

Chapitre 1 – B2 – Epreuve E5 et expression des besoins

Table des Matières :

MISSION1.....	3
---------------	---

```
pfSense 2.8.1-RELEASE amd64 20251024-1553
Bootup complete

FreeBSD/amd64 (pfSense.sio-exupery.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: c7050fd41dfe970d46bc

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan)   -> em0 -> v4: 192.168.1.101/24
LAN (lan)   -> em2 -> v4: 192.168.3.254/24
OPT1 (opt1) -> em1 -> v4: 192.168.2.254/24
OPT2 (opt2) -> em3 -> v4: 192.168.4.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: █
```

```
pfSense 2.8.1-RELEASE amd64 20251024-1553
Bootup complete

FreeBSD/amd64 (pfSense.sio-exupery.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 8993f0b9688f1652c472

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

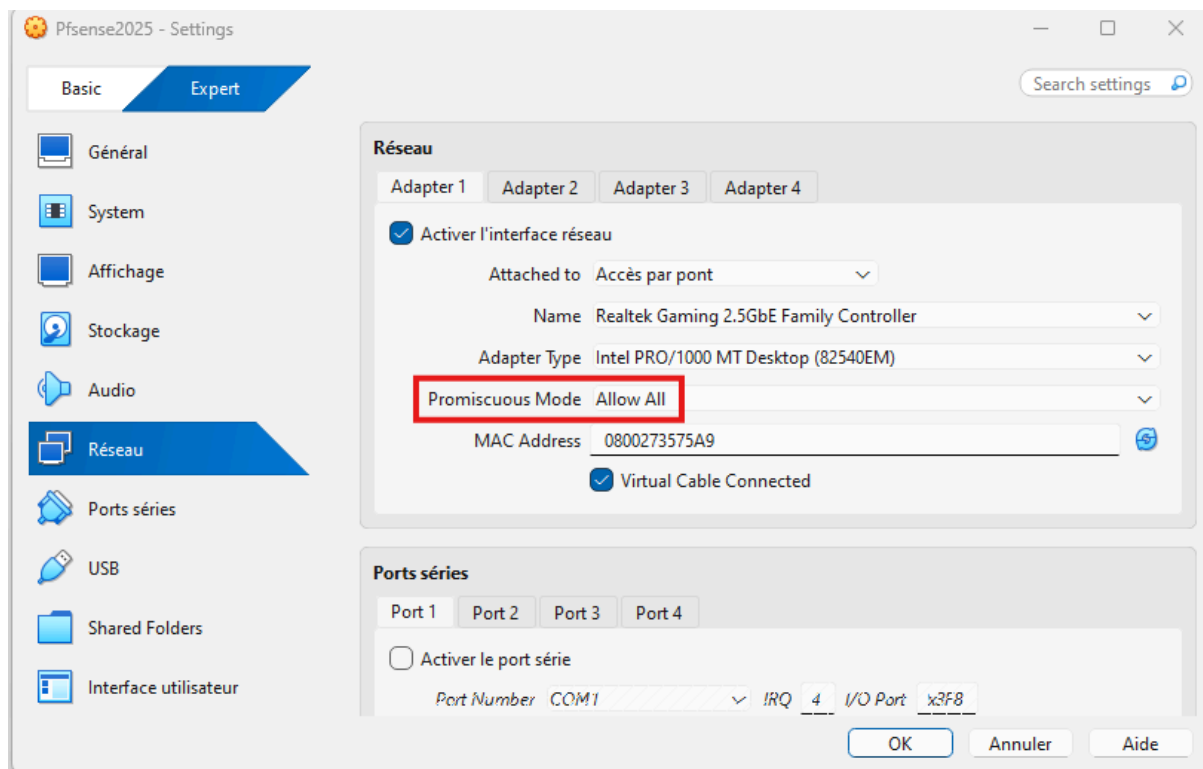
WAN (wan)   -> em0 -> v4: 192.168.1.102/24
LAN (lan)   -> em2 -> v4: 192.168.3.254/24
OPT1 (opt1) -> em1 -> v4: 192.168.2.254/24
OPT2 (opt2) -> em3 -> v4: 192.168.4.2/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

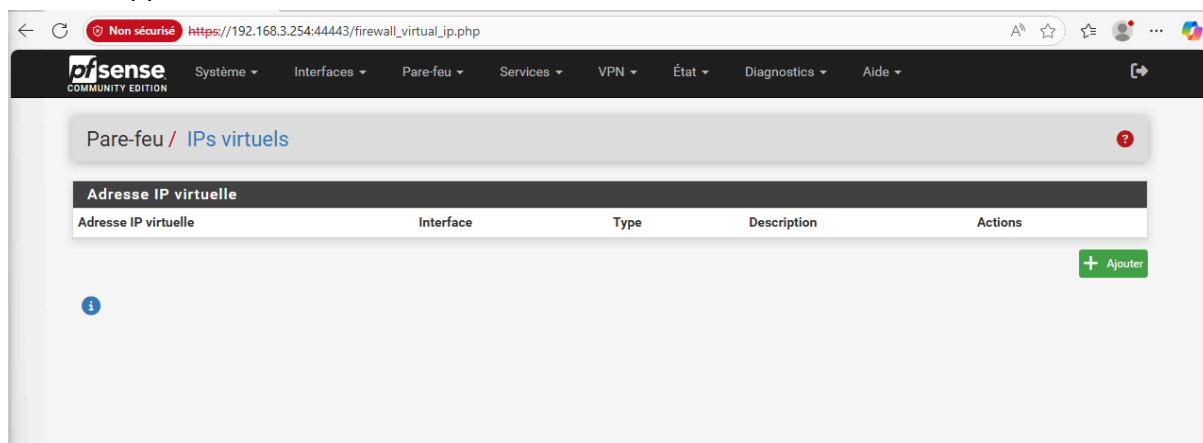
Enter an option: █
```

