

USG 100 VS ZyWALL 2 PLUS VPN IPsec 設定



虛擬私人網路利用現有的網路連線提供安全的通道傳輸,不需要租借昂貴的專線 一個安全的 VPN 通道必須組合一連串的加密認證方式,稽核跟規則開放 ZyWALL 所提供的 IPSec 為標準的 IPSec 通訊協定,包含一些標準的加密及 認證方式讓您在網際網路上建立安全的加密通道.

設定前 注意事項

- 1. 兩端設備的 LAN 網段需不同,避免路由規則上的錯亂.
- 2. 兩端設備設定的加密方式需相同。
- 3. 兩端底下電腦的防火牆請暫時關閉。
- USG100 的另一端設備,建議避開 USG 100 預設網段 192.168.1.0/24 ~192.168.3.0/24,若另一端無法改的話,且使用的是 USG 100 的中預設網段, 且該網段 USG 100 並未使用的話,請於介面的 IP 值改設為 0.0.0.0,避免路由發 生錯誤。

設定値

設定相關所需要 USG 100 與 ZyWALL 2 plus 的 WAN 及 LAN & IPsec VPN

www.zyxel.com.tw



Version 1.0

USG 100 端的設定

步驟 1:查看 WAN 及 LAN 的設定值,點選 "網路"→點選 "介面"→點選 "狀態" *ZyXEL*

🔗 Status	状態 連接埃角色	乙太網路	ppp 行動電話	WLAN	VLAN 虛擬區域網路 橋	接器	輔助 主幹		
	介面狀態								
	日名籍	状態	HA 狀態	臣城	IP 位址/網路這	¥	IP 指派	R8	動作
	🗄 wan1	100M/Full	n/a	WAN	61.221.211.143 / 255.2	255.255.	0 Static	n/a	n/a
	wan1 ppp	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0		Dynamic	n/a	n/a
	Elwan2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0		DHCP client	n/a	Renew
s	wan2 ppp	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0		Dynamic	n/a	n/a
同服器	lan1	Up	n/a	LAN1	192.168.1.1 / 255.255.	255.0	Static	DHCP server	n/a
P重新得用	lan2	Down	n/a	LAN2	192.168.2.1 / 255.255.	255.0	Static	DHCP server	n/a
AC STR	ext-wlan	Down	n/a	WLAN	10.59.0.1 / 255.255.25	5.0	Static	DHCP server	n/a
IAC PIAC	dmz	Down	n/a	DMZ	192.168.3.1 / 255.255.	255.0	Static	DHCP server	n/a
	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0		Dynamic	n/a	n/a
C VPN	III wlan-1	n/a	n/a	n/a	n/a / n/a		n/a	n/a	n/a
VPN	wlan-1-1	Down	n/a	WLAN	10.59.1.1 / 255.255.25	5.0	static	n/a	n/a
VPN	介面統計								
									重新
^	■名籍	狀態		傳送封包	接收封包		秘密	每秒傳送位元組	每秒接收位元
	🗏 wan1	100M/Full	16187		23621	0		0	0
	wan1_ppp	Inactive				0		0	0
	∃wan2	Down	0		0	0		0	0
	wan2_ppp	Inactive				0		0	0

步驟 2: ZyWALL →點選 "VPN" →點選 "IPsec VPN" →點選 "VPN 閘道器 "→按下 "新增" **〕**

ZyXEL						7 R 🛛 🕅
	> ZyWALL > VPN > IPSec VPN > VPN	Gateway				
Status ZyWALL 自授權 員 親路 一介面	VPN 並送案 集計 設定 総連線軟目:2 # △ 名等	器 SA 監控程式 我的位址	30 ♥ 毎頁連線數 安全開始		頁面: 匡 VPN 速線	I d 1 of 1 P P
総由 - 医域 - DDNS - 住疑何服器 - HTTP 重新導向 - ALG - TP/MAC 編定	1 IKE_Gateway	wani	114.33.236.83,0.0.0.0	VPN		
- 防火菌 N VPN - IPSec VPN - SSL VPN - L2TP VPN - 應用程式遂查		-	-			



