AUTHORIZED DOCUMENTATION

SSL VPN Server Guide

Novell
Access Manager

3.1 SP2

November 16, 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 data cannot be intercepted and only authorized users have access to the network. Users can access SSL VPN services from any Web browser.

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/TLS)
- 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

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

- *Novell Access Manager 3.1 SP2 SSL VPN User Guide*
- *Novell Access Manager 3.1 SP2 Installation Guide*
- *Novell Access Manager 3.1 SP2 Setup Guide*
- *Novell Access Manager 3.1 SP2 Administration Console Guide*
- *Novell Access Manager 3.1 SP2 Identity Server Guide*
- *Novell Access Manager 3.1 SP2 Access Gateway Guide*

Documentation Conventions

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

Introduction to SSL VPN

1

With more and more individuals working outside traditional office settings, the need for secure remote access to corporate resources has become more important than ever. No matter where users are: whether traveling nationally or internationally, working from home or on site at a partner location, they should be able to access corporate resources without compromising security. The Novell Access Manager Secure Socket layer Virtual Private Network (SSL VPN) is the product that allows secure “anywhere-, anytime-access”.

Novell's SSL VPN is a new type of VPN based on the Secure Sockets Layer (SSL) protocol used in e-commerce. SSL has been traditionally and widely deployed for securing web-based applications in the form of HTTPS. SSL is embedded in most IP stacks and occupies the architectural base of the application layer. It can be installed directly on the Linux Access Gateway, or on any host running SLES 9, 10 or 11. For more information on deployment scenarios, see (http://www.novell.com/documentation/novellaccessmanager/installation/?page=/documentation/novellaccessmanager/installation/data/bookinfo.html).

This document will look at the architecture of the Novell Access Manager SSLVPN solution, the flow of events within an SSLVPN session and look at troubleshooting tools available to help troubleshoot SSLVPN issues in your environment.

1.1 SSL VPN Solution Options

Novell's SSLVPN solution encompasses two options:

1.1.1 Kiosk Mode

Kiosk mode (uses a combination of the stunnel and dante open source projects at (http://www.stunnel.org/ and http://www.inet.no/dante/). In the Kiosk mode of SSL VPN, only a limited set of applications are enabled for SSL VPN. A non-admin or a non- root user who does not have the administrator access can connect to SSL VPN in the Kiosk mode. In Kiosk mode, applications that were opened before the SSL VPN connection was established are not SSL-enabled.

The Kiosk mode supports only TCP and UDP applications and not ICMP. 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 cannot force Kiosk mode when connected as a user with root or admin privileges.

1.1.2 Enterprise Mode

Enterprise mode uses the OpenVPN open source project at (http://openvpn.net/).You can access SSL VPN in the Enterprise mode if you have admin or root user access to the workstation, if you know the admin or root user credentials, or if you have preinstalled the client components on the workstation.

In Enterprise mode, all applications, including those on the desktop and the toolbar are SSL-enabled, regardless of whether they were opened before or after connecting to SSL VPN. In this approach, a thin client is installed on your workstation. This thin client takes care of the administrator activities required for the Enterprise mode of SSL VPN. In the Enterprise mode, the IP Forwarding feature is enabled by default on the server.

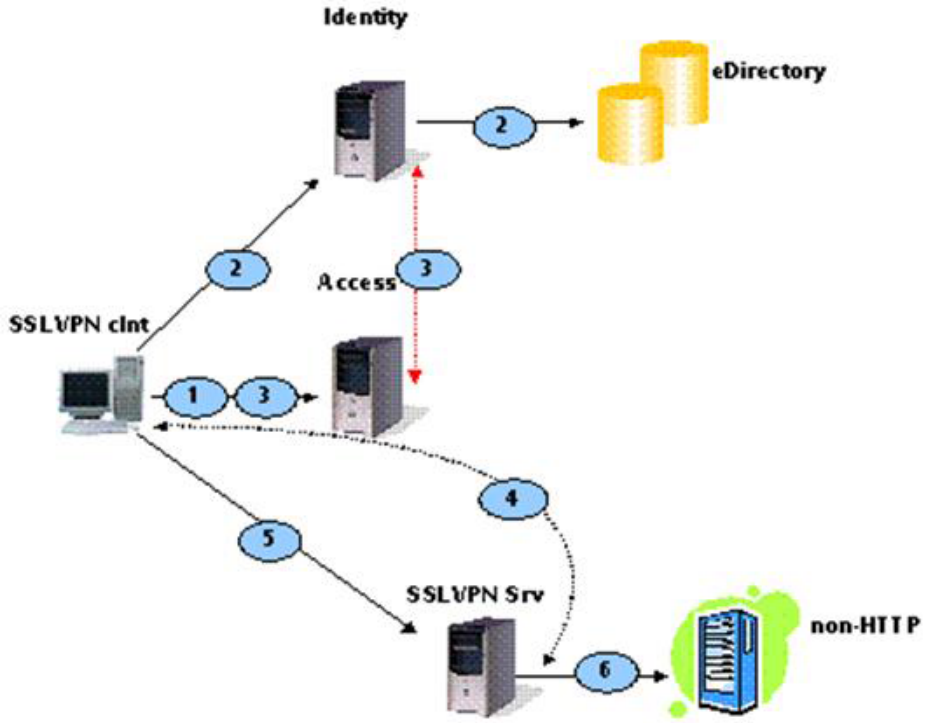
The Enterprise mode is recommended for devices that are managed by an organization, such as a laptop provided by the organization for its employees. The Enterprise mode of SSL VPN supports the following applications, which have problems in Kiosk mode:

- Protocols such as ICMP, NetBIOS and Microsoft RPC (used with outlook mail client).
- Applications that open TCP connections on both sides, such as VoIP, PCAnywhere and active FTP.
- Enterprise applications such as CRM and SAP.
- Applications such as Windows File Sharing systems, the Novell Client and Novell SecureLogin.

1.2 Architecture and High-Level Flow of Events

Before delving into the details of the various operation modes, one must look into the flow of events required to get an SSLVPN workstation connected to the server. This connection should be done in such a way that it can transmit data to the non HTTP application it is protecting. The diagram below shows a basic SSLVPN architecture where the SSLVPN server is running on its own hardware platform, with a non HTTP based application sitting behind it. In order to access this non- HTTP application from the SSLVPN client, the following steps need to take place.

Figure 1-1 *Accessing a non- HTTP application from the SSLVPN client*



1. The SSLVPN client workstation will hit the SSLVPN server protected resource on the Access Gateway. The Access Gateway must have a proxy service defined for the SSLVPN server so that all initial requests from a browser to the SSLVPN server (for path /sslvpn/login) will go to the Access Gateway.
2. If the user is not already authenticated for that protected resources, the user will be redirected to the Novell Identity Server (IDP) to login. The user will be presented with a login page where the credentials are entered and submitted. The credentials will then be validated against a back-end user store (eDirectory in the above example). Assuming the user's credentials are validated, an artifact gets sent from the Identity server to the browser.
3. The browser redirects the artifact to the Access Gateway. The Access Gateway sends the artifact back to the Identity server over the SOAP backchannel (direct communication between Access Gateway and IDP), and the IDP server responds with an assertion, including user specific details. After the Access Gateway consumes this assertion it sends another HTTP redirect back to the browser. A session cookie is sent back for use with subsequent requests for this SSLVPN resource, telling the browser to send the request to the SSLVPN server (/sslvpn/login).
4. The browser sends the request to the SSLVPN /sslvpn/login via the Access Gateway. The Access Gateway, with the SSLVPN Identity Injection enabled for this resource, adds the required headers (user information, sessionID and roles) to the HTTP headers of the outgoing request. For the header details, see (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html). The SSLVPN server receives this request from

the Access Gateway, identifies the user/role and locates the policy information for the role. This user policy information, as well as the SSLVPN client binaries (including the stunnel client) is sent back to the browser via the Access Gateway.

5 The SSLVPN client software is initialized on the client, and a connection to the SSLVPN server is made. This connection is direct from the SSLVPN client to the server, and not via the Access Gateway. (The only SSLVPN specific traffic that continues through the Access Gateway are regular keep-alives to make sure the SSLVPN server and browser client are still active). When an application on the client tries to access a protected resource behind the SSLVPN server, the application data is tunneled to the server. It is then proxied or forwarded to the client, depending on the mode of operation. More details are discussed below.

Before looking at the flow in more detail, let's look at the two SSLVPN modes of operation and the components associated with each.

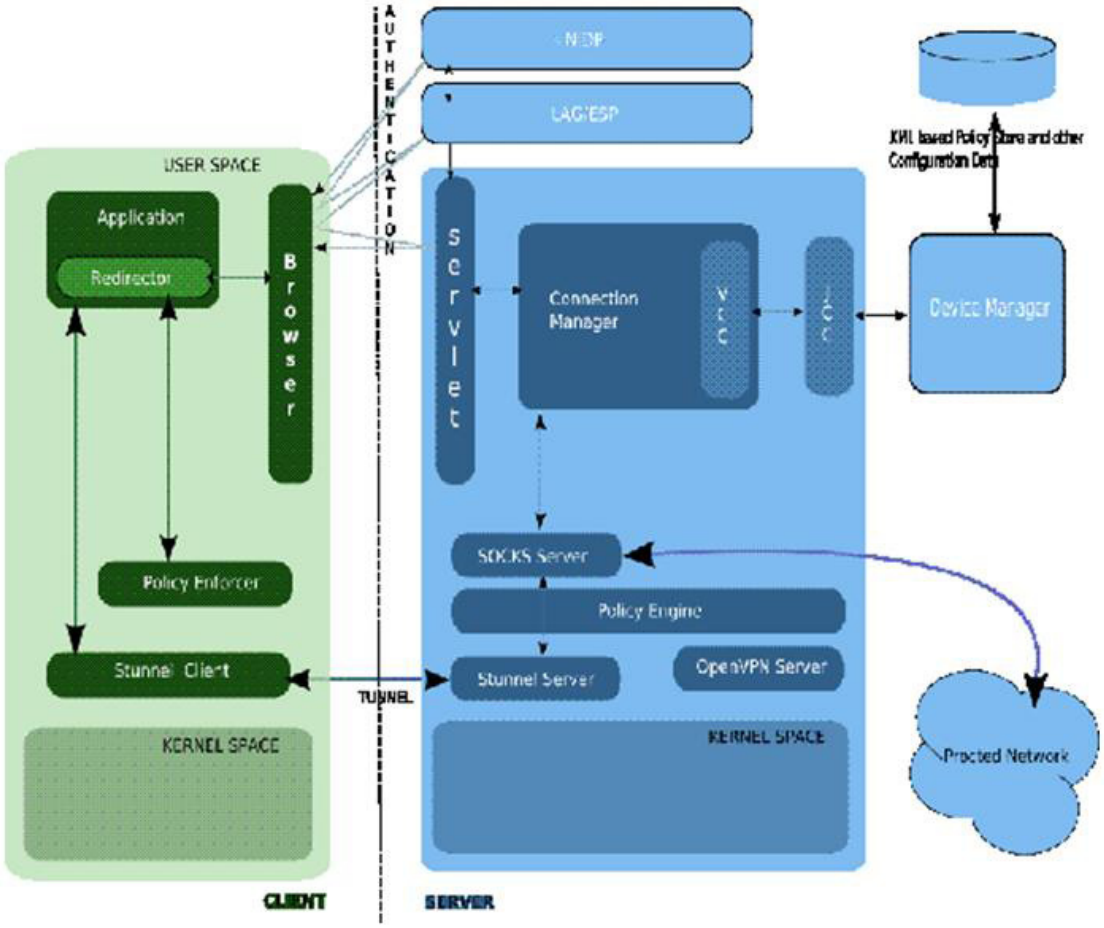
1.3 Kiosk Mode - Overall Architecture

The Kiosk, or Stunnel Mode of operation is based on the open source project at (http://www.stunnel.org/).

- Section 1.3.1, “SSLVPN Kiosk Mode - Server-side Components,” on page 15
- Section 1.3.2, “SSLVPN Kiosk Mode - Client-Side Components,” on page 16
- Section 1.3.3, “Kiosk Mode Authentication Flow,” on page 17
- Section 1.3.4, “Kiosk Mode Data Transfer Flow,” on page 18

The diagram below shows the components associated with the Kiosk Mode and briefly describes each of the components found in the solution:

Figure 1-2 *Kiosk Mode Architecture*



1.3.1 SSLVPN Kiosk Mode - Server-side Components

Servlet: The SSLVPN servlet component can be run on any tomcat or servlet engine, and it need not be installed on the actual SSLVPN server itself. If not installed on the SSLVPN server, administrators must modify the config.txt file in the `/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/` directory. For more information see (Configuring Load Balancing Through Servlets' under http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b6820mb.html.) This servlet package name is novl-sslvpn-servlet-3.* (Note: * depends on version). For the most part, this includes the `/var/opt/novell/tomcat5/webapps/sslvpn/*` files required by the servlet environment.The servlet receives the authenticated users sessions specific informatio n from the Access Gateway. The goal of the servlet is to:

- Handle incoming HTTP requests from the Access Gateway destined for the SSLVPN login (/sslvpn/login) page.
- Run individual communication channel with applet for the direct control of the client session, making sure that the session is open and valid, or closed and cleared.
- Send/receive control messages to/from SSLVPN connection manager. For example, this would include sending the user credentials, sending roles to the connection manager components, and processing the traffic policies coming back for that user.

Connection Manager: This is a TCP-based application running on a SLES server that listens out on TCP port 2010 and communicates with the above servlet. This component, as well as the others below, are all part of the novl-sslvpn-3.* (* depends on version). The connection manager service is in `/opt/novell/sslvpn/bin/connman`. It's main functions include the following:

1. Managing a server socket (UNIX domain) to communicate with:
   - Admin Console to synchronize the configuration changes
   - Socks and stunnel servers pushing changes out
   - Monitoring and Auditing module for interfacing into the NSure Auditing system
2. Dynamic connection management, such as:
   - Pulling out the policies from configuration database for a particular identity.
   - Communicating the change in data for Socks Server.

Policy Engine: There is a policy enforcer component at the server as well as on the client. Given a specific request passed to it by the socks server, this component checks against the policies saved in the policy.txt file at `/etc/opt/novell/sslvpn`. Depending on whether a match is found, the traffic is either allowed or denied.

Socks Server: This is a TCP-based application running on a SLES server that listens on TCP port 1080. The socks service is in `/opt/novell/sslvpn/bin/sockd`. The SOCKS 5 Server acts as a generic proxy between the SOCKS Client and the end host, which resides in the protected network. This component, together with Stunnel stack, provides the core SSL VPN functionality.

Stunnel Server: This is a TCP-based application running on a SLES server, listening on TCP port 7777 by default. The stunnel service is in `/opt/novell/sslvpn/bin/stunnel`. The stunnel program is designed to work as an SSL encryption wrapper between the remote client and a local (socks) server. The concept is that by having non-SSL aware daemons running on your system you can easily setup them to communicate with clients over a secure SSL channel

VCC/JCC: This is the protocol used to interface into the Access Manager configuration store so that all changes to the configuration are synchronized with the SSLVPN server components via the Connection Manager.

1.3.2 SSLVPN Kiosk Mode - Client-Side Components

Browser: The browser is initially required to contact the SSLVPN servlet via the Access Gateway. Once connected, keep-alive probes are continuously sent from the browser to the SSLVPN servlet to make sure that the existing session remains valid.

Application Redirector: On the workstation, all the outgoing traffic needs to be intercepted and treated differently, if it is destined for SSLVPN protected network. The mechanism used to intercept this traffic will be implemented differently for Linux and Windows workstations. On a Linux workstation, the LD_PRELOAD environmental variable is modified to load our own libsock.so library to handle the connect socket calls. On windows workstation, a similar approach of hooking into library is used.

Policy Enforcer: When the redirector intercepts the application level request, it checks with the policy enforcer to determine whether the request needs to out through the SSLVPN tunnel. This component checks the policies associated with this authenticated and checks whether the outgoing request conforms to the policies allowed for that user. Depending on the response, it allows or denies them.

Socks Client: Assuming that the policies allow the authenticated user access the remote application, the application level request is sent to the socks client on the workstation. This socks client appends a socks v5 header and proxies the application data within the socks payload. Once done, the request is passed to the Stunnel client on the same host.

Stunnel Client: With the socks data ready to be sent to the remote application server, the final step involves encrypting this data and packaging it within a new seat of headers. This is the role of the stunnel client. The stunnel client simply encrypts the socks data passed to it and adds information required to build transport and network layer headers. The main transport layer headers include the TCP destination port of 7777 by default. The corresponding IP header includes the IP address of the SSLVPN server external IP address, and not the IP address of the application server we are trying to communicate with. The stunnel client listens on both TCP and UDP. If the client host has been configured to use port X, it spawns a listener on both TCP and UDP port X. This avoids connection issues later if the transport layer has been changed on the SSLVPN server side.

1.3.3 Kiosk Mode Authentication Flow

The Kiosk mode authentication flow is based on the assumption that you are authenticated and have accesses to SSLVPN login page.

1. Proxy sends a request to the SSLVPN servlet (cookie and authenticated identity information are passed to the Servlet through this message).
2. The Servlet informs Connection Manager of a successful connection and awaits the user policies and client binaries.
3. At this time, Connection Manager becomes aware that a user has been successfully authenticated for SSL VPN session by an external authenticating agent (Access Gateway). The info it gets from the servlet at this stage includes the following:
   - User identity
   - Cookie for the http session between authenticating agent and browser
   - Client/browser identity (IP address and port), which can also be the dynamic NAT's identity.
   - Time of connection.
4. The Connection Manager validates such a connection request and the does the following:
   - Checks for the duplication of connection from the same client machine.
   - Builds the policy list (traffic and cic) for this particular user.
   - Sends the policies back to the servlet.
5. The servlet, upon receiving the above information from the connection manager
   - Generates a web page with Active-X controls or a Java Client applet (depending on whether client browser is IE or not). It includes the user policies and client binaries as a self-extractable download. The client binaries depend on the platform the client is running on (Windows, Linux, MAC) and include such things as an openssl, socks, stunnel client. The files may be found under the `/var/opt/novell/tomcat5/webapps/sslvpn/` directory of SSLVPN server.
   - Sends a 200 OK HTTP response back to the browser via the Access Gateway proxy, with the contents of the above web page.
6. The Access Gateway proxy sends the response back to the browser.

7 The browser processes the response and runs the self- extractable image it downloaded. The Client components are installed and Java Applet or Active-X controls starts running. Assuming everything initializes correctly, the Socks client will try to communicate with the Socks server. As this is a secure path, stunnel initiates the SSL negotiation.

8 The Stunnel client does not do the the SSL negotiation (exchanging certs, generating session keys) with the server to form the SSL channel until data is sent. In Kiosk mode, when the Java applet (UI) indicates that the SSL VPN connection is established, it's just an indication that the services have initialized successfully. The Enterprise mode client below works very differently at this stage.

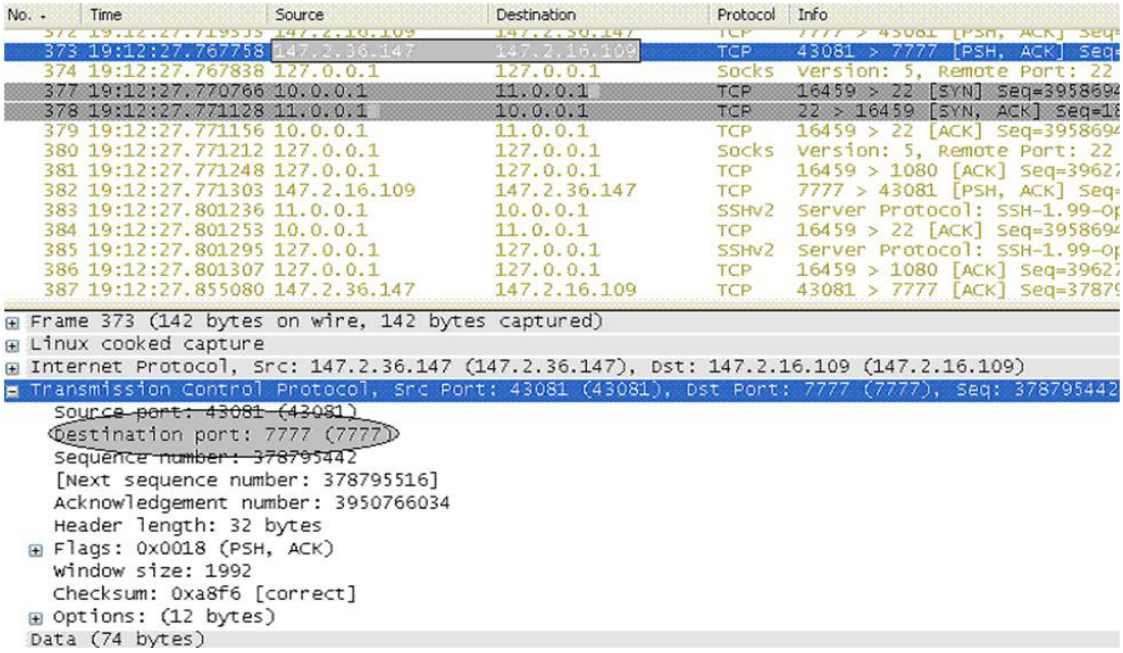
1.3.4 Kiosk Mode Data Transfer Flow

The kiosk mode data transfer flow is when the application data sent to remote host. When data is sent from the client application to the remote server, this application data is tunneled by the Kiosk mode SSLVPN client. Looking at the packet types visible on the network, when such a client tries to talk to a remote application server in Kiosk mode, you can see that the default transport layer protocol is TCP.

In the example below, a user on the workstation running the SSLVPN Kiosk mode client has tried to initiate an SSH session to the SSH server at 11.0.0.1, which is located on an internal network only accessible behind the SSLVPN private interface. The 147.2.36.147 is the IP address of the SSLVPN workstation where the client application is running. The SSLVPN server has two interfaces: the publicly accessible interface at 147.2.16.109, and the private interface 10.0.0.1 that is the next hop to all SSLVPN protected networks.

Packet 373 shows the SSH data being tunneled from the workstation to the public IP address of the SSLVPN server (147.2.16.109). The default SSLVPN configuration parameters are used, so the data is sent within a TCP segment destined for port 7777.

