

ARCHITECTURE D'ENTREPRISE H.A

(CISCO : ROUTAGE, POLITIQUES DE SÉCURITÉ ...)

Sous le module de protocoles de sécurité & sécurité des réseaux et des communications

RÉALISER PAR :

ZAKARIA OUAHI
ADIL EL KHAIDER
JIHANE ELMOUARABIT
SANOGO CHEICKNA
BOURHAT AYMANE

ENCADRE PAR :

PR. AZOUGAGHE ALI

Année universitaire: 2024/2025

TABLE DE CONTENU

01

Haut disponibilité

02

Problématique,
solutions

03

Outils

04

Protocole

05

Technologies

06

Configuration

07

Réalisation



HAUTE DISPONIBILITÉ
H.A

HIGH AVAILABILITY

La haute disponibilité (HA) dans un réseau informatique désigne la capacité du réseau à fonctionner de manière continue et fiable, même en cas de pannes matérielles ou logicielles. Cela repose sur l'utilisation de stratégies, de protocoles et de technologies spécifiques visant à réduire les interruptions et à garantir une disponibilité optimale des services.

OBJECTIFS DE HA

FIABILITÉ ACCRUE

La haute disponibilité garantit une résilience élevée en répartissant la charge de travail entre plusieurs serveurs ou nœuds. Ainsi, en cas de défaillance d'un élément, les autres prennent automatiquement le relais pour éviter toute interruption de service.

REDONDANCE

Les systèmes conçus pour la haute disponibilité intègrent des composants redondants. Si l'un d'eux tombe en panne, un composant de secours s'active immédiatement, assurant la continuité des opérations.

TEMPS D'ARRÊT MINIMISÉ

Les architectures HA permettent de réduire considérablement, voire d'éliminer, les interruptions en redirigeant automatiquement le trafic vers des ressources disponibles, que ce soit en cas de panne ou lors de maintenances planifiées.

OBJECTIFS DE HA

PERFORMANCE AMÉLIORÉE

En distribuant la charge de travail, l'architecture HA peut offrir des performances plus constantes même en cas de fluctuations de la demande.

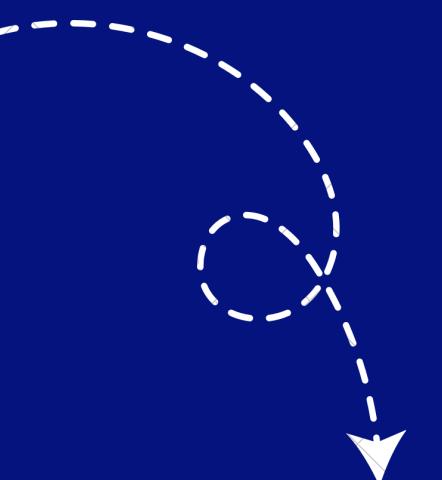
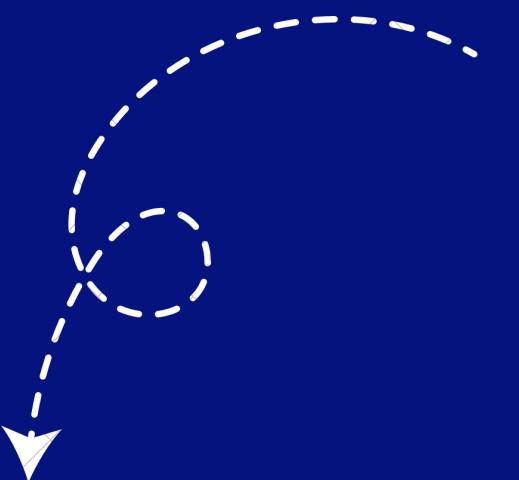
PLAN DE REPRISE APRÈS SINISTRE (PRAS)

Elle facilite la mise en place de plans de continuité des activités en assurant la disponibilité des services même en cas de sinistre majeur.

AMÉLIORATION DE LA TOLÉRANCE AUX ERREURS

Les architectures HA permettent de réduire considérablement, voire d'éliminer, les interruptions en redirigeant automatiquement le trafic vers des ressources disponibles, que ce soit en cas de panne ou lors de maintenances planifiées.

MODE



ACTIVE-PASSIVE

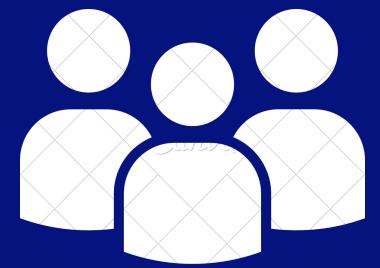
- le passif n'est déclenché que lorsque le primaire tombe en panne
- Le pare-feu primaire est celui qui répond au trafic réseau entrant et sortant.

ACTIVE-ACTIVE

- les deux pare-feu répondent au trafic réseau

PROBLEMATIQUE ET SOLUTIONS

PROBLEMATIQUE



Redondance
et Tolérance
aux Pannes

Comment concevoir une architecture qui minimise les interruptions de service en cas de défaillance ?



Scalabilité et
Evolutivité

Comment concevoir une architecture qui puisse s'adapter à la croissance de l'entreprise tout en maintenant une haute disponibilité ?



Gestion de
la Charge

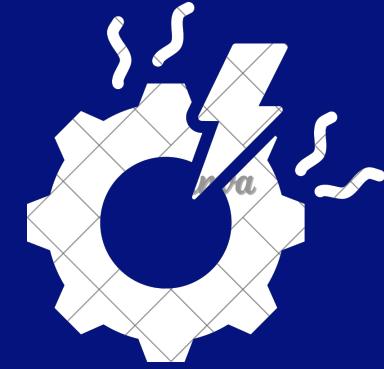
Comment répartir la charge de manière équilibrée entre les différents composants du systèmes ?



