TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

IPSEC - DIFFUSION RESTREINTE MODE

Product concerned: SNS in 4.3.21 LTSB and higher versions of 4.3 LTSB, SNS 4.7 and higher versions, VPN Client Exclusive in 7.4 and higher versions

Document last updated: December 13, 2023

Reference: sns-en-diffusion_restreinte_ipsec_mode_technical_note

Table of contents

Change log

Date	Description
December 13, 2023	- Spelling correction of custom parameter *NoNATTNegotiation* ("Creating a DR mode-compatible tunnel on SN VPN Client Exclusive" section)
November 2, 2023	- SNS 4.7 release
October 18, 2023	- Changes to sections "Assessing the impact of enabling DR mode", "Updating an SNS firewall that has already been configured in DR mode" and "Ensuring the compliance of the SNS firewall's configuration with DR mode" - Addition of section "Ensuring the compliance of a mobile IPsec client's configuration with DR mode"
September 12, 2022	- Addition of section "Stormshield IPsec VPN client" - Changes to the section "Selecting authentication and encryption algorithms"
December 08, 2021	- Changes to the section "Enabling verification of peer certificate revocation"
August 27, 2021	- Changes to section "Evaluating the impact of DR mode (SNS v4.2 and upwards)"
August 25, 2021	- New document

Getting started

"*Diffusion Restreinte* (DR)" (restricted) mode forces the firewall to comply with the ANSSI's (French national information security agency) recommendations on the use of coprocessors and cryptographic accelerators on products to be qualified. This mode must be enabled on networks that fall under the "Restricted" category.

This mode relies in particular on the use of software versions for asymmetric and symmetric cryptographic algorithms and random key generation algorithms.

In this technical note, "*Diffusion Restreinte* (DR)" mode is referred to in its short form "DR mode".

The sections in this technical note explain the operations that you can perform on SNS firewalls. Continue according the actions that you wish to perform:

- Assessing the impact of enabling DR mode,
- Updating an SNS firewall that has already been configured in DR mode,
- Enabling DR mode on an SNS firewall that does not have an existing IPsec configuration,
- Ensuring the compliance of the SNS firewall's configuration with DR mode,
- Ensuring the compliance of a mobile IPsec client's configuration with DR mode.

Assessing the impact of enabling DR mode

Carefully read the next section to assess the impact of enabling DR mode on an SNS firewall, and on the entire architecture.

Interoperability

When DR mode is enabled on a firewall in an SNS version that complies with the ANSSI's IPsec DR recommendations, VPN tunnels can only be negotiated with peers that also comply with these recommendations. This implies that **all IPsec DR-compatible peers in the architecture (SNSfirewalls, third-party devices and VPN clients) must comply with the ANSSI's IPsec DR recommendations**.

For example, firewalls in an SNS version that complies with these recommendations, and on which DR mode is enabled:

- Can set up VPN tunnels in DR mode with peers (SNS firewalls, third-party devices and VPN clients) that comply with the ANSSI's IPsec DR recommendations,
- Cannot set up VPN tunnels:
  - With any peers that do not comply with these recommendations, even if DR mode is enabled on them. This includes SNS versions that are not mentioned below,
  - With any peers in standard IPsec mode.

SNS versions that comply with the ANSSI's IPsec DR recommendations

- SNS in 4.3.21 LTSB and higher versions of 4.3 LTSB,
- SNS in 4.7 and higher versions.

Compatibility of Stormshield IPsec VPN clients with DR mode

Only SN VPN Client Exclusive 7.4.018 (and higher versions) can set up VPN tunnels in DR mode with firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations.

If you are using Stormshield standard VPN clients, enabling DR mode requires it to be uninstalled to make way for SN VPN Client Exclusive (a specific license must be purchased).

Impact on the network

IPsec VPN tunnel negotiation packets and ESP packets are exchanged exclusively over UDP port 4500.

If the firewall that will be configured in DR mode is separated from its peer by other security devices, UDP port 4500 must be allowed on these devices between the SNS firewall and its peer.

Conditions to be met for a tunnel to be compatible with DR mode

IKE and IPsec encryption profiles

IKE and IPsec encryption profiles must meet the following constraints, which have been established by IPsec DR guidelines:

- The Diffie-Hellman methods used must belong to either the DH19 NIST Elliptic Curve Group (256-bit) or DH28 Brainpool Elliptic Curve Group (256-bit).
- The algorithms imposed for phase 1 (*Parent Security Association*) and the protection of phase 2 renewals (*Child Security Association*) must either be:
  - AES_GCM_16. As this is an AEAD (Authenticated Encryption with Associated DATA) algorithm, it is not associated with any authentication algorithm.
  - Or AES_CTR, which must be associated with SHA256.

IKE protocol

Only version 2 of the IKE protocol is allowed.

