NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SD-WAN : SÉLECTIONNER LE MEILLEUR LIEN RÉSEAU

Produits concernés : SNS 5 et versions supérieures

Dernière mise à jour du document : 20 mai 2025

Référence : sns-fr-sd-wan_sélectionner_meilleur_lien_réseau-note_technique

Table des matières

Avant de commencer

Le SD-WAN (*Software Defined Wide Area Network*) est un ensemble de fonctionnalités logicielles permettant de faciliter la gestion de réseaux interconnectés et sécurisés ainsi que la gestion de liens WAN multiples.
Une des approches fonctionnelles du SD-WAN consiste à choisir de manière automatique et transparente les liens réseau à emprunter selon les flux et leurs contraintes de performances associées (latence acceptée, taux de disponibilité...).

Cette note technique s'adresse aux entreprises disposant d'accès WAN multiples (Internet, succursales...) et souhaitant optimiser la sélection des liens selon les flux (VoIP, Web, ERP...).

Pour mettre en œuvre cette approche, l'administrateur doit configurer les liens à sa disposition et définir des objets routeurs reprenant les contraintes de niveau de services (SLA - *Service Level Agreement*) souhaitées et qui seront utilisés, selon la configuration envisagée, en tant que passerelle par défaut, dans des routes statiques ou dans les règles de routage par politique (*Policy Based Routing* - PBR) pour les flux concernés.

Comprendre les différentes composantes du SD-WAN SNS

Comprendre les paramètres de supervision

Méthode de détection et Port

Deux méthodes de détection de disponibilité et de performance des liens sont proposées sur les firewalls SNS :

- La méthode de détection de type ICMP : cette méthode est basée sur l'envoi régulier de paquets de type *ICMP Request* sur chaque lien (envoi de deux paquets lors de chaque requête de détection).
- La méthode de détection de type *TCP Probe* : cette méthode est basée sur des requêtes vers le port TCP utilisé par le serveur applicatif à joindre.
  La disponibilité et les performances de chaque lien sont ainsi testées en initiant une connexion au service TCP depuis le firewall vers l'objet cible en utilisant le port associé (envoi d'une seule tentative de connexion lors de chaque requête de détection).

NOTE
La méthode de type ICMP est à privilégier sauf lorsque le protocole ICMP est bloqué par un équipement situé entre le firewall SNS et la cible, ou lorsque la cible n'accepte pas les requêtes ICMP.

Si plusieurs serveurs applicatifs sont utilisés pour un flux faisant l'objet de SLA SD-WAN, Stormshield recommande de positionner ces serveurs dans un objet réseau de type groupe et d'utiliser ce groupe comme cible des tests de disponibilité. Dans ce cas, les résultats des tests de disponibilité sont une moyenne des résultats des tests vers chacun des serveurs.

Délai d'expiration (s)

Il s'agit du délai maximal attendu pour une réponse à une tentative de connexion avec la méthode de détection choisie.

Au-delà de cette valeur, la tentative de connexion est considérée comme un échec et le nombre de tentatives s'incrémente d'une unité, jusqu'à atteindre le nombre d'échecs avant de déclarer que l'objet cible est injoignable ou que le lien est dégradé (si des seuils SLA sont configurés).

Intervalle de tests (s)

Il s'agit du laps de temps qui s'écoule entre deux tentatives de connexion.

Échecs avant dégradation

Il s'agit du nombre maximal de tentatives de connexion échouées avant de déclarer que l'objet cible est injoignable ou que le lien est dégradé (si des seuils SLA sont configurés).

Comprendre les métriques du SLA SD-WAN

La latence (ms)

La notion de latence SD-WAN sur les firewalls SNS représente le temps écoulé entre l'envoi d'un paquet et la réception d'une réponse à celui-ci. Il s'agit donc réellement d'une notion de RTT (*round-trip time*)
Ce paramètre est très dépendant du type de flux et des fournisseurs d'accès.
C'est le paramètre **Fréquence (s)** qui détermine le temps écoulé entre deux mesures de latence.
La latence affichée dans le module de supervision temps réel du SD-WAN correspond à la dernière valeur de latence mesurée pour chaque passerelle.

La gigue (ms)

La gigue représente la variation de la latence au cours du temps.
Elle est calculée par rapport à toutes les valeurs de latence mesurées au cours des 10 dernières minutes.
La valeur affichée dans le module de supervision temps réel du SD-WAN correspond donc à une moyenne de la gigue au cours des 10 dernières minutes.

Taux de perte de paquets (%)

Il s'agit du ratio entre le nombre de requêtes de connexion émises et le nombre de réponses reçues.
Sur un firewall SNS, ce pourcentage toléré est configurable au dixième près.
Il est calculé par rapport à tous les paquets perdus lors des tests de connexions sur les 10 dernières minutes.

La valeur affichée dans le module de supervision temps réel du SD-WAN correspond donc à une moyenne du taux de perte de paquets au cours des 10 dernières minutes.

Taux d'indisponibilité

Il s'agit du ratio entre le temps où une passerelle est disponible et le temps pendant lequel elle a été inaccessible.
Ce paramètre n'est pas un seuil SD-WAN à proprement parler : il permet principalement d'afficher des statistiques au sujet de la disponibilité des passerelles.
Il n'est donc pas pertinent de renseigner une valeur maximale pour ce paramètre.

La valeur affichée dans le module de supervision temps réel du SD-WAN représente une moyenne du taux d'indisponibilité au cours des 10 dernières minutes.

Évaluer les valeurs à appliquer à chaque métrique

Appliquer directement des seuils à un objet utilisé dans une politique de filtrage en production peut se révéler fastidieux et improductif (bascules régulières et injustifiées des flux sur les différents liens).

Pour évaluer les valeurs à appliquer à chaque métrique sans perturber la production, Stormshield vous suggère d'utiliser la méthode suivante :

1. Créer un objet routeur de test, sur lequel sont positionnées des valeurs de métriques conseillées et recueillies auprès de vos fournisseurs d'accès et de vos fournisseurs de solutions logicielles (VoIP, flux métier...).
2. Utiliser cet objet routeur dans une règle de filtrage neutre, placée en dernière position de la politique de sécurité (avant l'éventuelle règle de *deny all*), afin de déclencher la supervision du routeur, de ses passerelles et d'observer les comportements (changements de liens) liés aux valeurs des différentes métriques. Pour créer cette règle, vous pouvez vous référer à la partie Créer la règle de filtrage pour les flux VoIP.
3. Affiner ces valeurs jusqu'à obtenir le comportement souhaité vis à vis du flux considéré.

Ainsi, le changement des valeurs des métriques ne présente aucun impact sur les flux de production et permet d'affiner sereinement les valeurs avant de les adopter dans la règle de filtrage concernant le flux en production.

Lors de l'observation des valeurs relevées pour les différentes métriques (étapes 2 et 3), notez que les données affichées dans les graphes de supervision SD-WAN de l'interface Web d'administration SNS sont stockées dans une base de données locales et sont donc agrégées régulièrement afin de limiter l'espace disque utilisé.

Il est donc recommandé d'utiliser une solution de supervision basée sur SNMP (de type *Zabbix*, *Centreon*...) et sur la MIB STORMSHIELD-ROUTE-MIB v4.3.x, téléchargeable depuis le menu **Téléchargements** de MyStormshield, afin d'observer les valeurs en temps réel des différentes métriques et de stocker ces relevés sur de plus longues périodes pour une meilleure mise au point des valeurs appropriées.

Plus d'informations sur les métriques du SLA SD-WAN.

Comprendre le mécanisme de bascule et le choix des liens empruntés

Lors de chaque mesure / calcul de métrique, chaque lien est évalué : il s'agit de comparer la dernière mesure (latence) ou le dernier calcul (gigue, taux de perte de paquets) de métrique à la valeur définie dans le SLA SD-WAN. Si cette mesure ne respecte pas les seuils définis, le lien est considéré comme dégradé.

Un lien peut donc être caractérisé par 3 états possibles :

- Optimal : le lien est disponible et les calculs / mesures de métriques respectent les seuils SLA définis.
- Dégradé : une ou plusieurs métriques ne respectent pas les seuils SLA définis.
- Indisponible : le lien ne peut pas être utilisé suite à un incident.

Les tableaux ci-dessous présentent les mécanismes de bascule de liens et le choix des liens empruntés pour les différents types de connexions possibles.

Dans ce document, les 3 états possibles sont représentés par les symboles suivants :

-  : lien optimal,
-  : lien dégradé,
-  : lien indisponible.

Pour les nouvelles connexions entrantes

Dans le cas d'une configuration à 4 liens (2 liens principaux et 2 liens de secours), le tableau ci-dessous présente comment seront choisis les liens en fonction de leur état respectif à un instant donné, et selon la configuration choisie (partage de charge ou non, valeurs de seuils).

Liens principaux		Liens de secours		Liens utilisés dans l'ordre de la configuration				
				Sans partage de charge	Avec partage de charge			
					Lorsqu'au moins une passerelle est injoignable		Lorsque toutes les passerelles sont injoignables	
Lien 1	Lien 2	Lien 3	Lien 4			Activer toutes les passerelles de secours		Activer toutes les passerelles de secours
✅	✅	✅	✅	1	1,2	1,2	1,2	1,2
⚠	✅	✅	✅	2	2	2	2,3,4	2,3
⚠	⚠	✅	✅	3	3,4	3,4	3,4	3,4
⚠	⚠	⚠	✅	4	4	4	4	4
⚠	⚠	⚠	⚠	1	1,2	1,2	1,2	1,2
⚠	❌	⚠	⚠	1	1	1	1,3,4	1,3
⚠	❌	✅	⚠	3	3	3	3	3
❌	✅	⚠	⚠	2	2	2	2	2
❌	❌	⚠	⚠	3	3,4	3,4	3,4	3,4

Liens principaux		Liens de secours		Liens utilisés dans l'ordre de la configuration				
				Sans partage de charge	Avec partage de charge			
					Lorsqu'au moins une passerelle est injoignable		Lorsque toutes les passerelles sont injoignables	
Lien 1	Lien 2	Lien 3	Lien 4			Activer toutes les passerelles de secours		Activer toutes les passerelles de secours
✗	✗	✗	⚠	4	4	4	4	4
✗	✗	✗	✗	On applique la politique définie dans le champ **Si aucune passerelle n'est disponible** de l'objet routeur : • Routage par défaut (*OnFailPolicy = pass*), • Ne pas router (*OnfailPolicy = block*).				
✗	✗	✓	✗	3	3	3	3	3
✗	✓	✓	✗	2	2	2	2,3	2,3
✗	✓	✓	✓	2	2	2	2,3,4	2,3
✓	✓	✓	✓	1	1,2	1,2	1,2	1,2

Pour les connexions existantes

Cas d'une route par défaut avec redondance (*failover* - pas de répartition de charge) ou de routage statique

Impact d'un changement de passerelle sur les connexions traversantes	
Translation d'adresses (NAT)	**Changement de passerelle***
Sans NAT	Basculement avec conservation des connexions
Avec NAT (politique de NAT ou passage par le proxy)	Paquet RST envoyé au client d'une connexion TCP et nettoyage de la table des connexion (UDP et TCP)

*suivant les règles décrites dans le tableau Pour les nouvelles connexions entrantes.

Cas d'une route par défaut avec répartition de charge ou de routage par politique (*Policy Based Routing*)

<table>
<tr><th colspan="6">Impact d'un changement de passerelle sur les connexions traversantes</th></tr>
<tr><th rowspan="2">Translation d'adresses (NAT)</th><th colspan="5">Changement d'état de la passerelle</th></tr>
<tr><th>✓ → ⚠</th><th>✓ → ✗</th><th>⚠ → ✗</th><th>⚠ → ✓</th><th>✗ → ✓</th><th>✗ → ⚠</th></tr>
<tr><td>Sans NAT</td><td rowspan="2">Conservation des connexions</td><td colspan="2">Basculement avec conservation des connexions</td><td rowspan="2">Conservation des connexions</td><td colspan="2" rowspan="2">Aucun</td></tr>
<tr><td>Avec NAT (politique de NAT ou proxy)</td><td colspan="2">Paquet RST envoyé au client d'une connexion TCP et nettoyage de la table des connexions (UDP et TCP)</td></tr>
</table>

Cas des connexions initiées par le firewall

Impact d'un changement de passerelle sur les connexions initiées par le firewall
Changement de passerelle*
Nettoyage de la table des connexions (UDP et TCP) et reprise du service

*suivant les règles décrites dans le tableau Pour les nouvelles connexions entrantes.

