

# OpenVPN4UCS mit privacyIDEA



VPN wie es einfacher und sicherer kaum sein kann

Felix Kronlage

CFA – [kronlage@bytemine.net](mailto:kronlage@bytemine.net)



Entwicklungsmanufaktur für innovative Lösungen

# Fahrplan

- Kurze Vorstellung
- Was ist VPN?
- OpenVPN / OpenVPN im UCS
- Designentscheidungen
- Funktionsumfang Version 1.x
- Topologien / Screenshots
- Preismodell / Dokumentation
- Ausblick auf die Entwicklung

# bytemine GmbH - Kurze Vorstellung

- Linux- / Unix-Dienstleister mit Sitz in Oldenburg
- seit 2003 am Markt
- Entwicklungsmanufaktur für innovative Lösungen
- sichere, verfügbare Infrastrukturen
- 2nd und 3rd Level Support
- Housing & Hosting
- Sicherheit und Kryptographie
- Open Source Lösungen



# Was ist VPN?

- Virtuelles privates Netzwerk
- Ziel: Wahrung von Vertraulichkeit, Integrität, Echtheit
- **Anbindung mobiler Anwender**
  - Sicherung zwischen Client und Server
  - Zusätzlicher Schutz bei Funkverbindungen
- **Standortvernetzung**
  - Anbindung einer Aussenstelle
  - Anbindung verschiedener Gebäudeteile

# OpenVPN

- Werkzeug zur Erstellung eines virtuellen privaten Netzwerks
- Nutzung von SSL/TLS
- Port 443 oft verfügbar
- Funktioniert auch in Proxy-Umgebungen
- Auf allen relevanten Plattformen verfügbar
- Flexibilität ist ideal für Anbindung mobiler Anwender
- Standortvernetzung möglich

# OpenVPN im UCS

- Zentrales Identity-Management am UCS
- Nahtlose Integration der Anwender
- Kein zusätzliches Kennwort nötig
  
- Geringer administrativer Aufwand
- Verwendung der Zertifikatskette vom UCS
- Einsatz vertrauter UI Elemente

# Designaspekte

- Ein Klick (!) zur Erzeugung benötigter Client-Komponenten
- Bedienung über Univention Management Console / Overview
- Keine Kommandozeile erforderlich
- Keep it simple [and] stupid.



