

## Sécurité évolutive pour les réseaux des petits bureaux/télétravailleurs (SOHO), des bureaux distants/filiales (ROBO), des PME et des grandes entreprises

## Fiche technique

Aujourd'hui, les entreprises disposent d'un Internet haut débit, le nombre de dispositifs par utilisateur se développe de manière croissante et l'utilisation des données augmente à une rapidité fulgurante. Par conséquent, les appliances de sécurité de nouvelle génération doivent répondre aux besoins des futurs réseaux. La série NG de Cyberoam offre aux entreprises une sécurité évolutive en proposant un matériel et un logiciel de pointe et des vitesses de débit jusqu'alors inégalées.

### Série NG pour les TPE et les PME :

Les appliances de la série NG sont les « UTM les plus rapides » conçus pour le segment TPE et PME.

### Série NG pour les grandes entreprises :

Dédiées aux grandes entreprises, les appliances de la série NG offrent une protection par « pare-feu de nouvelle génération (NGFW) » avec des fonctionnalités NGFW hautement performantes indispensables pour les réseaux des futures entreprises.

Grâce à la série NG de Cyberoam, les entreprises s'assurent sécurité, connectivité et productivité. La technologie de couche 8 associe identité de l'utilisateur et sécurité, offrant ainsi une accélération des contrôles de sécurité. L'architecture de sécurité extensible (ESA) de Cyberoam prend en charge les améliorations fonctionnelles qui peuvent être rapidement développées et facilement déployées.



Série NG de Cyberoam : 15iNG, 25iNG/6P, 35iNG, 50iNG, 100iNG, 200iNG/XP, 300iNG/XP, 2500iNG

Série NG sans fil de Cyberoam : 15wiNG, 25wiNG, 25wiNG-6P, 35wiNG

## Description des fonctionnalités

### Pare-feu dynamique

- Pare-feu couche 8 (Utilisateur - Identité)
- Sécurité multizone
- Critères de contrôle d'accès (ACC) : identité de l'utilisateur, zone source et de destination, adresse MAC et IP, service
- Politiques UTM - IPS, filtrage Web, filtrage applicatif, antivirus, antispam et gestion de la bande passante
- Contrôle applicatif (couche 7) et visibilité
- Planification des accès
- NAT source et destination reposant sur des 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 antispam au niveau de la passerelle

- Détection et suppression des virus, vers et chevaux de Troie
- Protection contre les logiciels espions, les logiciels malveillants et l'hameçonnage
- 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 accessible
- Analyse et remise par taille de fichier
- Blocage en fonction des types de fichiers
- Ajout d'avis de non responsabilité / signature

### Antispam (passerelle)

- Analyse des entrées/sorties\*\*
- Liste noire en temps réel (RBL, Real-time Blacklist), contrôle des en-têtes MIME
- Filtrage en fonction de l'en-tête, la taille, l'expéditeur et le destinataire du message
- Étiquetage de la ligne objet
- 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 en libre service<sup>1</sup>
- Liste blanche/noire d'adresses IP
- Notification de spam via Digest<sup>2</sup>
- Filtrage en fonction de la réputation des IP

### Système de prévention des intrusions (IPS)

- Signatures : par défaut (plus de 4 500), personnalisées
- Politiques IPS : Multiples, personnalisées
- Création de politiques au niveau utilisateur
- Mises à jour automatiques en temps réel depuis les réseaux CRProtect
- Détection des anomalies de protocole
- Prévention contre les attaques DDoS

### Filtrage Web

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

### Filtrage applicatif

- Base de données intégrée des catégories d'applications
- Plus de 11 catégories d'applications (jeux, messagerie instantanée, P2P, proxy, etc.)
- Contrôle d'accès planifié
- Blocage
  - Applications P2P (ex. : Skype)
  - Proxys anonymes (ex. : Ultra surf)
  - Activités de type « Phone home »
  - Enregistreurs de frappe (keylogger)
- Visibilité Couche 7 (Application) et couche 8 (Utilisateur - Identité)

### Pare-feu d'application Web<sup>3</sup>

- 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, etc.
- Prise en charge de HTTP 0.9/1.0/1.1
- Prise en charge de serveurs d'arrière-plan : 5 à 200 serveurs

### Réseau privé virtuel (VPN)

- IPsec, L2TP, PPTP
- Chiffrement (3DES, DES, AES, Twofish, Blowfish, Serpent)
- Algorithmes de hachage (MD5, SHA-1)
- Authentification : Clés pré-partagées, certificats numériques
- IPsec NAT Traversal
- Support Dead Peer Detection et 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 extrémités du tunnel
- Redondance de 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 (Local)
- 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, Transfert de fichiers, Webcam, conversation privée ou en groupe
- Blocage en fonction du 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 WAN de secours

