FIMdefense 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 AlMdefense 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 AlMdefense 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	10.10.10/255.255.255.0	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

igenschat	ften von Ethernet 2	×	Eigenschaften von Internetprotok	oll, Version 4 (TCP/IPv4)
Netzwerk	Freigabe		Allgemein	
Verbindu	ng herstellen über: tel(R) Ethernet Connection (10) I219-V		IP-Einstellungen können automatis Netzwerk diese Funktion unterstüt Netzwerkadministrator, um die gee	ich zugewiesen werden, wenn das izt. Wenden Sie sich andernfalls an den eigneten IP-Einstellungen zu beziehen.
		Konfigurieren	O IP-Adresse automatisch bezie	ehen
Diese Ve	erbindung verwendet folgende Elemente	e:	Folgende IP-Adresse verwen	den:
V 📮	Client für Microsoft-Netzwerke Datei- und Druckerfreigabe für Microso	ft-Netzwerke	IP-Adresse:	10 . 10 . 10 . 9
v 📮	QoS-Paketplaner		Subnetzmaske:	255 . 255 . 255 . 0
Internetprotokoll, Version 4 (TCP/IPv4) INTERverkadapter		Standardgateway:		
⊻ ±	Microsoft-LLDP-Treiber Internetprotokoll, Version 6 (TCP/IPv6)		ODNS-Serveradresse automati	sch beziehen
			Folgende DNS-Serveradresse	en verwenden:
Insta	allieren Deinstallieren	Eigenschaften	Bevorzugter DNS-Server:	
Beschr TCP/I	eibung P. das Standardprotokoll für WAN-Netz	werke das den	Alternativer DNS-Server:	
Daten Netzw	austausch über verschiedene, miteinan erke ermöglicht.	der verbundene	Einstellungen beim Beenden	überprüfen Erweitert
	ОК	Abbrechen		OK Abbrechen

(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**

AIM defense	
Username:	
Password:	
	Login

3.AIMdefense FIREWALL Installation Wizard

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

- \cdot Generelle Einstellungen (Name, Sprache und DNS)
- · Datums-/Zeitzone
- $\cdot\,$ 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: DBlock 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 <u>https://aimdefense.tech</u> 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 \rightarrow Point-to-Point \rightarrow 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 \rightarrow AIMdefense License" und geben Sie ihn dort ein.

□	Lobby		Lobby: AIMdefense License
	Dashboard	6 10	Click have to visuate full All defense lisenes tout. You do seent the lisenes grow on the filling out the following form
	TUXGUARD License	4 <u>1</u> 4	Click here to view the full Almderense license text. You do accept the license agrement by filling out the following form.
	License	4 <u>1</u> 4	O License Key
	Password	a.	
	Reporting		③ AIMdefense
_	Sustem		Reseller
	System		Gustomer
	Access		License valid until
*	Interfaces		() Graceperiod
	Network Services		() Max. CPU
.63	Firewall	3	Max. RAM
0	VPN		O DynDNS
	Proxies		() Modules
44	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		
¢	Wireless		In case you want to reinitialize all of your modules klick the following button. Please note that this would take some time.
Э	Data Recovery		

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 agrement by filling out the following form.			
D License Key	04570172-059701f2-2d6c0421			
IMdefense				
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 AIM defense license text. You do accept the license agreent by filling out the following form.					
1 License Key	04570172-059701f2-2d6c0421				
O AIMdefense	Advanced				
Reseller	Secure 2 Fiber GmbH				
() Customer	Secure 2 Fiber GmbH				
O License valid until	04.12.2026 (+689 days left)				
() Graceperiod	01.01.2027				
Max. CPU	16				
1 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					

Die Lizenz wurde nun erfolgreich registriert.

Unter "Modules" sehen Sie die für Sie lizensierten 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 \rightarrow Settings \rightarrow AIMdefense Menuchanger" und klicken Sie den Button "Refresh Menu Cache".



6. AIMdefense FIREWALL Menuchanger

Sie können die Menüstruktur links unter "System $\hfill\square$ Settings $\hfill\square$ AlMdefense Menuchanger" anpassen.

