

Dial up IPsec Policy based Configuration on Version 4.0 MR2 onwards

My network

WAN1 : 192.168.140.202/23

Internal: 10.129.0.202/23

IPsec VPN network: 172.16.16.0/24 (DHCP range 172.16.16.1-254)

IPsec Phase 1 Configuration as below

Name	<input type="text" value="phase1"/>
Remote Gateway	<input type="text" value="Dialup User"/>
Local Interface	<input type="text" value="wan1"/>
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	<input type="text" value="Preshared Key"/>
Pre-shared Key	<input type="text" value="....."/>
Peer Options	
	<input checked="" type="radio"/> Accept any peer ID
	<input type="radio"/> Accept this peer ID <input type="text" value=""/>
	<input type="radio"/> Accept peer ID in dialup group <input type="text" value="Guest-group"/>
Advanced... (XAUTH, NAT Traversal, DPD)	
<input type="checkbox"/> Enable IPsec Interface Mode	
Local Gateway IP	<input checked="" type="radio"/> Main Interface IP
	<input type="radio"/> Specify <input type="text" value="0.0.0.0"/>
P1 Proposal	
	1 - Encryption <input type="text" value="3DES"/> Authentication <input type="text" value="SHA1"/>
	2 - Encryption <input type="text" value="AES128"/> Authentication <input type="text" value="SHA1"/>
DH Group	1 <input type="checkbox"/> 2 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 14 <input type="checkbox"/>
Keylife	<input type="text" value="28800"/> (120-172800 seconds)
Local ID	<input type="text" value=""/> (optional)
XAUTH <input checked="" type="radio"/> Disable <input type="radio"/> Enable as Client <input type="radio"/> Enable as Server	
NAT Traversal	<input checked="" type="checkbox"/> Enable
Keepalive Frequency	<input type="text" value="10"/> (10-900 seconds)
Dead Peer Detection <input checked="" type="checkbox"/> Enable	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

IPSec Phase 2 Configuration

Name

Phase 1

Advanced...

P2 Proposal

1- Encryption: Authentication:

2- Encryption: Authentication:

Enable replay detection

Enable perfect forward secrecy(PFS).

DH Group 1 2 5 14

Keylife: (Seconds) (KBytes)

Autokey Keep Alive Enable

DHCP-IPsec Enable

Quick Mode Selector

Source address	<input type="text" value="10.129.0.0/23"/>
Source port	<input type="text" value="0"/>
Destination address	<input type="text" value="172.16.16.0/24"/>
Destination port	<input type="text" value="0"/>
Protocol	<input type="text" value="0"/>

OK

Cancel

Please mention the source and destination IP address correctly

Configuring DHCP server for IPSec VPN clients > System > DHCP > Server >

Interface Name

Mode

Enable

Type Regular IPsec

IP Range -

Network Mask

Default Gateway

DNS Service Use System DNS Setting Specify

DNS Server 0

DNS Server 1

[Advanced...] (DNS, WINS, Custom Options, Exclude Ranges.)

OK

Cancel

Configure firewall policy and place this policy on top of all other firewall policies, and do not forget to specify the source and destination address, otherwise you will be not able to resolve the IP address from the fortigate itself, and also you will face the problem with fortiguard updates.

Source Interface/Zone	<input type="text" value="internal"/>	
Source Address	<input type="text" value="internal"/>	<input type="checkbox"/> Multiple
Destination Interface/Zone	<input type="text" value="wan1"/>	
Destination Address	<input type="text" value="172.16.16.0/24"/>	<input type="checkbox"/> Multiple
Schedule	<input type="text" value="always"/>	
Service	<input type="text" value="ANY"/>	<input type="checkbox"/> Multiple
Action	<input type="text" value="IPSEC"/>	
<input type="checkbox"/> Log Allowed Traffic		

VPN Tunnel	<input type="text" value="phase1"/>	
<input checked="" type="checkbox"/> Allow inbound	<input type="checkbox"/> Inbound NAT	
<input checked="" type="checkbox"/> Allow outbound	<input type="checkbox"/> Outbound NAT	

<input type="checkbox"/> UTM		
<input type="checkbox"/> Traffic Shaping	<input type="text" value="[Please Select]"/>	
<input type="checkbox"/> Reverse Direction Traffic Shaping	<input type="text" value="[Please Select]"/>	
<input type="checkbox"/> Per-IP Traffic Shaping	<input type="text" value="[Please Select]"/>	

Comments (maximum 63 characters)

Configure Forticlient > if you are specifying 0.0.0.0/0 in the remote network then all the traffic will go through the tunnel.

