



韌體版本: V 2.0.3Qno and later







Table of Contents

1. Introduction 概述 5

2. Main features:主要產品功能6

3. How To Install FVR9416-如何安裝 10

Hardware –硬體安裝介紹	10
FVR9416 前面板:	10
LED Status-面板燈號	10
Reset Button-硬體 Reset 按鈕	10
Replacing a Lithium Battery-更換系統內建電池	10
Setting up the Chassis-將 FVR9416 安裝於標準 19"機架上	11
Setting the Chassis on a desktop or other flat, secure surface	11
Rack-Mounting the Chassis	11
Wall-Mounting the Chassis-將 FVR9416 設備安裝在牆上	12
Connecting the FVR9416 to your Network-連接路由器到您的網路上	13

4. How To Manage FVR9416 15

Login-開始登入設定 FVR9416	15
Sitemap-網頁設定項目地圖總表	.錯誤! 尚未定義書籤。
Home-設定首頁	15
Port Statistics(硬體各埠口-Port 狀態即時顯示)	17
General Setting Status(一般設定狀態顯示)	19
Advanced Setting Status(進階設定狀態顯示)	19
Firewall Setting Status(防火牆設定狀態顯示)	20
VPN Setting Status(VPN 設定狀態顯示)	20
Log Setting Status: (系統日誌設定狀態顯示)	21
General Setting- 一般項目設定	22
Configure-設定	22
Multi WAN-多 WAN Port 設定	
QoS	
Password	
Time-系統時間設定	
Advanced Setting	41
DMZ Host-(Demilitarized Zone)	41



Forwarding	41
UPnP	45
Routing-路由通訊協定	46
One-to-One NAT 一對一 NAT 對應	48
DDNS-動態網域名稱	50
MAC Clone-變換實體 MAC 位置	52
DHCP-DHCP 發放 IP 伺服器	54
Setup-設定	54
Status-狀態顯示	56
Tool-工具程式	57
SNMP-網路通訊	57
Diagnostic-線上連線除錯測試	59
Restart-重新啓動	61
Factory Default-回復原出廠預設值	62
Firmware Upgrade-系統韌體升級	63
Setting Backup-系統設定參數儲存	64
Port Management-網路實體埠口管理	65
Port Setup-網路埠口設定	65
Port Status-網路埠口狀態即時顯示	66
Firewall-防火牆設定	67
General-一般	67
Access Rules-網路存取規則	68
Content Filter-網頁內容管制	72
VPN-虛擬私有網路	74
Summary-目前所有的 VPN 狀態顯示	74
Add New Tunnel-新增一條 VPN 通道	78
Gateway to Gateway-VPN 閘道器對閘道器的設定	78
Client to Gateway-VPN 客戶端對閘道器的設定	86
PPTP	97
VPN Pass Through-VPN 透通	98
Log-日誌	99
System Log-系統日誌	99
System Statistics-系統狀態即時監控	103
Logout	107



5. Troubleshooting 107

6. FAQ 107

7. Appendix A: VPN Configuration Sample 107

Sample VPN Environment 1: Gateway to Gateway	107
Sample VPN Environment 2: Gateway to Gateway	108
Sample VPN Environment 3: Client to Gateway (Tunnel)	109
Sample VPN Environment 4: Client to Gateway (GroupVPN)	110



1. Introduction 概述

FVR9416 為一台符合 SME 等級經濟型,高效能整合型之全功能新一代設計之防火牆系統,除了具備絕大多 數寬頻市場適用的對外連線能力外,還內建了 16 Port 10/100Mbps QoS 及 VLAN 交換器,以滿足多數企業對防 火牆的市場需求,FVR9416提供了硬體 DMZ 埠口為防火牆的標準配備使用外,並且提供四個 WAN ports.此四個 WAN ports 不僅可以支援高效能網路自動負載平衡模式(Intelligent Balancer by auto mode),亦可針對特定使 用者的 IP 群組,以提供分級服務 classes of service (CoS) (IP Group by Users).

配合新一代,多樣化之高安全整合性的防火牆設備需求環境,內建超高速的 Intel IXP 425 整合型 RISC CPU, 透過時脈 533Mhz 的高速處理架構下,發揮超高的網路效能,處理速度直逼中,大型企業用戶專用之昂貴防火牆 設備;可符合企業界廣泛的應用系統支援,防火牆效能可達 200Mbps 以上,且具備支援目前企業廣泛應用之虛擬 私有網路 VPN 硬體加速模式,包含 IPSec DES/3DES 等 VPN 加密,同時可以處理 200 條的 VPN 連線,以 3DES 方式運作效能可達 70Mbps 以上,不論式功能面,實用安全性等,十足超越目前大型昂貴設備之規格.

FVR9416 IPSec VPN 適用於各辦公室, 事業夥伴及遠端使用者一個安全便利的網路加密方式. 包括 168 bit Data Encryption Standard (3DES), 56 bit Data Encryption Standard (DES), 以及 AH/ESP 方式. VPN 功能 提供了各分支點間或大多數遠端使用者採 VPN 方式將資料自動加密解密的通訊方式,支援 Gateway To Gateway, Client To Gateway 與 Group VPNs 等模式

FVR9416 內建進階型防火牆功能,能夠阻絕大多數的網路攻擊行為,使用了 SPI 封包主動偵測檢驗技術 (Stateful Packet Inspection),封包檢驗型防火牆主要運作在網路的層級,但是藉由執行對每個連結的動態檢驗,也擁有應用程式的警示功能,讓封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結,預設自動偵測並阻擋. FVR9416 亦同時支援使用網路地址轉換 Network Address Translation (NAT)功能以及 Routing 路由模式,使網路環境架構更爲彈性,易於規劃管理.

Content Filtering 內容過濾功能允許企業內部自訂網路存取規則,管理頁面內建可新增移除的過濾名單,可讓 管理者選擇應該禁止存取或記錄監控哪些種類的網站,如此可對學校或企業的 Internet 管理有明確的策略.自 定過濾設定;透過完整的OS管理核心.FVR9416提供線上多樣化的日誌(SysLog)紀錄,支援線上管理設定工具, 可清楚易懂的網路設定組態、並加強管理全部的網路安全存取政策、VPN、及其他服務等.

FVR9416 能充分保障各型分支機構辦公室及各點間通訊的安全, 避免日益趨多的商業機密竊取與攻擊破壞等.專屬的 OS 獨立式作業平台, 使用者無須具備專業級的網路知識即可易於安裝使用. 透過瀏覽器如:IE, Netscape..來使用設定與管理 FVR9416 防火牆.



2. Main features:主要產品功能

Product Features

網路連線:

- One IP address to access the Internet over your entire network
- WAN: DHCP client, static IP, PPPoE,PPTP
- DMZ: DHCP client, static IP, PPPoE
- LAN: DHCP auto-assignment, Mac-assignment DHCP static IP, Static IP.

Multi-WAN 多線網路連結:

- 全自動型的負載平衡模式 Intelligent Balancer (Auto Mode)
- 網路服務偵測-NSD for Intelligent Balancer
- 特定使用者的 IP 群組,以提供分級服務 classes of service (CoS) (IP Group by Users)
- 協定綁定 Protocol Binding
- 服務質量 QoS

TCP/IP 通訊協定:

- DHCP Client/Server
- IP & MAC Binding
- PPPoE
- NAT with popular ALG support
- NAT with port forwarding
- NAT with port triggers
- DNS 轉送功能-DNS Relay
- ARP
- ICMP
- FTP/TFTP
- 密碼保護-Password protected configuration or management sessions for web access
- 全自動型的負載平衡模式 Intelligent Balancer (Auto Mode)
- 特定使用者的 IP 群組, 以提供分級服務 classes of service (CoS)
- 以埠口為基礎的頻寬政策 Port-based QoS
- 時間伺服器通訊協定 NTP Time Server



路由通訊協定:

- 支援動態路由 RIP 1, RIP 2 compatible, 靜態路由 Static routing
- 支援閘道器模式 Gateway/路由模式 Routing Mode Support

路由器管理功能:

- 網頁模式管理與政策設定-Comprehensive web based management and policy setting
- 支援網路管理通訊協定 SNMP v1/v2c
- 線上動態即時系統日誌 Monitoring, Logging, 系統告警功能 Alarms of system activities
- 具備由 Web 方式的韌體升級備份(Fault-tolerance Web upgrade new software)
- 具備雙份的可置換韌體儲存空間備份(Dual Firmware Backup or Restore)
- Supports filter capability (Service and IP)
- 支援系統日誌以及電子郵件自動告警功能(Support Syslog & E-Mail Alert.)

防火牆功能:

- 防火牆主動封包檢測技術-Stateful Packet Inspection Firewall
- IP 位置過濾功能-IP filtering; allows you to configure IP address filters
- 埠口位置過濾功能-Port filtering; allows you to configure TCP/UDP port filters
- 支援硬體式的 DMZ 獨立埠口-Support Hardware DMZ to protect your network
- 阻斷式攻擊-Denial of Service (DoS) prevention Dos attack prevention
- 網頁內容過濾機制-Inappropriate URL command line filter
- 可設定網路存取時間控制-Set Internet accessing time schedule
- 網路攻擊模式偵測-Syn Flooding/IP Spoofing/Win Nuke/Ping Of Death

VPN 虛擬私有網路功能:

- 支援高速 3DES VPN 連線效能速率可達 70Mbps-IPSec VPN 3DES Throughput 70Mbps UP.
- 支援 VPN 連線通道數 200 條-Support up to 200 VPN tunnels
- 支援 2 組群組 VPN 功能-Up to 2 Group VPNs support
- 簡單易懂的 VPN 設定與管理介面-Friendly VPN Tunnel Management
- 支援 IKE 功能-IKE : Pre-Shared keys
- 支援 IPSec 標準的 DES/3DES 加密-IPSec Encryption DES/3DES
- 支援以 IPSec 為標準的 MD5/SHA1 驗證-IPSec Authentication MD5/SHA1
- 支援 PMTU 的密鑰管理-Support PMTU Key management: IKE
- 支援網域名稱轉換 IP 位置 DNS Resolve



- 支援 PPTP 協定建立 VPN 通道
- 支援 VPN 透通功能-VPN Pass-through

其他功能:

- 虛擬主機 Virtual Server Port Forwarding.
- 特殊應用軟體 Port-Triggering Support
- 支援內建軟體式非軍事管制區 DMZ 功能-Support Software DMZ.
- 支援國際標準即插即用功能-UPnP Support
- 支援一對一的網路位置轉譯功能-One to One NAT Support.
- 動態 DNS 支援-DDNS Support
- 可變更的 WAN 網路實體位置-MAC Clone Change Support
- 線上對外線路測試功能-Diagnostic with DNS Lookup & Ping.
- 路由器參數設定備份或是儲存-Setting Backup with Import & Export.

封包傳輸效能:

- 防火牆效能-Firewall: 200Mbps
- VPN 虛擬私有網路效能-3DES 168bit VPN: Up to 70Mbps.

硬體規格:

- 中央處理器 CPU: Intel IXP425-533MHz RISC
- 記憶體 SDRAM: 64Mbyte
- 快閃記憶體 Flash Memory: 16Mbyte

網路支援通訊規格:

- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX

網路實體介面規格:

- 廣域網路 WAN 1~4: 10/100Base-T/TX RJ-45 ports
- DMZ: One 10/100Base-T/TX RJ-45 port
- 區域網路-LAN 1~11: 11 Port 10/100Base-T/TX RJ-45 ports
- 一個硬體重置按鈕可回覆出廠預設值-One reset button for factory default setting



LED顯示:

- 系統-電源與自我檢測功能 System: Power, DIAG
- 速度 Speed, 連線/動作 Link/Activity, 廣域網路 WAN,連結 Connect

操作環境:

- 工作溫度 Operating Temperature: 0⁰ ~ 45^oC (32⁰ ~ 113^oF)
- 儲存溫度 Storage Temperature: -20⁰ ~ 60⁰C (-4⁰ ~ 140⁰F)
- 溼度 Humidity: 0~90% non-condensing

安規驗證:

■ EMI/EMC: FCC Class A, CE Mark

外型尺寸:

■ 13" (L) x 9" (W) x 1.75" (H) Inch

電源供應:

■ Internal: AC100~240V / 50~60Hz

安裝方式:

- Desktop
- 19" Rack- Mount Tools Kit



3. How To Install FVR9416-如何安裝

Hardware –硬體安裝介紹

FVR9416 前面板:



LED Status-面板燈號

LED	顏色	Description
Power-電源	綠燈	綠燈亮: 電源開啓連接
DIAG-自我測試	橘燈	橘燈亮:系統尙未完成開機自我檢測功能. 橘燈熄滅:系統已經正常完成開機自我檢測功能.
Link/Act-連線/動作	綠燈	綠燈亮: 乙太網路連線正常 綠燈閃爍: 乙太網路埠口正在傳送/接收封包資料傳輸
Speed-速度	黃燈	黃燈亮:乙太網路連線在 100Mbps 的速度 黃燈熄滅:乙太網路連線在 10Mbps 的速度
WAN-廣域網路	綠燈	綠燈亮: 指定為廣域網路埠口 綠燈熄滅:指定為區域網路埠口
Connect-連結	綠燈	綠燈亮:當 WAN 端連線並取得 IP 位置. 綠燈熄滅:當 WAN 端連線並未取得 IP 位置

Reset Button-硬體 Reset 按鈕

Action	Description
按下 Reset 按鈕 5 秒	熱開機,重新啓動 FVR9416 DIAG 燈號: 橘色燈號慢慢閃爍
按下 Reset 按鈕 10 秒以上	回復原出廠預設值(Factory Default) DIAG 燈號: 橘色燈號快閃.

Replacing a Lithium Battery-更換系統內建電池

FVR9416 防火牆路由器內建有系統時間的電池. 此電池使用壽命約為 1~2 年. 當電池已經無法充電或是使用壽命到達後, FVR9416 將無法正確紀錄時間或是連接網際網路的同步 NTP 時間伺服器,您必須與您的系統廠商聯繫,以便取得更換電池的技術. Note: 請勿自行拆解機器,若您需要更換電池的話,請與我們聯繫!



Setting up the Chassis-將 FVR9416 安裝於標準 19"機架上

您可以將 FVR9416 放置於桌上使用,或是您有機房專用 19 吋標準機架的話,可以將 FVR9416 安裝於機架上,每一台 FVR9416 都有配備專用連接機架配件.

Setting the Chassis on a desktop or other flat, secure surface

若您需要安裝 FVR9416 於機架上的話,請不要將其他過重的物品堆疊或是放置於機器上,以免因承受重量過重而發生危險或是 損傷機器本體.

Rack-Mounting the Chassis

每一台 FVR9416 都有配備專用連接機架配件,包含 2 只 brackets 以及八顆專用螺絲提供與 FVR9416 連接安裝使用.



當您安裝鎖定 FVR9416 所提供的機架專屬配件後,您可以直接安裝於您的標準機架上,如下圖所示:





Wall-Mounting the Chassis-將 FVR9416 設備安裝在牆上

於 FVR9416 機器底部有二個十字孔位,您可以使用一般螺絲先旋轉鎖進牆壁上,確認牢固後,再將 FVR9416 的底 部二個十字孔位準確的掛在此二顆螺絲上即可完成安裝,如下圖所示:





Connecting the FVR9416 to your Network-連接路由器到您的網路上



以下架構爲如何連接 FVR9416 防火牆路由器到您的網路上,連接模式有分爲二種:.





Figure 2: 防火牆 DMZ 模式

FVR9416 防火牆路由器到您的網路上,連接模式有分爲以下二種:



設定廣域網路連線(WAN connection): WAN 埠口可以連接如 xDSL Modem, Switch HUB 或是外部路由器.

設定區域網路連線(LAN connection): LAN 埠口可以連接如 Switch HUB 或是直接與 PC 連線.

設定 DMZ 埠口: 此埠口可以連接如外部合法 IP 位置的伺服器, 如網頁 (Web) 以及電子郵件伺服器(Mail servers)等.

接下來請連接 FVR9416 背部電源線,然後會看到 FVR9416 的面板 Power 燈號亮起,以及一小段時間做自我開 機測試即可開始使用並進行設置工作!



4. How To Manage FVR9416

Login-開始登入設定 FVR9416

連線到 192.168.5.8	6 ? 🔀
	G
使用者名稱(U):	😰 admin 💌
密碼(P):	*****
	2記憶我的密碼(R)
	確定 取消

請輸入使用者名稱(User Name)與密碼(Password)於上方所示密碼驗證欄位當中,然後按下"確定"按鈕.

FVR9416 防火牆路由器其預設的使用者名稱(User Name)與使用者密碼(Password)皆為'admin',您可以於稍後設定時,更改此登入密碼!我們強烈建議您務必更改管理密碼!!

Home-設定首頁

此首頁畫面(Home)顯示 FVR9416 防火牆路由器目前系統所有參數以及狀態顯示資訊,此資訊僅提供管理者讀 取.若您想進一部查詢該細部相關設定的話,可以按下各系不選向前端之超連結按鈕,並可以快速立即進入該選 項設定當中.此畫面也顯示了兩種語言版本(英文與簡體中文).請按下要顯示語言版本的按鈕,此按鈕也會自動 改變成綠色顯示出目前的版本畫面.



System Information

\bigcirc			
ONO	Home		Logout
Home General Setting	English 简体中文		
Advanced Setting	System Information		
Tool	Serial Number : NIF204900003	Firmware version :	2.0.0-qnoRC10 (Jan 14 2005 16:40:05)
Port Management	CPU : Intel IXP425-533 System active time : 5 Days 13 Hours 18	DRAM : 64M 3 Minutes 37 Seconds	Flash: 16M
Firewall	Current time : Mon Jan 24 2005 11:47:57	1	

Serial Number:(機器序號)

此爲顯示 FVR9416 的機器序號.

Firmware version:(韌體版本資訊)

此爲顯示 FVR9416 的目前使用的韌體版本資訊.

CPU:

此爲顯示 FVR9416 使用的 CPU 型號為 Intel IXP425-533Mhz.

DRAM:

此為顯示 FVR9416 使用記憶體(DRAM)為 64MB.

Flash:

此爲顯示 FVR9416 使用快閃記憶體(Flash)為 16MB.

System active time:

此爲顯示 FVR9416 目前已經開機的時間.

Current time:

此爲顯示 FVR9416 目前正確時間,但是必須注意,您需要正確設定與遠端 NTP 伺服器的時間同步後才會正確 顯示.



Port Statistics(硬體各埠口-Port 狀態即時顯示)

1	Port Sta	tistics							
	Port ID	1	2	3	4	5	6	7	8
	Interface	r <mark>face</mark> LAN LA		LAN	LAN	LAN	LAN	LAN	LAN
Status Conr		Connected	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
	Port ID	9	10	11	12	13	14	15	DMZ
	Interface	LAN	LAN	LAN	WAN4	WAN3	WAN2	WAN1	DMZ
	Status	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Connected	Enabled

在此畫面會顯示系統各埠口(Port)目前即時狀態顯示,包含每一個 Port (Connected-已經連接, Enabled-開啓, Disabled-關閉).使用者可以按下此狀態按鈕,查看各埠口更詳細的資料顯示.於 summary table 總表,會顯示目前該埠口設定狀態如,網路連接 Link (up or down),埠口 Port 開啓或關閉 Disable(on or off),高低優先權 Priority (高 High or 一般 Normal),連接速率 Speed Status(10Mbps or 100Mbps),工作模式 Duplex Status(半雙工 half or 全雙工 full),乙太網路自動偵測 Auto negotiation(Enabled or Disabled).於此項目表格中(statistics table),他將會顯示此埠口的接收 receive/傳送 transmit 的封包數以及 Byte 數/封包錯誤率等並計算總數量.



