Sécurité Réseau avec /proc/sys/net/ipv4

Table of Contents

Introduction

En complément des règles de pare-feu, le système de fichiers /proc offre quelques améliorations significatives à vos réglages de sécurité réseau. Malheureusement, la plupart d'entre nous ignore tout en dehors de vagues rumeurs et de quelques conseils entendus sur cette bête. Dans cet article, je passerai en revue les bases essentielles du système de fichier /proc/sys/net/ipv4 pour améliorer la sécurité générale du réseau de votre serveur Linux.

Le système de fichiers /proc

Peut-être qu'une des parties les plus négligées de la configuration du pare-feu est en rapport avec le système de fichiers /proc. La structure en pseudo fichier au sein de /proc permet d'interfacer avec les structures de données internes du noyau, soit d'obtenir des informations sur le système soit de modifier des paramètres particuliers. Certaines parties de /proc sont en lecture seule alors que d'autres peuvent être modifiées. Il est souvent fait référence à un système de fichiers virtuel du fait qu'il n'occupe aucun espace disque réel; les fichiers sont crées à la demande lorsque l'on cherche à y accéder. Cet article, ce concentre en particulier sur /proc/sys/net/ipv4.

Autorisation de l'accès au système de fichier /proc

Pour profiter du système de fichiers /proc, il est nécessaire d'activer deux paramètres lors de la compilation du noyau. CONFIG*PROC*FS est le paramètre qui autorise l'accès et la visualisation du

système de fichier /proc et CONFIG_SYSCTL est le bit qui autorise réellement la modification des entrées /proc sans devoir redémarrer ou recompiler le noyau. Les paramètres sont accessibles uniquement au moment du démarrage, après le montage du système de fichier /proc.

Paramètres propres à ICMP

Protection contre le ping ICMP

L'usage habituel de ping est de déterminer quels hôtes sont actifs sur le réseau. On le fait habituellement en envoyant des paquets contenant la requête ICMP ECHO à l'hôte cible. Cette requête, en apparence inoffensive, est souvent bloquée par les administrateurs réseau afin d'améliorer leur anonymat. Les choix de bloquer ICMP ECHO nécessitent d'envoyer des requête de diffusion générale ou de multidiffusion et directement sur l'hôte. Les commandes respectives pour désactiver la protection sont:

```
echo "0" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo "0" > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Protection contre les redirections ICMP

La redirection des messages ICMP peut également être une gêne. Si votre ordinateur ne joue pas le rôle de routeur, vous voudrez probablement la désactiver :

```
echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects
```

Protection contre bogue RFC 1122

On rencontre parfois des routeurs qui répondent incorrectement à trames de diffusion. C'est une violation de la RFC 1122, “Critères pour les hôtes réseau —— couches de communications”. En conséquence, ces événements sont enregistrés par le noyau. Pour éviter d'encombrer inutilement le fichier de registre, il suffit d'indiquer au noyau d'ignorer ces avertissements:

```
 echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
```

Paramètres propres à IP

Désactivation du routage IP

Le routage IP entre interfaces est activé par défaut dans les scripts de démarrage de nombreux

systèmes. Si vous n'attendez pas que votre ordinateur transfère du trafic entre interfaces, ou si vous n'avez qu'une seule interface, c'est sans doute une bonne idée que de le désactiver. Notez que modifier cette valeur réinitialisera tout les paramètres de configuration à leur valeur par défaut; spécifiquement, la RFC1112 pour les hôtes et la RFC1812 pour les routeurs. Par conséquent, modifiez cette valeur avant tout autre paramètre de /proc.

