



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

VPN IPSEC MOBILE IKEV2 - AUTHENTIFICATION EAP AVEC CERTIFICAT

Produits concernés : SNS 4.8 et versions supérieures, SN VPN Client Exclusive 7.4 et versions supérieures

Dernière mise à jour du document : 9 juillet 2024

Référence : sns-fr-VPN_IPSec_Mobile_IKEv2_Authentification_EAP_Certificat_Note_Technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Prérequis	4
Limitations	4
Générer les identités des correspondants mobiles	5
Cas d'une PKI externe	5
Cas d'une PKI interne (PKI sur un firewall SNS)	5
Si la CA en charge des identités des correspondants mobiles doit être créée	5
Créer l'identité du firewall pour le VPN IPsec	6
Créer l'identité de chacun des correspondants	6
Exporter l'identité de chaque correspondant	7
Supprimer les clés privées des identités des correspondants sur le firewall (recommandé)	7
Autoriser les utilisateurs mobiles à établir un tunnel VPN IPsec	8
Créer un groupe contenant tous les utilisateurs autorisés à établir un tunnel VPN IPsec	8
Définir LDAP comme méthode d'authentification pour les utilisateurs nomades	8
Si aucune règle n'est présente dans la politique d'authentification	8
Si la politique d'authentification contient d'autres règles que celle nécessaire aux utilisateurs du VPN IPsec	9
Autoriser les utilisateurs mobiles à établir un tunnel VPN IPsec	10
Mettre en œuvre une configuration IPsec mobile	11
Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles	11
Créer les objets pour les ressources réseau accessibles aux correspondants mobiles	11
Créer le profil des correspondants VPN IPsec	12
Ajouter la CA ayant signé le certificat du firewall dans les autorités de confiance	13
Créer la politique IPsec	13
Politique mobile mode Config	13
Autoriser les accès VPN IPsec dans la politique de filtrage	14
Optimiser les flux ISAKMP lors de la négociation des tunnels IPsec et sécuriser l'authentification	14
Prérequis	15
Optimiser les flux liés aux tunnels en limitant les datagrammes IP	15
Recharger la politique IPsec pour prendre en compte les modifications précédentes	15
Optimiser les flux liés aux tunnels : limiter la MSS	15
Configurer le client VPN	16
Configurer la phase 1	16
Configurer la phase 2	17
Établir le tunnel VPN IPsec depuis le poste client	19
Afficher les détails des tunnels sur le firewall	21



Historique des modifications

Date	Description
9 juillet 2024	Nouveau document



Avant de commencer

Dans les versions antérieures à SNS 4.8, seuls les tunnels mobiles basés sur le protocole IKEv1 autorisaient une authentification multifacteur (MFA) pour les utilisateurs nomades par le biais de XAUTH : en effet, IKEv2 ne supporte pas la méthode XAUTH.

IKEv1 étant un protocole ancien, et l'ANSSI recommandant les solutions basées sur le protocole IKEv2 pour une sécurité accrue, la version SNS 4.8 introduit donc le support de l'authentification multifacteur (MFA) pour les tunnels nomades basé sur IKEv2 par le biais d'EAP (Extensible Authentication Protocol).

Cette authentification multifacteur peut être réalisée de deux manières :

- EAP-Generic Token Card : le correspondant mobile doit présenter un couple identifiant / mot de passe,
- Certificat et EAP-Generic Token Card : le correspondant mobile doit présenter un certificat et un couple identifiant / mot de passe.

NOTE

SN IPsec VPN Client Exclusive v7.4 ou supérieure doit être installé sur le poste client pour utiliser la compatibilité avec EAP.

Ce document décrit la configuration VPN nécessaire pour autoriser un utilisateur nomade à accéder au réseau interne de son entreprise via un tunnel mobile IPsec mode *Config* basé sur IKE v2 et utilisant la méthode Certificat et EAP-Generic Token Card. Le couple identifiant / mot de passe sont issus de l'annuaire LDAP interne du firewall.

Notez que les méthodes EAP-Generic Token Card et Certificat et EAP-Generic Token Card utilisent un couple identifiant / mot de passe qui peut être référencé dans un annuaire LDAP interne, un annuaire LDAP externe ou sur un serveur Radius par exemple.

