Novell Access Manager
SSL Virtual Private Network
Access Control – Policy Enforcement – Compliance Assurance
## Contents

Novell SSL VPN .................................................................................................................................................... 4  
Product Overview ................................................................................................................................................ 4  
Identity Server ................................................................................................................................................... 5  
Access Gateway ................................................................................................................................................ 5  
SSL VPN ........................................................................................................................................................... 6  
SSL VPN Features ............................................................................................................................................ 7  
Clientless Access ............................................................................................................................................... 7  
Client Integrity Check ...................................................................................................................................... 7  
Access Control .................................................................................................................................................. 9  
Security ............................................................................................................................................................. 9  
Applications ..................................................................................................................................................... 9  
Management .................................................................................................................................................... 9  
Auditing ........................................................................................................................................................... 9  
High Availability ............................................................................................................................................. 10  
Inactivity Time-Out .......................................................................................................................................... 10  
Keep-Alive ...................................................................................................................................................... 10  
Platforms ......................................................................................................................................................... 11  
Remote OS Supported ...................................................................................................................................... 11  
SSL VPN Feature List .................................................................................................................................... 12  
Frequently Asked Questions ............................................................................................................................. 13  
  
Do I need to keep the browser open after connecting to the Novell Access Manager SSL VPN Gateway? .... 13  
Is split tunneling supported with the Novell Access Manager SSL VPN? ..................................................... 13  
Can I create site-to-site VPN tunnels with the Novell Access Manager SSL VPN? ....................................... 13  
Can Non-administrators on Windows connect to the Novell Access Manager SSL VPN? ............................. 13  
How secure is the Novell Access Manager SSL VPN? .................................................................................... 13  
Can I use Microsoft Java with Novell Access Manager SSLVPN? ............................................................... 13  
What are the applications that can be accessed through Novell Access Manager SSL VPN? ................... 13
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 the 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 Gateway SSL VPN (Secure Socket layer Virtual Private Network) 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.

Utilizing existing infrastructure, SSL VPNs are economical and offer a simple and easy experience for employees and business partners.

**Product Overview**

The Novell Access Manager SSL VPN is designed to provide secure access to non-HTTP based applications inside a corporate network. It is combined with the powerful identity services of the Novell Access Manager in order to provide authentication and policy-controlled access to enterprise resources. Novell Access Manager supports industry-leading standards such as Liberty Alliance, WS-Security, and the Security Assertions Markup Language (SAML).

The Novell SSL VPN consists of an SSL VPN Gateway accelerated by reverse proxy and an Identity Server.

The following figure shows these components:
Identity Server

The Identity Server provides authentication services for all Novell Access Manager 3 components in addition to providing provider and consumer services for Liberty Alliance and SAML (1.1 and 2.0) requests. As with all Novell Access Manager 3 components, the Identity Server provides authentication services according to the Access Manager Policy specifications (see other Novell Access Manager 3 white papers in this series for more information).

The Identity Server is responsible for authenticating users and providing policy-constrained role information to facilitate authorization decisions.

The Identity Server also provides the full Liberty Alliance Web Service Framework to federate identity information. In addition to the standard Liberty Alliance Employee and Personal profiles, the Identity Server allows custom attributes to be defined, mapped and used in policy enforcement.

One additional technology that the Identity Server facilitates is Federated Provisioning, which automatically creates user accounts during a federation request. Without this feature, users would need to register (create a user account) with a Service Provider before they federate their identity.

Access Gateway

The Access Gateway is the HTTP proxy component of Novell Access Manager. In addition to providing the award-winning Novell security and proxy services (authorization, single sign-on and data encryption), it is also integrated with the new identity, role and policy services of the Novell Access Manager.

The Access Gateway provides the ability to transform Identity Provider authentication and services into standard web headers, form fill-in responses, and basic authentication responses; meaning that existing web applications may support the new identity standards without change.

