Introduction à NuFW

Vincent Deffontaines
Eric Leblond
INL

April 12, 2005

NuFW

- Now User Filtering Works
- Not a Usermode FireWall

Les motivations de NuFW

- Intégration de la notion d'utilisateur à la couche de filtrage IP
- Implémentation stricte des politiques de sécurité
- Extensions fonctionnelles :
  - Authentification Unique
  - QoS et routage par utilisateur

Historique du projet

- 2001, Travail sur NSM : ajout d'un support LDAP
- Période de définition et d'écriture de l'algorithme

Historique des filtres IP

- Pas de parefeu
- Inspection des états
- Nouvelles voies en recherche (?)

Les pistes nouvelles

- Filtrage de contenu
  - Remontée jusqu'aux couches hautes du modèle OSI
  - Filtrage Antivirus
  - etc.
- Authentification des utilisateurs

NuFW

- Authentification sécurisée de *chaque* connexion IP
- Intégration de la notion d'utilisateur aux règles de filtrage
- Intégration de la notion d'utilisateur à la politique de QoS
- Intégration aux composants applicatifs, Single Sign On

Authentification "classique" des utilisateurs

"Session" au cours de laquelle utilisateur = IP

- Login HTTPS sur le firewall
- Session SSH sur le firewall qui active un jeu de règles pour l'IP source (*authpf*)
- Association "en dur" au niveau des règles de filtrage
- Toutes ces solutions supposent utilisateur = IP et sont donc peu sécurisées

Faiblesses du modèle utilisateur = IP

- Machines multi-utilisateurs
- Durée de l'association : comment savoir quand l'association n'est plus valide?
- Attaques assez simples : spoofing IP

Apports de l'identification des paquets

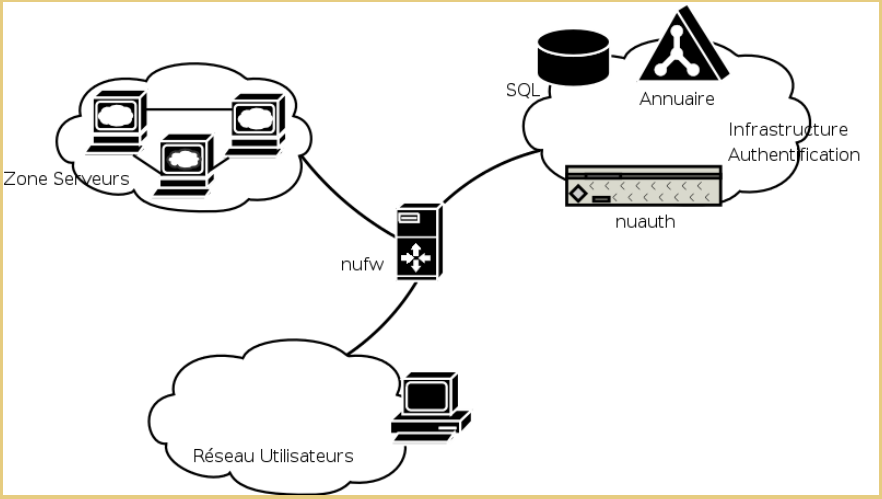
- Implémentation fine de la politique de sécurité
- Support des stations multi-utilisateurs
- Distinction du trafic des démons d'un système (utilisateurs systèmes)

Contraintes de l'identification des paquets

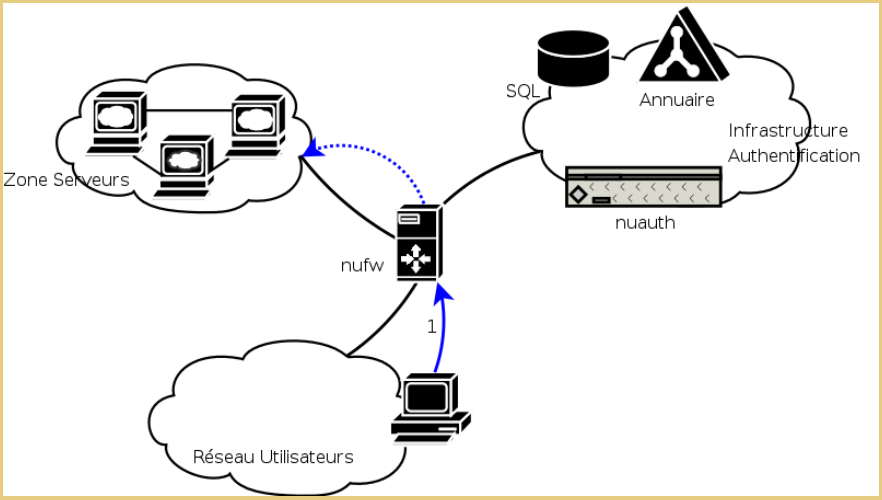
Un tel système apporte des contraintes pour garantir une authentification sûre des données de connexion :

