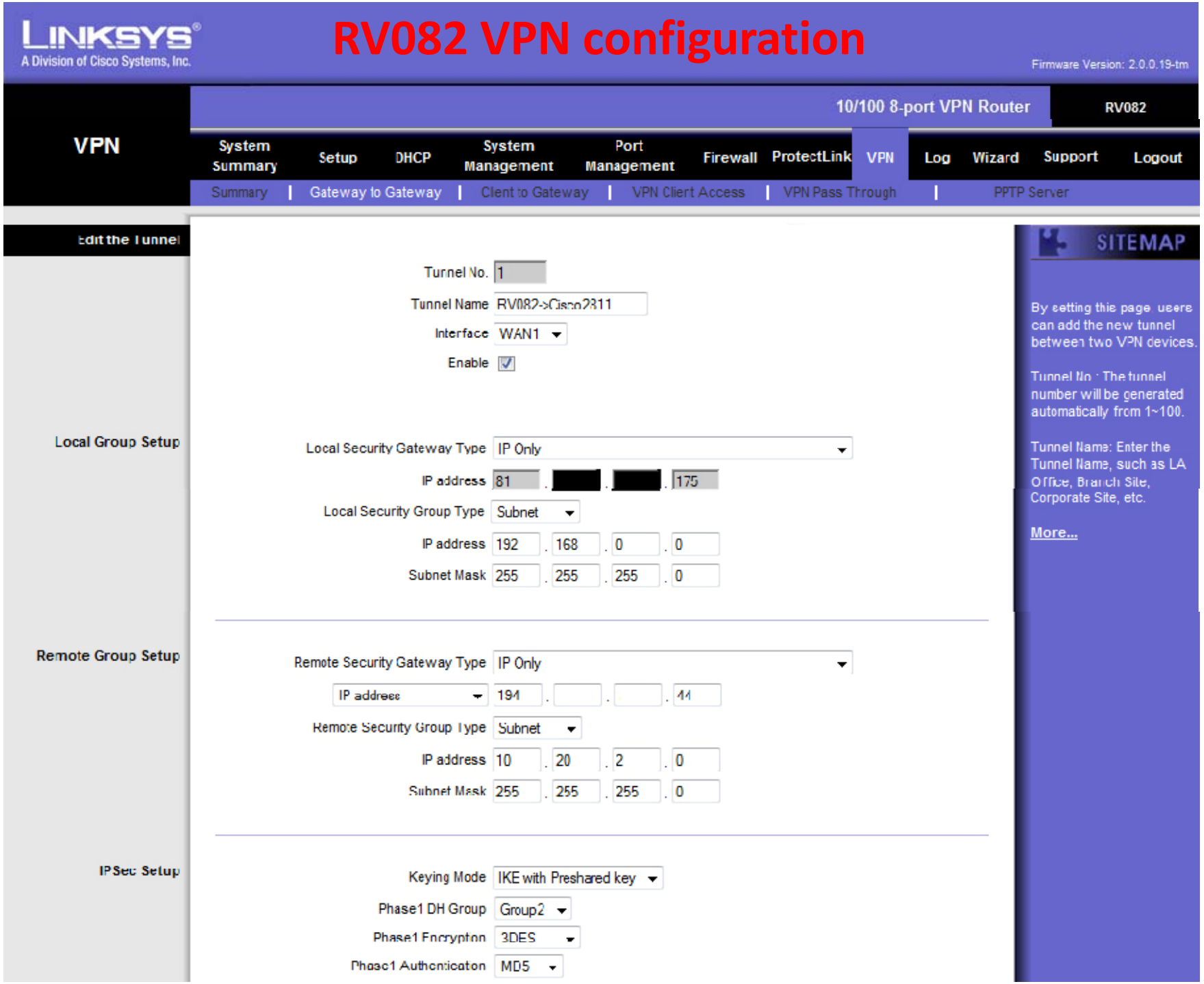
RV082 VPN configuration



IPSec Setup

Keying Mode: IKE with Preshared key

Phase1 DH Group: Group2

Phase1 Encryption: 3DES

Phase1 Authentication: MD5

Phase1 SA Life Time: 28800 seconds

Perfect Forward Secrecy: ☑

Phase2 DH Group: Group2

Phase2 Encryption: 3DES

Phase2 Authentication: MD5

Phase2 SA Life Time: 28800 seconds

Preshared Key: [redacted]

Advanced -

Advanced

☐ Aggressive Mode

☐ Compress (Support IP Payload Compression Protocol(IPComp))

☑ Keep-Alive

☐ AH Hash Algorithm: MD5

☐ NetBIOS broadcast

☐ NAT Traversal

☑ Dead Peer Detection (DPD) Interval: 10 seconds

☐ Tunnel Backup:

Remote Backup IP Address: 0 . 0 . 0 . 0

Local Interface: WAN1

VPN Tunnel Backup Idle Time: 30 sec. (Range:30~999 sec)

☐ Split DNS :

DNS1: . . .

