Leibniz Universität
IT Services

Leibniz
Universität
Hannover

Das VPN-Angebot des LUIS

Uwe Oltmann

Definition VPN

- Virtual Private Network
  - virtuelles Netzwerk, das über ein anderes Netzwerk übertragen wird
  - Häufig zum sicheren Zugriff auf entfernte Ressourcen verwendet
  - Varianten:
    - Site-to-Site-VPN:
      - Verbindung zweier entfernter Netze über VPN-Gateways
      - Überbrückung von Zwischennetzen
      - meist als dauerhafte Verbindung
    - Remote-Access-VPN:
      - Verbindung von (mobilen) Clients aus öffentlichen Netzen zu einem VPN-Gateway
      - Tunnel wird (meist temporär) durch Client aufgebaut
      - Zweck: Zugriff auf interne Ressourcen von externen Standorten aus
  - Unterschiedliche Protokolle: IPSec, SSL-VPN, L2TP, ...

Zentraler VPN-Dienst

- Wird seit vielen Jahren vom LUIS angeboten
  - Verbindung von außerhalb der Leibniz Universität Hannover
  - Client-IP-Adresse aus einem definierten Adressbereich der LUH
  - Anwendungsbereiche:
    - Zugriff auf LUH-weit erreichbare Dienste und Server
    - Recherchemöglichkeiten in vielen Verlagsangeboten der TIB
- Nutzung per Anyconnect-Client
  - SSL-VPN → nur Port 443 wird verwendet (TCP und UDP)!
  - sämtlicher Datenverkehr läuft über das VPN
  - Client für übliche Betriebssysteme verfügbar
    - Installation per Browser-Login auf Server
    - bei Mobilsystemen im App-Store
    - Unter Linux und Android auch OpenConnect (OpenSource-Client)

