equinux

VPN Configuration Guide

FortiOS

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinux has been advised of the possibility of such damages.

Every effort has been made to ensure that the information in this configuration guide is accurate. equinux is not responsible for printing or clerical errors.

Configuration guide revision 1

Created using Apple Pages.

www.equinux.com

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your Fortinet VPN gateway to establish a VPN connection between them.

Using the Configuration Guide

Part 1 – VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your Fortinet VPN gateway device using the web configuration interface.

⚠ This guide is a supplement to the documentation included with your Fortinet VPN gateway device, it can't replace it. Please read this documentation before starting.

Part 2 – VPN Tracker Configuration

In the second part, this guide will show you how to configure VPN Tracker to easily connect to your newly created VPN tunnel.

Part 3 – Troubleshooting and Supporting Multiple Users

Troubleshooting advice and instructions on how to set up the VPN to support multiple users using either static IP address assignment or Mode Config can be found in the final part of this guide.

💡 If you are setting up VPN on your device for the first time, we strongly recommend you keep to the tutorial-style setup in the first and second part of this document and make modifications only after you have tested the basic setup.

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser:

http://equinux.com

Links to Other Parts of this Guide

A → *Link* will take you to another place in the configuration guide. Simply click it if you are reading this guide on your computer.

Tips and Tricks

💡 This configuration guide contains lots of great tips. You can easily spot them by looking for the light bulb icon.

Warnings

⚠ This exclamation mark warns you when there is a setting or action where you need to take particular care.

Getting Help

VPN Tracker makes VPN simple. However, computer networking and VPNs can be complex and tricky at times, so we have also built in tools and helpful features that will assist you if you ever run into problems. Check out → *Troubleshooting* for more information.

Prerequisites

Your VPN Gateway

- This guide applies to **FortiOS**-based VPN gateways
- Make sure you have the **newest firmware** version installed that is available for your device. This guide was created based on FortiOS 4.0 MR1 Patch 3
- Older revisions of FortiOS (FortiOS 4.0 or FortiOS 3.0) should work fine for the basic setup as described in the first part of this document
- The setup using Mode Config that is described in the final part of this document requires at least FortiOS 4.0 MR1 Patch 3

Your Mac

VPN Tracker runs on Mac OS X 10.4, 10.5 and 10.6

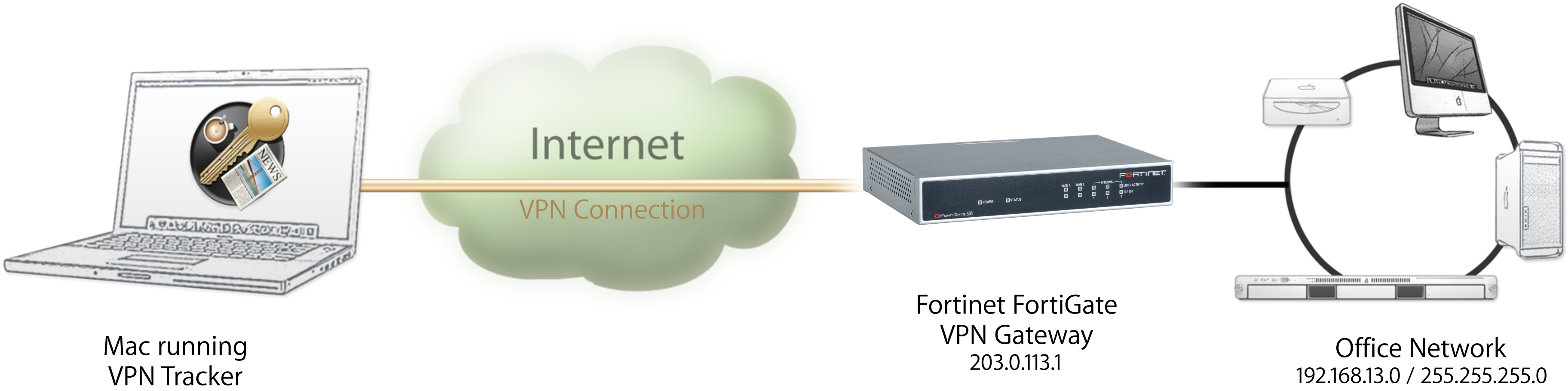
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from http://www.vpntracker.com

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram on the bottom of this page illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's Fortinet VPN gateway device (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address or DNS host name. In our example setup, we will be using a static IP address: 203.0.113.1.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network is using the network 192.168.13.0/24 (which is the same as 192.168.13.0/255.255.255.0). This is the network that will be accessed from the employee's Mac through the VPN. It is called the "Remote Network" in VPN Tracker.



Terminology

A VPN connection is often called a "tunnel" (or "VPN tunnel"). Every VPN tunnel is established between two "endpoints". In our example one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is called the other endpoint's "peer".

Please note that for each endpoint, the settings on the other endpoint are considered to be "remote", while its own settings are considered to be "local". That means a "local" setting from VPN Tracker's perspective, is a "remote" setting from the VPN gateway's perspective, and vice versa.

The sample configuration described in this guide is called a "Host to Network" configuration: a single computer, called a "Host" establishes a VPN tunnel to an entire "Network" behind the VPN gateway.

My VPN Gateway Configuration

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker. This information is marked with red numbers to make it easier to reference it later. You can print out this checklist to help keep track of the various settings of your Fortinet VPN gateway device.

IP Addresses

❶ LAN (internal) IP Address / Subnet Mask: ______.______.______.______ / ______.______.______.______

❷ WAN IP Address: ______.______.______.______ (or hostname ____________________________)

User Authentication (XAUTH)

❸ Username: ____

❹ Password: ____

Pre-Shared Key

❺ Pre-Shared Key: ____________________________________

Additional Settings (only for Option B – Assigning IP Addresses through Mode Config)

❻ Name of the Phase 1 Setup: ____

❼ Address Object for the Internal (LAN) Network: __________________________

❽ Mode Config Address Range: _____.______.______.______ – ❾ _____.______.______.

Task 1 – VPN Gateway Configuration

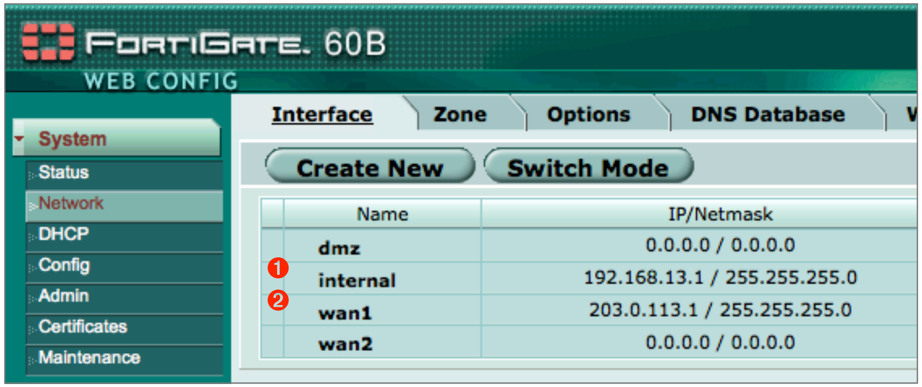
We will first set up VPN on the VPN gateway. If you already have VPN in place, it's helpful to follow along this tutorial to see how settings on the device fit together with VPN Tracker.

Step 1 – Retrieve Network Settings

- Connect to your VPN gateway through its web configuration interface

We have found **Firefox** to work best with the FortiOS Web Config interface (as of FortiOS 4.0). If you see extra options or some buttons do not work with your web browser, try using Firefox.

- Go to **System** > **Network**

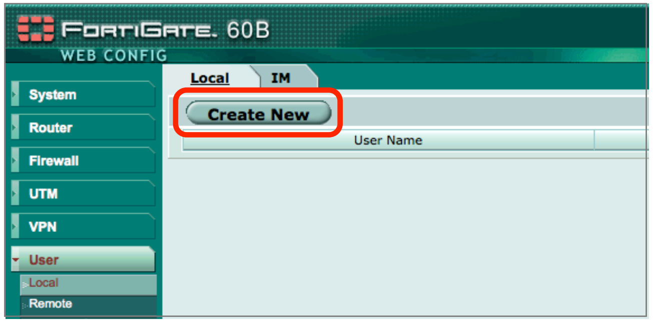


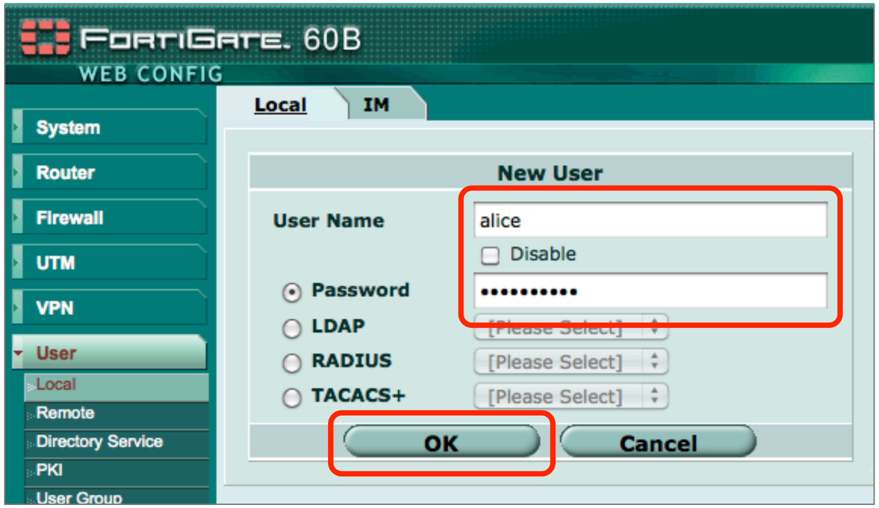
	Name	IP/Netmask
	dmz	0.0.0.0 / 0.0.0.0
❶	internal	192.168.13.1 / 255.255.255.0
❷	wan1	203.0.113.1 / 255.255.255.0
	wan2	0.0.0.0 / 0.0.0.0

- Write down the IP address of the **internal** network interface, including its subnet mask as ❶ on your → *Configuration Checklist*
- Write down the IP address of the **wan1** network interface (the part before the forward slash "/") as ❷ on your → *Configuration Checklist*. If your device has a DNS hostname (fixed or DynDNS), write it down instead.

