# FIMdefense 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	10.10.10/255.255.255.0	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

nernet 2 Properties	×	Internetprotokoll, Version 4 (TCP	/IPv4) Properties
etworking Sharing		General	
Connect using:		You can get IP settings assigned this capability. Otherwise, you need	automatically if your network supports eed to ask your network administrator
Intel(R) Ethemet Connection (10) I219-V	_	for the appropriate IP settings.	
	Jre	Obtain an IP address autom	atically
I his connection uses the following items:	_	O Use the following IP address	s:
<ul> <li>Client für Microsoft-Netzwerke</li> <li>Datei- und Druckerfreigabe für Microsoft-Netzwerke</li> </ul>	e	IP address:	10 . 10 . 10 . 9
QoS-Paketplaner		Subnet mask:	255 . 255 . 255 . 0
Internetprotokoll, Version 4 (TCP/IPV4)     Microsoft-Multiplexorprotokoll für Netzwerkadapter		Default gateway:	
<ul> <li>Microsoft-LLDP-Treiber</li> <li>Internetprotokoll, Version 6 (TCP/IPv6)</li> </ul>		Obtain DNS server address	automatically
		Use the following DNS serve	er addresses:
Install Uninstall Properti	ies	Preferred DNS server:	· · · ·
Description TCP/IP, das Standardprotokoll für WAN-Netzwerke, das	den	Alternative DNS server:	
Datenaustausch über verschiedene, miteinander verbund Netzwerke emröglicht.	dene	Validate settings upon exit	Advanced
		Validate settings upon exit	Advanced

(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: <b>root,</b> Password: <b>sysadm</b>

<b>FIIM</b> defense	
Username:	
Password:	
	Login

**¢**°

ß

Lobby

📐 Reporting

Settings

Snapshots

Wizard Log Files Diagnostics

Access

😧 VPN

Interfaces
 Network Services
 Firewall

System Firmware

### **3.AIMdefense FIREWALL Installation Wizard**

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

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



- · Internal network (LAN)
- $\cdot$  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 <u>https://aimdefense.tech</u> 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  $\rightarrow$ Point-to-Point  $\rightarrow$ Log File.

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



Secure 2 Fiber

Distribution GmbH -

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  $\rightarrow$  AIMdefense License" and enter it there.

	Lobby		Lobby: AIMdefense License
	Dashboard	6	
	TUXGUARD License	<u> (</u>	Click here to view the full AIMdefense license text. You do accept the license agrement by filling out the following form.
	License	<u> 4</u>	
	Password	a.	Ulcense Key
in.	Reporting		() AIMdefense
_			Reseller
	System		Customer
꺌	Access		Icense valid until
-	Interfaces		Graceperiod
	Network Services		Max. CPU
46	Firewall		Max. RAM
0	VDN		O DynDNS
			@ Modules
**	Proxies		
	Reverse Proxies		Register Check
Ŷ	Antivirus		
٠	Certificates		Click on the AppStore Button or change to System/Firmware/AIMdefense AppStore to install further modules.
С	High Availability		AppStore
v	Monitoring		
(0:	Wireless		In case you want to reinitialize all of your modules klick the following button. Please note that this would take some time.
Ð	Data Recovery		



#### 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.

Lobby: AIMdefense License	
Click here to view the full AIMdefense license text. You do accept the l	icense agrement by filling out the following form.
1 License Kev	
AIMdefense	04510112-05910112-206C0421
1 Reseller	
Customer     License valid until	
• Graceperiod	
Max. CPU	
1 DynDNS	
Modules	

### 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 l	icense agrement by filling out the following form.
1 License Key	04570172-059701f2-2d6c0421
AIMdefense	Advanced
Reseller	Secure 2 Fiber GmbH
Customer	Secure 2 Fiber GmbH
License valid until	04.12.2026 (+689 days left)
Graceperiod	01.01.2027
() Max. CPU	16
Max. RAM	128 GB
OynDNS	154245-1.aim.aimdefense.tech, 154245-2.aim.aimdefense.tech, 154245- 3.aim.aimdefense.tech, 154245-4.aim.aimdefense.tech
Modules	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  $\rightarrow$ Settings  $\rightarrow$ 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  $\rightarrow$ Settings  $\rightarrow$ AIMdefense Menuchanger.

Lobby	
Reporting	
🗮 System	
Firmware	Ħ
Settings	00
Administration	
Cron	
General	
Logging	
AIMdefense Menuchanger	
Miscellaneous	
Tunables	

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 beetween the following	g options:	
AlMdefense 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.	
AlMdefense Menu	The full AlMdefense menu style. However, the legacy menu is also available for those switching.	
Without AIM defense Menu	This is the legacy menu style provided by the first AIMdefense systems.	
		full help
Currently used	AlMdefense Menu with hidden Services	
Change to	AIMdefense Menu with hidden Services	
Save		
	AlMdefense Menu with hidden Services	
Please press the following button if you think the menu layout is corrup	AlMdefense Menu	
Refresh Menu Cache	Without AIMdefense Menu	



### 7. Adjust DynDNS

FIMdefense <				
Lobby Reporting System Access		Network Services: Dynamic DNS: S Accounts General settings	ettings	
M Interfaces M Network Services DHCPv4		O Enable O Verbose	2	
Dynamic DNS Settings Log File	•	Allow IPv6     O Interval	300	
Network Time OpenDNS	0	Backend	ddclient	
Unbound DNS 9 Firewall	*	Apply		
VPN				

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".

