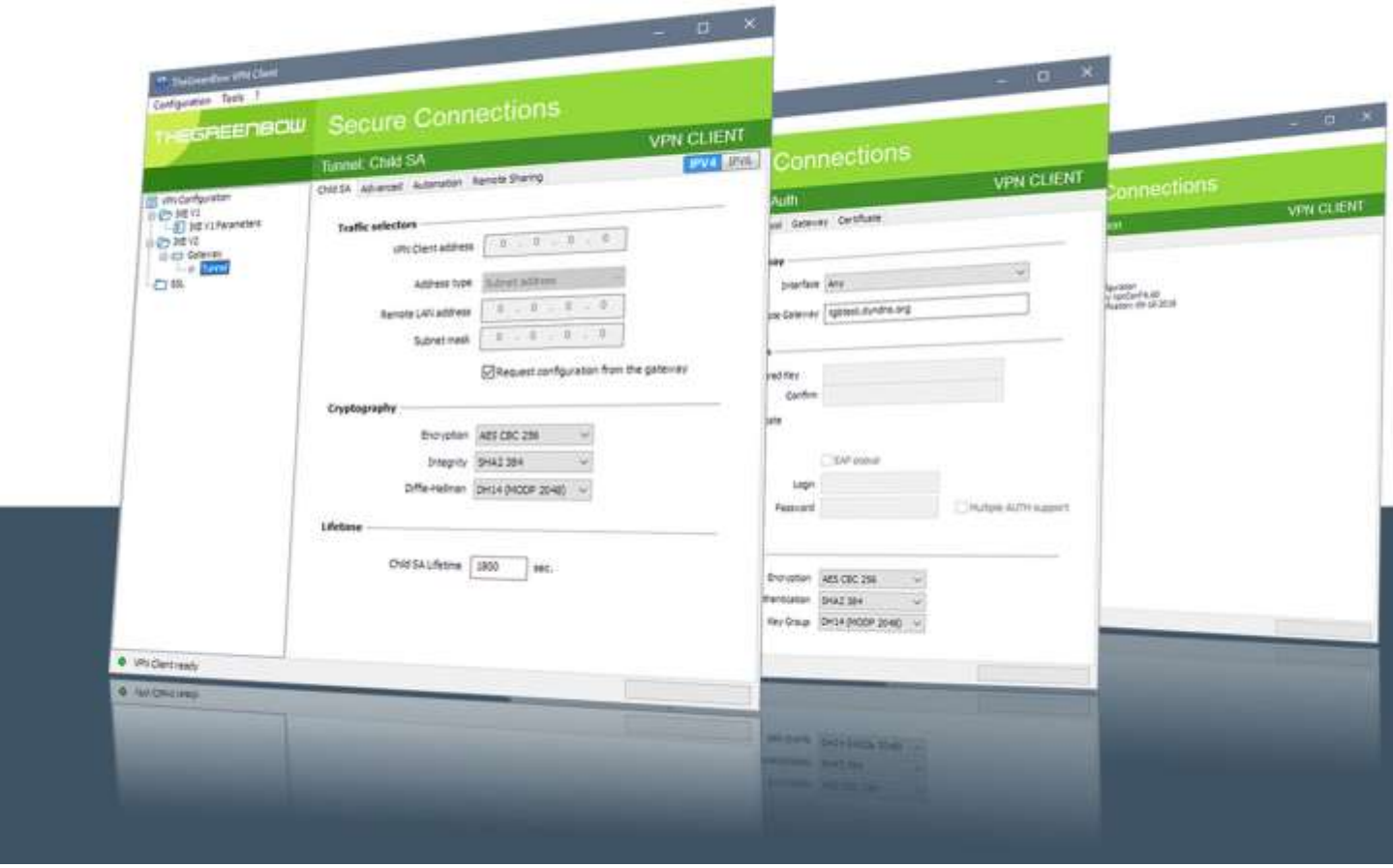


TheGreenBow IPsec VPN Client

Configuration Guide
Dynfi

Protocol - IKEv2

Website: **www.thegreenbow.com**
Contact: **support@thegreenbow.com**

Table of Contents

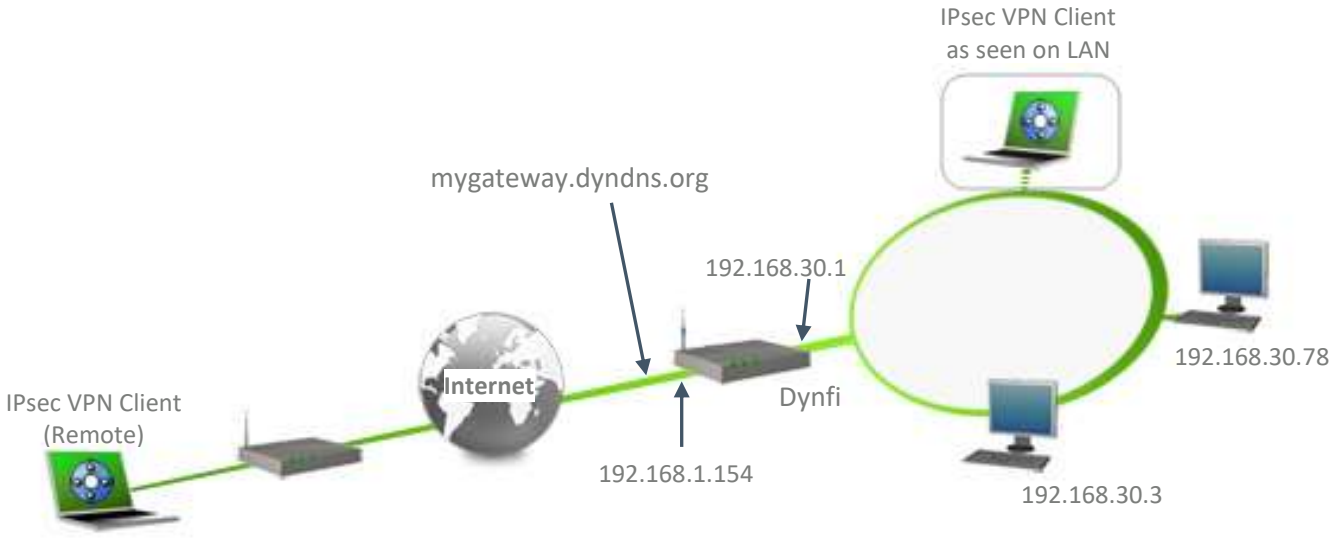
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a Dynfi VPN router to establish VPN connections for remote access to corporate network.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the Dynfi router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



1.3 Dynfi Restrictions

No known restrictions

1.4 Dynfi VPN Gateway

Our tests and VPN configuration have been conducted with Dynfi 20.0.

