

01 Réseaux

N° 127 / Avril 2003 / 4,60 €

LE PREMIER MAGAZINE DES TECHNOLOGIES DE L'INFORMATION

internet
Professionnel

TUTORIAL

InfiniBand, une technologie d'entrée-sortie universelle

Hautes performances, connexions sûres, faible consommation : les atouts pour connecter les serveurs en grappe. **PAGE 92**

EXPERT

L'annuaire d'entreprise, nouveau défi pour les DSI

► Par Olivier Guérin, directeur de l'activité e-Technologies de SoluCom.



PAGE 88

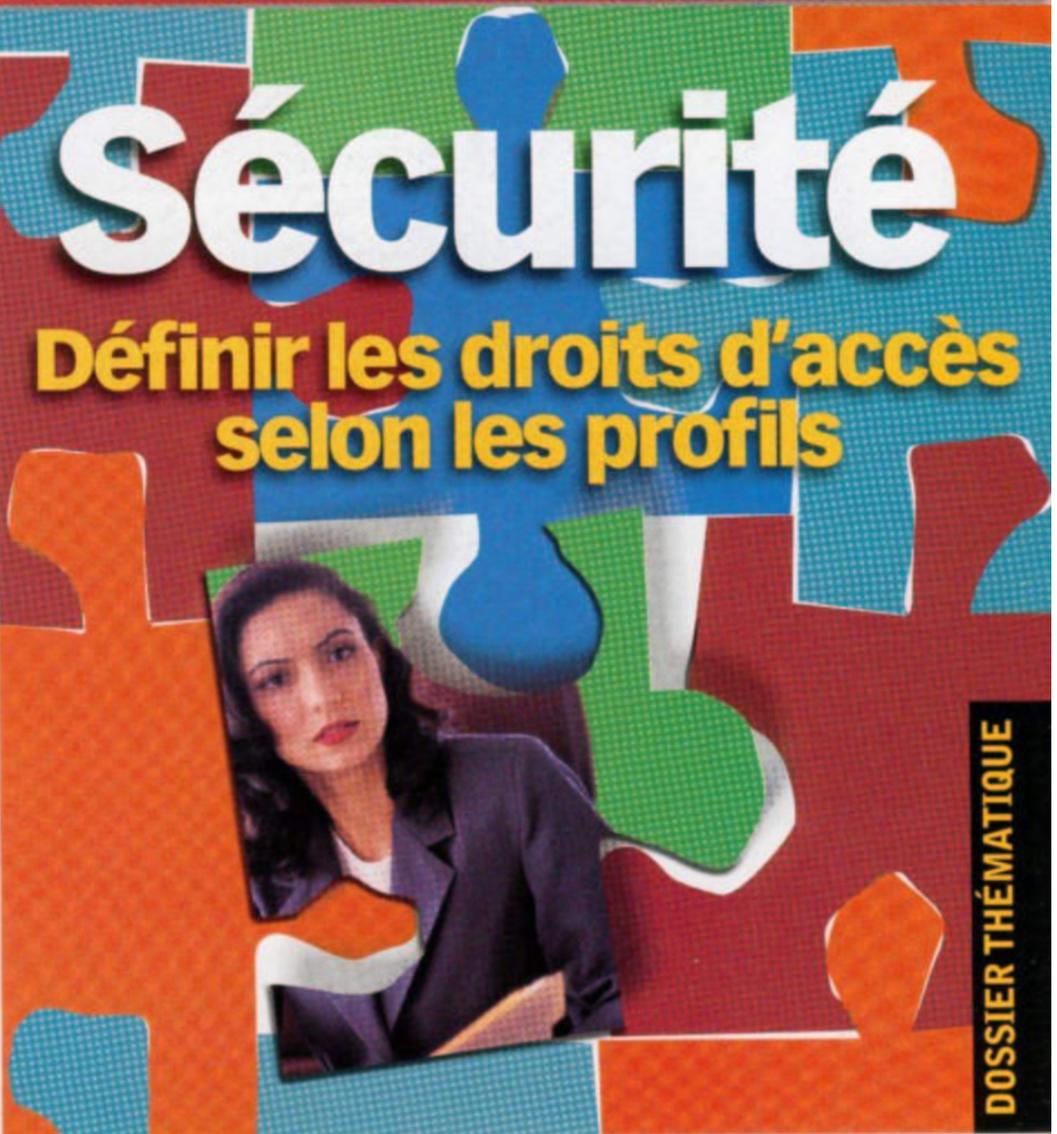
TENDANCE

L'intranet nouvelle génération

► Flash dans le back-office, des fonctions collaboratives, l'intranet mobile et les services web : le nouvel intranet au cœur de l'entreprise. **PAGE 106**

Sécurité

Définir les droits d'accès selon les profils



DOSSIER THÉMATIQUE

ÉVÉNEMENT CEBIT À HANOVRE

Communications sans fil et sécurité changent la donne



► Les communications sans fil remettent en cause non seulement les terminaux et les PC, mais aussi l'organisation de la sécurité des entreprises. **PAGE 7**

BANC D'ESSAI COMPARATIF

Quatre serveurs biprocesseurs en rack 2 u

► Les détails deviennent essentiels. **PAGE 94**

Recommandé par 01 Réseaux



DOSSIER THÉMATIQUE

SÉCURITÉ

Quel coût, pour quels services, chez un MSSP

Nous avons questionné les dix acteurs principaux sur leurs offres de services de sécurité. Les tarifs font souvent le grand écart entre les prestations ciblant les PME-PMI et celles qui sont destinées à séduire les grandes entreprises. Par Olivier Ménager

Le choix d'un MSSP (*Managed security service provider*) n'est pas chose facile. Le secteur est ultraconcurrentiel et en phase de maturation. Afin de clarifier l'état de l'offre, nous avons interrogé dix acteurs ayant un bureau en France, sur quatorze grands segments de la sécurité. Beaucoup se sont montrés fort réticents à communiquer