MISSION1

- Pour toutes les cartes des VM :



- Nous supprimons les éventuelles anciennes IP virtuelles :



- Sur le pfSense Master :
 - Nous créons les VIP (CARP) pour chaque interface :

The screenshot shows the 'Modifier l'IP virtuelle' (Modify Virtual IP) configuration page in pfSense. The 'Type' is set to 'CARP'. The 'Interface' is 'WAN'. The 'Type d'adresse' is 'Adresse unitaire'. The 'Adresse(s)' is '192.168.1.103' with a subnet mask of '24'. The 'Mot de passe d'IP virtuelle' is masked with '.....'. The 'Groupe VHID' is '100'. The 'Advertising Frequency' is set to '1' (Base) and '0' (Biais). The 'Description' is 'CARP WAN'.

The screenshot shows the 'Modifier l'IP virtuelle' (Modify Virtual IP) configuration page in pfSense. The 'Type' is set to 'CARP'. The 'Interface' is 'LAN'. The 'Type d'adresse' is 'Adresse unitaire'. The 'Adresse(s)' is '192.168.3.252' with a subnet mask of '24'. The 'Mot de passe d'IP virtuelle' is masked with '.....'. The 'Groupe VHID' is '101'. The 'Advertising Frequency' is set to '1' (Base) and '0' (Biais). The 'Description' is 'CARP LAN'.

Non sécurisé https://192.168.3.254:44443/firewall_virtual_ip_edit.php

pfSense COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Pare-feu / IPs virtuels / Modifier

Modifier l'IP virtuelle

Type Alias IP CARP Mandataire (proxy) ARP Autre

Interface OPT1

Type d'adresse Adresse unitaire

Adresse(s) 192.168.2.252 / 24
Le masque doit être le masque de sous-réseau du réseau. Il ne spécifie pas une plage CIDR.

Mot de passe d'IP virtuelle
 Entrez le mot de passe du groupe VHID. Confirm

Groupe VHID 102
Entrez le nom du groupe VHID qui sera partagé.

Advertising Frequency 1 Base 0 Biais
La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.

Description CARP DMZ
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Non sécurisé https://192.168.3.254:44443/firewall_virtual_ip.php







pfSense COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Pare-feu / IPs virtuels

Les modifications ont été appliquées avec succès.

