D-Link And TheGreenBow Solution

DFL-800
Netdefend IPS/UTM Firewall
Application Note

Version 2.01
(2009-10-24)
1. Introduction
The objective of this document is to provide a guide describing how to configure the devices to achieve the same environment as shown at the network topology.

Users of this document are expected to already possess basic knowledge of D-Link devices and TheGreenBow VPN software, and are familiar with how to perform basic configurations. Only important configurations, such as those pertaining to interfacing and integrating, will be described in this document.

For purpose of reference, configuration files for each device are available for download.

2. Audience
This document is intended for project engineers or end users that need to implement DFL series and TheGreenBow software at the sites.

3. Objective
This topology consists of the scenarios that integrate using TheGreenBow VPN program and D-Link Firewall and demonstrate integrations and network solutions to OBUs, and in addition, to Partners and Customers from D-Link International.
4. List of Equipment and Software
The table below shows the devices information.

<table>
<thead>
<tr>
<th>Device No.</th>
<th>Device Name</th>
<th>Device Model</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TheGreenBow VPN Client Software</td>
<td></td>
<td>4.61.003</td>
</tr>
<tr>
<td>2</td>
<td>Netdefend IPS Firewall DFL-800</td>
<td>DFL-800</td>
<td>2.26.0.06-12649</td>
</tr>
<tr>
<td>3</td>
<td>WinRadius Radius Server</td>
<td></td>
<td>4.00</td>
</tr>
</tbody>
</table>

5. Network Diagram

![Network Diagram]

*Note: Router is set to allow IPSec pass through.*

6. Configurations
In this document, we will only describe the main configurations for this Scenario. The configurations setting for all the D-Link products will not be described here and for more detail about the product you can download their user guide.

1) TheGreenBow VPN Client (IPSec) and D-Link Security Solutions (VPN Client → DFL-800)

2) TheGreenBow VPN Client (XAuth) and D-Link Security Solutions (VPN Client → DFL-800 → Radius Server)
6.1 TheGreenBow VPN Client (IPSec) and D-Link Security Solutions (VPN Client → DFL-800)

In this scenario the user can connect back to the headquarter database by using TheGreenBow VPN Client connection to DFL-800.

All configurations are based on DFL-800 (F/W: 2.26.00.06-12649) and TheGreenBow VPN Client (F/W: 4.61.003)

The steps in this configuration are:

- Setup DFL-800 for VPN tunneling
  - Setup Pre-shared Key
  - Phase 1 and Phase 2 algorithms setup
  - Setting up IPSec-Tunnel
  - Setup IP Rules

- Setup TheGreenBow VPN Client software
  - Setup Phase 1
  - Setup Phase 2
6.1.1) Setup DFL-800 for VPN tunneling

6.1.1.1) Setup Pre-Shared Key

1) Login to the DFL-800 and click “Authenticate Objects” and add a new “Pre-shared Key” and fill in the passphrase and name.

6.1.1.2) Phase 1 and Phase 2 algorithms setup

1) At the “IKE Algorithms”, select the Encryption and Integrity algorithms for your phase 1 authenticate.
2) Next is the “IPSec Algorithms”, select the Encryption and Integrity algorithms for the Phase 2.

6.1.1.3) Setting up IPSec-Tunnel

1) After we finish setting up the algorithms, next we will need to create the “IPSec-Tunnel” as show below.
2) Next, click on the “Authentication” tab and select the “Pre-Shared Key” you have setup at the steps 1.

3) After selecting the Pre-Shared Key, next is to enable the “Dynamically add route” at the routing tab.

4) Last step is to make sure the DH Group at the IKE setting is the same setting for the TheGreenBow VPN Client software.
6.1.1.4) **Setup IP Rules**

Now is to setup the IP Rules so there the DFL-800 knows where to direct all the traffic to.

1) First add a new interface group name **"IPSec-LAN"** by grouping up **"IPSec-Tunnel"** and **"LAN"**.

2) Next, click **"IP Rules"** and add a new IP rule as show below.
6.1.2) Setup TheGreenBow VPN Client Software

6.1.2.1) Setup Phase 1

1) Right click on the "Root" to add a new "Phase1", next fill in the IP address for this VPN client and Remote gateway IP follow by Preshared Key and IKE setting.

Note: the Preshared Key and IKE must be the same setting set in the DFL-800.
6.1.2.2) Setup Phase 2

1) Right click on the “Phase1” to add a new “Phase2”, next fill in the VPN Client address for this VPN client and Remote gateway IP follow by ESP setting.

Note: the ESP Encryption and Authentication setting must be the same in the DFL-800 IPSec-Tunnel.
6.2 TheGreenBow VPN Client Software (X-Auth) and D-Link security solutions (VPN Client → DFL-800)

In this scenario the client will authenticate (X-Auth) before the user can connect back to the headquarter database by using TheGreenBow VPN Client connection to DFL-800 authenticate by External Authentication (Radius Server).

All configurations are based on DFL-800 (F/W: 2.26.00.06), TheGreenBow VPN Client (F/W: 4.61.003) and WinRadius (Version 4.00)

Note: Before configuration this solution, please make sure that your DFL-800 and VPN Client had the IPSec setting configured. Please refer to (6.1 - TheGreenBow VPN Client software (IPSec) and D-Link Security Solutions (VPN Client → DFL-800))

The steps in this configuration are:

- **Setup DFL-800 for X-Auth**
  - Enable the X-Auth in DFL-800
  - Setup the External Authentication Server

- **Setup TheGreenBow VPN Client software**
  - Enable the X-Auth Function

- **Setup WinRadius Server**
  - Set the Secret Key
6.2.1) Setup DFL-800 for X-Auth

6.2.1.1) Enable the X-Auth in DFL-800

1) At the “Interfaces → IPSec”, select the IPSec tunnel you have created in the previous solution and at the “XAuth” tab, enable the function as show below.

