NuFW Howto

Eric Leblond

Vincent Deffontaines

Jean Baptiste Favre

NuFW Howto

par Eric Leblond

par Vincent Deffontaines

par Jean Baptiste Favre

Historique des versions

Version 0.6.1 2006/11/14
Compléments d'informations sur PAM/NSS. Mises à jour de certains liens.
Version 0.6 2006/10/12
Ajout d'informations récentes sur le noyau.
Version 0.5 2006/08/01
Modification de ce HowTo pour en faire une documentation sur la version 2.0.
Version 0.4.3 2005/11/23
Ajout d'informations sur le paramétrage de nuauth, notamment avec PAM. Diverses corrections mineures
Version 0.4.2 2005/11/22
Ajout d'informations sur la création des certificats et de leur signature par une AC.
Version 0.4.1 2005/08/01
Ajout d'informations, notamment sur les informations d'authentification et la rotation des logs
Version 0.4 2005/07/25
Ajout de précisions concernant RedHat et le portage pour powerpc
Version 0.3 2005/07/18
Relecture avec la publication de la version 1.0.10
Version 0.2 2005/03/30
Compléments
Version 0.1 2005/03/09
Première version

Table des matières

Chapitre 1. Introduction

1.1. Présentation

NuFW est un pare-feu d'entreprise qui effectue une authentification de chaque connexion qui le traverse. Ceci s'effectue de façon transparente en requérant les informations d'identification de l'utilisateur avant qu'une quelconque décision de filtrage ne soit prise. En pratique, cela signifie que les politiques de filtrage peuvent intégrer l'annuaire utilisateur, et amène cette notion d'ID utilisateur au niveau de la couche IP. NuFW repose sur Netfilter, l'état de l'art en matière de filtrage IP dans le noyau Linux. NuFW s'intègre parfaitement avec Netfilter et en étend même les fonctionnalités. Les serveurs sont actuellement disponibles pour Linux ; les clients existent pour Windows, Linux, FreeBSD et Mac OSX.

NuFW peut :

- Authentifier toute connection transitant par la passerelle ou simplement de/vers un sous-réseau précis ou encore un protocole précis (iptables est utilisé pour trier les connections à authentifier).
- Effectuer l'imputation, le routage et la qualité de service en se basant sur les utilisateurs et non plus simplement sur l'adresse IP.
- Filtrer le trafic en fonction du système d'exploitation et des applications utilisées par les utilisateurs distants.
- Constituer le coeur d'un système simple mais sécurisé d'authentification unique.

NuFW est composé de 2 services qui peuvent être installés sur des machines différentes. Le service principal nuauth intègre le support multithread. nuauth recourt à des modules pour toute interaction avec l'extérieur.

1.2. Pré-requis

Dans cette section, toutes les librairies utilisées doivent être installées sur le système. Les fichiers d'en-têtes doivent être situés dans des répertoires standards (afin que **configure** puisse les trouver).

1.2.1. Dépendances de Nuauth

1.2.1.1. Le service nuauth

nuauth dépend de :

- `libglib2.0` : nuauth utilise intensément cette librairie qui procure un ensemble d'objets de haut niveau particulièrement utiles. Il faut au minimum la version 2.4.
- `libgnutls` : le chiffrement des communications entre les différents composants du système est assuré par TLS
- `libsasl2` : l'authentification est effectuée par sasl
- `libtool` : requis pour la compilation des librairies et des modules

1.2.1.2. Journalisation par mysql

La librairie `libmysqlclient` est requise pour la compilation du module correspondant.

1.2.1.3. Journalisation par PostGreSql

La librairie `libpq` est requise pour la compilation du module correspondant.

1.2.1.4. Authentification et vérification des ACL via LDAP

`libldap2` est requis.

1.2.1.5. Authentification utilisateur via GDBM

`libgdbm3`

1.2.1.6. Authentification par défaut via ident

`libident`

1.2.2. Dépendances de nufw

Le service nufw ne dépend que de :

- `iptables` : `libipq.a` est requis pour la compilation du serveur nufw
- `libgnutls` : nufw communique avec nuauth via un tunnel chiffré par TLS

1.2.3. Dépendances pour le marquage utilisateur

Le système nécessite une version modifiée du module ip_queue et de sa librairie correspondante libipq.

1.2.4. Utiliser nfnetlink et obtenir les dernières fonctionnalités de NuFW

Depuis les noyau 2.6.14, ipq est obsolète et doit être remplacé par libnetfilter_queue qui utilise le système nfnetlink. Nous vous encourageons à utiliser cette dernière librairie dans la mesure où elle représente l'avenir. De plus, nfnetlink procure également libnetfilter_conntrack qui est utilisée par NuFW pour implémenter les ACL horaires.

