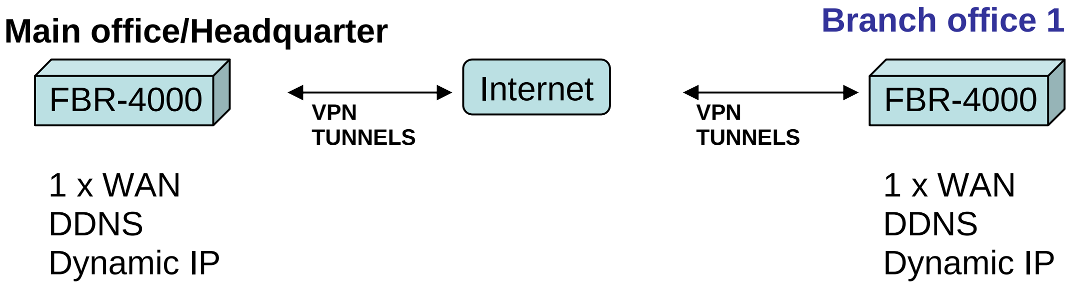
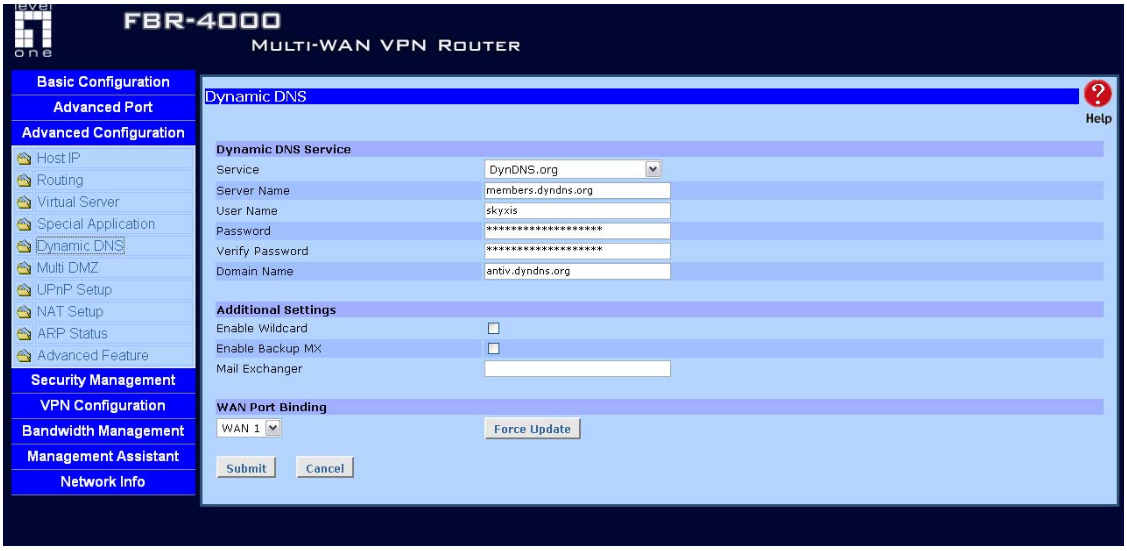


For this scenario we used the free Dynamic DNS service provided by www.dyndns.org. We have created an account with two domain names on which each unit updates:

1. FBR-4000(1) => **ivenue.dyndns.org**
2. FBR-4000(2) => **ddctt.dyndns.org**

To configure the respective FQDNs into each FBR-4000 perform the following:

3. Login into the GUI of the FBR-4000
4. Click on **Advanced Configuration**
5. Click on **Dynamic DNS**
6. Once on this page for the service select **DynDNS.org** from the drop down menu
7. Server Name leave as default "**members.dyndns.org**"
8. For the **User Name**, input the username you had registered
9. For the **Password**, input your "dyndns" password
10. For the **Verify Password**, re-enter your password
11. For the **Domain Name**, input the domain name for the respective unit (Refer step 1 & 2 above)
12. Omit the Additional Settings (Let all be blank)
13. Select the **WAN1** or **WAN2** as the WAN port to update its IP to the Dyndns.org servers
14. Click **Submit**



Dynamic DNS

Dynamic DNS Service

Service	DynDNS.org
Server Name	members.dyndns.org
User Name	skyxis
Password	******************
Verify Password	******************
Domain Name	antiv.dyndns.org

