Cyberoam NG series of Unified Threat Management appliances are the Next-Generation network security appliances that include UTM security features along with performance required for future networks. The NG series for SMEs are the “fastest UTMs” made for this segment. 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 to SMEs.

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: The fastest UTMs made for SMEs

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
  - Web Application Firewall

- Content Security
  - Anti-Virus/Anti-Spyware
  - Anti-Spam (Inbound/Outbound)
  - HTTPS/SSL Content Security

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

Connectivity

- Business Continuity
  - Multiple Link Management
  - High Availability

- 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
**Interfaces**

- Copper GE Ports: 8
- Configurable Internal/DMZ/WAN Ports: Yes
- Console Ports (RJ45): 1
- USB Ports: 2
- Hardware Bypass Segment*: 2

**System Performance**

- Firewall Throughput (UDP): 6,500 Mbps
- Firewall Throughput (TCP): 4,000 Mbps
- New sessions/second: 45,000
- Concurrent sessions: 1,000,000
- IPSec VPN Throughput (Mbps): 850
- No. of IPSec Tunnels: 2,000
- SSL VPN Throughput (Mbps): 300
- WAF Protected Throughput (Mbps): 450
- Anti-Virus Throughput (Mbps): 1,500
- IPS Throughput (Mbps): 1,600
- UTN Throughput (Mbps): 850

**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 certificate/IP-MAC filtering
- Spoof Prevention

**Intrusion Prevention System**

- Signatures: Default (4500+), Custom
- IPS policies: Pre-configured Zone-based multiple policies, Custom
- Filler based selection: Category, Severity, Platform and Target (Client/Server)
- IPS actions: Recommended, 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 HTTPS, FTP, SMTP/IPS, POP3, IMAP, IM, VPN Tunnels
- Customize individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size
- Block by file types

**Gateway Anti-Spam**

- inbound and Outbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Language and Content-agnostic spam protection using RPD Technology
- Zero Hour Virus Outbreak Protection
- Self Service Quarantine area
- IP address Block list/White list
- Spam Notification through Digest
- IPS 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, Controls based on URL, Keyword and File type
- CIPA Compliant
- Data leakage control by blocking HTTPS and HTTP uploads
- Schedule-based access control
- Custom Denied Message per Web Category
- Control various Commands and Functions

**Application Filtering**

- Layer 7 (Applications) & Layer B (User - Identity) Control and Visibility
- Inbound 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
- Visibility and Controls for HTTPS based Micro-Apps like Facebook chat, YouTube video upload
- Securing SCADA Networks

**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 etc.
- Support for HTTP 0.9, 0.91, 1.1
- Back-end servers supported: 5 to 300 servers

**Virtual Private Network**

- IPSec, L2TP, PPTP
- Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms - MDS, SHA-1
- Authentication: Preshared key, Digital certificates
- IPSec NAT Traversal
- Dead peer detection and FPS support
- SRF Fallback Groups: 1, 2, 5, 14, 15, 16
- MAC certificate/IP-MAC filtering
- Spoof Prevention

**SSL VPN**

- TCP & UDP Tunneling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam (Local)
- 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, SSL

**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
- Guaranteed & Burstable bandwidth policy
- Application & User based Identity Traffic Filtering
- Data Transfer Report for multiple Gateways

**Architecture**

- WRR based Multilink Load Balancing
- Automated Failover/Recovery
- Interface types: Alias, Multiprotocol Bridge, LAG (port trunking), VLAN, WWAN, TAP
- 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 HTTPS Proxy, Parent Proxy with FDGN
- Dynamic Routing: RIP v1/v2, OSPF, BGP, PIM-SM, Multicast Forwarding
- IP Source guard
- Support of ICMP to integrate third-party DLP, Web Filtering and AV applications
- Discover mode for PoC Deployments
- IPv6 Support:
  - Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
  - Management over IPv6
  - IPv6 Route: Static and Source
  - IPv6 tunneling (6in4, 6to4, 6rd, 6in6)
  - Alias and VLAN
  - DNSv6 and DHCPv6 Services

**Firewall Security over IPv6 traffic**

- High Availability for IPv6 networks

**High Availability**

- Active-Active
- Active-Active 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, v2c)
- Multi-lingual: English, Chinese, Hindi, French, Japanese, Cyberoam Central Console (Optional)

**User Authentication**

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

**Logging/Monitoring**

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

**On-Appliance Cyberoam-View Reporting**

- Integrated Web-based Reporting tool
- Integrated Fault reports
- Compliance reports - HIPAA, GLBA, SOX, PCI, FISMA
- Zone based application reports
- History and Real-time reports
- User & Group policy enforcement
- Default Dashboards: Traffic and Security
- Application, Web & Security Management, Checkpoint, User Threat Quotient (UTQ) for high risk users and more
- Client Types Report including BYOD Client Types
- Multi-factor reports - tabular, graphical
- Export reports in - PDF, Excel, HTML
- Email notification of reports
- Report customization - Custom view and custom logo
- Supports 3rd party PSA Solution - ConnectWise

**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
- Compact Flash: 4GB
- HDD: 250GB or higher

**Compliance**

- CE
- FCC

**Dimensions**

- H x W x D (inches): 17.9 x 14.6 x 17.3
- H x W x D (cm): 44.4 X 37.2 X 44
- Weight: 4 kg, 8.8 lbs

**Power**

- Input Voltage: 100-240 VAC
- Consumption: 99W
- Total Heat Dissipation (BTU): 338

**Environmental**

- Operating Temperature: 0 to 40 °C
- Storage Temperature: -25 to 75 °C
- Relative Humidity (Non condensing): 10 to 95%

*1 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. **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: +1-800-666-2360 | India: +91-80-1301-0013
APAC/Africa: +91-777-0368 | Europe: +44-808-120-3958

---

**Cyberoam**

- www.cyberoam.com | sales@cyberoam.com
- Copyright ©1999-2016 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.
- Cyberoam and Cyberoam logos 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 a information rather this is strictly testing purpose. Cyberoam will not be held liable for any damages or losses arising from the use of this publication without notice. 1-115-0-927389