



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.



CR SSL Series : CR-SSL-800, CR-SSL-1200, CR-SSL-2400

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.

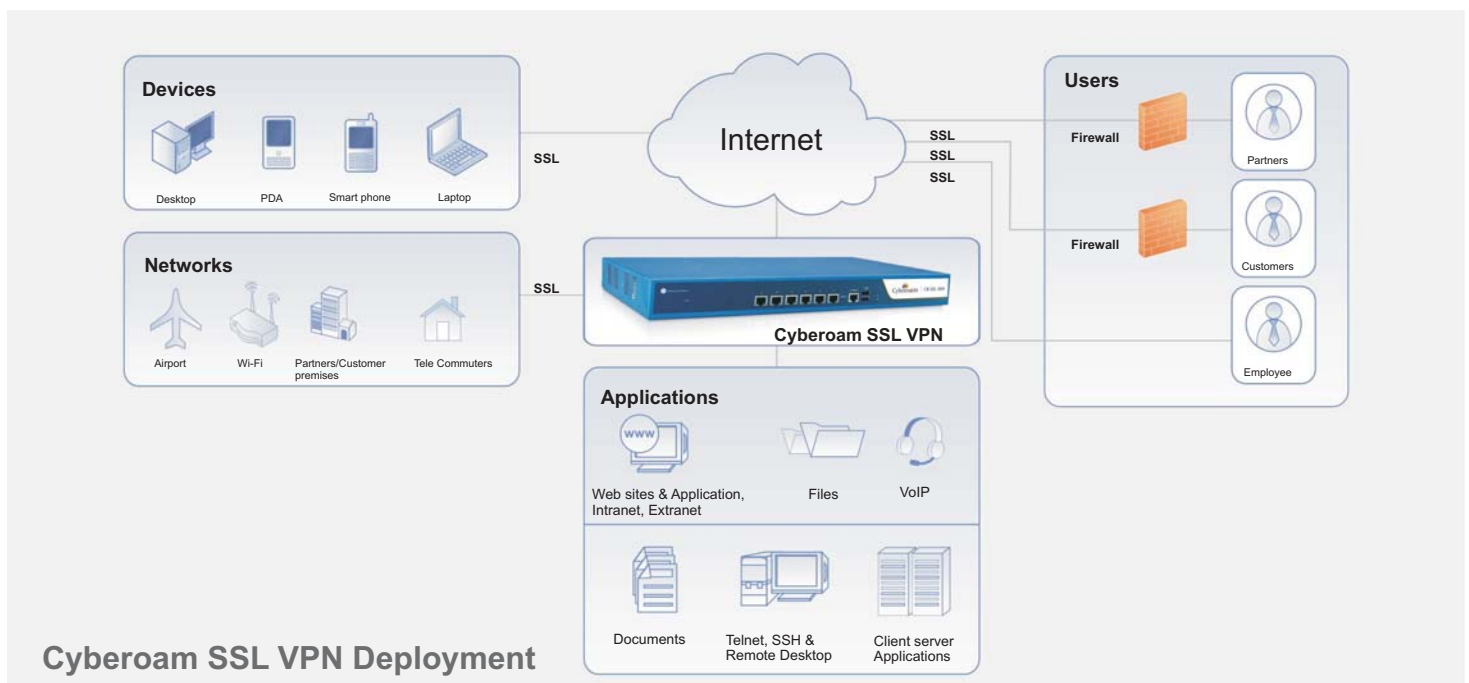
Single Mode Connectivity enables remote access to any application, including web-enabled and legacy applications, through a simple interface with the look and feel of the user's native desktop.

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

Feature Specifications

Deployment Scalability

- Scalable to 200,000 users
- Active-Active N+1 cluster
- Resource based VPN Load balancing with multiple load balancer
- Session Persistence

Gateway Features

- Hardened Gateway Operating System
- Can run on hardened Linux based platform, on any standard or custom hardware
- Runs on Virtualization platforms, VMWare, XenServer, Hyper-V

Access Security

- SSL 3.0 and TLS 1.0
- Encryption Standards: RC4 - 128 bits, 3DES, AES - 256 bits, MD5, SHA1
- Web Application URL masking
- Integrate behind any Firewall or NAT device
- VPN Chaining
- Application level gateway

