2013

ZyWALL Series Support Note V1





4/1/2013

Scenario 1 - Restricting Bandwidth Management Priority for Traffic

1.1 Application Scenario

In an enterprise network, there are various types of traffic. However, most company's Internet bandwidth is limited. All traffic will contend for it and may result in some important traffic, for example. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. A ZyWALL provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria. Here is the example to limit FTP traffic by BWM.



1.2 Configuration Guide

Network conditions:

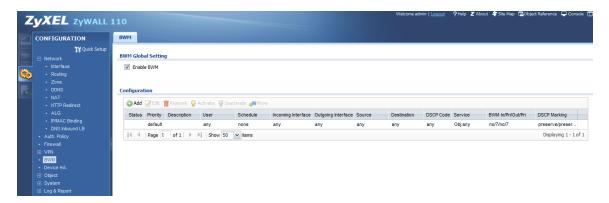
- WAN download bandwidth: 2M
- WAN upload bandwidth: 1M

Goals to achieve:

Restrict FTP download/upload bandwidth to 1000/500 kbps and set priority of FTP traffic to 4 for all users.

ZyWALL configuration:

Step 1: Configuration > BWM > check "Enable BWM"



Step 2: Configuration > BWM > Select the "Add"

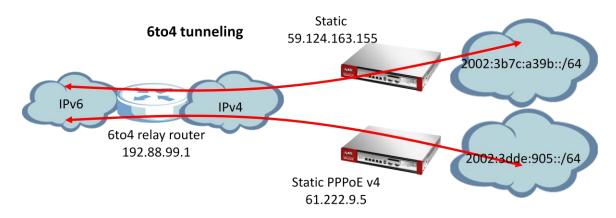
- (1) Select the "WAN trunk interface" in **incoming** and **outgoing** interface
- (2) And service object select the "FTP".
- (3) Limit the **inbound** 1000Kbps and **Outbound** 500Kbps and the all of the priority is **4**.

Z	YXEL ZYWALL :	110				Welcome admin <u>Logout</u>	?Help Z About 4
	CONFIGURATION	BWM	Address				
	TH Quick Setup		Add Policy Create new Object +				? ×
		BWM Global					A
Ô		🔽 Enable B		any 💌			
9.Q.			Schedule:	none			
		Configuration		TEM_DEFAULT_WAN_TRUNK ~			
		🕜 Add 📝	Outgoing Interface:	TEM_DEFAULT_WAN_TRUNK V			
		Status P	Source:	any			BW
		d	Destination:	any			no/
		4 4 P	DSCP Code:	any			
			Service Object:	FTP 👻			
	+ BWM		DSCP Marking				
			DSCP Marking	Inbound Marking: preserve 🗸			=
				Outbound Marking: preserve 💙			
			Bandwidth Shaping				
			Guaranteed Bandwidth	Inbound: 1000 kbps (0 : disabled)	Priority:	4	
				Maximize Bandwidth Usage	Maximum:	0 kbps	
				Outbound: 500 kbps (0 : disabled)	Priority:	4	
				Maximize Bandwidth Usage	Maximum:	0 kbps	
					- wollight.	v kups	-
				III			
						ок с	ancel

Scenario 2 - Assign IPv6 to your LAN to access remote IPv6 network

2.1 Application Scenario

Nowadays, more and more Internet service providers provide IPv6 environment. With IPv6 feature enabled on ZyWALL, it can assign an IPv6 to clients under it and pass IPv6 traffic through IPv4 environment to access remote IPv6 network.



2.2 6to4 IP Translate Introduction

Network conditions:

ZyWALL:

WAN1: 59.124.163.155(Static)

Goal to achieve:

A ZyWALL will assign IPv6 IP address to the clients behind it, and the clients can access remote IPv6 network by using the ZyWALL 6to4 tunnel.

ZyWALL Configuration:

Step 1: Configuration > System > IPv6 > Click Enable IPv6

Z	YXEL ZYWALL	110
9	CONFIGURATION	IPv6
	📲 Quick Setup	ch-h-lc-w
-	Network	Global Setting
	+ Auth. Policy	Enable IPv6
Ges	+ Firewall	
	⊕ VPN	
R.	+ BWM	
	+ Device HA	
	⊕ Object	
	🗆 System	
	+ Host Name	
	 USB Storage 	
	+ Date/Time	
	+ Console Speed	
	+ DNS	
	+ WWW	
	+ SSH	
	+ TELNET	
	+ FTP	
	+ SNMP	
	+ Language	
	+ IPv6	

Step 2: Setting the static IP on WAN1

	CONFIGURATION	Port Role Ethe	ernet PPP Cellul	lar Tunnel VLAN Bridge Trunk	
	TY Quick Setup				
	Network	Configuration			
	+ Interface	📝 Edit 🍵 Rem	ove 🧔 Activate 😡 Inacl	tivate 🖼 Create Virtual Interface 📴 Object Reference	
0	 Routing + Zone 	# Status	Name	IP Address	Mask
R .	+ DDNS	1 😡	wan1	STATIC 59.124.163.155	255.255.255.224
	NAT	2 😡	wan2	DHCP 0.0.0.0	0.0.0.0
	HTTP Redirect ALG	3 🧕	opt	STATIC 0.0.0.0	0.0.0.0
	+ IP/MAC Binding	4 🤬	lan1	STATIC 192.168.1.1	255.255.255.0
		5 🤬	lan2	STATIC 192.168.2.1	255.255.255.0
	+ Firewall	6 😡	ext-wlan	STATIC 10.59.0.1	255.255.255.0
	⊕ VPN	7 😡	dmz	STATIC 192.168.3.1	255.255.255.0
	BWM Device HA	🕅 🔍 🛛 Page	1 of 1 > > Sho	w 50 🗸 items	

Step 3: Setting IPv6 IP address on LAN1

 Go to Configuration > Interface > Ethernet > double click LAN1 interface in IPv6 configuration.

Zedit Ethernet		
IPv6 View 🔻 🗐 Hide Advanced Settings 🔠 Creat	te new Object	
General Settings		
Enable Interface		
General IPv6 Setting		
📝 Enable IPv6 🚺		
Interface Properties		
Interface Type:	internal	
Interface Name:	lan 1	
Port:	P4	
Zone:	LAN1	
MAC Address:	00:13:49:00:00:04	
Description:		(Optional)

(2) Convert WAN1 IP address to hexadecimal

Check Enable Stateless Address Auto-configuration (SLAAC) box and enter 2002:3b7c:a39b::/64 in the prefix table.

(3) Check IPv6 Router Advertisement Setting box and add the prefix in the Advertised Prefix Table.

