Cyberoam virtual network security appliances give complete control of security in virtual data-centers, Security-in-a-Box or Office-in-a-Box set-ups, to organizations and MSSPs. Based on the need, virtual security appliances can be deployed as a UTM or NGFW. With virtualized security appliances for virtual environments, Cyberoam enables scanning of inter-VM traffic, allowing granular firewall and security policies over inter-VM traffic, and offers comprehensive network security in virtualized environments to organizations without the need for deploying a hardware security appliance anymore. Cyberoam virtual security appliances allow organizations and MSSPs to optimize the resource utilization in their own/customer networks by capitalizing on lean and peak periods of activities in the networks.

Cyberoam’s licensing model for its virtual security appliances is based on the number of vCPUs, that gives deployment flexibility to organizations and MSSPs, unlike most competitor models that are based on concurrent sessions and number of users. Organizations get maximum benefits of Cyberoam’s multi-core processing architecture with virtual security appliances by flexibly allotting vCPUs from the virtual infrastructure to the virtual security appliance. With an easy upgrade feature using a simple activation key, organizations and MSSPs can match the growing needs of their business and customers in no time.

**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 (UCC): User-Identity, Source and Destination Zone, MAC and IP address, Service
- Security policies - IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and Geo
- Country-based Traffic Control
- Access Scheduling
- Policy based Source and Destination NAT, Gateway Specific NAT Policy
- H.323, SIP NAT Traversal
- Spooled Prevention: DNS and DoDOS attack prevention
- MAC and IP-MAC filtering

**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
- Self Service Quarantine area
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

**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

**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
- Anti-spam and QoS
- DNS-based inbound load balancing
- IP address Black list/White list
- Spam Notification through Digest
- IP Reputation based Spam filtering

**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, Active X, Google Cache pages
- CIRA Compliance
- 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

**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, DNS3, IEC, Bacnet, Omron FINS, Secure DNS3, Longtalk
- Control various Commands and Functions

**Web Application Firewall**
- Interface types: AALN, Bridge, Pas, LAG (port trunking), VLAN, WAN
- DNS-based inbound load balancing
- IP Address Assignment - Static, PPPOE (with Schedule Management), L2TP PPTP & DDNS, VLAN, 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 ICP to integrate third-party DLP, Web Filtering and AV appliance
- IPv4 Support: Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
- Management over IPv6
- IPv6 Route: Static and Source
- IPv6 tunneling (6in4, 6bis, 6rd, 4in6)
- Alias and VLAN
- DNS6v and DHCP6 Services
- Firewall security over IPv6 traffic
- High Availability for IPv6 networks

**High Availability**
- Active-active
- Active-Passive with state synchronization
- Stateless Failover with LAG Support

**Virtual Private Network**
- Encryption: 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms: MD5, SHA-1
- Authentication: Pre-shared key, Digital certificates
- IPSec NAT Traversal
- Dead peer detection and FPS support
- Diffsie 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 Tunneling (TFT) Technology

**SSL VPN**
- TCP & UDP Tunneling
- Certification - 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 - HTTPS, RDP, TERMINET, SSH

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

**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

**Networking**
- WRAP based Multilink Load Balancing
- Automated Failover/Failback
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1/v2, OSPF, BGP PIM-SM, Multicast Forwarding
- Support of ICP to integrate third-party DLP, Web Filtering and AV appliance
- IPv4 Support: Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
- Management over IPv6
- IPv6 Route: Static and Source
- IPv6 tunneling (6in4, 6bis, 6rd, 4in6)
- Alias and VLAN
- DNS6V and DHCP6 Services
- Firewall security over IPv6 traffic
- High Availability for IPv6 networks

**Application Control**
- 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, DNS3, IEC, Bacnet, Omron FINS, Secure DNS3, Longtalk
- Control various Commands and Functions

**Administration and System Management**
- Web-based management (Virtual)
- Role-based Access control
- Support of External Policy Manager (XMLAPI)
- Firmware Upgrades via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Style
- Command Line Interface (Serial, SSH, Telnet)
- SNMP (v1, v2)
- Multi-lingual support: English, Chinese, Hindi, French, Japanese
- Cyberoam Central Console (Optional)

