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 UTMs 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.

Cyberoam UTM features assure Security, Connectivity, Productivity.
**System Performance**
- Firewall Throughput (UDP) (Mbps): 3,700
- Firewall Throughput (TCP) (Mbps): 2,400
- New sessions/second: 21,000
- Concurrent sessions: 750,000
- IPSec VPN Throughput (Mbps): 280
- No. of IPSec Tunnel: 850
- SSL VPN Throughput (Mbps): 100
- WAF Protected Throughput (Mbps): 150
- Anti-Virus Throughput (Mbps): 600
- IPS Throughput (Mbps): 650
- UTM Throughput (Mbps): 300

**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, Antivirus, Anti-spoam 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
- Spam 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: Recommended, Allow Packet, Drop Packet, Disable, Drop Session, Bypass Session
- User-based policy creation
- Automatic signature updates via Cyberoam Threat Research Labs
- Protocol Anomaly Detection
- SCADA-aware IP 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/S, POP3, IMAP, IM, VPN Tunnels
- Customize individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size
- Block by file type

**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 blacklist/white list
- Spam Notification through Digest
- IP Reputation based Spam filtering

**Web Filtering Category**
- Blocking or URL 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 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
- Visibility and Controls for HTTPS based Micro-Apps like Facebook chat, Youtube video upload
- Securing SCADA Networks
  - SCADA/ICS Signature-based Filtering for Protocols Modbus, DN3P, IEC, BACnet, Omron FINS, Secure DN3P, Longtalk
  - Control various Commands and Functions

**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 Poisening etc.
- Support for HTTP 0.91/0.1,1
- 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: 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/Import Warrior connection configuration
- Domain name support for tunnel end points
- VPN connection redundy
- Overlapping Network support
- Hub & Spoke VPN support
- Threat Free Tunneling (TFT) Technology

**SSL VPN**
- TCP & UDP Tunneling
- Certification - 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, 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 MultiLoad Balancing
- Automated Failover/Fallback
- Interface types: Alias, Multiprotocol Bridge, LAG (port trunking), VLAN, WAN, TAP
- DNS-based multi-hop 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 FGDN
- Dynamic Routing: RIP v1/v2, OSPF, BGP, PIM-SM, Multipath Forwarding
- 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-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 through 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**
- Local 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 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 Admin Events
- Forensic Analysis with quick identification of network attacks and other traffic anomalies
- System Logs
- 4-eye Authentication

**On-Application Cyberoam-View Reporting**
- Integrated Web-based Reporting tool
- 2+1 user-friendly drilldown
- Compliance reports - HIPAA, GLBA, SOX, PCI, FISMA
- Zone based application reports
- Historical and Real-time reports
- Default Dashboards: Traffic and Security
- Username, Host, Email ID specific Monitoring Dashboard
- Reports – Application, Internal & 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 - Basic and AES interoperability
- IPv6 Ready Gold Logo
- Global Support Excellence - ITIL compliance (ISO 20000)

**Hardware Specifications**
- Memory: 2GB
- Compact Flash: 2GB
- HDD: 250GB or higher

**Compliance**
- CE
- FCC

**Dimensions**
- H x W x D (inches): 17.2 x 4.3 x 2.3
- Weight: 2.3 kg, 5.07 lbs

**Power**
- Input Voltage: 100-240 VAC
- Power Consumption: 47.8W
- Total Heat Dissipation (BTU): 163

**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.