

SECURE

Product Bulletin

Nortel Networks SSL VPN Module 1000

Extending secure remote access options for Contivity customers

SSL VPN Module 1000 overview

The Nortel Networks SSL VPN Module 1000 is a remote access security solution that extends the reach of enterprise applications and resources to remote employees, partners, and customers. By using the native capability of widely deployed Web browsers, the SSL VPN Module 1000 offers a convenient clientless-based alternative for providing secure access to remote users, without the need to install and manage client tunneling software on their PCs.

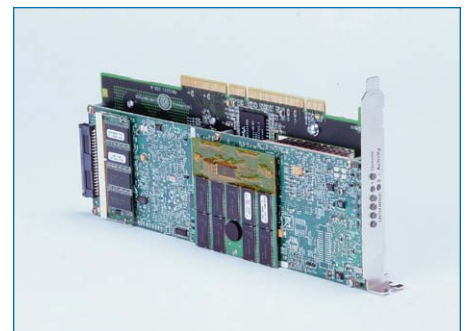
Nortel Networks Contivity* customers can now extend hybrid IPSec and SSL-based remote access to new and existing remote access deployment requirements. The SSL VPN Module 1000 leverages the same Contivity VPN administration and authentication that the enterprise currently uses for their existing IPSec VPN deployment.

Unlike other hybrid SSL/IPSec solutions in the market that offer limited features and low scalability, the SSL VPN Module 1000 incorporates optimized SSL hardware and a proven fully-featured third-generation SSL VPN implementation to deliver uncompromising levels of performance and scalability without adversely impacting other key functions on the Contivity platform. For example, client and branch IPSec VPN, firewall, and dynamic routing are not impacted by the intense processing demands of SSL VPN.

Supported by the Contivity 5.0 release, the SSL VPN Module 1000 takes limiting and complex technology choices “off the table” for enterprises, allowing them to instead deploy solutions that meet their broad deployment requirements (IPSec and SSL)—rather than forcing them to choose one technology or protocol over another.