Step 2 – Create a VPN User

- Go to **User** > **Local** and click **Create New**





New User

User Name	alice
	☐ Disable
● Password	••••••••••
○ LDAP	[Please Select]
○ RADIUS	[Please Select]
○ TACACS+	[Please Select]

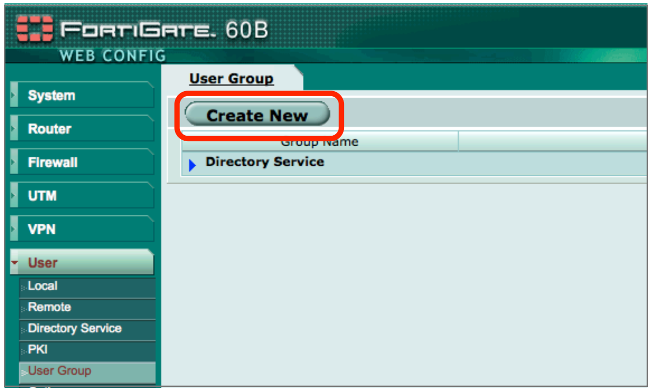
OK Cancel

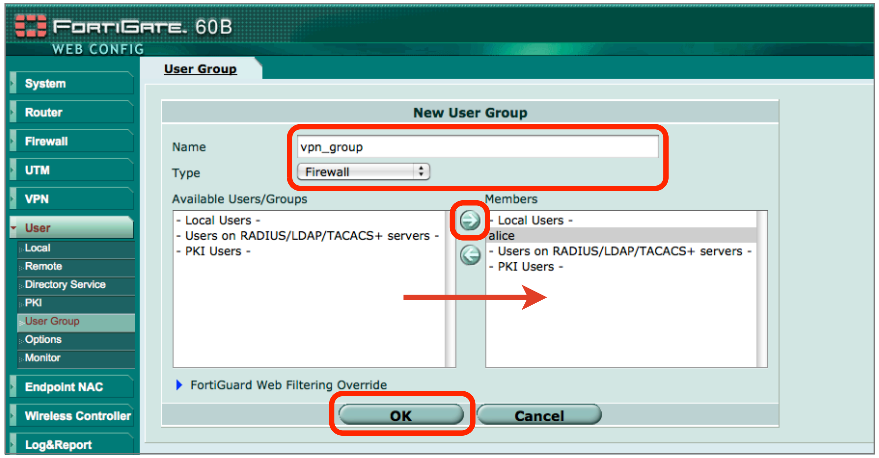
- **User Name**: Enter a username for the new user (here: **alice**). Write down the user name as ❸
- **Password**: Enter a password for this new user. Make sure to remember the password, or write it down as ❹
- Click **OK** to add the user

To add more users, simply repeat this step. You might want to connect the device to an existing (LDAP or RADIUS) authentication server, however, we recommend using a local user for the initial setup and testing.

Step 3 – Create a VPN User Group

- Go to **User** > **User Group** and click **Create New**





New User Group

Name: vpn_group

Type: Firewall

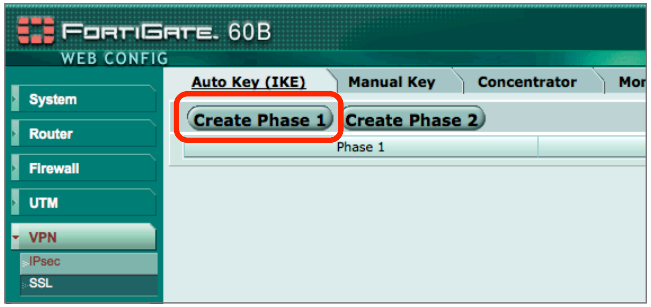
Available Users/Groups:
- Local Users -
- Users on RADIUS/LDAP/TACACS+ servers -
- PKI Users -

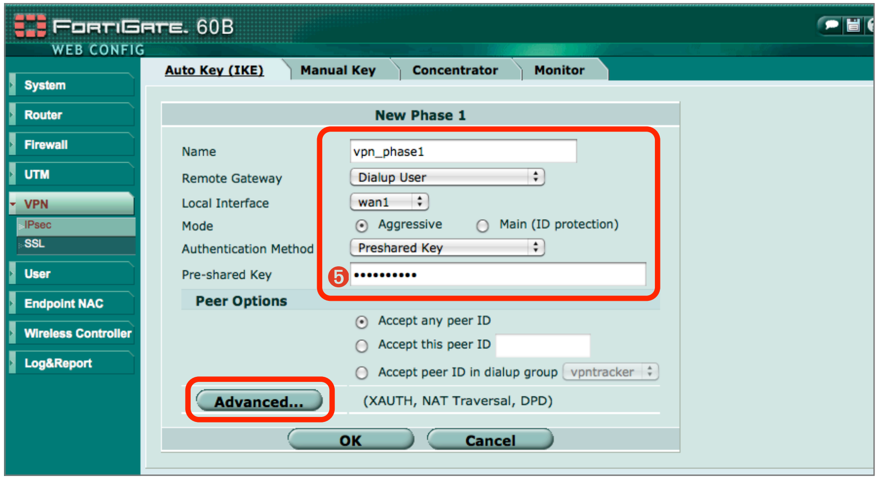
Members:
- Local Users -
alice
- Users on RADIUS/LDAP/TACACS+ servers -
- PKI Users -

- **Name:** Enter a name for the user group (here: **vpn_group**)
- **Type:** Choose **Firewall** from the popup list
- Move the user account(s) you created in → *Step 2* from the **Available Users/Groups** column into the **Members** column on the right
- Click **OK** to create the group

Step 4 – Set up Phase 1

- Go to **VPN** > **IPsec** and click **Create Phase 1**





New Phase 1

Name: vpn_phase1

Remote Gateway: Dialup User

Local Interface: wan1

Mode: ● Aggressive ○ Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key: ❺ ••••••••••

Peer Options

● Accept any peer ID

○ Accept this peer ID

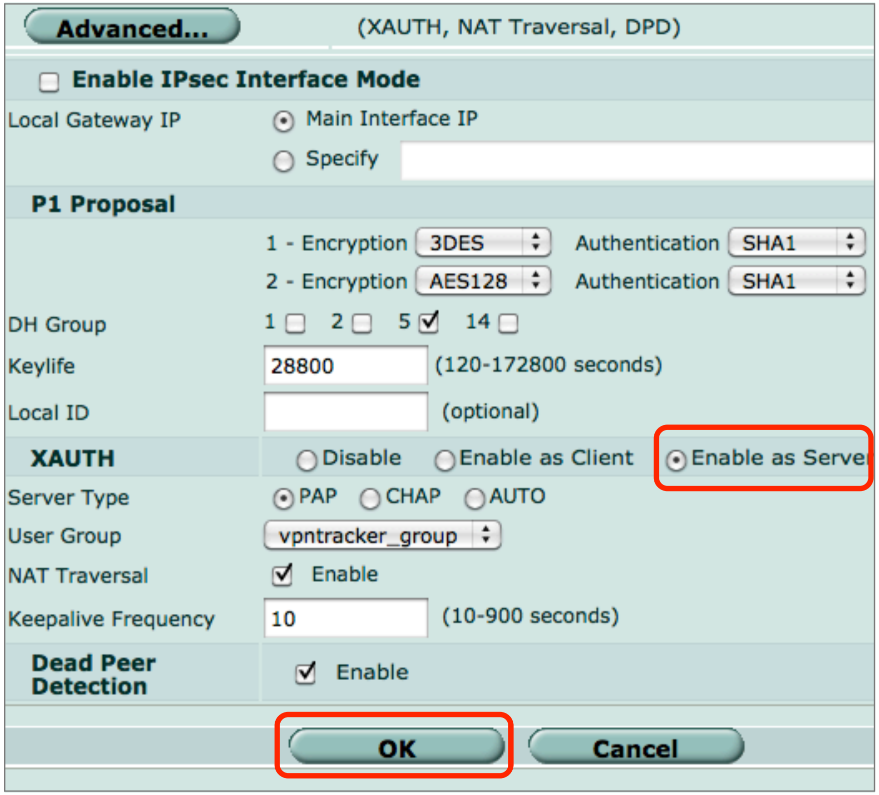
○ Accept peer ID in dialup group vpntracker

