



Katana Client to Fortinet VPN Gateway

Goal

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

Method

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

Fortinet gateway configuration

The Fortinet VPN gateway (Fortigate-50A) 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 101.101.101.77 for the external interface and 192.168.77.1/255.255.255.0 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 Fortinet VPN gateway will work in either case.



Fortinet gateway IKE Tunnel configuration

IKE configuration on Fortinet devices is tied to the gateway. When you select “VPN→IPSEC” and click on “Phase 1” tab, a list of all the remote gateways is displayed. While the road warrior (Dialup user) is not a remote gateway, an entry must be created here. Click the “New” button to create an entry for “Road warrior.”

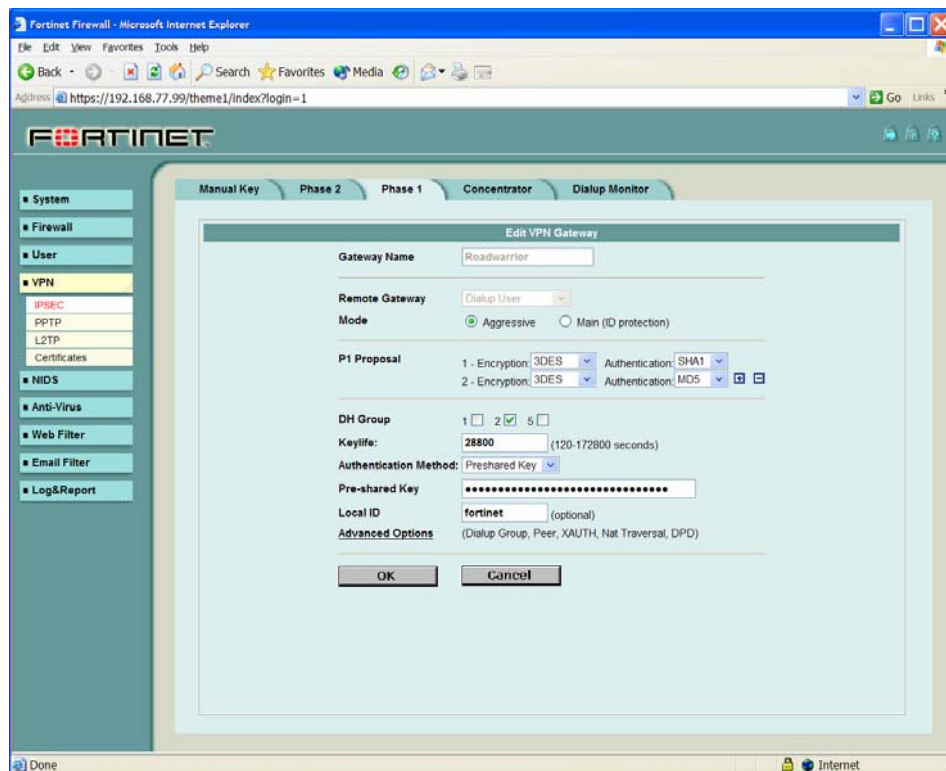


Figure 1: IKE Phase 1 proposals.

Remote Gateway:	Dialup User
Mode:	Aggressive
DH Group:	2
Keylife:	Key lifetime (28800seconds)
Pre-shared Key:	Secret for dialup user authentication (“abcdabcd” in this example)

Local ID:	ID of the Fortinet gateway (“fortinet” in this example)
-----------	---

Public IP address:	The current IP address of the client (101.101.101.2 in this example)
--------------------	--

Turn on the “Enable NAT-Traversal” option from the “Advanced Options.”



Next click on the “Phase 2” tab and add a new tunnel for the dialup user.

