eduVPN bei der GWDG

Überblick zu eduVPN und Setup bei der GWDG

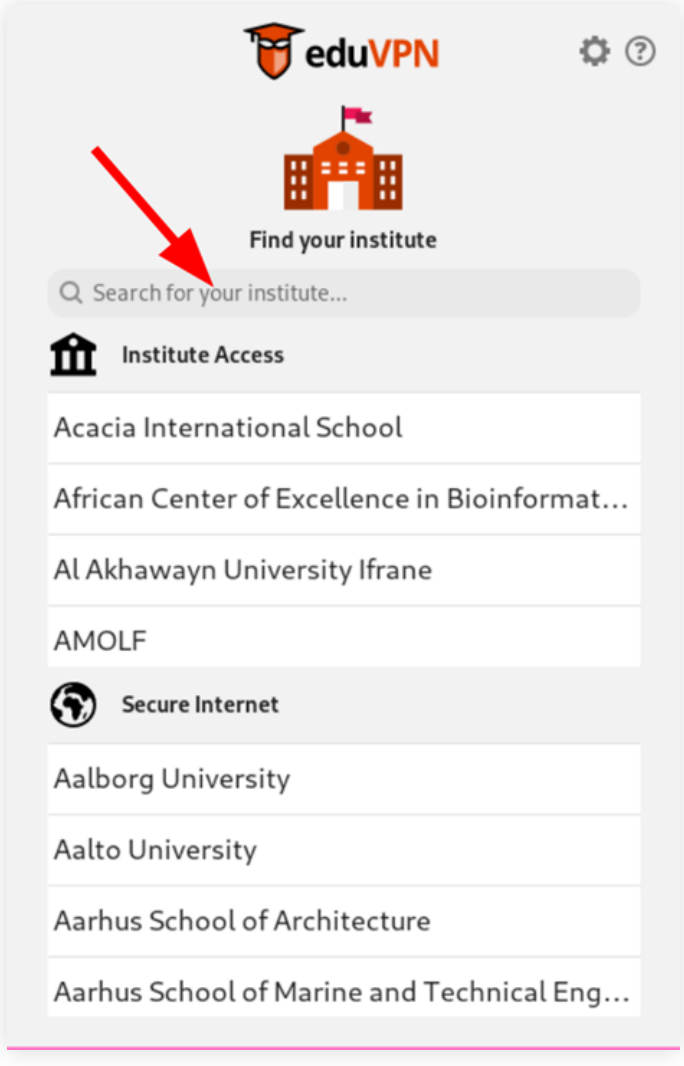
Was ist die GWDG?

- Gesellschaft für Wissenschaftliche Datenverarbeitung Göttingen mbH
- Hochschul-RZ der Uni Göttingen
- Cloud-Provider, Hosting und Housing der Max-Planck-Gesellschaft
- Cloud-Provider generell für Bildung und Forschung (Academiccloud)

Was ist eduVPN?

- OpenSource Projekt von GÉANT
- Ursprünglich von SURF entwickelt
- Server-Software läuft unter Linux
- Clients für alle gängigen Betriebssysteme
    - Windows, macOS, Linux
    - iOS, Android
- Authentifizierung im Webbrowser
- VPN Verbindungen mit WireGuard oder OpenVPN

