ZyWALL SSL 10

Integrated SSL-VPN Appliance



<u>Revision 1.0</u> <u>Dec. 2006</u>



INDEX

1. Deployment		4
1.1 DMZ Z	one	4
1.1.1	Deploy ZYWALL SSL 10 in DMZ zone	4
1.2 NAT M	ode	. 20
1.2.1	Deploy ZYWALL SSL 10 at the gateway	. 20
2. Integrated Ap	plication	. 29
2.1 Externa	l Authentication	. 30
2.1.1 I	External Authentication configuration	. 30
2.1.2	User/Group configuration	. 31
2.2 Objects	Configuration	. 33
2.2.1	SSL Application Object	. 33
2.2.2	VPN Network Object	. 37
2.2.3	Endpoint Security Object	. 38
2.2.4	Private IP Pool Object	. 42
2.3 SSL Po	licy Configuration	. 43
3. SSL VPN Sol	ution	.47
3.1 UTM II	ntegration: ZyWALL UTM+ZyWALL SSL10	.47
3.2 Seamle	ss Integrate SSL VPN into your existing IPSec VPN	. 52
4. Best Practice:	Stronger Password Security	. 64
4.1 Using T	Wo-factor authentication solution to provide stronger (FIPS 140 compliant	.)
security: SS	SL10+Authenex	. 64
5. FAQ		. 72
A. ZyWAL	L General FAQ	. 72
A01. I	How to access ZyWALL SSL10 web GUI?	. 72
A02. V	What do I need to use the ZyWALL?	. 72
A03. V	What is PPPoE?	. 72
A05. I	Does the ZyWALL support PPPoE?	.73
A06. I	How do I know I am using PPPoE?	. 73
A07. V	Why does my Internet Service Provider use PPPoE?	. 73
A08. I	How can I configure the ZyWALL?	. 73
A09. V	What can we do with ZyWALL?	.74
A10. I	Does ZyWALL support dynamic IP addressing?	.74
A11. V	What is the difference between the internal IP and the real IP from my ISP?	2.74
A12. I	How does e-mail work through the ZyWALL?	.74
	2	

A13. What DHCP capability does the ZyWALL support?	75
A14. How do I used the reset button, more over what field of parameter will be	
reset by reset button?	75
A15. My ZyWALL can not get an IP address from the ISP to connect to the	
Internet, what can I do?	75
A16. What is BOOTP/DHCP?	76
B. Firmware Upgrade FAQ	77
B01. How to perform the firmware upgrade on ZyWALL SSL10?	77
C. Registration for Service Activation FAQ	77
C01. Why do I have to register?	77
C02. In addition to registration, what can I do with myZyXEL.com?	77
C03. How to activate the SSL-VPN license?	78
D. SSL VPN FAQ	78
D01. Matrix table for the SSL VPN terms	78
D02. Why cannot some web pages displayed correctly?	78
D03. SSL VPN vs. PPTP VPN?	79
D04. What is the order of user authentication?	79
E. EPC(End Point Check) FAQ	79
E1. What is EPC on ZyWALL SSL10?	79
E2. What are the checking items of EPC on ZyWALL SSL 10?	80

1. Deployment

SSL topology encapsulates the sensitive data in SSL protocol to secure the communication between SSL client and SSL server via several encryption, authentication, and secret exchange method. ZyWALL SSL 10 which acts as a SSL server and easily to integrate with the existed firewall (ex. ZyWALL or 3rd party firewall) to provide SSL VPN solution. Depending on your current network topology, we have two suggestions for the deployment of ZYWALL SSL 10.

1.1 DMZ Zone

1.1.1 Deploy ZYWALL SSL 10 in DMZ zone

To deploy the ZYWALL SSL 10 to a network environment, people may ask where is the suggestion to put the device in the existing network. If the environment matches the following two criteria, put the SSL10 in DMZ zone is recommended.

- Customers who already installed a ZyWALL or a third party's firewall, like SonicWALL TZ170 or Juniper 5GT
- ZyWALL UTM or the third party's firewall provides security inspection such as Anti-Virus/IDP/firewall.

See following figure to show you the topology for example.



The network topology above is used to illustrate this application. We used one ZyWALL as main office's gateway which is connected to the branch office's ZyWALL. The ZyWALL SSL 10 is put behind main office's gateway at DMZ zone. Remote users could either access the main office's LAN resource or access the remote office's LAN resource via IPSec VPN tunnel after user pass the SSL authentication.

Since the SSL VPN traffic will be decrypted by ZyWALL SSL 10, the traffic could be further inspected by ZyWALL UTM or third party firewall which has security checking features like firewall, Anti-Virus, IDP and etc. In this way, MIS administrator will take it easy to eliminate the worry that remote "trust" PC may distribute virus or attacks to internal network.



Configuration information in this example:

ZyWALL UTM	ZyWALL SSL 10
WAN Address: 172.120.1.10	WAN Address: 192.168.3.2
DMZ Address: 192.168.3.1	VPN Network: 192.168.1.0/24
LAN Address: 192.168.1.1	Remote Users IP Address Pool:
	192.168.1.200 ~ 192.168.1.250

To achieve this, we have to complete the following tasks:

- Check ZyWALL UTM or 3rd party Firewall's setting matching the example.
- On ZyWALL SSL 10, using Wizard to setup the initial SSL VPN access network.

See the following step-by-step configuration.

Configuration on ZyWALL UTM

Two tasks:

- Configure the proper IP address for WAN, LAN, DMZ interfaces.
- Configure port 443 forwarding to ZyWALL SSL10 for SSL traffic.

Step1. Check if the WAN, LAN, DMZ IP address has been proper configured.

1) Go to the GUI > Network > DMZ, configure the DMZ IP address as 192.168.3.1.

DMZ	Static DHCP	IP Alias	Port Poles		
D.IL	Static Brief		TOTCHOICS		
DMZ TCP/IP					
IP Address		192 . 168 . 3	. 1	RIP Direction	Both 💌
IP Subnet f	1ask	255 . 255 . 255	. 0	RIP Version	RIP-1 💌
Multicast		None 🗾			
DHCP Setup					
DHCP		None 🔻			
IP Pool Sta	rting Address	0.0.0	. 0	Pool Size	128
DHCP Serv	er Address	0.0.0	0		
DHCP WIN:	S Server 1	0.0.0	. 0		
DHCP WIN:	S Server 2	0,0,0	0		
Windows Ne	tworking (NetBIO	S over TCP/IP)			
	etween DMZ and LA	N			
	etween DMZ and Wi	4N12			
	etween DMZ and WI	AN			
Note: You a	ilso need to create a	Firewall rule.			
		0 mmbrs			

2) Go to the GUI > Network > DMZ > Port Roles, define the port 4 belongs to DMZ zone.

DMZ				
	DMZ	Static DHCP	IP Alias	Port Roles
	Port Roles Se	tup		
		2yWALL 35		
			Apply	Reset

3) Go to the GUI > Network > WAN > WAN1, configure the WAN IP address as a proper one(ex. 172.120.1.10 in this example).

General	WAN 1	WAN 2	Traffic Redirect	Dial Backup	
ISP Parame	ters for Internet Acc	ess			
Encapsulat	ion	Ethernet			
Service Ty	pe	Standard			
WAN IP Add	ress Assignment				
🖲 Get Au	tomatically from ISP				
🔘 Use Fix	ed IP Address				
My Wa	AN IP Address		0.0.0	. 0	
My W/	AN IP Subnet Mask		0.0.0	. 0	
Gatew	av IP Address		0.0.0	. 0	
Advanced S	etup				
🔽 Enable	NAT (Network Address	Translation)			
RIP Directi	on		None		
RIP Versio	ר		RIP-1 🔽		
RIP Versio	ר		RIP-1		
RIP Version	n Multicast		RIP-1		
RIP Version Enable Multica:	n Multicast st Version		IGMP-v1		
RIP Version Enable Multica:	n Multicast st Version WAN MAC Address from	LAN	RIP-1		
RIP Version Enable Multica: Spoof Clone t	n Multicast st Version WAN MAC Address from be computer's MAC add	1 LAN	RIP-1 ▼ IGMP-v1 ▼	34	
RIP Version Enable Multica: Spoof Clone t	n Multicast st Version WAN MAC Address from he computer's MAC add) LAN Iress - IP Address	RIP-1 ▼ IGMP-v1 ▼	. 34	
RIP Version Enable Multica: Spoof Clone t	n Multicast st Version WAN MAC Address from he computer's MAC add) LAN Iress - IP Address	RIP-1 _	. 34	

4) Go to the GUI > Network > LAN, configure the LAN IP address as 192.168.1.1.

		Davit Dalas		
LAN Static DHLP	IP Allas	Port Roles		
LAN TCP/IP				
IP Address	192 . 168 . 1 .	1	RIP Direction	Both
IP Subnet Mask	255 . 255 . 255 .	0	RIP Version	RIP-1
Multicast	None 💌			
DHCP Setup				
DHCP	Server 💌			
IP Pool Starting Address	192 . 168 . 1 .	33	Pool Size	128
DHCP Server Address	0.0.0.	0		
DHCP WINS Server 1	0.0.0.	0		
DHCP WINS Server 2	0.0.0.	0		
For DNS setup please click he	ere .			
Wiedems bletwenkies (bletBt				
WINDOWS NELWORKING (NELBI	US OVER TCP/IP)			
Allow between LAN and V	VAN1			
Allow between LAN and V	VAN2			
🗌 🗌 Allow between LAN and D	MZ			
Allow between LAN and V	VLAN			
Note: You also need to create	e a <u>Firewall</u> rule.			
	Apply	Res	et	

Step2. Check if the Internet access is available on both LAN and DMZ network by ping from a LAN host and a DMZ host.

Step3. Check if UTM functions (ex. Firewall, Anti-Virus, and IDP) are enabled and without blocking the SSL traffic from WAN to DMZ.

Step4. Setup the port forwarding for SSL traffic.

 Go to the GUI > ADVANCED > NAT > Port Forwarding, add one rule to forward port 443 traffic to the ZyWALL SSL 10 (192.168.3.2)

NAT Over	view	Address M	apping	Port Forwardin	g Port Tri	ggering						
Port	Forwa	arding Rules										
WA	AN Inte	rface		WAN 1 💌								
De	fault S	erver		0.0.	0.0		Go	To P	age	1 💌		
#	Active	Name	Inco	mina Port(s)	Port	Translation	S	erve	r IP	Add	ress	
		SSL10	443	- 443	443	- 443	192	. 16	;8.	3		2
2	Г		0	- 0	0	- 0	0	. 0		0	•	0
3			0	- 0	0	- 0	0	. 0	ı.	0	•	0
4			0	- 0	0	- 0	0	. 0	ı.	0		0
5			0	- 0	0	- 0	0	. 0	ı.	0		0
6			0	- 0	0	- 0	0	. 0		0		0
7			0	- 0	0	- 0	0	. 0	ı.	0	•	0
8			0	- 0	0	- 0	0	. 0	ı.	0	•	0
9			0	- 0	0	- 0	0	. 0	ι.	0		0
10			0	- 0	0	- 0	0	. 0	ı.	0	•	0
No No	te 1: Yi te 2: Pi	ou may also n ort Translatior	eed to cr i is optior	eate a <u>Firewall</u> rul al.	e.							
				- Annta		Dent						

Step5. Go to the GUI > ADVANCED > REMOTE MGMT > WWW, change the ZyWALL UTM's HTTPS management port number from port 443 to another port number(ex. 8443). This is to make sure all HTTPS traffic via port 443 will be forwarded to ZyWALL SSL 10. But if IT staff needs to access the ZyWALL UTM by HTTPS, they can use <u>https://IP_address:8443</u> (which the IP_address could be the ZyWALL's LAN or DMZ or WAN IP address depending on your remote management setting).