Advanced... (XAUTH, NAT Traversal, DPD)

- **Name**: Enter a name for the phase 1 setup (here:**vpn_phase1**)
- **Remote Gateway**: Choose **Dialup User** from the popup list
- **Local Interface**: Choose **wan1** from the popup list
- **Mode**: Choose **Aggressive** mode
- **Authentication Method**: Select **Pre-Shared Key**
- Enter a **Pre-Shared Key**. Make sure to choose a good pre-shared key and remember it, or write it down as ❺

Advanced Settings

- Click **Advanced…** to reveal additional settings



Advanced… (XAUTH, NAT Traversal, DPD)

□ **Enable IPsec Interface Mode**

Local Gateway IP	● Main Interface IP ○ Specify
P1 Proposal	
	1 - Encryption 3DES Authentication SHA1 2 - Encryption AES128 Authentication SHA1
DH Group	1 □ 2 □ 5 ☑ 14 □
Keylife	28800 (120-172800 seconds)
Local ID	(optional)
XAUTH	○ Disable ○ Enable as Client ● Enable as Serve
Server Type	● PAP ○ CHAP ○ AUTO
User Group	vpntracker_group
NAT Traversal	☑ Enable
Keepalive Frequency	10 (10-900 seconds)
Dead Peer Detection	☑ Enable

If clicking **Advanced** does not work, your web browser might be incompatible with the web config interface. In our experience, Firefox works well for this task.

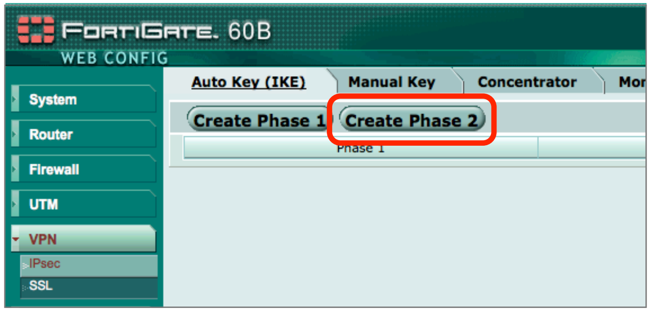
- **XAUTH**: Choose **Enable as Server**

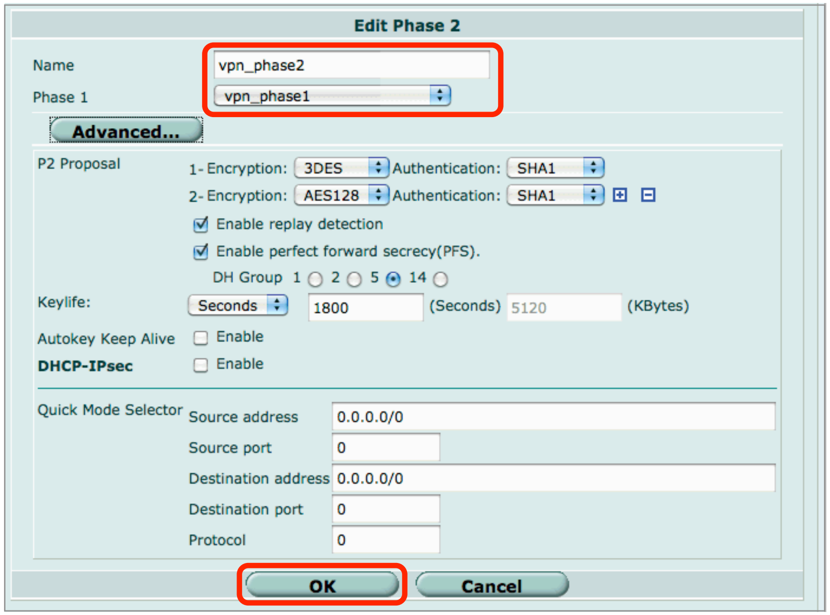
When **Enable as Server** option is not selectable, you may have skipped creating a **User Group** in → *Step 3*. Please go back and complete this step.

- Click **OK** to save the phase 1 settings

Step 5 – Set up Phase 2

- Click **Create Phase 2**





Edit Phase 2

Name	vpn_phase2
Phase 1	vpn_phase1

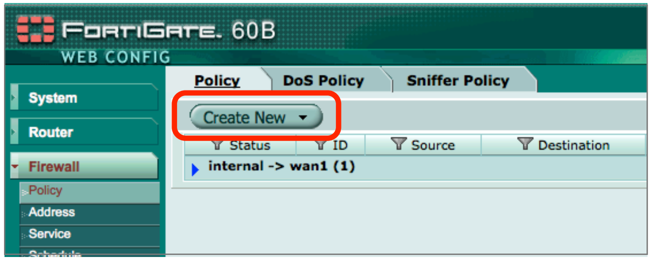
Advanced…

P2 Proposal	1- Encryption: 3DES Authentication: SHA1 2- Encryption: AES128 Authentication: SHA1 ☑ Enable replay detection ☑ Enable perfect forward secrecy(PFS). DH Group 1 ○ 2 ○ 5 ● 14 ○
Keylife:	Seconds 1800 (Seconds) 5120 (KBytes)
Autokey Keep Alive	□ Enable
DHCP-IPsec	□ Enable
Quick Mode Selector	Source address 0.0.0.0/0 Source port 0 Destination address 0.0.0.0/0 Destination port 0 Protocol 0

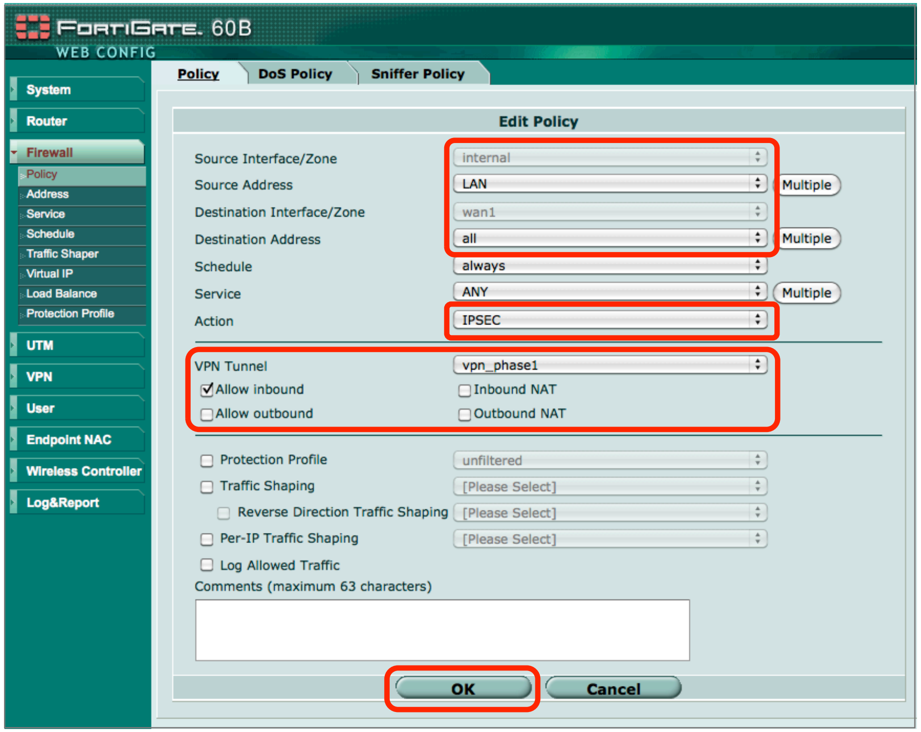
- **Name**: Enter a name for the phase 2 setup (here:**vpn_phase2**)
- **Phase 1:** Select the phase 1 setup you created in → *Step 4* from the popup list (here:**vpn_phase1**)
- Click **OK**

Step 6 – Set up a Firewall Policy

- Go to **Firewall** > **Policy** and click **Create New**



internal -> wan1 (1)



Edit Policy

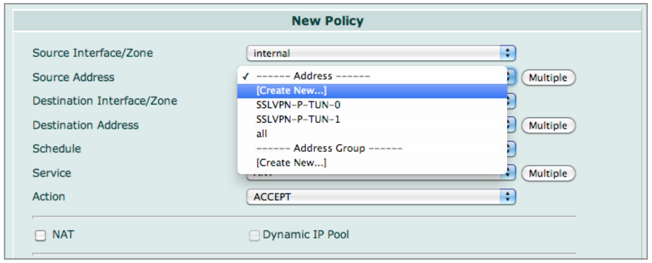
Source Interface/Zone	internal
Source Address	LAN
Destination Interface/Zone	wan1
Destination Address	all
Schedule	always
Service	ANY
Action	IPSEC
VPN Tunnel	vpn_phase1
☑ Allow inbound	☐ Inbound NAT
☐ Allow outbound	☐ Outbound NAT
☐ Protection Profile	unfiltered
☐ Traffic Shaping	[Please Select]
☐ Reverse Direction Traffic Shaping	[Please Select]
☐ Per-IP Traffic Shaping	[Please Select]
☐ Log Allowed Traffic	

