Cyberoam
Unified Threat Management

Cyberoam Virtual Network Security Appliances

کنترل امنیت شبکه های مجازی (Virtual) با محصول امنیت شبکه مجازی (Virtual) سایبروم

Tech Sheet

به وسیله محصولات امنیت شبکه ی مجازی (Virtual) سایبروم که مختص شبکه های مجازی یا اصطلاحاً Virtual می باشد (مانند Data center ها ، شرکت ها و ارائه کنندگان سرویس های امنیتی و ...) می توان امنیت این شبکه ها را به طور کامل تامین کرد . این ابزار به شرکت ها و مراکز تجاری بزرگ امکان می دهد بدون نیاز به صرف هزینه و تامین سخت افزار اضافه به هدف مطلوب خود دست یابند.

تکنولوژی و معماری چند هسته ای سایبروم این امکان را می دهد تا بسته به ابعاد شبکه و حجم اطلاعات انتقالی تعداد CPU مورد نظر را به این نرم افزار اختصاص داده و همین امر سبب بهره برداری حداکثری از سخت افزار و منابع موجود می شود . شبکه های مجازی (Virtual) که معمولاً تحت پلتفرم های Hyperv شرکت مایکروسافت و یا محصولات شرکت VMware از قبیل VMware workstation ، Vmware esx/esxi و VMware player و ... بهره برداری می گردند ، کاملاً با این نرم افزار سازگار بوده و به وسیله این نرم افزار می توان ترافیک درون این شبکه ها را به طور کامل کنترل و بر حسب نیاز سیاست ها و قوانین مورد نظر را اعمال کرد.

بر خلاف بیشتر شرکت های بزرگ مانند مایکروسافت که لایسنس خود را بر اساس تعداد user و یا تعداد اتصال همزمان عرضه می کنند ، مدل ارائه لایسنس سایبروم بر اساس تعداد هسته های اختصاص یافته به نرم افزار می باشد . همچنین فعال کردن نرم افزار توسط یک کد صورت می گیرد که موجب سهولت در فعال سازی و کاهش مشکلات مربوط به آن می شود.

Feature Specifications

Stateful Inspection Firewall
- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Access Control Criteria (ACC) : User-Identity, Source and Destination Zone, MAC and IP address, Service
- UTM policies - IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and Bandwidth Management
- Application (Layer 7) Control and Visibility
- Access Scheduling
- Policy based Source and Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS and DDoS attack prevention
- MAC and IP-MAC filtering and Spoof prevention

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
- Block by file types
- Add disclaimer/signature

Gateway Anti-Spam
- Inbound/Outbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- Image-spam filtering 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

Intrusion Prevention System
- Signatures: Default (4500+), Custom
- IPS Policies: Multiple, Custom
- User-based policy creation
- Automatic real-time updates from CRProtect networks
- Protocol Anomaly Detection
- DDoS attack prevention
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

Web Filtering
- Inbuilt Web Category Database
- URL, keyword, File type block
- Web Categories: Default(89+), Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Category-based Bandwidth allocation and prioritization
- Block Java Applets, Cookies, Active X
- CIPA Compliant
- Data leakage control via HTTP, HTTPS upload
- Schedule-based access control
- Custom block messages per category

Application Filtering
- Inbuilt Application Category Database
- 2,000+ Applications Supported
- Schedule-based access control
- Block
  - P2P applications e.g. Skype
  - Anonymous proxies e.g. Ultra surf
- Layer 7 (Applications) & Layer 8 (User - Identity) Visibility
- 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
- Extensive Logging and Reporting
- Back-end servers supported: 5 to 200 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

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
- 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

Bandwidth Management
- Application and User Identity based Bandwidth Management
- Category-based Bandwidth restriction
- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery
- Multi WAN bandwidth reporting

User Identity-based and Group-based Controls
- Access time restriction
- Time and Data Quota restriction, P2P and IM Controls
- Schedule-based Committed and Burstable Bandwidth

Networking
- Automated Failover/Failback, Multi-WAN
- WRR based Load balancing
- Policy routing based on Application and User
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding

High Availability*
- Active-Active
- Active-Passive with state synchronization
- Stateful Failover
- Alerts on Appliance Status change

Administration and System Management
- Web-based configuration wizard
- Role-based Access control
- 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: Chinese, Hindi, French, Korean
- Cyberoam Central Console (Optional)
- NTP Support

User Authentication
- Internal database
- Active Directory Integration
- Automatic Windows Single Sign On
- External LDAP/RADIUS database Integration
- Thin Client support - Microsoft Windows Server 2003 Terminal Services and Citrix XenApp
- RSA SecurID support
- External Authentication - Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

Logging and Monitoring
- Graphical real-time and historical Monitoring
- Email notification of reports, viruses and attacks
- Syslog support
- Log Viewer - IPS, Web filter, Anti-Virus, Anti-Spam, Authentication, System and Admin Events

On-Appliance Cyberoam - iView Reporting
- Integrated Web-based Reporting tool - Cyberoam-iView
- 1,200+ drilldown reports
- 45+ Compliance reports
- Historical and Real-time reports
- Multiple Dashboards
- Username, Host, Email ID specific Monitoring Dashboard
- Reports - Security, Spam, Virus, Traffic, Policy violations, VPN, Search Engine keywords
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Automated Report Scheduling

IPSec VPN Client[1]
- Inter-operability with major IPSec VPN Gateways
- Supported platforms: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit, Windows 8 RC1 32/64-bit
- Import Connection configuration

