NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

ENCAPSULATION NIVEAU 2

Produits concernés : SNS 2.3 et supérieures, SNS 3.x

Date : 21 avril 2021

Référence : sns-fr-encapsulation_niveau_2_note_technique

Table des matières

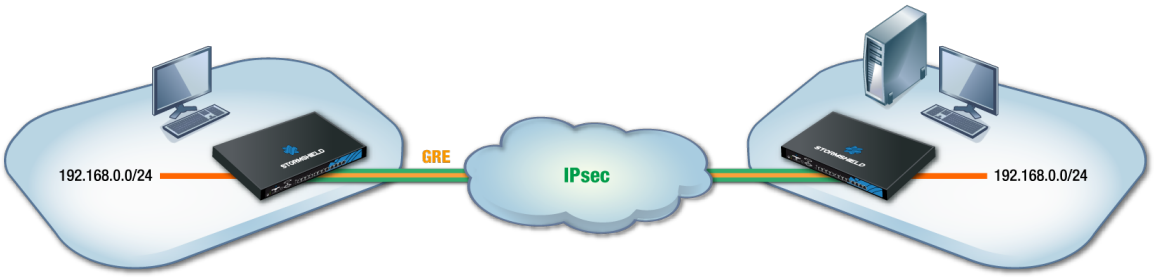
Introduction

Depuis la version de firmware 2.x, les Firewalls Stormshield Network peuvent encapsuler des flux de niveau 2 dans des tunnels GRE (Generic Routing Encapsulation) basés sur des interfaces GRETAP. Les tunnels GRE n'étant pas chiffrés nativement, il est possible de sécuriser les échanges en faisant transiter les flux GRE au travers d'IPSec.

L'utilisation de tunnels GRE basés sur des interfaces GRETAP permet par exemple de relier au travers d'un bridge des sites présentant le même plan d'adressage. Des services de type DHCP peuvent ainsi être partagés entre les deux sites. Ce type de tunnel permet également de transporter entre deux sites des VLAN identifiés et déclarés explicitement sur les firewalls.

Architectures présentées

Cas 1 : réunion de deux sites partageant le même plan d'adressage

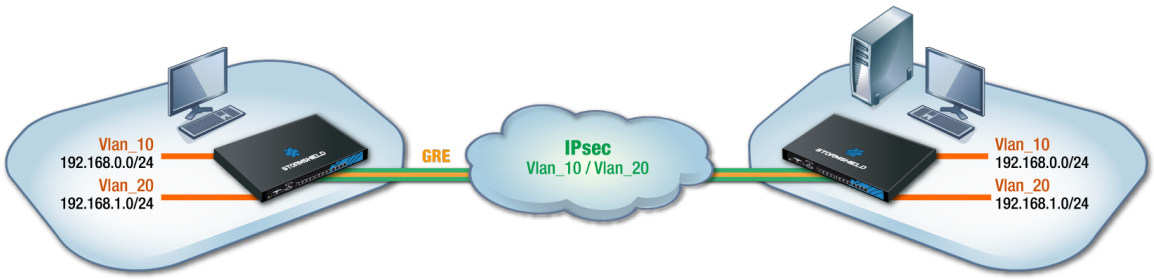


Cette section de la note technique présente le cas d'une entreprise souhaitant relier au travers d'un bridge deux sites partageant un plan d'adressage identique. Les services, DHCP par exemple, et les ressources réseau partagées seront ainsi vus comme des services locaux, quel que soit le site. Pour sécuriser ces échanges, les flux GRE seront chiffrés dans un tunnel IPsec.

NOTE

Les adresses IP attribuées aux équipements des deux sites doivent bien évidemment être uniques.

Cas 2 : transport de VLAN dans un tunnel GRE



Cette section de la note technique présente le cas d'une entreprise souhaitant partager deux VLAN entre deux sites au travers d'un tunnel GRE sécurisé par du chiffrement (IPsec). Y sont abordés la configuration propre à la création des interfaces GRETAP, au tunnel IPsec, au paramétrage des VLAN et à leur rattachement aux interfaces GRETAP.

