

# HA FortiGate

GUIDE EXPRESS POUR ADMINS  
PRESSÉS (ET STRESSÉS)



Assure la continuité même  
quand tout plante

---

2024/2025

---

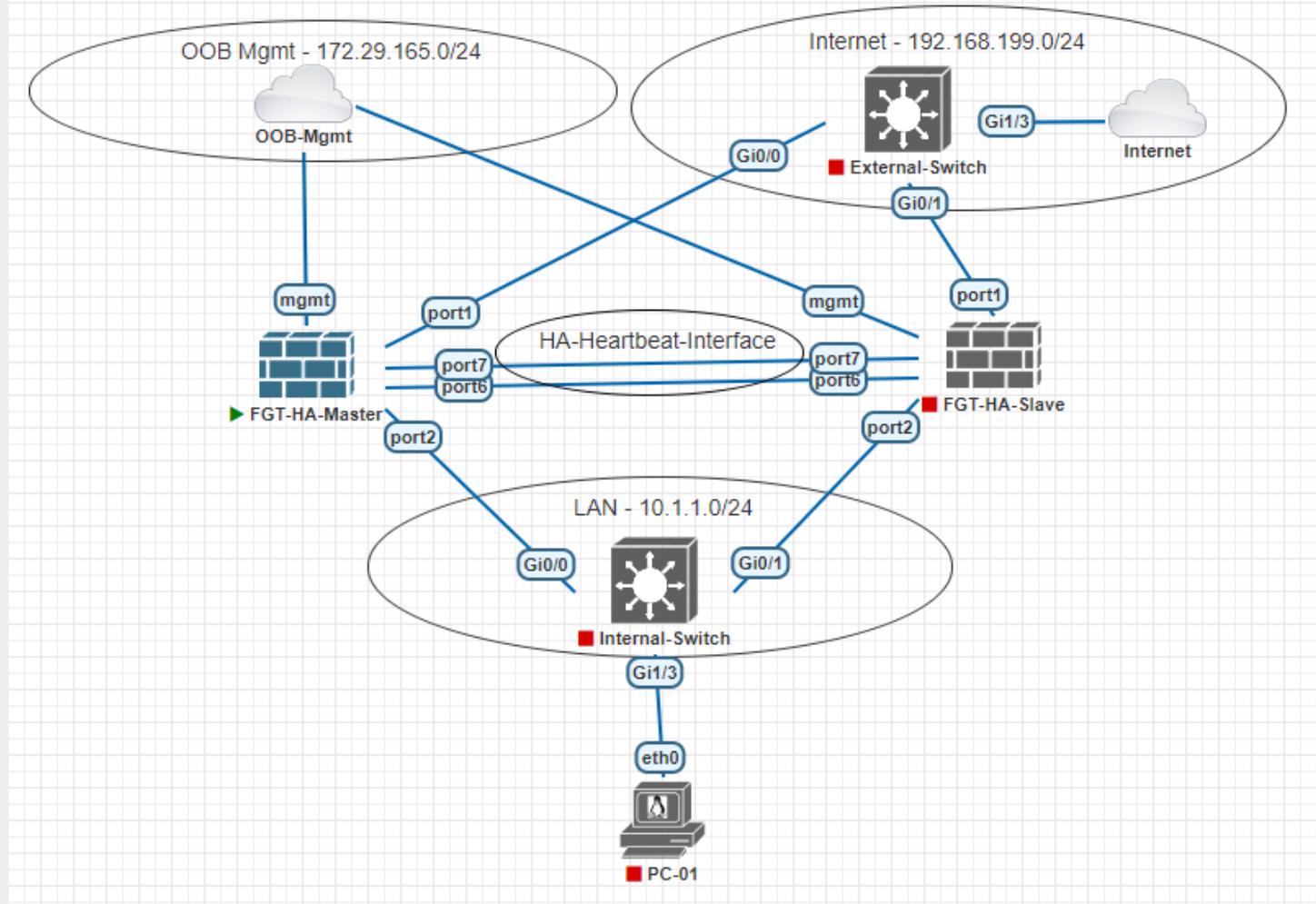
# **CONFIGURATION DE CLUSTER HAUTE DISPONIBILITÉ (HA) AVEC PARE-FEU FORTIGATE (ACTIF-PASSIF)**