	Port1 Information
Type	10Base-T / 100Base-TX
Interface	LAN
Link Status	Up
Port Activity	Port Enabled
Priority	Normal
Speed Status	100 Mbps
Duplex Status	Full
Auto negotiation	Enabled
atistics	
Port Receive Packet Count	166549
Port Receive Packet Byte Count	33804474
Port Transmit Packet Count	229102
Port Transmit Packet Byte Count	246994709
Port Packet Error Count	0





General Setting Status(一般設定狀態顯示)

General Setting Status		
LAN IP :	192.168.1.1	
<u>VVAN1 IP</u> :	192.168.5.178	Release Renew
WAN2 IP :	0.0.0.0	Release Renew
WAN3 IP :	0.0.0.0	Release Renew
WAN4 IP :	0.0.0.0	Release Renew
DMZ IP :	0.0.0.0	
<u>Default Gateway</u> (WAN1) : (WAN2) : (WAN3) : (WAN4) :	192.168.5.1 0.0.0.0 0.0.0.0 0.0.0.0	
DNS (WAN1): (WAN2): (WAN3): (WAN4):	192.168.5.1 168.168.5.20 192.168.5.1 192.168.5.2 192.168.5.1 192.168.5.2	
<u>QoS</u> (WAN1 WAN2 3 4) :	Off Off Off Off	

LAN IP: 此爲顯示路由器的 LAN 端目前的 IP 位置設定資訊,系統預設為 192.168.1.1,並且可以按下該超連結直 接進入該設定項目中.

WAN1~4 IP: 此為顯示路由器的 WAN 1 端目前的 IP 位置設定資訊,並且可以按下該超連結直接進入該設定項 目中.當使用者選擇自動取得 IP 位置時(Obtain an IP automatically),他會顯示二個按鈕分別為釋放-release 與更新-renew. 使用者可以按下釋放- release 按鈕去做釋放 ISP 端所核發的 IP 位置,以及按下更新- renew 按鈕去做更新ISP端所核發的IP位置. 當選擇WAN端連線使用如 PPPoE 或是 PPTP的話,他會變為顯示 連 接-Connect 與中斷連線-Disconnect.

DMZ IP: 此為顯示路由器的 DMZ 目前的 IP 位置設定資訊,並且可以按下該超連結直接進入該設定項目中.

Default Gateway: 此爲顯示路由器的預設閘道 IP 位置設定資訊,並且可以按下該超連結直接進入該設定項目中 DNS: 此為顯示路由器的 DNS(Domain Name Server)的 IP 位置設定資訊,並且可以按下該超連結直接進入該 設定項目中.

QoS: 此為顯示路由器的 WAN1~4 是否有使用 QoS,並且可以按下該超連結直接進入該設定項目中.

Advanced Setting Status(進階設定狀態顯示)

Advanced Setting Status

DMZ Host :	Disabled						
Working Mode :	Gateway						
DDNS (WAN1 WAN2 3 4) :	Off	Ι	Off	Ι	Off	L	Off

DMZ Host: 此爲顯示路由器的 DMZ 功能選項是否啓動,並且可以按下該超連結直接進入該設定項目中.系統預



設此功能爲關閉.

Working Mode: 此為顯示路由器的目前工作模式(可為 NAT Gateway 或是 Router 路由模式),並且可以按下該 超連結直接進入該設定項目中.系統預設此功能為 NAT Gateway 模式.

DDNS: 此為顯示路由器的 **DDNS** 動態 **DNS** 功能選項是否啓動,並且可以按下該超連結直接進入該設定項目中. 系統預設此功能為關閉.

Firewall Setting Status(防火牆設定狀態顯示)

Firewall Setting Status

SPI (Stateful Packet Inspection) :	Off
DoS (Denial of Service):	Off
Block WAN Request :	Off
Remote Management :	On

SPI (Stateful Packet Inspection): 此為顯示路由器是否開啓 SPI (Stateful Packet Inspection)主動封包偵測過濾防火牆功能選項是否啓動(開啓-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off.

DoS (Deny of Service): 此為顯示路由器是否阻斷來自 Internet 上的 DoS 攻擊功能選項,是否啓動(開啓-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off.

<u>Block WAN Request</u>: 此為顯示路由器是否阻斷來自 Internet 上的 ICMP-Ping 的回應功能選項,是否啓動(開 啓-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off.

<u>Remote Management</u>: 此為顯示路由器的遠端管理功能選項是否啓動(開啓-On/關閉-Off),並且可以按下該超 連結直接進入該設定項目中.系統預設此功能為關閉-Off.

VPN Setting Status(VPN 設定狀態顯示)

VPN Setting Status

 VPN Summary :
 0

 Tunnel(s) Used :
 0

 Tunnel(s) Available :
 200

 No Group VPN was defined.
 200

 PPTP Server :
 Disabled

VPN Summary: 此為顯示路由器的 VPN 功能選項內容資訊,並且可以按下該超連結直接進入該設定項目中. Tunnel(s) Used: 此為顯示路由器的 VPN 功能目前已經設定的 Tunnel 數量.

Tunnel(s) Available: 此為顯示路由器的 VPN 功能目前可使用的 Tunnel 數量...

Current Connected (The Group Name of Group VPN1) users: 為顯示路由器的 VPN 1 目前線上使用 Tunnel



數量

Current Connected (The Group Name of Group VPN2) users: 爲顯示路由器的 VPN 2 目前線上使用 Tunnel 數量

若是 GroupVPN 為無設置的狀態,會顯示"No Group VPN was defined."-沒有 GroupVPN 被設定的資訊.

Log Setting Status: (系統日誌設定狀態顯示)

Log Setting Status

E-mail cannot be sent because you have not specified an outbound SMTP server address.

E-Mail 的超連結將會連到系統日誌設定畫面中:

1.若您無設定電子郵件伺服器(Mail Server)於系統日誌設定中(Log page),他將顯示您無設定電子郵件伺服器 所以無法發送系統日誌電子郵件-"E-mail cannot be sent because you have not specified an outbound SMTP server address."

2.若您已經設定電子郵件伺服器(Mail Server)於系統日誌設定中(Log page),但是 Log 尚未達到設定傳送的條件時,它將顯示電子郵件伺服器已經設置-"E-mail settings have been configured."

3.若您已經設定電子郵件伺服器(Mail Server)於系統日誌設定中(Log page), Log 也已經傳送出去時,它將顯示 電子郵件伺服器已經設置,並且已經發送- "E-mail settings have been configured and sent out normally."

4. 若您已經設定電子郵件伺服器(Mail Server)於系統日誌設定中(Log page), 但是 Log 無法正確傳送出去時, 它將顯示電子郵件伺服器已經設置,但是無法傳送出去,可能是設定有問題-"E-mail cannot be sent out, probably use incorrect settings."



General Setting- 一般項目設定

Q			Lanut
ONO	General Setting => Configur	e	Logour
General Setting			
Multi WAN	Host Name:	FVR9416	(Required by some ISPs)
QoS Password Time	Domain Name:	: FVR9416	(Required by some ISPs)
Advanced Setting			
DHCP	LAN Setting		
Tool	()	MAC Address: 00-0e-a0-00	-24-e8)
Port Management	Device IP Address		Subnet Mask
Firewall	192 . 168 . 1	1	255 . 255 . 255 . 0
Log	Multiple Subnet	Multiple Subnet Setti i / Edit	ing

此一般項目設定-General Setting 畫面為 FVR9416 防火牆路由器為基本的安裝設定內容.對大多數的用戶來說, 此預設的項目已經足夠連接網際網路而不需做任何變更.當然有些情況下使用者需要一些 ISP 所提供的進一步 詳細資訊.其詳細細部設定,請參考以下各節說明:

Configure-設定

Configure

Host Name & Domain Name: 可輸入路由器的名稱-Host name 以及網域名稱-Domain Name,於大多數的環境中不需做任何設定即可使用,國外有一些 ISP 可能需要用到!

Host Name:	FVR9416	(Required by some ISPs)
Domain Name:	FVR9416	(Required by some ISPs)

LAN Setting

此為顯示路由器的 LAN 端內部網路目前的 IP 位置設定資訊,系統預設為 192.168.1.1,子網路遮罩為 255.255.255.0.,可以依照您實際網路架構更動!



(MAC Address: 00-	-0c-41-00-0)0-00		
Device IP Address	255	Subne	t Mask	
	200	. 200	. 200	
ble-Subnet Setting				
LAN IP Address: 100 1 1 0				
Cubact Mark				
Sublict Mask : 200 . 200 . 200 . 0				
Update this Entry				
10. 1. 1. 0/255. 255. 255. 0		-		
11. 1. 1. 0/255. 255. 255. 0 100. 1. 1. 0/255. 255. 255. 0				
Delete selected subnet	Add New			
Save Setting Cancel Changes	Exit			

此功能提供 User 可以將不同於路由器網段的 IP 群組直接填入到 Multiple-Subnet 後就可直接上網,也就是若原來內部環境已經有多組不同 IP 群組時,內部電腦不需做任何修改就可以上網,可以依照您實際網路架構更動!



WAN Setting

WAN Setting

Please choose how many WAN ports you prefer to use : 4 🔽 (Default value is 4)

Interface	Connection Type	Config.
VVAN1	Obtain an IP automatically	<u>Edit</u>
WAN2	Obtain an IP automatically	<u>Edit</u>
VVAN3	Obtain an IP automatically	Edit
VVAN4	Obtain an IP automatically	Edit

Please choose how many WAN ports you prefer to use	請選擇您要設定 WAN 埠口的數目,預設值為 4.您可以依照自己的需要加以更改.
Interface:	顯示為第幾個 WAN 埠口
Connection Type	廣域網路 Internet 連線型態設定:可以區分爲四種.
	Obtain an IP automatically:自動取得 IP 位置; Static IP: 固定 IP 位置連線; PPPoE (Point-to-Point Protocol over Ethernet):PPPoE 撥號連線; PPTP (Point-to-Point Tunneling Protocol): PPTP 撥號連線
Config.:	顯示進一步更改設定:點選 Edit 進入近一步設定畫面.

WAN Connection Type:廣域網路 Internet 連線型態設定

Obtain an IP automatically:自動取得 IP 位置(常用在纜線數據機 Cable Modem 或是 DHCP 自動取得 IP 連線型 態上)

此為路由器系統預設的連線方式,此連線方式為 DHCP Client 自動取得 IP 模式,多為應用於如 Cable Modem 等連接,若您的連線為其他不同的方式,請依照以下介紹並選取相關的設定.或是使用者自訂 DNS 的 IP 位置(Use the Following DNS Server Address),與此選項勾選並自訂填入 DNS 的 IP 位置.

Obtain an IP automatically	¥
----------------------------	---

📃 Use the	Followi	n	g DNS 9	66	rver A	do	dresses:
DNS Server (Required) 1:	0		0		0		0
2:	0		0		0		0



Use the Following DNS	選擇使用自訂的 DNS 解析伺服器的 IP 位置.
Server Address:	
Domain Name Server (DNS):	驗↓你的 ISP 所相完的么稱解析伺服哭 IP 位置 最小酒诣↓—組

Domain Name Server (DNS): 輸入您的 ISP 所規定的名稱解析伺服器 IP 位置,最少頃填入一組, 解析伺服器 最多可填二組.

Static IP: 固定 IP 位置連線

若您的 ISP 有核發固定的 IP 位置給您(如 1 個 IP 或是 8 個 IP 等),請您選擇此種方式連線,將 ISP 所核發的 IP 資訊分別依照以下介紹塡入相關設定參數中

Notes:請注意,有一些 ISP 雖會提供固定如一個 IP 位置給您,但是有可能是使用如 DHCP 自動取得 IP 或是 PPPoE 撥接取得一個固定 IP 模式,雖是每次都取得相同 IP 位置,但連線模式您依然要選擇相關之模式才可!

	Static IP		*	
Specify WAN IP Address:	0	. 0	. 0	. 0
Subnet Mask:	0	. 0	. 0	. 0
Default Gateway Address:	0	. 0	. 0	. 0
DNS Server (Required) 1:	0	. 0	. 0	. 0
2:	0	. 0	. 0	. 0

Specify WAN IP Address:	輸入您的 ISP 所核發的可使用固定 IP 位置
Subnet Mask:	輸入您的 ISP 所核發的可使用固定 IP 位置的子網路遮罩,如:
	發放 8 個固定 IP 位置:255.255.255.248 發放 16 個固定 IP 位置:255.255.255.240
Default Gateway IP Address:	輸入您的 ISP 所核發的預設通訊閘,若您是使用 ADSL 的話,一般說來 都是 ATU-R 的 IP 位置,入此台若是使用光纖接入請塡光纖轉換器 IP.
Domain Name Server (DNS):	輸入您的 ISP 所規定的名稱解析伺服器 IP 位置,最少須填入一組,最多可填二組.

PPPoE (Point-to-Point Protocol over Ethernet):PPPoE 撥號連線

此項為 ADSL 計時制使用(適用於 ADSL PPPoE),填入 ISP 給予的使用者連線名稱與密碼並以路由器內建的



PPP Over –Ethernet 軟體連線,若是您的 PC 之前已經有安裝由 ISP 所給予的 PPPoE 撥號軟體的話,請將其移除,不需要再使用此個別連接網路。

	PPPoE	*		
Us	er Name:			
Р	assword:			
🔘 Cor	nnect on Demand: Max	ldle Time ⁵	Min.	
🔘 Ке	ep Alive: Redial Period	5	Sec.	
User Name:	輸入您的 ISP 所核發的	的使用者名稱		
Password:	輸入您的 ISP 所核發的	的使用密碼		
Connect-on-demand:	此功能能夠讓您的 PP 若是有上網需求時,FVI 無使用時,則系統會自動	PoE 撥接連絡 R9416 會自動 動離線(自動离	泉能夠使用自動撥 動撥號連線,當網距 維線無封包傳送時	號功能,當使用端 各一段時間閒置 間預設為5分鐘).

 Keep Alive:
 此功能能夠讓您的 PPPoE 撥接連線能夠保持聯線,且斷線後會自動重 撥,並且可以依使用者使用方式自行設定重新撥接的時間,預設為30秒.

PPTP (Point-to-Point Tunneling Protocol): PPTP 撥號連線

此項為 PPTP (Point to Point Tunneling Protocol) 計時制使用,填入 ISP 給予的使用者連線名稱與密碼並以 FVR9416 內建的 PPTP 軟體連線,(多為歐洲國家使用)

[РРТР	~
Specify WAN IP Address	.0	0.0
Subnet Mask:	. 0 .	0
Default Gateway Address	. 0 .	0.0
User Name	:	
Password	:	
Onnect on	Demand: Max Idle T	īme ⁵ Min.
🔿 Keep Alive:	Redial Period 30	Sec.



Specify WAN IP Address:	此項爲設定固定 IP Address,設定的 IP 可由您的 ISP 所提供的位置輸入(此 IP 位置各 ISP 都於裝機後給予,請詢問您的 ISP 給予相關資訊)
Subnet Mask:	如上將 ISP 的子網路遮罩位址資料填入
Default Gateway Address:	輸入您的 ISP 所核發的可使用固定 IP 位置的預設通訊閘,若您是使用 ADSL 的話,一般說來都是 ATU-R 的 IP 位置.
User Name:	輸入您的 ISP 所核發的使用者名稱
Password:	輸入您的 ISP 所核發的使用密碼
Connect-on-demand:	此功能能夠讓您的 PPTP 撥接連線能夠使用自動撥號功能,當使用端若 是有上網需求時,FVR9416 會自動向預設的 ISP 自動撥號連線,當網路 一段時間閒置無使用時,則系統會自動離線(自動離線無封包傳送時間 預設為 5 分鐘).
Keep Alive:	此功能能夠讓您的 PPTP 撥接連線能夠斷線自動重撥,而且可以自行設定重新撥接的時間,預設為 30 秒.

DMZ Setting

於某些網路環境應用來說,您可能會需要用到獨立的 DMZ 非軍事管制區介面來置放您的對外服務伺服器,如 WEB 與 Mail 伺服器等; FVR9416 提供一組獨立的 DMZ 介面來設定連接於合法 IP 位置的伺服器.此 DMZ 介面為連接 Internet 與區域網路之間的溝通橋樑.

DMZ Setting

	Interface	IP Address	Config.
	DMZ	0.0.0.0	Edit
Interface:	顯示為 DMZ t	₽□	
IP Address:	顯示目前預設	的網域網定固定 IP 位置.	
Config.	顯示進一步更	改設定:點選 Edit進入近一步設定畫面.	
	DMZ		
	Static IP	~	
Specify DMZ IP	Address: 0 . 0	. 0 . 0	
Sub	net Mask: 0	. 0	

Specify DMZ IP Address: 請輸入 DMZ 介面的 IP 位置資訊以及子網路遮罩.



Multi WAN-多 WAN Port 設定

於多 WAN 的運作模式當中,提供了使用者三種模式選擇,分別為一全自動型的負載平衡模式 Intelligent

Banancer(Auto Mode)以及 特定使用者的 IP 群體模式 IP Group (By Users)還有 IP 負載均衡 IP Balance.

全自動型的負載平衡模式 Intelligent Banancer(Auto Mode)的情況下

系統會自動整合 WAN1 到 WAN4 四條線路最大頻寬做最佳的負載平衡.

