



# FortiGate

## Guide Ultime du Failover sur FortiGate

FAILOVER



Un guide clair et détaillé pour  
administrateurs réseaux qui veulent  
dormir tranquilles

# Chers lecteurs, bienvenue dans cette aventure

Si vous tenez ce livre entre vos mains aujourd'hui, c'est que vous avez choisi de renforcer vos compétences dans un domaine passionnant et stratégique : le réseau et la cybersécurité. Vous avez choisi de comprendre comment rendre vos infrastructures plus fiables, résilientes et sécurisées, et nous sommes honorés de vous accompagner dans ce parcours.

Notre initiative n'est pas seulement de transmettre du savoir technique ; elle est née d'un véritable désir de partage. Nous croyons que la connaissance doit circuler, se transmettre et surtout s'adapter aux besoins des professionnels comme vous, qui cherchez à grandir et à réussir dans leur carrière.

À travers ce livre, mais aussi via nos contenus sur LinkedIn, nous mettons à votre disposition des explications claires, des exemples pratiques et des conseils concrets. En nous suivant et en partageant notre page, vous devenez acteur d'une communauté de passionnés qui avance ensemble, pour que personne ne reste seul face aux défis complexes du monde numérique.

Nous faisons cela pour vous : pour vous donner la confiance nécessaire à déployer des solutions robustes, pour vous inspirer à progresser chaque jour, et pour vous aider à atteindre vos objectifs professionnels. Votre réussite est notre plus grande récompense.

Alors, avançons ensemble. Soutenez notre démarche en parlant de nous, en partageant nos contenus, et surtout en appliquant ce que vous apprendrez ici. Car votre carrière mérite de s'appuyer sur des bases solides et modernes, et nous sommes là pour vous guider.

## Restons en contact

Chers lecteurs,

Votre avis est précieux. Ce livre est avant tout conçu pour vous accompagner dans votre parcours en réseau informatique et en cybersécurité. Si au fil de votre lecture vous avez des questions, suggestions ou commentaires, n'hésitez pas à nous écrire. Nous croyons fermement que le dialogue et l'échange sont les clés de l'amélioration continue.

👉 Vous pouvez nous contacter directement à l'adresse suivante :  
**[info@reseauenclair.com](mailto:info@reseauenclair.com)**

De plus, si vous êtes passionné par le monde du réseau et de la cybersécurité, et que vous souhaitez participer activement à notre équipe, sachez que nous serions ravis d'accueillir de nouveaux talents. Envoyez-nous simplement un message à ce même courriel pour nous partager votre intérêt.

Nous construisons ensemble une communauté où l'entraide, le savoir et l'expérience se mettent au service de la réussite de chacun.

Bonne lecture, et surtout... bonne réussite dans votre parcours professionnel !



## Configurer un Route Failover

### Étapes principales

#### 1. Vérifier la configuration de Routing

##### \* Pages : 9 – 11

- Consulter les Static Routes existantes.
- Activer les colonnes Distance et Priority.
- Noter les valeurs de la Default Route.

#### 2. Configurer une seconde Default Route

##### \* Pages : 11 – 12

- Créer une Default Route via port2.
- Définir une Distance plus élevée (20).
- Définir une Priority plus élevée (5).

#### 3. Configurer les Firewall Policies

##### \* Pages : 13 – 14

- Modifier la règle Full\_Access pour activer le Logging (All Sessions).
- Créer une nouvelle règle Backup\_Access avec NAT activé.
- Activer le Logging pour toutes les sessions.

#### 4. Consulter la Routing Table

##### \* Page : 15

- Utiliser la commande CLI :
- `get router info routing-table all`  
`get router info routing-table database`
- Vérifier l'état actif/inactif des routes.

#### 5. Configurer les Link Health Monitors

##### \* Page : 16

- Créer un moniteur de lien pour port1.
- Créer un moniteur de lien pour port2.