Adresse IP virtuelle

Adresse IP virtuelle	Interface	Type	Description	Actions
192.168.1.103/24 (vhid: 100)	WAN	CARP	CARP WAN	 
192.168.3.252/24 (vhid: 101)	LAN	CARP	CARP LAN	 
192.168.2.252/24 (vhid: 102)	OPT1	CARP	CARP DMZ	 

État / CARP

CARP Maintenance

Statut CARP

Interface and VHID	Adresse IP virtuelle	Description	État
WAN@100	192.168.1.103/24	CARP WAN	▶ MASTER
LAN@101	192.168.3.252/24	CARP LAN	▶ MASTER
OPT1@102	192.168.2.252/24	CARP DMZ	▶ MASTER

State Synchronization Status

State Creator Host IDs:

- 8347bc71 (This node)

Pare-feu / NAT / Sortant

La configuration NAT a été modifiée.
Ces modifications doivent être appliquées pour prendre effet.

▪ Sur le pfSense Master :

Pare-feu / NAT / Sortant

Transfert de port 1:1 **Sortant** NPt

Mode NAT sortant

Mode	Description
<input type="radio"/>	Création automatique de règles NAT sortantes. (IPsec passthrough inclu)
<input checked="" type="radio"/>	Création hybride de règles NAT sortantes. (NAT sortant automatique + règles ci-dessous)
<input type="radio"/>	Création manuelle de règles NAT sortantes. (NSA - NAT sortant avancée)
<input type="radio"/>	Désactiver la création de règles NAT sortantes. (Aucune règle NAT sortant)

(ou Création manuelle)

Mappages

Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description	Actions
<input type="button" value="Ajouter"/> <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Toggle"/> <input type="button" value="Enregistrer"/>									

pfSense
COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Pare-feu / NAT / Sortant / Modifier

Modifier l'entrée NAT sortant avancée

Désactivé Désactiver cette règle

Ne pas faire de NAT Activer cette option va désactiver le NAT pour le trafic vérifiant cette règle et stopper le traitement des règles en sortie.
Dans la plupart des cas, cette option n'est pas nécessaire.

Interface WAN
L'interface via laquelle le trafic est vérifié lorsqu'il sort du pare-feu. Dans la plupart des cas, il s'agit de l'interface "WAN" ou d'une autre interface connectée en externe.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole Tous
Choisir à quel protocole cette règle devrait correspondre. La plupart du temps, "any" est spécifié.

Source Network or Alias 192.168.3.0 / 24
Type Le réseau source de la correspondance NAT sortante. Port ou plage

Destination Tous / 24
Type Le réseau destination de la correspondance NAT sortante. Port ou plage

Non
Inverser le sens de la vérification pour la destination.

Traduction

Adresse 192.168.1.103 (CARP WAN)
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Pare-feu / NAT / Sortant / Modifier

Modifier l'entrée NAT sortant avancée

Désactivé Désactiver cette règle

Ne pas faire de NAT Activer cette option va désactiver le NAT pour le trafic vérifiant cette règle et stopper le traitement des règles en sortie.
Dans la plupart des cas, cette option n'est pas nécessaire.

Interface WAN
L'interface via laquelle le trafic est vérifié lorsqu'il sort du pare-feu. Dans la plupart des cas, il s'agit de l'interface "WAN" ou d'une autre interface connectée en externe.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole Tous
Choisir à quel protocole cette règle devrait correspondre. La plupart du temps, "any" est spécifié.

Source Network or Alias 192.168.2.0 / 24
Type Le réseau source de la correspondance NAT sortante. Port ou plage

Destination Tous / 24
Type Le réseau destination de la correspondance NAT sortante. Port ou plage

Non
Inverser le sens de la vérification pour la destination.

Traduction

Adresse 192.168.1.103 (CARP WAN)
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

pfSense
Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Pare-feu / NAT / Sortant / Modifier ?

Modifier l'entrée NAT sortant avancée

Désactivé Désactiver cette règle

Ne pas faire de NAT Activer cette option va désactiver le NAT pour le trafic vérifiant cette règle et stopper le traitement des règles en sortie. Dans la plupart des cas, cette option n'est pas nécessaire.