IMPORTANT

Un bridge sera nécessaire pour chaque VLAN transporté. Il est donc essentiel de s'assurer que le firewall supporte le nombre de bridges envisagés.

La commande`system property`(menu **Système** >**Console CLI**) permet de recueillir cette information:

CONSOLE CLI

```
SYSTEM      : System commands
USER        : User related functions
VERSION     : Display server version
system property
[Result]
Type=Firewall
Model=V50-A
MachineType=amd64
Version=
ASQVersion=7.3.0
SerialNumber=V50XXA3E0000017
MTUmax=9198
LACP=0
Bridge=8
```

Cas n°1 : réunion de deux sites partageant le même plan d'adressage

Paramétrage du Firewall du site A

Création de l'interface GRETAP

Dans le module **Réseau** > **Interfaces**, cliquez sur **Ajouter** et choisissez **Ajouter une interface GRETAP**. Renseignez les champs obligatoires suivants:

Configuration globale

Nom: affectez un nom à l'interface GRETAP (gretap dans l'exemple).

Configuration de l'interface

Bridge: sélectionnez un bridge existant sur le Firewall. Il peut s'agir du bridge issu de la configuration par défaut ou d'un bridge créé pour cet usage.

NOTE

Il n'est pas possible de créer un bridge au sein de l'assistant de création de l'interface GRETAP.

NOTE

Il est possible de ne pas sélectionner de bridge pour l'interface GRETAP en choisissant l'option **Créer une interface GRETAP inactive**.L'interface pourra alors être activée ultérieurement en la déplaçant dans un bridge.

Configuration du tunnel GRETAP

Source du tunnel: sélectionnez l'interface physique par laquelle les flux GRE transiteront en sortie du Firewall. Dans l'exemple présenté, il s'agit de l'interface **Firewall_out**.

Destination du tunnel: sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).

Cliquez sur **Terminer** puis **Appliquer** pour valider la création de l'interface GRETAP.

Création du tunnel IPsec

Dans l'onglet *Politique de chiffrement - Tunnels* du module **VPN** > **VPN IPsec**, cliquez sur le bouton **Ajouter** et sélectionnez **Tunnel site à site**. Remplissez les différents champs présentés par l'assistant de création de tunnel puis validez:

- **Réseau local**: sélectionnez l'interface physique portant le tunnel GRE (**Firewall_out** dans l'exemple).
- **Réseau distant** : sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).

- **Choix du correspondant**: créez (ou sélectionnez le s'il existe déjà) un correspondant dont la passerelle distante sera un objet portant l'adresse IP publique du Firewall distant.

  NOTE

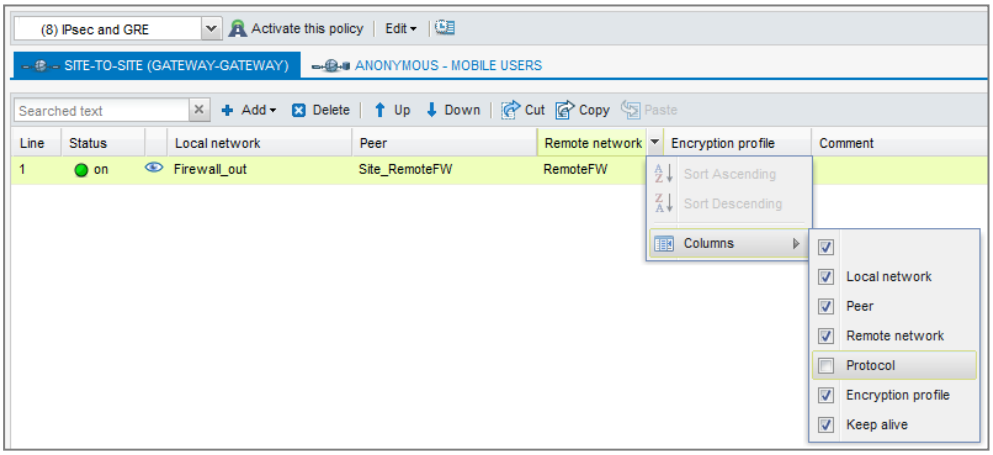
  Pour plus de détails concernant la création d'un correspondant utilisant les méthodes d'authentification par clé pré-partagée ou par certificats, veuillez consulter les documents VPN-IPsec - Authentification par clé pré-partagée et VPN IPsec: Authentification par certificats.