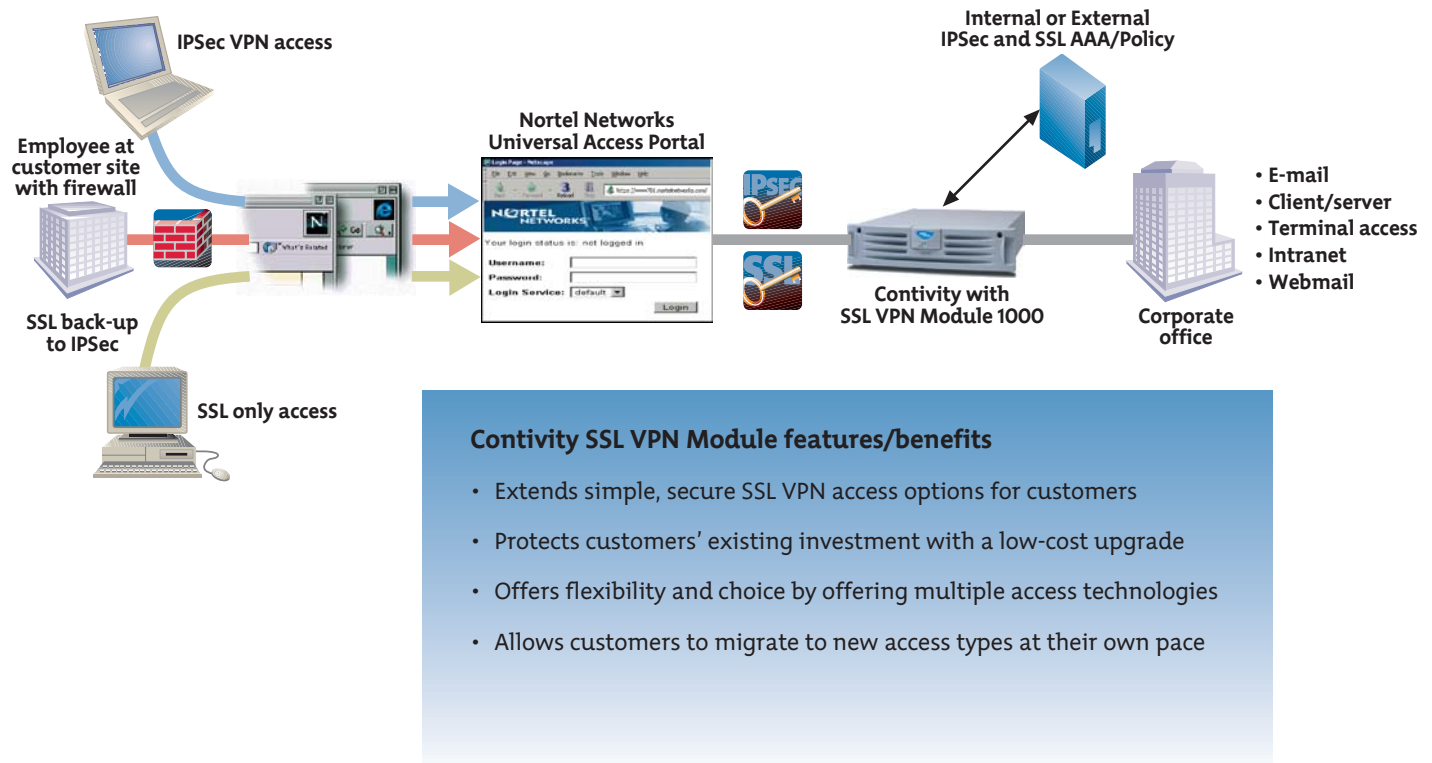
SSL VPN Module 1000 customer benefits

- Dedicated hardware-based SSL VPN add-on module designed for SSL VPN performance and scalability (up to 1,000 SSL VPN users) without impacting other critical security and routing Contivity gateway functions
- Protects customers' investment by allowing them to incrementally add SSL VPN capabilities to their existing (IPSec) remote access deployments and migrate to other access options as it makes sense
- Simplified, common administration for both IPSec and SSL VPN users with current Contivity VPN Web GUI within current deployment model
- Flexibility and choice—allows customers to leverage the most appropriate VPN technology to meet the remote access requirement (IPSec, SSL, or both)
- Industry-leading SSL VPN feature set that provides clientless remote access, on-the-fly content transformation, and browser-based tunneling of legacy applications



SSL VPN Module 1000

Figure 1. Contivity SSL VPN Module 1000 in action



Contivity SSL VPN Module features/benefits

- Extends simple, secure SSL VPN access options for customers
- Protects customers' existing investment with a low-cost upgrade
- Offers flexibility and choice by offering multiple access technologies
- Allows customers to migrate to new access types at their own pace

SSL VPN Module 1000 key features

Simplified administration and common user experience

The SSL VPN Module 1000 supports the Nortel Networks Universal Access Portal (see Figure 2) to further simplify the VPN user experience by transparently invoking the most appropriate VPN access method (IPSec or SSL) based on the user's access situation and/or the corporate resources they are trying to access.

For example, an administrator can configure mobile employees to always default to the standard Contivity IPSec VPN access, but in the event that IPSec cannot traverse a firewall or NAT function at some point in the network, the Universal Access Portal will seamlessly initiate an SSL VPN connection instead, allowing the user to access certain links, resources, and applications that they had authorization to access.

Although many enterprises might want to take advantage of the flexibility and usability of this new type of portal-based remote access paradigm (with pre-defined links, applications and resources), users can still operate the traditional Contivity IPSec VPN Client as they have always done in the past by simply gaining Internet access and double-clicking on the Contivity VPN Client icon.

Authentication

Enterprises using Contivity do not need to re-create user profiles when provisioning an SSL VPN Module 1000—the existing user profiles can be used to provide authentication and authorization for SSL VPN users.

The SSL VPN Module 1000 provides multiple authentication options including support for common authentication mechanisms such as LDAP, RADIUS, and Active Directory services. Alternatively, the SSL VPN Module 1000 can support the use of digital certificates. An enterprise can issue its client certificates with the option of having them validated by a certificate authority for enhanced authentication. And for the strongest levels of authentication, the SSL VPN Module 1000 supports token-based systems such as Secure Computing SafeWord™ and RSA SecurID®.

Application-layer proxy

The SSL VPN Module 1000 provides a high degree of mobility by enabling secure remote access to a broad range of applications from common Web browsers. Most businesses still rely on a range of client/server and legacy applications that are core to their operations and need to be accessed by remote employees. The SSL VPN Module 1000 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.