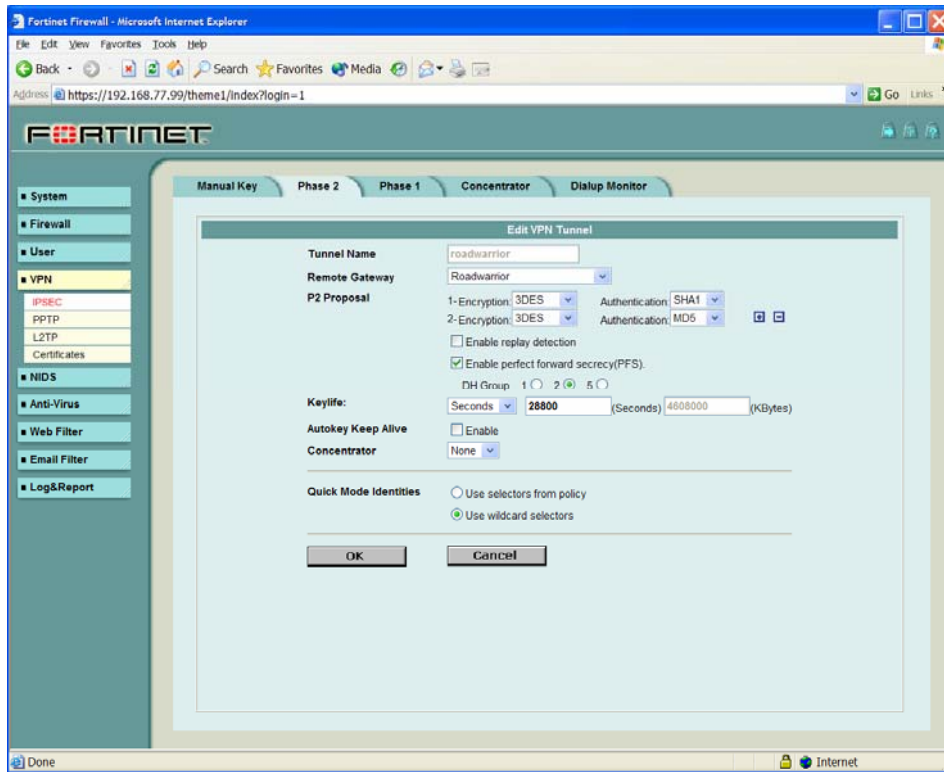


Figure 2: IKE Phase 2(IPsec) proposal.

Remote Gateway:	Gateway for dialup user (“Roadwarrior in this example)
P2 Proposal:	3DES-SHA1 and 3DES-MD5
Enable PFS:	Yes
DH Group:	2
Keylife:	28800 seconds
Concentrator:	None
Quick mode identifiers:	User wildcard selectors



Fortinet gateway policy configuration

The VPN gateways and tunnel must be associated with a security policy.

Start the Fortinet device management GUI and select the “Firewall” category in the left column. Click on “Edit” in the “From External To Internal” zone.

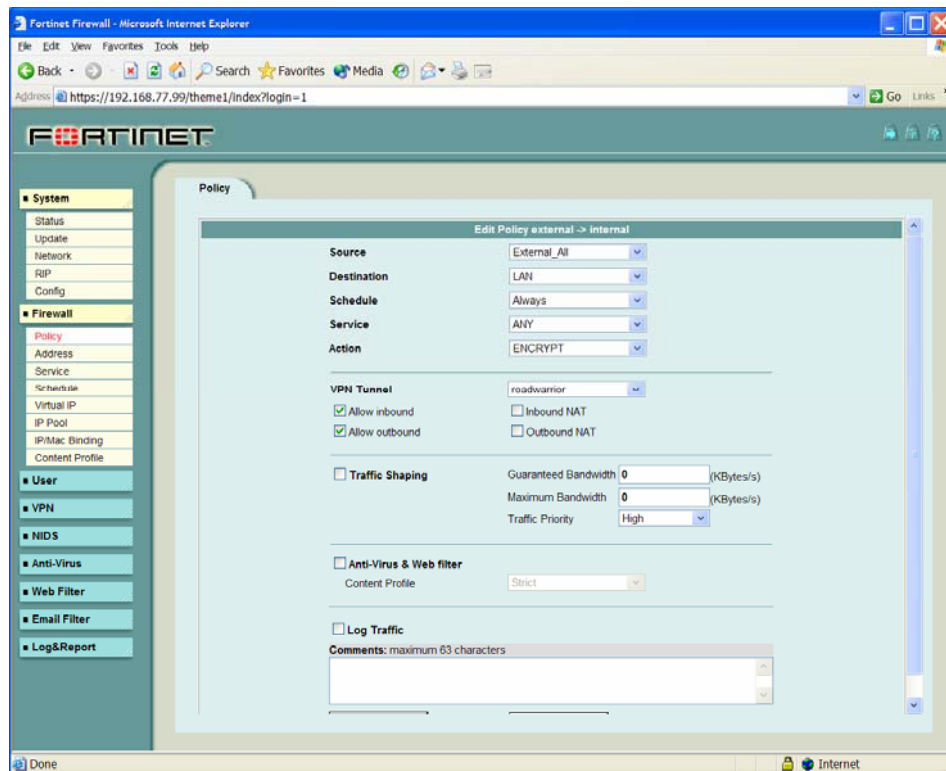


Figure 3: Dynamic gateway for remote access VPN.

Create a policy for incoming traffic from “Externall_All” (0.0.0.0/0) to the LAN (192.168.77.0/24 in this example) or to “Internal_All” and set the Action to “ENCRYPT.” Assign a name to the VPN tunnel.



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.