#### 6. Tester le Route Failover

##### \* Pages : 17 – 21

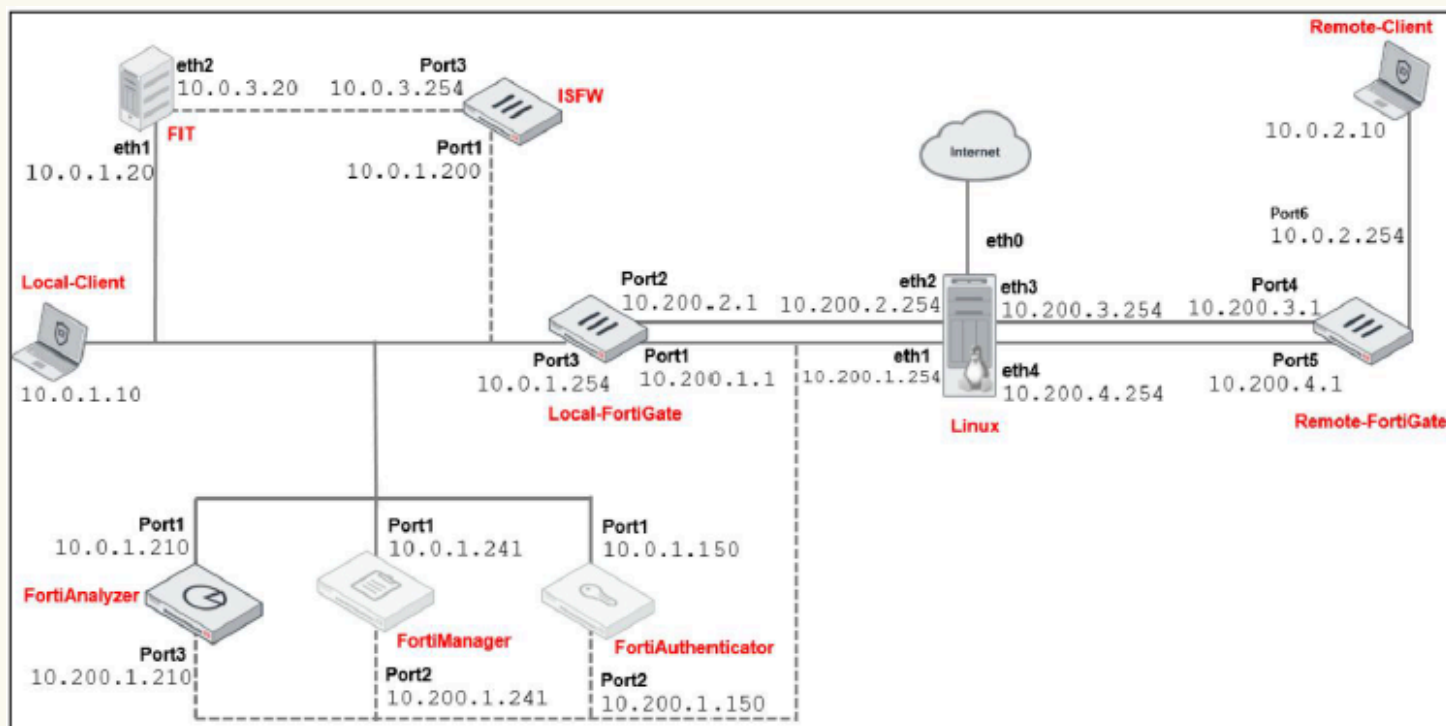
- Vérifier l'utilisation de port1 via les Forward Traffic Logs.
- Forcer un basculement en envoyant un ping invalide depuis port1.
- Observer le passage automatique vers port2.
- Vérifier les logs et la nouvelle Routing Table.

#### 7. Restaurer la Routing Table

##### \* Pages : 21 – 22

- Réinitialiser le Link Health Monitor de port1 avec une IP valide.
- Confirmer que la Default Route repasse sur port1.

# Topologie du réseau



# Laboratoire 1: Routage

Dans ce laboratoire, vous configurerez les paramètres du routeur et testerez des scénarios pour découvrir comment FortiGate prend des décisions de routage.

## Objectifs

- Acheminer le trafic en fonction de l'adresse IP de destination, ainsi que d'autres critères
- Répartir le trafic entre plusieurs chemins
- Mettre en œuvre une bascule de route (failover)
- Mettre en œuvre le routage basé sur des règles (policy routing)
- Diagnostiquer un problème de routage

