



---

## **OmniVPN/Katana Gateway to CISCO VPN Gateway**

### **Goal**

Configure a VPN tunnel between a Katana/OmniVPN gateway and a CISCO VPN gateway.

### **Method**

The Katana/OmniVPN gateway 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/OmniVPN gateway configuration**

In this example, the Katana/OmniVPN gateway has a public IP address of 101.101.101.11. The subnet behind it is 192.168.11.0/255.255.255.0.



## 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.

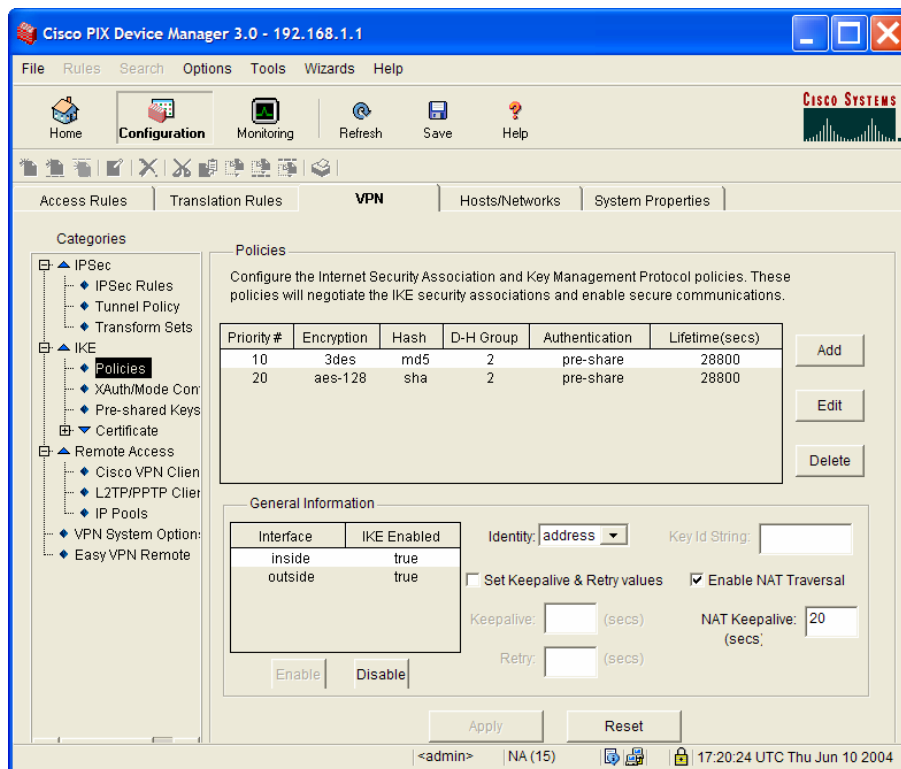


Figure 1: IKE policies.



## CISCO gateway IPsec configuration

Before specifying the IPsec proposals, a tunnel policy must be defined. For a site-to-site VPN, the tunnel policy type should be static. 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.