Tachia Chatalana Address Auto as		
Enable Stateless Address Auto-co	nfiguration (SLAAC)	
Link-Local Address:	fe80::213:49ff:fe00:4/64	
IPv6 Address/Prefix Length:	2002:3b7c:a39b::/64 (Optional)	
DHCPv6 Setting		
DHCPv6:	N/A 🗸	
IPv6 Router Advertisement Settin	9	
IPv6 Router Advertisement Settin	g	
	9	
Enable Router Advertisement		
 Enable Router Advertisement Router Preference: 	g Medium	
Enable Router Advertisement		
 Enable Router Advertisement Router Preference: 	Medium	
 Enable Router Advertisement Router Preference: 	Medium Y Add ZEdit TRemove	

Step 4: Enable 6 to 4 tunnel.

(1) Go to Configuration > Interface > Tunnel > Click Add button

0													
CONFIGURATION	P	ort Role	Ether	net	PPP	Cellular	Tunnel	VLAN	Bridge	Trunk			
🙀 Quick Setup													
Network	-	Ionfigur	ation										
Interface Routing		🔘 Adı	d 📝 Edit	👕 Ren	nove <table-cell></table-cell>	Activate 🧃	Inactivate	Object R	eference				
 Routing Zone 		#	Status	Name		IP Ac	Idress			Tunnel Mode	My Address	Remote Gateway Addre	955
DDNS													
• NAT		14 4	Page	1 of	1 🕨	▶ Show	50 🗸 item	5					No data to display

- (2) Select the 6to4 in that Tunnel Mode
- (3) Check the Prefix in the 6tp4 tunnel Parameter
- (4) Select the WAN1 interface as the gateway in the Gateway Setting

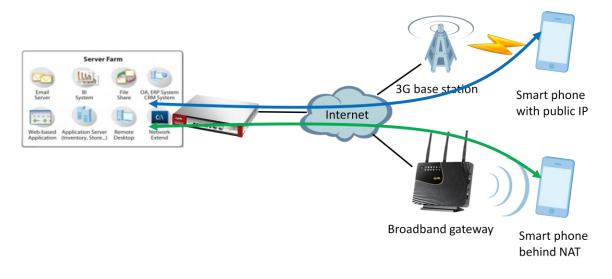
🔾 Add Tunnel	?
Show Advanced Settings	
e leur	
General Settings	
Enable	
Interface Properties	
Interface Name:	tunnel0
Zone:	TUNNEL 🗸
Tunnel Mode:	6to4 🗸
IPv6 Address Assignment	
IPv6 Address/Prefix Length:	(Optional)
Metric:	0 (0-15)
6to4 Tunnel Parameter	
6to4 Prefix:	2002::/16
Relay Router:	192.88.99.1 (Optional)
NOTE: traffic destinated to the n	on-6to4 prefix domain tunnels to the relay router
~	
Gateway Settings	
My Address	
Interface	wan1 💙 Static 59. 124. 163. 155/255. 255. 254
IP Address	0.0.0.0

After these configuration steps, connect your computer to the device and check that your computer received an IPv6 IP address from tunnel.

Scenario 3 – Dialing up L2TP VPN connection to ZyWALL by using iOS/Android mobile device

3.1 Application Scenario

Smart phone become increasingly popular with consumers. Though it brings us much more convenience, but also brings security concerns. A ZyWALL is compatible with iOS/Android mobile devices to establish L2TP VPN connection, provide secure and private mobile data transferring no matter if your mobile devices is behind NAT. In the following diagram, outside employees need to visit an internal website in Intranet, they can just dial up L2TP VPN to ZyWALL and access needed internal resource.



3.2 Configuration Guide

Network conditions:

ZyWALL:

- WAN1 IP: 59.124.163.150
- Local subnet: 192.168.1.0/24
- L2TP pool:192.168.100.0/24
- Intranet website: http://info.zyxel.com

iOS/Android mobile device:

- IP: 116.59.252.188 (3G mobile network)
- IP: 10.59.3.103 (Behind NAT device)

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: 3DES/3DES/DES Authentication algorithm:
- Authentication algorithm:

Phase 2:

- Encapsulation Mode: Transport mode
- Active protocol: ESP
- Encryption algorithm: 3DES/3DES/DES

SHA1/MD5/SHA1

- SHA1/MD5/SHA1 Perfect Forward Secrecy: none
- Key group: DH1

Goals to achieve:

Build up an L2TP over IPSec VPN tunnel for mobile users to access Intranet website.

ZyWALL configuration

Step 1: Click Configuration > VPN > IPSec VPN > VPN Gateway to visit VPN gateway configuration screen

CONFIGURATION	VPN Con	nection	VPN Gateway	Concentrator	Configuration Provisioning		
TH Quick Setup							
Network	Configu	iration					
 Interface 	(C) A	dd 📝 Edit	TRemove 😡 Ac	tivate 😡 Inactivat	e 📭 Object Reference		
 Routing 				0			
+ Zone	#	Status	Name		My Address	Secure Gateway	VPN Connection
+ DDNS	1	(g)	Default_L2TP_V	PN_GW	s wan1	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection
+ NAT		4 Dece	1 of 1 🕨 🕅	Chan Co			
 HTTP Redirect 	14	1 Page		Show So	tenis		

Step 2: Click the "Add" button to add a VPN gateway rule.

Step 3: Fill in the needed VPN gateway configuration.

eneral Settings			
V Enable			
VPN Gateway Name:	l2tp_gateway		
teway Settings			
/ Address	12		
Interface	wan1	 Static 59. 124. 163. 150/ 	255.255.255.224
🔘 Domain Name / IP			
er Gateway Address			
Static Address	Primary 0.0	0.0.0	
	Secondary 0.0	0.0.0	
Fall back to Primary Peer Ga	teway when possible		
Fall Back Check Interval:	300	(60-86400 seconds)	
Oynamic Address			
thentication			
Pre-Shared Key	12345678		
Certificate	default	×	
ocal ID Type:	IP	~	
Content:	0.0.0.0		
Peer ID Type:	Any	~	
Content:			
concerter			
ase 1 Settings			
12		(180 - 3000000 Seconds)	
A Life Time:	86400		
	Main	×	
Negotiation Mode:	Main		
legotiation Mode:	Constants.	Temove	
legotiation Mode:	Main	Temove	
egotiation Mode:	Main C Add ZEdit # Encryption	TRemove Authentication	
Negotiation Mode:	Main Add Edit # Encryption 1 3DES	Remove Authentication SHA1	
SA Life Time: Negotiation Mode: Proposal Key Group:	Main Add Edit Control Add Encryption Second Seco	Remove Authentication SHA1 MD5	
Negotiation Mode:	Main Add Ecryption 1 3DES 2 3DES	Remove Authentication SHA1 MD5	

CONFIGURATION	VPN Cor	nnection	VPN Gateway	Concentrator	Configuration Provisioning		
™ Quick Setup	Config	uration					
 Network Interface Routing 	© 4	vdd 📝 Edit	: 👕 Remove 💡 Ac	tivate 😡 Inactiva	ite 📴 Object Reference		
+ Zone	#	Status	Name		My Address	Secure Gateway	VPN Connection
	1	g	Default_L2TP_\	PN_GW	■ wan1	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection
	2	0	l2tp_gateway		s wan1	0.0.0.0, 0.0.0.0	
 HTTP Redirect ALG 		√ Page	1 of 1 > >	Show 50 🗸	items		