## Temps à prévoir

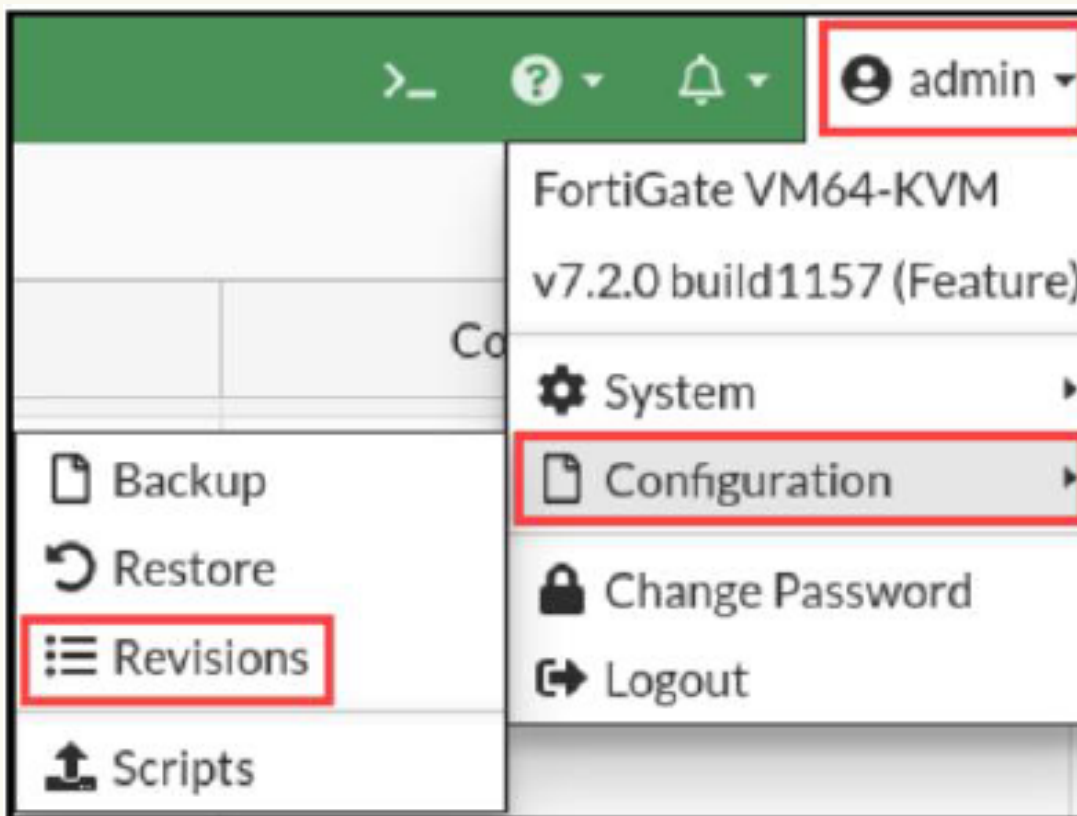
Durée estimée : 50 minutes

## Prérequis

Avant de commencer ce laboratoire, vous devez restaurer un fichier de configuration sur le Local-FortiGate.

### Pour restaurer le fichier de configuration du Local-FortiGate







1. Connectez-vous à l'interface graphique (GUI) du Local-FortiGate, puis connectez-vous avec le nom d'utilisateur admin et le mot de passe password.
2. Dans le coin supérieur droit de l'écran, cliquez sur admin, puis cliquez sur Configuration > Revisions.





3.Cliquez sur le signe + pour développer la liste.

4.Sélectionnez la configuration avec le commentaire initial, puis cliquez sur Revert.

 Delete	 Details	 Diff	 Revert	 Save
Config ID	Username	Date	Comments	
 7.2.0 build 1157 15				
38	admin	2022/04/25 14:14:12	local-logging	
37	admin	2022/04/25 14:03:26	local-ipsec-vpn	
36	admin	2022/04/25 14:00:32	local-central-nat	
35	admin	2022/04/25 13:56:10	local-diagnostics	
34	admin	2022/04/25 13:53:02	local-ha	
33	admin	2022/04/25 13:49:07	local-SSL-VPN	
32	admin	2022/04/25 13:46:34	local-FSSO	
31	admin	2022/04/25 13:44:11	local-vdom	
30	admin	2022/04/25 13:41:07	local-SF	
29	admin	2022/04/25 13:34:04	local-app-control	
28	admin	2022/04/25 13:31:22	local-web-filtering	
27	admin	2022/04/25 13:24:23	local-firewall-authentication	
26	admin	2022/04/25 13:21:05	local-nat	
25	admin	2022/04/25 13:05:11	local-firewall-policy	
23	admin	2022/04/25 10:53:52	initial	

5.Cliquez sur OK pour redémarrer.



## Noms d'utilisateur et mots de passe VM

VM	Username	Password
Local-Client	Administrator	password
Remote-Client	Administrator	password
Local-FortiGate	admin	password
Remote-FortiGate	admin	password
ISFW	admin	password
FortiAnalyzer	admin	password

## Exercice 1 : Configurer le basculement de route (Route Failover)

Dans le réseau de laboratoire, le Local-FortiGate dispose de deux interfaces connectées à Internet : port1 et port2.

Dans cet exercice, vous allez configurer la connexion port1 comme lien Internet principal et la connexion port2 comme lien Internet de secours.

Le Local-FortiGate doit utiliser la connexion port2 uniquement si la connexion port1 est hors service.

Pour atteindre cet objectif, vous allez configurer deux routes par défaut avec des distances administratives différentes, ainsi que deux moniteurs d'état de lien (link health monitors).

### Vérifier la configuration de routage

Vous allez vérifier la configuration de routage existante sur le Local-FortiGate.

### Relève le défi d'expert !

Sur l'interface graphique du Local-FortiGate (admin/password), effectuez les étapes suivantes :

- Consultez la configuration des routes statiques existantes sur le Local-FortiGate.
- Activez les colonnes Distance et Priority sur la page de configuration des routes statiques.
- Notez les valeurs de Distance et Priority de la route par défaut existante.

Si vous avez besoin d'aide, ou pour vérifier votre travail, utilisez les instructions détaillées pas à pas ci-dessous.

