NOTE TECHNIQUE
STORMSHIELD NETWORK SECURITY

INTERFACES VIRTUELLES IPSEC - CONFIGURATION AVEC AMAZON WEB SERVICES

Produits concernés : SNS 5.1 et versions supérieures

Dernière mise à jour du document : 3 aout 2026

Référence : sns-fr-VPN_IPsec-VTI_0thers_vendors_AWS-Note_Technique

Table des matières

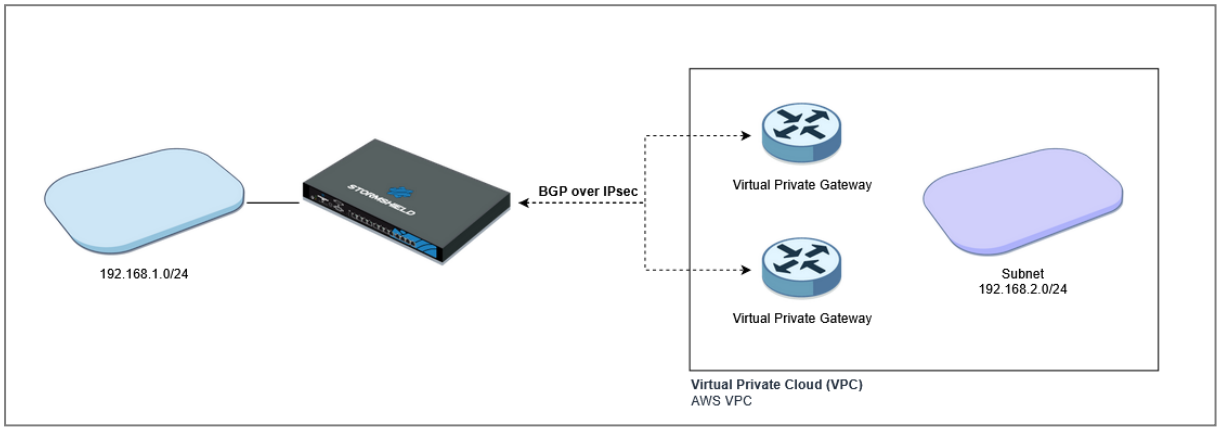
Historique des modifications

Date	Description
3 août 2026	Nouveau document

Avant de commencer

Ce document montre comment établir un tunnel IPsec redondant avec un Cloud Privé Virtuel (VPC) Amazon Web Services (AWS) grâce au protocole de routage dynamique BGP.

Il présente, dans une architecture servant d'exemple, les différentes configurations que vous devez réaliser. Les possibilités de configuration étant nombreuses, adaptez ces éléments selon votre architecture et vos besoins.



Prérequis

- Disposer d'un firewall SNS en version 5.1 ou supérieure,
- Disposer d'un compte Amazon Web Services (AWS) et avoir accès à la Console de gestion AWS.
- L'adresse IP utilisée pour établir les tunnels doit être statique et peut se trouver derrière un dispositif de translation d'adresses réseau (NAT). Pour plus d'informations sur la translation d'adresses réseau, reportez-vous à la note technique Intégration du NAT dans IPsec.

Configurer l'environnement Amazon Web Services (AWS)

Pour relier votre réseau local au Cloud privé virtuel AWS, Amazon propose de créer un tunnel redondant entre le firewall SNS et le VPC AWS et de router le trafic à l'aide du protocole de routage dynamique BGP. La configuration de l'environnement AWS s'appuie sur différentes ressources :

- Cloud privé virtuel (VPC) : il s'agit d'un réseau virtuel auquel sont rattachées les autres ressources. La configuration d'un VPC consiste principalement en un bloc CIDR (IPv4 et/ou IPv6). Le réseau choisi ne doit pas se chevaucher avec un réseau défini localement (on-premise).
- Sous-réseau : il est contenu dans le VPC. Un VPC peut contenir plusieurs sous-réseaux publics ou privés.
- Passerelle client : il s'agit du point de terminaison du tunnel IPsec sur le site client (on-premise).
- Passerelle privée virtuelle : il s'agit du point de terminaison du tunnel IPsec dans le VPC.

