Gestion unifiée des menaces

Sécurité Internet complète

Les nouvelles menaces Internet internes et externes

- Virus, vers, chevaux de Troie
- Spams
- Intrusions
- Logiciels espions
- Phishing et pharming
- Fuite des données
- Mauvaise utilisation de la bande passante

Aucune entreprise n'est à l'abri : petites ou grandes, toutes sont confrontées aux menaces Internet, que ce soit sur le réseau externe ou le réseau interne. Ainsi, d'un côté, les attaques externes prennent de plus en plus souvent la forme de menaces mixtes ciblées ; et de l'autre, les failles de sécurité engendrées par les menaces internes augmentent la vulnérabilité de l'entreprise face aux attaques. Dans un tel environnement où les menaces évoluent sans cesse et à une vitesse fulgurante, les entreprises ont besoin de dispositifs de sécurité multiples afin de protéger efficacement leur réseau.

Toutefois, les professionnels qui ont choisi de déployer des solutions de sécurité dédiées multiples pour obtenir une protection totale doivent faire face non seulement à une lourde administration et un processus de mise à jour conséquent mais également à un coût d'investissement et de fonctionnement non négligeable.

Gestion unifiée des menaces

Cette complexité d'administration n'étant pas satisfaisante, il convenait de développer une appliance de sécurité unifiée. C'est ainsi qu'est née la solution UTM (gestion unifiée des menaces), qui regroupe l'ensemble des dispositifs de sécurité sur une seule et même plate-forme.

Avec l'augmentation des attaques externes ciblées utilisateurs et des menaces internes, ces solutions de gestion unifiée des menaces s'avèrent les plus performantes lorsqu'elles intègrent l'identité de l'utilisateur comme critère de sécurité. Une telle sécurité basée sur l'utilisateur peut en effet identifier de manière efficace toute attaque, qu'elle provienne du réseau externe ou interne.

Cyberoam – Sécurité Internet complète

Cyberoam propose une gestion des menaces intuitive avec des contrôles basés sur l'identité de l'utilisateur. Cette nouvelle approche permet d'éviter toute faille de sécurité sur le réseau et représente une réelle alternative aux dispositifs multiples, parfois redondants, en réduisant la charge du processeur et le coût d'achat et en simplifiant l'administration et la configuration des politiques de sécurité.

Cyberoam est la seule solution UTM basée sur l'identité à proposer une sécurité Internet complète grâce à des politiques orientées identité de l'utilisateur et permettant des contrôles d'une extrême finesse. La fonction intégrée de haute disponibilité assurée par un basculement actif-actif garantit une protection contre les défaillances matériel ; le temps de disponibilité du réseau est ainsi optimisé et l'accès ininterrompu. Cette gestion basée sur l'identité est très facile d'utilisation et permet une très grande flexibilité aux entreprises, établissements scolaires, administrations et autres.

Les solutions Cyberoam du CR25i au CR1500i, satisfont pleinement aux exigences de sécurité des petites, moyennes et grandes entreprises, et des filiales et bureaux distants, de 5 à 5000 utilisateurs.

Les différentes solutions de Cyberoam peuvent être gérées et contrôlées de manière centralisée grâce à Cyberoam Central Console (CCC) qui permet une visibilité et une maîtrise globales, simplifie l'administration et améliore le contrôle de sécurité.

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

Caractéristiques

En intégrant sur une seule plate-forme les meilleures technologies existantes, les solutions Cyberoam garantissent une défense parfaitement coordonnée et constituent un bouclier complet et sûr contre les menaces Internet.

- Pare-feu axé sur l'identité
- Réseau privé virtuel - VPN
- Antivirus au niveau de la passerelle
- Antispam au niveau de la passerelle
- Détection et prévention des intrusions - IDP
- Filtrage de contenu
- Gestion de la bande passante
- Gestion des liens multiples
- Reporting intégré

Avantages

Cyberoam offre aux entreprises de nombreux avantages.