Peer authentication

Only certificate-based authentication is allowed. The following constraints apply to the generation of key pairs and signatures:

- The size of keys used in certificates has been set at 256 bits,
- ECDSA or ECSDSA signature on an ECP 256 (SECP) or BP 256 (Brainpool) curve,
- SHA256 as the hash algorithm.

IMPORTANT
These constraints apply to the entire trust chain, i.e., beginning from the peer certificate up to the first trust anchor (first CA or sub-CA) that complies with these specifications.

The **Peer ID** field must also be filled in, by using one of the following formats:

- *Distinguished Name* (DN). This is the subject of the peer certificate (e.g., C=FR,ST=Nord,L=Lille,O=Stormshield,OU=Doc,CN=DR-Firewall),
- *Subject Alternative Name* (SAN). This is one of the aliases that may be defined when the peer certificate is created (e.g., DR-Firewall.stormshield.eu).

NOTE
The possible length of a certificate's subject may cause compatibility issues with third-party devices, such as encryption mechanisms, VPN gateways, etc. that are not SNS firewalls. In this case, you are strongly advised to define a SAN when creating the peer certificate, and to use this SAN as the Peer ID.

Certificate revocation verification

A mechanism to verify Certificate Revocation Lists (CRLs) on the entire trust chain (Root CA, sub-CA and certificates) must be enabled on the firewall.

The *CRLrequired* configuration token must be set to *1* or *auto* in the firewall's VPN policy configuration in order for this mechanism to be enabled.

In addition to certificate revocation verification, the CRL must be present and valid at all times so that negotiation can function.

Hardware

On 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 and SNxr1200 firewalls, DR mode allows the use of the coprocessor's cryptographic hardware instruction sets. "AES-NI" instructions are exempt as they are made up of only “simple acceleration instructions” of certain cryptographic operations.

On SN160, SN160W, SN210, SN210W, and SN310 firewalls, DR mode will force such instruction sets to be disabled, causing performance to slow down during encryption.

Updating an SNS firewall that has already been configured in DR mode

To update a firewall that has already been configured in DR mode to a more recent SNS version that complies with the ANSSI's IPsec DR recommendations, additional operations may be required, depending on the original version.

From an SNS in 4.3.21 LTSB and higher versions of 4.3 LTSB or SNS in versions 4.7 and higher

Refer to the section Installing this version in Stormshield Network Security (SNS) release notes to update the firewall.

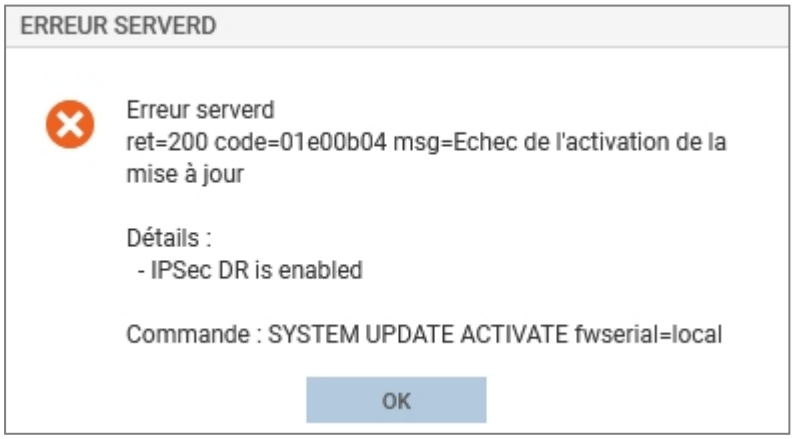
From an SNS in versions 4.2, 4.3 LTSB lower than 4.3.21 LTSB or 4.6

1. First, read the section Assessing the impact of enabling DR mode.
2. If you are using Stormshield VPN Exclusive clients, ensure that each client is in version 7.4.018 or higher, then add custom settings in the gateway configuration (IKE Auth). For more information, refer to the section Ensuring the compliance of a mobile IPsec client's configuration with DR mode".
3. Next, refer to the section Installing this version in Stormshield Network Security (SNS) release notes to update the firewall.

From an SNS version lower than 4.2

DR mode implemented in SNS 4.2 versions apply substantial changes compared to DR mode on previous versions. As such, firewalls on which DR mode is already enabled cannot be updated to SNS version 4.2 or higher.

During attempts to do so, an error will appear:



To update the SNS firewall:

1. First, read the section Assessing the impact of enabling DR mode.
2. In **Configuration** > **General configuration** tab > **Cryptographic settings** section, unselect **Enable "Diffusion Restreinte (DR)" mode** to disable DR mode. The name of the setting may differ from one SNS version to another.

3. Restart the SNS firewall to apply the choice of disabling DR mode.
4. Update the SNS firewall. For more information, refer to the Stormshield Network Security (SNS) release notes.
5. Ensure the compliance of the SNS firewall's configuration with DR mode.
6. Select **Enable "*Diffusion Restreinte* (DR)" 2021 version compliance mode** to enable DR mode.
7. Restart the SNS firewall to apply the choice of enabling DR mode.

