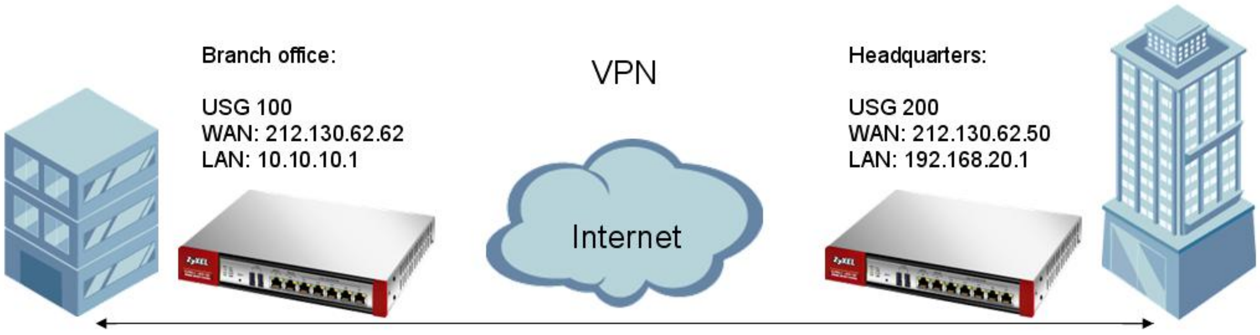
ZyWALL USG-Series

How to setup a Site-to-site VPN connection between two ZyWALL USG series.

Table of content

Introduction

This guide will explain how to configure a site-to-site VPN connection as shown in the picture below:



In the above scenario the clients at the Branch office wants to be able to access the Headquarters entire LAN subnet and vice versa. The setup will be the same regardless what ZyWALL USG model you are using. In this example we will be looking at a ZyWALL USG 100 and ZyWALL USG 200.

To setup this scenario you need to configure the following in both ZyWALL USG’s:

- Address object for remote subnet.
- VPN Gateway.
- VPN Connection.

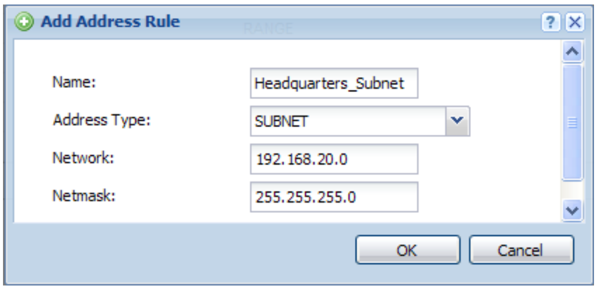
After configuring these three things on both ZyWALL USG’s, you will have established the connection.

ZyWALL USG 100

Creating the address objects

Go to Configuration > Object > Address and click the Add button.

Now create a Subnet address that contains the LAN Subnet of the opposite ZyWALL USG as shown in the picture below:



Add Address Rule

Name: Headquarters_Subnet

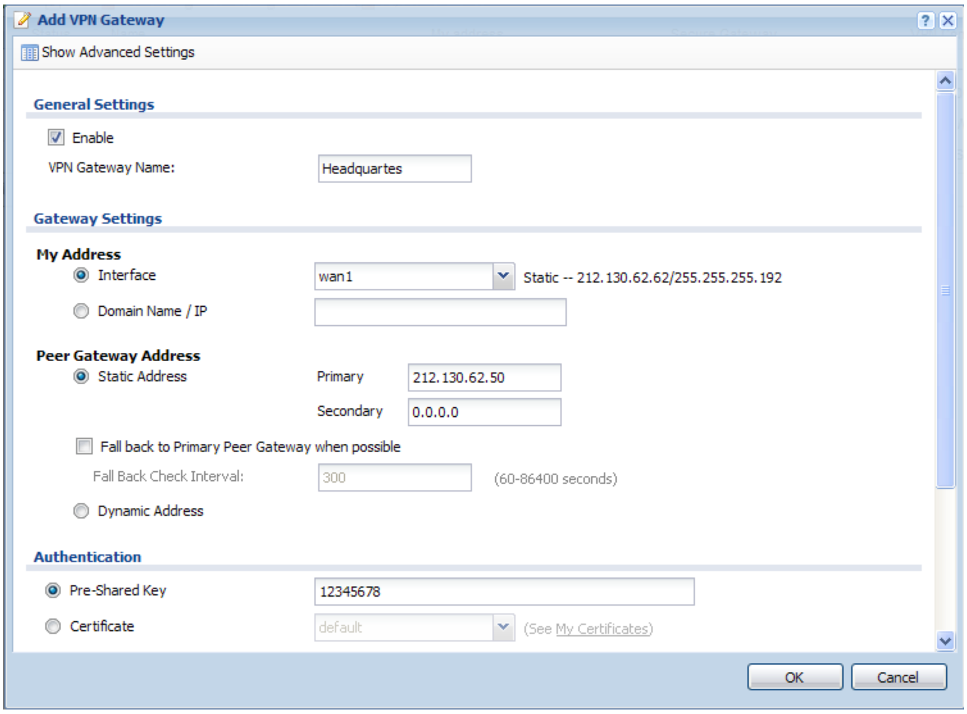
Address Type: SUBNET

Network: 192.168.20.0

Netmask: 255.255.255.0

Creating VPN Gateway

Go to Configuration > VPN > IPSec VPN > VPN Gateway and click the Add button. You need to make sure the Gateway is enabled. Fill in the Interface field with the WAN IP of the ZyWALL USG 100. For Peer Gateway Address you should chose Static Address and type in the remote ZyWALL USG 200 WAN IP. You also need to type in a Pre-Shared Key of the VPN connection. This key should match that of the remote ZyWALL USG 200.



Add VPN Gateway

Show Advanced Settings

General Settings

☑ Enable

VPN Gateway Name: Headquartes

Gateway Settings

My Address

● Interface wan1 Static -- 212.130.62.62/255.255.255.192

○ Domain Name / IP

Peer Gateway Address

● Static Address Primary 212.130.62.50

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

○ Dynamic Address

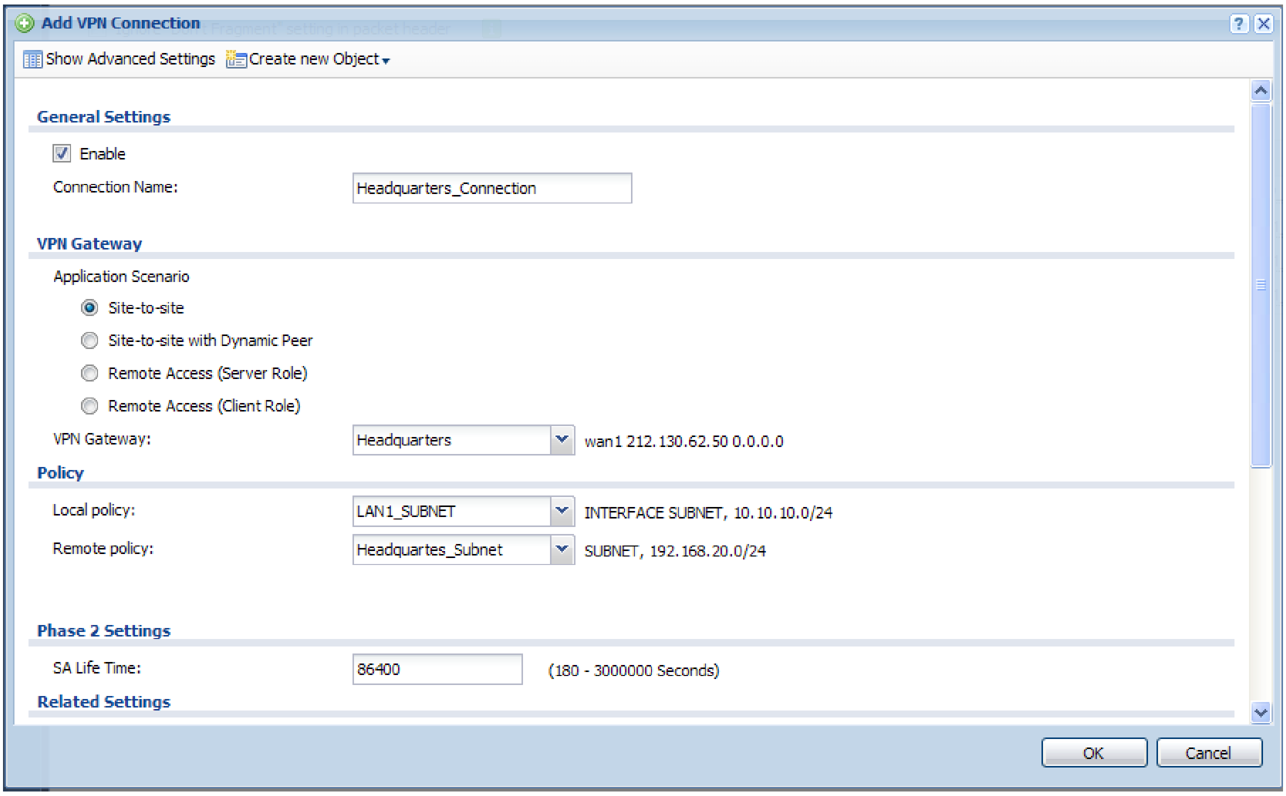
Authentication

● Pre-Shared Key 12345678

○ Certificate default (See My Certificates)

Creating VPN Connection

Go to Configuration > VPN > IPSec VPN > VPN Connection and click the Add button. Enable the Connection. Under Application Scenario chose Site-to-site. Make sure that you select the correct VPN Gateway, in this case Headquarters. In Local policy select the LAN Subnet of the ZyWALL USG 100. In Remote policy you need to select the Address object created earlier in this guide.



