USG 韌體版本 2.20, SSL 結合 LDAP server 驗證設定範例



範例: LDAP server 資訊

LDAP Server:10.100.100.50 建立的群組 Group(有 CSO、sales 群組)

Sales 群組成員(anney) CSO 群組成員 (jones,thomas) 該網域的管理者 manager

名稱解釋:			
Base DN	指的是 LDAP/Windows AD 的搜尋的物件的儲存路徑的啓始位置.		
	如需跟 nwa.idv.tw 網域中的使用者驗証或特定群組		
	Base DN 爲(ou=users,dc	=nwa,dc=idv,dc=tw)	
Bind DN	需要輸入儲存"足夠管理網	域的使用者權限"物件的儲存路徑,用於與AD or LDAP 連	
	線授權用・ (cn= leopard	, dc=nwa,dc=idv,dc=tw)	
	注意的是如果此處的使用:	者帳號沒有足夠的權限的話 ,那此 LDAP Client 是無法	
	認證 User 的		
LDAP 中	UID	的指使用者名稱	
Attribute	OU	OU 是一種 Active Directory 容器,您可以在其中放置	
	(OrganizationalUnitDN)	使用者、群組、電腦及其他 OU。OU 無法包含其他網	
		域中的物件。	
	UPN	指的登入網域 mail,如 manage@nwa.idv.tw	
	(userPrincipalName)		
	CN(Display Name)	使用者名稱_UserDN 的一般名稱 (CN) 值中的最多前	
		20 個字元, 指定安全性帳戶管理員 (SAM) 名稱做為	
		此使用者的唯一帳戶名	

設定五大要點:

- 1. 檢查韌體版本
- 2. 設定 LDAP Server 資訊
- 3. 設定帳唬登入時,所查詢的帳號資料庫。
- SSL VPN→設定存取規則 (可存取的使用者/群組、配置登入的使用者 IP 位址、可存取的資源)
- 5. Zone 的設定 SSL_VPN 的應用規則

步驟一:確認韌體版本為:2.20版本

Z	YXEL Zywa	LL USG 100			<u>ut</u> ?Help Z About	🐴 Site Map 🛛 🔁 Obje	ct Reference 📮 Console	CLI 🗔
	DASHBOARD						Widget Settings	
	Uirtual Device							<
	Rear Panel			NAME WAAD	LAVINLANDAZ	P7		-m
	T Device Informatio	n	• @ ¢ X	System Status			× @ ¢ >	× -
	System Name:	zywall-usg-100		System Uptime:		4 days, 01:08:31		
	Model Name:	ZyWALL USG 100		Current Date/Time:		2010-04-20 / 19:	08:22 GMT+08:00	
	Serial Number:	S080Z01008459		VPN Status:		<u>0</u>		
	MAC Address Range:	00:19:CB:76:F2:49 ~ 00:19:CB:76:F2:4	1E	DHCP Table:		<u>0</u>		
	Firmware Version:	2.20(AQQ.0)-20100413#49226 / 1.08 /	2010-04-13 20:07:37	Current Login User:		admin (unlimited /	00:29:58)	
			0000	Number of Login Us	ers:	1		
	System Resource	5	▲ ③ ¢ X	Boot Status:		ОК		
	CP0 Usage	5 %		Eicensed Servic	e Status			K
	Memory Usage			# Status	Name	Version	Expiration	
		36 %		1 📀	IDP Signature	v2.232	24	
	- Elach Hearra				A eti Minue		24	× ×

步驟二:以 LDAP 為範例,●先點選 Configuration→❷點選 Object(物件)→ ❸點 選 AAA Server→點選④ LDAP → ⑤點選 Add,手動建立新的驗證規則, 名稱為 thomas_LDAP。

Z	YXEL ZYWALL	USG 100	4		Welcome admin <u>Loqout</u>	? Help 🛛 About 🛛 🗘 Transform	🖬 Object Reference 🖵 Console 🛄 CLI
	CONFIGURATION	Active Directory	LDAP	RADIUS			
	TY Quick Setup	LDAP Server Su	mmary	•			
Ö	+ Firewall ⊡ VPN	🕜 Add 🦉	Remov	e 📳 Object Refere	nce		
R	+ IPSec VPN + SSL VPN	# Name 1 Idap			Server Address	Base DN	
	+ L2TP VPN + App Patrol	14 4 Page	1 of 1	Show 50	v items		Displaying 1 - 2 of 2
	Anti-X Anti-Virus				I CEIIIS		Displaying 1 2012
	• IDP • ADP						
	 Content Filter Anti-Spam 	4					
	⊖ Object 2						
	Address Service						
	Schedule Add Server						
	Auth. Method Certificate						
	ISP Account SSL Application						
	E Log & Report						