Pour pouvoir bénéficier de ces fonctionnalités, les librairies suivantes sont nécessaires:

- libnfnetlink
- libnetfilter_queue
- libnetfilter_conntrack

Vous pouvez trouver des versions fonctionnelles de ces librairies ici : http://nufw.org/download/libs/index.html Si vous utilisez GNU/Debian, les paquets adaptés sont disponibles là : http://www.nufw.org/debian/

Si vous souhaitez utiliser les ACL horaires, il est recommandé d'utiliser les versions 2.6.18 du noyau ou supérieures ou d'appliquer le correctif disponible sur le site de NuFW.

Chapitre 2. Compilation et installation

2.1. Préparation du noyau

Vous ne devrez modifier votre noyau à l'aide de patch-o-matic que si vous décidez d'utiliser le marquage utilisateur (à partir de la version 2.6.14 du noyau, cette modification est intégrée dans le noyau vanilla). Ceci est nécessaire si vous souhaitez marquer vos flux réseau en fonction de l'ID utilisateur afin, par exemple, d'implémenter une qualité de service basée sur l'utilisateur. Cette fonctionnalité n'est pas nécessaire pour le bon fonctionnement de NuFW. Pour l'activer, installez patch-o-matic et exécutez la commande

```
$./runme ip_queue_vwmark
```

2.2. Pour les versions de noyaux supérieurs à 2.6.14

Si la version de votre noyau est supérieure à 2.6.14 (et cela devrait être le cas!), vous devriez activer les paramètres suivatns :

```
CONFIG_NETFILTER_XT_TARGET_NFQUEUE=Y or m
CONFIG_NETFILTER_NETLINK=Y or m
CONFIG_IP_NF_CONNTRACK=m (Avertissement: ne paramétrez pas cette option pour être statiquem
CONFIG_IP_NF_CONNTRACK_EVENTS=Y
```

Activer ces options vous permettra d'utiliser la cible NFQUEUE ainsi que des règles Netfilter extrêmement simples pour le suivi de connexions.

2.3. Compilation de NuFW

Décompressez l'archive contenant les sources dans le répertoire de votre choix et rendez-vous dans le répertoire ainsi créé.

NuFW recourt à autoconf et automake pour la compilation. De plus, un script **configure** standard est fourni. Les options suivantes (entre autres), sont également disponibles :

- `--with-user-mark` Active le support du marquage utilisateur par le pare-feu NuFW (vous devrez éventuellement modifier votre noyau pour cela, voir ci-dessus)
- `--with-mysql-log` Active le support de la journalisation de l'activité utilisateur dans une base Mysql

- `--with-pgsql-log` Active le support de la journalisation de l'activité utilisateur dans une base PostgreSQL
- `--with-system-auth` Active le support de l'authentification PAM+NSS
- `--with-ldap` Active le support des annuaires LDAP pour le stockage des informations utilisateurs et des ACL
- `--enable-debug` Active l'affichage des messages de débogage

Une liste détaillée des options disponibles peut être obtenue grâce à la commande

```
$./configure --help
```

Vous pouvez donc exécuter **./configure** avec les options dont vous avez besoin puis commencer la compilation et l'installation:

```
$ ./configure --with-ldap --with-system-auth --with-mysql-log \\
  --sysconfdir=/etc/nufw/ --with-debug
$ make
$ sudo make install
```

Nous utilisons l'option de débogage afin d'obtenir un maximum de détails lors de nos tests.

2.4. Configuration initiale et tests

2.4.1. Installation des certificats et du client

Il s'agit ici de copier les certificats par défaut. Vous ne devriez vraiment pas procéder de la sorte sauf en cas de tests; dans le cas contraire, vous voudrez sûrement utiliser vos propres certificats : consultez pour cela la section suivante.

Pour nufw

```
cp conf/certs/nufw-*.pem /etc/nufw/
```

Pour nuauth :

```
cp conf/certs/nuauth*.pem /etc/nufw/
cp conf/certs/NuFW*.pem /etc/nufw/
```

2.4.2. Créer vos propres certificats

Générez votre propre Authorité de Certification:

```
mkdir private
```

```
chmod 700 private
openssl req -new -x509 -keyout private/CAkey.pem -out private/CAcert.pem
```

Vous devriez utiliser ici un mot de passe particulièrement robuste, et, bien entendu, le garder secret.

