STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

IKEV2 MOBILE IPSEC VPN - PRE-SHARED KEY AUTHENTICATION

Product concerned: SNS 3.7.x-LTSB, SNS 3.x, SNS 4.x, SN VPN Client Standard

Document last updated: April 11, 2024

Reference: sns-en-IKEv2_Mobile_IPSec_VPN_Pre-shared_Key_Authentication_Technical_Note

Table of contents

Change log

Date	Description
April 11, 2024	Section **Optimizing tunnel traffic and securing PSK authentication** replaced by section **Optimizing ISAKMP traffic during IPsec tunnel negotiations and securing authentication**
April 2020	New document

Read carefully before proceeding

This document is intended for administrators who wish to add mobile IKEv2 policies to their existing IKEv2 site-to-site IPsec tunnel configurations.

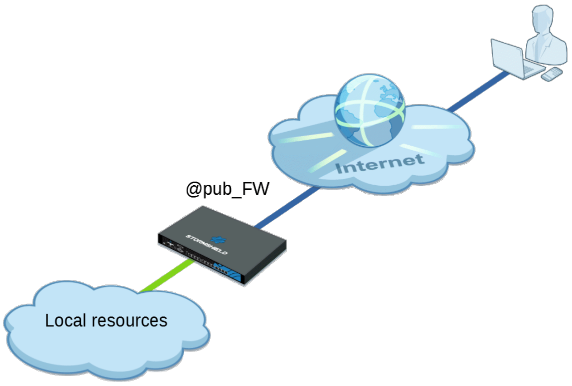
The ANSSI, France’s Network and Information Security Agency, recommends the use of IKEv2-based solutions for optimal security.

If your existing IPsec configuration already contains IKEv1 site-to-site IPsec tunnels and you wish to add a mobile IKEv2 policy to it, do note that there are several restrictions when IKEv1 and IKEv2 peers are used in the same IPsec policy:

- "Aggressive" negotiation mode is not allowed for IKEv1 peers using pre-shared key authentication. An error message appears when there is an attempt to enable the IPsec policy.
- The hybrid authentication method does not function for IKEv1 mobile peers.
- Backup peers are ignored. A warning message appears when the IPsec policy is enabled.
- In configurations that implement NAT-T (NAT-Traversal - transporting the IPsec protocol through a network that performs dynamic address translation), the peer local ID must be defined with the translated public IP adress that it presents to the remote peer during the negotiations. This identity must match the one associated to the pre-shared key configured for the remote peer.

In this case, we recommend that you refer to the tutorial **IKEv1 mobile IPsec VPN - Pre-shared key authentication**.

IKEv2 mobile IPsec VPN - Pre-shared key authentication



This document describes the VPN configuration required to allow remote users – also known as mobile or nomad users – to securely access their internal corporate networks from a Microsoft workstation on which SN VPN Client Standard has been installed.

The authentication method presented in this tutorial relies on the use of each user's pre-shared key.
The IPsec tunnels described in this technical note use version 2 of the IKE protocol.

Two configuration modes are covered here:

- *Config* mode, in which clients automatically receive all the network parameters needed to set up the IPsec VPN tunnel.
- Manual assignment of IP addresses to each user and manual configuration of the VPN client. Unlike *Config* mode, in this configuration, you can define several networks that are protected by the firewall and can be contacted by mobile users.

Requirements

- An LDAP directory must be configured on the firewall.
  If this has not yet been done, refer to the section Directories configuration in the **SNS User guide**.
- Every user defined in the LDAP directory must have an individual e-mail address.
- Install on the Microsoft client workstation **SNS VPN Client**, available in **Downloads** > **Stormshield Network Security** > **VPN Client** in your Mystormshield area (a software license is required after a trial period of 30 days) or from the IPsec VPN client TheGreenBow.
- The IPsec policy used must contain only IKEv2 IPsec peers (site-to-site and mobile tunnels).

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.

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

For an internal LDAP directory, go to **Configuration** > **Users** > **Users** :

1. Click on **Add group**.
2. In the **Group name** field, enter a representative name (e.g.: *Mobile_Users*).
   You can add a description.
3. Click on **Add**.
   A row appears in the grid of group members.
4. 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.
5. Repeat steps 3 and 4 to add all the users that must belong to this group.
6. When all members have been added, click on **Apply**.
7. Confirm by clicking on **Save**.

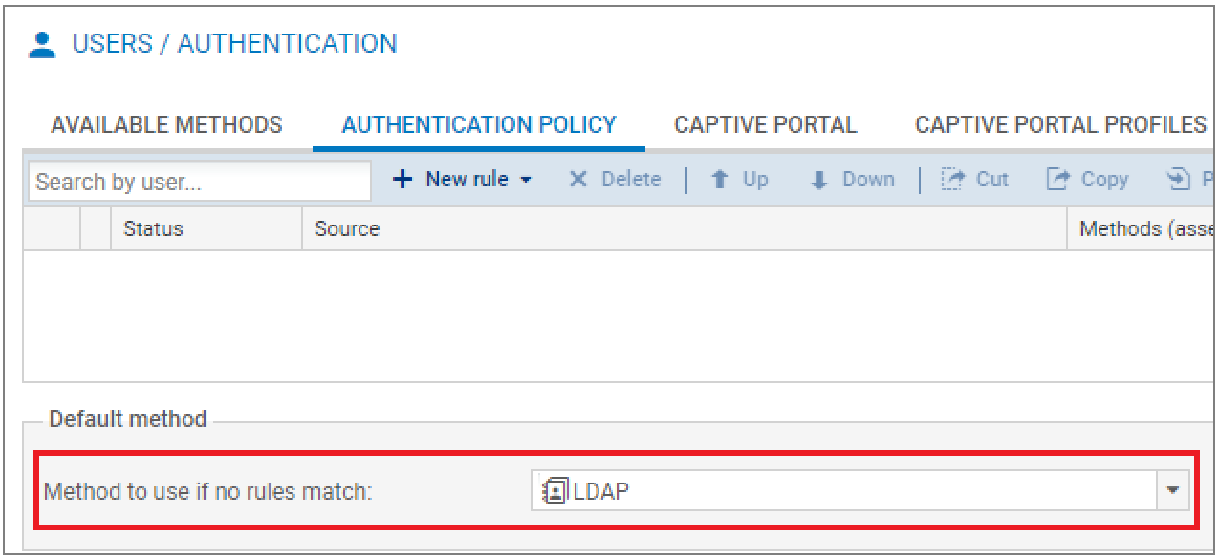
For an external directory (Microsoft Active Directory, LDAP or Posix LDAP), such groups must be created directly on one of the workstations that hosts the directory.