Bild: Aufbau allgemeines VPN

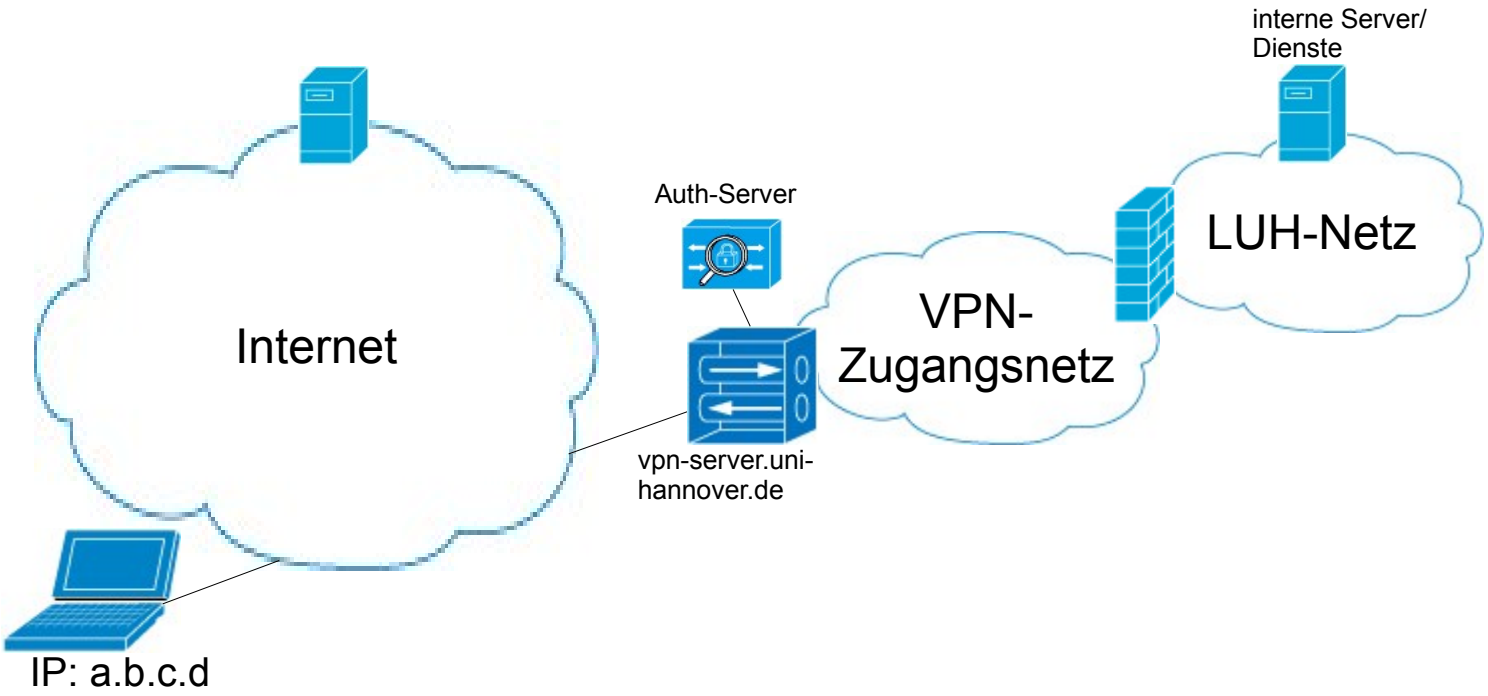
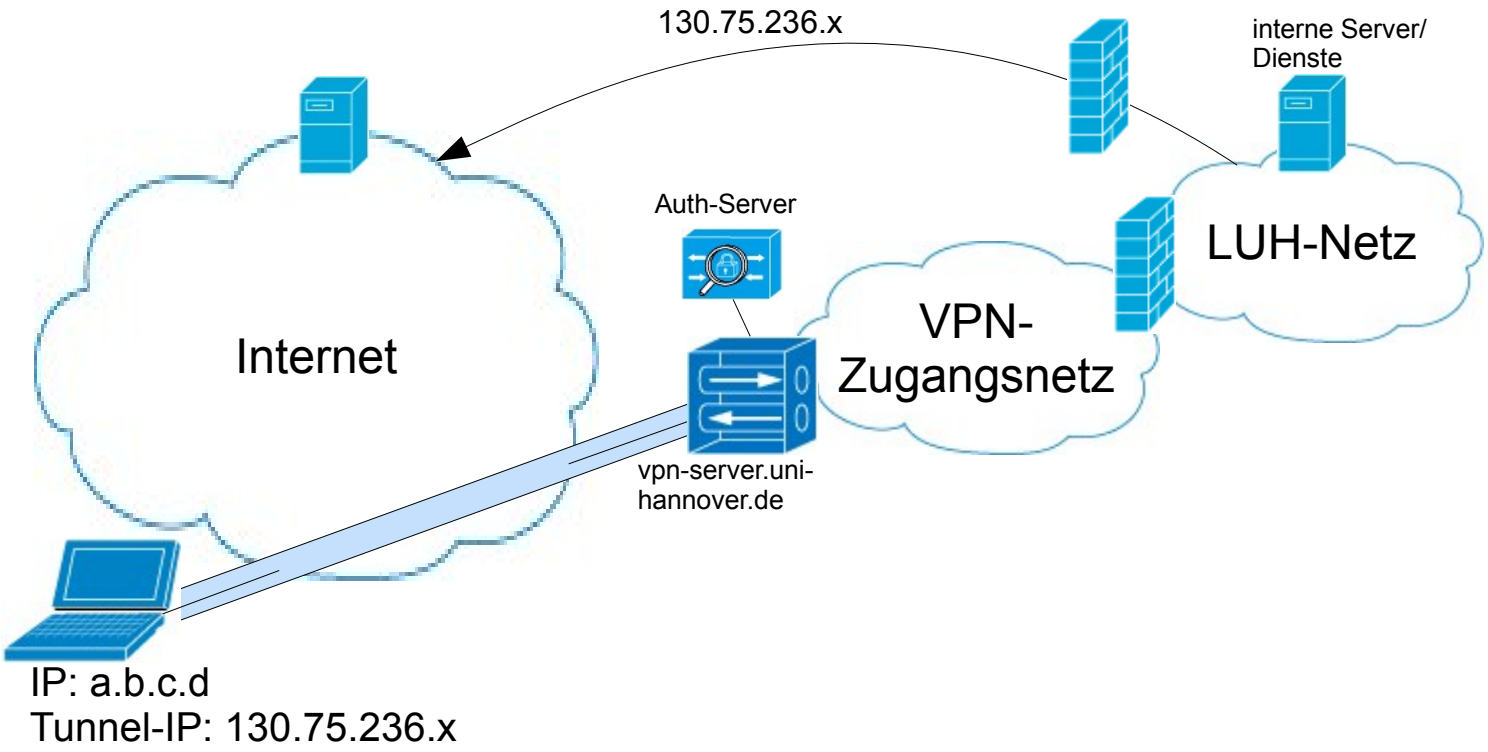