  NOTE

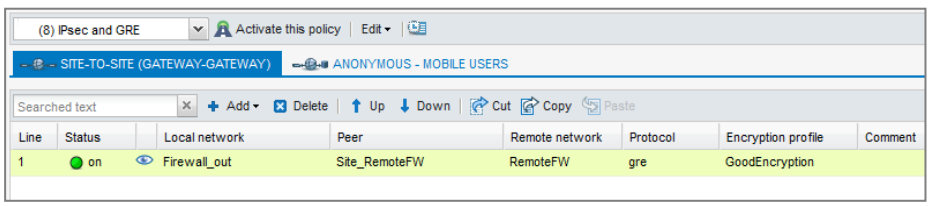
  La version du protocole IKE pour ce correspondant doit être identique à:

  - celle utilisée sur le Firewall distant,
  - celle des correspondants utilisés dans les autres règles de la politique IPsec concernée.

Afin de ne pas autoriser l'établissement du tunnel IPsec pour des protocoles autres que GRE et éviter le chiffrement de flux tels qu'ICMP (Ping), il est possible de spécifier le protocole GRE dans la colonne **Protocole**. Si cette colonne n'est pas affichée, passez votre souris sur le titre d'une colonne quelconque et déroulez le menu contextuel en cliquant sur la flèche. Sélectionnez **Colonne** puis cochez **Protocole**:



La politique VPN IPsec aura donc la forme suivante :



NOTE

Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Paramétrage du Firewall du site B

Création de l'interface GRETAP

En suivant la méthode utilisée sur le Firewall du site A, créez l'interface GRETAP:

Configuration globale

Nom: affectez un nom à l'interface GRETAP

Configuration de l'interface

Bridge: sélectionnez un bridge existant sur le Firewall. Il peut s'agir du bridge issu de la configuration par défaut ou d'un bridge créé pour cet usage.

Configuration du tunnel GRETAP

Source du tunnel: sélectionnez l'interface physique par laquelle les flux GRE transiteront sur le Firewall. Dans l'exemple présenté, il s'agit de l'interface **Firewall_out**.

Destination du tunnel: sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).

Cliquez sur **Terminer** puis **Appliquer** pour valider la création de l'interface.

Création du tunnel IPsec

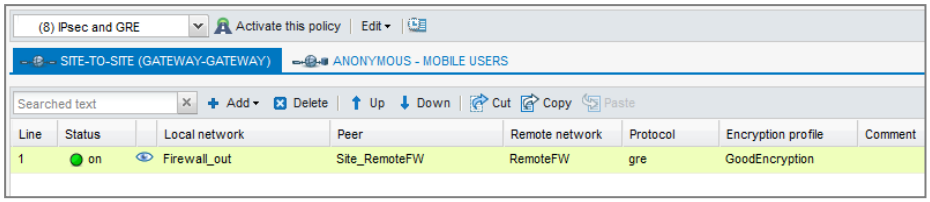
En suivant la méthode utilisée pour créer le tunnel IPsec sur le Firewall du site A, définissez un tunnel avec les valeurs suivantes:

- **Réseau local**: sélectionnez l'interface physique portant le tunnel GRE (**Firewall_out** dans l'exemple).
- **Réseau distant** : sélectionnez un objet portant l'adresse IP publique du Firewall distant (objet **Remote_FW** dans l'exemple).
- **Choix du correspondant**: créez (ou sélectionnez le s'il existe déjà) un correspondant dont la passerelle distante sera un objet portant l'adresse IP publique du Firewall distant.

> **NOTE**
>
> La version du protocole IKE pour ce correspondant doit être identique à:
>
> - celle utilisée sur le Firewall distant,
> - celle des correspondants utilisés dans les autres règles de la politique IPsec concernée.

