Cyberoam CR-SSL-2400

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 is an easy-to-use, simple application access and security solution for enabling high-trust, secure remote access to Enterprise applications and resources. Enterprises use Cyberoam SSL VPN to collaborate securely with employees, customers and partners. Cyberoam SSL VPN comes with unique network obfuscation feature that hides the internal network details from intentional or unintentional exploitation by a user or hacker.

Key Features

Application Support allows access to virtually any application, including all TCP, 802.11x and UDP applications, Microsoft Outlook, FTP, Citrix 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 SSL 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.

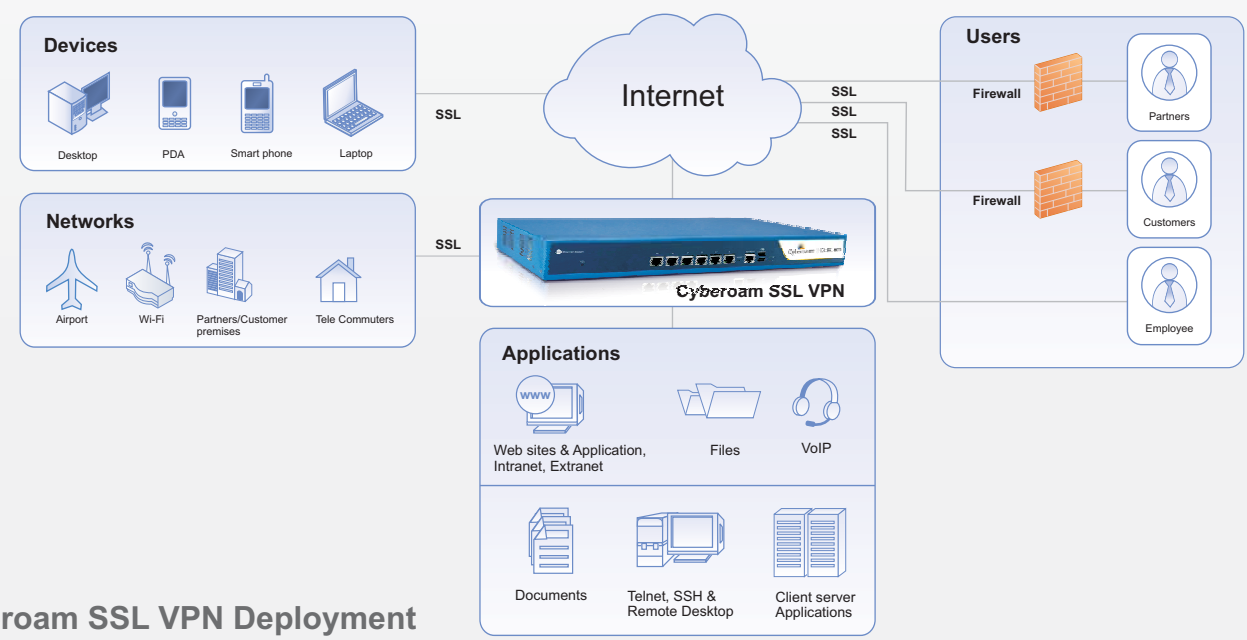
Single Mode Connectivity enables remote access to any application, including web-enabled and legacy applications, through a simple interface with the look and feel of the user's native desktop.

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 web browser. No clients to install or maintain.

