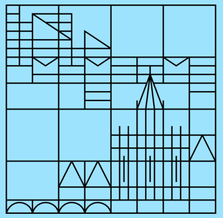
eduVPN

Auswahl, Funktionsprinzip,
Umstellung, Betriebserfahrung

Universität
Konstanz



Eduvpn

Universität Konstanz

Eduvpn

- OpenSource
- Problemlose Client-Updates via AppStores
- unterstützt WireGuard (Performance-Vorteil)
- OpenVPN (legacy)
- direkte IDM-Anbindung (Shibboleth) (neben LDAP, Radius, Lokal)
- einfache Integrationsmöglichkeit für 2FA
- User-ID Unterstützung möglich
- Wireguard über TCP
- Liste von Einrichtungen im Client (keine Serveradressen nötig)
- Manuelle WireGuard und OVPN Configs möglich
- Laufzeit der Configs einstellbar
- Berechtigung auf IDM-Attributen

Secure Internet

- Sicherer Internetzugang (Hotel, Ausland…)
- Wird vom DFN betrieben
- Anmeldung beim DFN nötig, alle Hochschulen sind bereits durch Shibboleth Föderation Sichtbar
- Verwechslungsgefahr (Support!!)

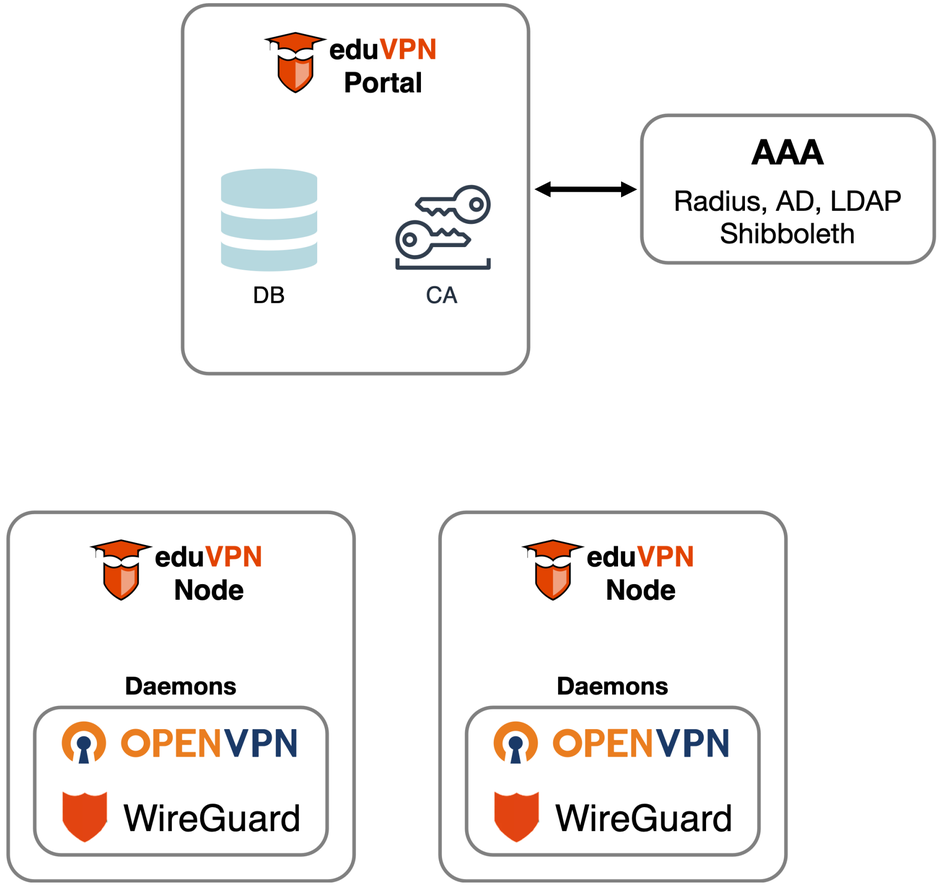
Let‘s Connect

- Core von EduVPN
- Ohne EduVPN Brandig
- Für Unternehmen

eduVPN

Funktionsprinzip

Universität Konstanz

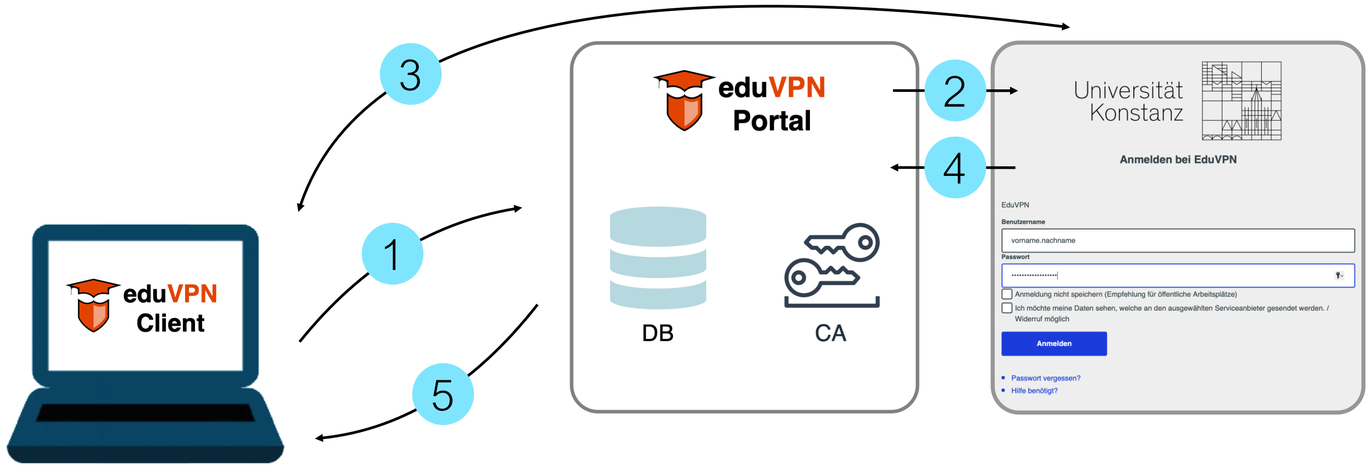


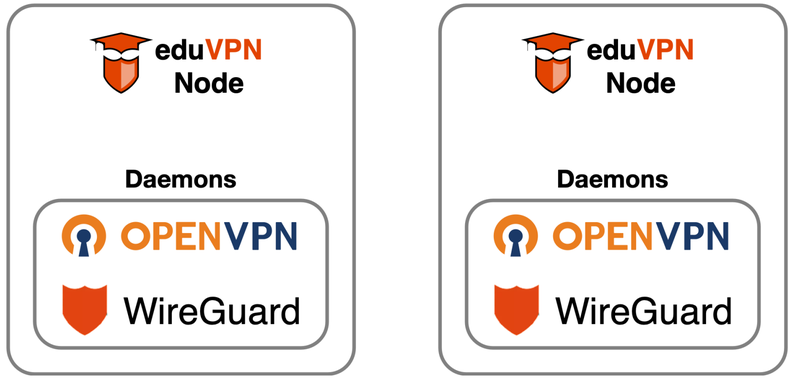
- eduVPN Portal/Controller
  - Datenbank
  - CA
  - Profile
- eduVPN Nodes
  - OpenVPN Daemon
  - WireGuard Daemon

