

# AIMdefense

## Firewall Setup

1. Connect/cable AIMdefense FIREWALL to Fritz!Box.....	Page 2
2. AIMdefense FIREWALL Commissioning.....	Page 3
3. AIMdefense FIREWALL Installation Wizard.....	Page 4
4. Troubleshooting WAN PPPoE.....	Page 4
5. AIMdefense FIREWALL License Key Import.....	Page 5
6. AIMdefense FIREWALL Menuchanger.....	Page 7
7. Adjust DynDNS.....	Page 8

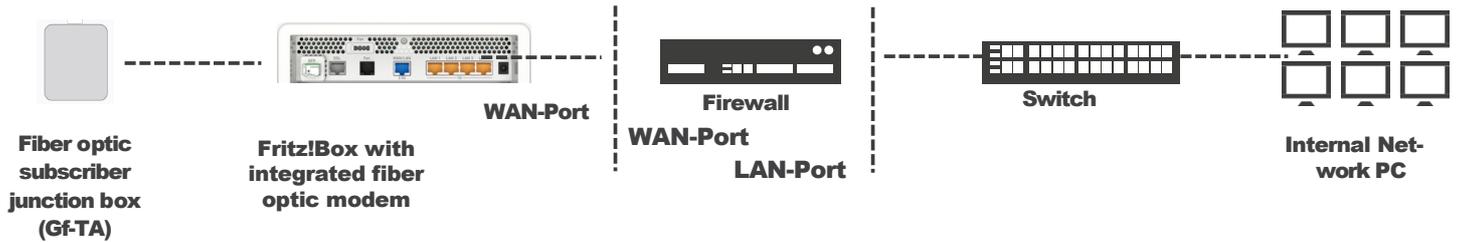
## 1. Connect/cable AIMdefense FIREWALL to Fritz!Box



Before you begin, make sure you have all the information from your Internet service provider and are connected to the Internet.

Before you start administering the firewall, you must connect the firewall to the internal and external networks.

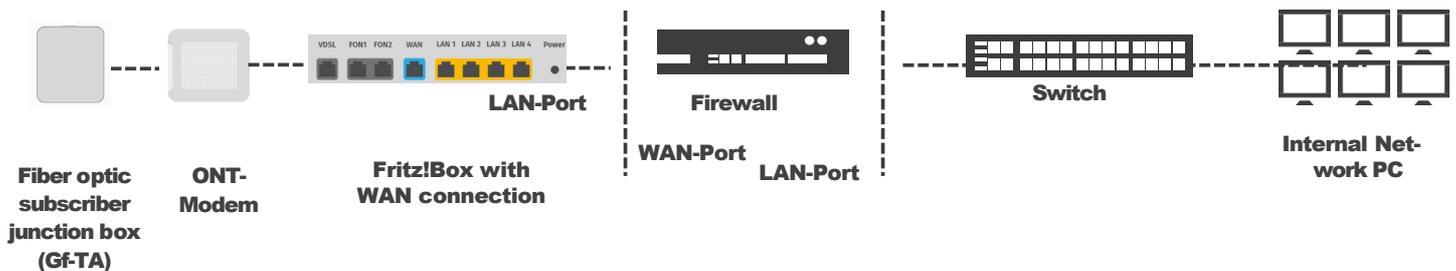
### Step 1 : Connecting the AIMdefense Firewall to a Fritz!Box with integrated fiber optic modem



Connect the junction box and the Fritz!Box with a fiber optic cable. Now establish a connection via the WAN port of the AVM-Fritz!Box to the WAN port of the firewall.

Establish the connection between the firewall (LAN port) and the switch using an RJ45 network cable. Note that your PC must be connected to this network.

### Step 2 : Connecting the AIMdefense Firewall and a Fritz!Box with WAN connection and external ONT modem



Connect the junction box and the ONT modem with a fiber optic cable. Then connect the ONT modem to the LAN port of the Fritz!Box using an RJ-45 network cable. Now establish a connection via the LAN port of the AVM-Fritz!Box to the WAN port of the firewall.