- Présence d'un client logiciel sur chaque machine ouvrant des connexions
- Mise en place d'une base d'utilisateurs centrale
- Mise en place d'une base d'ACLs pour définir les droits
- Complexification du système pare-feu

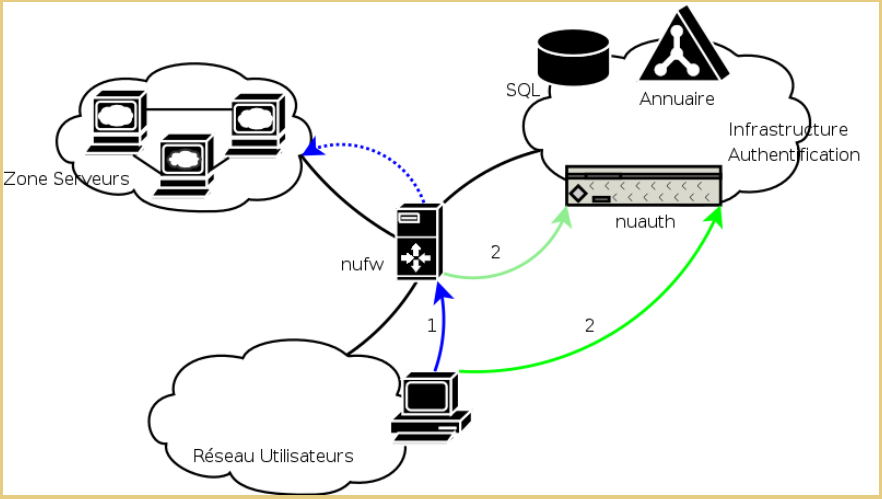
Architecture de NuFW



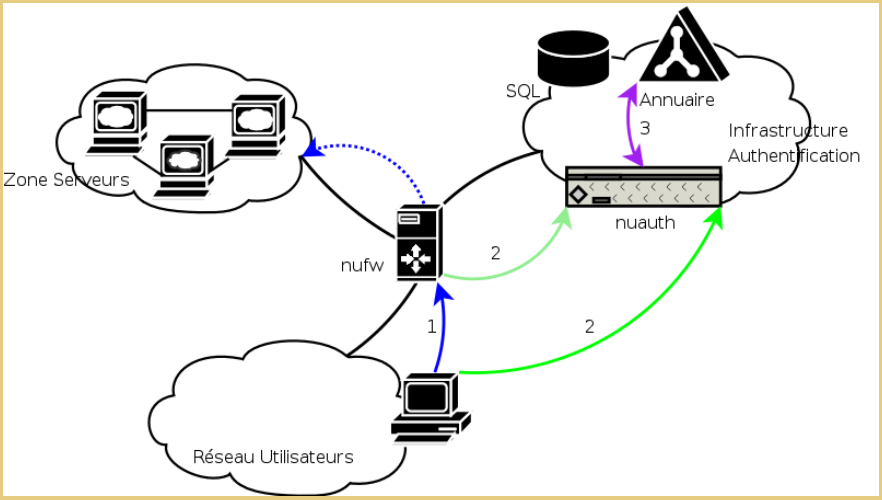
Architecture de NuFW



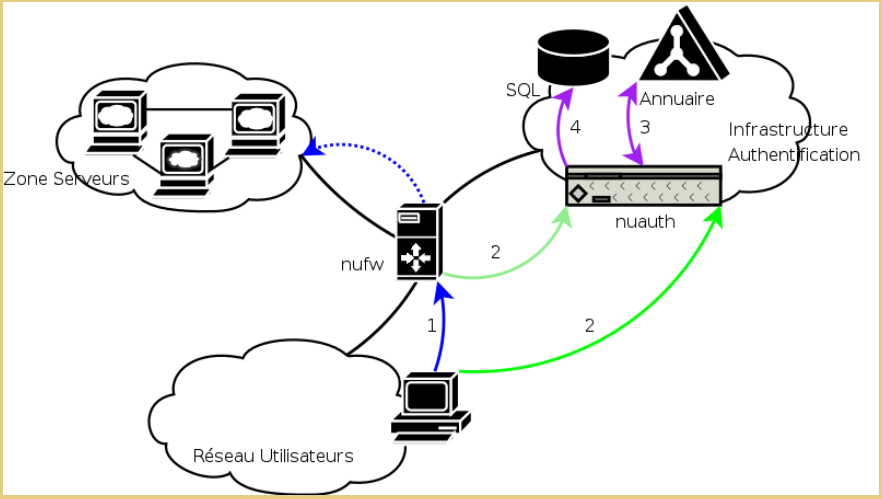
Architecture de NuFW



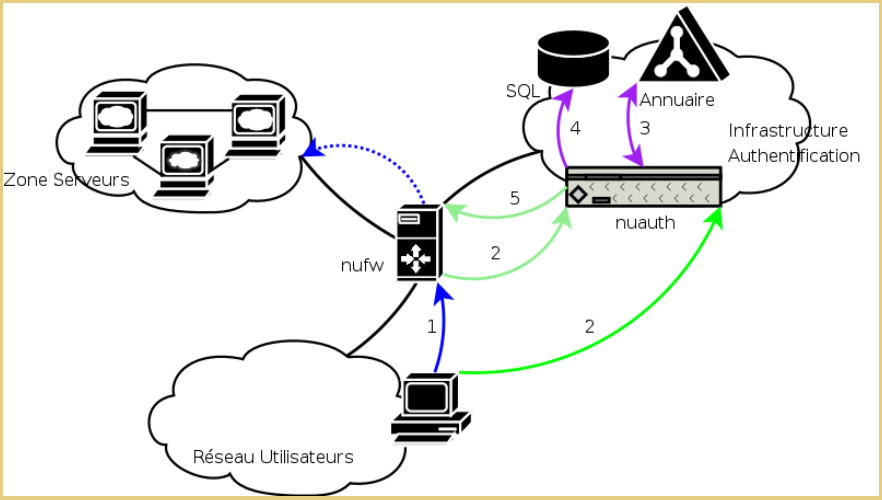
Architecture de NuFW



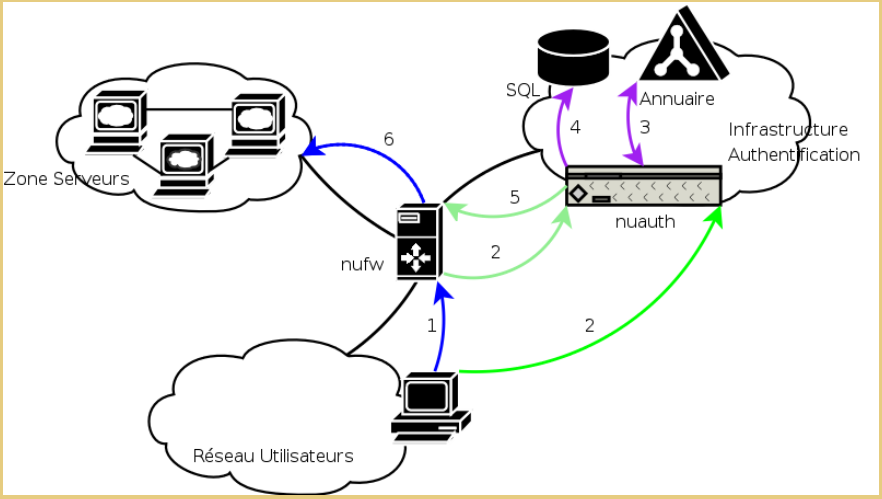
Architecture de NuFW



Architecture de NuFW



Architecture de NuFW



NuFW implémente

- Authentification de chaque connexion a posteriori
  dont les principes sont discutés dans le cadre du projet *Eficaas*
- Une authentification sûre pour chaque connexion
- Un suivi dans les journaux, avec suivi d'état et utilisateur associé à chaque connexion
- Transparence complète au niveau de la topologie du réseau (par opposition à un proxy socks)
- Surcouche Netfilter : parefeu classique et authentifiant