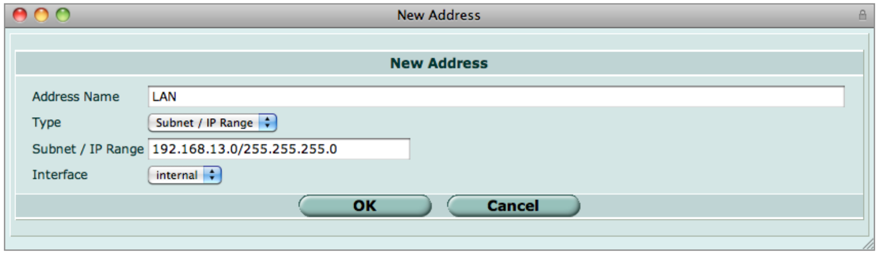
Comments (maximum 63 characters)

- **Source Interface/Zone**: Choose **internal** from the popup list
- **Source Address**: Select the address object representing your Fortinet VPN gateway's internal network (here: **LAN**). If you do not yet have such an address object, create a new one (see the right side if you don't know how)
- **Destination Interface/Zone**: Choose **wan1** from the popup list
- **Destination Address: Select all**
- **Action**: Choose **IPSEC** (earlier FortiOS versions: **ENCRYPT**) from the popup list. Additional options will become available:
  - **VPN Tunnel**: Select the phase 1 setup you have created in → *Step 4* (here: **vpn_phase1**) from the popup list
  - **Allow outbound**: The connection will always be initiated from VPN Tracker, never by the device, so you can deselect this option.
- Click **OK** to add the policy

Creating an address object representing the internal (LAN) network:

- Click **Create New…**





New Address

Address Name	LAN
Type	Subnet / IP Range
Subnet / IP Range	192.168.13.0/255.255.255.0
Interface	internal

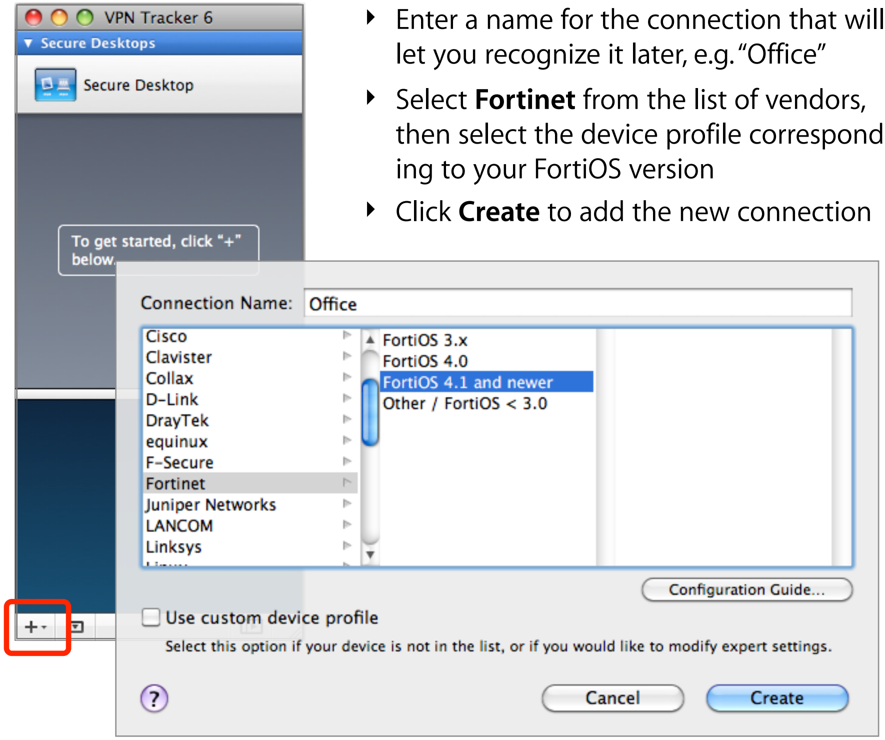
- **Address Name**: Enter a name for the new address object (e.g. **LAN**)
- **Type**: Select **Subnet / IP Range**
- **Subnet / IP Range**: Enter your VPN gateway's internal (LAN) network address and subnet mask. Make sure to **use the network address, not the LAN IP address**: With a 255.255.255.0 subnet mask this means setting the last part of LAN IP address ❶ to 0 (e.g. 192.168.13.1 becomes 192.168.13.0)
- **Interface**: Select **internal**
- Click **OK** to add the new address object

Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed → *configuration checklist* containing your Fortinet VPN gateway's settings. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection

Open VPN Tracker, and click the plus button in the bottom left corner of the window to add a new connection:



Connection Name: Office

Fortinet – FortiOS 4.1 and newer

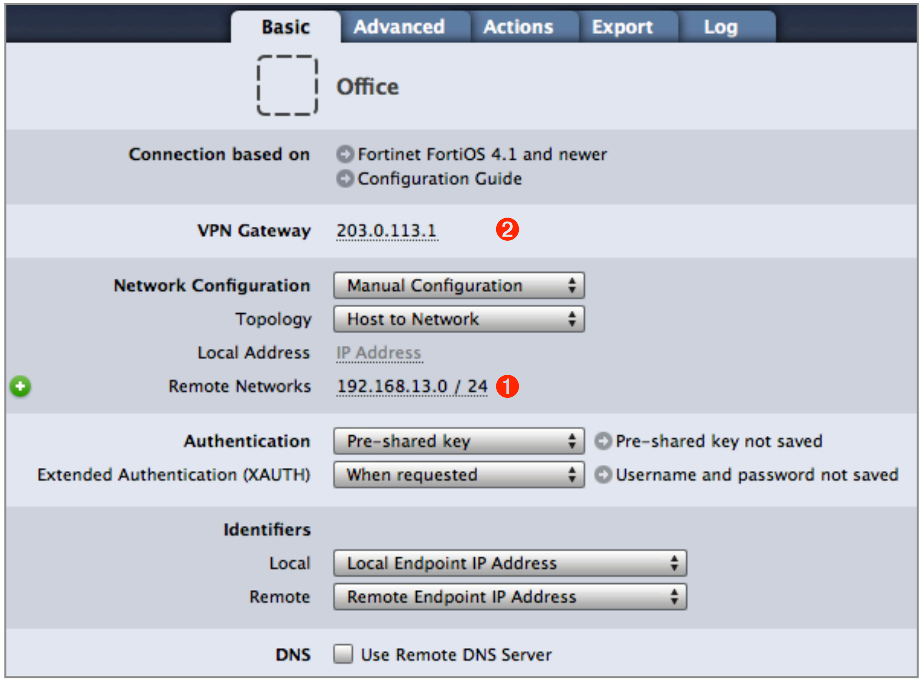
□ Use custom device profile

Select this option if your device is not in the list, or if you would like to modify expert settings.

- Enter a name for the connection that will let you recognize it later, e.g. "Office"
- Select **Fortinet** from the list of vendors, then select the device profile corresponding to your FortiOS version
- Click **Create** to add the new connection

Step 2 – Configure the VPN Connection

Once you have added the new connection, there are a few settings that need to be customized to match what is configured on your VPN gateway.



Connection based on: Fortinet FortiOS 4.1 and newer; Configuration Guide

VPN Gateway: 203.0.113.1 ❷

Network Configuration: Manual Configuration

Topology: Host to Network

Local Address: IP Address

Remote Networks: 192.168.13.0 / 24 ❶

Authentication: Pre-shared key — Pre-shared key not saved

Extended Authentication (XAUTH): When requested — Username and password not saved

Identifiers

Local: Local Endpoint IP Address

Remote: Remote Endpoint IP Address

DNS: □ Use Remote DNS Server

- **VPN Gateway**: Enter the WAN IP address (or hostname) of your VPN gateway that you wrote down as ❷
- **Local Address**: Leave empty for now. Depending on your setup, you may have to set a specific local address later. Refer to → *Supporting Multiple Users* on when and how to set a specific local address.
- **Remote Networks**: Enter the network address of the network that is being accessed through the VPN tunnel ❶. Separate the subnet mask with a forward slash („/").

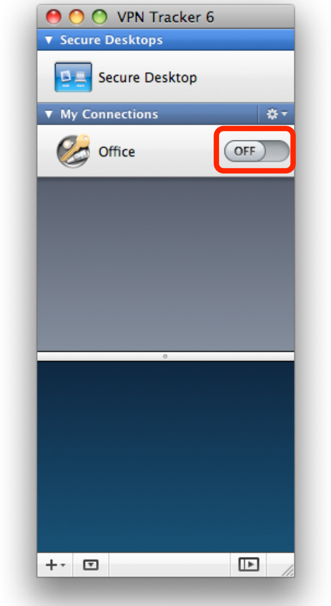
⚠ VPN Tracker will automatically turn the IP address into a network address. Double-check that the result is the same as the LAN address object configured for the policy in → *Step 6*

Step 3 – Test the VPN Connection

It 's time to go out!