**User Authentication**
- Internal database
- AD integration for support with OU-based Security Policies
- Automatic Windows/RADIUS Single Sign On
- External LDAP/AD/LSMP/E RADIUS database Integration
- Thin Client support
- RSA SecurID 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, HAF, Anti-Virus, Anti-Spam, Authentication, System and Admin Events
- Forensic Analysis with quick identification of network attacks and other traffic anomalies
- Local and Remote reporting
- Syslog support
- 4-eye Authentication

**On-Appliance - Cyberoam Web-view Reporting**
- Integrated Web-based Reporting tool
- 1,200+ shutdown 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 logos)
- Supports 3rd party PSA Solution – ConnectWise

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

**Certification**
- Common Criteria - EAL 4+
- FIPS 140-2
- Checkmarx Vulnerability
- VXdesk - AIPS and AESS interoperability
- IPv6 Ready Gold Logo
- Global Support Excellence – ITIL compliance (ISO 20000)

*Needs e1000/e1000e/VMXNET3 emulation
Additional Purchase Required
Technical Specifications

<table>
<thead>
<tr>
<th>Hypervisor Support</th>
<th>CRIV-1C</th>
<th>CRIV-2C</th>
<th>CRIV-4C</th>
<th>CRIV-8C</th>
<th>CRIV-12C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware ESX/ESXi 4.0/4.1/5.0, VMware Workstation 7.0/8.0/9.0/0, VMware Player 4.0/5.0, Microsoft Hyper-V 2008/2012, KVM, Citrix XenServer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCPU Support (Min / Max)</td>
<td>1 / 1</td>
<td>1 / 2</td>
<td>1 / 4</td>
<td>1 / 8</td>
<td>1 / 12</td>
</tr>
<tr>
<td>Network Interface Support (Min / Max)</td>
<td>3 / 10</td>
<td>3 / 10</td>
<td>3 / 10</td>
<td>3 / 10</td>
<td>3 / 10</td>
</tr>
<tr>
<td>Memory Support (Min / Max)</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 4 GB</td>
</tr>
</tbody>
</table>

System Performance*

| firewall throughput (udp) (mbps) | 1,500 | 3,000 | 3,500 | 4,000 | 4,000 |
| firewall throughput (tcp) (mbps) | 1,200 | 2,500 | 3,000 | 3,500 | 4,000 |
| new sessions/second | 25,000 | 30,000 | 40,000 | 50,000 | 60,000 |
| concurrent sessions | 230,000 | 525,000 | 1,200,000 | 1,500,000 | 1,750,000 |
| ipsec vpn throughput (mbps) | 200 | 250 | 300 | 350 | 400 |
| no. of ipsec tunnels | 200 | 1,000 | 1,500 | 2,000 | 2,500 |
| ssl vpn throughput (mbps) | 300 | 400 | 550 | 550 | 750 |
| waf protected throughput (mbps) | 300 | 500 | 800 | 1,400 | 1,550 |
| anti-virus throughput (mbps) | 900 | 1,500 | 2,000 | 2,200 | 2,450 |
| ips throughput (mbps) | 450 | 750 | 1,200 | 1,800 | 1,900 |
| fully protected throughput (mbps) | 250 | 450 | 1,000 | 1,400 | 1,550 |
| authenticated users/nodes | Unlimited | Unlimited | Unlimited | Unlimited | Unlimited |

*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. Fully Protected Throughput is measured with Firewall, IPS, Web & Application Filtering and Anti-Virus features turned on.

Virtual Data Center

**Virtual Data Center**

- vSwitch
- Cyberoam virtual security

MSSP/ Enterprise Security-in-a-box

**MSSP/ Enterprise Security-in-a-box**

- Customer/BO 1
- Customer/BO 2
- Customer/BO n

Office-in-a-box

**Office-in-a-box**

- vSwitch
- Cyberoam virtual security

Get a 30-day FREE Evaluation of Cyberoam virtual security appliance.

Actual performance may vary depending on the real network traffic environments. Performance values given above were observed using server with Intel Xeon E5645 (2.4 GHz) and E1000E Ethernet Drivers, running VMware version ESXi 5.0 (Update 1) with 4 GB vRAM assigned to CR Virtual Security Appliance. The Number depends on the Hypervisor you are using. 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. Fully Protected Throughput is measured with Firewall, IPS, Web & Application Filtering and Anti-Virus features turned on.

Toll Free Numbers

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