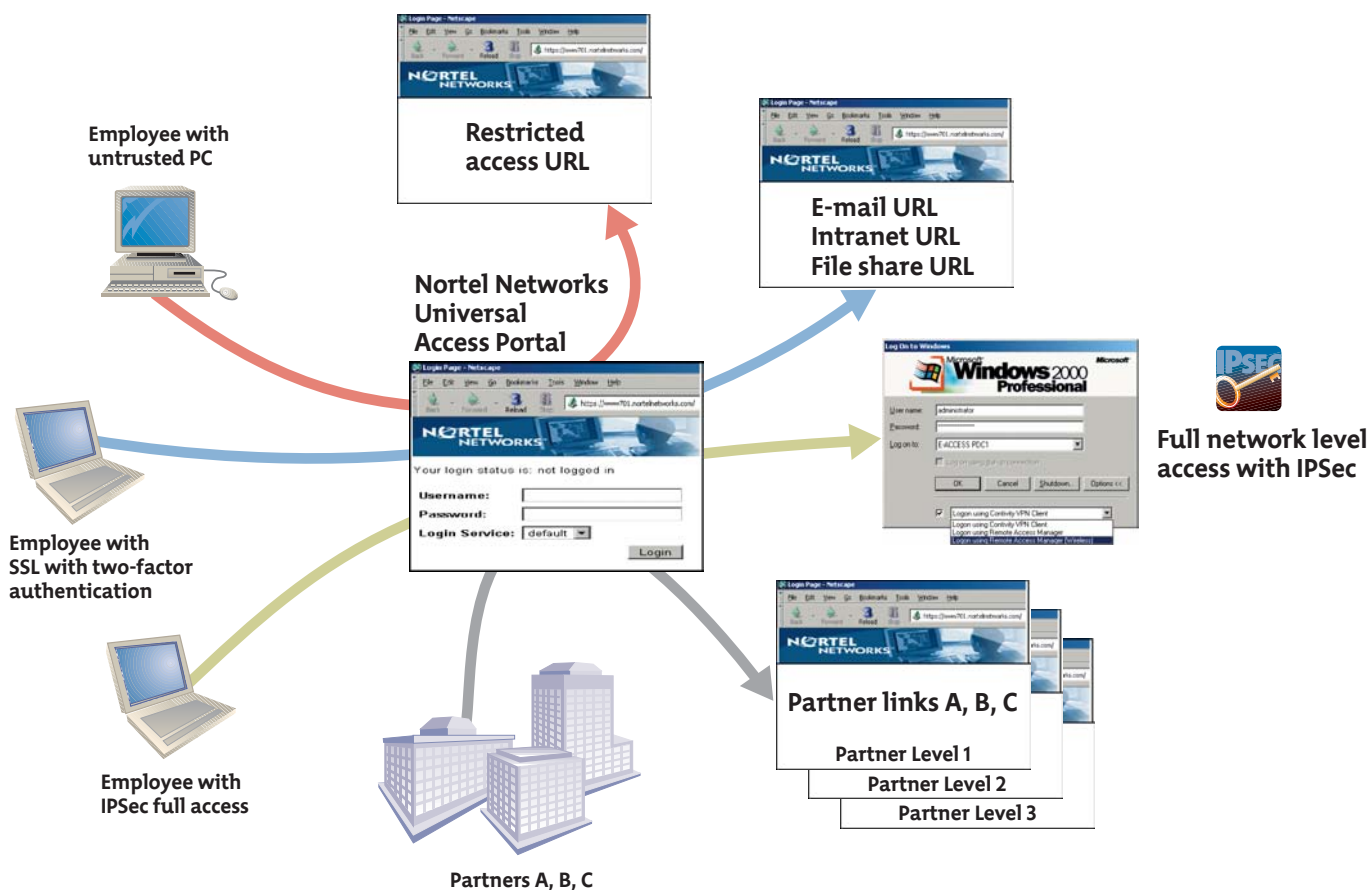
Clientless/enhanced browser modes

Web browsers themselves run on many different types of end-user devices, including PCs, Pocket PCs, PDAs, and cell phones. Even among common devices, the individual client configuration can prevent a particular browser from accepting or running a Java applet. To ensure support for the broadest range of applications, the SSL VPN Module 1000 adapts the session type to the potential capability of a particular client.

Client security

The SSL VPN Module 1000 provides a suite of safeguard features to protect against malicious intent and user negligence. A dynamic access policy 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, a cache-wiper feature is put on stand-by 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 SSL VPN Module 1000 will terminate any inactive connection after a brief countdown warning. This feature reduces the chance that a subsequent kiosk user could get access to the previous user's confidential session.

Figure 2. Nortel Networks Universal Access Portal—Delivering centralized and customized secure access



VPN load balancing

The SSL VPN Module 1000 can be deployed in multiple geographically distributed locations to provide redundant access points to the private network. By incorporating Nortel Networks 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.

Granular access control and auditing

The SSL VPN Module 1000 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 the 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. The SSL VPN Module 1000 aggregates a high number of SSL sessions and incorporates Nortel Networks proven hardware-assisted SSL acceleration technology to maintain peak application performance.

