TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

IPSEC - DIFFUSION RESTREINTE MODE

Product concerned: SNS 4.2 and higher versions

Document last update: August 27, 2021

Reference: sns-en-diffusion_restreinte_ipsec_mode_technical_note

Table of contents

Getting started

The **Enable "ANSSI Diffusion Restreinte (DR)" mode** option 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. It is an imperative on networks that fall under the "Restricted" mention.
This mode relies in particular on the use of software versions for asymmetric and symmetric cryptographic algorithms and random key generation algorithms. As for symmetric encryption algorithms, "AES-NI" instructions available on certain products (SNi20, SNi40, SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100) are exempt as they are made up only of "simple acceleration instructions" of certain cryptographic operations.

IMPORTANT
The ANSSI Diffusion Restreinte (DR) mode in SNS 4.2 versions and higher is not compatible with DR mode in earlier SNS versions.
Likewise, a firewall in DR mode cannot set up IPSec VPN tunnels with an SNS firewall or third-party device in "standard" IPSec mode.

Assessing the impact of implementing DR mode (SNS v4.2 and higher)

When the "ANSSI Diffusion Restreinte (DR)" mode is enabled in version 4.2 and higher, the following requirements must be met.

Network impact

ESP packets must be encapsulated in UDP over port 4500 and *NAT Traversal* mechanisms must be implemented once negotiations start.

If the firewall to be set in DR mode is separated from the peer by other security devices, UDP port 4500 must then be allowed between the SNS firewall and its peer on such devices.

Interoperability with many systems

When DR mode is enabled on SNS 4.2 versions and higher:

- A firewall in DR mode in SNS version 4.2 (or higher) cannot set up IPSec tunnels with an SNS firewall in DR mode in version SNS 4.1 or lower,
- A firewall in DR mode in SNS version 4.2 (or higher) cannot set up IPSec tunnels with an SNS firewall or third-party device in "standard" IPSec mode.

Peer authentication

Peers are allowed to authenticate only with certificates, and certificates used (from the end user certificate to the shared trusted CA) must comply with the following specifications:

- ECDSA or ECSDSA signature on an ECP 256 or BP 256 curve,
- SHA256 hash algorithm.

The **Peer ID** field must also be entered.

Certificates

Verifications must be enabled to ensure that the certificates used by peers are revoked.

IKE protocol

Only version 2 of the IKE protocol is allowed.

IKE/IPSec encryption profiles

Encryption algorithms must belong to DH19 NIST Elliptic Curve Groups (256 bits) or DH28 Brainpool Elliptic Curve Groups (256 bits).

The IPSec encryption algorithm used must be:

- Either AES_GCM_16 (AEAD: Authenticated Encryption with Associated DATA. AES_GCM_16 is therefore not associated with any authentication algorithm),
- Or AES_CTR, which must be associated with SHA256.

ESNs are imposed for negotiations and to prevent replay when sending/receiving packets. The size of the anti-replay window cannot be zero.

The Pseudo-Random Function (PRF) algorithm must be SHA256.

IMPORTANT
If the newly configured IPSec policy on the firewall uses parameters that are incompatible with DR mode in SNS 4.2 (or higher), enabling DR mode will disable this IPSec policy and display the warning message:
“ANSSI Diffusion Restreinte mode disabled the non-compliant VPN configuration”.

Hardware

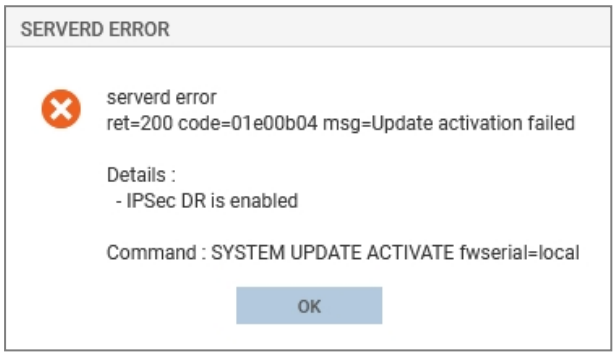
On firewalls equipped with Intel processors (SNi20, SNi40, SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100), the “ANSSI Diffusion Restreinte (DR)" mode allows the use of the coprocessor's cryptographic hardware instruction sets. On firewalls equipped with other types of processors (SN160, SN160W, SN210, SN210W et SN310), the “ANSSI Diffusion Restreinte (DR)" mode will force such instruction sets to be disabled, causing performance to slow down during encryption.

IMPORTANT
When “ANSSI Diffusion Restreinte (DR)” mode is enabled, the firewall must be restarted to apply the change.