General Settings

☑ Enable

Connection Name: Headquarters_Connection

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

VPN Gateway: Headquarters wan1 212.130.62.50 0.0.0.0

Policy

Local policy: LAN1_SUBNET INTERFACE SUBNET, 10.10.10.0/24

Remote policy: Headquartes_Subnet SUBNET, 192.168.20.0/24

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Related Settings

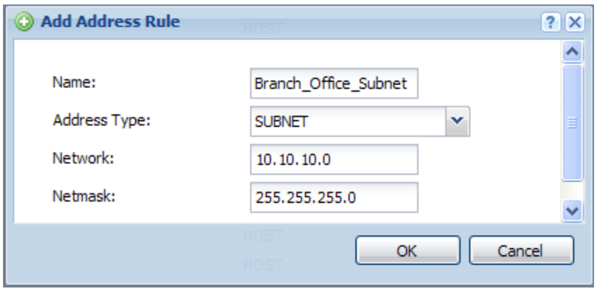
You have now finished the required configurations on the ZyWALL USG 100.

ZyWALL USG 200

Creating the address objects

Go to Configuration > Object > Address and click the Add button.

Now create a Subnet address that contains the LAN Subnet of the opposite ZyWALL USG as shown in the picture below:



Add Address Rule

Name: Branch_Office_Subnet

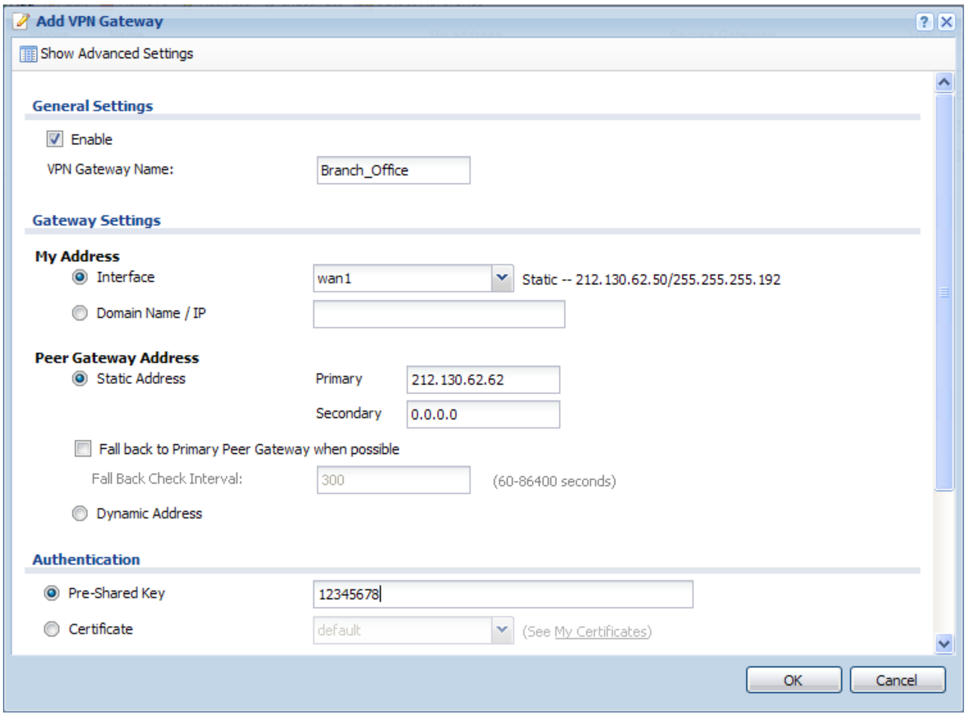
Address Type: SUBNET

Network: 10.10.10.0

Netmask: 255.255.255.0

Creating VPN Gateway

Go to Configuration > VPN > IPSec VPN > VPN Gateway and click the Add button. You need to make sure the Gateway is enabled. Fill in the Interface field with the WAN IP of the ZyWALL USG 200. For Peer Gateway Address you should chose Static Address and type in the remote ZyWALL USG 100 WAN IP. You also need to type in a Pre-Shared Key of the VPN connection. This key should match that of the remote ZyWALL USG 100.



