Cyberoam
A SOPHOS Company

Cyberoam Virtual Network Security Appliances

Tech Sheet

Take Control of Your Security Infrastructure!

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 appliance 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 (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

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

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
- Zero Hour Virus Outbreak Protection
- Self Service Quarantine area
- 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
- 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

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
- Securing SCADA Networks
  - SCADA/ICS Signature-based Filtering for Protocols Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk
  - Control various Commands and Functions

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

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

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
- WRR based Multilink Load Balancing
- Automated Failover/Failback
- Interface types: Alias, Bridge Pair, LAG (port trunking), VLAN, WLAN, WWAN
- 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, Multicast Forwarding
- Support of ICAP to integrate third-party DLP, Web Filtering and AV applications
- IPv6 Support:
  - Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
  - Management over Ipv6,
  - IPv6 routing protocols,
  - IPv6 tunneling (6in4, 6to4, 6rd, 4in6),
  - Alias and VLAN
  - DNSv6 and DHCPv6 Services
  - Firewall security over IPv6 traffic

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

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, v2, v3)
- 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 Single Sign On
- External LDAP/LDAPS/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, 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 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

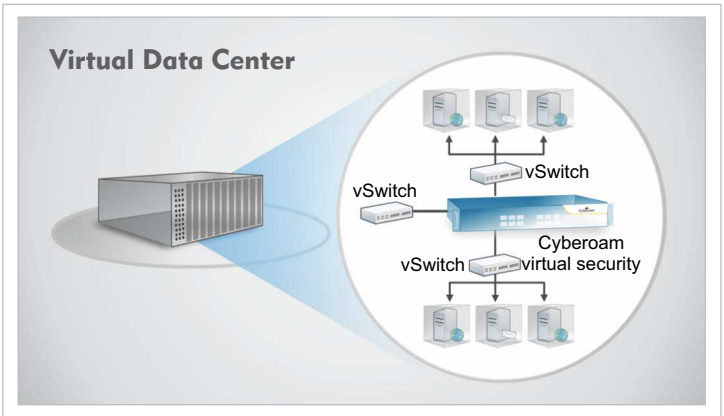
IPSec VPN Client#
- Inter-operability with major IPSec VPN Gateways
- Import Connection configuration

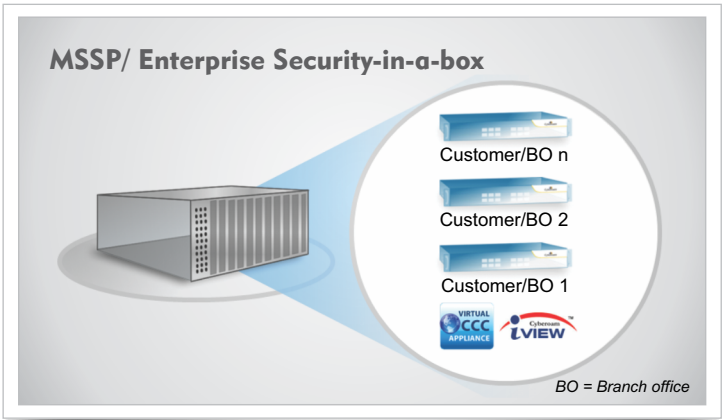
Certification
- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo
- Global Support Excellence - ITIL compliance (ISO 20000)

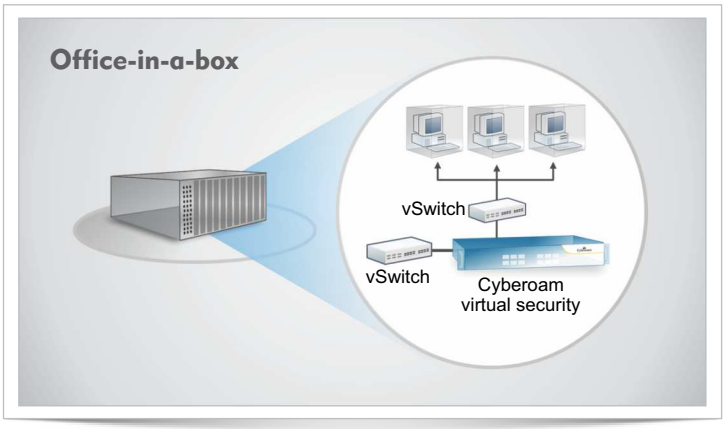
*Needs e1000/e1000e drivers emulation
#Additional Purchase Required

	CRiV-1C	CRiV-2C	CRiV-4C	CRiV-8C	CRiV-12C
Technical Specifications					
Hypervisor Support	Vmware ESX/ESXi 4.0/4.1/5.0, VMware Workstation 7.0/8.0/9.0, VMware Player 4.0/5.0, Microsoft Hyper-V 2008/2012, KVM, Citrix XenServer				
vCPU Support (Min / Max)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 12
Network Interface Support (Min / Max#)	3 / 10	3 / 10	3 / 10	3 / 10	3 / 10
Memory Support (Min / Max)	1 GB / 4 GB	1 GB / 4 GB	1 GB / 4 GB	1 GB / 4 GB	1 GB / 4 GB
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

Scenarios







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

Cyberoam
A SOPHOS Company