NOTE
Nous vous recommandons de consulter la documentation d'Amazon Web Services avant de suivre cette procédure :

- Documentation AWS Virtual Private Network
- Documentation Amazon Virtual Private Cloud

Connectez-vous à votre console AWS afin de réaliser toutes les étapes de configuration de l'environnement Amazon Web Services.

Configurer la ressource Cloud privé virtuel (VPC)

1. Rendez-vous dans **VPC** > **Cloud privé virtuel** > **Vos VPC**.
2. Cliquez sur **Créer un VPC**.
3. Renseignez les champs suivants :
   - **Ressources à créer** : sélectionnez **VPC uniquement**,
   - **Identification de nom** : indiquez le nom de la ressource (par exemple *AWS VPC*),
   - **Bloc d'adresses CIDR IPv4** : sélectionnez **Entrée manuelle CIDR IPv4**,
   - **CIDR IPv4** : indiquez l'adresse du réseau utilisé sur l'environnement AWS (par exemple 192.168.2.0/24),
   - **Bloc CIDR IPv6** : sélectionnez **Aucun bloc d'adresses CIDR IPv6**,
   - **Location** : laissez la valeur à **Par défaut**,
   - **Contrôle de chiffrement VPC** : sélectionnez **Aucun**.
4. Cliquez sur **Créer un VPC**.

Configurer la ressource Sous-réseau

1. Rendez-vous dans **VPC** > **Cloud privé virtuel** > **Sous-réseaux**.
2. Cliquez sur **Créer un sous-réseau**.
3. Dans la section **VPC** > **ID de VPC**, sélectionnez le VPC créé précédemment (AWS VPC dans l'exemple).
4. Dans la section **Paramètres du sous-réseau**, renseignez les champs suivants :
   - **Nom du sous-réseau (subnet)** : indiquez le nom du sous-réseau (par exemple *AWS Subnet*),
   - **Zone de disponibilité** : sélectionnez **Aucune préférence**,
   - **Bloc d'adresse CIDR IPv4 VPC** : indiquez le plan d'adressage dans lequel créer ce sous-réseau (par exemple 192.168.2.0/24),
   - **Bloc d'adresse CIDR de sous-réseau IPv4** : indiquez le plan d'adressage utilisé sur ce sous-réseau (par exemple 192.168.2.0/24 ou 192.168.2.96/27).
5. Cliquez sur **Créer un sous-réseau**.

Configurer la ressource Passerelle client

1. Rendez-vous dans **VPC** > **Réseau VPN** > **Passerelles client**.
2. Cliquez sur **Création d'une passerelle client**.
3. Renseignez les champs suivants :
   - **Balise Nom** : indiquez le nom de la passerelle (par exemple *SNS gateway*).
   - **Numéro ASN BGP** : indiquez le numéro de système autonome (ASN) de la passerelle SNS (par exemple 65532). Notez que la RFC 6996 définit les numéros de systèmes autonomes (ASN) à usage privé suivants :
     - 16 bits : 64512 - 65534,
     - 32 bits : 4200000000 - 4294967294.
   - **Adresse IP** : indiquez l'adresse IP publique de la passerelle SNS (par exemple 198.51.100.1).
4. Cliquez sur **Création d'une passerelle client**.

Configurer la ressource Passerelle privée virtuelle

1. Rendez-vous dans **VPC** > **VPN** > **Réseau VPN** > **Passerelles réseau privé virtuel**.
2. Cliquez sur **Création d'une passerelle privée virtuelle**.
3. Renseignez les champs suivants :
   - **Balise nom** : indiquez le nom de la passerelle (par exemple *AWS gateway*),
   - **Numéro de système autonome (ASN)** : sélectionnez **ASN personnalisé**,
   - **Saisir l'ASN personnalisé** : indiquez le numéro de système autonome (ASN) de la passerelle privée virtuelle (par exemple 65000). Notez que la RFC 6996 définit les numéros de systèmes autonomes (ASN) à usage privé suivants :
     - 16 bits : 64512 - 65534,
     - 32 bits : 4200000000 - 4294967294.
4. Cliquez sur **Création d'une passerelle privée virtuelle**.

