



CYBEROAM

Une application de sécurité basée sur l'identité

Cyberoam est une filiale de la société d'origine indienne Elitecore Technologies qui développe principalement des appliances UTM. L'ajout de la gestion de l'identité des utilisateurs permet ainsi de filtrer les différents flux réseaux de façon plus poussée afin de renforcer la sécurité globale. Fini les politiques de filtrage globales au niveau de l'entreprise, maintenant le pare feu est capable de gérer le profil professionnel de chaque utilisateur.

Quand vous achetez un boîtier Cyberoam vous aurez de base les fonctions Firewall, VPN, SSL VPN, gestion de bande passante, gestion des liens multiples, reporting intégré, service antispam basique. En option vous trouverez les passerelles antivirus, antispam, le filtrage web et applicatif, le système de prévention des intrusions, et un support « 24/7 ».

Prise en main

Comme tout boîtier de ce type, la première chose à faire est de configurer la partie réseau (choix du mode Gateway ou Bridge), adresses IP pour accéder aux différents segments de votre infrastructure (LAN, WAN, DMZ, VLAN), ceci s'effectuant en lançant le seul assistant de configuration.

Si vous optez pour l'installation en mode Bridge, vous vous privez d'un bon nombre des fonctions du boîtier, mieux vaut utiliser le mode Gateway pour en profiter pleinement. Vous

pouvez le configurer par l'accès console ou au travers de l'interface web. Celle-ci permet de tout administrer. Une fois connecté, vous arriverez sur le tableau de bord qui récapitule les principaux paramètres à contrôler. Première action à entreprendre, modifier les règles par défaut qui autorisent tout. Vous pourrez ainsi avoir le temps nécessaire pour configurer le reste.

Étape suivante, utiliser l'authentification des utilisateurs en se raccordant à l'annuaire de l'entreprise (LDAP, AD, Radius). Afin de bien comprendre les possibilités offertes, il est fortement conseillé aux futurs administrateurs de la solution de se documenter sur le site de Cyberoam à travers la base de connaissance (KnowledgeBase, ou KB). Cette KB est un des seuls endroits où il est fort heureusement possible de trouver des procédures de configuration adaptées à ses besoins. Certaines

informations utiles s'y trouvent pour mieux comprendre et configurer son intégration avec son annuaire. Il est ainsi possible de se connecter en mode SSO (Single Sign On, authentification unique) pour que, à chaque fois que l'on se connecte sur son poste client pour ouvrir une session de travail, on bénéficie en même temps des fonctions de sécurité configurées dans le Cyberoam.

Pour une meilleure gestion des utilisateurs de votre domaine, il est aussi recommandé de créer dans votre AD de nouveaux groupes qui seront spécifiquement utilisés par Cyberoam. Ceci pour une bonne raison : à chaque groupe on peut y associer des politiques de sécurité différentes, politiques qui peuvent ne pas être en adéquation avec votre gestion de groupes existante. Il existe toujours des utilisateurs dans un groupe (Commercial, Direction, Comptabilité, ...) qui nécessitent des droits d'accès différents.

Les autres moyens sécurisés de se connecter sont d'utiliser le portail captif (SSL VPN) ou d'installer un outil client.

Vous voici en mesure de faire connaissance avec les autres fonctions. Même si, avant, il faudra bien penser à s'enregistrer sur le site de Cyberoam pour pouvoir activer sa licence et utiliser toutes les options commandées.

Si votre entreprise n'utilise pas d'annuaire, vous aurez toujours le moyen d'utiliser une base de comptes locale au Cyberoam.

Pour ceux qui ont du mal avec l'anglais, il est possible de changer la langue de l'interface d'administration, vers le français, indiqué « French-Beta » – serait-ce une petite blague des développeurs ?

Fonctions

Le pare feu est certifié ICSA et ajoute, comme déjà évoqué, une gestion de l'identité des utilisateurs. La haute disponibilité est possible entre boîtiers avec un système de routage dynamique.

