Cyberoam
A SOPHOS Company

NG Future-ready

Next-Generation Firewalls for Enterprise networks

Tech Sheet

The mobilization of workforce, increasing number of external users like customers and partners 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 offers inline application inspection and control, website filtering, HTTPS inspection, Intrusion Prevention System, VPN (IPSec and SSL) and granular bandwidth controls. Additional features like WAF, FleXi Ports, 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 enterprises.

NG Series NGFW Appliances : 500iNG-XP, 750iNG-XP, 1000iNG-XP, 1500iNG-XP, 2500iNG-XP

Feature Specifications

Stateful Inspection Firewall
- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Location 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
- Spoof Prevention, DoS and DDoS attack prevention
- MAC and IP-MAC filtering

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

Intrusion Prevention System (IPS)
- 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

Administration and System Management
- Web-based configuration wizard
- Role-based Access control
- Support of External Policy Manager (XML API)
- 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: English, Chinese, Hindi, French, Japanese
- Cyberoam Central Console (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 and 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 - 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
- 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
- Web Category-based Bandwidth allocation and prioritization
- Block Java Applets, Cookies, Active X, Google Cache pages
- CIPA Compliant
- 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

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

*For details, refer Cyberoam's Technical Alliance Partner list on Cyberoam website.
#Additional Purchase Required

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, HTTPS, FTP, SMTP/S, POP3, IMAP, IM, VPN Tunnels
- Customize individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size

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

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-SM, 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
  - 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)

Specifications	500iNG-XP	750iNG-XP	1000iNG-XP	1500iNG-XP	2500iNG-XP
Interfaces					
Copper GbE Ports (Fixed)	8	8	10	10	10
Number of Slots for FleXi Ports Module	2	2	4	4	4
Port options per FleXi Ports Module* (1 GbE Copper / 1 GbE SFP / 10 GbE SFP)	8 / 8 / 4	8 / 8 / 4	8,4 / 8 / 4	8,4 / 8 / 4	8,4 / 8 / 4
Console Ports (RJ45)	1	1	1	1	1
USB Ports	2	2	2	2	2
Hardware Bypass Segments**	2	2	Yes#	Yes#	Yes#
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes	Yes
System Performance*					
Firewall Throughput (UDP) (Mbps)	25,000	28,500	120,000	140,000	160,000
Firewall Throughput (TCP) (Mbps)	18,000	20,000	45,000	60,000	70,000
New sessions/second	180,000	200,000	240,000	265,000	300,000
Concurrent sessions	4,500,000	6,400,000	13,000,000	15,000,000	20,000,000
IPSec VPN Throughput (Mbps)	3,200	4,200	5,000	8,000	10,000
No. of IPSec Tunnels	6,250	7,250	8,000	8,500	9,500
SSL VPN Throughput (Mbps)	650	750	850	1,050	1,450
WAF Protected Throughput (Mbps)	1,500	1,750	2,000	2,300	2,600
Anti-Virus Throughput (Mbps)	4,300	5,500	8,000	9,000	12,000
IPS Throughput (Mbps)	7,000	8,500	12,500	15,000	20,000
NGFW Throughput (Mbps)****	3,750	5,000	7,250	8,250	10,000
Fully Protected Throughput*****	3,000	4,000	5,800	6,750	8,250
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Dimensions					
H x W x D (inches)	1.7 x 17.44 x 18.75	1.7 x 17.44 x 18.75	3.54 x 17.52 x 23.23	3.54 x 17.52 x 23.23	3.54 x 17.52 x 23.23
H x W x D (cms)	4.4 X 44.3 X 47.62	4.4 X 44.3 X 47.62	9 x 44.5 x 59	9 x 44.5 x 59	9 x 44.5 x 59
Appliance Weight	5.1 kg, 11.24 lbs	5.1 kg, 11.24 lbs	19 kg, 41.8 lbs	19 kg, 41.8 lbs	19 kg, 41.8 lbs
Power					
Input Voltage	100-240 VAC	100-240 VAC	90-260 VAC	90-260 VAC	90-260 VAC
Consumption	208 W	208 W	258 W	258 W	258 W
Total Heat Dissipation (BTU)	345	345	881	881	881
Redundant Power Supply	-	Yes	Yes	Yes	Yes

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

*Additional Purchase required. **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. #Need to purchase the FleXi Ports module with LAN Bypass (4-port 1 GbE Copper Module).

Toll Free Numbers

USA : +1-800-686-2360 | **India :** 1-800-301-00013

APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Cyberoam® A SOPHOS Company