Advanced content transformation

The SSL VPN Module 1000 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.

Advanced filtering

The SSL VPN Module 1000 provides 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.

Summary

Nortel Networks Contivity Secure IP Services Gateway 5.0 Product Release delivers on Nortel Networks Secure Mobility vision by addressing our customers' continued requirement to extend secure and highly mobile remote access to an ever-growing population of users, locations, device types, and use cases.

For customers with existing Contivity IPsec VPN deployments, the SSL VPN Module 1000 provides new levels of deployment flexibility coupled with simplified end-user support requirements by leveraging the SSL VPN "clientless"-based access paradigm without having to deploy a second SSL-specific device or infrastructure.

Customers with SSL only and/or specific application-oriented access requirements should consider deploying the Nortel Networks VPN Gateway 3050, which is specifically designed to support these types of SSL VPN requirements.

Product specifications

The SSL VPN Module 1000 is a PCI-based card that fits into the PCI slot on Contivity 5000, 2700, and 1740.

Module specifications

- Pentium III 933 MHz; 512 MB RAM; 30 GB hard drive
- Mounted on PCI carrier card

Card comes loaded with Nortel Networks 4.2 SSL VPN software.

Performance

Maximum number of users

- 1,000 concurrent SSL connections

Encrypted throughput

- 3DES/RC4 (168 bit) 125 Mbps (approximately)

Maximum SSL transactions per second

- 600 TPS

Security features

Authentication

- RADIUS, including Challenge/Response
- LDAP
- Windows NT Domain (NTLM)
- Native local user database
- Secure Computing SafeWord (RADIUS)
- RSA SecurID
- ActivCard (RADIUS)
- Microsoft Active Directory (RADIUS or LDAP)
- Novell NDS/eDirectory (LDAP)
- Netegrity SiteMinder
- X.509 Digital Certificate (client and user)

Authorization

- Support two authorization profiles—base and extended
- Base profile includes network, service and application-level information (Layer 3, 4/7)
- Extended profile adds source network and authentication method

Security protocols

- SSL v2.0,3.0
- TLS 1.0 (RFC 2246)

Cipher suites

All ciphers covered by SSLv2.0, 3.0, and TLSv1.0, except the IDEA ciphers and the FORTEZZA ciphers

Accounting

Syslog/RADIUS account start and stop including username, gateway address, session ID, session time, and cause of termination

Client security

- Auto-logout with countdown prompt
- Rewriting to no-cache/no-store headers
- Cache cleansing of files and history (Only for Microsoft IE browsers)
- Dynamic access policies

Load balancing

- Source IP, round robin, least connections

Session persistence

- Source IP, SSL session ID, cookie information

Application health checking

- SSL w/TCP/IP/port
- Scriptable, configurable intervals

Application support/management

Web content and protocols

- HTML/DHTML
- JavaScript/Java Applets/XML
- HTTP/HTTPS
- VBScript

File share protocols

- Windows – SMB/CIFS
- Generic – FTP

E-mail/messaging protocols

- Microsoft Exchange (MAPI)
- IBM/Lotus Domino/Notes
- IMAP, SMTP, and POP3

Terminal access protocols

- Telnet
- SSH

Remote desktop protocols

- Citrix ICA
- Microsoft WTS (RDP)

Management

- Secure administrative Web GUI (HTTPS)
- Serial port to CLI
- SNMP v2
- Local logging, external Syslog

Web portal customization

- Hexadecimal color customizable
- Company logo (.gif), text
- Novice/Int/Advanced user views
- Portal pass-through

Browser support

Windows:

- MS IE 5.01/5.5/6.0 with Sun's JRE 1.3.x/1.4.x
- MS IE 5.01/5.5/6.0 with MS's JVM 4.x/5.x
- Mozilla 1.x with Sun's JRE 1.3.x/1.4.x
- Netscape Navigator 7.x with Sun's JRE 1.3.x/1.4.x
- Netscape Navigator 4.78 and 4.8 only with built-in Java engine

Unix:

- Mozilla 1.x with Sun's JRE 1.3.x/1.4.x
- Netscape Navigator 7.x with Sun's JRE 1.3.x/1.4.x
- Netscape Navigator 4.78 and 4.8 only with built-in Java engine

Other

Modes of operation

- Clientless – HTML to Browser
- Enhanced Clientless – Proxy with Java Applet
- Transparent – Client-based SSL
- Network – IPSec termination

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
Level 5, 495 Victoria Avenue, Chatswood, NSW, 2067, Australia, Phone: +61 2 8870 5200

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.

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

Copyright © 2004 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.

NN108262-050604