> **IMPORTANT**
> If the newly configured IPsec policy on the firewall uses parameters that are not compatible with DR mode, enabling DR mode will **disable this IPsec policy** and show the warning message: "*'Diffusion Restreinte' mode disabled the non-compliant VPN configuration*".

8. If you are using Stormshield IPsec VPN clients, ensure that you use SN VPN Client Exclusive in version 7.4.018 or higher, then check their configuration. For more information, refer to the section Ensuring the compliance of a mobile IPsec client's configuration with DR mode".

Enabling DR mode on an SNS firewall that does not have an existing IPsec configuration

To enable DR mode on a firewall in an SNS version that complies with the ANSSI's IPsec DR recommendations, and which is in factory configuration or does not have an existing IPsec policy:

1. First, read the section Assessing the impact of enabling DR mode.
2. Ensure the compliance of the SNS firewall's configuration with DR mode,
3. If you are using Stormshield IPsec VPN clients, ensure that you use SN VPN Client Exclusive in version 7.4.018 or higher, then check their configuration. For more information, refer to the section Ensuring the compliance of a mobile IPsec client's configuration with DR mode".
4. In **Configuration** > **General configuration** tab > **Cryptographic settings** section, select **Enable "*Diffusion Restreinte* (DR)" 2021 version compliance mode** to enable DR mode.
5. Restart the SNS firewall to apply the choice of enabling DR mode.

IMPORTANT
If the newly configured IPsec policy on the firewall uses parameters that are not compatible with DR mode, enabling DR mode will **disable this IPsec policy** and show the warning message: *"'Diffusion Restreinte' mode disabled the non-compliant VPN configuration".*

Ensuring the compliance of the SNS firewall's configuration with DR mode

This section explains how to ensure that the PKI and SNS firewall's IPsec policy comply with DR mode.

Ensuring the PKI's compliance with DR mode

Recap of IPsec DR recommendations for the PKI

Certificates, from the peer certificate up to the trust anchor, must comply with the following specifications:

- The size of keys used in certificates has been set at 256 bits,
- ECDSA or ECSDSA signature on an ECP 256 (SECP) or BP 256 (Brainpool) curve,
- SHA256 as the hash algorithm.

IMPORTANT
These constraints apply to the entire trust chain, i.e., beginning from the peer certificate up to the first trust anchor (first CA or sub-CA) that complies with these specifications.

External PKIs

If the PKI complies with IPsec DR recommendations (criteria described above)

From the certification authority that will manage the identities of DR mode-compatible peers:

1. Generate the identities of all IPsec peers to be made DR mode-compatible. Do note that SNS firewalls support the EST (enrollment over secure transport) protocol in a DR context.
2. Export these identities (certificate + private key).
3. Import each identity on the peer in question. For SNS firewalls, refer to the section Importing an identity on each peer to be made DR mode-compatible.

If the PKI does not comply with IPsec DR recommendations (criteria described above)

1. Go to your *Root CA* and create a sub-CA1 that complies with the above criteria.
2. Create a sub-CA2 under sub-CA1 that complies with the same criteria: this new sub-CA2 will be the trust anchor of the trust chain.
   Although the first sub-CA1 complies with IPsec DR recommendations regarding the signature of peer certificates, its own certificate was signed by the RootCA, which does not comply with these criteria. The certificate of the sub-CA1 therefore does not comply with IPsec DR recommendations.

From this trust anchor:

1. Generate the identities of all IPsec peers to be made DR mode-compatible.
2. Export these identities (certificate + private key).
3. Import each identity on the peer in question. For SNS firewalls, refer to the section Importing an identity on each peer to be made DR mode-compatible.

Internal PKIs (PKIs on an SNS firewall)

> **NOTE**
> In this example, the CA that signs the certificates of all peers that will be made compatible with DR mode exists/is created on the SNS firewall in a version that complies with IPsec DR recommendations.

If a CA (or sub-CA) that complies with IPsec DR recommendations already exists on the firewall

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. In the list of CAs and certificates, select the CA (or sub-CA) that will sign the IPsec certificates compatible with DR mode.
   Details of this CA (or sub-CA) will appear in the section on the right.
3. In **Details** > **Hashes** section, ensure that the signature algorithm is ecdsa-with-SHA256. If this is not the case, create a CA (or sub-CA) with a **Key type** set to SECP or BRAINPOOL and **Key size** set to 256 bits.
4. In the **Certificate profiles** tab, ensure that the URIs of the CA's (or sub-CA's) CRL distribution points have been specified. If this is not the case, add them.

   > **NOTE**
   > The certificates signed by this CA (or sub-CA) before CRL distribution points were added must be generated again to apply this change.

5. In the **Certificate profiles** tab, ensure in the **Certification authority**, **User certificates** and **Server certificates** sections that:
   - The **Key type** is set to SECP or BRAINPOOL,
   - The **Key size** is set only to 256 bits,
   - The **Checksum** is set to sha256.