Interface WAN
L'interface via laquelle le trafic est vérifié lorsqu'il sort du pare-feu. Dans la plupart des cas, il s'agit de l'interface "WAN" ou d'une autre interface connectée en externe.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole Tous
Choisir à quel protocole cette règle devrait correspondre. La plupart du temps, "any" est spécifié.

Source Network or Alias 192.168.4.0 / 24
Type Le réseau source de la correspondance NAT sortante. Port ou plage

Destination Tous / 24
Type Le réseau destination de la correspondance NAT sortante. Port ou plage

Non
Inverser le sens de la vérification pour la destination.

Traduction

Adresse 192.168.1.103 (CARP WAN)
Type Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Mappages

	Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description	Actions
<input type="checkbox"/>	✓ WAN	192.168.4.0/24	*	*	*	192.168.1.103 (CARP WAN)	*	↔		✎ ✏ 🗑
<input type="checkbox"/>	✓ WAN	192.168.2.0/24	*	*	*	192.168.1.103 (CARP WAN)	*	↔		✎ ✏ 🗑
<input type="checkbox"/>	✓ WAN	192.168.3.0/24	*	*	*	192.168.1.103 (CARP WAN)	*	↔		✎ ✏ 🗑

↑ Ajouter
↓ Ajouter
🗑 Supprimer
🔇 Toggle
📄 Enregistrer

- Nous devons le faire sur les deux PfSense
 - Nous appliquons le protocole Pfsync (pas XMLRPC)

The screenshot shows the pfSense web interface for High Availability configuration. The main heading is "Système / High Availability". Below it, there are two sections: "Paramètres de synchronisation d'état (pfsync)" and "Paramètres de synchronisation de configuration (XMLRPC Sync)".

Paramètres de synchronisation d'état (pfsync)

- Etat de la synchronisation:** Messages de pfsync pour état d'insertion, transfert, et suppression entre firewalls. (Detailed description follows)
- Synchroniser l'interface:** OPT2 (Dropdown menu)
- Filter Host ID:** 8347bc71 (Text input)
- IP de synchronisation pfsync du pair:** 192.168.4.2 (Text input)

Paramètres de synchronisation de configuration (XMLRPC Sync)

- Synchroniser la configuration avec IP:** 192.168.4.2 (Text input)

This screenshot shows the configuration page for remote synchronization. It includes fields for user and password, and a list of options to synchronize.

Nom d'utilisateur du système distant: admin

Mot de passe du système distant: [Redacted] / Confirmer

Synchronize admin: synchronize admin accounts and autoupdate sync password.

Sélectionnez les options à synchroniser:

- Gestion d'utilisateurs: Utilisateurs et Groupes
- Serveurs d'authentification (e.g LDAP, RADIUS)
- Listes des Autorités de Certification, Certificats, et Certificats de Révocation
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WoL Server settings
- Static Route configuration
- IPs virtuels
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Portail Captif
- Toggle All

Enregistrer (Button)

▪ Sur Pfsense2 :

Système / High Availability
☰ ?

Paramètres de synchronisation d'état (pfsync)

Etat de la synchronisation Messages de pfsync pour état d'insertion, transfert, et suppression entre firewalls.
 Chaque pare-feu envoie ces messages via multicast sur une interface spécifiée, en utilisant le protocole PFSYNC (protocole IP 240). Il écoute également cette interface pour des messages similaires provenant d'autres pare-feux et les importe dans la table d'état locale. Ce paramètre devrait être activé sur tous les membres d'un groupe de basculement. Cliquer sur "Enregistrer" forcera une synchronisation de configuration Si elle est activée! (Voir Paramètres de synchronisation de configuration ci-dessous)

Synchroniser l'interface
 Si les états de synchronisation sont activés, cette interface sera utilisée pour la communication. Il est recommandé de configurer cette option sur une interface autre que LAN ! Une interface dédiée fonctionne le mieux. Une IP doit être définie sur chaque machine participant à ce groupe de basculement. Une IP doit être affecté à l'interface sur les nœuds de synchronisation participants.

Filter Host ID
 Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.

IP de synchronisation pfsync du pair
 Le réglage de cette option obligera Pfsync à synchroniser sa table d'état avec cette adresse IP. La sélection par défaut est multicast dirigé.