NuFW s'interface sur

- LDAP, aussi bien pour les bases d'utilisateurs, que pour les ACLs. méthode recommandée pour les ACLs.
- System pour les utilisateurs : PAM + NSS
- Fichiers plats
- Autres méthodes (DBM, etc.)
- SQL ou syslog pour les journaux

Disponibilité des clients logiciels

- Linux (console et graphique)
- Windows :
  - Client graphique
  - Client en mode service (transparent)
- Autres OS à suivre

NuFW sans client

Un mode sans client, dit "dégradé", fonctionne également :

- Délègue l'authentification à un module externe, adjoint au serveur d'authentification
  Modules disponibles ou en développement : ident, smb
- Les postes de travail n'ont plus besoin de client logiciel
- L'autorité de confiance se retrouve déportée sur le client lui-même

NuFW et systèmes multiutilisateurs

NuFW fait la différence entre les utilisateurs, indépendamment des protocoles utilisés, même si plusieurs d'entre eux sont connectés sur une même station simultanément. Par exemple, l'un pourra envoyer des mails par SMTP, un autre pas.

Journalisation

- L'équivalent du *conntrack* de Netfilter, en SQL
- Suivi de toutes les connexions, par état, avec en plus la notion d'utilisateur
- L'interface ulog-php permet de suivre et résumer les activités par IP, par utilisateur, etc.

Performances

- Seuls les paquets d'ouverture de connexion sont authentifiés
  - *Aucun* impact sur la bande passante
  - Un délai pour chaque ouverture de connexion
- Nos essais, réalisés dans un schéma proche du DoS, montrent que les délais d'ouverture de connexion restent dans la même échelle de temps que sans NuFW.
- Depuis la branche 0.9, NuFW intègre une cache qui optimise les requêtes d'ACLs.

NuFW : surveillance des systèmes

- Un démon $\Longleftrightarrow$ un utilisateur système
- NuFW différencie donc le trafic venant de différents démons, et peut remonter des alarmes.

NuFW : filtrage par OS ou application

- Le client remonte à NuFW les informations sur l'OS et l'application, leurs versions, le hash SHA1 du binaire.
- Les ACLs peuvent incorporer ces informations
- *attention*: la confiance en ce qui concerne ces informations reste au niveau de la machine cliente.

NuFW : QoS et routage par utilisateur

- Chaque paquet peut être marqué par l'identifiant de son utilisateur
- Qualité de service par utilisateur
- Politique de routage différenciée

