

Cyberoam UTM

Die Cyberoam CR-Reihe beruht auf eingebauten, identitätsbasierten Sicherheitsvorrichtungen, die einen Echtzeitschutz gegen diverse Gefährdungen durch ihre einzigartigen benutzerorientierten Strategien bieten. Die Cyberoam Anwendungen stellen Enterprise-Class Stateful Inspection Firewall, VPN, Gateway Anti-Virus und Anti-Spyware, Gateway Anti-Spam, Erkennen und Vorbeugen von Eindringlingen, Inhaltsfilter, Bandbreitenmanagement, multiples Linkmanagement und eine umfassende Berichterstattung zur Verfügung. Diese Funktionen werden über eine einzige Plattform, die Cyberoam Central Console, zentral verwaltet. Das Merkmal der hohen Verfügbarkeit gewährleistet Schutz bei Hardware-Versagen, wodurch ein möglichst langer und ununterbrochener Netzzugang gesichert werden kann. Cyberoam schützt Unternehmen, Bildungsinstitutionen und staatliche Einrichtungen vor internen und externen Gefahren, u.a. vor Spyware, Phishing, Pharming, Viren, Würmer, Trojaner und DoS Angriffen (Angriffe durch Dienstverweigerung).



Séries Cr : 25i, 50i, 100i, 250i, 500i, 1000i, 1500i

Identitätsbasierte Sicherheit durch UTM

Cyberoam verwendet die Identität des Benutzers als Hauptkriterium der Sicherheit. Dadurch wird den Unternehmen an Stelle einer an eine feste IP-Adresse gebundene Sicherheit, eine innovative Verfahrensweise geboten. Die identitätsbasierte Sicherheit garantiert eine vollständige Geschäftsflexibilität, indem in jeglicher Umgebung - u.a. DHCP und Wi-Fi - durch das Erkennen der einzelnen Benutzer innerhalb des Netzwerks ein vollkommener Schutz gewährleistet ist. Die Benutzererkennung bezieht sich hierbei sowohl auf das Aufspüren von Gefahrenquellen als auch auf deren Opfer.