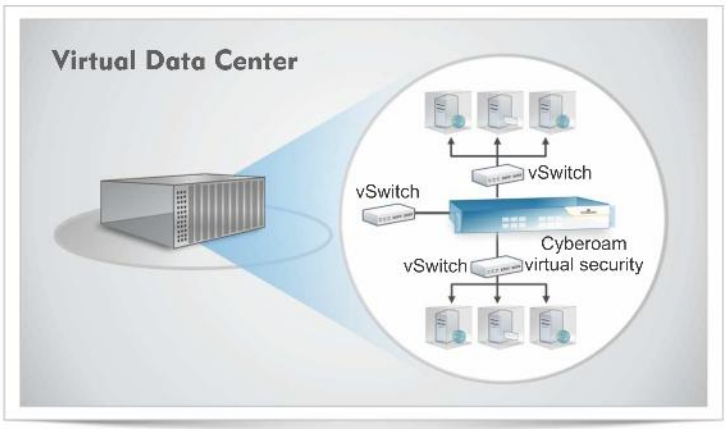
Instant Messaging (IM) Management
- Yahoo and Windows Live Messenger
- Virus Scanning for IM traffic
- Allow/Block: Login, File Transfer, Webcam, One-to-one/group Chat
- Content-based blocking
- IM activities Log
- Archive files transferred
- Custom Alerts

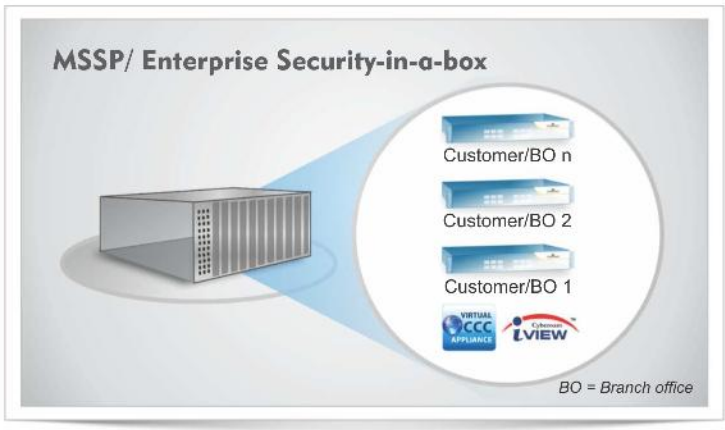
Certification
- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo

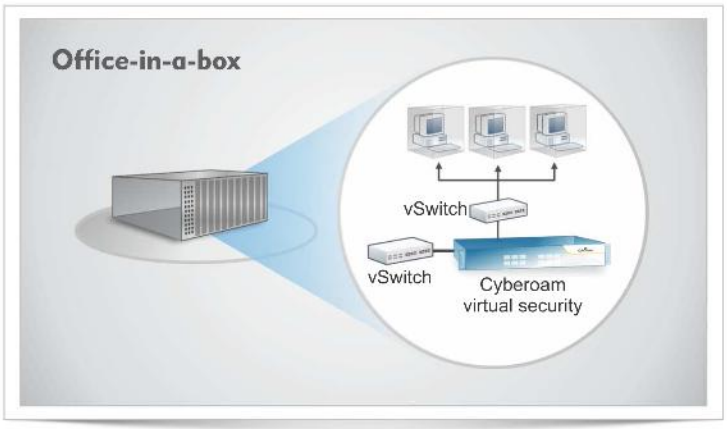
*Needs e1000/e1000e drivers emulation
[1] Additional Purchase Required

	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				
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.

گروه شرکت های کارنما
تهران، خیابان ولی عصر، بالاتر از سه راه عباس آباد، کوچه زرین، شماره ۱۳، طبقه دوم
تلفن: ۴۲۷۰۸ • فکس: ۸۸۵۵۴۳۸۷ • info@karnama.com • www.karnama.com

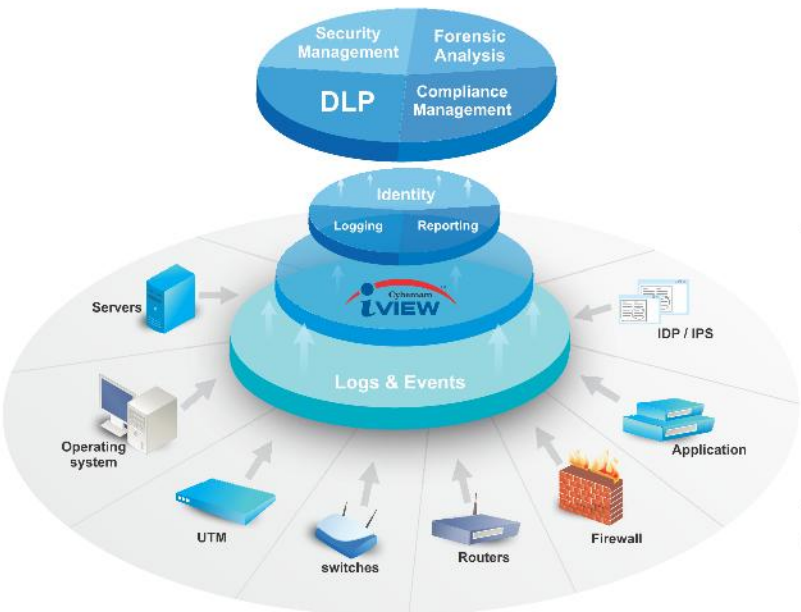
Cyberoam iVIEW TM

Tech Sheet

iview ابزاری هوشمند جهت جمع آوری اطلاعات از دستگاه های موجود در شبکه(که ممکن است در نقاط جغرافیایی مختلف قرار داشته باشند)، تهیه گزارشات این اطلاعات و نهایتا نمایش نحوه فعالیت آن ها در شبکه می باشد. پارامترهای مختلف شبکه از قبیل اطلاعات کاربران، هاست ها، مبدا و مقصد اطلاعات، پروتکل ها و ... همگی در داخل یک صفحه که اصطلاحا Dashboard گفته می شود قرار داده شده است و پیوسته بروز می گردد. این گزارشات یک نمای کلی از وضعیت امنیت در شبکه داده و می توان از آن برای اصلاح و بهبود وضعیت فعلی استفاده کرد.

