PFsense

Firewall & Virtualisation

Hes·SO GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

L'avenir est à créer

h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Plan

- Introduction
- Présentation
- Fonctionnalités
- Administration
- Réalisation : scénarios pédagogiques
    1- Statefull firewall pour les futurs étudiants.
    2- Filtrage du trafic à base de VLAN.
    3- Failover (redondance) de l'accès internet.
    4- Solution dual firewall (haute disponibilité) avec CARP.
    5- Système virtualisé avec KVM et supervision avec SHINKEN.
    6- Test de performance.
- Conclusion
- Démonstration : scénario 4 (dual firewall)
- Questions

PFsense : présentation

- Pfsense est une distribution **FreeBSD** dédié firewall / routeur.
- Le firewall est basé sur **P**aquet **F**ilter.

Toute la configuration du système est stocké dans un **fichier xml** (**/cf/conf/config.xml**).

- Performances sont liées au matériel.

PFsense : fonctionnalités

Firewall.

Routeur WAN / LAN.

Point d'accés wireless.

VPN (Ipsec, OpenVPN, L2TP ou PPTP).

Proxy et inverse proxy.

Serveur DHCP, DNS.

VOIP

PFsense : administration

Administration par **interface web**.

Administration en **CLI via le shell**.

Possibilité d'exécuter des **commandes PHP**.

Administration distante via **ssh** ou VPN.

config.xml

```
<interfaces>
 - <wan>
      <enable/>
      <if>em2</if>
      <blockpriv>on</blockpriv>
      <blockbogons>on</blockbogons>
    - <descr>
        <![CDATA[EXT]]>
      </descr>
      <ipaddr>129.194.184.98</ipaddr>
      <subnet>22</subnet>
      <gateway>WANGW</gateway>
      <media>autoselect</media>
  </wan>
 - <lan>
      <enable/>
      <if>em0</if>
    - <descr>
        <![CDATA[LAN]]>
      </descr>
      <spoofmac/>
      <ipaddr>192.168.1.1</ipaddr>
      <subnet>24</subnet>
  </lan>
 - <opt1>
    - <descr>
        <![CDATA[DMZ]]>
      </descr>
      <if>em1</if>
      <spoofmac/>
      <enable/>
      <ipaddr>10.1.0.1</ipaddr>
      <subnet>16</subnet>
  </opt1>
</interfaces>
```

```
10
11
12  $config['dhcpd']['lan']['disabled'] = false;
13  $config['dhcpd']['lan']['range']['from'] = "192.168.1.0";
14  $config['dhcpd']['lan']['range']['to'] = "192.168.1.150";
15
16  $config['interfaces']['lan']['enable'] = true;
17  $config['interfaces']['lan']['if'] = "em0";
18  $config['interfaces']['lan']['ipaddr'] = "192.168.1.1";
19  $config['interfaces']['opt1']['disabled'] = false;
20  $config['interfaces']['opt1']['if'] = "em1";
21  $config['interfaces']['opt1']['ipaddr'] = "10.1.01";
22  $config['interfaces']['opt1']['subnet'] = "16";
23
24  $config['interfaces']['wan']['disabled'] = false;
25  $config['interfaces']['wan']['if'] = "em2";
26  $config['interfaces']['wan']['blockpriv'] = "on";
27  $config['interfaces']['wan']['blockbogons'] = "on";
28  $config['interfaces']['wan']['ipaddr'] = "129.194.184.98";
29  $config['interfaces']['wan']['subnet'] = "22";
30  $config['interfaces']['wan']['gateway'] = "129.194.184.1";
31
32  $config['system']['dnsserver'] = "129.194.4.32";
33  $config['system']['dnsserver'] = "129.194.8.7";
34  $config['system']['dnsserver'] = "129.194.4.6";
35  $config['system']['dns1gwint'] = "wan";
36  $config['system']['dns2gwint'] = "wan";
37  $config['system']['dns3gwint'] = "wan";
38
39  $config['system']['enablesshd'] = true;
40
41  write_config();   //to save out the new config (config.xml)
```

PFsense : réalisation

Mise en place de scénario à but pédagogique :

1- Labo statefull firewall pour les futurs étudiants.
2- Filtrage du trafic à base de VLAN.
3- Failover (redondance) de l'accès internet.
4- Solution dual firewall avec CARP.
5- Système virtualisé et supervision avec SHINKEN
6- Test de performance