# Funktionsumfang Version 1.0

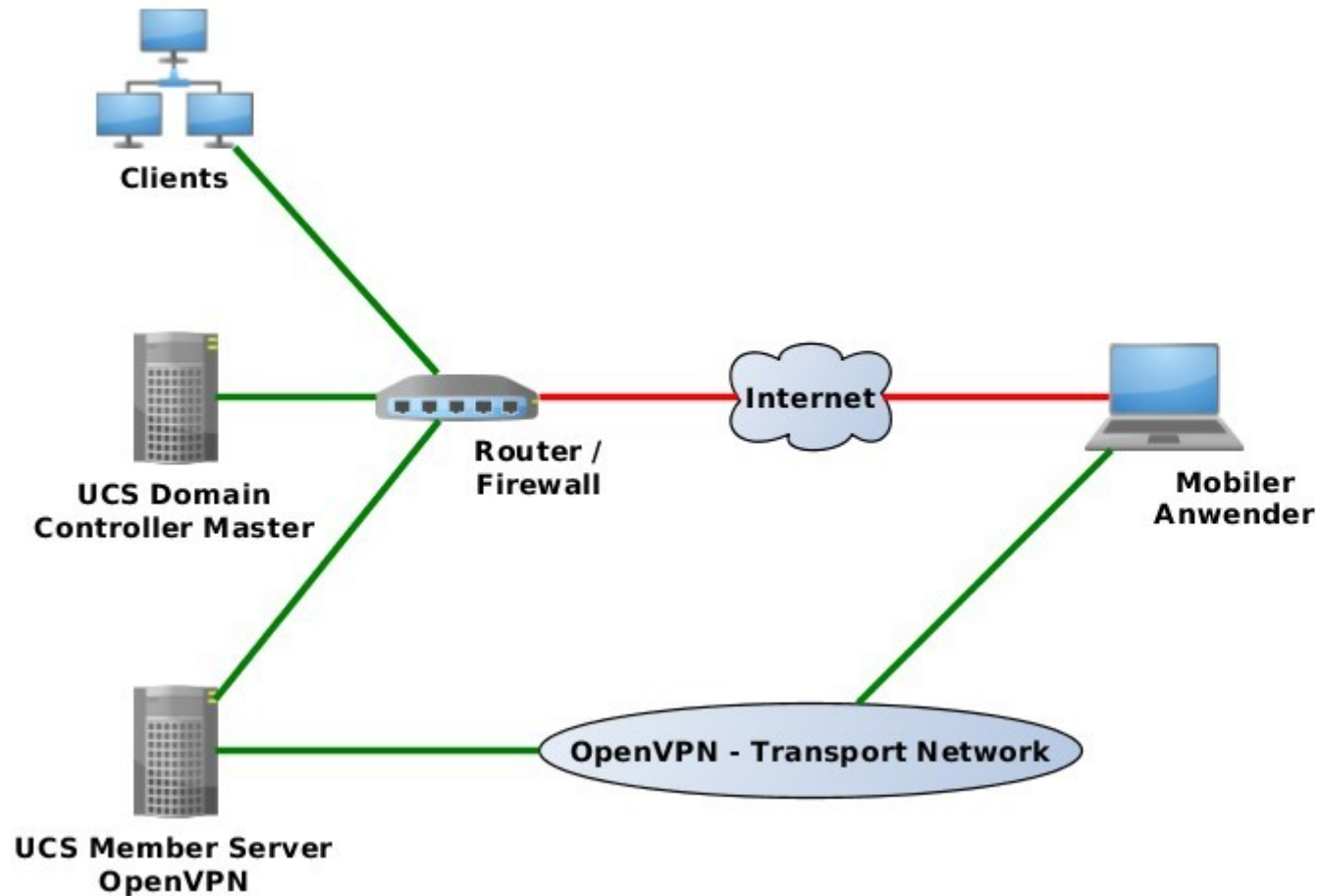
- OpenVPN Zugänge mit nur einem Klick erzeugen
- 'ready2go' Paket mit vollständiger Benutzerkonfiguration
- Dynamische Re-Generierung des 'ready2go' Pakets bei Serveränderungen
- Unterstützung für Linux- und Windows-Clients out-of-the-box
- Verbindungsübersicht verbundener Benutzer
- Site-to-Site Standortvernetzung (Business Edition)
- IPv4 und IPv6 Unterstützung

# Funktionsumfang Version 1.0.5

- Integration mit privacyIDEA
  - Integration mittels des privacyIDEA PAM Moduls
- Verschiedene Sicherheitsaspekte wurden verbessert
  - Bessere / sinnigere Permissions auf dem FS
  - Ready2go Pakete werden sauber entfernt bei Sperrung
- Verbindungsübersicht wurde erweitert

# Topologie – Benutzer VPN

OpenVPN4UCS - Benutzer VPN - Topologie (vereinfacht)



# UMC – Server / Benutzer-VPN

Computers: ucs-8906



## OpenVPN4UCS



OpenVPN4UCS license key (required to activate commercial features)




## User VPN

OpenVPN server active

**10.74.153.233**

(\* required) OpenVPN server address

**443**

(\* required) OpenVPN port

**172.16.16.0**

(\* required) OpenVPN transfer network IPv4 (default: /24)

OpenVPN transfer network IPv6

OpenVPN redirect gateway

OpenVPN duplicate

OpenVPN dual-factor authentication

OpenVPN fixed addresses

In order to use dual-factor authentication with privacyIDEA, this option has to be enabled.

OpenVPN user

IP address

+ New entry

# UMC – Benutzer

The screenshot shows the Univention Management Console (UMC) interface in a Chromium browser. The address bar shows the URL `https://10.1.2.15/univention-management-console/`. The page title is "Univention Manager". The user is logged in as "Administrator" on the domain `ucs-master.vpntesting.intranet`. The main content area is titled "Users: user0001".