Avantages techniques

- Protection en temps réel contre les menaces Internet
- Déploiement rapide
- Aucune configuration réseau
- Interface d'administration unique - interface graphique Web

Avantages financiers

- Faible coût d'investissement
- Faible coût de fonctionnement
- Retour sur investissement optimal

Avantages professionnels

- Environnement de travail sécurisé
- Maîtrise de la responsabilité légale
- Productivité optimale
- Exigences de conformité satisfaites

L’avantage d’une sécurité basée sur l’identité

Cyberoam est la seule solution UTM à inclure l’identité de l’utilisateur comme critère essentiel dans la configuration du pare-feu, et permet ainsi une visibilité instantanée et des contrôles proactifs sur les failles de sécurité. Elle intègre également l’authentification LDAP, Active Directory et RADIUS.

L’authentification ne se fait plus par adresses IP

Contrairement aux pare-feux classiques, le pare-feu Cyberoam, axé sur l’identité, n’a besoin d’aucune adresse IP pour être en mesure d’identifier l’utilisateur. Les administrateurs peuvent ainsi contrôler l’accès de chaque utilisateur indépendamment de l’IP de connexion.

Sécurité totale en environnement dynamique

Cyberoam assure une sécurité complète lors des connexions dynamiques DHCP ou Wi-Fi pour lesquelles une identification de l’utilisateur par adresse IP est impossible.

Une seule configuration de la politique de sécurité

L’ensemble des fonctionnalités Cyberoam est axé sur cette approche identité de l’utilisateur, permettant ainsi une application cohérente et efficace des stratégies propres à chaque fonctionnalité. Les contrôles sont totalement unifiés, et l’utilisation et la maintenance considérablement simplifiées.

Configuration dynamique des politiques

Cyberoam permet un aperçu clair et précis des schémas de navigation et des types de menaces. Les politiques de sécurité peuvent ainsi être modifiées en toute flexibilité et de manière dynamique afin de s’adapter aux besoins en constante évolution des différents utilisateurs.

Conformité avec la législation en vigueur

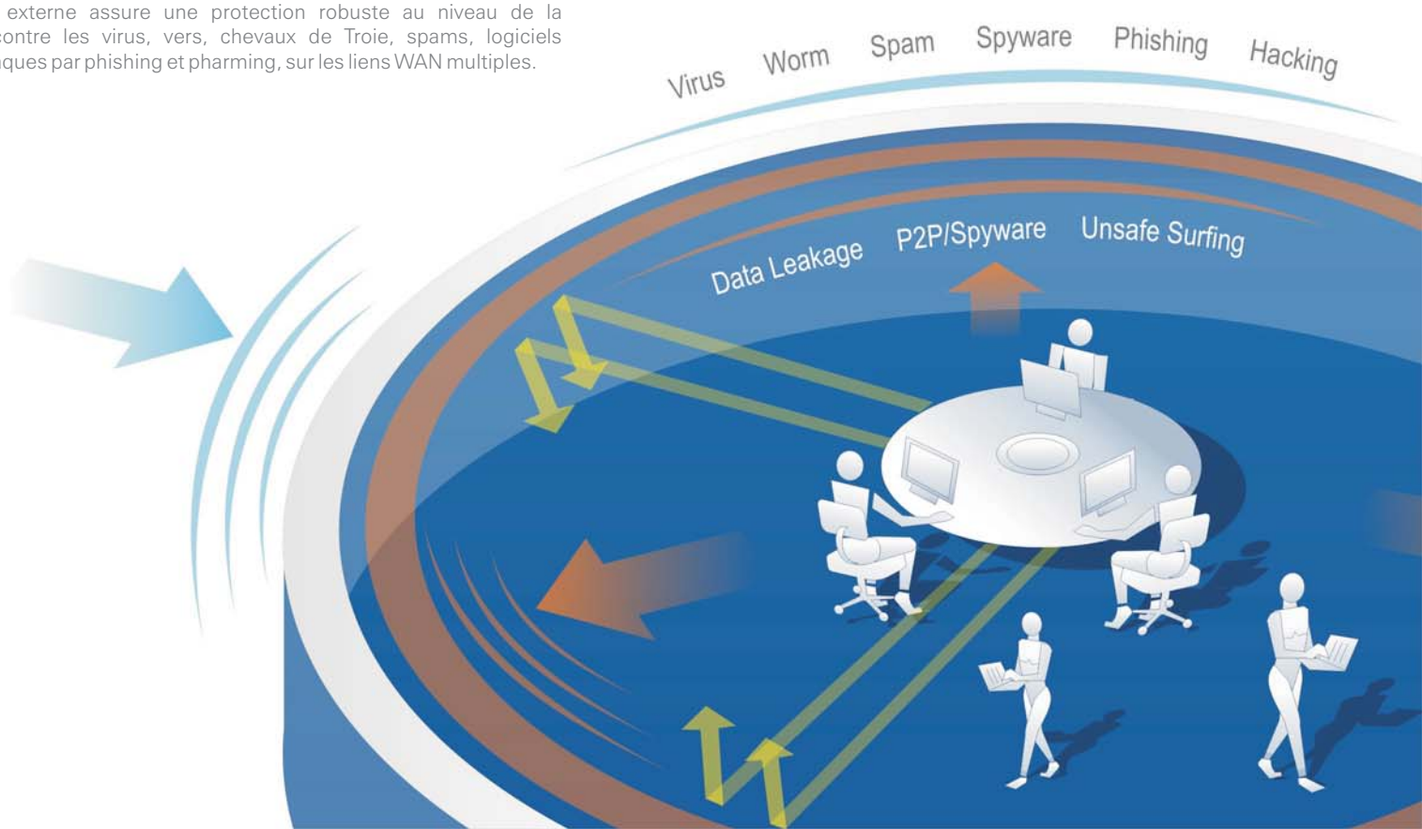
Grâce aux contrôles et à l’identification orientés utilisateurs de Cyberoam, les entreprises sont à même de répondre aux exigences et normes de conformité. La visibilité permanente et instantanée sur ‘qui a accès à quoi dans l’entreprise’ permet de simplifier les audits et les reportings.