Home Home General Setting Configure Multi WAN QoS Password Time Advanced Setting DHCP	General Sett Mode Intelligent Bala IP Group (By U IP Balance	ing => Multi WAN ancer (Auto Mode) sers)		Logout
Port Management Firewall Log	Interface Set	ting VAN1 VAN2 VAN3 VAN4 VAN4	Mode Auto Auto Auto Auto	Config. Edit Edit Edit Edit
Mode: Interface Setting Interface Mode	全自動型的負載 此模式主要是讓 IP 負載均衡:IPE 此為最傳統的負 網時依序每一條 可選擇所需要進 顯示出廣域網路: 在選擇完 Auto 後 Intelligent Balan	平衡模式:Intelligent B 路由器自行做每一條 Balance 載均衡,若選擇此方式, WAN 做一個 IP 分配. 一步設定的介面. 埠口的數目. 後,其顯示的結果.在全日 cer (Auto Mode)的情報	Balancer (Auto Mode) WAN 的頻寬自動負載均衡 則路由器會依照每一台電腦上 · 自動型的負載平衡模式 況之下,會自動顯示出自動分酯	-



	頻寬 Auto.
Config.	可經由點選 Edit 進行進一步的設定.
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

Multi-WAN Config setting

Home General Setting Configure	General Setting => Multi WAN
QoS Password Time	The Max. Bandwidth provided by ISP : Upstream 512 Kbit/Sec Downstream 512 Kbit/Sec
Advanced Setting DHCP Tool Port Management Firewall VPN Log	Retry count 5 Retry timeout 30 When Fail Remove the Connection Default Gateway ISP Host Remote Host DNS Lookup Host
Interface:	顯示現在所要設定的廣域網路埠口.
The Max. Bandwidth provided by ISP:	需填入此條廣域端口實際支持的上傳(Upstream)及下載 (Downstream)的實際 ISP 帶寬.其範圍介於 0~100Mbits 之間
Network Services Detection:	網路對外服務偵測機制.若勾選此項設定,則會出現 Retry Count,Retry Timeout等以下的訊息.
Retry Count:	對外連線偵測重試次數,預設値為五次.若是於此測試次數當 中,Internet 沒有回應的話,路由器會判斷此條廣域端口對外線路中斷!
Retry Timeout:	對外連線偵測逾時時間(秒),預設値為 30.秒.若是於此秒數當中,你所設定的針測點沒有回應的話,路由器會判斷此條廣域網對外線路中斷.
When Fail	 (1)Generate the Error Condition in the System Log:在系統日誌中會產生錯誤訊息的資訊:當偵測到與 ISP 連結失敗時,系統就會在系統日誌中將這項錯誤訊息紀錄下來,但依舊保持此線路不會移除,所以會有些原來在此條線路上的 User 無法正常使用. (2)Remove the Connection 移除有問題線路:當偵測到與 ISP 連結失敗時,系統不會在系統日誌中將這項錯誤訊息紀錄下來.原本在此



	WAN 端的封包傳遞會自動轉換到另一條廣域端口.等到原本斷線的廣 域端口恢復後會自行重新連結,則封包傳遞會自動轉換回來.
Default Gateway:	預設通訊閘道位置,如 ADSL 或纜線數據機及光纖轉換器的 IP 位置
ISP Host:	將此欄位填入 ISP 端的 DNS 解析伺服器,填入前請確定此 DNS 是會做回應. ISP 端的偵測位置,如 ISP 的 DNS IP 位置等,在設定此 IP 地址時請確認此 IP 地址是可以且穩定快速的得到回應. (建議填入 ISP 端 DNS IP)
Remote Host:	遠端的網路節點偵測位置,此 Remote Host IP 地址最好也是可以且穩定快速的得到回應.(建議填入 ISP 端 DNS IP)
DNS Lookup Host:	網域名稱端DNS的偵測位置網域名稱端DNS的偵測位置(此欄位只許 填入網址如"www.hinet.net",請勿填 IP 地址,另外, 兩條 WAN 的此欄位 不可以填入相同的網址.

Prot	tocol Binding		
	Service: Source IP: Distination IP: Enable:	SMTP [TCP/25~25] Service Management 192 . 168 . 1 . 0 to 0 0 . 0 . 0 . 0 . 0	
		Delete selected employeien	
		Delete selected application	
	Back	Apply Cancel	your future life

Protocol Binding-協定綁定

它提供使用者可將特定的 IP 或特定的應用服務端口 Service port 經由您限定的 WAN 出去.

Service:	在此選擇欲開啓的綁定服務端口 Service Port 預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!. 預設的 Service 為 SMTP。
Source IP:	使用者可以綁定特定的內部虛擬IP位置的封包經由特定的廣域端口出



	去。在此填上的內部虛擬 IP 位置範圍,例如 192.168.1.100 到 150.則 IP 地址 100到 150 為綁定範圍,如果使用者只需要設定特定的 Service Port 而不需設定特定的 IP 的話,則在 IP 的欄位皆填入 0,另外此 Source IP 是可以控制到 Class B 的範圍。
Destination IP:	在此填上的外部固定 IP 位置,例如若有一目標地址 210.11.1.1 使用 者限定只能從廣域端口 1 到達此目標地址.則在此填上的外部固定 IP 位置 210.11.1.1 to 210.11.1.1 如果使用者要設定一個範圍的目 的地為置,則填入方式可以為 210.11.1.1 to 210.11.255.254,則表示整 組 210.11.x.x 的 Class B 網段都限制走某一條廣域網,若只需要設定特 定的應用而不需設定特定的 IP 的話,則在 IP 的欄位皆填入 0.0.0.0
Enable:	開啓此條服務功能
Add to list:	新增此條管理服務至列表
Delete selected application:	從列表上刪除此條管理服務
Back:	按下此按鈕"Back"即會回到上一頁
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必 須於 Apply 儲存動作之前才會有效

以上服務表列的 Service port,為一些較常使用的項目,若您預開啓的項目沒有在表列中,您可以使用 Services Management:新增管理服務埠號列表功能達成,如以下所述:

Services Name:	在此自訂選擇欲開啓的服務埠號名稱加入列表中,如 Edonky 等
Protocol:	選擇所需管理的 Service port 爲 TCP or UDP 封包.
Port Range:	在此填上欲開啓的服務埠號的位置範圍,如 TCP/500~500 或是 UDP/2300~2310 等.
Add to List:	增加到開啓服務項目內容列表,最多可新增 30 組.
Delete Selected Services:	刪除所選擇的開啓服務項目之一筆內容
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效
Exit:	離開此功能設定畫面





特定使用者的 IP 群體模式 IP Group (By Users)

管理者可藉由設定"特定使用者的 IP 群組",以提供分級服務或指定某些 IP 或 Service Port 只能用那一條 WAN 進出且一經選擇指定後此條 WAN 也只能提供給這幾個 IP 或 Service Port 使用。管理者可將特定的 WAN 限定給"特定使用者的 IP 群組"使用, 群組內的成員, 即不用與其他非"特定使用者的 IP 群組"使用者分享頻寬,而可享 有較優的分級服務。若特定的 IP 使用者僅選定的網域埠口中選擇特定的服務時,則其他的服務會經由其餘的廣 域網路埠口傳送.

廣域端口 WAN 1 預設是保留做為非 IP 群體使用,也就是所有未設定到 WAN2-WAN4 的 IP 或 Service Port 都會 自動經由此端口進出,廣域端口 WAN2~4 則作為特定使用者使用.



Logout

Q
ONO
Home
General Setting
Configure Multi WAN
Password Time
Advanced Setting
DHCP
Tool
Port Management
Firewall
Log

General Setting => Multi WAN

Mode

- O Intelligent Balancer (Auto Mode)
- 💿 IP Group (By Users)
- O IP Balance

Interface Setting

Interface	Mode	Config.
WAN1	Dispatched by system	Edit
WAN2	Dispatched by system	Edit
WAN3	Dispatched by system	Edit
WAN4	Dispatched by system	Edit

A DESCRIPTION OF THE OWNER OWNER OF THE OWNER OWNER OF THE OWNER OWNE	
Annly	Cancel
Apply	Ganger

Mode:	特定使用者的 IP 群體模式 IP Group (By Users) :
	此模式主要是將某一條 WAN 2 到 WAN 4 指定給某些 IP 或 Service Port 單獨使用,當此 WAN 被設定後,只有設定的 IP 或 Service Port 可 以使用此條 WAN,另外,WAN1 是無法做指定的,以避免 WAN2-4 都被 設定後,其餘未被綁定的 IP 或 Service Port 有一條 WAN 可使用.
Interface Setting:	選擇要進一步設定的介面.
Interface:	顯示出廣域網路埠口的數目,預設值爲四個.
Mode:	在預設的情況下,WAN1 是給非指定到 WAN2 到 WAN4 的 IP 及 Service Port 所使用.WAN2~4 可以加以設定,若沒有設定會顯示出由系統自行 分配 Dispatched by system,也就是會跟 WAN1 由 Router 自己做 Load Balance.
Config.	可經由點選 Edit 進行進一步的設定.
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效



Q	Sitemap Logout
ONO	General Setting => Multi WAN
Home	
General Setting Configure Multi WAN QoS Password Time Advanced Setting DHCP	Interface : WAN2 The Max. Bandwidth provided by ISP : Upstream 512 Kbit/Sec Downstream 512 Kbit/Sec Illetwork service detection
Interface:	顯示為第幾個WAN埠口.在預設的情況WAN2~4是可以做為特定使用者的IP 群體模式 IP Group (By Users)
The Max. Bandwidth provided by ISP::	需手動填入此條廣域端口所能支持的上傳(Upstream)及下載 (Downstream)的網路流量.其範圍介於 0~100Mbits 之間
Network Service detection	在全自動型的負載平衡模式 Intelligent Banancer(Auto Mode)已經 有詳細介紹過.使用者可以回到全自動型的負載平衡模式中觀看.
Port Management	IP Group
VPN Log	Service: All Traffic [TCP&UDP/1~65535] Service Management Source IP: 192 .168 .1 to Distination IP: Enable: Add to list
	Delete selected application
	Back Apply Cancel
	your future life



QoS

FVR9416提供使用者在特定的廣域網路埠口上,提供流量速度控制Rate Control或者是服務優先性 Priority等兩種服務質量 QoS 的設定類型,以滿足特定使用者的頻寬需求.使用者在此只能夠在這兩種設定類型選擇其中的一種作頻寬服務質量 QoS.

在 Rate Control 的情况下

FVR9416 可以針對特定的廣域端口(WAN1-WAN4)提供針對特定 IP 或特定 Service port 的上下傳帶寬控制的服務或有保障的寬帶需求,來傳送重要的資訊封包.

Home Home General Setting Configure Multi WAN OoS Password Time Advanced Setting	General Setting => QoS Guality of Service Enable: WAH1 WAH2 WAH3 WAH4 Type: Rate Control Priority
DHCP Tool Port Management Firewall VPN Log	Service: SMTP [TCP/25-25] Service Management IP: 192 168 1 O to Direction: Upstream Mini. Rate: Kbit/sec Mini. Rate: Kbit/sec Max. Rate: Kbit/sec Add to list Delete selected application
	Apply Cancel your future life
Enable:	啓動選擇要執行此 QoS 限制的廣域端口
Туре:	點選流量速度控制 Rate Control
Services:	在此選擇限定的服務端口 Service Port:(如 All(TCP&UDP)0-65535), 如 WWW 爲 80(80~80), FTP 爲 21~21,可參考服務號碼預設列表!. 預 設的 Service 爲 SMTP。



Services Management:	新增或刪除管理服務埠號列表
Direction:	選擇上傳 uplink 或下載 down link 的限制服務
Minimum Rate (Min. Rate):	在此填入保證或最低的頻寬.例如:填入 15,系統自動會保證這項服務 至少有 15 Kbps 的頻寬保證
Maximum Rate (Max. Rate):	在此填入最高的頻寬.例如:填入 700,系統自動會保證這項服務不會 超過 700 Kbps 的頻寬
Enable:	開啓此服務功能
Add to List:	增加到開啓服務項目內容列表,最多可新增 30 組.
Delete Selected Services:	刪除所選擇的開啓服務項目之一筆內容
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

在服務優先性 Priority 的情況下

FVR9416 可以針對特定的廣域端口,保證在提供特定的服務時,可以區分成高,中或低的優先順序,來傳送重要的 資訊封包,其預設值爲中優先性.


Q	Sitemap Logout		
ONO	General Setting => QoS		
Home General Setting Configure Multi WAN OoS Password Time	Quality of Service Enable: WAN1 WAN2 WAN3 WAN4 Type: Rate Control O Priority		
DHCP Tool Port Management Firewall VPN Log	Service Direction Priority Enable SMTP [TCP/25~25] Upstream High Image: Comparison of the service Management Service Management Add to list		
	Delete selected application		
	Annhy Cancal		
	Appy Cancer		
	your future life		
Enable:	啓動選擇要執行此 QoS 的廣域網路埠口		
Туре:	點選 服務優先性 Priority		
Services:	在此選擇欲開啓的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如WWW 為 80(80~80), FTP 為 21~21,可參 考服務號碼預設列表!.		
Services Management:	新增或刪除管理服務埠號列表		
Direction:	選擇上傳 uplink 或下載 down link.		
Priority:	在選擇服務的優先性時,使用者可以選擇高優先性 High(60%) 與低 優先性 Low(10%) 兩種.其餘部份則為中優先性(30%).在列表中高 優先性的全部服務會均分系統 60%的頻寬.低優先性的全部服務會均 分系統 10%的頻寬.其餘中優先性的全部服務則均分 30%的頻寬.		
Add to List:	增加到開啓服務項目內容列表,最多可新增 30 組.		
Enable:	開啓此服務功能		
Delete Selected application:	刪除所選擇的開啓服務項目之一筆內容		
• •			



Cancel

FVR9416 SME Multi-WAN Firewall/VPN Router

按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效

Password

本功能設定多為 FVR9416 的進階管理項目-管理者密碼設定,本機使用密碼出廠值為"admin",您可當設定完成後修改此一存取密碼,但是記得設定完成後 Apply !.

GNO	General Setting => Password	Siter	nap Logout
Home General Setting Dual WAN Password Time Advanced Setting DHCP Tool Port Management Firewall VPN Log	User Name: Old Password: New Password: Confirm New Password:	admin	
	Ар	oly Cancel	your future life

User Name:	預設為 admin		
Old Password:	塡寫原本舊密碼		
New Password:	填寫所更改密碼		
Confirm New Password:	再填寫確認一次更改密碼		
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數		
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效		



Time-系統時間設定

FVR9416使用了正確的時間計算功能,您可以選擇與FVR9416內建的外部時間同步伺服器(NTP Server)或是自己設定正確時間參數,此項參數設置可以讓您在看FVR9416的系統紀錄或是設置網路存取時間功能時,可以正確的了解事件發生正確時間以及關閉存取或是開放存取 Internet 資源的依據條件.

Automatically:設定自動與網路上的 NTP 伺服器同步時間

請於 Time Zone 選項選擇您所在區域的時間參數以及日光節約時間,或是您有專屬使用的時間同步伺服器(NTP Server)的話,您可以輸入此時間同步伺服器的 IP 位置.

GNO Home	General Setting => Time	
General Setting Configure Dual WAN Password Time Advanced Setting	 Set the local time using Network Time Protocol (NTP) automatically Set the local time Manually 	
DHCP Tool Port Management Firewall VPN Log	Time Zone: Greenwich Mean Time: London (GMT+00:00) Daylight Saving: Enabled from 3 (Month) 28 (Day) to 10 (Month) 28 (Day) ITP Server: Image: Comparison of the server	
	Apply Cancel your future life	,

Manually:手動輸入日期時間參數



於此輸入正確小時(Hours), 分鐘(Minutes), 秒(Seconds), 月份(Month), 日(Day) 與年(Year).



按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數. 按下"Cancel"即會清除剛才所變動的修改設定內 容參數,但是必須於 Apply 儲存動作之前才會有效.



Advanced Setting

DMZ Host-(Demilitarized Zone)

當您使用 NAT 模式運作時,有時需要使用如 "網路遊戲" 等任何不支援虛擬 IP 位置的各種應用程式時,可將 FVR9416 的 WAN Port 的合法 IP 位置直接對應內部虛擬 IP 位置使用,設定如下填入下方的設定可用此功能 達成!



於選擇 "DMZ Host" 功能時,若您要取消此功能必須於後面設定虛擬 IP 位置地方填入"0" 的參數,才會停止此 功能使用.

按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數. 按下"Cancel"即會清除剛才所變動的修改設定內 容參數,但是必須於 Apply 儲存動作之前才會有效.

Forwarding

Port forwarding 虛擬主機架設,若是網路中含有伺服器功能(意指對外部的服務主機 WWW,FTP·Mail等) 可將此主機利用防火牆功能,將主機視為一虛擬的位置,可用 FVR9416 的外部合法 IP 位置<Public IP>,經 過 port 的轉換,(如 WWW 為 port 80),直接存取內部伺服器的服務。若於設定畫面中,選項填入WWW伺 服器位置,如 192.168.1.50 且 port 是 80 的話,當 Internet 要存取這個網頁時只要鍵入:



http://211.243.220.43(此為 FVR9416 的外部合法 IP 位址)

此時,就會透過 FVR9416 的 Public IP 位置去轉換到 192.168.1.50 的虛擬主機上的 Port 80 讀取網頁了。

其他的服務設定,如同上一般;只要將所用的 Server 的 UDP Port 號碼,以及虛擬主機的 IP 位置填入即可!.

Q	Sitemap Logout
ONO	Advanced Setting => Forwarding
Home	
General Setting	
Advanced Setting	Port Range Forwarding
DMZ Host Forwarding	Service IP Address Enable
UPnP	All Traffic [TCP&UDP/1~65535] V 192 . 168 . 1 .
Routing One to One NAT	Service Management Add to list
DDNS	
MAC Clone	
Tool	
Port Management	
Firewall	
VPN	Delete selected application

Services:	在此選擇欲開啓的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如WWW 為 80(80~80), FTP 為 21~21,可參 考服務號碼預設列表!.	
IP Address:	在此填上虛擬主機相對應的內部虛擬 IP 位置,如 192.168.1.100	
Enable:	開啓此服務功能	
Services Management:	新增或刪除管理服務埠號列表	
Add to List:	增加到開啓服務項目內容	

以上服務表列,一些為較常使用的項目,若您預開啓的項目沒有在表列中,您可以使用 Services Management: 新增或刪除管理服務埠號列表功能達成,如以下所述:

Port Range Forwarding:開啓埠號位置新增管理功能

Services Name:	在此自訂選擇欲開啓的服務埠號名稱加入列表中,如 Edonky 等
Protocol:	選擇此服務 Port 是 TCP 還是 UDP 封包.
Port Range:	開啓此服務功能在此塡上欲開啓的服務埠號的位置範圍,如 500~500 或是 2300~2310 等.
Add to List:	增加到開啓服務項目內容列表,最多可新增 30 組.



Delete Selected Services:	刪除所選擇的開啓服務項目之一筆內容	
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數	
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效	
Exit:	離開此功能設定畫面	

2	Service Management - Microsoft	Internet Explorer		×
				~
	Service Name	All Traffic [TCP&UDP/1~65535] DNS [UDP/53~53] TTP [TCP/21~21] HTTP [TCP/80~80] HTTP Secondary [TCP/8080~8080] HTTPS [TCP/443~443] HTTPS Secondary [TCP/8443~8443] IFTP [UDP/69~69] MAP [TCP/143~143] NNTP [TCP/119~119] POP3 [TCP/110~110] SNMP [UDP/161~161] SMTP [TCP/25~25] FELNET [TCP/23~23] FELNET Secondary [TCP/8023~8023]		
	Add to list	Delete selected service	 -	
	Арріу			~



Port Triggering

Po Po	ort Triggering			
	Application Hame	Trigger Port Range to to Add to list	Incoming Port Range	
		Delete selected application		
	Show Tables	: Apply Cancel	your fu	ture life

有一些特殊應用軟體其進出 Internet 的埠號(Port Number)為非對稱的,此時您必須使用此功能選項將一些特殊一用程式使用的埠號填入相關設定中,如以上畫面所示:

Application name:	您可以自訂此特殊應用軟體名稱,方便管理使用!	
Trigger Port Range:	輸入由 FVR9416 出 Internet 的使用埠口(Port Number)編號.(如 9000~10000)	
Incoming Port Range:	輸入由 Internet 進入的使用埠口(Port Number)編號. (如 2004~2005)	
Add to List:	增加到開啓服務項目內容列表.	
Delete Selected Application:	刪除所選擇的開啓服務項目之一筆內容	
Show Tables:	按下此按鈕即會顯示 Table 上的所有設定項目內容參數.	
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數	
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效	

以下為一些常用的埠號需設定到此功能項目中的列表:

Application	Outgoing Control	Incoming Data
Battle.net	6112	6112
DialPad	7175	51200, 51201,51210
ICU II	2019	2000-2038, 2050-2051
		2069, 2085,3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000



UPnP

Advanced Setting	dvanced Setting => UPnP	Sitemap Logout
DMZ Host Forwarding UPnP Routing One to One NAT DDNS MAC Clone DHCP Tool Port Management Firewall VPN	Service Nar DNS [UDP/53->53] Image: Comparison of the selected application of the selected applicat	Add to list
Log	Show Tables Apply	Cancel your future life

UPnP (Universal Plug and Play) 是微軟 Microsoft 所制定的一項通訊協定標準,若是您使用的虛擬主機電腦有支援 UpnP 機制的話(如 WindowsXP),而您也必須相同設定您的電腦使用 UpnP 功能開啓,以便與 FVR9416 路由器協調搭配使用.

