TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

TRANSITION DR MODE: GRADUALLY MAKE IPSEC ARCHITECTURE COMPATIBLE WITH DR MODE

Product concerned: SNS 5.0 and higher versions

Document last updated: May 20, 2025

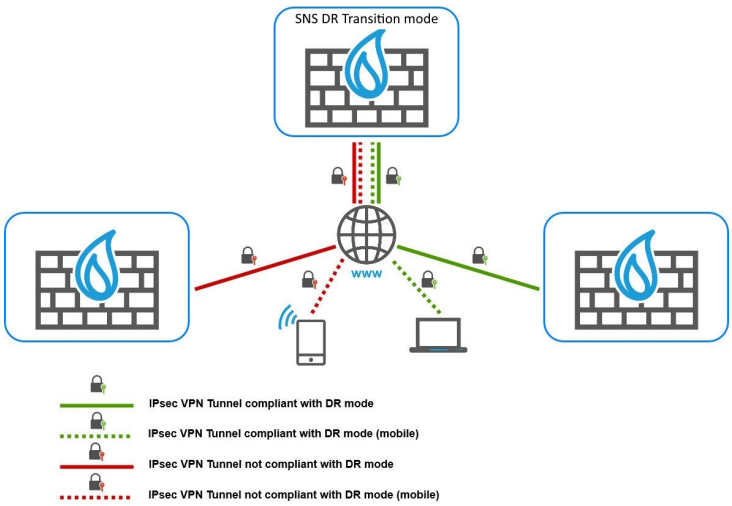
Reference: sns-en-ipsec_SNS_v5_Transition_DR_Mode_technical_note

Table of contents

Change log

Date	Description
May 20, 2025	New document

Getting started



In *Diffusion Restreinte* (DR) mode, which was introduced in SNS version 4.2, policies that comply with IPsec DR specifications set by the ANSSI are not allowed to coexist with policies that comply with the IPsec standard (RFC 7292 IKEv2bis).

Refer to the SNS user guide for more information on *Diffusion Restreinte* (DR) mode.

In SNS version 5, IPsec VPN tunnels that comply with DR mode requirements can be configured, while retaining the possibility of setting up IPsec VPN tunnels that do not comply with these requirements. This feature applies to complex architectures in which the process of making them DR-compliant has to go through a transitional phase, during which IPsec DR and standard (non-DR) policies are made to coexist.

To do so, a configuration option, which was introduced in version 5, makes it possible to determine on the IPsec peer whether tunnels that are negotiated with this peer have to comply with DR mode requirements. The constraints that are imposed by this configuration option are the same as those in DR mode, and the configuration of a DR-compliant IPsec VPN tunnel has to follow the requirements described in the section Assessing the impact of enabling DR mode.

As soon as all peers have been modified to be DR compliant, full DR mode can be enabled on the version 5 SNS firewall, and on its peers.

This option is referred to as "DR transition mode" in the rest of this technical note.

Understanding the impact of DR mode

This section explains several specific characteristics of DR mode, their impact on SNS firewalls, and on the IPsec architecture in question.

Interoperability

When DR mode is enabled on an SNS firewall that complies with the ANSSI's IPsec DR recommendations, under ordinary circumstances, VPN tunnels can only be negotiated with peers (SNS firewalls, third-party devices and VPN clients) that also comply with these recommendations.

The following SNS versions comply with these recommendations:

- SNS in 4.3.21 LTSB and later versions of 4.3 LTSB,
- SNS in 4.8 and later versions,
- SNS in 5.0 and later versions.

In SNS version 5, a configuration containing IPsec tunnels that are not compatible with DR mode can **progressively transition** to a configuration that is exclusively made up of DR-compliant tunnels.

Compatibility of DR modes across SNS versions

IPsec "mode"	Standard			DR			DR transition
SNS version	3.x	4.3.21 LTSB and higher	5.x	3.x	4.3.21 LTSB and higher	5.x	5.x
3.x	✓	✓	✓	✓	✗	✗	⚠
4.x	✓	✓	✓	✗	✓	✓	✓
5.x	✓	✓	✓	✗	✓	✓	✓

⚠ : Compatible only with IPsec tunnels in standard mode

NOTE
DR mode in SNS 3.x versions is not compatible with DR mode in SNS 4.x and 5.x versions. As such, a firewall in a 3.x version that needs to set up tunnels in DR mode with firewalls in 4.x or 5.x versions has to be updated to SNS version 4.3 LTSB or 4.8 in advance.