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



Cyberoam SSL VPN Deployment

Specification

Interfaces	
10/100/1000 GBE Ports	-
Console Ports (RJ45)	10
SFP (Mini GBIC) Ports	1
USB Ports	2
Performance	
Concurrent User	1000
Deployment Scalability	
- Scalability up to 200,000 users	Yes
- Active-Active N+1 clustering	Yes
- Resource based VPN Load balancing with multiple load balancer	Yes
- Session Persistence	Yes
Gateway Features	
- Hardened Gateway Operating System	Yes
- Can run on hardened Linux based platform, on any standard or custom hardware	Yes
- Runs on Virtualization platforms, VMWare, XenServer, Hyper-V	Yes
Access Security	
- SSL 3.0 and TLS 1.0	Yes
- Encryption Standards: RC4 - 128 bits, 3DES, AES - 256 bits, MD5, SHA1	Yes
- Web Application URL masking	Yes
- Integrate behind any Firewall or NAT device	Yes
- VPN Chaining	Yes
- Application level gateway	Yes
Access Modes	
- User Web Portal	Yes
- Clientless VPN with a browser agent for seamless access to applications	Yes
- No configuration required on end user machines	Yes
- Client platforms supported	Yes
- Windows 98/XP/Vista/Windows7	
- Windows server 2003/2008	
- Linux OS	
- MAC OS X PPC/Intel 10.4 and above	
- Site to Site connectivity	Yes
Authentication	
- Authentication based on user identity, endpoint identity, endpoint trust level	Yes
- Multiple User authentication options: static passwords, client certificates	Yes
- Local database with customization per user, password policies, password reset support	Yes
- External two factor authentication solutions	
- Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning	Yes
- Email based user provisioning	Yes
- Integration with external authentication and directory services - Active Directory/LDAP/RADIUS/RSA SecurID,	Yes
- Automatic fetching of group information from Active Directory/ LDAP/RADIUS	Yes
- Default group for Active Directory/LDAP server	Yes
- Multiple Authentication servers support	Yes
- Biometric authentication support	Yes
Device Profiling (Endpoint Security)	Yes
- Product checks - Antivirus, Firewall and Anti-spyware	1100+
- Products supported	Yes
- Real time status check for	
- Virus signature DAT file version for Zero day protection	
- Last update time	
- Last scan time	
- Real time protection check	Yes
- MAC address and IP address checks	Yes
- Application control based on device profile	Yes
- Mandatory profile for non-avoidable policy checks on all endpoints	Yes
- Quarantine profile for devices that fails all other profile	Yes
- Bypass or block endpoints that fails to comply to required policies	Yes

Authorization	
- External Authorization server support	Yes
- Publish applications rather than subnet or network	Yes
- Access control based on	Yes
- Device identity and profile	
- User Authentication method	
- User Role	
- Time based restriction policies	Yes
Application Support	
- All web based, TCP and UDP based client-server applications	Yes
- Windows File Shares and Drive Mapping	Yes
- Dynamic port based applications	Yes
- Special support for RDP virtual channels	Yes
- Application load balancing	Yes
- Session Caching for load balanced applications	Yes
- Application based compression switch	Yes
Management	
- Administration - Web based and Command Line console	Yes
- Menu driven console interface for configuration	Yes
- Wizard driven installation	Yes
- Self signed certificate generation	Yes
- Dashboard	Yes
- Real-time status and monitoring	Yes
- Role-based administration	Yes
- Secure Administration - Certificate based login for administrators	Yes
- Automatic expiry of User account	Yes
- Error for Unresolved Web URL	Yes
- Monitor and disconnect live users	Yes
Auditing & Logging	
- User logons activity log including: Time of access,Username, MAC Address and IP address of endpoint, Application accessed, Device Profile	Yes
- Endpoint security scan log	Yes
- Device scan log 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	Yes
- Session, connection, failed connection log	Yes
- Export Logs in CSV format	Yes
Dimensions	
H x W x D (inches	3.46 x 16.7 x 20.9
H x W x D (cms)	8.8 x 42.4 x 53.1
Weight	15.2 kg, 33.51 lbs
Power	
Input Voltage	90-264VAC
Consumption	210W
Total Heat Dissipation (BTU)	718
Redundant Power Supply	Yes
Environmental	
Operating Temperature	0 to 40 °C
Storage Temperature	-20 to 80 °C
Relative Humidity (Non condensing)	10 to 90%

Toll Free Numbers

USA : +1-781-460-2080 | **India :** 1-800-301-00013

APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Cyberoam® Unified Threat Management