		Q	Search	C	7 🕶	:=
Current IP	Updated	De	escription		Cor	nmai
					an .	0

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

Edit Account			×
D advanced mode			full help 🕥
1 Enabled			
Description	AIM DNS		
Service	Custom	•	
Protocol	DynDNS 2	•	
Server	aim.aimdefense.tech		
Username	15151515		
Password			
() Wildcard			
Hostname(s)	171717-1.aim.aimdefense.tech × S Clear All 22 Copy ■ Paste Text		
Check ip method	freedns	•	
Interface to monitor	None	•	
Check ip timeout	10		
Force SSL			
			Cancel Save



Installation Guide

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".

<b>FIM</b> defense										N@AM.S2Liscal 🕘 🔍	
묘 Lobby			1. 1911.0. 1								
🗯 Reporting		Network Services: Dynamic DNS: Settings						• c •			
≣ System											
혈 Access		Accounts General settings									
🛦 Interfaces										0	0 1 1
A Network Services										Q starch	5 /* m*
DHCPv4		C io	Enabled	Service	❤ Hostnames	Username	Interface	Current IP	Updated	Description	Commands
Dynamic DNS		9a175e67-1af6-4071-8a14-0225b	o616 🗹	Custom (DynDNS 2)	161616-1.aim.aimdefense.tech	15151515	None				108
Settings											+ E
Log File											changes the Laft sender
Network Time	0	4 1 1 1 x									proving 1 to 1 of 1 entries
Occord/WS											

The account has now been created.

RIMdefense <					
😐 Lobby		TCP port			
📐 Reporting			443		
🗮 System		HTTP Redirect	Disable web GUI redirect rule		
Firmware					
Settings	<b>O</b> <sup>0</sup>	U Login Messages	□ Disable logging of web GUI successful logins		
Administration		Session Timeout	240		
Cron					
General		1 DNS Rebind Check	□ Disable DNS Rebinding Checks		
Logging		Alternate Hostnames			
AIMdefense Menuchanger			Alternate Us the proof for DNC Debinding and UTTO DECEDED Charles		
Miscellaneous			Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks		
Tunables		HTTP Compression	Off		
Wizard	×				
Log Files	۲	Access log	Enable access log		
Diagnostics	( <b>©</b> )	Server Log	✓ Log server errors		
🔮 Access					
🚠 Interfaces		Listen Interfaces	All (recommended)		
A Network Services		HTTP REFERER enforcement	Disable HTTP_REFERER enforcement check		
S Firewall					

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  $\rightarrow$  Settings  $\rightarrow$  Advanced  $\rightarrow$  "Firewall Maximum Table Entries .

Firewall     AIMdefense	U	Firewall Optimization	normal -
Aliases		Bind states to interface	
Automation	¢.		
Categories	۲	1 Disable Firewall	Disable all packet filtering.
Groups	æ	Firewall Adaptive Timeouts	start
NAT	⇒		
Rules	~		
Shaper	T	Firewall Maximum States	
Intrusion Detection	U		
Settings	Q <sub>0</sub> <sup>0</sup>	Firewall Maximum Fragments	
Advanced			
Normalization		Firewall Maximum Table Entries	2000000
Schedules			

## Under the menu item "Firewall" $\rightarrow$ AIMdefense $\rightarrow$ Settings: Activate all aliases. Confirm with "Apply".

AIMdefense <		
🖵 Lobby	Firewalls AIM defenses Settings	
Reporting	Firewall: Aimdelense: Settings	
🗮 System	ID.4	
📽 Access	IFV4	
🚠 Interfaces		
A Network Services	✓ AIMdefense Basic	
✤ Firewall	1 AIMdefense Basic Alias	
AIMdefense 🛡	Enable VOIP	
Dashboard	✓ AIMdefense Advanced	
Black-/Whitelist		_
Settings	Enable Abuse	
Log File	1 Enable Attack	
Aliases	Enable Compromised	
Automation 🍄	Enable Malicious	
Categories 🖏	1 Enable Malware	
Groups	1 Enable Phishing	
NAT 🔁	Enable Proxies	
Rules 🗸	× AlMdefense Firewall Pules	
Shaper <b>T</b>		
Intrusion Detection	Hints for Firewall Rules	
Settings 😋	• Rule interfaces	WAN
Log Files 💿		Clear All Select All
Diagnostics 💼	Direction	any 👻
O VPN		Add Rule Remove Rules
Certificates	_	
C High Availability	Apply	