Update paths

To update a firewall to version 4.3, 4.8 or 5 from an older version, intermediate updates may be required depending on the original version:

From a 3.X version	Update to the latest 3.7.X LTSB or 3.11.X LTSB version available
From a 4.0.X version	Update to version 4.1.6

From a 4.1.6 version or higher	No intermediate updates required
From a V/VS-VU firewall	See Migrating a V/VS-VU model virtual firewall to an EVA model

Compatibility of IPsec VPN clients with DR mode

The following IPsec VPN clients can set up tunnels in DR mode with SNS firewalls:

- Stormshield Network VPN Client Exclusive 7.5.109 and later versions,
- TheGreenBow VPN Client Édition Enterprise 7.5.109 and later versions.

If you were previously using Stormshield Network VPN Client Standard clients, in order for DR mode to be enabled, these clients have to be uninstalled to make way for one of the compatible clients listed above.

If you were already using Stormshield Network VPN Client Exclusive, ensure that each client is in version 7.5.109 or higher, and verify that their configurations match the description in the section Creating a DR-compliant tunnel on a mobile client .

NOTE
Further on in this document, the mobile VPN client that is used will reference one of the compatible clients listed above, and will be given a generic name "DR-compliant VPN client".

Impact on the network

IPsec VPN tunnel negotiation packets and ESP packets are exchanged by default over UDP port 4500, in order to comply with ANSSI recommendations on DR mode.

If there are other security devices between the firewall to be configured in DR mode and its peers, UDP port 4500 must be allowed between the SNS firewall and its peers on these intermediate devices.

However, you can revert to the standard UDP port 500 by using the following CLI/Serverd command sequence.

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

More information about the command `CONFIG IPSEC PEER UPDATE`

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 and signature of key pairs:

- 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 by going up the chain from the peer certificate 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=Villeneuve d'Ascq,O=Stormshield,OU=Documentation,CN=DR-Compliant-Gateway-Peer.stormshield.eu*),
- *Subject Alternative Name* (SAN). This is one of the aliases that may be defined when the peer certificate is created (e.g., *DR-Compliant-Gateway-Peer.stormshield.eu*). When a peer's SAN has been entered in the **Peer ID** field, this SAN must also be entered in the **Local ID** field of the peer in question.

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.

To do so, the **CRL Required** field of a peer that is compatible with DR mode has to be set to **Auto** or **Mandatory**. Do note that by default (standard IPsec mode), the value of this field is **Auto**, and when DR mode is enabled, its value becomes **Mandatory**.

During the transition, it has to be set to **Mandatory**.

In addition to certificate revocation verification, the CRLs must be present and still valid so that negotiation can function.

Making the PKI compliant 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 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-compliant peers:

1. 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.

2. Generate the identities of all IPsec peers to be made DR compliant. Do note that SNS firewalls support the EST (enrollment over secure transport) protocol in a DR context.
3. Export these identities (certificate + private key).
4. 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 compliant.

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

1. Go to a CA in your PKI.
2. Create a sub-CA that complies with the criteria that were defined in the paragraph **Recap of IPsec DR recommendations for the PKI**.

From this sub-CA:

1. Generate the identities of all IPsec peers to be made DR compliant.
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 compliant.

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 or is created on the SNS firewall in version 5 or higher

If a CA (or sub-CA) that complies with IPsec DR recommendations already exists on the SNS firewall in version 5 or higher

On the version 5 SNS firewall in this example:

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 certificates of IPsec certificates that are 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 the version 5 SNS firewall in this example:

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** (*IPsec-DR-CA* 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 it on each of the CRL distribution points that were specified during the creation of the CA.

Creating the identity of the version 5 SNS firewall (if it does not exist) and of each peer

For gateway peers

On the version 5 SNS firewall in this example:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the CA that signs certificates for DR mode (*IPsec-DR-CA* in this example).
3. Click on **Add** and select **Server identity**.

4. Enter the fully qualified domain name of the peer (e.g., *DR-Compliant-Gateway-Peer.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 (*IPsec-DR-CA* 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. **Key size (bits)**: 256 must be selected.
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 the version 5 SNS firewall in this example:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the CA that signs certificates for DR mode (*IPsec-DR-CA* 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 (*IPsec-DR-CA* 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. **Key size (bits)**: 256 must be selected.
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 compliant

On the version 5 SNS firewall in this example:

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 compliant

On every gateway peer other than the version 5 SNS firewall:

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**.

For mobile peers, this operation is described in the section Creating a DR-compliant tunnel on a mobile client

Deleting the private keys of peer identities on the version 5 SNS firewall (recommended)

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

On the firewall that hosts the CA (the version 5 SNS firewall in this example):

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.

