How To – Setup Cyberoam VPN Client to connect a Cyberoam for remote access using preshared key

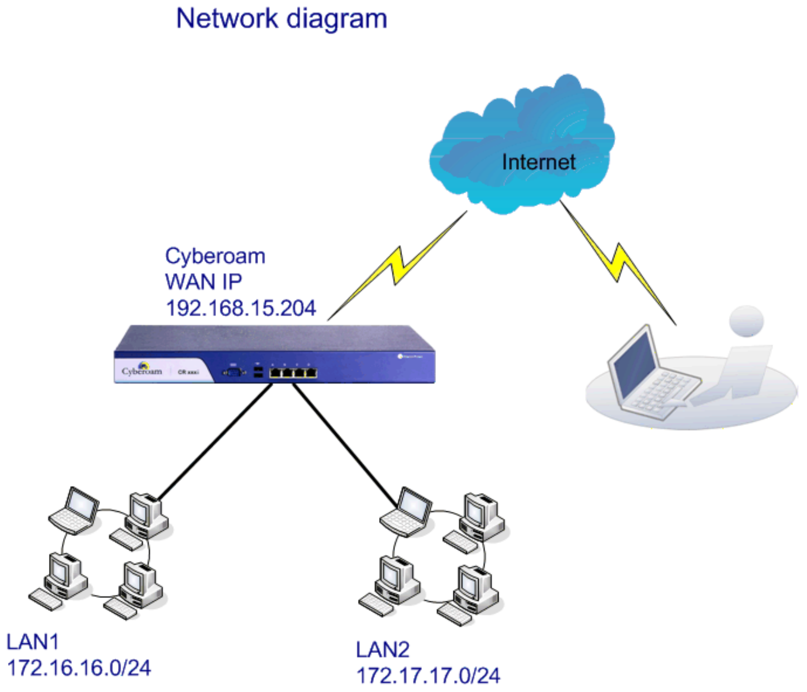
Objective

This article will detail how to setup Cyberoam VPN Client to securely connect to a Cyberoam for the remote access using preshared key.

This is commonly called a "road warrior" configuration, because the client is typically a laptop being used from remote locations, and connected over the internet using service providers and dialup connections. The most common use of this scenario is when you are at home or on the road and want access to the corporate network.

Throughout the article we will use the following network parameters.

Configuration Table



Configuration Parameters	Cyberoam	Cyberoam VPN Client
IPSec Connection (Road warrior)	**Local Network details**	**Local Network details**
	Cyberoam WAN IP address – 192.168.15.204	VPN Client IP address – *
	Local Internal Network – 172.16.16.0/24 172.17.17.0/24	Local Internal Network – 0.0.0.0/0
	Preshared Key - 0123456789	Preshared Key – 0123456789
	Remote Network details	**Remote Network details**
	Remote VPN server – IP address – *	Remote VPN server – IP address – 192.168.15.204
	Remote Internal Network – 0.0.0.0/0	Remote Internal Network – 172.16.16.0/24 172.17.17.0/24

