IBM SecureWay Boundary Server pour Windows NT et AIX

Guide de configuration et d'utilisation

Version 2.0

IBM SecureWay Boundary Server pour Windows NT et AIX

Guide de configuration et d'utilisation

Version 2.0

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'«Annexe B. Remarques» à la page 41.

Deuxième édition – novembre 1999

Réf. US : CT6RZNA

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

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

Ce manuel fournit des informations sur la planification, l'installation, la configuration, l'utilisation et la résolution des incidents du produit IBM SecureWay Boundary Server pour Windows NT et AIX.

L'installation et la configuration du produit SecureWay Boundary Server implique une solide connaissance des pare-feu, des réseaux privés virtuels, de la sécurisation des contenus et de l'administration des réseaux. Dans la mesure où vous devrez préalablement installer et configurer un pare-feu pour contrôler le trafic de votre réseau, vous devez connaître le fonctionnement de celui-ci. En particulier, vous devez connaître les principes de base des adresses IP, des noms qualifiés complets et des masques de sous-réseau.

A qui s'adresse ce manuel ?

Ce manuel est destiné aux administrateurs de la sécurité des systèmes ou des réseaux chargés d'installer, de gérer et d'utiliser IBM SecureWay Boundary Server.

Compatibilité avec l'an 2000

Ces produits sont conçus pour passer l'an 2000 sans incident. Utilisés conformément aux recommandations données, 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.

Service et prise en charge

Contactez IBM pour obtenir des services et une prise en charge pour tous les produits de l'offre IBM SecureWay FirstSecure. La documentation de certains de ces produits peut mentionner une assistance fournie par une société tiers. Si vous avez acquis ces produits dans le cadre de l'offre FirstSecure, contactez IBM pour bénéficier d'une assistance technique.

Organisation du manuel

Ce manuel contient les chapitres suivants :

- Le «Chapitre 1. Présentation générale de SecureWay Boundary Server» à la page 1 donne une présentation générale de SecureWay Boundary Server et de ses composants.
- Le «Chapitre 2. Présentation d'IBM SecureWay Boundary Server» à la page 5 explique l'utilité de SecureWay Boundary Server.
- Le «Chapitre 5. Installation et configuration de SecureWay Boundary Server» à la page 19 couvre l'installation et la configuration de SecureWay Boundary Server sur les systèmes d'exploitation AIX et Windows NT.

- Le «Chapitre 3. Préparation de l'installation de SecureWay Boundary Server» à la page 11 couvre la planification de l'installation de SecureWay Boundary Server.
- Le «Chapitre 4. Configuration requise pour l'installation de SecureWay Boundary Server» à la page 17 détaille la configuration requise pour l'installation du produit SecureWay Boundary Server.
- Le «Chapitre 6. Documentation annexe» à la page 35 indique où rechercher les autres documents consacrés à SecureWay Boundary Server et les documents rattachés aux produits annexes.

Conventions utilisées dans ce manuel

Ce manuel utilise les conventions suivantes :

Convention	Signification
gras	Eléments des interfaces utilisateur tels que les cases à cocher, les boutons et les commandes.
espacement fixe	Valeurs par défaut des commandes et des répertoires utilisés pour SecureWay Boundary Server.
->	Série de sélections dans un menu. Par exemple : Sélectionnez **Fichier → Exécuter** signifie : Cliquez sur **Fichier**, puis cliquez sur **Exécuter**.

Informations disponibles sur le Web

Des informations relatives aux dernières mises à jour de SecureWay Boundary Server sont disponibles à l'adresse suivante :

http://www.ibm.com/software/security/boundary/library

Des informations relatives aux mises à jour des autres produits IBM SecureWay FirstSecure sont disponibles à l'adresse suivante :

http://www.ibm.com/software/security/firstsecure/library

Nouveautés de la version 2.0

La version 2.0 de SecureWay Boundary Server contient un certain nombre de nouvelles fonctions. Les plus importantes sont présentées ci-après.

Intégration avec SecureWay Policy Director

Le produit SecureWay Policy Director permet de gérer les utilisateurs relais du pare-feu IBM Firewall si celui-ci a été configuré pour utiliser SecureWay Boundary Server. Les utilisateurs relais du pare-feu sont définis pour les services de pare-feu suivants :

- Telnet
- FTP

- HTTP
- Socks

Les données des utilisateurs et des règles de sécurité associées sont stockées dans une base de données LDAP (Lightweight Directory Access Protocol).

Le module LDAP de SecureWay Directory permet de stocker, de mettre à jour, d'extraire et d'échanger des données d'annuaire à partir d'une base de données centralisée. SecureWay Policy Director gère les utilisateurs relais d'IBM Firewall stockés dans la base de données LDAP.

Optimisation du routage

Les procédures de routage utilise un plug-in appelé SurfinGate (développé par Finjan) pour filtrer le contenu des transactions du réseau.

Blocage des intrusions

Des programmes de ligne de commande permettent de créer des règles d'interdiction dynamiques au niveau du pare-feu. Ces commandes de blocage des intrusions peuvent être intégrées dans un script automatisé.

IBM SecureWay Firewall 4.1

IBM SecureWay Firewall pour Windows NT offre les fonctions suivantes :

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 dans un format proche de celui d'un réseau local Ethernet.

Optimisation d'IBM SecureWay Firewall pour AIX 4.1

IBM SecureWay Firewall pour AIX offre les fonctions suivantes :

Support renforcé d'IPSec

IBM SecureWay Firewall 4.1 comprend des fonctions de gestion optimisées pour IPSec permettant notamment le triple codage DES et la gestion de nouveaux en-têtes. Il 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.

Multiprocesseurs symétriques (SMP)

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

Optimisation des filtres

Les filtres ont été améliorés pour optimiser les performances des configurations. Vous pouvez notamment augmenter les performances du

pare-feu en choisissant l'emplacement des différents types de règles de filtrage. De plus, le nombre d'utilisations des connexions peut être journalisé.

Assistant de configuration

La configuration initiale du pare-feu IBM SecureWay Firewall se fait à l'aide d'un assistant de configuration. Ce programme permet au nouvel utilisateur de mettre en place une configuration de base immédiatement exploitable après l'installation d'IBM Firewall.

Network Security Auditor

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

Support de langue nationale pour l'allemand

Le support de langue nationale gère désormais l'allemand, en plus du portugais, de l'anglais, du français, de l'italien, du japonais, du coréen, du chinois et de l'espagnol.

Conversion d'adresse de réseau (NAT)

La conversion d'adresse de réseau (NAT) permet désormais de gérer le mappage d'adresse de type 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.

Fonctions communes à AIX et Windows NT

Security Dynamics ACE/Server

Le module Security Dynamics ACE/Server propose deux modes d'authentification. Cette fonction avancée protège votre réseau et ses données contre les intrusions malveillantes ou fortuites potentiellement dangereuses.

Optimisation de Secure Mail Proxy

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

- Algorithmes de gestion des multidiffusions permettant de bloquer les envois d'émetteurs identifiés (liste d'exclusions), vérification de la validité des messages et de la possibilité d'y répondre (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 la fonction d'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 et 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. Le navigateur doit être configuré de manière à pouvoir utiliser un serveur relais HTTP.

MIMEsweeper 2.0 pour SecureWay

MIMEsweeper contient trois composants principaux : **MAILsweeper 4.1_2**, **WEBsweeper 3.2_5** et **WEBsweeper 1.0_2**. Les principales améliorations sont les suivantes :

MAILsweeper

MAILsweeper 4.1_2 pour SMTP constitue une remarquable avancée pour le produit phare de Content Technologies qu'est MIMEsweeper. Ses nouvelles fonctions sont les suivantes :

- Une architecture hiérarchisée et simple d'emploi permet d'appliquer les règles de sécurité de manière souple, aux différents niveaux de l'entreprise, par groupe ou par utilisateur.
- Une interface utilisateur graphique standard simplifie la configuration des logiciels et la création et l'administration des règles de sécurité.
- Une nouvelle fonction, Split Delivery, s'ajoute au dispositif de gestion hiérarchique des règles de sécurité de la version 4 ; si les messages ont plusieurs destinataires, les règles appropriées sont appliquées à chacun d'eux. Les destinataires autorisés reçoivent le message tandis que les autres ne l'ont pas.
- Le traitement multi-thread des messages (utilisation simultanée de plusieurs unités d'exécution) permet d'améliorer le débit et la fiabilité du réseau ; si une ou plusieurs unités d'exécution deviennent indisponibles, les autres prennent le relais pour assurer la poursuite du traitement des messages.
- Capable d'utiliser des programmes antivirus tiers, MAILsweeper permet de détecter les virus et de nettoyer les messages et les pièces jointes.
- Des fonctions avancées d'analyse de texte (avec opérateurs NEAR, AND, NOT et OR) permettent de créer facilement des procédures complètes et performantes reposant sur la syntaxe ou l'architecture des messages.
- De puissants utilitaires d'audit permettent de transmettre des données à n'importe quelle base de données compatible ODBC.

- MAILsweeper peut gérer le serveur RBL (Real-Time Black List) qui répertorie les sites connus pour envoyer des messages indésirables. MAILsweeper peut refuser les connexions provenant d'hôtes figurant dans cette liste.
- D'une gestion facile, la sécurisation des contenus se fait au moyen d'états, de graphiques et de tableaux représentant le trafic e-mail.
- Les annuaires LDAP peuvent être utilisés.
- Le service DSN (Delivery Service Notification) gère désormais le programme d'alerte SNMP et NT Alerter.

WEBsweeper

- Optimisation des performances pour augmentant la vitesse de traitement des données.
- Utilisation de programmes d'analyse antivirus pour le trafic HTTP et FTP.

WEBsweeper HTTPS

- WEBsweeper peut désormais prendre en charge les applications de commerce électronique par le biais d'une nouvelle solution de serveur relais HTTPS.

SurfinGate 4.05

Les améliorations de SurfinGate comprennent :

Analyse du contenu des scripts JavaScript

SurfinGate 4.05 surveille les actions des scripts JavaScript potentiellement dangereux pour le réseau et bloque ces scripts s'ils enfreignent les règles de sécurité définies. SurfinGate 4.05 permet à l'administrateur de définir et de mettre en application des règles centralisées pour les objets JavaScript, Java et ActiveX, avec filtrage sélectif pour les objets Visual Basic et les cookies.

Contrôle des performances critiques

SurfinGate 4.05 contient un utilitaire capable de détecter automatiquement les événements anormaux (par exemple les erreurs d'exécution) et de relancer SurfinGate en cas d'échec. Cette fonction est essentielle pour la continuité des opérations critiques.

Optimisation de la gestion des règles

SurfinGate entre les profils des applets non convertis dans la base de données pour assurer leur blocage automatique. L'administrateur peut modifier la liste des applets et des contrôles.

Support des protocoles FTP et SSL

SurfinGate 4.05 contrôle les canaux FTP transportant les codes mobiles pour surveiller les codes susceptibles de pénétrer dans le réseau à partir de l'Internet. Outre les canaux FTP, SurfinGate surveille également les codes mobiles dans le trafic HTTP et oriente les transactions HTTPS vers des unités appropriées.

Intégration par plug-in avec le serveur relais HTTP

SurfinGate peut fonctionner comme un serveur relais, dans une chaîne de serveurs relais, ou avec un plug-in WTE couplé au pare-feu IBM Firewall pour Windows NT.

