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.

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
- Security events and Admin Events
- Forensic Analysis with quick identification of 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 - HIPAA, GLBA, SOX, PCI, FISMA
- Zone based application reports
- Historical and Real-time report
- 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 using pre-defined key, digital certificates
- IPSec NAT Traversal
- Dead peer detection and IPSU support
- Diffsie Hellman Groups - 1, 2, 5, 14, 15, 16
- External Certificate Authority support
- Export Root Warner connection configuration
- Domain name support for tunnel end points
- VPN connection redundancy
- Overlapping Network support
- Hub & Spoke VPN
- Threat Free Tunneling (TFT) Technology

SSL VPN
- TCP & UDP Tunneling
- Authentication - AD, 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
- 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-Demand 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
- Scheduling and 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
- Posture Protection model
- Unique "Intuitive Website Flow Detector" technology
- Protection against SSL Injections, Cross-Site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning etc.
- Support for HTTPS 0.9.1.0.11
- Back-end supported servers - 5 to 300 servers

Additional purchased require. FlexiPorts are not HOT swappable. Appliance needs to be turned off prior to changing the FlexiPorts Module. Antivirus, IPS and Fully Protected Throughout performance is measured with Firewall, IPS and Web & Application Filtering features turned on. Full Protection is measured with Firewall, IPS, Web & Application Filtering and Anti-Virus features turned on. For details, refer to 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. “Need to purchase the FlexiPorts module with LAN Bypass (4-port 1 GbE Copper Modules). If Enabled, will bypass traffic only in case of power failure. 

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/IMAP, POP3, IMAP, VPN Tunnels
- Customizable individual user scanning
- Self Service Quarantine area
- Scan and delete file size
- Block by file types

Gateway Anti-Spam
- Inbound and Outbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filtering 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 Blacklist/White list
- Spam Notification through Digest
- IP Reputation based Spam filtering

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

Networking
- WRR based Multitlink Load Balancing
- Automated Failover/Failback
- Interface types: Alias, Multiport Bridge, LAG (port trunking), VLAN, WWAN, TAP
- DNS-based failover load balancing
- IP Address Assignment - Static, PPPoe (with Spectrum Management), L2TP, PPTP & DDNS, Client, Proxy ARP, Multiple DHCP Servers support, DHCP relay support
- Supports HTTP Proxy, Parent Proxy with FDQN Dynamic Routing: RIPv1 & v2, OSPF, BGP, PIM-SM, Multicast Forwarding
- Support for IPv6 ICAP to integrate third-party DLP, Web Filtering and AV applications
- Reporting for PoC Deployments
- IPv6 Support:
  - Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
  - Management over IPv6
  - IPv6 Route: Static and Source
  - IPv6 tunnels (6in4, 6to4, 6rd, 4in6)
  - Alias and VLAN
  - DNSv6 and DHCPv6 Services
  - Firewall security over IPv4 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: 16GB
- Compact Flash: 4GB
- HDD: 250GB or higher

Compliance
- 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%