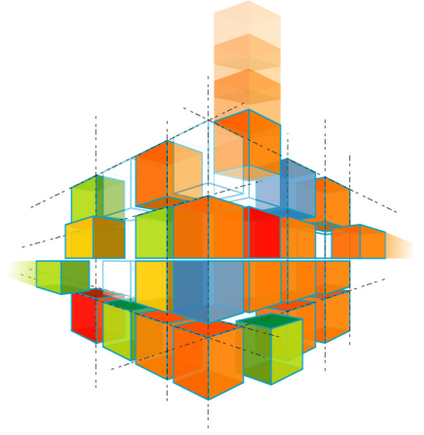
LIVRE BLANC

MAI 2006

UTM : UNE FORTERESSE POUR LA PME

ARKOON NETWORK SECURITY

Il est temps de passer d'une protection périmétrique à une protection panoramique, plus complète. L'UTM est le seul équipement de sécurité multifonction offrant cette faculté. Il apporte à l'entreprise étendue une protection globale, évolutive et économique de ses échanges numériques.



ADAPTIVE SECURITY

AMC SSL360 FAST360 Security BOX

L'UTM : LA SOLUTION TOUT-EN-UN, COHÉRENTE ET ÉCONOMIQUE

L'ATTENTE DE NOMBREUSES PME EN MATIÈRE DE SÉCURITÉ SE RÉSUME À UNE SOLUTION DE SÉCURITÉ GLOBALE ET SIMPLIFIÉE. L'UTM SÉCURISE TOUS LES ACCÈS AU RÉSEAU D'ENTREPRISE.

UNE RÉPONSE COMPLÈTE AUX VULNÉRABILITÉS

L'A210 d'Arkoon procure toutes les parades nécessaires aux PME.

Le défi actuel du système d'informations consiste à procurer des données et des traitements à la fois sécurisés et disponibles. Tout en offrant une pérennité aux investissements de la PME, l'UTM assure la prévention et la protection de ses ressources techniques. Depuis dix ans, la PME accumule des logiciels et des passerelles de sécurité. Cette inflation d'outils provoque une avalanche de journaux d'alertes, trop rarement consultés car complexes à interpréter. L'UTM apporte une protection intelligente en phase avec l'infrastructure actuelle. L'équipement tout en un renforce les segments locaux du siège, mais aussi les liaisons étendues vers les agences et vers les partenaires, ainsi que les serveurs stratégiques.

L'installation, le paramétrage, l'actualisation et l'administration de plusieurs outils de sécurité (pare-feu, antivirus, antispam, passerelle VPN...) finit par coûter cher à l'entreprise. L'UTM réunit toutes les fonctions de sécurité dans un seul boîtier économique et évolutif. Une corrélation d'événements lui permet de réagir avec discernement aux malveillances. Chaque réaction s'effectue de façon discrète et automatique le plus souvent. En outre, l'administration unifiée accélère le paramétrage des pare-feux, de l'antivirus, de la prévention d'intrusions, des règles de filtrage...

Bien sûr, les menaces en réseau vont continuer leur évolution avec l'élargissement du périmètre du réseau. C'est pourquoi les parades de l'UTM sont évolutives : combinées, elles protègent les ressources clés et l'ensemble des investissements technologiques de l'entreprise. Une dépollution efficace de la messagerie devient enfin possible grâce à l'antispam intégré. Avec l'UTM, tous les services s'avèrent plus disponibles, plus intègres et plus conformes. La sécurisation du réseau entre enfin au service de l'entreprise.