Superviser les liens SD-WAN depuis l'interface d'administration du firewall

Le module de supervision permet d'afficher l'état des passerelles SD-WAN ainsi que les valeurs des métriques liées aux seuils SLA.

Vue synthétique : le tableau de bord des indicateurs de santé

Le tableau de bord SD-WAN, disponible dans l'onglet **Monitoring** > module **Tableau de bord** > cadre **Indicateurs de santé** permet de visualiser en un coup d'œil l'état de tous les objets SD-WAN :

La couleur de l'icône SD-WAN varie selon l'état des routeurs et passerelles utilisés dans la configuration du firewall :

- Vert : toutes les passerelles des routeurs sont opérationnelles et respectent les critères SLA SD-WAN définis,
- Orange : un routeur est en état dégradé car l'une de ses passerelles est en état dégradé ou injoignable,
- Rouge : un routeur est injoignable car toutes ses passerelles sont injoignables.

Un clic sur cette icône renvoie directement dans le module **Supervision** > **SD-WAN**.

Vue détaillée : le module de supervision SD-WAN

Accessible depuis l'onglet **Monitoring** > **Supervision**, le module **SD-WAN** présente le détail des routeurs et passerelles utilisés dans le routage du firewall (route par défaut, routes statiques et routage par politique).

Onglet Temps réel

L'onglet **Temps réel** affiche des informations liées à l'état des routeurs et passerelles supervisés, ainsi que les valeurs SLA SD-WAN de ces passerelles.

Ces informations peuvent prendre les valeurs suivantes :

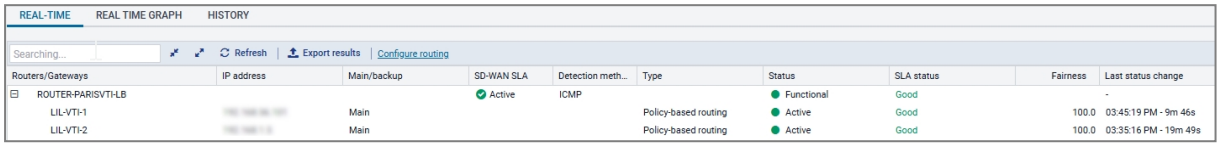
Type	État	Statut SLA
Passerelle	• Active, • En veille (redondance), • Injoignable.	• Bon, • Dégradé, • Injoignable.
Routeur	• Opérationnel (partage de charge), • Opérationnel (redondance - au moins une passerelle est en veille), • Dégradé, • Injoignable.	• Bon, • Dégradé, • Injoignable.

Exemple d'un routeur avec partage de charge

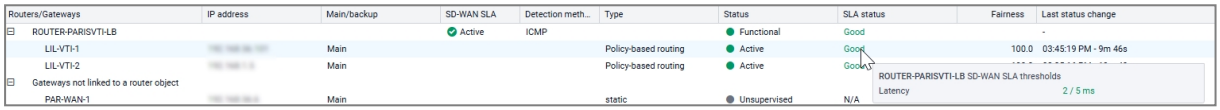
Pour obtenir plus de détails sur les valeurs que peuvent prendre ces différents indicateurs, consultez le module Supervision SD-WAN du Manuel Utilisateur Stormshield SNS v4.

Dans cet exemple, les deux passerelles sont actives.

La valeur de répartition de charge entre les deux passerelles est affichée : elle dépend du poids affecté à chaque passerelle. Lorsque toutes les passerelles ont un poids égal à 1, la répartition affichée est de 100% pour chacune :



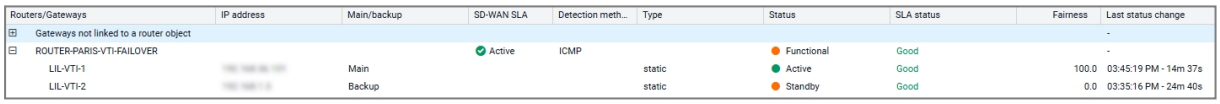
En survolant le statut SLA d'une passerelle avec la souris, la dernière valeur mesurée des indicateurs est affichée :



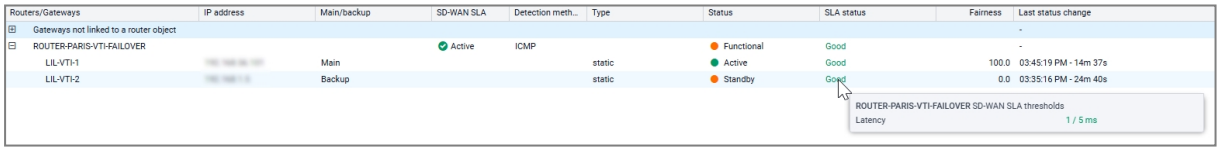
Exemple d'un routeur avec redondance

Une passerelle est active, l'autre est en veille.

La répartition de charge entre les deux passerelles est indiquée : la passerelle active indique 100% tandis que la passerelle en veille affiche 0%.



En survolant le statut SLA d'une passerelle avec la souris, la dernière valeur mesurée des indicateurs est affichée :

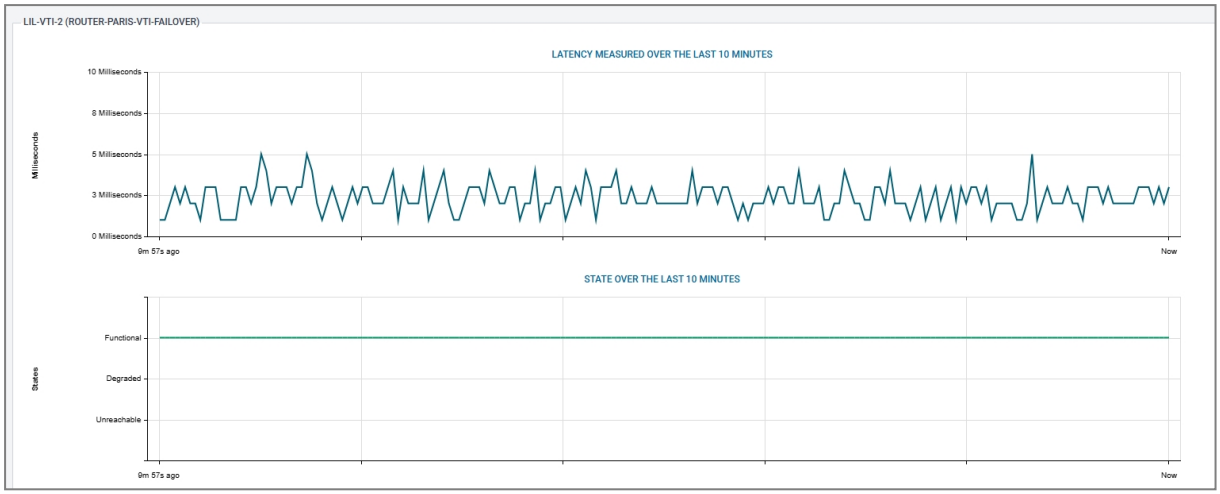


Onglet Graphe temps réel

Cet onglet permet de sélectionner une passerelle d'un routeur donné afin d'en afficher les courbes d'évolution des indicateurs SLA suivants sur les dix dernières minutes :

- Latence,
- Pourcentage de temps passé dans les différents états possibles (opérationnel, dégradé et injoignable).

Exemple :

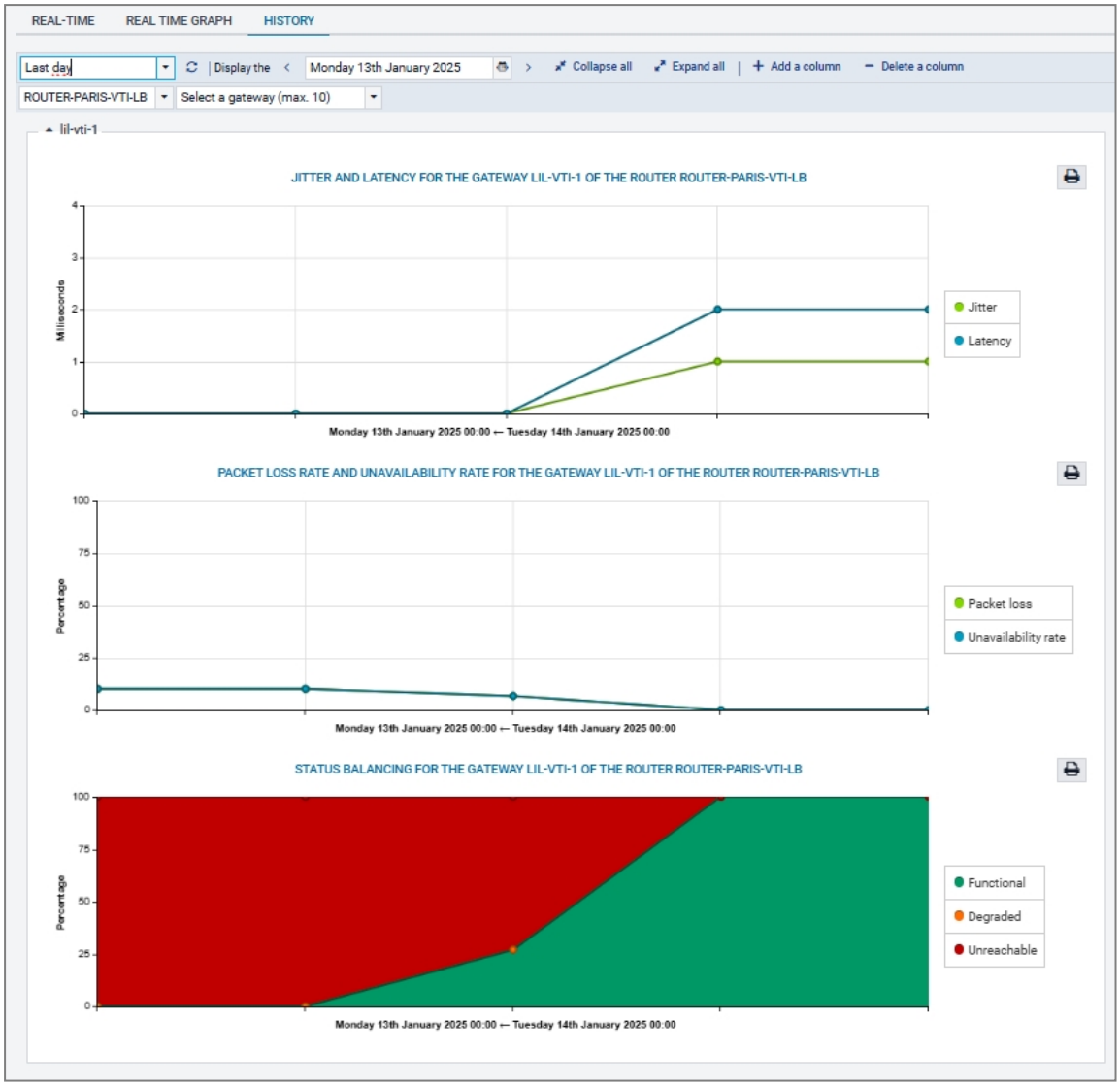


Onglet Historique

Cet onglet permet de sélectionner entre une et cinq passerelles d'un routeur donné afin d'en afficher les courbes d'évolution des différents indicateurs SLA sur la période choisie :

- Gigue et latence,
- Taux de perte de paquets et taux d'indisponibilité,
- Pourcentage de temps passé dans les différents états possibles (opérationnel, dégradé et injoignable).