Prérequis

- Les comptes utilisateurs utilisés pour le VPN IPsec sont déjà créés dans un annuaire LDAP configuré comme annuaire par défaut sur le firewall (annuaire interne dans ce document). La création d'un annuaire LDAP (interne ou externe) est décrite dans la section [Configuration des annuaires](#) du **Manuel Utilisateur SNS**.
- Une adresse e-mail doit être définie pour chaque utilisateur présent dans l'annuaire.
- Les postes clients Microsoft Windows doivent disposer du logiciel **SN VPN Client Exclusive**, 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 *Enterprise* [TheGreenBow](#).

Limitations

Les méthodes d'authentification Certificat et EAP-Generic Token Card ou EAP-Generic Token Card ne sont pas compatibles avec :

- Les tunnels basés sur IKEv1, qui doivent utiliser XAUTH pour une authentification multifacteur.
- Le mode Diffusion Restreinte (DR).



Générer les identités des correspondants mobiles

Cette section traite de la création des identités des utilisateurs nomades.

Elle suppose que les comptes des utilisateurs nomades sont déjà définis dans l'annuaire de référence pour le VPN IPsec (annuaire LDAP interne du firewall dans cet exemple).

Cas d'une PKI externe

Depuis l'autorité de certification (CA) en charge des identités des correspondants mobiles IPsec :

1. Générez les identités de tous les correspondants mobiles IPsec.
2. Exportez ces identités (certificat + clé privée).
3. Téléchargez l'identité de chaque correspondant mobile sur son poste de travail.

Cas d'une PKI interne (PKI sur un firewall SNS)

Si la CA en charge des identités des correspondants mobiles doit être créée

1. Placez-vous dans le module **Configuration > Objets > Certificats et PKI**.
2. Cliquez sur **Ajouter**
3. Sélectionnez **Autorité racine ou Sous-autorité** si cette CA est placée sous une CA racine de votre PKI.
Un assistant de création s'affiche.
4. Indiquez un **Nom** (EAP-IKEv2 dans cet exemple).
L'**Identifiant** se remplit automatiquement avec le nom de la CA. Vous pouvez le modifier.
5. Renseignez les **Attributs de l'autorité** :
 - Organisation [O],
 - Unité d'organisation [OU],
 - Ville [L],
 - État [ST],
 - Pays [C].



EXEMPLE

Organisation [O] : Stormshield
Unité d'organisation [OU] : Documentation
Ville [L] : Lille
État [ST] : Nord
Pays [C] : France

6. Cliquez sur **Suivant**.
7. Renseignez puis confirmez le **Mot de passe** protégeant la CA.
8. Vous pouvez indiquer une adresse **E-mail** de contact pour cette CA.
9. La durée de **Validité** proposée par défaut est de 3650 jours (valeur conseillée).
Vous pouvez la modifier.
10. **Type de clé** : il est recommandé de sélectionner une clé de type *SECP* ou *BRAINPOOL*.



11. Sélectionnez la **Taille de clé (bits)**.
12. Cliquez deux fois sur **Suivant**.
Un résumé des informations de la CA est affiché.
13. Validez en cliquant sur **Terminer**.
Si vous souhaitez définir cette CA comme CA par défaut du firewall :
 1. Sélectionnez cette CA,
 2. Cliquez sur le bouton **Actions** et choisissez **Définir comme défaut**.

Créer l'identité du firewall pour le VPN IPsec

Si l'identité du firewall utilisée pour le VPN IPsec n'existe pas :

1. Placez-vous dans le module **Configuration > Objets > Certificats et PKI**.
2. Sélectionnez la CA utilisée pour le VPN IPsec.
3. Cliquez sur **Ajouter** et sélectionnez **Identité serveur**.
4. Dans le champ **Nom de domaine qualifié (FQCN)**, saisissez le nom pour l'identité du firewall (exemple : *FW-EAP-IKEv2.stormshield.eu*).
L'**Identifiant** se remplit automatiquement avec le nom du correspondant. Vous pouvez le modifier.
5. Cliquez sur **Suivant**.
6. Renseignez le mot de passe de la CA signant cette identité.
7. Cliquez sur **Suivant**.
8. Sélectionnez une durée de **validité** en jours (365 jours proposés par défaut).
9. Sélectionnez le **Type de clé** : il est recommandé de sélectionner une clé de type *BRAINPOOL* ou *SECP*.
10. Sélectionnez une **Taille de clé**.
11. Cliquez deux fois sur **Suivant**.
Un résumé de l'identité s'affiche.
12. Cliquez sur **Terminer** pour valider la création de cette identité utilisateur.