Générer les clefs privées pour nufw et nuauth:

```
openssl genrsa -out private/nufw-key.pem

openssl genrsa -out private/nuauth-key.pem
```

Générer les demandes de certificats pour nufw et nuauth:

```
openssl req -new -key private/nufw-key.pem -out nufw.csr

openssl req -new -key private/nuauth-key.pem -out nuauth.csr
```

Signer les demandes de certificats grâce à l'AC:

```
openssl x509 -req -days 365 -in nufw.csr -CA private/CAcert.pem \
      -CAkey private/CAkey.pem -CAcreateserial -out nufw-cert.pem

openssl x509 -req -days 365 -in nuauth.csr -CA private/CAcert.pem \
      -CAkey private/CAkey.pem -CAcreateserial -out nuauth-cert.pem
```

Enfin, comme dans la section précédente, copier les fichiers comme demandé: Pour nufw:

```
cp private/nufw-key.pem /etc/nufw/

cp nufw-cert.pem /etc/nufw/
```

Pour nuauth:

```
cp private/nuauth-key.pem /etc/nufw/

cp nuauth-cert.pem /etc/nufw/
```

Avertissement: N'oubliez pas que les fichiers contenant les clefs privées (ici, nufw-key.pem et nuauth-key.pem) doivent rester secrètes.

2.4.3. Configuration basique de nuauth

NuFW fourni un exemple de fichier de configuration pour nuauth, `nuauth.conf`, qui est disponible dans le répertoire `conf`.

Les deux plus importantes directives de configuration sont : `nuauth_client_listen_addr` : définit l'adresse à laquelle **nuauth** va attendre les requètes des clients `nuauth_nufw_listen_addr` : définit l'adresse à laquelle **nuauth** va attendre les requètes de nufw. La liste des machines **nufw** autorisées à se connecter au serveur **nuauth** constitue la variable `nufw_gw_addr`.

Ensuite, vous devez choisir votre module d'authentification et de vérification des ACL. Les modules suivants sont disponibles :

- libldap : les informations utilisateur sont stockées dans un annuaire LDAP
- dbm : les informations utilisateur sont stockées dans une base gdbm
- plaintext : les informations utilisateur sont stockées dans un fichier texte
- system : l'authentification s'adosse à PAM et utilise les groupes existants dans le système. Ceci procure un moyen pratique d'utiliser nss et/ou pam-modules

Ceci est paramétrable via l'option `nuauth_user_check_module` dont la valeur par défaut est `libsystem` (si non défini dans le fichier de configuration). D'autre paramètres concernant la vérification des ACL doivent être précisés si vous choisissez l'authentification parmi :

- libldap
- plaintext

en définissant la variable `nuauth_acl_check_module`.

Afin d'être capable de procéder rapidement aux tests, nous utiliserons le module system pour l'authentification et le module plaintext pour les ACL. Un fichier d'exemple, `acls.nufw`, pour le module ACL plaintext est disponible dans le répertoire `conf`. Copiez le dans `/etc/nufw` et modifiez au besoin le groupe pour l'ACL ssh afin d'utiliser le groupe d'appartenance de l'utilisateur que vous allez utiliser pour les connexions de test.

2.5. Tests

2.5.1. Paramétrage de Netfilter pour un noyau avant la version 2.6.14

Nous devons ajouter les règles de filtrages de façon à déclencher une demande d'authentification pour

toute connection vers ssh:

```
iptables -A OUTPUT -s 192.168.75.0/24 -p tcp --dport 22 -m state --state NEW --syn -j QUEUE
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

1

2.5.2. Paramétrage de Netfilter pour un noyau à partir de la version 2.6.14

Nous devons ajouter les règles de filtrages de façon à déclencher une demande d'authentification pour toute connection vers ssh:

```
iptables -A OUTPUT -s 192.168.75.0/24 -p tcp --dport 22 -m state --state NEW --syn -j NFQUE
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2

2.5.3. Test du système d'authentification

En premier lieu, il faut démarrer le service nuauth dans un terminal

```
nuauth -vvvvvvvvv
```

Ensuite, nous démarrons

```
nufw -vvvvvvvvv
```

dans un autre terminal.

Enfin, nous pouvons essayer de connecter un utilisateur (au sens nufw du terme). Sous Linux, ceci peut être fait par la commande :

```
nutcpc -d -H [NUAUTH IP]
```

Entrez le login et le mot de passe d'un utilisateur.

Dans le terminal nuauth, vous devriez voir quelques chose comme:

```
user bill@nufw uses OS Linux, 3.0.10, #1 Tue Oct 19 23:51:32 CEST 2008
```

3

2.5.4. Premiers tests et débogage

La connection SSH va déclencher la procédure d'authentification :

- nufw reçoit un paquet de Netfilter :

```
[PID] Sending request for 3352783904
```

- nufw ouvre une connexion TLS vers nuauth :

```
[PID] Trying TLS connection
```

- nuauth reçoit la requète de nufw :

```
** Message: Packet :
** Message: Connection : src=192.168.75.2 dst=192.168.75.2 proto=6
** Message: sport=32848 dport=22
```

- nuauth envoie une demande d'authentification au client en fonction de l'IP source :

```
** Message: need to warn client
** Message: sending request
```