Winter Address: 1000000000000000000000000000000000000	WEL THURLING THE	We	ecome admin (Looss) ?Help Z About 🛊 St	e Map 😰 Object Reference 🖵 Console 了 CLI
Office Labor Server Address: Betch: Server Address: Betch: Server Address: Description: Server Address: Description: Server Address: Description:	STALL ZYWA SEdit LDAP			? ×
With LOAP Server Address: Bord Dir: Percention Server Address: Bord Dir: Percention Server Address: Bord Dir: Percention Server Address: Dir Dir: Percention Dir Dir: Dir Dir: Percention Dir: <	CONFIGURATION General Settings			
With the limit General With the limit Sever Address: With the limit Sever Address: </th <th>T¥Quick St Name:</th> <th>thomas_ldap</th> <th></th> <th></th>	T¥Quick St Name:	thomas_ldap		
I change of the later is a change of the data is a	+ DDNS Description: + NAT		Optional	
Image: State Sta	HTTP Redirect Server Settings			
<pre>************************************</pre>	ALG IP/MAC Binding Server Address:	10.100.100.50	(IP or FQDN)	
With and Strate Login Name Attribute: With and Strate Login Name Attribute: Search time Init: S Search time Init:	Auth. Policy Backup Server Address:		(IP or FQDN)Optional	tyxel,dc=com,dc=tw
· · · · · · · · · · · · · · · · · · ·	VPN Port:	389	(1-65535)	Displaying 1 - 2 of 2
Server Address: 10.100.100.50 (P or FQ0) Back D Server Address: 5 (1.300 seconds) Breadon Serv	IPSec VPN Base DN:	ou=cso,dc=rdb,dc=zyx		
Serd the left: 1:0:00 seconds) Serd the left: 1:0:00 seconds) Serd the left: 1:0:00 seconds) Server Address: 10:00.00.50 (P or FQN) Server Address: 10:00.00.50 (P or FQN) Backup Server Address: 10:00.00.50 (P or FQN) Pot: 399 Server Address: 1:0:00.00.50 (P or FQN) Pot: 399 Server Address: 1:0:00.00.50 (P or FQN) Pot: 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:	L2TP VPN Use SSL			
Image: Second Secon	App Patrol Search time limit:	5	(1-300 seconds)	
State Class ind Dit: immanger.dc=rdb.dc ind Dit: immanger.dc=rdb.dc immanger.dc=rdb.dc ind Dit: <td< th=""><th>Device HA</th><th></th><th></th><th></th></td<>	Device HA			
Person: ····································	Object Bind DN:	cn=manager,dc=rdb,dc		
· Ver Address: 10:100.100.59 (P or FQDN) · Ver Address: 00:000.000.59 (P or FQDN) · Ver Address:	+ Address Password:			
wide weak	+ Service			
· Order Automatic Login Hame Attribute: · Order Automatic Login Hame Attribute: · Order Automatic Control · Order Automatic Con	AAA Server			-
attender Login Name Attribute: Option attender Login Name Attribute: ID 100.100.50 Backup Server Address: ID 100.100.50 Port: 389 Backup Server Address: ID 100.100.50 Port: 389 Backup Server Address: ID 100.100.50 Port: 389 Base DN: ou=coso,dc=rdb,dc=zyx Voree: Image: dc=rdb,dc=zyx Search time limit: 5 rever Authentication Image: dc=rdb,dc Bind DN: memanager,dc=rdb,dc Parenative Login Name Attribute: ou Atternative Login Name Attribute: ou Option ou Atternative Login Name Attribute: ou Outomembership Attribute: ou Origin Name Attribute: ou Infiguration Validation Thomas Place enter a user account existed in the configured server to validate above settings. Bind user in ou use in ou exist in the configured server to validate above settings. Uservername: Thomas Test	Auth. Method Login Name Attribute: Certificate	uid		
image: content of the configured server to validate above settings. Search time limit: Conter limit Orgon Name Attribute: udd Option Add user find use find u	ISP Accounts	ttribute:	Optional	
www.meanseries the LADP Server Address: addup Server Address: backup Server Server to validate above settings. Jerver Address: backup Server Address: backup Server Address: backup Server Server to validate above settings. Jerver Address: backup Server Address: backup Server Server to validate above settings. Jerver Address: backup Server Server to validate above settings. Jerver Address: backup Server Server Server to validate above settings. Jerver Address: backup Server Ser	SSL Application Fortpoint Security			