Updating firewalls already configured in DR mode to version 4.2 (or higher)

DR mode implemented in SNS version 4.2 is significantly different from DR mode in earlier firmware versions.

As such, firewalls on which DR mode was already enabled cannot be updated directly to version 4.2. Any attempt to do so will result in a clear warning message:



To update firewalls configured with the DR mode of an earlier SNS version to version 4.2 (or higher):

1. Refer to the section Assessing the impact of implementing DR mode (SNS version 4.2 and higher)
2. In **Configuration** > **General configuration** tab > **Cryptographic settings**, unselect **Enable "ANSSI Diffusion Restreinte (DR)" mode** to disable DR mode.

> **IMPORTANT**
> When "ANSSI Diffusion Restreinte (DR)" mode is disabled, the firewall must be restarted to apply the change.

3. Update the firewall to version 4.2 or higher.
4. Ensure the compliance of the firewall's configuration with DR mode in SNS v4.2 (or higher).
5. Select **Enable "ANSSI Diffusion Restreinte (DR)" mode** to enable DR mode.

> **IMPORTANT**
> If the newly configured IPSec policy on the firewall uses parameters that are incompatible with DR mode in SNS 4.2 (or higher), enabling DR mode will disable this IPSec policy and display the warning message:
> "ANSSI Diffusion Restreinte mode disabled the non-compliant VPN configuration".

> **IMPORTANT**
> When "ANSSI Diffusion Restreinte (DR)" mode is enabled, the firewall must be restarted to apply the change.

Enabling DR mode on firewalls in SNS version 4.2 (or higher) without existing IPSec configurations

To enable DR mode on firewalls in SNS version 4.2 (or higher) and in factory configuration or without existing IPSec policies:

1. Refer to the section **Assessing the impact of implementing DR mode (SNS version 4.2 and higher)**,
2. **Ensure the compliance of the firewall's configuration with DR mode in SNS v4.2** (or higher),
3. In **Configuration > General configuration** tab > **Cryptographic settings**, select **Enable "ANSSI Diffusion Restreinte (DR)" mode** to enable DR mode.

IMPORTANT
If the newly configured IPSec policy on the firewall uses parameters that are incompatible with DR mode in SNS 4.2 (or higher), enabling DR mode will disable this IPSec policy and display the warning message:
"ANSSI Diffusion Restreinte mode disabled the non-compliant VPN configuration".

IMPORTANT
When "ANSSI Diffusion Restreinte (DR)" mode is enabled, the firewall must be restarted to apply the change.

Ensuring the compliance of the firewall's configuration with DR mode in SNS v4.2 (or higher)

This section explains the options to enable and the parameters to select to make the firewall's configuration compatible with DR mode in SNS 4.2 versions or higher.

Certificates and PKI

Certificates used to set up IPSec tunnels in DR mode (from the end user certificate to the trusted CA) must comply with the following specifications:

- ECDSA or ECSDSA signature on an SECP or Brainpool curve,
- SHA256 hash algorithm.

Verifying or selecting algorithms to sign local certificates

If the CA that will sign local IPSec certificates already exists on the firewall

In the menu **Configuration > Objects > Certificates and PKI**:

1. Select from the list of CAs and certificates the CA that will be used to sign local IPSec certificates.
   Details of the CA will appear on the right.
2. In the **Details** tab > under **Hash**, check whether the signature algorithm is ecdsa-with-SHA256. If it is not, create a CA with a **Key type** set to SECP or BRAINPOOL and a **Key size** of 256 bits.
3. In the **Certificate profiles** tab, check whether the CRL distribution points (URI) of the CA have been specified. Add CRLDPs if this is not the case.

   > **NOTE**
   > The certificates that were signed by this CA before the CRLDPs were added must be generated again to apply this change.

4. In the **Certificate profiles** tab, ensure in the **Certification authority**, **User certificates** and **Server certificates** boxes 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 these settings differs from the values imposed, change it to select the right value.
5. Click on **Apply** to apply any changes that you have made.

If you need to create a new CA to sign local IPSec certificates

Creating the CA

You can create a CA to sign local IPSec certificates by following the steps below.

In the menu **Configuration > Objects > Certificates and PKI**:

1. Click on **Add**
2. Select **Root authority**.
   A wizard will appear.

3. Enter a **Name**.
   The name of the CA will automatically be entered as the **ID**, but can be changed.
4. Enter the **Autority attributes**:
   - Organization (O),
   - Organizational Unit (OU),
   - City (L),
   - State (ST),
   - Country (C).

