



**STORMSHIELD**



NOTE TECHNIQUE

**STORMSHIELD NETWORK SECURITY**

# VPN IPSEC MOBILE IKEV1 - AUTHENTIFICATION PAR CLÉ PRÉ-PARTAGÉE

Produits concernés : SNS 3.7.x-LTSB, SNS 3.x, SNS 4.x, SN VPN Client Standard

Dernière mise à jour du document : 27 avril 2020

Référence : sns-fr-VPN\_IPSec\_Mobile\_IKEv1\_Authentification\_Cle\_Pre\_Partagee\_Note\_Technique



# Table des matières

Lire attentivement avant de commencer .....	4
VPN IPsec mobile IKEv1 - Authentification par clé pré-partagée .....	5
Prérequis .....	5
Autoriser les utilisateurs mobiles à établir un tunnel VPN IPsec .....	6
Créer un groupe contenant tous les utilisateurs autorisés à établir un tunnel VPN IPsec .....	6
Vérifier que la méthode d'authentification pour les utilisateurs nomades repose sur LDAP .....	6
Si aucune règle d'authentification n'est présente dans la grille .....	6
Si des règles d'authentification sont déjà présentes dans la grille .....	7
Autoriser les utilisateurs mobiles à établir un tunnel VPN IPsec .....	7
Optimiser les flux liés aux tunnels .....	9
Prérequis .....	9
Optimiser les flux liés aux tunnels : limiter les datagrammes IP des négociations ISAKMP .....	9
Optimiser les flux liés aux tunnels : limiter la MSS .....	9
Modifier un profil d'inspection TCP-UDP .....	10
Intégrer ce profil d'inspection TCP-UDP dans un profil d'inspection global .....	10
Mettre en œuvre une configuration pour une politique IPsec mobile en mode Config ...	11
Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles .....	11
Définir un objet réseau représentant le réseau local accessible aux correspondants mobiles en mode Config .....	11
Créer le profil des correspondants VPN IPsec .....	12
Ajouter des clés pré-partagées (PSK) à une politique existante .....	13
Créer la politique IPsec - Mode Config .....	14
Autoriser les accès VPN IPsec dans la politique de filtrage .....	15
Configurer le client VPN .....	15
Configurer la phase 1 .....	16
Configurer la phase 2 .....	17
Établir le tunnel VPN IPsec depuis le poste client .....	18
Fermer un tunnel depuis le poste client .....	19
Mettre en œuvre une configuration pour une politique IPsec mobile en mode standard	20
Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles .....	20
Définir l'objet réseau .....	20
Définir le ou les objet(s) réseau représentant le(s) réseau(x) accessible(s) aux correspondants mobiles .....	20
Créer le premier objet réseau .....	21
Créer le second objet réseau .....	21
Créer le profil des correspondants VPN IPsec .....	21
Ajouter des clés pré-partagées (PSK) à une politique existante .....	22
Créer la politique IPsec .....	23
Autoriser les accès VPN IPsec dans la politique de filtrage .....	24
Configurer le client VPN .....	25
Configurer la phase 1 .....	25
Configurer la phase 2 pour le premier réseau .....	26
Configurer la phase 2 pour le second réseau accessible .....	27
Établir un tunnel VPN IPsec depuis le poste client .....	27
Fermer un tunnel depuis le poste client .....	28



Afficher les détails d'un tunnel sur le firewall .....	29
Pour aller plus loin .....	30



## Lire attentivement avant de commencer

---

Ce document s'adresse tout particulièrement aux administrateurs qui utilisent une configuration IPsec active comportant des tunnels Site à Site en IKEv1, et qui souhaitent y ajouter rapidement une politique nomade IKEv1.

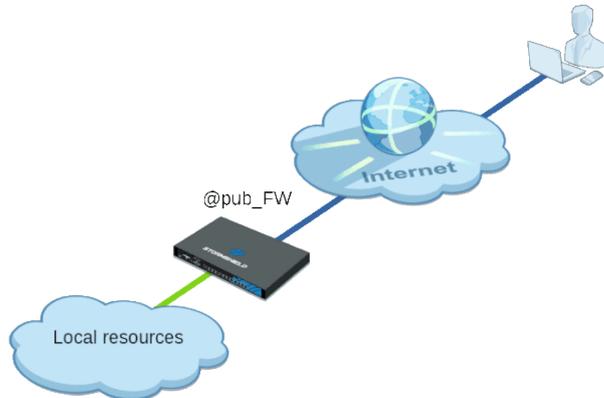
La solution basée sur IKEv1 et une authentification par clé pré-partagée peut en effet répondre à un besoin d'urgence, même si ce mode n'est pas le mode recommandé par l'ANSSI pour une sécurité optimale (un avertissement est affiché lors de la création de la politique IPsec).

Cependant :

- Si dans votre politique IPsec active, un correspondant IKEv2 est utilisé,
- Si dans votre politique IPsec active, un des correspondants utilisés a son champ **DSCP** (option non disponible en version SNS 3.7.x-LTSB) positionné à une valeur différente de "*00 Best effort*",
- Ou si vous souhaitez adopter une configuration recommandée par l'ANSSI, alors nous vous recommandons de vous référer au tutoriel [VPN IPsec mobile IKEv2 - Authentification par clé pré-partagée](#).



# VPN IPsec mobile IKEv1 - Authentification par clé pré-partagée



Ce document décrit la configuration VPN nécessaire pour autoriser un utilisateur distant (appelé également mobile ou nomade) à accéder de manière sécurisée au réseau interne de son entreprise, depuis un poste de travail Microsoft équipé du logiciel SN VPN Client Standard.

La méthode d'authentification présentée dans ce tutoriel est basée sur l'utilisation d'une clé pré-partagée propre à chaque utilisateur.

Les tunnels IPsec décrits dans cette note technique sont basés sur la version 1 du protocole IKE.

Deux types de configurations sont ainsi abordés :

- Utilisation du mode *Config* qui permet de fournir automatiquement aux clients tous les paramètres réseau nécessaires pour établir le tunnel VPN IPsec. Bien que plus simple au premier abord, ce mode présente une limitation importante : il ne permet de définir qu'un seul réseau protégé par le firewall pouvant être joint par les utilisateurs nomades. Il n'est donc pas possible de sélectionner un groupe de réseaux ou plusieurs réseaux.
- Attribution manuelle d'adresses IP à chaque utilisateur et paramétrage manuel du client VPN. Contrairement au mode *Config*, cette configuration permet de définir plusieurs réseaux protégés par le firewall et pouvant être joints par les utilisateurs nomades.

