



Cyberoam CR1500i

Comprehensive Network Security for Large Enterprises



Cyberoam UTM

Cyberoam CR1500i is an identity-based security appliance that delivers real-time network protection against evolving Internet threats to large enterprises through unique user based policies.

Large enterprises with limited security like firewall, anti-virus are exposed to Internet threats. Cyberoam delivers comprehensive protection from malware, virus, spam, phishing, pharming and more. Its unique identity-based security protects users from internal threats that lead to data leakage. Cyberoam features include Stateful Inspection Firewall, VPN (SSL & IPSec), Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, IPS, Content Filtering, Bandwidth Management, Multiple Link Management and can be centrally managed with Cyberoam Central Console.

Identity-based Security in UTM

Cyberoam attaches the user identity to security, taking enterprises a step ahead of conventional solutions that bind security to IP-addresses. Cyberoam's identity-based security offers full business flexibility while ensuring complete security in any environment, including DHCP and Wi-Fi, by identifying individual users within the network-whether they are victims or attackers.

Features	Description	Benefits
Stateful Inspection Firewall (ICSA Labs Certified)	Powerful stateful and deep packet inspection Fusion technology blends all the components of Cyberoam into a single firewall policy Prevents DoS & flooding attacks from internal & external sources Identity-based access control for applications like P2P, IM	Application layer protection Provides the right balance of security, connectivity and productivity Flexibility to set policies by user identity High scalability
Virtual Private Network	Threat Free Tunneling Industry standard: IPSec, SSL, L2TP, PPTP VPN VPN High Availability for IPSec and L2TP connections Dual VPNC Certifications - Basic and AES Interop	Safe and clean VPN traffic Secure connectivity to branch offices and remote users Low cost remote connectivity over the Internet Effective failover management with defined connection priorities
Gateway Anti-Virus & Anti-Spyware	Scans HTTP, FTP, IMAP, POP3 and SMTP traffic Detects and removes viruses, worms and Trojans Access to quarantined mails to key executives Instant user identification in case of HTTP threats	Complete protection of traffic over all protocols High business flexibility Protection of confidential information Real-time security
Gateway Anti-Spam	Scans SMTP, POP3 and IMAP traffic for spam Detects, tags and quarantines spam mail Enforces black and white lists Virus Outbreak Protection Content-agnostic spam protection including Image-spam using Recurrent Pattern Detection (RPD™) Technology Spam Notification through Digest IP Reputation-based Spam filtering	Enhances productivity High business flexibility Protection from emerging threats High scalability Zero hour protection incase of virus outbreaks Multi-language and Multi-format spam detection
Intrusion Prevention System - IPS	Database of over 3000 signatures Multi-policy capability with policies based on default & custom signatures, source and destination Prevents intrusion attempts, DoS attacks, malicious code, backdoor activity and network-based blended threats Blocks anonymous proxies with HTTP proxy signatures Blocks "phone home" activities	Low false positives Real-time Security in dynamic environments like DHCP and Wi-Fi Offers instant user-identification in case of internal threats Apply IPS policies on users
Content & Application Filtering	Automated web categorization engine blocks non-work sites based on millions of sites in over 82+ categories URL Filtering for HTTP & HTTPS protocols Hierarchy, department, group, user-based filtering policies Time-based access to pre-defined sites Prevents downloads of streaming media, gaming, tickers, ads Supports CIPA compliance for schools and libraries	Prevents exposure of network to external threats Blocks access to restricted websites Ensures regulatory compliance Saves bandwidth and enhances productivity Protects against legal liability Ensures the safety and security of minors online Enables schools to qualify for E-rate funding
Bandwidth Management	Committed and burstable bandwidth by hierarchy, departments, groups & users Category-based Bandwidth restriction	Prevents bandwidth congestion Prioritizes bandwidth for critical applications
Multiple Link Management	Security over multiple ISP links using a single appliance Load balances traffic based on weighted round robin distribution Link Failover automatically shifts traffic from a failed link to a working link	Easy to manage security over multiple links Controls bandwidth congestion Optimal use of low-cost links Ensures business continuity
On-Appliance Reporting	Complete Reporting Suite available on the Appliance Traffic discovery offers real-time reports Reporting by username	Reduced TCO as no additional purchase required Instant and complete visibility into patterns of usage Instant identification of victims and attackers in internal network