Additional Settings

Enable Wildcard	□
Enable Backup MX	□
Mail Exchanger	

WAN Port Binding

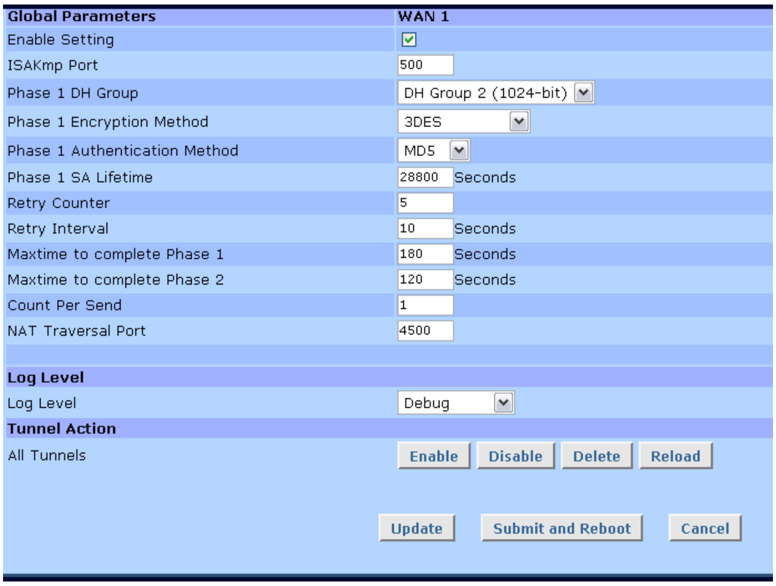
WAN 1

FBR-4000(1) Setup

1. Login into the GUI of the FBR-4000(1) and click on **VPN Configuration** then on **IKE Global Setup** to set the primary settings.

2. Once on this page input the following parameters:

    a. **Enable Setting:** select the check mark to enable the Global Parameters
    b. **ISAKmp Port:** Input 500 in the text box
    c. **Phase 1 DH Group:** select from the drop down menu DH Group 2 (DH1024-bit)
    d. **Phase 1 Encryption Method:** select from the drop down menu 3DES
    e. **Phase 1 Authentication Method:** select from the drop down menu MD5
    f. **Phase 1 SA Lifetime:** input in the text box 28800 seconds
    g. **Retry Counter:** enter in the text box 5 retries
    h. **Retry Interval:** enter in the text box 10 seconds
    i. **Maxtime to complete Phase 1:** input 180 seconds
    j. **Maxtime to complete Phase 2:** input 120 seconds
    k. **Count Per Send:** input 1 in the text box
    l. **NAT Traversal Port:** input port 4500
    m. **Log Level:** set the log level to Information/Debug



Global Parameters	WAN 1
Enable Setting	☑
ISAKmp Port	500
Phase 1 DH Group	DH Group 2 (1024-bit)
Phase 1 Encryption Method	3DES
Phase 1 Authentication Method	MD5
Phase 1 SA Lifetime	28800 Seconds
Retry Counter	5
Retry Interval	10 Seconds
Maxtime to complete Phase 1	180 Seconds
Maxtime to complete Phase 2	120 Seconds
Count Per Send	1
NAT Traversal Port	4500
Log Level	
Log Level	Debug
Tunnel Action	
All Tunnels	Enable Disable Delete Reload

IPSec Policy Setup Page

3. **Policy Entry, Traffic Binding and Local Identity Option:**
   a. **Name:** input a generic name in the text box, for this example we used **VPN**
   b. **State:** select the **ENABLED** check box
   c. **Interface:** select from the drop down box **WAN 1**
   d. **Session:** leave as defaulted
   e. **Local Identity type:** set to **None**

