

TheGreenBow IPsec VPN Client

Configuration Guide

Dynfi

Protocol - IKEv2

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

Table of Contents

1	Introduction	3
1.1	Goal of this document.....	3
1.2	VPN Network topology	3
1.3	Dynfi Restrictions	3
1.4	Dynfi VPN Gateway	3
1.5	Dynfi VPN Gateway product info	3
2	Dynfi VPN configuration	4
3	TheGreenBow IPsec VPN Client configuration	10
3.1	VPN Client - IKE Auth Configuration	10
3.2	VPN Client Phase 2 (Child SA) Configuration	13
3.3	Open IPsec VPN tunnels.....	14
4	Tools in case of trouble.....	15
4.1	A good network analyser: Wireshark.....	15
5	VPN IPsec Troubleshooting.....	16
5.1	“NO_PROPOSAL_CHOSEN” error (wrong IKE Auth).....	16
5.2	“AUTHENTICATION_FAILED” error	16
5.3	“No user certificate available for the connection” error.....	16
5.4	“Remote ID rejected” error.....	16
5.5	“NO_PROPOSAL_CHOSEN” error (wrong CHILD SA).....	17
5.6	“FAILED_CP_REQUIRED” error.....	17
5.7	I clicked on “Open tunnel”, but nothing happens.	17
5.8	The VPN tunnel is up but I can’t ping!	18
6	Contacts	19

