Abschlussprüfung Winter 2025

Fachinformatiker Systemintegration

Dokumentation zur betrieblichen Projektarbeit

Einführung einer zentralen Nextcloud-Plattform zur Dateiablage ohne Portweiterleitung

Prüfungsbewerber:

Omar-Mohammed-Qaid Mohammed

Graal-Müritzer-Straße 3

22885 Barsbüttel

Prüflingsnummer: 131 54051

Ausbildungsbetrieb:

CBM Projektmanagement GmbH

Süderstraße 63

20097 Hamburg

Betrieblicher Betreuer:

Svenja Faber

Tel: 040 / 23 78 22 – 88

Inhaltsverzeichnis

Anhang

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Glossar

Abkürzung	Langform	Erläuterung
CBM	CBM Projektmanagement GmbH	Ausbildungs- und IT-Dienstleistungsunternehmen
DMZ	Demilitarisierte Zone	Isolierter Netzwerkbereich für Server wie Nextcloud
DSGVO	Datenschutz-Grundverord-nung	EU-Verordnung zur Verarbeitung personenbezo-gener Daten sowohl private wie öffentliche
LAN	Local Area Network	Internes Netzwerk des Unternehmens/der Schule
NAT	Network Address Translation	Umsetzung interner IP-Adressen in andere Ad-ressbereiche durch die Firewal
VPN	Virtual Private Network	Verschlüsselter Fernzugriff auf interne Systeme
VPS	Virtual Private Server	Externer Server als WireGuard-Knotenpunkt
2FA	Two-Factor Authentication	Two-Factor Authentication (Zwei-Faktor-Authenti-fizierung)
DNS	Domain Name System	Dienst zur Namensauflösung
HTTP	Hypertext Transfer Protocol	Unverschlüsseltes Webprotokoll (Basis von HTTPS)
WebGUI	Web Graphical User Interface	Browserbasierte Administrationsoberfläche
WAN	Wide Area Network	Externes Netzwerk bzw. Internetanbindung
IP	Internet Protocol	Netzwerkadressierung für Geräte/Serve
TLS	Transport Layer Security	Verschlüsselungsprotokoll, Grundlage für HTTPS
VM	Virtuelle Maschine	Durch Proxmox bereitgestellte Serverinstanz
HTTPS	Hypertext Transfer Protocol Secure	Verschlüsseltes Webprotokoll zum sicheren Da-tenzugriff

1 Einleitung

1.1 Projektumfeld

Die CBM Projektmanagement GmbH ist ein Bildungs- und IT-Dienstleistungsunternehmen, das täglich eine große Anzahl von Teilnehmenden, Dozent*innen und internen Mitarbeitenden betreut. Für den Schulungs- und Verwaltungsbetrieb werden zuverlässige und sichere IT-Systeme benötigt. Dazu gehören unter anderem digitale Lernplattformen, zentrale Datenablagen und Tools für die Zusammenarbeit. Der Fachbereich stellte fest, dass bislang keine zentrale, geschützte Lösung für den Austausch von Dateien existierte.

Daten wurden häufig über unsichere Wege wie USB-Sticks oder per E-Mail ausgetauscht, was nicht nur unübersichtlich ist, sondern auch ein Sicherheitsrisiko darstellt. Um dieses Problem zu lösen, wurde der interne IT-Bereich beauftragt, eine DSGVO-konforme Kollaborationsplattform aufzubauen. Das Projekt wird im Rahmen meinem Praktikum zum Fachinformatiker Systemintegration umgesetzt und trägt gleichzeitig dazu bei, die bestehende Schulungsumgebung technisch zu erweitern und sicherer zu machen.

1.2 Projektbeschreibung

Ziel des Projektes ist die Einführung einer zentralen Kollaborationsplattform auf Basis von Nextcloud, betrieben in einer isolierten DMZ-Umgebung unter Proxmox VE. Die Plattform soll den sicheren Austausch von Dateien ermöglichen und eine klare Benutzer- und Rechteverwaltung bieten.

Die gesamte Umgebung wird durch eine OPNsense-Firewall geschützt, die für die Netztrennung (LAN/DMZ), Firewall-Regeln und VPN-Verbindungen zuständig ist. Zusätzlich wird ein externer VPS eingesetzt, über den ein verschlüsselter WireGuard-Tunnel zur OPNsense aufgebaut wird. Dadurch wird ein sicherer externer Zugriff ermöglicht – ohne das Schulnetz zu öffnen. Die Nextcloud-Instanz wird über HTTPS verschlüsselt bereitgestellt und sicherheitstechnisch gehärtet (2FA, Fail2ban, Security-Header, Berechtigungskonzept).

1.3 Projektbegründung

Im Schulungsbetrieb der CBM Projektmanagement GmbH entsteht täglich ein hoher Bedarf an einem sicheren und zentralen Austausch von Lernmaterialien, Projektdaten und Dokumenten. Bisher existiert keine einheitliche, datenschutzkonforme Lösung, über die Dozentinnen und Teilnehmerinnen zuverlässig zusammenarbeiten und Dateien strukturiert teilen können. Dadurch entstehen Medienbrüche, ineffiziente Abläufe und ein erhöhtes Risiko für Datenverlust. Zudem stellen Lernumgebungen Anforderungen an flexibles Arbeiten, sowohl innerhalb des Schulnetzwerks als auch standortunabhängig. Ein sicherer externer Zugriff wird jedoch durch die Netzwerkarchitektur des Schulstandorts eingeschränkt, da aus Sicherheitsgründen keine Portfreigaben am Schulrouter möglich sind.

Durch die Einführung einer Nextcloud-Plattform in einer isolierten DMZ-Umgebung auf Proxmox und der Absicherung über eine OPNsense-Firewall wird eine professionelle Infrastruktur geschaffen, die den Schutz der Daten und des Schulnetzwerks sicherstellt. Außerdem ermöglicht ein über einen externen VPS realisierter WireGuard-Tunnel einen geschützten Zugriff von außen, ohne die Sicherheit des Schulnetzes zu gefährden.

1.4 Projektziel

Das Projekt verfolgt das Ziel, eine sichere, zentral verwaltbare und DSGVO-konforme Plattform für den Datenaustausch innerhalb der CBM bereitzustellen.

Die Lösung soll Folgendes gewährleisten

- sichere Dateiablage und strukturierte Zusammenarbeit
- klare Trennung von internem Netz (LAN) und Servernetz (DMZ)
- verschlüsselte Übertragung aller Daten (HTTPS / VPN)
- Zugriff extern über WireGuard-Client

Durch das Projekt wird eine moderne Plattform geschaffen, die den Schulungs- und Verwaltungsbetrieb langfristig unterstützt und verbessert.

1.5 Projektschnittstellen

Proxmox-Virtualisierungsumgebung
Hier werden die virtuellen Maschinen für OPNsense und Nextcloud bereitgestellt. Proxmox bildet die technische Basis für die Serverbereitstellung und Ressourcenzuweisung.

OPNsense-Firewall
Dient als zentrale Netzwerkschnittstelle zwischen dem Schulnetz, der DMZ und der VPN-Verbindung.

DMZ (Servernetzwerk)
Isolierter Netzwerkbereich, in dem die Nextcloud-Instanz betrieben wird. Die DMZ ist nur über festgelegte Firewall-Regeln erreichbar.

Nextcloud-Server
Bietet die eigentliche Kollaborationsplattform für Dozent*innen und Teilnehmende. Schnittstellen bestehen zur Benutzerverwaltung, zum Webserver (HTTPS) und zum Speichersystem.

VPS (externer Server)
Dient als öffentlicher Einstiegspunkt für externe Nutzer per Wireguard, ohne dass Ports im Schulnetz geöffnet werden müssen.

WireGuard-VPN
Stellt einen verschlüsselten Tunnel zwischen VPS und OPNsense bereit, über den externen Nutzer nach erfolgreicher Authentifizierung auf die Nextcloud in der DMZ zugreifen können.

Endnutzer (Dozentinnen & Teilnehmerinnen)
Der Zugriff auf Weboberfläche der Nextcloud kann entweder intern aus dem Schulnetz über den Browser oder von extern über den VPN-Tunnel mittels Wireguard-Clients erfolgen.

Diese Schnittstellen gewährleisten, dass alle Systeme sauber miteinander kommunizieren und gleichzeitig die Sicherheit des Schulnetzes vollständig erhalten bleibt.

2 Projektplanung

2.1 Projektphasen

Für die Umsetzung des Projekts standen mir insgesamt 40 Stunden zur Verfügung. Damit die Arbeit strukturiert und nachvollziehbar ablaufen kann, habe ich die Zeit bereits vor Projektbeginn auf die typischen Phasen eines Systemintegrationsprojekts verteilt. Dazu gehören unter anderem die Analyse des Ist-Zustands, die Planung der Zielumgebung, die technische Umsetzung sowie die abschließenden Tests und die Dokumentation.

Eine erste Übersicht über die großen Projektphasen zeigt Listing 1: detaillierter Zeitplan Um die einzelnen Schritte besser darstellen zu können, habe ich jede Phase zusätzlich in kleinere Arbeitspakete unterteilt. Diese detaillierte Planung ist im Anhang A.1: Detaillierte Zeitplanung aufgeführt und beschreibt genau, welche Aufgaben in welcher Reihenfolge umgesetzt wurden,

Projektphase	Geplante Zeit
Analysephase	7 h
Entwurfsphase	3 h
Implementierungsphase	18 h
Erstellen der Dokumentation	12 h
Gesamt	**40h**

Table 1: Projektphasen

2.2 Ressourcenplanung

In der Übersicht im Anhang A.2: Verwendete Ressourcen sind alle Ressourcen aufgeführt, die für die Umsetzung des Projekts benötigt wurden. Dazu gehören sowohl Hard- und Softwarekomponenten als auch die eingesetzten personellen Ressourcen.

Bei der Auswahl der Software wurde darauf geachtet, ausschließlich kostenfreie Open-Source-Lösungen einzusetzen, wie Proxmox, OPNsense, WireGuard und Nextcloud. Dadurch konnten die Projektkosten geringgehalten und Lizenzgebühren vollständig vermieden werden.

Als Hardware kamen ein vorhandener Proxmox-Server sowie ein kleiner externer VPS für den WireGuard-Zugang zum Einsatz. Die Umsetzung, Konfiguration und Dokumentation wurden vollständig durch den Projektverantwortlichen durchgeführt

2.3 Ist Analyse

Derzeit existiert keine zentrale Cloud- oder Kollaborationslösung für Teilnehmer und Dozenten. Daten werden dezentral gespeichert und häufig über unsichere Kanäle wie USB-Sticks oder E-Mails ausgetauscht. Dadurch fehlen einheitliche Sicherheitsrichtlinien, zentrale Zugriffskontrollen und eine konsistente Strategie zur Datenverwaltung.

Die bestehende IT-Infrastruktur bietet keine getrennte Serverzone (DMZ) und keine sichere Möglichkeit, interne Dienste strukturiert und geschützt bereitzustellen. Es existiert weder ein zentraler Speicherort für Dokumente noch ein rollenbasiertes Berechtigungssystem. Der externe Zugriff auf interne Ressourcen ist nicht möglich, da keine sichere Anbindung vorhanden ist.

