



Katana Client to CISCO VPN Gateway

Goal

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

Method

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

CISCO gateway configuration

The CISCO VPN gateway (PIX-501) and firewall has one internal and one external 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 101.101.101.50 for the external interface and 192.168.1.1/255.255.255.0 for the internal interface.

Katana client configuration

In this example, the Katana client has an IP address of 101.101.101.10 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 CISCO VPN gateway will work in either case.



CISCO gateway IKE configuration

Start the CISCO PIX device manager (PDM) and select the “IKE→ Policies” category on the VPN tab. Add one or more IKE proposals and select the “Enable NAT traversal” option. We recommend setting the “NAT Keepalive” frequency to 20 seconds.

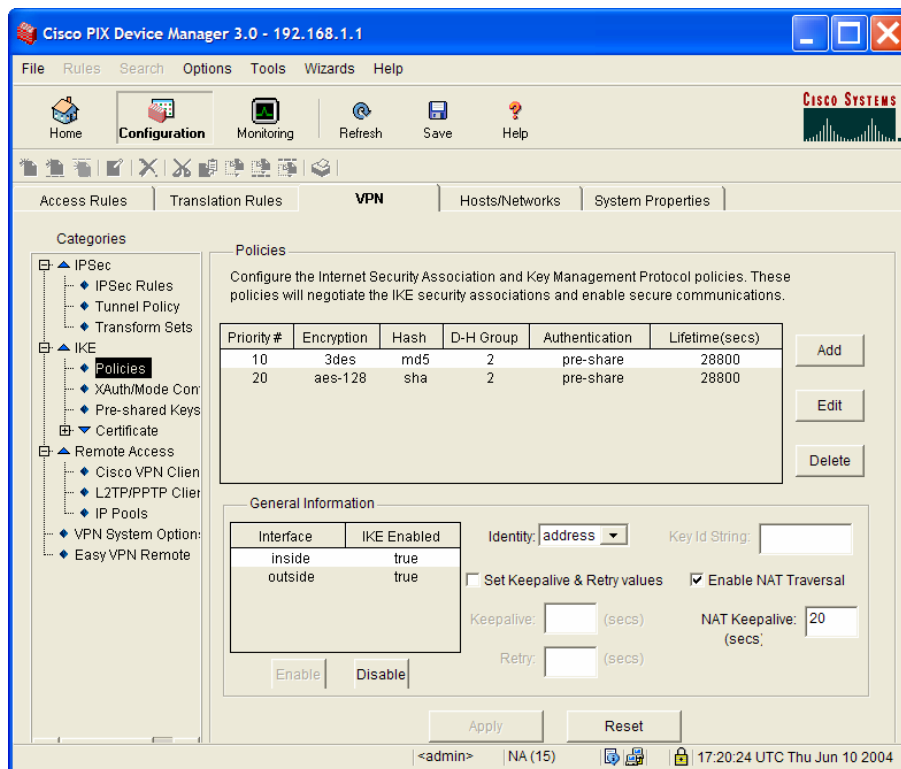


Figure 1: IKE policies.



CISCO gateway IPsec configuration

Before specifying the IPsec proposals, a tunnel policy must be defined. For a remote access VPN, the tunnel policy type should be dynamic. Select the “IPSec→Tunnel Policy” category on the VPN tab and click on “Add” to create a new policy. This example uses ESP-3DES-MD5 with perfect forward security (Diffie-Hellman group 2) and a tunnel lifetime of 8 hours.