Répartition du temps

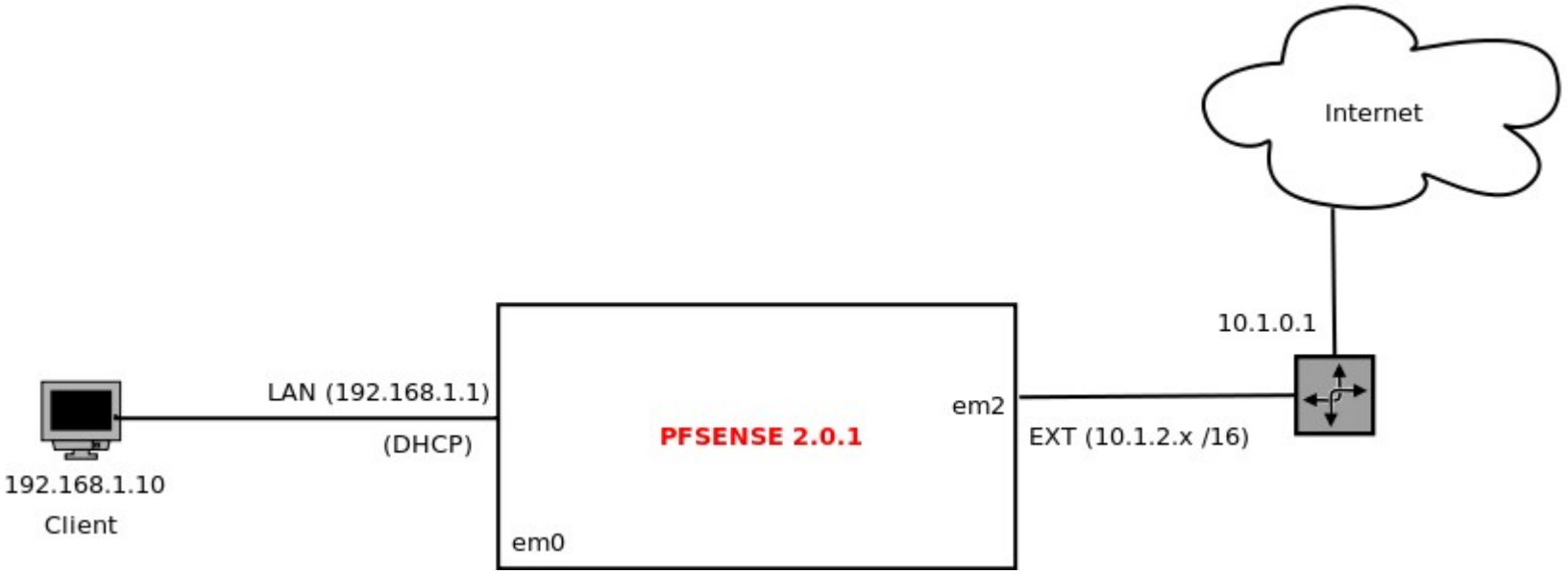
-Semaine 1-2 : Documentation et prise en main de pfsense.

-Semaine 3-4 : proposition des scénarios pédagogiques, réalisation du scénario 1, rédaction du rapport.

-Semaine 5 : réalisation des scénarios 2 et 3.

-Semaine 6-7-8 : réalisation des scénarios 4, 5, et 6. rédaction du rapport.

1- Statefull firewall



EXT LAN

pass
pass (disabled)

block
block (disabled)

reject
reject (disabled)

