OpenVPN4UCS mit privacyIDEA

VPN wie es einfacher und sicherer kaum sein kann

Felix Kronlage

CFA – kronlage@bytemine.net

bytemine

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

bytemine

Entwicklungsmanufaktur für innovative 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.

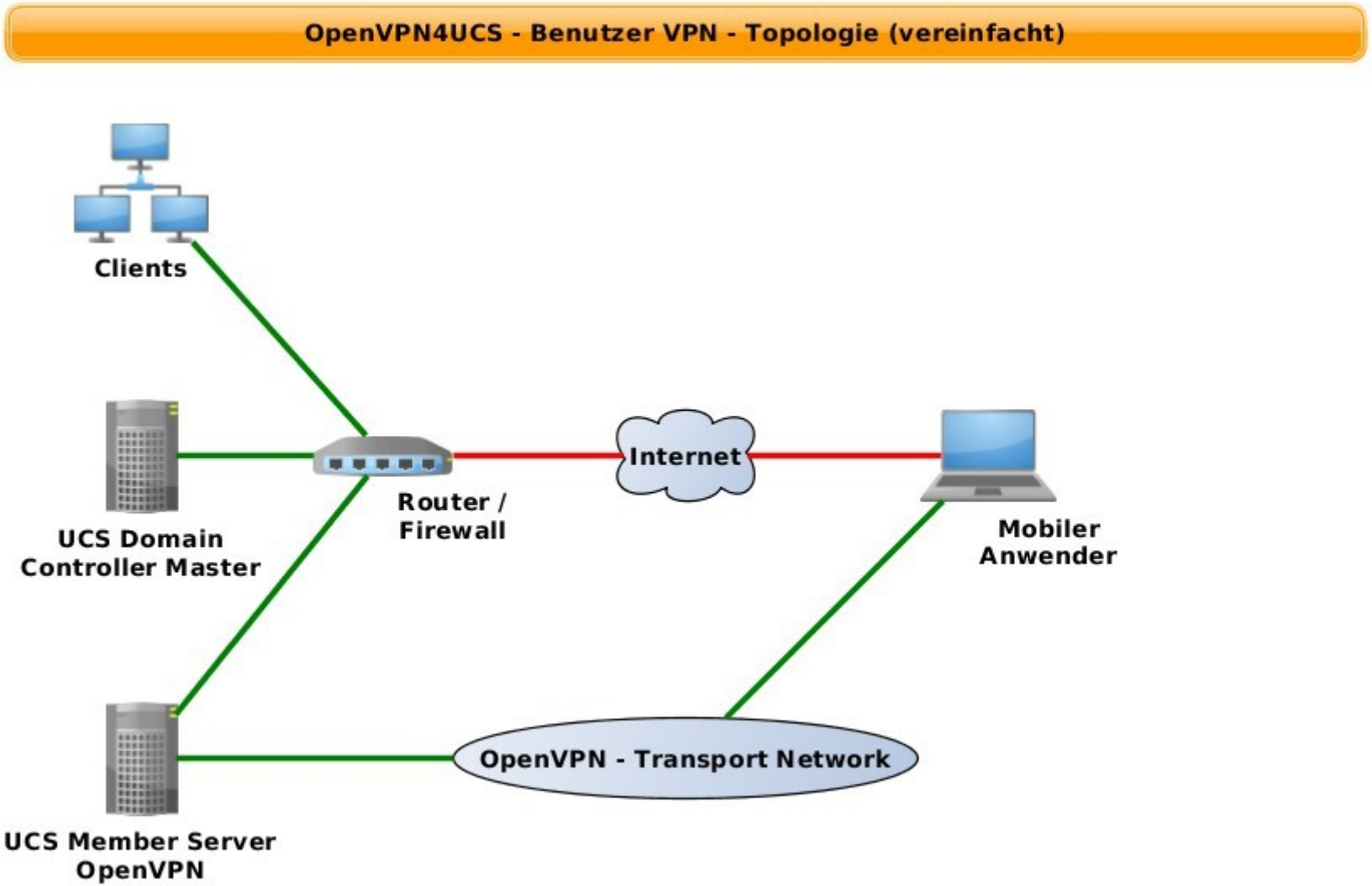