Funktionen	Beschreibung	Stärken
Stateful Inspection Firewall (ICSA Labs zertifiziert)	<ul style="list-style-type: none"> Effiziente Inspektion von Paketen (dynamisch und vertieft) Verhindert DoS und flooding Angriffe aus internen und externen Quellen Identitätsbasierte Zugriffskontrolle für die Anwendungen P2P und IM 	<ul style="list-style-type: none"> Schutz der Anwendungsschicht Flexibilität, Strategien durch die Benutzeridentität zu bestimmen Hohe Skalierbarkeit
Virtual Private Network (VPN)	<ul style="list-style-type: none"> Industriestandard: IPSec, L2TP, PPTP VPN Hohe Verfügbarkeit des VPN für IPSec und L2TP Verbindungen 	<ul style="list-style-type: none"> Geschützte Verbindungen für Filialen und Fernbenutzer Fernanschlussmöglichkeit über das Internet zu niedrigem Preis Effiziente Ausfallsicherung mit Prioritäten von vorbestimmten
Gateway Anti-Virus & Anti-Spyware	<ul style="list-style-type: none"> Scan von HTTP, FTP, IMAP, POP3 und SMTP traffic Erkennt und entfernt Viren, Würmer und Trojaner Zugriff auf in Quarantäne verschobene Mails für Administratoren Einschränkung des Datenverkehrs durch Passwörter Unmittelbare Benutzererkennung im Fall von HTTP-Gefährdungen 	<ul style="list-style-type: none"> Umfassender Schutz des Verkehrs über sämtliche Protokolle Hohe Geschäftsflexibilität Schutz von vertraulichen Daten Echtzeitschutz
Gateway Anti-Spam	<ul style="list-style-type: none"> Scannt SMTP, POP3 und IMAP traffic nach Spam Erkennt, bennet und schiebt Spam Mails in Quarantäne Milde oder strenge Regeln je nach Bedarf Verstärkt Schwarzweißlisten Schutz vor dem Eindringen von Viren Schutz vor Spam unabhängig ihres Inhalts und Image-Spam durch Verwendung von RPD-Technologie (Erkennen von wiederkehrenden Mustern) 	<ul style="list-style-type: none"> Erweitert die Leistungsfähigkeit Hohe Geschäftsflexibilität Schutz vor neu entstehenden Gefährdungen Hohe Skalierbarkeit Echtzeitschutz im Falle eines Eindringens von Viren Erkennen von Spam unabhängig von Format und Sprache
Erkennen und Vorbeugen von Eindringlingen (IDP)	<ul style="list-style-type: none"> Datenbank mit mehr als 3000 Signaturen; Fähigkeit, multiple Strategien, u.a. signatur-, sender- und empfangerbasiert zu erstellen Interne Benutzererkennung Erkennen und Vorbeugen gegen Eindringversuche durch die Verwendung von individuellen Signaturen Verhinderung von Eindringversuchen, DoS-Angriffen, bösartigen Quellen, backdoor activity und diversen netzwerkbasieren Gefährdungen Blockiert anonyme Proxies mit HTTP proxy Signaturen Blockiert "phone home" Aktivitäten 	<ul style="list-style-type: none"> Sehr niedrige Fehlerrate Echtzeitschutz in dynamischer Umgebung, wie DHCP und Wi-Fi Bietet unmittelbare Benutzererkennung im Falle von interner Gefährdung Applizieren von IDP-Strategien auf Benutzer
Inhaltsfilter	<ul style="list-style-type: none"> Eine automatisierte Web Kategorisierungsengine blockiert nicht funktionierende Seiten, basierend auf Millionen von Seiten in über 68 Kategorien URL-Filter für HTTP & HTTPS Protokolle Hierarchie-, unterteilungs-, gruppen- und benutzerbasierte Filterstrategien Zeitbasierter Zugriff auf vorbestimmte Seiten Verhindert das Herunterladen von Streaming Media, Spielen, Tickers und Ads (Werbung) Unterstützt CIPA-Zustimmung für Schulen und Bibliotheken 	<ul style="list-style-type: none"> Schützt das Netzwerk gegen externe Gefährdungen Blockiert Zugriff auf eingeschränkte Webseiten Einklang mit den gesetzlichen Bestimmungen gesichert Spart Bandbreite und erweitert die Leistungsfähigkeit Schützt vor gesetzlicher Haftungsverpflichtung Versichert Schutz von Minderjährigen im Internet Befähigt Schulen, sich für die E-Rate Förderung zu qualifizieren
Bandbreitenmanagement	<ul style="list-style-type: none"> Einschränkung und Erweiterung der Bandbreite nach Hierarchie, Unterteilung, Gruppen und Benutzer 	<ul style="list-style-type: none"> Verhindert Bandbreitenstau Sichert Vorrang von Bandbreite für wichtige Anwendungen
Multiples Linkmanagement	<ul style="list-style-type: none"> Sicherheit über mehrere ISP-Links durch das Benutzen einer einzigen Vorrichtung Ausgleichen des Traffics basierend auf der "Round Robin"-Aufteilung Ausfallsicherung von Links verschiebt den Traffic automatisch von einem fehlgeschlagenen auf einen funktionierenden Link 	<ul style="list-style-type: none"> Einfache Verwaltbarkeit der Sicherheit über mehrere Links Reguliert Bandbreitenstau Optimale Benutzbarkeit von preislich günstigen Links Versichert ununterbrochenen Geschäftsbetrieb
On-Appliance Reporting (Berichterstattung)	<ul style="list-style-type: none"> Vollständige Reporting Suite verfügbar Erkennen des Traffics ermöglicht Berichterstattung in Echtzeit Individuelle Berichterstattung mittels Benutzernamen 	<ul style="list-style-type: none"> Verringert die Gesamtbetriebskosten, da keine zusätzlichen kostenpflichtigen Anschaffungen nötig sind Unmittelbare und vollständige Sichtbarkeit der Navigationsmuster des Internets Unmittelbare Identifizierung von Opfer und Angreifer im internen Netzwerk

Hardware Spezifikationen	25i	50i	100i	250i	500i	1000i	1500i
Interfaces							
10/100 Ethernet ports	4	4	4	2	-	-	-
10/100/1000 GBE Ports	-	-	-	2	6	10	10
Konfigurierbare Internal/ DMZ/ WAN Ports	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Konsolen-Ports (RJ45)	-	-	1	-	1	1	1
SFP (Mini GBIC) Ports	-	-	-	-	-	2	2
COM port	1	2	-	2	-	-	-
USB ports	2	4	2	4	2	2	2
Dimensionen							
Höhe	5 cm	4,4 cm	4,4 cm	4,4 cm	4,4 cm	8,8 cm	8,8 cm
Breite	22,5 cm	42,7 cm	42,7 cm	42,7 cm	42,7 cm	42,4 cm	42,4 cm
Tiefe	20,5 cm	23,1 cm	23,1 cm	34 cm	34 cm	53,1 cm	53,1 cm
Speisung							
Eingangsspannung	100-240VAC, 24,8W	110-240VAC, 25,09W	110-240VAC, 30W	110-240VAC, 70,93W	110-240VAC, 82W	90-264VAC, 210W	90-264VAC, 210W
Umgebungsbedingung							
Betriebstemperatur	5 à 40 °C	0 à 40 °C	0 à 40 °C	0 à 40 °C	0 à 40 °C	0 à 40 °C	0 à 40 °C
Archivierungstemperatur	0 à 70 °C	-20 à 80 °C	-20 à 80 °C	-20 à 80 °C	-20 à 80 °C	-20 à 80 °C	-20 à 80 °C
Relative Feuchtigkeit (Ohne Kondensierung)	5 à 95%	10 à 90%	10 à 90%	10 à 90%	10 à 90%	10 à 90%	10 à 90%
Kühlungsventilatoren	1	2	4	2	4	7	7

