Sécurisation du réseau dans Oracle® Solaris 11.1

Référence : E36644–02
Février 2013

ORACLE

130327@25097

Table des matières

Préface

Dans ce guide, il est supposé que le Système d'exploitation Oracle Solaris (SE Oracle Solaris) est installé et que vous êtes prêt à sécuriser votre réseau.

Remarque – Cette version d'Oracle Solaris prend en charge des systèmes utilisant les architectures de processeur SPARC et x86. Les systèmes pris en charge sont répertoriés dans les listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*. Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

Utilisateurs de ce manuel

Ce manuel s'adresse aux personnes chargées de l'administration de systèmes en réseau exécutant Oracle Solaris. Pour utiliser ce manuel, vous devez avoir au moins deux ans d'expérience en administration de systèmes UNIX. Une formation en administration de systèmes UNIX peut se révéler utile.

Accès aux services de support Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P–1 Conventions typographiques

Type de caractères	Description	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

Le tableau suivant présente les invites système UNIX et les invites superutilisateur pour les shells faisant partie du système d'exploitation Oracle Solaris. Dans les exemples de commandes, l'invite de shell indique si la commande doit être exécutée par un utilisateur standard ou un utilisateur doté des privilèges nécessaires.

TABLEAU P–2 Invites de shell

Shell	Invite
Shell Bash, shell Korn et shell Bourne	`$`
Shell Bash, shell Korn et shell Bourne pour superutilisateur	`#`
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

1 Utilisation de la protection des liens dans des environnements virtualisés

Ce chapitre décrit la protection des liens et leur configuration sur un système Oracle Solaris. Ce chapitre comprend les sections suivantes :

Présentation de la protection des liens

Avec la généralisation de la virtualisation dans les configurations système, un administrateur hôte peut accorder à des machines virtuelles (VM) invitées un accès exclusif à un lien physique ou virtuel. Cette configuration améliore les performances du réseau en permettant au trafic du réseau de l'environnement virtuel d'être isolé du trafic général envoyé ou reçu par le système hôte. Dans le même temps, cette configuration peut exposer le système et l'ensemble du réseau à des paquets nuisibles susceptibles d'être générés par un environnement invité.

La protection des liens vise à prévenir les dommages pouvant être causés par des machines virtuelles potentiellement dangereuses invitées sur le réseau. Cette fonction offre une protection contre les menaces de base suivantes :

- Usurpation IP, DHCP et MAC
- Usurpation de trame de niveau 2 telle que les attaques BPDU (Bridge Protocol Data Unit)

Remarque – La protection des liens ne remplace pas le déploiement d'un pare-feu, en particulier pour des configurations présentant des besoins de filtrage complexes.

Types de protection des liens

Le mécanisme de protection des liens dans Oracle Solaris fournit les types de protection suivants :

`mac-nospoof`
: Active la protection contre l'usurpation de l'adresse MAC du système. Si le lien appartient à une zone, l'activation de `mac-nospoof` empêche le propriétaire de la zone de modifier l'adresse MAC du lien.

`ip-nospoof`
: Active la protection contre l'usurpation d'IP. Par défaut, les paquets sortants avec des adresses DHCP et des adresses IPv6 locales de lien sont autorisés.

  Vous pouvez ajouter des adresses à l'aide de la propriété de lien `allowed-ips`. Pour les adresses IP, l'adresse source du paquet doit correspondre à une adresse de la liste `allowed-ips`. Pour un paquet ARP, l'adresse du protocole de l'expéditeur du paquet doit se trouver dans la liste `allowed-ips`.

`dhcp-nospoof`
: Active la protection contre l'usurpation du client DHCP. Par défaut, les paquets DHCP dont l'ID correspond à l'adresse MAC du système sont autorisés.

  Vous pouvez ajouter des clients autorisés à l'aide de la propriété de lien `allowed-dhcp-cids`. Les entrées de la liste `allowed-dhcp-cids` doivent être formatées comme indiqué dans la page de manuel `dhcpagent(1M)`.

`restricted`
: Limite les paquets sortants aux paquets IPv4, IPv6 et ARP. Ce type de protection a été conçu pour empêcher le lien de générer des trames de contrôle de niveau 2 potentiellement dangereuses.

Remarque – Les paquets ignorés en raison de la protection des liens font l'objet d'un suivi par les statistiques du noyau pour les quatre types de protection : `mac_spoofed`, `dhcp_spoofed`, `ip_spoofed` et `restricted`. Pour consulter ces statistiques par lien, reportez-vous à la section "Affichage de la configuration et des statistiques de protection des liens" à la page 16.

Configuration de la protection des liens (liste des tâches)

Pour utiliser la protection des liens, définissez la propriété `protection` du lien. Si le type de protection fonctionne avec d'autres fichiers de configuration, tels que `ip-nospoof` avec `allowed-ips` ou `dhcp-nospoof` avec `allowed-dhcp-cids`, vous devez effectuer deux opérations globales. Vous devez tout d'abord activer la protection des liens. Puis vous devez personnaliser le fichier de configuration pour identifier les autres paquets dont la transmission est autorisée.

Remarque – Vous devez configurer la protection des liens dans la zone globale.

La liste des tâches suivante indique les procédures de configuration de la protection des liens sur un système Oracle Solaris.

Tâche	Description	Voir
Activation de la protection des liens	Limite les paquets envoyés à partir d'un lien et protège les liens contre l'usurpation.	"Activation de la protection des liens" à la page 13
Désactivation de la protection des liens	Supprime les protections des liens.	"Désactivation de la protection des liens" à la page 14
Spécification du type de protection des liens IP	Indique les adresses IP autorisées à traverser le mécanisme de protection des liens.	"Spécification des adresses IP pour la protection contre l'usurpation d'adresses IP" à la page 14
Spécification du type de protection des liens DHCP	Indique les adresses DHCP autorisées à traverser le mécanisme de protection des liens.	"Spécification des clients DHCP pour assurer une protection contre l'usurpation d'adresses DHCP" à la page 15
Affichage de la configuration de la protection des liens	Répertorie les liens protégés et les exceptions, et présente les statistiques de mise en oeuvre.	"Affichage de la configuration et des statistiques de protection des liens" à la page 16

▼ Activation de la protection des liens

Cette procédure restreint les types de paquets sortants et empêche l'usurpation des liens.

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Link Security (sécurité des liens du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Affichez les types de protection des liens disponibles.

```
# dladm show-linkprop -p protection
LINK      PROPERTY      PERM VALUE    DEFAULT    POSSIBLE
vnic0     protection    rw   --       --         mac-nospoof,
                                                 restricted,
                                                 ip-nospoof,
                                                 dhcp-nospoof
```

Pour obtenir une description des types possibles, reportez-vous à la section "Types de protection des liens" à la page 11 et à la page de manuel `dladm`(1M).

2 Activez la protection des liens en spécifiant un ou plusieurs types de protection.

`# dladm set-linkprop -p protection=`*value*`[,`*value*`,...]`** *link*

Dans l'exemple suivant, les quatre types de protection des liens sont activés sur le lien `vnic0` :

```
# dladm set-linkprop \
-p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof vnic0
```

3 **Vérifiez que les protections des liens sont activées.**

```
# dladm show-linkprop -p protection vnic0
LINK     PROPERTY        PERM VALUE          DEFAULT       POSSIBLE
vnic0    protection      rw   mac-nospoof    --            mac-nospoof,
                              restricted                   restricted,
                              ip-nospoof                   ip-nospoof,
                              dhcp-nospoof                 dhcp-nospoof
```

Le type de protection des liens sous `VALUE` indique que la protection est activée.

▼ Désactivation de la protection des liens

Cette procédure permet de réinitialiser la protection des liens sur la valeur par défaut, pas de protection des liens.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Link Security (sécurité des liens du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 **Désactivez la protection des liens en réinitialisant la propriété `protection` sur sa valeur par défaut.**

```
# dladm reset-linkprop -p protection link
```

2 **Vérifiez que les protections de liens sont désactivées.**

```
# dladm show-linkprop -p protection vnic0
LINK      PROPERTY      PERM VALUE    DEFAULT    POSSIBLE
vnic0     protection    rw   --       --         mac-nospoof,
                                                 restricted,
                                                 ip-nospoof,
                                                 dhcp-nospoof
```

Aucune liste d'un type de protection des liens sous `VALUE` n'indique que la protection des liens est désactivée.

▼ Spécification des adresses IP pour la protection contre l'usurpation d'adresses IP

Avant de commencer Le type de protection `ip-nospoof` est activé, comme indiqué dans la section "Activation de la protection des liens" à la page 13.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Link Security (sécurité des liens du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Vérifiez que vous avez activé la protection contre l'usurpation d'adresses IP.**

```
# dladm show-linkprop -p protection link
LINK     PROPERTY        PERM    VALUE          DEFAULT       POSSIBLE
link     protection      rw      ...
                                 ip-nospoof                   ip-nospoof
```

   L'affichage de `ip-nospoof` sous `VALUE` indique que ce type de protection est activé.

2. **Ajoutez des adresses IP à la liste des valeurs par défaut pour la propriété de lien `allowed-ips`.**

```
# dladm set-linkprop -p allowed-ips=IP-addr[,IP-addr,...] link
```

   L'exemple suivant illustre l'ajout des adresses IP `10.0.0.1` et `10.0.0.2` à la propriété `allowed-ips` du lien `vnic0` :

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 vnic0
```

   Pour plus d'informations, reportez-vous à la page de manuel `dladm`(1M).

▼ Spécification des clients DHCP pour assurer une protection contre l'usurpation d'adresses DHCP

Avant de commencer

Le type de protection `dhcp-nospoof` est activé, comme indiqué dans la section "Activation de la protection des liens" à la page 13.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Link Security (sécurité des liens du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Vérifiez que vous avez activé la protection contre l'usurpation d'adresses DHCP.**

```
# dladm show-linkprop -p protection link
LINK     PROPERTY        PERM    VALUE          DEFAULT       POSSIBLE
link     protection      rw      ...
                                 dhcp-nospoof                 dhcp-nospoof
```

   L'affichage de `dhcp-nospoof` sous `VALUE` indique que ce type de protection est activé.

2. **Indiquez une phrase ASCII pour la propriété de lien `allowed-dhcp-cids`.**

```
# dladm set-linkprop -p allowed-dhcp-cids=CID-or-DUID[,CID-or-DUID,...] link
```

   L'exemple suivant indique comment spécifier la chaîne `hello` en tant que valeur de la propriété `allowed-dhcp-cids` du lien `vnic0` :

```
# dladm set-linkprop -p allowed-dhcp-cids=hello vnic0
```

   Pour plus d'informations, reportez-vous à la page de manuel `dladm`(1M).

▼ Affichage de la configuration et des statistiques de protection des liens

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Link Security (sécurité des liens du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Affichez les valeurs des propriétés de protection des liens.

```
# dladm show-linkprop -p protection,allowed-ips,allowed-dhcp-cids link
```

L'exemple suivant affiche les valeurs des propriétés `protection`, `allowed-ips` et `allowed-dhcp-cids` du lien `vnic0` :

```
# dladm show-linkprop -p protection,allowed-ips,allowed-dhcp-cids vnic0
LINK    PROPERTY            PERM     VALUE           DEFAULT    POSSIBLE
vnic0   protection          rw       mac-nospoof     --         mac-nospoof,
                                     restricted                 restricted,
                                     ip-nospoof                 ip-nospoof,
                                     dhcp-nospoof               dhcp-nospoof
vnic0   allowed-ips         rw       10.0.0.1,       --         --
                                     10.0.0.2
vnic0   allowed-dhcp-cids   rw       hello           --         --
```

Remarque – La propriété `allowed-ips` n'est utilisée que si `ip-nospoof` est activé, comme indiqué sous `VALUE`. La propriété `allowed-dhcp-cids` n'est utilisée que si `dhcp-nospoof` est activé.

2 Affichez les statistiques de la protection des liens

La sortie de la commande `dlstat` est validée, cette commande est donc appropriée pour les scripts.

```
# dlstat -A
...
 vnic0
  mac_misc_stat
               multircv                      0
              brdcstrcv                      0
               multixmt                      0
              brdcstxmt                      0
           multircvbytes                     0
            bcstrcvbytes                     0
           multixmtbytes                     0
            bcstxmtbytes                     0
                txerrors                     0
              macspoofed                     0  <----------
               ipspoofed                     0  <----------
             dhcpspoofed                     0  <----------
              restricted                     0  <----------
                ipackets                     3
                  rbytes                   182
...
```

La sortie indique qu'il n'y a eu aucune tentative de transmission d'un paquet falsifié ou faisant l'objet d'une restriction.

Vous pouvez utiliser la commande `kstat`, mais la sortie correspondante n'est pas validée. Par exemple, la commande suivante affiche les statistiques `dhcpspoofed` :

```
# kstat vnic0:0:link:dhcpspoofed
module: vnic0                           instance: 0
name:   link                            class:    vnic
        dhcpspoofed                     0
```

Pour plus d'informations, reportez-vous aux pages de manuel `dlstat(1M)` et `kstat(1M)`.

◆ ◆ ◆ CHAPITRE 2

Réglage du réseau (tâches)

Ce chapitre explique le réglage des paramètres réseau qui affectent la sécurité dans Oracle Solaris.

Réglage du réseau (liste des tâches)

Tâche	Description	Voir
Désactivation du démon de routage du réseau.	Limite l'accès aux systèmes par des renifleurs de réseau	"Désactivation du démon de routage du réseau" à la page 20
Prévention de la diffusion d'informations sur la topologie du réseau.	Empêche la diffusion de paquets.	"Désactivation du transfert de paquets de diffusion" à la page 21
	Désactivation des réponses aux demandes d'écho de diffusion et aux demandes d'écho multidiffusion.	"Désactivation des réponses aux demandes d'écho" à la page 21
Pour les systèmes constituant des passerelles vers d'autres domaines, tels qu'un pare-feu ou un noeud de réseau privé virtuel (VPN), activation du multihébergement strict de la source et de la destination.	Empêche les paquets qui ne possèdent pas dans leur en-tête l'adresse de la passerelle de se déplacer au-delà de la passerelle.	"Définition du multihébergement strict" à la page 22
Prévention des attaques DOS en contrôlant le nombre de connexions incomplètes au système.	Limite le nombre maximal de connexions TCP incomplètes pour un processus d'écoute TCP.	"Définition du nombre maximal de connexions TCP incomplètes" à la page 23
Prévention des attaques DOS en contrôlant le nombre de connexions entrantes autorisées.	Spécifie le nombre maximal par défaut de connexions TCP en attente pour un processus d'écoute TCP.	"Définition du nombre maximal de connexions TCP en attente" à la page 23

Tâche	Description	Voir
Génération de nombres aléatoires forts pour les connexions TCP initiales.	Respecte la valeur de génération de numéro de séquence spécifiée par RFC 6528.	"Spécification d'un numéro aléatoire fort pour la connexion TCP initiale" à la page 24
Prévention de la redirection ICMP.	Supprime les indicateurs de la topologie du réseau.	"Prévention des redirections ICMP" à la page 24
Restauration des valeurs sécurisées par défaut des paramètres réseau.	Renforce la sécurité lorsqu'elle a été réduite par des actions d'administration.	"Réinitialisation des paramètres réseau sur des valeurs sécurisées" à la page 25

▼ Désactivation du démon de routage du réseau

Cette procédure permet d'empêcher le routage réseau après l'installation en spécifiant un routeur par défaut. Cette procédure peut aussi être effectuée après une configuration manuelle du routage.

Remarque – De nombreuses procédures de configuration requièrent la désactivation du démon de routage. Vous avez donc peut-être désactivé ce démon dans le cadre d'une procédure de configuration générale.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Assurez-vous que le démon de routage est en cours d'exécution.

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

Si le service n'est pas en cours d'exécution, vous pouvez vous arrêter ici.

2 Désactivez le démon de routage.

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 Vérifiez que le démon de routage est désactivé.

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
```

```
Reason: Disabled by an administrator.
   See: http://support.oracle.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

Voir aussi Page de manuel `routeadm(1M)`

▼ Désactivation du transfert de paquets de diffusion

Par défaut, Oracle Solaris transmet les paquets de diffusion. Si la stratégie de sécurité de votre site exige une réduction du risque de saturation par diffusions, modifiez la valeur par défaut à l'aide de cette procédure.

Remarque – En désactivant la propriété `_forward_directed_broadcasts`, vous désactivez les commandes ping des diffusions.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Définissez sur 0 la propriété de transfert des paquets de diffusion pour les paquets IP.

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2 Contrôlez la valeur en cours.

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts rw   0         --           0         0,1
```

Voir aussi Page de manuel `ipadm(1M)`

▼ Désactivation des réponses aux demandes d'écho

Cette procédure permet d'empêcher la diffusion d'informations sur la topologie du réseau.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Définissez sur 0 la propriété de réponse aux demandes d'écho de diffusion pour les paquets IP, puis contrôlez la valeur en cours.**

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2. **Définissez sur 0 la propriété de réponse aux demandes d'écho multidiffusion pour les paquets IP, puis contrôlez la valeur en cours.**

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

Voir aussi Pour plus d'informations, reportez-vous à la section "_respond_to_echo_broadcast et _respond_to_echo_multicast (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1* et à la page de manuel `ipadm`(1M).

▼ Définition du multihébergement strict

Pour les systèmes constituant des passerelles vers d'autres domaines, tels qu'un pare-feu ou un noeud de réseau privé virtuel (VPN), cette procédure permet d'activer le multihébergement strict. La propriété `hostmodel` contrôle le comportement d'envoi et de réception de paquets IP sur un système multihébergé.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Définissez la propriété `hostmodel` sur `strong` pour les paquets IP.**

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2. **Vérifiez la valeur actuelle et notez les valeurs possibles.**

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

Voir aussi Pour plus d'informations, reportez-vous à la section "hostmodel (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1* et à la page de manuel `ipadm`(1M).

Pour plus d'informations sur l'utilisation du multihébergement strict, reportez-vous à la section Protection d'un VPN avec IPsec en mode Tunnel.

▼ Définition du nombre maximal de connexions TCP incomplètes

Cette procédure permet d'empêcher les attaques par déni de service en contrôlant le nombre de connexions en attente incomplètes.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Définissez le nombre maximal de connexions entrantes.

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2 Contrôlez la valeur en cours.

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0  rw   4096      --           128       1-4294967295
```

Voir aussi Pour plus d'informations, reportez-vous à la section "_conn_req_max_q0" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1* et à la page de manuel `ipadm`(1M).

▼ Définition du nombre maximal de connexions TCP en attente

Cette procédure permet d'empêcher les attaques par déni de service en contrôlant le nombre de connexions entrantes autorisées.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Définissez le nombre maximal de connexions entrantes.

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2 Contrôlez la valeur en cours.

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

Voir aussi Pour plus d'informations, reportez-vous à la section "_conn_req_max_q" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1* et à la page de manuel `ipadm`(1M).

▼ Spécification d'un numéro aléatoire fort pour la connexion TCP initiale

Cette procédure définit le paramètre de génération du numéro de séquence initial TCP de manière à ce qu'il soit conforme à RFC 6528 (`http://www.ietf.org/rfc/rfc6528.txt`).

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant de l'autorisation `solaris.admin.edit/etc.default/inetinit` . Par défaut, le rôle `root` dispose de cette autorisation. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Modifiez la valeur par défaut de la variable `TCP_STRONG_ISS`.

```
# pfedit /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

2 Réinitialisez le système.

```
# /usr/sbin/reboot
```

▼ Prévention des redirections ICMP

Les routeurs utilisent les messages de redirection ICMP afin d'informer les hôtes de l'existence de routes plus directes vers une destination. Un message de redirection ICMP illicite risque de provoquer une attaque Man-in-the-middle.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Définissez sur 1 la propriété ignorer les réacheminements, puis contrôlez la valeur en cours.**

   Les messages de redirection ICMP modifient la table de routage de l'hôte et ne sont pas authentifiés. En outre, le traitement de paquets redirigés augmente la sollicitation de la CPU des systèmes.

```
# ipadm set-prop -p _ignore_redirect=1 ipv4
# ipadm set-prop -p _ignore_redirect=1 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4  _ignore_redirect  rw   1         1            0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6  _ignore_redirect  rw   1         1            0         0,1
```

2. **Empêchez l'envoi de messages de redirection ICMP.**

   Les messages de ce type incluent des informations issues de la table de routage qui peuvent révéler une partie de la topologie du réseau.

```
# ipadm set-prop -p _send_redirects=0 ipv4
# ipadm set-prop -p _send_redirects=0 ipv6
# ipadm show-prop -p _send_redirects ipv4
PROTO PROPERTY          PERM CURRENT  PERSISTENT   DEFAULT  POSSIBLE
ipv4  _send_redirects   rw   0        0            1        0,1

# ipadm show-prop -p _send_redirects ipv6
PROTO  PROPERTY        PERM CURRENT   PERSISTENT   DEFAULT  POSSIBLE
ipv6  _send_redirects  rw   0         0            1        0,1
```

   Pour plus d'informations, reportez-vous à la section "_send_redirects (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1* et à la page de manuel `ipadm`(1M).

▼ Réinitialisation des paramètres réseau sur des valeurs sécurisées

De nombreux paramètres réseau, sécurisés par défaut, sont réglables et peuvent donc avoir été modifiés. Si les conditions du site le permettent, restaurez les valeurs par défaut des paramètres réglables suivants.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Management (gestion du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 **Définissez sur 0 la propriété de transfert des packages source pour les paquets IP, puis contrôlez la valeur en cours.**

La valeur par défaut empêche les attaques par déni de service provenant de paquets falsifiés.

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

Pour plus d'informations, reportez-vous à la section "forwarding (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1*.

2 **Définissez sur 0 la propriété de réponse netmask pour les paquets IP, puis contrôlez la valeur en cours.**

La valeur par défaut empêche la diffusion d'informations sur la topologie du réseau.

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 **Définissez sur 0 la propriété de réponse de l'horodatage pour les paquets IP, puis contrôlez la valeur en cours.**

La valeur par défaut supprime les demandes supplémentaires des unités centrales par rapport aux systèmes et empêche la diffusion d'informations sur le réseau.

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp          rw   0         --           0         0,1
```

4 **Définissez sur 0 la propriété de réponse de diffusion de l'horodatage pour les paquets IP, puis contrôlez la valeur en cours.**

La valeur par défaut supprime les demandes supplémentaires des unités centrales par rapport aux systèmes et empêche la diffusion d'informations sur le réseau.

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast rw   0         --           0         0,1
```

5 **Empêchez le routage IP par la source.**

La valeur par défaut empêche les paquets de passer outre les mesures de sécurité du réseau. Les paquets routés par la source autorisent la source du paquet à suggérer un chemin différent du chemin configuré sur le routeur.

Remarque – Ce paramètre peut être défini sur `1` à des fins de diagnostic. Une fois le diagnostic terminé, revenez à la valeur `0`.

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
PROTO PROPERTY          PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp   _rev_src_routes   rw   0        --          0        0,1
```

Pour plus d'informations, reportez-vous à la section "_rev_src_routes" du manuel *Manuel de référence des paramètres réglables Oracle Solaris 11.1*.

Voir aussi Page de manuel `ipadm(1M)`

◆ ◆ ◆ CHAPITRE 3

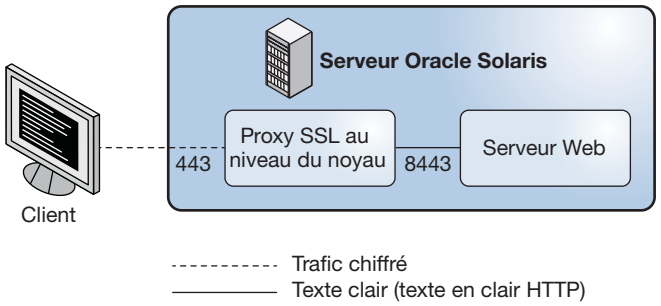
Serveurs Web et protocole SSL (Secure Sockets Layer)

Cette section décrit l'utilisation du protocole SSL (Secure Sockets Layer) pour chiffrer et accélérer les communications des serveurs Web d'un système Oracle Solaris.

Le proxy SSL au niveau du noyau chiffre les communications des serveurs Web

Tout serveur Web qui s'exécute sur Oracle Solaris peut être configuré de manière à utiliser le protocole SSL au niveau du noyau, c'est-à-dire le proxy SSL au niveau du noyau. C'est le cas par exemple du serveur Web Apache 2.2 et du serveur Oracle iPlanet Web Server. Le protocole SSL assure la confidentialité, l'intégrité des messages et l'authentification des points d'extrémité entre deux applications. Lorsque le proxy SSL au niveau du noyau s'exécute sur le serveur Web, les communications sont accélérées. L'illustration suivante présente la configuration de base.

FIGURE 3–1 Communications du serveur Web chiffrées par le noyau



Le proxy SSL au niveau du noyau met en oeuvre le côté serveur du protocole SSL. Il offre plusieurs avantages.

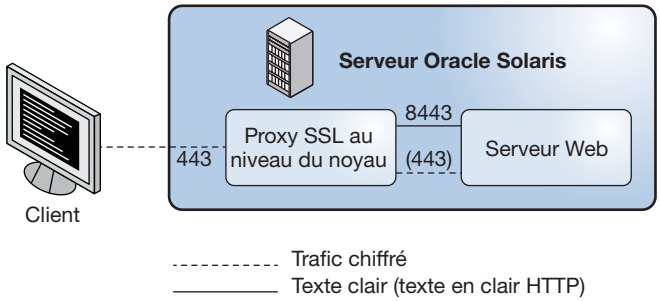
- Le proxy accélère les performances SSL pour les applications serveur, telles que les serveurs Web, de manière à ce qu'elles offrent de meilleures performances que des applications utilisant des bibliothèques SSL au niveau de l'utilisateur. L'amélioration des performances peut dépasser 35%, en fonction de la charge de travail de l'application.
- Le proxy SSL au niveau du noyau est transparent. Aucune adresse IP ne lui est affectée. Par conséquent, les serveurs Web voient les adresses IP client réelles et les ports TCP.
- Le proxy SSL au niveau du noyau et les serveurs Web sont conçus pour fonctionner ensemble.

  La Figure 3–1 illustre un scénario de base avec un serveur Web utilisant le proxy SSL au niveau du noyau. Le proxy SSL au niveau du noyau est configuré sur le port 443, tandis que le serveur Web est configuré sur le port 8443, où il reçoit des communications HTTP non chiffrées.
- Le proxy SSL au niveau du noyau peut être configuré de manière à utiliser le chiffrement au niveau de l'utilisateur comme solution de repli dans les cas où il ne prend pas en charge le chiffrement demandé.

  La Figure 3–2 illustre un scénario plus complexe. Le serveur Web et le proxy SSL au niveau du noyau sont configurés de manière à utiliser le protocole SSL de serveur Web au niveau de l'utilisateur comme solution repli.

  Le proxy SSL au niveau du noyau est configuré sur le port 443. Le serveur Web est configuré sur deux ports. Le port 8443 reçoit des communications HTTP non chiffrées, tandis que le port 443 est un port de repli. Le port de repli reçoit le trafic SSL chiffré pour les suites de chiffrement qui ne sont pas prises en charge par le proxy SSL au niveau du noyau.

FIGURE 3–2 Communications de serveur Web chiffrées par le noyau avec option de repli sur le chiffrement au niveau de l'utilisateur



Le proxy SSL au niveau du noyau prend en charge les protocoles SSL 3.0 et TLS 1.0, ainsi que la plupart des suites de chiffrement courantes. La page de manuel `kssl cfg(1M)` contient la liste complète. Le proxy peut être configuré de manière à se replier sur le serveur SSL au niveau de l'utilisateur pour les suites de chiffrement qui ne sont pas prises en charge.

Protection de serveurs Web à l'aide du proxy SSL au niveau du noyau (tâches)

Les procédures suivantes indiquent comment configurer des serveurs Web de manière à ce qu'ils utilisent le proxy SSL au niveau du noyau :

- "Configuration d'un serveur Web Apache 2.2 afin qu'il utilise le proxy SSL au niveau du noyau" à la page 31
- "Configuration d'un serveur Oracle iPlanet Web Server afin qu'il utilise le proxy SSL au niveau du noyau" à la page 33
- "Configuration du proxy SSL au niveau du noyau de manière à utiliser le protocole SSL d'Apache 2.2 comme solution de repli" à la page 35
- "Utilisation du proxy SSL au niveau du noyau dans les zones" à la page 38

▼ Configuration d'un serveur Web Apache 2.2 afin qu'il utilise le proxy SSL au niveau du noyau

Le proxy SSL au niveau du noyau peut améliorer la vitesse de traitement des paquets SSL sur un serveur Web Apache 2.2. Cette procédure implémente le scénario simple illustré à la Figure 3–1.

Avant de commencer

Vous avez configuré un serveur Web Apache 2.2. Ce serveur Web est inclus dans Oracle Solaris.

Vous devez prendre le rôle `root`.

1 Arrêtez le serveur Web.

```
# svcadm disable svc:/network/http:apache22
```

2 Placez la clé privée du serveur et le certificat du serveur dans un seul fichier.

Si seul le paramètre `SSLCertificateFile` est indiqué dans le fichier `ssl.conf`, le fichier spécifié peut être utilisé directement pour le proxy SSL au niveau du noyau.

Si le paramètre `SSLCertificateKeyFile` est également indiqué, vous devez combiner le fichier de certificat et le fichier de clé privée. Exécutez une commande semblable à l'exemple suivant pour combiner les fichiers :

```
# cat cert.pem key.pem > cert-and-key.pem
```

3 Déterminez les paramètres à utiliser avec la commande `ksslcfg`.

La page de manuel `ksslcfg(1M)` contient la liste complète des options. Voici les paramètres que vous *devez* fournir :

- *key-format* : utilisé avec l'option `-f` pour définir le certificat et le format de clé. Pour le proxy SSL au niveau du noyau, les formats pris en charge sont les suivants : `pkcs11`, `pem` et `pkcs12`.
- *key-and-certificate-file* : utilisé avec l'option `-i` pour définir l'emplacement du fichier qui stocke la clé de serveur et le certificat pour les options *key-format* `pem` ou `pkcs12`.
- *password-file* : utilisé avec l'option `-p` pour obtenir le mot de passe servant à chiffrer la clé privée pour les options *key-format* `pem` ou `pkcs12`. Pour `pkcs11`, le mot de passe est utilisé pour authentifier le jeton PKCS #11. Vous devez protéger le fichier de mots de passe à l'aide d'autorisations `0400`. Ce fichier est requis pour les réinitialisations sans l'intervention d'un opérateur.
- *token-label* : utilisé avec l'option `-T` pour indiquer le jeton PKCS #11.
- *certificate-label* : utilisé avec l'option `-C` pour sélectionner l'étiquette dans l'objet de certificat dans le jeton PKCS #11.
- *proxy-port* : utilisé avec l'option `-x` pour définir le port proxy SSL. Vous devez spécifier un port différent du port standard `80`. Le serveur Web est à l'écoute du trafic de texte en clair non chiffré sur le port proxy SSL. Généralement, la valeur est `8443`.
- *ssl-port* : indique le port d'écoute pour le proxy SSL au niveau du noyau. Généralement, la valeur est `443`.

4 Créez l'instance de service pour le proxy SSL au niveau du noyau.

Indiquez le port proxy SSL et les paramètres associés à l'aide de l'un des formats suivants :

- **Indiquez PEM ou PKCS #12 comme format de clé.**

  ```
  # ksslcfg create -f key-format -i key-and-certificate-file \
  -p password-file -x proxy-port ssl-port
  ```

- **Indiquez PKCS #11 comme format de clé.**

  ```
  # ksslcfg create -f pkcs11 -T PKCS#11-token -C certificate-label \
  -p password-file -x proxy-port ssl-port
  ```

5 **Vérifiez que l'instance de service est en ligne.**

```
# svcs svc:/network/ssl/proxy
STATE          STIME    FMRI
online         02:22:22 svc:/network/ssl/proxy:default
```

La sortie suivante indique que l'instance de service n'a pas été créée :

```
svcs: Pattern 'svc:/network/ssl/proxy' doesn't match any instances
STATE          STIME    FMRI
```

6 **Configurez le serveur Web pour qu'il soit à l'écoute sur le port proxy SSL.**

Modifiez le fichier `/etc/apache2/2.2/http.conf` et ajoutez une ligne pour définir le port proxy SSL. Si vous utilisez l'adresse IP du serveur, le serveur Web écoute uniquement sur cette interface. La ligne est similaire à ce qui suit :

```
Listen proxy-port
```

7 **Définissez une dépendance SMF pour le serveur Web.**

Le service du serveur Web peut uniquement démarrer une fois que l'instance proxy SSL au niveau du noyau a démarré. Les commandes suivantes établissent cette dépendance :

```
# svccfg -s svc:/network/http:apache22
svc:/network/http:apache22> addpg kssl dependency
...apache22> setprop kssl/entities = fmri:svc:/network/ssl/proxy:kssl-INADDR_ANY-443
...apache22> setprop kssl/grouping = astring: require_all
...apache22> setprop kssl/restart_on = astring: refresh
...apache22> setprop kssl/type = astring: service
...apache22> end
```

8 **Activez le service du serveur Web.**

```
# svcadm enable svc:/network/http:apache22
```

▼ Configuration d'un serveur Oracle iPlanet Web Server afin qu'il utilise le proxy SSL au niveau du noyau

Le proxy SSL au niveau du noyau peut améliorer la vitesse de traitement des paquets SSL sur un serveur Oracle iPlanet Web Server. Cette procédure implémente le scénario simple illustré à la Figure 3–1.

Avant de commencer

Vous avez installé et configuré un serveur Oracle iPlanet Web Server. Le serveur peut être téléchargé à partir du site Oracle iPlanet Web Server (`http://www.oracle.com/technetwork/middleware/iplanetwebserver-098726.html?ssSourceSiteId=ocomen`). Pour plus d'instructions, reportez-vous à Oracle iPLANET WEB SERVER 7.0.15 (`http://docs.oracle.com/cd/E18958_01/index.htm`).

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network Security (sécurité réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Arrêtez le serveur Web.

Utilisez l'interface Web de l'administrateur pour arrêter le serveur. Pour plus d'instructions, reportez-vous à Oracle iPLANET WEB SERVER 7.0.15 (`http://docs.oracle.com/cd/E18958_01/index.htm`).

2 Déterminez les paramètres à utiliser avec la commande `ksslcfg`.

La page de manuel `ksslcfg`(1M) contient la liste complète des options. Pour obtenir la liste des paramètres que vous *devez* fournir, reportez-vous à l'Étape 3 in "Configuration d'un serveur Web Apache 2.2 afin qu'il utilise le proxy SSL au niveau du noyau" à la page 31.

3 Créez l'instance de service pour le proxy SSL au niveau du noyau.

Indiquez le port proxy SSL et les paramètres associés à l'aide de l'un des formats suivants :

- **Indiquez PEM ou PKCS #12 comme format de clé.**

  ```
  # ksslcfg create -f key-format -i key-and-certificate-file \
  -p password-file -x proxy-port ssl-port
  ```

- **Indiquez PKCS #11 comme format de clé.**

  ```
  # ksslcfg create -f pkcs11 -T PKCS#11-token -C certificate-label \
  -p password-file -x proxy-port ssl-port
  ```

4 Vérifiez que l'instance est en ligne.

```
# svcs svc:/network/ssl/proxy
STATE          STIME    FMRI
online         02:22:22 svc:/network/ssl/proxy:default
```

5 Configurez le serveur Web pour qu'il soit à l'écoute sur le port proxy SSL.

Pour plus d'instructions, reportez-vous à Oracle iPLANET WEB SERVER 7.0.15 (`http://docs.oracle.com/cd/E18958_01/index.htm`).

6 Définissez une dépendance SMF pour le serveur Web.

Le service du serveur Web peut uniquement démarrer une fois que l'instance proxy SSL au niveau du noyau a démarré. Les commandes suivantes établissent cette dépendance, en supposant que le FMRI du service de serveur Web est `svc:/network/http:webserver7` :

```
# svccfg -s svc:/network/http:webserver7
svc:/network/http:webserver7> addpg kssl dependency
...webserver7> setprop kssl/entities = fmri:svc:/network/ssl/proxy:kssl-INADDR_ANY-443
...webserver7> setprop kssl/grouping = astring: require_all
...webserver7> setprop kssl/restart_on = astring: refresh
...webserver7> setprop kssl/type = astring: service
...webserver7> end
```

7 Activez le service du serveur Web.

```
# svcadm enable svc:/network/http:webserver7
```

▼ Configuration du proxy SSL au niveau du noyau de manière à utiliser le protocole SSL d'Apache 2.2 comme solution de repli

Dans cette procédure, vous configurez de toutes pièces un serveur Web Apache 2.2 et configurez le proxy SSL au niveau du noyau en tant que mécanisme de traitement de session SSL principal. Lorsque l'ensemble de chiffrements SSL proposé par le client n'inclut aucun chiffrement offert par le proxy SSL au niveau du noyau, le serveur Web Apache 2.2 sert de solution de repli. Cette procédure met en oeuvre le scénario complexe illustré à la Figure 3–2.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Sur le serveur Apache 2.2, créez un certificat de clé destiné à être utilisé par le proxy SSL au niveau du noyau du serveur.

a. Générez une demande de signature de certificat (CSR).

La commande suivante génère une demande de signature de certificat et la clé privée qui lui est associée pour le proxy SSL au niveau du noyau :

```
# cd /root
# openssl req \
> -x509 -new \
> -subj "/C=CZ/ST=Prague region/L=Prague/CN=‘hostname‘" \
> -newkey rsa:2048 -keyout webkey.pem \
> -out webcert.pem
Generating a 2048 bit RSA private key
.+++
........+++
writing new private key to ’webkey.pem’
Enter PEM pass phrase: JohnnyCashIsCool
Verifying - Enter PEM pass phrase:  JohnnyCashIsCool
#
# chmod 440 /root/webcert.pem ; chown root:webservd /root/webcert.pem
```

Pour plus d'informations, reportez-vous à la page de manuel `openssl(5)`.

b. Envoyez la demande de signature de certificat à votre autorité de certification (CA).

c. Remplacez le fichier `webcert.pem` par le certificat signé fourni par votre autorité de certification.

2 Configurez le proxy SSL au niveau du noyau avec une phrase de passe et le certificat de clé publique/privée.

a. Créez, enregistrez et protégez la phrase de passe.

```
# echo "RefrigeratorsAreCool" > /root/kssl.pass
# chmod 440 /root/kssl.pass; chown root:webservd /root/kssl.pass
```

Remarque – La phrase de passe ne peut pas contenir d'espace.

b. Rassemblez le certificat de clé privée et le certificat de clé publique dans un seul fichier.

```
# cat /root/webcert.pem /root/webkey.pem > /root/webcombo.pem
```

c. Configurez le proxy SSL au niveau du noyau avec le certificat de clé publique/privée et la phrase de passe.

```
# ksslcfg create -f pem -i /root/webcombo.pem -x 8443 -p /root/kssl.pass 443
```

3 Configurez le serveur Web de manière à ce qu'il écoute le texte en clair sur le port 8443.

Modifiez la ligne `Listen` dans le fichier `/etc/apache2/2.2/httpd.conf`.

```
# pfedit /etc/apache2/2.2/httpd.conf
...
## Listen 80
Listen 8443
```

4 Ajoutez le modèle de module SSL, `ssl.conf`, au répertoire de configuration Apache.

```
# cp /etc/apache2/2.2/samples-conf.d/ssl.conf /etc/apache2/2.2/ssl.conf
```

Ce module ajoute l'écoute des connexions chiffrées sur le port 443.

5 Activez le serveur Web pour déchiffrer la phrase de passe dans le fichier `/root/kssl.pass`.

a. Créez un script shell qui lit le fichier `kssl.pass`.

```
# pfedit /root/put-passphrase.sh
#!/usr/bin/ksh -p
## Reads SSL kernel proxy passphrase
/usr/bin/cat /root/kssl.pass
```

b. Définissez le script comme exécutable et protégez le fichier.

```
# chmod 500 /root/put-passphrase.sh
# chown webservd:webservd /root/put-passphrase.sh
```

c. Modifiez le paramètre `SSLPassPhraseDialog` dans le fichier `ssl.conf` de manière à appeler ce script shell.