   If any of the settings differ from the imposed values, change it to select the right value.
6. Click on **Apply** to apply any changes made.

If a CA that complies with IPsec DR recommendations must be created

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

Creating the CA

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Click on **Add.**
3. Select **Root authority**.
   A wizard will automatically appear.
4. Enter a **Name** (*CA-DR* in this example).
   The **ID** will automatically be filled in with the name of the CA. This name can be changed.

5. Enter the **attributes of the authority**:
   - Organization (O),
   - Organizational Unit (OU),
   - Locality (L),
   - State (ST),
   - Country (C).

> **EXAMPLE**
> Organization (O): Stormshield
> Organizational unit (OU): Documentation
> Locality (L): Lille
> State (ST): Nord
> Country (C): France.

6. Click on **Next**.
7. Enter then confirm the **Password** that protects the CA.
8. You can enter the contact **E-mail address** for this CA.
9. The default **validity** suggested for the CA is 3650 days (recommended value).
   This value can be changed.
10. **Key type**: SECP or BRAINPOOL must be selected.
11. **Key size (bits)**: 256 must be selected.
12. Click on **Next**.
13. **CRL distribution points**: add the URIs of the CRL distribution points that your peers' IPsec devices can contact to verify the validity of the certificates issued by your CA.
14. Click on **Next**.
    A summary of the information regarding the CA will be shown.
15. Confirm by clicking on **Finish**.

Uploading the CRL on distribution points

1. Select the CA created earlier.
2. Click on **Download.**
3. Select **CRL** then the export format (PEM or DER).
   A message will give you the download link.
4. Download the CRL by clicking on the link, then upload the CRL on each of the CRL distribution points that were specified during the creation of the CA.

Creating the identity of the firewall in DR mode (if it does not exist) and of each peer

For gateway peers

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the CA that signs certificates for DR mode (*CA-DR* in this example).
3. Click on **Add** and select **Server identity**.
4. Enter the fully qualified domain name of the corresponding firewall (e.g., *FW-Full-DR.stormshield.eu*).
   The **ID** will automatically be filled in with the fully qualified domain name. This name can be changed.

5. Click on **Next**.
6. Enter the password of the CA that signs this server identity (*CA-DR* in this example).
7. Click on **Next**.
8. Select a **validity** duration in days (365 days suggested by default).
9. The key type suggested by default is compatible with DR mode (BRAINPOOL or SECP): this is the key type of the CA that signs the server identity..
10. The **Key size** selected must be 256 bits.
11. Click on **Next**.
12. An alias can be added for this peer (optional).

> **NOTE**
> When an alias or *Subject Alternative Name* (SAN) is defined, it is indicated in the certificate's *SubjectAltName* field.
> It must be defined by the fully qualified domain name (FQDN) entered in step 4 so that this SAN can be used as the **Peer ID**. The syntax used is simpler than the one used in the certificate's full subject.

13. Click on **Next**.
    A summary of the identity will appear.
14. Click on **Finish** to confirm the creation of the server identity.

Repeat the process to create the identity of each peer concerned (gateways).

For mobile peers

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the CA that signs certificates for DR mode (*CA-DR* in this example).
3. Click on **Add** and select **User identity**.
4. In the **CN** field, enter the name of the peer (e.g., *John Doe*).
   The **ID** will automatically be filled in with the name of the peer. This name can be changed.
5. Enter the e-mail address of the peer (*john.doe@stormshield.eu* in this example).
6. Click on **Next**.
7. Enter the password of the CA that signs this server identity (*CA-DR* in this example).
8. Click on **Next**.
9. Select a **validity** duration in days (365 days suggested by default).
10. The key type suggested by default is compatible with DR mode (BRAINPOOL or SECP): this is the key type of the CA that signs the server identity..
11. The **Key size** selected must be 256 bits.
12. Click on **Next**.
    A summary of the identity will appear.
13. Click on **Finish** to confirm the creation of the user identity.

Repeat the process to create the identity of each mobile peer.

Exporting the identity of each peer to be made DR mode-compatible

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the server identity to export.
3. Click on **Download**: select **Identity** then **In P12 format**.
4. In the **Enter password** field: create a password that will be used to protect the P12 file.
5. **Confirm** the password.
6. Click on **Download certificate (P12)**.
7. Save this file in P12 format on your workstation.

Repeat the process to export the identity of each peer concerned (gateways and mobile peers).

Importing an identity on each peer to be made DR mode-compatible

On every gateway peer other than the firewall in an SNS version that complies with IPsec DR recommendations:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Click on **Add** and select **Import a file**.
3. In the **Password** field (if the file is a PKCS#12 container), enter the password that protects the .P12 file.
4. Click on **Import**.

Deleting the private keys of peer identities on the firewall (recommended)

Once the P12 file has been imported on the peer to be made DR mode-compatible, you are strongly advised to delete the private key of this peer's identity.

