



Cyberoam CR25ia

Comprehensive Network Security for Small and Remote Offices



Cyberoam UTM

Cyberoam Cr25ia is the identity-based security appliance that works on Layer 8, delivering real-time protection against evolving external and internal threats to Small Office-Home Office (SOHO) and Remote Office-Branch Office (ROBO) users.

Small, remote offices 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 (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)	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Application layer protection Provides the right balance of security, connectivity and productivity Flexibility to set policies by user identity High scalability
Virtual Private Network	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Complete protection of traffic over all protocols High business flexibility Protection of confidential information Real-time security
Gateway Anti-Spam	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Committed and burstable bandwidth by hierarchy, departments, groups & users Category-based Bandwidth restriction 	<ul style="list-style-type: none"> Prevents bandwidth congestion Prioritizes bandwidth for critical applications
Multiple Link Management	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Easy to manage security over multiple links Controls bandwidth congestion Optimal use of low-cost links Ensures business continuity
On-Appliance Reporting	<ul style="list-style-type: none"> Complete Reporting Suite available on the Appliance Traffic discovery offers real-time reports Reporting by username 	<ul style="list-style-type: none"> 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 Ethernet Ports	-		Granular access control to all the Enterprise Network resources
10/100/1000 GBE Ports	4		Administrative controls - Session timeout, Dead Peer Detection, Portal customization
Configurable Internal/DMZ/WAN Ports	Yes		
Console Ports (RJ45/DB9)	1		Bandwidth Management
USB Ports	1		Application and User Identity based Bandwidth Management
Hardware Bypass Segments	-		Guaranteed & Burstable bandwidth policy
			Application & User Identity based Traffic Discovery
			Multi WAN bandwidth reporting
			Category-based Bandwidth restriction
System Performance*			
Firewall throughput (Mbps)	225		User Identity and Group Based Controls
New sessions/second	3,500		Access time restriction
Concurrent sessions	130,000		Time and Data Quota restriction
168-bit Triple-DES/AES throughput (Mbps)	30/75		Schedule based Committed and Burstable Bandwidth
Antivirus throughput (Mbps)	65		Schedule based P2P and IM Controls
IPS throughput (Mbps)	70		
UTM throughput (Mbps)	50		
Stateful Inspection Firewall			
Multiple Zones security with separate levels of access rule enforcement for each zone	Yes		Networking
Rules based on the combination of User, MAC, Source & Destination Zone and IP address and Service	Yes		Multiple Link Auto Failover
Actions include policy based control for IPS, Content Filtering, Anti virus, Anti spam and Bandwidth Management	Yes		WRR based Load balancing
Access Scheduling	Yes		Policy routing based on Application and User
Policy based Source & Destination NAT	Yes		DDNS/PPPoE Client
H.323 NAT Traversal	Yes		Support for HTTP Proxy
802.1q VLAN Support	Yes		Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding
DoS & DDoS Attack prevention	Yes		Parent Proxy support with FQDN
MAC & IP-MAC filtering and Spoof prevention	Yes		DHCP Server and Relay
Gateway Anti-Virus & Anti-Spyware			
Virus, Worm, Trojan Detection & Removal	Yes		High Availability
Spyware, Malware, Phishing protection	Yes		Active-Active
Automatic virus signature database update	Yes		Active-Passive with state synchronization
Scans HTTP, FTP, SMTP, POP3, IMAP, VPN Tunnels	Yes		Stateful Failover
Customize individual user scanning	Yes		Alert on Appliance Status change
Self Service Quarantine area	Yes		
Scan and deliver by file size	Yes		Administration & System Management
