



Katana Client to NetGear VPN Gateway

Goal

Configure a VPN tunnel between a Katana client and a NetGear VPN gateway.

Method

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

NetGear gateway configuration

The NetGear VPN gateway (FVM-318) 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 101.101.101.72 for the external interface and 192.168.72.1/255.255.255.0 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 NetGear VPN gateway will work in either case.

A word of caution

If the Katana client is trying to connect to the NetGear 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, so if you are behind such a NAT router, you may not be able to access hosts behind the NetGear gateway even though an SA has been established.

Second, a bigger problem is that the NetGear 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 NetGear gateway have source (and destination) port as 500.

You can also easily crash NetGear VPN gateway by trying to do aggressive mode IKE with them when the OmniVPN client has incorrect configuration, e.g. pre-shared secret.

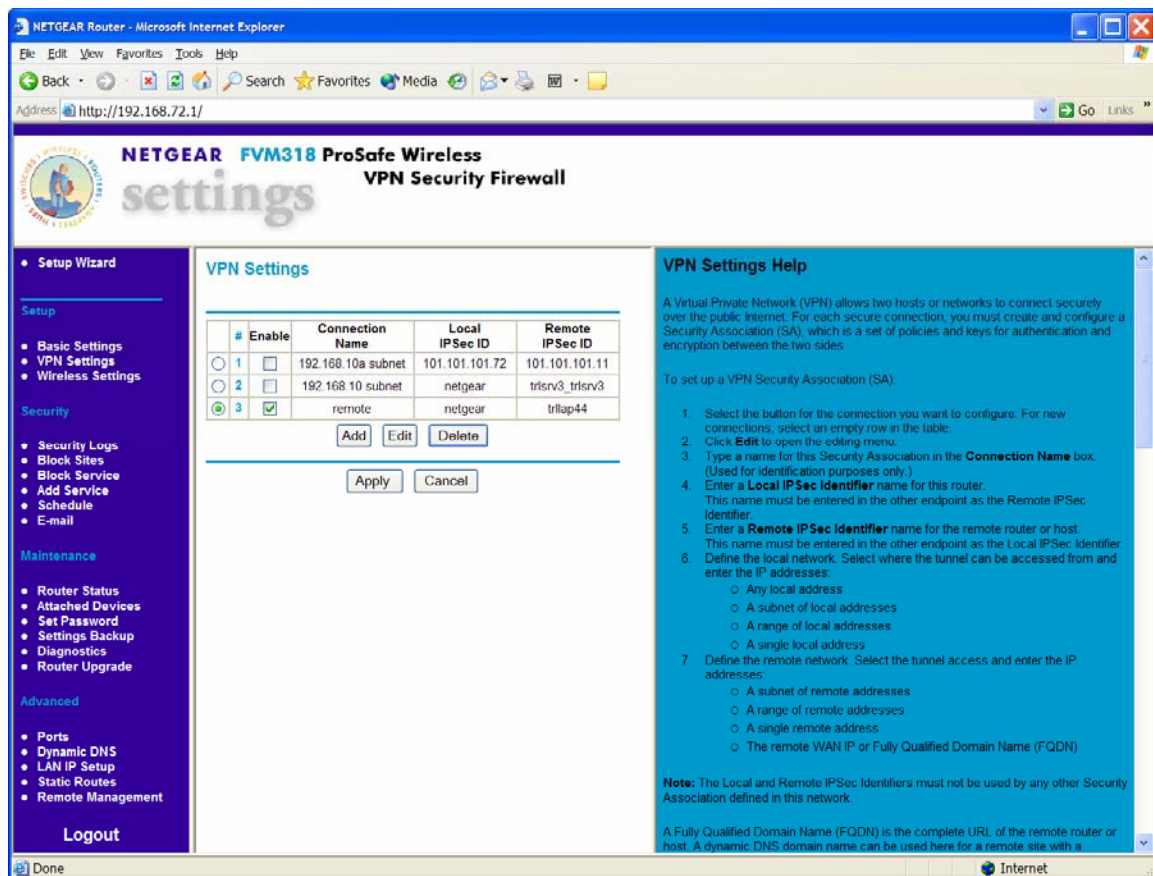
Our suggestion is that you purchase the OmniVPN or Katana gateway.



