

AIMdefense

AIMdefense-Anleitung zur Systemmigration von ICM Defense auf AIMdefense

AIMdefense-Anleitung zur Systemmigration von ICM Defense auf AIMdefense

Lesen Sie bitte diese Anleitung vor Beginn der Migration sorgfältig durch!

Falls Sie DynDNS benutzen, bitte die alten Daten aus der Config abspeichern, da diese nach der Migration neu eingerichtet werden müssen.

Falls Sie das Unifi Modul benutzen, bitte zuerst die Unifi-Update Anleitung durchlesen.

Eine Systemmigration auf AIMdefense ist nur ab der Version ICM Defense 22.7 möglich. Wenn eine ICM-Version älter als 22.7 vorliegt, bitte zunächst ein Update auf ICM-Version 22.7 ausführen und anschließend die Systemmigration auf AIMdefense starten. Andernfalls ist nur noch eine Neuinstallation per ISO-Datei möglich.

•Per SSH auf die Firewall zugreifen und sich einloggen mit:

Benutzername: **root**
Password: **sysadm**

•**Option 8** für Shell auswählen.

```
0) Logout                7) Ping host
1) Assign interfaces     8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system       12) Update from console
6) Reboot system          13) Restore a backup

Enter an option: 8

root@AIM:~ # curl -s -o migrate.sh https://pkg.aimdefense.tech/migrate.sh
root@AIM:~ # sh migrate.sh
```

„curl -s -o migrate.sh https://pkg.aimdefense.tech/migrate.sh “
ausführen (nicht pipen!).

```

  _ _ _ _ _
 /_/_/_/_/_/
/_/_/_/_/_/
/_/_/_/_/_/
Migration Tool v1.6.1

Please make sure this system has access to the internet!
Are you sure you want to continue? [y/N] █

```

- Mit „Y“ bestätigen.

```

>>> Cleaning up... done
>>> Reboot now? [y/N] █

```

- Mit „Y“ bestätigen.

- Falls ein DynDNS eingerichtet war, bitte neu einrichten.

Die DynDNS Adresse ändert sich dadurch wie folgt:

- Aus „**dyn.tgfw.de**“ wird „**dyn.aimdefense.tech**“.
- Aus „**icm.tgfw.de**“ wird „**aim.aimdefense.tech**“.
- Aus „**tg**“ wird „**s2f**“.

Hierzu Beispiele:

- tg-1-22.dyn.tgfw.de => s2f-1-22.dyn.aimdefense.tech
- 33321-2.icm.tgfw.de => 33321-2.aim.aimdefense.tech

Zur DynDNS Einrichtung mit dem neuen **ddclient** bitte die DynDNS Anleitung verwenden (bitte so lange updaten, bis diese sich von allein installiert).

Den Pfad hierzu finden Sie in der hinterlegten DynDNS Anleitung.

Das Migrationslog kann unter /root/migration_Zeitstempel.log gefunden werden.

Hinweis für Kunden mit dem Tools-Modul und einer Advance-Lizenz:

The screenshot displays the AIMdefense configuration interface. On the left is a navigation sidebar with categories like Lobby, Reporting, System, Access, Interfaces, Network Services, Firewall, and VPN. The main content area shows the 'Firewall' settings, specifically the 'Logging' and 'Miscellaneous' sections.

Logging Section:

- Default block: Log packets matched from the default block rules
- Default pass: Log packets matched from the default pass rules
- Outbound NAT: Log packets matched by automatic outbound NAT rules
- Bogon networks: Log packets blocked by 'Block Bogon Networks' rules
- Private networks: Log packets blocked by 'Block Private Networks' rules

Miscellaneous Section:

- Keep counters
- Debug: Generate debug messages only
- Firewall Optimization: normal
- Bind states to interface
- Disable Firewall: Disable all packet filtering
- Firewall Adaptive Timeouts: start
- Firewall Maximum States: [input field]
- Firewall Maximum Fragments: [input field]
- Firewall Maximum Table Entries: 2000000
- Static route filtering: Bypass firewall rules for traffic on the same interface
- Disable reply-to: Disable reply-to on WAN rules
- Disable anti-lockout: Disable administration anti-lockout rule
- Aliases Resolve Interval: [input field]
- Check certificate of aliases URLs: Verify HTTPS certificates when downloading alias URLs

Anti DDOS Section:

- Enable syncookies: never (default)

A 'Save' button is located at the bottom right of the configuration area.

Um alle **Aliase** (zu finden unter „**Firewall**“->„**Aimdefense**“-> „**Settings**“) zu aktivieren, muss vorher unter Firewall → Settings → Advanced → „**Firewall Maximum Table Entries**“ der Default Eintrag auf „**2000000**“ gesetzt werden. (Standard ist 1000000, ist zu klein.)

Technischer Hinweis: In seltenen Fällen kann es passieren, dass sich die Login-Shell von bereits existierenden Benutzern auf der AIMdefense während dem Update auf „**nologin**“ stellen kann und diese danach nicht mehr einloggen können. Falls Sie hiervon betroffen sein sollten, folgen Sie bitte den folgenden Schritten zur Problembeseitigung:

„**Access / Usermanagement /Users**“ User Edit klicken und dann die „**Login shell**“ mit der Eingabe: **/bin/sh** wieder umstellen und speichern.