## Prérequis

- Un annuaire LDAP doit être configuré sur le firewall.  
Si ce n'est pas le cas, veuillez vous référer à la section [Configuration des annuaires](#) du **Manuel Utilisateur SNS**.
- Une adresse e-mail doit être définie pour chaque utilisateur présent dans l'annuaire LDAP.
- Le poste client Microsoft doit être équipé du logiciel **SNS VPN Client**, disponible dans la section **Téléchargements > Stormshield Network Security > VPN Client** de votre espace [Mystormshield](#) (logiciel soumis à l'acquisition d'une licence et disposant d'une période d'évaluation de 30 jours) ou du client VPN IPsec [TheGreenBow](#).
- La politique IPsec utilisée doit contenir exclusivement des correspondants IPsec IKEv1 (tunnels site à site et tunnels nomades).



# Autoriser les utilisateurs mobiles à établir un tunnel VPN IPsec

La méthode proposée consiste à créer un groupe contenant tous les utilisateurs mobiles autorisés à établir un tunnel VPN IPsec, puis à attribuer le droit adéquat à ce groupe.

## Créer un groupe contenant tous les utilisateurs autorisés à établir un tunnel VPN IPsec

Dans le cas d'un annuaire LDAP interne, allez dans le module **Configuration > Utilisateurs > Utilisateurs** :

1. Cliquez sur **Ajouter un groupe**.
2. Dans le champ **Nom de Groupe**, saisissez un nom représentatif (exemple : *Mobile\_Users*). Vous pouvez ajouter une description.
3. Cliquez sur **Ajouter**.  
Une ligne s'ajoute dans la grille des membres du groupe.
4. Tapez les premières lettres de l'utilisateur à ajouter au groupe et sélectionnez l'utilisateur souhaité dans la liste proposée par le firewall.
5. Répétez les étapes 3 et 4 pour ajouter l'ensemble des utilisateurs devant appartenir à ce groupe.
6. Lorsque tous les membres ont été ajoutés, cliquez sur **Appliquer**.
7. Validez en cliquant sur **Sauvegarder**.

Dans le cas d'un annuaire externe (Microsoft Active Directory, LDAP ou LDAP de type Posix), ce groupe devra être créé directement sur l'une des machines hébergeant l'annuaire.

## Vérifier que la méthode d'authentification pour les utilisateurs nomades repose sur LDAP

Allez dans le module **Configuration > Utilisateurs > Authentification > onglet Politique d'authentification**.

### Si aucune règle d'authentification n'est présente dans la grille

Vérifiez que le champ **Méthode à utiliser si aucune règle ne peut être appliquée** est bien positionné sur LDAP :



Status	Source	Methods (assess)
--------	--------	------------------

Default method

Method to use if no rules match: LDAP

### Si des règles d'authentification sont déjà présentes dans la grille

Ajoutez une règle d'authentification LDAP pour les utilisateurs provenant du VPN IPsec :

1. Cliquez sur **Nouvelle règle** et choisissez **Règle standard**.
2. Dans le champ **Utilisateur ou groupe**, sélectionnez le groupe précédemment créé (*Mobile Users* dans l'exemple).
3. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Source**.
4. Cliquez sur **Ajouter une interface** et sélectionnez **VPN IPsec**.
5. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Méthodes d'authentification**.
6. Sélectionnez la ligne de la grille comportant **Méthode par défaut** et cliquez sur **Supprimer**.
7. Cliquez sur **Autoriser une méthode** et sélectionnez **LDAP**.
8. Cliquez sur **OK**.
9. Faites un double-clic dans la cellule correspondant à la colonne **État** afin d'activer cette règle.  
Son état passe à **ON**.
10. Cliquez sur **Appliquer** puis sur **Sauvegarder**.

La règle d'authentification obtenue est donc la suivante :

Status	Source	Methods (assess by order)
1	Mobile Users@stormshield.eu   ipsec	1 LDAP

### Autoriser les utilisateurs mobiles à établir un tunnel VPN IPsec

Dans le module **Configuration** > **Utilisateurs** > **Droit d'accès** > onglet **Accès détaillé** :

1. Cliquez sur **Ajouter**.  
Une ligne s'ajoute dans la grille.



2. Cliquez dans la cellule de cette ligne correspondant à la colonne **Utilisateur - groupe d'utilisateurs**.
3. Tapez les premières lettres du groupe et sélectionnez le dans la liste proposée par le firewall.
4. Cliquez dans la cellule de cette ligne correspondant à la colonne **IPSEC** et sélectionnez **Autoriser**.
5. Faites un double-clic dans la cellule de cette ligne correspondant à la colonne **État** pour afficher **Activé**.
6. Cliquez sur **Appliquer**.

Les utilisateurs contenus dans ce groupe sont désormais autorisés à établir des tunnels IPsec :

The screenshot shows the 'ACCESS PRIVILEGES' interface with the 'DETAILED ACCESS' tab selected. The table below lists the access settings for a user group.

Status	User - user group	SSL VPN Portal	IPSEC	SSL VPN	Sponsorship	Description
1 <span style="color: green;">●</span> Enabled	Mobile Users@stormshield.eu	Block	Allow	Block	Block	

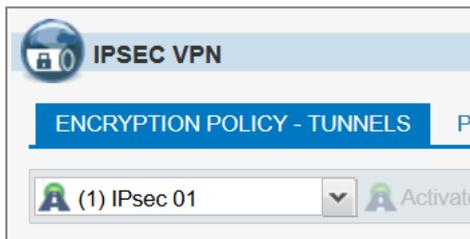


## Optimiser les flux liés aux tunnels

Il est recommandé de modifier plusieurs paramètres du firewall afin d'optimiser les flux liés aux tunnels IPsec.

### Prérequis

Pour les besoins des exemples, les optimisations et sécurisations recommandées supposent que la politique IPsec utilisée sur le firewall pour les utilisateurs mobiles, qu'il s'agisse du **mode Config** ou du **mode standard**, est la politique *IPsec\_01* (module **Configuration** > **VPN** > **VPN IPsec**) :



### Optimiser les flux liés aux tunnels : limiter les datagrammes IP des négociations ISAKMP

Selon les fournisseurs d'accès Internet, la taille maximale des paquets autorisés peut être très variable.

Stormshield conseille de limiter la taille des datagrammes IP des négociations ISAKMP à la valeur de 1280 octets :

1. Connectez-vous à l'interface Web d'administration du firewall.
2. Allez dans le module **Configuration** > **Système** > **Console CLI**.
3. Activez la fragmentation IKE en tapant la commande :  
`CONFIG IPSEC PEER UPDATE name=IPsec_Mobile_Profile_Name ike_frag=1`  
où *IPsec\_Mobile\_Profile\_Name* représente le nom donné au profil des correspondants IPsec [*IKEv1\_Mobile\_Users* dans l'exemple].
4. Fixez la taille maximale des datagrammes ISAKMP à 1280 octets à l'aide de la commande :  
`CONFIG IPSEC UPDATE slot=xy FragmentSize=1280`  
où *xy* représente le numéro de la politique IPsec mobile.  
Dans l'exemple, il s'agit de la politique *IPsec 01* : *xy* vaudra donc *01*.
5. Appliquez ces modifications en tapant la commande :  
`CONFIG IPSEC ACTIVATE`
6. Rechargez la politique IPsec afin de prendre en compte ces modifications :  
`CONFIG IPSEC RELOAD`  
Attention : cette commande réinitialise les tunnels déjà établis.

