user's identity.
4. The Identity Server propagates the session information to the Access Gateway through the Embedded Service Provider.
5. The Access Gateway has been configured with a Form Fill policy, which invokes the SSL VPN servlet along with the corresponding policy information for that user. The SSL VPN servlet creates a secure tunnel between the client and the SSL VPN server.
6. On successful SSL VPN connection, the Access Gateway performs a single sign-on to the Citrix MetaFrame Presentation Server. The user is authenticated to both the Citrix Presentation Server and to the SSL VPN server.
7. The Web session containing the list of published applications in the Citrix Presentation server is served to the client through the Access Gateway.
8. When the user connects to the published application, the data goes through the secure tunnel that is formed between the client and the SSL VPN server.

18.3 Configuring a Custom Login Policy for Citrix Clients

A custom-login policy must be configured to enable users to use a browser to access Citrix applications protected by Access Manager.This is because the browser settings of the client need to be modified so that connections to Citrix applications can happen through SSL VPN.

The following procedure configures a sample custom login policy for Citrix where all Linux users connecting from the Firefox browser on Linux are redirected to a page that modifies the browser settings and then redirects the user to the SSL VPN/login URL:

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Client Policies* from the policies section.
3. Click *New* in the *Custom Login* section.
4. Specify the following information in the *New* dialog box.

   Custom Action Name: Specify a name for the custom login policy. For example, modify_firefox_properties

   Redirect Condition:

   - Specify Firefox as the browser.
   - Specify Linux as the Operating Software.

   Redirect URL: Specify the redirect URL as http://<sslvpn-url>/sslvpn/pages/sslvpn-citrix.jar!configure_browser.html
5. Click *OK*.
6. Specify /login as the default URL. The user is redirected to this URL if none of the conditions are met.
7. To save your modifications, click *OK*, then click *Update* on the Configuration page.

18.4 Configuring the Access Gateway to protect the Citrix Server

To enable users to access Citrix applications through SSL VPN, you must first create a protected resource to protect the Citrix login page.

1. In the Administration Console, click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

   The reverse proxy can be set up to require SSL or not.
2. Click *Name of Proxy Service* > *Protected Resources* > *New*.
3. When configuring the protected resource, set up the following:

   - Select a contract that requires authentication. Usually this is a Name/Password contract, but it can be a certificate contract if your NFuse server is configured to use certificates.
   - For the URL Path List, specify the URL to the Citrix login page. This URL should include the filename of this login page.

   For more information, see "Configuring Protected Resources" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
4. On the Server Configuration page, click *OK*, then click *Update*.

18.5 Configuring Single Sign-On Between Citrix and SSL VPN

You need to create a Form Fill policy and assign it to the protected resource for the Citrix login page.

1. In the Administration Console, click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.
2. Click *Form Fill* > *Manage Policies* > *New*.
3. Name the Citrix policy, select *Access Gateway: Form Fill* as the type, then click *OK*.
4. In the *Actions* section, click *New* > *Form Fill*.
5. In the *Form Selection* section, identity the form on the Citrix login page.
6. In the *Fill Options* section, create the following:
   - Username input field
   - Password input field
   - (Optional) If your login page requires a domain, add a domain input field.
7. In the *Submit Options* section, configure the following:
   - Select *Auto Submit*.
   - Select *Enable JavaScript Handling*.
   - Click *Statements to Execute on Post*. Copy the Citrix Script found in the *Additional Resources* (http://www.novell.com/documentation/novellaccessmanager31/index.html) section in the Novell Documentation site.

     In the script:

     Replace <*ag-url*> with the following:

     - For a Traditional SSL VPN, use the hostname of the Access Gateway that is accelerating the SSL VPN server.
     - For an ESP-enabled SSL VPN, use the hostname of the SSL VPN server.

     Change the protocol to HTTPS if the secure protocol is used.

     Replace <*Webserver-path*> with the location of the Web server on which the `test.js` javaScript file is located. When this JavaScript file is used, it connects users from the outside through SSL VPN.

     Change the URL as follows, if you want to use the custom login method:

     http://<ag-url>/sslvpn/custom-login
8. Configure any other options to match your form and your network.

   For more information, see "Creating Form Fill Policies" in the *Novell Access Manager 3.1 SP1 Policy Management Guide*
9. In the *Actions* section, click *New* > *Form Login Failure*.

   Specify the procedures you want followed when login fails. For more information, see "Creating a Login Failure Policy" in the *Novell Access Manager 3.1 SP1 Policy Management Guide*

   Citrix displays login failures via the query string, so you'll need to use CGI matching.
10. Click *OK*, then click *Apply Changes*.
11. Click *Close*.

You should return to the Form Fill page for the protected resource.

12 Select the policy you just created, then click *Enable*.

13 Click *Configuration Panel*, then click *OK*.

14 On the Server Configuration page, click *OK*, then click *Update*.

Additional Configurations

19

You can also modify the SSL VPN server details, including moving the SSL VPN server to a different Administration Console, and configuring full tunneling.

19.1 Creating DH Certificates with Different Key Sizes

The Enterprise mode of SSL VPN uses DH certificates for encryption. These certificates are created automatically during the installation or upgrade, with a default key size of 1024. You can create DH certificates with key sizes of your choice up to a maximum key size of 4096.

To create a DH certificate with a key size of your choice, enter the following command:

```
sslvpnc -k <keysize>
```

Replace <*keysize*> with the key size of your choice.

19.2 Creating a Configuration File to Add Additional Configuration Changes

SSL VPN has many extended configuration options for both the SSL VPN Enterprise client and Enterprise server that can be saved and executed from a configuration file.

1. Browse to `/etc/opt/novell/sslvpn`.
2. Open the following files, depending on the changes you want to make:
   - Open `openvpn-client.conf` if you want to push configuration changes to the Enterprise mode client.
   - Open `openvpn-server.conf.tmpl` if you want to push configuration changes to the Enterprise server.
3. Add the commands for additional OpenVPN configuration to these files. For example, to decrease the MTU size of the TUN interface, specify the command in the following format in both files:

   ```
   link-mtu 1200
   ```
4. Save your changes.
5. Restart the server.

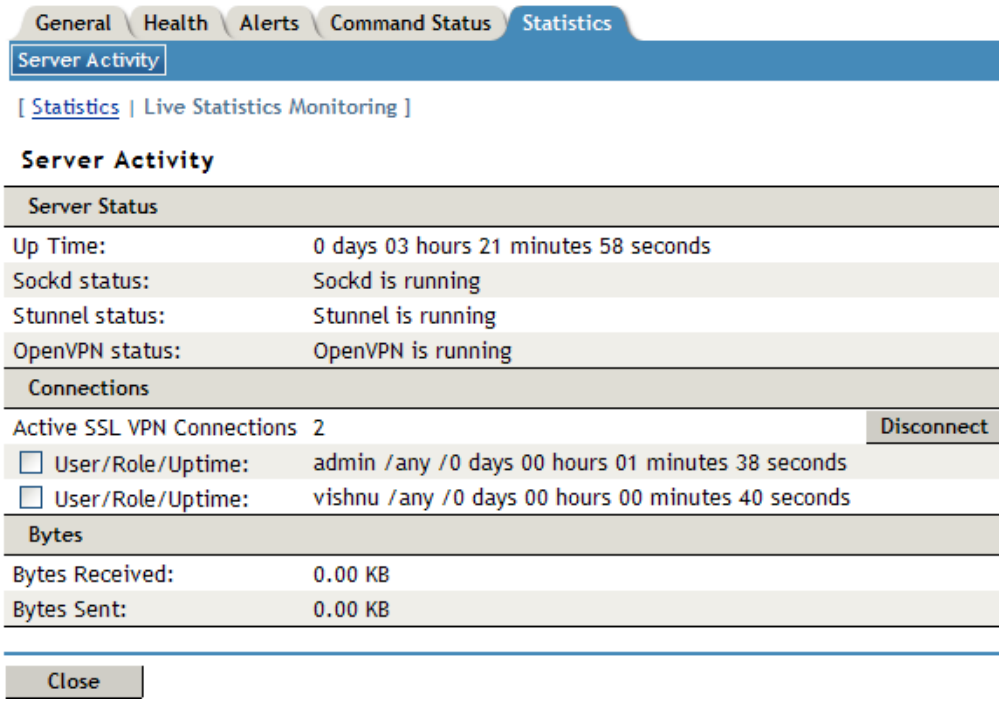
19.3 Disconnecting Active SSL VPN Connections

You can use the Administration Console to disconnect users who are connected to SSL VPN. You can either disconnect one user at a time or select and delete multiple users.

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Statistics*.

The Server Statistics page is displayed.

2 Click *Live Statistics Monitoring*. The Live Statistics Monitoring page is displayed.



3 Select the users that you want to disconnect, then click *Disconnect*.

4 Click *OK* to confirm your action.

19.4 Modifying SSL VPN Server Details

To edit the Gateway information:

1 In the Administration Console, click *Devices* > *SSL VPNs*.

2 Check the information that is displayed and make any necessary changes.

New Cluster: Displays the New Cluster dialog box. You can specify a name for your SSL VPN configuration and assign an Identity Server. When you click *OK*, the system displays the Create Cluster Configuration page, which lets you configure how your Identity Servers operate in an Access Manager configuration. For more information on clustering SSL VPN servers, see Chapter 21, "Creating a Cluster of SSL VPN Servers," on page 125.

Stop: To stop the SSL VPN server so that the power can be turned off, select the SSL VPN server, then click *Stop*.

Start: To start the SSL VPN server, select the SSL VPN server, then click *start*.

Refresh: Click this option to update the list of servers and their health status.

Actions: To delete an SSL VPN server, restart the embedded service provider, or modify cluster membership, select an SSL VPN server, then click *Actions*.

Name: Displays a list of servers added to the Administration Console. Click the particular server to view or modify its configuration. For more information, see Section 19.4, "Modifying SSL VPN Server Details," on page 118.

Status: Indicates the configuration status of the SSL VPN server. Possible states are pending, update, and current. Current indicates that all configuration changes have been applied. Update indicates that a configuration change has been made, but not applied. Click the *Update* link to apply the changes. Depending upon what has been modified, updating the complete configuration might cause logged-in users to lose data and lose their connections. Pending indicates that the server is processing a configuration change, but has not completed the process.

Health: Indicates whether the server is functional. Click the icon to view additional information about the operational status of the server. For more information, see Chapter 27, "Monitoring Health of SSL VPN Servers," on page 147.

Alerts: Indicates if any alert was sent. This option is not available to you if the alert count is 0. For more information, see Section 29.2, "Viewing SSL VPN Alerts," on page 152.

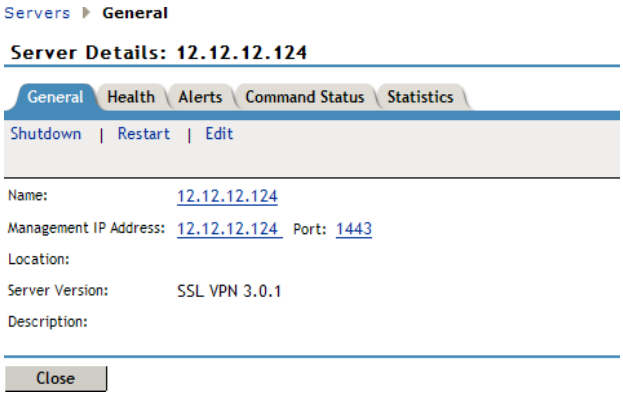
Commands: Indicates the status of commands issued to all servers. For more information, see Chapter 28, "Viewing the Command Status of the SSL VPN Server," on page 149.