Funktionsumfang Version 1.0

- 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

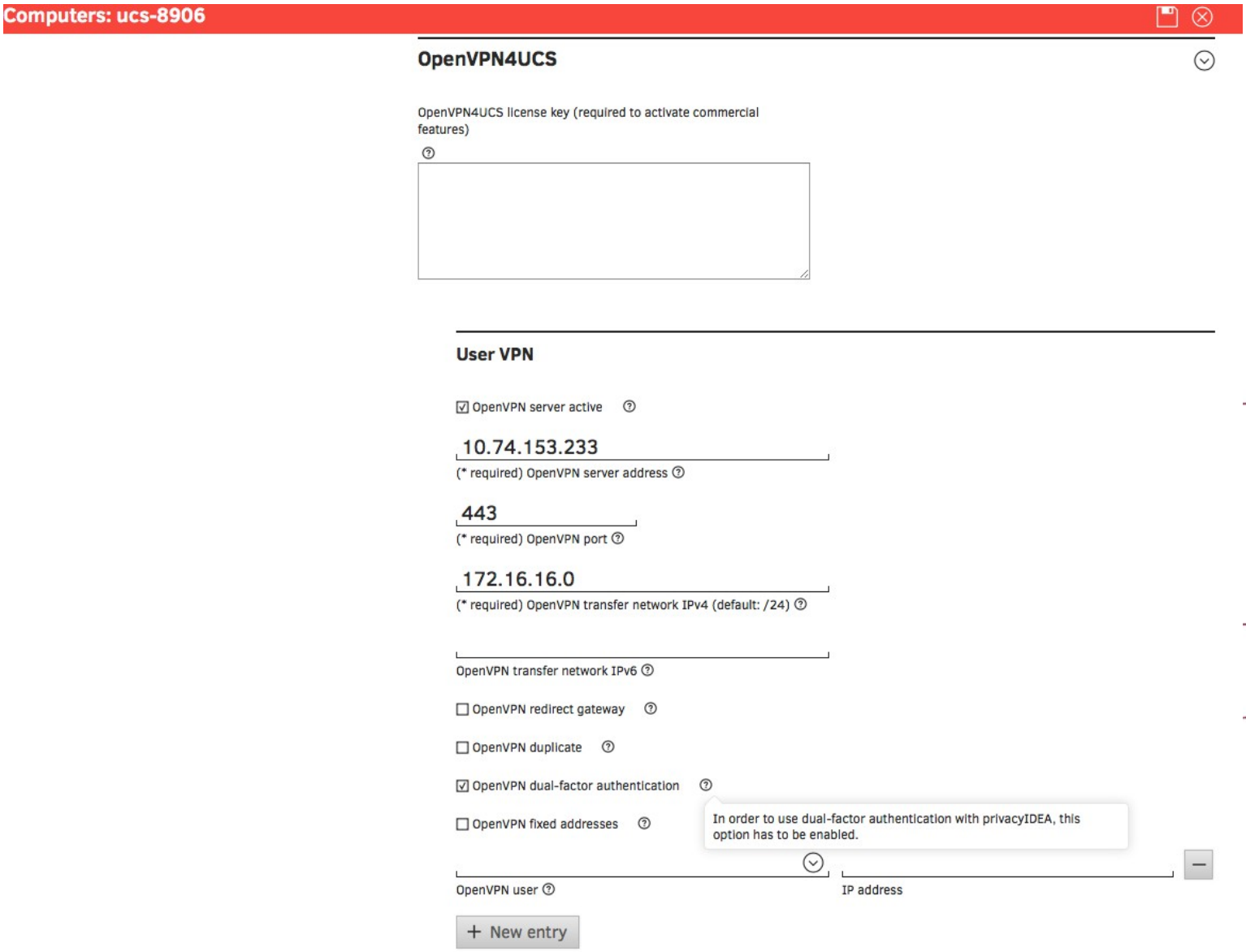
Funktionsumfang Version 1.0.5