Figure 1-3 *Packet 373, Port 7777*



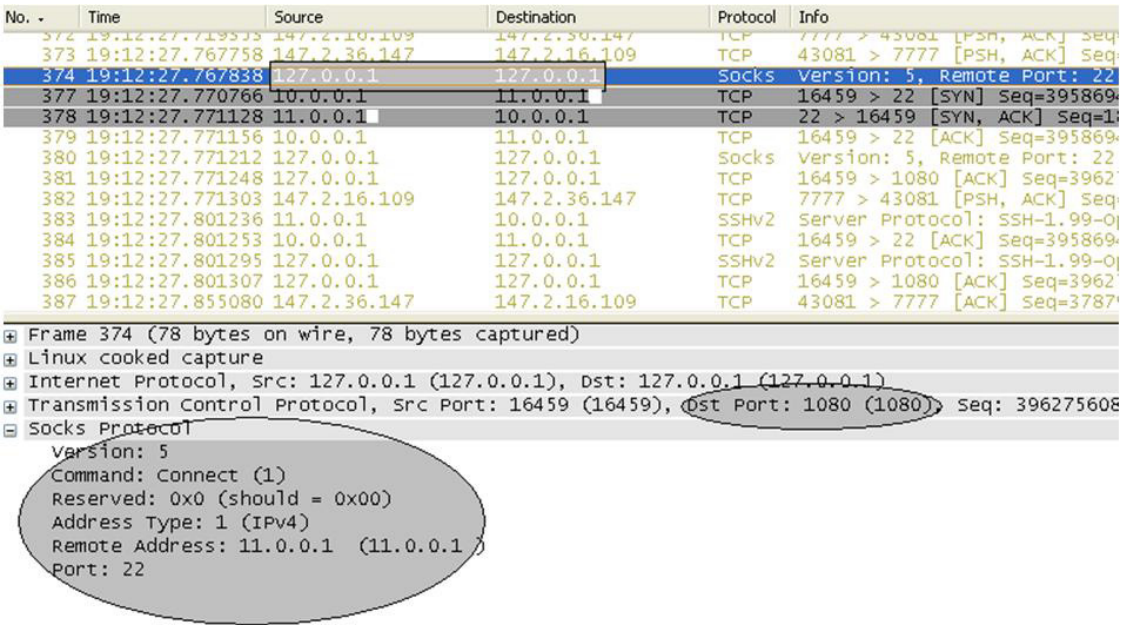
With tcpdump on a SLES host, you can trace packets on the loopback interface (e.g., using 'tcpdump -i any -n -s 0'). What we can see in packet 374 is the resulting packet after the SSLVPN server has unencrypted the packet (the Socks v5 data). The latest versions of Wireshark will decode the Socks headers and show the authentication process. An example of the Socks authentication process that goes on between the SSLVPN client and server would show the following: The client offers various authentication modes and server chooses most appropriate (username/pwd below). The client then sends the credentials specific for this users session and assuming that the Socks server can validate, then the client and server are authenticated, as shown below:

Socks Client <----------> Socks Server

Figure 1-4 *Socks Server credentials Validation*

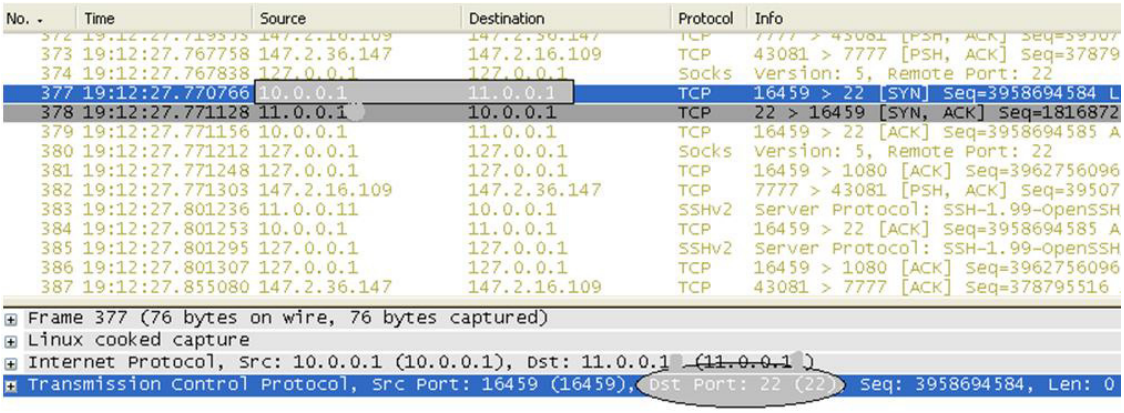
Once Socks authentication has been validated between the socks client and server, the socks payload (the ssh application data) can then by proxied to the remote host.

Figure 1-5 *Proxying the Socks Payload to the Remote Host*



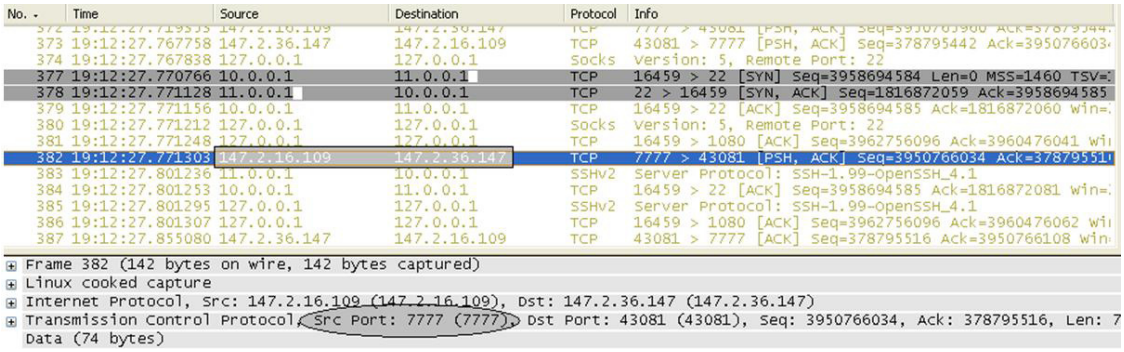
Packet 374 shows the data passed to the Socks server from the stunnel server. This is the SSH client request to the remote SSH server at 11.0.0.1 on TCP port 22. Note that this request is sent via the loopback interface to the SOCKS server on TCP port 1080.

Figure 1-6 *Packet 374: Data Passed to the Socks Server from the Stunnel Server*



Packet 377 now shows the TCP connect request at the application layer (triggered by packet 374) - visible through a TCP SYN from 10.0.0.1 (private interface of SSLVPN server) to 11.0.0. Because it is proxied, all outgoing requests to application servers on the private network will have a source IP address in the outgoing requests of 10.0.0.1. This is very different from the Enterprise mode client, which we will describe later.

Figure 1-7 *Packet Data Transmission*



When the response comes back from the SSH server (packet 378), we need to reverse the process before sending it back to the client. We need to pass it to the Socks application first (packet 380); then the Socks server builds the Socks data and passes it to the Stunnel server. The stunnel server encrypts the data and builds the response to send back to the SSLVPN client. This is shown in packet 382 above where the SSLVPN server (147.2.16.109) sends the tunneled data back to the SSLVPN client at 147.2.36.147.

Communication continues in this mode until the application client or server terminates the connection. If the application server terminates the connection via a TCP FIN, a corresponding Socks close request will be issued from the SSLVPN server to the client. This allows the TCP session on the client for this application session to be closed. If the application client terminates the request, the Socks close request will be sent to the Socks server side, so that the back-end application server is eventually notified of the close request. Note that this only terminates the session at the application layer – the SSLVPN client connection to the server still remains.

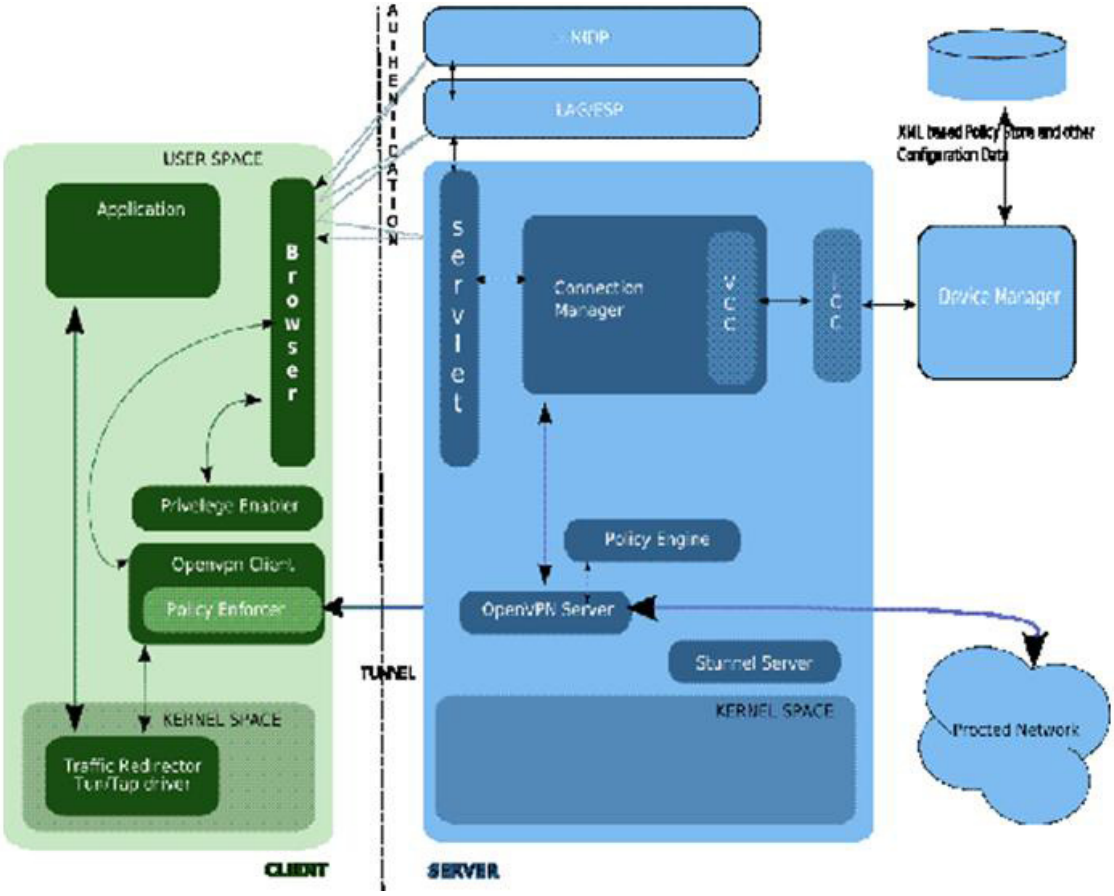
1.4 Enterprise Mode - Overall Architecture

The Enterprise, or OpenVPN mode of operation is based on the open source project at http://openvpn.net/. It is targeted for enterprise users. A high degree of user experience is achieved through this mode of access. In this mode, the user must either have administrator privileges in the machine, or an administrator privileged service needs to accepted when connecting to the SSLVPN server from a non-administrator privileges account. It also works at the IP layer, versus the Kiosk mode application layer, and routing becomes a key issue as we will see later.

- Section 1.4.1, “SSLVPN Enterprise Mode - Server-side Components,” on page 22
- Section 1.4.2, “SSLVPN Enterprise Mode - Client-side Components,” on page 24
- Section 1.4.3, “Enterprise Mode Authentication Flow,” on page 25
- Section 1.4.4, “Enterprise Mode Data Transfer Flow,” on page 26

The diagram below shows the components associated with the Enterprise Mode.

Figure 1-8 *Enterprise Mode Components*



1.4.1 SSLVPN Enterprise Mode - Server-side Components

Servlet: The SSLVPN servlet component can be run on any tomcat or servlet engine, and it need not be installed on the actual SSLVPN server itself. If it is not installed on the SSLVPN server, administrators must modify the config.txt file in the `/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/` directory. See (Configuring Load Balancing Through Servlets' under http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b6820mb.html) . This servlet package name is novl-sslvpn-servlet-3.* (* depends on version.) For the most part includes the `/var/opt/novell/tomcat5/webapps/sslvpn/*` files required by the servlet environment. The servlet receives the authenticated users sessions specific information from the Access Gateway. The goal of the servlet is to:

- Handle incoming HTTP requests from the Access Gateway destined for the SSLVPN login (/sslvpn/login) page.
- Run an individual communication channel with the applet for the direct control of the client session, making sure that the session is open and valid, or closed and cleared.
- Send/receive control messages to/from the SSLVPN connection manager. For example, this would include sending the user credentials, sending roles to the connection manager components, and processing the traffic policies coming back for that user.

Connection Manager: This is a TCP-based application running on a SLES server that listens on TCP port 2010 and communicates with the above servlet. This component, as well as the others below, are all part of the novl-sslvpn-3.* (* depends on version). The connection manager service is in /opt/novell/sslvpn/bin/connman. Its main functions include the following:

1. Managing a TCP socket to communicate with:
   - Admin Console, to synchronize the configuration changes
   - OpenVPN Server, pushing changes out
   - Monitoring and Auditing module, for interfacing into the NSure Auditing system

   NOTE: In Enterprise mode, the Connection Manager communicates with OpenVPN using the TCP socket. The port number is dynamically chosen and supplied to OpenVPN through its configuration file. In OpenVPN this is known as the management port.
2. Dynamic connection management such as:
   - Pulling out the policies from configuration database for a particular identity.
   - Communicating the change in data for OpenVPN server.

Policy Engine: As with the Kiosk mode solution, there is a policy enforcer component at the server as well as on the client. Given a specific request passed to it by the OpenVPN server, this component checks against the policies saved in the policy.txt file at `/etc/opt/novell/sslvpn` from policy store (obtained via the Connection Manager). Depending on whether a match is found, the traffic is either allowed or denied.

Traffic Redirector: The component sits at the kernel level as a network driver. The drivers used here are tun/tap drivers. Tun/Tap drivers are already installed on Linux systems, whereas by default the drivers for Windows system are delivered during the initial connection from the SSLVPN server that includes binaries. The Tun driver simply forwards traffic from stack to a userspace client (openvpn), and the openvpn server does the actual encryption/decryption service. Although both Tun and Tap drivers exist, Access Manager uses the Tun interface with no option to use Tap. The Tun mode uses a routing method, whereas the Tap mode uses bridging. The advantages of the routing mode include:

- Efficiency and scalability (scales well with more devices added)
- Better tuning of MTU for efficiency (very important when working with disparate networking topologies).

The disadvantage is that routes must be set up linking each subnet.

OpenVPN Server: This component is responsible for encrypting and tunneling data destined for one of the SSLVPN protected networks, and it is done at the network stack level. This component is only used for enterprise mode access, where the user needs to have a root privilege or the user system is already deployed with a thin service (Install Enabler). If a connected user has root privileges, the Enterprise mode is performed automatically; for users that do not have root privileges, the option to use Enterprise mode still exists through the 'Priveleged enabler' client component (see below).

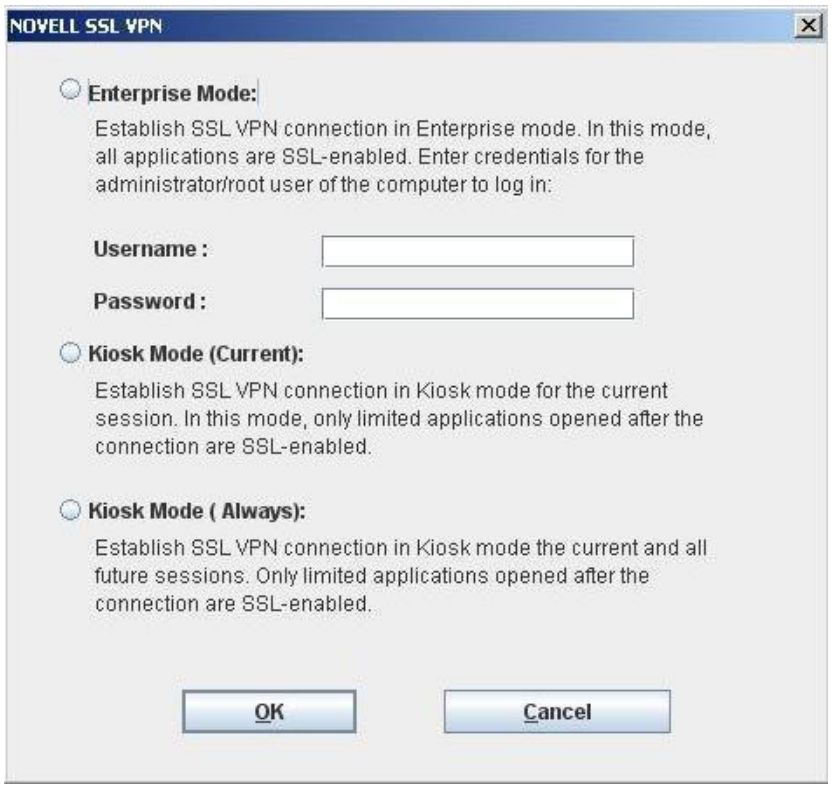
VCC/JCC: This is the protocol used to interface into the Access Manager configuration store. All changes to the configuration in the DeviceManager are synchronized with the SSLVPN server components via the Connection Manager.

1.4.2 SSLVPN Enterprise Mode - Client-side Components

Browser: The browser is initially required to contact the SSLVPN servlet via the Access Gateway. Once connected, keep-alive probes are continuously sent from the browser to the SSLVPN servlet to make sure that the existing session remains valid.

Privilege Enabler: This component is used to bypass the normal user limitations for Enterprise mode clients. When a non-privileged user connects to the SSLVPN server for the first time, that user is prompted for administrator credentials to provide the user the option of using Enterprise mode (see below). Administrator rights are required because the OpenVPN stack tunneling the data is required to redirect traffic at the network level. This service handles dynamic OpenVPN client launching and other privileged operations, which requires root privileges.

Figure 1-9 *SSL VPN Admin/Root Privileges*



OpenVPN Client: The OpenVPN client is a client daemon that associates itself to a Tun device and manages it. It is the primary component necessary for implementing SSL tunneling in enterprise mode access. When policies dictate that the traffic must be sent through the tunnel, the OpenVPN client sends the encrypted data out the Tap interface to go out the wire.

Policy Enforcer: When the OpevVPN client intercepts the application level request, it checks with the policy enforcer to determine whether the request needs to out out through the SSLVPN tunnel. This component checks the policies associated with this authentication and checks whether the outgoing request conforms to the policies allowed for that user. Depending on the response, it allows or denies them.

Traffic Redirector: In case of enterprise mode access, the traffic redirector sits at the kernel level as a network driver. The drivers used here are Tun/Tap drivers. Tun/Tap drivers are already installed on Linux systems, whereas the drivers for Windows systems are delivered from the SSLVPN server via the binary download. The Tun driver forwards traffic from the stack to a userspace client (OpenVPN), and this OpenVPN client does the actual encryption/decryption of application-level data.

1.4.3 Enterprise Mode Authentication Flow

The Enterprise mode authentication flow is based on the assumption that you are authenticated and have accesses to SSLVPN login page .Both Kiosk and Enterprise mode flow are almost same till step 7 and when the applet starts running, the following sequence of events start occuring in Enterprise mode from Step 8 onwards.

1. Proxy sends a request to the SSLVPN servlet (cookie and authenticated identity information are passed to the Servlet through this message).
2. The Servlet informs Connection Manager of a successful connection and awaits the user policies and client binaries.
3. At this time, Connection Manager becomes aware that a user has been successfully authenticated for SSL VPN session by an external authenticating agent (Access Gateway). The info it gets from the servlet at this stage includes the following:
   - User identity
   - Cookie for the http session between authenticating agent and browser
   - Client/browser identity (IP address and port), which can also be the dynamic NAT's identity.
   - Time of connection.
4. The Connection Manager validates such a connection request and the does the following:
   - Checks for the duplication of connection from the same client machine.
   - Builds the policy list (traffic and cic) for this particular user.
   - Sends the policies back to the servlet.
5. The servlet, upon receiving the above information from the connection manager
   - Generates a web page with Active-X controls or a Java Client applet (depending on whether client browser is IE or not). It includes the user policies and client binaries as a self-extractable download. The client binaries depend on the platform the client is running on (Windows, Linux, MAC) and include such things as an openssl, socks, stunnel client. The files may be found under the `/var/opt/novell/tomcat5/webapps/sslvpn/` directory of SSLVPN server.
   - Sends a 200 OK HTTP response back to the browser via the Access Gateway proxy, with the contents of the above web page.
6. The Access Gateway proxy sends the response back to the browser.
7. The browser processes the response and runs the self- extractable image it downloaded. The Client components are installed and Java Applet or Active-X controls starts running. Assuming everything initializes correctly, the Socks client will try to communicate with the Socks server. As this is a secure path, stunnel initiates the SSL negotiation.

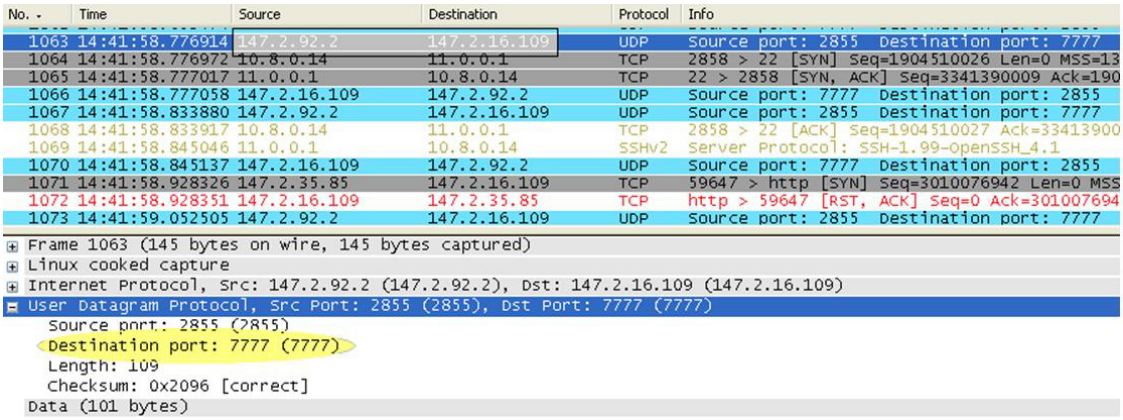
8. The applet evaluates the user privileges on the system being accessed. If the system has administrator privileges, or the user provides a valid user ID/password for an administrator account during the privileged enabler prompt, the applet starts the enterprise mode access.
9. The applet downloads all necessary components for enterprise mode access..
10. The applet launches the installation of the Tap driver if the driver has not already been found.
11. The applet launches the installation of a 'novell-sslvpn-service' service if such a service is not already found, or if the thin service is out of version compared to the one available in server.
12. The applet asks this novell-sslvpn-service service to launch the openvpn client binary by providing the necessary parameters. These could include the username and password received from the servlet through the browser, and a session token for the SSL negotiation.
13. The OpenVPN client then initiates an SSL negotiation for this user to the back end SSLVPN server external IP address. During this handshake, the openvpn client verifies the server certificate.
14. The OpenVPN server receives the username and password from the client and verifies it against the authentication store residing at the Connection Manager.
15. Assuming credentials are valid, the server sends a Success message to the client and then to applet.
16. The SSLVPN user interface displays a message that the connection is successful.

1.4.4 Enterprise Mode Data Transfer Flow

The Enterprise mode data transfer flow is when the application data sent to remote host. When data is sent from the client to the server, the application data is tunneled by the Enterprise mode client. Unlike the Kiosk mode client, the default transport layer protocol is UDP, as we can see below. In this example, a user on the workstation running the SSLVPN Enterprise mode client has tried to initiate an SSH session to the SSH server at 11.0.0.1, which is located on an internal network only accessible behind the SSLVPN private interface. The 147.2.92.2 is the IP address of the SSLVPN workstation where the client application is running.

Packet 163 shows the SSH data being tunneled from the workstation to the public IP address of the SSLVPN server (147.2.16.109). The default OpenVPN configuration parameters are used, so the data is being tunneled on UDP port 7777. OpenVPN uses UDP by default (benchmarks suggest that OpenVPN offers better performance when using UDP), but security policies within your organization may dictate that TCP is required (better control at the firewall with the stateful transport layer).

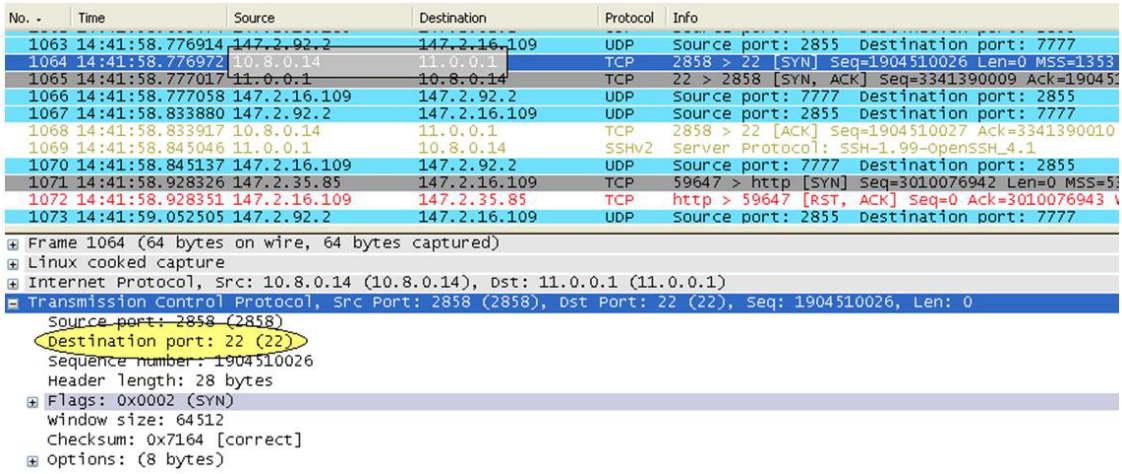
Figure 1-10 *SSH data tunneled from the workstation to the public IP address of the SSLVPN*



The OpenVPN server, listening out on UDP 7777 processes this incoming request, validates the SSL headers, and extracts the application data. Because it acts as a router, it forwards the original request to its destination.