Paramètres de synchronisation de configuration (XMLRPC Sync)

Synchroniser la configuration avec IP
 Entrez l'adresse IP du pare-feu à laquelle les sections de configuration sélectionnées doivent être synchronisées.

Nom d'utilisateur du système distant
 Entrez le nom d'utilisateur de WebConfigurator du système saisi ci-dessus pour la synchronisation de la configuration. N'utilisez pas l'option Synchroniser la configuration sur IP et le nom d'utilisateur sur les membres du cluster de sauvegarde !

Mot de passe du système distant
 Entrez le mot de passe du système de configuration Internet configuré ci-dessus pour la synchronisation de la configuration. N'utilisez pas l'option Synchroniser la configuration sur IP et mot de passe sur les membres du cluster de sauvegarde !

Synchronize admin synchronize admin accounts and autoupdate sync password.
 By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Sélectionnez les options à synchroniser

- Gestion d'utilisateurs: Utilisateurs et Groupes
- Serveurs d'authentification (e.g LDAP, RADIUS)
- Listes des Autorités de Certification, Certificats, et Certificats de Révocation
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WoL Server settings
- Static Route configuration
- IPs virtuels
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Portail Captif
- [Toggle All](#)

- Nous appliquons les règles sur le pfsense Master pour autoriser les flux pfsync et XML-RPC :

https://192.168.3.254:44443/firewall_rules.php?if=opt2

Pare-feu / Règles / OPT2

Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan. Surveiller le rechargement des filtres.

Flottant(e) WAN LAN OPT1 **OPT2**

Règles (Faire glisser pour changer l'ordre)

<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.4.0/24	*	Ce pare-feu (lui-même)	44443	*	aucun		Flux HTTPS pour la réplication XML-RPC	
<input type="checkbox"/>	✓ 0/0 B	IPv4 PFSYNC	192.168.4.0/24	*	Ce pare-feu (lui-même)	*	*	aucun		flux pfsync	

Ajouter Ajouter Supprimer Toggle Copier Enregistrer Séparateur

https://192.168.3.254:44443/firewall_rules_edit.php?id=6

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action Autoriser
Choisissez que faire des paquets qui correspondent aux critères ci-dessous. Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'envoyeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface OPT2
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole TCP
Choisissez quel protocole IP cette règle devrait correspondre.

Source

Source Invert match Réseau 192.168.4.0 / 24

Afficher les options avancées

La **plage de ports source** d'une connexion est généralement aléatoire et presque jamais égale au port de destination. Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, any.

Destination

Destination Invert match Ce pare-feu (lui-même) Destination Address

Plage de port de destination (autre) 44443 (autre) 44443
De Personnalisé(e) À Personnalisé(e)
Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A » peut rester vide seulement si le filtre est sur un seul port.

Options additionnelles

Journalise Journaliser les paquets gérés par cette règle
Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page Statut: Journaux système : Paramètres).

Description Flux HTTPS pour la réplication XML-RPC
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.

Options Avancées **Afficher les options avancées**

Modifier la règle de Pare-Feu

Action: Autoriser
 Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
 Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé: Désactiver cette règle
 Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface: OPT2
 Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse: IPv4
 Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole: PFSYNC
 Choisissez quel protocole IP cette règle devrait correspondre.

Source

Source Invert match Réseau 192.168.4.0 / 24

Destination

Destination Invert match Ce pare-feu (lui-même) Destination Address /

Options additionnelles

Journalise Journaliser les paquets gérés par cette règle
 Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page [Statut: Journaux système : Paramètres](#)).

Description: flux pfsync
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.

