IBM SecureWay FirstSecure

Planification et intégration

Version 2

SCT7-EHFR-00

IBM SecureWay FirstSecure

Planification et intégration

Version 2

SCT7-EHFR-00

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'«Annexe. Remarques» à la page 99.

Première édition – octobre 1999

Réf. US : SCT7-EHFR-00

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

Table des matières

Figures

Tableaux

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
Alt Gr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de ce manuel

IBM SecureWay FirstSecure (FirstSecure) est une solution complète qui permet de réaliser les tâches suivantes :

- Sécuriser tous les aspects d'un réseau ouvert sur le Web ou d'autres réseaux
- Utiliser les équipements e-business existants (des offres modulables permettent d'ajouter des fonctions de sécurité dans le cadre d'un déploiement planifié)
- Réduire le coût des investissements nécessaires pour mener une activité e-business sécurisée

Ce manuel décrit FirstSecure et ses composants, et vous guide dans la planification de l'utilisation de ces produits.

Les produits auxquels ce manuel fait référence sont commercialisés progressivement. Ces produits ne sont pas nécessairement tous disponibles en même temps, ni dans tous les pays. Contactez votre représentant IBM habituel pour connaître la disponibilité de ces produits.

Illustrations du manuel

Les illustrations contenues dans ce manuel sont proposées à titre d'exemples dans le cadre de la planification. Chaque illustration ne montre qu'une des innombrables possibilités de configuration que vous pouvez choisir pour installer les serveurs, les clients et les applications en fonction des besoins de votre entreprise.

Le format des illustrations dépend du type du manuel que vous consultez :

- La plupart des illustrations de la version PDF du manuel sont simplifiées pour économiser l'espace disque et s'imprimer plus rapidement.
- Celles de la version imprimée sont plus complètes.

Dans les deux cas, les illustrations montrent les mêmes fonctions et comportent des légendes et des mentions identiques.

A qui s'adresse ce manuel ?

Ce manuel est destiné aux administrateurs système en charge de la planification et de l'intégration des dispositifs de sécurité pour les systèmes utilisant le Web. A ce titre, le lecteur est supposé bien connaître son réseau et ses applications e-business.

Organisation du manuel

Ce manuel comprend les parties suivantes :

- La «Partie 1. Présentation générale de FirstSecure» à la page 1 offre une vue d'ensemble de FirstSecure, en décrivant ses différents composants et les offres disponibles.
- La «Partie 2. Planification d'un réseau sécurisé e-business» à la page 15 couvre la planification d'un réseau e-business sécurisé.
- La «Partie 3. Remarques sur l'installation et l'intégration des composants» à la page 53 décrit les conditions d'installation et d'intégration des produits de la solution FirstSecure.
- Le «Chapitre 16. Documentation des produits FirstSecure» à la page 87 décrit l'ensemble de la documentation fournie avec FirstSecure.
- Le «Glossaire» à la page 103 explique la signification des termes de sécurité utilisés dans ce manuel.

Le manuel propose également la bibliographie des documents disponibles pour chaque produit.

An 2000

La compatibilité de la solution IBM SecureWay FirstSecure avec l'an 2000 se caractérise de la façon suivante :

Composants de IBM SecureWay FirstSecure développés par IBM

Ces produits sont conçus pour passer l'an 2000 sans incident. Utilisés conformément aux recommandations de leurs manuels, ils peuvent accepter, traiter et générer des données comportant des dates comprises dans et entre le vingtième et le vingt-et-unième siècle dans la mesure où toutes les ressources (matériels, logiciels tiers et applications propriétaires) utilisées simultanément peuvent gérer ces dates sans incident.

Composants développés par d'autres fabricants

Les fabricants des autres produits ont certifié à IBM que leurs produits étaient prêts pour passer l'an 2000 sans incident. Cependant, IBM ne peut ni certifier, ni garantir, la compatibilité de ces produits avec le passage à l'an 2000. Pour toute question relative au passage à l'an 2000 pour ces produits, contactez le fabricant concerné. Les informations concernant les produits et services non développés par IBM sont des "nouvelles publications", au sens prévu par les dispositions du Information and Readiness Disclosure Act, basées sur les informations fournies par d'autres sociétés sur les produits et services qu'elles proposent. Ces fabricants ont certifié à IBM que leurs produits étaient prêts pour passer l'an 2000 sans incidents. Cependant, IBM ne peut ni certifier, ni garantir, la compatibilité de ces produits avec le passage à l'an 2000. Pour toute question relative au passage à l'an 2000 pour ces produits, contactez le fabricant concerné. IBM n'a pas vérifié le contenu de ces nouvelles

publications et décline toute responsabilité s'agissant de l'exactitude et de l'exhaustivité des informations qu'elles contiennent.

Service et prise en charge

Contactez IBM pour obtenir des services et une prise en charge pour tous les produits de l'offre SecureWay FirstSecure. Les manuels de certains de ces produits font référence à des services d'assistance autres que ceux d'IBM. Si vous avez acquis ces produits dans le cadre de l'offre SecureWay FirstSecure, contactez IBM pour bénéficier d'une assistance.

Conventions

Ce manuel utilise les conventions typographiques suivantes :

- Le **Gras** indique le nom d'un élément sélectionné, le nom d'une commande, le texte entré par l'utilisateur ou un exemple dans le corps du texte.
- L'`espacement fixe` indique un exemple (chemin d'accès ou nom de fichier donné à titre d'exemple) ou le texte affiché à l'écran.

Informations disponibles sur le Web

Des informations mises à jour concernant FirstSecure sont disponibles sur le site Web www.ibm.com/software/security aux adresses suivantes :

IBM SecureWay FirstSecure
www.ibm.com/software/security/firstsecure

La documentation se trouve à l'adresse
www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director
www.ibm.com/software/security/policy

La documentation se trouve à l'adresse
www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server
www.ibm.com/software/boundary

La documentation se trouve à l'adresse
www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority
www.ibm.com/software/security/trust

La documentation se trouve à l'adresse
www.ibm.com/software/securitytrust/library

Un document élaboré par l'ITSO, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498–00 se trouve à l'adresse www.ibm.com/redbooks sur l'Internet.

Partie 1. Présentation générale de FirstSecure

Cette partie donne une présentation générale de la solution FirstSecure et de ses composants. Elle contient une description sommaire de chaque produit.

Cette partie décrit également les services d'accompagnement d'IBM.

Chapitre 1. Présentation de FirstSecure

IBM SecureWay FirstSecure fait partie des solutions intégrées de sécurité proposées par IBM. FirstSecure comprend un ensemble de produits intégrés permettant de :

- créer un environnement e-business sécurisé ;
- simplifier la planification de la sécurité pour réduire son coût ;
- mettre en oeuvre des règles de sécurité plus facilement ;
- créer un environnement e-business plus fonctionnel.

Les composants de FirstSecure permettent de mettre en place des systèmes de protection contre les virus, de détection des intrusions, de contrôle des accès, de contrôle des données échangées, de chiffrement, de certificats numériques, de pare-feu et des boîtes à outils de développement d'applications. Ces fonctions sont assurées à la fois par des produits de la famille IBM SecureWay et par des produits d'autres fabricants, réunissant ainsi les meilleures techniques de sécurité actuellement disponibles. De plus, des Offres de services d'accompagnement FirstSecure sont disponibles pour les composants FirstSecure sélectionnés. Les différents composants de la solution FirstSecure sont les suivants :

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- Public Key Infrastructure, intégré à IBM SecureWay Trust Authority
- IBM SecureWay Toolbox

Dans la mesure où FirstSecure réunit plusieurs produits pouvant être installés séparément, vous pouvez planifier la sécurisation de votre environnement de façon contrôlée. Vous pouvez sécuriser une première zone dans votre réseau, évaluer les améliorations, puis passer progressivement aux autres zones. Ce système, plus simple et plus économique, permet aussi de déployer des applications et des ressources Web plus rapidement.

Utilité de FirstSecure

Vos données et vos ressources sont des éléments vitaux de votre e-business. Les produits réunis dans la solution FirstSecure apporte les services suivants :

Autorisation
Chaque utilisateur doit respecter les règles établies. Le service

d'autorisation n'autorise l'accès aux systèmes, aux données, aux applications et aux réseaux qu'à des utilisateurs dûment autorisés.

Contrôle d'activité
Le contrôle d'activité permet d'identifier qui a fait quoi et quand. Vous pouvez grâce à lui identifier l'auteur d'une action et les opérations réalisées pendant une période donnée.

Protection
Vous pouvez être assuré que le système tient ses promesses en matière de sécurité. Cette garantie vous permet de démontrer et de prouver que le niveau de sécurité prétendu est effectivement en vigueur.

Disponibilité
Le système est disponible lorsque vous en avez besoin. Cet aspect vous permet de proposer des systèmes, des données, des réseaux et des applications utilisables en permanence par les employés, les fournisseurs, les partenaires et les clients.

Administration
Vous pouvez définir les règles qui gouvernent votre réseau. Les outils d'administration permettent de définir, de gérer, de surveiller et de modifier les informations rattachées aux règles de gestion.

Les mesures de protection mises en oeuvre peuvent reposer sur des règles de sécurité appliquées à l'ensemble de l'entreprise pour créer un maillage de sécurité couvrant l'intégralité des réseaux, des systèmes et des applications de votre société. La présence d'un seul maillon vulnérable entre deux composants de ce maillage peut rendre inutile l'ensemble du dispositif.

Ce manuel relie chaque module de SecureWay aux autres modules dans les différents systèmes de protection décrits.

Modules de la solution FirstSecure

Les composants de FirstSecure peuvent s'obtenir sous la forme d'un ensemble de produits complémentaires ou sous la forme de produits connexes vendus séparément. Chacun de ces produits est lui-même composé de plusieurs modules. Vous pouvez commencer par installer n'importe lequel de ces produits puis compléter votre dispositif pour obtenir au final une solution de sécurité intégrée.

Policy Director

Policy Director est la pièce maîtresse de votre plan de sécurité. Policy Director apporte des services d'autorisation et de gestion qui permettent d'assurer une sécurité totale des ressources Web dans le cadre d'intranets et d'extranets distants. Policy Director fournit des fonctions d'authentification, d'autorisation, de sécurisation des données et de gestion des ressources. Ce

produit s'articule avec les applications Internet standard pour mettre en oeuvre des intranets fonctionnels et sécurisés. Policy Director comprend :

- Services de sécurité
- Console de gestion
- Serveur de gestion
- Gestionnaire de sécurité (NetSEAL et WebSEAL)
- NetSEAT Client
- Répartiteur des services de répertoire
- Serveur d'autorisations (support des applications tiers)

Policy Director est disponible pour Windows NT, AIX et Solaris.

Reportez-vous au «Chapitre 5. Planification de l'installation de Policy Director dans un réseau» à la page 31 pour une description plus complète de Policy Director.

SecureWay Boundary Server

Le produit SecureWay Boundary Server offre des fonctions de protection, d'administration et de contrôle d'activité des applications Web dédiées au e-business. Il est vital de sécuriser les frontières séparant les différentes entités d'un réseau. Ces frontières peuvent par exemple séparer des services (développement / ressources humaine), le réseau du siège et celui des sites locaux, ou encore, le réseau de la société et ses applications Web, d'une part, et les clients et fournisseurs d'autres part. Pour bénéficier d'une réelle sécurité des frontières, vous devez contrôler à la fois qui et quelles informations pénètrent dans votre réseau et en sortent.

Cette section décrit les modules composant SecureWay Boundary Server. Reportez-vous au «Chapitre 12. Remarques sur la procédure et les conditions d'installation de SecureWay Boundary Server» à la page 59 pour plus d'informations sur la planification et l'intégration de ce produit.

IBM SecureWay Firewall

IBM SecureWay Firewall, également appelé IBM Firewall, garantit la sécurité des opérations de e-business en contrôlant les communications échangées avec le réseau Internet. IBM Firewall remplit les trois fonctions vitales d'un pare-feu, filtrage, serveur relais et passerelle de niveau circuit, pour offrir le meilleur niveau de sécurité et de flexibilité.

ACE/Server

Le produit ACE/Server, développé par Security Dynamics, comprend des jetons SecurID (licences pour deux utilisateurs et deux jetons). ACE/Server ajoute au pare-feu IBM SecureWay Firewall une liaison d'administrateur et une connexion de *réseau privé virtuel*.

MIMEsweeper for IBM SecureWay Release 2

Le produit MIMEsweeper, développé par Content Technology, comprend des composants axés sur la sécurité des transactions Internet. MAILsweeper contrôle le courrier électronique pour empêcher la sortie de données confidentielles hors du e-business et l'entrée de courriers non autorisés.

WEBsweeper empêche les données Web indésirables de pénétrer dans votre système e-business. Il analyse les données en entrée et ne laisse passer que celles des applets Java, des codes exécutables et des sites Web autorisés.

SurfinGate

Le produit SurfinGate, créé par Finjan Software Ltd., est une solution de traitement des codes mobiles adaptée au e-business. Dans la mesure où des codes mobiles arrivent de façon automatique et quotidienne dans votre réseau e-business, à partir de sources extérieures à votre intranet, la protection des pare-feu n'est plus suffisante. Le programme SurfinGate protège votre réseau contre les attaques des codes Java, ActiveX et JavaScript. Il identifie le risque d'une attaque, loin des ressources sensibles, avant qu'elle n'atteigne le réseau. Les données suspectes sont mises en quarantaine pour que vous puissiez les analyser avant de les accepter.

Intrusion Immunity

Le produit Intrusion Immunity se compose de programmes dédiés à la détection des intrusions et à la protection des données. Reportez-vous au «Chapitre 13. Remarques sur la procédure et les conditions d'installation de Intrusion Immunity» à la page 67 pour plus d'informations sur les conditions d'installation de Intrusion Immunity. Intrusion Immunity comprend Tivoli Cross-Site for Security et Norton AntiVirus.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security permet de détecter les intrusions dans les systèmes potentiellement vulnérables. Tivoli Cross-Site for Security permet les opérations suivantes :

- Installer des agents Cross-Site for Security dans le réseau pour rapporter les incidents suspects au serveur de gestion de Cross-Site for Security
- Afficher les données de l'intrusion dans des états prédéfinis et personnalisés
- Détecter et journaliser les activités non autorisées ou suspectes en temps réel
- Configurer les agents de sécurité pour réduire le nombre de fausses alertes

Norton AntiVirus

Le programme Norton AntiVirus, développé par Symantec Corporation, figure parmi les meilleurs logiciels antivirus du monde. Norton AntiVirus peut être exécuté en permanence en arrière-plan pour protéger les ordinateurs contre les virus transportés par les documents joints aux courriers électroniques, les

contrôles ActiveX, les applets Java, les disquettes, les CD-ROM, ou encore les fichiers téléchargés à partir d'Internet ou d'un autre réseau. Norton AntiVirus peut mettre en quarantaine les fichiers infectés. Vous pouvez configurer Norton AntiVirus pour vous informer automatiquement des mises à jour du produit et des nouveaux virus découverts.

Public Key Infrastructure

IBM FirstSecure utilise les normes de cryptographie et d'interdépendance fonctionnelle Public Key Infrastructure (PKI) au travers du produit IBM SecureWay Trust Authority.

SecureWay Trust Authority est une solution de sécurité qui permet la délivrance, le renouvellement et la révocation des certificats numériques. Ces certificats peuvent être utilisés avec un large éventail d'applications Internet afin d'authentifier les utilisateurs et de sécuriser les communications. Trust Authority repose sur les spécifications PKI (*Public Key Infrastructure*) développées par le groupe de travail IETF (*Internet Engineering Task Force*). Ce système présente les caractéristiques suivantes :

- Support des serveurs IBM AIX et Microsoft Windows NT
- Autorité d'enregistrement (AE)
- Autorité de certification (AC)
- Interfaces utilisateur permettant de demander et d'administrer les certificats
- *IBM SecureWay Directory* (intégré)
- Sous-système d'*audit*
- Support du coprocesseur de chiffrement SecureWay 4758
- Support des *cartes à puce*

Cette infrastructure permet de gérer l'ensemble du cycle des certificats (enregistrement et première certification, mise à jour des paires de clés et des certificats, liste des certificats et des révocations de certificat, procédure de révocation des certificats). Pour plus d'informations, reportez-vous au «Chapitre 14. Remarques sur la procédure et les conditions d'installation de Public Key Infrastructure» à la page 75.

Toolbox

Le produit FirstSecure Toolbox comprend un ensemble d'utilitaires (boîtes à outils) de sécurité intégrés ou pouvant s'intégrer aux principaux composants de la solution FirstSecure. Les boîtes à outils permettent de réaliser les tâches suivantes :

- Intégrer vos applications à la solution FirstSecure
- Personnaliser les solutions et les applications avec FirstSecure
- Créer des applications ISV et OEM utilisant FirstSecure

Les API des boîtes à outils de FirstSecure Toolbox gèrent les fonctions de sécurité suivantes :

- Services d'autorisation
- Services de gestion et de certification
- Services d'annuaire
- Services de protocole SSL (Secure Sockets Layer)
- Services de sécurisation et de cryptographie KeyWorks
  - API IBM Key Recovery Service Provider 1.1.3.0 . Le composant IBM Key Recovery Service Provider permet de restaurer des informations codées.
  - IBM Key Recovery Server 1.1.3.0. Le produit IBM Key Recovery Server 1.1.3.0 est une application qui, sous réserve d'une requête autorisée, peut restaurer des informations codées dont la clé est indisponible, a été perdue ou altérée.

    Ces deux boites à outils contiennent des interfaces standard permettant aux applications d'accéder à des services de sécurité critiques. Les modules de sécurité peuvent également utiliser ces interfaces pour accéder au composant Toolkit. La conception de ces interfaces standard repose sur l'architecture CDSA (Common Data Security Architecture). Les deux boîtes à outils sont disponibles en version Windows NT, Solaris et AIX.

Offres de services d'accompagnement FirstSecure

Les services d'accompagnement FirstSecure peuvent vous aider à installer, configurer et démarrer votre solution FirstSecure plus rapidement et plus de efficacement. Ces services, facturables séparément, sont fournis par IBM et assurés par une équipe de consultants expérimentés. Les services d'accompagnement FirstSecure comprennent un module d'accompagnement à l'installation de FirstSecure et des services d'installation rapide pour chaque produit. IBM propose également des services d'intégration de système pouvant être adaptés à votre environnement personnel.

Pour obtenir plus d'informations et connaître les tarifs de ces services, prenez contact avec votre partenaire commercial IBM.

Chapitre 2. Nouveautés de l'édition 2

Cette nouvelle édition simplifie la planification et l'installation des produits de la solution IBM SecureWay FirstSecure. Les différents produits sont mieux intégrés, d'autres ont été ajoutés et la gestion et le contrôle sont davantage centralisés.

Policy Director

Les nouveautés de Policy Director sont les suivantes :

- Prise en charge d'IBM SecureWay Directory pour le stockage des données de droit d'accès des utilisateurs et des groupes ;
- Dernières mises à jour de la spécification de l'API d'autorisation développée par le Open Group ;
- Possibilité de définir et de modifier les droits d'accès des utilisateurs relais d'IBM Firewall à l'aide de la console de gestion de Policy Director ;
- Service d'acquisition de droits d'accès (SAD) de Policy Director permettant d'utiliser des services d'authentification externes ;
- Prise en charge de l'authentification par certificat de côté client à l'aide du nouveau service d'acquisition de droits d'accès de Policy Director ;
- Possibilité d'élaborer un service d'acquisition de droits d'accès personnalisé à l'aide de l'interface IDL (Interface Definition Language) qui permet d'utiliser WebSEAL en association avec le SAD de Policy Director. Policy Director apporte également des fonctions de serveur standard qui permettent de gérer les fonctions de son serveur SAD telles que le démarrage, l'enregistrement du serveur et la gestion des signaux.
- Possibilité d'utiliser la transmission par tunnel SSL en plus de la transmission par tunnel GSS ;
- Gestion des règles de connexion et de mot de passe à l'aide de l'interface de ligne de commande de Policy Director ;
- Gestion des utilisateurs, des groupes et des ressources SSO (destinations) à l'aide de la console de gestion ou de l'interface de ligne de commande de Policy Director ;
- Utilitaire Web de gestion des mots de passe des ressources SSO ;
- Procédure d'installation intégrée.

SecureWay Boundary Server

Les nouveautés de SecureWay Boundary Server sont les suivantes :

- Interface utilisateur graphique de configuration permettant de relier certaines fonctions de SecureWay Boundary Server et de Policy Director ;
- Nouveau guide des tâches de configuration permettant de relier certaines fonctions de SecureWay Boundary Server et de Policy Director.

Nouveautés d'IBM SecureWay Firewall pour AIX et NT

Les améliorations d'IBM SecureWay Firewall (IBM Firewall) sont les suivantes :

Optimisation du serveur relais de messagerie sécurisée

Le module IBM Firewall Secure Mail Proxy contient désormais les nouvelles fonctions suivantes :

- Algorithmes de gestion des multidiffusions permettant de bloquer les envois d'émetteurs identifiés (liste d'exclusions), vérification de la validité et de la possibilité de répondre aux messages (méthodes connues de blocage des messages indésirables), limitation du nombre de destinataires par message, limitation de la taille maximale des messages ;
- Dispositif de lutte contre le détournement d'adresse avec intégration de méthodes d'authentification complexes ;
- Support de l'interception SNMP et de la base d'informations de gestion MADMAN ;
- Suivi des messages avec possibilité de surveillance des messages échangés entre le pare-feu et Domino.

Optimisation du protocole Socks version 5

Le protocole Socks version 5 permet désormais l'authentification par nom d'utilisateur/mot de passe (UNPW), par question/réponse (CRAM) et par plusieurs plug-in d'authentification.

La fonction de journalisation a été améliorée et permet à présent de classifier les messages des fichiers journaux et de définir différents niveaux de journalisation.

Serveur relais HTTP

IBM SecureWay Firewall contient désormais une solution de serveur relais HTTP complète dérivée du produit IBM Web Traffic Express (WTE). Le serveur relais HTTP gère les requêtes des navigateurs au moyen du pare-feu IBM Firewall, ceci éliminant le besoin d'un serveur de sockets pour la navigation sur le Web. Les utilisateurs peuvent accéder aux informations de l'Internet sans menacer la sécurité de leurs réseaux internes ni nécessiter l'installation d'un serveur relais HTTP dans leur environnement client.

Service d'accès à distance

Le service d'accès à distance (SAD) Windows NT permet d'établir des connexions de réseau par modem, par RNIS, ou par support X.25 avec le protocole PPP (Point-to-Point Protocol). NDISWAN est un gestionnaire de réseau intégré au service SAD qui convertit les données PPP sous-jacentes en un format proche de celui d'un réseau local Ethernet.

Amélioration d'IBM SecureWay Firewall pour AIX

Le produit IBM SecureWay Firewall pour AIX comporte de nombreuses extensions :

Support renforcé d'IPSec

Support renforcé d'IPSec avec prise en charge de nouveaux en-têtes. Ce support permet également de gérer l'interdépendance fonctionnelle entre plusieurs serveurs IBM et les routeurs ainsi que de nombreux RPV non IBM utilisant les nouveaux en-têtes.

Support des multiprocesseurs

Les utilisateurs du pare-feu peuvent désormais utiliser les fonctions avec multiprocesseurs du système RS/6000 pour moduler et accroître les performances.

Optimisation des filtres

Optimisation des performances et de la flexibilité pour la configuration. Vous pouvez notamment augmenter les performances du pare-feu IBM SecureWay Firewall en choisissant l'emplacement des différents types de règle de filtrage. Un indicateur de fréquence indique le nombre d'utilisations d'une connexion.