- nuauth reçoit la réponse du client :

```
** Message: User :
** Message: Connection : src=192.168.75.2 dst=192.168.75.2 proto=6
** Message: sport=32848 dport=22
** Message: OS : Linux 2.6.9 #1 Tue Oct 19 23:51:32 CEST 2004
** Message: Application : /usr/bin/ssh
```

- nuauth renvoie sa réponse à nufw :

```
Sending auth answer 1 for 3352783904 on 0x42428482 ...
```

- nufw renvoie le paquet dans le noyau :

```
[PID] Accepting 3352783904
```

Notes

1. Seuls les paquets SYN sont envoyés vers QUEUE. Ce n'est pas assez pour effectuer une journalisation avancée des activités utilisateur, mais c'est largement suffisant pour une authentification du trafic.
2. Seuls les paquets SYN sont envoyés vers NFQUEUE. C'est suffisant pour effectuer une journalisation avancée des activités utilisateur dans la mesure où les évènements liés aux connections seront automatiquement envoyés à nufw par Netfilter. Ceci suppose, notamment, que l'option CONFIG_IP_NF_CONNTRACK_EVENTS du noyau soit activée.
3. Avertissement: ne lancez JAMAIS nutcpc avec l'adresse [NUAUTH IP] égale à 'localhost' ou '127.0.0.1', et ce même si nuauth est installé sur la même machine. En effet, dans ce cas, les paquets envoyés à nuauth par le pare-feu proviendront de la machine (avec une adresse égale à, par exemple, 192.168.0.1) alors que nuauth attend pour l'authentification une adresse égale à 127.0.0.1. De ce fait, l'authentification échouera systématiquement.

Chapitre 3. Paramétrage de NuFW

3.1. Utilisation du module LDAP pour vérifier les ACL

3.1.1. Configuration de slapd

Le fichier `acls.schema` doit être placé dans le répertoire `/etc/ldap/schema` et une ligne

```
include         /etc/ldap/schema/acls.schema
```

ajoutée au début du fichier `/etc/ldap/slapd.conf`. Au niveau du contrôle d'accès, on peut ajouter les lignes :

```
#INL access for acls
access to  dn="ou=acls,dc=inl,dc=fr"
       by dn="uid=nufw,ou=Users,dc=inl,dc=fr" write
       by dn="uid=nuauth,ou=Users,dc=inl,dc=fr" read
       by dn="cn=admin,dc=inl,dc=fr" write
       by * none
```

L'utilisateur nufw est autorisé à modifier la politique de sécurité alors que l'utilisateur nuauth n'a qu'un droit de lecture sur les ACL.

3.1.2. Configuration de nuauth

Pour activer la vérification des ACL sur un annuaire LDAP, nous devons modifier le fichier `nuauth.conf` comme suit :

```
nuauth_acl_check_module="libldap"
```

Ensuite, il faut préciser les paramètres de connection à l'annuaire :

```
ldap_bind_dn="uid=nuauth,ou=Users,dc=inl,dc=fr"
ldap_bind_password="secretpassword"
ldap_basedn="dc=inl,dc=fr"
ldap_acls_base_dn="ou=Acls,dc=inl,dc=fr"
```

3.1.3. Utilisation de nuface

INL (http://www.inl.fr) a développé un puissant générateur de règles pour NuFW et Netfilter. Cet outil s'appelle Nuface. Il est disponible ici : http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuFace Il

permet de générer des règles pour NuFW et Netfilter, règles qui sont directement applicables depuis l'interface web.

3.1.4. Configuration de nuaclgen

nuaclgen est un script qui vous permet de gérer des ACL dans un annuaire LDAP.

Il est préférable d'utiliser Nuface plutôt que Nuaclgen dans la mesure où le premier simplifie grandement les opérations. Notamment, lorsque vous utilisez nuaclgen, vous devez modifier manuellement les règles Netfilter alors que Nuface s'en charge pour vous.

Le fichier `nuaclgen.conf` renferme les informations de connexion à l'annuaire LDAP. Elle doivent être adaptées à votre configuration :

```
$ldap_host="localhost";
$username="uid=nufw,ou=Users,dc=inl,dc=fr";
$password="writepasswd";
$basedn="ou=Acls,dc=inl,dc=fr";
```

Pour autoriser les connexions SSH aux membres du groupe 513 à l'aide de l'application `/usr/bin/ssh`, la règle sera :

```
nuaclgen -A cn=ssh,ou=Acls,dc=inl,dc=fr -p 6 --dport 22 -AppName "/usr/bin/ssh" -j ACCEPT -
```

Ou pour une connexion vers un serveur web :

```
nuaclgen -A cn=apt,ou=Acls,dc=inl,dc=fr -p 6 --dport 80 \
  -AppName "/usr/lib/apt/methods/http" -j ACCEPT -g 1042
```

Cette ACL autorise les connexions aux membres du groupe 1042 qui est utilisé par les administrateurs de certains de nos serveurs. Ainsi, les administrateurs ne sont autorisés qu'à récupérer les mise à jour depuis Internet, mais tous les autres utilisateurs se verront refuser l'accès à Internet.