Checking whether the authentication method for mobile users is LDAP-based

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

If no authentication rules are found in the grid

Check whether the **Method to use if no rules match** field has been set to “LDAP”:



Default method

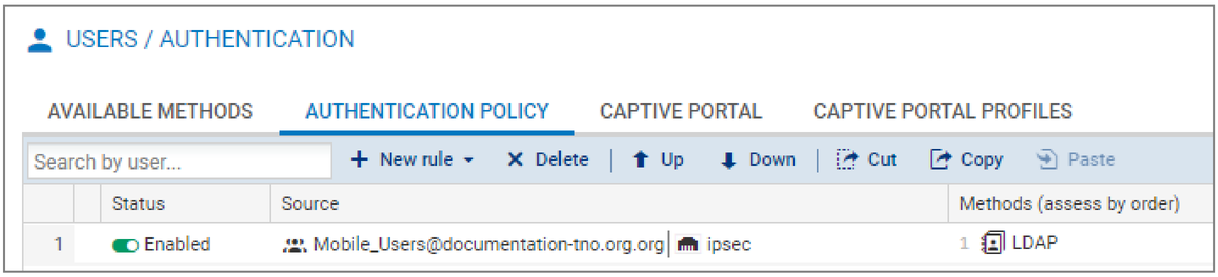
Method to use if no rules match: LDAP

If there are already authentication rules in the grid

Add an LDAP authentication rule for users from the IPsec VPN:

1. Click on **New rule** and select **Standard rule**.
2. In the **User or group** field, select the group created earlier (*Mobile_Users* in the example).
3. In the menu on the left side of this window, select **Source**.
4. Click on **Add an interface** and select **IPsec VPN**.
5. In the menu on the left side of this window, select **Authentication methods**.
6. Select the row in the grid that contains the **Default method** and click on **Remove**.
7. Click on **Authorize a method** and select **LDAP**.
8. Click **OK**.
9. Double-click on the cell corresponding to the **Status** column to enable this rule.
   Its status will switch to **Enabled**.
10. Click on **Apply** then on **Save**.

The authentication rule configured is therefore:



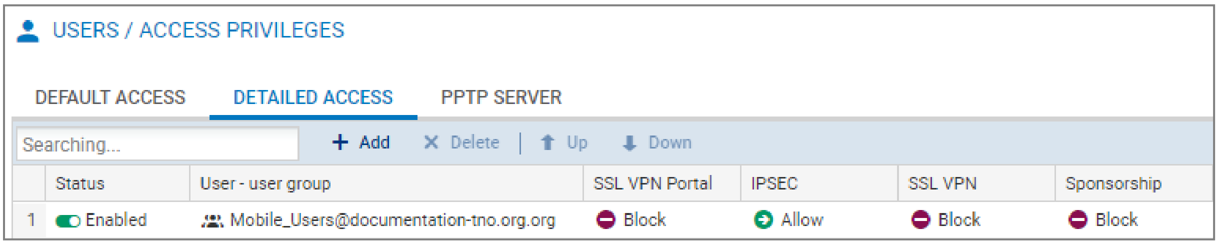
	Status	Source	Methods (assess by order)
1	Enabled	Mobile_Users@documentation-tno.org.org ipsec	1 LDAP

Allowing mobile users to set up IPsec VPN tunnels

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

1. Click on **Add**.
   A row appears in the grid.
2. Click on the cell in this row in the **User - user group** column.
3. Type the first few letters of the name of the group and select it from the list that the firewall suggests.
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**.

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



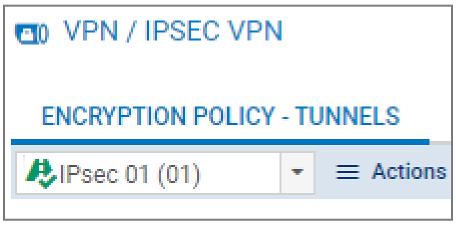
	Status	User - user group	SSL VPN Portal	IPSEC	SSL VPN	Sponsorship
1	Enabled	Mobile_Users@documentation-tno.org.org	Block	Allow	Block	Block

Optimizing ISAKMP traffic during IPsec tunnel negotiations and securing authentication

You are advised to modify several parameters on the firewall in order to optimize ISAKMP traffic during IPsec tunnel negotiation and secure PSK authentication against denial of service (DoS) attacks.

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*, regardless of whether ***Config* mode** or **standard mode** is used (**Configuration** > **VPN** > **IPsec VPN**):