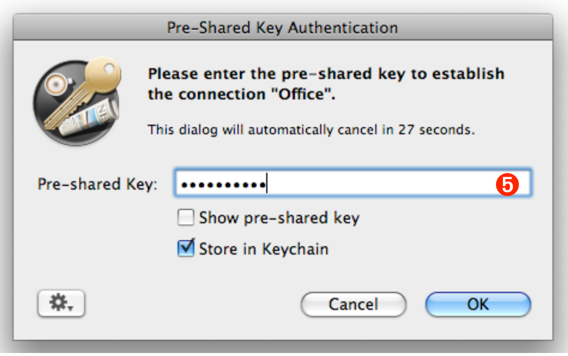
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting up a VPN connection to your home network, test it from an Internet cafe, or go visit a friend.

Start your connection



- Connect to the Internet
- Make sure that your Internet connection is working – open your Internet browser and try to connect to http://www.equinux.com
- Open VPN Tracker if it's not already running
- Slide the On/Off slider for the connection you have just configured to **On**

When prompted for your pre-shared key:



Pre-Shared Key Authentication

Please enter the pre-shared key to establish the connection "Office".

This dialog will automatically cancel in 27 seconds.

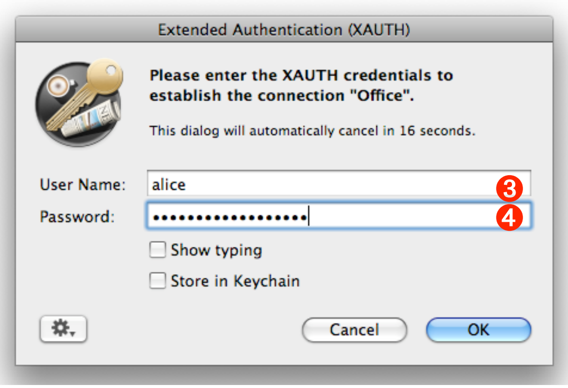
Pre-shared Key: •••••••••• ❺

□ Show pre-shared key

☑ Store in Keychain

- **Pre-shared key**: Enter the pre-shared key that you configured on the Fortinet VPN gateway in the phase 1 settings ❺
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**

When prompted for your Extended Authentication (XAUTH) credentials:



Extended Authentication (XAUTH)

Please enter the XAUTH credentials to establish the connection "Office".

This dialog will automatically cancel in 16 seconds.

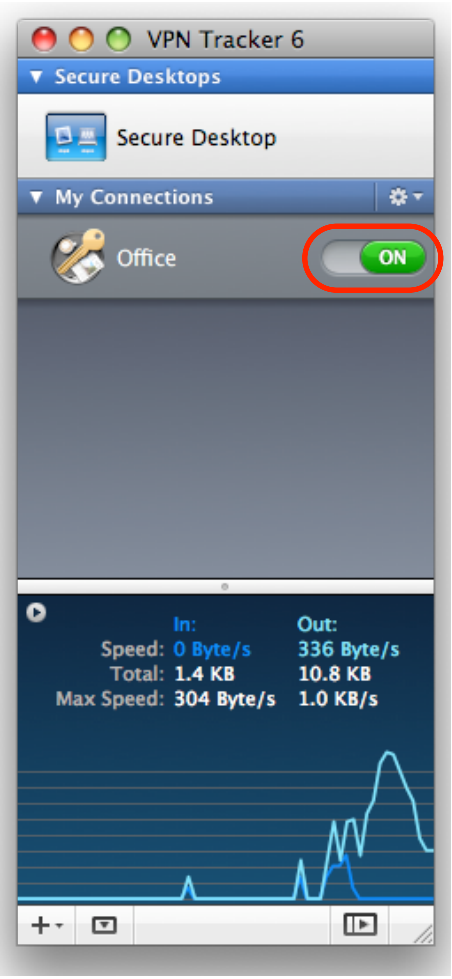
User Name: alice ❸

Password: ••••••••••••••••• ❹

□ Show typing

□ Store in Keychain

- **User Name**: Enter the name of the user you have added on the Fortinet VPN gateway (here: **alice**) ❸
- **Password**: Enter the password for the user ❹
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**



```
                In:          Out:
     Speed:  0 Byte/s     336 Byte/s
     Total:  1.4 KB       10.8 KB
 Max Speed:  304 Byte/s   1.0 KB/s
```

- If the slider goes back to **Off** after starting the connection, or after entering your pre-shared key or your XAUTH credentials, please read the → *Troubleshooting* section of this document
- If the slider goes to **On** and turns green after a while, you have successfully established a connection
- Congratulations!

Troubleshooting

In most cases, your connection should work fine if you follow the instructions above. If you cannot connect, please read on.

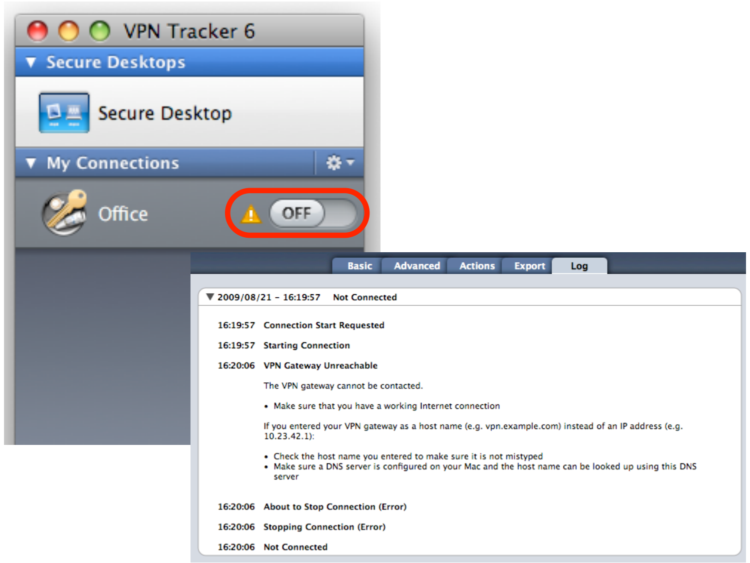
VPN Connection Fails to Establish

On/Off Slider goes back to “Off” right away

If the slider goes back to “Off” right away, please make sure you have entered all the required information. VPN Tracker will highlight fields that are missing or obviously incorrect information.

On/Off Slider goes back to “Off” after a while

If the connection ON/OFF slider goes back to “OFF” a while after attempting to start the connection, please go to the “Log” tab to get more information about the error (or click the warning triangle to be automatically taken to the “Log” tab). VPN Tracker will display detailed suggestions for a solution:



```
▼ 2009/08/21 – 16:19:57    Not Connected

  16:19:57   Connection Start Requested

  16:19:57   Starting Connection

  16:20:06   VPN Gateway Unreachable

             The VPN gateway cannot be contacted.

             • Make sure that you have a working Internet connection

             If you entered your VPN gateway as a host name (e.g. vpn.example.com) instead of an IP address (e.g.
             10.23.42.1):

             • Check the host name you entered to make sure it is not mistyped
             • Make sure a DNS server is configured on your Mac and the host name can be looked up using this DNS
               server

  16:20:06   About to Stop Connection (Error)

  16:20:06   Stopping Connection (Error)

  16:20:06   Not Connected
```

No Access to the Remote Network

If the connection slider goes to ON and turns green, but you cannot access resources (servers, email, etc.) in the VPN, please check the following points.

Connect to an IP address (instead of a host name)

If you are not connecting to the resource by IP address (e.g. 192.168.13.42), but are using a host name (e.g. server.example.com), please try using the resource’s IP address instead. If the connection works when using the IP address, but not when using a host name, please make sure that your Mac’s DNS server or the “Remote DNS” server that you have configured on your Fortinet VPN gateway is able to resolve this host name to an IP address.

Test VPN Availability again

In many networks your Mac will be behind a router that performs Network Address Translation (NAT). For a VPN connection to be established through such a router, VPN Tracker can use different methods, but not all of them may be supported by your local router or your VPN gateway.

VPN Tracker automatically runs a test to detect the proper method for your particular Internet connection when you first connect using this Internet connection. However, test results could become outdated by changes to the local router, so it is a good idea to test again if there are problems.

- Select “Tools > Test VPN Availability” from the menu
- Click “Test Again” and wait until the test has completed
- Try connecting again

Check that the IP address you are connecting to is part of the network(s) permitted in the split tunneling setup

Check that the IP address you are connecting to is actually part of the remote network(s) you permitted in the firewall policy in → *Step 6*. Also double-check the network mask(s) of the address object(s).

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

http://www.equinux.com/support

If you need to contact equinux Technical Support

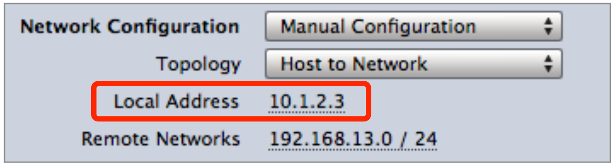
If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include at least the following information:

- The manufacturer and model and firmware revision of the VPN gateway
- A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings
- A description of the problem and the troubleshooting steps you have taken

Supporting Multiple Users

Once your VPN expands to multiple users you must ensure that IP addresses do not conflict by assigning each user their own IP address. VPN Tracker supports manually assigning IP addresses and assignment through Mode Config.

