# USG 系列,用 PPPOE 播上固 IP, 用戶端用 IPsec VPN Clinet 軟體,並用 PPPOE 播 上狀況.

1.請先設定 USG 的對外上網 PPPOE 的設定.



2.確認是否有播上及是否為您的固定 IP

點選"監視"→點選介面狀態 WAN1 的 PPP,看到 Sea 圖示代表有播上 PPPOE

条続狀態	介面狀態							
→ 埠統計	名稱	Port	狀態	區域	P位址網路遮罩	旧指派	服務	動作
<ul> <li>· 川里秋語</li> <li>· 川里秋語</li> </ul>	🖨 <u>wan1</u>	P1	1000M/Full	WAN	192.168.2.110 / 255.255.255.0	DHCP client	n/a	更新
<ul> <li></li></ul>	wan1 ppp	P1	Connected	WAN	118.168.95.246 / 255.255.255.255	Dynamic	n/a	6
→ DDNS 状態	lan1	P2, P3	Up	LAN1	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a
<ul> <li>         ·          ·          ·</li></ul>	lan2	P4	Down	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
• WLAN 狀態	- dmz	P5	Down	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
→ Cellular 狀態	🖻 <u>wlan-1</u>	PC Card 1	n/a	n/a	n/a / n/a	n/a	n/a	n/a
VPN 監視	wlan-1-1	PC Card 1	Down	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

3.設定 IPSec VPN,點選"VPN"→IPSec VPN→點選 VPN 閘道器→點選"新增"

- 設定 7¥Quick Setup □ 授權	VPN 連線 設定	•			
- ↑ 介面 + 路由 + 區域 + DDNS	● 和 Pa ● 和 Pa A ● 1996 # 状態 名稱 1 ● TOTA	、 我的位址 ewan1_ppp 行	安全開道 0.0.0.0, 0.0.0.0	VPN 連線 remote	顯示1-1行 共有1行
<ul> <li>NAT</li> <li>HTTP 重新導向</li> <li>ALG</li> <li>PMAC 錄完</li> <li>認道 策略</li> <li>防火播</li> <li>VPN</li> <li>SSL V</li> <li>BWM</li> <li>AntbX</li> <li>物件</li> <li>%統</li> <li>日誌 &amp; 報告</li> </ul>	○ VPN + IPSec \ + SSL VF		●新増 光 Ad	f a new n	1 相 相

藍色框框代為 Server& IPSec VPN Client 軟體需設相同的設定值

藏運階設定		
設設定		
☑ 啟用 VPN 閘道器名稱:	from_RM	
道設定		
<b>的位址</b> ③ 介面	wan1_ppp Vynamic 118. 168.95.246/255	255.255.255
◯ 網域有得/₽		
<b>等開道位址</b> ◎ 靜態位址	主要 0.0.0.0 次要 0.0.0.0	
◎ 動態位址		
预先共用金論	1234567890	
》 進發	「新日本」(新日本語道)	
k機 ID 類型:	Ib 🔪	
內容:	192.168.1.1	
时等装置 ID 類型:	IP 🛩	
內容:	192, 168, 10, 1	
後1設定		
A 留存時間:	86400 (180 - 3000000 秒數)	
岛商模式:	Main	
是議	◎新増 ≧编辑 書称件	
	# 加密 / 認證	
	1 DES MD5	
2.111111111111111111111111111111111111	DH1 🗸	
NAT 橫跨		
7] 斷線值測(Dead Peer Dete	ction ' DPD)	•

定 IPSec VPN,點選"VPN"→IPSec VPN→點選 VPN 連線→點選"新增"



VPN 連線 VPN 限	利道器						
全域設定							
<ul> <li>✓ 使用策略路由指</li> <li>② 忽略封包標題     <li>設定     </li> </li></ul>	<ul> <li>☑ 使用策略路由控制動態 IPSec 規則</li> <li>□ 忽略封包標題中的「切勿分割」設定</li> <li>1</li> <li>3</li> </ul>						
💿 新増 🍞 編輯		亭用 🕵 連接 🚷 中斷連線 📑 參考的物格	+				
# 狀態	名稱	VPN 閘道器	封装	演算法	策略		
1 💡 😪	remote	from_RM	TUNNEL	DES/SHA1	LAN1_SUBNET/ RM_host		
1 × 1 × 1	夏 共頃	安良線小 50 ¥ 11			顧小1-11, 天月11.		

