
Mise en place du protocole CARP entre deux serveur pfsense

Je vais installer deux serveur pfsense un master et l'autre slave

MASTER : 192.168.1.244

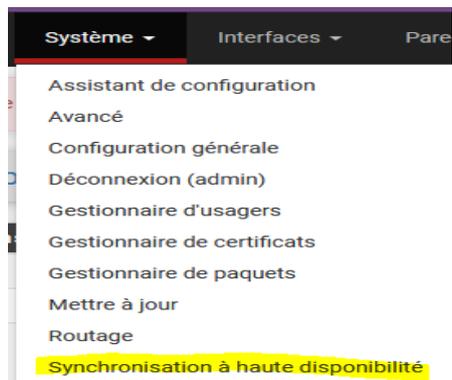
SLAVE = 192.168.1.243

IP_VIRTUELLE = 192.168.1.245

Tout en « /24 » bien sur

Nous allons d'abord synchroniser les deux routeurs

Sur le routeur master je me rend ici :



Ensuite je remplis comme ceci

Paramètres de synchronisation d'état (pfsync)	
Etat de la synchronisation	<input type="checkbox"/> 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	<input type="text" value="LAN"/> 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.
IP de synchronisation pfsync du pair	<input type="text" value="192.168.1.243"/> 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	<input type="text" value="192.168.1.243"/> Entrez l'adresse IP du pare-feu à laquelle les sections de configuration sélectionnées doivent être synchronisées. La synchronisation XMLRPC n'est actuellement prise en charge que sur les connexions utilisant le même protocole et le même port que ce système - assurez-vous que le port et le protocole du système distant sont définis en conséquence ! N'utilisez pas l'option Synchroniser la configuration sur IP et le mot de passe sur les membres du cluster de sauvegarde!
Nom d'utilisateur du système distant	<input type="text" value="admin"/> 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	<input type="password" value="....."/> <input type="password" value="....."/> 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 ! Confirmer
Synchronise admin	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Gestion d'utilisateurs: Utilisateurs et Groupes <input checked="" type="checkbox"/> Serveurs d'authentification (e.g LDAP, RADIUS) <input checked="" type="checkbox"/> Listes des Autorités de Certification, Certificats, et Certificats de Révocation <input checked="" type="checkbox"/> Règles du Pare-feu <input checked="" type="checkbox"/> Planifications du Pare-feu <input checked="" type="checkbox"/> alias du Pare-feu <input checked="" type="checkbox"/> Configuration NAT <input checked="" type="checkbox"/> Configuration IPsec <input checked="" type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync) <input checked="" type="checkbox"/> Paramètres du serveur DHCP <input checked="" type="checkbox"/> Paramètres du serveur WoL <input checked="" type="checkbox"/> Configuration des routes statiques <input checked="" type="checkbox"/> Adresses IP virtuel <input checked="" type="checkbox"/> Configuration du régulateur de flux <input checked="" type="checkbox"/> Configuration des limitations du régulation du trafic <input checked="" type="checkbox"/> Configurations du DNS Forwarder et du DNS Resolver <input checked="" type="checkbox"/> Portail captif <input checked="" type="checkbox"/> Toggle All

Je mets l'IP du pfsenseSlave ensuite je précise encore l'IP du pare-feu slave mais pour synchroniser toute la configuration de tout ce que j'ai coché

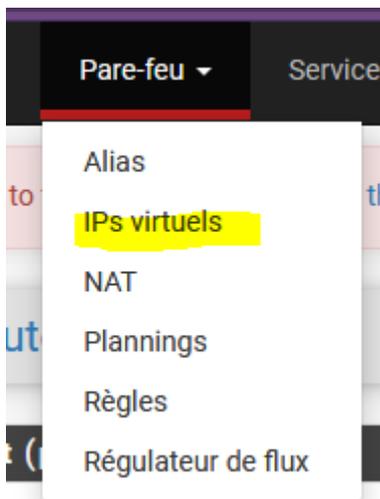
Pour le routeur slave

Je ne configure que la partie « pfsync » et non la partie « XMLRPC »

Comme ceci je précise l'ip du routeur master

Paramètres de synchronisation d'état (pfsync)	
Etat de la synchronisation	<input checked="" type="checkbox"/> 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	<input type="text" value="LAN"/> 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.
IP de synchronisation pfsync du pair	<input type="text" value="192.168.1.244"/> Le réglage de cette option obligera Pfsync à synchroniser sa table d'état avec cette adresse IP. La sélection par défaut est multicast dirigé.

Ensuite sur les deux routeurs je réalise la même configuration en me rendant dans le menu des IP virtuelles, la configuration sera automatiquement répliquer



Pare-feu / IPs virtuels / Modifier ?

Modifier l'IP virtuelle

Type Alias IP CARP Mandataire (proxy) ARP Autre

Interface LAN

Type d'adresse Adresse unitaire

Adresse(s) 192.168.1.245 / 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. Confirmer

Groupe VHID 1
Entrez le nom du groupe VHID qui sera partagé.

Fréquence d'annonce 1 Base 0 Blais
La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.

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

Je définis ici le type de protocole pour gérer cette IP virtuelle

L'adresse virtuelle qui sera utilisé ainsi que son masque

Le groupe VHID (un groupe différent par interface)

La fréquence d'annonce et la description

Lorsque je regarde l'état CARP sur les deux machines je vois ceci

Sur le master :

Interfaces CARP		
Interface CARP	adresse IP virtuelle	État
LAN@1	192.168.1.245/24	MASTER

Noeuds pfSync

noeuds pfSync:

```
1be73802
c600d8d7
fbc22bd1
```

Sur le slave :

Interfaces CARP		
Interface CARP	adresse IP virtuelle	État
LAN@1	192.168.1.245/24	BACKUP

Noeuds pfSync
noeuds pfSync:
1be73802
bb6e6849
c600d8d7
fbcc22bd1

Le ping vers l'IP fonctionne

```
64 bytes from 192.168.1.245: icmp_seq=124 ttl=64 time=0.229 ms
64 bytes from 192.168.1.245: icmp_seq=125 ttl=64 time=0.251 ms
64 bytes from 192.168.1.245: icmp_seq=126 ttl=64 time=0.197 ms
64 bytes from 192.168.1.245: icmp_seq=127 ttl=64 time=0.175 ms
64 bytes from 192.168.1.245: icmp_seq=128 ttl=64 time=0.208 ms
64 bytes from 192.168.1.245: icmp_seq=129 ttl=64 time=0.229 ms
64 bytes from 192.168.1.245: icmp_seq=130 ttl=64 time=0.213 ms
```

J'ai désactivé le protocole CARP sur le pfsense MASTER et voici le résultat sur le pfsense SLAVE il est passé master automatiquement

Interfaces CARP		
Interface CARP	adresse IP virtuelle	État
LAN@1	192.168.1.245/24	MASTER

Le ping passe toujours

```
64 bytes from 192.168.1.245: icmp_seq=124 ttl=64 time=0.229 ms
64 bytes from 192.168.1.245: icmp_seq=125 ttl=64 time=0.251 ms
64 bytes from 192.168.1.245: icmp_seq=126 ttl=64 time=0.197 ms
64 bytes from 192.168.1.245: icmp_seq=127 ttl=64 time=0.175 ms
64 bytes from 192.168.1.245: icmp_seq=128 ttl=64 time=0.208 ms
64 bytes from 192.168.1.245: icmp_seq=129 ttl=64 time=0.229 ms
64 bytes from 192.168.1.245: icmp_seq=130 ttl=64 time=0.213 ms
```