Exemple :


REAL-TIME
REAL TIME GRAPH
HISTORY
Last day
Display the
Monday 13th January 2025
Collapse all
Expand all
Add a column
Delete a column
ROUTER-PARIS-VTI-LB
Select a gateway (max. 10)
lil-vti-1
JITTER AND LATENCY FOR THE GATEWAY LIL-VTI-1 OF THE ROUTER ROUTER-PARIS-VTI-LB
Milliseconds
Jitter
Latency
Monday 13th January 2025 00:00 — Tuesday 14th January 2025 00:00
PACKET LOSS RATE AND UNAVAILABILITY RATE FOR THE GATEWAY LIL-VTI-1 OF THE ROUTER ROUTER-PARIS-VTI-LB
Percentage
Packet loss
Unavailability rate
Monday 13th January 2025 00:00 — Tuesday 14th January 2025 00:00
STATUS BALANCING FOR THE GATEWAY LIL-VTI-1 OF THE ROUTER ROUTER-PARIS-VTI-LB
Percentage
Functional
Degraded
Unreachable
Monday 13th January 2025 00:00 — Tuesday 14th January 2025 00:00

Exemple 1 : prioriser les flux VoIP

L'exemple de configuration présenté dans cette note technique est celui d'une entreprise disposant de trois accès distants :

- Deux liens associés à deux routeurs (appelés *Router1* et *Router2* dans cette note technique) chez un premier fournisseur d'accès,
- Un lien associé à un routeur (appelé *Router3* dans cette note technique) chez un autre fournisseur d'accès.

Les deux liens du premier fournisseur d'accès sont utilisés comme lien principaux, celui du second fournisseur d'accès est positionné en lien de secours.

Du partage de charge est défini sur les liens actifs.

La configuration SD-WAN décrite doit permettre aux flux VoIP d'emprunter de manière transparente les liens réseau les plus performants à un instant donné, les flux Web empruntant l'autre lien.

Le tableau ci-dessous indique comment seront choisis les liens en fonction de leur état respectif à un instant donné :

Lien 1 (Router1) Principal	Lien 2 (Router2) Principal	Lien 3 (Routeur3) Secours	**Liens utilisés pour la VoIP avec :** • **Partage de charge** • **Activation des passerelles de secours lorsqu'au moins une passerelle est injoignable**
✓	✓	✓	1,2
!	✓	✓	2,3
!	!	✓	3
!	!	!	1,2
!	✗	✓	3
!	✗	!	1,3
✗	✗	!	3
✗	✗	✗	Aucun lien - Route par défaut
✗	✗	✓	3
✗	✓	✓	2,3

Créer les objets

Cette étape consiste à créer les objets nécessaires à la configuration :

- Les objets de type machine correspondant aux passerelles des opérateurs (si ces objets n'existent pas déjà),
- Les objets de type machine correspondant aux serveurs VoIP (si ces objets n'existent pas déjà),
- Un objet de type routeur utilisant les passerelles des opérateurs et permettant de définir les contraintes liées aux flux VoIP.
  Cet objet routeur sera utilisé dans les règles de filtrage pour les flux VoIP.

Dans cette note technique, on suppose que 3 interfaces du firewall sont reliées aux 3 routeurs des opérateurs :

- Une interface est connectée au routeur n°1 du premier opérateur (*Router1*).
  Dans cet exemple, l'adresse IP de cette interface est 10.0.11.1/24.
- Une interface est connectée au routeur n°2 du premier opérateur (*Router2*).
  Dans cet exemple, l'adresse IP de cette interface est 10.0.12.1/24.
- Une interface est connectée au routeur du second opérateur (*Router3*).
  Dans cet exemple, l'adresse IP de cette interface est 10.0.13.1/24.

Créer les objets machine pour les passerelles des opérateurs

Dans le menu **Configuration** > **Objets** > **Objets réseau** :

1. Cliquez sur **Ajouter**.
   La fenêtre de création et d'édition d'objets s'affiche.
2. Dans le menu de gauche, sélectionnez **Machine**.
3. Nommez la machine (premier routeur du premier opérateur : *Router1*).
4. Indiquez son adresse IPv4 (exemple : 10.0.11.2).
5. Cliquez sur **Créer et dupliquer**.
6. Répétez les étapes 3 à 5 pour la passerelle suivante (deuxième routeur du premier opérateur). Les valeurs choisies dans cet exemple sont :

- Nom : *Router2*,
- Adresse IP : 10.0.12.2.

7. Répétez les étapes 3 à 4 pour la dernière passerelle (routeur du second opérateur). Les valeurs choisies dans cet exemple sont :

- Nom : *Router3*,
- Adresse IP : 10.0.13.2.

8. Cliquez sur **Créer.**

Créer les objets machine pour les serveurs VoIP

En suivant la méthode décrite dans la partie Créer les objets machine pour les passerelles des opérateurs, créez les objets correspondant aux serveurs VoIP.

Comme indiqué dans la partie Comprendre les paramètres de supervision, si vous disposez de plusieurs serveurs VoIP, il est recommandé de les rassembler au sein d'un groupe qui sera utilisé comme cible des tests de disponibilité.

Pour créer un groupe avec les serveurs VoIP

Dans le menu **Configuration** > **Objets** > **Objets réseau** :

1. Cliquez sur **Ajouter**.
   La fenêtre de création et d'édition d'objets s'affiche.
2. Dans le menu de gauche, sélectionnez **Groupe**.
3. Nommez ce groupe (exemple : *Remote_VoIP*).
4. Dans la grille de gauche, sélectionnez les serveurs à inclure dans ce groupe (touche [Ctrl] du clavier et sélection des différents objets).
5. Cliquez sur la flèche pour déplacer les serveurs dans le groupe en cours de création.
6. Validez la création de ce groupe en cliquant sur le bouton **Créer**.

Créer l'objet routeur destiné à appliquer les contraintes pour les flux VoIP

Dans le menu **Configuration** > **Objets** > **Objets réseau** :

1. Cliquez sur **Ajouter**.
   La fenêtre de création et d'édition d'objets s'affiche.
2. Dans le menu de gauche, sélectionnez **Routeur**.

Propriétés générales

3. Nommez l'objet (exemple : *SD-WAN_VoIP*).

Supervision

4. Pour la **Méthode de détection**, sélectionnez **ICMP**.
5. Ajustez le **Délai d'expiration (s)** selon vos besoins.
6. Ajustez l'**Intervalle de tests (s)** selon vos besoins.
7. Ajustez le nombre d'**Échecs avant dégradation** (3 par défaut).

SLA SD-WAN (seuils)

8. Cochez la case **SLA SD-WAN (seuils)**.
9. Ajustez la **Latence (ms)** selon vos besoins.
10. Ajustez la **Gigue (ms)** selon vos besoins.
11. Ajustez le **Taux de perte de paquets (%)** selon vos besoins.
12. Ne renseignez pas de **Taux d'indisponibilité (%)**.

Passerelles

13. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
14. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-1.
15. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.
16. Répétez les étapes 15 à 17 pour ajouter l'objet LIL-WAN-2.
17. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
18. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-3.
19. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

Configuration avancée

20. Dans le cadre **Configuration avancée**, sélectionnez l'option de **Répartition de charge** *Aucune Répartition de charge*.
21. Pour l'**Activation des passerelles de secours**, sélectionnez l'option *Lorsque toutes les passerelles sont injoignables*.
22. Cliquez sur **Appliquer** puis **Sauvegarder**.

Créer la règle de PBR pour les flux VoIP

Dans l'onglet **Configuration** > module **Politique de sécurité** > **Filtrage et NAT** :

1. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter la règle pour les flux VoIP.
2. Cliquez sur **Nouvelle règle**.
3. Sélectionnez **Règle simple**.
4. Une nouvelle règle inactive est ajoutée à la politique de filtrage.
   Cette règle est sélectionnée par défaut.
5. Effectuez un double clic sur cette règle.
   La fenêtre de configuration de la règle s'ouvre.
6. Cliquez sur le menu de gauche **Général.**
7. Dans le champ **État**, sélectionnez la valeur *On*.
8. Cliquez sur le menu de gauche **Action**.
9. Dans l'onglet **Général** :

- Pour le champ **Action**, choisissez *passer,*
- Pour le champ **Passerelle - routeur**, sélectionnez l'objet *SD-WAN_VoIP*.

10. Cliquez sur le menu de gauche **Destination**.
11. Dans l'onglet **Général**, pour le champ **Machines destinations**, cliquez sur **Ajouter** et sélectionnez le serveur ou le groupe de serveurs *Remote_VoIP*.
12. Cliquez sur le menu de gauche **Port / Protocole**.
13. Pour le champ **Port destination**, cliquez sur **Ajouter** et sélectionnez *sip_tcp*.
14. Validez la configuration de la règle en cliquant sur **OK** puis sur **Appliquer** pour activer la politique de filtrage modifiée.

Cette règle de filtrage prend donc la forme suivante :

Exemple 2 : tunnels VPN IPsec avec redondance de liens / partage de charge

Cet exemple présente deux cas de gestion de tunnels IPsec au travers d'objets routeurs :

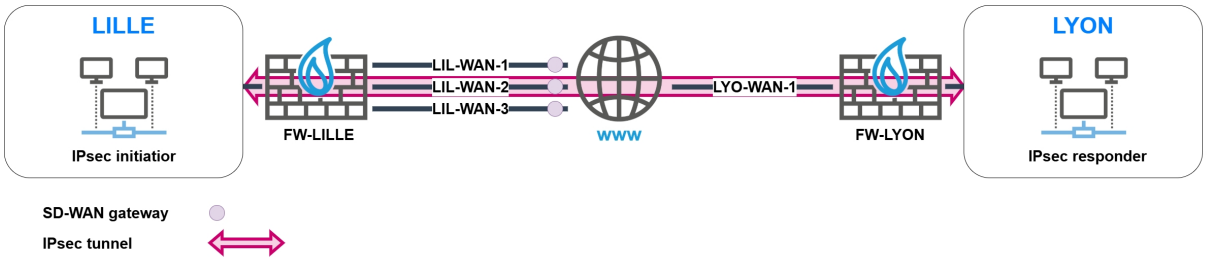
- Tunnels basés sur la politique IPsec (PB - Policy Based),
- Tunnels basés sur des interfaces IPsec virtuelles (VTI).

Tunnels basés sur la politique IPsec (PB - Policy Based)

Architecture réseau

- Le site principal de LILLE comporte trois liens WAN dont deux principaux (LIL-WAN-1 et LIL-WAN-2) et un de secours (LIL-WAN-3),
- Le site secondaire de LYON comporte un lien WAN (LYO-WAN-1).

Architecture IPsec



Les sites de LILLE et de LYON communiquent via un tunnel basé sur la politique IPsec en respectant les configurations décrites ci-dessous.

Site de LILLE

Plusieurs options de routage peuvent être utilisées pour établir le tunnel IPsec avec le site de LYON :

- Une route par défaut avec partage de charge via un objet routeur,
- Une route par défaut avec redondance via un objet routeur,
- Une route statique avec redondance via un objet routeur.

NOTE
Il n'est pas possible d'utiliser du routage par politique (PBR - Policy Based Routing) directement au sein d'une règle de filtrage dans ce type de configuration.

Dans cet exemple, le firewall FW-LILLE utilise un objet routeur en passerelle par défaut avec redondance (*failover*) : en cas de dégradation sur le lien utilisé, le tunnel doit être conservé en basculant sur un autre lien disponible.

Site de LYON

Plusieurs options de routage peuvent être utilisées pour établir le tunnel IPsec avec le site de LILLE :

- Une route par défaut,
- Une route statique.

NOTE
Il n'est pas possible d'utiliser du routage par politique (PBR - Policy Based Routing) directement au sein d'une règle de filtrage dans ce type de configuration.

Pour la partie IPsec :

- Le correspondant IPsec défini sur le firewall FW-LYON doit être de type mobile (solution plus rapide à mettre en œuvre) ou être configuré en mode *Responder-only* car le firewall FW-LYON n'a pas connaissance de l'accès WAN par lequel le site de LILLE se présente pour établir le tunnel,
- La configuration du firewall FW-LYON doit autoriser les trois adresses IP publiques de FW-LILLE à établir un tunnel IPsec site-à-site. Ceci impose de définir les trois clés pré-partagées ou les trois certificats pour les liens WAN du site de LILLE.

Ce document décrit l'utilisation d'un correspondant de type mobile avec authentification par clé pré-partagée.

Configurer le firewall FW-LILLE

Créer les objets correspondant aux LAN des sites de LILLE et LYON

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Réseau**.
4. Précisez le **Nom de l'objet** (LIL-LAN dans cet exemple).
5. Saisissez son **Adresse IP de réseau** sous la forme "réseau/masque de réseau". Le masque de réseau peut être renseigné au format CIDR ou décimal.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet LYO-LAN.
8. Cliquez sur **Créer**.

Créer les 3 objets correspondant aux passerelles / liens WAN de LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.