Conversion d'adresse de réseau (NAT)

Support du mappage d'adresse ″plusieurs à un″. Cette conversion permet d'associer plusieurs adresses de réseau privé non enregistrées à une unique adresse enregistrée utilisant des numéros de port déterminés.

Assistant de configuration

La configuration initiale du pare-feu IBM Firewall se fait à l'aide d'un assistant de configuration. L'assistant de configuration permet aux utilisateurs connaissant peu le fonctionnement du pare-feu IBM Firewall de mettre en place une configuration opérationnelle rapidement après l'installation.

Network Security Auditor

Le programme NSA (Network Security Auditor) analyse les serveurs du réseau et le pare-feu IBM Firewall et recherche les failles dans la sécurité ou les erreurs de configuration. La nouvelle version est plus rapide et plus puissante.

Nouveautés de MIMEsweeper for IBM SecureWay Release 2

Les améliorations de MAILsweeper sont les suivantes :

- Recherche de mots clés pour bloquer les courriers indésirables et empêcher les données sensibles de quitter le site de votre société ;
- Blocage des courriers envoyés en multi-diffusion ;
- Blocage de certains types de fichier en envoi et réception pour des utilisateurs ou des groupes ;
- Blocage ou mise en file d'attente des fichiers selon leur taille pour éviter l'encombrement du réseau.

Les améliorations de WEBsweeper sont les suivantes :

- Blocage de l'accès à certains sites sans relation avec l'activité de l'entreprise ;
- Protection contre les extractions de documents frauduleuses par HTML ou de données d'adresse électronique et de site par le biais de cookies.

Nouveautés de SurfinGate

Les nouveautés de SurfinGate sont les suivantes :

- Analyse du contenu des scripts JavaScript
- Surveillance des performances critiques
- Gestion optimisée des règles d'administration
- Prise en charge des protocoles FTP et HTTPS
- Intégration par plug-in avec le serveur relais HTTP
- Blocage des téléchargements pour certains types de fichier exécutable

Intrusion Immunity

Le produit Intrusion Immunity comprend désormais Tivoli Cross-Site for Security.

Nouveautés de Tivoli Cross-Site for Security

Le produit Tivoli Cross-Site for Security permet de détecter les intrusions. Il permet de surveiller les attaques contre le réseau et de protéger l'intégrité des données de votre e-business.

Nouveautés de Norton AntiVirus Solution Suite

Norton AntiVirus Solution Suite 3.0.4 comprend les versions mises à jour suivantes :

- Norton AntiVirus 5.02 pour Windows 95/98 et Windows NT Workstation
- Norton AntiVirus 5.02 pour Windows NT Server
- Norton AntiVirus pour IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 pour Lotus Notes 2.0
- Norton AntiVirus pour Lotus Notes 2.0
- Norton AntiVirus pour Microsoft Exchange 1.5.2

Public Key Infrastructure

Le produit Public Key Infrastructure intègre désormais le composant Trust Authority. Ce composant contient les éléments suivants :

- Un assistant d'installation destiné à faciliter l'installation sur Windows NT ;
- Une configuration prédéfinie pour le coprocesseur de chiffrement 4758 (vous pouvez modifier cette configuration) ;
- Un assistant de configuration qui contrôle l'exactitude des données avant le lancement des programmes de configuration en arrière-plan ;
- Des message d'erreur et une fonction de génération d'états ;
- Une documentation en ligne comprenant une aide contextuelle pour les assistants de configuration, l'interface de l'autorité d'enregistrement et une application client pour l'entité finale.

IBM SecureWay Toolbox

Les nouveautés de Toolbox sont les suivantes :

- API et documentation de Policy Director ;
- API des services d'annuaire ;
- API et documentation de Public Key Infrastructure (PKIX) ;
- IBM Key Recovery Server 1.1.3.0 (disponible uniquement en anglais).

Partie 2. Planification d'un réseau sécurisé e-business

La deuxième partie de ce manuel couvre la planification d'un réseau e-business sécurisé.

Les chapitres qui suivent décrivent les aspects généraux de la sécurité et des transactions dans l'Internet avant d'expliquer le fonctionnement des produits FirstSecure dans le cadre d'un réseau e-business.

Cette partie comprend les chapitres suivants :

- Le «Chapitre 3. Présentation générale d'un réseau e-business» à la page 17 décrit les caractéristiques d'un réseau e-business conventionnel et les types d'utilisateur, de ressource et d'interactions que l'on trouve dans ce type de réseau. Quelles que soient les fonctions de votre réseau, les questions et les besoins en matière de sécurité sont souvent les mêmes.
- Le «Chapitre 4. Planification de l'installation de FirstSecure dans un réseau e-business» à la page 29 explique le fonctionnement des produits FirstSecure par rapport au réseau.
- «Chapitre 5. Planification de l'installation de Policy Director dans un réseau» à la page 31
- «Chapitre 6. Planification de l'installation de SecureWay Boundary Server dans un réseau» à la page 35
- «Chapitre 7. Planification de l'installation de Intrusion Immunity dans un réseau» à la page 41
- «Chapitre 8. Planification de l'installation de Public Key Infrastructure dans un réseau» à la page 47

Chapitre 3. Présentation générale d'un réseau e-business

Un réseau e-business se compose de ressources : des données et des bases de données, des utilisateurs, des clients et des fournisseurs, des programmes, des équipements matériels, des données d'entreprises, etc. Examinons quelques-uns de ces domaines pour identifier les besoins en termes de sécurité.

L'Internet est un monde complexe. Les données le traversent de serveur en serveur et d'utilisateur en utilisateur, via des chemins indéfinis susceptibles de changer d'une transmission à une autre.

Vos transmissions de données par Internet se fondent dans l'ensemble des transactions en cours dans le réseau. Sur leur route, des données vitales pour votre entreprise peuvent passer par n'importe quel serveur, quelque soit sa localisation. N'importe quel utilisateur connecté à l'Internet peut tenter d'accéder à vos ressources, à vos employés et à vos données. Outre les transactions légitimes liées à l'éducation, le commerce ou les loisirs, l'Internet véhicule également des codes dangereux, qu'ils le soient délibérément ou non. La figure 1 à la page 18 donne une présentation générale de l'Internet et explique comment vos transactions rejoignent celles des autres utilisateurs du réseau.

FirstSecure permet de séparer vos transactions des autres et d'assurer leur sécurité.

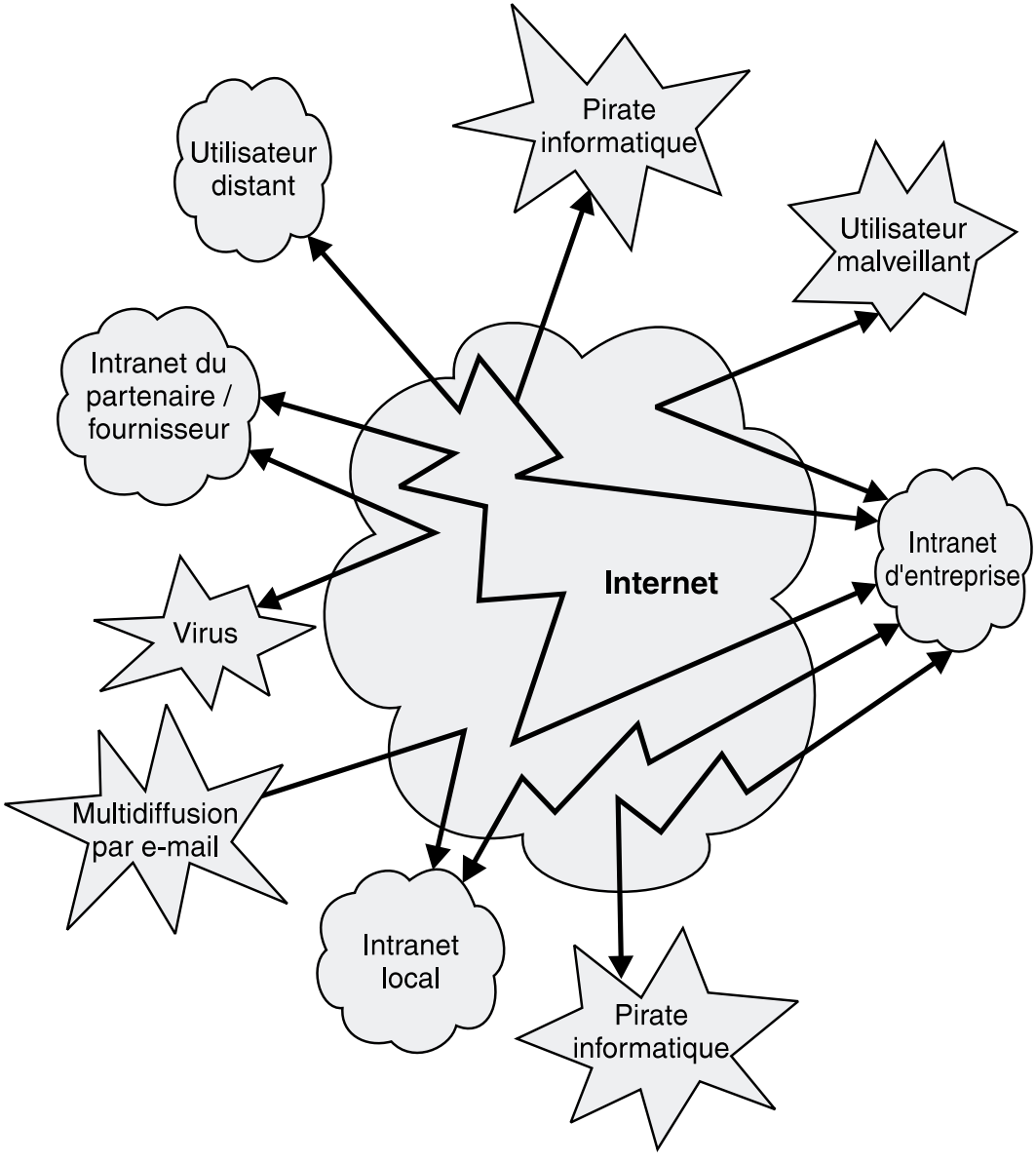


Figure 1. Présentation générale de l'activité de l'Internet

Cette situation ne peut naturellement pas vous satisfaire. Vous préféreriez celle de la figure 2 à la page 19 : une solution Internet sécurisée par FirstSecure.

L'Internet idéal protégé par FirstSecure

La plupart de vos transactions e-business transitent par l'Internet. Toutefois, vous ne désirez pas que vos données rejoignent un vaste rassemblement d'informations hétéroclites visibles par n'importe qui à partir d'un simple ordinateur domestique. La figure 2 montre l'Internet tel que vous aimeriez qu'il soit.

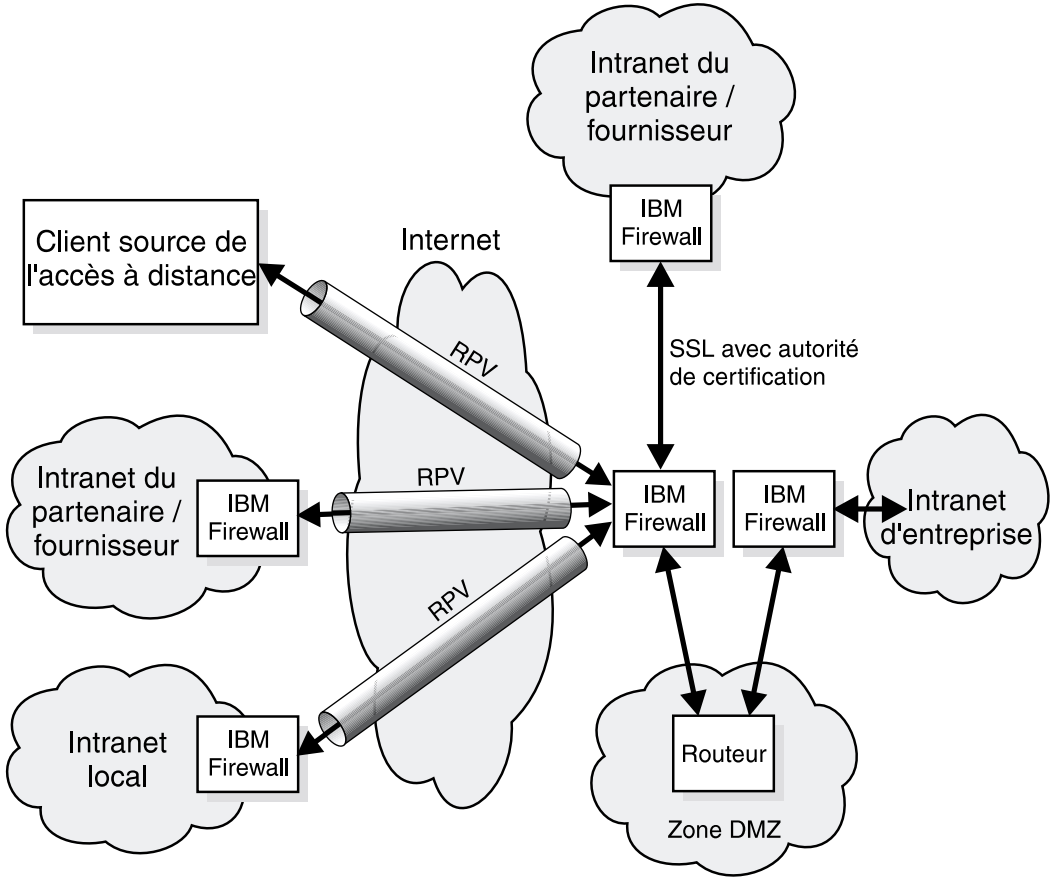


Figure 2. L'Internet idéal

Même si l'Internet propose nombre d'informations intéressantes, vous désirez néanmoins protéger votre entreprises contre certaines applications, données et types d'accès. Vous voulez notamment vous assurer que :

- vos employés ne soient pas distraits de leurs missions ;
- ils ne soient pas importunés par des messages sans intérêt ;
- les données sensibles de votre entreprise ne la quittent pas.

Réseau privé virtuel

Un réseau privé virtuel (RPV) repose sur le principe d'une connexion privée, inaccessible aux tiers par le biais de l'Internet. La figure 3 illustre un réseau privé virtuel conventionnel. La connexion avec chaque utilisateur final est protégée contre l'intrusion d'utilisateurs ou d'applications non désirés. Les produits FirstSecure, tels que IBM SecureWay Firewall, permettent de créer et d'administrer des RPV.

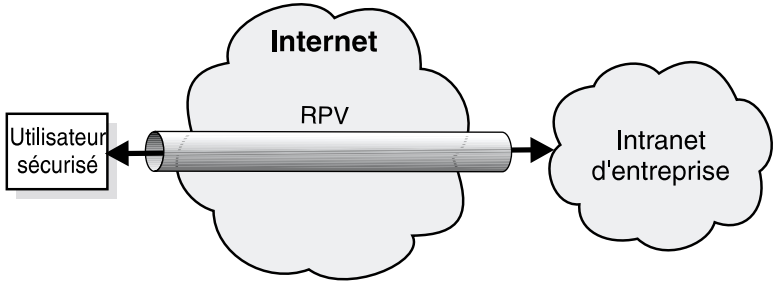


Figure 3. Un réseau privé virtuel conventionnel

Zone DMZ

La *zone DMZ* (zone démilitarisée) contient toutes les ressources auxquelles les utilisateurs externes peuvent accéder. Pour vous assurer que seuls les utilisateurs autorisés puissent accéder à la zone DMZ et aux ressources qui leur sont destinées, vous utiliserez IBM Firewall, MIMEsweeper et d'autres produits de la famille FirstSecure. La légitimité des transactions entrant ou quittant la zone DMZ doit être contrôlée.

Le catalogue de votre entreprise peut être dans la zone DMZ pour que vos clients puissent le consulter. Vous pouvez également y placer des documents d'information décrivant votre société. En revanche, les composant FirstSecure veilleront à ce que seuls les utilisateurs sécurisés accèdent aux informations situées au delà de la zone DMZ.

La figure 4 à la page 21 illustre une zone démilitarisée conventionnelle.

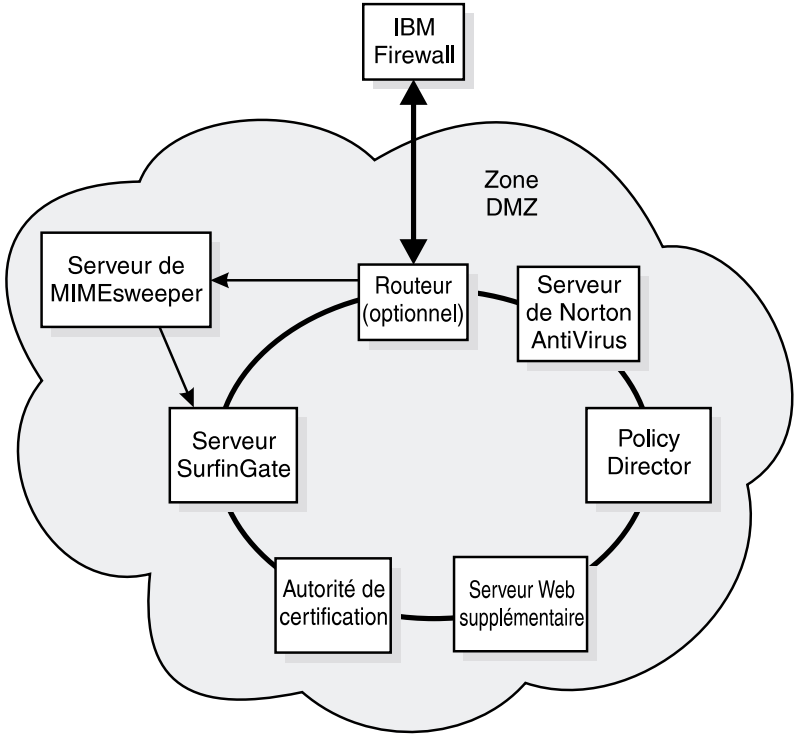


Figure 4. Zone démilitarisée standard avec ses ressources système

A mesure que vous développez des applications sécurisées, vous pouvez utiliser la zone DMZ pour évaluer la protection de votre intranet avant de laisser le public accéder à ces applications.

Examinons à présent le genre d'informations pour lequel vous utilisez l'Internet et votre intranet.

Intranet d'entreprise standard

L'intranet de votre entreprise est le lieu où votre société communique avec elle-même. Il contient des informations et des ressources non accessibles par l'Internet. Vos employés partagent des données, s'échangent des courriers, accèdent à des ressources de l'entreprise telles que des bases de données, des imprimantes et des scanners. La figure 5 à la page 22 illustre un intranet d'entreprise conventionnel.

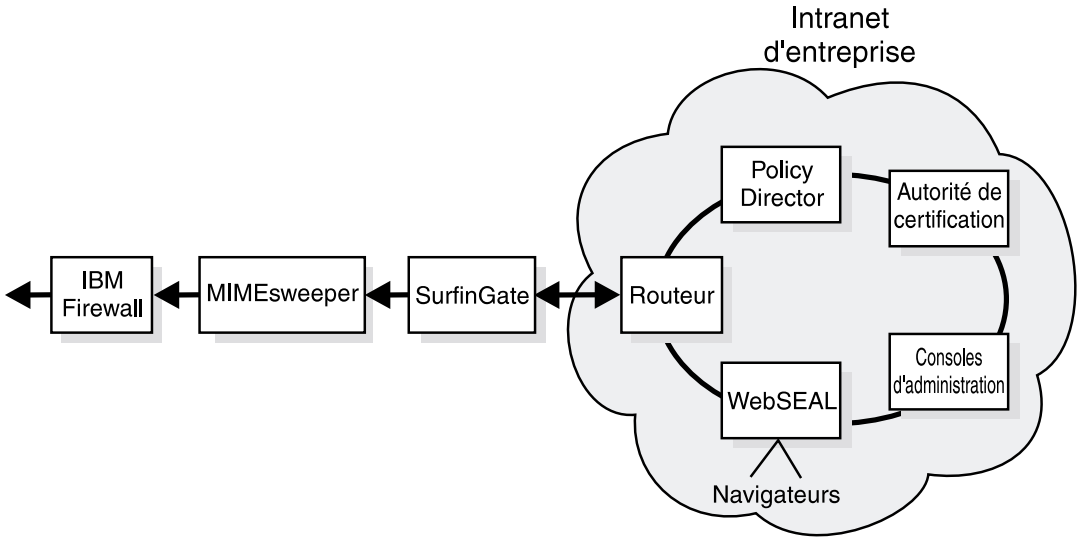


Figure 5. Un intranet d'entreprise standard

Vous devez vous assurer que les données confidentielles de votre société ne quittent pas celle-ci et que seules les personnes habilitées à utiliser ces données peuvent effectivement y accéder. En revanche, vos clients devront pouvoir accéder à d'autres données et les utiliser. Par exemple, dans le cas d'une banque, vos clients doivent pouvoir consulter le solde de leur compte sans pouvoir accéder aux renseignements concernant le personnel. Le pare-feu IBM Firewall protège la confidentialité des informations privées.

Les produits IBM FirstSecure préservent la sécurité de l'intranet. Policy Director permet de définir les règles d'accès. IBM SecureWay Trust Authority permet d'authentifier l'identité des utilisateurs. Tivoli Cross-Site for Security permet de détecter les tentatives d'accès frauduleuses aux ressources de l'intranet.

Intranet de succursale standard

Les employés des succursales ont besoin d'accéder aux mêmes données et ressources que ceux travaillant au siège de l'entreprise. Toutefois, les liaisons téléphoniques servant à envoyer ou recevoir des informations sont lentes et ne sont pas protégées contre les interférences malveillantes. Utiliser l'Internet peut occasionner des réductions de coût et apporter plus de sécurité aux transactions. La figure 6 à la page 23 illustre une communication entre une succursale et le siège central par le biais de l'Internet.

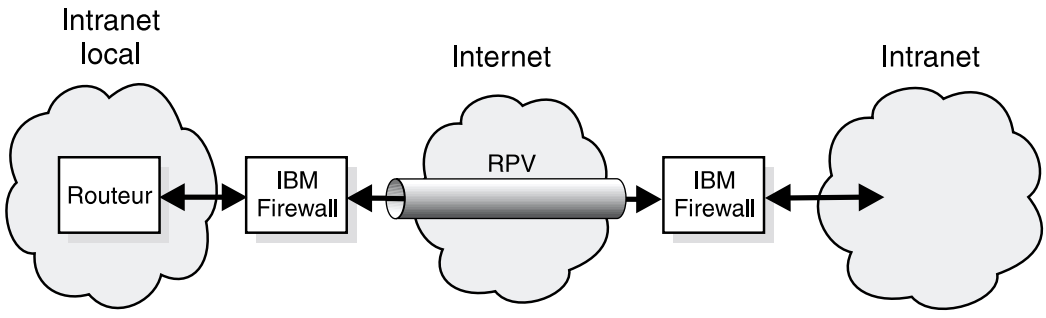


Figure 6. Succursale reliée au siège par le biais d'un réseau privé virtuel.

Vous désirez que vos transmissions et vos données soient aussi sécurisées que si elles s'échangeaient à l'intérieur de l'entreprise. Le *réseau privé virtuel* se comporte comme un tunnel traversant l'Internet. Dans cette situation, vous utilisez l'Internet comme s'il s'agissait d'un intranet privé.

Utilisateur distant standard

Certains employés peuvent, occasionnellement ou d'une façon permanente, travailler à l'extérieur du siège. Ces employés peuvent accéder au réseau de l'entreprise via l'Internet au moyen d'une liaison commutée ou spécialisée.