Coût et
Ressources

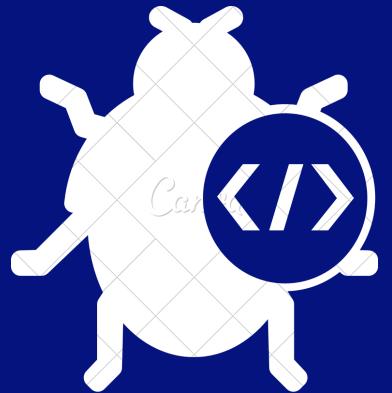
Comment maximiser la disponibilité tout en optimisant les coûts opérationnels ?

SOLUTIONS



Pannes matérielles

Assurer la continuité des services malgré la défaillance de serveurs, disques ou autres équipements.



Défaillances logicielles

Prévenir les interruptions causées par des bugs ou des plantages d'applications.



Surcharge du réseau

Répartir efficacement la charge pour éviter les goulets d'étranglement.



Maintenance planifiée

Permettre des mises à jour ou réparations sans interrompre les services.

OUTILS



GNS3

GNS3 est une plateforme de virtualisation de réseau utilisée pour créer, simuler et tester des réseaux informatiques. C'est un logiciel open-source qui permet aux utilisateurs de concevoir des topologies réseau complexes en utilisant des dispositifs virtuels.



VMware

VMware est une application de virtualisation populaire permettant de créer et de gérer des machines virtuelles sur un ordinateur hôte.

PROTOCOLES

PROTOCOLES DE GESTION ET DE SURVEILLANCE

HTTP

Pour gérer les FortiGate
via une interface web.

SSH

Accès sécurisé à la ligne
de commande des
switches

PROTOCOLES DE REDONDANCE ET HAUTE DISPONIBILITÉ

HSRP

Pour la redondance entre FTG-P et FTG-B, permettant un basculement automatique en cas de panne.

HA

spécifique à FortiGate : Pour synchroniser les configurations et gérer le basculement automatique entre les deux firewalls.

PROTOCOLES DE COMMUTATION

VLAN (802.1Q)

Utilisé pour transporter les VLANs IT et RH sur les liens entre les commutateurs (Switches)

STP

Évite les boucles dans le réseau commuté entre les switches .

PROTOCOLES POUR L'ACCÈS AU RÉSEAU

DHCP

Pour attribuer dynamiquement des adresses IP aux PC dans les VLANs IT et RH

DNS

Permet la résolution de noms pour les PC et les équipements du réseau.

TECHNOLOGIES

COMPONENTS

01



PC

02



Switch (cisco IOU 15.2d)

03



Firewall (Fortigate 7.0.0)

04



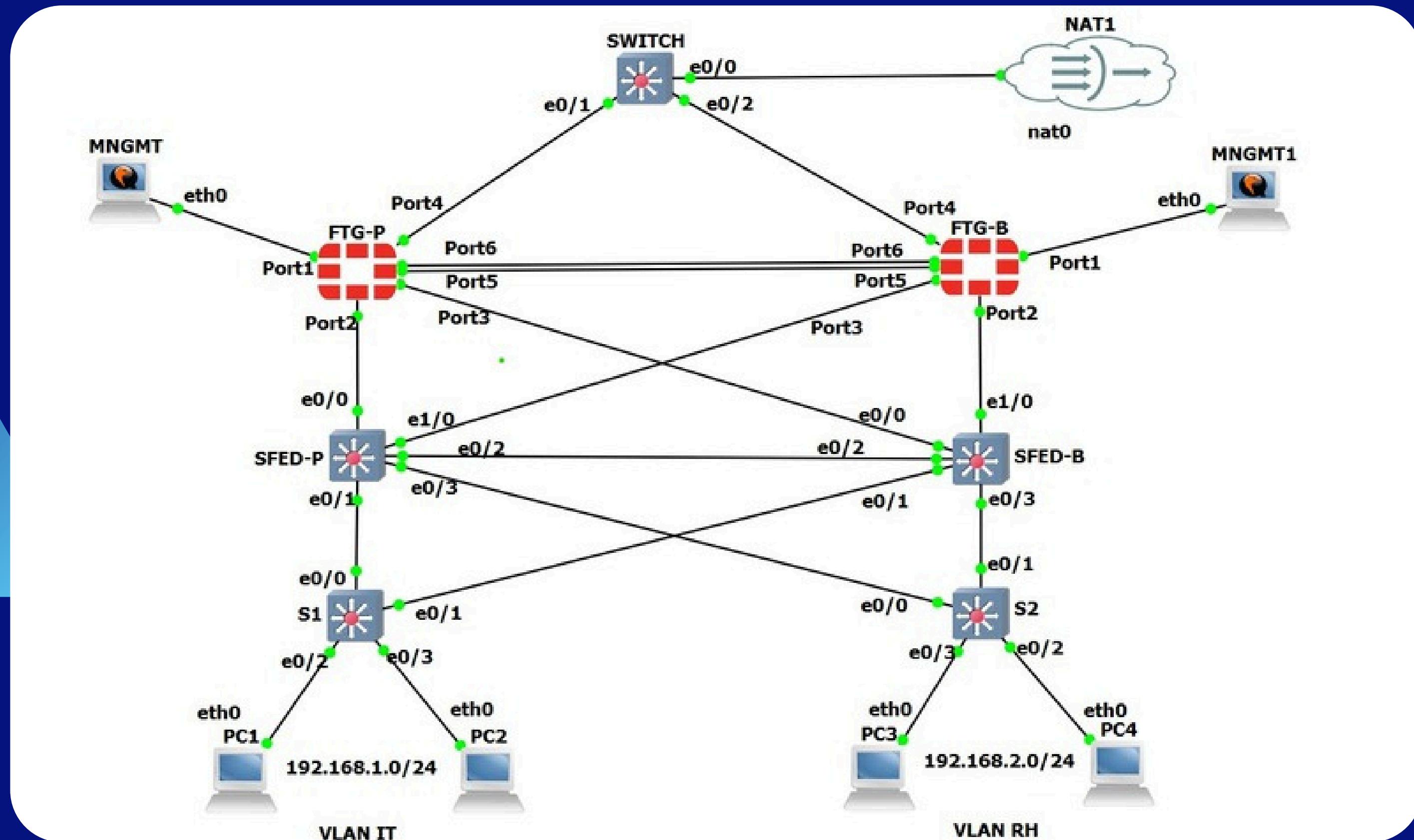
Cloud

CONFIGURATION

- CONFIGURATION INITIALE
- CONFIGURATION HA

CONFIGURATION INITIALE

ARCHITECTURE



CONFIGURATION DE FTG-P

CONFIGURATION DES INTERFACES :

