NOTE TECHNIQUE
STORMSHIELD NETWORK SECURITY

IPSEC - MODE DIFFUSION RESTREINTE

Produits concernés : SNS 4.3.21 LTSB et versions 4.3 LTSB supérieures, SNS 4.7 et versions supérieures, VPN Client Exclusive 7.4 et versions supérieures

Dernière mise à jour du document : 13 décembre 2023

Référence : sns-fr-ipsec_mode_diffusion_restreinte_note_technique

Table des matières

Historique des modifications

Date	Description
13 décembre 2023	- Correction orthographique du paramètre personnalisé *NoNATTNegotiation* (section "Créer un tunnel compatible avec le mode DR sur SN VPN Client Exclusive")
2 novembre 2023	- Sortie de SNS 4.7
18 octobre 2023	- Modification des sections "Évaluer l'impact de l'activation du mode DR", "Mettre à jour un firewall SNS déjà configuré en mode DR" et "Mettre en conformité la configuration du firewall SNS avec le mode DR" - Ajout de la section "Mettre la configuration d'un client mobile IPsec en conformité avec le mode DR"
12 septembre 2022	- Ajout de la section "Client VPN IPsec Stormshield" - Modification de la section "Sélectionner les algorithmes d'authentification et de chiffrement"
8 décembre 2021	- Modification de la section "Activer la vérification de révocation des certificats des correspondants"
27 août 2021	- Modification de la section "Évaluer l'impact du mode DR (SNS v4.2 ou supérieure)"
25 août 2021	- Nouveau document

Avant de commencer

Le mode « Diffusion Restreinte (DR) » impose au firewall de respecter les recommandations de l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, concernant l'usage des coprocesseurs et accélérateurs cryptographiques dans les produits visant une qualification. Elle est impérative sur les réseaux répondant à la mention « Diffusion Restreinte ».

Ce mode repose notamment sur l'utilisation de versions logicielles pour les algorithmes de cryptographie (asymétrique, génération d'aléa et symétrique).

Dans cette note technique, le mode "Diffusion Restreinte (DR)" est désigné sous la forme abrégée "mode DR".

Les sections de cette note technique détaillent des actions que vous pouvez effectuer sur les firewalls SNS. Poursuivez selon les actions que vous souhaitez effectuer :

- Évaluer l'impact de l'activation du mode DR,
- Mettre à jour un firewall SNS déjà configuré en mode DR,
- Activer le mode DR sur un firewall SNS sans configuration IPsec existante,
- Mettre en conformité la configuration du firewall SNS avec le mode DR,
- Mettre la configuration d'un client mobile IPsec en conformité avec le mode DR.

Évaluer l'impact de l'activation du mode DR

Lisez attentivement la section suivante afin d'évaluer l'impact de l'activation du mode DR sur un firewall SNS, et plus globalement, sur l'architecture complète.

Interopérabilité

Lorsque le mode DR est activé sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI, la négociation de tunnels VPN est possible uniquement avec des correspondants respectant également ces recommandations. Ceci implique donc que **tous les correspondants compatibles IPsec DR de l'architecture (firewalls SNS, équipements tiers et clients VPN) doivent respecter les recommandations IPsec DR de l'ANSSI**.

Par exemple, un firewall dans une version SNS respectant ces recommandations et avec le mode DR activé :

- Peut établir des tunnels VPN en mode DR avec des correspondants (firewalls SNS, équipements tiers et clients VPN) respectant les recommandations IPsec DR de l'ANSSI,
- Ne peut pas établir de tunnels VPN :
  - Avec tout correspondant ne respectant pas ces recommandations, même si le mode DR est activé sur celui-ci. Ceci inclut les versions SNS non mentionnées ci-dessous,
  - Avec tout correspondant en mode IPsec "standard".

Versions SNS respectant les recommandations IPsec DR de l'ANSSI

- SNS 4.3.21 LTSB et versions 4.3 LTSB supérieures,
- SNS 4.7 et versions supérieures.

Compatibilité des clients VPN IPsec Stormshield avec le mode DR

Seul SN VPN Client Exclusive 7.4.018 (et versions supérieures) peut établir des tunnels VPN en mode DR avec des firewalls dans une version SNS respectant les recommandations IPsec DR de l'ANSSI.