步驟 3:設定一個名稱來識別此通道要連線對外的 VPN 通道

紅色框框為兩端設備皆需相同的值。

ZyXEL		7 र ूह, व
Status	ZyWALL > VPN > IPSec VPN > VPN Gateway > Edit > #2	
ZyWALL	一機設定	名稱可自訂
□ 授權 ■ 網路 一介面	VPN 脱道器名稱 開道設定	IKE_Gateway
 粘由 直域 DDMS 重旋伺服器 HTTP重新導角 ALG IP/MAC 绑定 防火器 E VPN IPSec VPN 	 投始的位址 ① 介面 ○ 制成点 省() 10 動場構立址 ◎ 動態位址 	選您此端對外的 VPN 介面 want ♥ Static 61.221.211.143/255.255.255.0 1. [11433226.63 2. [00.0]
SSL VPN L2TP VPN 唐用程式巡查 O Anti-X 装置 HA 一致的	 · 預先共用金編 · 一日本 · 本様 ID 類型 · ・ · ・ · 回 · ·	ZyXEL1234
日初日 日系統 日推護	內容 對等裝置 ID 類型 內容	
	務後1設定	Q Basir
	SA 留存時間 協商規式 提議	2800 (180 - 300000 ₩9#) Man v # Junio: 1 DES v MoS v @
	全論評組 NAT構築 ダ	DH1 M
		(· 國定) () 版 / 前) · · · · · · · · · · · · · · · · · ·
	🛢 Message Ready.	(U)

步驟 4:ZyWALL→點選"VPN"→點選"IPsec VPN"→點選"VPN 連線"→按下 "新增" 🗗

ZyXEL					? \ \ \
	ZyWALL > VPN > IPSec VPN	> VPN Connection			
Status	VPN 連線 PN 開道器	集訊器 SA 監控程式			
2 yWALL ロ技権 自対権 自対権 の 方面 - 路由 - 医域 - DDNS - 虚域何服器 - HTTP 重新導合 - ALG - ITTP = ITTP = ITTP - ITTP = ITTP = ITTP - ITTP = ITTP = ITTP = ITTP - ITTP = ITTP	全域設定	Sec 現列 分割」設定 【	30 ♥ 每頁連線數 封發 液算法 TUINNEL DES/SHA 逐用 重致	頁面: 正 完略 LAN1_SURNET/rm	
LTT VPN 集用程式基查 RAnti-X 安置 IIA 取件 可 系裁 日 維護					
	e Message Ready.				CLI

www.zyxel.com.tw

Version 1.0



最後按	卜套用即完成	USG 100)端的設定。	

XEL		? K 🛡 K 🛡
ZyWALL > VPN > IPSec VPN > VPN Connection > Edit	t>#1	
Status		
一艘設定		Advanced
連線名稱	VPN	
		0
VPN 附近法 wr ED MLM		Advanced
5 ● 単語 2 ● 重新 2 前 AC 37定 VPN 制造器 ● 単語 2 レロット ● 単語 2 レロット ● 単語 2 レロット ● 単語 2 レロット ● 単語 2 レロット ● 単語 2 ・ ロット ● ロ ● ロ ● ロ ● ロ ● ロ ● ロ ● ロ ● ロ		
KE_Gateway 🛛 wan1 114.33.236. 83,	0.0.0.0	
c VPN 策略 VPN		Advanced
VPN 本援策略 式墨查 遠端策略	LANI_SUBNET VINTERFACE SUBNET, 192.168.1.0/24 Zywall2plus VSUBNET, 192.168.0.0/24	
階段 2 設定		🚱 Basic
5.4 留存時間 現用通訊院定 1.4該 提議	28800 (180 - 3000000 秒號) ESF マ Tunnat マ # 加税? 認識	ŧ
	1 DES 💙 SHA1 🗸	ta a la construcción de la const
完整性順向機密(Perfect Forward Secrecy / PFS) 相關語言	none 💙	
□ 將此 VPN 連線新增全 IPSec_VPN 區域。		
· · · · · · · · · · · · · · · · · · ·		
 智用進線檢查 檢查方法 檢查/或時 檢查/或時 檢查/使時 檢查/使時 檢查/使時 檢查/收容 ● 檢查/比位址 ● 檢查/追៉編/附單中的第一個反晶後一個 IP 位址 □目誌 	(5-30 秒數) (1-10 秒數) (1-10) (網域名稱或 IP 位址)	
THUE THUE	(確定) (取消)	
Message Ready		



