

Page d'accueil

Page de Titre

Sommaire



Page 1 de 36

Retour

Full Screen

Fermer

Quitter

Introduction à NuFW

Vincent Deffontaines

Eric Leblond

INL

April 12, 2005

Page d'accueil

Page de Titre

Sommaire



Page 2 de 36

Retour

Full Screen

Fermer

Quitter

NuFW

- Now User Filtering Works
- Not a Usermode FireWall

Page d'accueil

Page de Titre

Sommaire



Page 3 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 4 de 36

Retour

Full Screen

Fermer

Quitter

Historique du projet

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

Page d'accueil

Page de Titre

Sommaire



Page 5 de 36

Retour

Full Screen

Fermer

Quitter

Historique des filtres IP

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

Page d'accueil

Page de Titre

Sommaire



Page 6 de 36

Retour

Full Screen

Fermer

Quitter

Les pistes nouvelles

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

Page d'accueil

Page de Titre

Sommaire



Page 7 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 9 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 10 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 12 de 36

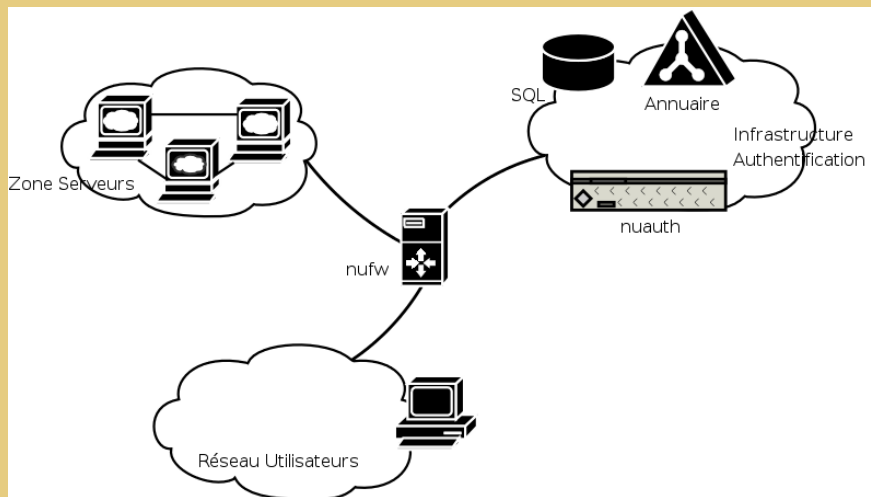
Retour

Full Screen

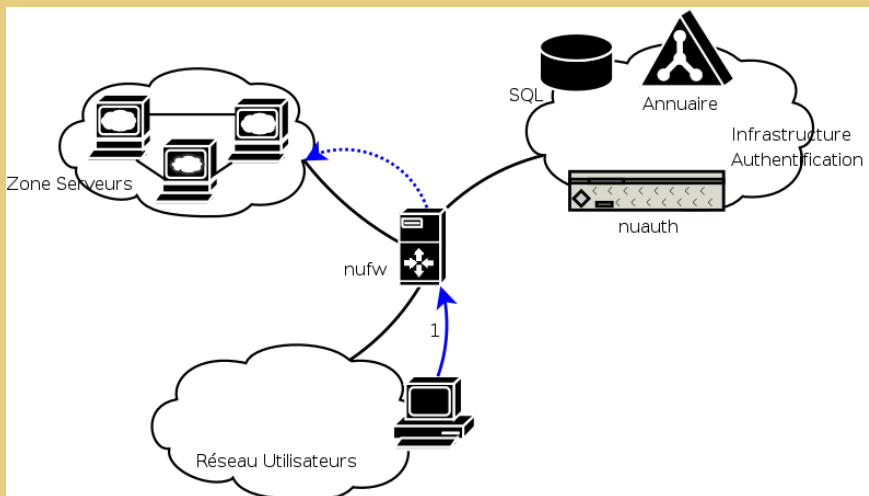
Fermer

Quitter

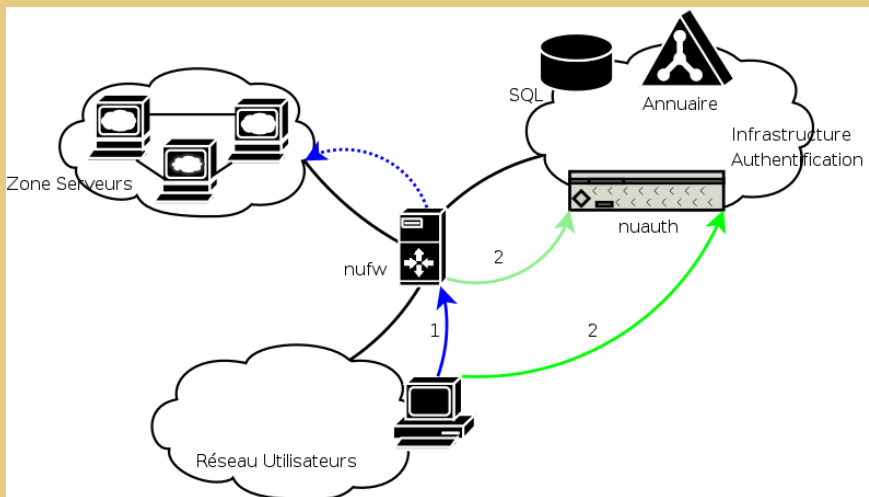
Architecture de NuFW



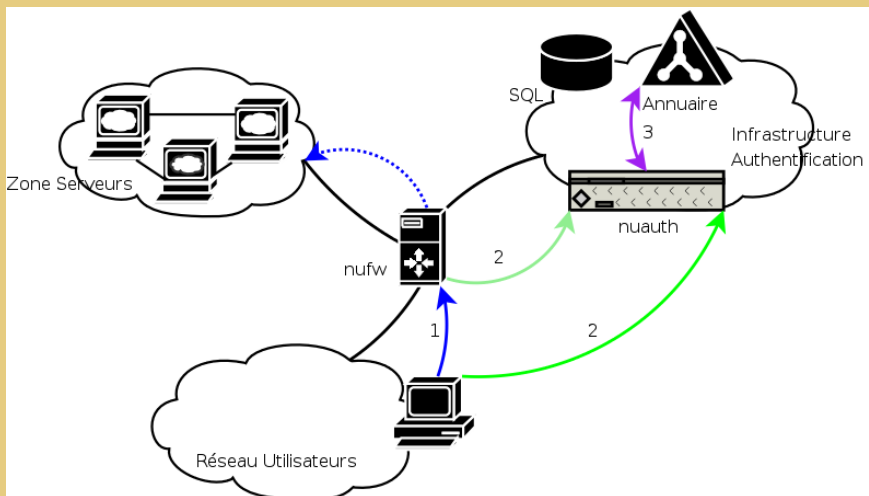
Architecture de NuFW



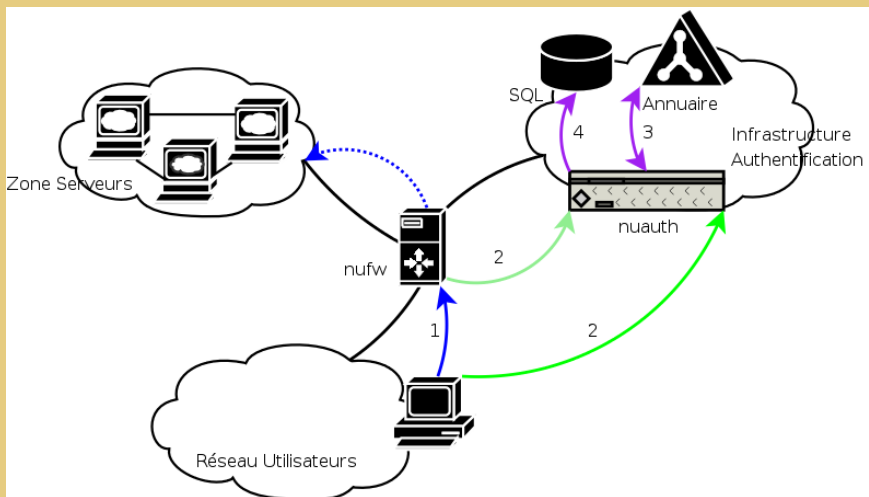
Architecture de NuFW



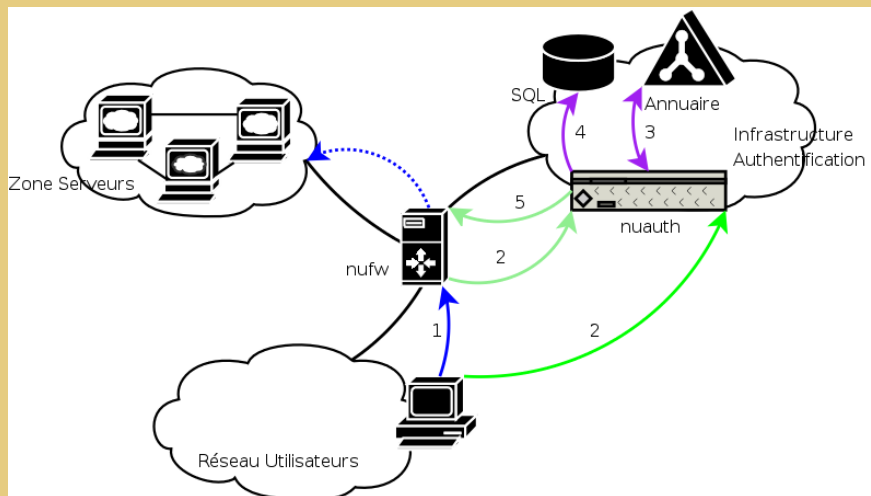
Architecture de NuFW



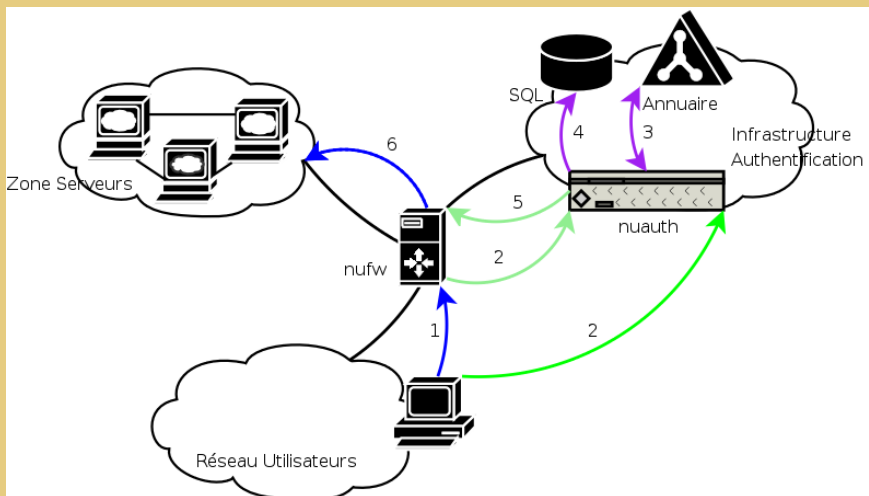
Architecture de NuFW



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

Page d'accueil

Page de Titre

Sommaire



Page 20 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 21 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 23 de 36

Retour

Full Screen

Fermer

Quitter

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.

Page d'accueil

Page de Titre

Sommaire



Page 24 de 36

Retour

Full Screen

Fermer

Quitter

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.

Page d'accueil

Page de Titre

Sommaire



Page 26 de 36

Retour

Full Screen

Fermer

Quitter

NuFW : surveillance des systèmes

- Un démon \iff 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

Page d'accueil

Page de Titre

Sommaire



Page 29 de 36

Retour

Full Screen

Fermer

Quitter

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

Page d'accueil

Page de Titre

Sommaire



Page 30 de 36

Retour

Full Screen

Fermer

Quitter

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

Ulogd interface - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop

The Mozilla Org... Latest Builds http://www.wor...

