

AIMdefense

Firewall-Einrichtung

1. AIMdefense FIREWALL mit Fritz!Box verbinden / verkabeln.....	Seite 2
2. AIMdefense FIREWALL Inbetriebnahme.....	Seite 3
3. AIMdefense FIREWALL Installation Wizard.....	Seite 4
4. Troubleshooting bei WAN PPPoE.....	Seite 4
5. AIMdefense FIREWALL Lizenz Key einspielen.....	Seite 5
6. AIMdefense FIREWALL Menuchanger.....	Seite 7
7. DynDNS anpassen	Seite 8

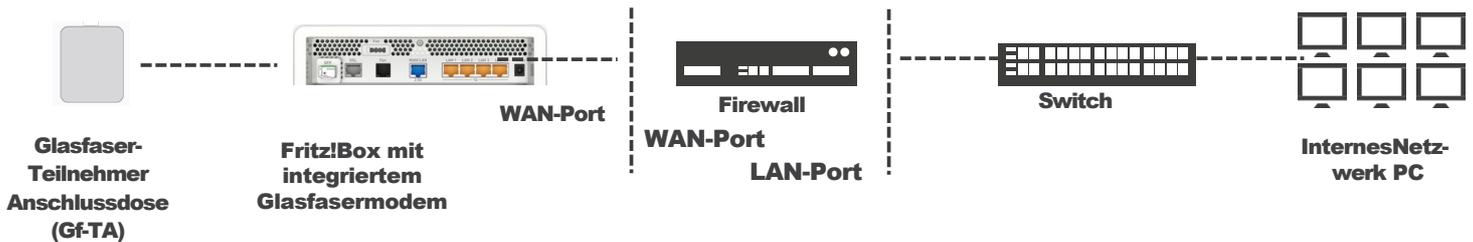
1. AIMdefense FIREWALL mit Fritz!Box verbinden / verkabeln



Bevor Sie beginnen, überprüfen Sie, ob Sie alle Daten von Ihrem Internet Service Provider vorliegen haben und mit dem Internet verbunden sind.

Bevor Sie mit der Administration der Firewall beginnen, müssen Sie die Firewall mit dem internen und externen Netzwerk verbinden.

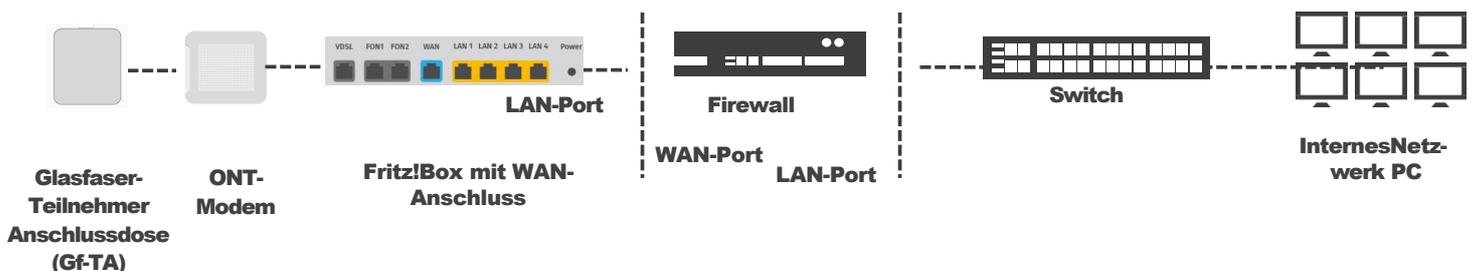
Aktion 1 : Anschließen der AIMdefense Firewall zu einer Fritz!Box mit integriertem Glasfasermodem



Verbinden Sie die Anschlussdose und die Fritz!Box mit einem Glasfaserkabel. Nun stellen Sie eine Verbindung über den WAN-Port der AVM-Fritz!Box zum WAN-Port der Firewall her.

Stellen Sie die Verbindung zwischen der Firewall (Lan-Port) und dem Switch mit einem RJ45-Netzwerkkabel her. Beachten Sie, dass Ihr PC mit diesem Netzwerk verbunden sein muss.