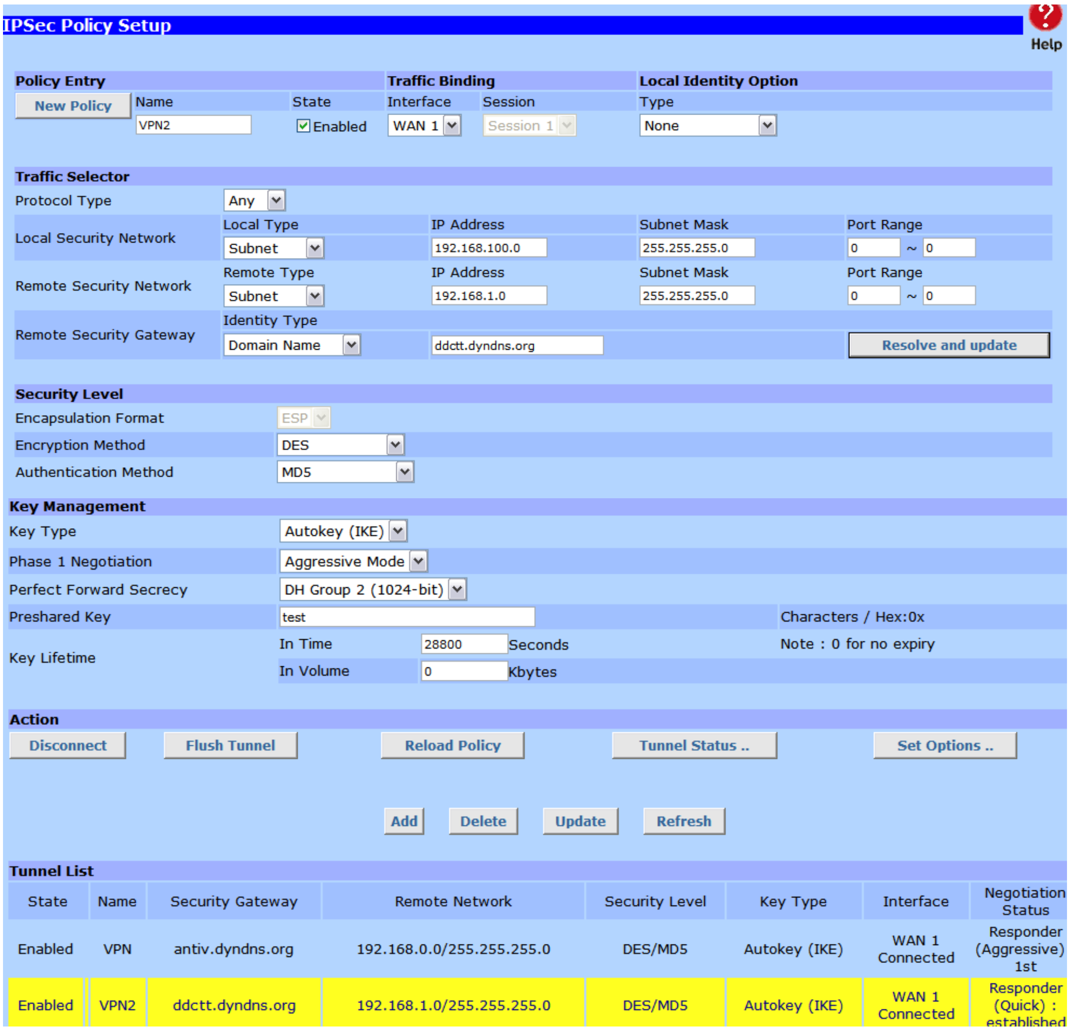
4. **Traffic Selector**
   a. **Protocol Type:** select from the drop down menu ANY
   b. **Local Security Network:** these settings apply to the local subnet on the FBR-4000(1)
   c. **Local Type:** select Subnet **IP Address:** input the local subnet ID. ex. **192.168.100.0**
   d. **Subnet Mask:** input the local subnet mask. ex. **255.255.255.0**
   e. **Port Range:** leave all ZEROs (**0** ~ **0**)
   f. **Remote Security Network:** these settings apply to the local subnet of the FBR-4000(2)
   g. **Remote Type:** select Subnet **IP Address:** input the remote subnet ID. ex. **192.168.1.0**
   h. **Subnet Mask:** input the remote subnet mask. ex. **255.255.255.0**
   i. **Port Range:** leave all ZEROs (**0** ~ **0**)
   j. **Remote Security Gateway:**
   k. **Identity Type:** select Domain Name and on the text box input the domain name of the FBR-4000(2). ex. **ddctt.dyndns.org**

5. **Security Level**

a. **Encapsulation Format:** leave as defaulted **ESP**
b. **Encryption Method:** select from the drop down menu **3DES**
c. **Authentication Method:** select from the drop down menu **MD5**

6. **Key Management**
   a. **Key Type:** select from the drop down menu **AUTOKEY (IKE)**
   b. **Phase 1 Negotiation:** select from the drop down menu **Aggressive MODE**
   c. **Perfect Forward Secrecy:** select from the drop down menu **DH Group 2 (1024-bit)**
   d. **Preshared Key:** input in the text box the word **test** (lower case)
   e. **Key Lifetime:**
      i. **In Time:** input in the textbox **28800** seconds
      ii. **In Volume:** input in the textbox **0** Kbytes

7. **Click the ADD button to save the policy.**



IPSec Policy Setup

Policy Entry
Name: VPN2
State: ☑ Enabled

Traffic Binding
Interface: WAN 1
Session: Session 1

Local Identity Option
Type: None

Traffic Selector
Protocol Type: Any
Local Security Network: Local Type: Subnet; IP Address: 192.168.100.0; Subnet Mask: 255.255.255.0; Port Range: 0 ~ 0
Remote Security Network: Remote Type: Subnet; IP Address: 192.168.1.0; Subnet Mask: 255.255.255.0; Port Range: 0 ~ 0
Remote Security Gateway: Identity Type: Domain Name; ddctt.dyndns.org

Security Level
Encapsulation Format: ESP
Encryption Method: DES
Authentication Method: MD5

Key Management
Key Type: Autokey (IKE)
Phase 1 Negotiation: Aggressive Mode
Perfect Forward Secrecy: DH Group 2 (1024-bit)
Preshared Key: test — Characters / Hex:0x
Key Lifetime: In Time: 28800 Seconds — Note : 0 for no expiry
In Volume: 0 Kbytes