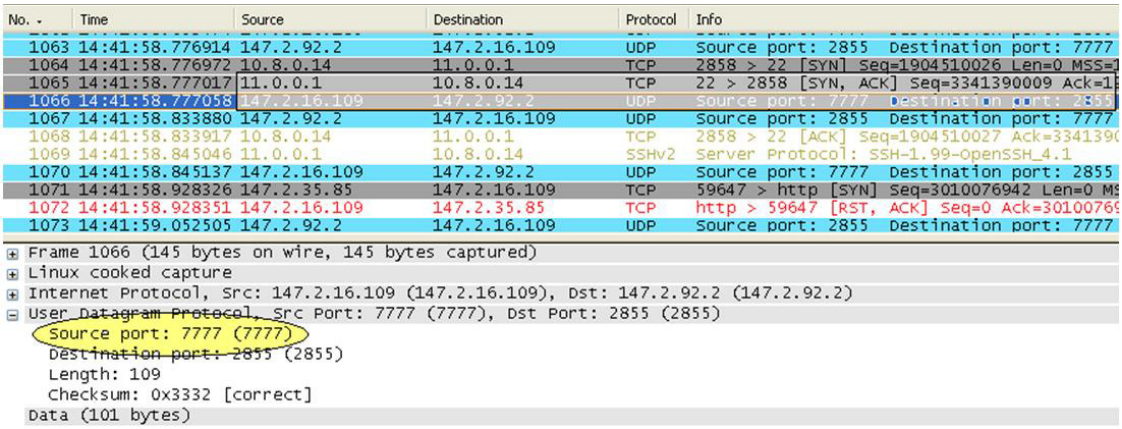
In packet 1064, we see that forwarding take place. The source IP address of the outgoing request is 10.8.0.14 - the OpenVPN IP address assigned by DHCP on the SSLVPN server. This is the IP address assigned to the Tap interface on the workstation. The destination IP address is that of the SSH server itself, on the private network (11.0.0.1). Because SSH is a TCP-based application, the request is now sent to TCP port 22 on the SSH server.

Figure 1-11 *Forwarding the Original Request to TCP Port 22 on the SSH Server*



Packet 1065 shows the TCP response to packet 1064. The key point here is that the response has come back to the SSLVPN client IP address via the SSLVPN server! If the routing table on the SSH server did not have an entry for the OpenVPN subnet (10.8.0.0/16) pointing to the SSLVPN server as the next hop, the response might a) never reach the SSLVPN client, or b) reach the SSLVPN client but be unencrypted, at which point the TCP segment would be dropped. It is imperative that all responses from the application server going to the SSLVPN client do so via the SSLVPN server

Figure 1-12 *SSLVPN Encrypted Response to the Client*

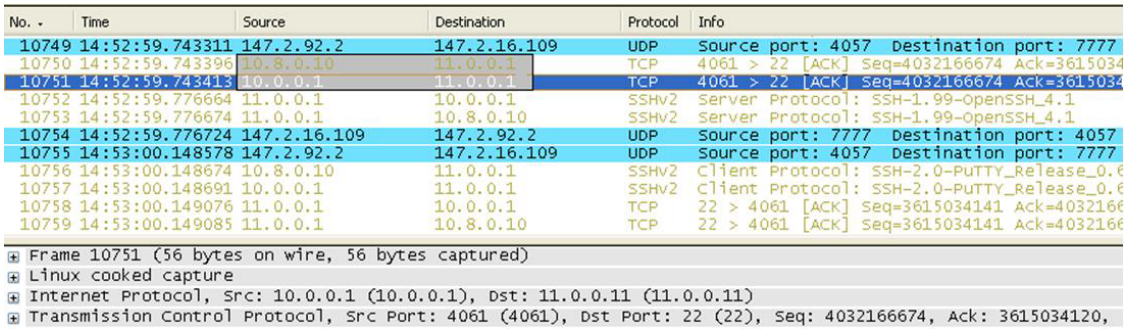


This example is not very realistic, as all remote hosts on the network need to know that the route back to the OpenVPN subnet address is done through the SSLVPN server private interface. A more practical example is shown below, where we use IPTABLES to rewrite the source IP address of the outgoing requests to the remote application servers. By executing the following on the SSLVPN server:

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/16 -j SNAT --to 10.0.0.1
```

All IP datagrams with a source IP address on the 10.8.0.0/16 subnet will get rewritten to 10.0.0.1. Because the 10.0.0.1 address is part of the internal network, all hosts should have a route back to this address.

Figure 1-13 *Re-writing 10.8.0.0/16 subnet datagrams to 10.0.0.1*



Looking at the same request this time around, we see that Packet 10749 shows the tunneled request from the SSLVPN client to the SSLVPN server external IP address.

Packet 10750 shows what we saw in earlier traces above - the OpenVPN decrypts the application request and now tries to forward to the SSH application server on 11.0.0.1. The source IP address is 10.8.0.10, and the IP address is assigned to the Tap interface.

Packet 10751 shows the result of the IPTABLES command above - the 10.8.0.10 source IP address has been rewritten to the private IP address of the SSLVPN server. For the SSH application server to respond to such a request, it will most likely not require any modifications to its routing table. This is the best approach to take.

Overview of SSL VPN

2

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 data cannot be intercepted and only authorized users have access to the network. Users can access SSL VPN services from any Web browser.

2.1 SSL VPN Features

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 computer, 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 SP2 SSL VPN User Guide*.

Support on 64-Bit Clients

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

High-Bandwidth and Low-Bandwidth Versions

Novell SSL VPN comes in high-bandwidth and low-bandwidth versions. The default low-bandwidth SSL VPN server is restricted to 249 simultaneous user connections and a transfer rate of 90 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 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 "Installing the Key for the High-Bandwidth SSLVPN" in the *Novell Access Manager 3.1 SP2 Installation Guide*.

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 Section 2.2, "Traditional and ESP-Enabled SSL VPNs," on page 32.

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 2.3.1, "Enterprise Mode," on page 35.

In Kiosk mode, only a limited set of applications are 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 2.3.2, "Kiosk Mode," on page 37.

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 select the mode in which the SSL VPN connection is made. For more information on how to do this, see Chapter 5, "Configuring How Users Connect to SSL VPN," on page 75. 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.

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 9.1, "Customizing the SSL VPN User Interface," on page 119.

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 Chapter 6, "Clustering the High-Bandwidth SSL VPN Servers," on page 87.

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 that are assigned. For more information on configuring end-point security, see Chapter 4, "Configuring End-Point Security and Access Policies for SSL VPN," on page 55.

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 "Ordering Traffic Policies" on page 67.

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 "Exporting and Importing Traffic Policies" on page 68

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 You can manually copy files to this folder, including files that you create or files that you download from your corporate network. This folder is automatically deleted along with its contents when you logs out of the SSL VPN connection. This is a very useful feature if you are browsing from an Internet connection and you do not want any sensitive information to reach other persons. For more information on the sandbox feature of SSL VPN, see "Using the Sandbox Feature" in the *Novell Access Manager 3.1 SP2 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 5.2.5, “Configuring a Custom Login Policy for SSL VPN,” on page 79.

2.2 Traditional and ESP-Enabled SSL VPNs

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.

2.2.1 ESP-Enabled Novell SSL VPN

In an 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:

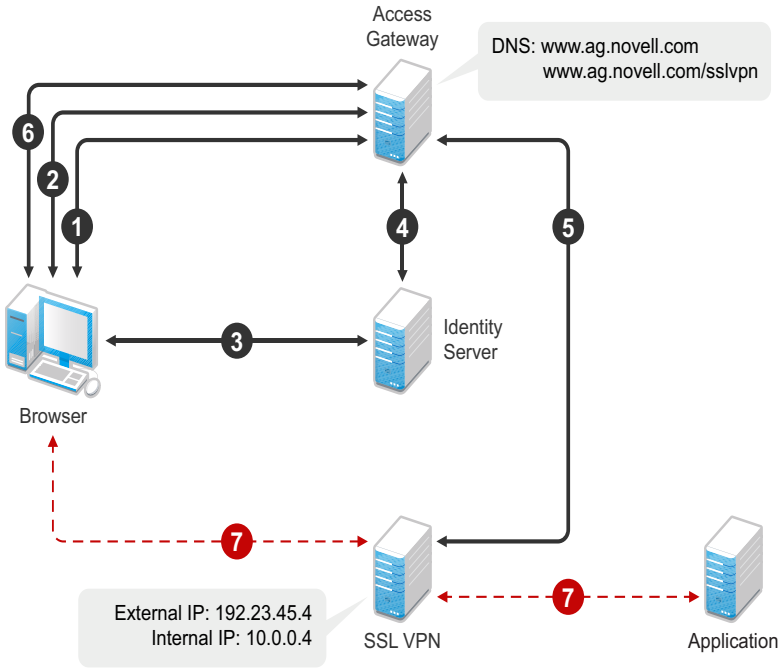
   `https://<www.sslvpn.novell.com>/sslvpn/login`

   <*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 Section 4.1, “Configuring Policies to Check the Integrity of the Client Machine,” on page 56.
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.

2.2.2 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>:8443/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 4.1, "Configuring Policies to Check the Integrity of the Client Machine," on page 56.

7. One of the following actions takes place, depending on the mode of the 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. The browser stays 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.

2.2.3 High-Bandwidth and Low-Bandwidth SSL VPNs

Novell SSL VPN comes in high-bandwidth 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 90 Mbits per second because of export restrictions.

High-Bandwidth Version: The high-bandwidth version does not have the connection and performance restrictions. It is 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 and 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 "Installing the Key for the High-Bandwidth SSLVPN" in the *Novell Access Manager 3.1 SP2 Installation Guide*.

2.3 SSL VPN Client Modes

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 users who have the administrator right in a Windows workstation or a `root` user privilege on Linux or Macintosh workstations. If a 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 the Access Manager 3.1 Support Pack 1 SSLVPN integration testing report (http://www.novell.com/support/viewContent.do?externalId=7004342&sliceId=1).

- Section 2.3.1, “Enterprise Mode,” on page 35
- Section 2.3.2, “Kiosk Mode,” on page 37

2.3.1 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 5.2.1, “Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode,” on page 76.

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

- “Prerequisites” on page 35
- “User Scenarios” on page 35

Prerequisites

A user can access SSL VPN in Enterprise mode if any one of the following prererequisites is in place:

- The user is an administrator or a `root` user of the machine, or a Super user or an Administrator user in Windows Vista user.
- The user is 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.

User Scenarios

Depending on which prerequisites are in place, users have different login scenarios.

- “Scenario 1: The User Is the Admin or Root User of the Machine” on page 36

- "Scenario 2: The User Is the Non-Admin or Non-Root User of Machine and Knows the Admin or Root Credentials" on page 36
- "Scenario 3: The User Is a Non-Admin or Non-Root User, but the Client Components Are Preinstalled on the Machine" on page 37

Scenario 1: The 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 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 5.2.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 76.

Scenario 2: The 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 2-2 *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 SP2 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 Section 5.1, "Preinstalling the SSL VPN Client Components," on page 75. 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.

2.3.2 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 5.2.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 76.

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

Figure 2-3 *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 switch to SSL VPN in Enterprise mode in the next session. For more information, see "Switching from Kiosk Mode to Enterprise Mode" in the *Novell Access Manager 3.1 SP2 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 5.2.4, "Configuring SSL VPN to Download the Java Applet on Internet Explorer," on page 79.

Basic Configuration for SSL VPN 3

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 "Installing the SSL VPN Server" in the *Novell Access Manager 3.1 SP2 Installation Guide*.
- Install the Linux Access Gateway, if you want to accelerate SSL VPN by using the Linux Access Gateway. For more information, see "Installing the Linux Access Gateway Appliance" in the *Novell Access Manager 3.1 SP2 Installation Guide*.
- Log in 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 SP2 Installation Guide*.
- Create an Identity Server configuration. For more information, see "Configuring an Identity Server" in the *Novell Access Manager 3.1 SP2 Identity Server Guide*.
- If you have upgraded from SSL VPN 3.0 to SSL VPN 3.1, update the SSL VPN servers before you proceed with any other configurations. For more information, see "Updating Configuration Changes to the Upgraded Server" in the *Novell Access Manager 3.1 SP2 Installation Guide*.

This section has the following information:

3.1 Configuring Authentication for the ESP-Enabled Novell SSL VPN

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.

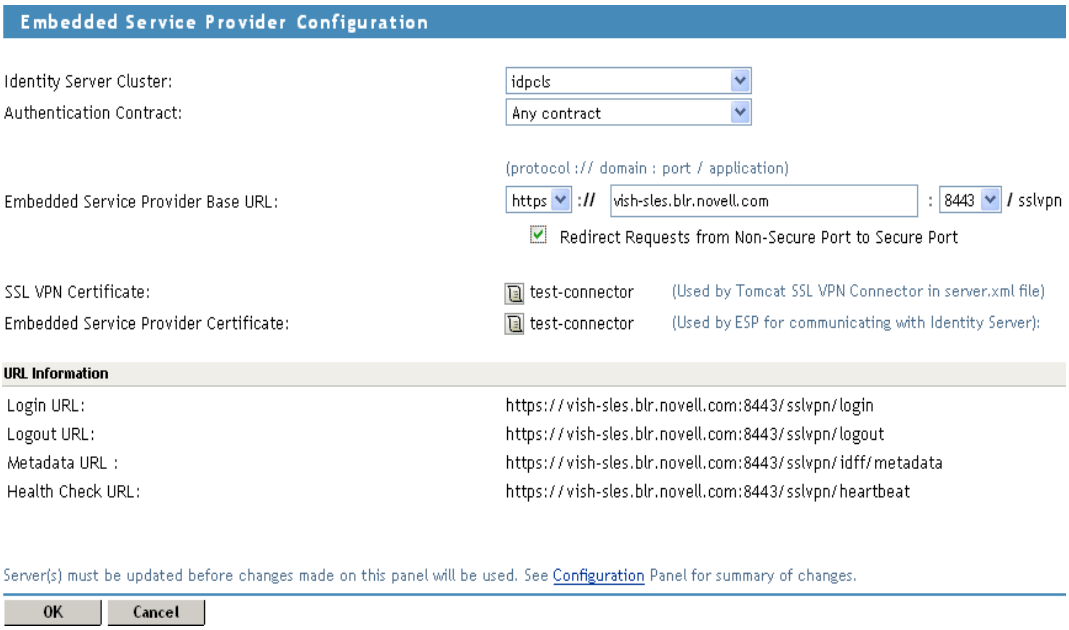
NOTE: If you have installed the Traditional SSL VPN, refer to Section 3.2, "Accelerating the Traditional Novell SSL VPN," on page 41.

---

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.



3 Fill in the following fields:

Identity Server Cluster: Specifies the Identity Server cluster that you want the SSL VPN 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, this option allows any contract defined for the Identity Server to be valid, or if the user has not authenticated, it 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 80 or 8080 for HTTP or 443 or 8443 for HTTPS. If you want to use port 80 or 433, select the port here, then select the *Redirect Requests from Non-Secure Port to Secure Port* option. Selecting 80 for HTTP and 443 for HTTPS implies that the port needs to be translated.

- **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.This certificate is used when SSL VPN communicates with the SSL VPN server.

You can click the icon to select the default test-connector certificate created for SSL VPN. The subject name of this certificate should match the DNS name of the SSL VPN server. For more information, see the Section 3.6, “Configuring Certificate Settings,” on page 53.

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. Make sure that the subject name of this certificate matches the DNS name of the SSL VPN server. For more information, see Section 3.6, “Configuring Certificate Settings,” on page 53.

NOTE: Before you proceed with the configuration, verify if SSL VPN certificates are imported into the trust store. To verify, log in to the Administration Console, select *Security* > *Trusted Roots*, click the down arrow for the trusted root that you are interested in. Make sure that two SSL VPN trust stores are displayed. If they do not exist, you must manually push the certificates to the trust store.

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 Section 3.3, “Configuring the IP Address, Port, and Network Address Translation (NAT),” on page 45, if you have not already configured the SSL VPN server details.

3.2 Accelerating the Traditional Novell SSL VPN

NOTE: If you have installed the ESP-enabled Novell SSL VPN, skip this section and make sure that you have completed Section 3.1, “Configuring Authentication for the ESP-Enabled Novell SSL VPN,” on page 39.

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

3.2.1 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*.

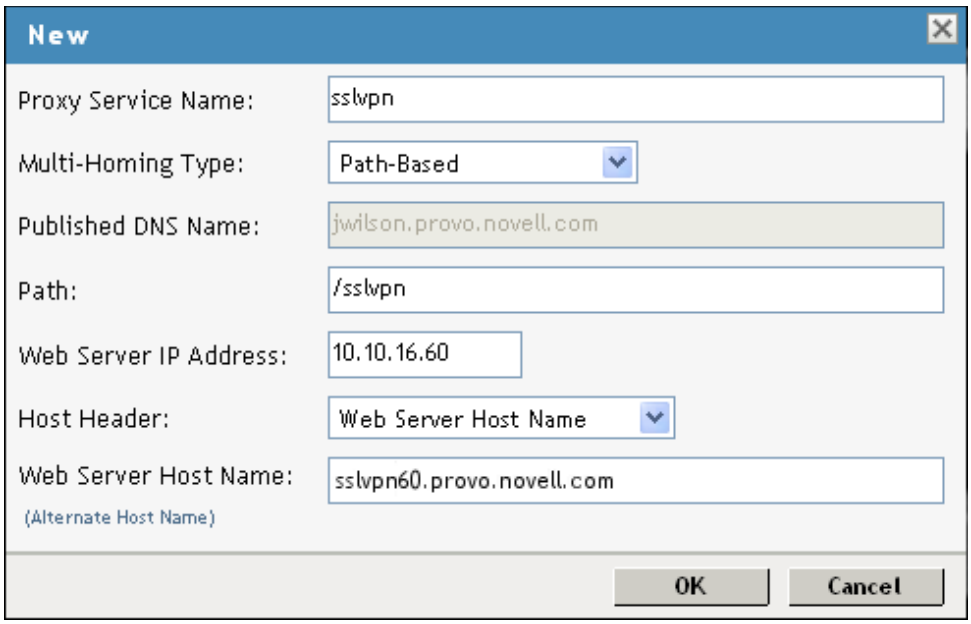
3.2.2 Injecting the SSL VPN Header

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 SP2 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.

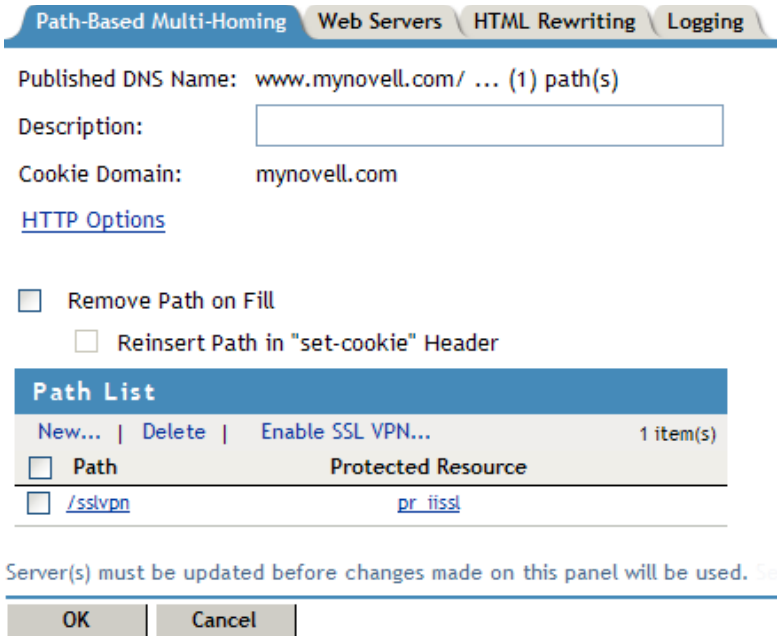
NOTE: If the SSL VPN server and the Linux Access Gateway are installed on the same machine, you must configure the loopback IP address 127.0.0.1 as the Web Server IP address. For more information on configuring the loopback IP address, see "Configuration Changes to the SSL VPN Server Installed with the Access Gateway Appliance" in the *Novell Access Manager 3.1 SP2 Installation Guide*.

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.

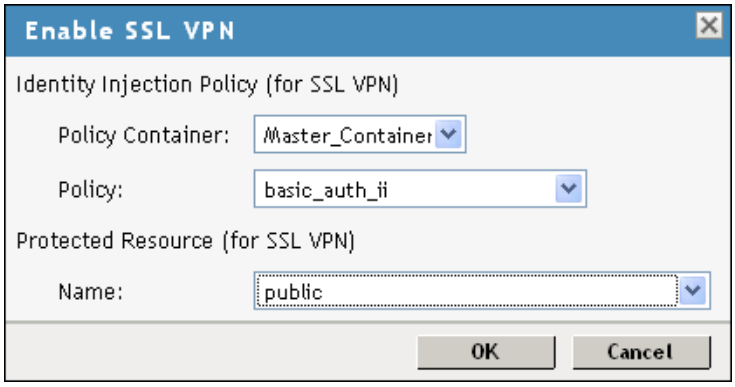
4 Click *OK*.

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*.



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 SP2 Policy 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 3.2.1, "Configuring the Default Identity Injection Policy," on page 42.

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.

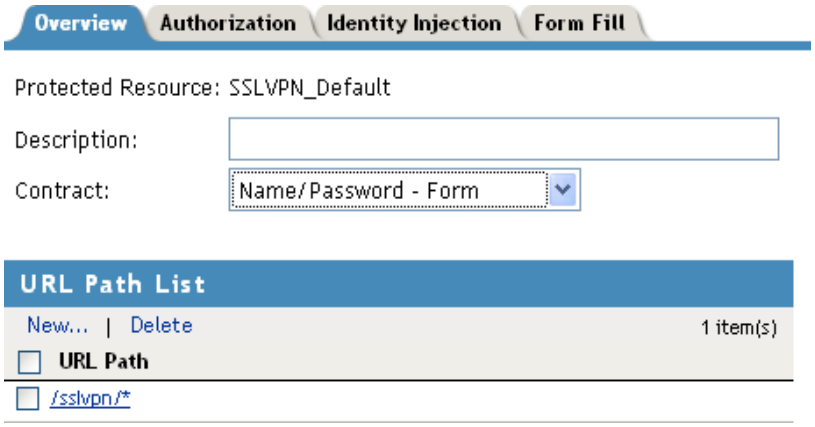
13 Select the *Protected Resources* tab.

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

15 Select an authentication contract from the *Authentication Procedure* drop-down list.

The user is assigned the timeout value of the contract used for authentication, and not the default timeout value.

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) If you have not already configured the SSL VPN server details, proceed with Section 3.3, “Configuring the IP Address, Port, and Network Address Translation (NAT),” on page 45.

3.3 Configuring the IP Address, Port, and Network Address Translation (NAT)

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.

- Section 3.3.1, “Configuring the SSL VPN Gateway behind NAT or L4,” on page 46
- Section 3.3.2, “Configuring the SSL VPN Gateway without NAT or an L4 Switch,” on page 48

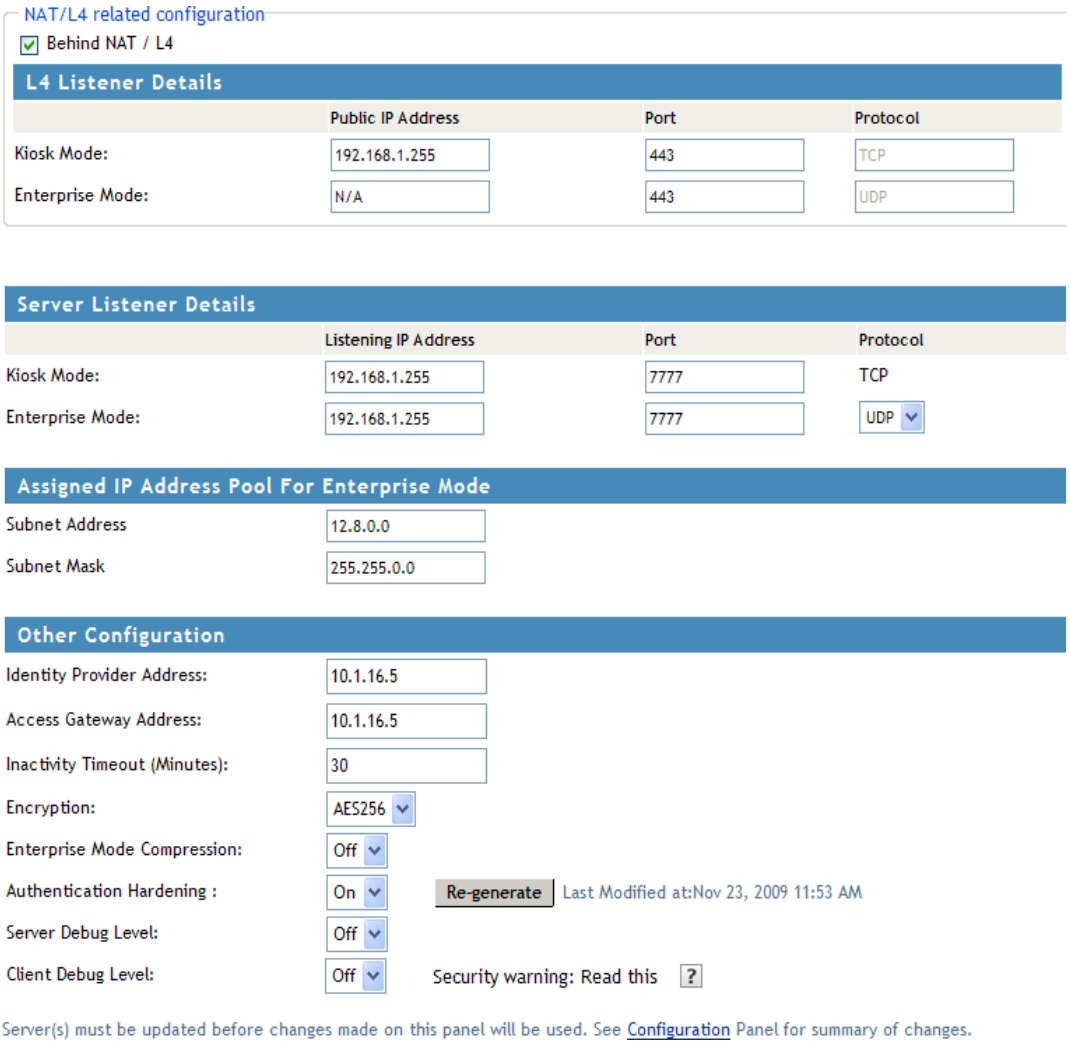
3.3.1 Configuring the SSL VPN Gateway behind NAT or L4

To configure SSL VPN behind NAT or by using an L4 switch:

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.



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 switch or a behind NAT.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN server is behind an L4 switch or behind 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 switch or behind 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 switch or behind 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 Section 3.4, “Configuring Route and Source NAT for Enterprise Mode,” on page 50.

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.

NOTE: IP pooling is not applicable for Kiosk mode. In Enterprise mode, if you have only one SSL VPN server installed, then you can configure only one IP pool. However, if you have multiple SSL VPN servers in a cluster, then each SSL VPN server must have separately defined IP pools.

---

6 Specify the other configuration as follows:

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

Identity Provider Address: Specify the IP addresses or the DNS name of the Identity Server if you are configuring SSL VPN for the full tunneling mode. For more information on full tunneling, see Section 4.4, “Configuring Full Tunneling,” on page 68.

Access Gateway Address: Specify the IP address or DNS name of the Access Gateway if your server is accelerated by the Access Gateway and if you are configuring SSL VPN for the full tunneling mode. This field is not present if you have installed the ESP-enabled SSL VPN. For more information on full tunneling, see Section 4.4, “Configuring Full Tunneling,” on page 68.

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.

Authentication Hardenings: This option is applicable to Enterprise mode clients only. When this option is enabled, it provides protection against active attacks by using a keyed Hash Message Authentication Code (HMAC) cryptographic hash such as SHA1 to sign and verify packets. When this option is enabled, a packet is examined by a stateless filter and dropped if the HMAC signature does not match.

To enable *Authentication Hardening,* select *On*. To manually regenerate the key click *Re-generate*. This option uses random number generation to regenerate the key.

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.This option is set to *Off* by default.

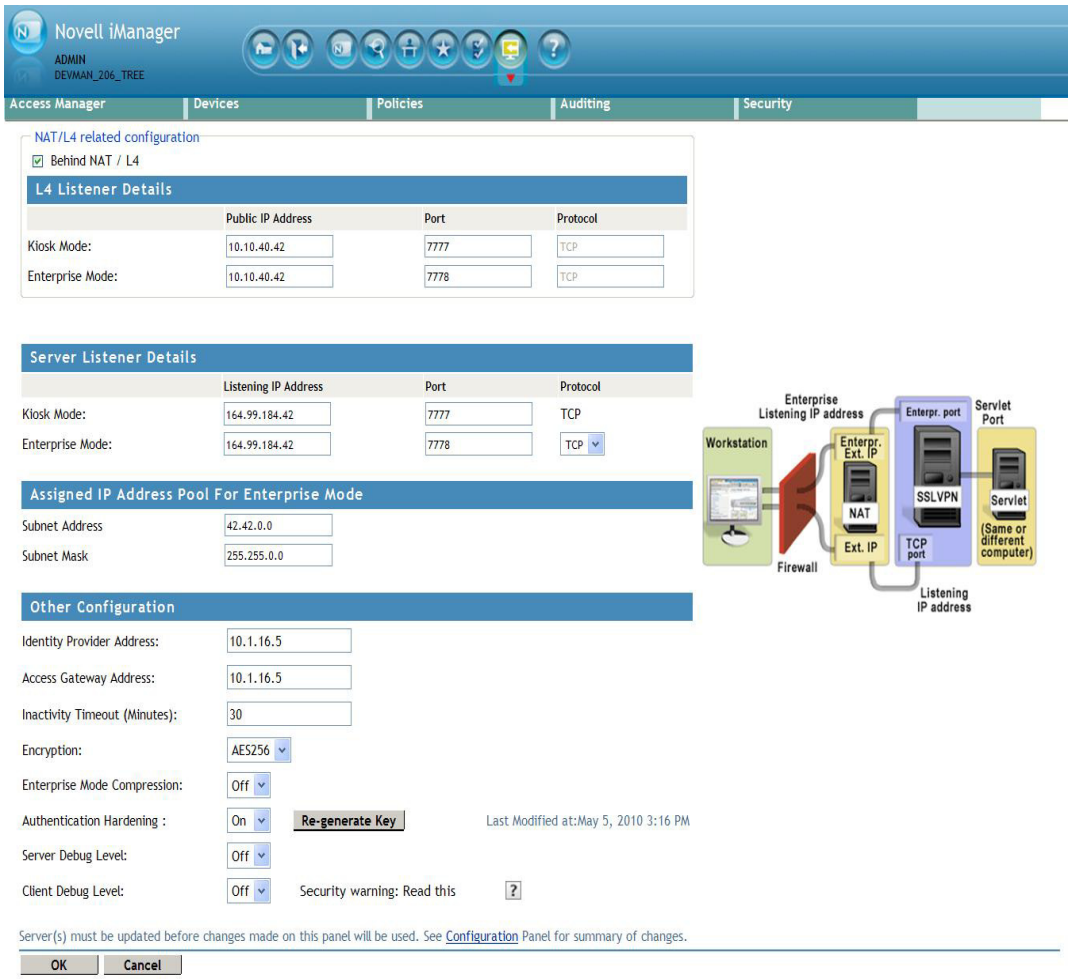
7 To save your modifications, click *OK,* then click *Update* on the Configuration page.

3.3.2 Configuring the SSL VPN Gateway without NAT or an L4 Switch

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.



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 switch or behind 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 switch or behind 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 Section 3.4, “Configuring Route and Source NAT for Enterprise Mode,” on page 50.

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.

Identity Provider Address: Specify the IP addresses or the DNS name of the Identity Server if you are configuring SSL VPN for the full tunneling mode. For more information on full tunneling, see Section 4.4, "Configuring Full Tunneling," on page 68.

Access Gateway Address: Specify the IP address or DNS name of the Access Gateway if your server is accelerated by the Access Gateway and if you are configuring SSL VPN for the full tunneling mode. This field is not present if you have installed the ESP-enabled SSL VPN. For more information on full tunneling, see Section 4.4, "Configuring Full Tunneling," on page 68.

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.

Authentication Hardening: This option is applicable to Enterprise mode clients only. When this option is enabled, it provides protection against active attacks, by using a keyed Hash Message Authentication Code (HMAC) cryptographic hash such as SHA1 to sign and verify packets. When this option is enabled, a packet is examined by a stateless filter and dropped if the HMAC signature does not match.

To enable *Authentication Hardening,* select *On*. To manually regenerate the key click *Re-generate Key*. This option uses random number generation to regenerate the key

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. This option is set to *Off* by default.

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

3.4 Configuring Route and Source NAT for Enterprise Mode

In Enterprise mode, SSL VPN assigns IP addresses to each client from the subnet specified in the configuration. 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.

For more information on configuring the IP address, see Section 3.3, "Configuring the IP Address, Port, and Network Address Translation (NAT)," on page 45.

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:

- Section 3.4.1, “Configuring the OpenVPN Subnet in Routing Tables,” on page 51

3.4.1 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.

3.5 Configuring DNS Servers

The DNS servers configured in the SSL VPN server are pushed to the client during the connection. When a Linux or Windows client connects to the SSL VPN server, the existing DNS entry on the client is pushed as the secondary entry and the DNS entry configured on the SSL VPN server is pushed as the primary DNS entry.

However, on a Mac client, the DNS entry configured on the SSL VPN server acts as the secondary DNS. After the SSL VPN connection, name resolution is done through the DNS entry configured before the SSL VPN connection. However, when the primary DNS server is not available, the DNS entry configured by the SSL VPN server takes care of DNS resolution for the client.

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.

- Section 3.5.1, “Configuring DNS Servers for Enterprise Mode,” on page 51
- Section 3.5.2, “Configuring DNS Servers for Kiosk Mode,” on page 52

3.5.1 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.

3 To configure a DNS server, click *New* in the *DNS Server*s 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.

3.5.2 Configuring DNS Servers for Kiosk Mode

The DNS servers can be configured for Kiosk mode during installation or by using YaST after the installation. The configuration procedure depends 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 “Configuring DNS Servers for Enterprise Mode” on page 51.

- “Configuring DNS Servers during Installation” on page 52
- “Configuring DNS Servers after the Installation” on page 52

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 SP2 Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html).

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.

3.6 Configuring Certificate Settings

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

When SSL VPN server is installed, it creates a test-connector certificate with the default DNS name of the SSL VPN server. However, if you have changed the default DNS name of the SSL VPN server, then you must create a new certificate and replace the test-connector.

The following instructions assume that you have already created a certificate. For more information on creating certificates, see "Security and Certificate Management" in the *Novell Access Manager 3.1 SP2 Administration Console Guide*.

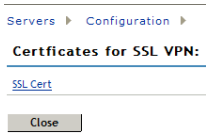
Before you proceed with the configuration, log in to the Administration Console, select *Security* > *Trusted Roots*, click the down arrow for the trusted root that you are interested in. Make sure that two SSL VPN trust stores are displayed. If they do not exist, you must manually push the certificates to the trust store.

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

