NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

MODE TRANSITION DR : RENDRE PROGRESSIVEMENT UNE ARCHITECTURE IPSEC COMPATIBLE AVEC LE MODE DR

Produits concernés : SNS 5.0 et versions supérieures

Dernière mise à jour du document : 20 mai 2025

Référence : sns-fr-ipsec_SNS_v5_Mode_transition_DR_note_technique

Table des matières

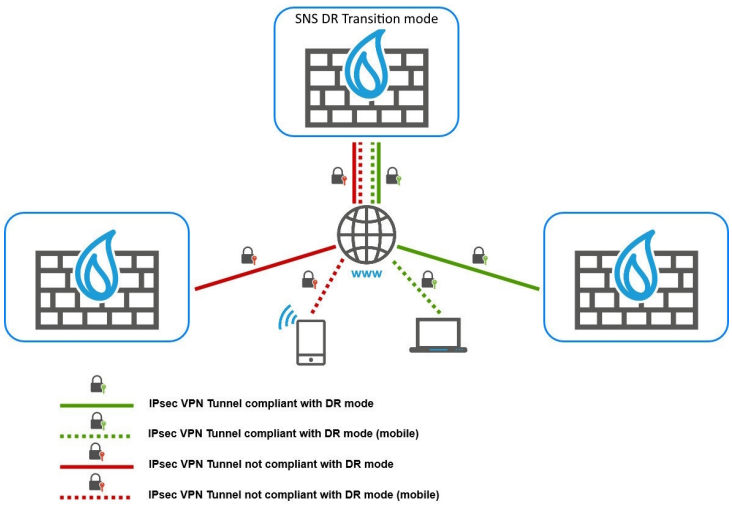
Historique des modifications ... 4
Avant de commencer ... 5
Comprendre l'impact du mode DR ... 6
Interopérabilité ... 6
Compatibilité des modes DR entre versions SNS ... 6
Chemins de mise à jour ... 6
Compatibilité des clients VPN IPsec avec le mode DR ... 7
Impacts réseau ... 7
Conditions à remplir pour qu'un tunnel soit compatible avec le mode DR ... 7
Profils de chiffrement IKE et IPsec ... 7
Protocole IKE ... 8
Authentification des correspondants ... 8
Vérification de révocation des certificats ... 8
Rendre la PKI conforme avec le mode DR ... 10
Rappel des recommandations IPsec DR pour la PKI ... 10
Cas d'une PKI externe ... 10
Si la PKI respecte les recommandations IPsec DR (critères décrits ci-dessus) ... 10
Si la PKI ne respecte pas les recommandations IPsec DR (critères décrits ci-dessus) ... 10
Cas d'une PKI interne (PKI sur un firewall SNS) ... 11
Si une CA (ou sous-CA) respectant les recommandations IPsec DR existe déjà sur le firewall SNS en version 5 ou supérieure ... 11
Si une CA respectant les recommandations IPsec DR doit être créée ... 11
Créer l'identité du firewall SNS en version 5 (si elle n'existe pas) et de chacun de ses correspondants ... 12
Exporter l'identité de chaque correspondant à rendre compatible avec le mode DR ... 14
Importer son identité sur chaque correspondant à rendre compatible avec le mode DR ... 14
Supprimer les clés privées des identités des correspondants sur le firewall SNS en version 5 (recommandé) ... 14
Activer la vérification de révocation des certificats des correspondants ... 15
Activer la récupération automatique des CRL ... 15
Vérifier la compatibilité d'une politique IPsec avec le mode DR ... 16
Onglet Profils de chiffrement ... 16
Onglet Correspondants ... 16
Onglet politique de chiffrement - Tunnels ... 19
Rendre la politique IPsec conforme avec le mode DR ... 20
Modifier la version IKE utilisée par le correspondant ... 20
Modifier la méthode d'authentification utilisée par le correspondant ... 20
Modifier les algorithmes d'authentification et de chiffrement ... 21
Ajouter la chaîne de confiance utilisée pour signer les certificats dans la liste des Autorités de certification acceptées ... 21
Optionnel - Définir les profils de chiffrement DR (ou les profils personnalisés compatibles) comme profils par défaut ... 21
Rendre la configuration d'un client mobile IPsec conforme avec le mode DR ... 23
Créer un tunnel compatible avec le mode DR sur un client mobile ... 23
Lancer et activer le client VPN compatible mode DR ... 23

Autoriser l'affichage des paramètres supplémentaires 23
Créer une nouvelle passerelle 23
Adapter les paramètres de la passerelle pour les rendre compatibles avec le mode DR 24
Créer le tunnel vers la passerelle compatible avec le mode DR 26
Adapter les paramètres du tunnel pour le rendre compatible avec le mode DR 26
Activer le mode DR sur l'ensemble des correspondants 28
Vérifier que l'ensemble de la configuration est bien compatible avec le mode DR 28
Activer le mode DR 28
Vérifier l'état des tunnels 29

Historique des modifications

Date	Description
20 mai 2025	Nouveau document

Avant de commencer



Le mode Diffusion Restreinte (DR) introduit en version SNS 4.2 ne permet pas de faire cohabiter des politiques respectant les spécifications IPsec DR définies par l'ANSSI et des politiques respectant la norme IPsec standard (RFC 7292 IKEv2bis).

Nous vous invitons à consulter le Manuel Utilisateur SNS pour obtenir plus d'informations sur le mode Diffusion Restreinte (DR).

La version 5 de SNS permet de configurer des tunnels VPN IPsec respectant les exigences du mode DR, tout en conservant la possibilité d'établir des tunnels VPN IPsec ne respectant pas ces exigences. Cette fonctionnalité s'applique aux architectures complexes dont le processus de mise en conformité avec le mode DR doit passer par une phase de transition pendant laquelle des politiques IPsec DR et standard (non-DR) seront amenées à coexister.

Pour cela, une option de configuration introduite en version 5 permet de définir, au niveau du correspondant IPsec, si les tunnels négociés avec ce correspondant doivent respecter les exigences du mode DR, ou non. Les contraintes imposées par cette option de configuration sont identiques à celles du mode DR, et la configuration d'un tunnel VPN IPsec compatible avec le mode DR doit suivre les exigences décrites dans la section Évaluer l'impact de l'activation du mode DR.

Une fois tous les correspondants modifiés pour être compatibles avec le mode DR, le mode DR complet peut être activé sur le firewall SNS en version 5 et sur ses correspondants.

Cette option est appelée "Mode Transition DR" dans la suite de cette Note Technique.

Comprendre l'impact du mode DR

Cette section permet de comprendre quelques spécificités du mode DR et leur impact sur un firewall SNS ainsi que sur l'architecture IPsec concernée.

Interopérabilité

Lorsque le mode DR est activé sur un firewall SNS respectant les recommandations IPsec DR de l'ANSSI, la négociation de tunnels VPN n'est normalement possible qu'avec des correspondants (firewalls SNS, équipements tiers et clients VPN) respectant également ces recommandations.

Les versions SNS respectant ces recommandations sont :

- SNS 4.3.21 LTSB et versions 4.3 LTSB supérieures,
- SNS 4.8 et versions supérieures.
- SNS 5.0 et versions supérieures.

La version 5 de SNS permet de **passer progressivement** d'une configuration comportant des tunnels IPsec non-compatibles avec le mode DR à une configuration exclusivement composée de tunnels compatibles avec le mode DR.