Statistics: Indicates the number of active client connections and the time when the server was started. Click *View* to get the statistics information. For more information, see Chapter 26, "Viewing SSL VPN Statistics," on page 143.

Type: Indicates whether the type of SSL VPN that is installed is high bandwidth or low bandwidth.

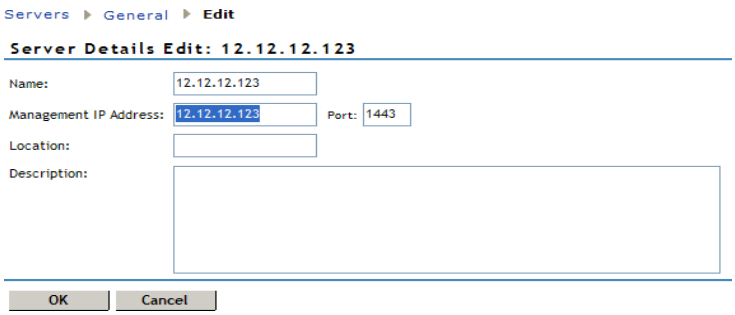
Configuration: Click *Edit* in the *Configuration* column of the SSL VPNs page to view and modify the configuration of the SSL VPN server. This page specifies the date and time when the last modification was made and lists the full distinguished name of the user who made the last modification. For more information, see Part III, "Configuring SSL VPN," on page 65.

3 Click the server. The Server Details page is displayed.



The *General* tab of the Server Details page displays information such as name, Management IP address, Port, Location, and the server version of the selected server.

4 Click *Edit*. The Server Details Edit page is displayed.



5 Check the information and make any necessary changes.

Name: Specify the IP address of the server. This field is mandatory.

Management IP Address: Specify the IP address used to manage the server. If the system on which the agent is installed has multiple IP addresses, you can select one from the drop-down list.

Port: Specify the port used for management. This field is mandatory.

Description: (Optional) Provide a brief description of the purpose of this SSL VPN Gateway or any other relevant information.

6 Click *OK* to save changes or click *Cancel* to discard the changes.

Clustering the High Bandwidth SSL VPN Servers

IV

The high bandwidth SSL VPN servers can now be clustered to provide load balancing and fault tolerance capabilities and act as a single server. Clients access the virtual IP address of the cluster presented on the L4 switch, and the L4 switch alleviates server load by balancing traffic across the cluster. Whenever a user accesses the virtual IP address (port 8080) assigned to the L4, the system routes the user to one of the SSL VPN servers in the cluster, as traffic necessitates.

Clustering enables the following features:

- Cluster configuration is synchronized to all members of the cluster.
- Each cluster member can handle sessions held by another server in the cluster. After a session is established, the same member usually handles all requests for that session. However, if that cluster member is not available to handle a request, another member processes the request.
- Load balancing among the cluster members.
- Transparent failover.

This section has the following information:

Overview of SSL VPN Clusters 20

SSL VPN systems can be set up in clusters. You can use clusters to create fault tolerance in an SSL VPN system.

20.1 Cluster Overview

The SSL VPN servers in a cluster share a common configuration and are managed on a single administration console. The servers are configured to balance load and failover. When a member of the SSL VPN cluster fails, the user sessions are transparently failed over to another SSL VPN server that is healthy. An SSL VPN tunnel is affected if the server that is serving the SSL VPN tunnel goes down. A cluster can be set up to function with an L4 server or the Access Gateway to handle load balancing. A cluster can be set up to function with an L4 server or by using the Access Gateway. You can have a cluster of servers in both HTTP and HTTPS.

Using L4 for Clustering: In this approach, the SSL VPN cluster is placed behind an L4 server. If the tunnel IP address configured in the administration console is the virtual IP address of an L4, an additional load balancing is done at this level. When a user is authenticated, all the members of the cluster are informed, so that the cluster members can handle failover. For more information on configuring the L4 server, see “Configuration Tips for the L4 Switch ” in the *Novell Access Manager 3.1 SP1 Setup Guide*.

Using Access Gateway for Clustering: In a direct connection, the client directly establishes contact with the tunneling component, which could be a NAT IP address and not through the L4 switch. This approach ensures that the load balancing of SSL VPN servers is achieved with the help of Access Gateway clusters. The client establishes connection with the first tunnel. For more information, see Chapter 23, “Clustering SSL VPNs By Using Access Gateway and Without L4,” on page 133.

20.2 Prerequisites

- ❑ An L4 server is installed. The LB algorithm can be anything (hash/sticky bit), defined at the Real server level.
- ❑ Persistence (sticky) sessions are enabled on the L4 server. You usually define this at the virtual server level.
- ❑ SSL VPN servers are installed and imported into the same administration console. The health status of all the imported servers must be green or yellow.
- ❑ The traffic policies must be imported into the SSL VPN servers before they are clustered.
- ❑ An SSL VPN Server configuration is created for the cluster, and all the SSL VPN servers are assigned to this configuration.

  The base URL DNS name of this configuration must be the virtual IP address of the L4 server. The L4 balances the load between the SSL VPN servers in the cluster.

- The following ports are open on the L4 server for SSL VPN communication:
  - 8080 (for HTTP communication)
  - 8443 (for HTTPS communication)
  - 7777 (for Stunnel over TCP and OpenVPN over UDP)
  - 7778 (for OpenVPN over TCP)

20.3 Limitations

You have the following limitations when you are clustering the SSL VPN servers:

- All SSL VPN servers must be running the high bandwidth version of SSL VPN.
- All members of an SSL VPN cluster should belong to only one type. For example, all the members of a cluster should be either an ESP-enabled Novell SSL VPN or a Traditional Novell SSL VPN. You cannot have a cluster where some members are ESP-enabled Novell SSL VPNs and some are Traditional Novell SSL VPNs.
- In the HTTPS mode, you cannot have a cluster of SSL VPNs where some servers are installed on a separate machine and some servers are installed along with the Identity Server.

Creating a Cluster of SSL VPN Servers

21

The system automatically enables clustering when multiple SSL VPN servers exist in a group. To create an SSL VPN cluster, you must create a cluster of SSL VPNs after you install an SSL VPN server, then assign one or more SSL VPN servers to that cluster.The Access Manager software configuration process is the same whether there is one server or multiple servers in a cluster.

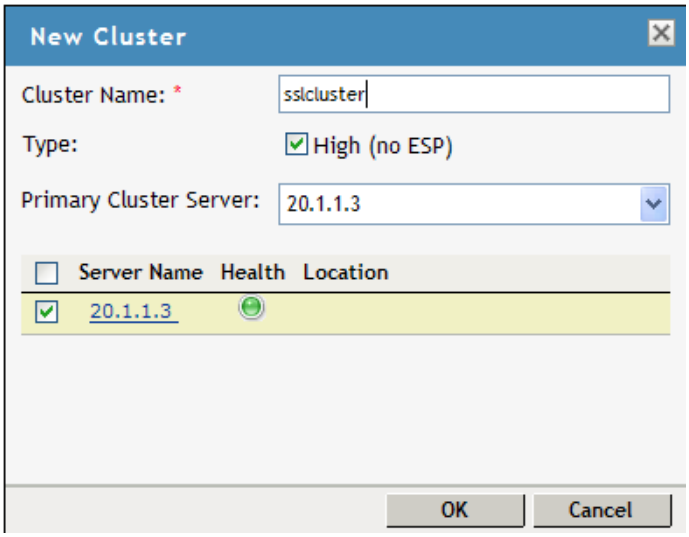
This section describes how to set up and manage a cluster of SSL VPN servers:

21.1 Creating a Cluster of SSL VPN Servers

To create a new SSL VPN server cluster, you start by creating a cluster configuration with a primary server.

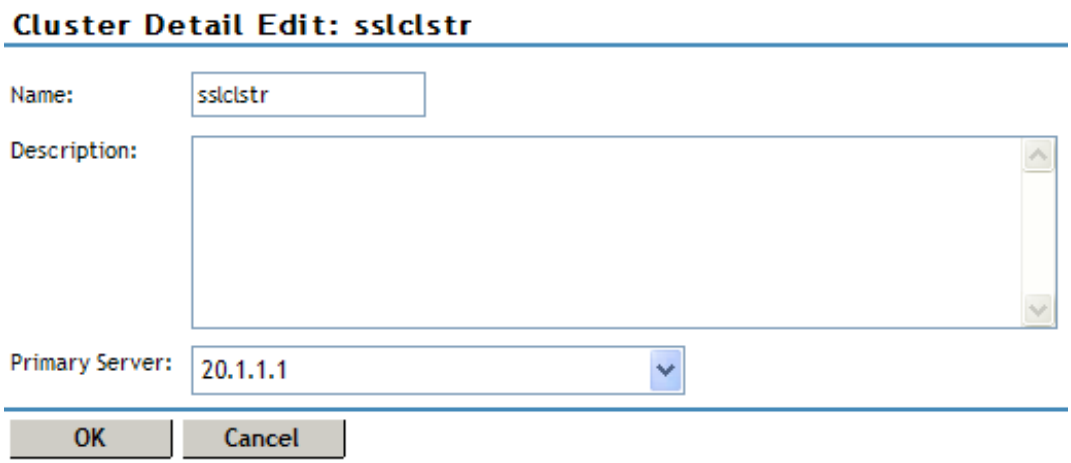
1. In the Administration Console, click *Devices* > *SSL VPNs* > *Servers*.
2. Select the SSL VPN server that you want to add to the cluster, then click *New Cluster*.

   The *New Cluster* dialog box appears.



3. Specify a name for the cluster configuration. If you selected the server in the previous step, the IP address of the server is displayed in the *Primary Server* drop-down list. If you have not selected a server in the previous step, you can now select the server or servers that you want to assign to this configuration.
4. Click *OK*.
5. Click the cluster configuration name that you created.

6 On the Cluster Details page, click *Edit*.



7 Fill in the following fields as required:

Name: Specifies the name of the SSL VPN server cluster configuration. You can modify the name of the cluster if you want.

Description: Specify a brief description of the SSL VPN cluster.

Primary Server: Specify the IP address of the primary server in the SSL VPN server cluster.

The *Cluster Members* section displays the IP address and other details of the SSL VPN servers that are assigned to the cluster.

