

**PROCEDURE  
D'INSTALLATION  
: ROUTAGE  
STORMSHIELD**



**PROJET  
CUB**

- **Objectif :** Assurer la sécurité du réseau via le filtrage du trafic, le chiffrement des communications (VPN), la gestion sécurisée, la surveillance des événements et la sauvegarde des configurations, afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes.

- **Prérequis**

- **Système d'exploitation**

- OS Stormshield

- **Ressources matérielles (minimum recommandé)**

- **CPU** : 1 cœurs
    - **RAM** : 1 Go
    - **Disque** : 32 Go (SSD recommandé)
    - **Connexion réseau** : 1 Gbit/s

## Routage système (route par défaut)

**ROUTAGE SYSTÈME**

- Routage : route par défaut

**NETWORK / ROUTING**

IPv4 STATIC ROUTES   IPv4 DYNAMIC ROUTING   IPv4 RETURN ROUTES

**General**

Default gateway (router):

**STATIC ROUTES**

Searching...   + Add   X Delete

Status	Destination network (host, network ...)
--------	---

**CREATE AN OBJECT**

**Host**

Object name: RTR\_Default

IPv4 address: 212.13.25.120

MAC address: 01:23:45:67:89:ab (optional)

**Resolution**

☒ None (static IP)   ☐ Automatic

Comments:

**CREATE**

La passerelle par défaut est renseignée dans l'onglet **ROUTES STATIQUES IPV4** du menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage**, paramètre **Passerelle par défaut (routeur)**. Ce paramètre peut prendre comme valeur :

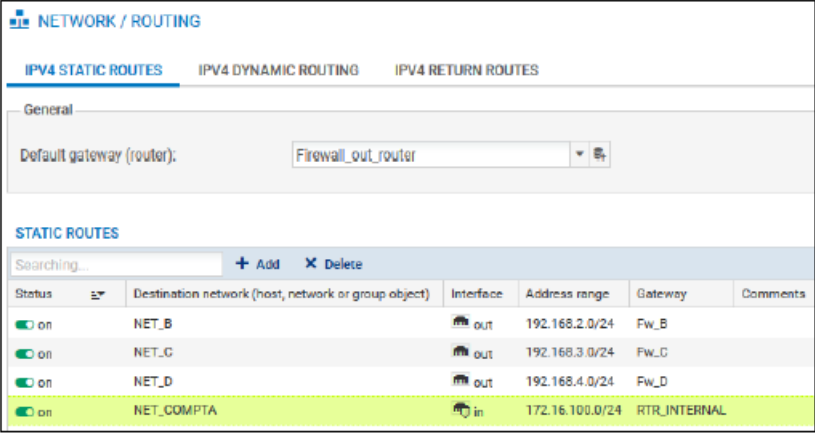
- **Un objet machine** : Pour spécifier une seule passerelle par défaut sans test de disponibilité, sans répartition de charge et sans passerelle de secours.
- **Un objet routeur** : Les différentes passerelles configurées dans l'objet routeur permettent d'effectuer des tests de disponibilité, de la répartition de charge et d'utiliser des passerelles de secours.

**NOTE** : sur une interface obtenant dynamiquement son adresse IP (par DHCP), l'obtention du bail DHCP donne lieu à la création d'un objet nommé « Firewall\_<nom\_interface>\_router », utilisable en tant que passerelle par défaut.

## ROUTAGE système (route statique)

**ROUTAGE SYSTÈME**

- Routage : route statique



The screenshot shows the 'NETWORK / ROUTING' configuration page. Under the 'IPv4 STATIC ROUTES' tab, the 'General' section has 'Default gateway (router):' set to 'Firewall\_out\_router'. The 'STATIC ROUTES' section contains a table with the following data:

Status	Destination network (host, network or group object)	Interface	Address range	Gateway	Comments
on	NET_B	out	192.168.2.0/24	Fw_B	
on	NET_C	out	192.168.3.0/24	Fw_C	
on	NET_D	out	192.168.4.0/24	Fw_D	
on	NET_COMPTA	in	172.16.100.0/24	RTR_INTERNAL	

Below the table, there is a search bar and buttons for '+ Add' and 'X Delete'. To the left of the table, there is a text label 'En cas de configuration incohérente'.