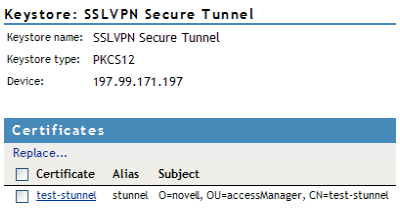
---

1 In the Administration Console, select *Devices* > *SSL VPN* > *Edit*.

2 Select *SSL VPN Certificates* from the *Security settings* section.



3 Click *SSL Cert*.



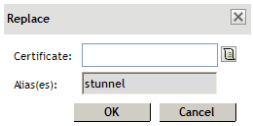
Certificates in the SSL VPN STunnel are used by SSL VPN services for encryption. This page contains the following information:

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

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

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

4 To replace the default certificate, click *Replace*.



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

4

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. 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.

SSL VPN also allows you to configure traffic policies to control access to resources based on the role of the client. You can then 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 "Configuring Applications for a Category" on page 57. If the client fails the integrity check, one of the following actions occurs:
   - If there is a traffic policy configured for that user's role and the security level is None, the SSL VPN connection is established with minimal access to that client.
   - If there is no traffic policy configured for that user's role and the security level is 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 4.2.1, "Client Security Levels," on page 63.
3. If the client adheres to the accepted security level, the SSL VPN connection is made and the secure tunnel is established between the SSL VPN client and server.
   - When the tunnel is up, if some changes are made to the client integrity check policy, the 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 4.3, "Configuring Traffic Policies," on page 64.

NOTE: All configurations done while the tunnel is up affect users who connect after the changes are applied. To apply the configuration changes to all users immediately, disconnect the active connections from the statistics page. For more information, see Section 7.4, "Disconnecting Active SSL VPN Connections," on page 104.

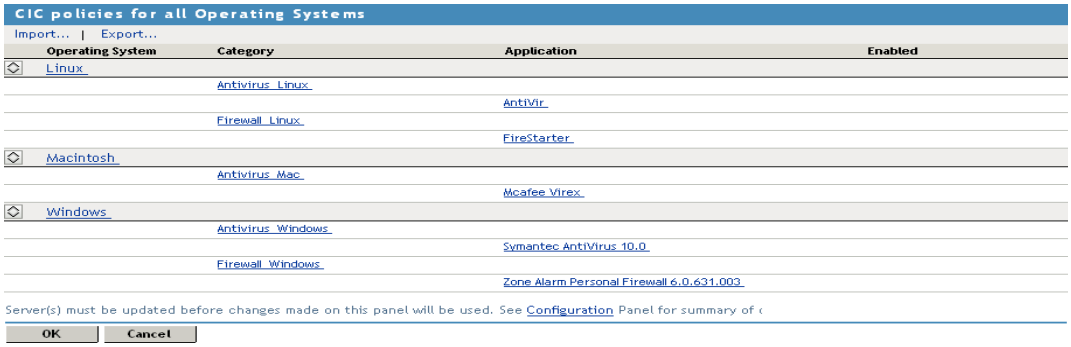
4.1 Configuring Policies to Check the Integrity of the Client Machine

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.

A category that you have configured can be deleted only if it is not assigned to any of the security levels.

4.1.1 Selecting the Operating System

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



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 "Configuring the Category" on page 57.

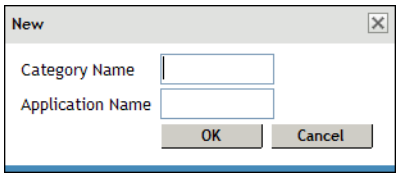
   For more information on exporting and importing client integrity check policies, see Section 4.1.5, "Exporting and Importing Client Integrity Check Policies," on page 62.

4.1.2 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.

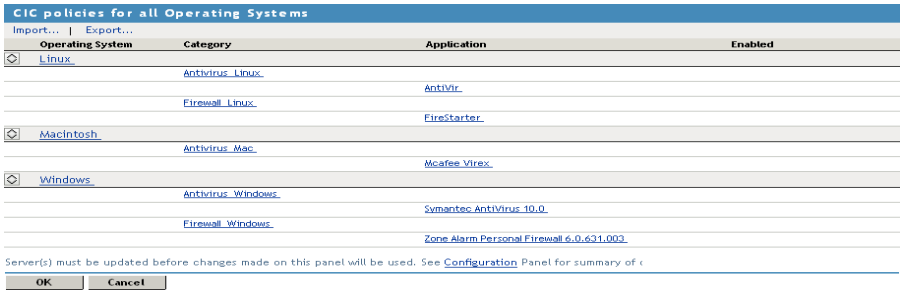
When multiple categories are configured for an operating system, if one of the enabled category does not exist on the client, the client integrity check fails.

1 To add a new category, click *New*.



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

3 Select the newly added 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*.

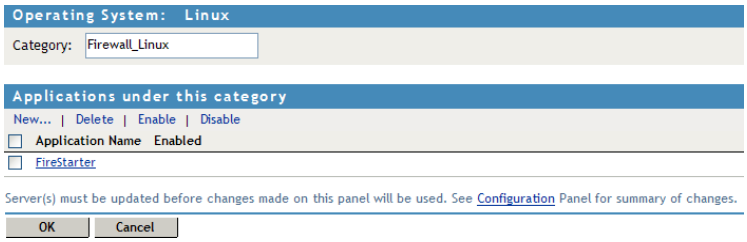
6 Click *OK* to save your modifications, then click *Update* on the Configuration page.

7 Continue with "Configuring Applications for a Category" on page 57.

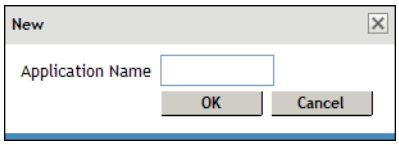
4.1.3 Configuring Applications for a Category

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. If at least one of the enabled application definition exists on the system, the client integrity check passes.

1 To configure or add applications to a category, click the category.



2 To add a new application, click *New*.



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

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

NOTE: To enable an application you must have already enabled the category that the application is part of.

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.

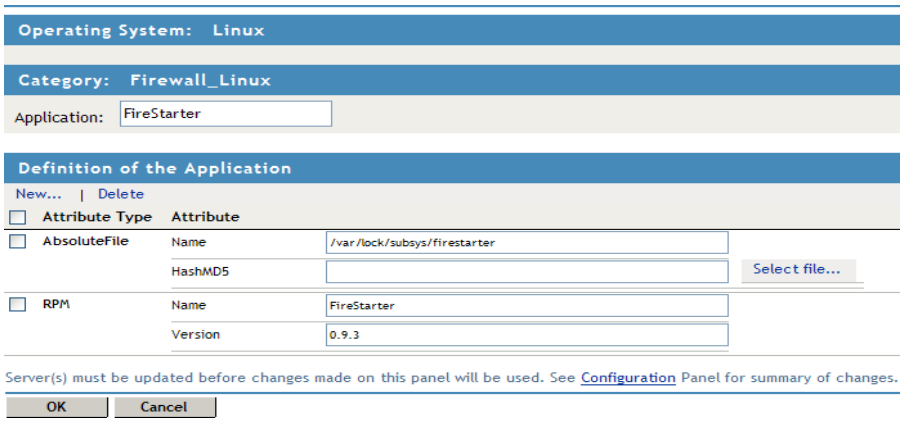
8 Continue with "Configuring Attributes for an Application" on page 58.

4.1.4 Configuring Attributes for an Application

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

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.



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 on the client machine. **Version:** Specify the version of the RPM that must be present on the client machine.
	Process	**Name:** Specify the name of the process that must be present on 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 on the client machine. **HashMD5:** Specify the MD5 checksum value of the absolute file. To calculate the MD5 checksum value of an absolute file located in your local system, click *Select File* to select the file. The MD5 checksum value of the selected file is displayed. To calculate the MD5 checksum value for an absolute file that is on another system, remotely connect to that system, calculate the MD5 value, then copy the value in the *HasMD5* field. **NOTE:** You can also copy the file from the remote system to the local system, then calculate the MD5 checksum by using the *Select File* option. However, this might change the MD5 value of the file during the process. If you want to use this method, then ensure that the file size and file contents did not change during the process.

Operating System	Attribute Type	Attribute Name
Macintosh	Package	**Name:** Specify the name of the software package that must be present on the client machine. **Version** Specify the version of the software package.
	Process	**Name:** Specify the name of the executable file that must be present on 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 on the client machine. **HashMD5:** Specify the MD5 checksum value of the absolute file. To calculate the MD5 checksum value of an absolute file located in your local system, click *Select File* to select the file. The MD5 checksum value of the selected file is displayed. To calculate the MD5 checksum value for an absolute file that is on another system, remotely connect to that system, calculate the MD5 value, then copy the value in the *HasMD5* field. **NOTE:** You can also copy the file from the remote system to the local system, then calculate the MD5 checksum by using the *Select File* option. However, this might change the MD5 value of the file during the process. If you want to use this method, then ensure that the file size and file contents did not change during the process.
Windows	Process	**Name:** Specify the name of the executable file that must be present on the client machine. **RegistryKeyName:** Specify the registry key name. When you add this name, make sure that you also specify a value for *RegistryKey Value*. **ValueName:** Specifies the value for RegistryKey configured. The data found in this key value should be the absolute path of the folder where the process file is present. **Version:** Specify the version of the software process that must be running in the client machine. **NOTE:** The version attribute specifies the Windows Explorer file version number.

Operating System	Attribute Type	Attribute Name
	RegistryKey	**Name:** Specify the name and absolute path of the registry key that must be present on 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 or REG_SZ can be a string value or, numeric or alphanumeric. 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`, a comparison operator of `=`, and a Value Data of `RegData`, the client integrity check process looks for the presence of `RegKey` with a value name `RegValue` = value data `RegData` on the client machine. If the registry is present with the specified values, the client passes the client integrity check. **NOTE:** Registry keys are not case sensitive, and they can contain either a single backslash (\) or double backslash (\\). For example: One of the registry key descriptions is HKEY_Local_Machine\\Software\\Symantec. It can also be written as HKEY_Local_Machine\Software\Symantec.
	Absolute File	**Name:** Specify the name and absolute path of the file that must be present on the client machine. **Version:** Specify the version of the absolute file that must be running on the client machine. **HashMD5:** Specify the MD5 checksum value of the absolute file. To calculate the MD5 checksum value of an absolute file located in your local system, click *Select File* to select the file. The MD5 checksum value of the selected file is displayed. To calculate the MD5 checksum value for an absolute file that is on another system, remotely connect to that system, calculate the MD5 value, then copy the value in the *HasMD5* field. **NOTE:** You can also copy the file from the remote system to the local system, then calculate the MD5 checksum by using the *Select File* option. However, this might change the MD5 value of the file during the process. If you want to use this method, then ensure that the file size and file contents did not change during the process.

Operating System	Attribute Type	Attribute Name
	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*.

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 4.2, “Configuring Client Security Levels,” on page 63.

4.1.5 Exporting and Importing Client Integrity Check Policies

You can export the client integrity check policy configuration into an XML file and import it back into the server.

You can modify the exported file without violating the schema format to include anew configuration. The new configuration is included when the file is imported.

- “Exporting Client Integrity Check Policies” on page 62
- “Importing Client Integrity Check Policies” on page 62

Exporting Client Integrity Check Policies

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

2 Click *Client Integrity Check Policies* in the Policies section. The Client Integrity Check Policies page is displayed.

3 Select the policies that you want to export, then click *Export*. This exports the configuration for all the platforms, categories, and applications.

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

5 Specify a location to save the XML file.

6 Click *OK* to save.

Importing Client Integrity Check Policies

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

2 Do one of the following:

- If you want to import the client integrity check policy configuration to an individual server, select the server, then click *Edit*.
- If you want to import the client integrity check policy configuration of a cluster, select the cluster, then click *Edit*.

3 Click *Client Integrity Check Policies* in the Policies section.

4 Click *Import*.

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

6 Click *OK*.

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

4.2 Configuring Client Security Levels

You can configure the 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.

4.2.1 Client Security Levels

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:

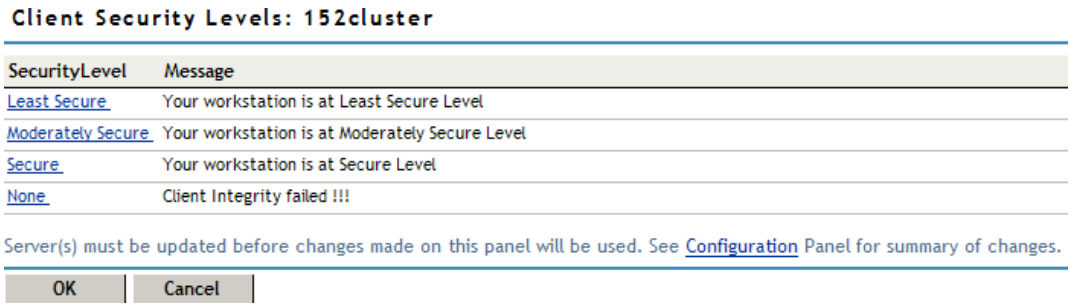
- If, during the client integrity check, a client is found to have a certain level of security, then all the policies under that level as well as the policies under the lower security levels are imposed on the client. For example, if the client passes the security level check as Moderately Secure, then 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.

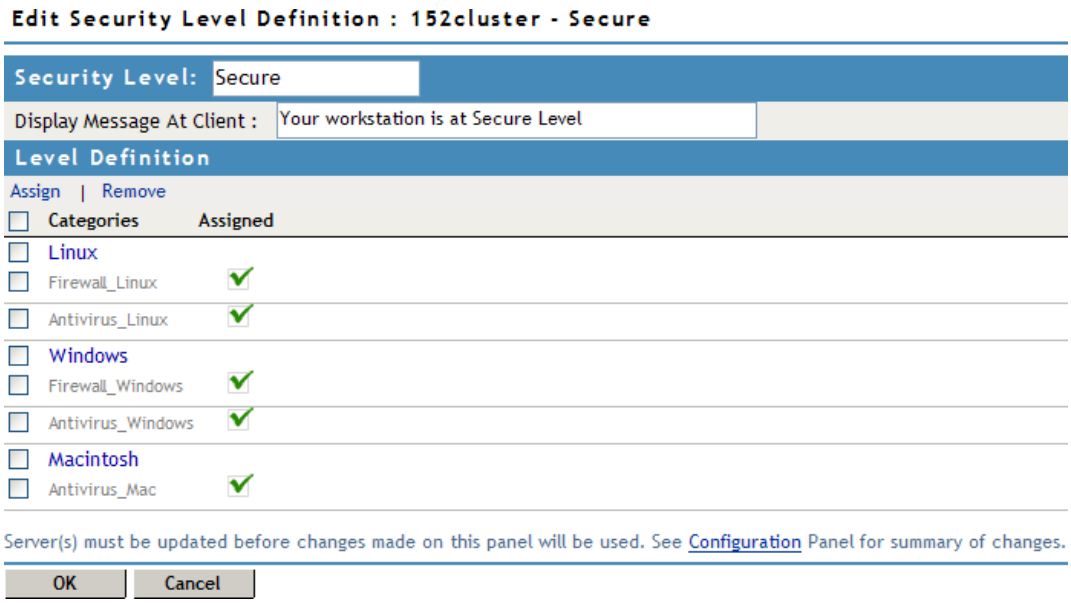
4.2.2 Configuring a Security Level

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.



3. Click a security level to configure it.



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 operating system, then click *Assign*.
5. To remove a category for a level, select the category, then click *Remove*.
6. Click *OK* to save your modifications, then click *Update* on the Configuration page.

4.3 Configuring Traffic Policies

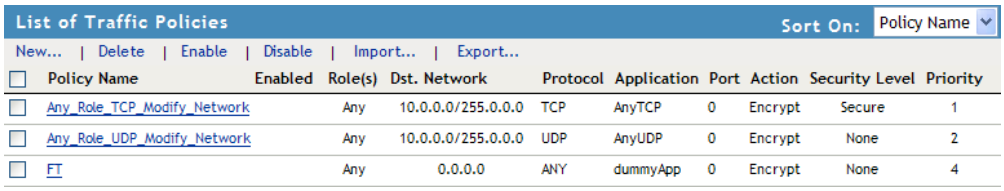
You can configure a maximum of 250 traffic rules per role, depending on the length of the policy name. If you have configured multiple traffic policies, the policies are prioritized based on the order of their creation.

The roles for a user are created in the Identity Server. These roles are displayed in the traffic policies page by default.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.

4.3.1 Configuring Policies

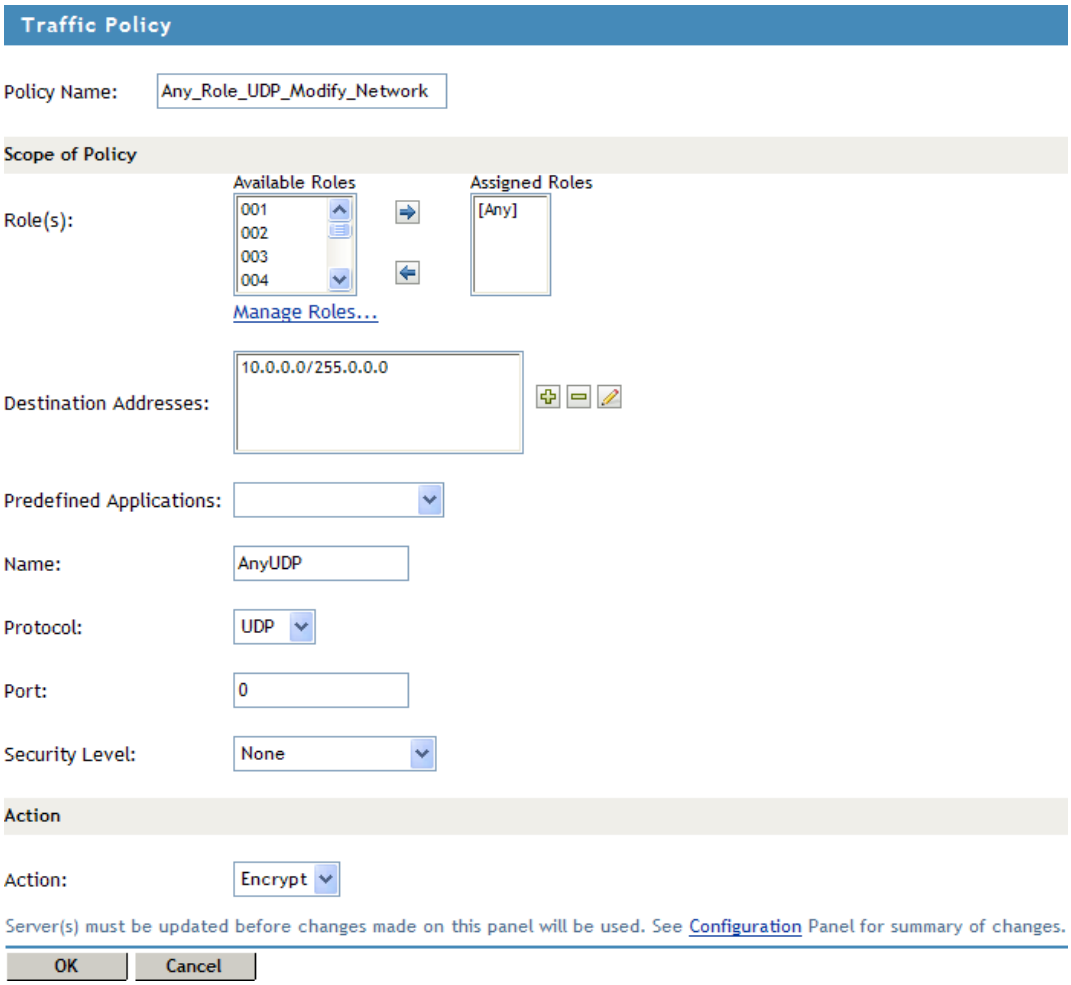
You can configure a different set of traffic policies for different roles as follows:

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



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. (Optional) To enable the full tunneling mode, select *Enabling Full Tunneling*.

   For more information, see Section 4.4, “Configuring Full Tunneling,” on page 68
6. Click the newly added traffic policy.

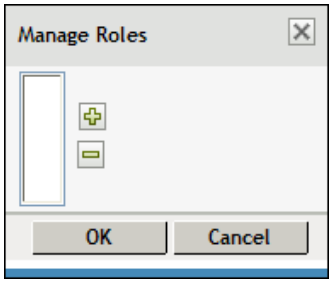


Fill in the following fields:

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 was 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 Addresses: Specify the destination IP address entries in any of the following formats:

- A single host IP address. For example, 192.168.1.1
- A range of IP addresses in the same subnet. For example, 192.168.1.1-192.168.1.10
- A combination of host address and network mask. For example, 192.168.1.0/255.255.255.0
- A full tunneling IP address 0.0.0.0.

NOTE: You can configure a traffic policy with a maximum of 20 IP address entries. However, in Enterprise Mode, the OpenVPN client can add a maximum of 100 routes.

To add an IP address, click the + icon. To delete an IP address, select the address that you want to delete, then click the - icon. You can also edit the existing IP address.

NOTE: If the traffic policy includes a host entry, you cannot change the subnet 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 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.

Specify 0 to allow all ports depending on the protocol.You can configure a maximum of 20 port entries for a traffic policy.

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 4.2, “Configuring Client Security Levels,” on page 63.

7 To delete a traffic policy, select the policy, then click *Delete*.

8 To enable a traffic policy, select the policy, then click *Enable*.

9 To disable a traffic policy, select the policy, then click *Disable*.

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

4.3.2 Ordering Traffic Policies

You can configure multiple traffic policies for a user’s role. These traffic policies can be sorted either based on their priority or alphabetically. Use the *Sort On* option in the traffic policies page to sort the traffic policies either based on the policy name or based on the priority of policies.

However, for a user, traffic policies are applied based on the order of the traffic policies. For example, the first traffic policy is applied to the user, followed by the second traffic policy, and so on. The rules set in the first traffic policy takes precedence over the next. For example, if you want to allow a user access to an application, and you place the policy as the third policy, the policy would work provided the first and second policy do not deny access to that particular application.

If you want to order the policies based on their priority, you can drag and drop the policies in the order that you want them to be placed. The *Sort On* option must be set to *Priority* in order to drag and drop the policies.

4.3.3 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.

4.4 Configuring Full Tunneling

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.

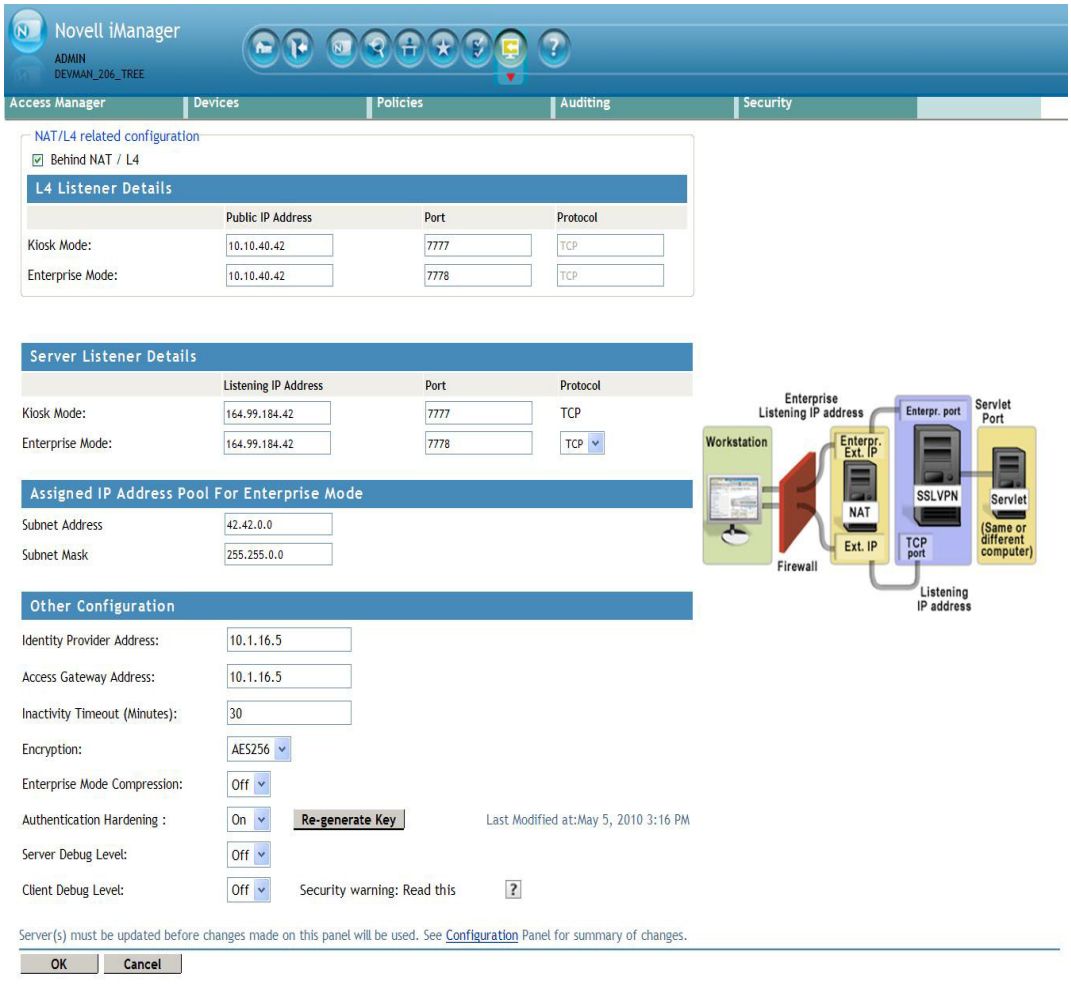
When you configure SSL VPN for full tunneling, all traffic to the protected network as well as the public network passes through the tunnel, thereby making the SSL VPN connection more secure. Any session management information between the client and the Identity server, Linux Access Gateway -- (for Traditional 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.

You must configure traffic 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 of the policy list and the full tunneling policy must be placed as the last policy.

For more information on Configuring Full Tunneling for SSL VPN, see (http://www.novell.com/communities/node/8699/configuring-full-tunneling-ssl-vpn)

4.4.1 Creating a Full Tunneling Policy

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Click *New* to create a new traffic policy.
3. Specify a name for the traffic policy.
4. Select *Enable Full Tunneling*.
5. Select *Encrypt* to allow the service in encrypted form or select *Deny* to deny services
6. Click *OK*.
7. Select *Gateway Configuration* from the *Basic Gateway Configuration* section.



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

4.4.2 Modifying Existing Traffic Policies for Full Tunneling

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

2 Click the traffic policy that you want to modify. The Edit Traffic Policy page is displayed.

3 Configure the following fields:

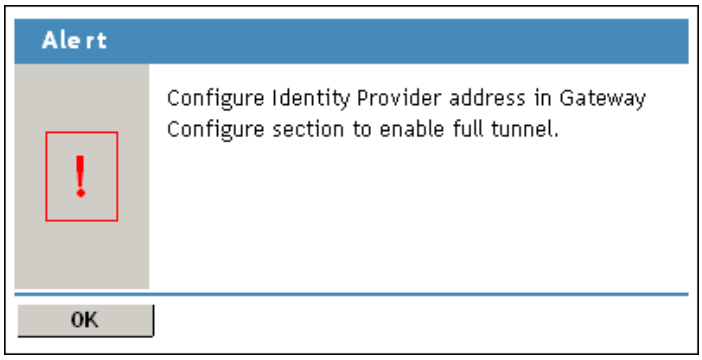
Destination Network: Specify 0.0.0.0 as the destination network IP address.

Action: Select *Encrypt* to allow the service in encrypted form or select *Deny* to deny services.

Leave the default values in the other fields unchanged.

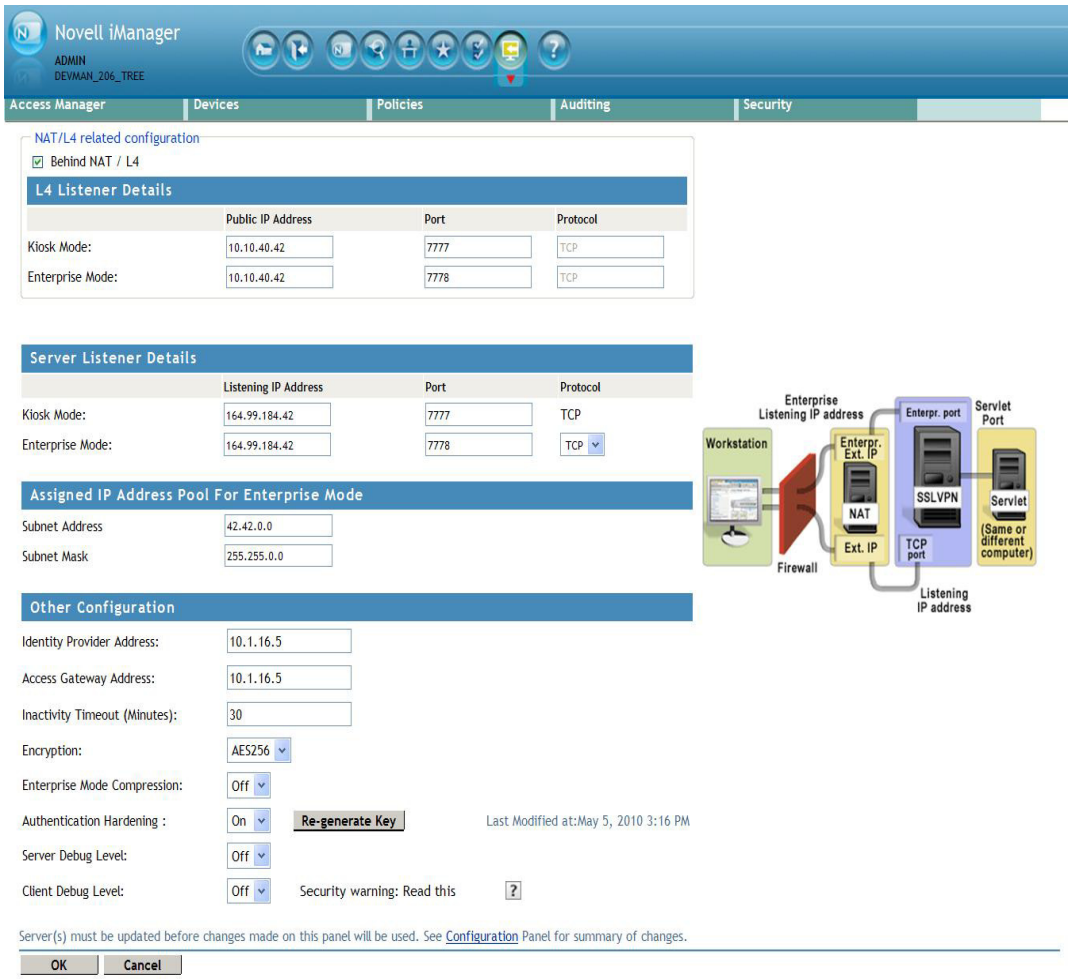
4 Click *OK* to save your changes.

If you are using Traditional SSL VPN, you are prompted to configure the IP address or DNS name of the Identity Server, and the Linux Access Gateway.



5 Click *OK*.

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



7 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.

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

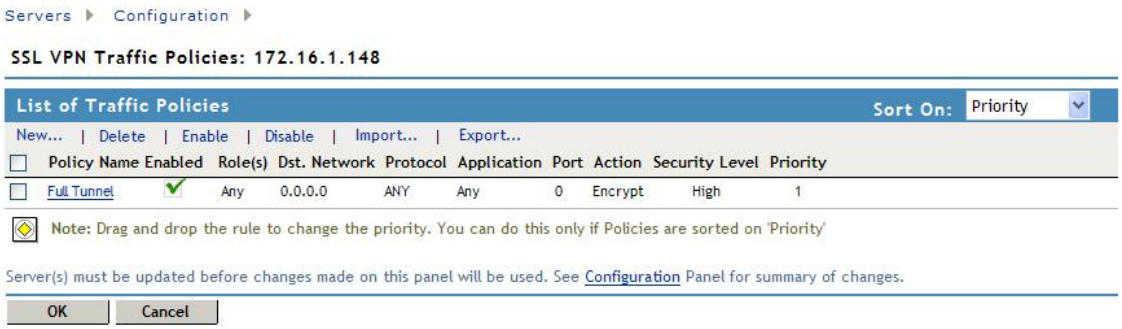
4.4.3 Examples for Full Tunneling Policy

The below examples displays different scenarios for Full Tunneling policy.

- "Example 1: Basic Full Tunneling Scenario" on page 72
- "Example 2: Only Groupwise Access is Allowed and All Access Are Denied Including Internet Access" on page 72
- "Example 3: Policies Are At The Same Roles and Security Level" on page 72
- "Example 4: Policies Are At The Same Roles With Different Security Levels" on page 73

Example 1: Basic Full Tunneling Scenario

If an administrator wants to allow all the traffic through the tunnel then you need to configure the full tunneling policy with the required CIC level. If the CIC level is not met then policy will not be downloaded to the client and all access will be denied as the SSL VPN connection itself will not go through and displays an error.



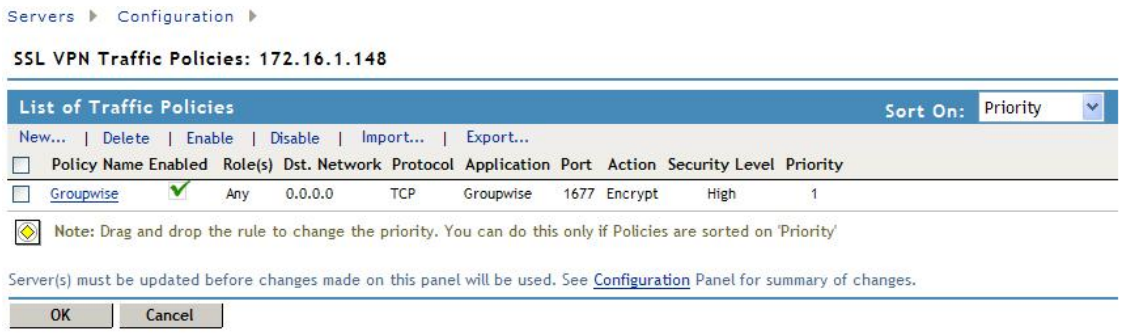
Example 2: Only Groupwise Access is Allowed and All Access Are Denied Including Internet Access

In the below example you can view the Groupwise server full tunneling access scenario.

If an administrator wants to:

- Allow access or encrypt only Groupwise server
- Deny all other access including Internet access
- CIC level not met or fails

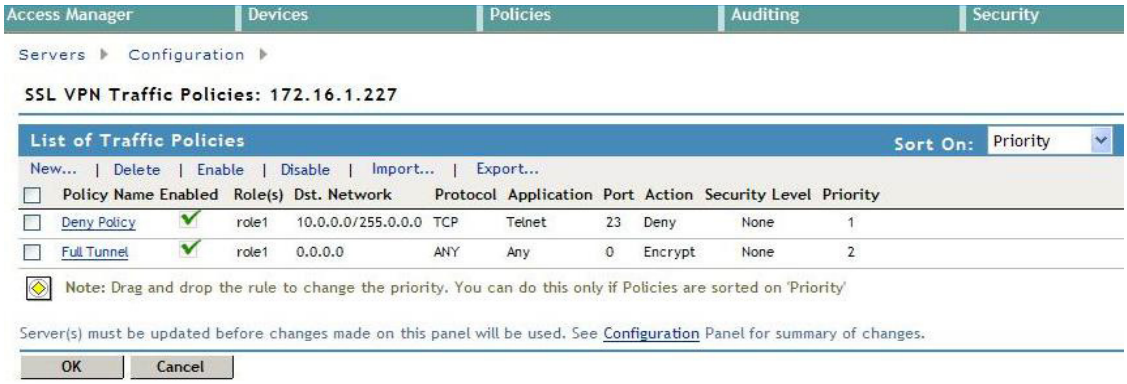
then the administrator has to configure the full tunneling encrypt policy allowing only access to Groupwise server.



Example 3: Policies Are At The Same Roles and Security Level

If an administrator wants all the user traffic to go through corporate network and deny access to Telnet server, then the administrator configures a telnet deny policy with higher priority and a full tunnel allow policy as shown below.

NOTE: Ensure that policies are at the same roles and security level.



Example 4: Policies Are At The Same Roles With Different Security Levels

If an administrator wants to allow or encrypt Telnet server from clients at *HIGH* security level (if the client is at a different security level) and deny access to the same application, then the administrator can define allow or encrypt policy for the *HIGH* security level to allow connection to Telnet server and define a deny policy for Telnet with *NONE* security level.

In the below example two traffic policies are configured with the same role out of which one of them is configured with a Security level for which traffic is allowed and the other is configured with the same application without security level.

Configuring How Users Connect to SSL VPN

5

You can configure client machines to control how users connect to SSL VPN.

5.1 Preinstalling the SSL VPN Client Components

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

5.1.1 Installing Client Components for Linux

1. On the client machine, download the following RPM from the `/var/opt/novell/tomcat5/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>`

5.1.2 Installing Client Components for Macintosh

1. On the client machine, download the following package for the PPC platform from the `/var/opt/novell/tomcat5/webapps/sslvpn/MacOS` directory:

   `novell-sslvpn-serv.tar.gz`

2. On the client machine, download the following package for the Intel* platform from the `/var/opt/novell/tomcat5/webapps/sslvpn/Maci386` directory:

   `novell-sslvpn-serv.tar.gz`

3. Enter the following command to untar the file:

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

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