Chapitre 1. Présentation générale de SecureWay Boundary Server

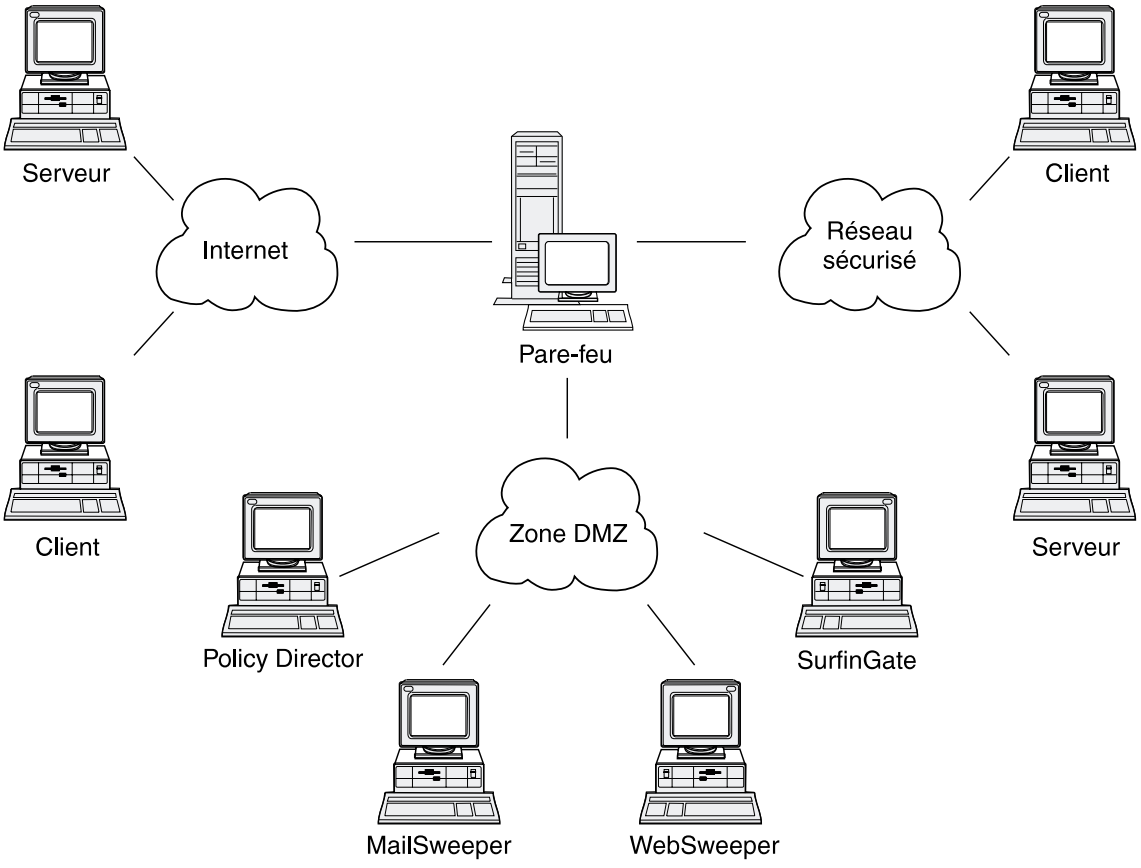

Figure 1. Exemple de configuration d'IBM SecureWay Boundary Server

Dans cet exemple, cinq stations de travail utilisent MAILsweeper, WEBsweeper, Policy Director et SurfinGate pour contrôler et router les transactions Web et les courriers échangés entre les clients et les serveurs via un pare-feu. Dans le cas présent, ces cinq stations de travail sont physiquement séparées.

Exemples de configuration standard de SecureWay Boundary Server

Il est recommandé d'utiliser les systèmes suivants pour créer une configuration de base :

Tableau 1. Configuration requise pour SecureWay Boundary Server

Produit	Machine
IBM Firewall	Windows NT ou AIX
MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

Pour bénéficier de toutes les fonctions de SecureWay Boundary Server, vous devez installer SecureWay Policy Director dans votre réseau. De cette manière, les utilisateurs relais du pare-feu IBM Firewall seront stockés dans le registre de SecureWay Directory (LDAP).

Exemple avec HTTP (IBM Firewall pour Windows NT) : Dans une situation standard, une requête HTTP de contenu Internet prend sa source sur la machine du client. La requête parvient d'abord au serveur WEBsweeper. En sortie, la requête est routée par WEBsweeper vers le serveur relais HTTP du pare-feu.

L'utilisateur est authentifié au niveau de ce serveur relais HTTP. Si cette requête est la première de la session de navigation du client, un message demande à l'utilisateur d'entrer son ID et son mot de passe. L'ID utilisateur permet de rechercher les règles de sécurité applicables dans la base de données LDAP administrée par Policy Director. Selon les règles d'authentification HTTP applicables au client, et selon le résultat du contrôle du mot de passe, la requête peut être rejetée ou acceptée. Le processus d'authentification peut nécessiter d'autres requêtes à la base de données LDAP ou au serveur ACE Security Dynamics. Pour les autres requêtes soumises au cours de la même session, le navigateur fournit automatiquement l'ID et le mot de passe de l'utilisateur. Par la suite, ces données d'identité ne sont plus demandées au client mais chaque nouvelle requête est authentifiée par le processus utilisé pour la première.

Si l'authentification réussit, la requête est transmise au serveur Internet demandé via le serveur relais HTTP du pare-feu.

Le contenu renvoyé par ce serveur Internet est réceptionné par le serveur relais HTTP d'IBM Firewall et analysé par le plug-in SurfinGate. Les données de groupe associées à l'utilisateur, extraites de la base de données LDAP, sont communiquées à SurfinGate pour la prise de décision. Si les données Internet ne contiennent rien de suspect pour SurfinGate, elles franchissent rapidement cette étape sans autre traitement. Les envois contenant des scripts JavaScript sont filtrés au niveau du plug-in SurfinGate. Ceux contenant des objets Java ou des contrôles ActiveX sont transmis au serveur SurfinGate, pour être filtrés, puis sont renvoyés au serveur relais HTTP du pare-feu. Le contenu issu du traitement par le plug-in SurfinGate est renvoyé au serveur WEBsweeper.

Parvenu au serveur WEBsweeper, le contenu est de nouveau filtré, sur la base des règles de sécurité de WEBsweeper, puis renvoyé au client.

Exemple avec HTTP (IBM Firewall pour AIX) : Dans le cas d'une configuration sur AIX, on retrouve un cheminement comparable, à ceci près qu'aucun plug-in SurfinGate n'est couplé au pare-feu. Le serveur SurfinGate doit donc être configuré comme un serveur relais membre d'une chaîne de serveurs relais reliant le client au pare-feu. WEBsweeper doit être configuré de manière à transmettre les requêtes au serveur SurfinGate au lieu de les adresser directement au serveur relais HTTP du pare-feu. Le serveur SurfinGate, pour sa part, doit être configuré pour transmettre les requêtes au serveur relais HTTP du pare-feu. Les données de groupe ne sont pas communiquées au serveur SurfinGate, aussi les décisions d'autorisation reposent-elles uniquement sur l'adresse IP.

Exemple de configuration pour le courrier électronique : MAILsweeper est configuré comme passerelle de service de messagerie. Le contenu des courriers parvenant au serveur MAILsweeper est filtré avant d'être transmis au serveur de messagerie suivant.

Chaque serveur de messagerie sécurisé doit être configuré de manière à transmettre au serveur MAILsweeper les requêtes de courrier des clients. Le programme d'échange de messages du pare-feu doit être configuré de manière à communiquer les courriers entrants au serveur MAILsweeper.

MAILsweeper doit être configuré pour transmettre au programme d'échange de messages du pare-feu les messages destinés aux domaines externes. MAILsweeper doit être configuré de manière à transmettre au serveur de messagerie sécurisé approprié les messages destinés aux domaines internes.

Chapitre 2. Présentation d'IBM SecureWay Boundary Server

Ce chapitre propose une présentation générale de SecureWay Boundary Server. Il comprend les sections suivantes :

Principes de SecureWay Boundary Server

IBM SecureWay Boundary Server est la première solution intégrée dédiée à la sécurisation des frontières des réseaux. Boundary Server offre des fonctions de pare-feu, de sécurité des contenus et de réseau privé virtuel (RPV). SecureWay Boundary Server réunit les meilleures technologies de sécurité sous la forme d'une solution intégrée bénéficiant du support et des services IBM. Cette solution comprend les produits suivants :

- IBM SecureWay Firewall 4.1 (avec Security Dynamics ACE/Server)
- MIMEsweeper (Content Technologies)
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - WEBsweeper HTTPS Proxy 1.0_2
- SurfinGate 4.05 (Finjan)
  - SurfinGate Server
  - SurfinConsole
  - Base de données SurfinGate
  - SurfinGate Plugin pour intégration de WTE pour Windows NT 1.0

Avantages de SecureWay Boundary Server

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. La sécurisation des frontières de votre réseau ne fait pas que protéger celui-ci en plus des applications et des informations qu'il héberge mais étend également l'accessibilité de vos ressources. Pour bien sécuriser ces frontières, vous devez contrôler à la fois qui et quelles informations pénètrent dans votre réseau et en sortent.

Intégration de SecureWay Boundary Server et FirstSecure

IBM SecureWay FirstSecure est un progiciel comprenant plusieurs produits intégrés. Cette solution complète permet de sécuriser tous les aspects des relations entre votre réseau et l'Internet ou d'autres réseaux. Composé de produits modulables, IBM SecureWay FirstSecure contribue à pérenniser vos équipements et à réduire le coût de détention des ressources nécessaires à la conduite d'un activité e-business sécurisée. La solution offre des fonctions de protection antivirus, de contrôle d'accès, de contrôle des échanges de données, de chiffrement, de gestion des certificats numériques, de pare-feu, ainsi que des services d'installation et des utilitaires.

Boundary Server est un progiciel qui comprend plusieurs modules et appartient à la famille des produits FirstSecure. Il établit une frontière entre votre réseau et l'Internet. Cette frontière vous permet de bloquer les virus potentiellement dangereux (à l'aide d'antivirus connexes), les scripts JavaScript et les applets Java, les contrôles ActiveX et les courriers électroniques indésirables. Boundary Server permet de contrôler précisément ce que vous voulez laisser entrer dans votre réseau en provenance de l'Internet. SecureWay Policy Director permet de gérer les utilisateurs relais utilisant le pare-feu IBM et leurs règles d'authentification.

Composants de SecureWay Boundary Server

Le progiciel SecureWay Boundary Server comprend trois produits distincts : IBM Firewall, MIMEsweeper et SurfinGate. SecureWay Boundary Server peut être utilisé conjointement avec IBM SecureWay Policy Director.

Présentation générale de SecureWay Boundary Server

IBM SecureWay Boundary Server est une solution destinée aux réseaux des grandes entreprises. Cette solution offre la protection, le contrôle d'accès et la sécurité des contenus nécessaires à la conduite d'une activité e-business ouverte sans risque aux clients, fournisseurs et autres partenaires. Ces fonctions sont notamment :

- Protection du réseau par pare-feu
- Fonction de réseau privé virtuel pour étendre l'accessibilité du réseau
- Analyse des contenus, pour le courrier électronique et les transactions Web, afin de protéger les données, l'image, la productivité et la responsabilité de l'entreprise

SecureWay Boundary Server réunit les meilleures technologies de sécurité sous la forme d'une solution intégrée bénéficiant du support et des services IBM. La solution est disponible pour les systèmes d'exploitation AIX et Windows NT.

Fonctionnement de SecureWay Boundary Server

Le serveur SecureWay Boundary Server utilise des technologies reposant sur le filtrage des paquets de données, les serveurs relais, les serveurs Socks et la sécurisation des contenus, pour masquer et protéger votre réseau et vos systèmes. Ces technologies permettent à l'administrateur de définir explicitement quelles données sont autorisées à entrer et à sortir du réseau. Ceci permet de prévenir les tentatives de contournement et de violation des interdictions d'accès visant à pénétrer le réseau, tout en protégeant votre responsabilité légale. SecureWay Boundary Server apporte une solution de

réseau privé virtuel qui permet de remplacer les serveurs distants et les banques de données accessibles par modem par une solution utilisant l'Internet.