Verifying the DR mode compliance of an IPsec policy

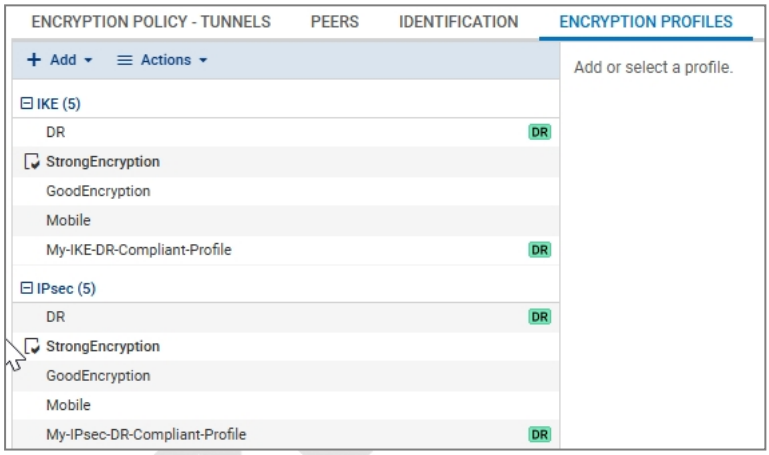
Once it has been installed, SNS in version 5 and higher easily identifies the elements in the IPsec policy that are DR mode compliant, and on the other hand, those that require changes to their configuration in order to make them compliant.

Go to **Configuration** > **VPN** > **IPsec VPN**.

Encryption profiles tab

Two preset profiles, named **DR,** are suggested by default. The associated icon DR indicates that these IKE and IPsec encryption profiles are DR mode compliant.

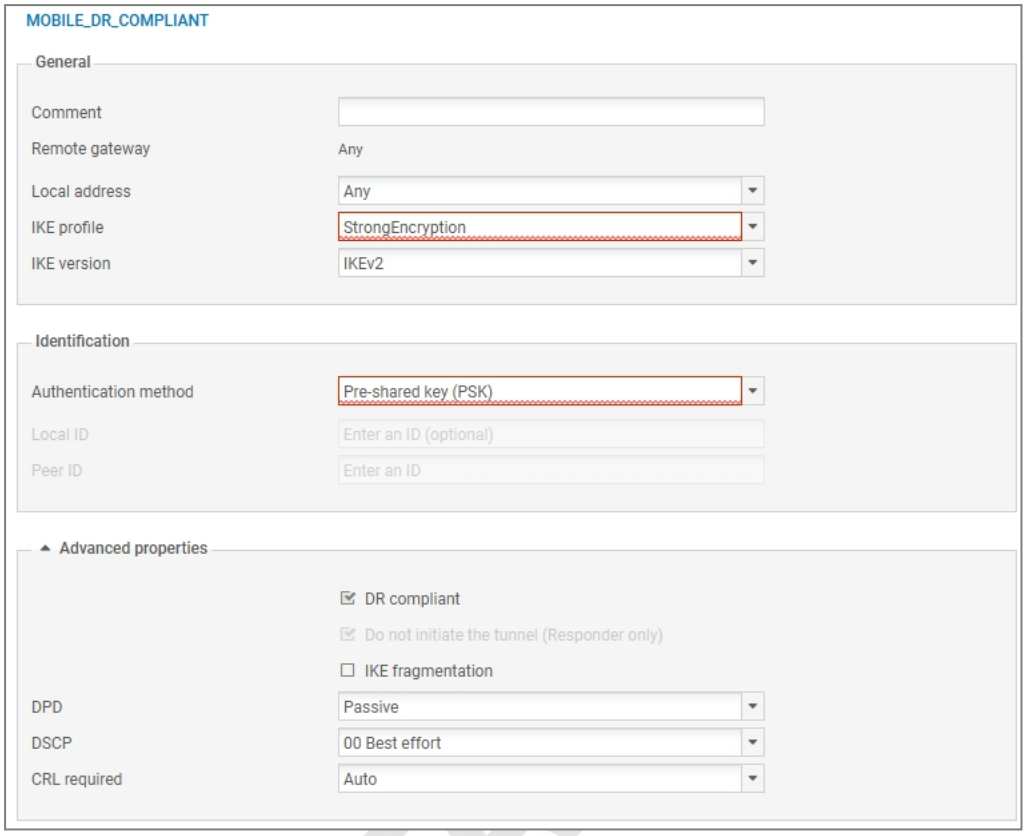
You can also add your own custom DR mode-compliant profiles, by cloning these preset **DR** profiles, for example. The icon DR will automatically appear next to these profiles.



