NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

INTERFACES VIRTUELLES IPSEC

Produits concernés : SNS 2.1 et versions supérieures, SNS 3.x, SNS 4.x

Date : 09 décembre 2019

Référence : sns-fr-interfaces_virtuelles_ipsec_note_technique

Table des matières

Avant de commencer

La version de firmware 2.x des Firewalls Stormshield Network offre la possibilité de mettre en œuvre des tunnels VPN IPsec routés. Ce ne sont plus les informations définies dans la Security Policy Database (SPD) mais les instructions de routage (routage statique, dynamique ou routage défini par le filtrage) qui déterminent si les paquets doivent transiter par ce tunnel IPSec.

Dans la définition d'un tunnel IPSec routé, des interfaces virtuelles jouent le rôle d'extrémités de trafic. Il n'est donc plus nécessaire de préciser les réseaux distants dans la politique IPSec.

L'utilisation combinée d'objets routeurs dans les règles de filtrage et de tunnels routés permet alors de mettre en œuvre différents types de configurations.

Basculement (Failover)

En cas de perte de lien, les flux (chiffrés ou non) passant par un réseau MPLS par exemple, peuvent maintenant être redirigés vers un tunnel VPN de secours, monté entre les sites via un accès Internet.

Load-Balancing

Les objets routeurs permettent notamment d'implémenter le partage de charge sur plusieurs passerelles d'accès à Internet. Une répartition de charge par type de flux peut également être mise en œuvre, à l'aide d'instructions de routage des paquets vers des tunnels IPSec différenciés.

Qualité de Service (QoS)

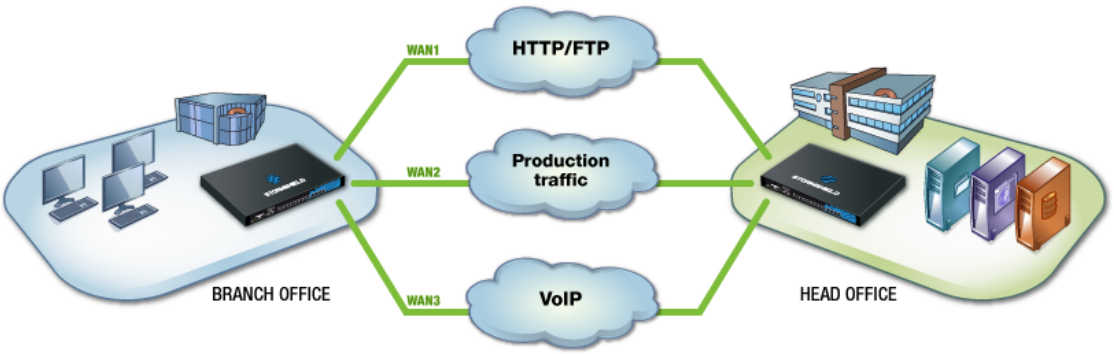
La valeur du champ DSCP (Differentiated Services Code Point) affecté aux paquets IP permet de les diriger vers des tunnels IPSec différenciés en fonction des instructions de routage définies.

Sécurisation d'un trafic non chiffré

Un trafic non chiffré (exemple : HTTP) peut ainsi être sécurisé en empruntant un tunnel IPsec basé sur le routage, tandis que le trafic chiffré (HTTPS) à destination du même serveur n'emprunte pas de tunnel.

Architecture présentée

Ce document décrit les étapes de configuration nécessaires pour réaliser l'architecture suivante:



Présentation générale

Une entreprise dispose de deux sites reliés par 3 routeurs d'accès. L'agence, composée exclusivement de postes clients, accède ainsi à des ressources serveur hébergées sur le siège:

- Accès à des portails Web de type intranet et transferts de fichiers via FTP,
- Utilisation d'applications dites « de production » (exemple : accès à des serveurs de bases de données SQL),
- Communications en voix sur IP via les serveurs PBX du siège.

L'entreprise souhaite sécuriser ces trois types de flux grâce à du chiffrement dans des tunnels IPSec. Elle choisit également de mettre en œuvre de la redondance entre les 3 liens afin d'assurer une continuité de service pour les flux « de production » et la VoIP.

Présentation détaillée

Dans l'architecture présentée, les flux entre les postes clients de l'agence et les serveurs sur le siège distant sont répartis sur plusieurs liens selon leur nature. Ces liens sont portés par des interfaces externes (non protégées) sur les deux Firewalls (chacune de ces interfaces bénéficie d'une adresse IP dédiée). La répartition des flux est réalisée grâce aux directives de routage précisées dans les règles de filtrage (Policy Based Routing) :

- les flux HTTP et FTP transitent par le lien nommé WAN1,
- les flux dits « de production » empruntent le lien nommé WAN2,
- le lien nommé WAN3 est utilisé pour les flux de Voix sur IP.

Paramétrage du Firewall protégeant les clients

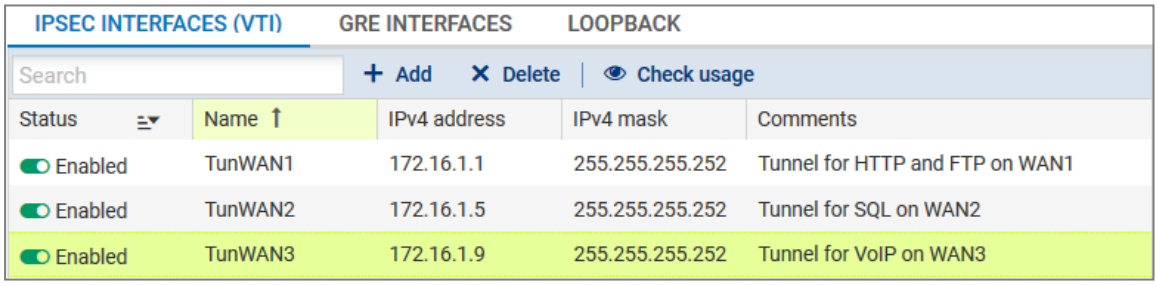
Les tunnels dans lesquels transitent les différents flux sont définis par des interfaces virtuelles IPSec.