Diese Situation führt zu erhöhten Sicherheitsrisiken, Datenverlustgefahr, unkontrollierten Freigaben und einem hohen organisatorischen Aufwand im täglichen Betrieb.

2.4 Soll-Analyse

Ziel ist der Aufbau einer sicheren, zentralen und DSGVO-konformen Plattform für den Austausch von Dateien im Schulungsbetrieb. Die Lösung soll vollständig im eigenen Netzwerk betrieben werden und über eine DMZ, eine OPNsense-Firewall und HTTPS abgesichert sein. Der Zugriff muss sowohl intern als auch extern möglich sein, wobei externe Verbindungen ausschließlich über einen verschlüsselten WireGuard-Tunnel erfolgen dürfen.

Die Plattform soll eine klare Benutzer- und Rechteverwaltung bieten, flexibel erweiterbar sein und sich sauber in die bestehende Proxmox-Infrastruktur der CBM integrieren lassen.

2.5 Wirtschaftlichkeitsanalyse

Aufgrund der in Abschnitt 1.3 (Projektbegründung) und 2.3 (Ist-Analyse) beschriebenen Probleme der aktuellen Dateiaustausch- und Kommunikationswege bei der CBM Projektmanagement GmbH ist die Umsetzung des Projekts nicht nur technisch erforderlich, sondern auch wirtschaftlich sinnvoll.

Der bisherige Einsatz unsicherer und dezentraler Austauschmethoden wie USB-Sticks, private Cloud-Dienste oder E-Mail verursacht einen hohen organisatorischen Aufwand, birgt Sicherheitsrisiken und erschwert eine datenschutzkonforme Arbeitsweise.

Die Einführung einer zentralen, geschützten und strukturierten Nextcloud-Plattform in einer Proxmox-Umgebung, abgesichert durch eine OPNsense-Firewall und ergänzt durch einen sicheren VPN-Zugang, ermöglicht eine deutliche Reduzierung des administrativen Aufwands und verbessert gleichzeitig die IT-Sicherheit und Effizienz.

In den folgenden Abschnitten wird die Wirtschaftlichkeit der Projektumsetzung näher erläutert und anhand relevanter Kriterien bewertet.

2.6 Make-or-Buy-Entscheidung

Bei der Planung musste entschieden werden, ob eine externe Cloudlösung eingekauft oder eine eigene Instanz aufgebaut wird. Es gibt zwar DSGVO-konforme Cloudanbieter, aber die fehlende Datenhoheit und Abhängigkeiten vom Anbieter haben mich dazu veranlasst, eine eigene Instanz aufzubauen.

Zudem erlaubt die Schulumgebung keine Portfreigaben, wodurch sich externe Lösungen technisch nicht sicher integrieren lassen. Auch wirtschaftlich wäre ein laufendes Lizenz- und Benutzerkostenmodell langfristig teurer gewesen und hätte sich nicht in die geplante DMZ-, Firewall- und VPN-Struktur einfügen lassen.

Stattdessen fiel die Entscheidung auf „Make“. Eine eigene Nextcloud bietet vollständige Kontrolle über alle Daten, kann sicher in die vorhandene Proxmox-, OPNsense- und WireGuard-Architektur eingebunden werden und verursacht keine Lizenzkosten, da ausschließlich Open-Source-Komponenten genutzt werden. Die Lösung ist flexibel, erweiterbar und kann exakt an die Bedürfnisse der CBM angepasst werden.

Damit wurde die Make-Variante gewählt, da sie technisch sicherer, datenschutzkonform, kostengünstiger und deutlich besser integrierbar ist.

2.7 Projektkosten

Die Projektlaufzeit betrug 6 Wochen mit einem geschätzten Gesamtaufwand von 40 Stunden. Die folgenden Kosten ergeben sich aus den notwendigen Arbeitsstunden zur Planung, Umsetzung, Konfiguration und Dokumentation. Da ausschließlich Open-Source-Software eingesetzt wurde, fallen keine monatlichen Lizenzkosten an.

Rolle / Tätigkeit	Zeit	Stundensatz	Kosten in €
Nutzer Computer			0,00
PC-Server			0,00
VPS für Wireguard			5,00
Analyse, Abstimmungen, Planung	10 h	25,00	250,00

Installation & Konfiguration (Proxmox, OPNsense, DMZ, Nextcloud, HTTPS, WireGuard, Routing)	20 h	25,00	500,00
Testphase (LAN, DMZ, VPN, Funktionstests Nextcloud)	5 h	25,00	125,00
Lizenzkosten		0,00	0,00
Projektdokumentation & Übergabe	5 h	25,00	125,00
Betreuer	5 h	55,00	275,00
Mietkosten	40 h	62,50	2.500,00
Betriebskosten	40 h	5,00	200,00
Gesamtkosten			3.980,00

Tabelle 2: Projektkosten

3 Entwurfsphase

3.1 Technischer Entwurf der Zielumgebung

Der technische Entwurf beschreibt, wie die Zielumgebung für die neue Nextcloud-Plattform aufgebaut sein soll. Die Lösung basiert auf einer Proxmox-Virtualisierungsumgebung und wird durch eine OPNsense-Firewall abgesichert. Die Nextcloud wird in einer separaten DMZ betrieben, um eine klare Trennung vom internen Schulnetz sicherzustellen.

Die Umgebung besteht ausfolgenden Komponenten:

- Proxmox-Server als Basis für alle virtuellen Maschinen
- OPNsense-Firewall zur Trennung von LAN, DMZ und VPN sowie zur Steuerung des Datenverkehrs
- DMZ-Netz (10.10.10.0/24), in dem der Nextcloud-Server betrieben wird
- Nextcloud-VM, die den Datei- und Kollaborationsdienst bereitstellt
- Externer VPS, der als öffentlich erreichbarer Endpunkt für den WireGuard-VPN-Tunnel dient

Der Zugriff erfolgt intern direkt über das Schulnetz, während externe Nutzer über einen verschlüsselten WireGuard-Tunnel auf die DMZ zugreifen. Durch diese Architektur wird eine sichere und leicht verwaltbare Infrastruktur geschaffen, die alle Anforderungen des Projekts erfüllt.

3.2 Detailkonzept der Umsetzung

Das Detailkonzept beschreibt die praktischen Schritte, mit denen die geplante Zielumgebung technisch umgesetzt wird. Die Umsetzung erfolgt strukturiert in mehreren Arbeitsschritten

Proxmox bereitstellen

Installation des Proxmox-Servers, Anlegen der benötigten virtuellen Maschinen und Grundkonfiguration der Netzwerkschnittstellen (LAN und DMZ).

OPNsense installieren und konfigurieren

Einrichtung der Firewall-VM mit WAN- und LAN-Interface, Anlegen der DMZ-Zone, Aktivieren von Routing und Erstellung der notwendigen Firewall-Regeln für LAN, DMZ und VPN.

Nextcloud-Server installieren

Bereitstellung einer Linux-VM in der DMZ, Installation von Nextcloud inkl. Webserver und Datenbank

Sowie Grundkonfiguration.

HTTPS-Verschlüsselung einrichten

Erstellung eines internen Zertifikats, Import in die Nextcloud und Umstellung der Verbindung auf HTTPS.

Benutzer- und Rechteverwaltung einrichten

Anlegen von Benutzergruppen für Dozenten und Teilnehmende sowie Festlegen der Upload-Limits Und Dateirechte.

VPN-Anbindung über VPS aufbauen

Installation von WireGuard auf dem externen VPS und der OPNsense, Aufbau des verschlüsselten Tunnels sowie Routing der externen Anfragen in die DMZ.

Funktionstests durchführen

Überprüfung der Erreichbarkeit, der Firewall-Regeln, des VPN-Zugangs und der grundlegenden Nextcloud-Funktionen.

Dieses Konzept stellt sicher, dass die technische Umsetzung strukturiert erfolgt und alle sicherheitsrelevanten Bereiche berücksichtigt werden.

4 Implementierungsphase

4.1 Installation & Einrichtung der Proxmox-Umgebung

Zu Beginn der technischen Umsetzung wurde der Proxmox-Server installiert und für das Projekt vorbereitet. Die Installation erfolgte über das offizielle Proxmox-ISO, das zunächst auf einen USB-Stick übertragen und anschließend auf dem Hostsystem gestartet wurde.

Nach dem Bootvorgang wurden die Festplatte ausgewählt, die Standardpartitionierung übernommen und grundlegende Einstellungen wie Hostname, Management-IP-Adresse sowie DNS- und Gateway-Konfiguration vorgenommen. Nach Abschluss der Installation stand die Weboberfläche zur Verfügung, über die alle weiteren Schritte durchgeführt wurden.

Für das Projekt war es notwendig, die Netzwerkinfrastruktur sauber zu trennen. Daher wurde die vorhandene Standard-Bridge vmbr0 für das interne Schulnetz verwendet und zusätzlich eine zweite Bridge erstellt, die exklusiv als DMZ für die Serverdienste dient. Über diese Netztrennung können virtuelle Maschinen klar voneinander isoliert werden.

Die Konfiguration der Network-Bridges sowie die zugewiesenen IP-Adressen sind in Abbildung 4 im Anhang dargestellt. Nach der Erstellung der Bridges wurden die Netzwerkkarten der zukünftigen VMs entsprechend zu gewiesen, sodass OPNsense später als Firewall zwischen LAN und DMZ fungieren kann. Durch diese Vorbereitung bot der Proxmox-Server eine stabile Grundlage für die nachfolgenden Installations- und Konfigurationsschritte.

Bereich	Interface	Subnetz	Aufgabe
LAN & WAN	vmbr0 → vtnet0	172.16.201.0/24	Internes Netzwerk
DMZ	vmbr1 → vtnet1	10.10.10.0/24	Server in der DMZ

Tabelle 3: Netzwerk Übersicht Proxmox

4.2 Installation & Einrichtung der OPNsense-Firewall

Nach der Vorbereitung der Proxmox-Umgebung wurde die OPNsense-Firewall als zentrale Sicherheits- und Routingkomponente installiert. Die virtuelle Maschine erhielt zunächst zwei Netzwerkschnittstellen: eine WAN und eine DMZ-Schnittstelle. Das WAN-Interface der OPNsense ist für die ausgehende Verbindung zum externen VPS zuständig, über das der WireGuard-Tunnel aufgebaut wird. Obwohl sich die physische Schnittstelle im internen Schulnetz befindet, erfüllt sie die logische Rolle eines WAN-Interfaces. Nach dem ersten Start erfolgte die grundlegende Systemeinrichtung, einschließlich der Vergabe der IP-Adressen, der Zuordnung der Interfaces sowie der Aktivierung zentraler Dienste wie dem DNS-Resolver und dem Zugriff auf die WebGUI.

Anschließend wurde die DMZ-Zone eingerichtet, die im Projekt als separates Servernetz mit dem Adressbereich 10.10.10.0/24 definiert ist. Die DMZ wird über ein separates Interface (OPT1) in der OPNsense angebunden, das logisch von LAN und WAN getrennt ist. Die Nextcloud-VM befindet sich in der DMZ, wodurch interne Clients nur kontrollierten Zugriff über die Firewall erhalten und externe VPN-Clients ausschließlich über wg0 auf die DMZ zugreifen können.