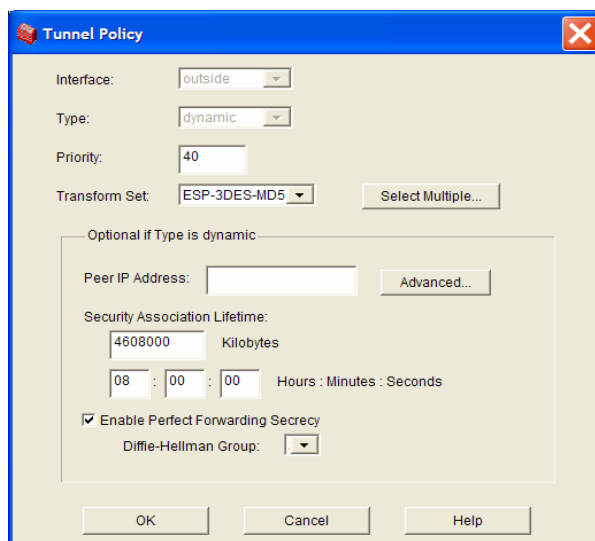
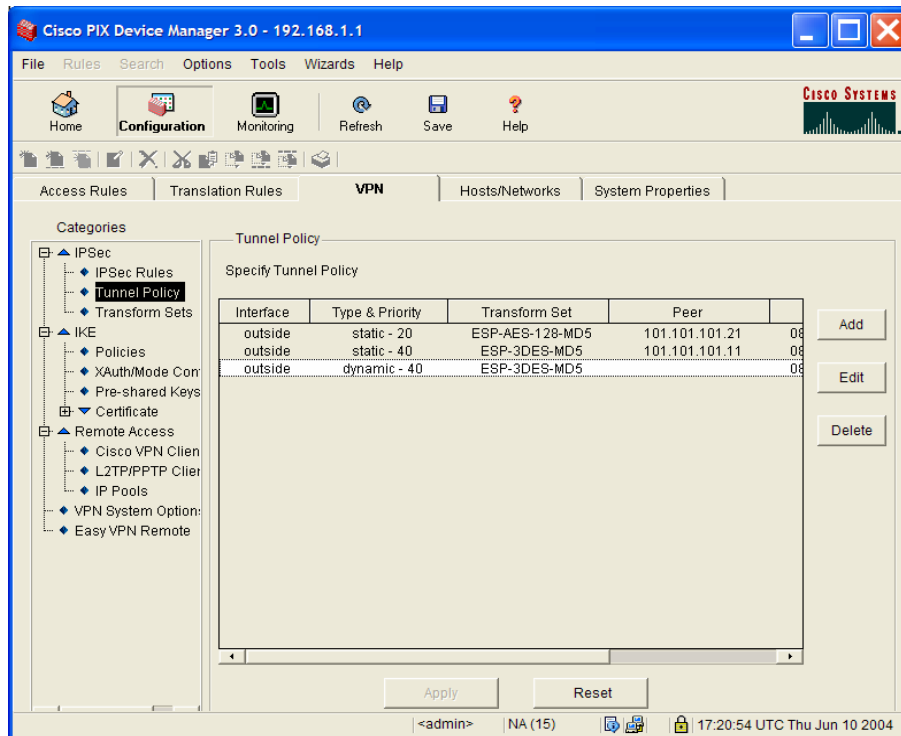


Figure 2: Defining dynamic tunnel policy.



Next, create a new IPsec rule from the local subnet (192.168.1.0/24 in this example) to “any” and attach the dynamic tunnel policy to it.

