



EdenWall
Technologies



NuFirewall

Open-source authenticating firewall

Who's that guy ?

- Eric Leblond
 -
 - CTO EdenWall Technologies
 - NuFW project leader
 - Netfilter developer
 - Ulogd2 maintener
- Regit
 - <http://home.regit.org/>
 - @Regiteric on twitter
- French
 - activate your babelfish to deal with my accent

Discovering NuFirewall

- NuFirewall at a glance
- Functionalities
- NuFW at another glance
- Architecture
- Demonstration
- Planned evolution

What is NuFirewall ?

- A ready-to-use Linux firewall gateway
 - Standard Netfilter firewall
 - Authentication via NuFW
 - Fully manageable through a graphical GUI
- A free distribution
 - Based on debian Lenny
 - Configuration via a QT-based GUI
- A free version of EdenWall appliance
 - Software
 - Free

Functionalities

- System and network configuration
- Firewalling
 - Netfilter configuration
 - NuFW setup and configuration
- Directory handling
 - LDAP (posix)
 - Active Directory
- Logs analysis
- Ipsec VPN

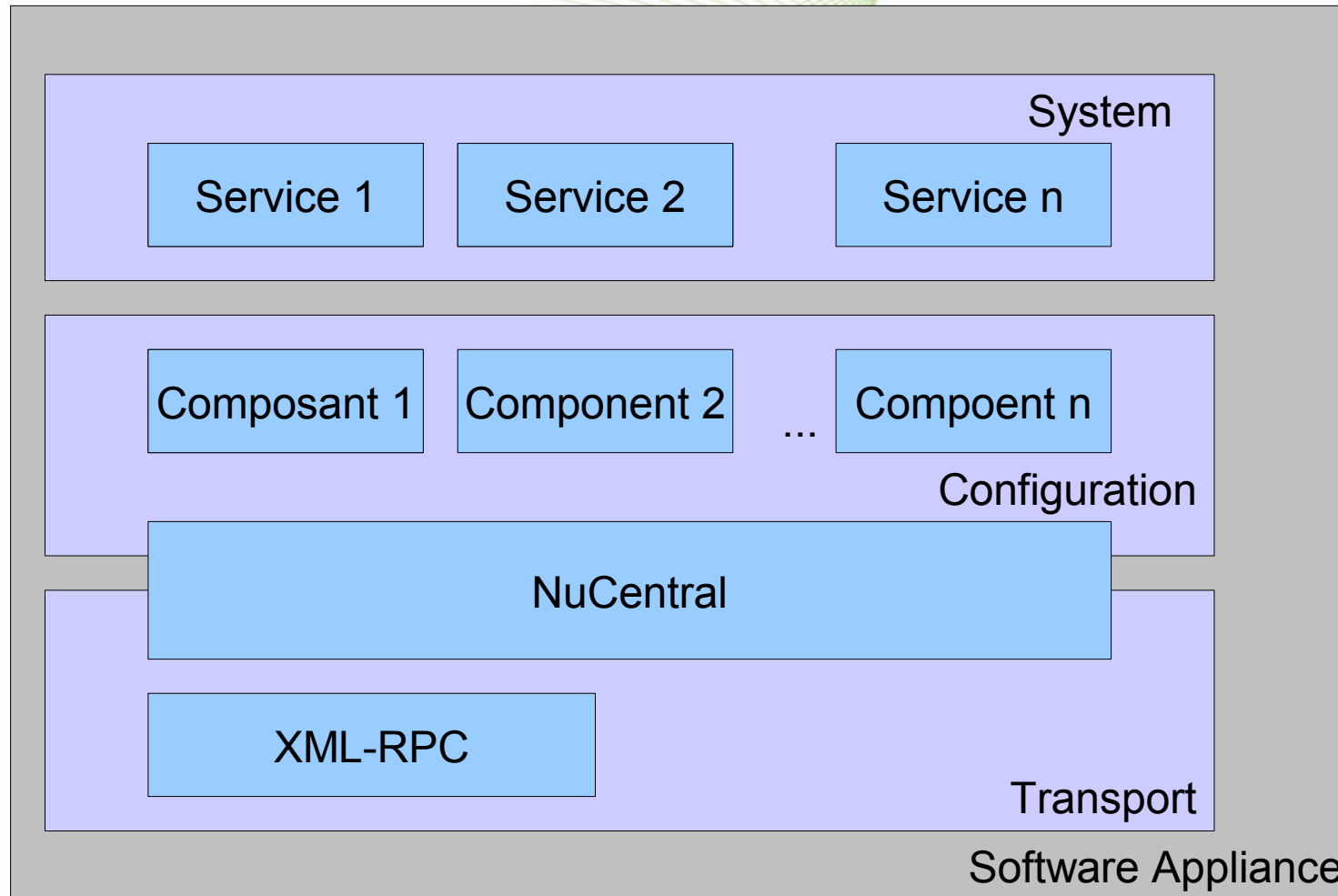
NuFW

- Bring identity to the network
 - Filtering rules with group match
 - Ability to do QoS and differentiated routing (via marks)
- « exclusive » algorithm
 - authentication on multi-users computer
 - Resist to basic attack (IP and arp spoofing)
- Développé by EdenWall Technologies
- Available under GPLv3 licence

Software architecture (1/2)

- Heavy client configuration
 - Python-QT GUI
 - Communication with firewall via XML-RPC over HTTPS
- Server Architecture
 - Server developed in python twisted
 - Core
 - Common functions
 - Transport
 - Components
 - Responsible of a function (network, filtering)
 - Dependence handling, ...

Software architecture (2/2)