DNS2: . . .

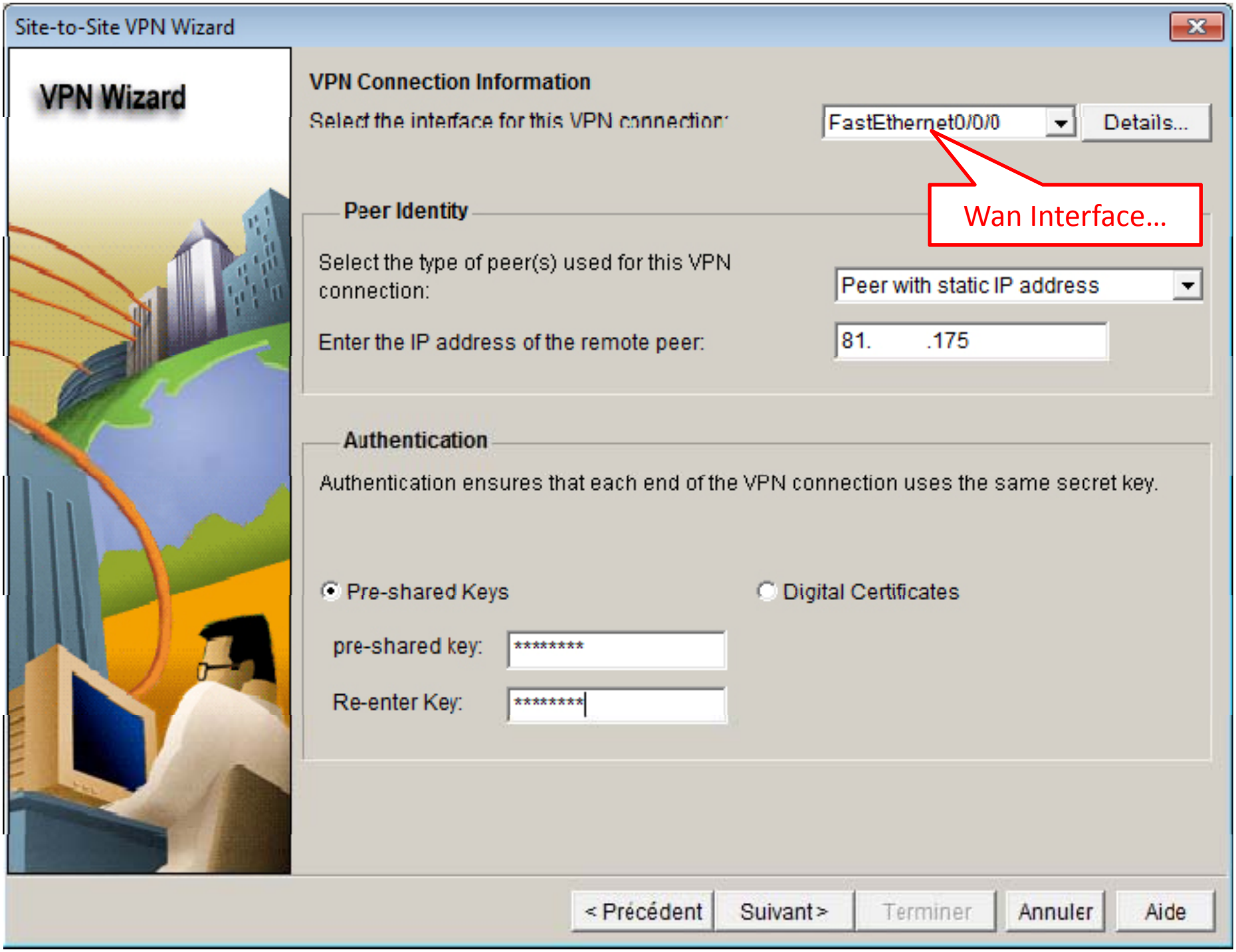
Domain Name 1: 2:

3: 4:

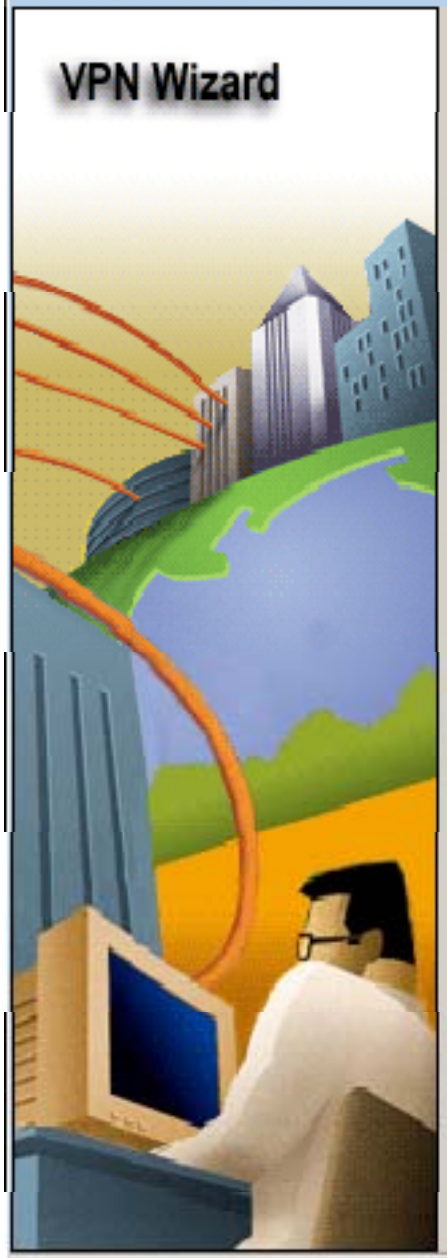
Save Settings | Cancel Changes

Cisco Systems

Cisco 2811 VPN configuration (with SDM Wizard)


Site-to-Site VPN Wizard
VPN Wizard
VPN Connection Information
Select the interface for this VPN connection:
FastEthernet0/0/0
Details...
Wan Interface...
Peer Identity
Select the type of peer(s) used for this VPN connection:
Peer with static IP address
Enter the IP address of the remote peer:
81. .175
Authentication
Authentication ensures that each end of the VPN connection uses the same secret key.
Pre-shared Keys
Digital Certificates
pre-shared key:
****
Re-enter Key:
****
< Précédent
Suivant >
Terminer
Annuler
Aide

Site-to-Site VPN Wizard



IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	SDM Default
	2	3DES	MD5	group2	PRE_SHARE	User Defined

Add... Edit...

Add IKE Policy

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

Encryption: 3DES

D-H Group: group2

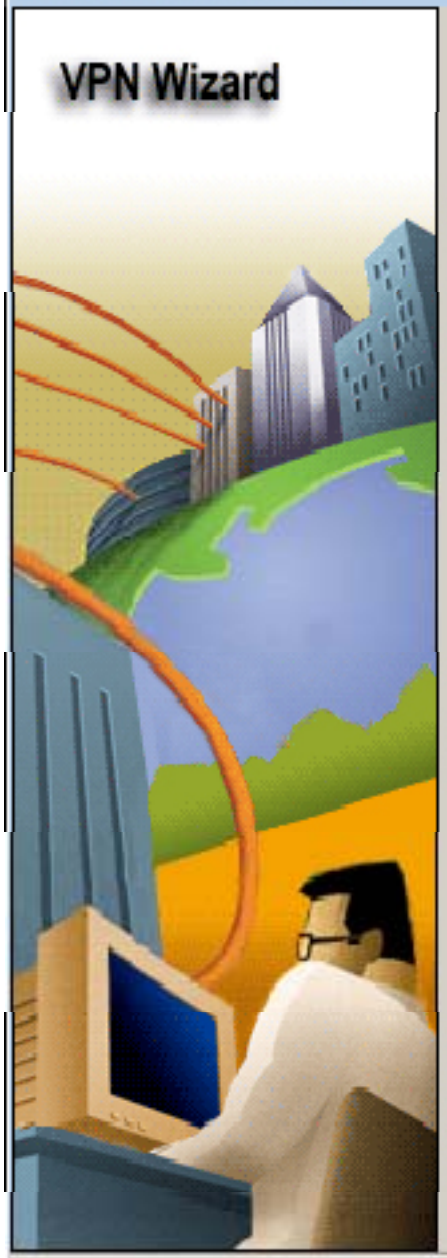
Hash: MD5

Lifetime: 8 0 0 HH:MM:SS

OK Cancel Help

< Précédent Suivant > Terminer Annuler Aide

Site-to-Site VPN Wizard



Transform Set

A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must communicate, the remote device must be configured with the same transform set as the one selected below.

Click the Add... button to add a new transform set.

Select Transform Set:

2811 RV082

Details of the specified transform

Name	ES
2811-RV082	ESP

Add... Edit...