On the left side, there is a navigation menu with the following items:

- General
- Groups
- Account
- Contact
- [Advanced settings]** (highlighted)
- [Options]
- [Policies]

Below the navigation menu, the "Advanced settings" section is expanded, showing:

- Type: *User*
- Position: *intranet.vpntesting/users*

On the right side, there are several expandable sections:

- Mail** (expanded)
- UMC preferences** (expanded)
- Windows terminal server** (expanded)
- OpenVPN4UCS** (expanded)


Under the "OpenVPN4UCS" section, there is a checked checkbox labeled "OpenVPN account".


# ready2go Download

OpenVPN4UCS | Download ready2go packages - Chromium

OpenVPN4UCS | Do x


https://10.1.2.15/download/

 OpenVPN4UCS

 Call us  
**+49 441.309197-69**

Download ready2go packages

Username:

 Contact

bytemine GmbH  
Im Technologiepark 4  
26129 Oldenburg

+49 441.309197-69  
info@bytemine.net

Imprint © by bytemine




# Verbindungsübersicht

OpenVPN4UCS | Connected Users - Chromium

OpenVPN4UCS | Co x

https://10.1.2.15/display\_users/



Call us  
+49 441.309197-69

### Connected users

Name	Connected	Type	Real Address	Virtual Addresses	Connected since	Connected for	Received	Sent	Disconnect
user0001.openvpn		v4 v6					0	0	
user0002.openvpn		v4 v6					0	0	
user0003.openvpn		v4 v6					0	0	
user0004.openvpn		v4 v6					0	0	
user0005.openvpn		v4 v6	10.1.2.14:36268	10.2.3.2	Thu Mar 12 18:25:05 2015	0:00:30	7687	10582	Disconnect
user0006.openvpn		v4 v6					0	0	
user0007.openvpn		v4 v6					0	0	