1.5 Dynfi VPN Gateway product info

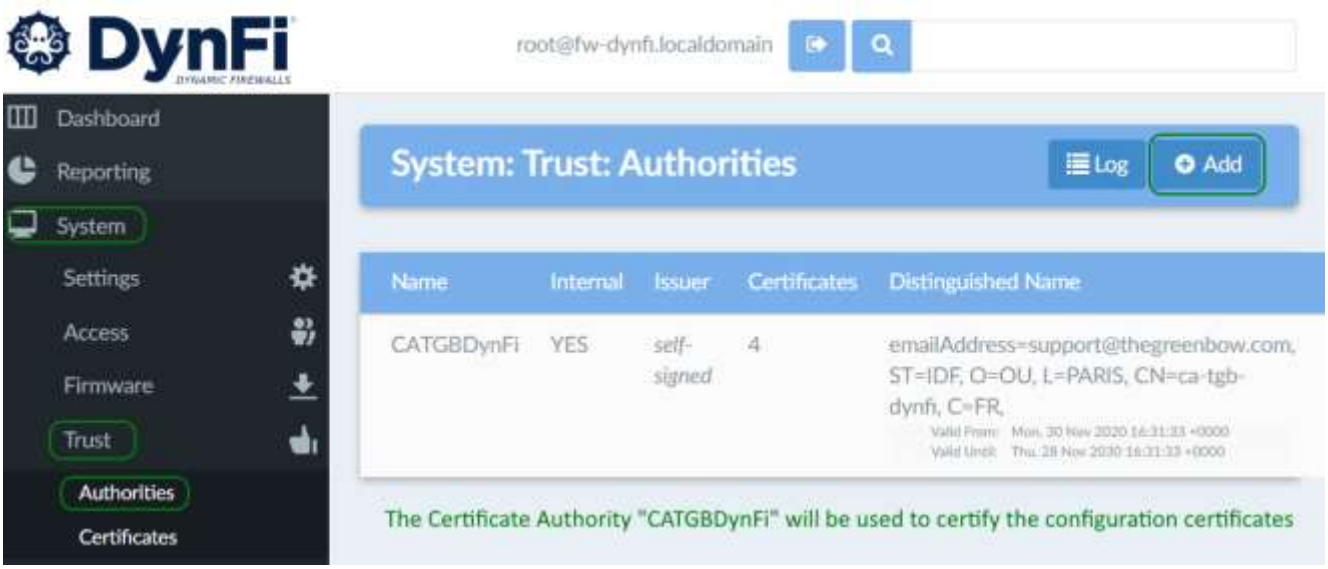
It is critical that users find all necessary information about Dynfi Gateway. All product info, User Guide and knowledge base for the Dynfi Gateway can be found on the Dynfi website: **https://dynfi.com/documentation/**

Dynfi Product page	**https://dynfi.com/**
Dynfi User Guide	**https://dynfi.com/documentation/**
Dynfi FAQ	**https://dynfi.com/faq**

2 Dynfi VPN configuration

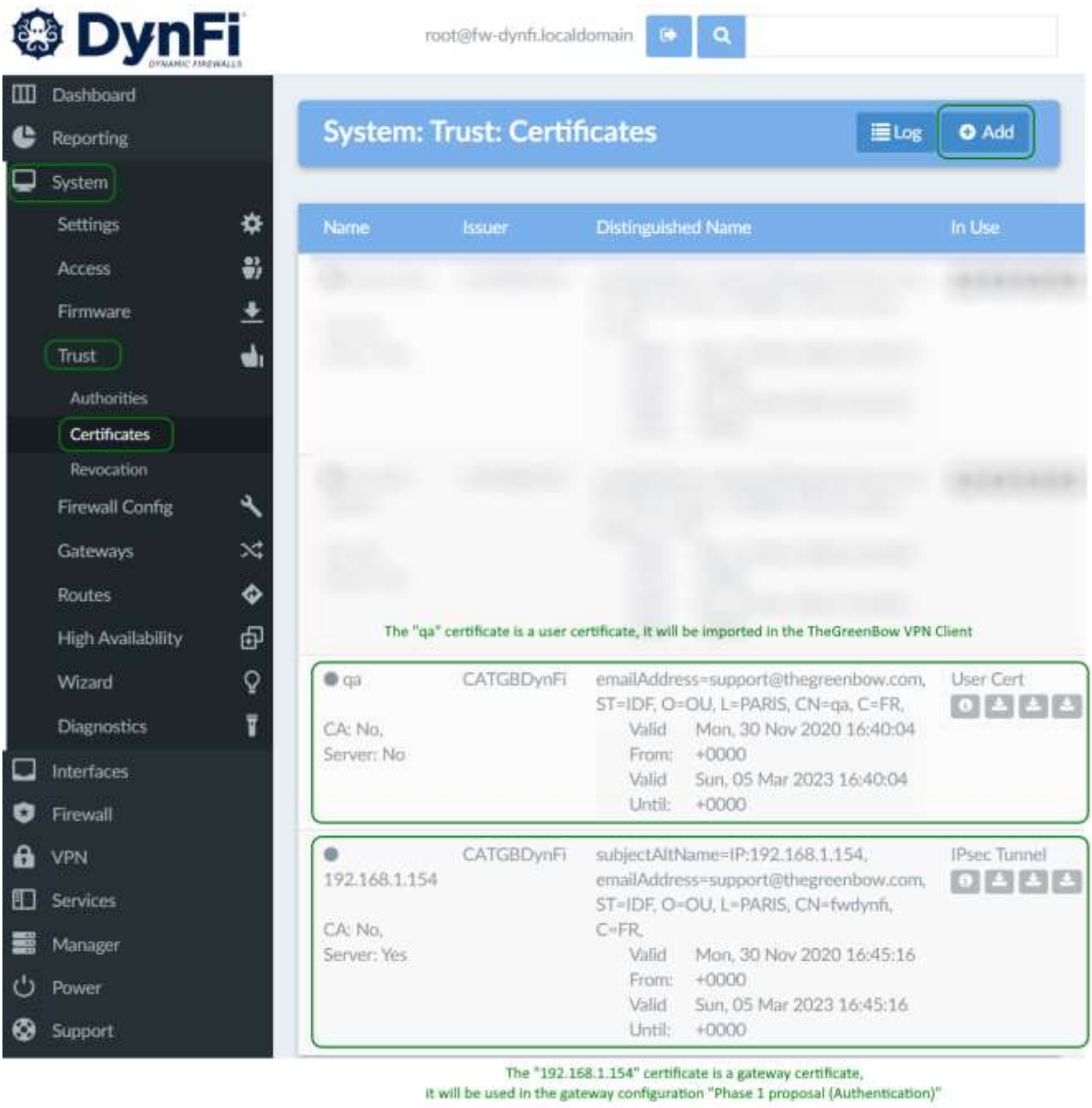
This section describes how to build an IPsec VPN configuration with your Dynfi router.