Si vous utilisez des clients VPN Standard Stormshield, l'activation du mode DR nécessite de le désinstaller au profit de SN VPN Client Exclusive (soumis à l'achat d'une licence spécifique).

Impacts réseau

Les paquets de négociation du tunnel VPN IPsec ainsi que les paquets ESP sont échangés exclusivement sur le port UDP/4500.

Si le firewall à paramétrer en mode DR est séparé de son correspondant par d'autres équipements de sécurité, vous devez autoriser le port UDP/4500 entre le firewall SNS et son correspondant sur ces équipements.

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 des bi-clés et de signature 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 à l'ensemble de la chaîne de confiance, c'est-à-dire en partant depuis le certificat du correspondant et en remontant 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=Lille,O=Stormshield,OU=Doc,CN=DR-Firewall),
- *Subject Alternative Name* (SAN). Il s'agit d'un des alias éventuellement définis lors de la création du certificat du correspondant (exemple : DR-Firewall.stormshield.eu).

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 List* (CRL) de l'ensemble de la chaîne de confiance (CA racine [*Root CA*], sous-CA et certificats) doit être actif sur le firewall.

Le jeton de configuration *CRLrequired* doit être positionné à la valeur *1* ou *auto* dans la configuration de la politique VPN du firewall pour que ce mécanisme soit actif.

En plus de la vérification de révocation des certificats, la CRL doit être présente et toujours valide pour que la négociation soit fonctionnelle.

Matériel

Sur les firewalls modèles SN-S-Series-220, SN-S-Series-320, SN510, N-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100, SNi20, SNi40 et SNxr1200), le mode DR permet l'utilisation des jeux d'instructions cryptographiques matérielles du coprocesseur. Les instructions dites "AES-NI" bénéficient d'une dérogation car elles sont uniquement constituées "d'instructions simples d'accélération" de certaines opérations cryptographiques.

Sur les firewalls modèles SN160, SN160W, SN210, SN210W et SN310, le mode DR force la désactivation de ces jeux d'instructions, ce qui entraîne des baisses de performances lors du chiffrement.

Mettre à jour un firewall SNS déjà configuré en mode DR

Pour mettre à jour un firewall déjà configuré en mode DR vers une version SNS plus récente respectant les recommandations IPsec DR de l'ANSSI, des manipulations supplémentaires peuvent être nécessaires selon la version d'origine.

Depuis une version SNS 4.3.21 LTSB et versions 4.3 LTSB supérieures ou SNS 4.7 et supérieures

Reportez-vous à la section Installer cette version des Notes de Version Stormshield Network Security (SNS) pour mettre à jour le firewall.

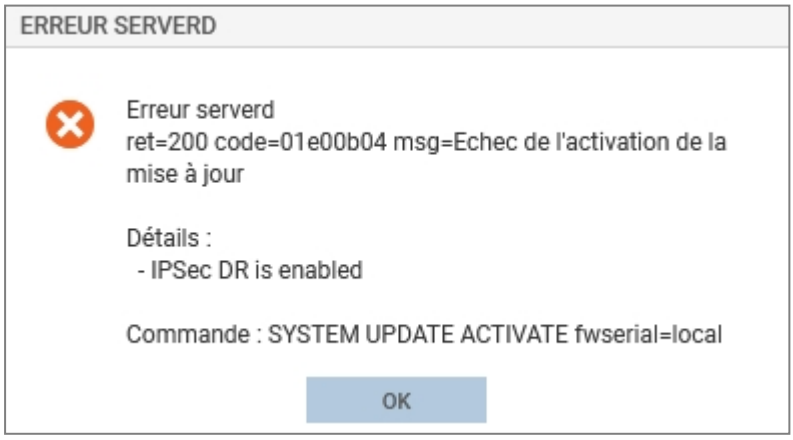
Depuis une version SNS 4.2, 4.3 LTSB inférieure à 4.3.21 LTSB ou 4.6

1. Consultez impérativement la section Évaluer l'impact de l'activation du mode DR.
2. Si vous utilisez des clients VPN Exclusive Stormshield, assurez-vous que chaque client est en version 7.4.018 ou supérieure, puis ajoutez des paramètres personnalisés dans la configuration des passerelles (IKE Auth). Pour plus d'informations, reportez-vous à la section Mettre la configuration d'un client mobile IPsec en conformité avec le mode DR.
3. Reportez-vous ensuite à la section Installer cette version des Notes de Version Stormshield Network Security (SNS) pour mettre à jour le firewall.