```
# pfedit /etc/apache2/2.2/ssl.conf
...
## SSLPassPhraseDialog  builtin
SSLPassPhraseDialog exec:/root/put-passphrase.sh
```

6 Placez les certificats de clés publique et privée du serveur Web aux emplacements appropriés.

Les valeurs des paramètres `SSLCertificateFile` et `SSLCertificateKeyFile` dans le fichier `ssl.conf` indiquent les emplacements et les noms attendus. Vous pouvez copier les certificats aux emplacements corrects ou créer des liens vers ces emplacements.

```
# ln -s  /root/webcert.pem /etc/apache2/2.2/server.crt      SSLCertificateFile default location
# ln -s /root/webkey.pem /etc/apache2/2.2/server.key        SSLCertificateKeyFile default location
```

7 Activez le service Apache.

```
# svcadm enable apache22
```

8 (Facultatif) Vérifiez que les deux ports fonctionnent.

Utilisez les commandes `openssl s_client` et `kstat` pour afficher les paquets.

a. Utilisez un chiffrement qui est disponible au proxy SSL au niveau du noyau.

```
# openssl s_client -cipher RC4-SHA -connect web-server:443
```

Une augmentation de 1 du compteur `kstat kssl_full_handshakes` vérifie que la session SSL a été traitée par le proxy SSL au niveau du noyau.

```
# kstat -m kssl -s kssl_full_handshakes
```

b. Utilisez un chiffrement qui n'est pas disponible au proxy SSL au niveau du noyau.

```
# openssl s_client -cipher CAMELLIA256-SHA -connect web-server:443
```

Une augmentation de 1 du compteur `kstat kssl_fallback_connections` vérifie que le paquet est arrivé mais que la session SSL a été traitée par le serveur Web Apache.

```
# kstat -m kssl -s kssl_fallback_connections
```

Exemple 3–1 Configuration d'un serveur Web Apache 2.2 afin qu'il utilise le proxy SSL au niveau du noyau

La commande suivante permet de créer une instance de service pour le proxy SSL au niveau du noyau qui utilise le format de clé `pem` :

```
# ksslcfg create -f pem -i cert-and-key.pem -p kssl.pass -x 8443 443
```

▼ Utilisation du proxy SSL au niveau du noyau dans les zones

Le proxy SSL au niveau du noyau fonctionne dans les zones avec les restrictions suivantes :

- L'ensemble de la gestion SSL au niveau du noyau doit être réalisée dans la zone globale. L'administrateur de la zone globale doit pouvoir accéder aux fichiers de clés et de certificat de la zone locale. Le serveur Web de la zone locale peut être démarré une fois que l'instance de service a été configurée à l'aide de la commande `ksslcfg` dans la zone globale.
- Un nom d'hôte ou une adresse IP spécifique doit être spécifié(e) avec la commande `ksslcfg` lorsque vous configurez l'instance. En particulier, l'instance ne peut pas spécifier `INADDR_ANY` pour l'adresse IP.

Avant de commencer

Le service du serveur Web est configuré et activé dans la zone non globale.

Vous devez vous connecter en tant qu'administrateur disposant des profils de droits Network Security (sécurité réseau) et Zone Management (gestion de zone). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Dans la zone non globale, arrêtez le serveur Web.

Par exemple, pour arrêter un serveur Web Apache dans la zone `apache-zone`, exécutez la commande suivante :

```
apache-zone # svcadm disable svc:/network/http:apache22
```

2 Dans la zone globale, créez l'instance de service pour le proxy SSL au niveau du noyau dans la zone.

Pour créer une instance de service pour `apache-zone`, utilisez une commande semblable à ce qui suit :

```
# ksslcfg create -f pem -i /zone/apache-zone/root/keypair.pem \
-p /zone/apache-zone/root/skppass -x 8443 apache-zone 443
```

3 Dans la zone non globale, activez l'instance de service web.

Activez par exemple le service Web dans `apache-zone`.

```
apache-zone # svcadm enable svc:/network/http:apache22
```

◆ ◆ ◆ CHAPITRE 4

IP Filter dans Oracle Solaris (présentation)

Ce chapitre fournit une présentation d'IP Filter, une fonction d'Oracle Solaris. Les tâches IP Filter sont décrites au Chapitre 5, “IP Filter (tâches)”.

Le présent chapitre contient les informations suivantes :

Introduction à IP Filter

La fonction IP Filter d'Oracle Solaris est un pare-feu qui assure un filtrage de paquets avec état et la translation d'adresse réseau (NAT). IP Filter permet également le filtrage de paquets sans état, ainsi que la création et la gestion des pools d'adresses.

Le filtrage de paquets assure une protection de base contre les attaques potentielles via le réseau. IP Filter peut filtrer les paquets par adresse IP, port, protocole, interface réseau et direction du trafic. IP Filter peut également filtrer en fonction d'une adresse IP source individuelle, d'une adresse IP de destination, d'une plage d'adresses IP ou par pools d'adresses.

IP Filter est dérivé du logiciel Open Source IP Filter. Les conditions de licence, attribution et déclarations de copyright pour Open Source IP Filter sont accessibles via le chemin par défaut `/usr/lib/ipf/IPFILTER.LICENCE`. Si vous avez installé Oracle Solaris à un autre emplacement que celui par défaut, modifiez le chemin indiqué afin d'accéder au fichier à l'emplacement où il a été installé.

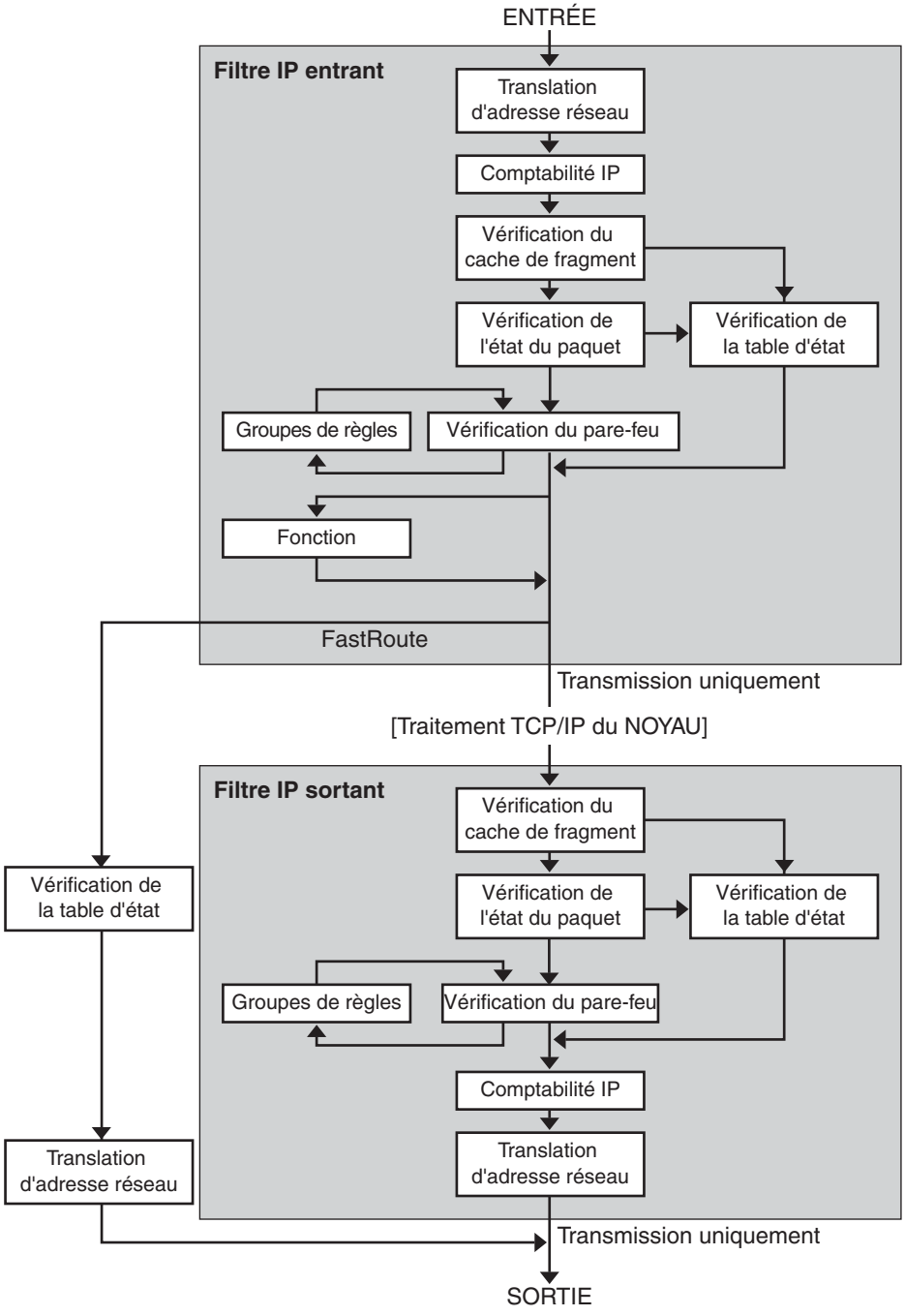
Sources d'informations pour Open Source IP Filter

La page d'accueil du logiciel Open Source IP Filter de Darren Reed se trouve à l'adresse `http://coombs.anu.edu.au/~avalon/ip-filter.html`. Ce site Web fournit des informations relatives au logiciel Open Source IP Filter, notamment un lien vers le didacticiel “IP Filter Based Firewalls HOWTO” (Brendan Conoboy et Erik Fichtner, 2002). Vous trouverez dans ce didacticiel les instructions de construction de pare-feux dans un environnement BSD UNIX, expliquées pas à pas. Bien qu'il soit destiné à un environnement BSD UNIX, ce didacticiel est également applicable à la configuration d'IP Filter sur Oracle Solaris.

Traitement des paquets avec IP Filter

Au cours du traitement d'un paquet, IP Filter exécute une séquence d'étapes. Le diagramme ci-dessous illustre les étapes du traitement d'un paquet et l'intégration du filtrage à la pile de protocole TCP/IP.

FIGURE 4–1 Séquence de traitement d'un paquet



Le traitement d'un paquet inclut les opérations suivantes :

- **Translation d'adresse réseau (NAT)**

  Translation d'une adresse IP privée vers une adresse publique, ou définition d'alias pour plusieurs adresses privées vers une adresse publique unique. NAT (Network Address Translation, translation d'adresse réseau) permet à une organisation de résoudre le problème d'épuisement des adresses IP lorsqu'elle utilise un réseau et requiert l'accès à Internet.

- **Comptabilité IP**

  Les règles d'entrée et de sortie peuvent être configurées séparément, avec enregistrement du nombre d'octets transmis. En cas de correspondance d'une règle, le nombre d'octets du paquet est ajouté à la règle et des statistiques en cascade sont rassemblées.

- **Vérification du cache de fragments**

  Par défaut, les paquets fragmentés sont mis en mémoire cache. Lorsque tous les fragments d'un paquet particulier arrivent, les règles de filtrage sont appliquées et les fragments sont soit autorisés, soit bloqués. Si `set defrag off` figure dans le fichier de règles, les fragments ne sont pas mis en cache.

- **Vérification de l'état du paquet**

  Si la règle contient l'instruction `keep state`, tous les paquets d'une session spécifiée sont automatiquement transmis ou bloqués, selon la spécification de la règle : `pass` (transmettre) ou `block` (bloquer).

- **Vérification du pare-feu**

  Les règles d'entrée et de sortie peuvent être configurées séparément, afin d'autoriser ou non la transmission d'un paquet, via IP Filter, vers les routines TCP/IP du noyau ou vers le réseau.

- **Groupes**

  Les groupes permettent d'écrire des ensembles de règles selon une structure arborescente.

- **Fonction**

  Une fonction correspond à l'action à réaliser. Les fonctions sont, par exemple, `block` (bloquer), `pass` (transmettre), `literal` (littéral) et `send ICMP response` (envoyer une réponse ICMP).

- **FastRoute**

  FastRoute indique à IP Filter de ne pas transmettre le paquet vers la pile UNIX IP pour le routage, ce qui entraîne une réduction TTL.

- **Authentification IP**

  Les paquets authentifiés ne sont transmis via les boucles du pare-feu qu'une seule fois, afin d'éviter le traitement multiple de certains paquets.

Recommandations relatives à l'utilisation d'IP Filter

- IP Filter est géré par le service SMF `svc:/network/ipfilter`. Pour une présentation complète de SMF, reportez-vous au Chapitre 1, “Gestion des services (présentation)” du manuel *Gestion des services et pannes dans Oracle Solaris 11.1*. Pour plus d'informations sur les procédures étape par étape associées à SMF, reportez-vous au Chapitre 2, “Gestion des services (tâches)” du manuel *Gestion des services et pannes dans Oracle Solaris 11.1*.
- IP Filter requiert la modification directe des fichiers de configuration.
- IP Filter est installé en tant que composant d'Oracle Solaris. Par défaut, le service IP Filter est activé lorsque votre système est configuré de façon à utiliser la mise en réseau automatique. Le profil réseau automatique, comme décrit dans les pages de manuel `nwam(5)` et `netadm(1M)`, active ce pare-feu. Pour une configuration personnalisée sur un système mis en réseau automatiquement, le service IP Filter n'est pas activé. Pour obtenir la description des tâches associées à l'activation du service, reportez-vous à la section “Configuration d'IP Filter” à la page 53.
- Pour gérer IP Filter, vous devez prendre le rôle `root` ou être en mesure de prendre un rôle incluant le profil de droits IP Filter Management (gestion IP Filter). Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer le rôle et l'attribuer à un utilisateur, reportez-vous à la section “Configuration initiale RBAC (liste des tâches)” du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.
- Le logiciel Oracle Solaris Cluster ne prend pas en charge le filtrage IP Filter pour les services évolutifs. En revanche, IP Filter est pris en charge pour les services de basculement. Pour connaître les recommandations et restrictions relatives à IP Filter dans un cluster, reportez-vous à la section “Restrictions concernant les fonctions du SE Oracle Solaris” dans le *Guide d'installation du logiciel Oracle Solaris Cluster*.
- Le filtrage interzones est pris en charge à condition que les règles IP Filter soient implémentées dans une zone qui fonctionne en tant que routeur virtuel pour les autres zones du système.

Utilisation des fichiers de configuration IP Filter

IP Filter peut assurer des services de pare-feu ou de translation d'adresse réseau (NAT, Network Address Translation). Aucune règle de pare-feu et de translation NAT n'est fournie par défaut. Vous devez créer des fichiers de configuration personnalisés et définir les chemins d'accès à ces fichiers en tant que valeurs de propriétés du service IP Filter. Une fois que le service est activé, ces fichiers sont chargés automatiquement lorsque le système est réinitialisé. Pour obtenir des exemples de fichiers de configuration, reportez-vous à la section “Exemples de fichiers de configuration IP Filter” à la page 78. Pour plus d'informations, reportez-vous à la page de manuel `svc.ipfd(1M)`.

Utilisation d'ensembles de règles IP Filter

Pour gérer le pare-feu, vous devez spécifier des ensembles de règles à l'aide d'IP Filter, puis filtrer le trafic réseau en fonction de ces ensembles de règles. Les types d'ensembles de règles suivants sont disponibles :

- Ensembles de règles de filtrage de paquets
- Ensembles de règles NAT (Network Address Translation, translation d'adresse réseau)

Par ailleurs, il est possible de créer des pools d'adresses pour référencer des groupes d'adresses IP. Ensuite, ces pools peuvent être utilisés dans un ensemble de règles. Les pools d'adresses permettent d'accélérer le traitement des règles. En outre, ils facilitent la gestion des grands groupes d'adresses.

Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter

Vous pouvez configurer le filtrage de paquets à l'aide des ensembles de règles de filtrage de paquets. La commande `ipf` permet d'utiliser les ensembles de règles de filtrage de paquets. Pour plus d'informations sur la commande `ipf`, reportez-vous à la page de manuel `ipf(1M)`.

Vous pouvez créer des règles de filtrage de paquets via la ligne de commande, à l'aide de la commande `ipf` ou dans un fichier de configuration de filtrage de paquets. Pour charger le fichier de configuration, vous devez le créer, puis indiquer son chemin d'accès au service IP Filter.

Avec IP Filter, deux ensembles de règles de filtrage de paquets peuvent coexister : l'ensemble de règles actif et l'ensemble de règles inactif. Dans la plupart des cas, vous utiliserez l'ensemble de règles actif. Toutefois, la commande `ipf -I` vous permet d'appliquer l'action de la commande à la liste de règles inactives. La liste de règles inactives n'est pas employée par IP Filter, sauf si vous la sélectionnez. La liste de règles inactives constitue l'emplacement auquel vous pouvez enregistrer des règles sans affecter le filtrage de paquets actif.

IP Filter traite les règles de la liste de règles du début à la fin de la liste de règles configurée, puis transmet ou bloque le paquet. Un indicateur permet à IP Filter de déterminer si un paquet doit être transmis ou non. Il parcourt l'intégralité de l'ensemble de règles et détermine si le paquet doit être transmis ou bloqué, en fonction de la dernière règle correspondante.

Il existe deux exceptions à ce processus. D'une part, si le paquet correspondant à une règle contenant le mot-clé `quick`, Si une règle inclut le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées. D'autre part, si le paquet correspond à une règle contenant le mot-clé `group`, seules les règles portant l'indicateur de ce group sont vérifiées.

Configuration des règles de filtrage de paquets

Appliquez la syntaxe suivante pour créer des règles de filtrage de paquets :

action `[in|out]` *option keyword, keyword...*

1. Chaque règle commence par une action. IP Filter applique l'action au paquet si celui-ci correspond à la règle. Les actions habituellement appliquées aux paquets sont répertoriées ci-dessous.

`block`	Empêche le paquet de traverser le filtre.
`pass`	Permet au paquet de traverser le filtre.
`log`	Consigne le paquet sans déterminer s'il est bloqué ou transmis. Exécutez la commande `ipmon` pour afficher le journal.
`count`	Inclut le paquet dans les statistiques du filtre. Exécutez la commande `ipfstat` pour afficher les statistiques.
`skip` *nombre*	Le filtre saute *nombre* règles de filtrage.
`auth`	Le paquet est authentifié par un programme utilisateur qui valide les informations qu'il contient. Le programme détermine si le paquet est transmis ou bloqué.

2. Le mot suivant est `in` ou `out`. Votre choix détermine si la règle de filtrage de paquets est appliquée à un paquet entrant (in) ou à un paquet sortant (out).
3. Ensuite, vous pouvez insérer toute une liste d'options. Si vous en utilisez plusieurs, elles doivent être dans l'ordre indiqué ci-dessous.

`log`	Consigne le paquet si la règle constitue la dernière règle correspondante. Exécutez la commande `ipmon` pour afficher le journal.
`quick`	Exécute la règle contenant l'option `quick` si un paquet lui correspond. Toute vérification de règle subséquente est interrompue.
`on` *nom-interface*	Applique la règle uniquement si le paquet entre ou sort via l'interface spécifiée.
`dup-to` *nom-interface*	Copie le paquet et envoie la copie sur *nom-interface* vers une adresse IP éventuellement spécifiée.
`to` *nom-interface*	Déplace le paquet vers une file d'attente sortante sur *nom-interface*.

4. Une fois les options spécifiées, vous avez le choix entre plusieurs mots-clés afin de déterminer si le paquet correspond à la règle. Les mots-clés doivent être utilisés dans l'ordre indiqué ci-dessous.

Remarque – Par défaut, le filtre autorise la transmission de tout paquet ne correspondant à aucune règle du fichier de configuration.

`tos`	Filtre les paquets en fonction de leur type de service, exprimé sous forme d'entier décimal ou hexadécimal.
`ttl`	Filtre les paquets en fonction de leur durée de vie. La durée de vie d'un paquet est une valeur enregistrée dans celui-ci qui indique la durée pendant laquelle le paquet peut se trouver sur le réseau avant d'être abandonné.
`proto`	Les paquets correspondant à la règle sont déterminés en fonction d'un protocole spécifique. Vous pouvez employer l'un des noms de protocole spécifiés dans le fichier `/etc/protocols` ou un nombre décimal représentant le protocole. Le mot-clé `tcp/udp` peut être utilisé pour filtrer les paquets TCP ou UDP.
`from/to/all/ any`	Filtre les paquets en fonction des éléments suivants : l'adresse IP source, l'adresse IP de destination et le numéro de port. Le mot-clé `all` permet d'accepter tous les paquets, quelles que soient leur source et leur destination.
`with`	Les paquets correspondant à la règle sont ceux qui sont associés à des attributs spécifiques. Insérez le mot `not` ou `no` devant le mot-clé pour indiquer qu'un paquet ne correspond à la règle qu'en l'absence de l'option.
`flags`	Employé pour TCP afin de filtrer les paquets en fonction des indicateurs TCP définis. Pour plus d'informations sur les indicateurs TCP, reportez-vous à la page de manuel `ipf(4)`.
`icmp-type`	Filtre les paquets en fonction du type d'ICMP. Ce mot-clé n'est employé que si l'option `proto` est définie sur `icmp` et que l'option `flags` n'est pas utilisée.
`keep` *keep-options*	Détermine les informations conservées pour le paquet. Les *keep-options* disponibles incluent l'option `state`. L'option `state` conserve des informations sur la session et peut être appliquée aux paquets TCP, UDP et ICMP.
`head` *number*	Crée un groupe pour les règles de filtrage, désigné par le numéro *numéro*.
`group` *number*	Ajoute la règle au groupe de numéro *numéro* au lieu du groupe par défaut. Toutes les règles de filtrage sont placées dans le groupe 0 si aucun autre groupe n'est spécifié.

L'exemple suivant illustre la constitution d'une syntaxe de règle de filtrage de paquets pour créer une règle. Pour bloquer le trafic entrant à partir de l'adresse IP `192.168.0.0/16`, ajoutez la règle suivante à la liste de règles :

```
block in quick from 192.168.0.0/16 to any
```

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles de filtrage de paquets, reportez-vous à la page de manuel `ipf(4)` Pour une description des tâches associées au filtrage de paquets, reportez-vous à la section "Gérez les ensembles de règles de filtrage de paquets d'IP Filter" à la page 60. Pour une explication du schéma d'adresse IP (`192.168.0.0/16`) présenté dans l'exemple, reportez-vous au Chapitre 1, "Planification du développement du réseau" du manuel *Configuration et administration de réseaux Oracle Solaris 11.1*.

Utilisation de la fonctionnalité NAT d'IP Filter

NAT configure des règles de mappage qui réalisent la translation des adresses IP source et de destination vers d'autres adresses Internet ou intranet. Ces règles modifient les adresses source et de destination des paquets IP entrants et sortants et envoient les paquets. Vous pouvez également utiliser NAT pour rediriger le trafic d'un port à un autre. NAT assure l'intégrité du paquet en cas de modification ou de redirection de celui-ci.

Vous pouvez créer des règles NAT à la ligne de commande, à l'aide de la commande `ipnat` ou dans un fichier de configuration NAT. Vous devez créer le fichier de configuration NAT et définir son chemin d'accès comme valeur de la propriété `config/ipnat_config_file` du service. La valeur par défaut est `/etc/ipf/ipnat.conf`. Pour plus d'informations, reportez-vous à la commande `ipnat(1M)`.

Les règles NAT peuvent s'appliquer à la fois aux adresses IPv4 et IPv6. Toutefois, vous ne pouvez pas spécifier les deux types d'adresses dans la même règle. Au contraire, vous devez définir des règles distinctes pour chaque type d'adresse. Dans une règle NAT qui inclut les adresses IPv6, vous ne pouvez pas utiliser les commandes NAT `mapproxy` et `rdrproxy` simultanément.

Configuration des règles NAT

Appliquez la syntaxe ci-dessous pour créer des règles NAT :

command interface-name parameters

1. Toute règle commence par l'une des commandes ci-dessous :

   `map` Mappe une adresse IP ou un réseau IP vers une autre adresse IP ou un autre réseau IP selon un processus circulaire non contrôlé.

`rdr` Redirige les paquets d'un couple port-adresse IP vers un autre couple port-adresse IP.

`bimap` Etablit une translation d'adresse réseau bidirectionnelle entre une adresse IP externe et une adresse IP interne.

`map-block` Etablit la translation basée sur les adresses IP statiques. Cette commande se base sur un algorithme qui force la translation des adresses vers une plage de destination.

2. Le mot suivant correspond au nom de l'interface, par exemple `bge0`.
3. Ensuite, vous avez le choix entre divers paramètres, afin de définir la configuration NAT. Les paramètres suivants sont disponibles :

   `ipmask` Désigne le masque réseau.

   `dstipmask` Désigne l'adresse cible de la translation de `ipmask`.

   `mapport` Désigne les protocoles `tcp`, `udp` ou `tcp/udp`, ainsi qu'une plage de numéros de port.

L'exemple ci-dessous indique comment construire une règle NAT. Pour réécrire un paquet sortant sur le périphérique `net2` avec l'adresse source `192.168.1.0/24` et pour afficher son adresse source comme étant `10.1.0.0/16`, ajoutez la règle ci-dessous à l'ensemble de règles NAT :

```
map net2 192.168.1.0/24 -> 10.1.0.0/16
```

Les règles suivantes s'appliquent aux adresses IPv6 :

```
map net3 fec0:1::/64 -> 2000:1:2::/72 portmap tcp/udp 1025:65000
map-block net3 fe80:0:0:209::/64 -> 209:1:2::/72 ports auto
rdr net0 209::ffff:fe13:e43e port 80 -> fec0:1::e,fec0:1::f port 80 tcp round-robin
```

Pour obtenir la syntaxe et la grammaire complètes, reportez-vous à la page de manuel `ipnat(4)`.

Utilisation de la fonctionnalité de pools d'adresses d'IP Filter

Les pools d'adresses constituent une référence unique pour nommer un groupe de paires adresse/masque de réseau. Les processus fournis pas les pools d'adresses permettent de trouver plus rapidement les adresses IP correspondant aux règles. En outre, ils facilitent la gestion des grands groupes d'adresses.

Les règles de configuration de pool d'adresses peuvent se trouver dans un fichier qui est chargé par le service IP Filter. Vous devez créer un fichier et définir son chemin d'accès comme valeur de la propriété `config/ippool_config_file` du service. La valeur par défaut est `/etc/ipf/ippool.conf` .

Configuration des pools d'adresses

Pour créer un pool d'adresses, appliquez la syntaxe suivante :

`table role =` *role-name* `type =` *storage-format* `number =` *reference-number*

`table` Définit la référence des adresses.

`role` Spécifie le rôle du pool dans IP Filter. A ce stade, vous ne pouvez faire référence qu'au rôle `ipf`.

`type` Spécifie le format de stockage du pool.

`numéro` Spécifie le numéro de référence utilisé par la règle de filtrage.

Par exemple, pour faire référence aux groupes d'adresses `10.1.1.1` et `10.1.1.2` et au réseau `192.16.1.0` à l'aide du numéro de pool `13`, insérez la règle suivante dans le fichier de configuration de pool d'adresses :

```
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24 };
```

Ensuite, pour faire référence au numéro de pool `13` dans une règle de filtrage, élaborez une règle similaire à la suivante :

```
pass in from pool/13 to any
```

Vous devez charger le fichier de pool avant de charger les règles contenant une référence au pool. Dans le cas contraire, le pool n'est pas défini, comme indiqué dans la sortie suivante :

```
# ipfstat -io
empty list for ipfilter(out)
block in from pool/13(!) to any
```

Si vous ajoutez le pool par la suite, l'ensemble de règle du noyau n'est pas mis à jour. Vous devez également recharger le fichier de règles faisant référence au pool.

Pour obtenir la syntaxe et la grammaire complètes, reportez-vous à la page de manuel `ippool(4)`.

IPv6 pour IP Filter

Ce filtrage peut se baser sur l'adresse IPv6 source/de destination, sur les pools contenant des adresses IPv6 et sur les en-têtes d'extension IPv6.

De nombreux aspects d'IPv6 sont similaires à IPv4. Toutefois, les en-têtes et tailles des paquets ne sont pas identiques dans les deux versions d'IP, ce qui constitue une considération de poids pour IP Filter. Les paquets IPv6 appelés *jumbogrammes* contiennent un datagramme de longueur supérieure à 65 535 octets. IP Filter ne prend pas en charge les jumbogrammes IPv6. Pour en savoir plus sur les autres fonctionnalités IPv6, reportez-vous à la section "Major Features of IPv6" du manuel *System Administration Guide: IP Services*.

Remarque – Pour plus d'informations sur les jumbogrammes, reportez-vous au document IPv6 Jumbograms, RFC 2675 de l'IETF (Internet Engineering Task Force). [`http://www.ietf.org/rfc/rfc2675.txt`]

Les tâches IP Filter associées à IPv6 ne sont pas très différentes d'IPv4. La différence la plus notable est l'emploi de l'option `-6` avec certaines commandes. Les commandes `ipf` et `ipfstat` incluent l'option `-6` à utiliser avec le filtrage de paquets IPv6. Appliquez l'option `-6` avec la commande `ipf` pour charger et vider les règles de filtrage de paquets IPv6. Pour afficher les statistiques IPv6, utilisez l'option `-6` avec la commande `ipfstat.` Les commandes `ipmon` et `ippool` prennent également en charge IPv6, même si aucune option n'est associée à la prise en charge d'IPv6. La commande `ipmon` a été optimisée pour autoriser la journalisation des paquets IPv6. La commande `ippool` prend en charge les pools avec les adresses IPv6. Vous pouvez créer des pools distincts pour les adresses IPv4 et IPv6, ou un pool contenant à la fois des adresses IPv4 et IPv6.

Pour créer des règles de filtrage de paquets IPv6 réutilisables, vous devez créer un fichier IPv6 spécifique. Puis vous définissez son chemin d'accès comme valeur de la propriété `config/ip6_config_file` du service d'IP Filter. La valeur par défaut est `/etc/ipf/ip6.conf`.

Pour plus d'information sur IPv6, reportez-vous au Chapitre 3, "Introducing IPv6 (Overview)" du manuel *System Administration Guide: IP Services*. Pour obtenir une description des tâches associées à IP Filter, reportez-vous au Chapitre 5, "IP Filter (tâches)".

Pages de manuel IP Filter

Le tableau ci-dessous décrit les pages de manuel portant sur IP Filter.

Page de manuel	Description
ipf(1M)	Gère les règles IP Filter, affiche les paramètres réglables et effectue d'autres tâches.
ipf(4)	Contient la grammaire et la syntaxe de création des règles de filtrage de paquets IP Filter.
ipfilter(5)	Décrit le logiciel IP Filter.
ipfs(1M)	Enregistre et restaure les informations NAT et les informations de table d'état d'une réinitialisation à l'autre.
ipfstat(1M)	Extrait et affiche les statistiques relatives au traitement des paquets.
ipmon(1M)	Ouvre le périphérique de journalisation et affiche les paquets consignés pour le filtrage de paquets et la translation NAT.
ipnat(1M)	Gère les règles NAT et affiche les statistiques NAT.
ipnat(4)	Contient la grammaire et la syntaxe pour la création de règles NAT.
ippool(1M)	Crée et gère des pools d'adresses.
ippool(4)	Contient la grammaire et la syntaxe de création des pools d'adresses IP Filter.
svc.ipfd(1M)	Fournit des informations sur la configuration du service IP Filter.

◆ ◆ ◆ CHAPITRE 5

IP Filter (tâches)

Ce chapitre fournit les instructions relatives à chaque étape des tâches. Pour obtenir des informations générales sur IP Filter, reportez-vous au Chapitre 4, “IP Filter dans Oracle Solaris (présentation)”.

Le présent chapitre contient les informations suivantes :

Configuration d'IP Filter

La liste des tâches ci-dessous répertorie les procédures permettant de créer des règles IP Filter ainsi que d'activer et de désactiver le service.

TABLEAU 5–1 Configuration d'IP Filter (liste des tâches)

Tâche	Voir
Affichage des fichiers utilisés par IP Filter et du statut du service.	“Affichage des valeurs par défaut du service IP Filter” à la page 54
Personnalisation des ensembles de règles de filtrage de paquets pour le trafic réseau, de paquets sur un NAT et de pools d'adresses.	“Création de fichiers de configuration IP Filter” à la page 55
Activation, désactivation ou actualisation du service IP Filter.	“Activation et actualisation d'IP Filter” à la page 56
Modification de la valeur par défaut des paquets arrivant en fragments.	“Désactivation du réassemblage des paquets” à la page 57
Filtrage du trafic entre les zones sur votre système.	“Activation du filtrage de loopback” à la page 58

TABLEAU 5–1 Configuration d'IP Filter (liste des tâches) *(Suite)*

Tâche	Voir
Arrêt de l'utilisation d'IP Filter.	"Désactivation du filtrage de paquets" à la page 59

▼ Affichage des valeurs par défaut du service IP Filter

Avant de commencer Pour exécuter la commande `ipfstat`, vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Affichez les noms de fichiers de configuration et les emplacements pour le service IP Filter.

```
% svccfg -s ipfilter:default listprop   | grep file
config/ipf6_config_file                      astring     /etc/ipf/ipf6.conf
config/ipnat_config_file                     astring     /etc/ipf/ipnat.conf
config/ippool_config_file                    astring     /etc/ipf/ippool.conf
firewall_config_default/custom_policy_file   astring     none
```

Des emplacements sont suggérés pour les trois premières propriétés de fichiers. Ces fichiers n'existent pas tant que vous ne les avez pas créés. Vous pouvez modifier l'emplacement d'un fichier de configuration en modifiant la valeur de la propriété de ce fichier. Pour plus d'informations sur cette procédure, reportez-vous à la section "Création de fichiers de configuration IP Filter" à la page 55.

Vous modifiez la quatrième propriété de fichier lorsque vous personnalisez vos propres règles de filtrage de paquets. Reportez-vous à l'Étape 1 et à l'Étape 2 de la section "Création de fichiers de configuration IP Filter" à la page 55.

2 Déterminez si le service IP Filter est activé.

- Sur un système en réseau manuel, IP Filter n'est pas activé par défaut.

  ```
  % svcs -x ipfilter:default
  svc:/network/ipfilter:default (IP Filter)
   State: disabled since Mon Sep 10 10:10:50 2012
  Reason: Disabled by an administrator.
     See: http://oracle.com/msg/SMF-8000-05
     See: ipfilter(5)
  Impact: This service is not running.
  ```

- Sur un système en réseau automatique sur un réseau IPv4, exécutez la commande suivante pour afficher la stratégie IP Filter :

  ```
  $ ipfstat -io
  ```

  Pour afficher le fichier qui a créé la stratégie, reportez-vous à `/etc/nwam/loc/NoNet/ipf.conf`. Ce fichier est en lecture seule. Pour modifier la stratégie, reportez-vous à la section "Création de fichiers de configuration IP Filter" à la page 55.

Remarque – Pour afficher la stratégie IP Filter sur un réseau IPv6, ajoutez l'option `-6`, comme dans : `ipfstat -6io`. Pour plus d'informations, reportez-vous à la page de manuel `ipfstat(1M)`.

Création de fichiers de configuration IP Filter

Pour modifier la stratégie IP Filter pour une configuration réseau configurée de manière automatique ou pour utiliser IP Filter dans un réseau configuré manuellement, créez des fichiers de configuration, informez le service de l'existence de ces fichiers, puis activez le service.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Spécifiez l'emplacement du fichier de stratégie pour le service IP Filter.

Ce fichier contient l'ensemble des règles de filtrage de paquets.

a. Définissez tout d'abord le fichier de stratégie sur `custom`.

```
$ svccfg -s ipfilter:default setprop firewall_config_default/policy = astring: "custom"
```

b. Indiquez ensuite l'emplacement.

Par exemple, placez votre ensemble de règles de filtrage de paquets à l'emplacement `/etc/ipf/myorg.ipf.conf`.

```
$ svccfg -s ipfilter:default \
setprop firewall_config_default/custom_policy_file = astring: "/etc/ipf/myorg.ipf.conf"
```

2 Créez votre ensemble de règles de filtrage de paquets.

Pour plus d'informations sur le filtrage de paquets, reportez-vous à la section "Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter" à la page 44. Pour consulter des exemples de fichiers de configuration, reportez-vous à la section "Exemples de fichiers de configuration IP Filter" à la page 78 et au fichier `/etc/nwam/loc/NoNet/ipf.conf`.

Remarque – Si le fichier de stratégie spécifié est vide, aucun filtrage n'est effectué. Un fichier de filtrage de paquets vide correspond à un ensemble de règles défini comme suit :

```
pass in all
pass out all
```

3 **(Facultatif) Créez un fichier de configuration de translation d'adresse réseau (NAT, Network Address Translation) pour IP Filter.**

Pour filtrer des paquets par le biais d'une NAT, créez un fichier destiné à contenir les règles NAT sous un nom pertinent, tel que `/etc/ipf/ipnat.conf` par exemple. Pour modifier ce nom, modifiez la valeur de la propriété de service `config/ipnat_config_file`, comme illustré ci-dessous :

```
$ svccfg -s ipfilter:default \
setprop config/ipnat_config_file = astring: "/etc/ipf/myorg.ipnat.conf"
```

Pour plus d'informations sur NAT, reportez-vous à la section "Utilisation de la fonctionnalité NAT d'IP Filter" à la page 47.

4 **(Facultatif) Créez un fichier de configuration de pool d'adresses.**

Pour pouvoir faire référence à un groupe d'adresses par le biais d'un pool d'adresses unique, créez un fichier contenant le pool sous un nom approprié, tel que `/etc/ipf/ippool.conf` par exemple. Pour modifier ce nom, modifiez la valeur de la propriété de service `config/ippool_config_file` , comme illustré ci-dessous :

```
$ svccfg -s ipfilter:default \
setprop config/ippool_config_file = astring: "/etc/ipf/myorg.ippool.conf"
```

Un pool d'adresses peut contenir un ensemble quelconque d'adresses IPv4 et IPv6. Pour plus d'informations sur les pools d'adresses, reportez-vous à la section "Utilisation de la fonctionnalité de pools d'adresses d'IP Filter" à la page 48.

5 **(Facultatif) Activez le filtrage du trafic en loopback.**

Pour filtrer le trafic entre les zones configurées sur le système, le cas échéant, activez le filtrage de loopback. Reportez-vous à la section "Activation du filtrage de loopback" à la page 58. Vous devez également définir des ensembles de règles applicables aux zones.

6 **(Facultatif) Désactivez le réassemblage des paquets fragmentés.**

Par défaut, les fragments sont réassemblés dans IP Filter. Pour modifier cette valeur par défaut, reportez-vous à la section "Désactivation du réassemblage des paquets" à la page 57.

▼ Activation et actualisation d'IP Filter

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Vous avez effectué les étapes de la section "Création de fichiers de configuration IP Filter" à la page 55.

1. **Activez IP Filter.**

   Pour activer IP Filter pour la première fois, saisissez la commande suivante :

   ```
   $ svcadm enable network/ipfilter
   ```

2. **Si vous modifiez des fichiers de configuration d'IP Filter alors que le service est en cours d'exécution, actualisez le service.**

   ```
   $ svcadm refresh network/ipfilter
   ```

Remarque – La commande `refresh` désactive brièvement le pare-feu. Pour ne pas désactiver le pare-feu, ajoutez des règles ou un nouveau fichier de configuration. Pour consulter des procédures illustrées à l'aide d'exemples, reportez-vous à la section "Utilisation des ensembles de règles IP Filter" à la page 59.

▼ Désactivation du réassemblage des paquets

Par défaut, les fragments sont réassemblés dans IP Filter. Pour désactiver le réassemblage, insérez une règle au début du fichier de stratégie.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter) ainsi que de l'autorisation `solaris.admin.edit/`*path-to-IPFilter-policy-file*. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Désactivez IP Filter.**

   ```
   $ svcadm disable network/ipfilter
   ```

2. **Ajoutez la règle suivante au début du fichier de stratégie IP Filter.**

   ```
   set defrag off;
   ```

   Utilisez la commande `pfedit`, comme illustré ci-dessous :

   ```
   $ pfedit /etc/ipf/myorg.ipf.conf
   ```

   Cette règle doit précéder toutes les règles `block` et `pass` définies dans le fichier. Toutefois, vous pouvez insérer des commentaires avant la ligne, comme dans l'exemple ci-dessous :

   ```
   # Disable fragment reassembly
   #
   set defrag off;
   # Define policy
   #
   block in all
   block out all
   other rules
   ```

3 Activez IP Filter.

```
$ svcadm enable network/ipfilter
```

4 Assurez-vous que les paquets ne sont pas réassemblés.

