Cyberoam®
## A SOPHOS Company

NG **CR 2500iNG**
Future-ready

Next-Generation Firewall for Large Enterprise Networks | CR2500iNG

The mobilization of workforce has led to demand for anytime-anywhere access to network resources. This, along with increasing number of users like customers and partners connecting to an enterprise network from outside, and trends like rise in number of network users and devices, application explosion, virtualization, and more are leading to loss of security controls for enterprises over their networks. Cyberoam Next-Generation Firewalls (NGFW) with Layer 8 Identity-based technology offer actionable intelligence and controls to enterprises that allow complete security controls over L2-L8 for their future-ready security. Cyberoam's Human Layer 8 acts like a standard abstract layer that binds with real Layers 2-7, enabling organizations to regain lost security controls.

Cyberoam NGFW appliances offer inline application inspection and control, website filtering, HTTPS inspection, Intrusion Prevention System, VPN (IPSec and SSL) and granular bandwidth controls. Additional security features like WAF, Gateway Anti-Virus, Anti-Spam are also available.

Cyberoam security appliances offer high performance, assured Security, Connectivity and Productivity and an Extensible Security Architecture (ESA) for future-ready security in large enterprises.
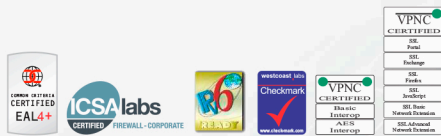
Next-Generation Firewalls for Large Enterprises:
Offering Actionable Intelligence and Controls

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 NGFW offers security across Layer 2-Layer 8 using Identity-based policies

VPNC CERTIFIED — SSL Portal, SSL Exchange, SSL Firefox, SSL JavaScript, SSL Basic Network Extension, SSL Advanced Network Extension

COMMON CRITERIA CERTIFIED EAL4+

ICSA labs CERTIFIED FIREWALL - CORPORATE

R6 READY

westcoast labs Checkmark www.checkmark.com

VPNC CERTIFIED — Basic Interop, AES Interop

Cyberoam NGFWs assure Security, Connectivity, Productivity

Security

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

Administrative Security
- Next-Gen UI
- iView- Logging & Reporting

Content Security
- Anti-Virus/Anti-Spyware
- Anti-Spam (Inbound/Outbound)
- HTTPS/SSL Content Security

Connectivity

Business Continuity
- Multiple Link Management
- High Availability

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	14
1GbE SFP (Mini GBIC) Ports	4
10GbE SFP (Mini GBIC) Ports	4
Configurable Internal/DMZ/WAN Ports	Yes
Console Ports (RJ45)	1
USB Ports	2
Hardware Bypass Segments*	2
RAID 1 (with two disk)	Yes

System Performance**

Firewall throughput (UDP) (Mbps)	40,000
Firewall throughput (TCP) (Mbps)	28,000
New sessions/second	200,000
Concurrent sessions	8,100,000
IPSec VPN throughput (Mbps)	8,000
No. of IPSec Tunnels	4,500
SSL VPN throughput (Mbps)	1,000
WAF throughput (Mbps)	2,000
Anti-Virus throughput (Mbps)	6,000
IPS throughput (Mbps)	8,000
NGFW throughput (Mbps)***	5,500
Fully Protected Throughput (Mbps)****	4,500

Stateful Inspection Firewall
- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- 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 Bandwidth Management
- Application (Layer 7) Control and Visibility
- Access Scheduling
- Policy based Source and Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS and DDoS Attack prevention
- MAC and IP-MAC filtering and Spoof prevention

Application Filtering
- Inbuilt Application Category Database
- 2,000+ Applications Supported
- Schedule-based access control
- Block
    - Proxy and Tunnel
    - File Transfer
    - Social Networking
    - Streaming Media
- Layer 7 (Applications) & Layer 8 (User - Identity) Visibility
- Securing SCADA Networks
    - SCADA/ICS Signature-based Filtering for Protocols
    - Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk
    - Control various Commands and Functions

Intrusion Prevention System (IPS)
- Signatures: Default (4500+), Custom
- IPS Policies: Multiple, Custom
- User-based policy creation
- Automatic real-time updates from CRProtect networks
- Protocol Anomaly Detection
- DDoS attack prevention
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

