



Cyberoam SSL VPN Plus

The Third-Generation VPN



Enterprises need to extend their application and data resources to remote users for true business mobility and employee productivity. However, easy mobility and accessibility of network resources to a vast number of users leads to serious security concerns. Cyberoam's SSL VPN appliances scan end points for outdated and non-compliant software or configurations, before admitting them to the enterprise network. This ensures remote end points remain secure and compliant with regulatory requirements of GLBA, HIPAA, PCI DSS and others.

Unlike IPSec VPNs that give full access to resources once users are within the network, Cyberoam's SSL VPN delivers granular, identity-based network access control to branch offices and other remote users for greater security. IPSec VPNs require mobile users to install VPN software client, demanding administrator support and restricting anywhere network access. Cyberoam's third-generation VPN offers clientless, easy to use and scalable solution for all types of users viz. branch office users, guests, partners, traveling users, and others.

"Cyberoam's SSL VPN Gateways deliver all the advantages of SSL VPNs user mobility, ease-of-use, policy-based resource access control and zero-client administration - plus the low latency, high data throughput and universal application support previously available only with IPsec VPNs."

Powered by NeoAccel

Cyberoam SSL VPN Plus

Cyberoam's SSL VPN solution is architected to address the deficiencies found in today's remote access solutions: lack of performance, security, return on investment and ease of use. The third-generation VPN appliances deliver flexibility and zero-client administration along with the functional and performance benefits of conventional IPSec VPNs. Faster and easier to deploy than IPSec VPNs, they reduce costs and increase IT control by eliminating the configuration, management and support complexities of IPSec VPN clients. They are most suitable for mobile devices, lossy wireless networks and enterprises requiring IPSec-VPN replacements.

Product Range

The Cyberoam SSL VPN family includes the CR-SGX800, CR-SGX1200 and CR-SGX2400, each with increasing capacity and performance. The Cyberoam Gateways support both remote access VPN users and site-to-site VPN connections. The capacity of each gateway can be expanded at any time, after installation, with software license upgrades up to the maximum capacity of each appliance.

Feature	CR-SGX800	CR-SGX1200	CR-SGX2400
Market	Entry-Level	Small-Medium Enterprise	Enterprise
Concurrent Users	Up to 50	Up to 250	Up to 2000
Throughput	100Mbps	250 Mbps	500 Mbps
Operating System	NHOS*	NHOS*	NHOS*
Gigabit Interfaces	2	2	4
High Availability	Yes	Yes	Yes
Hardware Acceleration	-	-	✓
Dual Power Supply	-	-	✓
Dual Hard Drives	-	-	✓

*NeoAccel Hardened OS

Features and Benefits

High Performance and Capacity

Cyberoam delivers all the advantages of SSL VPNs at speeds faster than IPsec VPNs. Conventional SSL VPN solutions suffer performance issues due to redundant tunneling of data, excessive packet processing and unnecessary data compression. Unique single-tunneling of data eliminates performance-degrading TCP-over-TCP meltdown. Kernel level-only processing of data eliminates excessive packet processing overhead and dynamic compression determines when compression is beneficial. Capacity of up to thousands of concurrent users per gateway, with ultra-fast response times and ultra-low latency, addresses the largest of deployments.

Endpoint Security

All endpoints are subjected to policy-based compliance checks before they are admitted to a network. Hundreds of pre-defined checks for updated operating system and security software, malware presence, and more, are done before authentication. Additional checks are easily configured. This ensures robust network security even when users access the network from home, public places like the Internet cafes or Wi-Fi zones, partner networks and more.

Return on Investment

Cyberoam's SSL VPNs eliminate client-side installs and updates, offering ease of use and secure remote access. Automatic re-connection between user and gateways and high availability clustering ensure continuous access to critical applications and data.

