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, offering unmatched throughput speeds compared to any other UTM appliance in this market. The FleXi Ports (XP) available in CR200iNG-XP UTM appliances offer flexible network connectivity with I/O slot that allows additional Copper/Fiber 1G/10G ports on the same security appliance. To SMEs who want to shift to Fiber 1GbE/10GbE connectivity, FleXi Ports give freedom from forced purchase of higher end security appliances to get desired I/O interfaces. FleXi Ports consolidate the number of devices in a network, offering benefits of power efficiency, reduced network complexity and reduced OPEX.

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 offers security across Layer 2-Layer 8 using Identity-based policies by treating Layer 8 as “User Identity.” This technology allows organizations to manage and secure user access to resources based on the identity of the user rather than just their IP address. This enhances security by providing granular access control and visibility into user activity.

Cyberoam’s Layer 8 Technology treats “User Identity” as the 8th Layer in the protocol stack. This technology offers instant visibility into the source of attacks by username rather than only IP address, adding speed to an organization’s security.

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/WMAX 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**
- Maximum available Ports: 14
- Fixed Copper GE Ports: 6
- Number of Slots for Flexi Ports Module: 8 / 4 / 4
- Port options per Flexi Ports Module**: **(GBE Copper/GBE Fiber/10GBE Fiber)
- Console Ports (RJ45): 1
- Configurable Internal/DMZ/WAN Ports: 1
- USB Ports: Yes
- Hardware Bypass Segment*: 2

**System Performance**
- Firewall Throughput (UDP): 14,000
- Firewall Throughput (TCP): 8,000
- New sessions/second: 85,000
- Concurrent sessions: 3,200,000
- IPsec VPN Throughput (Mbps): 1,150
- No. of IPS Tunnels: 4,500
- SSL VPN Throughput (Mbps): 450
- WAF Protected Throughput (Mbps): 1,000
- Anti-Virus Throughput (Mbps): 2,600
- IPS Throughput (Mbps): 30,000
- UTM Throughput (Mbps): 1,400

**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 OoS
- 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 (450+), Custom
- IPS Policies: Pre-configured Zone-based multiple policies, Custom
- Filtered selection category: Curation, 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
- 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 Outreach Protection
- Self Service Quarantine area
- IP address Black list/White list
- Spam Notification through Digest
- IP Reputation based Spam filtering

**Application Filtering**
- Layer 7 (Applications) & Layer 8 (User - Identity) Control and Visibility
- Inbuilt Application Category Database
- Controls 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, DNP3, IEC, BACnet, Omron FINS, 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 0.9/1.0, 1.1
- End-back 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 PFS support
- Diffsie Hellman Groups - 2, 5, 14, 15, 16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support and tunnel end points
- 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 (Portal) - 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, SHE

**Wireless WAN**
- USB port 3G/4G and WiMAX Support
- Primary WAN link
- WLAN Backlink

**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, Multiport Bridge, LG (port trunking), VLAN, WWAN, TAP
- DNS Server, DHCP, Domain load balancing
- IP Address Assignment - Static, PPPoE with (Session Management), L2TP, PPTP & DDNS, Client, Proxy ARP
- DHCP RADIUS 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 application
- Discover mode for PoE 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
- DNSv6 and DHCPv6 Services

**Application Filtering**
- Firewall security over IPv4 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 via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Style
- 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 O/U-based Security Policies
- Automatic Windows/RADIUS Single Sign On
- External 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 Admin Events
- Forensic Analysis with quick identification of network attacks and other traffic anomalies
- Syslog support
- 4-eye Authentication

**On-Apppliance Cyberoam-View Reporting**
- Integrated Web-based Reporting tool
- 1,200+ drilldown reports
- Compliance reports - HIPAA, GLBA, SOX, PCF, FISMA
- Zone based application reports
- Historical and real-time reports
- Default Dashboards: Traffic and Security
- Userband, Hot Email ID specific Monitoring Dashboard 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+
- ICISA 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**
- Height x Width x Depth (inches): 17 x 17.3 x 11.85
- Height x Width x Depth (cm): 44.4 x 43.9 x 30.1
- Weight: 5.1 kg, 11.24 lbs

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

**Environmental**
- Operating Temperature: 0 to 40 °C
- Storage Temperature: 0 to 70 °C
- Relative Humidity (Non-condensing): 10 to 90%