Add VPN Gateway

Show Advanced Settings

General Settings

☑ Enable

VPN Gateway Name: Branch_Office

Gateway Settings

My Address

● Interface wan1 Static -- 212.130.62.50/255.255.255.192

○ Domain Name / IP

Peer Gateway Address

● Static Address Primary 212.130.62.62

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

○ Dynamic Address

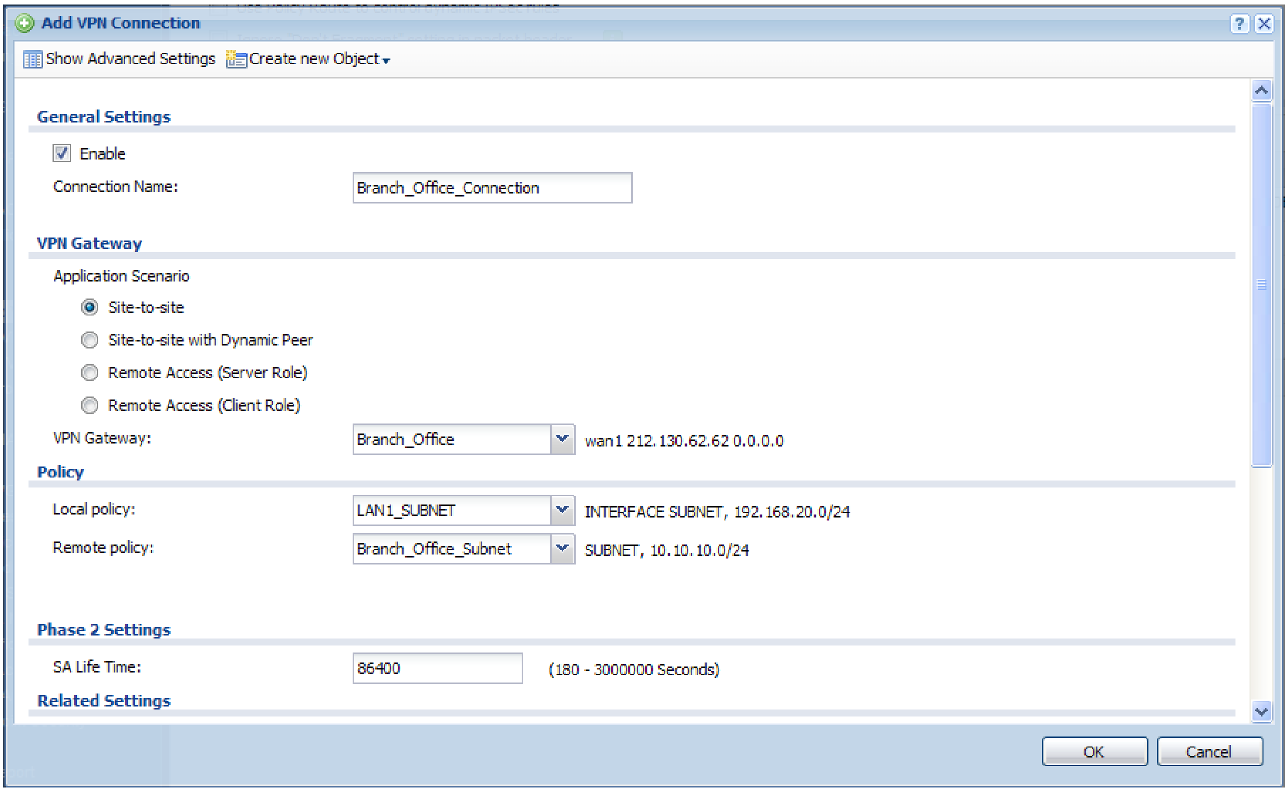
Authentication

● Pre-Shared Key 12345678

○ Certificate default (See My Certificates)

Creating VPN Connection

Go to Configuration > VPN > IPSec VPN > VPN Connection and click the Add button. Enable the Connection. Under Application Scenario chose Site-to-site. Make sure that you select the correct VPN Gateway, in this case Branch_Office. In Local policy select the LAN Subnet of the ZyWALL USG 200. In Remote policy you need to select the Address object created earlier in this guide.



General Settings

☑ Enable

Connection Name: Branch_Office_Connection

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

VPN Gateway: Branch_Office wan1 212.130.62.62 0.0.0.0

Policy

Local policy: LAN1_SUBNET INTERFACE SUBNET, 192.168.20.0/24

Remote policy: Branch_Office_Subnet SUBNET, 10.10.10.0/24

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Related Settings

You have now finished the required configurations on the ZyWALL USG 200.

Establish connection

Both ZyWALL USG's are now configured. The only thing left, is to establish the VPN connection. This can be done manually by selecting your VPN connection and clicking the Connect button in Configuration > VPN > IPSec VPN > VPN Connection. Alternatively you can edit the VPN Connection rule, click Show Advance Settings and enable Nailed-Up. With Nailed-Up enabled the VPN tunnel will connect up automatically when the ZyWALL USG boots up.

All devices at the Branch Office will now be able to access devices and computers on the Headquarters subnet and vice versa.