NetGear gateway remote access VPN configuration

On the NetGear gateway, the main VPN Settings page displays the tunnels that have been defined.

The remote access VPN is a tunnel that allows connecting from any remote IP address and subnet. To allow multiple remote access users, create separate VPN tunnels and use a different "Connection Name" and "Remote IPsec identifier" for each one.



The screenshot shows the NetGear VPN Settings page in a Microsoft Internet Explorer browser window. The page title is "NETGEAR FVM318 ProSafe Wireless VPN Security Firewall settings". The main content area is titled "VPN Settings" and contains a table with the following data:

#	Enable	Connection Name	Local IPsec ID	Remote IPsec ID
1	<input type="checkbox"/>	192.168.10a subnet	101.101.101.72	101.101.101.11
2	<input type="checkbox"/>	192.168.10 subnet	netgear	trlsrv3_trlsrv3
3	<input checked="" type="checkbox"/>	remote	netgear	trlap44

Below the table are buttons for "Add", "Edit", and "Delete". At the bottom of the table area are "Apply" and "Cancel" buttons. To the right of the table is a "VPN Settings Help" section with a blue background, containing a definition of a VPN and a list of 7 steps to set up a VPN Security Association (SA). A note at the bottom states: "Note: The Local and Remote IPsec Identifiers must not be used by any other Security Association defined in this network." The left sidebar contains navigation links for Setup Wizard, Setup, Security, Maintenance, Advanced, and Logout.

Figure 1: Main VPN configuration page for NetGear gateway.



NetGear gateway IKE / IPsec configuration

Select the tunnel that was created for remote access and click on the “Edit” button to configure IKE and IPsec proposals and identifiers.