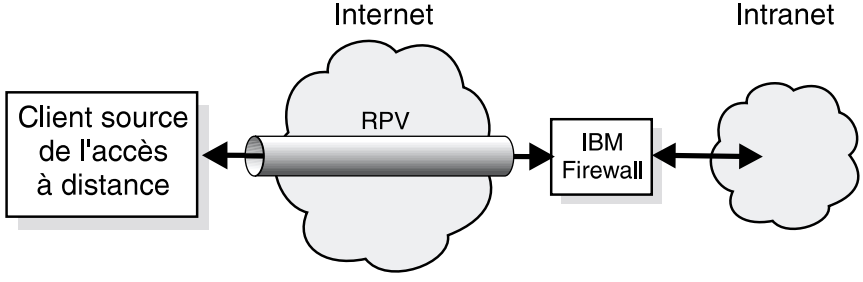


Figure 7. Client distant relié au siège via un réseau privé virtuel en accès commuté

Le pare-feu IBM Firewall protège les transmissions de l'employé.

Intranet de partenaires commerciaux standard

Votre entreprise sera plus efficace si vos partenaires commerciaux et vos fournisseurs peuvent accéder directement à certaines de vos données. Un fournisseur peut être autorisé à consulter le niveau des stocks et à vous envoyer de nouveaux produits à des niveaux donnés. Un autre partenaire pourra être autorisé à accéder à certains enregistrements. Votre comptable peut avoir besoin d'accéder aux données fiscales sans toutefois pouvoir accéder aux autres données. La figure 8 à la page 24 et la figure 9 à la page 24

illustrent la configuration standard d'un intranet ouvert aux fournisseurs et aux autres partenaires commerciaux d'une entreprise. Les transactions commerciales doivent pouvoir transiter par l'Internet comme s'il s'agissait d'une connexion privée.

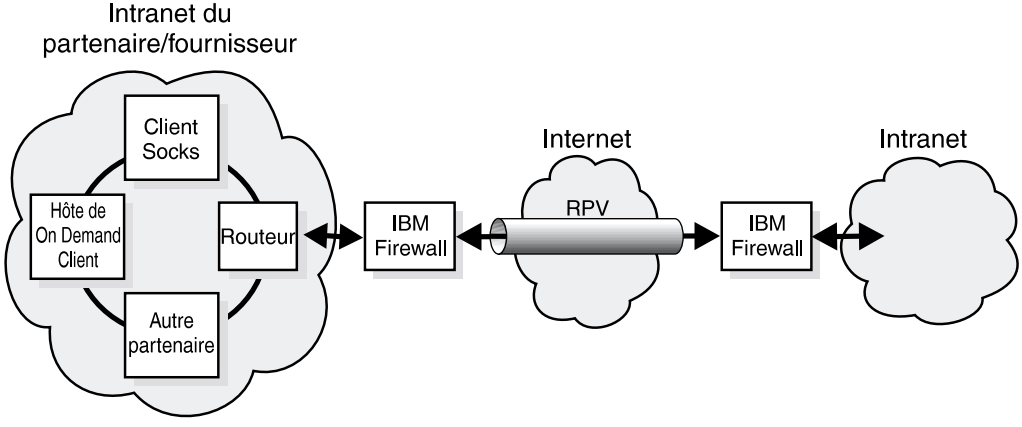


Figure 8. Configuration standard d'un intranet ouvert aux partenaires commerciaux et utilisant un réseau privé virtuel

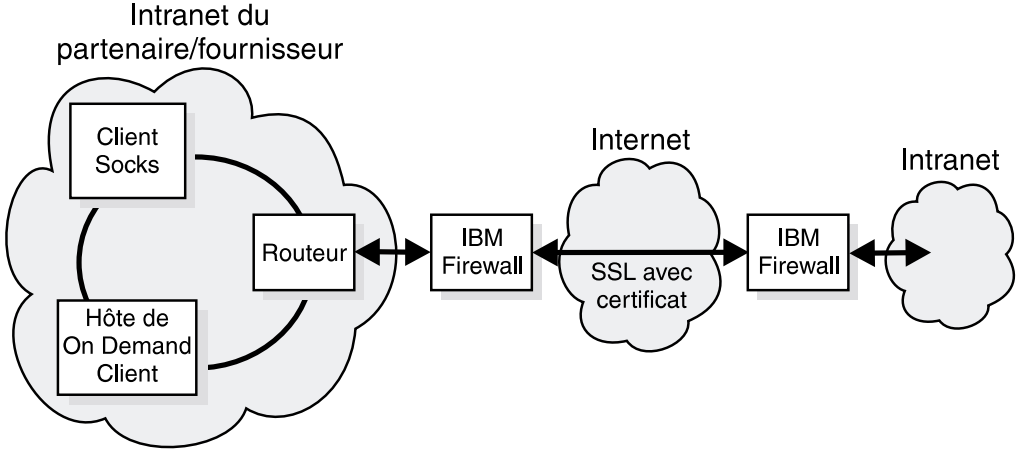


Figure 9. Configuration standard d'un intranet ouvert aux partenaires commerciaux et utilisant le protocole SSL

Ce partenaire utilise le protocole SSL au lieu d'un réseau privé virtuel. Dans cette situation, les transmissions sont codées d'un bout à l'autre de la transaction (l'utilisateur pourrait aussi utiliser un RPV pour ajouter un niveau de sécurité supplémentaire).

Ces utilisateurs autorisés doivent être protégés des autres utilisateurs, des interférences malveillantes et des intrus. Vous devez protéger leurs transmissions contre les écoutes et les émetteurs non autorisés. Vous devez également faire en sorte que ces utilisateurs n'accèdent qu'aux données qui leur sont destinées. Pour finir, vous voulez être certain que chacun de ces utilisateurs est bien celui qu'il prétend être et non un imposteur.

Données et bases de données

Les données comptent parmi les ressources les plus précieuses d'une entreprise. Certaines données e-business sont destinées à être utilisées par tous les utilisateurs d'Internet. Par exemple, un vendeur de matériel peut communiquer l'état de ses stocks et ses prix pour un service d'achat en ligne. Un détaillant en confection peut proposer un catalogue de vêtements en ligne avec des choix de styles, de couleurs et de tailles.

Avant de donner accès aux données, vous devez établir l'identité du demandeur et savoir pourquoi il souhaite ces informations. Le produit Trust Authority, qui permet de délivrer des certificats aux utilisateurs sécurisés, répond à cet objectif.

Autres domaines à protéger

Ce manuel ne couvre pas les autres aspects de la sécurité des réseaux. Notez cependant que vous devez aussi penser aux questions suivantes :

- Sécurité du site, accès et sortie, segmentation du réseau
- Sécurité physique des ordinateurs portables, des ordinateurs personnels (PC) et des stations de travail et autres matériels de même nature
- Sécurité des personnes
- Protection juridique de la responsabilité et autres aspects légaux
- Procédures de gestion telles que la gestion des clés, le contrôle des informations, la veille technologique et la formation en matière de sécurité

Système d'exploitation

La plupart des systèmes d'exploitation sont conçus pour offrir une accessibilité avancée et une palette de fonctions diversifiée. La démarche la plus sûre consiste à ne garder que les fonctions strictement nécessaires à l'exécution des tâches indispensables. Vous pouvez donc envisager de désinstaller ou de désactiver toutes les fonctions du système d'exploitation à protéger des intrus.

Utilisateurs standard

L'Internet connaît différents types d'utilisateur, plus ou moins opportuns. Dans le contexte du e-business, les utilisateurs qui vous intéressent sont des clients exécutant des recherches et des achats en ligne. Le dirigeant d'un

e-business désire également que ses partenaires commerciaux puissent accéder à des données définies, par exemple pour consulter l'état des stocks, pour lancer des fabrications, ou pour commenter des projets et des activités de l'entreprise. Naturellement, les employés d'un e-business doivent aussi pouvoir accéder aux données dont ils ont besoin pour remplir leurs missions.

L'Internet connaît aussi des utilisateurs dont un e-business n'a pas besoin : les pirates, les multidiffuseurs, les propagateurs de virus et les utilisateurs cherchant à accéder aux données sensibles. Ces utilisateurs peuvent exister au sein même de votre e-business.

Avant de lui donner accès à une quelconque ressource, vous devez savoir qui est l'utilisateur qui se présente, quel type d'accès aux données et aux applications lui accorder et comment garder la trace des utilisations.

Applications et création d'applications

Les applications peuvent être conçues avec des fonctions de sécurité intégrées. Vous pouvez notamment utiliser le codage des données transmises, la certification des utilisateurs demandant l'accès ainsi que les journaux d'audit des utilisateurs et des transactions.

Les API du module Toolbox permettent d'ajouter des fonctions de sécurité à vos applications.

Sécurité des matériels

Les serveurs et les banques de données font partie des éléments d'un système sécurisé. Bien que ce manuel ne détaille pas la sécurité des matériels, vous devez penser à assurer la sécurité physique des serveurs et des stations de travail utilisés pour gérer la sécurité de votre réseau.

Trust Authority et la sécurité des matériels

Cette section porte plus spécialement sur le composant Trust Authority mais s'applique également à tous les autres produits de la famille FirstSecure.

Isolation de la zone à protéger

Installez la machine du serveur dans une pièce isolée, réservée à l'administrateur de la sécurité. Si possible, cette pièce devra disposer de cloisons renforcées, d'une porte robuste, en bois ou en métal, et d'un plafond sans panneaux amovibles. Le plancher de la pièce devra également être surélevé pour éviter le risque d'électrocution par le sol en cas d'incendie.

Entretien de la zone à protéger

La pièce doit être équipée d'un système d'alimentation de secours, d'éclairages, de détecteurs de mouvements et d'un système d'air conditionné. Vous devez également prévoir sa ventilation pour lui assurer une température constante malgré la chaleur dégagée par les équipements.

Contrôle de l'accès à la zone protégée

L'accès à la zone physique peut être protégé de plusieurs manières : par l'utilisation de badges ou de verrous avec digicode. Pour empêcher les manipulations frauduleuses par une personne isolée, vous pouvez également établir des procédures de contrôle demandant la présentation d'une accréditation par au moins deux personnes habilitées.

Vous pouvez également établir un système de surveillance de la pièce pour consigner chaque accès et chaque personne y ayant pénétré. Pour une sécurité maximale, installez des détecteurs de mouvements à l'intérieur comme à l'extérieur de la pièce.

Contrôle des communications

Le serveur Trust Authority ne doit comporter aucun port ouvert en surnombre. Vous devez configurer le système de manière à ce qu'il n'écoute que les requêtes passant par les ports explicitement affectés aux applications Trust Authority actives.

Assurez la sécurité des matériels de votre e-business selon les procédures en vigueur dans votre entreprise.

Chapitre 4. Planification de l'installation de FirstSecure dans un réseau e-business

Les chapitres de cette deuxième partie du manuel explique le lien unissant les produits de la solution FirstSecure à votre système e-business. Il développe les configurations des illustrations du «Chapitre 3. Présentation générale d'un réseau e-business» à la page 17. Chaque produit est décrit dans ses grandes lignes. Pour une information plus complète sur un produit donné, reportez-vous à sa documentation. Les configurations décrites ne sont proposées qu'à titre d'exemples.

Chaque approche de déploiement des ressources suit les mêmes principes de base :

1. Réglez tous les composants du réseau sur une heure identique pour faciliter les procédures d'audit et les rendre plus précises.
2. Commencez à installer et à tester les composants à partir de l'intranet.
3. Une fois la configuration de l'intranet terminée, installez les applications à l'intérieur de la zone DMZ.
4. Les transactions entre l'intranet et la zone DMZ doivent franchir un pare-feu.
5. Installez les application Internet externes et testez-les avec des données d'évaluation.
6. Installez un pare-feu entre l'Internet et la zone DMZ.
7. Laissez les utilisateurs accéder au réseau.

Planification d'un système FirstSecure complet

A titre de suggestion, voici l'ordre dans lequel vous pouvez déployer les produits FirstSecure dans votre réseau. Cet ordre a l'avantage de simplifier la procédure d'installation. Pour plus d'informations sur les configurations logicielles et matérielles requises pour chaque produit ainsi que sur les aspects relatifs à l'intégration des produits, voir la «Partie 3. Remarques sur l'installation et l'intégration des composants» à la page 53. Consultez également les sections couvrant les conditions et les instructions d'installation de chaque produit. Des informations plus récentes sur de nombreux produits sont également disponibles sur l'Internet. La section «Informations disponibles sur le Web» à la page xv répertorie les sites WEB proposant des informations sur FirstSecure. Le document *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498 décrit de façon plus détaillée d'autres possibilités d'approche.

1. Planifiez les conditions de sécurité dont vous aurez besoin.
2. Installez Policy Director pour satisfaire ces conditions.
3. Créez et testez votre application de serveur. Conservez-la à l'intérieur de l'intranet d'entreprise pour le moment, sans l'ouvrir sur l'Internet.
4. Installez le pare-feu IBM Firewall chargé de protéger l'application serveur.
5. Installez SurfinGate dans la zone démilitarisée.
6. Dans cette zone démilitarisée (ou zone DMZ), installez également MIMEsweeper et Norton AntiVirus pour protéger les applications lorsqu'elles seront accessibles par l'Internet. Avant d'autoriser les transactions externes, configurez-les pour qu'elles utilisent systématiquement vos serveurs.
7. Installez Tivoli Cross-Site for Security pour détecter et parer les tentatives d'intrusion.
8. Dans la zone démilitarisée, installez les composants suivants :
   - Serveurs Web
   - Serveur de catalogues Web
   - Serveur d'inventaires Web
   - Applications client
   - Applications client sécurisées
   - Un ou plusieurs agents Cross-Site for Security

   Testez toutes vos applications à l'abri du pare-feu avant d'autoriser les transactions externes. Testez les règles que vous avez définies à l'aide de l'utilitaire NSA de SecureWay Boundary Server.
9. Installez une instance du pare-feu IBM SecureWay Firewall pour protéger les logiciels installés dans la zone démilitarisée. Pour que vous puissiez tester l'installation avant de l'ouvrir au public, la configuration par défaut ne doit pas accepter les transactions externes.«»
10. Installez Trust Authority et délivrez des certificats aux utilisateurs sécurisés.
11. Une fois l'évaluation terminée, autorisez l'accès aux applications par l'Internet.
12. Exécutez le programme Network Security Auditor, à partir d'un poste étranger au système, pour tester les règles d'accès avant d'annoncer l'ouverture du réseau au public.
13. Consultez les journaux d'audit créés par les programmes de FirstSecure pour vérifier l'absence d'incidents non décelés.
14. Continuez de vérifier les journaux d'audit et ajoutez des agents Cross-Site for Security à mesure que vous installez de nouvelles applications à votre réseau.

Chapitre 5. Planification de l'installation de Policy Director dans un réseau

Sur la base de règles d'accès définies, FirstSecure permet de contrôler de manière centralisée des environnements Web hétérogènes. Dans un environnement permettant aux utilisateurs d'accéder à plusieurs serveurs Web d'arrière-plan via un navigateur, le composant Policy Director offre les fonctions suivantes :

- Connexion unique pour chaque utilisateur Web
- Vérification des identités
- Contrôle d'autorisation pour les utilisateurs demandant accès à des pages Web protégées

Policy Director permet d'autoriser et de sécuriser les éléments suivants :

- Echanges TCP/IP tels que les transactions HTML, Telnet et POP3
- Applications tiers telles que les systèmes de base de données
- Outils de gestion de réseau
- Applications développées en interne

Dans le contexte de FirstSecure, les utilisateurs peuvent être authentifiés dans Policy Director à l'aide des méthodes suivantes :

- Authentification de base via le protocole SSL (Secure Sockets Layer)
- Connexion SSL par formulaires
- Connexion SSL avec certificats de client
- Connexion Kerberos

FirstSecure contrôle ensuite l'accès des utilisateurs authentifiés à chaque objet Web et service du réseau et limite l'accès des utilisateurs non autorisés à un ensemble de ressources restreint.

Déploiement de Policy Director

Policy Director gère les relations entre les utilisateurs et les groupes d'une part, et les ressources d'autre part. La console de gestion de Policy Director permet de :

- définir les utilisateurs et les groupes habilités à utiliser les ressources ;
- définir les objets nécessitant une protection (objets Web, ports TCP, méthodes, ou interfaces) ;

- définir le mode d'accès aux ressources et les règles protégeant celles-ci (droit de lecture, de modification, de gestion, d'exécution, de suppression, etc.).

Le tableau qui suit décrit les configurations les plus courantes pour l'installation des composants de Policy Director. Déterminez celle qui convient le mieux pour votre réseau. Sélectionnez ensuite ces composants pendant la procédure d'installation.

Pour plus d'informations, reportez-vous au manuel *IBM SecureWay Policy Director - Guide de configuration et d'utilisation*.

Configuration	**Composants installés**
Une seule instance du serveur de gestion pour l'ensemble du domaine sécurisé. Le serveur de gestion réside seul sur une machine dédiée. Il administre la base de données primaire des autorisations du domaine sécurisé, la duplique à travers le domaine sécurisé et gère les données d'emplacement des autres serveurs Policy Director définis dans le domaine sécurisé.	Serveur de gestion uniquement
Un serveur WebSEAL. Cette solution vise à protéger un espace Web. WebSEAL prend en charge des serveurs d'arrière-plan, pour permettre une accessibilité avancée et offrir un recours en cas de panne d'un serveur.	Gestionnaire de sécurité avec WebSEAL
Un serveur NetSEAL. Un serveur NetSEAL a pour mission de sécuriser un réseau privé virtuel et d'assurer le contrôle d'accès aux services des réseaux existants et des réseaux tiers.	Gestionnaire de sécurité avec NetSEAL
Combinaison d'un serveur WebSEAL et d'un serveur NetSEAL.	Gestionnaire de sécurité avec WebSEAL et NetSEAL
Un serveur permettant aux applications tiers d'appeler le service d'autorisation de Policy Director.	Serveur d'autorisations
Un serveur offrant un environnement de développement pour créer des applications tiers utilisant l'API d'autorisation.	Serveur d'autorisations et ADK
Un serveur proposant l'ensemble des services mentionnés dans les configurations précédentes.	Tous les composants

Policy Director est un système de sécurité distribuée dont les composants peuvent être installés selon diverses configurations, sur un ou plusieurs ordinateurs. Les sections qui suivent donnent une présentation générale de l'installation des composants de Policy Director dans un réseau. Les instructions d'installation sont détaillées dans le manuel *IBM SecureWay Policy Director - Guide de configuration et d'utilisation*.

1. Installez le serveur de sécurité de Policy Director.

   Le serveur de sécurité doit être installé sur au moins une machine du domaine sécurisé pour créer un domaine sécurisé par Policy Director. Reportez-vous aux manuels couvrant l'installation et l'administration de votre plate-forme ainsi qu'aux ressources de support technique disponibles.

   Les autres serveurs peuvent fonctionner avec des configurations ne comprenant que des clients DCE (ou NetSEAT pour les systèmes Windows NT).
2. Installez et configurez le serveur de SecureWay Directory (LDAP).
3. Installez Policy Director.
   - Le serveur de sécurité de Policy Director doit être installé en premier (voir l'étape 1).
   - Toute installation de serveur Policy Director requiert le module de base de Policy Director.
   - S'il s'agit du *premier* ou du *seul* ordinateur du domaine sécurisé, vous devez y installer le serveur de gestion.

     Dans le cas contraire et si le domaine sécurisé contient déjà un serveur de gestion, vous ne devez pas en installer un autre. Un domaine sécurisé ne doit contenir qu'une seule instance du serveur de gestion.
   - WebSEAL, NetSEAL et le serveur d'autorisations tiers sont des composants optionnels.
   - Le gestionnaire de sécurité s'associe à WebSEAL pour gérer le composant serveur HTTP WebSEAL et le contrôle d'accès avancé, et à NetSEAL pour gérer le contrôle d'accès TCP/IP standard.
4. Installez la console de gestion.

   La console de gestion nécessite d'installer soit un client DCE, soit NetSEAT pour Windows NT (voir l'étape 1).
5. Les applications développées avec le kit de développement Authorization ADK impliquent les conditions suivantes :
   - Vous devez posséder le progiciel Policy Director.
   - Installez le module IVAuthADK sur la machine hébergeant l'application.
   - Le système d'exploitation utilisé par l'application doit être associé, soit à un client DCE, soit à NetSEAT pour Windows NT.

- Le domaine sécurisé dans lequel l'application est exécutée doit contenir au moins un serveur d'autorisations. Un environnement de développement standard comprend le serveur d'autorisations et, sur le même système, le kit de développement Authorization ADK.

Chapitre 6. Planification de l'installation de SecureWay Boundary Server dans un réseau

FirstSecure assure la sécurité des applications Web exploitant des normes de sécurité telles que le protocole SSL, SOCKS et IPSec.

Si l'environnement d'exploitation comporte des connexions entre deux parties du réseau n'ayant pas le même niveau de sécurité, le composant SecureWay Boundary Server de FirstSecure peut répondre aux besoins ci-dessous.

- Connexions Internet protégées réduisant les risques d'accès non autorisé au réseau privé
- Infrastructures d'extranet à grande échelle pour un partage sélectif des données avec les partenaires commerciaux et les fournisseurs
- Utilisation d'Internet ou d'autres segments peu sécurisés du réseau en tant que réseau privé virtuel, pour garantir la confidentialité des messages lors de leur transmission

SecureWay Boundary Server utilise des techniques de filtrage des adresses réseau et des contenus, de serveur relais et de passerelle de niveau circuit. En combinant ces techniques, SecureWay Boundary Server contrôle les communications entre des réseaux n'ayant pas le même niveau de sécurité, ce qui permet d'effectuer des opérations e-business en toute sécurité, dans le respect des règles définies.

SecureWay Boundary Server comprend :

- IBM SecureWay Firewall (avec ACE/Server)
- MIMEsweeper for IBM SecureWay Release 2
- SurfinGate 4.05 for Windows NT
- Additifs de gestion des règles

Reportez-vous à la figure 10 à la page 36 pour une présentation générale des flux de données dans une installation avec SecureWay Boundary Server.

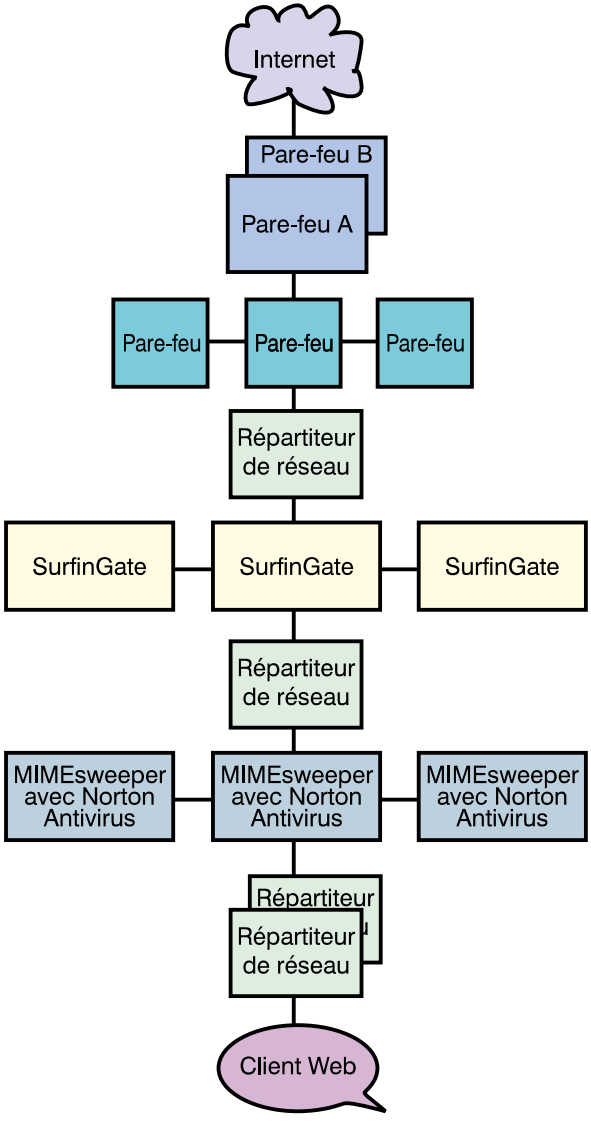


Figure 10. Présentation générale des flux de données dans les produits de SecureWay Boundary Server

Déploiement de IBM SecureWay Firewall

IBM SecureWay Firewall, également appelé IBM Firewall, contrôle les communications échangées avec le réseau Internet. IBM utilise cette technique de pare-feu pour protéger ses propres ressources.