LES 10 VULNÉRABILITÉS PRISES EN COMPTE PAR L'UTM

MENACES	CIBLES	IMPACTS	PARADES	PRINCIPES
Ver, virus, cheval de Troie, scripts malicieux...	Serveurs, Postes de travail	C P B	Antivirus, antispyware	Analyse des fichiers via bases de signatures
Spam	Messagerie électronique	C P B	Antispam client/serveur	Filtrage de messages par mots clés ou algorithmes statistiques
Ecoute du réseau, inspection de trafic	Infrastructure, Serveurs, Postes de travail	C P B	Pare-feu, chiffrement, patchs systèmes, audit	Filtrage, cryptage, encapsulation de flux
Usurpation d'identité	Infrastructure, Serveurs, Postes de travail	C P B	Changements réguliers des mots de passe, authentification forte, pare-feu applicatif	Filtrage d'accès ou de paquets, politique d'administration, examen des journaux
Intrusions, attaques (buffer overflow, force brute...)	Infrastructure, Serveurs, Postes de travail	C P B	Parefeu, prévention d'intrusions, patchs systèmes, fermeture des services inutiles	Reconnaissance d'attaques, vérifications comportementales
Détournement de services ToIP ou P2P	Infrastructure, Serveurs, Postes de travail	C P B	Blocage des services inutiles, chiffrement, patchs systèmes	Configuration d'équipements et correctifs
Dénis de services (distribués)	Infrastructure, Serveurs	C P B	Patchs systèmes	Adjonction ou correction corrigeant la vulnérabilité
Vagabondage Web	Postes de travail	C P B	Filtrage d'URL	Filtrage par mots clés
Ingénierie sociale	Infrastructure, Serveurs, Postes de travail	C P B	Comportement des utilisateurs	Charte de sécurité et formations
Sentiment de sécurité une fois les protections de base installées	Infrastructure, Serveurs, Postes de travail	C P B	Mise à jour des parades, tests d'intrusions	Politique d'administration de la sécurité, examen des journaux, veille sur les dernières menaces...

LÉGENDES : C = CONFIDENTIALITÉ • P = PRODUCTIVITÉ • B = BANDE PASSANTE • ROUGE = IMPACT FORT • ORANGE = IMPACT MOYEN • VERT = IMPACT NUL

LA SÉCURITÉ AU CŒUR DU RÉSEAU

FACE À DES MENACES DE PLUS EN PLUS COMPLEXES, LES BOÎTIERS TOUT-EN-UN REPRÉSENTENT LA MEILLEURE APPROCHE POUR LES PME.

L'entreprise n'est pas et n'a jamais été un lieu sûr. Qu'elles viennent de l'intérieur ou de l'extérieur, les menaces sont bien réelles. D'autant plus que le réseau se complexifie. Récemment, le développement des outils favorisant la mobilité ont encore renforcé le risque : le téléphone mobile des équipes commerciales, ou l'assistant numérique des responsables de production, les ordinateurs portables... autant de terminaux qui rendent le réseau d'information de l'entreprise vulnérable.

De plus, à une époque où la convergence des données et de la voix est bel et bien engagée, avec l'essor de la téléphonie sur IP (ToIP), l'enjeu sécuritaire devient plus que crucial. L'objectif des acteurs de la sécurité est donc de proposer une gamme de solutions capables de gérer cette complexité, en assurant une protection à plusieurs niveaux. La tâche est difficile : virus, vers profitent d'emails pour s'infiltrer sur les machines, pendant que les pirates tentent d'accéder aux serveurs et routeurs en utilisant des scripts, des backdoors (portes dérobées) ou des vulnérabilités de l'infrastructure. Pire, depuis peu, les attaques se combinent entre elles et deviennent encore plus difficiles à combattre.

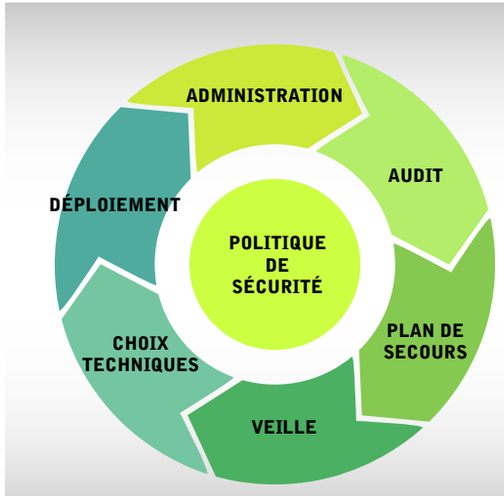
Dans les faits, le réseau est désormais au cœur de la politique de sécurité. La meilleure méthode pour répondre aux attaques reste de combiner réseau et logiciels, une approche qu'a bien évidemment choisi Arkoon. Des boîtiers matériels, baptisés UTM (Universal Threat Management, ou Gestion de Menaces Unifiée) savent combiner plusieurs fonctionnalités, à savoir services de sécurité, services de routage et qualité de service, afin de répondre à ces nouveaux besoins. Simples à administrer et peu coûteux, ils sont parfaits pour les entreprises de taille moyenne. Ces boîtiers agissent à l'entrée du réseau et ne nécessitent plus d'installer les logiciels sur les postes clients, comme les antivirus très fréquemment.