5. Sélectionnez la passerelle privée virtuelle que vous venez de créer (*AWS gateway* dans l'exemple) et cliquez sur **Actions**.
6. Sélectionnez **Attacher au VPC**.
7. Dans le menu déroulant **VPC disponibles**, sélectionnez la ressource VPC créée précédemment (*AWS VPC* dans l'exemple).
8. Cliquez sur **Attacher au VPC**.

Configurer le routage

Vous devez définir la manière dont les paquets sont acheminés entre les sous-réseaux de votre VPC et votre réseau local (on-premise).

Créer la ressource Table de routage

1. Rendez-vous dans **VPC** > **Cloud privé virtuel** > **Tables de routage**.
2. Cliquez sur **Créer une table de routage**.
3. Renseignez les champs suivants :
   - **Nom** : indiquez le nom de la table de routage (par exemple *AWS Route Table*),
   - **VPC** : sélectionnez dans le menu déroulant la ressource VPC créée précédemment (*AWS VPC* dans l'exemple).
4. Cliquez sur **Créer une table de routage**.
5. Sélectionnez la table de routage que vous venez de créer (*AWS Route Table* dans l'exemple) et cliquez sur **Actions**.
6. Sélectionnez **Modifier la propagation de routage**.
7. Cochez la case **Activer** de la passerelle (*AWS gateway* dans l'exemple) pour activer la propagation des routes.
8. Cliquez sur **Enregistrer**.

Propager les routes vers la ressource Sous-réseau

1. Rendez-vous dans **VPC** > **Cloud privé virtuel** > **Sous-réseaux**.
2. Sélectionnez le sous-réseau créé précédemment (*AWS subnet* dans l'exemple) et cliquez sur **Actions**.
3. Sélectionnez **Modifier une association des tables de routage**.
4. Dans le menu déroulant **ID de la table de routage**, sélectionnez la table de routage créée précédemment *(AWS Route Table* dans l'exemple).
5. Cliquez sur **Enregistrer**.

Configurer la ressource Connexion VPN

Vous devez définir la connexion VPN et sélectionner les ressources et les options de configuration nécessaires pour la connexion site à site.

1. Rendez-vous dans **VPC** > **Réseau VPN** > **Connexions VPN site à site**.
2. Cliquez sur **Création d'une connexion VPN**.

3. Renseignez les champs suivants :
   - **Balise Nom** : indiquez le nom de la connexion (par exemple *VPN with SNS*),
   - **Type de passerelle cible** : sélectionnez **Passerelle réseau privé virtuel**,
   - **Passerelle réseau privé virtuel** : sélectionnez la passerelle réseau virtuel créée précédemment (*AWS gateway* dans l'exemple),
   - **Passerelle client** : sélectionnez **Existant**,
   - **ID de la passerelle client** : sélectionnez la passerelle client créée précédemment (*SNS gateway* dans l'exemple),
   - **Options de routage** : sélectionnez **Dynamique (BGP requis)**,
   - **Stockage de la clé pré-partagée** : sélectionnez **Standard**,
   - **CIDR du réseau IPv4 local** : laissez ce champ vide,
   - **CIDR du réseau IPv4 distant** : laissez ce champ vide.
4. Vous pouvez laisser les paramètres par défaut des champs **Options du tunnel 1** et **Options du tunnel 2**, ou vous pouvez les personnaliser.
5. Cliquez sur **Création d'une connexion VPN**.

Télécharger la configuration IPsec

1. Rendez-vous dans **VPC** > **Réseau VPN** > **Connexions VPN site à site**.
2. Sélectionnez la connexion VPN créée précédemment (*VPN with SNS* dans l'exemple).
3. Cliquez sur **Télécharger la configuration**.
4. Dans la fenêtre pop-up qui s'affiche, renseignez les champs suivants :
   - **Fournisseur** : sélectionnez **Generic**,
   - **Plateforme** : sélectionnez **Generic**,
   - **Logiciel** : sélectionnez **Vendor Agnostic**,
   - **IKE version** : sélectionnez **ikev2**.
5. Cliquez sur **Télécharger**.

