



UTM Cyberoam

Les Cyberoam séries CR, appliances de sécurité intégrée basées sur l'identité, offrent une protection en temps réel contre les menaces mixtes actuelles grâce à leurs stratégies orientées utilisateurs.

Cyberoam propose aux entreprises des solutions adaptées comprenant, sur une seule et même plate-forme, un pare-feu, un VPN, un antivirus, un antispam, un IDP (détection et prévention des intrusions), un filtrage de contenu, ainsi qu'une gestion de la bande passante et des liens multiples. La Cyberoam Central Console permet une gestion centralisée de l'ensemble de ces fonctionnalités. Grâce à la fonction intégrée de haute disponibilité, ces solutions garantissent également une protection en cas de défaillance matériel et permettent d'optimiser le temps de disponibilité du réseau et d'assurer un accès ininterrompu. Les entreprises, les établissements scolaires et les administrations sont ainsi protégés efficacement contre les menaces internes et externes telles que logiciels espions, phishing, pharming, virus, vers, chevaux de Troie, attaques par déni de service, etc.

Sécurité basée sur l'identité pour une gestion unifiée

En intégrant l'identité de l'utilisateur comme élément essentiel de sécurité, Cyberoam propose aux entreprises d'oublier les solutions classiques basées sur les adresses IP, inadaptées aux environnements dynamiques, et d'opter pour des solutions innovantes et plus performantes. Grâce à cette sécurité axée sur l'identité, les professionnels peuvent exercer leur activité en toute flexibilité tout en bénéficiant en permanence d'une sécurité complète, y compris en connexion DHCP ou Wi-Fi. Les utilisateurs sont en effet identifiés en temps réel sur le réseau, qu'ils soient à l'origine de la menace ou qu'ils en soient simplement les victimes.



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

Fonctionnalités	Description	Points forts
Pare-feu axé sur l'identité (certifié ICSA Labs)	<ul style="list-style-type: none"> Inspection efficace des paquets (dynamique et approfondie) Protection contre les attaques internes et externes par déni de service ou inondation Contrôle d'accès basé sur l'identité pour le P2P et la MI 	<ul style="list-style-type: none"> Protection de la couche application Grande flexibilité pour définir les stratégies orientées utilisateurs Grande extensibilité
VPN	<ul style="list-style-type: none"> Norme industrielle : VPN IPSec, L2TP, PPTP Haute disponibilité VPN pour les connexions IPSec et L2TP Double certification VPNC - Basic and AES Interop 	<ul style="list-style-type: none"> Connexions sécurisées pour les filiales et utilisateurs distants Connexion Internet à distance à moindre coût Basculement efficace avec priorités de connexion définies
Antivirus au niveau de la passerelle	<ul style="list-style-type: none"> Scan du trafic HTTP, FTP, IMAP, POP3 et SMTP Détection et élimination des virus, vers et chevaux de Troie Accès aux courriers placés en quarantaine pour les administrateurs Limitation des transferts de fichiers par mots-clés Identification immédiate des utilisateurs en cas d'attaques HTTP 	<ul style="list-style-type: none"> Protection totale du trafic pour tous les protocoles Grande flexibilité professionnelle Protection des données confidentielles Sécurité en temps réel
Antispam au niveau de la passerelle	<ul style="list-style-type: none"> Scan du trafic SMTP, POP3 et IMAP Détection, marquage et mise en quarantaine des spams Politiques souples ou strictes selon les besoins des utilisateurs Création de listes blanches et noires Protection contre l'intrusion de virus Protection antispam (y compris spams images) indépendante du contenu, grâce à la technologie RPD™ (détection des signatures récurrentes) 	<ul style="list-style-type: none"> Meilleure productivité Grande flexibilité professionnelle Protection contre les nouvelles menaces Grande extensibilité Protection en temps réel en cas d'intrusions de virus Détection des spams quels que soient leur format et leur langue
Détection et prévention des intrusions (IDP)	<ul style="list-style-type: none"> Base de données comprenant plus de 3 000 signatures Elaboration de stratégies multiples grâce à des politiques basées sur la signature, l'expéditeur ou le destinataire Identification interne des utilisateurs Détection et prévention des intrusions par signatures personnalisées Protection contre les tentatives d'intrusions par portes dérobées, les dénis de service, les codes malicieux et les menaces mixtes du réseau Blocage des proxies anonymes avec signatures de proxy HTTP 	<ul style="list-style-type: none"> Taux de faux positifs quasi-nul Sécurité en temps réel dans les environnements dynamiques comme le DHCP et le Wi-Fi Identification immédiate des utilisateurs en cas de menaces internes Politiques IDP appliquées aux utilisateurs
Filtrage de contenu	<ul style="list-style-type: none"> Accès bloqué aux sites non professionnels grâce à un outil de catégorisation automatique classant des millions de sites dans plus de 68 catégories Politiques de filtrage orientées poste hiérarchique, département, groupe ou utilisateur Temps d'accès limité pour des sites prédéfinis Blocage des téléchargements de vidéos, de jeux et de publicités Conformité CIPA pour les écoles et bibliothèques 	<ul style="list-style-type: none"> Protection du réseau contre les attaques externes Conformité garantie avec les législations en vigueur Optimisation de la bande passante et meilleure productivité Protection contre la responsabilité légale Sécurité des mineurs garantie sur Internet Possibilité d'obtention de la subvention E-Rate pour les écoles grâce à la conformité CIPA
Gestion de la bande passante	<ul style="list-style-type: none"> Réservation et extension de la bande passante par postes hiérarchiques, départements, groupes et utilisateurs 	<ul style="list-style-type: none"> Pas de saturation de la bande passante Applications vitales privilégiées lors de l'allocation de la bande passante
Gestion des liens multiples	<ul style="list-style-type: none"> Sécurité des liens ISP multiples sur une seule appliance Répartition de charge basée sur le Round Robin pondéré Secours multiliens qui bascule automatiquement le trafic d'un lien rompu vers un lien opérationnel 	<ul style="list-style-type: none"> Sécurité des liens multiples facile à administrer Maîtrise des engorgements de la bande passante Utilisation optimale des liens à faible coût Pérennité des activités garantie
Reporting intégré	<ul style="list-style-type: none"> Suite de reporting complète et intégrée Rapports en temps réel grâce à la détection du trafic Reporting par nom d'utilisateur 	<ul style="list-style-type: none"> Coût total de possession moindre, aucun achat supplémentaire nécessaire Visibilité instantanée et exhaustive des schémas de navigation Internet Identification immédiate des utilisateurs à l'origine ou victimes des attaques sur le réseau interne