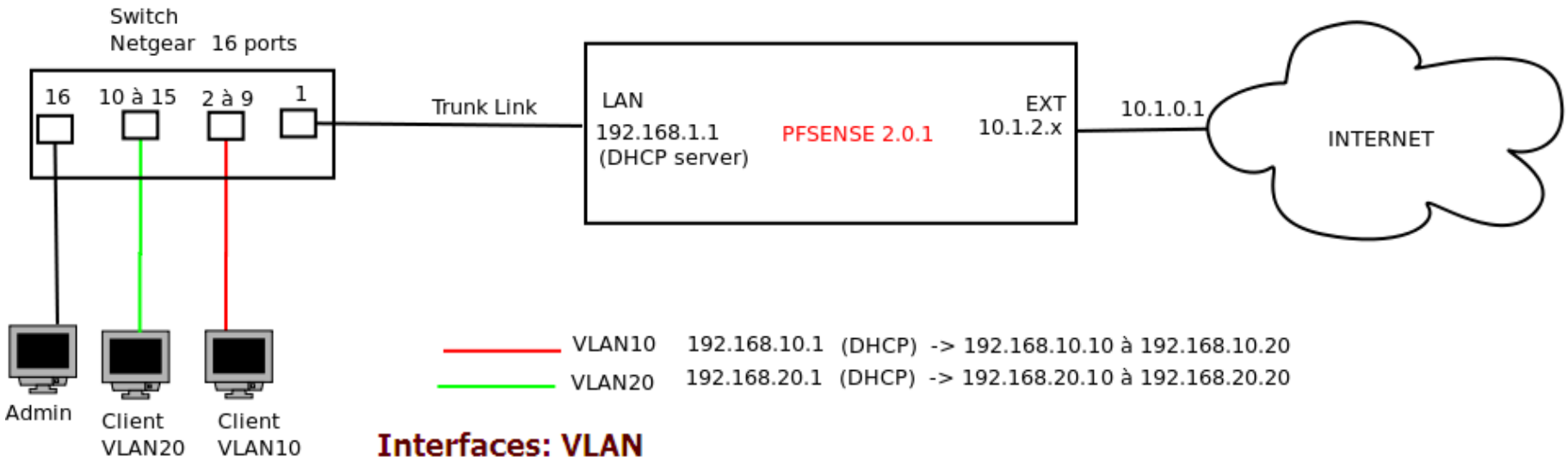
Proto	Source	Port	Destination	Port	Gateway
ICMP	LAN net	*	10.1.2.114	*	*

Interfaces

EXT	10.1.2.111
LAN	192.168.1.1

icmp	10.1.2.114:45836 <- 192.168.1.10	0:0
icmp	192.168.1.10:45836 -> 10.1.2.111:27048 -> 10.1.2.114	0:0

2- Filtrage par VLAN



Interfaces: VLAN

Interface assignments | Interface Groups | Wireless | VLANs | QinQs | PPPs | GRE | GIF | Bridges | LAGG

Interface	VLAN tag	Description
em0	10	LAN_10
em0	20	LAN_20

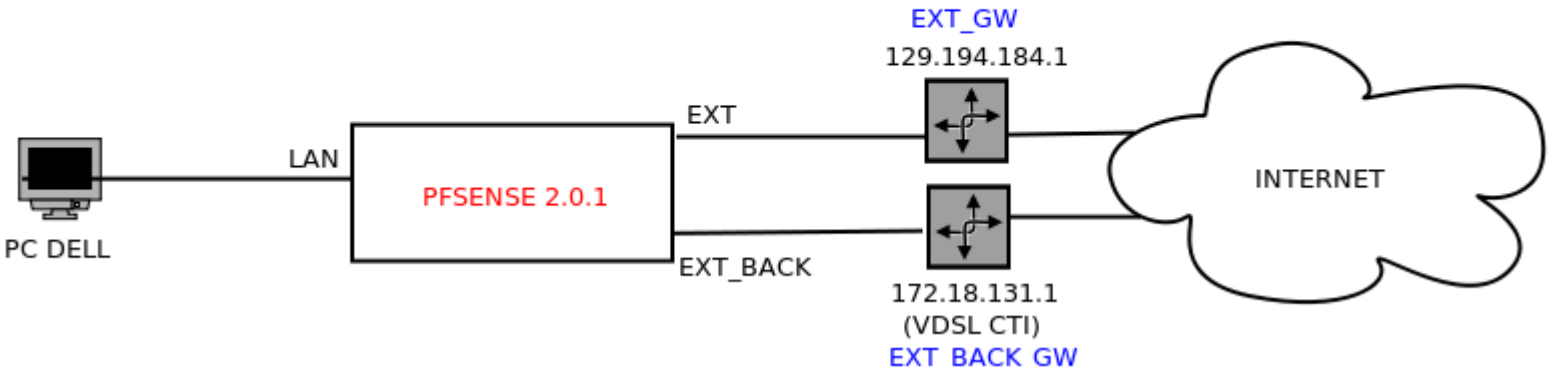
OPT2	VLAN 10 on em0 (LAN_10)
OPT3	VLAN 20 on em0 (LAN_20)

3- Failover de l'accès internet

Gateway | failover_internet ▼

LAN : 192.168.1.1
EXT : 129.194.184.98
EXT_BACK : 172.18.131.5 (DHCP)

```
apinger: ALARM: WANGW(129.194.184.1) *** down ***
check_reload_status: Reloading filter
php: : Default gateway down setting GW_OPT1 as default!
php: : MONITOR: WANGW is down, removing from routing group
```