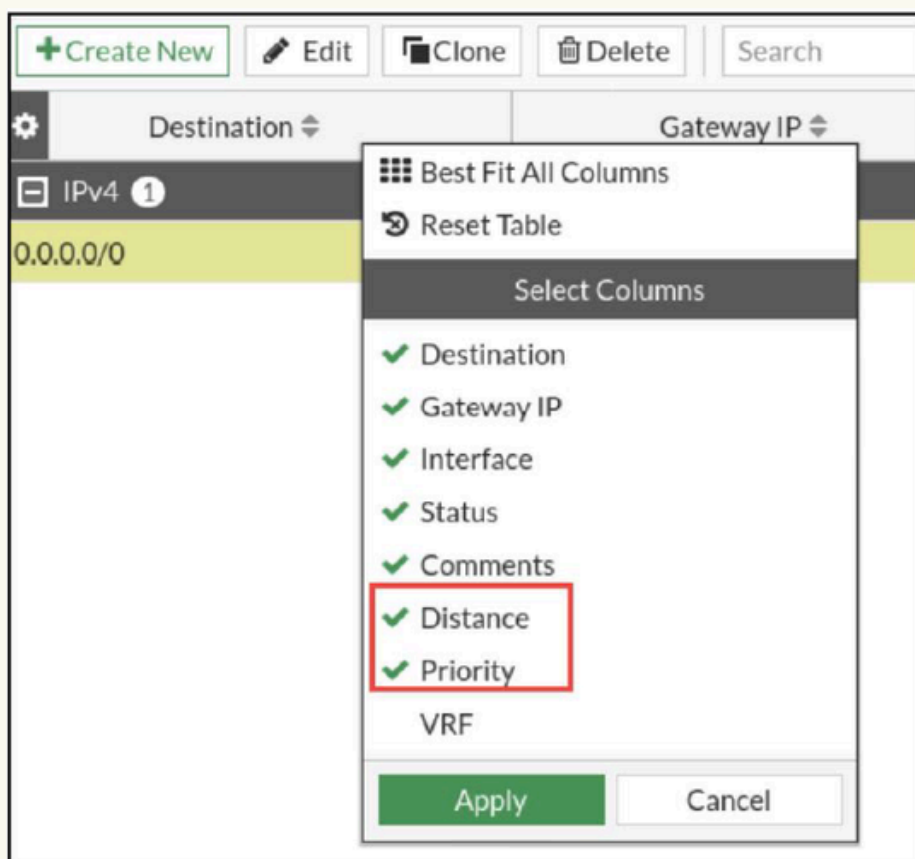
Après avoir terminé ce défi, consultez Configurer une deuxième route par défaut à la page 12.

## Pour vérifier la configuration de routage



- Connectez-vous à l'interface graphique du Local-FortiGate, puis connectez-vous avec le nom d'utilisateur admin et le mot de passe password.
- Cliquez sur Network > Static Routes.
- Vérifiez la route par défaut existante pour port1.

+ Create New Edit Clone Delete Search			
Destination	Gateway IP	Interface	Status
IPv4 1			
0.0.0.0/0	10.200.1.254	port1	Enabled

- Faites un clic droit sur l'une des colonnes pour ouvrir le menu contextuel.
- Dans la section Select Columns, sélectionnez Distance et Priority, puis cliquez sur Apply.



Les colonnes Distance et Priorité apparaissent dans l'interface graphique.

<div><span>+ Create New</span> <span>Edit</span> <span>Clone</span> <span>Delete</span> <input type="text" value="Search"/> <span>Q</span></div>						
Destination ↕	Gateway IP ↕	Interface ↕	Status ↕	Comments ↕	Distance ↕	Priority ↕
0.0.0.0/0	10.200.1.254	 port1	 Enabled		10	1

Notez que, par défaut, les routes statiques ont une valeur de distance de 10 et une valeur de priorité de 1.

## Configurer une deuxième route par défaut

Vous allez créer une deuxième route par défaut via l'interface port2. Pour garantir que cette deuxième route par défaut reste la route de secours, vous lui attribuerez une distance plus élevée.

## Relève le défi d'expert !

- Sur l'interface graphique du Local-FortiGate, configurez une deuxième route par défaut en utilisant port2.
- Attribuez-lui une Distance de 20 et une Priority de 5.

Si vous avez besoin d'assistance, ou pour vérifier votre travail, utilisez les instructions détaillées pas à pas ci-dessous.

Après avoir terminé ce défi, consultez Configurer les règles de pare-feu à la page 13.