### Optimiser les flux liés aux tunnels : limiter la MSS

Les paquets échangés étant encapsulés dans le tunnel, une "surcharge" de plusieurs dizaines d'octets des données provient des en-têtes ESP.

Il convient donc d'activer la limitation automatique de la taille des segments (MSS : Maximum Segment Size) échangés entre le client et le firewall.



Cette option permet d'éviter (ou de limiter au maximum) la fragmentation de paquets. En effet, elle impose, pour les échanges de paquets entre le client et le firewall, une taille de paquets inférieure à la MTU (Maximum Transmission Unit) des différents équipements réseaux traversés lors de ces échanges.

## Modifier un profil d'inspection TCP-UDP

Dans le module **Protection applicative** > **Protocoles** > **TCP-UDP** :

1. Sélectionnez le profil d'inspection TCP-UDP dans lequel vous souhaitez appliquer cette modification (*tcpudp\_03* dans l'exemple).  
Ce profil d'inspection sera ensuite sélectionné dans un profil global, lui-même appliqué à la règle de filtrage autorisant les accès des clients mobiles VPN.
2. Cochez la case **Imposer une limite MSS**.  
Saisissez la valeur **1300** (octets) (valeur conseillée par Stormshield).
3. Validez cette modification en cliquant sur **Appliquer**.
4. Confirmez en cliquant sur **Sauvegarder**.

## Intégrer ce profil d'inspection TCP-UDP dans un profil d'inspection global

Dans le module **Protection applicative** > **Profils d'inspection** :

1. Cliquez sur **Accéder aux profils**.
2. Dans la liste déroulante, sélectionnez le profil auquel vous souhaitez associer le profil TCP-UDP précédemment modifié avec l'option MSS. Dans l'exemple, le profil *IPS\_03* est sélectionné.
3. Sur la ligne TCP-UDP, cliquez sur le profil applicatif proposé et choisissez le profil modifié (*tcpudp\_03* dans l'exemple).
4. Validez cette modification en cliquant sur **Appliquer**.
5. Confirmez en cliquant sur **Sauvegarder**.  
C'est ce profil IPS pour le trafic entrant qui devra être sélectionné dans la règle de filtrage autorisant le trafic issu des tunnels IPsec mobiles.



## Mettre en œuvre une configuration pour une politique IPsec mobile en mode *Config*

Dans cette configuration, les utilisateurs nomades établissent le tunnel avec une adresse IP obtenue automatiquement par leur client VPN.

Pour définir une politique IPsec mobile en mode *Config*, les étapes de configuration du firewall sont les suivantes :

- Définir un objet réseau regroupant les adresses IP attribuées aux utilisateurs nomades lors de l'établissement du tunnel VPN IPsec,
- Définir un objet réseau représentant le réseau local accessible aux utilisateurs nomades connectés via un tunnel VPN IPsec,
- Créer le profil des correspondants IPsec IKEv1,
- Créer la politique IPsec IKEv1 utilisant le profil de correspondants défini précédemment,
- Mettre en place les règles de filtrage autorisant les flux depuis les clients mobiles vers le réseau interne.

### Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles

Il est impératif que le réseau attribué aux clients ne soit pas déjà connu du firewall : il ne doit s'agir ni d'un réseau directement connecté, ni d'un réseau connu par le biais du routage.

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

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réseau**.
3. Attribuez un **Nom** à cet objet (*Mobile\_Users\_Network* dans l'exemple).
4. Renseignez le champ **Adresse IP de réseau** sous la forme réseau/masque.  
Ce réseau doit contenir au moins autant d'adresses IP que d'utilisateurs susceptibles de se connecter via un tunnel VPN IPsec.

**Exemples :**

192.168.9.0/24 ou 192.168.9.0/255.255.255.0 : 254 adresses donc 254 phases 2.  
192.168.9.0/23 ou 192.168.9.0/255.255.254.0 : 510 adresses donc 510 phases 2.

5. Cliquez sur **Créer**.

### Définir un objet réseau représentant le réseau local accessible aux correspondants mobiles en mode *Config*

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

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réseau**.
3. Attribuez un **Nom** à cet objet (*Local\_Network\_Authorized\_IPsec* dans l'exemple).
4. Renseignez le champ **Adresse IP de réseau** sous la forme réseau/masque.

**Exemple :**

192.168.1.0/24 ou 192.168.1.0/255.255.255.0.

5. Cliquez sur **Créer**.



## Créer le profil des correspondants VPN IPsec

Dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants** :

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Nouveau correspondant mobile (nomade) IKEv2** ou **Nouveau correspondant anonyme (nomade) IKEv2** (jusque SNS v3.7.11-LTSB et SNS 3.10.1).
3. Donnez un nom à la configuration nomade (*IKEv1\_Mobile\_Users* dans l'exemple) puis cliquez sur **Suivant**.
4. Pour l'**Authentification du correspondant**, choisissez **Clé pré-partagée (PSK)** puis cliquez sur **Suivant**.
5. Dans le tableau d'**Identification des correspondants**, cliquez sur **Ajouter**.
6. Dans le champ **Identifiant**, saisissez l'adresse e-mail du correspondant.
7. Dans les champs **Clé pré-partagée (ASCII)** et **Confirmer**, tapez le mot de passe servant à établir le tunnel VPN IPsec pour ce correspondant.  
Pour des raisons évidentes de sécurité, choisissez des mots de passe uniques et respectant les [recommandations de l'ANSSI](#).
8. Cliquez sur **OK**.
9. Répétez les étapes 5 à 8 pour chacun des utilisateurs mobiles autorisés.
10. Cliquez sur **Suivant**.  
Une fenêtre résume le nom du correspondant, la politique et le type d'authentification choisie.
11. Validez en cliquant sur **Terminer**.
12. Sélectionnez le correspondant précédemment créé et remplissez le champ **Local ID**.  
Il s'agit en général du nom DNS (FQDN) du firewall. Exemple : *vpn-gw.stormshield.eu*.
13. Cliquez sur **Enregistrer** puis sur **Sauvegarder**.
14. Cliquez sur **Activer la politique**.

Le profil des correspondants mobiles IPsec obtenu est donc le suivant :



The screenshot shows the Stormshield IPSEC VPN configuration interface. The 'PEERS' tab is active, displaying a list of peers on the left and configuration details for 'Peer:IKEv1\_Mobile\_Users' on the right. The configuration includes fields for Comment, Remote gateway (Any), Backup configuration (None), IKE profile (StrongEncryption), and IKE version (IKEv1). The Identification section shows Authentication method (Pre-shared key (PSK)), Certificate (No certificate), and Local ID (Optional) (vpn-gw.stormshield.eu). The Advanced properties section includes Negotiation mode (aggressive), Backup mode (temporary), Local address (Any), Do not initiate the tunnel (Responder only) (checked), and DPD (Passive).