Components of the solution

- NuFirewall
- NuFirewall Administration Suite (NFAS)
 - Same version as EAS
 - But different icons (Nupik inside)
- Authentication Agents
 - Nutcpc : Console client for Linux and Unix
 - Nuapplet : Graphical Client written in QT
 - NuAgent : Windows Agent (freely available but proprietary)
 - EdenWall Agent : extended version of NuAgent
- Documentation



System configuration

The screenshot displays the NuFirewall Administration Suite interface. The main window is titled "Système - admin@192.168.1.1 - NuFirewall administration suite". The interface includes a menu bar (Fichier, Audit, Aide), a navigation pane (Résumé, Système, Services, Gestion des utilisateurs de EAS, Pare-feu, Logs, PKI), and a main content area titled "Configuration du réseau".

The "Configuration du réseau" section shows two network interfaces:

- eth0**: Type d'interface Ethernet, Libellé du serveur eth0. IP address: 10.0.2.0/24 (10.0.2.15/24).
- eth1**: Type d'interface Ethernet, Libellé du serveur eth1. IP address: 192.168.1.0/24 (192.168.1.1/24).

An "Éditeur de réseau" (Network Editor) dialog is open, allowing configuration for the selected interface (eth0). The dialog includes the following fields:

- Interface physique: eth0
- Adresse réseau: 192.168.40.0/24
- Adresses IP sur ce réseau: (Empty list)
- Libellé du réseau: network label

The dialog also displays an "Erreur d'entrée" (Input Error) section with a warning icon and the following messages:

- Réseau correct
- Veuillez indiquer au moins une adresse IP

The dialog has "Terminer" and "Annuler" buttons. The main interface also shows a "Modules" list on the left and a log of system events at the bottom.