Créer l'identité de chacun des correspondants

1. Placez-vous dans le module **Configuration > Objets > Certificats et PKI**.
2. Sélectionnez la CA utilisée pour le VPN IPsec.
3. Cliquez sur **Ajouter** et sélectionnez **Identité utilisateur**.
4. Dans le champ **Nom (CN)**, saisissez le nom du correspondant (exemple : *User1 EAP*).
L'**Identifiant** se remplit automatiquement avec le nom du correspondant. Vous pouvez le modifier.
5. Renseignez l'adresse e-mail du correspondant (*user1@stormshield.eu* dans cet exemple).

NOTE

Cette adresse e-mail doit être identique à celle définie pour le compte utilisateur utilisé pour la méthode EAP (annuaire interne dans cet exemple).

6. Cliquez sur **Suivant**.
7. Renseignez le mot de passe de la CA signant cette identité.



8. Cliquez sur **Suivant**.
 9. Sélectionnez une durée de **validité** en jours (365 jours proposés par défaut).
 10. Sélectionnez le **Type de clé** : il est recommandé de sélectionner une clé de type *BRAINPOOL* ou *SECP*.
 11. Sélectionnez une **Taille de clé**.
 12. Cliquez sur **Suivant**.
Un résumé de l'identité s'affiche.
 13. Cliquez sur **Terminer** pour valider la création de cette identité utilisateur.
- Répétez cette procédure pour chacun des correspondants mobiles.

Exporter l'identité de chaque correspondant

1. Placez-vous dans le module **Configuration > Objets > Certificats et PKI**.
 2. Sélectionnez l'identité utilisateur à exporter.
 3. Cliquez sur **Télécharger** : sélectionnez **Identité** puis **Au format P12**.
 4. Dans le champ **Entrez le mot de passe** : créez un mot de passe destiné à protéger le fichier P12.
 5. **Confirmez** ce mot de passe.
 6. Cliquez sur **Télécharger le certificat (P12)**.
 7. Enregistrez ce fichier au format P12 sur votre poste de travail.
Ce fichier devra être importé sur le poste de l'utilisateur lors du paramétrage de son tunnel dans SN VPN Client Exclusive.
- Répétez cette procédure pour exporter l'identité de chaque correspondant mobile.

Supprimer les clés privées des identités des correspondants sur le firewall (recommandé)

Lorsque le fichier P12 a été importé sur le poste du correspondant, il est fortement recommandé de supprimer la clé privée de l'identité de ce correspondant.

1. Placez-vous dans le module **Configuration > Objets > Certificats et PKI**.
2. Sélectionnez l'identité du correspondant pour lequel vous voulez supprimer la clé privée.
3. Cliquez sur **Action** : sélectionnez **Supprimer la clé privée**.
La clé privée est immédiatement supprimée.

Répétez cette procédure pour chacun des correspondants concernés.



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. Ce même groupe sera également utilisé dans la définition du profil de correspondant mobile.

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

NOTE

Dans le cas d'un annuaire externe, ce groupe devra être créé directement sur l'une des machines hébergeant l'annuaire.

1. Placez-vous dans le module **Configuration > Utilisateurs > Utilisateurs** :
2. Cliquez sur **Ajouter un groupe**.
3. Dans le champ **Nom du groupe**, saisissez un nom représentatif (exemple : *EAP-GTC-CERT Users*).
Vous pouvez ajouter une **Description**.
4. Cliquez sur **Ajouter**.
Une ligne s'ajoute dans la grille des membres du groupe.
5. Tapez les premières lettres de l'utilisateur à ajouter au groupe et sélectionnez l'utilisateur souhaité dans la liste proposée par le firewall.
6. Répétez les étapes 3 et 4 pour ajouter l'ensemble des utilisateurs à inclure dans ce groupe.
7. Lorsque tous les membres ont été ajoutés, cliquez sur **Appliquer**.
8. Validez en cliquant sur **Sauvegarder**.

Définir LDAP comme méthode d'authentification pour les utilisateurs nomades

Placez-vous dans le module **Configuration > Utilisateurs > Authentification > onglet Politique d'authentification**.

