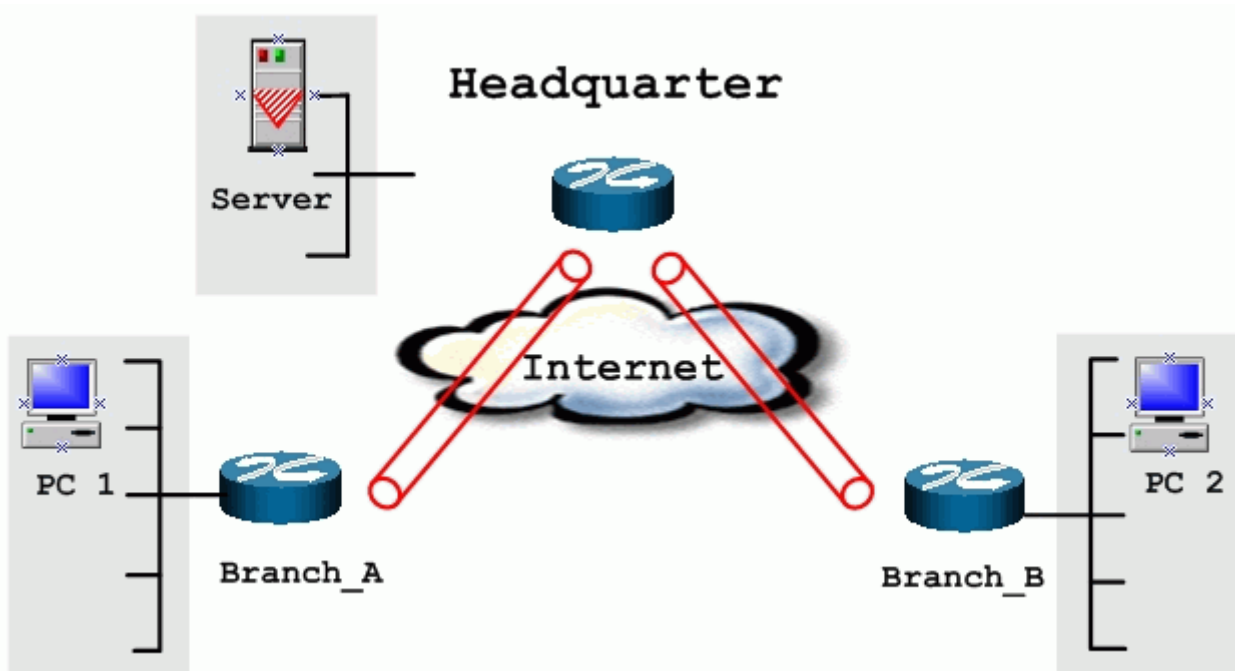


1. [Setup VPN in Branch Office A](#)
2. [Setup VPN in Branch Office B](#)
3. [Setup VPN in Headquarter](#)

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 LAN:192.168.3.1	WAN:202.1.1.1 LAN:192.168.1.1	WAN:202.2.1.1 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**.
6. 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**.

WIZARD

SETUP

SYSTEM

LAN

WAN

SUA/NAT

STATIC ROUTE

FIREWALL

CONTENT FILTER

VPN

CERTIFICATES

AUTH SERVER

REMOTE MGNT

UPnP

LOGS

MAINTENANCE

LOGOUT

Active
 Keep alive
 NAT Traversal

Name:

Key Management:

Negotiation Mode:

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name:

Password:

Local

Client to Site

Local IP Address:

Site to Site

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

Remote

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

DNS Server (for IPSec VPN):

Authentication Method

Pre-Shared Key:

Certificate: (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

My IP Address:

Secure Gateway Address:

Encapsulation Mode:

ESP
 AH

Encryption Algorithm:

Authentication 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.

Protocol	0
Enable Replay Detection	NO
Local Port	
Start	0
End	0
Remote Port	
Start	0
End	0
<hr/>	
Phase 1	
Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Key Group	DH1
<hr/>	
Phase 2	
Active Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy(PFS)	NONE
<hr/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	


Status: **Ready**

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.