8 Click *OK*.

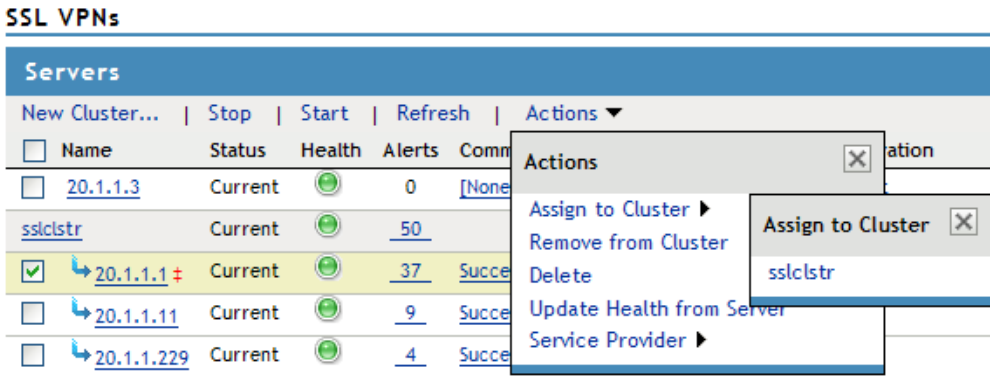
The status icons for the configuration and the SSL VPN Server should turn green. It might take several seconds for the SSL VPN server to start and for the system to display a green light.

21.2 Adding An SSL VPN Server to a Cluster

After you create a cluster and identify the primary member, you can add other SSL VPN servers to the cluster. You can add more than one SSL VPN server to the SSL VPN cluster.

1 In the Administration Console, click *Devices* > *SSL VPNs*.

2 On the Servers page, select the server, then click *Actions* > *Assign to Cluster*.



To select all the servers in the list, select the top-level Server check box.

3 Select the name of the cluster that you want to add the SSL VPN server to.

The health status of the SSL VPN server turns green, if the server is already configured and the trust relationship is established with the Identity Servers. Otherwise, the health status is displayed as yellow. It might take several seconds for the SSL VPN server to start and for the system to display the health icon.

21.3 Removing an SSL VPN Server from a Cluster

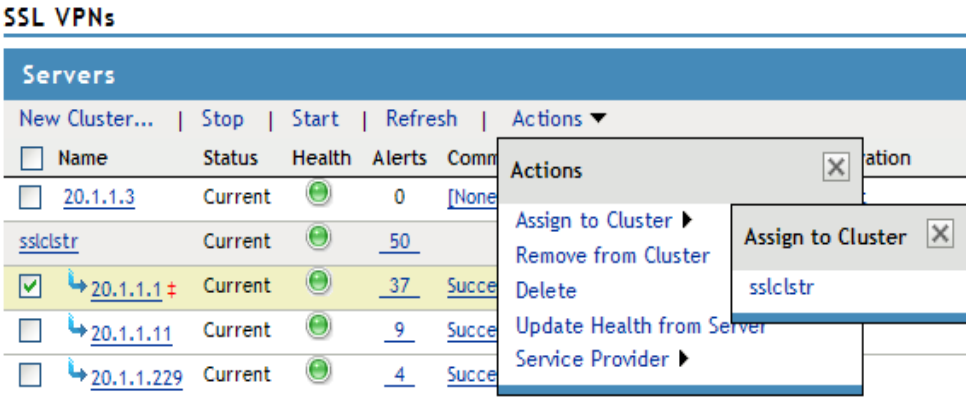
Removing an SSL VPN server from a cluster disassociates the SSL VPN server from the cluster configuration. You can either remove servers individually or remove all the clusters at the same time.

When you remove a server from a cluster, all of the configuration except the trust relationship remains unchanged and can be reassigned later or assigned to another server. The trust relationship established with the Identity Server is lost when a server is removed from the cluster.

1 In the Administration Console, click *Devices* > *SSL VPNs*.

2 Select the server, then click *Stop*. Wait for the *Health* tab to show a red icon, indicating that the server has stopped.

3 Select the server, then choose *Actions* > *Remove from Cluster*.



4 Click *OK*.

Clustering SSL VPN by Using L4

22

You configure the SSL VPN cluster to be behind a Layer 4 (L4) server because it is essential in order to assign multiple SSL VPN servers to the same configuration. You can use the same L4 server for SSL VPN server clustering, Identity Server clustering, and Access Gateway clustering, provided that you use different virtual IPs.

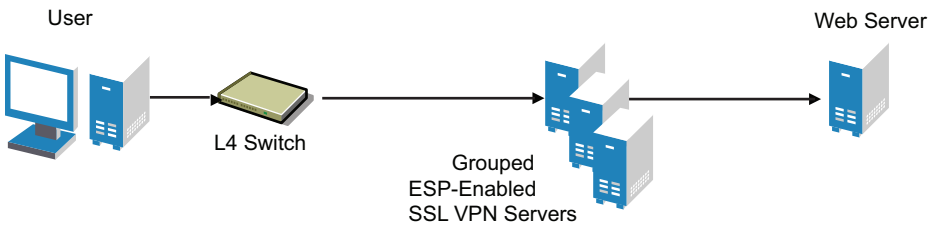
You can either have a cluster of traditional SSL VPN servers by using L4 and Access Gateways or you can have a cluster of ESP-enabled SSL VPNs by using the L4 server. In a cluster, policies such as the client integrity check policies, traffic policies, and client policies are common to all the cluster members. However, each of the secondary members of the cluster must have specific listening IP addresses for Kiosk mode and Enterprise modes and a specific subnet mask and subnet addresses configured for Enterprise mode.

Make sure that the base URL of SSL VPN is resolvable with its own IP address as well as the public IP address of L4 server. The Identity Server should be able to resolve the base URL of SSL VPN to the virtual IP address of SSL VPN cluster.

22.1 Configuring a Cluster of ESP-Enabled SSL VPNs

When you configure a cluster of SSL VPNs behind an L4, the client contacts the VIP of the L4 servers.

Figure 22-1 *Cluster of SSL VPNs behind L4*



To configure a cluster of ESP-enabled SSL VPNs behind an L4:

1. Install the ESP-enabled SSL VPN servers and import them into the same administration console.

   For more information on installing ESP-enabled SSL VPNs, see Section 4.3, “Installing ESP-Enabled SSL VPN,” on page 30.

2. Verify that the health of all the imported SSL VPNs is displayed as green or yellow.

For more information on verifying the health, see Section 4.7, “Verifying That Your SSL VPN Service Is Installed,” on page 42.

3 Configure the L4, gateway details, and Audit event in the SSL VPN server.

For more information on configuring the L4 and gateway details, see Chapter 11, “Configuring the IP Address, Port, and NAT,” on page 75. For more information on configuring the Audit events, see Chapter 25, “Enabling SSL VPN Audit Events,” on page 141.

4 Import the traffic policies into the server. For more information on importing the traffic policies, see Section 14.3.3, “Exporting and Importing Traffic Policies,” on page 100

5 Create a cluster of SSL VPNs.

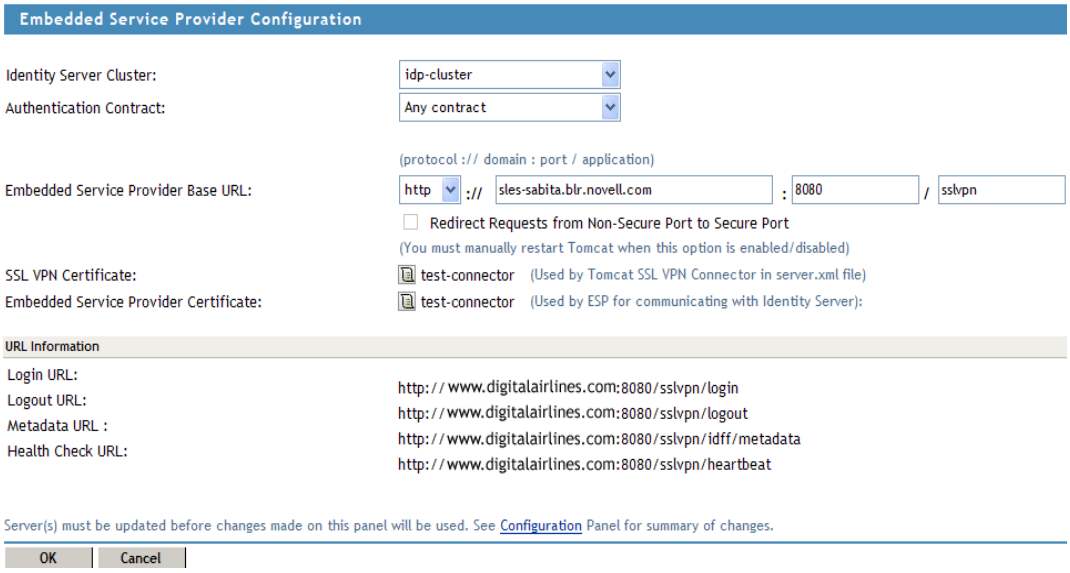
For more information on creating a cluster, see Section 21.1, “Creating a Cluster of SSL VPN Servers,” on page 125.

6 Assign all SSL VPN servers to the cluster.

For more information, see Section 21.2, “Adding An SSL VPN Server to a Cluster,” on page 126. The configuration details specific to a cluster, such as the client integrity check policies, traffic policies, and client policies are propagated to all the cluster members.

7 In the Administration Console, click *Devices* > *SSL VPNs* > *Edit,* then select the Gateway configuration page. Configure specific listening IP addresses for Kiosk mode and Enterprise modes and specific subnet mask and subnet addresses for Enterprise mode.

8 Select the Authentication Configuration link and configure the Embedded Service Provider



9 In the Embedded Service Provider Base URL, if you select HTTPS as the protocol, create and use a custom certificate.

10 Restart the Tomcat server when prompted.

11 To save your modifications, click *OK,* then click *Update* on the Configuration page.

22.2 Configuring a Cluster of Traditional SSL VPNs by Using L4

To configure a cluster of traditional SSL VPNs

1. Install the traditional SSL VPN servers and import them into the same administration console.

   For more information on installing ESP-enabled SSL VPNs, see Section 4.3, “Installing ESP-Enabled SSL VPN,” on page 30.

2. Verify that the health of all the imported SSL VPNs is displayed as green or yellow.

   For more information on verifying the health, seeSection 4.7, “Verifying That Your SSL VPN Service Is Installed,” on page 42.

3. Configure the L4, gateway details, and Audit event in the SSL VPN server that you want to mark as primary.

   For more information on configuring the L4 and gateway details, see Chapter 11, “Configuring the IP Address, Port, and NAT,” on page 75. For more information on configuring the Audit events, see Chapter 25, “Enabling SSL VPN Audit Events,” on page 141.

4. Import the traffic policies into the server. For more information on importing the traffic policies, see Section 14.3.3, “Exporting and Importing Traffic Policies,” on page 100

5. Create a cluster of SSL VPNs.

   For more information on creating a cluster, see Section 21.1, “Creating a Cluster of SSL VPN Servers,” on page 125.

6. Assign all SSL VPN servers to the cluster.

   For more information, see Section 21.2, “Adding An SSL VPN Server to a Cluster,” on page 126.

7. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit,* then select the Gateway configuration page. Configure the IP address, subnet mask and subnet address for each of the cluster members.

8. Accelerate the SSL VPN server by using the Access Gateway.

   For more information, see Chapter 10, “Accelerating the Traditional Novell SSL VPN,” on page 69.