Si aucune règle n'est présente dans la politique d'authentification

Assurez-vous que :

- Le champ **Action à appliquer par défaut** est positionné sur **Autoriser**.
- Le champ **Méthode à appliquer par défaut** est positionné sur **LDAP**.



USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES

Search by user... + New rule X Delete Up Down Cut Copy Paste

Status	Action	Source	Methods (assess by order)
--------	--------	--------	---------------------------

Default action

Default action to apply Allow

Default method

Method to use if no rules match LDAP

Si la politique d'authentification contient d'autres règles que celle nécessaire aux utilisateurs du VPN IPsec

Ajoutez une règle d'authentification :

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

La règle d'authentification obtenue est la suivante :

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES

Search by user... + New rule X Delete Up Down Cut Copy Paste

	Status	Action	Source	Methods (assess by order)	One-time password	Comment
1	Enabled	Allow	EAP-GTC-CERT Users @stormshield.eu ipsec	1 LDAP	<input type="checkbox"/>	



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**.
2. Dans le champ **Utilisateur - Groupe** : sélectionnez le groupes d'utilisateurs dans la liste proposée par le firewall (*EAP-GTC-CERT Users* dans cet exemple).
3. Cliquez sur **OK**.
Une ligne s'ajoute dans la grille.
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** puis sur **Sauvegarder**.

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

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS

DETAILED ACCESS

PPTP SERVER

Searching...

+ Add

✕ Delete

↑ Up

↓ Down

	Status	User - user group	SSL VPN Portal	IPSEC	SSL VPN	Sponsorship
1	<div><div></div>Enabled</div>	<div><div></div>EAP-GTC-CERT Users@stormshield.eu</div>	<div><div></div>Block</div>	<div><div></div>Allow</div>	<div><div></div>Block</div>	<div><div></div>Block</div>



Mettre en œuvre une configuration IPsec mobile

Dans ce document, les utilisateurs nomades établissent le tunnel avec une adresse IP obtenue automatiquement par leur client VPN auprès du firewall (mode *Config*).

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,
- Ni d'un réseau impliqué dans la configuration d'un autre tunnel IPsec.

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

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réseau**.
3. Attribuez un **Nom** à cet objet (*IKEv2_EAP_CERT_Clients_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 simultanément 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 simultanées.

192.168.9.0/23 ou 192.168.9.0/255.255.254.0 : 510 adresses donc 510 phases 2 simultanées.

5. Cliquez sur **Créer**.

Créer les objets pour les ressources réseau accessibles aux correspondants mobiles

L'objet représentant les ressources accessibles au travers du tunnel IPsec peut être :

- Une machine : pour autoriser l'accès à une seule machine via le tunnel IPsec,
- Un réseau : pour autoriser l'accès à un seul réseau protégé du firewall via le tunnel IPsec,
- Un groupe de machines / réseaux : pour autoriser l'accès à un groupe de machines et / ou de réseaux protégés via le tunnel IPsec.

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

1. Cliquez sur **Ajouter**.
2. Sélectionnez le type d'objet (**Machine**, **Réseau** ou **Groupe**).
3. Attribuez un **Nom** à cet objet (groupe *IKEv2-EAP-CERT-NET-GRP-DST* dans cet exemple).



4. Selon le type d'objet :
 - Machine : renseignez le champ **Adresse IP v4**,
 - Réseau : 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),
 - Groupe : sélectionnez les objets (machines et / ou réseaux) à inclure dans le groupe.
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**.
3. Donnez un nom à la configuration nomade (*mobile_IKEv2_EAP_CERT* dans l'exemple), choisissez **IKEv2** dans le champ **Version IKE**, puis cliquez sur **Suivant**.
4. Pour **Type d'authentification**, choisissez **EAP-Generic Token Card (GTC)** puis cliquez sur **Suivant**.
5. Dans le champ **Certificat**, sélectionnez le certificat présenté par le firewall pour établir les tunnels avec ces correspondants mobiles (*FW-EAP-IKEv2.stormshield.eu* dans cet exemple).
6. Dans le tableau **Groupes**, cliquez sur **Ajouter** et sélectionnez le(s) groupe(s) d'utilisateurs nomades utilisant ce profil de correspondant (groupe *EAP-GTC-CERT Users* dans l'exemple).
7. Cliquez sur **Suivant**.
8. Validez en cliquant sur **Terminer**.
9. Sélectionnez le correspondant précédemment créé et remplissez le champ **Local ID**. Il s'agit en général du nom DNS (FQDN) du firewall présent dans son certificat. Dans cet exemple : *FW-EAP-IKEv2.stormshield.eu*.
10. Cliquez sur **Appliquer** puis sur **Sauvegarder**.
11. Cliquez sur **Oui, activer la politique**.

