

Nokia Secure Access System

Nokia Secure Access System is an SSL remote access solution that enables an enterprise to provide secure, authenticated, and controlled access to any intranet or extranet from browser-based devices connected to the Internet.

With mobility comes increased freedom and efficiency for the business user—but also new challenges for the IT department. CIOs and IT Managers are faced with reducing costs and meeting the demands of these users by allowing anytime, anywhere access to needed corporate information, regardless of the access device. The same technology that can meet these needs can also put corporate assets at risk. A new problem emerges—that of knowing the identity of the user, the type of access device they are using, and how secure that device is—so that only *selected and appropriate* content can be accessed, locally stored and/or uploaded back to the network.

Nokia uniquely provides a portfolio of system level Mobile Connectivity solutions based on both IPSec and SSL-based technologies designed to enable IT departments to apply the right solution to specific problems.

A key component of that portfolio—Nokia Secure Access System—provides enterprises with cost effective SSL browser based

access to corporate email and applications for employees and partners. With Nokia, enterprises can control what information can be accessed, locally stored, and/or uploaded to the network based on who the user is, what device they are using, and how secure that device is at a given time. Nokia enables the freedom to do business—anywhere, anytime, and from any device while ensuring the integrity of the network.

Business Benefits

Increase productivity and reduce time-to-market: Enterprises can securely connect mobile employees, telecommuters and employees who do not have enterprise-issued devices using Nokia Secure Access System. It streamlines information flow and optimizes business processes.

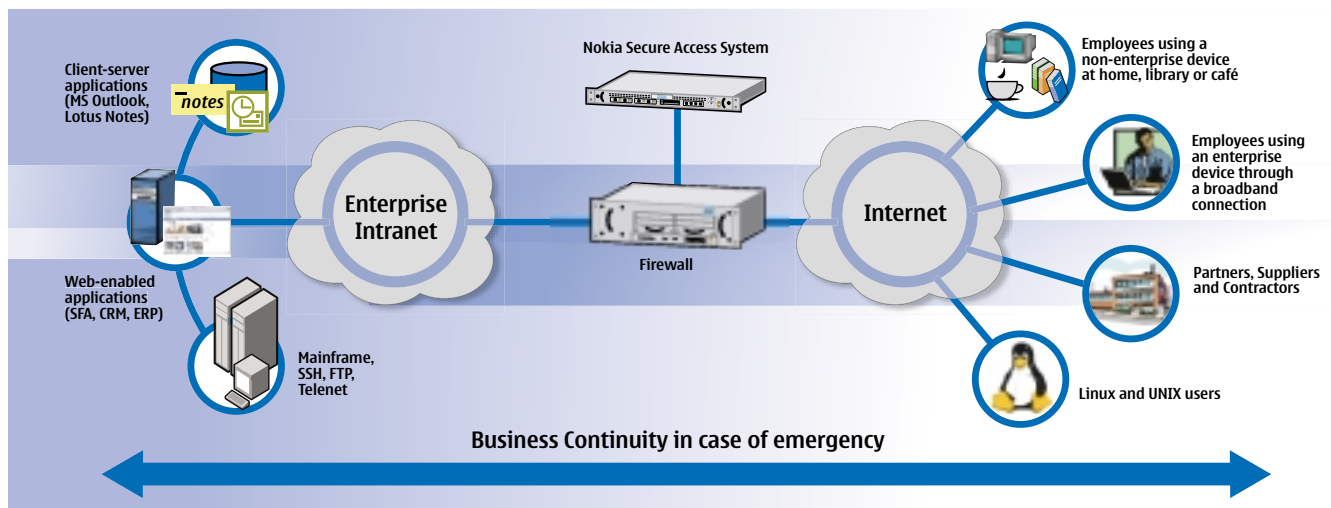
Reduce total cost of remote access: A significant cost of remote access systems comes from the distribution and management of numerous clients. By utilizing standard SSL browsers, Nokia Secure Access System enables easy management and ROI.

Protect enterprise information assets: When connecting partners with different VPN infrastructure, enterprises may be faced with using static IP routes through the firewalls. This short-term solution can become insecure and complex to manage as the number of partners increases and because it may leave open ports through the firewall. Nokia Secure Access System provides a simple scalable way to connect partners to specific enterprise applications without the need to build static routes or to deploy common VPN infrastructure.

Mobilize information: Intranets and extranets are widely deployed in the enterprise today. Email and mission-critical applications can be mobilized and delivered through any corporate or non-corporate device connected to the Internet to increase the availability of information.

Key Features and Benefits

Advanced Access Control: Nokia Secure Access System uniquely improves security by providing connection state-based access control. The level of access for the remote



NOKIA
CONNECTING PEOPLE

user can be increased or decreased depending upon the result of the Client Integrity Scan or presence of a digital certificate. A user may be allowed access to upload and download files only if the remote device has a certain level of anti-virus protection. The presence of a client-side digital certificate uniquely identifying a remote device can also govern the level of authorization granted to the user. Configuration of access control is simplified through the ability to add users and groups directly to resources.