Reportez-vous à la section «Remarques sur les composants de SecureWay Boundary Server» à la page 61 pour plus d'information sur l'installation.

L'installation d'un réseau implique la prise en compte des aspects suivants :

- La nécessité de se connecter à Internet tout en interdisant les accès non autorisés au réseau, aux applications et aux données de l'entreprise
- Le risque d'une utilisation abusive de vos ressources réseau par des utilisateurs internes
- Le déploiement d'une infrastructure d'extranet à grande échelle destinée aux partenaires commerciaux et aux fournisseurs en dépit du coût élevé de la gestion de la configuration
- Le coût élevé des liaisons spécialisées pour la connexion des filiales
- Une productivité insuffisante imputable à la mauvaise qualité des communications avec les partenaires commerciaux et les fournisseurs (inefficacité, lenteur ou mauvaise compatibilité)
- Le coût élevé que représente la gestion des logiciels en langues étrangères

IBM Firewall apporte une solution à ces questions. Grâce au pare-feu, qui ne laisse passer que les transmissions autorisées, IBM Firewall protège votre réseau des intrus. Pour une meilleure protection, un logiciel de recherche des failles est livré avec IBM Firewall, afin de *renforcer la sécurité* du serveur de IBM Firewall en empêchant les pirates de franchir le pare-feu. Les adresses IP et la configuration du réseau interne sont inaccessibles à partir du réseau non sécurisé. Toutes les données échangées à travers le pare-feu sont consignées et peuvent servir à créer des rapports sur les activités des utilisateurs.

IBM Firewall et ses applications de configuration de RPV vous permettent de déployer et de gérer des infrastructures de réseau privé virtuel à grande échelle et à moindre coût. Les études menées sur les réseaux ont montré que les clients pouvaient utiliser des réseaux privés virtuels pour réaliser des économies importantes par rapport au coût des liaisons spécialisées.

IBM Firewall permet d'installer un pare-feu pour chaque filiale et d'utiliser un tunnel IPSEC pour relier les filiales entre elles via Internet.

IBM Firewall est fourni avec ACE/Server, un produit de Security Dynamics Technologies Inc. qui fournit des services d'authentification centralisés et fiables permettant de limiter aux seuls utilisateurs autorisés l'accès aux fichiers, aux applications et aux communications d'un réseau d'entreprise. Associé à la technique brevetée du jeton SecurID de Security Dynamics Technologies, ACE/Server crée une véritable barrière contre les accès non autorisés. Le système d'authentification repose sur deux contrôles : les utilisateurs doivent *posséder* une carte SecurID et *connaître* leur numéro d'identification personnel (PIN) pour pouvoir être authentifiés.

Déploiement de MIMEsweeper

MIMEsweeper, produit de Content Technologies Ltd., effectue une analyse du contenu des données Internet et intranet pour identifier les menaces éventuelles et protéger les utilisateurs du réseau.

Reportez-vous à la section «Remarques sur les composants de SecureWay Boundary Server» à la page 61 pour plus d'information sur l'installation de ce produit.

MIMEsweeper comporte deux modules de base, MAILsweeper et WEBsweeper, qui offrent deux types de protection aux utilisateurs. A mesure qu'arrivent des messages ou des données du Web, MIMEsweeper vérifie l'adresse de l'émetteur et du destinataire et désassemble les fichiers. MAILsweeper et WEBsweeper analysent ensuite les différents éléments obtenus afin d'assurer la protection du réseau privé.

FirstSecure contient à la fois MAILsweeper 4.0 et WEBsweeper 3.2_5. Chaque module peut être installé, configuré et utilisé séparément.

MAILsweeper peut accomplir les tâches suivantes :

- Utiliser les programmes de détection de virus pour s'assurer que les fichiers désassemblés ne contiennent pas de virus
- Détecter et bloquer les macros dangereuses
- Rechercher des mots clés pour :
  - détecter toute atteinte aux bonnes moeurs dans les messages électroniques ;
  - garantir la confidentialité des données sensibles.
- Bloquer les multidiffusions de messages électroniques afin de limiter l'engorgement du réseau et ne pas compromettre la productivité des employés
- Empêcher des individus ou des groupes d'envoyer ou de recevoir certains types de fichiers, AVI ou MPEG, par exemple
- Intercepter ou retarder la transmission des fichiers, selon un critère de taille, en attendant que le réseau puisse mieux absorber le trafic

WEBsweeper peut accomplir les tâches suivantes :

- Interdire aux salariés l'accès à certains sites sans intérêt professionnel
- Contribuer à lutter contre la perte accidentelle de données sensibles ou confidentielles

De plus, MIMEsweeper contient une interface API qui permet d'intégrer les filtres d'URL tiers.

MIMEsweeper apporte donc une protection efficace contre les risques d'atteinte à la sécurité liés à l'utilisation d'Internet.

Remarque : Si vous avez acquis MIMEsweeper for IBM SecureWay Release 2 dans le cadre de l'offre SecureWay FirstSecure ou SecureWay Boundary Server, vous devez prendre contact avec IBM pour les services et le support techniques, même si la documentation de MIMEsweeper fournit les coordonnées de Content Technologies.

Déploiement de SurfinGate

SurfinGate, un produit de Finjan Software Ltd., contrôle les codes mobiles (code JavaScript, applets Java et contrôles ActiveX) pour protéger le réseau de toute altération (modification, suppression ou détournement illicites des données). SurfinGate contrôle les codes mobiles au niveau de la passerelle et identifie les codes dangereux avant qu'ils ne pénètrent dans votre réseau. La transmission du code mobile peut être interrompue de manière sélective, ou autorisée pour un utilisateur ou un département donné. Le code peut être admis ou refusé sur le réseau de l'entreprise, selon la fonction qu'il remplit. SurfinGate permet d'accepter les codes mobiles et de gérer, contrôler et appliquer les règles de sécurité de l'entreprise pour les contrôles ActiveX, les objets Java, les scripts JavaScript, les scripts Visual Basic, les plug-in et les cookies.

SurfinGate comprend les composants suivants :
- SurfinGate Server
- SurfinConsole
- Base de données SurfinGate
- Plug-in pour l'intégration de Web Traffic Express (WTE)

SurfinGate Server est utilisé en tant que serveur relais HTTP ou en tant que service destiné au pare-feu ou au serveur relais. SurfinGate Server peut être installé après le pare-feu de l'entreprise et les autres serveurs relais. Il peut aussi s'utiliser comme serveur HTTP. Cette architecture permet d'arrêter la transmission du code mobile et d'effectuer un contrôle afin d'éviter tout risque.

Le module SurfinConsole permet à l'administrateur du réseau de créer et gérer des règles de sécurité applicables aux codes mobiles à l'échelle de l'entreprise. SurfinConsole peut contrôler plusieurs serveurs SurfinGate Server sur le réseau et faire appliquer par chaque utilisateur ou groupe les règles définies dans l'entreprise à l'aide de listes personnalisées de codes acceptables/non acceptables.

La base de données SurfinGate stocke les données relatives aux profils ASP de sécurité liés aux applets, y compris les informations concernant les

utilisateurs, les groupes et les règles de sécurité associées. SurfinGate contrôlant le contenu du code mobile de manière dynamique, la base de données n'est pas indispensable à la sécurité mais améliore les performances des opérations à grande échelle.

Remarque : Si vous avez acquis SurfinGate pour Windows NT dans le cadre de l'offre SecureWay FirstSecure ou SecureWay Boundary Server, vous devez prendre contact avec IBM pour les services et le support techniques, même si la documentation de SurfinGate fournit les coordonnées de Finjan.

Chapitre 7. Planification de l'installation de Intrusion Immunity dans un réseau

Les techniques de sécurité décrites jusqu'à présent soulignent l'importance de la protection contre les risques d'atteinte à la sécurité. Cette sécurité serait incomplète si elle ne permettait pas aussi la détection de ces risques. Les produits anti-intrusion de FirstSecure fournissent des fonctions de détection des intrusions et des antivirus qui permettent à l'entreprise de détecter les menaces.

Les logiciels antivirus assurent une protection efficace contre tous les codes dangereux, tels que les chevaux de Troie, les vers, les macros, les contrôles ActiveX et les applets Java suspects. La protection contre les virus est un aspect essentiel des solutions de sécurité. Les produits antivirus de FirstSecure assurent les fonctions clé détaillées ci-dessous.

- Couverture d'un large éventail d'applications client pour répondre aux besoins des clients fixes et mobiles en matière d'antivirus.
- Service d'abonnement aux signatures de virus. La mise à jour régulière des listes de signatures de virus est essentielle pour une protection efficace contre les nouvelles formes de code dangereux.
- Distribution aux clients des mises à jour d'antivirus par l'intermédiaire des serveurs, conformément aux règles de sécurité définies, pour garantir la mise en oeuvre des règles de sécurité antivirus.

Déploiement de Tivoli Cross-Site for Security

Tivoli Cross-Site for Security permet de détecter les intrusions dans les réseaux potentiellement vulnérables. Vous pouvez installer les agents Tivoli Cross-Site for Security partout où votre domaine administratif est relié à l'Internet. Tivoli Cross-Site for Security surveille l'activité des réseaux et détecte les tentatives de fraude internes et externes. Ses avantages sont les suivants :

- Détection des intrusions en temps réel avec alerte à l'administrateur Cross-Site for Security en cas de risque d'agression
- Possibilité de définir différentes règles pour les agents installés dans la zone démilitarisée et dans l'intranet
- Modification en ligne des règles des agents de sécurité permettant de répondre rapidement à l'évolution des environnements
- Intégration avec les applications professionnelles de Tivoli pour compléter votre système de gestion Tivoli

Tivoli Cross-Site for Security peut accomplir les tâches suivantes :

- Détecter les analyses et les débordements
- Surveiller les transactions IP
- Surveiller les services des ports
- Détecter les requêtes et les réponses échangées entre le DNS, le service de montage et le système de fichiers du réseau
- Détecter les requêtes adressées au service de l'associateur de port et les refus de réponse
- Détecter les appels RStatd
- Détecter les requêtes contenant un masque hyperlien ou un nom de fichier particulier
- Détecter les agressions dirigées contre les serveurs de fichiers sur PC
- Détecter le protocole des messages de contrôle Internet

Cross-Site for Security permet de surveiller les transactions de réseau et de détecter les agressions et les tentatives d'intrusion. Ce contrôle concerne le trafic de la zone démilitarisée, qui isole l'intranet de l'Internet, comme celui du réseau interne.

Cross-Site for Security peut détecter les types d'intrusion suivants :

- Détection des signatures ou des modèles
- Détection des débordements
- Attaques provenant du réseau
- Attaques du réseau Windows
- Attaques par procédure à distance
- Utilisations frauduleuses des services
- Transactions de réseau non autorisées
- Activité suspecte

Cross-Site for Security protège votre réseau à l'aide de l'agent et du serveur de gestion Cross-Site for Security. Lorsqu'un agent détecte une agression, il envoie un message codé au serveur de gestion Cross-Site for Security qui consigne immédiatement ces informations et y répond. Vous pouvez configurer le serveur de gestion de Cross-Site for Security de manière à transmettre un message d'alerte à la console, un courrier électronique à un administrateur ou un appel d'urgence à l'administrateur de garde.

Obtention d'une clé de licence Tivoli Cross-Site for Security

L'activation du programme Tivoli Cross-Site for Security nécessite une clé de licence personnalisée.

Pour recevoir cette clé, vous devez contacter le site WEB de Tivoli Cross-Site et exécuter la procédure suivante :

1. Munissez-vous du justificatif de licence Passport Advantage, fourni avec les produits FirstSecure (dans la version avec le CD-ROM de Tivoli Cross-Site for Security et le manuel *Tivoli Cross-Site for Security Installation*).
2. Recherchez sur ce document le numéro d'ordre, un numéro à huit chiffres commençant par 5, et le numéro de client (de site), un numéro à sept chiffres commençant par 7. Ces numéros vous permettent d'accéder au site WEB de Tivoli Cross-Site lors de votre première connexion.
3. Connectez-vous au site WEB de Tivoli Cross-Site à l'aide d'un navigateur Web relié à l'Internet. L'adresse URL du site WEB est `www.cross-site.com/support/licensing/`.
4. Entrez votre numéro d'ordre, votre numéro de client et les renseignements personnels demandés. Vous devez également indiquer le nom de domaine du serveur sur lequel vous voulez installer Tivoli Cross-Site for Security.
5. Suivez les instructions données à l'écran.
6. En cas de problème d'accès au site WEB de Tivoli Cross-Site , contactez le service d'assistance de Tivoli Cross-Site au numéro 1–800–2–TIVOLI, poste 9396, ou envoyez un courrier électronique à l'adresse licensing@cross-site.com.

Produits Tivoli Cross-Site annexes

La famille des produits Tivoli Cross-Site comprend d'autres programmes non proposés dans la solution FirstSecure :

- Tivoli Cross-Site for Availability surveille et consigne la manière dont les utilisateurs finaux se connectent à votre site WEB.
- Tivoli Cross-Site for Deployment étend la couverture de votre entreprise en lui permettant de distribuer et de gérer ses applications critiques par l'Internet.

Ces produits, auxquels la documentation de Tivoli Cross-Site for Security peut faire référence, doivent être achetés séparément.

Surveillance du trafic avec Tivoli Cross-Site for Security

L'agent Cross-Site for Security assure la surveillance des activités d'un réseau. Il contrôle de manière continue les paquets de données échangés dans le réseau. L'agent Cross-Site for Security analyse ces paquets à la recherche de signatures témoignant d'une activité suspecte. Ces signatures peuvent révéler des tentatives d'attaque du réseau.

L'agent Cross-Site for Security s'exécute sous la forme d'un *démon* dans sa version UNIX, et sous celle d'un service sur Windows NT. Cross-Site for Security est configuré pour démarrer automatiquement à l'amorçage du système. Le programme reste en mémoire et s'exécute en arrière-plan, qu'un utilisateur soit connecté ou non.

Lorsqu'un risque d'attaque est détecté, l'agent identifie son niveau de gravité et décide d'avertir le serveur de gestion immédiatement ou de consigner l'alerte dans un fichier journal local. Les fichiers journaux sont périodiquement communiqués au serveur de gestion.

L'agent contacte régulièrement le serveur de gestion Cross-Site for Security pour lui faire savoir qu'il est toujours actif. Pour ce faire, il émet un *signal de présence*. Vous pouvez configurer l'intervalle de communication (ou intervalle de contact) de ce signal de présence.

Lorsque le serveur de gestion reçoit un signal de présence de la part de l'agent, il lui communique en retour toutes les nouvelles informations de configuration utiles telles que les nouvelles signatures et les plannings de téléchargement. L'agent télécharge automatiquement ces données et les installe.

Intégration de Tivoli Cross-Site for Security au réseau

Vous pouvez configurer Cross-Site for Security selon les besoins de votre entreprise. Les principales décisions à prendre sont les suivantes :

- Où installer le serveur de gestion de Cross-Site for Security ?
- Combien d'agents Cross-Site for Security sont nécessaires ?
- Où installer les agents Cross-Site for Security ?

Ces critères, auxquels s'ajoutent la taille, la topologie, la largeur de bande et le trafic de votre réseau, sont essentiels pour déterminer le nombre de serveurs de gestion et d'agents à installer. Reportez-vous à la section «Configurations logicielles et matérielles requises pour Intrusion Immunity» à la page 67 pour plus d'information sur l'installation de Tivoli Cross-Site for Security.

Remarque : Si vous avez acquis Tivoli Cross-Site for Security dans le cadre de l'offre SecureWay FirstSecure, vous devez prendre contact avec IBM pour les services et le support techniques, même si la documentation fait référence à un service d'assistance.

Déploiement de Norton AntiVirus

Le programme Norton AntiVirus, développé par Symantec Corporation, figure parmi les meilleurs logiciels antivirus du monde. Norton AntiVirus peut accomplir les tâches suivantes :

- Ecarter les fichiers infectés
- Protéger le système contre les virus, les contrôles ActiveX et les applets Java dangereux
- Protéger les ordinateurs des virus susceptibles d'être transmis par les documents joints aux messages électroniques, les disquettes, les CD-ROM, un réseau ou encore lors d'un téléchargement à partir d'Internet

Vous pouvez configurer Norton AntiVirus de manière à ce qu'il fonctionne en permanence en arrière-plan pour protéger votre ordinateur. Symantec ajoute continuellement de nouvelles signatures dans la liste des virus que Norton AntiVirus peut détecter. La fonction LiveUpdate permet d'extraire, chaque semaine et de manière automatique, les nouvelles définitions antivirus de Symantec.

La fonction de quarantaine de Norton AntiVirus isole les fichiers infectés ou suspects dans une zone sûre de l'ordinateur, éloignée des autres fichiers pour éviter la propagation du virus pendant l'intervention.

L'assistant Scan and Deliver permet d'envoyer les fichiers suspects à Symantec pour évaluation. Le centre Symantec AntiVirus Research Center (SARC) vous fournit une réponse pour vous aider à résoudre le problème.

Le scanner de Norton AntiVirus, *Bloodhound*, s'exécute en arrière-plan. Il surveille et classifie le comportement des applications susceptibles d'être infectées par de nouveaux virus. Si un programme a toutes les caractéristiques d'un virus et que les autres programmes risquent d'être touchés, Bloodhound peut interrompre le programme et éviter ainsi la propagation du virus jusqu'à ce que vous receviez les nouvelles mises à jour d'antivirus.

Les produits Norton AntiVirus Solution Release 3.04 fournis avec FirstSecure sont les suivants :

- Solutions pour poste de travail :
  - Norton AntiVirus 4.08 for DOS
  - Norton AntiVirus 4.08 for Windows 3.51
  - Norton AntiVirus 5.02 for Windows 95/98
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 5.03 for Macintosh
  - Norton AntiVirus 5.02 for OS/2
- Solutions pour serveur :
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 4.04 for NetWare
  - Norton AntiVirus 2.0 for Lotus Notes et OS/2
  - Norton AntiVirus 1.52 for Microsoft Exchange
- Solutions pour passerelle :
  - Norton AntiVirus 1.02A for Internet E-mail Gateways for NT
  - Norton AntiVirus 1.04 for Firewalls
- Administration :
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 for Macintosh Administrator
  - Norton AntiVirus Plus 5.0 for Tivoli Enterprise

- Norton AntiVirus Plus 5.0 for Tivoli IT Director
- Autres outils d'administration, parmi lesquels Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

Pour plus d'informations sur Norton AntiVirus, consultez le fichier contents.txt qui se trouve dans le répertoire racine du CD-ROM de Norton AntiVirus.

Remarque : Si vous avez acquis Norton AntiVirus Solution Release 3.04 dans le cadre de l'offre SecureWay FirstSecure, vous devez prendre contact avec IBM pour les services et le support techniques, même si la documentation de Norton AntiVirus vous indique les coordonnées de Symantec.

Pour plus d'informations sur la procédure d'installation, reportez-vous à la documentation fournie avec les différents produits et aux sections relatives aux configurations logicielles et matérielles requises dans le «Chapitre 13. Remarques sur la procédure et les conditions d'installation de Intrusion Immunity» à la page 67.

Chapitre 8. Planification de l'installation de Public Key Infrastructure dans un réseau

Le composant Trust Authority de Public Key Infrastructure permet aux applications Internet d'authentifier les utilisateurs et de sécuriser les communications. Basé sur les normes de cryptographie et d'interdépendance fonctionnelle PKI, le système Trust Authority permet de délivrer, de communiquer et de gérer des certificats numériques. Ce système présente les caractéristiques suivantes :

- Support des serveurs IBM AIX et Microsoft Windows NT
- Autorité d'enregistrement gérant les tâches d'administration liées à l'enregistrement des utilisateurs. Cette administration, qui peut être réalisée manuellement ou par le biais de processus automatisés, implique les taches suivantes :
  - Confirmation de l'identité d'un utilisateur
  - Acceptation ou rejet des requêtes d'obtention, de renouvellement ou de révocation des certificats
  - Vérification de la possession par l'utilisateur d'une clé privée correspondant à la clé publique contenue dans un certificat
  - Application des règles définies dans un processus ou dans un profil de certificat pour délivrer certains types de certificat à certains types d'utilisateur

  L'autorité d'enregistrement enregistre également les informations liées aux certificats dans un annuaire de clés publiques intégré, l'annuaire IBM SecureWay Directory (LDAP).
- Autorité de certification (AC) sécurisée. L'AC accomplit les tâches suivantes :
  - Délivrance des certificats numériques et création des paires de clés numériques permettant l'authentification des certificats
  - Gestion du cycle d'existence des certificats depuis l'inscription initiale jusqu'à la révocation en passant par le renouvellement
  - Actualisation instantanée de l'annuaire par l'autorité d'enregistrement chaque fois qu'un certificat est révoqué
  - Utilisation de périphériques de cryptographie tels que le coprocesseur de chiffrement IBM SecureWay 4758 PCI et les cartes Smart Cards, pour mieux protéger les clés
- Credential Central. Il s'agit d'une interface d'inscription par le Web qui simplifie l'obtention des certificats de navigateur, des certificats de serveur et des certificats de périphérique (pour les cartes Smart Cards par exemple).

L'administrateur peut également utiliser ces formulaires d'inscription pour pré-enregistrer les utilisateurs finaux en vue d'obtenir un certificat PKIX.

- Client Trust Authority, une interface Windows autonome qui permet à l'utilisateur d'obtenir, de renouveler et de révoquer des certificats PKIX sans utiliser de navigateur Web.
- RA Desktop, une interface d'administration par le Web qui permet à l'administrateur d'accepter ou de refuser des requêtes d'obtention, de renouvellement ou de révocation des certificats.
- Sous-système d'audit utilisant des codes d'authentification de message (codes MAC) pour garantir la possibilité d'authentifier les événements transmis par l'autorité d'enregistrement et l'autorité de certification de Trust Authority. Une option réglable permet également de protéger l'intégrité des rapports d'audit lors de leur journalisation.
- Plusieurs interfaces d'administration, permettant de configurer le système, de modifier les mots de passe sécurisés, de certifier réciproquement les autorités de certification, de contrôler l'intégrité des journaux d'audit et de démarrer ou d'arrêter les composants du système en toute sécurité.
- Interface de programmation d'application (API) permettant de créer des applications PKI personnalisées.
- Support intégré du SGBD IBM DB2 Universal Database. Il existe plusieurs bases de données pour les composants IBM SecureWay Directory, Autorité d'enregistrement, Autorité de certification et Audit.

Déploiement de Trust Authority

Pour plus d'informations sur la planification et l'installation de Trust Authority, reportez-vous au manuel *IBM SecureWay Trust Authority - Guide d'initiation*. Ce manuel décrit différentes approches possibles pour installer Trust Authority sur des serveurs Windows NT et AIX.