وجود یک ذخیره ساز برای اطلاعات جمع آوری شده، خواندن و باز یابی اطلاعات به راحتی انجام گرفته و پیاده سازی دستگاه نیز به سهولت انجام می گیرد. با استفاده از این ابزار شرکت ها می توانند گزارشات ریز و دقیق(که به صورت تودرتو بوده و می توان از حالت کلی به ریز گزارش رسید) کاربران را در هر مکان، تحت هر دستگاه مشاهده کنند. گزارش حملات بر اساس هویت کاربر مانند Top Attackers, Top Application Used by Attackers, Top Spam Recipients, Top Viruses و ... امکان می دهد تا نقاط ضعف را سریعا شناسایی و برطرف کرد و به سطح استانداردهای مورد نظر رسید. با استفاده از گزارشات مربوط به حجم مصرفی توسط کاربران، یک رول خاص و یا یک آی پی خاص، می توان کاربران، برنامه ها و رول هایی که بیشترین استفاده از حجم ترافیک را داشته اند مشاهده کرد و شرکت ها امکان می دهد تا منابع خود را بهتر مدیریت کرده و آن را بهبود بخشند.

iview از دستگاه ها و تکنولوژی سایر تولید کنندگان و تکنولوژی های نوظهور پشتیبانی کرده و نیاز به سیستم گزارش-گیری جداگانه برای هر دستگاه را برطرف می سازد.



Cyberoam iView Work Flow

Features & Benefits

مدیریت متمرکز رخدادها و گزارشات

با وجود دستگاه های مختلف در شبکه که هر کدام با تکنولوژی خاص خود کار کرده و رخدادها را با فرمت های متفاوت ذخیره می¬کنند، تجزیه و تحلیل این رخدادها امری پیچیده وزمان بر خواهد بود. iview امکان مدیریت متمرکز رخدادها و گزارشات بر اساس شناسه کاربر و به صورت پیوسته میسر ساخته و شرکت ها با با استفاده از این گزارشات می توانند تخلفات صورت گرفته توسط کاربران را بررسی و تصمیم لازم را اتخاذ کنند.

مدیریت امنیت

با وجود دستگاه ها، برنامه ها و پروتکل های مختلف در شبکه، خطرات و تهدیدات موجود نیز پیچیده تر و متنوع تر شده اند. با یک نگاه به داشبود iview و گزارشاتی که بر اساس شناسه کاربر تهیه شده اند می توان مبدا و مقصد حملات را موقعیت یابی، و نقاط ضعف سیستم را سریعا شناسایی کرد.

مدیریت ذخیره سازی اطلاعات

iview با استفاده از تکنولوژی Raid، محدودیت دیسک های موجود را برطرف کرده و ضمن افزایش کارآیی و ظرفیت ذخیره سازی اطلاعات، از پاک شدن احتمالی(در اثر خرابی و ...) اطلاعات جلوگیری می کند. همچنین با ذخیره سازی ایمن رخدادها و گزارشات در داخل یک پایگاه داده یکپارچه، امکان بررسی و مرور سریع اطلاعات را فراهم می کند. با وجود یک ذخیره ساز ترابایتی در داخل دستگاه، امکان ذخیره سازی و نگه داری لاگ ها تا مدت زمانی طولانی ممکن می شود.

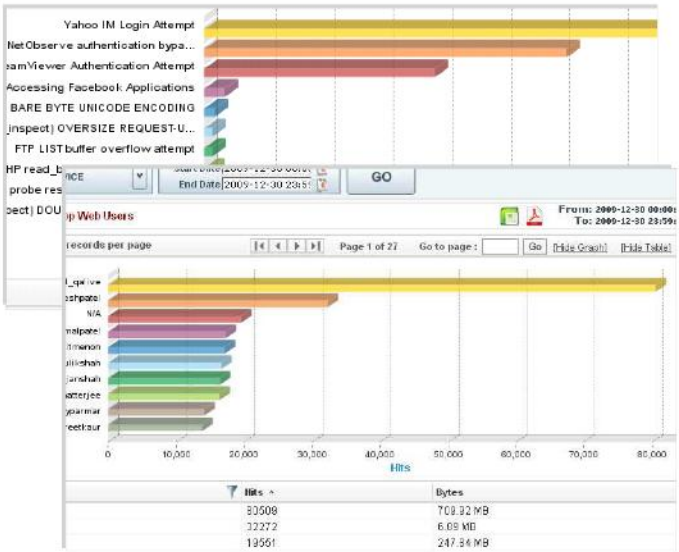
رسیدن به استانداردهای روز

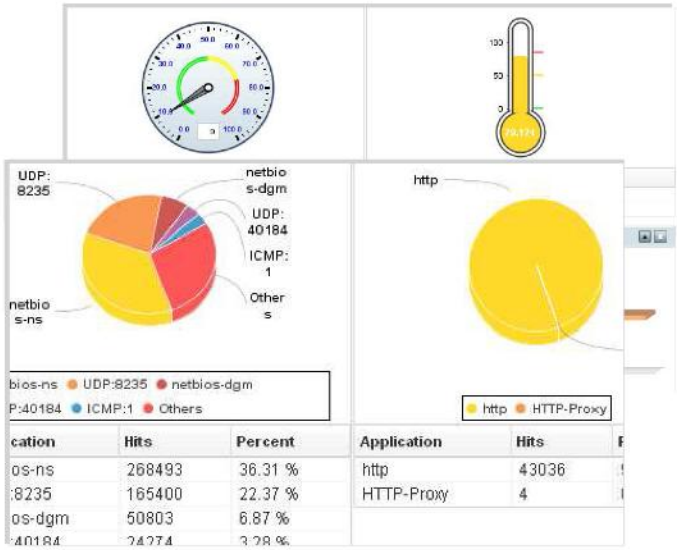
رسیدن به استانداردهای روز نیازمند بررسی اطلاعات جمع آوری شده از دستگاه های مختلف شبکه و تحلیل این اطلاعات می باشد که کاری زمان بر و پر هزینه خواهد بود. iview با کاهش در وقت وصرفه جویی در هزینه، با تولید گزارشات مختصر و مفید (که قابلیت ارائه جزئیات به صورت تو در تو را نیز دارد) شرکت ها را در تسهیل این امر یاری می کند.

پیگیری و تحلیل شواهد جرم

حفره های امنیتی می توانند هزینه های سنگینی به شرکت ها تحمیل کرده و حتی باعث ورشکستگی آن ها شوند. iview با استفاده از رخدادها و گزارشات موجود امکان بازسازی وقایع رخ داده حین ایجاد رخنه های امنیتی را داده و سبب کاهش هزینه های مربوط بررسی و آنالیز اطلاعات و گزارشات می شود.