Utilisé conjointement avec Policy Director, SecureWay Boundary Server permet d'authentifier les utilisateurs sur la base d'un système de règles d'autorisation centralisé. Un logiciel antivirus peut être couplé à SecureWay Boundary Server pour protéger votre site contre les virus informatiques.

Présentation générale d'IBM SecureWay Policy Director

Policy Director est une solution autonome de gestion des autorisations et de la sécurité des réseaux qui permet d'assurer une protection totale des ressources dans des réseaux internes et externes géographiquement distants. Un extranet est un réseau privé virtuel (RPV) qui utilise des fonctions de contrôle d'accès et de sécurité pour limiter à quelques personnes choisies l'usage d'un ou plusieurs intranets reliés à l'Internet. Policy Director propose des services d'authentification, d'autorisation, de sécurisation des données et de gestion des ressources. Ce produit s'utilise en association avec les applications Internet standard pour mettre en oeuvre des intranets et des extranets fonctionnels et sécurisés.

Fonctionnement d'IBM SecureWay Policy Director

Utilisé avec SecureWay Boundary Server, IBM SecureWay Policy Director peut stocker les règles applicables aux utilisateurs relais et leurs données d'authentification.

Présentation générale d'IBM SecureWay Firewall

IBM Firewall est un programme de sécurité de réseau. Un pare-feu (firewall) établit un écran de protection entre un ou plusieurs réseaux internes privés sécurisés et d'autres réseaux ou l'Internet. L'objectif d'un pare-feu est d'empêcher les communications non désirées ou non autorisées de pénétrer dans le réseau sécurisé ou d'en sortir.

Fonctionnement d'IBM SecureWay Firewall

Le pare-feu IBM SecureWay Firewall limite les transactions entre un réseau protégé et l'Internet ou d'autres réseaux. Outre ces fonctions, un pare-feu permet également de :

- obliger les utilisateurs à entrer dans le réseau par un unique point de contrôle ;
- empêcher les intrus d'accéder aux dispositifs de protection ;
- obliger les utilisateurs à sortir du réseau par un unique point de contrôle ;
- séparer les informations sensibles pour les rendre inaccessibles aux utilisateurs non autorisés ;
- contrôler les transactions entrant ou quittant le réseau.

Présentation générale de MIMEsweeper

MIMEsweeper permet de sécuriser les contenus en analysant les données de la messagerie électronique ou du Web traversant le pare-feu. La sécurisation des contenus permet de traiter efficacement les aspects de la gestion de réseau relatifs à l'utilisation de la messagerie électronique et du Web. Ces aspects concernent l'intégrité du réseau d'une part, et celle de l'entreprise d'autre part.

La protection de l'intégrité du réseau implique les mesures suivantes :

- Identifier et supprimer les virus contenus dans les courriers entrants et sortants
- Filtrer les types de fichier indésirables
- Gérer les fichiers trop volumineux
- Protéger les réseaux contre les effets de l'encombrement ou de la perte d'un service suite à un envoi de courrier piégé

La protection de l'intégrité de l'entreprise implique les mesures suivantes :

- Empêcher la divulgation d'informations confidentielles ou la perte de secrets commerciaux
- Limiter le risque d'implication de la responsabilité légale
- Réduire les charges résultant de l'utilisation de la messagerie électronique et des services Web
- Protéger des effets de la perte d'un service de réseau suite à une mauvaise utilisation ou à un acte malveillant

Les atteintes à l'intégrité du réseau peuvent altérer ou effacer des données, interrompre le trafic du courrier électronique et endommager les équipements. Tout ceci peut induire des arrêts du réseau, des pertes de productivité et des coûts importants en maintenance et en restauration.

Les atteintes à l'intégrité de l'entreprise peuvent être plus dommageables encore ; coûts des procédures juridiques, pertes de propriétés intellectuelles et atteinte à la réputation et à la crédibilité de l'entreprise. Ces atteintes peuvent provoquer l'arrêt pur et simple des activités commerciales de l'entreprise.

MIMEsweeper est le meilleur produit actuellement disponible pour protéger l'intégrité d'un réseau et d'une entreprise contre les effets nuisibles de l'utilisation de la messagerie électronique et de l'Internet.

Fonctionnement de MIMEsweeper

MIMEsweeper permet les opérations suivantes :

- Attacher des avis déclinant toute responsabilité légale aux courriers sortants
- Protéger les données et les documents confidentiels
- Autoriser et contrôler les utilisateurs de la messagerie électronique et du Web
- Ecarter ou bloquer des matériels dangereux
- Bloquer les courriers indésirables
- Analyser le contenu des fichiers joints et des téléchargements
- Arrêter les virus et les programmes hostiles
- Interdire l'accès à certains sites et pages Web
- Signaler, journaliser et archiver les événements

Présentation générale de SurfinGate

SurfinGate 4.05 est un utilitaire de sécurisation des codes mobiles conçu pour les entreprises utilisant l'Internet, un extranet ou un intranet pour réaliser des transactions commerciales. Par l'analyse des contenus des codes mobiles, notamment des scripts JavaScript, SurfinGate permet de protéger les réseaux informatiques contre les dommages fortuits ou intentionnels résultant d'actes d'espionnage industriel, de la modification des données ou de leur suppression. Le processus d'analyse des contenus de SurfinGate analyse le code mobile des objets Java, JavaScript et ActiveX au niveau de la passerelle, loin des ressources protégées, et lui affecte un ID unique et un profil ASP (applet security profile) contenant tous les risques d'atteinte à la sécurité envisageables. SurfinGate identifie un code potentiellement dangereux avant qu'il ne pénètre dans le réseau.

SurfinGate 4.05 comprend quatre composants :

- SurfinGate Server
- SurfinConsole
- Base de données SurfinGate
- SurfinGate Plugin pour intégration de WTE pour Windows NT

SurfinGate Server est utilisé en tant que serveur relais HTTP. Il peut s'intégrer dans une chaîne de serveurs relais à côté du serveur relais HTTP du pare-feu IBM Firewall et du serveur relais de WEBsweeper. Pour Windows NT, il peut aussi s'utiliser comme un plug-in couplé au serveur relais HTTP du pare-feu. Dans cette situation, SurfinGate aura pour tâche de réunir des informations sur le groupe de l'utilisateur relais soumettant une requête. Les règles de filtrage appliquées par SurfinGate peuvent reposer sur ces données de groupe. Cette architecture permet d'arrêter la transmission du code mobile et d'effectuer un contrôle afin d'éviter tout risque. Ce composant fournit une protection conforme aux règles de sécurité établie par l'entreprise.

SurfinConsole est une interface conviviale qui permet de définir et de gérer les règles de sécurité applicables aux codes mobiles. SurfinConsole peut contrôler plusieurs serveurs SurfinGate sur le réseau et faire appliquer les règles définies dans l'entreprise auprès de chaque utilisateur ou groupe ou à l'aide de listes personnalisées de codes acceptables et non acceptables.

La base de données de SurfinGate stocke les données des profils ASP, notamment des informations concernant les utilisateurs, les groupes et les règles de sécurité associées. Cette base de données peut utiliser un moteur de base de données intégré ou une base de données Oracle existante. 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.

Fonctionnement de SurfinGate

SurfinGate offre les fonctions suivantes :

- Analyse des contenus au niveau de la passerelle pour les applets Java, les contrôles Active X et les scripts JavaScript
- Contrôle en temps réel et dynamique
- Application des règles de sécurité aux codes mobiles en provenance du Web
- Analyse des codes mobiles (par exemple, applets Java, contrôles ActiveX, scripts JavaScript, scripts Visual Basic, plugins, cookies)

SurfinGate peut fonctionner avec un serveur relais, dans une chaîne de serveurs relais, ou avec un plug-in WTE couplé au pare-feu IBM Firewall pour Windows NT.

Chapitre 3. Préparation de l'installation de SecureWay Boundary Server

Ce chapitre décrit comment préparer l'installation de SecureWay Boundary Server avec l'assistant. Il comprend les sections suivantes :

- «Procédure de préparation»
- «SecureWay Boundary Server» à la page 13

Procédure de préparation

Cette section explique comment préparer l'installation des différents composants de SecureWay Boundary Server.

Intégration avec SecureWay Policy Director

Pour mettre en oeuvre une configuration standard d'IBM SecureWay Policy Director sur Windows NT ou AIX, procédez de la manière suivante :

1. Vérifiez que la configuration du système d'exploitation permet la prise en charge de Policy Director.
2. Déterminez les serveurs les mieux adaptés à vos besoins et les machines sur lesquelles vous désirez les installer.
3. Installez et configurez un DCE (environnement informatique partagé) si ce n'est déjà fait.
4. Installez et configurez SecureWay Directory (LDAP).
5. Configurez le service d'acquisition de droits d'accès (SAD) si vous envisagez de proposer ce service.
6. Installez le client NetSEAT.
7. Installez les composants du serveur Policy Director.
8. Installez la console de gestion.

Pour plus d'informations sur Policy Director, reportez-vous au manuel Policy Director 3.0 - Guide de configuration et d'utilisation.

SecureWay Firewall

Pour mettre en oeuvre une configuration standard d'IBM Firewall sur Windows NT ou AIX, procédez de la manière suivante :

1. Vérifiez que les conditions détaillées dans la section «Configuration matérielle» à la page 17 sont satisfaites.
2. Planifiez la configuration d'IBM Firewall. Choisissez les fonctions du pare-feu que vous voulez utiliser et la manière dont vous voulez le faire.
3. Définissez dans la configuration du pare-feu les interfaces connectées aux réseaux sécurisés. Pour fonctionner convenablement, le pare-feu doit disposer d'une interface sécurisée et d'une autre non sécurisée. A partir de l'arborescence de navigation du client de configuration, ouvrez le dossier d'administration du système,

puis cliquez sur **Interfaces** pour afficher la liste des interfaces de réseau du pare-feu. Pour modifier l'état de sécurité d'une interface, sélectionnez-la, puis cliquez sur **Modification**.

Remarque : Si vous prévoyez une liaison avec l'Internet, contactez votre fournisseur de service Internet pour obtenir une adresse IP enregistrée pour l'interface non sécurisée du pare-feu.

