Cyberoam

Unified Threat Management

Cyberoam CR100ia | **Comprehensive Network Security for Small & Medium Offices**

Gartner positions Cyberoam UTM as a "Visionary" in Magic Quadrant for SMB Multifunction Firewalls

Cyberoam Unified Threat Management appliances offer assured security, connectivity and productivity to small and medium enterprises (SMEs) by allowing user identity-based policy controls.

Cyberoam's User Layer 8 Technology treats user-identity as the 8th Layer or the HUMAN layer in the protocol stack. It attaches user identity to security, taking organizations a step ahead of conventional solutions that bind security to IP-addresses. This adds speed to an organization's security by offering instant visibility into the source of attacks by username rather than IP address – allowing immediate remediation to restore security or allowing proactive security. Layer 8 technology functions along with each of Cyberoam security features to allow creation of identity-based security policies.

Cyberoam's future-ready Extensible Security Architecture (ESA) offers an extensible platform that can grow with the future security needs of an organization without degrading system performance. ESA supports feature enhancements that can be developed rapidly and deployed with minimum efforts.

User Identity-based Security Policy Controls

L8	**USER**	
L7	**Application**	
L6	**Presentation**	ASCII, EBCDIC, ICA
L5	**Session**	L2TP, PPTP
L4	**Transport**	TCP, UDP
L3	**Network**	192.168.1.1
L2	**Data Link**	00-17-BB-8C-E3-E7
L1	**Physical**	
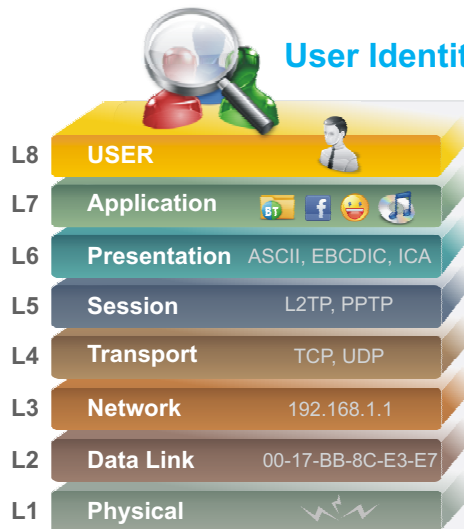
Cyberoam's Layer 8 Technology treats "User Identity" as the 8th Layer in the protocol stack

Cyberoam UTM offers security across Layer 2-Layer 8 using Identity-based policies

Cyberoam UTM features assure Security, Connectivity, Productivity

Security

Network Security
- Firewall
- Intrusion Prevention System
- Wireless security

Content Security
- Anti-Virus/Anti-Spyware
- Anti-Spam
- HTTPS/SSL Content Security

Administrative Security
- Next-Gen UI
- iView- Logging & Reporting

Connectivity

Business Continuity
- Multiple Link Management
- High Availability

Network Availability
- VPN
- 3G/WiMAX Connectivity

Future-ready Connectivity
- "IPv6 Ready" Gold Logo

Productivity

Employee Productivity
- Content Filtering
- Instant Messaging Archiving & Controls

IT Resource Optimization
- Bandwidth Management
- Traffic Discovery
- Application Layer 7 Management

Administrator Productivity
- Next-Gen UI

Interfaces

Copper GbE Ports	6
Configurable Internal/DMZ/WAN Ports	Yes
Console Ports (RJ45/DB9)	1
USB Ports	2
Hardware Bypass Segments	1*

System Performance**

Firewall throughput (UDP) (Mbps)	1250
Firewall throughput (TCP) (Mbps)	1000
New sessions/second	10,000
Concurrent sessions	400,000
168-bit 3DES/AES throughput (Mbps)	80/100
WAF Protected Throughput (Mbps)	60
Anti-Virus throughput (Mbps)	200
IPS throughput (Mbps)	300
UTM throughput (Mbps)	160

Stateful Inspection Firewall
- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Access Control Criteria (ACC) - User - Identity, Source & Destination Zone, MAC and IP address, Service
- UTM policies - IPS, Web Filtering, Application Filtering, Anti-Virus, Anti-Spam and Bandwidth Management
- Layer 7 (Application) Control & Visibility
- Access Scheduling
- Policy based Source & Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS & DDoS Attack prevention
- MAC & IP-MAC filtering and Spoof prevention

Gateway Anti-Virus & Anti-Spyware
- Virus, Worm, Trojan Detection & Removal
- Spyware, Malware, Phishing protection
- Automatic virus signature database update
- Scans HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IM, VPN Tunnels
- Customize individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

Gateway Anti-Spam
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- IP address Black list/White list
- Redirect Spam mails to dedicated email address
- Image-based Spam filtering using RPD Technology
- Zero hour Virus Outbreak Protection
- Self Service Quarantine area
- Spam Notification through Digest
- IP Reputation-based Spam filtering

Intrusion Prevention System
- Signatures: Default (3000+), Custom
- IPS Policies: Multiple, Custom
- User-based policy creation
- Automatic real-time updates from CRProtect networks
- Protocol Anomaly Detection
- DDoS attack prevention

Web Filtering
- Inbuilt Web Category Database
- URL, keyword, File type block
- Categories: Default(82+), Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Schedule-based access control
- Custom block messages per category
- Block Java Applets, Cookies, Active X
- CIPA Compliant
- Data leakage control via HTTP, HTTPS upload