Aktion 2 : Anschließen der AIMdefense Firewall und einer Fritz!Box mit WAN-Anschluss und externen ONT-Modem



Verbinden Sie die Anschlussdose und das ONT-Modem mit einem Glasfaserkabel. Dann schließen Sie das ONT-Modem an den LAN-Port der Fritz!Box mit einem RJ-45 Netzwerkkabel an. Nun stellen Sie eine Verbindung über den LAN-Port der AVM-Fritz!Box zum WAN-Port der Firewall her.

Stellen Sie die Verbindung zwischen der Firewall (Lan-Port) und dem Switch mit einem RJ45-Netzwerkkabel her. Beachten Sie, dass Ihr PC mit diesem Netzwerk verbunden sein muss.

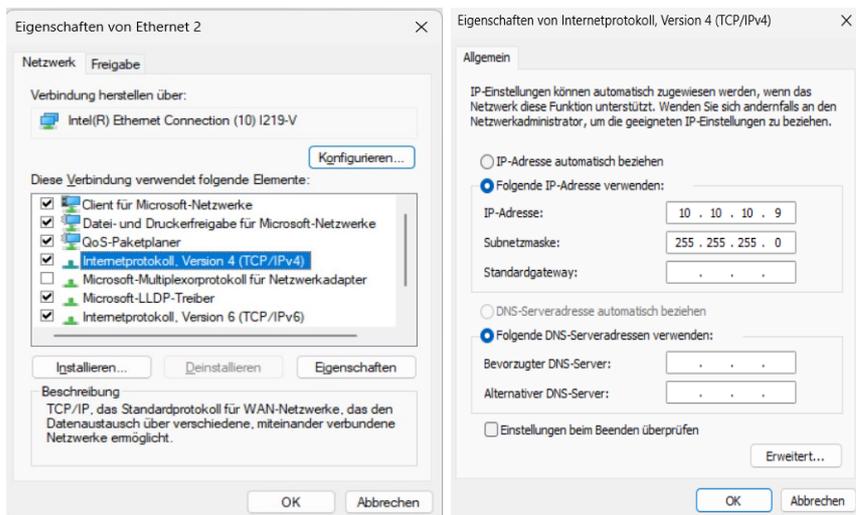
2. AIMdefense FIREWALL Inbetriebnahme

Port	IP Adresse	Funktion
LAN	10.10.10.10/255.255.255.0	LAN - Internes Netz
WAN	DHCP	WAN - Externes Netz
IP Adresse Admin Interface	Benutzername	Passwort
10.10.10.10	root	sysadm

Inbetriebnahme

Wenn Sie die AIMdefense FIREWALL verbunden haben, schalten Sie die Appliance am Netzschalter an. Der Netzschalter befindet sich neben dem Netzanschluss. Sobald die Appliance vollständig hochgefahren ist (ca. 2min), können Sie sich mit dem PC verbinden. Zuvor wird die Einrichtung der Client-PC benötigt.

Client PC einstellen



(Beispiel: Client-PC Einrichtung bei Windows.

Dazu „Eigenschaften von Ethernet“ aufrufen und dann „Internetprotokoll, Version 4(TCP/IPv4)“ und „Folgende IP-Adresse verwenden“ anklicken.

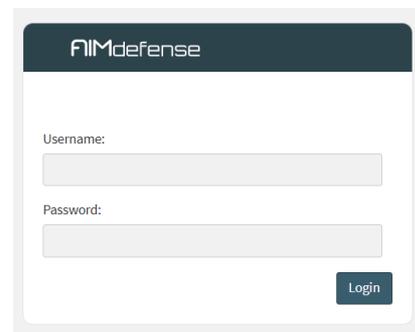
Stellen Sie Ihre Netzwerkkarte auf folgenden IP-Adresskreis 10.10.10.x ein. Subnetzmaske : 255.255.255.0.

Bitte anschließend speichern.

