FIMdefense

AIMdefense System Migration Guide from ICM Defense on AIMdefense



AIMdefense Guide to System Migration from ICM Defense to AIMdefense

Please read these instructions carefully before starting the migration!

If you use DynDNS, please save the old data from the config, as these will have to be set up again after the migration.

If you use the Unifi module, please read the Unifi update instructions first.

A system migration to AIMdefense is only possible from version ICM Defense 22.7. If you have an ICM version older than 22.7, please first update to ICM version 22.7 and then start the system migration to AIMdefense. Otherwise, only a new installation using an ISO file is possible.

Access the firewall via SSH and log in with:

| User Name: | root |
|------------|--------|
| Password: | sysadm |

• Select option 8 for Shell.

| 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 -sko migrate.sh https://pkg.aimdefense.tech/migrate.sh root@AIM:~ # sh migrate.sh | | | | | | |

Run "curl -sko migrate.sh https://pkg.aimdefense.tech/ migrate.sh" (do not pipe!).

FIMdefense SCALABLE CYBERSECURITY TECHNOLOGY





• If DynDNS was set up, please set it up again. The DynDNS address changes as follows:

- "dyn.tgfw.de" becomes "dyn.aimdefense.tech".
- "icm.tgfw.de" becomes "aim.aimdefense.tech".
- "tg" becomes "s2f".

Examples of this:

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

To set up DynDNS with the new **ddclient**, please use the DynDNS instructions (please update until it installs itself).

You can find the path to this in the provided DynDNS instructions.

The migration log can be found at /root/migration_Zeitstempel.log.

| AIMdefense < | | | |
|---------------------|--|--|--|
| 묘 Lobby | Logging | | |
| 📥 Reporting | | | |
| 🗮 System | O Default Diock | Log packets matched from the default block rules | |
| 📽 Access | Default pass | Log packets matched from the default pass rules | |
| 🛦 Interfaces | Outbound NAT | Los nockete metched hu submatic authound NAT rules | |
| A Network Services | | Li bag packets matched by abtomatic batbachd rear roles | |
| 5) Firewall | Bogon networks G Bogon networks Log packets blocked by 'Block Bogon Networks' rule | | |
| AIMdefense 🛡 | Private networks | Log packets blocked by 'Block Private Networks' rules | |
| Aliases | | n 1999 in a suide sa suide suide la suide suid | |
| Automation Ø | Miscellaneous | | |
| Categories | Keep counters | 0 | |
| NAT # | 0 Debug | Generate debug messages only 👻 | |
| Rules 🗸 | | | |
| Shaper T | Firewall Optimization | normal 👻 | |
| Intrusion Detection | Bind states to interface | | |
| Settings Oe | | | |
| Advanced | Oisable Firewall | Disable all packet filtering. | |
| Normalization | Firewall Adaptive Timeouts | start | |
| Schedules | | | |
| Log Files 🐵 | | | |
| Diagnostics | Firewall Maximum States | | |
| • VPN | | | |
| Certificates | Firewall Maximum Fragments | | |
| C High Availability | | | |
| V Monitoring | Firewall Maximum Table Entries | 2000000 | |
| Wireless | | _ | |
| Other Services | Static route filtering | Bypass firewall rules for traffic on the same interface | |
| Ø Services | Disable reply-to | Disable reply-to on WAN rules | |
| Data Recovery | O Disable anti-lockout | Disable administration anti-lockout rule | |
| 🗩 Power | | | |
| AIMdefense | O Aliases Resolve Interval | | |
| Ge Logout | Charle antificate of allower 1101 a | | |
| | er check deronicate of allases URLs | U verity HTTP's certificates when downloading alias UKLS | |
| | Anti DDOS | | |
| | Enable syncookies | never (default) * | |
| | | | |
| | | Save | |



In order to activate all **aliases** (can be found under "**Firewall**" -> "**Aimdefense**" -> "**Settings**"), the default entry must first be set to "**2000000**" under **Firewall** → **Settings** → **Advanced** → "**Firewall Maximum Table Entries**". (Default is 1000000, which is too low.)