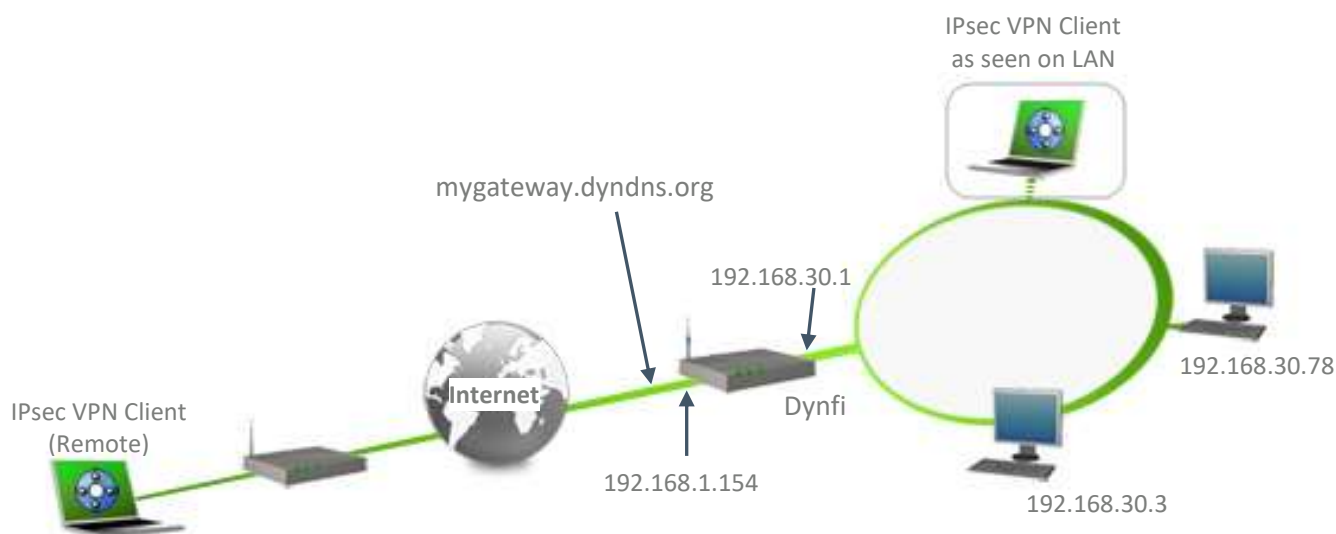
1 Introduction

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/>

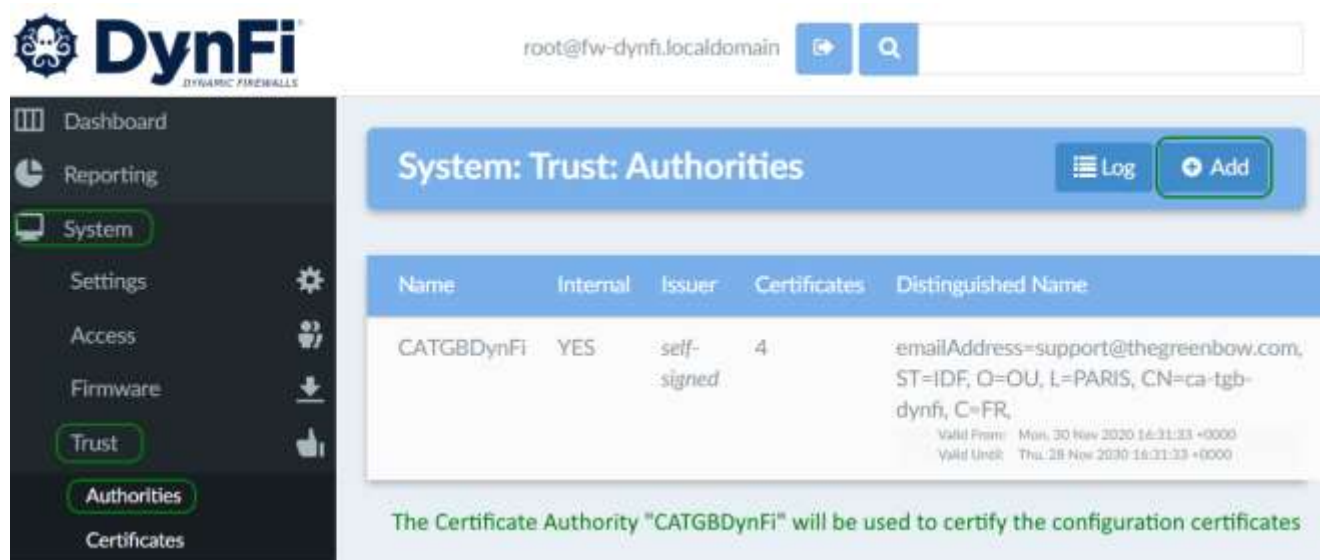
Dynfi Product page
Dynfi User Guide
Dynfi FAQ

<https://dynfi.com/>
<https://dynfi.com/documentation/>
<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.



The screenshot shows the DynFi web interface. The top left features the DynFi logo and a navigation menu with items: Dashboard, Reporting, System, Settings, Access, Firmware, Trust, Authorities, and Certificates. The top right shows the user 'root@fw-dynfi.localdomain' and a search bar. The main content area is titled 'System: Trust: Authorities' and includes a 'Log' button and an 'Add' button. Below this is a table with the following data:

Name	Internal	Issuer	Certificates	Distinguished Name
CATGBDynFi	YES	self-signed	4	emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=ca-tgb-dynfi, C=FR, Valid From: Mon, 30 Nov 2020 16:31:33 +0000 Valid Until: Thu, 28 Nov 2030 16:31:33 +0000

Below the table, a green message states: "The Certificate Authority "CATGBDynFi" will be used to certify the configuration certificates".

Configuration Guide

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.

The screenshot shows the DynFi web interface. The top navigation bar includes the DynFi logo, the user 'root@fw-dynfi.localdomain', and a search bar. The sidebar menu on the left has 'System' and 'Trust' highlighted, with 'Certificates' selected under 'Trust'. The main content area is titled 'System: Trust: Certificates' and features a table with the following data:

Name	Issuer	Distinguished Name	In Use
qa	CATGBDynFi	emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=qa, C=FR, CA: No, Server: No	User Cert
192.168.1.154	CATGBDynFi	subjectAltName=IP:192.168.1.154, emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=fwdynfi, C=FR, CA: No, Server: Yes	IPsec Tunnel

Below the table, there are two explanatory notes:



- The "qa" certificate is a user certificate, it will be imported in the TheGreenBow VPN Client
- The "192.168.1.154" certificate is a gateway certificate, it will be used in the gateway configuration "Phase 1 proposal (Authentication)"

