IBM eNetwork Firewall pour Windows NT

Guide de l'utilisateur

Version 3 Édition 2

GC11-1459-00

IBM eNetwork Firewall pour Windows NT

Guide de l'utilisateur

Version 3 Édition 2

GC11-1459-00

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section Annexe A, «Remarques», à la page 119.

Réf. US : GC31-8658-00

Première édition (avril 1998)

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

Par ailleurs, vous pouvez nous adresser tout commentaire sur ce document en utilisant le formulaire intitulé "REMARQUES DU LECTEUR" qui se trouve à la fin du document. IBM pourra disposer comme elle l'entendra des informations contenues dans vos commentaires, sans aucune obligation de sa part. Il va de soi que ces informations pourront continuer à être utilisées par leur auteur.

Dépôt légal : 2e trimestre 1998

Table des matières

À propos de ce guide

Ce guide décrit la configuration et l'administration d'IBM eNetwork Firewall sur les systèmes Windows NT** ; ce produit permet d'empêcher les connexions sur votre réseau sécurisé, ou depuis ce réseau, qu'elles soient non autorisées ou non souhaitées.

Ce guide s'adresse aux administrateurs de réseaux ou aux responsables de la sécurité des systèmes, et présente l'installation, la gestion et l'utilisation de IBM Firewall. Bien que ce guide décrive le mode d'accès au pare-feu par des programmes clients, il ne s'agit pas d'un guide de l'utilisateur pour ce type de programmes. Pour utiliser des programmes clients tels que Telnet ou FTP, consultez le guide d'utilisation des programmes TCP/IP.

Avant d'utiliser ce guide, consultez les instructions d'installation fournies avec le boîtier du CD-ROM.

Après le lancement du client de configuration, les informations proposées par le système d'aide en ligne vous aideront à compléter les zones de saisie du client de configuration et à passer d'une boîte de dialogue à l'autre.

Connaissances préalables

Il est important que vous possédiez certaines connaissances sur l'adressage TCP/IP, les masques et l'administration des réseaux, avant d'entreprendre l'installation et la configuration d'IBM Firewall. Comme il vous appartient d'installer et de configurer un pare-feu contrôlant les accès, en entrée et en sortie, à votre réseau, vous devez au préalable comprendre le mode de fonctionnement de ce réseau. Vous devez notamment maîtriser les concepts de base des adresses IP, des noms complets et des masques de sous-réseau.

Il existe un excellent ouvrage sur TCP/IP qui présente netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, le routage, et bien d'autres sujets ; il s'intitule *TCP/IP - Administration de réseau*. Reportez-vous à la *Bibliographie* pour obtenir des informations supplémentaires.

Pour les administrateurs de systèmes UNIX, il existe un excellent ouvrage qui porte également sur TCP/IP, le routage, les équipements réseau, DNS et sendmail ; il est intitulé *UNIX System Administration Handbook*. Reportez-vous à la Bibliographie pour obtenir des informations supplémentaires.

Caractéristiques de cette édition

Le produit IBM eNetwork Firewall pour Windows NT offre une grande variété de caractéristiques et peut mettre en place les trois architectures de pare-feu ci-dessous :

1. Relais d'applications
   - FTP ;
   - HTTP, y compris Gopher et WAIS ;
   - Telnet ;

- SafeMail.

HTTP, Telnet et FTP sont équipés de mécanismes d'authentification.

2. Passerelle, au niveau circuit, à l'aide du protocole Socks version 5, un standard Internet.
3. Filtrage — un ensemble complet et fiable de critères pour autoriser ou interdire le trafic. L'adresse TCP/IP, le port, le protocole, la direction, l'adaptateur (sécurisé/non sécurisé) ainsi que d'autres éléments sont des critères de filtrage.

   De nombreux services sont prédéfinis pour augmenter la rapidité de la configuration.

Protocole Socks version 5

Alliant souplesse et simplicité, le protocole Socks version 5 offre en plus les avantages suivants :

- Déploiement facile des méthodes d'authentification et de cryptage ;
- L'association UDP, qui permet de créer un circuit virtuel de relais pour traverser les circuits de relais basés sur UDP ;
- Socks V5 Watcher, qui affiche des informations en temps réel sur les performances de Socks.

Administration simplifiée

En utilisant des applications Java**, que vous pouvez administrer à partir d'une machine distante, vous pouvez aisément mettre à jour la configuration du pare-feu. En outre, différents niveaux d'autorisations peuvent être attribués aux administrateurs pour obtenir encore plus de contrôle sur les accès au pare-feu. Une seule interface utilisateur graphique, très intuitive, peut être utilisée pour administrer IBM Firewall sur les systèmes Windows NT et AIX.

Restrictions d'utilisation sous NT

Lorsque le pare-feu est installé, les protocoles non TCP/IP sont désactivés, ainsi que les services systèmes superflus et les connexions locales à partir de comptes utilisateurs qui n'ont pas les privilèges de l'administrateur.

Authentification rigoureuse

Prise en charge des mécanismes d'authentification les plus répandus, à base de jetons : SecurID, SecureNet Key, et bien d'autres.

Utilitaires de génération d'états

Les utilitaires de génération d'états permettent de soumettre une requête SQL concernant le fichier journal système lorsqu'il a été exporté dans une base de données.

Alerte, contrôle et journalisation

Une fonction de journalisation complète et détaillée enregistre toute l'activité du pare-feu, y compris les adresses TCP/IP, les identificateurs utilisateur, les TOD, les noms de fichier, les numéros de port, etc. Le processus Contrôle de journalisation est proposé pour surveiller les activités suspectes et vous avertir du dépassement des valeurs seuil.

Isolation des réseaux multiples

En utilisant plusieurs cartes d'interface réseau (NIC) dans votre pare-feu, vous pouvez isoler des sous-réseaux multiples.

Disponibilité en plusieurs langues

Une version du produit existe en anglais, japonais, coréen, français, chinois simplifié, chinois traditionnel, italien, espagnol et portugais (Brésil).

Saisie des adresses IP

Lors de la configuration du pare-feu, le système vous demandera d'entrer des adresses IP. Il convient d'entrer une adresse IP complète, au format décimal à point, comportant quatre octets. Le format est le suivant :

```
nnn.nnn.nnn.nnn
```

où chaque segment `nnn` est une série de trois chiffres compris entre 000 et 255.

Pour appeler le Centre d'assistance d'IBM

Le Centre d'assistance d'IBM dispose d'un service d'assistance téléphonique qui diagnostique et trouve une solution à vos difficultés.

Contactez votre représentant local IBM ou votre fournisseur IBM agréé pour en obtenir les coordonnées.

Chapitre 1. Présentation d'IBM Firewall

IBM eNetwork Firewall est un programme de sécurité de réseau pour AIX et Windows NT**. Un pare-feu sert essentiellement de barrage entre un ou plusieurs réseaux privés internes sécurisés et d'autres réseaux (non sécurisés) ou le réseau Internet. L'objectif d'un pare-feu est d'empêcher toute transmission de données non souhaitée ou non autorisée au départ ou à l'arrivée du réseau sécurisé. Le pare-feu se charge de trois fonctions essentielles :

- Appliquer vos règles de sécurité Internet ;
- Permettre aux utilisateurs de votre réseau d'accéder à des ressources autorisées à partir d'un réseau extérieur sans risquer de compromettre la sécurité des données et des autres ressources de votre réseau ;
- Interdire l'accès de votre réseau aux utilisateurs non autorisés.

Le concept de pare-feu

La connectivité totale offerte par Internet peut engendrer de nombreuses menaces en termes de sécurité. Il vous faut donc protéger vos données personnelles, de même que les accès aux machines situées au sein de votre réseau, contre les utilisations abusives d'origine extérieure. Pour cela, la première précaution est de limiter le nombre de points de connexion entre le réseau privé et Internet. La configuration idéale consiste à ce que le réseau privé soit relié à Internet par l'intermédiaire d'une passerelle unique, ce qui permet de contrôler le trafic en entrée et en sortie. Ce type de passerelle se nomme un pare-feu.

L'exemple ci-dessous vous permettra de comprendre le fonctionnement d'un pare-feu. Imaginons un immeuble pour lequel vous souhaitez restreindre les accès et contrôler les personnes qui y pénètrent. Le seul accès à cet immeuble se fait par le hall d'entrée. Dans ce hall, les hôtesses accueillent les personnes entrées dans l'immeubles, des agents de sécurité surveillent les allées et venues, des caméras enregistrent faits et gestes et les lecteurs magnétiques se chargent de reconnaître les identités.

Le fonctionnement de cette organisation est parfaite pour contrôler les entrées dans un immeuble privé. Mais sitôt qu'un individu sans autorisation est parvenu à franchir le hall d'entrée, il n'existe plus aucun moyen de protéger l'immeuble contre les agissements de cet individu. En revanche, si vous surveillez ses mouvements, vous pouvez éventuellement déceler un comportement suspect.

Lorsque vous définissez la stratégie d'un pare-feu, il peut vous paraître suffisant d'interdire tout ce qui peut présenter un risque pour votre entreprise et d'autoriser tout le reste. Pourtant, les nouvelles méthodes de piratage obligent les responsables de la sécurité à anticiper les attaques et, comme dans le cas de l'immeuble, à surveiller les symptômes indiquant une faille dans le système de défense. Il est généralement beaucoup plus grave et coûteux de réparer les dommages créés par une attaque réussie que de donner la priorité absolue à la prévention.

Outils d'IBM Firewall

IBM Firewall s'apparente à une boîte à outils avec laquelle vous construisez différentes architectures de pare-feu. Une fois que vous avez choisi votre architecture et votre stratégie de défense, vous sélectionnez les outils d'IBM Firewall dont vous avez besoin pour les mettre en œuvre. Le client de configuration d'IBM Firewall dispose d'une interface graphique utilisateur permettant une administration conviviale. IBM Firewall permet de retracer de façon exhaustive les événements significatifs tels que les modifications administratives et les atteintes à la sécurité du système.

IBM Firewall est, par essence, une passerelle IP qui divise le monde en deux réseaux ou plus : d'un côté, des réseaux sécurisés ; de l'autre, des réseaux non sécurisés. Internet est un exemple de réseau non sécurisé. Les réseaux sécurisés sont généralement vos propres réseaux IP d'entreprise. Voici quelques-uns des outils offerts par IBM Firewall :

- filtres experts ;
- serveurs relais ;
- serveurs Socks ;
- services spécifiques tels que DNS (Service de noms de domaines) et SafeMail.

Filtres experts

Les filtres experts sont des outils qui inspectent les paquets au niveau session en fonction de critères tels que l'heure, l'adresse IP et le sous-réseau. Les règles de filtrage, en association avec la passerelle IP, exigent que la machine soit équipée d'au moins deux interfaces réseau : l'une pour le réseau IP et l'autre pour le sous-réseau. L'une des interfaces est définie comme non sécurisée, l'autre (ou les autres) étant déclarée(s) comme sécurisée(s). Le filtre est positionné entre les deux ensembles d'interfaces, comme le montre la figure 1.

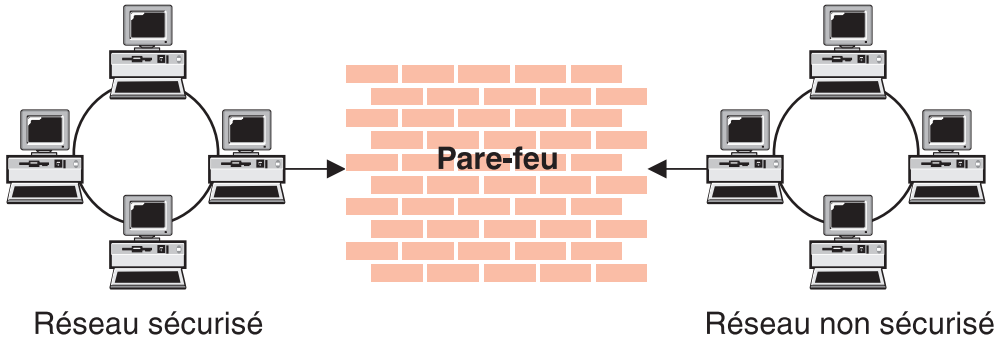

Figure 1. Pare-feu équipé d'un filtrage expert

Fonctions des filtres experts

Le filtrage expert est le mécanisme de protection de base du pare-feu. Les filtres permettent de contrôler le trafic qui passe par le pare-feu en fonction des caractéristiques des sessions IP ; cela permet de protéger le réseau sécurisé des menaces extérieures comme la recherche des serveurs sécurisés ou l'usurpation des adresses IP. Le filtrage doit être considéré comme l'outil de base sur lequel reposent les autres mécanismes.

Serveurs relais

Contrairement au filtrage, qui se contente d'inspecter les paquets, les serveurs relais sont des applications qui font partie du pare-feu et qui se chargent d'effectuer des fonctions TCP/IP spécifiques pour le compte d'un utilisateur du réseau. L'utilisateur contacte le serveur relais en utilisant une des applications TCP/IP (Telnet ou FTP). Le serveur relais établit la communication avec l'hôte distant, toujours pour le compte de l'utilisateur, ce qui permet de contrôler les accès tout en cachant la structure du réseau aux utilisateurs extérieurs. La figure 2 illustre un serveur relais Telnet qui intercepte une requête en provenance d'un utilisateur externe.

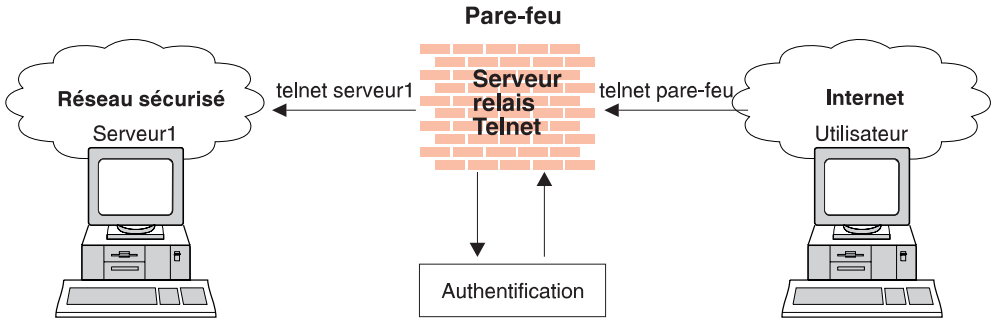

Figure 2. Pare-feu associé à un serveur relais

Les services relais proposés sont telnet, FTP, HTTP, WAIS, GOPHER, HTTPS et SafeMail.

Les serveurs relais d'IBM Firewall peuvent authentifier les utilisateurs à l'aide d'une grande diversité de méthodes d'authentification. Les utilisateurs accèdent aux informations dont ils ont besoin sur Internet sans compromettre la sécurité de leurs réseaux internes.

Fonctions des serveurs relais

Lors d'une connexion via un serveur relais, les connexions TCP/IP sont interceptées au niveau du pare-feu, ce qui réduit les risques de compromettre la sécurité du réseau sécurisé. Les utilisateurs doivent s'authentifier en utilisant une des méthodes d'authentification proposées.

La dissimulation des adresses est un des avantages des serveurs relais. Toutes les connexions sortantes du serveur relais utilisent l'adresse du pare-feu. Par ailleurs, le serveur relais est un garant de la sécurité. Les experts d'IBM ont développé ces serveurs relais pour se prémunir des brèches de sécurité, qui peuvent très bien se trouver sur une machine client.

Soulignons que le serveur relais ne nécessite aucune version spéciale du programme client sur la machine concernée. Ainsi, lorsque le pare-feu est installé, chaque utilisateur enregistré sur celui-ci peut accéder à la partie non sécurisée du réseau sans qu'il ne soit nécessaire d'installer des logiciels supplémentaires.

Serveur Socks

Socks est un standard pour les passerelles au niveau circuit qui permet la dissimulation des adresses sans entraîner la surcharge imposée par un serveur relais classique.

Le serveur Socks fonctionne de la même manière qu'un serveur relais dans la mesure où la session est interceptée par le pare-feu. En revanche, Socks prend en charge toutes les applications et ne requiert pas la mise en place d'un relais unique pour chaque application. De façon transparente, un client socks lance une session à l'aide du service socks de Windows NT sur l'hôte IBM Firewall puis vérifie que l'adresse source et l'ID utilisateur ont l'autorisation d'établir une connexion au réseau non sécurisé et crée la seconde session. La figure 3 illustre le fonctionnement d'un pare-feu et d'un serveur Socks.

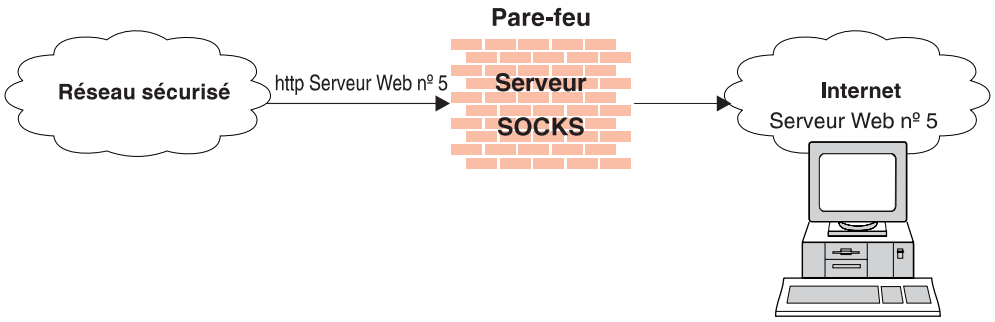

Figure 3. Pare-feu et serveur Socks

Des clients Socks sont proposés avec de nombreuses applications tel Netscape Navigator** ou Microsoft** Internet Explorer, ou avec des logiciels TCP/IP comme Aventail** AutoSocks**.

Fonctions du serveur Socks

Dans le cas de sessions sortantes (depuis un client sécurisé vers un serveur non sécurisé), le serveur Socks joue le même rôle qu'un serveur relais, c'est-à-dire l'interception de la session au niveau du pare-feu et la mise en place d'une porte sécurisée devant laquelle les utilisateurs doivent prouver leur identité pour entrer. Ce mécanisme présente l'avantage d'être simple pour l'utilisateur et ne requiert que peu d'administration supplémentaire.

Service de noms de domaine (DNS)

La possibilité d'accéder aux enregistrements des noms de domaines du réseau sécurisé peut constituer une aide appréciable pour les intrus ; en effet, cela leur permet d'obtenir la liste des hôtes attaquables. Un serveur DNS corrompu peut fournir un chemin d'accès à un intrus. Vis à vis du réseau externe, le serveur de noms du pare-feu ne connaît que lui-même et ne divulgue jamais les informations qui portent sur le réseau IP interne. Vis à vis du réseau interne, ce serveur de noms connaît Internet et permet d'accéder très facilement à n'importe quelle machine reliée à Internet en utilisant le nom de la machine.

Fonctions du serveur DNS

L'exécution d'un serveur DNS sur le pare-feu a pour double avantage d'empêcher que les requêtes de résolution de noms ne traversent le pare-feu et de protéger les hôtes sécurisés des menaces en provenance des environnements non sécurisés.

SafeMail

La messagerie électronique est l'une des principales raisons qui motivent les entreprises à se procurer un accès à Internet. SafeMail est une passerelle de courrier électronique IBM conçue pour dissimuler les noms de domaine de votre réseau interne. La fonction SafeMail ne stocke pas le courrier électronique sur la passerelle et ne se sert pas de l'ID de l'utilisateur root pour s'exécuter. Le nom du domaine public de la passerelle du pare-feu remplace les noms de domaine privé dans les messages électroniques sortants pour que ceux-ci apparaissent comme étant émis à partir de l'adresse du pare-feu et non à partir de l'adresse de l'utilisateur. SafeMail prend en charge le protocole SMTP (Simple Mail Transfer Protocol) et le type MIME (Multipurpose Internet Mail Extensions).

Utilisation du composant Network Security Auditor

Le composant Network Security Auditor se charge de l'analyse du réseau et recherche les brèches de sécurité ou les erreurs de configuration. Il contrôle l'apparition de problèmes ou de risques de sécurité (ports ouverts ou d'autres failles) sur les serveurs et les pare-feu et en établit une liste pour que vous puissiez y remédier. Utilisez-le en tant qu'outil d'analyse périodique des hôtes considérés comme stratégiques ou comme un outil de collecte d'informations ponctuelle. Son administration se fait très simplement à l'aide d'une interface de ligne de commande très conviviale. Avec Network Security Auditor, il est facile de rester vigilant quant à l'utilisation du pare-feu.

Les fonctions du composant Network Security Auditor sont les suivantes :

- Analyse des ports TCP et UDP ;
- Identification des serveurs sur des ports non standard ;
- Notification des services dangereux, des faiblesses connues, des versions obsolètes de serveurs et des serveurs ou services en infraction avec les règles de sécurité en vigueur sur le site ;
- Génération de rapports au format HTML facilitant la recherche d'informations.

Chapitre 2. Planification

Avant de configurer IBM Firewall, aidez-vous de la liste de contrôle et des formulaires de planification pour comprendre la configuration de votre réseau.

Liste de contrôle de la planification

1. Quel est votre objectif ? Désirez-vous :
   - Accéder à Internet (Telnet, FTP anonyme, etc.) ?
   - Partitionner votre réseau interne ?
   - Autoriser les accès *externes* à votre réseau ?
2. Évaluez la topologie de votre réseau au niveau du sous-réseau IP.
   - Une configuration à deux interfaces, l'une sécurisée et l'autre non sécurisée, vous convient-elle ?
   - Vos adresses autorisent-elles la prise en charge des masques de sous-réseau dans les règles ?
3. Choisissez le mode d'utilisation de DNS. Reportez-vous au Chapitre 6, «Gestion DNS (Service des noms de domaine)», à la page 31.
4. Choisissez le mode d'utilisation de safemail. Reportez-vous au Chapitre 7, «SafeMail», à la page 41.
5. Si vous souhaitez utiliser Socks, veillez à ce que les clients compatibles Socks, tels que Netscape Navigator ou le navigateur Microsoft, sont installés. Pour de plus amples informations sur l'utilisation de Socks, reportez-vous au Chapitre 11, «Configuration du serveur Socks», à la page 71.
6. Quel est le type d'authentification nécessaire ?
   - Si vous utilisez Security Dynamics ACE/Server** pour l'authentification des utilisateurs, installez le code client ACE/Server sur l'hôte du pare-feu. Nous vous conseillons d'installer le code du serveur ACE/Server sur un hôte quelconque situé à l'intérieur du réseau sécurisé.

     Pour plus d'informations concernant l'installation et l'utilisation d'un serveur Security Dynamics ACE/Server et de la carte SecurID, consultez la documentation fournie par la société Security Dynamics Technologies Inc.
   - Si vous comptez utiliser une carte AssureNet Pathways** SecureNetKey, achetez les cartes indépendamment du pare-feu IBM Firewall.
   - Si vous utilisez votre propre méthode d'authentification, consultez le chapitre qui porte sur l'utilisation des méthodes d'authentification fournies par l'utilisateur dans le *guide de référence d'IBM Firewall*.
   - Vous devez configurer le code client Windows qui met en œuvre la fonction de recherche des domaines Windows NT sécurisés, à des fins d'authentification, de sorte qu'il utilise TCP au lieu de NETBIOS. NETBIOS est alors désactivé. Les serveurs Windows NT sécurisés doivent avoir un nom d'hôte et une adresse TCP/IP ; ils doivent également utiliser TCP/IP comme protocole de connexion entre eux et avec le pare-feu. L'administrateur du pare-feu doit créer les connexions entre le pare-feu et les serveurs Windows NT sécurisés afin de permettre l'échange de données entre eux.

Définissez ce type de connexion en utilisant les services prédéfinis suivants :

a. Domain Controller Authentication - ce service permet l'utilisation de Domain Controller pour l'authentification des utilisateurs.

b. Diffusions par les services de noms NetBT - ce service permet les diffusions NetBIOS par les services de noms sur TCP/IP.

Utilisez les utilitaires de configuration NT pour définir les relations de confiance.

7. Si vous utilisez le filtrage, commencez par utiliser des règles de filtrage simples mais très restrictives. Prenez l'habitude de reconnaître les ports et les protocoles utilisés par les services dont vous avez besoin.
8. Choisissez une méthode d'archivage des fichiers journaux. L'archivage est une opération particulièrement adaptée à une prise en charge par le service Windows NT Scheduler. Reportez-vous au Chapitre 15, «Gestion des fichiers journaux et des archives», à la page 111.

Formulaire de planification pour la configuration de réseau

Complétez les zones ci-dessous pour planifier votre configuration d'IBM Firewall.

Nom d'hôte du pare-feu _____

Interface(s) réseau sécurisée(s) (connectée(s) au réseau interne sécurisé)

Adresse IP _____ Masque de sous-réseau _____

Adresse IP _____ Masque de sous-réseau _____

Adresse IP _____ Masque de sous-réseau _____

Adresse IP _____ Masque de sous-réseau _____

Interface(s) réseau non sécurisée(s) (connectée(s) au réseau non sécurisé suspect)

Adresse IP _____ Masque de sous-réseau _____

Adresse IP _____ Masque de sous-réseau _____

Adresse IP _____ Masque de sous-réseau _____

Adresse IP _____ Masque de sous-réseau _____

Nom du routeur _____

Adresse du routeur _____

Nom de domaine sécurisé _____

Adresse IP du serveur de noms de domaines sécurisés (DNS) _____

Adresse IP du serveur de noms de domaines non sécurisés (DNS) _____

Serveur de messagerie sécurisé _____

Nom de domaine public _____

Adresse IP du client de configuration _____

Adresse IP de client(s) distant(s) _____

Répertoire racine du pare-feu Windows NT _____
(appelé ROOTDIR dans la documentation)

c:\winnt (en supposant que Windows NT est installé dans ce répertoire)

Chapitre 3. Installation du serveur de configuration et du client de configuration

Le présent chapitre décrit comment installer le serveur et le client de configuration, autrement dit l'interface graphique utilisateur d'IBM Firewall.

Installation du serveur de configuration

Le serveur de configuration est l'interface entre le client de configuration et le pare-feu. Le serveur de configuration traite les requêtes en provenance du client de configuration. Il s'exécute sur la machine pare-feu et peut traiter les requêtes des clients de configuration, qu'ils soient locaux ou distants. Une fois installé, considérez-le comme un composant de la machine pare-feu.

Le numéro de port du serveur de configuration est indiqué dans le fichier des services NT situé dans le répertoire d'installation du système Windows : `c:\winnt\system32\drivers\etc\services`. La valeur par défaut du port est 1014, mais, pour améliorer la sécurité, vous pouvez le modifier en procédant de la manière suivante : arrêtez le serveur de configuration, modifiez le fichier des services et relancez le serveur.

Initialement, le serveur de configuration est configuré de sorte à n'accepter que les requêtes des clients de configuration qui résident sur la machine locale. Les requêtes initiales ne sont pas chiffrées. Pour modifier ces options, entrez `fwcfgsrv cmd=change` sur la ligne de commande.

localonly= Administration du pare-feu uniquement à partir d'une machine locale.

- **localonly=yes** La configuration ne peut avoir lieu que sur la machine locale (option par défaut).
- **localonly=no** La configuration peut être effectuée à partir de n'importe quelle machine.

encryption Le serveur de configuration s'attend au chiffrement SSL des données entrantes.

Si vous modifiez les options de chiffrement ou le fichier de clés SSL, vous devez arrêter le serveur de configuration et le relancer.

- **encryption=none** Aucun chiffrement n'est effectué (option par défaut).
- **encryption=ssl** Activation du chiffrement SSL.

sslfile= Nom du fichier de clés SSL utilisé par le chiffrement SSL ; le nom par défaut est `ROOTDIR\config\fwkey.kyr`. *ROOTDIR* est le répertoire que vous avez sélectionné comme répertoire cible pour IBM Firewall pendant la procédure d'installation. Pour de plus amples informations sur la création du fichier de clés, reportez-vous au *guide de référence d'IBM eNetwork Firewall.*

Si un client de configuration ne peut se connecter au pare-feu et s'il est situé sur une autre machine, utilisez la commande `fwcfgsrv cmd=liste` pour vérifier que l'option `localonly=no` n'est pas en vigueur. En outre, le client et le serveur doivent utiliser la même langue. Vérifiez également que le serveur de configuration est en cours d'exécution en utilisant le panneau des services pour voir l'état dans lequel il se trouve. Pour cela, ouvrez le Panneau de configuration, cliquez deux fois sur l'icône Services et vérifiez l'état de chacun des services. Si le serveur ne s'exécute pas, il doit être relancé.

Installation du client de configuration

Le client de configuration est automatiquement installé lors de l'installation d'IBM Firewall. Il peut également être installé séparément sur n'importe quelle machine Windows NT qui ne dispose pas de pare-feu, ce qui permet une administration à distance. Pour lancer le client de configuration, cliquez deux fois sur l'icône qui lui correspond dans le groupe de programmes IBM Firewall. Une fois lancé, vous devez d'abord vous connecter sur le pare-feu en utilisant le compte d'un administrateur NT.

Seuls les administrateurs Windows NT et les administrateurs du pare-feu ayant les droits d'administration adéquats, peuvent utiliser le client de configuration pour se connecter au pare-feu.

Après l'installation du pare-feu, tous les administrateurs Windows NT sont considérés comme des administrateurs de pare-feu principaux. Si nécessaire, utilisez le client de configuration pour vous connecter sur le serveur de configuration en utilisant un compte d'administrateur de pare-feu principal et définissez des noms d'administrateurs de pare-feu supplémentaires. Reportez-vous au Chapitre 12, «Administration des utilisateurs sur le pare-feu», à la page 77, pour obtenir des informations sur la méthode de définition des administrateurs du pare-feu à l'aide du client de configuration.

Pour que le client de configuration soit lancé dans la langue de votre environnement local, cliquez sur l'icône du client de configuration d'IBM Firewall, puis cliquez sur **Propriétés**. Modifiez les propriétés à l'aide de l'onglet **Raccourci**. Vous pouvez attribuer la valeur *20* au paramètre `timeout` ; 20 est le délai d'attente exprimé en secondes pour l'établissement de la connexion. Les machines rapides peuvent utiliser la valeur 10 ; nous recommandons aux machines lentes d'utiliser la valeur par défaut.

Pour augmenter le niveau des informations de débogage affichées sur la console Java, exécutez `ibmfw.bat` dans `ROOTDIR\cfgcli\gui` au lieu de cliquer sur l'icône du client de configuration. Cependant, cette fonction peut provoquer une dégradation des performances.

Connexion au client de configuration

Pour vous connecter au client de configuration (à partir d'une machine locale ou distante) :

- L'utilisateur doit être un administrateur du pare-feu ;
- L'administrateur du pare-feu doit avoir défini une méthode d'authentification. Reportez-vous à la section «Méthodes d'authentification des utilisateurs», à la page 83 ;

- L'utilisateur doit disposer des droits requis pour accomplir des fonctions de configuration spécifiques.

Activation de la configuration à distance à l'aide du client de configuration

Pour activer la configuration à distance au moyen du client de configuration, assurez-vous que l'administrateur sur le point de se connecter dispose des attributs suivants, définis sur la machine pare-feu :

- Si l'administrateur se trouve sur la partie sécurisée du réseau et qu'il utilise une interface sécurisée sur la machine pare-feu, cet administrateur doit être défini selon la méthode d'authentification qui permet une administration sécurisée. (La méthode d'authentification ne peut être Interdiction globale.) Cette condition s'applique également lorsque la connexion s'effectue localement sur le pare-feu ;
- De même, si l'administrateur se trouve sur la partie non sécurisée du réseau et qu'il utilise une interface non sécurisée sur la machine pare-feu, cet administrateur doit être défini selon la méthode d'authentification qui permet une administration non sécurisée. (La méthode d'authentification ne peut être Interdiction globale.)

Tous les attributs des utilisateurs peuvent être définis à l'aide de la boîte de dialogue Modification des utilisateurs du client de configuration, ou en utilisant la commande `fwuser`. Tous les champs ci-dessus seront complétés de manière appropriée pour les administrateurs du pare-feu après l'installation de ce dernier. Pour plus d'informations, consultez le Chapitre 12, «Administration des utilisateurs sur le pare-feu», à la page 77.