Chapitre 9. Planification de l'installation de SecureWay Toolbox

Vous devez installer FirstSecure Toolbox dans un environnement de développement et non pas dans votre réseau. De même, vous devez évaluer vos applications à l'intérieur de cet environnement de développement avant de les rendre accessibles aux utilisateurs externes.

Services d'autorisation

Le module Services d'autorisation permet de contrôler l'accès à votre site WEB. L'authentification repose sur des mots de passe ou des clés publiques. Ces mesures ont pour objectif de protéger l'intégrité et la confidentialité des données de votre site. Le module Services d'autorisation permet de créer des listes de contrôle d'accès qui définissent les utilisateurs pouvant accéder aux objets du site et la manière dont ils peuvent les utiliser. Le module Services d'autorisation permet également de définir des objets protégés et de créer des mots de passe pour la connexion unique. Tous ces utilitaires de sécurité sont centralisés pour faciliter la gestion des règles de sécurité. Les services d'autorisation sont pris en charge par les API d'autorisation d'IBM SecureWay Policy Director.

Services d'autorité de certification

Les services d'autorité de certification sont pris en charge par X.509 Public Key Infrastructure multi-plates-formes et IBM KeyWorks Toolkit.

Les services d'autorité de certification permettent de sécuriser le réseau par le biais de certificats numériques. Ces services comprennent des API qui permettent de gérer le cycle de ces certificats : la délivrance, le renouvellement et la révocation. Elles permettent également de publier les listes des révocations de certificat. Les API utilisent la cryptographie par clé publique et la technologie des cartes à puce pour authentifier les utilisateurs munis d'un certificat.

X.509 Public Key Infrastructure multi-plates-formes, également appelé PKIX, est fourni avec les API de PKIX. Ces API permettent de créer, de gérer, de stocker, de distribuer et de révoquer les certificats par le biais de l'entité finale, de l'autorité de certification et de l'autorité d'enregistrement. Elles peuvent s'utiliser en interface avec IBM SecureWay Trust Authority et reposent sur le produit IBMKeyWorks.

Pour plus d'informations sur les API de PKIX, reportez-vous au manuel *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*. Pour plus d'informations sur IBM KeyWorks, reportez-vous au «Chapitre 16. Documentation des produits FirstSecure» à la page 87, qui répertorie les documents fournis avec le produit Toolbox.

Services d'annuaire

Les services d'annuaire sont pris en charge par le client IBM SecureWay Directory.

Les services d'annuaire utilisent Lightweight Directory Access Protocol (LDAP) pour accéder aux annuaires, les organiser et les contrôler. Ces services reposent sur une architecture client-serveur qui permet à un client d'accéder à un serveur LDAP. Les services d'annuaire permettent de gérer les informations des annuaires à partir d'un emplacement centralisé, pour le stockage, la mise à jour, l'extraction et l'échange des données. Les services d'annuaire utilisent le protocole SSL (Secure Sockets Layer) pour coder les informations.

Pour plus d'informations sur les services d'annuaire, reportez-vous au «Chapitre 16. Documentation des produits FirstSecure» à la page 87, qui fournit la liste complète des documents rattachés au produit IBM SecureWay Directory Client fournis avec le programme Toolbox.

Services de sécurisation et de cryptographie de KeyWorks

Les services de gestion de la sécurisation et de la cryptographie sont pris en charge par le produit IBM KeyWorks Toolkit (ou KeyWorks).

Les services de sécurisation et de cryptographie de KeyWorks permettent de coder et de décoder les informations afin de contrôler leur accessibilité. Ces services créent et vérifient les signatures numériques pour authentifier les identités des individus et des ordinateurs connectés aux réseaux. Le module IBM Key Recovery Service Provider contient un système de restauration des clés qui permet de restaurer des informations codées sans avoir à en communiquer la clé.

KeyWorks est une boite à outils contenant des utilitaires de sécurisation et de cryptographie. Ce produit se compose d'une série de services de sécurité de différents niveaux et d'interfaces de programmation associées qui fournissent un ensemble de fonctions de sécurisation des données et des communications. Chaque niveau de service utilise les principaux services du niveau immédiatement inférieur. Les premiers niveaux utilisent des algorithmes de chiffrement, des nombres aléatoires, des données d'identification uniques. Les

derniers niveaux utilisent des certificats numériques, des systèmes de gestion et de restauration des clés et des protocoles de transaction sécurisés.

KeyWorks est compatible NLS (National Language Support). Ceci signifie que vous pouvez l'utiliser avec n'importe quelle langue, script, culture et jeu de caractères codés.

Pour plus d'informations sur les API de KeyWorks, reportez-vous au «Chapitre 16. Documentation des produits FirstSecure» à la page 87 qui donne la liste des documents rattachés à KeyWorks fournis avec le produit Toolbox.

Services de protocole Secure Sockets Layer

Les services de protocole Secure Sockets Layer sont pris en charge par le produit IBM Secure Sockets Layer (SSL) Toolkit.

Les services de protocole SSL permettent de déterminer qui aura accès aux données du réseau. Ces services codent les données à l'aide de clés publiques et privées, notamment pour l'authentification des utilisateurs mais aussi dans le but d'empêcher les accès non autorisés ou la manipulation frauduleuse des données. C'est à vous qu'il revient de choisir les destinataires des certificats et, par conséquent, les utilisateurs qui pourront accéder aux données de votre réseau. La technologie SSL est présente dans d'autres API, notamment pour le codage des données et la création des mots de passe.

Partie 3. Remarques sur l'installation et l'intégration des composants

Cette partie décrit la manière dont les différents composants s'articulent. Elle détaille les configurations logicielles et matérielles requises pour chaque produit ainsi que les applications et les bases de données nécessaires à l'installation.

Chapitre 10. Planification de l'installation de FirstSecure

Avant d'installer les composants de FirstSecure, lisez les sections suivantes pour vérifier si vous disposez du matériel et des logiciels requis. Des informations sur les dernières mises à jour de FirstSecure sont disponibles sur le site Web : www.ibm.com/software/security/firstsecure. Consultez ce site WEB pour connaître les dernières mises à jour disponibles avant d'installer les produits.

Des instructions détaillées d'installation et de configuration des composants de FirstSecure sont données dans la documentation fournie avec chaque produit.

Configuration système requise

Cette section décrit la configuration système requise pour l'installation des produits FirstSecure. Pour toute information sur les conditions matérielles requises pour un composant déterminé, reportez-vous à la section rattachée à ce composant.

Pour installer les composants de FirstSecure, vous devez disposer d'un matériel acceptant l'un des systèmes d'exploitation pour serveur suivants :

- Microsoft Windows NT version 4 avec Service Pack 5
- AIX Version 4.3.1 ou version ultérieure
- Sun Solaris version 2.6 ou version ultérieure

Remarque : Sur Solaris, le produit Toolbox nécessite Sun Solaris version 2.6 avec le Fix Pack de mai 1999.

Chaque composant FirstSecure peut être exécuté sur l'un des systèmes d'exploitation ci-dessus ou sur plusieurs. Pour chaque composant, une section présente les plates-formes supportées et les logiciels requis. Vous devrez installer sur ces systèmes des serveurs, des consoles de gestion et des programmes clients. Les sections qui suivent donnent une présentation générale de ces conditions d'installation.

Systèmes d'exploitation des serveurs et des clients

Reportez-vous au tableau 1 à la page 56 pour connaître les systèmes d'exploitation pris en charge par les produits SecureWay.

Tableau 1. Systèmes d'exploitation des serveurs et des clients

Système d'exploitation	Configuration minimale pour serveur	Configuration minimale pour client
Windows NT	Version 4.0, Service Pack 5	Version 4.0, Service Pack 5
IBM AIX	Version 4.3.1	Version 4.3.1
Sun Solaris	Version 2.6	Version 2.6
Windows 95	sans objet	toutes versions
Windows 98	sans objet	toutes versions
Windows 3.1 (Norton AntiVirus uniquement)	sans objet	toutes versions
IBM OS/2 (Norton AntiVirus uniquement)	sans objet	Version 4.0, FixPak 6 ou version ultérieure

Caractéristiques des composants et configurations requises

Les chapitres qui suivent indiquent les conditions matérielles et logicielles requises pour l'installation des composants de la solution FirstSecure. Ces chapitres décrivent les différents composants de FirstSecure et les configurations matérielles et logicielles requises pour chacun d'eux. Ils contiennent également une présentation générale de l'installation et de la configuration de chaque produit et abordent la question de leur intégration avec les autres composants.

- «Chapitre 11. Remarques sur la procédure et les conditions d'installation de Policy Director» à la page 57
- «Chapitre 12. Remarques sur la procédure et les conditions d'installation de SecureWay Boundary Server» à la page 59
- «Chapitre 13. Remarques sur la procédure et les conditions d'installation de Intrusion Immunity» à la page 67
- «Chapitre 14. Remarques sur la procédure et les conditions d'installation de Public Key Infrastructure» à la page 75
- «Chapitre 15. Remarques sur la procédure et les conditions d'installation de Toolbox» à la page 81

Chapitre 11. Remarques sur la procédure et les conditions d'installation de Policy Director

Ce chapitre détaille les configurations logicielles et matérielles requises pour l'installation de Policy Director. Il aborde également la question de l'intégration avec les autres produits de la solution FirstSecure.

Configuration logicielle et matérielle requise pour Policy Director

Le tableau 2 détaille la configuration matérielle requise pour installer Policy Director.

Tableau 2. Configuration matérielle requise pour Policy Director

Plate-forme	Espace disque minimum	RAM minimum
Serveur Windows NT : processeur Intel ou compatible, de type 80486, 133 MHZ ou supérieur	16 Mo	64 Mo
Serveur AIX : Système avec AIX 4.3.1	16 Mo	64 Mo
Serveur Solaris : Système avec Solaris 2.6	16 Mo	64 Mo

La configuration logicielle requise pour l'installation de Policy Director est la suivante :

Serveurs Policy Director

- Windows NT Server Version 4.0, Service Pack 5
- AIX Version 4.3.1
- Sun Solaris, Version 2.6

Clients NetSEAT

- Windows NT Server Version 4.0, Service Pack 5
- Windows 95
- Windows 98

Console de gestion

- Windows NT Workstation
- Windows NT Server Client
- AIX Version 4.3.1 Client
- Sun Solaris, Version 2.6 Client

Policy Director nécessite d'autres logiciels qui sont fournis avec le produit. Reportez-vous aux instructions du manuel *IBM SecureWay Policy Director - Guide de configuration et d'utilisation* pour installer les logiciels nécessaires à l'installation de Policy Director.

Remarques sur l'installation de Policy Director

Le site Web www.ibm.com/software/security/policy donne des informations récentes sur les composants prérequis pour l'installation de Policy Director.

Intégration de Policy Director et Trust Authority

Le produit IBM SecureWay Trust Authority permet l'authentification de l'identité des utilisateurs. Trust Authority délivre des certificats aux utilisateurs sur la base des informations contenues dans l'annuaire IBM SecureWay Directory, également appelé annuaire LDAP (Lightweight Directory Access Protocol).

Policy Director utilise ensuite ces certificats pour délivrer des autorisations aux utilisateurs, s'assurant ainsi que ceux-ci n'accèdent qu'aux ressources qui leur sont destinées. Policy Director enregistre aussi ses informations dans l'annuaire IBM SecureWay Directory.

Votre e-business peut être rattaché à une unique définition d'utilisateur contenant toutes les autorisations de Policy Director et toutes les informations de Trust Authority. Si vous décidez de stocker les données de SecureWay Boundary Server dans l'annuaire IBM SecureWay Directory, Policy Director peut également gérer cette fonction.

Chapitre 12. Remarques sur la procédure et les conditions d'installation de SecureWay Boundary Server

Ce chapitre détaille les configurations logicielles et matérielles requises pour l'installation de SecureWay Boundary Server. Il aborde également la question de l'intégration avec les autres produits de la solution SecureWay Boundary Server.

Configuration logicielle et matérielle requise pour SecureWay Boundary Server

Les conditions matérielles requises pour les composants de SecureWay Boundary Server sont présentées dans le tableau 3 et le tableau 4 à la page 60.

Tableau 3. Conditions matérielles requises pour les composants de SecureWay Boundary Server

Composant SecureWay Boundary Server	**Type de machine**	**Espace disque**	**Mémoire**	**Autre**
IBM SecureWay Firewall[1]	NT : Pentium 133 MHz ou supérieur AIX : machine RS/6000 supportant AIX 4.3.2	NT : 24 Mo[2] AIX : 307 Mo	NT : 64 Mo AIX : 64 Mo	2 cartes d'interface réseau
ACE/Server	Windows NT : Pentium 166 MHz ou supérieur (mono-processeurs uniquement) AIX : Machine supportant AIX 4.2	Logiciel du serveur principal : 50 Mo Serveur de secours : 22 Mo Base de données utilisateur initiale : 4 Mo Installation : 240 Mo	Minimum : 32 Mo	Les besoins réels dépendent du nombre d'utilisateurs
SurfinGate				

Tableau 3. Conditions matérielles requises pour les composants de SecureWay Boundary Server (suite)

Composant SecureWay Boundary Server	Type de machine	Espace disque	Mémoire	Autre
Serveur	Pentium 233 MHz ou supérieur	20 Mo	Minimum : 128 Mo, recommandé : 256 Mo	
Console	Pentium 233 MHz ou supérieur	15 Mo	Minimum : 32 Mo, recommandé : 64 Mo	
MIMEsweeper for IBM SecureWay Release 2				
MAILsweeper	Pentium 200 MHz ou supérieur	1 Go	64 Mo	1 carte d'interface réseau
WEBsweeper	Pentium 400 MHz ou supérieur	1 Go	128 Mo + 1 Mo pour chaque connexion Web simultanée	1 carte d'interface réseau
Remarques : 1. Reportez-vous à la documentation d'IBM Firewall pour plus d'informations. 2. 13 Mo d'espace disque sont également nécessaires pour le navigateur Netscape.				

Tableau 4. Conditions logicielles requises pour l'installation des composants de SecureWay Boundary Server

Composant SecureWay Boundary Server	Plates-formes Microsoft Windows		AIX	Solaris
	Client	Serveur	Serveur	Serveur
IBM SecureWay Firewall	Windows 95, client IPSec	Windows NT Server Version 4.0, Service Pack 5 [1]	AIX 4.3.2	Non disponible
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 ou version ultérieure	Windows NT Server Version 4.0, Service Pack 5 ou version ultérieure	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
Serveur	Non disponible	Windows NT 4.0[2]	Non disponible	Non disponible

Tableau 4. Conditions logicielles requises pour l'installation des composants de SecureWay Boundary Server (suite)

Composant SecureWay Boundary Server	**Plates-formes Microsoft Windows**		**AIX**	**Solaris**
	Client	**Serveur**	**Serveur**	**Serveur**
Console	Windows NT 4.0 ou version ultérieure[2] Windows 95, Windows 98	Non disponible	Non disponible	Non disponible
MIMEsweeper for IBM SecureWay Release 2				
MAILsweeper	Non disponible	Windows NT 4.0[3]	Non disponible	Non disponible
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 ou version ultérieure	Windows NT 4.0[4]	Non disponible	Non disponible

Remarques :

1. Consultez la documentation d'IBM Firewall pour Windows NT pour plus d'informations sur les correctifs requis.
2. De plus :
   - Le client Windows pour Microsoft Windows est requis.
   - Windows NT Workstation n'est pas pris en charge.
3. De plus :
   - NT 3.5.1 et Windows NT Workstation ne sont pas pris en charge.
   - L'un des environnements suivants est requis :
     - Microsoft Exchange
     - SMTP
     - cc:Mail
     - Groupwise
     - Lotus Notes
4. Reportez-vous à la section «Remarques sur MIMEsweeper» à la page 65 pour lire les recommandation sur MIMEsweeper.

Remarques sur les composants de SecureWay Boundary Server

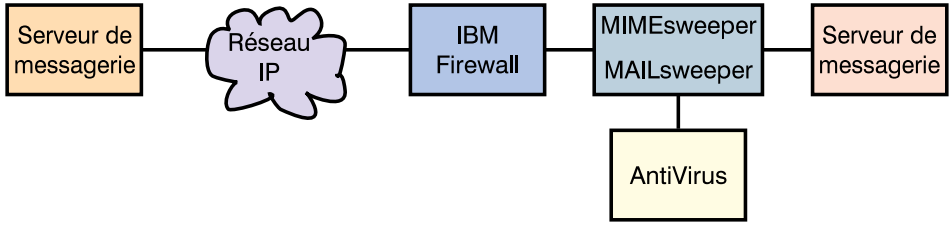
Les sections qui suivent décrivent différents aspects de l'installation et de la configuration des composants de SecureWay Boundary Server.

Remarques sur IBM Firewall

Choisir l'emplacement du réseau où vous allez installer IBM Firewall par rapport aux autres produits de SecureWay Boundary Server pose une véritable question.

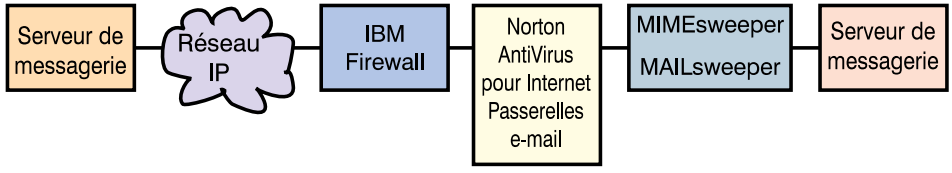
Exemples de configuration

Exemple de configuration pour IBM Firewall et MAILsweeper: Vous pouvez vous inspirer de la configuration décrite dans cette section pour installer à la fois IBM Firewall et MIMEsweeper.



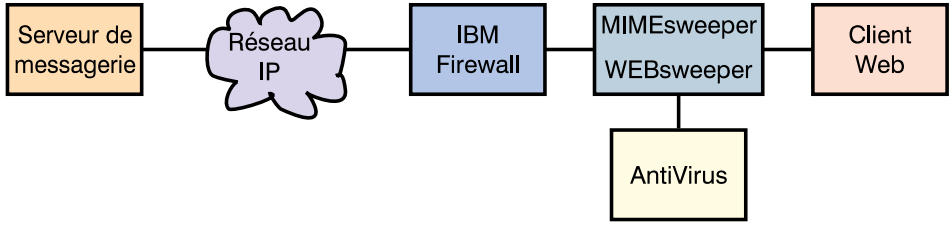
- MAILsweeper est un composant de MIMEsweeper qui vérifie le contenu des messages envoyés par courrier électronique. MAILsweeper est doté d'une fonction d'activation du contrôle antivirus.
- MAILsweeper est situé entre IBM Firewall et les serveurs SMTP sécurisés.
- IBM Firewall dirige ses requêtes vers MAILsweeper qui fait office d'hôte pour le réacheminement du courrier.
  - Pour permettre le trafic du courrier, des règles doivent être prédéfinies au niveau d'IBM Firewall.
- Les serveurs SMTP doivent également diriger leurs requêtes vers MAILsweeper qui fait office d'hôte pour le réacheminement du courrier.
- MAILsweeper vérifie le contenu des courriers électroniques transitant dans les deux directions.

Exemple de configuration pour IBM Firewall, Norton AntiVirus for Internet Email Gateways et MIMEsweeper: Si vous installez IBM Firewall, Norton AntiVirus for Internet Email Gateways et MIMEsweeper, vous pouvez utiliser l'exemple de configuration fourni dans cette section. Ce scénario associe en chaîne IBM Firewall, Norton AntiVirus for Internet Email Gateways et MAILsweeper pour rechercher les virus dans les courriers transmis et vérifier leur contenu, comme illustré par le diagramme ci-après.



- Le pare-feu dirige ses requêtes vers Norton AntiVirus for Internet Email Gateways qui fait office de serveur de courrier sécurisé. Pour permettre le trafic du courrier, il est nécessaire de définir les règles appropriées au niveau du pare-feu.
- Norton AntiVirus for Internet Email Gateways dirige ses requêtes vers MAILsweeper qui assure le réacheminement sécurisé du courrier et réoriente vers le pare-feu les requêtes de courrier sortantes.
- MAILsweeper réceptionne et vérifie le courrier qui lui est envoyé. Il le réoriente ensuite vers le serveur approprié en fonction des tables de routage ou des consultations des enregistrements MX. Si MAILsweeper et Norton AntiVirus for Internet Email Gateways sont installés sur la même machine, vous devez modifier le port de réception de MAILsweeper afin d'éviter tout conflit avec Norton AntiVirus for Internet Email Gateways.

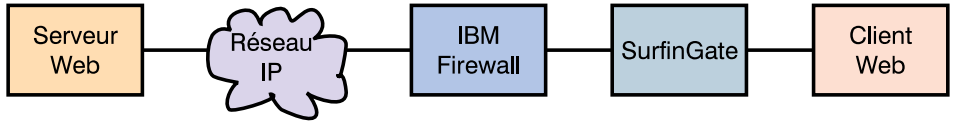
Exemple de configuration pour IBM Firewall et WEBsweeper: Vous pouvez vous inspirer de la configuration décrite dans cette section pour installer à la fois IBM Firewall et MIMEsweeper.



- WEBsweeper est un composant de MIMEsweeper qui vérifie le trafic Web. WEBsweeper est doté d'une fonction d'activation de la détection des virus.
- WEBsweeper fait office de serveur relais intermédiaire. Les clients dirigent leurs requêtes vers WEBsweeper qui constitue leur serveur relais. WEBsweeper est configuré pour réacheminer ensuite le trafic vers le serveur relais situé au niveau du pare-feu.
- Des règles doivent être définies au niveau du pare-feu pour permettre le trafic vers le serveur relais.
- Les requêtes adressées au serveur relais doivent provenir exclusivement du réseau sécurisé protégé par le pare-feu.

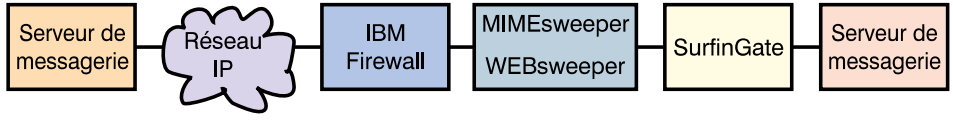
- HTTPS n'est pas supporté par WEBsweeper. Pour utiliser HTTPS, vous devez contourner WEBsweeper pour éviter tout conflit avec le pare-feu tout en maintenant la vérification du trafic Web. Vous devez adresser les requêtes directement au serveur relais du pare-feu. Le trafic Web est toujours sécurisé mais il n'est plus contrôlé par WEBsweeper.

Exemple de configuration pour IBM Firewall et SurfinGate: Si vous installez IBM Firewall et SurfinGate, vous pouvez utiliser l'exemple de configuration fourni dans cette section.



- SurfinGate vérifie le trafic Web et détecte les contrôles ActiveX et un certain nombre d'autres éléments.
- SurfinGate joue le rôle de serveur Web relais. Les clients adressent leurs requêtes à SurfinGate, qui constitue leur serveur relais pour les transmissions HTTP, FTP et HTTPS. SurfinGate transmet ensuite ces requêtes au serveur relais du pare-feu IBM Firewall.
- Des règles doivent être définies au niveau du pare-feu pour permettre le trafic vers le serveur relais.
- Les requêtes adressées au serveur relais doivent provenir exclusivement du réseau sécurisé protégé par le pare-feu.

Exemple de configuration pour IBM Firewall, MIMEsweeper et SurfinGate: Si vous installez IBM Firewall, MIMEsweeper et SurfinGate, vous pouvez utiliser l'exemple de configuration fourni dans cette section.