dit LDAP Server Address: 10.100.100.50 Backup Server Address: 0 Backup Server Address: 0 Port: 389 (1-55537 Base DN: ou=cso,dc=rdb,dc=zyx Bind DN: memanager,dc=rdb,dc=zyx Base DN: ou=cso,dc=rdb,dc=zyx Bind DN: memanager,dc=rdb,dc=zyx Bind DN: Bind DN: memanager,dc=rdb,dc ou=con,dc=rdb,dc Bind DN: Group Membership Attribute: ou Group Membership Attribute: ou ou Brease enter	System		OK Can	
dit LDAP Server Address: 10.100.100.50 (IP or FQDN)Optimal Base DN: med例為限定 Port: 339 (1-65535) Base DN: ou=coo,dc=rdb,dc=ryx Base DN: ou=coo,dc=rdb,dc=ryx Search time limit: 5 (1-300 seconds) Bind DN: on=manager,dc=rdb,dc Password: ou=coo,dc=rdb,dc Search time limit: 1 Search time limit: 5 Search time limit: 1 Search time limit: 1 Search time limit: 1 Search time limit: 1 Search time limit: <td< th=""><th>🛛 Log & Report</th><th></th><th></th><th></th></td<>	🛛 Log & Report			
Edit LDAP Server Address: 10.100.100.50 (IP or FQDN) Badup Server Address: (IP or FQDN)Optional 域做驗証,範例爲限定 Port: 389 (1-65533 Base DN: 用來識別該跟那/ 域做驗証,範例爲限定 rdb.zyxel.com.tw 中的 CSC 個群組的人才可連線 Search time limit: 5 (1-300 seconds) Search time limit: 5 (1-300 seconds) Search time limit: 5 (1-300 seconds) Server Authentication Bind DN: memanager,dc=rdb,dc Bind DN: on=manager,dc=rdb,dc Password: User Login Settings uid Optional Login Name Attribute: ou Optional Group Membership Attribute: ou Optional Group Membership Attribute: ou Group Name) Bj應 add user 的 use 的 ext-group-user 的 Group Identifier : CSO ot			_	
Edit LDAP Server Address: Data Port: 339 (1-55535) Base DN: Ources Base DN: Ources Server Address: Ort: Base DN: Ources Server Authentication Bind DN: Password: User Login Settings Login Name Attribute: Juid Option Group Membership Attribute: Our Option Please enter a user account existed in the configured server to validate above settings. Username: Thomas Or Configuration Validation Please enter a user account existed in the configured server to validate above settings. Username: Thomas Test			/	
Server Address: 10.100.100.50 (fr or FQDN) (pr or FQDN) Badup Server Address: (fr or FQDN) (pr or FQDN) (pr or FQDN) Port: 389 (1-55533) Base DN: ou=cso,dc=rdb,dc=zyx Server Authentication (fr or FQDN) (pr or FQDN) (pr or FQDN) Bind DN: ou=cso,dc=rdb,dc=zyx Server Authentication (fr or FQDN) (pr or FQDN) (pr or FQDN) Bind DN: ou=cso,dc=rdb,dc=zyx Bind DN: cn=manager,dc=rdb,dc Password: ou=cso,dc=rdb,dc User Login Settings Group Membership Attribute: Login Name Attribute: ou Optional Group Membership Attribute: Optional Group Name) Server authentibute: ou Login Name Attribute: ou Configuration Validation Please enter a user account existed in the configured server to validate above settings. Username: Thomas Thomas Test	Edit LDAP			Dase DN:用來識別該戚那個網
Badup Server Address: (P or PQDN)Optimal Port: 389 Base DN: ou=cso,dc=rdb,dc=zyxl Search time limit: 5 Server Authentication (1-300 seconds) Bind DN: cn=manager,dc=rdb,dc Password: ou=cso,dc=rdb,dc User Login Settings Group Membership Attribute: Login Name Attribute: ou Configuration Validation Please enter a user account existed in the configured server to validate above settings. Username: Thomas Thomas Test	Server Address:	10.100.100.50 (IP	P or FQDN)	试做驗証, 節例 個 電 限 完
Port: 389 (1-65535) Base DN: ou=cso,dc=rdb,dc=zyx Search time limit: 5 (1-300 seconds) Search time limit: 5 (1-300 seconds) Bind DN: cn=manager,dc=rdb,dc Bind DN: 需有該網域設定体 Password: ou=cso,dc=rdb,dc Ou=cso,dc=rdb,dc User Login Settings cn=manager,dc=rdb,dc Bind DN: 需有該網域設定体 Login Name Attribute: uid Optional Group Membership Attribute; Login Name Attribute: uid Optional Group Membership Attribute; Configuration Validation Please enter a user account existed in the configured server to validate above settings. Bind Duse mode Username: Thomas Test Mile	Backup Server Address:	(IP	or FQDN)Optional	