Il est donc nécessaire de créer trois interfaces virtuelles locales qui permettront d'établir trois tunnels IPSec distincts. Dans l'exemple, ces interfaces sont nommées **TunWAN1**, **TunWAN2** et **TunWAN3** (les interfaces distantes associées seront respectivement nommées **RemoteTunWAN1**, **RemoteTunWAN2** et **RemoteTunWAN3**).

Création des interfaces virtuelles locales

Sélectionnez l'onglet *Interfaces IPSec* du module **Configuration** > **Réseau** > **Interfaces virtuelles**. Cliquez sur Ajouter afin de créer la première interface virtuelle. Trois champs doivent obligatoirement être renseignés :

- **Nom** : précisez le nom de l'interface virtuelle créée (**TunWAN1** dans l'exemple),
- **Adresse IP** : indiquez l'adresse IP attribuée à l'interface (172.16.1.1 dans l'exemple),
- **Masque réseau** : la valeur proposée par défaut est un masque de type 255.255.255.252 permettant de définir une adresse pour l'interface virtuelle locale, et une adresse pour l'interface virtuelle distante. Dans cet exemple, le masque est laissé à sa valeur par défaut. L'adresse IP de l'interface virtuelle distante associée sera donc 172.16.1.2.



Répétez cette opération pour définir les interfaces **TunWAN2** (adresse IP / masque : 172.16.1.5 / 255.255.255.252) et **TunWAN3** (adresse IP / masque : 172.16.1.9 / 255.255.255.252).

Définition des interfaces virtuelles distantes

Les interfaces virtuelles du Firewall distant sont définies à l'aide d'objets réseaux. Elles seront utilisés comme passerelles au sein des routeurs et serviront à la définition des tunnels IPSec.

Dans l'exemple présenté, les interfaces distantes sont nommées **RemoteTunWAN1**, **RemoteTunWAN2** et **RemoteTunWAN3**.

Pour créer l'objet correspondant à la première interface virtuelle du Firewall distant, allez dans le module **Configuration** > **Objets** > **Objets réseau**, puis cliquez sur le bouton **Ajouter** et sur l'icône **Machine** du bandeau supérieur.

Attribuez un nom à l'objet (**RemoteTunWAN1** dans cet exemple) et indiquez l'adresse IP associée. Pour cet objet, il s'agira d'indiquer l'adresse IP de l'interface IPSec associée au lien WAN1 du Firewall distant, soit 172.16.1.2 dans l'exemple. Validez pour créer l'objet.

En suivant la même méthode, créez les objets **RemoteTunWAN2** (172.16.1.6) et **RemoteTunWAN3** (172.16.1.10).

Création des tunnels IPSec

Un tunnel IPSec porté par des interfaces virtuelles présente la particularité d'utiliser ces interfaces locale et distante comme extrémités de trafic. Le correspondant IPSec est défini de manière classique par son adresse IP publique.

- Dans le module **VPN IPSec**, créez un nouveau tunnel en cliquant sur **Ajouter** puis en sélectionnant **Tunnel site à site**.
- Pour le champ **Réseau local**, sélectionnez l'interface virtuelle locale **Firewall_TunWAN1.**
- Pour le champ **Réseau distant,** sélectionnez l'objet **RemoteTunWAN1**.

Créez (ou sélectionnez le s'il existe déjà) un correspondant, dont la passerelle distante sera un objet représentant l'adresse IP publique dédiée au lien WAN1 du Firewall distant.
Notez que la version du protocole IKE devra être la même pour l'ensemble des correspondants utilisés au sein de la politique VPN IPsec.

En suivant la même méthode, créez les deux autres tunnels avec les valeurs suivantes :

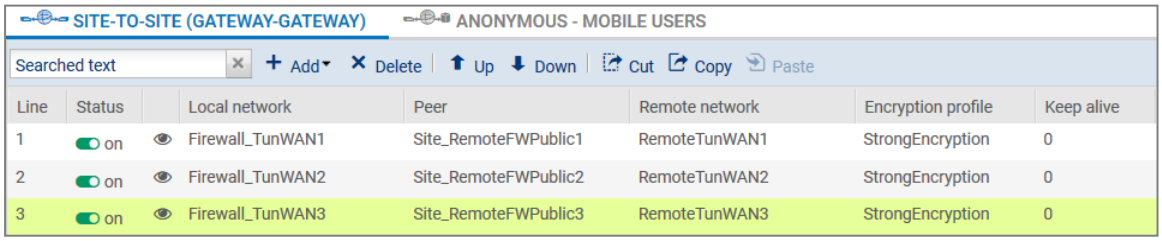
Tunnel pour le lien WAN2 :

- **Réseau local** : interface virtuelle **Firewall_TunWAN2**,
- **Réseau distant** : objet **RemoteTunWAN2**,
- **Passerelle du correspondant** : objet machine portant l'adresse IP publique dédiée au lien WAN2 du Firewall distant.