Services:	在此選擇欲開啓的 UPnP 的服務號碼預設列表,如 WWW 為80(80~80), FTP 為 21~21,可參考服務號碼預設列表!.
IP Address:	在此填上 UPnP 相對應的內部虛擬 IP 位置或名稱,如 192.168.1.100
Enable:	開啓此服務功能
Services Management:	新增或刪除管理服務埠號列表
Add to List:	增加到開啓服務項目內容
Delete Selected Services:	刪除所選擇的開啓服務項目之一筆內容
Show Tables:	顯示目前所開啓設定的 UpnP 列表
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效



Routing-路由通訊協定

Dynamic Routing-動態路由通訊協定

RIP是 Routing Information Protocol 的簡稱,在 IP 環境中有 RIP I / RIP II, 一般而言網路中大多只有一個路由器,所以決大部份我們會只使用 Static Route(靜態路由通訊), RIP 的使用時機是若存在與網路中有數個路由器,此時不想每台路由器都去定義繞徑表(Routing Table), 可自動選擇 RIP 通訊協定, 且自動將所有路徑更新!

RIP 也是一個很非常簡單的路由協定(Routing Protocol),是採用 Distance Vector 的方式,所謂 Distance Vector 是用以 Router 的個數來作爲傳送距離的判斷,而不以實際連線的速率來作判斷,所以在某 些時候所選的路徑是經過最少的 Router,但是並不一定反應速度最快的 Router.

	Advanced Setting => Routing	Sitemap Logout
Home General Setting Advanced Setting	Dynamic Routing	
DMZ Host Forwarding UPnP Routing One to One NAT DDNS MAC Clone	Working Mode: RIP: Receive RIP versions: Transmit RIP versions:	Gateway Router Enabled Oisabled Both RIP v1 and v2 RIPv2 - Broadcast

Working Mode:	選擇路由器運作模式為"Gateway"模式(NAT)或是一般路由(LAN to LAN Routing)模式.
RIP:	選擇按鈕"Enable"選擇使用 RIP 動態路由通訊
Transmit RIP Version:	可於上下選擇按鈕選擇使用動態路由通訊 None, RIPv1, RIPv2, Both RIPv1 and v2 為傳送動態路由通訊協定的 "TX" 功能
Receive RIP Version:	可於上下選擇按鈕選擇使用動態路由通訊 None, RIPv1, RIPv2-Broadcast, RIPv2-Multicast, 為接收動態路由通訊協定的 "RX"功能
Show Routing Table:	可使用圖中的功能按紐 "Show Routing Table "了解最新的路 徑表
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效



Static Routing-靜態路由通訊協定

如果在您的網路中有多個路由器與 IP 節點子網路,就必需設定 FVR9416 的靜態路由功能(Static Routing), 這些功能是讓整個不同的網路節點能自動找尋所需繞徑(Routing)且能讓不同網路節點能相戶存取;可使用圖 中的功能按紐 "Show Routing Table "了解最新的路徑表...

DHCP Tool	Statio	c Routing	
Firewall VPN Log		Destination IP:	
		Add to list	
		Show Routing Table Apply Cancel your future	life

Select Route entry:	可選擇靜態路由表格, FVR9416 共支援了多達 30 組路由表
Delete this entry	刪除一個路由表
Destination IP and Subnet Mask:	可填入欲繞徑的遠端網路 IP 節點與子網路節點位置, 如另一個子網路節點為 192.168.2.0/255.255.255.0
Default Gateway:	此網路節點欲繞徑的預設閘道器位置. 如 192.168.2.1
Hop Count:	此節點的路由器層數,如是在FVR9416下的二個路由器之一,此應填 爲 2,預設爲 1.(最大爲 15)
Interface	此網路節點的連接位置,是位於 WAN 端亦或是 LAN 端.
Delete Selected IP:	刪除一個路徑表
Show Routing Table:	顯示目前最新的路徑表



One-to-One NAT-- 一對一 NAT 對應

當您的寬頻網路為固定制(如 ADSL 固定 8 個 IP 位置)時,因 FVR9416 本身指佔用一個合法 IP 位置,以及 ATU-R 也使用一個合法 IP 位置後,所剩為 4 個合法 IP.欲將此其他的 4 個合法 IP 位置直接對應到 FVR9416 下的 4 個虛擬 IP,可用此功能達成!

使用方法:

當您有使用如 "網路遊戲" 等任何不支援虛擬 IP 位置的各種應用程式時,可將外部的合法 IP 位置直接 對應內部虛擬 IP 位置使用,設定如下填入上方的設定中即可!

範例:如您有5個可用IP位置,分別是210.11.1.1~6,而210.11.1.1已經給FVR9416的WAN 合法IP 使用於一般的NAT上,另外還有其他四個合法IP 可以分別設定到Multi-DMZ 當中,如下所述

210.11.1.4 → 192.168.1.3 210.11.1.5 → 192.168.1.4 210.11.1.6 → 192.168.1.5 210.11.1.7 → 192.168.1.6

Note: FVR9416 廣域網路 IP 位置(WAN IP -NAT Public) 無法納入此項目的範圍設定中.



Home General Setting Advanced Setting	Advanced Setting => One to One NAT
DMZ Host Forwarding UPnP Routing One to One NAT DDNS MAC Clone DHCP Tool Port Management Firewall VPN Log	Add Range Private Range Begin Public Range Begin Range Length 192.158.1. Add to list Delete selected range
	Apply Cancel your future life
One-to-One NAT:	啓動或關閉一對一 NAT 功能"Enable"開啓 Disable 關閉 (選擇 是否開啓此功能)
Private Range Begin:	虛擬 IP 位置起始 IP 位置
Public Range Begin:	外部合法 IP 位置起始 IP
Range Length:	外部合法 IP 位置終止 IP 的數量
Add to List:	加入此設定到一對一 NAT 列表中
Delete selected range:	刪除所選擇的一項一對一 NAT 列表
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Undo"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效

Note: 一對一的 NAT 模式(One-to-One NAT)將會改變防火牆運作的方式,您若設定了此功能, LAN 端所設定的 機器或 PC 將會曝露到 Internet 上,除非到防火牆的 Access Rule 中加入拒絕存取規則項目條件,才可以阻斷由 Internet 進到 LAN 端設定一對一 NAT 的機器或 PC.您可以按下新增一個一對一 NAT 位置項目(Add to List) 按 鈕或是選擇刪除一個一對一 NAT 位置(Delete selected range).



DDNS-動態網域名稱

"DDNS"目前支援 Dyndns.org 與 3322.org 的動態網址轉換功能,其目的是為了讓使用動態 IP 位置架站 或是遠端監控還有動態 IP 下需做 VPN 的連線為目的,如 ADSL PPPoE 計時制或是 Cable Modem 的使用者 的合法 IP 位置都會隨時間而改變,當此使用者欲架設網站之類的服務,但是因 IP 會隨時變動,所以本設備提供 了動態網址轉換功能,此服務可向 www.dyndns.org 或是 www.3322.org 提出申請,是完全免費的!!

0			Sitemap	~
ONO	Advanced Settin	g => DDNS	Log	gout
Home				
General Setting				
Advanced Setting	Interface	Status	Host Name	Config.
Advanced octaing	WAN1	Disabled		Edit
DMZ HOST	WAN2	Disabled	222	Edit
Forwarding	WAN3	Disabled		Edit
UPNP	WAN4	Disabled		Edit
Port Management Firewall VPN Log				

請在設定欄(Config.)的編輯(Edit) 按下該超連結直接進入該設定項目中.



KoreHomeGeneral SettingDMZ HostForwardingUPnPRoutingOne to One NATDDNSMAC CloneDHCPToolPort ManagementFirewallVPNLog	<image/>
Interface:	使用者所選取的廣域端口
DDNS Service:	DDNS 動態網址轉換功能可以選擇 Disable 關閉, DDNS.org 與 3322.org 等三項.
Username:	使用者名稱:向 DDNS 所設定的名稱
Password:	使用者密碼:向 DDNS 所設定的密碼
Host Name:	動態網址名稱:向 DDNS 所註冊的網址,如 abc.dyndns.org or xyz.3322.org 等.
Internet IP Address	目前向 ISP 所取得的之動態合法 IP 位置
Status:	目前 DDNS 的狀態:顯示目前的 DDNS 所更新 IP 功能狀態
Back:	按下此按鈕"Back"即會回到前一個畫面.
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Undo"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效



MAC Clone-變換實體 MAC 位置

此多為使用於雙向 Cable Modem 的用戶,若有發生類似鎖網卡的情況下,可使用此功能將原有網路卡實體層位置(MAC Address: 00-xx-xx-xx-xx)填入此項目中以解除鎖定問題!



請在設定欄(Config.)的編輯(Edit)按下該超連結直接進入該設定項目中.



	Sitema	ap Logout
Home	Advanced Setting => MAC Clone	
General Setting		
Advanced Setting	Interface : WAN1	
Forwarding UPnP	User Defined WAN MAC Address:	_ 0b _ 66
Routing One to One NAT DDNS MAC Clone	MAC Address from this PC: O 00-0e-a6-6b-70-d9	
DHCP Tool		
Firewall		
Log		
	васк Арріу Сапсеі	
		your future life

Interface:	使用者所選取的廣域端口
User Defined WAN1 MAC Address:	目前設備出廠預設的 MAC 位置.
MAC Address From this PC:	目前連接此 PC 的 MAC 位置.
Back:	按下此按鈕"Back"即會回到前一個畫面.
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Undo"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效



DHCP-DHCP 發放 IP 伺服器

Setup-設定

因 FVR9416 本身就含有 DHCP 伺服器,所以可以提供區域網路內的電腦自動取得 IP 的功能,(如同 NT 伺服 器中的 DHCP 服務,好處是每台 PC 不用去記錄與設定其 IP 位置,當電腦開機後,就可從 FVR9416 自動取 得,管理方便。.

 Enable DHCP Server:
 可選擇開啓 DHCP 伺服器自動派發 IP 位置功能;若為 Enable 選項,

 則所有 PC 都可使用自動取得 IP 位置,反之則無;每台 PC 必需去

 指定固定虛擬 IP 位置

	DHCP => Setup
Home General Setting Advanced Setting DHCP	✓ Enable DHCP Server
Setup Status Tool Port Management Firewall VPN Log	Dynamic IP Client Lease Time 1440 Minutes Dynamic IP Range Range Start : 192.168.1.100 Range End : 192.168.1.149
<i>Dynamic IP-</i> 動態 IP Client Lease Time:	此設定為發給 PC 端 IP 位置的租約時間,預設為 1440 分鐘(代表時間各一天) 您可以依昭實際需求來設定 以分鐘負單位
Range Start:	此 IP 位置是 DHCP Server 自動派送 IP 的啓使 IP,意指是從多少 IP 位址開始派送。系統預設為從 192.168.1.100 的 IP 位置開始發放.
Range End:	意指是從多少 IP 位址截止派送。系統預設為從 149 的 IP 位置開始 停止發放 IP,原廠設定値可供 50 台電腦自動取得 IP 位址,您可以是 實際情況增減使用!



Static IP- IP 位置綁定功能(IP by MAC)

Static IP address	輸入 PC 端固定虛擬 IP 位置			
MAC:	輸入 PC 端網路卡固定實體 MAC 位置			
Add to List:	加入此設定到 Static IP 列表中			
Delete selected Entry:	刪除所選擇的 Static IP 列表			
Add New	新增新的固定虛擬 IP 位置			
	Static IP			
	Static Entry Static IP Address: . MAC Address: . Add to list			
	DNS Server (Required) 1: 0 . 0 . 0 . 0 2: 0 . 0 . 0 . 0			
	WINS WINS Server : 0 . 0 . 0 . 0			
	Apply Cancel your future life			

DNS Server

此設定爲發給 PC 端 IP 位置的 DNS 網域伺服器查詢位置,您可以直接輸入此伺服器的 IP 位置.

DNS Server (Required)1 輸入 DNS 網域伺服器的 IP 位置.預設值為 0.

2 輸入 DNS 網域伺服器的 IP 位置.預設值為 0.

WINS

```
      若您的網路上有解析如 Windows 的電腦名稱伺服器的話,您可以直接輸入此伺服器的 IP 位置

      WIN Server
      輸入 WIN 網域伺服器的 IP 位置.預設值為 0.
```



 Apply:
 按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.

 Cancel:
 按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是

 必須於 Apply 儲存動作之前才會有效

Status-狀態顯示

Q					Sitemap Logou	t	
ONO	DHCP => Status						
Home							
Advanced Setting	Status						
DHCP		DHCP Server :	192.168.1.1				
Status	0	ynamic IP Used : Static IP Used :	0				
Tool		DHCP Available :	50				
Port Management		Total :	50				
VPN Log	Client Table						
	Client Host Name	IP Address	M	AC Address	Leased Time	Delete	
				Refresh			
				No. of Concession, Name	yourf	uture life	כ

此狀態表爲顯示 DHCP 伺服器的目前使用狀態與設定紀錄等,以便提供管理人員需要時做網路設定參考數據.以下針對其內 容做介紹:.

DHCP Server:	目前 DHCP 伺服器的 IP 位置
Dynamic IP Used:	目前 DHCP 伺服器已經發放動態 IP 的數量
Static IP Used:	目前 DHCP 伺服器已經發放固定 IP 的數量
DHCP Available:	目前 DHCP 伺服器可以發放的 IP 數量
Total:	目前 DHCP 伺服器所設定可發放的 IP 總數量
Client Host Name:	目前此台電腦的電腦名稱



IP Address:	目前此台電腦所取得的 IP 位置
MAC Address:	目前此台電腦的 MAC 網路實體位置
Leased Time:	DHCP 目前核發 IP 位置的租約時間
Delete:	刪除此筆核發 IP 紀錄

Tool-工具程式

SNMP-網路通訊

SNMP 為 Simple Network Management Protocol 的縮寫,意指網路管理通訊協定,此為網路上重要的管理項目 依據之一,透過此 SNMP 通訊協定,可以讓已經具備有網路管理的程式(如 SNMP Tools-HP Open View)等網管 程式做即時管理之通訊使用, FVR9416 支援標準 SNMP v1/v2c,可以搭配標準 SNMP 網路管理軟體來得知目 前所有網路上的機器運作情況,以便隨時掌握網路資訊.

	Tool => SNMP			Sitemap	Logout
Home General Setting Advanced Setting DHCP Tool SNMP Diagnostic Restart Factory Default Firmware Upgrade Setting Backup Port Management Firewall VPN		SIIMF System Name: System Contact: System Location: Get Community Name: Set Community Name: Trap Community Name: Send SNMP Trap to:	P: Enable Image: Constraint of the second		
		Арріу	Cancel		your future life



Enable SNMP:	將 SNMP 功能開啓,系統預設爲開啓此功能.
System Name:	設定機器的名稱,如 FVR9416
System Contact:	設定機器的管理聯繫人員名稱,如 John
System Location:	設定機器的目前所在位置,如 Taipei
Get Community Name:	設定一組管理者參數可以取得此機器的項目資訊,系統預設"Public"
Set Community Name:	設定一組管理者參數可以設定此機器的項目資訊,系統預設"Private"
Trap Community Name:	設定一組管理者參數可以傳送 Trap 的資訊
Send SNMP Trap to:	設定一組 IP 位置或是 Domain Name 名稱的接收 Trap 訊號主機
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Delete:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效



Diagnostic-線上連線除錯測試

FVR9416 提供簡易的線上測試機制方便於除錯時使用,此除錯機制包含 DNS Lookup 以及 Ping 二種.

Tool =	> Diagnostic	Sitemap	Logout
General Setting Advanced Setting DHCP	OHS Name Lookup	O Ping	
Tool SNMP Diagnostic Restart Factory Default Firmware Upgrade Setting Backup Port Management Firewall VPN Log	Look up the name:		
			your future life

DNS Name Lookup-網域名稱查詢測試

請於此測試畫面輸入您想查詢的網域主機位置名稱,如<u>www.abc.com</u> 然後按下 Go 的按鈕開始測試,測試結果 會顯示於此畫面上.



Ping-封包傳送/接收測試

	Tool => Diagnostic	Sitemap	Logout
General Setting Advanced Setting DHCP	🔘 DNS Name Lookup 💿 Ping		
1001 SINMP Diagnostic Restart Factory Default Firmware Upgrade Setting Backup Port Management	Ping host or IP address:		
Firewall VPN Log			
			your future life

此項目爲主要提供管理者了解對外連線的實際狀況,可以藉由此功能了解網路上的電腦是否存在!

請於此測試畫面輸入您想測試的主機位置 IP,如 192.168.5.20 按下 Go 的按鈕開始測試,測試結果會顯示於此 畫面上.



Restart-重新啓動

	Tool => Restart		Sitemap Logout
Home General Setting Advanced Setting DHCP Tool		Restart Router	
SNMP Diagnostic Restart Factory Default Firmware Upgrade Setting Backup Port Management			
Firewall VPN Log			
			your future life

透過此"Restart"按鈕來重新啓動 FVR9416,重新啓動後也會將此訊息傳送到系統日誌中.選擇後,請按下 Restart Router 按鈕即可重新開機啓動.



Factory Default-回復原出廠預設值

	Tool => Factory Default		Sitemap	Logout
Home General Setting Advanced Setting DHCP		Return to Factory Default Setting		
Tool SNMP Diagnostic Restart Factory Default Firmware Upgrade Setting Backup				
Port Management Firewall VPN Log				
				your future life

若是選擇"Return Factory Default Setting", FVR9416 會將所有的 FVR9416 上面的設定清除,並重新開機; 切記,使用此功能會將機器所有的資料清除!



Firmware Upgrade-系統韌體升級

	Tool => Firmware Upgrade
General Setting Advanced Setting DHCP Tool SNMP Diagnostic Restart Factory Default Firmware Upgrade Setting Backup Port Management Firewall VPN Log	Warning: 1. When choosing previous firmware versions, all settings will restore back to default value. 2. Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button. 3. Please don't close the window or disconnect the link, during the upgrade process.
	your future life

Firmware Upgrade

此設定可以於FVR9416的Web設定畫面中直接升級韌體的功能,並請您於升級前先確認韌體版本資訊,選擇瀏 覽至韌體-Firmware存放資料夾選擇該檔案後,按下 Firmware Upgrade Right Now 做升級.

