



**STORMSHIELD**



NOTE TECHNIQUE

**STORMSHIELD NETWORK SECURITY**

# SD-WAN : SÉLECTIONNER LE MEILLEUR LIEN RÉSEAU

Produits concernés : SNS 4.3 et versions supérieures

Dernière mise à jour du document : 20 mars 2022

Référence : sns-fr-sd-wan\_sélectionner\_meilleur\_lien\_réseau-note\_technique



# Table des matières

Avant de commencer .....	3
Comprendre les différentes composantes du SD-WAN SNS .....	4
Comprendre les paramètres de supervision .....	4
Méthode de détection et Port .....	4
Délai d'expiration [s] .....	4
Intervalle de tests [s] .....	4
Échecs avant dégradation .....	4
Comprendre les métriques du SLA SD-WAN .....	4
La latence [ms] .....	4
La gigue [ms] .....	5
Taux de perte de paquets [%] .....	5
Taux d'indisponibilité .....	5
Évaluer les valeurs à appliquer à chaque métrique .....	5
Comprendre le mécanisme de bascule et le choix des liens empruntés .....	7
Architecture présentée .....	8
Créer les objets .....	10
Créer les objets machine pour les passerelles des opérateurs .....	10
Créer les objets machine pour les serveurs VoIP .....	10
Pour créer un groupe avec les serveurs VoIP .....	11
Créer l'objet routeur destiné à appliquer les contraintes pour les flux VoIP .....	11
Créer la règle de PBR pour les flux VoIP .....	13
Superviser les liens SD-WAN depuis l'interface d'administration du firewall .....	14
Vue synthétique : le tableau de bord des indicateurs de santé .....	14
Vue détaillée : le module de supervision SD-WAN .....	14
Onglet Temps réel .....	14
Onglet Historique .....	15
Pour aller plus loin .....	16



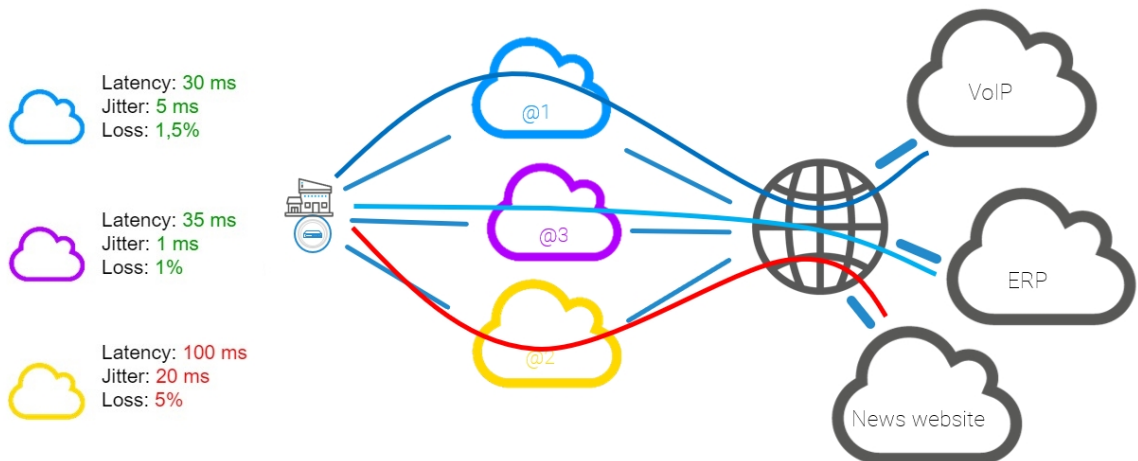
## Avant de commencer

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 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 *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.
- La méthode de détection de type ICMP : cette méthode est basée sur l'envoi régulier de paquets de type *ICMP Request* sur chaque lien.

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 mesurée 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.



# Comprendre le mécanisme de bascule et le choix des liens empruntés

Lors de chaque mesure / calcul de métrique, chaque lien fait l'objet d'un calcul de "score" : 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.

Le lien obtenant le meilleur "score" est choisi pour faire passer le flux.