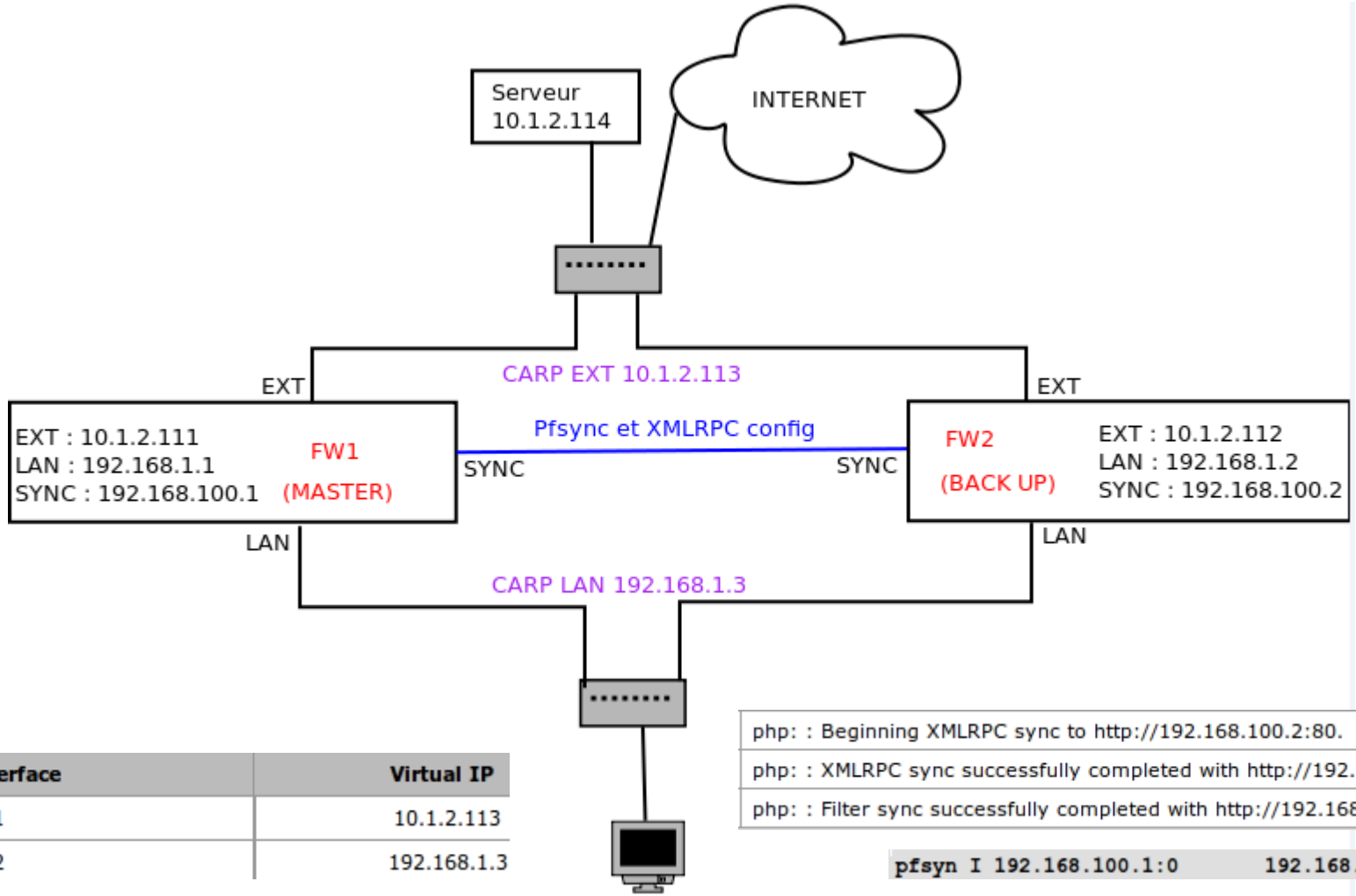


Gateways | Routes | Groups

Group Name	Gateways	Priority	Description
failover_internet	WANGW GW_OPT1	Tier 1 Tier 2	failover internet (UNI et VDSL CTI)