9. To save your modifications, click *OK,* then click *Update* on the Configuration page.

Clustering SSL VPNs By Using Access Gateway and Without L4

23

You can install and run the SSL VPN self-monitoring and failover scripts on each SSL VPN server in order to provide automatic monitoring and failover support for the SSL VPN servers that are behind a Linux Access Gateway.

When the health status of an SSL VPN server is bad, these scripts modify the IPTables entries on that server to stop the Access Gateway from sending connection requests to that particular SSL VPN server. When the SSL VPN server health status returns to normal, the scripts remove the iptables entries and allow the Access Gateway to communicate with the SSL VPN server. You must perform the following tasks to configure load balancing and fault tolerance through the Access Gateway:

1. Configuring the Access Gateway.
2. Installing the Scripts
3. Testing the Scripts

23.1 Configuring the Access Gateway

1 In the Administration Console, click *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.

2 Add all the SSL VPN servers that are part of the failover group as origin Web servers to the proxy service that you have defined.

3 Click *TCP Connect Options*.

4 Select *Round Robin* in the *Policy for Multiple Destination IP Addresses* field.

5 Select *Enable Persistent Connections*.

6 Save your changes and update the Access Gateway.

23.2 Installing the Scripts

1 Download the tar file containing scripts for SSL VPN automatic monitoring and failover from the Additional Resources section on the Novell Access Manager documentation page (http://www.novell.com/documentation/novellaccessmanager/index.html). The tar file contains `sslvpn-heartbeat.sh` and `sslvpn-heartbeat`.

2 Copy the `sslvpn-heartbeat.sh` script to the `/opt/novell/sslvpn/bin` directory in each of the SSL VPN servers.

3 Copy the `sslvpn-heartbeat` file to the `/etc/init.d/`directory.

4 Enter the following commands to change `sslvpn-heartbeat.sh` and `sslvpn-heartbeat` into executable files:

```
chmod +x sslvpn-heartbeat.sh
```

```
chmod +x sslvpn-heartbeat
```

5 Enter the following command to run the script every time the Access Gateway is started:

```
insserv /etc/init.d/sslvpn-heartbeat
```

23.3 Testing the Scripts

1. Enter the following command to stop the SSL VPN server:

   ```
   /etc/init.d/novell-sslvpn stop
   ```

2. Enter the following command to verify if the scripts have blocked port 8080:

   ```
   iptables -L
   ```

   The following lines are displayed if port 8080 is blocked:

   ```
   Chain    sslvpn-heartbeat-chain (1 reference)
   target    prot opt source      destination
   REJECT    tcp  --  anywhere      anywhere    tcp
   dpt:http-alt reject-with icmp-port-unreachable
   ```

3. In the Administration Console, click *Access Gateways* > *[Name of Server]* > *Health*. The following message is displayed if the SSL VPN server is down:

   ```
   The HTTP Reverse Proxy service <reverse proxy name> might not be
   functioning properly. Few of the Web servers being accelerated are
   unreachable <sslvpn server IP Address>:8080
   ```

   Click *Update from Server* to get the latest health status of the Access Gateway.

4. Connect to SSL VPN. Verify that your connection was sent to the SSL VPN that is running and not to the one that is marked as down by the Access Gateway.

5. Enter the following command to start the SSL VPN server:

   ```
   /etc/init.d/novell-sslvpn start
   ```

6. Enter the following command to verify if the script has removed the block on port 8080:

   ```
   iptables -L
   ```

   The following lines are displayed if the block on port 8080 is removed:

   ```
   Chain sslvpn-heartbeat-chain (1 references)
   target    prot opt source      destination
   ```

7. In the Administration Console, click *Access Gateways* > *[Name of Server]* > *Health*, then check that the SSL VPN server is up.

   Click *Update from Server* to get the latest health status of the Access Gateway.

8. Connect to SSL VPN. Verify if your connection was sent to the SSL VPN server that was restarted. It might require several attempts before you can connect to the desired Access Gateway.

9. Repeat Step 1 to Step 8 to verify if the SSL VPN health scripts are working on all the SSL VPN servers.

Configuring SSL VPN to Monitor Health of Cluster

24

The L4 servers use health checks to determine which cluster members are ready to receive requests and which cluster members are unhealthy and should not receive requests. You need to configure the L4 server to monitor the heartbeat URL of the Identity Servers and Access Gateways, so that the L4 server can use this information to accurately update the health status of each cluster member.

24.1 Services of the Real Server

A user’s authentication resides on the real (authentication) server cluster member that originally handled the user’s authentication. If this server malfunctions, all users whose authentication data resides on this cluster member must reauthenticate.

Requests that require user authentication information are processed on this server. When the system identifies a server as not being the real server, the HTTP request is forwarded to the appropriate cluster member, which processes the request and returns it to the requesting server.

24.1.1 A Note about Alteon Switches

When configuring an Alteon* switch for clustering, direct communication between real servers must be enabled. If direct access mode is not enabled and one of the real servers tries to proxy another real server, the connection fails and times out.

To enable direct communication on an Alteon switch:

1. Go to cfg > slb > adv > direct.
2. Specify *e* to enable direct access mode.

With some L4 switches, you should configure only the services that you are using. For example, if you configure the SSL service for the L4 and you have not configured SSL in Access Manager, then the HTTP service on the L4 does not work. If the health check for the SSL service fails, the L4 assumes that all the services configured to use the same virtual IP are down.

24.1.2 Real Server Settings Example

```
Current real server group 1:
  name , metric hash, backup none, realthr 0
  health script1, content
  DSR VIP health: enabled
  Operation: enabled
  adv health:
  real servers:
    1: 172.16.1.84, enabled, name , weight 1, timeout 10 mins, maxcon 200000
       group ena, backup none, inter 2, retry 4, restr 8, operator enabled
       remote disabled, proxy enabled, submac disabled
       cookie assignment server: disabled
       exclusionary string matching: disabled
    2: 172.16.1.85, enabled, name , weight 1, timeout 10 mins, maxcon 200000
       group ena, backup none, inter 2, retry 4, restr 8, operator enabled
       remote disabled, proxy enabled, submac disabled
       cookie assignment server: disabled
       exclusionary string matching: disabled
  real ports:
    7777: vport 7777, pbind clientip
      virtual server:  1, 10.4.0.172,      enabled
    7778: vport 7778, pbind clientip
      virtual server:  1, 10.4.0.172,      enabled
    8080: vport 8080, pbind clientip
      virtual server:  1, 10.4.0.172,      enabled
    8443: vport 8443, pbind clientip
      virtual server:  1, 10.4.0.172,      enabled
```

24.1.3 Virtual Server Settings Example

```
Current virtual server 1:
  10.4.0.172, enabled, cont 1024
    virtual ports:
      7777: rport 7777, group 1, pbind clientip, frags, cont 1024
          real servers:
             1: 172.16.1.84,     weight 1,  enabled, backup none, group ena
             2: 172.16.1.85,     weight 1,  enabled, backup none, group ena
      7778: rport 7778, group 1, pbind clientip, frags, cont 1024
          real servers:
             1: 172.16.1.84,     weight 1,  enabled, backup none, group ena
             2: 172.16.1.85,     weight 1,  enabled, backup none, group ena
      8080: rport 8080, group 1, pbind clientip, frags, cont 1024
          real servers:
             1: 172.16.1.84,     weight 1,  enabled, backup none, group ena
             2: 172.16.1.85,     weight 1,  enabled, backup none, group ena
      8443: rport 8443, group 1, pbind clientip, frags, cont 1024
          real servers:
             1: 172.16.1.84,     weight 1,  enabled, backup none, group ena
             2: 172.16.1.85,     weight 1,  enabled, backup none, group ena
```

24.2 Monitoring the SSL VPN Server Health

The health status of the SSL VPN server can be monitored by using the heartbeat URL. The heartbeat URL uses the DNS name of the SSL VPN server as follows:

```
https://<SSLVPN DNS NAME>/sslvpn/heartbeat
```

L4 switches require you to use the IP address rather than the DNS name. If the IP address of the SSL VPN Server is 10.10.16.50, and you have configured it for HTTPS, the heartbeat URL is:

```
https://10.10.16.50:8443/sslvpn/heartbeat
```

You must configure the L4 switch to use this heartbeat to perform a health check. If you have configured SSL on the SSL VPN servers and your L4 switch has the ability to do an SSL L7 health check, you can use HTTPS. The SSL L7 health check returns a value of `200 OK`, indicating everything is healthy. Any other status code indicates an unhealthy state.

For a Foundry* switch, the L7 health check script string should look similar to the following when the hostname is sslvpn1 and the IP address is 10.10.16.50:

```
healthck sslvpn1ssl tcp
  dest-ip 10.10.16.50
  port ssl
  protocol ssl
  protocol ssl url "GET /sslvpn/heartbeat HTTP/1.1\r\nHost: st160.lab.tst"
  protocol ssl status-code 200 200
  l7-check
```

If your switch does not support an SSL L7 health check, the HTTPS URL returns an error, usually a 404 error. The SSL VPN Server heartbeat URL listens on both HTTPS and HTTP, you can use an HTTP URL for switches that do not support the SSL L7 health check. For example:

```
http://10.10.16.50:8080/sslvpn/heartbeat
```

An Alteon switch does not support the L7 health check, so the string for the health check should look similar to the following:

```
open 8080,tcp
send GET /sslvpn/heartbeat HTTP/1.1\r\nHOST:heartbeat.lab.tst \r\n\r\n
expect HTTP/1.1 200
close
```

Monitoring the SSL VPN Servers

V

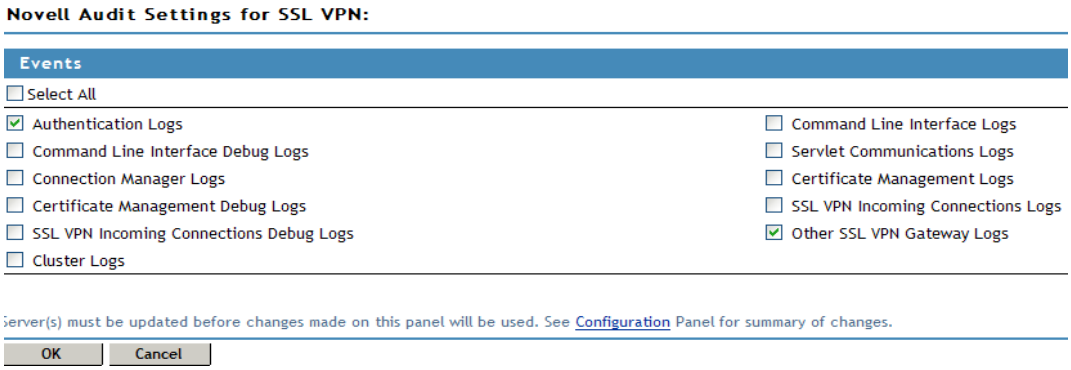
This section describes the various ways you can determine whether the SSL VPN server is functioning normally and whether an Internet attack is in progress.

Enabling SSL VPN Audit Events

25

The *Novell Audit Settings* option allows you to configure the events you want audited. The following steps assume that you have already set up Novell® Audit on your network. For more information, see "Configuring Access Manager for Novell Auditing" in the *Novell Access Manager 3.1 SP1 Administration Console Guide*.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Novell Audit Settings* from the *Novell Audit and Alerts* section. The Novell Audit Settings for SSL VPN page is displayed.