Edit Connection

Connection Name: test

VPN Type: Automatic IPsec, Manual IPsec, SSL VPN

Remote Gateway: 192.168.140.202

Remote Network: 10 . 129 . 0 . 0 / 255 . 255 . 254 . 0

Authentication Method: Preshared Key

Preshared Key: ■■■■

Buttons: Advanced, OK, Cancel

Advanced Settings

Policy:

IKE: Main mode; DH Group: 5; 3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1; Key life: 28800s; Nat-T: ON, Frequency 5s; DPD: ON;

IPSec: 3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1; DH Group: 5; Keylife: Seconds : 1800s ; Replay Detection: ON; PFS: ON;

Buttons: Legacy, Default, Config...

Advanced:

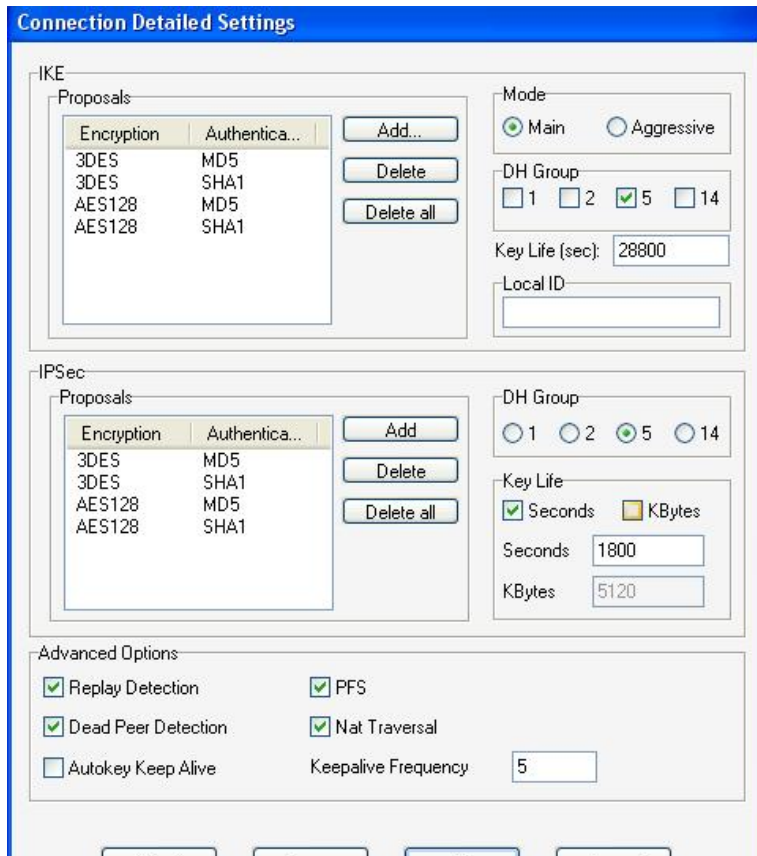
Acquire virtual IP address (Config...)

eXtended Authentication (Config...)

Remote Network:

IP address	Subnet Mask	
10.129.0.0	255.255.254.0	Add...
		Edit...
		Delete

Buttons: OK, Cancel



Please make sure that all the parameters are matching.

Then click on connect, you will be able to connect and then you can ping the internal resource 10.129.0.202, in the below image once I disconnect the tunnel I am not able to ping the resource.

FortiClient Console

FortiClient

General

VPN

- Connections
- Monitor
- My Certificates
- CA Certificates
- CRL

AntiVirus

Firewall

WebFilter

AntiSpam

AntiLeak

App Detection

VPN: Connections

Name	Gateway / Policy Server	VPN Type	Authentication	Status
Risk-Forticlient3	87.79.201.134	IPsec	Preshared Key	Down
test	192.168.140.202	IPsec	Preshared Key	Down

Connect

Options

- Start VPN before logging on
- Keep IPsec service running forever unless manually stopped
- Beep when connection error occurs
 - Continuously
 - Stop after seconds

Apply

```

C:\WINDOWS\system32\cmd.exe - ping 10.129.0.202
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\somurhs>ping 10.129.0.202

Pinging 10.129.0.202 with 32 bytes of data:

Reply from 10.129.0.202: bytes=32 time<1ms TTL=255
Reply from 10.129.0.202: bytes=32 time<1ms TTL=255
Reply from 10.129.0.202: bytes=32 time<1ms TTL=255
Reply from 10.129.0.202: bytes=32 time<1ms TTL=255

Ping statistics for 10.129.0.202:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\somurhs>ping 10.129.0.202

Pinging 10.129.0.202 with 32 bytes of data:

Request timed out.
Request timed out.
  
```