Die Zuordnung der virtuellen Netzwerkkarten der OPNsense-VM zu den entsprechenden Netzwerk-Bridges in Proxmox ist in Abbildung 6 im Anhang dargestellt. Das interne Schulnetz (LAN) ist nicht direkt erreichbar; Zugriffe erfolgen ausschließlich kontrolliert über definierte Firewall-Regeln oder den VPN-Tunnel.

Bereich	Subnetz	Aufgabe
LAN -> WAN	172.16.201.231/24	Intern / Extern
OPT1 -> DMZ	10.10.10.0/24	Servernetz / Nextcloud
WGAWS (wg0)	10.100.100.0/24	VPN Tunnel

Tabelle 4: OPNsense Interfaces und IP-Adressen

4.3 Konfiguration von Routing und Firewall-Regeln

Nach der Einrichtung der DMZ wurde in der OPNsense das Routing zwischen WAN, DMZ und dem WireGuard-VPN konfiguriert. Die OPNsense fungiert dabei als zentraler Router und trennt die Netzbereiche anhand der zugewiesenen Interfaces.

Das LAN erhält ausschließlich Zugriff auf die HTTPS-Schnittstelle der Nextcloud in der DMZ (10.10.10.20), während ausgehende Verbindungen von der DMZ ins LAN blockiert werden. Die Routing-Tabelle weist das DMZ-Netz 10.10.10.0/24 korrekt dem DMZ-Interface zu, sodass Anfragen gezielt weitergeleitet werden können.

Der externe Zugriff über WireGuard nutzt das Tunnelnetz 10.100.100.0/24. Wg0 ist das Interface, über das der gesamte VPN-Traffic von externen Clients in die DMZ geleitet wird. OPNsense „sieht“ den Traffic auf seinem wg0-Interface wie auf einem normalen Netzwerkschnittstellen-Interface. NAT und Routing sorgen dafür, dass die Antwortpakete über denselben Tunnel zum VPS zurückgehen und der Client erhält eine Antwort. Der externe Zugriff ausschließlich über den VPN-Tunnel erfolgen soll.

Die gesamte Firewall- und Routing-Konfiguration der OPNsense ist in Abbildung 7 dargestellt.

4.4 Installation der Nextcloud-Server-VM in der DMZ

Für die Nextcloud-Installation wurde PostgreSQL verwendet, da SQLite für produktive Umgebungen nicht empfohlen wird. PostgreSQL bietet eine hohe Stabilität, unterstützt parallele Zugriffe mehrerer Nutzer zuverlässig und gilt als eines der robustesten Open-Source-Datenbanksysteme. Die Installation sowie der aktivierte Datenbankdienst sind in Abbildung 10 dargestellt.

Die Datenbank läuft lokal auf der Nextcloud-VM, ist jedoch durch Firewall-Regeln so abgesichert, dass ausschließlich die Nextcloud-Anwendung über den lokalen Socket bzw. die interne Verbindung darauf zugreifen kann. Externe Datenbankverbindungen sind vollständig blockiert.

Die Absicherung erfolgt zusätzlich über ein starkes Passwort für den PostgreSQL-Superuser sowie einen dedizierten Nextcloud-Datenbankbenutzer mit eingeschränkten Rechten. Für die Datensicherung wird regelmäßig ein PostgreSQL-Dump erstellt, der gemeinsam mit den Datei-Backups der Nextcloud gesichert wird. Dadurch ist eine vollständige Wiederherstellung der Anwendung jederzeit möglich.

4.5 HTTPS-Konfiguration für Nextcloud (Self-Signed Zertifikat / interne CA)

Zur Absicherung des Zugriffs auf die Nextcloud-Instanz wurde die gesamte Kommunikation auf HTTPS umgestellt. Dafür wurde zunächst auf dem Server eine Zertifikatsanfrage erstellt und über die interne Zertifizierungsstelle signiert. Nach der Ausstellung wurden Zertifikat und privater Schlüssel in den Webserver eingebunden und die HTTP-Konfiguration vollständig auf eine verschlüsselte Verbindung umgestellt. Die HTTPS-Verbindung zur Nextcloud-Instanz ist in Abbildung 11 dargestellt.

Die interne CA wurde ausschließlich auf den Schulungsrechnern der CBM im lokalen Zertifikatsspeicher hinterlegt, sodass die Browser dieser Geräte dem Zertifikat automatisch vertrauen und keine Warnmeldungen anzeigen. Private Endgeräte externer Nutzer besitzen diese Vertrauensstellung nicht und zeigen daher nachvollziehbar eine HTTPS-Warnung an. Da der externe Zugriff jedoch ausschließlich über den verschlüsselten VPN-Tunnel erfolgt und die Verbindung technisch sicher bleibt, stellt dies im Projektkontext kein Risiko dar.

Für einen späteren produktiven Betrieb wäre alternativ der Einsatz eines öffentlich signierten Zertifikats sinnvoll, um auch externe Geräte ohne Warnhinweise unterstützen zu können.

4.6 DNS-Auflösung für externe und interne Zugriffe

Für den Zugriff auf die Nextcloud-Instanz wird die DNS-Auflösung zentral durch die OPNsense bereitgestellt. Der VPN-Client erhält beim Verbindungsaufbau automatisch die interne DNS-Adresse der OPNsense. Anfragen auf den Nextcloud-Hostnamen werden intern direkt auf die DMZ-Adresse der Nextcloud (10.10.10.x) aufgelöst, siehe Abbildung 12**.** Dadurch wird sichergestellt, dass der Zugriff ausschließlich über den gesicherten VPN-Tunnel erfolgen kann. Externe DNS-Server werden bewusst nicht verwendet, um Leaks oder direkte Verbindungen am VPN-Tunnel vorbei auszuschließen.

4.7 Nextcloud Grundkonfiguration

Nach der erfolgreichen Installation und Absicherung der Nextcloud-Instanz wurde im nächsten Schritt die Grundkonfiguration durchgeführt. Dabei wurden zunächst die notwendigen Benutzerkonten angelegt und in klar strukturierte Gruppen wie Dozenten und Teilnehmer eingeteilt, um eine übersichtliche Rechtevergabe zu gewährleisten, siehe Abbildung 14**.**

Zudem wurden zentrale Einstellungen wie Standard-Apps, Benachrichtigungsfunktionen und Speicherpfade angepasst, sodass die Umgebung sofort einsatzbereit war und die Nutzer die Plattform ohne weitere technische Hürden verwenden konnten, siehe Abbildung 13. Durch diese Grundkonfiguration entstand eine stabile Basis für die spätere Nutzung der Cloudlösung im Schulungsalltag.

4.8 Sicherheitshärtung der Nextcloud

Nach der Grundkonfiguration wurde die Nextcloud-Installation umfassend gehärtet, um einen sicheren und stabilen Betrieb zu gewährleisten. Ein zentraler Schritt war die Aktivierung der Zwei-Faktor-Authentifizierung für administrative Konten, um den Schutz vor unbefugten Zugriffen deutlich zu erhöhen, siehe Abbildung 16.

Zur Abwehr automatisierter Login-Versuche wurde auf dem Server Fail2ban eingerichtet. Das System überwacht fehlgeschlagene Anmeldeversuche und blockiert verdächtige IP-Adressen automatisch, wodurch Brute-Force-Angriffe effektiv verhindert werden, siehe Abbildung 17. Zusätzlich wurde die Webserver-Konfiguration um wichtige Security-Header erweitert, um gängige Angriffsvektoren wie MIME-Manipulation zu unterbinden. Auch die Dateisystem- und Ordnerberechtigungen wurden angepasst, sodass nur notwendige Dienste und Benutzer Zugriff auf sicherheitsrelevante Verzeichnisse erhalten.

Neben diesen Maßnahmen wurden weitere sicherheitsrelevante Optimierungen berücksichtigt. Für die zuverlässige Ausführung von Wartungsaufgaben wurde der Hintergrundprozess auf Cron umgestellt, was die Stabilität und Performance der Nextcloud deutlich verbessert. Ergänzend bietet die OPNsense-Firewall die Möglichkeit, Rate-Limits und zusätzliche Brute-Force-Schutzmechanismen auf Netzwerkebene zu aktivieren, um externe Angriffsversuche weiter einzuschränken. Die abschließende Sicherheitsübersicht der Nextcloud nach Umsetzung der Härtungsmaßnahmen ist in der Systemprüfung ersichtlich, siehe Abbildung 15.

Für den dauerhaften Betrieb ist ein klar definierter Update- und Patchprozess essenziell, damit sowohl das Betriebssystem als auch die Nextcloud-Anwendung kontinuierlich sicherheitsrelevante Aktualisierungen erhalten. Ebenso unverzichtbar ist eine belastbare Backup-Strategie. Für den produktiven Einsatz wird eine Kombination aus regelmäßigen PostgreSQL-Dumps und der Sicherung des Nextcloud-Datenverzeichnisses empfohlen. Diese Vorgehensweise stellt sicher, dass im Falle eines Ausfalls sowohl Anwendung als auch Daten vollständig wiederhergestellt werden können.

4.9 Einrichtung des externen Zugriffs über VPS und WireGuard

Da im Schulnetz keine eingehenden Portfreigaben möglich sind, wurde der externe Zugriff auf die Nextcloud über einen separaten VPS realisiert. Dieser fungiert ausschließlich als öffentlicher Zugangspunkt und baut einen verschlüsselten WireGuard-Tunnel zur OPNsense-Firewall auf.

OPNsense initiiert die Verbindung zum VPS (PersistentKeepalive sorgt dafür, dass der Tunnel dauerhaft steht). Beide tauschen ihre Public Keys zur gegenseitigen Authentifizierung aus. Nach erfolgreicher Verbindung existiert ein virtuelles Interface wg0 auf der OPNsense und ein Interface auf dem VPS mit unterschiedlichen Tunnel-IP-Adressen (10.100.100.0/24).

Dadurch können externe Nutzer ausschließlich über diesen VPN-Tunnel auf die Nextcloud zugreifen, ohne direkten Kontakt zum internen Schulnetz zu haben.

Der VPS übernimmt keine Routing- oder NAT-Aufgaben, sondern dient lediglich als Tunnel-Endpunkt. Für seinen Betrieb genügt das Aktivieren von IP-Forwarding. Die Verarbeitung und Weiterleitung des VPN-Verkehrs erfolgt vollständig auf der OPNsense: Der eingehende Datenstrom wird über das Interface wg0 angenommen und gezielt in die DMZ geleitet, wo ausschließlich der HTTPS-Zugriff auf die Nextcloud erlaubt ist, siehe Abbildung 18. Da keine Route vom VPN in das LAN existiert, ist ein Zugriff externer Nutzer auf interne Systeme technisch ausgeschlossen.

Der Aufbau der VPN-Verbindung wird von der OPNsense initiiert. Sie stellt die Verbindung aktiv über ihr WAN-Interface her, sodass am Schulrouter keinerlei Portfreigaben erforderlich sind. Der VPS nimmt die eingehende Verbindung lediglich entgegen und fungiert als stabiler Endpunkt. Durch diese klare Rollenverteilung, die eindeutigen Tunneladressen und das zentralisierte Routing entsteht eine transparente, sichere und leicht nachvollziehbare Lösung für den externen Zugriff.