Step 4: Click **Configuration > VPN > IPSec VPN > VPN Connection** to visit the

configuration screen to set phase 2 rule

N Conn	nection	VPN Gateway	Concentrator	Configuration Provisioning				
bal Se	etting							
/ Use	Policy Rou	te to control dynam	ic IPSec rules					
			TD based on E					
1 Iana	ore "Don't F	ragment" setting in						
1 Igno	ore "Don't F	ragment" setting in	IP neader					
-		ragment" setting in	IP neader 🚺					
nfigura	ation		_	e 😪 Connect 🐼 Disconnect 🖡	Object Reference			
nfigura	ation d 📝 Edit	📺 Remove – 🥥 Act	_	e 🍓 Connect 🚱 Disconnect 🛽	Object Reference	-		
nfigura	ation		_	e 🚷 Connect 🚱 Disconnect 🛽 VPN Gateway	Object Reference	Encapsulation	Algorithm	Policy
nfigura	ation d 📝 Edit	TRemove Q Act	_	VPN Gateway		Encapsulation TRANSPORT	Algorithm 3DES/SHA1 3DES/MD5 DES/SHA1	Policy /any

Step 5: Click the "Add" button to add a VPN connection rule.

Step 6: Fill in the needed VPN connection configuration.

eneral Settings		
Z Enable	Provide and a second	
Connection Name:	L2TP_VPN	
Nailed-Up		
Enable Replay Detection		
Enable NetBIOS broadcast over IPSec MSS Adjustment		
MSS Adjustment O Custom Size	0	(200 - 1460 Bytes)
	0	(200 - 1460 Byres)
Auto		
PN Gateway		
Application Scenario		
Site-to-site		
Site-to-site with Dynamic Peer		
Remote Access (Server Role)		
Remote Access (Client Role)		
VPN Gateway:	l2tp_gateway	van10.0.0.0 0.0.0.0
Manual Key		
Manual Key		
My Address:		
Secure Gateway Address:		
SPI:	(256 - 4095)	
Encapsulation Mode:	Tunnel	*
Active Protocol:	ESP	~
Encryption Algorithm:		~
Authentication Algorithm:		~
Encryption Key:		
Authentication Key:	-	1
Muchon occupient Ney:		
olicy		
Local policy:	WAN1_IP	✓ HOST, 59.124.163.150
21 W		
hase 2 Setting		
SA Life Time:	86400	(180 - 3000000 Seconds)
Active Protocol:	ESP	×
Encapsulation:	Transport	*
Proposal	Add WEdit 🍵 Rer	STIDVS
		Authentication
	# Encryption 1 3DES	SHA1
	2 3DES	MD5
	3 DES	SHA1
Perfect Forward Secrecy (PFS):	none	~
elated Settings		
	1	
Zone:	IPSec_VPN	
onnectivity Check		
Enable Connectivity Check		
Check Method:	icmp	~
Check Period:		
	(5-30 Seconds	
Check Timeout:	(1-10 Seconds	ls)
	(1-10)	
Check Fail Tolerance:		(Domain Name or IP Address)
Check Fail Tolerance: Check This Address 		(Doniali Mane or IF Address)
	·	(Domain value or the Address)
Check This Address	·	(Domain Maine of the Address)
 Check This Address Check the First and Last IP Addre Log 	·	(Contraint value of the Address)
Check This Address Check the First and Last IP Addre Log hound/Outbound traffic NAT	·	
Check This Address Check the First and Last IP Addre Log hound/Outbound traffic NAT Outbound Traffic	·	(Woniai i vane of itr Poures)
Check This Address Check the First and Last IP Addre Log hound/Outbound traffic NAT Outbound Traffic Source NAT	ss in the Remote Policy	
Check This Address Check the First and Last IP Addre Log hound/Outbound traffic NAT Outbound Traffic Source NAT Source:	Please select one	×
Check This Address Check the First and Last IP Addre Log hoound/Outbound traffic NAT Outbound Traffic Source NAT Source: Destination:	Please select one	
Check This Address Check the First and Last IP Addre Log nbound/Outbound traffic NAT Outbound Traffic Source NAT Source: Destination: SNAT:	Please select one	×
Check This Address Check the First and Last IP Addre Log nbound/Outbound traffic NAT Outbound Traffic Source NAT Source IDestination: SNAT: Inbound Traffic	Please select one	× ×
Check This Address Check the First and Last IP Addre Log nound/Outbound traffic NAT Outbound Traffic Source NAT Source: Destination: SNAT: Inbound Traffic Source NAT	Please select one Please select one	× ×
Check This Address Check the First and Last IP Addre Log nbound/Outbound traffic NAT Outbound Traffic Source NAT Source IDestination: SNAT: Inbound Traffic	Please select one	× ×
Check This Address Check the First and Last IP Addre Log nound/Outbound traffic NAT Outbound Traffic Source NAT Source: Destination: SNAT: Inbound Traffic Source NAT	Please select one Please select one	
Check This Address Check the First and Last IP Addre Log nound/Outbound Traffic NAT Outbound Traffic Source NAT SNIT: Inbound Traffic Source NAT Source NAT Source:	Please select one Please select one Please select one Please select one	
Check This Address Check the First and Last IP Addre Log nound/Outbound traffic NAT Outbound Traffic Source NAT Source I Inbound Traffic Source NAT Source: Destination: Source: Destination:	Please select one Please select one Please select one Please select one Please select one	× × × ×
Check This Address Check the First and Last IP Addre Log nbound/Outbound traffic NAT Outbound Traffic Source: Destination: SNAT: Destination: SNAT: Destination: SNAT: Destination: SNAT: Destination: SNAT: Destination NAT	Please select one Please select one Please select one Please select one Please select one	× × × ×
Check This Address Check the First and Last IP Addre Log nbound/Outbound traffic NAT Outbound Traffic Source NAT Source NAT Source NAT Source NAT Source I Destination: Source SNAT;	Please select one Please select one Please select one Please select one Please select one	× × × ×

Step 7: Click **Configuration > VPN > L2TP VPN** to visit L2TP VPN configuration screen

Step 8: Create a address object for L2TP users

L2TP VPN				
📰 Show Advanced Settings 🔚 Create new Object	t₹			
General Settings				
Enable L2TP Over IPSec				
VPN Connection:	PIPASP SPIPE DODP			
	Create Address		?)	×
IP Address Pool:				•
Authentication Method:	Name:	L2TP_Pool		
Allowed User:	Address Type:	SUBNET	¥	
Kaan Aliya Timan	Network:	100 100 100 0		
Keep Alive Timer:	Network:	192.168.100.0		
First DNS Server (Optional):	Netmask:	255.255.255.0		
Second DNS Server (Optional):	Custom Defined	~		
		OK	Cancel	
First WINS Server (Optional):				
Second WINS Server (Optional):				

Step 9: Fill in the needed L2TP VPN connection configuration.

