

Alteon Application Switch

Alteon SSL Accelerator



Nortel Networks

Alteon SSL VPN

A remote access gateway for today's extended enterprise

Alteon SSL VPN features

- Clientless remote access
- Application-layer security
- Supports TCP and UDP applications
- Client security with Dynamic Access Control
- Public/private-side SSL acceleration

Nortel Networks Alteon SSL VPN gateway is a remote access security solution that extends the reach of enterprise applications and file systems to mobile workers, telecommuters, partners, and customers. By using secure sockets layer (SSL) as the underlying security protocol, the Alteon SSL VPN allows for truly unrestricted remote access—using the Internet for remote connectivity and the ubiquitous Web browser as the client interface.

SSL is supported by virtually all Web servers and Web browsers, making it the defacto standard for securing Internet communications and an ideal remote access VPN technology. SSL operates

above the transport layer to secure data on behalf of the application and doesn't interfere with lower layer network services. These secure HTTPS sessions are universally regarded as standard Web traffic by firewalls and traffic filters, allowing for a reliable remote access service from any device on any network.

The Alteon SSL VPN gateway uses public key cryptography to establish a secure session with any browser-equipped device. The use of powerful application proxies expands support beyond Web applications to include legacy and custom developed client/server or mainframe applications.

Key features

Application-layer proxy

The Alteon SSL VPN provides freedom of mobility by providing secure remote access to a broad range of applications from any Web browser with Internet connectivity. With their basic capability to deliver HTML pages, most browser-based remote access solutions only support Web applications. The Alteon SSL VPN uses the Java capability of today's browsers to support an application-layer proxy that can channel non-Web protocols over a secure HTTPS session—providing secure remote access to TCP and UDP applications.

Clientless/Enhanced browser modes

Web browsers themselves run on many different types of end-user devices, including PCs, kiosks, PDAs, and cell phones. Even among common devices, the individual client configuration can prevent a particular browser from supporting a proxied session. To ensure support for the broadest range of applications, the Alteon SSL VPN gateway adapts the session type to the potential capability of a particular client.

- **Clientless browser mode**—Enables access to file systems and Web applications including dynamic HTML and complex JavaScript from any Web browser.
- **Enhanced browser mode**—Increases the breadth of available applications to client/server and mainframe systems from Java-capable Web browsers.

By supporting multiple browser modes, the Alteon SSL VPN establishes a basic session with restrictive browser configurations and a more sophisticated proxied connection with compatible browsers.

Transparent mode

For managed clients, such as employee PCs, a device-specific software client can be installed that allows users to remotely access applications using their native desktop environment and client interfaces. With this mode of operation, unrestricted access is provided to both Web and legacy applications.

Client security

Alteon SSL VPN gateways provide a suite of safeguard features to protect against malicious intent and user negligence. A dynamic access control feature can be used to specify restricted levels of access or even deny access altogether based on user parameters such as type of device, user IP address, or type of authentication being used. Whenever a new session is established, an ActiveX control is put on standby within the browser to clear all cached content and browser history upon session termination. And to help prevent a scenario where a vacated kiosk holds an open session, the Alteon SSL VPN will terminate any inactive connection after a brief countdown warning.

Global VPN load balancing

Large enterprise networks often connect geographically distributed offices from around the world. To provide optimal application performance for their end users, these networks require a remote access solution that dynamically adapts to the mobile user's location. The Alteon SSL VPN solution can be deployed in multiple geographically distributed locations to provide redundant access points to the private network. By incorporating Alteon's award-winning global server load balancing technology, users can be transparently re-directed to the closest or best performing access point regardless of their actual location.

Authentication

Increased freedom of mobility can introduce a security risk by allowing any Web browser to be a potential access point to private applications. The Alteon SSL VPN provides multiple authentication options, including support for common authentication mechanisms such as LDAP, RADIUS, and Active Directory services. Alternatively, the Alteon SSL VPN can support the use of digital certificates. An enterprise can issue their client certificates with the option of having them validated by a certificate authority for enhanced authentication. And for the strongest levels of authentication, the Alteon SSL VPN supports token-based systems such as RSA SecurID® and Secure Computing SafeWord™.

