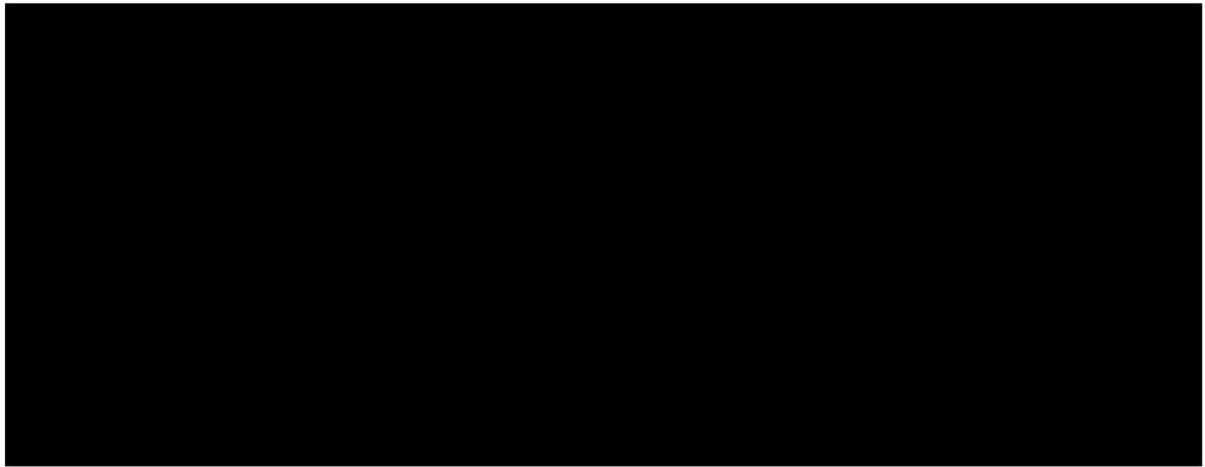


**Implementierung einer 2-stufigen Firewall mit DMZ zur
externen Bereitstellung eines Fileservers**

Abschlussprojekt Sommer 2025
Fachinformatikerin Systemintegration



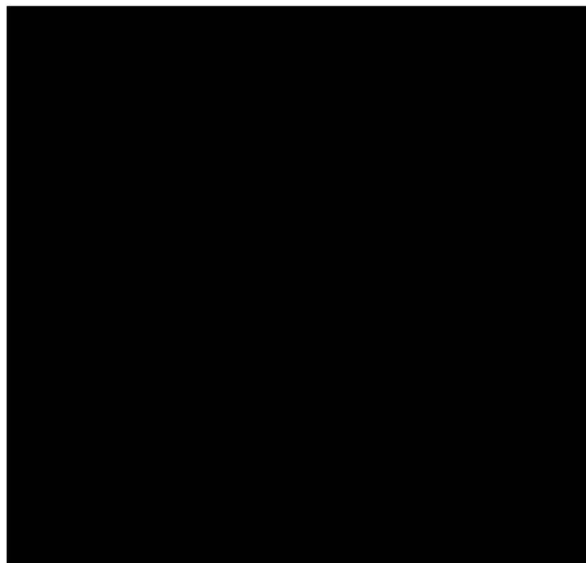
Prüfungsteilnehmerin:

Johanna Elisabeth Krüger

Geburtsdatum:

Ausbildungsbetrieb:

Projektbetreuer:



Inhaltsverzeichnis

Glossar.....	II
Tabellenverzeichnis.....	IV
1 Einführung.....	1
1.1 Projektumfeld.....	1
1.2 Ist-Zustand.....	1
2 Planungsphase	2
2.1 Soll-Konzept	2
2.2 Produktauswahl	3
2.2.1 Nutzwertanalyse.....	3
2.2.1.1 Auswertung Nutzwertanalyse.....	5
2.3 Ressourcenermittlung	5
2.3.1 Projektkostenberechnung.....	5
2.3.2 Fixkostenberechnung.....	6
2.3.2.1 Stromkosten.....	6
2.3.2.2 Wartungskosten	6
2.3.2.3 Monatliche Fixkosten	6
2.4 Erstellung eines Netzwerkplans	6
2.4.1 Adressbereiche.....	7
3 Durchführungsphase.....	7
3.1 Installation und Ersteinrichtung der Firewall.....	7
3.2 Einbau ins Rechenzentrum	8
3.2.1 Firewalls zugänglich machen	8
3.3 Konfiguration der Firewalls.....	9
3.3.1 DNS- und NTP-Delegierung.....	9
3.3.2 VPN konfigurieren.....	9
3.3.2.1 Server-Zertifikat anlegen.....	9
3.3.2.2 OpenVPN-Server konfigurieren.....	9
3.3.2.3 VPN-Nutzer anlegen	10
3.4 DMZ-Netz anlegen.....	10
3.4.1 ESXi-Hosts.....	10
3.4.2 Switches	11
3.4.3 Firewall	11
3.5 Externen Zugriff einrichten für die DMZ.....	11
3.6 Fileserver anpassen.....	12
3.6.1 Berechtigungen anpassen.....	12
4 Durchführung von Tests.....	13

5	Abschlussphase.....	13
5.1	Soll-Ist-Abgleich.....	13
	Literaturverzeichnis	i
	Anlage.....	i

Glossar

AD

Active Directory.....*Organisation von Benutzern, Gruppen und Computern*

BOGON.....*Öffentliche IPs bzw. Netzwerke, die nicht registriert sind*

CA

Certificate Authority

Zertifizierungsstelle

CN

Common Name.....*Name für den das Zertifikat ausgestellt wurde*

DAC-Kabel

Kupferkabel mit SFP-Anschlüssen

DC

Domain Controller.....*Authentifizierungsserver für Benutzer und Computer*

Diffie-Hellman.....*Symmetrisches Verfahren zum Schlüsselaustausch*

DMZ

Demilitarisierte Zone.....*Dienste sowohl im LAN als auch im WAN zugänglich machen*

DNS

Domain Name System.....*Übersetzt URL-Anfragen zu IP-Adressen*

ESXi.....*VMware Hypervisor*

FTP

File Transfer Protocol.....*Protokoll zum Austausch von Daten*

GPO

Group Policy Object.....*Gruppenrichtlinien*

GUI

Graphical User Interface.....*Benutzeroberfläche*

IDS

Intrusion Detection System

Überwacht verdächtigen Netzwerkverkehr

IPS

Intrusion Prevention System

Weißt verdächtigen Datenverkehr ab

ISP

Internet Service Provider

Internetanbieter

LACP.....*Protokoll, welches automatische Aushandlung macht*

LAGG

Link Aggregation..... *Physische Ports werden virtuell zu einem zusammengeschlossen*