Optimizing ISAKMP negotiation 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 the **Configuration** > **System** > **CLI** module.
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 (*IKEv2_Mobile_Users* 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
   ```

Securing PSK authentication against brute force attacks

To prevent DoS attacks during an attempt to connect via an IPsec VPN tunnel:

1. Go to the **Configuration** > **System** > **CLI console** module.
2. Enter the command:
   ```
   CONFIG IPSEC UPDATE slot=xy global=0 CookieThreshold=10
   BlockThreshold=5
   ```
   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*.
3. Apply these changes by typing:
   ```
   CONFIG IPSEC ACTIVATE
   ```

Reloading the IPsec policy to apply changes made earlier

1. Go to the **Configuration** > **System** > **CLI console** module.
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** > **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 will then be selected in a global profile, which in turn will be applied to the filter rule that grants access to VPN mobile clients.
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**.

Integrating this TCP-UDP inspection profile into a global inspection profile

In the **Application protection** > **Inspection profile** module:

1. Click on **Go to profiles**.
2. From the drop-down list, select the profile that you wish to associate with the TCP-UDP profile that was modified earlier with the MSS option. The profile *IPS_03* is selected in the example.
3. In the row TCP-UDP, click on the application profile suggested and select the modified profile (*tcpudp_03* in the example).
4. Confirm the change by clicking on **Apply**.
5. Confirm by clicking on **Save**.
   This is the IPS profile that must be selected for incoming traffic in the filter rule that allows traffic from mobile IPsec tunnels.

Implementing a mobile IPsec configuration in *Config* mode

In this configuration, mobile users set up the tunnel with an IP address that their VPN client obtained automatically.

To define a mobile IPsec policy in *Config* mode, configure the firewall as follows:

- Define a network object that groups the IP addresses assigned to mobile users during the setup of the IPsec VPN tunnel,
- Define a network object that represents the local network that connected mobile users can access via an IPsec VPN tunnel,
- Create the IKEv2 IPsec peer profile,
- Create the IKEv2 IPsec policy by using the peer profile defined earlier,
- Set up filter rules that allow traffic from mobile clients to the internal network.

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 can't be:

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

In the module **Configuration** > **Objects** > **Network**:

1. Click on **Add**.
2. Select **Network**.
3. Assign an **Object name** to this object (*Mobile_Users_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 at the same time via an IPsec VPN tunnel.
   Examples:
   192.168.9.0/24 or 192.168.9.0/255.255.255.0 : 254 addresses so 254 Phase 2.
   192.168.9.0/23 or 192.168.9.0/255.255.254.0 : 510 addresses so 510 Phase 2.
5. Click on **Create**.

Defining the local network that mobile peers in *Config* mode can access with network objects

In the module **Configuration** > **Objects** > **Network**:

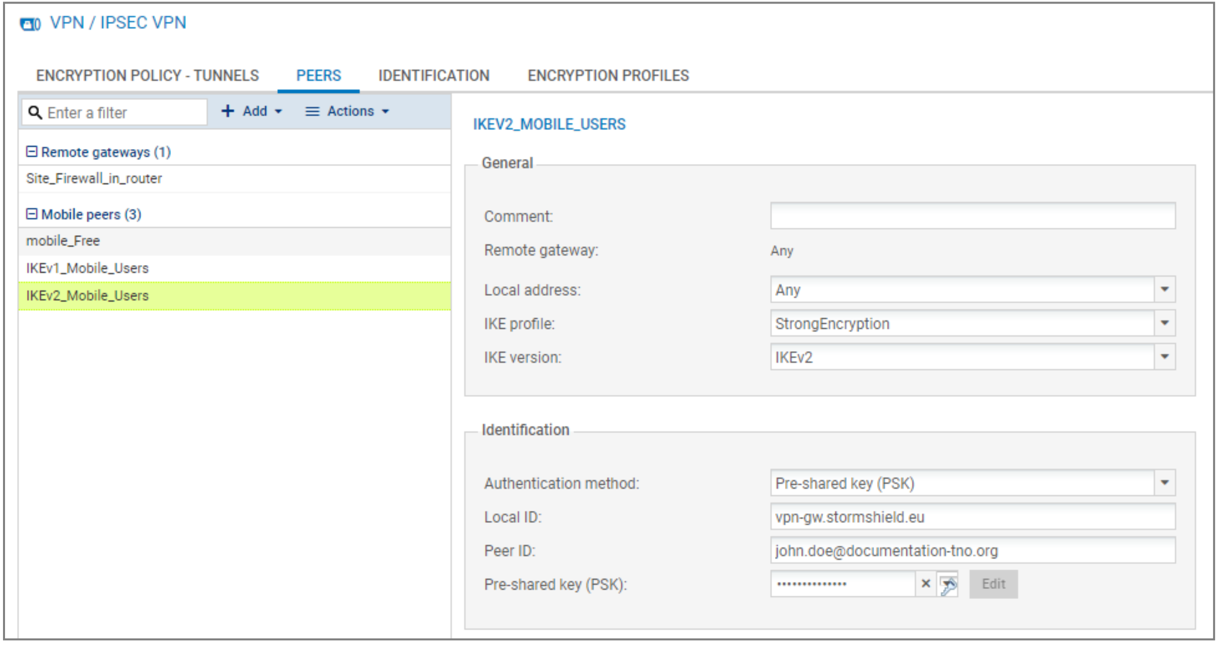
1. Click on **Add**.
2. Select **Network**.
3. Assign an **Object name** to this object (*Local_Network_Authorized_IPsec* in the example).
4. Enter the **Network IP address** field in the form of a network/mask.
   Example:
   192.168.1.0/24 or 192.168.1.0/255.255.255.0.
5. Click on **Create**.

Creating the profile of IPsec VPN peers

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

1. Click on **Add**.
2. Select **New remote peer**.
3. Name the mobile configuration (*IKEv2_Mobile_Users* in the example), select **IKEv2** in the field **IKE version**, then click on **Next**.
4. For **Authentication type**, select **Pre-shared key (PSK)**, then click on **Next**.
5. In the **Mobile tunnels: pre-shared keys (PSK)** table, click on **Add**.
6. In the **User ID** field, enter the e-mail address of the peer.
7. In the **Pre-shared key (ASCII)** and **Confirm** fields, enter the password used to set up the IPsec VPN tunnel for this peer.
   For obvious security reasons, choose unique passwords that meet ANSSI recommendations (in French).