ZyWALL 2 PLUS

步驟 6: 查看 LAN 的設定值,點選 NETWORK→點選 LAN 端。

避開原本的 192.168.1.1 的網段。

	AN Static DHCP IP Alias Port Roles	
	LAN TCP/IP	
	IP Address 192 . 168 . 0 . 1	RIP Direction Both
	IP Subnet Mask 255 . 255 . 0	RIP Version RIP-1 💌
	Multicast None 💌	
	DHCP Setup	
	DHCP Server 💌	
	IP Pool Starting Address 192 2 168 2 0 2 33	Pool Size 32
OF STATE	DHCP Server Address 0 . 0 . 0 . 0	
	DHCP WINS Server 2 0 0 0 0 0	
	For DNS setup please click here	
	Filter (17) FIAC bilding)	
	Drop packets that do not match static IP or Dynamic IP/MAC binding Note: Binding that check static IP/MAC table first, then Dynamic IP/MAC to	able
	Event packets in this IP address range	307e
	From 0 . 0 . 0 . 0	
x. 3	Το 0.0.0.0	
\mathbf{N}	Windows Networking (NetBIOS over TCP/IP)	
	Allow between LAN and WAN	

步驟 7:查看 WAN 的設定值,點選 NETWORK→點選 WAN 端。 此範例為播接式的固定 IP 制的對外網路。

L		
	WAN	
	Route WAN Tra	affic Redirect Dial Backup
	ISP Parameters for Internet Acc	<u>ess</u>
	Encapsulation	PPP over Ethernet 💌
	Service Name	ADSL (Optional)
	User Name	12345678@ip.hinet.net 播接式的固定P 請輸您的ads帳號
3	Password	
2	Retype to Confirm	
≤	Authentication Type	CHAP/PAP 💌
1	Nailed-Up	
	Idle Timeout	100 (Seconds)
	WAN IP Address Assignment	
	Cot Automatically from ISD	
	Use Fixed IP Address	
	My WAN IP Address	0.0.0
	Advanted Colum	
	Auvanced Setup	
1	Enable NAT (Network Address	s Translation)
	RIP Direction	None
	RIP Version	RP-1
	-	
	Enable Multicast	Internal International Interna
-	Multicast Version	IGAP-V1 (#



步驟 8:查看 WAN IP 是否正確取得。

	-						
	System In	formation				Security Services	the second s
	System Nan	ie	7-0141 - 2 Dive			Content Filter Expiration Date	License inactive
	Roothaca Vic	reion	V1 14 L 02/18/20	109		Web Site Blocked	N/A
	Firmware Ve	ersion	V4.04(XU.6) 03	/17/2009			
	Up Time		17:13:40	,		Latest Alerts	
	System Time		2009-11-19 12:	11.21 GMT+08	0.0	Date/Time Mess	aye
	Deutee Mede		2009-11-19 121	11:31 001+001	00		
	Eirowall	-	Disabled				
≤	System Re	sources					
	Flash				4/8 MB		
	Memory				21/32 MB	System Status	
	Sessions				30/3000	Port Statistics DHCP Table	VPN Bandwidth
ee	COU						
	CPU				190		
	Interfaces	Status	IP/Netmask	PAssignmen	t Renew		
	WAN	ChangeMe	114.33.236. 83/ 255.255.255.255	IPCP client	Drop		
	Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial		
	E LAN	100M/Full	192.168.0.1 / 255.255.255.0	DHCP server	N/A		
	+ WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A		
	DMZ	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A		

步驟9:VPN建立通道,點選SECURITY→點選VPN→按下"新增"

C	XEL ZyWALL 2 Plus Internet Security Appliance	e - Windows Internet Explorer				
🗿 🗢 🖻 http://	l' hpSys.html			💌 🗟 😽 🗙 👂 Bing		P -
檔案(E) 編輯(E) 檢補	見(Y) 我的最愛(A) 工具(I) 説明(H)					
🚖 我的最爱 🔡 🔹	🥭	🏉 新索引標籤		🟠 • 🗟 • 🗆 🖶	 網頁(P)・安全性(2)・ 	IAO • 🕜 •
ZvXEL						HELP (?)
HOME	VPN					
REGISTRATION	VPN Rules (IKE) VPN Rules (Ma	nual) SA Monitor Global	Setting			
NETWORK 🖾	VPN Rules					
FIREWALL						
CONTENT FILTER		Local Network	Internet VPN fungel	Remote Network		
VPN			Remote Gatew	tur		
AUTH SERVER						
	# VPN Rules				*	
LOGS	1 home	114.33.236.83	\$\$61.221.211.143	F Î	698	
MAINTENANCE			~		~~~	
LOGOUT						
1 / / •						
/ / s	tatus: Ready					

www.zyxel.com.tw



Version 1.0

步驟 10: VPN 建立通道(Gateway), Authentication Key 的 Pre-Shared Key and IKE Proposal 需與步驟 3(認証、階段 1 設定的値)完全相同,並按下 Apply 套用。