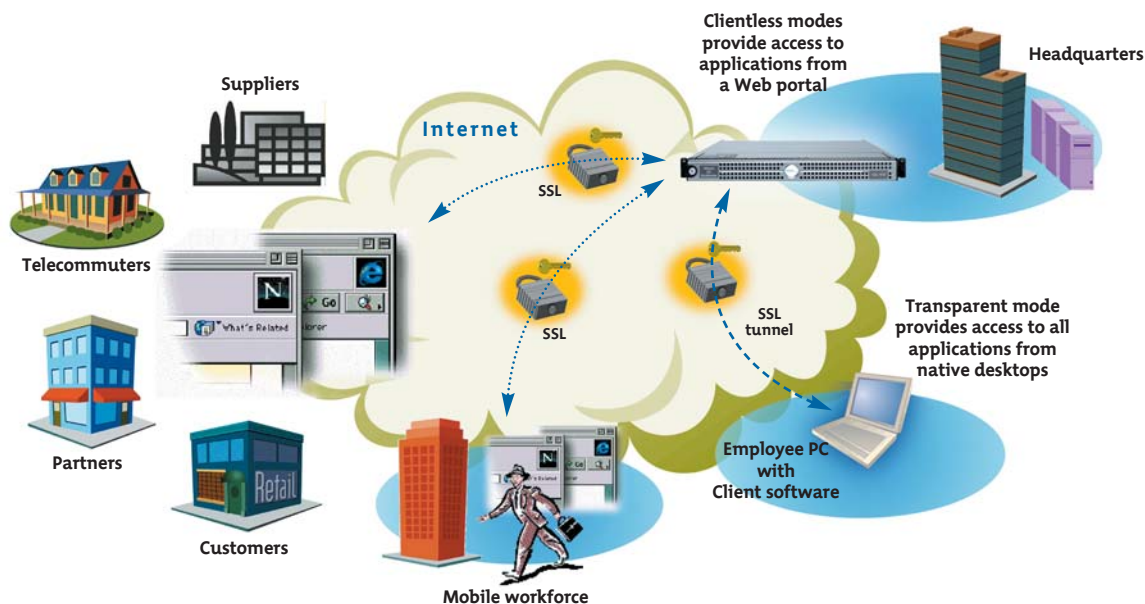
Granular access control and auditing

The Alteon SSL VPN gateway acts as a proxy server by intermediating requests and responses between the client and application or resource. At this point, the gateway decrypts all traffic and Alteon's application-layer inspection engine inspects session and application-layer data. Using this information, granular access control policies can be enforced for each user down to the application, URL path, and file levels. All activity is logged using a syslog event manager for detailed auditing support.

Integrated SSL acceleration

SSL uses public key cryptography during the initial handshake to establish a secure session. This process requires multiple complex mathematical operations that can tie up a general purpose processor and severely degrade its ability to perform other operations. Alteon SSL VPN gateways aggregate a high number of SSL sessions and incorporate Alteon's proven hardware-assisted SSL acceleration technology to maintain peak application performance.

Figure 1. The Alteon SSL VPN gateway provides secure remote access to applications



Optimized private-side encryption

Allowing partner access to business-critical applications or employee access to files containing sensitive information requires encryption across the private network as well as the public Internet. The Alteon SSL VPN gateway provides a variable cipher strength feature that allows administrators to adjust the level of encryption depending on the requirement of the application. Additionally, all application servers involved with private-side encryption are intelligently offloaded of the most compute-intensive tasks to protect against performance degradation and mitigate the need and cost of deploying additional servers.

Advanced content transformation

The Alteon SSL VPN incorporates advanced content transformation capabilities that prepare intranet content, applications, and file systems for browser-based remote access. Application Address Translation automatically converts Internal IP addressing to a format compatible with public DNS addressing structures and parses content on-the-fly to identify and rewrite any embedded links.

And a protocol conversion engine converts native Web protocols to secure HTTPS on the public-side of the gateway.

High-performance gateways

The Alteon SSL VPN gateways are specialized versions of the Alteon SSL Accelerator and Alteon Application Switch. The rich feature sets of these products allow users to configure the gateway to perform advanced traffic management and load balancing of applications.

VPN clustering

Alteon SSL VPN gateways can be deployed in an active-active or active-standby configuration and can be clustered in groups of up to 255 units. A unique Single System Image (SSI) capability allows the cluster to be managed as a single unit and provides plug-and-play scalability when additional units are deployed. Using an Alteon Application Switch provides the highest level of reliability, scalability, and performance by performing health checks and persistence-based load balancing of the SSL VPN gateways in the cluster.

Advanced filtering

Alteon SSL VPN gateways provide powerful application-layer filtering capabilities that can be used to block unwanted traffic. Policies can be established to block even authenticated users based on IP address, requested URL, application type, or cookie information. This added security feature complements firewalls and intrusion detection systems that cannot look into encrypted data.