Establish the connection between the firewall (LAN port) and the switch using an RJ45 network cable. Note that your PC must be connected to this network.

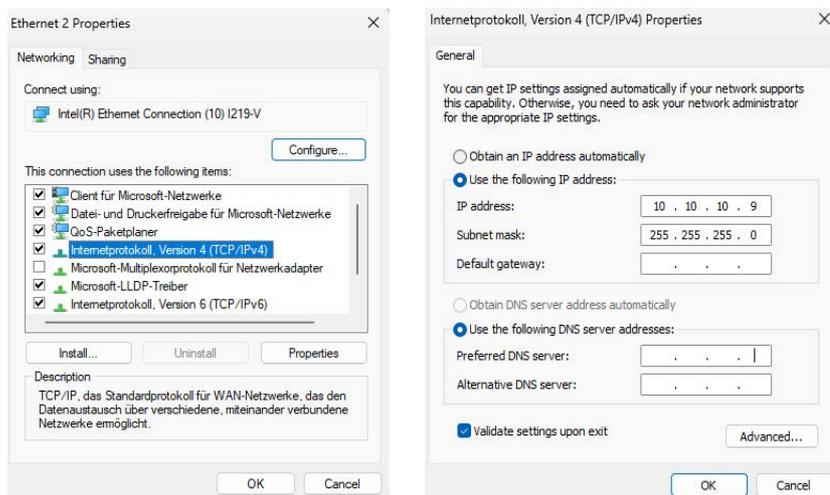
## 2. AIMdefense FIREWALL Commissioning

Port	IP Address	Function
LAN	10.10.10.10/255.255.255.0	LAN – Internes Netz
WAN	DHCP	WAN – Externes Netz
IP Address Admin Interface	User Name	Password
10.10.10.10	root	sysadm

### Commissioning

Once you have connected the AIMdefense FIREWALL, turn the appliance on using the power switch. The power switch is located next to the power connector. As soon as the appliance has completely booted up (approx. 2 minutes), you can connect to the PC. The client PC must first be set up.

### Set up Client PC



(Example: Client PC setup for Windows.

To do this, go to “Ethernet Properties” and then click “Internet Protocol, Version 4(TCP/IPv4)” and “Use the following IP address”.)

Set your network card to the following IP address range 10.10.10.x.

Subnet mask: 255.255.255.0.

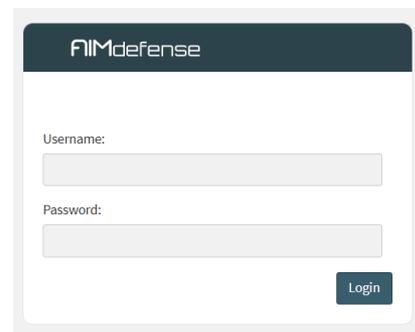
Please save the settings.

Now that you have established an existing connection between the PC and the FIREWALL, open the browser and enter

https://10.10.10.10.

Log in with the following default details:

Username: **root**, Password: **sysadm**



### 3. AIMdefense FIREWALL Installation Wizard

After successfully logging in, go to the System → Wizard menu item. Use the wizard to make the following settings:

- General settings (name, language and DNS)
- Date/time zone
- External network settings (WAN). The connection to the WAN depends on the type of Internet access.

 If a private IP is used as the WAN IP, disable the RFC1918 option.

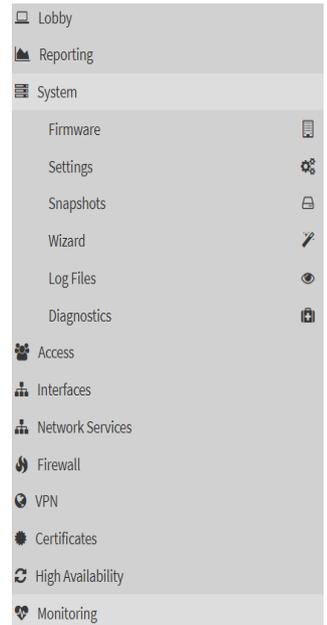
RFC1918 Networks

Block RFC1918 Private Networks:  Block private networks from entering via WAN

- Internal network (LAN)
- Set password for root

After you have successfully completed the wizard, you can connect to the Internet via the internal LAN interface.