3. Select the *Select All* option to receive logs for all the events, or select one or more of the following:

Event	Description
Authentication Logs	Generates a log file containing the authentication details.
Command Line Interface Logs	Generates a log file containing command line actions.
Command Line Interface Debug Logs	Generates a log file containing command line actions.
Servlet Communications Logs	Generates a log file containing information on servlet communication.
Connection Manager Logs	Generates a log file containing information on the connection activity.
Certificate Management Logs	Generates a log file containing certificate management information.
Certificate Management Debug Logs	Generates a log file containing certificate management information.
SSL VPN Incoming Connections Logs	Generates a log file containing information on the incoming connection.
SSL VPN Incoming Connections Debug Logs	Generates a log file containing debug information on the incoming connection.
Other SSL VPN Gateway Logs	Generates a log file containing miscellaneous information.
Cluster Logs	Generates a log file containing information about the SSL VPN cluster.

4 To save your modifications, click *OK,* then click *Apply Changes* on the Configuration page.

Viewing SSL VPN Statistics

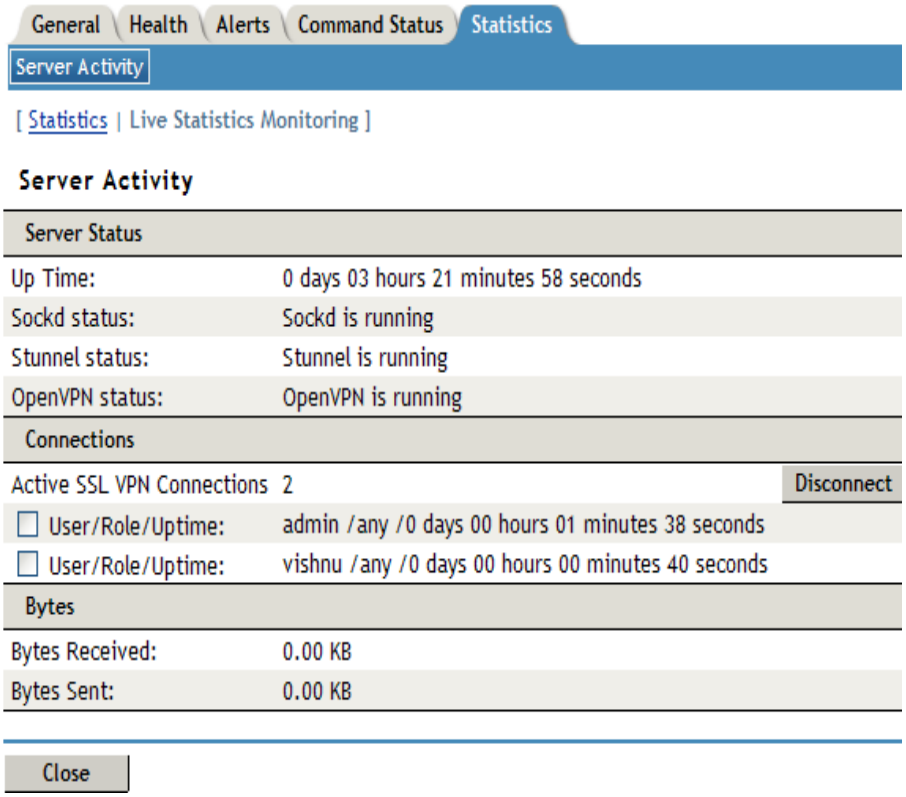
26

The Statistics page allows you to view such information as the number of active client connections and the time when the SSL VPN server was started.

26.1 Viewing Statistics of SSL VPN Server

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Statistics*.

The Server Statistics page is displayed.



Server Status information is gathered in the following sections:

Column	Description
Up Time	Displays the duration for which the server has been up and running.
Sockd Status	Displays if the sockd is running or not.

Column	Description
Stunnel Status	Displays if the Stunnel is running or not.

Connection information is gathered in the following sections:

Column	Description
Active SSL VPN Connections	Displays the number of active SSL VPN connections. The username, role of the user, and uptime of each user for each active connection.

Bytes information is gathered in the following sections:

Column	Description
Bytes Received	Displays the number of bytes received. You can also view a graph, which lists the number of bytes sent for fixed intervals. For more information, see Section 26.3, “Viewing the Bytes Graphs,” on page 145.
Bytes Sent	Displays the number of bytes sent. You can also view a graph, which lists the number of bytes sent for fixed intervals. For more information, see Section 26.3, “Viewing the Bytes Graphs,” on page 145.
Received Byte Rate	Displays the percentage of bytes received.
Sent Byte Rate	Displays the percentage of bytes sent.
Total Byte Rate	Displays the total percentage of bytes transferred.

2 Select one of the following options:

- **Statistics:** To display the number of active client connections and the time when the server was started, click *Statistics*.
- **Live Statistics Monitoring:** To refresh the above information for a specified interval, click *Live Statistics Monitoring*. You can select the refresh interval from the *Refresh Rate* drop-down list.

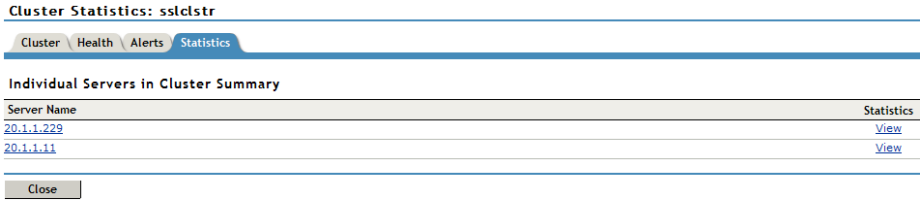
3 Click *Close* to close the *Statistics* tab.

26.2 Viewing Statistics of SSL VPN Server Cluster

Use this page to monitor a summary of the statistics for servers in a cluster. The following information is displayed:

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Cluster Name]* > *Statistics*.

The Cluster Statistics page is displayed.



2 The statistics page has the following information:

Server Name: The IP address identifying the SSL VPNs in the cluster. Click the *Edit* link to edit server information.

Statistics: Click the *View* link to get a summary of the statistics of individual servers in a cluster. For more information on viewing the statistics details of individual servers, see Section 26.1, “Viewing Statistics of SSL VPN Server,” on page 143.

3 Click *Close* to close the *Statistics* tab.

26.3 Viewing the Bytes Graphs

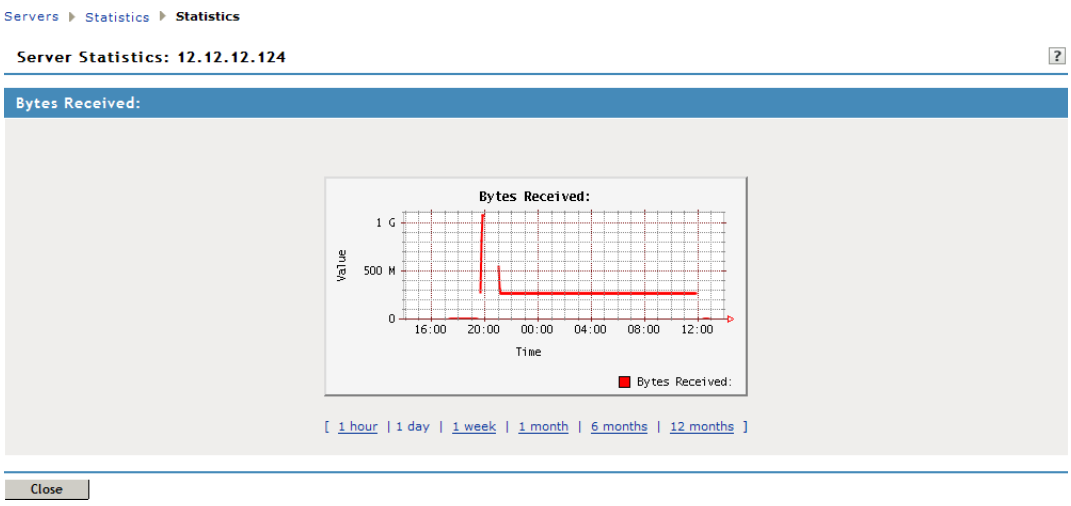
The number of bytes sent and bytes received can be viewed in the form of graphs. You can view graphs for the following time frames:

- **1 Hour:** The number of bytes sent or received every ten minutes.
- **1 Day:** The number of bytes sent or received every four hours.
- **1 Week:** The number of bytes sent or received every day.
- **1 Month:** The number of bytes sent or received every week.
- **6 Months:** The number of bytes sent or received every month for six months.
- **12 Months:** The number of bytes sent or received every month for one year.

To view graphs:

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Statistics*.

2 Select *Graphs* from either the *Bytes Received* or *Bytes Sent* section, depending on your needs.



3 Click *Close* to close the Graphs page.

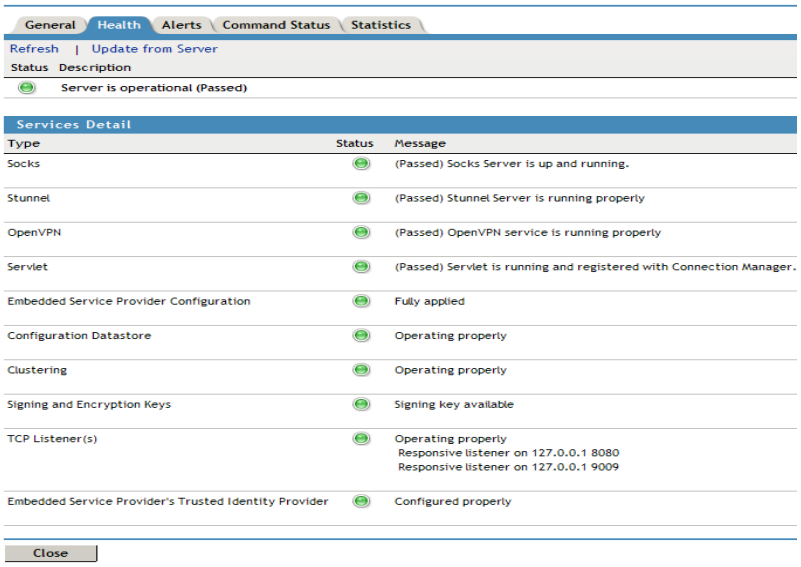
Monitoring Health of SSL VPN Servers

27

You can monitor the health of an SSL VPN Server through the Health page, which displays the current status of the server.

27.1 Monitoring Health of Single Server

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Health*.



The *Status* column displays the current state, and the *Description* column explains the significance of the current state.

The *Services Details* section provides the following information:

Type: Displays the type of service.

Status: Displays the status of the service.

Message: Displays a description of the status of the service.

2 To reload the current page with the latest status, click *Refresh*.

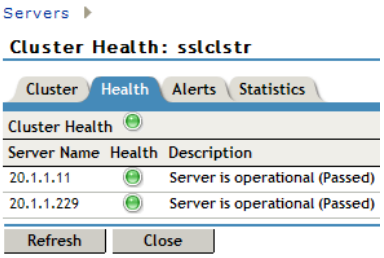
3 To send a request to the agent to update its status information, click *Update from Server*. Click *OK* in the confirmation dialog box. This can take a few minutes.