Benefits

Simplicity

Alteon SSL VPN gateways are designed to simplify all elements of deployment and usability. The solution integrates seamlessly into any network without firewall reconfiguration and uses existing embedded browser technology on the client end to minimize installation, operational, and support headaches. A Web-based GUI provides an easy-to-use utility for device administration and user management. And scalability is provided through a tiered licensing model and scaling beyond the unit's capacity is a plug-and-play procedure with additional appliances. For users, accessing secure

applications is as simple as reaching a Web site using the familiar Web browser interface. An intuitive Web portal greets users to provide the necessary remote access functionality and application access.

High performance, availability, and scalability

For remote access environments that support mission-critical applications, the Alteon SSL VPN solution can be optimized by Alteon Application Switches. These switches address the requirement for high performance, availability, and scalability by incorporating intelligent traffic management into the solution. This capability allows for improved performance by load balancing SSL VPN devices and transparently re-directing remote users to the access point with the fastest response time. If one access point becomes unreachable, this high-availability solution will bring them to the next active site for uninterrupted service. By clustering SSL VPN devices, either locally or globally, enterprises are free to scale their remote access solution effortlessly as demand dictates.

Unrestricted mobility

Unlike traditional remote access solutions, the Alteon SSL VPN does not tie the user to any particular site, network, or end-user device. This unrestricted mobility provides more opportunities for mobile workers to stay in touch with their business—resulting in improved frequency of communications with employees and customers. Similarly, partner access is not restricted to a particular device for simplified business-to-business (B2B) process integration.

Lower total cost of ownership

Simplicity translates directly into cost savings. The Alteon SSL VPN solution operates above the transport layer to minimize dependencies and utilize the services of existing infrastructure. Dial-up and dedicated circuit costs are mitigated by using the Internet for connectivity. And without the added cost of installing and managing client software, total cost of ownership can be reduced to a fraction of the cost of alternative solutions. Offloading the public key operations to optimized hardware lowers the cost of supporting the SSL sessions themselves by up to 70 percent.

Breadth of application support

The Enhanced Clientless and Transparent modes of operation improve the breadth of applications available to remote users beyond just Web applications. By combining SSL with application-layer proxies, the Alteon SSL VPN solution provides enterprises with secure remote access to terminal services, client/server, mainframe, and UDP applications.

Primary applications

Business extranets

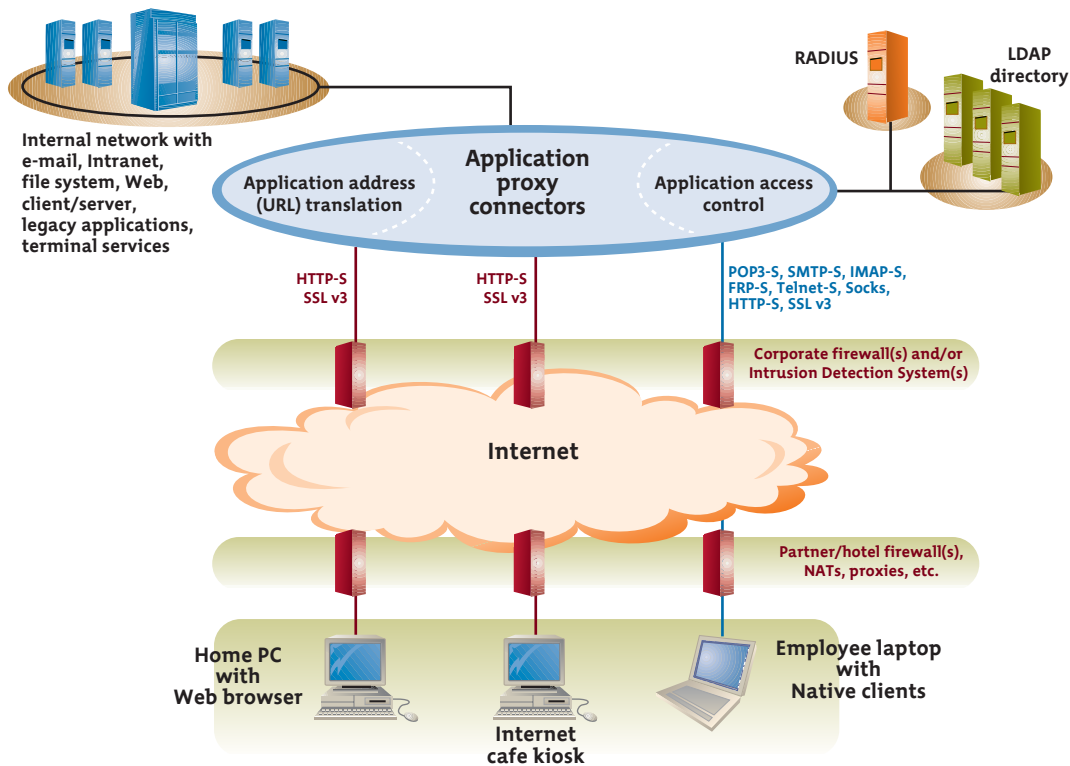
Integrating business partners with existing production systems can streamline supply chains and reduce inventory and production cycles. But providing business partners with a simple, secure connection to a particular production application can be difficult. The Alteon SSL VPN provides low-cost, secure partner access that does not require any additional tunneling software to be installed and maintained on partner PCs. Communications on TCP port 443 can traverse firewalls without interruption and granular access control binds users to particular applications, mitigating the need to police partner access. Partners appreciate the ability to access inventory and scheduling information from multiple locations rather than specific dedicated machines.