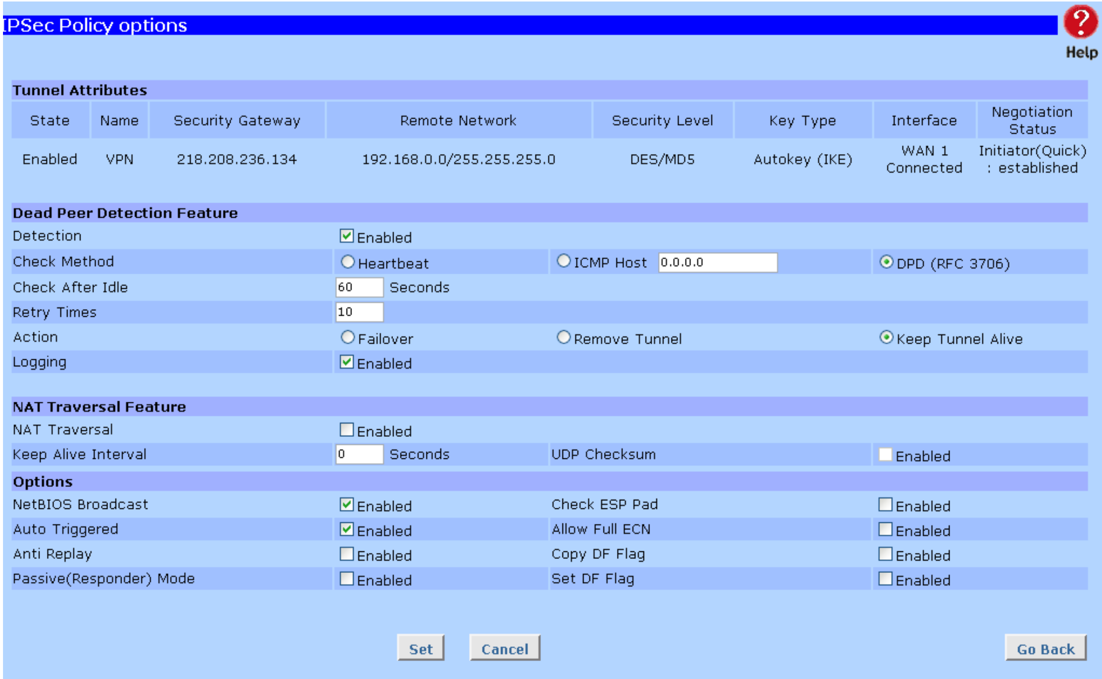
Action

Tunnel List

State	Name	Security Gateway	Remote Network	Security Level	Key Type	Interface	Negotiation Status
Enabled	VPN	antiv.dyndns.org	192.168.0.0/255.255.255.0	DES/MD5	Autokey (IKE)	WAN 1 Connected	Responder (Aggressive) 1st
Enabled	VPN2	ddctt.dyndns.org	192.168.1.0/255.255.255.0	DES/MD5	Autokey (IKE)	WAN 1 Connected	Responder (Quick) : established

IPSec Policy Setup – Set Options

8. Set Options Page
   a. After adding the policy on the same page, click on the **Set Options** button
   b. At the Dead Peer Detection Feature
      i. Check enabled the **Detection** check mark
   c. **Check Method:** select DPD (RFC 3706)
   d. **Check After Idle, and Retry Times:** leave as is
   e. **Action:** select Keep Tunnel Alive
   f. Click on the **SET** button
   g. Click on the **Update** button on the IPSec Policy Setup screen.



Tunnel Attributes

State	Name	Security Gateway	Remote Network	Security Level	Key Type	Interface	Negotiation Status
Enabled	VPN	218.208.236.134	192.168.0.0/255.255.255.0	DES/MD5	Autokey (IKE)	WAN 1 Connected	Initiator(Quick) : established

Dead Peer Detection Feature

Detection	☑ Enabled		
Check Method	○ Heartbeat	○ ICMP Host 0.0.0.0	● DPD (RFC 3706)
Check After Idle	60 Seconds		
Retry Times	10		
Action	○ Failover	○ Remove Tunnel	● Keep Tunnel Alive
Logging	☑ Enabled		

NAT Traversal Feature

NAT Traversal	□ Enabled		
Keep Alive Interval	0 Seconds	UDP Checksum	□ Enabled

Options

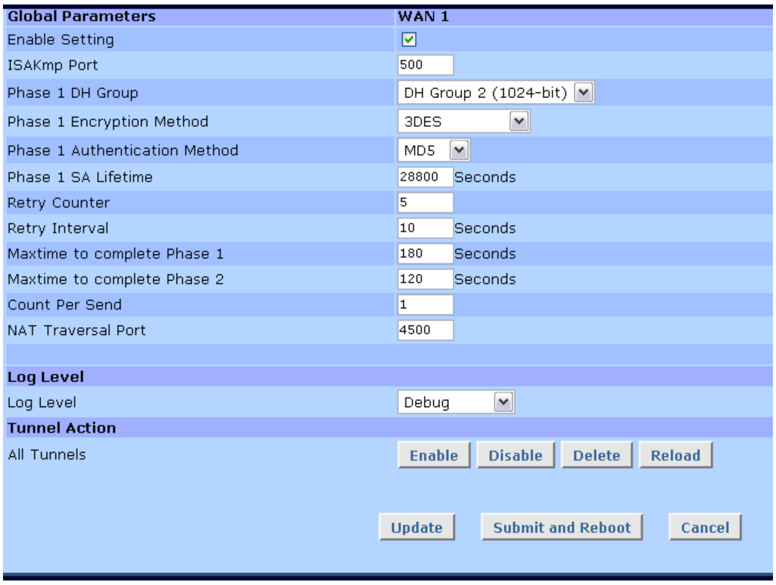
NetBIOS Broadcast	☑ Enabled	Check ESP Pad	□ Enabled
Auto Triggered	☑ Enabled	Allow Full ECN	□ Enabled
Anti Replay	□ Enabled	Copy DF Flag	□ Enabled
Passive(Responder) Mode	□ Enabled	Set DF Flag	□ Enabled

FBR-4000(2) Setup

1. Login into the GUI of the FBR-4000(2) and click on **VPN Configuration** then on **IKE Global Setup** to set the primary settings.