Peers tab

1. Select a peer.
2. Under **Advanced properties**, select the **DR compliant** checkbox to highlight the peer settings that need to be modified in order to make the peer DR compliant.

Example 1: DR non-compliant peer.



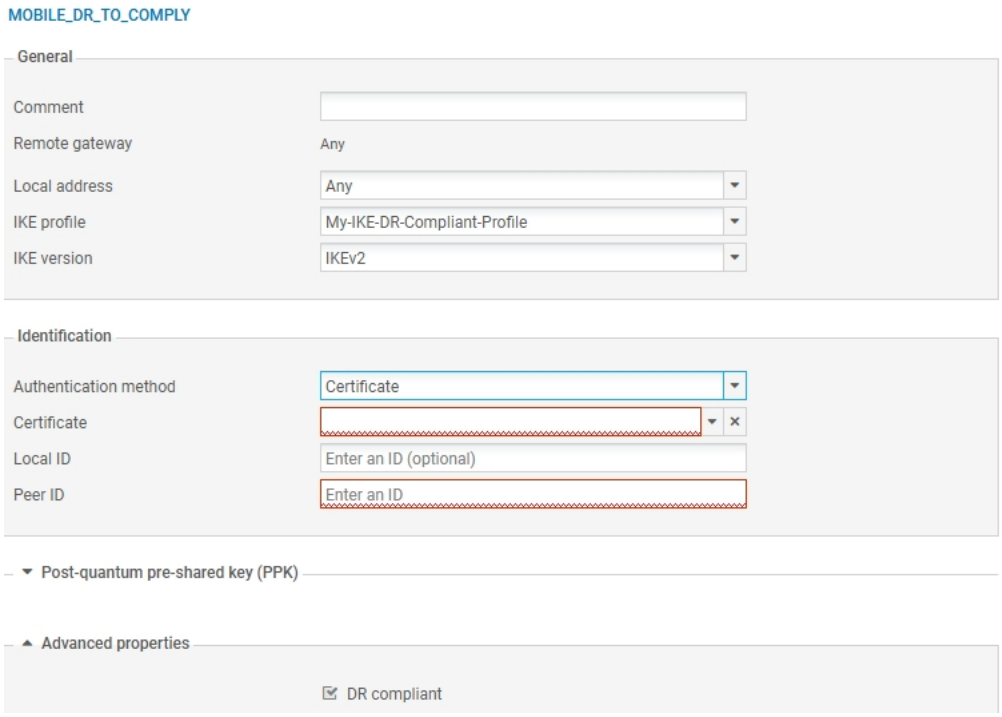
The settings that need to be changed are framed in red.

In this example, to make the peer DR compliant:

- Select an encryption profile that is DR compliant (preset **DR** profile or compliant custom profile),
- Change the authentication method to select certificate authentication.

Only DR-compliant choices are offered as alternative field values.

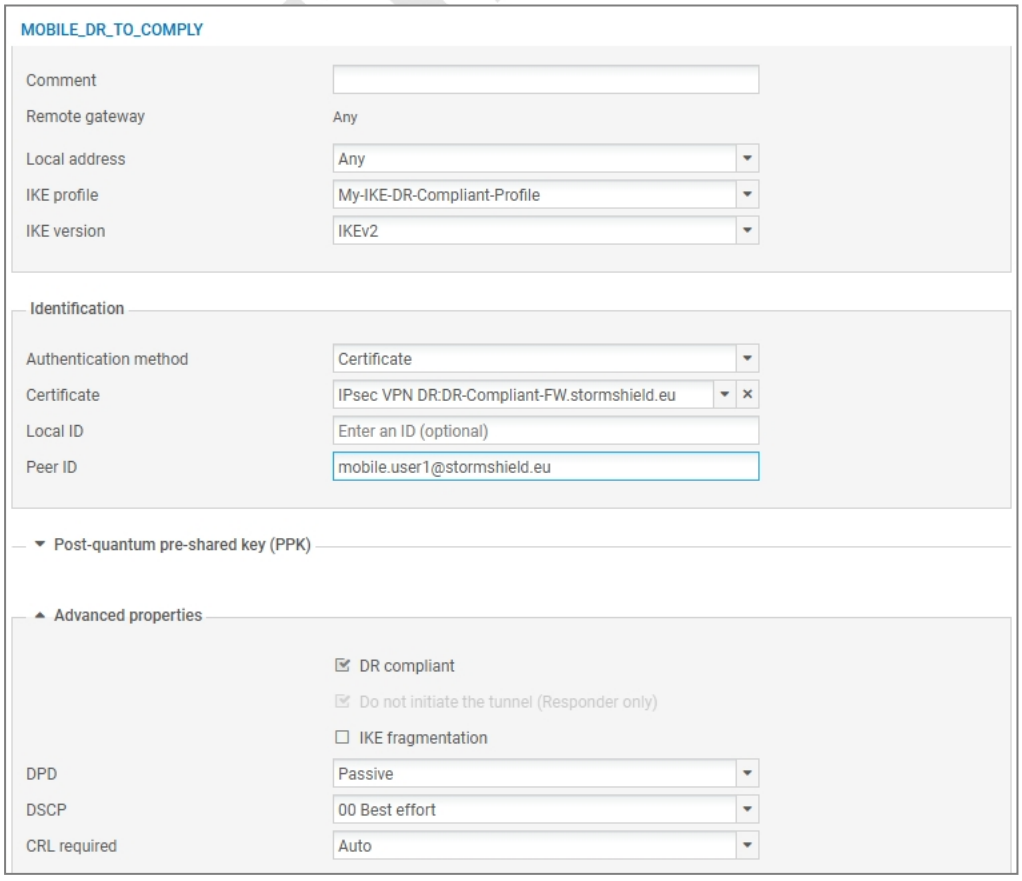
When a DR-compliant option is selected, other mandatory fields may be displayed as a result. For example, when the **Pre-shared key (PSK)** method is modified for the **Certificate** method, some of the mandatory fields associated with this authentication method are then highlighted:



In this case:

- Select the certificate presented by the local firewall,
- Specify a **Peer ID** reflecting the FQDN found in the peer certificate.

Example 2: DR-compliant peer.



For this peer, no settings need to be changed.

Encryption policy – Tunnels tab

When a peer is DR compliant (**DR compliant** checkbox selected, and all peer settings are compliant), the icon DR appears before the IPsec rule associated with this peer.

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

Making the IPsec policy compliant with DR mode

On the version 5 SNS firewall:

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Select the peer to be made compatible with DR mode (**Remote gateways** and **Mobile peers**).
3. In the **Advanced properties** section, select the **DR compliant** checkbox.

Peer settings that are not DR compliant are framed in red.

Follow the procedures below to change these settings if necessary.

Changing the IKE version used by the peer

1. Select **IKEv2** for the **IKE version** field.
2. This change must also be made on the peer in question. If it is a mobile tunnel, follow the compliance procedure described in the section Creating a DR-compliant tunnel on a mobile client.

Changing the authentication method used by the peer

1. In the **Identification** section, set the **Authentication method** field to **Certificate**.
2. Fill in the **Peer ID** field. 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=Villeneuve d'Ascq,O=Stormshield,OU=Documentation,CN=DR-Compliant-Gateway-Peer.stormshield.eu*),
   - *Subject Alternative Name* (SAN). This is one of the aliases that may be defined when the peer certificate is created (e.g., *DR-Compliant-Gateway-Peer.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 use the SAN that was set when the peer certificate was created.
3. This change must also be made on the peer in question. If it is a mobile tunnel, follow the compliance procedure described in the section Creating a DR-compliant tunnel on a mobile client.

Changing authentication and encryption algorithms

1. In the **General** section, ensure that the **IKE profile** field is set to a DR-compliant profile (**DR** profile provided by default or custom profile - *My DR Profile* in this example).
2. This change must also be made on the peer in question. If it is a mobile tunnel, follow the compliance procedure described in the section Creating a DR-compliant tunnel on a mobile client.

Adding the trust chain that was used to sign certificates in the list of Approved certification authorities

1. Go to **Configuration > VPN > IPsec VPN > Identification** tab.
2. In the **Approved certification authorities** grid, check whether the entire trust chain is there, meaning from the Root CA to the sub-CA that signed the certificates used for DR mode (*IPsec-DR-CA* in this example).
3. If this is not the case, click on **Add** and select the certification authority in question.
4. This change must also be made on the peer in question. If it is a mobile tunnel, follow the compliance procedure described in the section Creating a DR-compliant tunnel on a mobile client .

Optional - Setting DR encryption profiles (or compatible custom profiles) as default profiles

This procedure makes it possible to set **DR** profiles (or compatible custom profiles) as the profiles suggested by default for all future peers, and all IPsec rules that must be created on the firewall.

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 (or custom DR-compliant profile).
   Ensure that the profile has the following characteristics:
   - 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 changed.
3. Click on the **Actions** menu.
4. Select **Define the default profile**.
   This IKE profile is now used by default for new IPsec tunnels that are added to the firewall's configuration.
5. In the menu on the left, under the **IPsec** section, select the **DR** profile (or custom DR-compliant profile).
   Ensure that the profile has the following characteristics:
   - 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 changed.
6. Click on the **Actions** menu.
7. Select **Define the default profile**.
   This IPsec profile is now used by default for IPsec tunnels defined in the firewall's configuration.