LC

Lucent Connector*kleine Anschlüsse eines Glasfaserkabels*

LWL

Lichtwellenleiter*Glasfaserkabel*

NGFW

Next Generation Firewall*Beinhaltet mehr als die üblichen Firewall-Funktionen*

NTP

Network Time Protocol.....*Protokoll, um Geräte über das Internet mit der Uhrzeit zu synchronisieren*

On Premise *Dienste werden selbst gehostet*

OpenSource.....*Frei zugängliche Software*

OSPF

Open Shortest Path First*Routingprotokoll*

pfSense.....*Paketfilter Firewall-Distribution*

Postinstall.....*Übernimmt Einrichtungsaufgaben nach Installation*

Rack.....*Schrank im Rechenzentrum, in dem Server und Netzwerkgeräte eingebaut sind*

Registry..... *Konfigurationsdateien von Windows*

RFC1918..... *Private IP Adress-Bereiche*

RSA

Rivest-Shamir-Adleman.....*asymmetrischer Verschlüsselungsalgorithmus*

RTO

Recovery Time Objective..... *Zeit, die ein System maximal ausfallen darf*

SaaS

Software as a Service.....*Anwendung wird von Dritten über das Internet bereitgestellt*

SFP

Small Form-Factor Pluggable*Anschlussmodul für Netzwerkverbindungen*

SFTP

SSH File Transfer Protocol*Dateiübertragung über FTP mit SSH*

SHA-256

Secure Hash Algorithm.....*Hashfunktion, die einen 256 bit langen Wert ausgibt*

SPI

Stateful Packet Inspection*Verwaltet Netzwerkzugriffe mithilfe von Zustandstabellen*

SSH

Secure Shell *Protokoll, um sicher über das Netzwerk auf Geräte zuzugreifen*

Storage	<i>Speichermedium bzw. Speichersystem</i>
Transfernetz.....	<i>Verbindet zwei Router miteinander</i>
TrueNAS	<i>OpenSource Betriebssystem für NAS, bietet Speicherdienste</i>
vCenter	<i>Verwaltungsprogramm für VMware</i>
VLAN-Tagging.....	<i>VLAN bekommen eine ID zugewiesen</i>
VPN	
Virtual Private Network	<i>Netzwerkverbindung, die Daten verschlüsselt und IPs maskiert</i>
vSwitch.....	<i>Virtueller Switch auf ESXi-Hosts zur Verbindung VMs mit anderen Geräten</i>

Tabellenverzeichnis

Tabelle 1 Gegenüberstellung On Premise und SaaS	2
Tabelle 2 Nutzwertanalyse	4
Tabelle 3 Personalkostenberechnung	6
Tabelle 4 Stromkosten Supermicro	6
Tabelle 5 Monatliche Fixkosten	6

1 Einführung

In dieser Dokumentation werden, als Teil des IHK-Abschlussprojekts zur Ausbildung zur Fachinformatikerin für Systemintegration, alle Tätigkeiten erläutert, die im Rahmen des Projekts durchgeführt wurden.

Aus Gründen der besseren Lesbarkeit wird auf die Verwendung geschlechterspezifischer Sprache verzichtet und durchgehend die männliche Sprachform verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

1.1 Projektumfeld



Durch ein neues Ausbildungskonzept [REDACTED] soll den Auszubildenden die Möglichkeit gegeben werden, unter realen Bedingungen, abgegrenzt von der Produktivumgebung, Fähigkeiten im Umgang mit Virtualisierung, Aufsetzen und Verwalten von Servern zu erhalten. Als Unterstützung für diese Idee wurde eine Azubi-Testumgebung konfiguriert, welche durch dieses Projekt erweitert werden soll. Das Projekt wird im Bereich [REDACTED] durchgeführt.

1.2 Ist-Zustand

Die Azubi-Testumgebung ist durch einen eigenen Internetzugang [REDACTED] umfassend von den Netzwerkumgebungen [REDACTED] getrennt. Sie wird durch eine Firewall geschützt, in dessen LAN die Komponenten der Umgebung liegen [Anhang I.1](#). Zu den Komponenten gehören:

- Eine Supermicro als Firewall mit pfSense Installation
- Ein vCenter, welches 4 ESXi-Hosts verwaltet
- Ein Server als Storage mit TrueNAS Installation
- Eine Synology als Backup Medium
- Zwei Switches (weitere genutzte Switches werden [REDACTED] verwaltet)

Im vCenter befinden sich sechs VMs, welche als Windows Server 2022 eine Domänenstruktur bereitstellen. Diese besteht aus:

- Zwei redundanten Domänencontrollern mit DNS-Service und Zertifikatsstelle
- Zwei Fileservern (Benutzerprofile und Benutzerdaten)
- Einem Terminalserver mit einem Broker

Da die Testumgebung nicht extern erreichbar ist, können die Auszubildenden nur über eine interne Verbindung auf ihre Daten zugreifen. Da jedoch ein Zugang zu den Daten auch während der Berufsschulzeit für die Auszubildenden nützlich sein kann, soll der Zugriff von außen ermöglicht werden.

2 Planungsphase

Durch die vielen verschiedenen Anforderungen, die bei einer Bereitstellung von Daten im Internet erfüllt sein müssen, gab es mit einem Administrator [REDACTED] im Vorhinein ein Beratungsgespräch hinsichtlich der Umsetzung des Vorhabens.

In der Vorbesprechung wurden durch den Administrator folgende Punkte angebracht:

- Sicherheit des LANs muss stets gewährleistet sein
- Kostenfaktor Azubi-Testumgebung soll niedrig gehalten werden
- Verschlüsselte Datenübertragung soll sichergestellt werden

Nach dem Gespräch wurde der Zeitbedarf anhand eines Gantt-Diagramms ermittelt. [Anhang II.I](#)

2.1 Soll-Konzept

Damit Daten über das Internet bereitgestellt werden können, muss es ein Medium geben, welches die Daten teilt. In diesem Projekt steht die Auswahl dabei zwischen einer Cloud-Lösung und dem vorhandenen Fileserver.