Base DN: ou=cso.dc=rdb,dc=zyx Search time limit: 5 Search time limit: 6 Search time limit: 0 Jage Login Search time limit: 0 Login Name Attribute: 0 Optional Group Membership Attribute: Group Membership Attribute: 0 Search time account existed in the configured server to validate above settings. Username: Thomas Test	Port:	389 (1-	-65535	rdb.zyxel.com.tw 中的 CSO 這
base Unit Unit Unit Unit Unit Unit Unit Unit	Race DNr		/	
Search time limit: 5 (1-300 seconds) Bind DN: Image: descended of the second of the sec		ou=cso,uc=rub,uc=zyx		個群組的人才可連線
Search time limit: s (1-300 seconds) Bind DN: cn=manager,dc=rdb,dc Bind DN:需有該網域設定体的人,才能做連線查詢授体的人,非能做連線查詢授体的人,非能做理能做自動的和Laternative Login Name Attribute: Group Membership Attribute: Group Name) Soutput of the configured server to validate above settings. Username) Soutput of the configured server to validate above settings. Soutput of the configured server to validate above settings. Username: Thomas Test	Use 66L		L	
erver Authentication Bind DN: 需有該網域設定体 的人,才能做連線査詢授体 的人,才能做連線査詢授体 的人,才能做連線査詢授体 的人,才能做連線査詢授体 的人,才能做連線査詢授体 的人,才能做連線查詢授体 的人。才能做連線查詢授体 的人。才能做連線查詢授体 的人。非能做連線查詢授体 的人。非能做連線查 動 な な な な な な な な な な な な な な な な な な	Search time limit:	5 (1-	-300 seconds)	
erver Authentication Bind DN: Password: Username: Contemporation Validation Please enter a user account existed in the configured server to validate above settings. Username: Configured to rest Concel Conce Concel Concel Concel Concel Concel Conc				Bind DN:需有該網域設定權限
Bind DN:	erver Authentication			
Password:	Bind DN:	cn=manager,dc=rdb,dc		的人,才能做連線查詢授權
er Login Settings Login Name Attribute: uid Optional Group Membership Attribute Atternative Login Name Attribute: ou Group Name Attribute: ou Group Name) Infiguration Validation Please enter a user account existed in the configured server to validate above settings. Jsername: Thomas Test OK Cancel	Password:			
er Login Settings ogin Name Attribute: Wternative Login Name Attribute: aroup Membership Attribute: ou figuration Validation Mease enter a user account existed in the configured server to validate above settings. Jsername: Thomas Test Group Membership Attribute Group Name) 對應 add user 的 use 的 ext-group-user 的 Group Identifier : CSO OK Cancel			Г	
Login Name Attribute: Alternative Login Name Attribute: Group Membership Attribute: ou onfiguration Validation Please enter a user account existed in the configured server to validate above settings. Username: Thomas Test OK Cancel	er Login Settings			Group Membership Attribute
Alternative Login Name Attribute: Alternative Login Name Attribute: Group Membership Attribute: au Optional Group Membership Attribute: au Optional Group Membership Attribute: Defiguration Validation Please enter a user account existed in the configured server to validate above settings. Username: Thomas Test	Login Name Attribute:	uid		Group Memoership Autoute
Alternative Login Name Attribute: Optional Group Membership Attribute: Ou Group Membership Attribute: Ou Group Name) 對應 add user 的 use 的 ext-group-user 的 Group Identifier:CSO OK Cancel	Login Name Attribute.	uiu		爲 OU(範例使用的 OU 為
Group Membership Attribute: ou Infiguration Validation Group Name) Sername: Thomas Thomas Test OK Cancel	Alternative Login Name Attribute:	Op	otional	
nfiguration Validation Please enter a user account existed in the configured server to validate above settings. Jsername: Thomas Test III OK Cancel	Group Membership Attribute:	ou /		Group Name)
nfiguration Validation Please enter a user account existed in the configured server to validate above settings. Username: Thomas Test UM OK Cancel				
Please enter a user account existed in the configured server to validate above settings. Username: Thomas Test ext-group-user 的 Group Identifier:CSO OK Cancel	onfiguration Validation			對應 add user 的 use 的
Username: Thomas Test CSO Identifier : CSO	Please enter a user account existed in the	e configured server to validate a	above settings.	avt group user the Group
Identifier : CSO	Username:	Thomas	Test	ext-group-user by Group
		L		Identifier : CSO
OK Cancel				
			ОК	Cancel