4.10 Umsetzung des WireGuard-Tunnels zwischen VPS und OPNsense

Nachdem der externe Zugriff über den VPS vorbereitet war, wurde der WireGuard-Tunnel zwischen dem VPS und der OPNsense-Firewall eingerichtet. Dafür wurden auf beiden Systemen die notwendigen Schlüssel generiert und anschließend miteinander ausgetauscht, sodass eine gegenseitige Authentifizierung möglich war.

Nach der Konfiguration der jeweiligen WireGuard-Interfaces wurde der Tunnel aktiviert und die Verbindung erfolgreich hergestellt, siehe Abbildung 19. OPNsense übernahm dabei die Rolle des internen Endpunkts und leitete den eingehenden Datenverkehr aus dem Tunnel sicher in die DMZ weiter.

Ein externer Client verbindet sich über den Wireguard-Client mit dem WireGuard-Server auf dem VPS (über öffentliche-IP des VPS). VPS entschlüsselt die Pakete und weiß anhand der Peer-Konfiguration, dass die Pakete an OPNsense weitergeleitet werden sollen. Nur wenn der Public Key exakt zu einem konfigurierten Peer passt, wird der Peer akzeptiert und der Tunnel als aktiv markiert. Nach erfolgreicher Authentifizierung kann der VPS die Pakete entschlüsseln, anhand von AllowedIPs zuordnen und in den Tunnel zum OPNsense-WG-Interface (wg0) weiterleiten.

Durch die Anpassung der Routing-Einträge auf beiden Seiten konnte der gesamte Verkehr der externen Nutzer korrekt zur Nextcloud-Instanz geleitet werden. Mit dem stabil laufenden Tunnel stand nun eine zuverlässige und verschlüsselte Verbindung zur Verfügung, die den externen Zugriff vollständig vom Schulnetz trennt und gleichzeitig einen sicheren Zugang ermöglicht.

Die Routing-Statusseite der OPNsense zeigt die korrekte Zuordnung des Tunnelnetzes. Der Eintrag 10.100.100.0/24 (wg0) weist das gesamte VPN-Netz dem WireGuard-Interface zu, während die Adresse des VPS 10.100.100.1(wg0) als Peer eindeutig erkennbar ist. Die OPNsense selbst nutzt die Tunneladresse 10.100.100.3, welche intern über das Loopback-Interface verwaltet wird.

Durch diese Konfiguration wird der gesamte VPN-Verkehr zuverlässig in die DMZ geleitet, ohne dass eine Verbindung in das interne LAN möglich ist. Da die Interface-Zuordnung und die Firewall-Regeln die Trennung vollständig abbilden.

4.11 Firewall- und Routing-Anpassungen für den VPN-Tunnel

Nachdem der WireGuard-Tunnel erfolgreich eingerichtet worden war, wurden in der OPNsense die notwendigen Firewall- und Routing-Anpassungen vorgenommen, um den VPN-Datenverkehr sicher zur Nextcloud-Instanz in der DMZ zu leiten. Der VPN-Verkehr wurde so freigegeben, dass ausschließlich die für den Betrieb erforderlichen Dienste – insbesondere HTTPS zur Nextcloud und DNS – erreichbar sind. Alle anderen Verbindungen bleiben konsequent blockiert.

Die Routing-Tabelle weist das Tunnelnetz 10.100.100.0/24 eindeutig dem WireGuard-Interface zu. Statische Routen sorgen dafür, dass Anfragen externer Nutzer korrekt in Richtung DMZ weitergeleitet werden. Gleichzeitig verhindert die restriktive Regelbasis auf dem WireGuard-Interface, dass VPN-Clients Zugriff auf das interne LAN erhalten. Das bestehende NAT der OPNsense stellt sicher, dass Antworten der Nextcloud korrekt an die VPN-Clients zurückgesendet werden.

Zur Überprüfung der Netztrennung wurden gezielte Tests von der Nextcloud-VM durchgeführt. Weder Ping-Anfragen noch Portscans in Richtung LAN erzielten eine Antwort. Die Firewall-Logs dokumentierten ausschließlich Block-Einträge für Zugriffsversuche aus der DMZ oder vom VPN in Richtung LAN, während zulässiger HTTPS-Verkehr korrekt verarbeitet wurde. Damit ist die vollständige Isolation der DMZ nachweislich gewährleistet.

Zusätzlich wurden die OPNsense-Logs ausgewertet, um sicherzustellen, dass die Sicherheitsarchitektur konsistent umgesetzt wurde. Die Ergebnisse bestätigten, dass unerlaubte Kommunikationsversuche zuverlässig blockiert und erlaubte Verbindungen erwartungsgemäß weitergeleitet wurden. Für den zukünftigen Betrieb empfiehlt sich der Einsatz eines zentralen Logging- oder Monitoring-Systems, um sicherheitsrelevante Ereignisse dauerhaft zu überwachen und Anomalien frühzeitig zu erkennen.

5 Testphase

5.1 Funktionstests

Test 1: Zugriff aus dem LAN auf die Nextcloud (erwartet: erlaubt)

Ziel: Sicherstellen, dass LAN-Clients die Nextcloud über HTTPS erreichen.

Tool: curl, Browser

Ergebnis: http 200 OK, Antwortzeit stabil, siehe Abbildung 20.

Test 2: Zugriff aus der DMZ auf das interne LAN erwartet: blockiert

Ziel: Nachweis der Isolation der DMZ

Tools: ping, nmap

Ergebnis: Keine Antwort, Ports vollständig blockiert, siehe Abbildung 21.

Test 3: Externer Zugriff über WireGuard (erwartet: erlaubt)

Ziel: Überprüfung des sicheren externen Zugriffs.

Tools: WireGuard-Client, OPNsense „Handshake “-Status

Nextcloud über https://cloud.cbm.local erreichbar

Ergebnis: VPN-Verbindung stabil, Datenverkehr korrekt in die DMZ weitergeleitet, siehe Abbildung 22.

Testfall 4: VPN-Client versucht Zugriff auf das interne LAN (blockiert)

Ziel: Nachweis, dass AllowedIPs korrekt gesetzt sind.

Ergebnis: Blockiert, siehe Abbildung 23.

Testfall 5: Funktionstests der Nextcloud-Plattform

Ziel: Überprüfung zentraler Anwendungskomponenten.

Tools: Browser, Nextcloud-Webinterface, siehe Abbildung 24.

Test 6: TLS-/Zertifikat-Test

Ziel: Sicherstellen, dass Verschlüsselung korrekt eingesetzt wird

Ergebnisse:

- Schulungsrechner (interne CA installiert): keine Warnmeldung
- Privates Gerät: Zertifikatswarnung aufgrund nicht Überprüfbarkeit der Authentizität (interne CA nicht bekannt) Verbindung ist trotzdem technisch verschlüsselt und sicher, siehe Abbildung 25.

Test	Soll	Ist	Ergebnis
LAN → Nextcloud	erlaubt	erfolgreich	✓
DMZ → LAN	blockiert	blockiert	✓
VPN → DMZ	erlaubt	erfolgreich	✓
VPN → LAN	blockiert	blockiert	✓
HTTPS-Zertifikat	intern OK	intern OK	✓
Nextcloud-Funktionen	funktional	erfolgreich	✓

Tabelle 5: Testergebnisse

5.2 Abschlussüberprüfung und Systemvalidierung

Im Rahmen der finalen Validierung wurden alle Netzwerkpfade, Firewall-Regeln sowie die interne Kommunikation zwischen LAN, DMZ und VPN erneut überprüft. Die Firewall-Logs bestätigten, dass ausschließlich definierter Verkehr zugelassen wurde. Auch die Systemressourcen des Proxmox-Hosts (CPU, RAM, Storage) wurden überwacht und zeigten eine stabile Auslastung im Normalbetrieb. Zusätzlich wurde die WireGuard-Verbindung über längere Zeit getestet, um mögliche Paketverluste oder Instabilitäten auszuschließen. Die Nextcloud-Anwendung wurde im Administratorbereich auf Fehlermeldungen und Hintergrundprozesse (Cron-Jobs) geprüft – ohne Befunde. Alle Tests bestätigten, dass die implementierte Lösung stabil, sicher und vollständig betriebsbereit ist.

5.3 Abnahme des Projekts

Nach Abschluss aller Implementierungs- und Testarbeiten wurde das Projekt der internen IT-Abteilung zur Abnahme übergeben. Im Rahmen der Abnahme wurden sämtliche definierten Funktionen überprüft, darunter die Erreichbarkeit der Nextcloud-Plattform aus dem LAN, der erfolgreiche externe Zugriff über den WireGuard-Tunnel sowie die ordnungsgemäße Umsetzung der Sicherheitsmaßnahmen. Die IT-Abteilung bestätigte, dass die Plattform stabil läuft und die Lösung zuverlässig in die bestehende Infrastruktur integriert werden konnte. Zudem wurde die klare Trennung zwischen LAN und DMZ sowie die DSGVO-konforme Datenhaltung positiv hervorgehoben.

6 Fazit

Mit der Umsetzung der Nextcloud-Plattform in einer Proxmox-Umgebung und der Absicherung durch OPNsense sowie einen WireGuard-Tunnel wurde eine moderne, sichere und vollständig DSGVO-konforme Lösung geschaffen.

Die neu eingeführte DMZ-Struktur trennt interne und externe Bereiche sauber voneinander, während HTTPS und zusätzliche Sicherheitsmechanismen wie 2FA und Security-Header zu einem hohen Schutzlevel beitragen. Sowohl der interne Zugriff über das LAN als auch der externe Zugriff über den VPN-Tunnel funktionieren zuverlässig und stabil. Die Plattform erfüllt alle definierten Anforderungen und bietet der CBM Projektmanagement GmbH eine langfristige, skalierbare und klar administrierbare Kollaborationslösung

6.1 Soll-/Ist-Vergleich

Die im Projekt definierten Ziele wurden vollständig erreicht. Die Nextcloud-Plattform wurde wie geplant in einer eigenen DMZ bereitgestellt und durch die OPNsense-Firewall sicher vom internen Netzwerk getrennt. Alle Daten liegen im eigenen System und erfüllen damit die DSGVO-Anforderungen.

Der verschlüsselte Zugriff über HTTPS sowie der externe Zugang über den WireGuard-Tunnel funktionieren zuverlässig und ohne Portfreigaben im Schulnetz. Auch die Benutzer- und Gruppenverwaltung sowie die geplanten Sicherheitsmaßnahmen wurden wie vorgesehen umgesetzt. Insgesamt entspricht der erreichte Ist-Zustand dem Soll-Konzept.