```
$ ipf -T defrag
defrag  min 0   max 0x1 current 0
```

Si la valeur associée à `current` est `0`, les fragments ne sont pas réassemblés. Si la valeur associée à `current` est `1`, les fragments sont réassemblés.

▼ Activation du filtrage de loopback

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter) ainsi que de l'autorisation `solaris.admin.edit/`*path-to-IPFilter-policy-file*. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Le cas échéant, arrêtez IP Filter.

```
$ svcadm disable network/ipfilter
```

2 Ajoutez la règle suivante au début du fichier de stratégie IP Filter.

```
set intercept_loopback true;
```

Utilisez la commande `pfedit`, comme illustré ci-dessous :

```
$ pfedit /etc/ipf/myorg.ipf.conf
```

Cette ligne doit précéder toutes les règles `block` et `pass` définies dans le fichier. Toutefois, vous pouvez insérer des commentaires avant la ligne, comme dans l'exemple ci-dessous :

```
...
#set defrag off;
#
# Enable loopback filtering to filter between zones
#
set intercept_loopback true;
#
# Define policy
#
block in all
block out all
other rules
```

3 Activez IP Filter.

```
$ svcadm enable network/ipfilter
```

4. **Pour vérifier le statut du filtrage de loopback, exécutez la commande ci-dessous :**

```
$ ipf -T ipf_loopback
ipf_loopback    min 0   max 0x1 current 1
$
```

Si la valeur associée à `current` est `0`, le filtrage de loopback est désactivé. Si la valeur associée à `current` est `1`, le filtrage de loopback est activé.

▼ Désactivation du filtrage de paquets

Cette procédure supprime toutes les règles à partir du noyau et désactive le service. Si vous avez recours à cette procédure, vous devez activer IP Filter avec les fichiers de configuration appropriés pour redémarrer le filtrage de paquets et la translation NAT. Pour plus d'informations, reportez-vous à la section "Activation et actualisation d'IP Filter" à la page 56.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Pour désactiver le service, utilisez la commande `svcadm`.**

```
$ svcadm disable network/ipfilter
```

Pour tester ou déboguer le service, vous pouvez supprimer des ensembles de règles pendant que le service est en cours d'exécution. Pour plus d'informations, reportez-vous à la section "Utilisation des ensembles de règles IP Filter" à la page 59.

Utilisation des ensembles de règles IP Filter

Vous pouvez modifier ou désactiver le filtrage des paquets et les règles NAT dans les conditions suivantes :

- En vue de réaliser des tests
- En vue de résoudre des problèmes système qui semblent être causés par IP Filter

La liste des tâches ci-dessous identifie les procédures associées aux ensembles de règles IP Filter.

TABLEAU 5–2 Utilisation des ensembles de règles IP Filter (liste des tâches)

Tâche	Voir
Affichage de l'ensemble de règles de filtrage de paquets actif.	"Affichage de l'ensemble actif de règles de filtrage de paquets" à la page 61
Affichez un ensemble de règles inactif pour le filtrage de paquets.	"Affichage de l'ensemble inactif de règles de filtrage de paquets" à la page 61

TABLEAU 5–2 Utilisation des ensembles de règles IP Filter (liste des tâches) *(Suite)*

Tâche	Voir
Activez un nouvel ensemble de règles actif.	“Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour” à la page 61
Supprimez un ensemble de règles.	“Suppression d'un ensemble de règles de filtrage de paquets” à la page 62
Ajoutez des règles aux ensembles de règles.	“Ajout de règles à l'ensemble actif de règles de filtrage de paquets” à la page 63 “Ajout de règles à l'ensemble inactif de règles de filtrage de paquets” à la page 64
Basculez entre les ensembles de règles actif et inactif.	“Basculement entre les ensembles actif et inactif de règles de filtrage de paquets” à la page 65
Supprimez du noyau un ensemble de règles inactif.	“Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau” à la page 66
Affichez les règles NAT actives.	“Affichage des règles NAT actives dans IP Filter” à la page 67
Suppression des règles NAT.	“Désactivation des règles NAT dans IP Filter” à la page 67
Ajout de règles à des règles NAT actives.	“Ajout de règles aux règles de filtrage de paquets NAT” à la page 68
Affichez les pools d'adresses actifs.	“Affichage des pools d'adresses actifs” à la page 69
Supprimez un pool d'adresses.	“Suppression d'un pool d'adresses” à la page 69
Ajout de règles à un pool d'adresses.	“Ajout de règles à un pool d'adresses” à la page 70

Gérez les ensembles de règles de filtrage de paquets d'IP Filter

IP Filter autorise l'hébergement dans le noyau d'un ensemble de règles de filtrage de paquets actif et d'un ensemble de règles inactif. L'ensemble de règles actif détermine le filtrage appliqué aux paquets entrants et aux paquets sortants. L'ensemble de règles inactif contient également des règles. Ces règles ne sont pas appliquées, sauf si vous définissez l'ensemble de règles inactif comme l'ensemble de règles actif. Vous pouvez gérer, afficher et modifier les ensembles actif et inactif de règles de filtrage de paquets.

Remarque – Les procédures suivantes fournissent des exemples pour des réseaux IPv4. Pour les paquets IPv6, utilisez l'option `-6` tel que décrit à l'Étape 2 de la section “Affichage des valeurs par défaut du service IP Filter” à la page 54.

Affichage de l'ensemble actif de règles de filtrage de paquets

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichage de l'ensemble de règles de filtrage de paquets actif.**

  L'exemple ci-dessous présente la sortie de l'ensemble actif de règles de filtrage de paquets chargé dans le noyau.

```
$ ipfstat -io
empty list for ipfilter(out)
pass in quick on net1 from 192.168.1.0/24 to any
pass in all
block in on net1 from 192.168.1.10/32 to any
```

Affichage de l'ensemble inactif de règles de filtrage de paquets

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez l'ensemble inactif de règles de filtrage de paquets.**

  L'exemple ci-dessous présente la sortie d'un ensemble inactif de règles de filtrage de paquets.

```
$ ipfstat -I -io
pass out quick on net1 all
pass in quick on net1 all
```

Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour

Effectuez la procédure ci-dessous pour exécuter l'une ou l'autre des tâches suivantes :

- Activation d'un ensemble de règles de filtrage de paquets différent de celui que IP Filter utilise actuellement
- Rechargement du même ensemble de règles de filtrage mis à jour.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1. **Procédez de l'une des façons suivantes :**

   - Si vous souhaitez activer un ensemble de règles complètement différent, créez un nouvel ensemble de règles dans un fichier distinct.

- Mettez à jour l'ensemble de règles actuel dans votre fichier de configuration.

2 **Supprimez l'ensemble de règles actuel et chargez le nouvel ensemble de règles.**

```
$ ipf -Fa -f filename
```

Les règles présentes dans *filename* remplacent l'ensemble de règles actif.

Remarque – N'utilisez pas de commandes telles que `ipf -D` ou `svcadm restart` pour charger l'ensemble de règles mis à jour. Ces commandes affectent la sécurité du réseau, car elles désactivent le pare-feu avant de charger le nouvel ensemble de règles.

Exemple 5–1 Activation d'un nouvel ensemble de règles de filtrage de paquets

L'exemple suivant illustre le remplacement d'un ensemble de règles de filtrage de paquets par un autre ensemble de règles.

```
$ ipfstat -io
empty list for ipfilter(out)
pass in quick on net0 all
$ ipf -Fa -f /etc/ipf/ipfnew.conf
$ ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
```

Exemple 5–2 Rechargement d'un ensemble de règles de filtrage de paquets mis à jour

Dans l'exemple ci-dessous, un ensemble de règles de filtrage de paquets actuellement actif est rechargé suite à sa mise à jour.

```
$ ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any

(Edit the /etc/ipf/myorg.ipf.conf configuration file.)

$ svcadm refresh network/ipfilter
$ ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any
block in quick on net11 from 192.168.0.0/12 to any
```

▼ Suppression d'un ensemble de règles de filtrage de paquets

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Supprimez l'ensemble de règles.**

  ```
  $ ipf -F [a|i|o]
  ```

  `-a` Supprime toutes les règles de filtrage de l'ensemble de règles.

  `-i` Supprime les règles de filtrage pour les paquets entrants.

  `-o` Supprime les règles de filtrage pour les paquets sortants.

Exemple 5–3 Suppression d'un ensemble de règles de filtrage de paquets

Dans l'exemple ci-dessous, toutes les règles de filtrage sont supprimées de l'ensemble de règles de filtrage actif.

```
$ ipfstat -io
block out log on net0 all
block in log quick from 10.0.0.0/8 to any
$ ipf -Fa
$ ipfstat -io
empty list for ipfilter(out)
empty list for ipfilter(in)
```

▼ Ajout de règles à l'ensemble actif de règles de filtrage de paquets

L'ajout de règles à un ensemble de règles existant peut être utile lors de la réalisation de tests ou lors du débogage. Le service IP Filter reste activé lorsque les règles sont ajoutées. Toutefois, lorsque le service est actualisé, redémarré ou activé, les règles sont perdues, sauf si elles existent dans des fichiers constituant des propriétés du service IP Filter.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :**

  - Pour ajouter des règles à l'ensemble de règles via la ligne de commande, exécutez la commande `ipf -f -`.

    ```
    $ echo "block in on net1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
    ```

    Ces règles ajoutées ne font pas partie de la configuration d'IP Filter lorsque le service est actualisé, redémarré ou activé.

  - Exécutez les commandes ci-dessous :

    a. Créez un ensemble de règles dans le fichier de votre choix.

    b. Ajoutez les règles que vous avez créées à l'ensemble de règles actif.

```
$ ipf -f filename
```

Les règles présentes dans le fichier *filename* sont ajoutées à la fin de l'ensemble de règles actif. IP Filter utilise un algorithme de type "dernière règle correspondante", de sorte que les nouvelles règles déterminent les priorités de filtrage, sauf si l'utilisateur ajoute le mot-clé `quick`. Si le paquet correspond à une règle contenant le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées.

Si *filename* est la valeur de l'une des propriétés de fichiers de configuration IP Filter, les règles sont rechargées lorsque le service est activé, redémarré ou actualisé. Dans le cas contraire, les règles ajoutées forment un ensemble de règles temporaire.

Exemple 5–4 Ajout de règles à l'ensemble actif de règles de filtrage de paquets

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble actif de règles de filtrage de paquets à partir de la ligne de commande.

```
$ ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
$ echo "block in on net1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
$ ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on net1 proto tcp from 10.1.1.1/32 to any
```

▼ Ajout de règles à l'ensemble inactif de règles de filtrage de paquets

La création d'un ensemble de règles inactif dans le noyau peut être utile pour la réalisation de tests ou le débogage. Cet ensemble de règles peut être substitué à l'ensemble de règles actif sans qu'il soit nécessaire d'arrêter le service IP Filter. Toutefois, lorsque le service est actualisé, redémarré ou activé, l'ensemble de règles inactif doit être ajouté.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Créez un ensemble de règles dans le fichier de votre choix.

2 Ajoutez les règles que vous avez créées à l'ensemble de règles inactif.

```
$ ipf -I -f filename
```

Les règles présentes dans le fichier *filename* sont ajoutées à la fin de l'ensemble de règles inactif. IP Filter utilise un algorithme de type "dernière règle correspondante", de sorte que les

nouvelles règles déterminent les priorités de filtrage, sauf si l'utilisateur ajoute le mot-clé `quick`. Si le paquet correspond à une règle contenant le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées.

Exemple 5–5 Ajout de règles à l'ensemble de règles inactif

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble de règles inactif à partir d'un fichier.

```
$ ipfstat -I -io
pass out quick on net1 all
pass in quick on net1 all
$ ipf -I -f /etc/ipf/ipftrial.conf
$ ipfstat -I -io
pass out quick on net1 all
pass in quick on net1 all
block in log quick from 10.0.0.0/8 to any
```

▼ Basculement entre les ensembles actif et inactif de règles de filtrage de paquets

Le passage à un autre ensemble de règles dans le noyau peut être utile lors de la réalisation de tests ou du débogage. L'ensemble de règles peut être rendu actif sans qu'il soit nécessaire d'arrêter le service IP Filter.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Basculez entre les ensembles de règles actif et inactif.**

  ```
  $ ipf -s
  ```

  Cette commande permet de basculer entre les ensembles de règles actif et inactif dans le noyau. Si l'ensemble de règles inactif est vide, aucun filtrage de paquets n'est effectué.

Remarque – Lorsque le service IP Filter est actualisé, redémarré ou activé, les règles enregistrées dans des fichiers constituant des propriétés du service IP Filter sont restaurées. L'ensemble de règles inactif n'est pas restauré.

Exemple 5–6 Basculement entre les ensembles actif et inactif de règles de filtrage de paquets

L'exemple ci-dessous illustre l'utilisation de la commande `ipf -s`, laquelle a pour effet de rendre actif l'ensemble de règles inactif et de rendre inactif l'ensemble de règles actif.

- Avant l'exécution de la commande `ipf -s`, la sortie de la commande `ipfstat -I -io` met en évidence les règles de l'ensemble de règles inactif. La sortie de la commande `ipfstat -io` affiche les règles dans l'ensemble de règles actif.

```
$ ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on net1 proto tcp from 10.1.1.1/32 to any
$ ipfstat -I -io
pass out quick on net1 all
pass in quick on net1 all
block in log quick from 10.0.0.0/8 to any
```

- Après l'exécution de la commande `ipf -s`, les sorties des commandes `ipfstat -I -io` et `ipfstat -io` indiquent que le contenu des deux ensembles de règles a été échangé.

```
$ ipf -s
Set 1 now inactive
$ ipfstat -io
pass out quick on net1 all
pass in quick on net1 all
block in log quick from 10.0.0.0/8 to any
$ ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on net1 proto tcp from 10.1.1.1/32 to any
```

▼ Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Spécifiez l'ensemble de règles inactif via la commande "flush all".**

```
$ ipf -I -Fa
```

Remarque – Si vous exécutez ensuite la commande `ipf -s`, l'ensemble de règles inactif vide devient l'ensemble de règles actif. Si l'ensemble de règles actif est vide, *aucun* filtrage n'est effectué.

Exemple 5–7 Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau

Dans l'exemple ci-dessous, l'ensemble inactif de règles de filtrage de paquets est vidé afin de supprimer toutes les règles.

```
$ ipfstat -I -io
empty list for inactive ipfilter(out)
```

```
block in log quick from 10.0.0.0/8 to any
block in on net1 proto tcp from 10.1.1.1/32 to any
$ ipf -I -Fa
$ ipfstat -I -io
empty list for inactive ipfilter(out)
empty list for inactive ipfilter(in)
```

Gestion des règles NAT d'IP Filter

Appliquez les procédures suivantes pour gérer, afficher et modifier les règles NAT pour IP Filter.

▼ Affichage des règles NAT actives dans IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez les règles NAT actives.**

  L'exemple ci-dessous présente la sortie de l'ensemble de règles NAT actif.

```
$ ipnat -l
List of active MAP/Redirect filters:
map net0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

▼ Désactivation des règles NAT dans IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Supprimez les règles NAT du noyau.**

```
$ ipnat -FC
```

  L'option `-C` permet de supprimer toutes les entrées de la liste de règles NAT actuelle. L'option `-F` permet de supprimer toutes les entrées actives de la table de translation NAT qui indique les mappages NAT actifs.

Exemple 5–8 Suppression des règles NAT

Dans l'exemple ci-dessous, les entrées des règles NAT actuelles sont supprimées.

```
$ ipnat -l
List of active MAP/Redirect filters:
```

```
map net0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
$ ipnat -C
1 entries flushed from NAT list
$ ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
```

▼ Ajout de règles aux règles de filtrage de paquets NAT

L'ajout de règles à un ensemble de règles existant peut être utile lors de la réalisation de tests ou lors du débogage. Le service IP Filter reste activé lorsque les règles sont ajoutées. Toutefois, lorsque le service est actualisé, redémarré ou activé, les règles NAT sont perdues, sauf si elles existent dans un fichier constituant une propriété du service IP Filter.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :**
  - Pour ajouter des règles à l'ensemble de règles NAT via la ligne de commande, exécutez la commande `ipnat -f -`.

    ```
    $ echo "map net0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
    ```

    Ces règles ajoutées ne font pas partie de la configuration d'IP Filter lorsque le service est actualisé, redémarré ou activé.
  - Exécutez les commandes ci-dessous :
    a. Créez des règles NAT supplémentaires dans le fichier de votre choix.
    b. Ajoutez les règles que vous avez créées aux règles NAT actives.

       ```
       $ ipnat -f filename
       ```

       Les règles présentes dans le fichier *filename* sont ajoutées à la fin des règles NAT.

       Si *filename* est la valeur de l'une des propriétés de fichiers de configuration IP Filter, les règles sont rechargées lorsque le service est activé, redémarré ou actualisé. Dans le cas contraire, les règles ajoutées forment un ensemble de règles temporaire.

Exemple 5–9 Ajout de règles à l'ensemble de règles NAT

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble de règles NAT via la ligne de commande.

```
$ ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
$ echo "map net0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
$ ipnat -l
List of active MAP/Redirect filters:
map net0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

Gestion des pools d'adresses d'IP Filter

Appliquez les procédures ci-dessous pour gérer, afficher et modifier les pools d'adresses.

▼ Affichage des pools d'adresses actifs

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez le pool d'adresses actif.**

  Dans l'exemple ci-dessous, le contenu du pool d'adresses actif est affiché.

```
$ ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

▼ Suppression d'un pool d'adresses

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Supprimez les entrées du pool d'adresses actuel.**

```
$ ippool -F
```

Exemple 5–10 Suppression d'un pool d'adresses

Dans l'exemple ci-dessous, un pool d'adresses est supprimé.

```
$ ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
$ ippool -F
```

```
1 object flushed
$ ippool -l
```

▼ Ajout de règles à un pool d'adresses

L'ajout de règles à un ensemble de règles existant peut être utile lors de la réalisation de tests ou lors du débogage. Le service IP Filter reste activé lorsque les règles sont ajoutées. Toutefois, lorsque le service est actualisé, redémarré ou activé, les règles de pools d'adresses sont perdues, sauf si elles existent dans un fichier constituant une propriété du service IP Filter.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :

- Pour ajouter des règles à l'ensemble de règles via la ligne de commande, exécutez la commande `ippool -f -`.

  ```
  $ echo "table role = ipf type = tree number = 13
  {10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24};" | ippool -f -
  ```

  Ces règles ajoutées ne font pas partie de la configuration d'IP Filter lorsque le service est actualisé, redémarré ou activé.
- Exécutez les commandes ci-dessous :
  a. Créez des pools d'adresses supplémentaires dans le fichier de votre choix.
  b. Ajoutez les règles que vous avez créées au pool d'adresses actif.

     ```
     $ ippool -f filename
     ```

     Les règles présentes dans le fichier *filename* sont ajoutées à la fin du pool d'adresses actif.

2 Si les règles contiennent des pools qui ne figurent pas dans l'ensemble de règles d'origine, procédez comme suit :

a. Ajoutez les pools à une nouvelle règle de filtrage de paquets.

b. Ajoutez la nouvelle règle de filtrage de paquets à l'ensemble de règles actuel.

Suivez les instructions de la section "Ajout de règles à l'ensemble actif de règles de filtrage de paquets" à la page 63.

Remarque – N'actualisez ou ne redémarrez pas le service IP Filter ou vous allez perdre les règles de pools d'adresses ajoutées.

Exemple 5–11 Ajout de règles à un pool d'adresses

Dans l'exemple ci-dessous, un pool d'adresses est ajouté à l'ensemble de règles de pool d'adresses via la ligne de commande.

```
$ ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
$ echo "table role = ipf type = tree number = 100
 {10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24};" | ippool -f -
$ ippool -l
table role = ipf type = tree number = 100
        { 10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24; };
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

Affichage des statistiques et des informations relatives à IP Filter

TABLEAU 5–3 Affichage des statistiques et informations IP Filter (liste des tâches)

Tâche	Voir
Affichage des tables d'état.	"Affichage des tables d'état d'IP Filter" à la page 71
Affichage des statistiques sur l'état des paquets.	"Affichage des statistiques d'état d'IP Filter" à la page 72
Liste des paramètres réglables IP Filter.	"Affichage des paramètres réglables IP Filter" à la page 73
Affichage des statistiques NAT.	"Affichage des statistiques NAT d'IP Filter" à la page 73
Affichage des statistiques de pool d'adresses	"Affichage des statistiques de pool d'adresses d'IP Filter" à la page 74

▼ Affichage des tables d'état d'IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez la table d'état.**

```
$ ipfstat
```

Remarque – L'option `-t` permet d'afficher la table d'état au format de l'utilitaire `top` UNIX.

Exemple 5–12 Affichage des tables d'état d'IP Filter

L'exemple suivant illustre la sortie de la table d'état.

```
$ ipfstat
bad packets:            in 0    out 0
 IPv6 packets:          in 56286 out 63298
 input packets:         blocked 160 passed 11 nomatch 1 counted 0 short 0
output packets:         blocked 0 passed 13681 nomatch 6844 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  152     (out):  6837
IN Pullups succeeded:   0       failed: 0
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      14341469
Packet log flags set: (0)
        none
```

▼ Affichage des statistiques d'état d'IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez les statistiques d'état.**

```
$ ipfstat -s
```

Exemple 5–13 Affichage des statistiques d'état d'IP Filter

L'exemple suivant illustre la sortie des statistiques d'état.

```
$ ipfstat -s
IP states added:
        0 TCP
```

```
        0 UDP
        0 ICMP
        0 hits
        0 misses
        0 maximum
        0 no memory
        0 max bucket
        0 active
        0 expired
        0 closed
State logging enabled

State table bucket statistics:
        0 in use
        0.00% bucket usage
        0 minimal length
        0 maximal length
        0.000 average length
```

▼ Affichage des paramètres réglables IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez les paramètres réglables du noyau pour IP Filter.**

  La sortie suivante est tronquée.

```
$ ipf -T list
fr_flags    min 0    max 0xffffffff    current 0
fr_active    min 0    max 0    current 0
...
ipstate_logging    min 0    max 0x1    current 1
...
fr_authq_ttl    min 0x1    max 0x7fffffff    current sz = 0
fr_enable_rcache    min 0    max 0x1    current 0
```

▼ Affichage des statistiques NAT d'IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichage des statistiques NAT.**

```
$ ipnat -s
```

Exemple 5–14 Affichage des statistiques NAT d'IP Filter

L'exemple ci-dessous illustre les statistiques NAT.

```
$ ipnat -s
mapped  in      0       out     0
added   0       expired 0
no memory       0       bad nat 0
inuse   0
rules   1
wilds   0
```

▼ Affichage des statistiques de pool d'adresses d'IP Filter

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichage des statistiques de pool d'adresses**

```
$ ippool -s
```

Exemple 5–15 Affichage des statistiques de pool d'adresses d'IP Filter

L'exemple suivant illustre les statistiques de pool d'adresses.

```
$ ippool -s
Pools:  3
Hash Tables:    0
Nodes:  0
```

Utilisation des fichiers journaux IP Filter

TABLEAU 5–4 Utilisation des fichiers journaux IP Filter (liste des tâches)

Tâche	Voir
Créez un fichier journal IP Filter distinct.	"Configuration d'un fichier journal d'IP Filter" à la page 75
Affichage des journaux d'état, NAT et normaux.	"Affichage des fichiers journaux IP Filter" à la page 76
Vidage du tampon de journalisation des paquets	"Vidage du tampon du journal de paquets" à la page 77
Les paquets consignés peuvent être enregistrés dans un fichier afin d'être consultés par la suite.	"Enregistrement dans un fichier des paquets consignés" à la page 77

▼ Configuration d'un fichier journal d'IP Filter

Par défaut, toutes les informations de journal IP Filter sont enregistrées dans le fichier `syslogd`. Il est recommandé de créer un fichier journal distinct dans lequel enregistrer les informations de trafic IP Filter afin de séparer ces données des autres données susceptibles d'être consignées dans le fichier journal par défaut.

Avant de commencer Vous devez prendre le rôle `root`.

1 Déterminez quelle instance de service `system-log` est en ligne.

```
# svcs system-log
STATE          STIME    FMRI
disabled       13:11:55 svc:/system/system-log:rsyslog
online         13:13:27 svc:/system/system-log:default
```

Remarque – Si l'instance de service `rsyslog` est en ligne, modifiez le fichier `rsyslog.conf`.

---

2 Ajoutez les lignes suivantes au fichier `/etc/syslog.conf` :

```
# Save IP Filter log output to its own file
local0.debug             /var/log/log-name
```

Remarque – Dans votre entrée, utilisez la touche de tabulation (et non la barre d'espacement), pour séparer `local0.debug` de `/var/log/`*log-name*. Pour plus d'informations, reportez-vous aux pages de manuel `syslog.conf(4)` et `syslogd(1M)`.

---

3 Créez le fichier journal.

```
# touch /var/log/log-name
```

4 Actualisez les informations de configuration du service `system-log`.

```
# svcadm refresh system-log:default
```

Remarque – Actualisez l'instance de service `system-log:rsyslog` si le service `rsyslog` est en ligne.

Exemple 5–16 Création d'un journal IP Filter

L'exemple suivant crée le fichier `ipmon.log` pour archiver les informations IP Filter.

Dans `/etc/syslog.conf` :

```
## Save IP Filter log output to its own file
local0.debug<Tab>/var/log/ipmon.log
```

Sur la ligne de commande :

```
# touch /var/log/ipmon.log
# svcadm restart system-log
```

▼ Affichage des fichiers journaux IP Filter

Avant de commencer Vous avez effectué les étapes de la section "Configuration d'un fichier journal d'IP Filter" à la page 75.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichez le fichier journal normal, le fichier journal NAT ou le fichier journal d'état.**

  Pour afficher un fichier journal, tapez la commande ci-dessous, conjointement avec l'option adéquate :

  # ipmon -o [S|N|I] *filename*

  `S` Affiche le fichier journal d'état.

  `N` Affiche le fichier journal NAT.

  `I` Affiche le fichier journal IP normal.

  - **Pour afficher le fichier journal normal et les fichiers journaux d'état et NAT, appliquez les options :**

    # ipmon -o SNI *filename*

  - **Après avoir arrêté le démon `ipmon`, vous pouvez utiliser la commande `ipmon` pour afficher les fichiers journaux d'état, NAT et IP Filter :**

    ```
    # pkill ipmon
    # ipmon -a filename
    ```

    Remarque – N'utilisez pas la syntaxe `ipmon -a` si le démon `ipmon` est en cours d'exécution. Normalement, le démon démarre automatiquement à l'initialisation du système. L'exécution de la commande `ipmon -a` ouvre une seconde instance d'`ipmon`. Dans ce cas, les deux copies lisent les mêmes informations de journal, mais tout message du journal n'est reçu que par l'une d'elles.

  Pour plus d'informations sur l'affichage des fichiers journaux, reportez-vous à la page de manuel `ipmon`(1M).

Exemple 5–17 Affichage des fichiers journaux IP Filter

L'exemple ci-dessous présente la sortie du fichier `/var/ipmon.log`.

```
# ipmon -o SNI /var/ipmon.log
02/09/2012 15:27:20.606626 net0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

ou

```
# pkill ipmon
# ipmon -aD /var/ipmon.log
02/09/2012 15:27:20.606626 net0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

▼ Vidage du tampon du journal de paquets

Cette procédure efface le tampon et affiche la sortie à l'écran.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits IP Filter Management (gestion IP Filter). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Vidage du tampon de journalisation des paquets**

  ```
  # ipmon -F
  ```

Exemple 5–18 Vidage du tampon du journal de paquets

L'exemple ci-dessous présente la sortie obtenue en cas de suppression d'un fichier journal. Le système génère un rapport même si le fichier journal est vide, comme dans cet exemple.

```
# ipmon -F
0 bytes flushed from log buffer
0 bytes flushed from log buffer
0 bytes flushed from log buffer
```

▼ Enregistrement dans un fichier des paquets consignés

Vous pouvez enregistrer des paquets dans un fichier lors du débogage ou si vous souhaitez effectuer un audit manuel du trafic.

Avant de commencer Vous devez prendre le rôle `root`.

- **Enregistrez dans un fichier les paquets consignés.**

  ```
  # cat /dev/ipl > filename
  ```

Continuez la journalisation des paquets dans le fichier *filename* et interrompez la procédure en tapant `Ctrl-C` pour afficher de nouveau l'invite de ligne de commande.

Exemple 5–19 Enregistrement dans un fichier des paquets consignés

L'exemple ci-dessous présente les résultats obtenus lorsque les paquets consignés sont enregistrés dans un fichier.

```
# cat /dev/ipl > /tmp/logfile
^C#

# ipmon -f /tmp/logfile
02/09/2012 15:30:28.708294 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 52 -S IN
02/09/2012 15:30:28.708708 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2012 15:30:28.792611 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 70 -AP IN
02/09/2012 15:30:28.872000 net0 @0:1 p 129.146.157.149,33923 ->
 129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2012 15:30:28.872142 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 43 -AP IN
02/09/2012 15:30:28.872808 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2012 15:30:28.872951 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 47 -AP IN
02/09/2012 15:30:28.926792 net0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
.
.
(output truncated)
```

Exemples de fichiers de configuration IP Filter

Les exemples suivants illustrent les règles de filtrage de paquets qui s'appliquent à un hôte unique, un serveur et un routeur.

Les fichiers de configuration suivent les règles de syntaxe UNIX standard :

- Le signe dièse (#) indique qu'une ligne contient des commentaires.
- Une ligne peut contenir à la fois des commentaires et des règles.
- Vous pouvez ajouter des espaces supplémentaires afin de faciliter la lecture des règles.
- La définition d'une règle peut s'étaler sur plusieurs lignes. Insérez un backslash (\) à la fin d'une ligne pour indiquer que la règle continue sur la ligne suivante.

Pour plus d'informations sur la syntaxe, reportez-vous à la section “Configuration des règles de filtrage de paquets” à la page 45.

EXEMPLE 5–20 Configuration d'un hôte IP Filter

Cet exemple illustre une configuration définie sur une machine hôte avec une interface réseau `net0`.

```
# pass and log everything by default
pass in log on net0 all
pass out log on net0 all

# block, but don't log, incoming packets from other reserved addresses
block in quick on net0 from 10.0.0.0/8 to any
block in quick on net0 from 172.16.0.0/12 to any

# block and log untrusted internal IPs. 0/32 is notation that replaces
# address of the machine running IP Filter.
block in log quick from 192.168.1.15 to <thishost>
block in log quick from 192.168.1.43 to <thishost>

# block and log X11 (port 6000) and remote procedure call
# and portmapper (port 111) attempts
block in log quick on net0 proto tcp from any to net0/32 port = 6000 keep state
block in log quick on net0 proto tcp/udp from any to net0/32 port = 111 keep state
```

Cet ensemble de règles commence par deux règles sans restrictions qui permettent à tous les type de données d'entrer et de sortir via l'interface `net0`. Le deuxième ensemble de règles empêche tout paquet entrant issu des espaces d'adressage privés `10.0.0.0` et `172.16.0.0` de traverser le pare-feu. L'ensemble de règles suivant bloque des adresses internes spécifiques de la machine hôte. Enfin, le dernier ensemble de règles empêche l'entrée des paquets via les ports 6000 et 111.

EXEMPLE 5–21 Configuration d'un serveur IP Filter

Cet exemple présente la configuration d'une machine hôte tenant lieu de serveur Web. Cette machine possède une interface réseau `net0`.

```
# web server with an net0 interface
# block and log everything by default;
# then allow specific services
# group 100 - inbound rules
# group 200 - outbound rules
# (0/32) resolves to our IP address)
*** FTP proxy ***

# block short packets which are packets
# fragmented too short to be real.
block in log quick all with short

# block and log inbound and outbound by default,
# group by destination
block in log on net0 from any to any head 100
block out log on net0 from any to any head 200


# web rules that get hit most often
```

EXEMPLE 5–21 Configuration d'un serveur IP Filter *(Suite)*

```
pass in quick on net0 proto tcp from any \
to net0/32 port = http flags S keep state group 100
pass in quick on net0 proto tcp from any \
to net0/32 port = https flags S keep state group 100


# inbound traffic - ssh, auth
pass in quick on net0 proto tcp from any \
to net0/32 port = 22 flags S keep state group 100
pass in log quick on net0 proto tcp from any \
to net0/32 port = 113 flags S keep state group 100
pass in log quick on net0 proto tcp from any port = 113 \
to net0/32 flags S keep state group 100

# outbound traffic - DNS, auth, NTP, ssh, WWW, smtp
pass out quick on net0 proto tcp/udp from net0/32 \
to any port = domain flags S keep state group 200
pass in quick on net0 proto udp from any \
port = domain to net0/32 group 100

pass out quick on net0 proto tcp from net0/32 \
to any port = 113 flags S keep state group 200
pass out quick on net0 proto tcp from net0/32 port = 113 \
to any flags S keep state group 200

pass out quick on net0 proto udp from net0/32 to any \
port = ntp group 200
pass in quick on net0 proto udp from any \
port = ntp to net0/32 port = ntp group 100

pass out quick on net0 proto tcp from net0/32 \
to any port = ssh flags S keep state group 200

pass out quick on net0 proto tcp from net0/32 \
to any port = http flags S keep state group 200
pass out quick on net0 proto tcp from net0/32 \
to any port = https flags S keep state group 200

pass out quick on net0 proto tcp from net0/32 \
to any port = smtp flags S keep state group 200


# pass icmp packets in and out
pass in quick on net0 proto icmp from any to net0/32  keep state group 100
pass out quick on net0 proto icmp from net0/32 to any keep state group 200

# block and ignore NETBIOS packets
block in quick on net0 proto tcp from any \
to any port = 135 flags S keep state group 100

block in quick on net0 proto tcp from any port = 137 \
to any flags S keep state group 100
block in quick on net0 proto udp from any to any port = 137 group 100
block in quick on net0 proto udp from any port = 137 to any group 100
```

EXEMPLE 5–21 Configuration d'un serveur IP Filter *(Suite)*

```
block in quick on net0 proto tcp from any port = 138 \
to any flags S keep state group 100
block in quick on net0 proto udp from any port = 138 to any group 100

block in quick on net0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on net0 proto udp from any port = 139 to any group 100
```

EXEMPLE 5–22 Configuration d'un routeur IP Filter

Cet exemple présente la configuration d'un routeur possédant une interface interne, `net0`, et une interface externe, `net1`.

```
# internal interface is net0 at 192.168.1.1
# external interface is net1 IP obtained via DHCP
# block all packets and allow specific services
*** NAT ***
*** POOLS ***

# Short packets which are fragmented too short to be real.
block in log quick all with short

# By default, block and log everything.
block in log on net0 all
block in log on net1 all
block out log on net0 all
block out log on net1 all


# Packets going in/out of network interfaces that aren't on the loopback
# interface should not exist.
block in log quick on net0 from 127.0.0.0/8 to any
block in log quick on net0 from any to 127.0.0.0/8
block in log quick on net1 from 127.0.0.0/8 to any
block in log quick on net1 from any to 127.0.0.0/8


# Deny reserved addresses.
block in quick on net1 from 10.0.0.0/8 to any
block in quick on net1 from 172.16.0.0/12 to any
block in log quick on net1 from 192.168.1.0/24 to any
block in quick on net1 from 192.168.0.0/16 to any


# Allow internal traffic
pass in quick on net0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on net0 from 192.168.1.0/24 to 192.168.1.0/24


# Allow outgoing DNS requests from our servers on .1, .2, and .3
pass out quick on net1 proto tcp/udp from net1/32 to any port = domain keep state
pass in quick on net0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
pass in quick on net0 proto tcp/udp from 192.168.1.3 to any port = domain keep state
```

EXEMPLE 5–22 Configuration d'un routeur IP Filter *(Suite)*

```
# Allow NTP from any internal hosts to any external NTP server.
pass in quick on net0 proto udp from 192.168.1.0/24 to any port = 123 keep state
pass out quick on net1 proto udp from any to any port = 123 keep state


# Allow incoming mail
pass in quick on net1 proto tcp from any to net1/32 port = smtp keep state
pass in quick on net1 proto tcp from any to net1/32 port = smtp keep state
pass out quick on net1 proto tcp from 192.168.1.0/24 to any port = smtp keep state


# Allow outgoing connections: SSH, WWW, NNTP, mail, whois
pass in quick on net0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
pass out quick on net1 proto tcp from 192.168.1.0/24 to any port = 22 keep state

pass in quick on net0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass out quick on net1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass in quick on net0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
pass out quick on net1 proto tcp from 192.168.1.0/24 to any port = 443 keep state

pass in quick on net0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
block in quick on net1 proto tcp from any to any port = nntp keep state
pass out quick on net1 proto tcp from 192.168.1.0/24 to any port = nntp keep state

pass in quick on net0 proto tcp from 192.168.1.0/24 to any port = smtp keep state

pass in quick on net0 proto tcp from 192.168.1.0/24 to any port = whois keep state
pass out quick on net1 proto tcp from any to any port = whois keep state


# Allow ssh from offsite
pass in quick on net1 proto tcp from any to net1/32 port = 22 keep state


# Allow ping out
pass in quick on net0 proto icmp all keep state
pass out quick on net1 proto icmp all keep state


# allow auth out
pass out quick on net1 proto tcp from net1/32 to any port = 113 keep state
pass out quick on net1 proto tcp from net1/32 port = 113 to any keep state


# return rst for incoming auth
block return-rst in quick on net1 proto tcp from any to any port = 113 flags S/SA


# log and return reset for any TCP packets with S/SA
block return-rst in log on net1 proto tcp from any to any flags S/SA