4. Configurez les règles de sécurité générales par le biais de la boîte de dialogue **Règles de sécurité** du dossier d'administration du système. Pour les configurations de pare-feu standard :
   - autorisez les requêtes de DNS ;
   - interdisez la diffusion de messages vers l'interface non sécurisée ;
   - interdisez les connexions Socks sur les cartes non sécurisées.
5. Configurez votre service de nom de domaine et votre service de messagerie. Les communications ne seront pas optimisées si vous ne prévoyez pas un service de conversion des DNS. Vous pouvez accéder à ces fonctions à partir du dossier d'administration du système dans l'arborescence de navigation du client de configuration.
6. Définissez les composants clés du ou des réseaux dans la configuration du pare-feu, à l'aide de la fonction **Objets réseau**, dans l'arborescence de navigation du client de configuration. Cette fonction contrôle le trafic transitant par le pare-feu. Définissez les composants suivants comme objets de réseau :
   - Interface sécurisée du pare-feu
   - Interface non sécurisée du pare-feu
   - Réseau sécurisé
   - Chaque sous-réseau du réseau sécurisé
   - Un objet de réseau hôte pour les serveurs Security Dynamics et les serveurs du domaine Windows NT, le cas échéant
7. Activez les services du pare-feu. Il s'agit des méthodes (serveurs de sockets ou serveur relais) permettant aux utilisateurs d'accéder au réseau non sécurisé à partir du réseau sécurisé. Les services effectivement mis en oeuvre dépendent des décisions prises lors de la planification. L'établissement d'un service nécessite souvent de configurer des connexions adaptées pour permettre certains types de transaction. Par exemple, pour permettre aux utilisateurs sécurisés de surfer sur le Web par le biais du serveur relais HTTP, il vous faut configurer le démon de ce serveur mais également les connexions permettant les transactions HTTP. Pour configurer Policy Director, reportez-vous à la section «Intégration avec SecureWay Policy Director» à la page 11.
8. **Windows NT uniquement :** Dans la mesure où le processus de durcissement désactive NETBIOS, pour utiliser les mots de passe du domaine Windows NT pour l'authentification, vous devez configurer le code du client Windows chargé d'installer la fonction d'analyse des domaines Windows NT sécurisés. Les serveurs Windows NT sécurisés doivent avoir des noms et des adresses d'hôte TCP/IP et doivent être reliés entre eux et avec le pare-feu par des connexions TCP/IP. L'administrateur du pare-feu doit monter des connexions entre le pare-feu et les serveurs Windows NT sécurisés pour permettre le trafic entre ces composants.
9. Si vous prévoyez d'utiliser la conversion d'adresse réseau, contactez votre fournisseur de service Internet afin d'obtenir une adresse Internet enregistrée

permettant la conversion d'adresse de type plusieurs à un. Cette adresse s'ajoutera à celle demandée à l'étape de la section 3 à la page 11. Ouvrez ensuite le panneau Ajout de configuration NAT, puis ajoutez l'adresse Internet enregistrée dans le champ Adresse IP plusieurs à un.

Cette procédure permet d'installer et d'activer une configuration de pare-feu standard. IBM Firewall offre d'autres fonctions permettant de renforcer la sécurité du réseau, notamment des fonctions de journalisation des événements du système.

Si le pare-feu s'arrête, d'une façon normale ou non, les données de configuration ne sont pas menacées dans la mesure où elles sont stockées sur le disque dur et automatiquement réactivées au redémarrage du système. En revanche, les fichiers journaux consigneront des messages signalant l'interruption des connexions actives, par exemple pour les sessions FTP en cours.

SecureWay Boundary Server

L'assistant d'installation de SecureWay Boundary Server permet de configurer IBM Firewall de manière à pouvoir utiliser Policy Director pour l'administration des utilisateurs. Le cas échéant, l'assistant peut aussi configurer le serveur relais HTTP du pare-feu pour transmettre les données d'authentification au programme optionnel (plug-in) SurfinGate (Windows NT uniquement).

Les informations permettant l'intégration d'IBM Firewall à IBM SecureWay Boundary sont les suivantes :

- Le nom d'hôte et le nom du domaine du serveur IBM SecureWay Directory qu'utilisera le pare-feu
- Le numéro du port d'écoute du serveur IBM SecureWay Directory (le numéro de port par défaut est le 389)
- Le mot de passe SecurityMaster défini pour le serveur IBM SecureWay Directory
- Le nom de domaine à utiliser pour distinguer les utilisateurs relais utilisant ce pare-feu. Tout pare-feu utilisant ce nom aura la charge des mêmes utilisateurs. Il s'agit, en principe, du nom d'hôte qualifié complet de la machine du pare-feu.
- Le nom d'administrateur de pare-feu utilisé pour accéder aux utilisateurs relais définis dans l'annuaire SecureWay Directory. A ce nom seront associés des droits permettant de modifier tous les utilisateurs relais créés dans Policy Director. Entrez le nom d'hôte qualifié complet de la machine du pare-feu.
- Le DN qu'utilise IBM SecureWay Directory comme racine de départ des recherches d'utilisateurs du pare-feu dans la base de données. Il s'agit normalement du suffixe défini dans SecureWay Directory pour enregistrer les utilisateurs de Policy Director.
- Un mot de passe associé à l'ID de l'administrateur du pare-feu, pour les connexions au serveur d'IBM SecureWay Directory.

Vous devrez établir une connexion adaptée pour permettre les transactions entre le pare-feu et le serveur de SecureWay Directory.

Vérifiez que les conditions détaillées dans la section «Configuration matérielle» à la page 17 sont satisfaites.

SurfinGate

L'utilisation de SurfinGate nécessite d'installer le module Windows NT Service Pack 5. Vérifiez que les conditions détaillées dans la section «Configuration matérielle» à la page 17 sont satisfaites.

Pour préparer l'utilisation de SurfinGate :

- Configurez la base de données Oracle si vous prévoyez de l'utiliser.
- Si vous utilisez IBM Firewall pour Windows NT, vous devez choisir le mode plug-in ou relais.
- Pour activer le plug-in SurfinGate sur WTE, installez-le sur la machine du pare-feu, puis démarrez l'assistant d'installation de SecureWay Boundary Server.
- Vous devrez établir une connexion adaptée pour permettre les transactions entre le plug-in et le serveur SurfinGate.

MIMEsweeper

Avant d'utiliser MIMEsweeper, vous devez savoir comment votre réseau va fonctionner. Vérifiez que les conditions détaillées dans la section «Configuration matérielle» à la page 17 sont satisfaites.

MAILsweeper

Si vous configurez MIMEsweeper, les programmes MAILsweeper et WEBsweeper doivent être installés sur des machines séparées.

Effectuez les tâches suivantes avant de configurer MAILsweeper :

- Déterminez les domaines de messagerie utilisés en interne. MAILsweeper et le programme d'échange de messages du pare-feu doivent être configurés pour accepter les messages de chacun de ces domaines de messagerie.
- Déterminez les serveurs de messagerie sécurisée attachés aux différents domaines. MAILsweeper doit être configuré de manière à transmettre aux serveurs de messagerie sécurisée appropriés les messages destinés aux différents domaines.
- Déterminez l'adresse du serveur de MAILsweeper. Chaque serveur de messagerie sécurisée doit être configuré pour transmettre au serveur MAILsweeper les courriers émanant des clients internes.
- Déterminez l'adresse du pare-feu. MAILsweeper doit être configuré de manière à transmettre au programme d'échange de messages du pare-feu les messages destinés aux domaines externes.

WEBsweeper

Effectuez les tâches suivantes avant de configurer WEBsweeper :

- Déterminez l'adresse du serveur de WEBsweeper. Cette adresse sera nécessaire aux différents navigateurs Web installés dans votre réseau. Ces derniers doivent être configurés de manière à utiliser le serveur WEBsweeper comme serveur relais pour les requêtes HTTP, FTP et HTTPS.
- Déterminez l'adresse de l'interface sécurisée du pare-feu. WEBsweeper doit être configuré de manière à renvoyer les requêtes de relais au serveur relais HTTP installé sur le pare-feu.

- Pour que les clients ne puissent pas éviter le filtrage des contenus Web, vous devrez monter une connexion sur le pare-feu pour limiter l'accès par relais aux serveurs WEBsweeper et/ou SurfinGate.

Chapitre 4. Configuration requise pour l'installation de SecureWay Boundary Server

Ce chapitre décrit la configuration requise pour l'installation du produit SecureWay Boundary Server.

Configuration matérielle

Les conditions matérielles requises pour installer le produit SecureWay Boundary Server sont présentées dans le tableau ci-après.

Tableau 2. Configuration matérielle requise pour SecureWay Boundary Server

Composant	Type de machine	Espace disque	Mémoire	Autre
Policy Director	sans objet	64 Mo	16 Mo	sans objet
IBM Firewall	• Windows NT : 266 MHz ou supérieur • AIX : Système RS/6000 avec AIX 4.3.2	Windows NT : 200 Mo AIX : 200 Mo	Windows NT : 64 Mo AIX : 128 Mo	2 cartes d'interface réseau (NIC)
ACE/Server	• Windows NT : 166 MHz ou supérieur (mono-processeurs uniquement) • AIX : Machine supportant AIX 4.2	• Logiciel du serveur principal : 50 Mo • Serveur de sauvegarde : 22 Mo • Base de données utilisateur initiale : 4 Mo • Installation : 240 Mo	Minimum : 32 Mo	Les besoins réels dépendent du nombre d'utilisateurs
MAILsweeper	Windows NT : Processeur 400 MHz ou supérieur	1 Go	128 Mo	sans objet
WEBsweeper	Windows NT : Processeur 450 MHz ou supérieur	1 Go	128 Mo	sans objet
WEBsweeper (environnement avec volume de transactions important)	Windows NT : Processeur 450 MHz ou supérieur	3 Go	512 Mo	sans objet
SurfinGate 4.05 Server	Windows NT : Processeur 233 MHz ou supérieur	20 Mo	256 Mo	sans objet

Tableau 2. Configuration matérielle requise pour SecureWay Boundary Server (suite)

SurfinGate 4.05 Console	Windows NT : Processeur 233 MHz ou supérieur	15 Mo	64 Mo	sans objet

Remarque : Pour plus d'informations, reportez-vous au manuel IBM SecureWay Firewall pour AIX ou Windows NT - Guide de d'installation et de configuration multilingue. 138 Mo d'espace disque sont également nécessaires pour le navigateur Netscape.

Configuration logicielle

Les conditions logicielles requises pour installer le produit SecureWay Boundary Server sont présentées dans le tableau ci-après.

Tableau 3. Configuration logicielle requise pour SecureWay Boundary Server

Produit	Windows	AIX	Autre
Serveurs Policy Director	Windows NT version 4.0 avec Service Pack 5	4.3.1	sans objet
IBM Firewall	Windows NT version 4.0 avec Service Pack 5	4.3.2	sans objet
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	sans objet
MAILsweeper	Windows NT version 4.0 avec Service Pack 5, Internet Explorer 4.01 ou version ultérieure, Microsoft Management Console 1.1, unité NTFS, Windows Messaging	sans objet	Antivirus de votre choix
WEBsweeper	Windows NT version 4.0 avec Service Pack 5	sans objet	Antivirus de votre choix
SurfinGate Server	Windows NT version 4.0 avec Service Pack 5	sans objet	sans objet
SurfinGate 4.05 Console	Windows NT version 4.0 avec Service Pack 5 ou Windows 95	sans objet	sans objet

Chapitre 5. Installation et configuration de SecureWay Boundary Server

Ce chapitre explique comment installer et configurer SecureWay Boundary Server sur Windows NT et AIX.

Installation des composants de SecureWay Boundary Server

Cette section décrit comment installer IBM SecureWay Firewall, SurfinGate, et MIMEsweeper pour Windows NT et AIX.

Installation d'IBM SecureWay Firewall

Pour plus d'informations sur la mise en oeuvre d'une configuration de base de SecureWay Firewall pour Windows NT et AIX, reportez-vous à la section «Procédure de préparation» à la page 11. Cette section détaille comment définir une interface sécurisée, déterminer les règles de sécurité et créer les objets d'un réseau. Pour plus d'informations sur l'installation de SecureWay Firewall, reportez-vous au manuel IBM SecureWay Firewall - Guide d'installation pour AIX ou IBM SecureWay Firewall - Guide d'installation pour Windows NT.

Installation de SecureWay Directory

Si vous utilisez la fonction LDAP de SecureWay Boundary Server, vous devez installer également SecureWay Directory. Reportez-vous au manuel IBM SecureWay Policy Director 3.0 - Guide de configuration et d'utilisation.

Le serveur SecureWay Directory doit être installé du côté sécurisé du pare-feu ou à l'intérieur de la zone DMZ sécurisée du pare-feu.