Comme dans l'exemple ci -dessous, un fichier texte (.txt) portant l'ID de la connexion VPN créée précédemment (*VPN with SNS* dans l'exemple) est téléchargé. Il décrit la configuration à mettre en œuvre sur la passerelle SNS et contient :

- Les adresses IP des tunnels,
- Les adresses IP publiques des passerelles AWS,
- La clé pré-partagée (PSK) définie par AWS.

vpn-0d928d8b22f89021f.txt

```
[...]
#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is
associated with the IPSec tunnel. All traffic transmitted to the tunnel
interface is encrypted and transmitted to the Virtual Private Gateway.

The Customer Gateway and Virtual Private Gateway each have two addresses
that relate
to this IPSec tunnel. Each contains an outside address, upon which
encrypted
traffic is exchanged. Each also contain an inside address associated with
```

```
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer
Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway: 198.51.100.1                ◄ SNS PUBLIC IP ADDRESS
  - Virtual Private Gateway: 52.51.13.54           ◄ AWS PUBLIC IP ADDRESS

Inside IP Addresses
  - Customer Gateway: 169.254.238.178/30          ◄ LOCAL IP ADDRESS(SNS)
  - Virtual Private Gateway: 169.254.238.177/30   ◄ REMOTE IP ADDRESS
(AWS)

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes
[...]
```

Configurer le firewall SNS

Pour que le firewall SNS puisse servir de passerelle et permettre le routage, vous devez configurer :

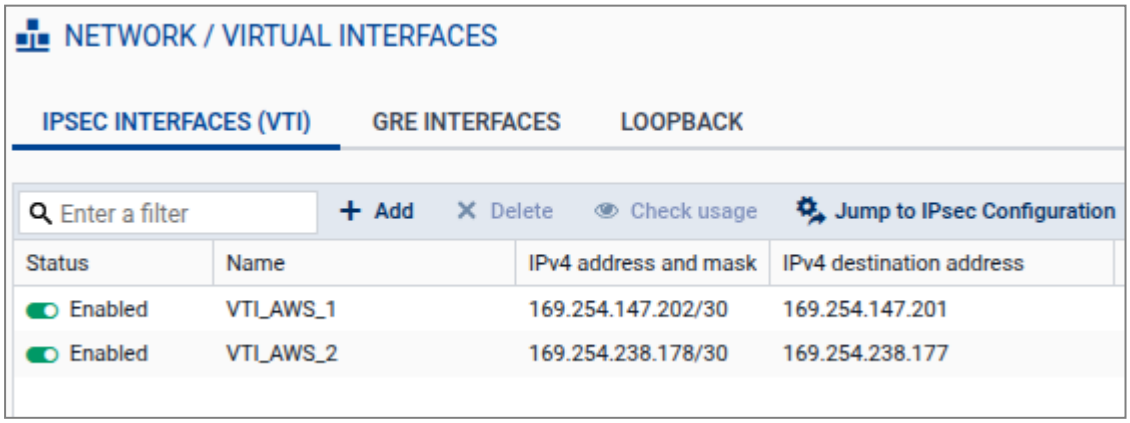
- Les interfaces virtuelles IPsec (VTI),
- Le tunnel IPsec,
- Le routage dynamique basé sur le protocole BGP.

Connectez-vous à l'interface Web d'administration du firewall SNS afin de réaliser toutes les étapes de sa configuration.

Configurer les interfaces virtuelles IPsec (VTI)

IMPORTANT
Le plan d'adressage utilisé doit obligatoirement être un sous-réseau /30 compris dans le réseau 169.254.0.0/16. Les adresses IP des interfaces sont définies lors de la configuration de l'environnement AWS. Vous pouvez les retrouver dans le fichier texte (.txt) obtenu précédemment (voir la section Télécharger la configuration IPsec).

