



AXs GUARD®

À LA CARTE

SECURE INTERNET COMMUNICATIONS



www.aXsGUARD.com



1 Table des matières

1	Table des matières	2
2	Copyrights et Conditions d'utilisation	3
3	À propos de ce document.....	3
4	Qu'est-ce que aXs GUARD?	4
5	Qu'est-ce que le "à la Carte Configurator"?	4
6	Que sont les "Points de performance aXs GUARD"?	5
7	Utilisateurs, ordinateurs, connexions	5
8	Software.....	5
8.1	Sommaire	5
8.2	Le système d'exploitation aXs GUARD	6
8.3	Modules de Logiciels.....	7
9	Hardware.....	15
9.1	Plate-formes	15
9.2	Interface de connexion Internet (toutes plate-formes)	17
9.3	Options Hardware supplémentaire pour une plate-forme Enterprise	18
10	Entretien	19
10.1	Sommaire	19
10.2	Maintenance des programmes et réparation du hardware sur place"	20
10.3	Maintenance des programmes et réparation du hardware "retour pour réparation" "	20
10.4	"Maintenance des programmes exclusivement"	20
10.5	Réduction sur la police d'entretien durant la première année.....	21
11	Installation et formation	21
11.1	Sommaire	21
11.2	Installation sur place et formation de base (1 jour)	21
11.3	Installation sur place des interfaces, options hardware ou un upgrade.....	22
11.4	Formation approfondie (1/2 jour ou 1 jour)	22
11.5	Consultance 2 heures minimum.....	22
12	A propos de Able	23
13	Lexique explicatif	24
14	Index.....	27



2 Copyrights et Conditions d'utilisation

Le Software et les Documents de Able contiennent des informations confidentielles et propres à la société. Able peut être en possession ou dans un processus de demande de brevets, marques déposées, copyrights ou autres propriétés intellectuelles relatifs au Software ou à la Documentation. aXs GUARD®, UNI-box™ et aXs GUARD à la Carte™ sont des marques déposées de Able. D'autres noms de sociétés ou de produits peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Le Software et la Documentation de Able sont fournis "en l'état" sans aucune obligation ou garantie. Able décline toute responsabilité pour les dommages ou coûts encourus par l'entreprise ou par des tiers suite à l'utilisation du ou l'impossibilité d'utiliser le Software ou la Documentation de Able, quelle que soit la cause.

Le présent document est protégé par la législation internationale en matière de copyright. Aucune partie de ce document ne peut être transmise, insérée, reproduite ou envoyée sous quelque forme que ce soit, sans l'autorisation formelle écrite de Able.

Toute forme de propriété ou d'intérêt dans l'aXs GUARD®, les mises à jour et les upgrades, y compris les licences de logiciels, les copyrights, les brevets, les droits sur l'information confidentielle, les droits sur la base de données sui generis et toute autre forme de propriété intellectuelle ou industrielle, sont administrés exclusivement par Able ou, conformément aux dispositions d'un contrat de licence, par le détenteur de la licence. Aucune partie des produits de Able ne peut être transmise, insérée, reproduite ou envoyée sous quelque forme ou pour quelque motif que ce soit, sans l'autorisation formelle de Able.

Copyright © 2003 Able. Tous droits réservés.

3 À propos de ce document

Ce document décrit brièvement:

- le aXs GUARD;
- le principe du "Configurator" et des points de performance aXs GUARD;
- les différents modules de programmes de aXs GUARD et de tiers;
- les modèles hardware de aXs GUARD et les options;
- les options de maintenance;
- l'installation et le service de consultance.

aXs GUARD est un produit européen, développé par Able NV (pour plus d'information sur Able NV consultez le chapitre 12). Ce document est un manuel qui accompagne la configuration du aXs GUARD à la Carte dont il décrit brièvement les différentes possibilités.



4 Qu'est-ce que aXs GUARD?

aXs GUARD est un système complet (Tout-en-1) constitué de hardware, de software et de support, situé entre votre réseau local (LAN) et l'Internet.

Grâce au contrôle effectué par aXs GUARD, vous surfez en envoyez du courrier en toute sécurité, connectez les filiales et les télétravailleurs aux VPN, hébergez un site Internet, etc. ,tout en étant protégé des virus et autres dangers propres à Internet. aXs GUARD tient les hackers à distance, vous permet de contrôler qui fait quoi et à quel moment sur Internet, filtre les messages indésirables (SPAM), limite les téléchargements, bloque les pièces jointes indésirables de la messagerie électronique (par ex. "exe", "mp3"), et bien plus encore...

Avec plus de mille installations aujourd'hui, le concept a fait ses preuves dans les entreprises, les institutions et les services publics comptant de 1 à 1500 utilisateurs.

Les modules de logiciels aXs GUARD peuvent être classés en 4 grands domaines d'application: **Communication, Protection, Restriction d'accès et Contrôle** et c'est ce qui fait de aXs GUARD un "security appliance" unique par comparaison à ses concurrents: c'est une solution complète, une solution 'TOUT-EN-UNE-FOIS' et pourtant vous payez uniquement les modules dont vous avez besoin (aujourd'hui). Si vos besoins changent, il suffira de commander d'autres options ou d'effectuer un upgrade du hardware. Votre investissement initial ne sera jamais perdu et aXs GUARD grandit en quelque sorte au même rythme que votre entreprise.

5 Qu'est-ce que le "à la Carte Configurator"?

aXs GUARD offre tellement de possibilités que pour les petites entreprises il arrive parfois que ce soit 'trop'. En outre, les entreprises disposent souvent déjà d'un certain type de hardware et software pour l'utilisation d'Internet.

Le concept unique "aXs GUARD à la Carte" vous permet, comme son nom l'indique, de composer votre propre système en fonction de vos desiderata.

Au moyen du "à la Carte Configurator" vous choisissez parmi plus de 20 modules de logiciels celui qui vous convient aujourd'hui en fonction de votre situation.

Ensuite, vous choisissez la plate-forme hardware aXs GUARD la plus appropriée en fonction de la performance souhaitée et des éventuels besoins en hardware (par ex. connexions Internet multiples). Tout ceci s'accompagne d'une police d'entretien, d'une installation aisée et d'une formation sur place et fait que vous disposez d'un système en exemplaire unique, répondant à vos besoins actuels en ce qui concerne Internet.

Si par après vous souhaitez ajouter des fonctionnalités, il suffira de les activer sur l'appareil au moyen d'un code de licence, le tout sans aucun coût d'intervention ou d'installation supplémentaire. De même, toute extension hardware ou upgrade du système est toujours possible.



6 Que sont les "Points de performance aXs GUARD"?

Durant le processus de configuration de votre aXs GUARD, des points de performance sont comptabilisés, selon le nombre d'utilisateurs, d'ordinateurs ou de connexions en association avec les modules de programmes choisis (cf. les 6 étapes ci-dessous). Le chiffre qui en résulte est une indication de la performance minimale du aXs GUARD hardware pour pouvoir répondre aux besoins de votre organisation.