WANGW **(default)**	EXT	129.194.184.1	129.194.184.1	WAN Gateway
GW_OPT1	EXT_BACK	172.18.131.1	172.18.131.1	Interfaceopt1dynamic gateway

4- Dual firewall



CARP Interface	Virtual IP
vip1	10.1.2.113
vip2	192.168.1.3

```
php: : Beginning XMLRPC sync to http://192.168.100.2:80.
php: : XMLRPC sync successfully completed with http://192.168.100.2:80.
php: : Filter sync successfully completed with http://192.168.100.2:80.
```

```
pfsyn I 192.168.100.1:0        192.168.100.2:0
```

Fonctionnement de CARP

-CARP est implémenté sur un hôte par un pseudo-device (virtual interface) appelé **carpN**

-permet de former des **groupes de redondances** identifiés chacun par un **VHID** (valeur : 1 à 255).

-toutes les adresses d'un groupe de redondance doivent appartenir au **même sous réseau**.

une adresse **multicast MAC** est utilisée pour envoyer les annonces (**advertisment**) aux membres du groupe.

-l'intervalle entre deux annonces est définie par la configuration de deux paramètres :

-**advbase** : intervalle entre deux annonce (défaut 1 seconde).

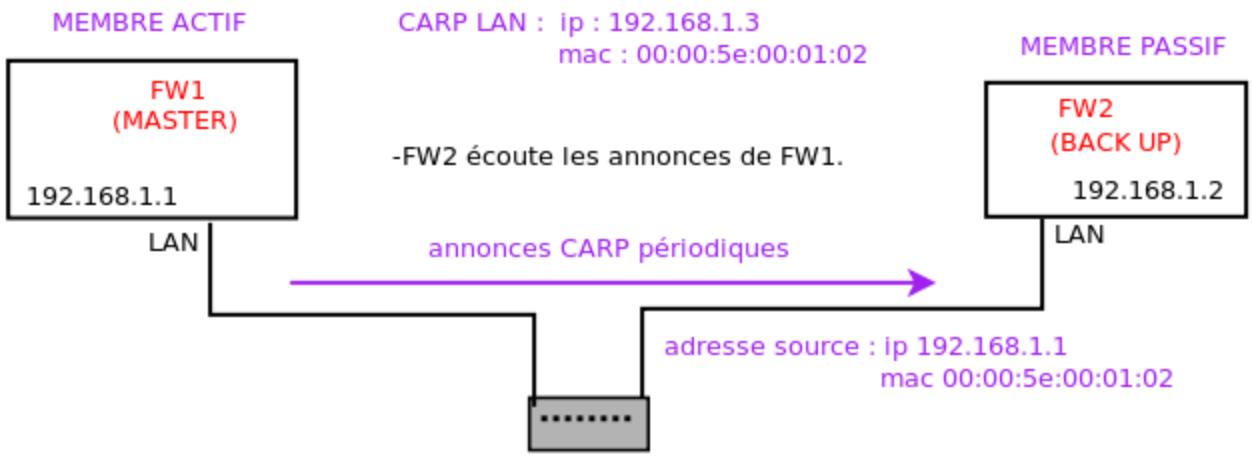
-**advskew** : décalage de l'intervalle (défaut 0 pour le maître).

Pris ensemble ces deux paramètres précisent la fréquence en seconde d'annonces :

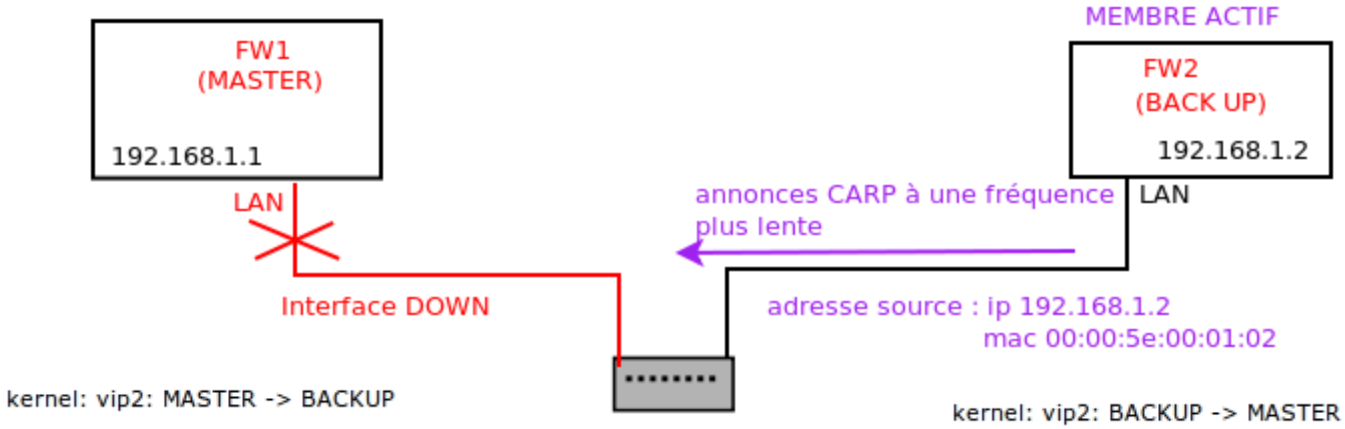
la formule : **advbase + (advskew / 255)**.