Further information about administration can be found on our website <https://aimdefense.tech> or via the search field at the top right of the admin interface.

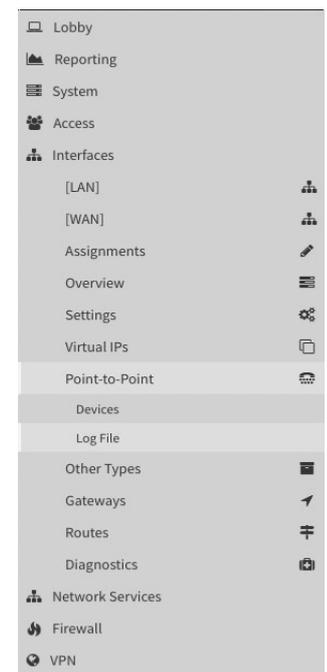


### 4. Troubleshooting WAN PPPoE

If you cannot get a connection with a connection via PPPoE, please go to the menu item Interfaces → Point-to-Point → Log File.

There you will find the log file with the information about your PPPoE connection.

 It may happen that DSL providers use a different MTU or VLAN tag. Please check this with your provider.  
Please check whether your modem has the latest firmware update.



# AIMdefense FIREWALL License Key Import

After you have successfully executed the wizard and the AIMdefense FIREWALL is connected to the Internet, you can import the AIMdefense license key. Go to the menu item “Lobby → AIMdefense License” and enter it there.

**You will receive the license key from your partner.**

Registering the license key unlocks various modules. You will also receive information about the expiration of the license, DynDNS name, maximum RAM and CPU.

Then click on the “Register” button.

If you register successfully, you will see the following display:

**Lobby: AIMdefense License**

Click here to view the full AIMdefense license text. You do accept the license agreement by filling out the following form.

<b>License Key</b>	04570172-059701f2-2d6c0421
<b>AIMdefense</b>	Advanced
<b>Reseller</b>	Secure 2 Fiber GmbH
<b>Customer</b>	Secure 2 Fiber GmbH
<b>License valid until</b>	04.12.2026 (+689 days left)
<b>Graceperiod</b>	01.01.2027
<b>Max. CPU</b>	16
<b>Max. RAM</b>	128 GB
<b>DynDNS</b>	154245-1.aim.aimdefense.tech, 154245-2.aim.aimdefense.tech, 154245-3.aim.aimdefense.tech, 154245-4.aim.aimdefense.tech
<b>Modules</b>	hostroute, mailproxy, tools, unifi

Register Check

The license has now been successfully registered.

Under “Modules” you can see the modules licensed for you. Click on the “Reinit all modules” button to subsequently install missing modules.

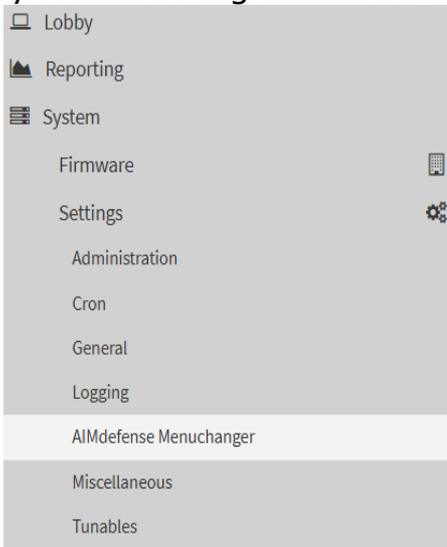
This process may take a few minutes.