Bei einer Cloud-Lösung gibt es verschiedene Möglichkeiten, diese zu implementieren. Diese sind On Premise und als SaaS. Beide Implementierungen bieten Vor- und Nachteile, welche in der folgenden Tabelle dargestellt sind:

	Pro	Kontra
SaaS	<ul style="list-style-type: none">– Geringerer administrativer Aufwand– Keine Anschaffungskosten für Hardware– Qualifizierter Support	<ul style="list-style-type: none">– Ungewissheit wo die Daten liegen, ggf. andere Länder und andere Datenschutzrechte– Ist sichere Datenübertragung gewährleistet?– Sicherheit der Rechenzentren gegenüber Angriffen– Abhängigkeit von Dritten
On Premise	<ul style="list-style-type: none">– Daten liegen bei einem selbst– Keine Leerkosten bzw. Mehrausgaben für nicht genutzte Lizenzen	<ul style="list-style-type: none">– Anschaffungskosten für Hardware– Zusätzlicher administrativer Aufwand– Schwerer zu skalieren bzw. längere Planungszeit

Tabelle 1 Gegenüberstellung On Premise und SaaS

Trotz der genannten Vorteile fiel die Entscheidung gegen eine Cloud-Lösung, da so die Datenquellen minimal gehalten werden und die Auszubildenden nicht zwischen mehreren Ressourcen Daten verteilen oder synchronisieren müssen. Ein weiterer Vorteil, den bereits vorhandenen Fileserver als „Cloud“ zu nutzen, ist der Kostenfaktor. Eine Cloud-Lösung einzukaufen würde die Kosten für dieses Projekt zusätzlich zu der weiteren Firewall erhöhen.

Zur Umsetzung der Anforderungen soll eine DMZ eingerichtet werden, in welcher der Fileserver zur Verfügung gestellt wird. Eine DMZ ist geeignet Dienste sowohl intern als auch extern bereitzustellen, da diese abgetrennt vom LAN in einer separaten Netzwerkumgebung liegt. Für die Einrichtung wird eine weitere Firewall benötigt. Durch das 2-stufige Firewall-

Konzept für die DMZ wird die Sicherheit erhöht, da das LAN durch eine weitere Firewall geschützt wird. Die erhöhte Sicherheit besteht darin, dass zwei Firewalls überwunden werden müssen. Falls z. B. durch einen Angreifer die Front-End Firewall überwunden werden sollte, bspw. durch Kenntnis von Anmeldedaten, dann kommt dieser dadurch noch nicht in das interne LAN, was bei dem Einsatz nur einer Firewall der Fall wäre.

Bezüglich der Datenübertragung über das Internet muss ein Verfahren gewählt werden, welches die Datenübertragung anhand des Kriteriums der Verschlüsselung gewährleistet.

Eine Möglichkeit den Datenzugriff zu realisieren, ist SFTP zu nutzen. Dabei wird eine FTP-Verbindung über SSH hergestellt, welche somit verschlüsselt ist. Durch SFTP wird die Verbindung vom Client bis zum Server verschlüsselt, anders als bei einem VPN, wo die Verschlüsselung bei der Firewall aufhört. Um SFTP nutzen zu können, ist es nötig, einen Client installiert zu haben, welcher die Verbindung zum Server aufbaut. Dafür gibt es OpenSource Software wie WinSCP. Nachteilig bei SFTP ist jedoch, dass es nicht skalierbar ist.

Dennoch ist ein VPN gegenüber SFTP zu bevorzugen. Bei einem VPN wird ein neues IP-Paket erstellt und das eigentliche Protokoll ist somit nicht einsehbar, da das gesamte ursprüngliche IP-Paket mit Nutzlast verschlüsselt wird. Ein VPN baut einen „Tunnel“ zum DMZ-Netz auf, was den Zugriff auf alle dort befindlichen Dienste ermöglicht und so für die perspektivische Erweiterung der bereitgestellten Dienste skalierbar ist. Auch für das VPN wird ein zusätzlicher Client benötigt.

Aufgrund der oben angeführten Argumente soll der Datenzugriff über ein VPN realisiert werden.

2.2 Produktauswahl

Die Auswahl der neuen Firewall wurde anhand einer Nutzwertanalyse getroffen. Diese ermöglicht das Abwägen vorher gesetzter Kriterien anhand eines gewichteten Punktesystems.

Es werden zwei mögliche Produkte verglichen. Das ist einmal die OpenSource Firewall pfSense auf einer Supermicro installiert, wovon bereits eine eingesetzt wird und zum anderen eine Firewall des Herstellers Fortinet, die FortiGate FG-60F [Anhang II.iii](#). Die Wahl fiel auf diesen Hersteller, da dessen Produkte bereits genutzt werden. So können die verschiedenen Netzwerkumgebungen möglichst einheitlich gehalten werden und die Administratoren können die Auszubildenden bei Bedarf mit ihrem Wissen zu dieser Produktfamilie unterstützen. Bei einem Hersteller wie bspw. Sophos, welcher noch nicht im Einsatz ist, wäre eine derart fachkundige Unterstützung der Auszubildenden womöglich nicht gegeben.

Da die Supermicro bereits vorhanden und seit März 2022 [Anhang II.iv](#) im Lager ist, kann hier, anders als bei der FortiGate, der Kaufpreis nicht herangezogen werden. Es muss eine Abrechnung gemäß der zeitlichen Wertminderung erfolgen.

Bei einer Lebensdauer von 6 Jahren, beträgt die Wertminderung 784,70 €, welche einen Vergleichspreis von 829,54 € bedeutet [Anhang II.v](#).

2.2.1 Nutzwertanalyse

Die Nutzwertanalyse wird anhand folgender Kriterien durchgeführt:

- **Firewall-Typ 10%**

Der Firewall-Typ ist ein Faktor, welchen es zu beurteilen gilt. Die gegenwärtig eingesetzte pfSense ist eine SPI-Firewall. Dieses Kriterium sollte die neue Firewall ebenfalls erfüllen. Funktionen einer NGFW sind in der Auswahl nicht weiter relevant, da es fraglich ist, ob diese bei der Testumgebung umfassend genutzt werden. Sollten sie jedoch vorhanden sein, wie bspw. ein IDS/IPS, ist das allerdings auch kein Ausschlusskriterium.

- **Hardwareausstattung 15%**

Die Hardware der neuen Firewall sollte idealer Weise zwei SFP-Ports beinhalten. Außerdem sind zwei Stromanschlüsse wünschenswert, da die Firewall die wichtigste Komponente der Testumgebung ist. Außerdem sollte die Firewall ins Rack einbaubar oder ein Rack-Kit verfügbar sein, damit die Firewall nahtlos ins Rechenzentrum [REDACTED] integriert werden kann.