```
installer -pkg novl-sslvpn-service.pkg -target "/"
```

5.1.3 Installing Client Components for Windows

1 On the client machine, download the following file from `/var/opt/novell/tomcat5/webapps/sslvpn/windows`:

```
novl-sslvpn-service-install.exe
```

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

5.2 Configuring Client Policies

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.

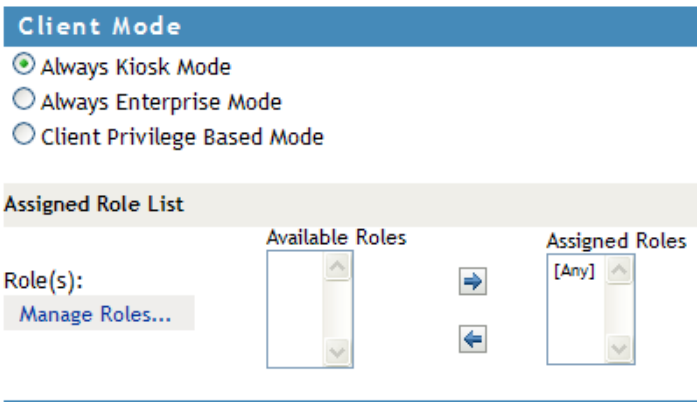
- Section 5.2.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 76
- Section 5.2.2, "Allowing Users to Select the SSL VPN Mode," on page 77
- Section 5.2.3, "Configuring Client Cleanup Options," on page 78
- Section 5.2.4, "Configuring SSL VPN to Download the Java Applet on Internet Explorer," on page 79
- Section 5.2.5, "Configuring a Custom Login Policy for SSL VPN," on page 79

5.2.1 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 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 modes, and do not configure the other roles for any mode, the roles without a specific configuration are by default assigned to 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 the *Always Kiosk 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 the client policy, 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.

5.2.2 Allowing Users to Select the SSL VPN Mode

To configure 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.

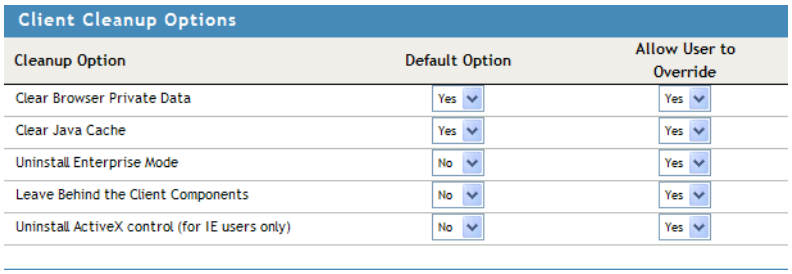
4 To save your modifications, click *OK*, then click *Update* on the Configuration page.

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

5.2.3 Configuring Client Cleanup Options

You can configure the cleanup options that are displayed to the user while disconnecting the SSL VPN connection.

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



3. Select any of the following options:

   Clear Browser Private Data: Select this option to clear the browser history and cache, saved password, authenticated sessions and auto form-fill data when the client logs out. When this option is selected, all the data and information that were saved after the SSL VPN connection was made are cleared from the client machine. In the Firefox browser, any previous browsing history or data that was present before the SSL VPN connection was made is not cleared.

   Clear Java Cache: Select this option to clear the Java cache when the client logs out. This clears not just the files and applets used by SSL VPN, but all files and applets in the cache. The Java cache is cleared when the browser window is closed.

   Uninstall Enterprise Mode: Select this option to uninstall the Enterprise mode client when the client logs out.

   Leave Behind the Client Components: Select this option to reduce the connection time when the client logs in again. When this option is selected, some of the SSL VPN components are left on the client and the connecting time is reduced because these components are not downloaded again.

   If this option is not enabled:

   - All client components downloaded for the connection are removed in Kiosk mode.
   - All client components other than the service RPM or service MSI are removed in Enterprise mode. This is because the service RPM or service MSI is mandatory for operation in this mode.

   Uninstall ActiveX control (for IE users only): When a user connects to SSL VPN through Internet Explorer, ActiveX is downloaded to the client machine to enable SSL VPN connection. You can select this option to remove the ActiveX control when the client logs out.

   To select any of these options, set *Default Option* to *Yes*.

If you set *Allow User to Override* to *Yes*, users can change any of the cleanup options set by you. To require users to retain the cleanup options you configured, set *Allow User to Override* to *No*.

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

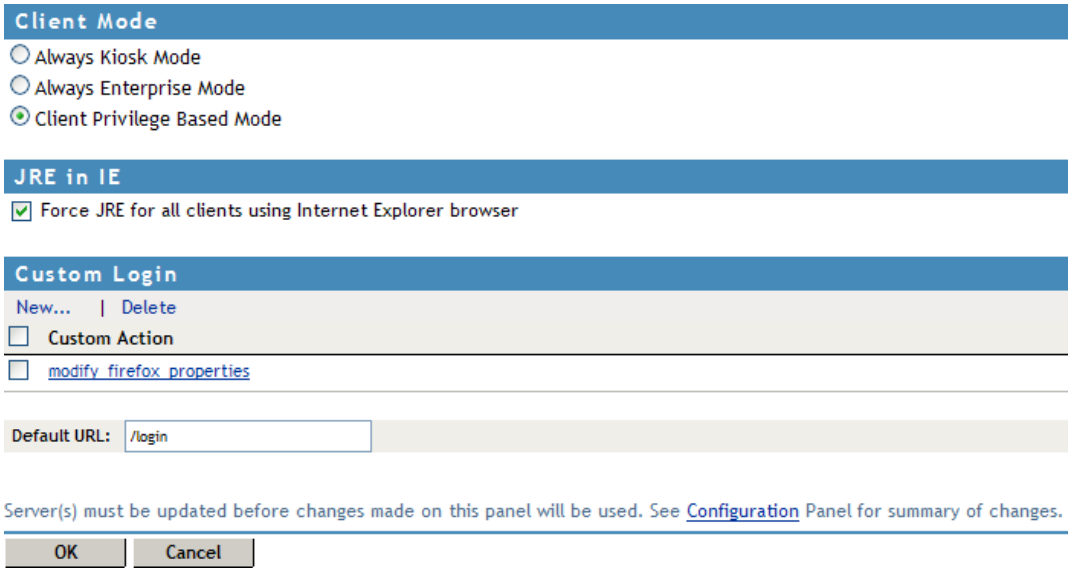
5.2.4 Configuring SSL VPN to Download the Java Applet on Internet Explorer

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 Internet Explorer.

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

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.

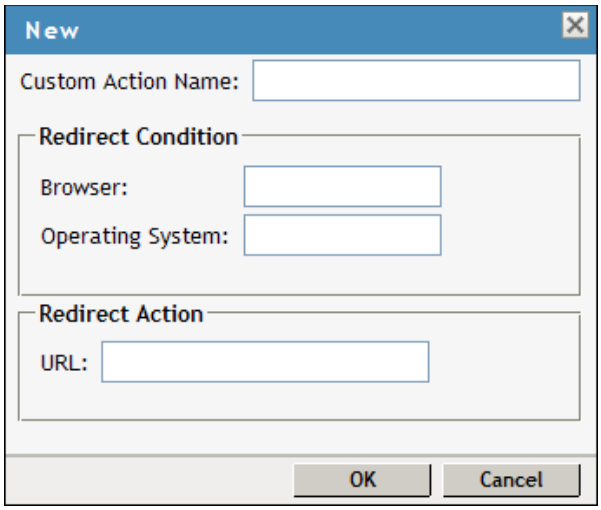
5.2.5 Configuring a Custom Login Policy for SSL VPN

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 configuration.

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:

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 5.4.3, "Configuring a Custom Login Policy for Citrix Clients," on page 83.

- The browser can be Firefox, Safari*, Internet Explorer, or any other. You can specify more than one browser, separated by ommas.
- 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.

5.3 Configuring SSL VPN to Connect through a Forward Proxy

The Novell SSL VPN can be configured to detect and connect through a forward proxy in both Kiosk and 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.

5.3.1 Understanding How SSL VPN Connects through a Forward Proxy

When a user initiates a connection to the 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:
   - 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.
   - 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 connection order information in the configuration file and connects either directly or through the proxy.

5.3.2 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=192.10.0.0:8080`
3. Add one of the following lines to specify the connection order:
   - To configure SSL VPN to connect through the proxy first, specify `ConnectionOrder=direct:proxy`
   - To configure SSL VPN to try a direct connection, specify `ConnectionOrder=proxy:direct`

If the connection order is not specified in the configuration file, SSL VPN connects directly without the proxy.

4 (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.

5 Save and close the file.

5.4 Configuring SSL VPN for Citrix Clients

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:

5.4.1 Prerequisites

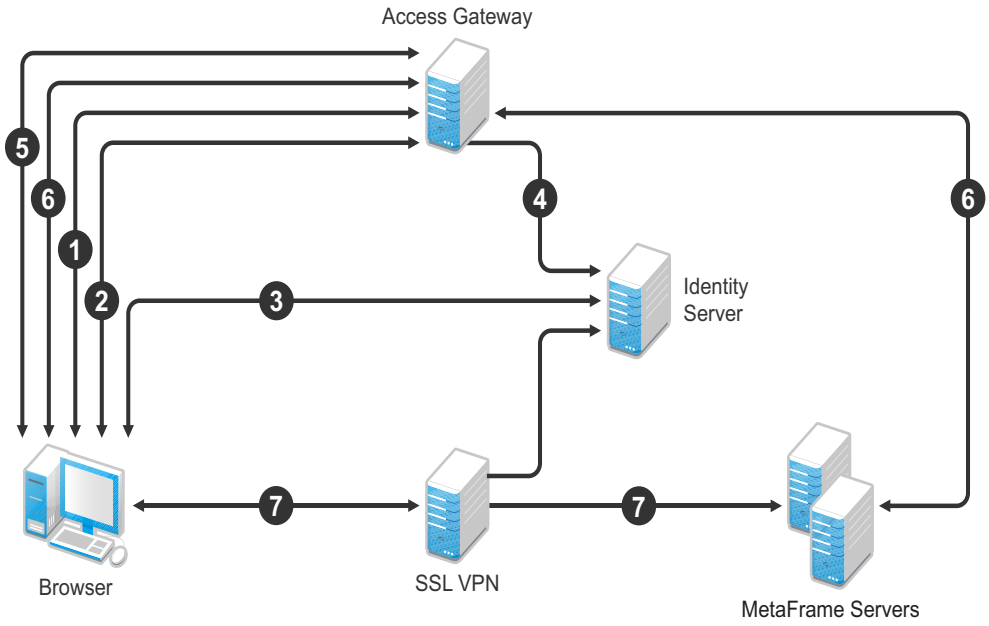
- ❑ NFuse server
- ❑ MetaFrame server
- ❑ Identity Server

  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
- ❑ Configure SSL VPN to use the same Identity Server as the Access Gateway.
- ❑ Download the `Citrix_Script.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.

5.4.2 How It Works

Access Manager can be configured to provide single sign-on for Citrix clients. Figure 5-1 illustrates this process for the Citrix Web client.

Figure 5-1 *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 erver 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.

5.4.3 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.

5.4.4 Configuring the Access Gateway to Protect the Citrix Server

To enable users to access Citrix applications through SSL VPN, you must 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 you configure 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 SP2 Access Gateway Guide*
4. On the Server Configuration page, click *OK*, then click *Update*.

5.4.5 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 Configure the following *Submit* options:

7a Select *Auto Submit*.

7b Select *Enable JavaScript Handling*.

7c 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.

7d 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.

7e Change the protocol to HTTPS if the secure protocol is used.

7f Replace <*Webserver-path*> with the location of the Web server on which the `Citrix_Script.js` javaScript file is located. When this JavaScript file is used, it connects users from the outside through SSL VPN.

7g 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 SP2 Policy Guide*.

9 In the *Actions* section, click *New* > *Form Login Failure*.

10 Specify the procedures you want followed when login fails.

For more information, see *Login Failure Policy* in the Novell Access Manager 3.1 SP2 Policy Guide (http://www.novell.com/documentation/novellaccessmanager31/policies/?page=/documentation/novellaccessmanager31/policies/data/bookinfo.html).

Citrix displays login failures via the query string, so you need to use CGI matching

11 Click *OK*, then click *Apply Changes*.

12 Click *Close*.

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

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

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

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

Clustering the High-Bandwidth SSL VPN Servers

6

You can cluster the high-bandwidth SSL VPN servers can now be clustered to provide load balancing and fault tolerance capabilities and act as a single server. 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 failed over to another SSL VPN server that is healthy.

Even though the SSL VPN authentication connection to the cluster remains unaffected during the session failover, the SSL VPN tunnel goes down and a new tunnel is established with the new SSL VPN server. This might affect applications such as FTP that were being accessed through the tunnel at the time of failover.

A cluster can be set up to function with an L4 switch or the Access Gateway to handle load balancing. A cluster can be set up to function with an L4 switch or by using the Access Gateway. You can have a cluster of servers in both HTTP and HTTPS.

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 switch, the system routes the user to one of the SSL VPN servers in the cluster, as traffic necessitates.

Using L4 for Clustering: In this approach, the SSL VPN cluster is placed behind an L4 switch. If the tunnel IP address configured in the administration console is the virtual IP address of an L4 switch, 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 switch, see "Configuration Tips for the L4 Switch " in the *Novell Access Manager 3.1 SP2 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 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 6.5, "Clustering SSL VPNs by Using the Access Gateway without an L4 Switch," on page 94.

This section has the following information:

6.1 Prerequisites

- ❑ An L4 switch 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 switch. 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 switch balances the load between the SSL VPN servers in the cluster.
- ❑ The following ports are open on the L4 switch 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)

6.2 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.

6.3 Creating a Cluster of SSL VPN Servers

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.

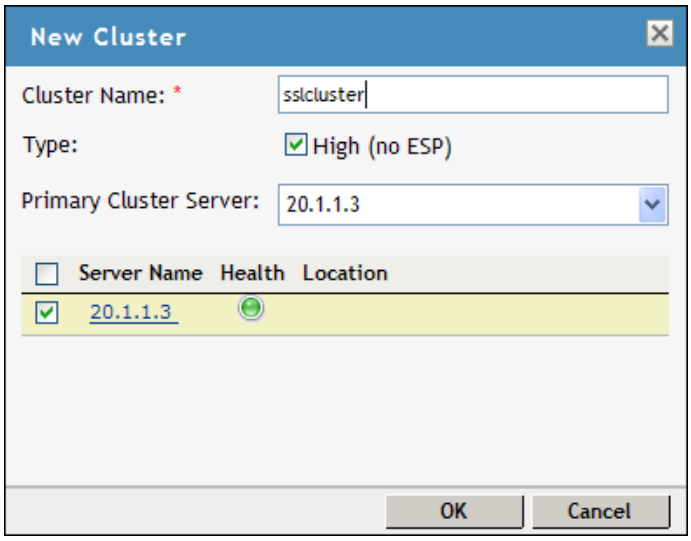
This section describes how to set up and manage a cluster of SSL VPN servers:

- Section 6.3.1, “Creating a Cluster of SSL VPN Servers,” on page 89
- Section 6.3.2, “Adding an SSL VPN Server to a Cluster,” on page 90
- Section 6.3.3, “Removing an SSL VPN Server from a Cluster,” on page 90

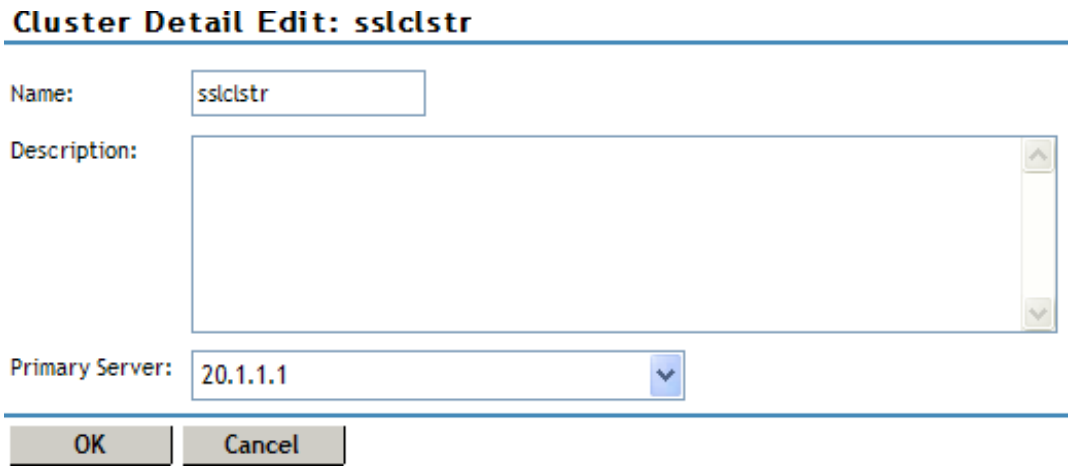
6.3.1 Creating a Cluster of SSL VPN Servers

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*.



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*.

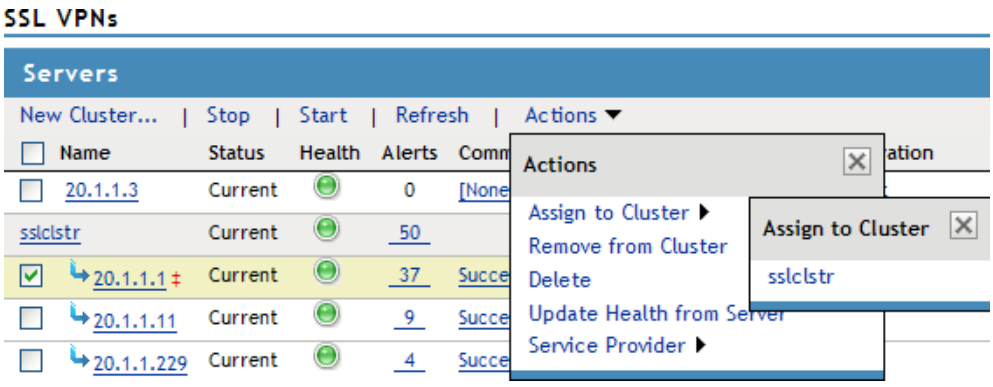
The status icons for the configuration and the SSL VPN Server should turn green. It might take several seconds for the SSL VPN server to start and for the system to display a green light.

6.3.2 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.

6.3.3 Removing an SSL VPN Server from a Cluster

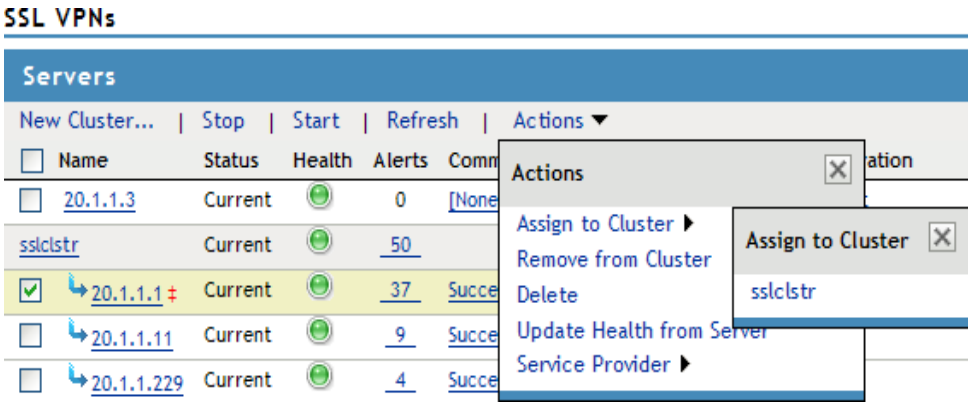
Removing an SSL VPN server from a cluster disassociates the SSL VPN server from the cluster configuration. You can either remove servers individually or remove all the clusters at the same time.

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*.

6.4 Clustering SSL VPN by Using an L4 Switch

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

You can either have a cluster of traditional SSL VPN servers by using L4 switches and Access Gateways or you can have a cluster of ESP-enabled SSL VPNs by using the L4 switch. 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.

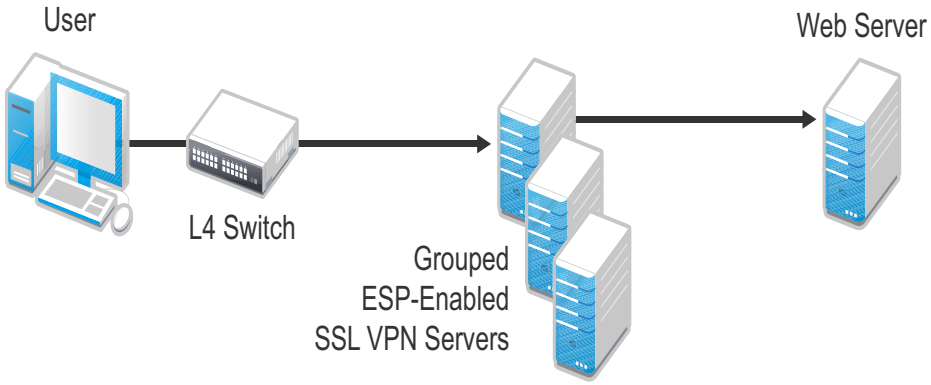
Make sure that the base URL of SSL VPN is resolvable with its own IP address as well as the public IP address of the L4 switch. The Identity Server should be able to resolve the base URL of SSL VPN to the virtual IP address of the SSL VPN cluster.

- Section 6.4.1, “Configuring a Cluster of ESP-Enabled SSL VPNs,” on page 91
- Section 6.4.2, “Configuring a Cluster of Traditional SSL VPNs by Using an L4 Switch,” on page 93

6.4.1 Configuring a Cluster of ESP-Enabled SSL VPNs

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

Figure 6-1 *Cluster of SSL VPNs behind an L4 switch,*



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

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 "Installing the ESP-Enabled SSL VPN".

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 "Verifying That Your SSL VPN Service Is Installed".

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

   For more information on configuring the L4 switch and gateway details, see Section 3.3, "Configuring the IP Address, Port, and Network Address Translation (NAT)," on page 45. For more information on configuring the Audit events, see Section 7.2, "Enabling SSL VPN Audit Events," on page 100.

4. Import the traffic policies into the server. For more information on importing the traffic policies, see "Exporting and Importing Traffic Policies" on page 68.

5. Create a cluster of SSL VPNs.

   For more information on creating a cluster, see Section 6.3.1, "Creating a Cluster of SSL VPN Servers," on page 89.

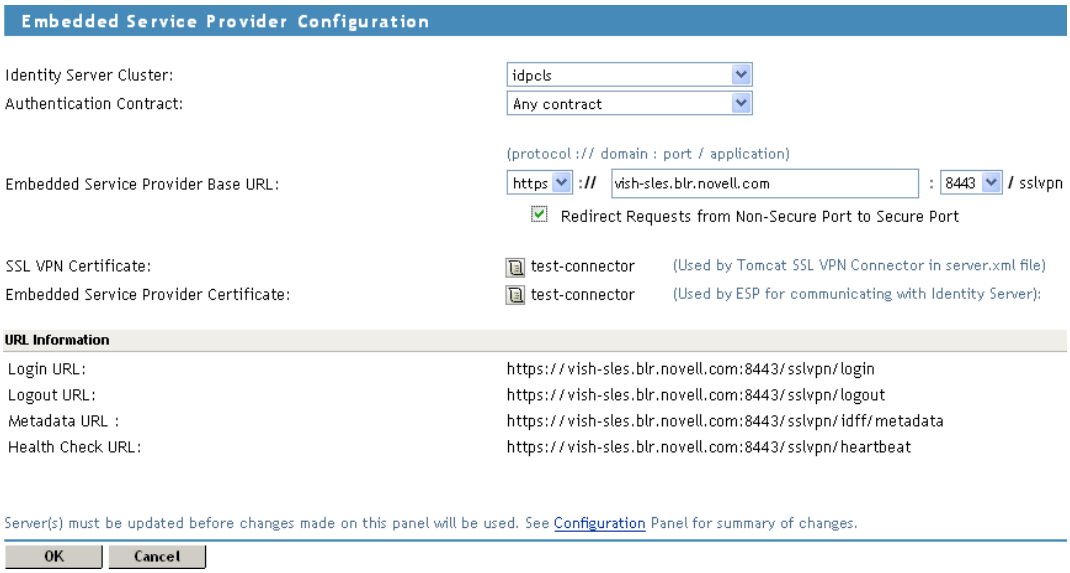
6. Assign all SSL VPN servers to the cluster.

   For more information, see Section 6.3.2, "Adding an SSL VPN Server to a Cluster," on page 90. 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. Make sure that each of the cluster members are assigned with different IP pools for Enterprise Mode.

   For more information, see Section 3.3, "Configuring the IP Address, Port, and Network Address Translation (NAT)," on page 45.

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.

6.4.2 Configuring a Cluster of Traditional SSL VPNs by Using an L4 Switch

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 "Installing the ESP-Enabled SSL VPN" in the *Novell Access Manager 3.1 SP2 Installation Guide*.

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 "Verifying That Your SSL VPN Service Is Installed" in the *Novell Access Manager 3.1 SP2 Installation Guide*.

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

For more information on configuring the L4 switch and gateway details, see Section 3.3, "Configuring the IP Address, Port, and Network Address Translation (NAT)," on page 45. For more information on configuring the Audit events, see Section 7.2, "Enabling SSL VPN Audit Events," on page 100.

4 Import the traffic policies into the server.

For more information on importing the traffic policies, see "Exporting and Importing Traffic Policies" on page 68.

5 Create a cluster of SSL VPNs.

For more information on creating a cluster, see Section 6.3.1, "Creating a Cluster of SSL VPN Servers," on page 89.

6 Assign all SSL VPN servers to the cluster.

For more information, see Section 6.3.2, “Adding an SSL VPN Server to a Cluster,” on page 90.

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. Configure specific listening IP addresses for Kiosk mode and Enterprise modes. Make sure that each of the cluster members are assigned to different IP pools for Enterprise mode. For more information, see Section 3.3, “Configuring the IP Address, Port, and Network Address Translation (NAT),” on page 45.

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

For more information, see Chapter 3.2, “Accelerating the Traditional Novell SSL VPN,” on page 41.

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

6.5 Clustering SSL VPNs by Using the Access Gateway without an L4 Switch

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:

- Section 6.5.1, “Configuring the Access Gateway,” on page 94
- Section 6.5.2, “Installing the Scripts,” on page 95
- Section 6.5.3, “Testing the Scripts,” on page 95

6.5.1 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.

6.5.2 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
   ```