Lobby		
Reporting		
📑 System		
Firmware		
Settings	Q o	
Administration		
Cron		
General		
Logging		
AIMdefense Menuchanger		
Miscellaneous		
Tunables		

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 beetween the following options:			
AIMdefense Menu with hidden Services	The full AIM defense menu style with removed Services menu. This would be the preferred option if you are new to AIM defense or to the underlying OPN sense 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	AMdefense 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. DynDNS anpassen

FIMdefense <				
Lobby		Notwork Servicest Dunamic DNS: 5	ottings	
Reporting		Network Services: Dynamic DNS: 5	ettings	
System				
Access		Accounts General settings		
Interfaces		C advanced mode		
Network Services		() Enable	53	
DHCPv4		() Verbose	2	
Dynamic DNS		@ Allow IPv6		
Settings		@ Interval	200	
Log File				
Network Time	Ø	() Backend	ddclient	-
OpenDNS				
Unbound DNS		tente		
Firewall		Африу		
VPN				
and a				

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		×
O advanced mode		full help 🕥
1 Enabled		
Description	AIM DNS	
Service	Custom	
Protocol	DynDNS 2	
Server	aim.aimdefense.tech	
1 Username	15151515	
1 Password		
1 Wildcard		
Hostname(s)	171717-1.aim.aimdefense.tech × ② Clear All 2 ⁰ Copy 1 ⁵ 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.

FilM defense									R@AMLs2Llocal 🔍 🔍	
교 Lobby		Nutrie Construction								
🗯 Reporting		Network Services: Dynamic DNS: Settings							> C	
System										
🗑 Access		Accounts General settings								
🛦 Interfaces									0	0 3 10
A Network Services									Q Starch	₩ E
DHCPv4		0 10	Enabled Service	❤ Hostnames	Username	Interface	Current IP	Updated	Description	Commands
Dynamic DNS		Sa175e67-1af6-4071-8a14-0225	b616 🗹 Custom (DynDNS 2)	161616-1.aim.aimdefense.tech	15151515	None				108
Settings										• 8
Log Flie										changes the Laft sector
Network Time	0	4 1 1 1 1								showing 1 to 1 or 1 entries
OpenDNS										

Der Account wurde somit angelegt.

RIMdefense <					
🖵 Lobby		CP nort			
Reporting		U TCP port	443		
📑 System		HTTP Redirect	Disable web GUI redirect rule		
Firmware		0 ,			
Settings	Φ ₀ ^o	 Login Messages 	□ Disable logging of web GUI successful logins		
Administration		Session Timeout	240		
Cron					
General Logging AlMdefense Menuchanger Miscellaneous Tunables		1 DNS Rebind Check	□ Disable DNS Rebinding Checks		
		Alternate Hostnames	171717-1.aim.aimdefense.tech Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks		
		HTTP Compression	Off		
Wizard	1				
Log Files	۲	Access log	Enable access log		
Diagnostics	(2)	3 Server Log	✓ Log server errors		
 Access Interfaces 			All (recommended)		
		UISTEN INTERTACES			
A Network Services		HTTP_REFERER enforcement	Disable HTTP_REFERER enforcement check		
S Firewall					

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 \rightarrow Settings \rightarrow Advanced \rightarrow "Firewall Maximum Table Entries" der Default Eintrag erhöht werden auf "2000000"

🚯 Firewall			
AIMdefense	U	• Firewall Optimization	normal
Aliases		Bind states to interface	
Automation	•		
Categories	۲	1 Disable Firewall	□ Disable all packet filtering.
Groups	#	Firewall Adaptive Timeouts	start
NAT	⇒		
Rules	~		
Shaper	T	Firewall Maximum States	
Intrusion Detection	U		
Settings	O ^o	Firewall Maximum Fragments	
Advanced			
Normalization		Firewall Maximum Table Entries	2000000
Schedules			

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

AIMdefense <			
🖵 Lobby	Eirowall: AMdofonco: Sottings		
A Reporting	Filewall. Aimdelense. Settings		
📑 System			
📽 Access			
👪 Interfaces			
A Network Services	✓ AIMdefense Basic		
ℰ Firewall	AIMdefense Basic Alias		
AIMdefense	D Enable VOIP		
Dashboard			
Black-/Whitelist		_	
Settings	Enable Abuse		
Log File	Enable Attack		
Aliases	Enable Compromised		
Automation	C Enable Malicious		
Categories	Enable Malware		
Groups	Enable Phishing		
NAT			
Rules	AlMdefence Firewall Pulse		
Shaper	 Aimdelense Firewalt Rules 		
Intrusion Detection	D Hints for Firewall Rules		
Settings	Rule interfaces	WAN 👻	
Log Files		O Clear All O Select All	
Diagnostics	Direction	any 👻	
O VPN		Add Dula Demous Dulas	
Certificates		Add Rule Remove Rules	
C High Availability	Apply		
AA			