Nachdem Sie nun eine bestehende Verbindung zwischen dem PC und der FIREWALL hergestellt haben, öffnen Sie den Browser und geben Sie https://10.10.10.10 ein.

Melden Sie sich mit den nachfolgenden Standarddaten an:

Benutzername: **root**, Passwort: **sysadm**



3. AIMdefense FIREWALL Installation Wizard

Nach erfolgreichem Login gehen Sie auf den Menüpunkt System → Wizard. Verwenden Sie den Assistenten, um folgende Einstellungen vorzunehmen:

- Generelle Einstellungen (Name, Sprache und DNS)
- Datums-/Zeitzone
- Externe Netzwerkeinstellungen (WAN). Die Verbindung zum WAN hängt von der Art des Internetzugangs ab.

 Falls als **WAN IP eine Private IP** verwendet wird, **deaktivieren** Sie die Option zu RFC1918.

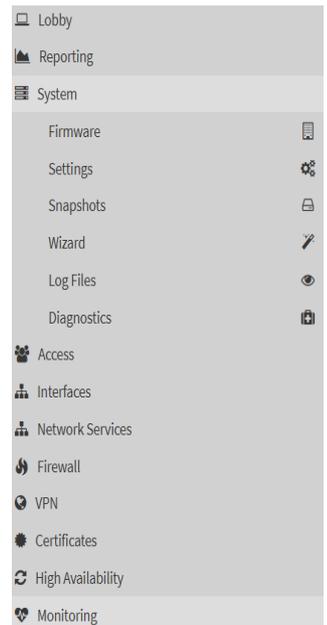
RFC1918 Networks

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

- Internes Netzwerk (LAN)
- Passwort setzen für root

Nachdem Sie den Wizard erfolgreich durchlaufen haben, können Sie über die interne Schnittstelle LAN mit dem Internet konnektieren.

Weitere Informationen zur Administration finden Sie auf unserer Website <https://aimdefense.tech> oder über das Suchfeld rechts oben auf dem Admin Interface.

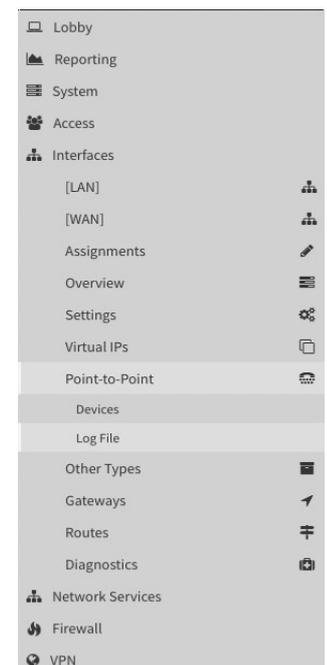


4. Troubleshooting bei WAN PPPoE

Sollten Sie mit einer Verbindung über PPPoE keine Verbindung bekommen, gehen Sie bitte zu dem Menüpunkt Interfaces → Point-to-Point → Log File.

Dort finden Sie das Logfile mit den Informationen zu Ihrer PPPoE Verbindung.

 Es kann bei DSL-Providern vorkommen, dass diese eine andere MTU oder VLAN Tag benutzen. Bitte prüfen Sie dies bei Ihrem Provider.
Bitte prüfen Sie, ob Ihr Modem über das neueste Firmware-Update verfügt.



5. AIMdefense FIREWALL Lizenz Key einspielen

Nachdem Sie erfolgreich den Wizard ausgeführt haben und die AIMdefense FIREWALL mit dem Internet verbunden ist, können Sie den AIMdefense Lizenz Key einspielen. Gehen Sie in dem Menüpunkt „Lobby → AIMdefense License“ und geben Sie ihn dort ein.

Lobby: AIMdefense License

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

License Key

AIMdefense

Reseller

Customer

License valid until

Graceperiod

Max. CPU

Max. RAM

DynDNS

Modules

Register **Check**

Click on the AppStore Button or change to System/Firmware/AIMdefense AppStore to install further modules.

AppStore

In case you want to reinitialize all of your modules click the following button. Please note that this would take some time.