At the bottom right, there is a log entry: '05:34:26 PM Network / Routing: Gateway is not routable 72ms'.

STORMSHIELD

5

La configuration des routes statiques s'effectue dans l'encadré **ROUTES STATIQUES IPV4** du premier onglet du menu **CONFIGURATION** ⇒ **RÉSEAU** ⇒ **Routage**.

L'encadré contient une barre de recherche et deux boutons pour **ajouter** ou **supprimer** une route. Il contient également une fenêtre qui **liste** toutes les routes statiques et leurs paramètres. Le bouton « Ajouter » ajoute une entrée à la liste. Les paramètres qui doivent obligatoirement être renseignés sur cette ligne sont :

- **Etat** : On / off
- **Réseau de destination** : Peut-être un objet machine, réseau ou un groupe.
- **Passerelle** : Un objet machine ou routeur qui représente l'adresse IP de la passerelle permettant d'atteindre le réseau de destination.

- **Interface** : Le processus de sélection de l'interface de sortie pour atteindre la passerelle. Le firewall détermine automatiquement le plan d'adressage en fonction des paramètres de l'interface. La sélection de l'interface est cruciale, surtout dans le cas d'un bridge contenant des interfaces protégées et non protégées, car elle permet de déterminer si le réseau doit être considéré comme protégé ou non. Si le plan d'adressage de l'interface et de la passerelle diffère, un message d'erreur indique que la passerelle n'est pas routable.

## **Routage avancé (routage dynamique)**

## ROUTAGE AVANCÉ

- Routage dynamique

The screenshot shows the 'NETWORK / ROUTING' configuration page. The 'IPV4 DYNAMIC ROUTING' tab is selected. Under the 'General' section, there is a 'General' sub-section with a 'OFF' toggle. Below this, there is a text area containing configuration comments and code snippets for 'protocol direct', 'protocol kernel', and 'protocol device'. The 'Advanced properties' section is expanded, showing two checkboxes: 'Restart dynamic routing when the firewall becomes active (high availability)' (unchecked) and 'Add IPv4 networks distributed via dynamic routing to the table of protected networks' (checked).

```
# The direct protocol automatically generates device routes to
# all network interfaces.
protocol direct {
}

# This pseudo-protocol performs synchronization between BIRD's routing
# tables and the kernel.
protocol kernel {
    learn;           # Learn all alien routes from the kernel
    persist;         # Don't remove routes on bird shutdown
    scan time 20;    # Scan kernel routing table every 20 seconds
    import all;      # Default is import all
    export all;      # Default is export none
    preference 254;  # Protect existing routes
}

# This pseudo-protocol watches all interface up/down events.
protocol device {
    scan time 10;    # Scan interfaces every 10 seconds
}
```

Advanced properties

- ☐ Restart dynamic routing when the firewall becomes active (high availability)
- ☒ Add IPv4 networks distributed via dynamic routing to the table of protected networks

8

Le routage dynamique peut se configurer depuis l'interface graphique dans l'onglet **ROUTAGE DYNAMIQUE IPV4** du menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage**. Les réseaux de destination ajoutés dans la table de routage par un protocole dynamique peuvent être ajoutés à la table des réseaux protégés.

**Routage avancée (routage par politique)**

## ROUTAGE AVANCÉ

- Routage par politique : configuration

The screenshot displays the Stormshield configuration interface. At the top, the title is 'SECURITY POLICY / FILTER - NAT'. Below it, there's a search bar and a table of filtering rules. Rule 1 is selected, and an arrow points to the 'EDITING RULE NO 1' dialog box. In this dialog, the 'ACTION' tab is active, and the 'Routing' section is highlighted. The 'Gateway - router' field is set to 'ROUTER\_ISP2'.

La mise en œuvre d'une directive de routage par politique s'effectue dans le champ Action d'une règle de filtrage. Deux types d'objet peuvent être renseignés au niveau de ce champ :

- **Un objet machine** : Pour spécifier une passerelle,
- **Un objet routeur** : Permet d'utiliser un objet routeur précédemment configuré et d'attribuer ses paramètres d'équilibrage et de répartition de charge à la règle de filtrage.

