Cyberoam®
A SOPHOS Company

CR35wiNG

NG Future-ready | CR35wiNG — Cyberoam

NG Future-ready — **CR35wiNG**

Future-ready Security with Wi-Fi Access Point for SOHO/ROBO networks

CR35wiNG is the Next-Generation Unified Threat Management appliance with Wi-Fi access points that offer "the fastest UTMs made for SMBs" to small offices with high performance security over WLAN. CR35wiNG appliances come with 3x3 MIMO technology that greatly enhances wireless range and performance . It supports 802.11a/b/g/n wireless standards. Combined with security over wired networks offered by its range of UTM appliances, Cyberoam enables organizations to overcome the physical limitations of securely accessing network resources and offers more user flexibility, user productivity and lower network ownership costs.

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.

Cyberoam's Layer 8 technology that treats user-identity as the 8th Layer or the HUMAN layer in the protocol stack, works even in WLAN environments, to allow Identity-based security policies in dynamic IP environment.

The 'Next-Generation' UTM Series for SOHO:
Faster performance, broader coverage with 3x3 MIMO Technology

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

COMMON CRITERIA CERTIFIED EAL4+ — ICSA labs CERTIFIED FIREWALL-CORPORATE — R6 READY — Checkmark www.check-mark.com — VPNC CERTIFIED Basic Interop AES Interop — VPNC CERTIFIED SSL Portal SSL Exchange SSL Firefox SSL JavaScript SSL Basic Network Extension SSL Advanced Network Extension

Cyberoam UTM features assure Security. Connectivity. Productivity

Security

Network Security
- Firewall
- Intrusion Prevention System
- Web Application Firewall
- Wireless Security

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

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	6
Configurable Internal/DMZ/WAN Ports	Yes
Console Ports (RJ45/DB9)	1
USB Ports	2

Built-in Wireless LAN

Wireless Standards	IEEE 802.11 a/b/g/n (WEP, WPA, WPA2, 802.11i , TKIP, AES, PSK)
Antenna	Detachable 3x3 MIMO
Access Points	Up to 8 bssid
Transmit Power (EIRP)	11n HT40 : +15dBm 11b CCK: +15dBm 11g OFDM:+15dBm
Receiver Sensitivity	-68dBm at 300Mbps -70dBm at 54Mbps -88dBm at 6Mbps
Frequency Range	2.412 GHz - 2.472 GHz 5.200 GHz - 5.825 GHz
Number of Selectable Channels	USA (FCC) - 11 channels, EU (ETSI) / Japan (TELEC) - 13 channels
Data Rate	802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54Mbps 802.11b: 1, 2, 5,5, 11Mbps 802.11n: up to 450Mbps

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 Tunnels	850
SSL VPN Throughput (Mbps)	100
WAF Protected Throughput	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
- Access Control Criteria (ACC) - User - Identity, Source & Destination Zone, MAC and IP address, Service
- Security policies - IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and QoS
- Access Scheduling
- Policy based Source & Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS & DDoS Attack prevention
- MAC & IP-MAC filtering and Spoof prevention

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

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 Black list/White list
- Spam Notification through Digest
- IP Reputation based Spam filtering

Intrusion Prevention System
- Signatures: Default (4500+), Custom
- 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
- Automatic signature updates via Cyberoam Threat Research Labs
- Protocol Anomaly Detection
- DDoS attack prevention
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

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
- Schedule-based access control
- Custom block messages per category
- Block Java Applets, Cookies, Active X
- CIPA Compliant
- Data leakage control by blocking HTTP and HTTPS upload
- Safe Search enforcement, YouTube for Schools

Application Filtering
- Layer 7 (Applications) & Layer 8 (User - Identity) Visibility
- Inbuilt Application Category Database
- 2,000+ Applications Supported
- 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
- 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 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&UDPTunneling
- Authentication - AD, LDAP, RADIUS, Cyberoam
- 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
- 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 Reports for multiple Gateways

Networking
- WRR based Multilink Load Balancing
- Automated Failover/Failback
- Interface types: Alias, Multiport Bridge, LAG (port trunking), VLAN, WLAN, WWAN, TAP
- DNS-based inbound 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-SIM, Multicast Forwarding
- Discover mode for PoC Deployments
- IPv6 Support:
  - Dual Stack Architecture: Support for IPv4 and IPv6
  - 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

Administration & System Management
- Web-based configuration wizard
- Role-based access control
- Firmware Upgrades via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Styler
- Command Line Interface (Serial, SSH, Telnet)
- SNMP (v1, v2c)
- Multi-lingual support: Chinese, Hindi, French, Korean
- Cyberoam Central Console (Optional)
- NTP Support

User Authentication
- Internal 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 logging and monitoring
- Syslog support
- Log Viewer - Firewall, IPS, Web filter, Anti Virus, Anti Spam, Authentication, System and Admin Events

On-Appliance Cyberoam-iView Reporting

- Integrated Web-based Reporting tool
- 1,200+ drilldown reports
- 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, 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
- Supported platforms: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit
- 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)	1.7 x 6 x 9.1
H x W x D (cms)	4.4 x 15.3 x 23.2
Weight	2.3kg, 5.07 lbs

Power

Input Voltage	100-240 VAC
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.

Cyberoam®
A SOPHOS Company