# return ICMP error packets for invalid UDP packets
block return-icmp(net-unr) in proto udp all
```

◆ ◆ ◆ CHAPITRE 6

Architecture IPsec (présentation)

L'architecture IPsec (IP security) offre la protection cryptographique des datagrammes IP dans les paquets réseau IPv4 et IPv6.

Le présent chapitre contient les informations suivantes :

Pour implémenter IPsec sur votre réseau, reportez-vous au Chapitre 7, "Configuration d'IPsec (tâches)". Pour des informations de référence, reportez-vous au Chapitre 8, "Architecture IPsec (référence)".

Introduction à IPsec

Pour protéger les paquets IP, IPsec les chiffre et/ou les authentifie. IPsec s'exécute dans le module IP. Par conséquent, une application Internet peut tirer profit d'IPsec sans pour autant avoir à modifier sa configuration. Une utilisation à bon escient d'IPsec en fait un outil efficace de sécurisation du trafic réseau.

La protection IPsec implique les composants principaux suivants :

- **Protocoles de sécurité :** les mécanismes de protection de datagramme IP. L'en-tête d'authentification (AH) inclut un hachage du paquet IP et garantit l'intégrité. Bien que le contenu du datagramme ne soit pas chiffré, le destinataire est sûr que le contenu du paquet n'a subi aucune modification et que l'expéditeur a envoyé les paquets. protocole ESP chiffre les données IP et obscurcit, par conséquent, le contenu des paquets lors de leur transmission. ESP garantit également l'intégrité des données par le biais d'une option d'algorithme d'authentification.
- **Associations de sécurité (SA) :** paramètres cryptographiques et protocole de sécurité IP appliqués à un flux de trafic réseau donné. Chaque SA dispose d'une référence unique appelée SPI (security parameter index, index de paramètres de sécurité).
- **Base de données des associations de sécurité (SADB) :** base de données qui associe un protocole de sécurité à une adresse IP de destination et un numéro d'indexation. Ce numéro d'indexation est appelé index du paramètre de sécurité. Ces trois éléments (protocole de sécurité, adresse de destination et SPI) identifient un seul paquet IPsec légitime. La base de données garantit que le paquet protégé est reconnu par le récepteur à son arrivée. Elle permet également au récepteur de déchiffrer la communication, de vérifier que les paquets n'ont pas été altérés, de rassembler les paquets et de livrer les paquets à leur destination finale.
- **Gestion des clés :** génération et distribution des clés des algorithmes cryptographiques et de SPI.
- **Mécanismes de sécurité :** algorithmes de chiffrement et d'authentification qui protègent les données des datagrammes IP.
- **SPD (Security Policy Database, base de données de stratégie de sécurité) :** base de données indiquant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP et identifie le mode de traitement des paquets. Un paquet peut être rejeté, passé au clair ou protégé à l'aide d'IPsec. En ce qui concerne les paquets sortants, les bases de données SPD et SADB déterminent le niveau de protection à appliquer. Pour les paquets entrants, la base de données SPD permet de déterminer l'acceptabilité du niveau de protection. Si le paquet est protégé par IPsec, une consultation de la base de données SPD est effectuée après déchiffrement et vérification du paquet.

IPsec applique les mécanismes de sécurité aux datagrammes IP circulant en direction de l'adresse IP de destination. A l'aide des informations contenues dans la base de données SADB, le destinataire vérifie que les paquets entrants sont légitimes et les déchiffre. Les applications peuvent appeler IPsec pour appliquer les mécanismes aux datagrammes IP au niveau de chaque socket.

Lorsque la stratégie IPsec est appliquée à un port sur lequel un socket est déjà connecté, le trafic qui utilise ce socket ne bénéficie pas de la protection IPsec. Bien sûr, les sockets ouverts sur un port *après* l'application de la stratégie IPsec en bénéficient aussi.

RFC IPsec

Le groupe IETF (Internet Engineering Task Force) a publié un certain nombre de documents RFC (Request for Comments, demande de commentaires) décrivant l'architecture de sécurité de la couche IP. Tous les RFC constituent la propriété intellectuelle de l'Internet Society. Pour plus d'informations sur les RFC, reportez-vous au site Web `http://www.ietf.org/`. Les références de sécurité IP les plus générales sont couvertes par les RFC suivants :

- RFC 2411, "IP Security Document Roadmap", novembre 1998
- RFC 2401, "Security Architecture for the Internet Protocol", novembre 1998
- RFC 2402, "IP Authentication Header", novembre 1998
- RFC 2406, "IP Encapsulating Security Payload (ESP)", novembre 1998
- RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)", novembre 1998
- RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP", novembre 1998
- RFC 2409, "The Internet Key Exchange (IKE)", novembre 1998
- RFC 3554, “On the Use of Stream Control Transmission Protocol (SCTP) with IPsec,” juillet 2003

Terminologie IPsec

Les documents RFC IPsec définissent un certain nombre de termes qui s'avèrent utiles lors de l'implémentation d'IPsec sur des systèmes. Les tableaux suivants répertorient les termes IPsec, leur acronyme et leur définition. Le Tableau 9–1 dresse la liste des termes de négociation de clé.

TABLEAU 6–1 Termes IPsec, acronymes et usages

Terme IPsec	Acronyme	Définition
Association de sécurité	SA (Security Association)	Paramètres cryptographiques et protocole de sécurité IP appliqués à un flux spécifique de trafic réseau. Le SA est défini par un triplé : protocole de sécurité, SPI unique et IP de destination.
Base de données d'associations de sécurité	SADB (Security Associations Database)	Base de données contenant toutes les associations de sécurité actives.
Index de paramètre de sécurité	SPI (Security Parameter Index)	Valeur d'indexation d'une association de sécurité. Une SPI est une valeur 32 bits qui différencie les SA partageant une destination IP et un protocole de sécurité.

TABLEAU 6–1 Termes IPsec, acronymes et usages *(Suite)*

Terme IPsec	Acronyme	Définition
Base de données de stratégie de sécurité	SPD (Security Policy Database)	Base de données déterminant si les paquets entrants et sortants présentent le niveau de protection spécifié.
Echange de clés		Processus de génération de clés utilisant des algorithmes cryptographiques asymétriques. Les principales méthodes utilisées sont RSA et Diffie-Hellman.
Diffie-Hellman	DH	Algorithme d'échange de clés permettant la génération et l'authentification de clés. souvent appelé *échange de clés authentifiées*.
RSA	RSA	Algorithme d'échange de clés permettant la génération et la distribution de clés. Ce protocole porte le nom de ses trois créateurs : Rivest, Shamir et Adleman.
Association de sécurité Internet et protocole de gestion des clés	ISAKMP	Structure courante d'établissement du format des attributs SA, et de négociation, modification et suppression des SA. ISAKMP est le standard IETF de gestion d'échanges IKE.

Flux de paquets IPsec

La Figure 6–1 illustre le traitement d'un paquet adressé à une IP, en tant que partie intégrante d'un datagramme IP lorsque IPsec est appelé sur un paquet sortant. Le diagramme du flux indique l'endroit auquel les en-têtes d'authentification AH et les associations de sécurité ESP sont susceptibles d'être appliqués au paquet. Les méthodes d'application de ces entités et de sélection des algorithmes sont décrites dans les sections suivantes.

La Figure 6–2 illustre le processus entrant IPsec.

FIGURE 6–1 Application d'IPsec au processus de paquet sortant

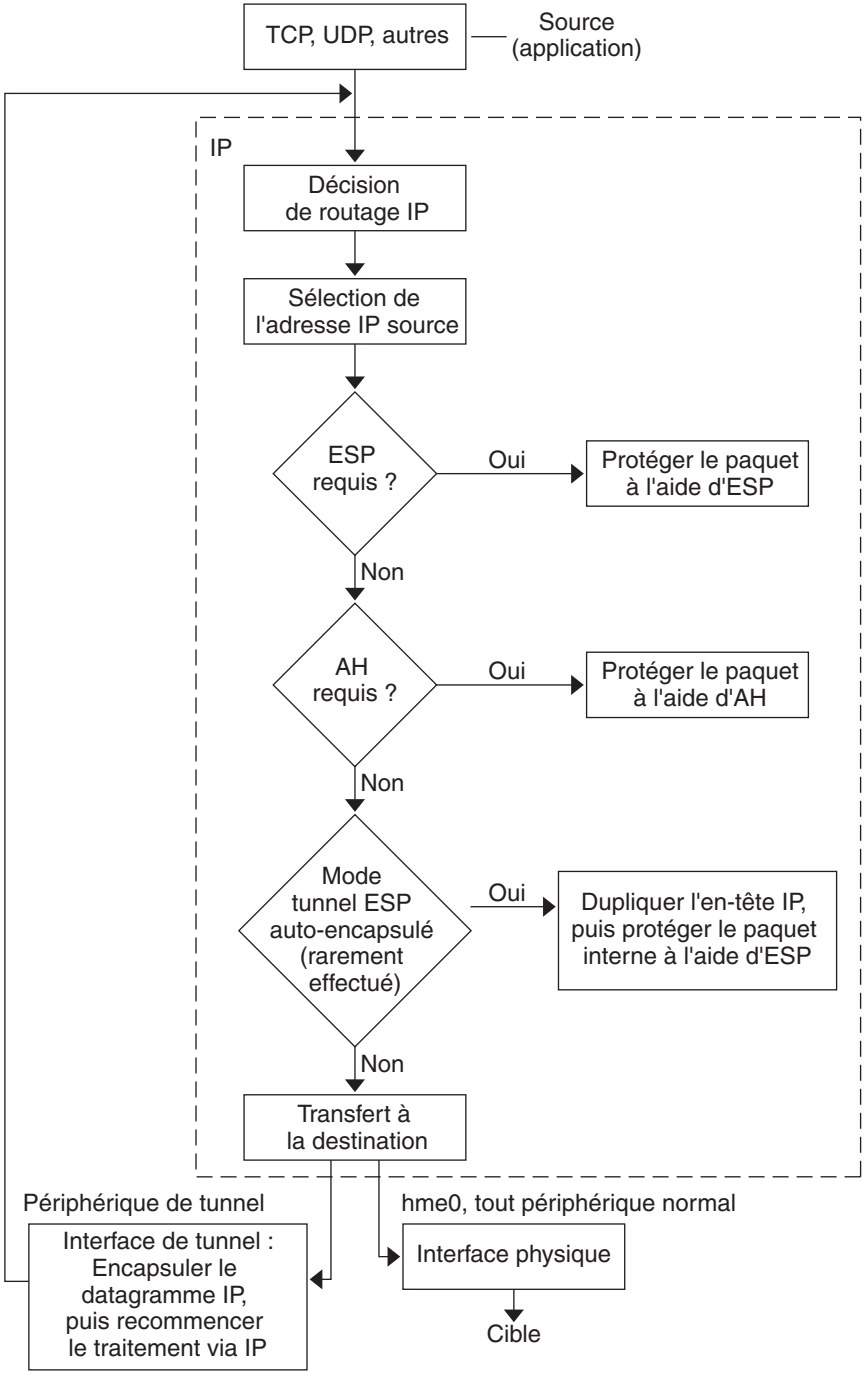
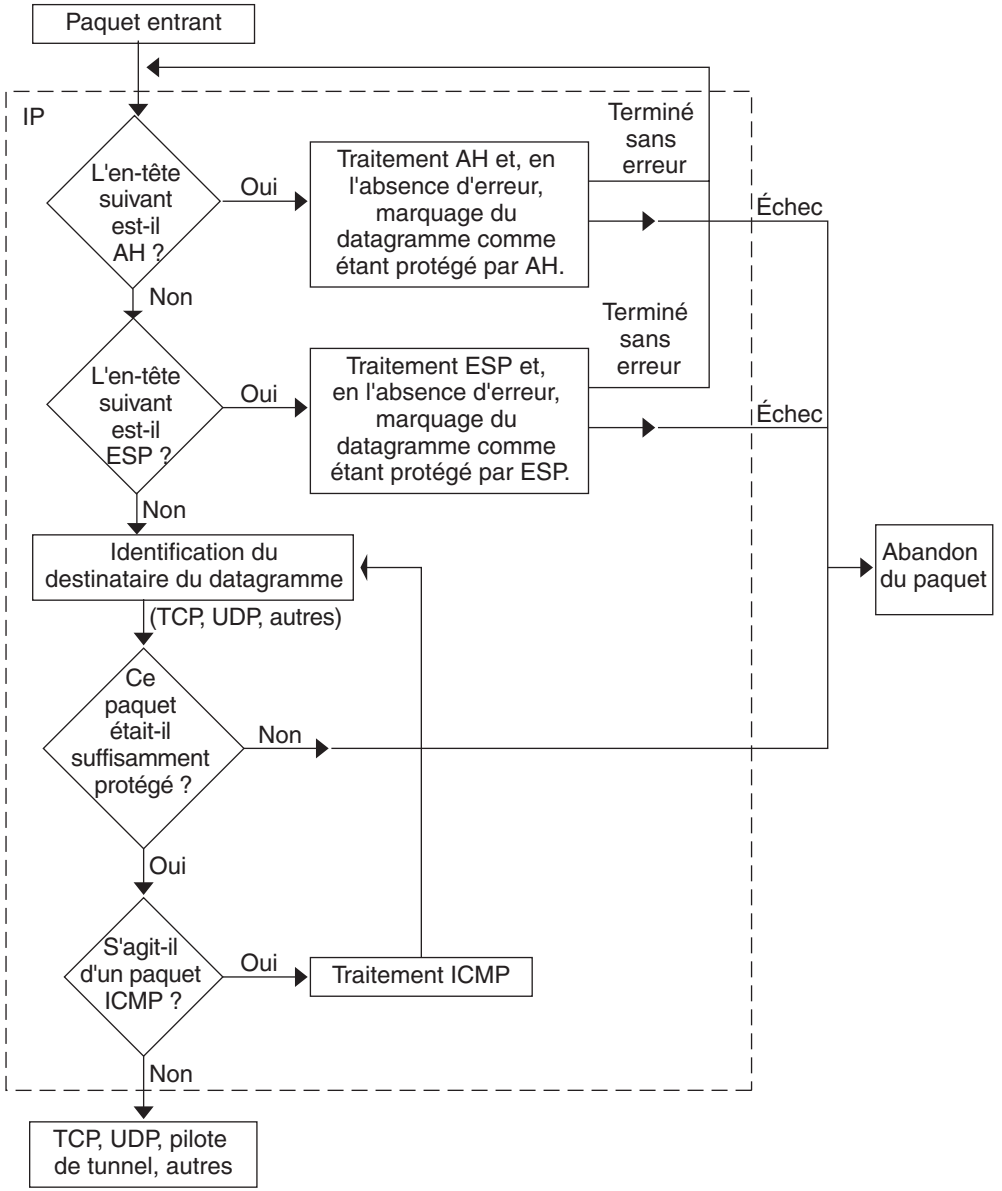


FIGURE 6–2 Application d'IPsec au processus de paquet entrant



Associations de sécurité IPsec

Une *association de sécurité* (SA, Security Association) IPsec spécifie les propriétés de sécurité que reconnaissent les hôtes lors de la communication. Une seule SA protège les données dans une direction. La protection s'applique à un seul hôte ou à une adresse de groupe (multidiffusion). La communication s'effectuant généralement entre homologues ou entre client et serveur, la sécurité du trafic dans les deux directions requiert la présence de deux SA.

Les trois éléments suivants identifient une SA IPsec de manière unique :

- Le protocole de sécurité (AH ou ESP)
- L'adresse IP de destination
- L'index du paramètre de sécurité

Le SPI, valeur arbitraire 32 bits, est transmis avec un paquet AH ou ESP. Les pages de manuel `ipsecah`(7P) et `ipsecesp`(7P) expliquent l'étendue de la protection AH et ESP. Une somme de contrôle d'intégrité permet d'authentifier un paquet. En cas d'échec de l'authentification, le paquet est rejeté.

Les associations de sécurité sont stockées dans une *base de données d'associations de sécurité* (SADB). Une interface d'administration socket, l'interface `PF_KEY`, autorise les applications privilégiées à gérer la base de données. Par exemple, l'application IKE et la commande `ipseckeys` font appel à l'interface socket `PF_KEY`.

- Pour une description détaillée de la SADB IPsec, reportez-vous à la section "Base de données des associations de sécurité IPsec" à la page 127.
- Pour plus d'informations sur la gestion de la SADB, consultez la page de manuel `pf_key`(7P).

Gestion des clés dans IPsec

Les associations de sécurité (SA) requièrent des numéros de clé pour l'authentification et le chiffrement. La gestion de ces numéros de clés s'appelle *gestion des clés*. Le protocole IKE (Internet Key Exchange, échange de clé Internet) gère les clés automatiquement. La commande `ipseckey` permet la gestion manuelle des clés.

Les SA sur les paquets IPv4 et IPv6 peuvent recourir à chacune des méthodes. Il est recommandé d'utiliser IKE à moins d'avoir une bonne raison de préférer la gestion manuelle.

La fonctionnalité d'utilitaire de gestion des services (SMF) d'Oracle Solaris fournit les services de gestion des clés suivants pour IPsec :

- Service `svc:/network/ipsec/ike:default` : service SMF de gestion automatique des clés. Le service `ike` exécute le démon `in.iked` pour la gestion automatique des clés. Le Chapitre 9, “Protocole IKE (présentation)” propose une description du protocole IKE. Pour plus d'informations sur le démon `in.iked`, reportez-vous à la page de manuel `in.iked`(1M). Pour plus d'informations sur le service `ike`, reportez-vous à la section “Service IKE” à la page 173.
- Service `svc:/network/ipsec/manual-key:default` : service SMF de gestion manuelle des clés. Le service `manual-key` exécute la commande `ipseckey` avec de nombreuses options pour gérer les clés manuellement. Pour obtenir une description de la commande `ipseckey`, reportez-vous à la section “Utilitaires de génération de clés SA dans IPsec” à la page 127. Pour obtenir une description détaillée des options de la commande `ipseckey`, reportez-vous à la page de manuel `ipseckey`(1M).

Mécanismes de protection IPsec

IPsec offre deux protocoles de sécurité dans le cadre de la protection des données :

- AH (Authentication Header, en-tête d'authentification)
- ESP (Encapsulating Security Payload, association de sécurité)

AH protège les données à l'aide d'un algorithme d'authentification. ESP protège les données à l'aide d'un algorithme de chiffrement, mais ESP peut et doit être utilisé avec un mécanisme d'authentification. Si vous ne traversez pas de NAT, vous pouvez combiner ESP à AH. Autrement, vous pouvez utiliser un algorithme d'authentification et un mécanisme de chiffrement avec ESP. Un algorithme en mode combiné tel que AES-GCM fournit le chiffrement et l'authentification dans un seul algorithme.

En-tête d'authentification

L'en-tête d'authentification offre l'authentification des données, un niveau élevé d'intégrité et la protection de rediffusion des datagrammes IP. AH protège la majeure partie du datagramme IP. Comme l'illustre la figure suivante, AH est inséré entre l'en-tête IP et l'en-tête de transport.

L'en-tête de transport peut être TCP, UDP, SCTP ou ICMP. Dans le cas de l'utilisation d'un tunnel, l'en-tête de transport peut être un autre en-tête IP.

ESP (Encapsulating Security Payload, association de sécurité)

Le module protocole ESP assure la confidentialité des encapsulations ESP. ESP propose également les services AH. Toutefois, ESP n'offre sa protection qu'à la partie des datagrammes d'encapsulation ESP. ESP fournit des services d'authentification facultatifs afin d'assurer l'intégrité du paquet protégé. Du fait qu'ESP utilise une technologie de chiffrement, un système fournissant ESP peut être soumis à des lois sur le contrôle des importations et exportations.

ESP encapsule ses données de sorte à protéger uniquement les données figurant à la suite de son commencement dans le datagramme, comme illustré ci-dessous.

Dans un paquet TCP, ESP encapsule uniquement l'en-tête TCP et ses données. Si le paquet est un datagramme IP-in-IP, ESP protège le datagramme IP interne. La stratégie par socket permet l'*auto-encapsulation*. Ainsi, ESP peut encapsuler les options IP, le cas échéant.

Lorsque l'auto-encapsulation est définie, l'en-tête IP est copié afin de créer un datagramme IP-in-IP. Par exemple, lorsque l'auto-encapsulation n'est pas définie sur un socket TCP, le datagramme est envoyé dans le format suivant :

```
[ IP(a -> b) options + TCP + data ]
```

Lorsque l'auto-encapsulation est définie sur ce socket TCP, le datagramme est envoyé dans le format suivant :

```
[ IP(a -> b) + ESP [ IP(a -> b) options + TCP + data ] ]
```

Pour plus d'informations, reportez-vous à la section "Modes Transport et Tunnel dans IPsec" à la page 94.

Considérations de sécurité lors de l'utilisation de AH et ESP

Le tableau suivant permet de comparer les protections AH et ESP.

TABLEAU 6–2 Protections assurées par AH et ESP dans IPsec

Protocole	Paquets protégés	Protection	Attaques contrées
AH	Protection des paquets de l'en-tête IP jusqu'à l'en-tête de transport	Intégrité élevée, authentification des données : ■ réception garantie des données exactes envoyées par l'expéditeur ■ attaques par rejeu possibles lorsqu'un AH n'active pas la protection par rejeu	Rejeu, couper-coller
Fournisseur de services aux entreprises	Protection des paquets figurant à la suite du début d'ESP dans le datagramme	Chiffrement de la charge utile IP à l'aide de l'option de chiffrement Confidentialité garantie	Ecoute électronique
		Protection identique à la protection AH à l'aide de l'option d'authentification	Rejeu, couper-coller
		Intégrité élevée, authentification des données et confidentialité à l'aide des deux options	Rejeu, couper-coller, écoute électronique

Authentification et chiffrement dans IPsec

Les protocoles de sécurité IPsec font appel à deux types d'algorithmes : les algorithmes d'authentification et les algorithmes de chiffrement. Le module AH recourt aux algorithmes d'authentification. Le module ESP peut utiliser aussi bien les algorithmes d'authentification que les algorithmes de chiffrement. La commande `ipsecalgs` affiche la liste des algorithmes présents sur le système, ainsi que leurs propriétés. Pour plus d'informations, reportez-vous à la page de manuel `ipsecalgs(1M)` Vous pouvez aussi utiliser les fonctions décrites dans la page de manuel `getipsecalgbyname(3NSL)`pour obtenir les propriétés des algorithmes.

IPsec utilise la structure cryptographique pour accéder aux algorithmes. Celle-ci offre un référentiel central d'algorithmes, en plus d'autres services. Elle permet à IPsec de tirer profit des accélérateurs cryptographiques hautes performances et

Pour plus d'informations, reportez-vous aux références suivantes :

- Chapitre 11, “Structure cryptographique (présentation)” du manuel *Administration d’Oracle Solaris 11.1 : Services de sécurité*
- Chapitre 8, “Introduction to the Oracle Solaris Cryptographic Framework” du manuel *Developer’s Guide to Oracle Solaris 11 Security*

Algorithmes d'authentification dans IPsec

Les algorithmes d'authentification génèrent une valeur de somme de contrôle d'intégrité, *digest*, à partir des données et d'une clé. Le module AH recourt aux algorithmes d'authentification. Le module ESP peut également y avoir recours.

Algorithmes de chiffrement dans IPsec

Les algorithmes de chiffrement chiffrent les données à l'aide d'une clé. Dans IPsec, le module ESP fait appel aux algorithmes de chiffrement. Les algorithmes agissent sur les données dans des unités d'une *taille de bloc*.

Stratégies de protection IPsec

Les stratégies de protection IPsec peuvent recourir aux mécanismes de sécurité, quels qu'ils soient. Vous pouvez appliquer les stratégies IPsec aux niveaux suivants :

- A l'échelle du système
- Par socket

IPsec applique la stratégie à l'échelle du système aux datagrammes entrants et sortants. Les datagrammes sortants sont envoyés avec ou sans protection. Si la protection est appliquée, les algorithmes sont soit spécifiques, soit non spécifiques. Vous pouvez appliquer d'autres règles aux datagrammes sortants, en raison des données supplémentaires connues du système. Les datagrammes sortants peuvent être acceptés ou rejetés. La décision d'accepter ou de rejeter un datagramme sortant est fonction de plusieurs critères qui peuvent se chevaucher et être contradictoires. Pour résoudre les conflits éventuels, il faut identifier la règle à analyser en premier. Le trafic est accepté automatiquement, sauf si une entrée de stratégie indique qu'il doit ignorer toutes les autres stratégies.

La stratégie qui protège normalement un datagramme peut être ignorée. Vous pouvez spécifier une exception dans la stratégie à l'échelle du système ou demander un contournement dans la stratégie par socket. Au niveau du trafic système, les stratégies sont mises en oeuvre, mais les mécanismes de sécurité à proprement parler ne sont pas appliqués. En revanche, la stratégie sortante sur un paquet interne au système se traduit par un paquet sortant auquel ces mécanismes ont été appliqués.

La configuration des stratégies IPsec s'effectue à l'aide du fichier `ipsecinit.conf` et de la commande `ipsecconf`. La page de manuel `ipsecconf(1M)` contient des exemples et des explications complémentaires.

Modes Transport et Tunnel dans IPsec

Les normes IPsec définissent deux modes distincts d'opération IPsec : le *mode Transport* et le *mode Tunnel*. Ces modes n'ont aucune incidence sur le codage des paquets. Les paquets sont protégés par AH, ESP ou ces deux protocoles dans chaque mode. L'application de la stratégie des modes est différente lorsque le paquet interne est un paquet IP :

- En mode Transport, l'en-tête extérieur détermine la stratégie IPsec qui protège le paquet IP interne.
- En mode Tunnel, le paquet IP interne détermine la stratégie IPsec qui protège son contenu.

En mode Transport, l'en-tête extérieur ainsi que l'en-tête suivant et tout port pris en charge par celui-ci permettent de déterminer la stratégie IPsec. En fait, IPsec peut mettre en oeuvre différentes stratégies en mode Transport entre deux adresses IP au niveau d'un seul port. Par exemple, si l'en-tête suivant est un en-tête TCP, qui prend en charge les ports, la stratégie IPsec peut alors être définie pour un port TCP de l'adresse IP externe. De même, si l'en-tête suivant est IP, l'en-tête extérieur et l'en-tête IP intérieur permettent de déterminer la stratégie IPsec.

Le mode Tunnel ne fonctionne que pour les datagrammes IP-in-IP. La mise sous tunnel en mode Tunnel peut s'avérer utile lorsque des personnes travaillant à domicile se connectent à un emplacement central. En mode Tunnel, la stratégie IPsec est mise en oeuvre sur le contenu du datagramme IP interne. Différentes stratégies IPsec peuvent être mises en oeuvre pour différentes adresses IP internes. En d'autres termes, l'en-tête IP interne, ainsi que son en-tête suivant et les ports que ce dernier prend en charge, peuvent mettre en oeuvre une stratégie. Contrairement au mode Transport, le mode Tunnel ne permet pas à l'en-tête IP extérieur de dicter la stratégie de son datagramme IP interne.

Par conséquent, en mode Tunnel, la stratégie IPsec peut être spécifiée pour les sous-réseaux d'un LAN derrière un routeur et pour les ports de ces sous-réseaux. La stratégie IPsec peut également être spécifiée pour des adresses IP données (des hôtes) sur ces sous-réseaux. Les ports de ces hôtes peuvent aussi avoir une stratégie IPsec spécifique. Toutefois, si un protocole de routage dynamique est exécuté sur un tunnel, veillez à ne pas utiliser de sélection de sous-réseau ou d'adresse, car la vue de la topologie réseau sur le réseau homologue pourrait être modifiée. Les modifications annuleraient la stratégie IPsec statique. La section "Protection d'un VPN à l'aide d'IPsec" à la page 108 contient des exemples de mises en tunnel comprenant la configuration de routes statiques.

Dans Oracle Solaris, le mode Tunnel ne peut être mis en oeuvre que sur une interface réseau de mise en tunnel IP. Pour plus d'informations sur les interfaces de création de tunnel, reportez-vous au Chapitre 6, "Configuration de tunnels IP" du manuel *Configuration et administration de réseaux Oracle Solaris 11.1*. La commande `ipsecconf` fournit un mot-clé `tunnel` pour sélectionner une interface réseau de mise en tunnel IP. Lorsque le mot-clé `tunnel` figure dans une règle, tous les sélecteurs spécifiés dans cette règle s'appliquent au paquet interne.

En mode Transport, ESP et/ou AH peuvent protéger le datagramme.

La figure suivante illustre un en-tête IP avec un paquet TCP non protégé.

FIGURE 6–3 Paquet IP non protégé transportant des informations TCP

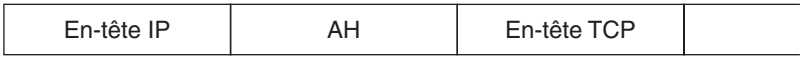
En mode Transport, ESP protège les données, comme illustré ci-dessous. La zone ombrée indique la partie chiffrée du paquet.

FIGURE 6–4 Paquet IP protégé transportant des informations TCP

Chiffré

En mode Transport, AH protège les données comme illustré ci-dessous.

FIGURE 6–5 Paquet protégé par un en-tête d'authentification



La protection AH, même en mode Transport, porte sur la majeure partie de l'en-tête IP.

En mode Tunnel, l'intégralité du datagramme figure *à l'intérieur* de la protection d'un en-tête IPsec. Le datagramme de la Figure 6–3 est protégé en mode Tunnel par un en-tête IPsec externe, ESP dans ce cas, comme indiqué sur l'illustration suivante.

FIGURE 6–6 Paquet IPsec protégé en mode Tunnel

Chiffré

La commande `ipsecconf` inclut des mots-clés permettant de définir des tunnels en mode Tunnel ou Transport.

- Pour plus d'informations sur la stratégie par socket, reportez-vous à la page de manuel `ipsec`(7P).
- La section "Utilisation d'IPsec pour protéger un serveur Web du trafic non-web." à la page 105 comprend un exemple de stratégie par socket.

- Pour plus d'informations sur les tunnels, reportez-vous à la page de manuel `ipsecconf(1M)`.
- La section "Protection d'un VPN avec IPsec en mode Tunnel" à la page 111 contient un exemple de configuration de tunnel.

Réseaux privés virtuels et IPsec

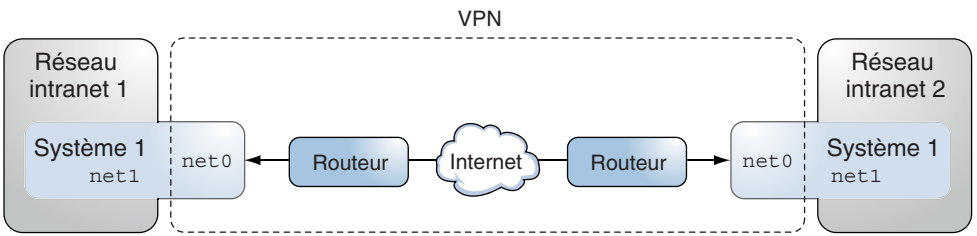
Un tunnel configuré est une interface point-à-point. Le tunnel permet l'encapsulation d'un paquet IP dans un autre paquet IP. Un tunnel correctement configuré requiert une source et une destination. Pour plus d'informations, reportez-vous à la section "Création et configuration d'un tunnel IP" du manuel *Configuration et administration de réseaux Oracle Solaris 11.1*.

Un tunnel crée une interface physique liée à IP. L'intégrité du lien physique est fonction des protocoles de sécurité sous-jacents. La configuration sécurisée des associations de sécurité (SA) rend le tunnel digne de confiance. Les paquets sortant du tunnel doivent provenir de l'homologue spécifié dans la destination de tunnel. Si la confiance est établie, vous pouvez avoir recours au transfert IP par interface pour créer un VPN.

Vous pouvez ajouter des protections IPsec à un VPN. IPsec sécurise la connexion. Par exemple, une organisation ayant recours à la technologie VPN pour connecter deux bureaux de réseaux distincts peut ajouter IPsec pour sécuriser le trafic entre ces deux bureaux.

La figure suivante illustre comment deux bureaux forment un VPN avec IPsec déployé sur leurs systèmes de réseau.

FIGURE 6–7 Réseau privé virtuel



Pour voir un exemple détaillé de la procédure de configuration, reportez-vous à la section "Protection d'un VPN avec IPsec en mode Tunnel" à la page 111.

Passage de la translation d'adresses et IPsec

IKE peut négocier des SA IPsec dans une zone NAT Cela permet aux systèmes de se connecter en toute sécurité à partir d'un réseau distant, même lorsqu'ils résident derrière un périphérique NAT. Par exemple, les employés travaillant à domicile ou se connectant depuis un site de conférence peuvent protéger leur trafic à l'aide d'IPsec.

NAT est l'acronyme de Network Address Translation (translation d'adresse réseau). Un routeur NAT permet d'associer une adresse interne privée à une adresse Internet unique. Les routeurs NAT équipent de nombreux points d'accès publics à Internet, comme ceux qu'on trouve dans les hôtels. Pour plus d'informations, reportez-vous à la section "Utilisation de la fonctionnalité NAT d'IP Filter" à la page 47.

L'utilisation d'IKE lorsqu'un routeur NAT figure entre les systèmes de communication correspond au NAT-T (NAT traversal). NAT-T présente les restrictions suivantes :

- Le protocole AH dépend d'un en-tête IP permanent, ce qui empêche son fonctionnement avec NAT-T. Le protocole ESP s'utilise avec NAT-T.
- Le routeur NAT n'applique pas de règles de traitement particulières. Un routeur NAT obéissant à des règles de traitement IPsec pourrait intervenir dans l'implémentation de NAT-T.
- NAT-T fonctionne uniquement lorsque l'initiateur IKE est le système derrière le routeur NAT. Un répondeur IKE ne peut pas se trouver derrière un routeur NAT, à moins que celui-ci ne soit programmé pour transférer des paquets IKE au système adéquat figurant derrière lui.

Les documents RFC suivants décrivent la fonctionnalité NAT et les restrictions de NAT-T. Vous pouvez obtenir des copies des RFC à l'adresse suivante : `http://www.rfc-editor.org`.

- RFC 3022, "Traditional IP Network Address Translator (Traditional NAT)", janvier 2001
- RFC 3715, "IPsec-Network Address Translation (NAT) Compatibility Requirements", mars 2004
- RFC 3947, "Negotiation of NAT-Traversal in the IKE", janvier 2005
- RFC 3948, "UDP Encapsulation of IPsec Packets", janvier 2005

Pour une utilisation conjointe d'IPsec et NAT, reportez-vous à la section "Configuration du protocole IKE pour les systèmes portables (liste des tâches)" à la page 163.

IPsec et SCTP

Oracle Solaris prend en charge le protocole SCTP (Streams Control Transmission Protocol). Bien que prise en charge, l'utilisation du protocole SCTP et du numéro de port SCTP dans le cadre de la spécification de la stratégie IPsec n'est pas stable. Les extensions IPsec pour SCTP spécifiées dans le document RFC 3554 ne sont pas encore implémentées. Ces restrictions peuvent être source de complications lors de la création de la stratégie IPsec pour SCPT.

SCTP peut avoir recours à plusieurs adresses source et cible dans le cadre d'une association SCTP unique. Lorsque la stratégie IPsec est appliquée à une seule adresse source ou cible, la communication peut échouer si SCTP change l'adresse source ou cible de cette association. La stratégie IPsec reconnaît uniquement l'adresse d'origine. Pour plus d'informations sur le protocole SCTP, consultez les documents RFC et "SCTP Protocol" du manuel *System Administration Guide: IP Services*.

IPsec et les zones Oracle Solaris

Pour les zones IP partagées, la stratégie IPsec est configurée à partir de la zone globale. Le fichier de configuration de la stratégie IPsec, `ipsecinit.conf`, existe uniquement dans la zone globale. Le fichier peut contenir des entrées s'appliquant aux zones non globales et des entrées s'appliquant à la zone globale.

Pour les zones IP exclusives, IPsec est configurée par zone non globale.

Pour plus d'informations à propos de l'utilisation d'IPsec avec des zones, reportez-vous à la section "Protection du trafic à l'aide d'IPsec" à la page 101. Pour obtenir des informations sur les zones, reportez-vous au Chapitre 15, "Introduction à Oracle Solaris Zones" du manuel *Administration d'Oracle Solaris 11.1 : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

IPsec et domaines logiques

Le protocole IPsec fonctionne avec des domaines logiques. Le domaine logique doit exécuter une version d'Oracle Solaris comprenant le protocole IPsec, comme la version Oracle Solaris 10.

Pour créer des domaines logiques, vous devez utiliser Oracle VM Server for SPARC. Cette application s'appelait auparavant Sun Logical Domains. Pour plus d'informations sur la configuration des domaines logiques, reportez-vous au *Guide d'administration d'Oracle VM Server for SPARC 2.2*.

Fichiers et utilitaires IPsec

Le Tableau 6–3 décrit les fichiers, commandes et identificateurs de service utilisés pour configurer et gérer IPsec. Exhaustif, ce tableau inclut les commandes et fichiers de gestion des clés.

Pour plus d'informations sur les identificateurs de service, reportez-vous au Chapitre 1, “Gestion des services (présentation)” du manuel *Gestion des services et pannes dans Oracle Solaris 11.1*.

- Pour obtenir des instructions sur la mise en oeuvre d'IPsec sur votre réseau, reportez-vous à la section “Protection du trafic à l'aide d'IPsec” à la page 101.
- Pour plus d'informations sur les fichiers et utilitaires IPsec, reportez-vous au Chapitre 8, “Architecture IPsec (référence)”.

TABLEAU 6–3 Liste des utilitaires et fichiers IPsec sélectionnés

Utilitaire IPsec, fichier ou service	Description	Page de manuel
`svc:/network/ipsec/ipsecalgs`	Service SMF qui gère les algorithmes IPsec.	`ipsecalgs`(1M)
`svc:/network/ipsec/manual-key`	Service SMF qui gère les SA IPsec dont les clés sont spécifiées manuellement.	`ipseckey`(1M)
`svc:/network/ipsec/policy`	Service SMF qui gère la stratégie IPsec.	`smf`(5), `ipsecconf`(1M)
`svc:/network/ipsec/ike`	Service SMF pour la gestion automatique des SA IPsec à l'aide d'IKE.	`smf`(5), `in.iked`(1M)
Fichier `/etc/inet/ipsecinit.conf`	Fichier de stratégie IPsec.	`ipsecconf`(1M)
	Le service `policy` de SMF utilise ce fichier pour configurer la stratégie IPsec à l'initialisation du système.	
Commande `ipsecconf`	Commande de stratégie IPsec. Utile pour afficher et modifier la stratégie IPsec actuelle, ainsi que pour effectuer des tests.	`ipsecconf`(1M)
	Le service `policy` de SMF s'en sert pour configurer la stratégie IPsec lors de l'initialisation du système.	
Interface socket `PF_KEY`	SADB (Interface for Security Associations Database, interface de la base de données des associations de sécurité). Responsable de la gestion manuelle et automatique des clés.	`pf_key`(7P)
Commande `ipseckey`	Commandes de génération de clés pour les SA IPsec `ipseckey` est un point d'entrée de commandes de l'interface `PF_KEY`. `ipseckey` permet de créer, supprimer ou modifier les SA.	`ipseckey`(1M)

TABLEAU 6–3 Liste des utilitaires et fichiers IPsec sélectionnés *(Suite)*

Utilitaire IPsec, fichier ou service	Description	Page de manuel
Fichier `/etc/inet/secret/ipseckeys`	Contient des SA dotés de clés attribuées manuellement. Le service `manual-key` de SMF s'en sert pour configurer les SA lors de l'initialisation du système.	
Commande `ipsecalgs`	Commande d'algorithmes IPsec. Utile pour l'affichage et la modification de la liste d'algorithmes IPsec et de leurs propriétés. Le service `ipsecalgs` de SMF s'en sert pour synchroniser les algorithmes IPsec connus avec le noyau lors de l'initialisation du système.	`ipsecalgs(1M)`
Fichier `/etc/inet/ipsecalgs`	Contient les définitions d'algorithme et les protocoles IPsec configurés. Ce fichier est géré par la commande `ipsecalgs` et ne doit jamais être modifié manuellement.	
Fichier `/etc/inet/ike/config`	Fichier de configuration et de stratégie IKE. Par défaut, ce fichier n'existe pas. La gestion des clés se base sur des règles et des paramètres généraux figurant dans le fichier `/etc/inet/ike/config`. Reportez-vous à la section "Utilitaires et fichiers IKE" à la page 135. Si ce fichier existe, le service `svc:/network/ipsec/ike` démarre le démon IKE, `in.iked`, pour la gestion automatique des clés.	`ike.config(4)`

◆ ◆ ◆ CHAPITRE 7

Configuration d'IPsec (tâches)

Ce chapitre fournit les procédures d'implémentation d'IPsec sur votre réseau. Ces procédures sont décrites dans les sections suivantes :

Vous trouverez une présentation d'IPsec au Chapitre 6, "Architecture IPsec (présentation)". Des informations de référence sur IPsec sont fournies au Chapitre 8, "Architecture IPsec (référence)".

Protection du trafic à l'aide d'IPsec

Cette section décrit les procédures permettant de sécuriser le trafic entre deux systèmes et de sécuriser un serveur Web. Pour protéger un VPN (Virtual Private Network, réseau privé virtuel), reportez-vous à la section "Protection d'un VPN à l'aide d'IPsec" à la page 108. Pour obtenir des informations sur les procédures supplémentaires de gestion d'IPsec et sur l'utilisation des commandes SMF avec IPsec et IKE, reportez-vous à la section "Gestion d'IPsec et d'IKE" à la page 115.

Les informations ci-dessous s'appliquent à toutes les tâches de configuration IPsec :

- **IPsec et zones :** pour gérer les clés et la stratégie IPsec dans le cas d'une zone non globale IP partagée, créez le fichier de stratégie IPsec dans la zone globale, puis exécutez les commandes de configuration IPsec à partir de la zone globale. Utilisez l'adresse source correspondant à la zone non globale à configurer. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.
- **IPsec et RBAC :** pour utiliser les rôles afin d'administrer IPsec, reportez-vous au Chapitre 9, "Utilisation du contrôle d'accès basé sur les rôles (tâches)" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*. La section "Configuration d'un rôle pour la sécurité réseau" à la page 117 présente un exemple.

- **IPsec et SCTP :** vous pouvez utiliser IPsec pour protéger les associations SCTP (Streams Control Transmission Protocol, protocole de transmission de contrôle de flux), mais avec prudence. Pour plus d'informations, reportez-vous à la section "IPsec et SCTP" à la page 98.
- **IPsec et étiquettes Trusted Extensions :** sur les systèmes configurés avec la fonctionnalité Trusted Extensions d'Oracle Solaris, il est possible d'ajouter des étiquettes aux paquets IPsec. Pour plus d'informations, reportez-vous à la section "Administration d'IPsec avec étiquettes" du manuel *Configuration et administration de Trusted Extensions*.
- **Adresses IPv4 et IPv6 :** les exemples IPsec dans ce guide utilisent des adresses IPv4. Oracle Solaris prend également en charge les adresses IPv6. Pour configurer IPsec pour un réseau IPv6, remplacez les adresses des exemples par des adresses IPv6. Lorsque vous protégez des tunnels avec IPsec, vous pouvez utiliser des adresses IPv4 et IPv6 en guise d'adresses internes et externes. Une telle configuration vous permet d'acheminer IPv6 via tunnel sur un réseau IPv4, par exemple.

La liste des tâches ci-dessous répertorie les procédures de configuration d'IPsec sur un ou plusieurs systèmes. Les pages de manuel `ipsecconf(1M)`, `ipseckey(1M)` et `ipadm(1M)` décrivent également des procédures utiles dans leurs sections d'exemples respectives.

Tâche	Description	Voir
Sécurisation du trafic entre deux systèmes	Protège les paquets transmis d'un système à un autre.	"Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 102
Sécurisation d'un serveur Web à l'aide de la stratégie IPsec	Requiert un trafic non-Web pour utiliser IPsec. Les clients Web sont identifiés par des ports particuliers : les vérifications IPsec sont ignorées.	"Utilisation d'IPsec pour protéger un serveur Web du trafic non-web." à la page 105
Affichage des stratégies IPsec	Affiche les stratégies IP actuellement mises en oeuvre, dans l'ordre de mise en oeuvre.	"Affichage des stratégies IPsec" à la page 107
Utilisation d'IKE pour créer automatiquement des numéros de clés pour les SA IPsec.	Fournit les données brutes des associations de sécurité.	"Configuration du protocole IKE (liste des tâches)" à la page 139
Configuration d'un réseau privé virtuel (VPN, Virtual Private Network) sécurisé	Définit IPsec entre deux systèmes sur Internet.	"Protection d'un VPN à l'aide d'IPsec" à la page 108

▼ Sécurisation du trafic entre deux systèmes à l'aide d'IPsec

Cette procédure correspond à la configuration suivante :

- Les systèmes s'appellent `enigma` et `partym`.
- Chaque système dispose d'une adresse IP. Il peut d'agir d'une adresse IPv4, IPv6 ou les deux.

- Chaque système nécessite le chiffrement ESP avec l'algorithme AES, qui requiert une clé de 128 bits, ainsi que l'authentification ESP avec la synthèse des messages SHA-2, qui requiert une clé de 512 bits.
- Chaque système utilise des associations de sécurité partagées (SA, Security Associations).

  Avec les SA partagées, une seule paire de SA est suffisante pour protéger les deux systèmes.

Remarque – Pour utiliser IPsec avec des étiquettes sur un système Trusted Extensions, reportez-vous aux étapes supplémentaires indiquées à la section "Application des protections IPsec dans un réseau Trusted Extensions multiniveau" du manuel *Configuration et administration de Trusted Extensions*.

Avant de commencer

La stratégie IPsec peut être configurée dans la zone globale ou dans une zone de pile IP en mode exclusif. La stratégie pour une zone de pile IP en mode partagé doit être configurée dans la zone globale. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

Pour exécuter les commandes de configuration, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau). Pour modifier les fichiers système et créer des clés, vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

1 Sur chaque système, ajoutez des entrées d'hôte au fichier `/etc/inet/hosts` .

Cette étape permet au SMF d'utiliser le système de noms sans dépendre de services de noms inexistants. Pour plus d'informations, reportez-vous à la page de manuel `smf(5)`.

a. Sur un système appelé `partym`, saisissez les lignes suivantes dans le fichier `hosts` :

```
# Secure communication with enigma
192.168.116.16 enigma
```

b. Sur un système appelé `enigma`, saisissez les lignes suivantes dans le fichier `hosts` :

```
# Secure communication with partym
192.168.13.213 partym
```

2 Sur chaque système, créez le fichier de stratégie IPsec.

Le nom de fichier est `/etc/inet/ipsecinit.conf`. Vous en trouverez un exemple dans le fichier `/etc/inet/ipsecinit.sample`.

3 **Ajoutez une entrée de stratégie IPsec au fichier `ipsecinit.conf`.**

a. **Sur le système `enigma`, ajoutez la stratégie ci-dessous :**

```
{laddr enigma raddr partym} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

b. **Sur le système `partym`, ajoutez la même stratégie :**

```
{laddr partym raddr enigma} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

La syntaxe des entrées de stratégie IPsec est décrite dans la page de manuel `ipsecconf(1M)`.

4 **Dans chaque système, configurez IKE afin d'ajouter une paire de SA IPsec entre les deux systèmes.**

Configurez IKE en suivant l'une des procédures de configuration décrites à la section "Configuration du protocole IKE (liste des tâches)" à la page 139. La syntaxe du fichier de configuration IKE est décrite à la page de manuel `ike.config(4)`.

Remarque – Si vous devez générer et maintenir vos clés manuellement, reportez-vous à la section "Création manuelle de clés IPsec" à la page 115.

---

5 **Vérifiez la syntaxe du fichier de stratégie IPsec.**

```
# ipsecconf -f -c /etc/inet/ipsecinit.conf
```

Corrigez les éventuelles erreurs, vérifiez la syntaxe du fichier, puis continuez.

6 **Actualisez la stratégie IPsec.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La stratégie IPsec est activée par défaut. *Actualisez*-la. Si vous avez désactivé la stratégie IPsec, activez-la.