1. Rendez-vous dans le menu **Configuration** > **Réseau** > **Interfaces virtuelles** et sélectionnez l'onglet **Interfaces IPsec (VTI)**.
2. Cliquez sur **Ajouter**.
3. Renseignez les champs suivants :
   - **Nom** : VTI_AWS_1 par exemple,
   - **Adresse IPv4 et masque** : 169.254.147.202/30 dans l'exemple,
   - **Adresse IPv4 de destination** : 169.254.147.201 dans l'exemple.
4. En suivant la même méthode, créez la seconde interface virtuelle IPsec avec les valeurs suivantes :
   - **Nom** : VTI_AWS_2 par exemple,
   - **Adresse IPv4 et masque** : 169.254.238.178/30 dans l'exemple,
   - **Adresse IPv4 de destination** : 169.254.238.177 dans l'exemple.



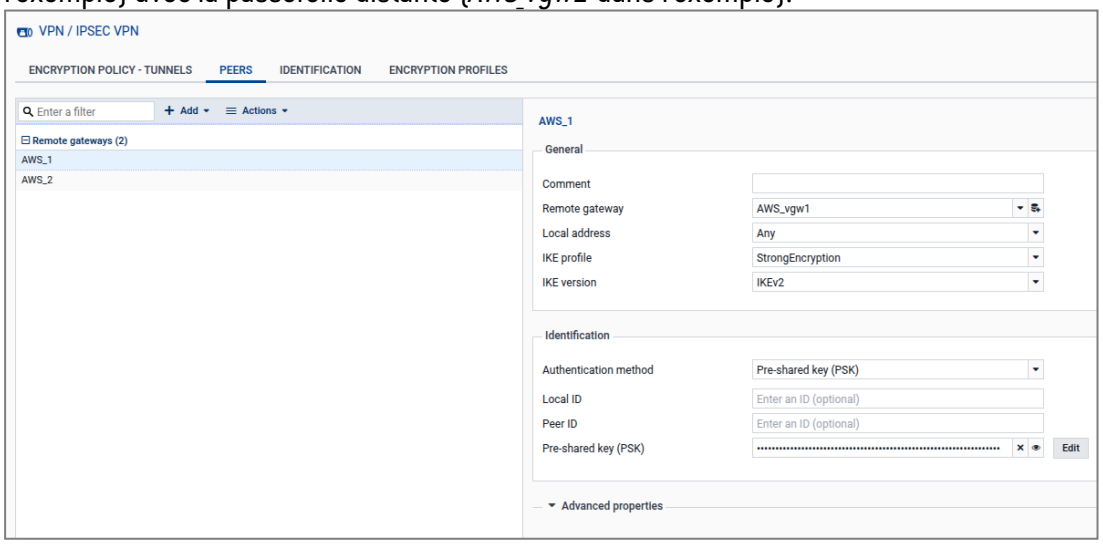
Configurer le tunnel IPsec

Configurer le correspondant IPsec

Amazon Web Services (AWS) privilégie par défaut la méthode d'authentification par clé pré-partagée (PSK). Vous pouvez utiliser la méthode d'authentification par certificat. Pour plus d'informations sur ces options d'authentification, vous pouvez consulter la Documentation AWS Virtual Private Network.

Les adresses IP des interfaces et la clé pré-partagée (PSK) sont définies lors de la configuration de l'environnement AWS. Vous pouvez les retrouver dans le fichier texte (.txt) obtenu précédemment (voir la section Télécharger la configuration IPsec).