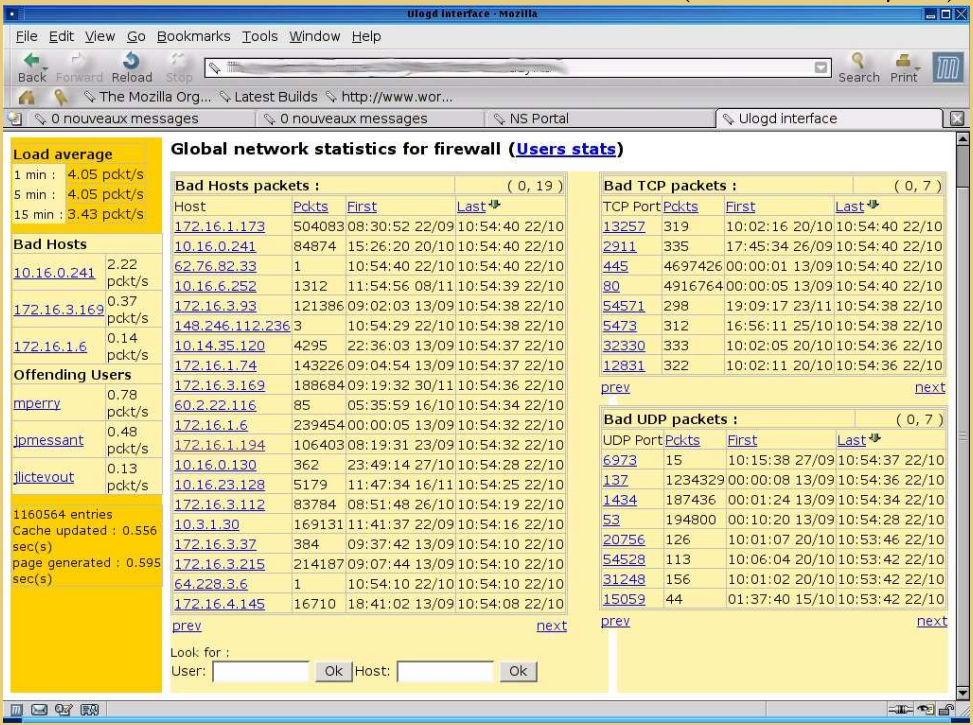
Et ce

- Sur machine multiutilisateur
- Pour les utilisateurs connectés à plusieurs points en même temps

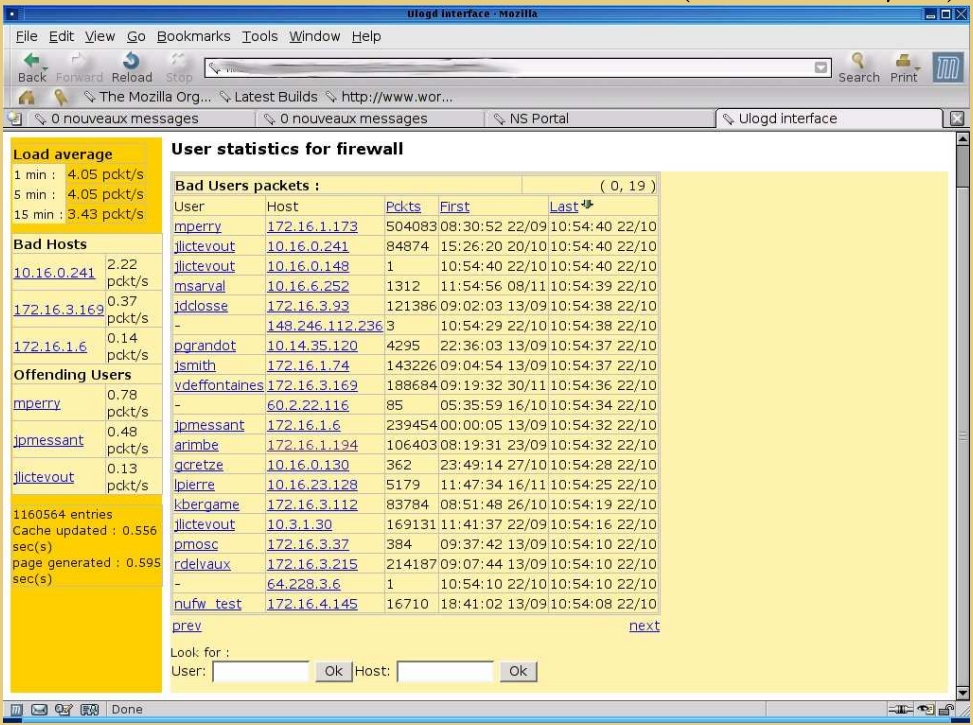
NuFW : Suivi de l'activité réseau

- Tous les événements de la vie d'une connexion sont journalisés
- Les informations sont facilement extractibles
- Durée des connexions, tentatives infructueuses, grand nombre de connexions