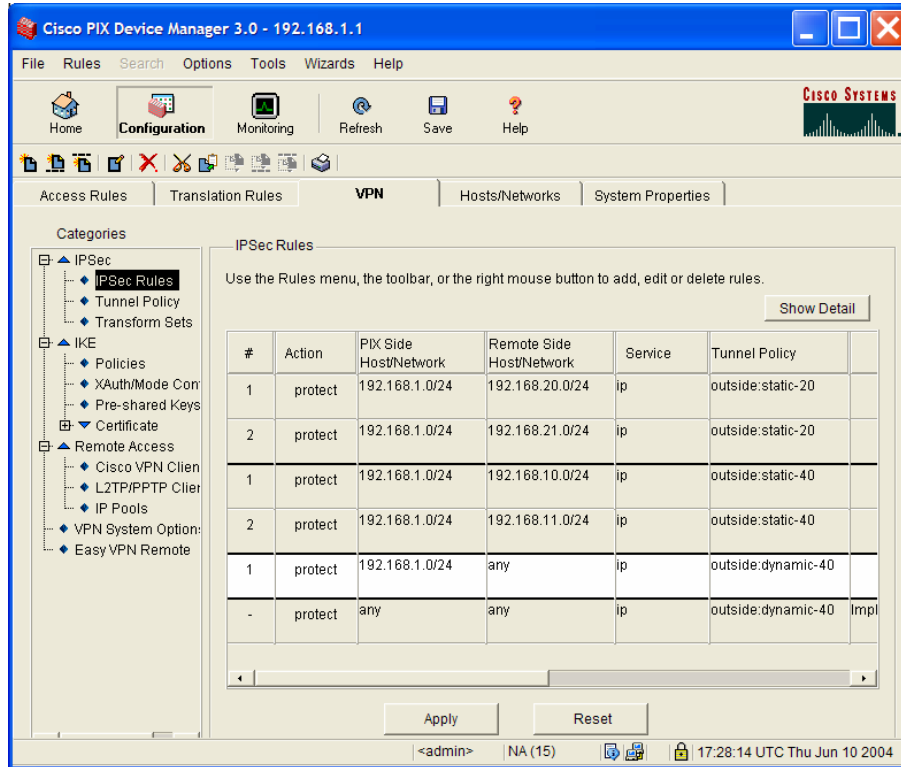


Figure 3: IPsec rules.

Alternatively, one may choose not to create a new IPsec rule and use the “any” to “any” rule instead.



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.

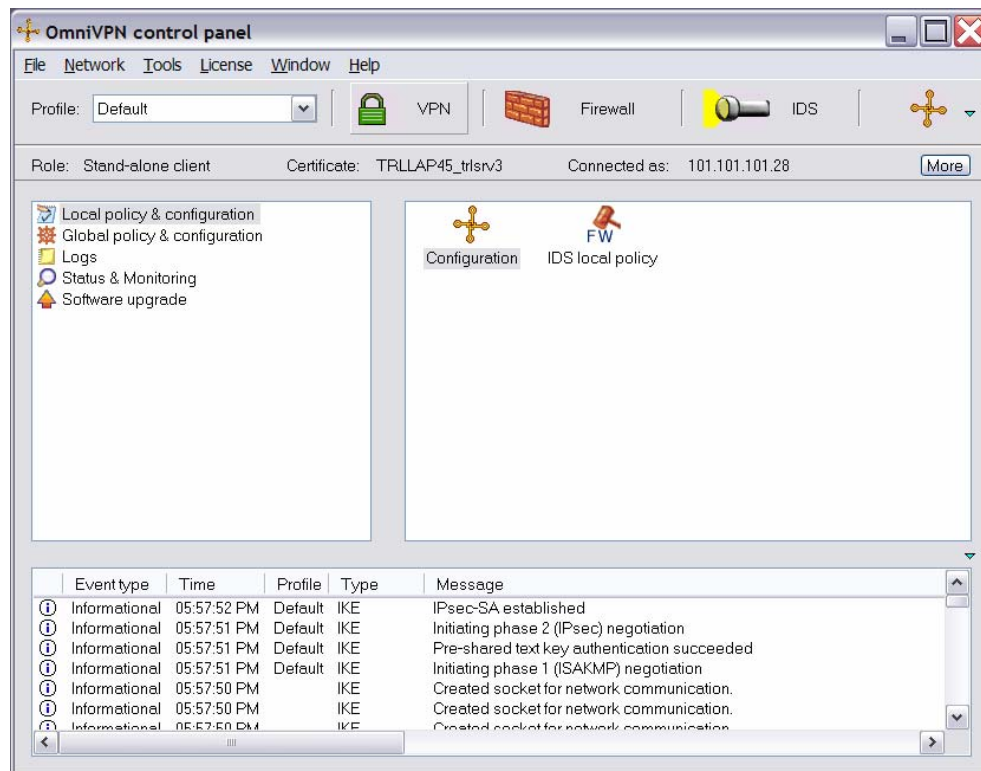


Figure 4: Katana control panel and configuration window



Enter the local (Katana side) and remote (CISCO 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" because the CISCO gateway does not support IKE aggressive mode. In addition, NAT Traversal must be enabled.