## Pour configurer une deuxième route par défaut

1. En restant dans l'interface graphique du Local-FortiGate, cliquez sur Network > Static Routes.
2. Cliquez sur Create New.
3. Configurez les paramètres suivants :

Field	Value
Gateway Address	10.200.2.254
Interface	port2
Administrative Distance	20

4. Cliquez sur le signe + pour développer la section Advanced Options.

5. Dans le champ Priority, saisissez 5.

New Static Route

Destination ⓘ Subnet Internet Service  
0.0.0.0/0.0.0.0

Gateway Address 10.200.2.254

Interface port2

Administrative Distance ⓘ 20

Comments Write a comment... 0/255

Status Enabled Disabled

Advanced Options

Priority ⓘ 5

OK Cancel

6. Cliquez sur OK.

Une deuxième route par défaut est ajoutée.

+ Create New





Edit

Clone

Delete

Search

Q

Destination	Gateway IP	Interface	Status	Comments	Distance	Priority
0.0.0.0/0	10.200.1.254	 port1	 Enabled		10	1
0.0.0.0/0	10.200.2.254	 port2	 Enabled		20	5

## Configurer les politiques de pare-feu

Vous allez modifier la règle de pare-feu existante Full\_Access afin de consigner (logger) toutes les sessions.

Vous allez également créer une deuxième règle de pare-feu pour autoriser le trafic via l'interface secondaire.

### Relève le défi d'expert !

- En restant dans l'interface graphique du Local-FortiGate, activez la journalisation (logging) de toutes les sessions dans la règle de pare-feu existante Full\_Access.
- Créez une deuxième règle de pare-feu nommée Backup\_Access.
- Configurez la règle Backup\_Access pour autoriser le trafic de port3 vers port2, avec la traduction d'adresse (NAT) activée.
- Activez la journalisation (logging) pour toutes les sessions dans la règle Backup\_Access.

Si vous avez besoin d'assistance, ou pour vérifier votre travail, utilisez les instructions détaillées pas à pas ci-dessous.

Après avoir terminé ce défi, consultez Afficher la table de routage à la page 15.

### Pour configurer les règles de pare-feu

1. En restant dans l'interface graphique du Local-FortiGate, cliquez sur Policy & Objects > Firewall Policy.
2. Double-cliquez sur la règle existante Full\_Access pour la modifier.
3. Activez la journalisation pour All Sessions.

**Logging Options**

Log Allowed Traffic ☒ Security Events **All Sessions**

Generate Logs when Session Starts ☐

Capture Packets ☐

Comments  0/1023

Enable this policy ☒



La journalisation en mode All Sessions garantit que tout le trafic est enregistré, et pas seulement les sessions inspectées par les profils de sécurité.

Cela vous aidera à vérifier le routage du trafic en utilisant les journaux Forward Traffic.

4. Cliquez sur OK.

5. Cliquez sur Create New.

6. Configurez une deuxième règle de pare-feu avec les paramètres suivants :

7. click OK

Field	Value
Incoming Interface	port3
Outgoing Interface	port2
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	Accept
NAT	Enabled
Log Allowed Traffic	All Sessions



## Pour afficher la table de routage

- Dans l'interface CLI du Local-FortiGate, connectez-vous avec le nom d'utilisateur admin et le mot de passe password.
- Entrez la commande suivante pour lister les entrées de la table de routage :

```
get router info routing-table all
```

Remarque : la deuxième route par défaut n'est pas affichée.

- Entrez la commande suivante pour lister les entrées de la base de données de la table de routage :

```
get router info routing-table database
```

- Vérifiez que la deuxième route par défaut est affichée comme inactive.

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S      0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C      *> 10.0.1.0/24 is directly connected, port3
C      *> 10.200.1.0/24 is directly connected, port1
C      *> 10.200.2.0/24 is directly connected, port2
C      *> 172.16.100.0/24 is directly connected, port8
```

## Configurer les moniteurs d'état de lien (Link Health Monitors)

Vous allez configurer deux moniteurs d'état de lien afin de surveiller l'état des routes port1 et port2.

### Pour configurer la surveillance de l'état de lien

1. En continuant dans la session CLI du Local-FortiGate, entrez les commandes suivantes pour créer un moniteur d'état de lien pour port1 sur le Local-FortiGate :

port1 on Local-FortiGate:

```
config system link-monitor
  edit port1-monitor
    set srcintf port1
    set server 4.2.2.1
    set gateway-ip 10.200.1.254
    set protocol ping
    set update-static-route enable
  next
end
```

2. Entrez les commandes suivantes pour configurer un autre moniteur d'état de lien pour port2 :