La performance des divers modèles hardware est également indiquée dans leur nom (par exemple Enterprise 1500 a une performance de 1500).

Un aXs GUARD en 6 ETAPES ?

1. Définissez le nombre d'utilisateurs, d'ordinateurs et de connexions;
2. Choisissez les modules de logiciels souhaités et les programmes tiers;
3. Choisissez parmi les plate-formes celle qui vous convient en tenant compte des points de performance aXs GUARD et de vos besoins;
4. Choisissez l'interface souhaitée pour votre connexion Internet;
5. Choisissez éventuellement certaines interfaces supplémentaires ou options hardware;
6. Choisissez la police d'entretien qui vous convient et l'installation.

7 Utilisateurs, ordinateurs, connexions

La première étape lorsque vous utilisez le "Configurator" consiste à définir le nombre maximal d'utilisateurs, d'ordinateurs et de connexions. Il convient de tenir compte de votre situation actuelle mais aussi du futur.

Les prix des modules de programmes dans une certaine catégorie varient selon les nombres que aurez définis. Les catégories suivantes sont possibles: 0-10, 11-25, 26-50, 51-100, 101-250, 251-500, 501-1000, 1001 ou plus.

8 Software

8.1 Sommaire

Tout aXs GUARD dispose à l'origine d'un système d'exploitation aXs GUARD, c'est-à-dire une série de fonctions de base comme celles que l'on rencontre sur un Routeur normal. En



plus de cela, vous choisissez les modules de programmes aXs GUARD et les modules tiers répondant à vos souhaits et/ou besoins.

8.2 Le système d'exploitation aXs GUARD

8.2.1 Interface Administrateur

Pour configurer un appareil tel que l'aXs GUARD, un grand nombre de paramètres doivent être ajustés. Afin d'alléger le travail de l'Administrateur du Système, l'aXs GUARD offre une sélection de paramètres facilement configurables, accessibles au moyen des pages HTML. Cela signifie que pour configurer divers paramètres, il suffit d'utiliser un navigateur web standard.

Le module de configuration est sécurisé au moyen d'un nom d'utilisateur et un mot de passe et pour éviter une «back attack» (de la part d'un hacker qui aurait accès au PC de l'administrateur du système), le module de configuration est pourvu de cookies sécurisés accompagnés d'une fonction «time out» avec la possibilité de fermer la session (logout).

Les modèles hardware aXs GUARD ont, à l'exception du modèle SOHO, un display LCD pourvu d'un tableau de commandes pour introduire quelques paramètres de base.

8.2.2 Logiciel de base

En plus des fonctions de routing, le système d'exploitation de base aXs GUARD traite également la Traduction des Adresses Réseau (NAT), Port Forwarding, Port Redirection, un serveur DHCP, un serveur local DNS, un serveur NTP et est équipé d'un système de contrôle de l'usage de mots de passe;

- NAT permet le trafic du réseau local par un ensemble d'adresses IP du réseau local ainsi que le trafic extérieur via une deuxième série d'adresses. La traduction des adresses externes en adresses internes IP permet à aXs GUARD de cacher le réseau interne derrière une seule adresse externe IP.
- Port forwarding peut être utilisé pour rendre accessible sur Internet un des serveurs internes.
- Port redirection permet de router le trafic d'un port sur le aXs GUARD vers un autre port sur le aXs GUARD.
- Serveur DHCP: Lorsqu'un ordinateur démarre, le serveur DHCP aXs GUARD lui envoie tous les paramètres TCP/IP nécessaires.
- Network Time Server: aXs GUARD synchronise son horloge interne via l'Internet au moyen d'une horloge de référence atomique.
- Contrôle de mots de passe: Le service de contrôle des mots de passe peut être activé sur aXs GUARD afin qu'il contrôle chaque nouveau mot de passe utilisé et le rejette s'il s'agit d'un mot de passe dangereux.

Les combinaisons possibles de 2 ou plusieurs interfaces(par exemple 10/100 Mbps Ethernet, 1000 Mbps Ethernet, ISDN, ADSL, ligne louée ou ligne analogique) font de aXs GUARD un Routeur très modulaire. Le hardware Enterprise peut être équipé de plusieurs interfaces.



8.3 Modules de Logiciels

8.3.1 Sommaire

aXs GUARD est conçu pour répondre aux besoins des organisations qui se servent du monde virtuel.

Le souci premier de ces organisations est la sécurité de leur communication en réseau et la possibilité de limiter et contrôler cette communication.

La solution aXs GUARD nous permet de simplifier cette donnée très complexe.

Les quatre défis sont: communication, protection, restriction d'accès et contrôle. Les modules de programmes et modules tiers du aXs GUARD y répondent spécifiquement. Il sont énumérés ci-après et décrits dans les chapitres qui suivent.

Communication	Protection
VPN	SPICT Firewall
IPSec SSH Logiciel client	DMZ extension Firewall
HTTP accelerating proxy & SMTP relay	Contrôle et IDS
"Dial Up" automatique (Dialler on demand)	Reverse HTTP & FTP proxy
Connexions Internet multiples	Antivirus HTTP et SMTP
Serveur de messagerie électronique	Haute disponibilité
Workgroup Connector	Gestion de la bande passante
Courrier électronique gratuit (Webmail)	
Serveur Web	
Fax	
Active directory integration	
DNS public	
Services d'Accès à Distance (RAS)	
Restriction d'accès	Contrôle
Scanneur du contenu & filtre	Journalisation (Logging)
Web	Statistiques et feed-back
E-mail	Surveillance et IDS
Spam	



8.3.2 Modules de communication

VPN

Les Réseaux Virtuels Privés (VPN) sont des canaux de communication sécurisés qui permettent d'avoir accès de façon temporaire ou permanente au réseau local, à partir d'un autre site et en utilisant l'Internet comme réseau.

aXs GUARD utilise les protocoles standards IPsec (IP security) et PPTP (Point to Point tunneling protocol) et les méthodes d'encryptage pour s'assurer que les données qui transitent par ce VPN soient protégées et donc illisibles pour des tiers.

L'utilisation de VPN nécessite éventuellement aussi une installation client VPN (en option) sur le PC du télétravailleur.

Logiciel Client IPSec SSH (module tiers)

Le protocole IPSec est plus sûr pour établir une connexion virtuelle avec l'entreprise. Le logiciel client IPSec est installé sur le PC de l'utilisateur et est muni d'un firewall personnel intégré. Dès que la connexion avec l'entreprise est établie, toute autre connexion avec l'Internet est exclue.

HTTP accelerating proxy et SMTP relay

C'est le module qui assure les fonctions de communication les plus importantes. Le proxy permet l'accès à Internet pour tous les utilisateurs en gardant localement les données demandées afin d'accélérer la reproduction des pages Internet et sauvegarde l'enregistrement de tout le trafic. SMT relay assure l'acheminement de l'e-mail vers un serveur de messagerie électronique interne.