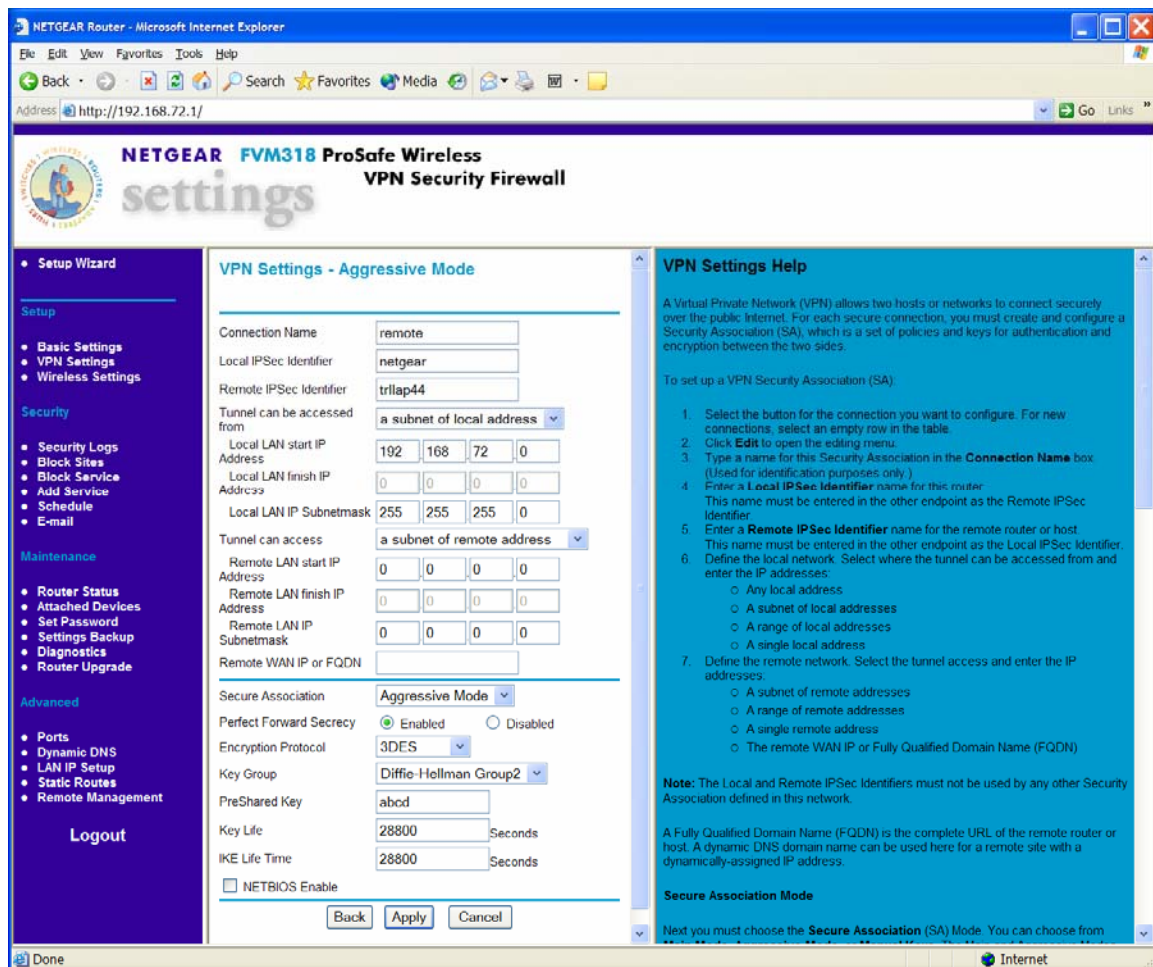


Figure 2: IKE and IPsec configuration.



Configure the tunnel parameters as follows:

Connection Name:	Enter a unique name for this connection. ("remote" in this example)
Local IPsec identifier:	Enter the name of the NetGear gateway. ("netgear" in this example)
Remote IPsec identifier:	Enter a unique name for the remote access user. ("trllap44" in this example)
Tunnel can be accessed from:	"a subnet of local address"
Local LAN start IP Address:	First IP address of the subnet (192.168.72.1 in this example)
Local LAN IP Subnet mask:	The subnet mask (255.255.255.0 in this example)
Tunnel can access:	"a subnet of remote address"
Remote LAN start IP:	0.0.0.0
Remote LAN IP subnet mask:	0.0.0.0
Remote WAN IP or FQDN:	Leave it blank.

Unlike other VPN gateways which support multiple and separate proposals for ISAKMP and IPsec, NetGear only allows one proposal and uses it for both ISAKMP and IPsec.

Configure the proposal as follows:

- Secure Association: Aggressive mode
- Perfect Forward Secrecy: Enabled
- Encryption Protocol: 3DES
- Key Group: Diffie-Hellman Group 2
- Pre-Shared Key: Enter the text for the pre-shared key
("abcd" in this example)
- Key Life: 28800 Seconds
- IKE Life Time: 28800 Seconds

Once the information has been entered, click the "Apply" button to save the settings.



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.

