



Katana Client to D-Link VPN Gateway

Goal

Configure a VPN tunnel between a Katana client and a D-Link VPN gateway.

Method

The Katana client and the D-Link VPN gateway must have consistent IKE/IPsec settings in order to establish a VPN tunnel.

D-Link gateway configuration

The D-Link VPN gateway (DI-804HV) and firewall has one internal (trusted) and one external (untrusted) interface. The external interface must be assigned a public IP address, and the internal interface must be assigned a subnet. In this example, we use 101.101.101.71 for the external interface and 192.168.71.1/255.255.255.0 for the internal interface.

Katana client configuration

In this example, the Katana client has an IP address of 101.101.101.2 and is not behind a NAT. However, it is possible that the client may have a non-routable IP address and be located behind a NAT router. The connection to the D-Link VPN gateway will work in either case.

A word of caution

If the Katana client is trying to connect to the D-Link VPN gateway from behind a NAT, it is almost impossible to establish a functional VPN tunnel. There are two reasons.

First, some NAT routers do not process IKE and IPsec packets correctly and if you are behind such a NAT router, you may not be able to access hosts behind the D-Link gateway even though an SA has been established.

Second, a bigger problem is that the D-Link VPN gateway has a bug and it does not process NATed IKE packets correctly. The only way a functional VPN tunnel can be established is when the IKE packets arriving at the D-Link gateway have source (and destination) port as 500.

Our suggestion is that you purchase the OmniVPN or Katana gateway.



D-Link gateway Dynamic VPN configuration

On the D-Link gateway, the main VPN configuration page displays the static tunnels with other VPN gateways. The D-Link VPN gateway also enables the user to configure a dynamic VPN tunnel through which remote access users can connect. The details of this dynamic tunnel can be viewed by clicking the “Dynamic VPN setup” button below the list of tunnels.



Figure 1: Main VPN configuration page for D-Link gateway.



When “Dynamic VPN” is enabled, the D-Link gateway will automatically fill in the local subnet information. If it does not, enter the local subnet (192.168.71.0/255.255.255.0 in this example). Also enter the “Pre-shared Key” that will be used during the IKE authentication.

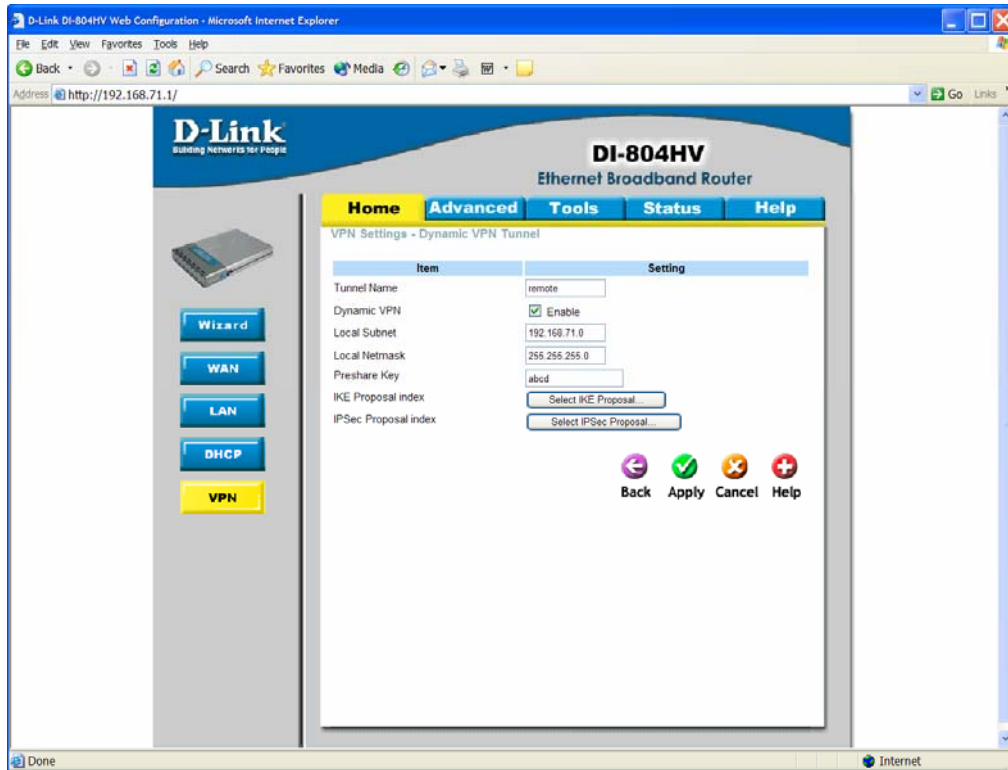


Figure 2: Configuration of dynamic VPN.



