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.

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

**Productivity**
- Employee Productivity
  - Content Filtering
  - Instant Messaging Archiving & Controls
- IT Resource Optimization
  - Bandwidth Management
  - Traffic Discovery
  - Application Visibility & Control
- Administrator Productivity
  - Next-Gen UI
Apac/mea:

- For details, refer Cyberoam’s Technical Alliance Partner list on Cyberoam website. *Additional Purchase Required.

Www.cyberoam.com

- Custom Denied Message per Web Category
- Block Java Applets, Cookies, Active X, Google Cache
- Block Malware, Phishing, Pharming URLs
- Web Categories: Default (89+), External URL Database
- IP Reputation based Spam filtering
- Spam Notification through Digest
- Self Service Quarantine area
- Zero Hour Virus Outbreak Protection
- Language and Content-agnostic spam protection using Subject line tagging
- Block by file types
- Spyware, Malware, Phishing protection
- Virus, Worm, Trojan Detection and Removal
- Protocol Anomaly Detection
- 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, 1.0, 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 - MD5, SHA-1
- Authentication: Pre-shared key, Digital certificates
- IPSec NAT Traversal
- Dead peer detection and PFS support
- Diffie Hellman Groups - 1, 2, 5, 14, 16
- Export Certificate Authority
- Export Road Warrior connection configuration
- Domain name support, Tunnel endpoint controls
- VPN connection redundancy
- Overlapping Network support
- Hub & Spoke VPN support
- Threat Free Tunneling (TFT) Technology

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 (IP): Access - Clientless access
- Lightweight SSL 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

Wireless WAN

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

Bandwidth Management

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

Networking

- WRR based Multilink Load Balancing
- Automated Failover/Failback
- Interface types: Alias, Multiprotot Bridge, LAG (port trunking), VLAN, WWAN, TAP
- DNS-based inbound load balancing
- IP Address Assignment - Static, PPPoE (with Schedule Management), L2TP, PPTP & DDNS5, Client, Proxy ARP5, Multicast DHCP Servers support, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1 v2, OSPF, BGP, PIM-SM, Multicast Forwarding
- Support of IACP 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, 4in6)
  - Alias and VLAN
  - DNS6v and DHCP6v Services

- Firewall security over IPv6 traffic
- High Availability for IPv6 networks

High Availability

- Active-Supervise
- 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 Theme
- 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 OU-based Security Policies
- Automatic Windows/RADIUS Single Sign On
- External LDAP/LDAPS/RADIUS database Integration
- Thin Client support
- 2-factor authentication: 3rd party support2
- SMS (Text-based) Authentication
- Layer & Identity over IPv6
- Secure Authentication – AD, LADAP, 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 Admin Events
- Forensic Analysis with quick identification of network attacks and other traffic anomalies
- Syslog support
- 4-eye Authentication

On-Device Cyberoam/View Reporting

- Integrated Web-based Reporting tool
- 1,200+ drilldown reports
- Complaint reports - HIPAA, GLBA, SOX, PCI, FISMA
- Zone based application reports
- History and Real-time reports
- Default Dashboards: Traffic and Security
- Reports – Application, Internet & Web Usage, Mail Usage, Attacks, Spam, Virus, Search Engine, User Threat quotient (UTQ) for high risk users and more
- Client Types Report including BYOD Client Types
- Multi-format 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 certified - AES interoperability
- IPv6 Ready Gold Logo
- Global Support Excellence - ITIL compliance (ISO 20000)

Hardware Specifications

- Memory
  - 2GB
- Hard Disk Flash
  - 4GB
- HDD
  - 250GB or higher

Compliance

- CE
- FCC

Dimensions

- Height X W X D (inches)
  - 19.0 X 17.3 X 11.85
- Weight
  - 11.04 lbs

Power

- Input Voltage
  - 100-240 VAC
- Consumption
  - 137W
- Total Heat Dissipation (BTU)
  - 467

Environmental

- Operating Temperature
  - 0 to 40 °C
- Storage Temperature
  - -20 to 70 °C

*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.