Full Access to All Applications

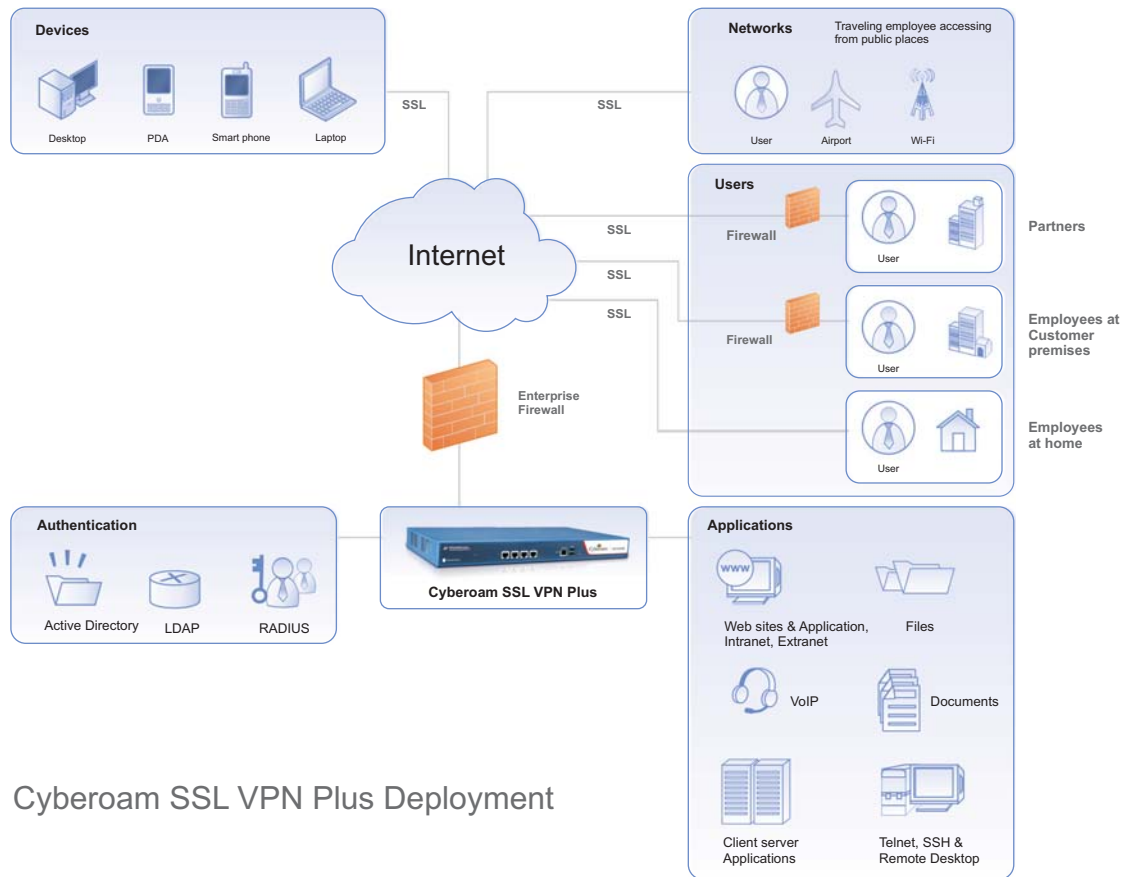
All enterprise applications are supported - full applications, Web applications, thin clients, fat-clients and legacy applications - hence only a single remote access solution is required.

Granular Network access

Powerful and easy policy management governs all network access, based on user and group policies. Security zones, with access control, provide flexibility and granularity of network access.

Ease of Use

Four modes of access provide as much, or as little, access as needed with minimal yet central configuration. The third-generation Cyberoam SSL VPNs support the most popular enterprise platforms Windows®, Mac OS and Linux® ensuring no user is left behind. Deployment into existing networks is facilitated by support of existing authentication solutions.



Cyberoam SSL VPN Plus Deployment

Who Requires Cyberoam SSL-VPN Plus

The need for client software installation and administrative support with IPSec VPNs has resulted in existing users wishing to upgrade their legacy VPNs. Enterprises need better ease of use, flexibility in levels of access, and anywhere anytime secure access to all applications and data on the network for their users.

Cyberoam SSL VPN's advanced technology makes it a true IPSec replacement as it overcomes performance limitations of conventional SSL VPNs with high performance, end-point security and granular access.

Remote/ Mobile Workforce

Enterprises need to provide secure, anywhere access to their remote or mobile workforce for all types of applications and end clients viz. PDA, smart phones, and more, leading to security concerns. Information leakage can result in financial loss, loss of customer trust and negative brand image for these enterprises.

Cyberoam's advanced SSL VPN solution offers secure network access to road warriors, tele-commuters and branch offices. Logs with user identity-based network access details like username, date and time of access, destination and source IP address and more allow you to securely extend your network with the knowledge of who is remotely accessing what in your network helping you meet regulatory compliance requirements.

