LIVRE BLANC

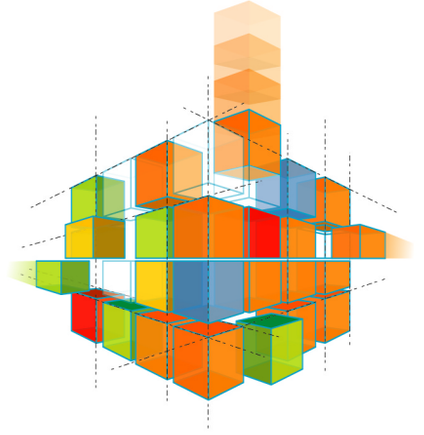
OCTOBRE 2007

COMMENT DISCERNER LES ACCÈS DISTANTS

LE VPN SSL MET DE L'ORDRE DANS LES CONNEXIONS

ARKOON NETWORK SECURITY

Accéder à distance aux ressources informatiques internes de l'entreprise devient fondamental. Mais cette accessibilité doit rester commode pour l'utilisateur, contrôlée et sécurisée par l'entreprise. L'appliance VPN SSL d'Arkoon offre un contrôle rigoureux des accès aux ressources partagées tout en permettant une configuration et une administration simple des groupes d'utilisateurs distants.



ADAPTIVE SECURITY

AMC SSL360 FAST360 Security BOX

LIBERTÉ, MOBILITÉ, SÉCURITÉ

LA MOBILITÉ DES UTILISATEURS PROFESSIONNELS EXIGE D'OUVRIR LE SYSTÈME D'INFORMATIONS TOUT EN DIFFÉRENTIANT LES ACCÈS DES MANAGERS, TÉLÉ-TRAVAILLEURS, EMPLOYÉS NOMADES ET PARTENAIRES DE L'ENTREPRISE.

La montée en puissance des réseaux sans fil et l'accès banalisé au réseau Internet profitent à l'entreprise qui envisage une nouvelle stratégie nomade. Si le scénario le plus fréquent reste l'accès au courrier électronique, de nouvelles applications mobiles apparaissent répondant à l'évolution des métiers et à celle des technologies. Le nomade a désormais accès aux progiciels intégrés de l'entreprise. Synonyme de liberté, la mobilité s'est développée ces dernières années de manière significative. Pour l'entreprise, elle a ce fabuleux avantage de permettre de générer un retour sur investissement rapide. Car les applications accessibles à distance font gagner du temps aux salariés. Elles fluidifient la circulation des informations et génèrent davantage de productivité pour l'entreprise. Mais ces nouvelles possibilités font surgir le besoin de nouveaux liens privés sécurisés. Comment s'assurer que les échanges de données sont toujours protégés ? Quelle confiance peut-on accorder au réseau emprunté ? Intrusions, virus et fuites de données font partie des menaces courantes dans un monde extérieur à l'entreprise. Ces questions deviennent donc prioritaires pour les directions informatiques. Le poste de travail nomade reste difficile à maîtriser puisque, par essence, il n'est pas toujours dans l'enceinte de l'entreprise. Si l'employé se connecte à distance depuis un poste en libre accès, les risques d'infection deviennent plus importants encore.

CONTRÔLER POUR MIEUX MAÎTRISER

La mobilité déplace certains risques au niveau du poste de travail comme le risque de perte de données. Pour la tranquillité des entreprises, les postes informatiques nomades devraient s'inscrire dans un périmètre maîtrisé avec une politique de sécurisation physique et logique mise en oeuvre. Mais, en pratique, les utilisateurs itinérants tentent de se connecter partout, depuis un nombre croissant de terminaux - PC portable, machine personnelle, assistant numérique ou téléphone intelligent.
La direction informatique est tentée d'imposer une politique de sécurité sur les seuls équipements appartenant à l'entreprise. Mais ce n'est pas toujours aussi simple. Les connexions depuis le domicile, le cybercafé ou l'hôtel se multiplient et, du point de vue de la sécurité, elles exposent le système d'informations à un nombre important de risques : systèmes non patchés, virus, chevaux de troie... Un axe retenu consiste à sécuriser la connexion. Un autre revient à construire un portail spécifique d'accès au système d'informations retenant des protocoles sécurisés. L'utilisation de tunnels chiffrés renforce la confidentialité des échanges, de la phase d'authentification jusqu'à la fourniture des données. Le VPN SSL forme une réponse efficace et une alternative avantageuse face au VPN IPSEC. Simple à installer et à administrer, le VPN SSL s'avère parfaitement adapté au développement de la mobilité dans l'entreprise.

