equinux

VPN Tracker 365

VPN Configuration Guide

Sophos XG Firewall

Revised 28 June 2018

www.equinux.com

Introduction

My VPN Gateway Configuration Checklist

Throughout this guide there will be certain pieces of information which are needed later on for configuring VPN Tracker. This information is marked with red numbers so it is easier for you to reference. Print out this checklist and use it to keep track of your device settings.

IP Addresses

1. WAN IP Address: _____._____._____._____

   or Host Name _____

2. LAN Network: _____._____._____._____ /_____._____._____._____

Authentification

3. Pre-Shared Key: _____
4. XAUTH Username: _____
5. XAUTH Password: _____

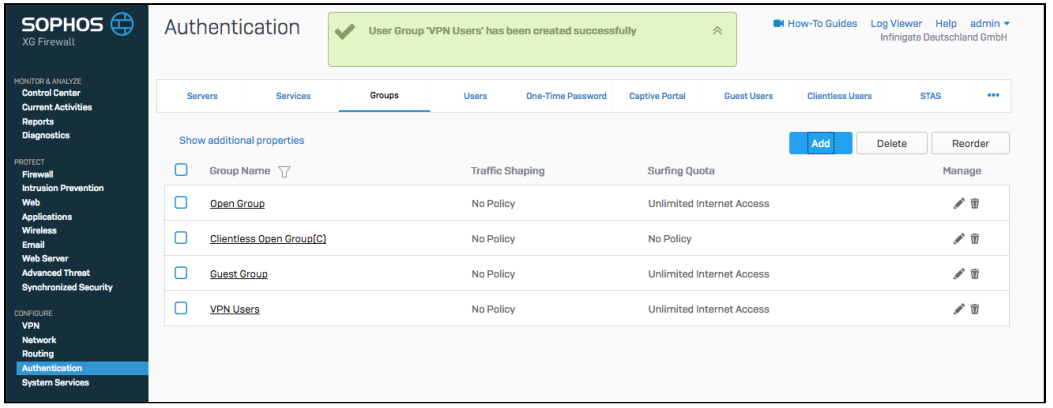
Identifiers

6. Local ID: _____
7. Remote ID: _____

Task One - Setting up your device

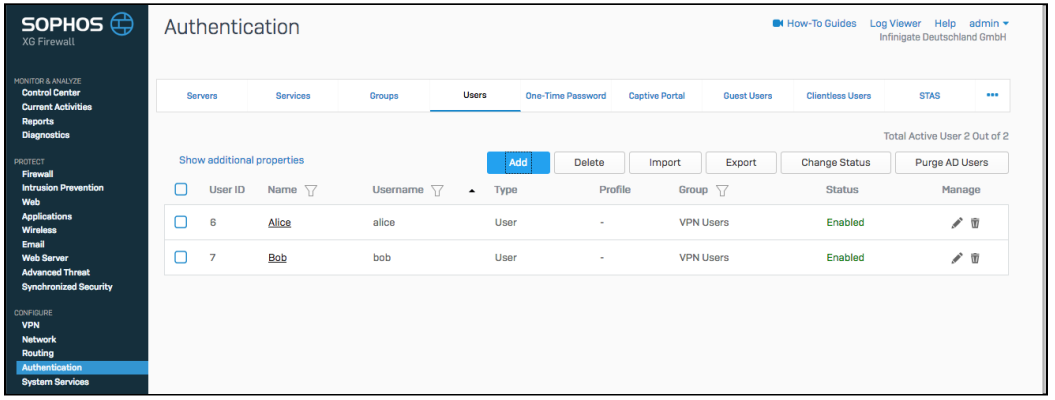
Step One: Create a user group*

- ➔ Launch your device's web interface
- ➔ Under "**Configure**", select "**Authentication**" and go to the "**Groups**" tab
- ➔ Click on "**Add**" to create a group
- ➔ Give your group a name e.g. "VPN Users"
- ➔ Under "**Access Time**", choose a time policy for your user group to determine when they have access to the VPN connection.
- ➔ For "**Traffic Shaping**", you can select "**No Policy**." For "**Surfing Quota**", choose "**Unlimited Internet Access**."



