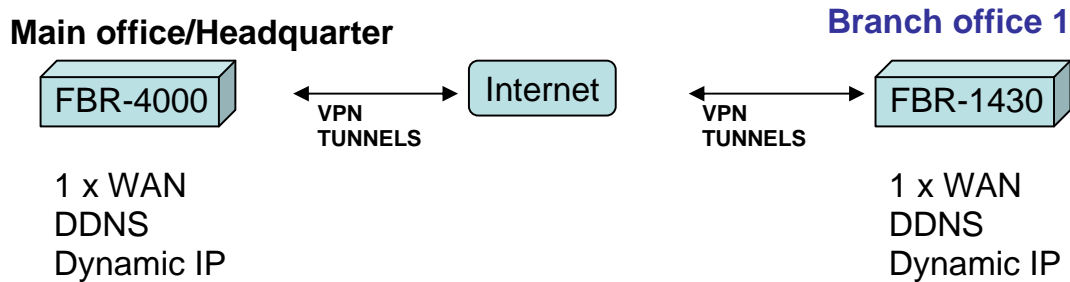


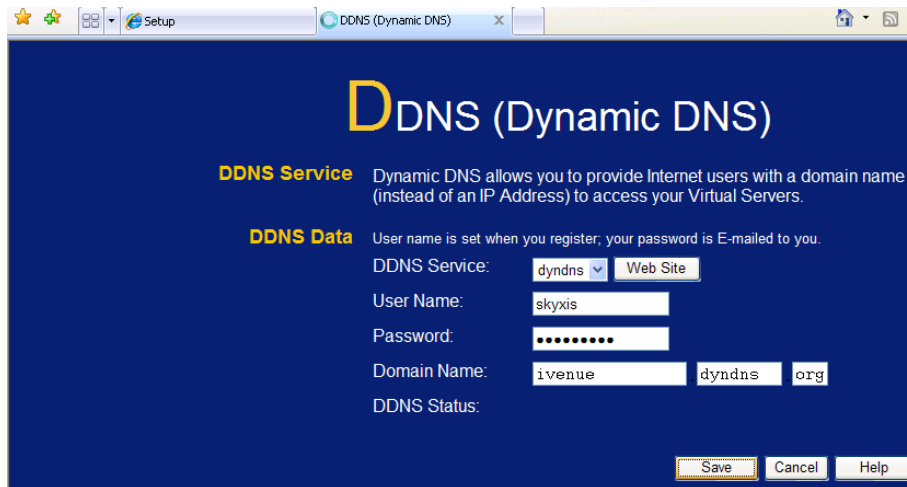


How to set up IPSec VPN using FBR-1430 & FBR-4000 with DDNS?



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 => ddctt.dyndns.org, IP address: 192.168.100.1
2. FBR-1430 => ivenue.dyndns.org, IP address: 192.168.1.1
To configure the Dynamic DNS into FBR-1430 perform the following:
3. Login into the GUI of the FBR-1430
4. Click on Advanced
5. Click on Dynamic DNS
6. Once on this page for the service select dyndns from the DDNS Service
7. For the User Name, input the username you have selected
8. For the Password, input your dyndns password
9. For the Domain Name, input the domain name for the respective unit (Refer step 2 above), (e.g.: ivenue.dyndns.org)
10. Click Save



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

11. Login into the GUI of the FBR-4000
12. Click on Advanced Configuration
13. Click on Dynamic DNS
14. Once on this page for the service select DynDNS.org from the drop down menu
15. Server Name leave as defaulted "members.dyndns.org"
16. For the User Name, input the username you have selected
17. For the Password, input your dyndns password
18. For the Verify Password, re-enter your password
19. For the Domain Name, input the domain name for the respective unit (Refer step 1 above) , (e.g.: ddctt.dyndns.org)
20. Omit the Additional Settings (Let all be blank)
21. Select the WAN1 or WAN2 as the WAN port to update its IP to the Dyndns.org servers
22. Click Submit



FBR-1430 Setup

1. Login into the GUI of the FBR-1430 and click on VPN then click on VPN Policies.
2. Click on Add New Policy



3. We can either use VPN Wizard to configure VPN or enter Setup Screen to configure the VPN parameter, let start with Setup Screen.

VPN Wizard

Check the VPN settings used by the remote VPN Server/Gateway.

This Wizard will configure your Router for a VPN connection to a remote VPN Endpoint (Server, Gateway, or Client).

- You will need to know the settings used on the remote VPN Endpoint.
- If using a Certificate for authentication, you must obtain your Certificate from a CA (Certification Authority) before running this Wizard.
- If you prefer to use a setup screen instead of a Wizard, click the "Setup Screen" button below.

