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.


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
- Secure SCADA Networks
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

**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
- Integration with support for OU-based Security Policies
- Automatic Windows/RADIUS Single Sign On
- External LDAP/RADIUS/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
- Authenticating using Captive Portal

**Logging and Monitoring**
- Real-time and Historical Monitoring
- Log Viewer - IPS, Web filter, WF, 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 - View Reporting**
- Integrated Web-based Reporting tool
- 1,200+ drilldown reports
- Compliance reports - HPAAA, 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 - MD2, SHA-1
- Authentication: Preshared key, Digital certificates
- IPSec NAT Traversal
- Dead peer detection and PFS support
- Diffie Hellman Groups - 1, 2, 5, 14, 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 Tunneling (TFT) Technology

**SSL VPN**
- TCP & UDP Tunneling
- Authentication - Active Directory, LDAP RADIUS, Cyberoam (Local)
- 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
- 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, Phishing URLs
- Web Category-based Bandwidth allocation and prioritization
- Block Java Applets, Cookies, Active X, Google Cache pages
- CIP 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
- 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: 2 to 300 servers

Gateway Anti-Virus & Anti-Spyware
- Virus, Worm, Trojan Detection and Removal
- Spyware, Malware, Phishing protection
- Automatic virus signature database update
- Scans HTTPS, FTP, SMTP, POP3, IMAP, IM, VPN Tunnels
- Customizable individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size

Gateway Anti-Spam
- 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
- SMTP Reputation based Spam filtering

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

Networking
- WRR based Multi-link Load Balancing
- Automated Failover/Failback
- Interface types:Aliases, Multiprotocol Bridge, DAG (port trunking), VLAN, WWAN, TAP
- DNS-based inbound load balancing
- IP/ICMP - Static, PPPoE (with Schedule Management), L2TP, PPTP & DUNs, Client, Proxy ARP, Multiple DHCP Servers supported, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1/v2, OSPF, BGP PEM-SM, Multicast Forwarding
- Support of IAPP 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 Router: Static and Source
  - IPv6 tunneling (6in4, 6to4, 6in6, 6in4n)
- Alias and VLAN
- DNSv6 and DHCPv6 Services
- Firewall security over IPv4 traffic
- High Availability for IPv6 networks

High Availability
- Active-Passive with state synchronization
- Stateful Firewall with LAG Support

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

Certification
- ISA - EAL4+
- ICSA Firewall - Corp
- Checkmark Certification
- VPAC - Basic and AES interoperability
- IPv4 Ready Gold Logo
- Global Support Excellence - ITIL compliance (ISO 20000)

For more details, refer Cyberoam’s Technical Alliance Partner list on Cyberoam website.
## Specifications

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>500iNG-XP</th>
<th>750iNG-XP</th>
<th>1000iNG-XP</th>
<th>1500iNG-XP</th>
<th>2500iNG-XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copper GbE Ports (Fixed)</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Number of Slots for FleXi Ports Module</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Port options per FleXi Ports Module</td>
<td>8 / 8 / 4</td>
<td>8 / 8 / 4</td>
<td>8.4 / 8 / 4</td>
<td>8.4 / 8 / 4</td>
<td>8.4 / 8 / 4</td>
</tr>
<tr>
<td>(1 GbE Copper / 1 GbE SFP / 10 GbE SFP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console Ports (RJ45)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>USB Ports</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Hardware Bypass Segments</td>
<td>2</td>
<td>2</td>
<td>Yes&quot;</td>
<td>Yes&quot;</td>
<td>Yes&quot;</td>
</tr>
<tr>
<td>Configurable Internal/DMZ/WAN Ports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## System Performance