Client Integrity Scan: A unique feature of Nokia Secure Access System, it scans the remote device for open TCP ports, bad files, good files and active processes to improve security of enterprise data. An unusual open port may indicate the presence of a trojan on the remote device. Known viruses and worms are examples of bad files. Good files are indicated by presence of the latest anti-virus definitions. The Windows task list can show an active process, such as a personal firewall, is up and running and can indicate the activity of suspicious software.

Session Persistence: A unique feature of Nokia Secure Access System, Session Persistence allows users to resume work without losing data if their SSL session has timed out due to lack of activity. There is no concern if a user is interrupted while connected through Nokia Secure Access System.

Authentication and Audit:

- Enables certificate-based authentication and authorization and allows the administrator to deploy multiple client certificates for a single user ID. An administrator can set up different levels of authorization for the same user, depending on the identity of the remote device.
- Allows the administrator to configure access by assigning users and groups directly to resources to simplify management. The administrator can also deploy two-factor authentication through SecureID over RADIUS.

- Provides support for a wide range of authentication methods including local, RADIUS, LDAP, NTLM and NIS.
- Keeps detailed logs of user activity, which can be posted to the syslog server with an option to log system events only.

Uses Standard Web-Browser as Client:

Widely deployed SSL-enabled browsers eliminate the need for distribution of remote clients. It improves security while reducing cost and the complexity of managing a corporate remote access system.

SSL Encryption: By combining access control, authentication and audit with SSL cryptography, as well as integrating unique security and productivity features, the Nokia solution enables secure, authenticated and controlled access to enterprise applications from any device with a web-browser connected to the Internet. SSL technology is used on the Internet to secure billions of dollars worth of transactions each year. By leveraging this widely available technology, Nokia Secure Access System increases the ROI of enterprise remote access systems.

Port-Forwarding Proxy: With Nokia Secure Access System, enterprises can connect client-server applications to partners and employees securely. Employees with laptops who are connecting from a remote location can use Nokia Secure Access System to access email using an MS Outlook client. A contract manufacturer running the ERP client can be connected securely to enter up-to-the-minute production data.

Benefits of the Nokia Complete System Approach: By leveraging the well-established Nokia complete system approach, Nokia Secure Access System brings security, reliability and manageability to the SSL remote access marketplace. Nokia IP Security Platforms have been trusted globally by leading companies and service providers to run mission critical firewall, VPN and IDS functions. Nokia Secure Access System is backed by an SCP-certified global support and services organization.

Specifications

Supported Nokia IP Security Platforms and Operating System

- Nokia IPSO™ 3.7
- Nokia IP130
- Nokia IP350
- Nokia IP380

Security Features

- Secure appliance with hardened Nokia IPSO operating system
- Access security through SSL2.0/TLS 1.0 encryption
- Supported encryption algorithms: 3DES, RC4, AES
- Advanced Access Control
 - Connection-state based authorization
 - Dynamically adjusts the level of access depending upon identity of remote device
- Client Integrity Scan
- Encrypts login information
- Non-caching operational mode
- Multiple Ethernet ports for physical security partitioning

Authentication and Audit Features

- Wide range of authentication methods: Local, RADIUS, LDAP, NTLM, NIS
- Two-factor authentication: SecureID over RADIUS
- X.509 client-side certificates
- Assign multiple certificates to single UserID
- Users/Groups to resources
- Logging for events by user, applications, resource, time and event with option to log system events only
- Reports to syslog server

Application Support Features

- Browsers: IE5.0 and upwards, Netscape 6.2x and 7.x, Mozilla 2.0
- Web protocols: HTML, Java Applets, JavaScript, HTTP/HTTPS, DHTML, VBScript
- File sharing protocols: Windows (CIFS), UNIX (NFS), FTP
- Client-server applications: MS Exchange, Lotus Notes
- Email and File transfer protocols: SMTP, POP, IMAP
- Terminal emulation protocols: Telnet, VT100, TN 3270

Management and Ease of Use Features

- Web-based management interface
- Telnet, FTP, HTTPS, SSH for configuration and management
- Nokia Horizon Manager 1.3 for backup, restore and push application package
- Transparent mode maps external URLs
- Session persistence prevents data loss due to SSL timeout

Americas
Tel: 1 877 997 9199
Email: ipsecurity.na@nokia.com

Asia Pacific
Tel: +65 6588 3364
Email: ipsecurity.apac@nokia.com

Europe, Middle East and Africa
France +33 170 708 166
UK +44 161 601 8908
Email: ipsecurity.emea@nokia.com

NOKIA
CONNECTING PEOPLE