eduVPN

Funktionsprinzip

Universität Konstanz



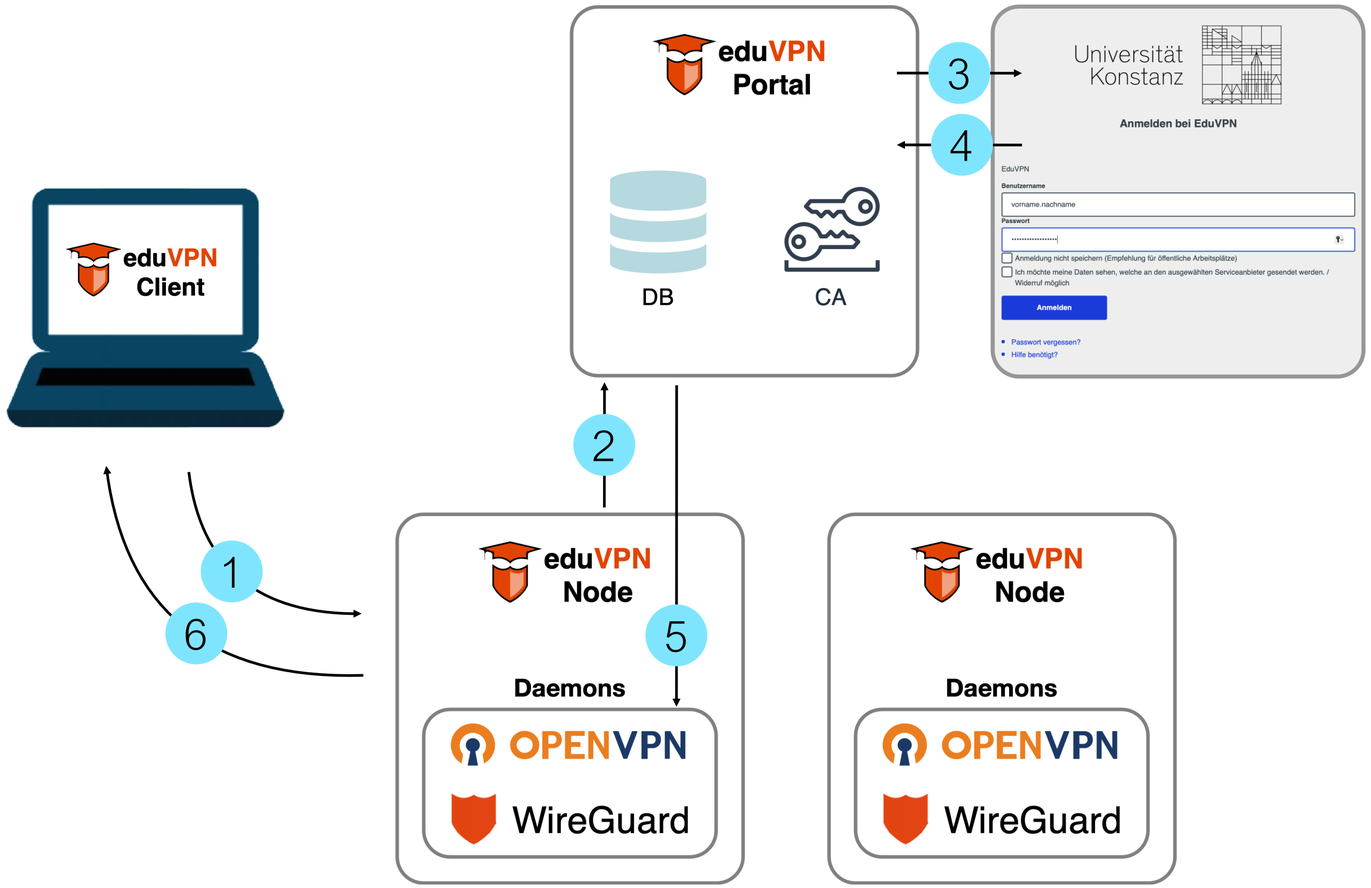


- Setup:
  - Client verbindet sich zum Portal und fragt nach einem Profil
  - Portal leitet die Anfrage per Shibboleth an IDM weiter
  - Der User authentisiert den Client über die Shibboleth-Seite
  - Das Portal erzeugt ein KeyPair/Zertifikat und übermittelt das mit dem angefragten Profil zum Client

eduVPN

Funktionsprinzip

Universität Konstanz



- Verbindung:
  - Client verbindet sich zum im Profil angegebenen Node
  - Node fragt beim Portal, ob der Key gültig ist
  - Das Portal fragt beim IDM, ob der User noch existiert (oder gesperrt ist)
  - Der Node übermittelt die Antwort vom Portal an den jeweiligen Daemon, der die Verbindung akzeptiert

RAS-VPN-Zugang (bisher)