Extending Company Extranet

Companies need to extend their network resources, not only to their own remote offices but also to third parties like partners, suppliers, prospective customers and more, to do business in real time. They need a secure and easily deployable solution requiring minimum administrative support and overhead costs.

Cyberoam's SSL VPN appliances enable you to offer 'anytime - anywhere secure access to your extranet. This helps you save tremendously on overhead costs of doing business and facilitates quick exchange of business information between your main office and business associates at various locations.

Guest Users

One of the limitations of IPSec VPN is that it doesn't allow different levels of access controls for network resources. Enterprises are thus forced to grant full access to remote or third-party users, exposing their network resources to all users alike.

Cyberoam's SSL VPN allows granular access controls through customized, resource-specific access policies by username or group. This allows you to provide third-party access to only the desired resource or application in your network, making your network safer.

Technical Specifications

Throughput and Capacity

Throughput

- CR-SGX800	100Mbps
- CR-SGX1200	250Mbps
- CR-SGX2400	500Mbps

Capacity:

- CR-SGX800 - Up to 50 Concurrent Users
- CR-SGX1200 - Up to 250 Concurrent Users
- CR-SGX2400 - Up to 2,000 Concurrent Users

- Logins/Second 1,800
- SSL Transactions/Sec 8,400
- Latency <10ms

Application Support

- All IP-based applications (TCP, UDP)
- Web-enabled applications
- Dynamic IP and port-based applications
- Legacy mainframe applications

Access Control Based on

- Internal/external group membership
- Block cut/copy/paste/print screen
- Protocol, IP address, time schedule
- Security Policies

Protocols

- SSL 3.0 and TLS 1.0
- Remote access VPNs
- Full, Split Tunneling, Local LAN Exception
- Encryption: DES, 3DES, AES (256), RC4
- Authentication: MD-5, SHA-1, RSA 1024, RSA 2048

Remote Access Methods

Web Access Terminal (WAT)

- For use with all browser-based applications
- Access through Web portal
- SSL VPN-Plus End Point Security enabled
- Access via any SSL-enabled browser
- Clientless

Virtual Application Terminal (VAT)

- For use with remote login and virtual desktop applications
- SSH, Telnet, Windows RDP, VNC

- Access via any SSL-enabled browser
- Session-only Java applets used
- Access through Web portal
- SSL VPN-Plus End Point Security enabled

Quick access terminal (QAT)

- For client-initiated TCP-based applications
- Access through Web portal
- SSL VPN-Plus End Point Security enabled
- Access via Microsoft Internet Explorer
- Java client

Full access terminal (PHAT)

- For use with all IP-based (TCP, UDP) applications
- Access via small footprint client (2MB footprint)
- Windows 2000, Windows XP, MacOS X, Linux
- Optional Access through Web Portal
- SSL VPN-Plus End Point Security enabled
- Layer 2-7 access controls

Endpoint Security Enforcement

Up to 40 Security Zones based on:

- Access control policy per group/user
- End point security policy compliance

Authentication

- Local database
- RADIUS
- LDAP
- Microsoft Active Directory
- RSA SecurID
- SSL Client via digital certificates
- Two-factor authentication via PKI, tokens

Pre-configured enforcement policies

- Anti-spyware (updated and active)
- Anti-spam (updated and active)
- Desktop search engine presence
- Inbound port scanning
- IP forwarding
- Microsoft Windows
- Service Packs (presence and updated)
- Security patches (presence and updated)
- Firewall enabled
- Automatic Update activated
- Internet Explorer security settings
- Network Bridge enabled

- Personal firewalls (presence and updated)
- Cache cleaning
- URL history
- Temporary Internet files
- Downloaded program files
- Stored cookies
- Virtual keyboard to prevent keylogging

Pre-configured enforcement rules

- By :files / process / registry entry / ports / service

Web Portal

Launch

- Desktop applications
- Web Applications
- Remote login and virtual desktop applications Tools

Networking

- Static routing
- Dynamic routing: RIP v1/v2, OSPF
- DHCP
- Address Pools
- Network Address Translation (NAT, NAPT)
- NTP
- 802.1q VLANs

High Availability

- Active/Passive

Device Management

- Single-user and role-based
- Command line interface
- Console, SSHv2
- Java-Based Web user interface
- HTTP, HTTPS

Logging and Monitoring

- Local and external Syslog server logging
- Logging : IP, port, user, resources accessed, login failures, bandwidth usage
- Per-user statistics
- 3rd-party log analyzer-compatible