6.2 Lessons Learned

Während der Umsetzung wurde deutlich, wie wichtig eine strukturierte Netzwerkplanung und eine klare Trennung von Sicherheitszonen ist. Die Einführung der DMZ und der Aufbau der Firewall-Regeln erforderten ein genaues Verständnis der Datenflüsse und erleichterten später die Fehlersuche erheblich. Zudem zeigte sich, wie wertvoll Open-Source-Technologien wie Proxmox, OPNsense und Nextcloud sind, da sie eine hohe Flexibilität bieten und dennoch professionellen Sicherheitsanforderungen entsprechen. Ein weiterer zentraler Lernpunkt war die Einrichtung des externen VPN-Zugangs über einen VPS, da dieser Lösungsweg eine kreative Alternative darstellt, wenn Portfreigaben in einem Schulnetz nicht möglich sind. Insgesamt hat das Projekt gezeigt, dass sorgfältige Planung, saubere Dokumentation und iterative Tests entscheidend für einen stabilen und sicheren Betrieb sind.

6.3 Ausblick

Die geschaffene Infrastruktur bietet eine solide Basis, die in Zukunft weiter ausgebaut werden kann. Denkbar wären zusätzliche Sicherheitsfunktionen wie Intrusion-Detection-Systeme, automatisierte Backups auf ein zweites Storage-System oder Monitoring mittels Prometheus und Grafana. Auch könnten weitere Dienste in der DMZ integriert werden, etwa ein internes GitLab oder ein Kollaborationstool wie OnlyOffice, das direkt in Nextcloud eingebunden wird.

Für den externen Zugriff könnte langfristig ein zweiter VPS als Ausfallsicherung dienen. Die Struktur ist bewusst modular aufgebaut und unterstützt zukünftige Erweiterungen ohne große Umbaumaßnahmen. Dadurch bleibt die Umgebung nicht nur sicher, sondern auch nachhaltig und flexibel für zukünftige Anforderungen.

Für den weiteren Betrieb wird empfohlen, eine verbindliche Backup- und Restore-Strategie festzulegen, da diese für den sicheren Betrieb einer Cloud-Plattform zwingend erforderlich ist. Dies umfasst sowohl die regelmäßige Sicherung der Datenbank als auch der Nextcloud-Dateistruktur.

Quellen

1- **Proxmox VE – Offizielle Dokumentation**
https://www.proxmox.com/en/proxmox-virtual-environment/documentation

2- **OPNsense – Offizielle Dokumentation**
https://docs.opnsense.org

3- **WireGuard – Offizielle Dokumentation**
https://www.wireguard.com/quickstart/

4- **Nextcloud – Offizielle Administrator-Dokumentation**
https://docs.nextcloud.com/server/latest/admin_manual/

5- **OpenSSL – Offizielle Dokumentation**
https://docs.openssl.org/master/

6- **draw.io / diagrams.net – Offizielle Seite**
https://www.diagrams.net

7- **Debian – Offizielle Dokumentation**
https://www.debian.org/doc/

8- **PuTTY – Offizielle Projektseite**
https://www.putty.org/

9- **Amazon Web Services**
https://aws.amazon.com/de/

Anhang

A.1 Detaillierte Zeitplanung

Analysephase	**7h**
Ist-Analyse	2h
Anforderungsaufnahme “Fachgespräche, Darw.io-Diagramm“	2h
Soll-Konzept	2h
Wirtschaftlichkeitsanalyse	1h
Entwurfsphase	3h
Technischer Entwurf der Zielumgebung	1h
Detailkonzept der Umsetzung	1h
Ressourcenplanung	1h
Implementierungsphase	**18h**
Installation Einrichtung der Proxmox-Umgebung	1h
Installation & Einrichtung OPNsense-Firewall	2h
Routing-Konfiguration & Firewall-Regeln	2h
Installation der Nextcloud-Server-VM in der DMZ	2h
HTTPS-Konfiguration für Nextcloud (Self-Signed Zertifikat / interne CA)	1h
Nextcloud Grundkonfiguration	1h
Sicherheitshärtung der Nextcloud	1h
Einrichtung des externen Zugriffs über VPS und WireGuard	1h
Umsetzung des WireGuard-Tunnels zwischen VPS und OPNsense	1h
Firewall- und Routing-Anpassungen für den VPN-Tunnel	2h
Funktionstests	1h
Abschlussüberprüfung und Systemvalidierung	1h
Abnahme	1h
Abnahme durch die Fachabteilung	1h
Dokumentation	**12h**
Projektdokumentation	10
Benutzerdokumentation	2h
Stunden gesamt	**40h**

Listing 1: detaillierter Zeitplan

A.2 Verwendete Ressourcen

Hardware:

Proxmox-Server (bestehendes System)

Wird als Virtualisierungsplattform genutzt und stellt die VMs für OPNsense und Nextcloud bereit.

Büroarbeitsplatz

Für Planung, Umsetzung, Verwaltung und Dokumentation des Projekts.

Externer VPS (Virtual Private Server)

Dient als öffentlich erreichbarer Endpunkt für den WireGuard-VPN-Tunnel.

Software:

Proxmox VE –Virtualisierungsplattform zur Bereitstellung der Serverumgebung

OPNsense Firewall – für Netztrennung, Firewall-Regeln, Routing und VPN

Nextcloud – Kollaborations- und Dateiablageplattform

WireGuard – VPN-Lösung für sicheren externen Zugriff

Debian / Ubuntu Linux – Betriebssysteme für Nextcloud und OPNsense

OpenSSL / interne CA – zur Erstellung und Verwaltung von HTTPS-Zertifikaten

Browser (Chrome / Firefox) – Zugriff auf Proxmox, OPNsense und Nextcloud

Draw.io – Erstellung von Netzwerk- und Architekturdiagrammen

SSH-Client (z. B. PuTTY / Windows Terminal) – Verwaltung und Konfiguration der Server

Notepad / Office-Tools – für Dokumentation und Projektnotizen

Personal:

IT-Abteilung

Definition der Anforderungen, fachliche Abstimmung und Abnahme der Lösung

Projektverantwortlicher (Fachinformatiker Systemintegration)

Planung, Installation, Konfiguration, Testing und Dokumentation des gesamten Sytems.

Dozent*innen / Teilnehmende (Endnutzer)