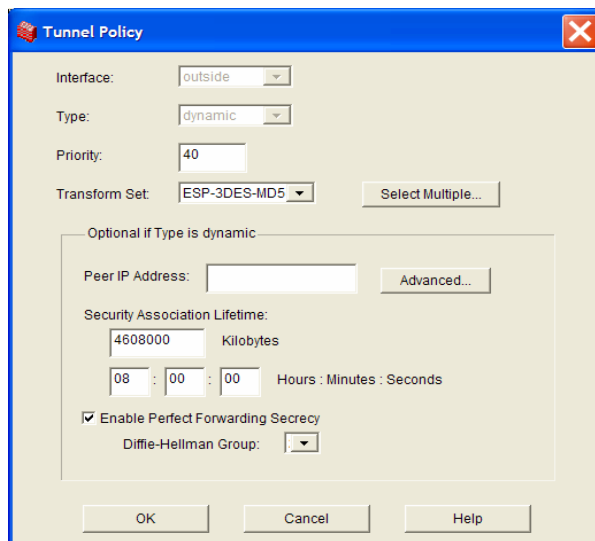
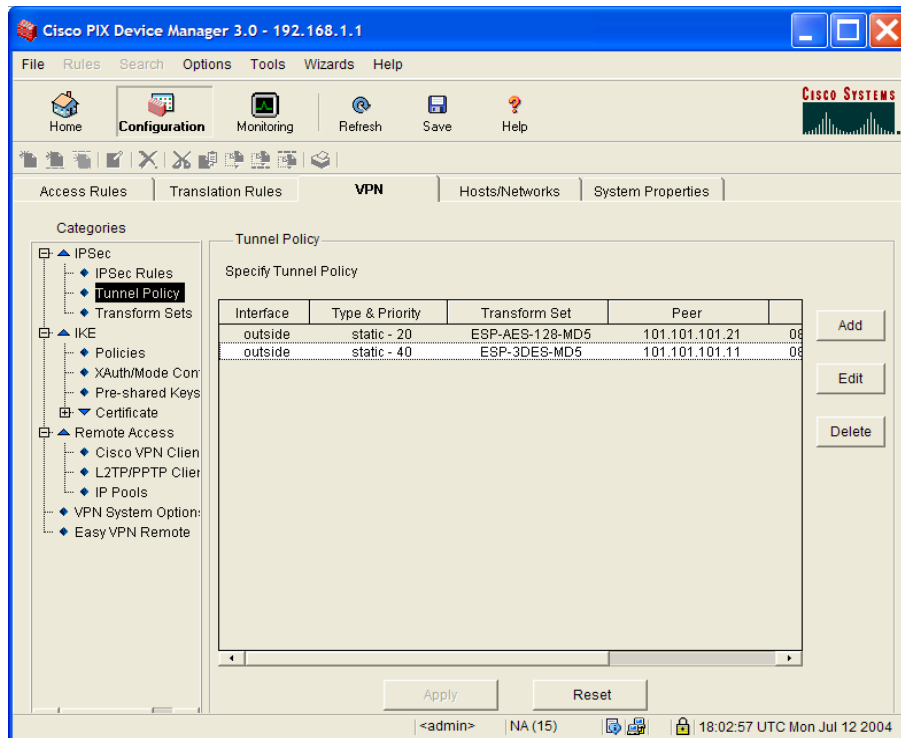


Figure 2: Defining tunnel policy.



Next, create a new IPsec rule from the local subnet (192.168.1.0/24 in this example) to the remote network (192.168.11.0/24 in this example) and attach the static tunnel policy to it.