XEL	Property
	Name
TRATION	NAT Traversal
	Gateway Policy Information
ITY 🖪	Construction in the second sec
VALL	zywali 2 plusłijwan ip
ENT FILTER	My Address TH-33.220.63 (Domain Name or IP Address) (Domain Name or IP Address)
	Wy bemain name down (See Dats) 部連入設備的wan ip
IFICATES	rimary definite doceway 01/221/11/49 (Domain Name or IP Address)
SERVER	Enable 1/Sec High Availability
NCED 🖂	(Domain Name or IP Address)
7	Fall back to Primary Remote Gateway when possible
	Pair Dack Creck Interval (180-86400 seconds)
IENANCE	"Fall Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.
л	Authentication Key
	7.VEI1924
	Pre-shared key Z/版供給 and another all all all all all all all all all al
	Local D Type P 文
N. 12	
	Peer ID Type
	Content 0.0.0
	Extensed Admentication
	Enable Extended Authentication
	O Server Mode (Search <u>Local User</u> first then <u>RADIUS</u>)
	Client Mode
	User Name
	Password
	IKE Proposal
	Negotiation Mode Man 💌
	Encryption Algorithm DES 💌
	Authentication Algorithm
	SA Life Time (Seconds) 28800
	Key Group DH1 V
	Enable Multiple Proposals
	Associated Network Policies
N.	Name Ioral Natural: Damata Natural:
No. 12	Anne Local Retwork Remote Retwork
	vpn-p2 255.255.0 255.255.0 U
	Apply

步驟 11:點選"新增 VPN 連線規則"

HELP (?)



步驟 12: 勾選 Active 點選,自訂一個 VPN 連線規則名稱,並選己建立的 VPN Gateway(home)剛剛步驟 10 所建立的, IPSec Proposal 需與步驟 5(階段 2 的 值)完全相同,並按下 Apply 套用。

HOME	VPN - NETWORK POLICY - EDIT	
REGISTRATION		
	Property	
FIREWALL	✓ Active	
CONTENT FILTER	Name vpn	
VPN	Protocol 0	
CERTIFICATES	V Nailed-Up	
AUTH SERVER	✓ Allow NetBIOS broadcast Traffic Through IPSec Tunnel	
	Check IPSec Tunnel Connectivity Log	
ADVANCED 🔛	Ping this Address	
LOGS	Gateway Policy Information	
MAINTENANCE	Sateway Policy home	
LOGOUT	Virtual Address Mapping Rule:	
D.C.	Active	
	Virtual Address Mapping Rule: Port Forwarding Rules	
N.	Type One-to-One M	
	Private starting IP Address 0 . 0 . 0 . 0	
	Virtual Starting IP Address 0 . 0 . 0 . 0	
	Virtual Ending IP Address 0 . 0 . 0	
	Local Network zywall 2 plus LAN 期段 允許透由 vpn存取的 ip 範圍	
	Address Type Subnet Address 🗸	
	Starting IP Address 192 . 168 . 0 . 0	
	Ending IP Address / Subnet Mask 255 . 255 . 255 . 0	
	Local Port Start 0 End 0	
	Remote Network	
	😯 Address Type Subnet Address 🗸	
	Starting IP Address 192 . 188 . 1 . 0	
X	Ending IP Address / Subnet Mask 255 , 255 , 255 , 0	
	Remote Port Start 0 End 0	
	IPSec Proposal	
X X	Encapsulation Mode Tunnel Y 2端設備務必要設相同的值	
	Active Protocol	
	Encryption Algorithm DES	
	Authentication Algorithm SHA1 V	
X	SA Life Time (Seconds) 2800	
	Perfect Forward Secrecy (PFS) NONE	
	Enable Replay Detection	
X		
12		
1. 1		
1 1	status: Keady	

步驟 13:點選 VPN→點選 SA Monitor 查看 VPN tunnel 是否建立成功。

ZyXEL		HELP
НОМЕ	VPN 查看是否Tunnel是否爲建立成功.	
REGISTRATION	VPN Rules (IKE) VPN Rules (Manual) SA Monitor Global Setting	
NETWORK 🖾	Security Associations Table	
SECURITY SIREWALL	# Name Local Network Remote Network Encapsulation IPSec Algorithm	
CONTENT FILTER	• 1 Vpn 255.255.0 255.255.0 Iunnel ESP DES-5HA1	
VPN		
CERTIFICATES	有看到此筆,即代表建立成功	
AUTH SERVER	rerean baconnex	
ADVANCED 🗵		
LOGS		
MAINTENANCE		
LOGOUT		