Tunnel pour le lien WAN3 :

- **Réseau local** : interface virtuelle **Firewall_TunWAN3**,
- **Réseau distant** : objet **RemoteTunWAN3**,
- **Passerelle du correspondant** : objet machine portant l'adresse IP publique dédiée au lien WAN3 du Firewall distant.

La politique VPN IPSec prendra donc la forme suivante :



Création des objets routeurs

L'utilisation d'objets routeurs permet d'assurer la notion de redondance entre les liens WAN. En effet, ces routeurs sont composés de différentes passerelles qui peuvent être définies comme actives ou de secours.

Les tests de disponibilité de ces passerelles consistent en une série de requêtes ICMP (Ping). Ils sont effectués à intervalle régulier (paramètre « frequency» - exprimé en secondes).

Après avoir émis une requête vers une passerelle, le firewall attend la réponse de celle-ci pendant un laps de temps défini (paramètre « wait » - exprimé en secondes). En cas d'absence de réponse, il émet de nouveau une requête, et ce jusqu'au nombre maximum d'essais infructueux

déterminé (paramètre « tries »). Après avoir atteint ce nombre d'essais, et si aucune réponse n'a été reçue, le firewall considère alors la passerelle comme injoignable. Une ou plusieurs passerelles de secours deviennent alors passerelle(s) principale(s).

Les paramètres « frequency », « wait » et « tries » sont exclusivement paramétrables via une commande CLI :

```
CONFIG OBJECT ROUTER NEW name=<router name> [tries=<int>] [wait=<seconds>]
[frequency=<seconds>] update=1.
```

Les valeurs recommandées pour ces paramètres sont les suivantes :

- « frequency » : 15 (secondes),
- « wait » : 2 (secondes),
- « tries » : 3.

Dans la configuration présentée, il est nécessaire de créer trois objets routeurs :

- Le premier (**HTTPRouter** dans l'exemple) est utilisé pour le transport des flux HTTP/FTP sur le lien WAN1, sans redondance,
- Le second (**ProductionRouter**) permet de garantir la redondance des flux de production du lien WAN2 vers les deux autres liens WAN1 et WAN3,
- Le troisième (**VoIPRouter**) assure le report des flux du lien WAN3 vers le lien WAN2.

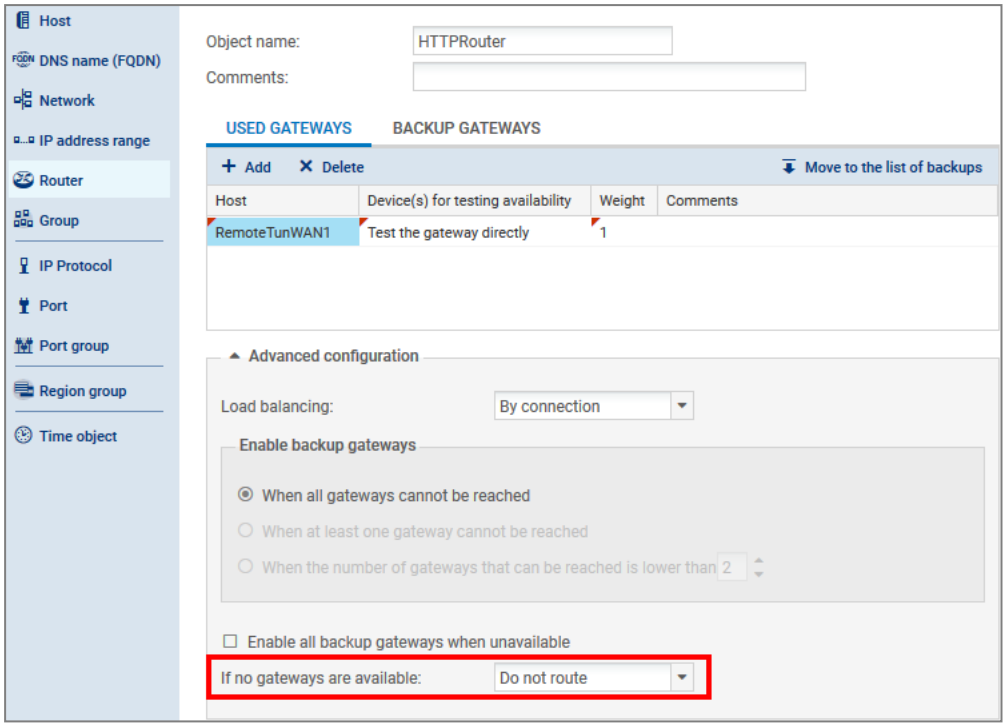
IMPORTANT

Pour des configurations de tunnel IPSec routés, les routes définies au sein des règles de filtrage doivent impérativement utiliser des passerelles distantes. Les objets routeurs utilisés dans cet exemple seront donc basés sur les interfaces virtuelles IPSec distantes.

Routeur pour les flux HTTP/FTP

Dans le menu **Configuration** > **Objets** > **Objets réseau**, cliquez sur **Ajouter** puis sur l'icône **Routeur** du bandeau supérieur.

- Renseignez le nom de l'objet (**HTTPRouter** dans l'exemple),
- Dans la liste des passerelles utilisées, sélectionnez le routeur distant associé au lien WAN1 (objet **RemoteTunWAN1** dans cet exemple),
- Dans la Configuration avancée de l'objet, sélectionnez l'option **Ne pas router** pour le champ **Si aucune passerelle n'est disponible**. De cette manière, en cas de défaillance du lien WAN1, les flux HTTP/FTP ne seront pas pris en charge par les directives de routage définies par défaut. Ces flux seront alors simplement ignorés par le Firewall.