4. Précisez le **Nom de l'objet** (LIL-WAN-1 dans cet exemple).
5. Saisissez son **Adresse IPv4**.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 à 6 pour créer l'objet LIL-WAN-2.
8. Répétez les étapes 4 et 5 pour créer l'objet LIL-WAN-3.
9. Cliquez sur **Créer**.

Créer l'objet correspondant au firewall FW-LYON

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (FW-LYON dans cet exemple).
5. Saisissez l'**Adresse IPv4** publique du lien WAN du site de LYON.
6. Cliquez sur **Créer.**

Créer l'objet routeur destiné à servir de route par défaut

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Routeur**.

Propriétés générales

4. Nommez l'objet (exemple : DEFAULT-ROUTER-LILLE).

Supervision

Pour obtenir plus d'informations sur les paramètre de supervision et les seuils SLA, veuillez consulter le Manuel Utilisateur SNS

5. Pour la **Méthode de détection**, sélectionnez **ICMP**.
6. Ajustez le **Délai d'expiration (s)** selon vos besoins.
7. Ajustez l'**Intervalle de tests (s)** selon vos besoins.
8. Ajustez le nombre d'**Échecs avant dégradation** (3 par défaut).

SLA SD-WAN (seuils)

9. Cochez la case **SLA SD-WAN (seuils)**.
10. Ajustez la **Latence (ms)** selon vos besoins.
11. Ajustez la **Gigue (ms)** selon vos besoins.
12. Ajustez le **Taux de perte de paquets (%)** selon vos besoins.
13. Ne renseignez pas de **Taux d'indisponibilité (%)**.

Passerelles

14. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
15. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-1.
16. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.
17. Répétez les étapes 14 à 16 pour ajouter l'objet LIL-WAN-2.
18. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
19. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-3.
20. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

Configuration avancée

21. Dans le cadre **Configuration avancée**, sélectionnez l'option de **Répartition de charge** *Aucune Répartition de charge*.
22. Pour l'**Activation des passerelles de secours**, sélectionnez l'option *Lorsque toutes les passerelles sont injoignable*s.
23. Cliquez sur **Appliquer** puis **Sauvegarder**.

Définir cet objet routeur comme passerelle du firewall FW-LILLE

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage**.
2. Dans le champ **Passerelle par défaut**, sélectionnez l'objet routeur précédemment créé (DEFAULT-ROUTER-LILLE dans cet exemple).
3. Cliquez sur **Appliquer** puis **Sauvegarder**.

Définir son correspondant IPsec pour le site de LYON

Ce correspondant est de type passerelle distante.

Dans cet exemple, l'authentification par clé pré-partagée est utilisée.

1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter** puis sur **Nouvelle passerelle distante**.
3. Dans le champ **Passerelle distante**, sélectionnez l'objet correspondant à l'adresse IP publique du firewall FW-LYON (LYO-WAN-1 dans cet exemple).
4. Indiquez un nom pour ce correspondant (FW-LYON dans l'exemple).
5. Sélectionnez la Version **IKEv2**.
6. Choisissez le **Profil IKE** à utiliser.
7. Cliquez sur **Suivant**.
8. Pour le **Type d'authentification**, sélectionnez **Clé pré-partagée (PSK)**.
9. Définissez la **Clé pré-partagée** et confirmez-la.
10. Cliquez sur **Suivant**.
    Un résumé du correspondant est proposé.
11. Cliquez sur **Terminer**.
    Le détail du correspondant est affiché.
12. Vérifier que le champ **Adresse locale** a bien la valeur **Any**.

> **NOTE**
> Pour permettre l'utilisation de l'un des 3 liens WAN de FW-LILLE, le champ **Adresse locale** doit prendre la valeur **Any**.

13. Dans le cadre **Configuration avancée**, positionnez le champ **DPD** sur **Haut**.

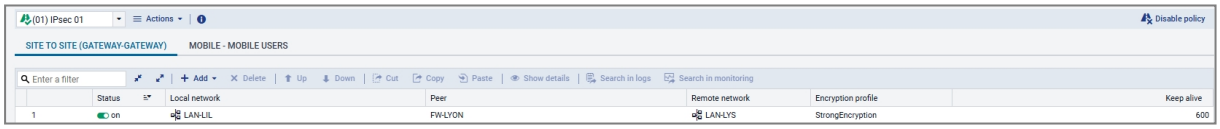
> **NOTE**
> L'option **DPD** (*Dead Peer Detection*) doit être positionnée sur **Haut** afin de provoquer au plus vite la renégociation du tunnel IPsec en cas de perte du lien.

14. Validez les modifications en cliquant sur **Appliquer** puis sur **Sauvegarder**.
15. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Créer la politique IPsec pour établir le tunnel avec le correspondant FW-LYON

1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** > onglet **Site à site (gateway-gateway)**.
2. Cliquez sur **Ajouter** puis sur **Tunnel site à site** simple.
3. Dans le champ **Ressources locales**, sélectionnez l'extrémité de trafic du site de LILLE (objet réseau LIL-LAN dans l'exemple).
   Il peut s'agir d'un groupe de réseaux.
4. Dans le champ **Choix du correspondant**, sélectionnez le correspondant créé pour le firewall de LYON (objet machine FW-LYON dans l'exemple).
5. Dans le champ **Réseaux distants**, sélectionnez l'extrémité de trafic du site de LYON (objet réseau LYO-LAN dans l'exemple).
   Il peut s'agir d'un groupe de réseaux.
6. Cliquez sur **Terminer**.
7. Cliquez dans la colonne **Keepalive** et choisissez une durée dans le menu déroulant (600 ms dans l'exemple).
   Ce paramètre permet de maintenir le tunnel ouvert même lorsque celui-ci n'est pas utilisé.
8. Double-cliquez dans la colonne **État** pour activer cette règle de la politique IPsec.
9. Cliquez sur **Appliquer** puis **Sauvegarder** pour enregistrer les modifications de configuration.
10. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Sur le firewall FW-LILLE, la politique IPsec entre les sites de LILLE et de LYON est donc la suivante :



Créer la règle de filtrage pour autoriser le dialogue entre les sites de LILLE et de LYON

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : sélectionnez l'objet correspondant au réseau local de LYON (LYO-LAN dans cet exemple).
7. Menu de gauche **Destination** : sélectionnez l'objet correspondant au réseau local de LILLE (LIL-LAN dans cet exemple).
8. Menu de gauche **Port / Protocole** : ajoutez à la grille des **Ports destination** les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Répétez les étapes 2 à 10 avec l'objet LIL-LAN en source et l'objet LYO-LAN en destination.
12. Cliquez sur **Appliquer**.

Configurer le firewall FW-LYON

Créer les objets correspondant aux LAN des sites de LILLE et LYON

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Réseau**.
4. Précisez le **Nom de l'objet** (LIL-LAN dans cet exemple).
5. Saisissez son **Adresse IP de réseau** sous la forme "réseau/masque de réseau". Le masque de réseau peut être renseigné au format CIDR ou décimal.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet LYO-LAN.
8. Cliquez sur **Créer**.

Créer l'objet correspondant à la passerelle / lien WAN de LYON

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (LYO-WAN-1 dans cet exemple).
5. Saisissez son **Adresse IPv4**.
6. Cliquez sur **Créer**.

Définir cet objet routeur comme passerelle du firewall FW-LYON

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage**.
2. Dans le champ **Passerelle par défaut**, sélectionnez l'objet machine précédemment créé (LYO-WAN-1 dans cet exemple).
3. Cliquez sur **Appliquer** puis **Sauvegarder**.

Définir le correspondant IPsec pour le site de LILLE

Ce correspondant est de type mobile car le firewall FW-LYON ne peut pas prévoir l'adresse utilisée par le firewall FW-LILLE pour établir le tunnel.

Comme sur le firewall FW-LILLE, l'option **DPD** (*Dead Peer Detection*) doit être positionnée sur **Haut** afin de provoquer immédiatement la renégociation du tunnel IPsec en cas de perte du lien.

1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter** puis sur **Nouveau correspondant mobile**.
3. Indiquez un nom pour ce correspondant (FW-LILLE dans l'exemple).
4. Sélectionnez la Version **IKEv2**.
5. Choisissez le **Profil IKE** à utiliser.
   Il doit être identique à celui utilisé sur le firewall FW-LILLE.
6. Cliquez sur **Suivant**.
7. Pour le **Type d'authentification**, sélectionnez **Clé pré-partagée (PSK)**.
8. Cliquez sur **Suivant**.

9. Cliquez sur **Ajouter** :
   a. Pour l'**Identifiant**, indiquez l'adresse IP publique du premier lien WAN du site de LILLE.
   Saisissez la **Clé pré-partagée** et confirmez-la.
   Elle doit être identique à celle définie sur le firewall FW-LILLE.
   b. Cliquez sur **Appliquer**.
   c. Répétez les étapes A à C afin de définir les clés pré-partagées utilisées pour les deux autres liens WAN du site de LILLE.
   Elles doivent être identiques à celle définie sur le firewall FW-LILLE.
10. Cliquez sur **Suivant**.
    Un résumé du correspondant est proposé.
11. Cliquez sur **Terminer**.
    Le détail du correspondant est affiché.
12. Vérifier que le champ **Adresse locale** a bien la valeur **Any**.
13. Dans le cadre **Configuration avancée**, positionnez le champ **DPD** sur **Haut**.

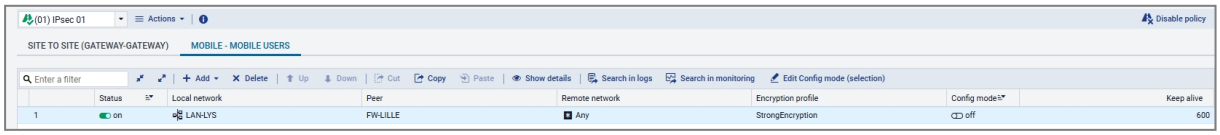
> **NOTE**
> Le correspondant étant de type mobile, il est automatiquement positionné en mode *Responder-only*.

14. Cliquez sur **Appliquer** puis sur **Sauvegarder**.
15. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Créer la politique IPsec pour établir le tunnel avec le correspondant FW-LILLE

1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** > onglet **Mobile - Utilisateurs nomades**.
2. Cliquez sur **Ajouter** puis sur **Nouvelle politique mobile** simple.
3. Dans le champ **Ressources locales**, sélectionnez l'extrémité de trafic du site de LYON (objet réseau LYO-LAN dans l'exemple).
   Il peut s'agir d'un groupe de réseaux.
4. Dans le champ Choix du correspondant, sélectionnez le correspondant créé pour le firewall de LILLE (objet machine FW-LILLE dans l'exemple).
5. Cliquez sur **Terminer**.
6. Cliquez dans la colonne **Keepalive** et choisissez une durée dans le menu déroulant (600 ms dans l'exemple).
   Ce paramètre permet de maintenir le tunnel ouvert même lorsque celui-ci n'est pas utilisé.
7. Double-cliquez dans la colonne **État** pour activer cette règle de la politique IPsec.
8. Cliquez sur **Appliquer** puis **Sauvegarder**.
9. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Sur le firewall FW-LYON, la politique IPsec entre les sites de LYON et de LILLE est donc la suivante :



Créer la règle de filtrage pour autoriser le dialogue entre les sites de LYON et de LILLE

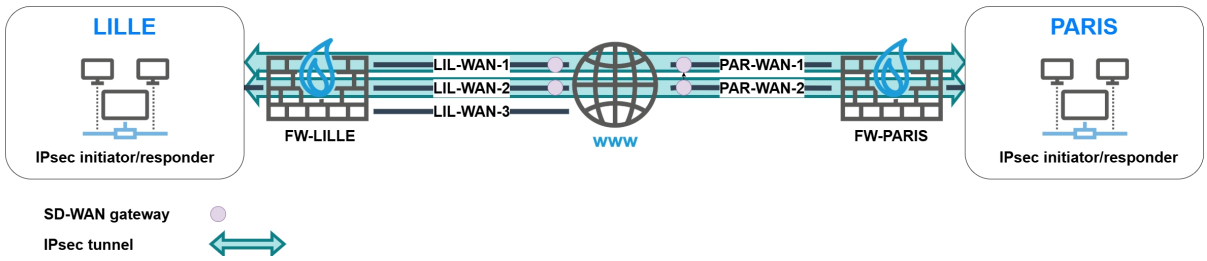
1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Faites un double clic dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passer l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : sélectionnez l'objet correspondant au réseau local de LILLE (LIL-LAN dans cet exemple).
7. Menu de gauche **Destination** : sélectionnez l'objet correspondant au réseau local de LYON (LYO-LAN dans cet exemple).
8. Menu de gauche **Port** / **Protocole** : ajoutez à la grille des **Ports destination** les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Répétez les étapes 2 à 10 avec l'objet LYO-LAN en source et l'objet LIL-LAN en destination.
12. Cliquez sur **Appliquer**.