3.2. Activer le suivi des connexions authentifiées avec

NuFW

3.2.1. Paramétrage de nuauth

Pour activer le suivi de connexion avec NuFW, il est nécessaire de paramétrer les options suivantes dans le fichier `nuauth.conf` :

```
nuauth_log_users_sync=1
nuauth_log_users=8
```

3.2.2. Configuration de SQL

Le suivi de connexion révèle toute sa puissance lorsqu'il est associé à la journalisation SQL. Nous allons décrire ici le paramétrage du module MySQL.

Vous devrez créer la base SQL à partir du fichier dump disponible dans le sous-répertoire conf/ de l'archive. Créez un utilisateur dans MySql. Celui-ci doit disposer des droits UPDATE et INSERT sur la table "conntrack_ulog". Enfin, ajoutez les informations de connexions au serveur SQL dans le fichier nuauth.conf.

Lors du déploiement de NuFW en environnement de production, vous devez utiliser le script clean_conntrack.pl qui est disponible dans le sous-répertoire scripts/ de l'archive NuFW à partir de la version 1.0.12. Pour les versions antérieures, vous pouvez récupérer le script ici : Nulog project homepage (http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuLog). Vous devrez créer un utilisateur SQL disposant des privilèges suivants: : SELECT et DELETE sur la table "conntrack_ulog", INSERT sur la table "ulog". Ce script doit être exécuté très régulièrement, à intervalles de quelques minutes seulement, par l'intermédiaire de cron, notamment en cas de trafic important. Si vous ne faites pas cela, la table "conntrack_ulog" sera vite saturée de connexions "mortes" ce qui provoquera un ralentissement de NuFW. La seule opération réalisée par le script est de transférer les connexions "mortes" (ie les connexions fermées ou refusées) vers la tables ulog, qui est en fait une table d'archivage. Celle-ci n'est pas utilisée en production, ni par NuFW, ni par les modules SSO.

Vous pouvez également envisager d'archiver régulièrement la table "ulog", afin d'éviter qu'elle ne grossisse indéfiniment. A partir de la version 1.0.12, les scripts nécessaires sont disponibles dans le sous-répertoire scripts/ de l'archive. Pour les versions antérieures, pour pouvez récupérer les 2 scripts concernés là : Nulog project homepage (http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuLog) Recherchez les scripts ulog_rotate_*.sh. Actuellement, vous devez exécuter ces scripts en tant que root via cron. Bien évidemment, une meilleure solution serait de créer un utilisateur particulier pour exécuter ces scripts, en lui donnant les droits appropriés. Merci de fournir une mise à jour à cette documentation si vous l'implémentez avant nous.

3.2.3. Configuration de Netfilter

3.2.3.1. Paramètres pour les noyaux post 2.6.14

Cette opération est nettement simplifiée par rapport aux noyaux antérieurs. Pour activer le suivi des connexions authentifiées, vous n'avez qu'à ajouter l'option `-C` à la commande de démarrage de nufw. Cette option indiquera à nufw de communiquer à nuauth tous les évènements Netfilter ESTABLISHED et DESTROY en provenance du système de suivi de connexions de Netfilter.

L'option ci-dessus risque de générer un nombre conséquent d'évènements que devra gérer nuauth. Afin d'éviter un déni de service dû à la saturation de nuauth, nufw offre la possibilité de sélectionner les évènements à envoyer. Cette fonctionnalité utilise les capacités de Netfilter en matière de marquage des connections, matérialisées par la cible CONNMARK. Cette cible permet de marquer automatiquement tous les paquets ESTABLISHED. Ce mode de fonctionnement est activé par l'option `-M` de nufw. Du côté de Netfilter, les règles suivantes devront être ajoutées:

```
iptables -A PREROUTING -t mangle -j CONNMARK --restore-mark
iptables -A POSTROUTING -t mangle -m mark ! --mark 0 -j CONNMARK --save-mark
```

En résumé, vous devriez toujours utiliser l'option `-C` si vous utilisez libnetfilter_conntrack (qui est disponible dans le noyau linux depuis la version 2.6.14), et l'option `-M` si vous envisagez d'utiliser le marquage des connections par l'identifiant utilisateur (vueillz noter que vous devrez alors appliquer le patch suivant transmit_mark patch (http://nufw.org/download/patches/transmit_mark.patch) à votre noyau. Cette dernière option fonctionnera beaucoup mieux avec un noyau 2.6.16 et supérieur.