Once connected to your Dynfi gateway, if it is not already done, you need to import or create the Certification Authorities (CA). To do so, click on the “System > Trust > Authorities” menu then on the “Add” button.

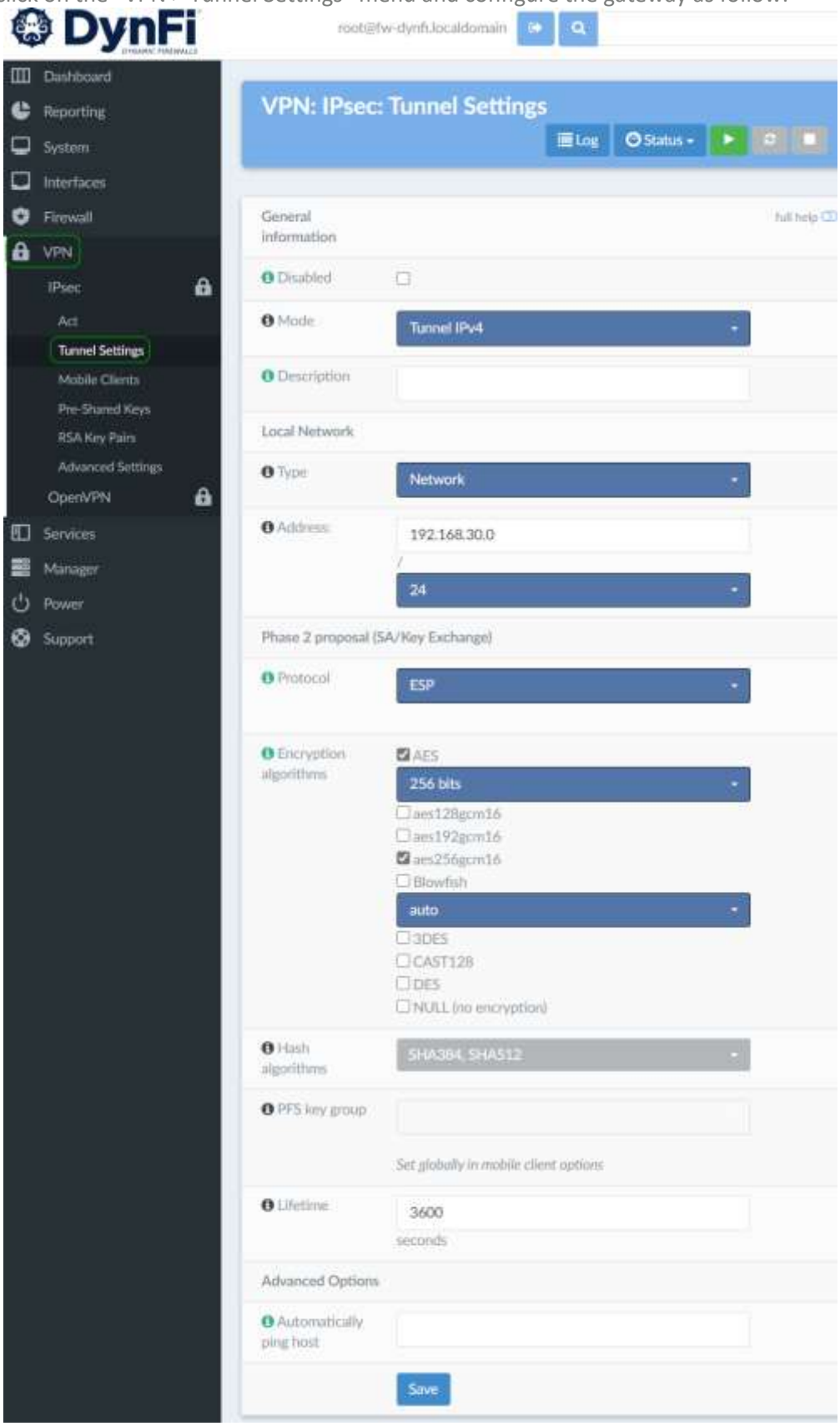


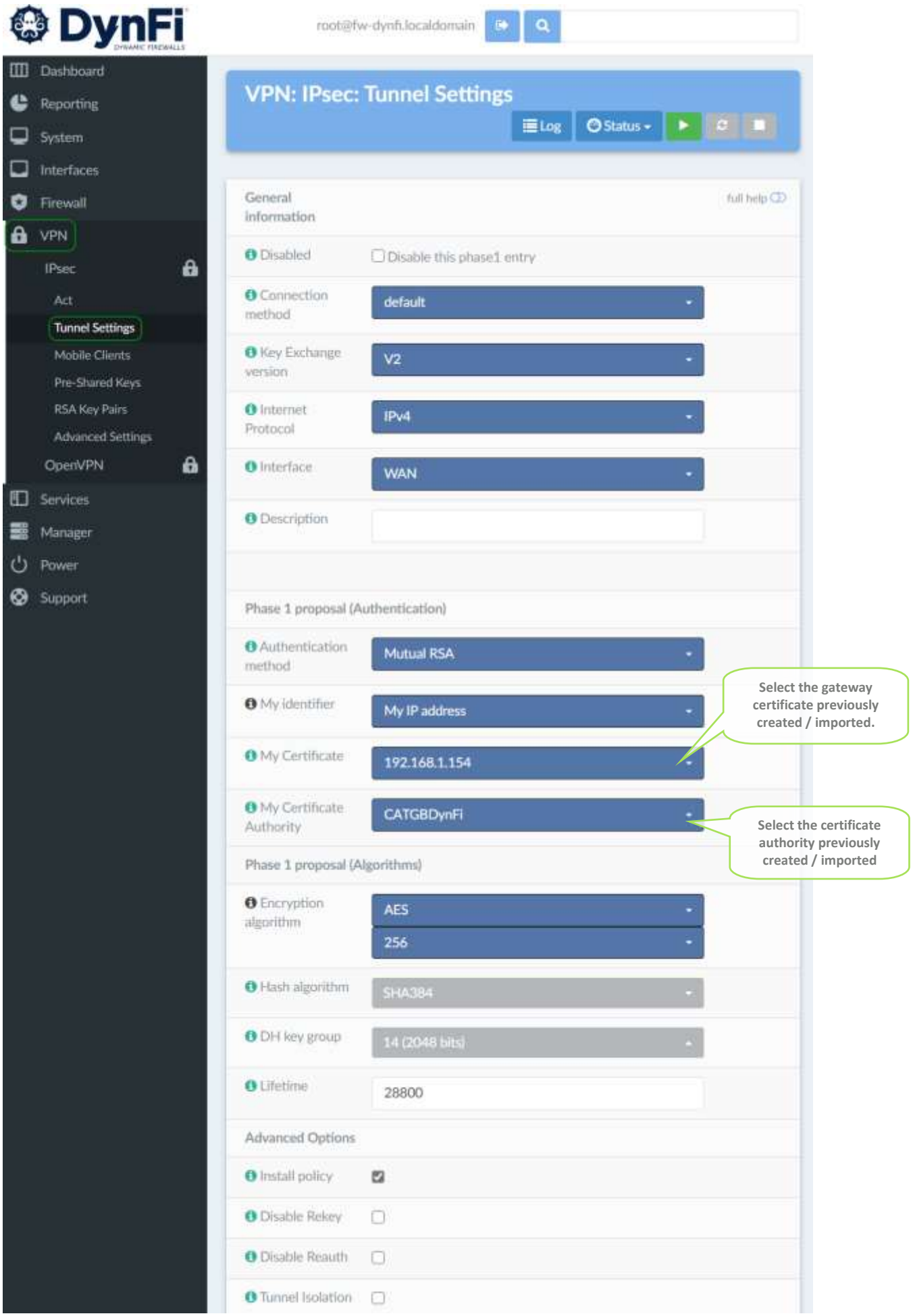
Now click on the “System > Trust > Authorities” menu to create or import the certificates. For our example, we will create / import 2 certificates :