Sécurité à double bouclier

La sécurité à double bouclier de Cyberoam permet une double protection contre les attaques externes et internes.

Le bouclier interne se charge des menaces internes, telles que fuite de données ou navigation Internet non appropriée, qui rendent les entreprises vulnérables face aux logiciels espions, au phishing ou au pharming.

Le bouclier externe assure une protection robuste au niveau de la passerelle contre les virus, vers, chevaux de Troie, spams, logiciels espions, attaques par phishing et pharming, sur les liens WAN multiples.



Quelques statistiques - Menaces externes

- 63 % des entreprises déclarent avoir subi des attaques de virus ou vers
- 58 % des entreprises ont subi des attaques par chevaux de Troie
- 60% des bots envoyant des spams envoient également des logiciels malveillants par le biais des emails
- 35 % des spams envoyés à travers le monde sont des spams images et prennent à eux seuls 70 % de la bande passante totale
- Chaque jour, environ 343 000 zombies nouvellement activés sont signalés
- Plus de 48 % des ordinateurs professionnels sont infestés par un logiciel espion quel qu'il soit

Source : wired.com, Commtouch Software Ltd.

Informez-vous sur les dernières intrusions sur le Centre de sécurité de Cyberoam *http://csc.cyberoam.com*

Pare-feu axé sur l'identité

Le pare-feu de Cyberoam offre une visibilité instantanée et une sécurité consolidée

Prise en charge de l'identité de l'utilisateur

Cyberoam inclut l'identité de l'utilisateur comme critère essentiel dans la configuration du pare-feu, ne prenant plus les adresses IP comme moyen d'identification et permettant ainsi une visibilité instantanée et des contrôles proactifs des failles de sécurité, même dans les environnements IP dynamiques. L'ensemble des dispositifs de sécurité est axé sur cette identité utilisateur afin de créer une sécurité unifiée et consolidée. Les administrateurs peuvent ainsi modifier les politiques de sécurité de manière dynamique et s'adapter aux évolutions de chaque utilisateur au sein de l'entreprise (départ, arrivée, promotion, etc.) grâce à une simplicité de configuration des différentes stratégies.

Gestion unifiée

Cyberoam propose de mettre en place, dès la configuration de la politique pare-feu une gestion centralisée des différentes fonctionnalités. La politique de sécurité globale est ainsi plus cohérente et unifiée et la configuration et la maintenance plus aisées.

Protection au niveau de la passerelle

Le pare-feu de Cyberoam assure une protection efficace grâce à une inspection approfondie et dynamique des paquets et une analyse minutieuse des en-têtes et des données utiles. Il protège également les réseaux des dénis de service, des attaques par inondation et des usurpations d'adresses IP.