Exemple de journalisation pour le serveur de configuration distant

L'exemple ci-dessous montre un extrait du journal d'activité du serveur de configuration distant :

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: Démarrage du serveur de
configuration distant.
Feb 03 13:52:21 1998 mr16n18: ICA2024i: Utilisateur administrateur
authentifié avec l'authentification NT depuis le réseau sécurisé:127.0.0.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: Utilisateur administrateur
authentifié pour le serveur d'administration distant avec
l'authentification NT depuis le réseau sécurisé:127.0.0.1.
```

Chapitre 4. Utilisation du client de configuration

Le client de configuration, sert d'interface graphique utilisateur, pour configurer et administrer IBM Firewall.

Lors de la première installation d'IBM Firewall, il est initialement configuré pour n'accepter que les requêtes en provenance du client de configuration de la machine locale. Vous pouvez cependant installer le client de configuration sur une autre machine et administrer le pare-feu à distance. Pour savoir comment réaliser cette opération, reportez-vous à la section «Installation du serveur de configuration», à la page 11.

Pour lancer le client de configuration dans la langue de votre environnement local, cliquez sur l'icône Client de configuration d'IBM Firewall, puis cliquez sur **Propriétés**. Modifiez les propriétés à l'aide de l'onglet **Raccourci**. Par défaut, le paramètre de préférence locale défini sur la machine hôte est utilisé. IBM Firewall prend en charge les langues suivantes :

- en_US - anglais (américain) ;
- ja_JP - japonais (EUC) ;
- Ja_JP - japonais (PC) ;
- ko_KR - coréen ;
- zh_CN - chinois simplifié (EUC) ;
- zh_TW - chinois traditionnel (Taiwan) ;
- Zh_TW - chinois traditionnel [Big 5] ;
- fr_FR - français ;
- it_IT - italien ;
- pt_BR - portugais (Brésil) ;
- es_ES - espagnol ;
- Es_ES - espagnol (PC).

L'utilisation du client de configuration nécessite une souris.

Vous trouverez un bouton **Aide** en haut du panneau principal du client de configuration. Cliquez sur **Aide** pour obtenir des informations sur n'importe quelle fonction.

Connexion au client de configuration

1. Pour le type de connexion, sélectionnez Environnement local si vous travaillez sur la même machine que celle du pare-feu. Environnement local est la valeur par défaut. Sélectionnez Administration à distance si vous désirez accéder à distance à un autre pare-feu. Pour l'accès à distance, vous devez spécifier un nom d'hôte.
2. Si vous avez sélectionné la connexion distante, vous devez entrer le nom d'hôte ou l'adresse IP du pare-feu auquel vous souhaitez vous connecter.

3. Sélectionnez SSL ou Aucun suivant le type de chiffrement utilisé pour le pare-feu. Pour le client, la valeur par défaut pour une connexion locale est Aucun et SSL, pour une connexion distante.
4. Entrez le nom d'utilisateur d'un administrateur du pare-feu ou d'un administrateur NT.
5. Entrez le numéro du port sur lequel le serveur écoute. La valeur par défaut est 1014.
6. Dans la zone Mode, sélectionnez Hôte si vous souhaitez configurer la machine pare-feu Windows NT sur laquelle vous êtes connecté. Avec l'administration en mode hôte, l'administrateur peut effectuer la mise à jour d'un seul pare-feu à la fois, en local ou à distance. Sélectionnez Entreprise pour l'administration EFM (Enterprise Firewall management) des pare-feu AIX.
7. Une fois que vous êtes connecté, des messages d'authentification s'affichent et vous invitent éventuellement à entrer un mot de passe si c'est la méthode d'authentification qui a été définie pour votre nom d'utilisateur. Si vous êtes invité à entrer un mot de passe, entrez-le dans la zone Réponse de l'utilisateur, puis appuyez sur la touche Entrée ou cliquez sur Validation. Si votre mot de passe est incorrect, un message s'affiche. Cliquez sur Fermeture et recommencez la procédure de connexion. Si vous n'êtes pas invité à entrer de mot de passe, il se peut que votre méthode d'authentification soit Autorisation globale. Dans ce cas, le panneau Client de configuration IBM Firewall s'affiche immédiatement.
8. Une fois authentifié, vous verrez apparaître le panneau de configuration principal.

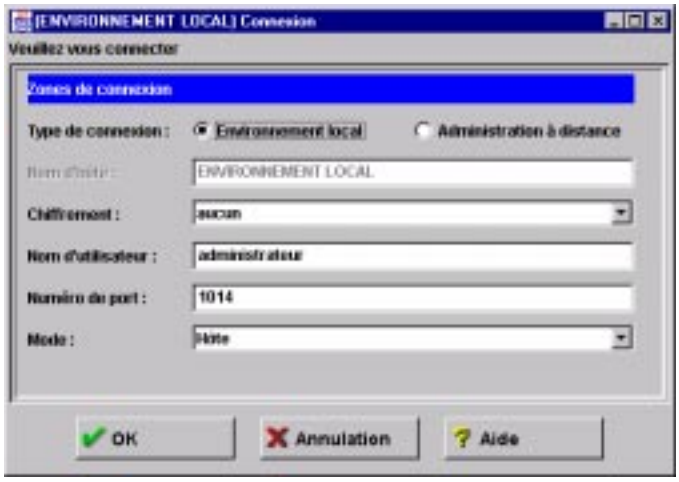

Figure 4. Connexion au client de configuration

Arborescence de navigation

Le client de configuration dispose d'une arborescence de navigation, que l'utilisateur peut développer ou réduire à souhait, située à gauche, comme illustré par la figure 5, à la page 17.

Lorsque des articles sont situés sous un nœud ou une fonction, une icône de dossier apparaît à gauche du nœud. Pour visualiser les fonctions inférieures,

cliquez deux fois sur l'icône pour développer la vue. Cliquez encore deux fois sur l'icône pour réduire le nœud et retourner à la vue initiale.

Lorsque vous cliquez sur une fonction quelconque, celle-ci est considérée comme sélectionnée et elle est mise en évidence. Les nœuds peuvent être développés et réduits sans entraîner de modification de la vue qui apparaît dans la fenêtre de droite. Lorsque l'arborescence développée ne tient pas dans l'espace disponible verticalement, une barre de défilement apparaît à droite de l'arborescence de navigation. Une barre de défilement horizontale apparaît lorsque l'un des noms de fonction est trop long pour tenir dans l'espace disponible.

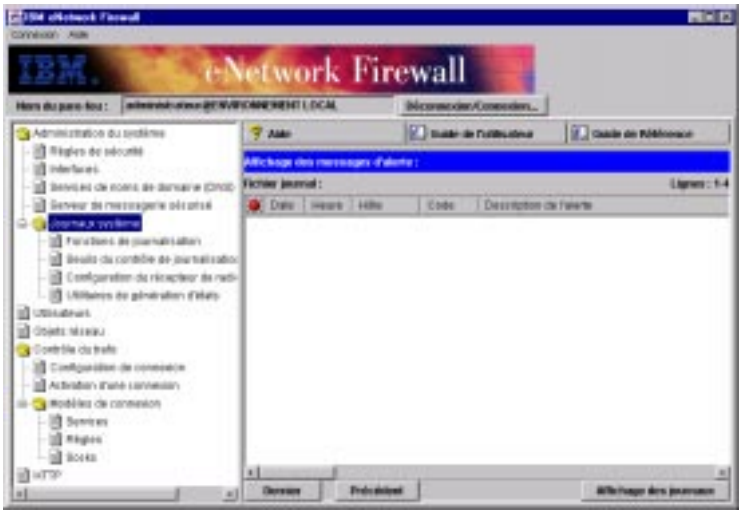

Figure 5. Arborescence de navigation du client de configuration

Fonctions générales du panneau principal

Au-dessus de la zone **Affichage des messages d'alerte**, vous disposez des trois boutons ci-dessous (voir la figure 5).

Aide Vous trouverez le bouton **Aide** en haut du panneau principal du client de configuration. Cliquez sur le bouton **Aide** pour obtenir des renseignements sur le lancement et l'exécution d'IBM Firewall.

Guide de l'utilisateur
Le bouton **Guide de l'utilisateur** situé en haut du panneau principal du client de configuration. Cliquez sur le bouton **Guide de l'utilisateur** pour visualiser la version électronique du présent document.

Guide de référence Le bouton **Guide de référence** situé en haut du panneau principal du client de configuration. Cliquez sur le bouton **Guide de référence** pour visualiser la version électronique de ce document.

Les autres boutons que vous trouverez sur le panneau principal sont les suivants :

Dernier Le bouton **Dernier** est situé en bas du panneau principal du client de configuration. Cliquez sur le bouton **Dernier** pour visualiser les messages d'alerte les plus récents.

Déconnexion/Connexion

Le bouton **Déconnexion/Connexion** est situé dans le coin supérieur droit du panneau du client de configuration. Il s'agit d'un bouton de reconnexion. Vous pouvez alors redémarrer la procédure de connexion afin de vous connecter sur un autre pare-feu ou sous un autre nom d'administrateur.

Pour vous déconnecter, cliquez sur Déconnexion, puis sur Annulation dans le panneau de connexion, puis fermez l'application.

Affichage des journaux

Le bouton **Affichage des journaux** est situé dans le coin inférieur droit du panneau du client de configuration. Il vous permet de consulter les fichiers journaux du pare-feu.

Précédent

Le bouton **Précédent** est situé en bas du panneau principal du client de configuration. Cliquez sur le bouton **Précédent** pour visualiser les messages d'alerte les moins récents.

Affichage des messages d'alerte

Vous pouvez afficher les messages d'alerte générés par le contrôle de journalisation du système dans la partie inférieure droite de la fenêtre du client de configuration, comme illustré par la figure 6, à la page 19.

Les messages d'alerte affichés proviennent du fichier identifié par le premier `journal d'alertes` défini dans `ROOTDIR\config\syslog.conf`. Si vous n'avez pas défini de `journal d'alertes`, aucun message ne s'affiche. Reportez vous à la section «Ajout des fonctions de journalisation», à la page 112 pour avoir plus d'informations sur la définition d'un `journal d'alertes`.

Le panneau indique le nom du fichier de messages d'alerte et le nombre de lignes de ce fichier actuellement affichées. Le bouton **Dernier** permet d'afficher les messages d'alerte les plus récents. Le bouton **Précédent** permet d'afficher les messages d'alerte les moins récents.

Chaque ligne affichée indique la date et l'heure de l'alerte, le nom d'hôte du pare-feu concerné par l'alerte, ainsi que le code et le texte du message d'alerte. Le code indique le type de l'alerte.

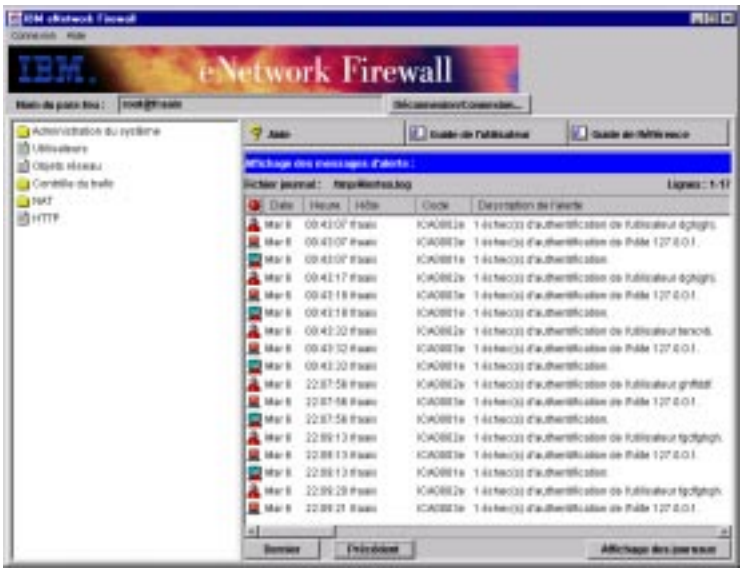

Figure 6. Affichage des messages d'alerte

Affichage des fichiers journaux

Cliquez sur le bouton **Affichage des journaux** pour faire apparaître la fenêtre de visualisation des fichiers journaux, comme illustré par la figure 7, à la page 20. L'affichage des fichiers journaux permet de visualiser les enregistrements de journalisation du pare-feu. Vous pouvez indiquer le fichier journal à visualiser et le nombre d'enregistrements que vous voulez examiner (25, par défaut).

Le fichier journal par défaut est le fichier identifié par le premier `journal de pare-feu défini dans` `ROOTDIR\config\syslog.conf`. Vous pouvez sélectionner un autre fichier journal cible dans le menu déroulant de la zone indiquant les noms de fichiers, ou encore taper le nom d'un fichier à visualiser.

Pour indiquer la première ligne du fichier journal à visualiser, cliquez sur **Démarrage à la ligne**, après avoir tapé un numéro de ligne dans la ligne adjacente à ce bouton. Pour visualiser les dernières lignes du fichier, cliquez sur **Fin**, ce qui vous conduira à la fin du fichier. Le bouton **Suivant** permet de visualiser l'ensemble de lignes suivant dans le fichier. Le bouton **Précédent** permet de visualiser l'ensemble de lignes précédent du fichier. Le bouton **Début** permet de visualiser le début du fichier. En cochant la case **Oui**, vous pouvez transformer les fichiers journaux de pare-feu en texte lisible.

Pour plus d'informations concernant les fichiers journaux, les fonctions, la surveillance et les messages d'alerte, reportez-vous à la section «Création de fichiers journaux et archivage à l'aide du client de configuration», à la page 111 et au Chapitre 14, «Contrôle des journaux du pare-feu», à la page 101.

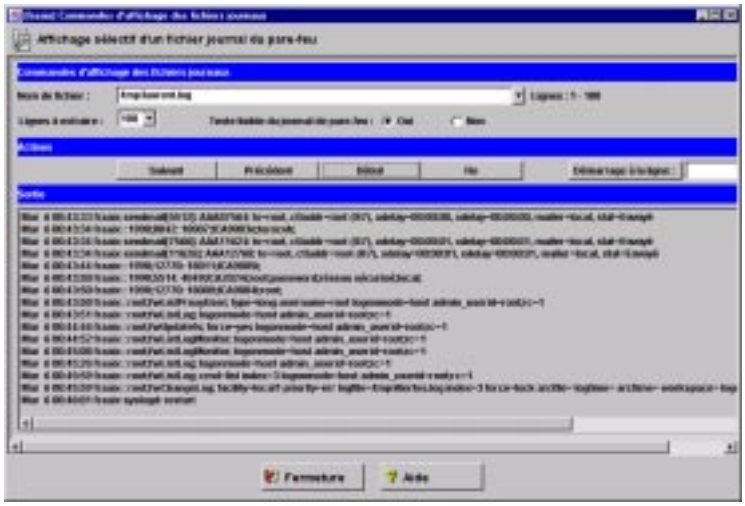

Figure 7. Affichage des fichiers journaux

Autres fonctions

Vous trouverez une zone **Recherche**, située en haut du coin gauche de certains panneaux. Vous pouvez entrer la chaîne de caractères recherchée et cliquer sur le bouton **Recherche**.

Vous trouverez également les boutons suivants sur un grand nombre de boîtes de dialogue du client de configuration :

Appliquer Cliquez sur le bouton **Appliquer** pour compléter la zone du panneau précédent en y insérant la sélection en cours, ou pour sauvegarder les modifications faites dans un panneau. Le bouton **Appliquer** conserve la fenêtre à l'écran.

Fin Cliquez sur **Fin** pour aller à la fin d'un panneau.

Annulation Cliquez sur le bouton **Annulation** pour fermer la fenêtre sans valider les modifications.

Fermeture Cliquez sur le bouton **Fermeture** pour supprimer la fenêtre de l'écran.

Copie Le bouton **Copie** permet de gagner du temps lorsque vous ajoutez de nouveaux éléments à une liste. Une fois que vous avez sélectionné un élément dans la liste, cliquez sur le bouton **Copie** pour créer un élément identique à celui que vous avez sélectionné. Le bouton **Copie** permet de créer un élément identique à la sélection en ouvrant un nouvel élément qui copie les valeurs contenues dans les zones de l'élément sélectionné. Vous pouvez ensuite modifier ces valeurs comme vous le souhaitez pour les attribuer au nouvel élément.

Suppression Cliquez sur le bouton **Suppression** pour supprimer un élément sélectionné dans la liste.

Déplacer vers le bas
Sélectionnez un élément dans la liste, puis cliquez sur **Déplacer vers le bas** pour le déplacer d'une position vers le

bas dans la liste. Chaque fois que vous cliquez sur ce bouton, l'élément sera déplacé d'une position vers le bas.

Déplacer vers le haut
Sélectionnez un élément dans la liste, puis cliquez sur **Déplacer vers le haut** pour le déplacer d'une position vers le haut. Chaque fois que vous cliquez sur ce bouton, l'élément se déplace d'une position vers le haut.

OK Cliquez sur le bouton **OK** pour sauvegarder les modifications et refermer la fenêtre.

Ouverture Après avoir sélectionné un élément dans une liste, cliquez sur le bouton **Ouverture** pour afficher ou modifier cet élément. Pour ajouter un nouvel élément, sélectionnez **Création** dans la liste et cliquez sur **Ouverture**.

Régénération Cliquez sur le bouton **Régénération** pour accéder de nouveau aux données du pare-feu et les réafficher dans le panneau.

Retrait Cliquez sur le bouton **Retrait** pour supprimer un élément sélectionné dans une liste. Cette opération supprime l'élément de la liste et n'a aucune incidence sur les autres endroits où l'élément est défini.

Sélection Cliquez sur le bouton **Sélection** pour accéder à la liste des objets sur lesquels peut s'appliquer une fonction.

Début Cliquez sur le bouton **Début** pour aller au début d'un panneau.

Zones communes

Vous trouverez également les zones suivantes sur un grand nombre de boîtes de dialogue du client de configuration :

Sortie Pendant l'exécution de la commande, des informations sur la progression de l'opération s'affichent dans cette fenêtre.

Nom Indiquez un nom d'option unique pour cette fonction spécifique du pare-feu. Ce nom ne doit PAS comporter de symbole (|), d'apostrophe (') ou de guillemets (") car ces caractères sont utilisés comme délimiteurs de fichiers SMIT. L'utilisation de ces caractères peut altérer les données.

Description Cette zone est facultative et sert à ajouter un commentaire ou des informations supplémentaires pour une option.

Particularités

Plusieurs particularités du client de configuration doivent être mentionnées.

Pour un client de configuration sous Windows 95 ou Windows NT, une résolution de 1024 x 768 pixels (au minimum) produit les meilleurs résultats.

Si vous maintenez enfoncé le bouton gauche de la souris en activant un compteur et que la souris est déviée sans que le bouton soit relâché, le compteur continue de tourner. Pour l'arrêter, cliquez une fois sur les flèches de direction du compteur avec le bouton gauche de la souris.

Chapitre 5. Mise en route d'IBM Firewall

Le présent chapitre indique les étapes de configuration de base nécessaires à la première mise en route d'IBM Firewall. Ce chapitre explique comment mettre en œuvre une interface sécurisée, définir une politique de sécurité et déterminer des composants d'un réseau.

Étapes de configuration de base

Pour réaliser la configuration de base d'IBM Firewall, procédez comme suit :

1. Planifiez la configuration d'IBM Firewall. Définissez préalablement les fonctions d'IBM Firewall que vous souhaitez utiliser et leur mode d'utilisation. Les chapitres suivants peuvent vous y aider :
   - Chapitre 1, «Présentation d'IBM Firewall», à la page 1
   - Chapitre 2, «Planification», à la page 7
   - Section «Considérations relatives à la planification», à la page 55
2. Indiquez au programme de pare-feu les interfaces qui sont connectées aux réseaux sécurisés. Vous devez disposer d'une interface sécurisée et d'une interface non sécurisée afin d'assurer le bon fonctionnement d'IBM firewall. À partir de l'arborescence de navigation du client de configuration, ouvrez le dossier Administration système, puis cliquez sur **Interfaces** pour afficher la liste des interfaces de réseau proposées dans le pare-feu. Pour modifier l'état de sécurité d'une interface, sélectionnez une interface et cliquez sur **Modification**. Pour plus d'informations, reportez-vous à la section «Définition de l'interface réseau», à la page 24.
3. Déterminez les **Règles de sécurité** dans la boîte de dialogue correspondante accessible via le dossier d'administration du système. Pour les configurations de pare-feu de base, les règles sont :
   - Autorisation des requêtes DNS ;
   - Interdiction des diffusions de messages vers l'interface non sécurisée ;
   - Interdiction d'utiliser Socks pour les cartes non sécurisées.

   Pour plus d'informations, reportez-vous à la section «Utilisation du client de configuration pour définir les règles de sécurité», à la page 26.
4. Définissez les services de nom de domaine et de courrier. Accédez à ces fonctions en passant par le dossier Administration du système ou par l'arborescence de navigation du client de configuration. Auparavant, reportez-vous au Chapitre 6, «Gestion DNS (Service des noms de domaine)», à la page 31.
5. Définissez les éléments clés du ou des réseau(x) sur le pare-feu à l'aide de la fonction **Objets réseau** dans l'arborescence de navigation du client de configuration. Les objets réseau permettent de contrôler le trafic via le pare-feu. Les éléments clés suivants doivent être considérés comme des objets réseau :
   - interface sécurisée du pare-feu ;
   - interface non sécurisée du pare-feu ;
   - réseau sécurisé ;
   - tout sous-réseau du réseau sécurisé ;

- un objet réseau d'hôte pour serveurs SDI et serveurs de domaine NT, si nécessaire.

Pour plus d'informations, reportez-vous à la section «Objets réseau», à la page 28.

6. Activez les services sur le pare-feu. Il s'agit de méthodes qui permettent aux utilisateurs au sein d'un réseau sécurisé d'accéder à un réseau non sécurisé (socks ou relais, par exemple). Le type de service à mettre en œuvre dépend des choix que vous avez effectués au cours de l'étape de planification. La mise en œuvre d'un service nécessite la plupart du temps la configuration de connexions autorisant certains types de communication. À titre d'exemple, pour autoriser les utilisateurs du réseau sécurisé à surfer sur Internet (Web) via le serveur relais HTTP, vous devez non seulement configurer le démon Serveur relais HTTP sur le pare-feu, mais vous devez aussi configurer les connexions afin d'autoriser les communications HTTP. Pour plus d'informations sur la configuration des connexions prenant en charge certains services, reportez-vous au Chapitre 9, «Exemples de services», à la page 55.
7. Configurez les utilisateurs du pare-feu. Si vous décidez de demander l'authentification d'utilisateurs, par exemple lors de l'accès au web en sortie, ou d'administrateurs de pare-feu, vous devez définir ces utilisateurs sur le pare-feu. Pour plus d'informations, reportez-vous au Chapitre 12, «Administration des utilisateurs sur le pare-feu», à la page 77.
8. Si vous souhaitez utiliser les mots de passe d'un domaine Windows NT lors de l'authentification, vous devez configurer en conséquence le code du client Windows mettant en œuvre la fonction de recherche dans des domaines Windows NT fiabilisés, afin d'utiliser TCP au lieu de NETBIOS. NETBIOS est alors désactivé. Les serveurs Windows NT fiabilisés doivent avoir un nom d'hôte et une adresse TCP/IP ; ils doivent également utiliser TCP/IP comme protocole de connexion entre eux et avec le pare-feu. L'administrateur du pare-feu doit créer les connections entre le pare-feu et les serveurs Windows NT fiabilisés afin de permettre la circulation des flux de données entre les deux.

Le respect de cette procédure doit vous aider à mettre en place une configuration de base d'IBM Firewall et d'assurer son fonctionnement. IBM Firewall propose d'autres fonctions, tels les journaux système qui servent à assurer la sécurité de votre réseau. Pour plus d'informations, reportez-vous au Chapitre 15, «Gestion des fichiers journaux et des archives», à la page 111.

Définition de l'interface réseau

Dans ce manuel, une distinction est toujours faite entre le caractère sécurisé ou non sécurisé des interfaces, des réseaux et des hôtes. Les interfaces sécurisées connectent l'hôte IBM Firewall au réseau d'hôtes d'un réseau interne, c'est-à-dire celui que vous devez protéger. **Le pare-feu doit disposer au minimum d'une interface sécurisée pour fonctionner.** Les interfaces non sécurisées assurent la connexion d'IBM Firewall à un ou plusieurs réseaux extérieurs ou à Internet. IBM Firewall doit disposer au minimum d'une interface non sécurisée.

Tous les réseaux reliés par une interface sécurisée sont considérés comme sécurisés. Pour différencier plusieurs sous-réseaux reliés par une interface sécurisée, utilisez les règles de filtrage spécifiques pour autoriser ou interdire à un

sous-réseau d'accéder à un autre sous-réseau en utilisant l'adresse IP ou un masque d'adresse.

Pour désigner les interfaces sécurisées et non sécurisées, ouvrez le dossier Administration du système dans l'arborescence de navigation du client de configuration. Toutes les interfaces (ou adaptateurs) connues sont indiquées et identifiées comme étant sécurisées ou non sécurisées.

Vous devez attribuer un nom à chaque interface avant de pouvoir réaliser le filtrage d'une interface déterminée.

Pour définir une interface réseau comme étant sécurisée ou non sécurisée, procédez comme suit :

1. Sélectionnez une interface et cliquez sur **Modification**.
2. Répétez cette procédure autant de fois que nécessaire.
3. Cliquez sur **Fermeture**.

Pour définir le caractère sécurisé ou non d'une interface et lui attribuer un nom significatif, cliquez sur **Ouverture**. Ce nom sera utilisé dans le filtrage d'interfaces spécifiques.

Utilisation du client de configuration pour définir les règles de sécurité

L'une des priorités à envisager lors de la configuration d'IBM Firewall est la détermination de règles générales de sécurité pour l'installation.

La boîte de dialogue, illustrée par la figure 8 est proposée par IBM Firewall pour vous aider à définir les règles de sécurité.

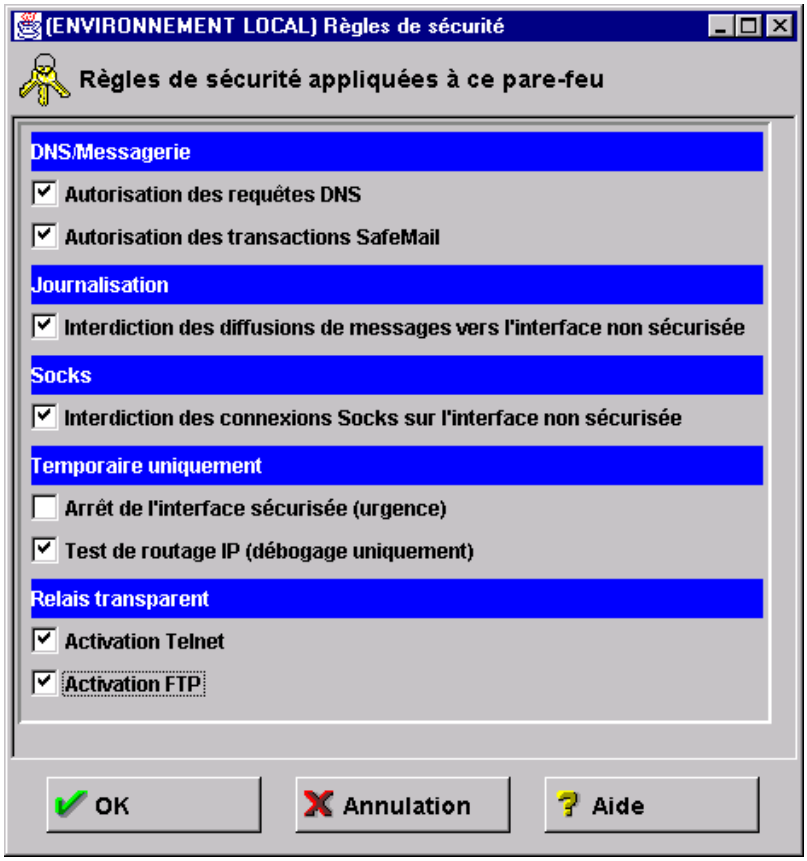

Figure 8. Règles de sécurité

Cliquez sur Aide pour avoir de plus amples informations sur le panneau des règles de sécurité.

Le panneau Règles de sécurité permet aux administrateurs de définir rapidement et simplement des règles globales pour le pare-feu. La plupart des cases à cocher de cette fenêtre permettent d'accéder rapidement à certains services prédéfinis qui s'appliqueront à tout le trafic du réseau transitant via le pare-feu. Il existe deux exceptions à cette règle : les cases à cocher de l'option Relais transparent qui servent à activer ou désactiver Telnet transparent et FTP transparent.

Lorsque vous sélectionnez une règle de sécurité, le pare-feu établit des critères de filtrage que vous devez ensuite activer. Le pare-feu active les services sélectionnés et les met globalement à disposition.

Remarque : Chaque fois que vous sélectionnez une option associée à un service prédéfini et que vous cliquez sur **OK**, vous devez valider ces modifications dans la fenêtre Activation d'une connexion. La validation est inutile si vous modifiez l'une des deux options de Relais transparent car elles ne concernent pas les services prédéfinis. Pour consulter la liste des services prédéfinis, reportez-vous à la section «Services prédéfinis», à la page 66.

Dans la liste d'options suivante, vous pouvez choisir les attributs reflétant les règles de sécurité qui caractérisent votre site. Les attributs sélectionnés concernent l'ensemble des adresses situées de part et d'autre du pare-feu.

- Sélectionnez l'option **Autorisation des requêtes DNS** pour autoriser les demandes de conversion DNS (Services de noms de domaine) et les réponses.
- Sélectionnez **SafeMail** pour autoriser l'acheminement des messages via le pare-feu.
- Sélectionnez **Interdiction des diffusions de messages vers l'interface non sécurisée** pour empêcher la réception de messages sur le port non sécurisé. Si l'interface non sécurisée du pare-feu est connectée à Internet, ce service peut avantageusement servir à réduire le nombre de connexions au pare-feu.
- Sélectionnez l'option **Interdiction des connexions Socks sur l'interface non sécurisée** pour empêcher le flux socks de pénétrer le pare-feu depuis le réseau non sécurisé.
- Sélectionnez **Arrêt de l'interface sécurisée (urgence)** pour désactiver toute transmission à destination ou en provenance du pare-feu via les interfaces sécurisées. Cette procédure est utilisée uniquement en cas d'urgence.
- Sélectionnez **Test de routage IP (débogage uniquement)** pour désactiver toute transmission à destination ou en provenance du pare-feu via une interface quelconque. Remarque : Si vous modifiez la valeur de cette option, vous devez enregistrer la modification en cliquant sur **OK**, puis la valider dans la fenêtre Activation d'une connexion. **L'utilisation de ce service peut générer des problèmes de sécurité pour le pare-feu. Soyez donc extrêmement prudent.**
- Sélectionnez **Activation Telnet** pour activer le protocole Telnet sur des serveurs relais transparents.
- Sélectionnez **Activation FTP** pour activer le protocole FTP sur des serveurs relais transparents.

Objets réseau

Les objets réseau représentent des composants existants sur le réseau, tels des hôtes, des réseaux, des routeurs, des réseaux privés virtuels ou des utilisateurs. Les objets réseau indiquent les adresses source et cible des services lors de la création de connexions.

Les objets peuvent être identifiés par leur nom, par une icône, par leur type et par description. Il existe plusieurs types d'objets réseaux, dont l'hôte et le pare-feu sont les plus courants. L'objet réseau par défaut livré avec IBM Firewall est "The World". Il s'agit d'un objet international reconnaissant tous les types possibles d'adresses IP. Une fois les formulaires de configuration de réseau renseignés (voir «Formulaire de planification pour la configuration de réseau», à la page 8), vous pouvez commencer à définir les objets réseau.

Vous pouvez créer un objet unique ou un groupe d'objets. Tous les objets réseau sont définis par une adresse IP et un masque d'adresse (masque de sous-réseau) ; un seul objet peut donc représenter une plage entière d'adresses réseau.

Utilisation du client de configuration pour définir les règles de sécurité

Pour définir un objet réseau unique, sélectionnez **Objets réseau** à partir de l'arborescence du client de configuration. La boîte de dialogue Objets réseau apparaît. Cliquez deux fois **Création**. La boîte de dialogue **Ajout d'un objet réseau** illustrée par la figure 9, s'affiche.

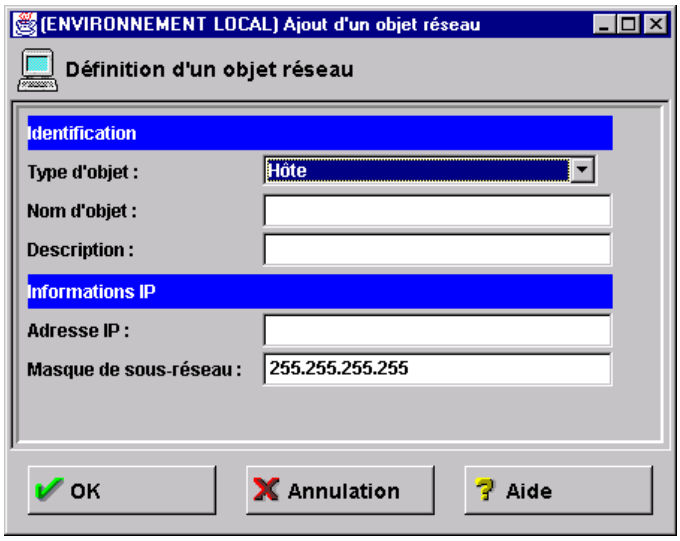

Figure 9. Ajout d'un objet réseau

1. Entrez le type d'objet. Cliquez sur le menu déroulant **Type d'objet** pour voir les types d'objets que vous pouvez créer. Pour ne pas diminuer les performances du système, il est recommandé de créer des objets de type réseau plutôt que de type hôte. Les types d'objets que vous pouvez créer sont les suivants :
   - Hôte - Poste du réseau dont l'adresse correspond au masque 255.255.255.255.
   - Réseau - ensemble des adresses de réseau comprenant une série d'adresses et un masque de sous-réseau.

- Pare-feu - Machine unique sur laquelle est installé un pare-feu et dont l'adresse correspond au masque 255.255.255.255. Seul un objet pare-feu peut être considéré comme cible d'un tunnel IBM ou d'un tunnel manuel.
- Routeur - Hôte acheminant les communications vers un ou plusieurs réseaux et dont l'adresse correspond au masque 255.255.255.255.
- Interface - Carte réseau sur une machine dont l'adresse correspondant au masque 255.255.255.255. Il ne s'agit pas nécessairement d'une carte installée sur le pare-feu.

2. Entrez le nom de l'objet.
3. Entrez la description. Cette zone est facultative.
4. Entrez une adresse IP identifiant cet objet réseau.
5. Entrez un masque de sous-réseau qui correspond aux bits dans l'adresse à comparer avec l'adresse du paquet IP.
6. Cliquez sur **OK**.

Groupes d'objets réseau

Un groupe est un ensemble d'objets réseau. Les groupes sont utilisés dans un but pratique pour mettre en place des connexions et éliminer les tâches répétitives. Par exemple, vous pouvez regrouper certaines adresses représentées individuellement par des objets réseaux, pour former un groupe d'objets réseaux correspondant à un département. Ce département peut servir d'adresse source ou cible lors d'une connexion.

Pour définir un groupe d'objets réseau, sélectionnez l'option Objets réseau à partir de l'arborescence du client de configuration. La boîte de dialogue **Objets réseau** apparaît. Cliquez deux fois sur **Création**. La boîte de dialogue **Ajout d'un objet réseau** s'affiche.

1. Entrez le nom du groupe.
2. Entrez une description. Cette zone est facultative.
3. Cliquez sur **Sélection** pour choisir les objets composant le groupe.
4. Cliquez sur **OK**.

Astuce : Dans la mesure du possible, regroupez des adresses réseau contiguës dans un seul objet réseau. Cette opération, illustrée par l'exemple ci-dessous, permet d'améliorer les performances de traitement des règles de connexion.