2. Once on this page input the following parameters:
   a. **Enable Setting:** select the check mark to enable the Global Parameters
   b. **ISAKmp Port:** Input 500 in the text box
   c. **Phase 1 DH Group:** select from the drop down menu DH Group 1 (DH768-bit)
   d. **Phase 1 Encryption Method:** select from the drop down menu 3DES

e. **Phase 1 Authentication Method:** select from the drop down menu MD5
f. **Phase 1 SA Lifetime:** input in the text box 28800 seconds
g. **Retry Counter:** enter in the text box 5 retries
h. **Retry Interval:** enter in the text box 10 seconds
i. **Maxtime to complete Phase 1:** input 180 seconds
j. **Maxtime to complete Phase 2:** input 120 seconds
k. **Count Per Send:** input 1 in the text box
l. **NAT Traversal Port:** input port 4500
m. **Log Level:** set the log level to Debug/Information



Global Parameters	WAN 1
Enable Setting	☑
ISAKmp Port	500
Phase 1 DH Group	DH Group 2 (1024-bit)
Phase 1 Encryption Method	3DES
Phase 1 Authentication Method	MD5
Phase 1 SA Lifetime	28800 Seconds
Retry Counter	5
Retry Interval	10 Seconds
Maxtime to complete Phase 1	180 Seconds
Maxtime to complete Phase 2	120 Seconds
Count Per Send	1
NAT Traversal Port	4500
Log Level	
Log Level	Debug
Tunnel Action	
All Tunnels	

IPSec Policy Setup Page

3. **Policy Entry, Traffic Binding and Local Identity Option:**
   a. **Name:** input a generic name in the text box, for this example we used **VPN**
   b. **State:** select the **ENABLED** check box
   c. **Interface:** select from the drop down box **WAN 1**
   d. **Session:** leave as defaulted
   e. **Local Identity type:** set to **None**

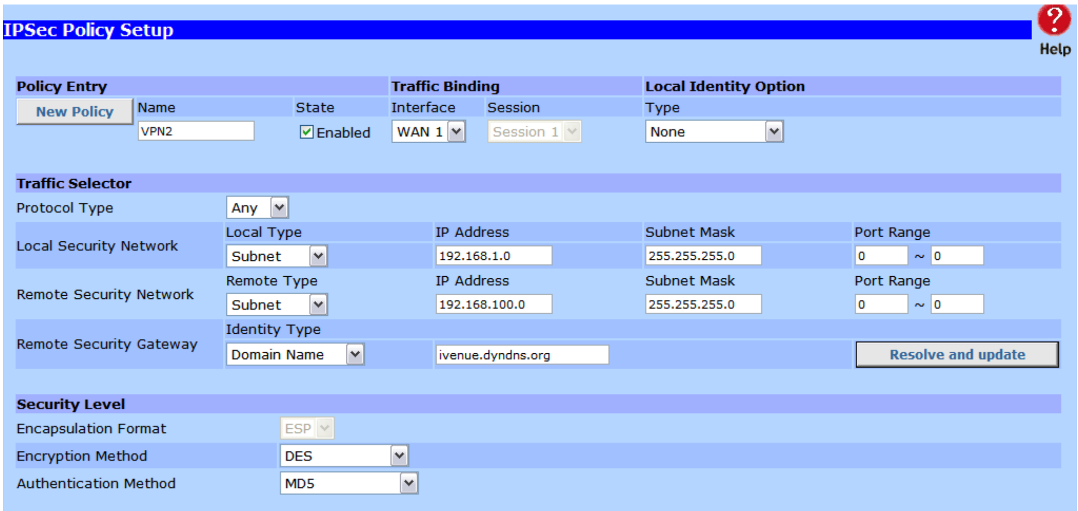
4. **Traffic Selector**
   a. **Protocol Type:** select from the drop down menu ANY
   b. **Local Security Network:** these settings apply to the local subnet on the FBR-4000(2)
   c. **Local Type:** select Subnet **IP Address:** input the local subnet ID. ex. **192.168.1.0**
   d. **Subnet Mask:** input the local subnet mask. ex. **255.255.255.0**
   e. **Prot Range:** leave all ZEROs (**0** ~ **0**)

f. **Remote Security Network:** these settings apply to the local subnet of the FBR-4000(1)
g. **Remote Type:** select Subnet **IP Address:** input the remote subnet ID. ex. **192.168.100.0**
h. **Subnet Mask:** input the remote subnet mask. ex. **255.255.255.0**
i. **Port Range:** leave all ZEROs (**0** ~ **0**)
j. Remote Security Gateway:
k. **Identity Type:** select Domain Name and on the text box input the domain name of the FBR-4000(1). ex. **ivenue.dyndns.org**