```
# svcadm enable svc:/network/ipsec/policy:default
```

7 **Activez les clés pour IPsec.**

- **Si le service `ike` n'est pas activé, activez-le.**

```
# svcadm enable svc:/network/ipsec/ike:default
```

- **Si le service `ike` est activé, redémarrez-le.**

```
# svcadm restart svc:/network/ipsec/ike:default
```

Si vous avez configuré les clés manuellement à l'Étape 4, suivez la procédure de la section "Création manuelle de clés IPsec" à la page 115 pour activer les clés.

8 **Assurez-vous que les paquets sont protégés.**

La procédure est décrite à la section "Vérification de la protection des paquets par IPsec" à la page 120.

Exemple 7–1 Ajout d'une stratégie IPsec lors de l'utilisation d'une connexion `ssh`

Dans cet exemple, l'administrateur ayant le rôle `root` configure la stratégie et les clés IPsec sur deux systèmes en utilisant la commande `ssh` pour atteindre le second système. L'administrateur est défini à l'identique sur les deux systèmes. Pour plus d'informations, reportez-vous à la page de manuel `ssh(1)`.

- Tout d'abord, l'administrateur configure le premier système en effectuant les étapes Étape 1 à Étape 5 de la procédure précédente.
- Ensuite, dans une autre fenêtre de terminal, l'administrateur utilise le nom et l'ID utilisateur définis de façon identique pour se connecter à distance avec la commande `ssh`.

```
local-system $ ssh -l jdoe other-system
other-system $ su - root
Enter password:
other-system #
```

- Dans la fenêtre de terminal de la session `ssh`, l'administrateur configure la stratégie IPsec et les clés du second système en effectuant les opérations décrites de l'Étape 1 à l'Étape 7.
- Ensuite, l'administrateur met fin à la session `ssh`.

```
other-system # exit
local-system $ exit
```

- Enfin, l'administrateur active la stratégie IPsec sur le premier système en suivant les procédures de l'Étape 6 et de l'Étape 7.

La prochaine fois que les deux systèmes communiquent, y compris par le biais d'une connexion `ssh`, la communication est protégée par IPsec.

▼ Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.

Un serveur Web sécurisé permet aux clients Web de communiquer avec le service Web. Sur un serveur Web sécurisé, le trafic non Web *doit* passer des tests de sécurité. La procédure suivante inclut les contournements pour le trafic Web. En outre, ce serveur Web peut effectuer des demandes client DNS non sécurisées. Tout autre trafic requiert ESP avec les algorithmes AES et SHA-2.

Avant de commencer

Vous devez configurer la stratégie IPsec dans la zone globale. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

Vous avez effectué les étapes de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 102 afin que les conditions suivantes soient remplies :

- La communication entre les deux systèmes est protégée par IPsec.
- Les numéros de clés sont générés par IKE.

- Vous avez vérifié que les paquets sont protégés.

Pour exécuter les commandes de configuration, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau). Pour modifier les fichiers système, vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

1 Déterminez les services qui doivent ignorer les vérifications de stratégie de sécurité.

Pour un serveur Web, ces services incluent les ports TCP 80 (HTTP) et 443 (HTTP sécurisé). Si le serveur Web assure la recherche de noms DNS, le serveur doit peut-être inclure également le port 53 pour TCP et UDP.

2 Ajoutez la stratégie du serveur Web au fichier de stratégie IPsec.

Ajoutez les lignes suivantes dans le fichier `/etc/inet/ipsecinit.conf` :

```
# Web traffic that web server should bypass.
{lport  80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-2.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Cette configuration permet uniquement au trafic sécurisé d'accéder au système, avec les exceptions de contournement décrites à l'Étape 1.

3 Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -f -c /etc/inet/ipsecinit.conf
```

4 Actualisez la stratégie IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

5 Actualisez les clés pour IPsec.

Redémarrez le service `ike`.

```
# svcadm restart svc:/network/ipsec/ike
```

Si vous avez configuré les clés manuellement, suivez les instructions de la section "Création manuelle de clés IPsec" à la page 115.

Votre installation est terminée. Si vous le souhaitez, vous pouvez effectuer l'Étape 6.

6 **(Facultatif) Autorisez un système distant à communiquer avec le serveur Web pour le trafic non-Web.**

Ajoutez les lignes suivantes dans un fichier `/etc/inet/ipsecinit.conf` stocké sur le système distant :

```
# Communicate with web server about nonweb stuff
#
{laddr webserver} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Vérifiez la syntaxe, puis actualisez la stratégie IPsec pour l'activer.

```
remote-system # ipsecconf -f -c /etc/inet/ipsecinit.conf
remote-system # svcadm refresh svc:/network/ipsec/policy:default
```

Un système distant peut communiquer de manière sécurisée avec le serveur Web pour le trafic non-Web uniquement lorsque les stratégies IPsec des systèmes sont identiques.

▼ Affichage des stratégies IPsec

Vous pouvez afficher les stratégies configurées dans le système lorsque vous exécutez la commande `ipsecconf` sans argument.

Avant de commencer

Vous devez exécuter la commande `ipsecconf` dans la zone globale. Dans une zone IP exclusive, vous devez exécuter la commande `ipsecconf` dans la zone non globale.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

- **Affichage des stratégies IPsec**

  - **Affichez les entrées de stratégie IPsec globales dans l'ordre dans lequel les entrées ont été insérées.**

    ```
    $ ipsecconf
    ```

    La commande affiche chaque entrée avec un *index* suivi d'un numéro.

  - **Affichez les entrées de stratégie IPsec dans l'ordre dans lequel les correspondances sont repérées.**

    ```
    $ ipsecconf -l -n
    ```

  - **Affichez les entrées de stratégie IPsec, y compris les entrées définies par tunnel, dans l'ordre dans lequel les correspondances sont repérées.**

    ```
    $ ipsecconf -L -n
    ```

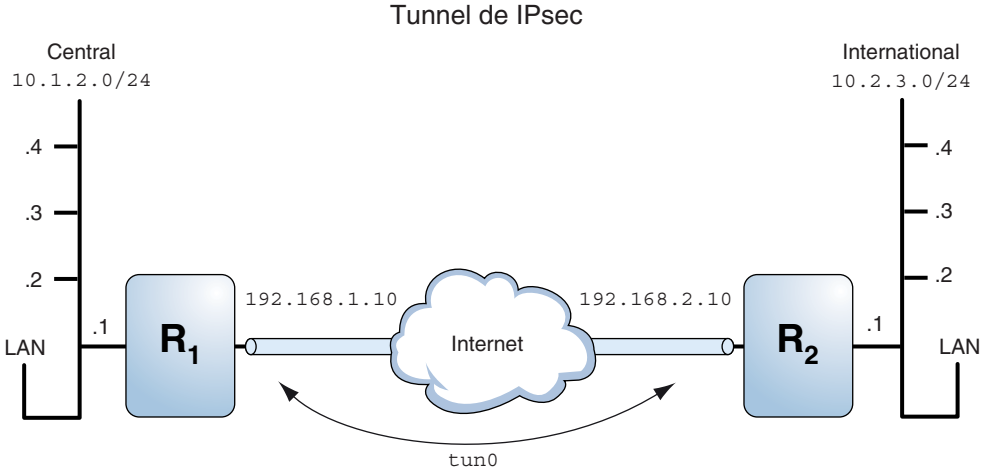
Protection d'un VPN à l'aide d'IPsec

Oracle Solaris peut configurer un réseau privé virtuel (VPN) protégé par IPsec. Vous pouvez créer des tunnels en *mode Tunnel* ou en *mode Transport*. Pour plus d'informations, reportez-vous à la section “Modes Transport et Tunnel dans IPsec” à la page 94. Les exemples et procédures de cette section utilisent des adresses IPv4, mais les exemples et procédures s'appliquent également aux réseaux privés virtuels IPv6. Pour une courte explication, reportez-vous à la section “Protection du trafic à l'aide d'IPsec” à la page 101.

Des exemples de stratégies IPsec pour les tunnels en mode Tunnel sont présentés à la section “Protection d'un VPN à l'aide d'IPsec en mode Tunnel (exemples)” à la page 108.

Protection d'un VPN à l'aide d'IPsec en mode Tunnel (exemples)

FIGURE 7–1 Tunnel protégé par IPsec



Les exemples ci-dessous considèrent que le tunnel est configuré pour tous les sous-réseaux des LAN :

```
## Tunnel configuration ##
# Tunnel name is tun0
# Intranet point for the source is 10.1.2.1
# Intranet point for the destination is 10.2.3.1
# Tunnel source is 192.168.1.10
# Tunnel destination is 192.168.2.10
```

```
# Tunnel name address object is tun0/to-central
# Tunnel name address object is tun0/to-overseas
```

EXEMPLE 7–2 Création d'un tunnel utilisable par tous les sous-réseaux

Dans cet exemple, l'ensemble du trafic des LAN locaux du LAN Central de la Figure 7–1 peut être mis en tunnel du routeur 1 au routeur 2, puis distribué à tous les LAN locaux du LAN Overseas. Le trafic est chiffré à l'aide d'AES.

```
## IPsec policy ##
{tunnel tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

EXEMPLE 7–3 Création d'un tunnel connectant deux sous-réseaux

Dans cet exemple, seul le trafic entre le sous-réseau `10.1.2.0/24` du LAN Central et le sous-réseau `10.2.3.0/24` du LAN Overseas est mis en tunnel et chiffré. En l'absence d'autres stratégies IPsec pour Central, si le LAN Central tente de transmettre des données pour d'autres LAN via ce tunnel, le trafic est abandonné au niveau du routeur 1.

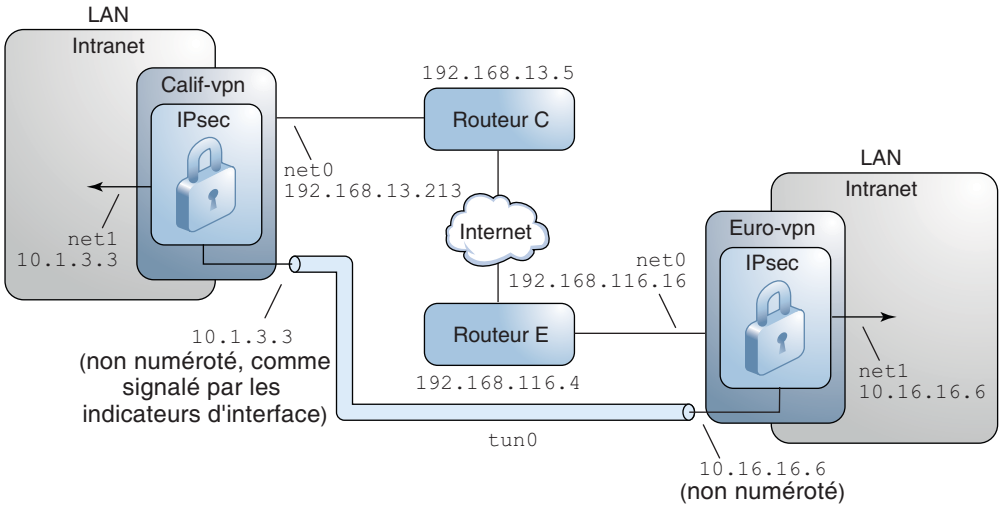
```
## IPsec policy ##
{tunnel tun0 negotiate tunnel laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs aes encr_auth_algs sha512 shared}
```

Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN

Les procédures suivant cette section sont définies pour la configuration ci-dessous. Le réseau est illustré à la Figure 7–2.

- Chaque système utilise un espace d'adressage IPv4.
- Chaque système possède deux interfaces. L'interface `net0` se connecte à Internet. Dans cet exemple, les adresses IP Internet commencent par `192.168`. L'interface `net1` se connecte au LAN de la société, son intranet. Dans cet exemple, les adresses IP intranet commencent par le numéro `10`.
- Chaque système nécessite l'authentification ESP avec l'algorithme SHA-2. Dans cet exemple, l'algorithme SHA-2 requiert une clé de 512 bits.
- Chaque système nécessite le chiffrement ESP avec l'algorithme AES. L'algorithme AES utilise une clé de 128 ou 256 bits.
- Chaque système peut se connecter à un routeur bénéficiant d'un accès direct à Internet.
- Chaque système utilise des associations de sécurité partagées (SA, Security Associations).

FIGURE 7–2 Exemple de VPN entre plusieurs sites connectés à Internet



Dans l'illustration précédente, les procédures utilisent les paramètres de configuration suivants.

Paramètre	Europe	Californie
Nom du système	`euro-vpn`	`calif-vpn`
Interface intranet du système	`net1`	`net1`
Adresse intranet du réseau, dite également adresse *-point* à l'Étape 6	`10.16.16.6`	`10.1.3.3`
Objet d'adresse intranet du système	`net1/inside`	`net1/inside`
Interface Internet du système	`net0`	`net0`
Adresse Internet du système, dite également adresse *tsrc* à l'Étape 6	`192.168.116.16`	`192.168.13.213`
Nom du routeur Internet	`router-E`	`router-C`
Adresse du routeur Internet	`192.168.116.4`	`192.168.13.5`
Nom du tunnel	`tun0`	`tun0`
Objet d'adresse de nom de tunnel	`tun0/v4tunaddr`	`tun0/v4tunaddr`

Pour plus d'informations sur les noms de tunnels, reportez-vous à la section "Configuration et administration du tunnel avec la commande dladm" du manuel *Configuration et administration de réseaux Oracle Solaris 11.1*. Pour plus d'informations sur les objets d'adresse,

reportez-vous à la section "Configuration d'une interface IP" du manuel *Connexion de systèmes à l'aide d'une configuration réseau fixe dans Oracle Solaris 11.1* et à la page de manuel `ipadm`(1M).

▼ Protection d'un VPN avec IPsec en mode Tunnel

En mode Tunnel, le paquet IP interne détermine la stratégie IPsec qui protège son contenu.

Cette procédure prolonge la procédure "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 102. La configuration est décrite à la section "Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN" à la page 109.

Pour une description plus détaillée des raisons pour lesquelles certaines commandes doivent être exécutées, reportez-vous aux étapes correspondantes à la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 102.

Remarque – Effectuez cette procédure sur les deux systèmes.

Outre la connexion de deux systèmes, vous connectez deux intranets qui leur sont connectés. Les systèmes de cette procédure fonctionnent comme des passerelles.

Remarque – Pour utiliser IPsec en mode Tunnel avec des étiquettes sur un système Trusted Extensions, reportez-vous aux étapes supplémentaires indiquées à la section "Configuration d'un tunnel au sein d'un réseau non autorisé" du manuel *Configuration et administration de Trusted Extensions*.

Avant de commencer

Vous devez vous trouver dans la zone globale pour configurer la stratégie IPsec pour le système ou pour une zone IP partagée. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

Pour exécuter des commandes de configuration, vous devez vous connecter en tant qu'administrateur disposant des profils de droits Network Management (gestion du réseau) et Network IPsec Management (gestion IPsec du réseau). Pour modifier des fichiers système, vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

1 Contrôlez le flux de paquets avant de configurer IPsec.

a. Désactivez la transmission IP et le routage d'IP dynamique.

```
# routeadm -d ipv4-routing
# ipadm set-prop -p forwarding=off ipv4
# routeadm -u
```

La désactivation de la transmission IP empêche le transfert de paquets d'un réseau vers un autre par l'intermédiaire de ce système. La commande `routeadm` est décrite à la page de manuel `routeadm`(1M).

b. Activez le multihébergement IP strict.

```
# ipadm set-prop -p hostmodel=strong ipv4
```

L'activation du multihébergement IP strict requiert que les paquets de l'une des adresses de destination du système arrivent à l'adresse de destination adéquate.

Lorsque le paramètre `hostmodel` est défini sur `strong`, les paquets arrivant sur une interface particulière doivent être adressés à l'une des adresses IP locales de cette interface. Tous les autres paquets sont abandonnés, même les paquets envoyés vers d'autres adresses locales du système.

c. Assurez-vous que la plupart des services réseau sont désactivés.

Vérifiez que les montages en loopback et le service `ssh` sont en cours d'exécution.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

2 Ajoutez la stratégie IPsec.

Modifiez le fichier `/etc/inet/ipsecinit.conf` afin d'ajouter la stratégie IPsec pour le VPN. Pour obtenir des exemples supplémentaires, reportez-vous à la section "Protection d'un VPN à l'aide d'IPsec en mode Tunnel (exemples)" à la page 108.

Dans cette stratégie, la protection IPsec n'est pas requise entre les systèmes du réseau local et l'adresse IP interne de la passerelle, d'où l'ajout d'une déclaration `bypass`.

a. Dans le système `euro-vpn`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-2.
{tunnel tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

b. Sur le système `calif-vpn`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}
```

```
# WAN traffic uses ESP with AES and SHA-2.
{tunnel tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

3 Sur chaque système, configurez IKE afin d'ajouter une paire de SA IPsec entre les deux systèmes.

Configurez IKE en suivant l'une des procédures de configuration décrites à la section "Configuration du protocole IKE (liste des tâches)" à la page 139. La syntaxe du fichier de configuration IKE est décrite à la page de manuel `ike.config(4)`.

Remarque – Si vous devez générer et maintenir vos clés manuellement, reportez-vous à la section "Création manuelle de clés IPsec" à la page 115.

---

4 Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -f -c /etc/inet/ipsecinit.conf
```

Corrigez les éventuelles erreurs, vérifiez la syntaxe du fichier, puis continuez.

5 Actualisez la stratégie IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La stratégie IPsec est activée par défaut. *Actualisez*-la. Si vous avez désactivé la stratégie IPsec, activez-la.

```
# svcadm enable svc:/network/ipsec/policy:default
```

6 Créez et configurez le tunnel, *nom-tunnel***.**

Les commandes suivantes configurent les interfaces internes et externes, créent le tunnel `tun0` et attribuent des adresses IP au tunnel.

a. Sur le système `calif-vpn`, créez le tunnel et configurez-le.

Si l'interface `net1` n'existe pas, la première commande la crée.

```
# ipadm create-addr -T static -a local=10.1.3.3 net1/inside
# dladm create-iptun -T ipv4 -a local=10.1.3.3,remote=10.16.16.6 tun0
# ipadm create-addr -T static \
-a local=192.168.13.213,remote=192.168.116.16 tun0/v4tunaddr
```

b. Sur le système `euro-vpn`, créez le tunnel et configurez-le.

```
# ipadm create-addr -T static -a local=10.16.16.6 net1/inside
# dladm create-iptun -T ipv4 -a local=10.16.16.6,remote=10.1.3.3 tun0
# ipadm create-addr -T static \
-a local=192.168.116.16,remote=192.168.13.213 tun0/v4tunaddr
```

Remarque – L'option `-T` de la commande `ipadm` spécifie le type d'adresse à créer. L'option `-T` de la commande `dladm` spécifie le tunnel.

Pour plus d'informations sur ces commandes, reportez-vous aux pages de manuel `dladm`(1M) et `ipadm`(1M), ainsi qu'à la section "Configuration d'une interface IP" du manuel *Connexion de systèmes à l'aide d'une configuration réseau fixe dans Oracle Solaris 11.1*. Pour obtenir des informations sur les noms personnalisés, reportez-vous à la section "Noms des périphériques réseau et des liaisons de données" du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

7 Sur chaque système, configurez le transfert.

```
# ipadm set-ifprop -m ipv4 -p forwarding=on net1
# ipadm set-ifprop -m ipv4 -p forwarding=off net0
```

Le transfert IP signifie que les paquets arrivant peuvent être transférés. Le transfert IP signifie également que les paquets quittant l'interface peuvent provenir d'un autre emplacement. Pour que le transfert de paquet s'effectue sans erreur, vous devez activer le transfert IP à la fois sur l'interface réceptrice et sur l'interface émettrice.

Etant donné que l'interface `net1` se trouve *dans* l'intranet, le transfert IP doit être activé pour `net1`. Comme `tun0` connecte les deux systèmes via Internet, la transmission IP doit être activée pour `tun0`. Le transfert IP de l'interface `net0` est désactivé afin d'éviter toute injection de paquets par un concurrent *externe* dans l'intranet protégé. Le terme *externe* fait référence à Internet.

8 Sur chaque système, empêchez la publication de l'interface privée.

```
# ipadm set-addrprop -p private=on net0
```

Même si le transfert de l'IP de `net0` est désactivé, l'implémentation d'un protocole de routage peut permettre d'annoncer l'interface. Par exemple, le protocole `in.routed` peut encore annoncer que `net0` est disponible pour transférer des paquets à ses homologues dans l'intranet. Pour éviter ces annonces, définissez l'indicateur *private* de l'interface.

9 Redémarrez les services réseau.

```
# svcadm restart svc:/network/initial:default
```

10 Ajoutez manuellement une route par défaut sur l'interface `net0`.

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

a. Sur le système `calif-vpn` ajoutez la route suivante :

```
# route -p add net default 192.168.13.5
```

b. Sur le système `euro-vpn`, ajoutez la route suivante :

```
# route -p add net default  192.168.116.4
```

Même si l'interface `net0` ne fait pas partie de l'intranet, `net0` n'a pas besoin de passer par Internet pour atteindre le système homologue. Pour trouver son homologue, `net0` requiert des informations sur le routage Internet. Pour le reste d'Internet, le système VPN apparaît comme étant un hôte, non un routeur. Par conséquent, vous pouvez utiliser un routeur par défaut ou exécuter le protocole de recherche de routeur pour rechercher le système. Pour plus d'informations, reportez-vous aux pages de manuel `route`(1M) et `in.routed`(1M).

Gestion d'IPsec et d'IKE

La liste des tâches suivantes fait référence à des tâches utiles dans le cadre de la gestion d'IPsec.

Tâche	Description	Voir
Création et remplacement manuels des associations de sécurité	Fournit les données brutes des associations de sécurité : ■ Nom d'algorithme IPsec et numéros de clé ■ Index de paramètre de sécurité (SPI) ■ Source IP et adresses de destination, et autres paramètres	"Création manuelle de clés IPsec" à la page 115
Création d'un rôle de sécurité réseau	Crée un rôle pouvant configurer un réseau sécurisé, mais possédant moins de permissions que le rôle `root`.	"Configuration d'un rôle pour la sécurité réseau" à la page 117
Gestion d'IPsec et des numéros de clés en tant qu'ensemble de services SMF	Décrit quand et comment utiliser les commandes permettant d'activer, de désactiver, d'actualiser et de redémarrer les services. Décrit également les commandes permettant de modifier les valeurs de propriété des services.	"Gestion des services IKE et IPsec" à la page 119
Vérification de la protection des paquets par IPsec	Recherche des en-têtes spécifiques indiquant la méthode de protection des datagrammes IP dans la sortie de commande `snoop`.	"Vérification de la protection des paquets par IPsec" à la page 120

▼ Création manuelle de clés IPsec

La procédure suivante fournit les numéros de clés de l'Étape 4 de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 102. Vous générez des clés pour deux systèmes, `partym` et `enigma`. Vous générez des clés sur un système, puis utilisez les clés du premier système sur les deux systèmes.

Avant de commencer

La gestion manuelle des numéros de clé pour une zone non globale s'effectue dans la zone globale.

Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Générez les numéros de clé pour les SA.

a. Déterminez les clés nécessaires.

Il vous faut trois numéros aléatoires hexadécimaux pour le trafic sortant et trois autres numéros aléatoires hexadécimaux pour le trafic entrant. Un système doit donc générer les numéros suivants :

- Deux numéros aléatoires hexadécimaux comme valeur du mot-clé `spi` : un numéro pour le trafic sortant et un numéro pour le trafic entrant. Chaque numéro peut comporter huit caractères maximum.
- Deux numéros aléatoires hexadécimaux pour l'algorithme SHA-2 pour AH. Chacun des numéros doit comporter 512 caractères. L'un d'eux est dédié à `dst enigma`, l'autre à `dst partym`.
- Deux numéros aléatoires hexadécimaux pour l'algorithme 3DES pour ESP. Chacun des numéros doit comporter 168 caractères. L'un d'eux est dédié à `dst enigma`, l'autre à `dst partym`.

b. Générez les clés requises.

- Si un générateur de nombres aléatoires est disponible sur votre site, utilisez-le.
- Utilisez la commande `pktool` comme indiqué dans la section "Génération d'une clé symétrique à l'aide de la commande pktool" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité* et dans l'exemple IPsec de cette section.

2 Dans le rôle `root` sur chaque système, ajoutez les clés au fichier de clés manuelles pour IPsec.

a. Modifiez le fichier `/etc/inet/secret/ipseckeys` sur le système `enigma` pour qu'il soit similaire à ce qui suit :

```
# ipseckeys - This file takes the file format documented in
#   ipseckey(1m).
#   Note that naming services might not be available when this file
#   loads, just like ipsecinit.conf.
#
#   Backslashes indicate command continuation.
#
# for outbound packets on enigma
add esp spi 0x8bcd1407 \
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg 3des \
   auth_alg sha512  \
   encrkey  d41fb74470271826a8e7a80d343cc5aa... \
   authkey  e896f8df7f78d6cab36c94ccf293f031...
#
# for inbound packets
add esp spi 0x122a43e4 \
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg 3des \
   auth_alg sha512  \
   encrkey dd325c5c137fb4739a55c9b3a1747baa... \
   authkey ad9ced7ad5f255c9a8605fba5eb4d2fd...
```

b. Protégez le fichier à l'aide d'autorisations de lecture seule.

```
# chmod 400 /etc/inet/secret/ipseckeys
```

c. Vérifiez la syntaxe du fichier.

```
# ipseckey -c -f /etc/inet/secret/ipseckeys
```

Remarque – Les numéros de clés utilisés sur chacun des systèmes *doivent* être identiques.

---

3 Activez les clés pour IPsec.

- **Si le service `manual-key` n'est pas activé, activez-le.**

  ```
  # svcadm enable svc:/network/ipsec/manual-key:default
  ```

- **Si le service `manual-key` est activé, actualisez-le.**

  ```
  # svcadm refresh ipsec/manual-key
  ```

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

▼ Configuration d'un rôle pour la sécurité réseau

Si vous administrez vos systèmes à l'aide de la fonctionnalité RBAC (Role-Based Access Control, contrôle d'accès à base de rôles) d'Oracle Solaris, suivez cette procédure pour générer un rôle de gestion ou de sécurité du réseau.

Avant de commencer Vous devez prendre le rôle `root` pour créer et affecter un rôle. Les utilisateurs standard peuvent répertorier et afficher le contenu des profils de droits disponibles.

1 Répertoriez les profils de droits disponibles relatifs au réseau.

```
% getent prof_attr | grep Network | more
Console User:RO::Manage System as the Console User...
Network Management:RO::Manage the host and network configuration...
Network Autoconf Admin:RO::Manage Network Auto-Magic configuration via nwamd...
Network Autoconf User:RO::Network Auto-Magic User...
Network ILB:RO::Manage ILB configuration via ilbadm...
Network LLDP:RO::Manage LLDP agents via lldpadm...
Network VRRP:RO::Manage VRRP instances...
Network Observability:RO::Allow access to observability devices...
Network Security:RO::Manage network and host security...:profiles=Network Wifi
Security,Network Link Security,Network IPsec Management...
Network Wifi Management:RO::Manage wifi network configuration...
Network Wifi Security:RO::Manage wifi network security...
Network Link Security:RO::Manage network link security...
Network IPsec Management:RO::Manage IPsec and IKE...
System Administrator:RO::Can perform most non-security administrative tasks:
profiles=...Network Management...
Information Security:RO::Maintains MAC and DAC security policies:
profiles=...Network Security...
```

Le profil de gestion du réseau est un profil supplémentaire inclus dans le profil d'administrateur système. Si vous avez attribué le profil de droits d'administrateur système à un rôle, alors ce dernier permet d'exécuter les commandes définies dans le profil de gestion du réseau.

2 Répertoriez les commandes dans le profil de droits Network Management.

```
% getent exec_attr | grep "Network Management"
...
Network Management:solaris:cmd:::/sbin/dlstat:euid=dladm;egid=sys
...
Network Management:solaris:cmd:::/usr/sbin/snoop:privs=net_observability
Network Management:solaris:cmd:::/usr/sbin/spray:euid=0 ...
```

3 Choisissez l'étendue des rôles de sécurité réseau sur votre site.

Basez votre choix sur les profils de droits définis au cours de l'Étape 1.

- Pour créer un rôle qui gère l'ensemble de la sécurité du réseau, utilisez le profil de droits Network Security.
- Pour créer un rôle qui gère IPsec et IKE uniquement, utilisez le profil de droits Network IPsec Management.

4 Créez un rôle de sécurité réseau incluant le profil de droits Network Management.

Un rôle auquel est appliqué le profil de droits Network Security ou Network IPsec Management, en plus du profil Network Management, peut exécuter les commandes `ipadm`, `ipseckey` et `snoop` entre autres, avec les privilèges appropriés.

Pour créer le rôle, l'affecter à un utilisateur et enregistrer les modifications auprès du service de noms, reportez-vous à la section "Configuration initiale RBAC (liste des tâches)" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Exemple 7–4 Répartition des responsabilités de sécurité réseau entre les rôles

Dans cet exemple, l'administrateur répartit les responsabilités de sécurité réseau entre deux rôles. Un rôle peut administrer la sécurité des connexions Wi-Fi et des liens et un autre rôle administrer IPsec et IKE. Chaque rôle est assigné à trois personnes, une personne par période de travail.

Ces rôles sont créés par l'administrateur comme suit :

- L'administrateur nomme le premier rôle LinkWifi.
  - L'administrateur attribue au rôle les profils de droits Network Wifi, Network Link Security et Network Management.
  - Ensuite, l'administrateur attribue le rôle LinkWifi aux utilisateurs appropriés.
- L'administrateur nomme le deuxième rôle Administrateur IPsec.
  - L'administrateur attribue au rôle les profils de droits Network IPsec Management et Network Management.

- Ensuite, l'administrateur attribue le rôle d'administrateur IPsec aux utilisateurs appropriés.

▼ Gestion des services IKE et IPsec

Les étapes suivantes présentent les utilisations les plus probables des services SMF pour IPsec, IKE et la gestion manuelle des clés. Par défaut, les services `policy` et `ipsecalgs` sont activés. Egalement par défaut, les services `ike` et `manual-key` sont désactivés.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Pour gérer la stratégie IPsec, effectuez l'une des opérations suivantes :

- **Après l'ajout de nouvelles stratégies au fichier `.conf`, actualisez le service `policy`.**

```
# svcadm refresh svc:/network/ipsec/policy
```

- **Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service `policy`.**

```
# svccfg -s policy setprop config/config_file=/etc/inet/MyIpsecinit.conf
# svccfg -s policy listprop config/config_file
config/config_file  astring  /etc/inet/MyIpsecinit.conf
# svcadm refresh svc:/network/ipsec/policy
# svcadm restart svc:/network/ipsec/policy
```

2 Pour gérer automatiquement les clés, effectuez l'une des opérations suivantes :

- **Après l'ajout d'entrées dans le fichier `/etc/inet/ike/config`, activez le service `ike`.**

```
# svcadm enable svc:/network/ipsec/ike
```

- **Après avoir modifié les entrées dans le fichier `/etc/inet/ike/config`, actualisez le service `ike`.**

```
# svcadm restart svc:/network/ipsec/ike:default
```

- **Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service.**

```
# svccfg -s ike setprop config/admin_privilege = astring: "modkeys"
# svccfg -s ike listprop config/admin_privilege
config/admin_privilege  astring  modkeys
# svcadm refresh svc:/network/ipsec/ike
# svcadm restart svc:/network/ipsec/ike
```

- **Pour arrêter le service `ike`, désactivez-le.**

```
# svcadm disable svc:/network/ipsec/ike
```

3. **Pour gérer manuellement les clés, effectuez l'une des opérations suivantes :**

   - **Après l'ajout d'entrées pour le fichier `/etc/inet/secret/ipseckeys`, activez le service `manual-key`.**

     ```
     # svcadm enable svc:/network/ipsec/manual-key:default
     ```

   - **Une fois que vous avez modifié le fichier `ipseckeys`, actualisez le service.**

     ```
     # svcadm refresh manual-key
     ```

   - **Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service.**

     ```
     # svccfg -s manual-key setprop config/config_file=/etc/inet/secret/MyIpseckeyfile
     # svccfg -s manual-key listprop config/config_file
     config/config_file  astring  /etc/inet/secret/MyIpseckeyfile
     # svcadm refresh svc:/network/ipsec/manual-key
     # svcadm restart svc:/network/ipsec/manual-key
     ```

   - **Pour empêcher la gestion manuelle des clés, désactivez le service `manual-key`.**

     ```
     # svcadm disable svc:/network/ipsec/manual-key
     ```

4. **Si vous modifiez le tableau des protocoles IPsec et des algorithmes, actualisez le service `ipsecalgs`.**

   ```
   # svcadm refresh svc:/network/ipsec/ipsecalgs
   ```

Erreurs fréquentes Pour connaître l'état d'un service, utilisez la commande de *service* `svcs`. Si le service est en mode `maintenance`, suivez les suggestions de débogage dans la sortie de la commande de *service* `svcs -x`.

▼ Vérification de la protection des paquets par IPsec

Pour vérifier que les paquets sont protégés, testez la connexion à l'aide de la commande `snoop`. Les préfixes suivants peuvent apparaître dans la sortie `snoop` :

- Le préfixe `AH:` indique que AH protège les en-têtes. `AH:` s'affiche si le trafic est protégé à l'aide d'`auth_alg`.
- Le préfixe `ESP:` indique le transfert de données chiffrées. `ESP:` s'affiche si le trafic est protégé à l'aide d'`encr_auth_alg` ou d'`encr_alg`.

Avant de commencer Vous devez avoir accès aux deux systèmes afin de tester la connexion.

Vous devez prendre le rôle `root` pour créer la sortie `snoop`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Sur un système, par exemple `partym`, prenez le rôle `root`.

```
% su -
Password:       Type root password
#
```

2 A partir du système `partym`, préparez l'analyse des paquets à l'aide de la commande snoop à partir d'un système distant.

Dans une fenêtre de terminal sur `partym`, analysez les paquets du système `enigma`.

```
# snoop -d net0 -v enigma
Using device /dev/bge (promiscuous mode)
```

3 Envoyez un paquet à partir du système distant.

Dans une autre fenêtre de terminal, connectez-vous à distance au système `enigma`. Entrez votre mot de passe. Ensuite, prenez le rôle `root` et envoyez un paquet à partir du système `enigma` au système `partym`. Le paquet doit être capturé à l'aide de la commande `snoop -v enigma`.

```
% ssh enigma
Password:       Type your password
% su -
Password:       Type root password
# ping partym
```

4 Examinez la sortie de la commande `snoop`.

Sur le système `partym`, la sortie devrait contenir les informations `AH` et `ESP` après les informations d'en-tête `IP` initiales. Les informations `AH` et `ESP` semblables à l'exemple ci-dessous indiquent que les paquets sont protégés :

```
IP:   Time to live = 64 seconds/hops
IP:   Protocol = 51 (AH)
IP:   Header checksum = 4e0e
IP:   Source address = 192.168.116.16, enigma
IP:   Destination address = 192.168.13.213, partym
IP:   No options
IP:
AH:  ----- Authentication Header -----
AH:
AH:  Next header = 50 (ESP)
AH:  AH length = 4 (24 bytes)
AH:  <Reserved field = 0x0>
AH:  SPI = 0xb3a8d714
AH:  Replay = 52
AH:  ICV = c653901433ef5a7d77c76eaa
AH:
ESP:  ----- Encapsulating Security Payload -----
ESP:
ESP:  SPI = 0xd4f40a61
ESP:  Replay = 52
ESP:     ....ENCRYPTED DATA....

ETHER:  ----- Ether Header -----
...
```

◆ ◆ ◆ CHAPITRE 8

Architecture IPsec (référence)

Ce chapitre contient les informations de référence suivantes :

Pour obtenir les instructions relatives à l'implémentation d'IPsec sur votre réseau, reportez-vous au Chapitre 7, "Configuration d'IPsec (tâches)". Pour une présentation d'IPsec, reportez-vous au Chapitre 6, "Architecture IPsec (présentation)".

