Projet tuteuré

UFWI

Simon BAROTTE, Valentin FROLICH, Cyril PIERRÉ,
Maxime ROBIN

27 mars 2012

Sommaire

Présentation

Historique

- La première version publique de NuFW par EdenWall est sortie le 01 septembre 2003.
- Le 18 août 2011, liquidation de NuFW et reprise du projet par la communauté (Ufwi).

Présentation

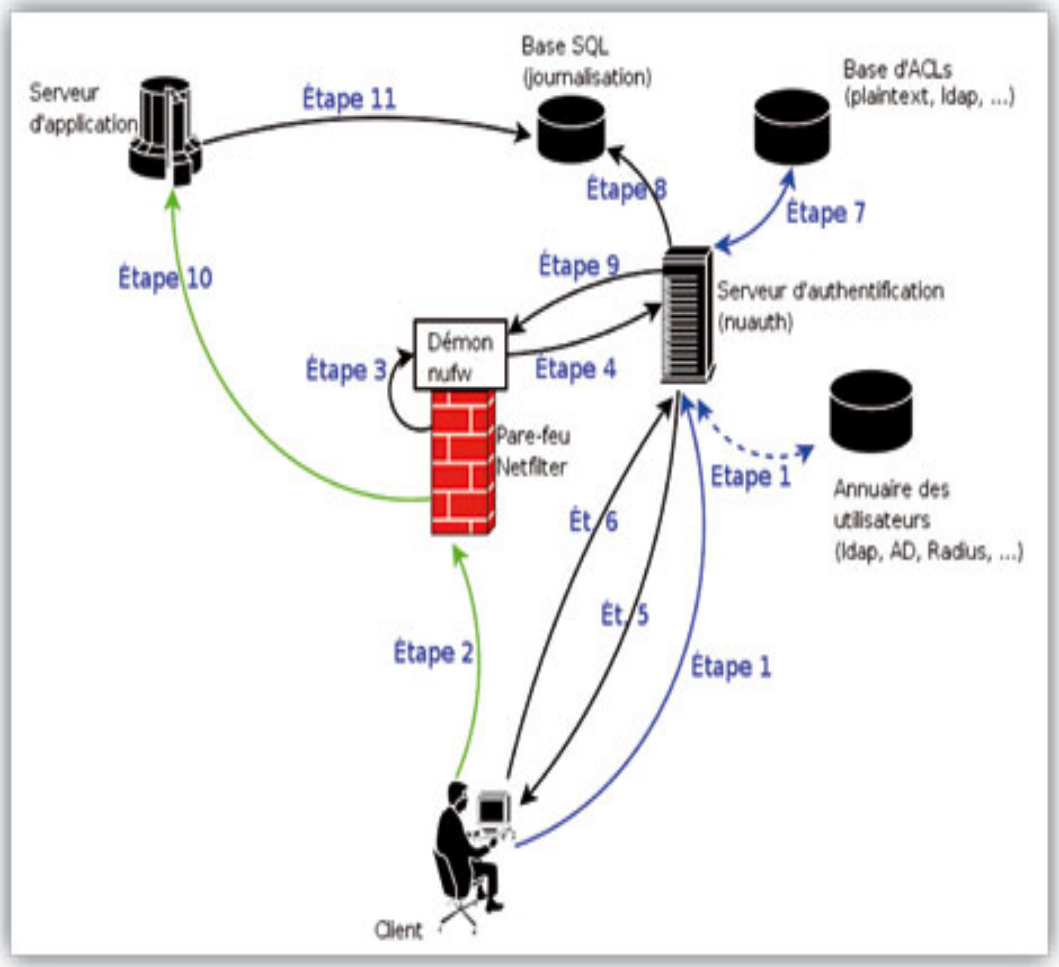
Historique

- La première version publique de NuFW par EdenWall est sortie le 01 septembre 2003.
- Le 18 août 2011, liquidation de NuFW et reprise du projet par la communauté (Ufwi).

Présentation

- Surveillance de l'activité réseau des serveurs.
- Paquets signés.
- Module de surveillance (logs).
- Identifier les utilisateurs par une authentification unique.

Algorithme


Serveur d'application
Étape 11
Base SQL (journalisation)
Base d'ACLs (plaintext, ldap, ...)
Étape 8
Étape 7
Étape 10
Étape 9
Serveur d'authentification (nuauth)
Démon nufw
Étape 3
Étape 4
Pare-feu Netfilter
Étape 1
Annuaire des utilisateurs (ldap, AD, Radius, ...)
Ét 6
Ét 5
Étape 2
Étape 1
Client

Modules

- Authentification
- Filtred
- Rcpd
- Client

Authentification

Présentation

- Daemon principale
- Gère toutes les authentifications

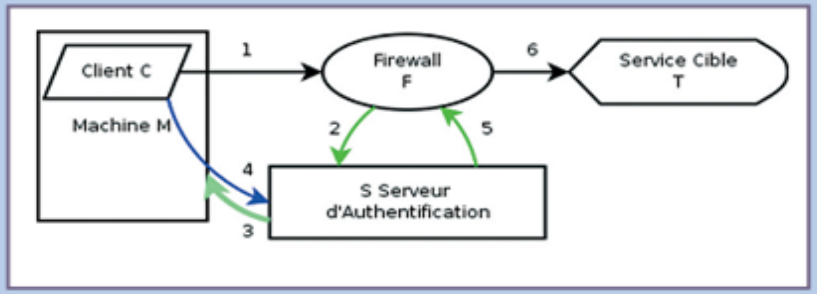
Configuration

- Module ldap, plaintext
- Journalisation des connexions
- Certificats

- Fonctionnement de l'authentification

Authentification

Algorithme d'authentification de paquet



1. L'application du client C émet un paquet P.
2. Le pare-feu intercepte le paquet et envoie une demande de décision au serveur d'authentification S.
3. S envoie une demande de mise à jour aux clients logiciels en activité sur la machine M.
4. Le logiciel du client C envoie une authentification pour P.
5. S combine les données provenant de C et du pare-feu et envoie sa décision au pare-feu.
6. Le pare-feu bloque ou transmet le paquet suivant la décision communiquée par S.

NuFW propose également d'autres méthodes, notamment un algorithme n'utilisant pas l'étape 3. L'étape 4 est dans ce cas réalisée par une vérification régulière par le client de l'activité réseau sur le système.

Filtred

- Présentation

Fonctionnalités

- Filtre le trafic
- Module de surveillance
- Contribue à la surveillance réseau
- Marque chaque paquet avec un ID unique

- Fichier de configuration

Rcpd

Présentation

- Manager

Types d'authentification

- alwaysok
- alwaysno
- basicdict
- file
- ldap

- Composants et servies
- Tâches planifiées

Client

- Présentation
- Différent client disponnible
- Multi-plateformes

Comparaison

- Différentes solutions de pare feu
  - AuthPF
  - NUFW
  - Cyberoam
  - CheckPoint

Comparaison

- Différentes solutions de pare feu
  - AuthPF
  - NUFW
  - Cyberoam
  - CheckPoint
- Installation, mise en oeuvre
- Modularité
- Sécutité
- Intérêts

Problèmes et Conclusion

- Problèmes lors de l'installation
- Problèmes de configuration
- Conclusion

Problèmes lors de l'installation

- Problèmes de dépendances
- Problèmes d'obsolèscence
- Problème dans le code
- Peu de documentation

Problèmes de configuration

- Problèmes de librairies
- Problèmes de certificats

Conclusion

- Projet Libre
- Projet ayant sa place dans la sécurité des entreprises
- Logiciels modulables et multi-plateformes
- Des lacunes