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