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

Active Keep alive NAT Traversal

Name:

Key Management:

Negotiation Mode:

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name:

Password:

Local

Client to Site

Local IP Address:

Site to Site

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

Remote

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

DNS Server (for IPSec VPN):

Authentication Method

Pre-Shared Key:

Certificate: (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

My IP Address:

Secure Gateway Address:

Encapsulation Mode:

ESP AH

Encryption Algorithm: Authentication 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.

The screenshot displays the ZyXEL VPN configuration interface. The left sidebar contains a navigation menu with the following items: WIZARD, SETUP, SYSTEM, LAN, WAN, SUA/NAT, STATIC ROUTE, FIREWALL, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER, REMOTE MGNT, UPnP, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled "VPN - VPN RULE - EDIT - ADVANCED" and features a yellow background. It is divided into three sections: 1. General settings: Protocol (0), Enable Replay Detection (NO), Local Port (Start: 0, End: 0), and Remote Port (Start: 0, End: 0). 2. Phase 1 settings: Negotiation Mode (Main), Encryption Algorithm (DES), Authentication Algorithm (MD5), SA Life Time (Seconds) (28800), and Key Group (DH1). 3. Phase 2 settings: Active Protocol (ESP), Encryption Algorithm (DES), Authentication Algorithm (SHA1), SA Life Time (Seconds) (28800), Encapsulation (Tunnel), and Perfect Forward Secrecy(PFS) (NONE). At the bottom of the configuration area are "Apply" and "Cancel" buttons. A status bar at the bottom left indicates "Status: Ready".

2. The second rule in Branch_B

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

WIZARD

SETUP

SYSTEM

LAN

WAN

SUA/NAT

STATIC ROUTE

FIREWALL

CONTENT FILTER

VPN

CERTIFICATES

AUTH SERVER

REMOTE MGNT

UPnP

LOGS

MAINTENANCE

LOGOUT

Active
 Keep alive
 NAT Traversal

Name:

Key Management:

Negotiation Mode:

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name:

Password:

Local

Client to Site

Local IP Address:

Site to Site

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

Remote

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

DNS Server (for IPSec VPN):

Authentication Method

Pre-Shared Key:

Certificate: (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

My IP Address:

Secure Gateway Address:

Encapsulation Mode:

ESP
 AH

Encryption Algorithm:

Authentication 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.

WIZARD

SETUP

SYSTEM

LAN

WAN

SUA/NAT

STATIC ROUTE

FIREWALL

CONTENT FILTER

VPN

CERTIFICATES

AUTH SERVER

REMOTE MGNT

UPnP

LOGS

MAINTENANCE

LOGOUT

Protocol	<input type="text" value="0"/>
Enable Replay Detection	<input type="text" value="NO"/>
Local Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
Remote Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
<hr/>	
Phase 1	
Negotiation Mode	<input type="text" value="Main"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="MD5"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Key Group	<input type="text" value="DH1"/>
<hr/>	
Phase 2	
Active Protocol	<input type="text" value="ESP"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Encapsulation	<input type="text" value="Tunnel"/>
Perfect Forward Secrecy(PFS)	<input type="text" value="NONE"/>
<hr/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Status: **Ready**

3. Setup VPN in Headquarter

1. The correspondent rule for Branch_A in headquarter

WIZARD

SETUP

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

MAINTENANCE

LOGOUT

- Active
 Keep alive
 NAT Traversal

Name
 Key Management
 Negotiation Mode

- Enable Extended Authentication
 Server Mode (Search [Local User](#) first then [RADIUS](#))
 Client Mode
 User Name
 Password

Local

- Client to Site
 Local IP Address
 Site to Site
 Address Type
 Starting IP Address
 Ending IP Address / Subnet Mask

Remote

- Address Type
 Starting IP Address
 Ending IP Address / Subnet Mask

DNS Server (for IPSec VPN)

Authentication Method

- Pre-Shared Key
 Certificate (See [My Certificates](#))
 Local ID Type
 Content
 Peer ID Type
 Content

My IP Address
 Secure Gateway Address
 Encapsulation Mode

- ESP AH
 Encryption Algorithm Authentication Algorithm
 Authentication Algorithm