-un paramètre **password** (virtual ip password) est utilisé comme identificateur.

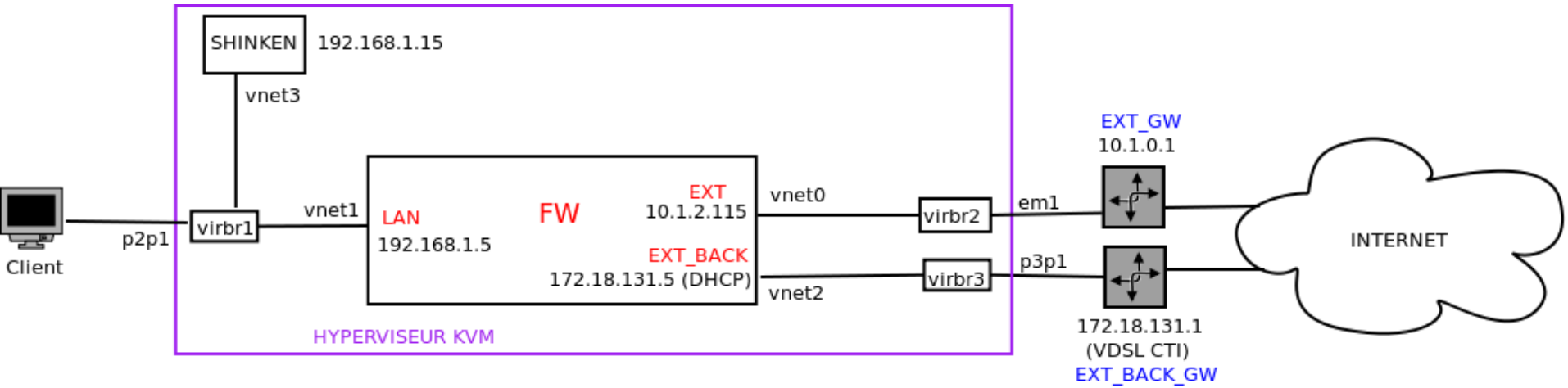
Fonctionnement de CARP



-Quand FW1 tombe, FW2 ne recevant plus d'annonce CARP, devient membre actif et envoie à son tour des annonces CARI
(mais à une fréquence moins élevé que le FW1)

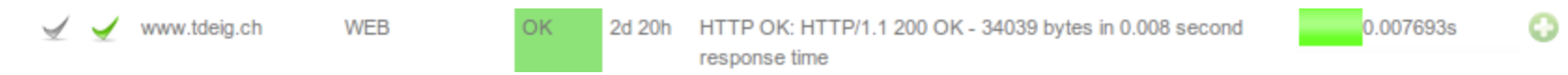


5- Virtualisation avec KVM




```
virbr1          8000.001b21287f7e       yes             p2p1
                                                        vnet1
                                                        vnet3
virbr2          8000.90e6ba91f83f       yes             em1
                                                        vnet0
virbr3          8000.001b21453d4e       yes             p3p1
                                                        vnet2
```