L2TP VPN				
🔲 Hide Advanced Settings 🔚 Create new	Object 🗸			
General Settings				
Enable L2TP Over IPSec				1
VPN Connection:	L2TP_VPN	*		
IP Address Pool:	L2TP_Pool	~		
Authentication Method:	default	~		
Authentication Server Certificate:	default	~		
Allowed User:	any	~		
Keep Alive Timer:	60 (1-180 secon	ıds)		
First DNS Server (Optional):	Custom Defined	~	192.168.1.1	
Second DNS Server (Optional):	Custom Defined	~	8.8.8.8	
First WINS Server (Optional):				
Second WINS Server (Optional):				

iOS mobile client configuration

Step 1: Settings > General > Network > Step VPN > Add configuration and insert needed L2TP VPN settings.

Step 2: Choose the VPN and turn on

Secret is the pre-shared key 12345678.

Cancel Add	Configura	tion Save	General	VPN
L2TP	PPTP	IPSec	VPN	OFF
Description	ı ZyWALL		Choose a Co	onfiguration
Server	59.124.163	.150	Iphone Custom	٥
Account	l2tpuser		Lv Custom	٥
RSA Secur	ID	OFF	Custom	٥
Password	•••••		Test2 Custom	٥
Secret	•••••		Test2222 Custom	2
Send All Tr	affic		Usg1000 Custom	٥
Proxy		Auto	✓ ZyWALL Custom	٥
Off	Manual	Auto	Add VPN	Configuration >

Step 3. Go to **Monitor > VPN Monitor > L2TP over IPSec** to check the L2TP session.

Session Monitor				
Current L2TP Session				
🗞 Disconnect 🔊 Refresh				
# 🔺 User Name	Hostname	Assigned IP	Public IP	
1 I2tpuser	-iPhone	192.168.100.1	116.59.252.188	
4 4 Page 1 of 1 ▶	▶ Show 50 v items		Displayin	g 1 - 1 of 1

Android mobile client configuration

Step 1: Settings > Wireless & networks > Step 2: Add VPN network VPN

🕼 🛜 .iil 💷 🛱 09:59	🖉 🫜 "III 💷 🛱 09:59
Wireless & networks	VPN
Airplane mode	Add VPN network
VPN	
Tethering & portable hotspot	
Internet pass-through Connect to the Internet via PC. Please plug in USB cable.	

Step 3: Select L2TP/IPSec PSK as the type and fill in the server address.

Step 4: Fill in the Pre-shared key 12345678 and click "Save".

	. <u>O</u> m	🕼 🛜 "📲 🖾 🗯 10:07	-	🕼 🛜 "📲 🏧 🖄 10:07
V	Edit VPN network		Edit VPN network	
Z C A	Name ZyWALL Type L2TP/IPSec PSK Server address 59.124.163.150 L2TP secret (not used) IPSec identifier		Server address 59.124.163.150 L2TP secret (not used) IPSec identifier (not used) IPSec pre-shared ke	
	Cancel	Save	Cancel	Save
	$\begin{array}{c} 2 \\ 3 \\ 4 \\ 5 \\ W \\ E \\ R \\ T \\ 7 \\ 4 \\ 5 \\ 7 \\ 7 \\ 7 \\ 7 \\ 7 \\ 7 \\ 7 \\ 7 \\ 7 \\ 7$	H J K L	$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ Q & W & E & R & T \\ \hline & & & & \\ P & & & & \\ A & S & D & F \\ \hline & & & & & \\ \hline & & & & & \\ \hline & & & &$	

Step 5: Click on "ZyWALL" to connect to the L2TP VPN. Fill in the L2TP password and click "Connect".

Step 6: Device will show connected when dial up successfully

-		🕼 🛜 💷 였 10:04	9	🕼 🛜II 💷 🗭 10:06
VF	PN		VPN	
Z	Connect to ZyWALL		ZyWALL Connected	
	Username			
А	l2tpuser		Add VPN network	
	Password			
	Save account in	nformation		
	Cancel	Connect		
1	2 3 4 5 ! @ # \$ % _ " ' () 1/2 : ,	6 7 8 9 0 6 & * ? / 0 - + ; ← . ABC ↓		

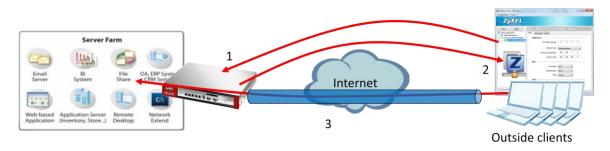
Step 7. Go to **Monitor > VPN Monitor > L2TP over IPSec** to check the L2TP session.

Session Monitor			
Current L2TP Session			
😪 Disconnect 🔊 Refresh			
# 🔺 User Name	Hostname	Assigned IP	Public IP
1 I2tpuser	anonymous	192.168.100.1	59.124.163.130
✓ Page 1 of 1 ▷ ▷ Sho	w 50 🗸 items		Displaying 1 - 1 of 1

Scenario 4 – One click Setup VPN connection to headquarter

4.1 Application Scenario

As an enterprise, employees often have business trip around the world. They might need to access the resource which inside headquarter during trip and it brings secure concerns. One of the solutions is to build a IPSec VPN tunnel to reach the purpose, but it has difficulty for non-technical employees and will increase work loading on network administrator to help them setup. A ZyWALL provides an EASY VPN solution to download a VPN configuration file from it and import the configuration file to build up the VPN connection.



- 1. Login ZyWALL via IPSec VPN client software for authentication.
- 2. Retrieve IPSec VPN configuration profile from ZyWALL.
- 3. Double click profile to build up IPSec VPN tunnel and access internal resource.

4.2 Configuration Guide

Network conditions:

ZyWALL:

- WAN 1 IP: 59.124.163.147
- Local subnet: 192.168.1.0/24

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: DES
- Authentication algorithm: MD5
- Key group: DH1

Outside user:

- IP: 114.16.87.56

Phase 2:

- Encapsulation Mode: Tunnel mode
- Active protocol: ESP
- Encryption algorithm: DES
- Authentication algorithm: SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

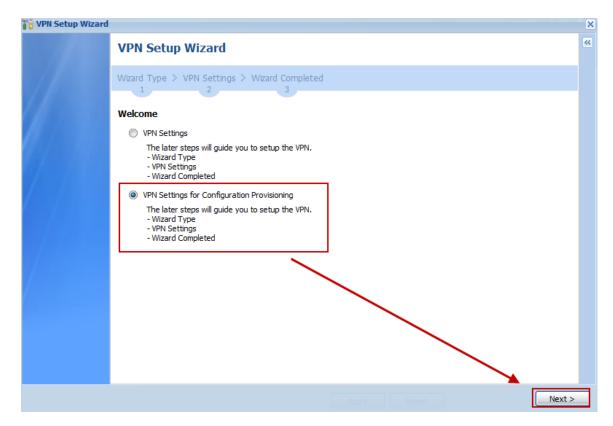
Provide an easy way for outside users to build up IPSec VPN tunnel by using the ZyWALL IPSec VPN Client for accessing internal resource.