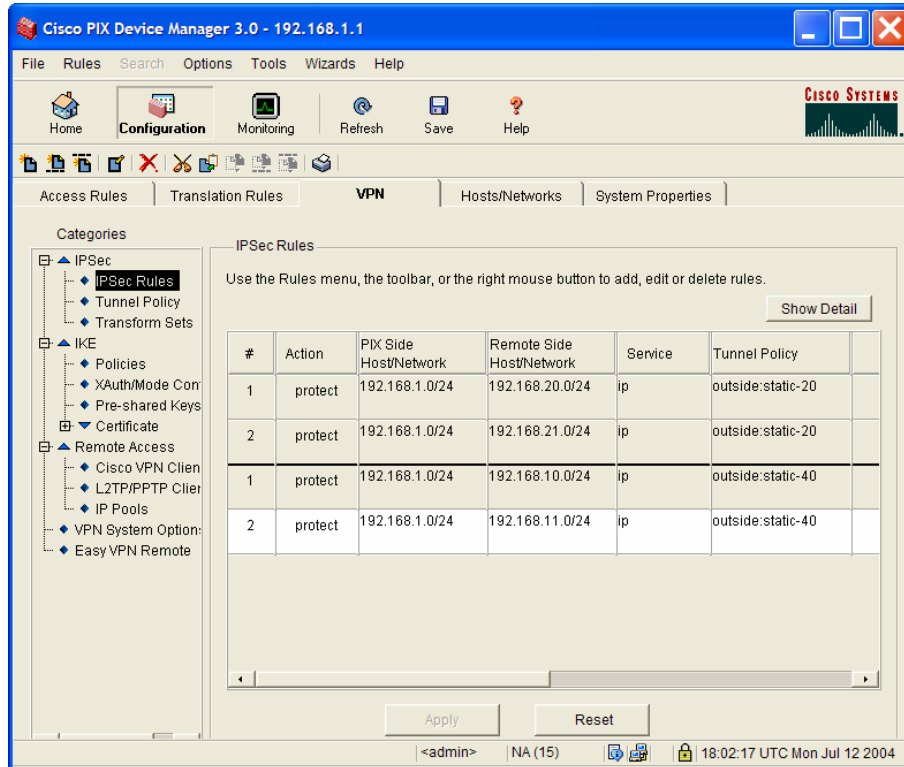


Figure 3: IPsec rules.



## Katana/OmniVPN gateway configuration

The OmniVPN gateway has a public IP address of 101.101.101.11, and its private subnet is 192.168.11.0/255.255.255.0. The policy must show secure communication between the private IP subnet behind the OmniVPN gateway and the private IP subnet behind the CISCO VPN gateway, i.e., the VPN lock icon is green and closed. There are three steps to completely configure the Katana/OmniVPN gateway:

- Define security policy
- Define the VPN (network) topology
- Define the pre-shared text keys

## Security Policy definition

The first step in establishing a VPN connection between the OmniVPN/Katana gateway and CISCO VPN gateway is to define the security policy for the VPN tunnel.