Installation de SecureWay Policy Director

Si vous utilisez la fonction LDAP de SecureWay Boundary Server, vous devez installer également SecureWay Policy Director. Reportez-vous au manuel IBM SecureWay Policy Director 3.0 - Guide de configuration et d'utilisation)

Installation de SecureWay Boundary Server

Pour installer SecureWay Boundary Server sur Windows NT :

- Installez SecureWay Firewall pour Windows NT.
- A partir du CD-ROM de SecureWay Boundary Server, exécutez le fichier setup.exe.
- Choisissez la langue désirée, puis cliquez sur **OK**
- L'assistant InstallShield vous demande si vous voulez installer SecureWay Boundary Server. Pour Windows NT, le répertoire d'installation par défaut est C:\Program Files\IBM\SBS
- Redémarrez le système.

Pour installer SecureWay Boundary Server sur AIX :

- Installez SecureWay Firewall pour AIX.
- Insérez le CD-ROM dans le lecteur approprié, puis procédez à l'installation avec SMITTY.
- Sélectionnez Installation et maintenance de logiciels.
- Sélectionnez Installation et mise à jour de logiciels.
- Sélectionnez Installation et mise à jour de tous les logiciels disponibles.
- Affichez la liste des unités d'entrée proposées et sélectionnez le lecteur de CD-ROM.
- Affichez la liste des logiciels à installer et sélectionnez SecureWay Boundary Server.
- Appuyez sur **Entrée** pour installer le logiciel.
- Redémarrez le système.

Installation de SurfinGate

SurfinGate comprend deux composants : SurfinGate Server et SurfinGate Console. Pour installer l'un ou l'autre de ces composants, reportez-vous au guide d'installation disponible dans le répertoire `\docs\install.pdf` du CD-ROM de SurfinGate.

Plug-in SurfinGate

Pour installer le plug-in SurfinGate avec IBM SecureWay Firewall pour Windows NT, reportez-vous au guide d'installation disponible dans le répertoire `\docs` du CD-ROM de SurfinGate.

Installation de MIMEsweeper

MIMEsweeper comprend trois composants : MAILsweeper, WEBsweeper et WEBsweeper HTTPS.

MAILsweeper 4.1 doit être installé dans une partition NTFS.

Installation de MAILsweeper

Pour installer MAILsweeper, reportez-vous au Guide de démarrage disponible dans le répertoire `\install\MSW4_0_2\docs\qsg.pdf` du CD-ROM de MIMEsweeper.

N'installez **PAS** MAILsweeper sur la même machine que le serveur relais WEBsweeper HTTP.

N'installez **PAS** MAILsweeper sur la même machine que le serveur relais WEBsweeper HTTPS.

Si vous installez la bibliothèque `MAPI32.dll` à partir du CD-ROM de Windows NT, puis que vous installez Microsoft Management Console 1.1 à partir du CD-ROM de MIMEsweeper, le fichier `MAPI32.dll` est remplacé par une version plus ancienne. Une fois Microsoft Management Console installé, prenez soin de réinstaller la bibliothèque `MAPI32.dll` version 4.0 ou ultérieure. La bibliothèque `dll` réside normalement dans le composant Windows Messaging.

Installation de WEBsweeper

Pour installer WEBsweeper, reportez-vous au Guide de l'administrateur disponible dans le répertoire `\install\WSW3_2_5\docs\manual.pdf` du CD-ROM de MIMEsweeper.

N'installez **PAS** WEBsweeper sur la même machine que MAILsweeper.

Installation de WEBsweeper HTTPS

Pour installer WEBsweeper HTTPS, reportez-vous au fichier readme.txt disponible dans le répertoire `\install\WSWHTTPS1_0_2\` du CD-ROM de MIMEsweeper.

N'installez **PAS** le serveur relais HTTPS WEBsweeper sur la même machine que MAILsweeper.

Configuration des composants de SecureWay Boundary Server

Configuration de SecureWay Firewall

Pour mettre en oeuvre une configuration de base d'IBM Firewall :

1. Planifiez la configuration d'IBM Firewall. Choisissez les fonctions du pare-feu que vous voulez utiliser et la manière dont vous le faire.
2. Définissez dans la configuration du pare-feu les interfaces connectées aux réseaux sécurisés. Pour fonctionner convenablement, le pare-feu doit disposer d'une interface sécurisée et d'une autre non sécurisée. A partir de l'arborescence de navigation du client de configuration, ouvrez le dossier d'administration du système, puis cliquez sur **Interfaces** pour afficher la liste des interfaces de réseau du pare-feu. Pour modifier l'état de sécurité d'une interface, sélectionnez-la, puis cliquez sur **Modification**.
3. Configurez les règles de sécurité générales par le biais de la boîte de dialogue **Règles de sécurité** du dossier d'administration du système. Pour les configurations de pare-feu standard :
   - autorisez les requêtes de DNS ;
   - interdisez la diffusion de messages vers l'interface non sécurisée ;
   - interdisez les connexions Socks sur les cartes non sécurisées.
4. Configurez votre service de nom de domaine et votre service de messagerie. Les communications ne seront pas optimisées si vous ne prévoyez pas un service de conversion des DNS. Vous pouvez accéder à ces fonctions à partir du dossier d'administration du système dans l'arborescence de navigation du client de configuration.
5. Définissez les composants clés de votre réseau dans la configuration du pare-feu, à l'aide de la fonction **Objets réseau**, dans l'arborescence de navigation du client de configuration. Cette fonction contrôle le trafic transitant par le pare-feu. Définissez les composants suivants comme objets de réseau :
   - Interface sécurisée du pare-feu
   - Interface non sécurisée du pare-feu
   - Réseau sécurisé
   - Chaque sous-réseau du réseau sécurisé

- Un objet de réseau hôte pour les serveurs Security Dynamics et les serveurs du domaine Windows NT, le cas échéant

6. Activez les services du pare-feu. Il s'agit des méthodes (serveurs de sockets ou serveur relais) permettant aux utilisateurs d'accéder au réseau non sécurisé à partir du réseau sécurisé. Les services effectivement mis en oeuvre dépendent des décisions prises lors de la planification. L'établissement d'un service nécessite souvent de configurer des connexions adaptées pour permettre certains types de transaction. Par exemple, pour permettre aux utilisateurs de naviguer sur le Web à l'aide d'un serveur relais HTTP, vous devez configurer le démon HTTP Proxy, sur le pare-feu mais également les connexions requises pour les transactions HTTP.
7. Définissez les utilisateurs du pare-feu. Si vous pensez avoir besoin d'une procédure d'authentification, par exemple pour les administrateurs du pare-feu ou pour les connexions Web sortantes, déclarez les utilisateurs concernés sur le pare-feu. Si vous prévoyez d'utiliser Policy Director pour enregistrer les utilisateurs relais dans le registre LDAP, ne créez pas ces utilisateurs relais à ce stade. Utilisez la console de gestion de Policy Director pour créer les utilisateurs relais d'IBM Firewall au cours de la configuration de Policy Director.

Cette procédure permet d'installer et d'activer une configuration de pare-feu standard. IBM Firewall offre d'autres fonctions permettant de renforcer la sécurité du réseau, notamment des fonctions de journalisation des événements du système.

Si le pare-feu s'arrête, d'une façon normale ou non, les données de configuration ne sont pas menacées dans la mesure où elles sont stockées sur le disque dur et automatiquement réactivées au redémarrage du système. En revanche, les fichiers journaux consigneront des messages signalant l'interruption des connexions actives, par exemple pour les sessions FTP en cours.

Configuration de SecureWay Firewall pour l'intégration de Policy Director

Le pare-feu doit être configuré de manière à utiliser IBM SecureWay Policy Director avec l'assistant de SecureWay Boundary Server pour bénéficier de l'intégration de Policy Director. Si vous n'utilisez pas Policy Director, les utilisateurs relais ne peuvent être définis qu'au moyen de l'interface utilisateur graphique d'IBM Firewall. Ces utilisateurs ne pourront pas être gérés par Policy Director dans ce cas.

Une connexion devra être établie pour permettre les communications entre SecureWay Firewall et SecureWay Directory. SecureWay Directory doit être installé du côté sécurisé du pare-feu (dans une zone DMZ sécurisée ou un réseau sécurisé).

Pour plus d'informations sur la mise en place des connexions, reportez-vous au manuel IBM SecureWay Firewall pour Windows NT - Guide de l'utilisateur ou IBM SecureWay Firewall pour AIX - Guide de l'utilisateur. Des informations sur ce sujet sont fournies dans la suite de ce chapitre.

Les règles applicables aux connexions sortantes (les requêtes) sont déterminées par les facteurs suivants :

- La source correspond à l'adresse de l'interface sécurisée du pare-feu.
- La destination correspond à l'adresse de SecureWay Directory.

- Le numéro de port de la source doit être supérieur à 1023.
- Le numéro de port de la destination est 389.
- L'interface doit être sécurisée.
- Le routage est de type local.
- La direction est en sortie (outbound).

Les règles applicables aux connexions entrantes (les réponses) sont déterminées par les facteurs suivants :

- La source correspond à l'adresse de SecureWay Directory.
- La destination correspond à l'adresse de l'interface sécurisée du pare-feu.
- Le numéro de port de la source est 389.
- Le numéro de port de la destination est supérieur à 1023.
- L'interface doit être sécurisée.
- Le routage est de type local.
- La direction est en entrée (inbound).

Voici un exemple de définition d'une connexion :

```
# Service : ldap
# Description :

permit 9.67.130.153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1023 eq 389 secure both
outbound l=y f=y t=0 e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.130.153
255.255.255.255 tcp/ack eq 389 gt 1023 secure local
inbound l=y f=y t=0 e=none a=none
```

Démarrez l'assistant de configuration de SecureWay Boundary Server. Sélectionnez l'option appropriée pour permettre au pare-feu de fonctionner avec Policy Director. Pour plus d'informations, reportez-vous à la section «Configuration de SecureWay Boundary Server pour l'intégration de Policy Director» à la page 25.

Configuration de SecureWay Firewall pour l'utilisation du plug-in SurfinGate (Windows NT uniquement

Une connexion devra être établie pour permettre les communications entre SecureWay Firewall et le serveur SurfinGate. Le serveur SurfinGate doit être installé du côté sécurisé du pare-feu.

Pour plus d'informations sur la mise en place des connexions, reportez-vous au manuel IBM SecureWay Firewall pour Windows NT - Guide de l'utilisateur. Des informations sur ce sujet sont fournies dans la suite de ce chapitre.

Les règles applicables aux connexions sortantes (les requêtes) sont déterminées par les facteurs suivants :

- La source correspond à l'adresse de l'interface sécurisée du pare-feu.

- La destination correspond à l'adresse du serveur SurfinGate.
- Le numéro de port de la source doit être supérieur à 1023.
- Le numéro de port de la destination est 3141.
- L'interface doit être sécurisée.
- Le routage est de type local.
- La direction est en sortie (outbound).

Les règles applicables aux connexions entrantes (les réponses) sont déterminées par les facteurs suivants :

- La source correspond à l'adresse du serveur SurfinGate.
- La destination correspond à l'adresse de l'interface sécurisée du pare-feu.
- Le numéro de port de la source est 3141.
- Le numéro de port de la destination est supérieur à 1023.
- L'interface doit être sécurisée.
- Le routage est de type local.
- La direction est en entrée (inbound).

Voici un exemple de définition d'une connexion :

```
# Service : SurfinGate Plugin Communication
# Description :

permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1023 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1023
secure local inbound  l=y f=y

Remarque : Les connexions doivent être définies sur une seule ligne.
```

Vous devez également configurer le serveur SurfinGate pour permettre l'analyse des données. Dans SurfinConsole (l'interface d'administration de SurfinGate), cochez l'option **Plugin Mode** dans l'onglet General. Entrez aussi l'adresse et le numéro de port du serveur relais HTTP du pare-feu dans le champ Next Proxy de l'onglet Proxy.

