

# NSRP Firewall - HA

lundi 5 décembre 2022 15:42

## Vérification des prérequis

Version FW-1 (Technobel 1876 SN:0185042010000315)

```
Configuration > Update > ScreenOS/Keys SSG140:NSRP(M)
```

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

Version FW-2 (Technobel 1877 SN:0185042010000320)

```
Configuration > Update > ScreenOS/Keys SSG140
```

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: ffffffff, data mac: ffffffff
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

The screenshot shows the configuration page for the Management IP on the Master Firewall. The interface is titled "Network > Interfaces > Edit" and "SSG140: NSRP". The selected interface is "ethernet0/0 (IP/Netmask: 10.0.10.1/24)". The "Basic" tab is active, showing the following settings: Interface Name: ethernet0/0 0010.dbff.2000; As member of group: none; Zone Name: Trust; Obtain IP using DHCP: none; Obtain IP using PPPoE: None; Static IP: selected; IP Address / Netmask: 10.0.10.1 / 24; Manageable: unchecked; Manage IP: 10.0.10.2, 2c6b.f56c.e580.

Sur le Firewall Backup

Set interface e0/0 manage-ip 10.0.10.3

The screenshot shows the configuration page for the Management IP on the Backup Firewall. The interface is titled "Network > Interfaces > Edit" and "SSG140: NSRP". The selected interface is "ethernet0/0 (IP/Netmask: 10.0.10.1/24)". The "Basic" tab is active, showing the following settings: Interface Name: ethernet0/0 0010.dbff.2000; As member of group: none; Zone Name: Trust.

Obtain IP using DHCP  Automatic update DHCP server parameters  
 Obtain IP using PPPoE  [Create new pppoe setting](#)  
 Static IP  
 IP Address / Netmask  /   Manageable  
 Manage IP

**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.

Network > Interfaces > Edit

Interface: ethernet0/0 (IP/Netmask: 10.0.10.1/24)

Properties: Basic Proxy ARP MIP DIP VIP Secondary IP IGMP Monitor 802.1X IRDP

Interface Name: ethernet0/0 0010.dbff.2000  
 As member of group: none  
 Zone Name: Trust

Obtain IP using DHCP  Automatic update DHCP server parameters  
 Obtain IP using PPPoE  [Create new pppoe setting](#)  
 Static IP  
 IP Address / Netmask  /   Manageable  
 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.

Network > NSRP > Cluster SSG140-NSRP(M)

NSRP Protocol Version: 2.0

Cluster ID 1  
 Not in Cluster  
 Local ID: 7137280 Active Units Discovered: 7136640 7137280  
 Number of Gratuitous ARPs to Retain: 0  
 NSRP Authentication Password  
 NSRP Encryption Password  
 Apply Cancel

Network > System Log > Event SSG140-NSRP(M)

List 20 per page

Date / Time	Level	Description
2022-12-06 12:13:17	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from backup to primary backup.
2022-12-06 12:13:16	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from primary backup to master, missing master.
2022-12-06 12:13:16	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from master to backup.
2022-12-06 12:13:16	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from not in primary backup, missing backup.
2022-12-06 12:12:45	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from inoperable to not in.
2022-12-06 12:13:13	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from primary backup to master.
2022-12-06 12:13:12	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from master to inoperable.
2022-12-06 12:12:45	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from backup to primary backup.
2022-12-06 12:13:08	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from not in master, missing master.
2022-12-06 12:13:09	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from not in to backup.
2022-12-06 12:11:51	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from inoperable to not in.
2022-12-06 12:11:54	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from inoperable to not in.
2022-12-06 12:11:48	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from master to inoperable.
2022-12-06 12:11:27	OK	Peer device 7137280 in the Virtual Security Device group 01 changed state from not in to master, missing master.
2022-12-06 12:11:32	OK	The local device 7136640 in the Virtual Security Device group 01 changed state from inoperable to not in.
2022-12-06 11:21:41	OK	Multiple login failures occurred for user returnren
2022-12-06 10:20:45	OK	Peer device 7137280 in the Virtual Security Device group 0 changed state from undefined to inoperable.
2022-12-06 10:20:44	OK	Peer device 7137280 was discovered.
2022-12-06 10:20:28	OK	NSRP: HA control channel change to ethernet0/0.
2022-12-06 10:19:31	OK	NSRP: HA control channel change to HA0_1(disconnected).

Network > NSRP > VSD Group SSG140-NSRP(M)

List 20 per page

Group ID	Priority	Preempt	Hold-Down Time	Mode	Master	Primary Backup	Group Members	Configure
0	50	yes	3	master	myself	7137280		Edit Remove

Network > NSRP > Synchronization SSG140-NSRP(M)

NSRP RTO Synchronization  
 NSRP Session Synchronization  
 NSRP Backup Session Timeout Acknowledgment  
 Non-vsd Session Synchronization  
 Route Synchronization  
 Master: 0  
 Apply Cancel

```
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

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

Routes

Route ID	IP/Network	Gateway	Interface	Protocol	Preference	Metric	Type	Description	Configure
1	10.0.10.0/24		ethernet0/0	C			Host		-
2	10.0.10.1/32		ethernet0/0	H			Host		-
3	10.0.10.2/24		ethernet0/0	C			Host		-
4	10.0.10.255/24		ethernet0/0	H			Host		-

Rules

ID	Source	Destination	Service	Action	Options	Configure	Enable	Preced
1	Any	Any	ANY	Deny	Log	LOG, CLASH, SALTIC	IP	1
2	Any	Any	ANY	Deny	Log	LOG, CLASH, SALTIC	IP	2

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=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=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.