Sample Reports





Feature Specifications

Logs
- Real-time logs
- Archived logs
- Audit logs
- Log storage (Backup/restore)

Reports
- 1000 + drilldown Reports
- Historical Reports
- Compliance Reports - HIPPA, SOX, FISMA, GLBA, PCI
- User and Group based Reports - Web, Email, IM, FTP, Application
- Internet Usage Reports - Data Transfer, Surfing Time
- Security Reports - Firewall, Attacks, Spam, Virus, Blocked Attempts
- Remote Access Reports - VPN, SSL VPN
- Search Engine Reports - Google, Yahoo, Bing, Wikipedia, Rediff, eBay
- Trend Reports
- Search Reports
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Email Alerts/automated Report Scheduling

Administration
- Web based Management Console
- Role-based administration
- Multiple Dashboards - Resource, Device, User, Host, Email Address
- Automatic Device Detection
- Device Grouping
  - device type
  - device models
- Bookmark Management
- Customized Report Views
- Data Retention

Operating Environment
- Hardened Linux OS

Supported Web Browsers
- Microsoft Internet Explorer 6.0+
- Mozilla Firefox 2.0+ (Best view)
- Google Chrome

Supported Network and Security Devices
- Custom/Proprietary devices including UTMs
- Proxy Firewalls
- Access Gateway
- Smart Wireless Router
- Web Server
- Endpoint Security Solution
- Syslog-compatible devices

Hardware Specifications

Hardware Specifications	CR-iVU25	CR-iVU100	CR-iVU200
Interfaces			
Ethernet Ports (GbE)	4	4	4
Console Ports	1 (RJ45)	1 (DB9)	1 (DB9)
USB Ports	1	Dual	Dual
Number of Hard Drives	2 (500GB each)	8 (500GB each)	8 (1TB each)
Total Available Storage	500GB	3.5TB	7TB
RAID Storage Management	RAID 1	RAID 5	RAID 5
RAM (GB)	2	4	4
Performance			
Events per Second (EPS)	250	500	1000
Devices supported (Max)	25	100	200
Dimensions			
H x W x D (inches)	1.72 x 10.83 x 17.32	3.46 x 16.7 x 20.9	3.46 x 16.7 x 20.9
H x W x D (cms)	4.4 x 27.5 x 44	8.8 x 42.4 x 53.1	8.8 x 42.4 x 53.1
Weight	3.78kg, 8.35lbs	16 kg, 36lbs	16 kg, 36lbs
Power			
Input Voltage	100-240 VAC	100-240 VAC	100-240 VAC
Consumption	65W	265W	265W
Total Heat Dissipation (BTU)	175	425	425
Environmental			
Operating Temperature	5 to 40 °C	5 to 40 °C	5 to 40 °C
Storage Temperature	20 to 70 °C	20 to 70 °C	20 to 70 °C
Relative Humidity (Non condensing)	20 to 70%	20 to 70%	20 to 70%

Cyberoam
Unified Threat Management

NG Future-ready

نسل جدید فایروال ها برای شبکه های بسیار بزرگ

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

رشد روزافزون کاربران چه در داخل شبکه و چه کاربرانی که از بیرون به شبکه متصل می شوند(مانند مشتریان، شرکا و سازمان ها) ، ثابت نبودن موقعیت مکانی این کاربران و همچنین با توجه به افزایش بی سابقه نرم افزارها و توسعه پلتفرم های مجازی سازی، تامین امنیت شبکه امری پیچیده به نظر می رسد.

نسل جدید فایروال های سایبروم به همراه تکنولوژی لایه هشت خود، امنیت شبکه شما را تضمین کرده و کنترل کامل روی لایه های ۲ تا ۸ را به شما می دهد. لایه ۸ به صورت یک لایه مجزا در بالای لایه های هفت گانه OSI قرار گرفته و هویت کاربر را مشخص می کند. بدین ترتیب می توان اعمال صورت گرفته توسط تک تک کاربران بررسی کرده و در صورت نیاز تصمیم لازم را اتخاذ کرد.

از جمله امکانات این فایروال ها می توان به بررسی و کنترل ترافیک برنامه ها، فیلترینگ وب، بررسی ترافیک HTTPS، IPS(intrusion prevention system)، VPN(Ipsec and SSL) و کنترل پهنای باند بر روی برنامه ها، کاربران و سرویس ها اشاره کرد. علاوه بر این، امکانات بیشتری از قبیل فایروال وب (WAF)، Flexi Port، آنتی ویروس (Gateway Anti Virus) و آنتی اسپم(Gateway Anti Spam) نیز موجود می باشد که در صورت نیاز باید لایسنس مربوطه تهیه گردد.

محصولات سایبروم ضمن تضمین امنیت و کارآیی بالا، دارای ساختاری می باشند که از لحاظ امنیتی قابلیت توسعه در آینده را نیز دارا می باشند.

Feature Specifications

Stateful Inspection Firewall
- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- 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 Bandwidth Management
- Application (Layer 7) Control and Visibility
- Access Scheduling
- Policy based Source and Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS and DDoS attack prevention
- MAC and IP-MAC filtering and Spoof prevention

Application Filtering
- Inbuilt Application Category Database
- 2,000+ Applications Supported
- Schedule-based access control
- Block
  - Proxy and Tunnel
  - File Transfer
  - Social Networking
  - Streaming Media
- Layer 7 (Applications) & Layer 8 (User - Identity) Visibility
- 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: Multiple, Custom
- User-based policy creation
- Automatic real-time updates from CRProtect networks
- Protocol Anomaly Detection
- DDoS attack prevention
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

User Identity-based and Group-based Controls
- Access time restriction
- Time and Data Quota restriction, P2P and IM Controls
- Schedule-based Committed and Burstable Bandwidth

Administration and System Management
- Web-based configuration wizard
- Role-based Access control
- 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)
- NTP Support

User Authentication
- Internal database
- Active Directory Integration
- Automatic Windows Single Sign On
- External LDAP/RADIUS database Integration
- Thin Client support - Microsoft Windows Server 2003 Terminal Services and Citrix XenApp
- RSA SecurID support
- External Authentication - Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