Reinit all modules

Den Lizenz Key bekommen Sie von Ihrem Partner mitgeteilt.



Die Registrierung des Lizenz Keys schaltet verschiedene Module frei. Auch erhalten Sie Informationen zum Ablauf der Lizenz, DynDNS Namen, maximalen RAM und CPU.

Klicken Sie anschließend auf den Button „Register“.

Lobby: AIMdefense License

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

License Key

AIMdefense

Reseller

Customer

License valid until

Graceperiod

Max. CPU

Max. RAM

DynDNS

Modules

Bei erfolgreicher Registrierung erhalten Sie die folgende Anzeige:

Lobby: AIMdefense License

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

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
DynDNS	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

Die Lizenz wurde nun erfolgreich registriert.

Unter „Modules“ sehen Sie die für Sie lizenzierten Module. Klicken Sie auf den Button „Reinit all modules“ um fehlenden Module nachträglich zu installieren.

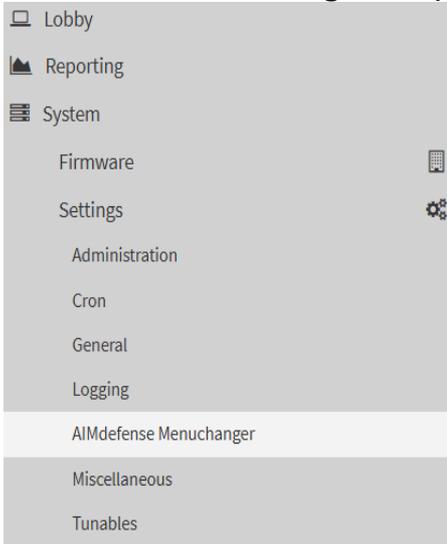
Dieser Vorgang kann einige Minuten in Anspruch nehmen.



Sollten Sie die Module nicht in der Menü-Übersicht sehen, wechseln Sie bitte im Menü auf „System → Settings → AIMdefense Menuchanger“ und klicken Sie den Button „Refresh Menu Cache“.

6. AIMdefense FIREWALL Menuchanger

Sie können die Menüstruktur links unter „System Settings AIMdefense Menuchanger“ anpassen.



Es stehen Ihnen 3 Optionen zur Verfügung. Nachdem Sie den „Menu Type“ geändert haben, klicken Sie den Button „Refresh Menu Cache“.

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

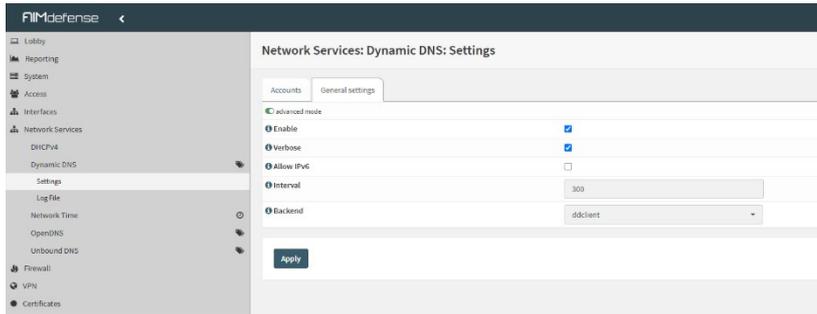
Change to:

Save

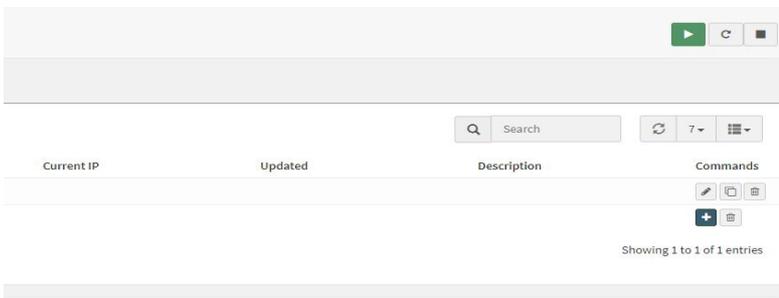
Please press the following button if you think the menu layout is corrupted:

AIMdefense Menu with hidden Services
AIMdefense Menu
Without AIMdefense Menu

7. DynDNS anpassen



Klicken Sie auf der linken Seite der Anwendung auf die Schaltfläche „Network Services“ -> „Dynamic DNS“-> „Settings“-> „General Settings“. Unter dem Menüpunkt „Backend“ stellen Sie den Reiter auf „ddclient“ und speichern die Änderung mit „Apply“.



