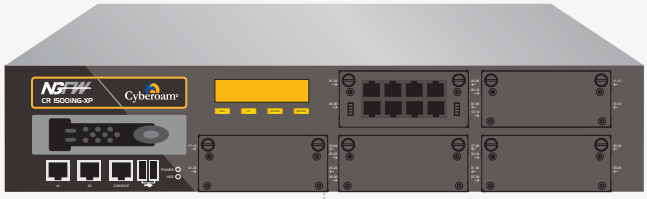
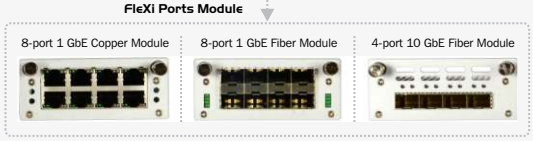
Cyberoam
A SOPHOS Company



FleXi Ports Module



CRI500iNG-XP
Future-ready

Next-Generation Firewall for Enterprise Networks | CRI500iNG–XP

Data Sheet

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 CR1500iNG-XP offers 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. The FleXi Ports (XP) available in CR1500iNG-XP appliances offer flexible network connectivity with I/O slots that allow additional Copper 1G, Fiber 1G/10G ports on the same security appliance.

Cyberoam security appliances offer high performance, assured Security, Connectivity and Productivity and an Extensible Security Architecture (ESA) for future-ready security in enterprises.

Next-Generation Firewall for 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

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
- FleXi Ports (XP)

Productivity

Employee Productivity
- Content Filtering
- Instant Messaging Archiving & Controls

IT Resource Optimization
- Bandwidth Management
- Traffic Discovery
- Application Visibility & Control

Administrator Productivity
- Next-Gen UI

Specification

Interfaces

Maximum number of Available Ports	42
Fixed Copper GbE Ports	10
Number of Slots for FleXi Ports Module	4
Port options per FleXi Ports Module* (GbE Copper/GbE Fiber/10GbE Fiber)	8 / 8 / 4
Console Ports (RJ45)	1
Configurable Internal/DMZ/WAN Ports	Yes
USB Ports	2

System Performance**

Firewall Throughput (UDP) (Mbps)	140,000
Firewall Throughput (TCP) (Mbps)	60,000
New sessions/second	265,000
Concurrent sessions	15,000,000
IPSec VPN Throughput (Mbps)	8,000
No. of IPSecTunnels	8,500
SSL VPN Throughput (Mbps)	1,050
WAF Protected Throughput (Mbps)	2,300
Anti-Virus Throughput (Mbps)	9,000
IPS Throughput (Mbps)	15,000
NGFW Throughput (Mbps)***	8,250
Fully Protected Throughput (Mbps)****	6,750

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 (4500+), Custom
- IPS Policies: Pre-configured Zone-based multiple policies, Custom
- Filter based selection: Category, 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

Application Filtering

- Layer 7 (Applications) & Layer 8 (User - Identity) Control and Visibility
- Inbuilt Application Category Database
- Control 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

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)
- Command Line Interface (Serial, SSH, Telnet)
- SNMP (v1, v2, v3)
- Multi-lingual : English, Chinese, Hindi, French, Japanese
- Cyberoam Central Console (Optional)

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 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-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

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 - AD, 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

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, Google Cache pages
- CIPA Compliant
- Data leakage control - block HTTP and HTTPS upload
- Schedule-based access control
- Safe Search enforcement, YouTube for Schools

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

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

Gateway Anti-Virus & Anti-Spyware

- Virus, Worm, Trojan Detection and Removal
- Spyware, Malware, Phishing protection
- Automatic virus signature database update
- Scans HTTP/S, FTP, SMTP/S, POP3, IMAP, 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
- 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

Wireless WAN

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

Networking

- WRR based Multilink Load Balancing
- Automated Failover/Failback
- Interface types: Alias, Multiport Bridge, LAG (port trunking), VLAN, 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
- Support of ICAP to integrate third-party DLP, Web Filtering and AV applications
- Discover mode for PoC 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
  - Firewall security over IPv6 traffic
  - High Availability for IPv6 networks

High Availability

- Active-Active
- Active-Passive with state synchronization
- Stateful Failover with LAG Support

IPSec VPN Client*******

- Inter-operability with major IPSec VPN Gateways
- 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	12GB
Compact Flash	4GB
HDD	250GB or higher

Compliance

CE
FCC

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	0 to 70 °C
Relative Humidity (Non condensing)	10 to 90%

*Additional purchase required. FleXi Ports are not HOT swappable. Appliance needs to be turned off prior to changing the FleXi Ports Module. **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. *****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.

Toll Free Numbers

USA : +1-800-686-2360 | **India :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Applicable to Hardware Version 1.0 – 10 February, 2014

Cyberoam
A SOPHOS Company