Cyberoam®
A SOPHOS Company

NG | Future-ready | CR 10iNG | Cyberoam®

CRIOiNG
Future-ready

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

L8	USER
L7	Application
L6	Presentation ASCII, EBCDIC, ICA
L5	Session L2TP, PPTP
L4	Transport TCP, UDP
L3	Network 192.168.1.1
L2	Data Link 00-17-BB-8C-E3-E7
L1	Physical

Cyberoam UTM offers security across Layer 2-Layer 8 using Identity-based policies

---
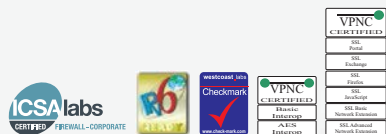
Cyberoam UTM features assure Security, Connectivity, Productivity

Security

Network Security
- Firewall
- Intrusion Prevention System

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

Interfaces

Copper GbE Ports	3
Configurable Internal/DMZ/WAN Ports	Yes
Console Ports (RJ45)	1
USB Ports	2

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
SSL VPN 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 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
- Spoof Prevention

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

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/S, POP3, IMAP, IM, VPN traffic
- Customize individual user scanning
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

Gateway Anti-Spam
- Inbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- Language and Content-agnostic spam protection using RPD Technology
- Zero Hour Virus Outbreak Protection
- IP address Black list/White list
- Spam Notification through Digest
- IP Reputation based Spam filtering

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, Active X, Google Cache pages
- Pre-defined CIPA compliance policy
- Data leakage control by blocking HTTP and HTTPS 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
- 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

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 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

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 - HTTP, HTTPS, RDP, TELNET, SSH

Wireless WAN
- USB port 3G/4G 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, Multiport 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, OSPF, BGP, PIM-SM, Multicast Forwarding
- IPv6 Support:
  - Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
  - IPv6 Route: Static and Source
  - IPv6 tunneling (6in4, 6to4, 6rd, 4in6)
  - 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 via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Styler
- Command Line Interface (Serial, SSH, Telnet)
- SNMP (v1, v2c)
- NTP Support
- Multi-lingual support: English, Chinese, Hindi, French, Japanese
- Cyberoam Central Console/CCMS (Optional)

User Authentication
- Internal database
- AD Integration with support for 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**
- User/MAC Binding
- SMS (Text-based) Authentication
- Layer 8 Identity over IPv6
  - Secure Authentication – AD, LDAP, Radius
  - Clientless Users
  - Authentication using Captive Portal

Logging/Monitoring
- Graphical real-time logging and monitoring
- Syslog support
- Log Viewer - Firewall, IPS, Web filter, Anti Virus, Anti Spam, Authentication, System and Admin Events

IPSec VPN Client***
- Inter-operability with major IPSec VPN Gateways
- Import Connection configuration

Certification
- ICSA Firewall - Corporate
- Checkmark Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo
- Global Support Excellence - ITIL compliance (ISO 20000)

Hardware Specifications

Memory	1GB
Storage	4GB

Compliance
CE
FCC

Dimensions

H x W x D (inches)	1.35 x 8.75 x 6.8
H x W x D (cms)	3.43 x 22.23 x 17.3
Weight	1.10 kg, 2.42 lbs

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%

*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.

Cyberoam®
A SOPHOS Company