



LA LETTRE D'INFORMATION EN RÉSEAU & COMMUNICATION

N°6 - JUIN 2001

TECHNOLOGIES DE DEMAIN OPERATIONNELLES DES AUJOURD'HUI

avec


ENTERASYS
NETWORKS


EDITO

Le monde de l'informatique, et à fortiori celui des réseaux et de la sécurité, évolue de façon permanente. Les modèles de communication changent et les risques qui y sont liés évoluent de concert. C'est pourquoi il devient impératif de savoir quels types de flux circulent sur les réseaux de façon à optimiser les communications et à les sécuriser en conséquence.

Pour répondre à ces besoins, D.C.I a mis en place un service Recherche & Développement chargé de mener pour vous une veille technologique de pointe.

Aujourd'hui, D.C.I. met en avant les nouvelles technologies au travers des produits de biométrie ou encore des solutions de détection d'intrusion et de communication sans fil.

De telles solutions, si elles relevaient hier de la science fiction, sont aujourd'hui bel et bien opérationnelles. De fait, elles constituent des à présent des compléments ergonomiques aux solutions existantes.

Laurent SAUNIER,
Responsable R&D.

BIOMETRIE : LA SECURITE AU BOUT DES DOIGTS...

L'EMPREINTE DIGITALE COMME IDENTIFIANT

WIRELESS : LA LIBERTE RETROUVEE

LE SANS-FIL VU PAR ENTERASYS : ROAM ABOUT

STOP AUX ATTAQUES DEPUIS LE WEB

LA DETECTION D'INTRUSION AVEC DRAGON

REDUCTION DES COÛTS, CONTRÔLE DES FLUX...

PENSEZ PACKETSHAPER

CAS PRATIQUE

Sécurité de haut niveau
une réalisation D.C.I

WIRELESS : La mobilité en toute sécurité

ENTERASYS
NETWORKS

En matière d'interconnexion de réseau, les solutions sont nombreuses. Qu'il s'agisse d'interconnexion de sites ou d'utilisateurs proches ou distants, les technologies sont variées et parfois difficiles à mettre en œuvre. C'est généralement le cas lorsqu'il s'agit d'interconnecter deux sites distants en environnement urbain. Dans ce cas, il peut être nécessaire de réaliser des travaux d'ampleur (travaux de génie civil, etc...). Or, dans bien des cas, ces travaux peuvent être évités par la mise en œuvre de solutions sans fil. De la même manière, ces solutions peuvent être déployées dans le cadre de besoins forts en mobilité.

Cette technologie est basée sur le principe de **faire transiter les flux de données via une liaison hertzienne**. De telles architectures peuvent être déployées tant en **extérieur** qu'en LAN via les équipements spécifiques appropriés et supportant le **standard IEEE 802.11b**. A cela, il faut prendre en considération deux impératifs .

Tout d'abord, pour les solutions extérieures, les **bâtiments** à interconnecter doivent être **à vue**. Cela implique l'absence d'éléments perturbateurs pouvant interférer sur la liaison, qu'elle soit Point à Point ou Multi-Point (feuillage, bâtiment tiers, etc...). Ensuite, cela suppose d'obtenir les **autorisations nécessaires** à la mise en œuvre de telles solutions (auprès du RLR dans la bande des 2,4GHz et de l'ART).

Précurseur sur cette technologie, **ENTERASYS Networks** propose une **offre globale** de solution in et out-door **répondant aux normes actuelles (802.11b)** mais également **évolutives** vers les normes émergentes (802.11a & HyperLAN II, 802.1x...).

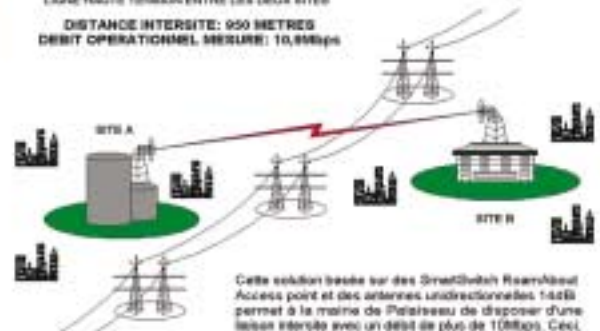
Elle est composée de **points d'accès** au réseau filaire et **des cartes réseau radio**. Celles-ci sont au format PCMCIA pour les postes nomades. Il existe également des adaptateurs pour postes fixes. Les systèmes supportés sont nombreux (Windows 95,98 NT, 2000, CE, Mac OS, Linux). Ces solutions sont complétées par des **antennes intérieures** (solution in-door), et **extérieures Uni ou Omnidirectionnelles** (solution out-door).

CARACTERISTIQUES :

- ✓ Support de 250 utilisateurs par point d'accès.
- ✓ Bande de fréquence de 2400 à 2483,5 Mhz
- ✓ Alimentation électrique par le câble Ethernet
- ✓ **SECURITE :**
- ✓ Authentification des utilisateurs
- ✓ Chiffrement 40 bits (option 128 Bits disponible)
- ✓ Nom de réseau sécurisé
- ✓ Sécurisation physique du point d'accès (fermeture à clef)

Le WIRELESS à la mairie de Palaiseau

SOLUTION OUT-DOOR POUR BÂTIMENTS À VUE
LIGNE HAUTE TENSION ENTRE LES DEUX SITES
DISTANCE INTERSITE: 950 METRES
DEBIT OPERATIONNEL SECURISE: 10,9Mbps



Cette solution basée sur des Directional Resources Access point et des antennes unidirectionnelles 14dB permet à la mairie de Palaiseau de disposer d'une liaison sécurisée avec un débit de plus de 10Mbps. Ceci, sans avoir recours à des travaux de génie civil ou à des liaisons spécialisées coûteuses et malgré la présence d'une ligne haute tension entre les bâtiments.

IDS DRAGON : Halte aux agressions informatiques

ENTERASYS DRAGON

La diversité des attaques en provenance d'Internet représente un danger grandissant pour les entreprises. Il peut s'agir d'attaques par dénis de service, de virus ou troyens circulants sur les flux SMTP, de vandales, d'Applets Java ou d'intrusions via des flux HTTP ou FTP. Chaque jour, de nouvelles attaques sont constatées. Il est donc impératif de pouvoir contrer de telles actions qui se révèlent généralement fortement préjudiciables pour l'entreprise et son système d'information.

En réponse à ces problématiques, **ENTERASYS Networks** propose une solution d'Intrusion Détection Système (IDS) appelée **DRAGON** et basée sur trois gammes de produits.

DRAGON SENSOR

Le sensor est une sonde réseau (NIDS) qui monitore en temps réel les tentatives d'intrusions au moyen de technologies d'analyse de signatures et d'analyse de comportement utilisateur. Chaque événement logué est ensuite classifié dans un groupe (virus, troyen, scan, suspect...), ce qui permettra d'effectuer une post analyse approfondie en cas d'attaque réussie. Avec plus de 1200 signatures répertoriées, Enterasys propose aujourd'hui la bibliothèque la plus complète du marché.

DRAGON SQUIRE

Le Squire est un agent de type host (HIDS) dont le but est de monitorer les attaques systèmes dirigées contre une machine: détection de tentatives de modification des fichiers systèmes, analyse de logs en provenance de firewalls (Enterasys, Pix, Check Point, Axent, Cyberguard...), d'applications (tels des serveurs Web par exemple) ou de l'OS lui-même.

DRAGON SERVER

Le Server est l'élément fédérateur des composants mentionnés ci dessus. Son rôle est double:

- corrélation des événements en provenance des différents Sensors et Squires
- administration de ces mêmes Squires et Sensors (interface Web, téléchargement des nouvelles librairies sur un parc...)

Différents outils d'analyse de données temps réels et d'exports (SNMP, SQL, scripts NMAP) sont fournis gratuitement avec le Dragon Server.

BIOMETRIE : Des équipements qui répondent au doigt et à l'œil.

La sécurisation des flux et des accès est un impératif pour l'ensemble des entreprises communicantes. La prise de conscience de la nécessité de déployer une politique de sécurité s'accompagne aujourd'hui de la nécessité de valider les accès logiques aux ressources réseaux. Parmi les différentes technologies existantes, une paraît aujourd'hui extrêmement novatrice : la biométrie.

Une technologie innovante :

En effet, on connaît généralement les solutions d'authentification forte au travers d'outils tels que les tokens ou encore les cartes à puces. Cependant, une nouvelle technologie émerge aujourd'hui : La biométrie. Ces solutions consistent à **valider et authentifier les accès** aux postes, aux serveurs, au réseau par **identification et reconnaissance de l'empreinte vocale, rétinienne ou digitale**. Parmi les solutions disponibles sur le marché, DCI a retenu la solution d'identification par empreinte digitale. L'aspect ergonomique de ce type de solution est impressionnant. Ainsi, la simple apposition d'un doigt permet de se connecter de façon sécurisée. **La biométrie propose d'identifier l'utilisateur par un élément qui lui est propre**, individuel et infalsifiable : ses empreintes digitales.

D'ores et déjà opérationnelle :

De telles solutions sont aujourd'hui parfaitement éprouvées et utilisées par de grands groupes internationaux. Les produits Secugen, solutions retenues par DCI (distributeur exclusif pour la France) sont exploitables sous différentes plates-formes. Pouvant être déployées soit en **version Desktop simple ou en version réseau**, elles s'intègrent facilement à **Windows 95/98/NT/2000 ou encore sous Novell**. Elles s'intègrent également aux **solutions d'annuaires centralisées** comme Active Directory ou encore NDS de Novell. Dans ces derniers cas, la biométrie permet d'authentifier l'utilisateur de façon performante et de lui attribuer un profil correspondant à des droits d'accès définis. La solution Secugen permet de sécuriser le poste à son ouverture mais également lorsque celui-ci est en veille. De plus les données qui s'y trouvent sont chiffrées via un système de cryptage des répertoires.

La Gamme des produits SECUGEN

LA SOURIS :

Remplace le périphérique de pointage tout en intégrant les fonctionnalités d'identification forte. Un outil fonctionnel et ergonomique facile à intégrer à une plate-forme existante.



Gestion des accès logiques

LE LOGICIEL :

Outre les périphériques d'acquisition, la solution SECUGEN s'appuie sur un logiciel performant et abouti. Celui-ci est chargé de gérer la vérification lors du scan de l'empreinte. De plus, il permet de crypter les fichiers jugés critiques par l'utilisateur. Enfin, la sortie de l'écran de veille se fait également via l'empreinte digitale. Le logiciel verrouille l'accès même lors d'un démarrage en mode sans échec.

Pour Desktop (USB ou Parallèle)
Pour Serveur (USB ou Parallèle)
Pour Portable (PCMCIA)

PRINCIPE DE FONCTIONNEMENT

Cette technologie est basée sur les principes d'acquisition et de vérification. Pour cela, le logiciel Secudesktop détecte les points identifiants de l'image de l'empreinte. Lors de l'apposition d'un doigt, une clé (équivalente à un mot de passe de 60 caractères !) est alors créée et stockée dans une base grâce à un algorithme de chiffrement.

A chaque nouvelle tentative d'accès, une nouvelle clé est générée et comparée à la base existante. Si les deux clés sont identiques, l'accès est alors autorisé.

Chiffrement des données



LE HAMSTER :

Un outil discret pour les portables, desktops ou serveurs. Il permet de disposer d'une solution de biométrie sans avoir à remplacer souris et clavier. Le complément sécurité idéal.



Sécurisation des postes et serveurs
à la connexion ou en mise en veille



LE CLAVIER :

L'outil idéal pour le contrôle d'accès logique. Il intègre la biométrie aux fonctions habituelles des claviers. Robuste et performant, il offre un réel agrément d'utilisation.

L'AVIS DE L'EXPERT :

Nous avons testé plusieurs solutions basées sur cette technologie. La qualité d'une solution de biométrie dépend essentiellement de la qualité des outils d'acquisition et de la pertinence de la partie logicielle qui les supporte. Ainsi, Secugen propose des outils variés et répondant aux critères de robustesse les plus exigeants. De plus, la partie applicative est très élaborée et permet une intégration transparente sur diverses plates-formes.

Laurent SAUNIER – Responsable R&D



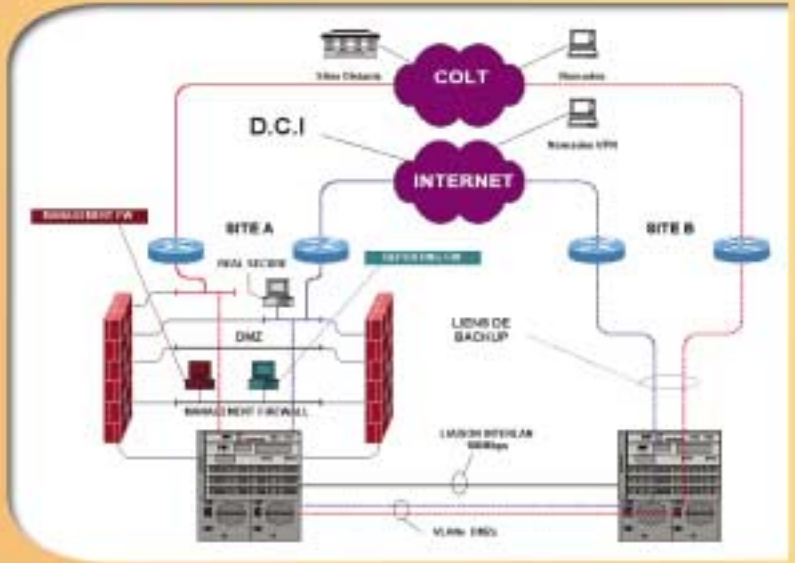
CAS PRATIQUE : Une sécurité de haut niveau

Pour répondre à un besoin de sécurisation maximale lié à son secteur d'activité, un important groupe financier a fait appel aux compétences de D.C.I. pour déployer une architecture redondante complexe.

Celle-ci est basée sur l'utilisation de Firewall redondés exploitant des liens primaires et de backup et permettant d'accéder de façon sécurisée tant à Internet qu'à l'Intranet Colt. Les liaisons entre les liens de backup arrivant sur le second site et les DMZ sont assurées via plusieurs réseaux logiques (VLANs).

Le management de la sécurité est assuré par D.C.I. grâce aux solutions d'info-gérance de Firewall que nous proposons. La société dispose ainsi d'un suivi performant et de la mise à disposition de rapports lui permettant d'optimiser sa sécurité.

Loïc GUILLEMOT - Responsable Sécurité



PACKETSHAPER : Pour tout savoir et tout contrôler sur vos flux Wan.



Répartition de la bande passante sans et avec PACKETSHAPER

Les flux circulants sur les réseaux sont de plus en plus nombreux et agressifs. Ils n'ont pas toujours un caractère prioritaire et occupent cependant une part grandissante d'une bande passante coûteuse.

Pour permettre la mise en place d'une politique de priorisation de flux performante, Packeteer propose la solution **PACKETSHAPER**. Celle-ci permet de garantir une bande passante aux applications critiques (Citrix, SAP, VoIP...), généralement gourmands, disposent de la bande passante restante.

PACKETSHAPER permet notamment d'analyser, de classer et de contrôler simplement vos flux d'une manière proactive et sans modification des structures existantes. Pour cela, il joue sur le fenêtrage TCP pour modifier la taille des paquets en fonction des priorités que vous définissez. Packetshaper reconnaît près de 300 types de flux. Il fournit également des rapports complets permettant de suivre le respect des règles mises en place et l'évolution des trafics. L'administration souple s'effectue via des interfaces de type Web, Telnet, SNMP...

Avec **PACKETSHAPER**, l'optimisation de la bande passante des flux critiques pour l'entreprise permet de réaliser d'importantes économies en supprimant ou retardant le redimensionnement des liaisons (LS, Frame Relay,...).

A PROPOS DE DATA CONCEPT INFORMATIQUE

D.C.I, fort de plus de 9 années d'expertise dans le monde des réseaux, est aujourd'hui composé d'équipes d'ingénieurs et techniciens qui mènent pour vous une veille technologique de premier ordre.

Nos partenariats forts avec les principaux acteurs du marché nous permettent de proposer à nos clients les meilleures solutions aux meilleurs coûts pour leur permettre de pérenniser leurs investissements.

Nos différents pôles de compétences (câblage, architecture, sécurité, système) nous permettent de vous proposer des solutions globales clé en main réalisées dans les règles de l'art et s'appuyant sur des conduites de projet personnalisées.

Notre croissance (40%) et nos résultats (36MF) sont les gages de notre professionnalisme et vous assure de la stabilité de notre structure. N'hésitez pas à faire appel à nos consultants.

CONTACTEZ NOUS

DATA CONCEPT INFORMATIQUE
01 69 79 94 00
www.dci.fr



ENTERASYS NETWORKS
www.enterasys.fr



SECUGEN
www.secugen.com



PACKETEER
www.packeteer.com