Cliquez sur **Créer et dupliquer** afin de valider cette configuration.

Routeur pour les flux de production

- Renseignez le nom de l'objet (**ProductionRouter** dans l'exemple),
- Dans la liste des passerelles utilisées, sélectionnez l'interface IPSec distante associée au le lien WAN2, c'est à dire l'objet **RemoteTunWAN2** dans cet exemple,
- Dans la liste des passerelles de secours, ajoutez les deux interfaces IPSec distantes susceptibles de recevoir les flux de production en cas d'indisponibilité du lien WAN2, à savoir **RemoteTunWAN1** et **RemoteTunWAN3,**
- Dans la configuration avancée de l'objet, cochez la case **Activer toutes les passerelles de secours en cas d'indisponibilité** : les deux passerelles de secours **RemoteTunWAN1** et **RemoteTunWAN3** seront alors simultanément activées en cas d'indisponibilité du lien principal WAN2:

> **NOTE**
>
> Si un poids différent est affecté aux deux passerelles de secours, une répartition de charge des nouvelles connexions établies est appliquée en cas de défaillance de la passerelle principale.
>
> **Exemple** :
>
> Un poids de 50 est affecté à la passerelle **RemoteTunWAN1**.
>
> Un poids de 10 est affecté à la passerelle **RemoteTunWAN3**.
>
> Lorsque ces deux passerelles deviendront actives, la passerelle **RemoteTunWAN1** supportera 50/(50+10)=83% des connexions. Les 17% restants des connexions seront prises en charge par la passerelle **RemoteTunWAN3**.

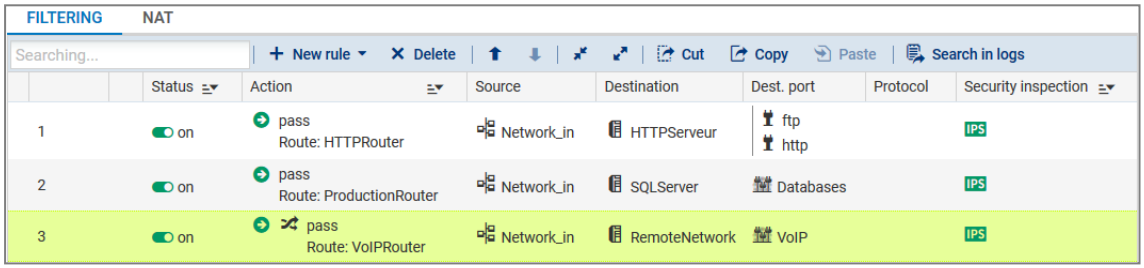
Routeur pour les flux de VoIP

Dans le menu **Configuration** > **Objets** > **Objets réseau**, cliquez sur **Ajouter** puis sur l'icône **Routeur** du bandeau supérieur.

- Renseignez le nom de l'objet (**VoIPRouter** dans l'exemple).
- Dans la liste des passerelles utilisées, sélectionnez le routeur distant supportant le lien WAN3, (objet **RemoteTunWAN3** dans l'exemple):
- Dans la liste des passerelles de secours, ajoutez la passerelle susceptible de recevoir les flux de VoIP en cas d'indisponibilité du lien WAN3 (objet **RemoteTunWAN2** dans l'exemple):

Règles de filtrage

Trois règles de routage basé sur le filtrage (PBR) sont nécessaires afin de faire transiter les flux au travers de leurs tunnels IPSec respectifs.



- la première règle autorise les flux HTTP et FTP depuis le réseau interne à destination du serveur (objet **HTTPServeur** dans l'exemple). Ces flux empruntent le routeur **HTTPRouter** (lien WAN1),
- la seconde autorise les flux dits de production (connexions SQL dans l'exemple) depuis le réseau interne vers le serveur (objet **SQLServer** dans l'exemple). Ces flux sont dirigés vers la passerelle **ProductionRouter** (lien WAN2),
- la troisième est dédiée aux flux de VoIP depuis le réseau interne vers le réseau distant. Ces flux empruntent le routeur **VoIPRouter** (lien WAN3).

Le routage vers le réseau des serveurs étant réalisé au sein des règles de filtrage, il n'est donc pas nécessaire de créer de route statique.

Règle pour les flux HTTP et FTP via le lien WAN1

Ajoutez une règle en reprenant les éléments suivants :

Action (onglet général)

Dans le champ **Action**, sélectionnez la valeur **Passer**. Dans le champ **Routage**, sélectionnez l'objet routeur **HTTPRouter**

Source (onglet général)

Dans le champ **Machines sources**, sélectionnez la machine, le groupe de machines ou le réseau autorisés à établir des connexions HTTP et FTP vers le serveur. Dans l'exemple, l'objet sélectionné est **Network_in**

Destination (onglet *général*)

Dans le champ **Machines destination** , sélectionnez la machine ou le groupe de machines hébergeant les services HTTP et FTP. Dans l'exemple, l'objet sélectionné est **HTTPServer**

Port – Protocole

Sélectionnez les objets correspondant aux ports autorisés. Dans l'exemple, HTTP et FTP ont été sélectionnés.

Règle pour les flux de production via le lien WAN2

Ajoutez une règle en reprenant les éléments suivants :

Action (onglet *général*)

Dans le champ **Action**, sélectionnez la valeur **Passer**. Dans le champ **Routage**, sélectionnez l'objet routeur **ProductionRouter.**

Source (onglet *général*)

Dans le champ **Machines sources**, sélectionnez la machine, le groupe de machines ou le réseau autorisés à établir des connexions vers le(s) serveur(s) de production. Dans l'exemple, l'objet sélectionné est **Network_in**.