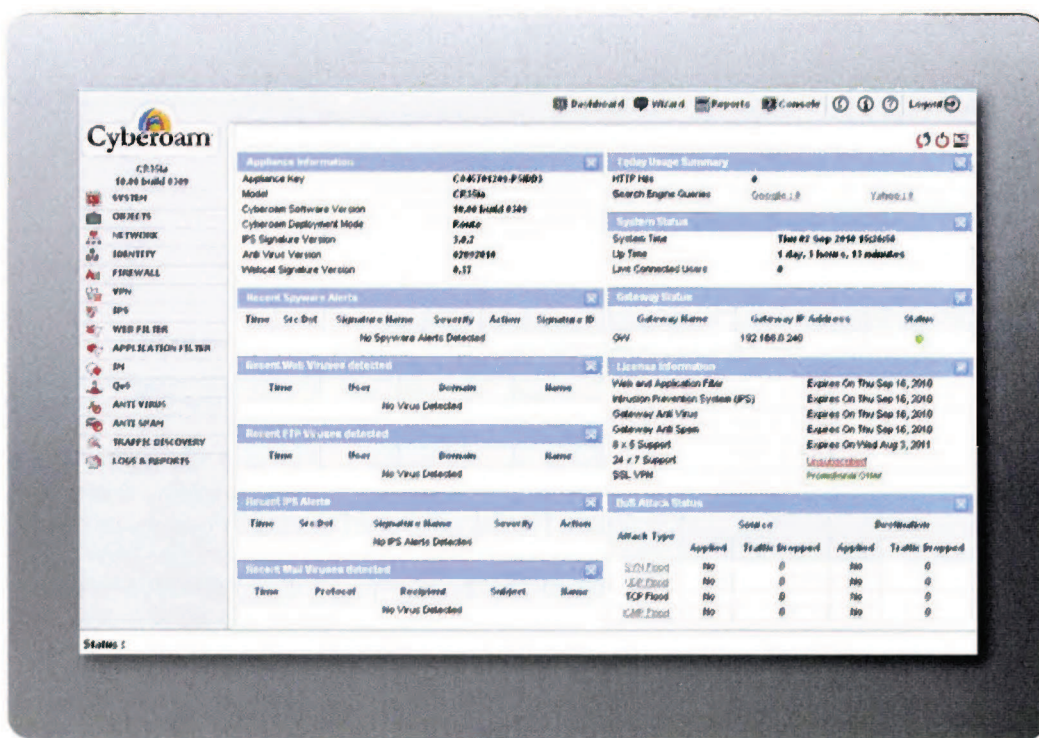
- Le VPN intègre la prise en charge de l'IPSec, L2TP, PPTP, SSL VPN. Il possède aussi une fonction de bascule VPN. Autre avantage, le boîtier génère lui-même les fichiers nécessaires à la configuration de client IPSec et SSL VPN, ce qui simplifie grandement la mise en place de ces solutions qui rebutent habituellement pas mal de monde.
- La gestion de la bande passante est aussi améliorée, grâce à l'authentification de l'utilisateur, on peut maintenant définir des politiques pour chaque application critique ou utilisateur privilégié.
- Si vous possédez plusieurs liens d'accès vers un ou plusieurs FAI, vous aurez la possibilité de répartir vos différents flux selon vos besoins, en définissant soit une répartition de charge du type round robin et/ou de routage des utilisateurs et applications en fonction de politiques basées sur l'identité.
- En ce qui concerne l'outil de reporting, il est intégré au boîtier et utilise le disque dur intégré dans la plupart des boîtiers pour stocker et gérer l'information. L'accès au module de reporting se fait dans une fenêtre/onglet





web indépendante de celle de la gestion du boîtier. Il est ainsi possible de générer des rapports personnalisés et automatisables. Vous pouvez savoir exactement qui fait quoi et en tirer des tendances. Là encore, l'analyse peut être plus ou moins poussée pour aller jusqu'au niveau de l'utilisateur afin de connaître son utilisation du réseau, sur quels sites il se connecte, combien de données il télécharge, etc. Cela permet de s'adapter très rapidement et de se conformer aux règles et effectuer des rapports d'audit plus facilement. Vous exportez les rapports en format Excel ou PDF.

- Le moteur utilisé pour la passerelle antivirus est celui de Kaspersky, celui du module antispam de Commtouch, deux moteurs réputés sur leur marché respectif. Si vous utilisez en plus le système de prévention d'intrusion, vous obtenez une solution complète de sécurité qui, pour chaque point, permet un niveau de granularité allant jusqu'à l'utilisateur. Même les systèmes de messagerie instantanée, comme MSN ou Yahoo Messenger, peuvent être filtrés. Vous pouvez, par exemple, décider de priver un ou plusieurs utilisateurs de la partie webcam, sinon les y autoriser à certaines heures de la journée.
- Enfin, parlons des fonctions qui s'occupent de filtrer les accès web et applicatif. Il est possible de filtrer l'accès à certains sites web, en utilisant soit des listes blanches et noires ou la gestion par Cyberoam de catégories de sites déjà répertoriés. Ce dernier moyen est très pratique car plus vous naviguez,



↑ Cyberoam offre un bon système de reporting qui permet vraiment de tout contrôler.

plus vous enrichissez le système. Chaque URL inconnue du système peut être envoyée chez Cyberoam, à des fins d'analyse et de classement dans une catégorie. Plus vous surfez, plus vous améliorez le filtrage. Pour les applications, vous pouvez décider de bloquer tout ce qui est P2P, les *anonymous proxy*, Skype et consorts, certains protocoles Internet ou services réseau, le streaming de media, etc. Ce filtrage est

bien sur applicable en fonction de l'identité.

