



Cyberoam SSL VPN



Cyberoam SSL VPN is an easy-to-use, simple application access and security solution for enabling high-trust, secure remote access to corporate applications and resources. Enterprises use Cyberoam SSL VPN to collaborate securely with employees, customers and partners.

Secure Application Gateway

Today, organizations of all sizes face the pressure of delivering applications and data to ever increasing numbers of mobile workers. Whether this is home users, roaming users, customers or partners, the need for a Secure Remote Access solution that is easy to use and yet secure is the key requirement; this is where Cyberoam SSL VPN can help.

When implementing the SSL VPN technology it is important for organizations to consider the technology. Current VPNs - either IPSec or SSL VPNs - rely on layer 2 VPNs to provide seamless access to applications. This creates a security hole in perimeter security deployed at corporate network and opens up the network to unknown vulnerabilities generated from unmanaged desktop machines. It should be noted that the requirement is to deliver the application and network services to end-users rather than necessarily bridging unknown endpoints placed at untrusted locations to the corporate network.

Cyberoam SSL VPN is an application gateway that provides secure access to the applications using standard-based SSL encryption. Cyberoam SSL VPN enables access only to specified applications rather than bridging the end-user's machine with the corporate network while maintaining full application compatibility. Cyberoam SSL VPN comes with unique network obfuscation feature which hides the internal network details from intentional or unintentional exploitation by a user or hacker.

Endpoint Security (Device Profiling)

The primary driving factor for wide adoption of SSL VPN is ubiquitous secure access from any device without any pre-requisites. However, this opens up a new challenge for organizations as unknown and unmanaged devices which could be potentially harmful devices can connect to corporate network. Moreover, compliance becomes a challenge as it becomes impossible to enforce corporate policies to end users.

Next generation SSL VPNs like Cyberoam SSL VPN bring strong device profiling features that measure and calibrate each endpoint connecting to the VPN against the corporate policies. Cyberoam SSL VPN provides a flexible policy framework for administrators to keep the corporate network safe from unclean devices either by keeping such devices out of the network, restricting them to a part of the network or remediating them to be able to access network services.

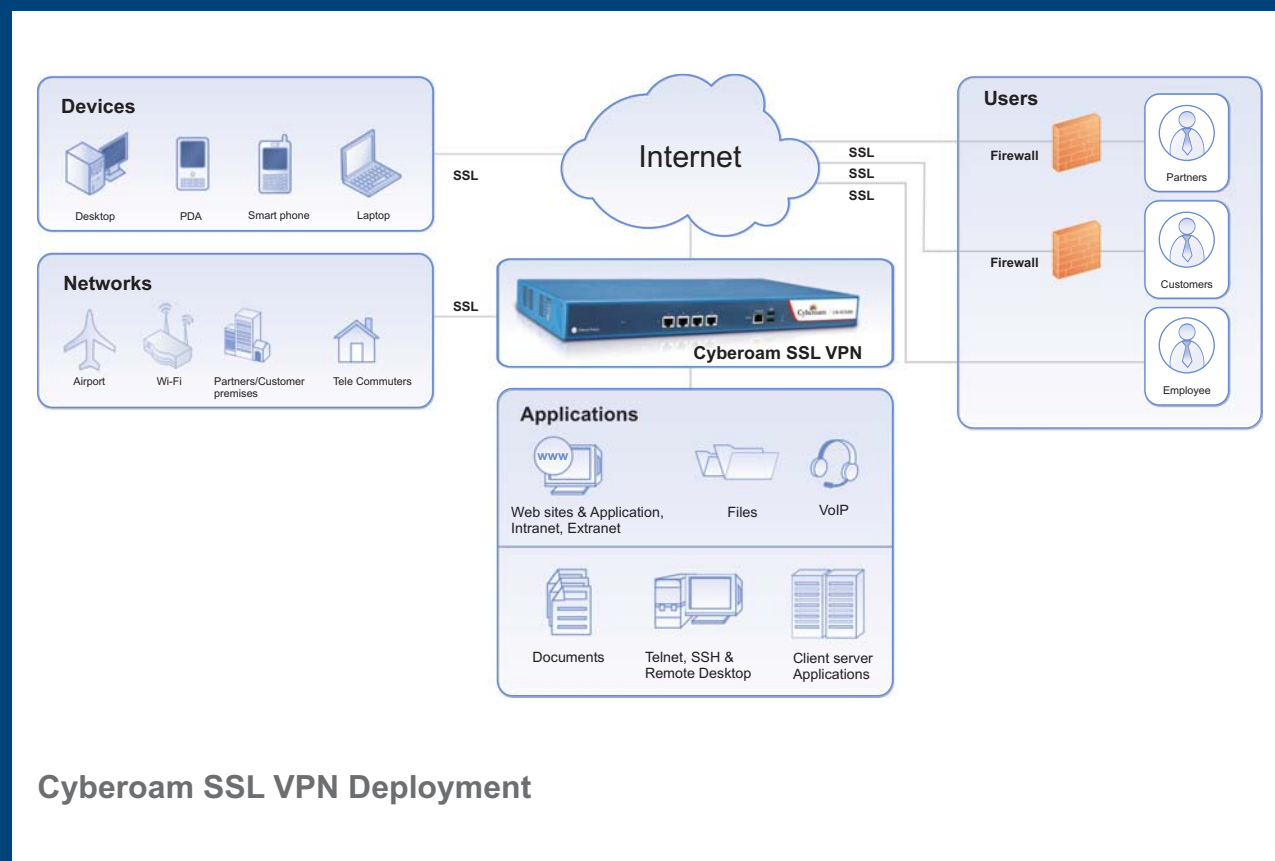
As part of device profiling, Cyberoam SSL VPN can check for status of endpoint security software like anti-virus, firewall and anti-spyware, OS and software updates and compliance to endpoint configurations. An intelligent cache wiper can clean the files and cache stored on the local hard disk by browsers or by users, including temporary folders or any of the drives. To protect from zero-day attacks, the Meta data about the latest virus signatures is pushed to the Cyberoam SSL VPN gateway every hour.