Risques de menaces moindres

Le NAT (traduction d'adresses réseaux) dynamique du pare-feu protège l'entreprise des accès externes non autorisés et permet ainsi aux réseaux internes de rester à l'abri des regards indiscrets extérieurs. Une protection interne empêche également tout accès non autorisé aux sous-réseaux et groupes de travail sur le réseau de l'entreprise.

Réseau privé virtuel - VPN

Une communication sécurisée est la base d'une entreprise saine et florissante.

Communication sécurisée

Les VPN conformes aux normes IPSec, L2TP et PPTP offrent aux entreprises une connectivité sécurisée exigeant peu de bande passante, protègent des fuites et du piratage de données et garantissent l'intégrité de l'hôte, des extrémités et des données. La double certification VPNC (Basic and AES Interop) garantit l'interopérabilité du VPN de Cyberoam avec les différents environnements VPN IPSec disponibles sur le marché. Cyberoam utilise des méthodes d'authentification et des algorithmes évolués pour proposer des connexions sécurisées site à site, hôte à réseau et hôte à hôte.

Connexions sécurisées et à faible coût

Le VPN de Cyberoam fonctionne en mode transport et tunnel, encapsulant un paquet IP existant dans un autre paquet pour l'acheminer en toute sécurité. Les entreprises ont ainsi la possibilité de se tourner vers le FAI de leur choix pour leur connexion et réduire ainsi les coûts en évitant la location onéreuse de lignes dédiées. Par ailleurs, le VPN PPTP rend inutile l'ajout d'un client supplémentaire sur les ordinateurs des utilisateurs individuels puisque celui-ci est intégré dans Windows. Les entreprises bénéficient ainsi d'un coût et d'une complexité moindres.

Haute disponibilité VPN

Cyberoam propose un basculement automatique de la connectivité VPN pour les connexions IPSec et L2TP afin de garantir une connectivité VPN permanente sur les passerelles de FAI multiples. Les filiales et utilisateurs distants peuvent établir une connexion VPN alternative sur la seconde passerelle si le lien WAN utilisé est rompu, assurant ainsi la pérennité des activités et la mobilité des employés. Un groupe de connexions VPN avec des priorités de connexion définies permet enfin une gestion simple et efficace du basculement.

Antivirus au niveau de la passerelle

Protection antivirus puissante en temps réel

Cyberoam assure une protection au niveau de la passerelle contre les virus, vers et autres codes malicieux grâce à sa solution antivirus qui intercepte les menaces avant une attaque. L'inspection et le blocage du trafic HTTP, FTP, SMTP, POP3 et IMAP au niveau de la passerelle permet une défense puissante et coordonnée de la navigation Internet et de la messagerie. Un contrôle 24h/24 et 7j/7 garantit une réponse rapide en cas de nouveaux virus. Enfin, Cyberoam propose une zone de quarantaine accessible en permanence.

Protection actualisée

La solution antivirus de Cyberoam analyse les virus grâce à sa vaste base de données de signatures de virus régulièrement mise à jour, assurant ainsi une protection totale. L'antivirus Cyberoam prend en charge un grand nombre de formats de fichiers, y compris les pièces jointes protégées par mot de passe.

Antispam au niveau de la passerelle

Solution antispam intuitive et personnalisable

Défense en temps réel

La solution antispam de Cyberoam assure une protection en temps réel grâce à sa technologie RPD™ (détection des signatures récurrentes) dont les performances de détection de spams et de menaces restent inégalées. Cette technologie RPD™, indépendante du contenu, détecte et bloque les intrusions de nouveaux spams y compris les spams images, PDF et Excel, et enregistre un taux de faux positifs quasi-nul. Les entreprises sont ainsi efficacement protégées des menaces émanant des emails.

L'antispam Cyberoam offre une grande extensibilité et est capable d'analyser des messages de taille conséquente à un débit très rapide. Il élimine un grand nombre de tentatives de logiciels espions, phishing et publiciels et bloque les spams à caractère pornographique. En préservant les systèmes de messagerie de toute inondation de spams, il permet aux entreprises de jouir d'une meilleure productivité. Par ailleurs, l'antispam Cyberoam est en mesure de configurer des listes blanches et noires sur la base de l'identité utilisateur, ce qui facilite la gestion et les contrôles granulaires de la messagerie.