3.2.3.2. Paramètres pour les noyaux antérieurs au 2.6.14

NuFW mémorise les états des connexions TCP suivants :

- opening : drapeau SYN envoyé
- established : drapeaux SYN et ACK envoyés
- closed : drapeaux FIN ou FIN,ACK envoyés

Pour détecter ces paquets, nous devons utiliser les options `--syn` et `--tcp-flags` de Netfilter. Voyons un exemple : notre serveur HTTP est protégé par un pare-feu NuFW. Ils sont positionnés dans le sous-réseau $DMZ. Les règles ci-après permettent de réaliser un suivi des connexions utilisateurs pour les connexions sortantes.

```
iptables -A FORWARD -p tcp -m state --state ESTABLISHED --tcp-flags ACK,FIN NONE -j ACCEPT
iptables -A FORWARD -d $DMZ -p tcp -m state --state ESTABLISHED --dport 80 --tcp-flags SYN,
iptables -A FORWARD -d $DMZ -p tcp -m state --state ESTABLISHED --dport 80 --tcp-flags FIN
iptables -A FORWARD -s $DMZ -p tcp -m state --state ESTABLISHED --sport 80 --tcp-flags SYN,
iptables -A FORWARD -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -d $DMZ -p tcp --syn --dport 80 -m state --state NEW -j QUEUE
```

La première règle accélère le fonctionnement de Netfilter en détectant la plus grande partie du trafic ESTABLISHED en l'acceptant. La dernière règle comportant l'option --state ESTABLISHED constitue la règle standard pour les connexions établies. Il est indispensable de l'ajouter après les règles de filtrage propres à NuFW.

3.2.3.3. Paramétrage pour les noyaux supérieurs à 2.6.14

Aucune régle compliquée n'est nécessaire, le noyau enverra automatiquement les nouveaux événements à NuFW. C'est pour cette raison que nous recommandons un noyau supérieur à 2.6.14.

3.2.4. Utiliser le suivi de connexions

nutop est un script perl fourni avec les sources de nufw. Il permet d'afficher en temps réel les connexions authentifiées actives de façon similaire à la commande top.

Le plus simple[2] afin d'exploiter la journalisation effectuée par le système de suivi de connexion est d'installer **nulog** (autrefois nommé ulog-php) qui fourni une interface web conviviale. **nulog** est disponible sous license GPL ici : http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuLog

3.3. Paramétrage de l'authentification unique (Single Sign On)

3.3.1. Apache

Tout ce dont vous avez besoin est de créer un utilisateur SQL disposant des droits SELECT sur la table "conntrack_ulog". Puis, paramétrez le module Apache mod_auth_nufw afin qu'il utilise les informations utilisateurs/base de données et table. Le code source du module pour Apache peut être récupéré là : NuFW Apache SSO page (http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/mod_auth_nufw)

3.3.2. Squid

De la même façon, il faut ajouter un utilisateur SQL disposant du droit SELECT sur la table "conntrack_ulog". Puis, paramétrez squid_nufw_helper pour qu'il utilise ces informations. Le code source correspondant est disponible ici : NuFW Squid SSO page (http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/squid_nufw_helper)

3.4. Authentification à l'aide de certificats

Il est possible d'employer des certificats clients : si un utilisateur en fourni un lors de l'établissement de la connexion TLS, nuauth va vérifier si le DN correspond à un utilisateur connu du système. Si c'est le cas, l'utilisateur est réputé authentifié et aucun mot de passe n'est demandé. Pour activer cette fonctionnalité, vous devez definir l'option `nuauth_tls_auth_by_cert` à 1. Dans ce cas de figure, `nuauth_tls_request_cert` doit être positionné à 1 ou 2.

3.5. Qualité de service par utilisateur

3.5.1. Paramétrage des noyaux ne disposant pas de libnetfilter_queue

Les noyaux officiels sont incapables d'utiliser le marquage de paquets conjointement avec ip_queue. Il est donc nécessaire de modifier le noyau (version antérieures à 2.6.14), ce qui est possible grâce au correctif `ip_queue_vwmark` intégré dans patch-o-matic-ng de Netfilter. Cette opération va à la fois fournir une version modifiée du module ip_queue et du fichier libipq.a.

Une fois libipq.a installé, vous pouvez alors compiler nufw :

```
./configure --with-user-mark ${EXTRA_OPTIONS_YOU_LIKE}
make
make install
```

3.5.2. Paramétrage de nufw

nufw peut alors être exécuter avec l'option `-m` pour activer le support du marquage utilisateur. Cette option est compatible avec l'option `-M` vue au-dessus.

