Cyberoam®

NG Future-ready

Firewalls der nächsten Generation für große Unternehmensnetzwerke

Technische Daten

Mobile Mitarbeiter, mehr und mehr externe Benutzer wie Kunden und Partner sowie Trends wie der Anstieg der Netzwerkbenutzer und -geräte, immer mehr Anwendungen, Virtualisierung uvm. führen dazu, dass Unternehmen in ihrem Netzwerk die Kontrolle bezüglich der Sicherheit verlieren.

Cyberoam Next-Generation Firewalls (NGFW) mit der auf Layer 8 identitätsbasierten Technologie bietet eine intelligente und funktionsreiche Lösung für Unternehmen. NGFW bietet umfassende Sicherheitskontrolle von L2-L8 für Sicherheit, die auch zukunftssicher ist. Der menschliche Layer 8 von Cyberoam funktioniert wie ein abstrakter Standardlayer, der die echten Layer 2-7 verbindet, damit Unternehmen wieder die verloren gegangene Sicherheitskontrolle in die Hand nehmen können.

Cyberoam NGFW bietet inline-Anwendungsanalyse und -kontrolle, Website-Filter, HTTPS-Analyse, Intrusion Prevention System, VPN (IPSec und SSL) und granulare Steuerung der Bandbreite. Weitere Funktionen wie WAF, Flexible Ports, Gateway Anti-Virus und Anti-Spam sind auch verfügbar.

Cyberoam Sicherheitsgeräte bieten hohe Performance, hohe Sicherheit, Konnektivität und Produktivität sowie eine Extensible Security Architecture (ESA) für zukunftssichere Sicherheit in Unternehmen.

NGFW-Geräte der NG Serie: : 500iNG-XP, 750iNG-XP, 2500iNG

Spezifikation der Features

Stateful Inspection Firewall
- Layer 8 (Benutzeridentität) Firewall
- Mehrere Sicherheitszonen
- Access Control Criteria (ACC): Benutzeridentität, Quell- und Zielzone, MAC- und IP-Adresse, Service
- Sicherheitsrichtlinien - IPS, Web Filtering, Application Filtering, Anti-Virus, Anti-Spam und Bandwidth Management
- Anwendung (Layer 7) Kontrolle & Transparenz
- Zeitplanung für den Zugriff
- Zugriffsbasiertes Quell- und Ziel-NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- Verhinderung von DoS & DDoS Angriffen
- MAC und IP-MAC-Filter und Spoof-Anwendung

Application Filtering
- Integrierte Datenbank mit Anwendungskategorien
- Unterstützt 2.000+ Anwendungen
- Auf Zeitplänen basierende Zugriffssteuerung
- Sperren
  - P2P-Anwendungen wie Skype
  - Anonyme Proxies wie Ultra surf
  - "Phone home" Aktivitäten
  - Keylogger
- Layer 7 (Anwendung) & Layer 8 (Benutzeridentität) Transparenz

Intrusion Prevention System (IPS)
- Signaturen Standard (4500+), Benutzerdefiniert
- IPS-Richtlinien: Mehrere, Benutzerdefiniert
- Erstellen benutzerbasierter Richtlinien
- Automatische Updates in Echtzeit von CRProtect Netzwerken
- Protocol Anomaly Detection (PAD)
- Verhinderung von DDoS Angriffen

Auf Benutzeridentität und auf Gruppen basierende Kontrollmechanismen
- Einschränkung der Zugriffszeit
- Einschränkung nach Zeit- und Datenkontingent, P2P- und IM-Kontrollen
- Zeitplanbasierte gebundene Bandbreite und Bandbreite nach Bedarf

Administration und Systemmanagement
- Webbasierter Konfigurationsassistent
- Auf Rollen basierende Zugriffssteuerung
- Firmware Upgrades über Web UI
- Web 2.0-fähige UI (HTTPS)
- Farbauswahl für Benutzeroberfläche
- Befehlszeilenschnittstelle (Seriell, SSH, Telnet)
- SNMP (v1, v2, v3)
- Unterstützung mehrerer Sprachen: Englisch, Chinesisch, Hindi, Französisch, Koreanisch
- Cyberoam Central Console (Optional)
- NTP Support

Benutzerauthentifizierung
- Interne Datenbank
- Active Directory Integration
- Automatisches einmaliges Anmelden unter Windows
- Externe LDAP/RADIUS Datenbankintegration
- Thin Client Support - Microsoft Windows Server 2003 Terminal Services und Citrix XenApp
- RSA SecurID Support
- Externe Authentifizierung – Benutzer und Administratoren
- Benutzer/MAC-Bindung
- Mehrere Authentifizierungsserver

