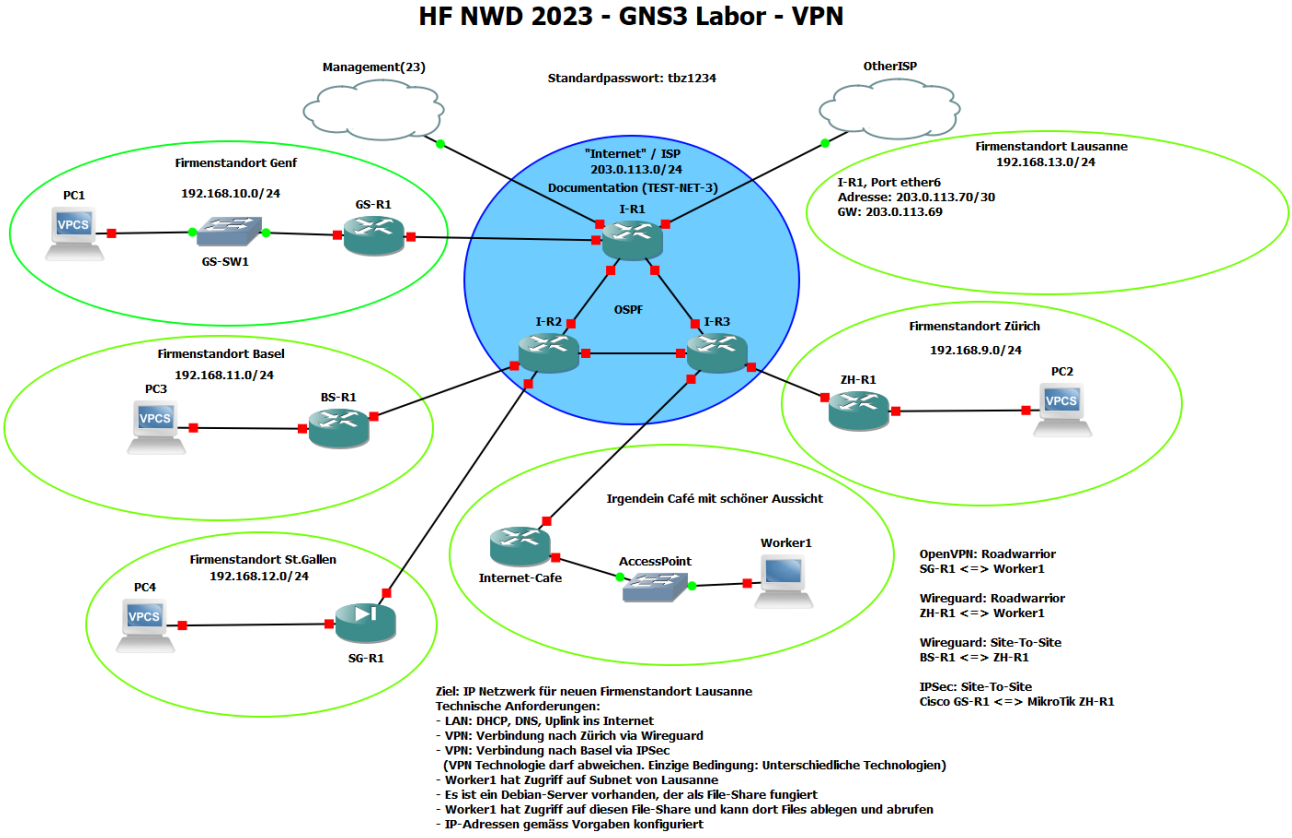
Technische Berufsschule Zürich TBZ
Höhere Fachschule

HF – NWD GNS3 Labor: VPN Technologien



1 Einleitung

Sie haben als Netzwerkingenieur den Auftrag erhalten in einem KMU einen zusätzlichen Geschäftsstandort per VPN zu erschliessen. Das KMU hat keinen eigenen Betriebsinformatiker. Jedes Mal, wenn eine Erweiterung des Netzwerkes benötigt wurde, hat das KMU eine andere IT-Firma beauftrag. Das hat zur Folge, dass überall unterschiedliche Geräte und VPN-Technologien eingesetzt wurden. Das ist eine optimale Gelegenheit, um neue VPN-Technologien kennenzulernen und zu vergleichen!

Die Wahl des Gerätes für Lausanne steht Ihnen frei. Alle anderen Standorte haben einen funktionierenden Internetanschluss und eine funktionierende VPN-Verbindung an den Hauptstandort in Zürich. In der Mitte finden Sie ein Netzwerk eines fiktiven ISP. Der verwendet OSPF als internes Routing-Protokoll (iBGP eignet sich für ISP besser). Über den ISP können sie auch auf das Internet zugreifen.

Lernziele:

- Unterschiedliche VPN-Technologien kennenlernen
- VPN auf einem Router konfigurieren, testen und dokumentieren

Die messbaren Ziele sind direkt im GNS3 Projekt zu finden (siehe Screenshot oben).

2 Themengebiete

Diese Laborübung beinhaltet folgende Themengebiete:

- Kernthema: VPN Technologien OpenVPN, Wireguard, IPsec
- IP-Protokolle, namentlich IPv4 und IPv6
- Standardprotokolle wie HTTP, DHCP, DNS, ARP, ICMP, usw.
- Bedienung bzw. Konfiguration und Steuerung von Netzwerkgeräten und Server über die CLI
- Betriebssysteme: Cisco IOS, MikroTik RouterOS, pfsense
- Netzwerkdokumentation

3 Allgemeine Instruktionen

Bitte lesen Sie diese Instruktionen sorgfältig durch und fragen Sie bei Unklarheiten den Kursleiter.