Configuration de SecureWay Firewall pour l'utilisation de MAILsweeper

Le programme d'échange de messages (Mail Exchanger) défini au niveau de SecureWay Firewall doit désigner la machine de MAILsweeper au lieu du serveur de messagerie sécurisé. MAILsweeper assurera lui-même la délivrance des messages aux différents serveurs de messagerie sécurisés.

Configuration de Policy Director

Vérifiez que SecureWay Directory a été installé. Vous devez connaître l'adresse de la machine sur laquelle SecureWay Directory est installé, son port d'écoute, l'ID de l'administrateur du serveur de SecureWay Directory et son mot de passe.

Installez le client LDAP de SecureWay Directory sur la même machine que Policy Director (ce client peut être déjà installé si vous utilisez la même machine pour SecureWay Directory et SecureWay Policy Director).

Vous devez modifier la structure du registre LDAP de SecureWay Directory pour prendre en charge les utilisateurs relais de Policy Director. Les données de ces modifications sont contenues dans deux fichiers fournis par Policy Director. Il s'agit des fichiers `secschema.def` et `puschema.def`, disponibles dans le répertoire `/schema` du CD-ROM de Policy Director.

Pour modifier la structure du registre LDAP présent sur le serveur de SecureWay Directory, exécutez les commandes suivantes sur la machine de Policy Director :

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT>  -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f secsche

ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f puschema
```

Où :

- `<LDAPHOST>` désigne le serveur SecureWay Directory.
- `<LDAPPORT>` désigne le port d'écoute du serveur.
- `<LDAPADMINUSER>` spécifie l'ID de l'administrateur.
- `<LDAPADMINPWD>` spécifie le mot de passe de l'administrateur.

Une fois la structure du registre LDAP modifiée pour prendre en charge les utilisateurs relais, vous devez activer la gestion des utilisateurs relais au niveau de la console de gestion de Policy Director. Pour cela, vous devez supprimer les commentaires de la ligne Proxyusers TaskView dans le fichier `console.properties`, dans le répertoire `\Program Files\IBM\IVConsole`.

Configuration de SecureWay Directory

Vous devez associer un suffixe à l'annuaire SecureWay Directory dans lequel les utilisateurs de Policy Director seront enregistrés. Pour ajouter un suffixe dans le registre LDAP, reportez-vous au manuel IBM SecureWay Directory - Guide de l'administrateur. Voici un exemple de suffixe conventionnel :

```
o=organisation,c=pays
```

Une fois défini le suffixe utilisé pour l'enregistrement des utilisateurs de Policy Director, vous devez lui associer une liste de contrôle d'accès (LCA). Vous devez associer tous les droits d'accès au nouveau suffixe pour le groupe d'utilisateurs Policy Director en charge de la sécurité. Le DN (nom distinctif) de ce groupe est :

```
cn=securitygroup,secauthority=default
```

Configuration de SecureWay Boundary Server pour l'intégration de Policy Director

Vous pouvez configurer le serveur de SecureWay Boundary Server à l'aide de l'assistant. L'assistant vous aide à configurer le pare-feu de manière à ce qu'il puisse fonctionner avec d'autres composants de Boundary Server et de Policy Director. Les écrans qui suivent vous posent des questions sur le serveur LDAP. Une fois les

renseignements demandés obtenus, l'assistant configure IBM Firewall de manière à ce qu'il utilise la même base de données LDAP que celle utilisée par Policy Director pour définir les règles applicables aux utilisateurs et aux groupes. Le cas échéant, l'assistant peut aussi modifier la configuration du serveur relais HTTP du pare-feu pour transmettre les données d'authentification au plug-in SurfinGate (IBM Firewall pour Windows NT).

Pour configurer IBM SecureWay Boundary Server, démarrez l'assistant de configuration. Sur AIX, entrez la commande **sbswizard**. Sur Windows NT, sélectionnez **Démarrer->Programmes->SecureWay Boundary Server**. L'assistant de configuration de SecureWay Boundary Server apparaît à l'écran.

1. Sélectionnez l'option **Set up Firewall to share an LDAP database with Policy Director**.
2. Répondez aux questions posées à l'aide des informations de la section «SecureWay Boundary Server» à la page 13.

Configuration de SecureWay Boundary Server pour l'utilisation du plug-in SurfinGate (Windows NT uniquement

Sélectionnez **Démarrer->Programmes->SecureWay Boundary Server**. L'assistant de configuration de SecureWay Boundary Server apparaît à l'écran.

1. Sélectionnez l'option **Configure the Firewall HTTP Proxy to pass authentication information to the SurfinGate plugin**.
2. Renseignez les autres champs.

Configuration de SurfinGate

Windows NT permet de configurer SurfinGate au choix :

- comme un serveur relais chaîné ;
- comme un plug-in couplé au serveur relais HTTP du pare-feu.

Sur AIX, SurfinGate peut être configuré uniquement :

- comme un serveur relais chaîné.

Configuration de SurfinGate comme serveur relais chaîné

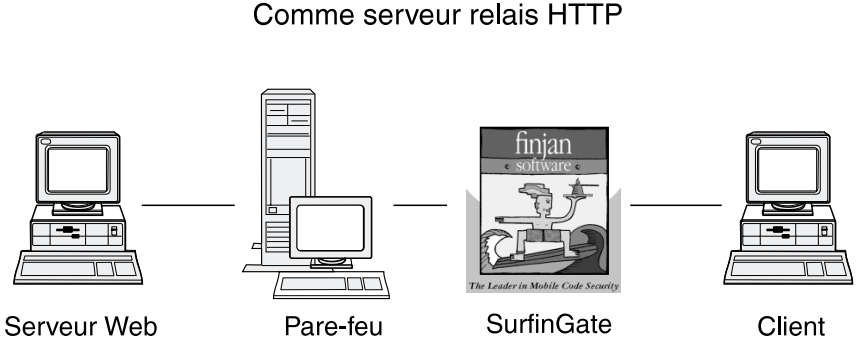

Figure 2. Configurations de SurfinGate

Les navigateurs Web doivent être configurés de manière à utiliser SurfinGate comme serveur relais pour les requêtes HTTP, FTP et HTTPS. N'oubliez pas de spécifier le numéro du port d'écoute de SurfinGate (la valeur par défaut est 8080).

Dans SurfinConsole (l'interface d'administration de SurfinGate), vous devrez cocher l'option **Proxy Mode** dans l'onglet General. Entrez aussi l'adresse et le numéro de port du serveur relais HTTP du pare-feu dans le champ Next Proxy de l'onglet Proxy. Le cas échéant, si d'autres serveurs relais sont déjà définis, vous pouvez en désigner un comme deuxième serveur relais.

Configuration de SurfinGate comme plug-in du serveur relais HTTP du pare-feu

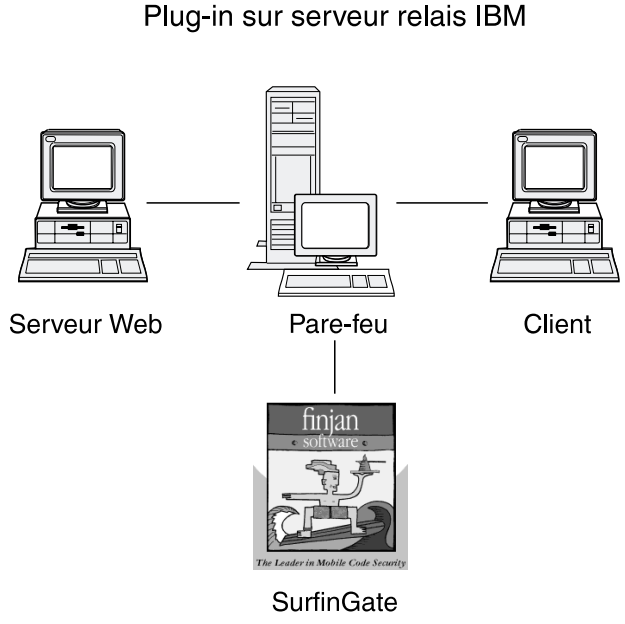

Figure 3. Configurations de SurfinGate

Les navigateurs Web doivent être configurés de manière à utiliser le serveur relais HTTP du pare-feu pour les requêtes HTTP, FTP et HTTPS. N'oubliez pas de spécifier le numéro du port d'écoute de serveur relais HTTP du pare-feu (la valeur par défaut est 8080).

Dans SurfinConsole (l'interface d'administration de SurfinGate), vous devez cocher l'option **Plugin Mode** dans l'onglet General. Entrez aussi l'adresse et le numéro de port du serveur relais HTTP du pare-feu dans le champ Next Proxy de l'onglet Proxy.

Remarque : Cette configuration n'est possible qu'avec SecureWay Firewall pour Windows NT.

Configuration de MIMEsweeper

Configuration de MAILsweeper

Figure 4. Configurations de MAILsweeper

Si votre environnement est peu développé, la configuration de MAILsweeper doit découler des questions posées lors de l'installation. Pour définir d'autres paramètres de configuration, sélectionnez **Démarrer->Programmes->MAILsweeper for SMTP->MAILsweeper for SMTP Console.** Pour plus d'informations, reportez-vous au manuel MAILsweeper Getting Started Guide (Guide de démarrage).

Configuration de WEBsweeper

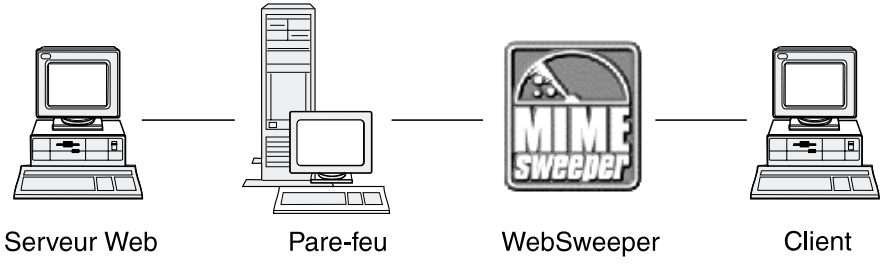

Figure 5. Configurations de WEBsweeper

Pour configurer WEBsweeper, ouvrez le panneau de configuration et sélectionnez l'applet WEBsweeper. Pour plus d'informations, reportez-vous au manuel WEBsweeper - Guide de l'administrateur, sur le CD-ROM de MIMEsweeper.

Configuration de WEBsweeper HTTPS

Pour configurer WEBsweeper HTTPS, ouvrez le panneau de configuration et sélectionnez l'applet WEBsweeper HTTPS. Pour plus d'informations, reportez-vous au manuel WEBsweeper - Guide de l'administrateur.

Blocage des intrusions

Utilisez les utilitaires de ligne de commande pour créer des filtres afin de bloquer des adresses IP définies. Les adresses à bloquer peuvent être déterminées dynamiquement à la suite d'analyses de contenus. Les commandes sont les suivantes :

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

Si vous entrez cette commande sans paramètres, une invite s'affichera pour vous demander de spécifier le format des paramètres obligatoires.

Ces paramètres sont les suivants :

ID du filtre (Dynamic Rule ID)

IBM Firewall pour Windows NT : Des ID peuvent être affectés aux filtres (ensembles de règles) afin de faciliter leur gestion. Ces ID sont définis par ordre croissant en partant de 1. Si vous entrez un ID supérieur à la valeur disponible suivante, c'est cette valeur qui sera affectée au filtre et non celle spécifiée avec la commande. Par exemple, s'il existe un ensemble de règles (un filtre) ayant l'ID 1 et que vous en créez un autre avec l'ID 3 alors que l'ID 2 est disponible, le filtre créé recevra l'ID 2. Plusieurs règles peuvent être regroupées sous un même numéro d'ID. Les règles supprimées par la commande delete_dynamic sont désignées par leur ID. Si vous regroupez ces règles par ID, vous devez vous attendre à supprimer l'ensemble du groupe si vous utilisez des ID communs à plusieurs règles.

Lorsqu'une règle est ajoutée, son numéro d'ID apparaît à l'écran.

ID du filtre (Dynamic Rule ID)

IBM Firewall pour AIX : Les ID peuvent être affectés aux filtres par numéro. Par exemple, si vous spécifiez l'ID 12 avec la commande, le filtre sera bien associé à l'ID 12. AIX ne permet pas d'affecter un même ID à plusieurs filtres. Chaque filtre possède son ID propre.

Adresse IP source (Source Address)

L'adresse IP de la source des paquets doit être entrée en notation décimale à points (par exemple, 255.255.255.255).

Masque IP source (Source Mask)

Ce champ doit être renseigné en relation avec l'adresse IP source. Sa valeur doit être entrée en notation décimale à points. Par exemple, si l'adresse IP source entrée est 10.5.8.0 et que le masque IP source est 255.255.255.0, la règle s'applique à tous les paquets provenant d'une adresse comprise entre 10.5.8.1 et 10.5.8.255.

Adresse IP de destination (Destination Address)

L'adresse IP de la destination des paquets doit être entrée en notation décimale à points (par exemple, 255.255.255.255).

Masque IP de destination (Destination Mask)
Ce champ doit être renseigné en relation avec l'adresse IP de destination. Sa valeur doit être entrée en notation décimale à points. Par exemple, si l'adresse IP de destination entrée est 10.5.8.0 et que le masque IP de destination est 255.255.255.0, la règle s'applique à tous les paquets provenant d'une adresse comprise entre 10.5.8.1 et 10.5.8.255.

Interface (Adapter)
La spécification d'interface est au choix :

S pour les interfaces sécurisées ;

N pour les interfaces non sécurisées ;

B pour toutes les interfaces (sécurisées ou non).

La règle créée s'appliquera aux paquets provenant des cartes correspondant au type défini.

Type (Scope)
Ce paramètre permet de spécifier le type de paquet concerné par la règle :

L pour les paquets locaux ;

R pour les paquets routés ;

B pour les paquets locaux et routés.

Direction
Spécifie le sens des transmissions (en entrée, en sortie ou les deux) :

I pour les transactions en entrée ;

O pour les transactions en sortie ;

B pour les transactions en entrée et en sortie.

Journalisation (Logging)
Entrez Y pour activer la journalisation des activités de filtrage dynamique ou N pour la désactiver.

fwdelete_dynamic

Si vous entrez cette commande sans paramètres, tous les filtres dynamiques définis apparaissent à l'écran.

