

VPN

- System Summary
 - Setup
 - DHCP
 - System Management
 - Port Management
 - Firewall
 - ProtectLink
 - VPN
 - Log
 - Wizard
 - Support
 - Logout
- Summary | Gateway to Gateway | Client to Gateway | VPN Client Access | VPN Pass Through | PPTP Server

Edit the Tunnel

Tunnel No.

Tunnel Name

Interface

Enable

Local Group Setup

Local Security Gateway Type

IP address . . .

Local Security Group Type

IP address . . .

Subnet Mask . . .

Remote Group Setup

Remote Security Gateway Type

IP address . . .

Remote Security Group Type

IP address . . .

Subnet Mask . . .

IPSec Setup

Keying Mode

Phase1 DH Group

Phase1 Encryption

Phase1 Authentication

SITEMAP

By setting this page users can add the new tunnel between two VPN devices.

Tunnel No: The tunnel number will be generated automatically from 1~100.

Tunnel Name: Enter the Tunnel Name, such as LA Office, Branch Site, Corporate Site, etc.

[More...](#)

IPSec Setup

Keying Mode IKF with Preshared key

Phase1 DH Group Group2

Phase1 Encrypton 3DES

Phase1 Authenticon MD5

Phase1 SA Life Time 28800 seconds

Perfect Forward Secrecy

Phase2 DH Group Group2

Phase2 Encrypton 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 2811 VPN configuration (with SDM 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 >

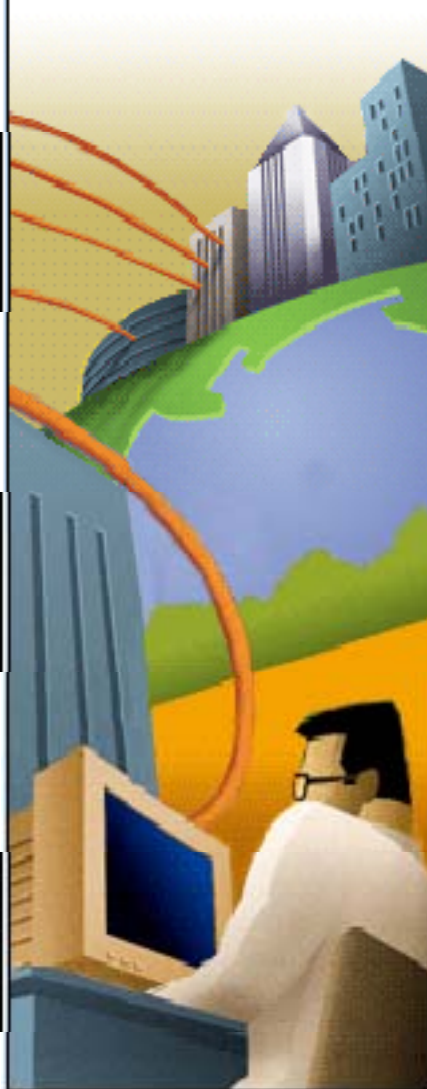
Terminer

Annuler

Aide



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	FRE_SHARE	SDM Default
	2	3DES	MD5	group2	FRE_SHARE	User Defined

Add... Edit...

Add IKE Policy X

Configure IKE Policy

Priority: <input type="text" value="2"/>	Authentication: <input type="text" value="PRE_SHARE"/>
Encryption: <input type="text" value="3DES"/>	D-H Group: <input type="text" value="group2"/>
Hash: <input type="text" value="MD5"/>	Lifetime: <input type="text" value="8"/> <input type="text" value="0"/> <input type="text" value="0"/> H:MM:SS

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 have the same transform set selected below.