Protokollierung und Überwachung
- Grafische Echtzeitüberwachung und Verlaufsüberwachung
- E-Mail-Benachrichtigung: Berichte, Viren und Angriffe
- Syslog Support
- Log Viewer - IPS, Web Filter, WAF, Anti-Virus, Anti-Spam, Authentifizierung, System- und Admin-Events

On-Appliance Cyberoam - iView Reporting
- Integriertes webbasiertes Berichterstattungstool - Cyberoam-iView
- Über 1.200 Detailberichte
- über 45 Compliance-Berichte
- Verlaufs- und Echtzeitberichte
- Mehrere Dashboards
- Spezielles Überwachungs-Dashboard für Benutzername, Host und E-Mail-ID
- Berichte - Sicherheit, Spam, Virus, Traffic, Richtlinienverstöße, VPN, Schlüsselwörter für Suchmaschinen
- Mehrformatige Berichte - tabellarisch, grafisch
- Exportfähige Formate - PDF, Excel
- Automatische Berichtsplanung

Virtuelles Privates Netzwerk (VPN)
- IPSec, L2TP, PPTP
- Verschlüsselung - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash-Algorithmen - MD5, SHA-1
- Authentifizierung: Preshared Key (PSK), digitale Zertifikate
- IPSec NAT Traversal
- Unterstützung für Dead Peer Detection (DPD) und PFS
- Diffie Hellman Gruppen - 1,2,5,14,15,16
- Unterstützung externer Zertifizierungsstellen
- Exportieren von Verbindungskonfigurationen mobiler Benutzer
- Unterstützung von Domänennamen für Tunnelendpunkte
- Redundanz für VPN-Verbindungen
- Überdeckende Netzwerkunterstützung
- Hub & Spoke VPN-Unterstützung

SSL VPN
- TCP & UDP Tunneling
- Authentifizierung - Active Directory, LDAP, RADIUS, Cyberoam (Lokal)
- Mehrschichtige Client-Authentifizierung - Zertifikat, Benutzername/Kennwort
- Durchsetzen von Benutzer- und Gruppenrichtlinien
- Netzwerkzugriff – Split- und Full-Tunneling
- Browserbasierter (Portal) Zugriff - Clientloser Zugriff
- Lightweight SSL VPN Tunneling Client
- Granulare Zugriffssteuerung auf alle Enterprise Netzwerkressourcen
- Administrative Kontrollen – Sitzungszeitüberschreitung, DPD (Dead Peer Detection), Portalanpassung
- TCP-basierter Anwendungszugriff - HTTP, HTTPS, RDP, TELNET, SSH

Web Filtering
- Integrierte Datenbank mit Web-Kategorien
- Sperre für URLs, Schlagwörter, Dateitypen
- Web-Kategorien: Standard (89+), Benutzerdefiniert
- Unterstützte Protokolle: HTTP, HTTPS
- Sperrt Malware-, Phishing- und Pharming-URLs
- Auf Kategorien basierte Bandbreitenzuweisung und Zuweisung von Prioritäten
- Sperrt Java Applets, Cookies und Active X
- CIPA konform
- Kontrolle bei Datenverlusten über HTTP, HTTPS Upload
- Auf Zeitplänen basierende Zugriffssteuerung
- Benutzerdefiniertes Sperren von Nachrichten nach Kategorie

Verwalten der Bandbreite
- Bandbreitenmanagement basierend auf Anwendungen und Benutzeridentität
- Bandbreiteneinschränkung basierend auf Kategorien
- Richtlinien für garantierte Bandbreite und Bandbreite nach Bedarf
- Anwendungs- & benutzeridentitätsbasierte Traffic Discovery
- Multi WAN-Bandbreitenberichte

Web Application Firewall
- Positives Schutzmodell
- Einmalige Technologie „Intuitive Website Flow Detector"
- Schutz gegen: SQL Injections, Cross-Site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning usw.
- Unterstützung für HTTP 0.9/1.0/1.1
- Unterstützt Back-End-Server: 5 bis 200 Server

Gateway Anti-Virus & Anti-Spyware
- Erkennt und entfernt Viren, Würmer und Trojaner
- Schützt vor Spyware, Malware und Phishing
- Automatische Aktualisierung der Datenbank mit Virensignaturen
- Scannt HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IM, VPN Tunnel
- Anpassbares Scannen einzelner Benutzer
- Self-Service Quarantine Area (selbstverwaltender Quarantänebereich)
- Scannt und sendet nach Dateigröße
- Sperrt anhand der Dateitypen
- Disclaimer/Signatur hinzufügen