Options Avancées [Afficher les options avancées](#)

▪ Nous vérifions sur la pfsenseB

Pare-feu / Règles / OPT2

Flottant(e) WAN LAN OPT1 **OPT2**

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 PFSYNC	192.168.4.0/24	*	*	*	*	aucun		Flux pfsync	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.4.0/24	*	Ce pare-feu (lui-même)	44443	*	aucun		Flux HTTPS pour la réplication XMLRPC	

[Ajouter](#) [Ajouter](#) [Supprimer](#) [Toggle](#) [Copier](#) [Enregistrer](#) [Séparateur](#)

Pare-feu / NAT / Sortant

Transfert de port 1:1 **Sortant** NPT

Mode NAT sortant

Mode

- Création automatique de règles NAT sortantes. (IPsec passthrough inclu)
- Création hybride de règles NAT sortantes. (NAT sortant automatique + règles ci-dessous)
- Création manuelle de règles NAT sortantes. (NSA - NAT sortant avancée)
- Désactiver la création de règles NAT sortantes. (Aucune règle NAT sortant)

Enregistrer

Mappages

<input type="checkbox"/>	Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description	Actions
<input checked="" type="checkbox"/>	WAN	192.168.4.0/24	*	*	*	192.168.1.103 (CARP WAN)	*	↔		
<input checked="" type="checkbox"/>	WAN	192.168.2.0/24	*	*	*	192.168.1.103 (CARP WAN)	*	↔		
<input checked="" type="checkbox"/>	WAN	192.168.3.0/24	*	*	*	192.168.1.103 (CARP WAN)	*	↔		

Ajouter Ajouter Supprimer Toggle Enregistrer

Test ping la machine physique :

Annuler **Filaire** Appliquer

Détails Identité IPv4 IPv6 Sécurité

Vitesse de la connexion 1000 Mb/s

Adresse IPv4 192.168.3.11

Adresse IPv6 fe80::a00:27ff:fea2:3644

Adresse matérielle 08:00:27:A2:36:44

Route par défaut 192.168.3.252

DNS 192.168.3.1

```

rtt min/avg/max/mdev = 9.904/13.410/65.281/3.482 ms, pipe 4
root@Ansible:~# ping 192.168.1.75
PING 192.168.1.75 (192.168.1.75) 56(84) bytes of data:
64 bytes from 192.168.1.75: icmp_seq=1 ttl=127 time=4.28 ms
64 bytes from 192.168.1.75: icmp_seq=2 ttl=127 time=4.78 ms
64 bytes from 192.168.1.75: icmp_seq=3 ttl=127 time=2.80 ms
64 bytes from 192.168.1.75: icmp_seq=4 ttl=127 time=2.62 ms
64 bytes from 192.168.1.75: icmp_seq=5 ttl=127 time=10.2 ms
    
```

TEST Ping machine physique depuis LAN (ou ping routeur cisco ou ping 8.8.8.8) puis arrêt pfsenseA :

Ip de la machine physique à ping :

