OPNsense Migration Legacy zu Instance, ohne neues Ausrollen von Konfigurationen

Sicher habt ihr schon die Meldung der OPNsense Firewall unter OpenVPN / Legacy gesehen

> **“ This component is reaching the end of the line, official maintenance will end as of version 26.1**

Die Migration zur Instanz ist nicht sonderlich kompliziert, jedoch gibt es zwei Fallstricke.

1. Deaktiviert den alten Server
2. Falls Shared Key verwendet wurde, unter Static Key diesen Text übernehmen, Mode Auth
3. Konfiguriert eure neue Instanz mit mindestens diesen Einstellungen
    1. Role: Server
    2. Enabled: yes
    3. Port Number: wie bisher, z. B. 1194
    4. Type: TUN
    5. Server IP: Hier den alten Wert von IPv4 Tunnel Network übernehmen, z. B. 172.16.1.0/24
    6. Toplolgy: subnet
    7. Certificate: hier den alten Eintrag von Server Certificate übernehmen
    8. Certificate Authority: hier den alten Eintrag von Peer Certificate Authority übernehmen
    9. Dann links oben Advanced Mode einblenden
    10. Unter TLS static key den vorher angelegten Key auswählen
    11. Auth: den alten Wert von Auth Digest Algorithm übernehmen, z. B. SHA256
    12. Autentication: den vorherigen Serveranbieten, z. B. DC, UCS, Zamba auswählen, wenn vorhanden
    13. Renegotiate Time: 3600
    14. Auth Token Lifetime: 43200
    15. Local Network: den alten Wert von IPv4 Local Network auswählen

16. Falls vorher bei Compression etwas ausgewählt war, selbst Disabled, dann Compression migrate unter Advanced anklicken
17. Weitere Parameter falls benötigt

Der technische Stand dieser Dokumentation ist von April 2025 und funktioniert mit der Version OPNsense 25.1.4_1-amd64.

Die Business Edition 24.10 verfügt noch nicht über den Compression Migrate. Daher muss die Version Business 25.x abgewartet werden!

Beispiel

Edit Instance

Protocol	UDP
Port number	1195
Bind address	
Type	TUN
Verbosity	3 (Normal)
Concurrent connections	
Keep alive interval	
Keep alive timeout	
Server (IPv4)	172.16.116.0/24
Server (IPv6)	
Topology	subnet

Trust

Certificate	Server-CA-Neu
Verify Remote Certificate	☐
Certificate Authority	VPN-CA-Neu
Certificate Revocation List	Nothing selected
Verify Client Certificate	required
Use OCSP (when available)	☐
Certificate Depth	Do Not Check
TLS static key	(auth (Authenticate control channel pack
Auth	SHA512 (512-bit)
Data Ciphers	Nothing selected Clear All Select All
Data Ciphers Fallback	None

Authentication

Authentication	UCS Clear All Select All
Enforce local group	None
Username as CN	☐
Strict User/CN Matching	No
Renegotiate time	3600
Auth Token Lifetime	43200
Auth Token Renewal	
Auth Token secret	⚙
Require Client Provisioning	☐

Routing

Local Network	192.168.115.0/24 × Clear All Copy Paste Text
Remote Network	 Clear All Copy Paste Text

Miscellaneous

Options	Nothing selected Clear All Select All
Push Options	Nothing selected Clear All Select All
Push Inactivity	

cz

Version #2
Erstellt: 9 April 2025 13:21:07 von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 9 April 2025 13:44:29 von Christian Zengel (sysops GmbH)