An example of the support for new identity services, is the policy-enabled Identity Injection feature of the Access Gateway1 which leverages the Liberty Alliance Web Services Framework, to extract identity information and inject a higher-quality identity into web headers or query strings.

SSL VPN

Traditional IPSec solutions require client software to secure the transactions and lack granularity the administrators require, to provide appropriate access to users. Novell's SSL VPN reduces the task of deploying and managing the client solutions (e.g., IPSec) thereby reducing the overall cost. The SSL VPN can also be used on machines which are not owned by the user and not managed by corporate.

Novell's SSL VPN is a Linux-based service and is accelerated by either the Linux Access Gateway or NetWare Access Gateway. After successful authentication of the user, the

1 Formerly known as OLAC (Object Level Access Control)
identity information is exchanged between the Access Gateway and SSL VPN, after which a Java agent/ActiveX agent is delivered to the client. This agent establishes a secure SSL tunnel providing access to different applications as determined by policy and user/resource role.

The following figure shows the SSL VPN client Interface:

![Illustration 2: SSL VPN User Interface](image-url)
**SSL VPN FEATURES**

**Clientless Access**

Novell SSL VPN is a clientless application and supports any Web browser as client. It provides access from any location, including behind a network address translation (NAT) firewall. This increases the number of points from where employees, partners, and customers can access remote network data. Clientless access simplifies the connection process for users as they do not have to install a client. It also simplifies the IT administrators’ job as there is no need to configure and manage the client.

Novell SSL VPN handles authentication, encryption, authorization, and session cleanup activities. The user will not see any change in applications accessed through the SSL VPN. The service is available to all users irrespective of whether root or non-root in Linux/Mac* or administrator or non-administrator in Windows*.

**Client Integrity Check**

As the user has the flexibility of using SSL VPN from any unmanaged device, there is a risk of client device compromise which can result in an undesirable damage to the corporate network through the SSL VPN tunnel.

The Client Integrity Check feature of Novell's SSL VPN verifies the integrity of the client device before establishing the session. A users’ workstation is verified for current and running antivirus services, firewalls, or other software, specified in the Client Integrity Check Policy, before a connection is established. Once the session is established, client integrity checks are carried out during the session to ensure that if any antivirus or firewall application running in the workstation is stopped, it is detected and the SSL VPN session is terminated.

The Novell SSL VPN provides built-in templates to use standard software such as Zone Alarm and Symantec. Administrator can decide on the list of softwares and configure them in the server accordingly.

The following figure shows a sample list of software configured:
Illustration 3: Configuring Client Integrity Check Policy
ACCESS CONTROL

Simultaneously accommodating the varying needs of remote workers and ensuring data confidentiality, the SSL VPN provides access to authorized users based on their roles (such as manager, engineer or finance) and the roles of the resource. Roles can be changed or assigned to new users/resources without modifying existing access policies.

Advanced access control provides administrators with the tools to easily set individual access privileges based on applications, networks or hosts. Users may be presented with a list of applications that can be accessed during the session.

Security

Novell’s Access Manager SSL VPN makes minimal use of client computer resources and does not store any sensitive information remotely. All certificate associations to the SSL VPN are easily configured via the Access Manager administration console.

Security options include:

- Encryption—256-bit or 128-bit AES encryption
- Integrity: Hash SHA;
- Authentication—Username/Password (such as Active Directory or Novell eDirectory);

Applications

With an SSL VPN connection established, users can access authorized application servers using the standard client applications rather than being required to use web-based application clients. These standard client applications include:

- Client/server TCP applications, such as Microsoft* Outlook, Microsoft* Windows Terminal Services, Citrix* MetaFrame* applications, Novell® Groupwise®, TELNET, SSH, Passive FTP
- UDP-based services such as DNS, SNMP

Management

The Novell Access Manager SSL VPN is configured and monitored using the Access Manager 3 administration console. Operational statistics, alerts and health checkup features provide NOC personnel all necessary administration tools. Newly installed Access Manager SSL VPNs are automatically discovered and integrated into the administration console as are any configuration modifications that are made using the command-line interface (CLI).