Compatibilité des modes DR entre versions SNS

"Mode" IPsec	Standard			DR			Transition DR
Version SNS	3.x	4.3.21 LTSB et supérieure	5.x	3.x	4.3.21 LTSB et supérieure	5.x	5.x
3.x	✓	✓	✓	✓	✗	✗	⚠
4.x	✓	✓	✓	✗	✓	✓	✓
5.x	✓	✓	✓	✗	✓	✓	✓

⚠ : Compatible uniquement avec les tunnels IPsec en mode standard

NOTE
Le mode DR des versions 3.x de SNS n'est pas compatible avec le mode DR des versions 4.x et 5.x de SNS. Un firewall en version 3.x devant établir des tunnels en mode DR avec des firewalls en version 4.x ou 5.x doit donc être préalablement mis à jour en version SNS 4.3 LTSB ou 4.8.

Chemins de mise à jour

Pour mettre à jour un firewall en version 4.3, 4.8 ou 5 depuis une version antérieure, des mises à jour intermédiaires peuvent être nécessaires selon la version d'origine :

Depuis une version 3.X	Mettre à jour vers la dernière version 3.7.X LTSB ou 3.11.X LTSB disponible
Depuis une version 4.0.X	Mettre à jour en version 4.1.6

Depuis une version 4.1.6 ou supérieure	Aucune mise à jour intermédiaire requise
Depuis un firewall V / VS-VU	Voir Migrer un firewall virtuel modèle V / VS-VU vers un modèle EVA

Compatibilité des clients VPN IPsec avec le mode DR

Les clients VPN IPSec pouvant établir un tunnel en mode DR avec des firewalls SNS sont les suivants :

- Stormshield Network VPN Client Exclusive 7.5.109 et versions supérieures,
- TheGreenBow VPN Client Édition Enterprise 7.5.109 et versions supérieures.

Si vous utilisiez des clients Stormshield Network VPN Client Standard, l'activation du mode DR nécessite de désinstaller ces clients au profit de l'un des clients compatibles listés ci-dessus.

Si vous utilisiez déjà Stormshield Network VPN Client Exclusive, assurez-vous que chaque client est en version 7.5.109 ou supérieure et vérifiez leur configuration comme décrit dans la section Créer un tunnel compatible avec le mode DR sur un client mobile.

NOTE
Dans la suite de ce document, le client VPN mobile utilisé fera référence à l'un des deux clients compatibles cités ci-dessus et sera nommé de manière générique "client VPN compatible mode DR".

Impacts réseau

Les paquets de négociation du tunnel VPN IPsec ainsi que les paquets ESP sont échangés par défaut sur le port UDP/4500 pour respecter les recommandations de l'ANSSI sur le mode DR.

Si d'autres équipements de sécurité sont situés entre le firewall à paramétrer en mode DR et ses correspondants, vous devez donc autoriser le port UDP/4500 entre le firewall SNS et ses correspondants sur ces équipements intermédiaires.

Vous pouvez cependant revenir au port standard UDP/500 à l'aide de la séquence de commandes CLI / Serverd suivante :

```
CONFIG IPSEC PEER UPDATE UDPEncapPreferred=0
CONFIG IPSEC ACTIVATE
```

Plus d'informations sur la commande `CONFIG IPSEC PEER UPDATE`

Conditions à remplir pour qu'un tunnel soit compatible avec le mode DR

Profils de chiffrement IKE et IPsec

Les profils de chiffrement IKE et IPsec doivent obligatoirement répondre aux contraintes suivantes, établies par le référentiel IPsec DR :

- Les méthodes Diffie-Hellman utilisées doivent obligatoirement appartenir aux groupes DH19 NIST Elliptic Curve Group (256-bits) ou DH28 Brainpool Elliptic Curve Group (256-bits).

- Les algorithmes imposés pour la phase 1 (*Parent Security Association*) et la protection des renouvellements de phase 2 (*Child Security Association*) doivent être :
  - Soit AES_GCM_16. Il s'agit d'un algorithme de type AEAD (Authenticated Encryption with Associated DATA) et il n'est donc associé à aucun algorithme d'authentification.
  - Soit AES_CTR, impérativement associé à l'algorithme d'authentification SHA256.

Protocole IKE

Seule la version 2 du protocole IKE est autorisée.

Authentification des correspondants

Seule l'authentification par certificat est autorisée. Les contraintes de génération et de signature des bi-clés sont les suivantes :

- Taille des clés utilisées dans les certificats fixée à 256 bits,
- Signature ECDSA ou ECSDSA sur courbe ECP 256 (SECP) ou BP 256 (BRAINPOOL),
- SHA256 comme algorithme de hachage.

IMPORTANT
Ces contraintes s'appliquent en remontant depuis le certificat du correspondant jusqu'au premier *Trust Anchor* (première CA ou sous-CA) respectant ces spécifications.

De plus, le champ **ID du correspondant** doit être obligatoirement renseigné en respectant l'un des deux formats suivants :

- *Distinguished Name* (DN). Il s'agit du sujet du certificat du correspondant (exemple : *C=FR,ST=Nord,L=Villeneuve d'Ascq,O=Stormshield,OU=Documentation,CN=DR-Compliant-Gateway-Peer.stormshield.eu*),
- *Subject Alternative Name* (SAN). Il s'agit d'un des alias éventuellement définis lors de la création du certificat du correspondant (exemple : I). Lorsque le champ **ID du correspondant** est renseigné avec le SAN d'un correspondant, vous devez également renseigner ce SAN dans le champ **Local ID** du correspondant concerné.

NOTE
La longueur possible d'un sujet de certificat peut poser des problèmes de compatibilité avec des matériels tiers comme les chiffreurs, passerelles VPN... autres que les firewalls SNS. Il est dans ce cas fortement conseillé de définir un SAN lors de la création du certificat du correspondant et d'utiliser ce SAN comme ID de correspondant.

Vérification de révocation des certificats

Un mécanisme de vérification des *Certificate Revocation Lists* (CRL) de l'ensemble de la chaîne de confiance (CA racine [*Root CA*], sous-CA et certificats) doit être actif sur le firewall.

Pour ce faire, le champ **CRL Required** d'un correspondant compatible avec le mode DR doit être positionné sur la valeur **Auto** ou **Obligatoire**. Notez que par défaut (mode IPsec standard), ce champ prend la valeur **Auto** et que lorsque le mode DR est activé, il prend la valeur **Obligatoire**.

Durant la phase de transition, il doit être positionné sur à la valeur **Obligatoire**.

En plus de la vérification de révocation des certificats, les CRL doivent être présentes et toujours valides pour que la négociation soit fonctionnelle.

Rendre la PKI conforme avec le mode DR

Rappel des recommandations IPsec DR pour la PKI

Les certificats, depuis le certificat du correspondant jusqu'au *Trust Anchor*, doivent respecter les spécifications suivantes :

- Taille des clés utilisées dans les certificats fixée à 256 bits,
- Signature ECDSA ou ECSDSA sur courbe ECP 256 (SECP) ou BP 256 (BRAINPOOL),
- SHA256 comme algorithme de hachage.

IMPORTANT
Ces contraintes s'appliquent en partant du certificat du correspondant et en remontant jusqu'au premier *Trust Anchor* (première CA ou sous-CA) respectant ces spécifications.

Cas d'une PKI externe

Si la PKI respecte les recommandations IPsec DR (critères décrits ci-dessus)

Depuis l'autorité de certification destinée à gérer les identités des correspondants compatibles avec le mode DR :

1. Vérifiez que les URI des points de distribution de CRL de la CA (ou sous-CA) sont bien précisés. Si ce n'est pas le cas, ajoutez-les.

