Lobotomo
Software

IPSecuritas 3.x

Configuration Instructions

for

AVM FRITZ!Box

Legal Disclaimer

Acknowledgments

Table of contents

Introduction

This document describes the steps necessary to establish a protected VPN connection between a Mac client and a AVM FRITZ!Box router/firewall. All information in this document is based on the following assumed network.
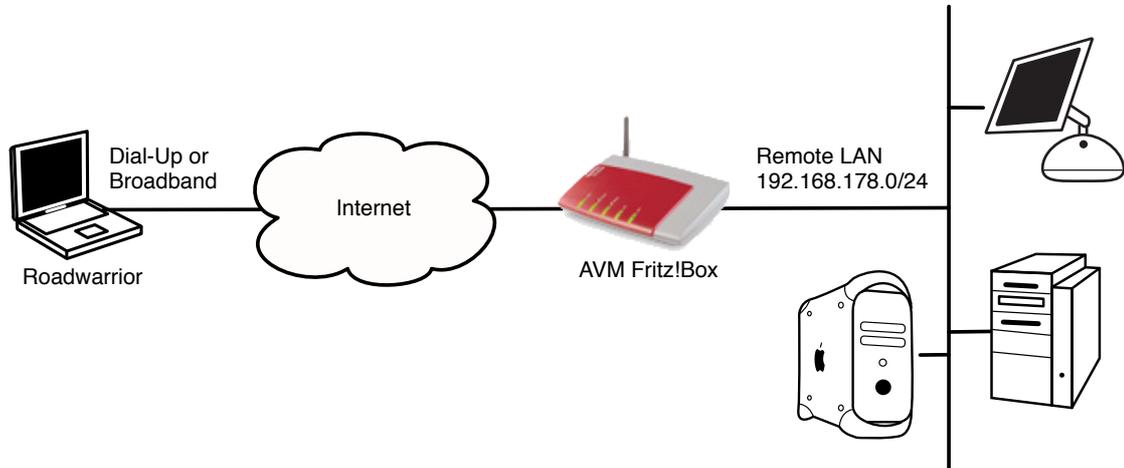
AVM FRITZ!Box Setup

This section describes the necessary steps to setup the FRITZ!Box to accept incoming connections.

Create Configuration File

Create a text-only file with the following content (the file can also be downloaded from http://www.avm.de/de/Service/Service-Portale/Service-Portal/images/Redaktionelle_Grafiken/vpn/fritzbox_macosx.cfg).

```
vpncfg {
        connections {
                enabled = yes;
                conn_type = conntype_user;
                name = "macosx@office.com";
                always_renew = no;
                reject_not_encrypted = no;
                dont_filter_netbios = yes;
                localip = 0.0.0.0;
                local_virtualip = 0.0.0.0;
                remoteip = 0.0.0.0;
                remote_virtualip = 192.168.178.201;
                remoteid {
                        user_fqdn = "macosx@office.com";
                }
                mode = phase1_mode_aggressive;
                phase1ss = "all/all/all";
                keytype = connkeytype_pre_shared;
                key = "supergeheimkey";
                cert_do_server_auth = no;
                use_nat_t = no;
                use_xauth = no;
                use_cfgmode = no;
                phase2ss = "esp-all-all/ah-none/comp-all/pfs";
                accesslist =
                        "permit ip 192.168.178.0 255.255.255.0
                         192.168.178.201 255.255.255.255";
        }
        ike_forward_rules = "udp 0.0.0.0:500 0.0.0.0:500",
                            "udp 0.0.0.0:4500 0.0.0.0:4500";
}
```

Please replace the value in **red** with suitable values for your network setup (please remember all values as you'll need them again when setting up IPSecuritas):

remote_virtualip: A virtual address to use when connecting. Best choose a free address from within the FRITZ!Box LAN address range.

key: A secure secret password. Please choose a password with at least 10 characters, numbers and special characters.

accesslist: The first two values should reflect the local LAN address and netmask of your local network behind the FRITZ!Box. The third value is the same virtual IP address you used for *remote_virtualip*.

Save your changes to the configuration file and upload it with the FRITZ!Box VPN Wizard.

IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the FRITZ!Box router.