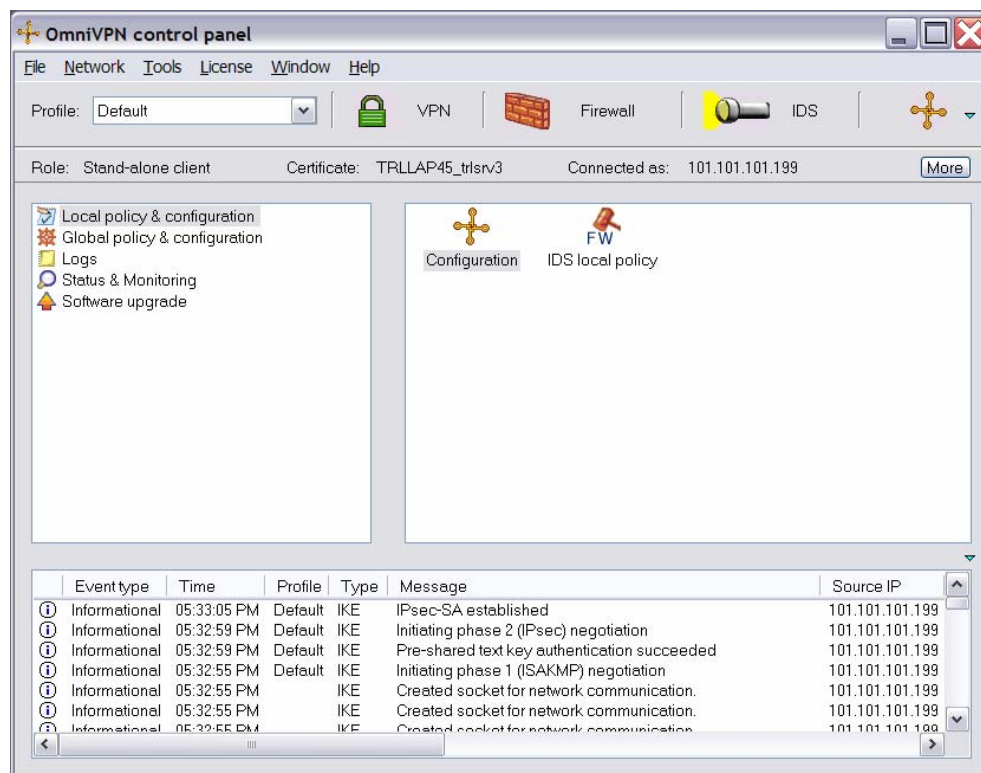


Figure 3: Katana control panel and configuration window



Enter the local (Katana side) and remote (NetGear 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 "FQDN" and the mode set to "Aggressive mode." In addition, NAT Traversal must be disabled.

For the "Local configuration," enter:

Client ID:	ID to be used by the client ("trllap44" in this example)
Subnet:	0.0.0.0 / 0 (required)
Public IP address:	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 NetGear gateway (101.101.101.72 in this example)
Subnet:	0.0.0.0 / 0 (required)
Public IP address:	Public IP address of the NetGear gateway (101.101.101.72 in this example)

Define tunnel

Tunnel is enabled

Tunnel name: NetGear Pre-shared secret: abcd

Local configuration:

Client ID: trllap44

Subnet: 0 . 0 . 0 . 0 / 0

Mask: 0 . 0 . 0 . 0

Public IP address: 101 . 101 . 101 . 2

Remote configuration:

Remote ID: 101.101.101.72

Subnet: 0 . 0 . 0 . 0 / 0

Mask: 0 . 0 . 0 . 0

Public IP address: 101 . 101 . 101 . 72

Additional IKE settings:

ID type: FQDN

Mode: Main mode Aggressive mode

Enable NAT Traversal

Renegotiate tunnel after it expires

Edit proposals Edit firewall rules

OK Cancel

Figure 4: 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 Aggressive mode, and NAT Traversal must be disabled. There are two proposals in this example, but more importantly, there is one proposal that will be accepted by the NetGear 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 NetGear 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: Aggressive 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
- 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	Encryption...	Key length
HMAC-SHA1	3DES	192
HMAC-MD5	3DES	192
HMAC-SHA1	DES	64
HMAC-MD5	DES	64
- Tunnel lifetime: 8 hours
-
-

Figure 5: 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.