Destination (onglet *général*)

Dans le champ **Machines destination**, sélectionnez la machine ou le groupe de machines hébergeant les services de production. Dans l'exemple, l'objet sélectionné est **SQLServer**.

Port – Protocole

Sélectionnez les objets correspondant aux ports autorisés. Dans l'exemple, il s'agit d'un groupe **Databases** comprenant différents ports de connexion aux bases de données SQL (PostgreSQL, MySQL,etc.).

Règle pour les flux de VoIP via le lien WAN3

Créez une règle de filtrage reprenant les éléments suivants :

Action (onglet *général*)

Dans le champ **Action**, sélectionnez la valeur **Passer**. Dans le champ **Routage**, sélectionnez l'objet routeur **VoIPRouter**

Action (onglet *Qualité de service*)

Il est possible de forcer le champ DSCP des paquets. Pour ce faire, cochez la case **Forcer la valeur** et dans le champ **Nouvelle valeur DSCP**, vous pouvez fixer un champ DSCP personnalisé (*18 Classe 2 or* dans l'exemple).

Source (onglet *général*)

Dans le champ **Machines sources**, sélectionnez la machine, le groupe de machines ou le réseau autorisés à établir des connexions vers le(s) serveur(s) de production. Dans l'exemple, l'objet sélectionné est Network_in.

Destination (onglet *général*)

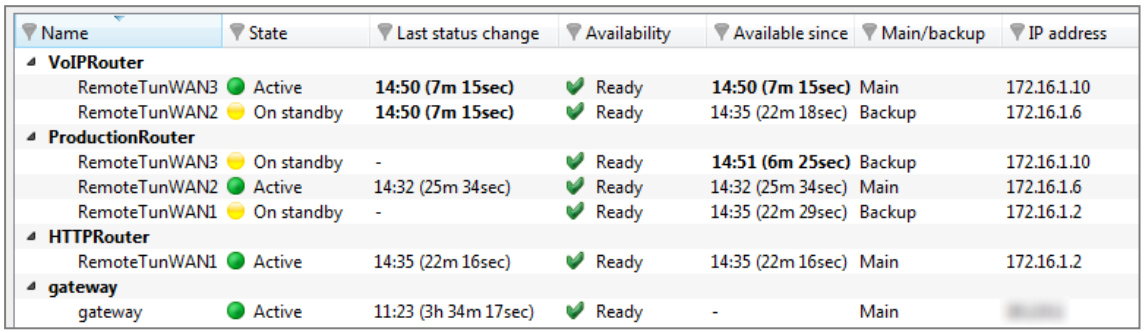
Dans le champ **Machines destination**, sélectionnez la machine, le groupe de machines ou le réseau avec lequel des connexions seront établies. Dans l'exemple, l'objet sélectionné est **RemoteNetwork**.

Port – Protocole

Sélectionnez les objets correspondant aux ports autorisés. Dans l'exemple, il s'agit d'un groupe **VoIP** comprenant différents ports nécessaire à la VoIP.

Vérification de l'état des routeurs

Le module **Routeurs** de Stormshield Network Real-Time Monitor affiche l'état de la passerelle par défaut et des passerelles composant chaque routeur utilisé dans la configuration du Firewall :



Name	State	Last status change	Availability	Available since	Main/backup	IP address
VoIPRouter						
RemoteTunWAN3	Active	**14:50 (7m 15sec)**	Ready	**14:50 (7m 15sec)**	Main	172.16.1.10
RemoteTunWAN2	On standby	**14:50 (7m 15sec)**	Ready	14:35 (22m 18sec)	Backup	172.16.1.6
ProductionRouter						
RemoteTunWAN3	On standby	-	Ready	**14:51 (6m 25sec)**	Backup	172.16.1.10
RemoteTunWAN2	Active	14:32 (25m 34sec)	Ready	14:32 (25m 34sec)	Main	172.16.1.6
RemoteTunWAN1	On standby	-	Ready	14:35 (22m 29sec)	Backup	172.16.1.2
HTTPRouter						
RemoteTunWAN1	Active	14:35 (22m 16sec)	Ready	14:35 (22m 16sec)	Main	172.16.1.2
gateway						
gateway	Active	11:23 (3h 34m 17sec)	Ready	-	Main	

Les informations affichées sont les suivantes :

- **Nom :** nom donné au routeur ou à la passerelle dans la configuration du Firewall.
- **État** : État de la passerelle. Les trois valeurs possibles sont : **Actif** (passerelle utilisée), **En veille** (passerelle de secours) ou **Non joignable** (les tests de disponibilité vers cette passerelle ont échoué).
- **Dernier changement d'état :** date du dernier changement d'état de la passerelle (exemple: passage de l'état **En veille** à l'état **Actif**). La durée écoulée depuis ce changement d'état est également précisée entre parenthèses.
- **Disponibilité :** il s'agit du résultat du dernier test de disponibilité. Les valeurs possibles sont **Prête** (passerelle opérationnelle) ou **Non disponible** (la passerelle n'a pas répondu).
- **Disponible depuis:** date depuis laquelle la passerelle est disponible. La durée écoulée depuis le premier test de disponibilité réalisé avec succès est également précisée entre parenthèses.
- **Principal/secours :** il s'agit du rôle par défaut de la passerelle au sein du routeur. Les valeurs sont **Principal** ou **Secours**.
- **Adresse IP :** adresse IP de la passerelle.
- **Répartition :** dans le cas d'une répartition de charge, il s'agit du taux d'utilisation de la passerelle au sein du routeur (pourcentage).