Step Two: Add users*

- ➔ Stay in "**Authentication**" and go to the "**Users**" tab.
- ➔ Click on "**Add**" to create a new user profile.
- ➔ Fill out your user profile with User ID, name, and username **(4)**, and create a password **(5)**.
- ➔ Under "**Type**", select "**User**"
- ➔ If desired, you can also choose a group for the user. The group settings will be automatically applied to the user.



Important: These are the users which are referred to later on in the guide during the authentication stage in VPN Tracker 365. Add them to your Configuration Checklist.

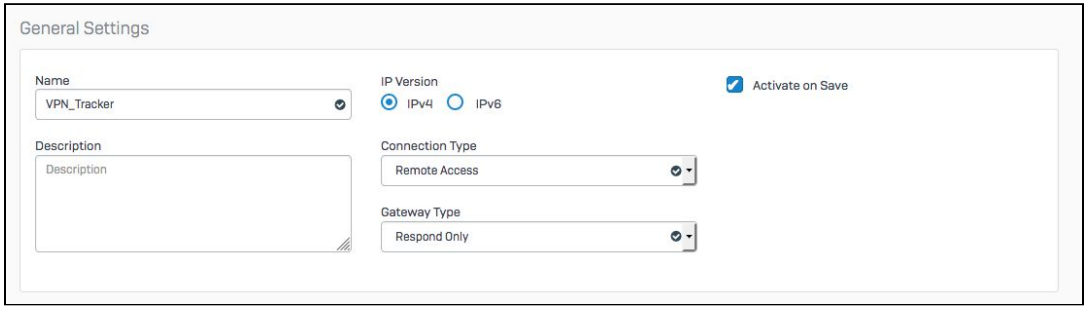
* Steps one and two are not required to configure the device but if you have multiple users, we recommend taking these steps to make the configuration process easier.

Step Three: Configuring the VPN

- ➔ Under "**Configure**" click on "**VPN**" and stay in the "**IPsec Connections**" tab.
- ➔ Under "**IPSec Connections**" click "**Add**" to configure a new connection.

General Settings:

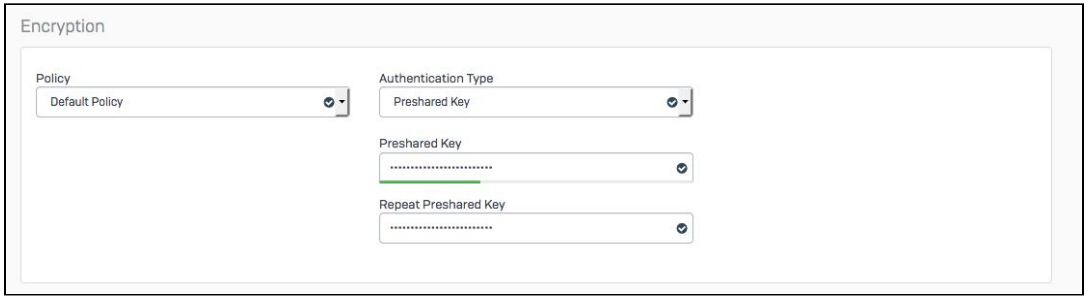
- ➔ Give your Connection a name e.g. "VPN_Tracker." This helps you to identify your connection if you are configuring multiple.
- ➔ Make sure "**IPv4**" is selected as the IP Version and check the box next to "**Activate on Save**."
- ➔ For "**Connection Type**", select "**Remote Access**."



Encryption:

- ➔ Under "**Policy**", select "**Default Policy**" from the drop down list.
- ➔ Select "**Preshared Key**" as your "**Authentication Type**"
- ➔ Now enter and repeat your Pre-Shared Key in the space provided.