REMOTE MAI	NAGEMENT					
www	SSH	TELNET	FTP	SNMP	DNS	CNM
LITTEC						
ппр						_
Server	Certificate	auto_genera	ated_self_signed_cert	🗾 (See <u>My Certific</u>	ates)	
🗆 Au	thenticate Client Certi	ficates (See <u>Truste</u>	d CAs)			
Server	Port	8443				
Server	Access	🔽 LAN 🔽	WAN1 🔽 WAN2	🗸 DMZ 🔽 WLAN		
Secure	Client IP Address	💿 all 💿	Selected 0	. 0 . 0 . 0	_	
HTTO						
nite						
Server	Port	80				
Server	Access	🔽 LAN 🔽	WAN1 🔽 WAN2	🔽 DMZ 🔽 WLAN		
Secure	e Client IP Address	💿 all 🕥	Selected 0	0 , 0 , 0		
Note 1 Note 2	: For <u>UPnP</u> to function : You may also need t	normally, the HTTP to create a <u>Firewall</u>	service must be a rule.	vailable for LAN com	nputers using UPnP.	
		Apply		Reset		

Note: However, if you have configured a port-forwarding-rule 443 to a web server. We would suggest to utilize another WAN IP address of ZyWALL UTM device for ZyWALL SSL10's access.

For example, if you have configured WAN1 IP forward port 443 to another web server, (ex. 192.168.3.10). We could use WAN2 interface (ex. IP address is 10.59.1.30) to forward 443 to ZyWALL SSL10 as following figure.

Por W	t Forwa 'AN Inter	rding Rules face	0	WAN 2 💌								
D	efault Se	rver		0,0,0	0.0		Go	To Pa	ge 1	•		
#	Active	Name	Incon	ning Port(s)	Port	Translation	Se	erver	IP 4	Add	res	5
- C		to-SSL10	443	- 443	443	- 443	192	. 168		3		2
2			0	- 0	0	- 0	0	. 0		0	•	0
3			0	- 0	0	- 0	0	. 0		0		0
4			0	- 0	0	- 0	0	. 0		0		0
5			0	- 0	0	- 0	0	. 0		0		0
6			0	- 0	0	- 0	0	. 0		0		0
7			0	- 0	0	- 0	0	. 0		0		0
8			0	- 0	0	- 0	0	. 0		0		0
9			0	- 0	0	- 0	0	. 0		0		0
10			0	- 0	0	- 0	0	. 0		0		0
N	ote 1: Yo	u may also r	eed to cre	ate a Firewall rule								

Configuration on ZyWALL SSL 10

1) Access ZyWALL SSL10 via <u>https://192.168.1.1</u> by default, login by entering username and password (default is **admin/1234**). Press **Login** button.

Note1: Depending on if you want to clean the HTTP cache after perform the tasks. If you are using your PC to configure ZyWALL SSL 10 without any security concern, leave it just as default 'I am connecting via **my own** computer'. Otherwise, choose 'I am connecting via **Public** computer' instead.

Note2: Please ensure you turn on JavaScript and ActiveX control setting on your browser.

🚰 ZyWALL SSL10 - Microsoft Internet Explorer 📃 💌
Eile Edit View Favorites Iools Help
🛛 🚱 Back 🔹 🕥 - 💌 😫 🏠 🔎 Search 🦖 Favorites 🚱 🔗 - 🌺 🕋 - 🔷 👋
Address 🚳 https://192.168.1.1:8443/login.htm
ZyXEL
ZyWALL SSL 10
Welcome to ZyWALL SSL 10 Enter User Name/password and click to login.
🙂 User Name:
🔁 Password:
💼 One-Time Password: (Optional)
(max. 30 alphanumeric, printable characters and no spaces)
I am connecting via my own computer.
C I am connecting via Public computer.
🌂 Note: Please enable Javascript on your Browser.
Login Reset

- 2) Then press **Yes** button to accept the system alert.
- 3) If you are the first time to configure ZyWALL SSL 10, the following page will be shown. Choose **Setup Wizard** button to enter wizard.



But if it's not your first time to configure ZyWALL SSL 10, the system will login to **Advanced Setup** page. Click the **Wizard** icon on the right top of page after successfully login.

🚰 .:: ZyWALL SSL 10 :: Microsoft Internet Explorer	- 🗆 🗙
File Edit View Favorites Tools Help	
🕞 Back 🔹 🕞 - 💌 😰 🏠 🔎 Search 🦖 Favorites 🤣 🔗 🌺 🕋 - 🛄 🕙 鑬 🖓	N
Address 🚳 https://192.168.1.1:8443/advanced.htm	nagit 🛃
A 🛛 Status	
Status Refresh Interval: None Refresh Now ZyWALL SSL 10 Device Information System Status	
The Sustain	

4) Choose the default "Install on Gateway's DMZ Port" and press Next button.

Welcome to the ZyWALL SSL VPN Setup Wizard The ZyWALL SSL 10 Setup Wizard is not compatible with your currently configured network settings. You may go to the Advanced Network configuration to make individual networking changess Or, you may continue with this ZyWALL SSL 10 Setup Wizard, but your current network configuration will be lost. The wizard will create a policy named "default". If this policy alreatexisted, this wizard will overwrite its setting. Image: Internet Image: Configuration of the Wizard Will create a policy named "default". If this policy alreatexisted, this wizard will overwrite its setting. Image: Image: Configuration of the Wizard Will overwrite its setting. Image: Image: Configuration of the Wizard Will overwrite its setting. Image: Image: Configuration of the Wizard Will overwrite its setting. Image: Image: Configuration of the Wizard Will overwrite its setting. Image: Image: Configuration of the Wizard Will overwrite its setting. Image: Image: Image: Configuration of the Wizard Will overwrite its setting. Image: Image: Image: Configuration of the Wizard Will overwrite its setting. Image:	168.1.1:8443 - ZyWALL SSL VI	PN Setup Wizard - Microsoft Internet Explorer
Welcome to the ZyWALL SSL VPN Setup Wizard The ZyWALL SSL 10 Setup Wizard is not compatible with your currently configured network settings. You may go to the Advanced Network configuration to make individual networking changes Or, you may continue with this ZyWALL SSL 10 Setup Wizard, but your current network configuration will be lost. The wizard will create a policy named "default". If this policy alreate existed, this wizard will overwrite its setting. Install on Gateway's DM2 Port YwALL or Gateway Internet ZyWALL or Gateway YwALL SSL VPN Install as New Gateway Internet ZyWALL SSL VPN Internet Internet ZyWALL SSL VPN Internet<		ZyX
Welcome to the ZyWALL SSL VPN Setup Wizard The ZyWALL SSL 10 Setup Wizard is not compatible with your currently configured network settings. You may go to the Advanced Network configuration to make individual networking changes Or, you may continue with this ZyWALL SSL 10 Setup Wizard, but your current network configuration will be lost. The wizard will create a policy named "default". If this policy alread existed, this wizard will overwrite its setting. Install on Gateway's DMZ Port Internet ZyWALL or Gateway I have ZyWALL or Gateway. I would like to install m ZyWALL SSL VPN Internet ZyWALL SSL VPN Install as New Gateway I have ZyWALL or Gateway. I would like to install m ZyWALL SSL VPN Internet ZyWALL SSL VPN Internet I have ZyWALL or Gateway. I would like to install m ZyWALL SSL VPN Internet ZyWALL SSL VPN Internet I have no Gateway. My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features		
The 2yWALL SSL 10 Setup Wizard is not compatible with your currently configured network settings. You may go to the <u>Advanced Network configuration</u> to make individual networking changes Or, you may continue with this 2yWALL SSL 10 Setup Wizard, but your current network configuration will be lost. The wizard will create a policy named "default". If this policy alre- existed, this wizard will overwrite its setting. Internet ZWWALL or Gateway I would like to install m ZyWALL SSL VPN Internet ZWWALL SSL VPN Install as New Gateway ZWWALL SSL VPN I have no Gateway. My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features	me to the ZyWALL SSL VP	N Setup Wizard
settings. You may go to the <u>Advanced Network configuration</u> to make individual networking changes Or, you may continue with this ZyWALL SSL 10 Setup Wizard, but your current network configuration will be lost. The wizard will create a policy named "default". If this policy alre- existed, this wizard will overwrite its setting. Internet ZyWALL or Gateway's DMZ Port I have ZyWALL or Gateway. I would like to install m ZyWALL SSL VPN I have ZyWALL SSL VPN device on my existed Gateway's I port I have no Gateway. My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features Network SSL VPN features	WALL SSL 10 Setup Wizard is not	compatible with your currently configured networking
 Install on Gateway's DMZ Port ZYWALL or Gateway I have ZyWALL or Gateway. I would like to install n ZyWALL SSL VPN device on my existed Gateway's l port Install as New Gateway ZyWALL SSL VPN Internet I have no Gateway, My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features 	y go to the <u>Advanced Network co</u> may continue with this ZyWALL ation will be lost. The wizard will this wizard will overwrite its sett	onfiguration to make individual networking changes. SSL 10 Setup Wizard, but your current network create a policy named "default". If this policy already ting.
ZyWALL or Gateway I have ZyWALL or Gateway. I would like to install n Internet DMZ ZyWALL SSL VPN Gateway Install as New Gateway I have no Gateway. My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features I have no Gateway and provide SSL VPN features	tall on Gateway's DMZ Port	
Install as New Gateway ZyWALL SSL VPN I have no Gateway. My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features	ZyWALL or Gateway	: have ZyWALL or Gateway. I would like to install my 2yWALL SSL VPN device on my existed Gateway's DMZ oort
ZywaLL SSL VPN I have no Gateway. My ZyWALL SSL VPN device ca Gateway and provide SSL VPN features	tall as New Gateway	
N	ZyWALL SSL VPN I rnet LAN	have no Gateway. My ZyWALL SSL VPN device can be Gateway and provide SSL VPN features
		Next >

5) Then choose "**Static**" for the device's WAN IP assignment for this example. Configure the IP address setting as shown below. Press **Next** button.

	STEP1 STEP2 ST	EP3 STEP4 STEP5	STEP6
nternet	Internet Access WAN IP Address Assign IP Address Assigment	ment Static 💌	
	My WAN IP Address	192.168.3.2	
	My WAN IP Subnet Mask	255.255.255.0	
DMZ Port	Gateway IP Address	192.168.3.1	
VALL UTM	First DNS Server	192.168.3.2	
	Second DNS Server		(optional)
ZyWALL SSL VPN			

6) We create one SSL VPN user for this example. Enter the username and password. Press **Next** button.

Install on Gatewa	y's DMZ port		ZyXEL
	STEP1 + STEP2	STEP3 STEP4 STEP5	STEP6
Internet	Adding a User for d here	efault policy by using §	SSL VPN to access
	Username	sharno	
	Password	••••	
	Confirm Password	••••	
ZyWALL SSL	9 VPN		
LAN			

7) Then configure the VPN network and the remote users IP address pool as below.

	STEP1 STEP2 🔶 ST	EP3 STEP4 STEP5 STEP6	le l
	SSL VPN Network Sett	tings	
Internet	VPN Network Enter the IP address of th provide remote clients ac	ne trusted network to which you would lik cess to resources on your local network.	e to
	VPN Network IP Address	192.168.1.0	
	Subnet Mask	255.255.255.0	
ZyWALL UTM	The IP range defines the assigned to remote users overlap or collide with an IP Address Range Begin	IP address pool from which addresses wi during SSL VPN sessions. The range mu y assigned addresses. 192.168.1.200	ill be st not
	IP Address Range End	192.168.1.250	
LAN		< Back Ne:	xt >

Note: In this example, we have the IP arrangement as shown in the picture below. The right mark in blue color, the "**VPN network**" is as the destination you plan to allow SSL VPN users to access to(as the "LAN zone"). The "**Remote users IP address pool**" means the IP address will be assigned to the remote SSL VPN users from the device in Full Tunneling mode. Since after SSL VPN users login successfully, they will be recognized as LAN users in the main office. Here we enter the IP address ranging from 192.168.1.200 to 192.168.1.250.



8) Then the system will remind you to remember configure the firmwall and UTM setting on the ZyWALL UTM or 3rd party's UTM firewall. Press **Next** button then.

https://192.168.1.1:8443	- ZyWALL SSL VPN Setup Wizard - Micros	oft Internet Explorer 📃	×
Install on Gateway's I)MZ port	ZyXE	L
	2		-
	STEP1 STEP2 STEP3 STEP4	STEP5 STEP6	
	Anti-Virus/IDP Integration with Z	YWALL UTM	
Internet	ZyWALL UTM IP Address		
	The ZyWALL SSL 10 can be easily deploy firewall as a secure remote acess solution ZyWALL UTM, you gain enhanced security protection.	ed alongside any third-party n. When depolyed alongside a y with Anti-Virus and IDP	
	Your Firewall IP Address: 192.168.3.1		
DMZ Port	🐧 Note:		
ZyWALL UTM	 You may also need to create a Fir ZyWALL UTM needs to activate An 	ewall rule on ZyWALL UTM. ti-Virus and IDP license.	
ZyWALL SSL VPN			
	Skip >	< Back Next >	
Cone		📔 🚰 🤝 Internet	111

9) It will give you a summery for the ZyWALL SSL 10's WAN IP setting. Press Activate SSL-VPN License button to register the device's information to myZyXEL.com. However, if you want to activate SSL-VPN license later, press Finish button.