How IP Addresses are Assigned to VPN Clients



Network Configuration: Manual Configuration

Topology: Host to Network

Local Address: 10.1.2.3

Remote Networks: 192.168.13.0 / 24

The **Local Address** in VPN Tracker is the IP address that the Mac will be using in the remote network when connected though VPN. In IPsec terms: The Local Address is the **local endpoint of the IPsec Security Association (SA)**.

- If the Local Address field contains a **fixed address** this address is used. The address must be unique among all users of the VPN connection

  → *Option A – Manually Assigning Fixed Local Addresses*

- When **Mode Config** mode is used, the local address is **assigned automatically** by the VPN gateway

  → *Option B – Assigning IP Addresses through Mode Config*

- If the Local Address field is left **empty**, the Mac's actual local IP address (as shown in System Preferences > Network) is used

⚠ It is **not** possible to use an empty Local Address if

- the VPN has **multiple users** (IPs might conflict)
- the VPN gateway is **not the default gateway (router)** in its network

Option A
Manually Assigning Fixed Local Addresses

Step 0 – Check Requirements

Manually assigning fixed local address **works with any setup**, however the administrative effort may be too high if the VPN has a large number of users or users change often.

Step 1 – Choose the Local Addresses

Choose the local addresses for your VPN clients so that

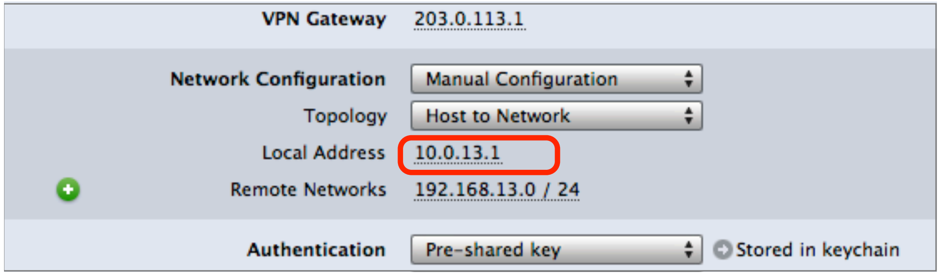
- the local addresses are **not** part of the VPN's remote network (= the Fortinet VPN gateway's LAN)
- each client has its **own, unique** IP address

⚠ The IP addresses may **not** come from the remote network because the Fortinet VPN gateway cannot act as an ARP proxy for manually assigned IP addresses.

Example: The Fortinet VPN gateway 's LAN in our example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). For the local addresses, choose an arbitrary private network that is not part of this network, such as 10.0.13.0/24. For each user, pick a different IP address from that network to be used as the Local Address in VPN Tracker:

User	IP Address
alice	10.0.13.1
bob	10.0.13.2
charlie	10.0.13.3
…	10.0.13...

Step 2 – Configure the Local Address in VPN Tracker



VPN Gateway 203.0.113.1

Network Configuration: Manual Configuration

Topology: Host to Network

Local Address: 10.0.13.1

Remote Networks: 192.168.13.0 / 24

Authentication: Pre-shared key — Stored in keychain

- **Local Address**: Enter the IP address that you have chosen for this user (here: 10.0.13.1 for the user alice)

If your VPN gateway is **not** the default gateway (router) of its network, you will have to ensure that traffic for the chosen IP addresses is routed back to the VPN gateway instead of to the usual default gateway (e.g. by adding a route on the default gateway to the VPN gateway for these IPs).

Option B
Assigning IP Addresses through Mode Config

Step 0 – Check Requirements

Assigning IP addresses through Mode Config **requires FortiOS 4.0 MR 1 Patch 3** or higher. It is necessary to switch the VPN setup to an interface mode (route-based) VPN and to use the command line interface (CLI) for some parts of the setup procedure.

Mode Config is only available with IPsec Interface Mode. We will therefore set up the connection to use interface mode.

FortiOS supports both Mode Config, as well as Cisco's EasyVPN extensions. Since VPN Tracker also supports EasyVPN, we will be using EasyVPN, although a setup using only Mode Config without Cisco's extensions would also be possible.

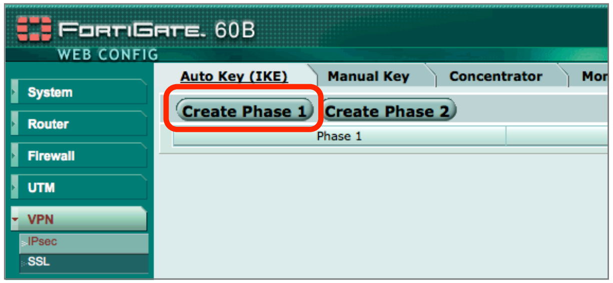
Steps 1 to 3 – Follow Steps 1 to 3 of Task 1

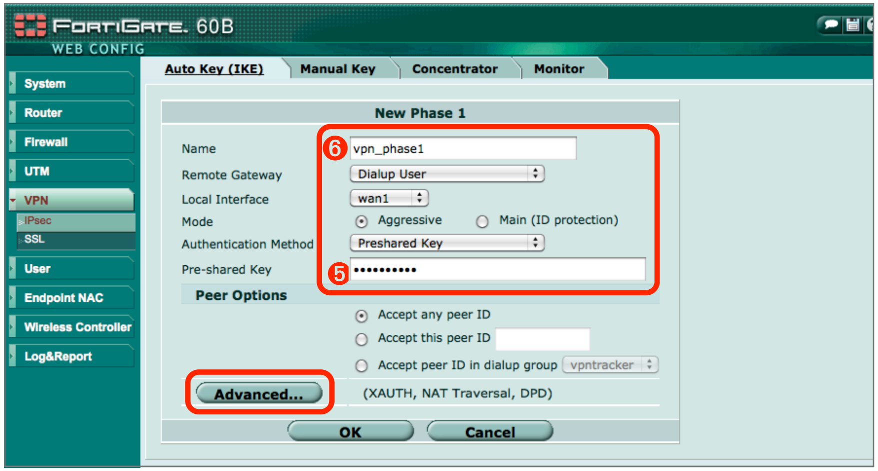
The first three steps of the setup are **the same as for the policy-based VPN in → *Task 1***.

- If you have already followed → *Steps 1 to 3 of Task 1*, simply remove the configuration created in → *Steps 4 to 6 of Task 1*
- If you have not yet set up anything, please follow → *Steps 1 to 3 of Task 1* now

Step 4 – Set up Phase 1

- Go to **VPN** > **IPsec** and click **Create Phase 1**





New Phase 1

Name ❻ vpn_phase1

Remote Gateway: Dialup User

Local Interface: wan1

Mode: ● Aggressive ○ Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key ❺ ••••••••••

Peer Options

● Accept any peer ID

○ Accept this peer ID

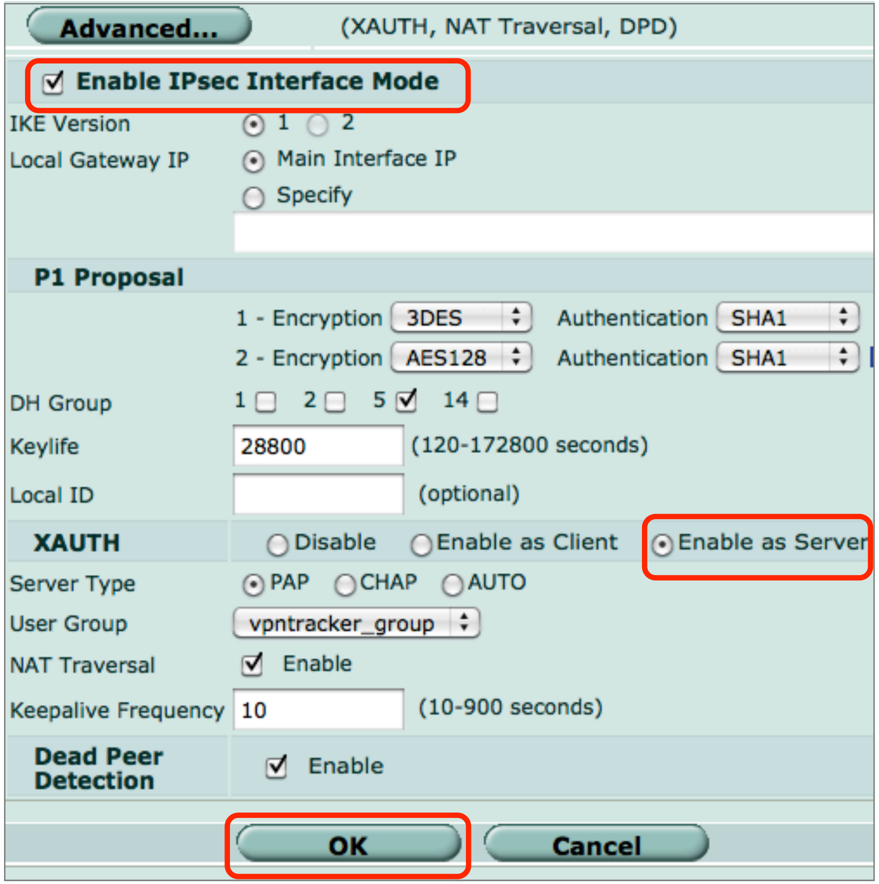
○ Accept peer ID in dialup group vpntracker