Institutszugriff und Secure Internet



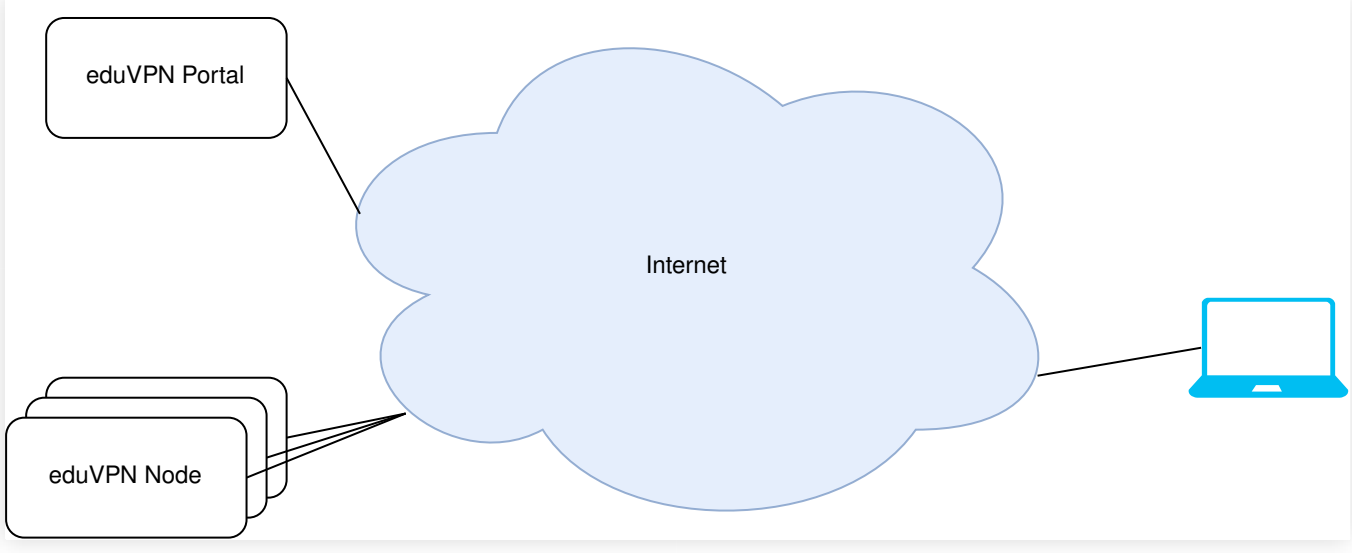
Secure Internet

- VPN-Zugänge mit Authentifizierung durch eduGAIN/DFN-AAI
- VPN-Gateways bei diversen NRENs, unter anderem dem DFN
- Verschlüsselte Tunnel in Forschungsnetze
- Umgehen von regionalen Zugriffsbeschränkungen
- Heute **nicht** im Fokus der Vorträge

Institute Access

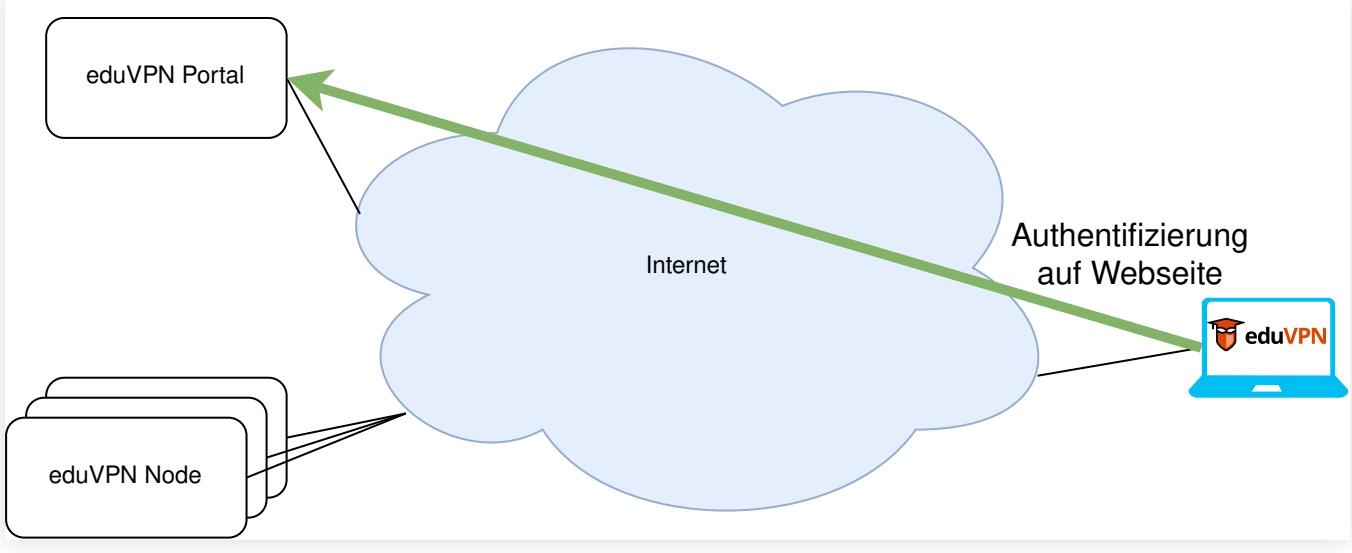
- VPN-Gateway im Institut, (On-Premise)
- Eigene Authentifizierungsmechanismen
    - LDAP
    - RADIUS
    - OIDC
    - SAML