On the firewall that hosts the CA (e.g., the firewall in an SNS version that complies with IPsec DR recommendations):

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the server identity of the peer whose private key you wish to delete.
3. Click on **Action**: select **Remove private key**.
   The private key will then be immediately deleted.

Repeat this procedure for each peer concerned (gateways and mobile peers).

Enabling verification of peer certificate revocation

The Certification authority (CA) that issues the certificates used to authenticate IPsec peers must implement a revocation mechanism (CRLs and CRL distribution points or OCSP servers). In addition, verification of certificates issued by this CA must be enabled on peers. When this parameter is enabled, you must have all the CRLs in the certification chain. Otherwise, the current IPsec policy will be disabled and the error message "Disabling CRL verification is not compatible with DR mode" will appear in the **Check policy** field found under the IPsec policy grid.

On all peers to which DR mode applies:

1. Go to **Configuration** > **System** > **CLI console**.
2. Type the following series of commands:
   ```
   CONFIG IPSEC UPDATE slot=x CRLrequired=1
   CONFIG IPSEC CHECK index=1
   CONFIG IPSEC ACTIVATE
   ```
   where x represents the number of the IPsec policy to modify.
3. Click on **Run**.

Enabling automatic CRL retrieval

On every peer concerned:

1. Go to **Configuration > General configuration** tab.
2. Select the checkbox **Enable regular retrieval of certificate revocation lists (CRL)**.

If the CRL of a peer's CA is not retrieved, tunnels cannot be set up with this peer.

Ensuring the compliance of an IPsec policy with DR mode

Checking/changing the IKE version used by peers

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Select a peer used in the IPsec policy, to make it compatible with DR mode (**Remote gateways** and **Mobile peers**).
3. In the **General** section, ensure that the **IKE version** field is set to **IKEv2**.
   If this is not the case, change the peer's IPsec configuration so that **IKEv2** is selected for this field.

Repeat this procedure for each peer concerned (gateways and mobile peers).

Checking/changing the authentication method used by peers

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Select a peer used in the IPsec policy, to make it compatible with DR mode (**Remote gateways** and **Mobile peers**).
3. In the **Identification** section, ensure that the **Authentication method** field is set to **Certificate**.
   If this is not the case, change the peer's IPsec configuration so that **Certificate** is selected for this field.
4. In the **Identification** section, ensure that the **Peer ID** is entered.
   This field must use one of the following formats:
   - *Distinguished Name* (DN). This is the subject of the peer certificate (e.g., C=FR,ST=Nord,L=Lille,O=Stormshield,OU=Doc,CN=DR-Firewall),
   - *Subject Alternative Name* (SAN). This is one of the aliases that may be defined when the peer certificate is created (e.g., DR-Firewall.stormshield.eu).

> **NOTE**
> The possible length of a certificate's subject may cause compatibility issues with third-party devices (encryption mechanisms encryption mechanisms, VPN gateways, etc. that are not SNS firewalls). In this case, you are strongly advised to define a SAN when creating the peer certificate, and to use this SAN as the Peer ID.

Repeat this procedure for each peer concerned (gateways and mobile peers).

Adding the CA that signs certificates to the list of trusted certification authorities

On every peer concerned (gateways only):

1. Go to **Configuration > VPN > IPsec VPN > Identification** tab.
2. In the **Approved certification authorities** grid, ensure that the certification authority that will be used to sign DR mode certificates is present (*CA-DR* in this example).
3. If this is not the case, click on **Add** and select the certification authority in question.

Checking/changing the authentication and encryption algorithms

On firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations:

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Select a peer used in the IPsec policy, to make it compatible with DR mode (**Remote gateways** and **Mobile peers**).
3. In the **General** section, ensure that the **IKE profile** field is set to a DR mode-compatible profile (**DR** profile provided by default of custom profile - *CUSTOM-DR-COMPLIANT* in this example).
   If this is not the case, change the peer's IPsec configuration and select a DR mode-compatible profile (**DR** profile provided by default of custom profile - *CUSTOM-DR-COMPLIANT* in this example) for this field.

Repeat this procedure for each peer concerned (gateways and mobile peers).

Setting DR encryption profiles as default profiles

This procedure makes it possible to set DR profiles as the profiles suggested by default for all future peers that must be created on the firewall.

On all peers concerned (gateways only):

1. Go to **Configuration > VPN > IPsec VPN > Encryption profiles** tab.
2. In the menu on the left, under the **IKE** section, select the **DR** profile.
   The characteristics of the profile will be shown:
   - Two Diffie-Hellman profiles are offered: DH28 Brainpool Elliptic Curve Group (256-bits), selected by default, and DH19 NIST Elliptic Curve Group (256-bits).
   - The AES_GCM_16 algorithm is selected as the default proposal, and AES_CTR as the second proposal.