PORT 1 LIÉ AU MGMT :

```
FortiGate-VM64-KVM # config system interface
```

```
FortiGate-VM64-KVM (interface) # edit port1
```

```
FortiGate-VM64-KVM (port1) # set mode dhcp
```

```
FortiGate-VM64-KVM (port1) # set allowaccess http ping
```

```
FortiGate-VM64-KVM (port1) # end
```

```
FortiGate-VM64-KVM #
```

Edit Interface

Name	port1
Alias	MNGMT
Type	Physical Interface
VRF ID	0
Role	Undefined

Address

Addressing mode	Manual	DHCP	Auto-managed by FortiPAM
Status	Connected		
Obtained IP/Netmask	192.168.72.169/255.255.255.0	Renew	
Expiry Date	2024/11/27 12:59:51		
Acquired DNS	192.168.72.1		
Retrieve default gateway from server	<input checked="" type="checkbox"/>		
Distance	5		
Override internal DNS	<input checked="" type="checkbox"/>		

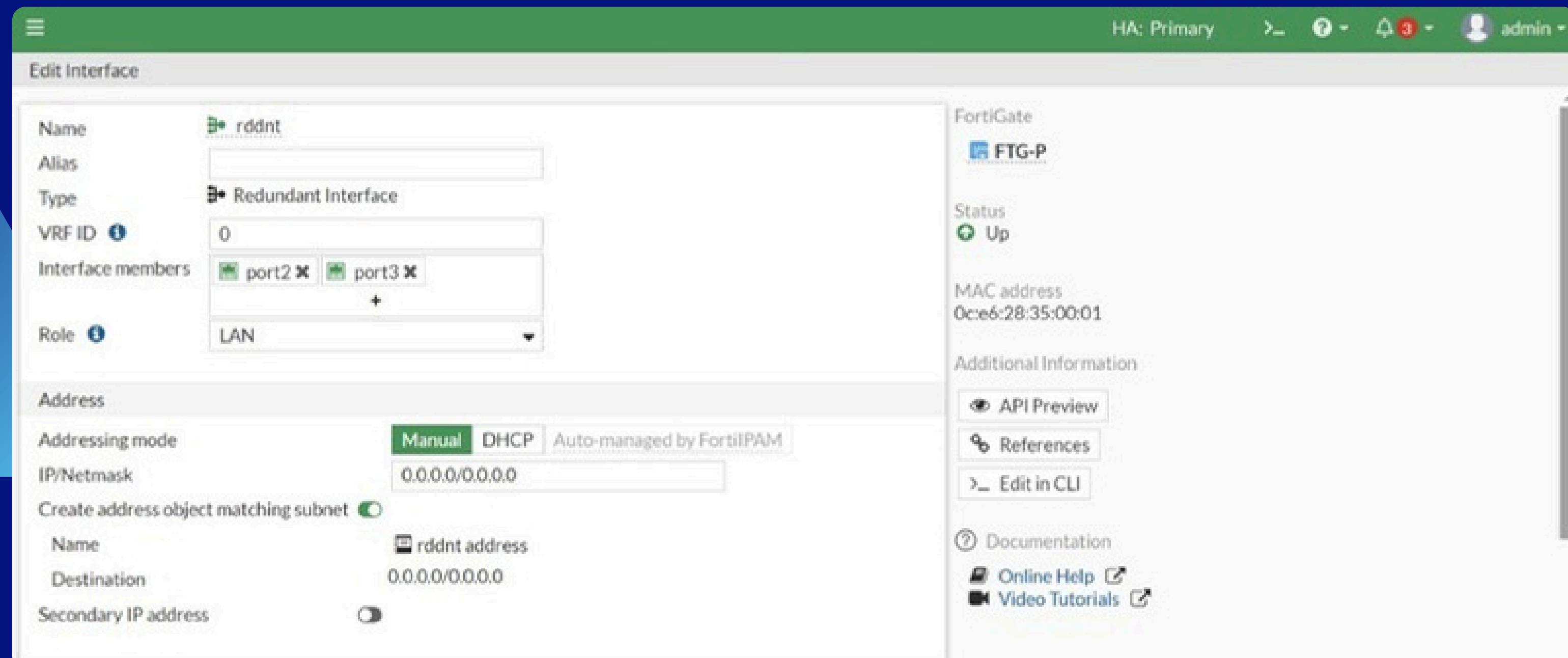
CONFIGURATION DES INTERFACES :

PORT 4 LIÉ AU SWITCH LIÉ AU CLOUD (WAN) :