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

Select Transform Set:

2811 RV082

Details of the specified transform set:

Name	ESP
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 >

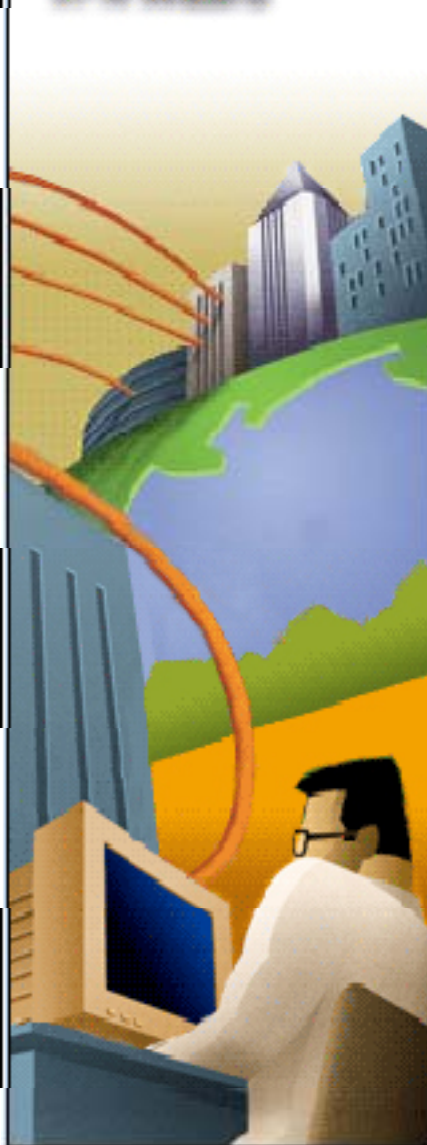
Terminer

Annuler

Aide



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:

Subnet Mask:

or 24



Remote Network

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

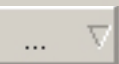
IP Address:

Subnet Mask:

or 24



- Create/Select an access-list for IPSec traffic



< Précédent

Suivant >

Terminer

Annuler

Aide

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

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.