Accès Internet

Un proxy est un serveur situé entre un poste de travail sur le réseau et l'Internet. Le poste de travail ne fait pas de demande directe au serveur web Internet mais au proxy, qui lui, exécute la demande adressée au serveur web Internet et renvoie la réponse au poste de travail. L'application Caching de aXs GUARD accélère fortement l'accès à l'Internet. Grâce à cette application, les paquets de données résultant d'une consultation d'Internet sont stockés temporairement sur le disque dur de l'aXs GUARD. L'utilisateur suivant qui consulte les pages du même site Internet reçoit ainsi les données provenant du disque dur de l'aXs GUARD sans que celles-ci doivent être recherchées une nouvelle fois sur le serveur web. Le Caching est utile pour l'accès aux sites web, le transfert de fichiers (FTP) et la conversion des noms de domaine en adresses IP (DNS).

Enregistrement (Logging)

Une des fonctions les plus importantes du Proxy est l'enregistrement de toute activité dans le but d'avoir une vue générale de toute la communication sur le réseau. Les fichiers logs ayant trait aux connexions du réseau, le courrier entrant et sortant, le surf, etc. peuvent également être téléchargés du aXs GUARD pour être analysés au moyen d'applications externes. Le logging permet aussi de générer les statistiques et les rapports du module Statistiques et Feed-back.



SMTP relay

aXs GUARD peut être utilisé comme Mail Transfer Agent (MTA) pour le Simple Mail Transfer Protocol (SMTP) relay, ainsi qu'en tant que propre serveur de messagerie électronique (voir ci-après point E-mail).

Le aXs GUARD SMTP relay réceptionne les messages électroniques du réseau local pour les envoyer ailleurs, vers l'Internet ou au sein du réseau, et il réceptionne l'e-mail en provenance de l'Internet et l'envoie à un serveur de messagerie interne (celui-ci pouvant être le serveur de messagerie électronique aXs GUARD, voir ci-après le point E-mail) ou n'importe quel autre serveur de messagerie sur le réseau tel que MS Exchange™, Novell GroupWise™, MS Mail™ ou Lotus Notes™.

De plus, le aXs GUARD SMTP relay est également pourvu d'une protection (anti-relay) qui empêchent les tiers d'abuser du serveur de messagerie aXs GUARD pour y répandre des virus ou des messages indésirables (SPAM).

"Dial Up" automatique

L'aXs GUARD, muni d'une carte ISDN, effectue automatiquement la connexion à l'Internet. De plus, afin de réduire vos frais de téléphone, cette connexion n'est établie que si elle est nécessaire. L'analyse intelligente du flux de données faite par l'aXs GUARD permet de distinguer trois types de trafic de données sur votre réseau:

- Le trafic local entre les différents ordinateurs du LAN
- Le trafic Internet "non-interactif" (par ex. le courrier électronique)
- Le trafic Internet interactif (par ex. la consultation de pages WEB et le FTP)

La première catégorie est complètement ignorée par l'aXs GUARD.

La deuxième catégorie est mise en attente pour une transmission ultérieure. Cela signifie que les e-mails ne sont pas envoyés immédiatement, mais mis en attente pour un envoi groupé.

Pour la troisième catégorie, l'aXs GUARD établit immédiatement une connexion avec le fournisseur d'accès à Internet. Avec une ligne ISDN, le temps nécessaire pour établir cette connexion est généralement inférieur à 3 secondes.

Une fois la connexion établie, l'aXs GUARD contrôle l'activité de la ligne, et coupe la connexion après une certaine période d'inactivité (3 minutes par défaut). Ceci contribue à la réduction des frais de télécommunications.

La connexion du aXs GUARD a une configuration multiposte et multitâche. Cela signifie que plusieurs utilisateurs peuvent simultanément accéder à l'Internet de manière interactive. Lors d'une connexion Internet (par ex. pour consulter un site web), l'aXs GUARD exécute automatiquement toutes les tâches non-interactives mises en attente, comme l'envoi et la réception des e-mails

Connexions Internet multiples (Multiple Internet Connections)

La connexion Internet utilisée principalement pour les connexions VPN prioritaires ou pour le trafic vers la zone DMZ nécessite une bande passante à haute disponibilité. Le trafic Internet moins prioritaire peut cependant occuper régulièrement toute la bande passante. Afin de pouvoir garantir la disponibilité de la bande passante pour le trafic prioritaire, aXs



GUARD permet de prévoir une deuxième connexion à Internet par laquelle est dévié le trafic non prioritaire HTTP et les messages (par exemple sur une connexion ADSL ou par câble bon marché). Cette option exige bien sûr que aXs GUARD soit équipé des interfaces Internet appropriées.

Serveur de Messagerie électronique

L'E-mail aXs GUARD est un serveur de Messagerie à part entière qui permet la création et la gestion de boîtes aux lettres électroniques pour plusieurs utilisateurs. Ceux-ci peuvent consulter leur courrier sur l'aXs GUARD par le biais de n'importe quel client e-mail en utilisant le protocole POP3 ou IMAP4.

L'utilisation du serveur de messagerie électronique aXs GUARD vous donne accès à une multitude d'options en matière de messagerie électronique: une adresse e-mail pour chaque utilisateur, réponse automatique au courrier (en cas d'absence), envoi automatique du courrier vers des adresses e-mail internes ou externes, liste de distribution (par exemple info@domaine.be), archivage automatique du courrier, utilisation de plusieurs noms de domaines, ...

Lecture des boîtes aux lettres externes

Il arrive qu'un utilisateur soit obligé de pouvoir consulter une boîte aux lettres externe à partir de son poste de travail. Toutefois, l'accès direct à un serveur externe implique un accès non-contrôlé à l'Internet sans scanning antivirus. Pour que cela puisse néanmoins se faire de façon contrôlée et sécurisée, aXs GUARD peut consulter la boîte aux lettres externe d'un utilisateur et déposer les messages dans la boîte aux lettres de l'utilisateur.

Fichier d'Adresses centralisé (LDAP)

L'aXs GUARD inclut un service relatif à l'administration centralisée d'un répertoire d'adresses de personnes, de sociétés et d'adresses e-mails. Ce service centralisé évite à tous les utilisateurs du LAN de devoir créer et mettre à jour leur propre carnet d'adresses. Tous les utilisateurs intégrés à l'aXs GUARD font automatiquement partie du carnet d'adresses, lorsque cette fonctionnalité est activée.

Ce module du serveur de messagerie dépend du module SMTP relay qui doit obligatoirement être présent dans votre configuration.

Workgroup Connector (pour MS Outlook™)

Le logiciel Workgroup Connector pour MS Outlook (sur l'ordinateur de l'utilisateur), associé au serveur de messagerie électronique aXs GUARD fait du aXs GUARD un serveur 'Groupware' complet. Ceci signifie que les agendas (par exemple salles de réunion, agenda directeur, ..), les fichiers contenant des données clients (l'ensemble des adresses), et les dossiers e-mail (par exemple sales@..) peuvent être partagés entre les utilisateurs qui ont installé le logiciel Workgroup Connector pour MS Outlook. Ce module d'extension fonctionne sur toutes les versions à partir de Outlook 98.