Granular Policy Control

An organization can have different types of users based on their location and their role. They can be trusted employees working from trusted or untrusted networks or they can be known partners, consultants who need access to applications from their location or workplace or they can be users completely unknown to the organization, requesting application access from just about any network. These users may use trusted or untrusted devices and may be working from trusted or untrusted networks. For each such use case, enterprises must protect the applications and network against unauthorized access and intentional or unintentional information leakage.

The remote access solution employed by the organization must provide a flexible and dynamic policy framework which can adjust on run time to accommodate users coming from different locations or devices but at the same time protect the applications in case the point of access becomes non-compliant to corporate security needs.

Cyberoam SSL VPN has a dynamic multi-layered policy engine that evaluates the user session at multiple levels before access to an application is granted. Each session is evaluated against policies set for the location of the user, method of authentication chosen by the user, trust level of the endpoint device and finally the role of the user. The evaluation is done on the fly and any application is restricted as per any of the failed criteria are hidden from the user.



Cyberoam SSL VPN Deployment

Key Features

Application Support allows access to virtually any application, including all TCP, 802.11x and UDP applications, Microsoft Outlook, FTP, Cyberoam TSE, and Microsoft Terminal Servers. Even custom or proprietary applications and protocols are supported by the Cyberoam SSL VPN.

Secure Firewall Traversal of TCP/UDP allows local desktops to access UDP-based remote data services, without segregating the network, exposing UDP port ranges to hackers, using routable IP addresses, or publishing internal routes externally. Cyberoam VPN works alongside existing firewalls, and NAT devices.

Authentication and Authorization Architecture supports different group access policies via leading protocols (LDAP, Active Directory, RADIUS, and more).

Centralized Access Control manages granular access control by source, destination, domain name, user group, port, host, or network, thereby increasing security and dramatically simplifying firewall configuration.

Single Mode Connectivity enables remote access to any application, including web-enabled and legacy applications, through a simple interface with the look and feel of the user's native desktop.

Load Balancing and High Availability automatically distributes application network traffic among multiple VPN Servers with integrated failover to available servers.

SSL VPN users may access applications from a standard portal interface or directly from their desktop, for an IPSec-like "in office" experience.

Clientless Browser-based Access provides secure remote access to applications through common web browsers. No clients to install or maintain.

Endpoint Security enforces access restrictions based on customizable policies such as Anti-virus, Anti-spyware and Firewall status.

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

Benefits

Reduced Costs - Centralize management; consolidate data centers, lower administration costs.

Investment Protection - Utilize existing networks, firewalls, servers, clients and software.

Trusted Remote Access - Extend access to regional offices, partners, customers, telecommuters, wireless users.