```
>>>>  Dynamic Rule Id           =  1
 >>>>>>>>  Jump                 =  0
 >>>>>>>>  Filter Action        =  Deny
 >>>>>>>>  Source Address       =  9.192.8.7
 >>>>>>>>  Source Mask          =  255.255.255.0
 >>>>>>>>  Destination Address  =  9.192.240.1
 >>>>>>>>  Destination Mask     =  255.255.255.0
 >>>>>>>>  Protocol             =  Any
 >>>>>>>>  Source Port          =  Any 0
 >>>>>>>>  Destination Port     =  Any 0
 >>>>>>>>  Adapter              =  Both (Secure and NonSecure)
 >>>>>>>>  Scope                =  Both (Routed and Local)
 >>>>>>>>  Direction            =  Both (Inbound and Outbound)
 >>>>>>>>  Tunnel Id            =  0
 >>>>>>>>  Logging Enabled      =  Unavailable
 >>>>>>>>  Fragments Allowed    =  No
```

Remarque : Utilisez d'abord la commande `fwdelete_dynamic` pour vérifier les ID des règles que vous voulez supprimer.

Lorsque vous entrez la commande avec un ID de filtre, le nombre de règles supprimées apparaît sous la forme d'un message.

AVERTISSEMENT : Si vous tentez de créer un filtre existant déjà, un message vous en informera. Si vous tentez de créer un filtre sans spécifier son ID, vous obtiendrez un message d'erreur.

Pour AIX, le blocage des intrusions peut être ignoré s'il existe des règles définies dans un jeu de règles de niveau supérieur. Si vous voulez utiliser le blocage des intrusions, la plupart des règles doivent être définies dans le jeu de règles du niveau inférieur. Les règles dynamiques interviennent entre ces deux jeux de règles. Si une règle de niveau supérieur permet une transaction, vous ne pouvez pas l'interdire par des règles dynamiques.

Test de la configuration

Une fois accomplies les opérations décrites jusqu'ici, vous devez valider la configuration définie. Pour tester la configuration de SecureWay Boundary Server :

1. Créez un utilisateur relais de pare-feu dans la console de gestion de Policy Director. Configurez cet utilisateur de manière à ce qu'il utilise un mot de passe de pare-feu pour les transactions Telnet sécurisées et définissez ce mot de passe.
2. Démarrez l'assistant de SecureWay Boundary Server pour établir une liaison entre le pare-feu IBM Firewall et l'annuaire SecureWay Directory (LDAP).
3. Ouvrez une session Telnet par serveur relais à partir d'un client sécurisé.
4. Entrez les données d'identité de l'utilisateur dans Policy Director.
5. Un message vous demande d'entrer un mot de passe.
6. Vous voici authentifié.

Chapitre 6. Documentation annexe

Les documents répertoriés dans ce chapitre contiennent des informations sur IBM SecureWay Boundary Server Version 2.0 et sur les produits annexes.

IBM SecureWay FirstSecure

Le manuel IBM SecureWay FirstSecure V. 2.0 - Guide de planification et d'intégration contient des informations sur FirstSecure. Il décrit FirstSecure et ses composants et permet de planifier l'utilisation des produits de la famille IBM SecureWay.

IBM SecureWay Firewall

Les documents suivants contiennent des informations sur IBM SecureWay Firewall pour Windows NT et sont disponibles en version PDF et HTM dans le répertoire `x:\books\en_FR` du CD-ROM d'IBM SecureWay Firewall :

- IBM SecureWay Firewall pour Windows NT - Guide de configuration et d'installation
- IBM SecureWay Firewall pour Windows NT - Guide de l'utilisateur
- IBM SecureWay Firewall pour Windows NT - Guide de référence
- Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3 (livre rouge)

Les documents suivants contiennent des informations sur IBM SecureWay Firewall pour AIX et sont disponibles en version PDF et HTM dans le répertoire `books/en_FR` du CD-ROM d'IBM SecureWay Firewall :

- IBM SecureWay Firewall pour AIX - Guide de configuration et d'installation
- IBM SecureWay Firewall pour AIX - Guide de l'utilisateur
- IBM SecureWay Firewall pour AIX - Guide de référence
- A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions (livre rouge)

MIMEsweeper

MAILsweeper

Les documents suivants contiennent des informations sur MAILsweeper et sont disponibles en version PDF et HTM dans le répertoire \install du CD-ROM de MIMEsweeper :

- Getting Started Guide (\install\MSW4_0_2\Doc\qsg.pdf)
- Fichier README (\install\MSW4_0_2\README.htm)

WEBsweeper

Les documents suivants contiennent des informations sur WEBsweeper et sont disponibles en version PDF et HTM dans le répertoire \install du CD-ROM de MIMEsweeper :

- WEBsweeper Administrator's Guide (\install\WSW3_2_5\Doc\manual.pdf)
- Release Note (\install\WSW3_2_5\Doc\RELNOTES.htm)

WEBsweeper HTTPS Proxy

Le document suivant contient des informations sur le serveur relais HTTPS WEBsweeper et est disponible en version TXT dans le répertoire \install du CD-ROM de MIMEsweeper :

- Fichier README (\install\WSWHTTPS1_0_2\readme.txt)

SurfinGate

Les documents suivants contiennent des informations sur SurfinGate et sont disponibles en version PDF dans le répertoire \docs du CD-ROM de SurfinGate :

- SurfinGate Installation Guide (\docs\install.pdf)
- SurfinGate User's Guide (\docs\manual.pdf)
- Release Note (\docs\SFG 405 RelNotes.pdf)
- Les informations relatives au plug-in SurfinGate se trouvent dans le répertoire \docs.

Annexe A. Résolution des incidents

Ce chapitre explique comment détecter et résoudre les incidents de fonctionnement de SecureWay Boundary Server.

Résolution des incidents courants d'IBM SecureWay Firewall

Incidents de routage

La boîte de dialogue **Règles de sécurité** de l'interface d'IBM Firewall propose une fonction appelée Test de routage IP, qui permet le débogage des incidents de routage. Cochez cette case, activez votre configuration de connexion et activez la journalisation des règles de connexion. Affichez ensuite le contenu du `fichier journal du pare-feu` pour examiner les entrées relatives aux paquets ayant traversé le pare-feu.

Faites les tests suivants, d'abord à partir des adresses IP, puis avec les noms d'hôte.

Impossible de contacter les hôtes à partir du Firewall (par commande ping)

Explication

Votre interface de réseau n'est pas configurée comme il convient.

Action recommandée

Reportez-vous à la documentation du système d'exploitation.

Explication

Votre connexion au réseau non sécurisé n'est pas configurée comme il convient.

Action recommandée

Demandez l'assistance de votre fournisseur de services Internet.

Explication

Si votre réseau sécurisé est placé derrière un routeur, votre pare-feu doit disposer d'une route statique vers ce routeur. Utilisez la commande `netstat -rn` pour vérifier l'existence d'une procédure de routage statique :

```
netstat -rn
```

La sortie doit ressembler à ceci pour la famille de protocoles 2 :

```
Destination  Gateway          Flags     ....
default      nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

Figure 6. Exemple de sortie de la commande netstat -rn.

nrr.nrr.nrr.nrr
représente le routeur vers Internet et est la route par défaut. La route par défaut est une route statique (attribut UG).

nnn.nnn.nnn
représente le domaine non sécurisé. Il s'agit d'une route d'interface (attribut U).

nnn.nnn.nnn.nnn
représente l'interface non sécurisée.

sss.sss.sss
représente le domaine sécurisé. Il s'agit d'une route d'interface (attribut U).

sss.sss.sss.sss
représente l'interface sécurisée.

ss1.ss1.ss1
représente un sous-domaine du côté sécurisé du réseau. srr.srr.srr.srr représente le routeur desservant ce sous-domaine. Il s'agit d'une route statique (attribut UG).

127.0.0.1
représente l'hôte local ou en boucle. Il s'agit d'une route d'interface (attribut U).

Vous devez disposer d'une route spécifique pour chaque interface et la route par défaut doit utiliser le routeur du côté non sécurisé du pare-feu.

Action recommandée
Ajoutez une route statique à la définition de votre routeur. Contactez l'administrateur du routeur. Utilisez la commande `route add`.

Explication
Le masque de sous-réseau de l'interface sécurisée ou de l'hôte que vous tentez de contacter est peut être mal défini.

Action recommandée
Modifiez les paramètres du masque à l'aide des utilitaires de configuration du client.

Impossible de contacter (par ping) des hôtes non sécurisés à partir d'hôtes sécurisés (ou l'inverse)

Explication
Chaque routeur associé au pare-feu doit posséder une route statique désignant le pare-feu comme passerelle pour les réseaux de destination situés au delà du pare-feu.

Action recommandée
Contactez l'administrateur du routeur.

