NSRP Firewall - HA

lundi 5 décembre 2022 15:42

Vérification des prérequis

Version FW-1 (Technobel 1876 SN:0185042010000315)

Current Firmware Version: 6.3.0r16.0 (Firewall+VPN)

Version FW-2 (Technobel 1877 SN:0185042010000320)

Current Firmware Version: 6.3.0r16.0 (Firewall+VPN)

Note : On a configuré le NTP sur chacun des Firewalls pour éviter des problèmes de synchronisation.

Configuration des interfaces

Set interface ethernet0/2 zone untrust
Set interface ethernet0/0 zone trust
Set interface ethernet0/2 ip 10.10.6.181/24
Set interface ethernet0/0 ip 10.0.10.1/24
Set interface ethernet0/3 zone HA

Note : La zone trust correspond à notre LAN, le zone untrust correspond au WAN et la zone HA sert à la communication entre les deux Firewalls pour le failover.

Get interface pour vérifier

```
A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name           IP Address                      Zone        MAC
 State VSD
eth0/0         10.0.10.1/24                    Trust       2c6b.f56c.e580
   D   -
eth0/1         0.0.0.0/0                       DMZ         2c6b.f56c.e585
   D   -
eth0/2         10.10.6.181/24                  Untrust     2c6b.f56c.e586
   D   -
eth0/3         0.0.0.0/0                       HA          2c6b.f56c.e587
   D   -
```

Création du cluster NSRP

Set nsrp cluster id 1
Set nsrp cluster name Prod_Cluster

Get nsrp pour vérifier

```
cluster info:
cluster id: 1, name: Prod_Cluster
local unit id: 7136640
active units discovered:
index: 0, unit id:   7136640, ctrl mac: ffffffffffff, data mac: ffffffffffff
total number of units: 1
```

Note : Les ID et noms doivent être identiques.

Configuration du monitoring des interfaces

Set nsrp monitor interface eth0/2
Set nsrp monitor interface eth0/0

Note : monitorer les interfaces permet le basculement automatique entre les Firewalls dans l'éventualité où une interface est down. Par défaut, le trafic est redirigé lorsqu'un nœud est éteint.

NTP

Set ntp no-ha-sync

Note : cette étape est facultative si le NTP est configuré en amont.

Configuration basique du Firewall Backup

Set interface ethernet0/3 zone HA
Set nsrp cluster id 1
Set nsrp cluster name Prod_Cluster
Set nsrp monitor interface eth0/0

Set nsrp monitor interface eth0/2
Set ntp no-ha-sync

Synchronisation de la configuration sur le Firewall Backup

Branchement d'un câble entre les deux Firewalls (eth 0/3 et eth0/3)
Exec nsrp sync global-config save

```
Prod_Cluster:SSG140(I)-> exec nsrp sync global-config save
Prod_Cluster:SSG140(I)-> load peer system config to save
Save global configuration successfully.
Continue to save local configurations ... Save local configuration successfully.
done.
Please reset your box to let cluster configuration take effect!
```

Reset
N
y

```
Prod_Cluster:SSG140(I)-> reset
Configuration modified, save? [y]/n n
System reset, are you sure? y/[n] y
In reset ...
```

Synchronisation RTO

Après le reboot du Firewall Backup, sur le Firewall Master

Set nsrp rto-mirror sync
Set nsrp rto-mirror route

```
Prod_Cluster:SSG140(I)-> set nsrp rto-mirror sync
Prod_Cluster:SSG140(I)-> Begin to sync all run-time-object to peer ...Received a
ll run-time-object from peer.

Done
configuration in sync
```

Priority Preempt

Sur le Firewall Master

Set nsrp vsd-group id 0 priority 50
Set nsrp vsd-group id 0 preempt

Sur le Firewall Backup

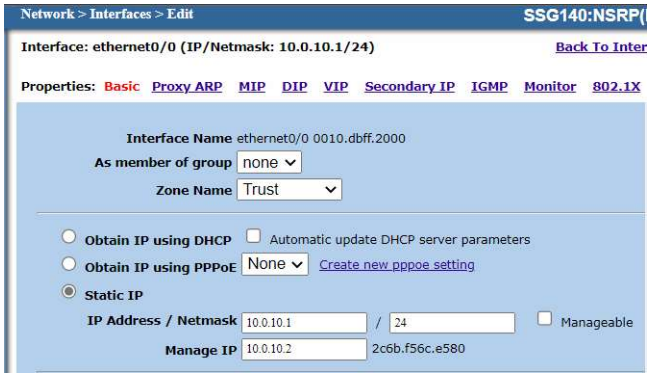
Set nsrp vsd-group id 0 priority 100

Note : Cela permet de définir quel Firewall sera priorisé. Si le Firewall Master tombe, le Backup prend le relais et devient Master jusqu'au rétablissement du Firewall avec la priorité la plus basse.
NB : la valeur par défaut est 100 mais nous préférons fixer la valeur.