Logging and Monitoring
- Graphical real-time and historical Monitoring
- Email notification of reports, viruses and attacks
- Syslog support
- Log Viewer - IPS, Web filter, WAF, Anti-Virus, Anti-Spam, Authentication, System and Admin Events

On-Appliance Cyberoam - iView Reporting
- Integrated Web-based Reporting tool - Cyberoam-iView
- 1,200+ drilldown reports
- 45+ Compliance reports
- Historical and Real-time reports
- Multiple Dashboards
- Username, Host, Email ID specific Monitoring Dashboard
- Reports - Security, Spam, Virus, Traffic, VPN, Search Engine keywords
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Automated Report Scheduling

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

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
- 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
- Inbuilt Web Category Database
- URL, keyword, File type block
- Web Categories: Default(89+), Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Category-based Bandwidth allocation and prioritization
- Block Java Applets, Cookies, Active X
- CIPA Compliant
- Data leakage control via HTTP, HTTPS upload
- Schedule-based access control
- Custom block messages per category

Bandwidth Management
- Application and User Identity based Bandwidth Management
- Category-based Bandwidth restriction
- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery
- Multi WAN bandwidth reporting

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 200 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, POP3, IMAP, IM, VPN Tunnels
- Customize individual user scanning
- Self Service Quarantine area
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

Gateway Anti-Spam
- Inbound Scanning
- Outbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- Image-spam filtering 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
- Automated Failover/Failback, Multi-WAN
- WRR based Load balancing
- Policy routing based on Application and User
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding

High Availability
- Active-Active
- Active-Passive with state synchronization
- Stateful Failover
- Alerts on Appliance Status change

IPSec VPN Client*
- Inter-operability with major IPSec VPN Gateways
- Supported platforms: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit, Windows 8 RC1 32/64-bit
- Import Connection configuration

Certification
- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo

*Additional Purchase Required

Specifications	500iNG-XP	750iNG-XP	1000iNG-XP	1500iNG-XP	2500iNG-XP
Interfaces					
Copper GbE Ports (Fixed)	8	8	10	10	10
FleXi Ports Module* (for XP Appliances) (1 GbE Copper / 1 GbE SFP / 10 GbE SFP)	8 / 8 / 4	8 / 8 / 4	8 / 8 / 4	8 / 8 / 4	8 / 8 / 4
Console Ports (RJ45)	1	1	1	1	1
USB Ports	2	2	2	2	2
Hardware Bypass Segments**	2	2	-	-	-
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes	Yes
System Performance*					
Firewall Throughput (UDP) (Mbps)	18,000	22,000	27,500	32,000	60,000
Firewall Throughput (TCP) (Mbps)	16,000	18,000	22,500	26,000	36,000
New sessions/second	100,000	140,000	240,000	265,000	300,000
Concurrent sessions	2,500,000	3,000,000	5,500,000	7,500,000	10,000,000
IPSec VPN Throughput (Mbps)	1,500	2,250	3,000	4,500	9,000
No. of IPSec Tunnels	1,000	1,500	3,000	4,000	5,000
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)	3,500	4,000	4,500	5,000	6,500
IPS Throughput (Mbps)	4,500	6,500	10,500	12,500	16,000
NGFW Throughput (Mbps)****	3,250	3,600	5,000	6,000	8,000
Fully Protected Throughput*****	1,650	1,800	3,000	3,600	5,500
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

گروه شرکت های کارنما
تهران، خیابان ولی عصر، بالاتر از سه راه عباس آباد، کوچه زرین، شماره ۱۳، طبقه دوم
www.karnama.com • info@karnama.com • فکس: ۸۸۵۵۴۳۸۷ • تلفن: ۴۲۷۰۸

Cyberoam
Unified Threat Management

NG Future-ready

امنیت آینده ی شبکه های SME و SOHO/ROBO

NG Series UTM Appliances

NG Series : 15iNG, 25iNG/6P, 35iNG, 50iNG, 100iNG, 200iNG/XP, 300iNG/XP

NG Wireless Series : 15wiNG, 25wiNG, 25wiNG-6P, 35wiNG

با فراگیر شدن اینترنت پرسرعت در شرکت ها و افزایش تعداد دستگاه های الکترونیکی هر کاربر که قابلیت اتصال به اینترنت را دارند، استفاده از اطلاعات رشد چشمگیری داشته و هر روز بر آن اضافه می گردد. از این رو ضمن برطرف ساختن نیاز کاربران، امنیت آن ها و شبکه را نیز باید تامین کرد.

سری NG سایبروم با ارائه سرعت وکارآیی بی نظیر، دارای سخت افزاری با بهترین کیفیت و نرم افزاری جامع و هماهنگ است. همچنین در مقیاس شبکه های SOHO و SME، جزو سریعترین UTMهای تولید شده برای این شبکه ها می باشد.

سری NG سایبروم امنیت، ارتباط و کارایی کسب و کار شما را تضمین کرده و با تکنولوژی لایه ۸ (استفاده از شناسه کاربری) امنیت شبکه شما را تامین و کنترل می کند. همچنین معماری امنیتی آن به گونه ای می باشد که قابلیت توسعه و تغییر را داشته و با توجه به امکانات روز و تکنولوژی های نوظهور، سریعا قابل تغییر بوده و قابلیت ارتقا را نیز دارد.