Depuis une version SNS inférieure à 4.2

Le mode DR implémenté dans les versions SNS 4.2 apporte des modifications importantes par rapport au mode DR des versions précédentes. Il n'est donc pas possible de mettre à jour en version SNS 4.2 et supérieure un firewall sur lequel le mode DR était déjà activé.

Lors d'une telle tentative, une erreur s'affiche :



Pour mettre à jour le firewall SNS :

1. Consultez impérativement la section Évaluer l'impact de l'activation du mode DR.
2. Dans le module **Configuration** > onglet **Configuration Générale** > cadre **Paramètres cryptographiques**, décochez la case **Activer le Mode "Diffusion restreinte" (DR)** pour désactiver le mode DR. L'intitulé peut-être différent d'une version SNS à une autre.

3. Redémarrez le firewall SNS pour prendre en compte la désactivation du mode DR.
4. Mettez à jour le firewall SNS. Pour plus d'informations, reportez-vous aux Notes de Version Stormshield Network Security (SNS).
5. Mettez en conformité la configuration du firewall SNS avec le mode DR.
6. Cochez la case **Activer le mode de conformité « Diffusion Restreinte (DR) » version 2021** pour activer le mode DR.
7. Redémarrez le firewall SNS pour prendre en compte l'activation du mode DR.

> **IMPORTANT**
> Si la politique IPsec nouvellement configurée sur le firewall utilise des paramètres incompatibles avec le mode DR, son activation **entraîne la désactivation de cette politique IPsec** et l'affichage du message d'avertissement : "*Le mode 'Diffusion Restreinte' a désactivé la configuration VPN non conforme*".

8. Si vous utilisez des clients VPN IPsec Stormshield, assurez-vous de bien utiliser SN VPN Client Exclusive en version 7.4.018 ou supérieure, puis vérifiez leur configuration. Pour plus d'informations, reportez-vous à la section Mettre la configuration d'un client mobile IPsec en conformité avec le mode DR.

Activer le mode DR sur un firewall SNS sans configuration IPsec existante

Pour activer le mode DR sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI et en configuration d'usine ou sans politique IPsec existante :

1. Consultez impérativement la section Évaluer l'impact de l'activation du mode DR.
2. Mettez en conformité la configuration du firewall SNS avec le mode DR,
3. Si vous utilisez des clients VPN IPsec Stormshield, assurez-vous de bien utiliser SN VPN Client Exclusive en version 7.4.018 ou supérieure, puis vérifiez leur configuration. Pour plus d'informations, reportez-vous à la section Mettre la configuration d'un client mobile IPsec en conformité avec le mode DR.
4. Dans le module **Configuration** > onglet **Configuration Générale** > cadre **Paramètres cryptographiques**, cochez la case **Activer le mode de conformité « Diffusion Restreinte (DR) » version 2021** pour activer le mode DR.
5. Redémarrez le firewall SNS pour prendre en compte l'activation du mode DR.

IMPORTANT
Si la politique IPsec nouvellement configurée sur le firewall utilise des paramètres incompatibles avec le mode DR, son activation **entraîne la désactivation de cette politique IPsec** et l'affichage du message d'avertissement : "*Le mode 'Diffusion Restreinte' a désactivé la configuration VPN non conforme*".

Mettre en conformité la configuration du firewall SNS avec le mode DR

Cette section explique comment mettre en conformité avec le mode DR la PKI et la politique IPsec du firewall SNS.

Mettre la PKI en conformité 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 à l'ensemble de la chaîne de confiance, c'est à dire en partant depuis le 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. 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.
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.

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

1. Placez-vous sous votre *Root CA* et créez une sous-CA1 respectant les critères précédents.
2. Créez une sous-CA2 de la sous-CA1 respectant ces mêmes critères : cette nouvelle sous-CA2 sera le *Trust Anchor* de la chaîne de confiance.
   En effet, bien que la première sous-CA1 respecte les recommandations IPsec DR pour la signature des certificats des correspondants, son propre certificat a été signé par la RootCA qui elle ne respecte pas ces critères. Le certificat de la sous-CA1 n'est donc pas conforme aux recommandations IPsec DR.

