Cyberoam
A SOPHOS Company

NG CRIOOiNG Évolutivité

Sécurité évolutive pour les réseaux des PME | CRIOOiNG

Fiche technique

Les appliances de gestion unifiée des menaces de la série NG de Cyberoam sont des appliances de sécurité réseau de nouvelle génération qui offrent des fonctionnalités de sécurité UTM ainsi que des performances capables de répondre aux besoins des futurs réseaux. Les appliances de la série NG pour PME sont les « UTM les plus rapides » conçus pour ce segment. Grâce à un matériel et un logiciel de pointe, la série NG offre des vitesses de débit supérieures à toutes les autres appliances UTM présentes sur ce segment de marché. Cela permet de garantir la prise en charge des futures tendances informatiques, notamment l'accès Internet haut débit et la multiplication du nombre de dispositifs dans les entreprises. Ainsi, les réseaux des PME bénéficient d'une sécurité évolutive.

Grâce à la série NG de Cyberoam, les entreprises s'assurent sécurité, connectivité et productivité. La technologie de couche 8 de Cyberoam considère l'identité de l'utilisateur comme la 8e couche (couche HUMAINE) de la pile de protocoles. Elle associe l'identité de l'utilisateur à la sécurité, ce qui permet d'accélérer les contrôles de sécurité et d'offrir à l'entreprise une visibilité immédiate sur l'origine des attaques en identifiant non seulement l'adresse IP, mais également le nom d'utilisateur. L'architecture de sécurité extensible (ESA) de Cyberoam prend en charge les améliorations fonctionnelles qui peuvent être rapidement développées et facilement déployées. Ainsi, les entreprises bénéficient d'une sécurité évolutive.

La série « nouvelle génération » :

Les UTM les plus rapides conçus pour les PME

La technologie de couche 8 de Cyberoam considère « l'identité de l'utilisateur » comme la 8e couche de la pile de protocoles

L8	UTILISATEUR	
L7	Application	
L6	Présentation	ASCII, EBCDIC, ICA
L5	Session	L2TP, PPTP
L4	Transport	TCP, UDP
L3	Réseau	192.168.1.1
L2	Liaison de données	00-17-BB-8C-E3-E7
L1	Physique	

L'UTM de Cyberoam offre la sécurité, de la couche 2 à la couche 8, à l'aide de politiques basées sur l'identité

Les fonctionnalités UTM de Cyberoam assurent Sécurité, Connectivité et Productivité

Sécurité

Sécurité du réseau
- Pare-feu
- Système de prévention des intrusions (IPS)
- Pare-feu d'application Web

Sécurité du contenu
- Antivirus/Antispyware
- Antispam (entrant/sortant)
- Sécurité du contenu HTTPS/SSL

Sécurité administrative
- IU nouvelle génération
- iView - Journalisation et Reporting

Connectivité

Continuité des activités
- Gestion des liens multiples
- Haute disponibilité

Disponibilité du réseau
- VPN
- Connectivité 3G/4G/WiMAX

Connectivité évolutive
- « IPv6 Ready » niveau Gold

Productivité

Productivité des employés
- Filtrage de contenu
- Archivage et contrôle des messageries instantanées

Optimisation des ressources informatiques
- Gestion de la bande passante
- Détection du trafic
- Visibilité et contrôle d'application

Productivité de l'administrateur
- IU nouvelle génération

Spécifications

Interfaces

Ports cuivre GbE	8
Ports internes/DMZ/WAN configurables	Oui
Ports console (Rj45)	1
Ports USB	2
Segment Hardware Bypass#	2

Performances du système*

Débit pare-feu (UDP) (Mbits/s)	4,500
Débit pare-feu (TCP) (Mbits/s)	3,500
Nouvelles sessions/seconde	45,000
Sessions simultanées	1,250,000
Débit VPN IPSec (Mbits/s)	450
Nombre de tunnels IPSec	250
Débit VPN SSL (Mbits/s)	400
Débit protégé WAF (Mbits/s)	700
Débit antivirus (Mbit/s)	1,400
Débit IPS (Mbits/s)	1,200
Débit UTM (Mbits/s)	750

Pare-feu dynamique

- Pare-feu couche 8 (Utilisateur - Identité)
- Zones de sécurité multiples
- Critères de contrôle d'accès (ACC) - Utilisateur - Identité, Zone source/destination, Adresse MAC/IP, Service
- Politiques UTM : IPS, filtrage Web, filtrage applicatif antivirus, antispam et gestion de la bande passante
- Contrôle et visibilité couche 7 (application)
- Planification des accès
- NAT source et destination basé sur les politiques
- H.323, SIP NAT Traversal
- Prise en charge VLAN 802.1q
- Prévention des attaques DoS et DDoS
- Filtrage MAC et IP-MAC, prévention contre l'usurpation