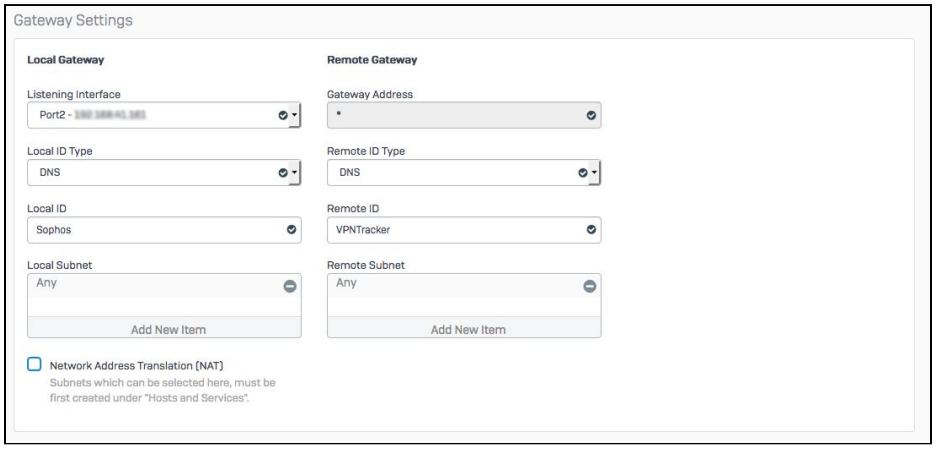
Important: You need to keep a note of your Pre-Shared key for later on. Enter this as **(3)** on your Configuration Checklist.



Gateway Settings

- ➔ For "**Local ID Type**", select "**DNS**" from the drop down list and enter your Local ID **(6)** e.g. "Sophos".
- ➔ For "**Remote ID Type**", select "**DNS**" again and enter your Remote ID **(7)** e.g. "VPNTracker".
- ➔ Select "**Any**" for both the "**Local Subnet**" and the "**Remote Subnet**"

Important: You will need these two IDs later on for the configuration in VPN Tracker. Add them to your Configuration Checklist.



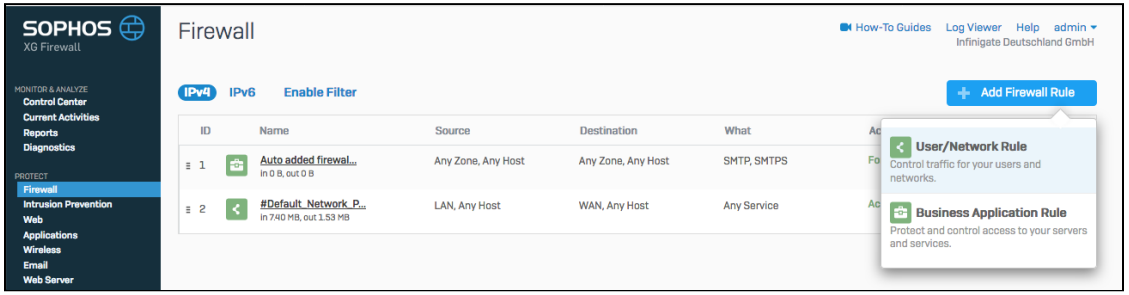
Advanced

- ➔ For "**User Authentication Mode**", select "**As Server**."
- ➔ Click on "**Add New Item**" to add the users you created in the previous stage. Click "**Save**" to save your settings for this VPN connection.

Step Four: Configuring the Firewall rules

The first rule mentioned in this step is important. You need to set this up to be able to access your server remotely via VPN.

- ➔ Go to the "**Protect**" in the menu on the left and click on "**Firewall.**"
- ➔ Click on "**Add Firewall Rule**" and choose "**User/Network**"
- ➔ First, name the rule. We suggest "**VPN to LAN.**" This rule allows you to access the LAN via your VPN connection.
- ➔ For "**Action**", select "**Accept**."
- ➔ For the Source Zones, select "**VPN.**"
- ➔ For the Destination Zones, select "**LAN.**"
- ➔ Under "**Identity**", uncheck the box labelled "**Match known users**."