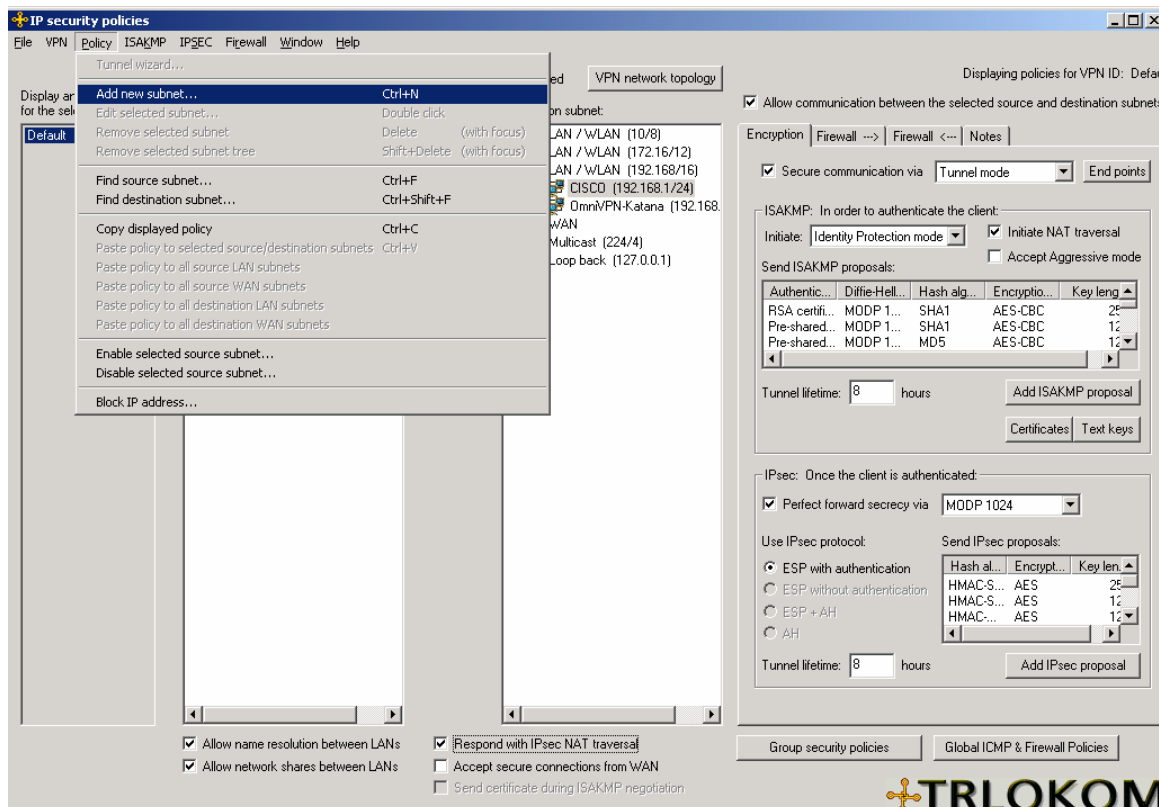


Figure 4: IP Security Policies window

Open the IP Security Policies window by clicking on the “IP security policies” button in the Configuration window. If you expect to have different security policies for each VPN



tunnel, you can create a subnet for each VPN site, but this may not be necessary. For example, if you have 192.168/16 to 10/8 as secure communication using IPsec tunnel mode, then there is no need to create separate subnets for 192.168.10/24 and 10.7/16 to secure communication using IPsec tunnel mode. It is good to minimize the number of created subnets because it keeps the security policy database compact.

If it is necessary to create a new subnet, select the “Add new subnet...” option from the Policy menu.

The image shows a dialog box titled "Define subnet" with a close button (X) in the top right corner. It contains three input fields: "Address:" with the value "192 . 168 . 1 .", "Mask:" with the value "255 . 255 . 255 . 0", and "Name of subnet:" with the value "CISCO". At the bottom, there are two buttons: "OK" and "Cancel".

Figure 5: Adding a new subnet in the policy editor.

The above figure shows the dialog box for creating a new subnet. Enter the subnet behind the CISCO VPN gateway and give the subnet a name to help you easily identify it later on. In this case the IP subnet is 192.168.1.0/24 and we have named it “CISCO.”



To view the policy for communication between the two subnets, select one of the two subnets in the “Source subnet” column and the other in the “Destination subnet” column. If the exact subnet is not there, select the one that contains the subnet in question.

On the right hand side of the policy editor, the encryption and firewall policies are shown for communication between the two subnets. If secure communication is desired, the lock icon should be closed and green. Select the mode to be “Tunnel mode.”