Note: Please make sure the Internet access is available before pressing activate SSL-VPN

license since the system will send the registration information to

http://www.myZyXEL.com.

nstall on Gateway's	DMZ port						ZyXE
		_	_	_	_	_	
	STEP1	STEP2	STEP3	STEP4 🔸	STEP5	STEP6	
	Summary						
Internet	WAN TP A	ddress					
	Mode:	duress		Static	IP		
	IP Address			192.10	58.3.2		
	Subnet Ma	sk:		255.25	55.255.0		
	Gateway:			192.1	58.3.1		
Zywall SSL VPN							
				Finish	Activa	ate SSL-VPN	License >

10) Enter the necessary information to register your user account, the device, and get ten SSL-VPN node licenses after registering successfully. Press **Finished** button to submit the information.

STEP1 STEP2	STEP3 STEP	STEP5 + STE	P6
Activate SSL VPN	License		
This device is not reg below to register yo please select "new m myZyXEL.com accou please go to <u>www.m</u>	gistered to myZyXI our device. If you yyZyXEL.com acco nt, but you forget <u>yZyXEL.com</u> for he	<mark>L.com. Please entresson and seven s</mark>	er information L.com account, nave a Password,
new myZyXEL.cc	om account C	existing myZyXEl	com account
User Name			
Password	Check you can	click to check if us	ername exists
Confirm Password	1		
E-Mail Address	[
Country Code	Select		•

Then you will complete the registration and initial setup.

Simulate a Internet host to access ZyWALL SSL 10 via the ZyWALL

Step1: Assume the PC_A is an Internet host which is at ZyWALL's WAN site. Open the IE browser to access ZyWALL's WAN IP address by HTTPS(ex. <u>https://172.120.1.10</u>). The ZyWALL SSL10 login page will be shown. Enter the username/password we just created (ex. sharno/1234 in this example.)

🗿 ZyWALL SSL10 - Microsoft Internet Explorer
Eile Edit View Favorites Iools Help
🕞 🕞 Back 🔹 💮 🖌 📓 🚮 🔎 Search 👷 Favorites 🚱 🔗 🖕 🎬 🐖 👋
Address https://172.120.1.10
· •
ZyXEL
ZyWALL SSL 10
Welcome to ZyWALL SSL 10 Enter User Name/password and click to login.
User Name:
Password:
One-Time Password: (Optional) (may 20 alphanumeric printable characters and no spaces)
(max. 30 apprairanteric, princable citaracters and ito spaces)
I am connecting via my own computer.
C I am connecting via Public computer.
🐧 Note: Please enable Javascript on your Browser.
Login Reset

It allows the PC_A to access internal resource. But after it successfully login, the remote user will see empty in the Application and File Sharing list as below.

ZyXEL	Application	File Sharing	bba 😭	7 🔊
	Application			
4.95			Туре	
A				
			(C) Copyright 2006 by ZyXEL C	ommunications Corp.

Besides, the user will find his PC got a PPP IP address (ex. 192.168.1.200) in the PC's network connections after successfully login.



The user can open the application tool to access the internal application server if he knows how to access. For example, a FTP server IP is 192.168.1.240. He can open the FTP tool(ex. CuteFTP) to access the server.

If IT stuff would like to pre-configure some access links for remote user's quick view, he needs further configuration. Please refer to chapter 2 for the detail.

1.2 NAT Mode

1.2.1 Deploy ZYWALL SSL 10 at the gateway

If your company's environment hasn't had ZyWALL or other firewall to provide security checking mechanism yet, it's suggested that you put ZYWALL SSL 10 at the network gateway and also perform the NAT feature to translate the private IP address to public.

See following figure to show you the topology for example.



The network topology is used to illustrate this application. We used one ZyWALL as main office's gateway which is connected to the branch office's ZyWALL. The ZyWALL SSL 10 is put at behind the main office's gateway. Remote users could either access the main office's LAN resource or access the remote office's LAN resource via IPSec VPN

tunnel after user pass the SSL authentication.



SSL VPN configuration table



To achieve this, we have to complete the following tasks:

• On ZyWALL SSL 10, using Wizard to setup the initial SSL VPN access network.

See the following step-by-step configuration.

Configuration on ZyWALL SSL 10

 Login ZyWALL SSL 10 GUI (default username is admin; password is 1234). Press Login button.

Note1: Depending on if you want to clean the HTTP cache after perform the tasks. If you are using your PC to configure ZyWALL SSL 10 without any security concern, leave it just as default 'I am connecting via **my own** computer'. Otherwise, choose 'I am connecting via **Public** computer' instead.

Note2: Please ensure you turn on JavaScript and ActiveX control setting on your browser.

ZyXE	
	ZyWALL SSL 10
	Welcome to ZyWALL SSL 10 Enter User Name/password and click to login.
	🎯 User Name: admin
	🚘 Password: 🗪
	(max. 30 alphanumeric, printable characters and no spaces)
	I am connecting via my own computer.
	C I am connecting via Public computer.
🐧 Note:	
Please turr Explorer.	on the Javascript and ActiveX control setting on Internet
	Login Reset

- 2) Then press **Yes** button to accept the system alert.
- If you are the first time to configure ZyWALL SSL 10, the following page will be shown. Choose Setup Wizard button to enter wizard.

ZyXEL	
Please select wizard or advanced mode The Setup Wizard walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your device or if you need to make basic configuration changes. Use advanced mode if you need access to more advanced features not included in wizard mode.	
The wizard is designed for first-time users that will help you quickly configure ZyWALL SSL 10.	
The advanced setup is designed for experienced user that can directly make individual networking changes.	

But if it's not your first time to configure ZyWALL SSL 10, the system will login to **Advanced Setup** page. Click the **Wizard** icon on the right top of page after successfully login.

🚰 .:: ZyWALL SSL 10 :: Micro	soft Internet Explorer 📃 🗖 🔀
File Edit View Favorites Tools	Help 🥂
🔇 Back 👻 🕥 - 💌 💈 🦿) 🔎 Search 🤺 Favorites 🤣 😥 - 🌽 🔟 - 🛄 🕘 鑬 🦓
Address 🗃 https://192.168.1.1:844	/advanced.htm 🗾 🔁 Go 🔵 Snagit 📷
ZyXEL	
· 2	itatus 💛 🛁
Status ZyWALL SSL 10 Registration	Refresh Interval: None 💌 Refresh Now Device Information System Status

4) Choose "Install as New Gateway" and press Next button.

tps://192.168.1.1:8443 - ZyWALL SSL	. VPN Setup Wizard - Microsoft Internet Explorer
	ZyXE
Welcome to the ZyWALL SSL	VPN Setup Wizard
The ZyWALL SSL 10 Setup Wizard is	not compatible with your currently configured networking
settings. You may go to the <u>Advanced Network</u> Or, you may continue with this ZyWA configuration will be lost. The wizard existed, this wizard will overwrite its :	<u>configuration</u> to make individual networking changes. LL SSL 10 Setup Wizard, but your current network will create a policy named "default". If this policy already setting.
C Install on Gateway's DMZ Por	t
ZyWALL or Gateway Internet DHZ LAN ZyWALL SSL VPN	I have ZyWALL or Gateway. I would like to install my ZyWALL SSL VPN device on my existed Gateway's DMZ port
6	
* Install as New Gateway Zywall SSL VPN Internet LAN	I have no Gateway. My ZyWALL SSL VPN device can be Gateway and provide SSL VPN features
	Next >
e	🔚 🜍 Internet

5) In this example, we choose "**Static**" for the device 's WAN IP assignment. Configure the IP address setting as shown below. Press **Next** button.

https://192.168.3.2:844	3 - ZyWALL SSL VPN Setup W	'izard - Microsoft Internet Ex	cplorer 📃 🗖 🗙
Install as New Gatew	ay		ZyXEL
	+ STEP1 STEP2 ST	EP3 STEP4 STEP5 ST	TEP6
	Internet Access		
Internet	ISP Parameters for Int Encapsulation	Ethernet	
	WAN IP Address Assign	ment	
	IP Address Assigment	Static	_
	My WAN IP Address	172.120.1.10	
ZyWALL SSL VPN	My WAN IP Subnet Mask	255.255.255.0	_
	Gateway IP Address	172.120.1.1	_
	Second DNS Server		(optional)
-	WAN MAC Address		
	Factory default		
LAN	Spoof this computer's IP Address	MAC Address	
		< Back	Next >
E Done			Internet

6) Configure the LAN IP assignment and the DHCP setting. Press **Next** button. It will pop up a warning message to remind you the LAN IP address will be changed. Your LAN PC needs to release and renew a new IP address from DHCP.

https://192.168.3.2:8443	- ZyWALL SSL VPN Set	up Wizard - Microsoft Internet Explorer	- 🗆 🗙
Install as New Gatewa	ıy		ZyXEL
			0
	STEP1 + STEP2	STEP3 STEP4 STEP5 STEP6	
	LAN IP Setup		
Internet	LAN TCP/IP		
	IP Address	192.168.1.1	
	IP Subnet Mask	255.255.255.0	
	DHCP Setup		
	DHCP Server	102 169 1 2	
ZyWALL SSL VPN	To	192.168.1.254	
		1	
LAN			
		< Back	Next >
E Done		📄 📄 🚔 🚱 Inte	ernet //



7) In this example, we create one SSL VPN user as the figure below. Press Next button.

https://192.168.3.2:844	3 - ZyWALL SSL VPN Setu	p Wizard - Microsoft Internet Explorer	- - ×
Install as New Gatew	ay		ZyXEL
	_		_
	STEP1 STEP2 🗭	STEP3 STEP4 STEP5 STEP6	
Internet	Adding a User for d here	efault policy by using SSL VPN to	access
	Username	test	
	Password	••••	
	Confirm Password		
ZYWALL SSL VPN	🏹 Note: If you have created now, you can skip ti policy.	l users already and don't want to ad his step to keep users no change in	d new user the default
LAN		Skip >< Back	Next >
Done		🔒 🔮 Inte	ernet //

8) Then configure the VPN network and the remote users IP address pool as following figure. Press **Next** button then.



Note: In this example, we have the IP arrangement as shown in the picture below. The right mark in blue color, the "**VPN network**" is as the destination you plan to allow SSL VPN users to access to(as the "LAN zone"). The "**Remote users IP address pool**" means the IP address will be assigned to the remote SSL VPN users from the device in Full Tunneling mode. Since after SSL VPN users login successfully, they will be recognized as LAN users in the main office. Here we enter the IP address ranging from 192.168.1.200 to 192.168.1.250.



9) It will give you a summery for the ZyWALL SSL 10's LAN and WAN IP setting. Press Activate SSL-VPN License button to register the device's information to myZyXEL.com. However, if you want to activate SSL-VPN license later, press **Finish** button.

Note: Please make sure the Internet access is available before pressing activate SSL-VPN license since the system will send the registration information to

http://www.myZyXEL.com.

https://192.168.3.2:8443	- ZyWALL SSL VPN Setup Wiza	d - Microsoft Internet Explore	×
Install as New Gatewa	ау		ZyXEL
	STEP1 STEP2 STEP3	STEP4 🔶 STEP5 STEP6	
	Summary		
	LAN IP Address		
Internet	IP Address:	192.168.1.1	
	Subnet Mask:	255.255.255.0	
	WAN IP Address		
	Mode:	Static IP	
•	IP Address:	172.120.1.10	
	Subnet Mask: Gateway:	255.255.255.0	
ZyWALL SSL VPN	Gatemay.	172,120,1,1	
•			
LAN			
		1	
		Finish Activate SSL-VPN	License >
Done		🔒 🥥 Inti	ernet //

10) Enter the necessary information to register your user account, the device, and get 10 SSL-VPN node licenses on myZyXEL.com. Press **Finish** button to submit the information.