```
SERVICE COMPTABILITE
   Machine de Georges 191.1.10.1
   Machine de Suzanne  191.1.10.3
   Machine d'Hélène  191.1.10.5
   Machine de Pierre 191.1.10.7
   Machine de Robert  191.1.10.9
```

Pour créer un objet réseau représentant ce service de comptabilité, vous entreriez l'adresse IP de ce groupe comme suit : 191.1.10.0, avec le masque de sous-réseau : 255.255.255.0. Cet objet réseau, autrement dit ce service de comptabilité, peut servir d'adresse source ou cible lors d'une connexion.

Sauvegarde de la configuration du pare-feu

Tous les fichiers de configuration du pare-feu sont sauvegardés dans `ROOTDIR\config`. Pour sauvegarder une configuration de pare-feu sans prendre en compte tous les fichiers Firewall, sauvegardez intégralement le contenu du répertoire `ROOTDIR\config`.

Pour rétablir une configuration de pare-feu sauvegardée, supprimez tous les fichiers existants du répertoire `ROOTDIR\config` puis restaurez les versions sauvegardées des fichiers. Régénérez et activez les règles de filtrage avant que la configuration restaurée entre en vigueur.

Les fichiers clés de configuration du pare-feu sont répertorisés ci-dessous. Il se peut que le répertoire `\config` ne contiennent pas tous ces fichiers. La plupart des fichiers de configuration sont de simples fichiers texte que vous pouvez visualiser à l'aide d'un éditeur de texte ; en revanche, **vous ne pouvez pas les éditer**.

- carriers.cfg - Définitions d'opérateurs de récepteur de radiomessagerie
- cfgfilt.output
- explode.cfg
- filters.active - Indique si le filtrage est actif
- fwadpt.cfg - Définitions des interfaces réseau
- fwconfig.map - Contient les noms des fichiers de configuration
- fwconns.cfg - Définitions des connexions filtres
- fwfilters.cfg - Filtres actuellement actifs
- fwhttp.cfg - Configuration du serveur relais HTTP
- fwmail.conf - Configuration de SafeMail
- fwobjects.cfg - Définitions d'objets réseau
- fwpolicy.cfg - Options des règles de sécurité
- fwrules.cfg - Définitions de modèles de règle de filtre
- fwservices.cfg - Définitions de services
- fwsocks.cfg - Règles Socks 5 du Client de configuration
- fwtdefn.conf - Définitions d'alertes
- fwtpproxy.cfg - Définitions de relais transparents
- fwusrdb.cfg - Base de données des utilisateurs du pare-feu
- logmgmt.cfg - Définitions des fichiers d'archivage
- modems.cfg - Définitions de modems
- pager.cfg - Définitions de récepteurs de radiomessagerie
- rcsfile.cfg - Paramètres des services de configuration
- Socks5.conf - Fichier de configuration Socks 5 généré
- Socks5.header.cfg - Parties du fichier Socks5.conf généré fournies par l'utilisateur
- syslog.conf - Définitions des fonctions de journalisation

Chapitre 6. Gestion DNS (Service des noms de domaine)

Le présent chapitre décrit la configuration de DNS (Service des noms de domaine) pour IBM Firewall. L'objectif de DNS est de fournir aux hôtes du réseau sécurisé un service de noms de domaines complet tout en fournissant un minimum d'informations aux hôtes extérieurs au réseau sécurisé. Cela permet aux utilisateurs à l'intérieur du réseau sécurisé d'accéder à tous les services offerts par Internet. Cependant, en refusant de divulguer des informations qui portent sur le réseau sécurisé, un intrus aura plus de difficultés pour localiser une machine à pirater.

Pour cela, trois serveurs DNS sont nécessaires :

1. Un serveur sur le pare-feu ;
2. Un serveur à l'intérieur du réseau sécurisé ;
3. Un serveur à l'extérieur du réseau sécurisé.

La figure 10 illustre le fonctionnement de DNS avec IBM Firewall.

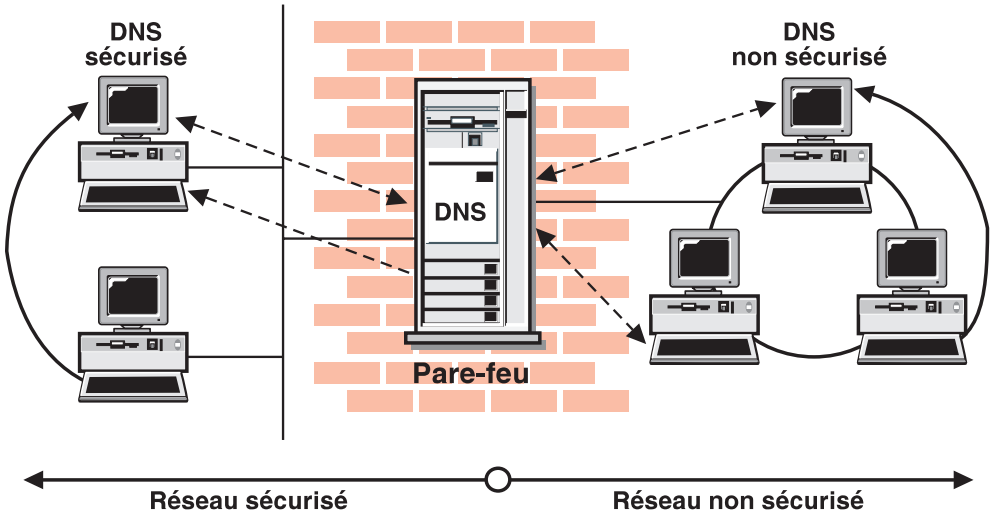

Figure 10. DNS, fonctionnement

Le pare-feu est configuré pour jouer le rôle de passerelle entre le(s) serveur(s) de noms du réseau sécurisé et celui(ceux) qui prennent en charge le réseau non sécurisé. Le serveur DNS sur le pare-feu ne contient aucune base de données ; il joue donc le rôle d'une *antémémoire de noms*.

La figure 10 illustre le rôle du pare-feu. Chaque fois que le pare-feu doit résoudre un nom pour ses propres besoins, il envoie une requête aux serveurs de noms de la zone sécurisée. Losqu'une requête est transmise au pare-feu, il la redirige à son tour vers les serveurs de noms de la zone non sécurisée.

Si un client du réseau sécurisé demande des informations qui concernent la zone sécurisée, il envoie une requête au DNS de la zone sécurisée et celui-ci lui répond. Si ce même client a besoin d'informations sur la zone non sécurisée, il envoie la requête au DNS de cette même zone sécurisée. Comme la requête concerne des informations non sécurisées, le DNS de la zone sécurisée ne peut répondre et transmet la requête au pare-feu.

Dans l'éventualité où un DNS non sécurisé transmet une requête au pare-feu, la requête sera redirigée sur le DNS du domaine non sécurisé ; aucune information sensible ne sera donc divulguée.

Configuration de DNS à l'aide du client de configuration

Pour configurer DNS, sélectionnez, à partir de l'arborescence de navigation du client de configuration, le dossier Administration système. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Sélectionnez l'option **Services de noms de domaine**. IBM Firewall affiche la configuration DNS en cours, que vous pouvez modifier.

Figure 11. Service de noms de domaine

Remarque : Lorsque vous ajoutez le service DNS, le pare-feu enregistre puis renomme les fichiers de configuration DNS existants.

1. La zone **Nom de domaine sécurisé** contient le nom de domaine que le pare-feu concaténera aux noms d'hôte incomplets.
2. La zone **Serveur de noms de domaine sécurisé** fait référence au serveur qui résoudra les noms et les adresses IP pour les hôtes protégés par IBM Firewall. Vous pouvez entrer des adresses IP, au format décimal à point, en les séparant par des espaces.
3. La zone **Serveur de noms de domaine non sécurisé** fait référence au(x) serveur(s) fourni(s) par votre prestataire de services Internet qui résoudront les informations qui concernent le réseau non sécurisé. Vous pouvez entrer des adresses IP, au format décimal à point, en les séparant par des espaces.

Remarque : Lorsqu'un serveur de noms s'initialise, il envoie une requête pour obtenir la liste des serveurs de noms principaux. La plupart des mises en œuvre conservent cette liste en mémoire. Celle de Microsoft réécrit la liste dans le fichier de configuration. Cela ne modifie pas le fonctionnement du serveur de noms mais les valeurs affichées dans la zone **Serveur de noms de domaine non sécurisé** ne seront pas les mêmes. Vous n'avez pas à vous en préoccuper.

Configuration du serveur de noms sécurisé

Le serveur de noms sécurisé doit être configuré de sorte à transmettre au pare-feu les requêtes non résolues. Si vous disposez d'une mise en œuvre de BIND standard, ajoutez les instructions *forwarders* et *cache* au fichier *boot* de votre serveur de noms sécurisé :

```
forwarders      aaa.bbb.ccc.ddd
cache           .               named.cache
```

Créez le fichier d'antémémoire *named.cache* et introduisez dans ce fichier des références au pare-feu comme suit :

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

où *private.com* désigne le nom de domaine utilisé dans la zone sécurisée et *aaa.bbb.ccc.ddd*, l'adresse IP du pare-feu.

De plus, vous pouvez ajouter le nom d'hôte du pare-feu dans les bases de données DNS. Les utilisateurs pourront alors accéder au serveur Socks, aux relais HTTP, Telnet et FTP du pare-feu en utilisant son nom d'hôte à la place de son adresse IP. Cela requiert deux étapes supplémentaires, décrites au *Chapitre 4* du manuel intitulé *DNS and BIND*. Reportez-vous à la *Bibliographie* pour obtenir des informations supplémentaires sur ce manuel.

Ajoutez d'abord un enregistrement A au fichier de base de données du domaine :

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

Ajoutez un enregistrement PTR au fichier des recherches inverses :

```
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

Si vous n'utilisez pas DNS pour votre réseau sécurisé, le pare-feu doit cependant être capable de résoudre ses propres informations. Configurez le pare-feu comme dans une situation normale, mais introduisez l'interface sécurisée du pare-feu dans la zone **Serveur de noms sécurisé**. Ajoutez la ligne suivante dans le fichier `c:\winnt\system32\dns\boot` :

```
primary ccc.bbb.aaa.in-addr.arpa c:\winnt\system32\dns\fwnamed.rev
```

Créez le fichier *fwnamed.rev* de sorte qu'il ressemble à :

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; Numéro de série
                          86400    ; Régénérer au bout d'un jour
                          300      ; Essayer à nouveau dans 5 minutes
                          654000   ; Expiration au bout d'une semaine
                          3600  )  ; TTL minimum d'une journée
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.      IN PTR   firewall.private.com.
```

Configuration des clients sécurisés

Les clients sur le réseau sécurisé doivent être configurés pour envoyer leurs requêtes au serveur de noms sécurisé, et non pas au pare-feu. C'est un élément important car cela garantit qu'aucune information concernant la zone sécurisée n'est stockée dans l'antémémoire du pare-feu. Par ailleurs, cela permet de ne pas trop augmenter la charge de travail du processeur du pare-feu car ce dernier ne sera pas concerné par des requêtes sauf si ces requêtes requièrent d'être transmises de la zone sécurisée à la zone non sécurisée.

Si vous n'utilisez pas DNS pour le réseau sécurisé, les clients devront utiliser le pare-feu comme serveur de noms.

Services accessibles au public

De nombreuses organisations souhaitent mettre leurs services à disposition de la communauté Internet. Il s'agit, en général, de services tels que la messagerie électronique ou des serveurs Web mais cela peut concerner des types quelconques de serveurs TCP/IP. Pour que ces services soient accessibles, vous devez placer le serveur à un endroit du réseau où il peut être joint et le faire répertorier par un serveur DNS public, afin que les utilisateurs puissent obtenir les informations le concernant.

Cela peut être fait de deux manières. Votre prestataire de services Internet peut répertorier vos serveurs comme faisant partie de son domaine (donc, de ses serveurs de noms) ; l'autre solution est de fournir votre propre serveur de noms et de l'enregistrer sur Internet. La première solution est de loin la solution la plus simple. Si vous pouvez adopter cette solution, vous devez indiquer à votre prestataire de services Internet les noms d'hôte et les adresses IP que vous souhaitez répertorier. Par exemple, si le nom de votre serveur web est *www.public.com*, et que son adresse IP est *50.100.150.200*, vous devez demander à votre prestataire de services de répertorier l'élément *www.public.com at 50.100.150.200*.

En outre, si vous souhaitez recevoir du courrier électronique, demandez-lui également de répertorier votre pare-feu comme *échangeur de courrier* pour votre domaine de messagerie électronique public. Votre prestataire de services a besoin du nom d'hôte, *(gateway.public.com)*, de son adresse IP, *(50.100.150.201)*, et du nom de domaine pour la réception du courrier électronique, *(public.com)*.

Si votre prestataire de services Internet ne vous offre pas ce type de services, il vous faudra le faire vous-même. Deux solutions s'offrent à vous. Vous pouvez placer un serveur DNS dans votre DMZ, positionné entre votre réseau privé et Internet (ce type de réseau est qualifiée de "zone démilitarisée") ; la deuxième solution est d'utiliser le pare-feu comme serveur de noms. L'utilisation du pare-feu comme serveur de noms n'entraîne pas de risques supplémentaires pour la sécurité, car les bases de données que vous y placerez ne contiennent pas d'informations sur le réseau sécurisé. Les seules informations qui y sont stockées ont trait aux services publics que vous avez choisi de rendre accessibles.

Vous trouverez des informations détaillées sur la mise en place d'un serveur DNS dans le chapitre 4 du manuel *DNS and BIND* dont la référence figure dans le chapitre *Bibliographie*. Nous vous conseillons vivement de lire ce manuel. La mise en place d'un serveur DNS étant une tâche complexe, elle est souvent confiée à des experts. Si vous en connaissez un, n'hésitez pas à faire appel à son expérience.

Pour de plus amples informations, reportez-vous à la section «Exemples de configurations», à la page 35.

Installation du serveur DNS de Microsoft

Pour installer le serveur DNS de Microsoft, allez dans le panneau de configuration, cliquez sur **Réseau**, l'onglet **Services**, puis sur **Ajouter**, sélectionnez **Serveur DNS Microsoft**. Le CD-ROM d'installation est requis pour cette opération.

Résolution des problèmes DNS

Le *guide de référence d'IBM eNetwork Firewall* contient un chapitre consacré à la résolution des problèmes d'IBM Firewall. Une des sections de ce chapitre traite la résolution des problèmes DNS. Elle contient également des suggestions sur l'utilisation de la commande *nslookup* pour localiser l'élément défaillant du système DNS.

Exemples de configurations

Cette section contient des exemples de configurations permettant la mise en place d'un pare-feu. Dans la plupart des cas, la configuration requise pour le fonctionnement de DNS est décrite. Il est probable qu'aucune de ces configurations ne correspondra à votre réseau ; cependant, étudiez soigneusement chaque exemple et appliquez-en les concepts en fonction de votre installation.

Exemple 1: Serveur DNS dans une DMZ située sur l'interface non sécurisée

Le premier exemple montre les fichiers requis pour le fonctionnement du serveur de noms dans une DMZ située à l'intérieur d'un réseau non sécurisé, comme l'illustre la figure 12.

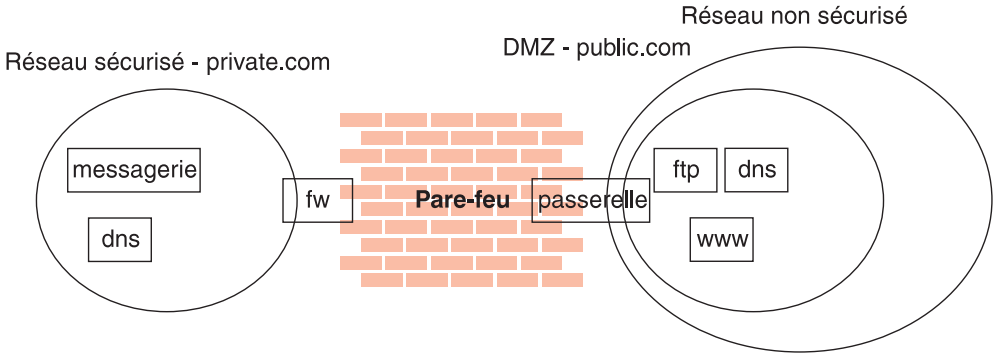

Figure 12. Serveur de noms dans une DMZ située à l'intérieur d'un réseau non sécurisé

Cette figure montre un réseau privé *private.com*, situé à l'arrière d'IBM Firewall dont l'interface sécurisée s'appelle *fw.private.com* et l'interface non sécurisée *gateway.public.com*. La DMZ de la société reliée à l'interface non sécurisée contient un serveur de noms *dns.public.com*, un serveur FTP *ftp.public.com* et un serveur web *www.public.com*.

Le serveur de noms*dns.public.com* contient les fichiers suivants permettant la mise en œuvre de ce scénario :

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; Numéro de série
                  10800       ; Régénération au bout de trois heures
                  3600        ; Nouvelle tentative au bout d'une heure
                  604800      ; Expiration au bout d'une semaine
                  86400 )     ; TTL minimum d'une journée
;
; Serveurs de noms
;
public.com           IN NS  dns.public.com.
;
; Hôtes dans la DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Entrées liées à la messagerie
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; Numéro de série
                  10800       ; Régénération au bout de trois heures
                  3600        ; Nouvelle tentative au bout d'une semaine
                  604800      ; Expiration au bout d'une semaine
                  86400 )     ; TTL minimum d'une journée
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; Numéro de série
                  10800       ; Régénération au bout de trois heures
                  3600        ; Nouvelle tentative au bout d'une semaine
                  604800      ; Expiration au bout d'une semaine
                  86400 )     ; TTL minimum d'une journée
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

La meilleure option pour ce fichier est d'acheminer sous FTP la liste des serveurs de noms root depuis *ftp://ftp.rs.internic.net/domain/named.root*.

boot

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

Pour définir le filtre du trafic autorisant le flux DNS approprié, activez l'option *Autorisation des requêtes DNS* dans le panneau **Règles de sécurité**.

Exemple 2: DNS dans une DMZ située sur une interface dédiée

Dans ce deuxième exemple, le DNS de la DMZ se trouve toujours sur un serveur de noms dédié ; en revanche, la DMZ est reliée à une interface distincte et non à la même interface, comme le réseau non sécurisé.

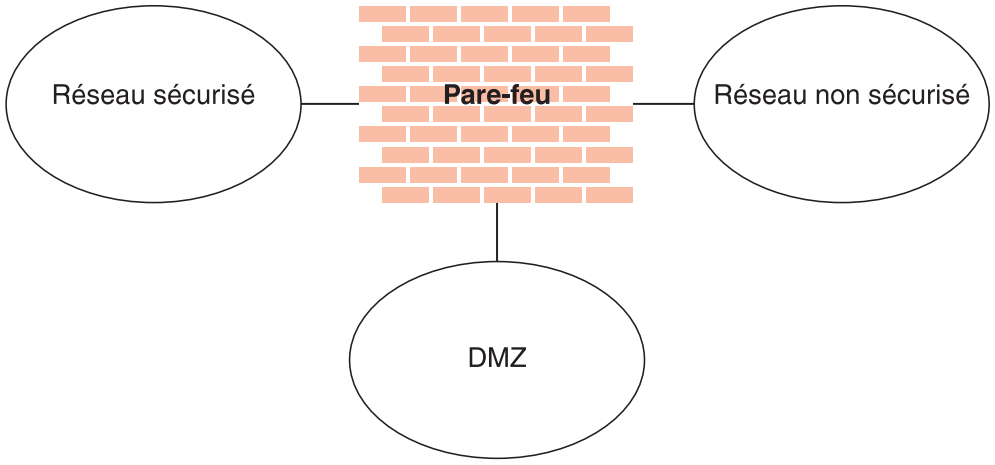

Figure 13. DNS dans une DMZ située sur une interface dédiée

Les fichiers de données DNS de *dns.public.com* sont les mêmes que pour l'exemple précédent. Pour permettre au réseau public d'accéder à ce serveur de noms, il est nécessaire d'ouvrir le filtre du trafic ou d'effectuer un transfert de zone afin de copier les fichiers de données vers le pare-feu.

Pour ouvrir le filtre du trafic, copiez les trois modèles de règles intitulés *DNS Server queries*, *DNS Replies* et *DNS Client queries*. Dans chaque règle, remplacez le paramètre d'acheminement *local* par *routage*. Insérez ensuite les trois nouveaux modèles de règles dans un service et configurez les indicateurs de flux comme suit :

- DNS Client queries: --->
- DNS Replies: <---
- DNS Server queries: --->
- DNS Server queries: <---

Insérez ce service dans une connexion qui utilise l'*extérieur* comme objet source et *dns.public.com* comme objet cible.

Pour réaliser un transfert de zone, vous devez définir le filtre du trafic et programmer les serveurs de noms pour copier les fichiers appropriés. Pour définir le filtre du trafic, procédez comme suit :

1. Dans le panneau **Règles de sécurité**, activez l'option *Autorisation des requêtes DNS*.
2. Ajoutez une connexion entre *dns.public.com* (objet source) et l'interface de la DMZ du pare-feu (objet cible) contenant le service *DNS Transfers*.

Pour activer le transfert de zone, ajoutez les lignes suivantes dans le fichier *boot* de `c:\winnt\system32\dns`:

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

Utilisez ensuite le Service Control Manager pour arrêter et relancer le service DNS Server.

Exemple 3: Utilisation du pare-feu comme serveur de noms sécurisé

Pour utiliser le pare-feu comme serveur de noms sécurisé, placez sur le pare-feu les fichiers de base de données qui devraient normalement résider sur le serveur sécurisé. Les clients pourront alors désigner le pare-feu comme leur serveur DNS. Le risque liée à cette méthode est que le serveur DNS ne peut pas distinguer une requête provenant du côté sécurisé d'une requête provenant du côté non sécurisé. En conséquence, il fournira des informations relatives au côté sécurisé à tous les clients qui en font la demande et vous ne pourrez plus masquer les données DNS sécurisées.

Pour la mise en place de cette méthode, commencez par configurer les fonctions DNS du pare-feu en utilisant le client de configuration. Dans la zone *Nom de domaine sécurisé*, entrez le nom de domaine que vous utiliserez dans le réseau sécurisé. Dans la zone *Serveur de noms sécurisé*, entrez l'interface sécurisée du pare-feu. Dans la zone *Serveur de noms non sécurisé*, entrez, comme d'habitude, le serveur de noms fourni par le fournisseur d'accès à Internet. Complétez cette configuration en créant un fichier de recherche inversée sur le pare-feu.

Créez le fichier `c:\winnt\system32\dns\fwnamed.rev` afin qu'il ressemble à l'exemple suivant.

Dans cet exemple, l'interface sécurisée du pare-feu s'appelle *fw.private.com* et son adresse IP est *10.100.100.1*.

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                  1           ; Numéro de série
                  10800       ; Régénération au bout de trois heures
                  3600        ; Nouvelle tentative au bout d'une semaine
                  604800      ; Expiration au bout d'une semaine
                  86400 )     ; TTL minimum d'une journée
1.100.100.10.in-addr.arpa.        IN NS fw.private.com.
1.100.100.10.in-addr.arpa.        IN A  fw.private.com.
```

Ajoutez la ligne suivante dans le fichier `c:\winnt\system32\dns\boot`

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

Dans ce scénario, les clients doivent être configurés pour désigner le pare-feu (10.100.100.1) comme leur serveur DNS. Le pare-feu vous aidera à résoudre les informations externes mais vous n'aurez aucune solution pour les informations du côté sécurisé. Ceci signifie que tout client du côté sécurisé désirant se connecter au serveur de configuration ou à l'un des serveurs relais du pare-feu, doit contacter le pare-feu en utilisant l'adresse IP et non le nom d'hôte.

Chapitre 7. SafeMail

SafeMail d'IBM Firewall fonctionne comme passerelle pour le trafic SMTP. SafeMail sert de relais entre le ou les serveurs de messagerie sécurisés et le côté non sécurisé, en masquant le nom des domaines sensibles. Il transmet les messages provenant du côté non sécurisé vers le domaine de messagerie sécurisé, protégeant ainsi le réseau sécurisé contre toute tentative d'accès illicite.

Bien que ne possédant aucune fonction de filtrage, SafeMail propose une routine utilisateur permettant de réaliser cette opération. Pour de plus amples informations, reportez-vous à la section «La routine utilisateur de SafeMail», à la page 43.

SafeMail transmet les messages de l'émetteur vers le destinataire en temps réel, afin d'éviter les risques et les complications liés à la maintenance d'une file d'attente de messages sur le pare-feu. Une configuration précise des domaines de messagerie adjacents est donc nécessaire. Il se peut que certaines installations ne soient pas compatibles avec la configuration requise. Dans ce cas, vous pouvez remplacer SafeMail par un serveur SMTP acquis séparément. Si vous choisissez d'installer un serveur SMTP complet, configurez-le en pensant à la sécurité. Pour de plus amples informations, consultez la section «Utilisation d'un serveur SMTP à la place de SafeMail», à la page 44.

Configuration de SafeMail à l'aide du client de configuration

Pour configurer SafeMail, sélectionnez le dossier d'administration du système dans l'arborescence de navigation du client de configuration. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Sélectionnez **SafeMail**. IBM Firewall affiche la liste des serveurs et des domaines de messagerie configurés. Vous devez configurer une entrée pour chaque domaine de messagerie d'un serveur privé en cours de configuration.

1. Pour ajouter un domaine, sélectionnez **Création** puis cliquez sur **Ouverture**. La boîte de dialogue **Ajout d'un serveur de messagerie** s'affiche.
2. La zone **Nom de domaine sécurisé** contient le nom sous lequel les utilisateurs connaissent le domaine de messagerie décrit, du côté sécurisé du pare-feu.
3. La zone **Serveur de messagerie sécurisé** contient le nom d'hôte ou l'adresse IP au format décimal à points du serveur de messagerie concerné par cette entrée. Ce serveur doit figurer parmi les réseaux sécurisés. Vous ne pouvez afficher qu'un seul serveur de messagerie pour un domaine déterminé.
4. La zone **Nom de domaine public** contient le nom sous lequel les utilisateurs connaissent le domaine de messagerie décrit, du côté non sécurisé du pare-feu. Ce nom remplace le nom de domaine sécurisé afin de masquer la topographie du réseau sécurisé.
5. Cliquez sur **OK**.

Modification d'une entrée de configuration de messagerie

Pour modifier une entrée de configuration de messagerie, sélectionnez une entrée dans la liste et cliquez sur **Ouverture**. La boîte de dialogue **Modification de la configuration du serveur de messagerie** apparaît.

La zone **Nom de domaine sécurisé** est désactivée, mais vous pouvez modifier d'autres zones, comme expliqué dans la section «Configuration de SafeMail à l'aide du client de configuration», à la page 41.

Remarques :

1. Si vous avez déjà configuré SafeMail et que vous définissez ici un serveur de messagerie sécurisé, ce dernier remplace le serveur de messagerie précédemment configuré.
2. Si vous n'avez *pas* configuré SafeMail et que vous définissez ici un serveur de messagerie sécurisé, ce dernier est ajouté à la configuration.

Suppression d'une entrée de configuration de messagerie

Pour supprimer une entrée d'une configuration SafeMail, sélectionnez-la dans la liste et cliquez sur **Suppression**. Un message d'avertissement de suppression s'affiche. Cliquez sur **OK** pour confirmer ou sur **Annulation**, si vous changez d'avis.

Configuration des serveurs sécurisés

Vous devez configurer les serveurs de messagerie sécurisés afin qu'ils affichent le pare-feu comme étant leur passerelle vis à vis des domaines inconnus. Ainsi, le courrier destiné au réseau non sécurisé peut être transmis au pare-feu. En outre, chaque serveur doit être configuré pour accepter les messages adressés à leur nom de domaine public en plus de leur nom de domaine privé. Lorsque le pare-feu transmet un message provenant d'un réseau non sécurisé, tous les destinataires sont affichés avec leurs noms de domaine du côté public.

Si le réseau sécurisé contient plusieurs domaines de messagerie différents, vous devez également configurer chaque serveur pour transmettre le courrier destiné à un autre domaine du côté sécurisé directement au serveur, sans passer par le pare-feu. Ainsi libéré d'une charge de travail inutile, le pare-feu peut transmettre les messages en temps réel sans aucune difficulté.

Configuration du domaine public

Le seul élément à configurer dans un réseau non sécurisé est l'affichage du pare-feu en tant qu'échangeur de courrier pour le réseau. Demandez au fournisseur d'accès d'ajouter les informations nécessaires sur leurs serveurs DNS. Pour plus d'informations, reportez-vous au Chapitre 6, «Gestion DNS (Service des noms de domaine)», à la page 31.

L'objectif est d'afficher le pare-feu en tant qu'*échangeur de courrier* pour chaque nom de domaine public pour lequel vous voulez accepter les messages. Par exemple, si vous utilisez le nom de domaine *prive.com* à l'intérieur d'un réseau sécurisé et *public.com* à l'extérieur d'un réseau sécurisé, vous pouvez attribuer au pare-feu le nom *gateway.public.com*. Dans ce cas, demandez au fournisseur d'accès d'afficher les noms d'hôte et adresses IP en tant qu'hôte (généralement

avec des enregistrements "A" et "PTR"). Ensuite, dans la mesure où vous acceptez la messagerie adressée à *user@public.com*, vous devez demander au fournisseur d'accès d'ajouter un enregistrement MX pour le domaine *public.com* qui fait apparaître *gateway.public.com* comme échangeur de courrier pour ce domaine. En outre, si vous décidez de recevoir du courrier adressé à *user@machinchose.com*, vous pouvez afficher un enregistrement MX supplémentaire qui indique également l'emplacement du pare-feu.

La routine utilisateur de SafeMail

SafeMail propose une routine utilisateur qui, lors de l'installation, permet de configurer SafeMail pour refuser tout trafic illicite. Pour de plus amples informations sur ce sujet, consultez, dans le *guide de référence d'IBM eNetwork Firewall*, la section dédiée aux développeurs de logiciels.