Cyberoam Configuration

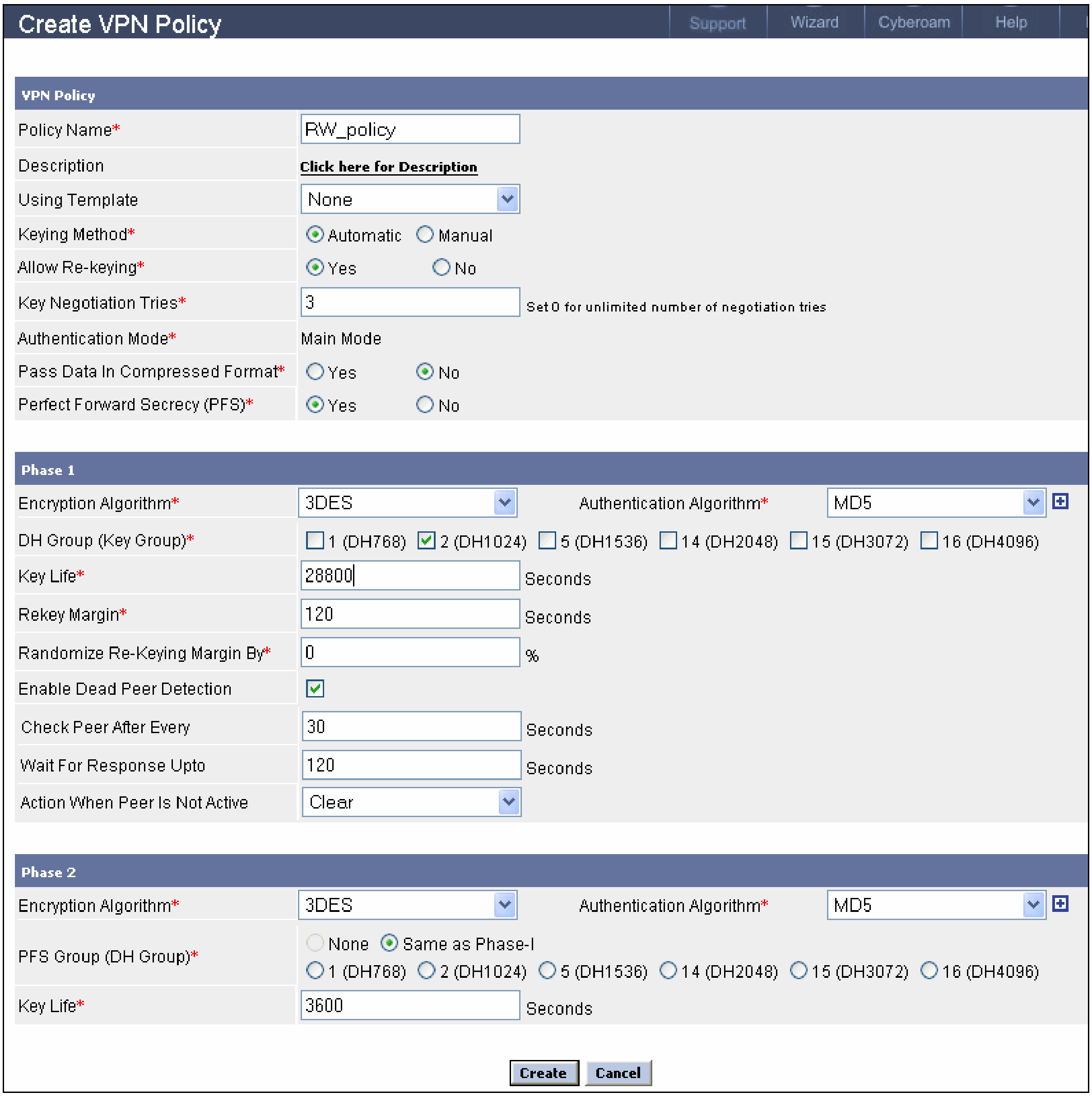
Applicable to - Version 9.4.0 build 2 and higher

Task list

- Define VPN policy - configure Phase 1 & Phase 2 parameters to authenticate the remote client and establish a secure connection
- Define VPN connection parameters – configure source and destination network
- Export VPN connection parameters
- Import VPN connection parameters in the VPN Client

Step 1: Create VPN Policy

To create VPN policy, go to **VPN** → **Policy** → **Create Policy**. Use the values specified in the below given image for creating policy.



Create VPN Policy

VPN Policy

Policy Name*	RW_policy
Description	Click here for Description
Using Template	None
Keying Method*	● Automatic ○ Manual
Allow Re-keying*	● Yes ○ No
Key Negotiation Tries*	3 Set 0 for unlimited number of negotiation tries
Authentication Mode*	Main Mode
Pass Data In Compressed Format*	○ Yes ● No
Perfect Forward Secrecy (PFS)*	● Yes ○ No