8. Click on **Apply**.
9. Repeat steps 5 to 8 for each authorized mobile user.
10. Click on **Next**.
    You will see a summary showing the name of the peer, the policy and type of authentication chosen.
11. Confirm by clicking on **Finish**.
12. Select the peer created earlier and fill in the **Local ID** field.
    In general, the DNS name (FQDN) of the firewall is used. Example: *vpn-gw.stormshield.eu*.
13. Click on **Apply**, then on **Save**.
14. Click on **Activate this policy**.

The profile configured for IPsec mobile peers is therefore:



Remote gateways (1)
Site_Firewall_in_router

Mobile peers (3)
mobile_Free
IKEv1_Mobile_Users
IKEv2_Mobile_Users

IKEV2_MOBILE_USERS

General

Comment:
Remote gateway: Any
Local address: Any
IKE profile: StrongEncryption
IKE version: IKEv2

Identification

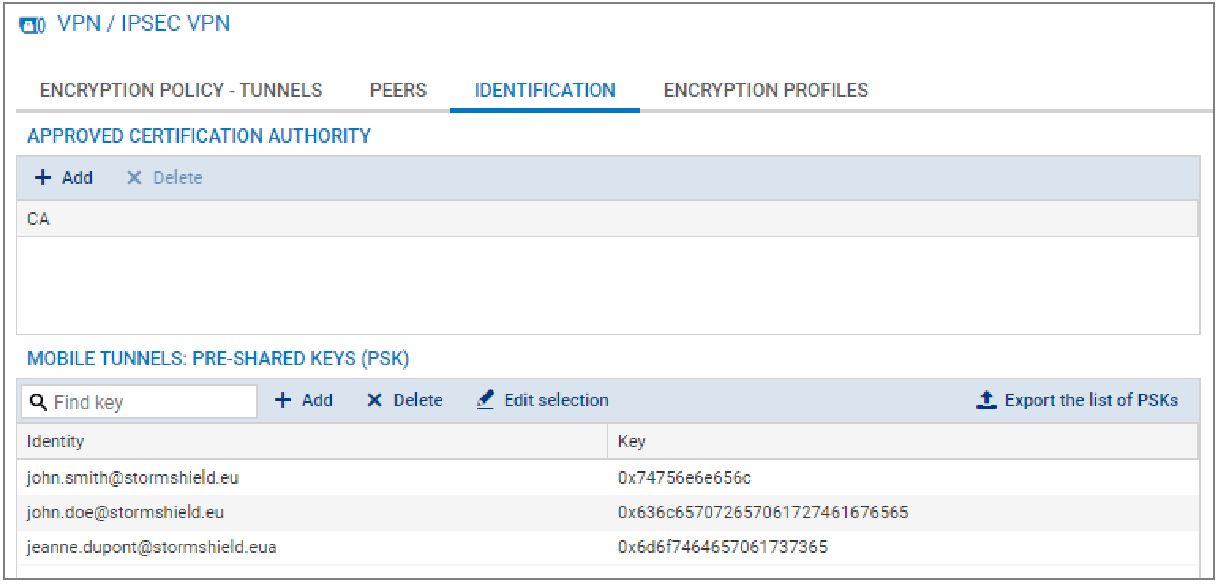
Authentication method: Pre-shared key (PSK)
Local ID: vpn-gw.stormshield.eu
Peer ID: john.doe@documentation-tno.org
Pre-shared key (PSK): ••••••••••••••

Adding pre-shared keys (PSK) to an existing policy

In the module **Configuration** > **VPN** > **IPsec VPN** > **Identification** tab:

1. Click on **Add** in the **Mobile tunnels: pre-shared keys** table.
2. In the **User ID** field, enter the e-mail address of the peer.
3. In the **Pre-shared key (ASCII)** and **Confirm** fields, enter the password used to set up the IPsec VPN tunnel for this peer.
   For obvious security reasons, choose unique passwords that meet ANSSI recommendations (in French).
4. Click on **OK**.
5. Repeat steps 1 to 4 for each PSK to be added.

Example of a table of pre-shared keys:



CA

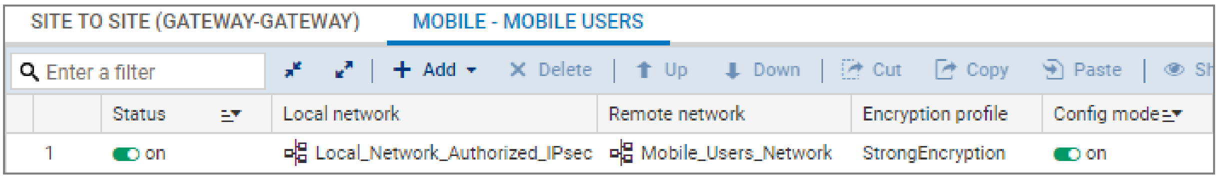
Identity	Key
john.smith@stormshield.eu	0x74756e6e656c
john.doe@stormshield.eu	0x636c65707265706172746167 6565
jeanne.dupont@stormshield.eua	0x6d6f7464657061737365

Creating the IPsec policy - *Config* mode

In the module **Configuration** > **VPN** > **IPsec VPN** > **Encryption policy – Tunnels** tab:

1. Select the IPsec policy that you wish to modify from the drop-down list (*IPsec 01* in the example).
2. Click on the **Mobile - Mobile users** tab.
3. Click on **Add**.
4. Select **New Config mode mobile policy**.
   A configuration wizard starts.
5. In the **Local ressources** field, select the network that mobile users can access through the IPsec VPN tunnel (object *Local_Network_Authorized_IPsec* created earlier in the example).
6. In the **Peer selection** field, select the mobile profile created earlier (*IKEv2_Mobile_Users* in the example).
   Reminder: only one network can be selected. Network groups cannot be selected.
7. 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 (*Mobile_Users_Network* in the example).
8. Click on **Finish**.
9. Click on **Apply** then confirm by clicking on **Save**.
10. Click on **Yes, activate the policy**.

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



	Status	Local network	Remote network	Encryption profile	Config mode
1	on	Local_Network_Authorized_IPsec	Mobile_Users_Network	StrongEncryption	on

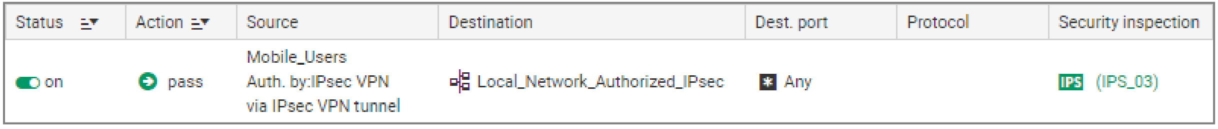
Allowing IPsec VPN access in filter policies

As an implicit filter rule manages the traffic needed to set up the IPsec VPN, the filter policy manages authenticated mobile users' access to internal resources via the VPN.

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 **Simple rule**.
   A new line will appear.
4. In the newly added row, double-click on the cell in the **Action** column.
   The configuration window of the rule opens.
   The **Action** section on the left in this configuration window is automatically selected.
5. In the **Action** field, select **pass**.
6. Select the **Source** menu on the left side of the configuration window.
7. In the **User** field, select the group of users allowed to set up IPsec VPN tunnels (*Mobile Users@stormshield.eu* in the example).
8. Click on the **Advanced properties** tab in the **Source** menu.
9. For the **Via** field, select **IPsec VPN tunnel**.
10. For the **Authentication method** field, select **IPsec VPN**.
11. Select the **Destination** menu on the left side of the configuration window.
12. Click on **Add** in the **Destination hosts** grid.
13. Select the network that mobile users can access through the IPsec VPN tunnel (object *Local_Network_Authorized_IPsec* in the example).