FIMdefense Lobby Reporting System System Access Interfaces Interfaces Network Services AIMdefense Basic

| ÷. | Interfaces | | | | |
|----------|---------------------|----|----------------------------|-----------------------|--|
| # | Network Services | | ✓ AIMdefense Basic | | |
| 59 | Firewall | | AIMdefense Basic Alias | | |
| | AIMdefense | U | Enable VOIP | | |
| | Dashboard | | V AlMdefense Advanced | | |
| | Black-/Whitelist | | Aimuelense Auvanceu | | |
| | Settings | | Enable Abuse | | |
| | Log File | | Enable Attack | | |
| | Aliases | | Enable Compromised | | |
| | Automation | ٠ | Enable Malicious | | |
| | Categories | ۲ | Enable Malware | | |
| | Groups | 4 | Enable Phishing | | |
| | NAT | = | Enable Proxies | | |
| | Rules | * | AlMdefense Sizewall Dulas | | |
| | Shaper | T | * Amdelense Firewall Rules | | |
| | Intrusion Detection | U | Hints for Firewall Rules | | |
| | Settings | o° | Rule interfaces | WAN | |
| | Log Files | ۲ | | Clear All | |
| | Diagnostics | | Direction | any | |
| 0 | /PN | | | | |
| • | Certificates | | | Add Rule Remove Rules | |
| C | High Availability | | Apply | | |
| Ş | Monitoring | | | | |
| ((1- | Wireless | | | | |
| ¢ | Other Services | | | | |



Technical note: In rare cases it can happen that the login shell of existing users on the AIM defense can be set to "nologin" during the update and they can no longer log in afterwards. If you are affected by this, please follow the troubleshooting steps below:

Click "Access / Usermanagement /Users" User Edit and then change the "Login shell" again by entering: /bin/sh and save.

| Market Access | - | | | | |
|-------------------------|-----------------|--------------------------------|----------------------|---|--|
| Usermanagement | 225 | Canguage | | Default | |
| Users | | O Login shell | | /bin/sh 👻 | |
| Groups | | | | | |
| FIM defense < | | | | | |
| 🖵 Lobby | | | | | |
| Reporting | | | Generate a scrambl | ed password to prevent local database logins for this user. | |
| System | 🚯 Full n | ame | System Administ | rator | |
| Access 🐸 | | | | | |
| Users | 🕄 E-Mai | L | | | |
| Groups | 6 Comr | nent | | | |
| Servers | Goom | | | | |
| Tester | | | | 11 | |
| Configuration 🤊 | A Profe | red landing page | | | |
| Firmware | Griele | rea miname hage | | | |
| Gateways 4 | Langu | lage | Default | | |
| High Availability | | ala II | | | |
| Routes Ŧ | Ulogin | snett | /bin/sh | - | |
| Settings Q ₆ | C Expira | ition date | | | |
| Trust | | | | | |
| Wizaro | Group | Memberships | Not Member Of | Not Member Of | |
| Log Files 🐨 | | | | | |
| biagnostics iza | | | | | |
| Access | | | | | |
| | | | | | |
| Groups | | | | | |
| Servers | | | | | |
| Tester | | | | | |
| 🛔 Interfaces | | | | | |
| Network Services | Effect | ive Privileges | Inherited from | | |
| Firewall | | | admins | | |
| VPN | | | | | |
| Certificates | | | | | |
| C High Availability | () User | Certificates | Name | CA | |
| Standard Monitoring | | | + | | |
| 🗢 Wireless | C | | | | |
| Other Services | API ke | ys | key | | |
| Services | | | + | | |
| Data Recovery | OTP s | eed | | | |
| 🖋 Power | | | Canarata pour soor | t (160 bit) | |
| AIMdefense | | | C denerate new secre | | |
| 🕒 Logout | | uthorized keys Paste an author | | red keys file here. | |
| | | | Save Save at | nd go back Cancel | |
| | | | | | |

Am Brambusch 24 – 44536 Lünen - Germany Fon: + 49 231 999 854 00 E-Mail: info@secure2fiber.com Web: www.secure2fiber.com