Sélectionnez **GRE** dans la colonne **Protocole** de la règle IPsec afin de limiter l'utilisation du tunnel aux flux GRE.

La politique VPN IPsec aura donc la forme suivante :



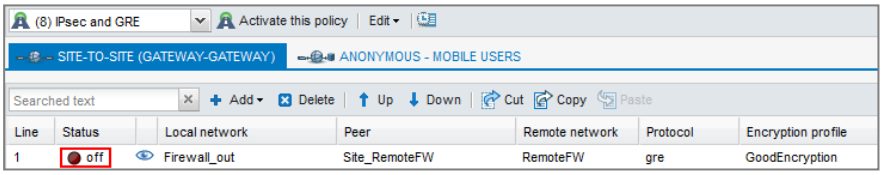
NOTE

Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Vérification des tunnels

Tunnel GRE

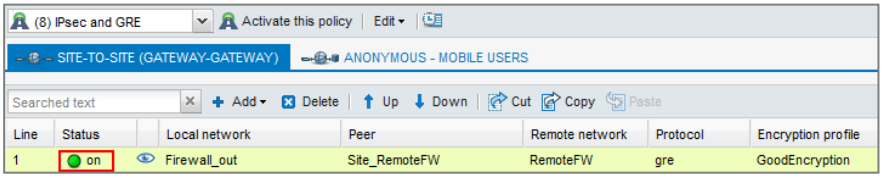
Pour vérifier le fonctionnement du tunnel GRE non chiffré entre les deux Firewalls, désactivez la règle IPsec sur chaque site en mettant son état à **off** et activez la politique IPsec:



Depuis un poste situé sur le réseau local du site A, lancez un test de disponibilité (Ping) vers une machine située sur le réseau local du site B. Cette machine doit répondre aux requêtes.

Tunnel GRE chiffré dans un tunnel IPsec

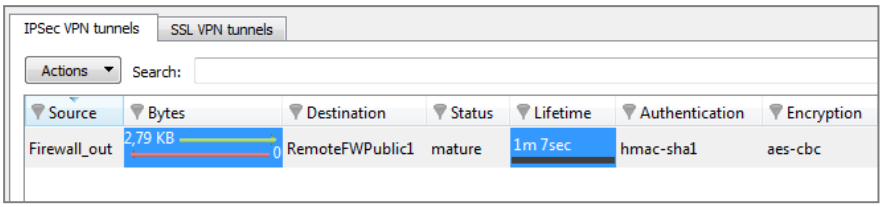
Sur chaque Firewall, activez la règle IPsec en fixant son état à **on** et activez la politique IPsec :



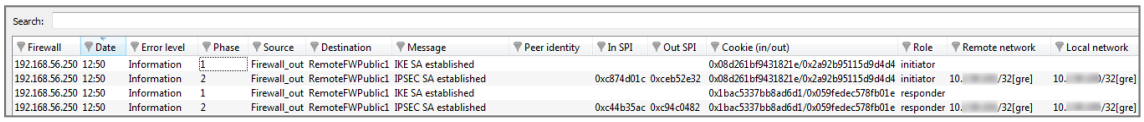
Depuis un poste situé sur le réseau local du site A, lancez un test de disponibilité (Ping) d'une machine située sur le réseau local du site B. Cette machine doit répondre aux requêtes.

Vérification depuis SN Real-Time Monitor

L'état du tunnel IPsec peut être visualisé dans l'onglet *Tunnels VPN IPsec* du module **Tunnels VPN** de SN Real-Time Monitor:



Les traces concernant l'établissement du tunnel IPsec peuvent être consultées dans le module **Traces** > **VPN**:



Vérification depuis l'interface Web des Firewalls

Depuis l'interface d'administration Web du Firewall, accédez aux journaux de traces et aux rapports afin de vérifier le fonctionnement de la configuration mise en place.