Messagerie électronique sur le Web

Ce module permet aux utilisateurs de lire le courrier électronique à partir de boîtes aux lettres du aXs GUARD-même (à condition que le module serveur messagerie ait été choisi)



ou sur un autre serveur de messagerie interne, et ceci sur n'importe quel ordinateur (à l'intérieur ou à l'extérieur de l'organisation) équipé d'un logiciel de navigation sur le Web et d'une connexion Internet.

Le webmail aXsGUARD consulte ces données sur le serveur de messagerie en utilisant le protocole IMAP4.

Serveur WEB

L'aXs GUARD compte 3 serveurs web. Le premier peut servir en tant que serveur web Intranet, c'est-à-dire un site web qui ne peut être consulté que sur le réseau local. Le deuxième en tant que webserver Internet public pour votre entreprise (ceci implique une connexion permanente avec l'Internet, ainsi qu'une adresse IP fixe et un nom de domaine) et le troisième en tant que webserver Internet public protégé (HTTPS) pour l'échange de données cryptées. Les pages web peuvent être facilement chargées grâce au serveur FTP. Pour éviter que certains scripts non sécurisés mettent en péril l'ensemble du système, les serveurs web fonctionnent dans un environnement « jail house ».

Fax

L'aXs GUARD peut éventuellement être étendu pour pouvoir être utilisé comme un puissant serveur FAX (pour tout le LAN), complètement intégré à votre environnement e-mail. L'envoi d'un fax à partir d'un PC en réseau devient aussi simple que l'impression d'un document. L'aXs GUARD extrait du document les informations nécessaires à l'envoi, comme le numéro de Fax et transmet après l'envoi une confirmation de l'envoi via e-mail à l'expéditeur.

Le paramétrage peut se faire de telle manière que chaque Fax envoyé et reçu soit automatiquement imprimé sur une imprimante du réseau et qu'une copie du message e-mail soit envoyée à une ou plusieurs autres adresses (par exemple pour l'archivage). Une confirmation d'envoi peut également être imprimée comme pour n'importe quel Fax classique.

Les fax entrants sont également reçus via aXs GUARD. Les messages par fax sont livrés en annexe sous format TIFF à une ou plusieurs boîtes aux lettres et peuvent être consultés au moyen d'un "image viewer" standard.

L'aXs GUARD peut être équipé de plusieurs lignes de fax.

Intégration Active Directory

Un service de Répertoire est un lieu où l'information relative aux systèmes du réseau, tels que utilisateurs, ordinateurs, imprimantes etc., peut être gérée et sauvegardée au niveau central. Il est également pourvu d'un système permettant de gérer de façon cohérente les noms, les descriptions, les lieux, les droits d'accès, etc. Active Directory fait partie du système d'exploitation Windows® Server. L'intégration aXs GUARD Active Directory permet une collaboration entre aXs GUARD et Microsoft® Active Directory afin de transmettre l'information de façon cohérente, que des paramètres aXs GUARD spécifiques viennent ensuite compléter dans l'aXs GUARD.



DNS public (Public DNS)

Grâce à ce module aXs GUARD peut faire office de serveur DNS public propre à la société et les demandes de traduction de noms de domaines vers une adresse IP peuvent être réalisées en interne. En outre, l'organisation peut gérer elle-même ses noms de domaines et n'est donc plus dépendante d'un fournisseur d'accès Internet (ISP) pour ce service.

Services Accès à Distance

L'aXs GUARD peut être utilisé comme serveur d'accès à distance, aussi bien analogique que via ISDN. Après que l'utilisateur se soit connecté et que son mot de passe ait été authentifié, son ordinateur fait partie du réseau de l'entreprise. Il peut utiliser toutes les applications comme s'il était installé à l'intérieur des bâtiments. Le logiciel doit être complété par les modems analogiques ou interfaces ISDN nécessaires.

8.3.2 Modules de Protection

Firewall SPICT

Le "Stateful Packet Inspection with Connection Tracking" (SPICT) est l'un des modules de protection les plus importants sur aXs GUARD. Le routeur avancé, équipé d'un module de programmes pare-feu protège votre réseau contre toutes les techniques de hacking connues et, en fixant certaines règles, il est possible de déterminer quel trafic est permis et vers où.

Les règles sur le aXs GUARD sont regroupées en entités logiques appelées "Policies". Les règles pare-feu les plus utilisées sont configurées d'avance et peuvent donc servir d'exemple lorsque de nouvelles règles sont créées.

Grâce à ce système de règles et "policies", l'aXs GUARD est facile et rapide à configurer. Lorsque vous configurez de nouvelles règles qui ne sont pas standard, vous pouvez aussi faire appel à notre service technique (cette aide est incluse dans notre police d'entretien).

Extension pare-feu DMZ

Il s'agit d'une extension du module pare-feu SPICT qui offre la possibilité de protéger davantage la zone DMZ. Ce module exige la présence du module pare-feu SPICT ainsi qu'une interface Ethernet supplémentaire.

Contrôle et IDS

aXs assure une protection préventive et signale les problèmes éventuels au moyen d'un journal et du Système détecteur d'intrusions (IDS). Les fichiers journaux (logfile) vous informent sur les temps de connexion, l'état du courrier entrant et sortant, l'utilisation Internet, les virus éventuels et les attaques de hackers et vous offre une série d'autres rapports intéressants relatifs au système et au pare-feu. Le vérificateur de journal contrôle ces fichiers en permanence et recherche les irrégularités. Si celles-ci apparaissent, un avertissement est envoyé à l'administrateur par e-mail. Cette protection pro-active permet donc de prendre les mesures appropriées contre les attaques que l'on a identifiées.



Reverse HTTP et FTP proxy

Ce module protège les serveurs internes HTTP et/ou FTP. Le serveur "reverse proxy" installé sur aXs GUARD reçoit les demandes HTTP et FTP d'Internet et les transmet au serveur interne (par exemple un Internet Information Server). Le serveur interne n'est donc jamais connecté directement à Internet ce qui renforce la protection car c'est généralement le serveur interne qui est le plus sensible aux tentatives d'intrusion.

Trend Micro HTTP et SMTP antivirus

Le scanner Trend Micro antivirus contrôle le courrier électronique, les pièces jointes, les téléchargements (FTP) et le surf en temps réel. Les fichiers infectés sont nettoyés ou supprimés si le virus ne peut pas être éliminé. aXs GUARD envoie un avertissement à la source, le destinataire, et l'administrateur du système, accompagné d'un bref rapport sur le virus et les mesures prises. aXs GUARD contrôle toutes les 15 minutes la disponibilité de nouveaux logiciels antivirus ou de fichiers modèles et les télécharge du serveur Able. Ensuite ils sont installés automatiquement.

