STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

IKEV2 MOBILE IPSEC VPN - EAP WITH CERTIFICATE AUTHENTICATION

Product concerned: SNS 4.8 and higher, SN VPN Client Exclusive 7.4 and higher

Document last updated: July 9, 2024

Reference: sns-en-IKEv2_Mobile_IPSec_VPN_EAP_With_Certificate_Authentication_Technical_Note

Table of contents

Change log ... 3

Getting started ... 4
- Requirements ... 4
- Limitations ... 4

Generating mobile peer identities ... 5
- External PKIs ... 5
- Internal PKIs (PKIs on an SNS firewall) ... 5
  - If the CA that manages the identities of mobile peers must be created ... 5
  - Creating the identity of the firewall for the IPsec VPN ... 6
  - Creating the identity of each peer ... 6
  - Exporting the identity of each peer ... 7
  - Deleting the private keys of peer identities on the firewall (recommended) ... 7

Allowing mobile users to set up IPsec VPN tunnels ... 8
- Creating a group that contains all the users allowed to set up IPsec VPN tunnels ... 8
- Setting LDAP as the authentication method for mobile users ... 8
  - If no rules are found in the authentication policy ... 8
  - If the authentication policy contains rules other than the one required for IPsec VPN users ... 9
- Allowing mobile users to set up IPsec VPN tunnels ... 10

Implementing a mobile IPsec configuration ... 11
- Defining a network object that contains IP addresses assigned to mobile peers ... 11
- Creating objects for network resources that are accessible to mobile peers ... 11
- Creating IPsec VPN peer profiles ... 12
  - Adding the CA that signed the firewall's certificate in trusted authorities ... 12
- Creating the IPsec policy ... 13
  - Config mode mobile policy ... 13
- Allowing IPsec VPN access in filter policies ... 13
- Optimizing ISAKMP traffic during the negotiation of IPsec tunnels and securing authentication ... 14
  - Requirements ... 14
  - Optimizing tunnel traffic by restricting IP datagrams ... 14
  - Reloading the IPsec policy to apply changes made earlier ... 15
  - Optimizing tunnel traffic: restricting MSS ... 15
- Configuring the VPN client ... 15
  - Configuring Phase 1 ... 16
  - Configuring Phase 2 ... 17

Setting up the IPsec VPN tunnel from the client workstation ... 18

Showing details of tunnels on the firewall ... 20

Glossary ... 22

Change log

Date	Description
July 9, 2021	New document

Getting started

In versions prior to SNS 4.8, only IKEv1-based mobile tunnels allowed multifactor authentication (MFA) for mobile users via Xauth. IKEv2 does not support Xauth.

As IKEv1 is an old protocol, and the ANSSI recommends IKEv2-based solutions for higher security, SNS version 4.8 introduces multifactor authentication (MFA) support for IKEv2-based mobile tunnels set up via EAP (Extensible Authentication Protocol).

There are two ways to proceed with this multifactor authentication:

- EAP-Generic Token Card: the mobile peer must present a login/password pair,
- Certificate and EAP-Generic Token Card: the mobile peer must present a certificate and login/password pair.

> **NOTE**
> SN IPsec VPN Client Exclusive v7.4 or a higher version has to be installed on the client workstation in order to be compatible with EAP.

This document describes the required VPN configuration that will allow mobile users to access their company's internal network through a mobile IKEv2-based IPsec tunnel in config mode, and which uses the Certificate and EAP-Generic Token Card method. The login/password pair is generated by the firewall's internal LDAP directory.

Do note that the EAP-Generic Token Card method, and Certificate and EAP-Generic Token Card method, use a login/password pair that can be referenced in an internal LDAP directory, external LDAP directory or on a Radius server, for example.

Requirements

- The user accounts to be used for the IPsec VPN have already been created in an LDAP directory that has been configured as the default directory on the firewall (internal directory in this document).
  The process of creating an LDAP directory (internal or external) is described in the Directory configuration section in the **SNS User Guide**.
- Every user configured in the directory must have an individual e-mail address.
- **SN VPN Client Exclusive** must be installed on Microsoft client workstations. It can be downloaded from **Downloads** > **Stormshield Network Security** > **VPN Client** in your Mystormshield area (a software license is required after a 30-day trial period) or from the TheGreenBow IPsec VPN Enterprise client.

Limitations

The Certificate and EAP-Generic Token Card method and EAP-Generic Token Card method are not compatible with:

- IKEv1-based tunnels, which must use Xauth for multifactor authentication.
- ANSSI *Diffusion Restreinte* (DR) mode.

Generating mobile peer identities

This section explains how to create mobile user identities

with mobile user accounts that have already been configured in the IPsec VPN reference directory (the firewall's internal LDAP directory in this example).

External PKIs

In the certification authority (CA) that manages the identities of IPsec mobile peers:

1. Generate the identities of all IPsec mobile peers.
2. Export these identities (certificate + private key).
3. Download the identities of individual mobile peers on their workstations.

