



YNOV CAMPUS - RM-IT

# MISE EN PLACE D'UN FIREWALL PFSENSE

OLIER CLÉMENT

2018-2019

MICKAËL RIGONNAUX

# Sommaire

Documentation de la mise en place d'un Firewall PFSense

<b>Introduction</b>	<b>3</b>
<b>Demandes</b>	<b>3</b>
<b>Réalisation</b>	<b>4</b>
Schéma réseau	4
Éléments du réseau	5
Plans d'adressages	5
Alias	5
Regles de Firewall	6
<b>Tests</b>	<b>9</b>

# Firewall PFSense

## Introduction

---

Cette documentation a pour but de présenter la mise en place d'un firewall PFSense installé dans le campus Ynov d'Aix-en-Provence.

Les différents acteurs sont :

- Le campus Ynov d'Aix-en-Provence, école privée accueillant à peu près 600 étudiants représentée par Mr Battistoni Eric. (<https://www.ynov-aix.fr/>)
- La société RM-IT, société de consulting et de prestation en informatique représentée par Mr Rigonnaux Mickael et Mr Olier Clément. (<https://www.rm-it.fr>)

## Demandes

---

La demande était la suivante, mettre en place un nouveau réseau pour le cours de sécurité des systèmes d'information basée sur un Firewall PFSense et sur des machines cliente Ubuntu.

Plus précisément, voici les demandes du Campus Ynov d'Aix :

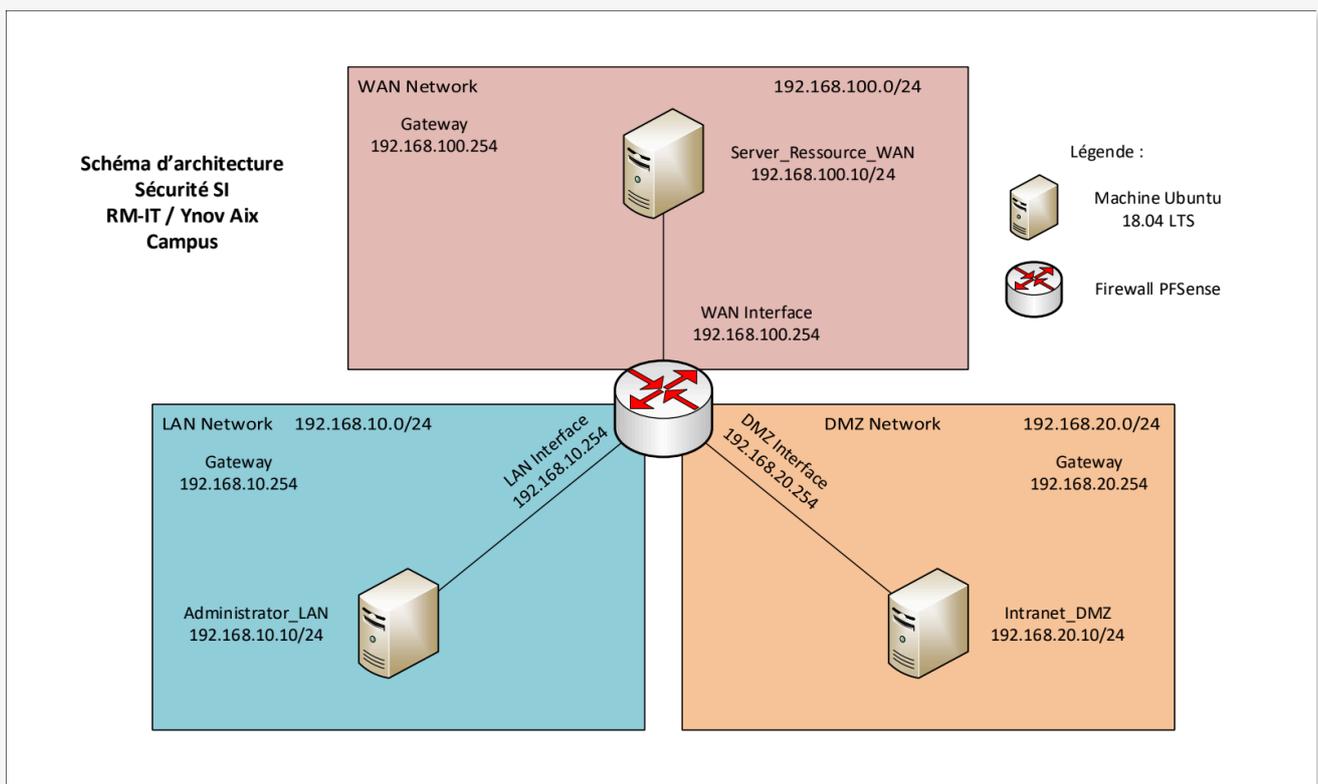
- Créer 3 réseaux (LAN, WAN, DMZ)
- Créer un plan d'architecture avec des plans d'adressages
- Interdire tout ce qui n'est pas explicitement demandé
- Installer une machine d'administration dans le réseau LAN
- Autoriser la machine d'administration à se connecter en SSH et HTTPS sur le Firewall
- Autoriser le réseau LAN vers le WAN seulement pour le protocole ICMP
- Autoriser le LAN à joindre tous les serveurs Web sur les ports 80 et 443
- Autoriser le LAN à faire des résolution DNS
- Installer un serveur dans le réseau DMZ (Intranet/Administration)
- Autoriser le trafic ICMP du réseau LAN vers DMZ
- Autoriser le trafic ICMP du réseau DMZ vers LAN et WAN
- Autoriser le trafic du poste d'Administration positionné dans le LAN vers l'Intranet dans la DMZ sur les ports 443 et 22