Nun klicken Sie unter „Settings“ auf „Accounts“. Dann klicken Sie auf das „+“ Symbol um einen Account zu erstellen.

Edit Account ×

advanced mode full help

Enabled

Description: AIM DNS

Service: Custom

Protocol: DynDNS 2

Server: aim.aimdefense.tech

Username: 15151515

Password:

Wildcard:

Hostname(s): 171717-1.aim.aimdefense.tech ×
Clear All Copy Paste Text

Check ip method: freedns

Interface to monitor: None

Check ip timeout: 10

Force SSL:

Cancel Save

Folgende Einstellungen sind unter „Edit Account“ vorzunehmen:

- „Enabled“ auswählen und anklicken.
- „Service“ auswählen und den Reiter auf „Custom“ stellen.
- „Protocol“ auswählen und den Reiter auf „DynDNS 2“ stellen.
- „Server“ auswählen und „aim.aimdefense.tech“ eintragen.
- „Username“ und „Password“ entsprechende Zugangsdaten eingeben.
- „Wildcard“ auswählen und den Haken entfernen.

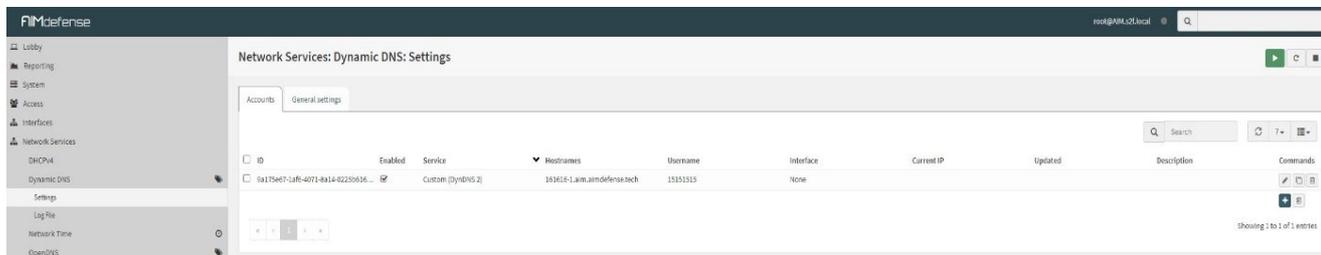
„Hostname“ eintragen: DynDNS (abhängig von der Lizenz), Beispiel:

„171717-1.aim.aimdefense.tech“.