Making the configuration of a mobile IPsec client compliant 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.

Compatible clients that can set up VPN tunnels in DR mode with a firewall in an SNS version that complies with the ANSSI's IPsec DR recommendations are listed in the section Compatibility of IPsec VPN clients with DR mode.

If you were previously using Stormshield Network VPN Client Standard, in order for DR mode to be enabled, the client has to be uninstalled to make way for one of the DR-compliant clients.

On the client workstation:

1. Download the DR-compliant client.
2. Uninstall SN VPN Client Standard if it had been installed on the workstation.
3. Install the DR-compliant client.

Creating a DR-compliant tunnel on a mobile client

For more information on Stormshield Network VPN Client Exclusive, refer to the Stormshield VPN Client Exclusive v7 administrator guide.

Running and enabling the DR-compliant VPN client

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

1. On the Windows desktop on the client workstation, run the DR-compliant VPN client.
2. The first time it is launched, enter the license number for the user in question.

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 of the DR-compliant VPN client:

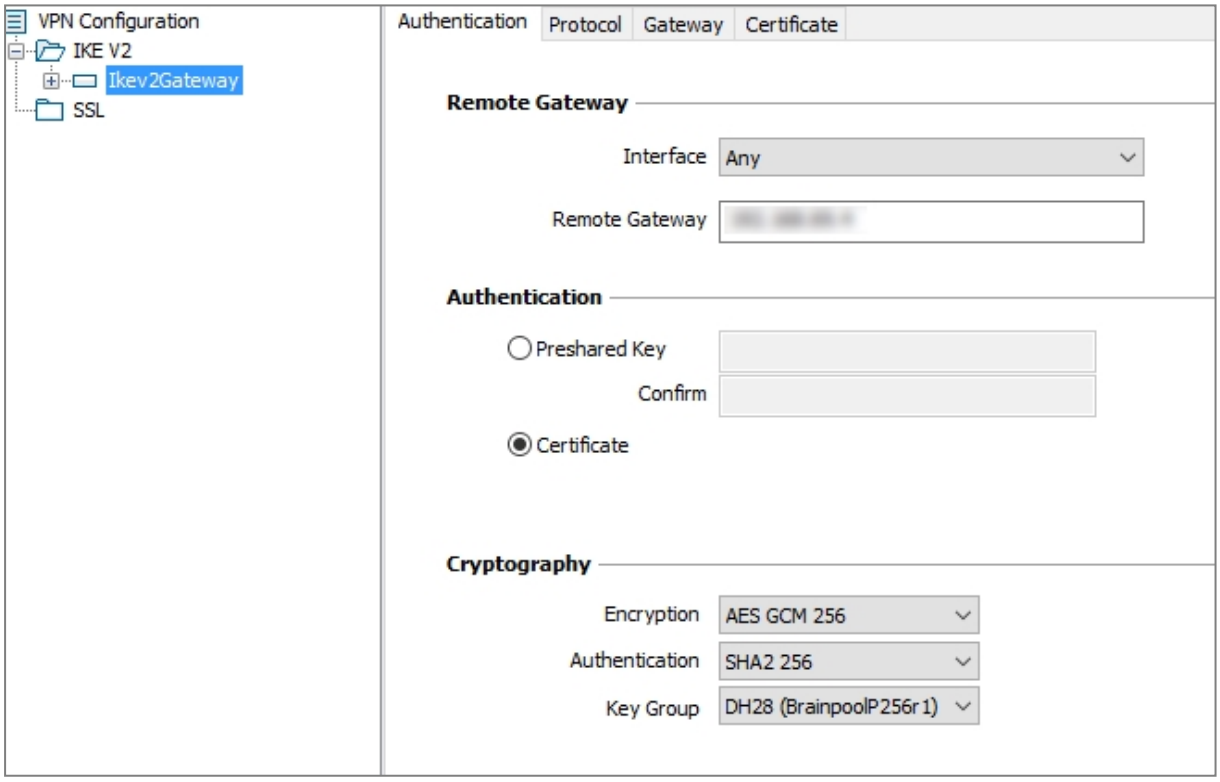
1. Right-click on IKEv2 and select **New IKE Auth**.
   A gateway, named *Ikev2Gateway* by default, is created.
2. It can be renamed by right-clicking on this gateway and selecting **Rename**.

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

Select the gateway created earlier.