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




The screenshot shows the DynFi web interface for configuring an IPsec VPN tunnel. The left sidebar contains a navigation menu with the following items: Dashboard, Reporting, System, Interfaces, Firewall, VPN (highlighted), IPsec (with a lock icon), Act, Tunnel Settings (highlighted), Mobile Clients, Pre-Shared Keys, RSA Key Pairs, Advanced Settings, OpenVPN (with a lock icon), Services, Manager, Power, and Support. The main content area is titled "VPN: IPsec: Tunnel Settings" and includes a "Log" button and a "Status" dropdown menu. The configuration is organized into several sections:

- General information:** Includes a "Disabled" checkbox (unchecked), a "Mode" dropdown set to "Tunnel IPv4", and a "Description" text input field.
- Local Network:** Includes a "Type" dropdown set to "Network", an "Address" text input field containing "192.168.30.0", and a "Subnet" dropdown set to "24".
- Phase 2 proposal (SA/Key Exchange):** Includes a "Protocol" dropdown set to "ESP".
- Encryption algorithms:** Includes a checked "AES" checkbox, a "256 bits" dropdown, and several other options: aes128gcm16, aes192gcm16, aes256gcm16 (checked), Blowfish, 3DES, CAST128, DES, and NULL (no encryption).
- Hash algorithms:** Includes a dropdown set to "SHA384, SHA512".
- PFS key group:** Includes an empty text input field and a note: "Set globally in mobile client options".
- Lifetime:** Includes a text input field set to "3600" with "seconds" indicated below it.
- Advanced Options:** Includes a checked "Automatically ping host" checkbox and an empty text input field.

A "Save" button is located at the bottom of the configuration form.

- Dashboard
- Reporting
- System
- Interfaces
- Firewall
- VPN**
 - IPsec 
 - Act
 - Tunnel Settings**
 - Mobile Clients
 - Pre-Shared Keys
 - RSA Key Pairs
 - Advanced Settings
 - OpenVPN 
- Services
- Manager
- Power
- Support

VPN: IPsec: Tunnel Settings

[Log](#) [Status](#)   

General information [full help](#)

Disabled Disable this phase1 entry

Connection method default

Key Exchange version V2

Internet Protocol IPv4

Interface WAN

Description

Phase 1 proposal (Authentication)

Authentication method Mutual RSA

My identifier My IP address

My Certificate 192.168.1.154

My Certificate Authority CATGBDynFi

Phase 1 proposal (Algorithms)

Encryption algorithm AES
256

Hash algorithm SHA384

DH key group 14 (2048 bits)