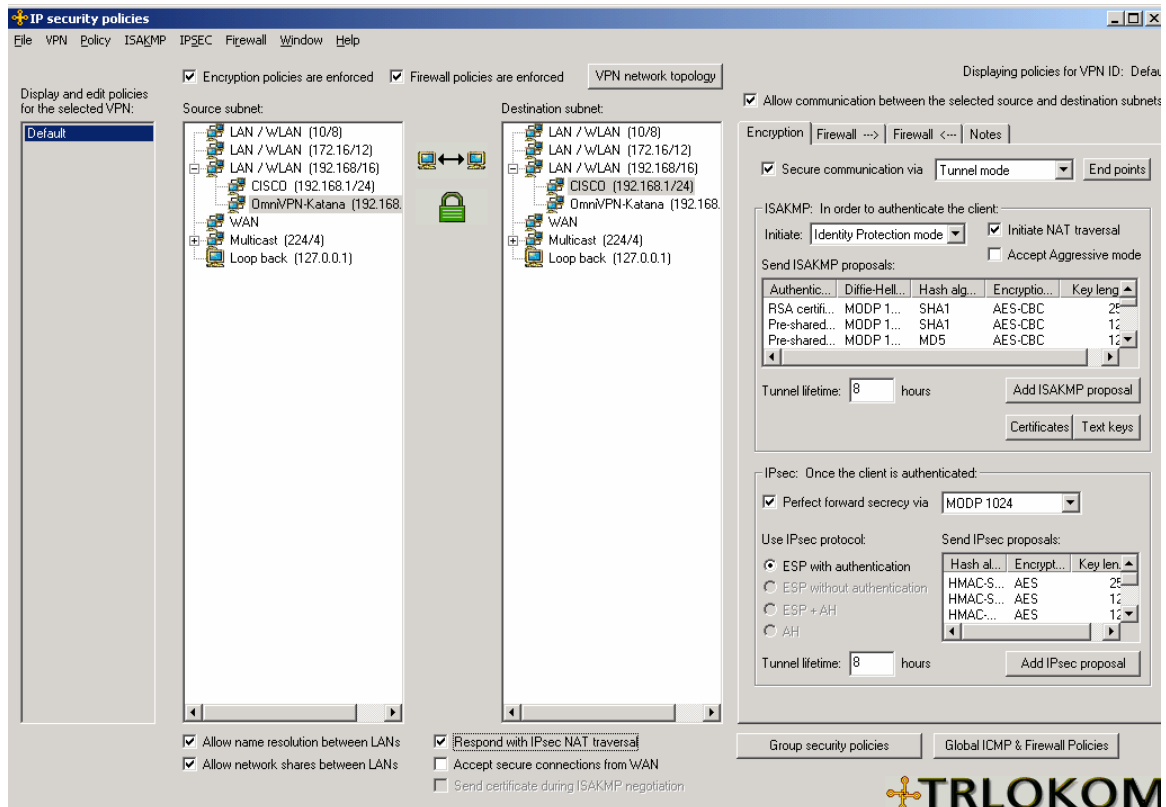


Figure 6: Tunnel policy between the two subnets.



If the policy requires secure communication, the user will be able to edit the IKE/ISAKMP and IPsec proposals. By default, several ISAKMP proposals are added, so it is typically not necessary to add extra proposals. To add a new proposal, click the “Add ISAKMP proposal” button. This proposal dictates how the two gateways will authenticate each other.

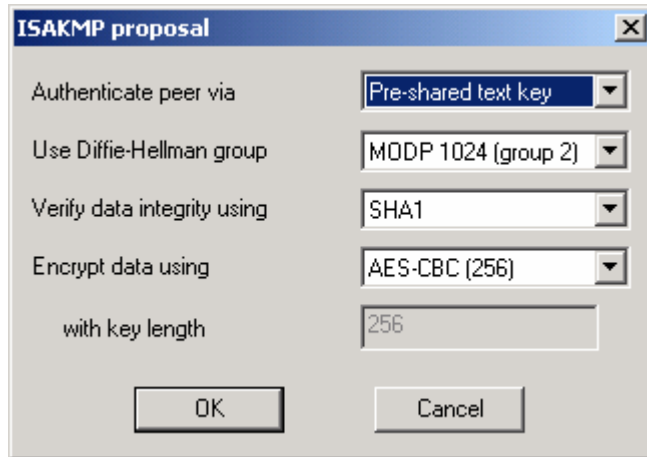


Figure 7: ISAKMP proposal

The proposal parameters are:

Authenticate peer via:	“Pre-shared text key”
Use Diffie-Hellman group:	MODP 1024(group 2)
Verify data integrity using:	SHA1 or MD5
Encrypt data using:	3DES or AES

The ISAKMP proposal added here should match one of the proposals at the CISCO VPN gateway.

The ISAKMP security association lifetime is common for all proposals and we recommend setting it to 8 hours or more. The two other flags are:

Initiate NAT-traversal:	Necessary if remote site is behind a NAT
Accept Aggressive mode:	Necessary if road warriors will connect to this VPN gateway.



Next, configure the IPsec proposals that dictate how the data will be encrypted. By default, several proposals are added, so it is typically not necessary to add extra proposals. To add a specific proposal, click the “Add IPsec proposal” button.