- Autoriser la machine intranet de la DMZ à administrer le Firewall sur les ports 22 et 443
- Ajouter un serveur de ressource sur le réseau WAN
- Autoriser la connexion du réseau LAN et WAN sur le serveur de ressource sur le port 443
- Autoriser le poste d'administration du réseau LAN à administrer le serveur de ressource en SSH

## Réalisation

La présente infrastructure est basée sur de la virtualisation avec VMWare Workstation 15, l'ensemble des réseaux sont configurés comme des réseaux privés.

## Schéma réseau



## Eléments du réseau

Nom	Réseau	IP	OS
<b>Administration_LAN</b>	LAN	192.168.10.10/24	Ubuntu 18.04 LTS
<b>Intranet_DMZ</b>	DMZ	192.168.20.10/24	Ubuntu 18.04 LTS
<b>Serveur_Ressource</b>	WAN	192.168.100.10/24	Ubuntu 18.04 LTS
<b>PFSense</b>	Interface 01 LAN Interface 02 WAN Interface 03 DMZ	192.168.10.254/24 192.168.100.254/24 192.168.20.254/24	PFSense 2.4.4

## Plans d'adressages

Voici les plans d'adressage des différents réseaux :

Nom	Adresse Réseau	Masque	Passerelle	DNS
<b>WAN (simulé)</b>	192.168.100.0	255.255.255.0	192.168.100.254	1.1.1.1
<b>LAN</b>	192.168.10.0	255.255.255.0	192.168.10.254	1.1.1.1
<b>DMZ</b>	192.168.20.0	255.255.255.0	192.168.20.254	1.1.1.1

## Alias

Firewall / Aliases / IP

IP Ports URLs All

Name	Values	Description	Actions
Administrator_LAN	192.168.10.10	Poste d'administration du réseau	
Cloud_DNS	1.1.1.1	DNS Cloudflare	
Intranet_DMZ	192.168.20.10	Serveur Intranet de l'entreprise RM-IT	
[REDACTED]	[REDACTED]	[REDACTED]	
Ressource_Server_WAN	192.168.100.10	Serveur de ressource de l'entreprise	

+ Add Import

Pour des raisons de lisibilité de maintenabilité de la plateforme des alias ont été créés. Ils permettent de créer des règles de Firewall en utilisant directement ces alias à la place d'IP ou de LAN directement, ce qui permet d'identifier directement les objets derrière ces noms.

## Règles de Firewall

Afin de répondre aux différentes demandes du Campus Ynov d'Aix-en-Provence plusieurs règles ont été créés dans les différents réseaux. Elles seront détaillées dans cette partie.

## LAN

Firewall / Rules / LAN

Floating   WAN   **LAN**   DMZ   INTERPFENSE

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 / 631 KIB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
Ressource Server										
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	Administrator_LAN	*	Ressource_Server_WAN	22 (SSH)	*	none		LAN To Ressource Server	
LAN to DMZ										
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	Administrator_LAN	*	Intranet_DMZ	22 (SSH)	*	none		Administrator to Intranet Server	
ICMP LAN TO ANY										
<input checked="" type="checkbox"/> 0 / 84 B	IPv4 ICMP any	LAN net	*	*	*	*	none		LAN to ANY ICMP	
LAN to WEB										
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		LAN to ANY HTTP	
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		LAN to ANY HTTPS	
LAN to DNS										
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP/UDP	LAN net	*	Cloud_DNS	53 (DNS)	*	none		LAN to Cloud DNS	
Deny All										
<input checked="" type="checkbox"/> 0 / 73 B	IPv4 *	*	*	*	*	*	none		Deny All	

Add   Add   Delete   Save   Separator

**La 1ère** règle nommée « Anti-Logout Rule » est ajoutée par défaut par PFSense, elle permet l'administration par l'ensemble du réseau.

Elle n'est pas modifiable et elle permet de ne jamais perdre l'accès d'administration sur le firewall. L'accès de la machine Administrator\_LAN aux interfaces d'administration est donc bien présent et répond à la demande du campus (n°5).

**La deuxième** règle « LAN To Ressource Server » permet au poste dans le LAN d'administrer le serveur de ressource situé sur le réseau WAN (demande n°16).

**La troisième** règle permet à la machine d'administration positionnée dans le LAN d'administrer la machine Intranet de la DMZ (demande n°12).