---



Dans ce tutoriel, nous allons apprendre à mettre en place un cluster de haute disponibilité (HA) en mode actif-passif à l'aide de deux pare-feu FortiGate. Avant de commencer la configuration, nous présenterons d'abord la topologie retenue, afin de bien comprendre l'architecture sur laquelle reposera notre scénario.

| Network  | Master           | Slave            | Cluster          |
|----------|------------------|------------------|------------------|
| OOB Mgmt | 172.29.165.81/24 | 172.29.165.82/24 | X                |
| Internet | X                | X                | 192.168.199.0/24 |
| Lan      | X                | X                | 10.1.1.0/24      |



## 01 - Topologie du réseau HA

Ayons une brève idée de la terminologie -

**Interface HA-Heartbeat** : grâce à ces interfaces, les pare-feu Fortigate communiquent entre eux via FGCP (Fortigate Clustering Protocol) et gèrent toutes les tâches de gestion de cluster. Par exemple, la synchronisation de la configuration, la récupération de session, etc. Dans notre configuration, nous avons réservé deux interfaces : les ports 7 et 6. Une seule interface Heartbeat est active à la fois. L'autre interface Heartbeat est utilisée en veille. De plus, aucune adresse IP n'est requise ; FGCP s'en charge.

**Pare-feu maître/esclave** : le pare-feu responsable de la transmission du trafic est appelé maître. L'autre pare-feu, en veille et prenant le relais en cas de défaillance du maître, est appelé esclave. C'est pourquoi nous avons choisi de qualifier notre configuration d'active-passive.

**Interfaces de gestion hors bande** : la configuration d'un cluster Fortigate présente une différence majeure par rapport aux implémentations haute disponibilité d'autres fournisseurs. Lors de la création d'un cluster, une seule adresse IP est partagée par ses membres . Le concept d'adresse IP virtuelle, comme c'était le cas avec VRRP/HSRP, n'est plus utilisé. Pour pallier ce problème et gérer les membres de notre cluster séparément, nous utiliserons une interface dédiée à la gestion afin de pouvoir atteindre les deux membres individuellement.

**Adresse IP Internet/LAN** : comme indiqué précédemment, lorsqu'un cluster à deux nœuds est opérationnel, une seule adresse IP est utilisée pour la connectivité interne/externe. Cette adresse IP est attribuée uniquement à l'unité maître. Dans notre cas, Internet : 192.168.199.91/24 et LAN : 10.1.1.1/24. En cas de panne de l'unité maître, ces adresses IP sont réattribuées à l'unité esclave, qui assume alors le rôle de maître. Il n'existe pas de concept d'adresse IP unique pour chaque unité ni d'adresse IP virtuelle pour le même sous-réseau (3 adresses IP), ce qui est courant avec des protocoles tels que VRRP/HSRP. Avec le protocole FGCP, une seule adresse IP d'interface est nécessaire, attribuée à l'unité maître/active du cluster.



## Configuration de la connectivité physique

Lors de la connexion physique des membres d'un cluster Fortigate au réseau (câblage réseau, etc.), il est important de préparer et de configurer les commutateurs avec les VLAN ou autres éléments requis pour les deux nœuds du cluster. Ensuite, point important : connectez uniquement le nœud Fortigate maître/actif au réseau. Ensuite, configurez tout le pare-feu : configuration de l'interface, politiques de pare-feu, SNMP, etc. Ensuite, connectez l'unité esclave/passive. Dans l'unité passive, configurez uniquement l'interface de gestion hors bande et les paramètres du cluster (comme l'interface Heartbeat, la priorité du cluster, etc.). Les membres du cluster se trouveront alors et l'unité esclave/passive synchronisera sa configuration avec celle de l'unité maître/active (autres adresses IP d'interface, politiques de pare-feu, etc.). Ces configurations seront désactivées dans l'unité esclave jusqu'à la défaillance de l'unité maître. Dès que l'unité maître actuelle tombe en panne, l'unité esclave reprendra la responsabilité du maître et activera les configurations désactivées.

## Configuration du pare-feu maître/actif

Nous avons configuré nos commutateurs pour les pare-feu actifs/passifs et connecté physiquement uniquement le pare-feu maître au réseau. Nous allons maintenant commencer sa configuration via l'interface OOB-Mgmt.

Configurons le port « mgmt » du pare-feu afin que nous puissions l'atteindre via le réseau.

FGT-HA-Master (mgmt) # afficher  
interface du système de configuration  
modifier « mgmt »  
!!! Attribuer une adresse IP à l'interface  
définir l'adresse IP 172.29.165.81 255.255.255.0  
!!! Activer l'accès à la gestion  
définir allowaccess ping https ssh fgfm  
type d'ensemble physique  
ensemble dédié à la gestion  
définir l'index snmp 1  
suivant  
fin

CLI

Nous pouvons maintenant accéder à notre pare-feu en utilisant <https://172.29.165.81> à partir d'un navigateur Web.

Après vous être connecté au pare-feu à partir de l'interface Web, nous avons configuré les éléments suivants pour le cluster HA :

The screenshot shows the FortiOS VM64-KVM interface with the title "FortiOS VM64-KVM FGT-HA-Master". The left sidebar is titled "HA" and includes options like "SNMP", "Replacement Messages", "FortiGuard", "Feature Visibility", "Certificates", "Policy & Objects", "Security Profiles", "VPN", "User & Authentication", "WiFi & Switch Controller", and "Log & Report". The main panel is titled "High Availability" and contains the following configuration:

- Mode:** Active-Passive (selected)
- Device priority:** 200
- Cluster Settings:**
  - Group name:** Cluster-Fgt
  - Password:** [REDACTED] Change
  - Session pickup:** Off
- Monitor interfaces:** [Empty]
- Heartbeat interfaces:** port6, port7 (highlighted with a yellow circle)
- Heartbeat Interface Priority:**
  - port6: 200
  - port7: 100
- Management Interface Reservation:**
  - Interface:** mgmt
  - Gateway:** 172.29.165.1
  - Destination subnet:** 0.0.0.0/0
- Unicast Heartbeat:** Off

At the bottom right are "OK" and "Cancel" buttons.

## 02 - Configuration HA principale

Les options sélectionnées ci-dessus sont simples. Nous avons sélectionné Actif-Passif, avec une priorité de périphérique de 200 (le périphérique de priorité supérieure devient actif). Nous devons définir un nom et un mot de passe pour le groupe de clusters ; dans notre cas, Cluster-Fgt/test123. Nous avons ensuite sélectionné les ports 6 et 7 comme interfaces de pulsation et attribué au port 6 une priorité plus élevée afin que seule cette interface soit utilisée pour FGCP en fonctionnement normal, tandis que le port 7 servira d'interface de pulsation de secours. Nous souhaitons gérer et atteindre notre cluster individuellement ; l'interface de gestion connectée au réseau OOB-Mgmt est donc réservée à la gestion.

Une chose importante que nous ne pouvons pas faire depuis l'interface web est d'attribuer un identifiant de groupe à notre cluster . Cette configuration est indispensable pour éviter tout conflit d'adresse MAC. Par exemple, si une autre personne connectée à notre FAI tente d'exécuter un cluster Fortigate, le risque est grand que notre cluster et celui de l'autre utilisent les mêmes adresses MAC virtuelles, ce qui peut engendrer un conflit d'adresses MAC. Par mesure de sécurité, il est donc conseillé de toujours configurer un identifiant de groupe lors de la configuration d'un cluster Fortigate. Examinons la configuration de notre cluster depuis l'interface de ligne de commande (CLI) avec la commande group-id ajoutée :

```
FGT-HA-Master (ha) # afficher
système de configuration ha
définir l'ID de groupe 251
définir le nom du groupe « Cluster-Fgt »
définir le mode ap
définir le mot de passe ENC JIWhU7dD+oHOU08gfRDEGdr0tw3fIE
définir hbdev "port6" 200 "port7" 100
activer ha-mgmt-status
configuration des interfaces ha-mgmt
    modifier 1
        définir l'interface « mgmt »
        définir la passerelle 172.29.165.1
    suivant
fin
définir le remplacement désactiver
définir la priorité 200
fin
```

Voilà, nous avons terminé la configuration de l'unité Master.

## Configuration du pare-feu esclave/passif

Nous allons maintenant connecter le pare-feu esclave au réseau. Nous allons uniquement configurer l'interface de gestion et les paramètres du cluster ; rien d'autre.

```
FGT-HA-Slave (gestion) # afficher
interface du système de configuration
modifier « mgmt »
définir l'adresse IP 172.29.165.82 255.255.255.0
définir allowaccess ping https ssh fgfm
type d'ensemble physique
ensemble dédié à la gestion
définir l'index snmp 1
suivant
fin
```

FortiOS VM64-KVM FGT-HA-Slave

Dashboard > High Availability

Mode: Active-Passive  
Device priority: 100

Cluster Settings

Group name: Cluster-Fgt  
Password: \*\*\*\*\* Change

Session pickup:

Monitor interfaces: +

Heartbeat interfaces: port6, port7 x

Heartbeat Interface Priority:

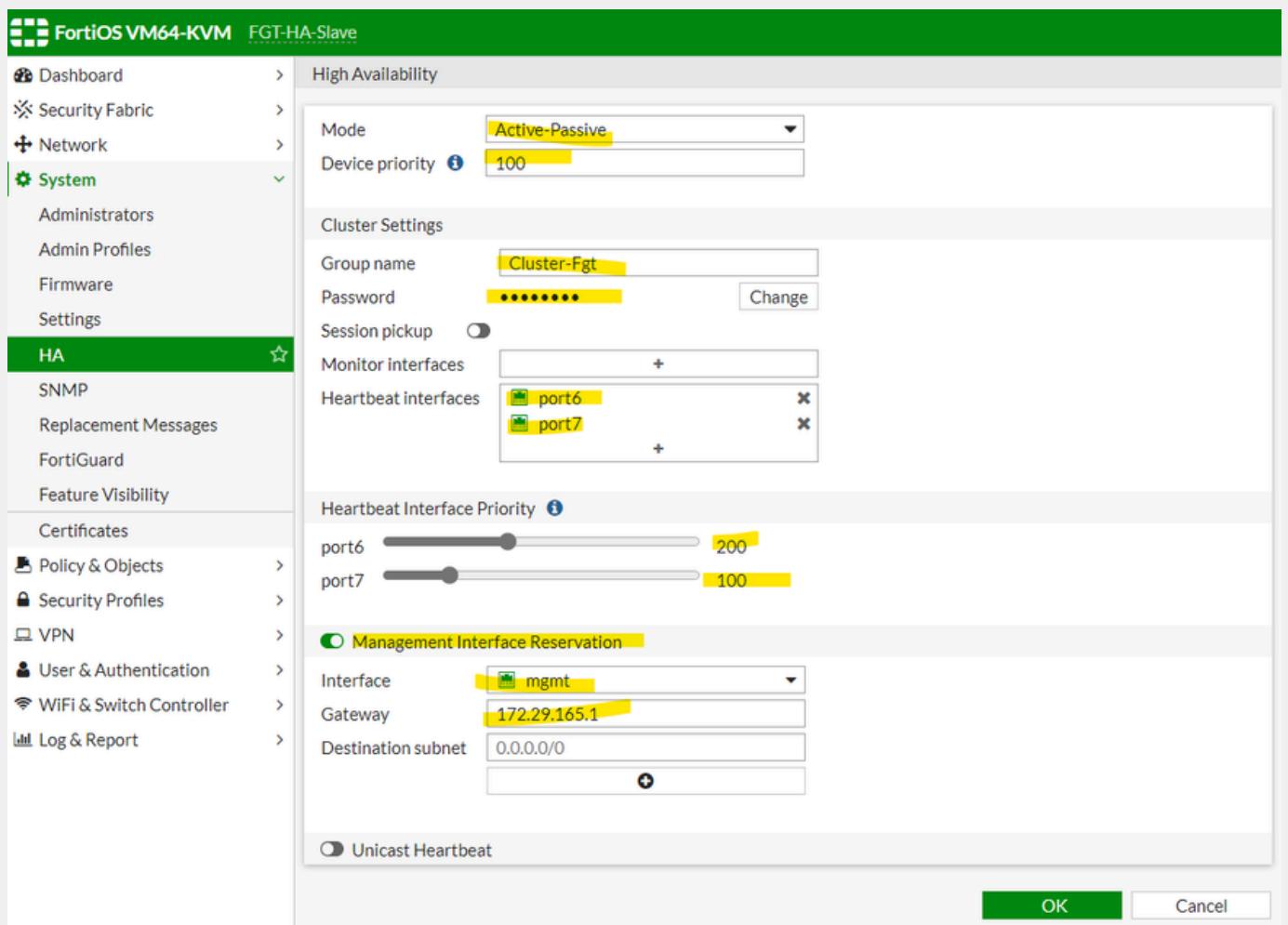
port6: 200  
port7: 100

Management Interface Reservation:

Interface: mgmt  
Gateway: 172.29.165.1  
Destination subnet: 0.0.0.0/0

Unicast Heartbeat:

OK Cancel



## 03 - Configuration HA esclave



Tous les paramètres du cluster sont les mêmes pour l'esclave ; nous lui attribuons simplement une faible priorité (100) afin qu'il devienne un nœud passif dans notre cluster.

```
FGT-HA-Slave (ha) # afficher
système de configuration ha
définir l'ID de groupe 251
définir le nom du groupe « Cluster-Fgt »
définir le mode ap
définir le mot de passe ENC kYemyzXqFZzHMc3VrG6jM7xnvqnCBU
définir hbdev "port6" 200 "port7" 100
activer ha-mgmt-status
configuration des interfaces ha-mgmt
    modifier 1
        définir l'interface « mgmt »
        suivant
    fin
    définir le remplacement désactiver
    définir la priorité 100
fin
```

## Synchronisation HA

Après la configuration ci-dessus sur les deux nœuds, ceux-ci se trouveront en communiquant via le protocole FGCP via l'interface Heartbeat. Le nœud esclave tentera ensuite de synchroniser sa configuration avec le nœud maître. Ce comportement est observable depuis la console CLI du nœud esclave.

```
FGT-HA-Slave # les fichiers externes du secondaire ne sont pas
synchronisés avec ceux du primaire, séquence : 0. (type CERT_LOCAL)
les fichiers externes du secondaire ne sont pas synchronisés avec ceux du
primaire, séquence : 1. (type CERT_LOCAL)
les fichiers externes du secondaire ne sont pas synchronisés avec ceux du
primaire, séquence : 2. (type CERT_LOCAL)
le secondaire a réussi à synchroniser les fichiers externes avec le primaire
la configuration du secondaire n'est pas synchronisée avec celle du
primaire, séquence : 0
la configuration du secondaire n'est pas synchronisée avec celle du
primaire, séquence : 1
la configuration du secondaire n'est pas synchronisée avec celle du
primaire, séquence : 2
le secondaire commence à se synchroniser avec le primaire
déconnecter tous les utilisateurs administrateurs
```

La synchronisation des configurations des nœuds prend un certain temps. Une fois la synchronisation terminée, nous pouvons le constater à la fois via l'interface web et la ligne de commande.

|               | Status  | Priority | Hostname      | Serial No.       | Role      |
|---------------|---|----------|---------------|------------------|-----------|
| FGT-HA-Master | <span style="color: green;">✓ Synchronized</span> | 200      | FGT-HA-Master | FOSVM1KIV5CQ2E48 | Primary   |
| FGT-HA-Slave  | <span style="color: green;">✓ Synchronized</span> | 100      | FGT-HA-Slave  | FOSVM12EEYRK_Q57 | Secondary |

## 04 - État de synchronisation HA

Depuis CLI -

```

FGT-HA-Master # get system ha status
HA Health Status: OK
Model: FortiOS-VM64-KVM
Mode: HA A-P
Group: 251
Debug: 0
Cluster Uptime: 4 days 0:18:10
Cluster state change time: 2021-02-16 01:34:53
ses_pickup: disable
override: disable
Configuration Status:
  FOSVM1KIV5CQ2E48(updated 3 seconds ago): in-sync
  FOSVM12EEYRK_Q57(updated 4 seconds ago): in-sync
System Usage stats:
  FOSVM1KIV5CQ2E48(updated 3 seconds ago):
    sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%,
    memory=38%
  FOSVM12EEYRK_Q57(updated 4 seconds ago):
    sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%,
    memory=35%
Primary : FGT-HA-Master , FOSVM1KIV5CQ2E48, HA cluster index = 0
Secondary : FGT-HA-Slave , FOSVM12EEYRK_Q57, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FOSVM1KIV5CQ2E48, HA operating index = 0
Secondary: FOSVM12EEYRK_Q57, HA operating index = 1

```

## Configuration de la connectivité LAN/Internet pour le réseau

Notre cluster est maintenant synchronisé. Nous allons configurer le reste du réseau : les politiques LAN, Internet et pare-feu afin que les périphériques LAN puissent se connecter à Internet. Pour ce faire, nous nous connectons au nœud maître via l'interface OOB-Mgmt . Toutes les modifications apportées au nœud maître seront synchronisées avec le nœud esclave via FGCP.

Je vais maintenant configurer l'interface LAN. Le LAN fournira également les services DNS et DHCP au réseau connecté. J'afficherai la configuration depuis l'interface de ligne de commande, même si j'ai configuré les paramètres depuis l'interface web.

```
FGT-HA-Master (port2) # show
config system interface
edit "port2"
set vdom "root"
set ip 10.1.1.1 255.255.255.0
set allowaccess ping https ssh
set type physical
set description "Lan"
set alias "Lan"
set device-identification enable
set snmp-index 3
next
end
```

```
FGT-HA-Master (2) # show
config system dhcp server
edit 2
set dns-service local
set default-gateway 10.1.1.1
set netmask 255.255.255.0
set interface "port2"
config ip-range
edit 1
set start-ip 10.1.1.101
set end-ip 10.1.1.200
next
end
next
end
```

```
FGT-HA-Master (dns-server) # show  
config system dns-server  
edit "port2"  
next  
end
```

Nous allons maintenant configurer l'interface Internet et une route par défaut pour sortir de cette interface.

```
FGT-HA-Master (port1) # show  
config system interface  
edit "port1"  
set vdom "root"  
set ip 192.168.199.91 255.255.255.0  
set allowaccess ping  
set type physical  
set description "Internet"  
set alias "Internet"  
set snmp-index 2  
next  
end
```

```
FGT-HA-Master (static) # show full  
config router static  
edit 1  
set status enable  
set dst 0.0.0.0 0.0.0.0  
set gateway 192.168.199.2  
set device "port1"  
next  
end
```

Il ne reste plus qu'à créer une politique de pare-feu autorisant le réseau local à accéder à Internet. Comme d'habitude, nous utiliserons une politique par zone.

```
FGT-HA-Master (zone) # show  
config system zone  
edit "Internet-Zone"  
set interface "port1"  
next  
edit "Lan-Zone"  
set interface "port2"  
next  
end
```



```
FGT-HA-Master (policy) # show
config firewall policy
edit 1
set uuid c6b37cda-7049-51eb-6807-117c3a840e60
set srcintf "Lan-Zone"
set dstintf "Internet-Zone"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set nat enable
next
end
```

Voilà, la configuration complète du réseau est terminée. Les modifications apportées au nœud maître seront automatiquement synchronisées avec le nœud esclave.

## Basculement/débogage du cluster

Nous allons maintenant essayer de faire un SSH vers 10.1.1.1/24 depuis PC-01 (10.1.1.101/24).

```
root@debian01:~# ssh admin@10.1.1.1
admin@10.1.1.1's password:
FGT-HA-Master #
```

D'après le résultat ci-dessus, nous constatons que lorsque nous nous connectons à l'adresse IP du pare-feu LAN, nous nous connectons au nœud maître, qui est actuellement le nœud actif. Notre affirmation d'utiliser une seule adresse IP est vérifiée.

Nous allons maintenant vérifier le basculement du cluster à l'aide d'une fonctionnalité appelée « **Surveillance des interfaces** ». Ainsi, lorsque le membre actif détecte une panne d'une interface surveillée, le membre passif prend en charge la transmission du trafic. Dans notre cas, nous allons surveiller notre interface LAN (port 2). Pour activer la surveillance, procédez comme suit uniquement sur le nœud maître ; l'esclave recevra cette modification via la synchronisation. Ensuite, si nous arrêtons l'interface du commutateur (commutateur interne) connectée au pare-feu maître, nous observerons un basculement du cluster. L'esclave deviendra alors le nouveau nœud actif.



## 05 - Interfaces de surveillance HA

Faisons la même vérification en exécutant un SSH vers notre pare-feu à partir du PC LAN ; cette fois, nous serons connectés au pare-feu esclave qui est désormais actif en raison d'une interface de surveillance défaillante.

```
root@debian01:~# ssh admin@10.1.1.1
admin@10.1.1.1's password:
FGT-HA-Slave #
```

La sortie du pare-feu -

```

FGT-HA-Slave # get system ha status
HA Health Status:
WARNING: FOSVM1KIV5CQ2E48 has mondev down;
Model: FortiOS-VM64-KVM
Mode: HA A-P
Group: 251
Debug: 0
Cluster Uptime: 0 days 0:42:20
Cluster state change time: 2021-02-16 04:04:44
Primary selected using:
<2024/02/16 04:04:44> FOSVM12EEYRK_Q57 is selected as the primary
because it has the least value 0 of link-failure + pingsvr-failure.
<2021/02/16 03:32:47> FOSVM1KIV5CQ2E48 is selected as the primary
because it has the largest value of override priority.
ses_pickup: disable
override: disable
Configuration Status:
FOSVM12EEYRK_Q57(updated 4 seconds ago): in-sync
FOSVM1KIV5CQ2E48(updated 1 seconds ago): in-sync
Primary : FGT-HA-Slave , FOSVM12EEYRK_Q57, HA cluster index = 1
Secondary : FGT-HA-Master , FOSVM1KIV5CQ2E48, HA cluster index = 0

```

Essayons un dernier scénario : que se passe-t-il si nous réactivons le port de commutation et que le nœud maître récupère son interface de surveillance ? Le nœud maître préemptera-t-il le nœud auxiliaire et reprendra-t-il la responsabilité du nœud actif ? La réponse par défaut est « NON » ; lorsqu'un nœud précédemment actif revient dans le cluster, il le rejoint en tant que nœud de secours. Il ne peut redevenir nœud principal qu'en cas de défaillance du nœud actif actuel. Ce choix réduit les perturbations de trafic.

```

get system ha status
HA Health Status: OK
Model: FortiOS-VM64-KVM
Mode: HA A-P
Group: 251
Debug: 0
Cluster Uptime: 0 days 0:48:33
Cluster state change time: 2021-02-16 04:04:44
Primary selected using:
<2024/02/16 04:04:44> FOSVM12EEYRK_Q57 is selected as the primary because it has the least value 0 of link-failure + pingsvr-failure.
<2021/02/16 03:32:47> FOSVM1KIV5CQ2E48 is selected as the primary because it has the largest value of override priority.
ses_pickup: disable
override: disable
Configuration Status:
FOSVM12EEYRK_Q57(updated 2 seconds ago): in-sync
FOSVM1KIV5CQ2E48(updated 4 seconds ago): in-sync
Primary : FGT-HA-Slave , FOSVM12EEYRK_Q57, HA cluster index = 1
Secondary : FGT-HA-Master , FOSVM1KIV5CQ2E48, HA cluster index = 0

```

Nous pouvons bien sûr modifier ce comportement ; si nous modifions les éléments suivants dans notre configuration de cluster :

```
FGT-HA-Slave # config system ha
```

```
FGT-HA-Slave (ha) # set override enable
```

Nous pouvons également effectuer un basculement manuel du nœud actif vers le nœud passif ; en exécutant la commande ci-dessous en mode actif -

```
FGT-HA-Slave # diagnose sys ha reset-upptime
```

Après cette commande, FGT-HA-Master sera à nouveau un nœud actif.

```
FGT-HA-Slave # get system ha status
HA Health Status: OK
Model: FortiOS-VM64-KVM
Mode: HA A-P
Group: 251
Debug: 0
Cluster Uptime: 0 days 0:54:36
Cluster state change time: 2021-02-16 04:21:42
Primary selected using:
<2024/02/16 04:21:42> FOSVM1KIV5CQ2E48 is selected as the primary because it has the largest value of override priority.
<2021/02/16 04:04:44> FOSVM12EEYRK_Q57 is selected as the primary because it has the least value 0 of link-failure + pingsvr-failure.
ses_pickup: disable
override: disable
Configuration Status:
FOSVM12EEYRK_Q57(updated 5 seconds ago): in-sync
FOSVM1KIV5CQ2E48(updated 2 seconds ago): in-sync
Secondary : FGT-HA-Slave , FOSVM12EEYRK_Q57, HA cluster index = 1
Primary : FGT-HA-Master , FOSVM1KIV5CQ2E48, HA cluster index = 0
```

## **Conclusion — HA FortiGate, l'essentiel à retenir**

Mettre vos pare-feux en HA (Active-Passive ou Active-Active) vous apporte tolérance de panne, mises à jour sans coupure, synchronisation d'état et capacité de montée en charge.

Si ce carrousel vous a été utile, laissez un commentaire avec votre contexte et repartagez le carrousel.

👉 En échange, nous vous enverrons la suite des configurations FortiGate : check-list pré-prod, schémas de câblage, commandes de vérif, runbook de bascule, bonnes pratiques (HA heartbeat, liens de failover, ARP/GRAT, STP), et pièges à éviter.

👉 Dites-nous en commentaire votre plus gros défi HA aujourd'hui, et repostez pour en faire profiter votre réseau.