Paramétrage du Firewall protégeant les serveurs

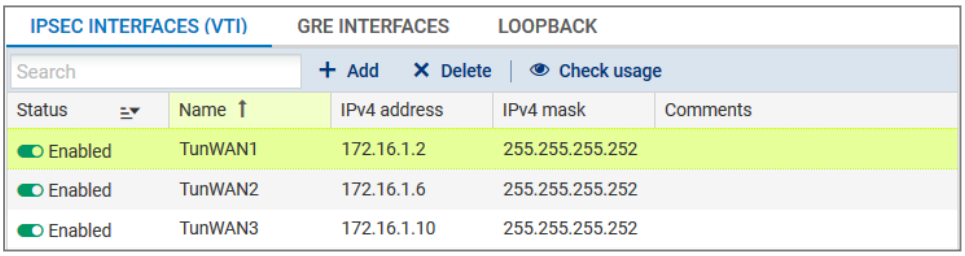
Les tunnels dans lesquels transitent les différents flux sont définis par des interfaces virtuelles IPSec.

Il est donc nécessaire de créer trois interfaces virtuelles locales qui permettront d'établir trois tunnels IPSec distincts. Dans l'exemple, ces interfaces sont nommées **TunWAN1**, **TunWAN2** et **TunWAN3** (les interfaces distantes associées seront respectivement nommées **RemoteTunWAN1**, **RemoteTunWAN2** et **RemoteTunWAN3**).

Création des interfaces virtuelles locales

En suivant la méthode décrite pour le Firewall protégeant les postes clients, définissez les 3 interfaces virtuelles locales. Afin de respecter le masque réseau choisi dans l'exemple, ces interfaces porteront les adresses IP suivantes :

- Interface **TunWAN1** : 172.16.1.2 (masque 255.255.255.252),
- Interface **TunWAN2** : 172.16.1.6 (masque 255.255.255.252),
- Interface **TunWAN3** : 172.16.1.10 (masque 255.255.255.252).



Définition des interfaces virtuelles distantes

En suivant la méthode décrite pour le Firewall protégeant les postes clients, définissez les 3 interfaces virtuelles distantes. S'agissant des interfaces virtuelles locales du Firewall côté clients, les adresses IP à utiliser sont donc les suivantes :

- Interface **RemoteTunWAN1** : 172.16.1.1,
- Interface **RemoteTunWAN2** : 172.16.1.5,
- Interface **RemoteTunWAN3** : 172.16.1.9.

Création des tunnels IPSec

En suivant la méthode décrite pour configurer les tunnels IPSec sur le Firewall protégeant les postes clients, définissez les 3 tunnels IPSec à l'aide des valeurs suivantes :

Tunnel sur le lien WAN1 :

- **Réseau local** : sélectionnez l'interface virtuelle locale **Firewall_TunWAN1**,
- **Réseau distant** : sélectionnez l'objet **RemoteTunWAN1**,
- Créez (ou sélectionnez le s'il existe déjà) un correspondant dont la passerelle distante sera un objet représentant l'adresse IP publique dédiée au lien WAN1 du Firewall distant. La version du protocole IKE doit être identique à celle utilisée sur le Firewall protégeant les clients.

Tunnel sur le lien WAN2 :

- **Réseau local** : interface virtuelle **Firewall_TunWAN2**,
- **Réseau distant** : objet **RemoteTunWAN2**,
- **Passerelle du correspondant** : objet machine portant l'adresse IP publique dédiée au lien WAN2 du Firewall distant.

Tunnel sur le lien WAN3 :

- **Réseau local** : interface virtuelle **Firewall_TunWAN3**,
- **Réseau distant** : objet **RemoteTunWAN3**,
- **Passerelle du correspondant** : Objet machine portant l'adresse IP publique dédiée au lien WAN3 du Firewall distant.

Routes de retour

Lorsque le Firewall protégeant les serveurs reçoit des flux provenant d'une interface virtuelle distante, il ne connaît pas la route permettant de diriger correctement les paquets retour. Il faut donc créer sur ce Firewall les 3 routes de retour correspondant aux trois interfaces IPSec distantes.

Dans l'onglet *Routes de retour* du module **Configuration** > **Réseau** > **Routage**, cliquez sur le bouton **Ajouter** et remplissez les champs comme suit pour le lien WAN1:

- **Etat** : **Activé**,
- **Passerelle** : sélectionnez (ou créez directement depuis ce champ) l'objet correspondant à la première interface virtuelle distante (**RemoteTunWAN1** dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle IPSec locale associée (**TunWAN1** dans l'exemple),
- **Commentaire** : vous pouvez ajouter un texte libre précisant le rôle de cette route.

Cliquez sur **Appliquer** pour activer cette route de retour.

Procédez de même pour créer les flux empruntant les liens WAN2 et WAN3 avec les valeurs suivantes :

Pour le lien WAN2

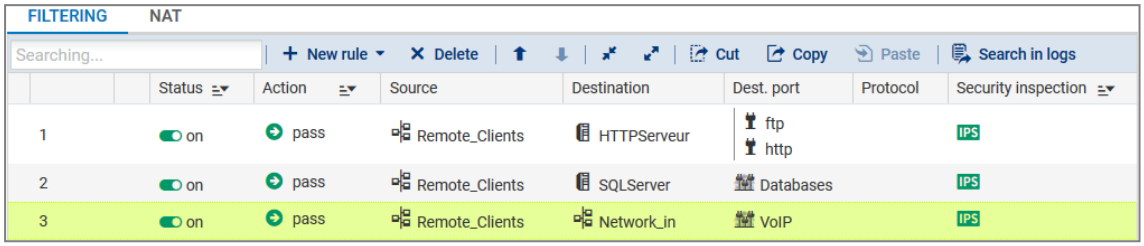
- **Etat** : **Activé**,
- **Passerelle** : objet **RemoteTunWAN2**,
- **Interface** : objet **TunWAN2**.