Antivirus et antispyware de passerelle

- Virus, vers et chevaux de Troie : Détection et suppression
- Protection contre les spywares, les logiciels malveillants et le phishing
- Mise à jour automatique de la base de données des signatures de virus
- Analyse de HTTP, HTTPS, FTP, SMTP, POP3, IMAP, MI, Tunnels VPN
- Personnalisation de l'analyse au niveau utilisateur
- Zone de quarantaine libre-service
- Analyse et remise selon la taille des fichiers
- Blocage selon le type de fichiers
- Ajout de l'avis de non-responsabilité/la signature

Antispam de passerelle

- Analyse des entrées/sorties
- Liste noire temps réel (RBL, Real-time Blacklist), contrôle des en-têtes MIME
- Filtrage selon l'en-tête, la taille, l'expéditeur et le destinataire du message
- Marquage de la ligne objet
- Liste blanche/noire d'adresses IP
- Redirection des spams vers une adresse e-mail dédiée
- Filtrage des spams images avec la technologie RPD
- Protection instantanée contre les épidémies virales
- Zone de quarantaine libre-service
- Notification de spam par le biais de rapports
- Filtrage des spams basé sur la réputation IP

Système de prévention des intrusions (IPS)

- Signatures : par défaut (plus de 4 500), personnalisées
- Politiques IPS : multiples, personnalisées
- Création de politiques basées sur l'utilisateur
- Mises à jour automatiques en temps réel depuis les réseaux CRProtect
- Détection des anomalies de protocole
- Prévention contre les attaques DDoS
- IPS SCADA avec catégories prédéfinies pour les signatures ICS et SCADA

Filtrage Web

- Base de données intégrée des catégories Web
- Blocage selon URL, mot-clé, type de fichiers
- Catégories : par défaut (plus de 82), personnalisées
- Protocoles pris en charge : HTTP, HTTPS
- Blocage des URL d'hameçonnage, de pharming et de logiciels malveillants
- Contrôle d'accès planifié
- Blocage personnalisé des messages par catégorie
- Bloque les applets Java, les cookies, les Active X
- Conformité CIPA
- Contrôle des fuites de données via téléchargement HTTP, HTTPS

Filtrage applicatif

- Base de données intégrée des catégories d'applications
- Prise en charge de plus de 2 000 applications
- Contrôle d'accès planifié
- Bloque :
  - Proxy et tunnel
  - Transfert de fichiers
  - Réseautage social
  - Média en streaming
  - Stockage et sauvegarde
- Visibilité Couche 7 (Applications) et couche 8 (Utilisateur - Identité)
- Sécurité des réseaux SCADA
  - Filtrage basé sur les signatures SCADA/ICS des protocoles
  - Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk
  - Contrôle différentes commandes et fonctions

Pare-feu d'application Web

- Modèle de protection positive
- Technologie unique de détection intuitive du trafic réseau (Intuitive Website Flow Detector)
- Protection contre les injections SQL, les attaques sur les éléments dynamiques (XSS), le détournement de session, le piratage d'URL, l'empoisonnement des cookies
- Prise en charge de HTTP 0.9/1.0/1.1
- Journalisation et reporting complets

Réseau privé virtuel (VPN)

- IPSec, L2TP, PPTP
- Chiffrement (3DES, DES, AES, Twofish, Blowfish, Serpent)
- Algorithmes de hachage (MD5, SHA-1)
- Authentification (clé pré-partagée, certificats numériques)
- IPSec NAT Traversal
- Dead peer detection et prise en charge PFS
- Groupes Diffie Hellman (1, 2, 5, 14, 15, 16)
- Prise en charge des autorités de certification externes
- Exportation des configurations de connexion pour les travailleurs nomades
- Prise en charge du nom de domaine pour les terminaux du tunnel
- Redondance des connexions VPN
- Prise en charge de la superposition de réseaux
- Prise en charge VPN Hub & Spoke

VPN SSL

- Tunneling TCP et UDP
- Authentification (Active Directory, LDAP, RADIUS, Cyberoam)
- Authentification client multicouches (certificat, nom d'utilisateur/mot de passe)
- Application d'une politique au niveau utilisateur et groupe
- Accès au réseau - Split/Full tunneling
- Accès par navigateur (Portail) - Accès clientless
- Client léger tunneling VPN SSL
- Contrôle d'accès granulaire à toutes les ressources du réseau d'entreprise
- Contrôles administratifs - Expiration de la session, Dead Peer Detection, Personnalisation du portail
- Accès application basé sur TCP - HTTP, HTTPS, RDP, TELNET, SSH

Gestion des messageries instantanées (MI)

- Yahoo et Windows Live Messenger
- Analyse de virus pour le trafic des MI
- Autoriser/bloquer connexion
- Autoriser/bloquer transfert de fichiers
- Autoriser/bloquer webcam
- Autoriser/bloquer chats privés ou en groupe
- Blocage selon le contenu
- Journal des activités des MI
- Fichiers archives transférés
- Alertes personnalisées

WAN sans fil

- Prise en charge port USB 3G/4G et WiMax
- Connexion WAN primaire
- Connexion de secours WAN