0 nouveaux messages 0 nouveaux messages NS Portal Ulogd interface

Global network statistics for firewall (Users stats)

Load average (0, 7)

1 min : 4.05 pkt/s
5 min : 4.05 pkt/s
15 min : 3.43 pkt/s

Bad Hosts packets :

Host	Pkts	First	Last
172.16.1.173	504083	08:30:52 22/09	10:54:40 22/10
10.16.0.241	84874	15:26:20 20/10	10:54:40 22/10
62.76.82.33	1	10:54:40 22/10	10:54:40 22/10
10.16.6.252	1312	11:54:56 08/11	10:54:39 22/10
172.16.3.93	121386	09:02:03 13/09	10:54:38 22/10
148.246.112.236	3	10:54:29 22/10	10:54:38 22/10
10.14.35.120	4295	22:36:03 13/09	10:54:37 22/10
172.16.1.74	143226	09:04:54 13/09	10:54:37 22/10
172.16.3.169	188684	09:19:32 30/11	10:54:36 22/10
60.2.22.116	85	05:35:59 16/10	10:54:34 22/10
172.16.1.6	239454	00:00:05 13/09	10:54:32 22/10
172.16.1.194	106403	08:19:31 23/09	10:54:32 22/10
10.16.0.130	362	23:49:14 27/10	10:54:28 22/10
10.16.23.128	5179	11:47:34 16/11	10:54:25 22/10
172.16.3.112	83784	08:51:48 26/10	10:54:19 22/10
10.3.1.30	169131	11:41:37 22/09	10:54:16 22/10
172.16.3.37	384	09:37:42 13/09	10:54:10 22/10
172.16.3.215	214187	09:07:44 13/09	10:54:10 22/10
64.228.3.6	1	10:54:10 22/10	10:54:10 22/10
172.16.4.145	16710	18:41:02 13/09	10:54:08 22/10

[prev](#) [next](#)

Bad TCP packets :

TCP Port	Pkts	First	Last
13257	319	10:02:16 20/10	10:54:40 22/10
2911	335	17:45:34 26/09	10:54:40 22/10
445	4697426	00:00:01 13/09	10:54:40 22/10
80	4916764	00:00:05 13/09	10:54:40 22/10
54571	298	19:09:17 23/11	10:54:38 22/10
5473	312	16:56:11 25/10	10:54:38 22/10
32330	333	10:02:05 20/10	10:54:36 22/10
12831	322	10:02:11 20/10	10:54:36 22/10

[prev](#) [next](#)

Bad UDP packets :

UDP Port	Pkts	First	Last
6973	15	10:15:38 27/09	10:54:37 22/10
137	1234329	00:00:08 13/09	10:54:36 22/10
1434	187436	00:01:24 13/09	10:54:34 22/10
53	194800	00:10:20 13/09	10:54:28 22/10
20756	126	10:01:07 20/10	10:53:46 22/10
54528	113	10:06:04 20/10	10:53:42 22/10
31248	156	10:01:02 20/10	10:53:42 22/10
15059	44	10:13:40 15/10	10:53:42 22/10

[prev](#) [next](#)

Offending Users

mperry 0.78 pkt/s
jpmessant 0.48 pkt/s
jlictevout 0.13 pkt/s

1160564 entries
Cache updated : 0.556 sec(s)
page generated : 0.595 sec(s)

Look for : Host:

Page d'accueil

Page de Titre

Sommaire



Page 31 de 36

Retour

Full Screen

Fermer

Quitter

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

Load average
1 min : 4.05 pkt/s
5 min : 4.05 pkt/s
15 min : 3.43 pkt/s

Bad Hosts

10.16.0.241	2.22 pkt/s
172.16.3.169	0.37 pkt/s
172.16.1.6	0.14 pkt/s

Offending Users

mperry	0.78 pkt/s
jpmessant	0.48 pkt/s
jlictevout	0.13 pkt/s

1160564 entries
Cache updated : 0.556
sec(s)
page generated : 0.595
sec(s)