   NOTE
   Les certificats signés par cette CA (ou sous-CA) avant l'ajout des points de distribution de CRL devront être à nouveau générés afin de prendre en compte cette modification.

2. Générez les identités de tous les correspondants IPsec à rendre compatibles avec le mode DR. À noter que les firewalls SNS supportent le protocole d'enrôlement EST dans un contexte DR.
3. Exportez ces identités (certificat + clé privée).
4. Importez chaque identité sur le correspondant concerné. Pour les firewalls SNS, référez-vous à la section Importer son identité sur chaque correspondant à rendre compatible avec le mode DR.

Si la PKI ne respecte pas les recommandations IPsec DR (critères décrits ci-dessus)

1. Placez-vous dans une CA de votre PKI.
2. Créez une sous-CA respectant les critères définis dans le paragraphe **Rappel des recommandations IPsec DR pour la PKI**.

Depuis cette sous-CA :

1. Générez les identités de tous les correspondants IPsec à rendre compatibles avec le mode DR.
2. Exportez ces identités (certificat + clé privée).

3. Importez chaque identité sur le correspondant concerné. Pour les firewalls SNS, référez-vous à la section Importer son identité sur chaque correspondant à rendre compatible avec le mode DR.

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

> **NOTE**
> Dans cet exemple, la CA signant les certificats de tous les correspondants destinés à être compatibles avec le mode DR existe ou est créée sur le firewall SNS en version 5 ou supérieure.

Si une CA (ou sous-CA) respectant les recommandations IPsec DR existe déjà sur le firewall SNS en version 5 ou supérieure

Sur le firewall SNS en version 5 dans cet exemple :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI**.
2. Dans la liste des CA et certificats, sélectionnez la CA (ou sous-CA) destinée à signer les certificats des correspondants IPsec compatibles avec le mode DR.
   Les détails de cette CA (ou sous-CA) s'affichent dans la partie droite.
3. Dans l'onglet **Détails** > cadre **Empreintes**, vérifiez que l'algorithme de signature est ecdsa-with-SHA256. Si ce n'est pas le cas, créez une CA (ou sous-CA) pour laquelle le **Type de clé** est positionné sur SECP ou BRAINPOOL avec une **Taille de clé** à 256 bits.
4. Dans l'onglet **Profils de Certificats**, vérifiez que les URI des points de distribution de CRL de la CA (ou sous-CA) sont bien précisés. Si ce n'est pas le cas, ajoutez-les.

   > **NOTE**
   > Les certificats signés par cette CA (ou sous-CA) avant l'ajout des points de distribution de CRL devront être à nouveau générés afin de prendre en compte cette modification.

5. Dans l'onglet **Profils de Certificats**, vérifiez que dans les cadres **Autorité de certification**, **Certificats Utilisateurs** et **Certificats Serveurs** :
   - Le **Type de clé** est positionné sur SECP ou BRAINPOOL,
   - La **Taille de clé** est positionnée exclusivement sur 256 bits,
   - La **Somme de contrôle** est positionnée sur sha256.

   Si l'un de ces paramètres diffère des valeurs imposées, modifiez-le pour choisir la valeur adéquate.
6. Cliquez sur **Appliquer** pour prendre en compte les éventuelles modifications que vous avez effectuées.

Si une CA respectant les recommandations IPsec DR doit être créée

Sur le firewall SNS en version 5 dans cet exemple :

Créer la CA

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI**.
2. Cliquez sur **Ajouter**
3. Sélectionnez **Autorité racine**.
   Un assistant de création s'affiche.

4. Indiquez un **Nom** (*IPsec-DR-CA* 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 l'adresse **E-mail** de contact pour cette CA.
9. La durée de **Validité** proposée par défaut pour la CA est de 3650 jours (valeur conseillée). Vous pouvez la modifier.
10. **Type de clé** : sélectionnez impérativement SECP ou BRAINPOOL.
11. **Taille de clé (bits)** : sélectionnez impérativement 256.
12. Cliquez sur **Suivant**.
13. **Points de distribution des CRL** : ajoutez les URI des points de distribution de CRL auxquels les équipements IPsec de vos correspondants pourront s'adresser afin de vérifier la validité des certificats émis par votre CA.
14. Cliquez sur **Suivant**.
    Un résumé des informations concernant la CA est affiché.
15. Validez en cliquant sur **Terminer**.

Déposer la CRL sur les points de distribution

1. Sélectionnez la CA précédemment créée.
2. Cliquez sur **Télécharger**.
3. Sélectionnez **CRL** puis le format d'export (PEM ou DER).
   Un message vous propose le lien de téléchargement.
4. Téléchargez la CRL en cliquant sur ce lien puis déposez-la sur chacun des points de distribution de CRL précisés lors de la création de la CA.

Créer l'identité du firewall SNS en version 5 (si elle n'existe pas) et de chacun de ses correspondants

Pour les correspondants de type passerelle

Sur le firewall SNS en version 5 dans cet exemple :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI.**
2. Sélectionnez la CA signant les certificats pour le mode DR (*IPsec-DR-CA* dans cet exemple).
3. Cliquez sur **Ajouter** et sélectionnez **Identité serveur**.
4. Saisissez le nom de domaine qualifié du correspondant (exemple : *DR-Compliant-Firewall.stormshield.eu*).
   L'**Identifiant** se remplit automatiquement avec le nom de domaine qualifié. Vous pouvez le modifier.
5. Cliquez sur **Suivant**.
6. Renseignez le mot de passe de la CA signant cette identité serveur (*IPsec-DR-CA* dans cet exemple).
7. Cliquez sur **Suivant**.
8. Sélectionnez une durée de **validité** en jours (365 jours proposés par défaut).
9. Le type de clé proposé par défaut est compatible avec le mode DR (BRAINPOOL ou SECP) : il s'agit de celui de la CA signant l'identité serveur.
10. **Taille de clé (bits)** : sélectionnez impérativement 256.
11. Cliquez sur **Suivant**.
12. Vous pouvez ajouter un alias pour ce correspondant (optionnel).

> **NOTE**
> Lorsqu'il est défini, l'alias ou *Subject Alternative Name* (SAN) prend place dans le champ *SubjectAltName* du certificat.
> Il est ainsi pertinent de le définir par le nom de domaine qualifié (FQDN) renseigné à l'étape 4 afin de pouvoir utiliser ce SAN comme **ID du correspondant**. En effet, la syntaxe est plus simple que celle du sujet complet du certificat.

13. Cliquez sur **Suivant**.
    Un résumé de l'identité s'affiche.
14. Cliquez sur **Terminer** pour valider la création de cette identité serveur.

Répétez cette procédure pour créer l'identité de chaque correspondant concerné (passerelles).

Pour les correspondants de type mobile

Sur le firewall SNS en version 5 dans cet exemple :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI.**
2. Sélectionnez la CA signant les certificats pour le mode DR (*IPsec-DR-CA* dans cet exemple).
3. Cliquez sur **Ajouter** et sélectionnez **Identité utilisateur**.
4. Dans le champ **CN**, saisissez le nom du correspondant (exemple : *John Doe*).
   L'**Identifiant** se remplit automatiquement avec le nom du correspondant. Vous pouvez le modifier.
5. Renseignez l'adresse e-mail du correspondant (*john.doe@stormshield.eu* dans cet exemple).
6. Cliquez sur **Suivant**.
7. Renseignez le mot de passe de la CA signant cette identité serveur (*IPsec-DR-CA* dans cet exemple).
8. Cliquez sur **Suivant**.
9. Sélectionnez une durée de **validité** en jours (365 jours proposés par défaut).

10. Le type de clé proposé par défaut est compatible avec le mode DR (BRAINPOOL ou SECP) : il s'agit de celui de la CA signant l'identité serveur.
11. **Taille de clé (bits)** : sélectionnez impérativement 256.
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 créer l'identité de chaque correspondant mobile.

Exporter l'identité de chaque correspondant à rendre compatible avec le mode DR

Sur le firewall SNS en version 5 dans cet exemple :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI.**
2. Sélectionnez l'identité serveur 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.

Répétez cette procédure pour exporter l'identité de chaque correspondant concerné (passerelles et correspondants mobiles).

Importer son identité sur chaque correspondant à rendre compatible avec le mode DR

Sur chaque correspondant de type passerelle autre que le firewall SNS en version 5 :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI**.
2. Cliquez sur **Ajouter** et sélectionnez **Importer un fichier**.
3. Dans le champ **Mot de passe du fichier (si PKCS#12)** : renseignez le mot de passe protégeant le fichier P12.
4. Cliquez sur **Importer**.

Pour les correspondants mobiles, cette manipulation est décrite dans la section Créer un tunnel compatible avec le mode DR sur un client mobile

Supprimer les clés privées des identités des correspondants sur le firewall SNS en version 5 (recommandé)

Une fois le fichier P12 importé sur le correspondant à rendre compatible avec le mode DR, il est fortement recommandé de supprimer la clé privée de l'identité de ce correspondant.

Sur le firewall hébergeant la CA (le firewall SNS en version 5 dans cet exemple) :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI.**
2. Sélectionnez l'identité serveur 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 (passerelles et correspondants mobiles).

Activer la vérification de révocation des certificats des correspondants

L'autorité de certification (CA) dont sont issus les certificats utilisés pour l'authentification des correspondants IPsec doit impérativement mettre en œuvre un mécanisme de révocation (CRL et points de distribution de CRL ou serveurs OCSP) et la vérification des certificats issus de cette CA doit être activée sur les correspondants. Lorsque ce paramètre est activé, il est nécessaire de disposer de toutes les CRL de la chaîne de certification. Dans le cas contraire, la politique IPsec courante est désactivée et le message d'erreur "Désactiver la vérification des CRL n'est pas compatible avec le mode DR" est affiché dans le champ **Vérification de la politique** situé sous la grille de la politique IPsec.

Sur tous les correspondants concernés par le mode DR :

1. Placez-vous dans le module **Configuration** > **Système** > **Console CLI**.
2. Tapez la suite de commandes :
```
CONFIG IPSEC UPDATE slot=x CRLrequired=1
CONFIG IPSEC CHECK index=1
CONFIG IPSEC ACTIVATE
```
Où x représente le numéro de la politique IPsec à modifier.
3. Cliquez sur **Exécuter**.

Activer la récupération automatique des CRL

Sur chaque correspondant concerné :

1. Placez-vous dans le menu **Configuration** > onglet **Configuration générale**.
2. Cochez la case **Activer la récupération régulière des listes de révocation de certificats (CRL)**.

En effet, si la CRL de la CA d'un correspondant n'est pas récupérée, les tunnels avec ce correspondant ne pourront pas s'établir.

Vérifier la compatibilité d'une politique IPsec avec le mode DR

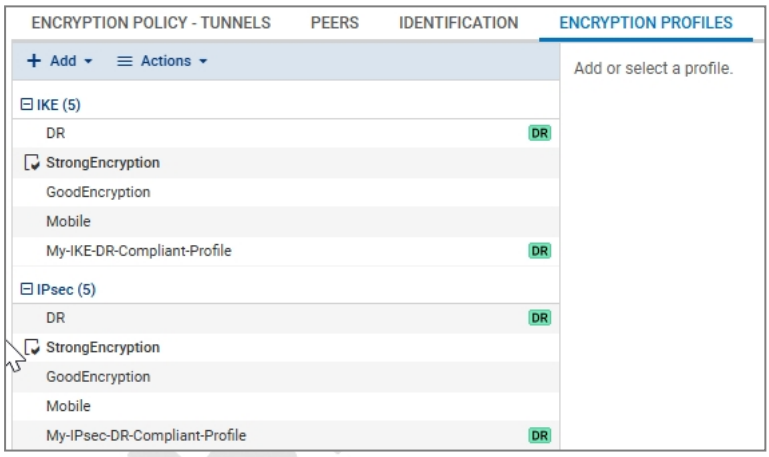
Une fois installée, la version SNS 5 ou supérieure permet d'identifier aisément les éléments de la politique IPsec compatibles avec le mode DR, et inversement, ceux nécessitant des modifications de configuration afin de les rendre compatibles.

Rendez-vous dans le module **Configuration** > **VPN** > **VPN IPsec**.

Onglet Profils de chiffrement

Deux profils prédéfinis, nommés **DR,** sont proposés par défaut. L'icône DR associée indique que ces profils de chiffrement IKE et IPsec sont compatibles avec le mode DR.

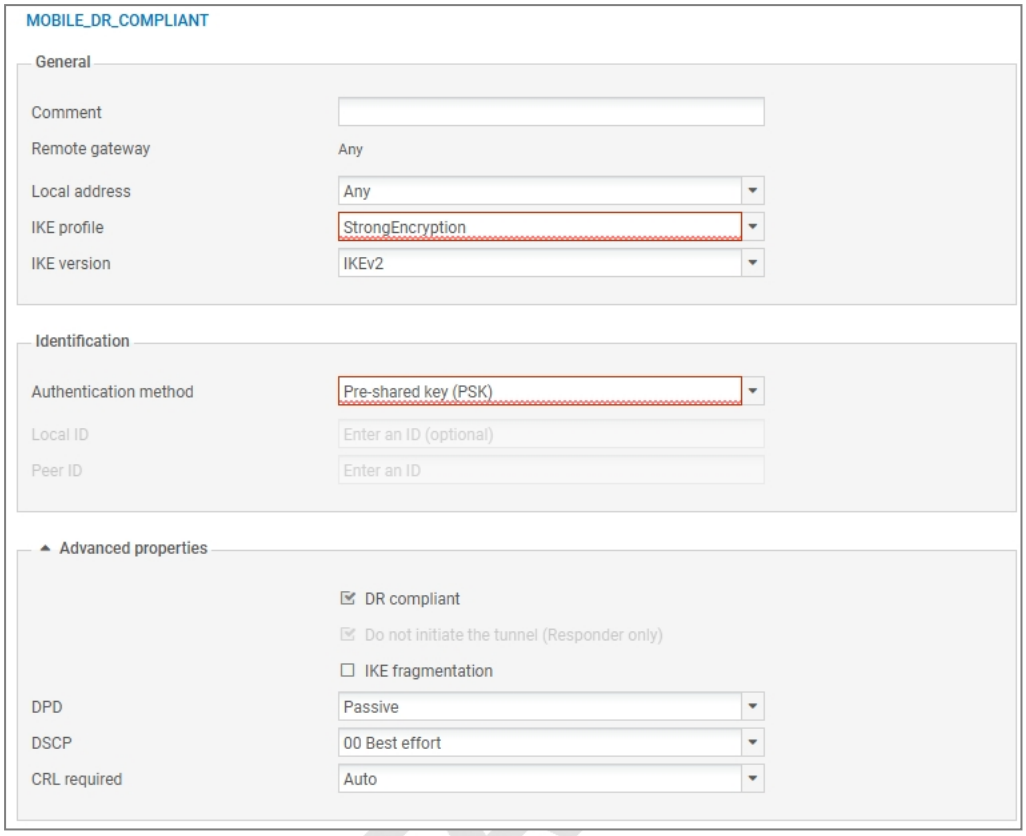
Vous pouvez également ajouter vos propres profils personnalisés compatibles avec le mode DR, en clonant ces profils **DR** prédéfinis par exemple. Ces profils seront automatiquement accompagnés de l'icône DR.



Onglet Correspondants

1. Sélectionnez un correspondant.
2. Dans le volet **Configuration avancée**, cochez la case **Compatible mode DR** pour mettre en évidence les paramètres du correspondant devant être modifiés afin de le rendre compatible avec le mode DR.

Exemple 1 : correspondant non compatible avec le mode DR.



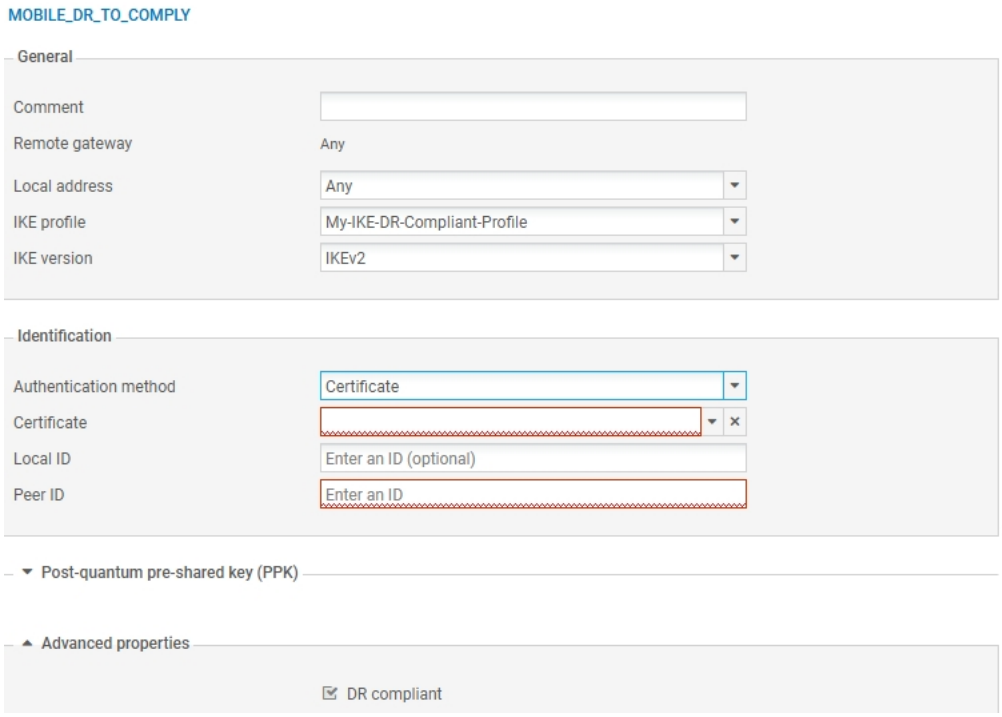
Les paramètres à modifier sont encadrés de rouge.

Dans cet exemple, pour rendre le correspondant compatible avec le mode DR, vous devez :

- Choisir un profil de chiffrement compatible avec le mode DR (profil prédéfini **DR** ou profil personnalisé compatible),
- Changer la méthode d'authentification pour sélectionner l'authentification par certificat.

Seuls les choix compatibles avec le mode DR vous sont proposés pour modifier les valeurs de ces champs.

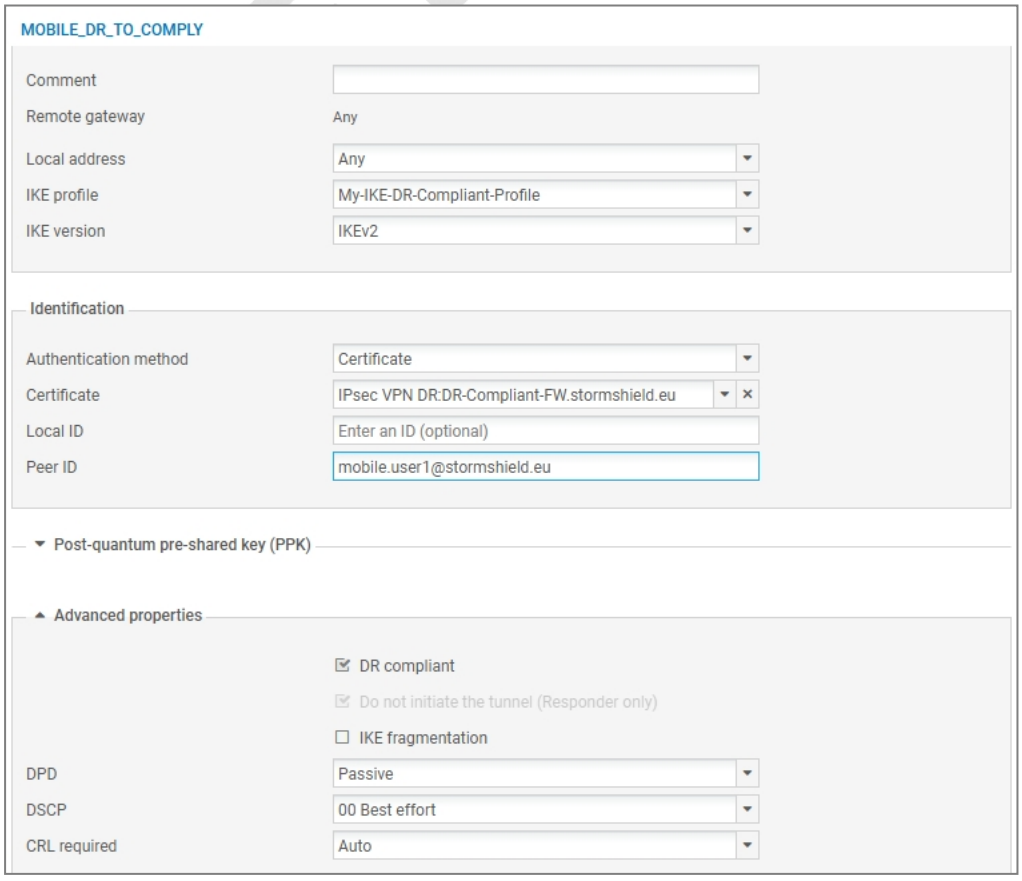
La sélection d'un choix compatible avec le mode DR peut entraîner l'affichage d'autres champs obligatoires. Par exemple, en modifiant la méthode **Clé pré-partagée (PSK)** pour la méthode **Certificat**, certains champs obligatoires liés à cette méthode d'authentification sont alors mis en évidence :



Vous devez dans ce cas :

- Sélectionner le certificat présenté par le firewall local,
- Préciser un **ID de correspondant** reflétant le FQDN présent dans le certificat du correspondant.

Exemple 2 : correspondant compatible avec le mode DR.



Pour ce correspondant, aucun paramètre ne nécessite de modification.

Onglet politique de chiffrement - Tunnels

Lorsqu'un correspondant est compatible avec le mode DR (case **Compatible mode DR** cochée et tous paramètres du correspondant compatibles), la règle IPsec associée à ce correspondant est précédée de l'icône DR.

	Status	Local network	Peer	Remote network	Encryption profile
DR	on	Network_in	Mobile_DR_To_Comply	Any	My-IPsec-DR-Compliant-Profile

Rendre la politique IPsec conforme avec le mode DR

Sur le firewall SNS en version 5 :

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants.**
2. Sélectionnez le correspondant à rendre compatible avec le mode DR (**Passerelles distantes** et **Correspondants mobiles**).
3. Dans le cadre **Configuration avancée**, cochez la case **Compatible mode DR**.

Les paramètres du correspondant qui ne sont pas compatibles avec le mode DR sont encadrés de rouge.

Suivez les procédures ci-dessous pour modifier ces paramètres si nécessaire.

Modifier la version IKE utilisée par le correspondant

1. Sélectionnez **IKEv2** pour le champ **Version IKE**.
2. Vous devez également réaliser cette modification sur le correspondant concerné. S'il s'agit d'un client mobile, suivez la procédure de mise en conformité décrite dans la section Créer un tunnel compatible avec le mode DR sur un client mobile.

Modifier la méthode d'authentification utilisée par le correspondant

1. Dans le cadre **Identification**, positionnez le champ **Méthode d'authentification** sur **Certificat**.
2. Renseignez le champ **ID du correspondant**. Ce champ doit respecter l'une des deux formes suivantes :
    - *Distinguished Name* (DN). Il s'agit du sujet du certificat du correspondant (exemple : *C=FR,ST=Nord,L=Villeneuve d'Ascq,O=Stormshield,OU=Documentation,CN=DR-Compliant-Gateway-Peer.stormshield.eu*),
    - *Subject Alternative Name* (SAN). Il s'agit d'un des alias éventuellement définis lors de la création du certificat du correspondant (exemple : *DR-Compliant-Firewall.stormshield.eu*).

> **NOTE**
> La longueur possible d'un sujet de certificat peut poser des problèmes de compatibilité avec des matériels tiers (chiffreurs, passerelles VPN... autres que les firewalls SNS). Il est dans ce cas fortement conseillé d'utiliser le SAN défini lors de la création du certificat du correspondant.

3. Vous devez également réaliser cette modification sur le correspondant concerné. S'il s'agit d'un client mobile, suivez la procédure de mise en conformité décrite dans la section Créer un tunnel compatible avec le mode DR sur un client mobile.

Modifier les algorithmes d'authentification et de chiffrement

1. Dans le cadre **Général**, assurez-vous que le champ **Profil IKE** est positionné sur un profil compatible avec le mode DR (profil **DR** fourni par défaut ou profil personnalisé - *My DR Profile* dans cet exemple).
2. Vous devez également réaliser cette modification sur le correspondant concerné. S'il s'agit d'un client mobile, suivez la procédure de mise en conformité décrite dans la section Créer un tunnel compatible avec le mode DR sur un client mobile.

Ajouter la chaîne de confiance utilisée pour signer les certificats dans la liste des Autorités de certification acceptées

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Identification**.
2. Dans la grille **Autorités de certification acceptées**, vérifiez la présence de l'ensemble de la chaîne complète de confiance, c'est à dire de la CA Racine (*Root CA*) jusqu'à la sous-CA ayant signé les certificats utilisés pour le mode DR (*IPsec-DR-CA* dans cet exemple).
3. Si ce n'est pas le cas, cliquez sur **Ajouter** et sélectionnez l'autorité de certification concernée.
4. Vous devez également réaliser cette modification sur le correspondant concerné. S'il s'agit d'un client mobile, suivez la procédure de mise en conformité décrite dans la section Créer un tunnel compatible avec le mode DR sur un client mobile.

Optionnel - Définir les profils de chiffrement DR (ou les profils personnalisés compatibles) comme profils par défaut

Cette procédure permet de définir les profils **DR** (ou les profils personnalisés compatibles) comme profils proposés par défaut pour tous les futurs correspondants et toutes les règles IPsec devant être créés sur le firewall.

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Profils de chiffrement.**
2. Dans le menu de gauche, section **IKE**, sélectionnez le profil **DR** (ou le profil personnalisé compatible avec le mode DR).
   Vérifiez que les caractéristiques du profil sont les suivantes :
   - Deux profils Diffie-Hellman sont proposés : DH28 Brainpool Elliptic Curve Group (256-bits), sélectionné par défaut, et DH19 NIST Elliptic Curve Group (256-bits).
   - L'algorithme AES_GCM_16 est sélectionné comme proposition par défaut, AES_CTR étant la deuxième proposition.

   Ne modifiez surtout pas la **Force de chiffrement** de l'algorithme choisi.
3. Cliquez sur le menu **Actions**.
4. Sélectionnez **Définir le profil par défaut**.
   Ce profil IKE est désormais utilisé par défaut pour les nouveaux tunnels IPsec ajoutés dans la configuration du firewall.

5. Dans le menu de gauche, section **IPsec**, sélectionnez le profil **DR** (ou le profil personnalisé compatible avec le mode DR).
   Vérifiez que les caractéristiques du profil sont les suivantes :
   - L'algorithme HMAC_SHA256 est sélectionné comme proposition d'authentification.
   - L'algorithme AES_GCM_16 est sélectionné comme proposition de chiffrement par défaut, AES_CTR étant la deuxième proposition.

   Ne modifiez surtout pas la **Force de chiffrement** de l'algorithme choisi.
6. Cliquez sur le menu **Actions.**
7. Sélectionnez **Définir le profil par défaut**.
   Ce profil IPsec est désormais utilisé par défaut pour les tunnels IPsec définis dans la configuration du firewall.

Rendre la configuration d'un client mobile IPsec conforme avec le mode DR

Cette section précise les options à activer et les paramètres à sélectionner pour rendre la configuration d'un client mobile IPsec compatible avec les recommandations IPsec DR de l'ANSSI.

Les clients compatibles pouvant établir un tunnel VPN en mode DR avec un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI sont précisés dans la section Compatibilité des clients VPN IPsec avec le mode DR.

Si vous utilisiez Stormshield Network VPN Client Standard, l'activation du mode DR nécessite de le désinstaller au profit de l'un des clients compatibles avec le mode DR.

Sur le poste client :

1. Téléchargez le client compatible mode DR.
2. Désinstallez SN VPN Client Standard s'il était installé sur le poste.
3. Installez le client compatible mode DR.

Créer un tunnel compatible avec le mode DR sur un client mobile

Pour obtenir plus d'informations sur Stormshield Network VPN Client Exclusive, veuillez consulter le Guide de l'administrateur Stormshield VPN Client Exclusive v7.

Lancer et activer le client VPN compatible mode DR

IMPORTANT
Pour pouvoir configurer le client VPN compatible mode DR, vous devez le lancer avec les privilèges d'un administrateur du poste client (clic droit sur l'icône du client VPN > **Exécuter en tant qu'administrateur**).

1. Sur le bureau Windows du poste client, lancez le client VPN compatible mode DR.
2. Au premier lancement, saisissez le numéro de licence pour l'utilisateur concerné.

Autoriser l'affichage des paramètres supplémentaires

1. Cliquez sur **Outils** > **Options** du menu général.
2. Dans l'onglet **Général** : cochez la case **Afficher plus de paramètres** et validez en cliquant sur **OK**.

Créer une nouvelle passerelle

Dans la colonne de gauche du client VPN compatible mode DR :

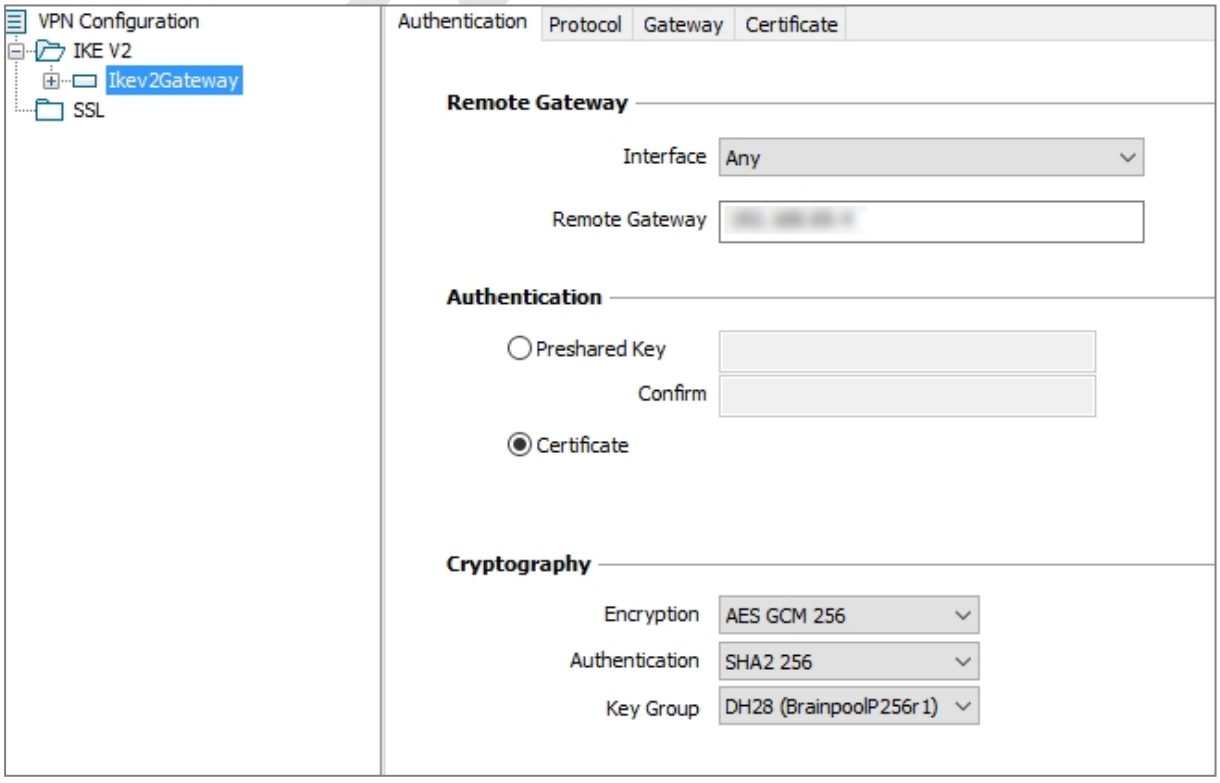
1. Faites un clic droit sur IKEv2 et sélectionnez **Nouvel IKE auth**.
   Une passerelle, nommée par défaut *Ikev2Gateway*, est créée.
2. Vous pouvez la renommer en effectuant un clic droit sur cette passerelle et en sélectionnant **Renommer**.

Adapter les paramètres de la passerelle pour les rendre compatibles avec le mode DR

Sélectionnez la passerelle créée précédemment.

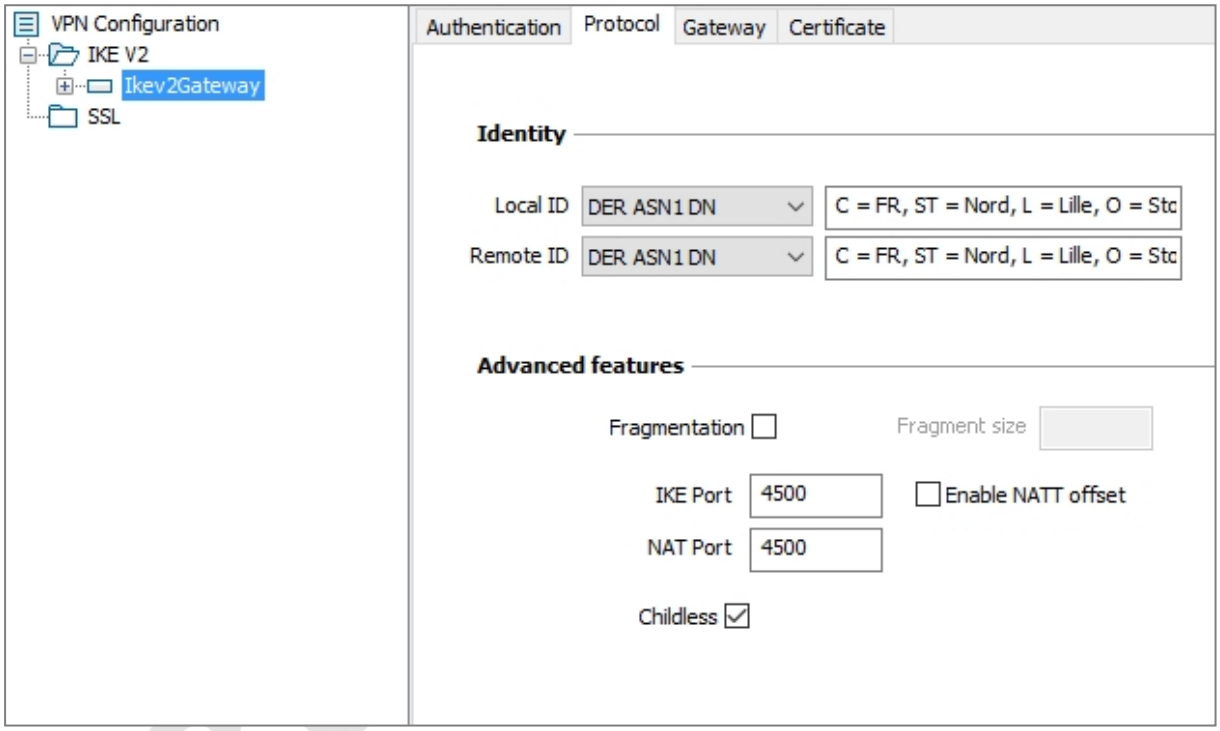
Onglet Authentification

1. Dans le champ **Adresse routeur distant**, saisissez l'adresse IP ou le FQDN du firewall avec lequel établir le tunnel compatible avec le mode DR.
2. Dans le cadre **Intégrité** sélectionnez **Certificat**.
   Vous basculez automatiquement dans l'onglet **Certificat**.
3. Cliquez sur le bouton **Importer un Certificat...**
4. Sélectionnez **Format P12** et cliquez sur **Suivant**.
5. Choisissez l'identité du client mobile précédemment exportée au format P12 sur le firewall concerné.
6. Saisissez le mot de passe protégeant cette identité.
7. Validez en cliquant sur **OK**.
8. Cliquez de nouveau sur l'onglet **Authentification**.
9. Dans le cadre **Cryptographie**, sélectionnez les valeurs correspondant aux valeurs sélectionnées sur le firewall concerné pour le profil de chiffrement DR :
   - **Chiffrement** : AES GCM 256 ou AES CTR 256,
   - **Intégrité** : SHA2 256,
   - **Groupe de clé** : DH28 (BrainpoolP 256r1) ou DH19 (ECP 256).



Onglet Protocole

1. Dans le cadre **Identité**, pour le champ **Remote ID** : sélectionnez **DER ASN1 DN** et indiquez le sujet du certificat de la passerelle SNS en version 5 (*C=FR,ST=Nord,L=Villeneuve d'Ascq,O=Stormshield,OU=Documentation,CN=DR-Compliant-Gateway-Peer.stormshield.eu* dans cet exemple).
2. Dans le cadre **Fonctions avancées** :
   a. Positionnez le **Port IKE** à 4500,
   b. Cochez la case **Initiation Childless**.



Onglet Passerelle

Vous pouvez laisser les paramètres par défaut.

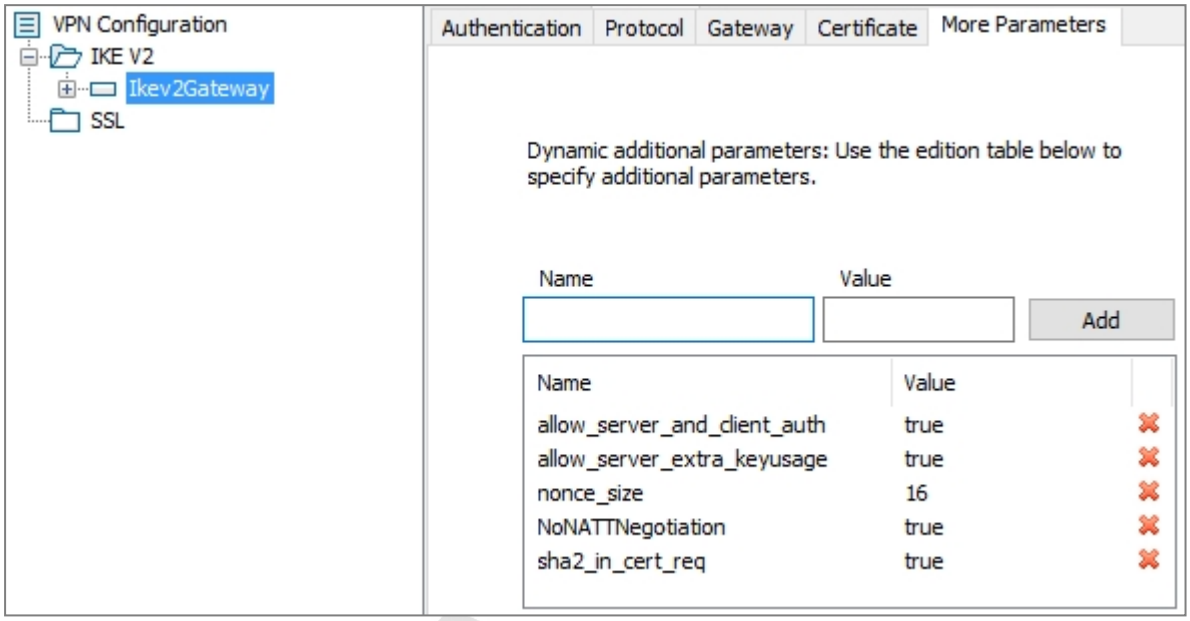
> **NOTE**
> Pour le paramètre durée de vie, il peut être intéressant de positionner une valeur inférieure à celle configurée sur la passerelle (firewall en mode DR) afin que les renégociations de phase 2 soient à l'initiative du client VPN compatible mode DR.

Onglet Plus de paramètres

1. S'il est présent, supprimez le paramètre "Method14_RSASSA_PKCS1".
2. Ajoutez les paramètres personnalisés avec les valeurs suivantes :

Nom	Valeur
nonce_size	16
NoNATTNegotiation	true
sha2_in_cert_req	true

allow_server_and_client_auth	true
allow_server_extra_keyusage	true



Sauvegarder la configuration

Cliquez sur **Configuration** > **Sauver** du menu général du client VPN compatible mode DR pour valider et sauvegarder cette configuration.

Créer le tunnel vers la passerelle compatible avec le mode DR

1. Faites un clic droit sur la passerelle précédemment créée et sélectionnez **Nouveau Child SA**. Un tunnel, nommé par défaut *Ikev2Tunnel,* est créé.
2. Vous pouvez le renommer en effectuant un clic droit sur ce tunnel et en sélectionnant **Renommer**.

Adapter les paramètres du tunnel pour le rendre compatible avec le mode DR

Sélectionnez le tunnel précédemment créé.

Onglet Child SA

1. Cochez la case **Obtenir la configuration depuis la passerelle**.
2. Dans le cadre **Cryptographie** :
   - Pour le champ **Chiffrement**, sélectionnez la même valeur que celle paramétrée pour la passerelle précédemment créée : AES GCM 256 ou AES CTR 256.
   - Pour le champ **Intégrité**, sélectionnez **auto**.
   - Pour le champ **Diffie Hellman**, sélectionnez la même valeur que celle paramétrée pour la passerelle précédemment créée : DH28 (BrainpoolP 256r1) ou DH19 (ECP 256).
   - Pour le champ **Numéro de séquence étendu**, sélectionnez **Automatique**.
3. Dans le cadre **Durée de vie**, pour le champ **Durée de vie Child SA**, sélectionnez **1800** (secondes).

Sauvegarder la configuration

Cliquez sur **Configuration** > **Sauver** du menu général du client VPN pour valider et sauvegarder cette configuration.

Activer le mode DR sur l'ensemble des correspondants

Vérifier que l'ensemble de la configuration est bien compatible avec le mode DR

Pour vérifier que la configuration est bien entièrement compatible avec le mode DR et éviter la désactivation de la politique VPN en cas d'anomalie, appliquez la procédure suivante sur le firewall en version SNS 5.0 ou supérieure :

1. Placez-vous dans le module **Système** > **Configuration** > **Console CLI**.
2. Exécutez la commande `CONFIG IPSEC CHECK index=<policy_idx> DRcompliant=1` où `<policy_idx>` correspond au numéro de la politique IPsec (exemple : index=1 pour la politique IPsec numéro 01).
   La réponse est `OK` lorsque la configuration est compatible avec le mode DR.

Activer le mode DR

Sur le firewall en version SNS 5.0 ou supérieure :

1. Placez-vous dans le module **Configuration** > **Système** > **Configuration** > onglet **Configuration générale**.
2. Dans le cadre **Paramètres cryptographiques**, cochez la case **Activer le mode « Diffusion Restreinte (DR) » version 2020**.
3. Redémarrez le firewall pour prendre en compte l'activation du mode DR.
4. Activez le mode DR sur chacun des correspondants de type passerelle.
5. Après redémarrage du firewall, vérifiez dans le module de supervision des tunnels IPsec que tous les tunnels sont établis.

Vérifier l'état des tunnels

Placez-vous dans l'onglet **Monitoring** de l'interface Web d'administration du firewall en version SNS 5.

Le module **Supervision** > **Tunnels VPN IPsec** vous permet d'afficher l'état des tunnels de la politique IPsec active.

L'icône DR vous permet d'identifier les tunnels entièrement compatibles avec le mode DR :

POLICIES

Type	Status	Local traffic endpoint	Local gateway	Local ID	Remote gateway	Peer ID	Remote traffic endpoint
Type : Gateway tunnels - DR compliant DR (1)							
	OK	Network_dmz1	Firewall_out	C=FR, ST=Nord, L=Lil...	IPsec-DR-Compliant	C=FR, ST=Nord, L=...	Remote_LAN_DR
Type : Mobiles / Roadwarriors - DR compliant DR (1)							
	OK	Network_dmz1		C=FR, ST=Nord, L=Lil...		C=FR, ST=Nord, L=...	
Type : Exception policies (bypass) (1)							
	Bypass	rfc5735_loopback	localhost		localhost		any

La sélection d'un tunnel particulier vous affiche le détail des Associations de sécurité (SA) IKE et IPsec de ce tunnel.

En savoir plus sur la supervision des tunnels IPsec (Manuel utilisateur SNS v4).

documentation@stormshield.eu