Specification

Interfaces			
10/100/1000 GBE Ports		10	
Configurable Internal/DMZ/WAN Ports		Yes	
Console Ports (RJ45)		1	
SFP (Mini GBIC) Ports		2	
USB ports		2	
Hardware Bypass Segments		2	
System Performance*			
Firewall throughput (Mbps)		6Gbps	
New sessions/second		40,000	
Concurrent sessions		1,000,000	
168-bit Triple-DES/AES throughput (Mbps)		600/750	
Antivirus throughput (Mbps)		900	
IPS throughput (Mbps)		2500	
UTM throughput (Mbps)		750	
Stateful Inspection Firewall			
Multiple Zones security with separate levels of access rule enforcement for each zone	Yes		
Rules based on the combination of User, MAC, Source & Destination Zone and IP address and Service	Yes		
Actions include policy based control for IPS, Content Filtering, Anti virus, Anti spam and Bandwidth Management	Yes		
Access Scheduling	Yes		
Policy based Source & Destination NAT	Yes		
H.323 NAT Traversal	Yes		
802.1q VLAN Support	Yes		
DoS & DDoS Attack prevention	Yes		
MAC & IP-MAC filtering and Spoof prevention	Yes		
Gateway Anti-Virus & Anti-Spyware			
Virus, Worm, Trojan Detection & Removal	Yes		
Spyware, Malware, Phishing protection	Yes		
Automatic virus signature database update	Yes		
Scans HTTP, FTP, SMTP, POP3, IMAP, VPN Tunnels	Yes		
Customize individual user scanning	Yes		
Self Service Quarantine area	Yes		
Scan and deliver by file size	Yes		
Block by file types	Yes		
Add disclaimer/signature	Yes		
Gateway Anti-Spam			
Real-time Blacklist (RBL), MIME header check	Yes		
Filter based on message header, size, sender, recipient	Yes		
Subject line tagging	Yes		
IP address Black list/White list	Yes		
Redirect spam mails to dedicated email address	Yes		
Image-based spam filtering using RPD Technology	Yes		
Zero hour Virus Outbreak Protection	Yes		
Self Service Quarantine area	Yes		
Spam Notification through Digest	Yes		
IP Reputation-based Spam filtering	Yes		
Intrusion Prevention System			
Signatures: Default (3000+), Custom	Yes		
IPS Policies: Multiple, Custom	Yes		
User-based policy creation	Yes		
Automatic real-time updates from CRProtect networks	Yes		
Protocol Anomaly Detection	Yes		
Block			
- P2P applications e.g. Skype	Yes		
- Anonymous proxies e.g. Ultra surf	Yes		
- "Phone home" activities	Yes		
- Keylogger	Yes		
Content & Application Filtering			
Inbuilt Web Category Database	Yes		
URL, keyword, File type block	Yes		
Categories: Default(82+), Custom	Yes		
Protocols supported: HTTP, HTTPS	Yes		
Block Malware, Phishing, Pharming URLs	Yes		
Custom block messages per category	Yes		
Block Java Applets, Cookies, Active X	Yes		
CIPA Compliant	Yes		
Data leakage control via HTTP upload	Yes		
Virtual Private Network - VPN			
IPSec, L2TP, PPTP	Yes		
Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent	Yes		
Hash Algorithms - MD5, SHA-1	Yes		
Authentication - Preshared key, Digital certificates	Yes		
IPSec NAT Traversal	Yes		
Dead peer detection and PFS support	Yes		
Diffie Hellman Groups - 1,2,5,14,15,16	Yes		
External Certificate Authority support	Yes		
Export Road Warrior connection configuration	Yes		
Domain name support for tunnel end points	Yes		
VPN connection redundancy	Yes		
Overlapping Network support	Yes		
Hub & Spoke VPN support	Yes		
SSL VPN			
TCP & UDP Tunneling	Yes		
Authentication - Active Directory, LDAP, RADIUS, Cyberoam	Yes		
Multi-layered Client Authentication - Certificate, Username/Password	Yes		
User & Group policy enforcement	Yes		
Network access - Split and Full tunneling	Yes		
Browser-based (Portal) Access - Clientless access	Yes		