Lifetime 28800

Advanced Options

Install policy

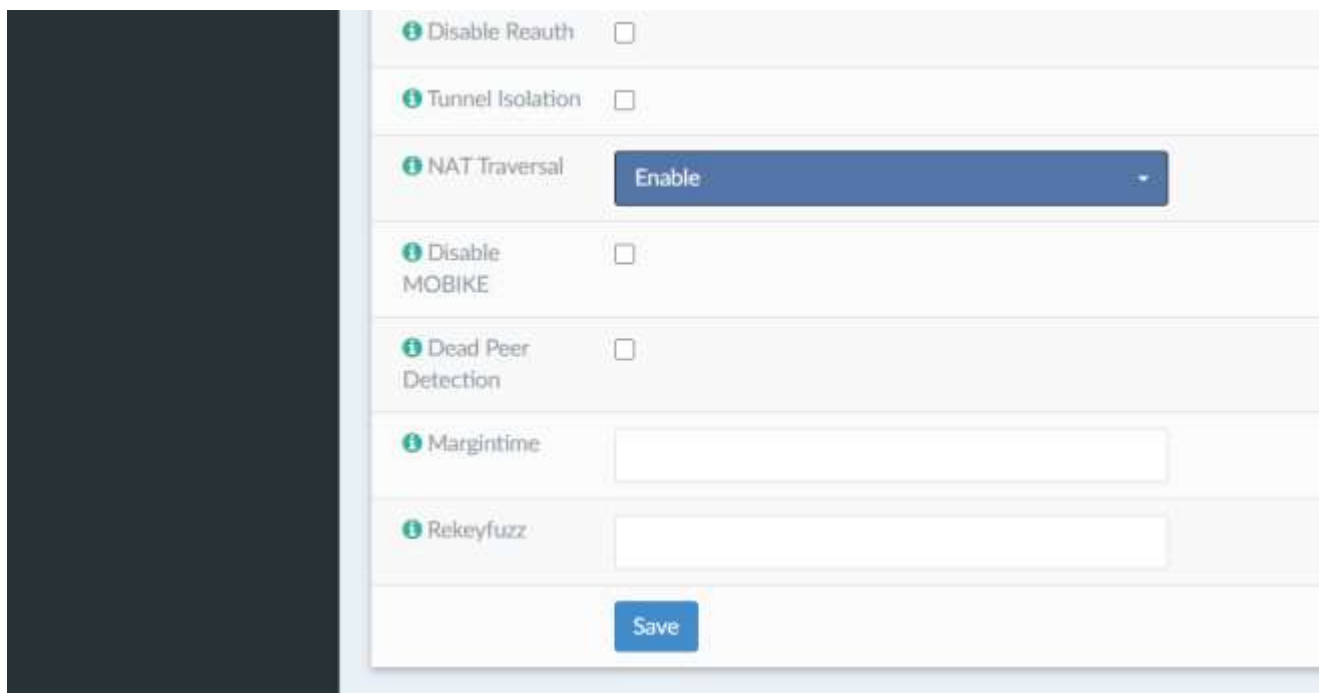
Disable Rekey

Disable Reauth

Tunnel Isolation

Select the gateway certificate previously created / imported.

Select the certificate authority previously created / imported



The screenshot shows a configuration panel with the following settings:

- Disable Reauth:
- Tunnel Isolation:
- NAT Traversal: Enable (dropdown menu)
- Disable MOBIKE:
- Dead Peer Detection:
- Margintime:
- Rekeyfuzz:

A blue "Save" button is located at the bottom of the configuration panel.

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

Configuration Guide

Then click on the “Mobile Clients” menu

The screenshot shows the DynFi web interface for configuring IPsec Mobile Clients. The left sidebar contains a navigation menu with the following items: Dashboard, Reporting, System, Interfaces, Firewall, VPN (highlighted), IPsec, Act, Tunnel Settings, Mobile Clients (highlighted), Pre-Shared Keys, RSA Key Pairs, Advanced Settings, OpenVPN, Services, Manager, Power, and Support. The main content area is titled "VPN: IPsec: Mobile Clients" and includes a "Log" button, a "Status" dropdown, and a play button. The configuration is organized into sections: "IKE Extensions" (with a "full help" link), "Extended Authentication (Xauth)", and "Client Configuration (mode-cfg)".

- IKE Extensions:** Enable IPsec Mobile Client Support
- Extended Authentication (Xauth):**
 - Backend for authentication: Local Database
 - Enforce local group: vpnuser
- Client Configuration (mode-cfg):**
 - Virtual Address Pool: Provide a virtual IP address to clients. Value: 10.70.70.0, 24.
 - Network List: Provide a list of accessible networks to clients.
 - Save Xauth Password: Allow clients to save Xauth passwords (Cisco VPN client only)
 - DNS Default Domain: Provide a default domain name to clients
 - Split DNS: Provide a list of split DNS domain names to clients
 - DNS Servers: Provide a DNS server list to clients
 - WINS Servers: Provide a WINS server list to clients
 - Phase 2 PFS Group: 14 (2048 bits)
 - Login Banner: Provide a login banner to clients

A "Save" button is located at the bottom of the configuration area.

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

The screenshot shows the 'TheGreenBow VPN Enterprise' configuration window. The main title is 'Secure Connections' and the sub-title is 'Ikev2Gateway: IKE Auth'. The interface is divided into a left sidebar and a main configuration area.

VPN Configuration Sidebar:

- IKE V1
 - IKE V1 Parameters
- IKE V2
 - Ikev2Gateway**
 - Ikev2Tunnel
- SSL

Main Configuration Area:

Authentication | Protocol | Gateway | Certificate

Remote Gateway

- Interface: Any
- Remote Gateway: mygateway.dyndns.org

Authentication

- Preshared Key
 - Confirm: [text input]
- Certificate
- EAP
 - EAP popup
 - Login: [text input]
 - Password: [text input]
 - Multiple AUTH support

Cryptography

- Encryption: AES CBC 256
- Authentication: SHA2 384
- Key Group: DH14 (MODP 2048)

VPN Client ready

Callout: A green callout box points to the 'Remote Gateway' field with the text: 'The remote VPN Gateway IP address is either an explicit IP address or a DNS Name'.