D-Link gateway IKE configuration

Click the “Select IKE Proposal” button to configure IKE (ISAKMP) policies. The D-Link gateway does not come pre-configured with proposals, so they must be added manually. In the example of Figure 3, we have added four proposals.

For each proposal, one must specify:

- Name
- Diffie-Hellman (DH) group
- Encryption algorithm
- Authentication algorithm
- Life Time
- Life Time Unit

Once the proposals have been configured, use the “Add to” button below the list to add the proposals to the IKE proposal index listed at the top of the page.

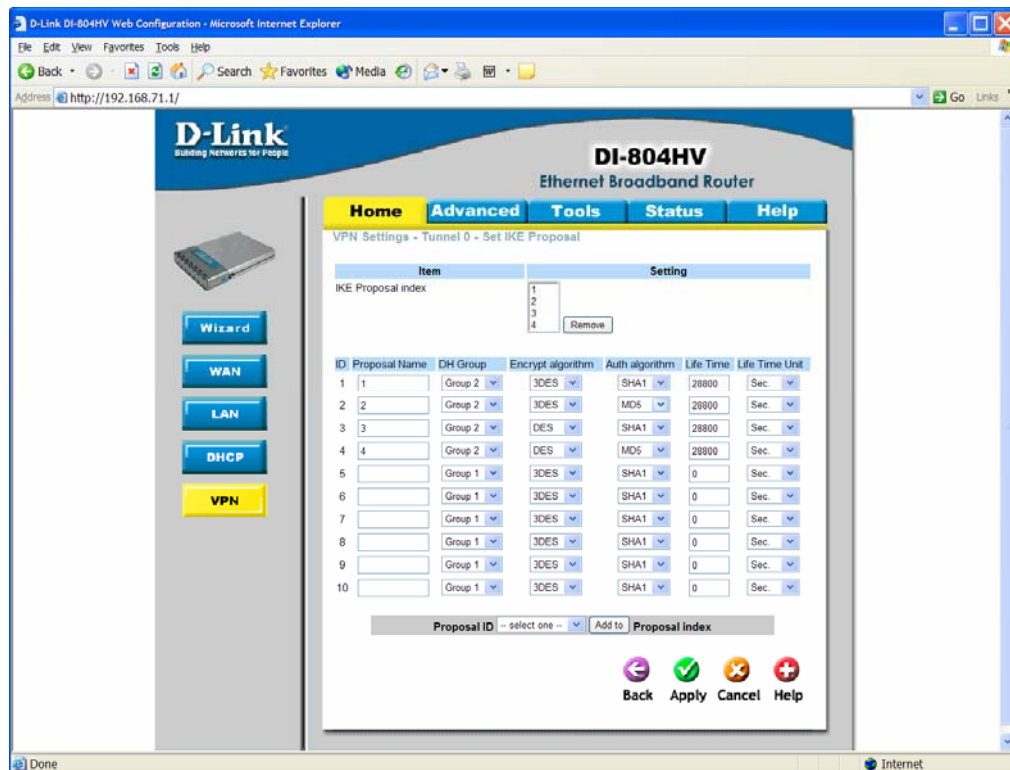


Figure 3: IKE Phase 1 (ISAKMP) proposals.



D-Link gateway IPsec configuration

Click on “Select IPsec Proposal” button in the Dynamic VPN Tunnel window to configure IPsec policies. The D-Link gateway does not come pre-configured with proposals, so they must be added manually. In the example of Figure 4, we have added four proposals.

For each proposal, one must specify:

- Name
- Encapsulation algorithm
- Diffie-Hellman (DH) group
- Encryption algorithm
- Authentication algorithm
- Life Time
- Life Time Unit

Once the proposals have been configured, use the “Add to” button below the list to add the proposals to the “IPsec proposal index” listed at the top of the page.