For the "Local configuration," enter:

Client ID:	Current IP address of the client (101.101.101.10 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 (101.101.101.10 in this example)

For the "Remote configuration," enter:

Remote ID:	Public IP address of the CISCO gateway (101.101.101.50 in this example)
Subnet:	Subnet behind the CISCO gateway (192.168.50.0 / 24 in this example)
Public IP address:	Public IP address of the CISCO gateway (101.101.101.50 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 Identity Protection mode, and NAT Traversal must be enabled. There are three proposals in this example, but more importantly, there is one proposal that will be accepted by the CISCO gateway, i.e., 3DES-MD5. The lifetime is set to 8 hours. To add more proposals, click the “Add ISAKMP proposal” button.

There is only one IPsec proposal, 3DES-MD5 and perfect forward secrecy 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:

Authenticat...	Diffie-Hell...	Hash algor...	Encryption ...	Key length
Pre-shared t...	MODP 768 ...	MD5	AES-CBC	128
Pre-shared t...	MODP 102 ...	SHA1	3DES-CBC	192
Pre-shared t...	MODP 102 ...	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 alg...	Encryptio...	Key length
HMAC-MD5	3DES	192
- Tunnel lifetime: 8 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.

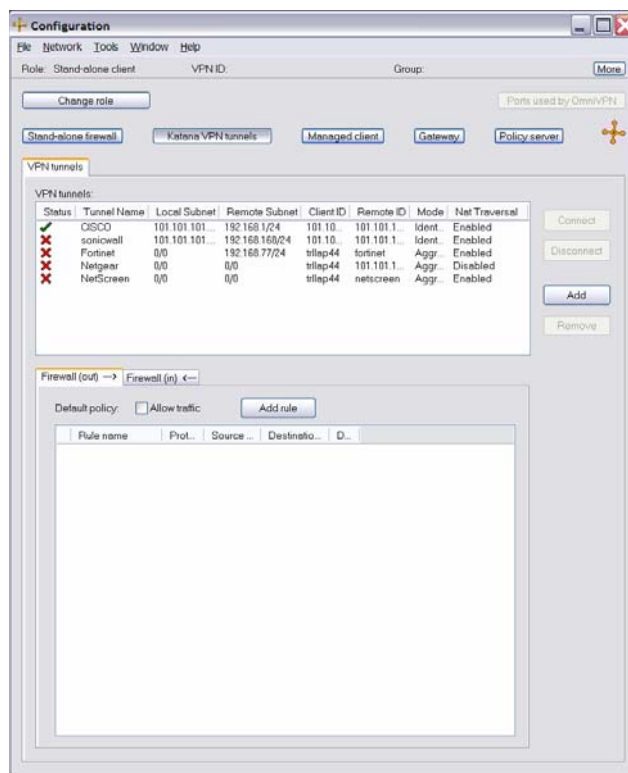


Figure 7: A green checkmark indicates that the tunnel is established.



After establishing a VPN tunnel between the Katana client and the CISCO 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
101.101.101.10	101.101.101.50	0x848734F3	Tunnel	ESP	HMAC-MD5	3DES (192)	06:42:06 PM	02:42:06 AM
101.101.101.50	101.101.101.10	0x0F912661	Tunnel	ESP	HMAC-MD5	3DES (192)	06:42:06 PM	02:42:06 AM

Figure 8: List of existing security associations.