The screenshot shows the 'TheGreenBow VPN Enterprise' configuration window. The title bar includes 'Configuration Tools ?'. The main header is 'THEGREENBOW Secure Connections'. The current configuration is for 'Ikev2Gateway: IKE Auth'. The interface is divided into a left sidebar and a main configuration area.

VPN Configuration (Left Sidebar):

- IKE V1
 - IKE V1 Parameters
- IKE V2
 - Ikev2Gateway**
 - Ikev2Tunnel
- SSL

Main Configuration Area:

Authentication | Protocol | Gateway | Certificate

Identity

Local ID: DER ASN1 DN (dropdown) | C = FR, ST = IDF, L = PARIS, O = OU (text box)

Remote ID: IPV4 Address (dropdown) | 192.168.1.154 (text box)

Advanced features

Fragmentation | Fragment size [text box]

IKE Port: 500 (text box) | Enable NATT offset

NAT Port: 4500 (text box)

Childless

VPN Client ready (Status bar)

The screenshot shows the 'TheGreenBow VPN Enterprise' configuration window. The main title is 'Secure Connections' and the sub-title is 'Ikev2Gateway: IKE Auth'. The left sidebar shows a tree view under 'VPN Configuration' with folders for 'IKE V1', 'IKE V2', and 'SSL'. Under 'IKE V2', there is a folder 'Ikev2Gateway' containing 'Ikev2Tunnel'. The main area has tabs for 'Authentication', 'Protocol', 'Gateway', and 'Certificate'. The 'Certificate' tab is active, displaying a table of certificates and buttons for 'View Certificate...', 'Import Certificate...', and 'CA Management...'. A green callout box highlights the 'qa' 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
<input type="checkbox"/> VPN Configuration File		
<input checked="" type="radio"/> qa	ca-tgb-dynfi	03-05-2023
<input type="checkbox"/> Axalto Cryptoflex .NET		

Import in the TheGreenBow VPN Client the user certificate previously created / imported

VPN Client ready

3.2 VPN Client Phase 2 (Child SA) Configuration

The screenshot shows the configuration window for 'Ikev2Tunnel: Child SA' in 'TheGreenBow VPN Enterprise'. The interface includes a left-hand navigation tree under 'VPN Configuration' with sub-items: IKE V1, IKE V1 Parameters, IKE V2, Ikev2Gateway, and SSL. The 'Ikev2Tunnel' item is selected. The main configuration area has tabs for 'Child SA', 'Advanced', 'Automation', and 'Remote Sharing', with 'IPV4' and 'IPV6' options. The 'Traffic selectors' section contains fields for 'VPN Client address' (0 . 0 . 0 . 0), 'Address type' (Subnet address), 'Remote LAN address' (0 . 0 . 0 . 0), and 'Subnet mask' (0 . 0 . 0 . 0). A checkbox 'Request configuration from the gateway' is checked. The 'Cryptography' section includes 'Encryption' (AES CBC 256), 'Integrity' (SHA2 384), 'Diffie-Hellman' (DH14 (MODP 2048)), and 'Extended Sequence Number' (Auto). The 'Lifetime' section shows 'Child SA Lifetime' set to 1800 sec. A green callout bubble points to the address fields with the text: 'Virtual IP address and Remote LAN address/subnet will be sent by Gateway through Mode CP'. At the bottom left, a green dot indicates 'VPN Client ready'.