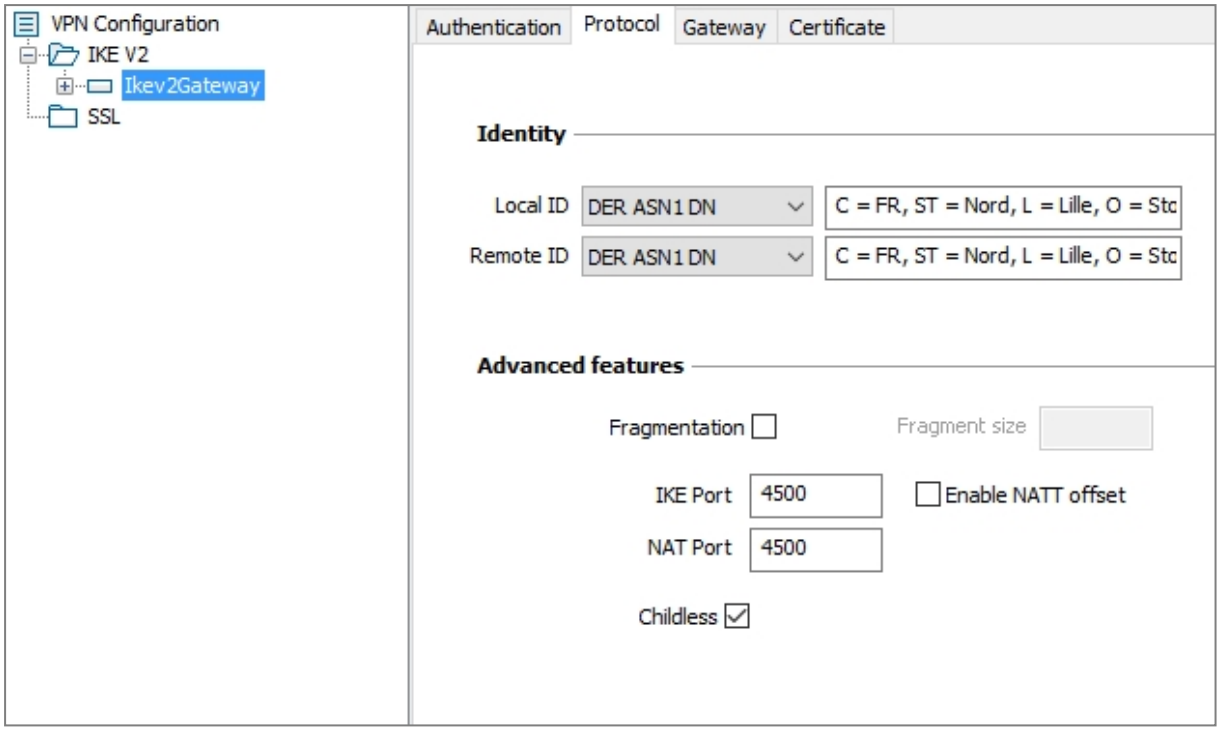
Authentication tab

1. In the **Remote Gateway** field, enter the IP address or FQDN of the firewall with which the DR-compliant tunnel will be set up.
2. In the **Integrity** 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 version 5 SNS firewall gateway certificate (*C=FR,ST=Nord,L=Villeneuve d'Ascq,O=Stormshield,OU=Documentation,CN=DR-Compliant-Gateway-Peer.stormshield.eu* in this example).
2. In the **Advanced properties** section:
   a. Set the **IKE Port** to 4500,
   b. Select the **Childless** checkbox.