Internal PKIs (PKIs on an SNS firewall)

If the CA that manages the identities of mobile peers must be created

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Click on **Add.**
3. Select **Root authority or Sub-authority** if this CA is under a root CA in your PKI.
   A wizard will automatically appear.
4. Enter a **Name** (*EAP- IKEv2* 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 a contact **E-mail address** for this CA.
9. The default **Validity** suggested is 3650 days (recommended value).
   This value can be changed.
10. **Key type**: *SECP* or *BRAINPOOL* key types are recommended.
11. Select the **Key size (bits)**.

12. Click twice on **Next**.
    A summary of the information on the CA will be shown.
13. Confirm by clicking on **Finish**.

If you wish to set this CA as the firewall's default CA:

1. Select this CA,
2. Click on **Actions** and select **Set as default**.

Creating the identity of the firewall for the IPsec VPN

If the identity of the firewall used for the IPsec VPN does not yet exist:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the CA used for the IPsec VPN.
3. Click on **Add** and select **Server identity**.
4. In the **Fully Qualified Domain Name (FQDN)** field, enter the name of the peer (e.g., *FW-EAP-IKEv2.stormshield.eu*).
   The **ID** will automatically be filled in with the name of the peer. This name can be changed.
5. Click on **Next**.
6. Enter the password of the CA that signs this identity.
7. Click on **Next**.
8. Select a **Validity** duration in days (365 days suggested by default).
9. Select the **Key type**: *BRAINPOOL* or *SECP* key types are recommended.
10. Select a **Key size**.
11. Click twice on **Next**.
    A summary of the identity will appear.
12. Click on **Finish** to confirm the creation of the user identity.

Creating the identity of each peer

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the CA used for the IPsec VPN.
3. Click on **Add** and select **User identity**.
4. In the **Common name (CN)** field, enter the name of the peer (e.g., *User1 EAP*).
   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 (*user1@stormshield.eu* in this example).

   > **NOTE**
   > This e-mail address must be the same as the one configured for the user account that is used for the EAP method (internal directory in this example).

6. Click on **Next**.
7. Enter the password of the CA that signs this identity.
8. Click on **Next**.
9. Select a **validity** duration in days (365 days suggested by default).
10. Select the **Key type**: *BRAINPOOL* or *SECP* key types are recommended.
11. Select a **Key size**.

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

Repeat this process for each mobile peer.

Exporting the identity of each peer

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the user 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.
   This file will need to be imported on the user's workstation when the user's tunnel is being configured in SN VPN Client Exclusive.

Repeat this process to export the identity of each mobile peer.

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

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

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Select the 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 process for each affected peer.

Allowing mobile users to set up IPsec VPN tunnels

The suggested method consists of creating a group that contains all the mobile users allowed to set up IPsec VPN tunnels, then assigning the appropriate privilege to this group. This group will also be used in the configuration of the mobile peer's profile.

Creating a group that contains all the users allowed to set up IPsec VPN tunnels

> **NOTE**
> For an external directory, such groups must be created directly on one of the workstations that hosts the directory.

1. Go to to **Configuration** > **Users** > **Users**:
2. Click on **Add group**.
3. In the **Group name** field, enter a representative name (e.g.: *EAP-GTC-CERT Users*).
   You can add a **Description**.
4. Click on **Add**.
   A row will be added to the grid of group members.
5. Type the first few letters of the name of the user to be added to the group and select the desired user from the list that the firewall suggests.
6. Repeat steps 3 and 4 to add all the users to include in this group.
7. When all members have been added, click on **Apply**.
8. Confirm by clicking on **Save**.

