FIMdefense

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	
Entei	r an option: 8			
root@AIM:~ # curl -sko migrate.sh https://pkg.aimdefense.tech/migrate.sh root@AIM:~ # sh migrate.sh				

"curl -sko migrate.sh https://pkg.aimdefense.tech/migrate.sh " ausführen (nicht pipen!).







```
•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:					
FIMdefense <					
모 Lobby	Logging				
Keporting	O Default black				
🗮 System	O Default Dick	Log packets matched from the default block rules			
Market Access	O Default pass	Log packets matched from the default pass rules			
A Interfaces	Outbound NAT	Log packets matched by automatic outbound NAT rules			
An intervent services	Bogan networks	Log packets blocked by 'Block Bogon Networks' rules			
AIMdefense 0	Private networks	I og nackets blocked hv 'Block Private Networks' rules			
Aliases		Log packets blocked by block Private Networks Tures			
Automation	Miscellaneous				
Categories	Keep counters				
Groups 🚠	0 Dohur				
NAT =	0.0005	Generate debug messages only *			
shaper T	Firewall Optimization	normal 👻			
Intrusion Detection	Dind states to interface				
Settings O _e	Conditionation of the nace				
Advanced	Disable Firewall	Disable all packet filtering.			
Normalization	Firewall Adaptive Timeouts	start			
Schedules					
Diagnostics (1)					
O VPN	Firewall Maximum States				
Certificates	Firewall Maximum Fragments				
C High Availability					
V Monitoring	Firewall Maximum Table Entries	2000000			
♥ Wireless	Static couts filtering	Discuss formall adaption for both on the same interface.			
Other Services	State rote menng	Bypass newall rules for tranic on the same interface			
© Services	Disable reply-to	Disable reply-to on WAN rules			
Druer	0 Disable anti-lockout	Disable administration anti-lockout rule			
AIMdefense	Aliases Resolve Interval				
🗭 Logout					
	O Check certificate of aliases URLs	□ Verify HTTPS certificates when downloading alias URLs			
	Anti DDOS				
	Enable syncookies	never (default) *			
		Save			



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

NM defense	

Lobby	Firew	all: AIMdefense: Settings	
Les Reporting	Them	au Aunderenser settings	
System	IDv4		
Market Access	11- 0-4		
🚠 Interfaces			
A Network Services	~ AIMo	defense Basic	
b Firewall	1 AIMde	fense Basic Alias	2
AIMdefense	0 Enable	e VOIP	
Dashboard	AIM.	defense Advanced	
Black-/Whitelist	* AIMC	Jerense Advanced	
Settings	1 Enable	e Abuse	
Log File	1 Enable	e Attack	
Aliases	CEnable	e Compromised	
Automation	C Enable	e Malicious	2
Categories	S Enable	e Malware	
Groups	d Enable	e Phishing	
NAT	≓ O Enable	e Proxies	
Rules	*		
Shaper	T Y AIMO	defense Firewall Rules	
Intrusion Detection	0 Hints	for Firewall Rules	
Settings	OS O Rule in	nterfaces	WAN
Log Files	۲		Clear All
Diagnostics	Direct	ion	any
• VPN			
Certificates			Add Rule Remove Rules
C High Availability	Apply		
V Monitoring		-	
♥ Wireless			
Other Services			

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 Problembehebung:

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

🔮 Access			
Usermanagement	*	① Language	Default
Users		O Login shell	/bin/sh
Groups			11
FIIMdefense <			
🖵 Lobby			
Reporting			Generate a scrambled password to prevent local database logins for this user.
System	Ful	Iname	System Administrator
Access			
Users	0 E-1	Tail	
Groups	0 Co	nment	
Servers			
Tester	-		
Configuration	9 • • • • •	forred landing page	
Firmware		nerred tanding page	
Gateways	1 O Lar	nguage	Default
High Availability	0		
Routes		țin snell	/bin/sh 👻
Settings	0%	iration date	
Trust	•		
Wizard	🕄 Gro	up Memberships	Not Member Of
Log Files	۲		
Diagnostics I	C 1		
Access			
Usermanagement			
Users			·*•
Servere			
Tester			
A Interfaces			
A Network Services	O Eff	ective Privileges	Inherited from
6) Firewall			admins
VPN			
Certificates			8
C High Availability	O Us	er Certificates	Name CA
V Monitoring			+
♥ Wireless			
Other Services	O AP	keys	key
Services			+
Data Recovery	6.01	Pseed	
🖋 Power	001		
AIMdefense			Generate new secret (160 bit)
Core Logout		horized keys	Paste an authorized keys file here.
			Save Save and go back Cancel
Secure 2 Fiber	Secure 2 Am Bran	Fiber Distribution GmbH abusch 24 – 44536 Lünen -	- Germany

Distribution GmbH —

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