Tunnels IPsec basés sur des interfaces IPsec virtuelles (VTI)

Architecture réseau

- Le site principal de LILLE comporte trois liens WAN (LIL-WAN-1, LIL-WAN-2 et LIL-WAN-3),
- Le site secondaire de PARIS comporte deux liens WAN principaux (PAR-WAN-1 et PAR-WAN-2).

Architecture IPsec



- Les sites de LILLE et de PARIS communiquent via deux tunnels IPSec basés sur des interfaces IPsec virtuelles (VTI).
- L'un des deux sites peut être configuré en *responder only*.

Site de LILLE

Le firewall FW-LILLE utilise deux routes statiques pour établir des tunnels IPsec avec le site de PARIS au travers des couples d'accès WAN LIL-WAN-1 / PAR-WAN-1 et LIL-WAN-2 / PAR-WAN-2. Ces tunnels sont basés sur des interfaces IPsec virtuelles.

Cette configuration impose la communication exclusive de LIL-WAN-1 avec PAR-WAN-1 et de LIL-WAN-2 avec PAR-WAN-2.

NOTE
Le site de PARIS possédant un accès WAN de moins que le site de LILLE, l'accès LIL-WAN-3 ne sera pas utilisé pour l'établissement des tunnels IPsec avec le site de PARIS.

Il convient de définir une route pour établir les tunnels avec le site de PARIS : ceci sera fait à l'aide d'un objet routeur utilisant les deux interfaces IPsec virtuelles du site de PARIS.

Ce routage peut être réalisé :

- Via du routage par politique (PBR - Policy Based Routing). Cette option autorise le partage de charge ou la redondance entre les deux passerelles de l'objet routeur,
- Via du routage statique. Cette option **impose** de définir de la redondance (*failover*) entre les deux passerelles de l'objet routeur. Le partage de charge ne peut pas être utilisé dans ce cas.

NOTE
Si le site de PARIS ne possédait qu'un seul lien WAN, cette configuration pourrait tout de même être déployée moyennant l'utilisation d'un alias ou d'une seconde adresse IP publique pour définir PAR-WAN-1.

Site de PARIS

La configuration du site de PARIS est le miroir de celle du site de LILLE.

Configurer le firewall FW-LILLE

Créer les objets correspondant aux LAN des sites de PARIS et LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Réseau**.
4. Précisez le **Nom de l'objet** (LIL-LAN dans cet exemple).
5. Saisissez son **Adresse IP de réseau** sous la forme "réseau/masque de réseau". Le masque de réseau peut être renseigné au format CIDR ou décimal.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet PAR-LAN.
8. Cliquez sur **Créer**.

Créer les objets correspondant aux passerelles / liens WAN du site de LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.

4. Précisez le **Nom de l'objet** (LIL-WAN-1 dans cet exemple).
5. Saisissez son **Adresse IPv4**.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet LIL-WAN-2.
8. Cliquez sur **Créer**.

Créer les objets correspondant aux passerelles / liens WAN du site de PARIS

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (PAR-WAN-1 dans cet exemple).
5. Saisissez l'**Adresse IPv4** publique du lien WAN-1 du site de PARIS.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet PAR-WAN-2 avec l'adresse IPv4 publique du lien WAN-2 du site de PARIS.
8. Cliquez sur **Créer.**

Créer les interfaces IPsec virtuelles du site de LILLE

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Interfaces virtuelles.**
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de l'interface à **Activée**.
4. Indiquez le **Nom** de l'interface IPsec virtuelle (LIL-VTI-1 dans cet exemple).
5. Indiquez l'**Adresse IPv4** et le **masque réseau** de cette interface (10.255.1.1/255.255.255.252 dans cet exemple).
6. Cliquez sur **Appliquer**.
7. Répétez les étapes 2 à 6 pour créer le deuxième interface IPsec virtuelle (LIL-VTI-2 et 10.255.2.1/255.255.255.252 dans cet exemple).
8. Cliquez sur le bouton **Appliquer**.

Créer les objets correspondant aux interfaces IPsec virtuelles du firewall de PARIS

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (PAR-VTI-1 dans cet exemple).
5. Saisissez l'**Adresse IPv4** de l'interface IPsec virtuelle (10.255.1.2/255.255.255.252 dans cet exemple).
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet PAR-VTI-2 dont l'adresse IP est 10.255.2.2/255.255.255.252 dans cet exemple.
8. Cliquez sur **Créer.**

Créer les routes de retour pour les interfaces IPsec virtuelles de FW-LILLE

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routes de retour IPv4**.
2. Cliquez sur **Ajouter**.

3. Passez l'**État** de la route de retour à **Activée**.
4. Indiquez la **Passerelle** distante de cette route de retour (PAR-VTI-1 dans cet exemple).
5. Indiquez l'**Interface** IPsec virtuelle locale à utiliser pour cette route de retour (LIL-VTI-1 dans cet exemple).
6. Répétez les étapes 2 à 5 avec les éléments suivants :
   - **Passerelle** : PAR-VTI-2,
   - **Interface** : LIL-VTI-2.
7. Cliquez sur le bouton **Appliquer**.

Créer les routes statiques nécessaires à l'établissement des tunnels IPsec

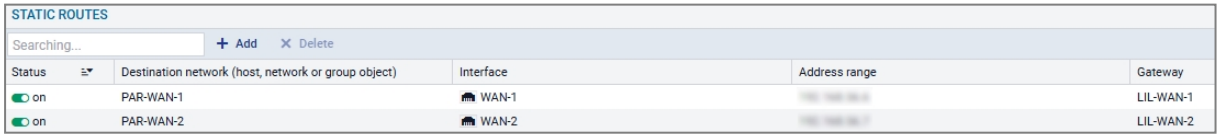
Il s'agit de définir une route statique vers chaque interface physique distante de telle sorte que :

- Le premier tunnel s'établisse entre les liens LIL-WAN-1 et PAR-WAN-1,
- Le second tunnel s'établisse entre les liens LIL-WAN-2 et PAR-WAN-2.

Pour ce faire :

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routage statique**.
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de la route à **On**.
4. Pour le **Réseau de destination**, sélectionnez l'objet correspondant à l'accès WAN 1 du site de PARIS (PAR-WAN-1 dans cet exemple).
5. Pour l'**Interface** locale devant être utilisée pour cette route, sélectionnez l'interface correspondant à l'accès WAN 1 de LILLE (WAN-1 dans cet exemple).
6. Pour la passerelle devant être utilisée pour cette route, sélectionnez l'objet LIL-WAN-1.
7. Répétez les étapes 2 à 6 avec les éléments suivants :
   - **Réseau de destination** : PAR-WAN-2,
   - **Interface** : WAN-2,
   - **Passerelle** : LIL-WAN-2.
8. Cliquez sur le bouton **Appliquer**.

Ces routes statiques prennent la forme suivante :



Créer l'objet routeur à utiliser dans la route vers le LAN du site de PARIS

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Routeur**.

Propriétés générales

4. Nommez l'objet (exemple : ROUTER-LILLE-VTI-FAILOVER ou ROUTER-LILLE-VTI-LB selon l'option de routage retenue).

Supervision

5. Pour la **Méthode de détection**, sélectionnez **ICMP**.
6. Ajustez le **Délai d'expiration (s)** selon vos besoins.
7. Ajustez l'**Intervalle de tests (s)** selon vos besoins.
8. Ajustez le nombre d'**Échecs avant dégradation** (3 par défaut).

SLA SD-WAN (seuils)

9. Cochez la case **SLA SD-WAN (seuils)**.
10. Ajustez la **Latence (ms)** selon vos besoins.
11. Ajustez la **Gigue (ms)** selon vos besoins.
12. Ajustez le **Taux de perte de paquets (%)** selon vos besoins.
13. Ne renseignez pas de **Taux d'indisponibilité (%)**.

Passerelles

14. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
15. Dans la colonne **Passerelle**, sélectionnez l'objet PAR-VTI-1.
16. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.
17. Si vous sélectionnez l'option de partage de charge : répétez les étapes 14 à 16 pour ajouter l'objet PAR-VTI-2.
18. Si vous sélectionnez l'option de redondance :
    a. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
    b. Dans la colonne **Passerelle**, sélectionnez l'objet PAR-VTI-2.
    c. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

Configuration avancée

19. Dans le cadre **Configuration avancée**, pour la valeur du champ **Répartition de charge** :
    a. Selon votre besoin, sélectionnez **Par connexion** ou **Par adresse IP source** si vous avez choisi l'option de partage de charge.
    b. Sélectionnez **Aucune Répartition** si vous avez choisi l'option de redondance.
20. Pour l'**Activation des passerelles de secours**, sélectionnez l'option **Lorsque toutes les passerelles sont injoignables**.

> **IMPORTANT**
> Pour le champ **Si aucune passerelle n'est disponible**, sélectionnez **Ne pas router** quel que soit votre choix de routage.
> Ceci évite que des flux non chiffrés ne soient envoyés vers des réseaux non protégés tels qu'Internet si aucune passerelle n'est disponible.

21. Cliquez sur **Appliquer** puis **Sauvegarder**.

Utiliser cet objet dans le routage pour joindre le LAN du site de PARIS

Cas du routage statique avec redondance

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routage statique**.
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de la route de retour à **Activée**.
4. Pour le **Réseau de destination**, sélectionnez l'objet correspondant au LAN du site de PARIS (PAR-LAN dans cet exemple).
5. Ne sélectionnez pas d'**Interface**.

6. Pour la passerelle devant être utilisée pour cette route, sélectionnez l'objet routeur défini avec de la redondance (ROUTER-LILLE-VTI-FAILOVER dans cet exemple).
7. Cliquez sur le bouton **Appliquer**.

Cette route prend la forme suivante :

Cas du routage par politique avec partage de charge

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Faites un double clic dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passer l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** :
   a. Cadre **Général** : positionnez l'**Action** à **passer**.
   b. Cadre **Routage** : sélectionnez l'objet routeur défini précédemment (ROUTER-LILLE-VTI-LB dans cet exemple).
6. Menu de gauche **Source** : faites un double-clic sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local du site de LILLE (LIL-LAN dans cet exemple).
7. Menu de gauche **Destination** : faites un double-clic sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local du site de PARIS (PAR-LAN dans cet exemple).
8. Menu de gauche **Port** / **Protocole** : ajoutez à la grille des Ports destination les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Cliquez sur **Appliquer**.

Cette règle de filtrage prend la forme suivante :

Définir les correspondants IPsec du site de PARIS

Ces correspondants sont de type passerelle distante.

Dans cet exemple, l'authentification par clé pré-partagée est utilisée.

Pour permettre l'utilisation de l'un des deux liens WAN de FW-LILLE lors de l'initialisation du tunnel, le champ **Adresse locale** doit prendre la valeur **Any**. De même, l'option **DPD** (*Dead Peer Detection*) doit être positionnée sur **Haut** afin de provoquer au plus vite la renégociation du tunnel IPsec en cas de perte du lien.

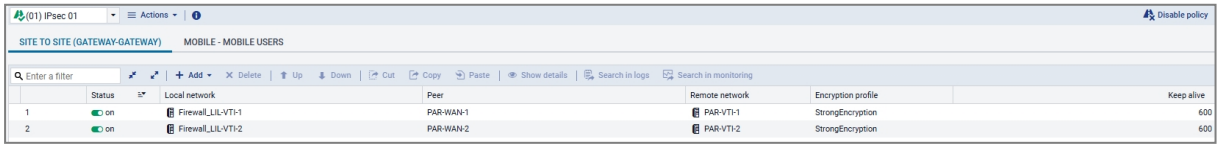
1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter** puis sur **Nouvelle passerelle distante**.
3. Dans le champ **Passerelle distante**, sélectionnez l'objet correspondant à la première adresse IP publique du firewall FW-PARIS (PAR-WAN-1 dans cet exemple).
4. Indiquez un nom pour ce correspondant (PAR-WAN-1 dans l'exemple).
5. Sélectionnez la Version **IKEv2**.