System configuration

- Network
 - Ethernet Interface
 - Vlan
 - Bonding
 - Routed network
- Authentication
 - Kerberos, kerberos/AD, password, radius, certificat
- Groups
 - LDAP, AD

NuPKI, PKI made simple

The screenshot shows the NuPKI administration interface. The main window displays a list of certificates under the 'Client' tab. The table below shows the data for the certificates:

Common Name	Courriel	Société	Division	Lieu	Département	Pays	État
Eric Leblond	eleblond@nufw.org	Nupik Inc.	Trolls	Pic du midi	Spicy	FR	Corrects
Nupik	nupik@nufw.org	Nupik Inc.	Trolls	Pic du midi	Spicy	FR	Corrects

A dialog box titled 'Créer un certificat' is open, showing the following fields:

- Le Common Name (CN) est le nom unique utilisé pour identifier votre certificat
- Common Name: [Empty text box]
- Courriel: [Empty text box]
- Type de certificat: client (dropdown menu)
- Date d'expiration: mercredi 6 juillet 2011 (dropdown menu)

Buttons at the bottom of the dialog: < Précédent, Suivant >, Annuler.

Firewall rules management

Rulesets Save Save As Ferret Undo Redo Test Ruleset Apply Ruleset

Object Library

Networks

Protocols

Filter: Clear

- ▲ Groupes
- DNS
- IPP
- Websurf
- ▲ Layer 3
- Any IPv4
- ▲ ICMP
- Any ICMP
- ICMP ping
- ICMP pong
- ▲ IGMP
- IGMP
- ▲ TCP
- Any TCP
- Appli compta
- DNS (tcp)
- FTP
- HTTP
- HTTPS
- IMAP
- IMAPS
- IPP (tcp)
- IRC
- LDAP
- MySQL

+ Create Create Group

Modifier Supprimer

User Groups

Applications

Operating Systems

Periodicities

Durations

IPv4 rules IPv6 rules NAT

Filters: Exact Match

	Utilisateur	Source	Decision	Destination	Advanced	Comment
< eth0 → eth2 > (default: DROP)						
1		Internet IPv4	FTP HTTP HTTPS	Web Server		Accès vers le serveur web
2		Internet IPv4	SMTP	Mail Server		Accès vers le serveur mail
3	admins		IMAPS	Mail Server		
< eth0 → eth3 > (default: DROP)						
1	Comptabilité Direction	Internet IPv4	HTTP HTTPS	Compta Server		Accès aux informations financières
< eth1 → eth0 > (default: DROP)						
1	Direction	LAN	IMAPS	Internet IPv4		
2	Users	LAN	Websurf	Internet IPv4		
3	Users	LAN	bzflag	Internet IPv4		
< eth1 → eth2 > (default: DROP)						
1	Users	LAN	IMAPS	Mail Server		
2	Users	LAN	SMTP Websurf	Web Server		
3	Techs	LAN	SSH	DMZ		
4		LAN		Proxy		

+ Create Up Down Edit Clone Delete

Information

FORWARD ACL #19 (IPv4):

Decision: ACCEPT

Chain: FORWARD

Sources: Internet IPv4

Destinations: Compta Server

Protocols: TCP HTTP
TCP HTTPS

User groups: Comptabilité
Direction


Applications: Internet Explorer

Durations: 15 Minutes

Logging: Oui, prefix="compta_"

Interfaces: eth0 → eth3

Comment: Accès aux informations financières



Firewall rules management

- Drag&Drop based interface
- Ipv4 and Ipv6 filtering
 - Netfilter
 - NuFW
- SNAT and DNAT
- Fonctionnalités
 - Coherence tests
 - Display filtering
 - Wizards

Logs analysis

[Résumé](#) | [Système](#) | [Services](#) | [Gestion des administrateurs](#) | [Pare-feu](#) | [Logs](#) | [PKI](#)

[Paramètres](#) | [Restaurer la vue par défaut](#) | [Rechercher](#) | [Imprimer un rapport](#) | [Actualiser](#) | [Mode cumulatif](#) | [Imprimer](#)