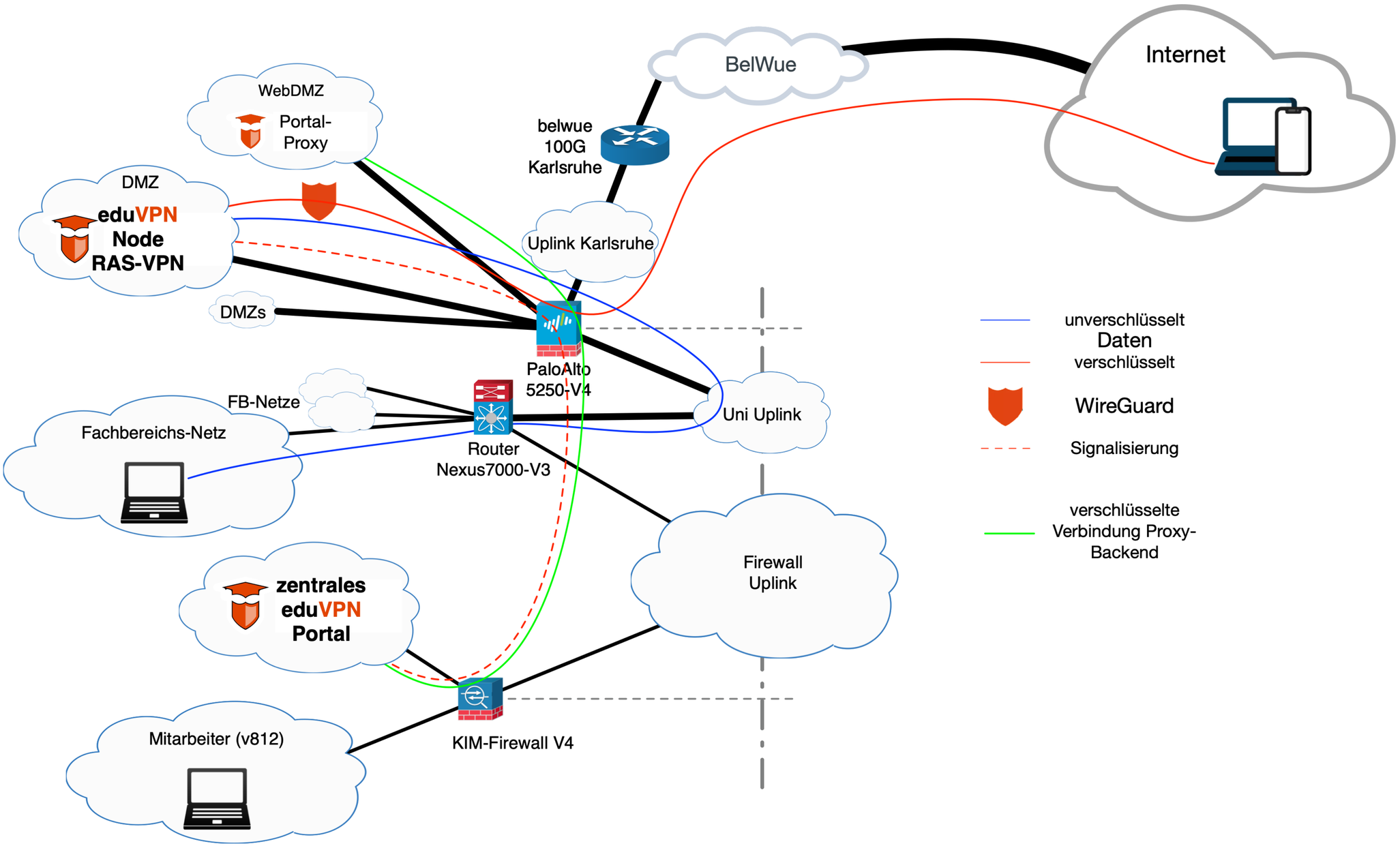
Universität Konstanz

- Cisco AnyConnect
- Authentisierung & Autorisierung über Radius

RAS-VPN-Zugang (neu)

Universität Konstanz

- ~~Cisco AnyConnect~~ -> eduVPN
- ~~Authentisierung & Authorisierung über Radius~~ -> Shibboleth


BelWue
Internet
WebDMZ
Portal-
Proxy
belwue
100G
Karlsruhe
DMZ
eduVPN
Node
RAS-VPN
Uplink Karlsruhe
DMZs
PaloAlto
5250-V4
FB-Netze
Fachbereichs-Netz
Router
Nexus7000-V3
Uni Uplink
Firewall
Uplink
zentrales
eduVPN
Portal
KIM-Firewall V4
Mitarbeiter (v812)
unverschlüsselt
Daten
verschlüsselt
WireGuard
Signalisierung
verschlüsselte
Verbindung Proxy-
Backend