5. **Security Level**
   a. **Encapsulation Format:** leave as defaulted **ESP**
   b. **Encryption Method:** select from the drop down menu **3DES**
   c. **Authentication Method:** select from the drop down menu **MD5**

6. **Key Management**
   a. **Key Type:** select from the drop down menu **AUTOKEY (IKE)**
   b. **Phase 1 Negotiation:** select from the drop down menu **Aggressive MODE**
   c. **Perfect Forward Secrecy:** select from the drop down menu **DH Group 2 (1024-bit)**
   d. **Preshared Key:** input in the text box the word **test** (lower case)
   e. **Key Lifetime:**
      i. **In Time:** input in the textbox **28800** seconds
      ii. **In Volume:** input in the textbox **0** Kbytes

7. **Click the ADD button to save the policy.**



IPSec Policy Setup

Policy Entry

Name: VPN2
State: ☑ Enabled

Traffic Binding

Interface: WAN 1
Session: Session 1

Local Identity Option

Type: None

Traffic Selector

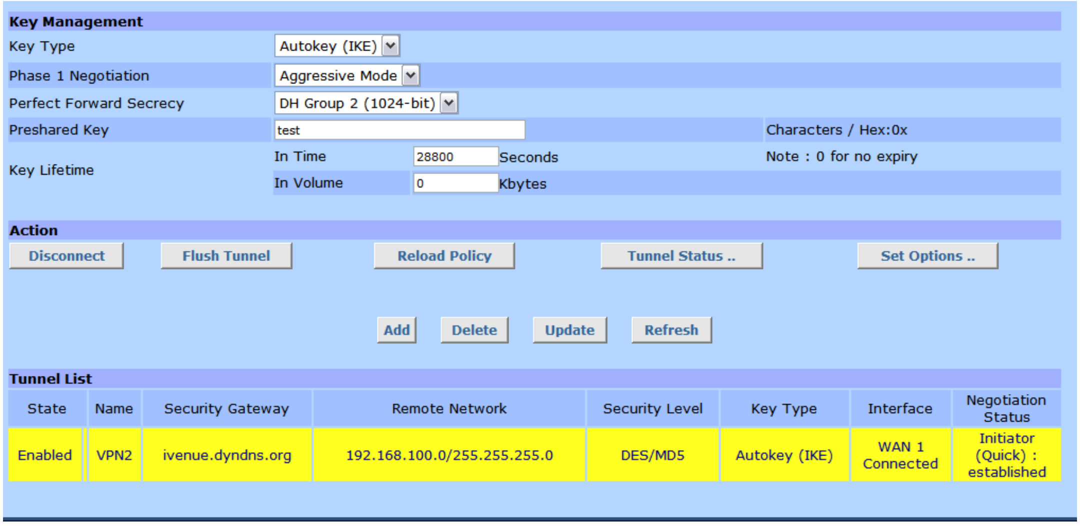
Protocol Type: Any

	Type	IP Address	Subnet Mask	Port Range
Local Security Network	Local Type: Subnet	192.168.1.0	255.255.255.0	0 ~ 0
Remote Security Network	Remote Type: Subnet	192.168.100.0	255.255.255.0	0 ~ 0

Remote Security Gateway: Identity Type: Domain Name — ivenue.dyndns.org

Security Level

Encapsulation Format: ESP
Encryption Method: DES
Authentication Method: MD5



Key Management

Key Type	Autokey (IKE)		
Phase 1 Negotiation	Aggressive Mode		
Perfect Forward Secrecy	DH Group 2 (1024-bit)		
Preshared Key	test		Characters / Hex:0x
Key Lifetime	In Time	28800 Seconds	Note : 0 for no expiry
	In Volume	0 Kbytes	