If you do not see the modules in the menu overview, please switch to „System →Settings →AIMdefense Menuchanger“ in the menu and click the “Refresh Menu Cache” button.

## 6. AIMdefense FIREWALL Menuchanger

You can customize the menu structure on the left under “System →Settings →AIMdefense Menuchanger.



There are 3 options available to you. After you have changed the “Menu Type”, click the “Refresh Menu Cache” button.

**System: Settings: AIMdefense Menuchanger**

Select the Menu style you prefer. You can choose between the following options:

AIMdefense Menu with hidden Services	The full AIMdefense menu style with removed Services menu. This would be the preferred option if you are new to AIMdefense or to the underlying OPNsense system.
AIMdefense Menu	The full AIMdefense menu style. However, the legacy menu is also available for those switching.
Without AIMdefense Menu	This is the legacy menu style provided by the first AIMdefense systems.

full help ⓘ

Currently used: AIMdefense Menu with hidden Services

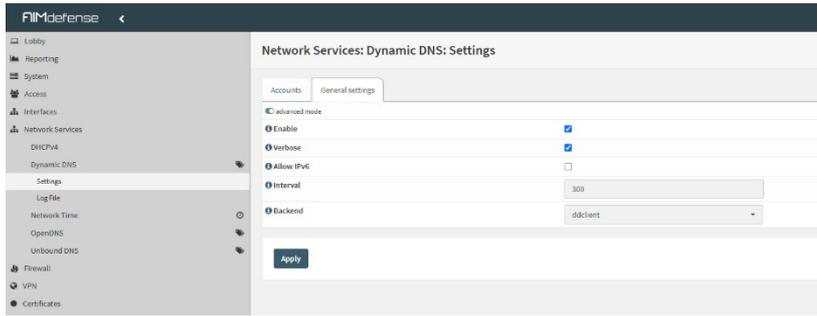
Change to:

Save

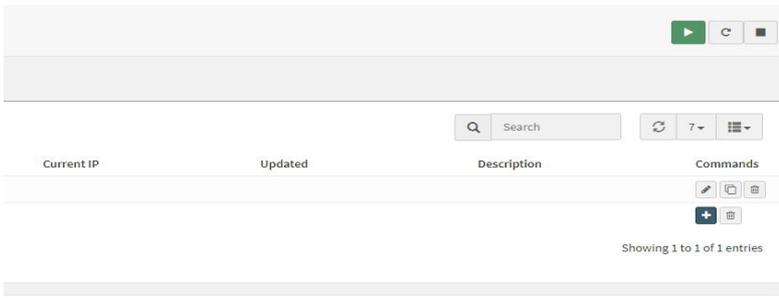
Please press the following button if you think the menu layout is corrupted