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port4
FortiGate-VM64-KVM (port4) # set mode dhcp
FortiGate-VM64-KVM (port4) # end
FortiGate-VM64-KVM # 
```

CONFIGURATION DES INTERFACES :

CONFIG DE PORT2 ET PORT3 COMME INTERFACE REDONDANTE :



The screenshot shows the FortiGate UI for editing an interface. The main configuration pane on the left is titled 'Edit Interface' and contains the following fields:

- Name:** rddnt
- Alias:** (empty)
- Type:** Redundant Interface
- VRF ID:** 0
- Interface members:** port2, port3
- Role:** LAN

Below this, the 'Address' section includes:

- Addressing mode:** Manual (selected)
- IP/Netmask:** 0.0.0.0/0.0.0.0
- Create address object matching subnet:**
- Name:** rddnt address
- Destination:** 0.0.0.0/0.0.0.0
- Secondary IP address:** (empty)

The right sidebar displays system status and links:

- FortiGate:** FTG-P
- Status:** Up
- MAC address:** 0c:e6:28:35:00:01
- Additional Information:**
 - API Preview
 - References
 - Edit in CLI
- Documentation:**
 - Online Help
 - Video Tutorials

CONFIGURATION DES INTERFACES :

CREATION DU VLAN IT :

HA: Primary     admin

Edit Interface

Name: **vlanit**

Alias:

Type: **VLAN**

Interface: **rddnt**

VLAN ID: **10** 

VRF ID: **0**

Role: **LAN**

FortiGate: **FTG-P**

Status: **Up**

MAC address: **0ce6:28:35:00:01**

Address

Addressing mode: **Manual** **DHCP** **Auto-managed by FortiIPAM**

IP/Netmask: **192.168.1.1/255.255.255.0**

Create address object matching subnet **ON**

Name: **vlanit address**

Destination: **192.168.1.1/255.255.255.0**

Secondary IP address: **OFF**

Additional Information

 **API Preview**

 **References**

 **Edit in CLI**

 **Documentation**

 **Online Help**  **Video Tutorials**

Administrative Access

CONFIGURATION DES INTERFACES :

CREATION DU VLAN RH :

HA: Primary admin

Edit Interface

Name	vlanrh
Alias	
Type	VLAN
Interface	rdmtn
VLAN ID	20
VRF ID	0
Role	LAN

Address

Addressing mode	