User statistics for firewall

Bad Users packets : (0, 19)

User	Host	Pkts	First	Last
mperry	172.16.1.173	504083	08:30:52 22/09	10:54:40 22/10
jlictevout	10.16.0.241	84874	15:26:20 20/10	10:54:40 22/10
jlictevout	10.16.0.148	1	10:54:40 22/10	10:54:40 22/10
msarval	10.16.6.252	1312	11:54:56 08/11	10:54:39 22/10
jdclosse	172.16.3.93	121386	09:02:03 13/09	10:54:38 22/10
-	148.246.112.236	3	10:54:29 22/10	10:54:38 22/10
pgrandot	10.14.35.120	4295	22:36:03 13/09	10:54:37 22/10
jsmith	172.16.1.74	143226	09:04:54 13/09	10:54:37 22/10
vdeffontaines	172.16.3.169	188684	09:19:32 30/11	10:54:36 22/10
-	60.2.22.116	85	05:35:59 16/10	10:54:34 22/10
jpmessant	172.16.1.6	239454	00:00:05 13/09	10:54:32 22/10
arimbe	172.16.1.194	106403	08:19:31 23/09	10:54:32 22/10
gcretze	10.16.0.130	362	23:49:14 27/10	10:54:28 22/10
lpierre	10.16.23.128	5179	11:47:34 16/11	10:54:25 22/10
kbergame	172.16.3.112	83784	08:51:48 26/10	10:54:19 22/10
jlictevout	10.3.1.30	169131	11:41:37 22/09	10:54:16 22/10
pmosc	172.16.3.37	384	09:37:42 13/09	10:54:10 22/10
rdelvaux	172.16.3.215	214187	09:07:44 13/09	10:54:10 22/10
-	64.228.3.6	1	10:54:10 22/10	10:54:10 22/10
nufw_test	172.16.4.145	16710	18:41:02 13/09	10:54:08 22/10

[prev](#) [next](#)

Look for : Host:

User:

Page d'accueil

Page de Titre

Sommaire

Page 32 de 36

Retour

Full Screen

Fermer

Quitter

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

Ulogd interface - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop

The Mozilla Org... Latest Builds http://www.wor...

0 nouveaux messages 0 nouveaux messages NS Portal Ulogd interface

Loqs Firewall pour firewan

Stats for user jlictevout

Bad Host 10.3.1.30 packets : (0, 19)