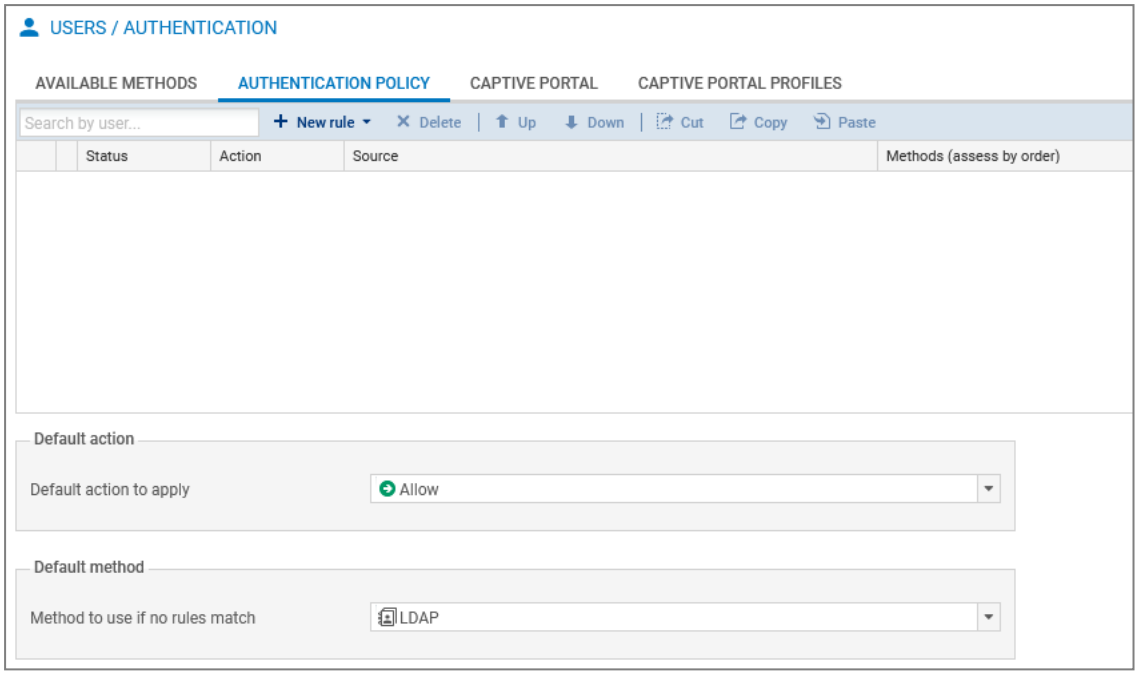
Setting LDAP as the authentication method for mobile users

Go to the **Configuration** > **Users** > **Authentication** > **Authentication policy** tab.

If no rules are found in the authentication policy

Ensure that:

- The **Default action to apply** field is set to **Allow**.
- The **Method to use if no rules match** field is set to **LDAP**.

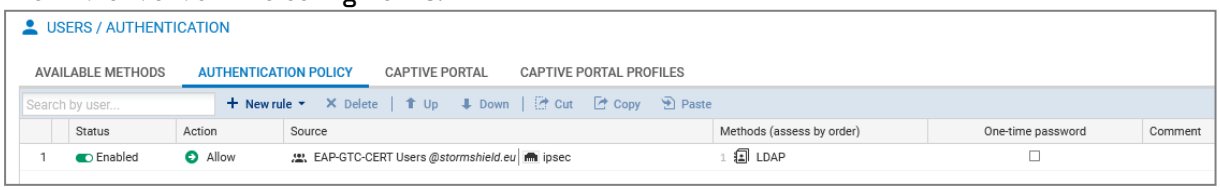


If the authentication policy contains rules other than the one required for IPsec VPN users

Add an authentication rule:

1. Click on **New rule** and select **Standard rule**.
   A rule configuration window opens.
2. In the menu on the left side of this window, click on **Action**.
3. In the **Action to apply for this rule** field, select **allow**.
4. In the menu on the left, click on **User**.
5. In the **User or group** field, select the group created earlier (*EAP-GTC-CERT Users* in the example).
6. In the menu on the left, click on **Source**.
7. Click on **Add an interface** and select **IPsec**.
8. In the menu on the left, select **Authentication methods**.
9. Select the row in the grid that contains the **Default method** and click on **Delete**.
10. Click on **Enable a method** and select **LDAP**.
11. Click on **OK**.
12. Double-click on the cell corresponding to the **Status** column to enable this rule.
    Its status will switch to **ON**.
13. Click on **Apply** then on **Save**.

The authentication rule configured is:

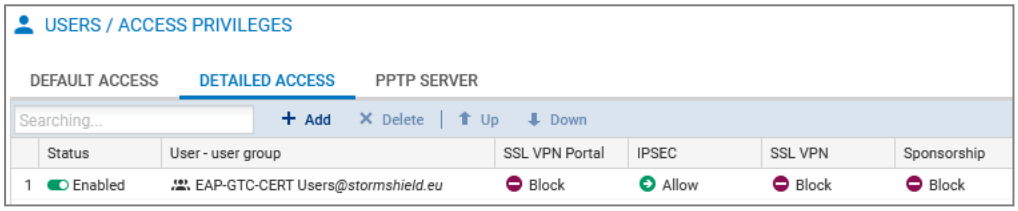


Allowing mobile users to set up IPsec VPN tunnels

In **Configuration** > **Users** > **Access privileges** > **Detailed access** tab:

1. Click on **Add**.
2. In the **User - Group** field: select the user group from the list suggested by the firewall (*EAP-GTC-CERT Users* in this example).
3. Click on **OK**.
   A row will be added to the grid.
4. Click on the cell in this row in the **IPsec** column and select **Allow**.
5. Double-click on the cell in this row in the **Status** column to show the status **Enabled**.
6. Click on **Apply** then on **Save**.

The users in this group are now allowed to set up IPsec tunnels:



Implementing a mobile IPsec configuration

In this document, mobile users set up tunnels with an IP address that was obtained automatically by their VPN client from the firewall (config mode).