Add Transform Set

Name: 2811-RV082

Data integrity with encryption (ESP)

Integrity Algorithm: ESP_MD5_HMAC

Encryption Algorithm: ESP_3DES

<< Hide Advanced

Data and address integrity without encryption (AH)

Integrity Algorithm: -Select an entry

Mode

Tunnel (Encrypt data and IP header)

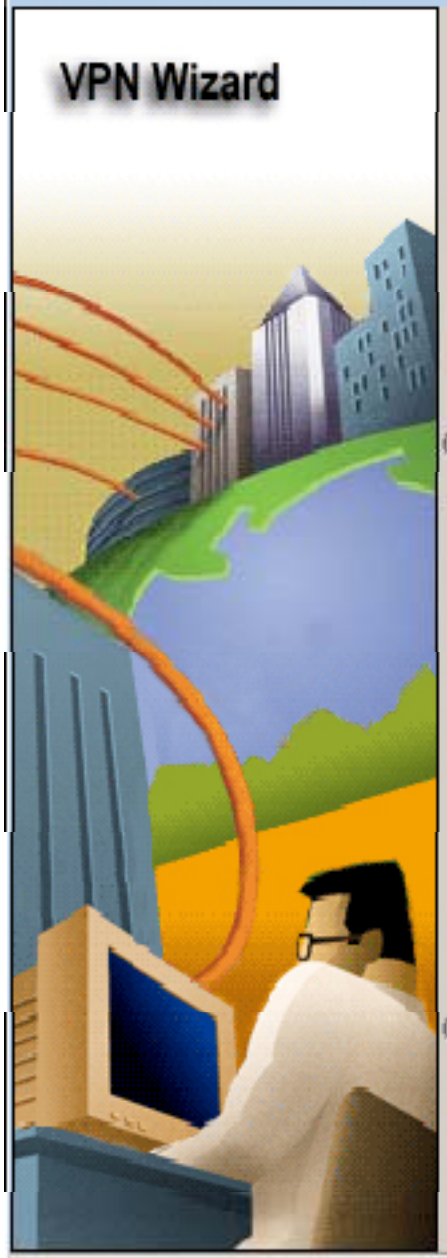
Transport (Encrypt data only)

IP Compression (COMP-LZS)

OK Cancel Help

< Précédent Suivant > Terminer Annuler Aide

Site-to-Site VPN Wizard



Traffic to protect

IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

(•) Protect all traffic between the following subnets

Local Network

Enter the IP address and subnet mask of the network where IPSec traffic originates.

IP Address: 10.20.2.0

Subnet Mask: 255.255.255.0 or 24

Remote Network

Enter the IP Address and Subnet Mask of the destination Network.

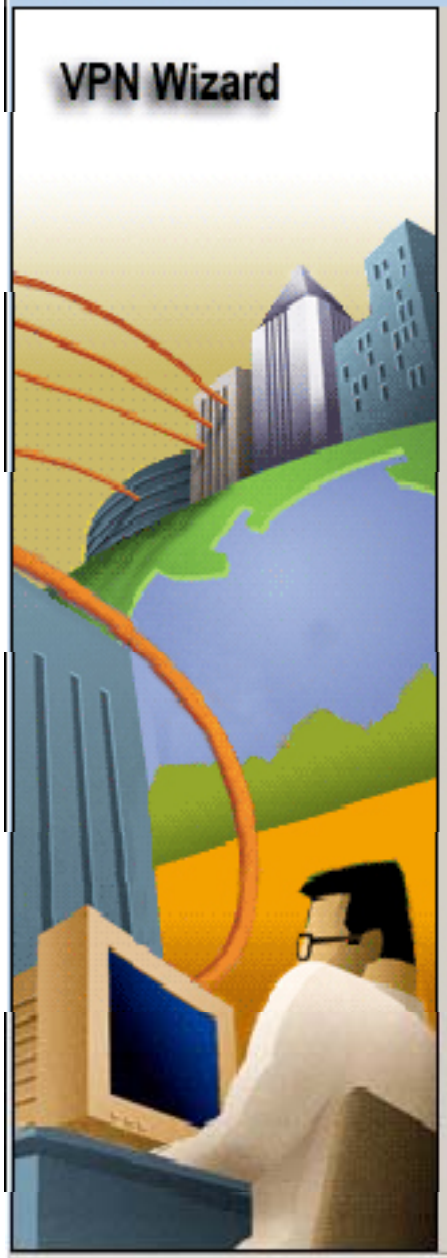
IP Address: 192.168.0.0

Subnet Mask: 255.255.255.0 or 24

( ) Create/Select an access-list for IPSec traffic

< Précédent | Suivant > | Terminer | Annuler | Aide

Site-to-Site VPN Wizard



Summary of the Configuration

Click Finish to deliver the configuration to the router.