Phase 1

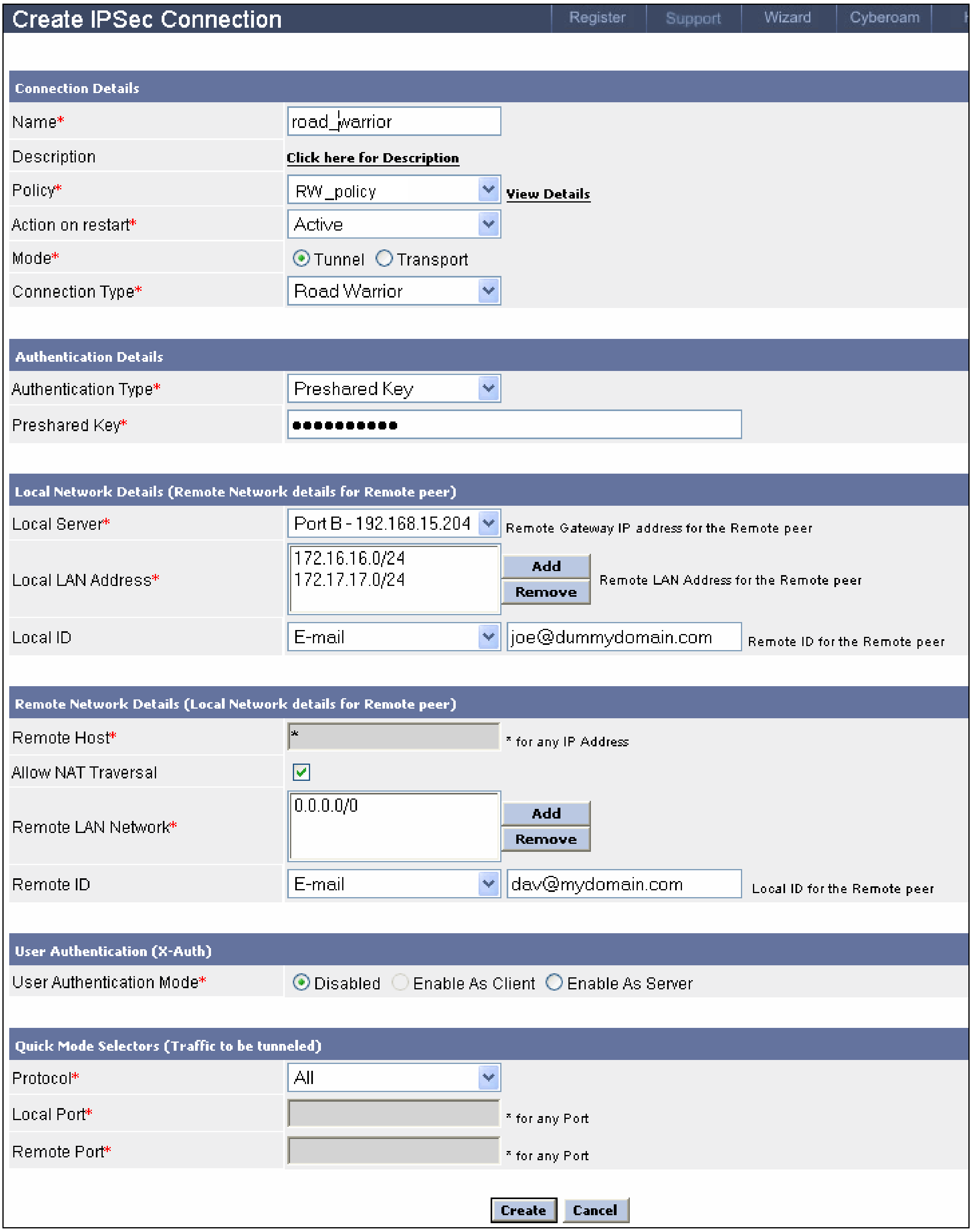
Encryption Algorithm*	3DES	Authentication Algorithm*	MD5
DH Group (Key Group)*	□ 1 (DH768) ☑ 2 (DH1024) □ 5 (DH1536) □ 14 (DH2048) □ 15 (DH3072) □ 16 (DH4096)		
Key Life*	28800 Seconds		
Rekey Margin*	120 Seconds		
Randomize Re-Keying Margin By*	0 %		
Enable Dead Peer Detection	☑		
Check Peer After Every	30 Seconds		
Wait For Response Upto	120 Seconds		
Action When Peer Is Not Active	Clear		

Phase 2

Encryption Algorithm*	3DES	Authentication Algorithm*	MD5
PFS Group (DH Group)*	○ None ● Same as Phase-I ○ 1 (DH768) ○ 2 (DH1024) ○ 5 (DH1536) ○ 14 (DH2048) ○ 15 (DH3072) ○ 16 (DH4096)		
Key Life*	3600 Seconds		

Step 2: Create VPN IPSec connection

To create connection, go to **VPN** → **IPSec Connection** → **Create Connection**. Use the VPN policy created in step 1 and other values as specified in the below given image for creating connection.



Create IPSec Connection

Connection Details

Name*	road_warrior	
Description	Click here for Description	
Policy*	RW_policy	View Details
Action on restart*	Active	
Mode*	● Tunnel ○ Transport	
Connection Type*	Road Warrior	

Authentication Details

Authentication Type*	Preshared Key
Preshared Key*	●●●●●●●●●●●

Local Network Details (Remote Network details for Remote peer)

Local Server*	Port B - 192.168.15.204	Remote Gateway IP address for the Remote peer
Local LAN Address*	172.16.16.0/24 172.17.17.0/24 Add Remove	Remote LAN Address for the Remote peer
Local ID	E-mail joe@dummydomain.com	Remote ID for the Remote peer

Remote Network Details (Local Network details for Remote peer)

Remote Host*	*	* for any IP Address
Allow NAT Traversal	☑	
Remote LAN Network*	0.0.0.0/0 Add Remove	
Remote ID	E-mail dav@mydomain.com	Local ID for the Remote peer

User Authentication (X-Auth)