ATERA ATERA ATERA ATERA	ercor A CTEDZ
STEPI STEP2 STEP3 STEP4	SIEPS # SIEPO
Activate SSL VPN License	
This device is not registered to myZyXEL.co	om. Please enter information
please select "new myZyXEL.com account"	below. If you have a
please go to <u>www.myZyXEL.com</u> for help.	r User Name or Password,
6	
	—
Check way and all	
Password	
Confirm Password	_
E-Mail Address	
Country Code Select	. ¥
	- Back Einished

Then you will complete the registration and initial setup. It allows a remote user to use 'test/1234' to connect to internal. But when a remote user successful login, he will see empty in the Application and File Sharing list since it needs further configuration.



To configure more users or groups and to specify a certain application for remote user's access, please refer to the additional configuration in the chapter 2.

2. Integrated Application

The authentication, policy and end point security requirement is the three essential elements to build up the SSL connection and give different privilege to different user/group to fulfill the vary access application requirement.



Application Diagram:

Background:

A company has daily operation with travel employee, sales and outside partner. They will use SSL VPN to access the internal system to gather necessary information for business operation. The company already deployed a Microsoft AD server for user management and authentication and the ZyWALL SSL10 also used this server for user authentication. There are three user groups pre configured in the AD; they are RD, sales and outsider.

There are different access resources available like web server and web base application for partner to check the new product information or place the order online. For sales, they travel around globalize and they can use SSL VPN connect back to head office to check internal information and the latest price list. For RD group, they may remote access the office PC from his home in case urgent and also checking or updating the file to the internal network for developing and sharing. By ZyWALL SSL 10 object based configuration design, the IT engineer can plan and deploy this application more effective.

2.1 External Authentication

ZyWALL SSL10 can smoothly deploy in a network environment which already had a central user database like Microsoft Activate Directory, RADIUS or LDAP available. User don't need to reconfigure the same user information in ZyWALL SSL10 local database. ZyWALL SSL10 provides a user friendly interface to configure the external database connection.



2.1.1 External Authentication configuration

Please login to ZyWALL SSL10 web GUI and switch to System > AAA Server

configuration page. There are two main block for the AAA server configuration. Upper is the Basic Configuration block including the Server Type, address and port. The next block is the Advance Configuration; this part is more complicated to setup. The AD' detail parameters are configured in this section and this information is confidential for data protect purpose and you may consult with AD administrator for these parameters. Remember to click "**OK**" button to save the configuration.

Status		
ZyWALL SSL 10 Registration	Basic Configuration	
⊖ System - WAN - LAN - Certificate	Server Type Server Address Server Port	AD 192.168.12.31 389
- AAA Server - Host Name	Advance Configuration	
- User/Group - SSL	Server Search Base	dc=NSA,dc=ZyXEL,dc=com
Object SSL Application	Server Bind Password	Vm6g4ru,6
- YPN Network - Endpoint Security	Retype Bind Password User ID Attribute	Vm6g4ru,6 sAMAccountName
- Monitor	Membership Attribute	memberOf
	Sud Attribute Name	Ch Cancel

2.1.2 User/Group configuration

Please switch to User/Group configuration page and click "add" icon to add a new user group.

	7 User/Group > Group			
Status	User Group			
ZyWALL SSL 10 Registration	Configuration			
# System	#	Group Name	Member	
User/Group - SSL				
Object				
Maintenance				

Add the RD group, because the group member had pre-configured in the AD server thus choose the option of "Group in the AAA server". Click OK to save the configuration.

> Configurat	ion > User/Group > Gro	up > Add		
Conf	iguration ne	RD		
C C	ber Group in the AAA Server Select members Available Member	<u>ek</u>	Selected Member(s)	

Follow the same steps to add the Sales group.

> Cor	figuration > User/Group > Grou	ıp > Add	
	Configuration		
	comparation		
	Name	sales	
	Member		
	Group in the AAA Server		
	O Select members		
	Available Member	Selected Member(s)	
	=== Empty ===	>>> === Empty ===	
		<<	
		OK	

Finally, adding the outsider group.

Configuration > User/Group > Group > Add				
	Configuration			
	Name	outsider		
	Member			
	Group in the AAA Server			
	C Select members			
	Available Member	Selected Member(s)		
	=== Empty ===	>> === Empty ===		
		555 J		
		OK		

We can check the user/group general page and found the three groups already settled.

> User/Group > Group					
User Group					
Config	guration				
	# Group Name	Member	t.		
	1 RD		B ² m		
	2 sales		B 🖻		
	3 outsider		B 🗇		

2.2 Objects Configuration

2.2.1 SSL Application Object

Please switch to Object > SSL Application and click the Add icon to add a new application.

Statue	> Object > 9	SSL Application			
ZyWALL SSL 10 Registration	SS	6L Application Configur	ation		
⊪ System		Name	Address	Туре	
-User/Group					
- SSL ⊡-Object					
SSL Application - VPN Network - Endpoint Security - Private IP Pool - Monitor - Maintenance					Click add icon to add new application

There are three SSL application types for user to configure. In this scenario, we will configure one **Web Application**, one **Application** and one **File Sharing** services.

7 Obj	ect > SSL Application > Ad	d	
	Object		
	Туре	Web Application	
	Add Web Application	Application File Sharing	
	Display Name		
	Address	(ex:http://192.168.1.1 or https://192.168.1.1)	
	Suffix		(Optional)
	Server Type	Web Server	
	Virtual Web Port	Note:You need to allow this port on your network. Only IE, Mozilla and Netscape browsers can support this	(Optional) 5 option
		Ok Cancel	

Web Application:

Select the **Web Application** from drop down menu and fill in the web application display name and address. The Display Name is the name show up in the user personal portal right after user login. The address field is for web server address and port. For example our web server uses IP 192.168.1.10 and port 8080 and then we should type http://192.168.1.10:8080. The ZyWALL SSL10 will access server port 80 or port 443 if the address starts with http:// or https:// and doesn't specific the port number.

> Obj	ect > SSL Application > A	dd	
	Object		
	Туре	Web Application	
	Add Web Application		
			_
	Display Name	Quick_Order	
	Address	http://192.168.1.10:8080 (ex:http://192.168.1.1 or https://192.168.1.1)	
	Suffix		(Optional)
	Server Type	Web Server 💌	
	Virtual Web Port	Note:You need to allow this port on your network. Only IE, Mozilla and Netscape browsers can support this	(Optional) s option
		Ok Cancel	

Application:

Select the **Application** from drop down menu and fill in the application display name and address. The Display Name is the name show up in the user personal portal right after user login. We provide some predefined application types and user also can custom their own application via setting portal and port. The **Address** field is the application server IP address.

7 Obj	ect > SSL Application > Ad	d	
	Object		
	Туре	Application	
	Add Application		
	Display Name Application Type Address Intranet Port Client Port	yallara SSH 192.168.1.20 22 22	
	Cilent Port	(Optional)	

File Sharing:

Select the **File Sharing** from drop down menu and fill in the display name and address. The Display Name is the name show up in the user personal portal right after user login. The **Address** field is the file sharing server IP address and the **Shared Folder** is used to specific the shared folder name. Please be noticed; fill in the folder name straight like **doc**/ when share server is Windows OS and add a '/' before the name like /**doc**/ in Linux system.

Object		
Туре	File Sharing	
Add File Sharing		
Display Name	NAS	
Address	192.168.1.30	(ex:192.168.1.1 or Fileserver
Shared Folder	doc/	(ex:Fileshare/dir1/dir2)
Shared Folder	doc/	(ex:192.168.1.1 or Filesen) (ex:Fileshare/dir1/dir2)
2.2.2 VPN Network Object

Please switch to Object > VPN Network and click the Add icon to add a new VPN network.

Status	Dbject > ¥PN Network	
ZyWALL SSL 10 - Registration - System - User/Group	Network Configuration	IPAddress/Mask
- SSL - SSL - SSL Application - VPN Network - Endpoint Security - Private IP Pool - Monitor		Click Add icon to add new VPN network

Fill in the Name for this VPN network and the network address and the netmask. For example, we have one subnet called RD_subnet and address is 192.168.2.0/255.255.255.0.

> Obj	ect > Network > Add		
[
	Create Network		
	Name	RD_subnet	
	Private Network	192.168.2.0	
	Private Netmask	255.255.255.0	
		OK Cancel	

2.2.3 Endpoint Security Object

End Point security help to make sure the SSL client have achieve the security requirement and ensure they won't be threatened the SSL network. Please switch to Object > Endpoint Security and click the Add icon to add a new endpoint security policy.

	> Object > End Point Security Policies
Status	
ZyWALL SSL 10 - Registration	List of End Point Security Policies
₽ System	End Point Security Name
-User/Group	
- SSL	
- Object	
- SSL Application	
- ¥PN Network	Click Add ison to add now
Endpoint Security	endation to add new
Private IP Pool	chapent occurs pointy
- Monitor	
Maintenance	

The endpoint security requirement may be different based on different user/group privileges. We must apply the most strict security policy to the user/group that has the full access right to internal network. Below I list the endpoint security requirement matrix table for this scenario.

	outsider	sales	RD
Check Windows Version	ν	ν	ν
Check Windows Service Pack Version	ν	ν	ν
Check Windows Auto Update	×	ν	ν
Check Personal Firewall Name	×	×	ν
Check Personal Firewall Version	×	×	×
Check Anti Virus manufactory	×	ν	ν
Check Anti Virus Version	×	ν	ν
Check Anti Virus Auto Protect	×	×	ν
Check Browser manufactory	×	×	×
Check Browser Version	×	×	×

We will start to configure three endpoint security policies for each user/group one by one.

Outsider Endpoint Security Policy:

The outsider means people who are not our company's employee but they still need to access the company's internal network resource for business cooperation. In order to secure our network; we will limit their application type in Web application only and checks if their windows version and service pack follow our policy.

EPC Name	outsider	
Check Windows Version	Windows XP 👻	
Check Windows Service Pack Version	2 (ex: 2 for Service Pack 2)	
Check Windows Auto Update	Don't Care 💌	
Check Personal Firewall Name	Don't Care 💌	
Check Personal Firewall Version	(ex:5 for 5.1.2.3)	
Check Anti Virus	Don't Care	
Check Anti Virus Version	(ex: 10 for 10.0.0.359)	
Check Anti Virus Auto Protect	Don't Care 💌	
Check Browser	Don't Care 💌	
Check Browser Version	(ex:6 for 6.0.2800.1106)	
	more	

Sales Endpoint Security Policy:

Normally, sales are traveling around the world and they need to get the latest info from company like the price or partner list update. It is not secure to get this kind of business confidential data via Email or normal web connection. Thus, we hope they can access our internal network via SSL tunnel. We will define more end point security requirements because sales are not only allowed to access web application also some internal resources.

EPC Name	calec
El C Mallio	
→ Check Windows Version	Windows XP 💌
Check Windows Service Pack Version	2 (ex: 2 for Service Pack 2)
Check Windows Auto Update	Enable 💌
Check Personal Firewall Name	Don't Care 💌
Check Personal Firewall Version	(ex:5 for 5.1.2.3)
─→ Check Anti Virus	Norton AntiVirus 🔽
→Check Anti Virus Version	2006 (ex: 10 for 10.0.0.359)
Check Anti Virus Auto Protect	Don't Care 💌
Check Browser	Don't Care 🔽
Check Browser Version	(ex:6 for 6.0.2800.1106)
	more
	Ok Cancel

_

RD Endpoint Security Policy:

RD needs the remote access back to company internal network to gather the critical information like coding or debugging in case urgent. The endpoint security requests more checking items to well protect the internal network. We will check the windows version and service pack for OS level and check the client security like personal firewall, antivirus software and signature update.

Add Policy	
EPC Name	RD
ightarrow Check Windows Version	Windows XP 💌
→ Check Windows Service Pack Version	2 (ex: 2 for Service Pack 2)
Check Windows Auto Update	Don't Care 💌
→ Check Personal Firewall Name	NAV
Check Personal Firewall Version	(ex:5 for 5.1.2.3)
→ Check Anti Virus	Norton AntiVirus 🔽
→ Check Anti Virus Version	2006 (ex: 10 for 10.0.0.359)
→ Check Anti Virus Auto Protect	Enable 🔽
Check Browser	Don't Care 💌
Check Browser Version	(ex:6 for 6.0.2800.1106)
1	more
	Ok Cancel

2.2.4 Private IP Pool Object

Private IP pool provides SSL client a virtual IP address for the linkage to internal VPN network. For example, the private IP pool is 192.168.2.x/24 subnet and VPN network is 192.168.1.x/24 subnet. ZyWALL SSL 10 will dispatch an IP address from private IP pool to the SSL client who is allowed to access the VPN network. Thus, the client can use this private IP address to talk with the host in the VPN network and vice versa.