Vues

- Tout
 - Vue principale
 - Derniers paquets
 - Connexions actives
 - Logs IDS-IPS
 - Logs du proxy
- Utilisateur
 - Tous les utilisateurs
 - Utilisateurs bloqués
 - Utilisateurs acceptés
- Application
 - Toutes les applications
 - Applications bloquées
 - Applications acceptées
- Hôtes
 - Tous les hôtes
 - Hôtes bloqués
 - Hôtes acceptés
- Rapports
 - Rapport utilisateurs
 - n premiers
- Signets
- Historique
 - Utilisateurs : Utilisateurs pollux

Informations

Applications utilisées :
xulrunner-stub

Statistiques :

- 17421 paquets
- 76 % de : Applications utilisées
- **Dernier paquet:** 12:24:48

Utilisateur : Utilisateur eric

Filters: **Utilisateur eric**

Liste des paquets

	Source	Destination	Protocole	Sport
1	192.168.33.176	ww-in-f147.google.com	tcp	43520
2	192.168.33.176	ww-in-f138.google.com	tcp	57897
3	192.168.33.176	ww-in-f102.google.com	tcp	48134
4	192.168.33.176	ww-in-f138.google.com	tcp	58203
5	192.168.33.176	ww-in-f103.google.com	tcp	43134
6	192.168.33.176	ww-in-f103.google.com	tcp	43135
7	192.168.33.176	fe.api.del.vip.ac4.yahoo.net	tcp	36862

Applications utilisées

IP de destination

	Destination	Paquets	Premier paquet	D
1	fe.feeds.del.vip.ac4.yahoo.net	3788	2009-08-21 17:27:02	12:2
2	fe.api.del.vip.ac4.yahoo.net	2723	2009-08-21 17:18:35	12:2
3	weather.noaa.gov	2433	2009-08-21 19:08:15	12:1
4	hebus.inl.fr	2127	2009-08-21 17:18:50	10:0
5	monde-pub.sdv.fr	1072	2009-08-25 22:57:21	2009
6	sd-6807.dedibox.fr	1023	2009-08-27 10:12:45	2009

Paquets bloqués

Logs analysis

- Firewall log analysis
 - Netfilter (via ulogd2 postgresql and mysql output)
 - NuFW
- Graphical display
 - Bar
 - Pie
 - Table
- Dashboard
- Basic report

Conclusion

- NuFirewall
 - Is a free authenticating firewall
 - Simple and friendly user interface
- Planned evolution
 - 1.0 this summer
 - Some components will be separately available :
 - Nuface : rules management
 - Nulog : log analysis
 - NuPKI : PKI
 - Update to follow EdenWall Appliance

NuFirewall will not evolved without them

- Pierre Chifflier (aka pollux, aka Mr Pare-feu Openoffice)
- Victor Stinner (aka Haypo)
- Feth Arezki, Pierre-Louis Bonicoli, Laurent Defert, Nicolas Frisoni, Kamel Messaoudi, Francois Toussenel
- Olivier Carrere, Julien Miotte
- Harmony Igolen
- ...

Questions ?

- More infos : <http://www.nufw.org/>
- Contact : eleblond@edenwall.com
- EdenWall Technologies : <http://www.edenwall.com/>

The background features a series of thin, light green lines that curve and flow across the page, creating a sense of movement and depth. The lines are most dense in the upper left and lower right corners, tapering off towards the center.