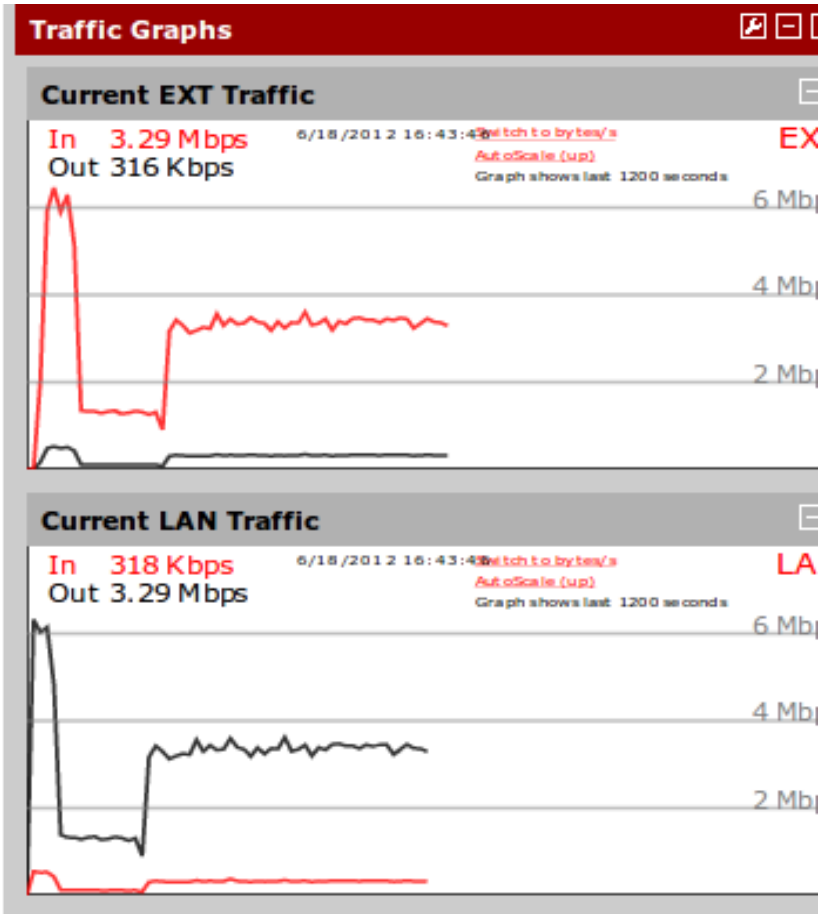
Supervision avec SHINKEN



6- Test de performance CPU/RAM

Test dans un environnement physique :

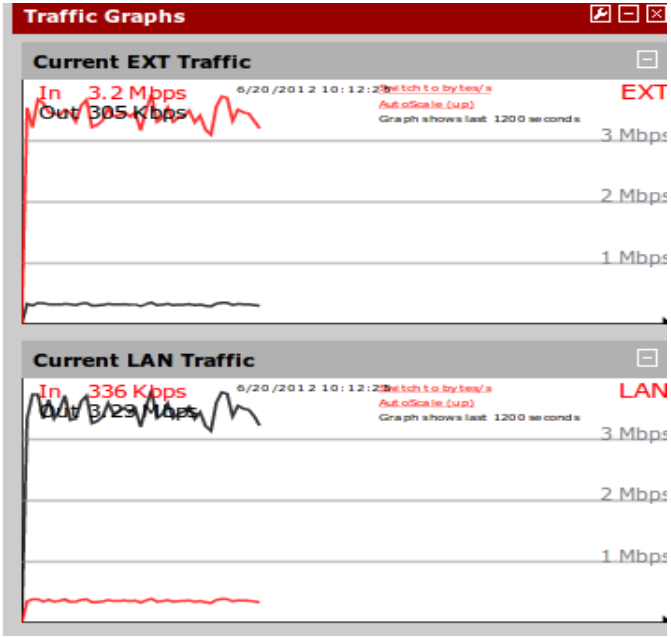
CPU Type	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz
Uptime	00:37
Current date/time	Mon Jun 18 16:44:23 CEST 2012
DNS server(s)	127.0.0.1 129.194.4.6
Last config change	Mon Jun 18 11:27:08 CEST 2012
State table size	11702/320000 Show states
MBUF Usage	2838/25600
CPU usage	2%
Memory usage	3%
SWAP usage	0%



6- Test de performance CPU/RAM

Test dans un environnement virtualisé :

CPU Type	QEMU Virtual CPU version 0.15.0
Uptime	1 day, 17:20
Current date/time	Wed Jun 20 10:12:25 CEST 2012
DNS server(s)	127.0.0.1 129.194.4.6 195.186.4.110 212.147.10.180
Last config change	Mon Jun 18 16:56:45 CEST 2012
State table size	13454/98000 Show states
MBUF Usage	902/25600
CPU usage	25%
Memory usage	8%
SWAP	