Services IPsec

L'utilitaire de gestion des services (SMF) fournit les services suivants pour IPsec :

- Service `svc:/network/ipsec/policy` : gère la stratégie IPsec. Par défaut, ce service est activé. La valeur de la propriété `config_file` détermine l'emplacement du fichier `ipsecinit.conf`. La valeur initiale est `/etc/inet/ipsecinit.conf`.
- Service `svc:/network/ipsec/ipsecalgs` : gère les algorithmes disponibles pour IPsec. Par défaut, ce service est activé.
- Service `svc:/network/ipsec/manual-key` : active la gestion manuelle des clés. Par défaut, ce service est désactivé. La valeur de la propriété `config_file` détermine l'emplacement du fichier de configuration `ipseckeys`. La valeur initiale est `/etc/inet/secret/ipseckeys`.
- Service `svc:/network/ipsec/ike` : gère IKE. Par défaut, ce service est désactivé. Pour les propriétés configurables, reportez-vous à la section "Service IKE" à la page 173.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au Chapitre 1, “Gestion des services (présentation)” du manuel *Gestion des services et pannes dans Oracle Solaris 11.1*. Voir aussi les pages de manuel `smf`(5), `svcadm`(1M) et `svccfg`(1M).

Commande `ipsecconf`

Utilisez la commande `ipsecconf` pour configurer la stratégie IPsec pour un hôte. A l'exécution de la commande de configuration de la stratégie, le système crée des entrées de stratégie IPsec dans le noyau. Elles lui permettent de vérifier la stratégie appliquée à tous les datagrammes IP entrants et sortants. Les datagrammes transférés ne sont pas soumis aux vérifications de stratégie ajoutées à l'aide de cette commande. La commande `ipsecconf` configure également la base de données de stratégie de sécurité (SPD, Security Policy Database). Pour consulter les options de stratégie IPsec, reportez-vous à la page de manuel `ipsecconf`(1M).

Vous devez prendre le rôle `root` pour exécuter la commande `ipsecconf`. La commande accepte les entrées qui protègent le trafic bidirectionnel. Elle accepte également celles qui protègent le trafic unidirectionnel.

Les entrées de stratégie au format d'adresse locale et d'adresse distante peuvent protéger le trafic dans les deux directions à l'aide d'une entrée de stratégie unique. Par exemple, les entrées de modèles `laddr host1` et `raddr host2` protègent le trafic dans les deux directions quand aucune direction n'est spécifiée pour l'hôte nommé. Par conséquent, une seule entrée de stratégie est nécessaire pour chaque hôte.

Les entrées de stratégie ajoutées par le biais de la commande `ipsecconf` ne sont pas conservées après la réinitialisation du système. Pour vous assurer que la stratégie IPsec est active lorsque le système démarre, ajoutez l'entrée de stratégie au fichier `/etc/inet/ipsecinit.conf` , puis actualisez ou activez le service `policy`. Pour obtenir des exemples, reportez-vous à la section “Protection du trafic à l'aide d'IPsec” à la page 101.

Fichier `ipsecinit.conf`

Pour activer la stratégie de sécurité IPsec lorsque vous démarrez Oracle Solaris, vous créez un fichier de configuration pour initialiser IPsec avec vos entrées de stratégie IPsec spécifiques. Le nom par défaut de ce fichier est `/etc/inet/ipsecinit.conf`. Reportez-vous à la page de manuel `ipsecconf`(1M) pour plus d'informations sur les entrées d'une stratégie et leur format. Une fois la stratégie configurée, vous pouvez l'actualiser avec la commande `svcadm refresh ipsec/policy`.

Fichier exemple ipsecinit.conf

Le logiciel Oracle Solaris inclut un exemple de fichier de stratégie IPsec, ipsecinit.sample. Vous pouvez l'utiliser comme modèle pour créer votre propre fichier ipsecinit.conf. Le fichier ipsecinit.sample contient les exemples suivants :

```
...
# In the following simple example, outbound network traffic between the local
# host and a remote host will be encrypted. Inbound network traffic between
# these addresses is required to be encrypted as well.
#
# This example assumes that 10.0.0.1 is the IPv4 address of this host (laddr)
# and 10.0.0.2 is the IPv4 address of the remote host (raddr).
#

{laddr 10.0.0.1 raddr 10.0.0.2} ipsec
    {encr_algs aes encr_auth_algs sha256 sa shared}

# The policy syntax supports IPv4 and IPv6 addresses as well as symbolic names.
# Refer to the ipsecconf(1M) man page for warnings on using symbolic names and
# many more examples, configuration options and supported algorithms.
#
# This example assumes that 10.0.0.1 is the IPv4 address of this host (laddr)
# and 10.0.0.2 is the IPv4 address of the remote host (raddr).
#
# The remote host will also need an IPsec (and IKE) configuration that mirrors
# this one.
#
# The following line will allow ssh(1) traffic to pass without IPsec protection:

{lport 22 dir both} bypass {}

#
# {laddr 10.0.0.1 dir in} drop {}
#
# Uncommenting the above line will drop all network traffic to this host unless
# it matches the rules above. Leaving this rule commented out will allow
# network packets that does not match the above rules to pass up the IP
# network stack. ,,,
```

Considérations de sécurité pour les commandes ipsecinit.conf et ipsecconf

La stratégie IPsec ne peut être modifiée pour les connexions établies. Un socket dont la stratégie ne peut pas être modifiée est appelé un *socket verrouillé*. Les nouvelles entrées de stratégie ne protègent pas les sockets qui sont déjà verrouillés. Pour plus d'informations, reportez-vous aux pages de manuel connect(3SOCKET) et accept(3SOCKET). En cas de doute, redémarrez la connexion.

Protégez votre système d'attribution de nom. Lorsque les deux conditions suivantes sont vérifiées, vos noms d'hôtes ne sont plus fiables.

- Votre adresse source est un hôte que vous pouvez rechercher sur le réseau.
- Votre système d'attribution de nom est compromis.

Les défaillances de sécurité proviennent souvent d'une mauvaise utilisation des outils, non des outils eux-mêmes. Utilisez la commande `ipsecconf` avec prudence. La commande `ssh`, une console ou autre TTY connecté offrent les modes d'opération les plus sûrs.

Commande `ipsecalgs`

La structure cryptographique fournit des algorithmes d'authentification et de chiffrement pour IPsec. La commande `ipsecalgs` permet d'établir la liste des algorithmes pris en charge par chacun des protocoles IPsec. La configuration `ipsecalgs` est stockée dans le fichier `/etc/inet/ipsecalgs`. En général, ce fichier n'a pas besoin d'être modifié. Cependant, si le fichier doit être modifié, utilisez la commande `ipsecalgs`. Le fichier ne doit jamais être édité directement. Les algorithmes pris en charge sont synchronisés avec le noyau à l'initialisation du système par le service `svc:/network/ipsec/ipsecalgs:default`.

Les protocoles et algorithmes IPsec valides sont décrits par le DOI, ISAKMP, traité dans le document RFC 2407. Au sens global, un DOI (Domain of Interpretation, domaine d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.

En particulier, le DOI ISAKMP définit les conventions d'attribution de nom et de numéro aux algorithmes IPsec valides et à leurs protocoles, `PROTO_IPSEC_AH` et `PROTO_IPSEC_ESP`. Chaque algorithme est associé à exactement un protocole. Ces définitions DOI ISAKMP figurent dans le fichier `/etc/inet/ipsecalgs.` Les numéros d'algorithme et de protocole sont définis par l'IANA (Internet Assigned Numbers Authority). La commande `ipsecalgs` permet d'allonger la liste des algorithmes IPsec.

Pour plus d'informations sur les algorithmes, reportez-vous à la page de manuel `ipsecalgs(1M)` Pour plus d'informations sur la structure cryptographique, reportez-vous au Chapitre 11, “Structure cryptographique (présentation)” du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Base de données des associations de sécurité IPsec

Les informations sur les numéros de clés des services de sécurité IPsec sont conservées dans la base de données des associations de sécurité (SADB). Les associations de sécurité (SA) protègent les paquets entrants et sortants. Les SADB sont gérées par un processus utilisateur, éventuellement par plusieurs processus de coopération, qui envoient des messages sur un socket de type spécial. Ce mode de gestion des SADB s'apparente à la méthode décrite à la page de manuel `route`(7P) Seul le rôle `root` peut accéder à la base de données.

Le démon `in.iked` et la commande `ipseckey` utilisent l'interface socket `PF_KEY` dans le cadre de la gestion des SADB. Pour plus d'informations sur la gestion des demandes et des messages par les SADB, reportez-vous à la page de manuel `pf_key`(7P).

Utilitaires de génération de clés SA dans IPsec

Le protocole IKE permet la gestion automatique des clés pour les adresses IPv4 et IPv6. Pour obtenir les instructions relatives à la configuration IKE, reportez-vous au Chapitre 10, “Configuration du protocole IKE (tâches)”. L'utilitaire de génération manuelle de clés est la commande `ipseckey` et sa description est disponible dans la page de manuel `ipseckey`(1M).

Utilisez la commande `ipseckey` pour remplir manuellement la base de données des associations de sécurité (SADB). En règle générale, les SA sont générées manuellement lorsqu'IKE n'est pas disponible pour une raison quelconque. Cependant, si les valeurs SPI sont uniques, la génération manuelle des SA et IKE peuvent être utilisés en même temps.

La commande `ipseckey` peut être utilisée pour afficher tous les SA connus du système, que les clés aient été ajoutées manuellement ou par IKE. Avec l'option `-c`, la commande `ipseckey` vérifie la syntaxe du fichier de clés que vous avez fourni en tant qu'argument.

Les SA IPsec qui sont ajoutées par le biais de la commande `ipseckey` ne sont pas conservées après la réinitialisation du système. Pour activer manuellement les SA ajoutés à l'initialisation du système, ajoutez des entrées au fichier `/etc/inet/secret/ipseckeys`, puis activez le service `svc:/network/ipsec/manual-key:default`. Pour la procédure, reportez-vous à la section “Création manuelle de clés IPsec” à la page 115.

Bien qu'elle présente un nombre limité d'options générales, la commande `ipseckey` prend en charge un langage de commande enrichi. Si vous le souhaitez, une interface de programmation de génération manuelle de clés peut transmettre les demandes. Pour plus d'informations, reportez-vous à la page de manuel `pf_key`(7P).

Considérations de sécurité pour la commande `ipseckey`

La commande `ipseckey` permet à un rôle auquel a été attribué le profil de droits Network Security ou Network IPsec Management de saisir des informations de clés cryptographiques confidentielles. Un utilisateur malintentionné accédant à ces informations peut compromettre la sécurité du trafic IPsec.

Remarque – Si possible, utilisez IKE avec `ipseckey` plutôt que la génération de clés manuelle.

Prenez en considération les points suivants lorsque vous gérez des informations de génération de clés à l'aide de la commande `ipseckey` :

- Avez-vous actualisé les informations relatives à la génération de clés ? L'actualisation périodique des clés est une pratique de sécurité essentielle. Elle permet de prémunir les éventuelles défaillances de l'algorithme et des clés, et de limiter les dommages subis par une clé exposée.
- Le TTY est-il connecté à un réseau ? La commande `ipseckey` est-elle en mode interactif ?
  - En mode interactif, la sécurité des informations de génération de clés constitue celle du chemin d'accès au réseau pour le trafic du TTY. Evitez d'exécuter la commande `ipseckey` lors d'une session rlogin ou telnet en clair.
  - Même les fenêtres locales sont vulnérables aux attaques d'un programme caché qui intercepte les événements de fenêtre.
- Avez-vous utilisé l'option `-f` ? Le fichier est-il en cours d'accès sur le réseau ? Le fichier est-il accessible en lecture par tout utilisateur ?
  - Un utilisateur malintentionné est en mesure de lire un fichier monté sur le réseau lorsque ce fichier est en cours de lecture. Le fichier contenant les informations de génération de clés ne doit pas être lisible par tous.
  - Protégez votre système d'attribution de nom. Lorsque les deux conditions suivantes sont vérifiées, vos noms d'hôtes ne sont plus fiables.
    - Votre adresse source est un hôte que vous pouvez rechercher sur le réseau.
    - Votre système d'attribution de nom est compromis.

Les défaillances de sécurité proviennent souvent d'une mauvaise utilisation des outils, non des outils eux-mêmes. Utilisez la commande `ipseckey` avec prudence. La commande `ssh`, une console ou autre TTY connecté offrent les modes d'opération les plus sûrs.

IPsec et commande snoop

La commande snoop permet l'analyse des en-têtes ESP et AH. En raison du chiffrement des données ESP, la commande snoop ne détecte pas les en-têtes chiffrés et protégés par ESP. AH ne chiffre pas les données. Par conséquent, la commande snoop peut contrôler le trafic protégé par AH. L'option -V de la commande signale l'utilisation d'AH sur un paquet. Pour plus d'informations, reportez-vous à la page de manuel snoop(1M).

La section How to Verify That Packets Are Protected With IPsec contient un exemple détaillé de sortie "Vérification de la protection des paquets par IPsec" à la page 120 sur un paquet protégé.

Des analyseurs de réseau tiers sont également disponibles, notamment le logiciel open-source gratuit Wireshark (http://www.wireshark.org/about.html) qui est intégré à cette version.

◆ ◆ ◆ CHAPITRE 9

Protocole IKE (présentation)

Le protocole IKE (Internet Key Exchange, échange de clés Internet) automatise la gestion des clés pour IPsec. Oracle Solaris implémente IKEv1. Ce chapitre aborde les sujets suivants :

Pour plus d'informations sur l'implémentation du protocole IKE, reportez-vous au Chapitre 10, "Configuration du protocole IKE (tâches)". Pour obtenir des informations de référence, reportez-vous au Chapitre 11, "Protocole IKE (référence)". Pour plus d'informations sur les protocoles IPsec, reportez-vous au Chapitre 6, "Architecture IPsec (présentation)".

Gestion des clés avec IKE

La gestion des numéros de clé des associations de sécurité (Security Associations, SA) pour IPsec est appelée *gestion des clés*. La gestion automatique des clés requiert un canal de communication sécurisé pour la création, l'authentification et l'échange des clés. Oracle Solaris utilise IKE version 1 pour automatiser la gestion des clés. IKE s'intègre facilement dans les environnement à grande échelle et peut fournir un canal sécurisé pour un grand volume de trafic. Les associations de sécurité IPsec sur paquets IPv4 et IPv6 peuvent utiliser le protocole IKE.

IKE peut profiter de l'accélération matérielle disponible et stocker sur des composants matériels. Les accélérateurs matériels permettent aux opérations de clés intensives d'être gérées hors du système. Le stockage des clés sur des composants matériels fournit une couche de protection supplémentaire.

Négociation des clés IKE

Le démon IKE, `in.iked`, négocie et authentifie de manière sécurisée le matériel de génération de clés pour les SA IPsec. Il utilise des valeurs de départ aléatoires pour les clés des fonctions internes fournies par le SE. Le protocole IKE assure une confidentialité de transmission parfaite (PFS, perfect forward secrecy). En mode PFS, les clés qui protègent la transmission des données ne sont pas utilisées pour générer des clés complémentaires. De même, les valeurs de départ utilisées pour créer des clés de transmission de données ne sont pas réutilisées. Reportez-vous à la page de manuel `in.iked`(1M).

Terminologie relative aux clés IKE

Le tableau ci-dessous répertorie les termes utilisés dans la négociation des clés et les acronymes les plus couramment employés. Vous y trouverez également une définition de chacun de ces termes ainsi que leur contexte d'utilisation.

TABLEAU 9–1 Terminologie de négociation des clés, acronymes et utilisation

Terminologie de négociation des clés	Acronyme	Définition et utilisation
Echange de clés		Processus de génération de clés pour les algorithmes cryptographiques asymétriques. Les principales méthodes utilisées sont les protocoles RSA et Diffie-Hellman.
Algorithme Diffie-Hellman	DH	Algorithme d'échange de clés permettant la génération et l'authentification de clés. souvent appelé *échange de clés authentifiées*.
Protocole RSA	RSA	Algorithme d'échange de clés permettant la génération et le transport de clés. Ce protocole porte le nom de ses trois créateurs : Rivest, Shamir et Adleman.
Confidentialité de transmission parfaite	PFS	Ne s'applique qu'à l'échange de clés authentifiées. Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.
Groupe Oakley		Méthode de création sécurisée de clés pour la phase 2. Le groupe Oakley s'emploie pour négocier des PFS. Reportez-vous à la section 6 de The Internet Key Exchange (IKE) (`http://www.faqs.org/rfcs/rfc2409.html`).

Phase 1 d'IKE

La phase 1 est connue sous le nom de *Main Mode* (mode principal). Pendant la phase 1, IKE utilise des méthodes de chiffrement de clé publique pour s'authentifier auprès d'entités IKE homologues. Il en résulte une association de sécurité (SA, security association) ISAKMP

(Internet Security Association and Key Management Protocol). Une SA ISAKMP est un canal sécurisé sur lequel IKE négocie les numéros de clé des datagrammes IP. Contrairement aux SA IPsec, les SA ISAKMP sont bidirectionnelles. Il n'est donc pas nécessaire de disposer de plus d'une association de sécurité.

La façon dont IKE négocie les numéros de clé lors de la phase 1 peut être configurée. IKE lit les informations concernant la configuration dans le fichier `/etc/inet/ike/config`. Ces informations incluent :

- Des paramètres généraux tels que le nom des certificats de clés publiques
- L'activation ou non du mode de confidentialité de transmission parfaite (PFS)
- Les interfaces concernées
- Les protocoles de sécurité et leurs algorithmes
- La méthode d'authentification

Les deux méthodes d'authentification utilisent respectivement les clés prépartagées et les certificats de clés publiques. Les certificats de clés publiques peuvent être autosignés ou émis par l'autorité de certification (CA) d'un fournisseur d'infrastructures de clés publiques (PKI).

Phase 2 d'IKE

La phase 2 est connue sous le nom de *Quick Mode* (mode rapide). Lors de la phase 2, IKE crée et gère les SA IPsec entre les systèmes qui exécutent le démon IKE. IKE utilise le canal sécurisé qui a été créé lors de la phase 1 pour protéger la transmission des numéros de clé. Le démon IKE crée les clés à partir d'un générateur de nombres aléatoires à l'aide du périphérique `/dev/random`. Le démon actualise les clés à une fréquence qui peut être configurée. Les numéros de clé sont accessibles aux algorithmes spécifiés dans le fichier de configuration `ipsecinit.conf` de la stratégie IPsec.

Choix de configuration IKE

Le fichier de configuration `/etc/inet/ike/config` contient des entrées de stratégie IKE. Pour que deux démons IKE puissent s'authentifier mutuellement, les entrées doivent être valides et les numéros de clé doivent être disponibles. Les entrées des fichiers de configuration déterminent la façon dont les numéros de clé seront utilisés pour authentifier l'échange qui a lieu lors de la phase 1. Il y a deux possibilités : les clés prépartagées ou les certificats de clés publiques.

Si l'entrée est `auth_method preshared`, ce sont les clés prépartagées qui sont utilisées pour authentifier l'échange. Si `auth_method` possède une valeur autre que `preshared`, l'authentification s'effectue à l'aide de certificats de clés publiques. Ces certificats peuvent être autosignés ou installés par un fournisseur de PKI. Pour plus d'informations, reportez-vous à la page de manuel `ike.config(4)`.

IKE avec l'authentification des clés prépartagées

Les clés prépartagées servent à authentifier au moins deux systèmes homologues. La clé prépartagée est un nombre hexadécimal ou une chaîne ASCII créée par un administrateur sur un système. Cette clé est ensuite partagée de manière sécurisée entre les différents administrateurs des systèmes homologues. Si la clé prépartagée est interceptée par un utilisateur malintentionné, celui-ci peut alors se faire passer pour l'un des systèmes homologues.

La clé prépartagée sur les systèmes homologues qui utilisent cette méthode d'authentification doit être identique. Les clés sont liées à une adresse IP donnée ou à une plage d'adresses. Les clés sont placées dans le fichier `/etc/inet/secret/ike.preshared` de chaque système.

Pour plus d'informations, reportez-vous à la page de manuel `ike.preshared(4)`.

IKE avec certificats de clés publiques

Grâce aux certificats de clés publiques, les systèmes communicants n'ont plus besoin de partager de numéros de clé secrets hors bande. Les clés publiques utilisent l'algorithme Diffie-Hellman pour authentifier et négocier les clés. Les certificats de clés publiques peuvent être soit autosignés, soit certifiés par une autorité de certification (CA).

Les certificats de clés publiques autosignés sont créés par l'administrateur. La commande `ikecert certlocal -ks` permet de créer la partie privée des biclés du système. Le certificat autosigné est ensuite émis, au format X.509, par le système distant. Le certificat du système distant est entré à l'aide de la commande `ikecert certdb` pour la partie publique de la clé. Les certificats autosignés résident dans le répertoire `/etc/inet/ike/publickeys` des systèmes communicants. Lorsque vous utilisez l'option `-T`, les certificats résident sur le matériel connecté.

Les certificats autosignés sont à mi-chemin entre les clés prépartagées et les CA. Contrairement aux clés prépartagées, les certificats autosignés peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté. Pour autosigner un certificat pour un système n'ayant pas de numéro fixe, utilisez un nom alternatif de `DNS` (`www.example.org`) ou d'`email` (`root@domain.org`).

Les clés publiques peuvent être délivrées par un fournisseur de PKI ou une CA. Elles doivent être installées, avec les certificats CA qui les accompagnent, dans le répertoire `/etc/inet/ike/publickeys`. Lorsque vous utilisez l'option `-T`, les certificats résident sur le matériel connecté. Les fournisseurs émettent également des listes des certificats révoqués (CRL). Outre les clés et les certificats CA, vous devez également installer les CRL dans le répertoire `/etc/inet/ike/crls`.

Les certificats CA présentent l'avantage d'être certifiés par une organisation externe, et non par l'administrateur du site. Il s'agit en quelque sorte de certificats "certifiés". Comme les certificats autosignés, les certificats CA peuvent être utilisés sur une machine portable ou sur un système

susceptible d'être renuméroté. Contrairement aux certificats autosignés, ils s'intègrent facilement aux environnement à grande échelle afin de protéger un grand nombre de systèmes communicants.

Utilitaires et fichiers IKE

Vous trouverez, dans le tableau ci-dessous, une liste des fichiers de configuration de la stratégie IKE, les emplacements de stockage des clés IKE et les différentes commandes et divers services permettant d'implémenter IKE. Pour plus d'informations sur les services, reportez-vous au Chapitre 1, “Gestion des services (présentation)” du manuel *Gestion des services et pannes dans Oracle Solaris 11.1*.

TABLEAU 9–2 Fichiers de configuration IKE, emplacements de stockage des clés, commandes et services

Fichier, emplacement, commande ou service	Description	Page de manuel
`svc:/network/ipsec/ike`	Service SMF qui gère IKE.	`smf`(5)
`/usr/lib/inet/in.iked`	Démon IKE (Internet Key Exchange). Permet la gestion des clés automatique lorsque le service `ike` est actif.	`in.iked`(1M)
`/usr/sbin/ikeadm`	Commande d'administration IKE permettant d'afficher et de modifier temporairement la stratégie IKE. Permet à l'utilisateur d'afficher les objets administratifs IKE, tels que les algorithmes de phase 1 et les groupes Diffie-Hellman disponibles.	`ikeadm`(1M)
`/usr/sbin/ikecert`	Commande de gestion de bases de données de certificats permettant de manipuler les bases de données locales détentrices de certificats de clés publiques. Les bases de données peuvent également être stockées sur le matériel connecté.	`ikecert`(1M)
`/etc/inet/ike/config`	Fichier de configuration par défaut de la stratégie IKE. Contient les règles du site pour la concordance des demandes IKE entrantes et la préparation des demandes IKE sortantes. Si le fichier existe, le démon `in.iked` démarre lorsque le service `ike` est activé. L'emplacement de ce fichier peut être modifié à l'aide de la commande `svccfg`.	`ike.config`(4)
`ike.preshared`	Fichier de clés prépartagées du répertoire `/etc/inet/secret`. Contient des numéros de clé secrets destinés à l'authentification pendant la phase 1. Ce fichier s'utilise lorsque IKE est configuré avec des clés prépartagées.	`ike.preshared`(4)
`ike.privatekeys`	Répertoire de clés privés de `/etc/inet/secret`. Contient les clés privées de la biclé.	`ikecert`(1M)
Répertoire `publickeys`	Répertoire de `/etc/inet/ike` contenant les fichiers de certificats et clés publiques. Contient la clé publique de la biclé.	`ikecert`(1M)

TABLEAU 9–2 Fichiers de configuration IKE, emplacements de stockage des clés, commandes et services *(Suite)*

Fichier, emplacement, commande ou service	Description	Page de manuel
Répertoire `crls`	Répertoire de `/etc/inet/ike` contenant les listes de révocation des clés publiques et des fichiers de certificats.	`ikecert`(1M)
Carte Sun Crypto Accelerator 6000	Matériel accélérant les opérations de clés publiques en les déchargeant du système d'exploitation. Les clés publiques, les clés privées et les certificats de clés publiques peuvent également être stockés sur cette carte. La carte Sun Crypto Accelerator 6000 est un périphérique certifié FIPS 140-2 Niveau 3.	`ikecert`(1M)

◆ ◆ ◆ CHAPITRE 10

Configuration du protocole IKE (tâches)

Ce chapitre décrit la procédure de configuration du protocole Internet Key Exchange (IKE) sur vos systèmes. Une fois configuré, ce protocole génère automatiquement les numéros de clé IPsec sur votre réseau. Le présent chapitre contient les informations suivantes :

Pour voir une présentation du protocole IKE, reportez-vous au Chapitre 9, "Protocole IKE (présentation)". Pour obtenir des informations de référence sur le protocole IKE, reportez-vous au Chapitre 11, "Protocole IKE (référence)". Pour consulter d'autres procédures, reportez-vous aux sections Exemples des pages de manuel `ikeadm`(1M), `ikecert`(1M) et `ike.config`(4).

Affichage des informations IKE

Vous pouvez afficher les algorithmes et les groupes qui peuvent servir aux négociations IKE de la phase 1.

▼ Affichage des groupes et algorithmes disponibles pour les échanges IKE de la phase 1

Dans cette procédure, vous déterminez quels groupes Diffie-Hellman peuvent être utilisés dans les échanges IKE de la phase 1. Vous pouvez afficher les algorithmes de chiffrement et

d'authentification qui peuvent servir aux échanges IKE de la phase 1. Les valeurs numériques correspondent aux valeurs spécifiées pour ces algorithmes par l'IANA (Internet Assigned Numbers Authority).

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Affichage de la liste des groupes Diffie-Hellman qu'IKE peut utiliser dans la phase 1.

Les groupes Diffie-Hellman définis configurent les SA IKE.

```
# ikeadm dump groups
Value Strength Description
1     66       ietf-ike-grp-modp-768
2     77       ietf-ike-grp-modp-1024
5     91       ietf-ike-grp-modp-1536
14    110      ietf-ike-grp-modp-2048
15    130      ietf-ike-grp-modp-3072
16    150      ietf-ike-grp-modp-4096
17    170      ietf-ike-grp-modp-6144
18    190      ietf-ike-grp-modp-8192

Completed dump of groups
```

Vous pouvez utiliser l'une de ces valeurs comme argument du paramètre `oakley_group` dans une plate-forme IKE de la phase 1, comme dans :

```
p1_xform
  { auth_method preshared oakley_group 15 auth_alg sha encr_alg aes }
```

2 Affichage de la liste des algorithmes d'authentification qu'IKE peut utiliser dans la phase 1.

```
# ikeadm dump authalgs
Value Name
1     md5
2     sha1
4     sha256
5     sha384
6     sha512

Completed dump of authalgs
```

Vous pouvez utiliser l'un de ces noms comme argument du paramètre `auth_alg` dans une plate-forme IKE de la phase 1, comme dans :

```
p1_xform
  { auth_method preshared oakley_group 15 auth_alg sha256 encr_alg 3des }
```

3 Affichage de la liste des algorithmes de chiffrement qu'IKE peut utiliser dans la phase 1.

```
# ikeadm dump encralgs
Value Name
3     blowfish-cbc
```

```
5     3des-cbc
1     des-cbc
7     aes-cbc

Completed dump of encralgs
```

Vous pouvez utiliser l'un de ces noms comme argument du paramètre `encr_alg` dans une plate-forme IKE de la phase 1, comme dans :

```
p1_xform
  { auth_method preshared oakley_group 15 auth_alg sha256 encr_alg aes }
```

Voir aussi Pour effectuer des tâches de configuration de règles IKE nécessitant ces valeurs, reportez-vous à la section "Configuration du protocole IKE (liste des tâches)" à la page 139.

Configuration du protocole IKE (liste des tâches)

L'authentification du protocole IKE peut s'effectuer à l'aide de clés prépartagées ou de certificats autosignés ou émanant d'autorités de certifications (CA). Les méthodes d'authentification IKE sont liées par une règle aux points d'extrémité protégés. Vous pouvez donc utiliser toutes les méthodes d'authentification IKE ou une seule d'entre elles sur un système. Un pointeur menant à une bibliothèque PKCS #11 permet à IKE d'utiliser un accélérateur matériel connecté.

Une fois le protocole IKE configuré, vous devez effectuer les tâches IPsec qui utilisent cette configuration. Le tableau ci-dessous répertorie les tâches correspondant aux différentes configurations IKE.

Tâche	Description	Voir
Configuration d'IKE avec des clés prépartagées	Protégez les communications entre deux systèmes en faisant en sorte qu'ils partagent une clé secrète.	"Configuration du protocole IKE avec des clés prépartagées (liste des tâches)" à la page 140
Configuration d'IKE avec des certificats de clés publiques	Protégez les communications à l'aide de certificats de clés publiques. Ces certificats peuvent être autosignés ou attestés par un fournisseur de PKI.	"Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)" à la page 145
Franchissement d'un boîtier NAT	Configurez les protocoles IPsec et IKE pour communiquer avec un système portable	"Configuration du protocole IKE pour les systèmes portables (liste des tâches)" à la page 163
Configuration d'IKE pour qu'il utilise un keystore matériel pour générer une paire de certificats	Activez une carte Sun Crypto Accelerator 6000 pour accélérer les opérations IKE et stocker des certificats de clés publiques.	"Configuration du protocole IKE en vue de l'utilisation du matériel connecté" à la page 170

Configuration du protocole IKE avec des clés prépartagées (liste des tâches)

Le tableau ci-dessous répertorie les procédures de configuration et de maintenance du protocole IKE avec des clés prépartagées.

Tâche	Description	Voir
Configuration d'IKE avec des clés prépartagées	Créez un fichier de configuration IKE ainsi qu'une clé à partager.	"Configuration du protocole IKE avec des clés prépartagées" à la page 140
Ajout de clés prépartagées à un système IKE en cours d'exécution.	Ajoutez une nouvelle entrée de stratégie IKE et de nouveaux numéros de clé à un système appliquant actuellement la stratégie IKE.	"Configuration d'IKE pour un nouveau système homologue" à la page 143

Configuration du protocole IKE avec des clés prépartagées

Les clés prépartagées sont la méthode d'authentification la plus simple pour IKE. Elles s'utilisent notamment lors de la configuration du protocole IKE sur deux systèmes homologues gérés par le même administrateur. N'oubliez cependant pas que, contrairement aux certificats de clés publiques, les clés prépartagées sont liées à des adresses IP. Les clés prépartagées peuvent être associées à des adresses IP ou des plages d'adresses IP spécifiques, et ne peuvent pas s'utiliser avec des systèmes portables ou des systèmes susceptibles d'être renumérotés, à moins que la renumérotation soit incluse dans la plage d'adresses IP spécifiée.

▼ Configuration du protocole IKE avec des clés prépartagées

La longueur des clés des algorithmes d'implémentation du protocole IKE est variable. Elle dépend du niveau de sécurité dont vous souhaitez doter le site. En règle générale, la longueur des clés est proportionnelle au niveau de sécurité.

Dans cette procédure, vous générez des clés au format ASCII.

Les noms de systèmes choisis pour illustrer cette procédure sont : `enigma` et `partym`. Remplacez `enigma` et `partym` par les noms de vos systèmes.

Remarque – Pour utiliser IPsec avec des étiquettes sur un système Trusted Extensions, reportez-vous aux étapes supplémentaires indiquées à la section "Application des protections IPsec dans un réseau Trusted Extensions multiniveau" du manuel *Configuration et administration de Trusted Extensions*.

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau), en plus de l'autorisation `solaris.admin.edit/etc/inet/ike/config`. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

1 Sur chaque système, créez un fichier `/etc/inet/ike/config`.

Vous pouvez utiliser le fichier `/etc/inet/ike/config.sample` comme modèle.

2 Entrez les règles et paramètres globaux dans le fichier `ike/config` sur chacun des systèmes.

Les règles et paramètres globaux de ce fichier doivent garantir le fonctionnement de la stratégie IPsec du fichier `ipsecinit.conf`. Les exemples de configuration IKE suivants vont de pair avec les exemples `ipsecinit.conf` de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 102.

a. Modifiez par exemple le fichier `/etc/inet/ike/config` sur le système `enigma` :

```
### ike/config file on enigma, 192.168.116.16

## Global parameters
#
## Defaults that individual rules can override.
p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
#
## The rule to communicate with partym
#  Label must be unique
{ label "enigma-partym"
  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  p1_xform
   { auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes }
  p2_pfs 5
}
```

b. Modifiez le fichier `/etc/inet/ike/config` sur le système `partym` :

```
### ike/config file on partym, 192.168.13.213
## Global Parameters
#
```

```
p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2

## The rule to communicate with enigma
#  Label must be unique
{ label "partym-enigma"
  local_addr 192.168.13.213
  remote_addr 192.168.116.16
p1_xform
 { auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes }
p2_pfs 5
}
```

3 Sur chaque système, vérifiez la syntaxe du fichier.

```
# /usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

4 Créez un fichier `/etc/inet/secret/ike.preshare` sur chacun des systèmes.

Placez la clé prépartagée dans chacun des fichiers.

a. Sur le système `enigma` par exemple, le fichier `ike.preshared` se présente comme suit :

```
# ike.preshared on enigma, 192.168.116.16
#...
{ localidtype IP
    localid 192.168.116.16
    remoteidtype IP
    remoteid 192.168.13.213
    # The preshared key can also be represented in hex
# as in 0xf47cb0f432e14480951095f82b
# key "This is an ASCII Cqret phrAz, use str0ng p@ssword tekniques"
}
```

b. Sur le système `partym`, le fichier `ike.preshared` se présente comme suit :

```
# ike.preshared on partym, 192.168.13.213
#...
{ localidtype IP
    localid 192.168.13.213
    remoteidtype IP
    remoteid 192.168.116.16
    # The preshared key can also be represented in hex
# as in 0xf47cb0f432e14480951095f82b
    key "This is an ASCII Cqret phrAz, use str0ng p@ssword tekniques"
    }
```

5 Activez le service IKE.

```
# svcadm enable ipsec/ike
```

Exemple 10–1 Actualisation d'une clé prépartagée IKE

Lorsqu'un administrateur IKE souhaite actualiser la clé prépartagée, il modifie les fichiers sur ses systèmes homologues et redémarre le démon `in.iked`.

Il commence par ajouter l'entrée de clé partagée, valide pour n'importe quel hôte sur le sous-réseau `192.168.13.0/24`.

```
#...
{ localidtype IP
    localid 192.168.116.0/24
    remoteidtype IP
    remoteid 192.168.13.0/24
    # enigma and partym's shared passphrase for keying material
key "LOooong key Th@t m^st Be Ch*angEd \'reguLarLy)"
    }
```

Ensuite, l'administrateur redémarre le service IKE sur chaque système.

```
# svcadm enable ipsec/ike
```

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

▼ Configuration d'IKE pour un nouveau système homologue

Si vous ajoutez des entrées de stratégie IPsec à une configuration de travail entre des systèmes homologues, vous devez actualiser le service de stratégie IPsec. Il n'est pas nécessaire de reconfigurer ou de redémarrer IKE.

Si vous ajoutez un nouveau système homologue à la stratégie IPsec, vous devez modifier non seulement IPsec, mais aussi la configuration IKE.

Avant de commencer Vous avez mis à jour le fichier `ipsecinit.conf` et actualisé la stratégie IPsec pour les systèmes homologues.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau), en plus de l'autorisation `solaris.admin.edit/etc/inet/ike/config`. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'Exemple 7–1.

1. **Créez une règle pour la gestion des clés par IKE, pour le nouveau système qui utilise IPsec.**

   a. **Par exemple, sur le système `enigma`, ajoutez la règle suivante au fichier `/etc/inet/ike/config` :**

   ```
   ### ike/config file on enigma, 192.168.116.16

   ## The rule to communicate with ada

   {label "enigma-to-ada"
    local_addr 192.168.116.16
    remote_addr 192.168.15.7
    p1_xform
    {auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes}
    p2_pfs 5
       }
   ```

   b. **Sur le système `ada`, ajoutez la règle suivante :**

   ```
   ### ike/config file on ada, 192.168.15.7

   ## The rule to communicate with enigma

   {label "ada-to-enigma"
    local_addr 192.168.15.7
    remote_addr 192.168.116.16
    p1_xform
    {auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes}
    p2_pfs 5
   }
   ```

2. **Créez une clé prépartagée IKE pour les systèmes homologues.**

   a. **Sur le système `enigma`, ajoutez les informations suivantes au fichier `/etc/inet/secret/ike.preshared` :**

   ```
   # ike.preshared on enigma for the ada interface
   #
   { localidtype IP
     localid 192.168.116.16
     remoteidtype IP
     remoteid 192.168.15.7
     # enigma and ada's shared key
     key "Twas brillig and the slivey toves did *s0mEtHiNg* be CareFULL hEEEr"
   }
   ```

   b. **Sur le système `ada`, ajoutez les informations suivantes au fichier `ike.preshared` :**

   ```
   # ike.preshared on ada for the enigma interface
   #
   { localidtype IP
     localid 192.168.15.7
     remoteidtype IP
     remoteid 192.168.116.16
     # ada and enigma's shared key
     key "Twas brillig and the slivey toves did *s0mEtHiNg* be CareFULL hEEEr"
   }
   ```

3 **Sur chaque système, actualisez le service `ike`.**

```
# svcadm refresh ike
```

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)

Le tableau ci-dessous répertorie les procédures de création de certificats de clés publiques pour IKE. Ces procédures incluent l'accélération et le stockage de certificats sur le matériel connecté.

Un certificat public doit être unique, ainsi le créateur d'un certificat de clé publique génère un nom unique et arbitraire pour ce certificat. En règle générale, on crée un nom distinctif X.509. Un autre nom peut également servir à l'identification. Le format de ces noms est *tag=value*. Les valeurs sont arbitraires, mais leur format doit correspondre au type de balise. Par exemple, le format de la balise `email` est *name@domain.suffix*.

Tâche	Description	Voir
Configuration du protocole IKE avec des certificats de clés publiques autosignés	Créez et placez deux certificats sur chaque système : ■ Un certificat autosigné ■ Certificat de clé publique du système homologue	"Configuration du protocole IKE avec des certificats de clés publiques autosignés" à la page 146
Configuration du protocole IKE avec un certificat PKI émanant d'une autorité de certification	Créez une demande de certificat et placez trois certificats sur chacun des systèmes : ■ Le certificat créé par l'autorité de certification (CA) suite à votre demande ■ Le certificat de clé publique de la CA ■ la CRL de la CA.	"Configuration du protocole IKE avec des certificats signés par une CA" à la page 151
Configuration de certificats de clés publiques sur le matériel local	Procédez de l'une des manières suivantes : ■ Générez un certificat autosigné sur le matériel local et ajoutez la clé publique d'un système distant sur le matériel. ■ Générez une demande de certificat dans le matériel local et ajoutez les certificats de clés publiques de la CA dans le matériel.	"Génération et stockage de certificats de clés publiques dans le matériel" à la page 157
Mise à jour de la liste des certificats révoqués (CRL) d'une PKI	Accédez à la CRL depuis un point de distribution central.	"Traitement des listes des certificats révoqués" à la page 160

Remarque – Pour étiqueter les paquets et les négociations IKE sur un système Trusted Extensions, effectuez les procédures décrites à la section "Configuration d'IPsec avec étiquettes (liste des tâches)" du manuel *Configuration et administration de Trusted Extensions*.

Les certificats de clés publiques sont gérés dans la zone globale sur les systèmes Trusted Extensions. Trusted Extensions ne change pas la manière dont les certificats sont gérés et stockés.

Configuration du protocole IKE avec des certificats de clés publiques

Grâce aux certificats de clés publiques, les systèmes communicants n'ont plus besoin de partager de numéros de clé secrets hors bande. Contrairement aux clés prépartagées, les certificats de clés publiques peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté.

Les certificats de clés publiques peuvent également être stockés dans le matériel connecté. Pour la procédure, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation du matériel connecté" à la page 170.

▼ Configuration du protocole IKE avec des certificats de clés publiques autosignés

Dans cette procédure, vous créez une paire de certificats. La clé privée est stockée sur le disque, dans la base de données de certificats locale, et peut être référencée par la sous-commande `certlocal`. La portion publique de la paire de certificats est stockée dans la base de données des certificats publics. Elle peut être référencée par la sous-commande `certdb`. Vous échangez la portion publique avec un système homologue. La combinaison des deux certificats sert à authentifier les transmissions IKE.

Les certificats autosignés nécessitent un temps système inférieur à celui des certificats publics émanant d'une CA, mais s'intègrent plus difficilement dans un environnement à grande échelle. A la différence des certificats émis par une CA, les certificats autosignés doivent être vérifiés hors bande.

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau), en plus de l'autorisation `solaris.admin.edit/etc/inet/ike/config`. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

1 Créez un certificat autosigné dans la base de données `ike.privatekeys`.