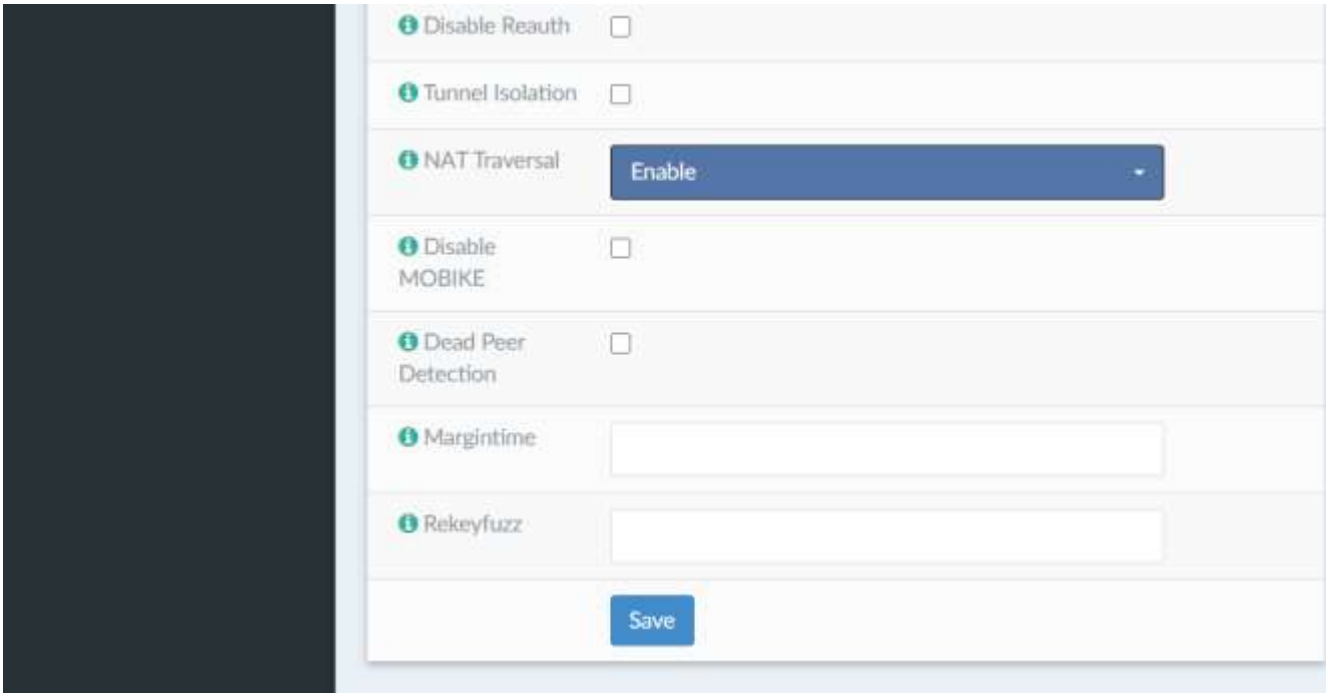
- The gateway certificate: 192.168.1.154.
- The user certificate: qa.



You need to click on the “VPN > Tunnel Settings” menu and configure the gateway as follow:

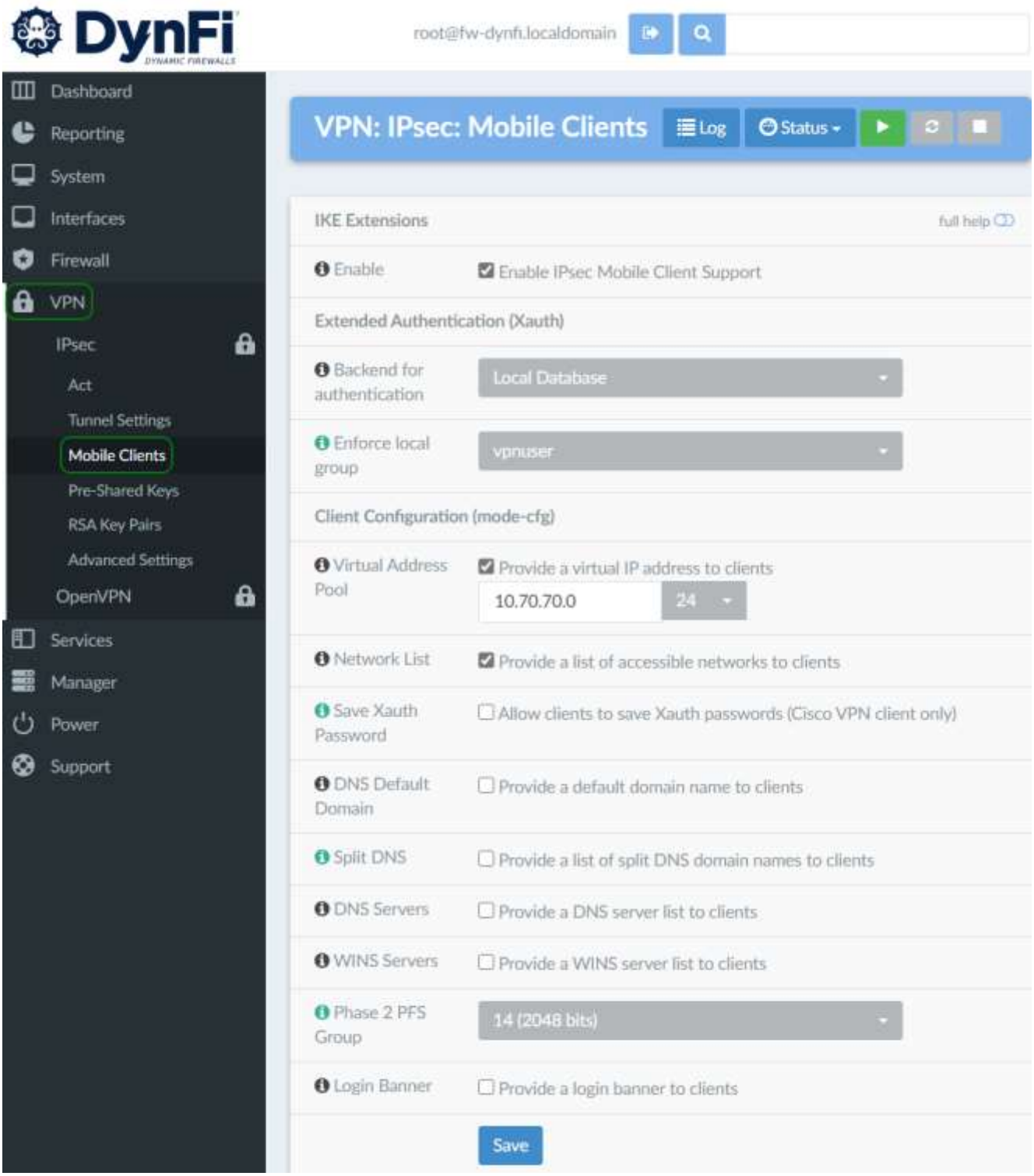






Validate the configuration by clicking on the “Save” button.