## Ajouter des clés pré-partagées (PSK) à une politique existante

Dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Identification** :

1. Cliquez sur le bouton **Ajouter** du tableau **Tunnels nomades : clés pré-partagées**.
2. Dans le champ **Identifiant**, saisissez l'adresse e-mail du correspondant.
3. Dans les champs **Clé pré-partagée (ASCII)** et **Confirmer**, tapez le mot de passe servant à établir le tunnel VPN IPsec pour ce correspondant.  
Pour des raisons évidentes de sécurité, choisissez des mots de passe uniques et respectant les [recommandations de l'ANSSI](#).
4. Cliquez sur **OK**.
5. Répétez les étapes 1 à 4 pour chacune des PSK à ajouter.

Exemple de table de clés pré-partagées :



Identity	Key
felix.thecat@stormshield.eu	0x40506f756e657474653039
john.doe2@stormshield.eu	0x40506f756e657474653037
john.doe@stormshield.eu	0x506f756e657474653034

## Créer la politique IPsec - Mode Config

Dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - Tunnels** :

1. Dans la liste déroulante, sélectionnez la politique IPsec que vous souhaitez modifier (*IPsec 01* dans l'exemple).
2. Cliquez sur l'onglet **Mobile - Utilisateurs Nomades** (ou **Anonyme - Utilisateurs Nomades**).
3. Cliquez sur **Ajouter**.
4. Sélectionnez **Nouvelle politique Mode Config**.  
Un assistant de configuration se lance.
5. Dans le champ **Correspondant nomade utilisé**, choisissez le profil nomade créé précédemment (*IKEv1\_Mobile\_Users* dans l'exemple).
6. Dans le champ **Réseau local**, sélectionnez le réseau auquel les utilisateurs nomades peuvent accéder au travers du tunnel VPN IPsec (l'objet *Local\_Network\_Authorized\_IPsec* précédemment créé dans l'exemple).  
Pour rappel, un seul réseau peut être sélectionné. Il ne peut pas s'agir d'un groupe de réseaux.
7. Dans le champ **Réseau nomade**, sélectionnez l'objet réseau créé à l'étape **Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles** (*Mobile\_Users\_Network* dans l'exemple).
8. Cliquez sur **Terminer**.  
Dans la zone **Vérification de la politique**, l'avertissement *L'authentification par clé pré-partagée en mode agressif dégrade fortement le niveau de sécurité* est affiché.
9. Cliquez sur **Enregistrer** puis validez en cliquant sur **Sauvegarder**.
10. Cliquez sur **Oui, activer la politique**.

La politique IPsec en mode *Config* obtenue est donc la suivante :

Line	Sta...	Local network	Mobile network	Encryption profile	Config mode
1	on	Local_Network_Authorized_IPSec	Mobile_Users_Network	StrongEncryption	on Edit



## Autoriser les accès VPN IPsec dans la politique de filtrage

Les flux nécessaires à l'établissement du VPN IPsec sont gérés par une règle de filtrage implicite. La politique de filtrage prend donc en charge l'accès des utilisateurs nomades authentifiés via le VPN aux ressources internes.

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

1. Dans la grille de filtrage, sélectionnez la ligne au-dessous de laquelle vous souhaitez ajouter la règle autorisant le VPN IPsec pour les nomades.
2. Cliquez sur **Nouvelle règle**.
3. Sélectionnez **Règle simple**.  
Une nouvelle ligne est ajoutée.
4. Sur la ligne nouvellement ajoutée, faites un double-clic dans la cellule correspondant à la colonne **Action**.  
La fenêtre de configuration de la règle s'ouvre.
5. Dans le champ **Action**, sélectionnez **passer**.
6. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Source**.
7. Dans le champ **Utilisateur**, sélectionnez le groupe d'utilisateurs autorisés à établir un tunnel VPN IPsec (*Mobile Users@stormshield.eu* dans l'exemple).
8. Cliquez sur l'onglet **Configuration avancée** de cette section **Source**.
9. Pour le champ **via**, sélectionnez **Tunnel VPN IPsec**.
10. Pour le champ **Méthode d'authentification**, sélectionnez **VPN IPSEC**.
11. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Destination**.
12. Cliquez sur le bouton **Ajouter** de la grille des **Machines destinations**.
13. Sélectionnez le réseau auquel les utilisateurs nomades peuvent accéder au travers du tunnel VPN IPsec (objet *Local\_Network\_Authorized\_IPsec* dans l'exemple).
14. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Inspection**.
15. Dans le champ **Profil d'inspection**, sélectionnez le profil IPS contenant le profil TCP-UDP avec **l'option MSS** (*IPS\_03* dans l'exemple).
16. Cliquez sur **OK**.
17. Faites un double-clic dans la cellule correspondant à la colonne **État** afin d'activer cette règle.  
Son état passe à **ON**.
18. Cliquez sur **Sauvegarder et activer** puis sur **Oui, activer la politique**.

La règle de filtrage obtenue est donc la suivante :

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass	Mobile Users Auth. by:IPSec VPN via IPSec VPN tunnel	Local_Network_Authorized_IPSec	Any		IPS (IPS_03)

## Configurer le client VPN

Sur le poste de travail Microsoft Windows de l'utilisateur, lancez la fenêtre des connexions du client VPN :

1. Faites un clic droit sur l'icône présente dans la barre des tâches Windows (icônes cachées) : 
2. Sélectionnez le menu **Panneau des connexions**.



## Configurer la phase 1

1. Dans l'arborescence **Configuration VPN**, faites un clic droit sur **IKEv1**.
2. Sélectionnez **Nouvelle phase 1**.  
Une entrée nommée par défaut *Ikev1Gateway* est ajoutée à l'arborescence **IKEv1**.
3. Faites un clic droit sur *Ikev1Gateway* et choisissez **Renommer** pour donner le nom souhaité à cette entrée (*IKEv1GwConfig* dans l'exemple).
4. Cliquez sur cette entrée.
5. Dans l'onglet **Protocole** > **Identité** > champ **Local ID** sélectionnez **E-mail** dans la liste déroulante et indiquez l'adresse e-mail de l'utilisateur du poste de travail.
6. Dans l'onglet **Protocole** > **Fonctions avancées**, cochez la case **Fragmentation** et indiquez la **taille des fragments IKE tels que définis au niveau du firewall** (1280 octets selon les recommandations de Stormshield).
7. Cochez également les deux cases **Mode Config** et **Mode Agressif**.

Ikev1GwConfig: Authentication

Authentication Protocol Gateway Certificate

**Identity**

Local ID Email john.doe@stormshield.eu

Remote ID

**Advanced features**

Fragmentation  Fragment size 1280

IKE Port   Enable NATT offset

NAT Port

Mode Config

Aggressive Mode  NAT-T Automatic

8. Dans l'onglet **Authentification** > **Adresse routeur distant** > champ **Adresse routeur distant**, indiquez l'adresse IP (adresse IP publique) ou le FQDN du firewall avec lequel le client VPN doit établir un tunnel.  
Si vous utilisez un FQDN, assurez-vous que celui-ci soit résolu par les serveurs DNS du poste de travail avant l'établissement du tunnel.