Access Modes

- User Web Portal
- 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 OS
 - MAC OS X PPC/Intel 10.4 and above
- Site to Site connectivity

Authentication

- Authentication based on user identity, endpoint identity, endpoint trust level
- Multiple User authentication options: static passwords, client certificates

- Local database with customization per user, password policies, password reset support
- External two factor authentication solutions
- Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning
- Email based user provisioning
- Integration with external authentication and directory services - Active Directory/LDAP/RADIUS/RSA SecurID,
- Automatic fetching of group information from Active Directory/LDAP/RADIUS
- Default group for Active Directory/LDAP server
- Multiple Authentication servers support
- Biometric authentication support

Device Profiling (Endpoint Security)

- Product checks - Antivirus, Firewall and Anti-spyware Products supported - 1100+
- Real time status check for
 - Virus signature DAT file version for Zero day protection
 - Last update time
 - Last scan time
 - Real time protection check
- MAC address and IP address checks
- Application control based on device profile
- Mandatory profile for non-avoidable policy checks on all endpoints
- Quarantine profile for devices that fails all other profile
- Bypass or block endpoints that fails to comply to required policies
- Integrated with OPSWAT™ endpoint security SDK

Authorization

- External Authorization server support
- Publish applications rather than subnet or network
- Access control based on
 - Device identity and profile
 - User Authentication method
 - User Role
- Time based restriction policies

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
- Application based compression switch

Management

- Administration - Web based and Command Line console
- Menu driven console interface for configuration
- Wizard driven installation
- Self signed certificate generation
- Dashboard
- Real-time status and monitoring
- Role-based administration
- Secure Administration - Certificate based login for administrators
- Automatic expiry of User account
- Error for Unresolved Web URL
- Monitor and disconnect live users

Auditing & Logging

- User logons activity log including: Time of access, Username, MAC Address and IP address of endpoint, Application accessed, Device Profile
- Endpoint security scan log
- 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
- Session, connection, failed connection log
- Export Logs in CSV format

Specifications

Interfaces

| | CR-SSL-800 | CR-SSL-1200 | CR-SSL-2400 |
|-----------------------|------------|-------------|-------------|
| 10/100/1000 GBE Ports | 6 | 6 | 10 |
| Console Ports (RJ45) | 1 | 1 | 1 |
| SFP (Mini GBIC) Ports | - | - | 2 |
| USB Ports | 2 | 2 | |

Performance

| | CR-SSL-800 | CR-SSL-1200 | CR-SSL-2400 |
|-----------------|------------|-------------|-------------|
| Concurrent User | 50 | 250 | 1000 |

Dimensions

| | CR-SSL-800 | CR-SSL-1200 | CR-SSL-2400 |
|--------------------|-------------------|----------------------|--------------------|
| H x W x D (inches) | 1.7 x 16.8 x 10.3 | 1.72 x 11.50 x 17.25 | 3.46 x 16.7 x 20.9 |
| H x W x D (cms) | 4.3 x 42.7 x 26.2 | 4.4 x 29.21 x 43.8 | 8.8 x 42.4 x 53.1 |
| Weight | 5.3 kg, 11.68 lbs | 5.54 kg, 12.188 lbs | 15.2 kg, 33.51 lbs |

Power

| | CR-SSL-800 | CR-SSL-1200 | CR-SSL-2400 |
|------------------------------|------------|-------------|-------------|
| Input Voltage | 115-230VAC | 100-240 VAC | 90-264VAC |
| Consumption | 90W | 128W | 210W |
| Total Heat Dissipation (BTU) | 200 | 375 | 718 |
| Redundant Power Supply | - | No | Yes |

Environmental

| | CR-SSL-800 | CR-SSL-1200 | CR-SSL-2400 |
|------------------------------------|--------------|--------------|--------------|
| Operating Temperature | 0 to 40 °C | 5 to 40 °C | 0 to 40 °C |
| Storage Temperature | -20 to 80 °C | -20 to 70 °C | -20 to 80 °C |
| Relative Humidity (Non condensing) | 0 to 90% | 0 to 90% | 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

www.cyberoam.com | sales@cyberoam.com

Copyright © 1999-2010 Elitecore Technologies Ltd. All Rights Reserved. Cyberoam and Cyberoam logo are registered trademark of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice. 1.0-0.34-20100128


Cyberoam[®]
 Unified Threat Management

 Elitecore Product