6.2.1.2) Setup the External Authentication Server (i.e. Radius)

1) Add the IP Address for the Radius Server in the “Address Book”.

![Image showing IPSec Tunnel configuration and Address Book entry for Radius server]
2) Select the “User Authentication → External User Database” and add a new “Radius Server” with the setting as show below.

\[ \text{Radius_server} \]

Note: the Shared Secret must be the same key in the Radius Server.

3) Next, add a New Rule in the “User Authentication Rules”.
4) At the “Authentication Options”, select the Radius Server you have created and select the Radius Method as “CHAP”.

5) Save and activate the setting.
6.2.2) Setup TheGreenBow VPN Client software

6.2.2.1) Enable the X-Auth Function

1) Inside the “P1 Advanced” menu, tick the box for the “X-Auth Popup”.

2) Click “Ok” and “Save &Apply” the setting.
6.2.3) Setup WinRadius Server

6.2.3.1) Set the Secret Key

1) Click the “System” from the “Setting” drop down list.

2) Key in the “NAS Secret”.

3) Click “OK”, close and start the WinRadius Server again.

Note: The NAS Secret must be the same key set in the DFL-800 “Shared Key”.
7. Interoperability Compliance Testing

7.1) **General Test Approach**

a. Open the VPN tunnel using different Negotiate Mode in phase 1 and phase 2:

<table>
<thead>
<tr>
<th>Series Negotiate Mode</th>
<th>Phase 1</th>
<th>Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-SHA</td>
<td>AES-SHA</td>
<td></td>
</tr>
<tr>
<td>AES-MD5</td>
<td>AES-SHA</td>
<td></td>
</tr>
<tr>
<td>3DES-MD5</td>
<td>AES-SHA</td>
<td></td>
</tr>
<tr>
<td>3DES-SHA</td>
<td>AES-SHA</td>
<td></td>
</tr>
<tr>
<td>DES-MD5</td>
<td>AES-SHA</td>
<td></td>
</tr>
<tr>
<td>DES-SHA</td>
<td>AES-SHA</td>
<td></td>
</tr>
<tr>
<td>AES-SHA</td>
<td>AES-MD5</td>
<td></td>
</tr>
<tr>
<td>AES-MD5</td>
<td>AES-MD5</td>
<td></td>
</tr>
<tr>
<td>3DES-MD5</td>
<td>AES-MD5</td>
<td></td>
</tr>
<tr>
<td>3DES-SHA</td>
<td>AES-MD5</td>
<td></td>
</tr>
<tr>
<td>DES-MD5</td>
<td>AES-MD5</td>
<td></td>
</tr>
<tr>
<td>DES-SHA</td>
<td>AES-MD5</td>
<td></td>
</tr>
<tr>
<td>AES-SHA</td>
<td>3DES-SHA</td>
<td></td>
</tr>
<tr>
<td>AES-MD5</td>
<td>3DES-SHA</td>
<td></td>
</tr>
<tr>
<td>3DES-MD5</td>
<td>3DES-SHA</td>
<td></td>
</tr>
<tr>
<td>3DES-SHA</td>
<td>3DES-SHA</td>
<td></td>
</tr>
<tr>
<td>DES-MD5</td>
<td>3DES-SHA</td>
<td></td>
</tr>
<tr>
<td>DES-SHA</td>
<td>3DES-SHA</td>
<td></td>
</tr>
<tr>
<td>AES-SHA</td>
<td>3DES-MD5</td>
<td></td>
</tr>
<tr>
<td>AES-MD5</td>
<td>3DES-MD5</td>
<td></td>
</tr>
<tr>
<td>3DES-MD5</td>
<td>3DES-MD5</td>
<td></td>
</tr>
<tr>
<td>3DES-SHA</td>
<td>3DES-MD5</td>
<td></td>
</tr>
<tr>
<td>DES-MD5</td>
<td>3DES-MD5</td>
<td></td>
</tr>
<tr>
<td>DES-SHA</td>
<td>3DES-MD5</td>
<td></td>
</tr>
<tr>
<td>AES-SHA</td>
<td>DES-SHA</td>
<td></td>
</tr>
<tr>
<td>AES-MD5</td>
<td>DES-SHA</td>
<td></td>
</tr>
<tr>
<td>3DES-MD5</td>
<td>DES-SHA</td>
<td></td>
</tr>
<tr>
<td>3DES-SHA</td>
<td>DES-SHA</td>
<td></td>
</tr>
</tbody>
</table>
b. Create users in the WinRadius and during the X-Auth popup, key in the users ID and Password from the WinRadius.
7.2) Test Result

a. The VPN tunnel will be open at any negotiate mode set in Phase 1 and Phase 2.
b. The DFL-800 will show the tunnel is up at their VPN status.

DFL-800 IPSec

b. Client is able to Ping to the remote network.
For the “X-Auth”, when the valid users are enter in the X-Auth popup. The Radius Server will show “Users Authentication OK” and open up the VPN tunnel.
8. Conclusion
The Application Notes demonstrate how D-Link VPN products and TheGreenBow VPN software combined perfectly address the requirements of the small and medium businesses worldwide. The joint VPN solution offer advantages around multiple access control and authorization mechanisms for users and tunneling capabilities to access the entire corporate network; it can also provide different access rights to different users.
D-Link Inc. All Rights Reserved
D-Link is the worldwide leader and an award-winning designer, developer, and manufacturer of Wi-Fi and Ethernet networking, broadband, multimedia, voice and data communications and digital electronics solutions.