ZyWALL configuration

CONFIGURATION	Port Role	Ethernet	PPP	Cellular	Tunnel	VLAN	Bridge	Trunk			
T ₩ Quick Setu □ Network	Configurati	ion									
+ Interface + Routing					T¥ Ou	ick Setup			×]	
+ Routing + Zone											
+ DDNS										DMZ-	-
+ NAT										P6	illi
 HTTP Redirect) (11
+ ALG									-		
+ IP/MAC Binding						Interface		VPN Setup			
 DNS Inbound LB Auth. Policy 						Quick Setting gh the steps		For creating secure communications bet			
+ Firewall					your	device conne	ected online.	nodes, VPN Quick Se	etting	0	
⊕ VPN								provides a simplified do that.	process to	0	
										0	
 Device HA 											
⊕ Object											
⊞ System											

Step 1: Click Configuration > Quick setup >VPN Setup

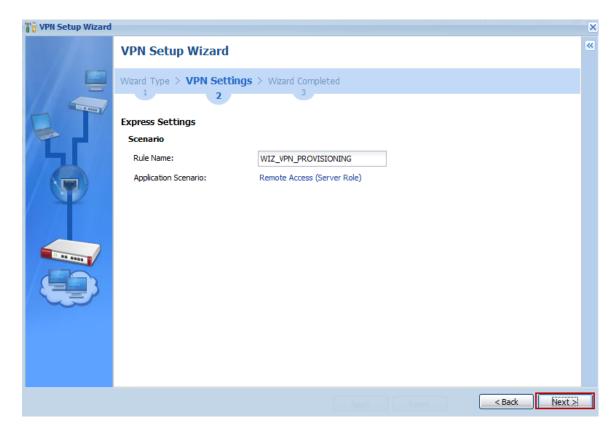
Step 2: Select "VPN settings for Configuration Provisioning"



Step 3: Select "Express" (or select "Advance" to define detail settings manually)

VPN Setup Wizard		×
	VPN Setup Wizard	«
	Wizard Type > VPN Settings > Wizard Completed	
	Please select the type of VPN policy you wish to setup.	
	Type of VPN policy © Express	
	Advanced	
	Apply Reset SAC	7

Step 4: Change Rule Name if needed



Step 5: Fill in Pre-shared key and Local policy

🚏 VPN Setup Wizard	Welcome admin Logoul	×
12	VPN Setup Wizard	~
	Wizard Type > VPN Settings > Wizard Completed	
	Express Settings	
	Configuration	
	Secure Gateway: Any	
	Pre-Shared Key: 12345678 Local Policy (IP/Mask) 192.168.1.0 / 255.255.255.0	
	Remote Policy (IP/Mask): Any	
	Aboly Select Sel	>

Step 6: Check if IPSec VPN configuration correct and save setting

背 VPN Setup Wizard			Welcome admin Logou	×			
11	VPN Setup Wizard	VPN Setup Wizard					
	Wizard Type > VPN Settin 1 2	gs > Wizard Completed					
	Express Settings						
	Summary		_				
651	Rule Name:	WIZ_VPN_PROVISIONING					
	Secure Gateway:	Any		=			
	Pre-Shared Key:	12345678					
	Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0					
	Remote Policy (IP/Mask):	Any					
	Configuration for Secure Ga	teway	- \				
	## Edit this shell script accor ## the comments before usin ## Check the peer-ip interfa ## Edit the WIZ_VPN_PROV ## Then remove the followin PLEASE REMOVE THIS LINE configure terminal isakmp policy WIZ_VPN_PROV ## If this device's wan 1 IP is ## consider using DDNS and	ng it in the remote gateway. ce. SIONING_LOCAL address-object. g line. /ISIONING dynamic,	E				
			Reset	Save			

Step 7: Click **Configuration > VPN > IPSec VPN > Configuration Provisioning** and enable Configuration Provisioning

	CONFIGURATION	VPN Connection	VPN Gateway	Concentrator	Configuration Provisioning	
	לאָלָ Quick Setup ⊂ Network + Interface + Routing	General Setting:	s guration Provisionin	g		
R.	Zone DDNS NAT HTTP Redirect ALG	Authentication Client Authentica Configuration	ation Method:	default	~	
	PMAC Binding DNS Inbound LB Auth. Policy Firewall VPN IPSec VPN SSL VPN	Status Pr	iority 🔺	VPN Connection	n	Allowed User

•	CONFIGURATION	VPN Connection	VPN Gateway	Concentrator	Configuration Provisioning	
	∎ Network	General Setting	5			
6	 Interface Routing 	Enable Configuration Provisioning				
R.	+ Zone + DDNS	Authentication				
	+ NAT	Client Authentic	ation Method:	default	~	
	HTTP Redirect ALG IP/MAC Binding	Configuration				
	DNS Inbound LB	🕜 Add 📝 Ed	t 🍵 Remove 💡 A	ictivate 😡 Inactiva	ite 🔐 Move	
	+ Auth. Policy	Status Pr	iority 🔺	VPN Connectio	n	Allowed User
	+ Firewall ⊡ VPN	· · · · · · · · · · · · · · · · · · ·		WIZ_VPN_PRO	VISIONING	any
	IPSec VPN	4 4 Page	1 of 1 > >	Show 50 🗸	items	
	SSL VPN L2TP VPN					

ZyWALL IPSec VPN Client software configuration

Step 1: Execute ZyWALL IPSec VPN Client

ZyWALL IPSec VPN Client				
Configuration Tools ?				
ZyXEL				
Save Apply	Global Parameters			
VPN Configuration	Global Parameters			
Global Parameters	Lifetime (sec.)			
		Default	Minimal	Maximal
	Authentication (IKE)	1800	360	28800
	Encryption (IPSec)	1200	300	28800
	Dead Peer Detection	n (DPD) —		
	Check interval	30 se	с.	
	Max. number of retries	5		
	Delay between retries	15 se	с.	
	Miscellaneous			
	Retransmissions	2	IKE Por	t
	X-Auth timeout	20	NAT Por	t
	🔲 Disable Split Tu	unneling		
VPN Client ready				

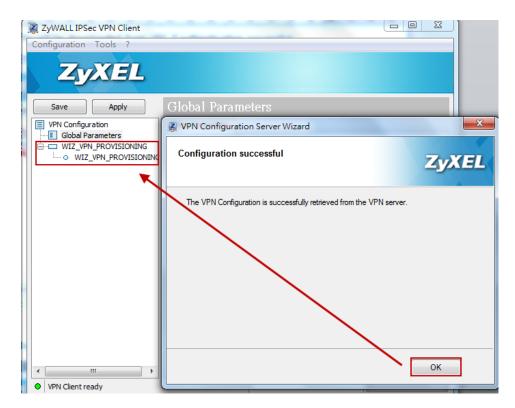
Step 2: Click Configuration > Get from Server