Advanced... (XAUTH, NAT Traversal, DPD)

- **Name**: Enter a name for the phase 1 setup (here:**vpn_phase1**). Write it down as ❻
- **Remote Gateway**: Choose **Dialup User** from the popup list
- **Local Interface**: Choose **wan1** from the popup list
- **Mode**: Choose **Aggressive** mode
- **Authentication Method**: Select **Pre-Shared Key**
- Enter a **Pre-Shared Key**. Make sure to choose a good pre-shared key and remember it, or write it down as ❺

Advanced Settings

- Click **Advanced…** to reveal additional settings



(XAUTH, NAT Traversal, DPD)

☑ Enable IPsec Interface Mode

IKE Version ● 1 ○ 2

Local Gateway IP ● Main Interface IP ○ Specify

P1 Proposal

1 - Encryption 3DES Authentication SHA1

2 - Encryption AES128 Authentication SHA1

DH Group 1 □ 2 □ 5 ☑ 14 □

Keylife 28800 (120-172800 seconds)

Local ID (optional)

XAUTH ○ Disable ○ Enable as Client ● Enable as Server

Server Type ● PAP ○ CHAP ○ AUTO

User Group vpntracker_group

NAT Traversal ☑ Enable

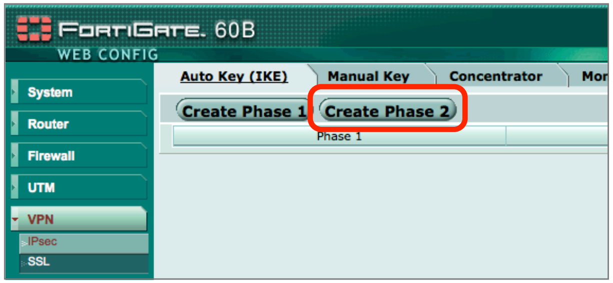
Keepalive Frequency 10 (10-900 seconds)

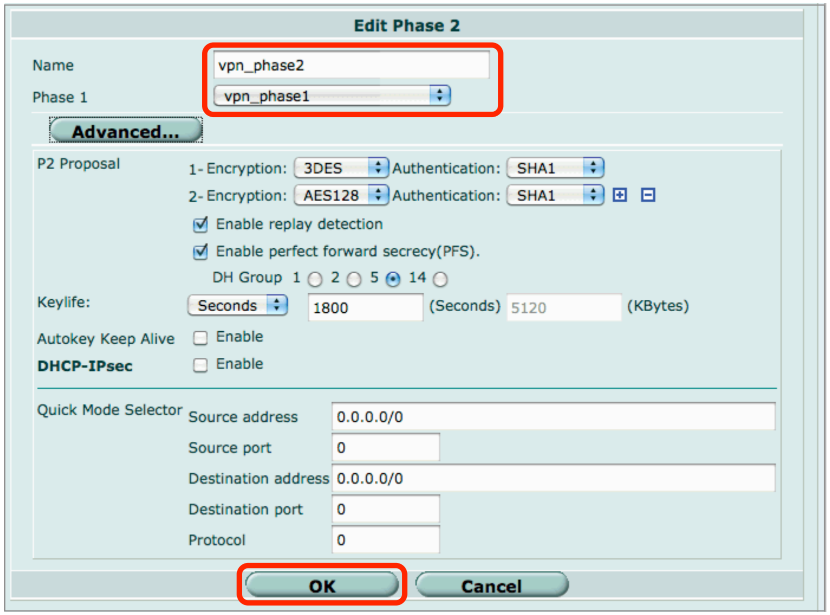
Dead Peer Detection ☑ Enable

- Check the box **Enable IPsec Interface Mode**
- **XAUTH**: Choose **Enable as Server**
- Click **OK** to save the phase 1 setup

Step 5 – Set up Phase 2

- Click **Create Phase 2**





Edit Phase 2

Name: vpn_phase2

Phase 1: vpn_phase1

P2 Proposal
1- Encryption: 3DES Authentication: SHA1
2- Encryption: AES128 Authentication: SHA1

☑ Enable replay detection

☑ Enable perfect forward secrecy(PFS).

DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: Seconds 1800 (Seconds) 5120 (KBytes)

Autokey Keep Alive □ Enable

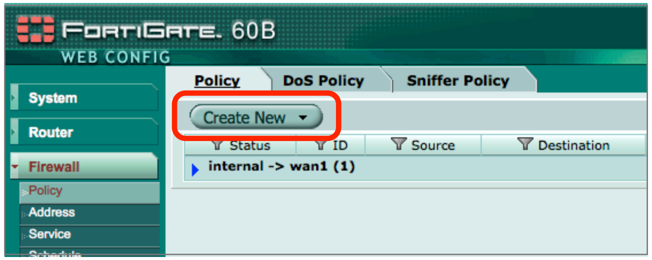
DHCP-IPsec □ Enable

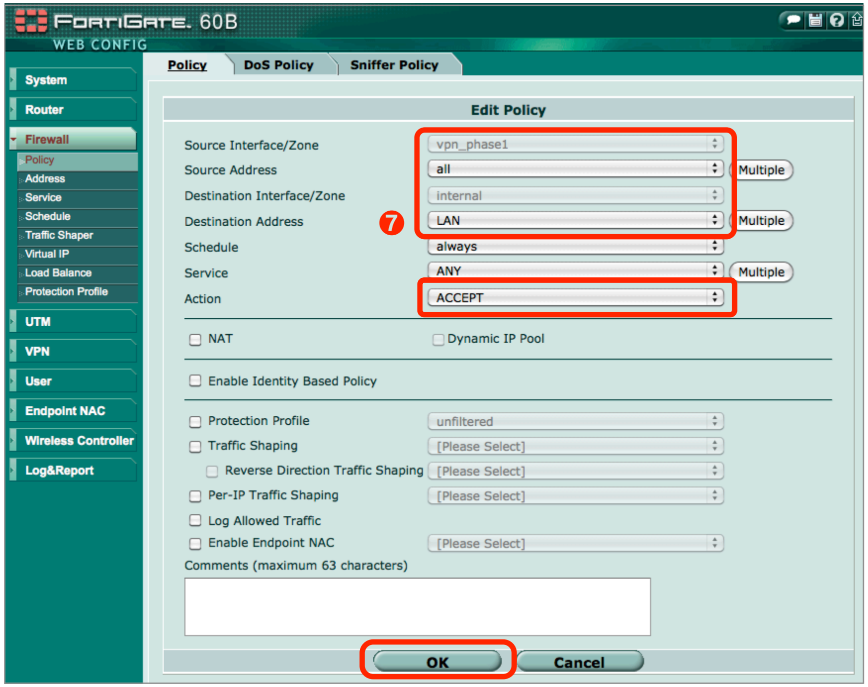
Quick Mode Selector
Source address 0.0.0.0/0
Source port 0
Destination address 0.0.0.0/0
Destination port 0
Protocol 0

- **Name**: Enter a name for the phase 2 setup (here:**vpn_phase2**)
- **Phase 1:** Select the phase 1 setup you created in → *Step 4* from the popup list (here:**vpn_phase1**)
- Click **OK**

Step 6 – Set up a Firewall Policy

- Go to **Firewall** > **Policy** and click **Create New**





Edit Policy

Source Interface/Zone: vpn_phase1

Source Address: all

Destination Interface/Zone: internal

Destination Address: LAN

Schedule: always

Service: ANY

Action: ACCEPT

□ NAT □ Dynamic IP Pool

□ Enable Identity Based Policy

□ Protection Profile unfiltered

□ Traffic Shaping [Please Select]

□ Reverse Direction Traffic Shaping [Please Select]

□ Per-IP Traffic Shaping [Please Select]

□ Log Allowed Traffic

□ Enable Endpoint NAC [Please Select]

Comments (maximum 63 characters)

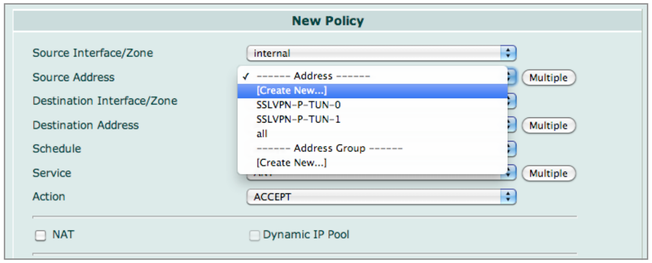
- **Source Interface/Zone**: Select the phase 1 setup you created in → *Step 4* from the popup list (here: **vpn_phase1**)
- **Source Address**: Select **all**

We will be setting up the VPN for **split tunneling**, i.e. only the traffic destined for the Fortinet VPN gateway internal network(s) will go through the VPN. A VPN Tracker user's remaining Internet traffic will continue to go out normally through their ISP.