Spécifications Matériel	25i	50i	100i	250i	500i	1000i	1500i
Interfaces							
Ports Ethernet 10/100	4	4	4	2	-	-	-
Ports GbE 10/100/1000	-	-	-	2	6	10	10
Ports configurables interne/DMZ/WAN	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Ports console (RJ45)	-	-	1	1	1	1	1
Ports SFP (Mini GBIC)	-	-	-	-	-	2	2
Port COM	1	2	-	2	-	-	-
Ports USB	2	4	2	4	2	2	2
Dimensions							
Hauteur	5 cm	4,4 cm	4,4 cm	4,4 cm	4,4 cm	8,8 cm	8,8 cm
Largeur	22,5 cm	42,7 cm	42,7 cm	42,7 cm	42,7 cm	42,4 cm	42,4 cm
Profondeur	20,5 cm	23,1 cm	23,1 cm	34 cm	34 cm	53,1 cm	53,1 cm
Alimentation							
Tension d'entrée	100-240VAC,	110-240VAC,	110-240VAC,	110-240VAC,	110-240VAC,	90-264VAC,	90-264VAC,
Alimentation redondante	24,8W	25,09W	30W	70,93W	82W	210W	210W
Conditions d'ambiance							
Température de fonctionnement	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
Température de stockage	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
Humidité relative (sans condensation)	5 à 95%	10 à 90%	10 à 90%	10 à 90%	10 à 90%	10 à 90%	10 à 90%
Système de refroidissement (ventilateur 40 mm)	1	2	4	2	4	7	7

Performances du système	25i	50i	100i	250i	500i	1000i	1500i
Sessions concurrentes	130.000	220.000	370.000	400.000	400.000	600.000	1.000.000
Nouvelles sessions/seconde	2.200	3.000	4.500	10.000	20.000	25.000	40.000
Débit pare-feu (Mbps)	100	175	200	500	2Gbps	3.5Gbps	6Gbps
Débit Triple-DES/AES 168-bit (Mbps)	30/75	50/60	80/100	150/170	200/250	400/500	600/750
Débit antivirus (Mbps)	30	40	150	225	450	600	800
Débit IDP (Mbps)	60	100	160	200	500	1000	2500
Débit UTM (Mbps)	25	35	100	135	320	450	600
Noeuds	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité
Utilisateurs authentifiés	10/25/Illimité	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité

Description des fonctionnalités

Modes et fonctionnalités pare-feu

- Sécurité multizones avec niveaux d'application des politiques d'accès distincts pour chaque zone
- Politiques basées sur l'association de la zone utilisateur/source/destinataire ainsi que les adresses et les services IP
- Contrôle stratégique intégré pour l'IDP, le filtrage de contenu, l'antivirus, l'antispam et la gestion de la bande passante
- Répartition d'accès
- NAT stratégique source et destinataire
- Traversée NAT H.323
- Support VLAN 802.1q
- Prévention contre les attaques par déni de service