14. Select the **Inspection** menu on the left side of the configuration window.
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 **OK**.
17. Double-click on the cell in 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	Mobile_Users Auth. by:IPsec VPN via IPsec VPN tunnel	Local_Network_Authorized_IPsec	Any		IPS (IPS_03)

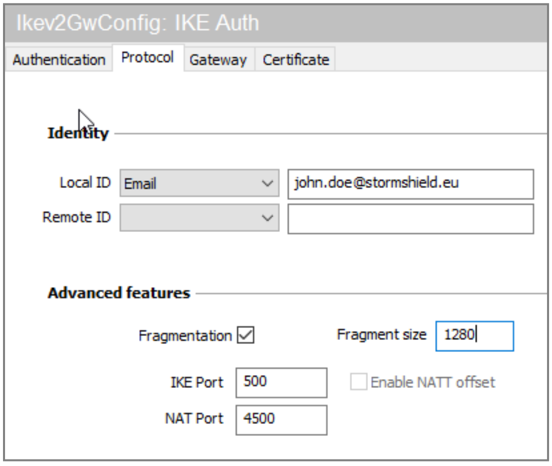
Configuring the VPN client

On the user's Microsoft Windows workstation:, open the connection window of the VPN client:

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

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 (*IKEv2GwConfig* in the example).
4. Click on this entry.
5. In the **Protocol** tab > **Identity** > **Local ID** field, select **E-mail** from the drop-down list and enter the e-mail address of the workstation user.
6. In the **Protocol** tab > **Advanced features** section, select the **Fragmentation** checkbox and indicate the size of IKE fragments as defined on the firewall (1280 bytes according to Stormshield's recommendations).



Identity

Local ID: Email john.doe@stormshield.eu

Remote ID:

Advanced features

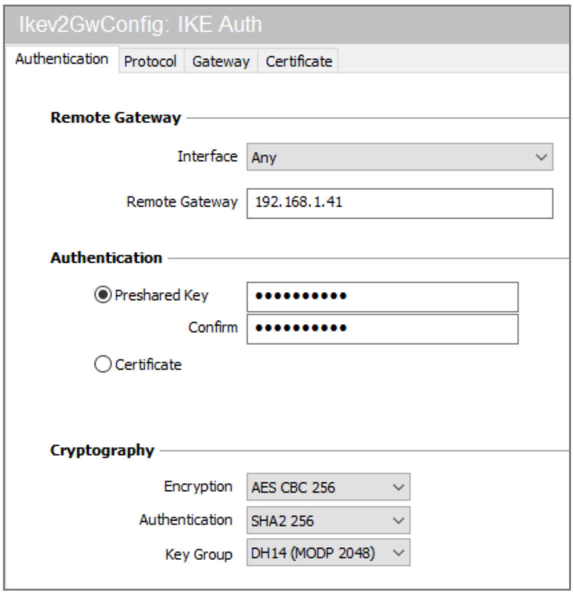
Fragmentation ☑ Fragment size 1280

IKE Port 500 ☐ Enable NATT offset

NAT Port 4500

7. In the **Authentication** tab > **Remote router address** > **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.

8. In the **Authentication** tab > **Authentication** > **Preshared key** field, enter and confirm the **pre-shared key defined for this user on the firewall**.



Remote Gateway

Interface: Any

Remote Gateway: 192.168.1.41

Authentication

● Preshared Key: ••••••••••

Confirm: ••••••••••

○ Certificate

Cryptography

Encryption: AES CBC 256

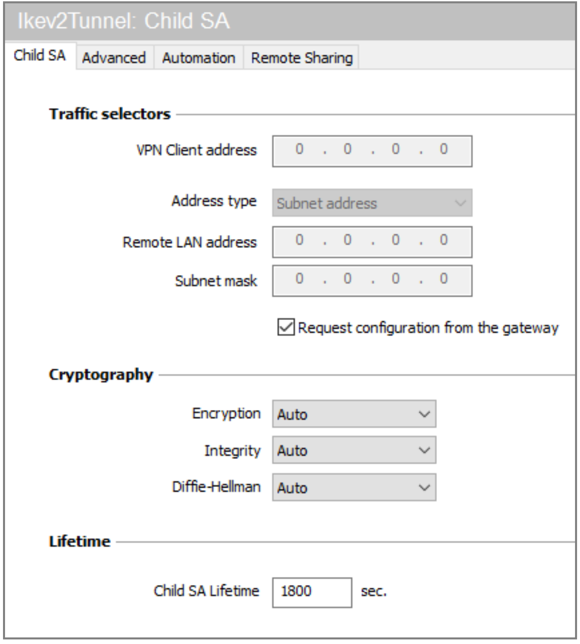
Authentication: SHA2 256

Key Group: DH14 (MODP 2048)

9. 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 (*IKEv2GwConfig* 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** tab > **Traffic selectors** section, select **Request configuration from the gateway**.
5. Click on the upper menu **Configuration** > **Save** to save this configuration.



Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption: Auto

Integrity: Auto

Diffie-Hellman: Auto

Lifetime

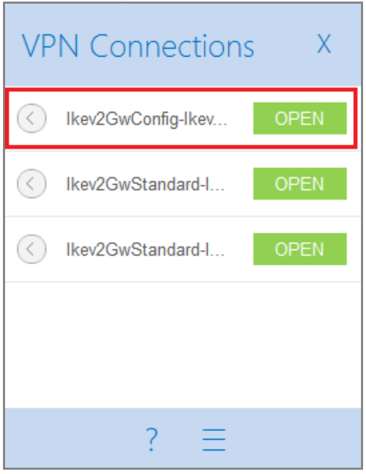
Child SA Lifetime: 1800 sec.

The VPN client is now configured to set up an IKEv2 tunnel in *Config* mode with the firewall.

Setting up the IPsec VPN tunnel from the client workstation

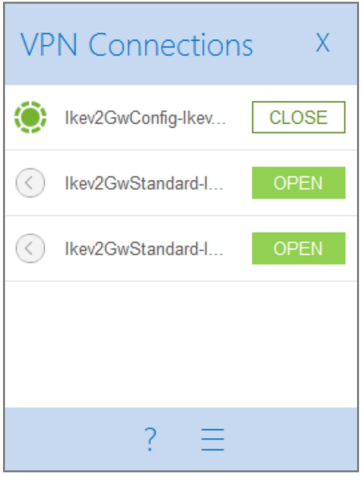
On the user's Microsoft Windows workstation:

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 (*Ikev2GwConfig-Ikev2Tunnel* in the example).
4. Click on **Open**.


VPN Connections X

○	Ikev2GwConfig-Ikev...	OPEN
○	Ikev2GwStandard-I...	OPEN
○	Ikev2GwStandard-I...	OPEN

The tunnel is set up.
A green icon appears in front of it, and the button next to it now indicates **Close**:


VPN Connections X

●	Ikev2GwConfig-Ikev...	CLOSE
○	Ikev2GwStandard-I...	OPEN
○	Ikev2GwStandard-I...	OPEN

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

Shutting down a 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 tunnel to shut down (*Ikev2GwConfig-Ikev2Tunnel* in the example).
4. Click on **Close**.

Implementing a mobile IPsec configuration in standard mode

In this configuration, mobile users set up the tunnel with an IP address entered in their VPN client.

To define a mobile IPsec policy in standard mode (not *Config* mode), configure the firewall as follows:

- Define a network object that groups the IP addresses assigned to mobile users during the setup of the IPsec VPN tunnel,
- Define one or several network objects corresponding to the network(s) that mobile users can access during the setup of the IPsec VPN tunnel,
- Create the IKEv2 IPsec peer profile,
- Create the IKEv2 IPsec policy by using the peer profile defined earlier,
- Set up filter rules that allow traffic from mobile clients to the internal network.

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

If VPN clients must reach *n* discontiguous networks, i.e., networks that cannot be grouped in an IP address range or in a single network, each VPN client will then need *n* IP addresses.

Defining the network object

In the module **Configuration** > **Objects** > **Network**:

1. Click on **Add**.
2. Select **Network**.