Block by file types	Yes		Web-based configuration wizard
Add disclaimer/signature	Yes		Role-based administration
			Multiple administrators and user levels
			Upgrades & changes via Web UI
			Multi-lingual support: Chinese, Hindi, French
			Web UI (HTTPS)
			Command line interface (Serial, SSH, Telnet)
			SNMP (v1, v2c, v3)
			Cyberoam Central Console
			Version Rollback
			NTP Server Support
Gateway Anti-Spam			
Real-time Blacklist (RBL), MIME header check	Yes		User Authentication
Filter based on message header, size, sender, recipient	Yes		Local database
Subject line tagging	Yes		Windows Domain Control & Active Directory Integration
IP address Black list/White list	Yes		Automatic Windows Single Sign On
Redirect spam mails to dedicated email address	Yes		External LDAP/RADIUS database Integration
Image-based spam filtering using RPD Technology	Yes		User/MAC Binding
Zero hour Virus Outbreak Protection	Yes		
Self Service Quarantine area	Yes		Logging/Monitoring
Spam Notification through Digest	Yes		Internal HDD
IP Reputation-based Spam filtering	Yes		Graphical real-time and historical monitoring
			Email notification of reports, viruses and attacks
			Syslog support
Intrusion Prevention System			
Signatures: Default (3000+), Custom	Yes		On-Appliance Reporting
IPS Policies: Multiple, Custom	Yes		Intrusion events reports
User-based policy creation	Yes		Policy violations reports
Automatic real-time updates from CRProtect networks	Yes		Web Category reports (user, content type)
Protocol Anomaly Detection	Yes		Search Engine Keywords reporting
Block			Data transfer reporting (By Host, Group & IP Address)
- P2P applications e.g. Skype	Yes		Virus reporting by User and IP Address
- Anonymous proxies e.g. Ultra surf	Yes		Compliance Reports
- "Phone home" activities	Yes		
- Keylogger	Yes		
Content & Application Filtering			
Inbuilt Web Category Database	Yes		VPN Client
URL, keyword, File type block	Yes		IPSec compliant
Categories: Default(82+), Custom	Yes		Inter-operability with major IPSec VPN Gateways
Protocols supported: HTTP, HTTPS	Yes		Supported platforms: Windows 98, Me, NT4, 2000, XP, Vista
Block Malware, Phishing, Pharming URLs	Yes		Import Connection configuration
Custom block messages per category	Yes		
Block Java Applets, Cookies, Active X	Yes		Certification
CIPA Compliant	Yes		ICSA Firewall - Corporate
Data leakage control via HTTP upload	Yes		VPNC - Basic and AES interoperability
			Checkmark UTM Level 5 Certification
Virtual Private Network - VPN			
IPSec, L2TP, PPTP	Yes		Compliance
Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent	Yes		CE
Hash Algorithms - MD5, SHA-1	Yes		FCC
Authentication - Preshared key, Digital certificates	Yes		
IPSec NAT Traversal	Yes		Dimensions
Dead peer detection and PFS support	Yes		H x W x D (inches)
Diffie Hellman Groups - 1,2,5,14,15,16	Yes		4.4 x 15.3 x 23.2
External Certificate Authority support	Yes		Appliance Weight
Export Road Warrior connection configuration	Yes		2.3 kg, 5.1 lbs
Domain name support for tunnel end points	Yes		
VPN connection redundancy	Yes		Power
Overlapping Network support	Yes		Input Voltage
Hub & Spoke VPN support	Yes		Consumption
			Total Heat Dissipation (BTU)
			100-240 VAC
			33.5W
			114
SSL VPN			
TCP & UDP Tunneling	Yes		Environmental
Authentication - Active Directory, LDAP, RADIUS, Cyberoam	Yes		Operating Temperature
Multi-layered Client Authentication - Certificate, Username/Password	Yes		0 to 40 °C
User & Group policy enforcement	Yes		Storage Temperature
Network access - Split and Full tunneling	Yes		0 to 70 °C
Browser-based (Portal) Access - Clientless access	Yes		Relative Humidity (Non condensing)
Lightweight SSL VPN Tunneling Client	Yes		-20 to 75%
			2

*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

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. AN-10-96039-090807



Distributore ufficiale per l'Italia:

Horus Informatica

Tel: (+39) 02 33510135

Fax commerciale: (+39) 02 33510199

Email: commerciale@horus.it

www.horus.it