Please switch to Object > Private IP Pool and click the Add icon to add a new private IP pool.

	🗿 Object > Private IP PooL	
ZyWALL SSL 10 Registration	Configuration	
System User/Group	Name	IP Address / Mask
- SSL - Object - SSL Application		
- ¥PN Network - Endpoint Security Private IP Pool - Monitor		Click Add icon to add new private IP pool object
■ Maintenance		

Private IP Pool configuration:

Fill in the Name for this Private IP Pool network and the network address and the netmask. For example, we have one subnet called SSL_client and the address is subnet 192.168.2.0/255.255.255.0. The DNS option is used when customer have an internal DNS server to resolve the internal FQDN hostname to IP address. The DNS server and WINS server are optional and it is not necessary to fill in these fields.

ject > rrivate ir rooi > Hau	
Private IP Pool	
Name	SSL_client
🔿 IP Range	From
 Subnet 	192.168.10.1 (IP address)/ 255.255.255.0 (mask)
Primary DNS	192.168.1.5
Secondary DNS	
WINS Server	
	Ok Cancel

2.3 SSL Policy Configuration

After pervious two sections, we already configured the external authentication server, user group and the different kinds of objects. Now, we can easily combine these parameters together to form up different SSL Policies according to different user/group's access privilege and security requirement.

We must assign the SSL policy to a specific user/group and then choose the endpoint security type and SSL applications which includes web application, application, file sharing and VPN network.



Outsider SSL Policy

Switch to SSL configuration page and add a new SSL policy for outsider. The outsider uses the endpoint security object outsider that we configured in previous section.

5 P	olicy > Policy Information > Add Po	licy		
Status				
ZyWALL SSL 10 - Registration	Configuration			
⊪ -System	Policy Name	outsider		
- User/Group	User List		User/Group Name	
- Object			RD	
- SSL Application			sales	_
- VPN Network			outsider	
- Endpoint Security				
Private IP Pool	Enable client certification	authentication		
- Monitor	End Point Security			
maintenance	End Point Security List		End Point Security Name	
			outsider	
			sales	
			RD	
	Periodical check	sec		

They are only allowed to use the web application "Quick_Order" and we won't assign them an internal VPN network.

> Po	licy > Policy Information > Add Polic	cy
Status	Periodical check	sec
ZyWALL SSL 10	SSL Application	
- Registration # System	SSL Application List	SSL Application
-User/Group		✓ Quick_Order
SSL		🗌 yallara
- Object		□ NAS
- SSL Application - VPN Network		
- Endpoint Security	Zullian col upplication day	
Private IP Pool	ZYWALL SSL-VPN Securitender	F
- Monitor	Enable	
■ Maintenance	VPN Remote Network List	Network Name
		RD_subnet
	Endpoint Private IP Pool	v
		Ok

Sales SSL Policy

Add another new SSL policy for sales. The sales use the endpoint security object sales that we configured in previous section.

~	Policy > Policy Information > Add Policy	licy	
Status			
ZyWALL SSL 10 Registration System - WAN - LAN - Certificate - AAA Server Host Name	Configuration Policy Name User List	sales User/Group Name RD Sales	
-SSL	Enable client certification a	authentication	
SSL Application	End Point Security		
- YPN Network - Endpoint Security - Private IP Pool - Monitor - Maintenance	End Point Security List	End Point Security Name outsider sales RD	
	Periodical check	sec	

They are only allowed to use the web application "Quick_Order" and file sharing "NAS"; we won't assign them an internal VPN network.

> Po	licy > Policy Information > Add Polic	у	
Status	SSL Application		
	SSL Application List	SSI Application	
- Registration			
∋System		V Quick_order	
WAN			
- LAN		V INAS	
- Certificate			
- AAA Server	ZyWALL SSL-VPN SecuExtender		
- Host Name	Ly mile ose millocaentonaon		
- User/Group	🗌 Enable		
- Object	VPN Remote Network List	Network Name	
-SSL Application		RD_subnet	
- ¥PN Network			
- Endpoint Security			
Private IP Pool			
- Monitor	Endpoint Private IP Pool	×	
Haintenance		Ok Cancel	

RD SSL Policy

Add another new SSL policy for RD. The RD uses the endpoint security object RD that we configured in previous section.

	Policy > Policy Information > Add Po	licy	
Status	Configuration		
ZyWALL SSL 10 - Registration	Policy Name	RD	
System	User List	User/Group Name	
WAN		✓ RD	
LAN			
- Certificate			
- AAA Server			
- Host Name	Enable client certification	authentication	
-User/Group			
SSL	End Point Security		
⊡ -Object	End Point Security List	End Point Security Name	
- SSL Application			
- VPN Network		outsider	
- Endpoint Security		sales	
Private IP Pool		RD RD	
- Monitor			
■ Maintenance			
	Periodical check	sec	

RD can use the most internal application like security telnat connection-SSH and VPN network. They are allowed to use the internal Linux server with SSH and file sharing server "NAS". We also assign them an internal VPN network and they will use the predefined

private IP pool to connect with VPN network.

2 Poli	cy > Policy Information > Edit Policy			
Status	SSL Application			
ZyWALL SSL 10 - Registration System - WAN - LAN - Certificate	SSL Application List		SSL Application Name Quick_Order yallara NAS	
AAA Server Host Name User/Group SSL Diject - SSL Application - VPN Network - Endopint Security	ZyWALL SSL-VPN SecuExtender		Network Name RD_subnet]
Private IP Pool Monitor	Endpoint Private IP Pool	SSL_client	Ok Cancel	

We can see three SSL policies in the Policy list table after we complete the three SSL policies. The list also shows the policy name, user/group, SSL application(s) and VPN network. Later on, user can add new policy or edit existing policy in this page.

ces	ss Control	Glob	al Setting							
су										
	Policy Name		L	lser/Group		SSL Application		VPN Network	ę.	
	outsider			outsider		Quick_Order			B 1	Ū.
	sales			sales		Quick_Order;NA	s		B 1	Ē.
	RD			RD		yallara;NAS		RD_subnet	B 1	Ē.

Now, we already finished the SSL environment setup and the remote user can start to enjoy the internal resource with highly security protect.

3. SSL VPN Solution

In the chapter one, we describe the integration of ZyWALL and SSL VPN. Furthermore, you could integrate a ZyWALL UTM and ZyWALL SSL 10 so that the traffic could be secure inspected first by ZyWALL UTM functions like Anti-Virus/IDP before ZyWALL SSL10's authentication. Beyond this, we could establish a VPN tunnel between the Main office's ZyWALL UTM and the remote office's so the SSL remote user will access the remote office's resource via central management.

3.1 UTM Integration: ZyWALL UTM+ZyWALL SSL10

One of IT staff's headache, virus/intrusion could always reach internal network even though they secure the network gateway with access control rules and apply all the latest service pack or signature update on server hosts. The reason is usually because user's notebook may access Internet from home or from some unsecured place. The virus may infect user's notebook because you think you just open a normal file. The intrusion may be injected to your notebook silently because user access internet without aware of a vulnerability is in his/her notebook.

So for those trusted user but untrusted notebook/PC, IT staff needs to apply the mechanism to block those virus/intrusions when they want to access company's internal recourse. We would suggest to integrate a ZyWALL SSL10 with a ZyWALL UTM or 3rd party's UTM firewall. The AV/IDP function will block abnormal traffic when virus or intrusions are detected.

Application Diagram:



Background Story:

ZyCompany has a security concern for remote users when they access internal resources via ZyWALL SSL10. Although ZyWALL SSL 10 can provide security checking for those trusted users, some virus or intrusions may still be able to reach the internal network through those trusted PCs without the user aware of it. IT staff would like to enable Anti-Virus/IDP inspection functions on ZyWALL UTM device for SSL-VPN traffic.

Configuration information in this example:



To achieve this, we have to complete the following tasks:

- On ZyWALL SSL 10, using Wizard to setup the initial SSL VPN access network.
- On ZyWALL UTM, register the device and enable the AV/IDP functions.

See the following step-by-step configuration.

Configuration on ZyWALL SSL10

Please refer to the chapter one to configure ZyWALL SSL10 in DMZ mode.

Configuration on ZyWALL UTM

Step1. Ensure you have completed the registration.

1) Activate AV/IDP license using the iCard

ZyNOS 4 + Turbo Card

ZyWALL UTM started to support AV/IDP service with latest firmware 4.00(ZyWALL 5 UTM start from 4.01(WZ.0)). In order to take full advantage of the AV/IDP service in ZyWALL UTM, it is mandatory to have a ZyWALL Turbo Card inserted in the Expansion Card Slot at the back of your ZyWALL UTM. This Turbo Card will guarantee your ZyWALL UTM can deliver its best performance.

IDP/AV License Activation

In **Registration** page, register your account if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select IDP/AV 3 months trial version to activate

cegisciación	Service	
Device Regis	tration	
Existing	myZyXEL.com	account
User Name		jacky1234
Password		(Type username and password from 6 to 20 characters.)
Service Activ	vation	th Trial
🖂 Content	im 3-month Tria	al (Service has been activated.)
IDP/AV	3-month Trial (Service has been activated.)
Note: For m	ore device serv	ices management, please go to <u>myZyXEL.com</u>

The ZyWALL UTM has IDP (Intrusion Detection Prevention) service, which will inspect all traffic going through ZyWALL 5 UTM to effectively stop/drop most Worms, Trojans, DoS and DDoS attacks.

In addition, the ZyWALL UTM has a stream based AV scan engine that will scan all traffics as them pass through ZyWALL. This stream based AV scan engine can precisely detect virus/worms and then destroy these infected files before they reach intranet hosts.

Step2. Setup the IDP service to prevent the attacks

- 1. In **IDP->General**, check the Enable Intrusion Detection and Prevention check box to enable IDP function.
- 2. In the traffic direction matrix, check all the send to LAN and DMZ's check boxes to have the inbound traffic to LAN and DMZ interfaces be protected.
- INTRUSION DETECTION AND PREVENTION General Signature Update Backup & Restore General Setup Enable Intrusion Detection and Prevention Installed Turbo Card LAN WAN DMZ WLAN То ~ ~ WAN DMZ WLAN * Protected Traffic Directio Apply Reset
- 3. Click on the **Apply** button to save the above settings.

Step3. Setup the ANTI-VIRUS service to inspect if the receiving file infected

- In ANTI-VIRUS->General, check the Enable Anti-Virus to enable the AV function and enable Zip File Scan to force the AV engine to scan the Zip file. ZyWALL can't inspect the Zip file when it protected by password.
- 2. For **FTP** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected accordingly, so that the FTP file upload/download traffic can be protected from the virus infection. And the system can give a warning to IT staff if a virus is found.
- 3. For **HTTP** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected accordingly, so that the Web surfing traffic can be protected from virus infection. And the "**Log**" can give a warning to IT staff if virus is found.
- 4. For **POP3** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected, so that the LAN users receive POP3 mails traffic can be protected from virus infection. And the system can give a warning to IT staff if a virus is found.

- 5. For **SMTP** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected so that the remote users send SMTP mails traffic can be protected from virus infection. And the system can give a warning to IT staff if a virus is found.
- 6. Click on the **Apply** button to save the settings.

NTI-VIRUS							
General	Signature	Up	date Bac	kup & Restor	e		
General Setup							
🗹 Enable Ar	nti-Virus						
🗹 Enable ZI	IP File Scan						
Turbo Car	rd	Installed					
Available Serv	vice						
Service		FTP (TCP 20/ HTTP (TCP 8/ POP3 (TCP 1 SMTP (TCP 2	(21) 0, 8080, 3128) 10) (5)				
🗹 Active FT	Р						
	То	LAN	WAN	DMZ	WLAN	¥ PN	
From							
LAN							
WAN							
DMZ							
WLAN							
¥PN							
	_				* Protected T	raffic Direction	
			Apply	Reset			

Note: Remember to make sure the AV signatures are most updated thereby the ZyWALL UTM AV engine can stay in the best status. (The "update" can be done manually or automatically).