Cas n°2 : transport de VLAN dans un tunnel GRE

Paramétrage du Firewall du site A

Création et activation de l'interface GRETAP

Création

Dans le module **Réseau** > **Interfaces**, cliquez sur **Ajouter** et choisissez **Ajouter une interface GRETAP**. Renseignez les champs obligatoires suivants:

Configuration globale

Nom: affectez un nom à l'interface GRETAP (GretapVLAN dans l'exemple).

Configuration de l'interface

Bridge: sélectionnez l'option **Créer une interface GRETAP inactive**. L'interface sera activée par la suite en lui attribuant une adresse IP dédiée.

NOTE

Ne pas rattacher l'interface GRETAP à un bridge permet de n'autoriser dans le tunnel GRE que les paquets réseau des VLAN rattachés à cette interface (VLAN10 et 20 dans l'exemple).

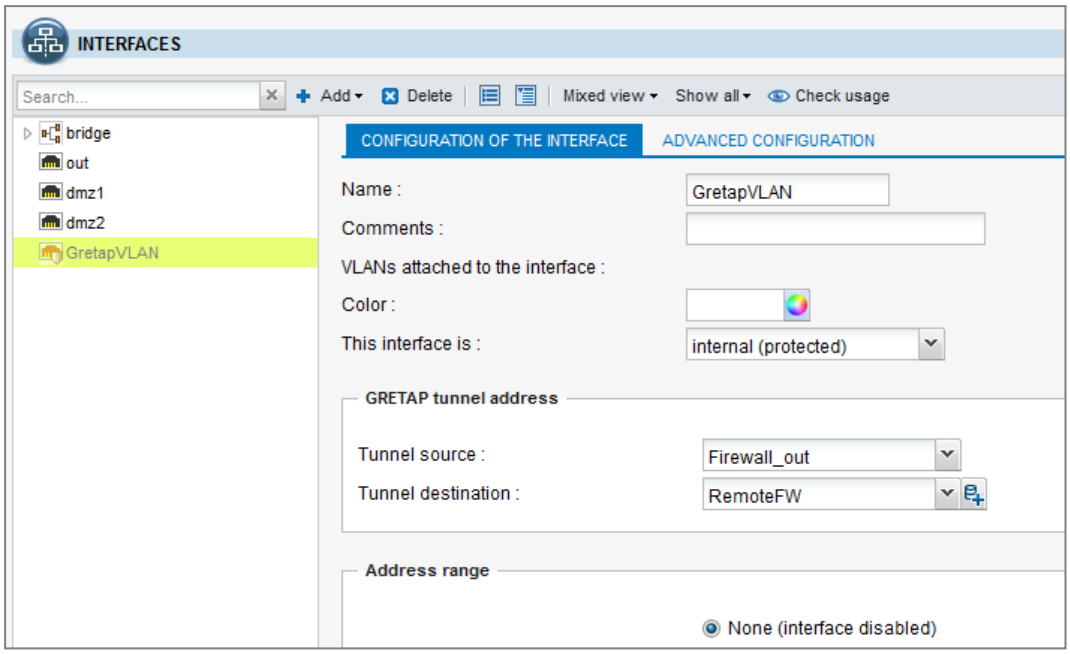
Configuration du tunnel GRETAP

Source du tunnel: sélectionnez l'interface physique par laquelle les flux GRE transiteront en sortie du Firewall. Dans l'exemple présenté, il s'agit de l'interface **Firewall_out**.

Destination du tunnel: sélectionnez un objet portant l'adresse IP publique du Firewall distant (**Remote_FW** dans l'exemple).

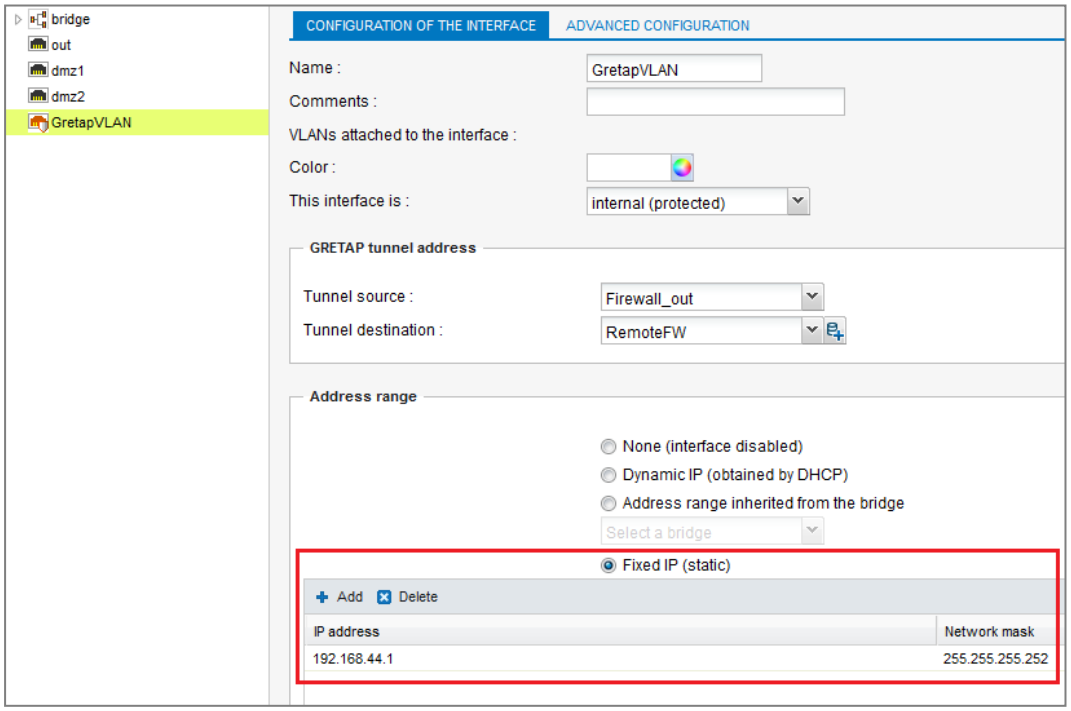
Cliquez sur **Terminer** puis **Appliquer** pour valider la création de l'interface GRETAP.

L'interface GretapVLAN créée apparaît alors grisée (inactive) dans la liste des interfaces:



Activation

Dans l'onglet *Configuration de l'interface*, attribuez une adresse IP à l'interface GRETAP en sélectionnant le choix **IP fixe (statique)** puis en renseignant l'adresse IP ainsi que le masque réseau. Validez la configuration en cliquant sur le bouton **Appliquer**. L'interface GRETAP est alors activée. Dans cet exemple, l'adresse IP et le réseau choisis ont pour valeur respective 192.168.44.1 et 255.255.255.252:

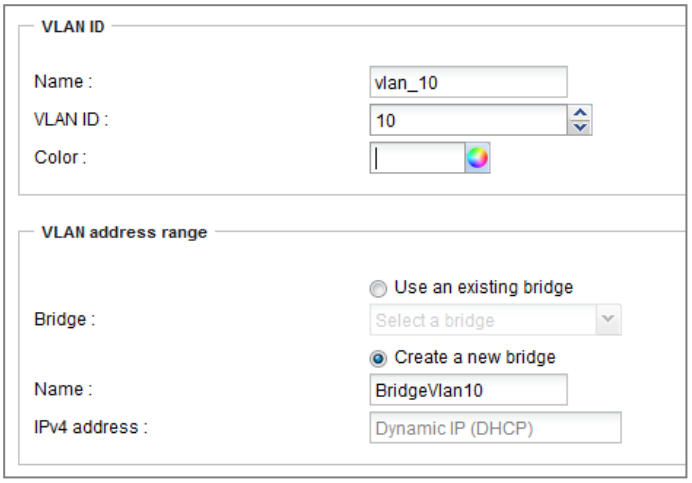


Création des VLAN

Création du VLAN 10

Dans le menu **Réseau** > **Interfaces**, cliquez sur **Ajouter** puis **Ajouter un VLAN**. Dans le premier écran de l'assistant de création, choisissez l'option **VLAN attaché à 2 interfaces (VLAN traversant)**.

Remplissez ensuite les champs des écrans de l'assistant comme suit:

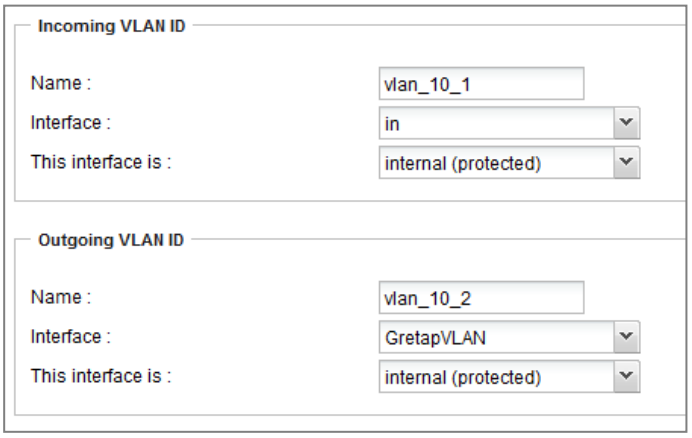


Identification du VLAN

- **Nom**: choisissez un nom pour ce VLAN (**vlan_10** dans l'exemple).
- **Identifiant de VLAN**: sélectionnez l'identifiant 802.1q associé au VLAN (10 dans l'exemple).

Plan d'adressage du VLAN

- Sélectionnez **Créer un nouveau bridge** et attribuez un nom à ce bridge (**BridgeVlan10** dans l'exemple).
- **Adresse IPv4**: laissez l'attribution d'IP dynamique (DHCP) proposée par défaut puis validez cet écran en cliquant sur **Suivant**.



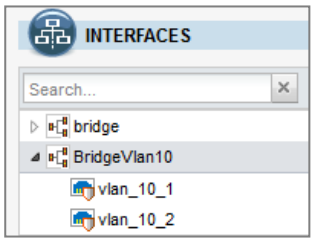
Identification du VLAN entrant

- **Nom**: choisissez un nom pour le VLAN rattaché à l'interface d'entrée des flux. Par défaut, il s'agit du nom de VLAN choisi dans le premier écran suffixé par la chaine "_1" (**vlan_10_1** dans l'exemple).
- **Interface**: sélectionnez l'interface par laquelle les paquets appartenant au VLAN entrent dans le firewall. Dans l'exemple, les machines étant sur le réseau interne, il s'agit de l'interface **in**.
- **Cette interface est**: indiquez que ce VLAN doit être considéré comme une interface interne (protégée).

Identification du VLAN sortant

- **Nom**: choisissez un nom pour le VLAN rattaché à l'interface de sortie des flux. Par défaut, il s'agit du nom de VLAN choisi dans le premier écran suffixé par la chaine "_2" (**vlan_10_2** dans l'exemple).
- **Interface**: sélectionnez l'interface GRETAP par laquelle les paquets appartenant au VLAN sortent du firewall. Dans l'exemple, il s'agit de l'interface **GretapVLAN**.
- **Cette interface est**: indiquez que ce VLAN doit être considéré comme une interface interne (protégée).

Après avoir validé la configuration, les VLAN et leur bridge associé sont alors visibles dans la liste des interfaces:



Création du VLAN 20

Pour la création du second VLAN devant être transporté dans le tunnel GRE, suivez la méthode décrite dans le paragraphe Création du VLAN 10 en utilisant les valeurs suivantes:

Identification du VLAN

- **Nom**: **vlan_20** dans l'exemple.
- **Identifiant de VLAN**: 20 dans l'exemple.

Plan d'adressage du VLAN

- Sélectionnez **Créer un nouveau bridge**. Nom de ce bridge: **BridgeVlan20** dans l'exemple.
- **Adresse IPv4**: attribution d'IP dynamique (DHCP).