Bild: Aufbau allgemeines VPN



Weitergehende Kundenanforderungen

- Netze innerhalb der LUH sind nach Einrichtungen separiert
  - üblicherweise sind institutsinterne Server und Dienste nur aus jeweiligem Netz erreichbar
  - Zugriff auf Institutsnetz meist nur von Festnetzanschlüssen in Institutsräumlichkeiten
- Wunsch von Einrichtungen, den eigenen Nutzern Zugriff in ihr „Institutsnetz“ zu ermöglichen
  - aus dem WLAN auf dem Campus
  - von extern
- mit allgemeinem VPN-Dienst nicht erreichbar

Bisherige Lösungen

- an einigen Einrichtungen existieren bereits Standalone-VPN-Lösungen
  - z.T. von der Einrichtung selbst eingerichtet und betrieben
  - z.T. mit Unterstützung des LUIS eingerichtet (ASA 5505/5506)
- Nachteile:
  - hoher Aufwand bei Ersteinrichtung sowie Sicherheitsupdates
  - keine Redundanz
  - bei Updates/Neustart werden bestehende Sessions beendet

Zentrale Bereitstellung von Instituts-VPNs

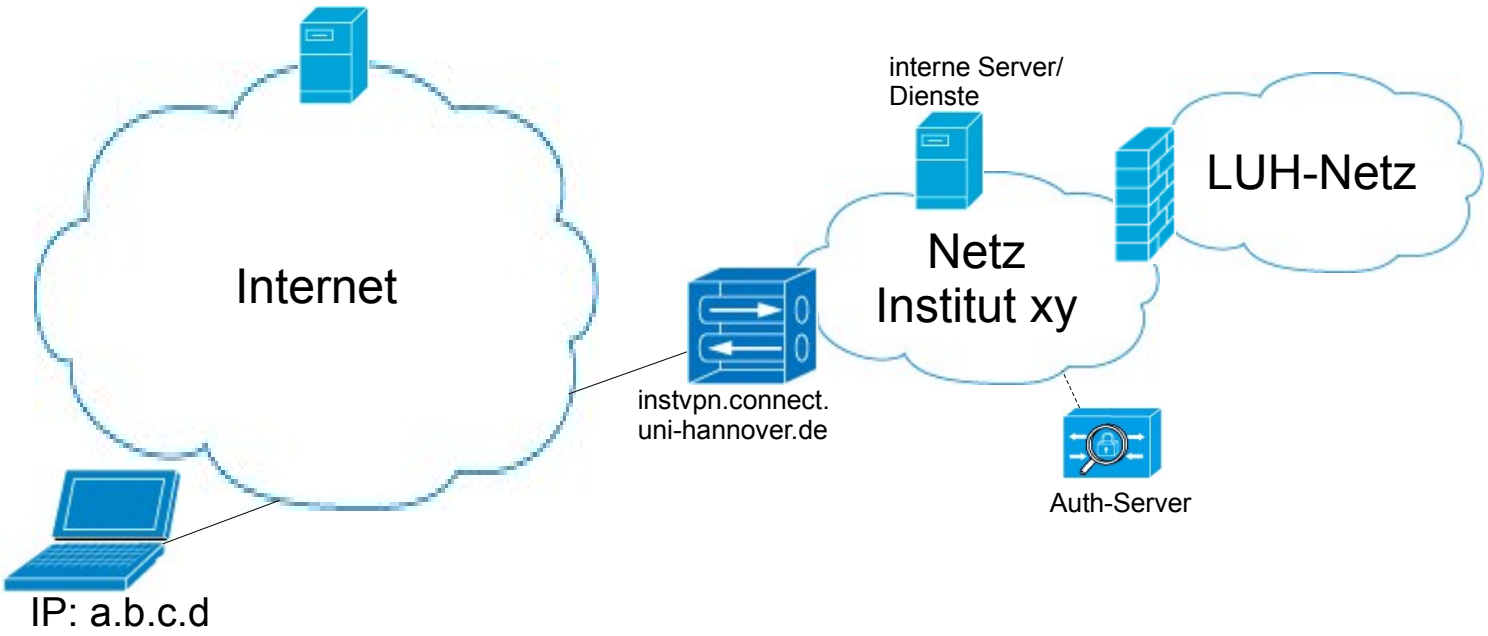
- Realisierung durch separate Kontexte auf gemeinsamer Hardware
- vergleichbare Features wie bei Standalone-Geräten
- Konfiguration (in Grenzen) an Institutsbedarf anpassbar
- Redundanz durch zwei im Failover-Verbund betriebene Geräte
- Anyconnect-VPN-Client nutzbar, keine Neuinstallation nötig
- Betriebssystem und Client-Versionen werden zentral aktualisiert
- Einschränkungen: kein Browser-Login / keine automatische Installation des Clients