- SurfinGate vérifie le trafic Web et détecte les contrôles ActiveX et un certain nombre d'autres éléments. Les vérifications auxquelles il procède sont différentes de celles effectuées par le composant WEBsweeper de MIMEsweeper.
- SurfinGate et WEBsweeper font office de serveurs relais Web intermédiaires. Les clients adressent leurs requêtes à SurfinGate, qui constitue leur serveur relais pour les communications HTTP et FTP. SurfinGate transmet ensuite ces requêtes à WEBsweeper qui les dirige à son tour vers le serveur relais du pare-feu IBM Firewall.

- Des règles doivent être définies au niveau du pare-feu pour permettre le trafic vers le serveur relais. Ces règles sont détaillées dans le manuel *IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide*.
- Les requêtes adressées au serveur relais doivent provenir exclusivement du réseau sécurisé protégé par le pare-feu.
- HTTPS n'est pas supporté par WEBsweeper. Lorsque vous utilisez HTTPS, il est préférable de contourner WEBsweeper pour éviter tout conflit avec le pare-feu tout en maintenant la vérification du trafic Web. Vous devez adresser les requêtes directement au serveur relais du pare-feu. Le trafic Web est toujours sécurisé mais il n'est plus contrôlé par WEBsweeper.

Remarques sur MIMEsweeper

Exemple de configuration conventionnelle d'un système avec WEBsweeper :

- Intel Pentium 400 MHz ou supérieur
- 1 Go d'espace disque et 128 Mo de RAM
- Windows NT Server ou Workstation Version 4.0 Server avec Service Pack 3 ou version ultérieure
- Protocole TCP/IP avec nom de domaine et de système hôte
- Utilitaires antivirus

Exemple de configuration pour un environnement avec WEBsweeper pouvant simultanément prendre en charge jusqu'à 500 utilisateurs :

- Intel Pentium II biprocesseur, 450 MHz ou supérieur
- 3 Go d'espace disque et 256 Mo de RAM
- Windows NT Server ou Workstation Version 4.0 Server avec Service Pack 3 ou version ultérieure
- Protocole TCP/IP avec nom de domaine et de système hôte
- Utilitaires antivirus

Si votre environnement doit traiter plus de 500 utilisateurs simultanément, il est conseillé d'installer plusieurs serveurs WEBsweeper.

Chapitre 13. Remarques sur la procédure et les conditions d'installation de Intrusion Immunity

Ce chapitre détaille les configurations logicielles et matérielles requises pour les composants de Intrusion Immunity, Tivoli Cross-Site for Security et Norton AntiVirus.

Configurations logicielles et matérielles requises pour Intrusion Immunity

La section suivante présente la documentation relative à l'installation et à la configuration des composants de Intrusion Immunity.

La configuration logicielle et matérielle requise pour l'installation de Tivoli Cross-Site for Security est détaillée dans le tableau 5, le tableau 6 à la page 68 et le tableau 7 à la page 68. La configuration logicielle et matérielle requise pour l'installation des composants de Norton AntiVirus est détaillée dans le tableau 8 à la page 69 et le tableau 9 à la page 69.

Tableau 5. Configuration logicielle et matérielle requise pour les serveurs Tivoli Cross-Site for Security

Eléments de la configuration	
Système d'exploitation	• AIX 4.3.2 • Windows NT Version 4.0, Service Pack 5 • Solaris 2.5.1 ou 2.6
Java	JDK 1.1.6 révision 04 ou version ultérieure
Serveur Web	Netscape Enterprise Server 3.51
Base de données	• IBM DB2 Version 5.2 • Oracle 7.3.4 (ou 8.0.4 recommandée) • Microsoft SQL Server
Espace disque	• 290 Mo pour Windows NT • 180 Mo pour AIX • 180 Mo pour Solaris
Mémoire	256 Mo
Espace de permutation	300 Mo (400 Mo recommandé)

Remarques :

1. Netscape Enterprise Server 3.51 et 3.6 ne sont pas pris en charge.
2. Reportez-vous à la section relative aux correctifs pour Solaris dans la documentation d'installation de Tivoli Cross-Site for Security.

Tableau 6. Configuration logicielle et matérielle requise pour la console de gestion de Tivoli Cross-Site for Security

Eléments de la configuration	
Systèmes d'exploitation	• Windows 95 • Windows 98 • Windows NT Version 4.0, Service Pack 5 (processeur 166 MHz ou supérieur recommandé) • Solaris 2.5.1 ou 2.6 sur Sun SPARC
Espace disque	25 Mo pour toutes les plates-formes
Mémoire	• 40 Mo pour Windows NT • 64 Mo pour AIX • 40 Mo pour Solaris

Tableau 7. Configuration logicielle et matérielle requise pour les agents de Tivoli Cross-Site for Security

Eléments de la configuration	
Systèmes d'exploitation	• Windows NT Version 4.0, Service Pack 5 ou version ultérieure • AIX 4.3.2 • Solaris 2.5.1 ou 2.6 sur Sun SPARC
Java	JDK 1.1.6 révision 04 ou version ultérieure sur Solaris (requis uniquement pour UNIX)
Espace disque	• 15 Mo pour Windows NT • 10 Mo pour AIX • 10 Mo pour Solaris
Mémoire	• 32 Mo pour Windows NT • 32 Mo pour AIX • 20 Mo pour Solaris

Remarques :

1. Netscape Enterprise Server 3.51 et 3.6 ne sont pas pris en charge.
2. Reportez-vous à la section relative aux correctifs pour Solaris dans la documentation d'installation de Tivoli Cross-Site for Security.

Le tableau 8 à la page 69 détaille la configuration matérielle requise pour Norton AntiVirus.

Tableau 8. Configuration matérielle requise pour Norton AntiVirus

Composant Intrusion Immunity	Type de machine	Espace disque	Mémoire	Autre
Norton AntiVirus	Processeur Intel	24 Mo	Minimum : 16 Mo, recommandé : 32 Mo	Unité de CD-ROM
Norton AntiVirus for Internet E-mail Gateways	Pentium 133 MHz ou supérieur	6 Mo	32 Mo	Unité de CD-ROM Entre 500 Mo et 5 Go pour la messagerie.

Tableau 9. Configuration logicielle requise pour Norton AntiVirus

Composant Intrusion Immunity	Plates-formes Microsoft Windows		OS/2
	Client	Serveur	Client
Norton AntiVirus[1]	Windows NT 4.0 Windows 95 et Windows 98	Windows NT 4.0	OS/2 2.11 ou version ultérieure
Remarque : 1. De plus, une connexion Internet TCP/IP est requise pour Norton AntiVirus for Internet Email Gateways.			

Norton AntiVirus n'est pas disponible sur AIX et Solaris.

Remarques sur l'installation de Tivoli Cross-Site for Security

Les illustrations qui suivent montrent la disposition habituelle des agents et des serveurs de gestion Cross-Site for Security dans un réseau e-business.

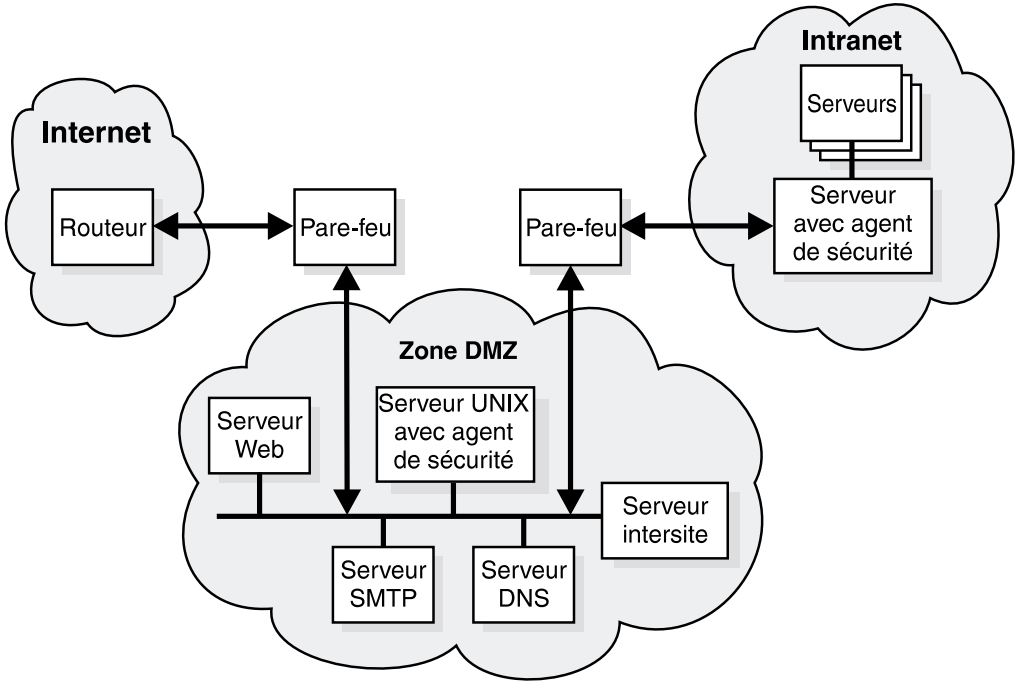


Figure 11. Installation du serveur de gestion Cross-Site for Security dans la zone démilitarisée

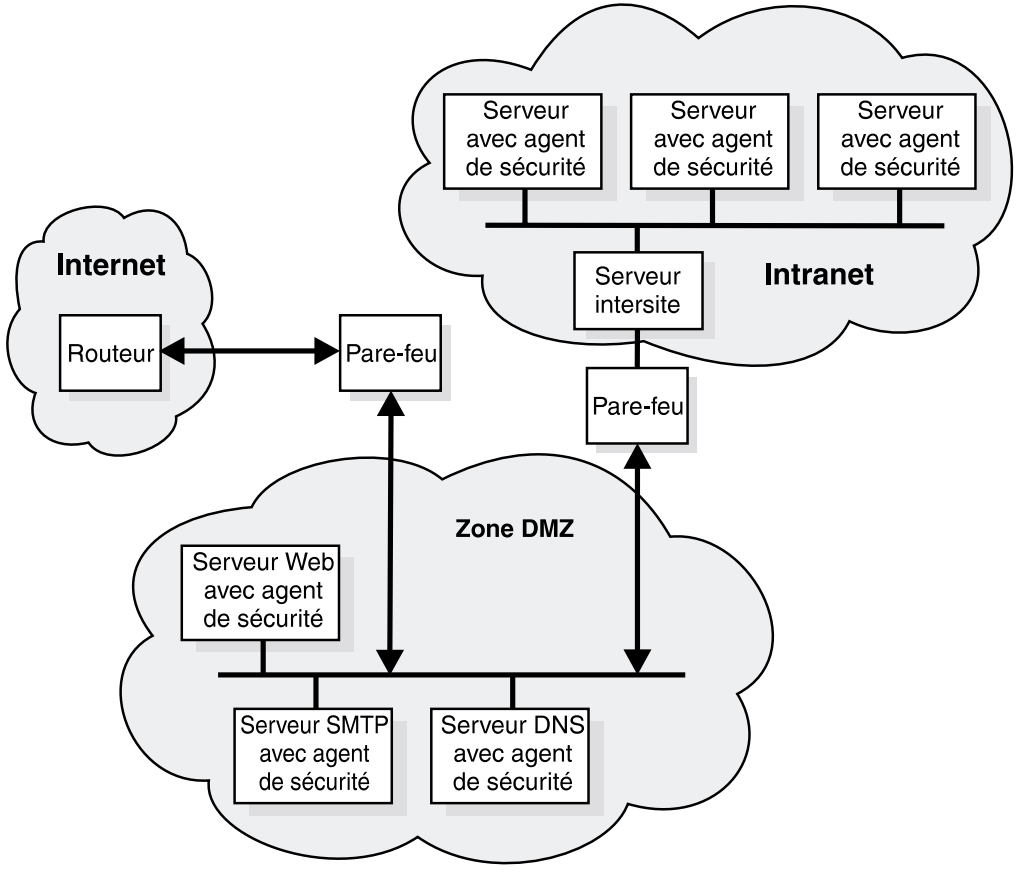


Figure 12. Installation du serveur de gestion Cross-Site for Security dans l'intranet

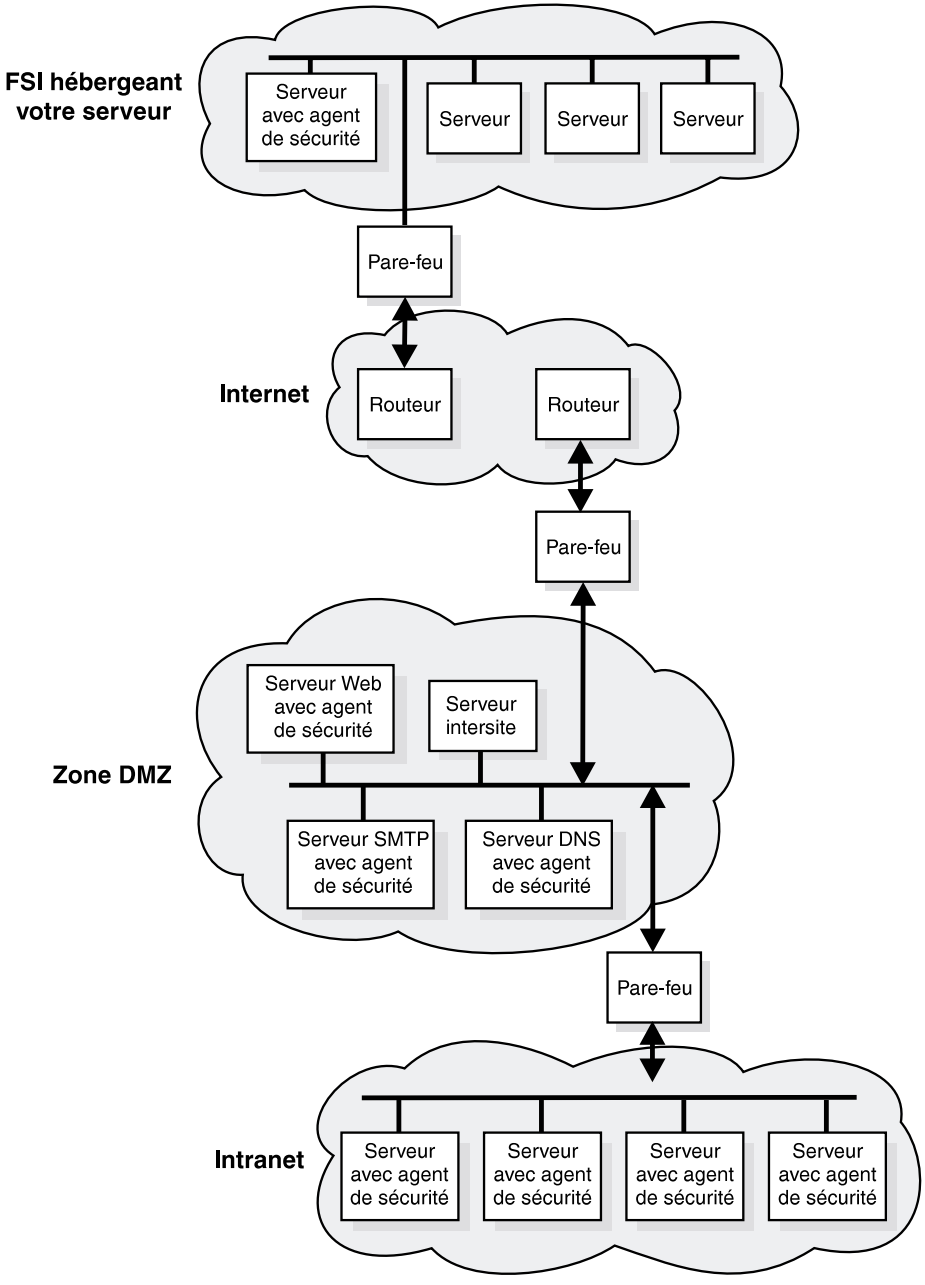


Figure 13. Installation du serveur de gestion Cross-Site for Security dans la zone démilitarisée contenant un serveur relié à Internet

Remarques sur l'installation de Norton AntiVirus

Pour toute information sur l'installation de Norton AntiVirus, consultez le fichier contents.txt, dans le répertoire racine du CD-ROM.

Chapitre 14. Remarques sur la procédure et les conditions d'installation de Public Key Infrastructure

Les entreprises actuelles ont besoin d'une infrastructure de clés publiques (PKI) capable de sécuriser les applications e-business. FirstSecure Trust Authority fournit deux niveaux de fonction qui permettent de créer cette infrastructure :

- Une gestion complète des certificats numériques, pendant toute leur durée de vie, qui offre :
  - la capacité de demander, renouveler et retirer des certificats ;
  - une autorité d'enregistrement pour valider les requêtes de certificat ;
  - une autorité de certification pour créer des certificats numériques et des listes de révocations.
- Des fonctions d'enregistrement avancées qui permettent aux entreprises d'enregistrer en ligne les entités e-business sécurisées. L'application d'enregistrement se fonde sur les principes énumérés ci-dessous.
  - Les certificats émis et gérés doivent offrir les garanties de sécurité exigées par les applications e-business particulièrement exposées, et l'autorité d'enregistrement doit elle aussi être capable de satisfaire ces exigences de sécurité.
  - L'application doit être suffisamment flexible pour supporter l'ensemble des règles d'enregistrement, parmi lesquelles les approbations manuelles ou automatiques, l'authentification flexible sur site et à l'extérieur et la possibilité d'isoler les règles d'enregistrement dans des domaines sécurisés séparés.

Le modèle de sécurisation permet de garantir l'accessibilité, la confidentialité, l'intégrité et l'origine des transaction électroniques. Par le codage numérique, la certification et la signature, Trust Authority sécurise l'activité e-business conduite sur l'Internet, dans un intranet ou dans un réseau privé virtuel. Pour sécuriser davantage sa clé de signature, l'autorité de certification travaille avec des données chiffrées.

Configuration logicielle et matérielle requise pour le serveur Trust Authority

Les programmes de serveur requis par Trust Authority sont détaillés dans le tableau 10 à la page 76.

Tableau 10. Programmes de serveur et configuration matérielle requis pour Public Key Infrastructure Trust Authority

Produit	Remarques
L'un des systèmes d'exploitation suivants : • IBM AIX/6000 (AIX), version 4.3.2 • Windows NT version 4.0 avec Service Pack 5	• Obligatoire • Vous devez installer tous les programmes de serveur de Trust Authority sur la même plate-forme. Il n'est pas possible de combiner des machines AIX et Windows NT dans une même configuration.
IBM SecureWay Directory Version 3.1.1	• Obligatoire et intégré au code de Trust Authority. • Vous pouvez installer le logiciel SecureWay Directory sur la même machine et en même temps que Trust Authority, ou l'installer sur une machine distante.
IBM WebSphere Application Server Version 2.02, Standard Edition. Comprend IBM HTTP Server Version 1.3.3 et le Sun Java Development Kit (JDK) 1.1.7.	• Obligatoire. Fourni avec Trust Authority. • Avant d'installer Trust Authority, vous devez installer le logiciel du serveur Web sur la machine où vous avez prévu d'installer Trust Authority et le serveur Trust Authority.
IBM DB2 Universal Database Enterprise Edition Version 5.2 avec mise à jour de maintenance 9.	• Obligatoire. Fourni avec Trust Authority. • Installez une instance du gestionnaire de bases de données pour chaque serveur. Avant d'installer Trust Authority, vous devez installer DB2 sur chaque machine destinée à héberger un serveur Trust Authority.
• Coprocesseur de chiffrement IBM SecureWay 4758 PCI 001 • IBM SecureWay 4758 CCA Support Program, version 1.3.0.0 avec mise à jour de maintenance 1.3.0.1	• *Facultatif* et uniquement disponible pour les systèmes AIX. Vous devez commander ce produit auprès de votre revendeur IBM habituel. • Avant d'installer Trust Authority, vous devez installer le coprocesseur 4758 et son gestionnaire sur le serveur destiné à héberger l'autorité de certification de Trust Authority. • Le coprocesseur de chiffrement 4758 requiert un bus PCI sur les systèmes RS/6000.

Le tableau 11 à la page 77 et le tableau 12 à la page 78 détaillent la configuration matérielle requise pour les serveurs Trust Authority.

Dans le tableau 11 à la page 77 et le tableau 12 à la page 78 :

- Un petit environnement de fabrication délivre plusieurs centaines de certificats quotidiennement.
- Un environnement de fabrication intermédiaire délivre quelques milliers de certificats quotidiennement.

- Un grand environnement de fabrication délivre plusieurs dizaines de milliers de certificats quotidiennement. Ceci peut concerner un système fournissant des services d'autorité de certification tiers à d'autres entreprises.

Dans le cas de Trust Authority pour Windows NT, IBM recommande d'installer le programme sur un système IBM NetFinity Server. Le tableau suivant fournit des recommandations pour définir la taille idéale de votre système en fonction du nombre de certificats que l'autorité de certification de Trust Authority peut être amenée à délivrer.

Tableau 11. Exemple de configuration pour une machine Windows NT

Type de machine	**Processeurs**	**Espace disque**	**Mémoire**
Petit environnement de fabrication			
Netfinity 3000	1 (450 MHz, Pentium II)	2 unités (9,1 Go)	256 Mo
Netfinity 5000	2 (450 MHz, Pentium II)	2 unités (9,1 Go)	512 Mo
Environnement de fabrication intermédiaire			
Netfinity 3000	1 (500 MHz, Pentium III)	4 unités (18,2 Go)	768 Mo
Netfinity 5000	2 (500 MHz, Pentium III)	4 unités (9,1 Go)	1 Go
Grand environnement de fabrication			
Netfinity 5500	2 (450 MHz, Pentium III)	4 unités (9,1 Go ultra-rapide)	1 Go
Netfinity 5500	4 (500 MHz, Pentium III Xeon avec 1024 Ko de mémoire cache de niveau 2)	4 unités (9,1 Go ultra-rapide)	1 Go
Netfinity 7000	2 (500 MHz, Pentium III avec 512 Ko de mémoire cache de niveau 2)	4 unités (9,1 Go ultra-rapide)	1 Go

Tableau 11. Exemple de configuration pour une machine Windows NT (suite)

Type de machine	Processeurs	Espace disque	Mémoire
Netfinity 7000	4 (500 MHz, Pentium III Xeon avec 1024 Ko de mémoire cache de niveau 2)	4 unités (18,2 Go)	2 Go

Dans le cas de Trust Authority pour AIX, IBM recommande d'installer le programme sur un système IBM RISC System/6000. La table suivante fournit des recommandations pour définir la taille idéale de votre système en fonction du nombre de certificats que l'autorité de certification de Trust Authority peut être amenée à délivrer.

Tableau 12. Exemple de configuration matérielle pour une machine AIX

Type de machine	Processeurs	Espace disque	Mémoire
Petit environnement de fabrication			
F40	2 (233 MHz)	2 unités (9,1 Go, Ultra 2 Fast Wide)	512 Mo
Environnement de fabrication intermédiaire			
F40	2 (233 MHz)	3 unités (9,1 Go, Ultra 2 Fast Wide)	1 Go
Grand environnement de fabrication			
F50	4 (332 MHz)	5 unités (une de 9,1 Go Ultra 2 Fast Wide et quatre de 9,1 Go SSA)	2 Go
H50	4 (332 MHz)	5 unités (une de 9,1 Go Ultra 2 Fast Wide et quatre de 9,1 Go SSA)	2 Go
R50	6 (200 MHz)	2 unités (9,1 Go, Ultra 2 Fast Wide)	1 Go
R50	8 (200 MHz)	5 unités (une de 9,1 Go Ultra 2 Fast Wide et une armoire 7133 SSA avec quatre unités de 9,1 Go SSA)	2 Go

Configuration logicielle et matérielle requise pour le client Trust Authority

IBM recommande la configuration suivante pour les stations de travail utilisant les formulaires d'inscription par navigateur et le programme client de Trust Authority.