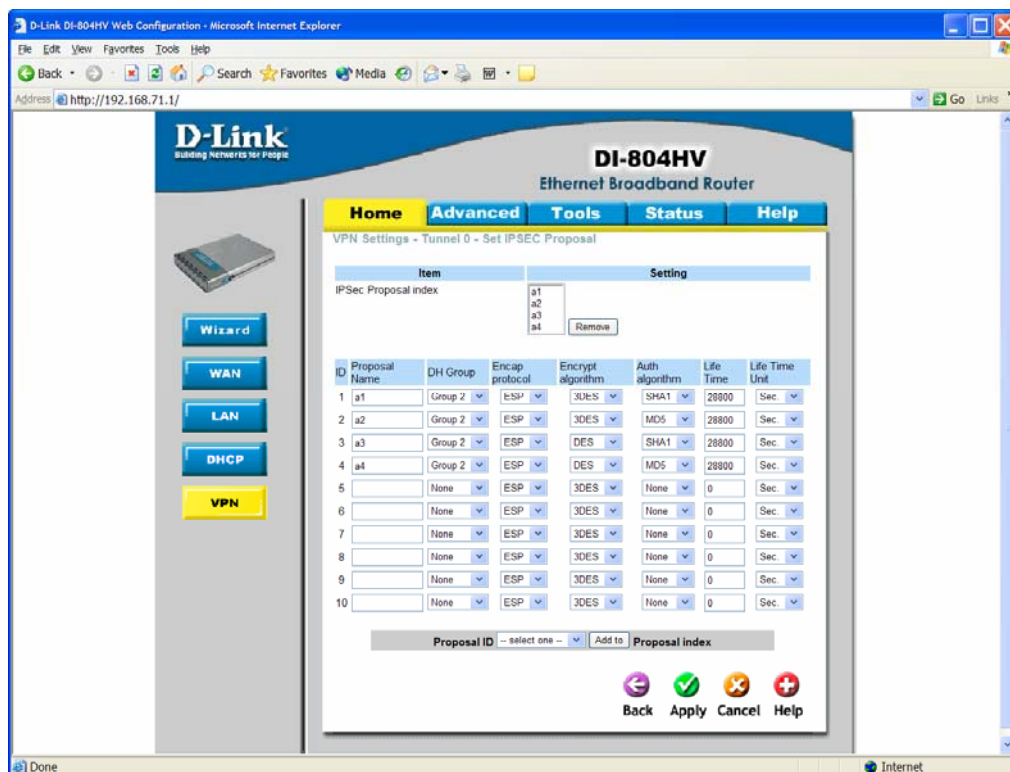


Figure 4: IKE Phase 2 (IPsec) proposals



Katana client tunnel configuration

The “Role” must be set to “Stand-alone client,” and the VPN button in the toolbar must show a lock that is closed and green. Multiple VPN tunnels can be defined, and each one can be activated or deactivated independently.

In the Configuration window, click the “Add” button to the right of the list of tunnels. This opens the dialog box to define tunnel parameters.