切記:當升級動作開始進行中時,請勿跳離此畫面,否則升級會失敗.



Setting Backup-系統設定參數儲存

	Tool => Setting Backup	Sitema	Logout
Home General Setting Advanced Setting DHCP Tool SNMP Diagnostic Restart	Import configuration File	[瀏覽] Import	
Pactory Default Firmware Upgrade Setting Backup Port Management Firewall VPN Log	Export configuration File	Export	
			your future life

Import Configuration File:

此功能為將之前客戶的所有設定參數值備份的內容回存到機器中!並請您於升級前先確認韌體版本資訊,選擇 瀏覽至備份參數檔案-"config.exp"存放資料夾選擇該檔案後,按下 Import 按鈕做設定檔案匯入.

Export Configuration File:

此功能爲儲存客戶的所有設定參數值備份, 按下 **Export** 按鈕,選擇存放資料夾位置然後按下儲存鍵將 "config.exp"存入即可.



Port Management-網路實體埠口管理

於 FVR9416 中,使用管理者可以設定廣域端口數與每一個乙太網路埠口連接速率(Speed),工作模式(Half & Full), 高低優先權(Priority)或是自動偵測(Auto-negotiation)等乙太網路埠口的功能.

Port Setup-網路埠口設定

eneral Setting							
vanced Setting		Plea	se choose	how many WA	W ports you prefer to us	e : 4 👽 (Default valu	e is 4)
DHCP							
Diloi	Port ID	Interface	Disable	Priority	Speed	Duplex	Auto Negotiation
1001	1	LAN		Normal 💌	0 10M 💿 100M	O Half 💿 Full	Enable
rt Management	2	LAN		Normal 🚩	○ 10M	🔾 Half 💿 Full	Enable
Port Setup	3	LAN		Normal 🚩	O 10M 💿 100M	🔘 Half 💿 Full	Enable
Port Status	4	LAN		Normal 🚩	O 10M 💿 100M	🔘 Half 💿 Full	Enable
Firewall	5	LAN		Normal 🚩	🔾 10M 💿 100M	🔾 Half 💿 Full	🗹 Enable
VPN	6	LAN		Normal 🚩	🔾 10M 💿 100M	🔾 Half 💿 Full	🗹 Enable
Log	7	LAN		Normal 💌	🔘 10М 💿 100М	🔿 Half 💿 Full	🗹 Enable
	8	LAN		Normal 💌	🔿 10M 💿 100M	🔿 Half 💿 Full	🗹 Enable
	9	LAN		Normal 😽	🔾 10M 💿 100M	🔿 Half 💿 Full	🗹 Enable
	10	LAN		Normal 💌	🔘 10М 💿 100М	🔘 Half 💿 Full	📃 Enable
	11	LAN		Normal 💟	🔾 10М 💿 100М	🔘 Half 💿 Full	🗹 Enable
	12	WAN4		Normal 💌	🔿 10M 💿 100M	🔿 Half 💿 Full	🗹 Enable
	13	WAN3		Normal 😽	🔿 10M 💿 100M	🔿 Half 💿 Full	🗹 Enable
	14	WAN2		Normal 💌	🔿 10M 💿 100M	🔿 Half 💿 Full	🗹 Enable
	15	WAN1		Normal 💌	O 10M 💿 100M	🔿 Half 💿 Full	🗹 Enable
	DMZ	DMZ		Normal 🗸	0 10M 0 100M	O Half . D Full	Enable

Basic Per Port Config乙太	網路埠口設定
Port ID:	顯示每個端口的順序.
Interface:	共有 LAN1~LAN 11, WAN1~WAN4, and DMZ 等埠口 .這些端口會根據 使用者所設定的廣域端口數而自動調整.
Port Disable:	此爲設定乙太網路的埠口開啓或是關閉的功能,若是打勾的話,則此乙 太網路埠口立即被關閉無法連接使用.預設爲開啓無打勾
Priority:	此爲設定此乙太網路的埠口封包傳送高低優先權設定,若是此 Port 設

第65頁,共111頁



	定為 High 的話,則最優先使用傳送封包的權利,預設值為-Normal 優先順序為一般
Speed:	此爲設定此乙太網路的埠口網路實體連接速率選項,您可以設定爲 10Mbps 或是 100Mbps 連接速度.
Duplex:	此爲設定此乙太網路的埠口網路實體連接速率工作模式選項,您可以 設定爲 Half — 半雙工模式或是 Full-全雙工模式運作.
Auto-negotiation:	此爲設定此乙太網路的埠口網路實體連接速率自動偵測模式,若是勾 選的話,自動偵測所有連接埠口的信號與調整.

按下 Apply 按鈕可以儲存設定或是按下 Cancel 按鈕可以取消設定更改.

Port Status-網路埠口狀態即時顯示

管理者可以於此項目中,選擇所需要監看的乙太網路埠口各項即時參數顯示,如下圖:

	Port Management => P	Sitemap Logout
Home General Setting Advanced Setting DHCP	Port ID : 1 💌	
1001	Туре	10Base-T / 100Base-TX
Port Management	Interface	LAN
Port Setup Port Status	Link Status	Down
Firewall	Port Activity	Port Enabled
VPN	Priority	Normal
	Speed Status	10 Mbps
Log	Duplex Status	Half
	Auto negotiation	Enabled
	Port Receive Packet Count Port Receive Packet Byte Count	164453 36108106
	Port Transmit Packet Count	237216
	Port Transmit Packet Byte Count	249909016
		Refresh your future life

於網路埠口狀態-Port Status 整體資訊(Summary) 表格項目中,此部份會顯示目前埠口硬體設定項目如網路連接型態(Type),線路連線狀態(Link Status),埠口使用狀態(Port Activity 開-on 或關-off),埠口優先權設定



(Priority- (高-High 或一般-Normal), 網路連接速率(Speed Status-10Mbps 或 100Mbps), 雙工模式(Duplex Status-半雙工 half 或全雙工-full),自動偵測模式(Auto negotiation).

於網路埠口即時顯示(statistics) 資訊表格項目中,將會顯示目前此端口的封包數據,包含傳送/接收封包計 算(receive/transmit packet count)/以及封包傳送/接收 Byte 數計算(packet byte count)與 錯誤封包統計 (Port Packet Error Count) 等.您可以按下 Refresh 按鈕重新整理所有的即時資訊顯示.

Firewall-防火牆設定

General-一般

FVR9416 預設防火牆功能為啓動狀態. 如果管理者關閉此防火牆選項功能的話(Firewall Disable), SPI, DoS, Block WAN Request 等功能將會自動關閉(disabled), 遠端管理功能(Remote Management) 將會開啓 (enabled),而網路存取規則(Access Rules) 與內容服務過濾器(Content Filter)也會關閉(disabled).





Firewall:	開啓或關閉防火牆功能
SPI:	此為封包主動偵測檢驗技術(Stateful Packet Inspection),防火牆主要 運作在網路的層級,但是藉由執行對每個連結的動態檢驗,也擁有應 用程式的警示功能,讓封包檢驗型防火牆可以拒絕非標準的通訊協定 所使用的連結.
DoS:	此爲保護 DoS 攻擊,如 SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing 等.
Block WAN Request:	若是選擇 Enable 的話,則 FVR9416 會關閉對外的 ICMP 與不正常 連線的封包回應,預設值爲開啓.(若您是使用 Cable 連線的話,此選項 請開啓),當 Enable 此功能時,遠端將無法 ping 到此台路由器,當 Disable 此功能時,遠端 ping 此台路由器廣域端口 IP 地址時會得到 回應.
Remote Management:	遠端管理功能,若您要透過遠端 Internet 直接連線進入路由器的設定 畫面,必需將此功能開啓,並於遠端使用 IE 於網址填入 FVR9416 的廣 域端口 IP 位置(WAN Port IP),並加上預設可修改的控制埠口(預設為 80,可更改爲其他端口),如
	http://210.11.11.1:8080 or http://210.11.11.1:8081
Multicast Pass Through:	網路上有許多影音串流媒體,使用廣播方式可以讓您的 Client 端接收 此類封包訊息格式.
MTU:	MTU 為 Maximum Transmission Unit 的縮寫, 一般預設的 default 為 1,500. 但是在不同的網路環境中, 應該是有不同的數值. 尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU Size:1492); 不過 許多的 Server 與 ADSL PPPoE 用戶的 MTU Size 有所相關,一般預 設 Auto 即可,不需做任何調整

Access Rules-網路存取規則

管理者可以設定 FVR9416 路由器關閉(deny)或是允許(allow)任何的封包進出 Internet . 您可以選擇設定不同的網路存取限制或開放,從內部到外部(Inside-LAN to Outside-WAN),從外部到內部(Outside-WAN to Inside-LAN)或是設定以 IP 位置及通訊埠口號碼(Port Number)不同的封包過濾於 Internet 存取規則條件.

網路存取規則依照 IP address(IP 位置), Destination IP address(目地端 IP 位置),與 IP protocol type(IP 通 訊協定型態)來管理所有的網路封包流量是否可以通過 FVR9416 防火牆的存取.

FVR9416 擁有簡而易懂的網路存取規則條例工具. 管理者可自訂的網路存取規則條例, 可以選擇關閉或是開啓並保護所有對網際網路 Internet 的存取.以下就針對 FVR9416 的網路存取規則條例做一說明:

以下為 FVR9416 預設的網路存取規則條例:

* All traffic from the LAN to the WAN is allowed-從 LAN 端到 WAN 端的封包預設為可以通過



- * All traffic from the WAN to the LAN is denied.- 從 WAN 端到 LAN 端的封包預設為關閉
- * All traffic from the LAN to the DMZ is allowed.- 從 LAN 端到 DMZ 端的封包預設為可以通過
- * All traffic from the DMZ to the LAN is denied-從 DMZ 端到 LAN 端的封包預設為關閉.
- * All traffic from the WAN to the DMZ is allowed-從 WAN 端到 DMZ 端的封包預設爲開啓.
- * All traffic from the DMZ to the WAN is allowed-從 DMZ 端到 WAN 端的封包預設為開啓.

使用者可以自定存取規則並且超越 FVR9416 的預設存取條件規則, 但是以下的四種額外服務項目為永遠開 啓,不受其他自訂規則所影響:

- * HTTP 的服務從 LAN 端到 FVR9416 預設為開啓的.(為了管理 FVR9416 使用)
- * DHCP 的服務從 LAN 端到 FVR9416 預設為開啓的. (為了從 FVR9416 自動取得 IP 位置使用)
- * DNS 的服務從 LAN 端到 FVR9416 預設為開啓的. (為了解析 DNS 服務使用)
- * Ping 的服務從 LAN 端到 FVR9416 預設為開啓的.(為了連通測試 FVR9416 使用)

C NO Home	Firew	/all =	> Ac	cess Rul	e			Sitemap	Logout	
General Setting Advanced Setting				Ju	mpto 1 🔽	/1 page	5 💌 er	ntries per page		
DHCP	Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
Tool		1	Allow	All Traffic [0]	LAN	Any	Any	Always		
Port Management		4	Deny	All Traffic [0]	WAN1	Any	Any	Always		
Firewall		1	Deny	All Traffic [0]	WAN2	Any	Any	Always		
Acess Rule Content Filter VPN Log					Add New I	Rule	Restore to Default	t Rules		
									your fut	ure life

除了預設規則以外,所有的網路存取規則都會顯示於此規則列表中,您可以依照或是自己選擇高低優先權 (Priority) 於每一個網路存取規則項目中.按下 Edit 按鈕可以設定網路存取規則項目,以及按下 Trash Can icon 可以刪除網路存取規則項目.



按下 Add New Rule 新增新的網路存取規則按鈕可以新增一項新的存取規則,或是按下 Restore to Default Rules 可以回覆原有預設存取規則項目,以及刪除所有的自訂規則內容回到出廠預設存取規則..

Add a new Rule-增加新的管制規則

	Firewall => Access Rule	Logout
Home General Setting Advanced Setting DHCP Tool Port Management Firewall General Acess Rule	Services Action : Allow Service : All Traffic [TCP&UDP/1~65535] Service Management Source Interface : LAN Source IP : Single Destination IP : Single	
Log	Apply this rule always V : to : (24-Hour Fo	rmat) Sat
	Back Apply Cancel	your future life

Services-服務管制內容

Action:	此為設定 FVR9416 的管制條例動作: Allow:允許此管制條例通過 Deny:關閉此管制條例
Service:	選擇服務項目內容,可以上下做選單的選擇.
Service Management:	若是您想要管制的服務內容沒有存在於預設列表內的話,您可以按下 右方的 Service Management服務管理新增一個服務內容,輸入 一個服務名稱-Service Name以及通訊協定與埠口-Protocol & Port,以及按下 Add-新增按鈕即可新增一個管制服務項目內容.
Log:	使用者可以選擇是否要將此管制條例存入 Log.若是符合此件的話,將此 Log 存入或是不需要 Log 的資訊



Source Interface:	選擇來源的封包位置介面(如 LAN, WAN1~WAN4, Any)項目內容,可以上下做選單的選擇.
Source IP:	選擇來源封包的 IP 位置(如 Any, Single or Range),若是選擇 Single 或是 Range 的話,請輸入此單一或是一區段範圍的 IP 位置.
Destination IP:	選擇目的端封包的 IP 位置(如 Any, Single or Range),若是選擇 Single 或是 Range 的話,請輸入此單一或是一區段範圍的 IP 位置.
Scheduling:	是否需要將此管制條例安排於特定的管制時間設定
Apply this rule (time parameter):	可選擇 Always(預設)-都關閉或開啓,或是選擇 From 每週那一天及從 幾點到幾點做管制

Services Management:管制服務內容項目管理

🕙 Service Management - Microso	ft Internet Explorer	
		~
Service Name Protocol TCP Port Range to	All Traffic [TCP&UDP/1~65535] DNS [UDP/53~53] FTP [TCP/21~21] HTTP [TCP/80~80] HTTP Secondary [TCP/8080~8080] HTTPS [TCP/443~443] HTTPS Secondary [TCP/8443~8443] TFTP [UDP/69~69] IMAP [TCP/143~143] NNTP [TCP/143~143] NNTP [TCP/119~119] POP3 [TCP/110~110] SNMP [UDP/161~161] SMTP [TCP/25~25] TELNET [TCP/23~23] TELNET Secondary [TCP/8023~8023]	
Add to list	Delete selected service	
Apply	Cancel Exit	
		~

Services Name:	新增服務項目內容,可自訂名稱.
Protocol:	新增服務項目通訊協定為 TCP 或是 UDP 封包格式.
Port Range:	設定開啓此服務的埠口位置範圍,如 Port 從 9000~9002.



Add to List:	增加此新增的服務項目內容到服務表列內
Delete Selected Services:	選擇刪除服務項目內容從服務表列內
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Delete:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效
Exit:	跳出此服務表管理畫面

Content Filter-網頁內容管制

Home General Setting	Firewall => Content Filter
Advanced Setting DHCP	Block Forbidden Domains Forbidden Domains
Port Management	Forbidden Domains Add: Add to list
Acess Rule Content Filter VPN Log	Delete selected domain
Block Forbidden Domains:	選擇打勾開啓網頁內容管制功能,預設為關閉
Forbidden Domains:	網頁管制內容項目.
Add:	填寫欲管制的網頁內容,如 www.playboy.com
Add to List:	按下 Add 按鈕新增此一欲管制的網頁內容.
Delete Selected Domain:	可以使用滑鼠點選一個或多個管制的網頁內容,然後按下即可刪除


Scheduling
Apply the rule always 🗹 : to : (24-Hour Format)
🗌 Everyday 💭 Sun 🗌 Mon 💭 Tue 💭 Wed 💭 Thu 💭 Fri 💭 Sat
Apply Cancel
your future life

Scheduling-管制內容排程時間

此日期與時間項目功能爲管制該條例所生效的實際時間才進行管制,如管制時間爲週一到週五,早上八點到下午 六點,您可以依照以下說明適當的管制您所需要的時間參數設定.

Apply this rule:

Apply the rule from 💉 00	: 00 to : (24-Hour Format) Sun Mon Tue Wed Thu Fri Sat
Apply this rule):	選擇打勾開啓網頁內容管制功能,預設爲關閉
Time parameter:	Always: 此管制規則持續開啓
	From:從何時到何時
	to: 此管制規則有時間限制內容,設定為 24 小時制,如 08:00 to 18:00 (早上 8 點到下午 6 點).
Day:	勾選 Every Day 每一天,或是依照實際的需要時間做管制



VPN-虛擬私有網路

	VPN -> Sur					Sitemap	Logout	
Home General Setting Advanced Setting	VI II => 3u	o International June	Tunnel(s) I	Jsed 200	Tunnel(s) Availabl	e Detail		
Tool Port Management Firewall	Tunnel Star	tus	Jump to 1	Add New 1	Tunnel	ntries per page		
Summary Gateway to Gateway Client to Gateway PPTP	No. Name	Status	S Enabled	2 Local Grp Group 0	Remote Group Tunnel(s) [Remote Gateway	Tunnel Test	Config.
Log	GroupVPN	Status						
	Group Name	Tunnels	Enc/Auth/Grp	Local Group	Remote Client	Client Status	Test	Config.
							your fi	uture life

Summary-目前所有的 VPN 狀態顯示

此 VPN 狀態可以顯示目前有關 VPN 方面的即時狀態包含通道-Tunnel,設定參數以及 GroupVPN-VPN 群組狀 態等資訊.

Summary:

0 Tunnel(s) Used 200 Tunnel(s) Available Detail

此為顯示目前有多少 VPN 通道已經設定使用,還剩下多少通道可以提供設定, FVR9416 可同時支援共 200 組 VPN 通道(tunnels).

Detail: 按下此 Detail 按鈕可以顯示如以下畫面的目前所有 VPN 組態,讓管理者清楚的管理所有 VPN 連接資訊.



WAN1 IP:	192.168.5.140	WAN2 IP: 0.0.0).0 WAN3 IP: ().0.0.0 WAN4 I	P: 0.0.0.0		Wed Sep	1 06:01:03 2004
No.	Name	Status	Pha Enc/A	se 2 uth/Grp	Local Group	Remot Group	e R G	emote ateway
				Close				
Tunnel	Status: VPN	通道目前狀態	顯示					
	- I Chatan							
- 10	nnei Status		_					
				Add New Tunn				
		Jur	mp to 1 🚩 /1	page	3 🔽 e	ntries per page		
No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
				· ·	•	· ·		

Add New Tunnel: 新增一條新的 VPN 通道設定

FVR9416 可以支援包含 Gateway to Gateway Tunnel 或是 Client to Gateway Tunnel

Gateway to Gateway:

以下的 VPN 網路連接為運作於 Gateway to Gateway 模式環境,VPN 通道連接為 2 台 VPN 路由器分別透過網 際網路 Internet 所組成,當您按下新增"Add Now"的話,將會直接導引到 Gateway to Gateway 的設定頁面上.