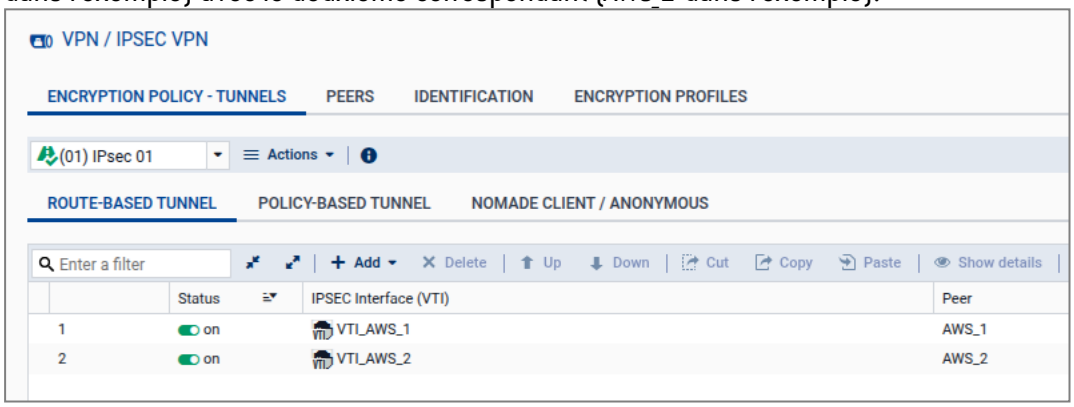
1. Rendez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** et sélectionnez l'onglet **Correspondants**.
2. Cliquez sur **Ajouter**.
3. Choisissez P**asserelle statique**. Un assistant s'affiche.
4. Sélectionnez la passerelle distante (*AWS_vgw1* dans l'exemple).
5. Saisissez le nom du correspondant (*AWS_1* dans l'exemple).
6. Sélectionnez **IKEv2** comme version IKE et cliquez sur **Suivant**.
7. Sélectionnez le type d'authentification par **Clé pré-partagée (PSK)**.
8. Dans les champs **Clé pré-partagée (PSK)** et **Confirmer**, saisissez la PSK définie par AWS (section "Internet Key Exchange Configuration").
9. Cliquez sur **Suivant** puis **Terminer**.
10. Cliquez sur **Appliquer**.
11. Suivez la même procédure pour configurer le deuxième correspondant (*AWS_2* dans l'exemple) avec la passerelle distante (*AWS_vgw2* dans l'exemple).



Définir la politique IPsec

Les adresses IP des interfaces sont définies lors de la configuration de l'environnement AWS. Vous pouvez les retrouver dans le fichier texte (.txt) obtenu précédemment (voir la section Télécharger la configuration IPsec).

1. Rendez-vous dans le menu **Configuration** > **VPN** > **VPN IPsec** et sélectionnez l'onglet **Politique de chiffrement - tunnels** > onglet **Tunnel basé sur le routage**.
2. Cliquez sur **Ajouter** puis sélectionnez **Tunnel basé sur le routage**. Un assistant s'affiche.
3. Dans **Interface IPsec (VTI)**, sélectionnez l'interface virtuelle IPsec créée précédemment (*VTI_AWS_1* dans l'exemple).
4. Dans **Choix du correspondant**, sélectionnez le correspondant (*AWS_1* dans l'exemple).
5. Cliquez sur **Suivant** puis **Suivant**.
6. Créez une route statique pour joindre la passerelle distante / VTI distante si celle-ci n'est pas déjà définie, ou décochez **Routage statique** - **Créer une route statique** si cette route existe.
7. Cliquez sur **Terminer**.
8. Activez la politique en positionnant le curseur d'**État** sur *Activé*.
9. Suivez la même procédure pour configurer la deuxième interface virtuelle IPsec (*VTI_AWS_2* dans l'exemple) avec le deuxième correspondant (*AWS_2* dans l'exemple).



Configurer le routage dynamique (BGP)

Pour configurer le routage dynamique à l'aide du protocole BGP, il est fortement recommandé de lire la note technique Routage Dynamique BIRD v2 et la documentation officielle de BIRD (en particulier les sections qui concernent la configuration des filtres, du protocole Kernel et du protocole BGP). La configuration de BIRD ci-dessous correspond à celle de l'exemple de notre note technique. Adaptez celle-ci (router id, filtres, adresses IP, ASN) en fonction de votre architecture.