6.5.3 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
   ```

4. Click *Update from Server* to get the latest health status of the Access Gateway.
5. 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.
6. Enter the following command to start the SSL VPN server:

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

7. 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
   ```

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

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

10 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.

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

6.6 Configuring SSL VPN to Monitor the Health of the Cluster

The L4 switches 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 switch to monitor the heartbeat URL of the Identity Servers and Access Gateways, so that the L4 switch can use this information to accurately update the health status of each cluster member.

6.6.1 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.

A Note about Alteon Switches

When you configure 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 switch and you have not configured SSL in Access Manager, then the HTTP service on the L4 switch does not work. If the health check for the SSL service fails, the L4 switch assumes that all the services configured to use the same virtual IP are down.

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
```

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
```

6.6.2 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, so 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 7

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.

7.1 Viewing and Editing SSL VPN Server Details

1. In the Administration Console, click *Devices* > *SSL VPNs*.
2. Click the server whose information you want to view. The following information about the server is displayed:

   Edit: Click this option to modify the general details of the selected SSL VPN server. For more information, see Section 8.3, “Modifying SSL VPN Server Details,” on page 116.

   The General page displays information about the selected server. If the field is empty, click *Edit* to add a value. The fields that contain links transfer you to another page where you can edit the information.

   Name: Specifies the Administration Console display name of the server. This field is mandatory. Click the link or click *Edit* to edit the name.

   Management IP Address: Specifies the IP address used to manage the server. This field is mandatory.

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

   Location: Specifies the location of the SSL VPN server. This information is optional, but useful if your network contains multiple SSL VPN servers.

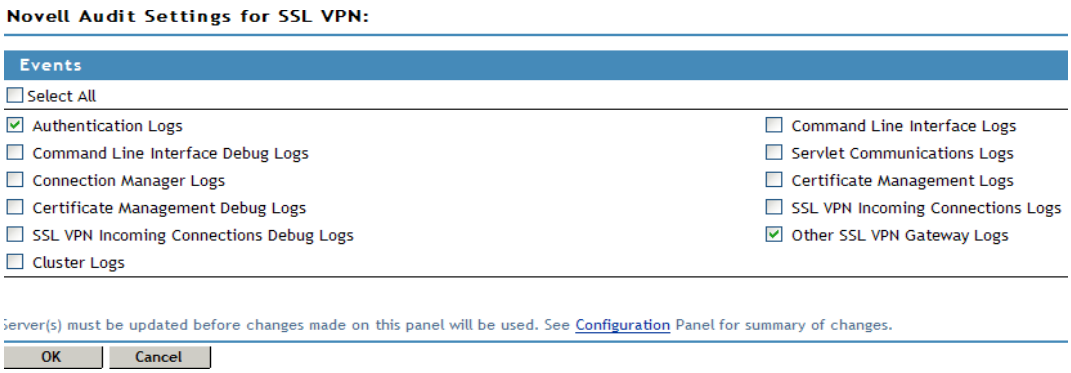
   Server Version: Specifies the version of the installed server RPM.

   Description: Provides a brief description of the SSL VPN server. This information is optional, but useful if your network contains multiple SSL VPN servers.
3. Click *Close* to save and close the General page.

7.2 Enabling SSL VPN Audit Events

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 the Administration Console* in the *Novell Access Manager 3.1 SP2 Administration Console Guide* (http://www.novell.com/documentation/novellaccessmanager31/adminconsole/?page=/documentation/novellaccessmanager31/adminconsole/data/bookinfo.html)

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Novell Audit Settings* from the *Novell Audit and Alerts* section.



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. These logs help in debugging errors.
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.

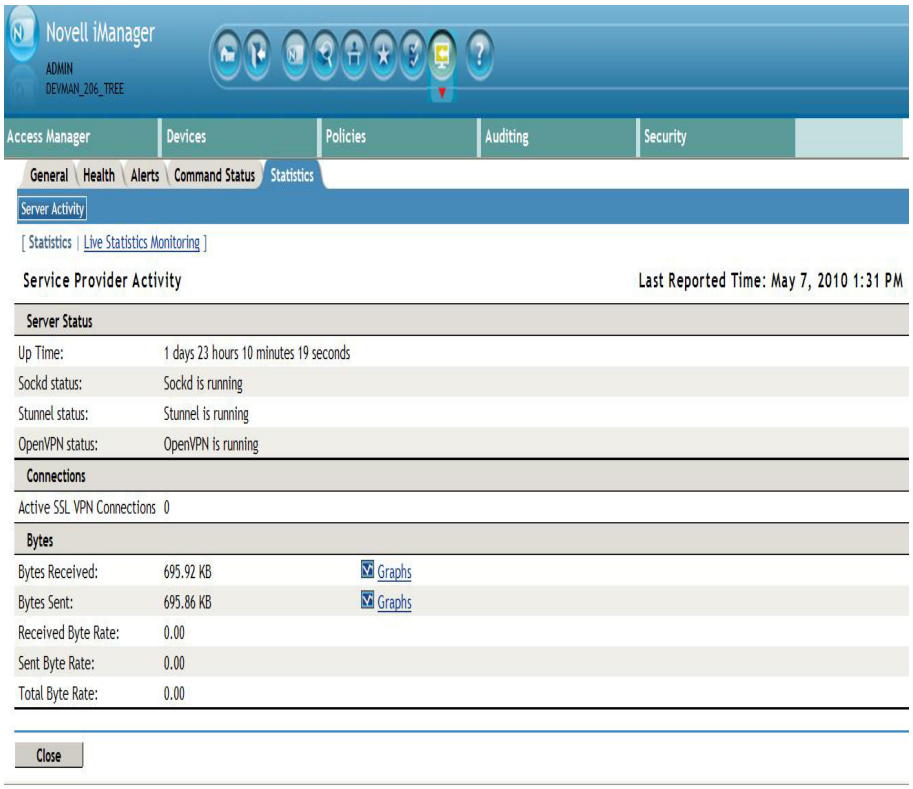
4 To save your modifications, click *OK,* then click *Apply Changes* on the Configuration page.

7.3 Viewing SSL VPN Statistics

The Statistics page allows you to view information such as the number of active client connections and the time when the SSL VPN server was started.

7.3.1 Viewing the SSL VPN Server Statistics

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



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.
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. Also displays 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 7.3.3, “Viewing the Bytes Graphs,” on page 104.
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 7.3.3, “Viewing the Bytes Graphs,” on page 104.
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.

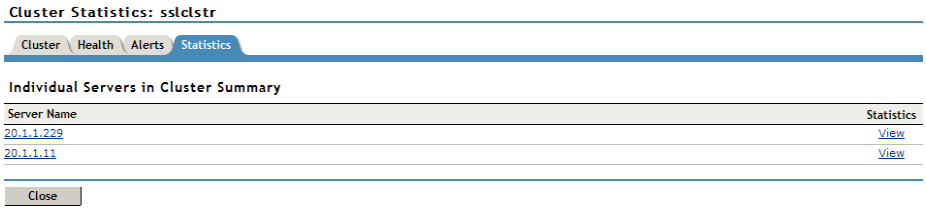
2 Select one of the following options:

- **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 statistics 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.

7.3.2 Viewing the SSL VPN Server Statistics for the Cluster

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



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 7.3, “Viewing SSL VPN Statistics,” on page 101.

3 Click *Close* to close the *Statistics* tab.

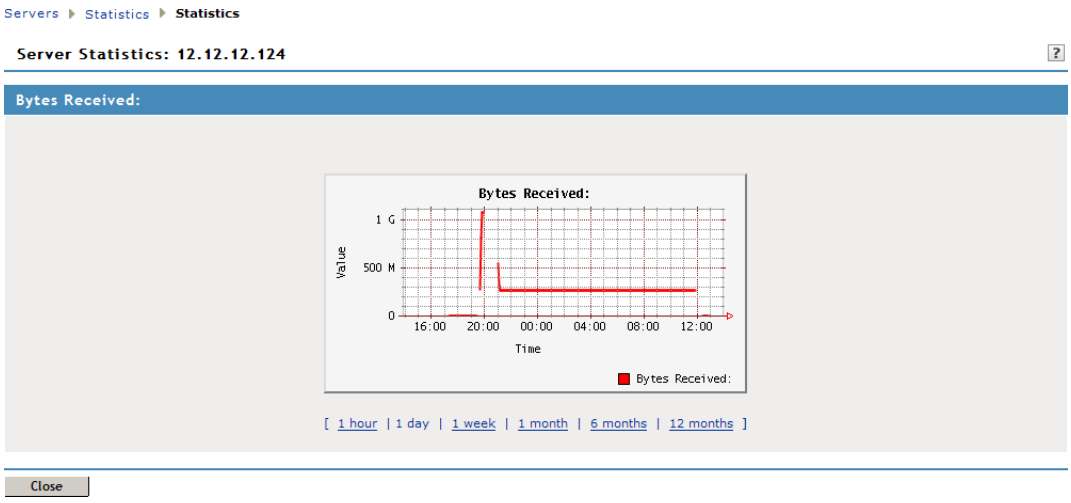
7.3.3 Viewing the Bytes Graphs

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.



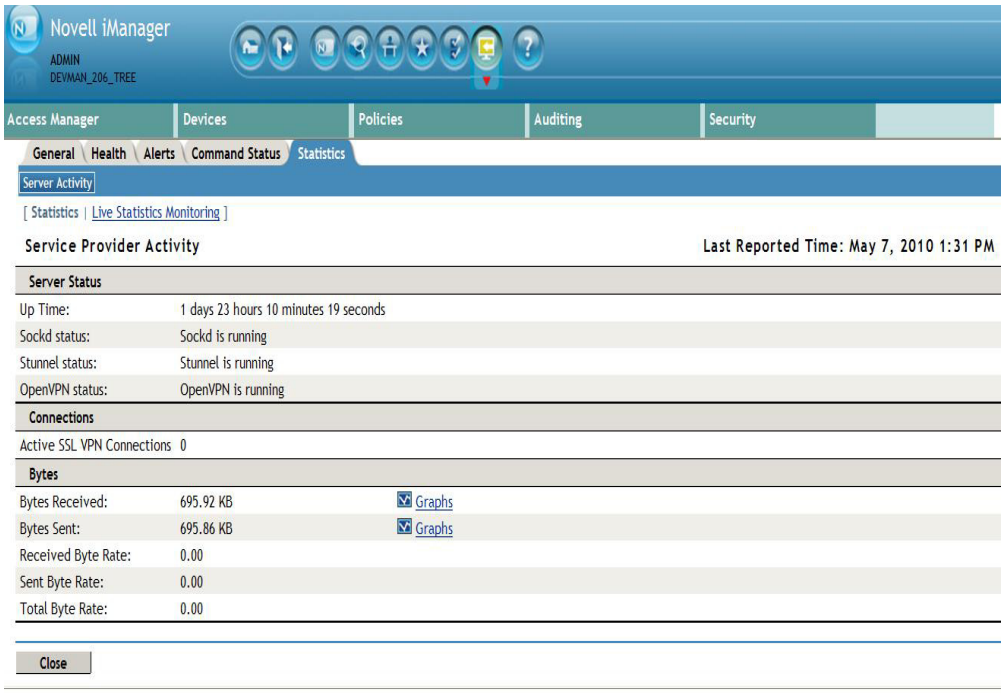
3. Click *Close* to close the Graphs page.

7.4 Disconnecting Active SSL VPN Connections

You can use the Administration Console to disconnect users who are connected to SSL VPN. You can 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*.



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

4 Click *OK* to confirm your action.

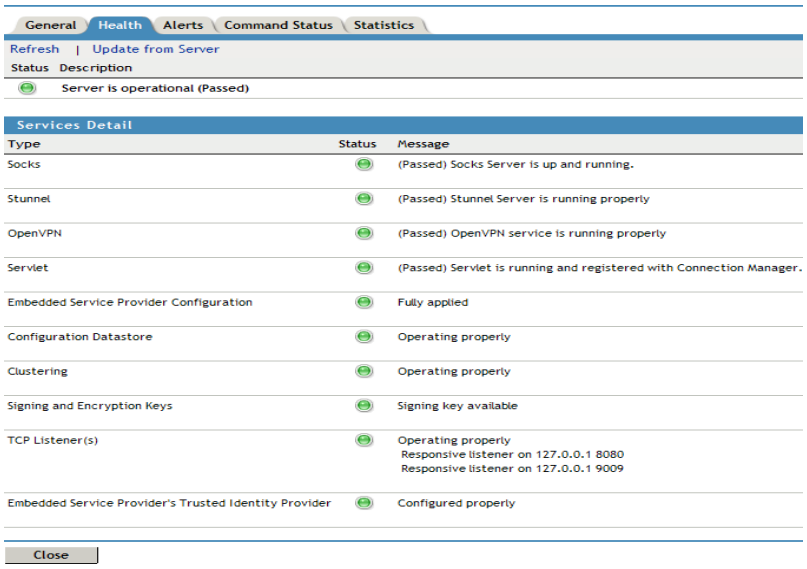
7.5 Monitoring the Health of SSL VPN Servers

You can monitor the health of an SSL VPN Server through the Health page, which displays the current status of the server.

- Section 7.5.1, “Monitoring the Health of a Single Server,” on page 105
- Section 7.5.2, “Monitoring the Health of an SSL VPN Cluster,” on page 106

7.5.1 Monitoring the Health of a 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*.

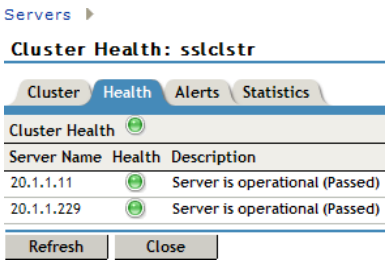
3 To send a request to the agent to update its status information, click *Update from Server*. Click *OK* in the confirmation dialog box. This can take a few minutes.

4 To close the Health page, click *Close*.

7.5.2 Monitoring the Health of an 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* section 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 the 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*.

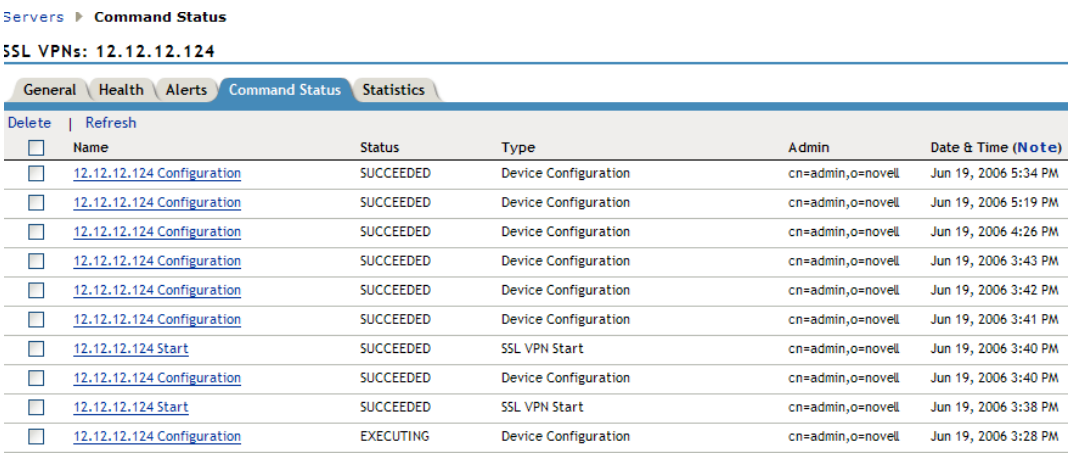
3 To send a request to the agent to update its status information, click *Update from Server*. Click *OK* in the confirmation dialog box. This can take a few minutes.

4 To close the Health page, click *Close*.

7.6 Viewing the Command Status of the SSL VPN Server

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*.



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 7.6, “Viewing the Command Status of the SSL VPN Server,” on page 107.

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*.

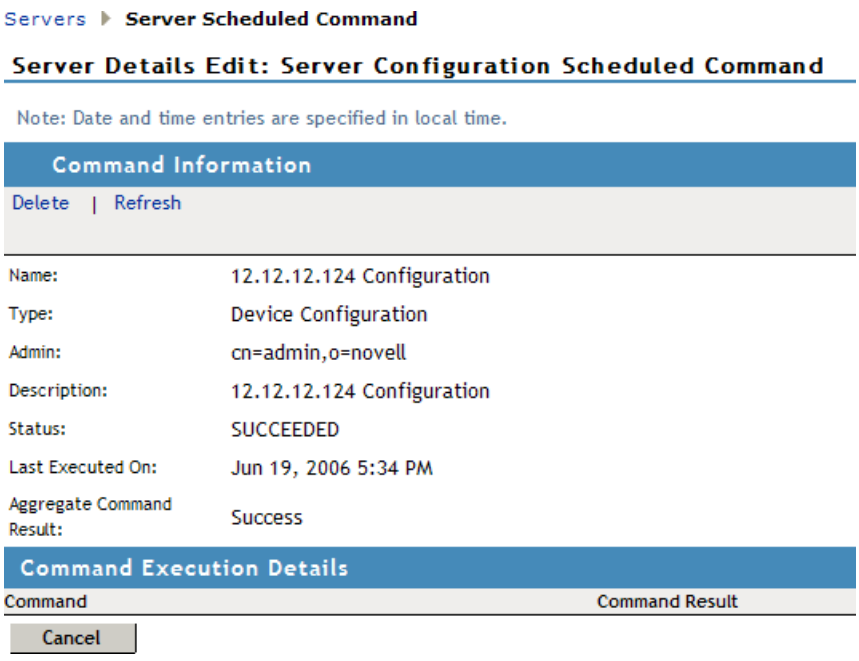
4 Click *Close* to close the Command Status page.

7.6.1 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.



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*.

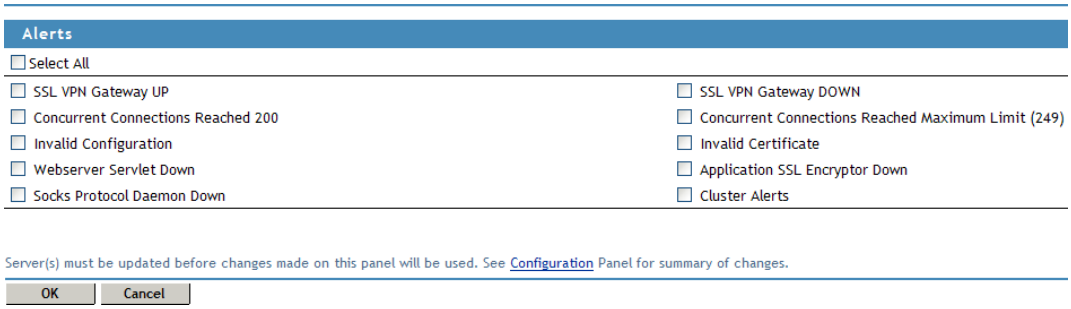
3 Click *Close* to return to the command status page.

7.7 Monitoring SSL VPN Alerts

The Alerts page allows you to view information about current system alerts and to clear the alerts. An alert is generated whenever the SSL VPN Gateway detects a condition that prevents it from performing normal system services.

7.7.1 Configuring SSL VPN Alerts

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



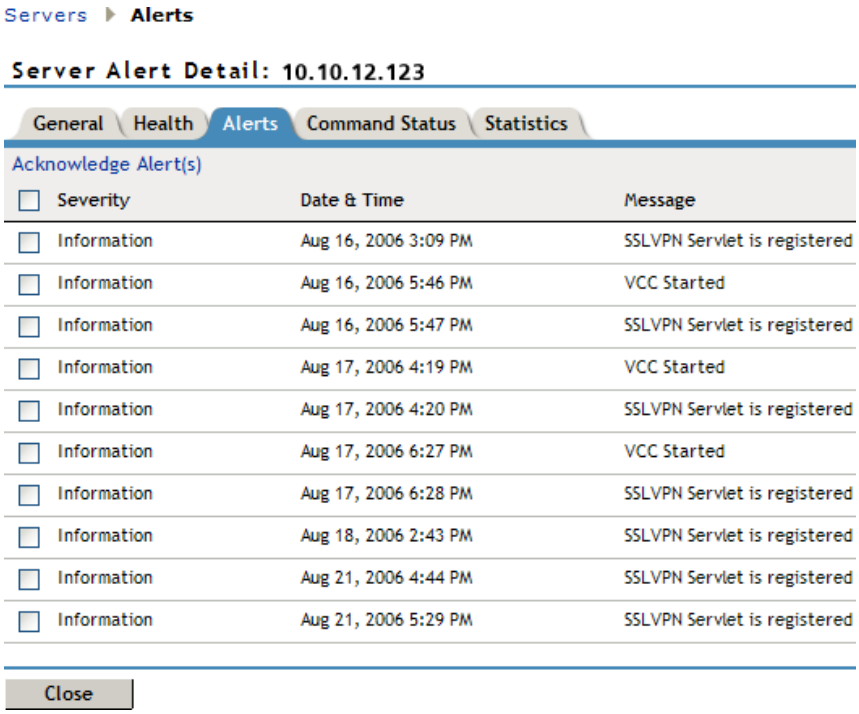
2 Select the *Select All* option to send alerts for all the events, or select one or more of the following:

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.
Application SSL encryptor down	Sends an alert whenever the SSL encryptor is down.