Application Filtering
- Inbuilt Application Category Database
- Application Categories: e.g. Gaming, IM, P2P, Proxy : 11+
- Schedule-based access control
- Block
    - P2P applications e.g. Skype
    - Anonymous proxies e.g. Ultra surf
    - "Phone home" activities
    - Keylogger
- Layer 7 (Applications) & Layer 8 (User - Identity) Visibility

Web Application Firewall##
- Positive Protection model
- Unique "Intuitive Website Flow Detector" technology
- Protection against SQL Injections, Cross-site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning
- Support for HTTP 0.9/1.0/1.1
- Extensive Logging & Reporting
- Back-end servers supported: 5

Virtual Private Network
- IPSec, L2TP, PPTP
- Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms - MD5, SHA-1
- Authentication - Preshared key, Digital certificates
- IPSec NAT Traversal
- Dead peer detection and PFS support
- Diffie Hellman Groups - 1,2,5,14,15,16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support for tunnel end points
- VPN connection redundancy
- Overlapping Network support
- Hub & Spoke VPN support

SSL VPN
- TCP & UDP Tunneling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam
- Multi-layered Client Authentication - Certificate, Username/Password
- User & Group policy enforcement
- Network access - Split and Full tunneling
- Browser-based (Portal) Access - Clientless access
- Lightweight SSL VPN Tunneling Client
- Granular access control to all the Enterprise Network resources
- Administrative controls - Session timeout, Dead Peer Detection, Portal customization
- TCP- based Application Access - HTTP, HTTPS, RDP, TELNET, SSH

Instant Messaging (IM) Management
- Yahoo and Windows Live Messenger
- Virus Scanning for IM traffic
- Allow/Block Login
- Allow/Block File Transfer
- Allow/Block Webcam
- Allow/Block one-to-one/group chat
- Content-based blocking
- IM activities Log
- Archive files transferred
- Custom Alerts

Wireless WAN
- USB port 3G and Wimax Support#
- Primary WAN link
- WAN Backup link

Bandwidth Management
- Application and User Identity based Bandwidth Management
- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery
- Multi WAN bandwidth reporting
- Category-based bandwidth restriction

User Identity and Group Based Controls
- Access time restriction
- Time and Data Quota restriction
- Schedule based Committed and Burstable Bandwidth
- Schedule based P2P and IM Controls

Networking
- Failover - Automated Failover/Failback, Multi-WAN failover, 3GModem failover
- WRR based load balancing
- Policy routing based on Application and User
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay
- Support for HTTP Proxy
- Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding
- Parent Proxy support with FQDN
- "IPv6 Ready" Gold Logo

High Availability
- Active-Active
- Active-Passive with State Synchronization
- Stateful failover
- Alerts on appliance status change

Administration & System Management
- Web-based configuration wizard
- Role-based access control
- Firmware Upgrades via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Styler
- Command Line Interface (Serial, SSH, Telnet)
- SNMP (v1, v2c, v3)
- Multi-lingual support: Chinese, Hindi, French, Korean
- Cyberoam Central Console (Optional)
- NTP Support

User Authentication
- Internal database
- Active Directory Integration
- Automatic Windows Single Sign On
- External LDAP/RADIUS database integration
- Thin Client support - Microsoft Windows Server 2003 Terminal Services and Citrix XenApp
- RSA securID support
- External Authentication - Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

Logging/Monitoring
- Graphical real-time and historical monitoring
- Email notification of reports, viruses and attacks
- Syslog support
- Log Viewer - IPS, Web filter, Anti Virus, Anti Spam, Authentication, System and Admin Events

On-Appliance Cyberoam-iView Reporting
- Integrated Web-based Reporting tool - Cyberoam-iView
- 1000+ drilldown reports
- 45+ Compliance Reports
- Historical and Real-time reports
- Multiple Dashboards
- Username, Host, Email ID specific Monitoring Dashboard
- Reports - Security, Virus, Spam, Traffic, Policy violations, VPN, Search Engine keywords
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Automated Report Scheduling

IPSec VPN Client***
- Inter-operability with major IPSec VPN Gateways
- Supported platforms: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit
- Import Connection configuration

Certification
- ICSA Firewall - Corporate
- Checkmark UTM Level 5 Certification
- VPNC - Basic and AES interoperability
- "IPv6 Ready" Gold Logo

Compliance
CE
FCC

Dimensions

H x W x D (inches)	1.7 x 16.8 x 10.3
H x W x D (cms)	4.3 x 42.7 x 26.2
Weight	5.3 kg, 11.68 lbs

Power

Input Voltage	100-240 VAC
Consumption	90W
Total Heat Dissipation (BTU)	200

Environmental

Operating Temperature	5 to 40 °C
Storage Temperature	0 to 70 °C
Relative Humidity (Non condensing)	10 to 90%

---

*If Enabled, will bypass traffic only in case of power failure. ##Subscription available in all the Models of CR50ia & above. For further details refer to WAF Datasheet.

**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.

***Additional Purchase Required. #3G card and modem details are not included. See http://www.cyberoam.com for supported USB devices. ##Subscription available in all the Models of CR50ia & above.

Cyberoam®
Unified Threat Management