Contact

bytemine GmbH  
Im Technologiepark 4  
26129 Oldenburg

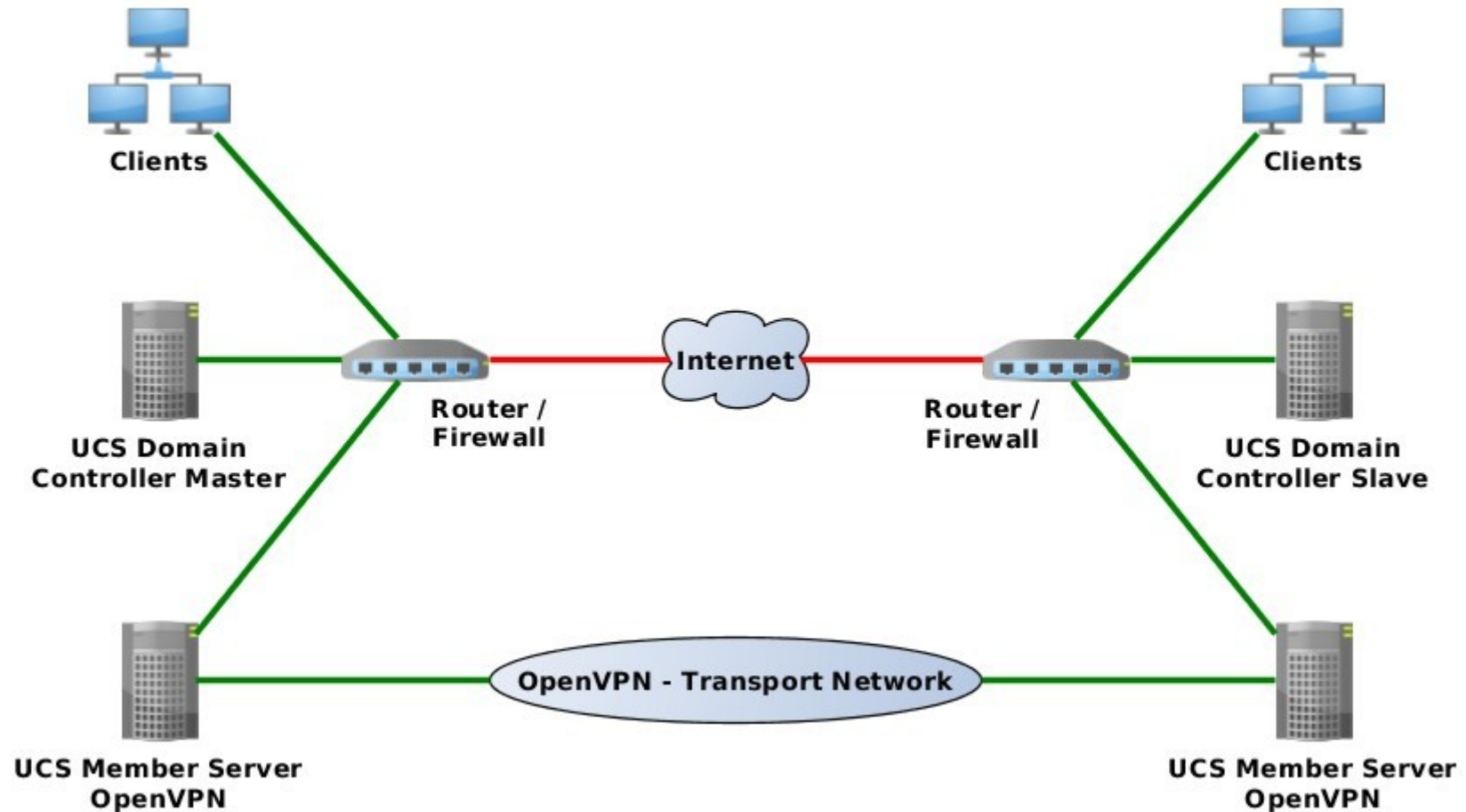
+49 441.309197-69  
info@bytemine.net

Imprint © by bytemine



# Topologie – Site-to-Site

OpenVPN4UCS - Site-to-Site VPN - Topologie (vereinfacht)





# UMC – Server / Site-to-Site

Univention Management Console - Chromium

Univention Manager x

https://10.1.2.15/univention-management-console/

Computers: ucs-master

OpenVPN transfer network IPv6

OpenVPN redirect gateway

OpenVPN duplicate

OpenVPN fixed addresses

OpenVPN user  IP address

+ New entry

---

Site-to-Site VPN

OpenVPN site-to-site active.

OpenVPN remote address

OpenVPN site-to-site port

OpenVPN internal local address

OpenVPN fixed IP address

Defines the fixed IP for the remote endpoint, which is only used inside the virtual transfer network.

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
4901e64b50953ec8f16388182746b7a0
fc9e723280e6fa1ddf8ecf1b4a794490
64e6980d7a6453ea693445403758097d
```

UVMM

# Preismodell / Dokumentation

Editionen / Features	Personal Use	Business	Personal Plus
Benutzer VPN	Ja	Ja	Ja
Standortvernetzung	Nein	Ja	Ja
Installationsupport	Nein	30 Tage per E-Mail	Nein
Benutzer - Basis / Max	5 / 5	10 / xxx	10 / 10
Preis Basis	n/a	150,- EUR / Jahr	60,- EUR / Jahr
Weitere 5 Benutzer	n/a	40,- EUR / Jahr	n/a
Kommentar	Entspricht Installation	Für Geschäftsumfeld	Für Privatanwender

- Web: <http://www.bytemine.net/de/leistungen/openvpn4ucs.html>

# Ausblick auf die Entwicklung (Ideen)

- ~~Integration mit PrivacyIDEA (OTP) auf UCS~~
- Ausbau verfügbarer Informationen in der UMC / Webseite
- Einbindung von Nicht-UCS Konzentratoren (Bedarf?)
- Mehrfach Site-to-Site Setups (Bedarf?)
- <IHR\_INPUT>

# Tadaaaa

- BSD Licensed!
- <https://github.com/bytemine/openvpn4ucs>

# Raum für Fragen

- Haben Sie Fragen?
- Feedback ist willkommen!

# Vielen Dank für die Aufmerksamkeit!

bytemine GmbH

Im Technologiepark 4  
26129 Oldenburg

info@bytemine.net  
www.bytemine.net

+49-441-309197-69