	Signature	Update	Backup & Restore
Signature	Information		
Current P	attern Version: v1.224		
Release D	ate: 2006-06-28 00:5	1:24	
Last Upda	te: 2006-06-29 02:24:	20	
Current A	nti-Virus Signatures: 8	00	
Signature	Jpdate		
Service S	atus: License Active		
Expiration	Date: 2008-08-30		
Synchroni	ze the IDP and Anti-Vi	rus Signature to t	ne latest version with the online update server.
Update Se	rver: myupdate.zywall.z	cyxel.com	Update Now
	Jpdate		
🗹 Auto I	ourly		
Auto I 🔿 Ho	1 22 44 4	D'clock)	
Auto I O Ho O D	ally 23 💌 (C	and the second second	IA
Auto I O He O D O W	eekly Sunday	0 🗠 (oʻc	0CK)

The AV signature update page

3.2 Seamless Integrate SSL VPN into your existing IPSec

VPN

For some company, they may have existing IPSec VPN tunnel between main and remote offices. In this chapter, we would introduce you how to integrate SSL VPN with it. That is, all the traffic to the remote access also need to be authenticated and pass the end-point security checking by ZyWALL SSL 10.

Application Diagram:



Background Story:

ZyCompany implements two ZyWALL devices in main office and in remote branch office. IT staff would like to establish the IPSec VPN between two offices. Furthermore, they would like to deploy the SSL VPN solution for remote users to access FTP, Mail, Web servers in main office and also to access the FTP server in the remote branch office.

Configuration information in this example:



	ZyWALL SSL 10	ZyWALL A (main)	ZyWALL B (remote)
•	WAN Address: 192.168.3.2	• WAN Address: 172.120.1.10	• WAN Address: 172.120.2.10
•	VPN Network: 192.168.0.0/16	• DMZ Address: 192.168.3.1/24	• LAN Address: 192.168.9.1/24
•	Remote Users IP Address Pool:	• LAN Address: 192.168.1.1/24	
	192.168.1.200~ 192.168.1.250		

To achieve this, we have to complete the following tasks:

- Configure the ZyWALL SSL 10 in DMZ mode by using Wizard
- On two ZyWALL devices, configure IPSec VPN settings.

See the following step-by-step configuration.

Configuration on ZyWALL SSL10

Please refer to the chapter one to configure ZyWALL SSL10 in DMZ mode. However, notice to configure the VPN network as192.168.0.0/16 to cover the LAN and DMZ network for main office and the LAN network of the remote office.

VPN Configuration on two ZyWALL devices

Configure VPN rules if ZyWALLs with Static WAN IP Address

This section describes an example configuration ZyWALL with static WAN IP address.

If ZyWALL is used as Internet gateway and public IP address is assigned on ZyWALL's WAN interface. ZyWALL uses this public WAN IP address for terminating the VPN tunnels from remote VPN gateways.

In following example, local VPN gateway (ZyWALL) uses a static public IP address.



- Configure the static Public IP address to WAN interface through Network > WAN1 (or 2)
 > WAN IP Address Assignment
- 2) Enter the WAN IP address as My Address in Gateway Policy
- On peer VPN gateway, use the same IP address as Remote Gateway Address in Gateway Policy
- 4) On Local VPN gateway, select **IP** as the **Local IP Type** and enter the public WAN IP

address as the **content** of identify. On remote VPN peer, select IP as the Peer ID Type and enter the same IP address as the content of identify.

Configure ZyWALL with Dynamic WAN IP Address

This section describes an example configuration ZyWALL with dynamic WAN IP address.

If ZyWALL uses PPPoE or Ethernet/DHCP for its Internet connection, WAN IP address is dynamically assigned by ISP. Since ZyWALL has no idea about its WAN IP address before it is assigned, it is difficult/impossible to use WAN IP Address for My Address in Gateway Policy.

To overcome this problem, **Dynamic DNS** can be used to resolving the VPN gateway. When new IP address is assigned to ZyWALL's WAN interface, ZyWALL will updates the related record in DDNS server. Therefore the peer VPN gateway can resolve ZyWALL's IP address to make a VPN tunnel.



In following example, local VPN gateway (ZyWALL) uses a dynamic WAN IP address (PPPoE with dynamic IP assignment).

WAN->WAN1 o	r WAN2		
Encapsulation	PPP over Ethernet		
User Name		(ohnousů	
Password	******		
WAN IP Address Assignment			
Get Automatically from I	;P		
Idle Timeout	100 (Seconda)		
DNS->DDNS		Configure a DDNS entry and bind it to WAN interface WAN P Asteos WAN	
Geteway Palicy Information	2 	Converse Paticy Information Converse Paticy Information Ny Address D0 D0 (Down News or Photom region Converse Conve]

- 4) Configure the DDNS entry under DNS-> DDNS and bind it to a WAN interface (WAN1 or WAN2).
- 5) Under Gateway Policy menu, select the DDNS entry from drop-down list and use it as **My Domain Name.**
- 6) Configure the DDNS entry in **Remote Gateway Address** on peer VPN gateway.
- 7) Both **DNS** and **E-mail** can be used as the Local ID & Peer ID for authentication.

Note: If Hi-Available (HA) for incoming VPN HA is necessary, enable the **HA** option while configure the DDNS entry under DNS-> DDNS ZyWALL will update its DDNS entry with another WAN interface when the specified WAN interface is not available. Therefore, the next coming VPN connection will go through second WAN interface.

Configure ZyWALL behind NAT Router

This section describes an example configuration ZyWALL behind NAT Router (Internet Gateway).

NAT routers sit on the border between private and public (Internet) networks, converting private addresses in each IP packet into legally registered public ones. NAT is commonly supported by Internet access routers that sit at the network edge. However, IPSec is NAT-sensitive protocol which means modification on IPSec traffic may cause failure of VPN connection.



By far the easiest way to combine IPSec and NAT is to completely avoid these problems by locating IPSec endpoints in public address space. This can be accomplished in two ways:

- 1) Perform NAT on a device located behind IPSec gateway
- 2) Use an IPSec gateway for both IPSec (VPN) and NAT (Internet Access).

However, in some situation, it is inevitable to locate IPSec gateway in public IP address and it must be placed behind the NAT router. For example, the NAT router has a different interface (e.g. leased line, ISDN) which are not supported by IPSec gateway. This example gives some guideline for configuring ZyWALL behind NAT router.

Configuration on NAT Router	If firewall is also running on the NAT Router
NAT Forwarding on NAT Router	Firewall Rule to allow IPSec traffic
Pack Function NUNT = Undext Server 0.0.0.0 2 Active 500 9 D P S 500 10 D P P ort 500 (IKE) traffic to 2xWWALL	Edit Service Available Services IPGPE 0 IPSEC_TRANSPORT/TUNNEL(AH:0) IPSEC_TUNNEL(ESP.0) INCITCAST(ISM) Firewall Rule to allow USSec AH/ESP traffic

- 1) UDP 500 (IKE) must be forwarded to ZyWALL to accept incoming VPN connection from peer VPN gateway or client.
- 2) If Firewall is running on the same NAT router, make sure a firewall rule is configured to allow IKE/IPSec (AH/ESP) traffic to pass-through.

Configuration	n on Local ZyWALL	Configuration on Peer VPN gatewa
WAN->WAN1 0	r WAN2	
Get Automatically from ISP Use Fixed IP Address My WAN IP Address ay worr IP Subnet bass Gateway IP Address	192 - 168 - 1 - 70 200 - 200 - 200 - 0 192 - 166 - 1 - 1	
VPN->VPN Rul Property NAT Traversal Name	e (IKE) on ZyWALL	4
Cateway Policy Information	e (IKE) on ZyWALL	VPN->VPN Rule (IKE) on ZyWALL Gateway Petry Petry Information Wy 2wMAL My Address Petry Information Remote Gateway Address 210 242 82 70 Petry Information Remote Gateway Address
Authentication Key © Pre-Shared Key © Certificate Local ID Type Content	12345678 Chinon self cent x (See My Certificates) P x 210.242.82.70	Authentication Key Pre-Shared Key Certificate Control Contro
Peer ID Type Content	210 242 82.1	Peer ID Type IP Content 210 242 82 70

- 3) On ZyWALL, enable "**NAT Traversal**" no matter if the front NAT router supports NAT Traversal (IPSec pass-through) or not. With this option enabled, ZyWALL can detect if it is placed behind NAT when peer VPN entity also support NAT Traversal function. If yes, the IPSec traffic will be encapsulated in UDP packet to avoid traversal problem on NAT routers.
- 4) Under VPN->Gateway Policy-> Gateway Policy Information configure the private

IP address as "My Address" on local ZyWALL gateway (behind NAT router).

5) On peer VPN gateway, use the public **WAN IP address of NAT Router** as the "**Remote Gateway Address**" of Gateway Policy rule.

The ID must be consistent no matter if IP/DNS/EMAIL is used. So long as if the ID Type and content are consistent on both VP entities.

Configure Port Forwarding rule for SSL VPN traffic on the ZyWALLA

 Go to the GUI > ADVANCED > NAT > Port Forwarding, add one rule to forward port 443 traffic to the ZyWALL SSL 10 (192.168.3.2)

NAT Overview	Address Mappin	ng Port Forwarding	Port Triggering	
Port Forwa	arding Rules			
WAN Inte	rface	WAN 1 💌		
Default S	erver	0.0.0	. 0	Go To Page 1 💌
# Active	Name I	ncomina Port(s)	Port Translation	Server IP Address
1 🔽	SSL10 44	3 - 443	443 - 443	192 . 168 . 3 . 2
2 🗌	0	- 0	0 - 0	0.0.0.0
3 🔲	0	- 0	0 - 0	0.0.0.0
4 🔲	0	- 0	0 - 0	0.0.0.0
5 🕅	0	- 0	0 - 0	0.0.0.0
6 🗖	0	- 0	0 - 0	0.0.0.0
7 🗖	0	- 0	0 - 0	0.0.0.0
8 🗖	0	- 0	0 - 0	0.0.0.0
9 🗖	0	- 0	0 - 0	0.0.0.0
10 🗖	0	- 0	0 - 0	0.0.0.0
Note 1: Y Note 2: P	ou may also need t ort Translation is op	o create a <u>Firewall</u> rule. vtional.		
		Apply	Reset	

2). Go to the GUI > ADVANCED > REMOTE MGMT > WWW, change the ZyWALL UTM's HTTPS management port number from port 443 to another port number (ex. 8443). This is to make sure all HTTPS traffic via port 443 will be forwarded to ZyWALL SSL 10. But when IT staff needs to access the ZyWALL UTM by HTTPS, they can use <u>https://IP_address:8443</u> (which the IP_address could be the ZyWALL's LAN or DMZ or WAN IP address depending on server access setting).

REMOTE MAI	NAGEMENT					
www	SSH	TELNET	FTP	SNMP	DNS	CNM
LITTEC						
ппр						_
Server	Certificate	auto_genera	ated_self_signed_cert	🗾 (See <u>My Certific</u>	ates)	
🗆 Au	thenticate Client Certi	ficates (See <u>Truste</u>	d CAs)			
Server	Port	8443				
Server	Access	🔽 LAN 🔽	WAN1 🔽 WAN2	🗸 DMZ 🔽 WLAN		
Secure	Client IP Address	💿 all 💿	Selected 0	. 0 . 0 . 0	_	
HTTO						
nite						
Server	Port	80				
Server	Access	🔽 LAN 🔽	WAN1 🔽 WAN2	🔽 DMZ 🔽 WLAN		
Secure	e Client IP Address	💿 all 🕥	Selected 0	0 , 0 , 0		
Note 1 Note 2	: For <u>UPnP</u> to function : You may also need t	normally, the HTTP to create a <u>Firewall</u>	service must be a rule.	vailable for LAN com	nputers using UPnP.	
		Apply		Reset		

Note: However, if you have configured a port-forwarding-rule 443 to a web server. We would suggest to utilize another WAN IP address of ZyWALL UTM device for ZyWALL SSL10's access.

For example, if you have configured WAN1 IP forward port 443 to another web server, (ex. 192.168.3.10). We could use WAN2 interface (ex. IP address is 10.59.1.30) to forward 443 to ZyWALL SSL10 as following figure.