Easy to Use - Fast installation and little ongoing management, reduced training, less down-time.

Continuous Access - provide reliable, available and scalable access.

Application Access

Email Access - Use your local Outlook or Lotus Notes client to access corporate email system.

File Shares and FTP - Directly access the files and shares residing on the corporate network.

Web Applications - Access any HTTP/S based applications.

Cyberoam TSE and Terminal Services - Secure connection to RDP-based applications.

Other Applications - Provide access to any TCP/UDP based applications.

Technical Specifications

Throughput

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

Capacity

- CR-SGX800 - Upto 100 Concurrent Users
- CR-SGX1200 - Upto 250 Concurrent Users
- CR-SGX2400 - Upto 2,000 Concurrent Users

Deployment Scalability

- Scalable to 200,000 users
- Active-Active N+1 cluster
- Resource-based VPN Load balancing with multiple load balancer
- Session Persistence: Users do not need to re-authenticate

Application Support

- All web-based, TCP and UDP based client-server applications
- Windows File Shares and Drive Mapping
- Dynamic port-based applications
- Special support for RDP virtual channels
- Application load balancing
- Session Caching for load balanced applications
- Per application-based compression switch

Access Security

- SSL 3.0 and TLS 1.0
- Encryption: Strongest available: DES, 3DES, AES(256), RC4
- Authentication: MD-5, SHA-1, RSA 1024, RSA 2048
- Internet network masking and IP address/hostname mangling
- Works with Network Address Translation (NAT) and Firewall
- VPN Chaining
- Application level gateway
- Hardened Gateway Operating System

Authentication

- Authentication based on user identity, endpoint identity, endpoint trust level
- Multiple User authentication options: static passwords, client certificates, External two factor authentication solutions
- Local database with full customization per user, password policies, password reset support
- Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning
- Enterprise PKI built-in with X509 standards
- Email based user provisioning

- Authentication method based application access control
- Integrates with AD/LDAP/RADIUS/RSA SecurID®, X.509 digital certificates
- Automatic fetching of group information from AD/LDAP/RADIUS
- Key Exchange - RSA & Diffie Hellman
- Biometric authentication support

Authorization

- Publish applications rather than subnet or network
- Simple access control mechanism
- Access control based on
 - Device identity and profile
 - User Authentication method
 - User Role
- Dynamic policy evaluation based on run time information about device, authentication method and user role
- Display of allowed applications and availability of the application server to users
- Time-based restriction policies
- Auto-detection of applications running in corporate network

Auditing & Logging

- Complete reporting of user logons and activity
- Information logged includes
 - Time of access
 - Username
 - MAC Address of endpoint
 - IP address of endpoint
 - Application accessed
 - Device Profile
- Logging of endpoint security scans
- Detailed logging per device scans including
 - Policies evaluated for user sessions
 - Current profile of endpoint
 - List of failed policies
 - List of policies for which remediation information is sent to user
- Session, connection, failed connection logging
- Administrative auditing
- Extract logs in CSV format for feeding to third party report generation
- Monitor and disconnect live users

Device Profiling (Endpoint Security)

- Support for checking for Anti-virus, Firewall and Anti-spyware products
- Real time status check for
 - Virus signature DAT file version
 - Last update time
 - Last scan time
 - Real time protection check

- Support for more than 200 products
- Support for checking for MAC ID and IP address
- Application control based on device profile
- Mandatory profile for non-avoidable policy checks on all endpoints
- Quarantine profile for devices that fails all other profiles
- Option to block endpoints that fails to comply to required policies or option to allow them to login by putting them in quarantine profile
- Real time updates about latest virus signature DAT file releases by AV/FW vendors are pushed to VPN gateway every hour to protect corporate network against any zero-day attacks
- Integrated with OPSWAT™ endpoint security SDK

Access Modes

- Web Portal for easy access by end users
- Clientless VPN with a browser agent for seamless access to applications
- No configuration required on end user machines
- Client platforms supported
 - Windows 98®/XP®/Vista®/Windows7®
 - Windows server 2003®/2008®
 - Linux
 - MAC OS X PPC/Intel 10.4 and above
- Site to Site access

Management

- Web-based management console
- Menu driven console interface for system configuration
- Wizard driven installation procedure
- Self-signed certificate generation CLI
- Real-time status and monitoring
- Delegated role-based administration
- Certificate based login for administrators