User Authentication Mode*	● Disabled ○ Enable As Client ○ Enable As Server

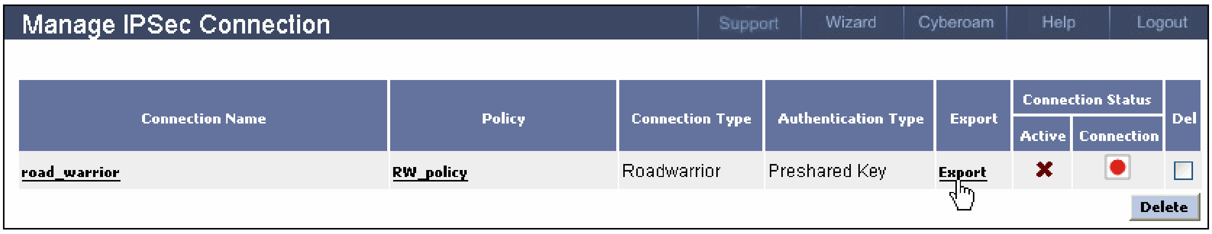
Quick Mode Selectors (Traffic to be tunneled)

Protocol*	All	
Local Port*		* for any Port
Remote Port*		* for any Port

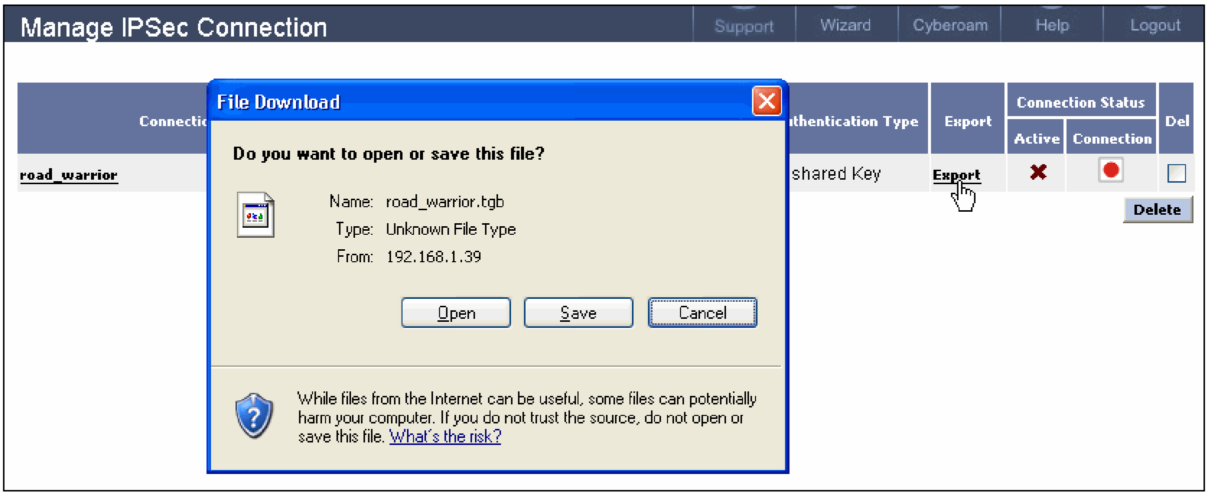
Create Cancel

Step 3: Export IPSec connection parameters

Go to **VPN** → **IPSec Connection** → **Manage Connection** and click Export against the connection whose detail is to be exported and used for connection. Cyberoam will prompt to save the connection parameter in the tgb format. Save and mail the saved file to the remote user.



Connection Name	Policy	Connection Type	Authentication Type	Export	Connection Status		Del
					Active	Connection	
road_warrior	RW_policy	Roadwarrior	Preshared Key	Export	✖	●	□



Do you want to open or save this file?

Name: road_warrior.tgb
Type: Unknown File Type
From: 192.168.1.39

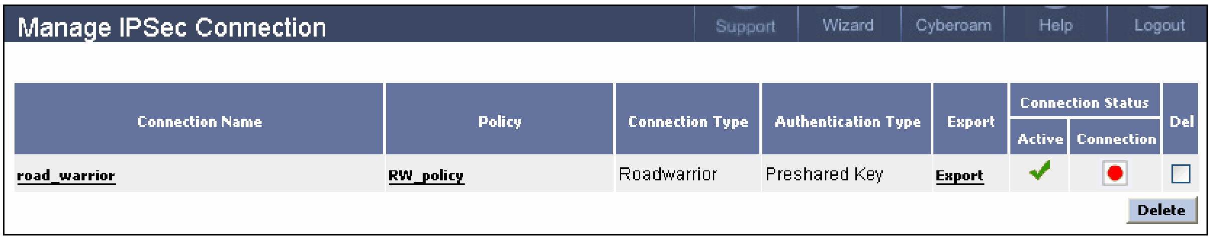
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Step 4. Activate Connection and establish Tunnel

Go to VPN → IPSec Connection → Manage Connection

To activate the connection, click ✖ under Connection Status against the road_warrior connection

✓ under Connection Status indicates that the connection is successfully activated



Connection Name	Policy	Connection Type	Authentication Type	Export	Connection Status		Del
					Active	Connection	
road_warrior	RW_policy	Roadwarrior	Preshared Key	Export	✓	●	□