Por W	t Forwa 'AN Inter	rding Rules face	0	WAN 2 💌								
D	efault Se	erver		0,0,0	0.0		Go	To Pa	ge 1	•		
#	Active	Name	Incon	ning Port(s)	Port	Translation	Se	erver	IP 4	Add	res	5
- C		to-SSL10	443	- 443	443	- 443	192	. 168		3		2
2			0	- 0	0	- 0	0	. 0		0	•	0
3			0	- 0	0	- 0	0	. 0		0		0
4			0	- 0	0	- 0	0	. 0		0		0
5			0	- 0	0	- 0	0	. 0		0		0
6			0	- 0	0	- 0	0	. 0		0		0
7			0	- 0	0	- 0	0	. 0		0		0
8			0	- 0	0	- 0	0	. 0		0		0
9			0	- 0	0	- 0	0	. 0		0		0
10			0	- 0	0	- 0	0	. 0		0		0
N	ote 1: Yo	u may also r	eed to cre	ate a Firewall rule								

Security Policy Configuration for SSL VPN traffic on the ZyWALL A

1). Switch to SECURITY > FIREWALL > Default Rule configuration page. Remember to turn on the firewall global switch otherwise all firewall ACL won't actually take effect on inspecting the packet. We allow the SSL VPN traffic to be forwarded to ZyWALL SSL10 at DMZ network. Thus, we **Drop** all traffic except SSL traffic from WAN to DMZ network. The exception is configured at the next step (2).

Default Rule	Rule	e Summary	Anti	-Probing		Thresho	ld	Servi	ce		
Default Rule	Default Rule Setup										
 Enable Firewall Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.) 											
From	Го	LAN		WAN		٩D	ız	wı	.AN	VP	И
LAN		Permit 😽 📃		Permit 💌		Permit	M 🗌	Permit	M 🗆	Permit	✓
WAN		Drop 💉 🗹		Drop 😽	~	Drop	Y 🗹	Drop	🖌 🗹	Drop	✓
DMZ		Drop 😽 🗹		Permit 💌		Drop	Y 🗹	Permit	Y	Permit	✓
WLAN		Drop 💉 🗹		Drop 💉	~	Drop	~	Drop	🖌 🔽	Drop	✓
¥PN		Permit 💌 🗌		Permit 💌		Permit	×	Permit	M 🗌	Permit	✓
									* 🔽	Log	

 Switch to Rule Summary page and select the packet direction from WAN to DMZ then insert a dedicate rule to allow any host to access the ZyWALL SSL10 via service type "HTTPS" (port 443).

FIREWALL		
Default Rule Rule Summar	y Anti-Probing Threshold Service	
Rule Summary		
Firewall Rules Storage Space	e in Use	
0%		100%
Packet Direction: LAN to LAN Default Policy: Per LAN to UAN LAN to UMA # Name Activ WAN to UMA Move rule 1 WAN to WA MOVE rule 1 WAN to WA DMZ to UAN DMZ to UAN	N / ZYWALL I / ZYWALL I I / ZYWALL I I I I I I I I I I I I I I I I I I	.og Modify

3) ZyWALL also can inspect packet/mails from WAN to DMZ by IDP/AV and AS features.

The configuration is similar to the firewall rule setting. There is a traffic direction matrix available in IDP/AV and AS General configuration page. Used the check box to decide if the traffic from WAN to DMZ needs to be inspected by scan engine.

ZvXEL							
HOME	INTRUSION	DETECTION	AND PI	REVENTI	ON		
REGISTRATION	General	Signature		Jpdate	Backup & Re:	store	
NETWORK 🛛	General 9	etup					
SECURITY 💌		la Intrucian Datacti	on and Droug	otion			
FIREWALL	Turb	o Card	Installed				
IDP ANTI-VIRUS					DN7		UDV
ANTI-SPAM			LAN	WAN	UMZ	WLAN	¥PN
CONTENT FILTER	From						
VPN		AN	✓				
CERTIFICATES	W	AN	V	V			
AUTH SERVER	C	MZ 🔳	V				
ADVANCED 🛛	W	LAN					
REPORTS 💌	×	PN	 Image: A start of the start of				
LOGS							
MAINTENANCE							
			[Apply	Reset]	
LOCOUT							

4. Best Practice: Stronger Password Security

Sometimes, your password may be compromised by people-in-the-back or by brute-attack. There are many ways to strong your password like you use a very long (ex.12-digit password) or a hard-to-guess password(ex. %#@9kersy62). ZyWALL SSL10 provides another solution with two-factor authentication. It's with an authenex server and token kits. User needs to enter not only the username and password but also the numbers generated from a trusted token. Without entering a valid number from token, user will always fail to log in.

4.1 Using Two-factor authentication solution to provide



stronger (FIPS 140 compliant) security: SSL10+Authenex

To achieve the scenario, we need to complete following tasks.

- Configure the ZyWALL SSL10 to use external RADIUS server for user authentication
- Configure the Authenex Server to accept the communication with ZyWALL SSL10 and assign the token bound with the user
- Simulate the access from a remote user

Configuration on ZyWALL SSL10

Step1. Create a group

Note: To use two-factor authentication, it's required to create a "group", rather than to create a "user".

1). Go to GUI > User/Group > Group, create a group by clicking the add icon.

	Vser/Group > Grou	p		
Status	User Grou	P		
ZyWALL SSL 10 Registration	Configuratio	n		
Bystem	#	Group Name	Member	(the second seco
User/Group				
- SSL - Object				

2). In this example, we create the group "testzywall" and choose the member from the AAA server as following figure. Click **OK**.

Name	testzywall	
ember		
💿 Group in the AAA Server		
O Select members		
Available Member		Selected Member(s)
aaaa	>>	=== Empty ===
	66	
		<u></u>
	OK	Cancel

Step2. Create a File Sharing

1). Go to GUI > Object > SSL Application, create one application rule by clicking the add icon.

- User/Group	Dbject > SSL Application	1		
- Object				
- VPN Network	SSL Application C	onfiguration		
- Endpoint Securit	Name	Address	Туре	
- Nonitor				

2). Choose type with **File_Sharing** and fill out the FTP server's IP address as following. Fill out the file server information as following. Click **OK** then.

Object		
Туре	File Sharing	
Add File Sharing		
Display Name	AD_En	
Address	172.23.32.15 Fileserver)	(ex:192.168.1.1 or
Shared Folder	Tools	(ex:Fileshare/dir1/dir2)
	P	
	Ok Cancel	

Step3. Setup AAA server

1) Go to GUI > System > AAA Server, choose **RADIUS** for the server type and fill out the other information as following. Click **OK** then.

2	System > AAA Server	
Status	r.	
ZyWALL SSL 10 Registration	Configuration	
System	Server Type	RADIUS 💌
- WAN	Server Address	172.23.32.44
- Certificate	Server Port	1812
- AAA Server	Server Timeout	60 sec
- Host Name - User/Group	Server Secret	•••••
- SSL	Retype Server Secret	•••••
🕀 Object	NAS Identifier	1
- Monitor ⊕Maintenance	Retry Count	5
		Ok Cancel

Step3. Create a SSL policy

1). Go to GUI > SSL > Policy, create a SSL policy by clicking the add icon.

- AAA Server	Policy	Access Cont	trol 📔 Global Se	etting		
Host Name User/Group –	List of	Policy				
SSL	#	Policy Name	User/Group	SSL Application	VPN Network	•
Jbject						

Check the user and the file sharing application that we just created. Click Ok.

Remote_auth
User/Group Name
🔽 testzywall
n authentication
End Point Security Name
sec
P AD_UI
der
ι ασταυπ
Ok Cancel

Configuration on Authenex Server

1). Connect to the Authenex Server via <u>http://IP-address:8080/asas/</u> where the IP address is the server's IP address you can reach from your network. If you access the server from the same host, you could use "localhost" or "127.0.0.1" for the IP address. After the IP address, append with ":8080/asas/" where the 8080 is the server's default port number.

Login the server by type the password you set.

3 1		
************************************	487 - Microsoft Internet Explorer	
(3 ±−具 + ⊙ + ≤ ≤] 🕜 🔑 搜尋 😚 荻的最愛 🕑 媒體 🚱 🔯 🗟	
網址(D) 🕘 http://127.0.0.1:808	D80/asas/	
Login open all close all	ASAS Web Mana	gement Console v3.0.0.0
ASAS Web Management	ASAS Web Management Console Login	
B-Reports	Please login using your A-Key and password below	
⊞-Manage A-Keys ⊞-Manage Users ⊞-Server Configuration	A-Key Password : •••••• Login	
Applet AKeyApplet started		

2). Go to Server Configuration > Add NAS Entry, create a NAS Entry by filling out the ZyWALL SSL10's information as following figure. Click **Add** button then.

Logout	Authenex"	ASAS Web Management Console v3.0.0.0		
open all close all	Strong Authentication & Encryption Applications			
ASAS Web Management Reports Manage A-Keys	Add NAS Entry Name	zywallssi10		
Search A-Keys Set A-Key Password Assign A-Keys	NAS Information			
-Manage Users -Search Users	IP Address	172.23.32.119		
Add User Import Users	Shared Secret	•••••		
Add/Edit Groups	Confirm Shared Secret	•••••		
Import Groups/Users	Group Information			
E-NAS Entries	RADIUS Attribute	11		
	Group Option G Single group. F C Single group. Multiple groups C Multiple groups	Format: eng Format: KEY=eng s. Format: eng;salse;acct, Grou s. Format: KEY=eng;salse;acct,	ıp Delimiter ; Group Delimiter ;	
	Group KEY	testzywall		
	Additional Information	ers 🗖 Sunnort Perhallenge		
	- Igible of Kildwir os		Clear	

Note: It's mandatory to set "11" for the field of RADIUS Attribute to ensure the communication properly between ZyWALL SSL10 and the Authenex server.

3). Go to Manage Users > Add User, create a user 'guest' and binds it with the group 'testzywall' and the resource 'zywallssl10' we just created. Click **Add** button.

Logout	Authenex	-	ASAS Web Ma
open all close all	Strong Authentication & Encryption Applications		215215 1105 1110
ASAS Web Management Reports Manage A-Keys Set A-Keys Set A-Key Password Assign A-Keys	Add User Page Add User below. Login Id Last Name First Name Description	guest	
Manage Users Manage Users Add User Import Users Manage Groups Add/Edit Groups Map Dynamic Groups/Users	Select group(s)	testzywall	
Server Configuration NAS Entries Add NAS Entry DAP Servers View License Info	Resource(s) To Allow	zywaliss!10	_Clear [Add]

Then edit the user and check the Assign only Users A-Keys option. Click Update User

button.

	Undete weer helewy			
1 Reports	opdate user below.			
⊐ Manage A-Keys				
Search A-Keys	Login Id	guest		
Set A-Key Password	Last Name			
Assign A-Keys	First Name			
B Manage Users	Description			
Search Users	Description			
Add User				
Import Users		Group(s) Selected	Group(s) Available	
Manage Groups				-
-Add/Edit Groups		testzywali	-> IBetaAuthenex	
-Map Dynamic Groups				
Import Groups/Users			<-	
Server Configuration				
NAS Entries				
Search NAS Entries		<i>k</i>		
Add NAS Entry		Resource(s) Allowed	Resource(s) Denied	
E LDAP Servers				~
View License Info		zywalissi10	-> iBeta	
			BBBBB	
			test	
		1	I	
	Assign a new A-Key to this user:			
	Assign only Users A-Keys			
	Get Unassigned A-Key			
	Make A-Key Active when assigned	Γ		
			-	1
			Reset Values	Update User

4). Go to Manage A-Keys > Assign A-Keys. Bind a certain token's A-key to the user.