Feature Specifications

Stateful Inspection Firewall
- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Access Control Criteria (ACC) : User-Identity, Source and Destination Zone, MAC and IP address, Service
- UTM policies - IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and Bandwidth Management
- Application (Layer 7) Control and Visibility
- Access Scheduling
- Policy based Source and Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS and DDoS attack prevention
- MAC and IP-MAC filtering and Spoof prevention

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
- Block by file types
- Add disclaimer/signature

Gateway Anti-Spam
- Inbound Scanning
- Outbound Scanning*
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- Image-spam filtering using RPD Technology
- Zero hour Virus Outbreak Protection
- Self Service Quarantine area[1]
- IP address Black list/White list
- Spam Notification through Digest[2]
- IP Reputation-based Spam filtering

Intrusion Prevention System
- Signatures: Default (4500+), Custom
- IPS Policies: Multiple, Custom
- User-based policy creation
- Automatic real-time updates from CRProtect networks
- Protocol Anomaly Detection
- DDoS attack prevention
- SCADA-aware IPS with pre-defined category for ICS and SCADA signatures

Web Filtering
- Inbuilt Web Category Database
- URL, keyword, File type block
- Web Categories: Default(89+), Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Category-based Bandwidth allocation and prioritization
- Block Java Applets, Cookies, Active X
- CIPA Compliant
- Data leakage control via HTTP, HTTPS upload
- Schedule-based access control
- Custom block messages per category

Application Filtering
- Inbuilt Application Category Database
- 2,000+ Applications Supported
- Schedule-based access control
- Block
  - Proxy and Tunnel
  - File Transfer
  - Social Networking
  - Streaming Media
- Layer 7 (Applications) & Layer 8 (User - Identity) Visibility
- 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[3]
- 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 200 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

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
- 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

Instant Messaging (IM) Management
- Yahoo and Windows Live Messenger
- Virus Scanning for IM traffic
- Allow/Block: Login, File Transfer, Webcam, One-to-one/group Chat
- Content-based blocking
- IM activities Log
- Archive files transferred
- Custom Alerts

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

Bandwidth Management
- Application and User Identity based Bandwidth Management
- Category-based Bandwidth restriction
- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery[4]
- Multi WAN bandwidth reporting

User Identity-based and Group-based Controls
- Access time restriction
- Time and Data Quota restriction, P2P and IM Controls
- Schedule-based Committed and Burstable Bandwidth

Networking
- Automated Failover/Failback, Multi-WAN
- WRR based Load balancing
- Policy routing based on Application and User
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay
- Supports HTTP Proxy, Parent Proxy with FQDN
- Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding

High Availability*
- Active-Active
- Active-Passive with state synchronization
- Stateful Failover
- Alerts on Appliance Status change

Administration and System Management
- Web-based configuration wizard
- Role-based Access control
- 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, Korean
- Cyberoam Central Console (Optional)
- NTP Support

User Authentication
- Internal database
- Active Directory Integration
- Automatic Windows Single Sign On
- External LDAP/RADIUS database Integration
- Thin Client support - Microsoft Windows Server 2003 Terminal Services and Citrix XenApp
- RSA SecurID support
- External Authentication - Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

Logging and Monitoring
- Graphical real-time and historical Monitoring
- Email notification of reports, viruses and attacks
- Syslog support
- Log Viewer - IPS, Web filter, WAF, Anti-Virus, Anti-Spam, Authentication, System and Admin Events

On-Appliance Cyberoam - iView Reporting[5]
- Integrated Web-based Reporting tool - Cyberoam-iView
- 1,200+ drilldown reports
- 45+ Compliance reports
- Historical and Real-time reports
- Multiple Dashboards
- Username, Host, Email ID specific Monitoring Dashboard
- Reports - Security, Spam, Virus, Traffic, Policy violations, VPN, Search Engine keywords
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Automated Report Scheduling

IPSec VPN Client[6]
- Inter-operability with major IPSec VPN Gateways
- Supported platforms: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit, Windows 8 RC1 32/64-bit
- Import Connection configuration

Certification
- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark UTM Level 5 Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo

*Available in all the Models except CR15iNG & CR15wiNG
[1]Additional Purchase Required
[2]Not supported in CR15iNG & WiFi series of appliances

Specifications	15iNG	25iNG/6P	35iNG	15wiNG	25wiNG/6P	35wiNG
Interfaces						
Copper GbE Ports	3	4/6	6	3	4/6	6
Console Ports (RJ45)	1	1	1	1	1	1
USB Ports	2	2	2	2	2	2
Hardware Bypass Segments*	-	-	-	-	-	-
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes	Yes	Yes
System Performance**						
Firewall Throughput (UDP) (Mbps)	1,000	1,500	2,300	1,000	1,500	2,300
Firewall Throughput (TCP) (Mbps)	750	1,000	2,000	750	1,000	2,000
New sessions/second	3,500	5,000	12,000	3,500	5,000	12,000
Concurrent sessions	60,000	150,000	350,000	60,000	150,000	350,000
IPSec VPN Throughput (Mbps)	110	210	250	110	210	250
No. of IPSec Tunnels	50	100	150	50	100	150
SSL VPN Throughput (Mbps)	50	75	100	50	75	100
WAF Protected Throughput (Mbps)	-NA-	100	150	-NA-	100	150
Anti-Virus Throughput (Mbps)	180	300	525	180	300	525
IPS Throughput (Mbps)	140	200	350	140	200	350
UTM Throughput (Mbps)	80	110	210	80	110	210
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Built-in Wireless LAN (Only for wiNG series)						
Wireless Standards	NA			IEEE 802.11 a/b/g/n (WEP, WPA, WPA2, 802.11i , TKIP, AES, PSK)		
Antenna				Detachable 3x3 MIMO		
Access Points				Up to 8 bssid		
Transmit Power (EIRP)				11n HT40 : –15dBm, 11b CCK: +15dBm, 11g OFDM:+15dBm		
Receiver Sensitivity				-68dBm at 300Mbps, -70dBm at 54Mbps, -88dBm at 6Mbps		
Frequency Range				2.412 GHz - 2.472 GHz		
				5.200 GHz - 5.825 GHz		
Number of Selectable Channels				USA (FCC) - 11 channels, EU (ETSI) / Japan (TELEC) - 13 channels		
Data Rate				802.11n: up to 450Mbps, 802.11b: 1, 2, 5,5, 11Mbps, 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps		
Dimensions						
H x W x D (inches)	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1
H x W x D (cms)	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2
Appliance Weight	1.5 kg, 3.307 lbs	2.3 kg, 5.07 lbs	2.3 kg, 5.07 lbs	1.5 kg, 3.307 lbs	2.3 kg, 5.07 lbs	2.3 kg, 5.07 lbs
Power						
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Consumption	13.2W	33.5W	47.8W	13.2W	33.5W	47.8W
Total Heat Dissipation (BTU)	45	114	163	45	114	163