- **Kosten 25%**

Die Kosten der Neuanschaffung sind bei einem Projekt nicht zu vernachlässigen. Die Summe von Software-, Lizenz-, Support- und Hardwarekosten können schnell steigen. Aus diesem Grund ist es wichtig, diese bei der Auswahl in Betracht zu ziehen. Außerdem ist darauf zu achten, wie lange das eingekaufte Produkt nutzbar ist und wann es End-Of-Life geht, um gegebenenfalls Doppelanschaffungen zu vermeiden. Da die Azubi-Testumgebung keine produktiven Aufgaben übernimmt, ist die Priorität, diese auszustatten, entsprechend niedrig und die Mittel, die dafür aufgewendet werden sollen, gering. Aufgrund dessen sollen die Ausgaben auf das Wesentliche beschränkt werden.

- **Nutzerfreundlichkeit 25%**

Die Nutzerfreundlichkeit ist bei der Auswahl der Firewall ebenfalls wichtig. Da diese zukünftig von Auszubildenden verwaltet wird, sollte die Einarbeitung nicht zu komplex sein, da es für viele das erste Mal sein wird, dass sie im administrativen Kontext mit Firewalls in Kontakt kommen. Notwendig ist dafür eine übersichtliche und intuitive GUI.

- **Support 10%**

Gerade bei einer so essenziellen Komponente wie einer Firewall ist es wichtig, dass diese reibungslos funktioniert. Jedoch muss beachtet werden, dass es sich um eine Testumgebung handelt, weswegen ein Ausfall dieser die Geschäftsfähigkeit nicht beeinträchtigt und die RTO dementsprechend hoch ist. Zusätzlich können Kollegen bei der Behebung von Problemen unterstützen.

- **VPN-Fähigkeit 15%**

Da der externe Zugriff auf den Fileserver über ein VPN erfolgen soll, muss die neue Firewall VPN-fähig sein. Auch hier gibt es mehrere Faktoren, die beachtet werden müssen. Dazu zählen zum Beispiel die Anzahl der Tunnel, die gleichzeitig aufgebaut werden können, sowie die VPN-Protokolle, welche zur Konfiguration zur Verfügung stehen.

Kriterium	Gewichtung	pfSense		FG-60F	
		Bewertung	gewichtet	Bewertung	gewichtet
Firewall-Typ	10	1	10	1	10
Hardwareausstattung	15	0,5	7,5	0	0
Kosten	25	1	25	0,5	12,5
Nutzerfreundlichkeit	25	1	25	1	25
Support	10	0,5	5	1	10
VPN-Fähigkeit	15	1	15	1	15
Gesamt	100		85,5		72,5

Tabelle 2 Nutzwertanalyse

Die Bewertung erfolgte mit Punkten von 0 bis 1. Die Idee dahinter ist, dass bei Vergabe einer 1 das Kriterium zur vollen Zufriedenheit erfüllt wurde. Bei 0.5 Punkten gibt es Verbesserungsbedarf und bei 0 Punkten ist das Kriterium nicht erfüllt.

2.2.1.1 Auswertung Nutzwertanalyse

Die Bewertung der Hardwareausstattung ist bei beiden Firewalls mittelmäßig ausgefallen. Bei der pfSense fehlt wie bei der FortiGate auch der zweite Stromanschluss. Zusätzlich dazu hat die FortiGate keine SFP-Ports.

Obwohl die pfSense-Variante bei der Anschaffung geringfügig teurer ist als die FG-60F, wird der Kostenfaktor gleich bewertet. Während es sich bei der pfSense durch die OpenSource-Software um Einmalkosten handelt, bestehen die Kosten bei der FortiGate aus zusätzlichen Lizenzen für bestimmte Funktionen oder professionellem Support.

Der Aspekt des Supports ist bei der pfSense weniger gut ausgeprägt als bei der Alternative, da es nur einen Community Support gibt und professioneller Support, anders als bei der FortiGate nicht dazu gekauft werden kann. Um den professionellen Support für pfSense zu erwerben, muss ein Softwareupgrade auf pfSense+ durchgeführt werden. Erst dieses Upgrade beinhaltet den Support.

Die Auswertung der Nutzwertanalyse spricht für eine pfSense Installation auf der Supermicro.

Allerdings gilt es, vor der endgültigen Entscheidung noch abzuwägen, ob es nicht dennoch sinnvoll wäre, die Firewall von Fortinet zu beschaffen. Dafür sprechen würde zum einen, eine erhöhte Sicherheit. Sollte es in der pfSense eine Sicherheitslücke geben, könnte diese ausgenutzt werden, um sowohl die Front-End Firewall als auch die Back-End Firewall zu überwinden. Wenn LAN und DMZ jedoch durch Firewalls von unterschiedlichen Herstellern geschützt werden, minimiert sich dieses Risiko. Dagegen ist anzuführen, dass es nutzerfreundlicher ist, eine Netzwerkumgebung homogen zu halten, nicht zuletzt wegen des Aufwands, sich eingehend mit unterschiedlichen Produkten auseinanderzusetzen und diese in der Tiefe zu beherrschen, wie es bei kritischen Komponenten wie einer Firewall erforderlich ist.

Aufgrund dessen wird das Ergebnis der Nutzwertanalyse unterstützt und die pfSense auf einer Supermicro als neue Front-End Firewall bestimmt.

2.3 Ressourcenermittlung

In der Ressourcenermittlung wird herausgearbeitet, wie viele Ressourcen benötigt werden, um das Projekt durchzuführen. Das wird anhand der geplanten Arbeitskraft berechnet. In den Fixkosten wird zudem die Höhe der benötigten Mittel berechnet, welche für die weitere Aufrechterhaltung des Projektergebnisses benötigt werden.

2.3.1 Projektkostenberechnung

Für die Projektkosten werden nur die Personalkosten berechnet. Aufgrund der Entscheidung, die pfSense zu verwenden, fallen keine Anschaffungskosten an, da die Supermicro durch die Abschreibung zu den Fixkosten gerechnet wird.