EXEMPLE DE PARAMÉTRAGE DES PROFILS

UTILISATEURS DISTANTS	LIEU DE CONNEXION	TERMINAL	CONFIDENTIALITÉ	PROFIL D'ACCÈS
TRAVAILLEUR MOBILE	PARTOUT	CONNU	4	MANAGER
TÉLÉTRAVAILLEUR	RÉSIDENCE	CONNU	4	EXPERT
EMPLOYÉ D'AGENCE	SUCCURSALE	CONNU	3	REMOTE
PARTENAIRE	BUREAU IDENTIFIÉ	INCONNU	5	PARTNER
OCCASIONNEL	WEB CAFÉ	INCONNU	5	SOUS-TRAITANT

Selon l'entreprise, des profils paramétrables sont définis par groupes d'utilisateurs connectés à distance.

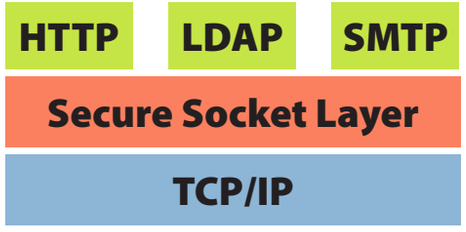
LE VPN SSL : UNE RÉPONSE SIMPLE ET SOUPLE

POUR RÉPONDRE AUX PROBLÉMATIQUES DE MOBILITÉ ET DE SÉCURITÉ, LA MISE EN PLACE D'UN VPN SSL FORME UNE RÉPONSE ADAPTÉE AUX CONTRAINTES DE L'ENTREPRISE. L'OUVERTURE DES RESSOURCES INTERNES DEMEURE CONDITIONNÉE AUX PROFILS D'UTILISATEURS DISTANTS.

Le VPN SSL consiste à mettre en place un canal sécurisé d'échanges de données, chiffré par un protocole au niveau applicatif. C'est ce qui le distingue du protocole IPSEC également utilisé dans la sécurisation des échanges. Le VPN SSL désigne aussi parfois la passerelle logicielle ou matérielle qui permet à un utilisateur de se connecter à distance. Ce n'est pas un équipement de sécurité réseau mais un serveur d'accès sécurisé qui présente les mêmes limites de sécurité qu'un serveur Web. Il ne doit pas être intégré à d'autres fonctionnalités de sécurité du réseau. C'est un équipement qui doit être installé seul sur une zone démilitarisée (DMZ).

Le VPN SSL se présente donc parfois sous la forme d'un équipement dédié - une appliance. C'est le cas du boîtier VPN SSL360 d'Arkoon. Aujourd'hui, le VPN SSL devient un composant essentiel de l'architecture réseau et de sécurité car il offre un accès polyvalent et sécurisé, en mode Web, aux ressources internes de l'entreprise. Il permet aux utilisateurs nomades de se connecter, où qu'ils se trouvent, au réseau local. Le SSL allège aussi considérablement la tâche de l'administrateur réseau. L'entreprise profite souvent des mêmes mécanismes pour gérer ses services extranets sécurisés, adaptés aux différentes familles d'utilisateurs.

Le VPN SSL permet de définir autant de portails de connexion que l'entreprise compte de populations de travailleurs distants. Chaque groupe n'a accès qu'aux applications et données qui le concerne : les serveurs de fichiers, la messagerie, les services Internet pour les commerciaux, l'accès aux services de la logistique pour les distributeurs ou encore la connexion telnet jusqu'aux équipements du réseau local pour l'administrateur. On définit l'accès aux applications sur un portail SSL en fonction de l'appartenance d'un utilisateur à un domaine d'authentification ou à un groupe ayant des privilèges spécifiques. Cette gestion des autorisations permet de définir sur un même portail des niveaux différents d'accès aux applications. L'entreprise peut ainsi attribuer, au sein du même extranet, des droits différents à certains partenaires, en fonction de ses contrats de coopération.



SSL intervient au niveau des applications et non de la couche transport comme IPSEC.