VPN Policy Definition

Name: Enable Policy
 Allow NetBIOS traffic

Remote VPN endpoint Dynamic IP
 Fixed IP:
 Domain Name:

Local IP addresses
Type: IP address: ~
Subnet Mask:

Remote IP addresses
Type: IP address: ~
Subnet Mask:

Authentication & Encryption

AH Authentication

ESP Encryption Key Size: (AES only)

ESP Authentication

Manual Key Exchange

IKE (Internet Key Exchange)

Direction:

Local Identity Type:

Local Identity Data:

Remote Identity Type:

Remote Identity Data:

Authentication: RSA Signature (requires certificate)
 Pre-shared Key

Authentication Algorithm:

Encryption: Key Size: (AES only)

Exchange Mode:

IKE SA Life Time: (secs)

IKE Keep Alive Ping IP Address:

IPSec SA Life Time: (secs)

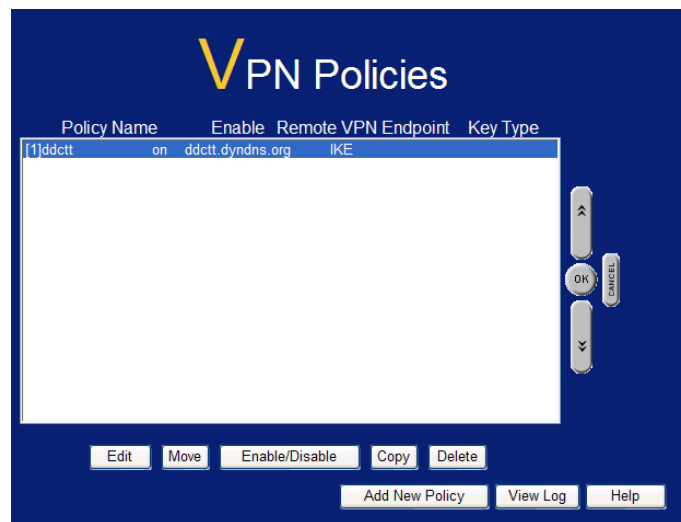
DH Group:

IKE PFS:

IPSec PFS:

4. Once on this page input the following parameters:
 - a) Name: input the text ddctt to the textbox
 - b) Enable Policy: select the check mark to enable the VPN Policy Definition
 - c) Allow NetBIOS traffic: select the check mark to enable the NetBIOS between two VPN network
 - d) Remote VPN endpoint: select the Domain Name enter ddctt.dyndns.org
 - e) Local IP addresses: select Subnet address: input the local IP address ID. ex. 192.168.1.0
 - f) Subnet Mask: input the local subnet mask. ex. 255.255.255.0

- g) Remote IP addresses: these settings apply to the local subnet of the FBR-1430, select Subnet 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) Authentication & Encryption: select the check mark to enable ESP Encryption as 3DES and Key Size as n/a
- j) Direction: select Responder only
- k) Local Identity Type: select Fully Qualified Domain Name
- l) Local Identity Data: type ivenue.dyndns.org
- m) Remote Identity Type: select Fully Qualified Domain Name
- n) Remote Identity Data: type ddctt.dyndns.org
- o) Authentication: select Pre-shared Key, and type test
- p) Authentication Algorithm: select MD5
- q) Encryption: select DES and n/a for Key Size
- r) Exchange Mode: select from the drop down menu Aggressive Mode
- s) IKE SA Life Time: input in the textbox 28800 seconds
- t) IKE Keep Alive: check the box to enable Keep Alive
- u) Ping IP Address: 202.188.0.133 (streamyx DNS)
- v) IPsec SA Life Time: input in the textbox 28800 seconds
- w) DH Group: select from the drop down menu Group 2 (1024 Bit)
- x) IKE PFS: select from the drop down menu Group 2 (1024 Bit)
- y) IPsec PFS: select from the drop down menu Disabled
- z) Click the ADD button to save the policy.



FBR-4000 Setup

1. Login into the GUI of the FBR-4000 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	<input checked="" type="checkbox"/>
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	<input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Reload"/>
<input type="button" value="Update"/> <input type="button" value="Submit and Reboot"/> <input type="button" value="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 Domain Name, input the local domain name. ex. ddctt.dyndns.org

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
- 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
- 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-1430. ex. ivenue.dyndns.org

5. Security Level

- a) Encapsulation Format: leave as defaulted ESP
- b) Encryption Method: select from the drop down menu DES
- 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 No PFS
- 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 Help

Policy Entry
 Name: VPN2 State: Enabled Traffic Binding: Interface: WAN 1 Session: Session 1 Local Identity Option: Domain Name: ddctt.dyndns.org

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 Domain Name: ivenuc.dyndns.org Resolve and update

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: No PFS
 Preshared Key: test Characters / Hex: 0x
 Key Lifetime: In Time: 28800 Seconds Note: 0 for no expiry
 In Volume: 0 Kbytes

Action
 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	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

Preshared Key: test Characters / Hex: 0x
 Key Lifetime: In Time: 28800 Seconds Note: 0 for no expiry

IPSec Policy Setup – Set Options

8. Set Options Page

- f) After adding the policy on the same page, click on the Set Options button
- g) At the Dead Peer Detection Feature
 - iii. Check enabled the Detection check mark
- h) Check Method: select DPD (RFC 3706)
- i) Check After Idle, and Retry Times: leave as is
- j) Action: select Keep Tunnel Alive
- k) Click on the SET button
- l) 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 DPD (RFC 3706)

Check After Idle Seconds

Retry Times

Action Failover Remove Tunnel Keep Tunnel Alive

Logging Enabled

NAT Traversal Feature

NAT Traversal Enabled

Keep Alive Interval 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

Set

Cancel

Go Back