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

The screenshot displays the Stormshield configuration interface for VPN IPsec. The 'PEERS' tab is active, showing a list of mobile peers on the left and the configuration details for 'MOBILE_IKEV2_EAP_CERT' on the right.

Left Panel (Mobile peers):

- Search bar: Enter a filter
- Buttons: + Add, Actions
- Section: Mobile peers (1)
- Peer: mobile_IKEv2_EAP_CERT

Right Panel (Configuration for MOBILE_IKEV2_EAP_CERT):

General

- Comment: [Empty text field]
- Remote gateway: Any
- Local address: Any
- IKE profile: StrongEncryption
- IKE version: IKEv2

Identification

- Authentication method: Certificate and EAP-Generic Token Card (GTC)
- Certificate: EAP-IKEv2:FW-EAP-IKEv2.stormshield.eu
- Local ID: FW-EAP-IKEv2.stormshield.eu
- Peer ID: Enter an ID (optional)

GROUPS

- Buttons: + Add, Delete, Up, Down
- Group 1: EAP-GTC-CERT Users@stormshield.eu



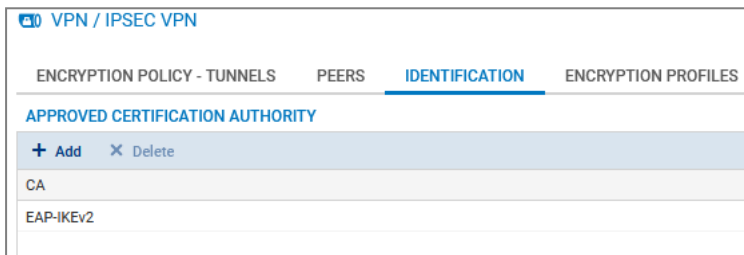
Ajouter la CA ayant signé le certificat du firewall dans les autorités de confiance

NOTE

Si la CA provient d'une PKI externe, son certificat devra au préalable être importé dans le module **Certificats et PKI** du firewall.

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

1. Dans le tableau **Autorités de certification acceptées**, cliquez sur le bouton **Ajouter**.
2. Sélectionnez la CA ayant signé le certificat du firewall (*EAP-IKEv2* dans cet exemple).
3. Cliquez sur **Appliquer** puis sur **Sauvegarder** pour enregistrer cette modification.



Créer la politique IPsec

1. Placez-vous dans le module **Configuration > VPN > VPN IPsec > onglet Politique de chiffrement - Tunnels**
2. Sélectionnez la politique IPsec que vous souhaitez modifier (*IPsec 01* dans l'exemple).
3. Cliquez sur l'onglet **Mobile - Utilisateurs Nomades**.

Politique mobile mode Config

1. Cliquez sur **Ajouter** et sélectionnez **Nouvelle politique mobile Mode Config**. Un assistant de configuration se lance.
2. Dans le champ **Ressources locales**, sélectionnez l'objet correspondant aux ressources (machine, réseau ou groupe de machine / réseaux) accessibles aux utilisateurs nomades au travers du tunnel VPN IPsec. Dans l'exemple il s'agit d'un groupe de réseaux nommé *IKEv2_EAP_LOCAL_NET_GRP*.
3. Dans le champ **Choix du correspondant**, choisissez le profil nomade créé précédemment (*mobile_IKEv2_EAP_CERT* dans cet exemple).
4. Dans le champ **Réseaux distants**, sélectionnez l'objet réseau créé à l'étape [Définir un objet réseau contenant les adresses IP attribuées aux correspondants mobiles](#) (*IKEv2_EAP_CERT_Clients_Network* dans cet exemple).
5. Cliquez sur **Terminer**.
6. Faites un double clic dans la colonne **État** pour activer la règle.
7. Cliquez sur **Appliquer** puis sur **Sauvegarder** pour valider et activer cette configuration.
8. Cliquez sur **Oui, activer la politique**.