Nutzerverwaltung

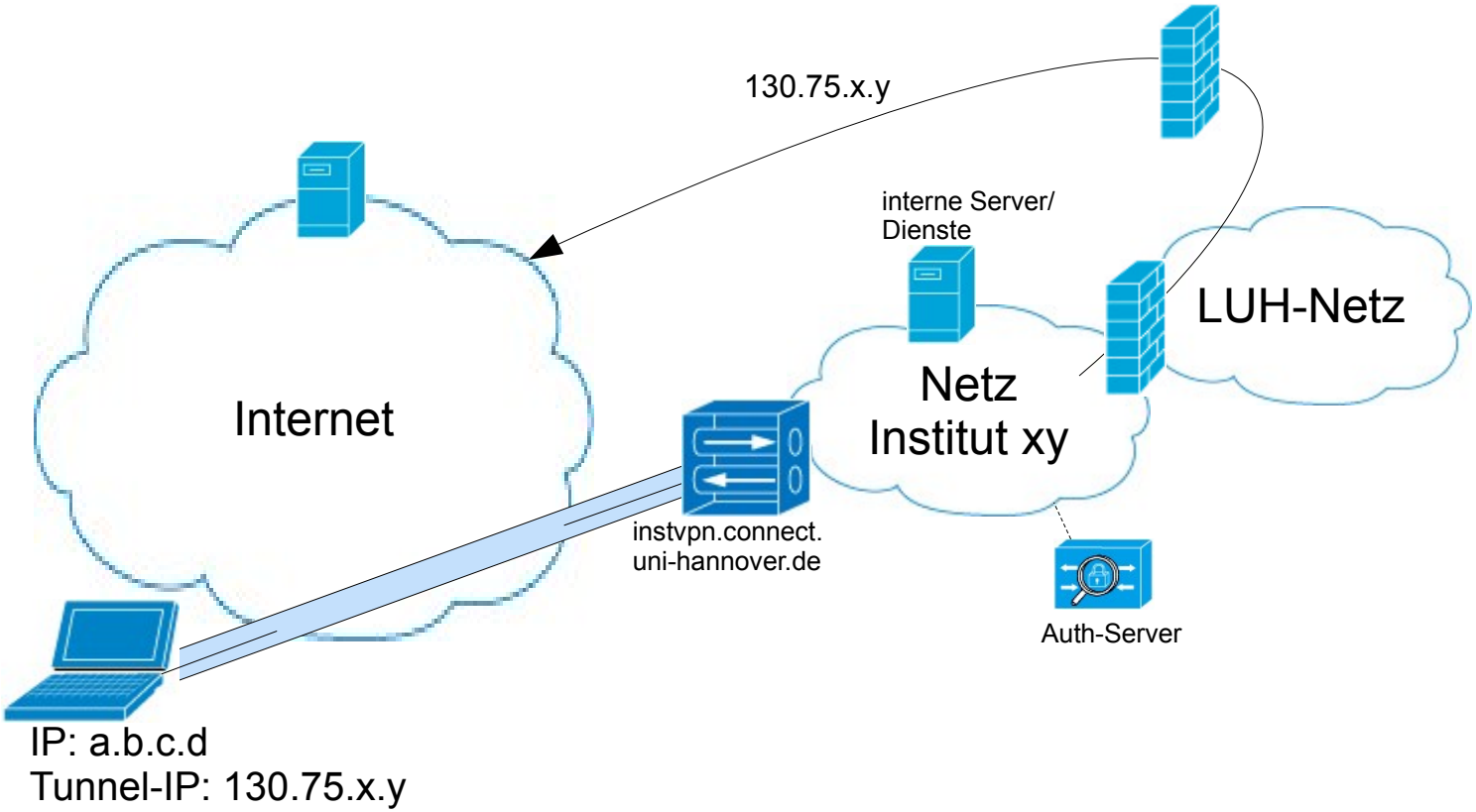
- Derzeit keine Anbindung an zentrale Nutzerverwaltung

- Möglichkeiten:
  - lokale Nutzerverwaltung auf dem eigenen VPN-Kontext durch Admins der Einrichtung
  - Falls in Einrichtung vorhanden: Anbindung an LDAP/Active Directory/RADIUS
  - Zertifikatsbasierte Authentifizierung, auch als 2.Faktor, möglich