步驟三:手動建立新的驗證規則,輸入 LDAP 相關資訊,名稱為 thomas_LDAP

步驟四:確認建立 LDAP 驗證規則為成功。

Z	YXEL ZYWALL U	USG 100	Welcome admin <u>Loqout</u>	? Help Z About 🛊 Site Map (⊒Object Reference 🖵 Console 🥳) CLI
1	CONFIGURATION	Active Directory LDAP R	RADIUS		
	↑ Auth. Policy • Firewall	LDAP Server Summary	Ohiert Reference		
	VPN IPSec VPN SSL VPN	# Name 1 Idap	Server Address	Base DN	
	L2TP VPN App Patrol Anti-X	2 thomas_ldap	10.100.100.50	ou=cso,dc=rdb,dc=zyxel,dc=com,dc=tw Displaying 1 - 2 of 2	
	 Anti-Virus IDP ADP Content Filter 				
	 Anti-Spam Device HA Object 				
	 User/Group Address Service 				
	Schedule AAA Server				

設定登入帳號的驗証方式,在USG 提供使用者登入的驗證方式有四種:

- 1. USG 設備中的建立的使用者帳號
- 2. 與網路中的 AD 伺服器進行驗證
- 3. 與網路中的 LDAP 伺服器進行驗證
- 4. 與網路中的 RADIUS 伺服器進行驗證

步驟五:若在 AAA server 是自己手動建的規則,非修改原本預設 ldap 規格名稱, 則需手動建立一個新使用者,點選❶Configuration→❷點選 Object(物 件)→ ❸點選 User/Group→④點選 User→ ⑤點選 Add

Z	YXEL ZYWALL	Welcome admin	? Help 🛛 About 🌴 Site Map 🕞 Object Reference 🖵 Console 🗔 CLI
	CONFIGURATION	User Group Setting	
	CONFIGURATION Configuration Firewall VPN App Patrol Anti-X Anti-Virus IDP ADP Content Filter Anti-Spam Device HA Object User/sforup Address Service Schedule AAA Server Auth. Method Certificate Sisp Account	User Group Setting Configuration Add Fedt Remove Configuration 4 admin 2 Idap-users 3 radius-users 4 ad-users 4 ad-users 1 of 1 M	Ject Reference
	SSL Application SSL Application Endpoint Security System Log & Report		

步驟六:手動建立一個新使用者(User Name 僅用於識別該群組作用),此使用 者用於與 AAA Server 中 LDAP 驗證查詢的資料庫使用,User type 需選 ext-group-user, Associated AAA Server Object 需套用在 AAA Server-LDAP 手動建立規則的名稱(此範例 thomas_ldap), Group Identifer 的值需對應 AAA server 的 Base DN 的值 及 Group Membership Attribute 使用的識別(object Attribute)再按下 ok 鈕