Defining a network object that contains IP addresses assigned to mobile peers

The network assigned to clients must not already be known to the firewall. It must not be:

- A directly connected network,
- A network known through routing,
- A network involved in the configuration of another IPsec tunnel.

In **Configuration** > **Objects** > **Network**:

1. Click on **Add**.
2. Select **Network**.
3. Assign a **Name** to this object (*IKEv2_EAP_CERT_Clients_Network* in the example).
4. Enter the **Network IP address** field in the form of a network/mask.
   This network must contain at least as many IP addresses as the number of users likely to connect simultaneously via an IPsec VPN tunnel.
   Examples:
   192.168.9.0/24 or 192.168.9.0/255.255.255.0 : 254 addresses, so 254 simultaneously in Phase 2.
   192.168.9.0/23 or 192.168.9.0/255.255.254.0 : 510 addresses, so 510 simultaneously in Phase 2.
5. Click on **Create**.

Creating objects for network resources that are accessible to mobile peers

The object representing resources that can be accessed through the IPsec tunnel may be:

- A host: to allow access to a single host through the IPsec tunnel,
- A network: to allow access to a single protected network on the firewall through the IPsec tunnel,
- A host/network group: to allow access to a group of hosts and/or protected networks through the IPsec tunnel.

In **Configuration** > **Objects** > **Network**:

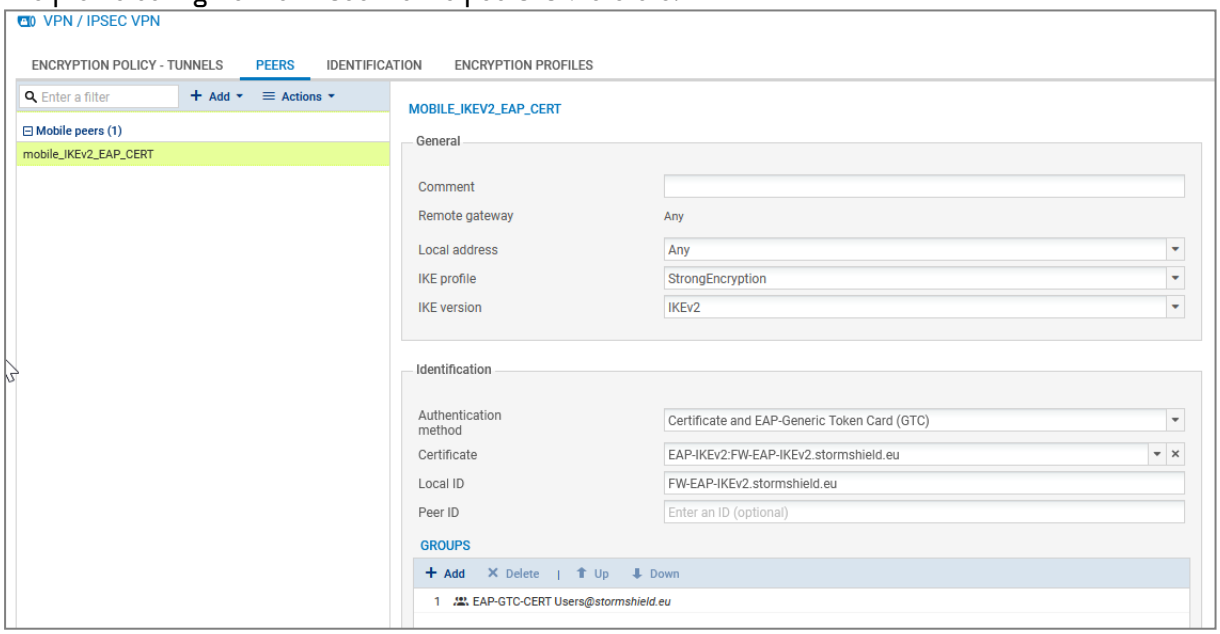
1. Click on **Add**.
2. Select the object type (**Host, Network** or **Group**).
3. Give this object a **Name** (*IKEv2-EAP-CERT-NET-GRP-DST* group in this example).
4. Depending on the object type:
   - Host: fill in the **IPv4 address** field,
   - Network: fill in the **Network IP address** field as a network/mask (**E.g.,** 192.168.1.0/24 or 192.168.1.0/255.255.255.0),
   - Group: select the objects (hosts and/or networks) to include in the group.
5. Click on **Create**.

Creating IPsec VPN peer profiles

In the module **Configuration** > **VPN** > **IPsec VPN**, **Peers** tab.