Cette routine permet de créer une fonction, *UsrCheck()*, qui est appelée chaque fois que SafeMail reçoit un paquet de l'émetteur. Une structure contenant plusieurs zones relatives à l'état du système est communiquée à la routine. Cette structure comprend un ID de session unique, les adresses IP de l'émetteur et du destinataire, des indicateurs des commandes précédemment reçues et une mémoire tampon contenant le texte en clair du paquet en cours d'analyse.

Cette fonction permet de réaliser les types de contrôles suivants :

- établir des listes d'hôtes *bannis* ;
- rechercher les séquences de caractères non autorisés, par exemple un langage ou des noms de code de projet inappropriés ;
- examiner les chaînes de texte imbriquées ;
- vérifier la longueur des messages.

Si vous le désirez, vous pouvez également utiliser la routine utilisateur pour mettre en place une interface vers un logiciel de filtrage d'un tiers.

Si la routine utilisateur décide de ne pas traiter un message, elle envoie un code d'erreur à SafeMail. Celui-ci rejette immédiatement la connexion du serveur SMTP émetteur. Parallèlement, un message et le code d'erreur renvoyé par la routine utilisateur sont enregistrés dans le fichier journal du pare-feu.

Lors de la programmation d'une routine utilisateur, n'oubliez pas que cette fonction est appelée à chaque réception de paquet. Veillez à l'écrire d'une manière aussi rationnelle que possible afin d'éviter une diminution des performances du système. En outre, cette routine s'exécutant dans un environnement avec unités d'exécution multiples, il est indispensable que sa programmation n'ait aucune incidence sur ces dernières. Vous pouvez programmer la routine utilisateur avec n'importe quel compilateur acceptant les opérations avec unités d'exécution multiples et pouvant utiliser le mode de liaison *_cdecl*. Des exemples de makefiles sont proposés pour IBM Visual Age C++ et Microsoft Visual C++.

Utilisation d'un serveur SMTP à la place de SafeMail

Désactivation de SafeMail

Pour éviter que SafeMail entre en conflit avec un autre produit du serveur SMTP, désactivez-le dans le **gestionnaire de contrôle des services**. Dans le menu **Démarrer** de Windows , sélectionnez **Paramètres, Panneau de contrôle, Services**. Sélectionnez *IBM Firewall SafeMail Server*. Cliquez sur **Démarrer**. Dans la zone **Type de démarrage**, sélectionnez **Désactivé**. Cliquez sur **OK**.

Configuration d'un serveur SMTP

Lors de l'installation d'un serveur SMTP complet à la place de SafeMail, vous devez considérer l'opération sous plusieurs aspects. Cette section décrit les fonctions de sécurité de SafeMail, afin que vous puissiez configurer un serveur SMTP pour assurer ces mêmes fonctions. Certains logiciels de serveur SMTP ne pouvant pas effectuer certaines tâches, lors de l'achat d'un produit, examinez les options proposées par rapport à vos besoins.

Certains intrus tentent de faire déborder, voire de corrompre la file d'attente des messages. Dans la mesure où aucun serveur entièrement opérationnel ne peut fonctionner sans file d'attente de messages, les risques liés à cette tâche sont réduits si vous lui dédiez un volume du disque. Cette mesure de sécurité minimise le risque qu'un débordement de file d'attente ait une incidence sur le bon fonctionnement du pare-feu.

Il est également important que le serveur de messagerie masque les informations concernant le réseau sécurisé. Selon les règles du protocole SMTP, chaque serveur qui achemine une partie d'un message doit insérer un en-tête de ligne *Received:*. Ces en-têtes de ligne peuvent être utilisés par un intrus pour mapper le réseau sécurisé. SafeMail élimine tous ces en-têtes lors du traitement d'un message ; configurez le serveur SMTP pour faire de même. De plus, SafeMail réécrit tous les noms d'hôte du côté privé en nom de domaine public. Ceci permet de supprimer encore des informations susceptibles d'être utilisées pour le mappage du réseau.

Extrait du journal d'activité de SafeMail

```
Feb 03 13:46:11 1998 mr16n18: ICA2163i: démarrage de safemail.
Feb 03 13:41:14 1998 mr16n18: ICA2177i: Connexion SafeMail 0xd71e7a19
réceptionnée depuis RACK3BD.
Feb 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail a transmis 215575
octets pour la connexion 0xd71e6118 entre 9.67.144.52 et 9.67.131.250.
Feb 03 13:41:21 1998 mr16n18: ICA2178i: La session SafeMail 0xd71e7a19
a été établie entre 9.67.144.52 et 9.67.131.250.
Feb 03 13:41:23 1998 mr16n18: ICA2177i: Connexion SafeMail 0xd71e831a
réceptionnée depuis RACK3BD.
Feb 03 13:41:36 1998 mr16n18: ICA2177i: Connexion SafeMail 0xd71e901b
réceptionnée depuis RACK3BD.
Feb 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail a transmis 215567
octets pour la connexion 0xd71e7a19 entre 9.67.144.52 et 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: La session SafeMail 0xd71e831a
a été établie entre 9.67.144.52 et 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: La session SafeMail 0xd71e901b
a été établie entre 9.67.144.52 et 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail a transmis 346
octets pour la connexion 0xd71e901b entre 9.67.144.52 et 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail a transmis 358
octets pour la connexion 0xd71e831a entre 9.67.144.52 et 9.67.131.250.
```

La signification des messages de journalisation est la suivante :

- ICA2177 - indique le démarrage d'une nouvelle connexion.
- ICA2179 - indique l'achèvement correct de l'opération.
- ICA2178 - indique que le contact a été établi avec le serveur SMTP destinataire.
- ICA2181 - indique que SafeMail a rejeté la session. Pour de plus amples informations concernant les messages d'erreur, consultez le *guide de référence d'IBM eNetwork Firewall*.
- ICA2180 - indique la fin de la session.
- ICA2182 - indique que, suite au traitement de la routine utilisateur, la session a été rejetée.

Chapitre 8. Gestion des données via le pare-feu

Le présent chapitre décrit comment utiliser le client de configuration pour contrôler le trafic réseau sur le pare-feu. À l'aide de filtres experts, le pare-feu effectue du filtrage de paquets au niveau session en fonction de plusieurs critères tels que l'heure du jour, l'adresse IP ou le sous-réseau. Le filtrage se produit entre les interfaces réseau sécurisée et non sécurisée et ne fait pas appel aux tables de routage du pare-feu.

Par défaut, le pare-feu n'autorise aucun trafic entre les réseaux sécurisé et non sécurisé. Pour cela, vous devez créer des connexions qui autoriseront certains types de trafic entre un réseau sécurisé et un réseau non sécurisé.

Utilisation du client de configuration pour établir des connexions

Les composants du client de configuration, illustrés par la figure 14, à la page 48, permettent de créer des objets réseau, des modèles de règles, des services et des connexions.

Connexions Elles associent les objets réseau aux services et/ou aux modèles de règles afin de définir les types de communications autorisés entre les extrémités. Chaque connexion définit un type de trafic IP, autorisé ou refusé, entre des objets réseau source et destination.

Services Les services sont construits sur un ou plusieurs modèles de règles. Un service définit également un type de trafic IP, autorisé ou refusé, entre des objets réseau source et destination. Vous pouvez, par exemple, construire un service qui autorise les accès Telnet mais refuse les accès par Ping. (L'un des services FTP, par exemple, est constitué de huit modèles de règles.) Le produit IBM Firewall est fourni avec un ensemble de services par défaut. Ces services par défaut sont préchargés et ne peuvent être supprimés, mais vous pouvez modifier le contenu de certaines zones. Toutefois, si les services préchargés ne répondent pas à vos besoins, vous pouvez en compléter la liste en utilisant les modèles de règles pour créer de nouvelles règles. Pour de plus amples informations, reportez-vous à la section «Définition des services», à la page 68.

Modèles de règles Ils fournissent des instructions au pare-feu pour autoriser ou refuser les paquets IP en fonction de leurs différents attributs.

Modèles Socks Ils fournissent au démon Socks du pare-feu des instructions qui lui pemet d'autoriser ou de refuser les paquets IP en fonction de leurs différents attributs.

Objets réseau Ils représentent les différents composants du réseau comme les hôtes, les utilisateurs et les sous-réseaux qui interagissent avec le pare-feu. Ils sont définis par une adresse IP et un masque d'adresse ; un seul objet peut donc représenter une plage entière d'adresses réseau. Les objets réseau peuvent être regroupés.

Groupes d'objets réseau

Un groupe représente un ou plusieurs objets réseau. Ces objets facilitent la mise en place des connexions et peuvent éliminer les tâches répétitives. Il est par exemple possible de regrouper plusieurs adresses, correspondant à un même département, au sein d'un groupe d'objets réseaux. Ce groupe d'objets réseau peut servir ensuite d'adresse source ou de destination lors d'une connexion.

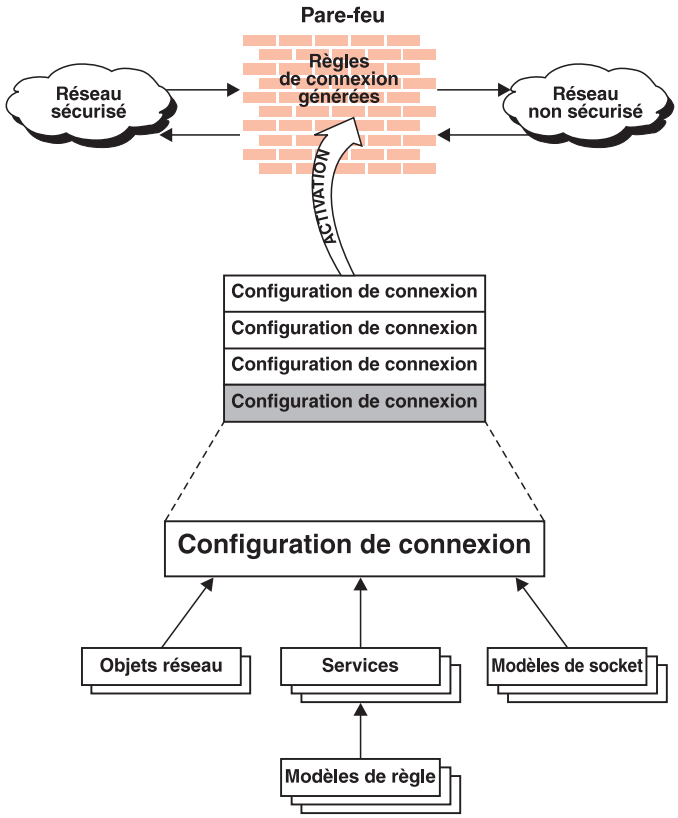

Figure 14. Mise en place des connexions

Connexions établies à l'aide des services prédéfinis

Pour autoriser ou refuser des types de communication entre deux objets réseau ou deux groupes d'objets réseau (les éléments à chaque extrémité du canal de communication), vous devez établir une connexion.

Une fois que vous avez défini vos objets réseau, vous pouvez créer les connexions. Pour cela, sélectionnez un objet ou un groupe d'objets réseau qui sera la source et un autre objet (ou groupe d'objets) qui sera la destination du flux de données qui passe par le pare-feu.

Pour établir une connexion, sélectionnez Contrôle du trafic dans l'arborescence du client de configuration, puis cliquez deux fois sur l'icône du dossier des programmes pour en visualiser le contenu. Sélectionnez l'option **Configuration de connexion**. La boîte de dialogue **Liste des connexions** s'affiche. Sélectionnez **Création** et cliquez sur **Ouverture**. La boîte de dialogue **Ajout d'une connexion**, telle qu'illustrée par la figure 15, à la page 49, apparaît.

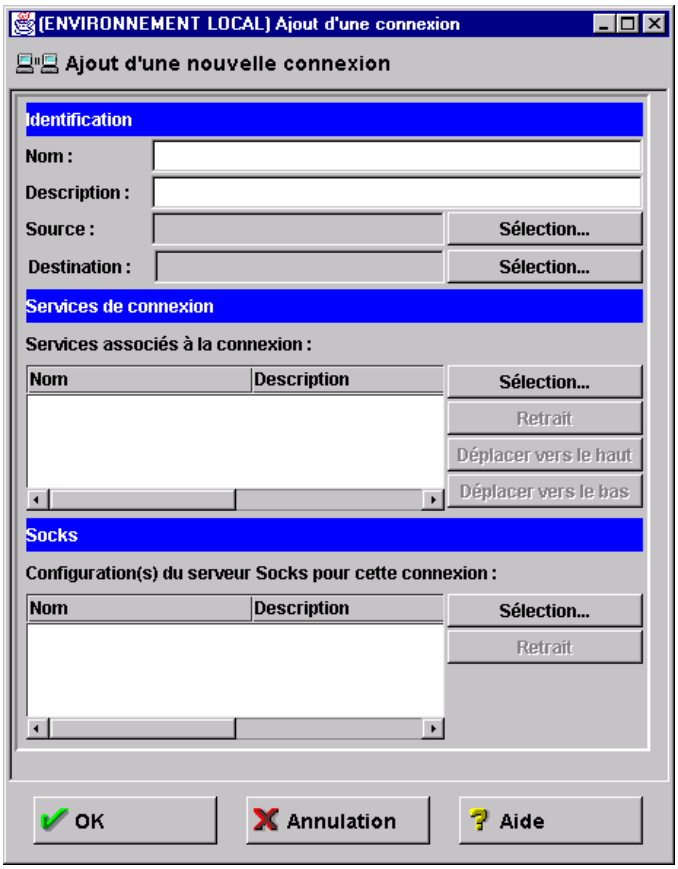

Figure 15. Ajout d'une connexion

1. Attribuez un nom à la connexion.
2. Entrez une description de la connexion.
3. Pour la zone Source, cliquez sur **Sélection** et choisissez un objet réseau dans la liste **Objets réseau**.
4. Pour la zone Destination, cliquez sur **Sélection** et choisissez un objet réseau dans la liste **Objets réseau**.
5. Pour choisir les services de cette connexion, cliquez sur **Sélection** et choisissez le type de trafic que vous souhaitez contrôler entre les deux extrémités de la connexion.
6. Choisissez un ou plusieurs services dans la liste afin d'ajouter le service concerné à la connexion.
7. Vous pouvez réorganiser votre liste en sélectionnant un service et en cliquant sur **Déplacer vers le haut** ou **Déplacer vers le bas**. Reportez-vous à la section «Ordre des connexions», à la page 50.
8. Vous pouvez supprimer un service de votre liste en le sélectionnant et en cliquant sur **Retrait**.
9. Utilisez **Configuration du serveur Socks pour la connexion** puis suivez les étapes 5–7 pour créer des connexions pour Socks.
10. Lorsque vous avez défini toutes les options, cliquez sur **OK**.
11. Activez toutes les connexions. Reportez-vous à la section «Activation des connexions», à la page 50.

Ordre des connexions

La plupart des utilisateurs d'IBM Firewall se servent de moins de 1 000 règles. Plus le nombre de règles est important, plus grand sera l'impact sur les performances.

Lorsqu'un paquet est reçu par une interface réseau en provenance ou en direction du pare-feu, les règles sont appliquées en commençant par le haut de la liste des règles de connexion générées. Lorsque les informations du paquet correspondent exactement à celles de la règle, l'action appropriée (autorisation ou refus) est exécutée. Lorsque le fichier fait l'objet d'une recherche intégrale sans qu'aucune correspondance ne soit trouvée, la requête est automatiquement refusée.

Astuce : En conséquence, nous vous conseillons de placer les connexions les plus spécifiques en début de liste et les connexions les moins spécifiques en fin de liste. Exemple : vous pouvez avoir un Département ABC à l'adresse 1.1.10.X, et au sein de ce département, une machine utilisée comme serveur dont l'adresse est le 1.1.10.7. Si vous souhaitez exclure la machine (1.1.10.7) parce qu'il s'agit d'un serveur qui n'est pas destiné au trafic Telnet, vous devez positionner la connexion `Refuser le protocole Telnet pour le serveur du Dept ABC` avant la connexion `Autoriser le protocole Telnet pour le Dept ABC`. Si vous inversez l'ordre des connexions, la règle de connexion de refus ne sera jamais prise en compte.

Activation des connexions

Remarque : Avant d'activer les connexions, assurez-vous que l'interface sécurisée a été définie.

Sélectionnez **Activation d'une connexion** à partir de l'arborescence de navigation du client de configuration, afin d'effectuer l'une des actions suivantes :

Régénération et activation des règles de connexion Le pare-feu établit les règles de connexion générées à partir de la configuration de connexion et active l'ensemble de règles.

Désactivation des règles de connexion Si vous désactivez les règles, la protection du pare-feu est alors assurée par les règles par défaut.

Affichage des règles de connexion en cours Cette action permet d'afficher l'ensemble de règles de connexion le plus récent. Si vous désactivez ces règles, elles ne seront pas utilisées.

Validation de la génération des règles Cette action permet de valider ou d'invalider les règles que vous avez créées.

Activation de la journalisation des règles de connexion Le pare-feu journalise le trafic sélectionné à l'aide du dispositif de `journalisation du pare-feu`.

Désactivation de la journalisation des règles de connexion Cette action prmet de désactiver la journalisation du pare-feu.

La boîte de dialogue **Activation d'une connexion**, telle qu'illustrée par la figure 16, à la page 51, apparaît.

Figure 16. Activation d'une connexion

Après avoir effectué une sélection, cliquez sur **Exécution**.

Exemple de résultats de journalisation suite à la régénération et l'activation de règles de connexion

Vous trouverez ci-dessous un exemple des résultats de journalisation quand vous régénérez et activez des règles de connexion :