Arkoon propose une gamme avec une base technologique (FAST) au cœur de son boîtier capable de fédérer plusieurs outils issus d'éditeurs différents. Ainsi, ces solutions, très complètes, intègrent à la fois un coupe-feu applicatif en temps réel (couche 3 à 7), la prévention et la détection d'intrusion, le filtrage des contenus web, de messagerie et FTP (antivirus, antispyware, antispam, heuristique, filtrage URL, filtrage web), la fonction de concentrateur VPN IPSec, l'authentification des utilisateurs, la gestion de la bande passante, le filtrage par VLAN et le routage dynamique.

L'UTM SIMPLIFIE LA SÉCURITÉ ET BAISSE LES COÛTS

Pour couvrir leurs besoins en sécurité, les entreprises installent souvent plusieurs boîtiers, avec des variations importantes au niveau de l'administration. En centralisant toutes les fonctionnalités nécessaires dans un seul boîtier, l'UTM simplifie la sécurité : l'administration se fait depuis un point unique, et les coûts sont considérablement réduits. L'originalité de ce type de boîtiers réside aussi dans le fait que l'on peut combiner plusieurs technologies de sécurité entre elles. De nos jours, les attaques sont complexes : un virus peut profiter d'un spam pour se propager, par exemple. Il y a une véritable convergence des menaces de sécurité. Ainsi, il devient nécessaire d'intégrer de plus en plus de fonctions harmonisées entre elles. Arkoon a choisi justement une approche spécialiste, par le biais de partenariats avec des éditeurs de la sécurité, plutôt qu'une approche généraliste beaucoup moins efficace. Le boîtier UTM ne sépare plus les fonctions, chaque moteur est complémentaire. Notre technologie au cœur du boîtier est capable par exemple de corréler plusieurs outils, et de rendre toutes les fonctionnalités cohérentes entre elles, avec une analyse fine des attaques, réduisant les risques de faux positifs.