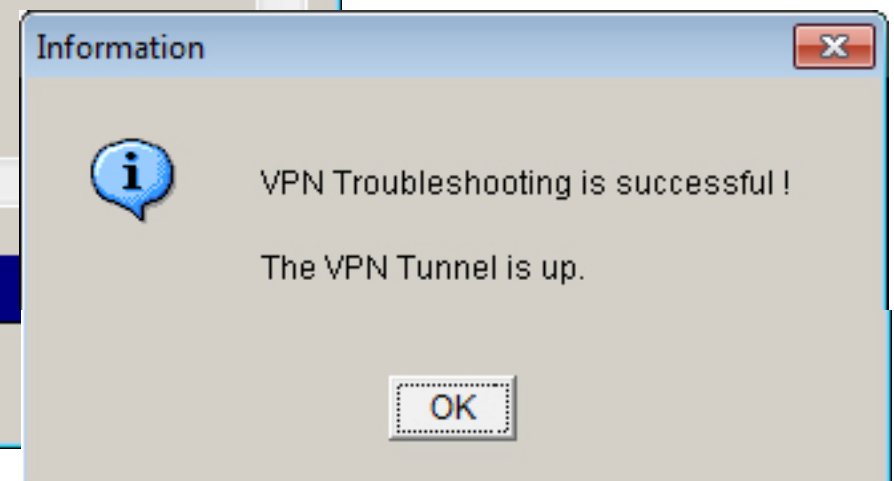
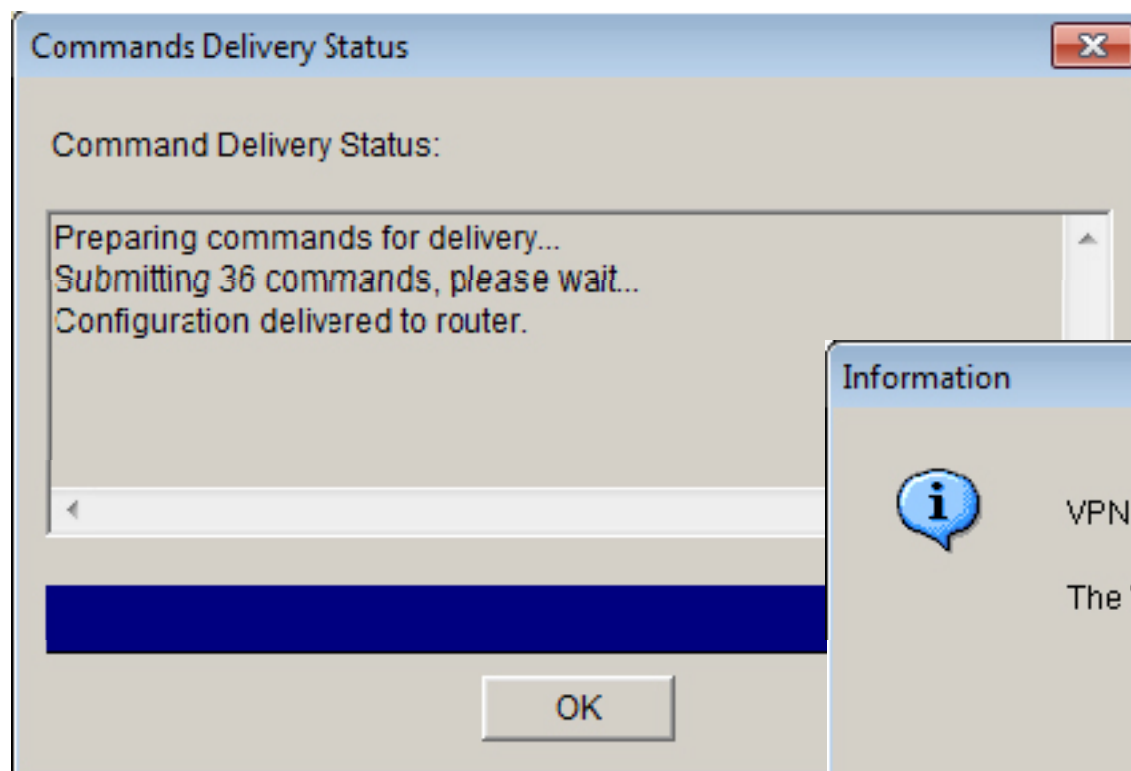
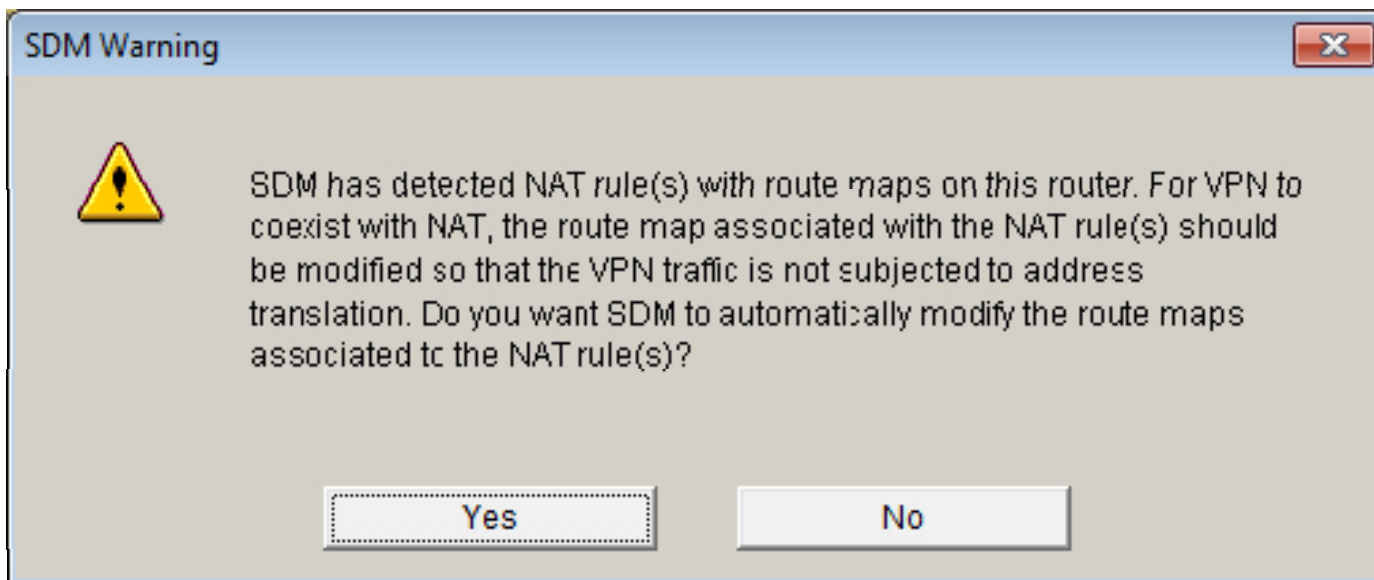
< Précédent

