



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



FBR-	4000 Multi-WAN VPN RI	OUTER	
Basic Configuration Advanced Port	Dynamic DNS		?
Advanced Configuration	Dynamic DNS Service		Неір
Antiperation Host IP	Service Server Name	DynDNS.org	
Virtual Server Special Application	User Name Password	skyxis	
Dynamic DNS Multi DMZ	Verify Password Domain Name	antiv.dyndns.org	
🖄 UPnP Setup 🖄 NAT Setup	Additional Settings		
ARP Status	Enable Wildcard Enable Backup MX		
Security Management	Mall Exchanger		
Bandwidth Management	WAN 1	Force Update	
Management Assistant Network Info	Submit Cancel		

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
 - I. 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
_	Update Submit and Reboot Cancel

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.

Policy Entry Traffic Binding Local Identity Option New Policy Name State Interface Session Type VPN2 ✓ Enabled WAN 1 ✓ Session 1 ✓ None ✓ Traffic Selector Man ✓ Session 1 ✓ None ✓ Protocol Type Any M Session 1 ✓ None ✓ Local Security Network Subnet IP Address Subnet Mask Port Range Local Security Network Subnet IP Address Subnet Mask Port Range Remote Security Network Identity Type 255.255.255.0 0 ~ 0 Remote Security Gateway Identity Type Security Level	ate
New Policy Name State Interface Session Type New Policy VPN2 VEnabled WAN 1 v Session 1 v None v Traffic Selector Protocol Type Any v Local Type IP Address Subnet Mask Port Range Local Security Network Subnet v 192.168.100.0 255.255.255.0 0 ~ 0 0 Remote Security Network Subnet v 192.168.1.0 255.255.255.0 0 ~ 0 0 Remote Security Gateway Identity Type Domain Name v dddtd.dyndns.org Resolve and update	ate
Traffic Selector Protocol Type Any • Local Security Network Local Type Image: Subnet • 192.168.100.0 Remote Security Network Remote Type Subnet • 192.168.1.0 Subnet • 192.168.1.0 Remote Security Network Subnet • Subnet • 192.168.1.0 Security Gateway Domain Name • ddctt.dyndns.org Resolve and upda	ate
Traffic Selector Protocol Type Any ♥ Local Security Network Local Type IP Address Subnet Mask Port Range Local Security Network Subnet ♥ 192.168.100.0 255.255.255.0 0 ~ 0 Remote Security Network Remote Type IP Address Subnet Mask Port Range Remote Security Gateway Identity Type Identity Type Resolve and update Security Level Economic Security Cateway Economic Security Cateway Resolve and update	ate
Traffic Selector Protocol Type Any Local Security Network Local Type Subnet 192.168.100.0 Remote Security Network Remote Type Subnet 192.168.1.0 Subnet 192.168.1.0 Remote Security Gateway Identity Type Domain Name ddctt.dyndns.org Resolve and update Eccared atom	ate
Protocol Type Any w Local Security Network Local Type IP Address Subnet Mask Port Range Subnet v 192.168.100.0 255.255.255.0 0 ~ 0 Remote Security Network Remote Type IP Address Subnet Mask Port Range Subnet v 192.168.1.0 255.255.255.0 0 ~ 0 Remote Security Gateway Identity Type Identity Type Resolve and update Security Level Eccarediation Format Eccarediation Format Eccarediation Format	ate
Local Security Network Local Type IP Address Subnet Mask Port Range Subnet 192.168.100.0 255.255.255.0 0 ~ 0 Remote Security Network Remote Type IP Address Subnet Mask Port Range Subnet 192.168.1.0 255.255.255.0 0 ~ 0 Remote Security Gateway Identity Type Identity Type Resolve and update Security Level Economic Economic Economic	ate
Local Security Network Subnet 192.168.100.0 255.255.255.0 0 ~ 0 Remote Security Network Remote Type IP Address Subnet Mask Port Range Subnet 192.168.1.0 255.255.255.0 0 ~ 0 Remote Security Gateway Identity Type Identity Type Resolve and update Security Level Eccareculation Format Eccareculation Format Eccareculation Format	ate
Remote Security Network Remote Type IP Address Subnet Mask Port Range Subnet 192.168.1.0 255.255.255.0 0 ~ 0 Remote Security Gateway Identity Type Identity Type Resolve and update Security Level Escargulation Format ESCargulation Format Security Secur	ate
Remote Security Network Subnet 192.168.1.0 255.255.255.0 0 ~ 0 Remote Security Gateway Identity Type Domain Name dddtt.dyndns.org Resolve and upda	ate
Remote Security Gateway Identity Type Domain Name dddtt.dyndns.org Resolve and upda Security Level Eccapeulation Ecom	ate
Security Level	ate
Security Level	
Security Level	
Encangulation Format FSP v	
Encryption Method DES	
Authentication Method MD5 👻	
Key Management	
Key Type Autokey (IKE)	
Nadez i regenadori a zagresor nada kilo za	
Perifect rolward secrecy DH Group 2 (1024-bit)	
Preshared Key test Characters / Hexity	
Key Lifetime 28800 Seconds Note : 0 for no expiry	
In Volume 0 Kbytes	
Action	1
Disconnect Flush Tunnel Reload Policy Tunnel Status Set Options	
Add Delete Update Refresh	
Tunnel List	
State Name Security Gateway Remote Network Security Level Key Type Interface	Status
WAN 1 R	esponder
Enabled VPN antiv.dyndns.org 192.168.0.0/255.255.255.0 DES/MD5 Autokey (IKE) Connected (Ag	gressive)
R	esponder
Enabled VPN2 ddctt.dyndns.org 192.168.1.0/255.255.25.0 DES/MD5 Autokey (IKE) Connected ((Quick):