LE VPN SSL REPOUSSE LES LIMITES D'IPSEC

Le protocole IPsec forme une solution valable pour la sécurisation des échanges intersites mais il atteint ses limites avec les connexions nomades. Le VPN SSL fournit les mêmes services qu'IPsec avec plus de flexibilité et pour un coût moindre. Il intervient, en effet, au niveau de la couche de transport et reste donc indépendant des applications. IPsec est plus contraignant. Sa mise en œuvre nécessite l'installation et la configuration d'un logiciel client sur chaque poste de travail distant. De son côté, le protocole SSL est un standard présent dans tous les navigateurs. Retenant le port 443, il n'est pas bloqué par les coupe-feux et s'appuie sur les interfaces web standard.

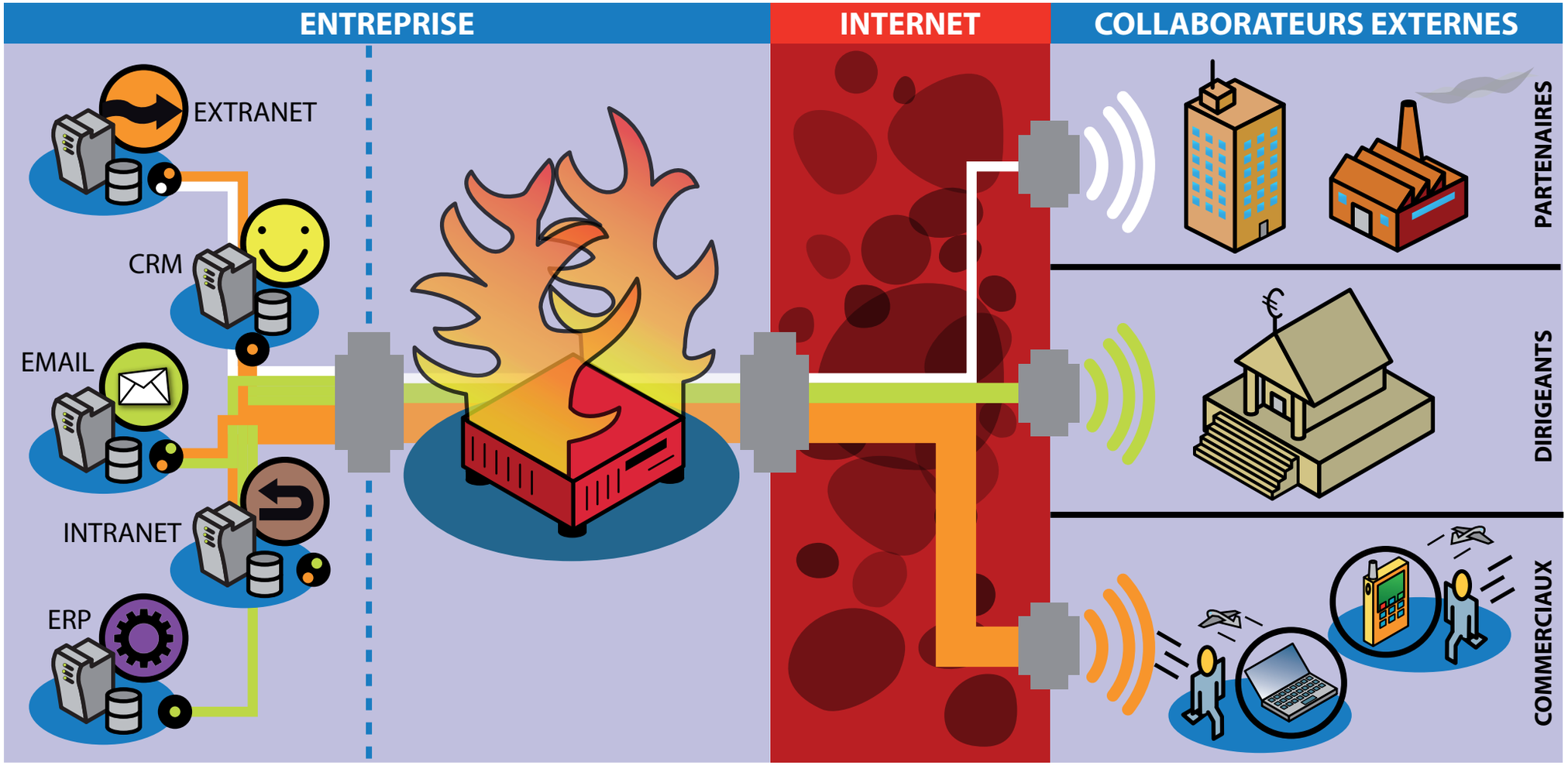
Pour mener à bien sa mission, le VPN SSL nécessite l'intégration d'un certain nombre de mécanismes de sécurité. Pour savoir qui se connecte, des mécanismes d'authentification sont mis en place. L'utilisateur devra ainsi se connecter à une première page web sécurisée (https). Le contrôle de l'identité de l'utilisateur se fera par login et mot de passe, via un serveur Radius ou au travers de l'annuaire Active Directory, LDAP ou NT. On pourra renforcer cette authentification via une carte à puce ou un token. Ensuite, la gestion des droits utilisateurs intervient.