😰 ZyWALL IPSec VPN Client			_	
Configuration Tools ?				
Import				
Export				
Get from Server				
Move to USB Drive	Global Parameters			
Wizard	Global Parameters			
Quit	Lifetime (sec.)			
	,	Default	Minimal	Maximal
	Authentication (IKE)	1800	360	28800
	Encryption (IPSec)	1200	300	28800
	V Dead Peer Detection	on (DPD) —		
	Check interval	30 se	ς.	
	Max. number of retries	5		
	Delay between retries	15 sec	Ξ.	
	Miscellaneous			
	Retransmissions	2	IKE Po	rt
	X-Auth timeout	20	NAT Po	rt
	🥅 Disable Split T	unneling		
VPN Client ready				

Step 3: Fill in authentication information and click "Next"

😰 VPN Configuratio	🛿 VPN Configuration Server Wizard							
Step 1: Authentication What are the parameters of the VPN Server Connection?								
		PN Configuration from the VPN Con mation required for the connection						
Gat	eway Address:	59.124.163.147	Port: 443					
	Authentication:	Login + Password	•					
	Login:	provision_user						
	Password:	••••						
		Next >	Cancel					

Step 4: The VPN profile will be downloaded from USG if authentication successful



Step 5: Double left click on the phase 2 profile to dial up IPSec VPN tunnel

ZyWALL IPSec VPN Client	
Configuration Tools ?	
ZyXEL	
Save Apply	WIZ_VPN_PROVISIONING: IPSec
VPN Configuration	IPSec Advanced Scripts Remote Sharing
Global Parameters	
WIZ VPN PROVISIONING	Addresses
	VPN Client address 0 . 0 . 0 . 0
	Address type Subnet address 🗸
	Remote LAN address 192 . 168 . 1 . 0
	Subnet mask 255 . 255 . 255 . 0
	ESP
	Encryption DES -
	Authentication SHA-1
	Mode Tunnel -
	PFS
	PFS Group
	Tunnel opened.
VPN Client ready	\ 00000000/

Step 6: You can reach the internal server

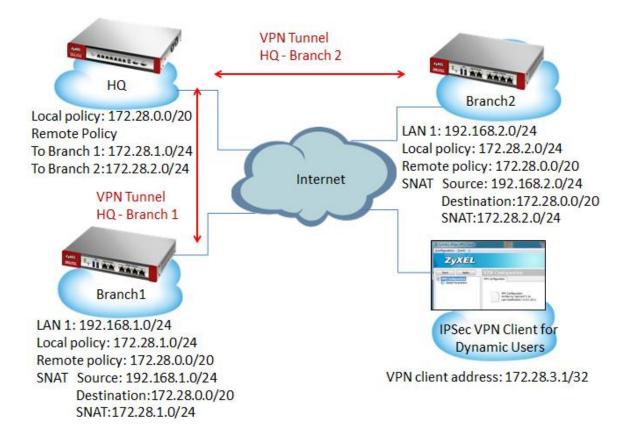
C:\Users\Emily>ping	192 168 1 34 -+	
	172.100.1.54	
Ping 192.168.1.34 <∱	使用 32 位元組的資料>:	
	位元組=32 時間=1ms TTL=126	
	位元組=32 時間=1ms TTL=126	
回覆自 192.168.1.34:	位元組=32 時間=1ms TTL=126	
回覆自 192.168.1.34:		
回覆自 192.168.1.34:	位元組=32 時間=2ms TTL=126	
回覆自 192.168.1.34:		
回覆自 192.168.1.34:	位元組=32 時間=1ms TTL=126	

Scenario 5 – Dynamic users communicate with HQ and all branch offices by using auto created VPN routes

5.1 Application Scenario

For world-wide enterprises, network communication between each branch and the headquarter office is very important. A VPN concentrator combines several IPSec VPN connections into one secure network for site-to-site VPN and reduces the number of VPN connections that need to be set up and maintained in the network. However a VPN concentrator is not suitable for every situation, many companies have several mobile users, travelers who are not located in a fixed office. When the network receives traffic from these dynamic users, we cannot know their subnets or IP addresses in advance.

Supposing a company has a headquarter and two branch offices. Two VPN tunnels are built up, each between the HQ and one of the branch offices. Undoubtedly, road warriors and telecommuters can access network of HQ and branch offices respectively by building IPSec VPN tunnel to each office. However, it is inconvenient and inefficient for mobile users to disconnect one VPN tunnel and then connect to another VPN tunnel if they just want to access some resource of branch office 1 while they're accessing resources of the HQ. How to let mobile users access the networks of HQ and branch offices at the same time with just one VPN tunnel? Now, you can achieve this goal via an "Auto-created VPN Route". If the subnets are aggregated, auto created VPN routes can achieve this request without VPN concentrator rules.



5.2 Configuration Guide

Network conditions:

ZyWALL:

Site	WAN IP	VPN Tunnel	VPN Policy(Local-Remote)
HQ	10.59.3.201	HQ-Branch 1	172.28.0.0/20 - 172.28.1.0/24
		HQ-Branch 2	172.28.0.0/20 - 172.28.2.0/24
Branch 1	10.59.3.200	Branch 1-HQ	172.28.1.0/24 - 172.28.0.0/20
			Outbound Traffic (SNAT)
			Source: 192.168.1.0/24
			Destination:172.28.0.0/20
			SNAT:172.28.1.0/24
			Inbound Traffic(DNAT)
			Original IP: 172.28.1.0/24
			Mapped IP: 192.168.1.0/24
Branch 2	10.59.3.37	Branch 2-HQ	172.28.2.0/24 - 172.28.0.0/20
			Outbound Traffic (SNAT)
			Source: 192.168.2.0/24
			Destination: 172.28.0.0/20
			SNAT:172.28.2.0/24
			Inbound Traffic(DNAT)
			Original IP: 172.28.2.0/24
			Mapped IP: 192.168.2.0/24

Goals to achieve:

Mobile users can communicate with headquarters and all branch offices with only one VPN tunnel.

ZyWALL configuration:

Task 1. Establish IPSec VPN between HQ and Branch 1.