Haute disponibilité

Ceci vous permet d'assurer une grande disponibilité entre deux systèmes aXs GUARD séparés mais identiques. Les deux systèmes travaillent de façon indépendante et sont connectés en permanence via Ethernet qui synchronise les données. Si l'une des deux machines tombait en panne, l'autre prend la relève et il n'y a donc pas d'interruption sur le réseau. Il est impératif que les machines soient identiques quant à l'équipement hardware.

Gestion de la Bande passante (Bandwidth management)

Les connexions Internet utilisées à des fins particulières, telles que les connexions VPN ou le trafic DMZ exigent une bande passante à haute disponibilité qui soit surtout permanente. Toutefois, la bande passante est influencée par le trafic Internet non prioritaire tels que le surf et le courrier. Le module de gestion de la bande passante sur l'aXs GUARD assure un contrôle permanent et peut gérer et dimensionner le trafic prioritaire et non prioritaire. Ce faisant, une connexion VPN importante entre sites est garantie en permanence et l'on peut réellement parler de Qualité du Service.

8.3.3 Modules de Restriction d'Accès

Scanneur de contenu et filtre

Ce module permet de contrôler la navigation sur Internet et le courrier électronique au moyen de trois filtres, en particulier le filtre Web, le filtre e-mail et le filtre spam. Ce module nécessite le 'HTTP accelerating proxy' et le module relay SMTP dans votre configuration aXs GUARD.



Filtre Web

L'aXs GUARD peut être configuré de manière à contrôler l'accès des utilisateurs ou groupes d'utilisateurs à certains sites ou durant certaines heures de la journée, par exemple les heures de travail. Ce contrôle s'effectue au moyen de filtres, c'est-à-dire une série de listes contenant certains mots clés et des horaires.

Lorsqu'un utilisateur souhaite accéder à Internet, il est obligé d'introduire son nom et son mot de passe de façon à obtenir l'accès conformément aux règles imposées (par exemple permission de surfer durant les heures de travail uniquement sur certains sites et/ou après les heures de travail sur tous les sites à l'exception de quelques sites, par exemple pornographiques).

Le filtre web est également utilisé pour filtrer les téléchargements pour certains utilisateurs ou groupes d'utilisateurs en bloquant l'extension du fichier (par exemple bloquer le téléchargement des fichiers .exe).

Filtres e-mail

Un contrôle similaire est possible pour le courrier électronique. Même si le serveur de messagerie électronique est interne, tout le courrier entrant et sortant peut passer par le serveur SMTP du aXs GUARD afin qu'il y ait toujours la possibilité de le filtrer ou de le bloquer.

Ces filtres permettent d'interdire à certains utilisateurs ou groupes d'utilisateurs d'envoyer certains fichiers (ex. « exe », « vbs »).

Le filtrage de courrier peut être effectué sur base du domaine, de l'adresse e-mail, de l'extension des fichiers et/ou si une certaine valeur est attribuée au courrier comme c'est le cas pour le filtrage de spams.

Il est également possible de limiter le nombre de domaines Internet auxquels ils peuvent envoyer ou dont ils peuvent recevoir du courrier électronique (par ex. uniquement à leurs collègues dans la société).

Filtres spam

Un mécanisme de scanning intelligent détecte immédiatement le courrier publicitaire (SPAM) lorsque celui-ci entre sur aXs GUARD.

Une certaine valeur est attribuée à tous les messages entrants selon certaines caractéristiques typiques de l'en-tête et du contenu du message. Dès qu'un message dépasse une certaine valeur, la ligne 'objet' est pourvue d'un repère permettant au logiciel de courrier électronique de procéder à d'autres filtrages. Il est également possible de supprimer le message avant qu'il n'atteigne la boîte aux lettres lorsqu'il dépasse une certaine valeur.

En outre, il est possible d'établir une liste d'adresses 'indésirables', dont tous les messages sont supprimés automatiquement comme par exemple les spammeurs, les concurrents, les adresses e-mail privées (hotmail par exemple), etc.



8.3.4 Modules de Contrôle

Enregistrement (Logging)

Chaque module aXs GUARD a ses propres possibilités d'enregistrement et toute activité peut donc être stockée. Cette information enregistrée peut ensuite être consultée dans l'interface de l'administrateur ou exportée vers des programmes d'analyse pour une analyse plus approfondie.

Statistiques et feed-back

Statistiques

Les statistiques sur aXs GUARD montrent, sous forme graphique, toutes les communications sur le réseau telles que HTTP, FTP, le courrier électronique, les virus interceptés, les messages SPAM, etc. Pour chaque type de trafic, quatre graphiques sont créés (par jour, semaine, mois et année).

Feed-back

Le feed-back vise à donner une synthèse claire et utile de l'utilisation d'Internet et du courrier électronique au sein de l'entreprise. Les données issues des fichiers journaux sont présentées sous forme de rapports synthétiques qui présentent en un coup d'œil un résumé de l'information souhaitée. Par exemple: combien d'e-mails ont été envoyés par une personne, quels sites ont été visités, qui est le surfeur le plus actif, ...

Contrôle et IDS

Voir Contrôle et IDS au point 8.3.2.

9 Hardware

9.1 Plate-formes

9.1.1 Sommaire

Le hardware aXs GUARD est proposé selon une configuration fixe telle que les modèles SOHO et Office ou selon une configuration modulaire, telle que la gamme Enterprise.

Le "à la Carte Configurator" propose automatiquement le hardware approprié en fonction du nombre d'utilisateurs, d'ordinateurs ou de connexions souhaitées et des modules de logiciels choisis (étape 1-3). Nous rappelons que seuls les modèles Enterprise peuvent recevoir des interfaces supplémentaires (par exemple connexions Internet multiples).



9.1.2 SOHO 500

Le modèle SOHO 500 est indiqué lorsque le total des points de performance (un total de points basé sur la combinaison du nombre d'utilisateurs, d'ordinateurs ou connexions et des modules de programmes souhaités) est inférieur à 500. Celui-ci est constitué de:

- Un dispositif hardware de Able
- Processeur intégré
- 20 GB Disque dur
- 256 MB RAM
- 1 RS232 port série (par exemple pour le module Fax)
- Interface Ethernet intégrée 10/100 Mbps
- Slot disponible pour 1 Ethernet, ADSL, ligne louée ou interface ISDN

9.1.3 Office 800

Similaire à SOHO 500 mais plus rapide, cette plate-forme est pourvue d'un afficheur qui indique le statut ainsi que d'un tableau de commandes permettant d'introduire les paramètres de base. La performance est de 800 points.

9.1.4 Office 1000

Modèle similaire à Office 800 mais avec une performance supérieure (1000 points performance aXs GUARD).