Explication
Si votre réseau sécurisé utilise des adresses de réseau non sécurisé non enregistrées, notamment des adresses privées telles que définies dans le document RFC 1597, les paquets ne seront pas renvoyés à leur émetteur.

Action recommandée

Pour Windows NT uniquement : Utilisez un client doté d'une adresse enregistrée. La fonction NAT (conversion d'adresse réseau) du pare-feu peut être utilisée pour les transactions TCP et UDP mais ne fonctionne pas pour les adresses contenues dans les paquets ICMP comme ceux qu'utilise la commande ping.

Action recommandée

Pour AIX uniquement : Utilisez un client doté d'une adresse enregistrée.

Echec du DNS

Remarque : Le DNS ne fonctionne qu'avec Windows NT.

Explication

Vous avez reçu des messages d'erreur du DNS car le service DNS Microsoft a été configuré avec Microsoft DNS Service Manager.

Action recommandée

Reportez-vous aux instructions d'installation, puis :

1. Supprimez le DNS Microsoft en supprimant l'intégralité du répertoire concerné : `\winnt\system32\DNS`
2. Réinstallez le DNS Microsoft.
3. Redémarrez le système.
4. Réinstallez le correctif du DNS.
5. Redémarrez le système.

Résolution des incidents courants de MIMEsweeper

Défaut de fonctionnement de WEBsweeper et MAILsweeper installés sur la même machine

Explication

Des incidents peuvent survenir lorsque l'on essaie d'exécuter MAILsweeper et WEBsweeper sur la même machine.

Action recommandée

Installez MAILsweeper sur une machine et WEBsweeper sur une autre.

Débit de WEBsweeper anormalement faible

Explication

Le téléchargement des contenus Web se fait trop lentement lorsque vous utilisez WEBsweeper.

Action recommandée

1. Désactivez la journalisation à l'aide du panneau de configuration de WEBsweeper.
2. Installez WEBsweeper sur la machine la plus rapide dont vous disposez.

Incidents au niveau de la licence d'utilisation de WEBsweeper

Explication

Si vous installez WEBsweeper 3.2_5 sur une machine ayant contenu une version antérieure, un conflit peut naître au niveau du code de la licence. Si au démarrage de WEBsweeper, le message d'erreur interne Windows numéro 2140 s'affiche, affichez le contenu du journal des applications dans l'afficheur des événements. WEBsweeper affiche un message signalant une erreur PAKMSG avec un conflit entre le nom d'utilisateur actuel et la licence précédemment définie.

Action recommandée

Supprimez l'ancien code de licence du registre Windows. Chargez l'utilitaire regedit et examinez le contenu du répertoire \\HKEY_LOCAL_MACHINE\SOFTWARE\Content Technologies\MIMEsweeper\License. S'il contient plusieurs clés, supprimez celle associée à l'étiquette ″IBM MIMEsweeper System″. Réamorcez le système.

Incidents lors du téléchargement de fichiers volumineux par WEBsweeper

Explication

WEBsweeper peut manquer de mémoire virtuelle pour stocker les fichiers pendant le filtrage des contenus.

Action recommandée

Augmentez la mémoire physique sur le serveur WEBsweeper.

Résolution des incidents courants de SurfinGate

Absence de réponse de SurfinConsole lorsque Microsoft Internet Explorer est ouvert

Explication

SurfinConsole peut se comporter de manière étrange ou cesser de répondre lorsque Internet Explorer est actif. Ces deux applications entrent en conflit et ne peuvent pas être exécutées simultanément.

Action recommandée

Ne chargez pas Internet Explorer et SurfinConsole en même temps.

Fonctionnement anormalement lent du plug-in SurfinGate

Explication

Le téléchargement des codes mobiles se fait d'une manière anormalement lente lorsque vous utilisez le plug-in SurfinGate.

Action recommandée

Vérifiez que le champ Next Proxy désigne le serveur relais HTTP du pare-feu IBM Firewall dans la section Proxy du menu de configuration de SurfinConsole.

Annexe B. 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 :

Site Counsel, IBM SWG
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Ce Logiciel n'est PAS soumis au contrat de License de Logiciels IBM. Ce Logiciel est soumis aux Conditions Internationales d'Utilisation des Logiciels IBM (IPLA).

Ce produit comprend un logiciel développé et distribué par CERN. Cette phrase doit figurer dans tout produit comprenant ce même logiciel ou des parties de ce logiciel.

Marques

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

AIX

IBM

Microsoft et Windows NT sont des marques de Microsoft Corporation.

SurfinGate est une marque de Finjan Software, Ltd.

MIMEsweeper, MAILsweeper, et WEBsweeper sont des marques de Content Technologies, Ltd.

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

Glossaire

A

adresse de serveur : Code unique affecté à tout ordinateur fournissant des services partagés à d'autres ordinateurs par le biais d'un réseau. Par exemple, un serveur de fichiers, un serveur d'impression ou un serveur de messagerie. Une adresse IP standard est une adresse 32 bits. L'adresse d'un serveur peut être une adresse IP en notation décimale à point ou un nom de système hôte.

adresse IP : Adresse de protocole Internet. Adresse 32 bits unique désignant l'emplacement physique d'une unité ou d'un poste de travail membre d'un réseau. Egalement appelée adresse Internet.

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

C

client : Système ou processus informatique demandant un service à un autre système ou processus informatique communément appelé un serveur. Plusieurs clients peuvent accéder aux services d'un même serveur.

D

délai d'expiration : Délai défini pour la réalisation d'une opération.

DMZ : Zone démilitarisée. Dispositif visant à empêcher les utilisateurs extérieurs d'accéder directement à un serveur contenant les données d'une entreprise.

F

FTP : File Transfer Protocol (protocole de transfert de fichiers). Protocole d'application utilisé pour le transfert de fichiers entre des ordinateurs membres de réseaux. Le protocole FTP demande un ID utilisateur et, parfois, un mot de passe pour autoriser l'accès aux fichiers d'un système hôte distant.

I

ICMP : Internet Control Message Protocol (protocole de contrôle des messages Internet). Protocole utilisé pour gérer les erreurs et contrôler les messages dans la couche de protocoles Internet (IP). Les incidents et les erreurs de destination des datagrammes font l'objet d'un message renvoyé à l'adresse d'origine des envois.

interface de rebouclage : Interface permettant d'éviter les fonctions de communication non indispensables lorsque des données sont routées vers une entité du même système.

Internet : Ensemble des réseaux interconnectés utilisant la suite de protocoles Internet et permettant un accès public à l'échelle planétaire.

intranet : Réseau privé sécurisé intégrant des normes et des applications Internet (telles que les navigateurs Web) à l'infrastructure du réseau informatique d'une organisation.

IP : Internet Protocol (protocole Internet). Protocole sans connexion permettant de router des données dans un réseau ou entre plusieurs réseaux interconnectés. Le protocole IP se comporte comme un intermédiaire entre les couches de protocoles supérieures et la couche physique.

IPSEC : Internet Protocol Security (sécurité de protocole Internet). Norme de développement pour la sécurité des communications au niveau de la couche de traitement des paquets de données ou de la couche réseau.

N

NAT : Network Address Translation (conversion d'adresses de réseau). Fonction de pare-feu permettant de convertir des adresses IP sécurisées en adresses enregistrées externes. La NAT permet d'établir des communications avec des réseaux externes tout en masquant les adresses IP utilisées du côté sécurisé du pare-feu.

P

pare-feu : Unité fonctionnelle ayant pour rôle de protéger et de contrôler la liaison entre un réseau et d'autres réseaux. Le pare-feu empêche les communications non désirées ou non autorisées de pénétrer dans le réseau protégé et ne laisse en sortir que les communications expressément autorisées.

passerelle : Unité fonctionnelle permettant de relier deux réseaux informatiques basés sur des architectures différentes.

PICS : Platform for Internet Content Selection (plate-forme de sélection de contenu Internet). Les clients compatibles PICS permettent aux utilisateurs de déterminer les services payants qu'ils désirent utiliser et, pour chaque service payant, les prix acceptables.

ping : Commande permettant d'envoyer une requête de renvoi d'appel ICMP à un système hôte, une passerelle ou un routeur, dans l'optique d'en recevoir une réponse (le retour d'un ″écho″ prouve l'existence et l'activité du destinataire).

port : Numéro identifiant une unité de communication logique. Les serveurs Web utilisent le port 80 par défaut.

protocole : Ensemble des règles qui contrôlent le fonctionnement des unités fonctionnelles d'un système de communication chaque fois qu'une communication doit être établie. Les protocoles peuvent déterminer le fonctionnement de base des interfaces de communication entre les machines, par exemple l'ordre dans lequel les bits d'un octet sont transmis, comme les modalités des échanges complexes entre les applicatifs, par exemple pour le transfert de fichiers.

R

RPV : Réseau privé virtuel. Réseau comprenant un ou plusieurs tunnels IP sécurisés reliant deux réseaux ou plus.

S

serveur : Ordinateur fournissant des services partagés à d'autres ordinateurs par le biais d'un réseau. Par exemple, un serveur de fichiers, un serveur d'impression ou un serveur de messagerie.

service : Fonction assurée par un ou plusieurs noeuds. Par exemple, HTTP, FTP, Telnet.

shell : Logiciel permettant de gérer et de traiter les lignes de commande entrées à partir du poste de travail d'un utilisateur. Le shell Korn est l'un des shells du système d'exploitation UNIX.

SMTP : Simple Mail Transfer Protocol (protocole de transfert de courriers simplifié). Protocole d'application, membre de la suite de protocoles Internet, permettant de transmettre des courriers entre des utilisateurs dans l'environnement Internet. Le protocole SMTP spécifie l'ordre d'envoi des messages et leur format. Le protocole sous-jacent utilisé par SMTP est TCP.

T

TCP : Transmission Control Protocol (protocole de contrôle des transmissions). Protocole de communication utilisé sur l'Internet. TCP permet d'échanger des informations entre systèmes hôtes. Le protocole sous-jacent utilisé est le protocole IP.

TCP/IP : Transmission Control Protocol/Internet Protocol. Suite de protocoles conçue pour permettre les communications entre des réseaux utilisant des techniques de communication différentes.

Telnet : Protocole d'émulation de terminal. Protocole d'application TCP/IP dédié aux connexions à distance. Telnet permet à un utilisateur d'accéder à un système hôte distant comme si son poste de travail était directement connecté à cet hôte.

U

UDP : User Datagram Protocol (protocole de datagramme d'utilisateur). Protocole, membre de la suite de protocoles Internet, offrant des services de transfert de datagrammes sans connexion et sans sécurité. Le protocole UDP permet à un applicatif ou à un processus résidant sur une machine d'envoyer un datagramme à un autre applicatif ou processus résidant sur une autre machine. Le transfert des datagrammes se fait au moyen du protocole Internet (IP).

V

valeur par défaut : Valeur, attribut ou option défini par le programme lorsque l'utilisateur n'en indique pas explicitement.

W

Web : Réseau constitué de serveurs HTTP proposant des fichiers et des programmes, notamment des documents hypertextes contenant des liens renvoyant à des documents stockés sur d'autres serveurs HTTP. Egalement appelé la Toile, ou le World Wide Web.

WTE : Web Traffic Express (Express trafic Web). Programme de serveur relais avec antémémoire permettant de raccourcir le temps de réponse à l'utilisateur final par le biais de systèmes de mise en antémémoire complexes. Le filtrage PICS permet aux administrateurs de réseau de contrôler l'accès aux informations du Web à partir d'une position centrale.

Référence: CT6RZFR

CT6RZFR

Spine information:

IBM SecureWay Boundary Server pour Windows NT et AIX

Guide de configuration et d'utilisation

Version 2.0