4 To close the Health page, click *Close*.

27.2 Monitoring Health of SSL VPN Cluster

You can monitor the health of an SSL VPN Server through the Health page, which displays the current status of the server.

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Cluster Name]* > *Health*.



The *Cluster Health* displays the current state, and the *Description* column explains the significance of the current state.

The *Services Details* section provides the following information:

Server Name: Displays name of the SSL VPN server in the cluster.

Health: Displays the health status of the server. The following health states are possible:

Icon	Description
	A green status indicates that the server has not detected any problems.
	A red status with a bar indicates that the server is stopped.
	A white status with disconnected bars indicates that the server is not communicating with the Administration Console.
	A yellow status indicates that the server might be functioning suboptimally because of configuration discrepancies.
	A yellow status with a question mark indicates that the server has not been configured.
	A red status with an x mark indicates that the server configuration might be incomplete or wrong, a dependent service might not be running or functional, or that the server is having a runtime error.

Click the icon to get the health status of individual servers.

Description: Displays a description of the status of the server.

2 To reload the current page with the latest status, click *Refresh*.

3 To send a request to the agent to update its status information, click *Update from Server*. Click *OK* in the confirmation dialog box. This can take a few minutes.

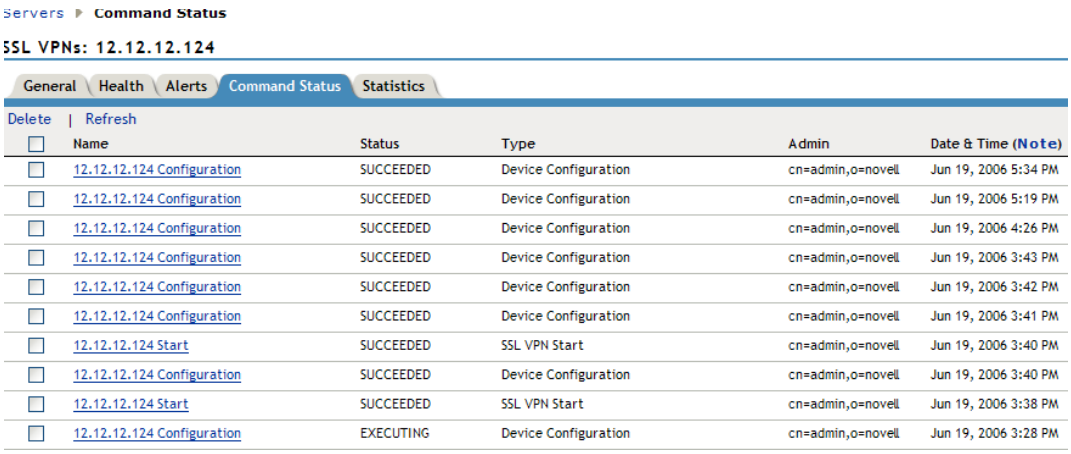
4 To close the Health page, click *Close*.

Viewing the Command Status of the SSL VPN Server

28

Use the Command Status page to view the command status of the selected SSL VPN server.

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Command Status*.



Name	Status	Type	Admin	Date & Time (Note)
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 5:34 PM
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 5:19 PM
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 4:26 PM
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:43 PM
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:42 PM
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:41 PM
12.12.12.124 Start	SUCCEEDED	SSL VPN Start	cn=admin,o=novell	Jun 19, 2006 3:40 PM
12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:40 PM
12.12.12.124 Start	SUCCEEDED	SSL VPN Start	cn=admin,o=novell	Jun 19, 2006 3:38 PM
12.12.12.124 Configuration	EXECUTING	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:28 PM

This page lists the command and the following information about the command:

Name: Contains the display name of the command. Click the link to view additional details about the command. For more information, see Section 28.1, “Viewing Command Information,” on page 149.

Status: Displays the status of the command. Some of the possible states include *Pending*, *Incomplete*, *Executing*, and *Succeeded*.

Type: Displays the type of command.

Admin: Indicates if the system or a user issued the command. If a user issued the command, the DN of the user is displayed.

Date & Time: Displays the local date and time the command was issued.

2 To delete a command, select the check box for the command, then click *Delete*. The selected command is cleared.

3 To update the current cache of recently executed commands, click *Refresh*.

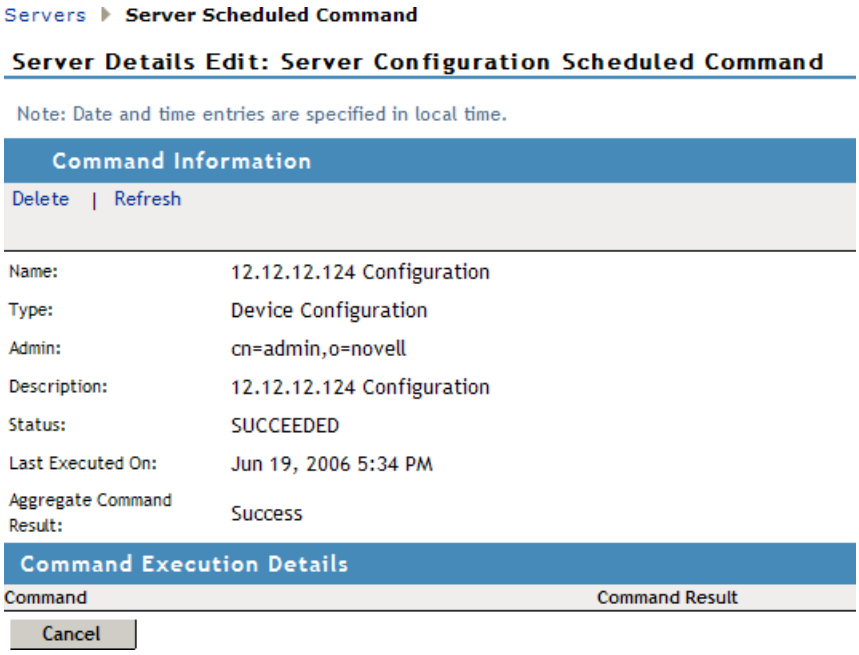
4 Click *Close* to close the Command Status page.

28.1 Viewing Command Information

To view configuration of individual commands:

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Command Status* >*[Individual Command]*.The command status page is displayed.

2 Click the command to get a detailed information on the command. The Server Configuration scheduled command page is displayed.



You can perform the following actions:

Delete: To delete a command, click *Delete*. Click *OK* in the confirmation dialog box.

Refresh: To update the current cache of recently executed commands, click *Refresh*.

3 Click *Close* to return to the command status page.

Monitoring SSL VPN Alerts

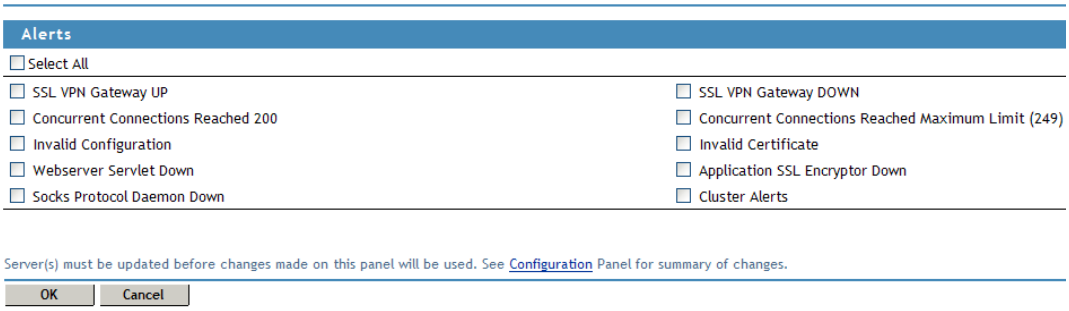
29

The Alerts page allows you to view information about current system alerts and to clear them. An alert is generated whenever the SSL VPN Gateway detects a condition that prevents it from performing normal system services.

29.1 Configuring SSL VPN Alerts

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Alert Settings*.

The Alert Settings Page is displayed.



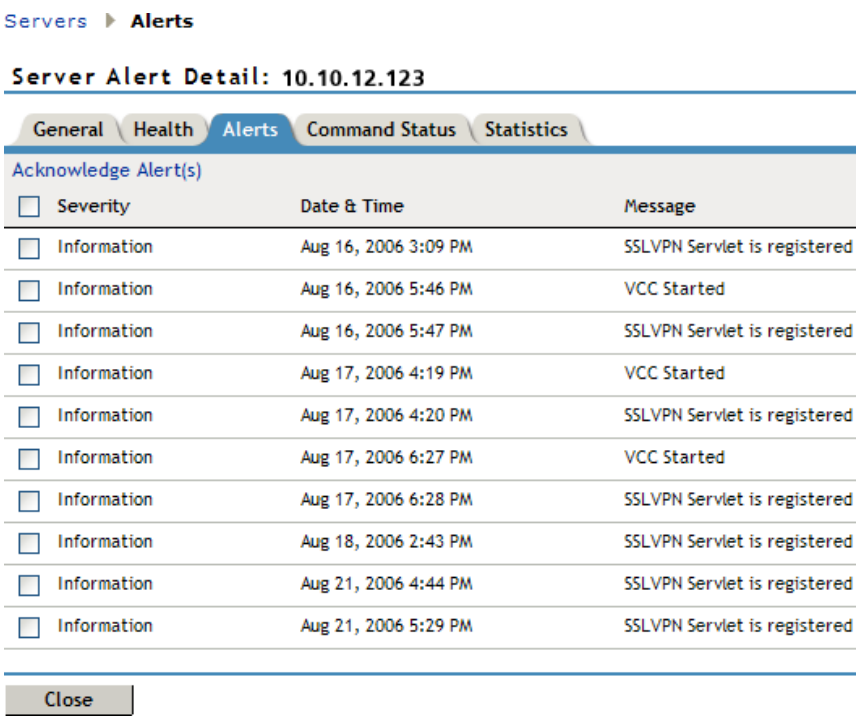
2 Select the *Select All* option to send alerts for all the events, or select one or more of the following:

Alert	Description
SSL VPN Gateway up	Sends an alert when the SSL VPN server is up and running.
SSL VPN Gateway down	Sends an alert when the SSL VPN server is down and is not functional.
Concurrent connections reached 200	Sends an alert when the number of concurrent connection reaches 200. The maximum is 249.
Concurrent connections reached maximum limit (249)	Sends an alert when the number of concurrent connections reaches 249.
Invalid configuration	Sends an alert when the configuration is not valid.
Invalid certificate	Sends an alert when the SSL VPN certificate used for encryption and communication is invalid.
Web Server servlet down	Sends an alert whenever a Web Server servlet is down.

Alert	Description
Application SSL encryptor down	Sends an alert whenever the SSL encryptor is down.
Socks Protocol Daemon down	Sends an alert whenever the socket protocol daemon is down.
Cluster Alerts	Sends alerts whenever the cluster node is up, down, or restarted.

29.2 Viewing SSL VPN Alerts

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Health*.