Z	XEL ZYWAL			min Leoold 🤍 Help Z About 🗍 Site Map 🔂 Object Reference 🖵 Console 🖾 C
	CONFIGURATION	User Group Setting		The set of the set
	Quick Set	up Configuration		
		Edit User letsCSO		? 🗙
Č¢.		User Configuration		
		User Name:	letsCSO	
		Liser Type:	evt-group-user	
	VPN PSec VPN	Group Identifier:	CSO	
		Associated AAA Server Object:	thomas_Idap	
		Description:	thomas_Idap	Displaying 1 - 5 of 5
		Configuration Validation		
	 Object User/Group Address 	Please enter a user account existed in User Name:	the configured group to validate abo	ove settings. Test
				OK Cancel



Group identifier 需對應 AAA server 的 Base DN 的值 及 Group Membership Attribute 使 用的識別(object)。

此範例我們在 LDAP server 上 group 有 sales and cso,但在 USG 系列 AAA server 的 LDAP 的 Base DN 是 ou=cso, Group Membership Attribute 所輸入為 OU,故此 Group Identifier 需輸入的 CSO。 步驟七:確認所建立的使用者。

ZyXEL ZYWALL	Welcome admin USG 100	PHelp Z About 🕈 Site Map 🔤 Object Reference 🖵 Console 💽
CONFIGURATION	User Group Setting	
T¥Quick Setup → Firewall ♥ VPN	Configuration	Ohiert Reference
◆ App Patrol ⊡ Anti-X	# A User Name	Description
Anti-Virus IDP	1 admin 2 Idap-users	Administration account External LDAP Users
 → ADP → Content Filter 	3 radius-users	External RADIUS Users
 → Anti-Spam → Device HA 	4 ad-users 5 letsCSO	External AD Users Local User
 Object User/Group Address Service Schedule AAA Server Auth. Method Certificate ISP Account SSL Application Endpoint Security System Log & Report 	. If f Page 1 of 1 ▶	Show 50 vitems Displaying 1 - 5 of 5

步驟八:點選●Configuration→❷點選 Object(物件)→ ❸點選 Auth. Methood→④ 點選 default 此筆 → 爭點選 edit 此筆進行編輯。

Welcome admin <u>Locout</u> ?Help Z About ₹ Site Map @Object Reference ♥ Console [] CLI JSG 100
Authentication Method
Configuration Object Reference Image: Configuration Image: Configuration Image: Configuration

SSL VPN 設定



SSL VPN 為讓出差在外的使用者從遠端,透過網際網路使用安全的加密方式來 存取內部資源,在無需安裝額外特定程式,使用瀏覽器即可連入 USG 並進行帳 號驗證。

步驟九:USG VPN 的 SSL 的 VPN 規則設定,新增一筆 SSL 的規則,請點選 ●Configuration→@點選 VPN→ 圖點選 SSL VPN→④點選 Add

Z	YXEL ZYWALL	Welcome adm	in] 20051 ?Help Z About 🛊	Site Map 📮 Object Reference 🖵 Console 💽 CLI
	CONFIGURATION	Access Privilege Global Se	etting	and the second second
	Quick Setup NAT HTTP Dedirect	Access Policy Summary		
٩	ALG IP/MAC Binding	Add Edit Remove	G Activate G Inactivate ↓ Mov User/Group	Access Policy Summary
E.	Auth. Policy Firewall VPN	↓ Page 1 of 1	Show 50 🗸 items	Displaying 1 - 1 of 1
	IPSec VPN SSL VPN L2TP VPN Ass Patral			
	App Pauloi Anti-X Device HA			
	User/Group Address Social			
	Schedule AAA Server			
	Certificate ISP Account			
	SSL Application Endpoint Security		Apply Reset	

步驟十:建立 SSL 存取的規則名稱,建議易於識別如:AAA_user_access (此範例:暫將規則名稱為 test)

若用的是 AAA Server default 規則設定的,請將 ldap-users 群組加入到右列清單, 此範例為自己建立 AAA Server 中的 LDAP 驗証規則,故需選取己套用自己建立 與 LDAP 規則驗証的使用者名稱(此範例: lets-CSO)

請將 lets-CSO 加入到右列清單,並於 Network extension 配置 SSL 登入的使用 者網段 IP 及 SSL 登入可存取的網路資源。



步驟十一:點選●Configuration→❷點選 Network→ ❸點選 Zone→點選 SSL_VPN 中確認是否有加入的 VPN→SSL VPN 新增一筆 SSL 的規 則名稱(此範例為 test)