Then click on the “Mobile Clients” menu

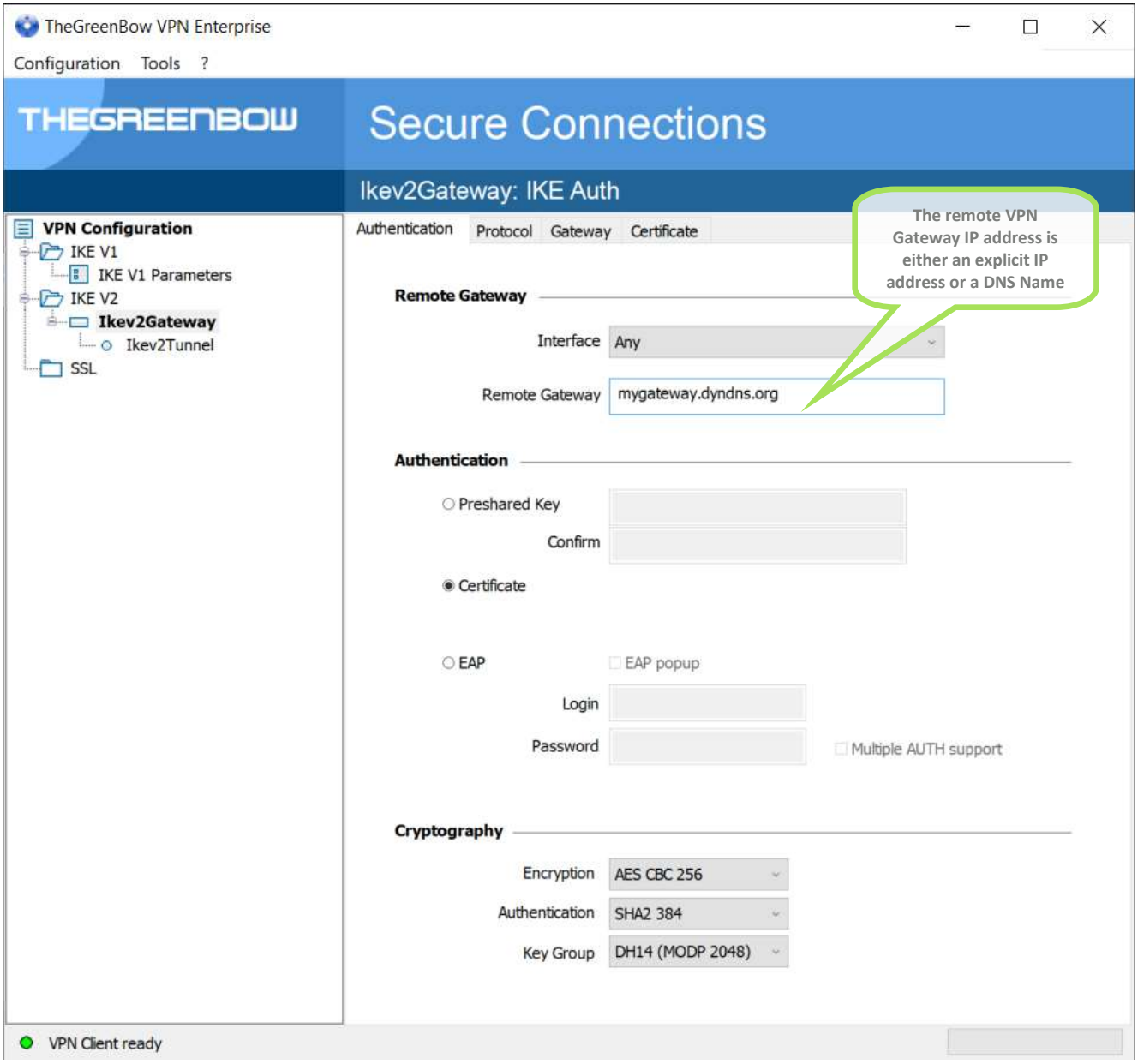


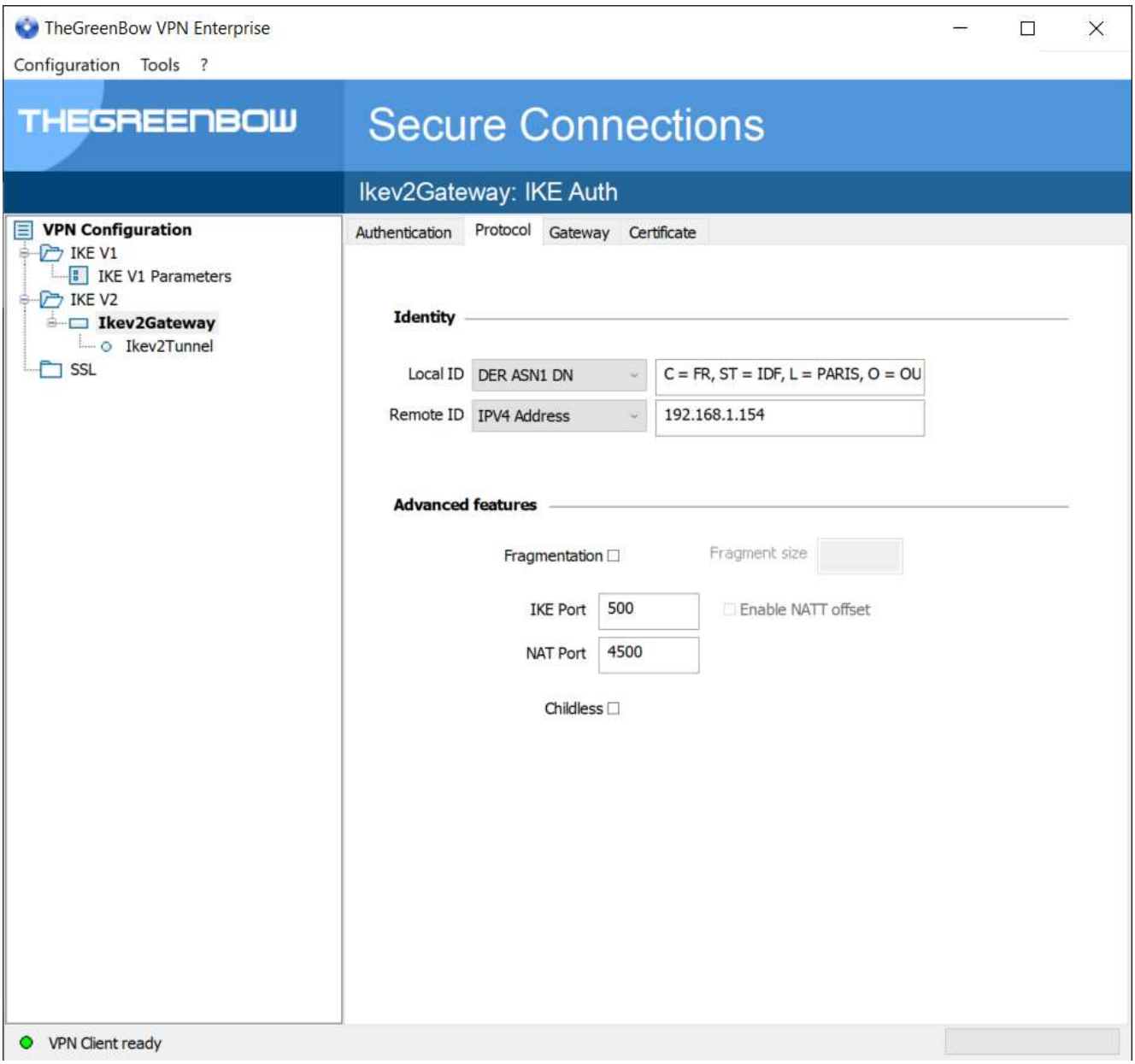
Validate the configuration by clicking on the “Save” button.

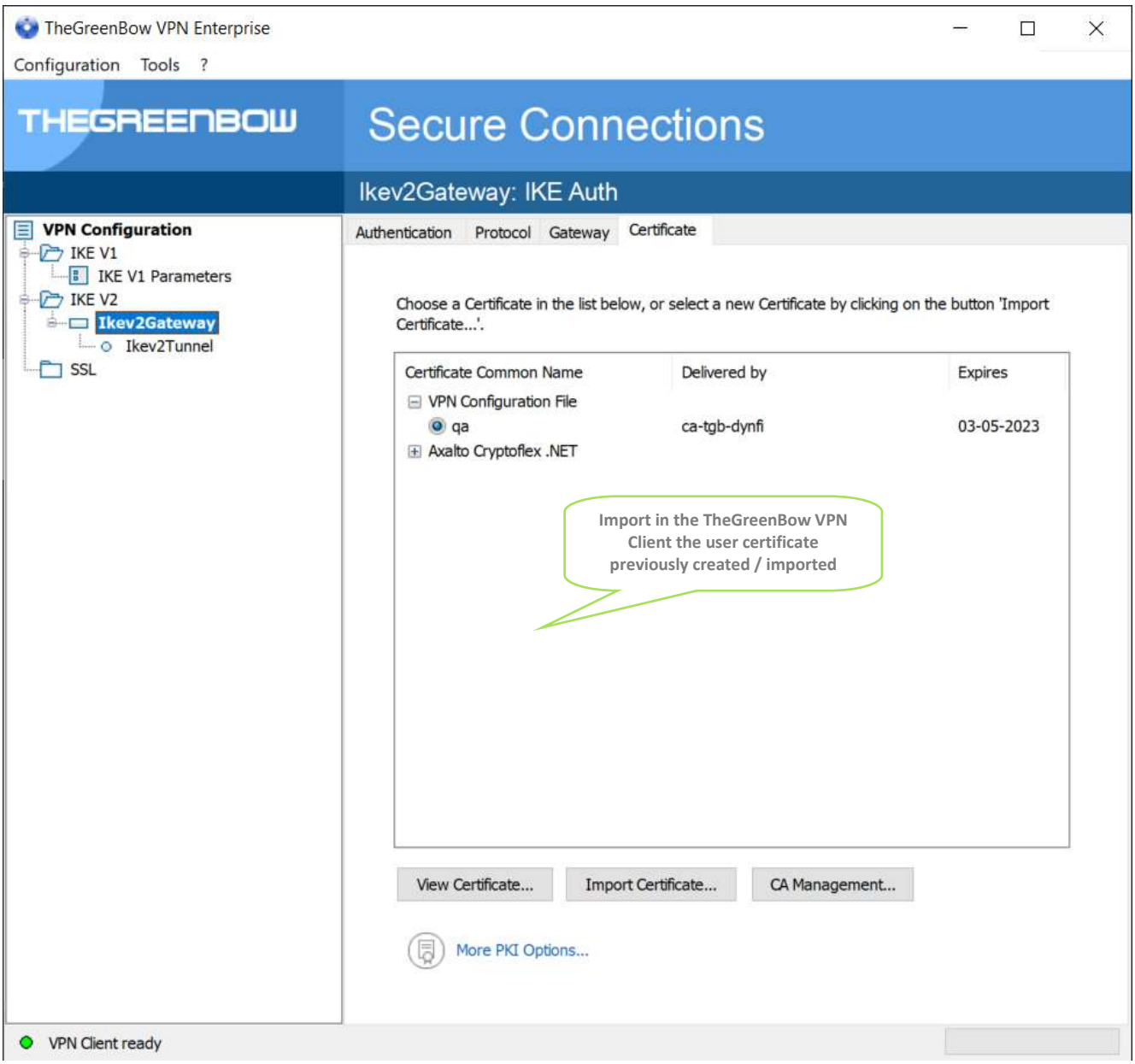
3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Dynfi router via VPN connections.
To download the latest release of TheGreenBow IPsec VPN Client software, please go to **http://www.thegreenbow.com/vpn_products.html**