Gateway tab

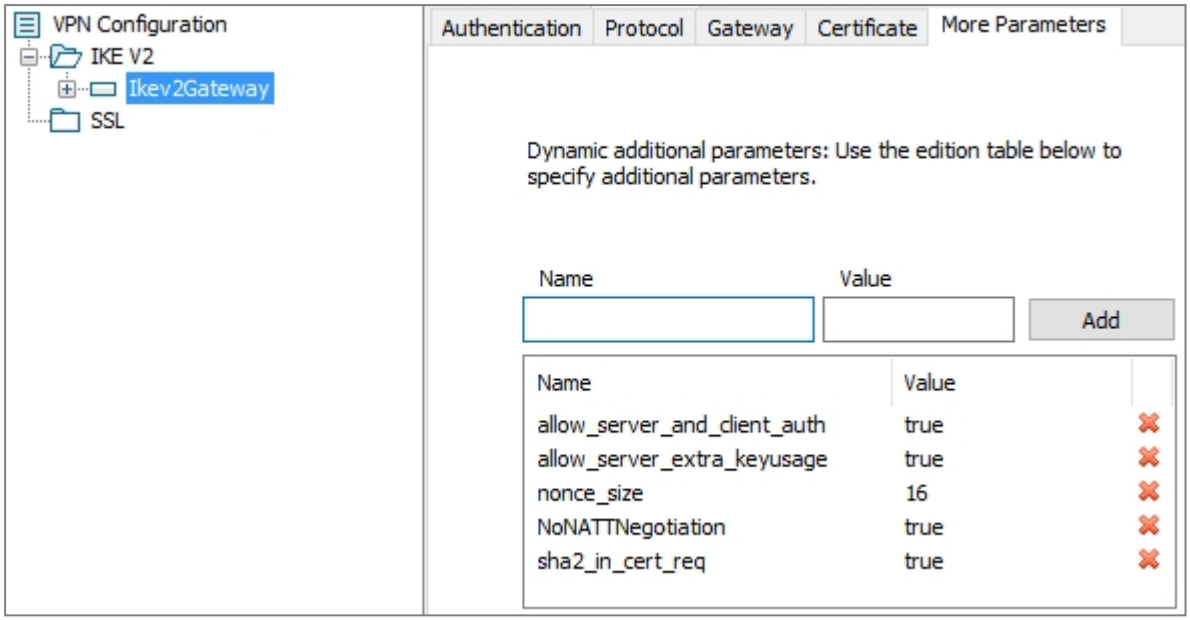
You can leave the default settings.

> **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 the DR-compliant VPN client initiates phase 2 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



Saving configurations

Click on **Configuration** > **Save** in the general menu of the DR-compliant VPN client to confirm and save the configuration.

Creating the tunnel to the DR-compliant gateway

1. Right-click on the gateway that was created earlier and select **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**.

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

Select the tunnel that was 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: 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: DH28 (BrainpoolP 256r1) or DH19 (ECP 256).
   - Select **Automatic** for the **Extended sequence number** field.
3. In the **Lifetime** section, select **1800** (seconds) for the **Child SA Lifetime** field.

Saving configurations

Click on **Configuration** > **Save** in the general menu of the VPN client to confirm and save this configuration.

Enabling DR mode on all peers

Verifying whether the entire configuration is DR compliant

To check whether the configuration is indeed fully compatible with DR mode, and to prevent the VPN policy from being disabled in the event of an anomaly, apply the following procedure to firewalls in SNS version 5.0 and higher:

1. Go to **System** > **Configuration** > **CLI console**.
2. Run `CONFIG IPSEC CHECK index=<policy_idx> DRcompliant=1` command where `<policy_idx>` is the IPsec policy number (example: index=1 when IPsec policy number is 01).
   Answer is `OK` when the configuration is compliant with DR mode.

Enabling DR mode

On the firewall in SNS version 5.0 or higher:

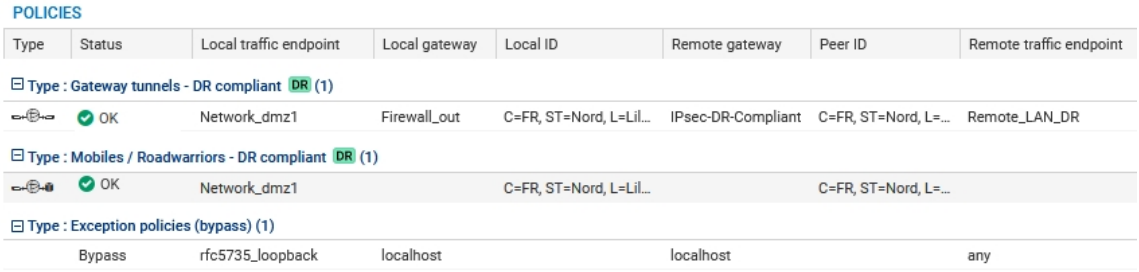
1. Go to **Configuration** > **System** > **Configuration** > **General configuration** tab.
2. In the **Cryptographic settings** section, select the **Enable "Diffusion Restreinte" (DR) mode version 2020** checkbox.
3. Restart the firewall to apply the activation of DR mode.
4. Activate DR mode on each gateway peer
5. After the firewall has restarted, check in the IPsec tunnel monitoring module whether all tunnels have been set up.

Verifying tunnel status

Go to the **Monitoring** tab in the web administration interface of the SNS version 5 firewall.

The **Monitoring > IPsec VPN tunnels** module allows you to view the status of tunnels in the active IPsec policy

The icon DR identifies tunnels that are fully compatible with DR mode:



When a tunnel is selected, the details of its IKE and IPsec security associations (SA) are shown.

Find out more on IPsec tunnel monitoring (SNS v4 user guide).

documentation@stormshield.eu