```
# ikecert certlocal -ks -m keysize -t keytype \
-D dname -A altname \
[-S validity-start-time] [-F validity-end-time] [-T token-ID]
```

`-ks`	Crée un certificat autosigné.
`-m` *keysize*	Taille de la clé. La *keysize* peut être 512, 1 024, 2 048, 3 072 ou 4 096.
`-t` *keytype*	Spécifie le type d'algorithme à utiliser. Le *keytype* (type de clé) peut être `rsa-sha1`, `rsa-md5` ou `dsa-sha1`.
`-D` *dname*	Nom distinctif X.509 de l'objet du certificat. *dname* se présente de la manière suivante : C=*country* (pays), O=*organization* (organisation), OU=*organizational unit*, (unité d'organisation) CN=*common name* (nom commun). Les balises valides sont C, O, OU et CN.
`-A` *altname*	Nom alternatif du certificat. *altname* se présente de la manière suivante : `tag=value`. Les balises valides sont `IP`, `DNS`, `email` et `DN`.
`-S`, *validity-start-time*	Indique la date de début de validité absolue ou relative du certificat.
`-F`, *validity-end-time*	Indique la date de fin de validité absolue ou relative du certificat.
`-T` *token-ID*	Permet à un jeton matériel PKCS #11 de générer les clés. Les certificats sont alors stockés sur le matériel.

a. Exécutée par exemple sur le système `partym`, la commande se présente comme suit :

```
# ikecert certlocal -ks -m 2048 -t rsa-sha1 \
-D "O=exampleco, OU=IT, C=US, CN=partym" \
-A IP=192.168.13.213
Creating private key.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEfdZgKjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
a...+
zBGi4QkNdI3f
-----END X509 CERTIFICATE-----
```

Remarque – Les valeurs des options `-D` et `-A` sont arbitraires. Ces valeurs servent uniquement à identifier le certificat. Elles ne permettent pas d'identifier un système, comme 192.168.13.213. Il s'agit en réalité de valeurs idiosyncrasiques, vous devez donc vérifier hors bande que le certificat correct est installé sur les systèmes homologues.

b. Exécutée sur le système `enigma`, elle se présente de la manière suivante :

```
# ikecert certlocal -ks -m 2048 -t rsa-sha1 \
-D "O=exampleco, OU=IT, C=US, CN=enigma" \
```

```
-A IP=192.168.116.16
Creating private key.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEBl5JnjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
...
y85m6LHJYtC6
-----END X509 CERTIFICATE-----
```

2 Enregistrez le certificat et envoyez-le au système distant.

La sortie est une version codée de la portion publique du certificat. Vous pouvez coller en toute sécurité ce certificat dans un e-mail. La partie réceptrice doit vérifier hors bande que le certificat correct est installé, comme indiqué dans l'Étape 4.

a. Par exemple, vous transmettez la portion publique du certificat `partym` à l'administrateur de `enigma`.

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEfdZgKjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
a...+
zBGi4QkNdI3f
-----END X509 CERTIFICATE------
```

b. L'administrateur de `enigma` vous transmet la portion publique du certificat `enigma`.

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: ----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEBl5JnjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
...
y85m6LHJYtC6
-----END X509 CERTIFICATE-----
```

3 Sur chaque système, ajoutez le certificat que vous avez reçu à la base de données de clés publiques.

a. Enregistrez l'e-mail de l'administrateur dans un fichier lisible par `root`.

b. Redirigez le fichier vers la commande `ikecert`.

```
# ikecert certdb -a < /tmp/certificate.eml
```

La commande importe le texte entre les balises `BEGIN` et `END`.

4 Vérifiez auprès de l'autre administrateur que ce certificat est bien de lui.

Par exemple, vous pouvez téléphoner à l'autre administrateur afin de vérifier que le hachage de son certificat public, que vous possédez, correspond au hachage de son certificat privé, que seul lui possède.

a. Répertoriez les certificats stockés sur `partym`.

Dans l'exemple suivant, la remarque 1 indique le nom distinctif du certificat dans l'emplacement 0. Le certificat privé de l'emplacement 0 possède le même hachage (reportez-vous à la remarque 3), ces certificats appartiennent donc à la même paire de certificats. Pour que les certificats publics fonctionnent, vous devez posséder une paire correspondante. La sous-commande `certdb` répertorie la portion publique, tandis que la sous-commande `certlocal` répertorie la portion privée.

```
partym # ikecert certdb -l

Certificate Slot Name: 0   Key Type: rsa
    (Private key in certlocal slot 0)
    Subject Name: <O=exampleco, OU=IT, C=US, CN=partym>     Note 1
    Key Size: 2048
    Public key hash: 80829EC52FC5BA910F4764076C20FDCF

Certificate Slot Name: 1   Key Type: rsa
    (Private key in certlocal slot 1)
    Subject Name: <O=exampleco, OU=IT, C=US, CN=Ada>
    Key Size: 2048
    Public key hash: FEA65C5387BBF3B2C8F16C019FEBC388
partym # ikecert certlocal -l
Local ID Slot Name: 0   Key Type: rsa
    Key Size: 2048
    Public key hash: 80829EC52FC5BA910F4764076C20FDCF     Note 3

Local ID Slot Name: 1   Key Type: rsa-sha1
        Key Size: 2048
        Public key hash: FEA65C5387BBF3B2C8F16C019FEBC388

Local ID Slot Name: 2   Key Type: rsa
    Key Size: 2048
    Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

Cette vérification a permis de confirmer que le système `partym` possédait une paire de certificats valide.

b. Vérifiez que le système `enigma` possède le certificat public de `partym`.

Vous pouvez communiquer la valeur de hachage par téléphone.

Comparez les hachages de la remarque 3 sur `partym` indiquée dans l'étape précédente avec la remarque 4 sur `enigma`.

```
enigma # ikecert certdb -l

Certificate Slot Name: 0   Key Type: rsa
        (Private key in certlocal slot 0)
        Subject Name: <O=exampleco, OU=IT, C=US, CN=Ada>
        Key Size: 2048
        Public key hash: 2239A6A127F88EE0CB40F7C24A65B818

Certificate Slot Name: 1   Key Type: rsa
        (Private key in certlocal slot 1)
        Subject Name: <O=exampleco, OU=IT, C=US, CN=enigma>
        Key Size: 2048
        Public key hash: FEA65C5387BBF3B2C8F16C019FEBC388

Certificate Slot Name: 2   Key Type: rsa
        (Private key in certlocal slot 2)
        Subject Name: <O=exampleco, OU=IT, C=US, CN=partym>
        Key Size: 2048
        Public key hash: 80829EC52FC5BA910F4764076C20FDCF     Note 4
```

Le hachage de clé publique et le nom du sujet du dernier certificat stocké dans la base de données de certificats publics de `enigma` correspond au certificat privé de `partym` issu de l'étape précédente.

5 Approuvez les deux certificats sur chacun des systèmes.

Editez le fichier `/etc/inet/ike/config` pour reconnaître les certificats.

L'administrateur du système distant fournit la valeur des paramètres `cert_trust`, `remote_addr` et `remote_id`.

a. Sur le système `partym` par exemple, le fichier `ike/config` se présente de la manière suivante :

```
# Explicitly trust the self-signed certs
# that we verified out of band. The local certificate
# is implicitly trusted because we have access to the private key.

cert_trust "O=exampleco, OU=IT, C=US, CN=enigma"

# We could also use the Alternate name of the certificate,
# if it was created with one.  In this example, the Alternate Name
# is in the format of an IP address:
# cert_trust "192.168.116.16"

## Parameters that may also show up in rules.

p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha256 encr_alg 3des }
p2_pfs 5

{
 label "US-partym to JA-enigmax"
```

```
 local_id_type dn
 local_id "O=exampleco, OU=IT, C=US, CN=partym"
 remote_id "O=exampleco, OU=IT, C=US, CN=enigma"

 local_addr  192.168.13.213
# We could explicitly enter the peer's IP address here, but we don't need
# to do this with certificates, so use a wildcard address. The wildcard
# allows the remote device to be mobile or behind a NAT box
 remote_addr 0.0.0.0/0


 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

b. Sur le système `enigma`, ajoutez les valeurs de `enigma` des paramètres locaux dans le fichier `ike/config`.

Pour les paramètres distants, utilisez les valeurs de `partym`. Assurez-vous que la valeur du mot-clé `label` est unique sur le système local.

```
...
{
 label "JA-enigmax to US-partym"
 local_id_type dn
 local_id "O=exampleco, OU=IT, C=US, CN=enigma"
 remote_id "O=exampleco, OU=IT, C=US, CN=partym"

 local_addr  192.168.116.16
 remote_addr 0.0.0.0/0
...
```

6 Sur les systèmes homologues, activez IKE.

```
partym # svcadm enable ipsec/ike

enigma # svcadm enable ipsec/ike
```

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

▼ Configuration du protocole IKE avec des certificats signés par une CA

Les certificats publics émanant d'autorités de certification (CA) requièrent une négociation avec une organisation externe. Ces certificats s'intègrent très facilement dans les environnements à grande échelle afin protéger un grand nombre de systèmes communicants.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau), en plus de l'autorisation

`solaris.admin.edit/etc/inet/ike/config`. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

1 La commande `ikecert certlocal -kc` permet de créer une demande de certificat.

Pour consulter la description des arguments de la commande, reportez-vous à l'Étape 1 de la section "Configuration du protocole IKE avec des certificats de clés publiques autosignés" à la page 146.

```
# ikecert certlocal -kc -m keysize -t keytype \
-D dname -A altname
```

a. La commande suivante permet par exemple de créer une demande de certificats sur le système `partym` :

```
# ikecert certlocal -kc -m 2048 -t rsa-sha1 \
> -D "C=US, O=PartyCompany\, Inc., OU=US-Partym, CN=Partym" \
> -A "DN=C=US, O=PartyCompany\, Inc., OU=US-Partym"
Creating software private keys.
  Writing private key to file /etc/inet/secret/ike.privatekeys/2.
Enabling external key providers - done.
Certificate Request:
  Proceeding with the signing operation.
  Certificate request generated successfully (.../publickeys/0)
Finished successfully.
-----BEGIN CERTIFICATE REQUEST-----
MIIByjCCATMCAQAwUzELMAkGA1UEBhMCVVMxHTAbBgNVBAoTFEV4YW1wbGVDb21w
...
lcM+tw0ThRrfuJX9t/Qa1R/KxRlMA3zckO80mO9X
-----END CERTIFICATE REQUEST-----
```

b. La commande suivante permet de créer une demande de certificat sur le système `enigma` :

```
# ikecert certlocal -kc -m 2048 -t rsa-sha1 \
> -D "C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax, CN=Enigmax" \
> -A "DN=C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax"
Creating software private keys.
...
Finished successfully.
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
8qlqdjaStLGfhDOO
-----END CERTIFICATE REQUEST-----
```

2 Soumettez la demande de certificat à un fournisseur de PKI.

Le fournisseur de PKI vous indiquera la procédure de soumission des demandes de certificat. Dans la plupart des cas, celle-ci s'effectue en remplissant un formulaire directement sur le site Web du fournisseur. Dans ce formulaire, vous devrez notamment indiquer la preuve de la légitimité de votre demande. Il suffit généralement de coller votre demande de certificat dans le formulaire. Après avoir vérifié votre demande, le fournisseur émet les deux objets de certificats suivants et une liste des certificats révoqués :

- Votre certificat de clé publique : ce certificat est basé sur la demande que vous avez envoyée au fournisseur. Cette demande est intégrée au certificat, qui vous identifie de manière unique.
- Un certificat CA : la signature du fournisseur. La CA vérifie que votre certificat de clé publique est légitime.
- Une liste des certificats révoqués (CRL) : la liste la plus récente des certificats révoqués par le fournisseur. Cette liste n'est pas expédiée sous la forme d'un objet de certificat séparé si l'accès à la CRL est intégré au certificat de clé publique.

  Si un URI de CRL est intégré au certificat de clé publique, IKE peut récupérer automatiquement la CRL. De la même façon, si une entrée de DN (nom de répertoire sur un serveur LDAP) est intégrée au certificat de clé publique, IKE peut récupérer la CRL sur un serveur LDAP que vous avez spécifié et la mettre en cache.

  Pour consulter un exemple d'URI et d'entrée de DN intégrés à un certificat de clé publique, reportez-vous à la section "Traitement des listes des certificats révoqués" à la page 160.

3 Ajoutez tous les certificats sur votre système.

L'option `-a` de la commande `ikecert certdb -a` ajoute l'objet collé à la base de données de certificats correspondante de votre système. Pour plus d'informations, reportez-vous à la section "IKE avec certificats de clés publiques" à la page 134.

a. Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Reportez-vous à l'Exemple 7–1.

b. Ajoutez le certificat de clé publique que vous avez reçu du fournisseur de PKI.

```
# ikecert certdb -a < /tmp/PKIcert.eml
```

c. Ajoutez le certificat CA émanant du fournisseur de PKI.

```
# ikecert certdb -a < /tmp/PKIca.eml
```

d. Si le fournisseur de PKI vous a envoyé une liste des certificats révoqués, ajoutez-la à la base de données `certrldb` :

```
# ikecert certrldb -a
     Press the Return key
     Paste the CRL:
-----BEGIN CRL-----
...
-----END CRL----
     Press the Return key
<Control>-D
```

4 Le mot-clé `cert_root` permet d'identifier le fournisseur de PKI dans le fichier `/etc/inet/ike/config`.

Utilisez le nom que le fournisseur de PKI vous a indiqué.

a. Sur le système `partym`, par exemple, le fichier `ike/config` peut se présenter de la manière suivante :

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

## Parameters that may also show up in rules.

p1_xform
 { auth_method rsa_sig oakley_group 1 auth_alg sha384 encr_alg aes}
p2_pfs 2

{
 label "US-partym to JA-enigmax - Example PKI"
 local_id_type dn
 local_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
 remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

 local_addr  192.168.13.213
 remote_addr 192.168.116.16

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

Remarque – Tous les arguments du paramètre `auth_method` doivent se trouver sur la même ligne.

b. Créez un fichier similaire sur le système `enigma`.

Le fichier `enigma ike/config` doit :

- Inclure la même valeur `cert_root`.
- Utiliser les valeurs de `enigma` pour les paramètres locaux.
- Utiliser les valeurs de `partym` pour les paramètres distants.
- Créer une valeur unique pour le mot-clé `label`. Elle doit différer de la valeur `label` du système distant.

```
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"
...
{
 label "JA-enigmax to US-partym - Example PKI"
 local_id_type dn
 local_id   "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
 remote_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

 local_addr  192.168.116.16
 remote_addr 192.168.13.213
...
```

5 Spécifiez le mode de traitement des CRL par le protocole IKE.

Choisissez l'option appropriée :

- **Pas de CRL disponible**

  Si le fournisseur de PKI ne fournit pas de CRL, ajoutez le mot-clé `ignore_crls` au fichier `ike/config`.

  ```
  # Trusted root cert
  ...
  cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example,...
  ignore_crls
  ...
  ```

  Le mot-clé `ignore_crls` indique au protocole IKE de ne pas chercher de CRL.

- **CRL disponible**

  Si le fournisseur de PKI vous communique un point de distribution central pour les CRL, vous pouvez modifier le fichier `ike/config` de manière à ce qu'il pointe sur cet emplacement.

  Pour consulter des exemples de ce type de configuration, reportez-vous à la section "Traitement des listes des certificats révoqués" à la page 160.

Exemple 10–2 Utilisation de rsa_encrypt lors de la configuration du protocole IKE

Lorsque vous utilisez `auth_method rsa_encrypt` dans le fichier `ike/config`, vous devez ajouter le certificat homologue à la base de données `publickeys`.

1. Envoyez ce certificat à l'administrateur du système distant.

   Vous pouvez le coller dans un e-mail.

   L'administrateur de `partym` envoie le message suivant :

   ```
   To: admin@ja.enigmaexample.com
   From: admin@us.partyexample.com
   Message: -----BEGIN X509 CERTIFICATE-----
   MII...
   ----END X509 CERTIFICATE-----
   ```

   L'administrateur de `enigma` envoie l'e-mail suivant :

   ```
   To: admin@us.partyexample.com
   From: admin@ja.enigmaexample.com
   Message: -----BEGIN X509 CERTIFICATE-----
   MII
   ...
   -----END X509 CERTIFICATE-----
   ```

2. Sur chacun des systèmes, ajoutez à la base de données `publickeys` locale le certificat envoyé par e-mail.

   ```
   # ikecert certdb -a < /tmp/saved.cert.eml
   ```

En cachant les identités à l'aide du protocole IKE, la méthode d'authentification utilisée en chiffrement RSA prévient les risques d'écoute électronique. Etant donné que la méthode `rsa_encrypt` cache l'identité de l'homologue, le protocole IKE ne peut récupérer son certificat. La méthode `rsa_encrypt` requiert donc que les homologues IKE connaissent leurs clés publiques respectives.

C'est pourquoi vous devez ajouter le certificat de l'homologue à la base de données `publickeys` lorsque vous utilisez la méthode `auth_method` de `rsa_encrypt` dans le fichier `/etc/inet/ike/config`. La base de données `publickeys` détient alors trois certificats pour chaque couple de systèmes communicants :

- Votre certificat de clé publique
- Le certificat CA
- Le certificat de clé publique de l'homologue

Dépannage la charge du protocole IKE, qui inclut les trois certificats, peut s'avérer trop importante pour le chiffrement via `rsa_encrypt`. L'apparition d'erreurs indiquant que l'autorisation a échoué ou que la charge n'est pas conforme peut signifier que la méthode `rsa_encrypt` est incapable de chiffrer la totalité de la charge. Pour réduire la charge, utilisez une autre méthode (par exemple, `rsa_sig`, qui ne requiert que deux certificats).

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

▼ Génération et stockage de certificats de clés publiques dans le matériel

Le processus de génération et de stockage de certificats de clés publiques sur du matériel est similaire au processus de génération et de stockage de certificats de clés publiques sur un système. Dans le premier cas, il convient d'identifier le matériel à l'aide des commandes `ikecert certlocal` et `ikecert certdb`, accompagnées de l'option `-T` et de l'ID de jeton.

Avant de commencer

- Le matériel doit être configuré.
- Excepté si le mot-clé `pkcs11_path` du fichier `/etc/inet/ike/config` pointe sur une autre bibliothèque, le matériel utilise `/usr/lib/libpkcs11.so`. Cette bibliothèque doit être implémentée conformément aux standards suivants : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki), c'est-à-dire une bibliothèque PKCS #11.

  Pour consulter les instructions de paramétrage, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 6000" à la page 170.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau), en plus de l'autorisation `solaris.admin.edit/etc/inet/ike/config`. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'Exemple 7–1.

1 Générez un certificat autosigné ou une demande de certificat et spécifiez l'ID de jeton.

Procédez de l'une des manières suivantes :

Remarque – Pour RSA, la carte Sun Crypto Accelerator 6000 prend en charge des clés d'une longueur maximum de 2 048 bits. Pour DSA, la longueur maximum des clés est de 1 024 bits.

- **Pour un certificat autosigné, utilisez la syntaxe suivante :**

```
# ikecert certlocal -ks -m 2048 -t rsa-sha1 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

L'argument de l'option `-T` est l'ID de jeton de la carte Sun Crypto Accelerator 6000 connectée.

- **Pour une demande de certificat, utilisez la syntaxe suivante :**

```
# ikecert certlocal -kc -m 2048 -t rsa-sha1 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

Pour obtenir une description des arguments de la commande `ikecert`, reportez-vous à la page de manuel `ikecert(1M)`.

2 Lorsque vous êtes invité à saisir le PIN, entrez le nom de l'utilisateur de la carte Sun Crypto Accelerator 6000 suivi de deux-points et du mot de passe de l'utilisateur.

Si la carte Sun Crypto Accelerator 6000 possède un utilisateur `ikemgr` dont le mot de passe est `rgm4tigt`, entrez :

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
```

Remarque – La réponse est stockée en *texte en clair* sur le disque.

Après entrée du mot de passe, le certificat s'imprime :

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
-----BEGIN X509 CERTIFICATE-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
oKUDBbZ9O/pLWYGr
-----END X509 CERTIFICATE-----
```

3 Envoyez votre certificat aux personnes concernées.

Procédez de l'une des manières suivantes :

- **Envoyez le certificat autosigné au système distant.**

  Vous pouvez le coller dans un e-mail.

- **Envoyez la demande de certificat à un fournisseur de PKI.**

  Pour ce faire, suivez les instructions du fournisseur de PKI. Pour plus d'informations, reportez-vous à l'Étape 2 de la section "Configuration du protocole IKE avec des certificats signés par une CA" à la page 151.

4 **Editez le fichier `/etc/inet/ike/config` sur votre système pour reconnaître les certificats.**

Procédez de l'une des manières suivantes :

- **Certificat autosigné**

  Utilisez les valeurs fournies par l'administrateur du système distant pour les paramètres `cert_trust`, `remote_id` et `remote_addr`. Sur le système `enigma` par exemple, le fichier `ike/config` se présente comme suit :

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.116.16"       Local system's certificate Subject Alt Name
cert_trust "192.168.13.213"       Remote system's certificate Subject Alt name


...
{
 label "JA-enigmax to US-partym"
 local_id_type dn
 local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
 remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

 local_addr  192.168.116.16
 remote_addr 192.168.13.213

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

- **Demande de certificat**

  Entrez le nom que le fournisseur de PKI vous a communiqué comme valeur du mot-clé `cert_root`. Sur le système `enigma` par exemple, le fichier `ike/config` peut se présenter comme suit :

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

...
{
 label "JA-enigmax to US-partym - Example PKI"
 local_id_type dn
 local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
 remote_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

 local_addr  192.168.116.16
 remote_addr 192.168.13.213

 p1_xform
```

```
  {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

5 **Placez les certificats de l'autre partie sur le matériel.**

Répondez à la demande de PIN comme vous l'avez fait au cours de l'Étape 2.

Remarque – Vous *devez* ajouter les certificats de clés publiques au matériel connecté qui a généré votre clé privée.

- **Certificat autosigné.**

  Ajoutez le certificat autosigné du système distant. Dans cet exemple, il est stocké dans le fichier `DCA.ACCEL.STOR.CERT`.

  ```
  # ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
  Enter PIN for PKCS#11 token:      Type user:password
  ```

  Si le certificat autosigné a utilisé `rsa_encrypt` comme valeur du paramètre `auth_method`, ajoutez le certificat de l'homologue au magasin du matériel.

- **Certificats émanant d'un fournisseur de PKI.**

  Ajoutez le certificat généré par le fournisseur suite à votre demande et ajoutez la CA.

  ```
  # ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
  Enter PIN for PKCS#11 token:      Type user:password

  # ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CA.CERT
  Enter PIN for PKCS#11 token:      Type user:password
  ```

  Pour ajouter une liste des certificats révoqués (CRL) communiquée par un fournisseur de PKI, reportez-vous à la section “Traitement des listes des certificats révoqués” à la page 160.

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

▼ Traitement des listes des certificats révoqués

Les listes des certificats révoqués (CRL) sont émises par une autorité de certification et contiennent les certificats périmés ou compromis. Vous pouvez traiter les CRL de quatre façons :

- Vous devez faire en sorte que le protocole IKE ignore les listes des certificats révoqués si votre CA n'en émet pas. Pour plus d'informations, reportez-vous à l'Étape 5 de la section “Configuration du protocole IKE avec des certificats signés par une CA” à la page 151.

- Vous pouvez faire en sorte que le protocole IKE accède aux CRL à partir d'un URI (uniform resource indicator, identificateur universel de ressources) dont l'adresse est intégrée au certificat de clé publique de la CA.
- Vous pouvez faire en sorte que le protocole IKE accède aux CRL à partir d'un serveur LDAP dont l'entrée de nom de répertoire (DN, directory name) est intégrée au certificat de clé publique de la CA.
- Vous pouvez traiter les CRL comme des arguments de la commande `ikecert certrldb`. Pour un exemple, reportez-vous à l'Exemple 10–3.

La section ci-dessous décrit la procédure permettant de paramétrer l'utilisation des CRL à partir d'un point de distribution central dans le protocole IKE.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

1 Affichez le certificat que vous avez reçu de la CA.

```
# ikecert certdb -lv certspec
```

`-l` Liste les certificats dans la base de données de certificats IKE.

`-v` Liste les certificats en mode détaillé. Utilisez cette option avec précaution.

certspec Modèle permettant de rechercher les certificats correspondants dans la base de données de certificats IKE.

Par exemple, le certificat suivant a été émis par Oracle. (les détails ont été modifiés).

```
# ikecert certdb -lv example-protect.oracle.com
Certificate Slot Name: 0   Type: dsa-sha1
   (Private key in certlocal slot 0)
 Subject Name: <O=Oracle, CN=example-protect.oracle.com>
 Issuer Name: <CN=Oracle CA (Cl B), O=Oracle>
 SerialNumber: 14000D93
   Validity:
      Not Valid Before: 2011 Sep 19th, 21:11:11 GMT
      Not Valid After:  2015 Sep 18th, 21:11:11 GMT
   Public Key Info:
      Public Modulus  (n) (2048 bits): C575A...A5
      Public Exponent (e) (  24 bits): 010001
   Extensions:
      Subject Alternative Names:
              DNS = example-protect.oracle.com
      Key Usage: DigitalSignature KeyEncipherment
      [CRITICAL]
   CRL Distribution Points:
      Full Name:
         URI = #Ihttp://www.oracle.com/pki/pkismica.crl#i
         DN = <CN=Oracle CA (Cl B), O=Oracle>
```

```
CRL Issuer:
Authority Key ID:
Key ID:             4F ... 6B
SubjectKeyID:       A5 ... FD
Certificate Policies
Authority Information Access
```

Notez l'entrée `CRL Distribution Points.` L'entrée URI indique que la CRL de cette organisation est disponible sur le Web. L'entrée DN indique que la CRL est disponible sur un serveur LDAP. Après que le protocole IKE a accédé à la CRL, celle-ci est mise en cache en vue de futures utilisations.

Pour accéder à la CRL, vous devez tout d'abord accéder à un point de distribution.

2 Choisissez l'une des méthodes suivantes pour accéder à la CRL depuis un point de distribution central.

- **Utilisez l'URI.**

  Ajoutez le mot-clé `use_http` au fichier `/etc/inet/ike/config` de l'hôte. Le fichier `ike/config` se présente comme suit :

  ```
  # Use CRL from organization's URI
  use_http
  ...
  ```

- **Utilisez un proxy Web.**

  Ajoutez le mot-clé `proxy` au fichier `ike/config.` Le mot-clé `proxy` adopte une URL comme argument, comme indiqué ci-dessous :

  ```
  # Use own web proxy
  proxy "http://proxy1:8080"
  ```

- **Utilisez un serveur LDAP.**

  Utilisez le nom du serveur LDAP comme argument du mot-clé `ldap-list` dans le fichier `/etc/inet/ike/config` de l'hôte. Le nom du serveur LDAP est fourni par votre organisation. L'entrée dans le fichier `ike/config` se présente comme suit :

  ```
  # Use CRL from organization's LDAP
  ldap-list "ldap1.oracle.com:389,ldap2.oracle.com"
  ...
  ```

Le protocole IKE récupère la CRL et la met en cache jusqu'à ce que le certificat expire.

Exemple 10–3 Ajout d'une CRL à la base de données certrldb locale

Si la CRL du fournisseur de PKI n'est pas disponible à partir d'un point de distribution central, vous pouvez ajouter cette liste manuellement à la base de données `certrldb` locale. Pour extraire la CRL dans un fichier, suivez les instructions du fournisseur de PKI, puis ajoutez la CRL à la base de données à l'aide de la commande `ikecert certrldb -a`.

```
# ikecert certrldb -a < Oracle.Cert.CRL
```

Configuration du protocole IKE pour les systèmes portables (liste des tâches)

Le tableau ci-dessous décrit les procédures permettant de configurer le protocole IKE pour gérer des systèmes qui se connectent à distance à un site central.

Tâche	Description	Voir
Etablissement de la communication avec un site central depuis un lieu hors site	Permettez aux systèmes hors site de communiquer avec un site central. Ces systèmes peuvent être portables.	"Configuration du protocole IKE pour les systèmes hors site" à la page 164
Utilisation d'un certificat public d'une CA et du protocole IKE sur un système central acceptant le trafic des systèmes mobiles	Configurez un système de passerelle pour accepter le trafic IPsec d'un système ne possédant pas d'adresse IP fixe.	Exemple 10–4
Utilisation d'un certificat public d'une CA et du protocole IKE sur un système ne possédant pas d'adresse IP fixe	Configurez le système portable de manière à protéger son trafic avec le site central (par exemple, le siège de l'entreprise).	Exemple 10–5
Utilisation de certificats autosignés et du protocole IKE sur un système central acceptant le trafic de systèmes mobiles	Configurez un système de passerelle avec des certificats autosignés pour accepter le trafic IPsec d'un système portable.	Exemple 10–6
Utilisation de certificats autosignés et du protocole IKE sur un système ne possédant pas d'adresse IP fixe	Configurez un système portable avec des certificats autosignés pour protéger son trafic avec un site central.	Exemple 10–7

Configuration du protocole IKE pour les systèmes portables

Lorsqu'ils sont configurés correctement, les ordinateurs portables peuvent communiquer avec les ordinateurs centraux de l'entreprise via IPsec et IKE. L'utilisation combinée d'une stratégie IPsec globale et d'une méthode d'authentification de clé publique permet de protéger le trafic des systèmes hors site avec le système central.

▼ Configuration du protocole IKE pour les systèmes hors site

Les protocoles IPsec et IKE requièrent un ID unique pour identifier la source et la destination. Pour les systèmes portables hors site ne possédant pas d'adresse IP unique, vous devez utiliser un autre type d'ID permettant d'identifier un système de manière unique (par exemple, `DNS`, `DN` ou `email`).

Il est toujours préférable de configurer les systèmes portables ou hors site possédant une adresse IP unique avec un autre type d'ID. Par exemple, si ces systèmes tentent de se connecter à un site central par l'intermédiaire d'un boîtier NAT, leur adresse unique n'est pas utilisée. Le boîtier NAT leur assigne une adresse IP arbitraire que le système central ne reconnaît pas.

Les clés prépartagées ne sont pas, elles non plus, un moyen d'authentification approprié pour les systèmes portables, car elles requièrent une adresse IP fixe. Les certificats autosignés ou les certificats PKI permettent par contre aux systèmes portables de communiquer avec le site central.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'Exemple 7–1.

1 Configurez le système central de manière à ce qu'il reconnaisse les systèmes portables.

a. Configurez le fichier `ipsecinit.conf`.

Le système central nécessite une stratégie autorisant une plage étendue d'adresses IP. Les certificats de la stratégie IKE garantissent ultérieurement la légitimité des systèmes connectés.

```
# /etc/inet/ipsecinit.conf on central
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}
```

b. Configurez le fichier de configuration IKE.

Le DNS identifie le système central et les certificats permettent d'authentifier le système.

```
## /etc/inet/ike/ike.config on central
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
```

```
ldap_server    "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root     "C=US, O=Domain  Org, CN=Domain STATE"
#
# List self-signed certificates - trust server and enumerated others
#cert_trust    "DNS=central.domain.org"
#cert_trust    "DNS=mobile.domain.org"
#cert_trust    "DN=CN=Domain Org STATE  (CLASS), O=Domain Org
#cert_trust    "email=root@central.domain.org"
#cert_trust    "email=user1@mobile.domain.org"
#

# Rule for mobile systems with certificate
{
  label "Mobile systems with certificate"
  local_id_type DNS
# CA's public certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

2 Connectez-vous à chacun des systèmes portables et configurez-les de manière à ce qu'ils trouvent le système central.

a. Configurez le fichier `/etc/hosts`.

Le fichier `/etc/hosts` n'a pas besoin d'une adresse pour le système portable, mais peut en fournir une. Il doit contenir une adresse IP publique pour le système central.

```
# /etc/hosts on mobile
central 192.xxx.xxx.x
```

b. Configurez le fichier `ipsecinit.conf`.

Le système portable doit être capable de trouver le système central à partir de son adresse IP publique. Les deux systèmes doivent avoir la même stratégie IPsec.

```
# /etc/inet/ipsecinit.conf on mobile
# Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}
```

c. Configurez le fichier de configuration IKE.

L'identificateur ne peut pas être une adresse IP. Pour les systèmes portables, les identificateurs valides sont les suivants :

- `DN=`*nom-répertoire-ldap*
- `DNS=`*adresse-DNS*
- `email=`*adresse-e-mail*

Les certificats permettent d'authentifier le système portable.

```
## /etc/inet/ike/ike.config on mobile
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server   "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root    "C=US, O=Domain Org, CN=Domain STATE"
#
# Self-signed certificates - trust me and enumerated others
#cert_trust    "DNS=mobile.domain.org"
#cert_trust    "DNS=central.domain.org"
#cert_trust    "DN=CN=Domain Org STATE (CLASS), O=Domain Org
#cert_trust    "email=user1@domain.org"
#cert_trust    "email=root@central.domain.org"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile with certificate"
    local_id_type DNS

# NAT-T can translate local_addr into any public IP address
# central knows me by my DNS

    local_id "mobile.domain.org"
    local_addr 0.0.0.0/0

# Find central and trust the root certificate
    remote_id "central.domain.org"
    remote_addr 192.xxx.xxx.x

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

3 Activez le service `ike`.

```
# svcadm enable svc:/network/ipsec/ike
```

Exemple 10–4 Configuration d'un ordinateur central pour qu'il accepte le trafic IPsec d'un système portable

Le protocole IKE peut commencer les négociations derrière un boîtier NAT, mais il est préférable de ne pas faire intervenir de boîtier de ce type. Dans l'exemple ci-dessous, le certificat public d'une CA a été placé sur le système mobile et sur le système central. Le système central

accepte les négociations IPsec émanant d'un système situé derrière un boîtier NAT. `main1` est le système acceptant les connexions de systèmes hors site. Pour paramétrer les systèmes hors site, reportez-vous à l'Exemple 10–5.

```
## /etc/hosts on main1
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server   "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site system with root certificate"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# CA's public certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
}
```

Exemple 10–5 Configuration d'un système situé derrière un boîtier NAT avec IPsec

Dans l'exemple ci-dessous, le certificat public d'une CA a été placé sur le système mobile et sur le système central. `mobile1` se connecte au siège de l'entreprise depuis son domicile. Le réseau du FAI (fournisseur d'accès Internet) utilise un boîtier NAT pour pouvoir assigner une adresse

privée à `mobile1`. Le boîtier NAT convertit l'adresse privée en une adresse IP publique partagée par d'autres noeuds du réseau du FAI. Le siège de l'entreprise ne se trouve pas derrière un boîtier NAT. Pour paramétrer l'ordinateur du siège de l'entreprise, reportez-vous à l'Exemple 10–4.

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server   "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site mobile1 with root certificate"
  local_id_type DNS
  local_id "mobile1.domain.org"
  local_addr 0.0.0.0/0

# Find main1 and trust the root certificate
  remote_id "main1.domain.org"
  remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

Exemple 10–6 Acceptation de certificats autosignés émanant d'un système portable

Dans l'exemple ci-dessous, les certificats autosignés ont été émis par le système portable et le système central, et ont été placés sur les deux systèmes. `main1` est le système acceptant les connexions de systèmes hors site. Pour paramétrer les systèmes hors site, reportez-vous à l'Exemple 10–7.

```
## /etc/hosts on main1
main1 192.168.0.100
```

```
## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Self-signed certificates - trust me and enumerated others
cert_trust    "DNS=main1.domain.org"
cert_trust    "jdoe@domain.org"
cert_trust    "user2@domain.org"
cert_trust    "user3@domain.org"
#
# Rule for off-site systems with trusted certificate
{
  label "Off-site systems with trusted certificates"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# Trust the self-signed certificates
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

Exemple 10–7 Utilisation de certificats autosignés pour contacter un système central

Dans l'exemple ci-dessous, `mobile1` se connecte au siège de l'entreprise depuis un domicile privé. Les certificats ont été émis par le système portable et le système central, et ont été placés sur les deux systèmes. Le réseau du FAI utilise un boîtier NAT pour assigner une adresse privée à `mobile1`. Le boîtier NAT convertit l'adresse privée en une adresse IP publique partagée par d'autres noeuds du réseau du FAI. Le siège de l'entreprise ne se trouve pas derrière un boîtier NAT. Pour paramétrer l'ordinateur du siège de l'entreprise, reportez-vous à l'Exemple 10–6.

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters

# Self-signed certificates - trust me and the central system
cert_trust    "jdoe@domain.org"
cert_trust    "DNS=main1.domain.org"
```

```
#
# Rule for off-site systems with trusted certificate
{
  label "Off-site mobile1 with trusted certificate"
  local_id_type email
  local_id "jdoe@domain.org"
  local_addr 0.0.0.0/0

# Find main1 and trust the certificate
  remote_id "main1.domain.org"
  remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

Configuration du protocole IKE en vue de l'utilisation du matériel connecté

Les certificats de clés publiques peuvent également être stockés sur du matériel connecté. La carte Sun Crypto Accelerator 6000 permet de stocker et de décharger les opérations de clés publiques du système.

▼ Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 6000

Avant de commencer La procédure suivante suppose que la carte Sun Crypto Accelerator 6000 est connectée au système. et que le ou les logiciels correspondants ont été installés et configurés. Pour obtenir des instructions, reportez-vous au manuel *Sun Crypto Accelerator 6000 Board Version 1.1 User's Guide* (`http://download.oracle.com/docs/cd/E19321-01/820-4144-12/820-4144-12.pdf`).

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Network IPsec Management (gestion IPsec du réseau). Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Pour un exemple, reportez-vous à l'Exemple 7–1.

1. **Assurez-vous que la bibliothèque PKCS #11 est liée.**

   IKE utilise les routines de la bibliothèque pour gérer la génération des clés et leur stockage sur la carte Sun Crypto Accelerator 6000. Entrez la commande suivante pour déterminer si une bibliothèque PKCS #11 a été liée :

   ```
   $ ikeadm get stats
   ...
   PKCS#11 library linked in from /usr/lib/libpkcs11.so
   $
   ```

2. **Déterminez l'ID de jeton pour la carte Sun Crypto Accelerator 6000 connectée.**

   ```
   $ ikecert tokens
   Available tokens with library "/usr/lib/libpkcs11.so":

   "Sun Metaslot                        "
   ```

   La bibliothèque renvoie un ID de jeton, également appelé nom du keystore, de 32 caractères. Dans l'exemple ci-dessous, vous pouvez utiliser le jeton `Sun Metaslot` avec la commande `ikecert` pour stocker et accélérer les clés IKE.

   Pour plus d'informations sur l'utilisation du jeton, reportez-vous à la section "Génération et stockage de certificats de clés publiques dans le matériel" à la page 157.

   Les espaces situés à la fin sont automatiquement remplis par la commande `ikecert`.