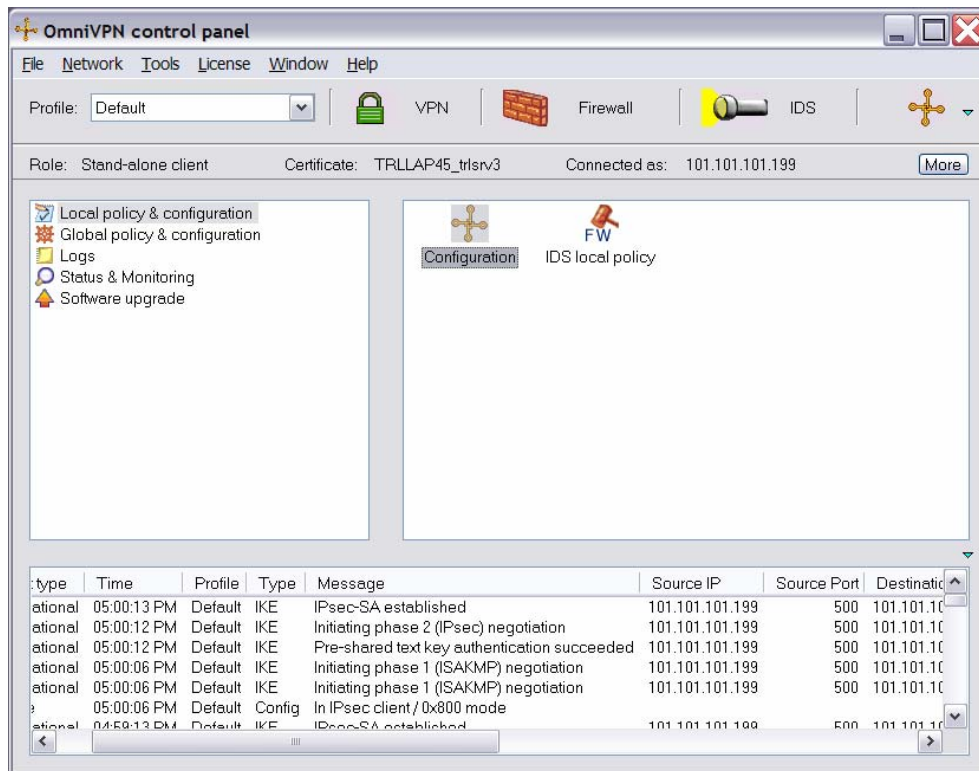


Figure 4: Katana control panel and configuration window



Enter the local (Katana side) and remote (Fortinet 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 enabled.

For the "Local configuration," enter:

Client ID:	ID to be used by the client ("Roadwarrior" 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 Fortinet gateway (101.101.101.77 in this example)
Subnet:	192.168.77.0 / 24
Public IP address:	Public IP address of the Fortinet gateway (101.101.101.77 in this example)

Figure 5: 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 four proposals in this example, but more importantly, there is one proposal that will be accepted by the Fortinet gateway, i.e., 3DES-MD5. The lifetime is set to 2 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 Fortinet gateway, i.e., 3DES-MD5. Perfect forward secrecy is enabled using MODP 1024 (the second Diffie-Hellman group). The lifetime is set to 2 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 settings:

- 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-Hell...	Hash algor...	Encryption ...	Key length
Pre-shared text key	MODP 102...	SHA1	AES-CBC	128
Pre-shared text key	MODP 102...	MD5	AES-CBC	128
Pre-shared text key	MODP 768...	SHA1	AES-CBC	128
Pre-shared text key	MODP 768...	MD5	AES-CBC	128
- 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	AES	128
HMAC-MD5	AES	128
HMAC-SHA1	3DES	192
HMAC-MD5	3DES	192
- Tunnel lifetime: 8 hours
-

Buttons: OK, Cancel

Figure 6: 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.

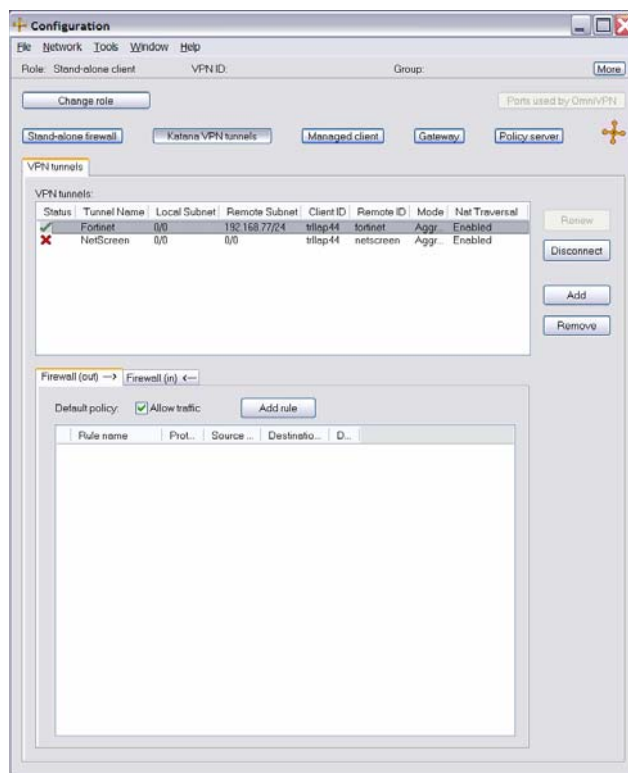


Figure 7: A green checkmark indicates that the tunnel is established.



After establishing a VPN tunnel between the Katana client and the Fortinet 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 address	Destination address	SPI	Mode	Protoc..	Authentication	Encryption	Created	Expires
101.101.101.2	101.101.101.77	0xDF3CB131	Tunnel	ESP	HMAC-SHA1	3DES (192)	05:18:01 PM	01:18:01 AM
101.101.101.77	101.101.101.2	0x0BA165F0	Tunnel	ESP	HMAC-SHA1	3DES (192)	05:18:01 PM	01:18:01 AM

Figure 8: List of existing security associations.