VPN4-Zugang (RZ-Firewall)

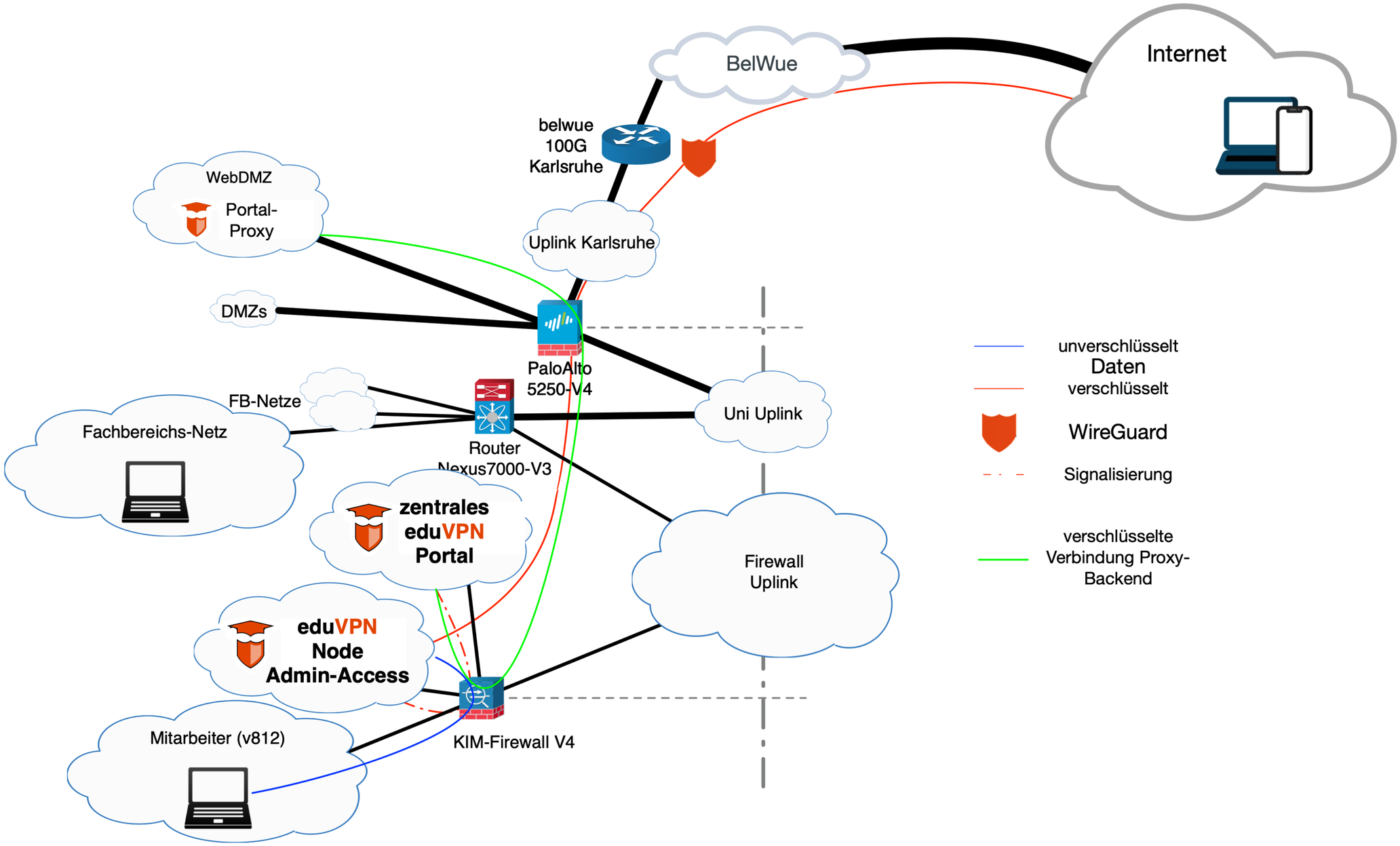
Universität Konstanz

- Cisco AnyConnect
- VPN-User lokal auf der Firewall angelegt
- ACLs mit User-ID statt IP-Adresse (auf der RZ-FW)
- VPN-Server = Firewall = Subnetz-Gateway

VPN4-Zugang (ab 16.3.)