- 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

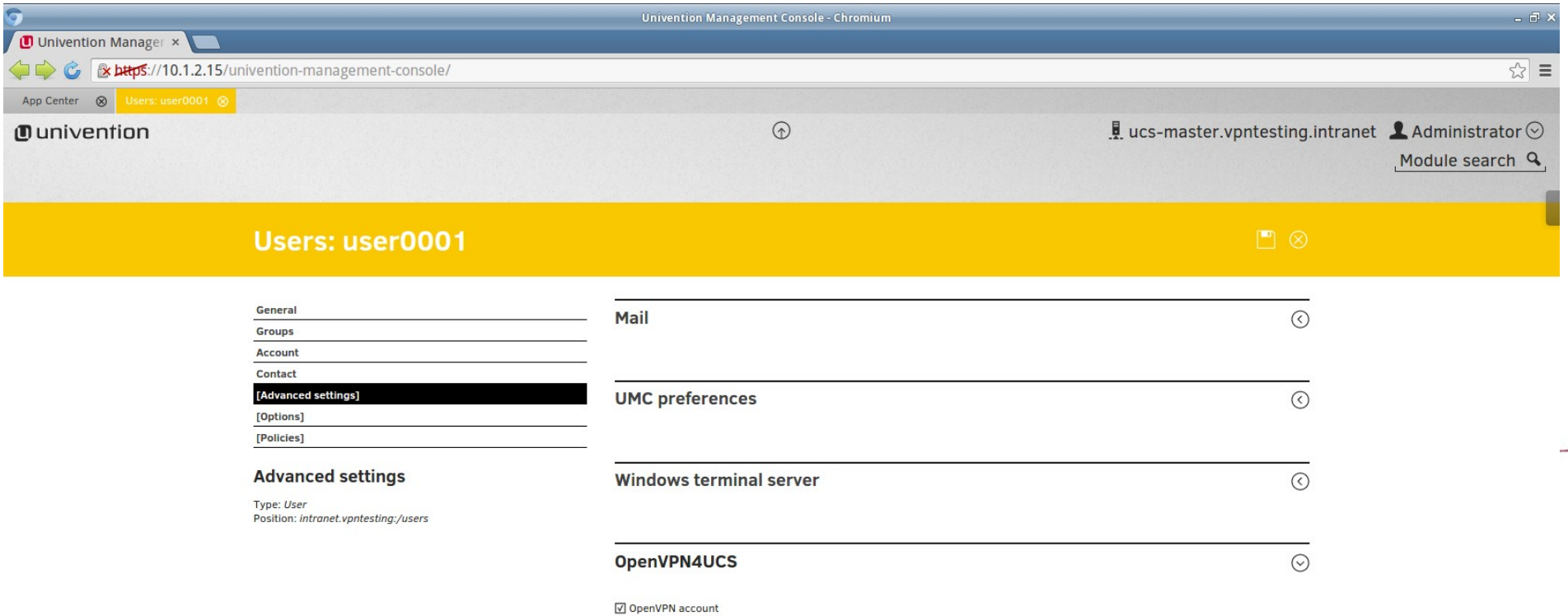
Topologie – Benutzer VPN



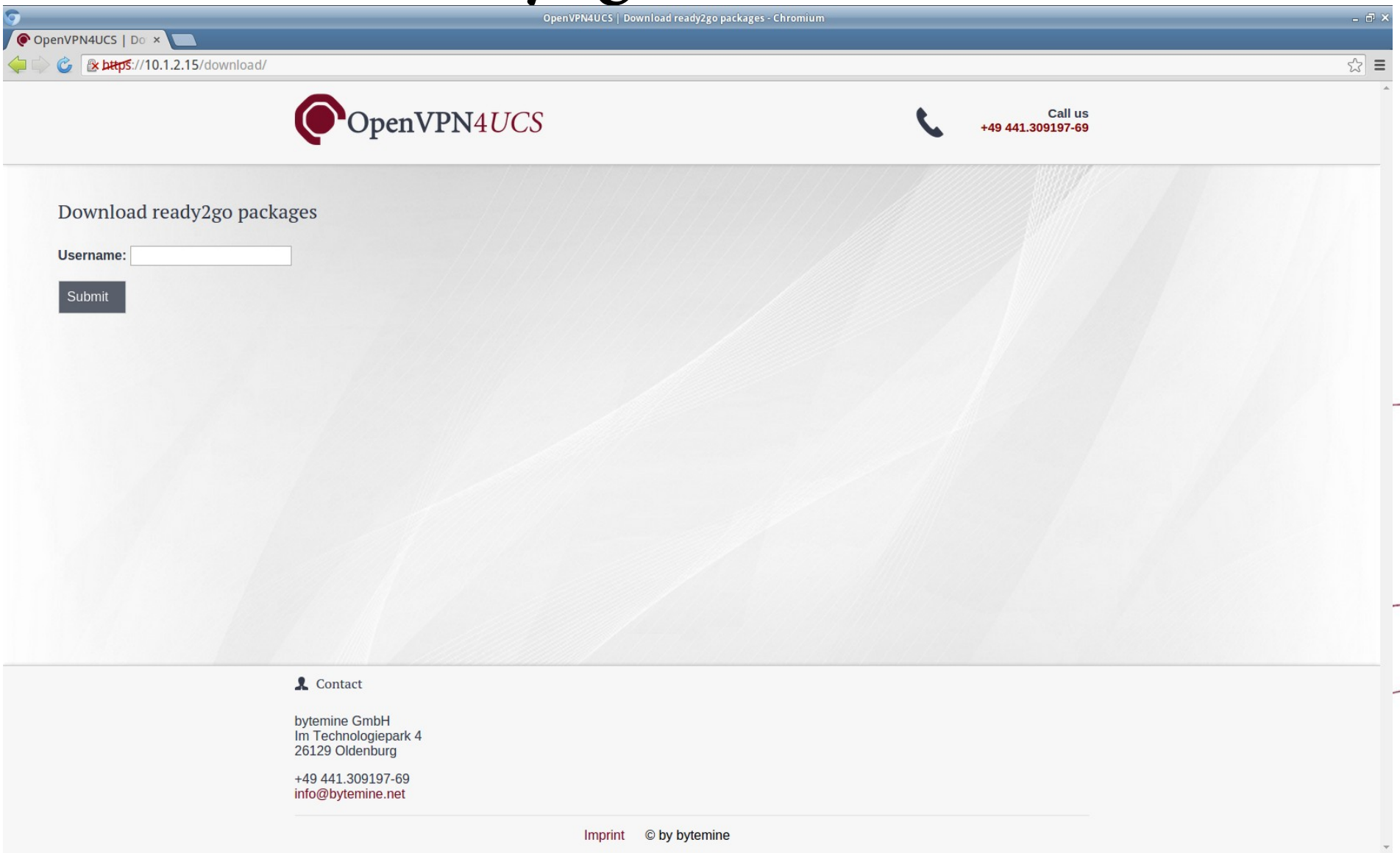