In diesem Modul arbeiten Sie mit der Netzwerksimulationssoftware GNS3, mit der Sie per Drag-and-Drop Topologien in Sekundenschnelle aufbauen können. Im Hintergrund arbeitet GNS3 mit Qemu-KVM VMs für die Switche und Router und verbindet diese bezüglich Ihrer Topologie mit Linux-Bridges. Weitere Informationen zum Aufbau der TBZ Cloud Infrastruktur finden Sie im Repository https://gitlab.com/ch-tbz-it/Stud/allgemein/tbzcloud-gns3

Sie arbeiten jeweils in Zweier-Teams am selben Labor auf demselben Server bzw. derselben TBZ Cloud GNS3 Instanz. Wie Sie eine Verbindung zu Ihrer Instanz aufbauen können, erfahren Sie unter https://gitlab.com/ch-tbz-it/Stud/allgemein/tbzcloud-gns3/-/tree/main/02_Bedienungsanleitung . Den OpenVPN Key zu Ihrer Instanz erhalten Sie vom Kursleiter.

Damit Sie die Aufgaben lösen können, müssen Sie selbstständig im Internet recherchieren. Nicht alle notwendigen Informationen sind in diesem Dokument vorhanden.

Folgende Zugangsdaten sind bekannt:

- MikroTik: Benutzername: `admin`, Passwort: `tbz1234`
- Debian: Benutzername: `debian`, Passwort: `debian`
- Cisco: Passwort: `tbz1234`
- Standardpasswörter zum Ausprobieren: `cisco`, `debian`, `admin1234`, `admin`

4 Aufgaben

4.1 VPN Technologien per Packet Capture analysieren

Die drei verwendeten VPN-Technologien bauen auf unterschiedlichen Netzwerkstacks auf. Analysieren Sie die unterschiedlichen Protokolle mithilfe von Wireshark Captures und halten Sie Unterschiede in den Netzwerkstacks fest. Beantworten Sie mithilfe der Packet Caputes zusätzlich folgende Fragen in Ihrem Bericht: Weshalb kann IPSec und NAT ein Problem darstellen?

4.2 Neuen Standort Anbinden

1. Lesen Sie die Anforderungen an das Netzwerk und das Ziel. Entscheiden Sie sich für einen Router-Typ und richten das Gerät ein.
2. Richten Sie den Zugriff für Worker1 ein. Worker1 hat bereits via OpenVPN und Wireguard Zugriff auf zwei Standorte.
3. Testen und Konfigurieren Sie so lange bis alle Anforderungen erfüllt sind.
4. Dokumentieren Sie alle getätigten Konfigurationen so, dass eine andere Fachperson Ihre Konfiguration möglichst schnell nachbauen kann und versteht, was sie dabei tut (Dazu gehört unter anderen auch, dass sie z.B. alle Befehle per Copy-Paste einfügen kann)

Wenn Sie den Bericht abgeben, muss ihr Netzwerk in einem funktionsfähigen Zustand sein. Der Kursleiter wird nebst dem Bericht auch ihr GNS3 Labor überprüfen.

5 Hinweise zur Dokumentation

- Beschränken Sie sich auf das Wesentliche. Unterlassen Sie es leere Sätze oder persönliche Statements zu schreiben. Fokussieren Sie sich auf die Sachlage.
- Nachvollziehbarkeit: Anhand ihrer Dokumentation müssen Dritte in der Lage sein, alles exakt genau gleich nachbauen zu können.
- Erstellen Sie pro Gruppe ein eigenes privates Repository mit dem Namen HF_NWD und pushen Sie dieses auf GitLab (Alternativ GitHub). Gewähren Sie der Lehrperson den Zugriff auf das Repository.
- Machen Sie bei der Abgabe einen Export des aktuellen Repository-Standes und geben diesen als ZIP-File via Teams-Aufgabe ab.
- Die gesamte Dokumentation muss in Markdown erfolgen. Fügen Sie erstellte Netzwerktopologien als Grafiken ein.
- Alle Grafiken sind scharf und müssen gut zu lesen sein.
- Als Inspiration können Sie die Vorlagen von diesem Repository verwenden: https://gitlab.com/alptbz/beispiel-lernjournal-fuer-laboruebungen . Lassen Sie die Reflexion und das aufführen ihrer neuen Lerninhalte **weg**.

6 Regeln

- Es dürfen keine Geräte entfernt oder hinzugefügt werden – ausser am Standort Lausanne.
- Es ist erlaubt zu Testzwecken z.B. ein Ubuntu Desktop an einem Port anzuschliessen – wie wenn Sie ein Laptop an einem «echten» Router oder Switch einstecken.
- Alle Kabelverbindungen zwischen den Geräten sind fix. Erstellen Sie keine neuen (Ausser die für Lausanne – siehe Hinweis im GNS3 Projekt).

7 Bewertungskriterien und Abgabetermin

Informieren Sie sich bei der Kursleitung betreffend Abgabetermin und Bewertungskriterien. Zu spät abgegebene (bis 24h) Arbeiten erhalten Abzug nach Ermessen der Kursleitung. 24 Stunden nach dem Abgabetermin werden keine Arbeiten akzeptiert und die Aufgabe gilt als nicht erfüllt.

8 Links

- Protokollstapel
- MikroTik
- RouterOS
- WireGuard
- Cisco IPsec Introduction
- Blogeintrag über WireGuard

Neue Versionen dieses Dokumentes ersetzen Vorherige. Es liegt in der Pflicht des Studenten sich jeweils die aktuelle Version des Dokumentes bei der Kursleitung zu beschaffen.