bird.conf

```
router id 1.1.1.1;

protocol device {
    scan time 10;
}

protocol kernel {
    scan time 10;
    learn all;
    ipv4 {
        import all;
        export all;
    };
}
```

```
# Filter routes imported from the AWS peer by accepting only the routes to
the Virtual Private Cloud (VPC)
filter aws_import_v4 {
    if net ~ 192.168.2.0/24 then accept;
    reject;
}

# Filter routes exported to the AWS peer by accepting only the routes to
the
# local network (in)
filter aws_export_v4 {
    if net ~ 192.168.1.0/24 then accept;
    reject;
}

protocol bgp aws_1 {
    local 169.254.147.202 as 65532;
    neighbor 169.254.147.201 as 65000;
    direct;
    ipv4 {
        import filter aws_import_v4;
        export filter aws_export_v4;
    };
}

protocol bgp aws_2 {
    local 169.254.238.178 as 65532;
    neighbor 169.254.238.177 as 65000;
    direct;
    ipv4 {
        import filter aws_import_v4;
        export filter aws_export_v4;
    };
}
```

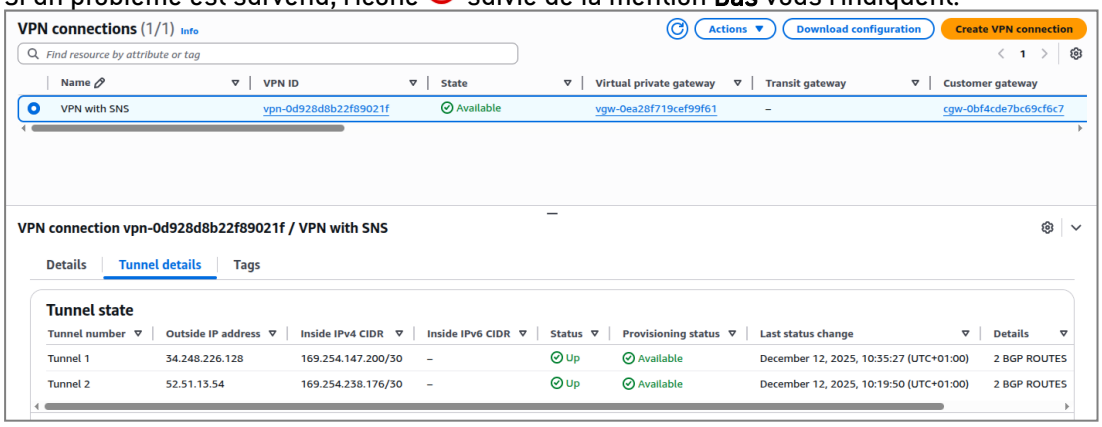
Superviser le trafic

Vérifier l'état des tunnels sur le firewall SNS

1. Rendez-vous dans le menu **Monitoring** > **Supervision** > **Tunnels VPN IPsec**.
2. Dans la colonne **État**, vérifiez l'état des tunnels : si le tunnel est correctement établi, l'icône suivie de la mention **OK** vous l'indiquent.
   Si un problème est survenu, l'icône suivie de la mention **Aucun tunnel** vous l'indiquent. Vous pouvez passer la souris sur cet état pour obtenir des informations concernant le problème rencontré et consulter les logs du VPN dans le menu **Monitoring** > **Logs-Journaux d'audit** > **VPN**.

Vérifier l'état des tunnels sur la console AWS

1. Rendez-vous dans **VPC** > **Réseau VPN** > **Connexions VPN site à site**.
2. Sélectionnez la ressource dans la liste (*VPN with SNS* dans l'exemple).
3. Cliquez sur l'onglet **Détails du tunnel**.
4. Dans la colonne **État**, vérifiez l'état des tunnels : si le tunnel est correctement établi, l'icône suivie de la mention **Disponible** vous l'indiquent.
   Si un problème est survenu, l'icône suivie de la mention **Bas** vous l'indiquent.



Vérifier le bon fonctionnement du routage dynamique BGP

Vous pouvez consulter les logs du routage dans le menu **Monitoring** > **Logs-Journaux d'audit** > **Routage**.

Vérifiez le bon fonctionnement du routage dynamique BGP à l'aide de BIRD v2.