6. Choisissez le **Profil IKE** à utiliser.
7. Cliquez sur **Suivant**.
8. Pour le **Type d'authentification**, sélectionnez **Clé pré-partagée (PSK)**.
9. Définissez la **Clé pré-partagée** et confirmez-la.
10. Cliquez sur **Suivant**.
    Un résumé du correspondant est proposé.
11. Cliquez sur **Terminer**.
    Le détail du correspondant est affiché.
12. Vérifier que le champ **Adresse locale** a bien la valeur **Any**.
13. Dans le cadre **Configuration avancée**, positionnez le champ **DPD** sur **Haut**.
14. Validez les modifications en cliquant sur **Appliquer** puis sur **Sauvegarder**.
15. Répétez les étapes 2 à 14 pour créer le correspondant basé sur la deuxième adresse IP publique du firewall FW-PARIS (PAR-WAN-2 dans cet exemple).
16. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Créer la politique IPsec pour établir les tunnels avec le site de PARIS

1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** > onglet **Site à site (gateway-gateway)**.
2. Cliquez sur **Ajouter** puis sur **Tunnel site à site** simple.
3. Dans le champ **Ressources locales**, sélectionnez l'extrémité de trafic du site de LILLE : il s'agit de la première interface IPsec virtuelle de FW-LILLE (objet réseau Firewall_LIL-VTI-1 dans l'exemple).
4. Dans le champ **Choix du correspondant**, sélectionnez le premier correspondant créé pour le firewall de PARIS (objet machine PAR-WAN-1 dans l'exemple).
5. Dans le champ **Réseaux distants**, sélectionnez l'extrémité de trafic du site de PARIS : il s'agit de la première interface IPsec virtuelle de FW-PARIS (objet réseau PAR-VTI-1 dans l'exemple).
6. Cliquez sur **Terminer**.
7. Cliquez dans la colonne **Keepalive** et choisissez une durée dans le menu déroulant (600 ms dans l'exemple).
   Ce paramètre permet de maintenir le tunnel ouvert même lorsque celui-ci n'est pas utilisé.
8. Double-cliquez dans la colonne **État** pour activer cette règle de la politique IPsec.
9. Répétez les étapes 2 à 8 pour créer le tunnel entre LIL-VTI-2 et PAR-VTI-2.
10. Cliquez sur **Appliquer** puis **Sauvegarder** pour enregistrer les modifications de configuration.
11. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Sur le firewall FW-LILLE, la politique IPsec entre les sites de LILLE et de PARIS est donc la suivante :



Créer la règle de filtrage pour autoriser la supervision des interfaces VTI du site de PARIS

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Faites un double clic dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passer l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : laissez l'objet **Any** proposé par défaut.
7. Menu de gauche **Destination** : faites un double-clic sur l'objet **Any** et remplacez-le par les objets correspondant aux interfaces VTI du site de PARIS (PAR-VTI-1 et PAR-VTI-2 dans cet exemple).
8. Menu de gauche **Port / Protocole** : pour le champ **Protocole IP** du cadre **Protocole**, sélectionnez l'objet **icmp**.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Cliquez sur **Appliquer**.

Créer la règle de filtrage pour autoriser le dialogue entre les sites de LILLE et de PARIS

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Faites un double clic dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passer l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : faites un double-clic sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local de PARIS (PAR-LAN dans cet exemple).
7. Menu de gauche **Destination** : faites un double-clic sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local de LILLE (LIL-LAN dans cet exemple).
8. Menu de gauche **Port / Protocole** : ajoutez à la grille des **Ports destination** les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Répétez les étapes 2 à 10 avec l'objet LIL-LAN en source et l'objet PAR-LAN en destination.

> **NOTE**
> Cette seconde règle n'a pas besoin d'être créée si vous avez utilisé le routage par politique pour joindre le LAN de PARIS.

12. Cliquez sur **Appliquer**.

Configurer le firewall FW-PARIS

Créer les objets correspondant aux LAN des sites de PARIS et LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Réseau**.
4. Précisez le **Nom de l'objet** (LIL-LAN dans cet exemple).
5. Saisissez son **Adresse IP de réseau** sous la forme "réseau/masque de réseau". Le masque de réseau peut être renseigné au format CIDR ou décimal.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet PAR-LAN.
8. Cliquez sur **Créer**.

Créer les objets correspondant aux passerelles / liens WAN du site de PARIS

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (PAR-WAN-1 dans cet exemple).
5. Saisissez son **Adresse IPv4**.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 et 5 pour créer l'objet PAR-WAN-2.
8. Cliquez sur **Créer**.

Créer les objets correspondant aux passerelles / liens WAN du site de LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (LIL-WAN-1 dans cet exemple).
5. Saisissez l'**Adresse IPv4** publique du lien WAN-1 du site de LILLE.
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 à 5 pour créer l'objet LIL-WAN-2 avec l'adresse IPv4 publique du lien WAN-2 du site de LILLE.
8. Cliquez sur **Créer.**

Créer les objets correspondant aux interfaces IPsec virtuelles du firewall de LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Machine**.
4. Précisez le **Nom de l'objet** (LIL-VTI-1 dans cet exemple).
5. Saisissez l'**Adresse IPv4** de l'interface IPsec virtuelle (10.255.1.1/255.255.255.252).
6. Cliquez sur **Créer et dupliquer.**
7. Répétez les étapes 4 à 5 pour créer l'objet LIL-VTI-2 dont l'adresse IP est 10.255.2.1/255.255.255.252 dans cet exemple.
8. Cliquez sur **Créer**.

Créer les interfaces IPsec virtuelles du site de PARIS

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Interfaces virtuelles.**
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de l'interface à **Activée**.
4. Indiquez le **Nom** de l'interface IPsec virtuelle (PAR-VTI-1 dans cet exemple).
5. Indiquez l'**Adresse IPv4** et le **masque réseau** de cette interface (10.255.1.2/255.255.255.252 dans cet exemple).
6. Cliquez sur **Appliquer**.
7. Répétez les étapes 2 à 6 pour créer le deuxième interface IPsec virtuelle (PAR-VTI-2 et 10.255.2.2/255.255.255.252 dans cet exemple).
8. Cliquez sur le bouton **Appliquer** situé au bas du module pour enregistrer cette configuration.

Créer les routes de retour pour les interfaces IPsec virtuelles de FW-PARIS

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routes de retour IPv4**.
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de la route de retour à **On**.
4. Indiquez la **Passerelle** distante de cette route de retour (LIL-VTI-1 dans cet exemple).
5. Indiquez l'**Interface** IPsec virtuelle locale à utiliser pour cette route de retour (PAR-VTI-1 dans cet exemple).
6. Répétez les étapes 2 à 5 avec les éléments suivants :
   - **Passerelle** : LIL-VTI-2,
   - **Interface** : PAR-VTI-2.
7. Cliquez sur le bouton **Appliquer** situé au bas du module pour enregistrer cette configuration.

Créer les routes statiques nécessaires à l'établissement des tunnels IPsec

Il s'agit de définir une route statique vers chaque interface physique distante de telle sorte que :

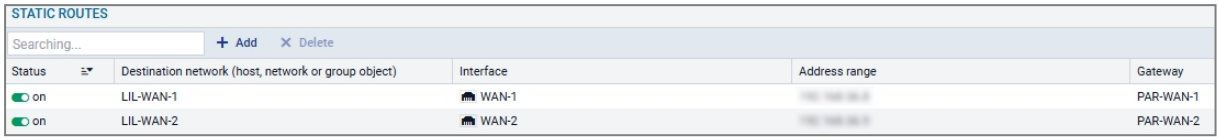
- Le premier tunnel s'établisse entre les liens LIL-WAN-1 et PAR-WAN-1,
- Le second tunnel s'établisse entre les liens LIL-WAN-2 et PAR-WAN-2.

Pour ce faire :

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routage statique**.
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de la route à **On**.
4. Pour le **Réseau de destination**, sélectionnez l'objet correspondant à l'accès WAN 1 du site de LILLE (LIL-WAN-1 dans cet exemple).
5. Pour l'**Interface** locale devant être utilisée pour cette route, sélectionnez l'interface correspondant à l'accès WAN 1 de PARIS (WAN-1 dans cet exemple).
6. Pour la passerelle devant être utilisée pour cette route, sélectionnez l'objet PAR-WAN-1.
7. Répétez les étapes 2 à 6 avec les éléments suivants :
   - **Réseau de destination** : LIL-WAN-2,
   - **Interface** : WAN-2,
   - **Passerelle** : PAR-WAN-2.

8. Cliquez sur le bouton **Appliquer** situé au bas du module pour enregistrer cette configuration.

Ces routes statiques prennent la forme suivante :



Créer l'objet routeur à utiliser dans la route vers le LAN du site de LILLE

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Routeur**.

Propriétés générales

4. Nommez l'objet (exemple : ROUTER-PARIS-VTI-FAILOVER ou ROUTER-PARIS-VTI-LB selon l'option de routage retenue).

Supervision

5. Pour la **Méthode de détection**, sélectionnez **ICMP**.
6. Ajustez le **Délai d'expiration (s)** selon vos besoins.
7. Ajustez l'**Intervalle de tests (s)** selon vos besoins.
8. Ajustez le nombre d'**Échecs avant dégradation** (3 par défaut).

SLA SD-WAN (seuils)

9. Cochez la case **SLA SD-WAN (seuils)**.
10. Ajustez la **Latence (ms)** selon vos besoins.
11. Ajustez la **Gigue (ms)** selon vos besoins.
12. Ajustez le **Taux de perte de paquets (%)** selon vos besoins.
13. Ne renseignez pas de **Taux d'indisponibilité (%)**.

Passerelles

14. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
15. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-VTI-1.
16. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.
17. Si vous sélectionnez l'option de partage de charge : répétez les étapes 14 à 16 pour ajouter l'objet LIL-VTI-2.
18. Si vous sélectionnez l'option de redondance :
    a. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
    b. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-VTI-2.
    c. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

Configuration avancée

19. Dans le cadre **Configuration avancée**, pour la valeur du champ **Répartition de charge** :
    a. Selon votre besoin, sélectionnez **Par connexion** ou **Par adresse IP source** si vous avez choisi l'option de partage de charge.
    b. Sélectionnez **Aucune Répartition** si vous avez choisi l'option de redondance.
20. Pour l'**Activation des passerelles de secours**, sélectionnez l'option **Lorsque toutes les passerelles sont injoignables**.

> **IMPORTANT**
> Pour le champ **Si aucune passerelle n'est disponible**, sélectionnez **Ne pas router** quel que soit votre choix de routage.
> Ceci évite que des flux non chiffrés ne soient envoyés vers des réseaux non protégés tels qu'Internet si aucune passerelle n'est disponible.

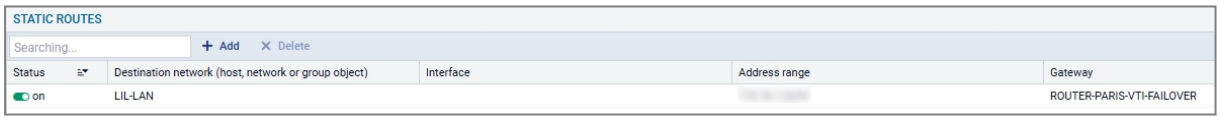
21. Cliquez sur **Appliquer** puis **Sauvegarder**.

Utiliser cet objet dans le routage pour joindre le LAN du site de LILLE

Cas du routage statique avec redondance

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routage statique**.
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de la route de retour à **Activée**.
4. Pour le **Réseau de destination**, sélectionnez l'objet correspondant au LAN du site de LILLE (LIL-LAN dans cet exemple).
5. Ne sélectionnez pas d'**Interface**.
6. Pour la passerelle devant être utilisée pour cette route, sélectionnez l'objet routeur défini avec de la redondance (ROUTER-PARIS-VTI-FAILOVER dans cet exemple).
7. Cliquez sur le bouton **Appliquer** situé au bas du module pour enregistrer cette configuration.