Further, the Novell SSL VPN Gateway can operate behind a NAT.

Auditing
Novell SSL VPN is integrated with Novell Audit and Sentinel to provide comprehensive details about SSL VPN sessions, SSL VPN Gateway activities and much more.

High Availability

The Novell Access Manager SSL VPN can be configured for high availability which makes the SSL VPN service available all the time. Administrator can configure more than one SSL VPN Gateway to service client requests in a round robin fashion.

Inactivity Time-Out

Sessions are automatically terminated if connection activity is quiescent for a configurable amount of time.

Keep-Alive

Similar to the inactivity time-out, SSL VPN sessions are advised of the continued operation of both the user and gateway side via keep-alive packets. If these packets are not received for a configurable amount of time then the session is terminated.
PLAT FORMS

Users can access the Novell Access Manager SSL VPN Gateway from a Windows, Linux or MAC based system. A thin ActiveX client is downloaded if the browser is Microsoft Internet Explorer, otherwise, a thin Java client is downloaded.

Remote OS Supported

- Microsoft Windows 2000 with SP4
- Microsoft Windows XP with SP2
- RedHat Linux 9.x
- Novell Linux Desktop
- SUSE 9.x
- SLED 10.x

SSL VPN FEATURE LIST

<table>
<thead>
<tr>
<th><strong>Client Integrity</strong></th>
<th>Checks for antivirus, firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Checks done throughout the session</td>
</tr>
<tr>
<td></td>
<td>Template available for standard antivirus and firewalls</td>
</tr>
<tr>
<td></td>
<td>Option to verify software installation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Operating Systems supported for VPN client</strong></th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Linux</td>
</tr>
<tr>
<td></td>
<td>Macintosh</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Granular Access Policies</strong></th>
<th>Networks, protocols, service (such as FTP Telnet), port</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Inactivity Timeout</strong></th>
<th>Default 30 min, configurable.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Management Interface</strong></th>
<th>Device Manager, centralized configuration.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Windows Agent</strong></th>
<th>Signed ActiveX control and Java applet.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Java Agent</strong></th>
<th>Signed Java applet.</th>
</tr>
</thead>
</table>
FREQUENTLY ASKED QUESTIONS

Do I need to keep the browser open after connecting to the Novell Access Manager SSL VPN Gateway?

Yes, The browser needs to be kept open. You can minimize the browser and use the applications to connect to the protected network.

Is split tunneling supported with the Novell Access Manager SSL VPN?

Yes, Split Tunneling is supported.

Can I create site-to-site VPN tunnels with the Novell Access Manager SSL VPN?

No, you cannot create site-to-site VPN tunnels with the Novell Access Manager SSLVPN.

Can Non-administrators on Windows connect to the Novell Access Manager SSL VPN?

Yes, non-administrators can connect to the SSL VPN gateway using Firefox or any other browsers that support JRE. Non-administrators or users with no administrative privilege cannot use Internet Explorer to connect to the SSL VPN Gateway as the Activex controls require administrative privilege.

How secure is the Novell Access Manager SSL VPN?

Novell Access Manager SSLVPN uses SSL to communicate between the clients and the server. Others cannot get the contents of the information transferred between the clients and the server, even if they get the network packets. The Inactivity Timeout feature ensures that the session is logged out if no information is passed between the client and the server for a configured time. User sessions are authenticated and cookies are cleaned up after logout. No traces of the session are left behind in the client machine after logout.

Can I use Microsoft Java with Novell Access Manager SSLVPN?

No. The Novell Access Manager SSL VPN supports only Sun Java.

What are the applications that can be accessed through Novell Access Manager SSL VPN?

Ideally you can access all TCP and UDP application. For more information on list of applications tested on SSL VPN, refer to the documentation.