Depuis ce *Trust Anchor* :

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 / est créée sur le firewall SNS dans une version respectant les recommandations IPsec DR.

Si une CA (ou sous-CA) respectant les recommandations IPsec DR existe déjà sur le firewall

Sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

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 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 un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

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** (*CA-DR* 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 cette CRL sur chacun des points de distribution de CRL précisés lors de la création de la CA.

Créer l'identité du firewall en mode DR (si elle n'existe pas) et de chacun de ses correspondants

Pour les correspondants de type passerelle

Sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI.**
2. Sélectionnez la CA signant les certificats pour le mode DR (*CA-DR* dans cet exemple).
3. Cliquez sur **Ajouter** et sélectionnez **Identité serveur**.
4. Saisissez le nom de domaine qualifié du firewall correspondant (exemple : *FW-Full-DR.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 (*CA-DR* 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. Sélectionnez impérativement 256 bits pour la **Taille de clé**.
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 un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

1. Placez-vous dans le module **Configuration** > **Objets** > **Certificats et PKI.**
2. Sélectionnez la CA signant les certificats pour le mode DR (*CA-DR* 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 (*CA-DR* 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. Sélectionnez impérativement 256 bits pour la **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 créer l'identité de chaque correspondant mobile.

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

Sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

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 dans une version SNS respectant les recommandations IPsec DR :

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**.

Supprimer les clés privées des identités des correspondants sur le firewall (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 (par exemple, le firewall dans une version SNS respectant les recommandations IPsec DR) :

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.

Mettre la politique IPsec en conformité avec le mode DR

Vérifier / Modifier la version IKE utilisée par les correspondants

Sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants.**
2. Sélectionnez un correspondant utilisé dans la politique IPsec à rendre compatible avec le mode DR (**Passerelles distantes** et **Correspondants mobiles**).
3. Dans le cadre **Général**, vérifiez que le champ **Version IKE** est sur **IKEv2**.
   Si ce n'est pas le cas, vous devez modifier la configuration IPsec du correspondant en ce sens et de sélectionner **IKEv2** pour ce champ.

Répétez cette procédure pour chacun des correspondants concernés (passerelles et correspondants mobiles).

Vérifier / Modifier la méthode d'authentification utilisée par les correspondants

Sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants.**
2. Sélectionnez un correspondant utilisé dans la politique IPsec à rendre compatible avec le mode DR (**Passerelles distantes** et **Correspondants mobiles**).

3. Dans le cadre **Identification**, vérifiez que le champ **Méthode d'authentification** est positionné sur **Certificat**.
   Si ce n'est pas le cas, vous devez (faire) modifier la configuration IPsec du correspondant en ce sens et de sélectionner **Certificat** pour ce champ.
4. Dans le cadre **Identification**, vérifiez que le champ **ID du correspondant** est renseigné.
   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=Lille,O=Stormshield,OU=Doc,CN=DR-Firewall),
   - *Subject Alternative Name* (SAN). Il s'agit d'un des alias éventuellement définis lors de la création du certificat du correspondant (exemple : DR-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 de définir un SAN lors de la création du certificat du correspondant et d'utiliser ce SAN comme ID de correspondant.

Répétez cette procédure pour chacun des correspondants concernés (passerelles et correspondants mobiles).

Ajouter dans les Autorités de certification acceptées la CA utilisée pour signer les certificats

Sur chaque correspondant concerné (passerelles uniquement) :

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Identification**.
2. Dans la grille **Autorités de certification acceptées**, vérifiez que l'autorité de certification utilisée pour signer les certificats du mode DR est présente (*CA-DR* dans cet exemple).
3. Si ce n'est pas le cas, cliquez sur **Ajouter** et sélectionnez l'autorité de certification concernée.