Packet Id	User	Src	Dest	Proto	Sport	Dport	Date	Log Prefix
22906796	jlictevout	10.3.1.30	206.173.193.10	tcp	2871	www (80)	11:32:32 22/12	INTRANET->INTERNET RJCT
22906780	jlictevout	10.3.1.30	206.173.193.10	tcp	2871	www (80)	11:32:26 22/12	INTRANET->INTERNET RJCT
22906768	jlictevout	10.3.1.30	206.173.193.10	tcp	2871	www (80)	11:32:23 22/12	INTRANET->INTERNET RJCT
22906585	jlictevout	10.3.1.30	206.173.193.10	tcp	2863	smtp (25)	11:31:32 22/12	INTRANET->INTERNET RJCT
22906563	jlictevout	10.16.0.241	206.173.193.10	tcp	2863	www (80)	11:31:26 22/12	INTRANET->INTERNET RJCT
22906551	jlictevout	10.3.1.30	206.173.193.10	tcp	2863	www (80)	11:31:23 22/12	INTRANET->INTERNET RJCT
22906372	jlictevout	10.3.1.30	206.173.193.10	tcp	2860	www (80)	11:30:32 22/12	INTRANET->INTERNET RJCT
22906344	jlictevout	10.16.0.241	206.173.193.10	tcp	2860	pop2 (109)	11:30:26 22/12	INTRANET->INTERNET RJCT
22906327	jlictevout	10.16.0.241	206.173.193.10	tcp	2860	www (80)	11:30:23 22/12	INTRANET->INTERNET RJCT
22906094	jlictevout	10.3.1.30	206.173.193.10	tcp	2849	www (80)	11:29:32 22/12	INTRANET->INTERNET RJCT
22906080	jlictevout	10.3.1.30	206.173.193.10	tcp	2849	www (80)	11:29:26 22/12	INTRANET->INTERNET RJCT
22906069	jlictevout	10.3.1.30	206.173.193.10	tcp	2849	www (80)	11:29:23 22/12	INTRANET->INTERNET RJCT
22905741	jlictevout	10.3.1.30	206.173.193.10	tcp	2848	www (80)	11:28:32 22/12	INTRANET->INTERNET RJCT
22905693	jlictevout	10.3.1.30	206.173.193.10	tcp	2848	www (80)	11:28:26 22/12	INTRANET->INTERNET RJCT
22905677	jlictevout	10.3.1.30	206.173.193.10	tcp	2848	www (80)	11:28:23 22/12	INTRANET->INTERNET RJCT
22905304	jlictevout	10.3.1.30	206.173.193.10	tcp	2845	www (80)	11:27:32 22/12	INTRANET->INTERNET RJCT
22905252	jlictevout	10.3.1.30	206.173.193.10	tcp	2845	www (80)	11:27:26 22/12	INTRANET->INTERNET RJCT
22905230	jlictevout	10.3.1.30	206.173.193.10	tcp	2845	www (80)	11:27:23 22/12	INTRANET->INTERNET RJCT
22904922	jlictevout	10.3.1.30	206.173.193.10	tcp	2839	www (80)	11:26:32 22/12	INTRANET->INTERNET RJCT
22904880	jlictevout	10.3.1.30	206.173.193.10	tcp	2839	ssh (22)	11:26:26 22/12	INTRANET->INTERNET RJCT

[prev](#) [next](#)

Look for:

Port: TCP Host:

Done

Page d'accueil

Page de Titre

Sommaire



Page 33 de 36

Retour

Full Screen

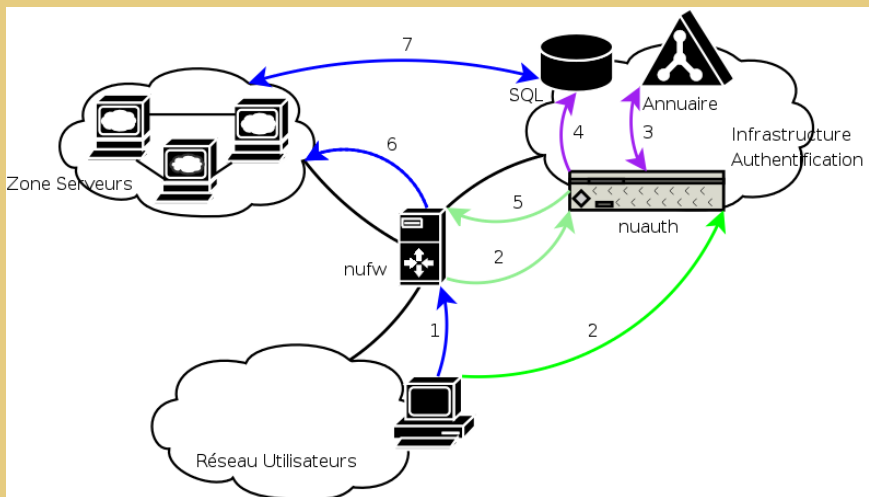
Fermer

Quitter

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



Page d'accueil

Page de Titre

Sommaire



Page 35 de 36

Retour

Full Screen

Fermer

Quitter

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...

Page d'accueil

Page de Titre

Sommaire



Page 36 de 36

Retour

Full Screen

Fermer

Quitter

Conclusion

- Algorithme d'authentification strict
- Code développé par



- Logiciel Libre innovant