UMC – Server / Benutzer-VPN



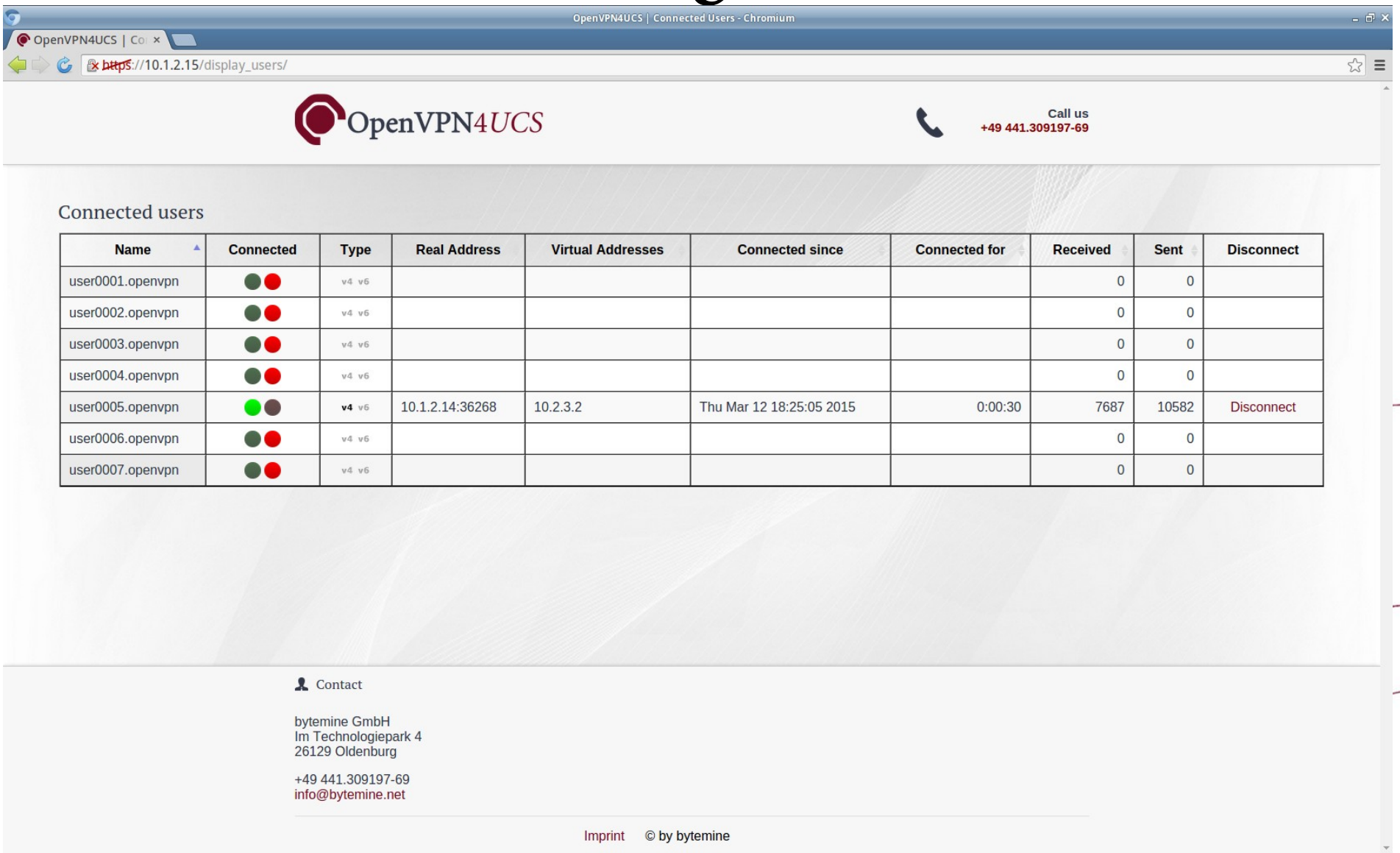
UMC – Benutzer



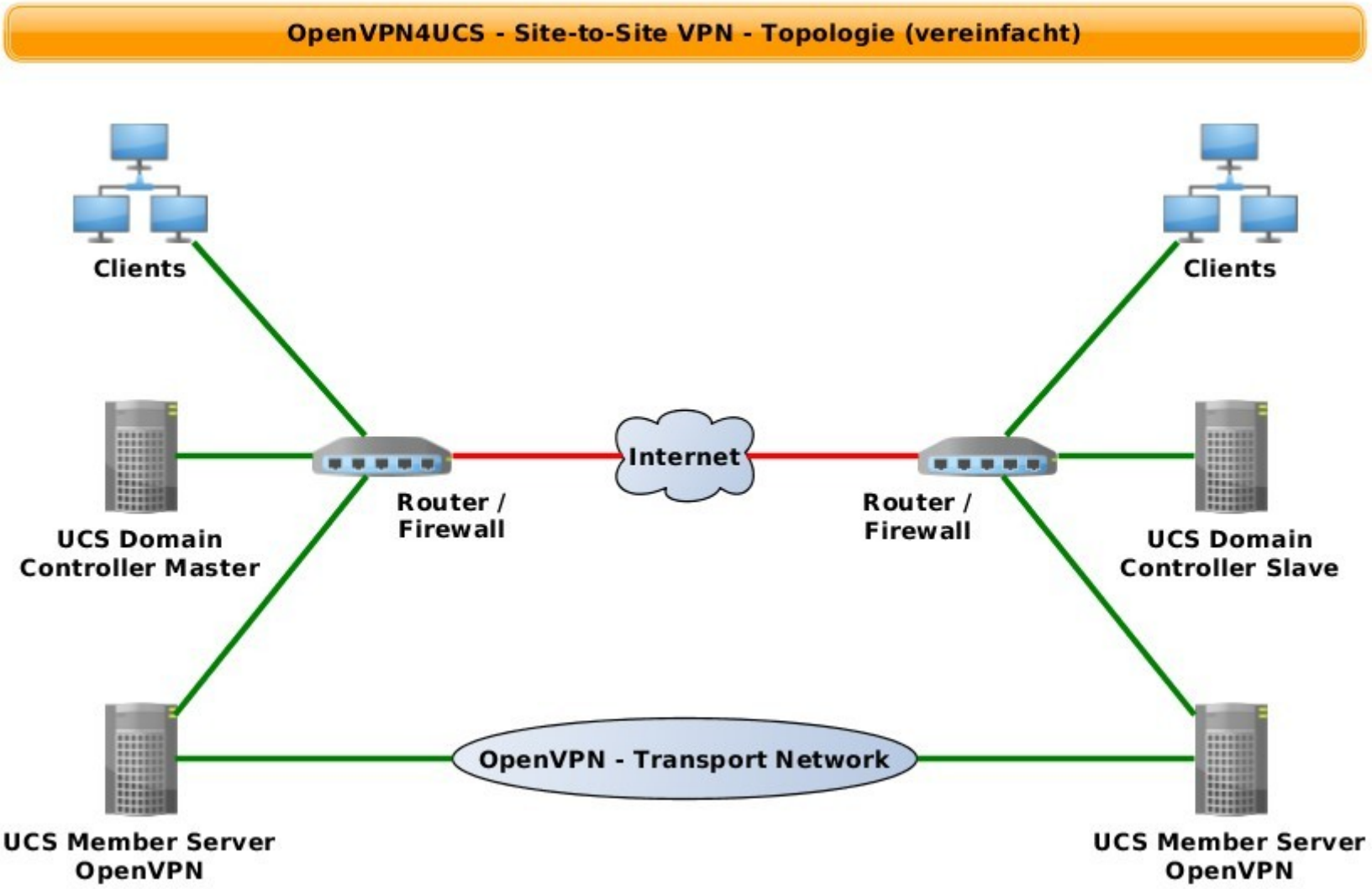
ready2go Download