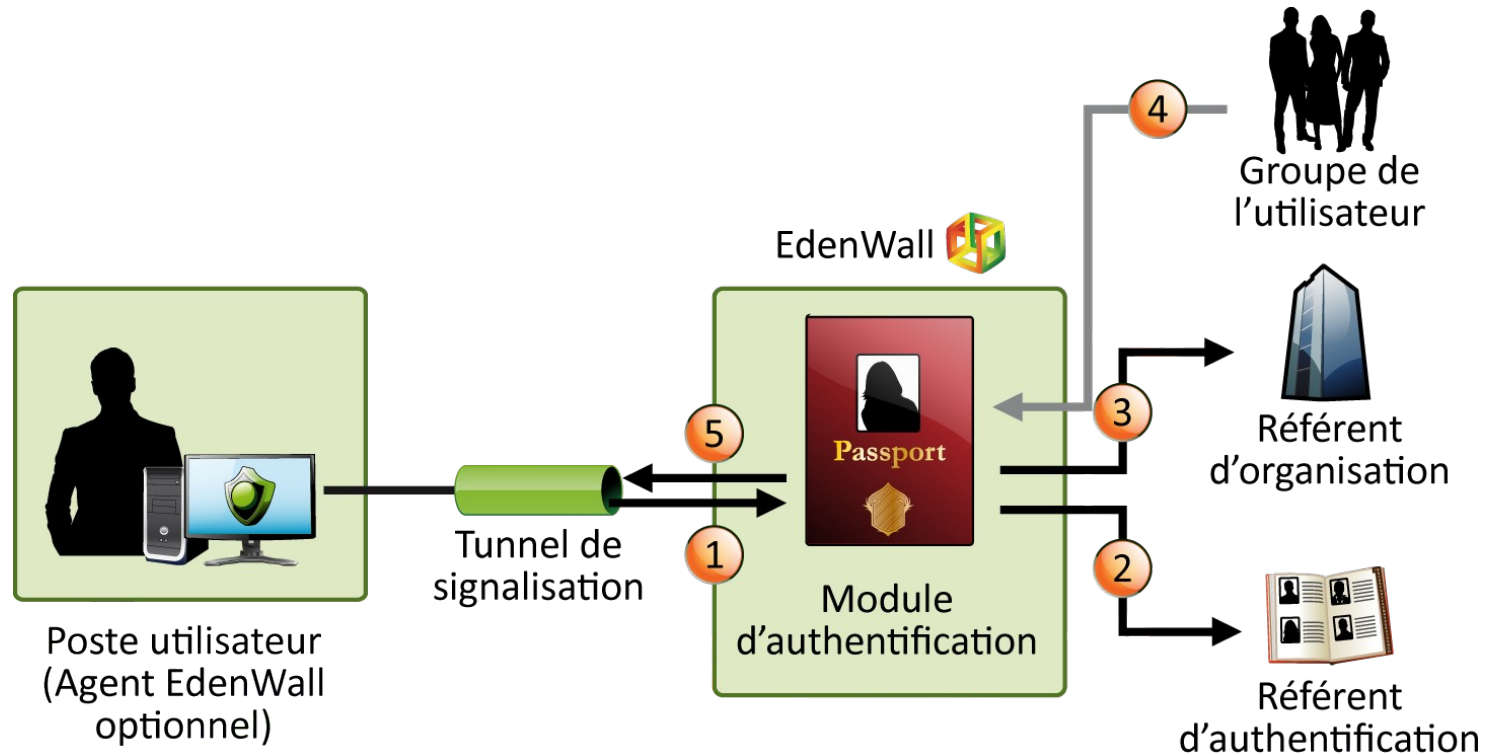
Annexes

NuFW

Algorithmes

Principe de fonctionnement

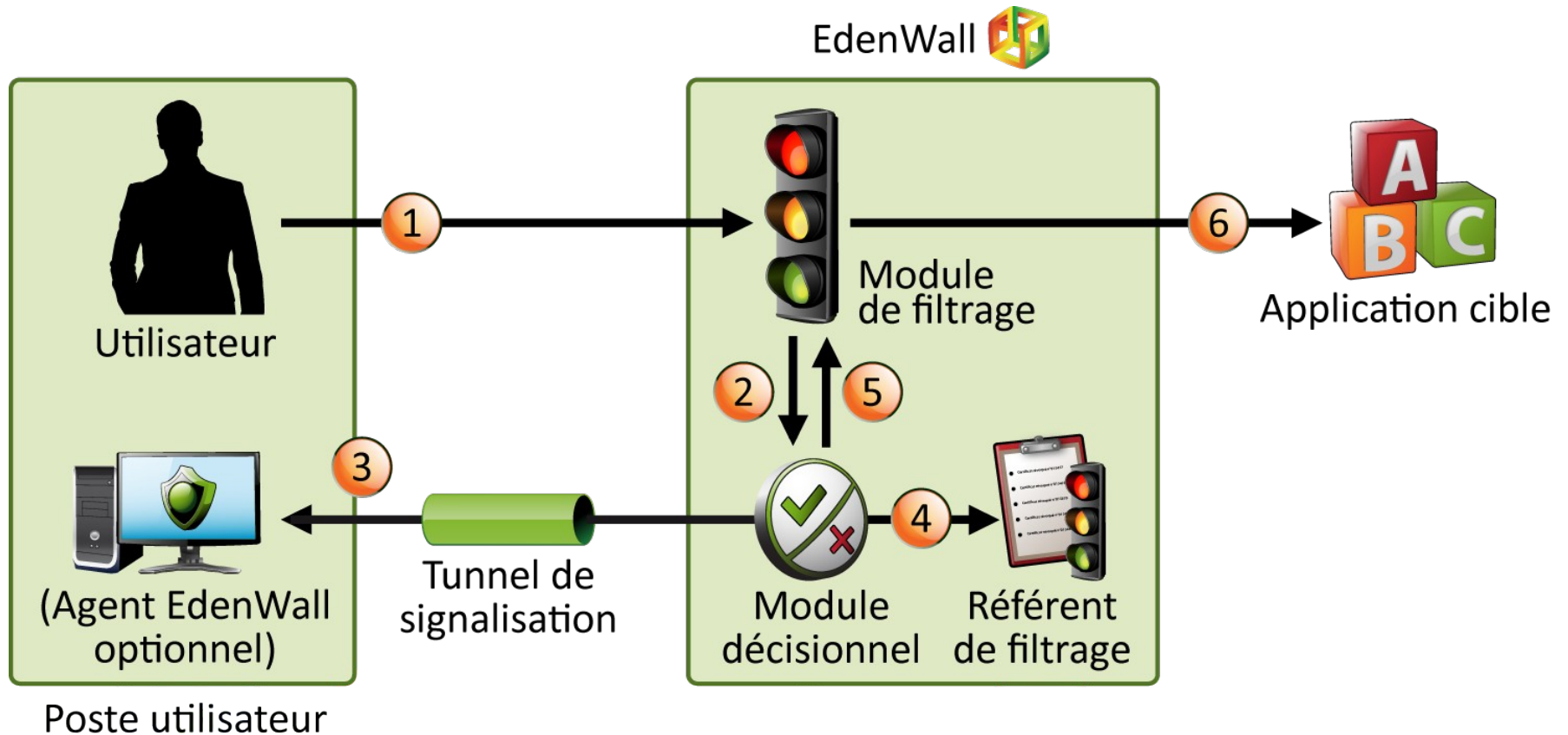
Phase 1: Identification des utilisateurs et groupes associés



1. Ouverture d'un tunnel chiffré de signalisation vers le firewall par l'agent de l'utilisateur
2. Vérification des informations d'identité par le module d'authentification auprès d'un référent d'organisation (LDAP, Radius)
- 3 et 4. Récupération des groupes utilisateurs auprès d'un référent d'organisation (annuaire LDAP)
5. Association entre l'identité de l'utilisateur et ses groupes par le module d'authentification

Principe de fonctionnement

Phase 2: Identification du premier paquet de connexion



❶ Interception du *premier paquet* de connexion par le module de filtrage

❷ à ❸ Analyse par le module décisionnel

- Validation de l'identité de la source
- Validation de l'accès à l'application cible

Differences between EdenWall/NuFirewall

- EdenWall is an hardware solution
- High availability
- Centralised Administration (multi firewall)
- Multi-user administration (profil, external authentication)
- UTM fonctionnalities
- Professional support