Cette route prend la forme suivante :



Cas du routage par politique avec partage de charge

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** :
   - Cadre **Général** : positionnez l'**Action** à **passer**.
   - Cadre **Routage** : sélectionnez l'objet routeur défini précédemment (ROUTER-PARIS-VTI-LB dans cet exemple).
6. Menu de gauche **Source** : faites un double-clic sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local du site de PARIS (PAR-LAN dans cet exemple).
7. Menu de gauche **Destination** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local du site de LILLE (LIL-LAN dans cet exemple).
8. Menu de gauche **Port / Protocole** : ajoutez à la grille des Ports destination les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Cliquez sur **Appliquer**.

Cette règle de filtrage prend la forme suivante :

Définir les correspondants IPsec du site de LILLE

Ce correspondant est de type passerelle distante.

Dans cet exemple, l'authentification par clé pré-partagée est utilisée.

Pour permettre l'utilisation de l'un des deux liens WAN de FW-PARIS lors de l'initialisation du tunnel, le champ **Adresse locale** doit prendre la valeur **Any**. De même, l'option **DPD** (*Dead Peer Detection*) doit être positionnée sur **Haut** afin de provoquer au plus vite la renégociation du tunnel IPsec en cas de perte du lien.

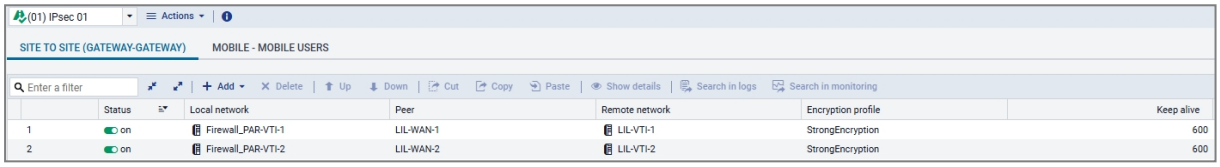
1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter** puis sur **Nouvelle passerelle distante**.
3. Dans le champ **Passerelle distante**, sélectionnez l'objet correspondant à la première adresse IP publique du firewall FW-LILLE (LIL-WAN-1 dans cet exemple).
4. Indiquez un nom pour ce correspondant (LIL-WAN-1 dans l'exemple).
5. Sélectionnez la Version **IKEv2**.
6. Choisissez le **Profil IKE** à utiliser.
7. Cliquez sur **Suivant**.
8. Pour le **Type d'authentification**, sélectionnez **Clé pré-partagée (PSK)**.
9. Définissez la **Clé pré-partagée** et confirmez-la.
10. Cliquez sur **Suivant**.
    Un résumé du correspondant est proposé.
11. Cliquez sur **Terminer**.
    Le détail du correspondant est affiché.
12. Vérifier que le champ **Adresse locale** a bien la valeur **Any**.
13. Dans le cadre **Configuration avancée**, positionnez le champ **DPD** sur **Haut**.
14. Cliquez sur **Appliquer** puis sur **Sauvegarder**.
15. Répétez les étapes 2 à 14 pour créer le correspondant basé sur la deuxième adresse IP publique du firewall FW-LILLE (LIL-WAN-2 dans cet exemple).
16. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Créer la politique IPsec pour établir les tunnels avec le site de LILLE

1. Placez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** > onglet **Site à site (gateway-gateway)**.
2. Cliquez sur **Ajouter** puis sur **Tunnel site à site** simple.
3. Dans le champ **Ressources locales**, sélectionnez l'extrémité de trafic du site de PARIS : il s'agit de la première interface IPsec virtuelle de FW-PARIS (objet réseau Firewall_PAR-VTI-1 dans l'exemple).
4. Dans le champ **Choix du correspondant**, sélectionnez le premier correspondant créé pour le firewall de PARIS (objet machine LIL-WAN-1 dans l'exemple).
5. Dans le champ **Réseaux distants**, sélectionnez l'extrémité de trafic du site de PARIS : il s'agit de la première interface IPsec virtuelle de FW-PARIS (objet réseau LIL-VTI-1 dans l'exemple).
6. Cliquez sur **Terminer**.

7. Cliquez dans la colonne **Keepalive** et choisissez une durée dans le menu déroulant (600 ms dans l'exemple).
   Ce paramètre permet de maintenir le tunnel ouvert même lorsque celui-ci n'est pas utilisé.
8. Double-cliquez dans la colonne **État** pour activer cette règle de la politique IPsec.
9. Répétez les étapes 2 à 8 pour créer le tunnel entre LIL-VTI-2 et PAR-VTI-2.
10. Cliquez sur **Appliquer** puis sur **Sauvegarder**.
11. Vous pouvez appliquer immédiatement les modifications en cliquant sur **Oui, activer la politique**.

Sur le firewall FW-PARIS, la politique IPsec entre les sites de LILLE et de PARIS est donc la suivante :



Créer la règle de filtrage pour autoriser la supervision des interfaces VTI du site de LILLE

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : laissez l'objet **Any** proposé par défaut.
7. Menu de gauche **Destination** : sélectionnez les objets correspondant aux interfaces VTI du site de PARIS (LIL-VTI-1 et LIL-VTI-2 dans cet exemple).
8. Menu de gauche **Port / Protocole** : pour le champ **Protocole IP** du cadre **Protocole**, sélectionnez l'objet **icmp**.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Cliquez sur **Appliquer**.

Créer la règle de filtrage pour autoriser le dialogue entre les sites de LILLE et de PARIS

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passer l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local de LILLE (LIL-LAN dans cet exemple).
7. Menu de gauche **Destination** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local de PARIS (PAR-LAN dans cet exemple).
8. Menu de gauche **Port / Protocole** : ajoutez à la grille des **Ports destination** les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.

9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Répétez les étapes 2 à 10 avec l'objet PAR-LAN en source et l'objet LIL-LAN en destination.

> **NOTE**
> Cette seconde règle n'a pas besoin d'être créée si vous avez utilisé le routage par politique pour joindre le LAN de LILLE.

12. Cliquez sur **Appliquer**.

Tunnels IPsec basés sur des interfaces IPsec virtuelles (VTI) en mode Hub & Spoke

Cet exemple est une variante du cas des tunnels basés sur des interfaces IPsec virtuelles (VTI) entre les sites de LILLE et PARIS. En plus des échanges chiffrés entre les sites de LILLE et PARIS, le site de PARIS utilise les tunnels IPsec pour accéder à Internet via l'un des trois accès WAN de LILLE.

L'architecture est identique à celle du cas des tunnels basés sur des interfaces IPsec virtuelles (VTI) entre les sites de LILLE et PARIS et n'est donc pas détaillée dans cette section.

Seuls les impératifs liés au type d'objet routeur à utiliser pour le routage sur chacun des deux sites, ainsi que les règles de NAT à créer sur le site de LILLE sont décrits dans cette section.

Site de LILLE

Dans le cas du mode Hub & Spoke, le routage sur le site de LILLE peut être réalisé :

- Via une route par défaut au travers d'un objet routeur utilisant de la redondance (*failover*) entre ses deux passerelles,
- Via du routage par politique (PBR - Policy Based Routing) au travers d'un objet routeur utilisant de la redondance entre ses deux passerelles,
- Via du routage statique au travers d'un objet routeur utilisant de la redondance entre ses deux passerelles.

Le partage de charge dans l'objet routeur ne peut pas être utilisé dans ce cas : il n'est pas compatible avec des interfaces sources non protégées, ce qui est le cas par défaut des interfaces IPsec virtuelles.

Site de PARIS

Dans le cas du mode Hub & Spoke, le routage sur le site de PARIS peut être réalisé :

- Via une route par défaut au travers d'un objet routeur utilisant de la redondance (*failover*) entre ses deux passerelles,
- Via du routage statique au travers d'un objet routeur utilisant de la redondance entre ses deux passerelles.
- Via du routage par politique (PBR - Policy Based Routing) au travers d'un objet routeur utilisant de la redondance entre ses deux passerelles,

- Via du routage par politique au travers d'un objet routeur utilisant de la répartition de charge, à la condition que les interfaces IPsec virtuelles de PARIS soient déclarées non protégées, ce qui est la configuration par défaut. En effet, mettre en place du partage de charge avec des passerelles basées sur des interfaces protégées entraînerait la levée d'alarmes bloquantes d'usurpation d'identité sur le firewall de LILLE.

Configurer le firewall FW-LILLE

Suivez toutes les étapes de configuration du firewall de LILLE décrites dans la section Configurer le firewall FW-LILLE de l'exemple traitant des tunnels IPsec basés sur des interfaces IPsec virtuelles (VTI).

Comme indiqué en tête de la présente section, l'option de redondance est impérative lors de la création de l'objet routeur utilisé dans la route vers le LAN du site de PARIS.

Les paragraphes suivants présentent les configurations spécifiques au cas du Hub & Spoke.

Utiliser l'objet routeur dans le routage pour joindre le LAN du site de PARIS

Option de la route par défaut

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage**.
2. Dans le champ **Passerelle par défaut**, sélectionnez l'objet routeur précédemment créé.
3. Cliquez sur **Appliquer** puis **Sauvegarder**.

Option du routage statique

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage** > onglet **Routage statique**.
2. Cliquez sur **Ajouter**.
3. Passez l'**État** de la route de retour à **Activée**.
4. Pour le **Réseau de destination**, sélectionnez l'objet correspondant au LAN du site de PARIS (PAR-LAN dans cet exemple).
5. Ne sélectionnez pas d'**Interface**.
6. Pour la passerelle devant être utilisée pour cette route, sélectionnez l'objet routeur précédemment créé.
7. Cliquez sur **Appliquer**.

Option du routage par politique (PBR - Policy Based Routing)

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** :
   a. Cadre **Général** : positionnez l'**Action** à **passer**.
   b. Cadre **Routage** : sélectionnez l'objet routeur précédemment créé.
6. Menu de gauche **Source** : sélectionnez l'objet correspondant au réseau local du site de LILLE (LIL-LAN dans cet exemple).
7. Menu de gauche **Destination** : sélectionnez l'objet correspondant au réseau local du site de PARIS (PAR-LAN dans cet exemple).
8. Menu de gauche **Port** / **Protocole** : ajoutez à la grille des Ports destination les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.

9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Cliquez sur **Appliquer**.

Créer les règles de translation d'adresses (NAT) pour les flux à destination d'Internet

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **NAT**.

Premier accès WAN de LILLE

2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Source originale**, grille des **Machines sources** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau LAN de PARIS (PAR-LAN dans cet exemple).
6. Menu de gauche **Destination originale** :
   a. Dans l'onglet **Général**, grille des **Machines destinations** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet **Internet**.
   b. Dans l'onglet **Configuration avancée**, champ **Interface de sortie** : sélectionnez l'objet correspondant à la première interface WAN de LILLE (WAN-1 dans l'exemple).
7. Menu de gauche **Source translatée** :
   a. Champ **Machine source translatée** : sélectionnez l'objet correspondant à la première adresse IP publique du firewall (Firewall_WAN-1 dans cet exemple).
   b. Champ **Port source translaté** : sélectionnez l'objet **ephemeral_fw**.
   c. Cochez la case **Choisir aléatoirement le port source translaté**.
8. Menu de gauche **Options** : cochez la case **NAT dans le tunnel IPsec (avant chiffrement, après déchiffrement)**.
9. Cliquez sur **OK**.

Répétez les étapes 2 à 9 pour créer les règles de NAT correspondant aux deux autres accès WAN du site de LILLE avec les objets suivants :

Deuxième accès WAN de LILLE

Champ	Valeur
Source originale - Machines destination	PAR-LAN
Destination originale - Machines destination	Internet
Destination originale - Interface de sortie	WAN-2
Source translatée - Machine source translatée	Firewall_WAN2

Troisième accès WAN de LILLE

Champ	Valeur
Source originale - Machines destination	PAR-LAN

Destination originale - Machines destination	Internet
Destination originale - Interface de sortie	WAN-3
Source translatée - Machine source translatée	Firewall_WAN3

Les règles de translation d'adresses sur le firewall de LILLE prennent donc la forme suivante :

Status	Original traffic (before translation)			Traffic after translation				Protocol	Options
	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port		
on	PAR-LAN	Internet interface: WAN-1	Any	Firewall_WAN-1		Any			NAT inside IPsec tunnel
on	PAR-LAN	Internet interface: WAN-2	Any	Firewall_WAN-2		Any			NAT inside IPsec tunnel
on	PAR-LAN	Internet interface: WAN-3	Any	Firewall_WAN-3		Any			NAT inside IPsec tunnel

Configurer le firewall FW-PARIS

Suivez toutes les étapes de configuration du firewall de PARIS décrites dans la section Configurer le firewall FW-PARIS de l'exemple traitant des tunnels IPsec basés sur des interfaces IPsec virtuelles (VTI).