1. Click on **Add**.
2. Select **New mobile peer**.
3. Name the mobile configuration (*mobile_IKEv2_EAP_CERT* in the example), select **IKEv2** in the **IKE version** field, then click on **Next**.
4. Select **EAP-Generic Token Card (GTC)** as the **Authentication type**, then click on **Next**.
5. In the **Certificate** field, select the certificate that the firewall has to present to set up tunnels with these mobile peers (*FW-EAP-IKEv2.stormshield.eu* in this example).
6. In the **Groups** table, click on **Add** and select the mobile user group(s) that use(s) this peer profile (*EAP-GTC-CERT Users* group in the example).
7. Click on **Next**.
8. Confirm by clicking on **Finish**.
9. Select the peer created earlier and fill in the **Local ID** field.
   In general, the DNS name (FQDN) of the firewall is used in the peer's certificate. In this example: *FW-EAP-IKEv2.stormshield.eu*.
10. Click on **Apply** then on **Save**.
11. Click on **Yes, activate the policy.**

The profile configured for IPsec mobile peers is therefore:



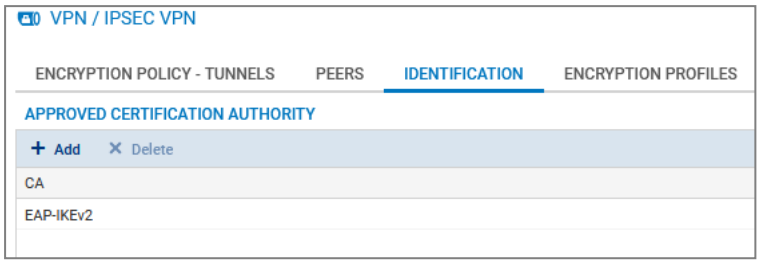
Adding the CA that signed the firewall's certificate in trusted authorities

> **NOTE**
> If the CA was issued from an external PKI, its certificate will need to be imported in advance in the firewall's **Certificates and PKIs** module.

In **Configuration** > **VPN** > **IPsec VPN**, **Identification** tab:

1. In the **Accepted certification authorities** table, click on **Add**.
2. Select the CA that signed the firewall's certificate (*EAP-IKEv2* in this example).

3. Click on **Apply**, then on **Save** to save the changes.



Creating the IPsec policy

1. Go to **Configuration** > **VPN** > **IPsec VPN** > **Encryption Policy - Tunnels** tab.
2. Select the IPsec policy that you wish to edit (*IPsec 01* in the example).
3. Click on the **Mobile - Mobile users** tab.

Config mode mobile policy

1. Click on **Add** and select **New config mode mobile policy**.
   A configuration wizard will start.
2. In the **Local resources** field, select the object representing the resources (host, network, or host/network group) that mobile users can access through the IPsec VPN tunnel. In the example, this object is the network group named *IKEv2_EAP_LOCAL_NET_GRP*.
3. In the **Peer selection** field, select the mobile profile created earlier (*mobile_IKEv2_EAP_CERT* in this example).
4. In the **Remote networks** field, select the network object created in the step **Defining a network object that contains IP addresses assigned to mobile peers** (*IKEv2_EAP_CERT_Clients_Network* in this example).
5. Click on **Finish**.
6. Double-click on the **Status** column to enable the rule.
7. Click on **Apply**, then on **Save** to confirm and enable this configuration.
8. Click on **Yes, activate the policy.**

The IPsec policy configured in *Config* mode is therefore:

Allowing IPsec VPN access in filter policies

The traffic that is required in order to set up the IPsec VPN is managed by an implicit filter rule. The filter policy will therefore manage how mobile users who were authenticated via the VPN access internal resources.

In the module **Configuration** > **Security policy** > **Filter - NAT** > **Filtering** tab:

1. In the filter policy, select the row below the one in which you wish to add the rule allowing mobile users to use the IPsec VPN.
2. Click on **New rule**.

3. Select **Single rule**.
   A new row appears.
4. In the newly added row, double-click on the cell in the **Action** column.
   The configuration window of the rule opens.
5. In the **Action** field, select **pass**.
6. In the menu on the left side of this window, select **Source**.
7. In the **User** field, select the group of users allowed to set up IPsec VPN tunnels (*EAP-GTC-CERT Users@stormshield.eu* in this example).
8. Click on the **Advanced properties** tab in the **Source** section.
9. For the **Via** field, select **IPsec VPN tunnel**.
10. For the **Authentication method** field, select **IPsec VPN**.
11. In the menu on the left side of this window, select **Destination**.
12. Click on **Add** in the **Destination hosts** grid.
13. Select the network that mobile users can access through the IPsec VPN tunnel (group *IKEv2_EAP_LOCAL_NET_GRP* in the example).
14. In the menu on the left side of this window, select **Inspection**.
15. In the **Inspection profile** field, select the IPS profile that contains the TCP-UDP profile with the MSS option (*IPS_03* in the example).
16. Click on **OK**.
17. Double-click on the cell corresponding to the **Status** column to enable this rule.
    Its status will switch to **ON**.
18. Click on **Apply**, then on **Yes, activate the policy**.

The filter rule configured is therefore:

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass	EAP-GTC-CERT Users Auth. by:IPsec VPN via IPsec VPN tunnel	IKEv2_EAP_LOCAL_NET_GRP	Any		IPS (IPS_03)

Optimizing ISAKMP traffic during the negotiation of IPsec tunnels and securing authentication

You are advised to modify several parameters on the firewall in order to optimize ISAKMP traffic during the negotiation of IPsec tunnels, and to secure the authentication process.