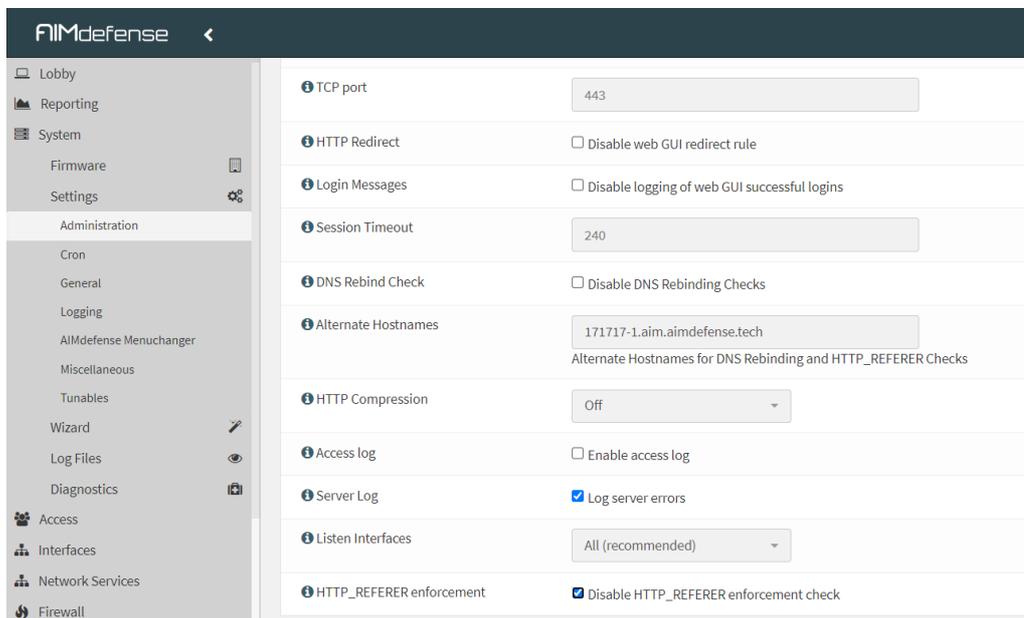
„Check ip methode“ auswählen und umstellen auf „freedns“.

„Check ip timeout“ auswählen und den Wert 10 eintragen bzw. überprüfen.

„Force SSL“ auswählen, anklicken und alle Änderungen mit „Save“ speichern.



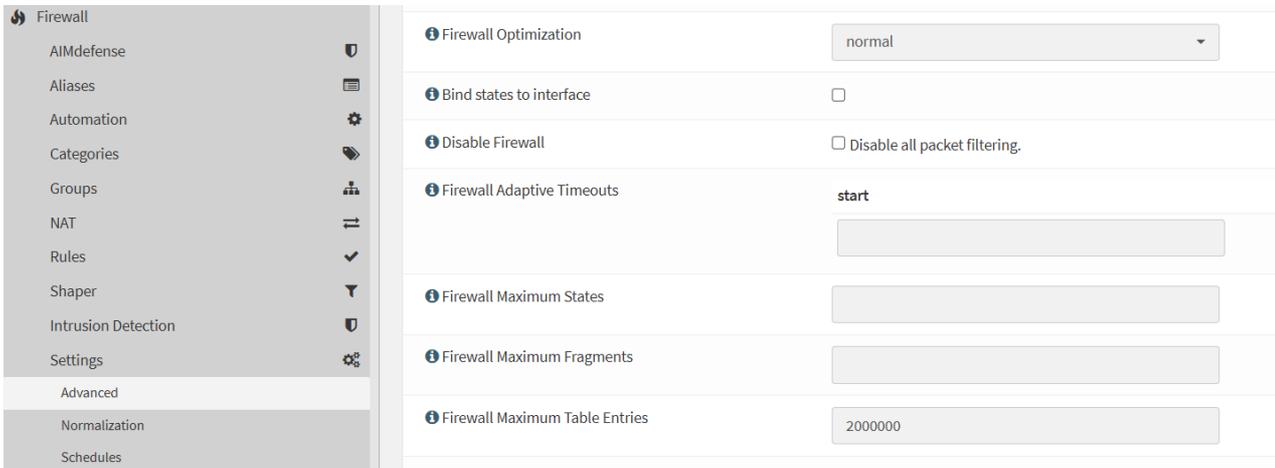
Der Account wurde somit angelegt.



Klicken Sie nun auf der linken Seite der Anwendung auf die Schaltfläche System->Settings->„Administration“. Unter „Alternate Hostnames“: „xxx.dyn/aim.aimdefense.tech“ eintragen.

Bei „HTTP_REFERER enforcement“ ein Haken für „Disable HTTP_REFERER enforcement check“ setzen und speichern.

Um alle Aliase zu aktivieren, muss vorher unter Firewall → Settings → Advanced → „Firewall Maximum Table Entries“ der Default Eintrag erhöht werden auf „2000000“



Unter dem Menüpunkt: Firewall → AIMdefense → Settings: Alle Aliase aktivieren. Mit Apply bestätigen.

