TheGreenBow IPSec VPN Client
Configuration Guide

Digital China
Unified Threat Management
DCFW-1800E-UTM

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com

Configuration Guide written by:
Writer: TheGreenBow TechSupport Team
Company: www.thegreenbow.com
Table of contents

1 Introduction .................................................................................................................................................... 3
  1.1 Goal of this document ............................................................................................................................ 3
  1.2 VPN Network topology ........................................................................................................................... 3
  1.3 Digital China DCFW 1800E UTM Restrictions ....................................................................................... 3
  1.4 Digital China DCFW 1800E UTM VPN Gateway ................................................................................... 3
  1.5 Digital China DCFW 1800E UTM VPN Gateway product info ........................................................... 3

2 Digital China DCFW 1800E UTM VPN configuration ..................................................................................... 4
  2.1 Add a Security Gateway to the DCFW 1800E UTM ............................................................................... 4
  2.2 Add a IPSec VPN Tunnel to the DCFW 1800E UTM ............................................................................. 5

3 TheGreenBow IPSec VPN Client configuration ............................................................................................. 8
  3.1 VPN Client Phase 1 (IKE) Configuration ................................................................................................ 8
  3.2 VPN Client Phase 2 (IPSec) Configuration ............................................................................................ 9
  3.3 Open IPSec VPN tunnels ....................................................................................................................... 9

4 Tools in case of trouble ................................................................................................................................ 11
  4.1 A good network analyser: Wireshark ............................................................................................ ....... 11

5 VPN IPSec Troubleshooting .................................................................................................. ................... 12
  5.1 "PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) ................................................................. 12
  5.2 « INVALID COOKIE » error .................................................................................................................. 12
  5.3 « no keystate » error ............................................................................................................................ 12
  5.4 « received remote ID other than expected » error ................................................................................ 12
  5.5 « NO PROPOSAL CHosen » error .................................................................................................... 13
  5.6 « INVALID ID INFORMATION » error .................................................................................................. 13
  5.7 I clicked on “Open tunnel”, but nothing happens ................................................................................. 13
  5.8 The VPN tunnel is up but I can’t ping ! ................................................................................................. 13

6 Contacts....................................................................................................................................................... 15
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client software with a Digital China DCFW 1800E UTM VPN router.

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 Digital China DCFW 1800E UTM 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 Digital China DCFW 1800E UTM Restrictions

No known restrictions.

1.4 Digital China DCFW 1800E UTM VPN Gateway

Our tests and VPN configuration have been conducted with Digital China DCFW 1800E UTM firmware release 8.0.4.016017.

1.5 Digital China DCFW 1800E UTM VPN Gateway product info


<table>
<thead>
<tr>
<th>Digital China DCFW 1800E UTM Product page</th>
<th>Digital China DCFW 1800E UTM Upgrade</th>
</tr>
</thead>
</table>
2 Digital China DCFW 1800E UTM VPN configuration

This section describes how to build an IPSec VPN configuration with your Digital China DCFW 1800E UTM VPN router.

2.1 Add a Security Gateway to the DCFW 1800E UTM

Once connected to your Digital China DCFW 1800E UTM VPN gateway, navigate to ‘VPN’ > ‘IPSec’ > ‘Security Gateway’. Click on ‘Add’ to add a security gateway.

Select ‘Mobile Host’, as we use dynamic VPN. Outgoing Interface is WAN interface of the DCFW 1800E UTM router.

Fill in Preshared Key in the field ‘Key’.

If you would like to configure IKE Phase 1 algorithm Proposals, you can configure it in ‘VPN’ > ‘IPSec’ > ‘IKE Proposal’ > ‘Phase 1 Proposal’ tab. Then here you can choose “User Defined” and select the particular proposal. But here, we’ve chosen ‘Compatible’.

Once you configured, press ‘Submit’ to save.
2.2 Add a IPSec VPN Tunnel to the DCFW 1800E UTM

Navigate to ‘VPN’ > ‘IPSec’ > ‘Auto Key Tunnel’. Click on ‘Add’ to add an Auto Key Tunnel.