Universität Konstanz

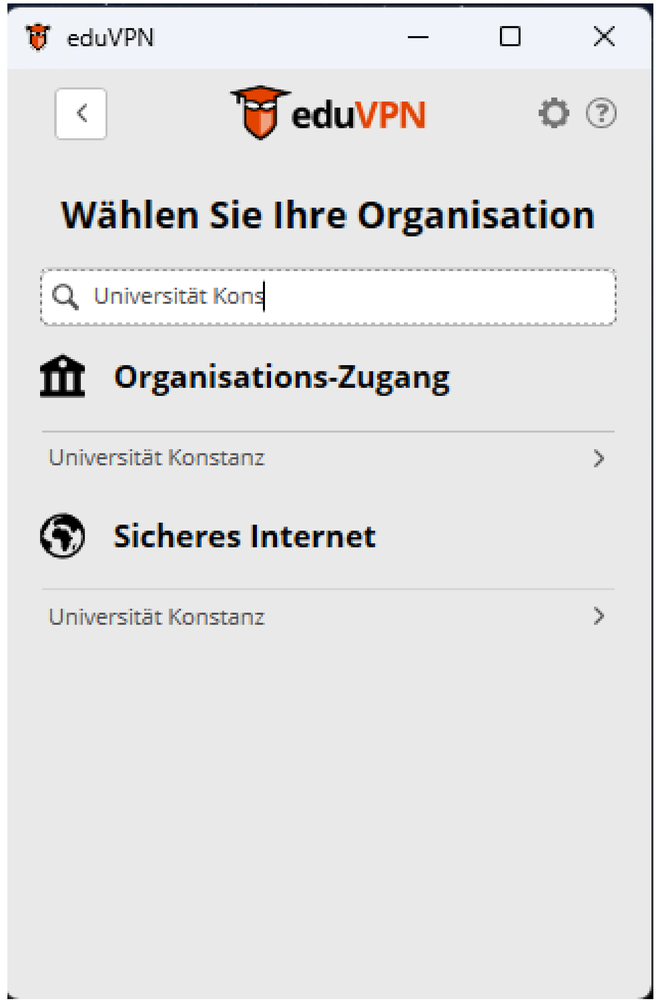
- ~~Cisco AnyConnect~~ -> eduVPN
- ~~VPN-User lokal auf der Firewall angelegt~~ -> IDM
- ACLs mit User-ID statt IP-Adresse ~~(auf der RZ-FW)~~ -> (später) auf allen Palo-FW
- ~~VPN-Server = Firewall = Subnetz-Gateway~~ -> dedizierter VPN-Server **an** der FW


BelWue
Internet
belwue
100G
Karlsruhe
WebDMZ
Portal-
Proxy
Uplink Karlsruhe
DMZs
PaloAlto
5250-V4
FB-Netze
Fachbereichs-Netz
Router
Nexus7000-V3
Uni Uplink
zentrales
eduVPN
Portal
Firewall
Uplink
eduVPN
Node
Admin-Access
Mitarbeiter (v812)
KIM-Firewall V4
unverschlüsselt
Daten
verschlüsselt
WireGuard
Signalisierung
verschlüsselte
Verbindung Proxy-
Backend

Erfahrungen

Universität Konstanz

- Supportaufwand deutlich zurückgegangen im Vergleich zu Anyconnect
- Sehr gute Dokumentation, Support und Kontakt zum Entwickler, Mailingliste, Bugtracker
- Neue Features ProxyGuard (WG über TCP), Profile als JSON
- Intuitive Bedienung, verwechselung von Institution und Secure Internet problematisch
- kein Stateful Failover
- keine Binaries des Clients außerhalb der AppStores erhältlich (China!)
- keine Banner-Meldung im Client
- keine 'Start before Logon' (SBL) (Anmeldungsmöglichkeit an AD per VPN für verwaltete Windows-Geräte)



EduVPN Client

UNIVERSITÄT KONSTANZ

Vielen Dank!

Maximilian Ortwein, M.Sc.

Netzwerkarchitekt

KIM · Forschung Lehre Infrastruktur · Netz- und Sprachdienste

Universität Konstanz