Pour le lien WAN3

- **Etat** : **Activé**
- **Passerelle** : objet **RemoteTunWAN3**,
- **Interface** : objet **TunWAN3**.

Règles de filtrage

Créez les trois règles nécessaires pour autoriser les différents flux autorisés vers le réseau local:



Règle pour les flux HTTP et FTP

Ajoutez une règle en reprenant les éléments suivants :

Action (onglet *général*)

Dans le champ **Action**, sélectionnez la valeur **Passer**

Source (onglet *général*)

Dans le champ **Machines sources**, sélectionnez la machine, le groupe de machines ou le réseau autorisés à établir des connexions HTTP et FTP vers le serveur. Dans l'exemple, l'objet sélectionné est le réseau **Remote_clients**.

Destination (onglet *général*)

Dans le champ **Machines destination** , sélectionnez la machine ou le groupe de machines hébergeant les services HTTP et FTP. Dans l'exemple, l'objet sélectionné est **HTTPServer.**

Port – Protocole

Sélectionnez les objets correspondant aux ports autorisés. Dans l'exemple, **HTTP** et **FTP** ont été sélectionnés.

Règle pour les flux de production via le lien WAN2

Ajoutez une règle en reprenant les éléments suivants :

Action (onglet *général*)

Dans le champ **Action**, sélectionnez la valeur **Passer.**

Source (onglet général)

Dans le champ **Machines sources**, sélectionnez la machine, le groupe de machines ou le réseau autorisés à établir des connexions vers le(s) serveur(s) de production. Dans l'exemple, l'objet sélectionné est le réseau **Remote_clients**.

Destination (onglet *général*)

Dans le champ **Machines destination**, sélectionnez la machine ou le groupe de machines hébergeant les services de production. Dans l'exemple, l'objet sélectionné est **SQLServer**.

Port – Protocole

Sélectionnez les objets correspondant aux ports autorisés. Dans l'exemple, il s'agit d'un groupe **Databases** comprenant différents ports de connexion aux bases de données SQL (PostgreSQL, MySQL,etc.).

Règle pour les flux de VoIP

Créez une règle de filtrage reprenant les éléments suivants :

Action (onglet *général*)

Dans le champ Action, sélectionnez la valeur **Passer**

Source (onglet *général*)

Dans le champ **Machines sources**, sélectionnez la machine, le groupe de machines ou le réseau autorisés à établir des connexions vers le(s) serveur(s) de production. Dans l'exemple, l'objet sélectionné est **Remote_clients**.

Destination (onglet *général*)

Dans le champ **Machines destination**, sélectionnez la machine, le groupe de machines ou le réseau avec lequel des connexions seront établies. Dans l'exemple, l'objet sélectionné est **Network_in**.

Port – Protocole

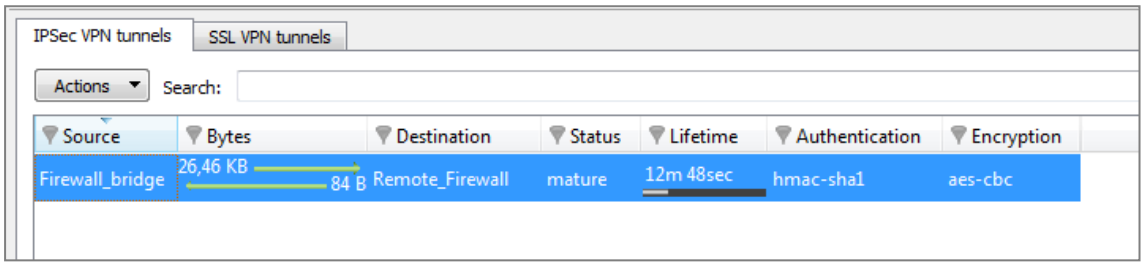
Sélectionnez les objets correspondant aux ports autorisés. Dans l'exemple, il s'agit d'un groupe **VoIP** comprenant différents ports nécessaire à la VoIP.

La configuration du firewall protégeant les postes clients est à présent terminée. Nous allons vérifier que cette configuration est opérationnelle.

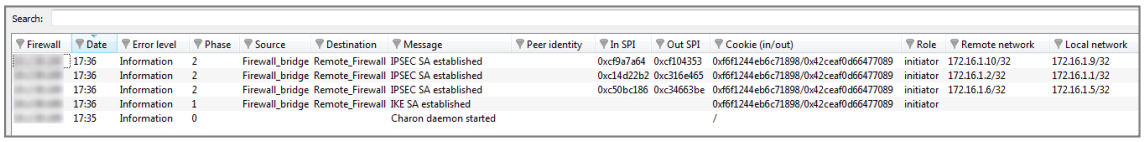
Vérification des tunnels

Vérification depuis SN Real-Time Monitor

Lorsque des connexions empruntant les liens WAN sont établies, l'état des tunnels correspondants peut être visualisé dans l'onglet *Tunnels VPN IPSec* du module **Tunnels VPN** :



Les traces concernant l'établissement des différents tunnels peuvent être consultées dans le module **Traces** > **VPN**:



Vérification depuis l'interface Web des Firewalls

Depuis l'interface d'administration Web du Firewall, accédez au module **Monitoring** > **Logs - Journaux d'audit** (vue VPN / logs VPN IPsec) afin de vérifier le fonctionnement de la configuration mise en place.