Verbindungsaufbau



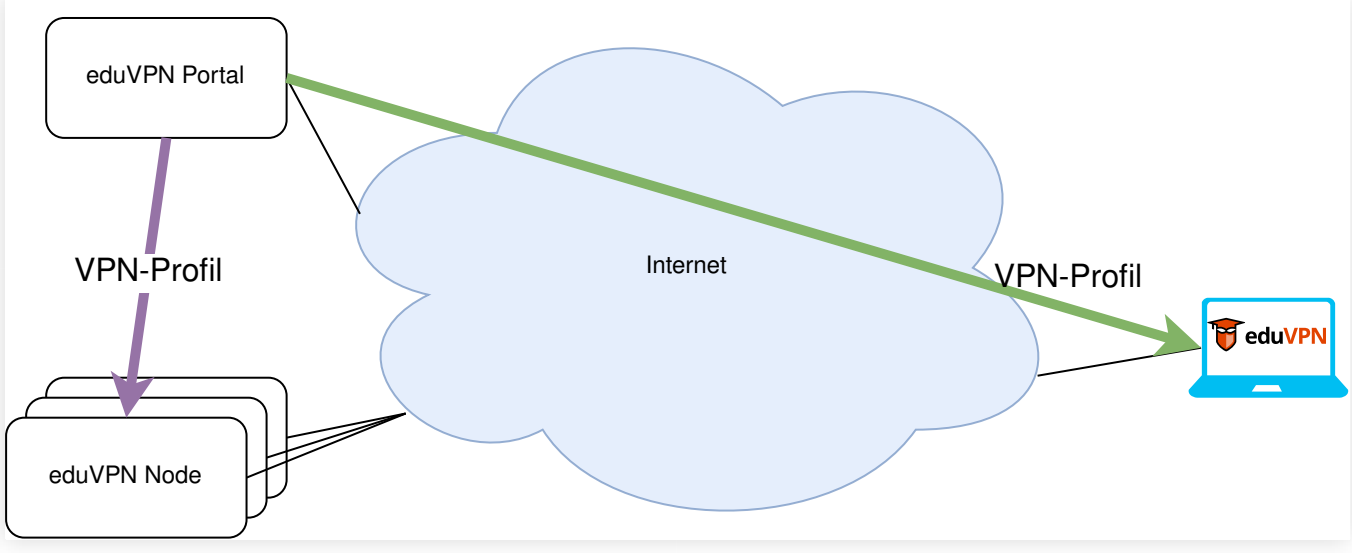
eduVPN Portal Node und Client

Verbindungsaufbau



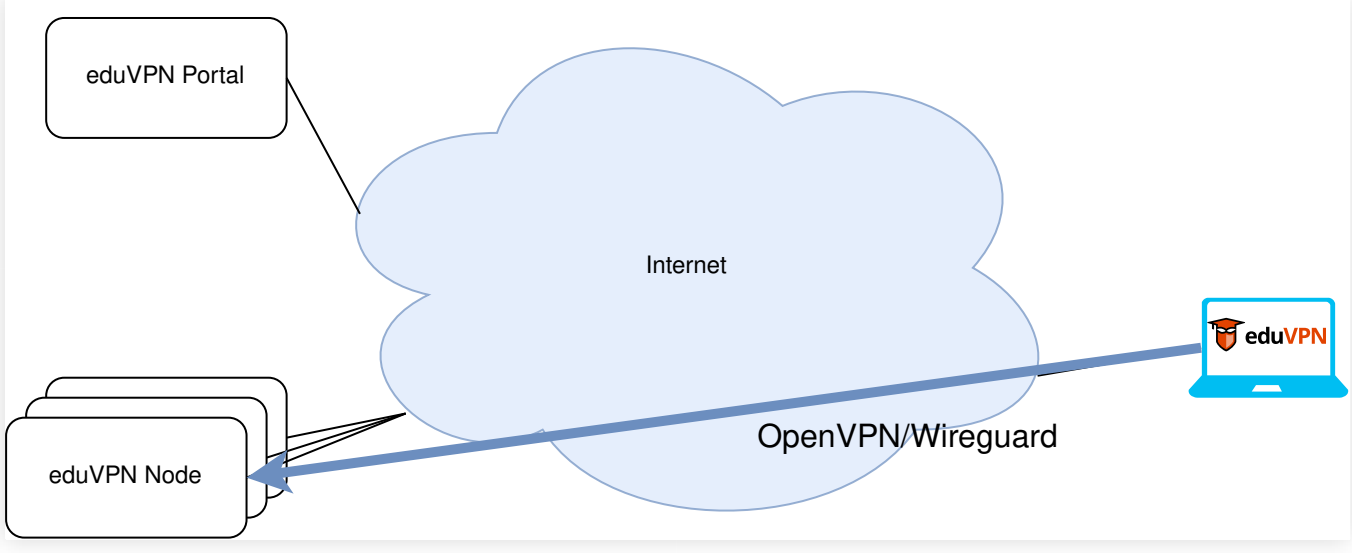
Authentifizierung durch Nutzer*in im Browser

Verbindungsaufbau



Ausliefern des VPN-Profils an Client und Node(s)

Verbindungsaufbau



Aufbau der Wireguard- oder OpenVPN-Verbindung

eduVPN bei der GWDG

Anforderungen

- Skalierbarkeit:
  - ~5000 gleichzeitige Verbindungen
  - ~500 Profile
- Sicherheit:
  - Tägliche interaktive Nutzerauthentifizierung
  - Keine Authentifizierung ohne 2.Faktor
  - Erfahrungen:
    - Bisher häufige brute-force Angriffe VPN-Gateways
    - Passwörter aus z.B. Phishing
- Verfügbarkeit:
  - Redundante VPN Endpunkte
  - VPN auch aus eingeschränkten Netzen

Entscheidungen

- Anmeldung mit SSO (OIDC)
- Kurze Laufzeit der VPN-Konfigurationen (16h)
    - immer Abfrage des 2. Faktors
- Portal und Node auf eigene Server
- Redundante VPN-Nodes
    - Failover über BGP
- Portal nicht redundant
- Langfristig nur Wireguard
- Konfigurationsmanagement mit Ansible und IPAM
    - Automatisches anlegen neuer Profile
- Kein NAT auf VPN-Gateways

Details zum Setup

Redundanz

- Zwei Nodes die Service IP und VPN-Netze per BGP announcen
  - Längerer AS-Pfad auf einem der Nodes
  - BIRD als BGP-Daemon
- Identisches Deployment auf mehrere Nodes nicht vorgesehen
  - Doppelter Aufruf des Deployment-Scriptes
  - Umbiegen des Zielhosts per unshare und bind-mount der `/etc/hosts`
- Synchronisieren der offenen Verbindungen (TBD)
  - `contrackd`