Note

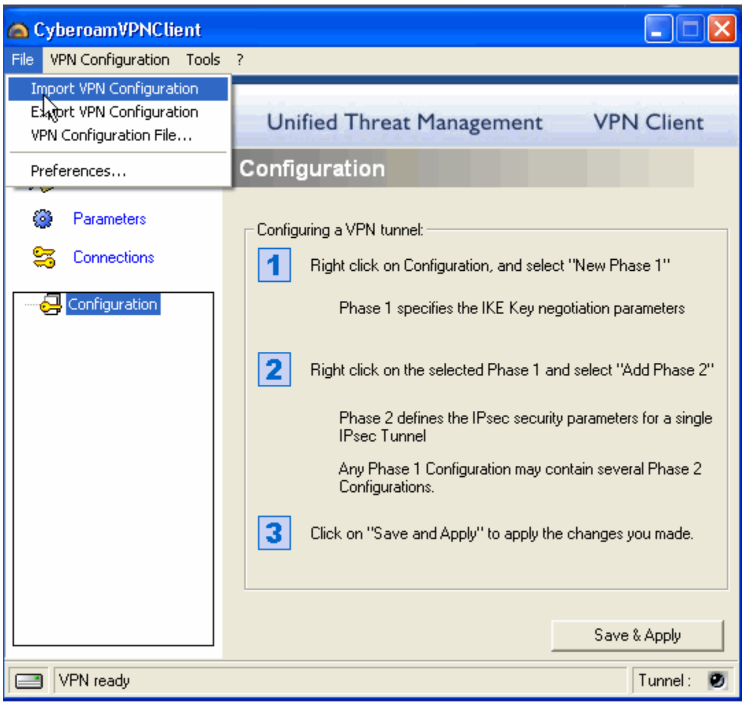
At a time only one connection can be active if both the types of connection - Digital Certificate and Preshared Key - are created with the same source and destination. In such situation, at the time of activation, you will receive error 'unable to activate connection' hence you need to deactivate all other connections.

VPN Client Configuration

Step 5. Launch Cyberoam VPN client and go to File>Import VPN Configuration to import connection parameter file (.tgb) received from the remote end. (step 3).

Note

- Importing VPN configuration will over-write the existing VPN configuration.
- VPN Client creates one phase 1 policy based on the VPN connection.
- VPN Client creates phase 2 policy for each internal network specified in the VPN connection.



Configuring a VPN tunnel:

1 Right click on Configuration, and select "New Phase 1"

Phase 1 specifies the IKE Key negotiation parameters

2 Right click on the selected Phase 1 and select "Add Phase 2"

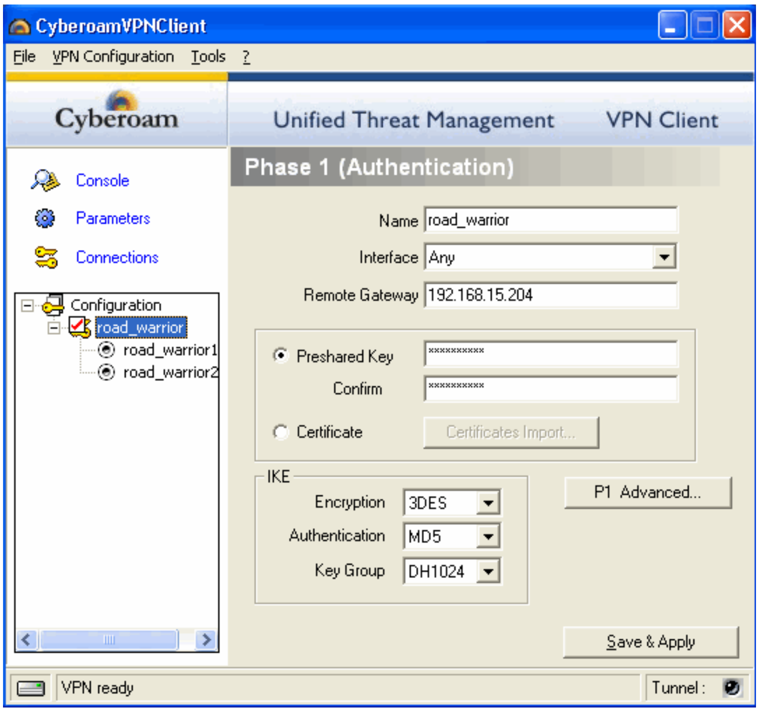
Phase 2 defines the IPsec security parameters for a single IPsec Tunnel

Any Phase 1 Configuration may contain several Phase 2 Configurations.

3 Click on "Save and Apply" to apply the changes you made.

VPN ready

In our example, as two internal networks are configured in the VPN connection (step 2), VPN Client creates two phase 2 policies i.e. one policy for each internal network.