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

SITE TO SITE (GATEWAY-GATEWAY)									
MOBILE - MOBILE USERS									
Q	Enter a filter	+ Add	X Delete	Up	Down	Cut	Copy	Paste	Show details
	Status	Name	Local network	Peer	Remote network	Protocol	Encryption profile	Config mode	
1	on	18e8a9e6a6e1	IKEv2_EAP_LOCAL_NET_GRP	mobile_IKEv2_EAP_CERT	IKEv2_EAP_CERT_Clients_Network	All	StrongEncryption	on	



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 (*EAP-GTC-CERT Users@stormshield.eu* dans cet 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 (groupe *IKEv2_EAP_LOCAL_NET_GRP* 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 **Appliquer** 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	EAP-GTC-CERT Users Auth. by:IPsec VPN via IPsec VPN tunnel	IKEv2_EAP_LOCAL_NET_GRP	Any		IPS (IPS_03)

Optimiser les flux ISAKMP lors de la négociation des tunnels IPsec et sécuriser l'authentification

Il est recommandé de modifier plusieurs paramètres du firewall afin d'optimiser les flux ISAKMP de la négociation des tunnels IPsec et de sécuriser l'authentification.



Prérequis

Pour les besoins des exemples, les optimisations et sécurisations recommandées supposent que la politique IPsec utilisée sur le firewall pour les utilisateurs mobiles est la politique *IPsec_01* (module **Configuration** > **VPN** > **VPN IPsec**).

Optimiser les flux liés aux tunnels en limitant les datagrammes IP

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. Placez-vous 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 (*mobile_IKEv2_EAP_CERT* 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`

Recharger la politique IPsec pour prendre en compte les modifications précédentes

1. Placez-vous dans le module **Configuration** > **Système** > **Console CLI**.
2. Rechargez la politique IPsec en tapant la commande :
`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** > **protocoles IP** > **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 est sélectionné automatiquement dans le profil global portant le même indice (03 dans l'exemple) et qui est appliqué dans la règle destinée à [Autoriser les accès VPN IPsec dans la politique de filtrage](#).
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**.

Configurer le client VPN

Sur le poste de travail Microsoft Windows de l'utilisateur, lancez la fenêtre des connexions du client VPN Exclusive en utilisant les droits Administrateur :

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

Configurer la phase 1

1. Dans l'arborescence **Configuration VPN**, faites un clic droit sur **IKEv2**.
2. Sélectionnez **Nouvel IKE auth**.
Une entrée nommée par défaut *Ikev2Gateway* est ajoutée à l'arborescence **IKEv2**.
3. Faites un clic droit sur *Ikev2Gateway* et choisissez **Renommer** pour donner le nom souhaité à cette entrée (*IKEv2GwEAPCERT* dans cet exemple).
4. Cliquez sur cette entrée.
5. 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.
6. Dans l'onglet **Authentification** > **Intégrité**, cochez les cases :
 - **EAP**,
 - **EAP popup**,
 - **Multiple AUTH support**.
7. Cliquez sur Importer un certificat et cochez **Format P12**.
8. Sélectionnez le **Certificat P12** de l'utilisateur déposé préalablement sur le poste de l'utilisateur.



- Entrez le mot de passe de protection du P12 défini lors de l'export de l'identité utilisateur sur le firewall et validez en cliquant sur **OK**.

IKEv2GwEAPCERT: IKE Auth

Authentication | Protocol | Gateway | Certificate

Remote Gateway

Interface: Any

Remote Gateway: 172.20.155.1

Integrity

☐ Preshared Key

Confirm

☐ Certificate

☒ EAP

☒ EAP popup

Login

Password

☒ Multiple AUTH support

Cryptography

Encryption: AES CBC 256

Integrity: SHA2 256

Key Group: DH14 (MODP 2048)

- 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).