In Security Gateway, select ‘VPNGW01’ (which we created earlier).

If you would like to configure IKE Phase 2 algorithm Proposals, you can configure it in ‘VPN’ > ‘IPSec’ > ‘IKE Proposal’ > ‘Phase 2 Proposal’ tab. Then, here you can choose “User Defined” and select the particular proposal. But here, we’ve chosen ‘Compatible PFS On’.

Once you configured, press ‘Submit’ to save.
Navigate to VPN > IPSec > IPSec Channel. Click on Add to add an IPSec Channel.

Local Subnet/Mask is the LAN subnet to reach by VPN Client computer. In Gateway tunnel, select “VPNTUN01”. Peer IP/Mask is the VPN Client IP address inside tunnel.

Navigate to ‘VPN’ > ‘IPSec’ > ‘NAT-Traversal’. Select the option to enable NAT-Traversal and press ‘Submit’ to save.
To save and apply the configuration changes, click on ‘Disk’ icon.

Click on ‘Submit’ to apply changes.
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Digital China DCFW 1800E UTM VPN router.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Configuration

![Phase 1 configuration](image)

You may use either Preshared, Certificates with the Digital China DCFW 1800E UTM router. This configuration is one example of can be accomplished in term of User Authentication. You may want to refer to either the Digital China DCFW 1800E UTM router user guide or TheGreenBow IPSec VPN Client User Guide for more details on User Authentication options.
### 3.2 VPN Client Phase 2 (IPSec) Configuration

![VPN Client Phase 2 Configuration](image)

#### Phase 2 Configuration

#### 3.3 Open IPSec VPN tunnels

Once both Digital China DCFW 1800E UTM 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. Click on "Save & Apply" to take into account all modifications we've made on your VPN Client configuration.
2. Click on "Open Tunnel", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser).
3. Select "Connections" to see opened VPN Tunnels.
4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Digital China DCFW 1800E UTM VPN router.
20090630 14525 Default (SA Gateway2-F1) SEND phase 1 Main Mode [SA][MD][MD][MD][MD]
20090630 14525 Default (SA Gateway2-F1) PECV phase 1 Main Mode [SA][MD][MD]
20090630 14525 Default (SA Gateway2-F1) SEND phase 1 Main Mode [KEY_EXCH][NONCE][NAT_D][NAT_D]
20090630 14525 Default (SA Gateway2-F1) PECV phase 1 Main Mode [KEY_EXCH][NONCE][NAT_D][NAT_D]
20090630 14525 Default (SA Gateway2-F1) SEND phase 1 Main Mode [HASP][ID][NOTIFY]
20090630 14525 Default (SA Gateway2-F1) PECV phase 1 Main Mode [HASP][ID]
20090630 14525 Default phase 1 done initiator d1.163.205.151, responder d1.168.162.151. responder d1.168.162.151.
20090630 14525 Default (SA Gateway2-Tunnel3-P2) SEND phase 2 Quick Mode [HASP][SA][KEY_EXCH][NONCE][ID][ID]
20090630 14527 Default (SA Gateway2-Tunnel3-P2) PECV phase 2 Quick Mode [HASP][SA][KEY_EXCH][NONCE][ID][ID]
20090630 14527 Default (SA Gateway2-Tunnel3-P2) SEND phase 2 Quick Mode [HASP]
20090630 14555 Default (SA Gateway2-P1) SEND Internal [HASP][NOTIFY] type DPD_R_U THERE
20090630 14555 Default (SA Gateway2-P1) PECV Internal [HASP][NOTIFY] type DPD_R_U THERE_ACK.
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 http://www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (http://www.wireshark.org/docs/).
5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 « INVALID COOKIE » error

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 « no keystate » error

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

5.4 « received remote ID other than expected » error

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
5.5 « NO PROPOSAL CHOSEN » error

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

5.6 « INVALID ID INFORMATION » error

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

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 and protocol ESP (protocol 50).

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 Phase 2 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
• 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 (http://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 web site: [http://www.thegreenbow.com](http://www.thegreenbow.com)

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com