EXAMPLE
Organization (O): Stormshield
Organizational unit (OU): Documentation
City (L): Lille
State (ST): Nord
Country (C): France,

5. Click on **Next**.
6. Enter and confirm the **Password** that protects the CA.
7. You can enter a contact **E-mail** address for this CA.
8. The **Validity** period suggested by default for the CA is 3650 days (recommended), but can be changed.
9. **Key type**: select only SECP or BRAINPOOL.
10. **Key size (bits)**: select only 256.
11. Click on **Next**.
12. **CRL distribution points**: add the URIs of the CRL distribution points that the IPSec devices of your peers can contact to verify the validity of certificates issued by your CA.
13. Click on **Next**.
    A summary of the information about the CA will appear.
14. Confirm by clicking on **Finish**.

Uploading CRLs to 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 this link and uploading this CRL to each of the CRLDPs specified when the CA was created.

Exporting the certificate of the CA that signs local certificates

In the menu **Configuration > Objects > Certificates and PKI**:

1. Select the CA that signs local certificates.
2. Click on **Download** and select **Certificate**.
3. Select the export format (PEM or DER).

You can then provide your peers with this certificate so that they can import it into their devices.

Importing the certificate of the CA that signs peer certificates

In the menu **Configuration > Objects > Certificates and PKI**:

1. Click on **Add** and select **Import a file**.
2. Select the certificate of the remote CA in either DER or PEM.
3. Click on **Import**.
   The certificate of the peer's CA will now appear in the list of CAs and certificates.

Enabling verification of peer certificate revocation

The certification authority (CA) that issues the certificates used in the authentication of IPSec peers must implement a revocation mechanism (CRL and CRL distribution points or OCSP servers) and enable the verification of certificates issued from this CA.

In **Configuration** > **System** > **CLI console**:

1. 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 edit.
2. Click on **Launch**.

When the verification of peer certificate revocation is not enabled, the current IPSec policy will be disabled and the error message "CRL verification cannot be disabled in DR mode" appears in the **Checking the policy** field below the IPSec policy grid.

Enabling automatic CRL retrieval

In **Configuration** > **General configuration** tab: select **Enable regular retrieval of certificate revocation lists (CRL)**.

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

IPSec policy

Verifying the IKE version used by peers

In **Configuration** > **VPN** > **IPSec VPN** > **Peers** tab, for each peer listed on the left (**Remote gateways** and **Mobile peers**):

1. Select each peer used in the active IPSec policy.
2. In the **General** section, ensure that the **IKE version** field is set to **IKEv2**.
   If it is not, the peer's IPSec configuration must be changed by selecting **IKEv2** for this field.

Verifying the authentication method used by peers

In **Configuration** > **VPN** > **IPSec VPN** > **Peers** tab, for each peer listed on the left (**Remote gateways** and **Mobile peers**):

1. Select each peer used in the active IPSec policy.
2. In the **identification** section, ensure that the **Authentication method** field is set to **Certificate**. If it is not, the peer's IPSec configuration must be changed by selecting **Certificate** for this field.
3. In the **Identification** section, ensure that the **Peer ID** is entered.
   This field represents your peer: the ID entered must be in the form of an IP address, a domain name (FQDN or *Fully Qualified Domain Name*), an e-mail address (user@fqdn) or the subject of the peer's certificate, if it is known (C=*country*, ST=*state*, O=*organization*, OU=*organizational unit*, Cn=*common name* [the CN can be an e-mail address]).

Selecting authentication and encryption algorithms

DR mode requires the use of encryption algorithms that belong to Diffie-Hellman groups 19 and 28. Two preconfigured encryption profiles can be selected for easier configuration.

In **Configuration** > **VPN** > **IPSec VPN** > **Encryption profiles** tab:

1. In the menu on the left, under **IKE**, select the **DR** profile.
   The properties of the profile appear.
   Two Diffie-Hellman profiles are offered: DH19 NIST Elliptic Curve Group (256 bits), selected by default, and DH28 Brainpool Elliptic Curve Group (256 bits).
   AES_GCM_16 is selected as the default proposal, and AES_CTR is the second. The **Encryption strength** of each algorithm can be increased.
2. Click on the **Actions** menu.
3. Select **Define the default profile**.
   The IKE DR profile is now used by default for all new IPSec tunnels added in the firewall's configuration.
4. In the menu on the left, under **IPSec**, select the **DR** profile.
   The properties of the profile appear.
   HMAC_SHA256 is selected as the authentication proposal.
   AES_GCM_16 is selected as the default encryption proposal, and AES_CTR is the second. The **Encryption strength** of each algorithm can be increased.
5. Click on the **Actions** menu.
6. Select **Define the default profile**.
   The IPSec DR profile is now used by default for all IPSec tunnels created in the firewall's configuration.

documentation@stormshield.eu