IP/Netmask	192.168.2.1/255.255.255.0

Create address object matching subnet

Name	vlanrh address
Destination	192.168.2.1/255.255.255.0
Secondary IP address	

FortiGate

FTG-P

Status Up

MAC address 0c:62:35:00:01

Additional Information

API Preview

References

Edit in CLI

Documentation

Online Help

Video Tutorials

CONFIGURATION DES INTERFACES :

POLITIQUE DE SÉCURITÉ VLAN IT - WAN :

HA: Primary admin

Edit Policy

Name: **VLANITtoWAN**

Incoming Interface: **vlanit**

Outgoing Interface: **port4**

Source: **all**

Destination: **all**

Schedule: **always**

Service: **ALL**

Action: **✓ ACCEPT** **✗ DENY**

Inspection Mode: **Flow-based** Proxy-based

Firewall / Network Options

NAT: **On**

IP Pool Configuration: **Use Outgoing Interface Address** **Use Dynamic IP Pool**

Preserve Source Port: **On**

Protocol Options: **PROT default**

Statistics (since last reset)

ID	1
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0B
Current bandwidth	0B/s

Clear Counters

Additional Information

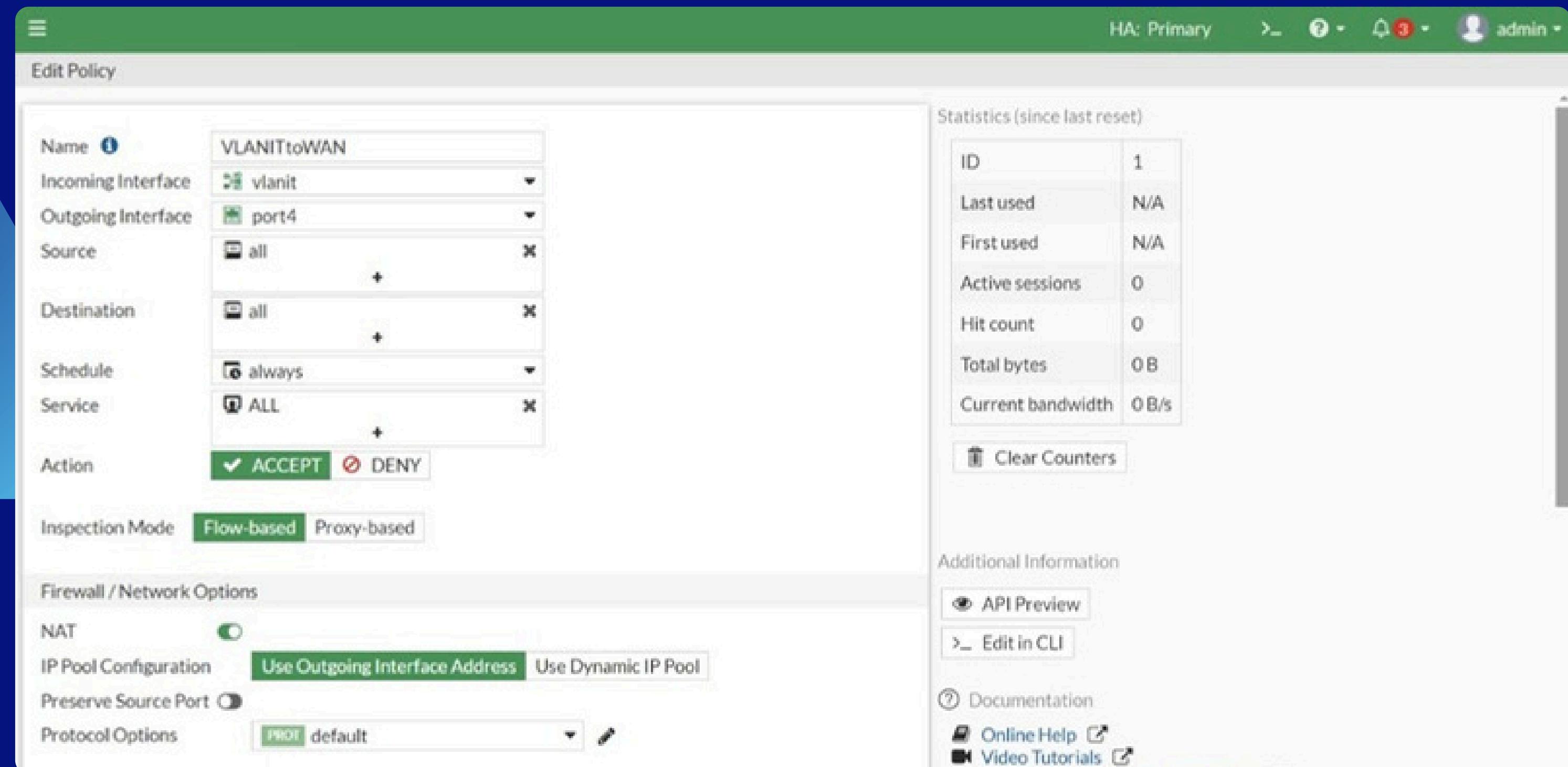
API Preview

Edit in CLI

Documentation

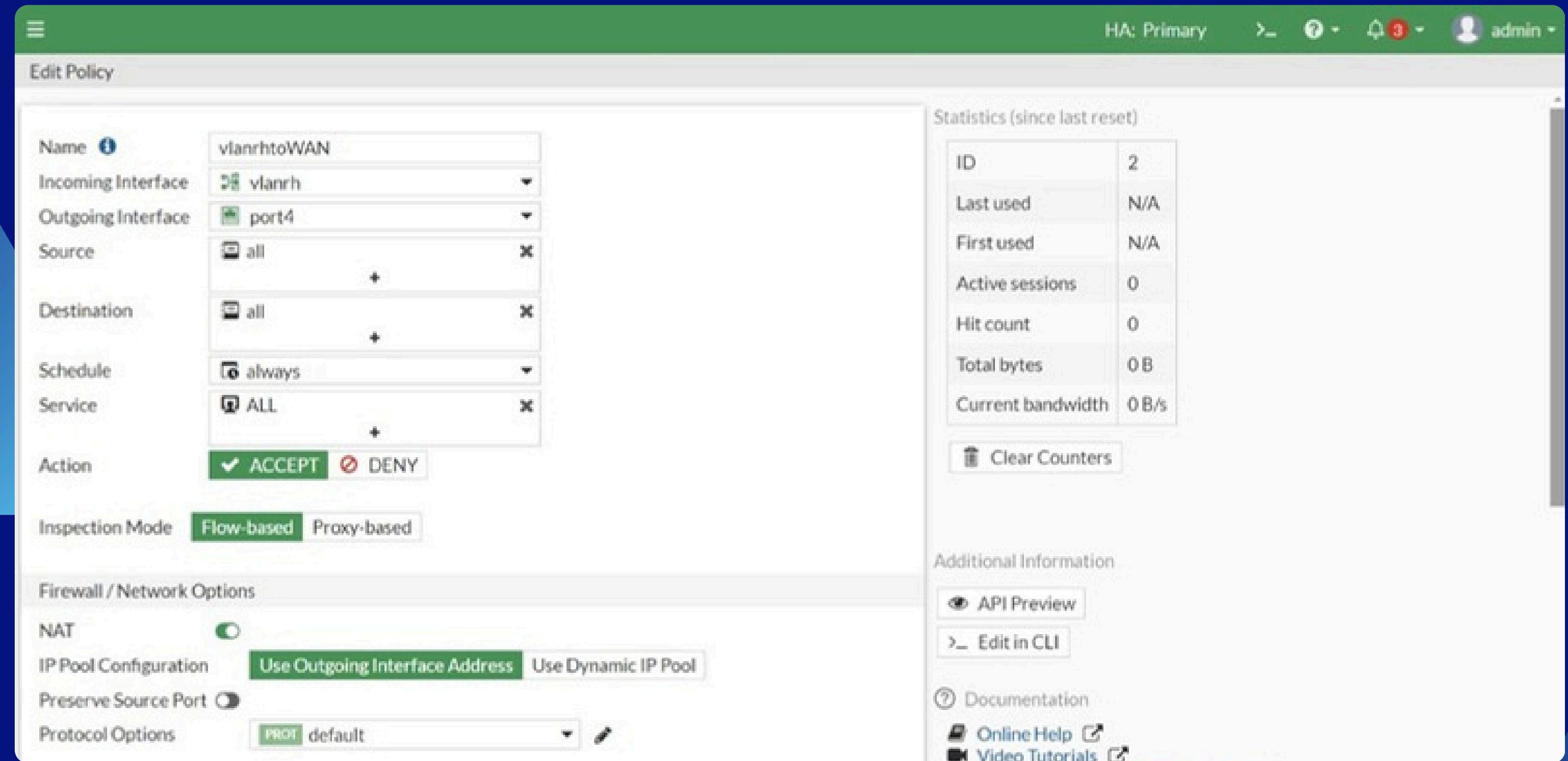
Online Help 

Video Tutorials 



CONFIGURATION DES INTERFACES :

POLITIQUE DE SÉCURITÉ VLAN RH - WAN :



The screenshot shows a network policy configuration interface with the following details:

- Name:** vianrhtoWAN
- Incoming Interface:** vlanrh
- Outgoing Interface:** port4
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT DENY

Inspection Mode: Flow-based (selected)

Firewall / Network Options:

- NAT:**
- IP Pool Configuration:** Use Outgoing Interface Address (selected)
- Preserve Source Port:**
- Protocol Options:** PROT default

Statistics (since last reset):

ID	2
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 B/s

Additional Information:

- API Preview
- Edit in CLI
- Documentation
 - Online Help
 - Video Tutorials

CONFIGURATION DE FTG-B

CONFIGURATION DES INTERFACES :

PORT 1 :

```
FortiGate-VM64-KVM # config system interface
```

```
FortiGate-VM64-KVM (interface) # edit port1
```

```
FortiGate-VM64-KVM (port1) # set mode dhcp
```

```
FortiGate-VM64-KVM (port1) # set allowaccess http ping
```

```
FortiGate-VM64-KVM (port1) # end
```

```
FortiGate-VM64-KVM #
```

Edit Interface

Name	port1
Alias	MNGMT
Type	Physical Interface
VRF ID	0
Role	Undefined

Address

Addressing mode	Manual	DHCP	Auto-managed by FortiPAM
Status	Connected		
Obtained IP/Netmask	192.168.72.169/255.255.255.0	Renew	
Expiry Date	2024/11/27 12:59:51		
Acquired DNS	192.168.72.1		
Retrieve default gateway from server	<input checked="" type="checkbox"/>		
Distance	5		
Override internal DNS	<input checked="" type="checkbox"/>		

CONFIGURATION DES INTERFACES :

PORT 4 :

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port4
FortiGate-VM64-KVM (port4) # set mode dhcp
FortiGate-VM64-KVM (port4) # end
FortiGate-VM64-KVM # 
```

CONFIGURATION DES SWITCHES

LES VLANS DU SWITCH SFED-P :

```
IOU1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1, Et3/2, Et3/3
10 VLAN0010	active	
20 VLAN0020	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

```
IOU1#
```

MEME CHOSE POUR LE SWITCH SFED-B

LES INTERFACES DU SWITCH SFED-P :

```
IOU1#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	trunk	auto	auto	unknown
Et0/1		connected	trunk	auto	auto	unknown
Et0/2		connected	trunk	auto	auto	unknown
Et0/3		connected	trunk	auto	auto	unknown
Et1/0		connected	trunk	auto	auto	unknown
Et1/1		connected	1	auto	auto	unknown
Et1/2		connected	1	auto	auto	unknown
Et1/3		connected	1	auto	auto	unknown
Et2/0		connected	1	auto	auto	unknown
Et2/1		connected	1	auto	auto	unknown
Et2/2		connected	1	auto	auto	unknown
Et2/3		connected	1	auto	auto	unknown
Et3/0		connected	1	auto	auto	unknown
Et3/1		connected	1	auto	auto	unknown
Et3/2		connected	1	auto	auto	unknown
Et3/3		connected	1	auto	auto	unknown

MEME CHOSE POUR LE SWITCH SFED-B

SPT POUR LE SWITCH SFED - P :

```
IOU1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
    Root ID    Priority    24577
                Address     aabb.cc00.0100
                This bridge is the root
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    24577 (priority 24576 sys-id-ext 1)
                Address     aabb.cc00.0100
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time  300 sec

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Et0/0          Desg FWD 100      128.1      Shr
  Et0/1          Desg FWD 100      128.2      Shr Peer(STP)
  Et0/2          Desg FWD 100      128.3      Shr
  Et0/3          Desg FWD 100      128.4      Shr Peer(STP)
  Et1/0          Desg FWD 100      128.5      Shr
  Et1/1          Desg FWD 100      128.6      Shr
  Et1/2          Desg FWD 100      128.7      Shr
  Et1/3          Desg FWD 100      128.8      Shr

  --More--  [ ]
```

SPT POUR LE SWITCH SFED-B :

```
SFED-B#show spanning-tree
```

VLAN0001

Spanning tree enabled protocol rstp

Root ID Priority 24577

Address aabb.cc00.0100

Cost 100

Port 3 (Ethernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28673 (priority 28672 sys-id-ext 1)

Address aabb.cc00.0200

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----------	------	-----	------	----------	------

Et0/0	Desg	FWD	100	128.1	Shr
-------	------	-----	-----	-------	-----

Et0/1	Desg	FWD	100	128.2	Shr Peer(STP)
-------	------	-----	-----	-------	---------------

Et0/2	Root	FWD	100	128.3	Shr
-------	------	-----	-----	-------	-----

Et0/3	Desg	FWD	100	128.4	Shr Peer(STP)
-------	------	-----	-----	-------	---------------

Et1/0	Desg	FWD	100	128.5	Shr
-------	------	-----	-----	-------	-----

Et1/1	Desg	FWD	100	128.6	Shr
-------	------	-----	-----	-------	-----

Et1/2	Desg	FWD	100	128.7	Shr
-------	------	-----	-----	-------	-----

--More-- □

CONFIGURATION DU SWITCH S1 :

```
S1#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
	Et0/0	connected	trunk	auto	auto	unknown
	Et0/1	connected	trunk	auto	auto	unknown
	Et0/2	connected	10	auto	auto	unknown
	Et0/3	connected	1	auto	auto	unknown
	Et1/0	connected	1	auto	auto	unknown
	Et1/1	connected	1	auto	auto	unknown
	Et1/2	connected	1	auto	auto	unknown
	Et1/3	connected	1	auto	auto	unknown
	Et2/0	connected	1	auto	auto	unknown
	Et2/1	connected	1	auto	auto	unknown
	Et2/2	connected	1	auto	auto	unknown
	Et2/3	connected	1	auto	auto	unknown
	Et3/0	connected	1	auto	auto	unknown
	Et3/1	connected	1	auto	auto	unknown
	Et3/2	connected	1	auto	auto	unknown
	Et3/3	connected	1	auto	auto	unknown

CONFIGURATION DU SWITCH S2 :

```
S2#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
	Et0/0	connected	trunk	auto	auto	unknown
	Et0/1	connected	trunk	auto	auto	unknown
	Et0/2	connected	20	auto	auto	unknown
	Et0/3	connected	1	auto	auto	unknown
	Et1/0	connected	1	auto	auto	unknown
	Et1/1	connected	1	auto	auto	unknown
	Et1/2	connected	1	auto	auto	unknown
	Et1/3	connected	1	auto	auto	unknown
	Et2/0	connected	1	auto	auto	unknown
	Et2/1	connected	1	auto	auto	unknown
	Et2/2	connected	1	auto	auto	unknown
	Et2/3	connected	1	auto	auto	unknown
	Et3/0	connected	1	auto	auto	unknown
	Et3/1	connected	1	auto	auto	unknown
	Et3/2	connected	1	auto	auto	unknown
	Et3/3	connected	1	auto	auto	unknown

```
S2#
```

CONFIGURATION DU SWITCH VERS CLOUD :

```
IOU5#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	1	auto	auto	unknown
Et0/1		connected	trunk	auto	auto	unknown
Et0/2		connected	trunk	auto	auto	unknown
Et0/3		connected	1	auto	auto	unknown
Et1/0		connected	1	auto	auto	unknown
Et1/1		connected	1	auto	auto	unknown
Et1/2		connected	1	auto	auto	unknown
Et1/3		connected	1	auto	auto	unknown
Et2/0		connected	1	auto	auto	unknown
Et2/1		connected	1	auto	auto	unknown
Et2/2		connected	1	auto	auto	unknown
Et2/3		connected	1	auto	auto	unknown
Et3/0		connected	1	auto	auto	unknown
Et3/1		connected	1	auto	auto	unknown
Et3/2		connected	1	auto	auto	unknown
Et3/3		connected	1	auto	auto	unknown

```
IOU5#
```

CONFIGURATION

H.A

CONFIGURATION FTG-P NOUS ACCÉDONS AU SYSTÈME DU FTG-P ET NOUS MODIFIONS LES PARAMÈTRES DE LA HAUTE DISPONIBILITÉ (HA) COMME SUIT.

FTG-P

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- System
 - Administrators
 - Admin Profiles
 - Firmware
 - Settings
- HA
- SNMP
- Replacement Messages
- FortiGuard
 - 1
- Feature Visibility
- Certificates
- Security Fabric
- Log & Report

High Availability

Mode: Active-Passive

Device priority: 150

Cluster Settings

Group name: CLUSTER

Password: password

Session pickup:

Monitor interfaces:

Heartbeat interfaces: port5 port6

Heartbeat Interface Priority

port5: 50

port6: 50

Management Interface Reservation

Unicast Heartbeat

OK Cancel

HA Status

Mode	Active-Passive
Group	CLUSTER
Primary	<input checked="" type="checkbox"/> FTG-P
Uptime	00:00:04:53
State Changed	00:00:04:32

LE PORT DE GESTION (PORT 1) POURRAIT AVOIR CHANGÉ D'ADRESSE IP, DONC ON VÉRIFIER:

```
fortilink  static  0.0.0.0 0.0.0.0  10.255.1.1 255.255.255.0  up  disable  aggregate  enable
port1    dhcp   0.0.0.0 0.0.0.0  192.168.72.167 255.255.255.0  up  disable  physical  enable
port2    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port3    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port4    dhcp   0.0.0.0 0.0.0.0  192.168.122.7 255.255.255.0  up  disable  physical  enable
port5    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port6    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port7    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port8    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port9    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port10   static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
rddnt   static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  redundant  enable
```

```
FortiGate-VM64-KVM # show system interface Timeout
```

```
FTG-P login: admin
```

```
Password:
```

```
Welcome!
```

```
WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.  
It is strongly recommended that you check the file system consistency before proceeding.
```

```
Please run 'execute disk list' and then 'execute disk scan <ref#>'.
```

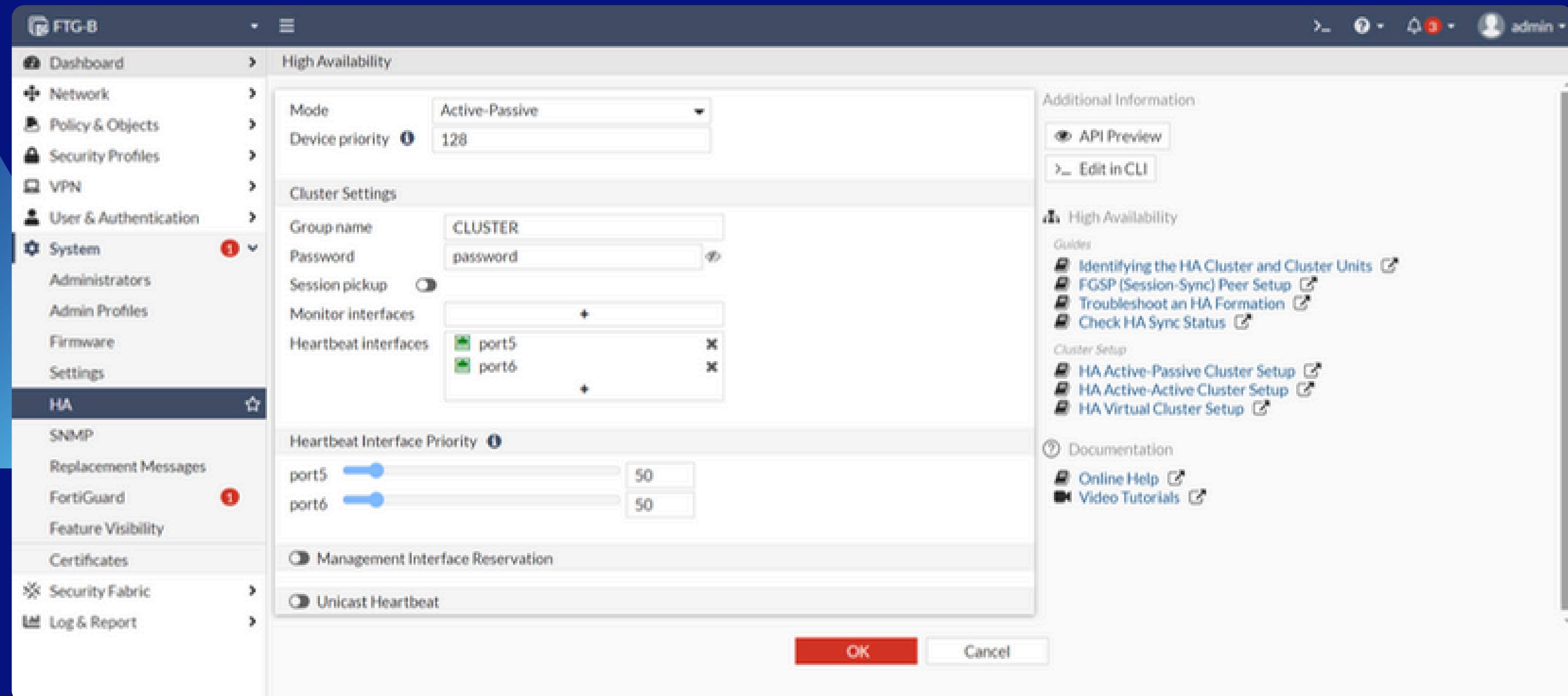
```
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
```

```
FTG-P # show system interface
```

```
name  Name.
```

```
fortilink  static  0.0.0.0 0.0.0.0  10.255.1.1 255.255.255.0  up  disable  aggregate  enable
port1    dhcp   0.0.0.0 0.0.0.0  192.168.72.169 255.255.255.0  up  disable  physical  enable
port2    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port3    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port4    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port5    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port6    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port7    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port8    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port9    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
port10   static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  physical  enable
rddnt   static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up  disable  redundant  enable
```

CONFIGURATION FTG-B NOUS ACCÉDONS AU SYSTÈME DU FTG-B ET NOUS MODIFIONS LES PARAMÈTRES DE LA HAUTE DISPONIBILITÉ (HA) COMME SUIT.



The screenshot shows the FortiGate Management Interface with the following configuration for High Availability:

- Mode:** Active-Passive
- Device priority:** 128
- Cluster Settings:**
 - Group name:** CLUSTER
 - Password:** password
 - Session pickup:** Enabled
 - Monitor interfaces:** port5, port6
 - Heartbeat interfaces:** port5, port6
- Heartbeat Interface Priority:**
 - port5: Priority 50
 - port6: Priority 50
- Management Interface Reservation:** Enabled
- Unicast Heartbeat:** Enabled

The interface includes a sidebar with various system settings and a right-hand panel with additional information and documentation links.

ON PEUT VÉRIFIER LA CONFIGURATION H.A COMME CECI :

```
FTG-B # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:16:9
Cluster state change time: 2024-11-26 14:19:04
Primary selected using:
    <2024/11/26 14:19:04> FGVMEVUTBNAIAC35 is selected as the primary because its override priority is larger than peer member FGVMEVLRKYDMDR83.
ses_pickup: disable
override: disable
Configuration Status:
    FGVMEVLRKYDMDR83(updated 0 seconds ago): out-of-sync
    FGVMEVUTBNAIAC35(updated 1 seconds ago): in-sync
System Usage stats:
    FGVMEVLRKYDMDR83(updated 0 seconds ago):
        sessions=4, average-cpu-user/nice/system/idle=0%/0%/2%/31%, memory=35%
    FGVMEVUTBNAIAC35(updated 1 seconds ago):
        sessions=19, average-cpu-user/nice/system/idle=9%/0%/5%/2%, memory=36%
HBDEV stats:
    FGVMEVLRKYDMDR83(updated 0 seconds ago):
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=2311173/5163/0/0, tx=188686/617/0/0
        port6: physical/1000auto, up, rx-bytes/packets/dropped/errors=2191651/4856/0/0, tx=145094/327/0/0
    FGVMEVUTBNAIAC35(updated 1 seconds ago):
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=186497/611/0/0, tx=2308527/5157/0/0
        port6: physical/1000auto, up, rx-bytes/packets/dropped/errors=142779/321/0/0, tx=2189461/4852/0/0
Secondary : FTG-B
Primary  : FTG-P
number of vcluster: 1
vcluster 1: standby 169.254.0.1
Secondary: FGVMEVLRKYDMDR83, Secondary : FTG-B
Primary: FGVMEVUTBNAIAC35, Primary : FTG-P
FTG-B # number of vcluster: 1
FGVMEVUTBNAIAC35(updated 1 seconds ago):
    port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=186497/611/0/0,
    port6: physical/1000auto, up, rx-bytes/packets/dropped/errors=142779/321/0/0,
, FGVMEVLRKYDMDR83, HA cluster index = 1
, FGVMEVUTBNAIAC35, HA cluster index = 0
```

VÉRIFICATION DE SYNCHRONISATION DE FTG-P AVEC FTG-B:

LA SYNCHRONISATION NÉCESSITE QUELQUES SECONDES À QUELQUES MINUTES POUR SE COMPLÉTER. POUR VÉRIFIER L'ÉTAT DE LA HAUTE DISPONIBILITÉ (HA), VOUS POUVEZ UTILISER LA COMMANDE :

GET SYSTEM HA STATUS

```
FTG-B # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:28:18
Cluster state change time: 2024-11-26 14:19:04
Primary selected using:
    <2024/11/26 14:19:04> FGVMEVUTBNAIAC35 is selected as the primary because its override priority is larger than peer member FGVMEVLRKYDMDR83.
ses_pickup: disable
override: disable
Configuration Status:
    FGVMEVLRKYDMDR83(updated 4 seconds ago): in-sync
    FGVMEVUTBNAIAC35(updated 4 seconds ago): in-sync
System Usage stats:
```



MAINTENANT , LES DEUX PARE-FEUX SONT EN SYNCHRONISATION

HA: Primary   admin

FortiGate VM64-KVM 1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24

FTG-P (Primary)

Refresh Edit Remove device from HA cluster

Status	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
 Synchronized	150	FTG-P	FGVMEVUTBNAIAC35	Primary	21m 28s	15	37.00 kbps
 Synchronized	128	FTG-B	FGVMEVLRKYDMD				

FortiGate VM64-KVM 1 3 5 7 9 11 13
2 4 6 8 10 12 14

FTG-P (Primary)

RÉALISATION

**MERCI POUR
VOTRE
ATTENTION**



MARRAKECH

جامعة القاضي عياض

UNIVERSITÉ CADI AYYAD

ÉCOLE NATIONALE DES SCIENCES
APPLIQUÉES DE MARRAKECH



GCDSTE
ENSA-M

ARCHITECTURE D'ENTREPRISE H.A

(CISCO : ROUTAGE, POLITIQUES DE SÉCURITÉ ...)

Sous le module de protocoles de sécurité & sécurité des réseaux et des communications

RÉALISER PAR :

ZAKARIA OUAHI
ADIL EL KHAIDER
JIHANE ELMOUARABIT
SANOGO CHEIKHNA
BOURHAT AYMANE

ENCADRE PAR :

PR. AZOUGAGHE ALI

Année universitaire: 2024/2025