- Dans l'onglet **Authentification** > **Authentification** > champ **Clé Partagée**, saisissez et confirmez la **clé pré-partagée définie sur le firewall pour cet utilisateur**.

Ikev1GwConfig: Authentication

Authentication Protocol Gateway Certificate

**Remote Gateway**

Interface Any

Remote Gateway 192.168.1.41

**Authentication**

Preshared Key

Confirm

Certificate

**X-Auth**

Enabled  X-Auth Popup

Login

Password

Once  Hybrid Mode

**Cryptography**

Encryption AES256

Authentication SHA-256

Key Group DH14 (2048)

- Cliquez sur le menu supérieur **Configuration** > **Sauver** pour enregistrer cette configuration.

## Configurer la phase 2

- Dans l'arborescence **Configuration VPN** > **IKEv1**, faites un clic droit sur la phase 1 précédemment créée (*IKEv1GwConfig* dans l'exemple).
- Sélectionnez **Nouvelle Phase 2**.  
Une entrée nommée par défaut *Ikev1Tunnel* est ajoutée sous la phase 1 sélectionnée.
- Faites un clic droit sur *Ikev1Tunnel* et choisissez **Renommer** pour donner le nom souhaité à cette entrée.
- Dans l'onglet **IPsec** > **Adresses** > champ **Type d'adresse**, sélectionnez **Adresse réseau**.
- Dans le champ **Adresse réseau distant**, indiquez l'adresse du premier réseau joignable (192.168.1.0 dans l'exemple).



6. Dans le champ **Masque réseau**, indiquez le masque associé à ce réseau (255.255.255.0 dans l'exemple).

Ikev1 Tunnel: IPsec

IPsec Advanced Automation Remote Sharing **IPV4**

**Addresses**

VPN Client address 0 . 0 . 0 . 0 ⓘ

Address type Subnet address

Remote LAN address 192 . 168 . 1 . 0

Subnet mask 255 . 255 . 255 . 0

**ESP**

Encryption AES256

Authentication SHA-256

Mode Tunnel

**PFS**

PFS Group DH14 (2048)

**Lifetime**

IPsec Lifetime 1800 sec.

Le client VPN est configuré pour établir un tunnel IKEv1 en mode *Config* avec le firewall.

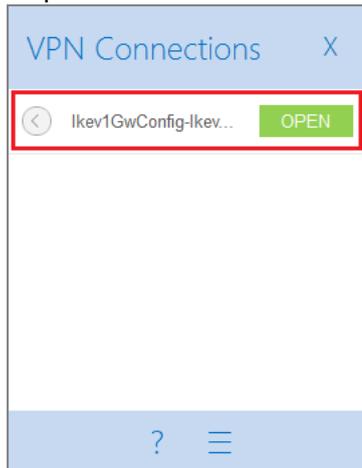
## Établir le tunnel VPN IPsec depuis le poste client

Sur le poste de travail Microsoft Windows de l'utilisateur :

1. Faites un clic droit sur l'icône présente dans la barre des tâches Windows [icônes cachées] : 
2. Sélectionnez le menu **Panneau des connexions**.
3. Repérez la connexion créée dans les étapes précédentes (*Ikev1GwConfig-Ikev1Tunnel* dans l'exemple).



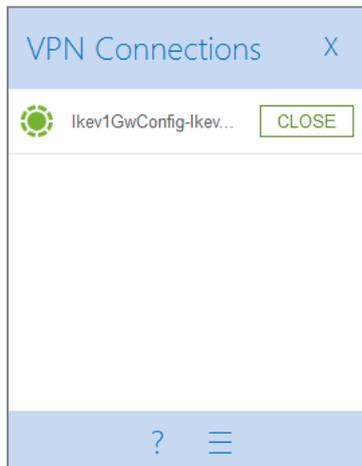
4. Cliquez sur le bouton **Ouvrir** :



Le tunnel s'établit.

Il apparaît précédé d'une icône verte et le bouton associé indique désormais l'action

**Fermer** :



5. Vous pouvez fermer la fenêtre des connexions (clic sur la croix) sans craindre de fermer le tunnel.

## Fermer un tunnel depuis le poste client

Sur le poste de travail Microsoft Windows de l'utilisateur :

1. Faites un clic droit sur l'icône présente dans la barre des tâches Windows (icônes cachées) : 
2. Sélectionnez le menu **Panneau des connexions**.
3. Repérez le tunnel à fermer (*Ikev1GwConfig-Ikev1Tunnel* dans l'exemple).
4. Cliquez sur le bouton **Fermer**.



# Mettre en œuvre une configuration pour une politique IPsec mobile en mode standard

Dans cette configuration, les utilisateurs nomades établissent le tunnel avec une adresse IP renseignée dans leur client VPN.

Pour définir une politique IPsec mobile en mode standard (pas de mode *Config*), les étapes de configuration du firewall sont les suivantes :

- Définir un objet réseau regroupant les adresses IP attribuées aux utilisateurs nomades lors de l'établissement du tunnel VPN IPsec.
- Définir un ou plusieurs(s) objet(s) réseau correspondant au(x) réseau(x) accessible(s) aux utilisateurs nomades lors de l'établissement du tunnel VPN IPsec.
- Créer le profil des correspondants IPsec IKEv1,
- Créer la politique IPsec IKEv1 utilisant le profil de correspondants défini précédemment,
- Mettre en place les règles de filtrage autorisant les flux depuis les clients mobiles vers le réseau interne.

## Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles

Notez bien que si  $n$  réseaux non contigus (c'est à dire ne pouvant pas être rassemblés dans une plage d'adresses IP ou dans un seul et même réseau) doivent être joignables par les clients VPN :

- Il sera nécessaire de configurer  $n$  phases 2 sur chaque client VPN,
- Chaque client VPN aura ainsi besoin de  $n$  adresses IP.

Cela impacte donc directement la taille du réseau dédié aux clients VPN.

## Définir l'objet réseau

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

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réseau**.
3. Attribuez un **Nom** à cet objet (*Mobile\_Users\_Network* dans l'exemple).
4. Renseignez le champ **Adresse IP de réseau** sous la forme réseau/masque.  
Ce réseau doit contenir au moins autant d'adresses IP que d'utilisateurs susceptibles de se connecter via un tunnel VPN IPsec.

### Exemples :

192.168.9.0/24 ou 192.168.9.0/255.255.255.0 : 254 adresses donc 254 phases 2.  
192.168.9.0/23 ou 192.168.9.0/255.255.254.0 : 510 adresses donc 510 phases 2.

5. Cliquez sur **Créer**.

## Définir le ou les objet(s) réseau représentant le(s) réseau(x) accessible(s) aux correspondants mobiles

Les utilisateurs mobiles peuvent avoir à accéder à un ou plusieurs réseaux protégés par le firewall.