Comme indiqué en tête de la présente section, l'option de redondance est impérative lors de la création de l'objet routeur utilisé dans la route vers le LAN du site de PARIS.

Les paragraphes suivants présentent les configurations spécifiques au cas du Hub & Spoke.

Cet exemple présente l'option du routage par politique sur le site de PARIS.

Utiliser l'objet routeur dans le routage pour accéder à Internet

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** :
   a. Cadre **Général** : positionnez l'**Action** à **passer**.
   b. Cadre **Routage** : sélectionnez l'objet routeur précédemment créé.
6. Menu de gauche **Source** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet correspondant au réseau local du site de PARIS (PAR-LAN dans cet exemple).
7. Menu de gauche **Destination** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet **Internet**.
8. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
9. Cliquez sur **OK**.
10. Cliquez sur **Appliquer**.

La règle de routage par politique prend la forme suivante :

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass Route: ROUTER-PARIS-VTI-FAILOVER	PAR-LAN	Internet	Any		IPS

Exemple 3 : règles de NAT avec redondance entre les trois liens sortants du site de LILLE

Cet exemple présente un cas de redondance entre les trois liens WAN d'accès à Internet du site de LILLE au travers d'un objet routeur.

Créer l'objet routeur destiné à servir de route par défaut

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Routeur**.

Propriétés générales

4. Nommez l'objet (exemple : ROUTER-LILLE-WAN-FAILOVER).

Supervision

5. Pour la **Méthode de détection**, sélectionnez **ICMP**.
6. Ajustez le **Délai d'expiration (s)** selon vos besoins.
7. Ajustez l'**Intervalle de tests (s)** selon vos besoins.
8. Ajustez le nombre d'**Échecs avant dégradation** (3 par défaut).

SLA SD-WAN (seuils)

9. Cochez la case **SLA SD-WAN (seuils)**.
10. Ajustez la **Latence (ms)** selon vos besoins.
11. Ajustez la **Gigue (ms)** selon vos besoins.
12. Ajustez le **Taux de perte de paquets (%)** selon vos besoins.
13. Ne renseignez pas de **Taux d'indisponibilité (%)**.

Passerelles

14. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
15. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-1.
16. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.
17. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
18. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-2.
19. Répétez les étapes 17 et 18 pour ajouter l'objet LIL-WAN-3.
20. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

Configuration avancée

21. Dans le cadre **Configuration avancée**, pour la valeur du champ **Répartition de charge**, sélectionnez **Aucune Répartition de charge**.
22. Pour l'**Activation des passerelles de secours**, sélectionnez l'option **Lorsque toutes les passerelles sont injoignables**.
23. Cliquez sur **Appliquer** puis **Sauvegarder**.

Définir cet objet routeur comme passerelle du firewall FW-LILLE

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage**.
2. Dans le champ **Passerelle par défaut**, sélectionnez l'objet routeur précédemment créé (ROUTER-LILLE-WAN-FAILOVER dans cet exemple).
3. Cliquez sur **Appliquer** puis **Sauvegarder**.

Créer la règle de filtrage autorisant les réseaux internes à accéder à Internet

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Action**, onglet **Général** : positionnez l'**Action** à **passer**.
6. Menu de gauche **Source** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet **Network_internals**.
7. Menu de gauche **Destination** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet **Internet.**
8. Menu de gauche **Port / Protocole** : ajoutez à la grille des **Ports destination** les différents objets correspondant aux ports à autoriser dans cette règle de filtrage.
9. Menu de gauche **Inspection** : il est conseillé de laisser le **Niveau d'inspection** proposé par défaut, **IPS**.
10. Cliquez sur **OK**.
11. Cliquez sur **Appliquer**.

Créer les règles de translation d'adresses (NAT) pour les flux à destination d'Internet

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **NAT**.

Premier accès WAN de LILLE

2. Cliquez sur **Nouvelle règle** > **Règle simple**.
3. Double-cliquez dans l'une des colonnes de cette règle.
4. Menu de gauche **Général** : passez l'**État** de la règle à **On**.
5. Menu de gauche **Source originale**, grille des **Machines sources** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet **Network_internals**.
6. Menu de gauche **Destination originale** :
   a. Dans l'onglet **Général**, grille des **Machines destinations** : double-cliquez sur l'objet **Any** et remplacez-le par l'objet **Internet**.
   b. Dans l'onglet **Configuration avancée**, champ **Interface de sortie** : sélectionnez l'objet correspondant à la première interface WAN de LILLE (WAN-1 dans l'exemple).

7. Menu de gauche **Source translatée** :
   a. Champ **Machine source translatée** : sélectionnez l'objet correspondant à la première adresse IP publique du firewall (Firewall_WAN-1 dans cet exemple).
   b. Champ **Port source translaté** : sélectionnez l'objet **ephemeral_fw**.
   c. Cochez la case **Choisir aléatoirement le port source translaté**.
8. Cliquez sur **OK**.

Répétez les étapes 2 à 9 pour créer les règles de NAT correspondant aux deux autres accès WAN du site de LILLE avec les objets suivants :

Deuxième accès WAN de LILLE

Champ	Valeur
Source originale - Machines destination	**Network_internals**
Destination originale - Machines destination	Internet
Destination originale - Interface de sortie	WAN-2
Source translatée - Machine source translatée	Firewall_WAN-2

Troisième accès WAN de LILLE

Champ	Valeur
Source originale - Machines destination	**Network_internals**
Destination originale - Machines destination	Internet
Destination originale - Interface de sortie	WAN-3
Source translatée - Machine source translatée	Firewall_WAN-3

Ces règles de NAT prennent donc la forme suivante :

Status	Original traffic (before translation)				Traffic after translation			
	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
on	Network_internal	Internet interface: WAN-1	Any		Firewall_WAN-1	ephemeral_fw	Any	
on	Network_internal	Internet interface: WAN-2	Any		Firewall_WAN-2	ephemeral_fw	Any	
on	Network_internal	Internet interface: WAN-3	Any		Firewall_WAN-3	ephemeral_fw	Any	

Exemple 4 : utilisation d'objets routeur par le proxy SSL

Cet exemple présente l'utilisation d'un objet routeur pour assurer de la redondance au sein du proxy SSL : les deux premiers liens WAN-1 et WAN-2 sont définis comme passerelles principales, le lien WAN-3 étant défini comme une passerelle de secours.

Notez qu'il est également possible d'utiliser un objet routeur avec du partage de charge entre ses passerelles.

Pour plus d'informations sur le filtrage des flux SSL, veuillez consulter la Note Technique Filtrer les connexions HTTPS.

Principe du routage

Le proxy SSL peut utiliser :

- Une route par défaut au travers d'un objet routeur assurant de la redondance (*failover*),
- Du routage par politique de filtrage.

Lorsqu'une passerelle composant l'objet routeur devient injoignable, un paquet RST est envoyé au navigateur web du poste client et ce dernier établit une nouvelle connexion via le Proxy SSL sur un des liens WAN disponibles.

Créer l'objet routeur destiné au routage

1. Placez-vous dans le menu **Configuration** > **Objets** > **Réseau.**
2. Cliquez sur **Ajouter**.
3. Dans la colonne de gauche de la fenêtre de création d'objet, sélectionnez **Routeur**.

Propriétés générales

4. Nommez l'objet (exemple : ROUTER-LILLE-WAN-FAILOVER).

Supervision

5. Pour la **Méthode de détection**, sélectionnez **ICMP**.
6. Ajustez le **Délai d'expiration (s)** selon vos besoins.
7. Ajustez l'**Intervalle de tests (s)** selon vos besoins.
8. Ajustez le nombre d'**Échecs avant dégradation** (3 par défaut).

SLA SD-WAN (seuils)

9. Cochez la case **SLA SD-WAN (seuils)**.
10. Ajustez la **Latence (ms)** selon vos besoins.
11. Ajustez la **Gigue (ms)** selon vos besoins.
12. Ajustez le **Taux de perte de paquets (%)** selon vos besoins.
13. Ne renseignez pas de **Taux d'indisponibilité (%)**.

Passerelles

14. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
15. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-1.
16. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

17. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
18. Dans la colonne **Passerelle**, sélectionnez l'objet LIL-WAN-2.
19. Répétez les étapes 17 et 18 pour ajouter l'objet LIL-WAN-3.
20. Dans la colonne **Cible(s) des tests**, sélectionnez **Tester directement la passerelle**.

Configuration avancée

21. Dans le cadre **Configuration avancée**, pour la valeur du champ **Répartition de charge**, sélectionnez **Aucune Répartition de charge**.
22. Pour l'**Activation des passerelles de secours**, sélectionnez l'option **Lorsque toutes les passerelles sont injoignables**.
23. Cliquez sur **Appliquer** puis **Sauvegarder**.

Cas du routage par défaut

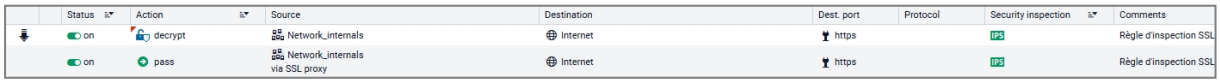
Ajouter l'objet routeur comme route par défaut

1. Placez-vous dans le menu **Configuration** > **Réseau** > **Routage**.
2. Dans le champ **Passerelle par défaut**, sélectionnez l'objet routeur précédemment créé (ROUTER-LILLE-WAN-FAILOVER dans cet exemple).
3. Cliquez sur **Appliquer** puis **Sauvegarder**.

Créer la règle d'inspection SSL

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle** > **Règle d'inspection SSL**.
3. Dans le champ **Machines sources** : laissez l'objet **Network_internals** proposé par défaut ou sélectionnez un objet correspondant à vos machines clientes.
4. Dans le champ **Port dest.** : sélectionnez l'objet **https**.
5. Si vous n'avez pas défini de **Profil d'inspection** spécifique ou de **Politique de filtrage SSL**, vous pouvez laisser les autres valeurs proposées par défaut. Sinon, sélectionnez votre profil d'inspection et / ou votre politique de filtrage SSL.
6. Cliquez sur **Terminer**.
7. Cliquez sur **Appliquer** pour valider ces modifications de la politique de filtrage.
8. Choisissez si vous souhaitez **Activer maintenant** cette politique ou l'activer **Plus tard**.

La règle d'inspection SSL prend la forme suivante :



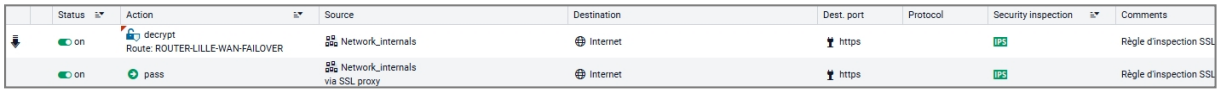
Cas du routage par politique de filtrage

Créer la règle d'inspection SSL

1. Placez-vous dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.

2. Cliquez sur **Nouvelle règle** > **Règle d'inspection SSL**.
3. Dans le champ **Machines sources** : laissez l'objet **Network_internals** proposé par défaut ou sélectionnez un objet correspondant à vos machines clientes.
4. Dans le champ **Port dest.** : sélectionnez l'objet **https**.
5. Si vous n'avez pas défini de **Profil d'inspection** spécifique ou de **Politique de filtrage SSL**, vous pouvez laisser les autres valeurs proposées par défaut. Sinon, sélectionnez votre profil d'inspection et / ou votre politique de filtrage SSL.
6. Cliquez sur **Terminer**.
7. Double-cliquez dans la colonne **Action** de la règle de déchiffrement nouvellement créée.
8. Dans l'onglet **Général**, pour le champ **Passerelle - routeur**, sélectionnez l'objet routeur destiné au routage (ROUTER-LILLE-WAN-FAILOVER dans cet exemple).
9. Cliquez sur **OK** puis **Appliquer** pour valider ces modifications de la politique de filtrage.
10. Choisissez si vous souhaitez **Activer maintenant** cette politique ou l'activer **Plus tard**.

La règle d'inspection SSL prend la forme suivante :



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu