



Katana Client to SonicWall VPN Gateway

Goal

Configure a VPN tunnel between a Katana client and a SonicWall VPN gateway (TELE3 SP).

Method

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

SonicWall gateway configuration

The SonicWall VPN gateway (TELE3 SP) and firewall has one internal (trusted or LAN) and one external (untrusted or WAN) 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 101.101.101.168 for the external interface and 192.168.168.1/255.255.255.0 for the internal interface.

Katana client configuration

In this example, the Katana client has an IP address of 101.101.101.5 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 SonicWall VPN gateway will work in either case.



SonicWall gateway remote access VPN configuration

On the SonicWall VPN gateway, the main VPN settings page displays the global VPN options. These options are applicable to all VPN connections. The following global VPN settings must be checked.

- ✓ Enable VPN
- ✓ Enable Fragmented Packet Handling
- ✓ Enable NAT Traversal

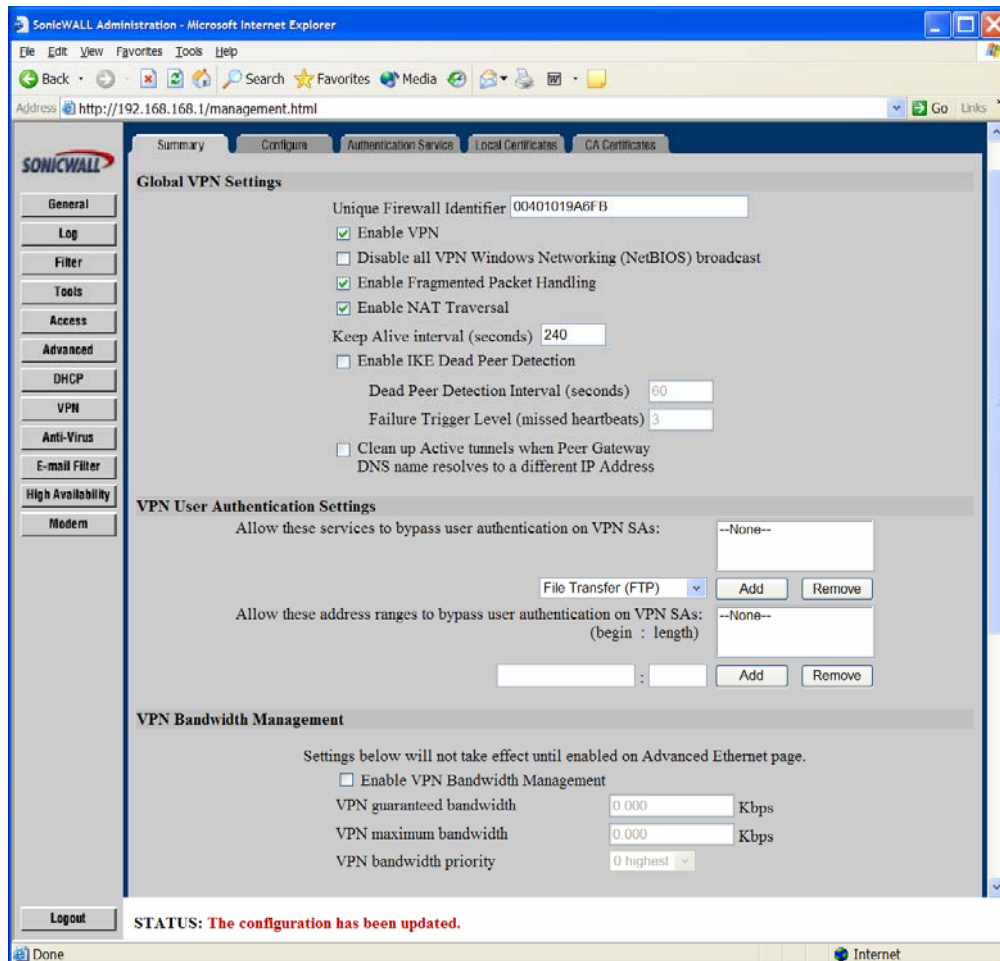


Figure 1: Main VPN configuration page for SonicWall gateway.



SonicWall gateway IKE / IPsec configuration

The “GroupVPN” security association (or VPN tunnel) allows the remote access users to connect from any remote IP address. All remote access users must use the same remote access VPN tunnel. There does not appear to be any way to configure multiple remote access tunnels or to allow more than one remote access connection at a time.

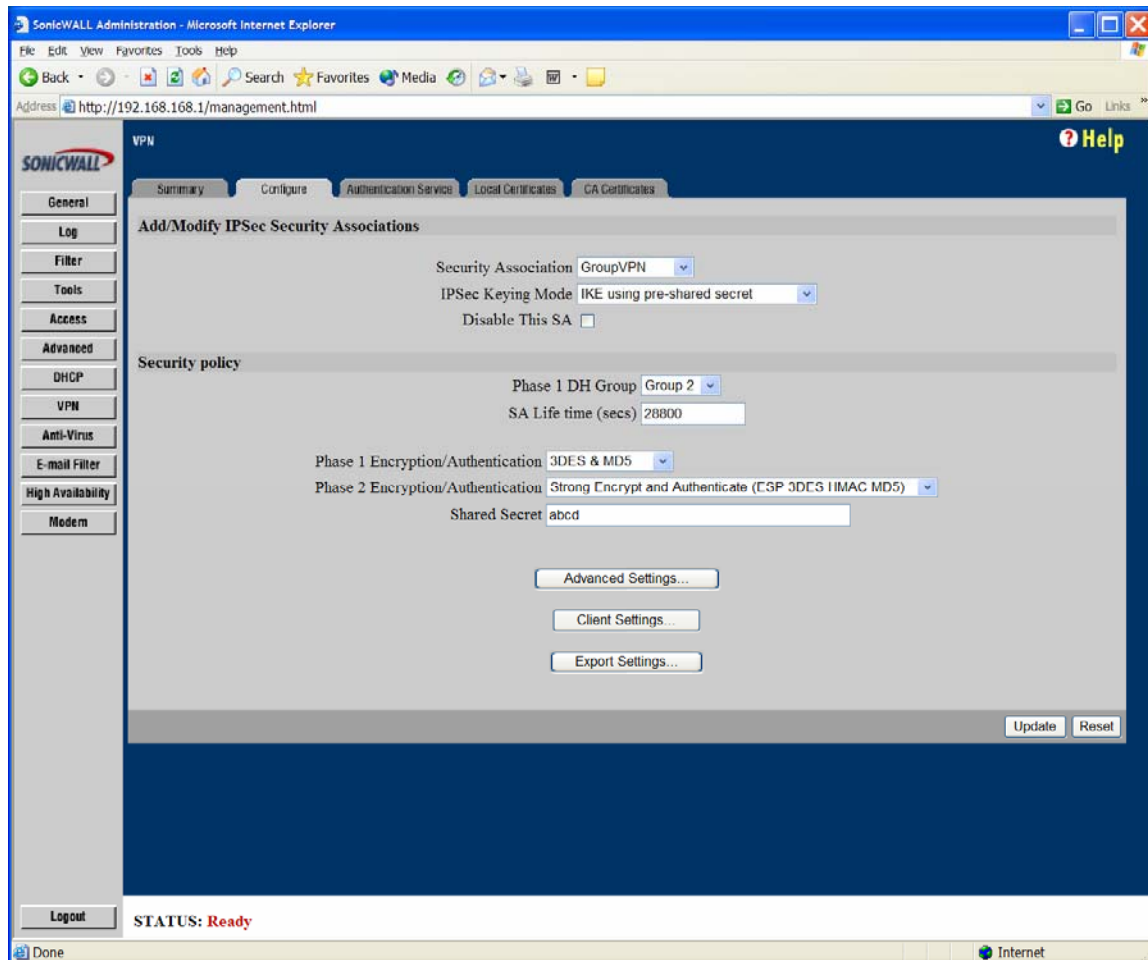


Figure 2: Main VPN configuration page for SonicWall gateway.



Select the “Group VPN” security association from the list of security associations.

IPsec keying: IKE using pre-shared secret
Disable this SA: Unchecked

Security policy

Phase 1 DH Group: Group 2
SA Lifetime (secs): 28800
Phase 1 Encryption/Authentication: 3DES & MD5
Phase 2 Encryption/Authentication: ESP 3DS HMAC MD5
Shared Secret: “abcd” in this example

Once the tunnel policies and identifiers are configured, click on the “Advanced Settings” button at the bottom of the page to configure additional IPsec parameters.

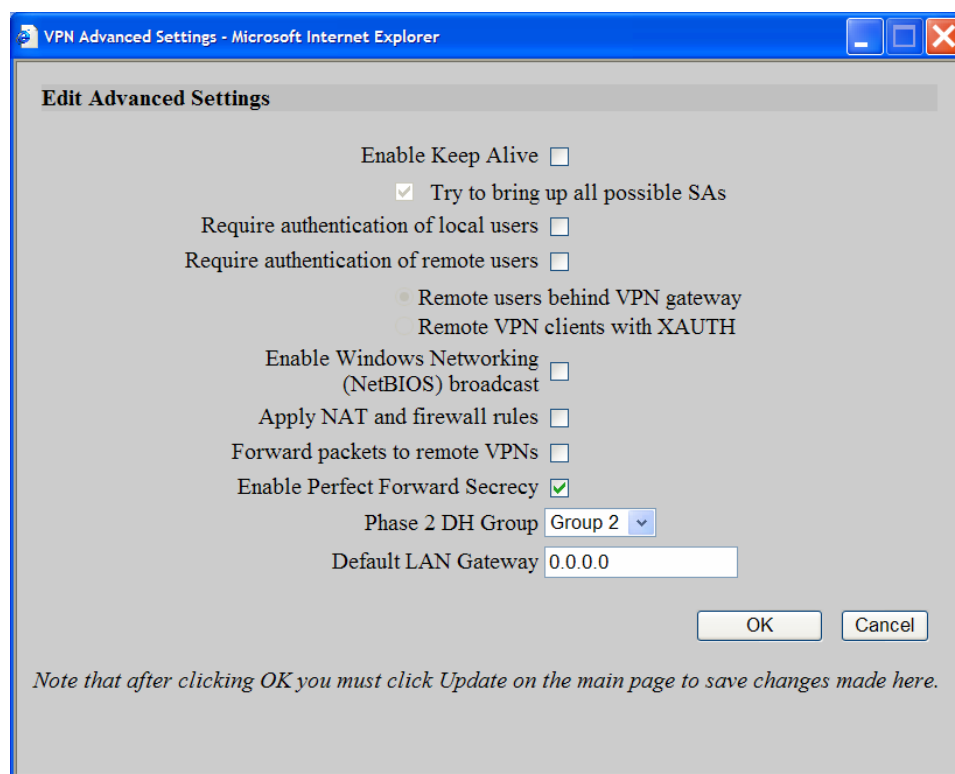


Figure 3: IKE and IPsec proposals.

Check the “Enable Perfect Forward Secrecy” box and select the “Phase 2 DH Group” to “Group 2.”

After additional IPsec parameters have been configured, click “OK” to save the proposals and return to the VPN configure page. It is critical that the same Phase 1 and Phase 2 proposals appear in the list of proposals at the remote client.



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.

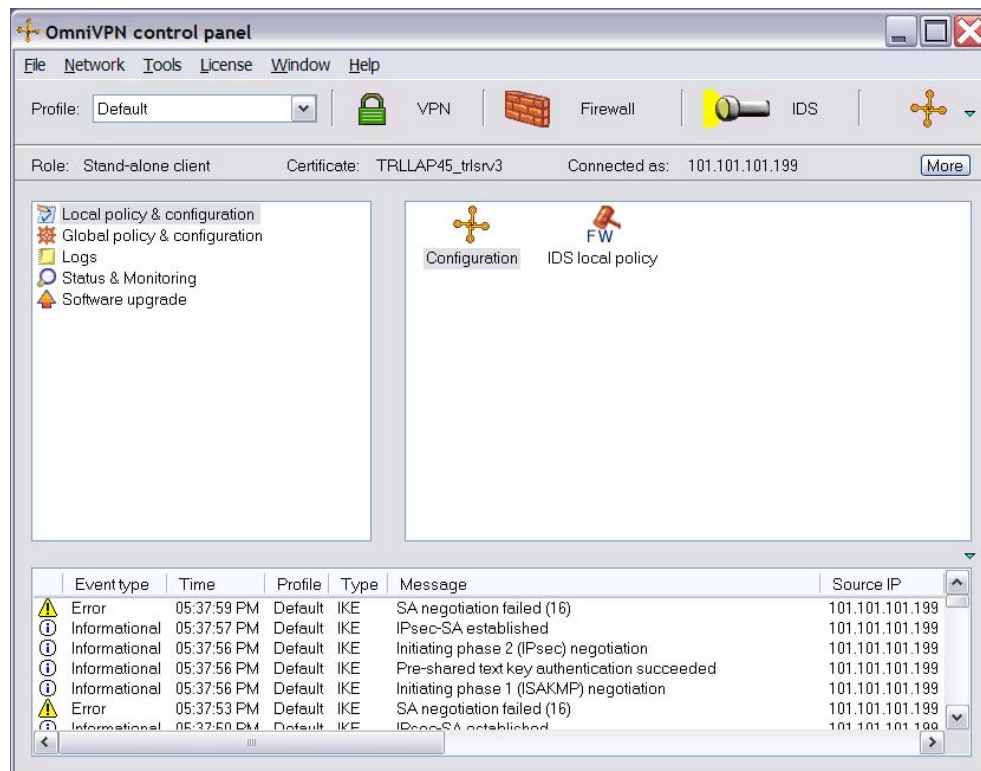


Figure 4: Katana control panel and configuration window



Enter the local (Katana side) and remote (SonicWall 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 (101.101.101.5 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 (101.101.101.5 in this example) |

For the "Remote configuration," enter:

| | |
|--------------------|---|
| Remote ID: | Public IP address of the SonicWall gateway (101.101.101.168 in this example) |
| Subnet: | Subnet behind the SonicWall gateway (192.168.168.0 / 24 in this example) |
| Public IP address: | Public IP address of the SonicWall gateway (101.101.101.168 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 proposal defined on the Katana client must match the proposal defined at the SonicWall VPN gateway exactly. There must be only one proposal.

The IKE (ISAKMP) settings must be Tunnel mode using Identity Protection mode, and NAT Traversal must be enabled. There is only one proposal for both ISAKMP and IPsec, i.e., 3DES-MD5. The lifetimes are set to 8 hours. Perfect forward secrecy is enabled using MODP 1024 (the second Diffie-Hellman group). **Please make sure that the proposals are identical to those entered on the SonicWall VPN gateway.**

The screenshot shows the 'Edit proposals' window 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 768 (group 1) | SHA1 | 3DES-CBC | 192 |
| Pre-shared text key | MODP 768 (group 1) | 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: 6 hours
 -
-

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.

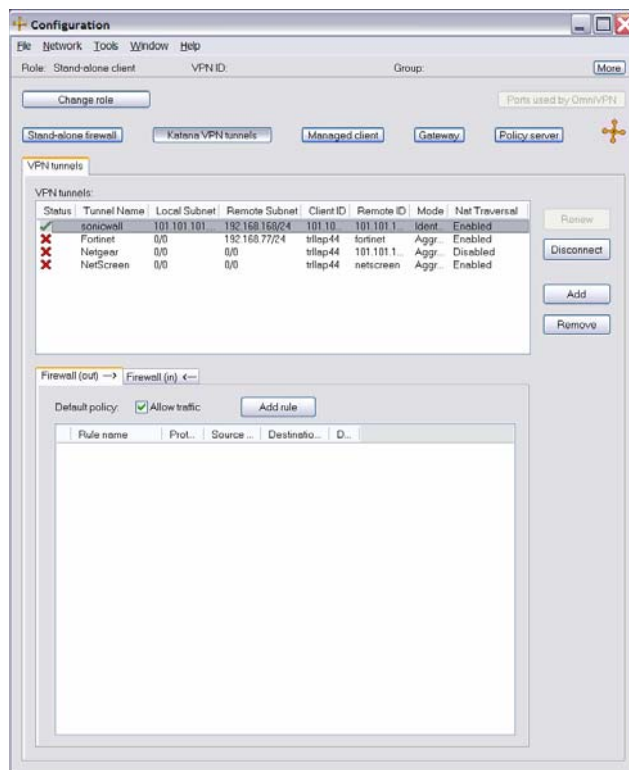


Figure 7: A green checkmark indicates that the tunnel is established.



After establishing a VPN tunnel between the Katana client and the SonicWall 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 |
|-----------------|------------------|------------|--------|-----------|----------------|------------|-------------|-------------|
| 101.101.101.5 | 101.101.101.1... | 0x1C09D451 | Tunnel | ESP | HMAC-SHA1 | 3DES (192) | 02:14:25 PM | 08:14:25 PM |
| 101.101.101.168 | 101.101.101.5 | 0x0F2D1C79 | Tunnel | ESP | HMAC-SHA1 | 3DES (192) | 02:14:25 PM | 08:14:25 PM |

Figure 8: List of existing security associations.