The following information is displayed:

Severity: Describes the type of alert. An alert can be informational, critical, or a warning.

Date & Time: Indicates the date and time when an alert was issued. The date and time are given in the local time.

Message: Displays the message that was sent with the alert. This information is optional.

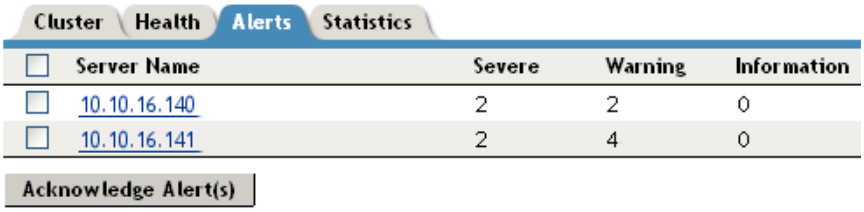
2 To send an acknowledgement, select the check box next to the alert, then click *Acknowledge Alert(s)*. When you acknowledge an alert, the alert is cleared from the list.

3 Click *Close* to close the Alerts page.

29.3 Viewing SSL VPN Cluster Alerts

To view information about current alerts for all members of a cluster:

1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Name of Cluster]* > *Alerts*.



2 Analyze the data displayed in the table.

Column	Description
Server Name	Lists the name of the SSL VPN server that sent the alert. To view additional information about the alerts for a specific SSL VPN, click the specific SSL VPN.
Severe	Lists the number of critical alerts that have been sent and not acknowledged.
Warning	Lists the number of warning alerts that have been sent and not acknowledged.
Information	Lists the number of informational alerts that have been sent and not acknowledged.

3 To acknowledge all alerts for an SSL VPN server, select the check box next to the SSL VPN server, then click *Acknowledge Alert(s)*. When you acknowledge an alert, you clear the alert from the list.

4 To view information about a particular alert, click the server name.

Troubleshooting SSL VPN

VI

You might sometimes encounter issues while installing or configuring the SSL VPN servers. The SSL VPN server might not work the way you intended because of problems encountered during installation or configuration. The following sections list some of the scenarios that you might encounter and the steps to troubleshoot such issues:

Troubleshooting SSL VPN Installation

30

This section has information on how you can troubleshoot problems while you are installing the SSL VPN server.

30.1 Manually Uninstalling the Enterprise Mode Thin Client

To manually uninstall the Enterprise mode thin client, do one of the following, depending on your operating software:

- **Windows:** If you are a Windows user, log in as admin and run `uninstall.exe` located in the `c:/Program Files/Novell sslvpn service` directory. You can also uninstall the SSL VPN service through *Start* > *Control Panel* > *Add or Remove Programs*.
- **Linux:** If you are a Linux user, log in as `root` and enter the following command on the Linux workstation:

  ```
  rpm -e novl-sslvpn-service
  ```

- **Macintosh:** If you are a Macintosh user, log in as root and do the following on the Macintosh workstation:

  1. Enter the following command to stop the SSL VPN services:

     ```
     /System/Library/StartupItems/novell-sslvpn-service/novell-sslvpn-service stop
     ```

  2. Enter the following command to remove all the contents of the package:

     ```
     rm -rf /System/Library/StartupItems/novell-sslvpn-service
     rm -rf /Library/Receipts/novl-sslvpn-service.pkg
     rm -f /usr/sbin/novl-sslvpn-service
     rm -f /usr/sbin/novl-sslvpn-service-upgrade
     rm -f /etc/novell-sslvpn-serv.conf
     ```

NOTE: If you are an administrator or a `root` user of the machine, you cannot switch from Enterprise mode to Kiosk mode unless your system administrator has configured you to connect only in Kiosk mode.

30.2 SSL VPN Health Status is Yellow After an Upgrade

If the status of SSL VPN server installed with Linux Access Gateway is yellow and the *Health* tab displays the following message:

```
The HTTP Reverse Proxy service "soapbc" is functioning properly. The HTTP
Reverse Proxy service <reverse proxy> might not be functioning properly. Few
of the webservers being accelerated are unreachable <Webserver IP>:8080.
```

Modify the existing path-based service accelerating SSL VPN server and configure the loopback IP 127.0.0.1 as the Web server IP. For more information, see Section 5.7, “Configuration Changes to the SSL VPN Server Installed with the Linux Access Gateway,” on page 50.

Troubleshooting SSL VPN Configuration

31

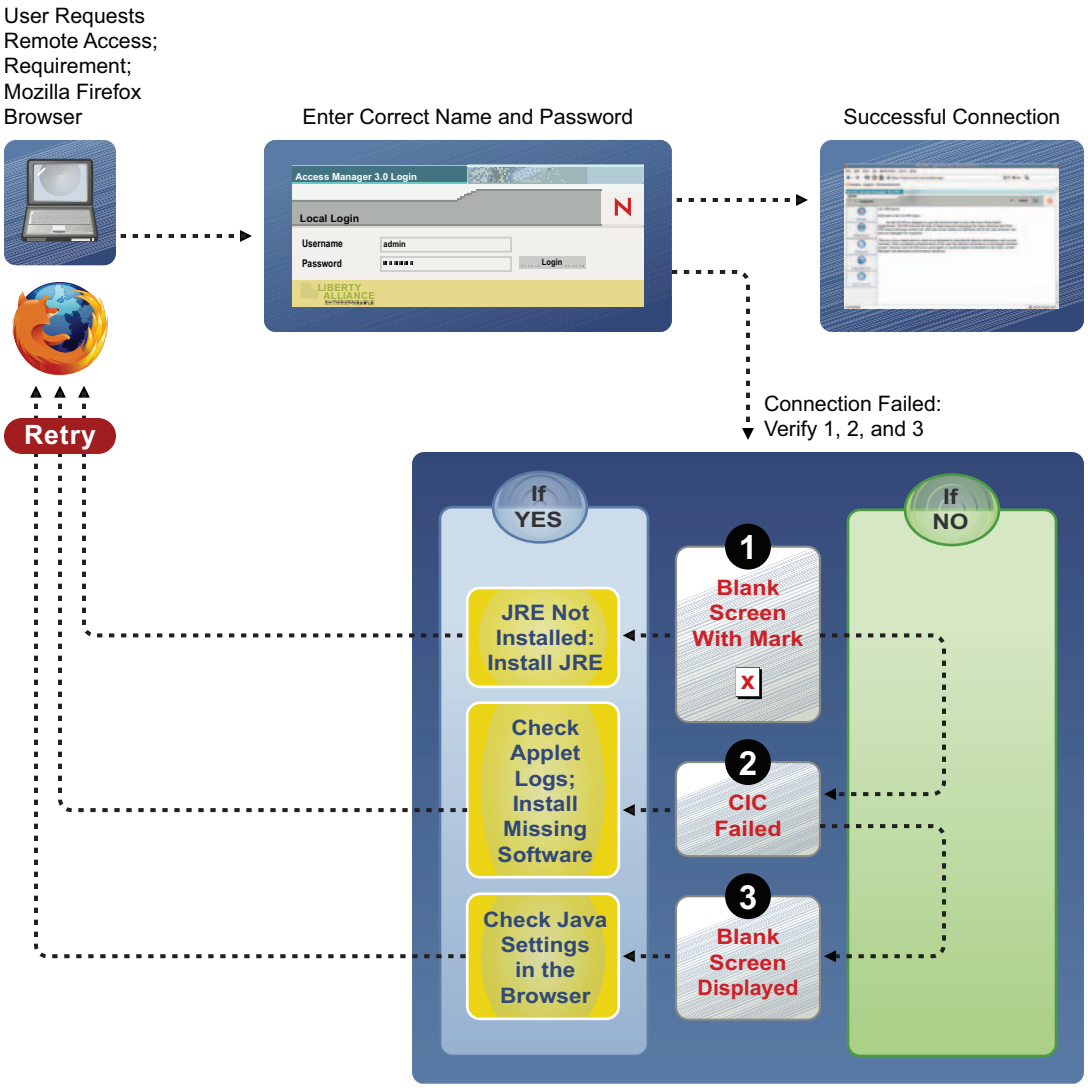
This section provides various troubleshooting scenarios that you might encounter while configuring SSL VPN.

31.1 Successfully Connecting to the Server

You can access the protected resources that are using SSL VPN by authenticating to the proxy server. The proxy server loads the SSL VPN client on your browser. The following sections describe some of the problems that clients might encounter:

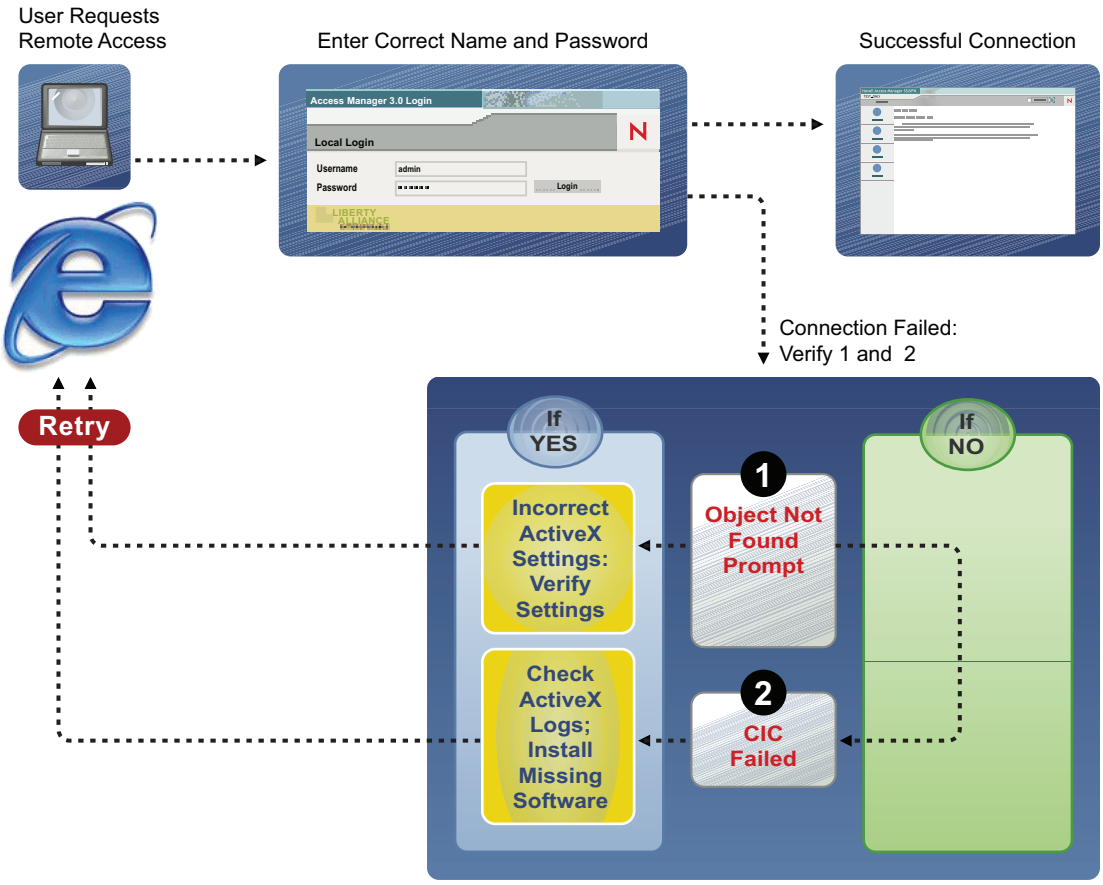
31.1.1 Connection Problems with Mozilla Firefox

Figure 31-1 *Using Mozilla Firefox to Connect to the SSL VPN Server*



31.1.2 Connection Problems with Internet Explorer

Figure 31-2 *Using Internet Explorer to Connect to the SSL VPN Server*



31.2 The SSL VPN Server Is in a Pending State

The SSL VPN server sometimes gets into a pending state even when all of its commands have been successful.

