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 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.
Interface
- Copper GbE Ports: 8
- Configurable Internal/DMZ/WAN Ports: Yes
- Console Ports (RJ45): 1
- USB Ports: 2
- Hardware Bypass Switch: 2

System Performance
- Firewall Throughput (UDP) (Mbps): 8,000
- Firewall Throughput (TCP) (Mbps): 5,000
- No. of IPS Tunnels: 60,000
- Concurrent sessions: 3,000,000
- IPSec VPN Throughput (Mbps): 400
- WAF Protected Throughput (Mbps): 700
- Anti-Virus Throughput (Mbps): 2,200
- IPS Throughput (Mbps): 2,500
- UTM Throughput (Mbps): 1,050

Stateful Inspection Firewall
- Layer 2 & 3 (IPv4 & IPv6)
- Multiple Security Zones
- Location-aware and Device-aware Identity-based Access Control
- 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 Service and Destination NAT, Gateway
- Specific NAT Policy
- H.323, SIP NAT Traversal
- DoS and DDoS attack prevention
- MAC address 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 HTTP, HTTPS, FTP, SMTP/POP3, POP3, IMAP, IM, VPN Tunnels
- Customizable user session
- 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), BBL 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
- IPS reputation based spam filtering

Web Filtering
- Cloud-based Web categorization
- Controls based on URL, Keyword and file type
- Web categorization: Default (98+), External URL Database, Custom
- Protocols supported: HTTP, HTTPS
- Blacklist Malware, Phishing, Phishing URLs
- Block Java Applets, Cookies, Active X, Google Cache pages
- GIP Compliant
- Data leakage control by blocking HTTP and HTTPS upload
- Schedule-based access control
- Custom Denied Message by Web Category
- Safe Search enforcement, YouTube for Schools

Application Layer
- Layer 7 (Applications) & User - Identity) Control and Visibility
- Inbuilt Application Category database
- Control over 2,000+ Applications classified in 21 categories
- Filter based selection: Category, Risk, Level, and Technology
- Schedule-based access control
- Visibility and Controls for HTTP based Micro-Apps like Facebook chat, YouTube video upload
- Securing SCADA Networks
  - SCADA/ICS Signature-based Filtering for Protocols Modbus, DNP3, IEC, Bacnet, OMM, DNS Secure
  - DNP3, 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 Poisoning etc.
- Support for HTTP 0.9/0.10/1.1
- 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: Pre-shared key, Digital certificates
- IPSec NAT Traversal
- Dead Peer detection and PFS support
- Diffie Hellman Groups - 1, 2, 5, 14, 15, 16
- MAC address filtering
- Export Route Watchdog connection configuration
- Domain name support
- Tunnel endpoint bolster
- 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 (RD) 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
- WiFi Backup link

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

Lossless Wired multid Link Load Balancing
- Automated Failover/Failback
- Interface types: 10/100/1000Base-T, Fiber, Port A, Port B
- DNS-based 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, PIM-SM, multicast forwarding
- Support of IACP to integrate third-party DLP, Web filtering and AV applications
- Discovery mode for PoC Deployments
- IPv6 Support.
- Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
- Management over IPv6
- IPv6 routing: Static and Source
- IPv6 tunneling (6in4, 6to4, 6rd, 6in6)
- Alias and VLAN
- DNSv6 and DHCPv6 Services