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: Mise à jour automatique des
interfaces de pare-feu le Tue Feb  3 13:46:53 1998.
Feb 03 13:46:55 1998 mr16n18: ICA1032i: Règles de filtrage mises à
jour à 13:46:55 le Feb-03-1998
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 autorisation 0.0.0.0 0.0.0.0 0.0.0
.0 0.0.0.0 udp eq  53 eq 53 les deux local les deux l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 autorisation 0.0.0.0 0.0.0.0 0.0.0
.0 0.0.0.0 udp gt  1023 eq 53 les deux local les deux l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 autorisation 0.0.0.0 0.0.0.0 0.0.0
.0 0.0.0.0 udp eq  53 gt  1023 les deux local les deux l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 autorisation 0.0.0.0 0.0.0.0 0.0.0
.0 0.0.0.0 tcp     gt  1023 eq 25 les deux local les deux l=y f=y t=0 e=aucun
a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 autorisation 0.0.0.0 0.0.0.0 0.0.0
.0 0.0.0.0 tcp/ack eq  25 gt 1023 les deux local les deux l=y f=y t=0 e=aucun
a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 autorisation 9.67.144.49
255.255.255.240  9.67.130.154 255.255.248.0 all any 0 any 0 les deux les deux
les deux l=y f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 autorisation 9.67.130.154
255.255.248.0 9.67.144.49 255.255.255.240 all any 0 any 0 les deux les deux
les deux l=y f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 autorisation 9.67.144.49
255.255.255.240  9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 sécurisé
local entrant l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 autorisation 9.67.131.250
255.255.255.255  9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 sécurisé
local sortant l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 autorisation 9.67.131.250
255.255.255.255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 sécurisé
local sortant l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 autorisation 9.67.144.49
255.255.255.240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 sécurisé
local entrant l=n f=y t=0 e=aucun a=aucun
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 autorisation 9.67.144.49
255.255.255.240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 sécurisé
local entrant l=n f=y t=0 e=aucun a=aucun
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 interdiction 0.0.0.0 0.0.0.0 0.0.0
.0 0.0.0.0 all any 0 any 0 les deux les deux les deux l=y f=y t=0 e=aucun a=aucun
```

Détermination de l'état des règles

Les règles d'IBM Firewall peuvent se trouver dans l'un des états suivants :

1. La configuration n'est pas activée.

   Vous n'avez pas encore utilisé le client de configuration pour activer cette dernière, ou vous avez désactivé la configuration. La configuration se trouve dans cet état lorsque vous installez IBM Firewall pour la première fois et que vous relancez votre système. Cette situation peut provenir également de la désactivation des règles de filtrage. Des filtres par défaut sont en place afin de protéger votre réseau contre les intrusions lors de la première installation du pare-feu.

   Accès au pare-feu :

   - La configuration par défaut des filtres autorise la totalité du trafic entrant et sortant.

2. La configuration est activée mais comporte des erreurs.

   Vous avez activé la configuration. Cependant, elle comporte des erreurs (règles non valides), ou aucun élément n'a été configuré. Les messages d'erreur et les avertissements sont affichés dans la fenêtre des résultats de l'activation.

   Accès au pare-feu :

   - Autorise le trafic entrant local ;
   - Autorise le trafic sortant.

3. La configuration est activée et valide. Notez que certains avertissements peuvent apparaître, notamment pour les doublons de règles de filtrage.

   Vous avez activé la configuration dque vous avez définie en utilisant la partie Contrôle du trafic du client de configuration.

   Remarque : Le fichier de configuration peut être valide et ne contenir aucune règle. Dans ce cas, la règle implicite «refuser tous les accès» est appliquée.

   Accès au pare-feu :

   - Accès déterminé par le fichier de configuration.

     Chaque paquet reçu ou sur le point d'être envoyé par une interface réseau quelconque est examiné ; son contenu est comparé à chacune des règles de l'ensemble des règles de connexion générées. Lorsqu'une correspondance est trouvée, l'action (autorisation ou interdiction d'accès) indiquée par la règle en question est exécutée.

   - Lorsqu'aucune règle ne s'applique au paquet, la règle implicite «Interdiction globale» s'applique et entraîne le rejet du paquet.

Chapitre 9. Exemples de services

Le présent chapitre décrit comment configurer le pare-feu pour qu'il effectue les tâches les plus courantes. Les tâches considérées ici servent uniquement d'exemple, mais leur compréhension vous aidera à configurer votre pare-feu pour pouvoir utiliser tous les services fournis.

Considérations relatives à la planification

Le contrôle du trafic effectué par le pare-feu est organisé en terme de connexions qui définissent les types de communication autorisés ou interdits entre des paires d'extrémités. Il est donc fondamental de planifier les connexions en fonction de ces extrémités.

Comme il est décrit au Chapitre 8, «Gestion des données via le pare-feu», à la page 47, les extrémités d'une connexion sont représentées dans le pare-feu par des objets réseau. Si vous ne l'avez pas déjà fait, nous vous conseillons de remplir les formulaires de planification du réseau (voir le Chapitre 2, «Planification», à la page 7), puis de créer les objets nécessaires à la représentation de votre réseau.

Les exemples présentés dans ce chapitre utilisent les objets réseau suivants :

Interface sécurisée L'interface sécurisée du pare-feu.

Interface non sécurisée
L'interface non sécurisée du pare-feu.

Réseau sécurisé
L'ensemble des adresses accessibles par l'interface sécurisée du pare-feu. Il peut s'agir d'un groupe d'objets réseau contenant plusieurs domaines distincts, chaque domaine étant représenté par son propre objet réseau.

Le monde extérieur Le réseau non sécurisé.

Chaque type de communication souhaité doit être envisagé en terme des deux extrémités qui communiqueront. À ce stade, il vous faut décider si le pare-feu mettra en place ces communications par le biais d'un relais ou s'il les acheminera lui-même.

Si le pare-feu sert de relais, il effectue les actions nécessaires pour le compte de l'utilisateur sécurisé, et le(s) hôte(s) non sécurisé(s) n'ont jamais connaissance de l'existence d'un hôte sécurisé. Si le pare-feu a pour fonction d'acheminer les données, une communication directe est instaurée entre l'hôte sécurisé et l'hôte non sécurisé.

Si vous utilisez le pare-feu comme relais, les extrémités de la communication comporteront le pare-feu, comme illustré par la figure 17, à la page 56.

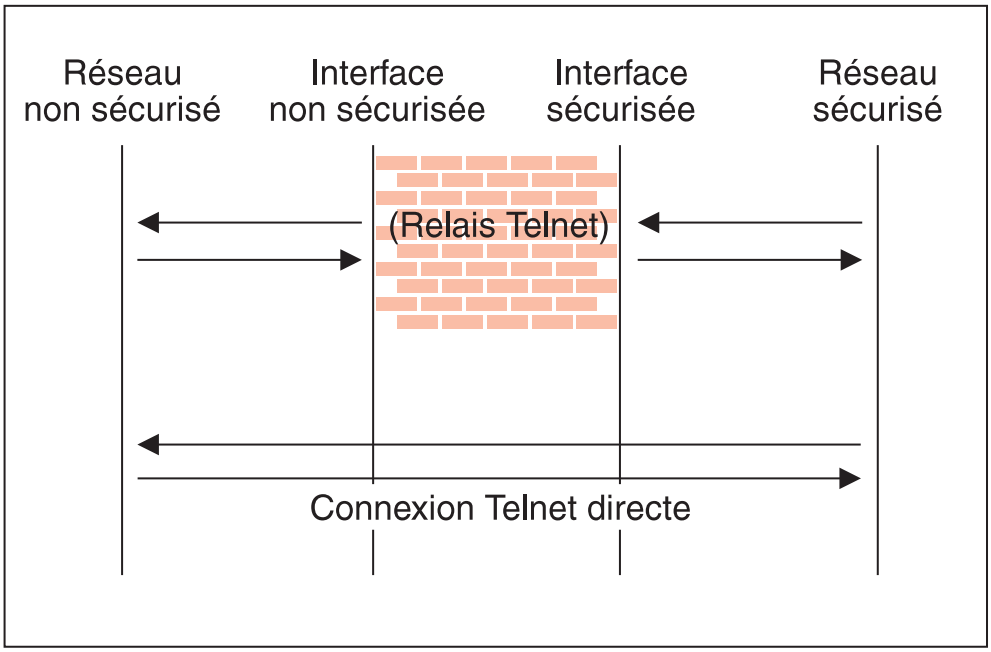

Figure 17. Relais Telnet et connexion Telnet directe

Exemple de relais Telnet

Ce premier exemple décrit une simple connexion sortante à un relais Telnet. Dans ce cas, les utilisateurs qui résident sur le réseau sécurisé sont autorisés à se servir du relais Telnet du pare-feu pour accéder aux services Telnet des hôtes du réseau non sécurisé.

Comme le montre la figure 17, deux connexions sont établies :

1. Le client situé à l'intérieur du réseau sécurisé est connecté au relais Telnet du pare-feu ;
2. Le relais Telnet du pare-feu est connecté à un hôte du réseau non sécurisé et agit pour le compte de l'utilisateur sécurisé.

Pour configurer le contrôle du trafic effectué par le pare-feu, pour ce type de communication, deux connexions doivent être mises en place :

Tableau 1. Relais Telnet

Objet source	**Objet cible**	**Services requis**
Réseau sécurisé	Interface sécurisée	Relais Telnet en sortie 1/2
Interface non sécurisée	Le monde extérieur	Relais Telnet en sortie 2/2

Exemple de connexion Telnet filtrée

Comparez l'exemple ci-dessus avec une simple connexion Telnet filtrée. Dans ce cas, le client situé dans la partie sécurisée est connecté directement à l'hôte de la partie non sécurisée.

Tableau 2. Telnet filtré

Objet source	Objet cible	Services requis
Réseau sécurisé	Le monde extérieur	Telnet direct en sortie

Comme nous l'avons mentionné, cette configuration entraîne une exposition des adresses des clients sécurisés lorsqu'ils se connectent à des hôtes non sécurisés.

Exemple de relais HTTP

La plupart des installations souhaiteront donner l'autorisation de naviguer sur Internet à quelques clients sécurisés. IBM Firewall propose un service HTTP direct en sortie pour permettre l'acheminement des requêtes HTTP et qui fonctionne de la même manière que la connexion Telnet filtrée montrée en exemple. Le pare-feu propose également un relais HTTP.

Le protocole HTTP diffère de Telnet dans le sens où il peut encapsuler d'autres protocoles. La plupart des utilisateurs, même s'ils se contentent de naviguer simplement, auront non seulement besoin de services HTTP mais aussi de services FTP. Pour que toutes les fonctions HTTP soient assurées, il convient également que les protocoles Gopher et WAIS soient autorisés, bien que leur usage soit moins fréquent.

Notez cependant que si ces protocoles supplémentaires sont utilisés, ils sont enveloppés dans le protocole HTTP entre le client et le relais. Dans ce cas, la communication s'apparente au schéma de la figure 18.

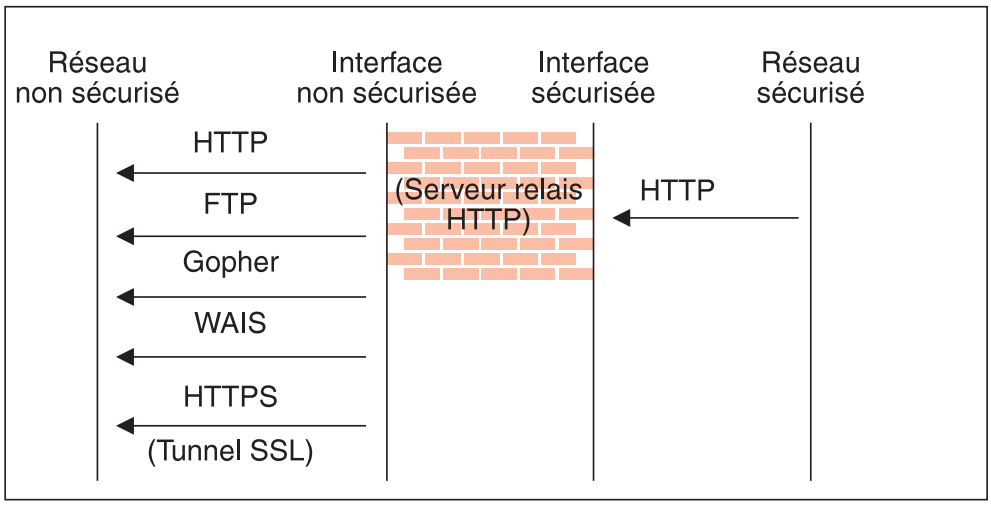

Figure 18. Relais HTTP

Étant donné qu'il existe deux paires d'extrémités de connexion, deux connexions doivent être mises en place.

Tableau 3. Relais HTTP		
Objet source	**Objet cible**	**Services requis**
Réseau sécurisé	Interface sécurisée	Relais HTTP sortant 1/2
Interface non sécurisée	Le monde extérieur	Choisissez parmi • Relais HTTP en sortie 2/2 • Relais FTP en sortie 2/2 • Relais Gopher en sortie 2/2 • Relais WAIS en sortie 2/2 • Relais HTTPS en sortie 2/2

Pour de plus amples informations concernant le relais HTTP, reportez-vous au Chapitre 13, «Configuration des serveurs relais», à la page 91.

Exemple d'utilisation de Socks

Socks implique les mêmes contraintes que le relais HTTP car le démon socks traite un grand nombre de protocoles différents et les encapsule dans un flux de données unique entre le pare-feu et le client. Socks est plus souple que le relais HTTP car il accepte tout protocole orienté TCP ou UDP et il permet de configurer le pare-feu indépendamment des filtres de contrôle des communications.

Compte tenu de cette flexibilité supplémentaire, la configuration de Socks nécessite une troisième connexion en plus de celles qui ont été présentées pour le relais HTTP. Les deux connexions de base permettent l'échange de paquets en provenance et en direction du pare-feu ; la troisième connexion est nécessaire pour indiquer au démon socks de relayer les requêtes à la réception des paquets.

Tableau 4. Socks		
Objet source	**Objet cible**	**Services requis**
Réseau sécurisé	Interface sécurisée	Socks 1/2
Interface non sécurisée	Le monde extérieur	Choisissez parmi • Relais HTTP en sortie 2/2 • Relais FTP en sortie 2/2 • Relais Telnet en sortie 2/2 (Tout autre moitié de service relais dont la prise en charge est souhaitée)
Réseau sécurisé	Le monde extérieur	Dans la fenêtre Configuration de Socks, choisissez... • Autorisation du protocole HTTP avec sockets • Autorisation du protocole FTP avec sockets • Autorisation du protocole Telnet avec sockets

Il va de soi que les clients situés dans votre réseau interne doivent être compatibles Socks et configurés pour utiliser le pare-feu comme serveur Socks.

Pour plus de renseignements concernant le protocole Socks, voir le Chapitre 11, «Configuration du serveur Socks», à la page 71.

Suggestions pour une configuration DNS

Il est rare d'obtenir des communications efficaces en l'absence de résolution DNS. Reportez-vous au Chapitre 6, «Gestion DNS (Service des noms de domaine)», à la page 31 pour des informations détaillées sur la configuration de DNS. N'oubliez pas d'activer l'option "Autorisations des requêtes DNS" dans le panneau Règles de sécurité.

Suggestions pour les clients Socks non sécurisés

La panneau Règles de sécurité contient une case à cocher intitulée **Interdiction des connexions Socks sur l'interface non sécurisée**. Si cette case est cochée, tout paquet adressé au démon Socks en provenance d'une interface non sécurisée sera refusé ; cela renforce considérablement la sécurité de votre pare-feu.

Pour permettre aux clients d'accéder au réseau à partir du réseau non sécurisé, *ne cochez pas* cette case.

Chapitre 10. Personnalisation du contrôle du trafic

Le présent chapitre vous aide à définir les règles et les services de filtrage. Les services constituent un ensemble de règles ou d'instructions qui permettent d'autoriser ou de refuser un type particulier de communication via le pare-feu, par exemple, une session Telnet. Vous pouvez compléter la liste des services en créant des règles au moyen des modèles de règles. Vous pouvez également supprimer certains services. Les services Socks s'appliquent aux connexions utilisant le protocole Socks.

IBM Firewall est fourni avec un ensemble de services par défaut préchargés. Vous pouvez personnaliser les services prédéfinis en fonction de vos besoins particuliers, ou même créer des services.

Création de modèles de règles au moyen du client de configuration

Utilisez la procédure ci-dessous pour ajouter une nouvelle règle à la liste des modèles de règles existants.

1. À partir de l'arborescence de navigation du client de configuration, sélectionnez l'option Contrôle du trafic et cliquez deux fois sur l'icône du dossier. Sélectionnez **Modèles de connexion**, puis **Règles**.
2. Dans la boîte de dialogue **Liste des règles**, cliquez deux fois sur **Création**.

   IBM Firewall affiche la boîte de dialogue **Ajout d'une règle IP** illustrée par la figure 19, afin que vous puissiez définir une règle.

Figure 19. Ajout d'une règle IP

3. Entrez le nom de la règle.
4. Entrez la description de la règle. Cette zone est facultative.
5. Ouvrez le menu déroulant Action et choisissez d'autoriser ou d'interdire l'accès au pare-feu.
6. Ouvrez le menu déroulant Protocole et effectuez votre sélection parmi les options suivantes :

   tous Cette règle s'applique quel que soit le protocole utilisé.

   tcp Cette règle s'applique si le protocole de transmission de paquets est TCP (Transmission Control Protocol).

   tcp/ack Cette règle s'applique si le protocole de transmission de paquets est TCP (Transmission Control Protocol) avec accusé de réception.

   udp Cette règle s'applique si le protocole de transmission de paquets est UDP (User Packet Protocol).

   icmp Cette règle s'applique si le protocole de transmission de paquets est ICMP (Internet Control Message Protocol).

   ospf Cette règle s'applique si le protocole de transmission de paquets est OSPF (Open Shortest Path First). Lorsque le protocole spécifié est ospf, l'opération effectuée sur le port source et la valeur de ce dernier sont utilisées comme type d'enregistrement ospf. Le filtrage peut aussi être effectué sur le type ospf. La valeur de type **toutes** peut être définie et les zones associées au port cible doivent être complétées avec **toutes 0**. Toute autre valeur est ignorée.

   ipip Cette règle s'applique si le protocole de transmission de paquets est IPIP (IP-in-IP Protocol). Lorsque le protocole IPIP est spécifié, les zones associées aux ports doivent être complétées avec **toutes 0**.

   esp Cette règle s'applique si le protocole de transmission de paquets est le protocole de sécurité utilisé par le réseau privé virtuel pour transmettre des paquets IP encapsulés.

   ah Le protocole d'authentification des en-têtes est le protocole de transmission de paquets utilisé par le réseau privé virtuel pour envoyer des paquets IP associés à une clé d'authentification.
7. Le protocole numérique vous permet de définir un protocole au moyen de sa valeur décimale (RFC-1700). Les valeurs admises sont comprises entre 1 et 252. Notez que les zones associées aux ports pour cette règle doivent être complétées avec la valeur 0 (tous les ports) si vous utilisez cette option. Reportez-vous au document RFC-1700 pour obtenir la liste de tous les protocoles. Vous pouvez aussi accéder directement au site de l'IANA (Internet Assigned Numbers Authority) à l'aide d'un navigateur.
8. Les opérandes de l'opération et du numéro de port sont utilisés conjointement. Les opérations source et logique établissent une relation entre le numéro de port (cible ou source) du paquet et les opérandes des numéros de port source et cible. Par exemple, si le port cible du paquet est 20, et que l'opération et le numéro du port cibles sont «ge 15», le paquet satisfait à la règle, car la valeur du port 20 est supérieure ou égale à la valeur du port 15.

Si vous utilisez une opération sur le port source ou cible ayant la valeur **toutes**, le filtre ne tient pas compte du numéro de port car tout port est valide. Dans ce cas, le numéro de port ne peut pas être modifié.

Pour le protocole ICMP, spécifiez un type ICMP au lieu d'indiquer un port source et spécifiez un code ICMP au lieu d'indiquer un port cible. L'opérateur logique spécifié est appliqué au type ou au code et, comme pour les ports, l'opérateur toutes signifie que n'importe quelle valeur de type et/ou de code satisfera à cette règle. Dans ce cas, le numéro de port ne peut pas être modifié.

Les valeurs valides pour l'opération sont :

- Toutes
- Egal à
- Différent de
- Inférieur à
- Supérieur à
- Inférieur ou égal à
- Supérieur ou égal à

Les ports ci-dessous nécessitent des mesures de protection particulières. Les numéros de port doivent être compris entre 1 et 65 535 :

Port	Utilisation
20	Données FTP
21	Contrôle FTP
23	Telnet
25	Messagerie
53	Serveur de noms de domaine
70	Gopher
80	HTTP
111	RPC
161	SNMP
1080	Socks

Voici des exemples de types ICMP et les codes correspondants :

Type	Code et description
0	0 - Réponse ping
8	0 - Requête ping
3	1 - Hôte inaccessible
3	3 - Port inaccessible
5	1 - Redirection vers l'hôte

9. Ouvrez le menu déroulant **Interface** pour sélectionner le type d'interface (adaptateur).

   Les deux Pour les paquets entrant ou sortant via l'interface sécurisée ou non sécurisée.

   Sécurisée Pour les paquets entrant ou sortant via l'interface sécurisée.

   Non sécurisée Pour les paquets entrant ou sortant via l'interface non sécurisée.

   Spécifique À utiliser dans la zone du nom d'interface lors du choix d'une interface, si vous avez donné un nom à l'interface.

10. Lorsque vous sélectionnez un type d'interface spécifique, le nom de cette dernière apparaît dans la zone Nom.
11. Cliquez sur le type de routage désiré :

    les deux Applicable à tous les trafics.

    local Implique que le paquet est traité localement par l'hôte du pare-feu. En d'autres termes :

    - Les paquets locaux entrants sont reçus par l'interface et sont destinés à l'hôte du pare-feu ; ils ne seront donc pas acheminés vers un autre hôte. Leur destination est locale.
    - Les paquets sortants sont transmis à partir de l'interface, et sont émis par l'hôte du pare-feu. Leur origine est locale.

    acheminé Implique que le paquet est acheminé par l'hôte du pare-feu. En d'autres termes :

    - Les paquets locaux entrants sont reçus par l'interface et sont destinés à un autre hôte ; ils ne résident donc plus sur le pare-feu. Leur destination est distante.
    - Les paquets sortants sont transmis à partir de l'interface, et sont émis par un autre hôte. Leur origine est distante.

12. Cliquez sur la destination désirée :

    les deux Pour les paquets entrant ou sortant via l'interface sélectionnée.

    entrant Pour les paquets acheminés à partir du réseau vers l'interface sélectionnée.

    sortant Pour les paquets acheminés à partir de l'interface sélectionnée vers le réseau.

13. Si vous choisissez Oui dans la zone Contrôle de journalisation, tous les paquets satisfaisant à cette règle sont enregistrés dans le `fichier journal du pare-feu` avec le niveau de priorité `Error`. Si ce paramètre n'est pas défini, la valeur par défaut est no.
14. Ouvrez le menu déroulant **Commande de fragmentation** pour sélectionner la commande de fragmentation désirée. Pour que les données d'un paquet IP soient conformes à la définition d'une commande de fragmentation de règle, elles doivent satisfaire aux conditions suivantes :

    Oui Les en-têtes de fragments, les fragments et les paquets non fragmentés satisfont à cette règle. Pour les fragments, les informations sur le port sont ignorées et supposées valables.

Uniquement Seuls les fragments et les en-têtes de fragments satisfont à cette règle. Pour les en-têtes de fragments, les informations sur le port doivent obligatoirement correspondre. Pour les fragments, les informations sur le port sont ignorées.

Non Seuls les paquets non fragmentés satisfont à cette règle. Ce paramètre exclut les en-têtes de fragments et les fragments.

En-têtes Seuls les paquets non fragmentés et les en-têtes de fragments satisfont à cette règle. Ce paramètre exclut les fragments.

Lorsque ce paramètre n'est pas défini, la valeur par défaut des règles d'autorisation et de refus est Oui.

Remarque : Quel que soit le paramétrage de cette commande, les fragments IP avec un décalage de 1 sont supprimés. Cette opération permet d'éliminer une méthode d'attaque connue qui consiste à utiliser des fragments de paquets pour remplacer les indicateurs d'en-têtes TCP.

Pour qu'un en-tête de paquet soit conforme à une règle IP définie, les informations contenues dans le paquet doivent correspondre à tous les paramètres définis dans la règle codée. Pour les fragments de paquets, tous les paramètres servent à vérifier la correspondance, sauf les informations relatives au port.

Les fragments de paquets seront refusés par la dernière règle ajoutée à la fin du fichier de règles, s'ils n'ont pas été autorisés par une règle antérieure codée avec Oui ou Uniquement.

Modification de l'entrée de configuration des règles IP

Pour modifier une règle IP que vous avez créée, procédez comme suit :

1. Cliquez deux fois sur une règle existante dans la **Liste des règles**. La boîte de dialogue **Modification de règle IP** s'affiche.
2. Modifiez les zones appropriées comme indiqué dans le Chapitre 10, «Personnalisation du contrôle du trafic», à la page 61, et cliquez sur **OK** pour valider les changements.

Suppression d'une entrée de configuration de règles

Pour supprimer une règle, sélectionnez-la dans la **Liste des règles** et cliquez sur **Suppression**.

Services prédéfinis

IBM Firewall est fourni avec un ensemble de services par défaut préchargés. Les services correspondent à un ensemble de règles ou d'instructions qui autorisent ou interdisent un type particulier de trafic via le pare-feu, par exemple, une session Telnet. Vous pouvez compléter la liste des services en créant des règles au moyen des modèles de règles.

Les services par défaut ci-dessous sont préchargés :

All non-secure Interdit tout type de trafic via l'interface non sécurisée.

All permit Autorise tout type de trafic (à des fins de débogage uniquement).

All permit, in one direction Autorise tout type de trafic (à des fins de débogage uniquement).

All secure Interdit tout trafic via l'interface sécurisée (en cas de violation des règles de sécurité).

All shutdown Interdit tous les paquets (arrêt ou débogage).

Anti Spoofing Interdit les paquets non sécurisés entrants qui sont associés à une adresse source sécurisée.

Broadcasts Interdit les diffusions de messages vers l'interface non sécurisée.

Config Client non-secure Autorise l'utilisation du client de configuration à partir du réseau non sécurisé.

Config Client secure Autorise l'utilisation du client de configuration à partir du réseau sécurisé.

CU-SeeMe Vidéo CU-SeeMe sur les ports par défaut 7649 et 7648.

DNS queries (RÈGLE DE SÉCURITÉ) Autorise les requêtes DNS.

DNS transfers Autorise les transferts de zones DNS (pour les serveurs de noms secondaires).

Domain Controller Authentication Autorise l'utilisation du contrôleur de domaine pour l'authentification des utilisateurs.

FTP proxy in 1/2 Autorise le trafic FTP en provenance du réseau non sécurisé vers le pare-feu.

FTP proxy in 2/2 Autorise le trafic FTP en provenance du pare-feu vers le réseau sécurisé.

FTP proxy out 1/2 Autorise le trafic FTP en provenance du réseau sécurisé vers le pare-feu.

FTP proxy out 2/2 Autorise le trafic FTP en provenance du pare-feu vers le réseau non sécurisé.

Gopher proxy in 2/2 Autorise les requêtes gopher acheminées à partir du pare-feu vers le réseau sécurisé.

Gopher proxy out 2/2 Autorise les requêtes gopher acheminées à partir du pare-feu vers le réseau non sécurisé.

HTTP deny non-secure Interdit le trafic HTTP vers les interfaces non sécurisées.

HTTP direct out Autorise le trafic HTTP acheminé directement vers le réseau non sécurisé à partir du réseau sécurisé.

HTTP proxy in 2/2 Autorise le trafic HTTP en provenance du pare-feu vers le réseau sécurisé.

HTTP proxy out 1/2 Autorise le trafic HTTP (port 8080) en provenance du réseau sécurisé vers le pare-feu.

HTTP proxy out 2/2 Autorise le trafic HTTP en provenance du pare-feu vers le réseau non sécurisé.

HTTPS direct out Autorise le trafic HTTPS (SSL) en provenance du réseau sécurisé vers le réseau non sécurisé.

HTTPS proxy out 2/2 Autorise le trafic HTTPS (tunnel SSL) en provenance du pare-feu vers le réseau non sécurisé.

IDENTD Autorise l'identification d'utilisateurs avec des protocoles Socks.

Mail (RÈGLE DE SÉCURITÉ) Autorise l'acheminement du courrier via le pare-feu.

NetBT Name Services broadcasts Autorise les diffusions NetBIOS via les services de noms TCP/IP.

Ping Autorise les commandes ping lancées à partir du réseau sécurisé vers n'importe quel système.

SDI authentication Autorise une connexion au serveur SecurID ACE sur le réseau sécurisé.

Socks 1/2 Autorise l'utilisation du protocole Socks pour le trafic acheminé à partir du réseau sécurisé vers le pare-feu.

Socks deny non-secure Interdit le trafic Socks en provenance des adaptateurs non sécurisés.

Socks in 1/2 Autorise l'utilisation du protocole Socks pour le trafic acheminé à partir du réseau non sécurisé vers le pare-feu.

Telnet direct out Autorise le trafic Telnet en provenance du réseau sécurisé vers le réseau non sécurisé.

Telnet proxy in 1/2 Autorise le trafic Telnet en provenance du réseau non sécurisé vers le pare-feu.

Telnet proxy in 2/2 Autorise le trafic Telnet en provenance du pare-feu vers le réseau sécurisé.

Telnet proxy out 1/2 Autorise le trafic Telnet en provenance du réseau sécurisé vers le pare-feu.

Telnet proxy out 2/2 Autorise le trafic Telnet en provenance du pare-feu vers le réseau non sécurisé.

VDOLIVE Direct In Autorise le trafic en provenance du client non sécurisé vers le serveur sécurisé.

Notez que les utilisateurs doivent configurer les propriétés de chaque lecteur pour que seul le port UDP 7001 soit utilisé.

VDOLIVE Direct Out Autorise le trafic en provenance du client sécurisé vers le serveur non sécurisé.

WAIS proxy in 2/2 Autorise les requêtes WAIS (z39.50) acheminées à partir du pare-feu vers le réseau sécurisé.

WAIS proxy out 2/2 Autorise les requêtes WAIS (z39.50) acheminées à partir du pare-feu vers le réseau non sécurisé.

Définition des services

Après avoir défini une ou plusieurs règles, vous devez les ajouter à un service. Sélectionnez l'option Contrôle du trafic à partir de l'arborescence de navigation du client de configuration, puis cliquez deux fois sur Modèles de connexion et sélectionnez Services. La boîte de dialogue Liste des services apparaît à l'écran. Cliquez deux fois sur Création pour afficher la boîte de dialogue Ajout d'un service illustrée par la figure 20.

Figure 20. Ajout d'un service

Création de services au moyen du client de configuration

1. Entrez le nom de service choisi.
2. Entrez une description.
3. La zone **Contrôle de journalisation de substitution** permet de redéfinir les paramètres de contrôle de la journalisation dans les modèles de règles qui ont été sélectionnés pour ce service. À titre d'exemple, si vous définissez un ensemble de modèles de règles dont le paramètre du contrôle de journalisation est généralement défini sur non, vous pouvez redéfinir ce paramètre en choisissant oui pour les besoins de ce service.
   Le paramètre de substitution s'applique à toutes les règles de ce service. Dans la zone **Contrôle de journalisation de substitution**, entrez une des options suivantes :
   - pas de substitution - la fonction de redéfinition est désactivée, les paramètres des règles continuent à s'appliquer

- oui - un enregistrement est créé lorsqu'une correspondance est établie avec une règle de ce service
- non - aucun enregistrement n'est créé lorsqu'une correspondance est établie avec une règle de ce service

Lorsqu'un enregistrement est créé pour une règle de filtrage, les valeurs affichées dans le journal correspondent aux valeurs réelles du paquet IP. La journalisation des règles de filtrage pour lesquelles des correspondances ont été établies peut fournir de précieuses informations sur le contenu des paquets IP examinés par le pare-feu (par exemple, protocole et numéros de ports spécifiés).

4. La zone **Commande de fragmentation de substitution** permet de redéfinir le paramétrage de la commande de fragmentation dans les modèles de règles qui ont été sélectionnés pour ce service. À titre d'exemple, si vous définissez un jeu de modèles de règles dont la commande de fragmentation est généralement paramétrée sur non, vous pouvez redéfinir ce paramètre en choisissant oui pour les besoins de ce service. Le paramètre de substitution s'applique à toutes les règles de ce service. Dans la zone **Commande de fragmentation de substitution**, entrez une des options suivantes :
   - pas de substitution - la fonction de redéfinition est désactivée, les paramètres des règles continuent à s'appliquer
   - oui - correspondance avec n'importe quel paquet IP, par exemple, les paquets non fragmentés, les en-têtes de fragment et les fragments sans en-tête
   - non - correspondance uniquement avec les paquets non fragmentés. Aucune correspondance avec les en-têtes de fragment ou les fragments sans en-tête
   - uniquement - correspondance uniquement avec les en-têtes de fragment et les fragments sans en-tête. Aucune correspondance avec les paquets non fragmentés
   - en-têtes - correspondance uniquement avec les paquets non fragmentés et les en-têtes de fragment. Aucune correspondance avec les fragments sans en-tête
5. Les commandes de date et d'heure permettent d'associer un intervalle de temps à chaque service. Le service sera donc opérationnel uniquement pendant la période spécifiée. Si aucun intervalle de temps n'est associé au service, celui-ci est opérationnel en permanence.

   Contrôle en temps réel

   Sélectionnez cette option pour activer ou désactiver ce service en fonction des heures de début et de fin de journée. Utilisez le format 24 heures. Si cette option n'est pas sélectionnée, le contrôle s'effectuera 24 heures sur 24.

Contrôle par jours Sélectionnez cette option pour activer ou désactiver ce service en fonction d'un calendrier basé sur les jours de la semaine ou les dates. Notez que l'activation ou la désactivation d'un service dépend de la valeur définie dans la zone Action des commandes de dates et heures.

Action des commandes de dates et heures

Choisissez **Activation du service aux périodes spécifiées** pour activer ce service à des heures précises. Ce service est désactivé en dehors des heures définies.

Choisissez **Désactivation de services pendant les périodes spécifiées** pour désactiver ce service à des heures précises. Ce service est activé en dehors des heures définies.

6. Cliquez sur **Sélection** pour choisir les règles qui composent ce service.
7. Le bouton à bascule Flux permet de définir le mode d'affectation des valeurs source et cible de la connexion aux filtres lors de leur enregistrement dans la table des règles.

   ```
   ---> Le sens de gauche à droite indique que les valeurs source et
        cible de la connexion sont inscrites directement dans la règle
        pendant leur enregistrement dans la table des règles.

   <--- Le sens de droite à gauche indique que les valeurs source et
        cible de la connexion sont inversées pendant leur
        enregistrement dans la table des règles.
   ```

8. Lors de la réception d'un paquet, IBM Firewall compare les informations qu'il contient aux règles figurant dans le fichier de configuration de règles, en commençant par le début du fichier. Le pare-feu arrête la recherche dès qu'il trouve la première correspondance. Il exécute alors l'action spécifiée par la règle.

   Une fois que vous avez ajouté un ensemble de règles dans le service, vous pouvez modifier leur ordre. Sélectionnez une règle dans la liste des **objets règle** et cliquez sur le bouton **Déplacer vers le haut** ou **Déplacer vers le bas** afin de replacer la règle à l'endroit souhaité. Vous pouvez également cliquer sur **Retrait** pour supprimer une règle. Le client de configuration affiche la liste de règles régénérée. Cliquez sur **OK** pour sauvegarder les modifications.

Chapitre 11. Configuration du serveur Socks

Socks est une norme Internet pour les passerelles au niveau des connexions.

Le serveur Socks permet d'effectuer la conversion d'adresses si votre application utilise TCP, comme les navigateurs Web, FTP, ou les applications Telnet. Socks vous aide à accéder à Internet, tout en masquant vos adresses IP internes.

Pour les requêtes sortantes, émises par un client sécurisé vers un serveur non sécurisé, le serveur Socks remplit une mission identique à celle d'un serveur relais : il contrôle la session au niveau du pare-feu et met en œuvre une barrière sécurisée à partir de laquelle les utilisateurs peuvent accéder au réseau extérieur non sécurisé, tout en protégeant l'adressage et la structure du réseau interne. Le serveur Socks présente l'avantage d'être simple d'utilisation et ne requiert qu'un travail d'administration limité.

Le serveur Socks peut intercepter toutes les requêtes TCP sortantes qui circulent entre le réseau et Internet. Il fournit une interface de programmation d'application à distance, de sorte que les fonctions exécutées par les programmes d'un client dans des domaines sécurisés sont acheminées vers les postes du pare-feu via des serveurs sécurisés, tout en masquant l'adresse IP du client. L'accès est contrôlé par des filtres qui sont associés aux règles du serveur Socks.

Le serveur Socks est similaire au serveur relais. Cependant, alors que le serveur relais exécute la fonction TCP/IP au niveau du pare-feu, le serveur Socks identifie simplement l'utilisateur et redirige la fonction via le pare-feu. La fonction TCP/IP réelle est mise en œuvre au niveau du poste de travail client, et non sur le pare-feu. Ce mécanisme permet de diminuer la charge de travail au niveau du pare-feu. Les utilisateurs faisant partie d'un réseau sécurisé peuvent faire appel aux nombreux produits TCP/IP qui supportent la norme Socks. La figure 21 illustre le serveur Socks interceptant une requête HTTP émise par un client du réseau sécurisé.

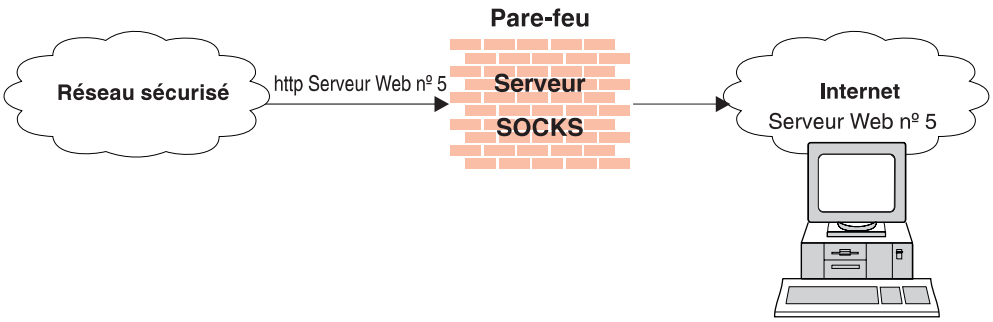

Figure 21. Serveur Socks

Le serveur Socks masque les adresses IP internes, qui sont invisibles par le monde extérieur.

IBM Firewall inclut le protocole Socks version 5 pour permettre aux clients d'un réseau sécurisé de s'authentifier avant d'accéder aux applications du réseau non sécurisé. Il assure également l'authentification des serveurs relais génériques et sert de relais dans le cadre des communications de données audio et vidéo.

Le démon Socks s'exécute comme un service Windows NT et démarre automatiquement en même temps que le système. En outre, un agent de surveillance permet de contrôler l'activité du serveur. Vous pouvez démarrer l'agent manuellement.

IBM Firewall permet de procéder à une migration en douceur en proposant trois profils d'authentification ; ainsi, les clients peuvent continuer à utiliser les protocoles client Socks version 4 installés lors de la mise en œuvre des protocoles client Socks version 5.

1. Le profil le plus souple n'active pas l'authentification en sortie et autorise tout utilisateur utilisant un protocole client Socks version 4 ou version 5, à se connecter. Dans ce cas, les connexions entrantes sont refusées.
2. Le profil de migration permet aux utilisateurs du protocole Socks version 4 de communiquer sans s'authentifier, mais exige que les utilisateurs du protocole Socks version 5 s'authentifient. Les connexions entrantes via le protocole Socks version 4 sont refusées et les connexions entrantes du protocole Socks version 5 doivent s'authentifier. Il s'agit du profil par défaut.
3. Le profil offrant le plus haut niveau de sécurité oblige tous les utilisateurs à se servir du protocole Socks version 5 et à s'authentifier.

Lorsque le pare-feu est installé, le serveur Socks est activé, mais le fichier de configuration de Socks ne contient aucune règle. Pour permettre aux clients Socks d'utiliser le serveur Socks, vous devez configurer le serveur à l'aide du client de configuration. Un exemple de configuration d'un service Socks est décrit dans la section «Exemple d'utilisation de Socks», à la page 58.

Protocoles pris en charge par le serveur Socks version 5

Le serveur Socks version 5 prend en charge, entre autres, les protocoles TCP et UDP suivants :

- Archie ;
- Finger ;
- FTP ;
- Gopher ;
- HTTP ;
- HTTP Proxy ;
- News ;
- SNMP ;
- Telnet ;
- TFTP ;
- RealAudio ;
- RealPlayer ;
- Whois ;
- X-Windows.

En outre, la plupart des clients de messagerie sont supportés. Le niveau de support de ces protocoles varie en fonction de leur mise en œuvre.

Configuration du serveur Socks à l'aide du client de configuration

Modèles Socks sont des règles de contrôle de sécurité mises en œuvre via le serveur Socks. Les modèles Socks permettent de personnaliser, d'ajouter, de copier ou de supprimer les modèles existants. Ces modèles Socks, à leur tour, peuvent être utilisés dans les définitions des connexions sur le pare-feu, de la même manière que les modèles de règles.

Ajout d'une règle Socks

Pour ajouter une règle au fichier de configuration de Socks à l'aide d'un modèle Socks fourni par le client de configuration, sélectionnez Contrôle du trafic à partir de l'arborescence de navigation du client de configuration. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Sélectionnez Modèles de connexion. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Sélectionnez **Socks**. La boîte de dialogue **Socks** s'ouvre.

1. Cliquez deux fois sur **Création** pour ajouter un modèle Socks.

   La boîte de dialogue **Ajout d'une règle Socks** s'ouvre, comme illustré dans la figure 22.

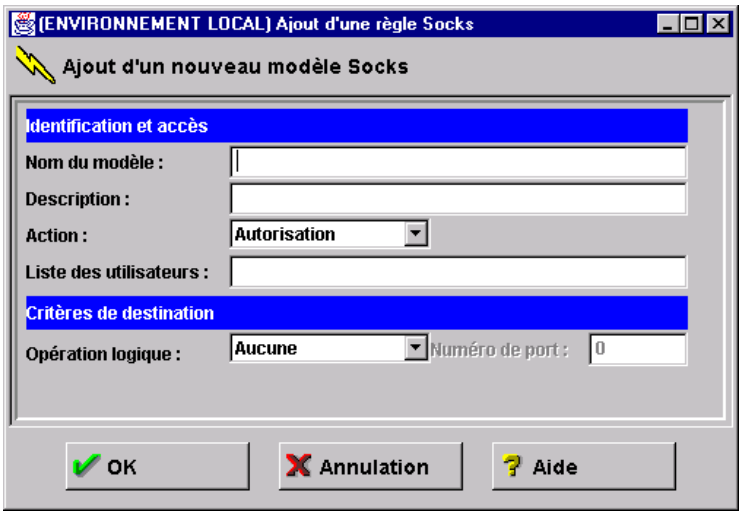

Figure 22. Ajout d'une règle Socks

2. Entrez le nom de l'entrée Socks dans la zone **Nom du modèle**. Ce nom doit être unique et ne doit pas comporter de symbole (|), d'apostrophe (') ou de guillemets (") car ces caractères sont utilisés comme délimiteurs de fichiers. Ces caractères altèrent les données.
3. Entrez une description.
4. Ouvrez le menu déroulant et choisissez d'autoriser ou de refuser l'accès à un système cible à partir d'un système source.

Lorsqu'un datagramme parvient au serveur Socks, ce dernier compare les spécifications du datagramme avec chacune des règles du fichier de configuration, en partant de la première, jusqu'à ce qu'il trouve une règle correspondant parfaitement. Le programme arrête alors la recherche et exécute l'opération appropriée (permission ou interdiction d'accès) sur cette règle. En l'absence de correspondance parfaite, l'accès est automatiquement refusé.

5. Dans la zone **Liste des utilisateurs**, vous pouvez entrer un ID utilisateur ou une liste d'ID utilisateur. Si vous entrez une liste, séparez chacun des éléments par une virgule. N'utilisez pas d'espaces, de tabulations, le symbole (|) ou les guillemets (") dans la liste des utilisateurs.
   - La liste des utilisateurs est limitée à 396 caractères.
   - Les ID utilisateur doivent correspondre à des identificateurs du système hôte source, et non de l'hôte cible, ni de l'hôte du serveur Socks.
   - Un ID utilisateur peut comprendre entre 1 et 8 caractères :
     - a à z
     - A à Z
     - 0 à 9
     - _ (trait de soulignement)
6. Un ID utilisateur ne doit contenir ni le symbole (|), ni le symbole (").
7. Si vous utilisez des noms de fichier, ils doivent être complets (le signe "/" doit les précéder pour qu'ils ne soient pas interprétés comme des ID utilisateur). Chaque fichier peut contenir une liste d'ID utilisateur, avec un ou plusieurs ID par ligne séparés par des virgules. Un fichier peut aussi contenir des commentaires, ces derniers étant délimités par le caractère #. Il est également possible d'insérer des lignes ne contenant que des commentaires, celles-ci devant commencer par le caractère #. Chaque ligne du fichier peut comporter jusqu'à 1023 caractères et doit se terminer par un retour chariot.
8. Dans la zone **Opération logique**, entrez l'opérateur permettant d'exécuter l'opération logique souhaitée sur le numéro de port :

   eq Égal à
   neq Différent de
   lt Inférieur à
   gt Supérieur à
   le Inférieur ou égal à
   ge Supérieur ou égal à

   Lorsqu'il est utilisé avec le numéro de port, l'opérateur logique établit un lien qui doit être respecté. Par exemple, si vous entrez l'opérateur gt et le numéro de port 23, la règle appelée exigera que le numéro de port soit supérieur à 23.
9. Entrez un numéro dans la zone **Numéro de port**. Le numéro de port est utilisé conjointement avec l'opérateur pour établir la condition de relation à satisfaire. Par exemple, si vous entrez l'opérateur gt et le numéro de port 23, la règle appelée exigera que le numéro de port soit supérieur à 23. Si l'opération et le numéro de port sont omis, la règle s'applique à tous les numéros de ports de destination.

La boîte de dialogue **Ajout d'une règle Socks** permet d'autoriser ou de refuser l'accès au pare-feu à des hôtes du réseau, selon l'adresse IP.

Modification d'une règle Socks

1. Cliquez deux fois sur une entrée dans la boîte de dialogue **Socks**.

   La boîte de dialogue **Modification d'une règle Socks** s'ouvre.

2. Modifiez les zones appropriées comme indiqué dans la section «Ajout d'une règle Socks», à la page 73 et cliquez sur **OK**.

Suppression d'une règle Socks

Sélectionnez une entrée dans la boîte de dialogue **Socks** et cliquez sur **Suppression**. Le système vous demande de confirmer la suppression de la règle Socks. Cliquez sur **OK** pour supprimer la règle.

Activation des règles de connexion

Outre les règles de filtrage, vous devez activer des règles Socks. Cliquez sur **Activation d'une connexion** dans l'arborescence de navigation du client de configuration, sélectionnez **Régénération et activation des règles de connexion**, puis cliquez sur **Exécution**.

Le pare-feu copie les règles contenues dans le fichier de configuration de Socks dans les règles du pare-feu, puis active ces règles. Lorsque les règles sont activées, les nouvelles règles sont enregistrées dans le fichier journal du pare-feu.

Exemple de résultat de journalisation pour Socks

Extrait du journal d'activité de Socks.

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Démarrage du serveur Sockd
Feb 03 13:47:31 1998 mr16n18: ICA3010i: Démarrage de la session
Feb 03 13:47:31 1998 mr16n18: ICA3011i: Démarrage de la session
Feb 03 13:49:15 1998 mr16n18: ICA3007i: Unités d'exécution trop nombreuses
Feb 03 13:58:31 1998 mr16n18: ICA3015i: Arrêt de la session
```

Considérations liées au client sur l'utilisation du serveur Socks

La majorité des navigateurs web est reconnue par Socks et vous pouvez vous procurer des piles compatibles Socks pour la plupart des plates-formes. Des clients compatibles Socks utilisés pour d'autres applications TCP/IP sont disponibles sur le marché. Pour un client spécifique à Socks, consultez la documentation de ce client. Pour de plus amples informations, consultez les sites web suivants :

http://www.raleigh.ibm.com/sng/sng-socks.html
http://www.socks.nec.com

Chaînage de serveurs Socks

Le chaînage de serveurs Socks est une fonction grâce à laquelle un serveur Socks peut résider derrière au autre serveur Socks tout en permettant l'accès au réseau situé au-delà du serveur Socks le plus à l'extérieur. Cette fonction s'avère très utile dans un scénario intranet.