1. Connectez-vous en SSH et lancez l'utilitaire **birdc**.
2. Affichez l'état des sessions BGP à l'aide de la commande :

```
show protocols
```

   La première information affichée est la version de BIRD.

```
VMSNSX01B2085A9>birdc
BIRD 2.15.1 ready.
bird> show protocols
Name       Proto      Net Type   Table      State  Since         Info
device1    Device     Undefined  ---        up     09:33:05.237
kernel1    Kernel     ipv4       master4    up     09:33:05.237
aws_1      BGP        Undefined  ---        up     09:34:28.195
Established
aws_2      BGP        Undefined  ---        up     09:33:13.332
Established
```

3. Affichez les routes apprises par un protocole donné (*aws_1* et *aws_2* dans l'exemple) à l'aide de la commande :

```
show route protocol <proto>
```

```
bird> show route protocol aws_1
Table master4:
192.168.2.0/24       unicast [aws_1 09:35:29.808] * (100) [AS65000i]
       via 169.254.147.201 on ipsec0(VTI_AWS_1)
bird> show route protocol aws_2
Table master4:
192.168.2.0/24       unicast [aws_2 09:35:14.362] (100) [AS65000i]
       via 169.254.238.177 on ipsec1(VTI_AWS_2)
```

4. Affichez les routes annoncées par un protocole donné (*aws_1* et *aws_2* dans l'exemple) à l'aide de la commande :

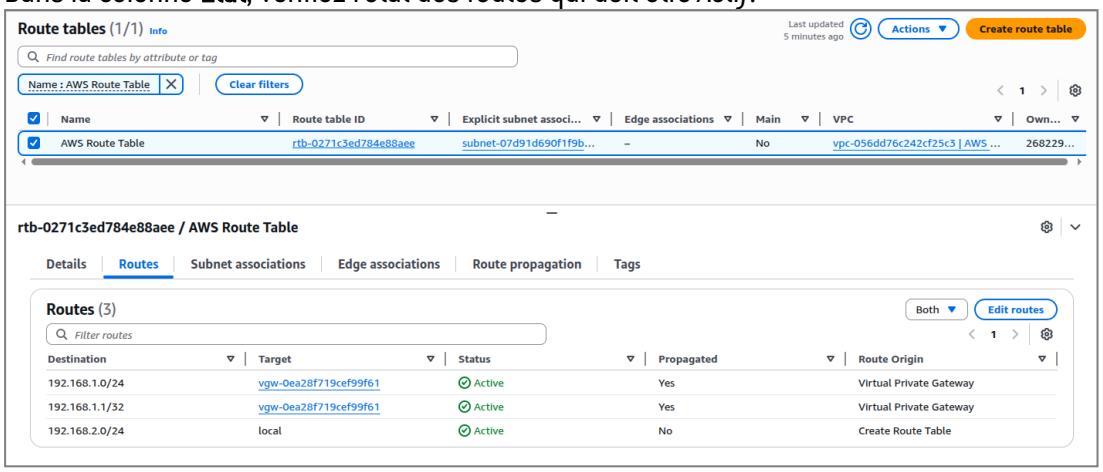
```
show route export <proto>
```

```
bird> show route export aws_1
Table master4:
192.168.1.1/32       unicast [kernel1 09:33:05.242] * (10)
       dev lo0(loopback)
192.168.1.0/24       unicast [kernel1 09:33:05.242] * (10)
       dev vtnet1(in)
bird> show route export aws_2
Table master4:
192.168.1.1/32       unicast [kernel1 09:33:05.242] * (10)
       dev lo0(loopback)
192.168.1.0/24       unicast [kernel1 09:33:05.242] * (10)
       dev vtnet1(in)
```

Vérifier l'état des routes sur la console AWS

1. Rendez-vous dans **VPC** > **Cloud privé virtuel** > **Tables de routage**.
2. Sélectionnez la ressource dans la liste (*AWS Route Table* dans l'exemple).
3. Cliquez sur l'onglet **Routes**.

4. Dans la colonne **État**, vérifiez l'état des routes qui doit être *Actif*.



Pour aller plus loin

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

Pour plus d'informations, reportez-vous à :

- La documentation AWS :
  - Documentation AWS Virtual Private Network
  - Documentation Amazon Virtual Private Cloud
- Les notes techniques suivantes :
  - Interfaces virtuelles IPsec
  - Routage dynamique BIRD v2

documentation@stormshield.eu

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

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.