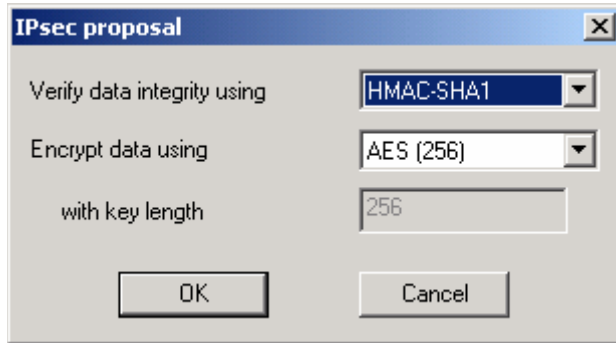


Figure 8: IPsec proposal dialog box.

The proposal parameters are:

Verify data integrity using: SHA1 or MD5  
Encrypt data using: 3DES or AES

The lifetime and PFS are common to all IPsec proposals. We recommend using PSF via MODP 1024 (Diffie-Hellman group 2) and setting the lifetime to 8 hours.



## VPN Topology definition

The second part of the VPN tunnel is the VPN topology. This is necessary for defining the VPN tunnel end-points. It tells the Katana/OmniVPN gateway the public IP address of each subnet. For each subnet that is behind a remote gateway, a global route (or VPN topology entry) must be created.

Figure 9: Global route.

To add a new entry to the VPN topology, click the “End points” button on the Encryption tab in the IP Security Policies window or open the VPN Topology window and edit the global routes. Figure 9 shows the dialog box for defining a global route.

Subnet:	Subnet behind the CISCO VPN gateway (192.168.1.0/24 in this example)
Public address:	Public IP address (or domain name) of the CISCO VPN gateway (101.101.101.50 in this example)
ID type:	ID type to be used by IKE (“Address” in this example)
WAN bandwidth:	Bandwidth to the Internet. This is useful when using the QoS features of OmniVPN.
Supports End-to-End mode	Leave unchecked



## Pre-Shared Text Keys

As part of VPN tunnel establishment, the Katana/OmniVPN gateway and the CISCO gateway will authenticate each other. This authentication is based on a pre-shared secret. To enter a pre-shared secret, click the “Text keys” button in the IP Security Policies window and select the “Add new key...” option from the Key menu.

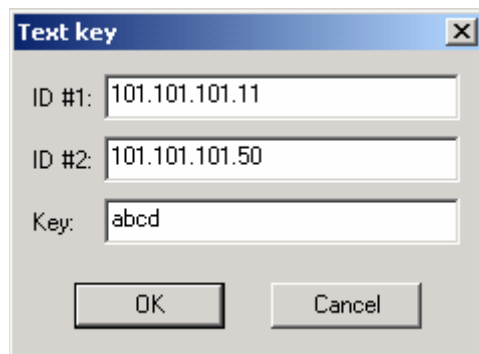


Figure 10: Entering a pre-shared secret.

The above figure shows the dialog box to enter a pre-shared secret.

- ID #1: OmniVPN/Katana gateway ID  
(101.101.101.11 in this example)
- ID #2: CISCO VPN gateway ID  
(101.101.101.50 in this example)
- Key: The pre-shared secret  
(“abcd” in this example)



The IP address-based pre-shared secret between the OmniVPN/Katana gateway and the CISCO VPN gateway appears in the list of “Pre-shared text keys.”

The screenshot shows a window titled "Pre-shared text keys" with a menu bar containing "File", "Key", "Window", and "Help". Below the menu bar, it says "Displaying policies for VPN ID: Default". The main content is a table with three columns: "Address #1", "Address #2", and "Key".

Address #1	Address #2	Key
101.101.101.70	101.101.101.71	blbudfajap
101.101.101.70	101.101.101.80	jhzymloqzf
101.101.77.77	101.101.88.88	szjihchztk
road_warrior	trlsrv3_trlsrv3	abcd
101.101.101.11	101.101.101.50	abcd

Figure 11: The pre-shared keys list.



After establishing a VPN tunnel between the OmniVPN/Katana gateway 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.

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 12: List of existing security associations.