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 pour la VoIP selon la configuration avancée de l'objet routeur				
Lien @1 (Router1)	Lien @2 (Router2)	Lien @3 (Router3)	Lien @4 (Router3)	Sans partage de charge		Partage de charge		
						Lorsqu'au moins une passerelle est injoignable		Lorsque toutes les passerelles sont injoignables
						Activer toutes les passerelles de secours		Activer toutes les passerelles de secours
✓	✓	✓	✓	Lien @1	Lien @1 & Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2
⚠	✓	✓	✓	Lien @2	Lien @2	Lien @2	Lien @2 & Lien @3	Lien @2 & Lien @3 & Lien @4
⚠	⚠⚠	✓	✓	Lien @3	Lien @3 & Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4
⚠	⚠⚠	⚠	✓	Lien @4	Lien @4	Lien @4	Lien @4	Lien @4
⚠	⚠⚠	⚠	⚠⚠	Lien @1	Lien @1 & Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2
⚠⚠	⚠	⚠	⚠⚠	Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2	Lien @1 & Lien @2
⚠	✗	⚠	⚠⚠	Lien @1	Lien @1	Lien @1	Lien @1 & Lien @3	Lien @1 & Lien @3 & Lien @4
⚠	✗	⚠⚠	⚠	Lien @1	Lien @1	Lien @1	Lien @1 & Lien @4	Lien @1 & Lien @3 & Lien @4
⚠	✗	✓	⚠	Lien @3	Lien @3	Lien @3	Lien @3	Lien @3
✗	✗	⚠⚠	⚠	Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4
✗	✗	⚠	⚠⚠	Lien @3	Lien @3 & Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4	Lien @3 & Lien @4
✗	✗	✗	⚠	Lien @4	Lien @4	Lien @4	Lien @4	Lien @4
✗	✗	✗	✗	Aucun lien - Route par défaut	Aucun lien - Route par défaut	Aucun lien - Route par défaut	Aucun lien - Route par défaut	Aucun lien - Route par défaut
✗	✗	✓	✗	Lien @3	Lien @3	Lien @3	Lien @3	Lien @3
✗	✓	✓	✗	Lien @2	Lien @2	Lien @2	Lien @2 & Lien @3	Lien @2 & Lien @3
✗	✓	✓	✓	Lien @2	Lien @2	Lien @2	Lien @2 & Lien @3	Lien @2 & Lien @3 & Lien @4

## Légende

- ✓ Lien optimal
- ⚠ Lien dégradé (ne respectant pas les seuils SLA)
- ⚠⚠ Lien fortement dégradé (si plusieurs liens sont dégradés : lien présentant le moins bon "score")
- ✗ Lien indisponible



## Architecture présentée

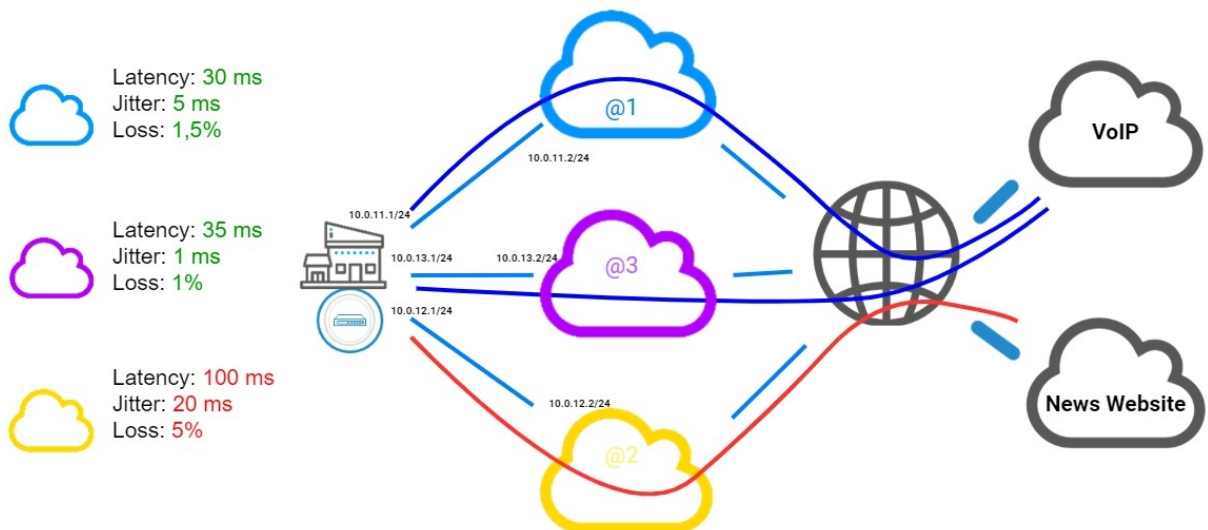
L'exemple de configuration présenté dans cette note technique est celui d'une entreprise disposant de trois accès distants :