Berechnet werden die Personalkosten nach einer internen Tabelle „Kosten eines Arbeitsplatzes 2024“ (KeAP) [Anhang II.vi](#) und mit Hilfe zusätzlicher Informationen der Personalabteilung bzgl. der KeAP für Auszubildende im dritten Lehrjahr [Anhang II.vii](#). Die Kosten eines Arbeitsplatzes setzen sich aus Personal-, Verwaltungs-, Sach- und IT-Kosten zusammen. Als Referenz wird die Tabelle aus 2024 verwendet, da die Berechnung für das laufende Kalenderjahr noch nicht erfolgt ist.

Der Stundenlohn eines Auszubildenden aus dem dritten Lehrjahr beträgt 21,95 € [Anhang II.viii](#) und der eines Administrators [REDACTED] beträgt 67,38 €. Folgende Tabelle zeigt die Personalkosten für das Projekt.

	Stunden	Stundenlohn	Gesamtlohn
Auszubildender 3. Lehrjahr	40	21,95 €	878,00 €
Angestellter	2	67,38 €	134,76 €
Gesamtkosten			1.012,76 €

Tabelle 3 Personalkostenberechnung

Somit belaufen sich die voraussichtlichen Personalkosten des Projektes auf 1.012,76 €.

2.3.2 Fixkostenberechnung

2.3.2.1 Stromkosten

Die Stromkosten der Supermicro werden nach der Maximalleistung des Netzteils berechnet. Diese beträgt 60 Watt, was 0,06 kWh entspricht. Die Stromkosten für Bestandskunden betragen zur Zeit des Projekts 35 ct/kWh.

	Monat (30d)	Jahr
Stromverbrauch	43,2 kWh	518,4 kWh
Stromkosten	15,12 €	181,44 €

Tabelle 4 Stromkosten Supermicro

Es ergeben sich also Energiekosten von maximal 15,12 € im Monat und 181,44 € im Jahr. Allerdings muss man beachten, dass es unwahrscheinlich ist, dass diese hohen Kosten auftreten, da die Supermicro aller Erwartung nach nicht dauerhaft auf Voll-Last läuft.

2.3.2.2 Wartungskosten

Diese Kosten treten auf, wenn an der Firewall Wartungsarbeiten nötig sind. Diese beinhalten das Bearbeiten des Regelsets, sonstiger Einstellungen oder das Verwalten der User.

Da die Testumgebung eine sehr statische Netzwerkstruktur hat, fallen selten Wartungsarbeiten an. Auf das Jahr hochgerechnet werden vermutlich ca. 10 Stunden für die Administration der Firewall aufgewendet. Da die Testumgebung von Auszubildenden des dritten Lehrjahres betreut wird, betragen die Wartungskosten im Jahr 219,50 €, heruntergerechnet auf einen Monat 18,29 €. [Anhang II.x](#)

2.3.2.3 Monatliche Fixkosten

Die monatlichen Fixkosten setzen sich zusammen aus den Strom- und Wartungskosten sowie aus der monatlichen Abschreibung der Supermicro [Anhang II.v](#).

	Stromkosten	Supermicro	Wartungskosten	Gesamt
Pro Monat	15,12 €	22,42 €	18,29 €	55,83 €

Tabelle 5 Monatliche Fixkosten

Daraus ergeben sich Kosten von 55,83 € pro Monat.

2.4 Erstellung eines Netzwerkplans

Zunächst gilt es, einen Netzwerkplan zu erstellen, anhand dessen das Projekt umgesetzt wird [Anhang II.i](#).

Die zusätzliche Firewall, welche als Front-End Firewall eingesetzt werden soll, wird direkt an die Back-End Firewall angeschlossen. Aufgrund der Verteilung der Netzwerkkarten an der gewählten Supermicro werden sie nicht redundant verbunden. Da beide in Frage kommenden Ports an demselben Netzmodul angeschlossen sind, würde bei einem Ausfall eines Ports der andere mit hoher Wahrscheinlichkeit ebenfalls nicht mehr funktionieren.

Die neue Firewall wird über zwei weitere Ports mit je einem der beiden Switches verbunden. Diese Verbindungen dienen dazu, Zugang ins DMZ-Netz zu erhalten. Redundant wird sie deshalb gesteckt, damit sichergestellt ist, dass bei dem Ausfall eines Switches der Zugang zur DMZ gewährleistet ist.

Die vier ESXi-Hosts sind bereits redundant mit den Switches verbunden, diese Redundanz dient dazu, dass bei Ausfall eines Switches die Möglichkeit zu arbeiten, gewährleistet ist. Die ESXi-Hosts werden mit einer weiteren Verbindung an je einen Switch angeschlossen. Somit sind dann an jedem Switch zwei ESXi-Hosts angeschlossen, um auf das DMZ-Netz zuzugreifen. Die nicht-redundante Verbindung der einzelnen ESXi-Hosts hat folgenden Grund. Selbst bei einem Ausfall eines Switches und beim Wegfall des Fileservers würde die Arbeitsfähigkeit gegeben bleiben. Allerdings müsste für die schnelle Wiedererreichbarkeit des Servers, dieser mit seinen Computing Ressourcen im vCenter händisch auf einen anderen Host verschoben werden, der an dem funktionierenden Switch angeschlossen ist. Das ist ein kurzer administrativer Aufwand, der bei einem Server durchaus akzeptabel ist. Wenn allerdings die DMZ erweitert wird und mehr relevante Dienste in dieser beheimatet werden, sollte man erneut evaluieren, ob die Verbindung der ESXi-Hosts mit den Switches redundant ausgeführt werden sollte.

2.4.1 Adressbereiche

Der neue Adressbereich der DMZ wird im 10.3.15.0/24 Netz liegen [Anhang I.III](#). Dies entspricht den Namenskonventionen der Testumgebung, in dem das dritte Oktett der IPv4-Adresse mit den letzten beiden Zahlen der VLAN-ID übereinstimmt. So wird die Übersichtlichkeit innerhalb der unterschiedlichen Netze bewahrt. Die letzte Adresse im Netz ist dem Gateway vorbehalten. Somit hat die Front-End Firewall ein Interface mit der 10.3.15.254/24. Zudem wird eine Adresse für den Fileserver benötigt.

Ein /24 Netz ist für das geplante Setup zwar zu groß und es sind viele ungenutzte Host-Adressen vorhanden, dennoch fiel die Wahl bei der Initialkonfiguration der Azubi-Testumgebung auf diese Subnetzmaske. Diese lässt zum einen viel Raum zur Erweiterung der Umgebung und zum anderen, steht die Testumgebung abgetrennt von den produktiven Umgebungen. Die Adressen sind ohnehin frei und werden anderweitig nicht benötigt.