Pour les besoins de l'exemple présenté dans ce tutoriel, considérons que les clients mobiles peuvent accéder via IPsec à deux réseaux distincts et non contigus : le réseau 192.168.1.0/24 et le réseau 192.168.128.0/24. Cette configuration nécessite donc de créer deux objets de type réseau.

Il est en effet nécessaire de créer autant d'objets réseau que le nombre de réseaux non contigus joignables par les clients VPN.

## Créer le premier objet réseau

Dans le module **Configuration** > **Objets** > **Objets réseau**, créez le premier objet réseau :

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réseau**.
3. Attribuez un **Nom** à cet objet (*Local\_Network\_Authorized\_IPsec* dans l'exemple).
4. Renseignez le champ **Adresse IP de réseau** (sous la forme réseau/masque) avec le premier réseau protégé accessible aux utilisateurs mobiles : 192.168.1.0/24 ou 192.168.1.0/255.255.255.0.
5. Cliquez sur **Créer**.

## Créer le second objet réseau

En suivant la méthode décrite pour le premier objet réseau, créez le second objet réseau nommé *Local\_Network\_Authorized\_IPsec2* dans l'exemple et correspondant au réseau 192.168.128.0/24 (ou 192.168.128.0/255.255.255.0).

Notez bien que ces deux objets réseaux peuvent être regroupés dans un objet de type groupe. Pour les besoins de l'exemple, nous ne les regroupons pas volontairement afin de bien visualiser que plusieurs réseaux destination peuvent être sélectionnés lors de la [création de la politique mobile IPsec standard](#).

## Rappel

Si  $n$  réseaux non contigus (c'est à dire ne pouvant pas être rassemblés dans une plage d'adresses IP ou dans un seul et même réseau) doivent être joignables par les clients VPN :

- Il sera nécessaire de configurer  $n$  phases 2 sur chaque client VPN,
- Chaque client VPN aura ainsi besoin de  $n$  adresses IP.

Cela impacte donc directement la [taille du réseau dédié aux clients VPN](#).

## Créer le profil des correspondants VPN IPsec

Dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants** :

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Nouveau correspondant mobile (nomade) IKEv2** ou **Nouveau correspondant anonyme (nomade) IKEv2** (jusque SNS v3.7.11-LTSB et SNS 3.10.1).
3. Donnez un nom à la configuration nomade (*IKEv1\_Mobile\_Users* dans l'exemple) puis cliquez sur **Suivant**.
4. Pour l'**Authentification du correspondant**, choisissez **Clé pré-partagée (PSK)** puis cliquez sur **Suivant**.
5. Dans le tableau d'**Identification des correspondants**, cliquez sur **Ajouter**.
6. Dans le champ **Identifiant**, saisissez l'adresse e-mail du correspondant.



7. Dans les champs **Clé pré-partagée (ASCII)** et **Confirmer**, tapez le mot de passe servant à établir le tunnel VPN IPsec pour ce correspondant.  
Pour des raisons évidentes de sécurité, choisissez des mots de passe uniques et respectant les [recommandations de l'ANSSI](#).
8. Cliquez sur **OK**.
9. Répétez les étapes 5 à 8 pour chacun des utilisateurs mobiles autorisés.
10. Cliquez sur **Suivant**.  
Une fenêtre résume le nom du correspondant, la politique et le type d'authentification choisie.
11. Validez en cliquant sur **Terminer**.
12. Sélectionnez le correspondant précédemment créé et remplissez le champ **Local ID**.  
Il s'agit en général du nom DNS (FQDN) du firewall. Exemple : *vpn-gw.stormshield.eu*.
13. Cliquez sur **Enregistrer** puis sur **Sauvegarder**.
14. Cliquez sur **Activer la politique**.

Le profil des correspondants mobiles IPsec obtenu est donc le suivant :

The screenshot shows the 'IPSEC VPN' configuration page in the Stormshield management console. The 'PEERS' tab is active, displaying a list of peers on the left and configuration details for the selected peer 'Peer:IKEv1\_Mobile\_Users' on the right.

**Peer List:**

Name
IKEv1_Mobile_Users

**Peer Configuration Details:**

- Peer: IKEv1\_Mobile\_Users
- Comment: (empty)
- Remote gateway: Any
- Backup configuration: None
- IKE profile: StrongEncryption
- IKE version: IKEv1
- Identification:**
  - Authentication method: Pre-shared key (PSK)
  - Certificate: No certificate
  - Local ID (Optional): vpn-gw.stormshield.eu
  - [Click here to edit the PSK list](#)
- Advanced properties:**
  - Negotiation mode: aggressive
  - Backup mode: temporary
  - Local address: Any
  - Do not initiate the tunnel (Responder only):
  - DPD: Passive

## Ajouter des clés pré-partagées (PSK) à une politique existante

Dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Identification** :

1. Cliquez sur le bouton **Ajouter** du tableau **Tunnels nomades : clés pré-partagées**.
2. Dans le champ **Identifiant**, saisissez l'adresse e-mail du correspondant.



3. Dans les champs **Clé pré-partagée (ASCII)** et **Confirmer**, tapez le mot de passe servant à établir le tunnel VPN IPsec pour ce correspondant.  
Pour des raisons évidentes de sécurité, choisissez des mots de passe uniques et respectant les [recommandations de l'ANSSI](#).
4. Cliquez sur **OK**.
5. Répétez les étapes 1 à 4 pour chacune des PSK à ajouter.

Exemple de table de clés pré-partagées :

MOBILE TUNNELS: PRE-SHARED KEYS	
Identity	Key
felix.thecat@stormshield.eu	0x40506f756e657474653039
john.doe2@stormshield.eu	0x40506f756e657474653037
john.doe@stormshield.eu	0x506f756e657474653034

## Créer la politique IPsec

Dans le module **Configuration > VPN > VPN IPsec > onglet Politique de chiffrement - Tunnels** :

1. Dans la liste déroulante, sélectionnez la politique IPsec que vous souhaitez modifier (*IPsec 01* dans l'exemple).
2. Cliquez sur l'onglet **Mobile - Utilisateurs Nomades** (ou **Anonyme - Utilisateurs Nomades**).
3. Cliquez sur **Ajouter**.
4. Sélectionnez **Nouvelle politique**.  
Un assistant de configuration se lance.
5. Dans le champ **Correspondant nomade utilisé**, choisissez le profil nomade créé précédemment (*IKEv1\_Mobile\_Users* dans l'exemple).
6. Dans le champ **Ressources locales**, sélectionnez les réseaux (ou le groupe de réseaux) auxquels les utilisateurs nomades peuvent accéder au travers du tunnel VPN IPsec (les objets *Local\_Network\_Authorized\_IPsec* et *Local\_Network\_Authorized\_IPsec2* précédemment créés dans l'exemple).
7. Cliquez sur **Terminer**.  
Dans la zone **Vérification de la politique**, l'avertissement *L'authentification par clé pré-partagée en mode agressif dégrade fortement le niveau de sécurité* est affiché.
8. Cliquez sur **Enregistrer** puis validez en cliquant sur **Sauvegarder**.