Logout	Authenex"	ASAS Web Management Console v3.0.0.0	
open an i ciose an	Strong Authentication & Encryption Applications	<u> </u>	
ASAS Web Management	Assign A-Keys		
t Reports	Either:	uindemend collections available # Key Olick #collan	
🖨 Manage A-Keys	- Select a single user from the user w	ad user below by clicking 'Automatically Assign All'	
Search A-Keys	Please choose both a User and an A	Akey before pressing the 'Assign' button.	
Set A-Key Password	Only show keys that have User privile	erres 🔽 Artivate A-Key when assigned 🔽 Select	
Assign A-Keys	enij eleti koje klatitare obel plilite		
⊟ Manage Users			
Search Users	sslauthenex - ,	71086858 [User]	<u> </u>
Add User	guest - ,	71086859 [User]	
- Import Users		73009809 [User]	
E-Manage Groups		73009014 [User]	
Add/Edit Groups		73009015 [User]	
Man Dynamia Crouns		73009817 [User]	
Tasset Crows (Users		73009819 [User]	
- Import Groups/osers		[73009824 [User]	
Server Configuration		73009825 [User]	
E-NAS Entries		73009826 [User]	
Search NAS Entries		73009827 [User]	
Add NAS Entry		73009828 [User]	
E-LDAP Servers		73009829 [User]	
····· View License Info		73009830 [User]	
		[73009831 [User]	
		[73009832 [User]	
		[73009833 [User]	
		[73009834 [User]	
		1/2009020 [USBI]	
		Clear Autom	atically Assign all Assign

5). Go to Manage A-Keys > Search A-Keys, search the user to make sure the setting is done as following figure.

Logout open all close all	ASAS Web Management Console v3.0.0.0								
ACAC Web Merseners	A-Key Management								
H-Reports	Please select a range of ESN numbers to search from.								
🖹 Manage A-Keys	From ESN	To ESN	Enabled All	Registered	All	Clear	Search		
Search A-Keys	ESN	User Information		Access Level	Active	Registered	Enabled	Delete	
Set A-Key Password	71086819	pga eddy , U	nassign	User 💌	N	F	V	Delete	
Assign A-Keys	73009836	pm yvonne ;	Unassign	User 💌	N	Γ	M	Delete	
Search Users	71086838	pm justin , Ur	assign	User 💌	2	F	1V	Delete	
Add User	71086837	pm jerry , Un	assign	User 💌	N		V	Delete	
Import Users	73009839	pm jason , Ur	nassign	User 💌	2	F		Delete	
E-Manage Groups	71086836	pm jacky , Ur	assign	User 💌	2		V	Delete	
- Add/Edit Groups	71086839	pm felix , Una	assign	User 💌	2		V	Delete	
Map Dynamic Groups	73009837	pm chiron . U	nassian	User 💌		E	V	Delete	
Server Configuration	73009819	quest Unass	iign	User 💌	N	I	V	Delete	
- NAS Entries	10000001	Not Assigned (Click to	Assign)	User 💌		F		Delete	
Search NAS Entries	1000002	Not Assigned (Click to	Assign)	User 💌			I	Delete	
Add NAS Entry	71086800	Not Assigned (Click to	Assign)	User 💌			Γ	Delete	
E-LDAP Servers	71086801	Not Assigned (Click to	Assign)	User 💌	Г	E		Delete	
····· View License Info	71086802	Not Assigned (Click to	Assign)	User 💌				Delete	
	71086803	Not Assigned (Click to	Assign)	User 💌			—	Delete	
	71086804	Not Assigned (Click to	Assign)	User				Delete	
	71086805	Not Assigned (Click to	Assign)	User 💌			F	Delete	
	71086806	Not Assigned (Click to	Assign)	User 💌		F	F	Delete	
	71086807	Not Assigned (Click to	Assign)	User 💌				Delete	
	71086808	Not Assigned (Click to	Assign)	User 💌			П	Delete	
				Export to CSV E	revious <u>Next</u>	Reset Val	ues 🚺 Up	date Values	

6). Restart the service by choose your PC's Start > Authenex > ASAS_3.0 > Restart

Authenex Radius Server

🥨 Windows Catalog 🍪 Windows Update				
m Apache Tomcat 5.5	•			
🧰 Authenex	•	asas_3.0	• 6) DBImport
🛅 Ethereal	•	🖡 Assign Password to A-Key		Edit authserver.properties
🛅 FileZilla	→T			Edit config.properties
🛅 Microsoft Exchange	•	×	5	📱 Restart Authenex Radius Server
🛅 Symantec Client Security	r ▶	N:	-	
🛗 Windows Support Tools	•			

Access from a remote user

1). Login to ZyWALL SSL10 by typing the username, password and the six number generated from your token.

	ZyWALL SSL 10	
	Welcome to ZyWALL SSL 10 Enter User Name/password and click to login.	
	() User Name: testzywall	enter the six numbe
	🖻 Password: 🚥	generated from you
🗎 On	e-Time Password: ••••••	Optional)
()	nax. 30 alphanumeric, printable characters and no spac	es)
	I am connecting via my own computer.	
	C I am connecting via Public computer.	
Note:		
Please enabl	e Javascript on your Browser.	

2). After successful login, you could see the file sharing link from the interface. Double click it to access the file server.

-1

Elle Sharing	
_ ric ondring	
	and the second s
AD En	
nv_LII	
	-
	-
	-
	1000
	_

5. FAQ

A. ZyWALL General FAQ

A01. How to access ZyWALL SSL10 web GUI?

You can connect your PC to ZyWALL SSL10 LAN port with Ethernet cable and get the IP address automatically from DHCP. Open web browser and connect to its GUI through IP address (default is <u>http://192.168.1.1</u>). The default administration username is "**admin**", and password is "**1234**".

A02. What do I need to use the ZyWALL?

You need an xDSL modem or cable modem with an Ethernet port to use the ZyWALL. The ZyWALL has two Ethernet ports: LAN port and WAN port. You should connect the computer to the LAN port and connect the external modem to the WAN port. If the ISP uses PPPoE Authentication you need the user account to enter in the ZyWALL.

A03. What is PPPoE?

PPPoE stands for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.
A05. Does the ZyWALL support PPPoE?

Yes. The ZyWALL supports PPPoE encapsulation.

A06. How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the ZyWALL if you are using PPPoE service provided by your ISP.

A07. Why does my Internet Service Provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

A08. How can I configure the ZyWALL?

- Telnet remote management- CLI command line
- Web browser- web server embedded for easy configurations

A09. What can we do with ZyWALL?

Browse the World Wide Web (WWW), send and receive individual e-mail, and up/download data on the internet. These are just a few of many benefits you can enjoy when you put the whole office on-line with the ZyWALL Internet Access Sharing Router.

A10. Does ZyWALL support dynamic IP addressing?

The ZyWALL supports both static and dynamic IP address from ISP.

A11. What is the difference between the internal IP and the real IP from my

ISP?

Internal IPs is sometimes referred to as virtual IPs. They are a group of up to 255 IPs that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP from ISP, instead, can be recognized or pinged by another real IP on the internet. The ZyWALL Internet Access Sharing Router works like an intelligent router that route between the virtual IP and the real IP.

A12. How does e-mail work through the ZyWALL?

It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through ZyWALL Internet Access Sharing Router using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right. If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address. Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through ZyWALL Internet Access Sharing Router using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access right.

A13. What DHCP capability does the ZyWALL support?

The ZyWALL supports DHCP client on the WAN port and DHCP server on the LAN port. The ZyWALL's DHCP client allows it to get the Internet IP address from ISP automatically. The ZyWALL's DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

A14. How do I used the reset button, more over what field of parameter will be

reset by reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 10 second, the unit will be reset. When the reset button is pressed the device's all parameter will be reset back to factory default.

The default IP address is 192.168.1.1, Password 1234, ESSID Wireless.

A15. My ZyWALL can not get an IP address from the ISP to connect to the

Internet, what can I do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

- 1. Check if the 'MAC address' is valid
- 2. Check if the 'Host Name' is valid, e.g., @home

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or the ZyWALL is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP. The ZyWALL supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in WAN menu of the ZyWALL web configurator.

2. Your ISP checks the 'Host Name'

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer Name' of the PC in the 'Networking' settings. When the ZyWALL is attached to the cable modem to connect to the ISP, we should configure this host name in the ZyWALL's system (menu 1).

A16. What is BOOTP/DHCP?

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the ZyWALL Internet Access Sharing Router is a BOOTP/DHCP server. WinXP/2000 and WinNT clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IP or utilize BOOTP/DHCP to request an IP address.

B. Firmware Upgrade FAQ

B01. How to perform the firmware upgrade on ZyWALL SSL10?

It could be done by web GUI(menu **Maintenance** > **Firmware**) or by FTP (ftp to the ZyWALL SSL10's IP address ex. <u>ftp://192.168.1.1</u> and upgrade the firmware by using command "put 1.00(AQH.0)C0.bin ras" which the "1.00(AQH.0)C0.bin" is the firmware file name. After firmware upgrade, the system will restart to take the new firmware effect.

C. Registration for Service Activation FAQ

C01. Why do I have to register?

- 1. If you wanted to use the free SSL-VPN of ZyWALL, your have to activate it from within myZyXEL.com. After activating, it will allow up to 10 users to login via SSL connection.
- 2. If you purchased iCard for a security service, you must activate the security service from within myZyXEL.com. You could upgrade the license to allow up to 25 users to login via SSL connection.

C02. In addition to registration, what can I do with myZyXEL.com?

- 1. Access firmware and security service updates.
- 2. Get ZyWALL alerts on services, firmware, and products.
- 3. Manage (activate, change or delete) your ZyWALL security services online.

In summary, myZyXEL.com delivers a convenient, centralized way to register all your ZyWALL security appliances and security services. It eliminates the hassle of registering individual ZyWALL appliances and upgrades to streamline the management of all your ZyWALL security services.

Instead of registering each ZyWALL product individually, using myZyXEL.com you have a

single user profile where you can manage all your product registration and service activation.

C03. How to activate the SSL-VPN license?

You need to buy an iCard for SSL-VPN 10 notes or 25 notes first to get a valid license key. Login the ZyWALL SSL10 via GUI > **Registration** menu. Enter your user account information and the license key. It will activate the SSL-VPN applications for 10 users or 25 users.

D. SSL VPN FAQ

D01. Matrix table for the SSL VPN terms

Modes for SSL VPN	Corresponding setting in ZyWALL SSL10	
Reverse Proxy Mode	Choose Web-Application type or File-Sharing type in GUI	
	menu SSL application	
Port Forwarding Mode	Choose Application type in GUI menu SSL application	
Full Tunnel Mode / Network	Configure in GUI menu VPN network and Private IP Pool.	
Extension Mode	Or configure SSL VPN via Wizard.	

D02. Why cannot some web pages displayed correctly?

There are some notes when you are using Reverse Proxy mode.

(1)The URL-rewriting method does not work perfect on all case. For example it can not rewrite the URL in JavaScript, VBScript, and dynamically constructed URLs.

(2)Some applications, like Applets, Flash, do not work since them need to connect to the external server.

(3)We cannot guarantee every web pages in the world to be able to display correctly.

We recommend using full tunneling mode to display all pages properly.

D03. SSL VPN vs. PPTP VPN?

Here we compare the characteristic between SSL VPN and PPTP VPN.

	SSL VPN	PPTP VPN
Users need to Pre-Install	No (Using browser)	No (Using native MS client)
Software?		
Users need to configure?	No	Yes (at least 5 steps to setup)
Has Access Control?	Yes	No
Can check the Endpoint's	Yes	No
Security?		

D04. What is the order of user authentication?

For user authentication, system will check the local database on ZyWALL SSL 10 > User/Group first. If no any user or group matched, it will check the external database which is defined in AAA server.

E. EPC(End Point Check) FAQ

E1. What is EPC on ZyWALL SSL10?

EPC stands for End Point Check(a.k.a. EPS-End Point Security). The EPC is a centrally managed method of monitoring and maintaining client-system security. It will verify that the client PC is compliant with security policy defined by administrator before granting access.

The ZyWALL SSL 10 provides endpoint security features such as client integrity checking, browser cache cleaner, and support for many versions of antivirus and firewall software. If the protection configured requires a specific process not to be running, the system can ask the user to halt the process.

E2. What are the checking items of EPC on ZyWALL SSL 10?

The EPC will follow the security policy defined by administrator to check the client's device to ensure the device is secure before it connects to the network.

On ZyWALL SSL 10, the checking items include:

- [1] General checks(Windows platform only)
- Operating system service pack versions
- Security patches
- Browser versions
- Application versions and patch versions
- Personal Firewalls (versions, active/inactive)
- Anti-Virus software (versions, active/inactive)
- Rogue processes

[2] Customizable checks(Windows platform only)

- Registry entries
- File system entries
- Process table entries
- [3] Session Information Protection
- Cleaning browser caches, history, cookies, credentials (IE only)
- Disabling auto-completion
- [4] Web-page protection
- Encrypted view-source (IE only)