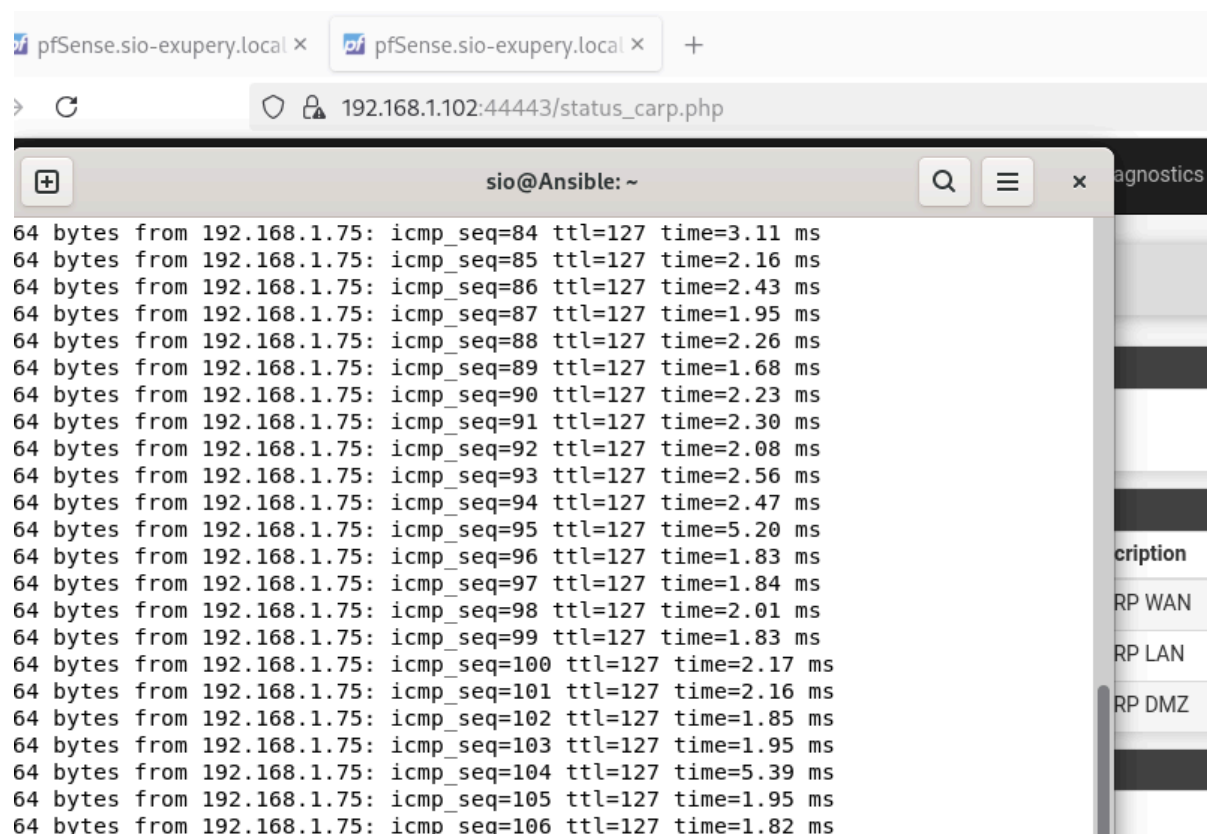
```
Carte Ethernet Ethernet :  
  
Suffixe DNS propre à la connexion. . . . :  
Adresse IPv6. . . . . : 2a02:842a:83c7:b001:7a0d:1b75:26bc:5a5b  
Adresse IPv6 temporaire. . . . . : 2a02:842a:83c7:b001:202e:c3bf:2b15:371b  
Adresse IPv6 de liaison locale. . . . . : fe80::c98e:792:6a1:f08e%17  
Adresse IPv4. . . . . : 192.168.1.75  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : fe80::ce19:a8ff:fecf:70df%17  
192.168.1.1  
  
Carte réseau sans fil Connexion au réseau local* 9 :
```

Avec pfsense A

The screenshot shows a browser window with the URL `192.168.1.101:44443/status_carp.php`. In the foreground, a terminal window shows the command `ping 192.168.1.75` being executed, with 19 successful pings. In the background, the pfSense web interface is visible, showing a table of network interfaces:

Description	État
RP WAN	▶ MASTER
RP LAN	▶ MASTER
RP DMZ	▶ MASTER

Nous arrêtons pfsenseA pour laisser place au pfsenseB



La pfsenseB prend bien le relais



Nous testons de ping 8.8.8.8

```
sio@Ansible: ~  
root@Ansible:~# ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.0 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=15.3 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=11.6 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.6 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=12.3 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=14.8 ms  
64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=13.9 ms  
64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=13.5 ms  
64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=15.6 ms  
64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=12.7 ms  
64 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=15.1 ms  
64 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=15.0 ms  
64 bytes from 8.8.8.8: icmp_seq=13 ttl=118 time=13.3 ms  
64 bytes from 8.8.8.8: icmp_seq=14 ttl=118 time=14.6 ms  
64 bytes from 8.8.8.8: icmp_seq=15 ttl=118 time=13.2 ms  
64 bytes from 8.8.8.8: icmp_seq=16 ttl=118 time=12.0 ms  
64 bytes from 8.8.8.8: icmp_seq=17 ttl=118 time=11.7 ms  
64 bytes from 8.8.8.8: icmp_seq=18 ttl=118 time=14.2 ms  
64 bytes from 8.8.8.8: icmp_seq=19 ttl=118 time=11.5 ms  
64 bytes from 8.8.8.8: icmp_seq=20 ttl=118 time=13.7 ms  
64 bytes from 8.8.8.8: icmp_seq=21 ttl=118 time=16.0 ms  
64 bytes from 8.8.8.8: icmp_seq=22 ttl=118 time=10.9 ms
```