Client to Gateway:

以下的 VPN 網路連接為運作於 Client to Gateway 模式環境, VPN 通道連接為一台 PC 以及一台 VPN 路由器分 別透過網際網路 Internet 所組成,當您按下新增"Add Now" 的話,將會直接導引到 Client to Gateway 的設 定頁面上.





以下就針對"Tunnel Status" VPN 通道目前狀態顯示做完整解說:

Page: Previous page, Next page, Jump to page / 200 pages and entries per page	您可以按下上一頁(Previous page)與下一頁(Next page)按鈕跳到您 想監看的 VPN 通道畫面上,或者您可以直接選擇每一次所顯示的頁次, 來監看您的所有 VPN 通道狀態,如(3, 5, 10, 20, All).
Tunnel No	當您設定 FVR9416 內建之 VPN 功能時,請選擇您要設定的 Tunnel 通 道編號,最多可支援 200 條 VPN 通道設定(Gateway To Gateway 或 Client To Gateway
Status:	於此狀態顯示已經連線成功-Connected,電腦連線名稱-Hostname Resolution Failed, Resolving Hostname 以及等待連線-Waiting for Connection 等資訊,若是管理者選擇手動-Manual 設定 IPSec 通道,則 此狀態會顯示手動-Manual 設定與沒有測試此項手動設定功能狀態模 式
Name:	目前連線 VPN 通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設爲不同,以免混淆
	Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時, 有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道 才會順利連線開啓!.
Phase2 Encrypt/Auth/Group:	於此顯示加密(DES/3DES)以及驗證(MD5/SHA1)以及群組 Group (1/2/5)等設定模式. 若是您選擇手動(Manual)設定 IPSec 的話,於此將不會顯示 Phase 2 DH 群組
Local Group:	此爲顯示本地區域端的 VPN 連線安全群組設定
Remote Group:	此爲顯示遠端的 VPN 連線安全群組設定
Remote Gateway:	此為設定為欲與遠端 VPN 設備連線的 IP 位置,請設定為遠端的 VPN 路由器之對外合法 IP 位置或是 Domain Name 等
Tunnel Test:	可以按下連接按鈕-Connect 去驗證此通道的狀態,測試結果將會更新 於此狀態上.
Configure:	設定項目包含編輯-Edit 以及刪除圖示
	若您按下編輯按鈕- Edit,將會連接到此設定的項目當中,您可以修改



	其中的設定.若您選擇按下垃圾桶圖示的話 🛄,所有此通道的設定將 會被刪除.
Tunnel(s) Enable and	於此顯示此通道是否開啓 (Tunnel(s) Enable)以及此通道是否已經設
Tunnel(s) Defined:	定過(Tunnel(s) Defined).

Group VPN Status: 群組 VPN 狀態顯示

若您無選擇並設定群組 VPN 模式(GroupVPNs), 此將不顯示出會群組 VPN(GroupVPNs)狀態.

GroupVPN Status

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.
Group ID Name):	目前設定連線	GroupVPNs	通道連接名稱.			
Connected Tur	nels:	於此顯示已經	連線的 VPNG	roups 通道.			
Phase2 Encrypt/Auth/0	Broup:	於此顯示加密(DES/3DES)以及驗證(MD5/SHA1)以及群組 Group (1/2/5)等設定模式. 若是您選擇手動(Manual)設定 IPSec 的話,於此將不會顯示 Phase 2 DH 群組					
Local Group:		此爲顯示本地	區域端的群組	VPN 連線安全郡	羊組設定		
Remote Client:		此爲顯示此 Group VPN.遠端的 VPN 連線安全群組設定					
Remote Clients	s Status:	若您按下更多 包1 時	·資訊列表(<u>Det</u> 含群組名稱(Gro 間資訊等.	<mark>ail List)</mark>	比將會顯示更差 位置(IP Addres	多有關資訊, ss)以及連線	
Tunnel Test:		可以按下連接於山	接鈕-Connect 比狀態上.	去驗證此通道	的狀態,測試結	果將會更新	
Config:		如下圖所示,設定項目包含編輯-Edit 以及刪除圖示					
		若您按下編輯 其『 的詞	按鈕- <u>Edit</u> ,; 中的設定.若您 设定將會被刪除	將會連接到此設 選擇按下垃圾榨 <<	定的項目當中, 靜圖示的話 🕕,	您可以修改 所有此通道	

Group VPN Connection List		Refresh Close
Group Name	IP address	Connection Time (seconds)



Add New Tunnel-新增一條 VPN 通道

Gateway to Gateway-VPN 閘道器對閘道器的設定

透過以下的設定說明,使用者就可以在兩台 FVR9416 之間建立一條 VPN 通道.

Tunnel No.:	當您設定 FVR9416 內建之 VPN 功能時,請選擇您要設定的 Tunnel 通 道編號,FVR9416 可支援最高 200VPN 通道設定
Interface:	您可以選擇哪一個介面位置做為此 VPN 通道的節點,一開始的預設 WAN 端共有四個 WAN1~4 可作為此 VPN 通道的使用.
Tunnel Name:	設定此通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設爲不同,以免混淆
	Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時, 有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道 才會順利連線開啓!.
Enable:	勾選 Enable 選項,將此 VPN 通道開啓. 此項目為預設為啓動 Eanble, 當設定完成後,可以再選擇是否啓動通道設定.
	Tunnel No. 1
	Tunnel Name
	Interface WAN1 💌
	Enable 🧹
Local Group Setup:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同.
Local Group Setup: Local Security Gateway	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同. 區域端群組設定,有五種操作模式項目選擇,分別為:
Local Group Setup: Local Security Gateway Type:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同. 區域端群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證 IP + Domain Name(FQDN) Authentication,-IP+網域名稱
Local Group Setup: Local Security Gateway Type:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同. 區域端群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證 IP + Domain Name(FQDN) Authentication,-IP+網域名稱 IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件
Local Group Setup: Local Security Gateway Type:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同. 區域端群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證 IP + Domain Name(FQDN) Authentication,-IP+網域名稱 IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件 Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置 +網域名稱
Local Group Setup: Local Security Gateway Type:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同. 區域端群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證 IP + Domain Name(FQDN) Authentication,-IP+網域名稱 IP + E-mail Addr.(USER FQDN) Authentication,-iP+電子郵件 Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置 +網域名稱 Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱
Local Group Setup: Local Security Gateway Type:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同. 區域端群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證 IP + Domain Name(FQDN) Authentication,-IP+網域名稱 IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件 Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置 +網域名稱 Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱



	Local Security Gateway Type IP Only
	IP address 192 . 168 . 5 . 86
	(2) IP + Domain Name(FQDN) Authentication:若您選擇 IP +網域名稱型態的話,請輸入您所驗證的網域名稱以及 IP 位置然後 FVR9416 的 WAN IP 位置,將會自動填入此項目空格內,您不需要 在進行額外設定. FQDN 是指主機名稱以及網域名稱的結合,也必 須存在於 Internet 上可以查詢的到,如 vpn.server.com.此 IP 位置 以及網域名稱必須與遠端的 VPN 安全開道器設定型態相同才可以 正確連接.
	Local Security Gateway Type IP + Domain Name(FQDN) Authentication
	Domain Name
	IP address 192 . 168 . 5 . 86
	(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話,只有固定填入此 IP 位置以及電子郵件位置可以存取此通道,然後 FVR9416 的 WAN IP 位置,將會自動填入此項目空格內,您不需要在進行額外設定
	Local Security Gateway Type IP + E-mail Addr.(USER FQDN) Authentication
	E-mail address @
	IP address 192 . 168 . 5 . 86
	(4) Dynamic IP + Domain Name(FQDN) Authentication:
	若是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN, ,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線; 若您選擇此型 態連接 VPN,請輸入網域名稱即可
	 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication ▼
	 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication
	 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication ▼ Domain Name (5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若 是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型態連接 VPN,請輸入電子郵件認證到 E-Mail 位置空格欄位中即可
	 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication ▼ Domain Name (5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication:若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型態連接 VPN,請輸入電子郵件認證到 E-Mail 位置空格欄位中即可 Local Security Gateway Type Dynamic IP + E-mail Addr.(USER FQDN) Authentication ▼
	 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication ▼ Domain Name (5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若 是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型態連接 VPN,讀輸入電子郵件認證到 E-Mail 位置空格欄位中即可 Local Security Gateway Type Dynamic IP + E-mail Addr.(USER FQDN) Authentication ▼ E-mail address
	 若是您使用動態IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN, 當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication ▼ Domain Name (5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若 是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型態連接 VPN,請輸入電子郵件認證到 E-Mail 位置空格欄位中即可 Local Security Gateway Type Dynamic IP + E-mail Addr.(USER FQDN) Authentication ▼ E-mail address @@
Local Security Group Type	 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型 態連接 VPN,請輸入網域名稱即可 Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication ▼ Domain Name (5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若 是您使用動態 IP 位置連接 FVR9416 時,您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;若您選擇此型態連接 VPN,請輸入電子郵件認證到 E-Mail 位置空格欄位中即可 Local Security Gateway Type Dynamic IP + E-mail Addr.(USER FQDN) Authentication ▼ E-mail address @ 此為設定本地區域端的 VPN 連線安全群組設定,以下有幾個關於本地 區域端設定的項目,請您選擇並設置適當參數:



此項目爲允許此 VPN 通道連線後,只有輸入此 IP 位置的本地端電 腦可以連線.
Local Security Group Type 🛛 P
IP address 192 . 168 . 1 . 0
以上的設定參考為:當此 VPN 通道連線後,於 192.168.1.0~255 的 此網段的 IP 位置範圍的電腦可以連線.
(2) Subnet 此項目為允許此 VPN 通道連線後,每一台於此網段的本地端電腦 都可以連線
Local Security Group Type Subnet 💌
IP address 192 , 168 , 1 , 0
Subnet Mask 255 , 255 , 255 , 192

以上的設定參考為:當此 VPN 通道連線後,只有 192.168.1.0,子網 路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 連線

Remote Group Setup:遠端安全群組設定:此項目的遠端閘道安全群組設定(Remote Security Gateway Type)型態必須與連接遠端的近端閘道安全群組設定(Local Security Gateway Type)型態相同.

Remote Security Gateway Type:	遠端安全群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證
	IP + Domain Name(FQDN) AuthenticationIP+網域名稱
	IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件
	Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置 +網域名稱
	Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP
	位置+電子郵件名稱
	(1) IP Only: 若您選擇 IP Only型態的話,只有固定填入此 IP 位置可以 存取此通道,
	Remote Security Gateway Type IP Only
	IP address
	若是使用者不曉得遠端客戶的 IP address,則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.



Remote Security Gateway Type		IP Only	*
	IP by DNS Resolved 💌		

(2) IP + Domain Name(FQDN) Authentication:若您選擇 IP

+網域名稱型態的話,請輸入 IP 位置以及您所驗證的網域名稱 FQDN 是指主機名稱以及網域名稱的結合,使用者可以輸入一個符 合 FQDN 的網域名稱即可.此 IP 位置以及網域名稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接.

Remote Security Gateway Type		IP + Domain Name(FQDN) Authentication	*
	IP address 🛛 👻		
	Domain Name		

若是使用者不曉得遠端的 IP address,則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address.此網域名稱必須存在 Internet 上可以查詢的到.並且在設定完成後在 Summary 的遠端 閘道下面自動顯示出相對應的 IP address.

Remote Security Gateway Type		IP + Domain Name(FQDN) Authentication	*
[IP by DNS Resolved 💌		
	Domain Name		

(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話,只有固定填入此 IP 位置以及電子郵 件位置可以存取此通道,

Remote Security Gateway Type	IP + E-mail Addr.(USER FQDN) Authentication	
IP address 💉		
E-mail address	@	

若是使用者不曉得遠端客戶的 IP address,則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.

Remote Security Gateway Type		IP + E-mail Addr.(USER FQDN) Authentication	
	IP by DNS Resolved 🔽		
	E-mail address	@	

(4) Dynamic IP + Domain Name(FQDN) Authentication: 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇動態 IP 位置加上主機名稱以及網域名稱的結合

Remote Security Gateway Type	Dynamic IP + Domain Name(FQDN) Authentication	*
Domain Name		

(5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若



	是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接	-
	VPN,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時,	
	FVR9416 將會開始驗證並回應此 VPN 通道連線; 請輸入電子郵	
	件認證到 E-Mail 位置空格欄位中	
	Remote Security Gateway Type Dynamic IP + E-mail Addr.(USER FQDN) Authentication 💌	
	E-mail address @	
Remote Security Group	此爲設定本地區域端的 VPN 連線安全群組設定,以下有幾個關於本地	
Туре:	區域端設定的項目,請您選擇並設置適當參數:	
	(1) IP Address 此項目為允許此 VPN 通道連線後,只有輸入此 IP 位置的本地端電腦 可以連線.	
	Remote Security Group Type 🛛 IP 🔍	
	N 上的乳空鼻老母・党件 \/DN 泽洋海角络 钛 102 169 1 0 255 的	
	此網段的 IP 位置範圍的電腦可以連線.	
	(2)Subnet	
	此項目為允許此 VPN 通道連線後,每一台於此網段的本地端電腦	
	都可以連線	
	Remote Security Group Type Subnet 🛛 👻	
	IP address	
	Subnet Mask 255 , 255 , 255 , 0	
	以上的設定參考為:當此 VPN 通道連線後,只有 192.168.1.0,子網 路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 連線	
	(3)IP Range 此項目為允許此 VPN 通道連線後,只有輸入此 IP 位置範圍的本地端 電腦可以連線	
	Remote Security Group Type IP range 🗸	
	IP range 0 , 0 , 0 ~ 0	
	以上的設定參考為:當此 VPN 通道連線後,只有 192.168.1.0 到	

192.168.1.254 的 IP 位置範圍的電腦可以連線

IPSec Setup

若是任何加密機制存在的話,此兩個 VPN 通道的加密機制必須要相同才可以將此通道連接,並於傳輸資料中加上標準的 IPSec 密鑰,我們稱為加密密鑰 "key". FVR9416 提供了以下二種加密管理模式 Key Management,分



別為手動(Manual)以及 IKE 自動加密模式- IKE with Preshared Key (automatic)如下圖所示.

	Keying Mode	Manual	×
	Incoming SPI		
	Outgoing SPI		
	Encryption	DES 💌	
	Authentication	MD5 💌]
	Encryption Key		
	Authentication Key		
Key Management:	此選項設定第 後,必須設定 數相同;設定 設定時請您證	為富您設定 一組交換密 的方式有自 選擇其中一	在WVPN 通道使用何種加密模式以及驗證模式 密碼,並請注意此參數必須與遠端的交換密碼參 自動 Auto (IKE)或是手動 Manual.設定二種:於 ·種設定方式即可! PSec Setup
		Keuine Mede	II/E with Decelored law
		Keying wode	IKE WITH Preshared Key
	Pha	se1 DH Group	Group1
	Pha	se1 DH Group	Group1 V DES V
	Pha Phas Phase1 / Phase	se1 DH Group e1 Encryption Authentication	Group1 V DES V MD5 V
	Pha Phas Phase1 / Phase Perfect Forv	xeying Mode se1 DH Group e1 Encryption Authentication 1 SA Life Time ward Secrecy	Group1 V DES V MD5 V 28800 seconds
	Pha Phas Phase1 Phase Perfect For Pha	xeying Mode se1 DH Group e1 Encryption Authentication 1 SA Life Time ward Secrecy se2 DH Group	Group1 V DES V MD5 V 28800 seconds
	Pha Phase Phase1 Phase Perfect Forv Pha Pha	et 2 Encryption Authentication 1 SA Life Time ward Secrecy se2 DH Group	Group1 V Group1 V Group1 V DES V Group1 V DES V
	Phas Phase1 Phase1 Phase Perfect Forv Phas Phase2	Authentication Authentication 1 SA Life Time ward Secrecy se2 DH Group e2 Encryption Authentication	Group1 V Group1 V Group1 V DES V Group1 V DES V MD5 V
	Phas Phase1 Phase1 Phase Perfect Forv Phas Phase2 Phase2	Authentication Authentication 1 SA Life Time ward Secrecy se2 DH Group se2 Encryption Authentication 2 SA Life Time	Group1 V Group1 V 28800 seconds Croup1 V DES V MD5 V MD5 V 3600 seconds

IKE with Preshared Key (automatic):透過 IKE 產生共用的金鑰來加密與驗 證遠端的使用者. 若將 PFS(Perfect Forward Secrecy)啓動後,則會再第二階 段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證.當 PFS 啓動後, 透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內,進一步得到第 二把金鑰.

PFS:若您將 PFS 選項勾選後,記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啓.

Phase1/Phase2 DH Group:

於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是 Group2/Group5.

Phase1/Phase2 Encryption:

此加密選項設定為設定此 VPN 通道使用何種加密模式,並請注意設置 此參數必須與遠端的加密參數相同: DES: 64-位元加密模式 3DES:.128-位元加密模式.



Phase1/Phase2 Authentication: 此驗證選項設定為設定此 VPN 通道使用何種驗證模式,並請注意設置 此參數必須與遠端的驗證模式參數相同: "MD5"/"SHA".

Phase1 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 28800秒(8小時),於此有效時間內的 VPN 連線,系統會自動的將於有效時間後,自動的生成其他的交換密碼以確保安全.

Phase2 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 3600 秒(1 小時),於此有效時間內的 VPN 連線,系統會自動的將於有效 時間後,自動的生成其他的交換密碼以確保安全

Preshared Key:於 Auto (IKE), 選項中,您必須輸入一組交換密碼於 "Pre-shared Key" 的欄位中,在此的範例設定為 test,您可以輸入數字 或是文字的交換密碼,系統將會自動的將您輸入的數字或是文字的交換 密碼自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數字或是文 字的交換密碼最高可輸入 30 個文字組合.

Manual-手動方式

Keying Mode	Manual
Incoming SPI	
Outgoing SPI	
Encryption	DES 💌
Authentication	MD5 💌
Encryption Key	
Authentication Key	

若您選擇手動模式 Manual 的話,此提供您自訂加密密鑰,而此密鑰不需經過任何交握(negotiation).

Manual 為手動方式設定交換密碼,於此分成加密密碼"Encryption KEY"以及驗證密碼"Authentication KEY"二種,您可以輸入數字或是文字的交換密碼,系統將會自動的將您輸入的數字或是文字的交換密碼 自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數字或是文字的 交換密碼最高可輸入 23 個文字組合.

另外還需要設定"Inbound SPI"的交換字串以及"Outbound SPI"交換字串,此字串必須與遠端 VPN 設備連接時相同;於此的 Inbound SPI 設定參數,您必須在遠端的 VPN 設備的 Outbound SPI 設定相同字串,而於本地端的 Outbound SPI 設定字串,也必須與在遠端的 VPN 設備 的 Inbound SPI 設定相同字串!