3.5.3. Paramétrage de Netfilter

Dans la mesure où NuFW n'utilise que les premiers paquets de chaque connexion, il ne peut effectuer le marquage des autres. Il est donc nécessaire d'utiliser la cible CONNMARK[3]. Cette cible mémorise et rétabli automatiquement le marquage sur tous les paquets concernés d'une connexion. Exemple de paramétrage simple :

```
iptables -A PREROUTING -t mangle -j CONNMARK --restore-mark
iptables -A POSTROUTING -t mangle -j CONNMARK --save-mark
```

La première règle récupère le marquage existant à l'arrivée d'un paquet et la seconde sauvegarde le marquage appliqué afin de pouvoir le restaurer plus tard.

3.5.4. Utiliser le marquage par l'identifiant utilisateur

Le marquage Netfilter peut être utilisé pour la qualité de service et le routage.

Il devient donc possible de préciser des routes spécifiques à tel ou tel utilisateur grâce, par exemple, à la commande :

```
ip rule add fwmark XXX lookup TABLE
```

Il en va de même pour les opération de QoS: en utilisant la commande **tc filter** on peut alors répartir le trafic dans des classes spécifiques en fonction de l'identifiant utilisateur :

```
tc filter add dev IFACE prio 5 protocol ip handle 102 fw flowid FLOWID
```

Pour plus d'information sur le routage avancé et la qualité de service, on se référera utilement au guide lartc (http://www.lartc.org).

3.6. Chaîner les modules dans nuauth

3.6.1. Syntaxe

Chaque option définissant l'utilisation d'un module doit être de la forme d'une liste de modules, séparés d'un espace

Pour chaque module, la syntaxe doit être de la forme : `name[:type[:config file]]` Exemples :

- `name`: charge le module "name" dont les directives de configuration se trouvent dans le fichier nuauth.conf
- `name:type`: charge le module "type" dont les directives de configuration se trouvent dans le fichier CONFIG_DIR/modules/name.conf
- `name:type:conf`: charge le module "type" dont les directives de configuration se trouvent dans le fichier "conf"

3.6.2. Quelques exemples

Analysons les exemples suivants : `nuauth_user_logs_module="syslog dblocal:mysql maindb:mysql:/etc/nufw/mainmysql.conf"` Les paquets seront journalisés plusieurs fois :

1. Par syslog
2. Dans une base MySql en utilisant le fichier de configuration /etc/nufw/modules/dblocal.conf
3. Dans une autre base MySql en utilisant le fichier de configuration /etc/nufw/mainmysql.conf

3.7. Sécuriser l'installation de NuFW

3.7.1. Vérification des certificats par nufw

Il est particulièrement recommandé de placer nuauth dans un endroit protégé afin de garantir la sécurité des communications entre nufw et nuauth[4]. Dans la mesure où la décision du pare-feu dépend de la réponse de nuauth, il est important de pouvoir valider l'identité du serveur nuauth. Pour cela, nous pouvons demander à `nufw` de vérifier le certificat présenté par `nuauth` lors de l'établissement du tunnel TLS. Ceci peut être mis en place grâce à l'option `-a` suivie du nom du fichier contenant le certificat d'autorité racine. Cette option est ajoutée à la ligne de commande démarrant `nufw`. Ce faisant, `nufw` vérifiera la validité du certificat présenté par `nauth`.

3.7.2. Côté client

Du côté du client, le système doit être intègre pour que les informations conernant les applications et le système d'exploitation soient pertinentes. Vous devez toujours garder à l'esprit que seul l'agent installé côté client est capable d'obtenir ces renseignements. En cas d'attaque, il est évident que ces informations PEUVENT et SERONT faussées par l'installation d'un agent NuFW modifié.

Vous devez impérativement tenir compte de cet avertissement et ne surtout pas oublier que cette fonctionnalité permet de sécuriser des flux qui auraient dû être ouvert sans vérification sur un système basique[5].

La pertinence du filtrage d'application et/ou de système d'exploitation dépend de la confiance que vous placez dans le système qui réalisera l'authentification. Elle est "relativement bonne" sur un système sécurisé sur lequel les utilisateurs ne peuvent installer de logiciels.

3.8. Configuration de l'authentification sur Nuauth

3.8.1. Authentification PAM

PAM permet simplement d'étendre les méthodes d'authentification à des annuaires "exotiques". Par exemple, PAM vous permet d'interfacer nuauth avec un domaine NT, Active Directory, Radius, etc.