Lightweight SSL VPN Tunneling Client	Yes		
Granular access control to all the Enterprise Network resources	Yes		
Administrative controls - Session timeout, Dead Peer Detection, Portal customization	Yes		
Bandwidth Management			
Application and User Identity based Bandwidth Management	Yes		
Guaranteed & Burstable bandwidth policy	Yes		
Application & User Identity based Traffic Discovery	Yes		
Multi WAN bandwidth reporting	Yes		
Category-based Bandwidth restriction	Yes		
User Identity and Group Based Controls			
Access time restriction	Yes		
Time and Data Quota restriction	Yes		
Schedule based Committed and Burstable Bandwidth	Yes		
Schedule based P2P and IM Controls	Yes		
Networking			
Multiple Link Auto Failover	Yes		
WRR based Load balancing	Yes		
Policy routing based on Application and User	Yes		
DDNS/PPPoE Client	Yes		
Support for HTTP Proxy	Yes		
Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding	Yes		
Parent Proxy support with FQDN	Yes		
DHCP Server and Relay	Yes		
High Availability			
Active-Active	Yes		
Active-Passive with state synchronization	Yes		
Stateful Failover	Yes		
Alert on Appliance Status change	Yes		
Administration & System Management			
Web-based configuration wizard	Yes		
Role-based administration	Yes		
Multiple administrators and user levels	Yes		
Upgrades & changes via Web UI	Yes		
Multi-lingual support: Chinese, Hindi	Yes		
Web UI (HTTPS)	Yes		
Command line interface (Serial, SSH, Telnet)	Yes		
SNMP (v1, v2c, v3)	Yes		
Cyberoam Central Console	Yes		
Version Rollback	Yes		
NTP Support	Yes		
User Authentication			
Local database	Yes		
Windows Domain Control & Active Directory Integration	Yes		
Automatic Windows Single Sign On	Yes		
External LDAP/RADIUS database Integration	Yes		
User/MAC Binding	Yes		
Logging/Monitoring			
Internal HDD	Yes		
Graphical real-time and historical monitoring	Yes		
Email notification of reports, viruses and attacks	Yes		
Syslog support	Yes		
On-Appliance Reporting			
Intrusion events reports	Yes		
Policy violations reports	Yes		
Web Category reports (user, content type)	Yes		
Search Engine Keywords reporting	Yes		
Data transfer reporting (By Host, Group & IP Address)	Yes		
Virus reporting by User and IP Address	Yes		
Compliance Reports	45+		
VPN Client			
IPSec compliant	Yes		
Inter-operability with major IPSec VPN Gateways	Yes		
Supported platforms: Windows 98, Me, NT4, 2000, XP, Vista	Yes		
Import Connection configuration	Yes		
Certification			
ICSA Firewall - Corporate	Yes		
VPNC - Basic and AES interoperability	Yes		
Checkmark UTM Level 5 Certification	Yes		
Compliance			
CE	Yes		
FCC	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		90-264 VAC	
Consumption		210W	
Total Heat Dissipation (BTU)		718	
Environmental			
Operating Temperature		0 to 40 °C	
Storage Temperature		-20 to 80 °C	
Relative Humidity (Non condensing)		10 to 90%	
Cooling System - Fans		7	

*Antivirus, IPS and UTM performance is measured based on HTTP traffic as per RFC 3511 guidelines. Actual performance may vary depending on the real network traffic environments.

Toll Free Numbers

USA : +1-877-777-0368 | India : 1-800-301-00013

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

www.cyberoam.com | sales@cyberoam.com

Copyright© 1999-2009 Elitecore Technologies Ltd. All Rights Reserved.
Cyberoam and Cyberoam logo are registered trademarks 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. PL-10-96030-090630


Cyberoam[®]
Unified Threat Management

 Elitecore Product