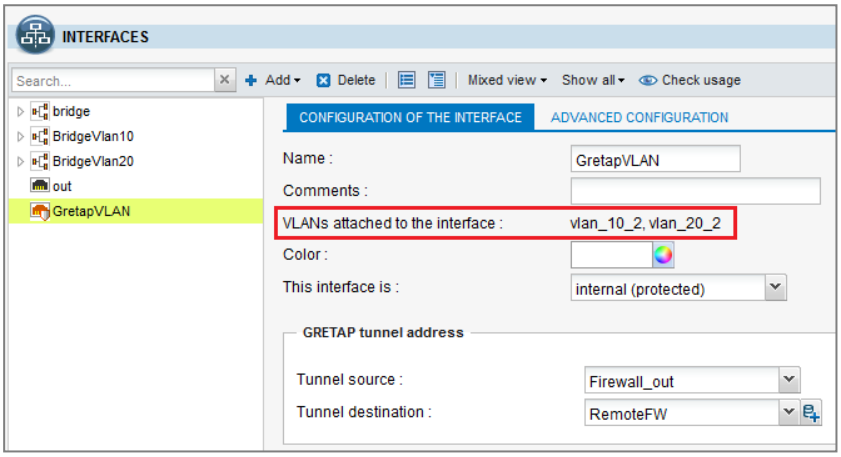
Identification du VLAN entrant

- **Nom**: **vlan_20_1** dans l'exemple.
- **Interface**: **in** dans l'exemple.
- **Cette interface est**:indiquez que ce VLAN doit être considéré comme une interface interne (protégée).

Identification du VLAN sortant

- **Nom**: vlan_20_2 dans l'exemple.
- **Interface**: GretapVLAN dans l'exemple.
- **Cette interface est**: indiquez que ce VLAN doit être considéré comme une interface interne (protégée).

En cliquant sur l'interface GRETAP, il est possible de vérifier que les deux VLAN vlan_10_2 et vlan_20_2 lui sont bien rattachés:



Création du tunnel IPsec

Pour la création du tunnel IPsec sur le firewall du site A, veuillez-vous référer à la section Création du tunnel IPsec du cas n°1.

NOTE

Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Paramétrage du Firewall du site B

Création de l'interface GRETAP

Pour la création de l'interface GRETAP sur le firewall du site B, suivez la méthode exposée dans le paragraphe Création de l'interface GRETAP sur le site A. Pour l'exemple présenté, les valeurs utilisées seront les suivantes:

- **Adresse IP**: 192.168.44.2.
- **Masque**: 255.255.255.252.

Création des VLAN

Pour la création des VLAN 10 et 20 et leur affectation à l'interface GRETAP sur le second Firewall, suivez la méthode décrite dans le paragraphe Création des VLAN pour le Firewall du site A.

Création du tunnel IPsec

Pour la création du tunnel IPsec sur le firewall du site B, veuillez-vous référer à la section Création du tunnel IPsec du cas n°1.

NOTE

Le firewall étant à l'initiative de l'émission des paquets réseau GRE, il n'est donc pas nécessaire de créer de règles de filtrage pour ce protocole.

Vérification

Depuis une machine du site A appartenant au VLAN 10 ou au VLAN 20, faites un test de disponibilité (Ping) vers une machine du site B appartenant au même VLAN: la machine du site B doit répondre aux requêtes.

Il est également possible de vérifier que les VLAN sont bien transportés dans le tunnel en effectuant une capture réseau sur l'interface d'entrée du tunnel du firewall du site B. Dans ce cas, les paquets réseaux capturés laissent ainsi apparaître le protocole GRE encapsulant le VLAN transporté (VLAN 20 dans l'exemple):

```
15:41:06.019669 00:90:fb:2c:5d:b2 > 00:0d:b4:0c:c6:b6, ethertype IPv4 (0x0800), length 108: 172.16.3.1 > 172.16.2.1: GREv0,
proto TEB (0x6558), length 74: 18:03:73:8b:51:d8 > 01:00:5e:00:00:fc, ethertype 802.1Q (0x8100), length 70: vlan 20, p 0,
ethertype IPv4, 192.168.1.10.50677 > 224.0.0.252.5355: UDP, length 24
```

STORMSHIELD

documentation@stormshield.eu