```
if [ -r /proc/sys/net/ipv4/ip_forward ]; then
  echo "Désactivation routage IP"
  echo "0" > /proc/sys/net/ipv4/ip_forward
fi
```

Protection contre la contrefaçon de trame de diffusion

Si au contraire vous décidez d'activer le routage, vous pourrez également modifier le paramètre rp*filter*setting; un point souvent mal compris par les administrateurs réseau. Le rp*filtert peut rejeter les paquets entrant si leur adresse source ne correspond pas à l'interface sur laquelle ils arrivent, ce qui permet de lutter contre les adresses IP contrefaites. Le fait de l'activer aura pour conséquence que le noyau pourrait rejeter du trafic valide si l'hôte à plusieurs adresses IP sur des interfaces différentes, ou une seule interface avec plusieurs adresses IP. Si l'on souhaite recourir à un réseau virtuel privé tel que AT&T VPN services afin de protéger davantage les paramètres réseau. Il est également important de noter que même si l'on n'active pas rp*filter, la protection contre la contrefaçon de trame de diffusion générale est toujours active. Ainsi, la protection qu'il apporte concerne uniquement les adresses internes contrefaites; les adresses externes pouvant toujours l'être. Par défaut il est désactivé. Pour l'activer :

```
if [ -r /proc/sys/net/ipv4/conf/all/rp_filter ]; then
  echo "Activation rp_filter"
  echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
fi
```

Note: Vous avez peut-être noté le sous-répertoire “all” dans ce dernier exemple. dans /proc/sys/net/ipv4/conf il y a un sous-répertoire pour chaque interface et un répertoire appelé “all”. La modification des répertoires propres à une interface n'affectera que cette interface, alors que les changements du répertoire “all” concernera toutes les interfaces du système.

Protection contre la contrefaçon de trame de diffusion

Si le noyau a été compilé avec CONFIG_SYSCOOKIES, il est possible d'activer ou de désactiver optionnellement la protection contre les attaques par inondation de SYN. Notez, la précision, la compilation du noyau avec cette valeur ne l'active pas par défaut. Elle s'active en émettant 'syncookies' quand la file d'arriéré SYN d'une socket déborde. Il est souvent mal compris que l'arriéré de la socket ne soit pas géré par les systèmes d'exploitation récents, ce qui signifie que vos messages d'erreurs peuvent ne pas être reçus par le système gênant. Donc, si on trouve dans avertissements de synflood dans les registres, il faut s'assurer qu'ils ne sont pas causés par la surcharge d'un serveur avant d'activer ce paramètre. Ils peuvent aussi causer des problèmes de connexion pour les autres hôtes qui tentent de vous joindre. Par conséquent, si vous voulez l'activer, exécutez le script ci-dessous:

```
if [ -r /proc/sys/net/ipv4/tcp_syncookies ]; then
   echo "Activation tcp_syncookies"
   echo "1" > /proc/sys/net/ipv4/tcp_syncookies
fi
```

Protection contre le routage source

Normalement, un hôte n'a pas de contrôle sur la route prise par un paquet donné après son premier saut. Ce sont les autres hôtes sur le réseau qui sont chargés de terminer l'envoi. Le Routage IP Source(RIS) est une méthode spécifiant le chemin exact qu'un paquet doit prendre parmi les autres hôtes pour atteindre sa destination. C'est généralement une mauvaise idée du point de vue la sensation de sécurité que quelqu'un puisse diriger les paquets qui vous sont destinés à travers une interface de confiance et effectivement contourner votre sécurité dans certains cas. Un bon exemple est le trafic, SSH ou telnet qui est bloqué sur une interface puisse arriver par une autre de votre système si le routage source est activé, ce qui n'est peut-être pas prévu dans les réglages de votre pare-feu. Vous voudrez sans doute désactiver ce réglage avec :

```
 if [ -r /proc/sys/net/ipv4/conf/all/accept_source_route ]; then
   echo "Désactivation du routage source"
   echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route
 fi
```

Activation de l'enregistrement des marsiens

Les paquets qui ont une adresse source mais pas de route connues sont qualifiés de “marsiens”. Par exemple, s'il y a deux sous-réseaux branchés sur le même concentrateur, les routeurs à chaque terminaison se verront réciproquement comme des “marsiens”. Pour enregistrer de tels paquets dans le journal du noyau, ce qui ne devrait pas se produire, vous devez exécuter:

```
if [ -r /proc/sys/net/ipv4/conf/all/log_martians ]; then
   echo "Activation de l'enregistrement des marsiens"
   echo "1" > /proc/sys/net/ipv4/conf/all/log_martians
fi
```