## 調整區域

	設定	
		719快速設定
	④ 授權	
	🛛 網路	
Qos	+ 介面	
	92 H	
<b>R</b> .	+ 區域	
	+ DDNS	

# 將 IPSEC VPN 按下编輯

Æ				
◎新増 🣝 編輯	<b>自</b> 移除 📑 參考的物件			
# ~	名稱	封鎖內部區域流量	成員	
间 4   第 1	頁,共1頁 ▶ ▶ 每頁顯示 50	<b>v</b> 17		沒有任何資料
統領蒙				
🥜 編輯 📑 參考的	物件			
<mark>子編輯</mark> 등参考的 Edit the select	的件 tted rule 名稱	封鎖內部區域流量	成員	
<mark>泛編輯</mark> 医参考的 Edit the select	物件 ted rule 3稱 LAN1	封鎖內部區域流量 no	成員 lan1	
✔編輯 Edit the select 1 2	物件 ted rule 名稱 LAN1 LAN2	封鎖內部區域流量 no no	成員 lan1 lan2	
● 編輯 Edit the select 1 2 3	的件 Lted rule 皆解 LAN1 LAN2 WLAN	封鎖內部區域流量 no no no	成員 lan1 lan2 wlan-1-1	-
● 編輯 Edit the select 1 2 3 4	附件 Lted rule 皆解 LAN1 LAN2 WLAN WAN	封鎖內部區域流量 no no no yes	成員 lan1 lan2 wlan-1-1 wan1,wan1_ppp	-
➢編輯 Edit the select 1 2 3 4 5	地特件 Lean 1 LAN1 WLAN WLAN WLAN WLAN DMZ	封鎖內部區域流量 no no yes yes	成員 lan1 lan2 wlan-1-1 wan1,wan1_ppp dmz	-
● 編輯 Edit the select 1 2 3 4 5 6	地特件 Lan1 Lan2 WLAN WAN DMZ SSL VPN	封鎖內部區域流量 no no yes yes yes	成員 lan1 lan2 wlan-1-1 wan1,wan1_ppp dmz	

## 將 IPSEC VPN 閘道器建立的物件加入成員

詳細成員         名稱:       IPSec_VPN         受 封鎖內部區域流量       1         成員清單          可用          remote          Imit       Imit         Imit       Imit	🔾 Add Zone					? ×
名稱: IPSec_VPN ● 封鎖內部區域流量           成員清單       成員         可用	群組成員					
▼ 封鎖內部區域流量       成員清單       可用       === VPN Tunnel ===       remote         ●	名稱:	IPSec_VPN				
成员清單 可用 remote wtwo Devices and the second sec	🔽 封鎖內部區域流量	<b>1</b>				
■用 remote ● ●	成員清單					
=== VPN Tunnel === remote €	可用			成員		
remote	=== VPN Tun	nel ===				
	remote					
			+			
			+			
VEAC AX78					確定	取消

群組成員 名稱: IPSec_VPN ☑ 封鎖內部區域流量	
名稱: IPSec_VPN	
☑ 封鎖內部區域流量	
成員清單 成員	
可用 成員	
=== VPN Tunnel ===	
remote	
•	
•	
· · · · · · · · · · · · · · · · · · ·	取消

區域

設定				
③新増 🃝 編輯 🎁	▋移除 🔚 參考的物件			
# ^	名稱	封鎖內部區域流量	成員	
4 4   第 1 頁	〔,共1頁│ ▶ ▷│ │ 毎頁篇	順示 50 🖌 行		沒有任何資料
条統預設				
2編輯 📑參考的	物件			
# -	名稱	封鎖內部區域流量	成員	
1	LAN1	no	lan1	
2	LAN2	по	lan2	
3	WLAN	no	wlan-1-1	
4	WAN	yes	wan1,wan1_ppp	
5	DMZ	yes	dmz	
6	SSL_VPN	yes		
7	IPSec_VPN	yes	remote	
◎ ◎ 第 1 頁	[,共1頁│ ▶ ▶      毎頁露	項示 50 🖌 行		顯示 1 - 7 行, 共有 7 行