Specifications	50iNG	100iNG	200iNG/XP	300iNG/XP
Interfaces				
Copper GbE Ports	8	8	10 / 6	10 / 6
FleXi Ports Module*** (for XP Appliances) (1 GbE Copper / 1 GbE SFP / 10 GbE SFP)	-	-	8 / 8 / 4	8 / 8 / 4
Console Ports (RJ45)	1	1	1	1
USB Ports	2	2	2	2
Hardware Bypass Segments*	2	2	2	2
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes
System Performance**				
Firewall Throughput (UDP) (Mbps)	3,250	4,500	10,000	12,000
Firewall Throughput (TCP) (Mbps)	3,000	3,500	8,000	9,500
New sessions/second	30,000	45,000	70,000	85,000
Concurrent sessions	1,000,000	1,250,000	1,500,000	2,000,000
IPSec VPN Throughput (Mbps)	400	450	800	1,200
No. of IPSec Tunnels	200	250	300	400
SSL VPN Throughput (Mbps)	300	400	450	500
WAF Protected Throughput (Mbps)	450	700	1,000	1,250
Anti-Virus Throughput (Mbps)	1,000	1,400	2,200	2,600
IPS Throughput (Mbps)	750	1,200	2,000	2,400
UTM Throughput (Mbps)	550	750	1,200	1,500
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited
Dimensions				
H x W x D (inches)	1.7 x 14.6 x 17.3	1.7 x 14.6 x 17.3	1.7 x 17.3 x 11.85	1.7 x 17.3 x 11.85
H x W x D (cms)	4.4 X 37.2 X 44	4.4 X 37.2 X 44	4.4 x 43.9 x 30.1	4.4 x 43.9 x 30.1
Appliance Weight	5 kg, 11.02 lbs	5 kg, 11.02 lbs	5.1 kg, 11.24 lbs	5.1 kg, 11.24 lbs
Power				
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Consumption	99W	99W	137W	137W
Total Heat Dissipation (BTU)	338	338	467	467

Web Application Firewall Subscription on Cyberoam UTM appliances

Protecting Web Applications from hackers

Cyberoam
Unified Threat Management

فایروال برنامه های تحت وب

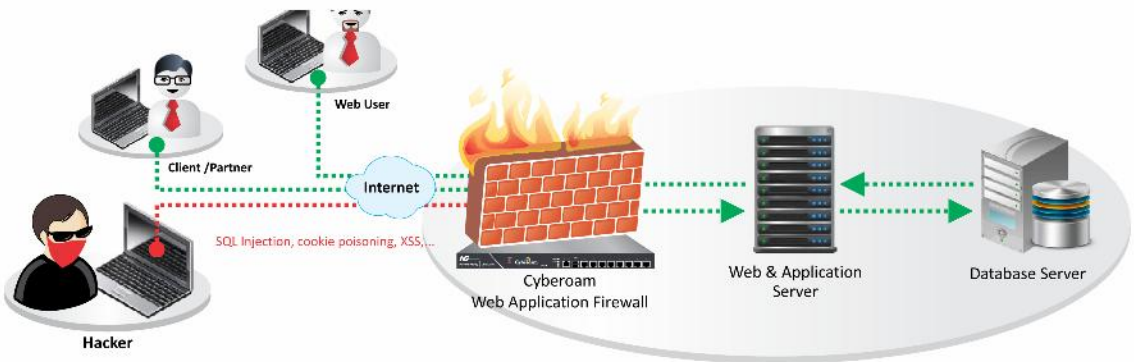
با وجود برنامه های اداری حیاتی نظیر CRM ، ERP ، نرم افزارهای اتوماسیون اداری ، نرم افزارهای بانکی و ... که تحت وب می باشند و همچنین رشد روز افزون برنامه های تحت وب ، هکرها نیز اهداف خود را به طور ویژه ای بر روی حفره ها و آسیب پذیری های موجود روی این نرم افزارها متمرکز کرده اند. بنابراین نیاز به فایروالی که بتواند اینگونه حملات را کنترل و دفع کند ضروری به نظر می رسد.

سایبروم در این زمینه برنامه کامل و جامعی به عنوان فایروال برنامه های تحت وب (Web Application Firewall) را برای شبکه های فیزیکی و مجازی ارائه می دهد . این فایروال به صورت یک ماژول اشتراکی بر روی محصولات سایبروم موجود بوده وکاربر در صورت نیاز آن را فعال و حق اشتراک آن را می پردازد.

از جمله قابلیت های این نرم افزار می توان به حفاظت وب سایت ها و برنامه های تحت وب در برابر حملاتی مانند Cross-site ، SQL Injection Scripting (XSS) ، URL Parameter Tampering و ... و همچنین محافظت در برابر حفره های کشف شده موجود در سایت OWASP Top 10 می باشد .

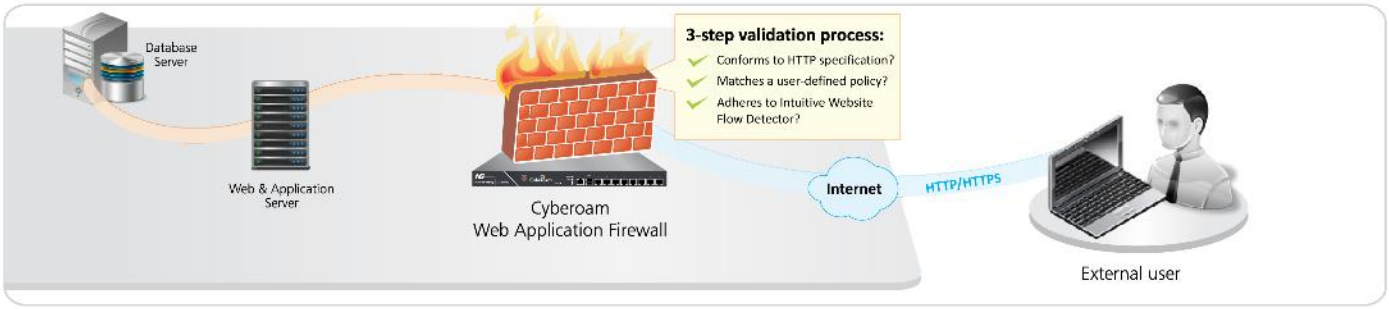
WAF با تفکیک ترافیک ورودی و خروجی سرور باعث ایجاد یک لایه حفاظتی اضافه شده و توسط آن ، قبل از اینکه حملات متوجه سرور شود از آن جلوگیری می کند . همچنین به طور خودکار رفتارها و ترافیک برنامه ها را بررسی و سلامت آن را تایید و سرور را در برابر رفتارهای مشکوک و خطرناک محافظت می کند

