



Cyberoam NG series of Unified Threat Management appliances are the Next-Generation network security appliances that include UTM security features and performance required for future networks. The NG series for SOHO offer “the fastest UTM’s made for SMBs” to small offices. The best-in-class hardware along with software to match, enables the NG series to offer unmatched throughput speeds, compared to any other UTM appliance in this market segment. This assures support for future IT trends in organizations like high-speed Internet and rising number of devices in organizations – offering future-ready security for small office networks.



With Cyberoam NG series, businesses get assured Security, Connectivity and Productivity. The Layer 8 Technology treats User-Identity as the 8th Layer or the HUMAN layer in the protocol stack. It attaches User-Identity to security, which adds speed to an organization’s security by offering instant visibility into the source of attacks by username rather than only IP address. Cyberoam’s Extensible Security Architecture (ESA) supports feature enhancements that can be developed rapidly and deployed with minimum efforts, offering future-ready security to organizations.

The ‘Next-Generation’ Series for SOHO:

Offering “the fastest UTM’s made for SMBs” to Small Offices

Cyberoam’s **Layer 8 Technology** treats “User Identity” as the 8th Layer in the protocol stack



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 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
- Content Security**
 - Anti-Virus/Anti-Spyware
 - Anti-Spam
 - HTTPS/SSL Content Security
- Administrative Security**
 - Next-Gen UI



Connectivity

- Business Continuity**
 - Multiple Link Management
- Network Availability**
 - VPN
 - 3G/4G/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 Visibility & Control
- Administrator Productivity**
 - Next-Gen UI



Specification

Interfaces

Copper GbE Ports	3
Configurable Internal/DMZ/WAN Ports	Yes
Console Ports (RJ45)	1
USB Ports	2

System Performance*

Firewall throughput (UDP) (Mbps)	1,000
Firewall throughput (TCP) (Mbps)	750
New sessions/second	3,500
Concurrent sessions	60,000
IPSec VPN throughput (Mbps)	110
No. of IPSec Tunnels	50
SSL VPN Throughput (Mbps)	50
Anti-Virus throughput (Mbps)	180
IPS throughput (Mbps)	140
UTM throughput (Mbps)	80

Stateful Inspection Firewall

- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Location-aware and Device-aware Identity-based Access Control Policy
- Access Control Criteria (ACC): User-Identity, Source and Destination Zone, MAC and IP address, Service
- Security policies - IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and QoS
- Country-based Traffic Control
- Access Scheduling
- Policy based Source and Destination NAT, Gateway Specific NAT Policy
- H.323, SIP NAT Traversal
- DoS and DDoS attack prevention
- MAC and IP-MAC filtering
- Spoof Prevention

Intrusion Prevention System

- Signatures: Default (4500+), Custom
- IPS Policies: Pre-configured Zone-based multiple policies, Custom
- Filter based selection: Category, Severity, Platform and Target (Client/Server)
- IPS actions: Allow Packet, Drop Packet, Disable, Drop Session, Reset, Bypass Session
- User-based policy creation
- Automatic signature updates via Cyberoam Threat Research Labs
- Protocol Anomaly Detection
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

Gateway Anti-Virus & Anti-Spyware

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

Gateway Anti-Spam

- Inbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- Language and Content-agnostic spam protection using RPD Technology
- Zero Hour Virus Outbreak Protection
- IP address Black list/White list
- Spam Notification through Digest
- IP Reputation based Spam filtering

Web Filtering

- On-Cloud Web Categorization
- Controls based on URL, Keyword and File type
- Web Categories: Default (89+), External URL Database, Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Block Java Applets, Cookies, Active X, Google Cache pages
- CIPA Compliant
- Data leakage control by blocking HTTP and HTTPS upload
- Schedule-based access control
- Custom Denied Message per Web Category
- Safe Search enforcement, YouTube for Schools

Application Filtering

- Layer 7 (Applications) & Layer 8 (User - Identity) Control and Visibility
- Inbuilt Application Category Database
- Control over 2,000+ Applications classified in 21 Categories
- Filter based selection: Category, Risk Level, Characteristics and Technology
- Schedule-based access control
- Securing SCADA Networks
 - SCADA/ICS Signature-based Filtering for Protocols Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk
 - Control various Commands and Functions