State table size	31/98000 Show states
MBUF Usage	902/25600
CPU usage	14%
Memory usage	8%

State table size	12790/98000 Show states
MBUF Usage	902/25600
CPU usage	15%
Memory usage	8%

State table size	13838/98000 Show states
MBUF Usage	902/25600
CPU usage	69%
Memory usage	8%

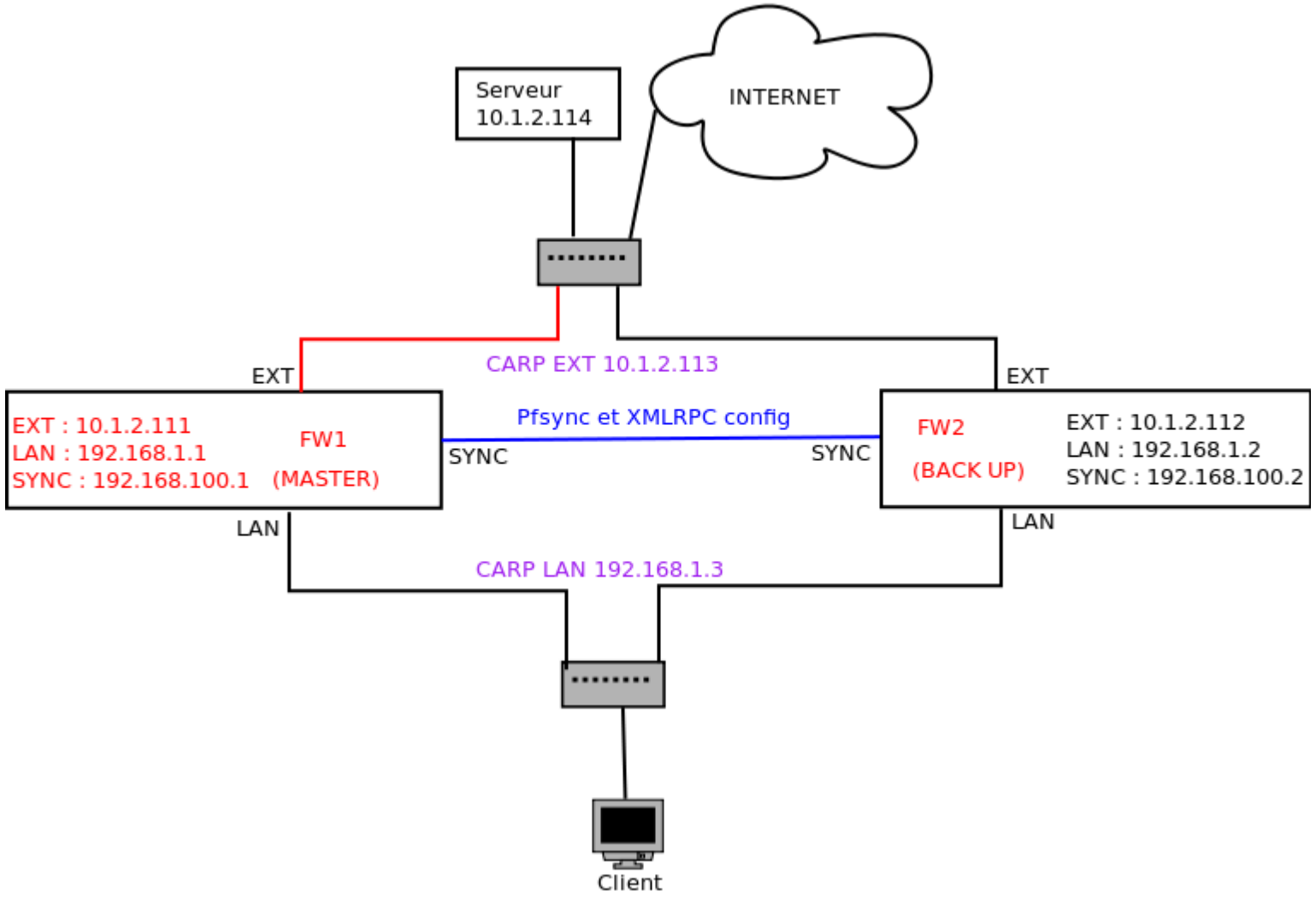
conclusion

- Solution riche et performante à moindre coût (basé sur des logiciels libres).

- Solution légère pouvant être déployé sur des configuration minimal.

- Interface web intuitive et efficace.

Demonstration



Questions