- La configuration matérielle suivante :
  - Processeur Intel 486 166 MHz avec RAM de 32 Mo au minimum (recommandé : processeur Intel Pentium 200 MHz avec au moins 64 Mo de mémoire)

  - Carte graphique
  - Ecran vidéo VGA ou qualité supérieure
  - Souris ou périphérique de pointage équivalent
- L'un des systèmes d'exploitation suivants :
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT, version 4.0
- L'un des navigateurs Web suivants :
  - Netscape Navigator ou Netscape Communicator, version 3.0 ou ultérieure
  - Microsoft Internet Explorer, version 4.0 ou ultérieure (activer Java)

Interaction entre IBM KeyWorks Toolkit et IBM SecureWay Trust Authority

N'installez pas IBM KeyWorks Toolkit sur le même serveur que IBM SecureWay Trust Authority.

Chapitre 15. Remarques sur la procédure et les conditions d'installation de Toolbox

Le produit FirstSecure Toolbox contient plusieurs interfaces de programmation d'applications (API) qui permettent de créer des applications sécurisées pour votre e-business.

- Services d'autorisation
- Services de gestion et de certification
- Services d'annuaire
- Services de protocole SSL (Secure Sockets Layer)
- Services de sécurisation et de cryptographie KeyWorks
  - API IBM Key Recovery Service Provider 1.1.3.0 . Le composant IBM Key Recovery Service Provider permet de restaurer des informations codées.
  - IBM Key Recovery Server 1.1.3.0. Le produit IBM Key Recovery Server 1.1.3.0 est une application qui, sous réserve d'une requête autorisée, peut restaurer des informations codées dont la clé est indisponible, a été perdue ou altérée.

    Ces deux boites à outils contiennent des interfaces standard permettant aux applications d'accéder à des services de sécurité critiques. Les modules de sécurité peuvent également utiliser ces interfaces pour accéder au composant Toolkit. La conception de ces interfaces standard repose sur l'architecture CDSA (Common Data Security Architecture). Les deux boîtes à outils sont disponibles en version Windows NT, Solaris et AIX.

Configuration logicielle et matérielle requise pour Toolbox

La configuration matérielle requise pour Toolbox est détaillée dans le tableau 13.

Tableau 13. Configuration matérielle requise pour Toolbox

Plate-forme	Espace disque	Mémoire
Version 4.0, Service Pack 5	2 à 4 Go	64 Mo
AIX 4.3.2	9,1 Go	1 Go
Sun Solaris, Version 2.6, avec le Fix Pack de mai 1999	4,2 Go	128 Mo

Tableau 14. Conditions matérielles requises pour les composants Toolbox

Toolkit	Type de machine	Espace disque	Mémoire
IBM KeyWorks Toolkit	Système supportant les produits exécutés sur : Windows NT Version 4.0, Service Pack 5 ou version ultérieure Windows 95 AIX 4.2 ou version ultérieure Sun Solaris	50 Mo	32 Mo
IBM Key Recovery Service Provider	Matériel supportant les produits exécutés sous : Windows NT Version 4.0, Service Pack 5 ou version ultérieure Windows 95 AIX 4.2 ou version ultérieure Sun Solaris	50 Mo	32 Mo

Les conditions logicielles requises pour l'installation des composants de Toolbox sont présentées dans le tableau ci-après.

Tableau 15. Conditions logicielles requises pour l'installation des composants de Toolbox

Composant Toolbox	Plates-formes Microsoft Windows		AIX	Solaris
	Client	Serveur	Serveur	Serveur
IBM KeyWorks Toolkit	Windows NT Version 4.0, Service Pack 5 ou version ultérieure Windows 95	Windows NT Version 4.0, Service Pack 5 ou version ultérieure Windows 95	AIX 4.2 ou version ultérieure[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT Version 4.0, Service Pack 5 ou version ultérieure[2] Windows 95	Windows NT Version 4.0, Service Pack 5 ou version ultérieure	AIX 4.2 ou version ultérieure	Sun Solaris

Remarques :
1. Le client AIX est également supporté.
2. De plus, IBM KeyWorks Toolkit est requis.

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1 offre aux développeurs d'applications une méthode ouverte, extensible et standard permettant d'accéder aux fonctions de chiffrement et de sécurité dans des environnements d'exploitation différents.

IBM KeyWorks Toolkit fournit des API standard à l'aide desquelles les applications peuvent accéder à des services critiques de chiffrement, de sécurisation et de sécurité, ainsi que des interfaces standard utilisées par les modules complémentaires Service Provider pour accéder au composant Toolkit. Ces interfaces standard reposent sur l'architecture CDSA (Common Data Security Architecture), un standard de Open Group développé initialement par Intel Corporation puis par IBM pour aboutir au produit KeyWorks Toolkit. Lorsque vous utilisez des interfaces standard :

- Votre entreprise choisit le système de chiffrement et de sécurisation le mieux adapté à ses besoins sans modifier les applications utilisant les services de sécurité.
- La productivité des programmeurs d'applications et de logiciels intermédiaires est accrue.

IBM KeyWorks Toolkit joue un rôle d'isolant entre les applications et les logiciels intermédiaires, les fonctions de chiffrement et les modules Service Provider. Cette boîte à outils comporte un logiciel de base et des modules Service Provider complémentaires.

Le logiciel de base fournit aux applications l'interface API CSSM (Common Security Services Manager), basée sur l'architecture CDSA d'Intel Corporation et dotée d'un grand nombre de fonctionnalités. IBM a optimisé l'API CSSM en y ajoutant des fonctions de récupération de clés. Avec IBM KeyWorks Toolkit, l'application peut :

- chiffrer et déchiffrer les informations ;
- contrôler les signatures numériques à diverses fins ;
- extraire des répertoires les certificats et les listes de retrait de certificats ;
- créer des zones pour la récupération des clés et la sauvegarde du chiffrement ;
- décider si un certificat peut être considéré comme sécurisé, sur la base des critères établis par les ingénieurs système et les programmeurs d'après les instructions des utilisateurs.

En général, une entreprise ou un constructeur OEM intègre IBM KeyWorks Toolkit et IBM Key Recovery Service Provider Toolkit aux applications et aux logiciels intermédiaires pour leur permettre d'utiliser les interfaces API CSSM avec la fonction CSSM. Le produit de cette intégration est un ensemble d'applications d'exécution et intermédiaires destiné aux clients et aux serveurs répartis dans le ou les environnements d'exploitation. Les autres éléments de FirstSecure dépendront, à plus long terme, d'IBM KeyWorks Toolkit pour les services de chiffrement et les opérations de sécurisation.

La personne utilisant IBM KeyWorks Toolkit pour réaliser les intégrations doit pouvoir se faire assister par des ingénieurs système et des programmeurs ayant une bonne expérience de la programmation et de la conception des systèmes de cryptographie, des logiciels intermédiaires et des logiciels de base, dans son entreprise ou dans le cadre d'une collaboration avec un sous-traitant ou un constructeur OEM ayant une expérience dans ces domaines.

Le logiciel de base offre aux fournisseurs de services l'interface standard Service Provider Interface (SPI), fondée sur l'architecture CDSA de Open Group. IBM a étendu les fonctionnalités de l'interface SPI en y ajoutant des fonctions de récupération de clés.

IBM KeyWorks Toolkit (SDK) comporte des modules complémentaires, fournis par des fournisseurs de services, qui supportent des normes ouvertes et des certificats à clé publique propriétaires. Ces modules sont les suivants : PKCS#11, fonctions de chiffrement BSAFE de RSA Data Security, certificats

X.509 V3, règles de sécurisation Entrust et VeriSign et protocole Lightweight Directory Access Protocol (LDAP). Le logiciel de base intègre de manière parfaite les fonctions de chiffrement, de sécurisation et de sécurité fournies par les modules conçus par des fournisseurs de services indépendants.

IBM KeyWorks Toolkit fournit les fonctions d'administration clé énumérées ci-dessous.

- Protection contre tout risque de non respect de certaines étapes essentielles du processus d'utilisation de KeyWorks
- Vérification de la bonne marche des modules complémentaires Service Provider avant utilisation
- Utilisation des modules complémentaires Service Provider uniquement en association avec le logiciel de base
- Support des normes de chiffrement et de sécurité en vigueur dans un pays ou dans une entreprise

IBM KeyWorks Toolkit présente les avantages suivants :

- Possibilité de modifier ou de remplacer les modules Service Provider sans devoir réécrire les applications et les logiciels intermédiaires
- Support transparent du chiffrement matériel et des signatures numériques
- Support des annuaires LDAP et de la norme de signature DSA
- Libre choix de l'autorité de certification utilisée

Pour plus d'informations sur IBM KeyWorks Toolkit, reportez-vous au manuel *IBM KeyWorks Toolkit Developer's Guide*.

Interaction entre IBM KeyWorks Toolkit et IBM SecureWay Trust Authority

N'installez pas IBM KeyWorks Toolkit sur le même serveur que IBM SecureWay Trust Authority.

IBM Key Recovery Service Provider Toolkit 1.1

IBM Key Recovery Service Provider 1.1.3.0 , fourni sous la forme d'une boîte à outils, est un module Service Provider qui utilise les fonctions standard offertes par IBM KeyWorks Toolkit. Il permet de restaurer des informations chiffrées, transmises puis stockées sans extraire, ni dévoiler les clés privées, ceci sans fragiliser le système de chiffrement.

Dans la mesure où IBM Key Recovery Service Provider utilise les fonctions standard fournies par IBM KeyWorks Toolkit, la fonction de récupération de clés peut être utilisée avec différents produits de chiffrement, avec des certificats standard émis par des autorités de certification différentes, avec les règles de sécurisation VeriSign et Entrust et avec n'importe quel annuaire

accessible à l'aide du protocole LDAP. IBM Key Recovery Service Provider crée des informations de récupération de clés basées sur la clé de session associée à la communication établie entre les correspondants.

Pour plus d'informations sur IBM Key Recovery Service Provider, consultez le manuel *Key Recovery Server Installation and Usage Guide*, fourni dans le Documentation Pack de FirstSecure.

Chapitre 16. Documentation des produits FirstSecure

Chaque composant de la solution FirstSecure est livré avec sa documentation. Ce chapitre contient des informations sur la documentation fournie avec chacun de ces composants.

Pour chaque offre SecureWay FirstSecure, SecureWay, Policy Director et SecureWay Boundary Server, un Media Pack et un Documentation Pack sont disponibles. Les Media Pack contiennent les CD-ROM du produit qui permettent d'installer les différents composants de l'offre, accompagnés dans certains cas d'une documentation en ligne. Lorsqu'elle est disponible, la copie papier des manuels est fournie sous la forme d'un Documentation Pack. Le contenu des Documentation Packs est détaillé dans la section «Documentation pack de FirstSecure» à la page 95.

Policy Director

Les produits Policy Director sont fournis avec la documentation suivante :

IBM SecureWay Policy Director - Guide de configuration et d'utilisation
: Explique comment installer et configurer IBM SecureWay Policy Director.

IBM SecureWay Policy Director - Guide d'administration
: Explique comment administrer IBM SecureWay Policy Director. Ce manuel est fourni au format PDF.

IBM SecureWay Policy Director - Guide de programmation et de référence
: Explique comment créer des programmes pour IBM SecureWay Policy Director. Ce manuel est fourni au format PDF.

Fichier README du produit
: Ces informations sont disponibles sur le site Web : www.ibm.com/software/security/policy

SecureWay Boundary Server

Le manuel suivant décrit les composants de SecureWay Boundary Server, leurs conditions d'utilisation et leurs interactions.

IBM SecureWay Boundary Server pour Windows NT et AIX - Guide de configuration et d'utilisation
: Ce manuel imprimé décrit les composants de SecureWay Boundary Server.

Les sections ci-après présentent la documentation fournie avec les composants de SecureWay Boundary Server.

IBM SecureWay Firewall

Toute la documentation du produit IBM Firewall est fournie sous forme de fichiers. IBM Firewall s'accompagne de la documentation ci-dessous.

IBM SecureWay Firewall pour AIX - Setup and Installation
: Instructions d'installation et de configuration d'IBM SecureWay Firewall pour AIX.

IBM SecureWay Firewall pour Windows NT - Setup and Installation
: Instructions d'installation et de configuration d'IBM SecureWay Firewall pour Windows NT.

IBM SecureWay Firewall pour AIX - Guide de l'utilisateur
: Instructions d'installation et de configuration d'IBM SecureWay Firewall pour Windows NT.

IBM SecureWay Firewall pour Windows NT - Guide de l'utilisateur
: Informations sur l'utilisation d'IBM Firewall pour Windows NT.

IBM SecureWay Firewall pour Windows NT - Manuel de référence
: Contient des informations de référence sur l'utilisation d'IBM Firewall pour Windows NT.

IBM SecureWay Firewall pour AIX - Manuel de référence
: Contient des informations de référence sur l'utilisation d'IBM Firewall pour AIX.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
: Contient des instructions pour l'identification des incidents.

IBM SecureWay Firewall VPN Client User's Guide
: Explique comment créer et utiliser un réseau privé virtuel.

MIMEsweeper

MIMEsweeper est fourni avec la documentation ci-dessous.

MIMEsweeper Administrator's Guide
: Contient une section sur les notes d'édition, suivie d'informations sur la planification et l'installation.

  Ce document est fourni au format HTML sur le CD-ROM du produit. Vous pouvez le consulter en ligne en ouvrant le fichier \DOC\MANUAL.HTM avec un navigateur Web.

MIMEsweeper Release Notes
: Contient des informations mises à jour sur l'installation du produit et sur la procédure d'affichage de la documentation en ligne.

Ce document est fourni au format HTML sur le CD-ROM du produit. Vous pouvez le consulter en ligne en ouvrant le fichier \DOC\RELNOTES.HTM avec un navigateur Web.

MIMEsweeper Configuration Editor Help
Contient des informations sur l'édition des fichiers de configuration de MIMEsweeper.

Ce document est fourni au format HTML sur le CD-ROM du produit.

SurfinGate

SurfinGate est fourni avec la documentation ci-dessous.

SurfinGate Installation Guide
Informations relatives à l'installation et à la configuration des composants de SurfinGate 4.05 sur Windows NT. Ce document est fourni au format PDF sur le CD-ROM du produit, dans le fichier \docs\install.pdf.

SurfinGate User Guide
Document concernant la planification et l'utilisation de SurfinGate. Ce document est fourni au format PDF sur le CD-ROM du produit, dans le fichier \docs\manual.pdf.

SurfinGate 4.05 for Windows NT Release Notes
Document concernant SurfinGate 4.05, et plus particulièrement les conditions système requises et les limitations du produit. Ce document est fourni au format PDF sur le CD-ROM du produit, dans le fichier \docs\relnotes.pdf.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
Document en ligne couvrant les dernières modifications de SurfinGate. Ce document est disponible sur le CD-ROM du produit, dans le fichier \docs\rnappen.pdf.

Intrusion Immunity

Les sections suivantes présentent la documentation fournie avec le composant Intrusion Immunity.

Tivoli Cross-Site for Security

Le produit Tivoli Cross-Site for Security, Version 1.1 comprend la documentation suivante au format PDF :

Tivoli Cross-Site for Security Installation
Ce document détaille les conditions requises pour l'installation et vous guide à travers les étapes de cette procédure.

Tivoli Cross-Site for Security User's Guide
Ce document contient une présentation générale du produit, les

instructions d'utilisation de la console et d'exécution des tâches, des informations de référence, notamment sur les interface de ligne de commande et les fichiers de configuration, et un glossaire. Ce manuel est disponible sur le CD-ROM du produit.

Norton AntiVirus

Norton AntiVirus est fourni avec une documentation sur les composants pris en charge par FirstSecure. Tous les documents, à l'exception du fichier contents.txt, sont fournis au format PDF sur le CD-ROM de Norton AntiVirus. Le fichier contents.txt est un fichier ASCII.

Documentation du CD-ROM de Norton AntiVirus Solution Release 3.04

Le CD-ROM du produit Norton AntiVirus Solution Release 3.04 contient une fichier appelé \contents.txt qui répertorie tous les documents présents sur le CD-ROM.

Solutions d'administration :

Norton AntiVirus Solution Implementation Guide
Fichier \docs\admin\navimp.pdf sur le CD-ROM du produit.

Norton AntiVirus Command-Line Scanner
Fichier \docs\navc\navcugd.pdf sur le CD-ROM du produit.

Emergency Rescue Disk creation
Fichier \navc\readme.txt sur le CD-ROM du produit.

Solutions pour serveur :

Norton AntiVirus for Windows NT Server Administrator's Guide
Fichier \docs\admin\navnts50.pdf sur le CD-ROM du produit.

Norton AntiVirus for NetWare User's Guide
Fichier \docs\NAVNLM\NVN4.pdf sur le CD-ROM du produit.

Norton AntiVirus for Lotus Notes Installation Guide
Fichier \docs\NAVNOTES\NAVNOTES.pdf sur le CD-ROM du produit.

Norton AntiVirus for Lotus Notes Installation Guide
Fichier \docs\NAVNOTES\NAVNOTES.pdf sur le CD-ROM du produit.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
Fichier \docs\NOTESOS2\NOTESOS2.pdf sur le CD-ROM du produit.

Norton AntiVirus for Microsoft Exchange Installation Guide
Fichier \docs\NAVXCHNG\NAVXCHNG.pdf sur le CD-ROM du produit.

Solutions pour passerelle :

Norton AntiVirus for Internet Email Gateway User's Guide
Fichier \docs\navieg\navieg.pdf sur le CD-ROM du produit.

Norton AntiVirus for Firewalls Administrator's Guide
Fichier \docs\navfw\navfw.pdf sur le CD-ROM du produit.

Solutions pour poste de travail :

Norton AntiVirus User's Guide for Windows 3.1/DOS
Fichier \docs\navwks\nav4dusr.pdf sur le CD-ROM du produit.

Norton AntiVirus Reference Guide for Windows 3.1/DOS
Fichier \docs\navwks\nav4dref.pdf sur le CD-ROM du produit.

Norton AntiVirus for Windows 95/98 User's Guide
Fichier \docs\navwks\nav98usr.pdf sur le CD-ROM du produit.

Norton AntiVirus for Windows 95/98 Reference Guide
Fichier \docs\navwks\nav98ref.pdf sur le CD-ROM du produit.

Norton AntiVirus for Windows NT User's Guide
Fichier \docs\navwks\nav5nusr.pdf sur le CD-ROM du produit.

Norton AntiVirus for Windows NT Reference Guide
Fichier \docs\navwks\nav5nref.pdf sur le CD-ROM du produit.

Norton AntiVirus v4.0 User's Guide for Windows NT
Fichier \docs\351\navntugd.pdf sur le CD-ROM du produit.

Norton AntiVirus v4.0 Reference Guide for Windows NT
Fichier \docs\351\navntref.pdf sur le CD-ROM du produit.

Norton AntiVirus User's Guide for OS/2
Fichier \docs\navos2\navos2ug.pdf sur le CD-ROM du produit.

Norton AntiVirus Distribution Guide for OS/2
Fichier \docs\navos2\navos2dg.pdf sur le CD-ROM du produit.

Norton AntiVirus for Macintosh User's Guide
Fichier \docs\navmac\navmac.pdf sur le CD-ROM du produit.

Livres blancs sur le CD-ROM de Norton AntiVirus Solution Release 3.04 :
Le répertoire \sarc du CD-ROM contient une série de livres blancs. Chaque livre blanc est au format PDF.

Séquences vidéo du CD-ROM de Norton AntiVirus Solution Release 3.04 :
Le CD-ROM contient également des séquences vidéo. Pour visualiser ces séquences, vous devez disposer du programme Media Player ou d'un autre programme capable de lire les fichiers .AVI. Ces fichiers sont les suivants :

SARC \sarc\sarc.avi

About Viruses (A propos des virus)
\sarc\aboutvir.avi

Norton AntiVirus: the Guided Tour (Visite guidée)
\navtour\guided\demo32.exe

How to Respond When Norton AntiVirus Alerts You (Comment répondre en cas d'alerte de Norton AntiVirus)
\navtour\alert\demo32.exe

A Tour of Norton System Center (Visite du Norton System Center)
\nsctour\setup.exe

ou, pour lancer la visite directement à partir du CD-ROM,

\nsctour\demo32.exe

Des informations supplémentaires sur la visite sont disponibles dans le fichier \ncstour\readme.txt

Trust Authority

La documentation du produit IBM SecureWay Trust Authority est disponible au format PDF et HTML dans le CD-ROM *Trust Authority Documentation*. De nombreuses publications ont été traduites dans les langues prises en charge par Trust Authority. Pour savoir comment accéder au document présenté dans la langue de votre choix, reportez-vous au fichier *README* du produit. La dernière version du fichier *README* est disponible sur le site WEB de IBM SecureWay Trust Authority à l'adresse
http://www.ibm.com/software/security/trust/library

La bibliothèque de Trust Authority comprend les documents suivants :

IBM SecureWay Trust Authority - Guide d'initiation
Ce document donne une présentation générale du produit. Il détaille ses conditions et ses procédures d'installation et explique comment accéder à l'aide en ligne pour chaque composant. Outre dans le fichier proposé sur le CD-ROM *Documentation*, ce manuel est également fourni en version imprimée avec le produit.

IBM SecureWay Trust Authority - Guide d'administration système
Ce manuel contient des informations générales sur l'administration du système Trust Authority. Il détaille les procédures de démarrage et d'arrêt des serveurs, de modification des mots de passe, d'administration de l'autorité de certification, d'audit et de contrôle d'intégrité des données.

IBM SecureWay Trust Authority - Guide de configuration
Ce manuel explique comment utiliser le programme Assistant de

configuration pour configurer un système Trust Authority. Vous pouvez accéder à la version HTML de ce manuel tout en affichant l'aide en ligne de l'assistant.

IBM SecureWay Trust Authority - Guide du bureau de l'autorité d'enregistrement
Ce manuel explique comment utiliser le programme RA Desktop pour gérer les certificats au cours de leur existence. Vous pouvez accéder à la version HTML de ce manuel tout en affichant l'aide en ligne du bureau.

IBM SecureWay Trust Authority - Guide de l'utilisateur
Ce manuel explique comment obtenir des certificats. Il décrit comment utiliser les formulaires d'inscription de Trust Authority pour demander des certificats pour les navigateurs, les serveurs et les unités. Il montre également comment se faire pré-enregistrer pour obtenir un certificat PKIX et comment utiliser le client Trust Authority pour stocker et gérer ces certificats. Vous pouvez accéder à la version HTML de ce manuel tout en affichant l'aide en ligne du client.

Toolbox

Les sections ci-après présentent la documentation fournie avec les composants de Toolbox.

Les API de Toolbox

Toute la documentation de Toolbox est disponible sur le site WEB suivant : `www.ibm.com/software/security/firstsecure/library`. Ce site propose les documents suivants :

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
Propose une présentation générale des API et de iKeyman. Ce manuel décrit chaque API, sa syntaxe et son utilisation.

IBM SecureWay Directory Client SDK Programming Reference
Comprend plusieurs échantillons de client LDAP et une bibliothèque de clients LDAP permettant aux applications d'accéder aux serveurs LDAP. Ces programmes existent en langage C et Java.

IBM SecureWay Policy Director - Guide de programmation et de référence
Ce manuel décrit chaque API, sa syntaxe et son utilisation.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide Décrit les instructions et les conditions d'installation du produit.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
Fournit des informations destinées aux programmeurs d'applications utilisant le produit IBM SecureWay X.509 Public Key Infrastructure multi-plates-formes, également appelé PKIX. Ce manuel fournit une

présentation générale du produit et décrit les instructions servant à créer des programmes pour les différents composants de PKIX. Il décrit également les API de PKIX.