```
config system link-monitor
  edit port2-monitor
    set srcintf port2
    set server 4.2.2.2
    set gateway-ip 10.200.2.254
    set protocol ping
    set update-static-route enable
```

## Tester le basculement de route (Route Failover)

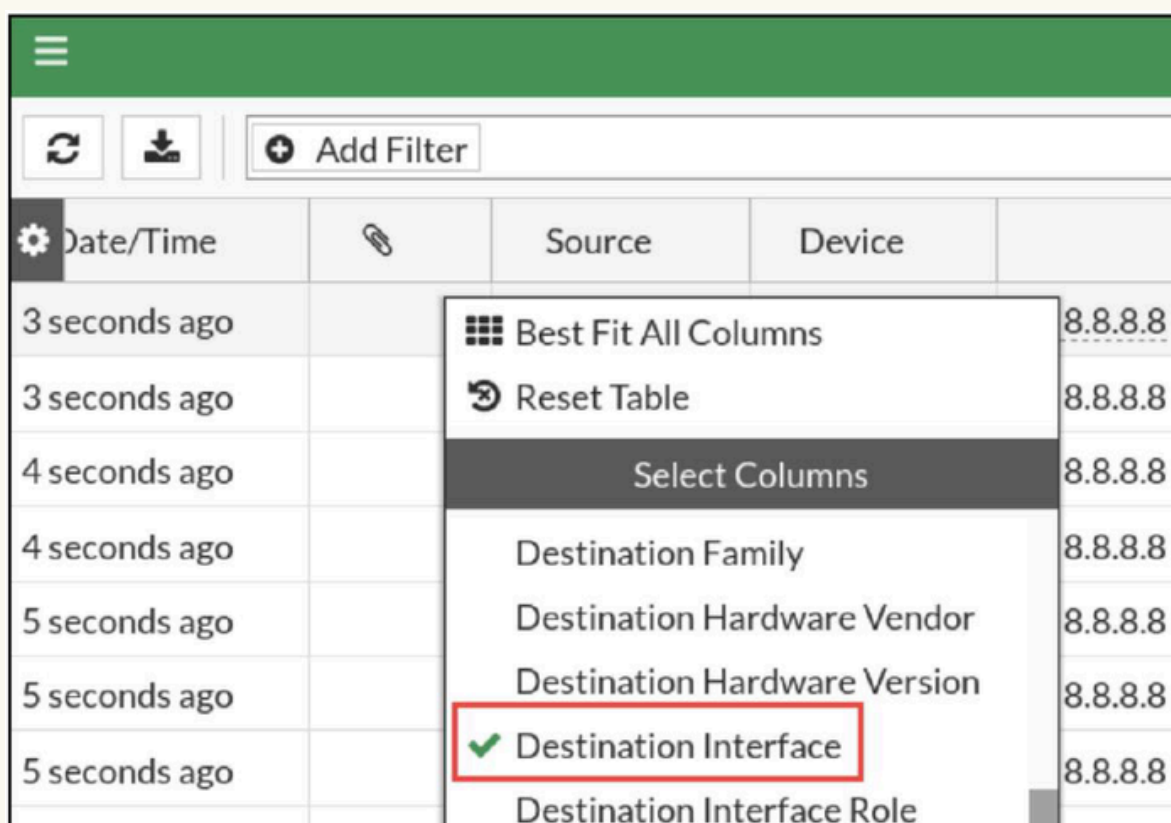
Tout d'abord, vous allez accéder à différents sites web et utiliser les journaux Forward Traffic pour vérifier que la route port1 est bien utilisée.

Ensuite, vous forcerez un basculement en reconfigurant le moniteur d'état de lien de port1 afin qu'il envoie un ping vers une adresse IP invalide.

Vous générerez alors du trafic supplémentaire et utiliserez les journaux Forward Traffic pour vérifier que la route port2 est utilisée.

### Pour confirmer que la route via port1 est la route principale

1. Dans l'interface graphique du Local-FortiGate, cliquez sur Log & Report > Forward Traffic.
2. Faites un clic droit sur l'une des colonnes pour ouvrir le menu contextuel.
3. Dans la section Select Columns, sélectionnez Destination Interface.



4.Faites défiler vers le bas dans le menu contextuel, puis cliquez sur Apply.

La colonne Destination Interface s'affiche.

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2 minutes ago		10.0.1.10	8.8.8.8			✓ 71 B / 179 B	Full Access (1)	port1
2 minutes ago		10.0.1.10	8.8.8.8			✓ 71 B / 143 B	Full Access (1)	port1
2 minutes ago		10.0.1.10	8.8.8.8			✓ 77 B / 185 B	Full Access (1)	port1
2 minutes ago		10.0.1.10	8.8.8.8			✓ 77 B / 149 B	Full Access (1)	port1
2 minutes ago		10.0.1.10	8.8.8.8			✓ 84 B / 145 B	Full Access (1)	port1

5.Sur la machine virtuelle Local-Client VM, ouvrez quelques nouveaux onglets dans le navigateur et visitez quelques sites web, par exemple :

6.Dans l'interface graphique du Local-FortiGate, cliquez sur Log & Report > Forward Traffic.

7.Cliquez sur l'icône refresh (actualiser).

Date/Time		Source	Device	Destination
2022/08/16 09:08:33		10.0.1.10		100.21.215.181 (www.testingmcafee.es.com)
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)
2022/08/16 09:07:12		10.0.1.10		54.188.94.105 (push.services.mozilla.com)

8. Localisez les entrées de journaux correspondant aux trois sites web que vous avez consultés et vérifiez que leur Destination Interface indique port1.

Date/Time	%	Source	Device	Destination	Applic...	Result	Policy	Destination Interface
2022/08/16 09:10:21		10.0.1.10		142.251.126.95 (safebrowser.googleapis.com)		2.47 kB / 0.00 kB	Full Access (2)	port1
2022/08/16 09:09:40		10.0.1.10		54.54/68.244 (eu.httpbin.org)		3.94 kB / 1.55 MB	Full Access (2)	port1
2022/08/16 09:09:39		10.0.1.10		54.54/68.244 (eu.httpbin.org)		1.67 kB / 89.70 kB	Full Access (2)	port1
2022/08/16 09:09:39		10.0.1.10		54.54/68.244 (eu.httpbin.org)		3.95 kB / 628.35 kB	Full Access (2)	port1
2022/08/16 09:09:27		10.0.1.10		100.21.215.181 (www.testingmofeetles.com)		1.31 kB / 4.81 kB	Full Access (1)	port1
2022/08/16 09:08:33		10.0.1.10		100.21.215.181 (www.testingmofeetles.com)		216 B / 112 B	Full Access (2)	port1
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulbenefunmagic.neverssl.com)		1.56 kB / 2.90 kB	Full Access (2)	port1
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulbenefunmagic.neverssl.com)		971 B / 3.06 kB	Full Access (1)	port1
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulbenefunmagic.neverssl.com)		216 B / 112 B	Full Access (1)	port1

Cela vérifie que la route port1 est actuellement la route utilisée.

## Pour forcer le basculement (failover)

1.Revenez à la session CLI du Local-FortiGate, puis entrez les commandes suivantes pour modifier le moniteur de lien du port1 :