Configuration des adresses de Management

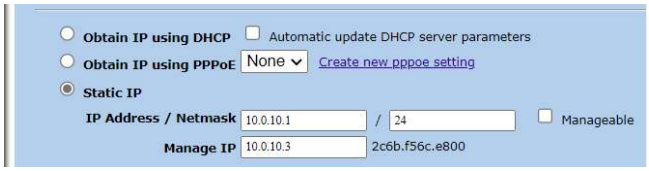
Sur le Firewall Master

Set interface e0/0 manage-ip 10.0.10.2

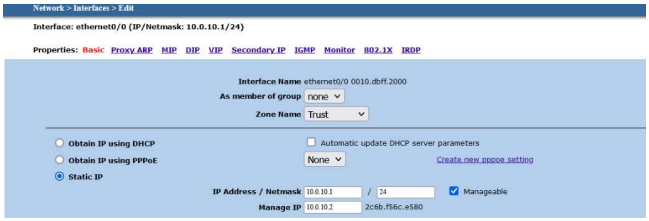


Sur le Firewall Backup

Set interface e0/0 manage-ip 10.0.10.3



Note : Cette adresse Manage IP nous permet de rentrer dans les interfaces des deux Firewalls individuellement contrairement à l'adresse 10.0.10.1 qui correspond à la VIP du cluster. Il faut cocher la case "Manageable" pour pouvoir se connecter sur l'interface en 10.0.10.1 en plus des adresses Manage IP.



Vérification de la synchronisation

Firewall Backup
set nsrp vsd-group id 0 monitor interface ethernet0/2
set nsrp vsd-group id 0 monitor interface ethernet0/0
set nsrp vsd-group id 1 monitor interface ethernet0/2
set nsrp vsd-group id 1 monitor interface ethernet0/0

Set nsrp rto-mirror sync

Firewall Master
set nsrp vsd-group id 0 monitor interface ethernet0/2
set nsrp vsd-group id 0 monitor interface ethernet0/0
set nsrp vsd-group id 1 monitor interface ethernet0/2
set nsrp vsd-group id 1 monitor interface ethernet0/0

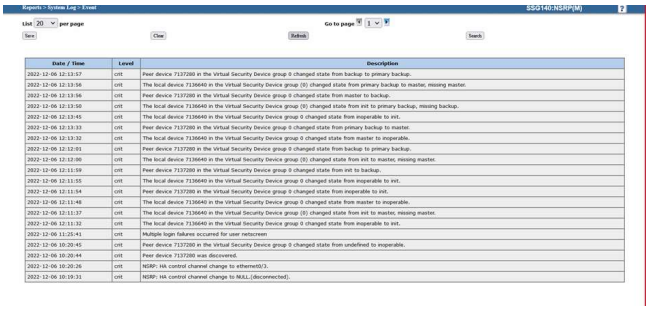
Set nsrp rto-mirror sync
Exec nsrp sync global-config check-sum

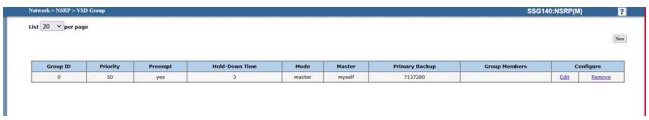
```
Prod_Cluster:SSG140(M)-> Exec nsrp sync global-config check-sum
Prod_Cluster:SSG140(M)-> configuration in sync
```

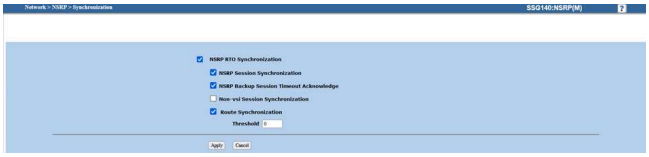
Vérification du Cluster

Sur le Firewall Master

Vérifier si on identifie bien tous les ID.