Refresh Menu Cache

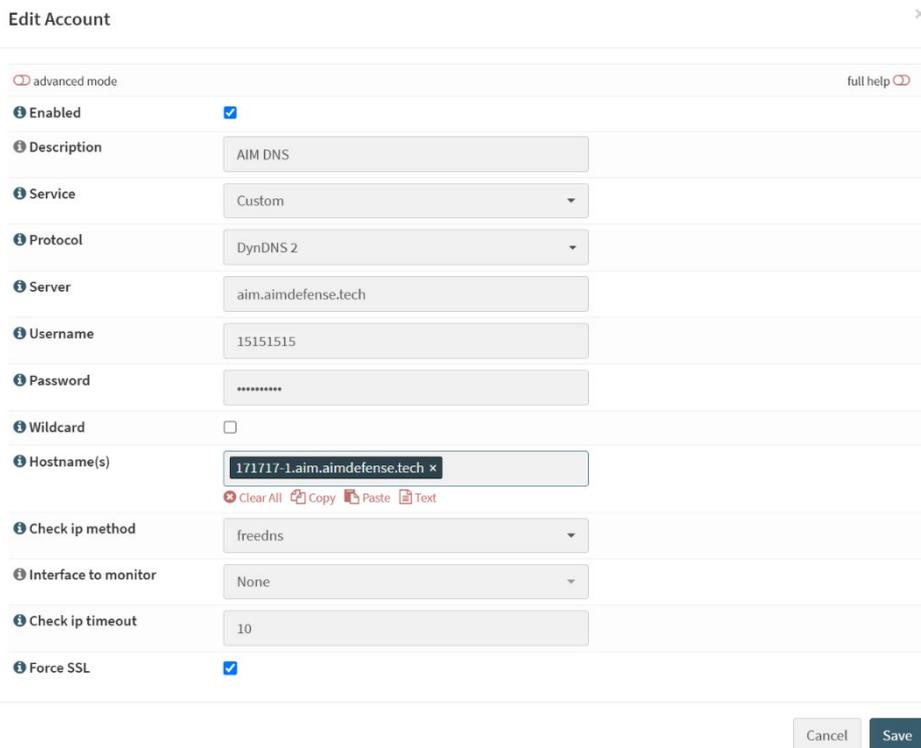
# 7. Adjust DynDNS



Click the "Network Services" button on the left side of the application -> > "Dynamic DNS"-> „Settings“-> General Settings“. Under the “Backend” menu item, set the tab to “ddclient” and save the change with “Apply”.



Now click on “Accounts” under “Settings”. Then click on the “ + ” symbol to create an account.



The following settings must be made under “Edit Account”:

Select and click “Enabled”.

Select “Service” and set the tab to “Custom”.

Select “Protocol” and set the tab to “DynDNS 2”.

Select “Server” and enter “aim.aimdefense.tech”.

Enter the corresponding access data “Username” and “Password”.

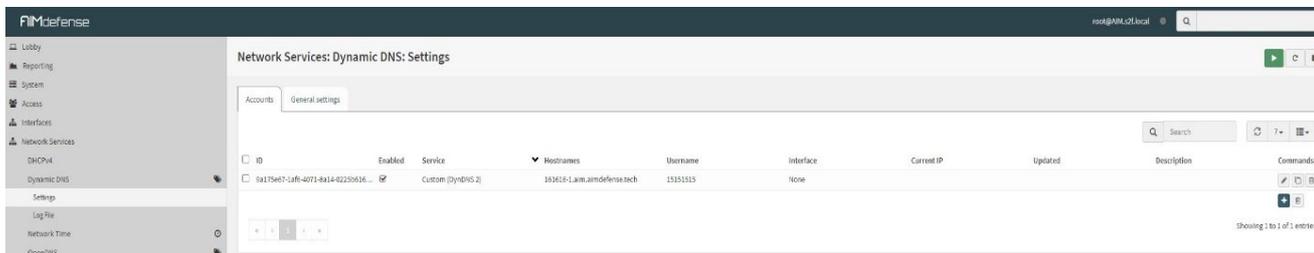
Select “Wildcard” and uncheck it.

Enter “Hostname”: DynDNS (depending on the license), example:

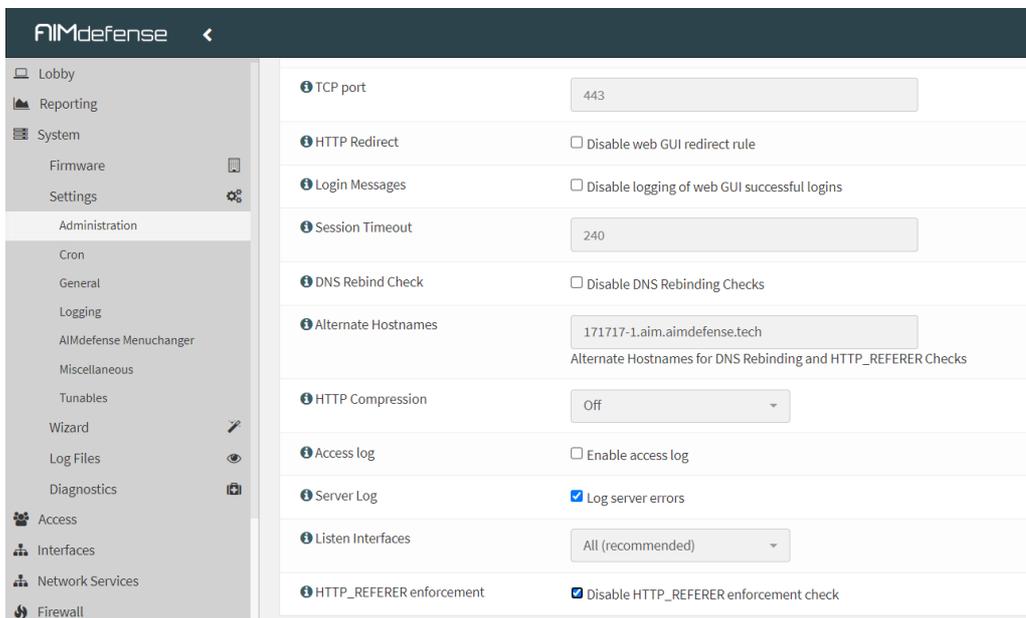
“171717-1.aim.aimdefense.tech”.

Select “Check ip method” and switch to “freedns”.

Select “Check ip timeout” and enter or check the value 10. Select “Force SSL”, click and save all changes with “Save”.



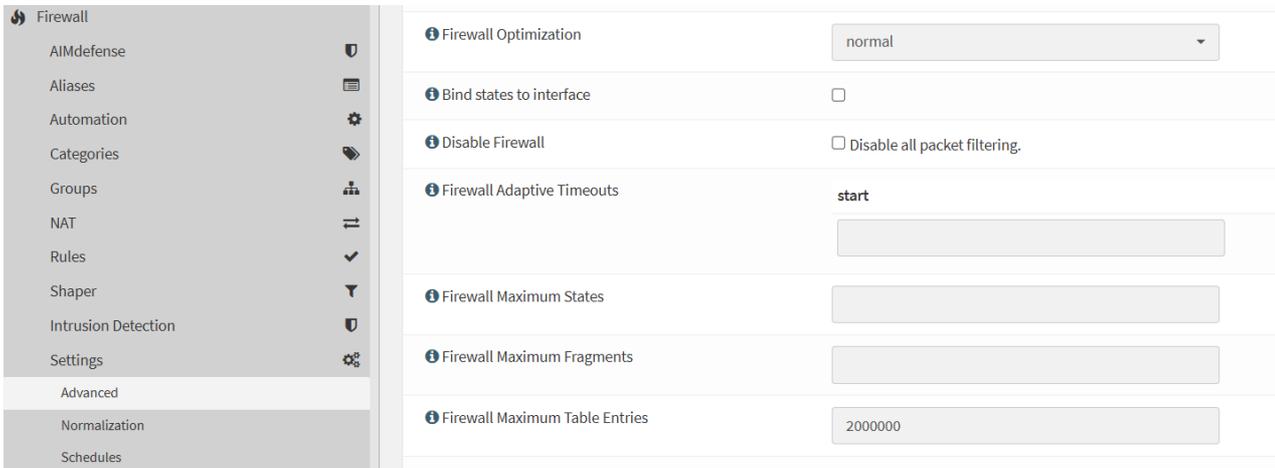
The account has now been created.



Now click on the System->Settings->“Administration” button on the left side of the application. Under “Alternate Hostnames”: enter “xxx.dyn/aim.aimdefense.tech”.

For “HTTP\_REFERER enforcement” check “Disable HTTP\_REFERER enforcement check” and save.

In order to activate all aliases, the default entry must first be increased to "2000000" under Firewall → Settings → Advanced → "Firewall Maximum Table Entries".



Under the menu item "Firewall" → AIMdefense → Settings: Activate all aliases. Confirm with "Apply".