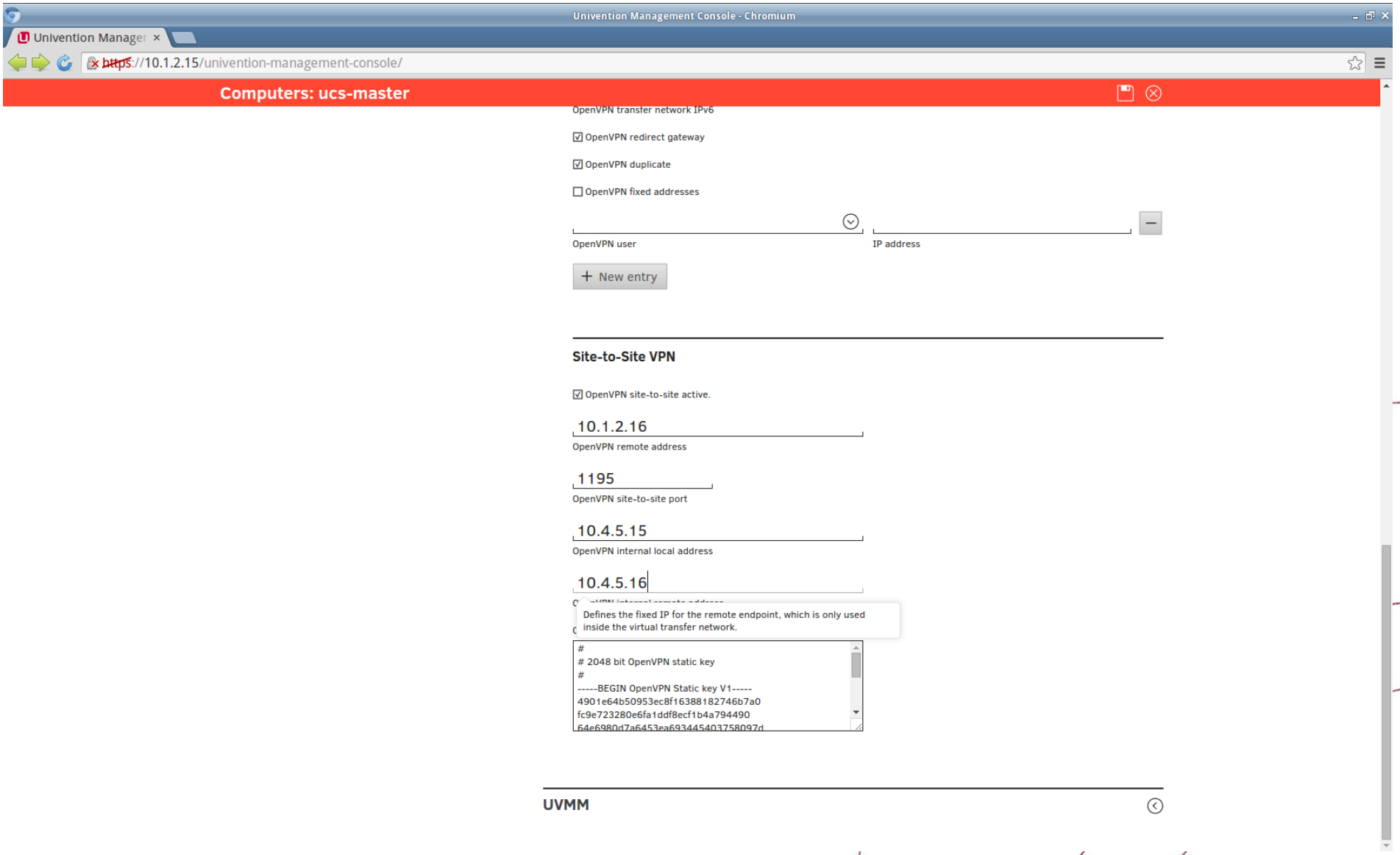
Verbindungsübersicht



Topologie – Site-to-Site



UMC – Server / Site-to-Site



Preismodell / Dokumentation

Editionen / Features	Personal Use	Business	Personal Plus
Benutzer VPN	Ja	Ja	Ja
Standortvernetzung	Nein	Ja	Ja
Installationssupport	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