3. Assign a **Name** to this object (*Mobile_Users_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 via an IPsec VPN tunnel.
   Examples:
   192.168.9.0/24 or 192.168.9.0/255.255.255.0 : 254 addresses so 254 Phase 2.
   192.168.9.0/23 or 192.168.9.0/255.255.254.0 : 510 addresses so 510 Phase 2.
5. Click on **Create**.

Defining the network(s) that mobile peers can access with network objects

Mobile users may need to access one or several networks protected by the firewall.

For the purposes of the example presented in this tutorial, assume that mobile clients can access two separate, discontiguous networks via IPsec: Network 192.168.1.0/24 and Network 192.168.128.0/24. Two network objects therefore need to be created for this configuration.

You need to create as many network objects as the number of discontiguous networks that the VPN clients can reach.

Creating the first network object

Create the first network object in the module **Configuration** > **Objects** > **Network**:

1. Click on **Add**.
2. Select **Network**.
3. Assign an **Object name** to this object (*Local_Network_Authorized_IPsec* in the example).
4. Fill in the **Network IP address** (in the form of a network/mask) with the first protected network that mobile users can access:
   192.168.1.0/24 or 192.168.1.0/255.255.255.0.
5. Click on **Create**.

Creating the second network object

By following the method described for the first network object, create the second network object named *Local_Network_Authorized_IPsec2* in the example, corresponding to the network 192.168.128.0/24 (or 192.168.128.0/255.255.255.0).

Do note that both of these network objects can be grouped as a group object.
For the purposes of illustration, we will deliberately not group them to show that several destination networks can be selected when creating the standard IPsec mobile policy.

Reminder

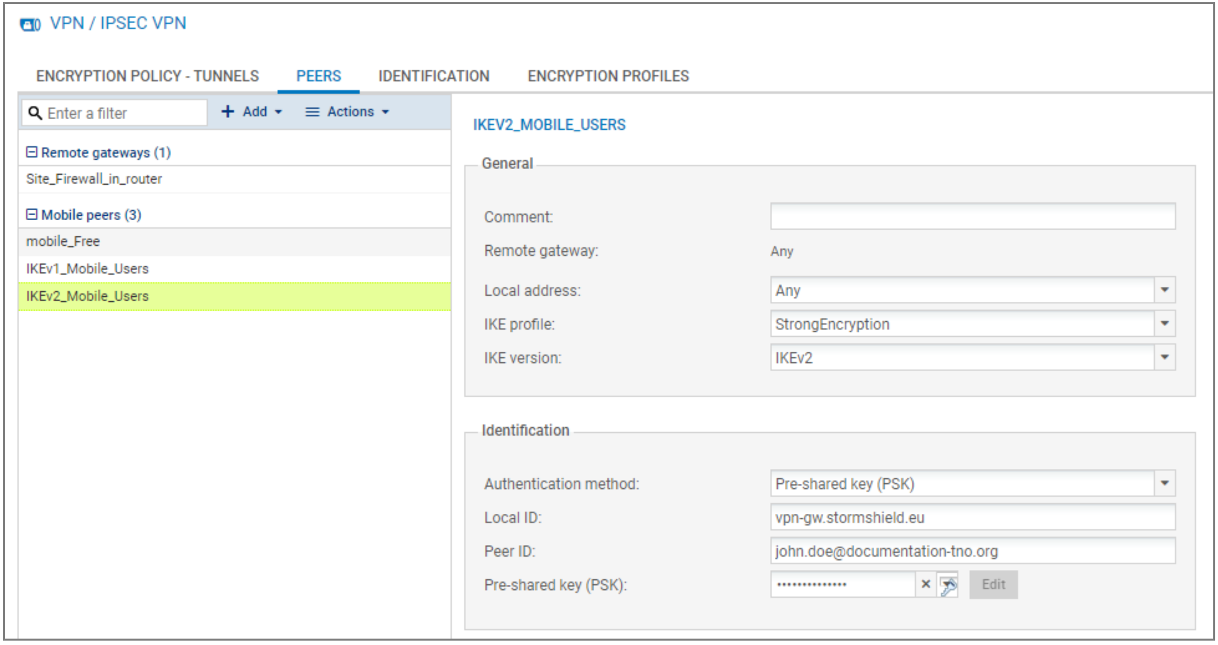
If VPN clients must reach *n* discontiguous networks, i.e., networks that cannot be grouped in an IP address range or in a single network, *n* Phase 2 configurations must be created on each VPN client.

Creating the profile of IPsec VPN peers

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

1. Click on **Add**.
2. Select **New remote peer**.
3. Name the mobile configuration (*IKEv2_Mobile_Users* in the example), select **IKEv2** in the field **IKE version**, then click on **Next**.
4. For **Authentication type**, select **Pre-shared key (PSK)**, then click on **Next**.
5. In the **Mobile tunnels: pre-shared keys (PSK)** table, click on **Add**.
6. In the **User ID** field, enter the e-mail address of the peer.
7. In the **Pre-shared key (ASCII)** and **Confirm** fields, enter the password used to set up the IPsec VPN tunnel for this peer.
   For obvious security reasons, choose unique passwords that meet ANSSI recommendations (in French).
8. Click on **Apply**.
9. Repeat steps 5 to 8 for each authorized mobile user.
10. Click on **Next**.
    You will see a summary showing the name of the peer, the policy and type of authentication chosen.
11. Confirm by clicking on **Finish**.
12. Select the peer created earlier and fill in the **Local ID** field.
    In general, the DNS name (FQDN) of the firewall is used. Example: *vpn-gw.stormshield.eu*.
13. Click on **Apply**, then on **Save**.
14. Click on **Activate this policy**.

The profile configured for IPsec mobile peers is therefore:



⊟ Remote gateways (1)
- Site_Firewall_in_router

⊟ Mobile peers (3)
- mobile_Free
- IKEv1_Mobile_Users
- IKEv2_Mobile_Users

IKEV2_MOBILE_USERS

General

Comment:

Remote gateway: Any

Local address: Any

IKE profile: StrongEncryption

IKE version: IKEv2

Identification

Authentication method: Pre-shared key (PSK)

Local ID: vpn-gw.stormshield.eu

Peer ID: john.doe@documentation-tno.org

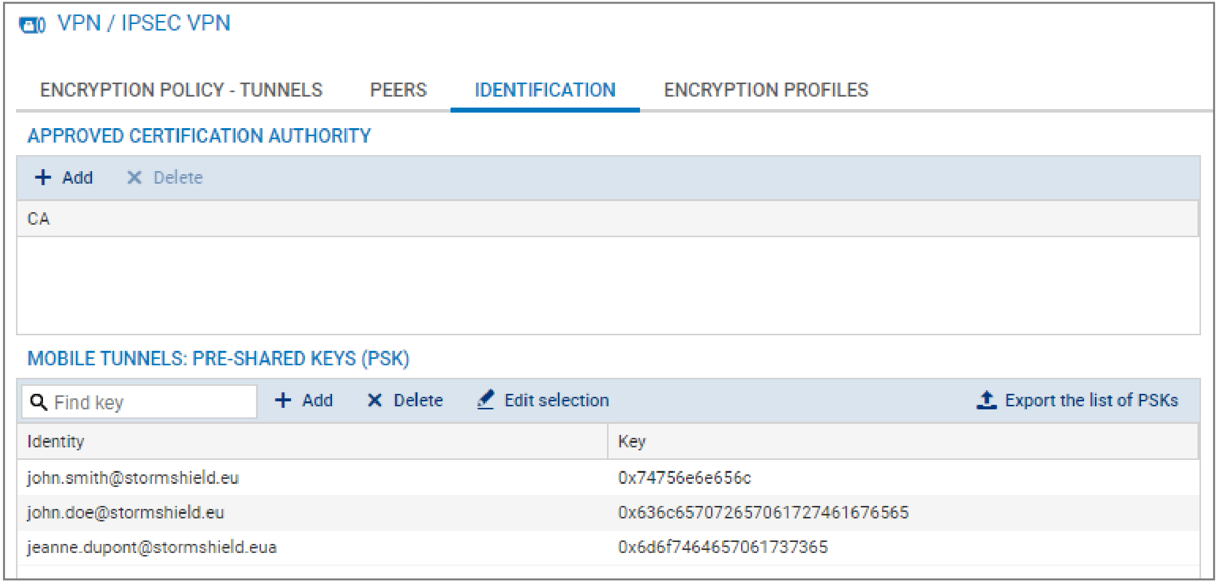
Pre-shared key (PSK): •••••••••••••• Edit

Adding pre-shared keys (PSK) to an existing policy

In the module **Configuration** > **VPN** > **IPsec VPN** > **Identification** tab:

1. Click on **Add** in the **Mobile tunnels: pre-shared keys** table.
2. In the **User ID** field, enter the e-mail address of the peer.
3. In the **Pre-shared key (ASCII)** and **Confirm** fields, enter the password used to set up the IPsec VPN tunnel for this peer.
   For obvious security reasons, choose unique passwords that meet ANSSI recommendations (in French).