9. Cliquez sur **Oui, activer la politique.**

La politique IPsec obtenue est donc la suivante :

Line	Stat...	Local network	Mobile network	Encryption profile	Config mode	Comment
1	on	Local_Network_Authorized_IPSec2	Any	StrongEncryption	off	
2	on	Local_Network_Authorized_IPSec	Any	StrongEncryption	off	

## Autoriser les accès VPN IPsec dans la politique de filtrage

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

1. Dans la grille de filtrage, sélectionnez la ligne au-dessous de laquelle vous souhaitez ajouter la règle autorisant le VPN IPsec pour les nomades.
2. Cliquez sur **Nouvelle règle.**
3. Sélectionnez **Règle simple.**  
Une nouvelle ligne est ajoutée.
4. Sur la ligne nouvellement ajoutée, faites un double-clic dans la cellule correspondant à la colonne **Action.**  
La fenêtre de configuration de la règle s'ouvre.  
La section **Action** (menu de gauche de cette fenêtre de configuration) est automatiquement sélectionnée.
5. Dans le champ **Action**, sélectionnez **passer.**
6. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Source.**
7. Dans le champ **Utilisateur**, sélectionnez le groupe d'utilisateurs autorisés à établir un tunnel VPN IPsec.
8. Cliquez sur l'onglet **Configuration avancée** de cette section **Section.**
9. Pour le champ **via**, sélectionnez **Tunnel VPN IPsec.**
10. Pour le champ **Méthode d'authentification**, sélectionnez **VPN IPSEC.**
11. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Destination.**
12. Cliquez sur le bouton **Ajouter** de la grille des **Machines destinations.**
13. Sélectionnez les réseaux auxquels les utilisateurs nomades peuvent accéder au travers du tunnel VPN IPsec (objets *Local\_Network\_Authorized\_IPsec* et *Local\_Network\_Authorized\_IPsec2* dans l'exemple).
14. Dans le menu de gauche de cette fenêtre, sélectionnez la section **Inspection.**
15. Dans le champ **Profil d'inspection**, sélectionnez le profil IPS contenant le profil TCP-UDP avec l'option MSS (*IPS\_03* dans l'exemple).
16. Cliquez sur **OK.**
17. Faites un double-clic dans la cellule correspondant à la colonne **État** afin d'activer cette règle.  
Son état passe à **ON.**

La règle de filtrage obtenue est donc la suivante :

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass	Mobile Users Auth. by:IPSec VPN via IPSec VPN tunnel	Local_Network_Authorized_IPSec Local_Network_Authorized_IPSec2	Any		IPS (IPS_03)



## Configurer le client VPN

Sur le poste de travail Microsoft Windows de l'utilisateur, lancez la fenêtre des connexions du client VPN :

1. Faites un clic droit sur l'icône présente dans la barre des tâches Windows [icônes cachées] : 
2. Sélectionnez le menu **Panneau des connexions**.

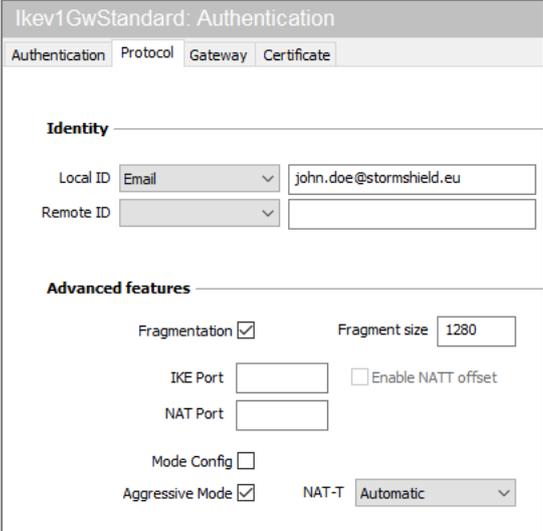
Pour les besoins de l'exemple présenté dans ce tutoriel, nous avons considéré que les clients mobiles pouvaient accéder via IPsec à deux réseaux distincts et non contigus : le réseau 192.168.1.0/24 et le réseau 192.168.128.0/24.

Cette configuration nécessitera donc de créer deux phases 2 distinctes, une pour chacun des réseaux. Il est en effet nécessaire de créer autant de phases 2 que le nombre de réseaux non contigus joignables par les clients VPN.

Notez bien que chacune de ces phases 2 utilisera une adresse IP distincte de client VPN.

## Configurer la phase 1

1. Dans l'arborescence **Configuration VPN**, faites un clic droit sur **IKEv1**.
2. Sélectionnez **Nouvelle phase 1**.  
Une entrée nommée par défaut *Ikev1Gateway* est ajoutée à l'arborescence **IKEv1**.
3. Faites un clic droit sur *Ikev1Gateway* et choisissez **Renommer** pour donner le nom souhaité à cette entrée (*Ikev1GwStandard* dans l'exemple).
4. Cliquez sur cette entrée.
5. Dans l'onglet **Protocole** > **Identité** > champ **Local ID** sélectionnez **E-mail** dans la liste déroulante et indiquez l'adresse e-mail de l'utilisateur du poste de travail.
6. Dans l'onglet **Protocole** > **Fonctions avancées**, cochez la case **Fragmentation** et indiquez la **taille des fragments IKE tels que définis au niveau du firewall** (1280 octets selon les recommandations de Stormshield).
7. Cochez également la case **Mode Agressif**.



The screenshot shows the configuration window for 'Ikev1GwStandard: Authentication'. It has four tabs: 'Authentication', 'Protocol', 'Gateway', and 'Certificate'. The 'Authentication' tab is active. Under the 'Identity' section, 'Local ID' is set to 'Email' with the value 'john.doe@stormshield.eu'. Under 'Advanced features', 'Fragmentation' is checked with a 'Fragment size' of 1280. 'IKE Port' and 'NAT Port' are empty. 'Mode Config' is unchecked. 'Aggressive Mode' is checked. 'NAT-T' is set to 'Automatic'.

8. Dans l'onglet **Authentification** > **Adresse routeur distant** > champ **Adresse routeur distant**, indiquez l'adresse IP (adresse IP publique) ou le FQDN du firewall avec lequel le client VPN doit établir un tunnel.  
Si vous utilisez un FQDN, assurez-vous que celui-ci soit résolu par les serveurs DNS du poste de travail avant l'établissement du tunnel.



9. Dans l'onglet **Authentification** > **Authentification** > champ **Clé Partagée**, saisissez et confirmez la **clé pré-partagée définie sur le firewall pour cet utilisateur**.