Interface:FastEthernet0/0/0
Peer Device:81. .175
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

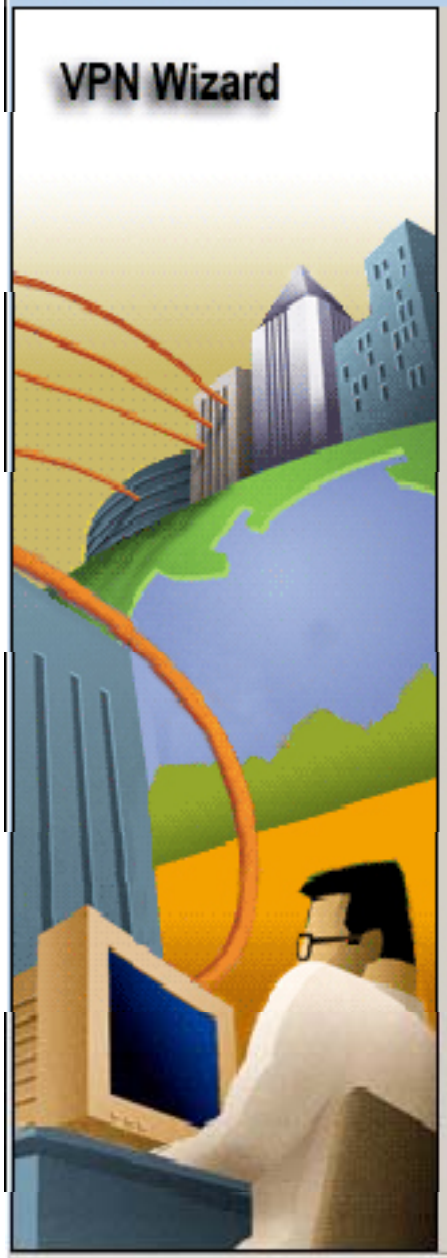
Hash	DH Group	Authentication	Encryption
MD5	group2	PRE_SHARE	3DES
SHA_1	group2	PRE_SHARE	3DES

Transform Sets:
Name:2811-RV082
ESP Encryption:ESP_3DES
ESP Integrity:ESP_MD5_HMAC
Mode:TUNNEL

☐ Test VPN connectivity after configuring.

< Précédent | Suivant > | Terminer | Annuler | Aide

Site-to-Site VPN Wizard



Summary of the Configuration

Click Finish to deliver the configuration to the router.

Interface:FastEthernet0/0/0
Peer Device:81. .175
Authentication Type : Pre-shared key
pre-shared key:******

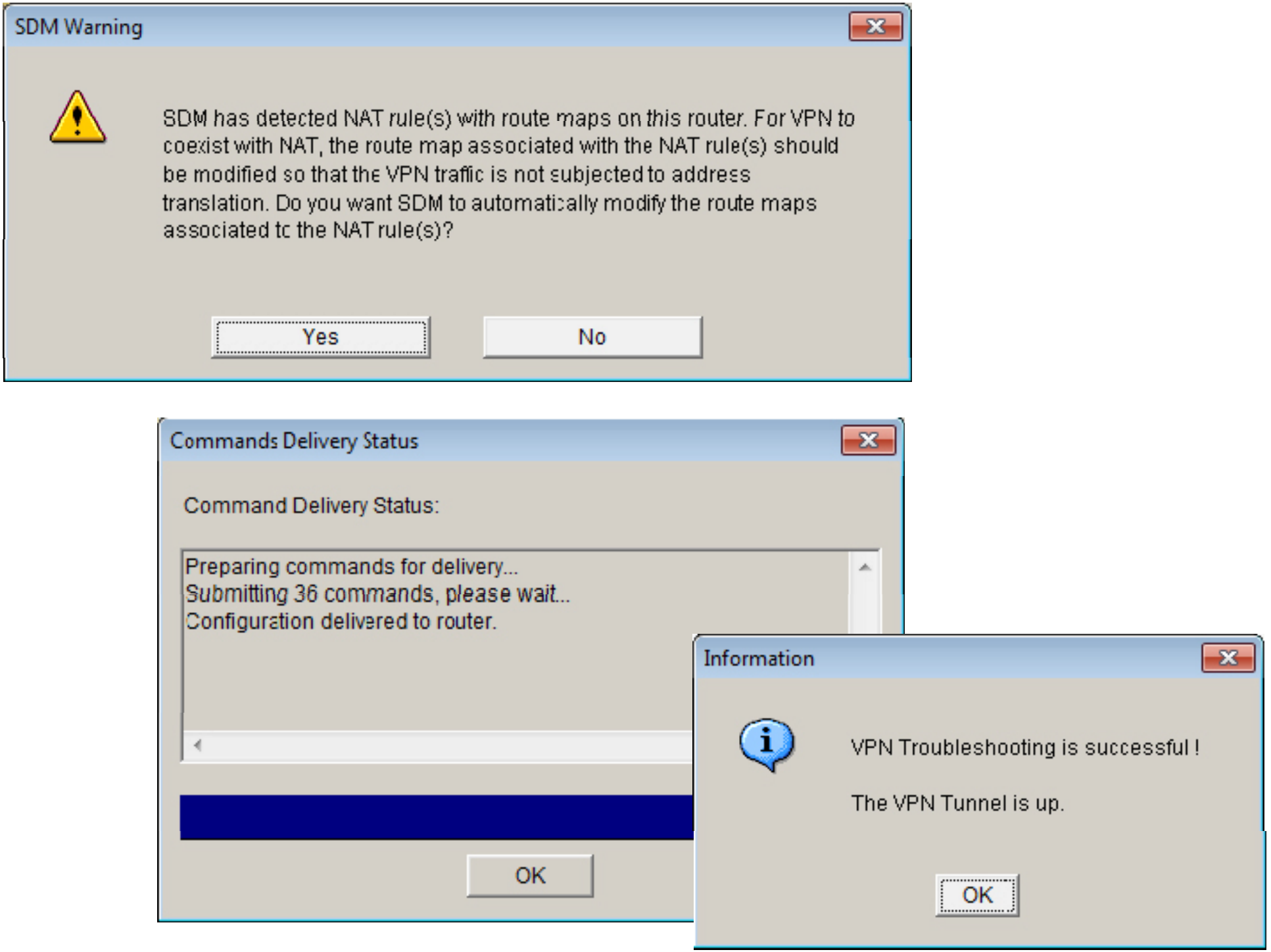
IKE Policies:

Hash	DH Group	Authentication	Encryption
MD5	group2	PRE_SHARE	3DES
SHA_1	group2	PRE_SHARE	3DES

Transform Sets:
Name:2811-RV082
ESP Encryption:ESP_3DES
ESP Integrity:ESP_MD5_HMAC
Mode:TUNNEL

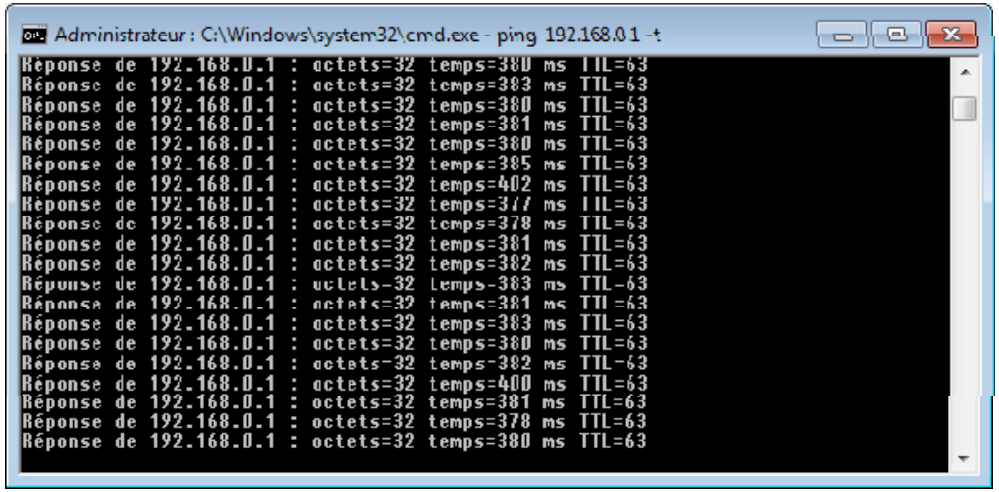
☐ Test VPN connectivity after configuring.