- **Destination Interface/Zone**: Choose **internal** from the popup list
- **Destination Address:** Select the address object representing your VPN gateway's internal network (here: **LAN**) and write its name down as ❼. If you do not yet have such an address object, create a new one (see below).
- **Action**: Select **ALLOW** from the popup list
- Click **OK** to add the policy

Creating an address object representing the internal (LAN) network:

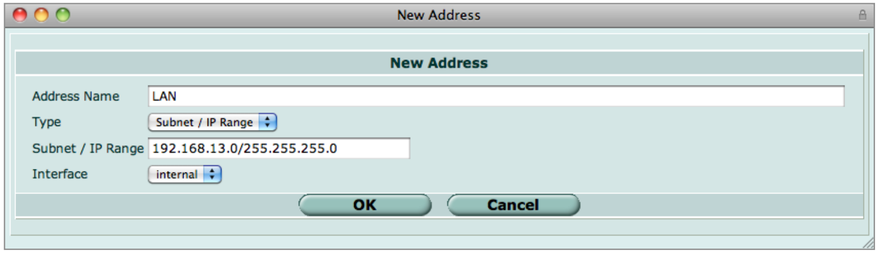
- Click **Create New…**



New Policy

Source Interface/Zone	internal
Source Address	✓ ------ Address ------ [Create New...] SSLVPN-P-TUN-0 SSLVPN-P-TUN-1 all ------ Address Group ------ [Create New...]
Destination Interface/Zone	
Destination Address	
Schedule	
Service	
Action	ACCEPT

□ NAT □ Dynamic IP Pool



New Address

New Address

Address Name	LAN
Type	Subnet / IP Range
Subnet / IP Range	192.168.13.0/255.255.255.0
Interface	internal

- **Address Name**: Enter a name for the new address object (e.g. **LAN**). Write down the name as ❼
- **Type**: Select **Subnet / IP Range**
- **Subnet / IP Range**: Enter your VPN gateway's internal (LAN) network address and subnet mask. Make sure to **use the network address, not the LAN IP address**: With a 255.255.255.0 subnet mask this means setting the last part of LAN IP address ❶ to 0 (e.g. 192.168.13.1 becomes 192.168.13.0)
- **Interface**: Select **internal**
- Click **OK** to add the new address object

Step 7 – Choose an IP Address Range

You will need to decide which IP addresses to assign to VPN clients through Mode Config. The choice is between assigning them IP addresses **from the Fortinet VPN gateway's inside (LAN) network**, or using a **different, unrelated network** for this purpose.

IP Addresses from the Inside (LAN) Network

You can use IP addresses from the inside network if you have enough free IP addresses on the inside network for the maximum number of VPN clients you expect.

Choose a range of IP addresses and write them down as ❽ and ❾.

Using IP addresses from the inside network is the best solution if your VPN gateway is not the default gateway (router) of its network since it can act as an ARP proxy for those IP addresses.

IP Addresses from a Different Network

If you don't use IP addresses from the Fortinet VPN gateway's inside network, simply choose an arbitrary private network that is not used anywhere on your the VPN gateway's network (or the computers that need to be reachable through VPN).

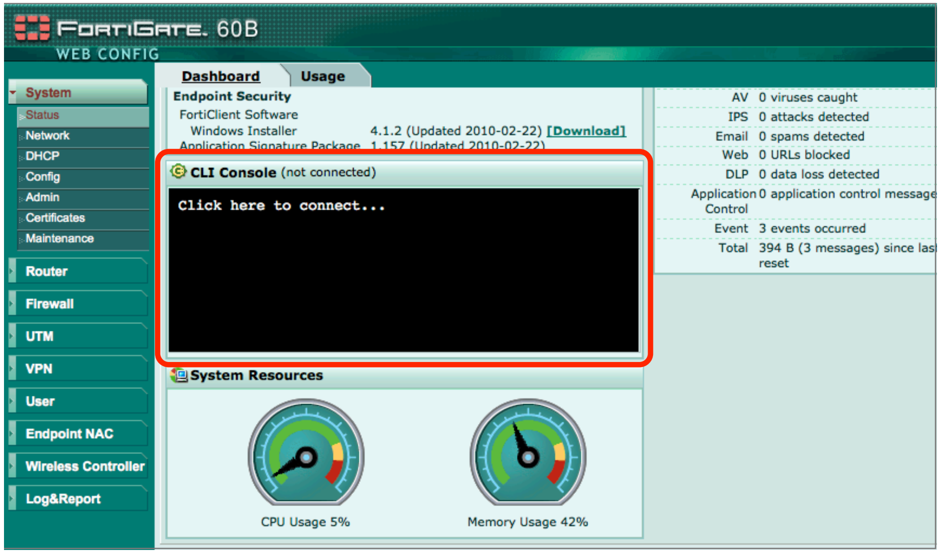
In our example, the Fortinet VPN gateway's inside network is 192.168.13.0/24. We choose to take the IP addresses from the **completely unrelated, unused private network** 10.13.121.0/24., starting with IP 10.13.121.100 and ending with IP 10.13.121.199. The range of IP addresses must be large enough (preferably larger) than the maximum number of expected VPN clients.

Choose a range of IP addresses and write them down as ❽ and ❾.

If your VPN gateway is **not** the default gateway (router) of its network, you will have to ensure that traffic for the chosen IP addresses is routed back to the VPN gateway instead of to the usual default gateway (e.g. by adding a route on the default gateway to the VPN gateway for these IPs).

Step 8 – Set up Mode Config

- Mode Config can currently only be set up on the command line
- Go to **System** > **Status** and find the **CLI Console** on the Dashboard
- Click inside the **CLI Console** to connect to the VPN gateway by command line interface (CLI)



Endpoint Security
FortiClient Software
Windows Installer 4.1.2 (Updated 2010-02-22) [Download]
Application Signature Package 1.157 (Updated 2010-02-22)

AV 0 viruses caught
IPS 0 attacks detected
Email 0 spams detected
Web 0 URLs blocked
DLP 0 data loss detected
Application Control 0 application control message
Event 3 events occurred
Total 394 B (3 messages) since last reset

CLI Console (not connected)

```
Click here to connect...
```

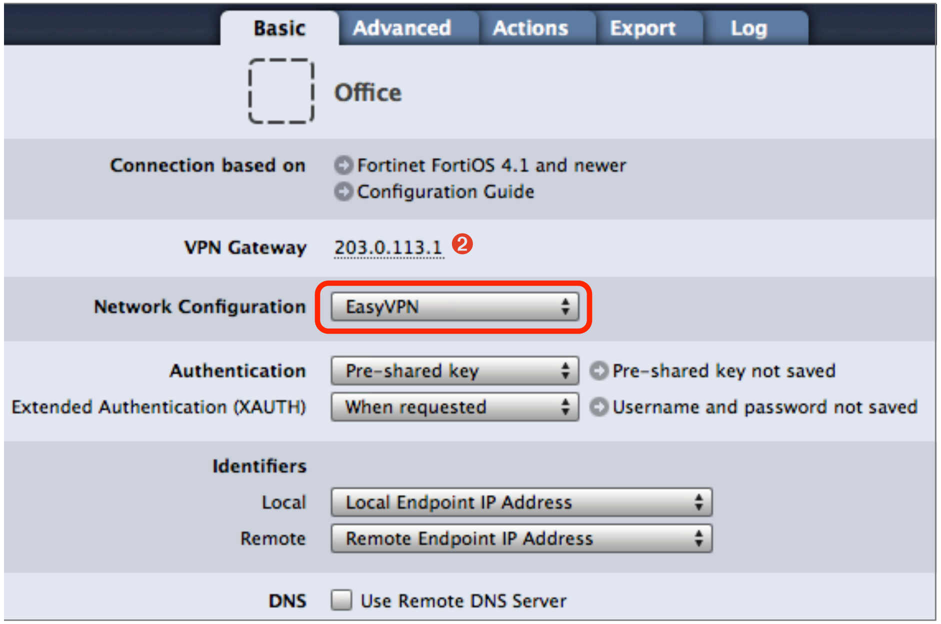
- Enter the following commands:

```
config vpn ipsec phase1-interface
      edit "vpn_phase1"                ❻
             set mode-cfg enable
             set ipv4-start-ip 10.0.13.100   ❽
             set ipv4-end-ip   10.0.13.199   ❾
             set ipv4-split-include "LAN"    ❼
end
```

Replace the numbered settings (name of the phase 1 setup, start/end IP address of the Mode Config address range, and the address object representing the inside (LAN) network) with the settings from your own checklist.

Step 9 – Configure the VPN Connection

Once you have added the new connection, there are a few settings that need to be customized to match what is configured on your VPN gateway.



Connection based on: ○ Fortinet FortiOS 4.1 and newer ○ Configuration Guide

VPN Gateway: 203.0.113.1 ❷

Network Configuration: EasyVPN

Authentication: Pre-shared key — Pre-shared key not saved

Extended Authentication (XAUTH): When requested — Username and password not saved

Identifiers
Local: Local Endpoint IP Address
Remote: Remote Endpoint IP Address

DNS: □ Use Remote DNS Server

- **VPN Gateway**: Enter the WAN IP address (or hostname) of your VPN gateway that you wrote down as ❷
- **Network Configuration**: Select **Cisco EasyVPN** from the popup list
- You can now proceed to test the connection as described in → *Step 3 – Test the VPN Connection*