Basculement vers un lien de secours

Lorsqu'un lien WAN est défaillant, la passerelle distante correspondante est alors injoignable. La ou les passerelles de secours définies dans le routeur dédié à ce lien WAN deviennent alors actives. Ce changement d'état peut être visualisé dans le module **Routeurs** de SN Real-Time Monitor. L'exemple décrit ci-dessous détaille le comportement du routeur **ProductionRouter** en cas de défaillance du lien WAN2.

Tous les liens WAN sont opérationnels

Name	State	Last status change	Availability	Available since	Main/backup	IP address
VoIPRouter						
RemoteTunWAN3	Active	**14:50 (7m 15sec)**	Ready	**14:50 (7m 15sec)**	Main	172.16.1.10
RemoteTunWAN2	On standby	**14:50 (7m 15sec)**	Ready	14:35 (22m 18sec)	Backup	172.16.1.6
ProductionRouter						
RemoteTunWAN3	On standby	-	Ready	**14:51 (6m 25sec)**	Backup	172.16.1.10
RemoteTunWAN2	Active	14:32 (25m 34sec)	Ready	14:32 (25m 34sec)	Main	172.16.1.6
RemoteTunWAN1	On standby	-	Ready	14:35 (22m 29sec)	Backup	172.16.1.2
HTTPRouter						
RemoteTunWAN1	Active	14:35 (22m 16sec)	Ready	14:35 (22m 16sec)	Main	172.16.1.2
gateway						
gateway	Active	11:23 (3h 34m 17sec)	Ready	-	Main	[illegible]

Conformément à la définition des routeurs décrite dans le paragraphe Création des objets routeurs, SN Real-Time Monitor laisse apparaître que les flux de production doivent emprunter le lien WAN2 (passerelle principale: **RemoteTunWAN2**). En cas de défaillance de ce lien, ces flux doivent alors être répartis sur les liens WAN1 et WAN3 (passerelles de secours: **RemoteTunWAN1** et **RemoteTunWAN3**).

Le lien WAN2 est défectueux

Name	State	Last status change	Availability	Available since	Main/backup	IP address
VoIPRouter						
RemoteTunWAN3	Active	-	Ready	-	Main	172.16.1.10
RemoteTunWAN2	Unreachable	-	Unavailable	-	Backup	172.16.1.6
ProductionRouter						
RemoteTunWAN3	Active	-	Ready	-	Backup	172.16.1.10
RemoteTunWAN2	Unreachable	-	Unavailable	-	Main	172.16.1.6
RemoteTunWAN1	Active	-	Ready	-	Backup	172.16.1.2
HTTPRouter						
RemoteTunWAN1	Active	-	Ready	-	Main	172.16.1.2
gateway						
gateway	Active	-	Ready	-	Main	[illegible]

Dans l'illustration ci-dessus, le lien WAN2 n'est plus opérationnel. La passerelle **RemoteTunWAN2** apparaît alors comme injoignable et donc non disponible. Pour le routeur **ProductionRouter**, les deux passerelles **RemoteTunWAN1** et **RemoteTunWAN3** sont devenues actives et les flux de production empruntent alors les tunnels portés par les liens WAN1 et WAN3.

Résolution d'incidents - Erreurs communes

Dans la suite de cette section, le Firewall protégeant les clients (à l'initiative de l'établissement des tunnels) est appelé *initiator.* Le Firewall distant est appelé *responder*.

Symptôme: Le tunnel ne s'établit pas.

- Un message "Remote seems to be dead " en phase 1 est présent dans le module **Traces** > **VPN** de SN Real-Time Monitor pour le Firewall "initiator".
- Aucun message n'apparaît dans le module **Traces** > **VPN** de SN Real-Time Monitor pour le Firewall "responder".

Solutions: vérifiez que:

- les interfaces physiques sur lesquelles repose le lien WAN correspondant sont bien disponibles,
- les interfaces IPSec virtuelles définissant le tunnel sont bien activées,
- la règle de filtrage correspondant au flux devant emprunter ce tunnel est correctement définie et que le routeur utilisé dans cette règle repose sur les bonnes interfaces virtuelles.

Symptôme: Le tunnel ne s'établit pas.

- Un message "IKE SA establishment failed: received AUTHENTICATION_FAILED notify error" en phase 1 est présent dans le module **Traces** > **VPN** de SN Real-Time Monitor pour le Firewall *initiator*.
- Un message "Tried 1 shared key but MAC mismatched" en phase 1 est présent dans le module **Traces** > **VPN** de SN Real-Time Monitor pour le Firewall *responder*.

Solution: la clé pré-partagée (paramètres du correspondant) est différente sur les Firewalls *initiator* et *responder*.

Symptôme: Le tunnel ne s'établit pas.

- Un message "Invalid major version X" est présent dans le module **Traces** > **VPN** de SN Real-Time Monitor pour le Firewall *initiator*.
- Un message "Invalid major version Y" est présent dans le module **Traces** > **VPN** de SN Real-Time Monitor pour le Firewall *responder*.

Solution: la version du protocole IKE (paramètres du correspondant) est différente sur les Firewalls *initiator* et *responder*.

documentation@stormshield.eu