XEL THALL	1160 100				
YALL ZYWALL	056 100				
CONFIGURATION	Zone				
V Quick Setup	User Configuration				
Licensing		Remove ne Object P	eference		
+ Interface	That P Lat	Name	Plack latra zano	Mambar	
+ Routing + Zone		Name	DIOCK IIII a-2016	member	
DDNE	4 4 Page 1	of 1 ▶ ▶∥ Sh	ow 50 🔻 items		No data to display
 NAT HTTP Redirect 	System Default				
+ ALG					
Auth. Policy		Name	Block Intra zone	Nambar	
Firewall	1	LAN1	no	lan1	
VPN VPN VPSec VPN	2	LAN2	no	lan2	
+ SSL VPN	3	WLAN	no	ext-wlan,wlan-1-1	
+ L2TP VPN + App Patrol	B 4	WAN	yes	wan1,wan2,wan1_ppp,wa	n2_ppp,aux
⊕ Anti-X	6	SSL_VPN	yes	test	
Device HA Device HA	7	IPSec_VPN	yes 🔨	test_p2	
⊕ System	4 4 Page 1	of 1 🕨 🕅 Sh	ow 50 🗸 items	\backslash	Displaying 1 - 7 of 7
O Add Zone					? ×
O Add Zone					? ×
O Add Zone Group Member	rs				? ×
Add Zone Group Member Name:	rs	SSL_VPN			? ×
Add Zone Group Member Name:	rs	SSL_VPN	 指的 SSL VP	N的規則名稱	? (X)
Add Zone Group Member Name: Block Intra	rs -zone Traffic 👔	SSL_VPN	指的 SSL VP	N的規則名稱	? ×
Add Zone Group Member Name: Block Intra Member List	rs -zone Traffic 👔	SSL_VPN	指的 SSL VP	N的規則名稱	?×
Add Zone Group Member Name: Block Intra Member List Available	rs -zone Traffic 👔	SSL_VPN	指的 SSL VP	N的規則名稱	? ×
Add Zone Group Member Name: Block Intra Member List Available	rs -zone Traffic 👔	SSL_VPN	指的 SSL VP	N 的規則名稱	? (X)
Add Zone Group Member Name: Block Intra Member List Available ==: Default LZTP	rs -zone Traffic (1)	SSL_VPN	指的 SSL VP	N 的規則名稱 L VPN ===	? ×
Add Zone Group Member Name: Block Intra Member List Available === Default_L2TP_N	rs -zone Traffic (1) = VPN Tunnel === PN_Connection	SSL_VPN	指的 SSL VP	N 的規則名稱 L VPN ===	? ×
Add Zone Group Member Name: Block Intra Member List Available ==: Default_L2TP_N	rs -zone Traffic i = VPN Tunnel = = = PN_Connection	SSL_VPN	指的 SSL VP	N 的規則名稱 LVPN===	?×
Add Zone Group Member Name: Block Intra Member List Available ==: Default_L2TP_N	rs -zone Traffic 👔 = VPN Tunnel = = = /PN_Connection	SSL_VPN	指的 SSL VP	N 的規則名稱 L VPN ===	?
Add Zone Group Member Name: Block Intra Member List Available ==: Default_L2TP_N	rs -zone Traffic 1 = VPN Tunnel = = = (PN_Connection	SSL_VPN €	指的 SSL VP	N 的規則名稱 LVPN===	? ×
Add Zone Group Member Name: Block Intra Member List Available === Default_L2TP_V	rs -zone Traffic (1) = VPN Tunnel === /PN_Connection	SSL_VPN €	指的 SSL VP	N 的規則名稱 L VPN ===	? ×
Add Zone Group Member Name: Block Intra Member List Available ==: Default_L2TP_N	rs -zone Traffic 👔	SSL_VPN	指的 SSL VP	N 的規則名稱	
Add Zone Group Member Name: Block Intra Member List Available ==: Default_L2TP_N	rs	SSL_VPN €	指的 SSL VP	N 的規則名稱 LVPN ===	
Add Zone Group Member Name: Block Intra Member List Available === Default_L2TP_M	rs -zone Traffic 1 = VPN Tunnel === (PN_Connection	SSL_VPN €	指的 SSL VP	N 的規則名稱	
Add Zone Group Member Name: Block Intra Member List Available === Default_L2TP_N	rs	SSL_VPN	指的 SSL VP	N 的規則名稱	
Add Zone Group Member Name: Block Intra Member List Available ==: Default_L2TP_N	rs -zone Traffic 👔	SSL_VPN €	指的 SSL VP	N 的規則名稱	