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.



```
VPN Console ACTIVE
Save Stop Clear Reset IKE
20200805 14:32:59:722 T3KEV2_ikev2Gateway SEND IKE_SA_INIT [HDR][SA][NONCE][NAT_DETECTION_SOURCE_IP][NAT_DETECTION_DESTINATION_IP][KE
20200805 14:32:59:737 T3KEV2_ikev2Gateway RECV IKE_SA_INIT [HDR][INVALID_IKE_PAYLOAD]
20200805 14:32:59:737 T3KEV2_ikev2Gateway SEND IKE_SA_INIT [HDR][SA][NONCE][NAT_DETECTION_SOURCE_IP][NAT_DETECTION_DESTINATION_IP][KE
20200805 14:32:59:839 T3KEV2_ikev2Gateway RECV IKE_SA_INIT [HDR][SA][NONCE][NAT_DETECTION_SOURCE_IP][NAT_DETECTION_DESTINATION_IP][N[HTTP_CERT_LOOKUP_SUPPORTED]][CERTREQ][VID][VID]
20200805 14:32:59:853 T3KEV2_ikev2Gateway IKE SA 1 SPI 927CF12E1519EBA3 R SPI 92EFAD547F9F7A30
20200805 14:32:59:853 T3KEV2_ikev2Gateway SEND IKE_AUTH [HDR][ID][AUTH][CP][SA][TS][TS][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20200805 14:32:59:972 T3KEV2_ikev2Gateway RECV IKE_AUTH [HDR][ID][AUTH][CP][SA][TS][TS][N(ESP_TFC_PADDING_NOT_SUPPORTED)][N(NON_FIRST_FRAGMENTS_ALSO)]
20200805 14:32:59:984 T3KEV2_ikev2Gateway Outbound SPI CAP94472 192.168.2.9/255.255.255.255 => 192.168.1.0/255.255.255.0
20200805 14:32:59:984 T3KEV2_ikev2Gateway Inbound SPI F0252D40 192.168.1.0/255.255.255.0 => 192.168.2.9/255.255.255.0
20200805 14:33:00:006 T3KEV2_ikev2Gateway IKE CHILD renewal in 1566 seconds (14:59:06)
20200805 14:33:00:006 T3KEV2_ikev2Gateway IKE AUTH renewal in 1702 seconds (15:01:22)
20200805 14:33:00:006 T3KEV2_ikev2Gateway [VirtualTf] Virtual interface properly configured for instance 1 and TfIndex 13
Current line: 12 Max. lines: 10000
```

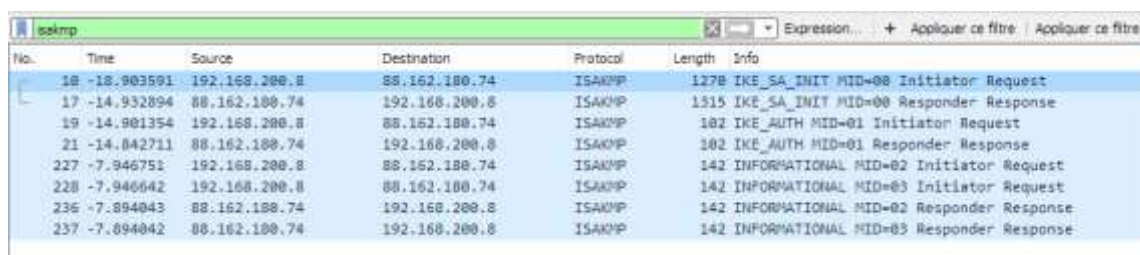
Sample log

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/).



No.	Time	Source	Destination	Protocol	Length	Info
16	-18.903591	192.168.200.8	88.162.100.74	ISAKMP	127B	IKE_SA_INIT MID=00 Initiator Request
17	-14.932894	88.162.100.74	192.168.200.8	ISAKMP	1315	IKE_SA_INIT MID=00 Responder Response
19	-14.981354	192.168.200.8	88.162.100.74	ISAKMP	102	IKE_AUTH MID=01 Initiator Request
21	-14.042711	88.162.100.74	192.168.200.8	ISAKMP	102	IKE_AUTH MID=01 Responder Response
227	-7.946751	192.168.200.8	88.162.100.74	ISAKMP	142	INFORMATIONAL MID=02 Initiator Request
228	-7.946642	192.168.200.8	88.162.100.74	ISAKMP	142	INFORMATIONAL MID=03 Initiator Request
236	-7.894043	88.162.100.74	192.168.200.8	ISAKMP	142	INFORMATIONAL MID=02 Responder Response
237	-7.894042	88.162.100.74	192.168.200.8	ISAKMP	142	INFORMATIONAL MID=03 Responder Response

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(FRAGMENTATION_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(FRAGMENTATION_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