4. Click on **OK**.
5. Repeat steps 1 to 4 for each PSK to be added.

Example of a table of pre-shared keys:



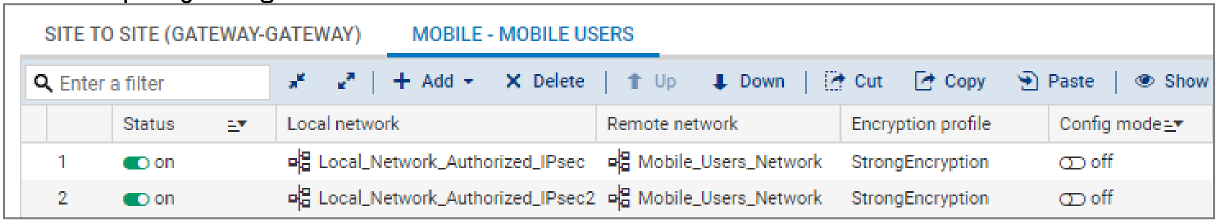
Identity	Key
john.smith@stormshield.eu	0x74756e6e656c
john.doe@stormshield.eu	0x636c6570726570617274461676565
jeanne.dupont@stormshield.eua	0x6d6f7464657061737365

Creating the IPsec policy

In the module **Configuration** > **VPN** > **IPsec VPN** > **Encryption policy – Tunnels** tab:

1. Select the IPsec policy that you wish to modify from the drop-down list (*IPsec 01* in the example).
2. Click on the **Mobile - Mobile users** tab.
3. Click on **Add**.
4. Select **New standard mobile policy**.
   A configuration wizard starts.
5. In the **Local resources** field, select the networks or network group(s) that mobile users can access through the IPsec VPN tunnel (objects *Local_Network_Authorized_IPsec* and *Local_Network_Authorized_IPsec2* in the example).
6. In the **Peer selection** field, select the mobile profile created earlier (*IKEv2_Mobile_Users* in the example).
7. Click on **Finish**.
8. Click on **Apply** then confirm by clicking on **Save**.
9. Click on **Yes, activate the policy**.

The IPsec policy configured is therefore:



	Status	Local network	Remote network	Encryption profile	Config mode
1	on	Local_Network_Authorized_IPsec	Mobile_Users_Network	StrongEncryption	off
2	on	Local_Network_Authorized_IPsec2	Mobile_Users_Network	StrongEncryption	off

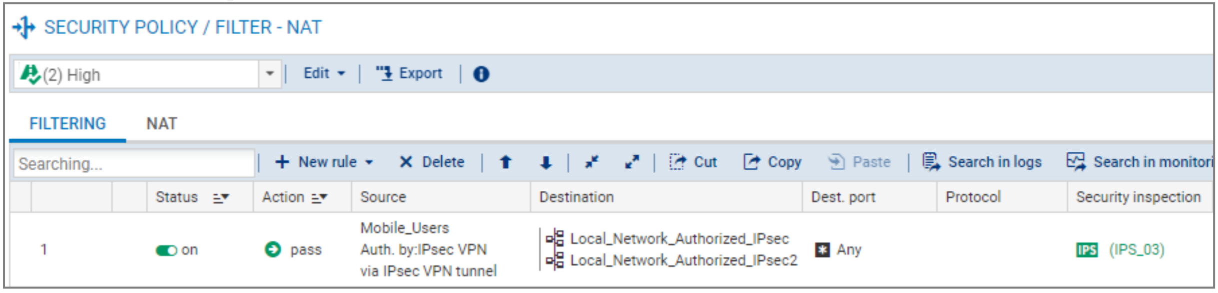
Allowing IPsec VPN access in filter policies

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 **Simple 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.
   The **Action** section on the left in this configuration window is automatically selected.
5. In the **Action** field, select **pass**.
6. Select the **Source** menu on the left side of the configuration window.
7. In the **User** field, select the group of users allowed to set up IPsec VPN tunnels (*Mobile Users@stormshield.eu* in the example)..
8. Click on the **Advanced properties** tab in the **Source** menu.
9. For the **Via** field, select **IPsec VPN tunnel**.
10. For the **Authentication method** field, select **IPsec VPN**.
11. Select the **Destination** menu on the left side of the configuration window.
12. Click on **Add** in the **Destination hosts** grid.

13. Select the networks that mobile users can access through the IPsec VPN tunnel (objects *Local_Network_Authorized_IPsec* and *Local_Network_Authorized_IPsec2* in the example).
14. Select the **Inspection** menu on the left side of the configuration window.
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 **OK**.
17. Double-click on the cell in 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
1	on	pass	Mobile_Users Auth. by:IPsec VPN via IPsec VPN tunnel	Local_Network_Authorized_IPsec Local_Network_Authorized_IPsec2	Any		IPS (IPS_03)

Configuring the VPN client

On the user's Microsoft Windows workstation:, open the connection window of the VPN client:

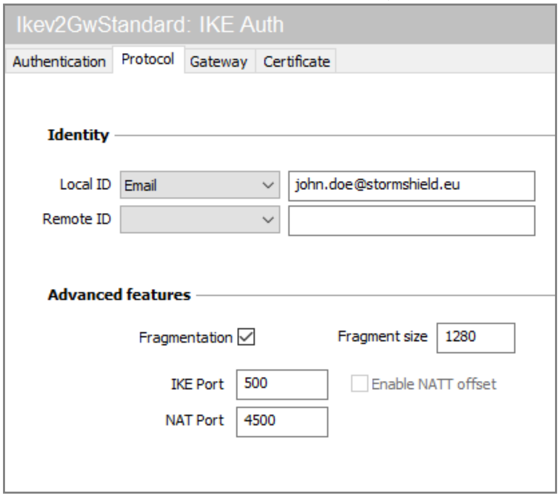
1. Right-click on the icon found in the Windows system tray (hidden icons):
2. Select **Configuration panel**.

For the purposes of the example presented in this tutorial, we assumed that mobile clients could access two separate, discontiguous networks via IPsec: Network 192.168.1.0/24 and Network 192.168.128.0/24.
Two separate Phase 2 configurations therefore need to be created for this configuration – one for each network. You need to create as many Phase 2 configurations as the number of discontiguous networks that the VPN clients can reach.
Do note that each of these Phase 2 configurations will use a separate VPN client IP address.

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 (*Ikev2GwStandard* in the example).
4. Click on this entry.
5. In the **Protocol** tab > **Identity** > **Local ID** field, select **E-mail** from the drop-down list and enter the e-mail address of the workstation user.

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



Ikev2GwStandard: IKE Auth

Identity

Local ID: Email — john.doe@stormshield.eu

Remote ID:

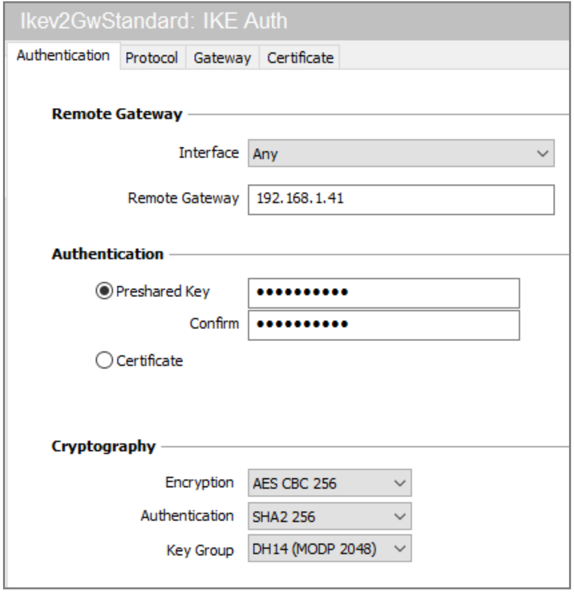
Advanced features

Fragmentation ☑ Fragment size: 1280

IKE Port: 500 □ Enable NATT offset

NAT Port: 4500

7. In the **Authentication** tab > **Remote router address** > **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.