Alert	Description
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.

7.7.2 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.

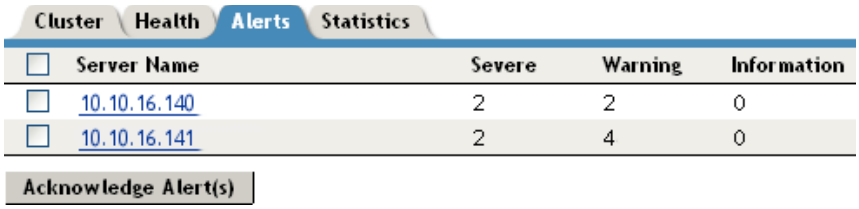
2 To send an acknowledgement, select the check box next to the alert, then click *Acknowledge Alert(s)*. When you acknowledge an alert, the alert is cleared from the list.

3 Click *Close* to close the Alerts page.

7.7.3 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 that is displayed.

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.

Server Configuration Settings

8

This section describes the configuration settings that affect SSL VPN servers.

8.1 Managing SSL VPN Servers

Use the Servers page to view the status of SSL VPN servers, to modify their configuration, to create or delete clusters, or to stop and start the server.

1. In the Administration Console, click *Devices* > *SSLVPNs*.
2. Select one of the following options:

   New Cluster: Displays the New Cluster dialog box, where 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.

   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: Use this option to update the list of servers and their health status.
3. To perform an action available in the *Actions* drop-down menu, select an SSL VPN server, then select one of the following:

   Assign to Cluster: To add the selected SSL VPN server to a cluster, select *Assign to Cluster*, then select the cluster. This SSL VPN is reconfigured with the configuration of the primary cluster server.

   Remove from Cluster: To remove the selected SSL VPN server from a cluster, select *Remove from Cluster*. The SSL VPN server retains its configuration from the cluster, but no traffic is sent to it until it is reconfigured. You can assign it to a different cluster and have it updated with the new cluster’s configuration, or you can delete all of its reverse proxies and start a new configuration.

   Delete: To remove the selected SSL VPN server from the list of servers that can be managed from this Administration Console, select *Delete*. If the SSL VPN server is a member of a cluster, you must first remove it from the cluster before you can delete it.

   IMPORTANT: When an SSL VPN server is deleted from the Administration Console, you can no longer manage it. To access it again, you must manually trigger an auto-import, which causes it to import into an Administration Console.

   Update Health from Server: Click this action to send a request to the server for updated health information. If you have selected multiple servers, a request is sent to each one. The health status changes to an animated circle until the reply returns.

Service Provider: Select one of the following actions:

- **Start Service Provider:** To start the Embedded Service Provider associated with the selected SSL VPN, click *Start Service Provider*. The Embedded Service Provider is the module within the SSL VPN that communicates with the Identity Server.

  The Embedded Service Provider should be restarted whenever you enable or modify logging on the Identity Server.

- **Stop Service Provider:** To stop the Embedded Service Provider associated with the selected SSL VPN, click *Stop Service Provider*. The Embedded Service Provider is the module within the SSL VPN that communicates with the Identity Server.

  When an SSL VPN is not functioning correctly, you should always try stopping and starting the service provider before stopping and starting the SSL VPN.

- **Restart Service Provider:** To restart the Embedded Service Provider associated with the selected SSL VPN, click *Restart Service Provider*. This command stops the Embedded Service Provider and then starts it. The Embedded Service Provider is the module within the ESP-enabled SSL VPN that communicates with the Identity Server.

  When an Access Gateway is not functioning correctly, you should always try restarting the Embedded Service Provider before stopping and starting the Access Gateway.

4 Use the following links to manage a cluster or an SSL VPN server:

Name: Displays a list of servers that can be managed from this administration console. This also displays the name of the cluster, if you have configured one. Click the link of a particular server to view or modify its configuration. For more information, see Viewing and Editing SSL VPN Server Details.

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 this link to apply the changes.
- *Pending* indicates that the server is processing a configuration change, but has not completed the process.

Health: Indicates the health of the SSL VPN server. Click the icon to view additional information about the functional status of an SSL VPN server.

Alerts: Indicates whether any alerts have been sent. Click the link to view additional information about alerts. This option is not available to you if the alert count is 0. For more information, see Viewing SSL VPN Alerts.

Commands: Indicates the status of commands issued to servers. For more information, see Viewing the Command Status of the SSL VPN Server.

Statistics: Indicates the number of active client connections and the time when the Gateway was started. Click *View* to get the statistics information. For more information, see Viewing the SSL VPN Server Statistics.

Type: Indicates the type of SSL VPN that is installed. This section indicates whether the SSL VPN server installed is an SSL VPN protected by the Access Gateway or if it is a standalone SSL VPN. It also indicates if the SSL VPN version is high-bandwidth or low-bandwidth. For example, if the high-bandwidth version of SSL VPN protected by the Access Gateway is installed, then the *Type* displayed is *High (non-ESP)*.

Configuration: Indicates the date and time when the last modification was made. It also indicates the fully distinguished name of the user who made the last modification. Click *Edit* to view and modify the SSL VPN configuration. For more information, see Configuring SSL VPN Servers.

8.2 Configuring SSL VPN Servers

The Configuration page allows you to view the configuration status and to configure the features of a cluster or a single SSL VPN server.

All configuration changes are applied from the SSL VPNs page. The links from this page allow you to accept or cancel any changes, but the changes are not sent to the SSL VPN server from the other pages.

1 In the Administration Console, *Devices* > *SSLVPNs* > *Edit*.

To edit an SSL VPN server that is not a member of a cluster, click the *Edit* button next to the server that you want to edit.

To edit the configuration of a cluster, click the *Edit* button next to the cluster.

The Server configuration page is displayed with the following information:

Services: A list of the services available for configuration.

Last Changed: The date and time the service was last modified.

Change By: The distinguished name of the user who made the last modification.

2 Select one of the following configuration options:

- The Gateway configuration section allows you to configure the SSL VPN gateway and DNS server list information. You can select one of the following options:

  Basic Configuration: Allows you to configure the gateway. For more information, see Configuring the IP Address, Port, and Network Address Translation (NAT).

  Advanced Configuration: Allows you to configure SNAT entries for the SSL VPN server. For more information, see Configuring Route and Source NAT for Enterprise Mode.

  Authentication Configuration: Allows you to configure the Embedded Service Provider. This link is not enabled of you have installed SSL VPN with the Linux Access Gateway. For more information, see Configuring Authentication for the ESP-Enabled Novell SSL VPN.

  DNS Servers List: Allows you to configure the DNS server list. For more information, see Configuring DNS Servers.

- The policies section allows you to configure policies that determine the resources a client can access, depending on the role and the security measures adhered to by the client.

  Client Integrity Check Policies: Allows you to configure the client integrity check policies. For more information, see Configuring Policies to Check the Integrity of the Client Machine.

  Client Security Levels: Allows you to configure different security levels for different client roles. For more information see Client Security Levels.

  Traffic Policies: Allows you to configure traffic policies. For more information, see Configuring Traffic Policies.

Client policies: Allows you to configure policies that determine if clients should access SSL VPN in Kiosk mode only, or in Enterprise mode only, or if the mode selection can be done by the clients. For more information, see Configuring Full Tunneling.

- The Novell Audit and Alerts section allows you to set up alerts so that notifications are sent when specified events occur.

  Novell Audit Settings: Allows you to configure Novell Audit settings. For more information, see Enabling SSL VPN Audit Events.

  Alerts Settings: Allows you to configure alerts settings. For more information, see Configuring SSL VPN Alerts.

- The security settings section allows you to view and modify the current security configuration for the SSL VPN server.

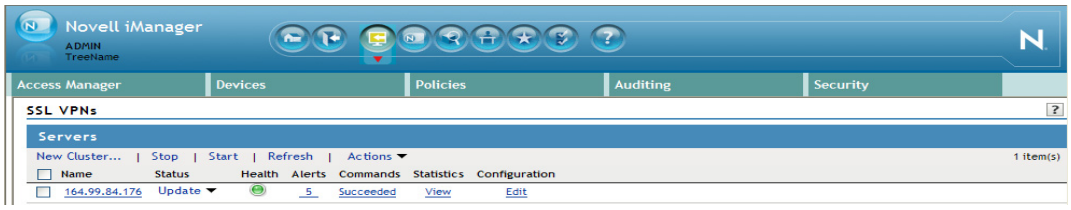
  SSL VPN Certificates: Allows you to configure certificate details for SSL VPN. For more information, see Configuring Certificate Settings.

3 To apply and save changes, select one of the following actions:

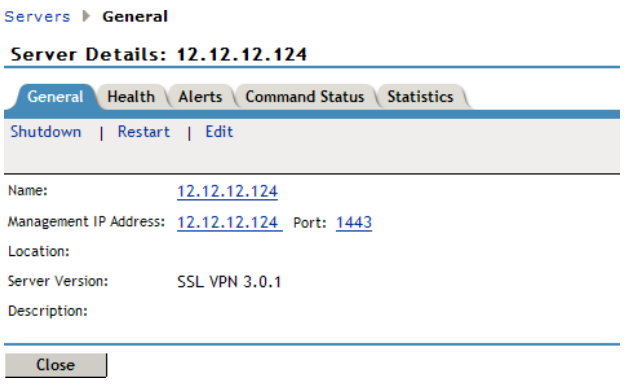
- **OK:** To save all the configuration changes that have been made, click *OK*. When you leave this page, the changes are accepted and the SSL VPN server is scheduled for an update.
- **Cancel:** To close without saving any pending changes, click *Cancel*, then click *OK* at the confirmation dialog box.
- **Revert:** To cancel configuration changes that you have already accepted and return to the previous configuration, click *Revert*.

8.3 Modifying SSL VPN Server Details

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

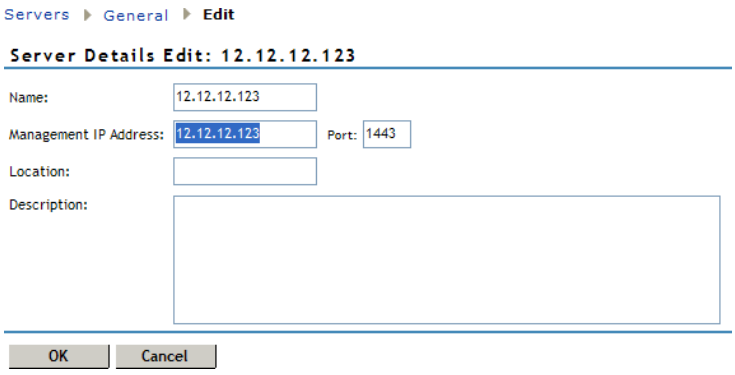


2 Click the server.



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.

3 Click *Edit*.



4 Verify 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.

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

Additional Configurations

9

The following sections describe additional configurations for the SSL VPN server:

9.1 Customizing the SSL VPN User Interface

You can customize the contents of the SSL VPN home page, the exit page, and the error messages, depending on your organization’s requirements.

9.1.1 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 `<div id=”homecontent”>` tags.

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

9.1.2 Customizing Error Messages

To customize the error messages:

1. Browse and open the following file:

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

2. Edit the file to modify existing error messages and to add new messages as necessary.
3. Save and close the file.

9.2 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.

9.3 Creating a Configuration File to Add Additional Configuration Changes

You can use a configuration file to create and execute many extended configuration options for both the SSL VPN Enterprise client and the Enterprise server.

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.

Troubleshooting SSL VPN Configuration

A

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:

This section provides various troubleshooting scenarios that you might encounter while configuring SSL VPN.

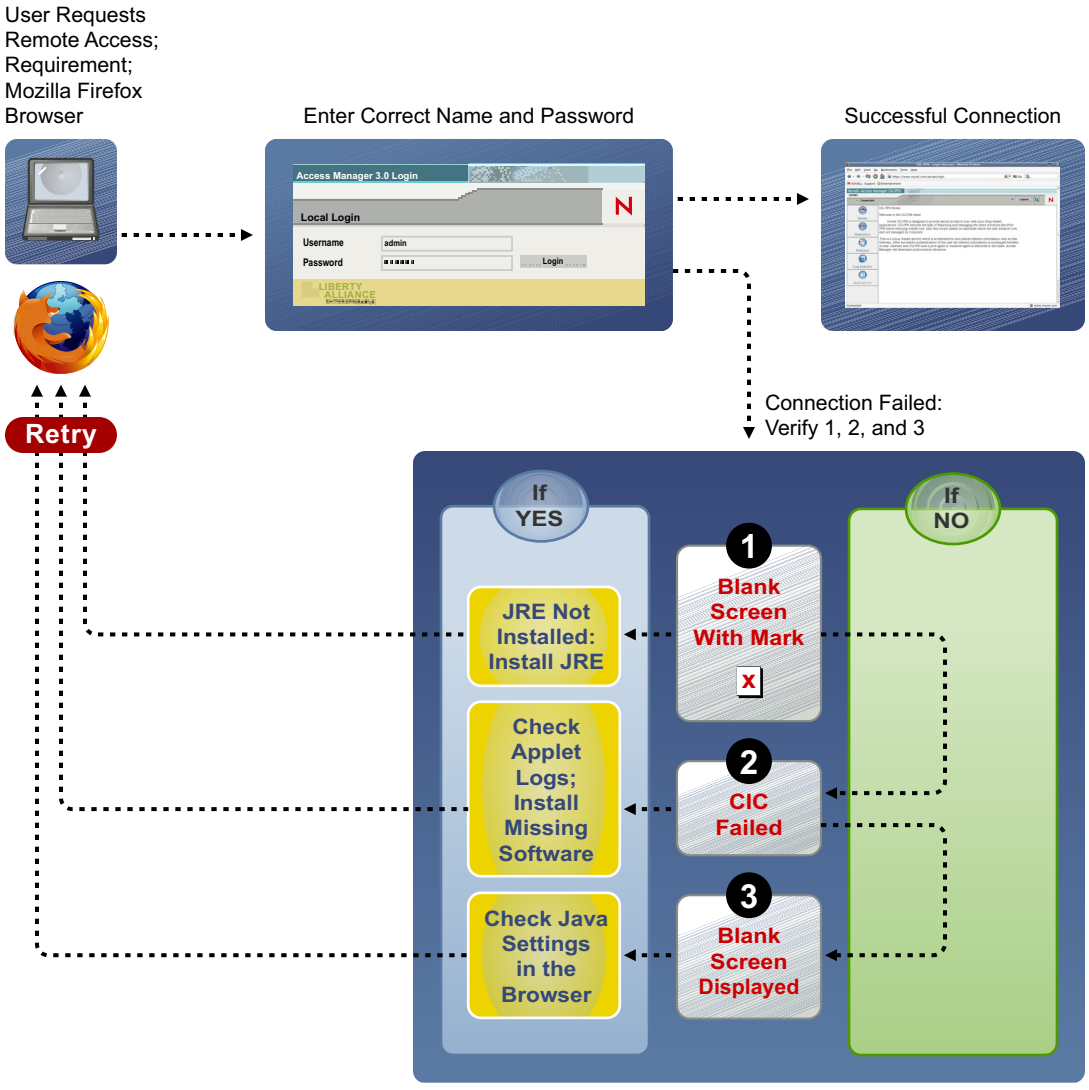
A.1 Successfully Connecting to the Server

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:

- “Connection Problems with Mozilla Firefox” on page 122
- “Connection Problems with Internet Explorer” on page 123

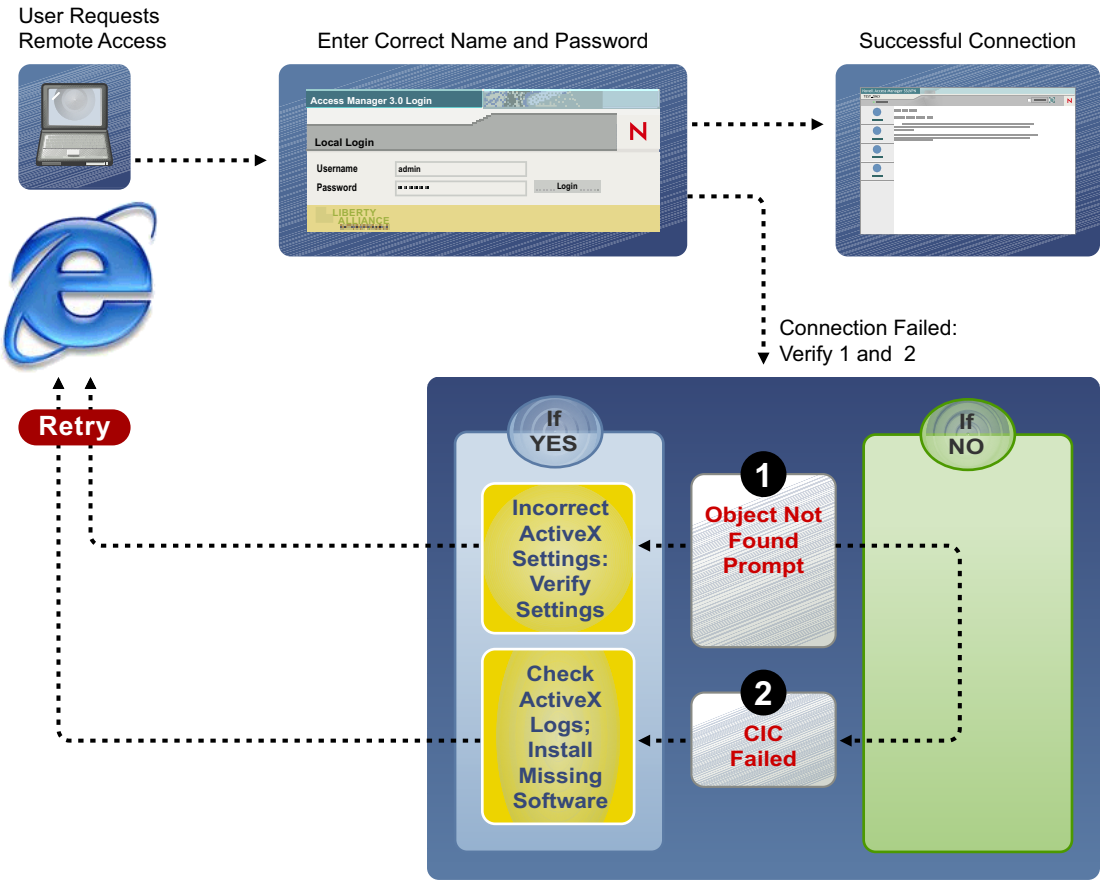
A.1.1 Connection Problems with Mozilla Firefox

Figure A-1 *Using Mozilla Firefox to Connect to the SSL VPN Server*



A.1.2 Connection Problems with Internet Explorer

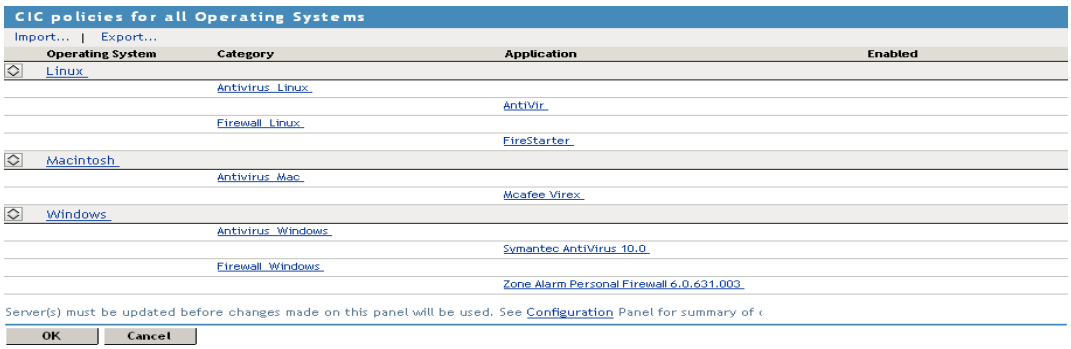
Figure A-2 *Using Internet Explorer to Connect to the SSL VPN Server*



A.2 Adding Applications for Different Versions of Windows

You can configure different applications for different flavors of Windows such as Windows Vista, Windows XP or Windows 7 in the same Client Integrity Check category. For example:

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



3 Click *Windows* from *Operating System*.

4 Create a Category.

5 Create an application for Windows Vista.

6 Specify an attribute for the application. You can either specify a registry key, process, service or an AbsoluteFile.

For example, add *RegistryKey*, then specify the registry key values for Windows Vista.

7 Create an application for Windows XP.

8 Specify an attribute for the application. You can either specify a registry key, process

For example, add *RegistryKey*, then specify the registry key values for Windows XP.

9 You can similarly add registrykey values for other flavors of Windows.

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

A.3 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.

A.4 Error: Failed to Fetch CIC Policy from the Server

The HTTPS connection to the SSL VPN Kiosk mode might fail on a Windows XP machine, with the following log message:

```
Error: Failed to Fetch CIC Policy from the Server
```

This error is caused because of a problem with the certificate. To work around this issue, remove old certificates from the server and create new ones. For more information, see Section 3.6, “Configuring Certificate Settings,” on page 53.

A.5 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 5.3, “Configuring SSL VPN to Connect through a Forward Proxy,” on page 80.

A.6 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 Section 3.4, “Configuring Route and Source NAT for Enterprise Mode,” on page 50.
- You are not using source NAT to route packets.

A.7 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.

A.7.1 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
```

A.7.2 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
```

A.8 Verifying SSL VPN Components

Use the commands and processes described in the following sections to verify that the SSL VPN components are running:

A.8.1 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`

A.8.2 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`

A.8.3 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`

A.8.4 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.

A.9 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.

A.10 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).

A.11 The SSL VPN Connection Is Successful But There Is No Data Transfer

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 Public 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 Public 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 3.3, “Configuring the IP Address, Port, and Network Address Translation (NAT),” on page 45.

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 3.3, “Configuring the IP Address, Port, and Network Address Translation (NAT),” on page 45.

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.

Action: 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.

A.12 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.

A.13 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 this, see Section A.8, "Verifying SSL VPN Components," on page 125.

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.

A.14 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 A.8, "Verifying SSL VPN Components," on page 125.

A.15 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. To work around this problem, you must reinstall the SSL VPN server and configure a new SSL certificate.

A.16 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.

A.17 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
```

A.18 Connection Manager Log Does Not Display the Client IP Address

When the ESP-enabled SSL VPN is installed, you might see `UNKNOWN HOST` displayed in the Connection Manager logs instead of the IP address of the client.This is because this information is provided by the Access Gateway and is available only if the Traditional Novell SSL VPN server is deployed.

A.19 SSL VPN Full Tunnel Connection Disconnects on VMware

Possible Cause: An SSL VPN full tunnel connection might disconnect because of no keepalive response if the 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 is added to the client routing table to route the keepalive packet to the SSL VPN server through the default gateway. Because the SSL VPN gateway is on a host-only network on a VMware, the keepalive packet might not reach the SSL VPN server through the 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 the physical network from the 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`.

A.20 Clustering Issues

A.20.1 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
```

A.20.2 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. Use the `ps` command to check whether the `openvpn`, `stunnel`, and `sockd` binaries are still running.

   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.

A.20.3 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 on all of 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.