< Précédent | Suivant > | Terminer | Annuler | Aide

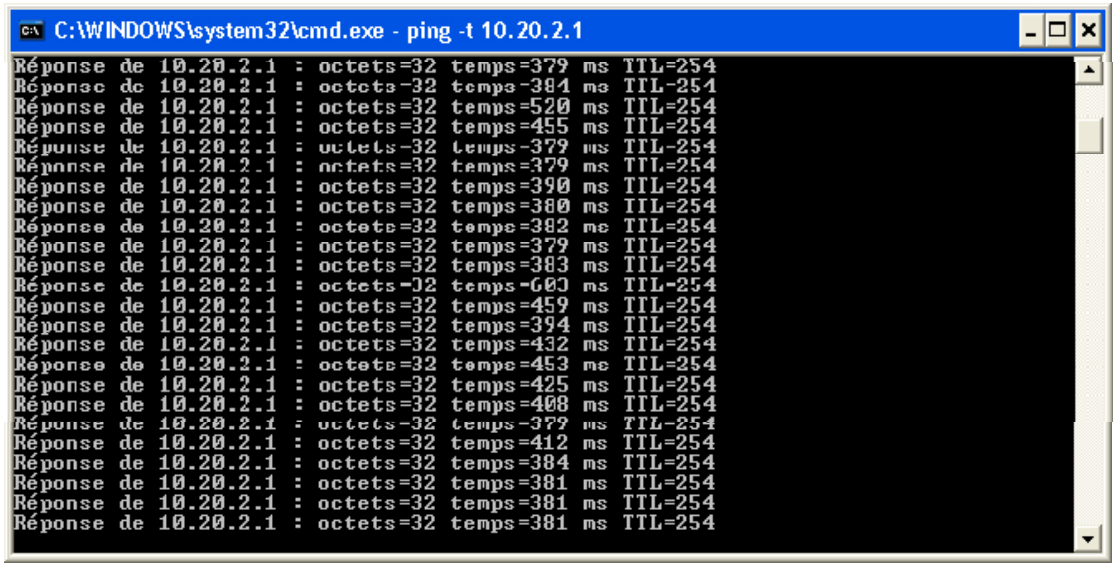

SDM Warning
SDM has detected NAT rule(s) with route maps on this router. For VPN to coexist with NAT, the route map associated with the NAT rule(s) should be modified so that the VPN traffic is not subjected to address translation. Do you want SDM to automatically modify the route maps associated to the NAT rule(s)?
Yes
No
Commands Delivery Status
Command Delivery Status:
Preparing commands for delivery...
Submitting 36 commands, please wait...
Configuration delivered to router.
OK
Information
VPN Troubleshooting is successful !
The VPN Tunnel is up.
OK

Ping test at T = 0 minutes

Cisco 2811 side

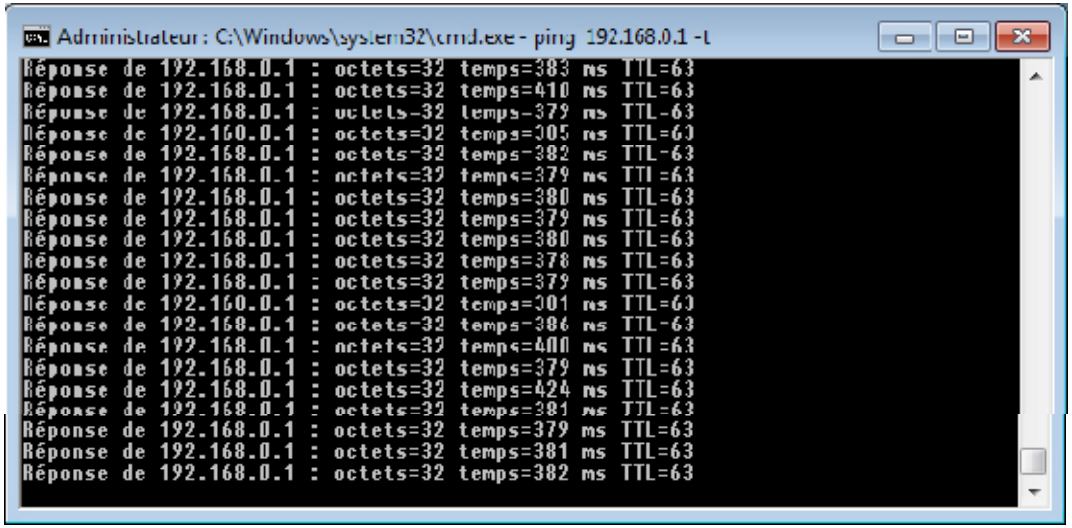


RV082 side

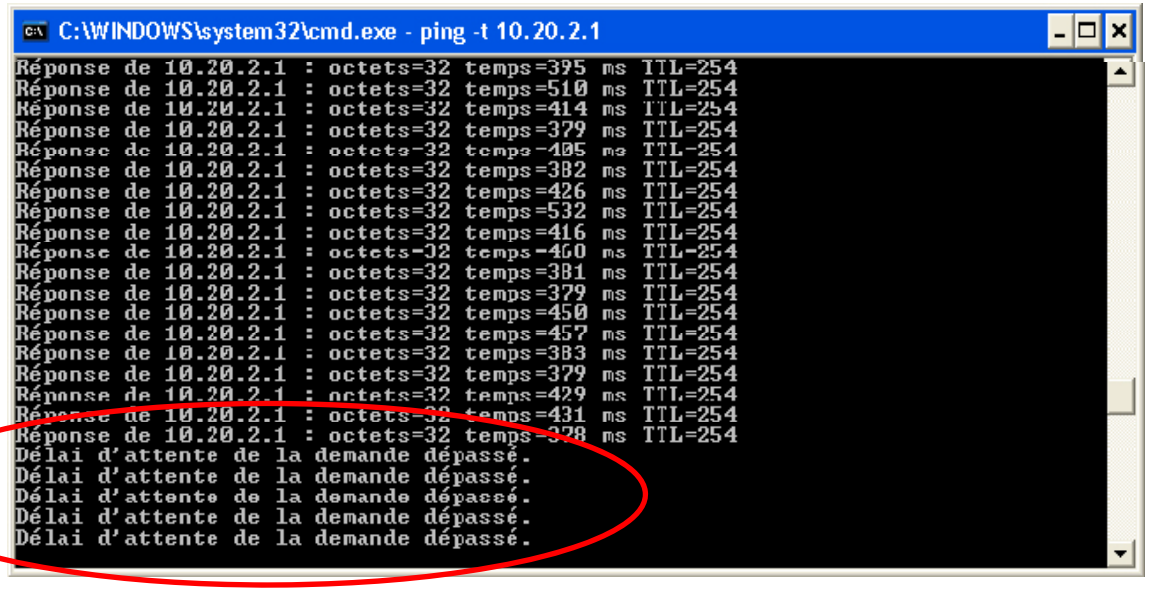


Ping test at T = 3 minutes !!!!