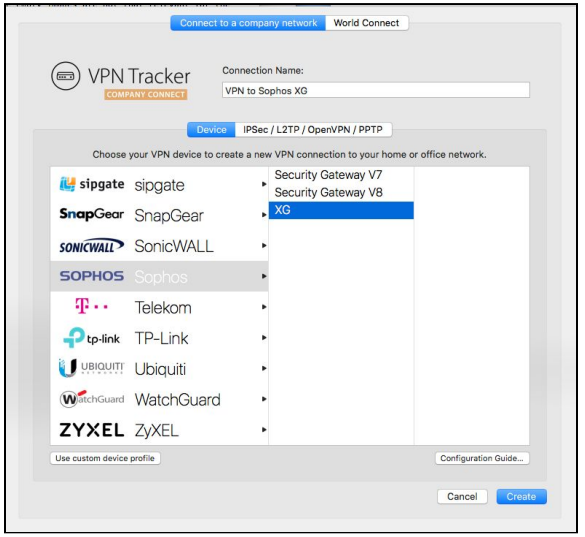


- ➔ Under "**Advanced**", go to "**NAT & Routing**" and uncheck the box "**Rewrite source address (Masquerading).**"
- ➔ Click "**Save**" when done."

The second rule is optional and allows LAN users to communicate with VPN users. You don't need this rule if you are only using your VPN connection to access your company's server via your VPN.

- ➔ Name this rule "**LAN to VPN.**" Select "**Accept**" for Action.
- ➔ For the Source Zones, select "**LAN.**""
- ➔ For the Destination Zones, select "**VPN.**"
- ➔ Under "**Identity**", uncheck the box labelled "**Match known users**."
- ➔ Under "**Advanced**", go to "**NAT & Routing**" and uncheck the box "**Rewrite source address (Masquerading).**"
- ➔ Click "**Save**" when done."

Task Two - Configuration in VPN Tracker



Step One: Add a connection

- ➔ Open VPN Tracker 365.
- ➔ Click on "**Create a connection**", or click on the + in the bottom left corner of the app window.
- ➔ Select **Sophos** from the list.
- ➔ Select **XG**

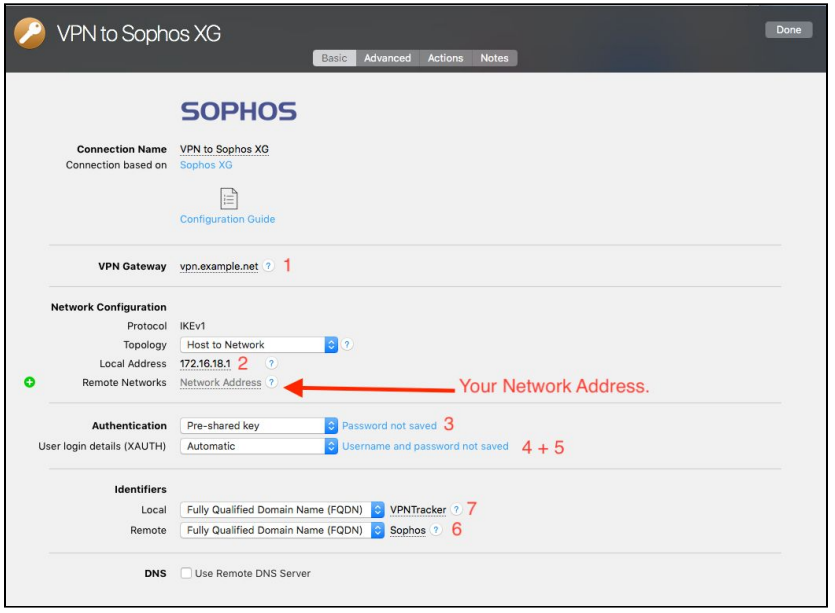
Step Two: Configure the VPN connection

- ➔ Go to the "**Basic"** tab.
- ➔ Next to "**VPN Gateway**", enter your device's IP address **(1)**

Network Configuration

- ➔ For "**Topology**", "**Host to Network**" should be automatically selected.
- ➔ Local address: Enter your unique **LAN address (2)** here. Remote Networks: Enter the network address you want to connect to.