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 Po	icv opti	ons								2
										Help
Tunnel At	tributes									
State	Name	Security Gateway		Remote Net	twork		Security Level	Кеу Туре	Interface	Negotiation Status
Enabled	VPN	218.208.236.134	192.168.0.0/255.255.255.		.255.255.0	I	DES/MD5	Autokey (IKE)	WAN 1 Connected	Initiator(Quick) : established
Dead Pee	r Detecti	on Feature								
Detection			🗹 Ena	bled						
Check Met	hod:		OHea	artbeat			MP Host 0.0.0.0		⊙ DPD (RFC	3706)
Check Afte	er Idle		60	Seconds						
Retry Times			10	10						
Action O Faile		Failover O Remove Tunnel				⊙Keep Tunnel Alive				
Logging			🗹 Ena	abled						
NAT Trave	ersal Fea	ture	_							
NAT Trave	rsal		Ena	bled						
Keep Alive	Interval		0 Seconds		l	UDP Checksum		Enabled		
Options										
NetBIOS B	roadcast		🗹 Enabled		0	Check ESP Pad		Enabled		
Auto Triggered		🗹 Ena	abled	/	Allow Full ECN		Enabled			
Anti Replay Enabled		0	Copy DF Flag		Enabled					
Passive(Re	esponder)	Mode	🗌 Ena	abled	9	Set DI	F Flag		Enabled	
				Set	Cancel					Go Back

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

Created by **IVENUE** Solutions Sdn Bhd Enginer: Lai Yit Hua P



- 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
- I. 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	Enable Disable Delete Reload
	Update Submit and Reboot Cancel

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)

Created by IVENUE Solutions Sdn Bhd Enginer: Lai Yit Hua Pa



- 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				
				Неір
Policy Entry		Traffic Binding	Local Identity Option	
New Policy Name	State	Interface Session	Туре	
VPN2	Enabled	WAN 1 💌 Session 1 🜱	None 💌	
Traffic Selector				
Protocol Type	Any 🖌			
La cal Grandha Nabarah	Local Type	IP Address	Subnet Mask	Port Range
Local Security Network	Subnet 🖌	192.168.1.0	255.255.255.0	0 ~ 0
Demote Consulty Nature	Remote Type	IP Address	Subnet Mask	Port Range
Remote Security Networ	subnet 🖌	192.168.100.0	255.255.255.0	0 ~ 0
Demote Convite Cotour	Identity Type			
Remote Security Gatewa	Domain Name 💌	ivenue.dyndns.org		Resolve and update
Security Level				
Encapsulation Format	ESP 👻			
Encryption Method	DES	~		
Authentication Method	MD5	v		