Set nsrp rto-mirror sync

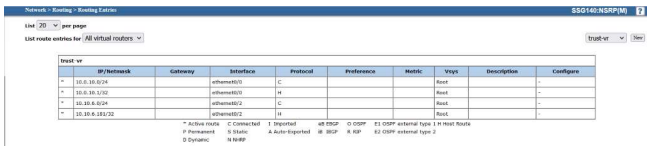
Get config

```
set nsrp rto-mirror sync
set nsrp rto-mirror route
set nsrp rto-mirror session ageout-ack
```

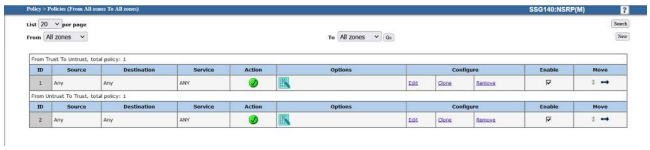
Batterie de tests

Eléments configurés en vue de réaliser la batterie de tests pour valider le failover et le monitoring du cluster.

Routes



Rules



Adresse IP de la SVI sur le switch dans le LAN (zone Trust)

```
Switch#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.0.10.200     YES manual up                    up
```

Configuration IP du poste client dans le WAN (zone Untrust)

```
Carte Ethernet Ethernet - Juniper 06 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6. . . . . . . . . . . . . .: 2001:db8:acad:caff::3
   Adresse IPv6 de liaison locale. . . . .: fe80::40e4:900c:25d0:b93a%10
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.6.189
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : fe80::1%10
                                            10.10.6.181
```

Ping de l'interface zone Untrust depuis le poste client

```
C:\Users\Student>ping 10.10.6.181

Envoi d'une requête 'Ping'  10.10.6.181 avec 32 octets de données :
Réponse de 10.10.6.181 : octets=32 temps<1ms TTL=64
Réponse de 10.10.6.181 : octets=32 temps<1ms TTL=64
Réponse de 10.10.6.181 : octets=32 temps<1ms TTL=64
Réponse de 10.10.6.181 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.10.6.181:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Arrêt du Firewall Master pendant le ping du poste client vers la SVI du switch

```
C:\Users\Student>ping 10.0.10.200 -t

Envoi d'une requête 'Ping'  10.0.10.200 avec 32 octets de données :
Réponse de 10.0.10.200 : octets=32 temps=4 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Délai d'attente de la demande dépassé.
Réponse de 10.0.10.200 : octets=32 temps=4 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=5 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254

Statistiques Ping pour 10.0.10.200:
    Paquets : envoyés = 8, reçus = 7, perdus = 1 (perte 12%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 5ms, Moyenne = 3ms
```

Note : On perd un paquet et le failover reprend immédiatement sur le Firewall Backup.

Démarrage du Firewall Master pendant le ping

```
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Délai d'attente de la demande dépassé.
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=7 ms TTL=254

Statistiques Ping pour 10.0.10.200:
    Paquets : envoyés = 96, reçus = 95, perdus = 1 (perte 1%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 20ms, Moyenne = 2ms
```

Note : On perd de nouveau un paquet pendant le changement de master node.

Débranchement du câble reliant le Firewall Master au switch pendant le ping pour tester le monitoring

```
C:\Users\Student>ping 10.0.10.200 -t

Envoi d'une requête 'Ping'  10.0.10.200 avec 32 octets de données :
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=4 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=3 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254

Statistiques Ping pour 10.0.10.200:
    Paquets : envoyés = 20, reçus = 20, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 4ms, Moyenne = 2ms
```

Note : On ne perd aucun paquet, le basculement est immédiat.

Rebranchement du câble reliant le Firewall Master au switch

```
C:\Users\Student>ping 10.0.10.200 -t

Envoi d'une requête 'Ping'  10.0.10.200 avec 32 octets de données :
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=4 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=2 ms TTL=254
Réponse de 10.0.10.200 : octets=32 temps=1 ms TTL=254

Statistiques Ping pour 10.0.10.200:
    Paquets : envoyés = 19, reçus = 14, perdus = 5 (perte 26%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 4ms, Moyenne = 1ms
```

Note : plusieurs paquets ont été perdu pendant la négociation entre les interfaces.