Das Transfernetz zwischen den beiden Firewalls erhält ein Netzwerk mit einer /30 Subnetzmaske, da für dieses nur 2 Host-Adressen benötigt werden. Das Transfernetz hat die Netzadresse 10.3.0.252/30 [Anhang I.III](#).

3 Durchführungsphase

3.1 Installation und Ersteinrichtung der Firewall

Die Installationsversion der pfSense ist die neuste 2.7.2. Sie kann über einen bootfähigen USB-Stick auf der Supermicro installiert werden. Bei der Installation wird automatisch ein WAN- und ein LAN-Port festgelegt. Der LAN-Port hat standardmäßig die IP 192.168.1.1, über die lokal auf die pfSense zugegriffen werden kann.

Bei der Ersteinrichtung der Firewall muss neben einem neuen Passwort für den Admin-User auch ein Hostname vergeben werden. Dieser orientiert sich an der bereits vorhandenen Firewall und wird dementsprechend XXXXXXXXXX benannt.


Da die genannte Firewall den Internetzugang übernehmen soll, muss folglich das WAN-Interface konfiguriert werden. Dazu muss auf der pfSense ein neues Gateway angelegt werden, welches auf Seiten des ISPs liegt und als Default Gateway gesetzt wird [Anhang III.II](#). Dies ist erforderlich, da das gesetzte Default Gateway alle Anfragen, für die keine anderen Routen festgelegt sind, weiterleitet. Das WAN-Interface bekommt eine IP vom ISP, welche

eingetragen werden muss. Ebenso muss das eben genannte Gateway als „Upstream Gateway“ ausgewählt werden, damit das Interface als WAN-Interface erkannt wird und man von diesem aus eine Ebene höher kommt. [Anhang iii.i.iii](#)

Die pfSense setzt zwei essentielle Regeln, welche überprüft werden müssen, bevor das WAN-Interface angeschlossen wird. Das ist zum einen eine Regel, die alle Anfragen von RFC1918 Netzwerken blockiert und zum anderen eine, welche sogenannte BOGON Netzwerke blockiert [Anhang iii.i.iv](#).

Um nach dem Einbau der Firewall Zugriff auf die interne Firewall zu erhalten, ist es nötig, ein Transfernetz zwischen den beiden anzulegen. Dazu müssen auf den für den Verbund genutzten Interfaces IP-Adressen aus eben diesem Netz gesetzt werden. Damit diese eingetragen werden können, müssen die physischen Ports zuerst einem Interface zugewiesen werden. Die WAN-Firewall erhält die 10.3.0.254 und die interne Firewall dementsprechend die 10.3.0.253. Dieses Interface der internen Firewall muss zusätzlich als Gateway angelegt werden. [Anhang iii.i.i](#), [Anhang iii.i.v](#), [Anhang iii.ii.ii](#)

3.2 Einbau ins Rechenzentrum

Die Firewall wird zu den anderen Komponenten der Azubi-Testumgebung ins Rechenzentrum  eingebaut [Anhang i.iv](#). Dabei wird diese unter die bereits vorhandene Back-End Firewall ins Rack angebracht. Die beiden Firewalls werden über ein DAC-Kabel direkt miteinander verbunden.

Die Verbindungen zu den Switchen werden mit 10 GB LC-LC Multimode Glasfaserkabeln gesteckt. Aufgrund der räumlichen Gegebenheiten wird die Supermicro jedoch nicht direkt mit den Switchen verbunden, sondern über LWL-Patchpanel geführt.

Die ESXi-Hosts werden wieder direkt über 1 GB Kupferkabel mit den Switchen verbunden, da diese direkt untereinander eingebaut sind.

3.2.1 Firewalls zugänglich machen

Da nun der WAN-Anschluss der Firewalls umgesteckt worden ist, ist es nur noch möglich, direkt über die LAN Schnittstelle auf die jeweilige Firewall zuzugreifen, solange kein funktionierendes VPN eingerichtet ist.

Nach dem Einbau musste die interne Firewall über die Front-End zugänglich gemacht werden. Da die interne Firewall keinen direkten Internetanschluss mehr hat, muss ein neues Gateway und WAN-Interface definiert werden. Wie in 3.1 beschrieben, muss im Transfer-Interface analog zu dem WAN-Interface ein Upstream Gateway eingestellt werden [Anhang iii.ii.ii](#). Außerdem ist es notwendig, dass das Default Gateway auf die Transfernetz IP-Adresse der Front-End Firewall geändert wird [Anhang iii.ii.i](#). Nach diesen Einstellungen wird jeglicher Datenverkehr, welcher in Netze geht, die nicht direkt an der internen Firewall anliegen, zur WAN-Firewall geroutet.

Da auf der WAN-Firewall das Transfer-Interface zwar als zusätzliches Gateway angelegt, aber nicht als Default Gateway ausgewählt ist, müssen Routen angelegt werden, welche zu der internen Firewall führen [Anhang iii.ii.ii](#). Das wird über statisches Routing realisiert. Dynamisches Routing wäre auch eine Option, denn man kann bei der pfSense ein Paket für OSPF installieren. Bei dem jetzigen Aufbau ist das allerdings wenig sinnvoll, da nur zwei Router miteinander verbunden sind und die dahinterliegenden Netze nicht häufig geändert werden. Daher ist es vertretbar, die Routen statisch zu setzen und händisch zu verwalten. Eine Route wird für die Netze der Azubi-Testumgebung benötigt (10.3.0.0/8) und eine für die internen Netze der pfSense (192.168.0.0/16).

3.3 Konfiguration der Firewalls

3.3.1 DNS- und NTP-Delegierung

Da nun zwei Firewalls hintereinandergeschaltet sind, kann man eine DNS- und NTP-Delegierung vornehmen. Sinnvoll ist eine Delegation der Dienste deshalb, da die interne Firewall Anfragen an den DNS- oder NTP-Server ohnehin über die WAN-Firewall senden muss, damit diese ins Internet kommen. Um also einen Mehraufwand bei der internen Firewall zu vermeiden, werden durch eine Delegation die Anfragen direkt an die Front-End Firewall gesendet.

Zur DNS-Delegierung wird auf der Front-End Firewall der DNS-Server eingetragen, welcher genutzt werden soll [Anhang iii.i.vii](#). Bei der Back-End Firewall muss dann in derselben Einstellung die Front-End Firewall angegeben werden. Außerdem ist zusätzlich eine Einstellung zu setzen, die besagt, dass die Back-End Firewall nur Remote-DNS-Server benutzt und den lokalen ignoriert [Anhang iii.ii.iii](#). Diese Einstellung ist deswegen von Vorteil, weil die interne Firewall dann keinen DNS-Cache anlegt und verwaltet.