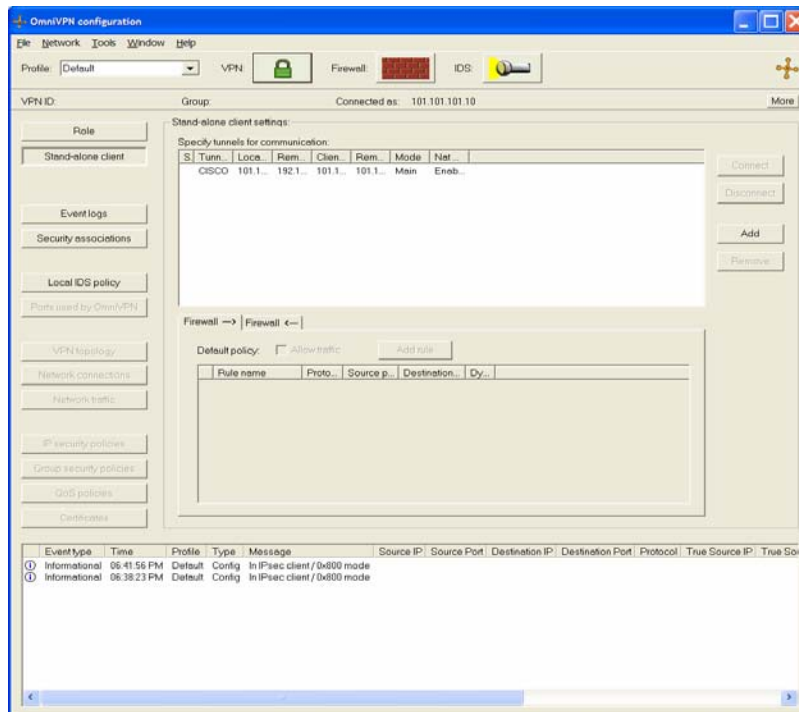


Figure 5: Katana configuration window



Enter the local (Katana side) and remote (D-Link side) configuration. If the client subnet mask is set to 32 (255.255.255.255), the IP address and client ID will be automatically set to the client's address. At the bottom left, the "ID type" must be set to "Address" and the mode set to "Main mode." In addition, NAT Traversal must be enabled.

For the "Local configuration," enter:

Client ID:	Current IP address of the client (101.101.101.2 in this example)
Subnet:	Current subnet of the client (101.101.101.0 / 32 in this example)
Public IP address:	Same as the current IP address of the client (101.101.101.2 in this example)

For the "Remote configuration", enter:

Remote ID:	Public IP address of the D-Link gateway (101.101.101.71 in this example)
Subnet:	Subnet behind the D-Link gateway (192.168.71.0 / 24 in this example)
Public IP address:	Public IP address of the D-Link gateway (101.101.101.71 in this example)

Figure 6: Tunnel definition.



Katana client IKE/IPsec configuration

To configure the IKE and IPsec parameters to match those on the gateway, click the “Edit proposals” button in the "Define tunnel" window. This will open the “Edit proposals” window where the IKE and IPsec parameters are specified.

The IKE (ISAKMP) settings must be Tunnel mode using Identity Protection mode, and NAT Traversal must be enabled. There are four proposals in this example, but more importantly, there is one proposal that will be accepted by the D-Link gateway, i.e., 3DES-MD5. The lifetime is set to 8 hours. To add more proposals, click the “Add ISAKMP proposal” button.

There are four IPsec proposals in this example, but more importantly, there is one proposal that will be accepted by the D-Link gateway, i.e., 3DES-MD5. Perfect forward secrecy is enabled using MODP 1024 (the second Diffie-Hellman group). The lifetime is set to 8 hours. To add more proposals, click on “Add IPsec proposal” button.

To change a proposal in either list, double-click on it. To re-arrange proposals in either list, select one, hold down the Ctrl key, and press the up or down arrow keys.

The screenshot shows the 'Edit proposals' dialog box with the following configuration:

- Secure communication via: Tunnel mode
- ISAKMP: In order to authenticate the client:
 - Initiate: Identity Protection mode
 - Initiate NAT traversal
 - Accept Aggressive mode
- Send ISAKMP proposals:

Authentication	Diffie-Hellman	Hash algor...	Encryption ...	Key length
Pre-shared text key	MODP 1024 (group 2)	SHA1	3DES-CBC	192
Pre-shared text key	MODP 1024 (group 2)	MD5	3DES-CBC	192
Pre-shared text key	MODP 1024 (group 2)	SHA1	DES-CBC	64
Pre-shared text key	MODP 1024 (group 2)	MD5	DES-CBC	64
- Tunnel lifetime: 8 hours
- IPsec: Once the client is authenticated:
 - Perfect forward secrecy via: MODP 1024
- Use IPsec protocol:
 - ESP with authentication
 - ESP without authentication
 - ESP + AH
 - AH
- Send IPsec proposals:

Hash algorithm	Encryptio...	Key length
HMAC-SHA1	3DES	192
HMAC-MD5	3DES	192
HMAC-SHA1	DES	64
HMAC-MD5	DES	64
- Tunnel lifetime: 8 hours

Buttons: OK, Cancel, Add ISAKMP proposal, Add IPsec proposal

Figure 7: IKE (ISAKMP) and IPsec proposals.



Conclusion

After the VPN tunnel is defined, Katana will automatically attempt to establish it. A green checkmark will appear next to the tunnel if it is established successfully. If a tunnel cannot be established, no icon will be displayed. If the tunnel has been disabled, a red cross will be displayed.

To disconnect a tunnel, select it and click the “Disconnect” button to the right of the list of tunnels. Since VPN tunnels are created on demand, the tunnel may be re-established automatically. To disable a tunnel, turn off the “Tunnel is enabled” option at the top of the "Define tunnel" window.