DAVID DUPRÉ
RESPONSABLE DU MARKETING PRODUITS D'ARKOON

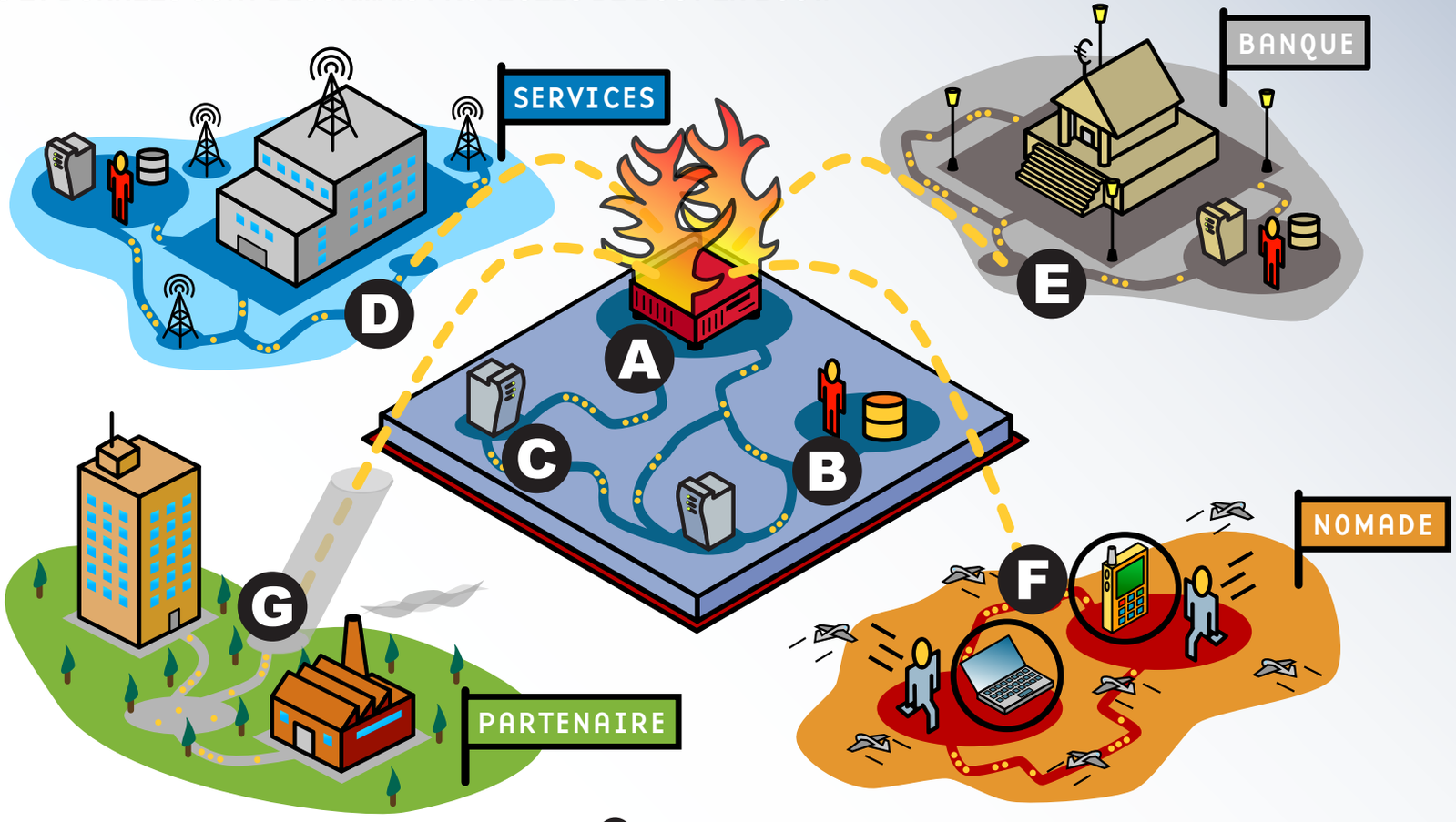


UN CYCLE DE VIE À GÉRER

A chacun selon ses règles et sa politique de sécurité. Pour contrer les malveillances du réseau, internes et externes, il convient de suivre des boucles d'amélioration et de gérer le cycle de vie des outils mis en place. L'UTM apporte une supervision et des mises à jour unifiées qui facilitent la gestion du cycle de vie de la sécurité et de la qualité des services réseau.

UNE PROTECTION RENFORCÉE POUR L'ENTREPRISE ÉTENDUE

L'UTM PERMET DE PASSER D'UNE PROTECTION PÉRIMÉTRIQUE À UNE PROTECTION PANORAMIQUE. TRANSACTIONS ET DONNÉES SONT DÉSORMAIS PROTÉGÉES DE BOUT EN BOUT.