Détection précoce des intrusions

Avec sa technologie proactive de détection des virus, Cyberoam identifie les épidémies virales véhiculées par les emails dès qu'elles se présentent, dans un délai inférieur à une heure, permettant ainsi d'éviter la propagation du virus à des millions d'utilisateurs. Cyberoam parvient à ce résultat grâce à la mise en oeuvre d'une première ligne de défense essentielle, à savoir le blocage intuitif des emails suspects dès les premiers signes d'intrusion d'un virus.

Filtrage multicouches

Les politiques de contrôles granulaires de Cyberoam se basent sur le nom de l'expéditeur et du destinataire, l'adresse IP, l'en-tête mime et la taille des messages. Elles sont ainsi parfaitement adaptées aux besoins professionnels et aux exigences de conformité de l'entreprise. Cyberoam prend en charge l'ensemble des protocoles, à savoir SMTP, POP3 et IMAP, pour une protection complète. De plus, la technologie RPD™ permet une protection quels que soient le format et la langue utilisés dans les spams.

Options de flexibilité

L'antispam Cyberoam propose une configuration flexible grâce à des options permettant par exemple de délivrer le spam au destinataire, de le supprimer ou de le rediriger vers une adresse prédéfinie, comme celle d'un administrateur ou d'un chef de service.

*Commtouch Software Ltd.

Quelques statistiques - Menaces internes

- Les menaces internes représentent 50 % des problèmes de sécurité.
- Les menaces sur MI augmentent de 50 % par mois
- 1/3 des utilisateurs de messagerie instantanée a déjà reçu des spims/spams.
- 51% des cadres avouent consulter des sites non professionnels pendant leurs heures de travail
- Les pertes financières engendrées par l'accès non autorisé à des données et le vol d'informations confidentielles ont augmenté.

Source : CSO Metrics, Yankee group

Détection et prévention des intrusions - IDP

L'IDP de Cyberoam assure une protection contre les menaces en bloquant les attaques Internet avant qu'elles n'affectent le réseau. Le système de reporting et de politique unique basé sur l'identité de l'utilisateur permet une détection et une prévention des intrusions des plus performantes, réduisant considérablement le nombre de faux positifs. L'IDP de Cyberoam bloque les tentatives d'intrusions, les attaques par déni de service, la transmission de codes malicieux, les intrusions par portes dérobées et les menaces mixtes, sans pour autant influer sur les performances du réseau.

Protection complète

Grâce à une des plus vastes bases de données de signatures, l'IDP de Cyberoam détecte instantanément le trafic potentiellement malveillant en s' appuyant sur des politiques préétablies. Les entreprises disposent ainsi d'un système IDP intuitif et intelligent. Des analyses multiples, une détection dynamique et des politiques basées sur l'identité de chaque utilisateur plutôt que sur des stratégies globales permettent d'assurer une protection totale au niveau de la couche application et de la couche réseau.

Protection basée sur l'identité

Les stratégies de Cyberoam, basées sur l'identité de l'utilisateur, offrent une protection d'une extrême finesse, identifient les utilisateurs malveillants sur le réseau et alertent les administrateurs, permettant ainsi de prendre des contre-mesures en temps réel. Grâce à une parfaite visibilité de l'utilisation faite des applications par chaque utilisateur, les administrateurs peuvent facilement identifier les utilisateurs et les systèmes malveillants.

Signatures IDP personnalisées

L'IDP de Cyberoam prend en charge les signatures personnalisées afin de permettre aux entreprises de créer leurs propres signatures, leur assurant ainsi une protection en temps réel contre les nouvelles menaces et un haut degré de granularité. De plus, la base de données des signatures IDP inclut les signatures de proxy HTTP afin d'empêcher tout utilisateur de se dissimuler sur Internet par le biais d'un proxy ouvert.

Mises à jour disponibles en ligne

Les mises à jour sont disponibles en ligne afin de favoriser l'application des politiques aux failles de sécurité avant que celles-ci ne soient exploitées.