Key Manag	jement											
Кеу Туре			Autokey (IKE) 💌									
Phase 1 Ne	gotiatior	ı	Aggressive M	Aggressive Mode 💌								
Perfect For	ward Se	crecy	DH Group 2 (1024-bit)									
Preshared K	(ey		test					Characters	/ Hex:0x			
Kev Lifetime	e		In Time	2880	00 S	econds		Note : 0 for	no expiry			
In Volume 0 Kbytes												
Action	Action											
Disconne	Disconnect Flush Tunnel Reload Policy Tunnel Status Set Options											
						-						
				Add	Delete	Update	e Refresh					
Tunnel List	t											
State	Name	Security Gatew	ау	Remote	e Network		Security Level	Кеу Туре	Interface	Negotiation Status		
Enabled	VPN2	ivenue.dyndns.	org 192	.168.100.0	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 Featurei. 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.

DSec Dol	icy opti	ons							2
PSECPO		ons							Help
Tunnel Att	tributes								
State	Name	Security Gateway		Remote Network		Security Level	Кеу Туре	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	r Detecti	on Feature							
Detection			🗹 Ena	abled					
Check Met	hod		OHea	artbeat		1P Host 0.0.0.0		• DPD (RFC 3	3706)
Check Afte	er Idle		60	Seconds					
Retry Time	s		10						
Action			○ Fai	lover	ORen	nove Tunnel		Keep Tunne	el Alive
Logging			🗹 Ena	abled					
NAT Trave	ersal Fea	ture							
NAT Trave	rsai		L Ena	abled				-	
Keep Alive	Interval		0	Seconds	UDP C	necksum		Enabled	
Options									
NetBIOS B	roadcast		🗹 Ena	abled	Check	ESP Pad		Enabled	
Auto Trigg	ered		🗹 Ena	abled	Allow Full ECN		Enabled		
Anti Replay	/		🗌 Ena	abled	Сору [DF Flag		Enabled	
Passive(Re	sponder)	Mode	Ena	abled	Set DF	Flag		Enabled	

Created by **IVENUE** Solutions Sdn Bhd Enginer: Lai Yit Hua

Page 8/10



		- 1		
Set	t (Cancel		Go Back

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

<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookma	rks Toole Help
< - 🔶 - 🥑 😣 🏠 🗈	http://192.168.0.1/
🏟 Getting Started 🔝 Latest Headlin	es 📄 Ivenue.com.my 🕒 And more 🗋 Sales Experience
FBR one	4000 Multi-WAN VPN Router
Basic Configuration	
Advanced Port	Success
Advanced Configuration	
Security Management	VPN TURRET VPN IS ESTADIISTING
VPN Configuration	Click to go back
🗠 IKE Global Setup	
A IPSec Policy Setup	
Mesh Group	
Bandwidth Management	
Management Assistant	
Network Info	
INCLWOIR IIIO	
	i de la constante de

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.

level" one

How to establish an IPSec VPN Tunnel with 2 FBR-4000 using DDNS

 C:WHNDOWSkystem32kmd.exe = ping 192.168.100.1 -t Kicrosoft Windows XP [Ueresion 5.1.2600] C: Oopyright 1985-2001 Microsoft Corp. C: Oopwright 1985-2001 Microsoft Corp. C: Ooeuments and Settings-Vuenue notebook>ping 192.168.100.1 Pinging 192.168.100.1 with 32 bytes of data: Reply from 192.168.100.1: bytes=32 tine=35ns TIL=254 Reply from 192.168.100.1: bytes=32 tine=37ns TIL=254 Reply from 192.168.100.1: bytes=32 tine=38ns TIL=254 Reply from 192.168.100.1: bytes=32 tine=39ns TIL=254 Reply from 192.168.100.1: bytes=32 tine=36ns TIL=254 	-€ ◆ ○ Failover	Wireless Network Connection Status General Support Connection Idus Address Type: Assigned by DHG PAddress: 122.168.0 Subnet Mask: 255.255.255 Default Gateway: 132.168.0 Details Windows did not detect problems with this connection. If you cannot connect, click Repair.	C • Google
Network Info NAT Traversal Feature NAT Traversal Keep Alive Interval Options NetBIOS Broadcast Auto Triggered Anti Replay Passive(Responder) Mode	Enabled Enabled Enabled Enabled Enabled Enabled Enabled	UDP Checksum Check ESP Pad Allow Full ECN Copy DF Flag Set DF Flag	Enabled Enabled Enabled Enabled Enabled Enabled