Advanced(進階作業模式)-只供給使用自動交換密鑰模式使用(IKE Preshareed Key Only)



Advanced settings are only for IKE with	Advan	ce Mode:(進階作業模式)
Preshared Key mode of		Aggressive Mode
IPSec.		Compress (Support IP Payload Compression Protocol(IPComp))
		Keep-Alive
		AH Hash Algorithm 🛛 >MD5 🛛 🐱
		NetBIOS broadcast
		Dead Peer Detection (DPD) Interval 10 seconds
	在FVR	9416 的進階設定項目中,分別有主要模式 Main Mode 以及進降

模式 **Aggressive Mode**, Main mode 是 FVR9416 的預設 VPN 作業模式而且與大多數的其他 VPN 設備使用連接方式爲相同;另外 Aggressive mode 大多爲遠端的設備採用,如使用動態 IP 連接時,爲了加強其安全控管機制,.

Compress:

若選擇此項目勾選,則連接的 VPN 通道中 FVR9416 支援 IP 表頭型態的 壓縮(IP Payload compression Protocol).

Keep-Alive:

若選擇此項目勾選,則連接的 VPN 通道中會持續保持此條 VPN 連接不會中斷,此使用多爲分公司遠端節點對總部的連接使用,或是無固定 IP 位置的遠端使用.

AH Hash Algorithm:

AH (Authentication Header) 驗證表頭封包格式,可選擇 MD5/DSHA-1

NetBIOS Broadcast:

若選擇此項目勾選,則連接的 VPN 通道中會讓 NetBIOS 廣播封包通過., 有助於微軟的系統網路芳鄰等連接容易,但是相對的佔用此 VPN 通道的 流量就會加大!

Dead Peer Detection(DPD):

若選擇此項目勾選,則連接的VPN通道中會定期的傳送HELLO/ACK 訊息封包來偵測是否VPN 通道的兩端仍有連線存在.當有一端斷線則 FVR9416 會自動斷線,然後再建立新連線.使用者可以選擇每一次 DPD 訊息封包傳遞的時間,預設值為 10 秒.



Client to Gateway-VPN 客戶端對閘道器的設定

透過以下的設定說明,管理人員就可以在客戶端與 FVR9416 之間建立一條 VPN 通道.

管理者可以選擇這一條 VPN 通道在客戶端是只供一個客戶所使用(Tunnel)或者是由一群客戶所使用(Group VPN).若由一群客戶所使用則可以節省個別設定遠端的客戶,只需設定的一條通道供一組客戶所使用,以節省設定時的麻煩.

在 Tunnel 的情況:

Tunnel No.:	當您設定 FVR9416 內建之 VPN 功能時,請選擇您要設定的 Tunnel 通 道編號,FVR9416 可支援最高 200VPN 通道設定.
Interface:	您可以選擇哪一個介面位置做為此 VPN 通道的節點,一開始的預設 WAN 端共有四個 WAN1~4 可作為此 VPN 通道的使用.
Tunnel Name:	設定此通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設爲不同,以免混淆
	Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時, 有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道 才會順利連線開啓!.
Enable:	勾選 Enable 選項,將此 VPN 通道開啓. 此項目為預設為啓動 Eanble, 當設定完成後可以再選擇是否啓動通道設定.
	Tunnel No. 1 Tunnel Name Interface WAN1 💌 Enable 💟
Local Group Setup:	此項目的近端閘道安全群組設定(Local Security Gateway Type)型 態必須與連接遠端的閘道安全群組設定(Remote Security Gateway Type)型態相同.
Local Security Gateway Type:	區域端群組設定,有五種操作模式項目選擇,分別為: IP Only-只使用 IP 作為認證 IP + Domain Name(FQDN) Authentication,-IP+網域名稱 IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件 Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置 +網域名稱 Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱
	(1) IP Only: 若您選擇 IP Only 型態的話,FVR 9416 會依據你所選擇的 廣域端口位置將其 IP 自動填入此項目空格內,您不需要在進行額外設 定.



	Local Security Gateway Type IP Only
	IP address 192 . 168 . 5 . 86
	(2) IP + Domain Name(FQDN) Authentication: 若您選擇 IP+網域名稱型態的話,請輸入您所驗證的網域名 稱,FVR9416的WAN IP位置,將會自動填入IP Address項目內,您不需 要在進行額外設定. FQDN 是指主機名稱以及網域名稱的結合,也必須 存在於 Internet 上可以查詢的到,如 vpn.server.com.此 IP 位置以及網 域名稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接.
	Local Security Gateway Type IP + Domain Name(FQDN) Authentication
	Domain Name
	IP address 192 . 168 . 5 . 86
	(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話,只要將電子郵件位置填入, 然後 FVR9416 的 WAN IP 位置,將會自動填入此項目空格內,您不需要 在進行額外設定
	Local Security Gateway Type IP + E-mail Addr.(USER FQDN) Authentication
	E-mail address @
	IP address 192 . 168 . 5 . 86
	(4) Dynamic IP + Domain Name(FQDN) Authentication:
	若是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN, ,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線; 若您選擇此型 態連接 VPN,請輸入網域名稱即可
	Local Security Gateway Type Dynamic IP + Domain Name(FQDN) Authentication
	Domain Name
	(5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若是您使用動態 IP 位置連接 FVR9416時,您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線;請輸入電子郵件認證到 E-Mail 位置空格欄位中即 可
	Local Security Gateway Type Dynamic IP + E-mail Addr.(USER FQDN) Authentication 👻
	E-mail address @
Local Security Group Type	此爲設定本地區域端的 VPN 連線安全群組設定,以下有幾個關於本地 區域端設定的項目,請您選擇並設置適當參數:
	(1)IP Address(單一 IP 地址) 此項目爲允許此 VPN 通道連線後,只有輸入此 IP 位置的本地端電腦可 以連線.



Local Security Group Type

ity Group Type	IP	*			
IP address	192	, 168].	1	0

以上的設定參考為:當此 VPN 通道連線後,於 192.168.1.0~255 的 此網段的 IP 位置範圍的電腦可以連線.

(2)Subnet

此項目為允許此 VPN 通道連線後,每一台於此網段的本地端電腦都可 以連線..

Local Security Group Type	Subnet	~		
IP address	192	. 168	. 1	. 0
Subnet Mask	255	, 255	, 255	. 192

以上的設定參考為:當此 VPN 通道連線後,只有 192.168.1.0,子網路遮 罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 連線

Remote Client Setup 遠端客戶端設定:

此項目的遠端閘道安全群組設定(Remote Security Gateway Type)型態必須與連接遠端的近端閘道安全群

組設定(Local Security Gateway Type)型態相同.

Remot Client:	遠端客戶設定,有五種操作模式項目選擇,分別為:
	IP Only-只使用 IP 作為認證
	IP + Domain Name(FQDN) Authentication,-IP+網域名稱
	IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件
	Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置
	+網域名稱
	Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP
	位置+電子郵件名稱
	出項目的遠端間道安全群組設定(Remote Security Gateway Type)

型態必須與連接遠端的近端閘道安全群組設定(Local Security Gateway Type) Gateway Type)型態相同.

(1) IP Only: 若您選擇 IP Only 型態的話,只有固定填入此 IP 位置可以 存取此通道,

Remote	Security Gateway Type	IP Only			*
	IP address 🛛 👻				

若是使用者不曉得遠端客戶的 IP address,則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端 閘道下面顯示出相對應的 IP address.



Remote	Security Gateway Ty	be	IP Only	*
	IP by DNS Resolved	~		

(3) IP+Domain Name(FQDN) Authentication:

若您選擇 IP+網域名稱型態的話,請輸入 IP 位置以及您所驗證的網域 名稱 FQDN 是指主機名稱以及網域名稱的結合,使用者可以輸入一個 符合 FQDN 的網域名稱即可.此 IP 位置以及網域名稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接.

Remote Security Gateway Type	IP + Domain Name(FQDN) Authentication	~
IP address 💌		
Domain Name		

若是使用者不曉得遠端的 IP address,則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address.此網域名稱必須存在 Internet 上可以查詢的到.並且在設定完成後在 Summary 的遠端 閘道下面自動顯示出相對應的 IP address.

Remote Security Gateway Type	IP + Domain Name(FQDN) Authentication	*
IP by DNS Resolved 🔽		
Domain Name		

(4) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話,只有固定填入此 IP 位置以及電子郵件位置可以存取此通道

IP address	*	IP + E-mail Addr.(USER FQDN) Authentication	Remote Security Gateway Type	
			IP address 💌	
(5) E-mail address @		@	E-mail address	(5)

若是使用者不曉得遠端客戶的 IP address,則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.

Remote Security Gateway Type	P + E-mail Addr.(USER FQDN) Authentication
IP by DNS Resolved 💟	
E-mail address	@
(4) Dynamic IP + Doma 用動態 IP 位置連接 I 名稱以及網域名稱的	ain Name(FQDN) Authentication: 若是您使 FVR9416時,您可以選擇動態 IP 位置加上主機 a結合
Remote Security Gateway Type Domain Name	Dynamic IP + Domain Name(FQDN) Authentication

(5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若



是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 連線時, FVR9416 將會開始驗證並回應此 VPN 通道連線; 請輸入電子郵 件認證到 E-Mail 位置空格欄位中

Remote Security Gateway Type	Dynamic IP + E-mail Addr.(USER FQDN) Authentication 💌
E-mail address	@

IPSec Setup

若是任何加密機制存在的話,此兩個 VPN 通道的加密機制必須要相同才可以將此通道連接,並於傳輸資料中加上標準的 IPSec 密鑰,於此我們稱為加密密鑰 "key". FVR9416 提供了以下二種加密管理模式,分別為手動 (Manual) 以及 IKE 自動加密模式-IKE with Preshared Key (automatic)如下圖所示.

Key Management:

此選項設定為當您設定此 VPN 通道使用何種加密模式以及驗證模式後,必須設定一組交換密碼,並請注意此參數必須與遠端的交換密碼參數相同;設定的方式有自動 Auto (IKE)或是手動 Manual.設定二種:於設定時請您選擇其中一種設定方式即可!

	IPSec Setup
Keying Mode	IKE with Preshared key 💌
Phase1 DH Group	Group1 💌
Phase1 Encryption	DES 💌
Phase1 Authentication	MD5 💌
Phase1 SA Life Time	28800 seconds
Perfect Forward Secrecy	
Phase2 DH Group	Group1 💌
Phase2 Encryption	DES 💌
Phase2 Authentication	MD5 💌
Phase2 SA Life Time	3600 seconds
Preshared Key	

IKE with Preshared Key (automatic):透過 IKE 產生共用的金鑰來加密與驗 證遠端的使用者. 若將 PFS(Perfect Forward Secrecy)啓動後,則會再第二階 段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證.當 PFS 啓動後, 透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內,進一步得到第 二把金鑰.

PFS:若您將 PFS 選項勾選後,記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啓.

Phase1/Phase2 DH Group:

於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是



Group2/Group5.

Phase1/Phase2 Encryption:

此加密選項設定為設定此 VPN 通道使用何種加密模式,並請注意設置 此參數必須與遠端的加密參數相同: DES: 64-位元加密模式 3DES:.128-位元加密模式.

Phase1/Phase2 Authentication:

此驗證選項設定爲設定此 VPN 通道使用何種驗證模式,並請注意設置 此參數必須與遠端的驗證模式參數相同: "MD5"/"SHA".

Phase1 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 28800秒(8小時),於此有效時間內的 VPN 連線,系統會自動的將於有效 時間後,自動的生成其他的交換密碼以確保安全.

Phase2 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 3600 秒(1 小時),於此有效時間內的 VPN 連線,系統會自動的將於有效 時間後,自動的生成其他的交換密碼以確保安全

Preshared Key:於 Auto (IKE), 選項中,您必須輸入一組交換密碼於 "Pre-shared Key" 的欄位中,在此的範例設定為 test,您可以輸入數字 或是文字的交換密碼,系統將會自動的將您輸入的數字或是文字的交換 密碼自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數字或是文 字的交換密碼最高可輸入 23 個文字組合.

Manual-手動方式

Keying Mode	Manual
Incoming SPI	
Outgoing SPI	
Encryption	DES 💌
Authentication	MD5 💌
Encryption Key	
Authentication Key	

若您選擇手動模式 Manual 的話,此提供您自訂加密密鑰,而此密鑰不 需經過任何交握(negotiation).

Manual 為手動方式設定交換密碼,於此分成加密密碼"Encryption KEY"以及驗證密碼"Authentication KEY"二種,您可以輸入數字或是 文字的交換密碼,系統將會自動的將您輸入的數字或是文字的交換密碼 自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數字或是文字的 交換密碼最高可輸入 23 個文字組合.

另外還需要設定"Inbound SPI"的交換字串以及"Outbound SPI"交換字串,此字串必須與遠端 VPN 設備連接時相同;於此的 Inbound SPI 設定參數,您必須在遠端的 VPN 設備的 Outbound SPI 設定相同字串,



而於本地端的 Outbound SPI 設定字串,也必須與在遠端的 VPN 設備的 Inbound SPI 設定相同字串!

Advanced(進階作業模式)-只供給使用自動交換密鑰模式使用(IKE Preshareed Key Only) Advanced settings are Advance Mode:(進階作業模式)

Advanced settings are Advar only for IKE with Preshared Key mode of IPSec.

Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive



NetBIOS broadcast

Dead Peer Detection (DPD) Interval 10 seconds

在 FVR9416 的進階設定項目中,分別有主要模式 Main Mode 以及 進 階模式 Aggressive Mode, Main mode 是 FVR9416 的預設 VPN 作業 模式而且與大多數的其他 VPN 設備使用連接方式為相同;另外 Aggressive mode 大多為遠端的設備採用,如使用動態 IP 連接時,為了 加強其安全控管機制,.

Compress:

若選擇此項目勾選,則連接的 VPN 通道中 FVR9416 支援 IP 表頭型態的 壓縮(IP Payload compression Protocol).

Keep-Alive:

若選擇此項目勾選,則連接的 VPN 通道中會持續保持此條 VPN 連接不會中斷,此使用多爲分公司遠端節點對總部的連接使用,或是無固定 IP 位置的遠端使用.

AH Hash Algorithm:

AH (Authentication Header) 驗證表頭封包格式,可選擇 MD5/DSHA-1

NetBIOS Broadcast:

若選擇此項目勾選,則連接的VPN通道中會讓NetBIOS 廣播封包通過., 有助於微軟的系統網路芳鄰等連接容易,但是相對的佔用此VPN 通道的 流量就會加大!

Dead Peer Detection(DPD):

若選擇此項目勾選,則連接的VPN通道中會定期的傳送HELLO/ACK訊息封包來偵測是否VPN通道的兩端仍有連線存在.當有一端斷線則FVR9416會自動斷線,然後再建立新連線.使用者可以選擇每一次DPD訊息封包傳遞的時間,預設值為10秒.

在 Group VPN 的情况:

Group No.:

最多可以設定兩組 Group VPN.



	FVR9416 SME Multi-WAN Firewall/VPN Router		
Interface:	您可以選擇哪一個介面位置做爲此 VPN 通道的節點,一開始的預設 WAN 端共有四個 WAN1~4 可作爲此 VPN 通道的使用.		
Group Name:	設定此通道連接名稱,如XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設爲不同,以免混淆		
	Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時, 有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道 才會順利連線開啓!.		
Enable:	勾選 Enable 選項,將此 VPN 通道開啓. 此項目為預設為啓動 Eanble, 當設定完成後可以再選擇是否啓動通道設定.		
	Tunnel No. 1 Tunnel Name Interface WAN1 Enable		
Local Group Setup: Local Security Group	此爲設定本地區域端的 VPN 連線安全群組設定,以下有幾個關於本地 區域端設定的項目,請您選擇並設置適當參數:		
Туре:	(1)IP Address 此項目為允許此 VPN 通道連線後,只有輸入此 IP 位置的本地端電腦可 以連線.		
	Local Security Group Type IP		
	IP address 192 , 168 , 1 , 0		
以上的設定參考爲:當此 VPN 通道連線後,於 192.168.1.0 此網段的 IP 位置範圍的電腦可以連線.			
	(2)Subnet 此項目為允許此 VPN 通道連線後,每一台於此網段的本地端電腦 都可以連線		
	Local Security Group Type Subnet 💌		
	IP address 192 . 168 . 1 . 0		
	Subnet Mask 255 , 255 , 255 , 192		
	以上的設定參考為:當此 VPN 通道連線後,只有 192.168.1.0,子網路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 連線		

Remote Client Setup:遠端客戶端設定

Remote Client:

遠端客戶端設定,有三種操作模式項目選擇,分別為:

Domain Name(FQDN),-網域名稱



E-mail Address(USER FQDN),- 電子郵件名稱 Microsoft XP/2000 VPN Client,- 微軟 XP/2000 VPN 客戶端

(1) Domain Name(FQDN):

若您選擇網域名稱型態的話,請輸入您所驗證的網域名稱.FQDN 是指 主機名稱以及網域名稱的結合,也必須存在於 Internet 上可以查詢的到, 如 vpn.server.com.此網域名稱必須與客戶端的近端設定型態相同才 可以正確連接

Remote Clier	nt Domain Name(FQDN)
Domain Nam	e
(2) E-mail Ad	dr.(USER FQDN):
若您選擇電子 此通道	郵件型態的話,只有固定填入此電子郵件位置可以存取
Remote Client	E-mail Address(USER FQDN)
E-mail address	@
(3) Microsoft	XP/2000 VPN Client:

若您選擇微軟 XP/2000 VPN 客戶端型態的話,您不需要在進行額外 設定.

Remote Client Microsoft XP/2000 VPN Client 🗸

IPSec Setup

若是任何加密機制存在的話,此兩個 VPN 通道的加密機制必須要相同才可以將此通道連接,並於傳輸資料中加 上標準的 IPSec 密鑰,於此我們稱爲加密密鑰 "key". FVR9416 提供了以下二種加密管理模式,分別爲手動 (Manual)以及 IKE 自動加密模式-IKE with Preshared Key (automatic).在選擇 Group VPN 的情況之下或 者是在遠端閘道安全型態 Remote Security Gateway Type 中使用動態位置 IP 時,Aggressive mode 會自動啓 動,沒有手動 Manual 模式.

Key Management:

Keying Mode	Manual
Incoming SPI	
Outgoing SPI	
Encryption	DES 💌
Authentication	MD5 💌
Encryption Key	
Authentication Key	



Keying Mode:	IKE with Preshared key
Phase1 DH Group	Group1 💌
Phase1 Encryption	DES 💌
Phase1 Authentication	MD5 💙
Phase1 SA Life Time	28800
Perfect Forward Secrecy	
Phase2 DH Group	Group1 💌
Phase2 Encryption	DES 💌
Phase2 Authentication	MD5 💌
Phase2 SA Life Time	3600
Preshared Key	

IKE with Preshared Key (automatic):透過 IKE 產生共用的金鑰來加密與驗 證遠端的使用者. 若將 PFS(Perfect Forward Secrecy)啓動後,則會再第二階 段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證.當 PFS 啓動後, 透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內,進一步得到第 二把金鑰.

PFS:若您將 PFS 選項勾選後,記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啓.

Phase1/Phase2 DH Group:

於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是 Group2/Group5.

Phase1/Phase2 Encryption:

此加密選項設定爲設定此 VPN 通道使用何種加密模式,並請注意設置 此參數必須與遠端的加密參數相同:

DES: 64-位元加密模式 3DES:.128-位元加密模式.

