



## Cyberoam CR100ia

### Comprehensive Network Security for Small and Medium Offices



### Cyberoam UTM

Cyberoam CR100ia is an identity-based security appliance that delivers real-time network protection against evolving Internet threats to small and medium enterprises (SMEs) through unique user based policies.

CR100ia 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
<b>Stateful Inspection Firewall (ICSA Labs Certified)</b>	<ul style="list-style-type: none"> <li>Powerful stateful and deep packet inspection</li> <li>Fusion technology blends all the components of Cyberoam into a single firewall policy</li> <li>Prevents DoS &amp; flooding attacks from internal &amp; external sources</li> <li>Identity-based access control for applications like P2P, IM</li> </ul>	<ul style="list-style-type: none"> <li>Application layer protection</li> <li>Provides the right balance of security, connectivity and productivity</li> <li>Flexibility to set policies by user identity</li> <li>High scalability</li> </ul>
<b>Virtual Private Network</b>	<ul style="list-style-type: none"> <li>Threat Free Tunneling</li> <li>Industry standard: IPSec, SSL, L2TP, PPTP VPN</li> <li>VPN High Availability for IPSec and L2TP connections</li> <li>Dual VPNC Certifications - Basic and AES Interop</li> </ul>	<ul style="list-style-type: none"> <li>Safe and clean VPN traffic</li> <li>Secure connectivity to branch offices and remote users</li> <li>Low cost remote connectivity over the Internet</li> <li>Effective failover management with defined connection priorities</li> </ul>
<b>Gateway Anti-Virus &amp; Anti-Spyware</b>	<ul style="list-style-type: none"> <li>Scans HTTP, FTP, IMAP, POP3 and SMTP traffic</li> <li>Detects and removes viruses, worms and Trojans</li> <li>Access to quarantined mails to key executives</li> <li>Instant user identification in case of HTTP threats</li> </ul>	<ul style="list-style-type: none"> <li>Complete protection of traffic over all protocols</li> <li>High business flexibility</li> <li>Protection of confidential information</li> <li>Real-time security</li> </ul>
<b>Gateway Anti-Spam</b>	<ul style="list-style-type: none"> <li>Scans SMTP, POP3 and IMAP traffic for spam</li> <li>Detects, tags and quarantines spam mail</li> <li>Enforces black and white lists</li> <li>Virus Outbreak Protection</li> <li>Content-agnostic spam protection including Image-spam using Recurrent Pattern Detection (RPD™) Technology</li> <li>Spam Notification through Digest</li> <li>IP Reputation-based Spam filtering</li> </ul>	<ul style="list-style-type: none"> <li>Enhances productivity</li> <li>High business flexibility</li> <li>Protection from emerging threats</li> <li>High scalability</li> <li>Zero hour protection incase of virus outbreaks</li> <li>Multi-language and Multi-format spam detection</li> </ul>
<b>Intrusion Prevention System - IPS</b>	<ul style="list-style-type: none"> <li>Database of over 3000 signatures</li> <li>Multi-policy capability with policies based on default &amp; custom signatures, source and destination</li> <li>Prevents intrusion attempts, DoS attacks, malicious code, backdoor activity and network-based blended threats</li> <li>Blocks anonymous proxies with HTTP proxy signatures</li> <li>Blocks "phone home" activities</li> </ul>	<ul style="list-style-type: none"> <li>Low false positives</li> <li>Real-time Security in dynamic environments like DHCP and Wi-Fi</li> <li>Offers instant user-identification in case of internal threats</li> <li>Apply IPS policies on users</li> </ul>
<b>Content &amp; Application Filtering</b>	<ul style="list-style-type: none"> <li>Automated web categorization engine blocks non-work sites based on millions of sites in over 82+ categories</li> <li>URL Filtering for HTTP &amp; HTTPS protocols</li> <li>Hierarchy, department, group, user-based filtering policies</li> <li>Time-based access to pre-defined sites</li> <li>Prevents downloads of streaming media, gaming, tickers, ads</li> <li>Supports CIPA compliance for schools and libraries</li> </ul>	<ul style="list-style-type: none"> <li>Prevents exposure of network to external threats</li> <li>Blocks access to restricted websites</li> <li>Ensures regulatory compliance</li> <li>Saves bandwidth and enhances productivity</li> <li>Protects against legal liability</li> <li>Ensures the safety and security of minors online</li> <li>Enables schools to qualify for E-rate funding</li> </ul>
<b>Bandwidth Management</b>	<ul style="list-style-type: none"> <li>Committed and burstable bandwidth by hierarchy, departments, groups &amp; users</li> <li>Category-based Bandwidth restriction</li> </ul>	<ul style="list-style-type: none"> <li>Prevents bandwidth congestion</li> <li>Prioritizes bandwidth for critical applications</li> </ul>
<b>Multiple Link Management</b>	<ul style="list-style-type: none"> <li>Security over multiple ISP links using a single appliance</li> <li>Load balances traffic based on weighted round robin distribution</li> <li>Link Failover automatically shifts traffic from a failed link to a working link</li> </ul>	<ul style="list-style-type: none"> <li>Easy to manage security over multiple links</li> <li>Controls bandwidth congestion</li> <li>Optimal use of low-cost links</li> <li>Ensures business continuity</li> </ul>
<b>On-Appliance Reporting</b>	<ul style="list-style-type: none"> <li>Complete Reporting Suite available on the Appliance</li> <li>Traffic discovery offers real-time reports</li> <li>Reporting by username</li> </ul>	<ul style="list-style-type: none"> <li>Reduced TCO as no additional purchase required</li> <li>Instant and complete visibility into patterns of usage</li> <li>Instant identification of victims and attackers in internal network</li> </ul>