Test und spätere Nutzung der Nextcloud-Plattform

Listing 2: verwendete Ressourcen

A.3 Netzwerkarchitektur – Gesamtübersicht

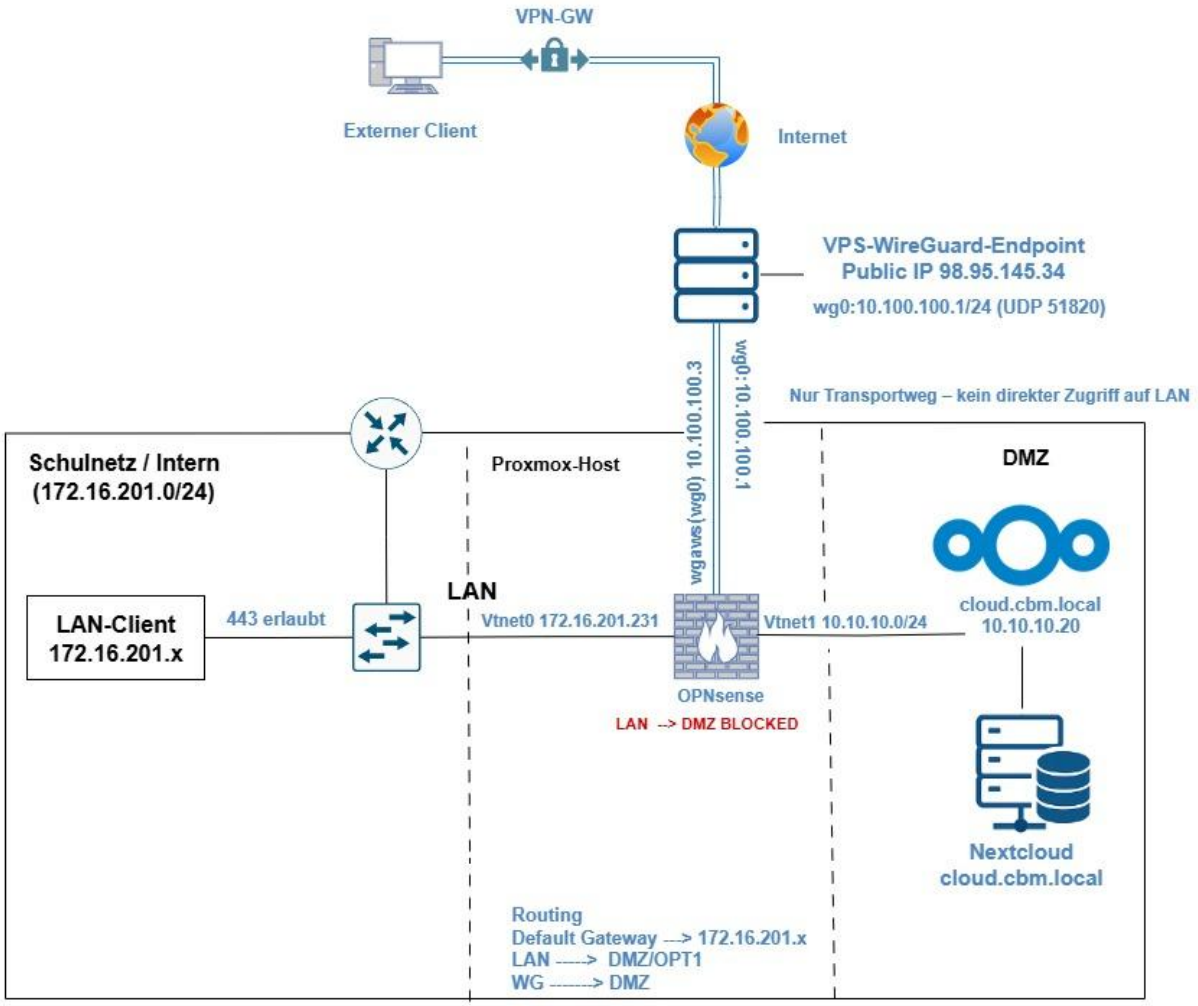

Abbildung 1: Netzwerkarchitektur

A.4 Firewall- und Routing-Flow

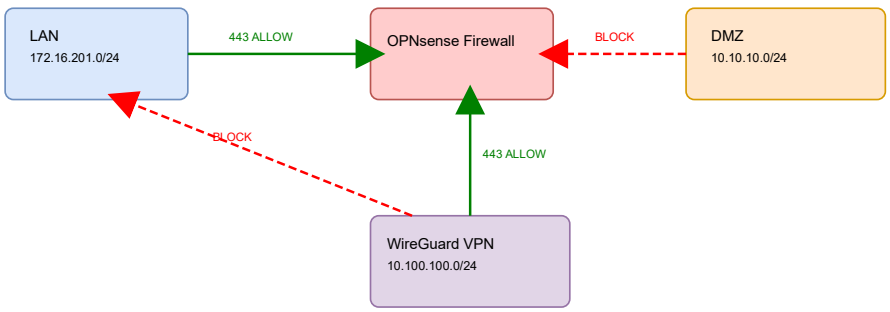

Abbildung 2: Firewall- und Routing-Flow

A.5 Proxmox-Weboberfläche nach der Installation

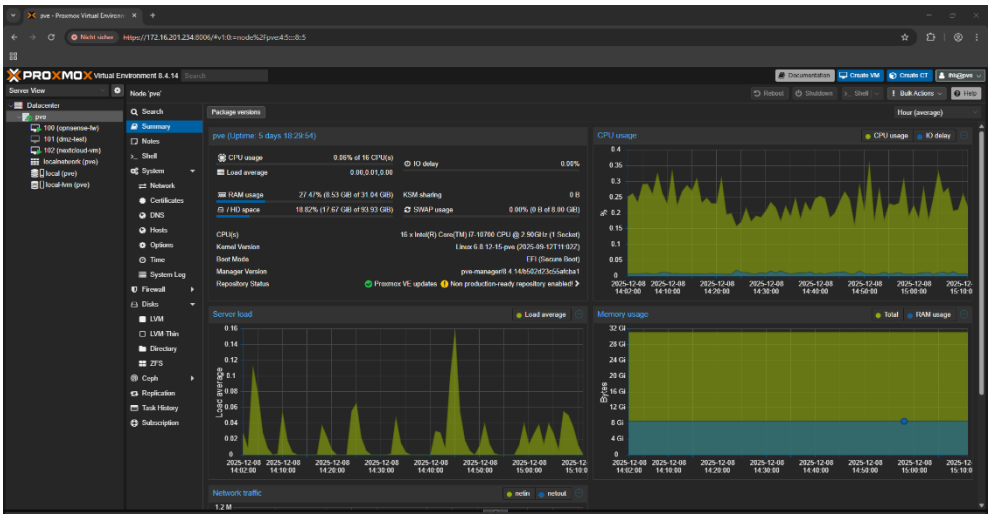

Abbildung 3: Proxmox Weboberfläche

A.6 Konfiguration der Netzwerk-Bridges in Proxmox

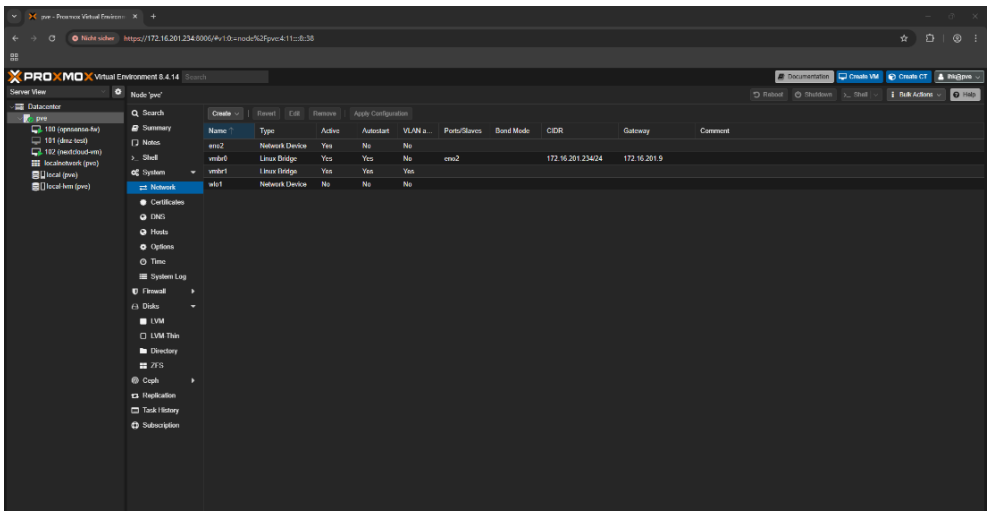

Abbildung Test 4: Netzwerkbridges in Proxmox

A.7 Interface Assigniert (Zuordnung der Netzwerkkarten)

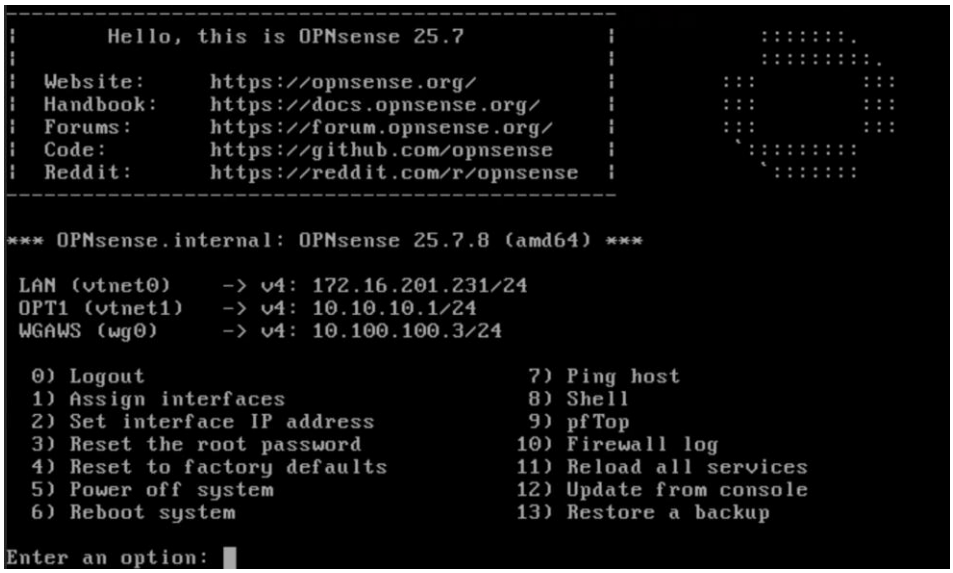

Abbildung 5: Zuordnung Netzwerkkarten

A.8 Zuordnung der Netzwerkkarten der OPNsense-Firewall

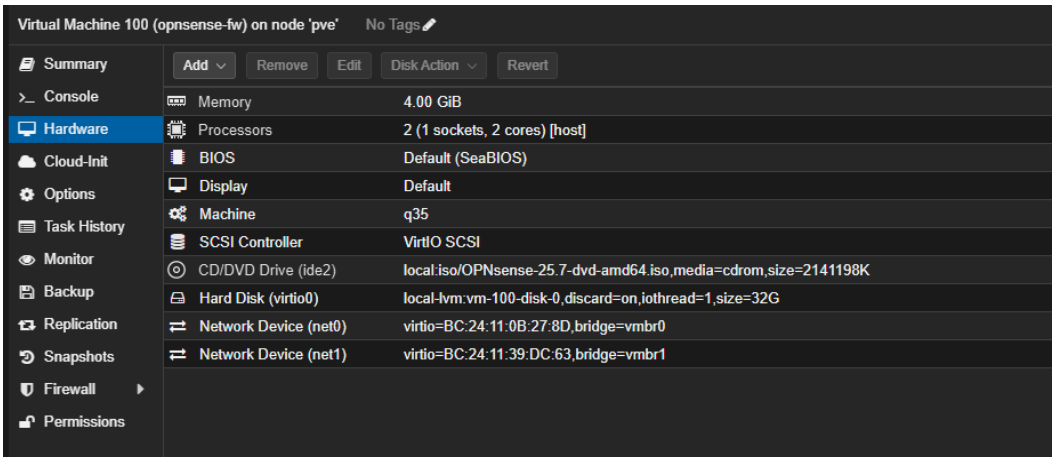

Abbildung 6: OPNsense Netzwerkkarten Zuordnung

A.9 Firewall-Regeln LAN Allow LAN → Nextcloud

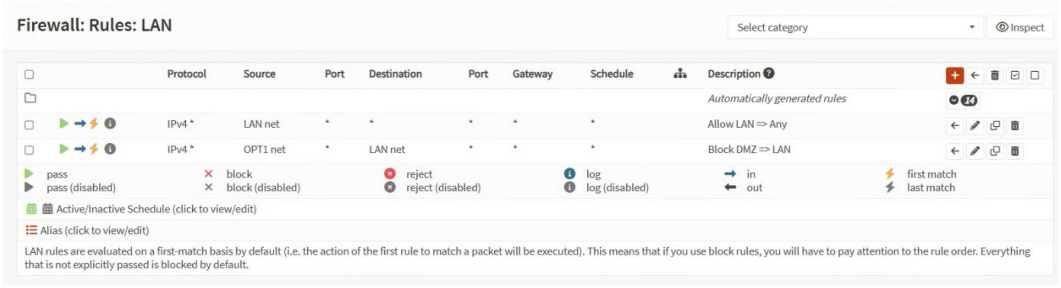

Abbildung 7: Firewall Regel LAN

A.10 Firewall-Regeln des DMZ-Interfaces (OPT1)