Gateway Anti-Spam
- Scannen beim Senden
- Scannen beim Empfangen
- Real-Time Blacklist (RBL), MIME Header Prüfung
- Filter basierend auf Header, Größe, Sender und Empfänger der Nachrichten
- Kennzeichnen der Themazeile
- Weiterleiten von Spam-E-Mails an eine dedizierte E-Mail-Adresse
- Filter für Image-Spam mit RPD-Technologie
- Zero Hour Virus Outbreak Schutz
- Self-Service Quarantine Area (selbstverwaltender Quarantänebereich)
- Schwarze und Weiße Listen für IP-Adressen
- Spam-Benachrichtigung als Zusammenfassung
- IP Reputation-Based Spam-Filter

Drahtloses WAN
- USB-Port 3G/4G und WiMax Unterstützung
- Primärer WAN-Link
- WAN Backup-Link

Networking
- Automated Failover/Failback, Multi-WAN
- WRR-basierter Lastausgleich
- Richtlinien-Routing nach Anwendung und Benutzer
- Zuweisung der IP-Adresse - Statisch, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP Server, DHCP Relay
- Unterstützt HTTP Proxy, Parent Proxy mit FQDN
- Dynamisches Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding

Hohe Verfügbarkeit
- Active-Active
- Active-Passive mit Statussynchronisierung
- Stateful Failover
- Warnhinweise bei Statusänderungen des Geräts

IPSec VPN Client#
- Interoperabilität mit großen IPSec VPN Gateways
- Unterstützte Plattformen: 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
- Verbindungskonfiguration importieren

Zertifizierung
- Common Criteria - EAL4+
- ICSA Firewall - Corporate
- Checkmark-Zertifizierung
- VPNC - Basic und AES Interoperabilität
- IPv6 Ready Gold Logo

#Zusatzkauf erforderlich

Spezifikation	500iNG-XP	750iNG-XP	2500iNG
Schnittstellen			
Kupfer GbE Ports	8	8	14
1/10 GbE SFP (Mini GBIC) Ports	-	-	4/2
FleXi Ports Module* (für XP-Geräte) (1 GbE Kupfer / 1 GbE SFP / 10 GbE SFP)	8 / 8 / 4	8 / 8 / 4	-
Consolen Ports (RJ45)	1	1	1
USB Ports	2	2	2
Hardware Bypass-Segmente**	2	2	2
Konfigurierbare interne/DMZ/WAN Ports	Ja	Ja	Ja
System Performance*			
Firewall-Durchsatz (UDP) (Mbit/s)	18,000	22,000	40,000
Firewall-Durchsatz (TCP) (Mbit/s)	16,000	18,000	28,000
Neue Sitzungen/Sekunde	100,000	140,000	200,000
Gleichzeitige Sitzungen	2,500,000	3,000,000	3,500,000
IPSec VPN Durchsatz (Mbit/s)	1,500	2,250	8,000
Anz. An IPSec Tunnel	1,000	1,500	4,500
SSL VPN Durchsatz (Mbit/s)	650	750	1,000
WAF-geschützter Durchsatz (Mbit/s)	900	950	1,000
Antivirus-Durchsatz (Mbit/s)	3,500	4,000	6,000
IPS-Durchsatz (Mbit/s)	4,500	6,500	8,000
NGFW-Durchsatz (Mbit/s)****	3,250	3,600	5,500
Authentifizierte Benutzer / Knoten	unbegrenzt	unbegrenzt	unbegrenzt
Abmessungen			
H x W x D (Inch)	1.7 x 17.44 x 18.75	1.7 x 17.44 x 18.75	3.54 x 17.52 x 23.23
H x W x D (cm)	4.4 X 44.3 X 47.62	4.4 X 44.3 X 47.62	9 x 44.5 x 59
Gerätegewicht	5.1 kg, 11.24 lbs	5.1 kg, 11.24 lbs	19 kg, 41.8 lbs
Stromversorgung			
eingangsspannung	100-240 VAC	100-240 VAC	90-260 VAC
Verbrauch	208 W	208 W	258 W
Wärmeabfuhr gesamt (BTU)	345	345	881
Redundante Stromversorgung	-	Ja	Ja

Umgebungsbedingungen: Betriebstemperatur 0 °C bis 40 °C, Lagertemperatur -25 °C bis 75 °C, Relative Luftfeuchtigkeit (nicht kondensierend)) 10% bis 90%
*Zusatzkauf erforderlich **Bei Aktivierung wird der Traffic nur bei Stromausfall umgangen.
***Die Antivirus- und IPS-Performance wurde anhand von RFC 3511 Richtlinien basierend auf HTTP-Traffic gemessen. Die tatsächliche Performance kann abhängig von der vorliegenden Umgebung (Datenverkehr im Netzwerk) abweichen. ****NGFW-Durchsatz wurde mit aktivierten Modulen für Firewall, IPS und Web & Application Filtering gemessen.

Kostenlose Telefonnummern
USA : +1-800-686-2360 | **Indien :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europa :** +44-808-120-3958

Cyberoam®