Vérifier / Modifier les algorithmes d'authentification et de chiffrement

Sur un firewall dans une version SNS respectant les recommandations IPsec DR de l'ANSSI :

1. Placez-vous dans le module **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Sélectionnez un correspondant utilisé dans la politique IPsec à rendre compatible avec le mode DR (**Passerelles distantes** et **Correspondants mobiles**).
3. Dans le cadre **Général**, vérifiez que le champ **Profil IKE** est positionné sur un profil compatible avec le mode DR (profil **DR** fourni par défaut ou profil personnalisé - *CUSTOM-DR-COMPLIANT* dans cet exemple).
   Si ce n'est pas le cas, vous devez modifier la configuration IPsec du correspondant en ce sens et de sélectionner un profil compatible avec le mode DR (profil **DR** fourni par défaut ou profil personnalisé - *CUSTOM-DR-COMPLIANT* dans cet exemple) pour ce champ.

Répétez cette procédure pour chacun des correspondants concernés (passerelles et correspondants mobiles).

Définir les profils de chiffrement DR comme profils par défauts

Cette procédure permet de définir les profils DR comme profils proposés par défaut pour tous les futurs correspondants devant être crées sur le firewall.

Sur l'ensemble des correspondants concernés (passerelles uniquement) :

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**.
   Les caractéristiques du profil s'affichent :
   - 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**.
   Le profil IKE DR 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**.
   Les caractéristiques du profil s'affichent :
   - 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**.
   Le profil IPsec DR est désormais utilisé par défaut pour les tunnels IPsec définis dans la configuration du firewall.

Mettre la configuration d'un client mobile IPsec en conformité 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.

Rappel concernant les clients VPN IPsec Stormshield

Seul SN VPN Client Exclusive 7.4.018 (et versions supérieures) peut établir des tunnels VPN en mode DR avec des firewalls dans une version SNS respectant les recommandations IPsec DR de l'ANSSI.

Si vous utilisez des clients VPN Standard Stormshield, l'activation du mode DR nécessite de le désinstaller au profit de SN VPN Client Exclusive (soumis à l'achat d'une licence spécifique).

Sur le poste client :

1. Désinstallez SN VPN Client Standard.
2. Téléchargez SN VPN Client Exclusive. Pour plus d'informations, reportez-vous à la section Télécharger cette version des Notes de Version Stormshield VPN Client Exclusive.
3. Installez SN VPN Client Exclusive. Pour plus d'informations, reportez-vous à la section Installation du Guide de l'administrateur Stormshield VPN Client Exclusive.

Créer un tunnel compatible avec le mode DR sur SN VPN Client Exclusive

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

Lancer et activer SN VPN Client Exclusive

1. Sur le bureau Windows du poste client, lancez Stormshield VPN Client Exclusive.
2. Au premier lancement, saisissez le numéro de licence de Stormshield VPN Client Exclusive 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 de Stormshield VPN Client Exclusive :

1. Faites un clic droit sur IKEv2 et sélectionnez **Nouvel IKE auth**.
Une passerelle, nommée par défaut *Ikev2Gateway*, est créée.

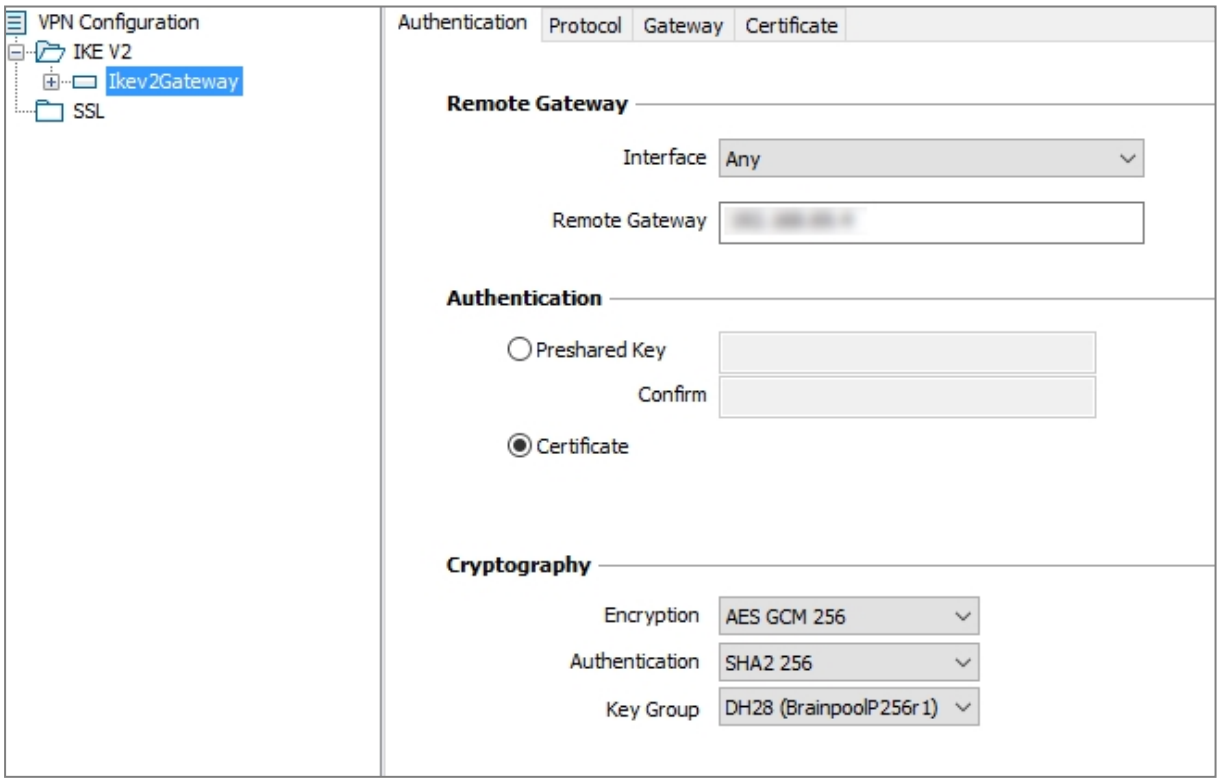
2. Vous pouvez la renommer en effectuant un clic droit sur cette passerelle et en sélectionnant **Renommer**.