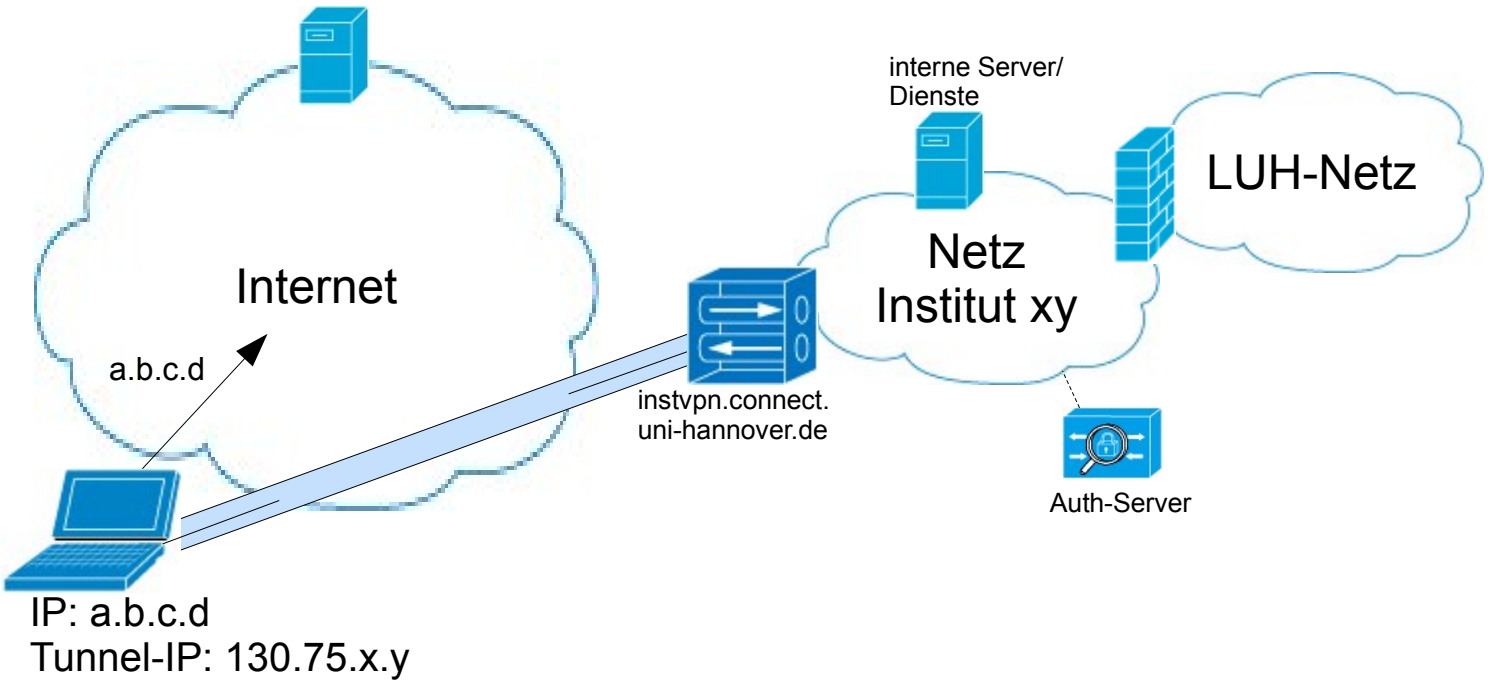
Schema eines Instituts-VPNs (1)