```
config system link-monitor
edit port1-monitor
set server 10.200.1.13
next
end
```

1.Revenez à la session CLI du Local-FortiGate, puis entrez les commandes suivantes pour modifier le moniteur de lien du port1 :

2.Attendez quelques secondes.

Comme 10.200.1.13 est un hôte inexistant dans le réseau de laboratoire, le moniteur d'état de lien ne reçoit aucune réponse.

De ce fait, le moniteur d'état de lien suppose que la connexion Internet du port1 est hors service et supprime la route correspondante de la table de routage.

3.Laissez votre session CLI du Local-FortiGate ouverte.

## Pour vérifier le changement de route

Dans l'interface graphique du Local-FortiGate, cliquez sur Log & Report > System Events > General System Events.

Vérifiez que le Local-FortiGate a bien détecté la panne du lien et supprimé la route correspondante du port1.

<div><div><div><div></div></div><div><div></div></div><div><div>Add Filter</div></div></div><div><div>add System Events -</div><div></div><div>Details</div></div></div>				
Date/Time	Level	User	Message	Log Description
34 seconds ago	<div><div></div><div></div><div></div><div></div><div></div></div>		Static route on interface port1 may be removed by link-monitor port1-monitor...	Routing information changed
34 seconds ago	<div><div></div><div></div><div></div><div></div><div></div></div>		Link Monitor initial state is dead, protocol: ping	Link monitor status
37 seconds ago	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div>admin</div>	Edit system/link-monitor port1-monitor	Object attribute configured
4 minutes ago	<div><div></div><div></div><div></div><div></div><div></div></div>		Static route on interface port2 may be added by link-monitor port2-monitor R...	Routing information changed
4 minutes ago	<div><div></div><div></div><div></div><div></div><div></div></div>		Link Monitor changed state from dead to alive, protocol: ping.	Link monitor status
4 minutes ago	<div><div></div><div></div><div></div><div></div><div></div></div>		Static route on interface port1 may be added by link-monitor port1-monitor R...	Routing information changed

2.Cliquez sur Dashboard > Network, puis cliquez sur Routing pour l'agrandir en plein écran.

3.Vérifiez que la route port2 a remplacé la route port1 dans la table de routage.

Routing					Static & Dynamic
<div> <div>5 Routes</div> <div> <div>Connected</div> <div>Static</div> </div> </div>		<div> <div>5 Routes</div> <div> <div>port2</div> <div>port3</div> <div>port1</div> <div>portB</div> </div> </div>			
Route Lookup	View	Create Address	Search		
Network	Gateway IP	Interfaces	Distance	Type	
0.0.0.0/0	10.200.2.254	port2	20	Static	