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
- Threat Free Tunnelling (TFT) Technology

SSL VPN

- TCP & UDP Tunnelling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam (Local)
- Multi-layered Client Authentication - Certificate, Username/Password
- User & Group policy enforcement
- Network access - Split and Full tunnelling
- Browser-based (Portal) Access - Clientless access
- Lightweight SSL VPN Tunnelling 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

Wireless WAN

- USB port 3G/4G and WiMAX Support
- Primary WAN link
- WAN Backup link

Bandwidth Management

- Application, Web Category and Identity based Bandwidth Management
- Schedule-based Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery
- Data Transfer Report for multiple Gateways

Networking

- Multilink Load Balancing
- Automated Failover/Failback
- WRR based Load balancing
- Interface types: Alias, Bridge Pair, LAG (port trunking), VLAN, VVLAN
- DNS-based inbound load balancing
- IP Address Assignment - Static, PPPoE (with Schedule Management), L2TP, PPTP & DDNS, Client, Proxy ARP, Multiple DHCP Servers support, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding
- IPv6 Support:
 - Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
 - Management over IPv6
 - IPv6 routing protocols
 - IPv6 tunneling (6in4, 6to4, 6rd, 4in6)
 - Alias and VLAN
 - DNSv6 and DHCPv6 Services
 - Firewall security over IPv6 traffic

High Availability

- Active-Active
- Active-Passive with state synchronization
- Stateful Failover with LAG Support

Administration & System Management

- Web-based configuration wizard
- Role-based Access control
- Support of API
- Firmware Upgrades via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Styler
- Command Line Interface (Serial, SSH, Telnet)
- SNMP (v1, v2, v3)
- NTP Support
- Multi-lingual support: English, Chinese, Hindi, French, Japanese
- Cyberoam Central Console/CCMS (Optional)

User Authentication

- Internal database
- AD Integration with support for OU-based Security Policies
- Automatic Windows Single Sign On
- External LDAP/LDAPS/RADIUS database Integration
- Thin Client support
- 2-factor authentication: 3rd party support**
- User/MAC Binding
- SMS (Text-based) Authentication
- Layer 8 Identity over IPv6
 - Secure Authentication - AD, LDAP, Radius
 - Clientless Users
 - Authentication using Captive Portal

Logging/Monitoring

- Real-time Logging and Monitoring
- Log Viewer - IPS, Web filter, Anti-Virus, Anti-Spam, Authentication, System and Admin Events
- Forensic Analysis with quick identification of network attacks and other traffic anomalies
- Syslog support
- 4-eye Authentication

IPSec VPN Client**

- Inter-operability with major IPSec VPN Gateways
- Import Connection configuration

Certification

- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo
- Global Support Excellence - ITIL compliance (ISO 20000)

Hardware Specifications

Memory	2GB
Storage	4GB

Compliance

- CE
- FCC

Dimensions

H x W x D (inches)	1.7 x 6 x 9.1
H x W x D (cms)	4.4 x 15.3 x 23.2
Weight	1.5 kg, 3.307 lbs

Power

Input Voltage	100-240 VAC
Consumption	13.2W
Total Heat Dissipation (BTU)	45

Environmental

Operating Temperature	0 to 40 °C
Storage Temperature	-25 to 75 °C
Relative Humidity (Non condensing)	10 to 90%

*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.

For details, refer Cyberoam's Technical Alliance Partner list on Cyberoam website. *Additional Purchase Required. For list of compatible platforms, refer to OS Compatibility Matrix on Cyberoam DOCS.

Toll Free Numbers

USA : +1-800-686-2360 | India : 1-800-301-00013

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

Applicable to Hardware Version 1.0 – 23/08/2013

Copyright © 1999-2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.
Cyberoam and Cyberoam logo are registered trademark of Cyberoam Technologies Pvt. Ltd. Although Cyberoam has attempted to provide accurate information, Cyberoam assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Cyberoam has the right to change, modify, transfer or otherwise revise the publication without notice. PL-10-1000252-100423