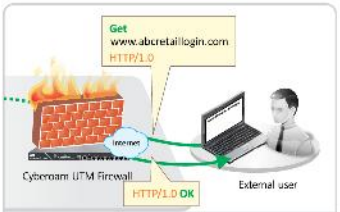
از دیگر ویژگی های WAF می توان به دفع حملات از رنج وسیعی از نرم افزارهای تجاری و متن باز مانند Nessus ، WebInsp و ... که به منظور کشف حفره های موجود در سیستم استفاده می شوند ، اشاره کرد.



Cyberoam Web Application Firewall Protection against Web-based Application Attacks

How Cyberoam Web Application Firewall Works?

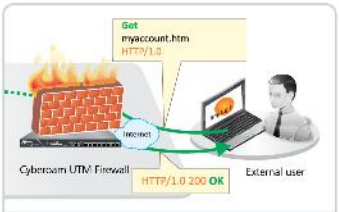




1 HTTP Protocol Specification

Supports HTTP protocol specification versions 1.0/1.1

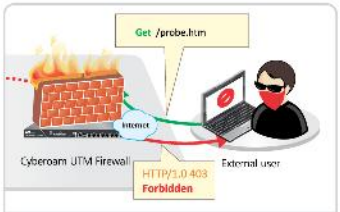
```
<html>
  <head>
    <title>Home Page</title>
  </head>
  <body>
    <a href="myaccount.htm">Page 2</a>
    <img src="images/img1.gif" />
  </body>
</html>
```



2 Intuitive Website Flow Detector

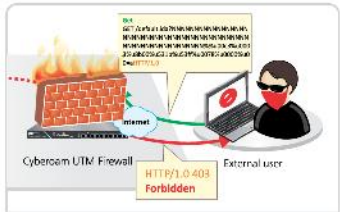
Request is legitimate and adheres to the Intuitive Website Flow Detector's "self-learning" in the past, when such a request was last made to the Web server.

```
<html>
  <head>
    <title>Page 2 </title>
  </head>
  <body>
    <a href="myservices.htm">Page 3</a>
    <img src="images/img2.gif"/>
  </body>
</html>
```



3 User-defined policies

The server request was not found valid under the Intuitive Website Flow Detector's knowledge from the past – the requested URL cannot be the entry point and it is, hence, blocked from reaching the Web server and the browser receives an HTTP 403 Forbidden response code. No other information is exposed as decided under the User Defined Policy.



Code Red Attack (or any variant)

The request doesn't pass any of the 3 validation steps. Web server is thus protected from present/future URL-based HTTP attacks.

مدل حفاظتی Positive بدون استفاده از جدول Signature

سایبروم با زیر نظر گرفتن گردش کار وب سایت ، به طور خودکار حملات را شناسایی و برطرف می کند. این کار بدون استفاده از هیچ گونه جدول Signature یا سیستم تشخیص الگوی مخرب انجام می شود که اصطلاحاً مدل حفاظتی Positive خوانده می شود.

حفاظت کامل Business Logic

WAF از حملاتی از قبیل SQL injection , cross-site scripting (XSS) و cookie-poisoning که به دنبال بهره برداری از Business Logic برنامه های وب هستند ، جلوگیری می کنند.

SSL Offloading

با توجه به تدابیر امنیتی در ارتباطات HTTPS -SSL که معمولاً در سازمان ها و شرکت هایی که اطلاعات حساس تبادل می کنند کاربرد دارد ، هکرها نمی توانند خطری را متوجه سیستم کنند. WAF نه تنها امنیت ارتباطات را تامین می کند ، بلکه تاخیرترافیک های SSL را نیز کم می کند.

ایمن سازی وب سرور در لحظه

WAF محیط های تحت وب مانند Web Sphere , Apache , IIS و ... که اشتباه پیکربندی شده اند و همچنین حفره های موجود در نرم افزارهای 3rd-party را محافظت می کند.

پراکسی معکوس برای ترافیک ورودی HTTP/HTTPS

WAF برای ترافیک ورودی به صورت پراکسی عمل می کند به این صورت که ابتدا ترافیک درخواستی کاربران وب را دریافت کرده و سپس تحویل سرور می دهد . به این ترتیب کاربران هیچ گاه دسترسی مستقیم به سرور نخواهند داشت و مشخصات سرور برای کاربران مخفی خواهد ماند.

ایمن سازی URL ها ، فرم ها و کوکی ها

WAF از URLها ، فرم های HTML و کوکی ها در برابر حملات و تغییرات ناخواسته محافظت می کند . WAF به صورت خودکار درخواست هایی که تلاش می کنند با دستکاری URLها و کوکی های قلابی به account کاربر دست یابند را شناسایی و مسدود می کند.

نظارت و گزارش گیری

WAF با دادن اطلاعاتی از قبیل نوع حملات ، منبع حملات و اعمال صورت گرفته حین حمله و ایجاد هشدار در هنگام حملات شرکت ها را در تطبیق با نیازهای PCI DSS یاری می کند.

سایر ویژگی ها :

- مسدود و یا ایجاد هشدار برای IP های خاص
- ایجاد پیام های دلخواه برای IP های Block شده
- ایجاد تدابیر حفاظتی بر اساس نرخ اتصال

گروه شرکت های کارنما

تهران ، خیابان ولی عصر ، بالاتر از سه راه عباس آباد ، کوچه زرین ، شماره ۱۳ ، طبقه دوم

تلفن: ۴۲۷۰۸ • فکس: ۸۸۵۵۴۳۸۷ • info@karnama.com • www.karnama.com