Diese Delegation kann auch bei NTP-Diensten vorgenommen werden. Dazu muss der NTP-Dienst auf der Front-End Firewall aktiviert sein. In der Back-End Firewall muss die WAN-Firewall als NTP-Server eingetragen werden und das Transfer-Interface als ausgehendes Interface für Anfragen ausgewählt werden [Anhang iii.ii.iii](#), [Anhang iii.ii.iv](#).

3.3.2 VPN konfigurieren

Um administrativen Zugang zur Testumgebung zu erhalten, muss wie in dem alten Aufbau ein VPN konfiguriert werden. Dazu muss auf der pfSense zuerst eine CA angelegt werden, damit der neue VPN-Server zertifiziert werden kann. Dafür wird die CA der Back-End Firewall auf die Wan-Firewall importiert [Anhang iv.i](#). Das eingestellte OpenVPN auf der internen Firewall kann dann entfernt werden, da diese nicht mehr im Internet ist und die neue VPN-Verbindung über die WAN-Firewall geführt wird.

3.3.2.1 Server-Zertifikat anlegen

Für den neuen VPN-Server muss ein Server-Zertifikat erstellt werden. Dabei sind wichtige sicherheitsrelevante Einstellungen zu setzen. Zum einen muss ein Verschlüsselungsalgorithmus und die dazugehörige Schlüssellänge gewählt werden. Gewählt ist hier RSA mit einer Schlüssellänge von 4096, was dem derzeitigen BSI Standard entspricht.¹ Auch muss eine Hashfunktion ausgewählt werden, dafür wird SHA-256 verwendet, welcher ebenfalls laut BSI zulässig ist.² Zusätzlich dazu muss noch ausgewählt werden, ob es sich um ein User- oder Server-Zertifikat handelt. In diesem Fall ist es demnach ein Server-Zertifikat. [Anhang iv.ii](#)

3.3.2.2 OpenVPN-Server konfigurieren

Nach Anlegen des Server-Zertifikats, kann ein neuer VPN-Server erstellt werden. Dabei sind ebenfalls einige wichtige Einstellungen zu beachten. Zum einen muss man einen Servermodus auswählen, in diesem Fall Remote Access mit SSL/TLS und User Authentifikation. Auch muss zwischen Transport- und Tunnelmodus entschieden werden. Gewählt wurde der Tunnelmodus, da dieser zusätzlich zur Verschlüsselung des Pakets auch die IP-Verschleierung beinhaltet. Der Port für den Server ist standardmäßig 1194. In den kryptographischen Einstellungen muss dann das zuvor angelegte Server-Zertifikat ausgewählt und die Schlüssellänge des Diffie-Hellman Algorithmus angegeben werden. Hier wird ebenfalls auf Empfehlung des BSI eine Länge über 3000 bit gewählt. In diesem Fall die Länge von 4096

¹ Vgl. Bundesamt für Sicherheit in der Informationstechnik. *BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen"*. 2025. S. 35.

² Vgl. ebd, S. 50

bit.³ Außerdem ist es ratsam festzulegen, dass bei einem Loginversuch der angegebene Username mit dem angegebenen Namen im Zertifikat verglichen werden muss. Es muss für das Tunnelnetzwerk ein Netzbereich angegeben werden, aus welchem die User eine IP-Adresse bekommen, sobald sie mit dem VPN verbunden sind. Auch aktiviert werden sollte die Einstellung, dass sich verbundene Clients nach einer IP-Adressenänderung automatisch wieder verbinden dürfen. Die Zeit nach der ein Client durch Inaktivität automatisch vom VPN getrennt wird, wird von 5 Minuten auf 1 Stunde hochgesetzt. Außerdem kann man dem VPN-Server Routen mitgeben, auf welche Bereiche Nutzer des VPN-Zugriff haben sollen. Da das gesamte interne Netz innerhalb des Bereiches 10.3.0.0 liegt, ist es sinnvoll hier eine Route anzuwenden, die den Zugriff auf diese Netze explizit erlaubt. [Anhang iv.iii](#)

3.3.2.3 VPN-Nutzer anlegen

Für die VPN-Nutzer lohnt es sich, im Voraus eine separate Gruppe anzulegen. Dieser Gruppe wird dann eine Berechtigung zugewiesen, welche erlaubt, dass sich die Nutzer an der pfSense anmelden können, um ihr Passwort zu ändern. [Anhang iv.v](#) Es ist vor allem initial wichtig, dass die Auszubildenden die vorhergesetzten Kennwörter ändern, sodass diese dem Admin danach unbekannt sind.

Als nächstes muss ein User angelegt werden, welcher Zugang zu dem VPN erhält. Dabei wird neben Nutzernamen und Passwort auch ein User-Zertifikat angelegt, falls gewünscht. Diese Option sollte ausgewählt und auf den Standardeinstellungen belassen werden. Die Schlüssellänge des RSA entspricht mit 2048 bit zwar nicht den Empfehlungen des BSI, allerdings ist es bei den User-Zertifikaten so, dass dort zusätzlich noch ein Passwort nötig ist, um dieses Zertifikat gegenüber dem Server zu validieren. Daher wird die kleinere Schlüssellänge als ausreichend erachtet. Auch kann der Benutzer direkt der `vpn_users` Gruppe zugewiesen werden [Anhang iv.vi](#). Nach der Erstellung des Benutzers muss man diesen dann erneut bearbeiten, um das entsprechende Zertifikat zu erstellen. Dabei lässt man die Voreinstellungen bestehen und trägt nur den CN ein.

Anschließend kann man über ein zusätzlich installiertes Paket den Client aus OpenVPN exportieren. Dabei kann man wählen, was exportiert werden soll. Wenn der betreffende Nutzer bereits den OpenVPN-Client installiert hat, genügt das Bundle Archive. Wenn der Client auf dem Gerät allerdings noch nicht vorhanden ist, bietet sich der Windows Installer an, da dort nicht nur der OpenVPN-Client Installer enthalten ist, sondern nach der Installation direkt die Konfiguration eingefügt wird. [Anhang iv.vii](#)

3.4 DMZ-Netz anlegen

Der nächste Schritt, das DMZ-Netz anzulegen, ist umfangreicher in dem Sinne, als dass es mehrere unterschiedliche Komponenten des Netzwerks miteinschließt. Es müssen die ESXi-Hosts, die Switches und die neue Firewall konfiguriert werden.