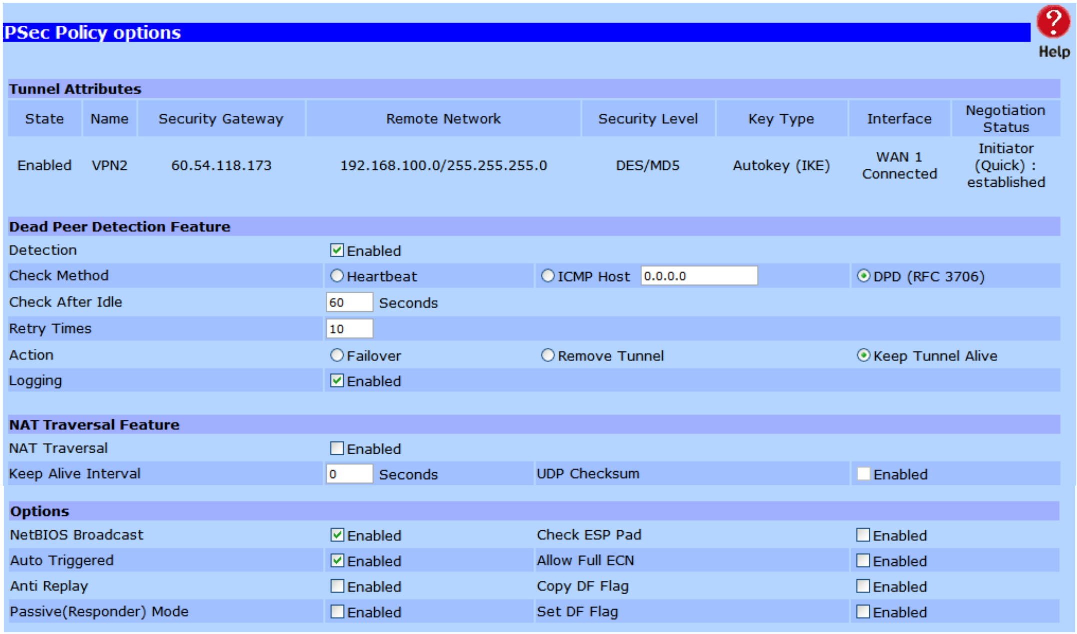
Action

Tunnel List

State	Name	Security Gateway	Remote Network	Security Level	Key Type	Interface	Negotiation Status
Enabled	VPN2	ivenue.dyndns.org	192.168.100.0/255.255.255.0	DES/MD5	Autokey (IKE)	WAN 1 Connected	Initiator (Quick) : established

IPSec Policy Setup – Set Options

8. Set Options Page
   a. After adding the policy on the same page, click on the **Set Options** button
   b. At the Dead Peer Detection Feature
      i. Check enabled the **Detection** check mark
   c. **Check Method:** select DPD (RFC 3706)
   d. **Check After Idle, and Retry Times:** leave as is
   e. **Action:** select Keep Tunnel Alive
   f. Click on the **SET** button
   g. Click on the **Update** button on the IPSec Policy Setup screen.



PSec Policy options

Tunnel Attributes

State	Name	Security Gateway	Remote Network	Security Level	Key Type	Interface	Negotiation Status
Enabled	VPN2	60.54.118.173	192.168.100.0/255.255.255.0	DES/MD5	Autokey (IKE)	WAN 1 Connected	Initiator (Quick) : established

Dead Peer Detection Feature

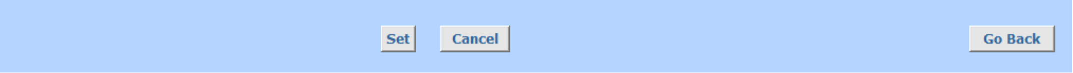
Detection	☑ Enabled		
Check Method	○ Heartbeat	○ ICMP Host 0.0.0.0	● DPD (RFC 3706)
Check After Idle	60 Seconds		
Retry Times	10		
Action	○ Failover	○ Remove Tunnel	● Keep Tunnel Alive
Logging	☑ Enabled		

NAT Traversal Feature

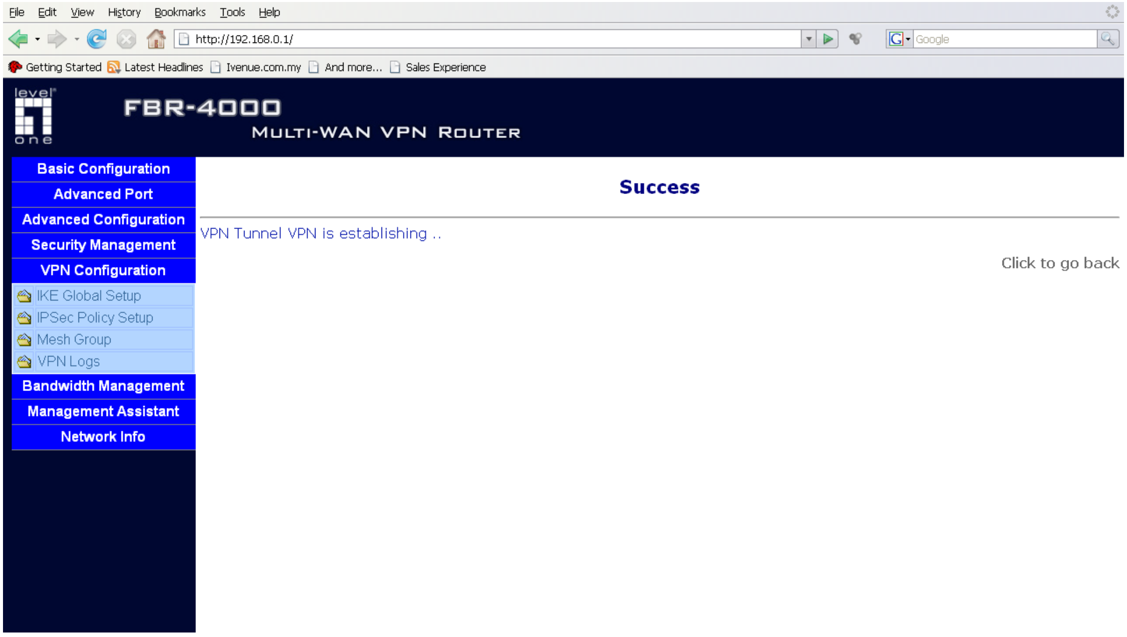
NAT Traversal	□ Enabled		
Keep Alive Interval	0 Seconds	UDP Checksum	□ Enabled