9.1.5 Enterprise 1500

Le modèle Enterprise 1500 supporte une combinaison de nombre d'utilisateurs, d'ordinateurs ou de connexions et de modules de programmes souhaités dont les points de performance sont inférieurs à 1500. La plate-forme comprend:

- Structure montable en armoire de 19 inch 4U
- Dispositif hardware de Able (Q1-2004)
- Clavier et afficheur montrant l'état et permettant le paramétrage de base
- 30 GB Disque dur
- 256 MB RAM
- 2 x RS232 ports série (par exemple pour module Fax et UPS)
- Slot CPU board
- Interface Ethernet 1 x 10/100 Mbps
- 4 slots disponibles permettant plusieurs combinaisons d'interfaces

9.1.6 Enterprise 2000

Similaire au modèle Enterprise 1500 mais avec une performance supérieure.

9.1.7 Enterprise 2750

Similaire au modèle Enterprise 2000 mais avec une performance supérieure, un disque dur 40 GB et 512 MB RAM.



9.1.8 Entreprise 3500

Similaire au modèle Entreprise 2750 mais doté d'une performance de 3500.

9.2 Interface de connexion Internet (toutes plate-formes)

9.2.1 Sommaire

Tous les modèles aXs GUARD de série possèdent une interface Ethernet 10/100 Mbps pour la connexion avec le réseau local. Une seconde interface pour la connexion avec Internet peut être choisie parmi les possibilités suivantes. (Les modèles Entreprise supportent plusieurs interfaces (voir point 9.3)

Le choix de la deuxième interface pour la connexion Internet dépend du Fournisseur d'Accès (ISP), de votre type d'abonnement et de la vitesse et des possibilités de votre connexion Internet. La société Able peut vous conseiller en la matière afin de choisir l'interface appropriée.

9.2.2 10/100 Mbps Ethernet (avec utilisation d'appareillage externe)

Certains fournisseurs d'accès assurent une connexion Internet en fournissant eux-mêmes le dispositif de raccordement (par exemple un routeur, un modem 'câble', un modem ADSL). Dans ce cas vous pouvez connecter cet appareil au aXs GUARD en prévoyant une deuxième interface 10/100 Mbps Ethernet dans l'aXs GUARD.

9.2.3 ADSL pour ligne analogique (PSTN)

Cette interface vous permet de raccorder directement la connexion Internet ADSL livrée sur une ligne téléphonique analogique, à l'aXs GUARD (y compris le câble).

9.2.4 ADSL sur ligne ISDN

Comme ci-dessus mais pour une connexion Internet ADSL via une ligne téléphonique ISDN.

9.2.5 Leased Line X.21

Vous permet de raccorder une ligne louée sur aXs GUARD. La ligne louée a une interface de raccordement X.21. L'installation comprend l'interface et le câble.

9.2.6 Leased Line V.35

Comme ci-dessus pour X.21 mais la ligne louée est livrée avec un raccordement V.35, pouvant être relié directement sur l'interface V.35.



9.2.7 ISDN

Cette interface pourvoit l'aXs GUARD d'une connexion Internet ISDN à distance (2 canaux). Voir aussi le chapitre "Dial up automatique"

9.2.8 2 x 10/100 Mbps Ethernet

L'interface 2 x 10/100 Mbps Ethernet vous permet d'équiper aXs GUARD de 2 raccordements Ethernet supplémentaires, ce qui peut être utile si vous souhaitez la configuration suivante sur un aXs GUARD SOHO ou Office: 1 lien vers le LAN, 1 lien vers le routeur externe, 1 lien pour la zone DMZ ou un 2^e segment Ethernet.

9.3 Options Hardware supplémentaire pour une plateforme Enterprise

9.3.1 Sommaire

Les modèles aXs GUARD Enterprise disposent de plusieurs slots disponibles permettant de brancher des interfaces de communication supplémentaires. Les interfaces suivantes sont disponibles.

9.3.2 10/100 Mbps Ethernet (DMZ, 2^e LAN)

Une interface Ethernet 10/100 Mbps supplémentaire peut être commandée pour une zone DMZ par exemple ou un deuxième raccordement LAN.

9.3.3 1000 Mbps Ethernet

Comme l'option précédente mais supporte Ethernet Gigabit.

9.3.4 ADSL via ligne analogique PSTN

Cette interface vous permet de raccorder directement la connexion Internet ADSL supplémentaire livrée sur une ligne téléphonique analogique, à l'aXs GUARD (y compris le câble). Ceci peut s'avérer utile si par exemple vous souhaitez traiter un trafic Internet particulier sur une ligne séparée.

9.3.5 ADSL via ISDN

Comme ci-dessus mais pour une connexion Internet ADSL supplémentaire via une ligne téléphonique ISDN.

9.3.6 2 x 10/100 Mbps Ethernet

L'interface Ethernet 2 x 10/100 Mbps vous permet d'équiper aXs GUARD de deux raccordements Ethernet supplémentaires.



9.3.7 4 x 10/100 Mbps Ethernet

Cette option vous permet d'équiper aXs GUARD de quatre raccordements Ethernet 10/100 supplémentaires

9.3.8 Leased Line X.21

Vous permet de connecter directement une 2^e ligne louée avec connexion X.21 sur aXs GUARD.

9.3.9 Leased Line V.35

Vous permet de connecter directement une 2^e ligne louée avec connexion V.35 sur aXs GUARD.

9.3.10 ISDN

Cette interface munit l'aXs GUARD d'une connexion Internet ISDN à distance (2 canaux).

9.3.11 Disques durs redondants

RAID 1 (Redundant Array of Independent (or Inexpensive) Disks) fait référence à une combinaison de deux disques durs identiques qui assurent une meilleure performance et garantissent la disponibilité du aXs GUARD. Les disques fonctionnent ensemble en permanence et se synchronisent constamment. Par conséquent, si l'un des deux ne fonctionne plus, le second dispose d'un back-up et le fonctionnement de l'aXs GUARD n'est donc jamais interrompu. Le disque tombé en panne peut aisément être remplacé et la synchronisation ensuite remise en place.

9.3.12 Alimentation redondante

Alors que l'option précédente concerne les conséquences de problèmes de disques durs, celle-ci prévoit une solution en cas de panne de l'alimentation électrique. La seconde alimentation prend automatiquement le relais si la première tombe en panne. De plus, nous vous conseillons d'utiliser cette option avec un UPS (uninterruptible power supply).

10 Entretien

10.1 Sommaire

Chaque appareil aXs GUARD est accompagné d'une garantie hardware d'un an. Durant les 3 premiers mois après la livraison, les réparations et remplacements éventuels sont effectués chez le client (Benelux). Après ces 3 mois, le client est invité à renvoyer l'appareil à Able pour réparation.



Toutefois, la société Able offre une garantie étendue présentée en détail ci-après. Le prix des polices d'entretien est fixé suivant un pourcentage sur les modules de logiciels choisis et sur le hardware tel que l'a configuré le client.

