# Table of Contents

1 Introduction ............................................................................................................................................ 3  
1.1 Goal of this document.................................................................................................................... 3  
1.2 VPN Network topology ................................................................................................................ 3  
1.3 Palo Alto Restrictions .................................................................................................................. 3  
1.4 Palo Alto VPN Gateway ............................................................................................................... 3  
1.5 Palo Alto VPN Gateway product info .......................................................................................... 3  
2 Palo Alto VPN configuration ............................................................................................................... 4  
3 TheGreenBow IPsec VPN Client configuration ..................................................................................... 6  
3.1 VPN Client - IKE Auth Configuration .......................................................................................... 6  
3.2 VPN Client Child SA Configuration ............................................................................................ 8  
3.3 Open IPsec VPN tunnels ............................................................................................................. 9  
4 Tools in case of trouble ......................................................................................................................... 10  
4.1 A good network analyser: Wireshark ....................................................................................... 10  
5 VPN IPsec Troubleshooting .................................................................................................................. 11  
5.1 “NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)................................................................. 11  
5.2 “AUTHENTICATION_FAILED” error ....................................................................................... 11  
5.3 “No user certificate available for the connexion” error ............................................................. 11  
5.4 “Remote ID rejected” error ....................................................................................................... 11  
5.5 “NO_PROPOSAL_CHOSEN” error (wrong CHILD SA) ............................................................ 11  
5.6 “FAILED_CP_REQUIRED” error ............................................................................................... 12  
5.7 I clicked on “Open tunnel”, but nothing happens ................................................................. 12  
5.8 The VPN tunnel is up but I can’t ping ! ................................................................................... 12  
6 Contacts ................................................................................................................................................ 13
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a Palo Alto 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 Palo Alto 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 Palo Alto Restrictions

No known restrictions

1.4 Palo Alto VPN Gateway

Our tests and VPN configuration have been conducted with Palo Alto version 7.

1.5 Palo Alto VPN Gateway product info

It is critical that users find all necessary information about Palo Alto VPN Gateway. All product info, User Guide and knowledge base for the Palo Alto VPN Gateway can be found on the Palo Alto website: https://www.paloaltonetworks.com

<table>
<thead>
<tr>
<th>Palo Alto Product page</th>
<th><a href="https://www.paloaltonetworks.com/products">https://www.paloaltonetworks.com/products</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Palo Alto FAQ/Knowledge Base</td>
<td><a href="https://www.paloaltonetworks.com/resources/faq/">https://www.paloaltonetworks.com/resources/faq/</a></td>
</tr>
</tbody>
</table>
2 Palo Alto VPN configuration

This section describes how to build an IPsec VPN configuration with your Palo Alto VPN router. Once connected to your Palo Alto VPN gateway, select “Network” > “IKE Gateways” > “General” tab.

Create a Gateway configuration

- "Local Certificate" Select the Gateway Certificate generated in Palo Alto.
- "Local Identification" Select the subject of Gateway certificate.
- "Peer Identification" Select the subject of Client’s certificate.

Note: Version selected here is "IKEV2 only mode". For IKEV1, it is possible to select IKEv1 here, but matching configuration needs to be created in VPN Client under IKEv1.
Click on "Advanced Options" and set as indicated.

Click on "IPSec Tunnels" > "General" tab. Select the Gateway name "Cert" configured in previous step in "IKE Gateway".

Set the Proxy IDs tab with networks to be reached by VPN Client.
3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Palo Alto VPN router via VPN connections. To download the latest release of TheGreenBow IPsec VPN Client software, please go to www.thegreenbow.com/vpn_down.html.

3.1 VPN Client - IKE Auth Configuration

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Palo Alto router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.
Certificate configuration

Import the Client certificate generated in Palo Alto.
3.2 VPN Client Child SA Configuration
3.3 Open IPsec VPN tunnels

Once both Palo Alto 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 Palo Alto VPN router.
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](http://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/](http://www.wireshark.org/docs/)).
5  VPN IPsec Troubleshooting

5.1 “NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)

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

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

5.3 “No user certificate available for the connexion” error

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

5.4 “Remote ID rejected” error

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)
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

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.

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 computer. You can check that your pings arrive inside the LAN.
6  Contacts

News and updates on TheGreenBow website:  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