Filtrage de contenu

Une navigation non appropriée représente la principale source de menaces Internet

Base de données complète de sites classés

Grâce à son outil de catégorisation de sites Web, WebCat, Cyberoam assure un filtrage de contenu totalement fiable. Des millions de sites à travers le monde sont ainsi classés dans plus de 68 catégories et constituent une base de données complète et optimale, qui garantit la sécurité des mineurs en ligne et permet aux écoles et bibliothèques de se conformer aux exigences de la norme CIPA.

Contrôles granulaires

Cyberoam veut rompre définitivement avec les politiques globales basées sur l'attribution statique des adresses IP en se tournant vers une politique granulaire basée sur l'identité de l'utilisateur afin de pouvoir appliquer des stratégies spécifiques de navigation à chaque utilisateur, et ce, sur la totalité du réseau.

Les options de personnalisation et de flexibilité offertes par Cyberoam permettent aux entreprises de définir et d'appliquer des stratégies orientées application, groupe ou utilisateur selon le poste hiérarchique et /ou le département. Cyberoam peut également limiter l'accès à certains sites à certaines heures de la journée.

Trafic P2P-MI

La sécurité Internet offerte par Cyberoam va bien au-delà du trafic Web classique en incluant les messageries instantanées (Yahoo, MSN, Skype) et les échanges en peer-to-peer. La visibilité totale et les contrôles axés sur les utilisateurs assurent la flexibilité nécessaire pour s'adapter aux applications dynamiques et faire face aux différentes menaces.

Gestion de la bande passante

Une bonne gestion de la bande passante est essentielle pour permettre à l'entreprise une productivité optimale

L'interface graphique utilisateur proposée par Cyberoam est facile d'utilisation et offre de nombreuses options de personnalisation pour l'allocation de la bande passante, avec par exemple la possibilité de définir des politiques par groupes, sous-groupes ou départements.

Une bande passante jamais saturée

Cyberoam dispose d'un outil puissant de productivité qui permet de réduire l'engorgement de la bande passante grâce à une maîtrise de la bande allouée aux applications non vitales et à la navigation Internet à caractère non professionnel comme le téléchargement audiovisuel, les jeux et les publicités.

Applications vitales privilégiées

La bande passante peut être réservée ou étendue en temps réel pour les applications sensibles (ERP, etc.). Les politiques de Cyberoam permettent d'allouer la bande selon l'urgence et l'importance de l'application concernée.

Répartition de la bande passante

La solution Cyberoam est unique en ce qu'elle permet aux administrateurs de répartir et d'ajuster la bande sur une base temps pour les différents utilisateurs et groupes hôtes, fluidifiant ainsi le trafic tout au long de la journée. La bande passante est ainsi allouée avec précision en fonction du temps d'accès prédéfini et des tendances de navigation, avec un transfert défini des données.

Gestion intelligente des ressources

Les rapports détaillés concernant l'utilisation de la bande passante fournissent aux entreprises les éléments-clés pour Gestion intelligente des ressources de bande et optimiser les ressources.

Gestion des liens multiples

Une utilisation optimale des liens multiples pour une connexion infaillible et des économies non négligeables

L'appliance Cyberoam intègre également un gestionnaire multiliens qui contrôle le trafic des liens WANS multiples. Ce dispositif permet de gérer efficacement le trafic, d'optimiser les liens et d'assurer une connexion très haut débit, tout en optimisant le retour sur investissement.

Répartition de charge

Le gestionnaire multiliens permet une fiabilité optimale de la connexion de l'entreprise en gérant le trafic Internet sortant sur les liens FAI multiples. La répartition de charge du trafic se fait selon la technique du Round Robin pondéré pour une gestion dynamique du trafic.

Secours multiliens

Le gestionnaire multiliens contrôle la disponibilité des liens de toutes les connexions WAN et redirige le trafic d'un lien rompu vers un lien opérationnel. La connectivité est assurée en permanence et les activités professionnelles peuvent se poursuivre sans problème.