Ikev1GwStandard: Authentication

Authentication Protocol Gateway Certificate

**Remote Gateway**

Interface Any

Remote Gateway 192.168.1.41

**Authentication**

Preshared Key

Confirm

Certificate

**X-Auth**

Enabled  X-Auth Popup

Login

Password

Once  Hybrid Mode

**Cryptography**

Encryption AES256

Authentication SHA-256

Key Group DH14 (2048)

10. Cliquez sur le menu supérieur **Configuration** > **Sauver** pour enregistrer cette configuration.

## Configurer la phase 2 pour le premier réseau

1. Dans l'arborescence **Configuration VPN** > **IKEv1**, faites un clic droit sur la phase 1 précédemment créée (*Ikev1GwStandard* dans l'exemple).
2. Sélectionnez **Nouvelle Phase 2**.  
Une entrée nommée par défaut *Ikev1Tunnel* est ajoutée sous la phase 1 sélectionnée.
3. Faites un clic droit sur *Ikev1Tunnel* et choisissez **Renommer** pour donner le nom souhaité à cette entrée (*Ikev1Net1Tunnel* dans l'exemple).
4. Dans l'onglet **IPsec** > **Adresses** > champ **Adresse du client VPN**, renseignez l'adresse IP du client (192.168.9.1 dans l'exemple). Cette adresse doit faire partie du réseau défini dans la section **Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles**.
5. Dans l'onglet **IPsec** > **Adresses** > champ **Type d'adresse**, sélectionnez **Adresse réseau**.
6. Dans le champ **Adresse réseau distant**, indiquez l'adresse du premier réseau joignable (192.168.1.0 dans l'exemple).



7. Dans le champ **Masque réseau**, indiquez le masque associé à ce réseau (255.255.255.0 dans l'exemple).

Ikev1Net1 Tunnel: IPsec

IPsec | Advanced | Automation | Remote Sharing | **IPV4**

**Addresses**

VPN Client address: 192 . 168 . 9 . 1

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

**ESP**

Encryption: AES256

Authentication: SHA-256

Mode: Tunnel

**PFS**

PFS Group: DH14 (2048)

**Lifetime**

IPsec Lifetime: 1800 sec.

8. Dans l'onglet **Avancé** > **Serveurs alternatifs**, vous pouvez si nécessaire définir un **Suffixe DNS** et des **Serveurs (DNS) alternatifs** à utiliser pour ce tunnel VPN IPsec.

Le tunnel pour joindre le premier des deux réseaux de l'exemple est configuré.

## Configurer la phase 2 pour le second réseau accessible

Appliquez la méthode décrite dans la section [Configurer la phase 2 pour le premier réseau](#) pour définir le tunnel permettant d'accéder au second réseau.

Dans l'exemple donné, les paramètres utilisés pour ce second tunnel sont les suivants :

- Nom de phase 2 : *Ikev1Net2Tunnel*
- Adresse IP du client : 192.168.9.2
- Adresse IP du réseau : 192.168.128.0
- Masque : 255.255.255.0

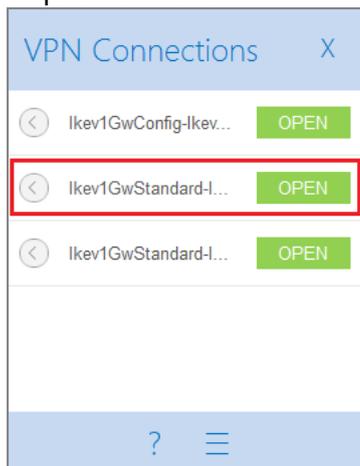
## Établir un tunnel VPN IPsec depuis le poste client

Sur le poste de travail Microsoft Windows de l'utilisateur :

1. Faites un clic droit sur l'icône présente dans la barre des tâches Windows (icônes cachées) :
2. Sélectionnez le menu **Panneau des connexions**.
3. Repérez la première connexion créée dans les étapes précédentes (*Ikev1GwStandard-Ikev1Net1Tunnel* dans l'exemple).



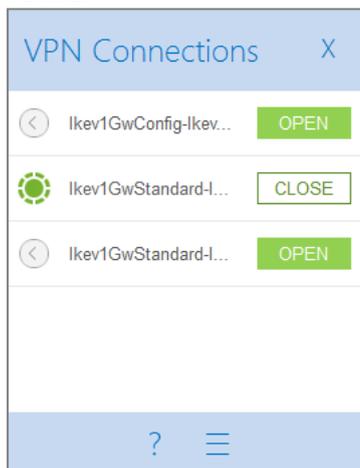
4. Cliquez sur le bouton **Ouvrir** :



Le tunnel s'établit.

Il apparaît précédé d'une icône verte et le bouton associé indique désormais l'action

**Fermer** :



5. Vous pouvez fermer la fenêtre des connexions (clic sur la croix) sans craindre de fermer le tunnel.

Répétez les étapes 2 à 4 pour ouvrir le second tunnel.

## Fermer un tunnel depuis le poste client

Sur le poste de travail Microsoft Windows de l'utilisateur :

1. Faites un clic droit sur l'icône présente dans la barre des tâches Windows (icônes cachées) : 
2. Sélectionnez le menu **Panneau des connexions**.
3. Repérez le tunnel à fermer (*Ikev1GwStandard-Ikev1Net1Tunnel* dans l'exemple).
4. Cliquez sur le bouton **Fermer**.



## Afficher les détails d'un tunnel sur le firewall

Le module **Supervision > Supervision des tunnels IPsec** permet de visualiser les **tunnels établis** ainsi que différentes **informations et statistiques** les concernant :

- Nom de la passerelle locale (firewall),
- Durée écoulée depuis l'établissement du tunnel,
- Octets émis par le firewall,
- Octets reçus par le firewall,
- État du tunnel,
- Algorithme de chiffrement utilisé,
- Algorithme d'authentification utilisé.

The screenshot shows the 'IPSEC VPN TUNNEL MONITORING' interface. It includes a 'Refresh' button, a 'Policies' section with a search filter, and a table of policies. Two policies are highlighted with a green border, each showing '1 Tunnel(s)'. Below this is a 'Tunnels' section with a checkbox to filter by policy and a table showing tunnel statistics for the 'Firewall\_bridge'.

State	Local network name	Local gateway name	Direction	Remote gateway name	Remote network name	From	ID
Policy: none	rfc5735_loopback		← in		any_v4		0
Policy: none	rfc4291_loopback		← in		any_v6		0
Policy: none	rfc5735_loopback		→ out		any_v4		0
Policy: none	rfc4291_loopback		→ out		any_v6		0
✓ 1 Tunnel(s)	Network_bridge_v4	Firewall_bridge	← in			1m	1
✓ 1 Tunnel(s)	Network_bridge_v4	Firewall_bridge	→ out			1m	1

Local gateway name	Remote gateway name	From	Bytes out	Bytes in	State	Encryption	Authenticat...
Firewall_bridge		1m of 30m used	868 B	787 B	mature	aes-cbc	hmac-sha256



## Pour aller plus loin

---

Des informations complémentaires et réponses à vos éventuelles questions 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.*