Pour définir un chaînage de serveurs socks avec le serveur Socks, modifiez le fichier `socks5.header.cfg` résidant dans le sous-répertoire `config` du pare-feu en y ajoutant les instructions suivantes :

- Une instruction *no proxy*, pour indiquer le ou les sous-réseaux auxquels le pare-feu a directement accès.
- Une instruction *socks4*, pour indiquer le ou les sous-réseaux accessibles via un serveur Socks version 4.
- Une instruction *socks5*, pour indiquer le ou les sous-réseaux accessibles via un serveur Socks version 5.

Dans l'exemple suivant, le département Recherche dispose d'un petit réseau privé appelé *q.private.com*, situé derrière leur propre pare-feu. Le sous-réseau du département Recherche est 10.007.007.0/255.255.255.0. Le réseau privé de la société, *private.com*, inclut le réseau 10.0.0.0/255.0.0.0 tout entier. Le serveur Socks version 4 de la société, *socks.private.com*, fournit l'accès à Internet.

Ajoutez les deux lignes suivantes dans le fichier `socks5.header.cfg` du serveur Socks *socks.q.private.com* du département Recherche.

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

Enfin, ajoutez une connexion Contrôle du trafic pour permettre à *socks.q.private.com* de communiquer avec *socks.private.com*. Ceci a peut être déjà été effectué par un service plus général. Ajoutez une connexion dont la source est l'interface non sécurisée du pare-feu *q.private.com*, dont la destination est *socks.private.com* et qui inclut le service de *chaînage des serveurs relais Socks*. Réactivez ensuite les règles de contrôle du trafic.

Chapitre 12. Administration des utilisateurs sur le pare-feu

Le présent chapitre décrit les tâches administratives qui doivent être effectuées chaque jour sur IBM Firewall. Il s'agit notamment des opérations suivantes :

- Ajout d'utilisateurs sur IBM Firewall afin qu'ils puissent accéder aux hôtes situés hors de votre réseau sécurisé ;
- Modification des attributs des utilisateurs accédant au pare-feu ;
- Suppression des utilisateurs n'ayant plus besoin d'accéder aux systèmes externes à votre réseau ;

Vous ne devez pas éditer directement les fichiers de configuration ; si vous les éditez, les attributs des utilisateurs d'IBM Firewall ne seront pas définis correctement. Exécutez toutes les tâches d'administration d'IBM Firewall à l'aide de la ligne de commande ou des boîtes de dialogue du client de configuration.

Ajout d'un utilisateur sur IBM Firewall

IBM Firewall définit trois types d'utilisateurs et enregistre les informations correspondantes dans deux bases de données d'utilisateurs.

Types d'utilisateurs

IBM Firewall classe les utilisateurs dans trois catégories :

Utilisateurs relais Ces utilisateurs font appel aux services du pare-feu, tels que le service relais HTTP, pour accéder aux sites Web d'Internet à partir d'un réseau d'entreprise. Ils peuvent utiliser les services via le pare-feu, mais n'ont pas accès au système pare-feu proprement dit, et ne peuvent pas s'y connecter localement.

Administrateurs du pare-feu

Ces utilisateurs peuvent faire appel aux services relais du pare-feu et ont également la possibilité de le configurer en s'y connectant à partir d'un hôte distant et en utilisant le client de configuration. Comme les utilisateurs relais, les administrateurs du pare-feu ne peuvent pas se connecter localement au pare-feu.

Les administrateurs du pare-feu peuvent créer et modifier des définitions d'utilisateurs relais. En revanche, ils ne peuvent pas créer ni modifier les définitions d'autres administrateurs.

Administrateurs principaux du pare-feu

Ces utilisateurs remplissent les mêmes fonctions que les administrateurs du pare-feu. Ils peuvent également se connecter localement à la machine pare-feu. Les administrateurs principaux peuvent créer et modifier les définitions d'autres administrateurs du pare-feu.

Types de bases de données

Il existe deux types de bases de données d'utilisateurs.

Base de données d'utilisateurs du pare-feu

Cette base de données contient les attributs de pare-feu associés à chaque utilisateur relais et à chaque administrateur. Il s'agit notamment du mot de passe défini pour l'utilisateur sur le pare-feu et des règles correspondantes, ainsi que des méthodes permettant d'authentifier l'utilisateur pour chaque service.

Si l'utilisateur relais n'est pas défini dans la base de données d'utilisateurs du pare-feu et qu'il tente de faire appel aux services relais, l'enregistrement utilisateur par défaut, `fwdfusr`, sera employé pour définir les attributs et les méthodes d'authentification servant à le valider.

Les administrateurs principaux du pare-feu ne peuvent pas être définis dans la base de données d'utilisateurs. Utilisez l'enregistrement par défaut associé aux administrateurs du pare-feu, `fwdfadm`, pour définir les attributs des administrateurs.

Si les administrateurs du pare-feu sont également définis dans la base de données d'utilisateurs Windows NT, leur mot de passe de connexion à NT sera employé lorsqu'ils font appel aux services nécessitant une authentification au moyen de ce mot de passe. La même remarque s'applique aux utilisateurs relais.

Base de données d'utilisateurs Windows NT

Cette base de données contient les mots de passe de connexion à NT attribués aux utilisateurs. En général, il n'est pas nécessaire de définir les utilisateurs relais dans la base de données d'utilisateurs NT sauf s'ils doivent être authentifiés au moyen de leur mot de passe de connexion à NT.

Si d'autres méthodes sont employées pour authentifier les utilisateurs relais, ces derniers ne doivent pas nécessairement être définis dans la

base de données d'utilisateurs Windows NT.

Les administrateurs principaux du pare-feu sont comparables à des utilisateurs Windows NT qui appartiennent à un groupe d'administrateurs NT et doivent être définis dans la base de données d'utilisateurs Windows NT.

Ajout d'un utilisateur au moyen du client de configuration

En ajoutant un utilisateur sur IBM Firewall, vous lui permettez d'accéder au réseau externe.

1. À partir de l'arborescence de navigation du client de configuration, sélectionnez l'option Utilisateurs. La boîte de dialogue **Administration des utilisateurs** s'affiche.
2. Sélectionnez **Création** dans la boîte de dialogue **Administration des utilisateurs** et cliquez sur **Ouverture**. La boîte de dialogue **Ajout d'un utilisateur** illustrée par la figure 23, s'affiche.

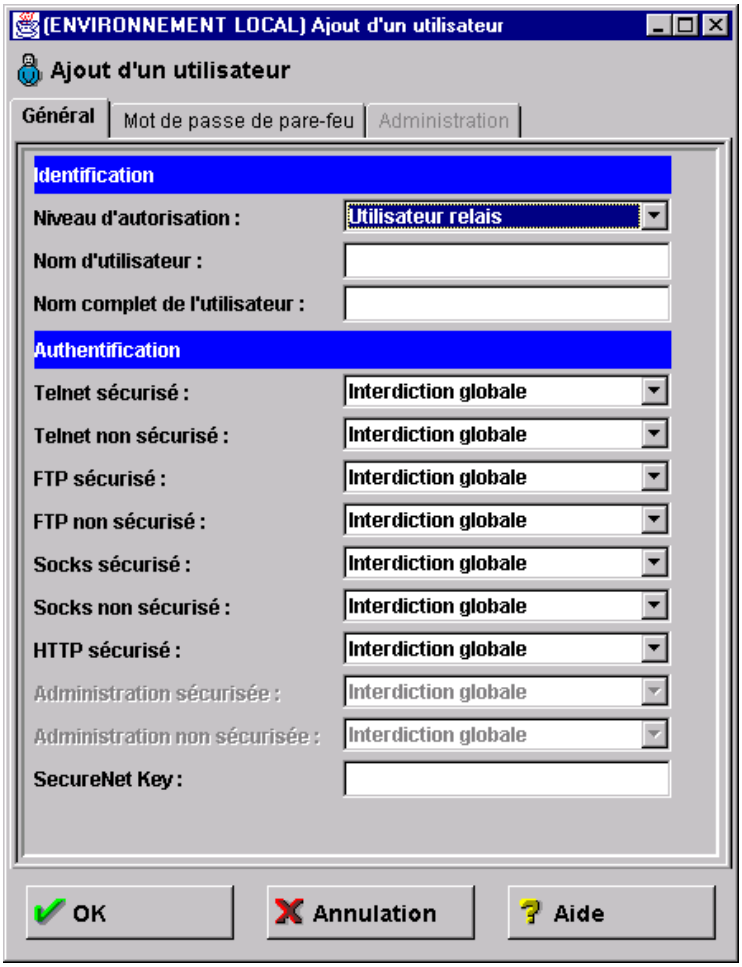

Figure 23. Ajout d'un utilisateur

3. Entrez les informations suivantes :

Niveau d'autorisation

Cet attribut définit le niveau d'autorisation attribué à l'utilisateur. Ouvrez le menu déroulant **Niveau d'autorisation** pour sélectionner le type d'utilisateur.

Utilisateur relais
L'utilisateur défini peut accéder au serveur Socks et au serveur relais. Il ne dispose d'aucun droit d'administration. Il s'agit de l'option par défaut.

Administrateur du pare-feu
L'administrateur dispose de tous les attributs d'un utilisateur ; il peut également se connecter au pare-feu et exécuter des tâches administratives. Il est doté d'attributs supplémentaires définissant le type de fonctions administratives qu'il est autorisé à exécuter. Un administrateur peut créer des utilisateurs, mais pas d'autres administrateurs. Il ne peut pas se connecter localement à la machine pare-feu. Il doit accéder au serveur de configuration à partir d'un système distant.

Administrateur principal du pare-feu
L'administrateur principal est autorisé à se connecter localement à la machine pare-feu. Il a accès à toutes les fonctions administratives, sans aucune restriction. Il peut créer d'autres administrateurs du pare-feu, à l'exception des administrateurs principaux.

Pour définir l'administrateur principal du pare-feu, créez un utilisateur dans la base de données NT et ajoutez-le au groupe d'administrateurs NT. Modifiez l'enregistrement `fwdfadm` pour spécifier les attributs de l'administrateur principal.

Nom d'utilisateur

Cet attribut définit le nom de l'utilisateur. Ce nom d'utilisateur est utilisé pour la connexion au serveur Telnet ou FTP sur IBM Firewall. Il ne s'agit pas obligatoirement du nom d'hôte ou du nom d'utilisateur TCP/IP.

Un nom d'utilisateur peut comporter entre 1 et 20 caractères, parmi les suivants :

a à z
A à Z

0 à 9
_ (trait de soulignement)

Les noms d'utilisateurs peuvent être entrés indifféremment en minuscules ou en majuscules.

Le pare-feu est fourni avec deux utilisateurs préinstallés.

a. Utilisateur par défaut ou `fwdfuser`. Lorsqu'un utilisateur n'est pas défini dans la base de données du pare-feu, `fwdfuser` sert à déterminer ses attributs, et notamment les méthodes employées pour l'authentifier.

   Lorsque `fwdfuser` est créé pendant l'installation, toutes les méthodes d'authentification ont la valeur Interdiction globale. Les droits accordés à `fwdfuser` déterminent la façon dont le pare-feu va traiter les noms d'utilisateurs non définis.

   En utilisant le client de configuration ou la ligne de commande, l'administrateur peut afficher `fwdfuser` ou modifier la méthode d'authentification. Toutefois, `fwdfuser` ne peut pas être supprimé et doit toujours être présent sur le pare-feu. En outre, le mot de passe associé au pare-feu et SNK ne sont pas des types d'authentification valides pour `fwdfuser`. Pour de plus amples informations, reportez-vous au *guide de référence d'IBM eNetwork Firewall.*

b. Administrateur principal du pare-feu ou `fwdfadm`. fwdfadm définit les attributs de pare-feu associés à tous les administrateurs principaux. Cet enregistrement sert à définir les méthodes utilisées pour authentifier les administrateurs principaux car ceux-ci n'ont pas d'entrée utilisateur dans la base de données du pare-feu.

   Toutes les méthodes d'authentification associées à `fwdfadm` sont affectées de la valeur *Interdiction globale* lors de l'installation, à l'exception des méthodes sécurisées et non sécurisées qui sont affectées de la valeur Mot de passe de connexion NT. Les administrateurs principaux du pare-feu peuvent visualiser et modifier cette entrée, mais ils ne peuvent pas la supprimer. En outre, le mot de passe associé au pare-feu et SNK ne sont pas des types d'authentification valides pour `fwdfadm`.

Nom complet de l'utilisateur
Cette information définit l'utilisateur.

Les zones ci-dessous font référence aux méthodes d'authentification. Ouvrez le menu déroulant pour sélectionner une méthode d'authentification dans la liste. Les options sont décrites dans la section «Méthodes d'authentification des utilisateurs», à la page 83.

Telnet sécurisé Indique si l'utilisateur doit être authentifié d'une manière ou d'une autre lorsqu'il se connecte à partir du réseau sécurisé.

Telnet non sécurisé
Indique si l'utilisateur doit être authentifié d'une manière ou d'une autre lorsqu'il se connecte à partir du réseau non sécurisé.

FTP sécurisé Définit le niveau d'authentification dont l'utilisateur a besoin pour accéder au pare-feu via le protocole FTP à partir du réseau sécurisé.

FTP non sécurisé Définit le niveau d'authentification dont l'utilisateur a besoin pour accéder au pare-feu via le protocole FTP à partir du réseau non sécurisé.

Socks sécurisé Indique la méthode d'authentification Socks version 5 utilisée pour les connexions des clients Socks établies depuis la partie sécurisée du pare-feu. Ouvrez le menu déroulant afin de sélectionner l'option désirée. Ces options sont décrites dans la section «Méthodes d'authentification des utilisateurs», à la page 83.

Socks non sécurisé
Indique la méthode d'authentification Socks version 5 utilisée pour les connexions des clients Socks établies depuis la partie non sécurisée du pare-feu. Ouvrez le menu déroulant afin de sélectionner l'option désirée. Ces options sont décrites dans la section «Méthodes d'authentification des utilisateurs», à la page 83.

HTTP sécurisé Spécifie une authentification du type ID utilisateur/mot de passe pour les requêtes sortantes des relais HTTP. Ouvrez le menu déroulant afin de sélectionner l'option désirée. Ces options sont décrites dans la section «Méthodes d'authentification des utilisateurs», à la page 83.

Le navigateur vous demande d'entrer un ID utilisateur et un mot de passe. Par conséquent, si vous utilisez SDI, indiquez un code d'accès (PASSCODE) à l'invite correspondante.

La méthode d'authentification fournie par l'utilisateur doit tenir compte du fait que Socks/mot de passe ne supporte pas les boîtes de dialogue interactives.

Administration sécurisée
Définit la méthode d'authentification que vous devez utiliser pour vous connecter à partir du client de configuration via une interface sécurisée. Notez que lors d'une connexion locale (définie comme telle dans le panneau de connexion), vous vous trouvez toujours dans un environnement sécurisé : il s'agit par conséquent de la méthode d'authentification utilisée.

Administration non sécurisée

Définit la méthode d'authentification que vous devez utiliser pour vous connecter à partir du client de configuration via une interface non sécurisée.

SecureNet Key

Définit la chaîne de caractères qui doit être entrée par un utilisateur distant disposant d'une carte AssureNet Pathways SecureNet Key. Indiquez le code également utilisé pour initialiser la carte. Pour obtenir des instructions concernant la sélection et l'installation du code, consultez la documentation relative à SecureNet Key.

Remarques :

a. Cette zone n'est pas utilisée avec la carte SecurID.

b. Pour chaque utilisateur, vous devez créer une clé aléatoire unique.

c. Lorsque vous attribuez la clé à la carte SecureNet Key, vous devez suivre la procédure d'installation AssureNet Pathways et sélectionner le **Mode 5**.

Pour de plus amples informations, reportez-vous à la section «Méthodes d'authentification», à la page 88.

Méthodes d'authentification des utilisateurs

Les méthodes d'authentification suivantes sont disponibles :

Interdiction globale L'accès est refusé à l'utilisateur.

Autorisation globale

Aucune authentification n'est nécessaire.

Mot de passe de connexion à NT

Le mot de passe de connexion à NT garantit un niveau de sécurité moins élevé que le mot de passe associé au pare-feu. Toutefois, si des utilisateurs sont déjà définis dans un domaine Windows NT, vous pouvez employer le mot de passe de connexion à Windows NT pour éviter que plusieurs mots de passe soient attribués aux utilisateurs.

Si vous choisissez cette méthode d'authentification, votre ID utilisateur et votre mot de passe seront vérifiés par rapport à la base de données locale des utilisateurs Windows NT. Si le pare-feu est configuré pour établir des relations de confiance avec d'autres serveurs NT, les définitions d'utilisateurs seront recherchées sur ces derniers.

Avant d'établir des relations de confiance entre le pare-feu Windows NT et les serveurs NT sécurisés, une connexion doit être définie pour permettre le trafic TCP/IP entre ces différents systèmes.

Définissez cette connexion en utilisant les services prédéfinis suivants :

1. Domain Controller Authentication - ce service permet d'utiliser le contrôleur de domaine pour l'authentification des utilisateurs.

2. NetBT Name Services broadcasts - ce service autorise les diffusions NetBIOS via les services de noms TCP/IP.

Faites appel aux utilitaires de configuration NT pour définir les relations de confiance.

SecureNet Key L'authentification s'effectue à l'aide d'une clé AssureNet Pathways SecureNet Key.

Dans la zone SecureNet Key, entrez le code également utilisé pour initialiser la carte SecureNet Key.

Remarques :

1. Pour chaque utilisateur, vous devez créer une clé aléatoire unique.
2. Chacune des 8 valeurs octales composant la clé doit être comprise entre 1 et 377.
3. Lorsque vous attribuez la clé à la carte SecureNet Key, vous devez suivre la procédure d'installation AssureNet Pathways et sélectionner le **Mode 5**.

Pour de plus amples informations, reportez-vous à la section «Méthodes d'authentification», à la page 88.

Carte SecurID L'authentification s'effectue à l'aide d'une carte de sécurité Security Dynamics SecurID ou d'une carte d'identification personnelle. *N'utilisez pas* la zone SecureNet Key. Le numéro d'identification (PIN) doit être défini pour que cette méthode d'authentification puisse être utilisée avec IBM Firewall.

Pour le protocole FTP, SecurID n'assure pas la prise en charge des nouveaux modes d'identification par PIN et de retour d'authentification.

Pour de plus amples informations, reportez-vous à la section «Méthodes d'authentification», à la page 88.

Méthode d'authentification fournie par l'utilisateur 1, 2 et 3

La méthode d'authentification est fournie par l'utilisateur. Vous pouvez définir au maximum trois méthodes de ce type sur le pare-feu. Pour de plus amples informations sur la création et la compilation d'un sous-programme pour cette méthode d'authentification, reportez-vous au *guide de référence d'IBM eNetwork Firewall*.

Mot de passe de pare-feu

L'utilisateur doit entrer un mot de passe correct. Lorsque ce panneau est complété, IBM Firewall vous invite à définir un mot de passe pour le nouvel utilisateur.

Le mot de passe associé au pare-feu offrant un plus haut niveau de sécurité que le mot de passe de connexion à Windows NT, cette méthode est recommandée pour la définition des mots de passe.

Changement du mot de passe

Cliquez sur Oui ou sur Non pour indiquer si l'utilisateur doit changer son

mot de passe lors de la prochaine authentification.

Verrouillage du mot de passe
Cliquez sur Oui ou sur Non pour indiquer si le mot de passe doit être verrouillé. Ce paramètre prend la valeur Oui lorsque le nombre maximal de tentatives de connexion autorisées est dépassé, ou lorsque le mot de passe n'a pas été utilisé pendant la durée spécifiée dans la zone Nombre maximal de jours avant verrouillage.

L'administrateur peut lui donner la valeur Oui pour empêcher un utilisateur de faire appel à l'authentification par mot de passe.

Remarques :

1. La distinction majuscules/minuscules doit être respectée pour la saisie des mots de passe. Si le mot de passe que vous définissez contient des minuscules et des majuscules, l'utilisateur doit l'entrer tel que vous l'avez spécifié. Entrez les mots de passe des utilisateurs en majuscules sur les postes de travail qui n'acceptent que ce type de caractère.
2. Le système d'exploitation vous permet de définir des règles relatives aux mots de passe. Ces règles s'appliquent lorsqu'un utilisateur change un mot de passe. Elles ne s'appliquent pas aux modifications effectuées par les administrateurs. Les règles associées aux mots de passe sont les suivantes :

   Nombre de jours de préavis avant expiration (jours)
   Délai (en nombre de jours) pendant lequel l'utilisateur est autorisé à changer son mot de passe avant qu'il n'expire.

   Nombre maximal de semaines avant expiration
   Délai (en nombre de semaines) au-delà duquel l'utilisateur doit changer son mot de passe.

   Nombre maximal de semaines avant interdiction d'accès
   Délai (en nombre de semaines) au-delà duquel le mot de passe est verrouillé, s'il n'est pas utilisé.

   Nombre maximal de tentatives de connexion
   Nombre maximal de tentatives de connexion autorisées avant que le mot de passe soit verrouillé.

Nombre de mots de passe avant réutilisation
Nombre de mots de passe enregistrés dans l'historique des mots de passe. Un mot de passe ne peut pas être remplacé par une entrée de l'historique. Ce paramètre n'est valide que si la règle Nombre de semaines avant réutilisation du mot de passe a la valeur 0.

Nombre de semaines avant réutilisation du mot de passe
Délai (en nombre de semaines) pendant lequel les mots de passe sont conservés dans l'historique. Un mot de passe ne peut pas être remplacé par une entrée de l'historique.

Longueur minimale Nombre minimum de caractères autorisés dans un mot de passe.

Nombre minimal de caractères alphabétiques
Nombre minimum de caractères alphabétiques autorisés dans un mot de passe.

Nombre minimal de caractères autres
Nombre minimum de caractères non alphabétiques autorisés dans un mot de passe.

Nombre maximal d'occurrences d'un même caractère
Nombre maximum d'occurrences d'un même caractère autorisées dans un mot de passe.

Nombre minimal de caractères différents
Nombre minimum de caractères différents autorisés dans un mot de passe.

Cliquez sur l'onglet **Mot de passe de pare-feu** pour personnaliser ces valeurs pour chaque utilisateur, comme illustré par la figure 24, à la page 87.

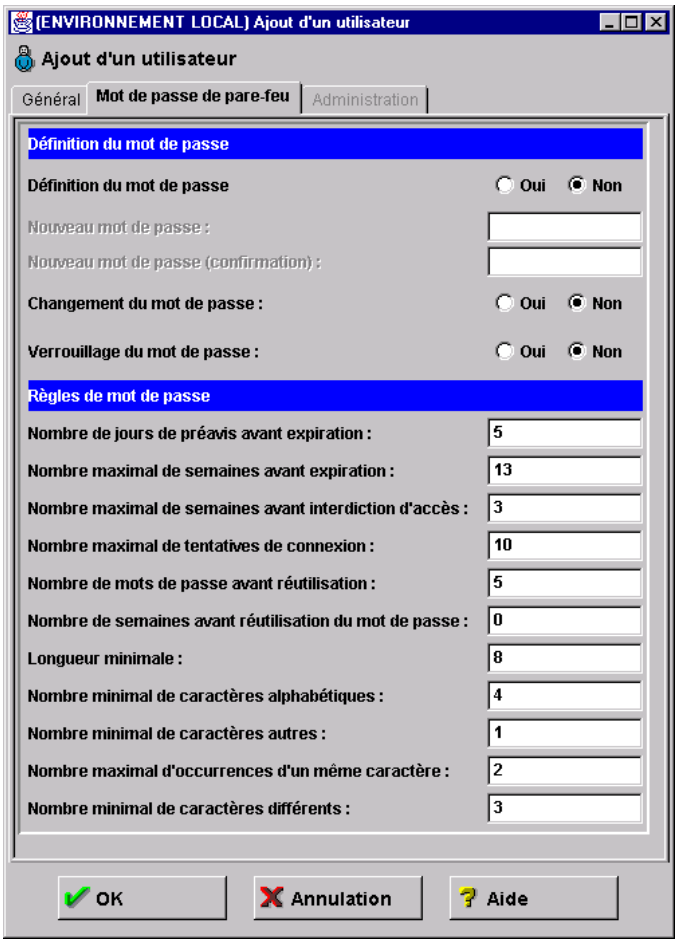

Figure 24. Onglet Mot de passe de pare-feu

Modification de l'accès utilisateur

Après avoir ajouté un utilisateur sur le pare-feu, vous pouvez modifier ses attributs de sécurité dans la boîte de dialogue **Modification d'un utilisateur**.

1. Sélectionnez l'utilisateur dont vous voulez modifier les attributs dans la boîte de dialogue **Utilisateurs** et cliquez sur **Ouverture**.
2. Modifiez les paramètres appropriés dans la boîte de dialogue **Modification d'un utilisateur** qui apparaît à l'écran. Pour connaître la liste des attributs d'utilisateurs modifiables, reportez-vous à la section «Ajout d'un utilisateur sur IBM Firewall», à la page 77.
3. Une fois les modifications apportées, cliquez sur **OK**.

Suppression d'un utilisateur d'IBM Firewall

Remarque : Ne supprimez pas les utilisateurs `fwdfuser` et `fwdfadm`.

Pour supprimer un utilisateur, cliquez sur **Suppression** dans le panneau **Liste des utilisateurs**.

Niveau d'autorisation de l'administrateur par fonction

Seul l'*administrateur principal du pare-feu* est habilité à créer et à modifier des administrateurs. Il peut également déterminer les fonctions que ces administrateurs ont le droit de mettre en œuvre sur le pare-feu. Par exemple, vous pouvez restreindre les droits d'un administrateur pour qu'il soit habilité à exécuter uniquement les fonctions relatives aux utilisateurs et au contrôle de journalisation.

Dans la boîte de dialogue **Ajout d'un utilisateur**, sélectionnez Administrateur du pare-feu dans la zone **Niveau d'autorisation**. Pour de plus amples informations sur l'utilisation de la boîte de dialogue **Ajout d'un utilisateur**, reportez-vous à la section «Ajout d'un utilisateur sur IBM Firewall», à la page 77.

Sélectionnez l'onglet **Administration** en haut de la boîte de dialogue **Ajout d'un utilisateur**. Choisissez les fonctions que l'administrateur est habilité à mettre en œuvre.

Méthodes d'authentification

Les diverses méthodes d'authentification disponibles sont décrites ci-dessous.

Interdiction globale

IBM Firewall interdit l'accès au serveur.

Autorisation globale

Aucune méthode d'authentification n'est requise. Le serveur ne tente pas de vous authentifier, mais il affiche une invite vous permettant d'accéder à un hôte distant.

Mot de passe de pare-feu

Avant de poursuivre, le serveur vous demande d'entrer votre mot de passe de pare-feu (qui ne s'affiche pas).

```
Mot de passe :
```

Entrez votre mot de passe de pare-feu. Il s'agit de celui utilisé lors de l'ajout de votre nom d'utilisateur sur le pare-feu.

Authentification avec la carte SecurID

Utilisez cette méthode si vous disposez d'une carte SecurID et que votre réseau fait appel à Security Dynamics ACE/Server.

Avant de poursuivre, le serveur vous demande d'entrer votre code d'accès (PASSCODE). Ce code ne s'affiche pas.

```
Entrez le PASSCODE :
```

Vous devez indiquer un numéro d'identification SecurID à 4 chiffres, suivi d'une virgule et du code de la carte SecurID. Ainsi, si vous voulez vous connecter en tant que NOUVELUTIL alors que votre numéro d'identification est 1234 et que le code de votre carte SecurID est 179091, vous devez fournir les informations ci-dessous.

```
connexion : NOUVELUTIL
Entrez le PASSCODE : 1234,179091
```

Si les utilisateurs emploient initialement FTP, l'authentification au moyen de la carte SecurID échoue car FTP n'autorise pas le changement de mot de passe. Ils doivent utiliser Telnet lors de la première tentative d'authentification SecurID qui permet de définir un numéro d'identification. Ce numéro d'authentification peut ensuite être employé avec FTP, HTTP, etc.

Si la carte SecurID est utilisée en mode de création PIN, vous devez définir le numéro d'identification avant d'employer cette méthode d'authentification avec IBM Firewall.

Authentification avec SecureNet Key

Utilisez cette méthode si vous disposez d'une carte Assurenet Pathways SecureNet Key. Lorsque vous initialisez la carte SNK, utilisez les paramètres suivants :

- format d'affichage (hexadécimal) ;
- fonction d'effacement (activée ou désactivée) ;
- fonction d'authentification à un chiffre (désactivée).

Avant de poursuivre, le serveur relais attend qu'une réponse lui soit fournie par la carte SecureNet Key.

```
Use SNK for challenge   ######## for user user_id
Ed:
```

La question ######## correspond à un code à 8 chiffres que vous entrez sur la carte SecureNet Key.

1. Lorsque cette invite s'affiche, activez la carte SecureNet Key et entrez le numéro d'identification fourni avec la carte .
2. Entrez le code tel qu'indiqué par le serveur.

   Par exemple, si vous vous connectez au serveur et que l'invite suivante s'affiche :

   ```
   Use SNK for challenge      78987648 for user NEWUSER
   Ed:
   ```

   Entrez la valeur 78987648 dans la carte SecureNet Key. La carte affiche alors la réponse que vous devez fournir au serveur relais.
3. Communiquez la réponse au serveur relais.

   Si la carte SecureNet Key affiche 8AE222A9 en réponse à la question, vous devez indiquer la valeur 8AE222A9 au serveur :

   ```
   logon: NEWUSER
      Use SNK for challenge 78987648 for user NEWUSER
   Ed:8AE222A9
   ```

SecurNetKey (SNK) a été renommé en Defender Handheld Token** (DHT) par AXENT** Technologies.

Mot de passe de connexion à NT

Si vous choisissez cette méthode d'authentification, votre ID utilisateur et votre mot de passe seront vérifiés par rapport à la base de données locale des utilisateurs NT. Si le pare-feu est configuré pour établir des relations de confiance avec d'autres serveurs NT, les définitions d'utilisateurs seront recherchées sur ces derniers.

Méthode d'authentification fournie par l'utilisateur 1, 2 et 3

Vous pouvez utiliser la méthode d'authentification fournie par l'utilisateur pour FTP et Telnet. Pour de plus amples informations, reportez-vous au *guide de référence d'IBM eNetwork Firewall*.

Chapitre 13. Configuration des serveurs relais

Ce chapitre contient des informations générales sur la configuration et l'utilisation des serveurs relais à partir des postes de travail qui se trouvent à l'intérieur et à l'extérieur du réseau sécurisé.

Serveur relais HTTP

Relais HTTP traite les requêtes du navigateur par l'intermédiaire du pare-feu IBM, ce qui évite d'utiliser un serveur socks pour effectuer des recherches sur le Web. Les utilisateurs peuvent accéder à Internet, sans nuire à la sécurité du réseau interne ni modifier leur environnement client pour mettre en œuvre le relais HTTP.

Le relais HTTP n'est pas un serveur. L'utilisateur final ne peut pas charger de fichiers sur ce relais, ni en décharger. Il n'a pas non plus d'antémémoire. Une requête HTTP ne donne lieu à aucun enregistrement sur le pare-feu.

Sessions permanentes

Les connexions permanentes autorisent un client et un serveur à signaler la fermeture d'une connexion TCP. Cette procédure utilise une zone d'en-tête de connexion.