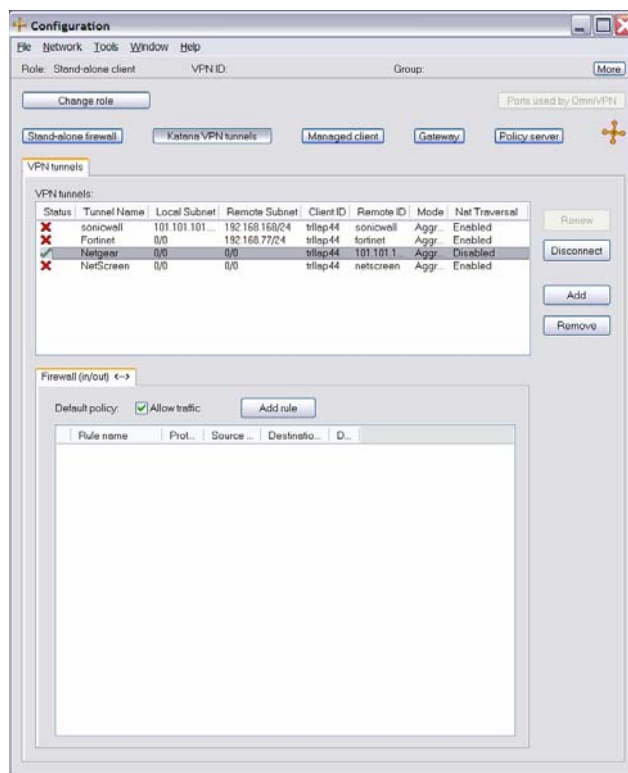
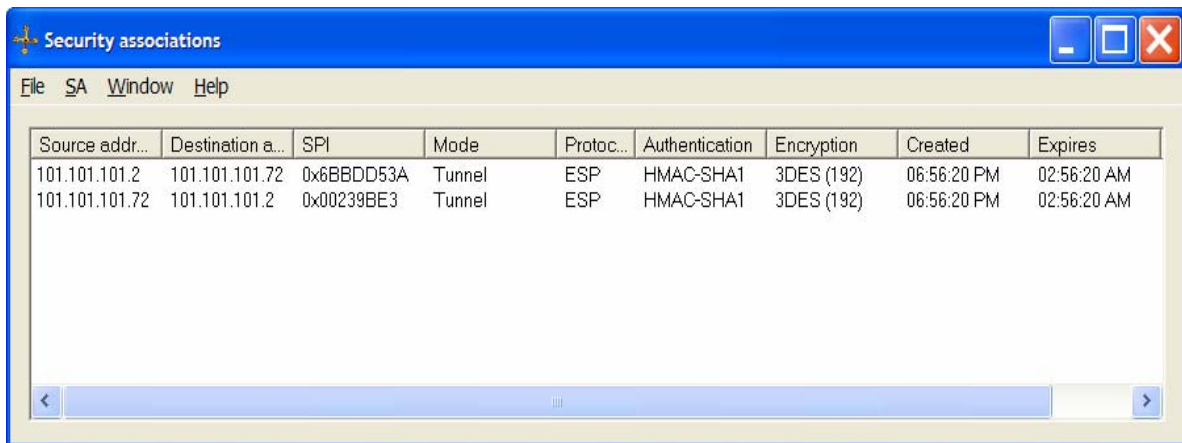


Figure 6: A green checkmark indicates that the tunnel is established.



After establishing a VPN tunnel between the Katana client and the NetGear 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	101.101.101.72	0x6BBDD53A	Tunnel	ESP	HMAC-SHA1	3DES (192)	06:56:20 PM	02:56:20 AM
101.101.101.72	101.101.101.2	0x00239BE3	Tunnel	ESP	HMAC-SHA1	3DES (192)	06:56:20 PM	02:56:20 AM

Figure 7: List of existing security associations.

Please note that successfully establishing a SA may not be sufficient to connect to machines behind the NetGear gateway. Some NAT routers do not process IKE and IPsec packets correctly, so if you are behind such a NAT router, you may not be able to access hosts behind the NetGear gateway even though an SA has been established.

The NetGear VPN gateway also requires that IKE source and destination port both be 500. Because of this, it is almost impossible to even establish an SA with a NetGear VPN gateway if a NAT is present.

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