   The **Encryption strength** of the chosen algorithm must not be modified.
3. Click on the **Actions** menu.
4. Select **Define the default profile**.
   The IKE DR profile is now used by default for new IPsec tunnels added to the firewall's configuration.
5. In the menu on the left, under the **IPsec** section, select the **DR** profile.
   The characteristics of the profile will be shown:
   - The HMAC_SHA256 algorithm is selected as the authentication proposal.
   - The AES_GCM_16 algorithm is selected as the default encryption proposal, and AES_CTR as the second proposal.

   The **Encryption strength** of the chosen algorithm must not be modified.
6. Click on the **Actions** menu.
7. Select **Define the default profile**.
   The IPsec DR profile is now used by default for IPsec tunnels defined in the firewall's configuration.

Ensuring the compliance of a mobile IPsec client's configuration with DR mode

This section explains the options to enable and the settings to select to make the configuration of mobile IPsec clients compatible with the ANSSI's IPsec DR recommendations.

Reminder regarding Stormshield IPsec VPN clients

Only SN VPN Client Exclusive 7.4.018 (and higher versions) can set up VPN tunnels in DR mode with firewalls in an SNS version that complies with the ANSSI's IPsec DR recommendations.

If you are using Stormshield standard VPN clients, enabling DR mode requires it to be uninstalled to make way for SN VPN Client Exclusive (a specific license must be purchased).

On the client workstation:

1. Uninstall SN VPN Client Standard
2. Download the SN VPN Client Exclusive For more information, refer to the section Download this version in the Stormshield VPN Client Exclusive release notes.
3. Install the SN VPN Client Exclusive For more information, refer to the section on Installation in the Stormshield VPN Client Exclusive administration guide.

Creating a DR mode-compatible tunnel on SN VPN Client Exclusive

IMPORTANT
To configure SN VPN Client Exclusive, you must run it with administrator privileges on the client workstation (right-click on the Stormshield VPN Client Exclusive icon > **Run as administrator**).

Running and enabling SN VPN Client Exclusive

1. On the Windows desktop on the client workstation, run Stormshield VPN Client Exclusive.
2. The first time it is launched, enter the Stormshield VPN Client Exclusive license number for the user concerned.

Allowing the display of additional parameters

1. Click on **Tools** > **Options** in the general menu.
2. In the **General** tab: select **Show more parameters** and confirm by clicking on **OK**.

Creating a new gateway

In the left column in Stormshield VPN Client Exclusive:

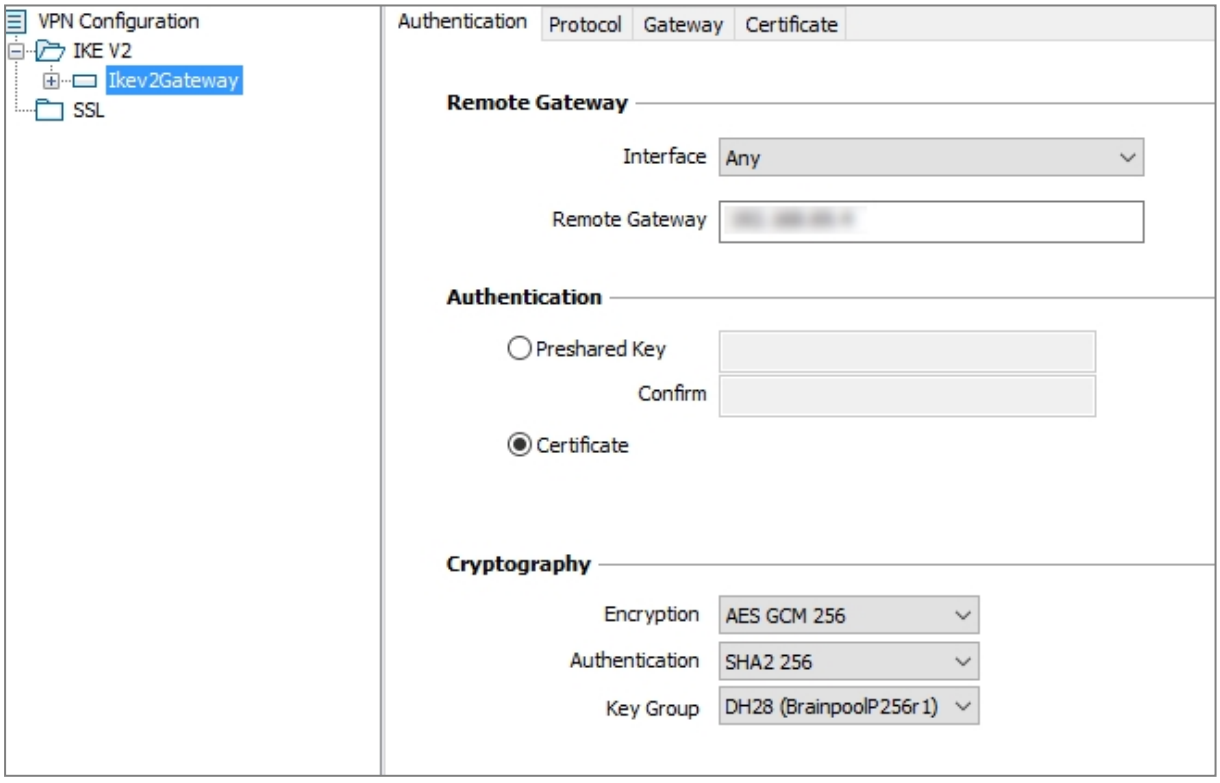
1. Right-click on IKEv2 and select **New IKE Auth**.
   A gateway, named *Ikev2Gateway* by default, is created.
2. It can be renamed by right-clicking on this gateway and selecting **Rename**.