Le relais d'IBM Firewall prend en charge les connexions permanentes entre un client et le relais. Les conditions *Nombre maximal de requêtes permanentes* et *Délai de connexion permanente* contrôlent la durée de ce type de connexion. Lorsqu'un de ces événements se produit, la connexion via la socket entre le relais et le client prend fin. Si les conditions *Nombre maximal de requêtes permanentes* et *Délai d'expiration des connexions permanentes* ne sont pas réunies, la connexion reste ouverte ; il appartient au client de déterminer la fin de l'exécution d'une requête.

Si elle est analysée de façon incorrecte, un message indiquant que la connexion est utilisée peut s'afficher, alors que le trafic est inexistant. Ainsi par exemple, l'icône animée d'un navigateur peut continuer à s'exécuter même si la page a été chargée dans son intégralité. Cliquez sur **Arrêt** pour mettre fin à l'animation. Pour plus d'informations sur ces paramètres, voir «Nombre maximal de requêtes permanentes», à la page 93 et «Délai d'expiration des connexions permanentes», à la page 94.

Configuration du relais HTTP à l'aide du client de configuration

Pour configurer le relais HTTP, procédez comme suit :

1. Pour que le relais HTTP fonctionne correctement, autorisez les requêtes DNS. Pour ce faire, cliquez sur Règles de sécurité dans le dossier Administration du système de l'arborescence de consultation du client de configuration, puis cliquez sur Autorisation des requêtes DNS.
2. Activez les filtres.
3. Ajoutez une connexion. Pour savoir comment configurer une connexion du côté non sécurisé du réseau, reportez-vous à la section «Exemple de relais HTTP», à la page 57.

4. Pour configurer le relais HTTP, sélectionnez HTTP dans l'arborescence de navigation du client de configuration. IBM Firewall affiche la boîte de dialogue **Relais HTTP**, comme représenté dans la figure 25, à la page 92.

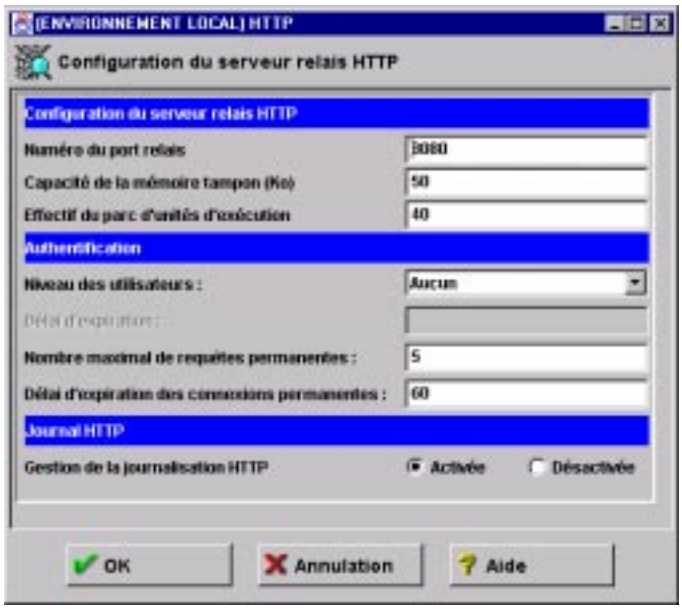

Figure 25. HTTP

5. Pour arrêter le relais, sélectionnez `my computer/panneau de configuration/services`. Choisissez le relais HTTP d'IBM Firewall et cliquez sur *Arrêt*.

   L'exécutable phttpd est un service du système paramétré pour démarrer automatiquement lorsque le système est lancé.

Configurez les paramètres dans la boîte de dialogue **Relais HTTP**. Si vous modifiez un paramètre, le service de relais HTTP du pare-feu s'interrompt, puis redémarre. Les requêtes des utilisateurs du relais actif seront finalisées avant que le relais soit relancé (il se produit quelques secondes).

Numéro du port relais

Ce paramètre permet de spécifier le numéro de port à associer au relais. Si vous modifiez ce numéro, vous devez configurer vos filtres de façon à autoriser ou interdire la circulation de données via les ports. Les numéros de port inférieurs à 1024 sont réservés aux applications TCP/IP. 8080 et 8088 sont les numéros de ports généralement utilisés pour les serveurs relais du Web.

Les règles de filtrage par défaut interdisent le trafic interne et non sécurisé sur le port 8080, mais y autorisent en revanche le trafic sécurisé. Le relais refusera uniquement les demandes non sécurisées. La valeur par défaut est `8080`. Si vous modifiez cette valeur, le numéro de port doit également être modifié dans les services définis pour cette configuration. Si vous modifiez l'un des ces paramètres, vous devez redémarrer le processus phttpd.

Capacité de la mémoire tampon
Ce paramètre permet de définir la taille du tampon contenant les données dynamiques générées par un serveur, c'est-à-dire les sorties de programmes CGI, y compris le côté serveur et des API. Ces données ne proviennent pas d'un relais.

Entrez une valeur en kilo-octets (ko). La valeur par défaut est `50`.

Effectif du parc d'unités d'exécution
Ce paramètre définit le nombre fixe d'unités d'exécution activables à un moment donné. Le serveur relais garde les nouvelles requêtes en attente jusqu'à ce qu'une requête en cours se termine et qu'une unité d'exécution devienne disponible. Généralement, plus le système est puissant, plus la valeur de ce paramètre peut être élevée. Si le système commence à passer trop de temps à exécuter des opérations de servitude telles que l'échange de pages mémoire, essayez de réduire cette valeur. Précisez un nombre entier tel que 60, par exemple. La valeur par défaut est `200`.

Niveau des utilisateurs
Ce paramètre indique le niveau d'authentification des utilisateurs au relais. Spécifiez la valeur all, new ou none. La valeur par défaut est none. Les valeurs possibles sont les suivantes :

all Tous les navigateurs recevront la réponse d'authentification du relais leur indiquant qu'ils doivent afficher une invite pour demander un ID utilisateur et un mot de passe. Si le navigateur ne prend pas en charge cette réponse, la page d'erreur le signale. Dans le cas contraire, l'invite demandant l'ID utilisateur et le mot de passe s'affiche.

new Est utilisé comme aide à la migration. Il renvoie uniquement une réponse d'authentification 407 pour demander au navigateur de générer une invite ID utilisateur/mot de passe à un navigateur client qui s'identifie comme étant HTTP/1.1. Dans Internet Explorer 4.0, vous pouvez forcer les requêtes émises à s'identifier comme HTTP/1.1. Netscape et les autres s'identifient eux-mêmes comme des requêtes HTTP/1.0.

none Ne vérifie pas les requêtes du navigateur. N'affiche pas d'invite pour demander un ID utilisateur et/ou un mot de passe.

Délai d'expiration
Ce paramètre indique la durée, en l'absence de requête du client, au-delà de laquelle le relais demande à l'utilisateur de se réauthentifier. Un utilisateur est authentifié à partir de l'adresse IP et de l'ID utilisateur au moment de l'authentification, qui a précédé cette période d'inactivité. Entrez une durée exprimée en minutes. La valeur par défaut est 60.

Tant que l'utilisateur est actif, le délai n'est pas pris en compte.

Nombre maximal de requêtes permanentes
Ce paramètre indique le nombre maximal de requêtes qu'un relais peut recevoir sur une connexion permanente HTTP/1.1. Il s'agit d'un outil de performance qui influe directement sur le délai d'expiration de l'authentification. Aucun test d'authentification d'un utilisateur n'est effectué avant la fin d'une session permanente. Entrez une durée exprimée en minutes. Précisez un nombre entier (25, par exemple). La valeur par défaut est 5.

Délai d'expiration des connexions permanentes

Ce paramètre indique la durée en secondes de maintien d'une connexion permanente HTTP/1.1 avec un navigateur client, après qu'un navigateur compatible HTTP/1.1 démarre une session avec le relais. Il s'agit d'un outil de performance qui influe directement sur le délai d'expiration de l'authentification. Aucun test d'authentification d'un utilisateur n'est effectué avant la fin d'une session permanente. Entrez une durée exprimée en minutes. Entrez une durée exprimée en secondes. La valeur par défaut est 60.

Gestion de la journalisation HTTP

Ce paramètre permet au relais de consigner les requêtes de démarrage/arrêt et toutes les requêtes du relais dans le journal du pare-feu. Il utilise le niveau de journalisation LOG_NOTICE. Activez-le si vous souhaitez contrôler l'activité des requêtes HTTP. Les événements sont consignés dans le `fichier journal du pare-feu`.

Configuration du navigateur

Le navigateur client doit être configuré de façon à se connecter au port associé au relais HTTP.

Si HTTPS est utilisé, pointez aussi vers le relais HTTP sur IBM Firewall pour le relais de sécurité.

Pour que le serveur relais considère votre navigateur Internet Explorer comme un navigateur HTTP/1.1, procédez comme suit :

- Ouvrez le menu déroulant *Affichage*.
- Sélectionnez *Options*.
- Sélectionnez l'onglet *Avancées*.
- Descendez jusqu'aux Paramètres HTTP 1.1 et activez les options.

Connexions SSL

Les tunnels SSL sont pris en charge pour les connexions sécurisées HTTP aux autres serveurs. Dans ce cas, IBM Firewall fonctionne comme une passerelle. Un tunnel relie le client au serveur par l'intermédiaire du pare-feu. Utilisez le port standard 443 pour les connexions sécurisées via HTTP, comme indiqué dans l'exemple suivant :

```
https://www.ibm.com:443
```

Utilisez aussi le service prédéfini `Relais HTTPS en sortie 2/2`.

Si HTTPS est utilisé, pointez aussi vers le relais HTTP sur IBM Firewall pour le relais de sécurité.

Pour plus d'informations, reportez-vous à la section «Exemple de relais HTTP», à la page 57.

Méthodes prises en charge

Le relais HTTP prend en charge les méthodes suivantes, qui constituent plusieurs moyens d'utiliser Internet :

- FTP ;
- Gopher ;
- HTTP ;
- HTTPS ;
- WAIS.

Exemple de journalisation de l'activité du relais HTTP

L'exemple suivant est un extrait de la journalisation des requêtes de lecture authentifiées du serveur relais HTTP :

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> Serveur relais HTTP
non authentifié
pour utilisateur <Inconnu>, sur 9.67.140.162, via le réseau sécurisé ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> État: 407 du client
9.67.140.162, dont la requête "GET http://9.67.128.69/ HTTP/1.1" a
généré 0 octets.
Mar 06 14:05:05 1998 fire3: ICA2024i: Utilisateur jean authentifié
avec l'authentification NT depuis le réseau sécurisé:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: Utilisateur jean authentifié pour le serveur
HTTP avec l'authentification NT depuis le réseau sécurisé:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> Serveur relais HTTP
authentifié
pour utilisateur (jean), sur 9.67.140.162, via le réseau sécurisé...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> État: 200 du client
9.67.140.162, dont la requête "GET http://9.67.128.69/HTTP/1.1" a généré
2693 octets.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> Serveur relais HTTP
authentifié
pour utilisateur (jean), sur 9.67.140.162, via le réseau sécurisé...RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> État: 200 du client
9.67.140.162, dont la requête "GET http://9.67.128.69/Admin/lgsplash.gif
HTTP/1.1"
a généré 211 octets.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> Serveur relais HTTP
authentifié
pour utilisateur (jean), sur 9.67.140.162, via le réseau sécurisé...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> État: 200 du client
9.67.140.162, dont la requête "GET http://9.67.128.69/Admin/lgmast.gif
HTTP/1.1"
a généré 211 octets.
```

La fonction de journalisation est expliquée ci-dessous :

- ICA2099i - affiche le code de retour 407 signifiant que l'authentification a échoué pour cette requête de lecture.

  Le navigateur invite alors l'utilisateur à s'authentifier en entrant un ID utilisateur et un mot de passe.

- ICA2140i - l'utilisateur Jean a été authentifié.

La procédure d'authentification est lancée à chaque requête de lecture pour chaque élément de la page web.

FTP

1. Le relais FTP permet d'accéder à l'hôte du pare-feu. (Nous utiliserons `ftp_gw.domain.net.com` comme nom d'hôte pour le pare-feu).

   ```
   ftp ftp_gw.domain.net.com
   ```

   Le serveur relais vous invite à entrer votre nom d'utilisateur :

   ```
   login:
   ```

2. Le nom d'utilisateur qui vous est affecté doit être autorisé à utiliser le pare-feu :

   ```
   login: jane_doe
   ```

Pour valider votre identité, le serveur utilise la méthode d'authentification choisie lorsque votre nom d'utilisateur a été ajouté au pare-feu (voir «Ajout d'un utilisateur sur IBM Firewall», à la page 77). Pour plus d'informations sur le mode d'authentification des utilisateurs par les serveurs relais, reportez-vous à la section «Méthodes d'authentification», à la page 88.

Une fois que vous êtes authentifié, le serveur relais affiche une invite de commande FTP.

```
ftp>
```

Lancez les commandes FTP `quote` et `site` pour vous connecter à l'hôte étranger :

```
ftp> quote site forhost.network.outside.com
```

L'hôte étranger vous invite ensuite à entrer un nom d'utilisateur et un mot de passe qui vous permettront de vous connecter. Il s'agit probablement d'un nom d'utilisateur et d'un mot de passe différents de ceux utilisés pour les liaisons FTP avec le pare-feu.

La valeur par défaut du dépassement de durée pour la connexion est 60 secondes ; pour le relais inactif elle correspond à 7200 secondes. Pour changer les valeurs par défaut, consultez la section «Remplacement des valeurs des délais d'attente pour les relais FTP et Telnet», à la page 98.

FTP en mode transparent

Vous pouvez utiliser ftp en mode transparent via le pare-feu. Les relais transparents n'exigeant aucune authentification, leurs utilisateurs ne doivent pas être nécessairement définis en tant qu'utilisateurs relais du pare-feu. Les relais transparents sont uniquement autorisés depuis le côté sécurisé du pare-feu vers la partie non sécurisée du pare-feu. Pour que le relais transparent soit opérationnel, vous devez le sélectionner dans le panneau Règles de sécurité du client de configuration.

1. Utilisez ftp pour accéder à l'hôte du pare-feu. (Nous utiliserons `ftp_gw.domain.net.com` comme nom d'hôte pour le pare-feu).

   ```
   ftp ftp_gw.domain.net.com
   ```

2. Le serveur relais vous invite à entrer votre nom d'utilisateur :

   ```
   USER:
   ```

3. Entrez votre nom d'utilisateur au niveau du réseau non sécurisé :

   ```
   USER:  nom_utilisateur@nom_hôte_site_distant
   ```

4. L'hôte cible vous invite à entrer votre mot de passe associé au `nom d'utilisateur` entré lors de l'étape précédente.

   ```
   password:
   ```

5. Entrez votre mot de passe.

La valeur par défaut du délai d'attente pour la connexion est 60 secondes ; elle est de 7200 secondes (2 heures) pour le relais inactif. Pour changer les valeurs par défaut, reportez-vous à la section «Remplacement des valeurs des délais d'attente pour les relais FTP et Telnet», à la page 98.

Telnet

À l'aide du relais telnet, connectez-vous au serveur relais du pare-feu. Vous pouvez utiliser au choix le nom de l'hôte ou l'adresse Internet. Ensuite, une fois que vos références sont authentifiées, vous pouvez utiliser la commande telnet au niveau du pare-feu pour vous connecter à l'hôte souhaité. Par exemple, utilisons telnet au sein du réseau sécurisé, via le pare-feu avec le nom d'hôte `telnet_gw`, pour accéder à votre destination ultime, `forhost.network.outside.com`.

1. Pour démarrer le processus, utilisez telnet, qui permet d'accéder à l'hôte du pare-feu. (Nous utiliserons telnet_gw.domain.net.com comme nom d'hôte pour le pare-feu.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. Le serveur relais vous invite à entrer votre nom d'utilisateur :

   ```
   login:
   ```

3. Le nom d'utilisateur qui vous est affecté doit être autorisé à utiliser le pare-feu :

   ```
   login: jane_doe
   ```

Pour valider votre identité, le serveur utilise la méthode d'authentification choisie lorsque votre nom d'utilisateur a été ajouté au pare-feu (voir «Ajout d'un utilisateur sur IBM Firewall», à la page 77). Pour plus d'informations sur le mode d'authentification des utilisateurs par les serveurs relais, reportez-vous à la section «Méthodes d'authentification», à la page 88.

Vous utiliserez le shell oneact. Avec le démon telnet relais d'IBM Firewall, toutes les communications passent par le pare-feu.

Si vous utilisez le shell oneact, une fois que vous êtes authentifié, le serveur relais affiche :

```
Entrez un hôte :
```

Tapez :

```
telnet forhost.network.outside.com
```

Étant donné que vous êtes identifié sur cet hôte, l'hôte étranger vous demande votre nom d'utilisateur et votre mot de passe. Ces noms peuvent être différents de ceux utilisés sur le serveur relais du pare-feu.

La valeur par défaut du dépassement de durée pour la connexion est 60 secondes ; pour le relais inactif elle correspond à 7200 secondes. Pour changer les valeurs par défaut, consultez la section «Remplacement des valeurs des délais d'attente pour les relais FTP et Telnet».

Telnet en mode transparent

Vous pouvez utiliser telnet en mode transparent via le pare-feu. Les relais transparents n'exigeant aucune authentification du pare-feu, leurs utilisateurs ne doivent pas être nécessairement définis en tant qu'utilisateurs relais du pare-feu. Les relais transparents sont uniquement autorisés depuis le côté sécurisé du pare-feu vers la partie non sécurisée du pare-feu. Pour que le relais transparent soit opérationnel, vous devez le sélectionner dans le panneau Règles de sécurité du client de configuration.

1. Utilisez telnet pour accéder à l'hôte du pare-feu. (Nous utiliserons `ftp_gw.domain.net.com` comme nom d'hôte.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. Le serveur relais vous invite à entrer votre nom d'utilisateur :

   ```
   Login:
   ```

3. Entrez votre nom d'utilisateur au niveau du réseau non sécurisé :

   ```
   connexion@hôte_distant
   ```

Étant donné que vous êtes identifié sur cet hôte, l'hôte étranger vous demande votre nom d'utilisateur et votre mot de passe. Ces noms peuvent être différents de ceux utilisés sur le serveur relais du pare-feu.

La valeur par défaut du délai d'attente pour la connexion est 60 secondes ; elle est de 7200 secondes (2 heures) pour le relais inactif. Pour changer les valeurs par défaut, reportez-vous à la section «Remplacement des valeurs des délais d'attente pour les relais FTP et Telnet».

Remplacement des valeurs des délais d'attente pour les relais FTP et Telnet

Des valeurs des délais d'expiration sont associées à FTP et à Telnet pour les connexions et les délais d'inactivité. Par défaut, la session doit être active au moins une fois toutes les 60 secondes pendant la connexion et l'authentification de l'utilisateur. Il s'agit du délai de connexion.

Une fois que vous êtes connecté, la session doit être active au moins une fois toutes les 7200 secondes : lorsque ce délai est dépassé, la session est fermée.

Vous pouvez changer ces valeurs par défaut en créant un fichier `fwTimeout.cfg` dans le répertoire `ROOTDIR\config` et en spécifiant de nouvelles valeurs de délais d'expiration exprimées en secondes. Le fichier `fwTimeout.cfg` doit avoir le format suivant :

```
telnet
proxyTimeout=7200
loginTimeout=60

ftp
proxyTimeout=7200
loginTimeout=60
```

Chapitre 14. Contrôle des journaux du pare-feu

Ce chapitre traite du contrôle de la journalisation des alertes en temps réel. Une alerte est générée lorsqu'un seuil configuré est violé.

IBM Firewall surveille les messages transmis au journal du pare-feu pour détecter les problèmes éventuels, en fonction de seuils définis par l'utilisateur. En cas de violation d'un seuil, le pare-feu envoie une alerte, selon une méthode définie par l'administrateur du pare-feu.

Définitions de seuils

Un seuil est constitué de paramètres relatifs au nombre et à la durée — si un nombre (d'événements spécifiques) est dépassé dans la durée définie (minutes), le seuil est violé et un message d'avertissement est généré. Le contrôle de journalisation reconnaît quatre types de seuils :

1. Seuils d'échec d'authentification ;
2. Nombre d'échecs d'authentification par ID utilisateur ;
3. Nombre d'échecs d'authentification par système hôte ;
4. Occurrences d'un code de message dans le journal.

Tous les seuils peuvent être configurés à l'aide du client de configuration client ou de la ligne de commande. Les modifications apportées aux définitions de seuils sont captées automatiquement par IBM Firewall.

Messages d'avertissement

Lorsqu'un seuil est atteint, IBM Firewall génère un message d'avertissement. L'envoi d'un message d'avertissement peut être effectué selon l'une des méthodes suivantes :

1. Entrée dans un fichier journal :
   - Par l'intermédiaire du `journal des alertes`, configurable via le client de configuration ou la ligne de commande ;
   - Dans le `journal du pare-feu`.
2. Courrier adressé à une liste d'utilisateurs, via une transaction safemail.
3. Récepteur de radiomessagerie, selon la configuration adoptée. Voir la section «Support de notification du récepteur de radiomessagerie», à la page 103.
4. Exécution d'une commande définie par l'utilisateur, avec le message d'avertissement comme premier paramètre.

Le message d'avertissement contient des informations concernant le seuil qui est violé. Par exemple :