即完成 USG 端設定

# 電腦端用 IPSEC VPN 軟體設定

### LAN 端用 PPPOE 播上, 區域連線設定 IP:192.168.10.1

網路連線詳細資料		📙 區域連線 狀態	X
網路連線詳細資料①:		一般	
内容	值		
連線特定 DNS 尾碼 描述 實體位址 DHCP 已散用 IPv4 位址 IPv4 子網路遮罩 IPv4 預設開道 IPv4 預設開道 IPv4 DNS 伺服器 IPv4 WINS 伺服器 IPv4 WINS 伺服器 NetBIOS over Topip 已	Marvell Yukon 88E8072 PCI-E Gigabit E 00-25-B3-5A-07-32 否 192.168.10.1 255.255.255.0	2年版 IPv4 連線能力: IPv6 連線能力: 媒體狀態: 連線時間: 速度: 詳細資料(E) 活動 日傳送 —	<ul> <li>無網際網路存取</li> <li>無網路存取</li> <li>已散用</li> <li>00:46:44</li> <li>1.0 Gbps</li> </ul>
		位元組: 1,123,0	69   7,570,380
		- 🧐 內容 (2)  🛞 停用 (2)	) 診斷(()
			[關閉(C)]

### 確認 PPPOE 有播上

-h #*	/#
装置名稱	WAN Miniport (PPPOE)
裝置類型	PPPoE
驗證	PAP
壓縮	(無)
PPP 多重連結架構	關閉
用戶端 IPv4 位址	118.168.87.167
伺服器 IPv4 位址	168.95.98.254
NAP狀態	不支援 NAP
原始位址	(無法辨識)
目的地位址	(無法辨識)

#### 設定 IPsec VPN Client 軟體

![](_page_6_Picture_1.jpeg)

Z ZyWALL	IPSec VPN Cli	ent	1000	1777		×
File VPN (	Configuration	View Too	ols ?			
Zy	XEL					
🔎 Con	sole	Tunne	ls view			
Parameters					Conne	ction Panel
S Con	nections	Host		IP	Mode	Crypto
	New Pha Reset Cor Move VP	se1	tion to USB	Drive		lose Tunnel
	eady				<u>S</u> ;	ave & Apply

ZyWALL IPSec VPN Client	Second	
<u>File VPN Configuration</u> V	ie <u>w</u> <u>T</u> ools <u>?</u>	
ZyXEL		
Q Console	Phase1 (Authentication)	
Parameters	Name Gateway1	
	Interface Any	<b>_</b>
Root	Remote Gateway 118.168.95.246	
Gateway1	Preshared Key     Confirm:     *********************************	
	C Certificate Certificate Mar	nagement 請參考下一頁
	IKE	Advanced Settings
	Encryption DES	
	Key Group DH1 V	
		Save & Apply
VPN Tunnel opened		Tunnel 🔘
Phase1 Advanced		
	ZyXEL	
Advanced features		
Conrig Mode Re	NAT-T Automatic	
X-Auth		本 USC 20 VDN 問題
□ X-Auth Popup	Login / 学社	5 USG 20 VPN 闸迫
Looal and Remote ID Choose the type	of ID: Set the value for the ID:	
Local ID IP Address	192.168.10.1	
Remote ID IP Address	▼ 192.168.1.1	
L		
	OK Cancel	

Z ZyWALL IPSec VPN C	lient 🗾 🗖 🗖 🖉
File VPN Configuratio	n View Tools ?
ZyXEL	
💫 Console	Phase1 (Authentication)
🙀 Parameters	Name Gateway1
S Connections	Interface Any
Root	Remote Gateway 118.168.95.246
⊞-Sateward	Add Phase2 by XXXXXXXXXX
	Remove
	C Certificate Certificate Management
	IKEAdvanced Settings
	Save & Apply
VPN Tunnel opened	lunnel
Z ZyWALL IPSec VPN Clien File VPN Configuration	It I I I I I I I I I I I I I I I I I I
Console	
S Connections	VPN Client address 192 . 168 . 10 . 1
□	Address type Subnet address Remote LAN address 192 . 168 . 1 . 1 Subnet Mask 255 . 255 . 0
	ESP Encryption DES  P2 Advanced Authentication SHA-1  Scripts Mode Tunnel
	F PFS Group None
	Save & Apply
Apply VPN configuration.	Tunnel 🥑