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

### Légende

- ✓ Lien optimal
- ! Lien dégradé (ne respectant pas les seuils SLA)
- !! Lien fortement dégradé (si plusieurs liens sont dégradés : lien présentant le moins bon "score")
- ✗ Lien indisponible



## 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 le ou les objets correspondant au(x) serveur(s) 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 l'exemple décrit dans ce document, on utilise le port TCP/5060 correspondant au protocole SIP.

La disponibilité et les performances de chaque lien sont ainsi testées en initiant une connexion au serveur distant VoIP depuis le firewall vers en utilisant le port TCP/5060.

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 *TCP Probe*.
5. Pour le **Port**, sélectionnez *sip\_tcp*.
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** (5 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 Router1.
16. Dans la colonne **Cible(s) des tests**, sélectionnez le serveur VoIP distant ou le groupe de serveurs VoIP distants (objet *Remote\_VoIP* dans cette note technique).
17. Répétez les étapes 14 à 16 pour ajouter l'objet Router2.
18. Dans l'onglet **Passerelles de secours**, cliquez sur **Ajouter**.
19. Dans la colonne **Passerelle**, sélectionnez l'objet Router3.
20. Dans la colonne **Cible(s) des tests**, sélectionnez le serveur VoIP distant ou le groupe de serveurs VoIP distants (objet *Remote\_VoIP* dans cette note technique).

#### Configuration avancée

Afin de conserver une qualité de lien optimale dans un maximum de cas, l'objet routeur VoIP est configuré avec de la répartition de charge entre les liens utilisés. De même, il est configuré pour utiliser un lien de secours dès lors qu'un lien principal est dans un état dégradé ou inaccessible.

21. Dans le cadre **Configuration avancée**, sélectionnez l'option de **Répartition de charge Par connexion**.
22. Pour l'**Activation des passerelles de secours**, sélectionnez l'option *Lorsqu'au moins une passerelle est injoignable*.
23. 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 :

	Status ▾	Action ▾	Source	Destination	Dest. port	Protocol	Security inspection ▾
	on	pass Route: SD-WAN_VoIP	Any	Remote_VoIP	sip_tcp		IPS

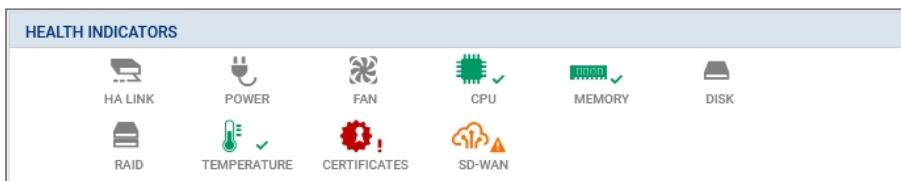


# Superviser les liens SD-WAN depuis l'interface d'administration du firewall

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 sont opérationnelles et respectent les critères SLA SD-WAN définis,
- **Orange** : une passerelle (au moins) est en état dégradé,
- **Rouge** : une passerelle (au moins) n'est pas joignable.

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 comme passerelle par défaut et dans les règles de routage par politique (PBR : Policy Based Routing).

## Onglet Temps réel

L'onglet **Temps réel** affiche des informations liées au SLA SD-WAN pour les passerelles et routeurs supervisés.

Sur la ligne correspondant à un routeur :

- L'état du routeur associé à un code couleur selon les mêmes critères que sur le tableau de bord (**vert**, **orange** ou **rouge**),
- Les seuils fixés pour chaque métrique (Latence, Gigue, Taux de perte de paquets),
- Le statut SLA du routeur.

Sur la ligne correspondant à une passerelle composant ce routeur :

- L'état de la passerelle associé à un code couleur (**vert** : opérationnelle, **orange** : dégradée ou **rouge** : injoignable),
- La valeur de chaque métrique associée à un code couleur (**vert**, **orange** ou **rouge**) permettant de visualiser aisément si elles respectent ou non les seuils fixés.
- Le statut SLA de la passerelle.