Phase 1 (Authentication)

Name: road_warrior

Interface: Any

Remote Gateway: 192.168.15.204

● Preshared Key: **********

Confirm: **********

○ Certificate

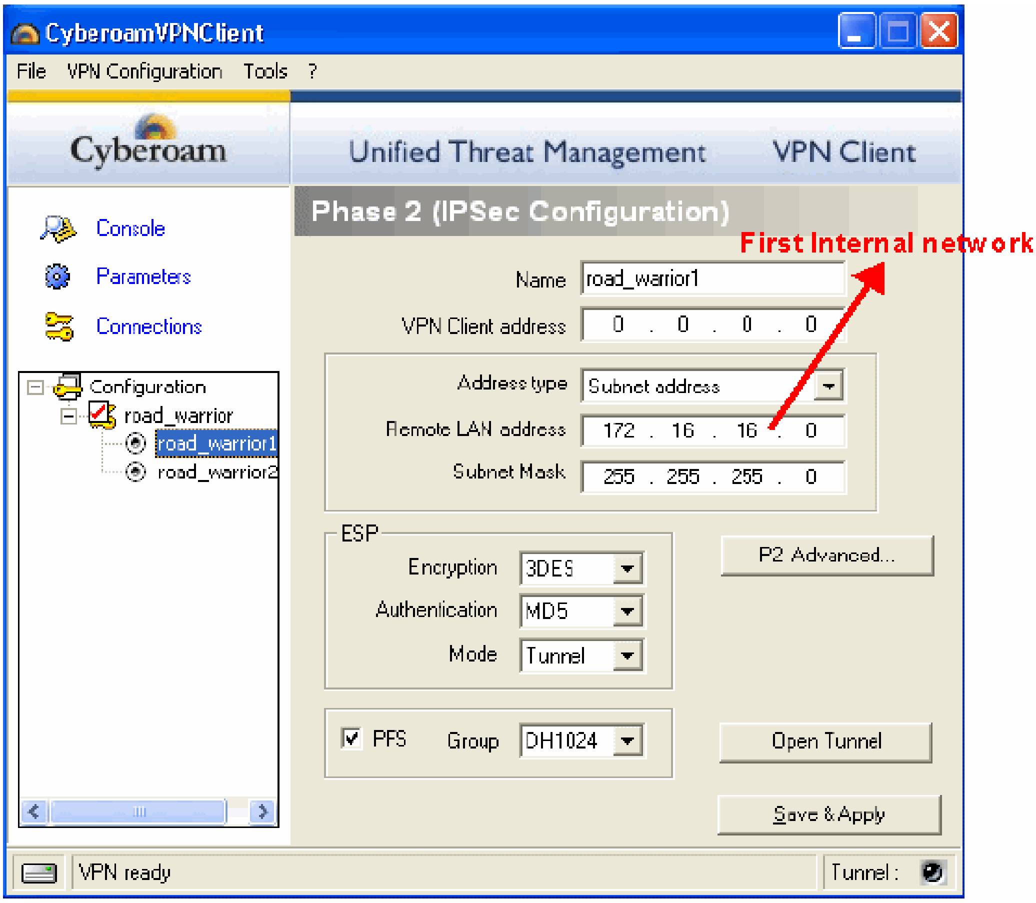
IKE

Encryption: 3DES

Authentication: MD5

Key Group: DH1024

VPN ready



Phase 2 (IPSec Configuration)

First Internal network

Name: road_warrior1

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 172 . 16 . 16 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