Plattform

- Nodes:
  - VMs auf Proxmox Hosts
  - 20G Uplink
  - 4 CPU-Kerne, 8GB RAM
  - Debian 12
- Portal:
  - VM im ESX-Cluster (Standortredundant)
  - 4 CPU-Kerne, 8GB RAM
  - Debian 12

Management

- Setup mit Ansible
    - Profile und Netzwerkpräfixe aus IPAM
    - `bird` BGP-Konfiguration
    - `nftables` Firewallkonfiguration
- Script zum deployen neuer Profile auf Nodes angepasst:
    - Unterbrechungsfrei für WireGuard verbindungen


Groups - Client-Networks - eduVPN-stage - GWDG Example WireGuard:exampleRole:wireguard
GWDG Example WireGuard:exampleRole:wireguard
Tag
Details
Tags
Tagged Objects
Tagged Objects
Count: 2
Type to quickfilter...
OBJECT
198.51.100.0/25 (GWDG)
2001:DB8::/64

```
eduvpn_prefixes_v4:
- 198.51.100.0/25
eduvpn_prefixes_v6:
- 2001:db8::/64
eduvpn_profiles:
  GWDG Example WireGuard:
    group: exampleRole
    wRangeFour: 198.51.100.0/25
    wRangeSix: 2001:db8::/64
```

Wireguard über TCP/HTTPS

- UDP VPN-Verbindungen in manchen Netzen nicht möglich
  - Hotel WLANs
  - Staaten mit Restriktionen beim Internetzugriff
- OpenVPN über TCP funktioniert oft auch nicht
  - Zwei Protokolle machen das Setup komplizierter
  - Pro Profil ein TCP-Port (nicht alles auf 443)
- Neues Feature in eduVPN: ProxyGuard
  - WireGuard UDP-Pakete werden durch HTTPs getunnelt
  - Proxy kann auf eigenem Server laufen
  - Automatischer Wechsel bei Verbindungsproblemen über UDP
  - Noch nicht auf iOS und macOS

Connect before Logon

- VPN Verbindungsaufbau vor der Benutzeranmeldung an Windows
- Bisher mit AnyConnect möglich
- Anwendungsfälle:
    - Roaming-Profile (durch Microsoft deprecated)
    - AD-Anmeldung
    - Manche Gruppenrichtlinien
- Von eduVPN nicht unterstützt
    - Fehlende APIs in Windows
- Lösungsansatz: System-VPN
    - Wireguard Tunnel mit langer Gültigkeit
    - Nur auf gemanagten Geräten
    - Nur während der Anmeldung nötige Zugriffe

Erfahrungen

Innerhalb der GWDG

- VPN für alle privilegierten Zugriffe
    - Keine Adminnetze mehr im Büro
    - Alle Admins fast immer im VPN
- Client funktioniert gut auf allen verwendeten Betriebssystemen
    - Rollout über das Clientmanagement
- Anmeldung mit YubiKey und Fido2/U2F komfortabel
- Stabile IPs und Sessions
    - SSH-Sessions leben nach Standby oder Netzwechsel weiter
- 24h timeout sorgt für Probleme -> 16h
- CLI-Client ist beliebt

Universität

- Rollout zuerst bei Studierenden
  - Keine größeren Probleme mit dem Client
  - Erster Dienst mit MFA-Zwang
- Aktuell, Rollout bei den Mitarbeiter*innen
  - Für die meisten, erster Dienst mit MFA-Zwang
  - Teilweise Connect Before Logon nötig

Performance

- Bisher kaum sichtbare CPU-Auslastung auf Server
- Benutzererfahrung: deutlich performanter als AnyConnect
- 8Gbit/s durch ProxyGuard mit 4 CPU-Kernen
    - AES Instruktionen in VM durchreichen lohnt sich
    - Oder `CHACHA-POLY` Ciphers benutzen

Fragen

Sebastian Klamt sebastian.klamt@gwdg.de
Steffen Klemer steffen.klemer@gwdg.de