La passerelle VPN SSL gère les droits par domaines d'authentification et par groupes d'utilisateurs. Chaque groupe a le droit de se connecter à un ou plusieurs portails. Sur chaque portail, les utilisateurs ont le droit ou non d'accéder à chaque application, selon leur profil prédéfini.

Les VPN SSL assurent la confidentialité des données par chiffrement de la connexion. La passerelle SSL intègre aussi des technologies pour nettoyer la mémoire du navigateur web. Ainsi, aucune information à caractère confidentiel ne peut être stockée sur le poste distant, le PC en libre service d'un cybercafé, par exemple.

LE VPN SSL360 DÉLIMITE TOUS LES ACCÈS DISTANTS

LE VPN SSL360 ÉTABLIT DES TUNNELS CHIFFRÉS POUR AUTHENTIFIER LES UTILISATEURS DISTANTS PUIS LEUR ATTRIBUER L'ACCÈS AUX RESSOURCES PARTAGÉES, CONFORMÉMENT À LEUR RÔLE DANS L'ENTREPRISE. CONTRAIREMENT À LA TECHNOLOGIE IPSEC, LE VPN SSL RÉPOND EFFICACEMENT, DE FAÇON SIMPLE ET SÛRE, AUX DEMANDES D'ACCÈS DISTANTS DES UTILISATEURS MOBILES.



3 ÉTAPES POUR GÉRER SES ACCÈS DISTANTS

PLACÉE SUR UNE ZONE DÉMILITARISÉE, LA PASSERELLE VPN SSL S'INTÉGRERA DANS L'ARCHITECTURE DE SÉCURITÉ DE L'ENTREPRISE. CETTE DISPOSITION PERMET DE COORDONNER LES CANAUX SSL AUX FONCTIONNALITÉS DE FILTRAGE DU PARE-FEU.

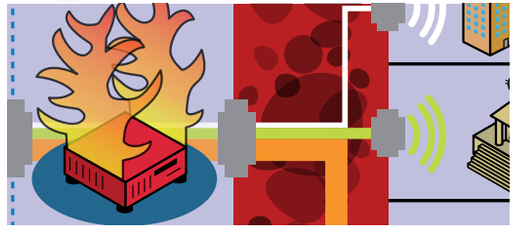
1 IDENTIFIER LES UTILISATEURS

Arkoon Network Security préconise trois étapes pour gérer les échanges professionnels et réduire simultanément le coût de gestion des accès distants. La première consiste à identifier les différentes familles d'utilisateurs distants ou mobiles. On classera, par exemple, les membres du comité de direction, puis les télétravailleurs, les employés du terrain et enfin les partenaires de la distribution. Chaque groupe utilise sa propre configuration matérielle (téléphone intelligent, ordinateur portable ou équipement de bureau). En configurant des profils distincts, on aide à fournir les bons services et on limite les accès aux seules ressources vraiment nécessaires à chacun.

2 CERNER LES RESSOURCES

La seconde étape vise précisément à identifier les ressources auxquelles chaque groupe d'utilisateurs distants pourra accéder, via son navigateur Internet. Les serveurs d'applications et les volumes disques partagés sont regroupés à leur tour, en fonction des rôles définis par l'entreprise. Les clients privilégiés peuvent ainsi visualiser, via l'extranet, l'avancement de leurs commandes en scrutant une partie du système d'information logistique. Cloisonner les ressources partagées évite au distributeur de découvrir le taux de remise concédé à ses confrères et néanmoins concurrents.