Start Wizard

Unless it is already running, you should start IPSecuritas now. Change to **Connections** menu and select **Edit Connections** (or press ⌘-E). Start the Wizard by clicking on the following symbol:

Enter Name of New Connection

Connection Wizard

Welcome to the connection setup wizard, which will help you to configure the most common setups.

Please enter the name of this connection into the field below:

Name: Office

Cancel ▶

Enter a name for the connection (any arbitrary name).

Click on the right arrow to continue with the next step.

Select Router Model

Hersteller und Modell des Firewalls

Bitte wählen Sie den Hersteller und das Modell Ihres Firewalls:

Hersteller: AVM

Modell: FRITZ!Box

Abbrechen ◀ ▶

Select **AVM** from the manufacturer list and **FRITZ!Box** from the model list.

Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

Firewall Public IP Address or Hostname

Please enter the public IP address or the hostname of the into the text field:

Address: firewall.mycompany.com

Examples: firewall.mycompany.com
or
123.321.1.1

Cancel ◀ ▶

Enter the public IP address or hostname of your AVM FRITZ!Box router. In case your ISP assigned you a dynamic IP address, you should register with a dynamic IP DNS service (like http://www.dyndns.org).

Click on the right arrow to continue with the next step.

Enter a Virtual IP Address

Enter a virtual local IP address. This address appears as the source address of any packet going through the tunnel. If no address is specified, the real local IP address is used instead.

This address has to be identical to the address you used for **remote_virtualip** in the setup of the FRITZ!Box above.

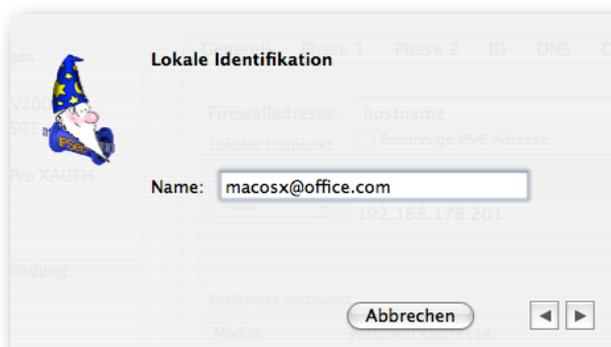Click on the right arrow to continue with the next step.

Enter Remote Network

Enter the remote network address and netmask (please note that the netmask needs to be entered in **CIDR** format). This has to match with the settings of the FRITZ!Box local LAN address.

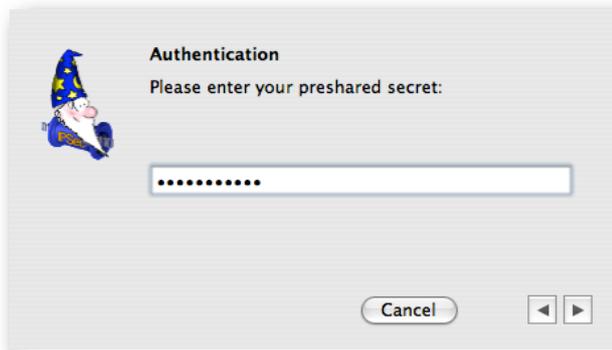Click on the right arrow to continue with the next step.

Enter Remote Identification

Enter the FRITZ!Box's remote identification (which is `macosx@office.com` if you used the configuration file depicted in the section describing the FRITZ!Box configuration above).

Click on the right arrow to continue with the next step.

Enter Preshared Key

Enter the same **Preshared Key** that you used for the FRITZ!Box.

Click on the right arrow to finish the connection setup.

You're now done with the configuration of IPSecuritas. You can establish the tunnel by clicking on **Start IPSec** in the main window or choose the start function in the IPSecuritas menu bar item or the Dashboard widget.

Diagnosis

Reachability Test

To test reachability of the remote host, open an **Terminal Window** (Utilities -> Terminal) and enter the command **ping**, followed by the FRITZ!Box **local IP address**. If the tunnel works correctly, a similar output is displayed:

```
[MacBook:~] root# ping 192.168.178.1
PING 192.168.178.1 (192.168.178.1): 56 data bytes
64 bytes from 192.168.178.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 192.168.178.1: icmp_seq=1 ttl=64 time=19.290 ms
64 bytes from 192.168.178.1: icmp_seq=2 ttl=64 time=12.823 ms
```