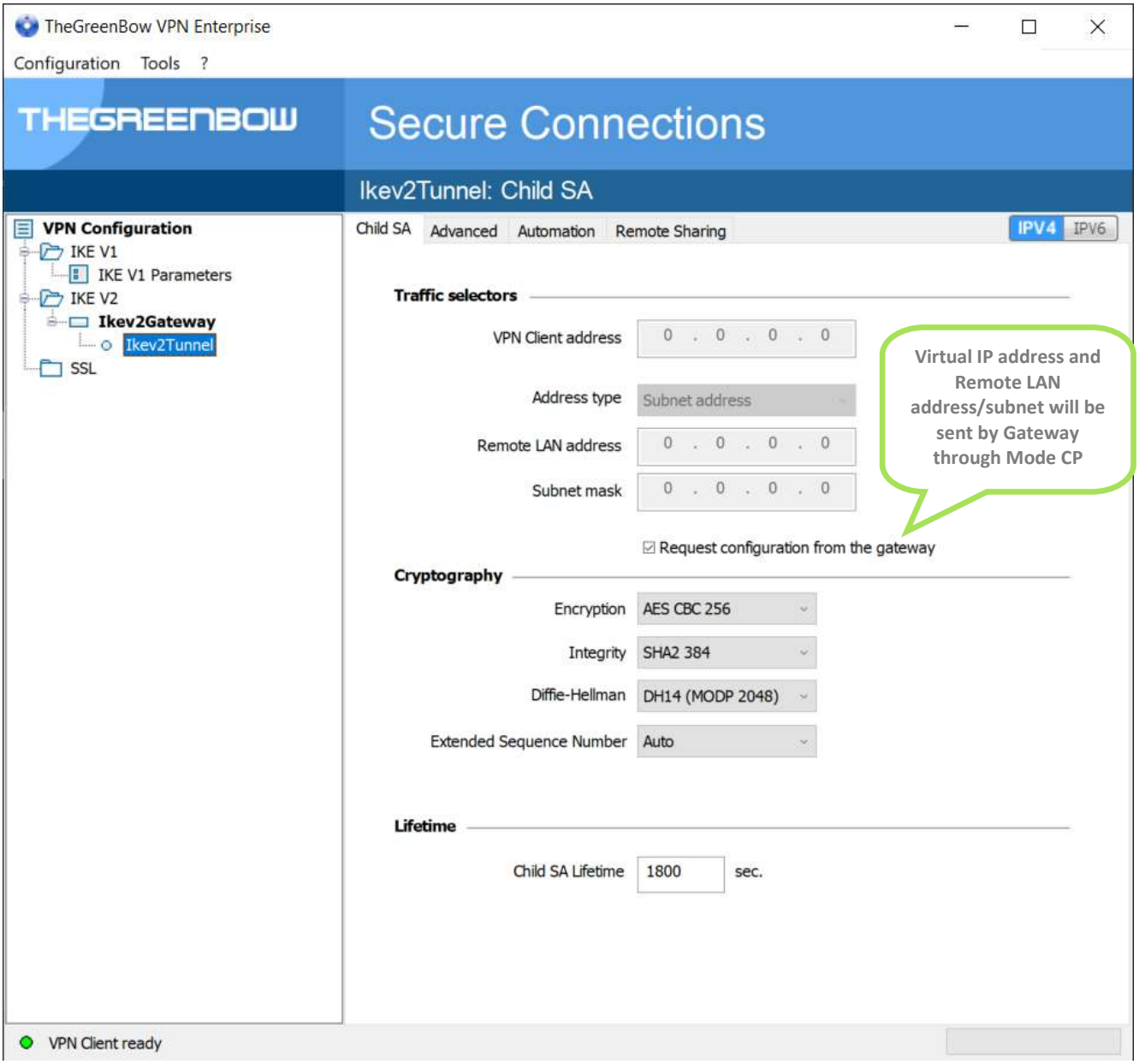
3.1 VPN Client - IKE Auth Configuration




TheGreenBow VPN Enterprise
Configuration
Tools
?
THEGREENBOW
Secure Connections
Ikev2Gateway: IKE Auth
VPN Configuration
IKE V1
IKE V1 Parameters
IKE V2
Ikev2Gateway
Ikev2Tunnel
SSL
Authentication
Protocol
Gateway
Certificate
Identity
Local ID
DER ASN1 DN
C = FR, ST = IDF, L = PARIS, O = OU
Remote ID
IPV4 Address
192.168.1.154
Advanced features
Fragmentation
Fragment size
IKE Port
500
Enable NATT offset
NAT Port
4500
Childless
VPN Client ready


TheGreenBow VPN Enterprise
Configuration
Tools
?
THEGREENBOW
Secure Connections
Ikev2Gateway: IKE Auth
VPN Configuration
IKE V1
IKE V1 Parameters
IKE V2
Ikev2Gateway
Ikev2Tunnel
SSL
Authentication
Protocol
Gateway
Certificate
Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'.
Certificate Common Name
Delivered by
Expires
VPN Configuration File
qa
ca-tgb-dynfi
03-05-2023
Axalto Cryptoflex .NET
Import in the TheGreenBow VPN Client the user certificate previously created / imported
View Certificate...
Import Certificate...
CA Management...
More PKI Options...
VPN Client ready

3.2 VPN Client Phase 2 (Child SA) Configuration



The configuration of the other tabs is left by default

3.3 Open IPsec VPN tunnels

Once both Dynfi router and TheGreenBow IPsec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPsec traffic.

1/ Select menu "**Configuration**" and "**Save**" to take into account all modifications we've made on your VPN Client configuration.

2/ Double Click on your Child SA tunnel name or Click "**Open**" button in Connection panel to open tunnel.

3/ Select menu "**Tools**" and "**Console**" if you want to access to the IPsec VPN logs. The following example shows a successful connection between TheGreenBow IPsec VPN Client and a Dynfi router.