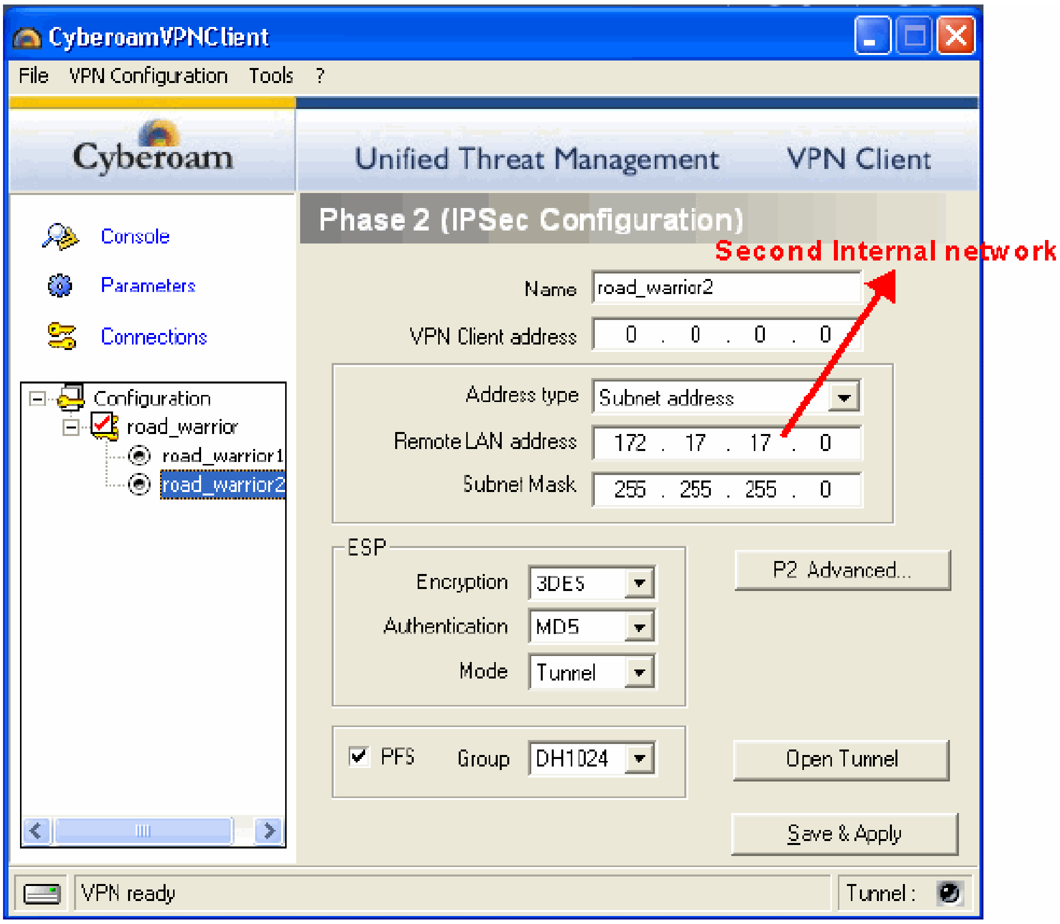
Encryption: 3DES

Authentication: MD5

Mode: Tunnel

☑ PFS Group: DH1024

VPN ready



Phase 2 (IPSec Configuration)

Second Internal network

Name: road_warrior2

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 172 . 17 . 17 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: MD5

Mode: Tunnel

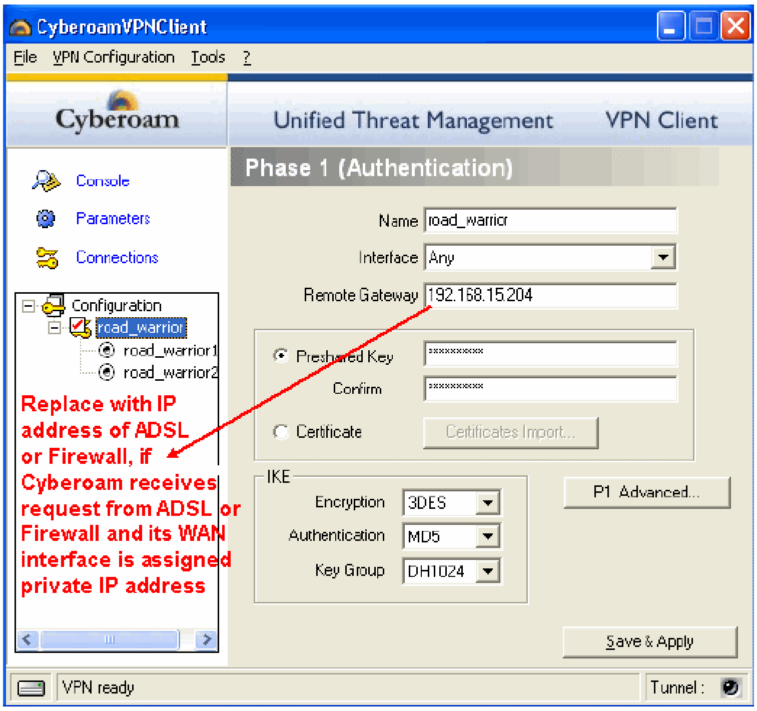
☑ PFS Group: DH1024

VPN ready

Case I: Private IP address assigned to Cyberoam WAN interface

This situation occurs when Cyberoam is deployed behind any firewall or ADSL device and ADSL device port forwards the request to the Cyberoam.

In this case, specify the public IP address of firewall or ADSL manually in the Remote Gateway field in Phase 1 of VPN Client as connection parameter file will forward private IP address to the VPN Client.