### Gestion de la bande passante

- Gestion de la bande passante basée sur les applications et l'identité de l'utilisateur
- Restriction de la bande passante en fonction des catégories
- Politique de bande passante garantie et étendue
- Détection<sup>4</sup> du trafic basée sur les applications et l'identité de l'utilisateur<sup>4</sup>
- Reporting bande passante multi-WAN

### 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, Contrôles P2P et MI
- Réserve et extension de la bande passante planifiées

### Activité réseau

- Basculement/Restauration automatisé, Multi-WAN
- 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, proxy parent avec FQDN
- Routage dynamique : RIP v1 et v2, OSPF, BGP, acheminement de multicast

### Haute disponibilité<sup>5</sup>

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

### Administration et gestion système

- Assistant de configuration avec interface Web
- Contrôle d'accès basés sur les rôles
- Mise à jour du firmware via une interface Web
- Interface utilisateur compatible Web 2.0 (HTTPS)
- Interface utilisateur Color Styler
- Interface en ligne de commande (série, SSH, Telnet)
- SNMP (v1, v2, v3)
- Prise en charge multilingue : Chinois, hindi, français, coréen
- Cyberoam Central Console (en option)
- Prise en charge NTP

### 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 - Terminal Microsoft Windows Server 2003 Services et Citrix XenApp
- Prise en charge de RSA SecurID
- Authentification externe (utilisateurs et administrateurs)
- Association utilisateur/MAC
- Serveurs d'authentification multiples

### Journalisation et contrôle

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

### Cyberoam iView : reporting intégré<sup>6</sup>

- Auto 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, spam, virus, trafic, violations des politiques, VPN Mots-clés pour les moteurs de recherche
- Rapports multiformat (tableaux, graphiques)
- Formats exportables (PDF, Excel)
- Planification de rapports automatisés

### Client VPN IPsec<sup>6</sup>

- 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, Windows 8 RC1 32/64 bits
- Importation de configuration de connexion

### Certification

- Pare-feu d'entreprise certifié ICSA
- Certification niveau 5 Checkmark UTM
- VPNC (interopérabilité Basic et AES)
- IPv6 Ready niveau Gold

<sup>1,2,3,4,5,6</sup> Disponible pour tous les modèles à l'exception du CR15iNG et du CR15wiNG

<sup>7</sup> Achat supplémentaire requis

<sup>8</sup> Pas pris en charge sur l'appliance CR15iNG et la série sans fil

<sup>9</sup> Les filtrages antispam entrant et sortant ne peuvent pas être utilisés simultanément.

Spécifications	15iNG	25iNG/6P	35iNG	15wiNG	25wiNG/6P	35wiNG
----------------	-------	----------	-------	--------	-----------	--------

**Interfaces**

Ports cuivre GbE	3	4/6	6	3	4/6	6
Ports console (RJ45)	1	1	1	1	1	1
Ports USB	2	2	2	2	2	2
Segments Hardware Bypass*	-	-	-	-	-	-
Ports internes/DMZ/WAN configurables	Oui	Oui	Oui	Oui	Oui	Oui

**Performances du système\***

Débit pare-feu (UDP) (Mbits/s)	1,000	1,500	2,300	1,000	1,500	2,300
Débit pare-feu (TCP) (Mbits/s)	750	1,000	2,000	750	1,000	2,000
Nouvelles sessions/seconde	3,500	5,000	12,000	3,500	5,000	12,000
Sessions simultanées	60,000	150,000	350,000	60,000	150,000	350,000
Débit VPN IPSec (Mbits/s)	110	210	250	110	210	250
Nombre de tunnels IPSec	50	100	150	50	100	150
Débit VPN SSL (Mbits/s)	50	75	100	50	75	100
Débit protégé WAF (Mbits/s)	-NA-	45	65	-NA-	45	65
Débit antivirus (Mbit/s)	180	300	525	180	300	525
Débit IPS (Mbits/s)	140	200	350	140	200	350
Débit UTM (Mbits/s)	80	110	210	80	110	210
Utilisateurs/nœuds authentifiés	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité

**LAN sans fil intégré** (uniquement pour la série wiNG)

Normes sans fil	IEEE 802.11 a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, AES, PSK)
Antenne	3x3 MIMO détachable
Points d'accès	Jusqu'à 8 bssid
Puissance d'émission (PIRE)	11n HT40 : +15 dBm, 11b CCK : +15 dBm, 11g OFDM : +15 dBm
Sensibilité de réception	-68 dBm à 300 Mbits/s, -70 dBm à 54 Mbits/s, -88 dBm à 6 Mbits/s
Plage de fréquence	2 412 GHz - 2 472 GHz
	5 200 GHz - 5 825 GHz
Nombre de canaux sélectionnables	États-Unis (FCC) - 11 canaux, Union européenne (ETSI) / Japon (TELEC) - 13 canaux
Vitesse de transfert	802.11n : jusqu'à 450 Mbits/s, 802.11b : 1, 2, 5, 11 Mbits/s, 802.11g : 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s

**Dimensions**

H x L x P (pouces)	1.7 x 6 x 9.1					
H x L x P (cm)	4.4 x 15.3 x 23.2					
Poids de l'apppliance	1.5 kg, 3.307 lbs	2.3 kg, 5.07 lbs	2.3 kg, 5.07 lbs	1.5 kg, 3.307 lbs	2.3 kg, 5.07 lbs	2.3 kg, 5.07 lbs

**Câble**

Tension d'entrée	100-240 VAC					
Consommation	13.2 W	33.5 W	47.8 W	13.2 W	33.5 W	47.8 W
Dissipation thermique totale (BTU)	45	114	163	45	114	163
Alimentation redondante	-	-	-	-	-	-

Spécifications	50iNG	100iNG	200iNG/XP	300iNG/XP	2500iNG
----------------	-------	--------	-----------	-----------	---------

**Interfaces**

Ports cuivre GbE	8	8	10 / 6	10 / 6	14
1/10 GbE SFP (Mini GBIC) Ports	-	-	-	-	4 / 2
Ports Module Flexi** (Pour XP électroménager) (1 GbE cuivre / 1 GbE SFP / 10 GbE SFP)			8 / 8 / 4	8 / 8 / 4	
Ports console (RJ45)	1	1	1	1	1
Ports USB	2	2	2	2	2
Segments Hardware Bypass*	2	2	2	2	2
Ports internes/DMZ/WAN configurables	Oui	Oui	Oui	Oui	Oui

**Performances du système\***

Débit pare-feu (UDP) (Mbits/s)	3,250	4,500	10,000	12,000	40,000
Débit pare-feu (TCP) (Mbits/s)	3,000	3,500	8,000	9,500	28,000
Nouvelles sessions/seconde	30,000	45,000	70,000	85,000	200,000
Sessions simultanées	1,000,000	1,250,000	1,500,000	2,000,000	3,500,000
Débit VPN IPSec (Mbits/s)	400	450	800	1,200	8,000
Nombre de tunnels IPSec	200	250	300	400	3,000
Débit VPN SSL (Mbits/s)	300	400	450	500	1,000
Débit protégé WAF (Mbits/s)	300	500	650	850	1,000
Débit antivirus (Mbit/s)	1,000	1,400	2,200	2,600	6,000
Débit IPS (Mbits/s)	750	1,200	2,000	2,400	8,000
Débit UTM (Mbits/s)	550	750	1,200	1,500	4,500
Utilisateurs/nœuds authentifiés	Illimité	Illimité	Illimité	Illimité	Illimité

**Dimensions**

H x L x P (pouces)	1.7 x 14.6 x 17.3	1.7 x 14.6 x 17.3	1.7 x 17.3 x 11.85	1.7 x 17.3 x 11.85	3.54 x 17.52 x 23.23
H x L x P (cm)	4.4 X 37.2 X 44	4.4 X 37.2 X 44	4.4 x 43.9 x 30.1	4.4 x 43.9 x 30.1	9 x 44.5 x 59
Poids de l'apppliance	5 kg, 11.02 lbs	5 kg, 11.02 lbs	5.1 kg, 11.24 lbs	5.1 kg, 11.24 lbs	19 kg, 41.8 lbs

**Câble**

Tension d'entrée	100-240VAC	100-240VAC	100-240VAC	100-240VAC	90-260VAC
Consommation	99W	99W	137W	137W	258W
Dissipation thermique totale (BTU)	338	338	467	467	881
Alimentation redondante	-	-	-	-	Oui

**Conditions ambiantes :** Température de fonctionnement 0 °C à 40 °C, Température de stockage -25 °C à 75 °C, Humidité relative (sans condensation) 10 % à 90 %  
 \*Si activé, le trafic ne sera réacheminé qu'en cas de panne de courant.  
 \*\*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