A L'UTM filtre en temps réel les codes malveillants et assure la prévention d'intrusions

B L'administrateur peut poursuivre ses projets sans être accaparé par la surveillance des vulnérabilités

C Les serveurs sont débarassés des passerelles de sécurité, gourmandes en ressources CPU et en mémoire

D L'UTM protège les échanges avec les prestataires de services

E Virements bancaires et télédéclarations aux administrations gagnent des transactions sécurisées

F Sur le terrain, cadres et techniciens reçoivent et envoient des informations chiffées, sans délai

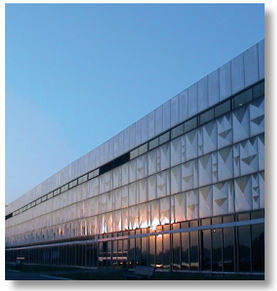
G Lorsque l'entreprise agit pour le compte d'un donneur d'ordres, elle bâtit un tunnel sécurisé (VPN IPSEC ou SSL)

L'UTM ARKOON SÉCURISE LES TROIS SITES DU CENTRE DE CONGRÈS ET EXPOSITION DE BORDEAUX

PLUS DE 75 FLUX IP SE CROISENT SUR LES TROIS SITES DE CEB À BORDEAUX. POUR SUPERVISER LES ÉCHANGES, BLOQUER LES CODES MALVEILLANTS ET DONNER L'ALERTE, L'UTM A210 D'ARKOON APPORTE UN PARAMÉTRAGE SIMPLE ET RICHE À LA FOIS.

PHILIPPE SINET
Directeur du Système d'informations de CEB.

Le CEB tisse une vingtaine de réseaux locaux virtuels entre trois sites distants de plus de 2 kilomètres : le Parc des Expositions, le Palais des Congrès et le Hangar 14. Ces trois sites totalisent plus d'un millier de prises Ethernet, toutes potentiellement irriguées par le réseau Internet à haut débit, depuis l'an 2000 : « Nous avons remis à niveau nos commutateurs Ethernet 100 Mbps, mais un raz de marée de spams nous a démontré, en 2003, que les solutions de sécurité intégrées aux environnements serveurs de Microsoft étaient insuffisantes », retrace Philippe Sinet, le directeur des systèmes d'informations de CEB. D'où l'adoption d'une méthode plus évoluée de marquage des flux et des e-mails. L'analyse des échanges informatiques s'avère beaucoup plus fine à présent. La solution retenue - l'UTM A210 d'Arkoon - précise clairement les flux bloqués en entrée, qu'ils émanent d'une source suspecte ou bien présentent des requêtes non conformes.



Menée jusqu'aux applications (niveau 7) grâce à une sonde Sécuralis, l'analyse des flux réseaux procure une supervision globale de tout ce qui passe sur le réseau informatique. Une approche capitale lorsque l'entreprise partage une partie de sa bande passante avec ses clients, comme lors des congrès. Il s'agit alors de protéger l'ensemble des VLAN au travers de règles toujours simples. CEB bloque tout ce qui est illicite et non prévu contractuellement : l'accès aux sites de hackers, les contenus violents, le téléchargement d'égal à égal, les Web-TV, les spam, vers, spyware, virus...

« L'UTM Arkoon apporte l'analyse et le contrôle permanent. Cela nous permet de respecter la loi et d'empêcher des actions répréhensibles du personnel ou même d'utilisateurs temporaires ». En parallèle, une suite antivirus est conservée pour croiser les filtres et rendre le réseau privé le plus étanche possible aux codes malveillants. Les temps de réponse des utilisateurs n'en souffrent même pas : « le boîtier Arkoon a remplacé un proxy serveur placé en DMZ, un PC vieillissant qui provoquait des allers-retours avec l'ancien pare-feu. En fait, nos temps de >>> réponse Internet ont accéléré depuis », note Philippe Sinet. En outre, l'UTM a détecté certaines anomalies et permis de réagir immédiatement : « Nous savons non seulement qu'il y a une attaque toutes les 30 minutes, mais aussi s'il s'agit de simples curieux ou bien de tentatives plus sérieuses de piratage ». En exportant les traces de ces attaques, l'entreprise peut déposer plainte auprès des autorités compétentes.

La surveillance des flux devient nécessaire à mesure que le nombre d'applications croît : « Nous comptons plus de 75 applications, dont le progiciel de gestion intégré et l'outil de gestion de la relation client. L'administration unifiée d'Arkoon nous aide à nous y retrouver facilement. En comparaison, l'interface d'autres équipementiers s'avère peu exploitable et les outils de supervision spécialisés coûtent trop cher pour une PME ». Remplacer toutes les fonctionnalités de l'UTM mises en oeuvre à Bordeaux exigerait quatre produits de sécurité distincts et priverait la direction informatique d'une console unifiée très pratique au quotidien.