<table>
<thead>
<tr>
<th></th>
<th>500iNG-XP</th>
<th>750iNG-XP</th>
<th>1000iNG-XP</th>
<th>1500iNG-XP</th>
<th>2500iNG-XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (UDP) (Mbps)</td>
<td>25,000</td>
<td>28,500</td>
<td>120,000</td>
<td>140,000</td>
<td>160,000</td>
</tr>
<tr>
<td>Firewall Throughput (TCP) (Mbps)</td>
<td>18,000</td>
<td>20,000</td>
<td>45,000</td>
<td>60,000</td>
<td>70,000</td>
</tr>
<tr>
<td>New sessions/second</td>
<td>180,000</td>
<td>200,000</td>
<td>240,000</td>
<td>265,000</td>
<td>300,000</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>4,500,000</td>
<td>6,400,000</td>
<td>13,000,000</td>
<td>15,000,000</td>
<td>20,000,000</td>
</tr>
<tr>
<td>IPSec VPN Throughput (Mbps)</td>
<td>3,200</td>
<td>4,200</td>
<td>5,000</td>
<td>8,000</td>
<td>10,000</td>
</tr>
<tr>
<td>No. of IPSec Tunnels</td>
<td>6,250</td>
<td>7,250</td>
<td>8,000</td>
<td>8,500</td>
<td>9,500</td>
</tr>
<tr>
<td>SSL VPN Throughput (Mbps)</td>
<td>650</td>
<td>750</td>
<td>850</td>
<td>1,050</td>
<td>1,450</td>
</tr>
<tr>
<td>WAF Protected Throughput (Mbps)</td>
<td>1,500</td>
<td>1,750</td>
<td>2,000</td>
<td>2,300</td>
<td>2,600</td>
</tr>
<tr>
<td>Anti-Virus Throughput (Mbps)</td>
<td>4,300</td>
<td>5,500</td>
<td>8,000</td>
<td>9,000</td>
<td>12,000</td>
</tr>
<tr>
<td>IPS Throughput (Mbps)</td>
<td>7,000</td>
<td>8,500</td>
<td>12,500</td>
<td>15,000</td>
<td>20,000</td>
</tr>
<tr>
<td>NGFW Throughput (Mbps)***</td>
<td>3,750</td>
<td>5,000</td>
<td>7,250</td>
<td>8,250</td>
<td>10,000</td>
</tr>
<tr>
<td>Fully Protected Throughput</td>
<td>3,000</td>
<td>4,000</td>
<td>5,800</td>
<td>6,750</td>
<td>8,250</td>
</tr>
<tr>
<td>Authenticated Users/Nodes</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

## Dimensions

<table>
<thead>
<tr>
<th></th>
<th>500iNG-XP</th>
<th>750iNG-XP</th>
<th>1000iNG-XP</th>
<th>1500iNG-XP</th>
<th>2500iNG-XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>H x W x D (inches)</td>
<td>1.7 x 17.44 x 18.75</td>
<td>1.7 x 17.44 x 18.75</td>
<td>3.54 x 17.52 x 23.23</td>
<td>3.54 x 17.52 x 23.23</td>
<td>3.54 x 17.52 x 23.23</td>
</tr>
<tr>
<td>H x W x D (cms)</td>
<td>4.4 x 44.3 x 47.62</td>
<td>4.4 x 44.3 x 47.62</td>
<td>9 x 44.5 x 59</td>
<td>9 x 44.5 x 59</td>
<td>9 x 44.5 x 59</td>
</tr>
<tr>
<td>Appliance Weight</td>
<td>5.1 kg, 11.24 lbs</td>
<td>5.1 kg, 11.24 lbs</td>
<td>19 kg, 41.8 lbs</td>
<td>19 kg, 41.8 lbs</td>
<td>19 kg, 41.8 lbs</td>
</tr>
</tbody>
</table>

## Power

<table>
<thead>
<tr>
<th></th>
<th>500iNG-XP</th>
<th>750iNG-XP</th>
<th>1000iNG-XP</th>
<th>1500iNG-XP</th>
<th>2500iNG-XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Voltage</td>
<td>100-240 VAC</td>
<td>100-240 VAC</td>
<td>90-260 VAC</td>
<td>90-260 VAC</td>
<td>90-260 VAC</td>
</tr>
<tr>
<td>Consumption</td>
<td>208 W</td>
<td>208 W</td>
<td>258 W</td>
<td>258 W</td>
<td>258 W</td>
</tr>
<tr>
<td>Total Heat Dissipation (BTU)</td>
<td>345</td>
<td>345</td>
<td>881</td>
<td>881</td>
<td>881</td>
</tr>
<tr>
<td>Redundant Power Supply</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 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.
- Anti-Virus, IPS and Fully Protected Throughput 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

http://www.cyberoam.com | sales@cyberoam.com

Copyright© 1999-2016 Cyberoam Technologies Pvt. Ltd. All Rights Reserved 1.1-10.6.2-290316