IBM KeyWorks Toolkit

Toute la documentation fournie avec IBM KeyWorks Toolkit est disponible en ligne, au format PDF, sur le CD-ROM du produit. Ces documents sont énumérés ci-après :

IBM KeyWorks Toolkit Developer's Guide
Donne une présentation générale de la boîte à outils. Ce manuel indique également comment intégrer la boîte à outils aux applications et contient un échantillon d'application.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
Définit l'interface que les développeurs d'applications utilisent pour accéder aux services de sécurité fournis par le logiciel de base et les modules des fournisseurs de services.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
Décrit les fonctions communes à tous les modules de la boîte à outils. Ce document doit être utilisé avec Service Provider Interface Specifications pour la création d'un module de fournisseur de service.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
Décrit le modèle d'interface que doivent respecter les modules des fournisseurs de service de chiffrement pour être accessibles via la boîte à outils.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
Décrit le modèle d'interface que doivent respecter les modules des fournisseurs de service d'extraction de clés pour être accessibles via la boîte à outils.

IBM KeyWorks Toolkit Trust Policy Interface Specification
Décrit le modèle d'interface que doivent respecter les autorités de certification, les émetteurs de certificats et les développeurs d'applications de sécurité, pour ajouter à la boîte à outils des règles spécifiques aux modèles ou aux applications.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
Décrit le modèle d'interface que doivent respecter les développeurs de bibliothèques de certificats pour fournir des services de manipulation de certificats aux applications de type boîte à outils et aux modules de règles de sécurisation.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
Décrit le modèle d'interface que doivent respecter les développeurs de bibliothèques pour créer des solutions de stockage permanent des certificats, avec ou sans distinction de format.

IBM Key Recovery Service Provider

La documentation ci-dessous est fournie avec IBM Key Recovery Service Provider, au format PDF, sur le CD-ROM du produit.

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide Décrit le concept de récupération de clés, indique comment mettre en place une solution de récupération de clés dans une entreprise et présente la procédure à suivre pour installer, configurer et exécuter IBM Key Recovery Server.

Livres rouges de la sécurité

Les livres rouges suivants, produits par l'ITSO (IBM International Technical Support Organization), couvrent les produits et les processus en rapport avec la sécurité. Vous pouvez vous les procurer sur le site Web suivant : www.us.ibm.com/redbooks.

- *Understanding the IBM SecureWay FirstSecure Framework*
- *High Availability IBM eNetwork Firewall*

Documentation packs

Les documentation packs suivants sont disponibles pour le produit IBM SecureWay FirstSecure.

Documentation pack de FirstSecure

Le documentation pack de FirstSecure contient les documents suivants :

- FirstSecure License Information
- *IBM SecureWay FirstSecure - Guide de planification et d'intégration*
- *IBM SecureWay Policy Director - Guide de configuration et d'utilisation*
- *IBM SecureWay Boundary Server pour Windows NT et AIX - Guide de configuration et d'utilisation*
- *IBM SecureWay Trust Authority - Guide d'initiation*
- *Tivoli Cross-Site for Security Installation*

Documentation pack de Policy Director

Le documentation pack de Policy Director contient les documents suivants :

- Policy Director License Information
- *IBM SecureWay Policy Director - Guide de configuration et d'utilisation*

Documentation pack de SecureWay Boundary Server

Le documentation pack de SecureWay Boundary Server contient les documents suivants :

- SecureWay Boundary Server License Information

- *IBM SecureWay Boundary Server pour Windows NT et AIX - Guide de configuration et d'utilisation*

Partie 4. Annexes

Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Cela ne signifie pas qu'IBM ait l'intention de les y annoncer. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM.

Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM.

Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Le présent document peut également contenir des programmes réduits fournis par IBM à titre de simple exemple et d'illustration. Ces programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. LES GARANTIES IMPLICITES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS SONT EXPRESSEMENT EXCLUES.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document.

La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes

La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux termes du Contrat sur les produits et services IBM, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut

confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation dans certains pays :

AIX
AIX/6000
DB2
DB2 Universal Database
eNetwork
Global Sign-On
GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Les termes qui suivent sont des marques d'autres sociétés :

Intel et Pentium sont des marques d'Intel Corporation dans certains pays.

Java et toutes les marques et logos incluant Java, sont des marques de Sun Microsystems, Inc.

Lotus, Lotus Notes, Domino et cc:Mail sont des marques de Lotus Development Corporation déposées dans certains pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation dans certains pays.

Tivoli est une marque de Tivoli Systems Inc. dans certains pays.

UNIX est une marque enregistrée aux Etats-Unis et/ou dans d'autres pays. Unix et utilisée avec l'autorisation exclusive de la société X/Open Company Limited.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Glossaire

Ce glossaire définit les termes et acronymes utilisés dans ce manuel, en particulier les termes nouveaux, peu usités ou ayant un intérêt spécifique. Il comprend des termes et définitions issus des ouvrages suivants :

- IBM Dictionary of Computing, New York, McGraw-Hill, 1994.
- American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- Answers to Frequently Asked Questions, Version 3.0, California, RSA Data Security Inc., 1996.

A

ActiveX : Dans le contexte des programmes Microsoft, ensemble de technologies et de termes de programmation orientée objet.

agent : Dans le contexte de Tivoli Cross-Site for Security, programme de contrôle des paquets IP chargé d'intercepter les paquets, de contrôler leur contenu dans les différentes couches du réseau, de consigner l'état des connexions établies et de produire des statistiques.

API : Application programming interface (interface de programme d'application).

appel de procédure à distance : (1) Egalement appelé ″appel RPC″ (Remote Procedure Call). Fonction que peut utiliser un client pour demander l'exécution d'un appel de procédure à partir d'un serveur. Cette fonction utilise une bibliothèque de procédures et une représentation externe des données. (2) Requête qu'un client adresse à un fournisseur de service situé sur un autre noeud du réseau.

applet : Programme informatique, écrit sous Java, qui s'exécute dans le cadre d'un navigateur compatible Java tel que Netscape Navigator. Egalement appelé ″applet Java″.

application Web : Application conçue pour être utilisée via le World Wide Web.

assistant : Programme interactif intégré à une application, qui guide pas à pas l'utilisateur dans une tâche au moyen d'instructions.

authentification : Processus consistant à établir de manière certaine l'identité d'une partie impliquée dans une communication.

autorisation : Processus visant à déterminer les types d'activité qu'un utilisateur peut exercer. D'une manière générale, l'autorisation intervient après l'authentification.

autorité de certification : Entité, organisme ou logiciel chargé d'appliquer les règles de sécurité élaborées par une organisation et d'attribuer des identités électroniques sécurisées sous la forme de certificats. L'autorité de certification administre les requêtes d'obtention, de renouvellement et de révocation des certificats.

B

Bloodhound : Dans le contexte de Norton AntiVirus, nom du composant chargé de rechercher et d'éliminer les virus.

C

canal : Chemin emprunté par les signaux envoyés.

cellule : Dans le contexte d'un environnement informatique partagé (DCE), groupe d'utilisateurs, de systèmes ou de ressources partageant une mission et des frontières communes pour la sécurité, l'administration et la désignation. Une cellule comprend généralement des utilisateurs, des machines et des ressources

partageant une même finalité et un niveau de sécurisation supérieur à celui dont ils jouissent à l'extérieur de cette cellule.

certificat numérique : Droit d'accès électronique délivré par un tiers sécurisé à une personne ou à une entité. Un certificat contient des informations sur l'entité qu'il certifie.

chiffrement : Transformation des informations visant à permettre exclusivement à une personne détenant la clé de déchiffrement appropriée de leur rendre leur forme d'origine. Synonyme de codage.

clé publique : Clé de la paire de clés publique/privée pouvant être communiquée aux tiers. La clé publique permet aux tiers d'acheminer une transaction jusqu'à son propriétaire et de vérifier une signature numérique. Les données codées avec la clé publique ne peuvent être décodées qu'avec la clé privée associée. Voir aussi *paire de clés publique/privée*.

client : (1) Unité fonctionnelle destinataire des services partagés d'un serveur. (2) Ordinateur ou programme demandant à accéder à un service fourni par un autre ordinateur ou programme.

code mobile : Caractérise les opérations réalisées à partir d'un ordinateur portable par un utilisateur changeant fréquemment de lieu et utilisant différents types de connexion de réseau (par modem, par réseau local, ou liaison sans fil, par exemple).

commerce électronique : Ce terme couvre les transactions commerciales passées au moyen de réseaux et d'ordinateurs, à l'exclusion des transferts de fonds. Il désigne les achats et ventes de biens et services (impliquant des clients, des fournisseurs, des fabricants, etc.) réalisés sur l'Internet. Le commerce électronique est la composante principale du e-business.

contrôle d'accès : Dans le contexte de la sécurité informatique, processus visant à s'assurer que les ressources d'un système informatique soient exclusivement utilisées par des utilisateurs et d'une manière autorisés.

D

DCE : Distributed Computing Environment (environnement informatique partagé).

démon : Dans le contexte d'AIX, programme résident chargé de répondre à un type de requête défini.

E

e-business : Désigne les transactions commerciales passées au moyen de réseaux et d'ordinateurs. Ce terme recouvre les achats et ventes de biens et services ainsi que les transferts de fonds réalisés par le biais de communications électroniques.

environnement de développement intégré : Programme de développement d'applications permettant de coder une application, de l'exécuter pas à pas et de recevoir une aide au diagnostic des erreurs de programmation.

environnement informatique partagé : Egalement appelé DCE (Distributed Computing Environment). Ensemble des services et des utilitaires de création, d'utilisation et de gestion des applications partagées dans un environnement informatique hétérogène.

espace des noms : Dans le contexte de l'annuaire, représentation externe des noms accessible aux utilisateurs.

extranet : Réseau externe inspiré de la technologie de l'Internet. Certaines sociétés commencent à intégrer les outils de communication du Web, le commerce électronique, la messagerie et les applications de travail en groupe à l'usage de leurs clients, partenaires ou salariés.

F

fichier d'audit : Données indiquant un chemin logique reliant une suite d'événements. Le processus d'audit permet le suivi des transactions et la gestion de l'historique d'une

activité donnée. Par exemple, il peut surveiller l'activité du compte d'un utilisateur.

File Transfer Protocol (FTP) : Protocole de transaction client-serveur pour Internet, utilisé pour le transfert de fichiers entre ordinateurs.

filtrage des adresses de réseau : Processus consistant à contrôler les adresses contenues dans les messages entrant et sortant du réseau pour vérifier la validité du destinataire ou de l'émetteur.

filtrage des contenus : Analyse syntaxique du contenu d'une transmission en vue de déterminer si ce contenu respecte des normes spécifiques.

I

IDE : Integrated development environment (environnement de développement intégré).

incident : Dans le contexte de Tivoli Cross-Site for Security, activité suspecte pouvant témoigner d'une tentative d'intrusion dans le système.

interface de programme d'application : Interface d'exploitation permettant à un programme d'application écrit dans un langage haut niveau d'utiliser des fonctions définies.

Internet : Structure internationale reliant des réseaux et permettant d'établir des communications électroniques entre ordinateurs. Le réseau mondial Internet permet aux ordinateurs de communiquer entre eux à l'aide de logiciels tels que les navigateurs Web ou les programmes de messagerie électronique. Des universités, des entreprises et autres organisations, disposent de réseaux qui, reliés à d'autres réseaux de même nature, constituent l'Internet.

intranet : Réseau interne d'entreprise habituellement protégé des communications provenant de l'extérieur par un ou plusieurs pare-feu. Ce type de réseau est inspiré de la technologie de l'Internet. Sur un plan technique, un intranet est une simple extension de l'Internet. Le langage HTML (langage permettant de créer des représentations graphiques des informations) et le protocole HTTP (protocole de transfert de fichier hypertexte dans l'Internet) sont deux outils fondamentaux de l'Internet.

intrus : Egalement appelé "hacker". Personne essayant de pénétrer dans une machine ou un système sans autorisation. En général, les intrus tentent d'utiliser des ressources sans autorisation.

IPSec : Internet Protocol Security. Protocole de communication Internet standard développé par le IETF. Le protocole IPSec est un protocole de réseau conçu pour apporter des services de sécurité cryptographiques permettant de combiner des processus d'authentification et de contrôle d'accès tout en assurant l'intégrité et la confidentialité des données. Ses fonctions d'authentification performantes l'ont fait adopter par plusieurs concepteurs de réseaux privés virtuels pour les connexions bilatérales sécurisées sur l'Internet.

ISV : Independent Software Vendor (éditeur de logiciel indépendant).

J

Java : Ensemble de technologies d'informatique de réseau, indépendantes des plate-formes, développées par Sun Microsystems. L'environnement Java comprend le système d'exploitation Java OS, les machines virtuelles correspondant aux différentes plates-formes, le langage de programmation orientée objet Java et plusieurs bibliothèques de classes d'objets.

JavaScript : Langage dédié à la création de scripts, proche de Java et développé par Netscape pour les besoins du navigateur Netscape.

jeton SecurID : Méthode d'authentification du produit ACE/Server, développée par Security Dynamics. Cette méthode utilise un ID utilisateur et un jeton (ou carte) SecurID. Lorsque l'utilisateur se connecte à distance, son mot de passe lui est délivré à partir du jeton SecurID. Ce mot de passe change toutes les 60 secondes et ne peut être utilisé qu'une seule fois. Même si un

autre utilisateur l'intercepte dans le réseau, le mot de passe ne peut pas être réutilisé.

K

Kerberos : Méthode sécurisée permettant d'authentifier un service demandant à accéder à un ordinateur. La méthode Kerberos a été développée dans le cadre du projet Athena par le MIT (Massachussets Institute of Technology). Dans la mythologie grecque, Kerberos est un chien tricéphale gardant la porte de l'enfer. Kerberos permet à l'utilisateur de demander un ticket codé à un processus d'authentification pour demander accès à un service donné d'un serveur. De cette manière, l'utilisateur n'a pas besoin de communiquer son mot de passe.

L

LCA : Liste de contrôle d'accès.

LDAP : Lightweight Directory Access Protocol (protocole simplifié d'accès à l'annuaire).

Lightweight Directory Access Protocol : Dans le contexte d'IBM SecureWay Directory, le module LDAP permet de stocker, de mettre à jour, d'extraire et d'échanger des données d'annuaire à partir d'une base de données centralisée.

liste de contrôle d'accès : Dispositif permettant de limiter l'utilisation d'une ressource à une sélection d'utilisateurs autorisés.

M

macro bombe : Ensemble de commandes envoyé à un utilisateur par un autre en vue de créer des dommages.

MPEG : Norme en cours de développement par le MPEG (Moving Pictures Experts Group) pour la compression et le stockage numériques des séquences vidéo et des animations.

multidiffusion : Envoi de courriers électroniques non sollicités, souvent à un grand nombre de destinataires.

N

navigateur Web : Programme client, exécuté à partir d'un PC, qui permet à l'utilisateur de naviguer dans le World Wide Web ou de visualiser des pages HTML locales. Le navigateur est un outil d'extraction qui permet un accès géographiquement illimité à l'ensemble des ressources multimédia disponibles sur le Web et sur l'Internet. Les navigateurs les plus connus sont Netscape Navigator et Microsoft Internet Explorer. Voir aussi *serveur*.

non-contestation : Utilisation d'une clé privée numérique visant à empêcher le signataire d'un document de contester indûment sa signature.

O

objet Web : Objet auquel l'utilisateur accède par le biais d'un navigateur Web. Un objet Web peut être une page Web ou une partie d'un page Web, un fichier, une image, un répertoire, un programme CGI ou un applet Java.

OEM : Original Equipment Manufacturer (fabricant de matériel, par opposition aux assembleurs de matériels).

Offres de services d'accompagnement FirstSecure : Service d'assistance sur site proposé par IBM.

P

paire de clés publique/privée : La paire de clés publique/privée est un élément du concept de cryptographie par paire de clés introduit en 1976 par Diffie et Hellman pour résoudre la problématique de la gestion des clés. Selon ce concept, chaque utilisateur doit obtenir une paire de clés, une appelée la clé publique et l'autre la clé privée. La clé publique peut être communiquée aux tiers tandis que la clé privée doit rester secrète. L'émetteur et le destinataire des données n'ont pas besoin de partager des informations secrètes ; toutes les communications se font au moyen de la clé publique et la clé privée n'a besoin d'être ni transmise, ni divulguée. Dès lors, il n'est plus

nécessaire de sécuriser un canal de communication pour éviter l'interception illicite ou le détournement des données. La seule règle imposée est que la clé publique doit être associée à son propriétaire d'une manière sûre (authentifiée), par exemple, dans un annuaire sécurisé. Chacun peut envoyer un message confidentiel au moyen d'une clé publique. En revanche, ce message ne peut être décodé qu'avec une clé privée que seul le destinataire prévu doit posséder. En outre, la cryptographie par paire de clés peut être utilisée pour sauvegarder la confidentialité des données (par le chiffrement) mais aussi pour l'authentification (par la signature numérique).

pare-feu : Système ou ensemble de systèmes permettant d'établir et de protéger des frontières entre deux réseaux ou davantage.

passerelle : Système permettant à des réseaux ou applications incompatibles de communiquer ensemble.

passerelle de niveau circuit : Dans le contexte d'un pare-feu, serveur relais chargé de réorienter la requête d'un client vers le serveur de destination, via le pare-feu.

plug-in : Logiciel pouvant s'intégrer dans une application telle qu'un navigateur Web.

principal : Dans le contexte d'un DCE, entité pouvant pouvant établir des communications sécurisées avec une autre entité grâce aux dispositifs de sécurité du DCE. Un principal peut être un utilisateur, un serveur ou un ordinateur.

protocole SOCKS : Protocole permettant à une application d'un réseau sécurisé de communiquer à travers un pare-feu par le biais d'un serveur de sockets.

R

répartiteur de requêtes d'objet : Dans le contexte de la programmation orientée objet, logiciel servant d'intermédiaire transparent pour permettre aux objets d'échanger des requêtes et des réponses.

réseau privé virtuel : Réseau de données privé utilisant l'Internet au lieu des lignes téléphoniques pour établir des connexions avec des systèmes distants. Dans la mesure où les utilisateurs accèdent aux ressources du réseau de l'entreprise par l'intermédiaire d'un fournisseur de service Internet au lieu d'un opérateur de téléphonie, le coût de l'accès à distance s'en trouve notablement diminué. Un réseau privé virtuel accroît également la sécurité des échanges de données. Dans le contexte d'un pare-feu standard, le contenu d'un message peut être codé mais les adresses de sa source et de sa destination ne peuvent pas l'être. Dans le cadre d'un RPV, l'utilisateur peut établir une connexion par tunnel qui permettra d'imbriquer et de coder l'ensemble des données (contenu et en-tête).

RPC : Remote Procedure Call (appel de procédure à distance). Terme utilisé dans le contexte d'un DCE.

RPV : Réseau privé virtuel.

S

Secure Sockets Layer (SSL) : (1) Couche de sockets sécurisée. Protocole de communication standard développé par l'IETF intégrant des services de sécurité aussi transparents que possible vis-à-vis de l'utilisateur final. Le protocole SSL établit un canal de communication sécurisé numériquement. (2) Un serveur compatible SSL accepte généralement les requêtes de connexion par SSL sur un autre port que celui utilisé pour les requêtes de connexion HTTP standard. Le protocole SSL ouvre une session au cours de laquelle l'échange de protocoles n'intervient qu'une seule fois. Une fois l'échange de protocoles terminé, les communications sont codées. Le contrôle de l'intégrité des messages est continu jusqu'à la fin de la session SSL.

serveur : (1) Dans le contexte d'un réseau, station de travail fournissant des données et des fonctions à d'autres stations de travail (par exemple, un serveur de fichiers). (2) Dans le contexte de TCP/IP, système membre d'un réseau qui gère les requêtes d'un système installé

dans un autre site, dans le cadre d'une architecture client-serveur.

serveur Apache : Ensemble de logiciels de serveur Web gratuits.

serveur IntraVerse : Dans le contexte du produit IntraVerse, système du réseau qui contient le logiciel du serveur IntraVerse et qui peut communiquer avec tous les systèmes hôtes utilisant le logiciel client NetSEAT. Le terme de serveur IntraVerse désigne un système ou un ensemble de systèmes qui exécutent les programmes associés au produit.

serveur relais : Dispositif intermédiaire situé entre l'ordinateur à l'origine de la demande d'accès (ordinateur A) et l'ordinateur auquel l'accès est demandé (ordinateur B). Si un utilisateur final soumet une requête d'utilisation d'une ressource dépendante de l'ordinateur A, cette requête est adressée à un serveur relais. Le serveur relais transmet la requête à l'ordinateur B, réceptionne sa réponse, puis la restitue à l'utilisateur final (A). Les serveurs relais permettent notamment d'accéder à des ressources du World Wide Web à partir d'un domaine protégé par un pare-feu.

serveur Socks : Passerelle de niveau circuit établissant une connexion unidirectionnelle à travers un pare-feu vers des serveurs d'un réseau non sécurisé.

serveur Web : Programme de serveur qui répond aux requêtes d'accès aux informations adressées par les programmes de navigation.

service de répertoire de cellules : Egalement appelé service d'annuaire de réseaux. Composant d'un environnement informatique partagé (DCE) qui gère une base de données d'informations sur les ressources dans une cellule de DCE.

signal de présence : Signal envoyé par un programme à un programme de gestion pour confirmer son état d'activité. Le programme indique ainsi au programme de gestion qu'il est toujours actif et mobilisé par ses tâches.

site protégé : Un site protégé utilise le chiffrement pour empêcher la divulgation des informations qu'il contient à des personnes non autorisées telles que les administrateurs système ou les propriétaires d'autres sites protégés. Il utilise également les signatures numériques pour protéger les données contre la manipulation frauduleuse, et les certificats numériques pour empêcher leur divulgation à des tiers. Un site protégé utilise aussi le chiffrement, la signature et la certification pour transmettre des informations à d'autres sites protégés en toute sécurité.

T

TCP/IP : Transmission Control Protocol/Internet Protocol.

Telnet : Protocole, membre de la suite de protocoles Internet, offrant des services de connexion de terminal à distance. Ce protocole permet aux utilisateurs d'un système hôte de se connecter à un système hôte distant et de l'utiliser comme s'ils s'y étaient directement connectés.

Transmission Control Protocol/Internet Protocol : Protocole de contrôle de transmission/Protocole Internet. Série de protocoles de communication permettant des fonctions de connectivité bilatérale pour les réseaux longue distance (WAN) et les réseaux locaux.

U

Universal Resource Locator : Egalement appelé ″adresse URL″. Identificateur d'emplacement de ressource universel. Convention de désignation utilisée pour les communications sur le World Wide Web. La syntaxe du chemin d'un objet Web comprend le nom du service, suivi de celui de l'organisation, du chemin puis du nom du fichier. Par exemple, http://www.ibm.com/software/security/firstsecure.

URL : Universal Resource Locator.

V

ver : Type de virus informatique particulièrement dangereux.

X

X.509 : Norme de certificat largement acceptée et conçue pour assurer une gestion et une distribution sécurisées des certificats numériques PKI entre les réseaux Internet sécurisés. Le certificat X.509 définit des structures de données qui appliquent les procédures de distribution des clés publiques portant les signatures numériques de tiers sécurisés.

Index

J

K

L

M

N

O

P

R

S

T

U

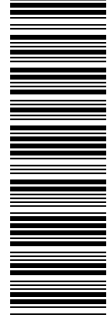
V

W

X

Z

Référence: CT7EHFR



CT7EHFR

SCT7-EHFR-00