IKEv2GwEAPCERT: IKE Auth

Authentication | Protocol | Gateway | Certificate

Identity

Local ID: DER ASN1 DN | mailAddress = user1@stormshield.eu

Remote ID

Advanced features

Fragmentation ☒ Fragment size: 1280

IKE Port: 500 ☐ Enable NATT offset

NAT Port: 4500

Childless ☐

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

Configurer la phase 2

- Dans l'arborescence **Configuration VPN > IKEv2**, faites un clic droit sur la phase 1 précédemment créée (*IKEv2GwEAPCERT* dans l'exemple).
- Sélectionnez **Nouveau Child SA**.
Une entrée nommée par défaut *Ikev2Tunnel* est ajoutée sous la phase 1 sélectionnée.
- Faites un clic droit sur *Ikev2Tunnel* et choisissez **Renommer** pour donner le nom souhaité à cette entrée.
- Dans l'onglet **Child SA > Trafic sélecteurs**,



5. Cochez la case **Obtenir la configuration depuis la passerelle**.
6. Cliquez sur le menu supérieur **Configuration** > **Sauver** pour enregistrer cette configuration.

IKEv2GwEAPCERT: Child SA

Child SA | Advanced | Automation | Remote Sharing

Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☒ Request configuration from the gateway

Cryptography

Encryption: Auto

Integrity: Auto

Diffie-Hellman: Auto

Extended Sequence Number: Automatique

Lifetime


Child SA Lifetime: 3600 sec.

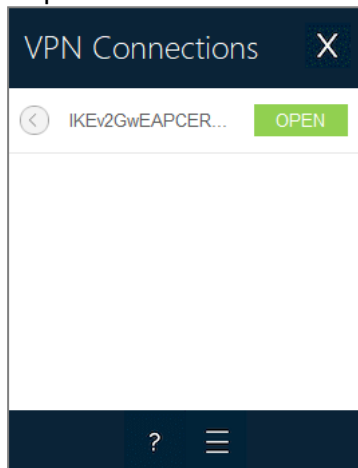
Le client VPN est configuré pour établir avec le firewall un tunnel IKEv2 en mode *Config* basé sur EAP et Certificat.



Établir le tunnel VPN IPsec depuis le poste client

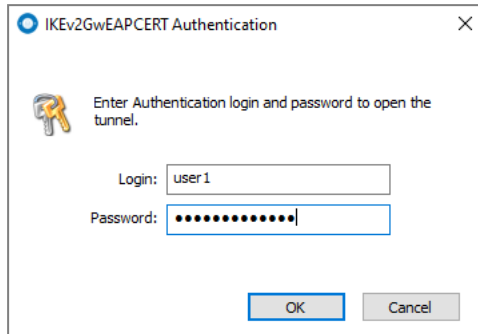
Sur le poste de travail Microsoft Windows de l'utilisateur :

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 (*IKEv2GwEAPCERT* dans l'exemple).
4. Cliquez sur le bouton **Ouvrir** :



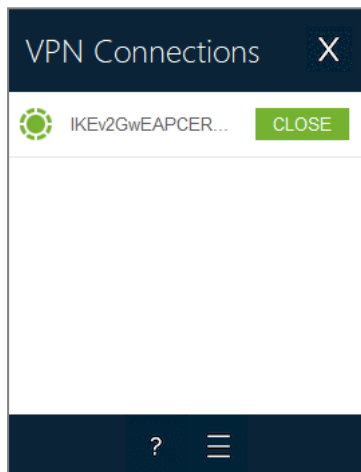


5. Saisissez l'identifiant et le mot de passe définis dans l'annuaire de référence (utilisateur *user1* de l'annuaire interne du firewall dans l'exemple).



Le tunnel s'établit.

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



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



Afficher les détails des tunnels 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.

MONITOR / IPSEC VPN TUNNELS

Refresh

Configure the IPsec VPN service

POLICIES

Type	Status	Local traffic endpoint	Local gateway	Local ID	Remote gateway	Peer ID	Remote traffic endpoint	PPK protection
Type : Mobile tunnels (2)								
		Network_in		FW-EAP-IKEv2.stormshield.eu	N/A	%any		Not required
		Network_dmz1		FW-EAP-IKEv2.stormshield.eu	N/A	%any		Not required

Security Association (SA) IKE

Status	established	Local ID	Anonymized	Authentication	sha2_256	PPK protection	Disabled
Local gateway	Anonymized	Peer ID	Anonymized	Encryption	aes/256		
Remote gateway		Lifetime	lapsed 3m	PRF	sha256		
Side	responder	NAT-T	none	PFS	14		

Security Association (SA) IPsec

Status	installed	Bytes in		Authentication	hmac_sha256
Local gateway	Anonymized	Bytes out		Encryption	aes/256
Remote gateway		Lifetime	lapsed 3m	ESN	Enabled
				UDP encapsulation	Disabled



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.