Systemleistung	25i	50i	100i	250i	500i	1000i	1500i
Gleichlaufende Sessions	130,000	220,000	370,000	400,000	400,000	600,000	1,000,000
Neue Sessions/Sekunde	2,200	3,000	4,500	10,000	20,000	25,000	40,000
Firewall Datenfluss (Mbps)	100	175	200	500	2Gbps	3.5Gbps	6Gbps
168-bit Triple-DES/AES Datenfluss (Mbps)	30/75	50/60	80/100	150/170	200/250	400/500	600/750
Antivirus Datenfluss (Mbps)	30	40	150	225	450	600	800
IDP Datenfluss (Mbps)	60	100	160	200	500	1000	2500
UTM Datenfluss (Mbps)	25	35	100	135	320	450	600
Knoten	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt
Beglaubigte Benutzer	10/25/Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt

Merkmalspezifikationen

Stateful Inspection Firewall

- Multiple Zonensicherheit mit verschiedenen Ebenen von Reglements bzgl. der Zugriffsmöglichkeiten für jede Zone
- Regeln beruhend auf der Zusammensetzung von Benutzer-, Quellen- und Zielzonen, sowie der IP Adresse und Service
- Aktionen beinhalten strategienbasierte Kontrolle über IDP, Inhaltsfilter, Antivirus, Antispam und Bandbreitenmanagement
- Zugriffsplanung
- Strategienbasiertes Quellen- und Ziel NAT-Verfahren
- H.323 NAT Traversal
- Unterstützt 802.1q VLAN
- Verhinderung von DoS Angriffen

Gateway Antivirus & Antispamware

- Entfernen und Erkennen von Viren, Würmern und Trojanern
- Schutz vor Spyware, Malware und Phishing
- Automatisches Aktualisieren der Signaturdatenbank von Viren
- Scant HTTP, FTP, SMTP, POP3, IMAP
- Individuelle Einrichtung der Benutzeruntersuchung
- Selbst bedienbare Quarantänenzone
- Scannen und Zustellen je nach Dateigröße
- Blockieren je nach Dateityp
- Hinzufügen von Disclaimer/ Signatur

Gateway Antispam

- Schwarze Listen in Echtzeit (RBL), MIME Header Check
- Filter beruhend auf Mitteilungsheder (Kensatz), -größe, -sender, -empfänger
- Identifizieren der Kopfzeile
- Schwarze Liste von IP-Adressen
- Umleiten von Spam Mails an zugehörige Email Adresse
- Image-Spamfilter beruhend auf RPD Technologie
- Echtzeitschutz vor dem Eindringen von Viren
- Selbst bedienbare Quarantänenzone

Dynamisches Erkennen und Vorbeugen von Eindringlingen (IDP)

- Signaturen: Voreingestellt (3000+), Benutzerdefiniert
- IDP-Strategien: Multiple, Benutzerdefiniert
- Benutzerbasiertes Erstellen von Regeln
- Automatische Echtzeitaktualisierung von den CRProtect Netzwerken
- Anomalitätenerkennung von Protokollen
- Blockieren des HTTP Proxy Traffics
- P2P Anwendungssignaturen, einschl. Skype

Inhaltsfilter

- Eingebaute Datenbank zur Kategorisierung von Internetseiten
- Blockieren von URL, Schlüsselwörtern und Dateitypen
- Kategorien: Voreingestellt (68+), Benutzerdefiniert
- Unterstützte Protokolle: HTTP, HTTPS
- Blockiert Malware, Phishing, Pharming URLs
- Benutzerdefinierte Blockierungsnachrichten für jede Kategorie
- Blockiert Java Applets, Cookies, Active X, HTTP Upload
- CIPA-konform