3 SOIGNER L'INFRASTRUCTURE



Pour coordonner l'appliance VPN SSL au réseau d'entreprise et optimiser la sécurité des échanges, la passerelle doit être placée, seule, en zone démilitarisée (DMZ). Pourquoi l'isoler sur un segment du pare-feu ? Car il s'agit d'un serveur d'accès restant exposé aux connexions TCP provenant d'Internet. En l'isolant dans la DMZ, les flux entrants dans le réseau d'entreprise sont aiguillés vers ce segment spécifique qui se comporte comme un sas de sécurité. Les flux y sont déchiffrés puis retournés vers le pare-feu en clair. A ce stade, les différents modules du pare-feu analysent les contenus.

DES ACCÈS DISTANTS COORDONNÉS AU PARE-FEU

En suivant le cheminement du flux SSL dans le réseau d'entreprise, on saisit mieux les rôles respectifs de la passerelle VPN et de l'appliance pare-feu. Le flux en provenance d'Internet entre chiffré dans le pare-feu pour être transmis sur la DMZ. Là, le boîtier VPN SSL le déchiffre puis le retourne au pare-feu qui peut ainsi analyser son contenu avant qu'il n'atteigne les serveurs d'applications et les ressources de l'entreprise.
Les mécanismes d'encapsulation, de décodage et de filtrage sont ainsi coordonnés. Le canal SSL une fois monté, la connexion s'effectue toujours avec le même utilisateur distant.

UN PARAMÉTRAGE SIMPLE DES ACCÈS DISTANTS

LE GROUPE GT A ADOPTÉ LA TECHNOLOGIE VPN SSL POUR UN PROSPECT EXIGEANT. A PRÉSENT, L'APPLIANCE SSL360 S20 MONTE TOUS LES TUNNELS CHIFFRÉS DE L'ENTREPRISE, SANS SURCHARGER L'ADMINISTRATEUR.

Nous devions trouver une solution du marché, ultra sécurisée, sans toucher aux stations de travail de nos clients. Nos accès distants devaient rester opérationnels 24 heures sur 24 et 7 jours sur 7 », souligne Cédric Chaubaron, le responsable informatique du groupe familial GT. Le Groupe GT propose des prestations logistiques et de transports dédiés. Ses accès distants au système d'information s'avèrent précieux, surtout dans un contexte de forte expansion des métiers de la logistique santé. Or, les clients de ce secteur doivent surveiller de près l'intégrité et la confidentialité des échanges électroniques avec leurs sous-traitants. Un groupe pharmaceutique devait ainsi accéder aux systèmes d'information du groupe GT sans avoir à reconfigurer ses postes de travail, tout changement à ce niveau pouvant déclencher plus d'un an d'études et de tests avant validation.

Grâce au boîtier SSL360 S20 d'Arkoon, le Groupe GT peut proposer des liaisons distantes très souples à ses clients et prospects. Où qu'ils se trouvent, les dirigeants de l'entreprise accèdent également aux applications critiques, comme l'ERP ou le portail d'entreprise, depuis un simple navigateur Web. Les prestataires informatiques peuvent intervenir sans délais sur les serveurs d'application, tout en garantissant un cloisonnement dans leur domaine d'intervention.

PLUS DE SOUPLESSE DANS LE TRAVAIL

Une fois l'utilisateur distant authentifié - via l'appliance Arkoon et l'environnement Citrix -, un tunnel chiffré est établi automatiquement pour conduire ses transactions jusqu'aux services internes qui lui sont attribués : *« l'équipement Arkoon, très efficace, est désormais utilisé par tout le personnel nomade de l'entreprise. Tous les collaborateurs ont gagné en souplesse de travail. L'accès distant sécurisé permet la mise à jour des documents et l'utilisation d'outils d'aide à la décision, partout et à tout moment »*, apprécie-t-il avant de rappeler que l'équipe informatique est composée de trois personnes seulement pour un effectif total de 1300 professionnels du transport.

Une procédure a été mise au point pour permettre à tout employé distant de se connecter, de façon transparente, sans connaissance particulière en informatique. Un administrateur surveille toutefois l'ouverture et la fermeture des connexions et il peut bloquer l'accès à un point sensible du système lorsqu'il le faut. Cette supervision a fait l'objet d'un transfert de compétences entre Arkoon et le groupe GT, le jour même de l'installation de l'appliance : *« Le transfert de compétence effectué par Novenci, notre prestataire, en parallèle de l'installation, a suffi à nous mettre sur la bonne voie. Le paramétrage des accès distants s'avère très simple, chaque travailleur nomade restant cadré sur son propre domaine »*.

Déployer un réseau privé virtuel de type VPN SSL avec l'appliance Arkoon n'exige aucun paramétrage au niveau du terminal distant. *« Le coût de maintenance s'avère pratiquement nul. C'est un gain de temps appréciable pour l'administrateur en même temps qu'un atout financier »*, conclut Cédric Chaubaron.

UN ROI INFÉRIEUR À UN AN

L'investissement du boîtier SSL360 sera amorti avant un an par le groupe GT. Des liens VPN gérés par l'opérateur auraient coûté, selon l'usage, de dix à quinze fois plus cher chaque mois. Une autre solution interne a été envisagée, mais elle exigeait une procédure de génération de clés bien trop lourde ainsi qu'un complément logiciel sur chaque poste de travail. La solution d'Arkoon a été préférée pour sa simplicité de mise en œuvre et d'utilisation. L'activation d'une applet Java, le temps de la connexion, s'avère très souple et entièrement transparente pour l'utilisateur distant.

GLOSSAIRE

ACL : Liste de contrôle d'accès établie pour gérer la fourniture des ressources partagées du réseau d'entreprise aux systèmes des utilisateurs locaux ou distants.

Applet : Petit programme informatique écrit en java, par exemple, et apporté en réponse à une requête http. Il est délivré par le réseau IP puis exécuté dans le navigateur Web.

Appliance : Equipement spécifique du réseau optimisé pour réaliser certaines fonctionnalités précises comme l'établissement des tunnels chiffrés du réseau privé virtuel.

Certificat : moyen numérique d'assurer l'identité des systèmes interconnectés.

Chiffrement : procédure à base d'algorithme transformant l'information numérique pour la rendre incompréhensible des systèmes et utilisateurs illégitimes.

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 agit 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 la conformité du paquet à un protocole attendu et gère l'ouverture des ports dynamiques.

Détection d'intrusion : Système combinant logiciel et matériel visant à détecter et à neutraliser en temps réel les tentatives d'intrusion sur un réseau.

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.

FAST360 : Le nom de la gamme des appliances UTM d'ARKOON Network Security.

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 chiffrement.

UTM : Unified Threats Management, appliance de sécurité multifonction intégrant plusieurs moteurs de protection réseau, protocolaire et de contenu : Antivirus, Antispam, VPN IPsec...

VoIP : Voice Over Internet Protocol - Ensemble de protocoles applicatifs permettant d'établir la communication et le transport d'information temps réel : Voix, Messagerie Instantanée et Vidéo.

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

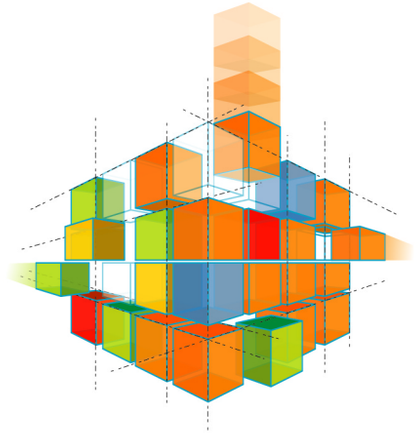
VPN SSL : Réseau privé virtuel établissant des connexions sécurisées vers tout terminal distant supportant le protocole de sécurité SSL (Secure Sockets Layer) via son navigateur Web.

SSL360 : Le nom de la gamme des appliances VPN SSL d'Arkoon.

POUR EN SAVOIR PLUS

ARKOON
NETWORK SECURITY

Arkoon propose un boîtier VPN SSL unique, simple à déployer et à administrer. Il sécurise les accès distants des télétravailleurs et des utilisateurs mobiles ainsi que les services extranet. L'appliance SSL360 S20 assure le contrôle de toutes les identités et centralise tous les accès distants aux ressources locales.



ADAPTIVE SECURITY

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

speedfire mediArchitects
Un livre blanc réalisé par Speedfire mediArchitects
www.speedfire.com / 0952 20 75 00 / infos@speedfire.com