Les quatre pattes réseau de l'UTM Arkoon permettent de gérer les segments locaux du site (jusqu'à 150 utilisateurs en fonction des salons et congrès) et de disposer de plusieurs fournisseurs d'accès au réseau Internet : « les boîtiers d'équilibre de charge entre plusieurs ISP sont souvent chers et sophistiqués. Cela permet de disposer d'une puissance temporaire en plus avec une bascule automatique et une répartition suivant nos règles de qualification. Par exemple, les VLAN 4, 5 et 6 utiliseront un accès ISP et une partie de la bande passante d'un second accès WAN ».

UN SEUL CENTRE DE CONTRÔLE AVEC L'UTM

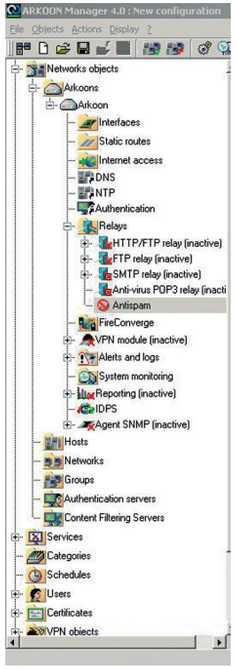
GÉRER TOUTES LES FONCTIONS DE L'UTM À PARTIR D'UNE MÊME INTERFACE D'ADMINISTRATION DEVIENT UN SÉRIEUX ATOUT POUR GAGNER DU TEMPS ET RÉDUIRE LES COÛTS D'EXPLOITATION DE L'INFORMATIQUE.

Une approche traditionnelle de la sécurité informatique consiste à intervenir en mode pompier, c'est à dire à éteindre le feu lorsqu'il devient trop vif. Les deux foyers d'infection privilégiés des hackers restent les serveurs Web et les serveurs de messagerie électronique. L'entreprise déploie donc, lorsqu'elle suit cette stratégie, plusieurs solutions les unes après les autres, en piochant dans les catalogues de différents fournisseurs. Cette approche requiert un budget conséquent pour filtrer successivement les virus, le spam, les spywares, contrer le phishing et les dénis de services...

Il faut aussi prévoir des tests, une formation pour chaque outil puis déceler les services compatibles avant de les déployer sur les plates-formes présentes dans l'entreprise. La gestion des services hétérogènes de sécurité au travers de leurs propres consoles s'avère contraignante et dévoreuse de temps.

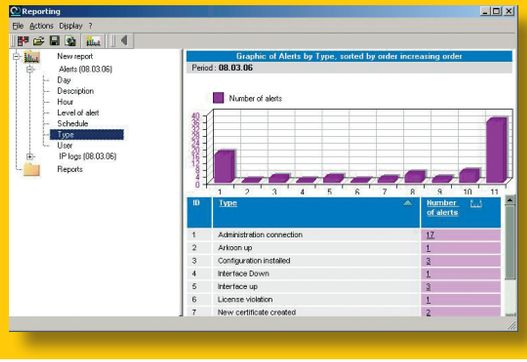
Le boîtier UTM procure, pour sa part, un centre de contrôle unifié. Ce centre permet de régler tout ce qui entre et sort du réseau. Une seule interface cohérente suffit à paramétrer l'ensemble des fonctions de sécurité de l'entreprise. Le périmètre du réseau sécurisé évolue-t-il car l'entreprise change de distributeur, de fournisseur ou déploie des terminaux mobiles sur le terrain ? Inutile de tout reconsidérer. Il suffit de paramétrer les accès distants via la passerelle VPN intégrée, les règles de sécurité déjà implémentées seront adaptées automatiquement. Quand bien même il faudrait ajouter de nouvelles règles, c'est une opération simple, rapide et économique. Les fonctions d'alertes et de reporting sont corrélées dans le boîtier de sécurité multifonction. Du coup, l'administrateur du réseau reçoit une seule alerte pour un même problème. Il n'a pas besoin de consulter de volumineux journaux pour comprendre et corriger chaque problème.