L'utilisation, les possibilités mais également les dangers que représente Internet pour la communication de votre entreprise évoluent très rapidement. Il est donc indispensable que vous puissiez disposer d'un produit qui évolue suivant vos besoins. C'est pourquoi la SA Able compte renouveler en permanence les applications, services et protections du aXs GUARD. Celui-ci contrôle à heures fixes (plusieurs fois par jour) si de nouveaux compléments (patch) ou de nouvelles versions sont disponibles et peut ainsi renouveler les modules de logiciels de façon très simple. Le nouveau complément est téléchargé et automatiquement activé parce que l'administrateur du système ne remarquera rien de l'adaptation. Lorsqu'il s'agit d'une toute nouvelle version, l'administrateur du système est averti par e-mail après le téléchargement, de la présence de la nouvelle version. Les mises à jour du software font partie des contrats de maintenance décrits ci-après.

10.2 Maintenance des programmes et réparation du hardware sur place"

Cette police étend l'application de la garantie type du hardware aXs GUARD à une maintenance complète sur place, réparation et/ou remplacement, à chaque fois pour une période de 12 mois, ainsi que la maintenance du software qui comprend les éléments suivants:

- Installation automatique via Internet de toutes les corrections relatives aux fonctions existantes;
- Installation immédiate de tout patch de sécurité ou correction d'une erreur;
- Participation au développement de nouvelles fonctions;
- Back-up automatique de tous les paramètres chez Able (pas les données d'utilisateurs);
- Support par e-mail, Internet et par téléphone à propos de, et lors de l'utilisation de aXs GUARD.

10.3 Maintenance des programmes et réparation du hardware "retour pour réparation" "

Cette option implique que toute panne de hardware survenant après les trois premiers mois sera résolue si le client envoie l'appareil par courrier rapide à ses frais à Able. La société Able s'engage à réparer ou remplacer l'appareil et à le renvoyer le jour ouvrable suivant pour être réinstallé chez le client. Les coûts de renvoi sont à charge de Able. Cette police comprend également la maintenance complète des programmes suivant la description au point 10.2

10.4 "Maintenance des programmes exclusivement"

Cette police étend l'application de la garantie type sur le hardware aXs GUARD durant les 12 premiers mois à la maintenance des programmes comme décrit ci-dessus au point 10.2



10.5 Réduction sur la police d'entretien durant la première année

Une police d'entretien ne se conclut que pour une période minimum de 2 ans. Si une des trois polices d'entretien susmentionnées est commandée en même temps que aXs GUARD, le client bénéficie d'une réduction sur le prix de la police.

11 Installation et formation

11.1 Sommaire

La société Able conçoit, développe, fabrique et distribue l'aXs GUARD depuis 1996. Depuis lors, celui-ci est devenu de fait, une référence en matière de protection et communication en Europe. L'expérience, le développement permanent, la demande des clients pour de nouvelles fonctionnalités, etc. font que les collaborateurs de Able sont experts dans le domaine de la protection de réseaux. C'est pourquoi la société Able met ses compétences à la disposition de ses clients sous la forme de consultance, de formations et d'aide à l'installation, décrites ci-dessous.

11.2 Installation sur place et formation de base (1 jour)

Il va sans dire que la société Able a une grande expérience de l'installation de aXs GUARD dans des environnements réseau très différents. Cette option inclut l'installation physique et la configuration chez le client combinée à une formation pour 3 personnes maximum.

L'aXs GUARD est livré avec les modules de logiciels activés et pourvu des interfaces réseau nécessaires. L'aXs GUARD est d'abord connecté au hub (ou switch) du réseau via l'une des interfaces Ethernet et est ensuite connecté à Internet via une interface commandée à cet effet. L'étape suivante consiste à installer les paramètres pour les divers modules de logiciels via l'afficheur sur le tableau de réglage ou via le module de configuration.

Durant la formation l'on passe en revue avec le client le menu de configuration et l'on introduit les paramètres nécessaires. Dans le même temps, le client reçoit l'information détaillée sur les options et les possibilités. Le client apprend également à configurer quelques postes de travail pour les faire fonctionner avec aXs GUARD. La configuration de tous les postes de travail n'est pas incluse dans le prix mais peut être commandée sous forme de consultance (voir ci-après). Le niveau de l'installation et de la formation est entièrement adapté au niveau et à l'expérience du client.

Il est impératif de planifier cette installation et cette formation à l'avance afin que celles-ci soient aussi efficaces que possible. Généralement, la société Able a un contact préalable avec le fournisseur d'accès pour s'informer sur une série d'éléments (par exemple les caractéristiques de la messagerie électronique) et reste à la disposition de ses clients par e-mail ou téléphone pour les aider, avant et après l'installation.



11.3 Installation sur place des interfaces, options hardware ou un upgrade

L'aXs GUARD est un système modulaire et flexible conçu pour évoluer en fonction des besoins du client. Lorsque celui-ci commande d'autres modules de programmes, il suffit très simplement de les activer en introduisant un code.

Les extensions hardware, après l'installation d'origine, telles que l'ajout d'interfaces (par exemple lors de l'installation d'une seconde ligne Internet) et les upgrades du hardware sont effectués par les collaborateurs de Able chez le client.

11.4 Formation approfondie (1/2 jour ou 1 jour)

Forte de son expertise, la société Able a mis au point des formations approfondies qui traitent de sujets TIC plus complexes. Il est possible de choisir un module pour 1/2 jour de formation ou une combinaison de modules pour un jour de formation.

Les sujets suivants y sont abordés:

Pare-feu, VPN, E-mail, contrôle d'accès à Internet et authentification des utilisateurs.

11.5 Consultance 2 heures minimum

Able met son expertise à la disposition du client sous la forme de consultance pour aider ses clients à résoudre certains problèmes de réseau ou de protection ou pour former le personnel chez le client en matière de protection de réseau par exemple.



12 A propos de Able

La SA Able, une société belge indépendante située à Boortmeerbeek, conçoit, développe et commercialise aXs GUARD connu auparavant sous le nom UNI-Box. Celui-ci fut développé dans le but de répondre aux problèmes complexes de protection qui ne cessent de croître à mesure que l'utilisation d'Internet s'intensifie dans les entreprises..

aXs GUARD est une solution complète (Tout-en-1), constituée de hardware, software et de support qui répond à tous vos besoins en matière de sécurité et communications Internet. Les clients peuvent composer leur aXs GUARD à la Carte et payent donc uniquement les options dont ils ont besoin aujourd'hui. Ce concept fait que aXs GUARD répond aux souhaits à la fois des PME et des grandes entreprises.

97% des clients qui utilisent aXs GUARD depuis 1996 sont restés fidèles à aXs GUARD. Parce qu'ils croient en sa fiabilité à long terme et sa flexibilité à l'égard des innovations. Tandis qu'aXs GUARD protège leurs communications Internet, ils peuvent dormir tranquilles et se concentrer sur leurs propres activités. Dernièrement, Data Testlab qui fait autorité, a placé aXs GUARD en tête du classement dans cette gamme et celui-ci surpasse tous ses concurrents (internationaux).

aXs GUARD est distribué dans le monde entier via un réseau dans le Benelux, au Royaume-Uni, au Portugal, les pays scandinaves et le Moyen-Orient.