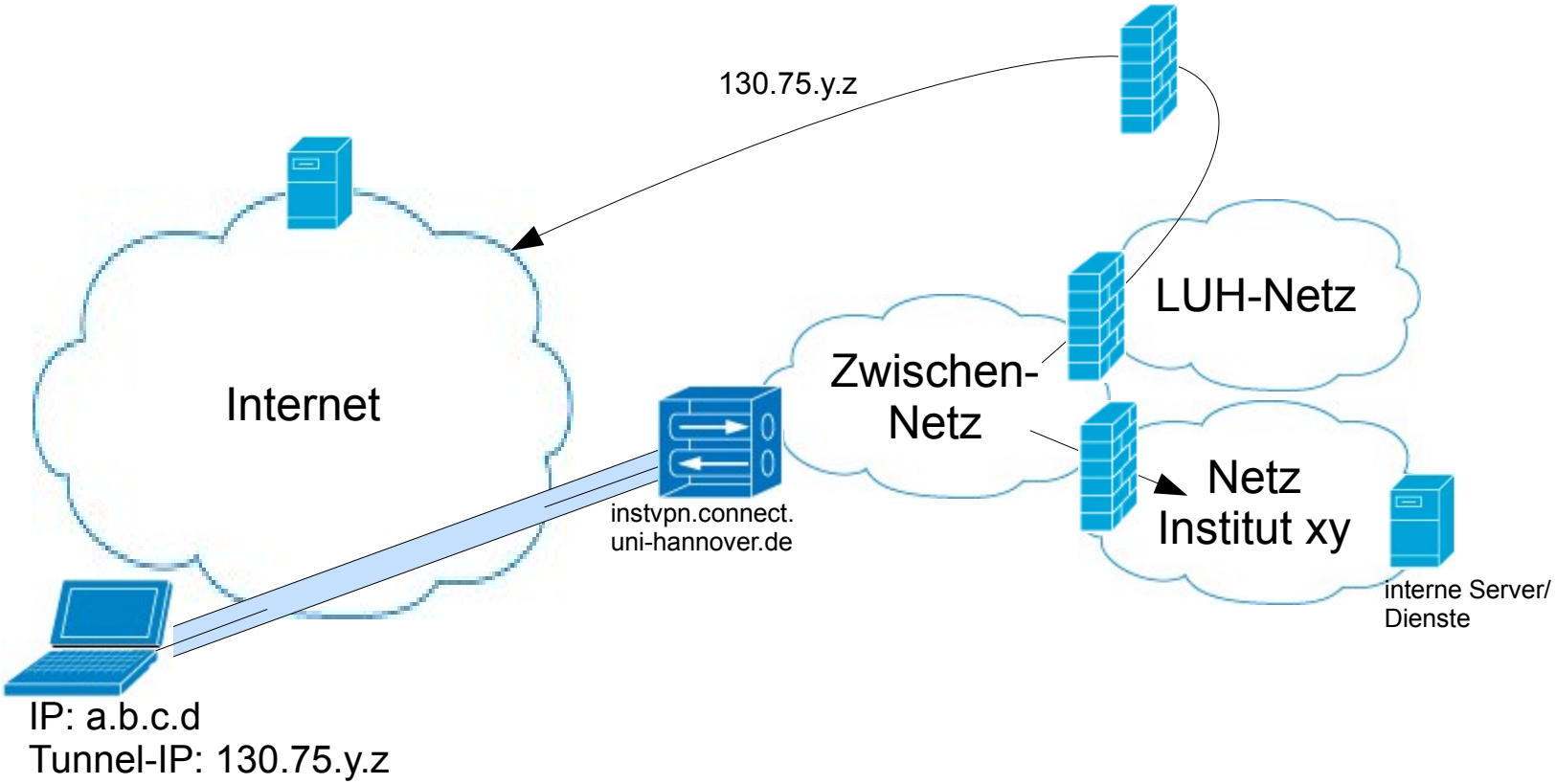
Schema eines Instituts-VPNs (2)