Options

NetBIOS Broadcast	☑ Enabled	Check ESP Pad	□ Enabled
Auto Triggered	☑ Enabled	Allow Full ECN	□ Enabled
Anti Replay	□ Enabled	Copy DF Flag	□ Enabled
Passive(Responder) Mode	□ Enabled	Set DF Flag	□ Enabled



To establish the VPN tunnel on the Advance Settings page click the connect button below. You will see this message:



Success

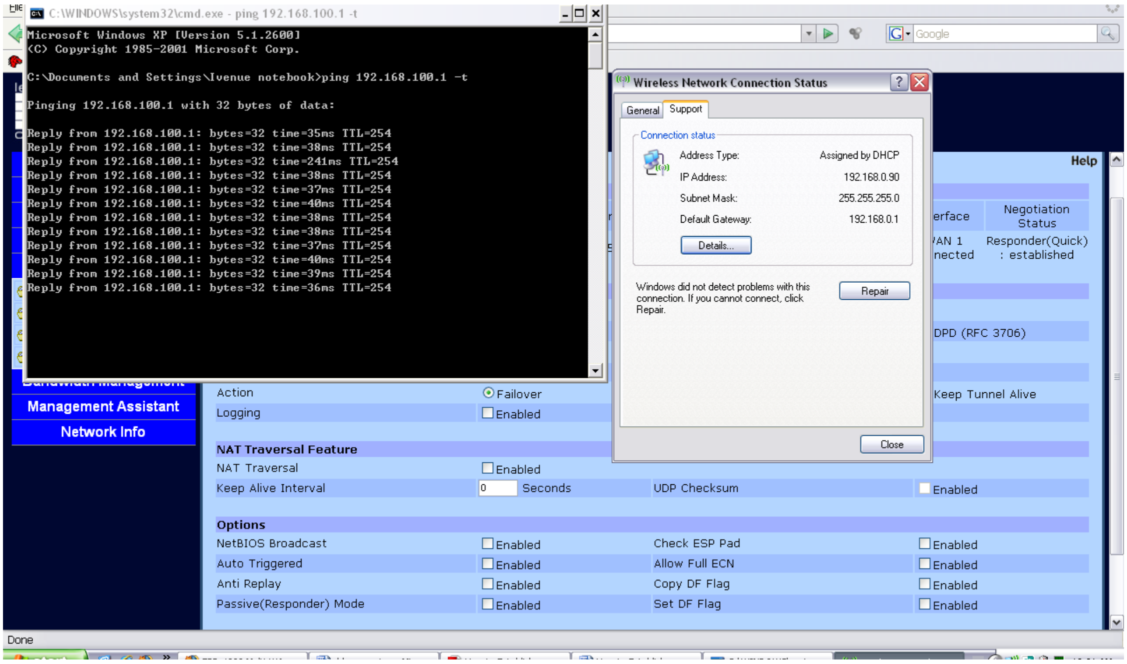
VPN Tunnel VPN is establishing ..

Click to go back

Once the VPN tunnel has been established, proceed to test the VPN connectivity by pinging the internal IP address of the FBR-4000(1) from the FBR-4000(2) network or vice versa.

Ex. Ping 192.168.100.1 –t

If you get replies from 192.168.100.1 (LAN IP address of the FBR-4000(1), in our example), then the VPN Connectivity has been configured properly.



C:\WINDOWS\system32\cmd.exe - ping 192.168.100.1 -t

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Ivenue notebook>ping 192.168.100.1 -t

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time=35ms TTL=254
Reply from 192.168.100.1: bytes=32 time=38ms TTL=254
Reply from 192.168.100.1: bytes=32 time=241ms TTL=254
Reply from 192.168.100.1: bytes=32 time=38ms TTL=254
Reply from 192.168.100.1: bytes=32 time=37ms TTL=254
Reply from 192.168.100.1: bytes=32 time=40ms TTL=254
Reply from 192.168.100.1: bytes=32 time=38ms TTL=254
Reply from 192.168.100.1: bytes=32 time=38ms TTL=254
Reply from 192.168.100.1: bytes=32 time=37ms TTL=254
Reply from 192.168.100.1: bytes=32 time=40ms TTL=254
Reply from 192.168.100.1: bytes=32 time=39ms TTL=254
Reply from 192.168.100.1: bytes=32 time=36ms TTL=254
```

Wireless Network Connection Status

Connection status

Address Type:	Assigned by DHCP
IP Address:	192.168.0.90
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1

Windows did not detect problems with this connection. If you cannot connect, click Repair.

erface	Negotiation Status
AN 1 nected	Responder(Quick) : established

DPD (RFC 3706)

Keep Tunnel Alive

Action	● Failover
Logging	□ Enabled

NAT Traversal Feature

NAT Traversal	□ Enabled		
Keep Alive Interval	0 Seconds	UDP Checksum	□ Enabled

Options

NetBIOS Broadcast	□ Enabled	Check ESP Pad	□ Enabled
Auto Triggered	□ Enabled	Allow Full ECN	□ Enabled
Anti Replay	□ Enabled	Copy DF Flag	□ Enabled
Passive(Responder) Mode	□ Enabled	Set DF Flag	□ Enabled