```
ICA0001e : ALERTE – 20 échecs d'authentification.
ICA0002e : ALERTE – 10 échecs d'authentification de l'utilisateur root.
ICA0003e : ALERTE – 15 échecs d'authentification de l'hôte 56.67.78.89
ICA0004e : ALERTE – Code ICA1234e avec 3 entrées de fichier journal.
```

Les messages d'avertissement et les autres messages provenant du Contrôle de journalisation ne sont pas contrôlés.

Configuration du Contrôle de journalisation à l'aide du client de configuration

Cette section traite de l'utilisation du client de configuration pour configurer le Contrôle de journalisation en temps réel. À partir de l'arborescence de navigation du client de configuration, sélectionnez Journaux système. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Cliquez sur **Seuils de contrôle de journalisation**.

Dans la boîte de dialogue **Administration des seuils du contrôle de journalisation**, vous pouvez ajouter, modifier ou supprimer une définition de seuil.

Ajout d'un contrôle de journalisation

Pour ajouter une définition de seuil, sélectionnez **Création** dans la boîte de dialogue **Administration des seuils du contrôle de journalisation** et cliquez sur **Ouverture**. La boîte de dialogue **Ajout d'un contrôle de journalisation** s'ouvre. Complétez les zones suivantes :

1. Pour choisir un type de classe, cliquez sur la flèche associée à la zone **Type de classe**. Ces types sont les suivants :
   - Notification par courrier ;
   - Exécution de commande ;
   - Seuil d'échecs d'authentification par utilisateur ;
   - Seuil total d'échecs d'authentification ;
   - Seuil d'échecs d'authentification par hôte ;
   - Seuil de messages.
2. Si vous avez sélectionné le type de classe Notification par courrier, entrez une adresse électronique. Vous pouvez définir plusieurs classes de notification de courrier.

   Tous les messages signalant une violation de seuil sont envoyés à l'adresse indiquée.
3. Si vous avez sélectionné le type de classe Exécution de commande, entrez un nom de fichier de commande.

   Le contrôle de journalisation exécute cette commande avec le message d'avertissement comme premier paramètre. Vous pouvez définir seulement une classe de commande d'exécution.
4. Si vous avez sélectionné le type de classe Seuil de messages, entrez un code de message, un code standard issu des messages de journal d'IBM Firewall à contrôler.
5. Si vous avez sélectionné une des classes de seuils, complétez la zone Comptage des seuils.

   Cette valeur correspond au nombre maximal d'erreurs autorisées dans la période de temps spécifiée.
6. Si vous avez sélectionné une des classes de seuils, complétez la zone Durée du seuil.

Cette durée correspond au nombre de minutes à partir de la première occurrence d'un événement.

7. Si vous avez sélectionné une des classes de seuils, cliquez sur Oui ou Non pour indiquer si vous souhaitez que la notification par récepteur de radiomessagerie soit active.
8. L'ajout d'un commentaire est facultatif.
9. Cliquez sur **OK**.

Modification d'une définition de seuil

Pour modifier une définition de seuil, sélectionnez l'élément à modifier dans la boîte de dialogue **Administration des seuils du contrôle de journalisation** et cliquez sur **Ouverture**. La boîte de dialogue **Modification du contrôle de journalisation** s'ouvre.

1. Entrez les modifications souhaitées dans les zones de comptage et de durée des seuils.

   Le comptage des seuils correspond au nombre maximal de messages indiquant une erreur d'authentification, détectée au cours d'une période donnée. La durée du seuil correspond au nombre de minutes à partir de la première occurrence d'un message.

2. Cliquez sur **OK**.

Suppression d'une définition de seuil

Pour supprimer une définition de seuil, sélectionnez l'élément à supprimer dans la boîte de dialogue **Seuils de contrôle de journalisation** et cliquez sur **Suppression**. Un message vous invite à confirmer la suppression. Cliquez sur **Oui** pour confirmer. Cela ne signifie pas que l'élément est supprimé du fichier journal. Seule la définition est supprimée.

Support de notification du récepteur de radiomessagerie

Le pare-feu peut envoyer un message au bipeur de l'administrateur lorsque des alertes d'intrusion se produisent au niveau du pare-feu. Pour configurer le support de notification par récepteur de radiomessagerie, vous devez configurer les trois composants suivants :

1. Personnalisation des commandes - Ce composant doit être créé et modifié à l'aide du client de configuration. Il définit les valeurs par défaut associées à la commande du récepteur de radiomessagerie, qui est utilisée par le contrôle de journalisation et peut être lancée depuis la ligne de commande. Ce composant contient une entrée unique qui définit l'environnement du récepteur de radiomessagerie. Pour plus d'informations sur la configuration et la personnalisation de ce composant, consultez la section «Personnalisation des commandes», à la page 105.
2. Administration des opérateurs - Vous devez définir un opérateur approprié avant de connecter votre modem. Ce composant comprend une liste d'opérateurs par défaut utilisés aux États-Unis. Si l'opérateur auquel vous faites appel n'en fait pas partie, ajoutez-le dans ce composant. Pour plus d'informations, consultez la section «Administration des opérateurs», à la page 106.

Validez les numéros de téléphone existants des opérateurs en vous renseignant auprès d'eux. Veillez à vous procurer le numéro d'appel du modem et d'autres paramètres utiles pour le service que vous avez acquis.

3. Administration des modems - Avant de connecter votre modem, vous devez créer des définitions de modem adéquates. Ces définitions comprennent toutes les informations nécessaires sur le modem que le support de notification du récepteur de radiomessagerie utilisera. Une liste de modems est incluse dans ce composant. Vous pouvez compléter cette liste. Toutefois, il se peut que certains modems ne soient pas compatibles avec votre opérateur. Pour plus de détails sur la gestion des définitions de modem, reportez-vous à la section «Administration des modems», à la page 108.

Remarque : IBM Firewall prend en charge le protocole TAP (Tele-AlphaNumeric Protocol) pour la notification du récepteur de radiomessagerie.

Opérateurs et modems pris en charge

Le fichier de la base de données des opérateurs contient une liste d'opérateurs et de paramètres de transmission associés. Vous pouvez ajouter d'autres opérateurs. Outre le nom de l'opérateur et les numéros d'appel de modem, certains paramètres sont les suivants :

- Longueur maximale d'un message pour un récepteur alphanumérique et nombre maximal de chiffres pour un récepteur numérique ;
- Débit en bauds, parité, longueur des bits de données et des bits d'arrêt.

Avant de faire appel à un opérateur spécifique, assurez-vous que l'opérateur utilise le protocole TAP.

Le code du récepteur de radiomessagerie est assorti des définitions de modem par défaut. Ces définitions sont les suivantes :

- IBM MOD 448 14400 bps ;
- IBM 5853 2400 bps ;
- IBM 7852 28800 bps ;
- IBM 7855 2400 bps ;
- Generic Hayes compatible ;
- US Robotics Courier 9600 bps ;
- Zoom V.34.

Configuration du support de notification du récepteur de radiomessagerie

L'option Configuration du récepteur de radiomessagerie sert à configurer le fichier de personnalisation des commandes et à gérer les opérateurs et les modems. Si vous possédez un récepteur de radiomessagerie, vous devez utiliser l'option Configuration du récepteur de radiomessagerie pour personnaliser l'environnement de votre récepteur avant d'utiliser Contrôle de journalisation.

Avant de commencer, vous devez vous procurer les numéros d'appel du modem, l'ID du récepteur et les paramètres de modem auprès de votre opérateur.

Pour configurer le support de notification du récepteur de radiomessagerie,

sélectionnez, à partir de l'arborescence de navigation du client de configuration, le dossier Administration système. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Sélectionnez **Journaux système**. Cliquez deux fois sur l'icône du dossier pour en visualiser le contenu. Sélectionnez **Configuration du récepteur de radiomessagerie**.

Personnalisation des commandes

L'option **Configuration du récepteur de radiomessagerie** vous permet de sélectionner un opérateur et un modem pour utiliser le récepteur et écrire des messages.

Paramètres de personnalisation des commandes

Lorsque vous sélectionnez **Configuration du récepteur de radiomessagerie** dans l'arbre de navigation, la boîte de dialogue **Configuration du récepteur de radiomessagerie** s'ouvre ; elle contient des paramètres de personnalisation des commandes similaires à ceux illustrés dans la figure 26.

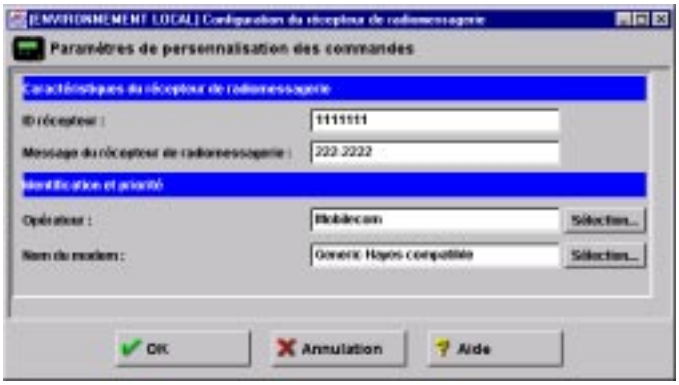

Figure 26. Configuration du récepteur

Tapez ou sélectionnez les valeurs à ajouter dans les zones de saisie.

1. Entrez l'ID de récepteur de radiomessagerie. Il s'agit généralement d'un numéro d'identification personnel unique attribué à votre récepteur de radiomessagerie par votre opérateur.
2. Entrez le message du récepteur de radiomessagerie. Il s'agit d'une chaîne comportant le message par défaut que l'utilisateur veut envoyer. Pour les systèmes numériques, entrez uniquement des chiffres. Dans le cas de récepteurs alphanumériques, vous pouvez entrer une chaîne de caractères. Veillez à ne pas dépasser la longueur maximale admise pour les messages, qui est spécifiée par votre opérateur, faute de quoi votre message risque d'être tronqué. Veillez à ne pas utiliser le signe deux-points (:). Si vous ne respectez pas cette consigne, ce signe sera remplacé par un espace.
3. Si aucun nom d'opérateur n'est répertorié, cliquez sur **Sélection** pour en définir un. La boîte de dialogue **Administration de l'opérateur de radiomessagerie** s'ouvre. Pour savoir comment compléter ce panneau, reportez-vous à la section «Administration des opérateurs», à la page 106.
4. Si aucun nom de modem n'est répertorié, cliquez sur **Sélection** pour en définir un. La boîte de dialogue **Administration du modem du récepteur de**

radiomessagerie s'ouvre. Pour savoir comment compléter ce panneau, reportez-vous à la section «Administration des modems», à la page 108.

5. Cliquez sur **OK**.

Modifications apportées à la personnalisation des commandes

Lorsque vous sélectionnez Configuration du récepteur de radiomessagerie dans l'arbre de navigation, la boîte de dialogue correspondante contenant des paramètres de personnalisation des commandes s'ouvre.

1. Tapez ou sélectionnez les valeurs en remplacement des paramètres courants dans les zones de saisie.
2. Cliquez sur **OK**.

Suppression de la personnalisation des commandes

1. Vous pouvez supprimer une entrée de la boîte de dialogue **Administration de l'opérateur de radiomessagerie** ou de la boîte **Administration du modem du récepteur de radiomessagerie** en sélectionnant un élément de la liste et en cliquant deux fois sur **Suppression**.

   Un message vous invite à confirmer la suppression.

2. Cliquez sur **Oui** pour confirmer la suppression ou sur **Non** pour revenir à la boîte de dialogue **Configuration du récepteur de radiomessagerie**.

S'il n'y a pas d'entrée personnalisée, le support de notification du récepteur ne peut pas envoyer de signal.

Administration des opérateurs

Dans la boîte de dialogue **Configuration du récepteur de radiomessagerie**, positionnez le curseur sur la zone Nom de l'opérateur et cliquez sur **Sélection**. La boîte de dialogue **Administration de l'opérateur du récepteur de radiomessagerie**, telle qu'elle est illustrée dans la figure 27, à la page 107, s'ouvre.

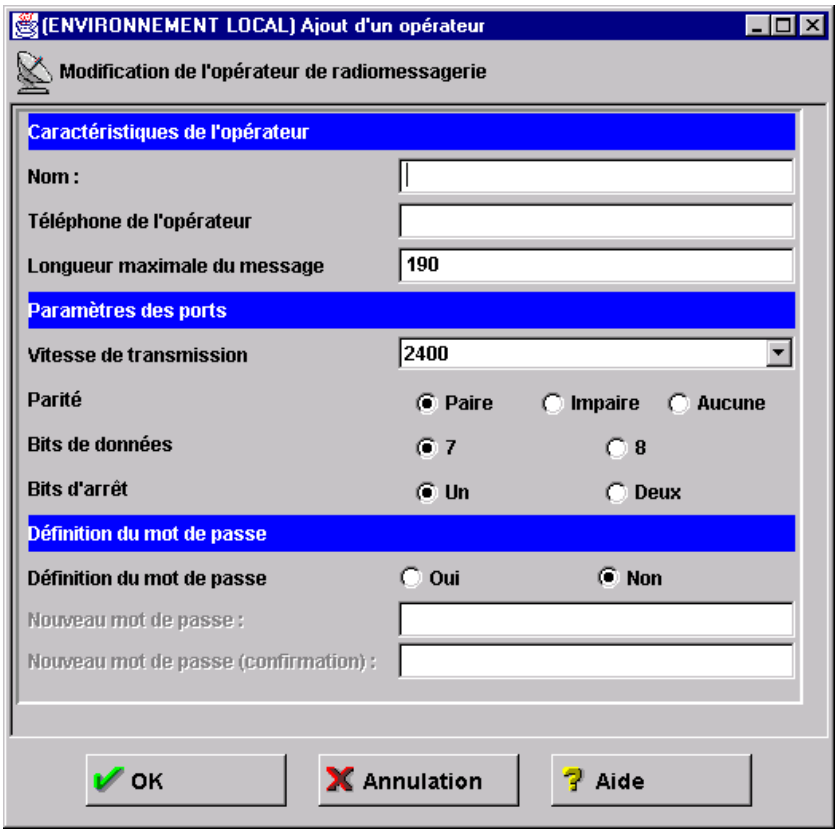

Figure 27. Administration de l'opérateur de radiomessagerie

Ajout d'un opérateur

Pour ajouter un opérateur, sélectionnez **Création** dans la boîte de dialogue **Administration de l'opérateur de radiomessagerie** et cliquez sur **Ouverture**. Tapez ou sélectionnez les valeurs à ajouter dans les zones de saisie appropriées.

1. Entrez le nom de l'opérateur. Il peut être aussi long que vous le souhaitez, sous condition d'être unique et suffisamment explicite.
2. Entrez le numéro de téléphone de l'opérateur, qui correspond à un numéro de modem (et non un récepteur de messages vocaux ni un autre numéro de service). Le modem doit avoir une couverture régionale ou nationale et être compatible avec un récepteur numérique ou alphanumérique, conformément aux spécifications du système de radiomessagerie et du service auquel vous avez souscrit.
3. Entrez TAP pour la méthode d'appel ; il s'agit de la seule valeur autorisée.
4. Entrez le mot de passe si l'opérateur en autorise la saisie ou la requiert.
5. Entrez la longueur maximale d'un message pour un récepteur alphanumérique et le nombre de chiffres maximal pour un récepteur numérique.
6. Entrez le débit en bauds. Cliquez sur la flèche et choisissez une valeur dans la liste.
7. Cliquez sur **Paire**, **Impaire** ou **Aucune** pour définir la parité.
8. Choisissez le nombre de bits de données par défaut ; cliquez sur **7** ou sur **8**.
9. Choisissez les bits d'arrêt par défaut ; cliquez sur **1** ou sur **2**.

10. Cliquez sur **OK**.

Modification des paramètres de l'opérateur

1. Sélectionnez l'opérateur dont vous souhaitez modifier les paramètres dans la boîte de dialogue **Administration de l'opérateur de radiomessagerie** et cliquez sur **Ouverture**.
2. Pour une description détaillée des zones à modifier, reportez-vous à la section «Ajout d'un opérateur», à la page 107. Le nom de l'opérateur ne peut pas être changé. Cette zone est désactivée.
3. Effectuez les modifications souhaitées.
4. Cliquez sur **OK**.

Suppression d'un opérateur

1. Sélectionnez l'opérateur à supprimer dans la boîte de dialogue **Administration de l'opérateur de radiomessagerie** et cliquez sur **Suppression**.
2. Un message vous invite à confirmer la suppression. Cliquez sur **Oui** pour confirmer.

   Remarque : La base de données des opérateurs doit toujours comporter au moins une entrée. Si aucun opérateur n'est défini, le support de notification du récepteur de radiomessagerie n'est pas opérationnel.

Administration des modems

Votre modem manuel comprendra des informations utiles sur la procédure d'initialisation du modem. Il se peut que vous ayez à harmoniser les paramètres du modem avec ceux de votre opérateur. En général, seuls les modems compatibles Hayes, qui utilisent les commandes de modem standard, sont pris en charge.

Dans la boîte de dialogue **Configuration du récepteur de radiomessagerie**, positionnez le curseur sur la zone Nom du modem et cliquez sur **Sélection**. Une boîte de dialogue **Administration du modem du récepteur de radiomessagerie** similaire à celle illustrée dans la figure 28 s'ouvre.

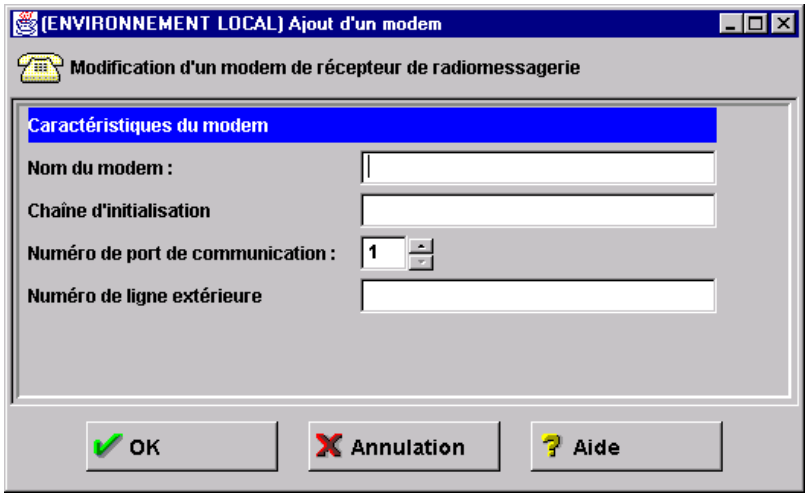

Figure 28. Administration du modem du récepteur de radiomessagerie

Vous pouvez ajouter, modifier ou supprimer différents modems via cette boîte de dialogue.

Ajout d'un modem

Pour ajouter un fichier de définitions de modem, sélectionnez **Création** dans la boîte de dialogue **Administration du modem du récepteur de radiomessagerie** et cliquez sur **Ouverture**. Dans la boîte de dialogue **Ajout d'un modem**, tapez ou sélectionnez les valeurs dans les zones de saisie.

1. Entrez le nom du modem. Il peut être aussi long que vous le souhaitez, sous condition d'être unique et suffisamment explicite.
2. Entrez le numéro du port COM, qui définit le numéro du port série auquel est connecté le modem. Indiquez un nombre inférieur à 10. Alors que le modem doit être configuré au niveau matériel comme étant relié à ce port, il ne doit pas être défini sur Windows NT ; sinon, les fonctions du récepteur de radiomessagerie se verraient refuser l'accès à ce port. Si le modem ne correspond pas aux paramètres matériels, le code du récepteur de messagerie tentera d'accéder au modem de façon répétitive, et ce pendant longtemps avant d'échouer.
3. Entrez la chaîne d'initialisation, qui doit définir le modem comme un modem de données avec un écho sur X level4 et une vitesse en bauds constante définie par le site local. N'incluez pas de commande AT. La fonction du récepteur de radiomessagerie l'insérera au début de la chaîne d'initialisation.
4. Entrez le préfixe de ligne externe. Il s'agit du numéro à composer pour sortir de l'entreprise.
5. Cliquez sur **OK**.

Modification de paramètres du modem

1. Pour modifier un fichier de définitions de modem, sélectionnez un nom de modem dans la boîte de dialogue **Administration du modem du récepteur de radiomessagerie** et cliquez sur **Ouverture**.

   Dans la boîte de dialogue **Modification des paramètres du modem** apparaît une liste de zones relatives à la définition du modem que vous pouvez modifier. Pour des explications détaillées sur ces zones, reportez-vous à la section «Ajout d'un modem».
2. Cliquez sur **OK**.

Suppression d'un modem

1. Pour supprimer un fichier de définitions de modem, sélectionnez un nom de modem dans la boîte de dialogue **Administration du modem du récepteur de radiomessagerie** et cliquez sur **Suppression**.
2. Un message vous invite à confirmer la suppression. Cliquez sur **Oui** pour confirmer.

Journalisation du support de notification du récepteur de radiomessagerie

Le processus de notification du récepteur se sert du journal du pare-feu pour créer des journaux de sortie. Tous les messages et les erreurs générés par le récepteur sont transmis au syslog du pare-feu d'ordre général. Pour plus d'informations sur la configuration et l'utilisation des fichiers journaux du pare-feu, consultez le Chapitre 15, «Gestion des fichiers journaux et des archives», à la page 111.

Test de la configuration du récepteur de radiomessagerie

Pour vérifier la configuration du récepteur, utilisez la commande `pager`. Pour en savoir plus, consultez le *guide de référence d'IBM eNetwork Firewall*. Nous vous conseillons vivement d'utiliser la commande du récepteur chaque fois que vous définissez ou modifier la configuration, afin de vous assurer que le système, le modem, l'opérateur et les récepteurs sont compatibles et que l'envoi et la réception de messages sont possibles.

Exécution de commandes

Vous pouvez paramétrer l'exécution d'un programme chaque fois qu'un seuil d'alerte est atteint. Pour spécifier un programme, procédez comme suit :

1. Cliquez sur **Contrôle de journalisation**, puis cliquez deux fois sur **Création**.

   La boîte de dialogue **Ajout d'un contrôle de journalisation** s'ouvre.

2. Dans la zone de liste déroulante **Type de classe**, sélectionnez **Commande d'exécution**. Ce choix active la zone **Nom de fichier de commande** du panneau.

3. Dans la zone **Nom de fichier de commande**, entrez le nom complet du chemin du programme qui doit être appelé lorsqu'un seuil d'alerte est atteint.

   Le pare-feu transmet le message d'alerte dans son intégralité en tant que premier paramètre du programme :

   ```
   Alerte - Nombre total d'échecs d'authentification : ICA0001e
   Alerte - Nombre d'échecs d'authentification de l'utilisateur : ICA0002e
   Alerte - Nombre d'échecs d'authentification de l'hôte : ICA0003e
   Alerte - Seuil de messages : ICA0004e
   ```

Pour une description complète de ces messages, reportez-vous au *guide de référence d'IBM eNetwork Firewall*.

Chapitre 15. Gestion des fichiers journaux et des archives

Ce chapitre explique comment utiliser les fonctions de journalisation par l'intermédiaire du client de configuration. Étant donné que les utilisateurs tentent d'accéder aux hôtes via les divers serveurs d'IBM Firewall, le programme IBM Firewall consigne les entrées dans le fichier journal géré par le `service de journalisation d'IBM Firewall`.

Selon la configuration de votre pare-feu, IBM Firewall peut générer d'importants volumes de données de journalisation. Les entrées peuvent provenir de différents endroits comme par exemple le serveur Socks et les filtres experts. En outre, différents niveaux de gravité peuvent être associés aux fichiers journaux ; par exemple, *le débogage, l'information* ou *l'erreur*. Ce chapitre indique également comment utiliser les fonctions d'administration et d'archivage des journaux pour contrôler la taille des fichiers d'archive et des fichiers journaux.

Création de fichiers journaux et archivage à l'aide du client de configuration

Le client de configuration permet de gérer les fonctions de journalisation et l'archivage des journaux. L'espace disque dont vous disposez doit être suffisant pour contenir toutes les données de journalisation. Le pare-feu fournit une routine de débogage et des messages d'erreur au `fichier journal du pare-feu`. Seul l'administrateur principal du pare-feu dispose d'un accès au `journal du pare-feu`. Les messages d'avertissement sont consignés dans le journal des alertes. Les données d'administration sont consignées dans le journal d'audit.

Pour que les utilitaires de génération d'états fonctionnent correctement, il est important que seuls les messages du journal du pare-feu apparaissent dans leurs fichiers d'entrées. Aucune autre fonction ne doit être dirigée vers le même fichier que le `journal du pare-feu` ; vous devez donc définir la journalisation du pare-feu en conséquence.

Si vous souhaitez que les messages d'avertissement apparaissent dans l'écran principal du client de configuration, les alertes doivent être dirigées vers un fichier nommé `journal des alertes`. Ce fichier doit être exclusif.

Les niveaux de priorité ci-dessous viennent en complément du programme de *débogage*, qui enregistre la plupart des informations. Le niveau *critique* ne concerne que les événements les plus graves survenant au niveau du pare-feu.

- Débogage ;
- Informations ;
- Avertissement ;
- Erreur ;
- Critique.

Nous vous conseillons d'utiliser le niveau *Informations* jusqu'à ce que les procédures de pare-feu soient stables. Vous pourrez ensuite paramétrer le niveau *Avertissement* ou *Erreur* pour réduire l'activité de journalisation et la taille du journal système.

Les niveaux de priorité ne correspondent pas exactement aux suffix des codes de message *(i,e,w,s..)*. Vous devrez probablement apprendre de façon empirique comment *interrompre* certain messages.

Ajout des fonctions de journalisation

À partir de l'arborescence de navigation du client de configuration, cliquez deux fois sur l'icône du dossier Administration système pour en visualiser le contenu. Cliquez deux fois sur l'icône des fichiers journaux pour en visualiser le contenu. Sélectionnez Fonctions de journalisation. La boîte de dialogue **Fonctions de journalisation** s'ouvre, affichant les paramètres de journalisation activés.

1. Sélectionnez **Création** dans la boîte de dialogue **Fonctions de journalisation** et cliquez sur **Ouverture** pour ajouter une entrée du journal système à celles qui sont activées.

   La boîte de dialogue **Ajouter des fonctions de journalisation** s'affiche, comme illustré dans la figure 29.

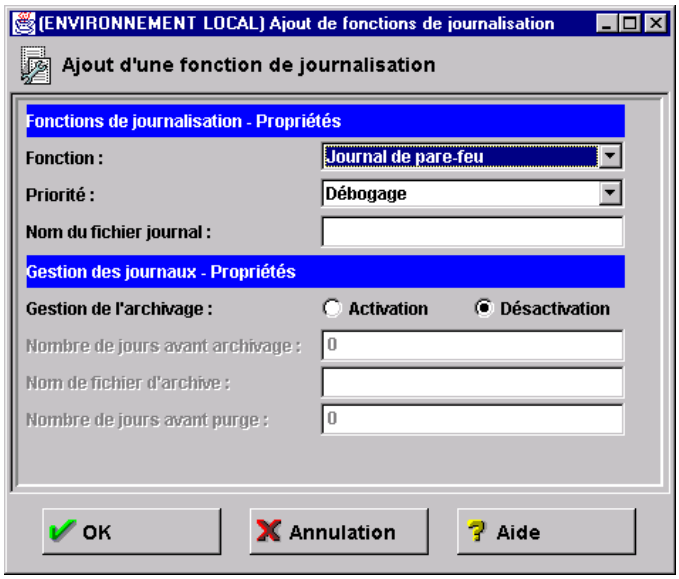

Figure 29. Ajouter des fonctions de journalisation

2. Ouvrez le **menu déroulant** (en cliquant sur la flèche) pour sélectionner le type. Le type correspond au nom de fichier.
3. La fonction de journalisation détermine le type et la source des informations journalisées. Ouvrez le menu déroulant des **fonctions** afin de sélectionner une des fonctions de journalisation suivantes :
   - Journal de pare-feu - journaux de pare-feu d'ordre général, dont une journalisation des filtres ;
   - Journal des alertes - état du démon de contrôle des journaux et avertissements des violations de seuil, utilisés pour compléter l'affichage des messages d'alerte ;
   - Journal de messagerie.
4. Ouvrez le menu déroulant des **priorités** pour sélectionner la priorité. Les priorités de journalisation sont répertoriées par ordre croissant de gravité. Le niveau de priorité sélectionné déterminera le niveau de journalisation minimum.

5. Entrez le nom du fichier journal. Le nom doit contenir le chemin d'accès complet (commençant par une unité et un '/') qui doit exister.
6. La gestion des archives ne peut être utilisée qu'avec une fonction de journalisation de type *nom de fichier*. Une fois activé, le fichier journal peut être compressé à intervalles réguliers. En activant la gestion des archives, vous définissez des paramètres dont dépend la commande `fwlogmgmt`. Voir la section «Archivage des fichiers journaux», à la page 114. Vous pouvez activer ou désactiver les paramètres de gestion d'archives.
7. Sélectionnez le délai en nombre de jours entiers, au-delà duquel les enregistrements d'un journal actif doivent être archivés. Cette valeur doit être supérieure ou égale à zéro. L'archivage est effectué lorsque la commande `fwlogmgmt -l` qui a été lancée détecte des enregistrements de journaux actifs qui répondent à ce critère. La gestion du journal n'inclut pas le jour en cours dans le calcul du nombre de jours d'archivage.
8. Entrez un nom de fichier d'archives et son chemin d'accès complet. IBM Firewall offre une fonction d'archivage par défaut, qui utilise un répertoire. Toutefois, vous pouvez aussi utiliser des fonctions d'archivage plug-in (externes).
9. Sélectionnez le délai en nombre de jours entiers, au-delà duquel un fichier journal archivé doit être supprimé. Cette valeur doit être supérieure ou égale à zéro. La purge est effectuée lorsque la commande `fwlogmgmt -a` qui a été lancée détecte des fichiers archivés qui répondent à ce critère. La gestion du journal n'inclut pas le jour en cours dans le calcul du nombre de jours d'archivage d'un fichier.
10. Cliquez sur **OK**.

Modification des fonctions de journalisation

1. Sélectionnez l'entrée de journalisation de pare-feu à modifier dans la boîte de dialogue **Fonctions de journalisation** et cliquez sur **Ouverture**.

   La boîte de dialogue **Modification des fonctions de journalisation** s'ouvre.
2. Modifiez les zones concernées. Pour une description détaillée des zones, reportez-vous à la section «Ajout des fonctions de journalisation», à la page 112.
3. Cliquez sur **OK**.

Suppression des fonctions de journalisation

1. Sélectionnez une entrée de journalisation du pare-feu de la liste des entrées activées dans la boîte de dialogue **Fonctions de journalisation** et cliquez sur **Suppression**.

   Le panneau **Avertissement - Suppression en cours !** apparaît à l'écran.
2. Cliquez sur **OK** si vous souhaitez poursuivre le processus de suppression. Cliquez sur **Annulation** pour annuler l'opération. Le fichier journal réel n'est pas supprimé.

Archivage des fichiers journaux

Ce processus inclut les opérations suivantes :

- Suppression des enregistrements concernés du journal actif ;
- Déplacement des enregistrements dans un fichier indépendant ;
- Compression du fichier résultant ;
- Déplacement du nouveau fichier dans un répertoire d'archives.

Pour démarrer un programme de journalisation permettant d'archiver les enregistrements des journaux accumulés, vous disposez des deux possibilités suivantes :

1. Lancez de temps en temps la commande `fwlogmgmt -l` depuis la ligne de commande, ou
2. Définissez la commande `fwlogmgmt -l` en tant que service planifié de NT.

La purge des archives de journaux consiste à supprimer les fichiers archivés correspondants du répertoire d'archives.

Pour purger les fichiers archivés, deux méthodes sont à votre disposition :

1. Lancez de temps en temps la commande `fwlogmgmt -a` depuis la ligne de commande, ou
2. Définissez la commande `fwlogmgmt -a` en tant que service planifié de NT.

Les enregistrements et les fichiers qui répondent aux critères sont spécifiés dans les définitions des fonctions de journalisation, comme décrit dans la section «Ajout des fonctions de journalisation», à la page 112.

Le moyen le plus efficace ou le plus pratique pour lancer ce processus consiste à le configurer sous forme de service planifié de NT. Lancez-le en utilisant l'objet Services dans le panneau de configuration.

Par exemple, si vous souhaitez configurer le processus d'archivage pour qu'il s'exécute chaque jour à 3 h du matin, tapez :

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

DLL externes

Pour de plus amples informations concernant les DLL externes que vous pouvez utiliser pour remplacer les DLL par défaut du pare-feu, consultez le *guide de référence IBM eNetwork Firewall*.

Gestion des journaux en sortie

La fonction de gestion des journaux effectue certains contrôles d'intégrité préliminaires avant de prendre en charge des activités d'administration. En cas de problème, les diagnostics sont envoyés au journal du pare-feu lorsque vous lancez la commande `fwlogmgmt` depuis la ligne de commande.

Les fonctions de journalisation de la messagerie ou d'audit (local0) sont soumises à des règles d'archivage qui diffèrent de celles des autres fonctions. L'archivage des journaux exigent que la fonction ait été activée. Toutefois, les enregistrements des

journaux du pare-feu (local4) et des alertes (local1) sont archivés uniquement si leurs dates sont postérieures à celles utilisées par la fonction au moment de l'exécution de la procédure d'archivage, alors que l'*intégralité* du fichier journal de messagerie ou d'audit est archivé à chaque exécution. En outre, les informations stockées dans le journal de la messagerie sont utilisées à des fins de débogage et leur archivage est de moindre intérêt. En revanche, le journal du pare-feu (local4) contient des informations généralement plus utiles.

Utilitaires de génération d'états

Vous pouvez faire appel aux fonctions de l'utilitaire d'édition d'états pour vous aider à générer des états à partir des fichiers journaux courants ou archivés. Ces utilitaires génèrent des fichiers de tableaux contenant des informations d'ordre administratif, organisés et mis en forme de façon à faciliter la mise en correspondance avec les tableaux des bases de données relationnelles. Ces tableaux aident l'administrateur du pare-feu à analyser les éléments suivants :

- Utilisation générale du pare-feu ;
- Erreurs liées au pare-feu ;
- Tentatives d'accès non autorisées au réseau sécurisé.

Avec les utilitaires et le journal du pare-feu, l'administrateur peut créer un fichier texte ordinaire contenant les messages. En outre, les fichiers sous forme de tableaux peuvent être générés et importés dans des tableaux d'un système de gestion de base de données relationnelle, comme la famille de produits DB2. L'administrateur peut ensuite utiliser SQL (Structured Query Language) pour lancer des requêtes et générer des états.

Les utilitaires de génération d'états sont installés en même temps que le pare-feu. Ils peuvent également être installés séparément et exécutés sur un hôte qui n'est pas un pare-feu. Le client de configuration peut les exécuter sur un pare-feu. Sur une machine qui ne dispose pas d'un pare-feu, utilisez la ligne de commande.

Pour que les utilitaires de génération d'états fonctionnent correctement, il est important que seuls les messages du `journal du pare-feu` apparaissent dans les fichiers d'entrée. Aucune autre fonction ne doit être dirigée vers le même fichier que le `journal du pare-feu` ; vous devez donc définir la journalisation du pare-feu en conséquence.

N'essayez pas d'employer les utilitaires de génération d'états sur des fichiers journaux antérieurs à IBM Firewall pour AIX version 3.1. Vous pouvez en revanche les utiliser pour traiter les journaux d'IBM Firewall d'AIX version 3.1 ou postérieure. Vous pouvez également les utiliser pour traiter les journaux SU AIX. Pour de plus amples informations sur les utilitaires de génération d'états, reportez-vous au *guide de référence d'IBM eNetwork Firewall*.

Exécution des utilitaires de génération d'états à l'aide du client de configuration

À partir de l'arborescence de navigation du client de configuration, cliquez deux fois sur l'icône du dossier Administration système pour en visualiser le contenu. Cliquez deux fois sur l'icône des fichiers journaux pour en visualiser le contenu. Sélectionnez **Utilitaires de génération d'états**. La boîte de dialogue **Utilitaires de génération d'états** s'ouvre, comme illustré dans la figure 30, à la page 117.

1. Pour l'outil d'archivage fourni avec IBM Firewall, le chemin d'accès au fichier d'archive des journaux est le répertoire qui contient les fichiers journaux compressés. Dans la zone Chemin d'accès au fichier d'archive des journaux, entrez le nom de répertoire que vous avez spécifié dans la zone associée au répertoire d'archive de la boîte de dialogue **Fonctions de journalisation**. Précisez le chemin d'accès complet au répertoire d'archives. Pour afficher un fichier journal qui n'est pas archivé, ne complétez pas cette zone.
2. Sélectionnez le **type d'état**. Pour visualiser l'intégralité du texte du journal des messages, sélectionnez **Fichier journal texte**. Pour créer des fichiers sous forme de tableaux à utiliser avec DB2, sélectionnez **Journal des tables**. Si vous importez les fichiers obtenus dans DB2, vous pouvez exécuter des requêtes SQL sur les données consignées. Pour plus d'informations, reportez-vous au *guide de référence d'IBM eNetwork Firewall*.
3. Le nom du fichier journal correspond à l'un des fichiers d'archives compressés ou à un autre `journal du pare-feu` valide, ou bien encore à un fichier journal su AIX. Si vous avez complété la zone correspondant au nom du répertoire d'archive, cliquez sur la flèche associée à la zone **Nom du fichier journal** pour choisir le journal à utiliser. Si vous n'avez pas complété cette zone, vous devez saisir ici le nom correct d'un fichier journal pare-feu non compressé, ou d'un fichier journal su AIX. Vous devez spécifier un chemin d'accès complet.
4. Sélectionnez le **type de journal**, **pare-feu** ou **su d'AIX**.
5. Entrez le **nom du fichier et le chemin d'accès au texte de sortie**.
6. Sélectionnez **Oui** pour ajouter les résultats d'une demande de journal sous forme de tableau aux fichiers de tableaux existants, ou choisissez **Non** pour remplacer les fichiers existants.
7. Cette zone vous permet de sélectionner certains types de messages à copier dans le fichier texte de sortie. Le contenu de la zone est considéré comme les paramètres d'une commande `Recherche` standard sous Windows NT. Par exemple, si vous entrez "ICA0" dans la zone (vous devez intégrer les guillemets), c'est comme si vous exécutiez la commande suivante :

   ```
   fwlogtxt < my.log | find "ICA0"
   ```

   Voici certaines entrées types que vous pouvez définir dans cette zone et les résultats qui s'ensuivent :

   ```
   FILTRE                          RÉSULTAT
   "ICA0"          Affiche les messages d'avertissement des seuils dans
                   le cadre du contrôle de journalisation
   "ICA3"          Affiche des messages relatifs à Socks (#ICA3000 - 3999)
   "ICA2010"       Affiche uniquement les occurrences du message ICA2010
   /V "ICA3"       Affiche tous les messages à l'exception de ceux relatifs à Socks
   /C "ICA001"     Compte le nombre de messages ICA0001
   ```

8. Lorsque vous cliquez sur **OK**, le fichier demandé est transféré dans le répertoire de sortie spécifié sur la machine du pare-feu.
9. La zone Résultats des utilitaires de génération d'états affiche tous les messages d'erreur générés par l'utilitaire qui a été exécuté. Pour visualiser le texte d'un état de fichier journal texte, cliquez sur **Affichage des journaux** dans l'écran principal du client de configuration du pare-feu, et entrez le nom du fichier de sortie complet. Les fichiers .tbl résultant d'un état du journal des tables peuvent être chargés dans une base de données, comme indiqué dans le *guide de référence d'IBM eNetwork Firewall*..

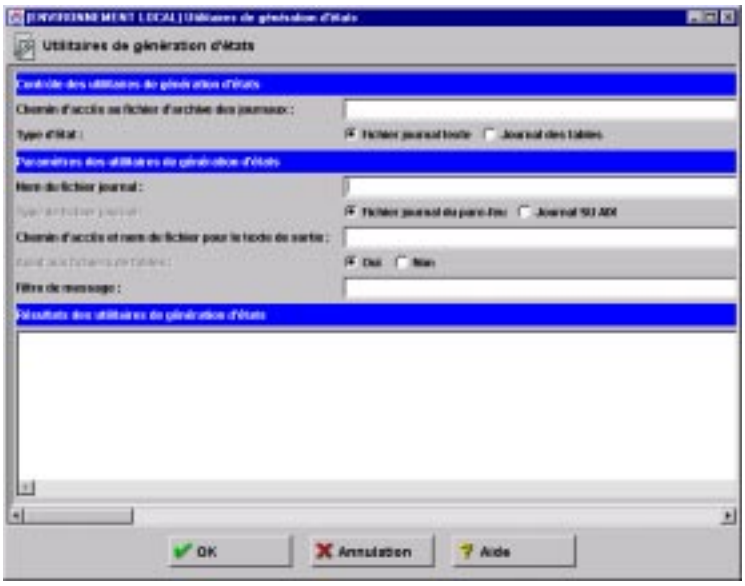

Figure 30. Utilitaires de génération d'états

Annexe A. 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 QUALITÉ MARCHANDE OU D'ADAPTATION À VOS BESOINS SONT EXPRESSÉMENT 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 brevet. 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

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

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
U.S.A.

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

Ce produit comprend des logiciels développés par l'université de Berkeley en Californie et ses collaborateurs.

Marques

Les termes suivants sont des marques d'International Business Machine Corporation dans certains pays :

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft, Windows, Windows NT et le logo Windows 95 sont des marques de Microsoft Corporation.

Java et HotJava sont des marques de Sun Microsystems, Inc.

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

Bibliographie

Pour plus d'informations sur la sécurité dans l'environnement Internet, consultez la page d'accueil d'IBM eNetwork Firewall à l'adresse suivante : **http://www.software.ibm.com/enetwork/firewall**.

Informations contenues dans les publications IBM

Les autres sources d'informations d'IBM sur les pare-feu, la sécurité sur Internet et la sécurité en général sont répertoriées ci-dessous.

Pare-feu

Les documents suivants sont fournis avec le CD-ROM d'IBM Firewall et sont disponibles sur la page d'accueil d'IBM eNetwork Firewall.

- *Guide de l'utilisateur d'IBM eNetwork Firewall*, GC11-1459-00
- *Guide de référence d'IBM eNetwork Firewall*, SC11-1460-00

Internet et le Web

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Sécurité générale

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Publications informatiques

Publications consacrées à TCP/IP et UNIX :

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

Publications consacrées aux pare-feu et à la sécurité dans l'environnement Internet :

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)

- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Glossaire

Vous pouvez accéder au glossaire IBM Software à l'adresse suivante : **http://www.networking.ibm.com/nsg/nsgmain.htm**.

Index

T

U

REMARQUES DU LECTEUR

Réf. : GC11-1459-00

Titre : IBM eNetwork Firewall pour Windows

Guide de l'utilisateur

Vos commentaires nous permettent d'améliorer la qualité de nos documents : ils jouent un rôle important lors de leur mise à jour.

Si vous avez des observations sur le(s) document(s) ci-joint(s), nous vous serions reconnaissants de nous en faire part en les faisant précéder, au besoin, des rubriques ou des numéros de pages et de lignes concernés. Elles seront étudiées avec le plus grand soin par les responsables du Centre de francisation.

Par ailleurs, nous vous rappelons que pour toute question technique ou pour toute demande de document, vous devez vous adresser à votre partenaire commercial IBM.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie de ces informations que, de votre côté, vous pourrez évidemment continuer à exploiter.

Envoyez vos remarques à :

Pour la France	Pour le Canada
IBM FRANCE	**IBM CANADA Ltée**
Centre de francisation	**Services linguistiques**
4, avenue Montaigne	**1250, boul. René-Levesque ouest**
93881 Noisy-le-Grand Cedex	**Montréal (Québec) H3B 4W2**

Si vous désirez une réponse, n'oubliez pas de mentionner vos nom et adresse.

Merci de votre collaboration.

MODIFICATIONS OU ÉCLAIRCISSEMENTS DEMANDÉS :

Page ou rubrique *Commentaires*

Compagnie IBM France
Tour Septentrion
20, avenue André Prothin
La Défense 4
92400 Courbevoie

Document réalisé et composé par le Centre de francisation

à Noisy-le-Grand

Avril 1998

Imprimé au Danemark par IBM Danmark A/S.

GC11-1459-00