Adapting the gateway's parameters to make it compatible with DR mode

Select the gateway created earlier.

Authentication tab

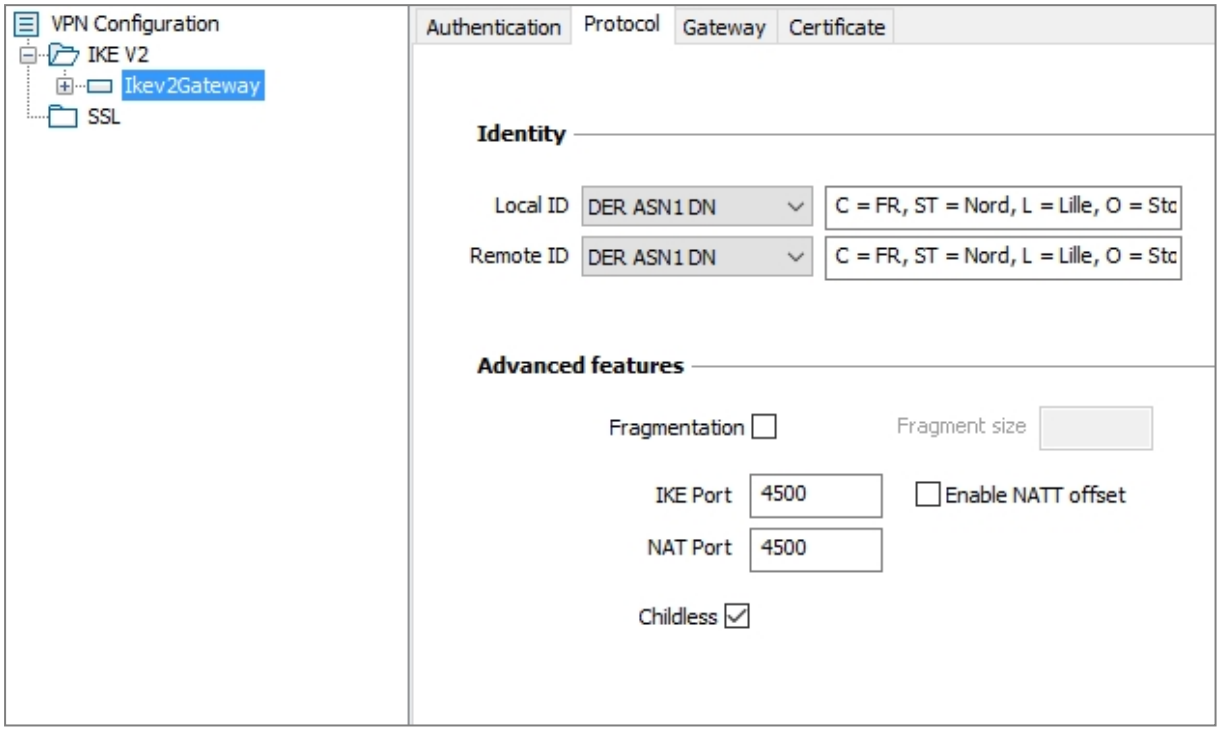
1. In the **Remote Gateway** field, enter the IP address or FQDN of the firewall with which the DR mode-compatible tunnel will be set up.
2. In the **Authentication** section, select **Certificate**.
   You will be automatically directed to the **Certificate** tab.
3. Click on **Import a certificate**.
4. Select **P12 format** and click on **Next**.
5. Select the identity of the mobile client that was exported earlier in P12 format on the firewall in question.
6. Enter the password that protects this identity.
7. Confirm by clicking on **OK**.
8. Click on the **Authentication** tab again.
9. In the **Cryptography** section, select the values that match those selected for the DR encryption profile on the firewall in question:
   - **Encryption**: AES GCM 256 or AES CTR 256,
   - **Integrity**: SHA2 256,
   - **Key group**: DH28 (BrainpoolP 256r1) or DH19 (ECP 256).