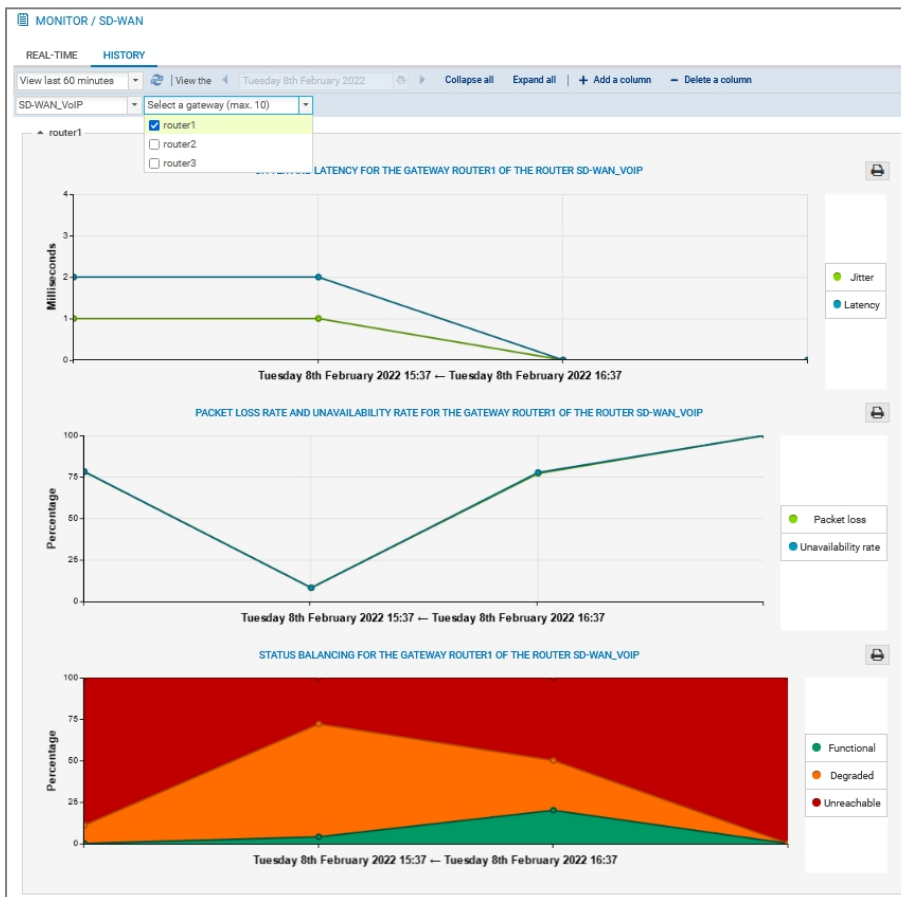
Pour obtenir plus de détails sur les valeurs que peuvent prendre ces différents indicateurs, consultez le module [Supervision SD-WAN du Manuel Utilisateur Stormshield SNS v4](#).

MONITOR / SD-WAN											
REAL-TIME HISTORY											
Search	Refresh	Export results	Configure routing	reset columns							
Routers/Gateways	IP address	Main/backup	SD-WAN SLA	Detection method	Type	Status	Latency (ms)	Jitter (ms)	Packet loss (%)	SLA status	
SD-WAN_VoIP			Active	TCP Probe (slp_tcp)		Functional	Threshold:500	Threshold:30	Threshold:10	Degraded	
Router1		Principal	Active		Policy-based routing	Active	1	2	0.6	Good	
Router2		Principal	Active		Policy-based routing	Active	2	1	0.6	Good	
Router3		Backup	Unreachable		Policy-based routing	Unreachable	N/A	N/A	100	Unreachable	

### Onglet Historique

Cet onglet permet de sélectionner, pour un routeur donné, de 1 à 5 passerelles afin d'afficher les courbes d'évolution de la latence, de la gigue, du taux de perte de paquets, du taux de disponibilité et de la proportion de temps passée dans les différents états pour chacune des passerelles sélectionnées.

Exemple pour la passerelle *Router1* du routeur *SD-WAN\_VoIP* :





## Pour aller plus loin

---

Des informations complémentaires et réponses à vos éventuelles questions sur la haute disponibilité sont disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).





**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.*

*Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.*