Customer services

Providing customer services and support via the Internet is common practice. The Alteon SSL VPN provides enterprises with the ability to enhance Web-based customer services without compromising security. By incorporating client authentication and granular access control, enterprises are free to offer customers a rich, personalized experience and share sensitive data to improve customer acquisition and retention.

Sample application	Mode of operation		
	Clientless <i>Browser only</i>	Enhanced Clientless <i>Browser+Java</i>	Transparent <i>SSL Client</i>
Web mail	✓	✓	✓
Native e-mail		✓	✓
File sharing	✓	✓	✓
Intranet	✓	✓	✓
Web applications	✓	✓	✓
Terminal services (WTS, Citrix, etc.)		✓	✓
Terminal services (VT100/320, TN3270/5250)		✓	✓
UDP applications			✓
JavaScript	✓	✓	✓
Client/server		✓	✓

Figure 2. The Alteon SSL VPN gateway establishes secure client-to-application sessions through standard firewall, proxy, and NAT services.



Telecommuters

Telecommuting provides employee flexibility and improves productivity. Many employees that work remotely take advantage of today's inexpensive cable or DSL broadband access services. Casual telecommuters that work from home often use their residential broadband connections in conjunction with secure client tunneling software to provide a remote access VPN solution. In search of incremental revenues, Internet Service Providers (ISPs) are now cracking down on these workers by blocking IPSec ports on non-commercial ISP accounts; forcing users to upgrade to a telecommuter service at up to twice the cost. The Alteon SSL VPN solution allows telecommuters to access their applications through any available Internet access service without the concern of blocked ports. By only using standard Internet traffic for secure communications, client-to-application sessions can be established through all standard firewall, proxy, and NAT services.

Mobile employees

Mobile employees are frequent travelers that require access to a broad range of applications. Primary applications include e-mail, scheduling, file transfer, and popular Customer Relationship Management (CRM), or Sales Force Automation (SFA) applications. With limited opportunity to dial-in or find a "friendly" Internet drop that will support their secure client, traditional remote access solutions can show their shortcomings in mobile applications. The Alteon SSL VPN solution provides true freedom of mobility by giving mobile workers more opportunities to communicate and share information. Workers can access applications from their portable laptop computer, a PC at a customer site, Web browser equipped PDA, or any available Internet kiosk at hotels, airports, or convention centers.

Security within the perimeter

Not all applications on a corporate network require the same level of security. Subscription or license-based databases have strict access constraints, departmental applications contain sensitive information, Human Resources applications provide confidential personal data, and financial systems require restricted access. These applications, among many others, warrant additional security within the corporate network. The Alteon SSL VPN solution can provide application-specific authentication for internal access control, and client-to-application encryption within the private network for confidentiality and privacy. This additional level of security can protect sensitive data and applications from internal risks.

For more invitation, visit:
www.nortelnetworks.com/alteon

In the United States:

Nortel Networks
35 Davis Drive
Research Triangle Park, NC 27709
USA

In Canada:

Nortel Networks
8200 Dixie Road,
Suite 100
Brampton, Ontario L6T 5P6
Canada

In Caribbean and Latin America:

Nortel Networks
1500 Concorde Terrace
Sunrise, FL 33323
USA

In Europe:

Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead Berkshire SL6 3QH
UK

In Asia:

Nortel Networks Asia
6/F Cityplaza 4,
Taikooshing,
12 Taikoo Wan Road,
Hong Kong

The logo for Nortel Networks, featuring the word "NORTEL" in a bold, blue, sans-serif font with a stylized globe icon integrated into the letter "O". Below it, the word "NETWORKS" is written in a similar bold, blue, sans-serif font with a trademark symbol (TM) to its upper right.

NORTEL NETWORKS™

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at:

www.nortelnetworks.com

For more information, contact your Nortel Networks representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

**GSA Schedule GS-35F-0140L
1-888-GSA-NTEL**

*Nortel Networks, the Nortel Networks logo, the globemark design, and Alteon are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2003 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

NN102960-073103