To completely disconnect from the VPN, click the VPN button in the toolbar. The lock will open and turn red.

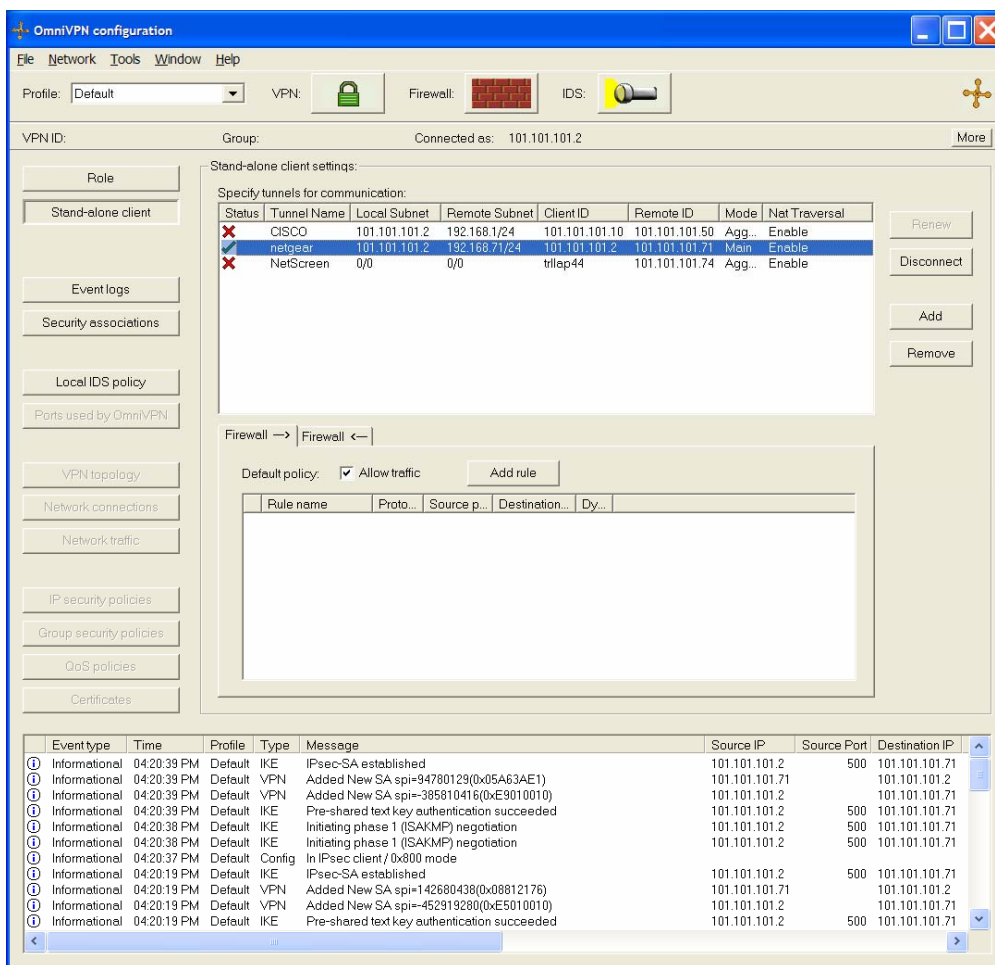


Figure 8: A green checkmark indicates that the tunnel is established.



After establishing a VPN tunnel between the Katana client and the D-Link gateway, the details of the security association (SA) can be viewed by clicking the “Security associations” button in the Configuration window. To delete an SA, select it in the Security Associations window and press the “Delete” button on the keyboard.

The screenshot shows a window titled "Security associations" with a menu bar containing "File", "SA", "Window", and "Help". The main area contains a table with the following data:

Source addr...	Destination a...	SPI	Mode	Protoc...	Authentication	Encryption	Created	Expires
101.101.101.2	101.101.101.74	0x4F54FCBE	Tunnel	ESP	HMAC-SHA1	AES (128)	02:33:47 PM	04:33:47 PM
101.101.101.74	101.101.101.2	0x0D57AD3E	Tunnel	ESP	HMAC-SHA1	AES (128)	02:33:47 PM	04:33:47 PM

Figure 9: List of existing security associations.