Important: In the case of multiple users, your administrator should provide each user with a unique LAN address to ensure the connection works for all users.



Authentication

- ➔ Enter your **Pre-shared key (3)** from your checklist
- ➔ Enter your **XAUTH Login (4)** and **Password (5)**

Identifiers

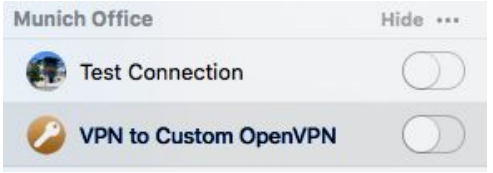
- ➔ Next to "**Local**", enter your **Remote ID (7)**
- ➔ Next to "**Remote**", enter your **Local ID (6)**

Important: Please note that the Local and Remote Identifier in VPN Tracker must be swapped, as what is considered local for VPN Tracker is remote for the Firewall.

Task Three - Testing the VPN connection

In order 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, try it out at home, or from an Internet cafe, or go visit a friend.

Connect to your VPN



- ➔ Check first of all that your internet connection is working as it should be. Use this link as a test: http://www.equinux.com
- ➔ Start the VPN Tracker 365 app.
- ➔ Click on the On/Off slider to turn on your connection.

IMPORTANT:

If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

- ➔ Depending on your setup, You will be prompted to enter your pre-shared key. To save time for the future, 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.

Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that’s great – you’re connected! Now is a great time to take a look at the VPN Tracker Manual. It shows you how to use your VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up. Click the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log.

TIP: Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

VPN Tracker Manual

The VPN Tracker Manual contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) can be found at: http://www.vpntracker.com/support

Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact us via http://www.vpntracker.com/support

Please include the following information with any request for support:

- ➔ A description of the problem and any troubleshooting steps that you have already taken.
- ➔ A VPN Tracker Technical Support Report (Log > Technical Support Report).
- ➔ TP-Link model and the firmware version running on it.
- ➔ Screenshots of the VPN settings on your VPN gateway.

IMPORTANT: A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is not included in a Technical Support Report.

Remote DNS Setup (Advanced)

This point is **optional**. VPN Tracker can use DNS servers on the remote network of the VPN to look up host names of resources on the remote network of the VPN.

Requirements

If you or your organization operate a DNS server on your Sophos device's network, VPN Tracker can use it to look up the host names of internal resources (e.g. for turning intranet.ny.example.com into the IP address 192.168.13.94).
Remote DNS is entirely optional for Host to Network connections. You can always use IP addresses instead of host names, that's just less convenient.

DNS Server

To set up remote DNS, you need to know the IP address(es) of the DNS server(s) that you want to use. You can get this from your administrator.

My DNS Server: _____._____._____._____

Domain

VPN Tracker can use the remote DNS server for all DNS lookups (All Domains) or just for some domains (Search Domains). If you want VPN Tracker to use the remote DNS servers only for some domains (e.g. everything ending in "ny.example.com"), write down these domains here:

Search Domains: _____

Setup in VPN Tracker

Remote DNS can be set up in VPN Tracker without making any changes to your device.

- ➔ Click on your VPN connection
- ➔ Click "**Configure**" and go to the "**Basic**" tab
- ➔ Check the box "**Use Remote DNS Server**"
- ➔ Now fill in your information from above for "**DNS Servers**" and "**Search Domains**" to configure for your network.