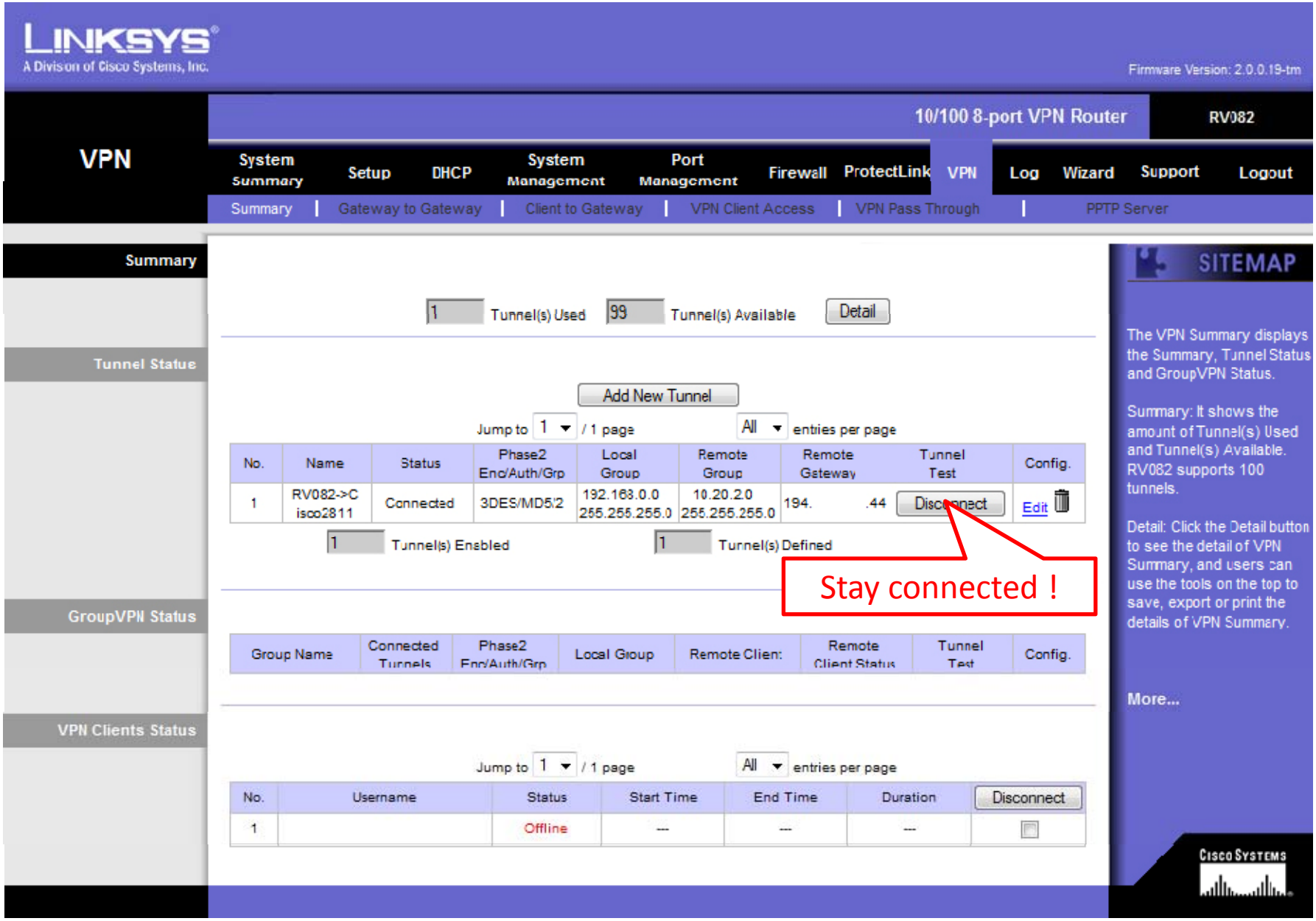
Cisco 2811 side !!!!



RV082 side !!??



RV082 VPN Status at T = 3 minutes



If I want to use my VPN tunnel again, I must restart it (only from the RV082) and only for 3 minutes again !!