Gestion de la bande passante

- Gestion de la bande passante basée sur l'application et l'identité de l'utilisateur
- Politique de bande passante garantie et étendue
- Détection du trafic basée sur l'application et l'identité de l'utilisateur
- Reporting bande passante multi-WAN
- Restriction de bande passante selon la catégorie

Contrôles basés sur l'identité de l'utilisateur et le groupe d'utilisateurs

- Restriction du temps d'accès
- Restriction avec quotas sur le temps et les données
- Réservation et extension de la bande passante planifiées
- Contrôles P2P et MI planifiés

Activité réseau

- Basculement (automatisation basculement/restauration, basculement multi-WAN, basculement modem 3G)
- Répartition de charge basée sur WRR
- Politique de routage basée sur l'application et l'utilisateur
- Attribution des adresses IP (statique, PPPoE, L2TP, client DDNS et PPTP, proxy ARP, serveur DHCP, relais DHCP)
- Prise en charge proxy HTTP
- Routage dynamique : RIP v1 et v2, OSPF, BGP, acheminement multicast
- Prise en charge du proxy parent avec FQDN
- « IPv6 Ready » niveau Gold

Haute disponibilité

- Actif-Actif
- Actif-Passif avec synchronisation d'état
- Basculement dynamique
- Alertes sur les changements d'état de l'appliance

Administration et gestion du système

- Assistant de configuration avec interface Web
- Contrôle d'accès en fonction des rôles
- Mises à niveau du firmware via une IU Web
- IU compatible Web 2.0 (HTTPS)
- IU Color Styler
- Interface de ligne de commande (série, SSH, Telnet)
- SNMP (v1, v2c, v3)
- Prise en charge multilingue : Chinois, hindi, français, coréen
- Cyberoam Central Console (en option)
- Prise en charge du protocole NTP (Network Time Protocol)

Authentification de l'utilisateur

- Base de données interne
- Intégration Active Directory
- Authentification unique Windows automatique
- Intégration base de données LDAP/RADIUS externe
- Prise en charge de client léger – Services de terminal Microsoft Windows Server 2003 et Citrix XenApp - Novell eDirectory
- Prise en charge de RSA SecurID
- Authentification externe (utilisateurs et administrateurs)
- Association utilisateur/MAC
- Serveurs d'authentification multiples

Journalisation/Contrôle

- Surveillance graphique et historique en temps réel
- Notification par email des rapports, des virus et des attaques
- Prise en charge de Syslog
- Visionneur de journaux (Pare-feu, IPS, filtrage Web, antivirus, antispam, authentification, événements système et admin)

Cyberoam iView : reporting intégré

- Outil de création de rapports intégré avec interface Web - Cyberoam-iView
- Plus de 1 000 rapports détaillés
- Plus de 45 rapports de conformité
- Rapports historiques et en temps réel
- Nombreux tableaux de bord
- Tableau de bord de contrôle par nom d'utilisateur, hôte, ID e-mail
- Rapports (sécurité, virus, spam, trafic, violations des politiques, VPN, mots-clés pour les moteurs de recherche)
- Rapports multiformats (tableaux, graphiques)
- Formats exportables (PDF, Excel)
- Planification de rapports automatisés

Client VPN IPSec**

- Interopérabilité avec les principales passerelles VPN IPSec
- Plateformes prises en charge : Windows 2000, WinXP 32/64 bits, Windows 2003 32 bits, Windows 2008 32/64 bits, Windows Vista 32/64 bits, Windows 7 RC1 32/64 bits
- Import de la configuration de connexion

Certification

- Critères communs - EAL4+
- Pare-feu d'entreprise certifié ICSA
- Certification niveau 5 Checkmark UTM
- VPNC (interopérabilité Basic et AES)
- « IPv6 Ready » niveau Gold

Spécifications matérielles

Mémoire	2Go
Carte mémoire flash	4Go
Disque dur	250Go ou plus

Conformité

CE FCC
UL

Dimensions

H x L x P (pouces)	1,7 x 14,6 x 17,3
H x L x P (cm)	4,4 x 37,2 x 44
Poids	5 kg, 11,02 lbs

Alimentation

Tension d'entrée	100-240 VCA
Consommation	99 W
Dissipation thermique totale (BTU)	338

Conditions ambiantes

Température de fonctionnement	0 à 40 °C
Température de stockage	-25 à 75 °C
Humidité relative (sans condensation)	10 à 90 %

#Si activé, le trafic ne sera réacheminé qu'en cas de panne de courant. **Achat supplémentaire requis.

*Les performances de l'antivirus, de l'IPS et de l'UTM sont calculées en fonction du trafic HTTP conformément aux directives RFC 3511. Les performances effectives peuvent varier en fonction des environnements du trafic réseau réels.

Numéros d'appel gratuits

États-Unis : +1-800-686-2360 | **Inde** : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Cyberoam® A SOPHOS Company