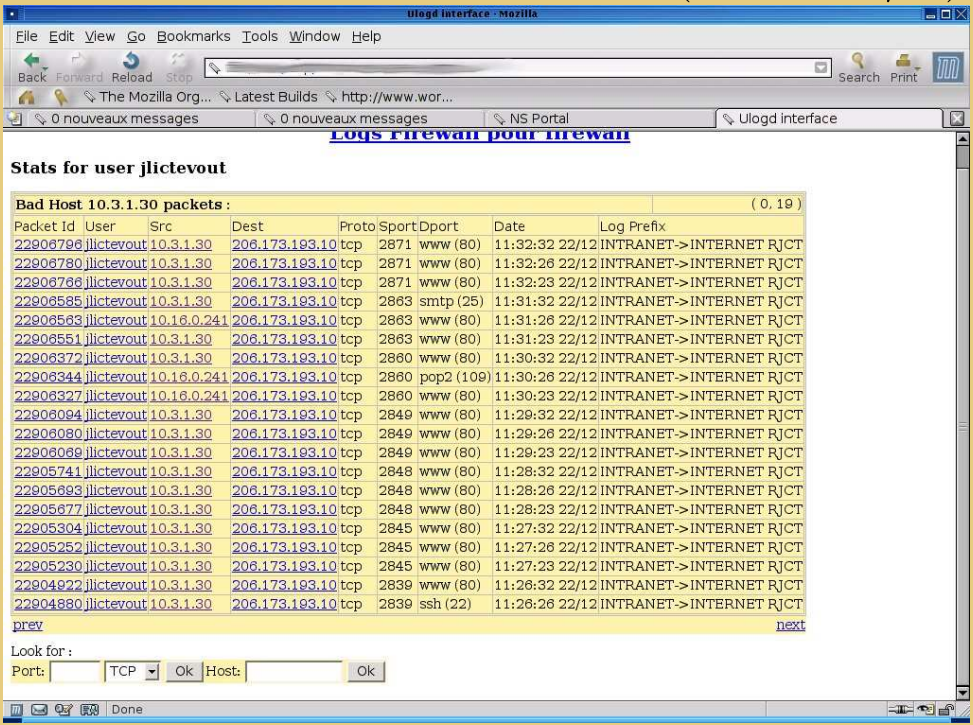
Suivi de l'activité réseau (écran 1/3)



Suivi de l'activité réseau (écran 2/3)



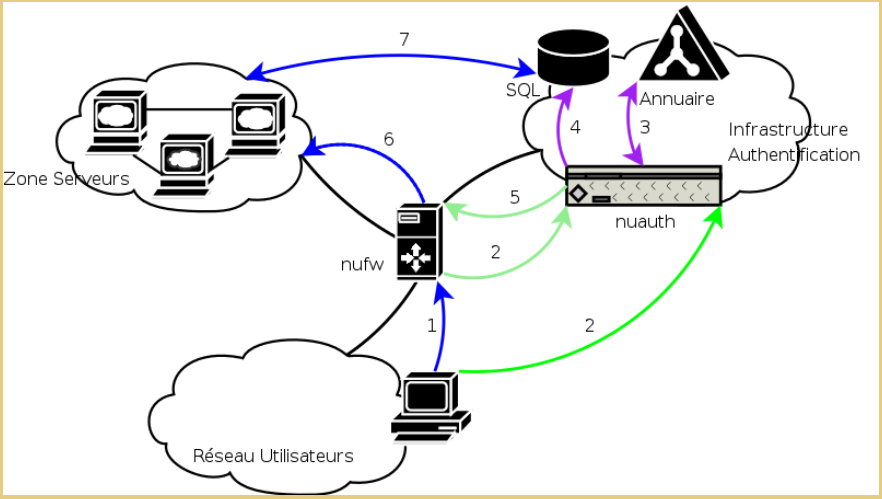
Suivi de l'activité réseau (écran 3/3)



NuFW : Authentification Unique (SSO)

- Le serveur n'a qu'une requête SQL à faire pour trouver de manière sûre l'utilisateur à la source d'une connexion
- Single Sign On totalement indépendant du protocole.
- A ce jour, deux modules sont développés : un module Apache (1.3 ou 2.0), et un module pour Squid.

Authentification Unique - Architecture



Quelques applications pratiques

- NuFW en soi permet une implémentation rigoureuse de la politique de sécurité
- Sécurité des réseaux sans-fils
- Surveillance d'un parc de serveurs
- Ainsi que toutes les étendues du SSO...

Conclusion

- Algorithme d'authentification strict
- Code développé par

- Logiciel Libre innovant