HQ configuration

Step1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit

Edit VPN Gateway HQtoBranch1			? ×
Show Advanced Settings			
General Settings			- I I I I I I I I I I I I I I I I I I I
I Enable			
VPN Gateway Name:	HQtoBranc		
Gateway Settings			
My Address			
Interface	ge2	DHCP client 10.59.3.201/255.2	55.255.0
Ø Domain Name / IP			10 A
Peer Gateway Address			
Static Address	Primary	10.59.3.200	
	Secondary	0.0.0.0	
Fall back to Primary Peer G	ateway when p	sible	
Fall Back Check Interval:	300	(60-86400 seconds)	
Oynamic Address			
Authentication			
Pre-Shared Key	12345678		
Certificate		cer (See My Certificates)	-

Edit VPN Connection HQto	Franch1	?
Show Advanced Settings 🗎	Create new Object -	
General Settings		
Enable		
Connection Name:	HQtoBranch1	
VPN Gateway		
Application Scenario		
Site-to-site		
Site-to-site with Dyna	mic Peer	
Remote Access (Sen	er Role)	
Remote Access (Cler	t Role)	
VPN Gateway:	HQtoBranch1 Y ge2 10.59.3.200 0.0.	0.0
Policy		
Local policy:	vlan172_0	20
Remote policy:	vlan172_1 ¥ SUBNET, 172.28.1.0/	24
Phase 2 Setting		
SA Life Time:	86400 (180 - 3000000 Seconds)	
		OK Cancel

Step2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

Branch 1 configuration

Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit

Edit VPN Gateway Branch1toHQ	2		? >
Show Advanced Settings			
General Settings			
Enable			
VPN Gateway Name:	Branch1toH	Q	
Gateway Settings			
My Address			
Interface	wan1	DHCP clent 10.59.3.200/255.255.255.	
O Domain Name / IP			Ŧ
Peer Gateway Address			
Static Address	Primary	10.59.3.201	
	Secondary	0.0.0.0	
Fall back to Primary Peer G	ateway when p	ssble	
Fall Back Check Interval:	300	(60-86400 seconds)	
O Dynamic Address			
Authentication			
Pre-Shared Key	12345678		
Certificate	default	(See My Certificates)	

Edit VPN Connection Bran	ch1toHQ	?]
🔝 Show Advanced Settings 🖹	Create new Object+	
General Settings		
Enable		
Connection Name:	Branch1toHQ	
VPN Gateway		
Application Scenario		
Site-to-site		
Site-to-site with Dyr	amic Peer	
Remote Access (Ser	ver Role)	
Remote Access (Cle	nt Role)	
VPN Gateway:	Branch1toHQ 👻 v	wan1 10.59.3.201 0.0.0.0
Policy		
Local policy:	vlan172_1 👻 5	SUBNET, 172.28.1.0/24
Remote policy:	vlan172_0 👻 S	SUBNET, 172.28.0.0/20
Phase 2 Setting		
SA Life Time:	86400 (180 - 3	3000000 Seconds)
		OK Cancel
		OK Cancel

Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

Step 3. Do an SNAT rule in VPN tunnel.

Source: 192.168.1.0/24

Destination:172.28.0.0/20

SNAT:172.28.1.0/24

	(7) ×
	^
ET 👻	
×	
ans	
one and M	
one M	
one M	_
one M	End
	End

Step 4. Configuration > Network > Routing > Policy Route,

Add a policy route

Source: any

Destination: 172.28.0.0/20

Next-hop: VPN tunnel

Z Edit Policy Route			? ×
🔟 Show Advanced Settings 🛅 Create new Obj	ect •		
Configuration			
Enable Description:		(Optional)	
Criteria			
User:	any	~	
Incoming:	any (Excluding ZyWALL) 👻	8
Source Address:	any	~	
Destination Address:	vlan172_0	~	
DSCP Code:	any	~	
Schedule:	none	~	
Service:	any	~	
Next-Hop			
Type:	VPN Tunnel	~	
VPN Tunnel:	Branch1toHQ	*	
			OK Cancel

Task 2. Establish IPSec VPN between HQ and Branch 2

HQ configuration

Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit

Edit VPN Gateway HQtoBranch2			?)
Show Advanced Settings			
General Settings			
Enable			
VPN Gateway Name:	HQtoBranch	2	
Gateway Settings			
My Address			
Interface	ge2	 DHCP client 10.59.3.201/255.255 	5.255.0
O Domain Name / IP			
Peer Gateway Address			
Static Address	Primary	10.59.3.37	
	Secondary	0.0.0.0	
Fall back to Primary Peer G	ateway when p	ossible	
Fall Back Check Interval:	300	(60-86400 seconds)	
Oynamic Address			
Authentication			
Pre-Shared Key	12345678		
Certificate		t.cer 😽 (See <u>My Certificates</u>)	

Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

Edit VPN Connection HQtoBranch	2			?
Show Advanced Settings 🔚 Create	new Object+			
General Settings				
V Enable				
Connection Name:	HQtoBranch2			
VPN Gateway				
Application Scenario				
Site-to-site				
Site-to-site with Dynamic Pee	ir.			
Remote Access (Server Role)				
C Remote Access (Clent Role)				
VPN Gateway:	HQtoBranch2	*	ge2 10.59.3.37 0.0.0.0	
Policy				
Local policy:	vlan172_0	*	SUBNET, 172.28.0.0/20	
Remote policy:	vlan172_2	¥	SUBNET, 172.28.2.0/24	
Phase 2 Setting				
SA Life Time:	86400	(180	- 3000000 Seconds)	
				OK Cancel

Branch 2 configuration

Step1.	Configuration	> VPN >	IPSec VPN >	VPN Gateway	/ > Edit
--------	---------------	---------	-------------	-------------	----------

Edit VPN Gateway Branch2toHQ							? ×
Show Advanced Settings							
General Settings							
V Enable							
VPN Gateway Name:	Branch2toF	łQ					
Gateway Settings							
My Address							
 Interface 	wan1		Y DHC	P client 10.	59.3.37/255	.255.255.0	
O Domain Name / IP				1			E
Peer Gateway Address				-			
Static Address	Primary	10.59.3.201	1	1			
	Secondary	0.0.0.0					
Fall back to Primary Peer G	ateway when p	ossible					
Fall Back Check Interval:	300	((50-86400	seconds)			
O Dynamic Address							
Authentication							
Pre-Shared Key	12345678						
Certificate	default		× (See				

Step2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

Edit VPN Connection Bran	nch2toHQ			2.5
Show Advanced Settings	Create new Object+			
General Settings				, in the second s
V Enable				
Connection Name:	Branch2toHQ			
VPN Gateway				
Application Scenario				1
Site-to-site				
Site-to-site with Dy	namic Peer			
Remote Access (Se	erver Role)			
Remote Access (C)	ent Role)			
VPN Gateway:	Branch2toHQ	~	wan1 10.59.3.201 0.0.0.0	
Policy				
Local policy:	vlan172_2	v	SUBNET, 172.28.2.0/24	
Remote policy:	vlan172_0	*	SUBNET, 172.28.0.0/20	
Phase 2 Setting				
SA Life Time:	86400	(180	- 3000000 Seconds)	
				OK Cancel
				Cances

Step 3. Do an SNAT rule in VPN tunnel.

Source: 192.168.2.0/24

Destination:172.28.0.0/20

SNAT:172.28.2.0/24

	/PN Connection	Branch2toHQ			-			?
Hide	Advanced Setting	ps 🛅 Create new	object.					
	Log							
nbou	nd/Outbound t	traffic NAT						
Out	ound Traffic							
1	Source NAT							
	Source:		LAN1_SUBNET	*				
	Destination:	1	vlan172_0	~				
	SNAT:		vian172_2	*				
Inbo	und Traffic							
1	Source NAT							
	Parament		Please select one	2				
	Source:							
	Destination:		Please select one	~				
	Destination:		Please select one	~				
1	Destination: SNAT:	λŦ	Please select one Please select one	~				
1	Destination: SNAT: Z Destination NA	λŦ	Please select one Please select one	~	Original Port End	Mapped Port	Mapped Port	
1	Destination: SNAT: 2 Destination NA Add 2555 figst 18	\T emove ⊮N Move	Please select one Please select one Please select one	8	Original Port End	Mapped Port	Mapped Port	

Step 4. Configuration > Network > Routing > Policy Route,

Add a policy route

Source: any

Destination: 172.28.0.0/20

Next-hop: VPN tunnel

A Edit Policy Route			7.12
🔟 Show Advanced Settings 🔚 Create n	ew Object+		
Configuration			
📝 Enable			
Description:		(Optional)	
Criteria			
User:	any	~	
Incoming:	any (Excluding ZyWALL) ~	1
Source Address:	any	~	
Destination Address:	vlan172_0	~	
DSCP Code:	any	~	
Schedule:	none	~	
Service:	any	~	
Next-Hop			
Type:	VPN Tunnel	~	
VPN Tunnel:	Branch2toHQ	*	
			OK Cancel

Task 3. Establish Dynamic VPN for mobile users

HQ configuration

Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit

Edit VPN Gateway HQtoMobileU	lser				(?) >
Show Advanced Settings					
General Settings					
Enable					
VPN Gateway Name:	HQtoMobile	User	1		
Gateway Settings					
My Address					
Interface	ge2		* D	OHCP client 10.59.3.201/25	
O Domain Name / IP					E
Peer Gateway Address					
Static Address	Primary	0.0.0.0			
	Secondary	0.0.0.0			
Fall back to Primary Peer G	Sateway when p	ossible			
Fall Back Check Interval:	300		(60-864	100 seconds)	
Oynamic Address					
Authentication					
Pre-Shared Key	123456789).			
Certificate			× (See My Certificates)	

Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

Edit VPN Connection HQtoMobile	eUser			? X
🔲 Show Advanced Settings 🚞 Create	e new Object+			
General Settings				
💟 Enable				
Connection Name:	HQtoMobileUser			
VPN Gateway				
Application Scenario				=
Site-to-site				
Site-to-site with Dynamic Pression of Control Site Pression (Control Site)	eer			
Remote Access (Server Ro)	e)			
Remote Access (Client Role)			
VPN Gateway:	HQtoMobieUser	*	ge2 0.0.0.0 0.0.0.0	-
Policy				
Local policy:	vlan1/2_0	v	SUBNET, 172.28.0.0/20	
Phase 2 Setting				
SA Life Time:	86400	(180	- 3000000 Seconds)	
Related Settings				
				OK Cancel

Step 3. IPSec VPN client setting

🕎 ZyWALL IPSec VPN Client		_ □ 🔀					
Configuration Tools 2							
ZyXEL							
Save Apply	Gateway: Authentication						
VPN Configuration Global Parameters	Authentication Advanced Certificate						
Global Parameters	Addresses						
L-🕑 Tunnel	Interface Any	~					
	Remote Gateway 10.59.3.2	01					
	Authentication						
	Preshared Key	•••					
	Confirm ••••••	•••					
	OCertificate						
	IKE						
	Encryption 30ES	*					
	Authentication SHA-1	×					
	Key Group DH1	v					
 VPN Client ready 							

Step 4. In Phase 2, assign one IP for IPSec VPN Client manually.

ZyWALL IPSec VPN Client	
ZyXEL	
Save Apply	Tunnel: IPSec
VPN Configuration Global Parameters Gateway	IPSec Advanced Scripts Remote Sharing Addresses VPN Client address 172 - 28 - 3 - 1
	Address type Subnet address Remote LAN address 172 - 28 - 0 - 0 Subnet mask 255 - 255 - 240 - 0
	Esp Encryption DES v Authentication SHA-1 v
	Mode Tunnel PFS PFS Group
VPN Client ready	

Step 5. Disable "Use Policy Route to control dynamic IPSec rules" on HQ device.

Configuration > VPN > IPSec VPN > VPN Connection > Global Setting

12.1						
	Use Policy Rout	e to control dynamic IPSec rules				
1	Ignore "Don't P	ragment" setting in IP header 📋				
	UUNICESS					
	Contraction of the					
100	Add CEPIE 1	Remove Q Activate Q Inactiste	Connect 🐘 Department 🔚 Objest	ct Reference		
v	THE IS SHOT					
ř	Status	Name	VPN Gateway	Encapsulation	Algorithm	Policy
*			VPN Gateway	and the second se	Algorithm 2DES/SHA1 3DES/ND6 DES/	1.
* 1	Status	Name	VPN Gateway	Encapsulation	And the second statement of th	1.
* 1 2 3	Status 9 %	Name Default_L2TP_VPN_Connecti	VPN Gateway Default_L2TP_VPN_GW	Encapsulation TRANSPORT	DESISHAT DESIMDS DESI.	Jany

HQ Routing Packet Flow

Maintenance > Packet Flow Explore > Routing Status



Verification

IPSec VPN client can ping HQ, branch 1 and branch 2 successfully at the same time.

C: Documents and Settings user>ping 172.28.0.33 Pinging 172.28.0.33 with 32 bytes of data: Reply from 172.28.0.33: bytes=32 time=1ms TTL=126 Reply from 172.28.0.33: bytes=32 time=2ms TTL=126 Reply from 172.28.0.33: bytes=32 time=3ms TTL=126 Reply from 172.28.0.33: bytes=32 time=1ms TTL=126 C: Documents and Settings user>ping 172.28.1.33 Pinging 172.28.1.33 with 32 bytes of data: Reply from 172.28.1.33: bytes=32 time=4ms TTL=123 Reply from 172.28.1.33: bytes=32 time=3ms TTL=123 Reply from 172.28.1.33: bytes=32 time=3ms TTL=123 Reply from 172.28.1.33: bytes=32 time=3ms TTL=123 C: Documents and Settings\user>ping 172.28.2.33 Pinging 172.28.2.33 with 32 bytes of data: Reply from 172.28.2.33: bytes=32 time=7ms TTL=123 Reply from 172.28.2.33: bytes=32 time=3ms TTL=123 Reply from 172.28.2.33: bytes=32 time=3ms TTL=123 Reply from 172.28.2.33: bytes=32 time=3ms TTL=123