Remarque

Attention, l'authentification de l'utilisateur par la partie Firewall, ne doit pas être utilisé quand vous vous connectez à partir d'Internet. Comme l'utilisateur est associé à l'adresse IP qu'il utilise, une fois authentifié, un pirate pourrait récupérer votre adresse et l'utiliser pour accéder à votre réseau interne. Ce système d'authentification de l'utilisateur est uniquement prévu pour sécuriser votre LAN, ou alors en utilisant une connexion sécurisée par VPN.

En pratique

En pratique

Mise en place d'un VPN PPTP

Beaucoup de travailleurs nomades utilisent ce moyen pour se connecter à leurs entreprises de manière sécurisée. L'avantage est de trouver sous Windows un client en standard pour se connecter. Mes premières tentatives ont échoué : pas moyen de trouver dans les documentations fournies avec le boîtier de réponses, et ce, même en téléchargeant à partir du site de Cyberoam un document destiné à toute la partie VPN ! En contactant le distributeur, on m'a conseillé de me connecter sur la KB du site, et là, en effet, une procédure est

- Un nombre de fonctionnalités important, au détriment cependant de la facilité de prise en main.
- Évidemment, la couche d'authentification de l'utilisateur, qui est un plus indéfectible qui bénéficie à l'ensemble des fonctions.
- Des tarifs compétitifs si on prend un des bundles d'option.
- Un bon système de reporting qui permet vraiment de tout contrôler et de s'adapter aux futurs et nouveaux usages du Net.
- L'interface en français.

- La documentation en anglais qui manque cruellement de procédures de configuration et qui se contente de descriptions de l'interface.
- La prise en main nécessite un bon transfert de compétence de la part du revendeur – du fait de son nombre de fonctionnalités étendues.



Cyberoam

SSL VPN User Portal

Help Logout

Welcome, admin!

SSL VPN Client (Tunnel access mode)

Web access mode

Enter URL

Configure of Bookmarks

No.	Bookmarks Name	Bookmarks URL	Format
1	SSLVPN	http://192.168.0.230/	HTTPS
2	OST	http://192.168.0.20000/	HTTP

Application access mode

Configure of Bookmarks

No.	Bookmarks Name	Bookmarks URL	Format
1	RDP	http://192.168.18.162/	RDP

Paramétrage d'un accès à distance à un poste client en RDP.

donnée. Et je comprends enfin pourquoi j'avais des difficultés. Les boîtiers ne gèrent pas, pour le moment – un nouveau firmware arrive bientôt – les protocoles MS-CHAP et MS-CHAP2. Il suffit donc de configurer le client PPTP en mode PAP ou CHAP.

Je me suis donc demandé s'il n'existait pas un moyen plus pratique de se connecter à distance à son entreprise et me suis intéressé au SSL VPN.

Mise en place du portail web SSL VPN

Cette fois ci, je me suis directement connecté au site de la KB pour trouver la procédure de configuration.

Seul bémol, la procédure porte sur un firmware en 9.x et non en 10, néan-

moins cela reste facilement transposable. Pour une première configuration, le document est le bienvenu, et une fois la logique assimilée, il n'y a pas de souci pour recommencer sans procédure sous les yeux.

J'ai donc configuré la partie Certificat, puis les liens qui permettront à partir du portail de se connecter à un certain nombre de ressources, dont une application web interne et un accès à distance à un poste client en RDP.

J'ai juste rencontré un problème, non pas avec Cyberoam, mais avec mon routeur, pour me permettre de transférer le port réseau à utiliser afin d'accéder au portail.

Une fois résolu, tout fonctionne au



Il est recommandé de créer dans votre AD de nouveaux groupes qui seront spécifiquement utilisés par Cyberoam.

mieux. Bien faire attention à partir d'un poste Windows 7 de démarrer son navigateur web en mode administrateur, afin de pouvoir ouvrir les liens en mode application, comme l'accès RDP. De plus, à partir de ce portail, en saisissant dans le champ URL une adresse internet, vous pouvez naviguer en toute sécurité à partir du réseau sur lequel vous vous connectez (Wifi à l'hôtel, cybercafé).

Conseil

Pour la première installation, mieux vaut passer par un prestataire qui puisse effectuer un transfert de compétences et indiquer où l'on peut trouver l'aide adéquate par la suite. ■

Précision

Dans le dernier numéro de *L'Informaticien* (n° 83, daté septembre 2010), l'article sur le produit *Edenwall* peut introduire une confusion entre le projet *Open Source Nufirewall* et le nom du produit *d'Edenwall* que nous avons testé, *Edenwall Security Appliance*.

Pour en savoir plus

Liens utiles:

www.cyberoam.com/fr

Distributeurs:

www.eiptec.com

www.hermitagesolutions.com/produits/cyberoam/