Schema eines Instituts-VPNs (Split Tunneling)



Instituts-VPN mit Zwischennetz



Voraussetzungen für teilnehmende Einrichtungen

- Einbindung in Sicherheitskonzept (auf welche Daten kann per VPN zugegriffen werden?)
- eigene Nutzerverwaltung
- IP-Adresspool für Clients muss aus Institutsnetz bereitgestellt werden
- Anzahl benötigter Adressen: max. gleichzeitig verbundene Clients +2 für Interfaces
- Administrationszugriff für Instituts-Admins auf eigenen Kontext möglich:
  - per SSH (Kommandozeile)
  - ASDM-Administrationstool (javabasiert, kann unter Windows lokal installiert werden)

Sicherheitserwägungen

- Umgehung von Netzschutz/Firewall durch VPN-Zugang
- mögliche Verbreitung von Schadsoftware von Privatrechnern
- Gefahr des Ausspähens von internen Daten
- Klärung: ist Zugriff auf personenbezogene Daten möglich?
- mögliche Maßnahmen zur Erhöhung der Sicherheit:
  - Erreichbarkeit des VPN auf das LUH-interne Netz einschränken (Nutzung aus dem WLAN)
  - 2-Faktor-Authentifizierung (z.B. Nutzung nur mit dienstlichen Geräten)
  - Verzicht auf Split-Tunneling
  - Client-IP-Adresse aus Zwischennetz mit selektivem Zugriff auf interne Dienste

Fazit und Ausblick

- Zentrale Instituts-VPN-Lösung für Einrichtungen der LUH ist jetzt verfügbar
- ermöglicht Nutzung interner Dienste aus dem WLAN und auch von extern
- Nutzerverwaltung durch Einrichtung
- Aber: neue Möglichkeiten bergen auch neue Gefahren
- Zugriff auf kritische Daten sollte eingeschränkt werden

- Bei Bedarf werden Kapazitätserweiterungen des Dienstes vorgenommen