Pour réaliser l'authentification utilisateur en s'appuyant sur PAM, vous devez paramétrer nuauth.conf (pour la 1.0):

```
nuauth_user_check_module="system"
```

En complément, il faut configurer correctement PAM. Ce point ne fait pas directement partie des objectifs de ce document. Voici quelques exemples de fichiers de configuration PAM basé sur la distribution GNU/Debian afin de permettre à nuauth d'utiliser l'authentification PAM : /etc/pam.d/nuauth :

```
#This is to set PAM-LDAP, modify to suit your needs!
  auth    required      /lib/security/pam_env.so
  auth    sufficient    /lib/security/pam_ldap.so
  auth    required      /lib/security/pam_deny.so

  account required      /lib/security/pam_ldap.so

  session required      /lib/security/pam_limits.so
  session optional      /lib/security/pam_ldap.so
```

Le fichier /etc/nsswitch.conf doit également être adapté :

```
#This is to set PAM-LDAP, modify to suit your needs!
  passwd:         compat ldap
  group:          compat ldap
```

(ne modifiez pas les autres lignes). Vous souhaiterez également adapter la configuration du fichier /etc/pam_ldap.conf. Ce fichier fonctionne correctement chez nous :

```
  host 127.0.0.1
  ldap_version 3
  scope one
  pam_password crypt
  nss_base_passwd         ou=Users,dc=nufw,dc=org?one
  nss_base_group          ou=Group,dc=nufw,dc=org?one
```

Vous devrez également installer et configurer libnss-ldap. La configuration suivante fonctionne pour nous (toujours sous Debian) :

```
host 127.0.0.1
base replace_with_your_base
ldap_version 3
rootbinddn cn=admin,dc=replace_with_your_base
#Optional, set if you need these :
nss_base_passwd ou=users,dc=replace_with_your_base?one
nss_base_group ou=groups,dc=replace_with_your_base?one
```

Bien entendu, vous devez adapter ce qui précède à vos besoins propres. Souvenez-vous que ces directives ne sont peut-être pas adaptées à d'autres distribution que GNU/Debian!

3.8.2. Authentification LDAP

C'est relativement limpide à réaliser : le gros du travail doit être effectué dans le fichier nuauth.conf (les différentes options sont documentées dans le fichier lui-même). Souvenez-vous qu'utiliser une authentification directe sur un LDAP vous obligera à utiliser un schéma LDAP spécifique à NuFW ce qui pourrait se révéler bloquant pour vous. Dans ce cas, envisagez sérieusement l'utilisation de PAM comme décrit ci-dessus.

Notes

1. Comme nuaclgen.conf contient des informations sensibles, ses permissions doivent être les plus restrictives possible.
2. au moment d'écrire cette documentation en tout cas
3. CONNMARK est disponible dans patch-o-matic version antérieure à 2.6.11, et est inclu dans le noyau depuis la version 2.6.12
4. Même si tous les paquets sont chiffrés par TLS
5. Merci d'éviter le syndrome ABS : « Nous avons plus de sécurité, nous pouvons prendre plus de risques et freiner plus tard »

Chapitre 4. Divers

4.1. Architectures "Big endian"

Ce type d'architecture est supporté depuis la version 1.0.11. Les versions antérieures ne fonctionnent pas.

4.2. Spécificités Debian

NuFW est inclu dans la distribution Debian. Les paquets sont aussi stables que possible mais n'hésitez pas à sauvegarder votre configuration avant une mise à jour. Dans le même ordre d'idée, tout retour d'expérience est le bienvenu. Depuis la version 1.0.16, les paquets Debian sont considérés comme particulièrement stables.

4.3. Spécificités Mandrake/Mandriva

NuFW est inclu dans Mandriva Corporate Server 4.

4.4. Spécificités Suse

La version 9 de Suse semble utiliser une très ancienne version de Glib, qui n'est pas compatible avec NuFW. Il semble que cela soit le cas pour toutes les version de Suse jusqu'à la 9.

4.5. Spécificités Redhat

4.5.1. RedHat Enterprise Linux 4

RHEL4 étant fournie avec la version 2.6.9 du noyau, ce système est sujet au problème lié à ip_queue comme mentionné ci-après. Le problème s'est systématiquement posé avec ce noyau (en tout cas sur les machines multi-processeurs).

4.6. Problèmes connus

4.6.1. Problème avec ip_queue sur les noyaux antérieurs au 2.6.12

Il existe un bug ip_queue dans les moyaux antérieurs au 2.6.12. Il provoque un crash du système lorsque qu'une décision ACCEPT est prise dans la chaîne INPUT. N'utilisez donc pas la cible QUEUE dans la chaîne INPUT avec ces noyaux ou vous risquez de geler votre machine. Dans tous les cas de figure vous devriez vraiment utiliser un noyau plus récent et la cible NFQUEUE, comme expliqué plus haut dans ce document.

Glossaire

nufw

nufw est le service qui tourne sur le pare-feu. Il reçoit les paquets du noyau, les envoie au service d'authentification et récupère la réponse.

nuauth

nuauth est le service d'authentification qui reçoit les paquets en provenance de nufw et du client, prend une décision concernant la connexion et la renvoie à nufw.