## Routage avancée (répartition de charge)

## ROUTAGE AVANCÉ

- Objet routeur : création et configuration

CREATE AN OBJECT

Object name: RTR\_OBJECT\_INTERNET

Comments:

USED GATEWAYS

Host	Device(s) for testing availability	Weight	Comments
RTR_ISP1	Test the gateway directly	3	
RTR_ISP2	dns1.google.com	1	

BACKUP GATEWAYS

Move to the list of backups

Advanced configuration

Load balancing: By connection

Enable backup gateways

☒ When all gateways cannot be reached

☐ When at least one gateway cannot be reached

☐ When the number of gateways that can be reached is lower than 2

☐ Enable all backup gateways when unavailable

If no gateways are available: Default route

CLOSE CREATE AND DUPLICATE CREATE

La configuration d'un routage par répartition de charge s'effectue dans un objet routeur. Les différentes passerelles doivent être ajoutées dans l'onglet **LISTE DES PASSERELLES UTILISÉES**. Chaque ligne permet de renseigner :

- La passerelle : avec un objet machine
- Test de disponibilité : Permet de tester la disponibilité de la passerelle en utilisant des pings. Ce paramètre peut avoir plusieurs valeurs :
  - Pas de test de disponibilité** : La disponibilité de la passerelle n'est pas testée.
  - Tester directement la passerelle** : Des commandes ping sont envoyées directement à la passerelle pour tester sa disponibilité.
  - Une machine ou groupe de machine** : se trouvant derrière la passerelle, vers lesquelles les pings sont envoyés pour tester la disponibilité et le fonctionnement de la passerelle.

Par défaut, l'état de chaque passerelle est vérifié toutes les 15 secondes en envoyant un ping à chaque machine renseignée. Dans le cas où aucune réponse



n'est reçue au bout de 2 secondes, le firewall recommence 3 fois avant de considérer la passerelle indisponible. L'état des passerelles est visible dans le menu routes de la supervision.

## ROUTAGE AVANCÉ

- Objet routeur : création et configuration

13

Le poids (encadré rouge) permet d'affecter à une passerelle un pourcentage du trafic géré par l'objet routeur. La valeur d'un poids doit être comprise entre 1 et 1024.

L'algorithme utilisé (encadré bleu) pour la répartition de charge est configuré par le paramètre **Répartition de charge (Configuration avancée)** :

- **Aucune répartition** : Le trafic est transmis exclusivement à la première passerelle qui apparaît dans la liste.
- **Par connexion** : Répartit le trafic en fonction des adresses IP et des numéros de ports source et destination. Cet algorithme est recommandé parce qu'il permet de répartir également les connexions provenant d'une même machine.

- **Par adresse IP source** : Répartit le trafic en fonction de l'adresse source. Il permet de s'assurer que le trafic d'une machine sera toujours renvoyé vers la même passerelle.

**ROUTAGE AVANCÉ**

- **Objet routeur : création et configuration**

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name: RTR\_OBJECT\_INTERNET

Comments:

USED GATEWAYS

BACKUP GATEWAYS

+ Add - Delete Move to the list of backups

Host	Device(s) for testing availability	Weight	Comments
RTR_SP1	Test the gateway directly	3	
RTR_SP2	dns1.google.com	7	

Advanced configuration

Load balancing: By connection

Enable backup gateways

☒ When all gateways cannot be reached

☐ When at least one gateway cannot be reached

☐ When the number of gateways that can be reached is lower than 2

☐ Enable all backup gateways when unavailable

If no gateways are available: Default route

Default route  
Do not route

STORMSHIELD

14

Lorsqu'un objet routeur est utilisé par une règle de filtrage (routage par politique), et qu'aucune passerelle de cet objet n'est joignable, le comportement du firewall peut être configuré par le paramètre **Si aucune passerelle n'est disponible** :

- **Routage par défaut** : Le trafic est transmis au routeur par défaut.
- **Ne pas router** : Le trafic est bloqué par le firewall.

La répartition de charge peut fonctionner avec **64 passerelles au maximum**.