# Specification

<b>Interfaces</b>		Granular access control to all the Enterprise Network resources	Yes
10/100 Ethernet Ports	-	Administrative controls - Session timeout, Dead Peer Detection, Portal customization	Yes
10/100/1000 GBE Ports	6		
Configurable Internal/DMZ/WAN Ports	Yes		
Console Ports (RJ45/DB9)	-		
COM Ports	1	<b>Bandwidth Management</b>	
USB Ports	2	Application and User Identity based Bandwidth Management	Yes
Hardware Bypass Segments	1*	Guaranteed & Burstable bandwidth policy	Yes
		Application & User Identity based Traffic Discovery	Yes
		Multi WAN bandwidth reporting	Yes
		Category-based Bandwidth restriction	Yes
<b>System Performance*</b>		<b>User Identity and Group Based Controls</b>	
Firewall throughput (Mbps)	1,000	Access time restriction	Yes
New sessions/second	10,000	Time and Data Quota restriction	Yes
Concurrent sessions	400,000	Schedule based Committed and Burstable Bandwidth	Yes
168-bit Triple-DES/AES throughput (Mbps)	80/100	Schedule based P2P and IM Controls	Yes
Antivirus throughput (Mbps)	200		
IPS throughput (Mbps)	300	<b>Networking</b>	
UTM throughput (Mbps)	160	Multiple Link Auto Failover	Yes
		WRR based Load balancing	Yes
<b>Stateful Inspection Firewall</b>		Policy routing based on Application and User	Yes
Multiple Zones security with separate levels of access rule enforcement for each zone	Yes	DDNS/PPPoE Client	Yes
Rules based on the combination of User, MAC, Source & Destination Zone and IP address and Service	Yes	Support for HTTP Proxy	Yes
Actions include policy based control for IPS, Content Filtering, Anti virus, Anti spam and Bandwidth Management	Yes	Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding	Yes
Access Scheduling	Yes	Parent Proxy support with FQDN	Yes
Policy based Source & Destination NAT	Yes	DHCP Server and Relay	Yes
H.323 NAT Traversal	Yes		
802.1q VLAN Support	Yes	<b>High Availability</b>	
DoS & DDoS Attack prevention	Yes	Active-Active	Yes
MAC & IP-MAC filtering and Spoof prevention	Yes	Active-Passive with state synchronization	Yes
		Stateful Failover	Yes
		Alert on Appliance Status change	Yes
<b>Gateway Anti-Virus &amp; Anti-Spyware</b>		<b>Administration &amp; System Management</b>	
Virus, Worm, Trojan Detection & Removal	Yes	Web-based configuration wizard	Yes
Spyware, Malware, Phishing protection	Yes	Role-based administration	Yes
Automatic virus signature database update	Yes	Multiple administrators and user levels	Yes
Scans HTTP, FTP, SMTP, POP3, IMAP, VPN Tunnels	Yes	Upgrades & changes via Web UI	Yes
Customize individual user scanning	Yes	Multi-lingual support: Chinese, Hindi, French	Yes
Self Service Quarantine area	Yes	Web UI (HTTPS)	Yes
Scan and deliver by file size	Yes	Command line interface (Serial, SSH, Telnet)	Yes
Block by file types	Yes	SNMP (v1, v2c, v3)	Yes
Add disclaimer/signature	Yes	Cyberoam Central Console	Yes
		Version Rollback	Yes
		NTP Server Support	Yes
<b>Gateway Anti-Spam</b>		<b>User Authentication</b>	
Real-time Blacklist (RBL), MIME header check	Yes	Local database	Yes
Filter based on message header, size, sender, recipient	Yes	Windows Domain Control & Active Directory Integration	Yes
Subject line tagging	Yes	Automatic Windows Single Sign On	Yes