Reporting intégré

Cyberoam propose des rapports d'analyse sur le trafic afin d'identifier les modifications des tendances de navigation Internet

Rapports d'analyse complets

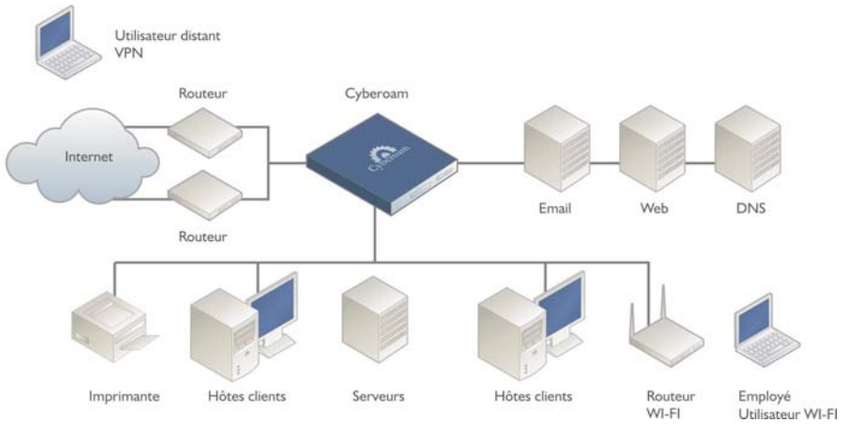
Ces rapports proposés par Cyberoam permettent aux responsables informatiques d'identifier les modifications dans les schémas d'utilisation d'Internet et d'adapter les politiques de l'entreprise en conséquence. La productivité et la sécurité de l'entreprise sont ainsi optimisées.

Contrôle du réseau et des applications

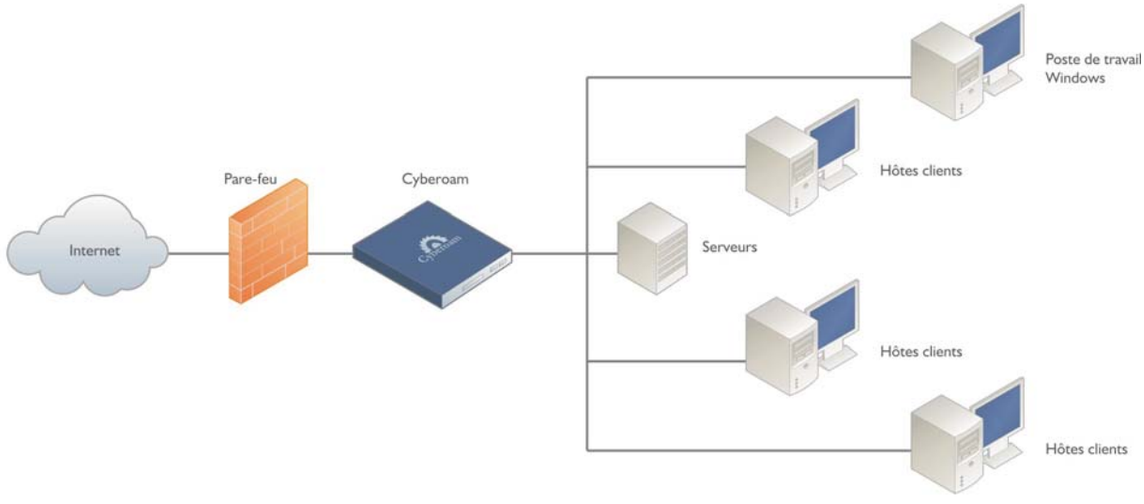
Les rapports de détection du trafic de Cyberoam fournissent des informations précises sur les données transférées, les applications utilisées, etc. Tout trafic suspect est ainsi mis en exergue et les administrateurs peuvent prendre les contre-mesures immédiates qui s'imposent, évitant ainsi la saturation du réseau et la propagation d'une attaque.

Scénarios de déploiement de Cyberoam

Mode passerelle



Mode pont
avec pare-feu existant



eLITE CORE®
TECHNOLOGIES LTD.

www.elitecore.com I www.cyberoam.com

Amérique du Nord
Cyberoam
Elitecore Technologies
29 Water Street
Newburyport, MA 01950
USA
Tél : +1-978-465-8400
Fax : +1-978-293-0200

Inde
Elitecore Technologies
904, Silicon Tower,
B/h Pariseema Building,
Off C.G.Road,
Ahmedabad-380 006. INDIA.
Tél : +91-79-66065606
Fax : +91-79-26407640

Contact
info@cyberoam.com

Version:1.0-9501-Août.07