步驟十二:驗証設定是否正確,使用登入帳號為 AD Server 上的帳號,輸入使用者帳號及密碼並點選 SSL 登入。



步驟十三:在登入後 SSL,需安裝 Active x 並請允許執行 JRE(jave runtime 環境)。



步驟十四:請安裝附加元件。

🚖 我的最愛	🏉 .:: Welcome to Portal::.	🚹 • 🗟 · 🗆 🖶 • 網頁② • 安全性③ • 工具◎ • ⑧ •
這個網站想要要安裝,請招	要安裝下列附加元件:來自 ZyXEL Communications C 安這裡	Corporation'的 2 為這部電腦上所有的使用者安裝此附加元件(<u>d</u>) 1 ¹¹ ,而且想 ×
Z	vXEL	
		Application File Sharing
		English
	File Sharing	
	Welcome	X
	Welcome to SSL VPN	
n.	You might need to click the yellow warr installation. If you can not install ActiveX	rning bar at the top of the browser window to show the X object, please contact with administrator.
	Note: Click the information bar and	choose Install ActiveX Control to allow installation to
	proceed, of it will try to full with th	
T		
		······································
		+
Internet	Explorer - 安全性警告	<u> </u>
是否要	安裝這個軟體?	
	名稱: ZwWALL SecuEv	dender ActiveX
	發行者: Zy¥EL Comm	nnications Corporation
	STITE. DYALD COMM	
≥更	多選項(0)	安裝① 不要安裝①
	雖然來白網際網路的檔案可	「能是有用的,但是這個檔案類型有可能會傷
9	害您的電腦。諸只安裝來自	您所信任發行者的軟體。有什麼樣的風險?"
	. SecuExtender Setun	
16 0) 1100		
7.0	Welcome to	o the ZvWALL
Zy	SecuExtend	der Setup Wizard
	The Setup Wizard will in	install ZVWALL SecuExtender on your
	computer. Click "Next" Setup Wizard.	"to continue or "Cancel" to exit the
1		
		按下 Next 進行安裝
	< Barl	ck Next > Cancel

🛃 ZyWALL SecuExtender Setup	
Select Installation Folder	ZvXEL
This is the folder where ZyWALL SecuExtender will be installed	
To install in this folder, click "Next". To install to a different fold "Browse".	der, enter it below 下 Browse 來變更路徑。
Eolder: C:\Program Files\ZyXEL\ZyWALL SecuExtender\	Browse
Advanced Installer	Next > Cancel
id Zy₩ALL SecuExtender Setup	×
Ready to Install	7.YEI
The Setup Wizard is ready to begin the ZyWALL SecuExtende	r installation
Click "Install" to begin the installation. If you want to review installation settings, click "Back". Click "Cancel" to exit the wiz	or change any of your ard.
	按下 Install 開始進行安裝。
Advanced Installer	Install Cancel
13 Zywall Seculatender Serup	
ZyXEL Completing the Zy SecuExtender Setu	/WALL up Wizard
Click the "Finish" button to exit the S	5etup Wizard.
	按下 Finish 完成安裝並關閉此視窗。
< Back Ein	Cancel

在電腦工作列上即可看到您取得的 IP 位置

Z	ZyWALL SecuExtend	ler Status		×	
	Connection Status				
	SecuExtender IP Addr	ess:	9.9.9.9		
	DNS Server 1:		0.0.0.0		
	DNS Server 2:		0.0.0.0		
	WINS Server 1:		0.0.0.0		
	WINS Server 2:		0.0.0.0		
	Network 1:	10.100.100	.0/255.255.255.0		
	Network 2:		Not configured		
	Network 3:		Not configured		
	Network 4:		Not configured		
Activity					
	Connection Time	00:00:03			
	Transmitted	490 Bytes	5 Packet:	s	
	Received	0 Bytes	0 Packet:	s	