**La quatrième** règle « LAN to ANY ICMP » est présente pour autoriser le protocole ICMP depuis le réseau LAN vers toutes les destinations, elle englobe donc deux demandes du campus Ynov, la n°6 et la n°10. C'est-à-dire autoriser le protocole ICMP depuis le réseau LAN vers le WAN et la DMZ.

**La cinquième et sixième** règles « LAN to ANY HTTP(S) » permettent d'autoriser l'ensemble du réseau LAN à accéder à tous les serveurs de tous les réseaux sur les ports 443 et 80 (demande n°7).

Ces règles permettent également de répondre aux demandes n°12 (poste d'administration LAN vers Intranet sur le port 443) et une partie de la demande n°15 (LAN vers le serveur de ressource sur le port 443).

**La septième** règle « LAN to Cloud DNS » permet à l'ensemble du réseau LAN d'accéder au serveur DNS public 1.1.1.1, demande n°8.

**La dernière** règle bloque l'ensemble du trafic qui ne correspond pas aux règles décrites au-dessus, elle répond en partie à la demande n°3.

## WAN

The screenshot shows the Mikrotik WinBox interface for Firewall Rules configuration. The breadcrumb is 'Firewall / Rules / WAN'. The 'WAN' tab is selected. The 'Rules (Drag to Change Order)' table contains one rule:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> <span style="color: red;">✘</span>	0 / 73 B	IPv4 *	*	*	*	*	*	none	Deny All	

Buttons at the bottom: Add (up), Add (down), Delete, Save, Separator.

La seule règle présente dans la partie WAN est la règle qui bloque l'ensemble du trafic entrant sur la carte WAN du Firewall car aucune demande dans ce sens n'a été formulée par le campus Ynov d'Aix-en-Provence.

## DMZ

The screenshot shows the Mikrotik WinBox interface for Firewall Rules configuration. The breadcrumb is 'Firewall / Rules / DMZ'. The 'DMZ' tab is selected. The 'Rules (Drag to Change Order)' table contains five rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<b>DMZ Admin to Pfsense</b>										
<input type="checkbox"/> <span style="color: green;">✔</span>	0 / 0 B	IPv4 TCP	Intranet_DMZ	*	DMZ address	443 (HTTPS)	*	none	DMZ Admin to PFSense DMZ	
<input type="checkbox"/> <span style="color: green;">✔</span>	0 / 0 B	IPv4 TCP	Intranet_DMZ	*	DMZ address	22 (SSH)	*	none	DMZ Admin to PFSense DMZ	
<b>ICMP to ANY</b>										
<input type="checkbox"/> <span style="color: green;">✔</span>	0 / 0 B	IPv4 ICMP	DMZ net	*	*	*	*	none	ICMP DMZ TO ANY	
<b>Deny ALL</b>										
<input type="checkbox"/> <span style="color: red;">✘</span>	0 / 73 B	IPv4 *	*	*	*	*	*	none	Deny All	

Buttons at the bottom: Add (up), Add (down), Delete, Save, Separator.

**Les deux premières** règles permettent à la machine d'administration/intranet du réseau DMZ d'accéder aux interfaces d'administration du Firewall (demande n°13).

**La troisième** règle répond à la demande n°11 et permet à l'ensemble du réseau DMZ d'atteindre avec le protocole ICMP les réseaux LAN et WAN.

**La dernière** règle bloque l'ensemble du trafic qui ne correspond pas aux règles décrites au-dessus, elle répond en partie à la demande n°3.

## Tests

L'ensemble des tests ont été réalisés avec l'outil netcat pour des raisons de simplicité (sauf pour le SSH et l'ICMP).

Source	Destination	Protocole	Résultat
<b>Administrator_LAN</b>	LAN Address PFSense	SSH (22)	OK
<b>Administrator_LAN</b>	LAN Address PFSense	HTTPS (443)	OK
<b>Administrator_LAN</b>	WAN Address PFSense	ICMP	OK
<b>Administrator_LAN</b>	DMZ Address PFSense	ICMP	OK
<b>Administrator_LAN</b>	Ressource_Server_WAN	HTTPS (443)	OK
<b>Administrator_LAN</b>	Ressource_Server_WAN	HTTP (80)	OK
<b>Administrator_LAN</b>	Ressource_Server_WAN	SSH (22)	OK
<b>Administrator_LAN</b>	Cloud_DNS	DNS (53)	OK
<b>Administrator_LAN</b>	Intranet_DMZ	SSH (22) & HTTPS (443)	OK
<b>Intranet_DMZ</b>	LAN Address PFSense	ICMP	OK
<b>Intranet_DMZ</b>	WAN Address PFSense	ICMP	OK
<b>Intranet_DMZ</b>	DMZ Address PFSense	HTTPS (443)	OK
<b>Intranet_DMZ</b>	DMZ_Address PFSense	SSH (22)	OK

L'ensemble de ces tests nous permettent de valider l'ensemble des demandes faites pas le Campus Ynov d'Aix-en-Provence.

# YNOV CAMPUS