8. In the **Authentication** tab > **Authentication** > **Preshared key** field, enter and confirm the pre-shared key defined for this user on the firewall.



Ikev2GwStandard: IKE Auth

Remote Gateway

Interface: Any

Remote Gateway: 192.168.1.41

Authentication

● Preshared Key: ••••••••••

Confirm: ••••••••••

○ Certificate

Cryptography

Encryption: AES CBC 256

Authentication: SHA2 256

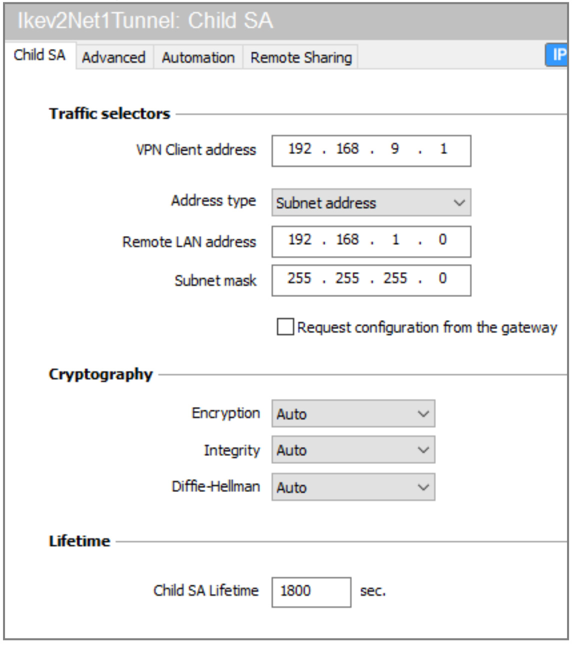
Key Group: DH14 (MODP 2048)

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

Configuring Phase 2 for the first network

1. In the **VPN configuration** > **IKEv2** tree, right-click on the Phase 1 configuration created earlier (*Ikev2GwStandard* 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 (*Ikev2Net1Tunnel* in the example).

4. In the **Child SA** tab > **Traffic selectors** > **VPN Client address** field, enter the IP address of the client (*192.168.9.1* in the example). This address must belong to the network defined in the section Defining a network object that contains IP addresses assigned to mobile peers.
5. In the **Child SA** tab > **Traffic selectors** > **Address type** field, select **Network address**.
6. In the **Remote network address** field, enter the address of the first reachable network (*192.168.1.0* in the example).
7. In the **Subnet mask** field, enter the mask associated with this network (*255.255.255.0* in the example).



Traffic selectors

VPN Client address: 192 . 168 . 9 . 1

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

□ Request configuration from the gateway

Cryptography

Encryption: Auto

Integrity: Auto

Diffie-Hellman: Auto

Lifetime

Child SA Lifetime: 1800 sec.

8. In the **Advanced** tab > **Alternative servers**, if necessary, define a **DNS suffix** and **Alternative (DNS) Servers** to be used for this IPsec VPN tunnel.
9. Click on the upper menu **Configuration** > **Save** to save this configuration.

The IKEv2 tunnel to reach the first network in the example is now configured.

Configuring Phase 2 for the second accessible network

Apply the method described in the section Configuring Phase 2 for the first network to define the tunnel that enables access to the second network.

In the example given, the parameters used for the second tunnel are:

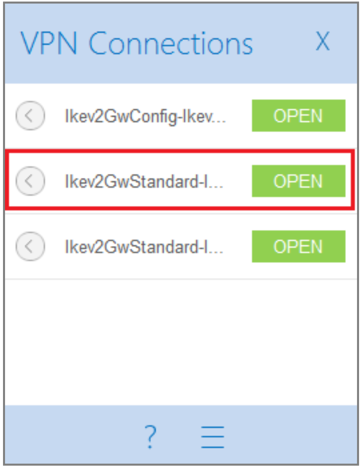
- Phase 2 name: *Ikev2Net2Tunnel*
- VPN client IP address: 192.168.9.2
- Network IP address: 192.168.128.0
- Mask: 255.255.255.0

Setting up an IPsec VPN tunnel from the client workstation

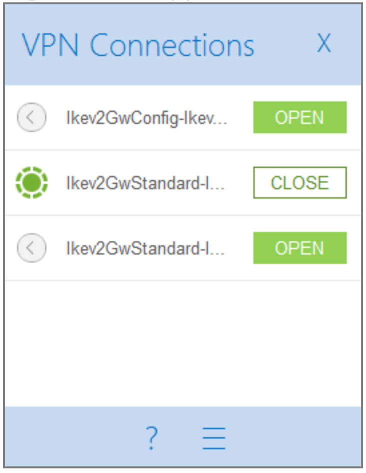
On the user's Microsoft Windows workstation:

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

3. Locate the first connection created in the earlier steps (*Ikev2GwStandard-Ikev2Net1Tunnel* in the example).
4. Click on **Open**.



The tunnel is set up.
A green icon appears in front of it, and the button next to it now indicates **Close**:



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

Repeat steps 2 to 4 to open a second tunnel.

Shutting down a tunnel from the client workstation

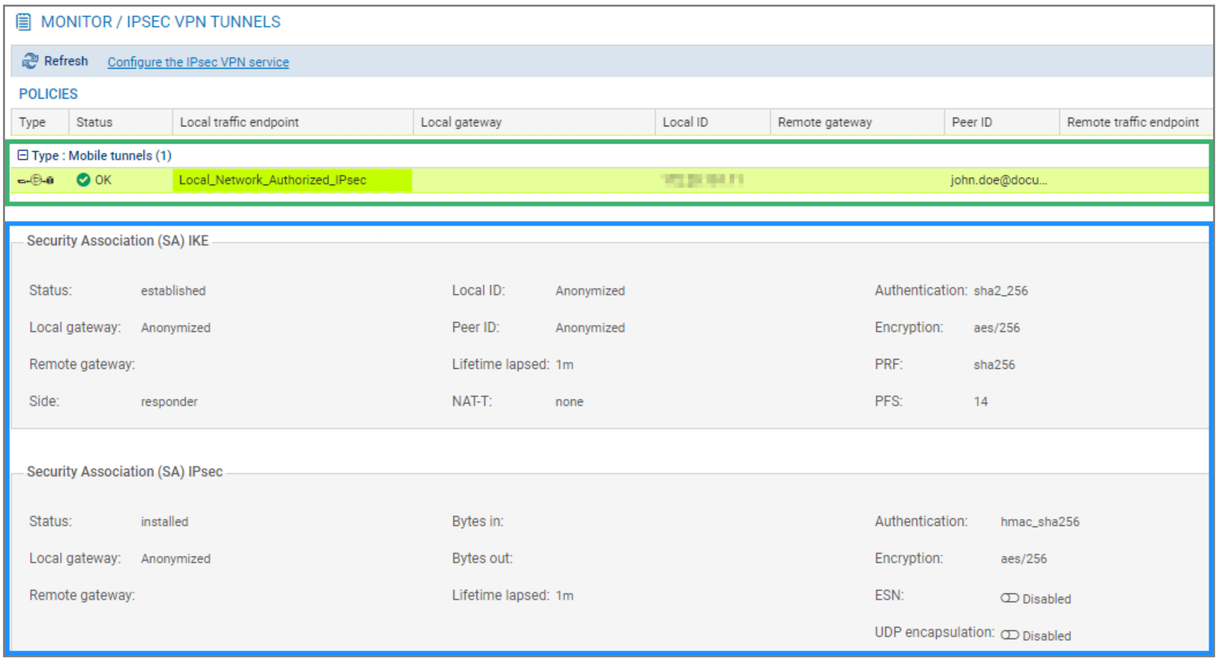
On the user's Microsoft Windows workstation:

1. Right-click on the icon found in the Windows system tray (hidden icons): 🌐
2. Select **Connection panel**.
3. Locate the tunnel to shut down (*Ikev2GwStandard-Ikev2Net1Tunnel* in the example).
4. Click on **Close**.

Showing details of a tunnel 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.



MONITOR / IPSEC VPN TUNNELS

Refresh Configure the IPsec VPN service

POLICIES

Type	Status	Local traffic endpoint	Local gateway	Local ID	Remote gateway	Peer ID	Remote traffic endpoint
⊟ Type : Mobile tunnels (1)							
	✓ OK	Local_Network_Authorized_IPsec		[redacted]		john.doe@docu...	

Security Association (SA) IKE

Status:	established	Local ID:	Anonymized	Authentication:	sha2_256
Local gateway:	Anonymized	Peer ID:	Anonymized	Encryption:	aes/256
Remote gateway:		Lifetime lapsed:	1m	PRF:	sha256
Side:	responder	NAT-T:	none	PFS:	14

Security Association (SA) IPsec

Status:	installed	Bytes in:		Authentication:	hmac_sha256
Local gateway:	Anonymized	Bytes out:		Encryption:	aes/256
Remote gateway:		Lifetime lapsed:	1m	ESN:	○ Disabled
				UDP encapsulation:	○ Disabled

Further reading

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

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.