To work around this problem:

1. In the Administration Console, click *Devices* > *SSL VPNs*.
2. Click the *Commands* link.
3. Select all the pending commands, then click *Delete* > *Close*.
4. If the device is still in a pending state, click *Auditing* > *Troubleshooting*.
5. In the *Device Pending with No Commands* section, select the SSL VPN server and remove the pending state.

31.3 SSL VPN Connects in Kiosk Mode, But There Is No Data Transfer

If the user is able to successfully connect in Kiosk mode, but the data transfer does not happen, check to see if the user is configured to connect through a forward proxy, then verify that the entries in the `proxy.conf` file are correct. For more information, see Chapter 17, "Configuring SSL VPN to Connect through a Forward Proxy," on page 109.

31.4 The TFTP Application and GroupWise Notify Do Not Work in Enterprise Mode

If the TFTP application and GroupWise® Notify do not work in Enterprise mode, make sure you have done the following:

- You have configured a route using the default gateway. For more information, see Chapter 12, "Configuring Route and Source NAT for Enterprise Mode," on page 81.
- You are not using source NAT to route packets.

31.5 SSL VPN Not Reporting

If SSL VPN is not reporting, you must verify the status of JCC and the SSL VPN server and restart them if they are down. If restarting any of these components does not work, reconfigure SSL VPN. If none of these work, you must delete and reimport the SSL VPN server.

31.5.1 Verifying and Restarting JCC

To check the status of JCC, enter the following command:

```
/etc/init.d/novell-jcc status.
```

If it is not running, enter the following command to restart JCC:

```
/etc/init.d/novell-jcc restart
```

31.5.2 Verifying and Restarting the SSL VPN Server

To verify the status of the SSL VPN server, enter the following command:

```
/etc/init.d/novell-sslvpn status
```

If any component is down, stop and start the SSL VPN server by using the following commands:

```
novell-sslvpn stop
novell-sslvpn start
```

31.6 Verifying SSL VPN Components

Use the commands and processes described in the following sections to verify that the SSL VPN components are running:

31.6.1 SSL VPN Server

To verify the status of the SSL VPN components, use the commands listed in the table below:

Component	Command
Connection Manager	`pgrep connman`
Sock Daemon	`pgrep sockd`
Secure Tunnel	`pgrep stunnel`
OpenVPN	`pgrep openvpn`

31.6.2 SSL VPN Linux Client

Component	Command
Policy Resolver for Kiosk mode	`pgrep polresolver`
Secure Tunnel for Kiosk mode	`pgrep stunnel`
OpenVPN for Enterprise mode	`pgrep openvpn`

31.6.3 SSL VPN Macintosh Client

Component	Command
Policy Resolver for Kiosk mode	`ps -A | grep polresolver | grep -v grep`
Secure Tunnel for Kiosk mode	`ps -A | grep stunnel | grep -v grep`
OpenVPN for Enterprise mode	`ps -A | grep openvpn | grep -v grep`

31.6.4 SSL VPN Windows Client

Check to see if the stunnel and polresolver processes are up and running if SSL VPN is in Kiosk mode, and check openVPN if SSL VPN is in Enterprise mode.

31.7 Unable to Contact the SSL VPN Server

In the client browser, if you encounter the message `SSLVPN Gateway is in bad state` or the message `SSLVPN Gateway is not available`, verify the following:

- **Error Status:** Check the status at `/var/log/messages`, `/var/log/stunnel.log`, and `/var/log/novell-openvpn.log`.
- **SSL VPN Status:** At the command prompt, enter the following command:

  `/etc/init.d/novell-sslvpn status`
- **Message Log:** Check the `/var/log/messages` file for more information.

31.8 Unable to Get Authentication Headers

If the browser displays the `Unable to Get Authentication Headers` error while accessing the SSL VPN URL, check whether the custom HTTP headers required for SSL VPN are configured and enabled in the Access Gateway. In the Administration Console, click *Access Gateways > [Configuration Link] > [Name of Reverse Proxy] > [Name of SSL VPN Proxy Service] > [Name of SSL VPN Protected Resource] > Identity Injection*.

The SSLVPN_Default policy should be enabled. This policy injects an authentication header and two custom headers (X-SSLVPN-PROXY-SESSION-COOKIE and X-SSLVPN-ROLE).

31.9 The SSL VPN Connection Is Successful But There Is No Data Transfer

Possible Cause: If this issue appears in Kiosk mode, the private address specified during the server configuration might be incorrect.

Action: In the Administration Console, click *Devices > SSL VPNs > Edit > Gateway Configuration*, then check the private address configuration. Make sure that this is the IP address of the private interface of the SSL VPN server.

Possible Cause: This issue might occur in both Kiosk and Enterprise modes of SSL VPN. If the SSL VPN server is behind a NAT, the external IP address specified during server configuration might be incorrect.

Action: In the Administration Console, click *Devices > SSL VPNs > Edit > Gateway Configuration*. Make sure that the external IP address is configured to be the IP address of a NAT through which the external user on the Internet can access the SSL VPN server.

Possible Cause: If this issue appears in Enterprise mode, it could be because the NAT configuration is wrong.

Action: At the command prompt, enter `iptable -L` to check the configuration details. For more information, see Section 11, “Configuring the IP Address, Port, and NAT,” on page 75.

Possible Cause: If this issue appears in Enterprise mode, it could be because the router configuration is wrong.

Action: Check the router configuration. For more information, see Section 11, “Configuring the IP Address, Port, and NAT,” on page 75.

Possible Cause: If this issue appears in Enterprise mode, the TUN interface might be down.

Action: At the command prompt, enter `ifconfig` to check if the TUN0 interface is down. If it is down, enter the `etc/init.d/novell-sslvpn restart` command to restart the SSL VPN services.

If you are using a 64-bit machine and have changed the TUN interface, check to make sure the interface is up. If it is down, enter the `etc/init.d/novell-sslvpn restart` command to restart the SSL VPN services.

31.10 Unable to Connect to the SSL VPN Gateway

Possible Cause: A forward proxy is enabled in Internet Explorer.

Action: In the Administration Console, select *Devices* > *Access Gateways* > *Edit* > *Reverse Proxy* > *Proxy List* > *Path-Based Multi-Homing* > *HTTP Options*. Select the *Allow Pages to Be Cached by the Browser* check box.

31.11 Multiple Instances of SSL VPN Are Running

If you get this error while trying to connect to SSL VPN, it could be because there was an improper logout in the previous session and some of the processes did not close properly. Verify if any of the SSL VPN processes are running. For more information on how to verify, see Section 31.6, “Verifying SSL VPN Components,” on page 163.

If this error occurs, manually kill the process if you are an admin or a root user of the machine. If you are a non-admin or non-root user of the machine, restart the machine.

31.12 Issue with the Preinstalled Enterprise Mode Client

If you preinstalled the Enterprise mode client for a non-admin or a non-root user of the machine, the user should be connected to SSL VPN without being prompted to enter the credentials of the admin user. If the user is still prompted to specify the credentials of the admin user, check to make sure the SSL VPN service is running. For more information on how to check the SSL VPN service, see Section 31.6, “Verifying SSL VPN Components,” on page 163.

31.13 Socket Exception Error After Upgrading SSL VPN

You might randomly get a socket exception error after upgrading the ESP-enabled SSL VPN cluster if the SSL certificate is configured in HTTPS mode. You are getting this error because the SSL VPN certificate is missing from the keystore. You must reinstall the SSL VPN server and configure a new SSL certificate to work around this problem.

31.14 SSL VPN Server Is Unable to Handle the Session

If the SSL VPN server failed because of SSL VPN component failure and you restarted the server by using the `novell-sslvpn start` command, the server cannot handle the subsequent sessions. To work around this issue, restart Tomcat by using the `novell-tomcat5 restart` command.

31.15 Embedded Service Provider Status Is Red

If the status of the Embedded Service Provider is red or if the Embedded Service Provider does not come up after installation, restart Tomcat by entering the following command:

```
novell-tomcat5 restart
```

31.16 Connection Manager Log Does Not Display the Client IP Address

You might see `UNKNOWN HOST` displayed in the Connection Manager logs instead of the IP address of the client, when ESP-enabled SSL VPN is installed. This is because this information is provided by the Access Gateway and is available only if the Traditional Novell SSL VPN server is deployed.

31.17 SSL VPN Full Tunnel Connection Disconnects on VMware

Possible Cause: SSL VPN full tunnel connection might disconnect due to no keepalive response if Novell Access Manager setup is on a host-only network, on a VMware interface of the client.

Explanation: After full tunnel is enabled, a new route entry would be added to the client routing table to route the keepalive packet to SSL VPN server through default gateway. Because SSL VPN gateway is on host-only network on a VMware, keepalive packet might not reach the SSL VPN server through default gateway.

Action:

1. Add a virtual address to the SSL VPN gateway.

   For example, if the primary address is 200.200.200.140, add 200.200.200.141.
2. Disconnect physical network from client to make sure that there is no default gateway to the Internet.
3. Manually add a default route.

   For example, `route add 0.0.0.0 mask 0.0.0.0 200.200.200.141 metric 5`.

31.18 Clustering Issues

31.18.1 Bringing Up the Server If a Cluster Member Is Down

Action: Check the Administration Console for the component that is down in the cluster member. If the component is `openvpn`, `stunnel`, or `sockd`, restart SSL VPN by using the following command:

```
/etc/init.d/novell-sslvpn restart
```

You can check for the status by using the following command:

```
/etc/init.d/novell-sslvpn status
```

31.18.2 Bringing Up a Binary If It Is Down

Action: If the `openvpn`, `stunnel`, or `sockd` binaries are not running:

1. Stop the server by using the following command:

   ```
   /etc/init.d/novell-sslvpn stop
   ```

2. Check whether the `openvpn`, `stunnel`, and `sockd` binaries are still running, by using the `ps` command.

   If the binaries are running, kill the processes and start the server.

3. Restart Tomcat if it is not responding.
4. Check the status of the SSL VPN server.

31.18.3 Debugging a Cluster If Session Sharing Doesn't Properly Happen

Action: Check the connectivity among the cluster members by using the following command:

```
netstat -anp | grep 8900
```

Restart Tomcat in all the machines if each cluster member doesn't have a TCP connection with other members.

When a user is added, you can see the username in `/var/log/messages of all cluster members`.

NOTE: 8900 is the default port used for session sharing among cluster members. If a different port is configured, `grep` for session sharing.