En outre, la SA Able est propriétaire, avec le groupe français Ingenica, de BioWise, une entreprise spécialisée dans les solutions d'authentification biométriques.

Able SA/NV
Leuvensesteenweg 282b
3190 Boortmeerbeek
Belgique
Tél +32 15 50 44 00
Fax +32 15 50 44 09

www.able.be
www.axsguard.com
info@able.be

13 Lexique explicatif

A l'origine, l'explication des termes ci-dessous vient de: <http://www.webopedia.com>.

Terme	Définition
ADSL	Asymmetric Digital Subscriber Line : cette technologie permet d'accroître la vitesse des données sur une ligne téléphonique classique. Les débits varient de 1,5 à 9 mégabits par seconde (Mbps) à la réception, et de 16 à 640 kilobits par seconde (Kbps) à l'émission. Un modem ADSL est nécessaire pour utiliser cette application
DHCP	Dynamic Host Configuration Protocol : Ce protocole attribue des adresses IP dynamiques à un appareil du réseau. Cela signifie qu'un ordinateur peut avoir une autre adresse IP à chaque fois qu'il redémarre.
DMZ	La "Zone démilitarisée" est une zone publique du réseau qui est gérée par le firewall. Dans cette zone du réseau sont placés des serveurs qui doivent être publiquement accessibles.
DNS	Le Domain Name System (ou Service) est un service Internet qui traduit les noms en adresses IP
E-mail	Courrier électronique
FTP	File Transfer Protocol : protocole permettant de déplacer les fichiers via Internet.
HTTP	Hyper Text Transfer Protocol : c'est un protocole sous-jacent pour la reproduction graphique des données.
HTTPS	Hyper Text Transfer Protocol Secure : un protocole permettant d'envoyer des données sécurisées sur Internet, le protocole SSL correspondant établit une connexion sécurisée entre le poste de travail et le serveur Web. Ce protocole est surtout destiné à garantir à l'utilisateur le respect de sa vie privée.
IDS	Intruder Detection System : système de détection des intrusions sur le système, qui contrôle tout le flux des données entrantes et sortantes en ce qui concerne les schémas suspects signalant d'éventuelles attaques.
IMAP4	Internet Mail Access Protocol Version 4 : protocole pour la lecture des e-mails. Les messages sont conservés sur le serveur de courrier pendant la consultation.
IP	Internet Protocol : IP détermine le format des paquets de données, appelés aussi datagrammes, et les schémas d'adresses.
IPSec	Internet Protocol Security Protocol : abréviation d'IP Security, un ensemble de protocoles pour l'échange sécurisé des données sur la couche IP. Il est généralement utilisé pour la mise en place de réseaux privés virtuels (VPN).



Terme	Définition
ISDN	Integrated Services Digital Network : une norme internationale de communication pour l'envoi de sons, d'images et de données via les lignes téléphoniques numériques. L'ISDN soutient des vitesses de données de 64 Kbps (64 000 bits par seconde).
ISP	Internet Service Provider : l'entreprise qui donne accès à Internet pour un coût mensuel fixe.
LAN	Local Area Network : un réseau informatique dans un environnement local, par exemple, le bâtiment de l'entreprise.
LDAP	Lightweight Directory Access Protocol : un protocole pour demander des fichiers d'adresses e-mail.
NAT	Network Address Translation : est une norme Internet par laquelle un ensemble d'adresses IP du réseau local utilisent une ou plusieurs adresses IP publiques.
NTP	Network Time Protocol : un protocole standard Internet qui permet la synchronisation parfaite de l'horloge des ordinateurs en réseau.
PC	Personal Computer (généralement "compatible IBM").
POP3	Post Office Protocol Version 3 : protocole utilisé pour relever le courrier électronique.
PPTP	Point-to-point tunneling protocol : une technologie pour la mise en oeuvre de réseaux virtuels privés (VPN).
PSTN	Public Switched Telephone Network : communication téléphonique analogique.
RAID	Redundant Array of Independent Disks : deux ou plusieurs disques durs qui sont connectés, pour se dupliquer l'un l'autre en permanence ou pour accroître les performances.
RAS	Remote Access Services : une application permettant d'établir une connexion avec un réseau informatique, par une ligne téléphonique ou par Internet.
SMTP	Simple Mail Transfer Protocol : un protocole utilisé pour envoyer des messages e-mails entre serveurs de courrier.
SSL	Secure Socket Layer : un protocole d'encryptage développé par Netscape pour garantir la confidentialité des données qui sont envoyées par Internet.
TCP	Transmission Control Protocol : c'est le protocole de TCP/IP qui établit et contrôle la connexion entre deux ordinateurs.



Terme	Définition
UPS	Uninterruptible Power Supply : une alimentation électrique basée sur une batterie qui fournit momentanément du courant, pendant une panne d'électricité.
VPN	Virtual Private Network : réseau virtuel privé : la connexion virtuelle d'un ordinateur externe au réseau ou la connexion virtuelle de réseaux par Internet, l'établissement de la connexion et le transfert des données intervenant de manière encryptée.
Webmail	La lecture des messages e-mails avec le navigateur web.



14 Index

à la Carte Configurator.....	4
Able.....	23
Accès Internet.....	8
Alimentation redondante.....	19
Connexions Internet multiples.....	9
Consultance.....	22
Contrôle et IDS.....	12
Disques durs redondants.....	19
DNS public.....	12
Extension pare-feu DMZ.....	12
Fax.....	11
Feed-back.....	15
Fichier d'Adresses centralisé (LDAP).....	10
Filtre Web.....	14
Filtres e-mail.....	14
Filtres spam.....	14
Firewall SPICT.....	12
Gestion de la Bande passante.....	13
Hardware Entreprise supplémentaire.....	18
Haute disponibilité.....	13
http accelerating proxy et SMTP relay.....	8
Installation et formation.....	21
Intégration Active Directory.....	11
Interface Administrateur.....	6
Interface de connexion Internet (toutes plate-formes).....	17
Lecture des boîtes aux lettres externes.....	10
Lexique explicatif.....	24
Logging.....	8, 15
Logiciel Client IPSec SSH.....	8
Logiciel de base.....	6
Maintenance	
réduction.....	21
réparation retour pour réparation.....	20
réparation sur place.....	20
Maintenance des programmes exclusivement.....	20
Messagerie électronique sur le Web.....	10
Plate-formes	
Entreprise 1500.....	16
Entreprise 2000.....	16
Entreprise 2750.....	16
Entreprise 3500.....	17
Office 1000.....	16
Office 800.....	16
SOHO 500.....	16
points de performance aXs GUARD.....	5
Reverse HTTP et FTP proxy.....	13
Scanneur de contenu et filtre.....	13
Serveur de Messagerie électronique.....	10
Serveur Web.....	11
Services Accès à Distance.....	12
SMTP relay.....	9
Statistiques.....	15
Trend Micro HTTP et SMTP antivirus.....	13
utilisateurs, ordinateurs, connexions.....	5
VPN.....	8
Workgroup Connector.....	10