Phase 1 (Authentication)

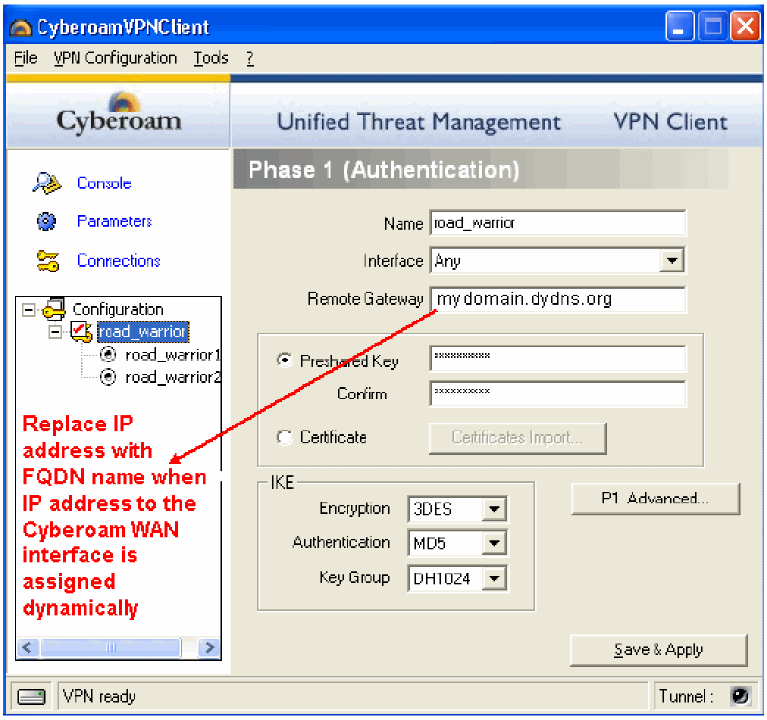
Name: road_warrior
Interface: Any
Remote Gateway: 192.168.15.204
● Preshared Key: **********
Confirm: **********
○ Certificate
IKE
Encryption: 3DES
Authentication: MD5
Key Group: DH1024

VPN ready

Replace with IP address of ADSL or Firewall, if Cyberoam receives request from ADSL or Firewall and its WAN interface is assigned private IP address

Case II: Dynamic IP address assigned to Cyberoam WAN interface

When Cyberoam WAN interface is assigned IP address dynamically via DHCP or PPPoE and Dynamic DNS is used to map dynamic IP address with a static FQDN, specify FQDN name manually in the Remote Gateway field in Phase 1 of VPN Client.



Phase 1 (Authentication)

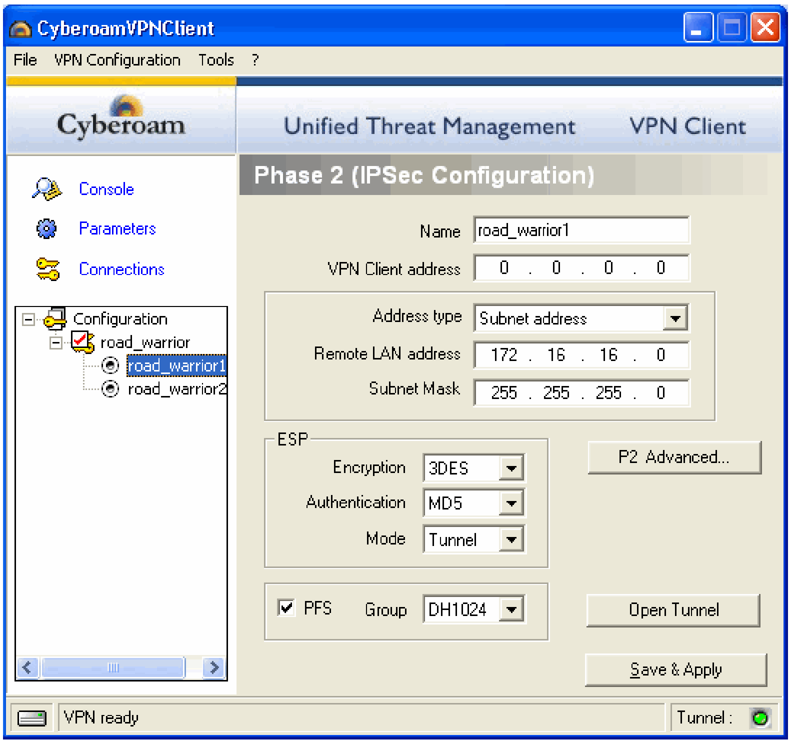
Name: road_warrior
Interface: Any
Remote Gateway: my domain.dydns.org
● Preshared Key: **********
Confirm: **********
○ Certificate
IKE
Encryption: 3DES
Authentication: MD5
Key Group: DH1024

VPN ready

Replace IP address with FQDN name when IP address to the Cyberoam WAN interface is assigned dynamically

Step 6. Establish connection

VPN Client automatically opens tunnel on traffic detection. Status bar displays green light for “Tunnel” if connection is successfully established.



Phase 2 (IPSec Configuration)

Name: road_warrior1
VPN Client address: 0 . 0 . 0 . 0
Address type: Subnet address
Remote LAN address: 172 . 16 . 16 . 0
Subnet Mask: 255 . 255 . 255 . 0

ESP
Encryption: 3DES
Authentication: MD5
Mode: Tunnel

☑ PFS Group: DH1024

VPN ready
Tunnel : ●

Document Version: 1.0-15/09/2007