Phase1/Phase2 Authentication:

此驗證選項設定爲設定此 VPN 通道使用何種驗證模式,並請注意設置 此參數必須與遠端的驗證模式參數相同:

"MD5"/"SHA".

Phase1 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 28800秒(8小時),於此有效時間內的 VPN 連線,系統會自動的將於有效 時間後,自動的生成其他的交換密碼以確保安全.

Phase2 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 3600 秒(1 小時),於此有效時間內的 VPN 連線,系統會自動的將於有效 時間後,自動的生成其他的交換密碼以確保安全

Preshared Key:於 Auto (IKE), 選項中,您必須輸入一組交換密碼於 "Pre-shared Key"的欄位中,在此的範例設定為 test,您可以輸入數字 或是文字的交換密碼,系統將會自動的將您輸入的數字或是文字的交換 密碼自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數字或是文 字的交換密碼最高可輸入 23 個文字組合.



Advanced(進階作業模式)-只供給使用自動交換密鑰模式使用(IKE Preshareed Key Only) Advanced settings are Advance Mode:(進階作業模式) only for IKE with

Preshared Key mode of IPSec.

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- 📃 🛛 AH Hash Algorithm MD5 💽
- NetBIOS broadcast

在 FVR9416 的進階設定項目中,分別有 Main Mode 以及 Aggressive. 模式, Main mode 是 FVR9416 的預設 VPN 作業模式而且與大多數的其 他 VPN 設備使用連接方式為相同;另外 Aggressive mode 大多為遠端 的設備採用,如使用動態 IP 連接時,為了加強其安全控管機制.在選擇 Group VPN 時,Aggressive mode 會自動啓動.

Compress:

若選擇此項目勾選,則連接的 VPN 通道中 FVR9416 支援 IP 表頭型態的 壓縮(IP Payload compression Protocol).

Keep-Alive:

若選擇此項目勾選,則連接的 VPN 通道中會持續保持此條 VPN 連接不會中斷,此使用多爲分公司遠端節點對總部的連接使用,或是無固定 IP 位置的遠端使用.

AH Hash Algorithm:

AH (Authentication Header) 驗證表頭封包格式,可選擇 MD5/DSHA-1

NetBIOS Broadcast:

若選擇此項目勾選,則連接的 VPN 通道中會讓 NetBIOS 廣播封包通過., 有助於微軟的系統網路芳鄰等連接容易,但是相對的佔用此 VPN 通道的 流量就會加大!



PPTP

FVR9416 提供支援 Window XP/2000 的 PPTP 對我們 FVR9416 做點對點通道協定,讓遠端使用此種協定建 立 VPN 連線.

GNO	VPN => PPTP	Sitemap	Logout
General Setting Advanced Setting DHCP		Enable PPTP Server	
Tool Port Management Firewall VPN Summary	PPTP IP Address I	Range Range Start : 192 . 168 . 1 . 200 Range End : 192 . 168 . 1 . 209	
Gateway to Gateway Client to Gateway PPTP VPN Pass Through Log	Users	User Name : New Password : rm New Password : Add to list	
	Connection List User Name	Remote Address PPTP IP Address Refresh Apply Cancel	
			your future life

Enable PPTP Server:	當使用者勾選後即可以啓動點對點隧道協定 PPTP 伺服器.
PPTP IP Address Range:	請輸入近端 PPTP IP 位址的範圍,其目的是要給遠端的使用者一個可進入近端網路的入口 IP.輸入起始範圍 Range Start:請在最後一欄輸入數值.輸入結束範圍 Range End:請在最後一欄數入數值.
User Name:	請輸入遠端使用者的名稱
New Password and	輸入使用者帳號密碼及請再次確認輸入遠端使用者新的帳號密碼



Confirm New Password:	
Add to list:	新增輸入的帳號與密碼
Delete selected User:	刪除使用者
Connection List:	顯示出使用 PPTP 伺服器通道的使用相關資訊.
User Name:	連線建立後的遠端使用者名稱
Remote Address:	連線建立後的遠端使用者的 IP 位置
PPTP IP Address:	連線建立後,近端 PPTP 伺服器的 IP 位置
Back:	按下此按鈕"Back"即會回到上一頁
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是 必須於 Apply 儲存動作之前才會有效

VPN Pass Through-VPN 透通:封包穿透路由器功能



GNO Home	/PN => VPN Pass Through	Sitemap	Logout
General Setting Advanced Setting DHCP Tool Port Management Firewall VPN Summary Gateway to Gateway Client to Gateway PPTP VPN Pass Through Log	IPSec Pass Through : PPTP Pass Through : L2TP Pass Through :	 Enable Enable Disable Enable Disable 	
	Арріу	Cancel	your future life

IPSec Pass Through:	若是選擇 Enable 的話,則允許 PC 端使用 VPN- IPSec 封包穿透 FVR9416 以便與外部 VPN 設備連線
PPTP Pass Through:	若是選擇 Enable 的話,則允許 PC 端使用 VPN-PPTP 封包穿透 FVR9416 以便與外部 VPN 設備連線
L2TP Pass Through:	若是選擇 Enable 的話,則允許 PC 端使用 VPN-L2TP 封包穿透 FVR9416 以便與外部 VPN 設備連線

Log-日誌

System Log-系統日誌



Q			Sitemap Logout
ONO	Log => System Log		
Home			
General Setting	_		
Advanced Setting	Syslog		
DHCP		Enable Syslog	
Tool	Syslog Server:	0.0.0.0	(Name or IP Address)
Port Management			
Firewall	E mail		
VPN			
Log	Mail Commu	Enable E-Mail Alert	
System Log	Send E mail to		(Name or in Address)
Traffic Statistic	Sond E-mail to		
	Log Queue Length:	50	entries
	Log Time Threshold:	10	minutes
		E-mail Log Now	

FVR9416 系統日誌(System Log)提供三種功能項目,分別為-Syslog, E-mail and Log Setting.

Syslog-系統日誌

Enable Syslog:若是此選項勾選的話, Syslog 功能將被開啓Syslog Server:FVR9416 提供了外部 Syslog 伺服器收集系統資訊功能. Syslog 為
一項工業標準通訊協定,於網路上動態擷取有關的系統資訊.
FVR9416 的 Syslog 提供了包含動作中的連線來源位置(source IP
Address)與目地(destination IP Address)位置, 服務編號(Port
Number)以及型態(IP service),若要使用此功能,請輸入 Syslog 伺服
器名稱或是 IP 位置於" Syslog Server" 的空格欄位內.

E-mail-電子郵件

 Enable E-Mail Alert:
 若是此選項勾選的話,電子郵件告警(E-Mail Alert)將會被開啓

 Mail Server
 若您希望所有的 Log 電子郵件都可以寄出的話,請於此輸入電子郵件

 伺服器的名稱或是 IP 位置,如 mail.abc.com



Send E-mail To:	此爲設定 Log 收件人電子郵件信箱,如 abc@mail.abc.com	
Log Queue Length (entries):	自訂 Log entries 數量,系統預設爲 50 個 entries. 當到達此數量 時,FVR9416 將會自動 Mail 傳送 Log.	
Log Time Threshold (minutes):	自訂傳送 Log 間隔時間,系統預設為 10 分鐘. 當到達此時間時,FVR9416 將會自動 Mail 傳送此 Log. FVR9416 將會自動判別當 entries 數量或是間隔時間哪一個參數先 到達,就 Mail 傳送 Log 訊息給管理者.	
E-mail Log Now:	使用管理者可以即時直接按下此鈕傳送 Log.	

Log Setting-系統日誌設定

Log Setting		
	Alert Log	
Syn Flooding	IP Spoofing	Vin Nuke
Ping Of Death	🗹 Unauthorized Login At	tempt
	General Log	
🗹 System Error Messages	Deny Policies	Allow Policies
Configuration Changes	Authorized Login	
View System Log Outgoi	ng Log Table Incoming	Log Table Clear Log Now
,	Apply Cancel	
		your future life

Alert Log-選擇需要告警的內容

FVR9416 提供了包含以下的告警內容訊息,您只要打勾點選即可. Syn Flooding, IP Spoofing, Win Nuke, Ping of Death / Unauthorized Login Attempt.

Syn Flooding:	即在短時間內傳送大量的 syn packet,造成系統記錄連線的記憶體溢 滿.
IP Spoofing:	駭客透過封包監聽程式來攔截網路上所傳送資料,並在讀取後藉由程 式修改原發送端位址(source IP address),進入原目的端的系統內, 存取資源.
Win Nuke:	透過侵入或設陷阱的方式將木馬程式送入對方伺服器中.
Ping of Death:	透過傳送來產生超過 IP 協定所能夠允許的最大封包,造成系統當機.
Unauthorized Login Attempt:	當系統發現有企圖進入FVR9416的入侵者時,就會將訊息傳到系統日誌中.



General Log-一般系統日誌資訊

FVR9416 提供了包含以下的一般告警內容訊息,您只要打勾點選即可.系統錯誤訊息(System Error Messages),封鎖的政策(Deny Policies),通過的政策(Allow Policies),網頁過濾資訊(Content Filtering), Data Inspection, 登入設備(Authorized Login),設定變更(Configuration Changes).

System Error Message:	提供系統中各種錯誤訊息給系統日誌.如:不正確的設定,功能異常狀況發生,system重啓,PPPoE斷線等等
Deny Policies:	當遠端使用者因為Access Rule 而無法進入系統,此資訊會傳送到系統日誌中.
Allow Policies:	當遠端使用者因爲符合Access Rule 進入系統,此資訊會傳送到系統 日誌中.
Configuration Changes	當系統的設定改變時,此資訊回傳送到系統日誌中.
Authorized Login	每一個成功進入系統如:從遠端進入或從LAN端Login進入此台路由 器的資訊都會傳送到系統日誌中.

以下有四個有關線上查詢 Log 的按鈕,分別敘述如下:

View System Log: 此為查看系統日誌使用,其資訊內容分別可以於 FVR9416 線上讀取,包含全部訊息讀取 -ALL, 系統日誌-System Log, Access Log, Firewall Log 以及 VPN Log.如下圖所示:

1	🗿 system log - Microsoft Internet Explorer						
System Log Current Time: Fri Aug 27 08:15:37 2004		Aug 27 08:15:37 2004	ALL Refresh Clear Close				
	Time Event-Type		Message				
	Aug 27 08:03:15 2004	System Log	192.168.5.70 login attempt				
	Aug 27 08:03:09 2004	System Log	192.168.5.70 login				

Outgoing Log Table: 查看內部 PC 出 Internet 的系統封包日誌,此日誌內涵內部網路位置(LAN IP),目的地位置(Destination URL/IP) 以及所使用的通訊服務埠口(Port Number)型態(Type)等資訊.如下圖所示:



🚰 Outgoing Log Table - M			
Outgoing Log Table		Refresh	e 🔨
Time Event-Type		Message	

Incoming Log Table: 查看外部進入 FVR9416 防火牆的系統封包日誌,此日誌內涵外部來源網路位置(Source IP Address),目的地位置與通訊埠號(Destination Port Number)等資訊.如下圖所示:

🗿 Incoming Log Table - 1			
Incoming Log Table		Refresh Close	^
Time	Event-Type	Message	

Clear Log Now: 此按鈕為清除所有目前 FVR9416 的 Log 相關資訊.

System Statistics-系統狀態即時監控



Home								
		Home						
anaral Catting								
elleral Setting					Next page			
vanced Setting								
DHCD	Interface	LAN	DMZ	WAN1	WAN2			
DHCP	Device Name	ixpO	ixp5	ixp1	ixp2			
Tool	Status	Connected	Down	Connected	Down			
	IP Address	192.168.1.1	0.0.0.0	192.168.5.140	0.0.0.0			
Management	MAC Address	00-0c-41-00-00-00	00-0c-41-00-00-05	00-07-40-ca-0b-33	00-0c-41-00-00-02			
Firewall	Subnet Mask	255.255.255.0	0.0.0.0	255.255.255.0	0.0.0.0			
Firewall	Default Gateway		0.0.0.0	192.168.5.1	0.0.0.0			
VPN	DNS	192.168.1.1	222	192.168.5.20 192.168.5.1	0.0.0.0			
Log	Received Packets	17911	0	202302	0			
stem Lon	Sent Packets	16620	0	19729	0			
am Statistic	Total Packets	34531	0	222031	0			
in Statistic	Received Bytes	2805045	0	18139722	0			
ic statistic	Sent Bytes	8995414	0	6261079	0			
	Total Bytes	11800459	0	24400801	0			
	Received Bytes/Sec	0	0	2759	0			
	Sent Bytes/Sec	0	0	2420	0			
	Error Packets Received	0	0	0	0			
	Dropped Packets Received	0	0	0	0			
	Sessions			0	0			
	New Sessions Soc			0	0			

FVR9416 的 System Statistics 管理功能可以提供系統目前運作資訊包含 Device Name(機器名稱), Status(目前 WAN 端連線狀態), IP Address(IP 位置), MAC Address(網路實體位置), Subnet Mask(子網路遮罩), Default Gateway(預設通訊閘), DNS(網域名稱伺服器),Received Packets(收到的封包數量), Sent Packets(傳送的封包數量), Total Packets(全部的封包數量統計), Received Bytes(收到的封包 Byte 數量統計), Sent Bytes(傳送的封包 Byte 數量統計), Total Bytes(全部的封包 Byte 數量統計), Error Packets Received(收到的錯誤封包統計) 以及 Dropped Packets Received(LAN, WAN1 ~ WAN4 丟棄的封包統計),Session(聯線數), New Session/Sec(每秒新的聯線數)等資訊.

Traffic Statistic:

有六種資訊會顯示在流量統計的網頁裡,來提供管理對於流量有更好的管理與控制.



Q		Sitem	ap Logout
ONO	Log => Traffic Statistic		
General Setting			
Advanced Setting	Traffic Type : Inbound IP Source Address 🛛 👻		
DHCP	Source IP	bytes/sec	%
Tool	192.168.5.177	2925	92
1001	192.168.1.100	245	7
VPN Log System Log System Statistic Traffic Statistic			
		Refresh	your future life

Inbound IP Source Address:對內流量來源位置 IP 位置

在此圖表中顯示了來源端的 IP 位址, 每秒有多少 byte 與百分比.

Traffic Type : Inbound IP Source Address	*	
Source IP	bytes/sec	%
192.168.1.100	4	100

Outbound IP Source Address: 對外流量來源位置 IP 位置

在此圖表中顯示了來源端的 IP 位址, 每秒有多少 byte 與百分比.

Traffic Type : Outbound IP Source Address 🔽

Source IP	bytes/sec	%
192.168.5.173	422	99
192.168.1.100	4	0



Inbound IP Service:對內流量 IP 服務端口號

在此圖表中顯示了網路的協定的種類,目的端 IP 位址,每秒有多少 byte 與百分比.

Traffic Type : Inbound IP Service 🛛 👻

Protocol	Dest. Port	bytes/sec	%
TCP	http(80)	1270	99
TCP	1863	4	0

Outbound IP Service: 對外流量 IP 服務端口號

在此圖表中顯示了網路的協定的種類,目的端 IP 位址,每秒有多少 byte 與百分比..

Traffic Type : Outbound IP Service 🛛 🗸

Protocol	Dest. Port	bytes/sec	%
TCP	1161	216	67
TCP	http(80)	102	32

Inbound IP session:對內流量 IP 聯機數

在此圖表中顯示了來源端的 IP 位址,網路的協定的種類,來源端的埠口,目的端 IP 位址,目的端的埠口,每秒有多 少 byte 與百分比.

т	raffic Type : Inbo	und IP Session	*				
	Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
	192.168.1.100	TCP	3563	66.35.229.141	80	57	100

Outbound IP Session:對外流量 IP 聯機數

此圖表中顯示了來源端的 IP 位址,網路的協定的種類,來源端的埠口,目的端 IP 位址,目的端的埠口,每秒有多少 byte 與百分比

Fraffic Type : Outb	ound IP Session	*				
Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%



Logout



FVR9416 的網頁畫面右下方有一個 Logout 的按鈕,此按鈕為終止管理 FVR9416 並登出此管理畫面,若您下 次想再進入 FVR9416 管理畫面時,您必須再輸入管理驗證使用名稱與密碼.

5. Troubleshooting

6. FAQ

7. Appendix A: VPN Configuration Sample

Sample VPN Environment 1: Gateway to Gateway



Firewall Setting: Firewall >General >Block WAN Request = Disable

VPN Setting: VPN→Summary→Add New	Tunnel→Gateway to Gateway
----------------------------------	---------------------------

FVR9416 VPN Configuration for	Head Office A	Head Office B
Tunnel Name	НОВ	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	Subnet
Local Security Group Type → IP Address	20.20.20.0	10.10.10.0



Local Security Group Type -> Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	IP	IP
Remote Security Gateway Type → IP	100.100.100.100	200.200.200.200
Address		
Remote Security Group Type	Subnet	Subnet
Remote Security Group Type → IP Address	10.10.10.0	20.20.20.0
Remote Security Group Type → Subnet	255.255.255.0	255.255.255.0
Mask		
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Both sides should use the same key.	

Sample VPN Environment 2: Gateway to Gateway



VPN Setting: VPN→Summary→Add New Tunnel→Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type → IP Address	20.20.20.0	10.10.10.10
Local Security Group Type→ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	Domain Name	IP
Remote Security Gateway Type→ Domain	Company domain Name	
Name		
Local ID→ Domain Name		Company domain Name
Remote Security Gateway Type→ IP	100.100.100.100	200.200.200.200
Address		


FVR9416 SME Multi-WAN Firewall/VPN Router

Remote Security Group Type	IP	Subnet
Remote Security Group Type → IP Address	10.10.10.10	20.20.20.0
Remote Security Group Type→ Subnet		255.255.255.0
Mask		
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Sample VPN Environment 3: Client to Gateway (Tunnel)



Server A

VPN Setting: VPN→Summary→Add New Tunnel→Client to Gateway→Tunnel

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type→ IP Address	20.20.20.0	100.100.100.100
Local Security Group Type→ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type→IP		200.200.200.200
Address		
Remote Client	Email Address	
Remote Client→ Email Address	User Email Address	
Local ID -> Email Address		User Email Address
Remote Client→ IP Address	100.100.100.100	
Remote Security Group Type		Subnet
Remote Security Group Type → IP Address		20.20.20.0



FVR9416 SME Multi-WAN Firewall/VPN Router

Remote Security Group Type → Subnet		255.255.255.0
Mask		
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Sample VPN Environment 4: Client to Gateway (GroupVPN)



VPN Setting: VPN→Summary→Add New Tunnel→Client to Gateway→Group VPN

	Head Office A	HomeN (VPN Client SW)
Group Name/Tunnel Name	GroupVPN1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type → IP Address	20.20.20.0	Client IP Address
Local Security Group Type → Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type→IP		200.200.200.200
Address		
Remote Client	Domain Name	
Remote Client→ Email Address	Company Domain Name	



FVR9416 SME Multi-WAN Firewall/VPN Router

Local ID -> Email Address		Company Domain Name
Remote Security Group Type		Subnet
Remote Security Group Type → IP Address		20.20.20.0
Remote Security Group Type → Subnet		255.255.255.0
Mask		
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	
Advanced	Aggressive Mode	

Note: All Clients can sign up into one Group VPN simultaneously