User Identity and Group Based Controls
- Access time restriction
- Time and Data Quota restriction
- Schedule-based Committed and Burstable Bandwidth
- Schedule-based P2P and IM Controls

Administration and 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, v2, v3)
- Multi-lingual support: English, Chinese, Hindi, French, Japanese
- Cyberoam Central Console (Optional)
- Network Time Protocol Support

User Authentication
- Internal database
- Active Directory Integration
- Automatic Windows Single Sign On
- External LDAP/RADIUS database integration
- Thin Client support - Microsoft Windows Server 2003/2008

- Terminal Services and Citrix XenApp - Novell eDirectory
- RSA SecurID support
- External Authentication - Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

Logging and Monitoring
- Graphical real-time and historical monitoring
- Email notification of reports, gateway status, viruses and attacks
- Syslog support
- Log Viewer - Firewall, IPS, Web filter, WAF, Anti Virus, Anti Spam, Authentication, System and Admin Events

On-Appliance Cyberoam-iView Reporting
- Integrated Web-based Reporting tool - Cyberoam-iView
- 1200+ drilldown reports
- 45+ Compliance Reports
- Historical and Real-time reports
- Multiple Dashboards
- Username, Host, Email ID specific Monitoring Dashboard
- Reports - Security, Virus, Spam, Traffic, VPN, Search Engine keywords
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Automated Report Scheduling

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 and Spoke VPN support

SSL VPN
- TCP and UDP Tunneling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam (Local)
- Multi-layered Client Authentication - Certificate, Username/Password
- User and 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

Web Filtering
- Inbuilt Web Category Database
- URL, keyword, File type block
- Categories: Default(89+), 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 via HTTP, HTTPS upload

Bandwidth Management
- Application and User Identity based Bandwidth Management
- Guaranteed and Burstable bandwidth policy
- Application and User Identity based Traffic Discovery
- Multi WAN bandwidth reporting
- Category-based bandwidth restriction

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

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, IMAP, IM, VPN Tunnels
- Customize individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

Gateway Anti-Spam
- Inbound/Outbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- IP address Black list/White list
- Redirect Spam mails to dedicated email address
- Image-based Spam filtering using RPD Technology
- Zero hour Virus Outbreak Protection
- Self Service Quarantine area
- Spam Notification through Digest
- IP Reputation-based Spam filtering

Wireless WAN
- USB port 3G/4G and Wimax Support
- Primary WAN link
- WAN Backup link

Networking
- Failover - Automated Failover/Failback, Multi-WAN Failover, 3G/4G Modem Failover
- WRR based load balancing
- Policy routing based on Application and User
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay
- Support for HTTP Proxy
- Dynamic Routing: RIP v1 and v2, OSPF, BGP, Multicast Forwarding
- Parent Proxy support with FQDN
- "IPv6 Ready" Gold Logo

High Availability
- Active-Active
- Active-Passive with State Synchronization
- Stateful failover
- Alerts on appliance status change

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 32/64-bit
- Import Connection configuration

Certification
- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark Certification
- VPNC - Basic and AES interoperability
- "IPv6 Ready" Gold Logo

Hardware Specifications

Memory	6GB
HDD (HOT Swappable)	250GB or higher

Compliance
CE
FCC
UL

Dimensions

H x W x D (inches)	3.54 x 17.52 x 23.23
H x W x D (cms)	9 x 44.5 x 59
Weight	19kg, 41.8lbs

Power

Input Voltage	90-260 VAC
Consumption	258 W
Total Heat Dissipation (BTU)	881
Redundant Power Supply	Yes

Environmental

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

*If Enabled, will bypass traffic only in case of power failure. **Antivirus, IPS and Fully Protected Throughput performance is measured based on HTTP traffic as per RFC 3511 guidelines. Actual performance may vary depending on the real network traffic environments.***NGFW throughput is measured with Firewall, IPS and Web & Application Filtering features turned on. ****Fully Protected Throughput is measured with Firewall, IPS, Web & Application Filtering and Anti-Virus features turned on. *****Additional Purchase Required.

Yuriana
SERVICE S.A.C.
Consultoría & Soporte Tecnológico Empresarial