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

Sélectionnez la passerelle créée précédemment.

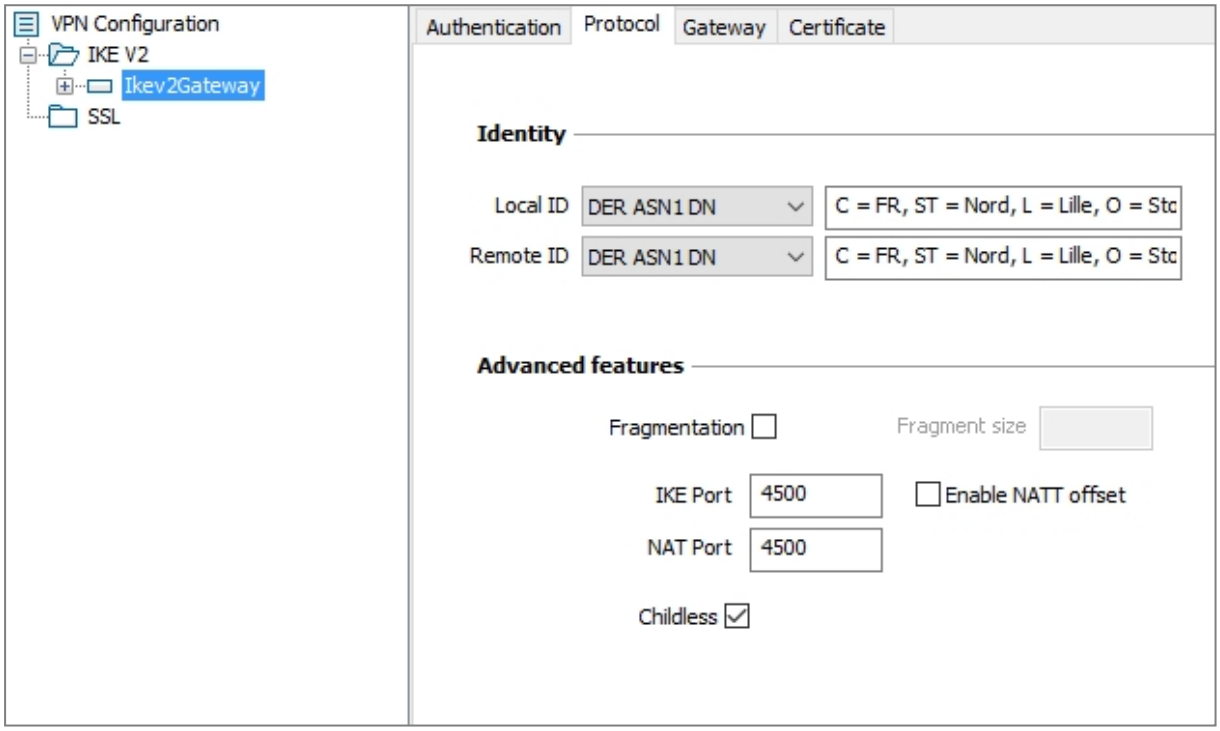
Onglet Authentification

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 **Authentification** 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 en version SNS 4.3 Transition DR (*C = FR, ST = Nord, L = Lille, O = Stormshield, OU = Doc, CN = DR-Compliant.stormshield.eu* dans cet exemple).
2. Dans le cadre **Fonctions avancées** :
   1. Positionnez le **Port IKE** à 4500,
   2. Cochez la case **Initiation Childless**.



Onglet Passerelle

Vous pouvez laisser les paramètres par défaut.

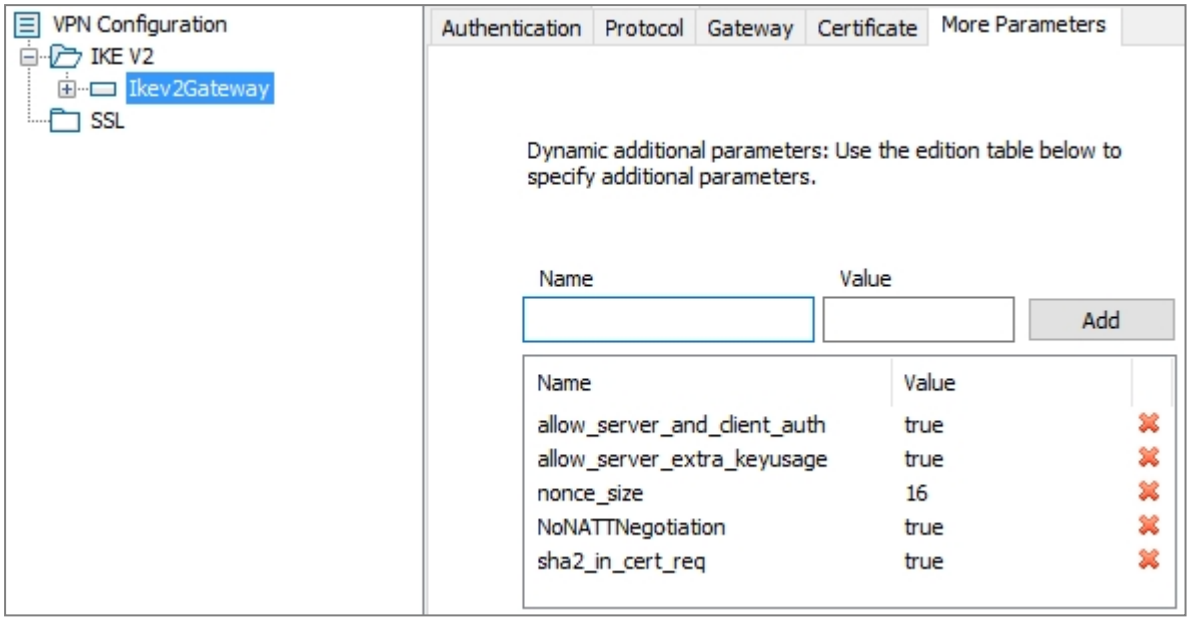
> **NOTE**
> Pour le paramètre durée de vie, il peut être intéressant de positionner une valeur inférieure à celle configurée sur la passerelle (firewall en mode DR) afin que les renégociations soient à l'initiative de SN VPN Client Exclusive.

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 de SN VPN Client Exclusive 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 (*FW_DR* dans cet exemple) 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**.
   Le nom choisi dans cet exemple est *Tunnel_DR*.

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

Sélectionnez le tunnel créé précédemment.

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 (*FW_DR* dans cet exemple) : 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 (*FW_DR* dans cet exemple) : DH28 (BrainpoolP 256r1) ou DH19 (ECP 256).
   - Pour le champ **Numéro de séquence étendu**, sélectionnez *auto*.

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 de SN VPN Client Exclusive pour valider et sauvegarder cette configuration.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur le mode DR sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

STORMSHIELD

documentation@stormshield.eu