10.0.1.0/24	0.0.0.0	port3	0	Connected	
10.200.1.0/24	0.0.0.0	port1	0	Connected	
10.200.2.0/24	0.0.0.0	port2	0	Connected	
172.16.100.0/24	0.0.0.0	portB	0	Connected	

Pour vérifier les journaux de trafic

1. Sur la machine virtuelle Local-Client VM, ouvrez quelques nouveaux onglets dans le navigateur et visitez quelques sites web, par exemple :
  - <http://neverssl.com>
  - <http://www.testingmcafeesites.com>
  - <http://eu.httpbin.org>
2. Revenez à l'onglet du navigateur où vous êtes connecté à l'interface graphique du Local-FortiGate, puis cliquez sur Log & Report > Forward Traffic.
3. Localisez les entrées de journaux correspondant aux trois sites web que vous avez consultés et vérifiez que leur Destination Interface indique port2.

Date/Time	Source	Device	Destination	App.	Result	Policy	Destination Interface
2022/08/16 09:30:00	10.0.1.10		51.147.68.244 (eu.httpbin.org)		✓ 216 B / 112 B	Backup_Access(2)	port2
2022/08/16 09:33:16	10.0.1.10		10.216.36.56 (www.testingmcafeesites.com)		✓ 216 B / 112 B	Backup_Access(2)	port2
2022/08/16 09:29:01	10.0.1.10		54.223.124.45 (uniqueip.liverlightcloudservices.com)		✓ 216 B / 112 B	Backup_Access(2)	port2
2022/08/16 09:29:00	10.0.1.10		31.223.124.45 (uniqueip.liverlightcloudservices.neverssl.com)		✓ 1.56 kB / 2.90 kB	Backup_Access(2)	port2

## Restaurer la table de routage

Avant de commencer le prochain exercice, vous allez restaurer la configuration du serveur du moniteur d'état de lien du port1 avec une adresse hôte valide.

Cela permettra de rétablir la route par défaut du port1 comme meilleure route dans la table de routage.

## Restaurer la table de routage



Avant de commencer le prochain exercice, vous allez restaurer la configuration du serveur du moniteur d'état de lien du port1 avec une adresse hôte valide.

Cela permettra de rétablir la route par défaut du port1 comme meilleure route dans la table de routage.

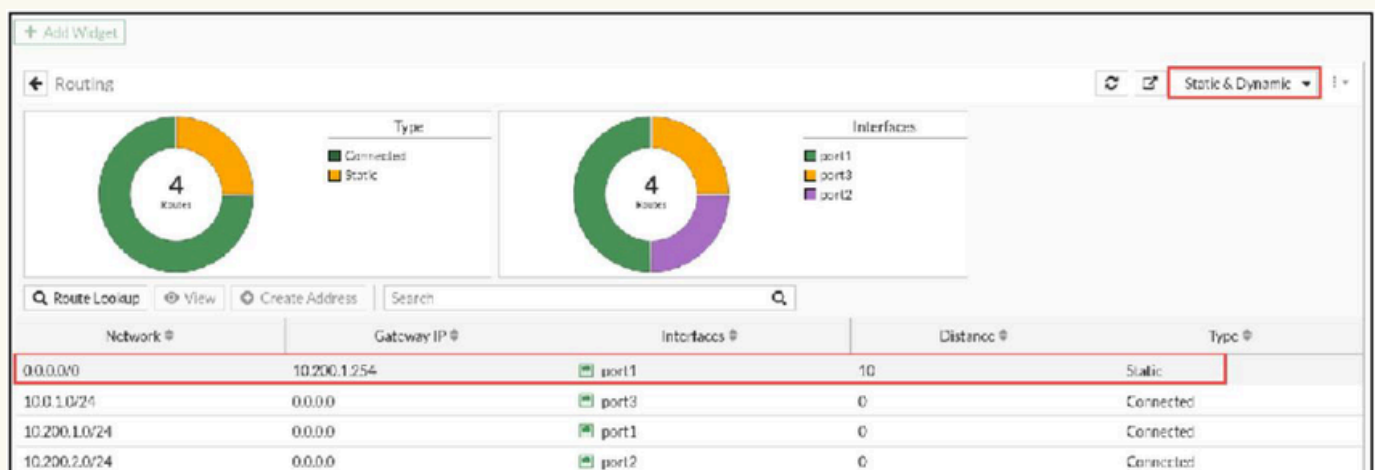
## Restaurer la configuration du moniteur d'état de lien du port1

```
config system link-monitor
edit port1-monitor
set server 4.2.2.1
next
end
```

2.Fermez la session CLI du Local-FortiGate.

## Pour vérifier la table de routage

- 1.Dans l'interface graphique du Local-FortiGate, cliquez sur Dashboard > Network, puis cliquez sur Routing pour l'agrandir en plein écran.
- 2.Vérifiez que la route du port1 a remplacé la route du port2 dans la table de routage.



Network #	Gateway IP #	Interfaces #	Distance #	Type #
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected

## Restons en contact

👉 Vous pouvez nous contacter directement à l'adresse suivante :  
**[info@reseauenclair.com](mailto:info@reseauenclair.com)**