Requirements

For the purposes of illustration, the recommended optimizations and security measures assume that the IPsec policy used on the firewall for mobile users is *IPsec_01* (**Configuration** > **VPN** > **IPsec VPN**):

Optimizing tunnel traffic by restricting IP datagrams

The maximum packet size allowed may vary widely depending on your ISP.

Stormshield recommends that you restrict IP datagrams in ISAKMP negotiations to 1280 bytes:

1. Log in to the web administration interface of the firewall.
2. Go to **Configuration** > **System** > **CLI console**.

3. Enable IKE fragmentation by typing:
   `CONFIG IPSEC PEER UPDATE name=IPsec_Mobile_Profile_Name ike_frag=1`
   where *IPsec_Mobile_Profile_Name* represents the name given to the IPsec peer profile (*mobile_IKEv2_EAP_CERT* in the example).
4. Set the maximum size of ISAKMP datagrams to 1280 bytes using the command:
   `CONFIG IPSEC UPDATE slot=xy FragmentSize=1280`
   where *xy* represents the number of the mobile IPsec policy.
   In the example, this would be *IPsec 01*: the value of *xy* is therefore *01*.
5. Apply these changes by typing:
   `CONFIG IPSEC ACTIVATE`

Reloading the IPsec policy to apply changes made earlier

1. Go to **Configuration** > **System** > **CLI console**.
2. Reload the IPsec policy by typing:
   `CONFIG IPSEC RELOAD`
   Warning: this command will reset tunnels that have already been set up.

Optimizing tunnel traffic: restricting MSS

Since packets are encapsulated in the tunnel, ESP headers add several dozen bytes of data to the full size of each packet.

The size of segments (MSS: Maximum Segment Size) exchanged between the client and the firewall must therefore be automatically restricted.

With this option, packet fragmentation can be avoided or kept to a minimum. For packets exchanged between the client and the firewall, MSS imposes a packet size below the MTU (Maximum Transmission Unit) on the various network devices that intercept these packets.

Modifying a TCP-UDP inspection profile

In the **Application protection** > **Protocols** > **IP protocols > TCP-UDP** module:

1. Select the TCP-UDP inspection profile in which you wish to apply this change (*tcpudp_03* in the example). This inspection profile is automatically selected in the global profile that has the same index (03 in the example), and which is applied in the rule **Allowing IPsec VPN access in filter policies**.
2. Select the **Impose MSS limit** checkbox.
   Enter the value **1300** (bytes) (recommended by Stormshield).
3. Confirm the change by clicking on **Apply**.
4. Confirm by clicking on **Save**.

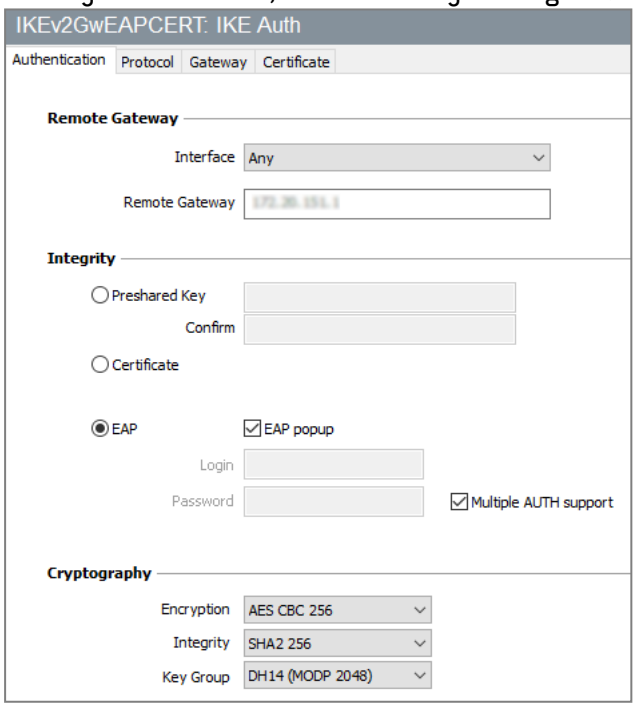
Configuring the VPN client

On the user's Microsoft Windows workstation, open the connection window of VPN Exclusive client by using administrator privileges:

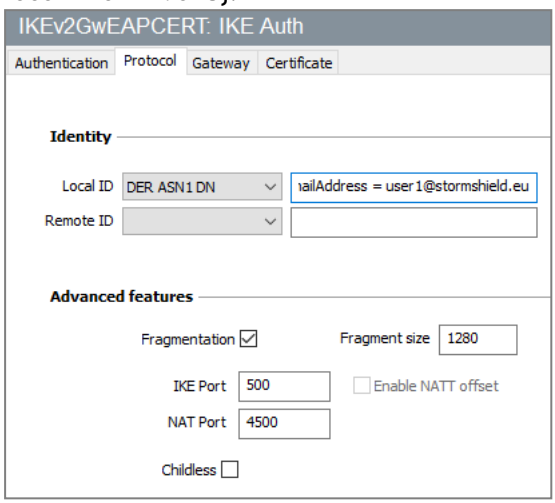
1. Right-click on the icon found in the Windows system tray (hidden icons): 
2. Select the **Configuration panel** menu.

