



Cyberoam CR35ia

Comprehensive Network Security for Small and Medium Offices



Cyberoam UTM

Cyberoam CR35ia 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.

CR35ia 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) | <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 | | 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 | 4 | | |
| Configurable Internal/DMZ/WAN Ports | Yes | Bandwidth Management | |
| Console Ports (RJ45/DB9) | 1 | Application and User Identity based Bandwidth Management | Yes |
| USB Ports | 1 | Guaranteed & Burstable bandwidth policy | Yes |
| Hardware Bypass Segments | - | Application & User Identity based Traffic Discovery | Yes |
| | | Multi WAN bandwidth reporting | Yes |
| | | Category-based Bandwidth restriction | Yes |
| System Performance* | | User Identity and Group Based Controls | |
| Firewall throughput (Mbps) | 500 | Access time restriction | Yes |
| New sessions/second | 5,500 | Time and Data Quota restriction | Yes |
| Concurrent sessions | 175,000 | Schedule based Committed and Burstable Bandwidth | Yes |
| 168-bit Triple-DES/AES throughput (Mbps) | 50/80 | Schedule based P2P and IM Controls | Yes |
| Antivirus throughput (Mbps) | 125 | | |
| IPS throughput (Mbps) | 150 | Networking | |
| UTM throughput (Mbps) | 90 | Multiple Link Auto Failover | Yes |
| | | WRR based Load balancing | Yes |
| Stateful Inspection Firewall | | 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 | High Availability | |
| 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 |
| Gateway Anti-Virus & Anti-Spyware | | Administration & System Management | |
| 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 |
| Gateway Anti-Spam | | NTP Server Support | Yes |
| Real-time Blacklist (RBL), MIME header check | Yes | User Authentication | |
| Filter based on message header, size, sender, recipient | Yes | Local database | Yes |
| Subject line tagging | Yes | Windows Domain Control & Active Directory Integration | Yes |
| IP address Black list/White list | Yes | Automatic Windows Single Sign On | Yes |
| Redirect spam mails to dedicated email address | Yes | External LDAP/RADIUS database Integration | Yes |
| Image-based spam filtering using RPD Technology | Yes | User/MAC Binding | Yes |
| Zero hour Virus Outbreak Protection | Yes | | |
| Self Service Quarantine area | Yes | Logging/Monitoring | |
| Spam Notification through Digest | Yes | Internal HDD | Yes |
| IP Reputation-based Spam filtering | Yes | Graphical real-time and historical monitoring | Yes |
| | | Email notification of reports, viruses and attacks | Yes |
| Intrusion Prevention System | | Syslog support | Yes |
| Signatures: Default (3000+), Custom | Yes | On-Appliance Reporting | |
| IPS Policies: Multiple, Custom | Yes | Intrusion events reports | Yes |
| User-based policy creation | Yes | Policy violations reports | Yes |
| Automatic real-time updates from CRProtect networks | Yes | Web Category reports (user, content type) | Yes |
| Protocol Anomaly Detection | Yes | Search Engine Keywords reporting | Yes |
| Block | | Data transfer reporting (By Host, Group & IP Address) | Yes |
| - P2P applications e.g. Skype | Yes | Virus reporting by User and IP Address | Yes |
| - Anonymous proxies e.g. Ultra surf | Yes | Compliance Reports | 45+ |
| - "Phone home" activities | Yes | VPN Client | |
| - Keylogger | Yes | IPSec compliant | Yes |
| Content & Application Filtering | | Inter-operability with major IPSec VPN Gateways | Yes |
| Inbuilt Web Category Database | Yes | Supported platforms: Windows 98, Me, NT4, 2000, XP, Vista | Yes |
| URL, keyword, File type block | Yes | Import Connection configuration | Yes |
| Categories: Default(82+), Custom | Yes | Certification | |
| 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 | Compliance | |
| CIPA Compliant | Yes | CE | Yes |
| Data leakage control via HTTP upload | Yes | FCC | Yes |
| Virtual Private Network - VPN | | Dimensions | |
| IPSec, L2TP, PPTP | Yes | H x W x D (inches) | 1.7 x 6 x 9.1 |
| Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent | Yes | H x W x D (cms) | 4.4 x 15.3 x 23.2 |
| Hash Algorithms - MD5, SHA-1 | Yes | Appliance Weight | 2.3 kg, 5.1 lbs |
| Authentication - Preshared key, Digital certificates | Yes | Power | |
| IPSec NAT Traversal | Yes | Input Voltage | 100-240 VAC |
| Dead peer detection and PFS support | Yes | Consumption | 47.8W |
| Diffie Hellman Groups - 1,2,5,14,15,16 | Yes | Total Heat Dissipation (BTU) | 163 |
| External Certificate Authority support | Yes | Environmental | |
| Export Road Warrior connection configuration | Yes | Operating Temperature | 0 to 40 °C |
| Domain name support for tunnel end points | Yes | Storage Temperature | 0 to 70 °C |
| VPN connection redundancy | Yes | Relative Humidity (Non condensing) | -20 to 75% |
| Overlapping Network support | Yes | Cooling System - Fans | 2 |
| 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 | | |

*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. AN-10-98030-090807