IP address Black list/White list	Yes	External LDAP/RADIUS database Integration	Yes
Redirect spam mails to dedicated email address	Yes	User/MAC Binding	Yes
Image-based spam filtering using RPD Technology	Yes		
Zero hour Virus Outbreak Protection	Yes	<b>Logging/Monitoring</b>	
Self Service Quarantine area	Yes	Internal HDD	Yes
Spam Notification through Digest	Yes	Graphical real-time and historical monitoring	Yes
IP Reputation-based Spam filtering	Yes	Email notification of reports, viruses and attacks	Yes
		Syslog support	Yes
<b>Intrusion Prevention System</b>		<b>On-Appliance Reporting</b>	
Signatures: Default (3000+), Custom	Yes	Intrusion events reports	Yes
IPS Policies: Multiple, Custom	Yes	Policy violations reports	Yes
User-based policy creation	Yes	Web Category reports (user, content type)	Yes
Automatic real-time updates from CRProtect networks	Yes	Search Engine Keywords reporting	Yes
Protocol Anomaly Detection	Yes	Data transfer reporting (By Host, Group & IP Address)	Yes
Block		Virus reporting by User and IP Address	Yes
- P2P applications e.g. Skype	Yes	Compliance Reports	45+
- Anonymous proxies e.g. Ultra surf	Yes		
- "Phone home" activities	Yes	<b>VPN Client</b>	
- Keylogger	Yes	IPSec compliant	Yes
		Inter-operability with major IPSec VPN Gateways	Yes
<b>Content &amp; Application Filtering</b>		Supported platforms: Windows 98, Me, NT4, 2000, XP, Vista	Yes
Inbuilt Web Category Database	Yes	Import Connection configuration	Yes
URL, keyword, File type block	Yes		
Categories: Default(82+), Custom	Yes	<b>Certification</b>	
Protocols supported: HTTP, HTTPS	Yes	ICSA Firewall - Corporate	Yes
Block Malware, Phishing, Pharming URLs	Yes	VPNC - Basic and AES interoperability	Yes
Custom block messages per category	Yes	Checkmark UTM Level 5 Certification	Yes
Block Java Applets, Cookies, Active X	Yes		
CIPA Compliant	Yes	<b>Compliance</b>	
Data leakage control via HTTP upload	Yes	CE	Yes
		FCC	Yes
<b>Virtual Private Network - VPN</b>		<b>Dimensions</b>	
IPSec, L2TP, PPTP	Yes	H x W x D (inches)	1.7 x 16.8 x 10.3
Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent	Yes	H x W x D (cms)	4.3 x 42.7 x 26.2
Hash Algorithms - MD5, SHA-1	Yes	Weight	5.3 kg, 11.68 lbs
Authentication - Preshared key, Digital certificates	Yes		
IPSec NAT Traversal	Yes	<b>Power</b>	
Dead peer detection and PFS support	Yes	Input Voltage	115-230 VAC
Diffie Hellman Groups - 1,2,5,14,15,16	Yes	Consumption	90W
External Certificate Authority support	Yes	Total Heat Dissipation (BTU)	200
Export Road Warrior connection configuration	Yes		
Domain name support for tunnel end points	Yes	<b>Environmental</b>	
VPN connection redundancy	Yes	Operating Temperature	0 to 40 °C
Overlapping Network support	Yes	Storage Temperature	-20 to 80 °C
Hub & Spoke VPN support	Yes	Relative Humidity (Non condensing)	0 to 90%
		Cooling System -Fans	2
<b>SSL VPN</b>			
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		

\*If Enabled, will bypass traffic only in case of Power failure.

\*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 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. PL-10-98034-091117

  
**Cyberoam**<sup>®</sup>  
Unified Threat Management

 Elitecore Product