Automatic Open mode         Automatically open this tunnel when VPN Client starts after logon.         Automatically open this tunnel when USB stick is inserted.         Automatically open this tunnel on traffic detection.         Gina Mode         Enable before Windows logon.         Alternate servers         DNS Server         0       0         WINS Server	nase2 Advanced
Automatic Open mode         Automatically open this tunnel when VPN Client starts after logon.         Automatically open this tunnel when USB stick is inserted.         Automatically open this tunnel on traffic detection.         Gina Mode         Enable before Windows logon.         Alternate servers         DNS Server       0         0       0         WINS Server       0	ZvXEL
Automatic Open mode         Automatically open this tunnel when VPN Client starts after logon.         Automatically open this tunnel when USB stick is inserted.         Automatically open this tunnel on traffic detection.         Gina Mode         Enable before Windows logon.         Alternate servers         DNS Server       0         0       0	
Automatically open this tunnel when VPN Client starts after logon. Automatically open this tunnel when USB stick is inserted. Automatically open this tunnel on traffic detection. Gina Mode Enable before Windows logon. Alternate servers DNS Server 0 0 0 0 0 0 WINS Server 0 0 0 0 0	Automatic Open mode
Automatically open this tunnel when USB stick is inserted. Automatically open this tunnel on traffic detection.  Gina Mode Enable before Windows logon.  Alternate servers DNS Server 0.0.0.0 WINS Server 0.0.0	Automatically open this tunnel when VPN Client starts after logon.
Automatically open this tunnel on traffic detection.  Gina Mode  Enable before Windows logon.  Alternate servers  DNS Server 0.0.0.0  WINS Server 0.0.0.0	Automatically open this tunnel when USB stick is inserted.
Gina Mode   Enable before Windows logon.  Alternate servers  DNS Server  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Automatically open this tunnel on traffic detection.
Enable before Windows logon.   Alternate servers  DNS Server  0  0  0  0  0  0  0  0  0  0  0  0  0	Gina Mode
Alternate servers           DNS Server         0         0         0           WINS Server         0         0         0	Enable before Windows logon.
DNS Server 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0	Alternate servers
WINS Server 0.0.0.0	DNS Server 0 . 0 . 0
	WINS Server 0 . 0 . 0 . 0
OK Cancel	OK Cancel

ZyWALL IPSec VPN Clien	t ×
File VPN Configuration	Vie <u>w</u> Iools <u>?</u>
ZyXEL	
Res Console	Phase2 (IPSec Configuration)
Parameters	Name Tunnel1
Sonnections	VPN Client address 192 , 168 , 10 , 1
⊡-🤂 Root ⊡-S Gateway1 Tunnel1	Address type Subnet address Remote LAN address 192 . 168 . 1 . 1 Subnet Mask 255 . 255 . 0
	ESP Encryption DES  P2 Advanced Authentication SHA-1 Mode Tunnel
	PFS Group None
VPN ready	Tunnel 🥑

ZyWALL IPSec VPN Clie	int	
<u>File VPN Configuration</u>	Vie <u>w</u> <u>T</u> ools <u>?</u>	
ZyXEL		
🔎 Console	Tunnels view	
Parameters		Connection Panel
S Connections	Host	Mode Crypto
E S Root Gateway1	S Gateway1-Tunnel1-P2 192.168.1	Tunnel ESP DES
		Close Tunnel
VPN Tunnel opened		Tunnel 👩

# USG 20W 畫面 當 IPSec VPN 建立成功後

監控	IPSec					1.27			
<ul> <li>● 糸統狀態</li> <li>□ VPN 監視</li> </ul>	使用中	的IPSec安	全性關聯						
	名稱:	1							
<ul> <li>IPSec</li> <li>SSL</li> </ul>	策略	i.				搜尋			
❶ Anti-X 統計		山町連線							
「日前の	#	名稱▲	封裝	策略	演算法	已執行時間	等候時間	進向(位元組)	外撥(位元…
	1	remote	Tunnel	192.168.1.0/24<>1	esp/des/sha1	416	804	2(76 bytes)	6(5872 bytes)
	M	🛯 🗍 第 1	員,并1頁 🛛 🕅	▶ 母見親不 50 ¥	ĨŢ			顯示	1-1行, 共有1行