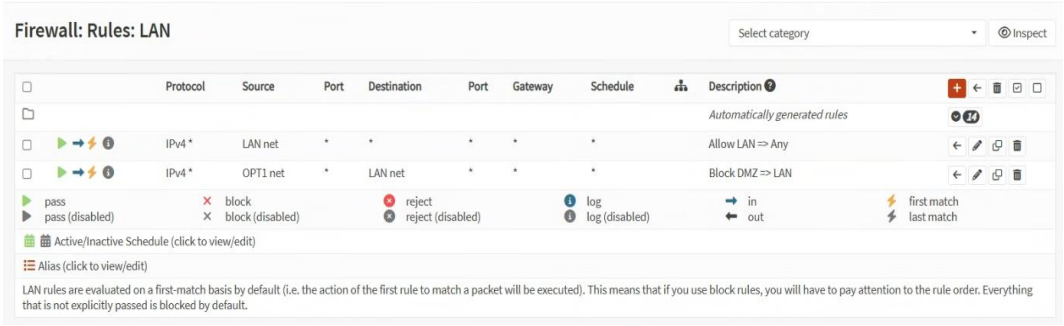

Abbildung 8: Firewall Regel DMZ

A.11 Routing-Tabelle der OPNsense

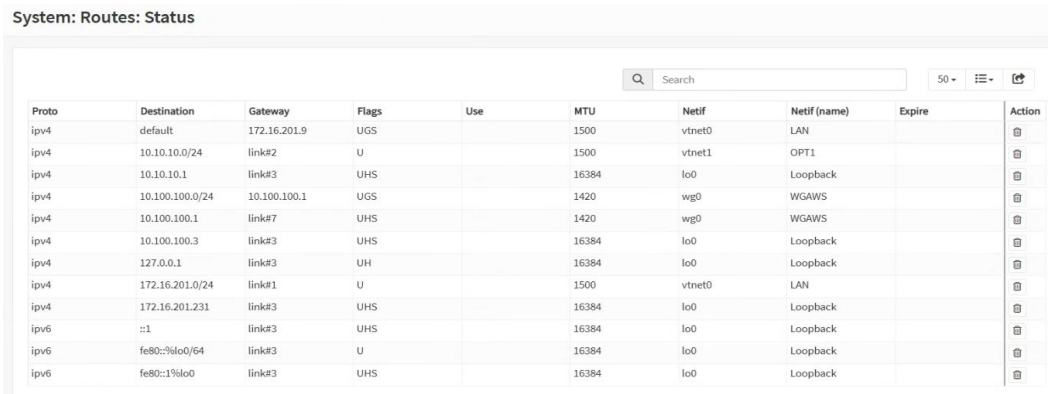

Abbildung 9: OPNsense Routingtabelle

A.12 PostgreSQL installiert & Dienst aktiviert

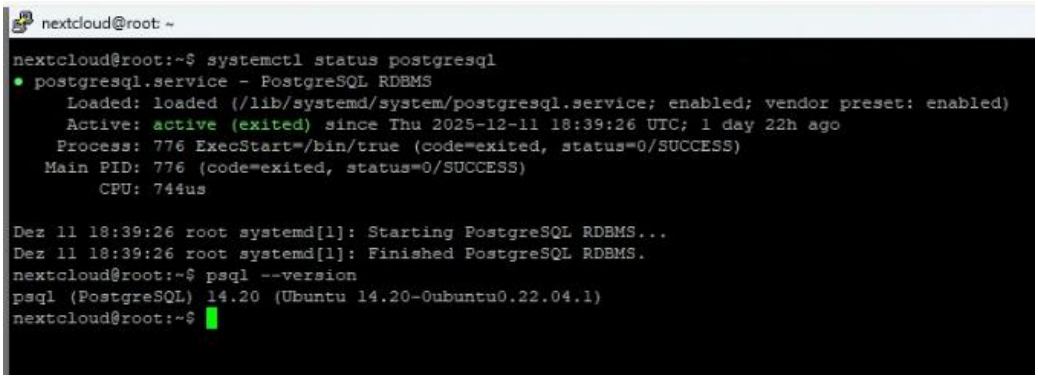

Abbildung 10: PostgreSQL

A.13 Erfolgreich aktivierte HTTPS-Verbindung zur Nextcloud-Instanz

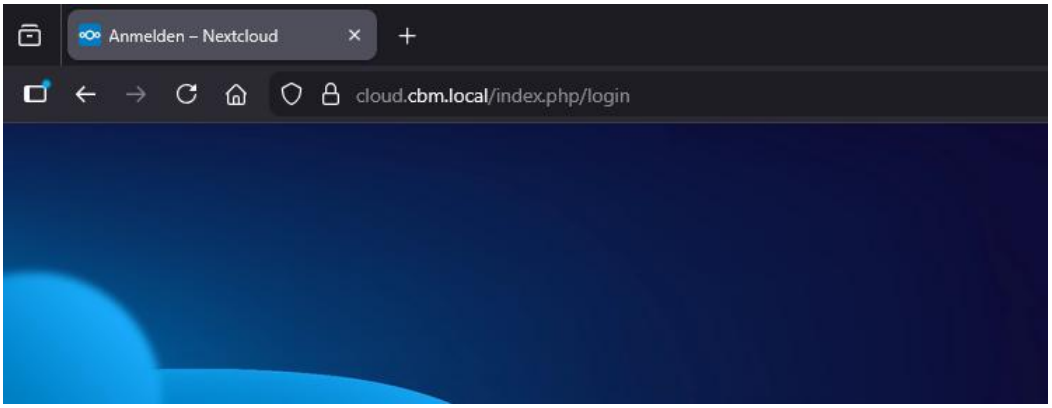

Abbildung 11: HTTPS Nexctloud Verbindung

A.14 DNS-Auflösung für interne & VPN-Zugriffe

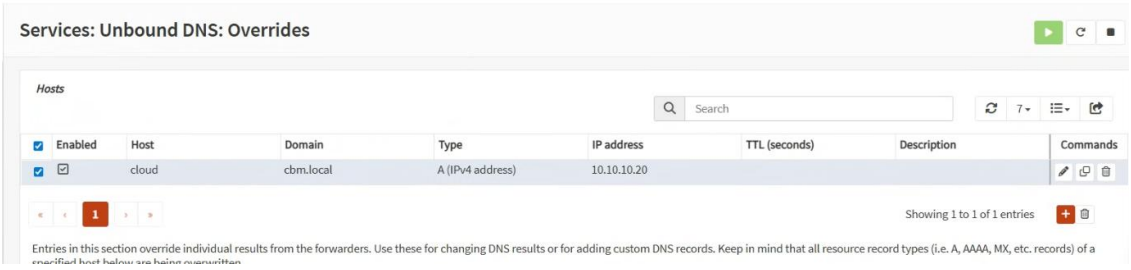

Abbildung 12: DNS Konfiguration

A.15 Systemeinstellungen der Nextcloud mit aktivierten Standard-Apps

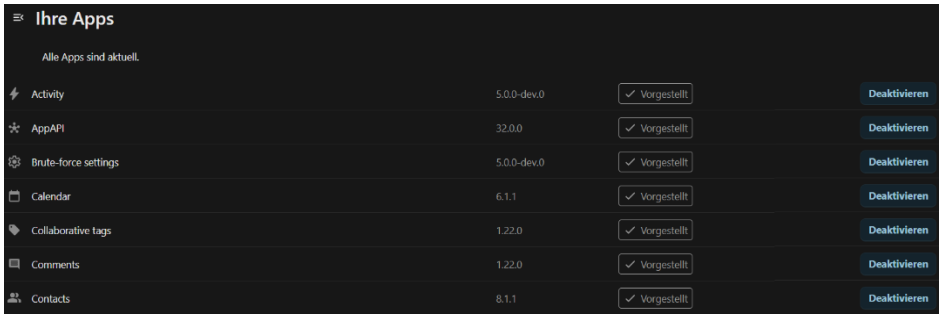

Abbildung 13: Nextcloud System Konfiguration

A.16 Benutzer- und Gruppenverwaltung der Nextcloud

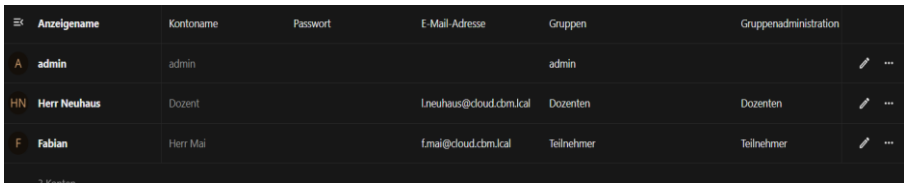

Abbildung 14: Benutzer und Gruppenverwaltung

A.17 Nextcloud Sicherheitsübersicht nach der Umsetzung der Härtungsmaßnahmen

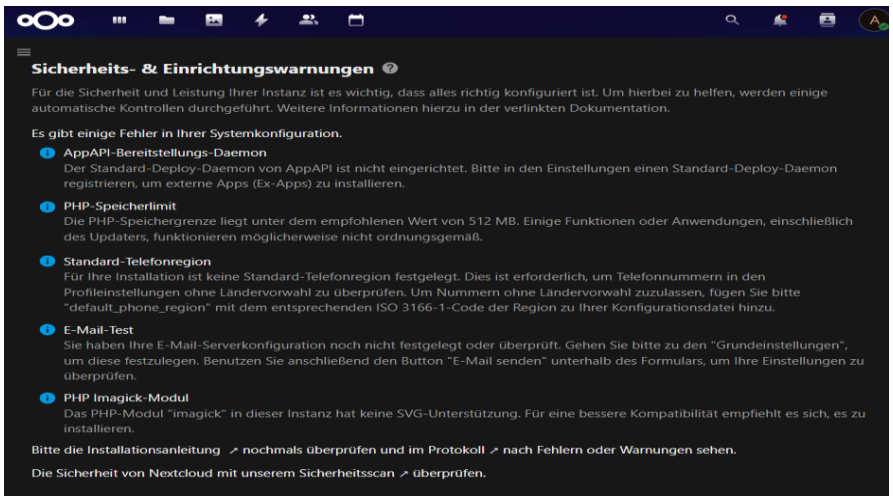

Abbildung 15: Sicherheitsübersicht Nextcloud

A.18 Aktivierte Zwei-Faktor-Authentifizierung für administrative Konten

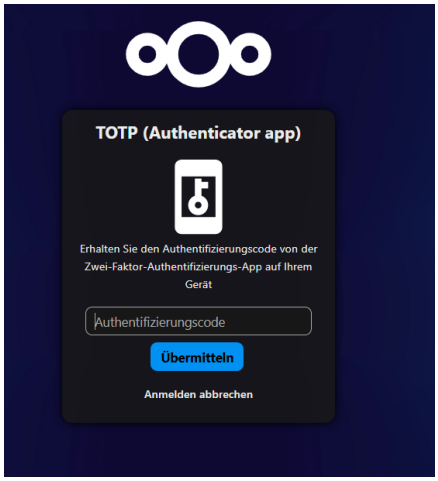

Abbildung 16: 2MFA

A.19 Aktivierter Fail2ban-Dienst zur Abwehr von Brute-Force-Angriffen

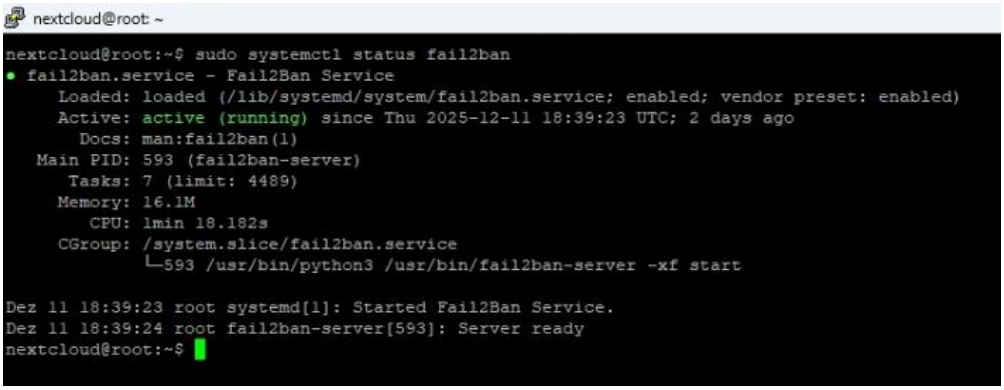

Abbildung 17: Fail2ban-Dienst

A.20 Firewall-Regeln für WireGuard (wg0 Interface)

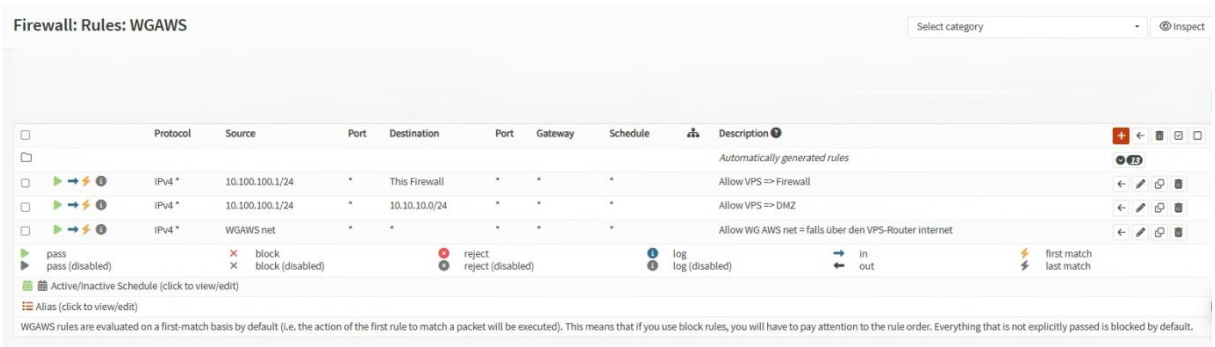

Abbildung 18: Firewall Regel WireGuard

A.21 OPNsense WireGuard-Statusseite (wg0 aktiv, Peer verbunden)