## Routage avancée (passerelles de secours)

### ROUTAGE AVANCÉ

- Les passerelles de secours : création et configuration

The screenshot shows the 'CREATE AN OBJECT' window for configuring backup gateways. On the left is a sidebar with navigation options: Host, DNS name (FQDN), Network, IP address range, Router, Group, IP Protocol, Port, Port group, Region group, and Time object. The main area is divided into 'USED GATEWAYS' and 'BACKUP GATEWAYS' tabs. The 'BACKUP GATEWAYS' tab is active, showing a table with two entries:

	Host	Device(s) for te...	Weight	Comments
1	RTR_ISP3	dns1.google.com	2	
2	RTR_ISP4	dns2.google.com	1	

Below the table is the 'Advanced configuration' section. It includes a 'Load balancing' dropdown set to 'By connection'. Under 'Enable backup gateways', there are three radio button options: 'When all gateways cannot be reached' (selected), 'When at least one gateway cannot be reached', and 'When the number of gateways that can be reached is lower than 2'. There is also a checkbox for 'Enable all backup gateways when unavailable' and a dropdown for 'If no gateways are available' set to 'Default route'. At the bottom are buttons for 'CLOSE', 'CREATE AND DUPLICATE', and 'CREATE'.

16

Plusieurs passerelles de secours peuvent être ajoutées dans l'onglet **LISTE DES PASSERELLES DE SECOURS** d'un objet routeur. Pour chaque passerelle de secours, on peut définir un équipement de test et un poids comme pour les passerelles principales.

La configuration avancée permet de configurer deux éléments :

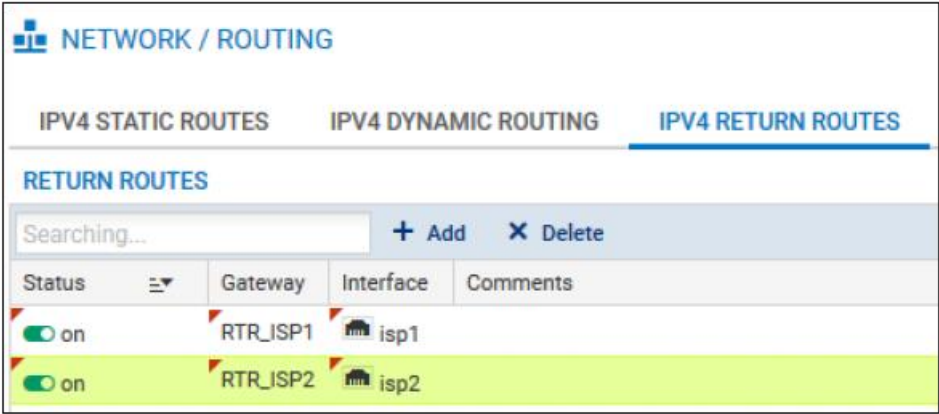
- Quand la ou les passerelles de secours doivent être activées :
  - Lorsque toutes les passerelles principales sont injoignables,
  - Lorsqu'au moins une passerelle principale est injoignable,
  - Lorsque le nombre de passerelles principales joignables est inférieur à un certain seuil. ( $1 < \text{seuil} \leq \text{nombre de passerelles principales}$ ).
- S'il faut activer une ou toutes les passerelles de secours : par défaut, seule la première passerelle de secours joignable

dans la liste est utilisée sauf si l'option **Activer toutes les passerelles de secours en cas d'indisponibilité** est sélectionnée.

## Routage avancée (route de retour)

ROUTAGE AVANCÉ

- Route de retour : création et configuration



The screenshot shows the 'NETWORK / ROUTING' section of the Stormshield configuration interface. It features three tabs: 'IPv4 STATIC ROUTES', 'IPv4 DYNAMIC ROUTING', and 'IPv4 RETURN ROUTES'. The 'IPv4 RETURN ROUTES' tab is selected. Below the tabs, there is a 'RETURN ROUTES' section with a search bar and '+ Add' and 'X Delete' buttons. A table lists the configured return routes.

Status	Gateway	Interface	Comments
on	RTR_ISP1	isp1	
on	RTR_ISP2	isp2	

STORMSHIELD 18

La configuration d'une route de retour s'effectue dans l'onglet **ROUTE de RETOUR** du menu **CONFIGURATION** ⇒ **RÉSEAU** ⇒ **Routage**. Il faut ajouter une ligne pour chaque route, dans laquelle il faut spécifier la passerelle, et l'interface par laquelle elle est joignable.