leurs tarifs et le détail des services, même pour les prestations standards (pare-feu ou IDS réseau). Certes, dès que l'on parle de services, les prix varient considérablement selon les options choisies. Par exemple, là où Kerberos s'appuie sur SonicWALL, une solution adaptée aux petites

structures, Thales Secure Solutions (TSS) décline une offre variant depuis un coupe-feu jusqu'à un système à double *firewalling*, intégrant du *stateful inspection* en frontal pour absorber la charge, suivi d'un pare-feu de type *proxy* pour affiner l'analyse.

Les prix que nous publions constituent souvent un « ticket d'entrée ». Quant aux raisons précises du choix des produits, aucun MSSP n'a vraiment détaillé cette partie. Chez ISS, par exemple, l'offre combine uniquement des produits maison (IDS et outil d'évaluation des vulnérabilités), associés aux pare-feu VPN de Check Point-Nokia et de Cisco.



L'un des six SOC (Security operation centers) de Symantec. Situé en Angleterre, c'est un ancien bunker, souterrain. Vingt personnes y travaillent.

LES DIX MSSP CONSULTÉS

MSSP	Nombre d'analystes sécurité		Nombre de SOC		
	Total	Francophones	France	Europe	Monde
ISS	NC	NC	0	2	6
Kerberos	3	11	1	1	1
Securialis	4	7	1	1	1
Security Keepers	15	15	1	1	1
Symantec	140	10	0	2	6
Telindus	20	20	0	3	3
Thales Secure Solutions	15	15	1	0	0
Ubizen	50	38	0	2	3
Unisys	NA	NA	NA	NA	NA
VIA Net.Works	5	5	1	1	1

NC : non communiqué, NA : non applicable

Les MSSP ciblent généralement les grandes entreprises, mais Securialis s'intéresse plutôt aux importantes PME-PMI ; et Security Keepers ou Kerberos, aux plus petites.

« Nous préférons nous concentrer sur quelques technologies que nous maîtrisons pour apporter des solutions globales, plutôt que d'offrir un catalogue complet d'outils de sécurité », explique Thierry Bedos, directeur d'ISS France.

Beaucoup déclarent que les produits intégrés sont avant tout ceux qui sont demandés par leurs clients... même s'ils font l'objet de plus de failles que leurs concurrents, ou s'ils n'autorisent pas une configuration précise de l'analyse d'un flux de communication ! Nous avons nommé les pare-feu FireWall-1, de Check Point, et PIX, de Cisco, les plus répandus sur le marché ! TSS affiche la panoplie la plus large, allant des utilitaires Linux aux produits d'Arkoon, Cisco, NetASQ, NetScreen, SonicWALL et MATRAnet. « De quoi répondre aux différentes architectures de nos clients », assure Franck Perrin, directeur du pôle Exploitation et services chez TSS. Ubizen, pour sa part, propose la supervision de deux

pare-feu à technologie de proxy (Secure Computing et CyberGuard), appréciés des experts en sécurité.

Une tarification à multiples facettes

Outre les coûts d'installation, plusieurs MSSP facturent séparément supervision et administration, tandis que d'autres unifient les deux prestations. La supervision correspond à l'analyse en temps réel des alarmes (Log) et à la corrélation des événements remontés par les équipements. L'administration désigne l'installation de correctifs, et l'ajout de nouveaux utilisateurs ou de règles... Chez TSS, la supervision d'un pare-feu revient ainsi de 850 à 1 650 € par mois, tandis que l'administration coûte de 420 à 650 €. Côté VPN, ce MSSP n'intègre, pour l'heure, que les solutions d'Arkoon, Check Point, Cisco et NetASQ. Et paradoxalement, alors qu'un IDS est souvent plus cher à administrer qu'un pare-feu, TSS le facture

DOSSIER THÉMATIQUE

SÉCURITÉ

► au même prix. Il s'appuie alors sur SecureIDS, de Cisco, Snort ou Dragon, d'Enterasys. La partie Open Source (Snort) est personnalisée, afin de réduire les faux positifs et les faux négatifs. Ce que fait également Security Keepers. Si Trend Micro est fréquemment cité comme passerelle antivirale, TSS y ajoute les offres de Network Associates et de Sophos, tandis que VIA Net Works y adjoint Kaspersky. Un MSSP se doit alors d'être pro-actif. « Nous avons verrouillé l'attaque sur SQL Server dès le 25 juillet 2002, et aucun de nos clients n'a eu à souffrir du ver Slammer », affirme Franck Perrin, de TSS. Concernant le filtrage d'URL, c'est souvent la seule solution de Websense qui est proposée. Les coûts de l'installation initiale ne sont pas à négliger. Chez ISS, ils s'élèvent à 1 995 € pour un pare-feu, 2 195 € pour un IDS réseau, et 450 € pour un IDS serveur. Les coûts mensuels d'administration, incluant ici la supervision, débutent, pour ces offres, respectivement à 995, 895 et 595 €. Des prix qui

L'INFOGÉRANCE DE LA SÉCURITÉ POUR 1 000 € PAR MOIS

Lorans (160 personnes et 32 millions d'euros de chiffre d'affaires) est un distributeur spécialisé en robinetterie. Son responsable sécurité, Olivier Person, a confié à Sodifrance la supervision 24 heures sur 24	des équipements de raccordement à internet : le firewall (Cisco PIX 515), les VPN d'accès distants des commerciaux, et la passerelle antivirus InterScan, de Trend Micro. « Le coût est de 1 000 € par mois, location des	matériels et rapports mensuels compris. Lors de l'appel d'offres, un grand prestataire avait répondu avec une offre surdimensionnée à 150 000 €, rien que pour l'installation et le logiciel ! »	Pourquoi avoir « outsourcé » ? « Être spécialiste de la sécurité réclame du temps et une formation coûteuse », répond Olivier Person, qui gère toutefois l'antivirus Norton sur ses serveurs et PC.
---	---	--	---

tranchent avec ceux que pratique un acteur modeste tel que Security Keepers. Ce dernier dispose pourtant de quelques grandes références, dont le monde bancaire. Son offre, à base de solutions Open Source, associe pare-feu, IDS réseau, VPN, proxy, contrôle d'intégrité et gestion de bande passante, à partir de 420 € par mois ! « Ce n'est pas du dumping, assure George Bell, le directeur. Nos offres sont packagées, et nous les déclinons au fur et à mesure, forts de nos cinq ans d'expérience en ce domaine. » De même, un acteur comme Kerberos se montre très peu cher, avec une offre ciblée PME-PMI. Pourquoi les MSSP semblent-ils pré-

férent les grands comptes ? Parce que l'investissement est souvent considérable en termes de connaissance des produits, des bases de vulnérabilité et des plateformes de supervision. Certains, à l'instar d'Unisys, imposent même à leurs clients une armoire sécurisée, où les serveurs seront protégés par onduleur et accessibles via modem.

Les modestes PME-PMI proscrites de la sécurité ?

Une modeste PME-PMI devra se replier sur les offres de Kerberos. Si les prix semblent élevés, il faut se souvenir que, pour une entreprise, s'appuyer sur un MSSP équivaut

à réduire les coûts en personnel, si l'on considère qu'il faut huit personnes spécialisées pour une supervision 24 heures sur 24. À noter que certains acteurs, notamment américains, n'ont de SOC (Security operation centers) qu'à l'étranger, avec des experts dialoguant en anglais, la barrière linguistique pouvant parfois retarder d'autant la compréhension des problèmes. En conclusion, il faut faire jouer la concurrence, sachant que l'engagement est au minimum d'un an. Si les grands noms semblent des valeurs refuges, il ne faut pas hésiter à contacter des acteurs plus modestes mais parfois tout aussi efficaces. ■

EXEMPLES DE « TICKETS D'ENTRÉE » MENSUELS SELON LES MSSP

Équipement	Supervision	Administration	Prestataires
Offre tout-en-un	De 420 € à 2 700 €	-	Security Keepers (pare-feu, VPN, IDS, etc.) et Symantec (SGS)
Pare-feu passerelle	De 99 € (équipement SonicWALL) à 1 900 €	De 99 € à 700 €	ISS, Kerberos, Securalis, Security Keepers, Symantec, Telindus, Thales Secure Solutions, Ubizen, Unisys et VIA Net Works
IDS réseau	À partir de 199 € ; 2 500 € (administration incluse)	De 199 € à 650 €	ISS, Kerberos, Securalis, Security Keepers, Symantec, Telindus, Thales Secure Solutions, Ubizen et Unisys
IDS hôte	De 360 € à 1 650 €	De 360 € à 650 €	ISS, Symantec et Thales Secure Solutions
Passerelle antivirale	De 250 € à 1 650 € ou 1 € par utilisateur	À partir de 250 €	Security Keepers, Symantec, Thales Secure Solutions, Ubizen, Unisys et VIA Net Works
Passerelle de messagerie	À partir de 79 €, ou 110 € pour 50 utilisateurs	-	Kerberos, Securalis, Security Keepers, Unisys et VIA Net Works
Filtrage d'URL	À partir de 290 €, ou 15 € par utilisateur	À partir de 420 €	Kerberos, Securalis, Security Keepers, Symantec, Thales Secure Solutions, Ubizen et VIA Net Works
Filtrage de contenu actif	Voir passerelle antivirale	-	Securalis, Symantec et Ubizen
Attaques applicatives	À partir de 290 €	À partir de 790 €	Ubizen
VPN	À partir de 166 €	À partir de 1 083 €	ISS, Kerberos, Securalis, Security Keepers, Symantec, Telindus, Thales Secure Solutions, Ubizen, Unisys et VIA Net Works
PKI	Non applicable	À partir de 7,5 € par an et certificat	Thales Secure Solutions et Ubizen
Évaluation des vulnérabilités	19 000 € pour 16 adresses IP par an	-	ISS, Securalis, Symantec et VIA Net Works

L'offre de base supervise les pare-feu (voire les VPN associés) et les IDS réseaux. Le filtrage de contenu actif est considéré par Symantec, Security Keepers et Securalis comme une fonction de l'IDS réseau ou de la passerelle antivirale.