Configuring Phase 1

1. In the **VPN configuration** tree, right-click on **IKEv2.**
2. Select **New IKE auth**.
   An entry named *Ikev2Gateway* by default is added to the **IKEv2** tree.
3. Right-click on *Ikev2Gateway* and select **Rename** to give this entry the name of your choice (*IKEv2GwEAPCERT* in this example).
4. Click on this entry.
5. In the **Authentication** > **Remote router address** tab > **Remote router address** field, enter the public IP address or FQDN of the firewall with which the VPN client must set up a tunnel.
   If you choose to use an FQDN, ensure that the DNS servers on the workstation have resolved it before you set up the tunnel.
6. In the **Authentication** > **Integrity** tab**,** select the checkboxes:
   - **EAP**,
   - **EAP popup**,
   - **Multiple AUTH support**.
7. Click on **Import certificate** and select **P12 format**.
8. Select the user's **P12 certificate**, which must have been installed in advance on the user's workstation.
9. Enter the password to protect the certificate, which was set when exporting the user's identity on the firewall, and confirm by clicking on **OK**.



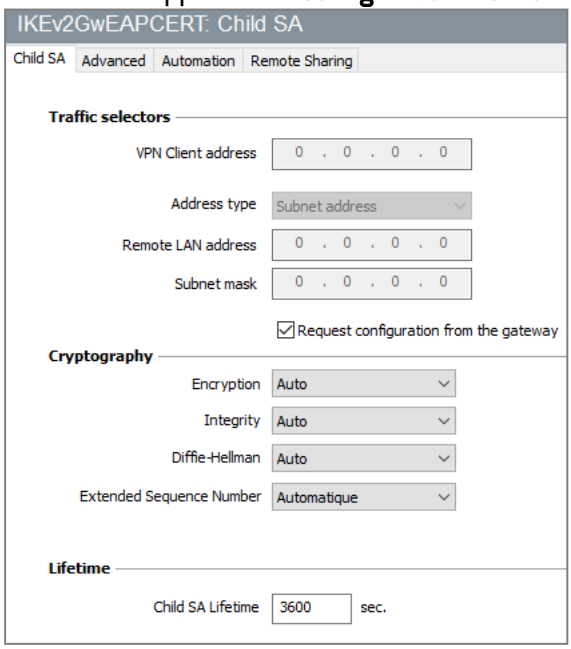
10. In the **Protocol** > **Advanced features** tab, select the **Fragmentation** checkbox and indicate the size of IKE fragments as defined on the firewall (1280 bytes according to Stormshield's recommendations).



11. Click on the upper menu **Configuration** > **Save** to save this configuration.

Configuring Phase 2

1. In the **VPN configuration** > **IKEv2** tree, right-click on the Phase 1 configuration created earlier (*IKEv2GwEAPCERT* in the example).
2. Select **New Child SA**.
   An entry named *Ikev2Tunnel* by default is added to the selected Phase 1 configuration.
3. Right-click on *Ikev2Tunnel* and select **Rename** to give this entry the name of your choice.
4. In the **Child SA** > **Traffic selectors** tab,
5. Select the checkbox **Request configuration from the gateway**.
6. Click on the upper menu **Configuration** > **Save** to save this configuration.

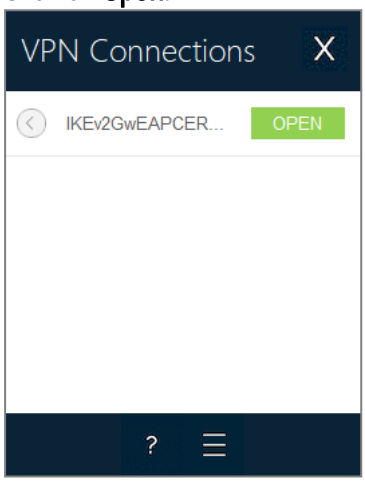


The VPN client has been configured to set up an IKEv1 tunnel with the firewall in *Config* mode based on EAP and certificate authentication.