Suivant >

Terminer

Annuler

Aide



Ping test at T = 0 minutes

Cisco 2811 side

```
Administrateur : C:\Windows\system32\cmd.exe - ping 192.168.0.1 -t
Réponse de 192.168.0.1 : octets=32 temps=380 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=383 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=380 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=381 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=380 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=385 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=402 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=377 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=378 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=381 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=382 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=383 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=381 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=383 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=380 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=382 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=400 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=381 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=378 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=380 ms TTL=63
```

RV082 side

```
C:\WINDOWS\system32\cmd.exe - ping -t 10.20.2.1
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=384 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=520 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=455 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=390 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=380 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=382 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=383 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=600 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=459 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=394 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=432 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=453 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=425 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=408 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=412 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=384 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=381 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=381 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=381 ms TTL=254
```

Ping test at T = 3 minutes !!!!

Cisco 2811 side !!!!

```
Administrateur: C:\Windows\system32\cmd.exe - ping 192.168.0.1 -t
Réponse de 192.168.0.1 : octets=32 temps=383 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=410 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=379 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=305 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=382 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=379 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=380 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=379 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=380 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=378 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=379 ns TTL=63
Réponse de 192.160.0.1 : octets=32 temps=301 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=386 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=400 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=379 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=424 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=381 ns TTL=63
Réponse de 192.168.0.1 : octets=32 temps=379 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=381 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=382 ms TTL=63
```

RV082 side !!??

```
C:\WINDOWS\system32\cmd.exe - ping -t 10.20.2.1
Réponse de 10.20.2.1 : octets=32 temps=395 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=510 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=414 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=405 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=382 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=426 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=532 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=416 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=460 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=381 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=450 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=457 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=383 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=379 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=429 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=431 ms TTL=254
Réponse de 10.20.2.1 : octets=32 temps=378 ms TTL=254
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

RV082 VPN Status at T = 3 minutes

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 2.0.0.19-tm

10/100 8-port VPN Router RV082

VPN

System Summary | Setup | DHCP | System Management | Port Management | Firewall | ProtectLink | VPN | Log | Wizard | Support | Logout

Summary | Gateway to Gateway | Client to Gateway | VPN Client Access | VPN Pass Through | PPTP Server

Summary

1 Tunnel(s) Used | 99 Tunnel(s) Available | Detail

Tunnel Status

Add New Tunnel

Jump to 1 / 1 page | All entries per page

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	RV082->C isco2811	Connected	3DES/MD5/2	192.168.0.0 255.255.255.0	10.20.2.0 255.255.255.0	194. .44	Disconnect	Edit

1 Tunnel(s) Enabled | 1 Tunnel(s) Defined

GroupVPN Status

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.
------------	-------------------	---------------------	-------------	---------------	----------------------	-------------	---------

VPN Clients Status

Jump to 1 / 1 page | All entries per page

No.	Username	Status	Start Time	End Time	Duration	Disconnect
1		Offline	--	--	--	

SITEMAP

The VPN Summary displays the Summary, Tunnel Status and GroupVPN Status.

Summary: It shows the amount of Tunnel(s) Used and Tunnel(s) Available. RV082 supports 100 tunnels.

Detail: Click the Detail button to see the detail of VPN Summary, and users can use the tools on the top to save, export or print the details of VPN Summary.

More...

CISCO SYSTEMS

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