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.

The ‘Next-Generation’ Series for SOHO:
Offering “the fastest UTMs made for SMBs” to Small Offices

Cyberoam’s Layer 8 Technology treats “User Identity” as the 8th Layer in the protocol stack

Cyberoam UTM features assure Security, Connectivity, Productivity

**Security**
- Network Security
  - Firewall
  - Intrusion Prevention System
- Content Security
  - Anti-Virus/Anti-Spyware
  - Anti-Spam
  - HTTPS/SSL Content Security
- Administrative Security
  - Next-Gen UI

**Connectivity**
- Business Continuity
  - Multiple Link Management
- 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
**System Performance**
- Firewall throughput (UDP) (Mbps): 400
- Firewall throughput (TCP) (Mbps): 300
- New sessions/second: 2,000
- Concurrent sessions: 27,500
- IPSec VPN throughput (Mbps): 100
- No. of IPSec Tunnels: 25
- SSLVPN Throughput (Mbps): 25
- Anti-Virus throughput (Mbps): 100
- IPS throughput (Mbps): 90
- UTM throughput (Mbps): 60

**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 GoS
- 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

**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, 15, 16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support for tunnel end points
- VPN connection redundancy
- Overlapping Network support
- Hub & Spoke VPN support
- Threat Free Tunnelling (TFT) Technology

**Gateway Anti-Virus & Anti-Spyware**
- Virus, Worm, Trojan Detection and Removal
- Spyware, Malware, Phishing protection
- Automatic virus signature database update
- Scans HTTP, FTP, SMTP, POP3, IMAP, IM, VPN traffic
- Customize individual user scanning
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

**Intrusion Prevention System**
- Signatures: Default, Custom
- IPS Policies: Pre-configured Zone-based multiple policies, Custom
- Filter based selection: Category, Severity, Platform and Target (Client/Server)
- IPS actions: Allow Packet, Drop Packet, Disable, Drop Session, Reset, Bypass Session
- User-based policy creation
- Regular signature updates via Cyberoam Threat Research Labs
- Protocol Anomaly Detection
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

**SSL VPN**
- TCP & UDP Tunnelling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam (Local)
- Multi-layered Client Authentication - Certificate, Username/Password, User & Group policy enforcement
- Network access - Split and Full tunnelling
- Browser-based (Portal) Access - Clientless access
- Lightweight SSL VPN Tunnelling Client
- Granular access control to all the enterprise network resources
- Administrative controls - Session timeout, Dead Peer Detection, Portal customization
- TCP based Application Access - HTTPS, RDP, TELNET, SSH

**Wireless WAN**
- USB port 3G/HG and WiMAX Support
- Primary WAN link
- WAN Backup link

**Bandwidth Management**
- Application, Web category and Identity based Bandwidth Management
- Schedule-based 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, Multiprot Bridge, LAG (port trunking), VLAN, WWAN
- DNS-based inbound load balancing
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS, Client, Proxy ARP Multiple DHCP Servers support, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1,v2,v, OSPF, BGP PIM-SM, Multicast forwarding
- IPv4 Support
- Dual Stack Architecture: Support for IPv4 and IPv6
- IPv6 Route: Static and Source

**Application Filtering**
- Layer 7 (Applications) & Layer 8 (User - Identity)
- Control and Visibility
- In-built Application Category Database
- 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 Filtering**
- On-Cloud Web Categorization
- Controls based on URL, Keyword and File type
- Web Categories: Default (89*), External URL Database, Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Block Java Applets, Cookies, ActiveX, Google Cache pages
- Pre-defined CIPA compliance policy

**Compliance**
- CE
- FCC

**Power**
- Input Voltage: 100-240 VAC
- Consumption: 22 W
- Total Heat Dissipation (BTU): 75

**Environmental**
- Operating Temperature: 0 to 40 °C
- Storage Temperature: -25 to 75 °C
- Relative Humidity (Non condensing): 10 to 90%

**Specifications**
- Total Heat Dissipation (BTU)
- Input Voltage
- Storage Temperature
- Relative Humidity (Non condensing)

**System Performance**
- Firewall throughput (UDP) (Mbps): 400
- Firewall throughput (TCP) (Mbps): 300
- New sessions/second: 2,000
- Concurrent sessions: 27,500
- IPSec VPN throughput (Mbps): 100
- No. of IPSec Tunnels: 25
- SSLVPN Throughput (Mbps): 25
- Anti-Virus throughput (Mbps): 100
- IPS throughput (Mbps): 90
- UTM throughput (Mbps): 60

**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 GoS
- 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

**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, 15, 16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support for tunnel end points
- VPN connection redundancy
- Overlapping Network support
- Hub & Spoke VPN support
- Threat Free Tunnelling (TFT) Technology

**Gateway Anti-Virus & Anti-Spyware**
- Virus, Worm, Trojan Detection and Removal
- Spyware, Malware, Phishing protection
- Automatic virus signature database update
- Scans HTTP, FTP, SMTP, POP3, IMAP, IM, VPN traffic
- Customize individual user scanning
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

**Intrusion Prevention System**
- Signatures: Default, Custom
- IPS Policies: Pre-configured Zone-based multiple policies, Custom
- Filter based selection: Category, Severity, Platform and Target (Client/Server)
- IPS actions: Allow Packet, Drop Packet, Disable, Drop Session, Reset, Bypass Session
- User-based policy creation
- Regular signature updates via Cyberoam Threat Research Labs
- Protocol Anomaly Detection
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

**SSL VPN**
- TCP & UDP Tunnelling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam (Local)
- Multi-layered Client Authentication - Certificate, Username/Password, User & Group policy enforcement
- Network access - Split and Full tunnelling
- Browser-based (Portal) Access - Clientless access
- Lightweight SSL VPN Tunnelling Client
- Granular access control to all the enterprise network resources
- Administrative controls - Session timeout, Dead Peer Detection, Portal customization
- TCP based Application Access - HTTPS, RDP, TELNET, SSH

**Wireless WAN**
- USB port 3G/HG and WiMAX Support
- Primary WAN link
- WAN Backup link

**Bandwidth Management**
- Application, Web category and Identity based Bandwidth Management
- Schedule-based 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, Multiprot Bridge, LAG (port trunking), VLAN, WWAN
- DNS-based inbound load balancing
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS, Client, Proxy ARP Multiple DHCP Servers support, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1,v2,v, OSPF, BGP PIM-SM, Multicast forwarding
- IPv4 Support
- Dual Stack Architecture: Support for IPv4 and IPv6
- IPv6 Route: Static and Source

**Application Filtering**
- Layer 7 (Applications) & Layer 8 (User - Identity)
- Control and Visibility
- In-built Application Category Database
- 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 Filtering**
- On-Cloud Web Categorization
- Controls based on URL, Keyword and File type
- Web Categories: Default (89*), External URL Database, Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Block Java Applets, Cookies, ActiveX, Google Cache pages
- Pre-defined CIPA compliance policy