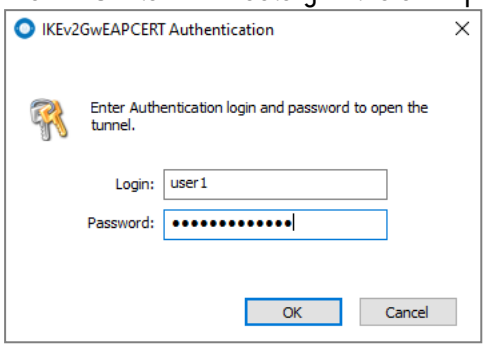
Setting up the IPsec VPN tunnel from the client workstation

On the user's Microsoft Windows workstation:

1. Right-click on the icon found in the Windows system tray (hidden icons): 
2. Select **Connection panel**.
3. Locate the connection created in the earlier steps (*IKEv2GwEAPCERT* in the example).
4. Click on **Open**.

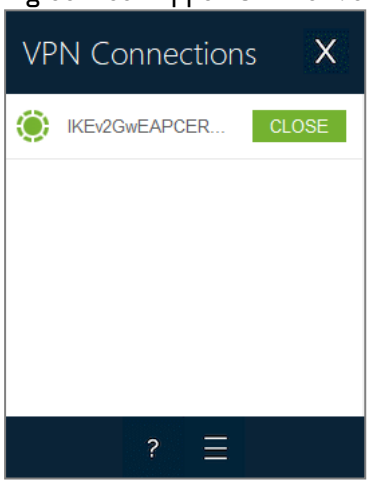


5. Enter the login and password configured in the reference directory (for *user1* in the firewall's internal directory in the example).



The tunnel is set up.

A green icon appears in front of it, and the button next to it now indicates **Close**:

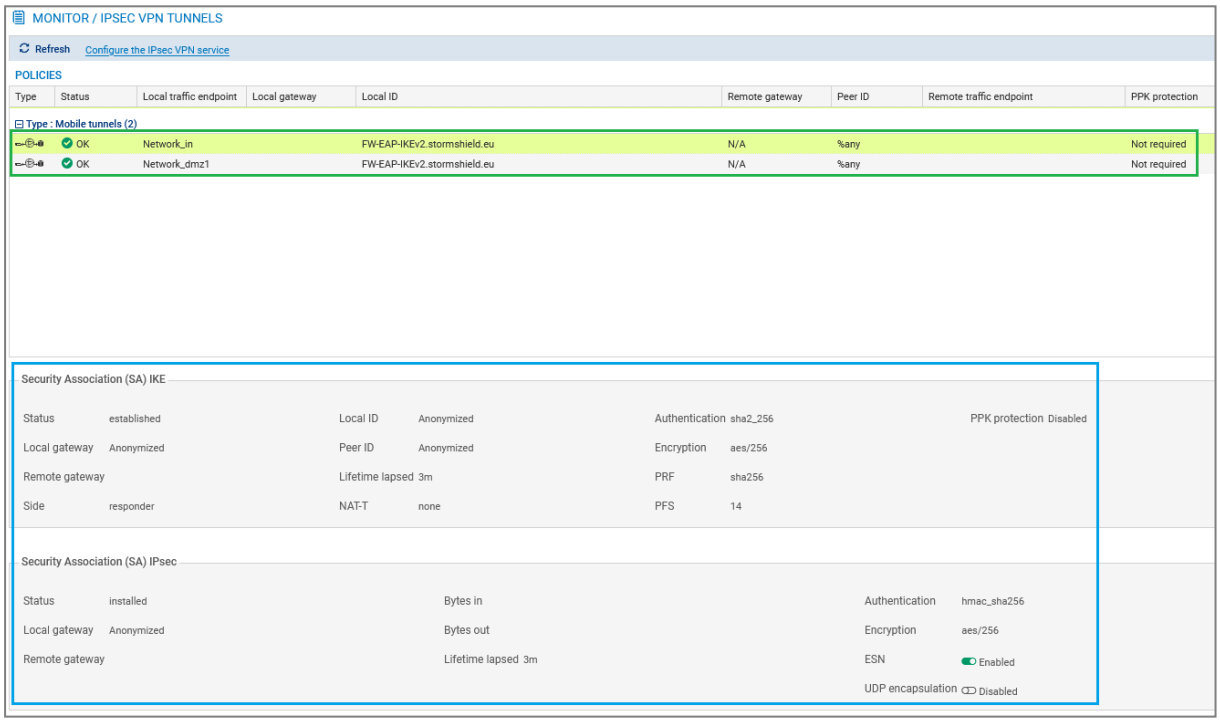


6. When you close the connection window by clicking on the cross, the tunnel will remain open.

Showing details of tunnels on the firewall

The **Monitoring** > **IPsec VPN tunnel monitoring** module shows the tunnels that have been set up and information and statistics about them:

- Local gateway name (firewall),
- Time lapsed since the tunnel was set up,
- Bytes sent by the firewall,
- Bytes received by the firewall,
- Status of the tunnel,
- Encryption algorithm used,
- Authentication algorithm used.



STORMSHIELD

documentation@stormshield.eu

Glossary

T

Term 1

Definition for Term 1.

Term 2

Definition for Term 2.

Term 3

Definition for Term 3.