Lorsqu'on doit sécuriser les échanges entre plusieurs sites, les performances de l'UTM s'avèrent essentielles. Le boîtier tout-en-un peut chiffrer les flux tout en assurant les fonctions de coupe-feu, de prévention d'intrusions et de filtrage (URL, antivirus, applicatif...). Sa mise en oeuvre en environnement multisite réduit le nombre d'équipements dédiés ainsi que la consommation d'énergie. L'adressage est également simplifié. En outre, toutes les règles sont gérées de façon centrale, ce qui évite de dépêcher des techniciens dans chaque bureau. Les bases de signatures antivirales et les bases d'attaques sont regroupées ce qui offre des mises à jour plus simples et plus rapides. Outre un avantage économique, l'UTM améliore donc les processus de sécurité de l'entreprise.



Tous les objets supervisés par Arkoon Manager sont accessibles en un clic. Cela permet d'intégrer les règles de sécurité propres à l'entreprise plus rapidement qu'au travers des interfaces d'administration de chaque produit : passerelle VPN, antivirus, antispam, prévention d'intrusions, filtrage d'URL...

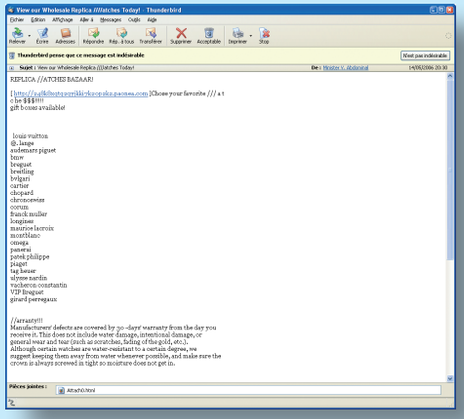
ARKOON MONITORING APPORTE UNE SUPERVISION COHERENTE



La technologie brevetée FAST (Fast Applicative Shield Technology) regroupe toutes les fonctions de sécurité essentielles à la PME. Une supervision cohérente devient possible à partir d'une seule et même console. Arkoon Monitoring procure à l'administrateur une interface complète pour le diagnostic, l'évolution et la surveillance du boîtier multifonction. Toutes les interfaces réseaux deviennent rapidement accessibles. L'administrateur peut remonter dans le temps pour comparer le nombre et la criticité des alertes quotidiennes rapportées par l'UTM. La consultation des messages et des journaux facilite le paramétrage et l'instauration de nouvelles règles de filtrage. Enfin, la visualisation des rapports prédéfinis simplifie les tâches de supervision.

GLOSSAIRE DE LA SÉCURITÉ

Antispam : Logiciel de sécurité qui filtre les emails parasites (spam) envoyés par des expéditeurs inconnus.



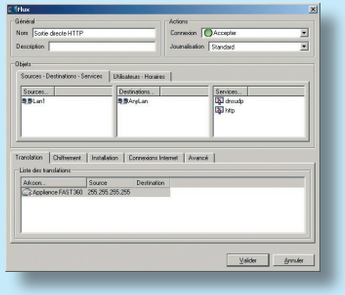
Antivirus : Logiciel capable d'identifier un virus tentant de s'introduire dans le système d'exploitation, ou dans un quelconque fichier, stocké sur le disque dur de l'ordinateur. L'antivirus bloque la tentative d'infection, et prévient l'utilisateur par une alerte.

Backdoors : Un backdoor est un programme malicieux visant à détourner les fonctionnalités d'un service ou d'un système. Il est souvent mis en place à l'aide d'un cheval de troie.

Cheval de Troie : Autrement appelé Trojan (ou Trojan horse), un cheval de Troie est un programme d'aspect anodin, mais qui masque un code exécutable malicieux visant à déclencher une attaque. Il est souvent aussi utilisé pour ouvrir une porte dérobée.