Protocol tab

1. In the **Identity** section, in the **Remote ID** field: select **DER ASN1 DN** and indicate the subject of the gateway certificate in SNS version 4.3 Transition DR (*C = FR, ST = Nord, L = Lille, O = Stormshield, OU = Doc, CN = DR-Compliant.stormshield.eu* in this example).

2. In the **Advanced properties** section:
   1. Set the **IKE Port** to 4500,
   2. Select the **Childless** checkbox.



Gateway tab

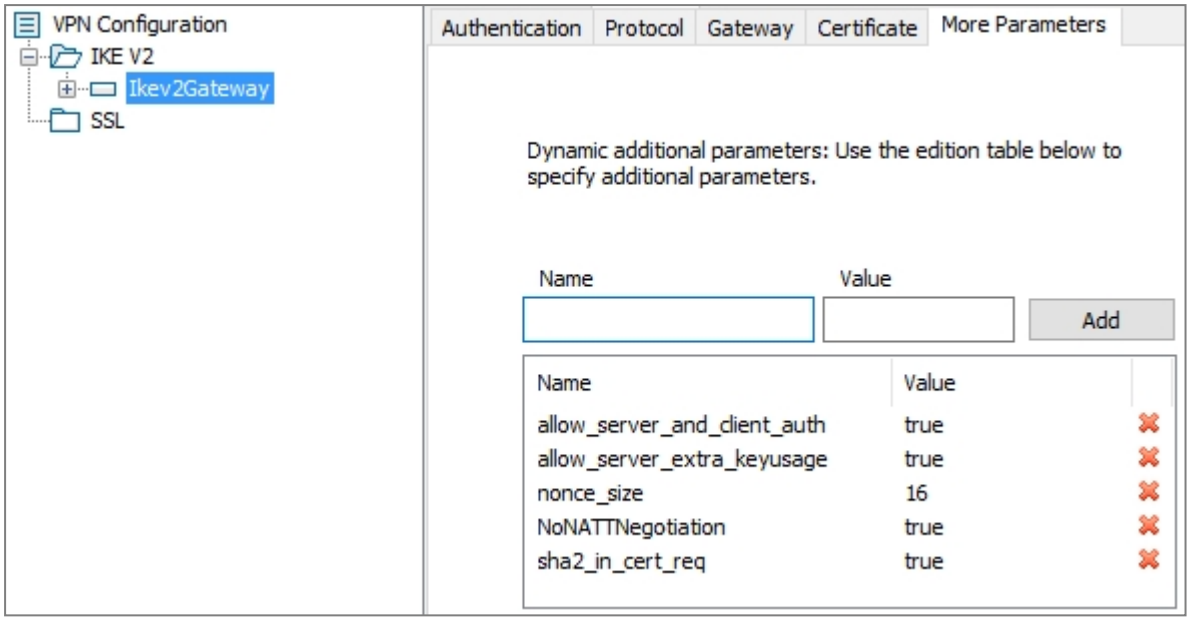
You can leave the default settings.

> **NOTE**
> For the lifetime setting, it may be helpful to set a value lower than the one configured on the gateway (firewall in DR mode) so that SN VPN Client Exclusive initiates renegotiations.

More parameters tab

1. If the parameter "Method14_RSASSA_PKCS1" is present, delete it.
2. Add the custom parameters with the following values:

Name	Value
nonce_size	16
NoNATTNegotiation	true
sha2_in_cert_req	true
allow_server_and_client_auth	true
allow_server_extra_keyusage	true



Backing up the configuration

Click on **Configuration** > **Save** in the SN VPN Client Exclusive general menu to confirm and save this configuration.

Creating the tunnel to the DR mode-compatible gateway

1. Right-click on the gateway that was created earlier (*FW_DR* in this example) and selected **New Child SA**.
   A tunnel, named *Ikev2Tunnel* by default, is created.
2. It can be renamed by right-clicking on this tunnel and selecting **Rename**.
   The name chosen in this example is *Tunnel_DR*.

Adapting the tunnel's parameters to make it compatible with DR mode

Select the tunnel created earlier.

Child SA tab

1. Select the checkbox **Request configuration from the gateway**.
2. In the **Cryptography** section:
   - In the **Encryption** field, select the same value as the one configured for the gateway that was created earlier (*FW_DR* in this example): AES GCM 256 or AES CTR 256.
   - Select *auto* for the **Integrity** field.
   - In the **Diffie-Hellman** field, select the same value as the one configured for the gateway that was created earlier (*FW_DR* in this example): DH28 (BrainpoolP 256r1) or DH19 (ECP 256).
   - Select *auto* for the **Extended sequence number** field.
3. In the **Lifetime** section, select *1800* (seconds) for the **Child SA Lifetime** field.

Backing up the configuration

Click on **Configuration** > **Save** in the SN VPN Client Exclusive general menu to confirm and save this configuration.

Further reading

Additional information and responses to questions you may have about DR mode are available in the Stormshield knowledge base (authentication required).

STORMSHIELD

documentation@stormshield.eu