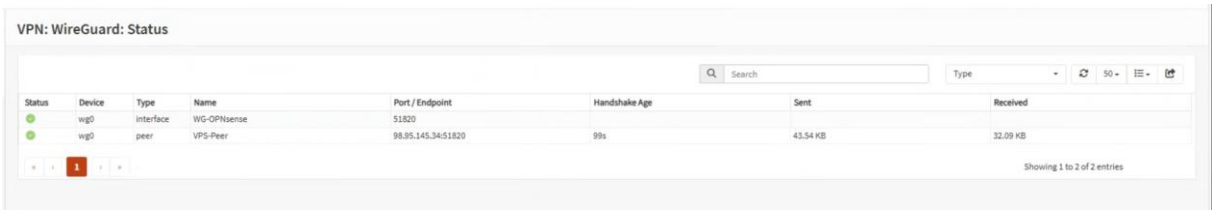

Abbildung 19: WireGuard Statusseite

A.22 Test: 1: Zugriff aus dem LAN auf die Nextcloud

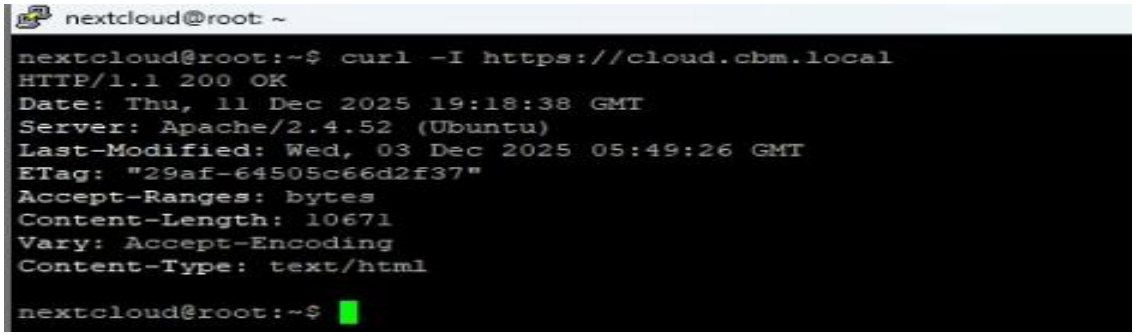

Abbildung 20: Test:1

A.23 Test: 2 Nachweis der Isolation der DMZ

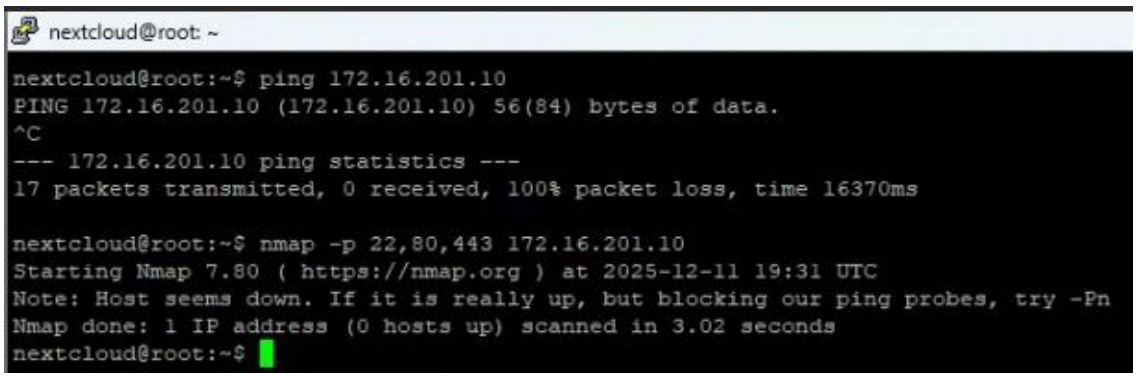

Abbildung 21: Test:2

A.24 Test: 3 Überprüfung des sicheren externen Zugriffs

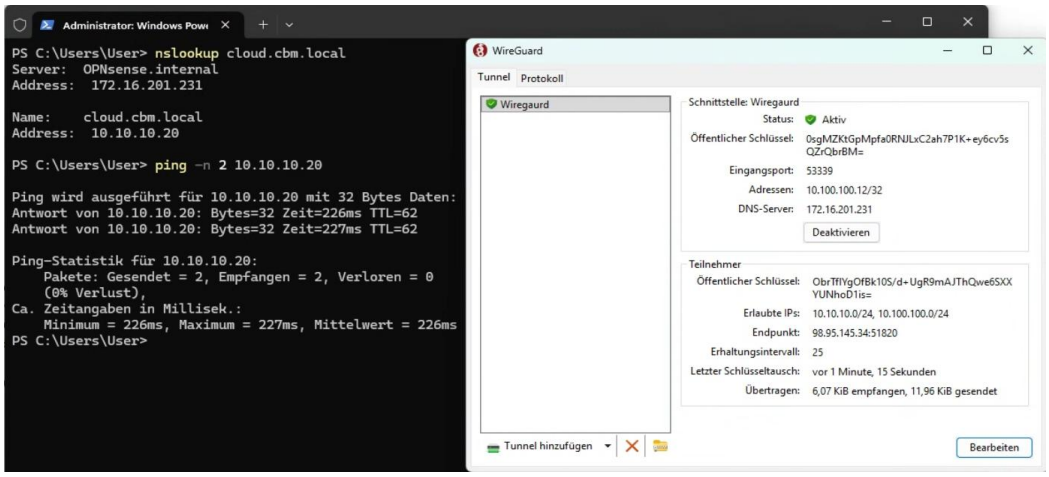

Abbildung 22: Test:3

A.25 Test: 4 VPN-Client versucht Zugriff auf das interne LAN (blockiert)

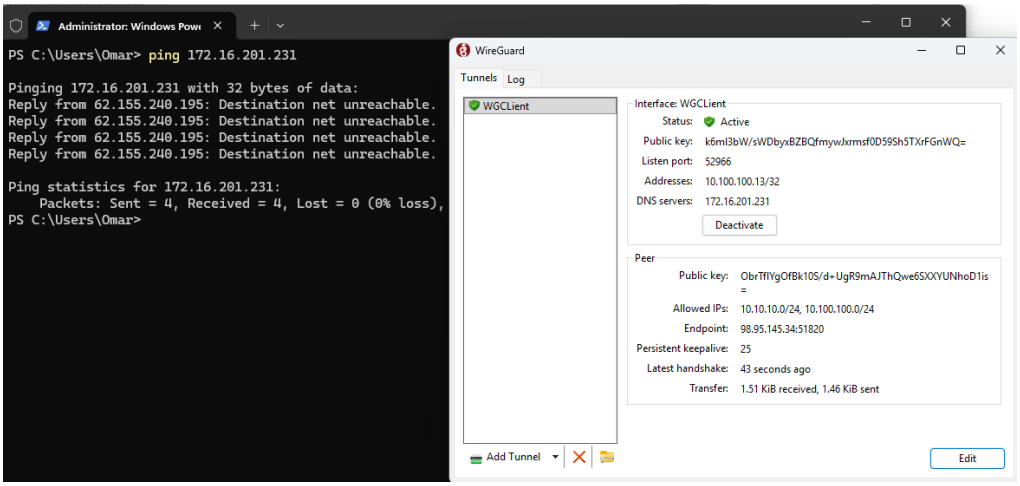

Abbildung 23: Test:4

A.26 Test: 5 Funktionstests der Nextcloud-Plattform

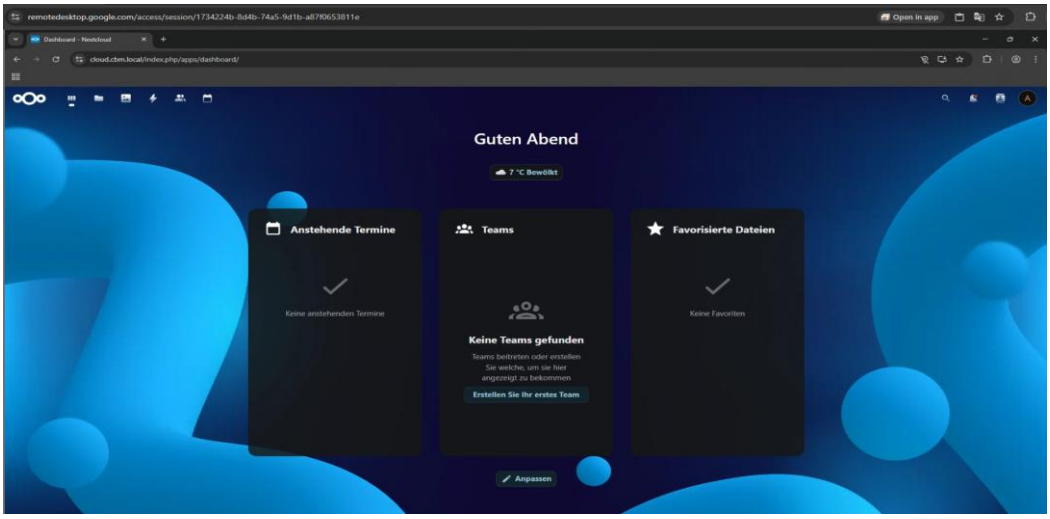

Abbildung 24: Test:5

A.27 Test: 6 Privates Gerät: Zertifikatswarnung & Schulungsrechner: Zertifikatswarnung keine Warnmeldung

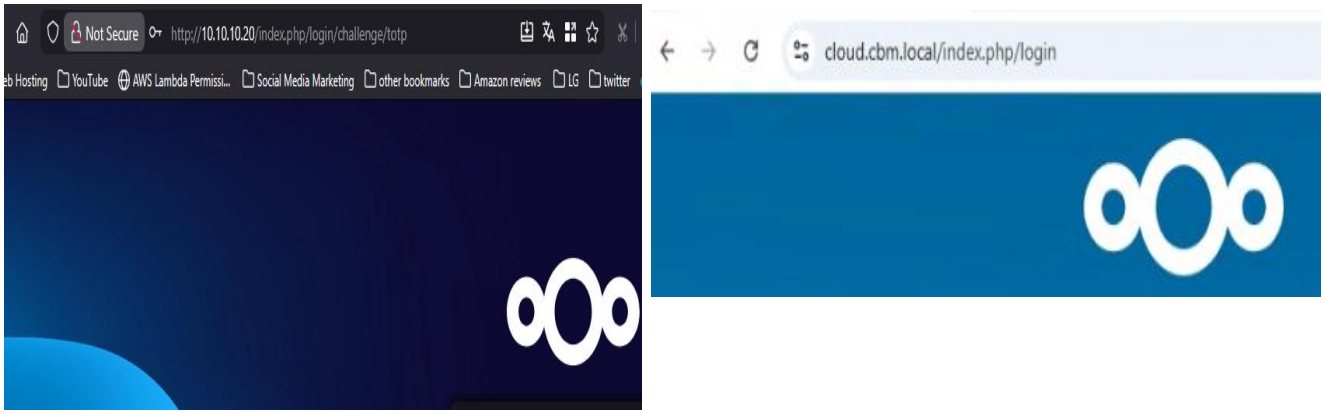

Abbildung 25: Test:6