Virtual Private Network – VPN

- IPSec, L2TP, PPTP
- Chiffrierung - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash-Algorithmen - MD5, SHA-1
- Authentifizierung: Pre-Shared Key (vorher vereinbarter Schlüssel), Digitale Zertifikate
- IPSec NAT Traversal
- Unterstützt Dead Peer Detection und PFS
- Diffie Hellman Gruppen - 1, 2, 5, 14, 15, 16
- Übernimmt externe Zertifizierung
- Export von Konfigurationen an mobile Benutzer
- DNS-Unterstützung für Tunnelendpunkte
- VPN-Verbindung nicht nötig

Bandbreitenmanagement

- Verwaltung der Bandbreite basierend auf Anwendung und Benutzeridentität
- Regeln, beruhend auf der Erweiterbarkeit der Bandbreite
- Erkennen des Traffics beruhend auf Anwendung und Benutzeridentität
- Multi-WAN Berichterstattung bzgl. der Bandbreite

Kontrollen beruhend auf Benutzeridentität und Gruppen

- Beschränkung der Zugriffszeit
- Zeitliche Beschränkung für Kontingente
- Zeitplan-basierte Einschränkung und Erweiterung der Bandbreite
- Einschränkung des Datenkontingents
- Zeitplan-basierte P2P und IM Regelungen

Vernetzung

- Automatische Ausfallsicherung von multiplen Links
- Aufteilung beruhend auf dem Weighted Round Robin-Verfahren
- Routingregeln beruhend auf Anwendung und Benutzer
- DDNS/PPPoE Klient
- Unterstützung für TCP MSS-Konfiguration
- Unterstützung für HTTP Proxy Mode Deployment (Betriebsbereitstellung)
- Unterstützung von Parent-Proxy
- Dynamisches Routing: RIP v1&v2, OSPF, BGP
- Multicast Forwarding

Hohe Verfügbarkeit*

- Aktiv-passiv mit State-Synchronisierung
- Zustandsorientierte Ausfallsicherung
- Meldung bei Zustandsänderung der Vorrichtung

Administration

- Web-basierter Konfigurations Assistent
- Rollenbasierte Administration
- Multiple Administratoren und verschiedene Benutzerniveaus
- Upgrades und Änderungen via Web UI

System Management

- Kontrollinterface
- Web UI (HTTPS)
- Command Line Interface
- Secure Command Shell (SSH)
- SNMP (v1, v2c, v3)
- Cyberoam Central Console

Authentifizierung des Benutzers

- Lokale Datenbank
- Windows Domain Controller & Active Directory Integration
- Automatisches Windows Single Sign On
- Externe LDAP/RADIUS Datenbank-Integration

Protokollierung / Kontrolle

- Internes Festplattenlaufwerk
- Grafische und historische Kontrolle in Echtzeit
- Email-Benachrichtigung von Berichten, Viren und Angriffen
- Unterstützt Syslog

Ausführliche Berichterstattung

- Eindringlingen
- Web-Kategorien (Benutzer, Art des Inhalts)
- Verletzungen der Regeln
- In Suchmaschinen eingegebene Schlüsselwörter
- Datentransfer (nach Host, Gruppen und IP-Adresse)
- Viren, nach Benutzer und IP-Adresse
- Mehr als 45 Compliance Reports

VPN Client

- IPSec-konform
- Kompatibilität mit größeren IPSec VPN Gateways
- Unterstützte Plattformen: Windows 98, Me, NT4, 2000, XP, Vista
- Importkonfiguration

Regelbefolgung/Zustimmung

- CE
- FCC

Zertifizierung

- ICSA Firewall - Corporate
- VPN - Basic and AES interoperability
- Checkmark UTM Level 5 Certification

*Hohe Verfügbarkeit (High availability) ist nur in den CR50, CR100, CR250, CR500, CR1000 und CR1500-Vorrichtungen vorhanden



Ganesh Consulting - 12 rue du Clos - CH 1800 Vevey

info@ganesh-consulting.ch - tel : +41 21 921 76 74

Copyright © 1999 - 2008 Elitecore Technologies Ltd.
Elitecore Technologies Ltd. versucht, akkurate und verlässliche Information zum Zeitpunkt der Veröffentlichung zur Verfügung zu stellen. Dennoch übernimmt Elitecore Technologies keine Verantwortung für eventuell auftauchende Fehler und behält das Recht vor, Änderungen am Produkt selbst oder an dessen Design ohne Bekanntmachung vorzunehmen.
PL-21-95417-080504