Coupe-feu : Système (ou réseau de systèmes) configuré spécialement pour contrôler le trafic circulant entre plusieurs réseaux. Un coupe-feu peut être de deux natures : à filtre de paquets (packet filter) ou à relais applicatifs (proxy).

Coupe-feu applicatif : Il s'agit d'un coupe-feu agissant au niveau 7 (applicatif). Chaque type de pare-feu est optimisé pour un certain type d'applications, ces dernières étant gérées par des modules différents pour pouvoir être activées ou désactivées. Il vérifie à la fois la conformité du paquet à un protocole attendu (comme par exemple que seul http puisse passer par le port TCP 80), mais aussi il gère l'ouverture des ports dynamiques.



Déni de service (ou DoS) : Attaque consistant à saturer une ressource en effectuant de manière malveillante des demandes de réservation excessives ou en occupant le service illicitement (SYN flooding, UDP flooding, ping of death, LAND attack, SMURF attack, mail bombing...)

Détection d'intrusion : Système combinant logiciel et matériel, qui vise à détecter et neutraliser en temps réel les tentatives d'intrusion sur un réseau. Deux méthodes sont utilisées : la reconnaissance de signatures et la détection d'anomalies. Une évolution récente va jusqu'à la prévention d'intrusion, avec des systèmes capables en théorie d'anticiper dynamiquement les tentatives d'intrusion en se basant sur des analyses statistiques.

DMZ : Littéralement zone démilitarisée, il s'agit d'une zone neutre entre le réseau interne et un réseau externe comme Internet. Cette zone, souvent délimitée par les coupe-feu, agit comme un sas de sécurité, dans laquelle transitent tous les flux échangés.

IPSec : Protocole standardisé créé afin de pallier aux manques de sécurité de l'IP, comme les attaques de type IP-sniffing (écoute), ou d'ursupation d'identité (IP-Spoofing). IPSEC garantit l'authenticité l'intégrité et la confidentialité des paquets IP échangés entre deux entités en s'appuyant sur les techniques de cryptographie.

UTM : Unified Threat Management. Nouveau type d'appliances (boîtiers) tout-en-un. Evolution du coupe-feu traditionnel, sorte de couteau-suisse de la sécurité intégrant anti-virus, anti-spam, détection d'intrusion, ou filtrage.

VPN : Virtual Private Network (Réseau Privé Virtuel). Réseau de données isolé et sécurisé s'appuyant sur IPSec.

POUR EN SAVOIR PLUS

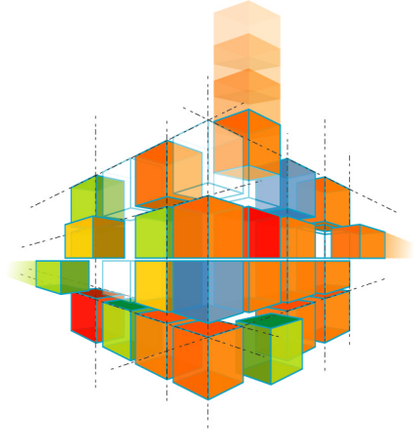
ARKOON
NETWORK SECURITY

L'UTM permet d'élever une forteresse efficace autour du réseau d'entreprise. Ce boîtier multifonction permet à toute PME de réduire ses coûts d'exploitation, de faire évoluer son infrastructure et de soutenir de nombreux échanges, en toute sécurité.

SIÈGE SOCIAL
1 PLACE VERRAZZANO
CS 30603
69258 LYON CEDEX 09
TÉL : +33 (0)4 72 53 01 01
FAX : +33 (0)4 72 53 12 60

ILE DE FRANCE
IMMEUBLE LE PELISSIER
220 AV. PIERRE BROSSOLETTE
92240 MALAKOFF
TEL : +33 (0)1 57 63 67 00
FAX : +33 (0)1 57 63 67 37

www.arkoon.net / info@arkoon.net



ADAPTIVE SECURITY

Un livre blanc réalisé par Speedfire mediArchitects
www.speedfire.com / 08 70 27 64 00