Exemple 10–8 Découverte et utilisation de jetons metaslot

Les jetons peuvent être stockés sur le disque, sur une carte connectée ou dans le keystore softtoken fourni par la structure cryptographique. L'ID de jeton du keystore de softtoken peut se présenter comme suit :

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot                      "
```

Pour créer une phrase de passe pour un keystore de softtoken, reportez-vous à la page de manuel `pktool(1)`.

La commande ci-dessous permet d'ajouter un certificat au keystore de softtoken. `Sun.Metaslot.cert` est le fichier contenant le certificat CA.

```
# ikecert certdb -a -T "Sun Metaslot" < Sun.Metaslot.cert
Enter PIN for PKCS#11 token:      Type user:passphrase
```

Étapes suivantes Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

◆ ◆ ◆ CHAPITRE 11

Protocole IKE (référence)

Ce chapitre aborde les sujets suivants :

Pour plus d'informations sur l'implémentation du protocole IKE, reportez-vous au Chapitre 10, “Configuration du protocole IKE (tâches)”. Pour obtenir une présentation du protocole, reportez-vous au Chapitre 9, “Protocole IKE (présentation)”.

Service IKE

Service `svc:/network/ipsec/ike:default` : l'utilitaire de gestion des services (SMF) fournit le service `ike` qui permet de gérer IKE. Par défaut, ce service est désactivé. Avant d'activer ce service, vous devez créer un fichier de configuration IKE, `/etc/inet/ike/config`.

Les propriétés de service `ike` suivantes sont configurables :

- **Propriété** `config_file` : emplacement du fichier de configuration IKE. La valeur initiale est `/etc/inet/ike/config`.
- **Propriété** `debug_level` : niveau de débogage du démon `in.iked`. La valeur initiale est `op`, ce qui signifie opérationnelle. Pour connaître les valeurs possibles, reportez-vous au tableau sur les niveaux de débogage sous *Object Types* de la page de manuel `ikeadm`(1M).
- **Propriété** `admin_privilege` : niveau de privilège du démon `in.iked`. La valeur initiale est `base`. Les autres valeurs sont `modkeys` et `keymat`. Pour plus d'informations, reportez-vous à la section “Commande `ikeadm`” à la page 175.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au Chapitre 1, "Gestion des services (présentation)" du manuel *Gestion des services et pannes dans Oracle Solaris 11.1*. Voir aussi les pages de manuel `smf`(5), `svcadm`(1M) et `svccfg`(1M).

Démon IKE

Le démon `in.iked` automatise la gestion des clés cryptographiques pour IPsec sur les systèmes Oracle Solaris. Il négocie avec un système distant exécutant le même protocole pour fournir, de manière protégée, des numéros de clé authentifiés destinés aux associations de sécurité (SA). Le démon doit s'exécuter sur tous les systèmes qui sont censés communiquer en toute sécurité.

Par défaut, le service `svc:/network/ipsec/ike:default` n'est pas activé. Après que vous avez configuré le fichier `/etc/inet/ike/config` et activé le service `ike`, le démon `in.iked` se lance à l'initialisation du système.

Une fois le démon IKE en cours d'exécution, le système s'authentifie auprès de son entité IKE homologue lors de la phase 1. L'homologue, ainsi que les méthodes d'authentification, sont définis dans le fichier de stratégie IKE. Le démon crée alors les clés pour la phase 2. Les clés IKE sont actualisées automatiquement à un intervalle spécifié dans le fichier de stratégie. Le démon `in.iked` est à l'écoute des demandes IKE entrantes émanant du réseau et des demandes de trafic hors bande via le socket `PF_KEY`. Pour plus d'informations, reportez-vous à la page de manuel `pf_key`(7P).

Le démon IKE est pris en charge par deux commandes. La commande `ikeadm` peut être utilisée pour afficher et modifier temporairement la stratégie IKE. Pour modifier de manière définitive la stratégie IKE, vous devez modifier les propriétés du service `ike`. Pour modifier les propriétés du service IKE, reportez-vous à la section "Gestion des services IKE et IPsec" à la page 119. La commande `ikeadm` peut également servir à afficher les SA Phase 1, les règles de stratégie, les clés prépartagées, les groupes Diffie-Hellman disponibles, les algorithmes d'authentification et de chiffrement Phase 1, et le cache de certificat.

et la commande `ikecert` d'afficher et de gérer les bases de données de clés publiques. Cette dernière gère les bases de données `ike.privatekeys` et `publickeys` locales, ainsi que les opérations de clés publiques et le stockage de ces clés sur du matériel.

Fichier de configuration IKE

Le fichier de configuration IKE, `/etc/inet/ike/config`, gère les clés des interfaces protégées dans le fichier de stratégie IPsec, `/etc/inet/ipsecinit.conf`.

La gestion des clés avec IKE inclut des règles et des paramètres globaux. Les règles IKE identifient les systèmes ou réseaux sécurisés par les numéros de clé. Elles spécifient également la méthode d'authentification. Les paramètres globaux incluent des éléments tels que le chemin

vers un accélérateur matériel connecté. Pour consulter des exemples de fichiers de stratégie IKE, reportez-vous à la section "Configuration du protocole IKE avec des clés prépartagées (liste des tâches)" à la page 140. Pour des exemples et une description des entrées de stratégies IKE, consultez la page de manuel `ike.config(4)`.

Les SA IPsec prises en charge par IKE protègent les datagrammes IP conformément aux stratégies paramétrées dans le fichier de configuration des stratégies IPsec, `/etc/inet/ipsecinit.conf`. Le fichier de stratégie IKE détermine si la confidentialité de transmission parfaite (PFS, perfect forward security) est utilisée lors de la création des SA IPsec.

Le fichier `/etc/inet/ike/config` peut inclure le chemin vers une bibliothèque implémentée conformément au standard suivant : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). IKE utilise la bibliothèque PKCS #11 pour accéder au matériel d'accélération et de stockage des clés.

En matière de sécurité, les considérations concernant le fichier `ike/config` sont similaires à celles concernant le fichier `ipsecinit.conf`. Pour plus d'informations, reportez-vous à la section "Considérations de sécurité pour les commandes `ipsecinit.conf` et `ipsecconf`" à la page 125.

Commande `ikeadm`

La commande `ikeadm` permet d'effectuer les opérations suivantes :

- Afficher les différents aspects de l'état d'IKE
- Modifier les propriétés du démon IKE.
- Afficher les statistiques concernant la création de SA pendant la phase 1.
- Déboguer les échanges du protocole IKE.
- Affiche les objets du démon IKE tels que les SA Phase 1, les règles de stratégie, les clés prépartagées, les groupes Diffie-Hellman disponibles, les algorithmes d'authentification et de chiffrement Phase 1, et le cache de certificat.

Pour consulter des exemples et une description complète des options de cette commande, reportez-vous à la page de manuel `ikeadm(1M)`

Le niveau de privilège du démon IKE en cours d'exécution détermine les aspects du démon IKE susceptibles d'être affichés et modifiés. Trois niveaux de privilège sont possibles.

Niveau `base`	Vous ne pouvez ni afficher ni modifier les numéros de clé. Le niveau `base` est le niveau de privilège par défaut.
Niveau `modkeys`	A ce niveau, vous pouvez supprimer, modifier et ajouter des clés prépartagées.
Niveau `keymat`	Ce niveau vous permet d'afficher les numéros de clé actuels à l'aide de la commande `ikeadm`.

Pour modifier temporairement un privilège, vous pouvez utiliser la commande `ikeadm`. Pour une modification permanente, modifiez la propriété `admin_privilege` du service `ike`. Pour la procédure, reportez-vous à la section "Gestion des services IKE et IPsec" à la page 119.

En matière de sécurité, les considérations concernant la commande `ikeadm` sont similaires à celles concernant la commande `ipseckey`. Pour plus d'informations, reportez-vous à la section "Considérations de sécurité pour la commande `ipseckey`" à la page 128.

Fichiers de clés prépartagées IKE

Lorsque vous créez des clés manuellement, elles sont stockées dans des fichiers du répertoire `/etc/inet/secret`. Le fichier `ike.preshared` contient les clés prépartagées des SA ISAKMP (Internet Security Association and Key Management Protocol) et le fichier `ipseckeys` contient les clés prépartagées des SA IPsec. Ces fichiers sont protégés en mode `0600` et le répertoire `secret` en mode `0700`.

- Lorsque vous configurez le fichier `ike/config` pour demander des clés prépartagées, vous créez un fichier `ike.preshared`. Vous entrez les numéros de clé des SA ISAKMP, c'est-à-dire de l'authentification IKE, dans le fichier `ike.preshared`. Les clés prépartagées étant utilisées pour authentifier la phase 1, le fichier doit être valide avant le démarrage du démon `in.iked`.
- Le fichier `ipseckeys` contient les numéros de clé des SA IPsec. Pour consulter des exemples de gestion manuelle de ce fichier, reportez-vous à la section "Création manuelle de clés IPsec" à la page 115. Le démon IKE n'utilise pas ce fichier. Les numéros de clé générés par IKE pour les SA IPsec sont stockés dans le noyau.

Commandes et bases de données de clés publiques IKE

La commande `ikecert` permet de manipuler les bases de données de clés publiques du système local. Utilisez-la lorsque le fichier `ike/config` requiert des certificats de clés publiques. Ces bases de données étant utilisées par IKE pour authentifier la phase 1 de l'échange, elles doivent être alimentées avant l'activation du démon `in.iked`. Trois sous-commandes permettent de gérer chacune des trois bases de données : `certlocal`, `certdb` et `certrldb`.

La commande `ikecert` permet aussi de gérer le stockage des clés. Les clés peuvent être stockées sur disque, sur une carte Sun Crypto Accelerator 6000 connectée ou dans un fichier keystore de clés softtoken. Ce fichier est disponible lorsque le metaslot de la structure cryptographique est utilisé pour communiquer avec le matériel. La commande `ikecert` utilise la bibliothèque PKCS #11 pour localiser le lieu de stockage des clés.

Pour plus d'informations, consultez la page de manuel `ikecert(1M)` Pour plus d'informations sur le metaslot et sur le fichier keystore de clés softtoken, reportez-vous à la page de manuel `cryptoadm(1M)`.

Commande `ikecert tokens`

L'argument `tokens` répertorie les ID de jetons disponibles. Les ID de jetons permettent aux commandes `ikecert certlocal` et `ikecert certdb` de générer des certificats de clés publiques et des demandes de certificats. Ces certificats et demandes de certificats peuvent également être stockés par la structure cryptographique dans le fichier keystore de clés softtoken ou sur une carte Sun Crypto Accelerator 6000 connectée. La commande `ikecert` utilise la bibliothèque PKCS #11 pour déterminer l'emplacement de stockage des certificats.

Commande `ikecert certlocal`

La sous-commande `certlocal` gère la base de données des clés privées. Les options de cette sous-commande permettent d'ajouter, d'afficher et de supprimer des clés privées. Cette sous-commande permet également de créer un certificat autosigné ou une demande de certificat. L'option `-ks` crée un certificat autosigné et l'option `-kc` une demande de certificat. Les clés sont stockées sur le système, dans le répertoire `/etc/inet/secret/ike.privatekeys`, ou sur un composant matériel connecté (option `-T`).

Lorsque vous créez une clé privée, les options de la commande `ikecert certlocal` doivent avoir des entrées connexes dans le fichier `ike/config`. Le tableau ci-dessous détaille les correspondances entre les options `ikecert` et les entrées `ike/config`.

TABLEAU 11–1 Correspondances entre les options `ikecert` et les entrées `ike/config`

Option `ikecert`	Entrée`ike/config`	Description
`-A` *nom-alternatif-sujet*	`cert_trust` *nom-alternatif-sujet*	Pseudonyme identifiant le certificat de manière unique. Il peut s'agir d'une adresse IP, d'une adresse e-mail ou d'un nom de domaine.
`-D`, *nom-distinctif-X.509*	*nom-distinctif-X.509*	Nom complet de l'autorité de certification, incluant le pays (C), le nom de l'organisation (ON), l'unité d'organisation (OU) et le nom commun (CN).
`-t dsa-sha1`	`auth_method dsa_sig`	Méthode d'authentification légèrement plus lente que RSA.

TABLEAU 11–1 Correspondances entre les options `ikecert` et les entrées `ike/config` *(Suite)*

Option `ikecert`	Entrée`ike/config`	Description
`-t rsa-md5` et `-t rsa-sha1`	`auth_method rsa_sig`	Méthode d'authentification légèrement plus rapide que la méthode DSA. La clé publique RSA doit être suffisamment importante pour chiffrer la charge utile la plus lourde. Les charges les plus lourdes sont habituellement les données d'identité (par exemple, le nom distinctif X.509).
`-t rsa-md5` et `-t rsa-sha1`	`auth_method rsa_encrypt`	Le chiffrement RSA met les identités d'IKE à l'abri des écoutes électroniques, mais implique que les homologues IKE connaissent leurs clés publiques respectives.

Lorsque vous émettez une demande de certificat à l'aide de la commande `ikecert certlocal -kc`, vous envoyez la sortie de cette commande à un fournisseur de PKI ou à une CA. Si votre entreprise possède sa propre PKI, vous envoyez cette sortie à votre administrateur de PKI. Le fournisseur de PKI, la CA ou votre administrateur de PKI crée alors les certificats. Ceux qui vous sont transmis par le fournisseur de PKI ou la CA sont entrés dans la sous-commande `certdb`. La liste des certificats révoqués (CRL) que le fournisseur de PKI vous envoie est entrée dans la sous-commande `certrldb`.

Commande `ikecert certdb`

La sous-commande `certdb` gère la base de données des clés publiques. Les options de cette sous-commande vous permettent d'ajouter, d'afficher et de supprimer des certificats et des clés publiques. Cette sous-commande accepte l'entrée de certificats générés par la commande `ikecert certlocal -ks` sur un système distant. Pour plus d'informations sur cette procédure, reportez-vous à la section “Configuration du protocole IKE avec des certificats de clés publiques autosignés” à la page 146. Cette commande accepte également l'entrée de certificats émanant de fournisseurs PKI ou de la CA. Pour plus d'informations sur cette procédure, reportez-vous à la section “Configuration du protocole IKE avec des certificats signés par une CA” à la page 151.

Les certificats et les clés publiques sont stockés sur le système, dans le répertoire `/etc/inet/ike/publickeys` . L'option `-T` permet de stocker les certificats, les clés privées et les clés publiques sur les composants matériels connectés.

Commande `ikecert certrldb`

La sous-commande `certrldb` gère la base de données des listes des certificats révoqués (CRL), `/etc/inet/ike/crls`. Cette base de données met à jour les listes de révocation des clés publiques. Les certificats qui ne sont plus valides figurent dans ces listes. Lorsqu'un fournisseur de PKI vous fait parvenir une CRL, vous pouvez l'installer dans cette base de données à l'aide de

la commande `ikecert certrldb`. Pour plus d'informations sur cette procédure, reportez-vous à la section "Traitement des listes des certificats révoqués" à la page 160.

Répertoire `/etc/inet/ike/publickeys`

Le répertoire `/etc/inet/ike/publickeys` contient la partie publique des biclés et leur certificat, qui sont stockés dans des fichiers ou à des *emplacements*. Ce répertoire est protégé en mode `0755` et peut être alimenté à l'aide de la commande `ikecert certdb`. L'option `-T` permet de stocker les clés sur une carte Sun Crypto Accelerator 6000 plutôt que dans le répertoire `publickeys`.

Les emplacements contiennent, sous forme chiffrée, le nom distinctif X.509 des certificats qui ont été générés sur un autre système. Si vous utilisez des certificats autosignés, vous devez indiquer le certificat que l'administrateur du système distant vous a envoyé comme entrée de commande. Si vous utilisez des certificats d'une CA, vous installez deux certificats signés d'une CA dans la base de données. Vous installez un certificat basé sur la demande de signature de certificat envoyée à la CA. Vous installez également un certificat de la CA.

Répertoire `/etc/inet/secret/ike.privatekeys`

Le répertoire `/etc/inet/secret/ike.privatekeys` contient des fichiers de clés privées qui font partie de biclés. Ce répertoire est protégé en mode `0700`. La commande `ikecert certlocal` permet d'alimenter le répertoire `ike.privatekeys`. Les clés privées sont effectives uniquement lors de l'installation de leur clé publique homologue, de certificats autosignés ou de certificats CA. Les clés publiques homologues sont stockées dans le répertoire `/etc/inet/ike/publickeys` ou sur du matériel pris en charge.

Répertoire `/etc/inet/ike/crls`

Le répertoire `/etc/inet/ike/crls` contient les fichiers des listes des certificats révoqués (CRL). Chaque fichier correspond à un fichier de certificat public du répertoire `/etc/inet/ike/publickeys`. Les fournisseurs de PKI fournissent les CRL correspondant à leurs certificats. La commande `ikecert certrldb` permet d'alimenter la base de données.

Glossaire

3DES Voir Triple-DES.

adresse à usage local Adresse unicast dont la portée du routage est exclusivement locale (au sein du masque de sous-réseau ou d'un réseau d'abonnés). Cette adresse peut également avoir un caractère local ou global.

adresse anycast Adresse IPv6 attribuée à un groupe d'interfaces (appartenant généralement à des noeuds différents). Un paquet envoyé à une adresse anycast est acheminé vers l'interface *la plus proche* possédant cette adresse. La route suivie par le paquet est conforme à la mesure de distance du protocole de routage.

adresse CIDR Classless Inter-Domain Routing, routage interdomaine sans classe. Format d'adresse IPv4 non basé sur les classes de réseau (classe A, B et C). Les adresses CIDR ont une longueur de 32 bits. Elles utilisent le format de notation décimal avec points IPv4 standard en plus d'un préfixe réseau. Ce préfixe définit le numéro de réseau et le masque de réseau.

adresse de diffusion Adresses réseau IPv4 avec la partie hôte de l'adresse ne comportant que des zéros (10.50.0.0) ou des valeurs à un bit (10.50.255.255). Un paquet envoyé à une adresse de diffusion à partir d'un ordinateur situé sur le réseau local est transmis à tous les ordinateurs reliés au réseau.

adresse de multidiffusion Adresse IPv6 identifiant un groupe d'interfaces d'une manière particulière. Un paquet envoyé à une adresse de multidiffusion est diffusé à toutes les interfaces du groupe. La fonctionnalité de l'adresse de multidiffusion IPv6 est similaire à celle de l'adresse de diffusion IPv4.

adresse de site local (site-local-use) Désignation utilisée pour l'adressage sur un site unique.

adresse lien-local Dans IPv6, désignation utilisée en guise d'adresse d'une liaison simple lors d'une configuration d'adresse automatique, par exemple. Par défaut, l'adresse lien-local est créée à partir de l'adresse MAC du système.

adresse privée Adresse IP impossible à acheminer via le réseau Internet. Les adresses privées peuvent être utilisées par des réseaux internes sur des hôtes n'ayant pas besoin d'établir une connexion Internet. Ces adresses sont définies dans Allocation d'adresses aux Internets privés (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`) et souvent appelées adresses "1918".

adresse unicast Adresse IPv6 identifiant une interface unique sur un noeud IPv6. Le préfixe de site, l'ID du sous-réseau et l'ID de l'interface sont les trois composantes de l'adresse unicast.

AES Standard de chiffrement avancé (Advanced Encryption Standard). Technique de chiffrement de données symétrique par blocs de 128 bits. Le gouvernement des Etats-Unis a adopté la variante Rijndael de l'algorithme comme norme de chiffrement en octobre 2000. AES remplace le chiffrement DES comme norme administrative.

algorithme Diffie-Hellman Egalement appelé cryptographie par clé publique. Protocole d'accord de clés cryptographiques asymétriques mis au point par Diffie et Hellman en 1976. Ce protocole permet à deux utilisateurs d'échanger une clé secrète via un moyen non sécurisé sans secrets préalables. Diffie-Hellman est utilisé par le protocole IKE.

association de sécurité SA, Security Association. Association définissant les propriétés en matière de sécurité entre un premier hôte et un deuxième hôte.

attaque par réflexion Attaque consistant à envoyer à distance des paquets de demande d'écho ICMP à une adresse de diffusion IP ou à plusieurs adresses de diffusion dans le but de congestionner le réseau ou de provoquer de graves interruptions de service.

attaque par rejeu Dans IPsec, attaque impliquant la capture d'un paquet par un intrus. Le paquet stocké remplace ou réplique l'original par la suite. Pour se protéger contre ce type d'attaque, il suffit que le paquet contienne un champ qui s'incrémente pendant la durée de vie de la clé secrète assurant la sécurité du paquet.

autorité de certification (CA) Organisation ou société "tiers de confiance" publiant des certificats numériques utilisés pour créer des signatures numériques et des biclés. La CA garantit l'identité d'une personne ayant reçu un certificat unique.

base de données des stratégies de sécurité SPD, Security Policy Database. Base de données définissant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP afin de déterminer s'il est nécessaire de rejeter un paquet, de le transmettre en clair ou de le protéger avec IPsec.

Blowfish Algorithme de chiffrement par bloc symétrique de longueur de clé variable (entre 32 et 448 bits). Son créateur, Bruce Schneier, affirme que Blowfish est optimisé pour les applications pour lesquelles la clé n'a pas besoin d'être régulièrement modifiée.

CA Voir autorité de certification (CA).

charge utile Données transportées dans un paquet. La charge utile n'inclut pas les informations d'en-tête nécessaires pour amener le paquet à destination.

classe Dans IPQoS, groupe de flux de réseau dotés de caractéristiques identiques. Vous définissez les classes dans le fichier de configuration IPQoS.

comptabilisation des flux Dans IPQoS, processus visant à collecter et à enregistrer les informations sur les flux de trafic. Pour ce faire, il convient de définir les paramètres du module `flowacct` dans le fichier de configuration IPQoS.

compteur Module de l'architecture Diffserv mesurant le débit du trafic d'une classe particulière. L'implémentation IPQoS inclut deux compteurs, `tokenmt` et `tswtclmt`.

configuration automatique Processus selon lequel un hôte configure automatiquement son adresse IPv6 à partir du préfixe de site et des adresses MAX locales.

configuration automatique sans état Processus par lequel un hôte génère ses propres adresses IPv6 en combinant son adresse MAC et un préfixe IPv6 publié par un routeur IPv6 local.

couche liaison Couche située immédiatement sous IPv4/IPv6.

cryptographie par clé asymétrique Système de chiffrement dans lequel l'expéditeur et le destinataire du message utilisent différentes clés pour chiffrer et déchiffrer le message. Les clés asymétriques servent à établir un canal sécurisé pour le chiffrement par clé symétrique. L'algorithme Diffie-Hellman est un exemple de protocole de clé asymétrique. Voir aussi cryptographie par clé symétrique.

cryptographie par clé publique Système cryptographique utilisant deux clés différentes : une clé publique connue de tous et une clé privée présentée exclusivement au destinataire du message. IKE fournit des clés publiques à IPsec.

cryptographie par clé symétrique Système de chiffrement dans lequel l'expéditeur et le destinataire d'un message partagent une clé unique commune. Cette clé commune sert au chiffrement et au déchiffrement du message. Les clés symétriques permettent de chiffrer l'ensemble de la transmission de données dans IPsec. DES est un exemple de système de cryptographie par clé symétrique.

datagramme Voir datagramme IP.

datagramme IP Paquet d'informations transporté par IP. Un datagramme IP contient un en-tête et des données. L'en-tête inclut les adresses de la source et de la destination du datagramme. Les autres champs de l'en-tête permettent d'identifier et de recombiner les données avec les datagrammes associés lorsqu'ils arrivent à destination.

DES Standard de chiffrement de données (Data Encryption Standard). Méthode de chiffrement à clé symétrique développée en 1975 et standardisée par l'ANSI en 1981 comme ANSI X.3.92. Le DES utilise une clé de 56 bits.

détection de réparation Processus permettant de déterminer à quel moment une NIC ou le chemin de la carte vers un périphérique de couche 3 est de nouveau fonctionnel après un échec.

détection de routeur Processus selon lequel les hôtes localisent des routeurs résidant sur une liaison directe.

détection des voisins Mécanisme IP permettant à des hôtes de localiser d'autres hôtes résidant sur une liaison directe.

DOI Un DOI (Domain of Interpretation, domaine d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.

double pile Protocole TCP/IP intégrant IPv4 et IPv6 au niveau de la couche réseau, le reste de la pile étant identique. Lorsque vous activez le protocole IPv6 lors de l'installation d'Oracle Solaris, l'hôte reçoit la version double pile du protocole TCP/IP.

DSA Algorithme de signature numérique (Digital Signature Algorithm). Algorithme de clé publique dont la longueur de clé varie de 512 à 4 096 bits. La norme du gouvernement américain, DSS, atteint 1 024 bits. L'algorithme DSA repose sur l'algorithme SHA-1 en entrée.

DSCP DS Codepoint, point de code DS. Valeur de 6 bits qui, si elle figure dans le champ DS d'un en-tête IP, indique le mode de transfert d'un paquet.

en-tête Voir en-tête IP.

en-tête d'authentification En-tête d'extension assurant l'authentification et l'intégrité des datagrammes IP, mais pas leur confidentialité.

en-tête de paquet Voir en-tête IP.

en-tête IP Vingt octets de données identifiant de manière unique un paquet Internet. L'en-tête inclut l'adresse source et l'adresse de destination du paquet. Une partie facultative de l'en-tête permet d'insérer des octets supplémentaires.

encapsulation Processus selon lequel un en-tête et une charge utile sont placés dans le premier paquet, puis insérés dans la charge utile du deuxième paquet.

encapsulation IP-in-IP Mécanisme de mise en tunnel des paquets IP au sein de paquets IP.

encapsulation minimal Forme facultative IPv4 de la mise en tunnel IPv4 prise en charge par les agents locaux, les agents étrangers et les noeuds mobiles. L'encapsulation permet d'économiser 8 ou 12 octets de surcharge par rapport à l'encapsulation IP-in-IP.

filtrage de paquets Fonction de pare-feu pouvant être configurée pour autoriser ou interdire le transit de paquets particuliers via un pare-feu.

filtre Ensemble de règles définissant les caractéristiques d'une classe dans le fichier de configuration IPQoS. Le système IPQoS sélectionne les flux de trafic conformes aux filtres du fichier de configuration IPQoS en vue de leur traitement. Voir filtrage de paquets.

filtre de paquets dynamique Voir filtre de paquets sans état.

filtre de paquets sans état filtrage de paquets permettant de contrôler l'état des connexions actives et d'identifier, à l'aide des informations obtenues, les paquets du réseau autorisés à franchir le pare-feu. En assurant le suivi et la coordination des demandes et des réponses, un filtre de paquets sans état a la possibilité d'écarter une réponse non satisfaisante.

gestion des clés La façon dont vous gérez les associations de sécurité.

groupe anycast Groupe d'interfaces dotées de la même adresse anycast IPv6. L'implémentation du protocole IPv6 dans Oracle Solaris n'est pas compatible avec la création de groupes et d'adresses anycast. Cependant, les noeuds IPv6 Oracle Solaris peuvent assurer le transport du trafic vers des groupes anycast.

HMAC Méthode de hachage à clé pour l'authentification de messages. HMAC est un algorithme d'authentification à clé secrète. HMAC est utilisé avec une fonction de repère cryptographique répétitive, telle que MD5 ou SHA-1, combinée avec une clé secrète partagée. La puissance cryptographique de HMAC dépend des propriétés de la fonction de repère sous-jacente.

hôte Système qui n'effectue pas le transfert des paquets. Lors de l'installation d'Oracle Solaris, un système est désigné comme hôte par défaut et ne peut plus transmettre de paquets. Un hôte possède généralement une seule interface physique, mais peut également en avoir plusieurs.

hôte multihébergé Système doté de plusieurs interfaces physiques et qui ne transfère pas les paquets. Un hôte multihébergé peut exécuter des protocoles de routage.

ICMP Internet Control Message Protocol, protocole Internet des messages de contrôle. Ce protocole sert à gérer les messages d'erreur ainsi que les messages de contrôle des échanges.

IKE Internet Key Exchange, échange de clé Internet. IKE automatise la mise en service de matériel d'identification authentifié pour les associations de sécurité IPsec.

index du paramètre de sécurité SPI, Security Parameter Index. Nombre entier indiquant la rangée de la SADB qui permettra au récepteur de décrypter un paquet reçu.

interface de réserve Interface physique prévue pour gérer le trafic des données uniquement en cas de défaillance d'une autre interface physique.

interface physique Mode de raccordement d'un système à une liaison. Ce mode de raccordement est souvent mis en oeuvre sous la forme d'un pilote de périphérique et d'une NIC. Certaines cartes d'interface réseau (`igb`, par exemple) peuvent disposer de plusieurs points de connexion.

interface réseau virtuelle (VNIC) Pseudo-interface offrant une connectivité réseau virtuelle qu'elle soit ou non configurée sur une interface réseau physique. Des conteneurs, tels que des zones IP exclusives, sont configurés sur des VNIC afin de former un réseau virtuel.

IP Voir protocole Internet (IP, Internet Protocol), IPv4, IPv6.

IPQoS Fonction logicielle qui permet l'implémentation du modèle Diffserv standard en plus de la comptabilisation des flux et du marquage 802.1 D des réseaux locaux virtuels. A l'aide d'IPQoS, il est possible de fournir différents niveaux de services réseau aux clients et applications, comme indiqué dans le fichier de configuration IPQoS.

IPsec Sécurité IP. Architecture de sécurité assurant la protection des datagrammes IP.

IPv4 Protocole Internet, version 4. IPv4 est parfois appelé IP. Cette version prend en charge un espace d'adressage à 32 bits.

IPv6 Protocole Internet, version 6. IPv6 prend en charge un espace d'adressage à 128 bits.

liaison IP Utilitaire ou moyen de communication à l'aide duquel les noeuds peuvent communiquer dans la couche liaison. La couche liaison se trouve immédiatement sous IPv4/IPv6. Les réseaux Ethernet (simple ou reliés par un pont) ou les réseaux ATM sont des exemples de liaisons IP. Une liaison IP est définie par un ou plusieurs numéros ou préfixes de masque de sous-réseau IPv4. Un même numéro ou préfixe de masque de sous-réseau ne peut pas être attribué à plusieurs liaisons IP. Dans le système ATM LANE, une liaison IP est un LAN à émulation simple. Lorsque vous utilisez le système ARP, la portée du protocole ARP correspond à une liaison IP simple.

liste des certificats révoqués (CRL) Liste des certificats de clés publiques ayant fait l'objet d'une révocation par une CA. Les CRL sont stockées dans la base de données des CRL, gérée par IKE.

MAC MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.

marqueur 1. Module de l'architecture diffserv et IPQoS attribuant une valeur au champ DS d'un paquet IP. Cette valeur indique la manière dont est traité le paquet. Dans l'implémentation IPQoS, le module du marqueur est `dscpmk`.

2. Module dans l'implémentation IPQoS qui marque l'indicateur de réseau local virtuel d'un datagramme Ethernet par une valeur de priorité utilisateur. La valeur de priorité utilisateur indique comment les datagrammes sont transmis sur un réseau comportant des périphériques VLAN. Ce module est appelé `dlcosmk`.

MD5 Fonction de hachage cryptographique répétitive utilisée pour authentifier les messages, y compris les signatures numériques. Elle a été développée en 1991 par Rivest.

modèle Diffserv Norme d'architecture du groupe IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet) destinée à l'implémentation de services différenciés sur les réseaux IP. Les modules principaux comprennent la classification, la mesure, le marquage, l'ordonnancement et le rejet. IPQoS implémente les modules de classification, de mesure et de marquage. Le modèle Diffserv est décrit dans le document RFC 2475, *An Architecture for Differentiated Services*.

MTU Maximum Transmission Unit, unité de transmission maximale. Taille, exprimée en octets, des données pouvant être transmises via une liaison. Ainsi, la MTU d'une liaison Ethernet est de 1 500 octets.

NAT Voir translation d'adresse réseau.

NIC Network Interface Card, carte d'interface réseau. Carte réseau jouant le rôle d'interface d'un réseau. Certaines NIC ont plusieurs interfaces physiques. C'est le cas des cartes `igb`.

noeud Dans IPv6, tout système IPv6, qu'il s'agisse d'un hôte ou d'un routeur.

nom du keystore Nom qu'un administrateur attribue à une zone de stockage, ou keystore, sur une NIC. Le nom du keystore est également appelé jeton ou ID de jeton.

paquet Groupe d'informations transmis sous forme d'une unité sur les lignes de communications. Un paquet contient un en-tête IP et une charge utile.

paquet de demande d'écho ICMP Paquet transmis à une machine sur Internet en vue de solliciter une réponse. De tels paquets sont communément appelés paquets "ping".

pare-feu Dispositif ou logiciel prévu pour isoler le réseau privé ou le réseau intranet d'une organisation d'Internet, afin de le protéger contre d'éventuelles intrusions. Un pare-feu peut inclure le filtrage de paquets, des serveurs proxy et les valeurs NAT (Network Address Translation, translation d'adresse réseau).

périphérique VLAN Interface réseau permettant de renvoyer le trafic vers le niveau Ethernet (liaison de données) de la pile de protocole IP.

PFS Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.

PFS s'applique à l'échange de clés authentifiées uniquement. Voir aussi algorithme Diffie-Hellman.

PHB Per-Hop Behavior, comportement par saut. Priorité accordée à une classe de trafic. Le comportement par saut indique la priorité des flux de cette classe par rapport aux autres classes de trafic.

pile Voir pile IP.

pile de protocole Voir pile IP.

pile IP TCP/IP est souvent appelé une "pile". Ce terme fait référence aux couches (TCP, IP et parfois d'autres) par lesquelles transitent toutes les données aux extrémités client et serveur d'un échange de données.

PKI Public Key Infrastructure, infrastructure de clé publique. Système de certificats numériques, d'autorités de certification et d'autres autorités d'enregistrement prévu pour vérifier et authentifier la validité de chaque partie impliquée dans une transaction Internet.

priorité utilisateur Valeur de 3 bits ayant pour effet de mettre en oeuvre des marqueurs de classe de services, qui définissent la façon dont les datagrammes Ethernet sont transférés sur un réseau de périphériques VLAN.

protocole de transport de contrôle de flux SCTP, Stream Control Transport Protocol. Protocole de la couche transport assurant des communications orientées connexion sous une forme similaire au protocole TCP. De plus, SCTP gère le multihébergement (une des extrémités de la connexion peut être associée à plusieurs adresses IP).

protocole ESP Encapsulating Security Payload, association de sécurité. Extension de l'en-tête assurant l'intégrité et la confidentialité des datagrammes. ESP est l'un des cinq composants de l'architecture de sécurité IP (IPsec).

protocole Internet (IP, Internet Protocol) Méthode ou protocole utilisé pour envoyer les données d'un ordinateur à l'autre via Internet.

publication des voisins Réponse à un message de sollicitation de voisinage ou processus selon lequel un noeud envoie des publications de voisinage non sollicitées pour signaler une modification de l'adresse de couche liaison.

publication du routeur Processus selon lequel les routeurs annoncent leur présence (avec divers paramètres de connexion et paramètres Internet) de façon périodique ou en réponse à un message de sollicitation d'un routeur.

reconfiguration dynamique (DR) Fonction permettant de reconfigurer un système en cours d'exécution sans incidence ou presque sur les opérations en cours. La reconfiguration dynamique n'est pas prise en charge par toutes les plates-formes Sun d'Oracle. Certaines plates-formes Sun d'Oracle ne prennent en charge que la reconfiguration dynamique de certains types de matériel comme les NIC.

redirection Dans un routeur, technique permettant de signaler à un hôte le meilleur noeud (prochain saut) en vue d'atteindre une destination particulière.

reniflage Action d'espionner les communications des réseaux informatiques. Cette technique est fréquemment employée avec des programmes automatisés pour extirper hors ligne des informations telles que des mots de passe en clair.

répartition de charge Processus consistant à distribuer le trafic entrant et sortant au sein d'un groupe d'interfaces. La répartition de charge permet d'augmenter le rendement. Elle ne se produit que lorsque le trafic réseau se dirige vers plusieurs destinations utilisant plusieurs connexions. Il existe deux types de répartition de charge : la répartition de charge entrante pour le trafic entrant et la répartition de charge sortante pour le trafic sortant.

réseau virtuel Regroupement de ressources et fonctionnalités réseau logicielles et matérielles gérées en tant qu'entité logicielle unique. Un réseau virtuel *interne* regroupe les ressources réseau sur un seul système, parfois appelé "réseau en boîte".

résultat Action à réaliser à l'issue de la mesure du trafic. Les compteurs IPQoS aboutissent à trois résultats signalés par la couleur rouge, jaune et verte. Vous définissez ces codes couleur dans le fichier de configuration IPQoS.

routeur Système généralement composé de plusieurs interfaces ayant pour fonction d'exécuter des protocoles de routage et de transférer des paquets. Vous pouvez configurer un système à une seule interface en guise de routeur à condition que le système se trouve à l'extrémité d'une liaison PPP.

RSA Méthode permettant d'obtenir des signatures numériques et des systèmes de cryptographie par clé publique. Cette méthode datant de 1978 a été décrite par trois développeurs (Rivest, Shamir et Adleman).

SA Voir association de sécurité.

SADB Security Associations Database, base de données des associations de sécurité. Table définissant les clés cryptographiques et les algorithmes cryptographiques. Les clés et les algorithmes ont pour intérêt de sécuriser la transmission des données.

saut Mesure permettant l'identification du nombre de routeurs séparant deux hôtes. Si trois routeurs séparent une source et une destination, les hôtes se trouvent à quatre sauts l'un de l'autre.

SCTP Voir protocole de transport de contrôle de flux.

sélecteur Elément définissant de façon spécifique les critères à appliquer aux paquets d'une classe particulière en vue de sélectionner ce trafic dans le flux du réseau. Vous définissez les sélecteurs dans la clause de filtrage du fichier de configuration IPQoS.

serveur proxy Serveur faisant l'interface entre une application client (telle qu'un navigateur Web) et un autre serveur. Ce type de serveur permet de filtrer les demandes afin d'interdire l'accès à certains sites Web, par exemple.

SHA-1 Algorithme de hachage sécurisé (Secure Hashing Algorithm). L'algorithme s'applique à toute longueur d'entrée inférieure à 2^{64} afin d'obtenir une synthèse des messages. L'algorithme SHA-1 sert d'entrée à l'algorithme DSA.

signature numérique Code numérique associé à un message électronique qui identifie l'expéditeur de manière unique.

sollicitation des voisins Sollicitation envoyée par un noeud afin de déterminer l'adresse de couche liaison d'un voisin. Une telle sollicitation consiste à vérifier qu'un voisin est toujours accessible par une adresse de couche liaison mise en cache.

sollicitation du routeur Processus selon lequel les hôtes demandent à des routeurs de générer immédiatement des publications du routeur, et non pas lors de la prochaine exécution programmée.

SPD Voir base de données des stratégies de sécurité.

SPI Voir index du paramètre de sécurité.

TCP/IP Transmission Control Protocol/Internet Protocol, protocole de contrôle de la transmission/protocole Internet. TCP/IP est le langage de communication ou protocole de base sur Internet. Il peut également servir de protocole de communication sur un réseau privé (intranet ou extranet).

translation d'adresse réseau NAT, Network Address Translation. Traduction d'une adresse IP utilisée au sein d'un réseau sous une adresse IP différente connue au sein d'un autre réseau. Cette technique sert à limiter le nombre d'adresses IP globales nécessaires.

Triple-DES Triple-Data Encryption, triple chiffrement des données. Méthode de chiffrement par clé symétrique. Elle nécessite une clé de 168 bits. L'abréviation de Triple-DES est 3DES.

tunnel Chemin suivi par un datagramme pendant son encapsulation. Voir encapsulation.

tunnel bidirectionnel Tunnel pouvant transmettre des datagrammes dans les deux directions.

tunnel inverse Tunnel débutant à l'adresse d'hébergement du noeud mobile et se terminant au niveau de l'agent local.

usurpation Action d'accéder par intrusion à un ordinateur en envoyant un message avec une adresse IP provenant prétendument d'un hôte de confiance. Pour ce faire, un pirate doit d'abord utiliser différentes techniques pour identifier l'adresse IP d'un hôte fiable, puis modifier les en-têtes de paquets pour donner l'impression que les paquets proviennent de cet hôte.

valeur de hachage Nombre généré à partir d'une chaîne de texte. Les fonctions de hachage garantissent que les messages transmis n'ont pas été sabotés. MD5 et SHA-1 sont des exemples de fonctions de hachage unidirectionnel.

VPN Virtual Private Network, réseau privé virtuel. Réseau logique sécurisé utilisant des tunnels dans un réseau public tel qu'Internet.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z