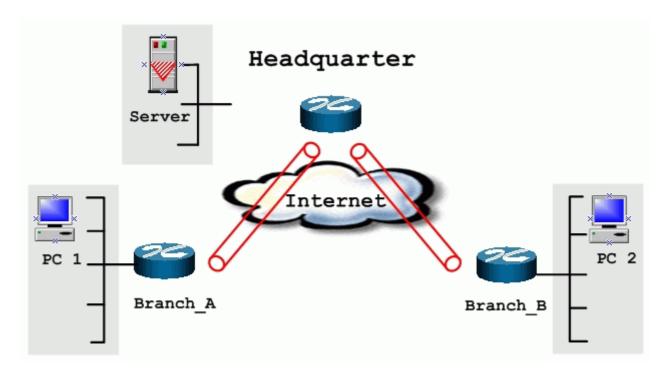
- 1. Setup VPN in Branch Office A
- 2. Setup VPN in Branch Office B
- 3. Setup VPN in Headquarter

This page guides us how to setup VPN routing between branch offices through headquarter. So that whenever branch office A wants to talk to branch office B, headquarter plays as a VPN relay. Users can gain benefit from such application when the scale of branch offices is very large, because no additional VPN tunnels between branch offices are needed. In this support note, we skip the detailed configuration steps for Internet access and presume that you are familiar with basic ZyNOS VPN configuration.

As the figure shown below, each branch office have a VPN tunnel to headquarter, thus PCs in branch offices can access systems in headquarter via the tunnel. Through VPN routing, ZyWALL series now provide you a solution to let PCs in branch offices talk to each other through the existing VPN tunnels concentrated on the headquarter. This feature is available in ZyWALL10, ZyWALL50 and ZyWALL100.



The IP addresses we use in this example are as shown below.

Branch_A	Headquarter	Branch_B
WAN:202.3.1.1	WAN:202.1.1.1	WAN:202.2.1.1
LAN:192.168.3.1	LAN:192.168.1.1	LAN:192.168.2.1

LAN of Branch_A	LAN of Headquarter	LAN of Branch_B
192.168.3.0/24	192.168.1.0/24	192.168.2.0/24

#### 1. Setup VPN in branch office A

Because VPN routing enables branch offices to talk to each other via tunnels concentrated on headquarter. In this step, we configure an IPSec rule in ZyWALL (Branch\_A) for PCs behind branch office A to access both LAN segments of headquarter and branch office B. Because the LAN segments of headquarter and branch office B are continuous, we merge them into one single rule by including these two segments in **Remote** section. If by any chance, the two segments are not continuous, we strongly recommend you to setup different rules for these segments.

- 1. Click **Advanced**, and click **VPN** tab on the left.
- 2. On the **SUMMARY** menu, Select a policy to edit by clicking **Edit**.
- 3. On the **CONFIGURE-IKE** menu, check **Active** check box and give a name to this policy.
- 4. Give this VPN rule a name, **Branch\_A**.
- 5. Select **Key Management** to **IKE** and **Negotiation Mode** to **Main**.
- In Local section, select Address Type to Range Address, set IP Address Start to 192.168.3.0, and End to 192.168.3.255. This section covers the LAN segment of branch office A.
- 7. In **Remote** section, select **Address Type** to **Range Address**, set **IP Address Start** to **192.168.1.0** and **End** to **192.168.2.255**. This section covers the LAN segment of both headquarter and branch office B.
- 8. My IP Addr is the WAN IP of this ZyWALL, 202.3.1.1.
- 9. Set Secure Gateway Addr to the IP address of Headquarter, 202.1.1.1.
- 10. Select **Encapsulation Mode** to **Tunnel**.
- 11. Check the **ESP** check box. (AH can not be used in SUA/NAT case)
- 12.Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA-1**. These parameters are for IKE phase 2 negotiation. You can set more detailed configuration by pressing **Advanced** button.
- 13.Enter the key string 12345678 in the Pre-shared Key text box, and click Apply.

#### **VPN - VPN RULE - EDIT** WIZARD ■ NAT Traversal ☐ Keep alive ☑ Active SETUP SYSTEM Lan Name Branch A WAN **Key Management** IKE SUA/NAT **Negotiation Mode** Main STATIC ROUTE **FIREWALL CONTENT FILTER** ☐ Enable Extended Authentication VPN Server Mode (Search Local User first then RADIUS) **CERTIFICATES** Client Mode **AUTH SERVER** REMOTE MGNT **User Name UPnP** Password LOGS Local MAINTENANCE Client to Site LOGOUT **Local IP Address** 0.0.0.0 Site to Site Address Type Range Address 🔻 Starting IP Address 192.168.3.0 **Ending IP Address / Subnet** 192.168.3.255 Remote Range Address 🔻 Address Type Starting IP Address 192.168.1.0 **Ending IP Address / Subnet Mask** 192.168.2.255 DNS Server (for IPSec VPN) 0.0.0.0 **Authentication Method** 12345678 Pre-Shared Key auto\_generated\_self\_signed\_cert 🔽 (See My Certificate Certificates) Local ID Type Content 0.0.0.0 Peer ID Type Content 0.0.0.0 My IP Address 202.3.1.1 Secure Gateway Address 202.1.1.1 **Encapsulation Mode** Tunnel • ESP O AH **Encryption Algorithm** Authentication Algorithm | MD5 | 🔽 DES 🔻

You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.

Advanced

**Authentication Algorithm** 

SHA1 🔻

Apply

Cancel

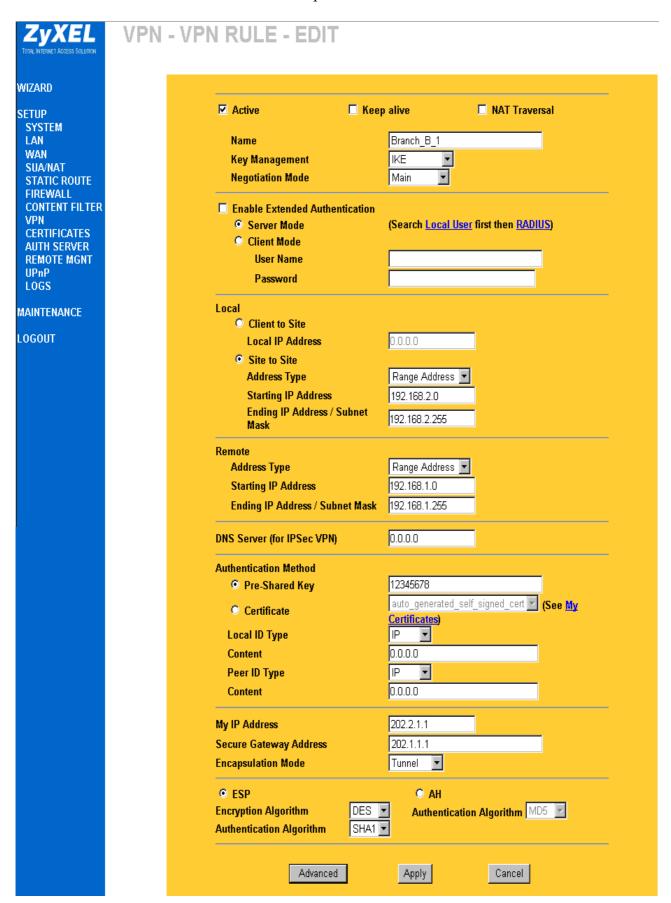
JP .	Protocol	0
'STEM An	Enable Replay Detection	NO 🔽
N AN	Local Port	
A/NAT	Start	0
ATIC ROUTE REWALL	End	0
NTENT FILTER	Remote Port	
N EDTIFICATES	Start	0
ERTIFICATES UTH SERVER	End	0
EMOTE MGNT	Phase 1	
PnP OGS	Negotiation Mode	Main 🔻
	Encryption Algorithm	DES 🔻
INTENANCE	Authentication Algorithm	MD5 🔻
GOUT	SA Life Time (Seconds)	28800
	Key Group	DH1 🔽
	Phase 2	
	Active Protocol	ESP 🔽
	Encryption Algorithm	DES 🔽
	Authentication Algorithm	SHA1 🔽
	SA Life Time (Seconds)	28800
	Encapsulation	Tunnel
	Perfect Forward Secrecy(PFS)	NONE 🔽
	Apply	Cancel

### 2. Setup VPN in branch office B

Be very careful about the remote IP address in branch office B, because for systems behind branch office B want to systems behind branch office A and headquarter, we have to specify these two segments in **Remote** section. However if we include these two segments in one rule, the LAN segment of branch office B will be also included in this single rule, which means intercommunication inside branch office B will run into VPN tunnel. To avoid such situation, we need two separate rules to cover the LAN segment of branch office A and headquarter.

#### 1. The first rule in Branch\_B.

This rule is for branch office B to access headquarter.



You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.

UP	Post cond	
YSTEM	Protocol	0
AN	Enable Replay Detection Local Port	NO 🔽
an Ja/nat	Start	0
TATIC ROUTE	End	0
REWALL Ontent filter	Remote Port	
PN	Start	0
ERTIFICATES UTH SERVER	End	0
EMOTE MGNT	Phase 1	
PnP OGS	Negotiation Mode	Main ▼
	Encryption Algorithm	DES 🔻
INTENANCE	Authentication Algorithm	MD5 🔻
GOUT	SA Life Time (Seconds)	28800
	Key Group	DH1 🔻
	Phase 2	
	Active Protocol	ESP ▼
	Encryption Algorithm	DES 🔽
	Authentication Algorithm	SHA1 ▼
	SA Life Time (Seconds)	28800
	Encapsulation	Tunnel
	Perfect Forward Secrecy(PFS)	NONE 🔽
	Apply	Cancel
	Apply	Odifoot

### 2. The second rule in Branch\_B

This rule is for branch office B to access branch office A.

#### **VPN - VPN RULE - EDIT** WIZARD ☐ Keep alive ✓ Active ■ NAT Traversal SETUP SYSTEM LAN Name Branch\_B\_2 WAN **Key Management** IKE • SUA/NAT **Negotiation Mode** Main STATIC ROUTE FIREWALL **CONTENT FILTER** ☐ Enable Extended Authentication VPN Server Mode (Search Local User first then RADIUS) **CERTIFICATES** Client Mode **AUTH SERVER User Name** REMOTE MGNT **UPnP** Password LOGS Local MAINTENANCE Client to Site OGOUT **Local IP Address** 0.0.0.0 Site to Site Range Address Address Type Starting IP Address 192.168.2.0 **Ending IP Address / Subnet** 192.168.2.255 Remote Address Type Range Address 🔻 Starting IP Address 192.168.3.0 **Ending IP Address / Subnet Mask** 192.168.3.255 DNS Server (for IPSec VPN) 0.0.0.0 **Authentication Method** Pre-Shared Key 12345678 auto\_generated\_self\_signed\_cert / (See My Certificate <u>Certificates</u> Local ID Type Content 0.0.0.0

Peer ID Type Content

My IP Address

ESP

Secure Gateway Address

**Encapsulation Mode** 

**Encryption Algorithm** 

**Authentication Algorithm** 

You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.

Advanced

0.0.0.0

202.2.1.1

202.1.1.1

O AH

Apply

Authentication Algorithm MD5 🔽

Cancel

Tunnel

DES ▼ SHA1 ▼

	Protocol	0
STEM N	Enable Replay Detection	NO 🔻
AN	Local Port	
A/NAT ATIC ROUTE	Start	0
REWALL	End	0
NTENT FILTER	Remote Port Start	
PN ERTIFICATES JTH SERVER	End	0
MOTE MGNT np	Phase 1	
OGS	Negotiation Mode	Main 🔽
NTENANCE	Encryption Algorithm	DES 🔽
NTENANCE	Authentication Algorithm	MD5 💌
SOUT	SA Life Time (Seconds)	28800
	Key Group	DH1 🔽
	Phase 2	
	Active Protocol	ESP 🔽
	Encryption Algorithm	DES 🔽
	Authentication Algorithm	SHA1 🔽
	SA Life Time (Seconds)	28800
	Encapsulation	Tunnel 🔽
	Perfect Forward Secrecy(PFS)	NONE 🔽
	Apply	Cancel

### 3. Setup VPN in Headquarter

 $1. \ \ The \ correspondent \ rule \ for \ Branch\_A \ in \ head quarter$ 

# ZYXEL TOTAL INTERNET ACCESS SOLUTION

## VPN - VPN RULE - EDIT

#### WIZARD

SETUP
SYSTEM
LAN
WAN
SUA/NAT
STATIC ROUTE
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER
REMOTE MGNT
UPnP
LOGS

MAINTENANCE

LOGOUT

Name	to_Branch_A	
Key Management	IKE 🔻	
Negotiation Mode	Main 🔻	
☐ Enable Extended Authentication	/C	- C (I DADIUC)
<ul><li>Server Mode</li><li>Client Mode</li></ul>	(Search <u>Local Use</u>	<u>r</u> first then <u>RADIUS</u> )
User Name		
Password		
r assworu		
Local		
Client to Site	0000	_
Local IP Address	0.0.0.0	
<ul><li>Site to Site</li><li>Address Type</li></ul>	Range Address 🔻	1
Starting IP Address	192.168.1.0	
Ending IP Address / Subnet		_
Mask	192.168.2.255	
Remote		
Address Type	Range Address 🔻	
Starting IP Address	192.168.3.0	
Ending IP Address / Subnet Mask	192.168.3.255	
DNS Server (for IPSec VPN)	0.0.0.0	
Authentication Method		
Pre-Shared Key	12345678	
		lf_signed_cert (See My
C Certificate	Certificates)	in_orgined_core in (3ee inty
Local ID Type	IP 🔽	
Content	0.0.0.0	
Peer ID Type	IP ▼	
Content	0.0.0.0	
My IP Address	202.1.1.1	
Secure Gateway Address	202.3.1.1	
Encapsulation Mode	Tunnel 🔻	
Encapsulation work	Tulliel 1	
● ESP	O AH	
Encryption Algorithm DES		on Algorithm MD5 🔽
Authentication Algorithm SHA1	▼	

	Protocol	0
EM	Enable Replay Detection	NO 🔻
	Local Port	
AT	Start	0
C ROUTE	End	0
IALL Ent filter	Remote Port	
	Start	0
FICATES SERVER	End	0
TE MGNT	Diagram 4	
	Phase 1 Negotiation Mode	Main <b>▼</b>
	Encryption Algorithm	DES 🔽
NANCE	Authentication Algorithm	MD5 🔽
r e	SA Life Time (Seconds)	28800
	Key Group	DH1 🔽
	Phase 2	FOR
	Active Protocol	ESP V
	Encryption Algorithm	DES V
	Authentication Algorithm	SHA1 🔽
	SA Life Time (Seconds)	28800
	Encapsulation	Tunnel
	Perfect Forward Secrecy(PFS)	NONE 👤
	Apply	Cancel
		<del></del>

2. The correspondent rule for  $Branch\_B\_1$  in headquarter

# ZYXEL TOTAL INTERNET ACCESS SOLUTION

## VPN - VPN RULE - EDIT

#### WIZARD

SETUP
SYSTEM
LAN
WAN
SUA/NAT
STATIC ROUTE
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER
REMOTE MGNT
UPnP
LOGS

MAINTENANCE

LOGOUT

Name	to_Branch_B_1	
Key Management	IKE 🔽	
Negotiation Mode	Main 🔻	
☐ Enable Extended Authentica		
Server Mode	(Search <u>Local l</u>	<u>Jser</u> first then <u>RADIUS</u> )
Client Mode		
User Name		
Password		
Local		
Client to Site		
Local IP Address	0.0.0.0	
<ul><li>Site to Site</li></ul>		
Address Type	Range Address	<b>v</b>
Starting IP Address	192.168.1.0	
Ending IP Address / Subn Mask	192.168.1.255	
Remote		
Address Type	Range Address	▼
Starting IP Address	192.168.2.0	<del>-</del>
Ending IP Address / Subnet N	Mask 192.168.2.255	
DNS Server (for IPSec VPN)	0.0.0.0	
Authentication Method		
Pre-Shared Key	12345678	
C. Carlinata	auto generated	self_signed_cert (See My
C Certificate	<u>Certificates</u> )	
Local ID Type	IP <b>▼</b>	
Content	0.0.0.0	
Peer ID Type	IP ▼	
Content	0.0.0.0	
My IP Address	202.1.1.1	
Secure Gateway Address	202.2.1.1	
Encapsulation Mode	Tunnel	
© ESP	O AH	
Encryption Algorithm		ation Algorithm MD5 🔽
	HA1 ▼	

	Protocol	0
	Enable Replay Detection	NO 🔽
	Local Port	
TE	Start	0
TE	End	0
.TER	Remote Port	
:S	Start	0
R	End	0
NT	Phase 1	
	Negotiation Mode	Main 🔻
	Encryption Algorithm	DES 🔻
	Authentication Algorithm	MD5 🔽
	SA Life Time (Seconds)	28800
	Key Group	DH1 🔽
	Phase 2	
	Active Protocol	ESP 🔻
	Encryption Algorithm	DES 🔽
	Authentication Algorithm	SHA1 ▼
	SA Life Time (Seconds)	28800
	Encapsulation	Tunnel
	Perfect Forward Secrecy(PFS)	NONE 🔽
	Annly	Cancel
	Apply	Cancel

2. The correspondent rule for  $Branch\_B\_2$  in headquarter

# ZYXEL TOTAL INTERNET ACCESS SOLUTION

## VPN - VPN RULE - EDIT

#### WIZARD

SETUP
SYSTEM
LAN
WAN
SUA/NAT
STATIC ROUTE
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER
REMOTE MGNT
UPnP
LOGS

MAINTENANCE

LOGOUT

Name	to_Branch_B_2
Key Management	IKE 🔻
Negotiation Mode	Main 🔽
☐ Enable Extended Authentica	
© Server Mode	(Search <u>Local User</u> first then <u>RADIUS</u> )
Client Mode	
User Name	
Password	
Local	
Client to Site	
Local IP Address	0.0.0.0
Site to Site	
Address Type	Range Address 🔽
Starting IP Address	192.168.3.0
Ending IP Address / Subi Mask	net 192.168.3.255
Remote	
Address Type	Range Address 🔻
Starting IP Address	192.168.2.0
Ending IP Address / Subnet	Mask 192.168.2.255
DNS Server (for IPSec VPN)	0.0.0.0
Authentication Method	
Pre-Shared Key	12345678
C Certificate	auto_generated_self_signed_cert / (See My
	Certificates)
Local ID Type	IP ▼
Content	0.0.0.0
Peer ID Type	IP ▼
Content	0.0.0.0
My IP Address	202.1.1.1
Secure Gateway Address	202.2.1.1
Encapsulation Mode	Tunnel
• ESP	○ АН
Encryption Algorithm	DES Authentication Algorithm MD5
Authentication Algorithm	SHA1 🔻

# ZyXEL TOTAL INTERNET ACCESS SOLUTION

## **VPN - VPN RULE - EDIT - ADVANCED**

WIZARD

SETUP
SYSTEM
LAN
WAN
SUA/NAT
STATIC ROUTE
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER
REMOTE MGNT
UPnP
LOGS

MAINTENANCE

OGOUT

Protocol	0
Enable Replay Detection	NO 🔽
Local Port	
Start	0
End	0
Remote Port	
Start	0
End	0
Phase 1	
Negotiation Mode	Main 🔻
Encryption Algorithm	DES 🔽
Authentication Algorithm	MD5 ▼
SA Life Time (Seconds)	28800
Key Group	DH1 🔽
Phase 2	
Active Protocol	ESP 🔽
Encryption Algorithm	DES 🔽
Authentication Algorithm	SHA1 ▼
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy(PFS)	NONE <b>T</b>

Status: Ready