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

Protocol	<input type="text" value="0"/>
Enable Replay Detection	<input type="text" value="NO"/>
Local Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
Remote Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
<hr/>	
Phase 1	
Negotiation Mode	<input type="text" value="Main"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="MD5"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Key Group	<input type="text" value="DH1"/>
<hr/>	
Phase 2	
Active Protocol	<input type="text" value="ESP"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Encapsulation	<input type="text" value="Tunnel"/>
Perfect Forward Secrecy(PFS)	<input type="text" value="NONE"/>
<hr/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Status: **Ready**

2. The correspondent rule for Branch_B_1 in headquarter

WIZARD

SETUP

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

MAINTENANCE

LOGOUT

- Active
 Keep alive
 NAT Traversal

Name
 Key Management
 Negotiation Mode

- Enable Extended Authentication
 Server Mode (Search [Local User](#) first then [RADIUS](#))
 Client Mode
 User Name
 Password

Local

- Client to Site
 Local IP Address
 Site to Site
 Address Type
 Starting IP Address
 Ending IP Address / Subnet Mask

Remote

Address Type
 Starting IP Address
 Ending IP Address / Subnet Mask

DNS Server (for IPSec VPN)

Authentication Method

- Pre-Shared Key
 Certificate (See [My Certificates](#))
 Local ID Type
 Content
 Peer ID Type
 Content

My IP Address
 Secure Gateway Address
 Encapsulation Mode

- ESP AH
 Encryption Algorithm Authentication Algorithm
 Authentication Algorithm

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

Protocol	<input type="text" value="0"/>
Enable Replay Detection	<input type="text" value="NO"/>
Local Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
Remote Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
<hr/>	
Phase 1	
Negotiation Mode	<input type="text" value="Main"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="MD5"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Key Group	<input type="text" value="DH1"/>
<hr/>	
Phase 2	
Active Protocol	<input type="text" value="ESP"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Encapsulation	<input type="text" value="Tunnel"/>
Perfect Forward Secrecy(PFS)	<input type="text" value="NONE"/>
<hr/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Status: **Ready**

2. The correspondent rule for Branch_B_2 in headquarter

WIZARD

SETUP

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

MAINTENANCE

LOGOUT

- Active
 Keep alive
 NAT Traversal

Name
 Key Management
 Negotiation Mode

- Enable Extended Authentication
 Server Mode (Search [Local User](#) first then [RADIUS](#))
 Client Mode
 User Name
 Password

Local

- Client to Site
 Local IP Address
 Site to Site
 Address Type
 Starting IP Address
 Ending IP Address / Subnet Mask

Remote

- Address Type
 Starting IP Address
 Ending IP Address / Subnet Mask

DNS Server (for IPSec VPN)

Authentication Method

- Pre-Shared Key
 Certificate (See [My Certificates](#))
 Local ID Type
 Content
 Peer ID Type
 Content

My IP Address
 Secure Gateway Address
 Encapsulation Mode

- ESP AH
 Encryption Algorithm Authentication Algorithm
 Authentication Algorithm

WIZARD

SETUP

SYSTEM

LAN

WAN

SUA/NAT

STATIC ROUTE

FIREWALL

CONTENT FILTER

VPN

CERTIFICATES

AUTH SERVER

REMOTE MGNT

UPnP

LOGS

MAINTENANCE

LOGOUT

Protocol	<input type="text" value="0"/>
Enable Replay Detection	<input type="text" value="NO"/>
Local Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>
Remote Port	
Start	<input type="text" value="0"/>
End	<input type="text" value="0"/>

Phase 1

Negotiation Mode	<input type="text" value="Main"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="MD5"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Key Group	<input type="text" value="DH1"/>

Phase 2

Active Protocol	<input type="text" value="ESP"/>
Encryption Algorithm	<input type="text" value="DES"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
SA Life Time (Seconds)	<input type="text" value="28800"/>
Encapsulation	<input type="text" value="Tunnel"/>
Perfect Forward Secrecy(PFS)	<input type="text" value="NONE"/>

Apply

Cancel

Status: **Ready**