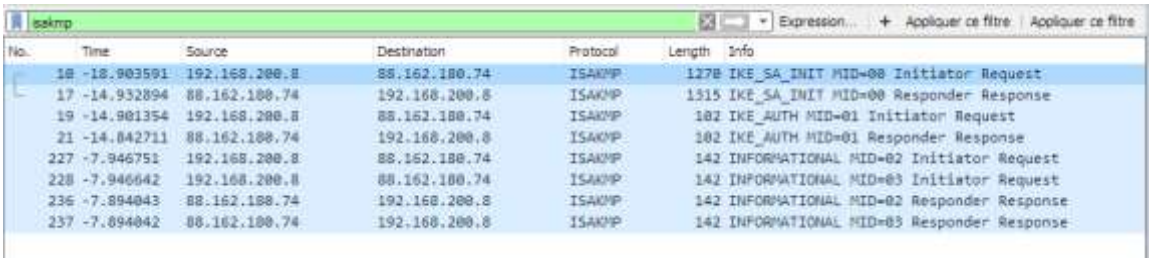
Sample log

4 Tools in case of trouble

Configuring an IPsec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: Wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website **www.wireshark.org**. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (**www.wireshark.org/docs/**).



5 VPN IPsec Troubleshooting

5.1 “NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)

```
20XX0913 16:08:53:387 TIKEV2_Tunnel SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE][VID][N(FR
AGMENTATION_SUPPORTED)]
20XX0913 16:08:53:419 TIKEV2_Tunnel RECV IKE_SA_INIT [HDR][N(NO_PROPOSAL_CHOSEN)]
```

If you have an “NO_PROPOSAL_CHOSEN” error you might have a wrong Phase 1 [IKE Auth], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 “AUTHENTICATION_FAILED” error

```
20XX0913 16:15:22:032 TIKEV2_Tunnel RECV IKE_AUTH [HDR][N(AUTHENTICATION_FAILED)]
20XX0913 16:15:22:032 TIKEV2_Tunnel Remote endpoint sends error AUTHENTICATION_FAILED
```

If you have an “AUTHENTICATION_FAILED” error, it means that the certificate or the Pre-shared key is not matching. Check the Gateway if the user certificate or Pre-shared key is valid.

5.3 “No user certificate available for the connection” error

```
20XX0913 16:18:07:491 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERTREQ][
N(FRAGMENTATION_SUPPORTED)][N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:18:07:491 TIKEV2_Tunnel IKE SA I-SPI 8D4467C52C91C316 R-SPI 9DF0F0E4A91F8867
20XX0913 16:18:07:491 TIKEV2_Tunnel No user certificate available for the connexion
20XX0913 16:18:07:491 TIKEV2_Tunnel Connection aborted.
```

Check if the certificate is selected or the Token (smartcard) is available on the computer.

5.4 “Remote ID rejected” error

```
20180913 16:24:32:087 TIKEV2_Tunnel ID types do not match. Expecting ID_RFC822_ADDR.
Receiving ID_DER_ASN1_DN
20180913 16:24:32:087 TIKEV2_Tunnel Remote IDr rejected
```

The “Remote ID” value (see “Protocol” tab) does not match what the remote endpoint is expected.

5.5 “NO_PROPOSAL_CHOSEN” error (wrong CHILD SA)

```
20XX0913            16:25:14:933            TIKEV2_Tunnel            SEND            IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE][N(FRAGMEN
TATION_SUPPORTED)]
20XX0913            16:25:15:118            TIKEV2_Tunnel            RECV            IKE_SA_INIT
[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERTREQ][
N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:25:15:118 TIKEV2_Tunnel IKE SA I-SPI E389FC49EE7078F1 R-SPI 00F37D557ED307FC
20XX0913            16:25:15:118            TIKEV2_Tunnel            SEND            IKE_AUTH
[HDR][IDi][CERT][CERTREQ][AUTH][CP][SA][TSi][TSr][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NOT
_SUPPORTED)]
20XX0913            16:25:15:165            TIKEV2_Tunnel            RECV            IKE_AUTH
[HDR][IDr][CERT][AUTH][CP][N(AUTH_LIFETIME)][N(NO_PROPOSAL_CHOSEN)]
20XX0913 16:25:15:165 TIKEV2_Tunnel IKE AUTH renewal in 1654 seconds (16:52:49)
20XX0913            16:25:15:165            TIKEV2_Tunnel            SEND            CHILD_SA
[HDR][SA][NONCE][KE][TSi][TSr][N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20XX0913 16:25:15:202 TIKEV2_Tunnel RECV CHILD_SA [HDR][N(NO_PROPOSAL_CHOSEN)]
20XX0913 16:25:15:202 TIKEV2_Tunnel Remote endpoint sends error NO_PROPOSAL_CHOSEN
20XX0913 16:25:15:202 TIKEV2_Tunnel SEND INFORMATIONAL [HDR][DELETE]
```

If you have an “NO_PROPOSAL_CHOSEN” error, check that the “Child SA” encryption algorithms are the same on each side of the VPN Tunnel.

5.6 “FAILED_CP_REQUIRED” error

```
20XX0913            16:29:46:780            TIKEV2_Tunnel            RECV            IKE_AUTH
[HDR][IDr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPTABLE)]
20180913 16:29:46:780 TIKEV2_Tunnel Remote endpoint sends error FAILED_CP_REQUIRED
20XX0913 16:29:46:780 TIKEV2_Tunnel Remote endpoint is expecting a configuration request
from the client
```

If you have an “FAILED_CP_REQUIRED” error, then the Gateway is configured to use Mode CP. Go to Traffic selectors and enable "Request configuration from the gateway".

5.7 I clicked on “Open tunnel”, but nothing happens.

```
20XX1003 11:08:34:031 [VPNCONF] TGBIKE_STARTED received
20XX1003            11:21:34:379            TIKEV2_vRHEL75            SEND            IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003            11:21:39:397            TIKEV2_vRHEL75            SEND            IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003            11:21:44:409            TIKEV2_vRHEL75            SEND            IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003 11:21:49:423 TIKEV2_vRHEL75 3 attempts with no response. Aborting connection.
```

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPsec Client uses UDP port 500.
Check if the remote server is online.

5.8 The VPN tunnel is up but I can't ping!

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Child SA settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP and if the protocol 50 is allowed to pass traffic in your firewalls.
- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark for example). You will have an indication that encryption works.
- Check the "default gateway" value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no "Default gateway" setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install Wireshark (**www.wireshark.org**) on one of your target computers. You can check that your pings arrive inside the LAN.

6 Contacts

News and updates on TheGreenBow web site: **www.thegreenbow.com**

Technical support by email at: **support@thegreenbow.com**

Sales contacts by email at: **sales@thegreenbow.com**

Secure, Strong, Simple

TheGreenBow Security Software