Antivirus

- Détection et élimination des virus, vers, chevaux de Troie
- Protection contre les logiciels espions/malveillants et le phishing
- Mise à jour automatique des signatures de virus
- Scans HTTP, FTP, SMTP, POP3, IMAP
- Scan utilisateur personnalisé
- Zone de quarantaine accessible à tout moment
- Scan et réception selon la taille des fichiers
- Blocage par type de fichiers
- Ajout d'avis de non responsabilité/signature

Antispam

- Liste noire en temps réel (RBL)
- Contrôle des en-têtes MIME
- Filtre basé sur l'en-tête, la taille, l'expéditeur et le destinataire
- Marquage de l'objet
- Liste blanche/noire des adresses IP
- Spams redirigés sur une adresse email dédiée
- Filtrage des spams images grâce à la technologie RPD
- Protection en temps réel contre les intrusions de virus

Détection et prévention dynamique des intrusions

- Plus de 3 000 signatures de détection des intrusions
- Politiques IDP : multiples, personnalisées
- Mise en œuvre de politiques orientées utilisateurs
- Mises à jour automatiques depuis les réseaux CRProtect
- Détection des anomalies au niveau protocolaire
- Création de signatures personnalisées
- Blocage du trafic HTTP proxy
- Signatures d'applications P2P y compris Skype

Filtrage de contenu

- Base de données intégrée de catégorisation des sites Internet
- Blocage par URL, mot-clé, type de fichier
- Base de données comprenant plus de 68 catégories par défaut
- Personnalisation des catégories
- Blocage de téléchargement HTTP
- Blocage des URL sources d'applications malveillantes, de phishing et de pharming
- Messages de blocage personnalisés par catégorie
- Blocage des applications Java, des cookies et des Active X
- Conformité CIPA

VPN

- IPSec, L2TP, PPTP
- Algorithmes de chiffrement - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Algorithmes de hachage - MD5, SHA-1
- Authentification : clés prépartagées, certificats numériques
- Traversée NAT pour IPSec
- Support Dead Peer Detection et PFS
- Groupes Diffie-Hellman - 1, 2, 5, 14, 15, 16
- Prise en charge de la certification externe
- Exportation des configurations vers les utilisateurs mobiles
- Support DNS pour les extrémités de tunnel
- Connexion VPN redondante

Gestion de la bande passante

- Gestion de la bande passante basée sur les applications vitales et l'identité utilisateur
- Politique de disponibilité et d'extension de la bande passante
- Détection du trafic basée sur les applications et l'identité utilisateur
- Reporting de bande passante des liens WAN multiples

Contrôles axés sur l'identité utilisateurs et groupes

- Temps d'accès limité
- Quota horaire
- Réservation et extension prédéfinies de la bande passante
- Quota de données
- Contrôles P2P et IM prédéfinis

Mise en réseau

- Secours multiliens automatique
- Répartition de charge Round Robin pondéré
- Support multizones
- Règles de routage basées sur les applications et les utilisateurs
- DNS dynamique
- Client PPPoE
- Support pour la configuration du MSS TCP
- Support pour le déploiement du mode proxy HTTP
- support proxy parent
- Routage dynamique (RIP v1 et v2, OSPF)

Haute disponibilité*

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

Administration

- Assistant de configuration Web
- Administration basée sur les rôles
- Niveaux d'administrateurs et utilisateurs multiples
- Mises à jour et modifications par le biais d'une IU Web

Administration système

- Interface console
- Interface utilisateur Web (HTTPS)
- Interface de ligne de commande
- Secure Command Shell (SSH)
- SNMP (v1, v2c, v3)
- Cyberoam Central Console

Authentification de l'utilisateur

- Base de données locale
- Contrôleur de domaine Windows et support Active Directory
- Identification unique Windows automatique
- Support de la base de données LDAP/RADIUS

Journalisation / contrôle

- Disque dur interne
- Contrôle historique et graphique en temps réel
- Notification par email des rapports, virus et attaques
- Prise en charge de Syslog

Reporting intégré

- Reporting sur les activités d'intrusion
- Reporting sur les violations des politiques
- Reporting sur les catégories de sites (utilisateur, type de contenu)
- Reporting sur les mots-clés des moteurs de recherche
- Reporting sur le transfert des données (par hôte, groupe et Adresse IP)
- Reporting sur les virus par utilisateur et adresse IP

Client VPN

- Conformité IPSec
- Interopérabilité avec les principales passerelles VPN IPSec
- Plates-formes prises en charge : Windows 98, Me, NT4, 2000, XP, Vista
- Configuration d'importation

Conformité

- CE
- FCC

Certification

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

*Haute disponibilité disponible uniquement sur les appliances CR50, CR100, CR250, CR500, CR1000 et CR1500



Etats-Unis - Tél : +1-978-465-8400, Fax : +1-978-293-0200
 Inde - Tél : +91-79-66065606, Fax : +91-79-26407640

Copyright © 1999 - 2008 Elitecore Technologies Ltd. All rights reserved.
 Cyberoam and Cyberoam logo are registered trademarks of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice. PL-21-95417-080504