3.4.1 ESXi-Hosts

Auf den ESXi-Hosts werden neue vSwitches benötigt, welche ausschließlich in das DMZ-Netz führen. Diese müssen auf den vier Hosts separat angelegt werden. Dabei ist darauf zu achten, dass die Benennung konsistent ist, sodass die Netze vom vCenter als identisch erkannt werden und eine Migration der Fileserver VM reibungslos möglich ist. [Anhang v.i](#)

Der vSwitch ist dafür verantwortlich, dass innerhalb des vCenters auf VMs in verschiedenen Netzen zugegriffen werden kann. Sie haben einen oder mehrere physische Adapter und können intern beliebig viele Netze enthalten. Diese Netze werden in Portgruppen definiert,

³ Vgl. ebd, S. 39

welche an den Switch „angeschlossen“ werden. Den Portgruppen können neben dem Namen auch eine VLAN-ID mitgegeben werden.

Für den virtuellen Switch wird jeweils nur ein physischer Adapter verwendet. Es sind zwar sowohl an den Servern als auch an den Switchen genug Ports vorhanden, sodass jeder vSwitch zwei physische Adapter und damit eine redundante Anbindung an beide Switches haben könnte. Jedoch ist es nicht außer Acht zu lassen, dass die DMZ zum Zeitpunkt dieses Projektes nur aus einem Server besteht, weswegen hier die einfachere Variante gewählt wird. Bei einer Vergrößerung der DMZ ist die Anbindung der Switches selbstverständlich dementsprechend auszubauen.

Die Portgruppe der DMZ ist ohne VLAN-ID konfiguriert, da an diesem Adapter nur das DMZ-Netz angeschlossen wird und somit kein VLAN-Tagging nötig ist. [Anhang v.i](#)

Um die Sicherheit innerhalb der DMZ weiter zu erhöhen, ist das DMZ-Netz im vCenter für die Auszubildenden gesperrt. Dafür wurde auf das Netz eine Berechtigung gesetzt, welche den Mitgliedern der Auszubildenden-Gruppe den Zugriff auf dieses Netz untersagt [Anhang v.ii](#). So können nur Administratoren in diesem Netz VMs erstellen und bearbeiten.

3.4.2 Switches

Zentrales Element des Netzwerks sind die Layer-2-Switches, da bei ihnen unterschiedlicher Netzwerkverkehr zusammenläuft und weiter verteilt werden muss. Aus diesem Grund muss die Konfiguration der beiden Switches ebenfalls angepasst werden.

Es ist nötig, dass auf den Switches ein neues VLAN für die DMZ angelegt wird.

Außerdem muss auf jedem Switch je ein Port konfiguriert werden, an welchem die Front-End Firewall angeschlossen ist. Da diese Ports nur für das DMZ-VLAN genutzt werden, sind diese als Access-Port konfiguriert. Ebenso Access-Ports sind diejenigen, an welchen die ESXi-Hosts angeschlossen sind. An jedem der beiden Switches sind zwei ESXi-Hosts angeschlossen. [Anhang v.ii](#)

3.4.3 Firewall

Um das DMZ-Netz über die Front-End Firewall erreichbar zu machen, muss der Zugang zu den Switches konfiguriert werden. Die Firewall wird, wie im vorherigen Kapitel beschrieben, an die Switches angeschlossen. Es wird auf der Firewall ein Failover LAGG eingerichtet. Dies ermöglicht es, dass im Falle eines Ausfalls eines der Switches die Firewall automatisch die andere Leitung für den Datenverkehr nimmt. Natürlich bietet das Failover nicht den Vorteil einer Link Aggregation, bei der sich die Datenrate durch den Verbund der beiden Ports verdoppelt. Allerdings ist das in diesem Fall nicht möglich, da LACP nicht auf den Switches konfiguriert ist und die Ziele des LAGGs auf unterschiedlichen Geräten liegen.

Nachdem dem eingerichteten LAGG ein Interface zugewiesen wurde, kann man für dieses Regeln definieren. Zum einen muss eine Regel definiert werden, welche den Zugang zum Internet erlaubt. Das ist unter anderem deswegen wichtig, damit der Server Updates erhält.

Außerdem müssen noch Regeln für den Zugriff auf das Admin-Netz erstellt werden. Aufgrund dessen, dass der Fileserver Mitglied in einer Domäne ist, müssen bestimmte Ports in das Netz des DCs freigegeben werden. Dazu zählen AD spezifische Ports, welche die Kommunikation mit dem DCs sicherstellen sollen, sowie weitere Ports, welche Zugriff auf die bereitgestellten Services bieten, wie DNS- oder NTP-Dienste. [Anhang iii.i.vi](#)

3.5 Externen Zugriff einrichten für die DMZ

Um das VPN anzulegen, womit die Auszubildenden nur in die DMZ kommen, müssen die Schritte wie in Kapitel 3.3.2.1 bis 3.3.2.3 mit einigen Abweichungen befolgt werden. Zum einen

muss bei der Serverkonfiguration darauf geachtet werden, dass ein anderer Port für die VPN-Anfragen gewählt wird. Standardmäßig wird der Port allerdings automatisch hochgezählt. Auch muss in den Konfigurationen festgelegt werden, dass das einzig erreichbare Netz das DMZ-Netz ist [Anhang iv.iv](#). Ergänzend ist beim Clientexport darauf zu achten, dass vor dem Export der entsprechende VPN-Server ausgewählt wird, für den die exportierte Konfiguration gültig sein soll. [Anhang iv.viii](#)

3.6 Fileserver anpassen

Damit der Fileserver über das konfigurierte VPN erreichbar wird, muss dieser noch an den richtigen vSwitch auf dem ESXi-Host angeschlossen und die IP demnach angepasst werden. [Anhang v.iii.i](#)

Nachdem der Fileserver in die DMZ verschoben wurde, wurde dieser jedoch sehr langsam und die auf der VM befindlichen Programme stürzten häufig ab. Nachdem das Hochsetzen der CPU-Kerne und des Arbeitsspeichers erfolglos blieb, wurde die Fehlerursache bei der Firewall gesucht und gefunden. In den Logs der WAN-Firewall war ersichtlich, dass aus dem DMZ-Netz Anfragen über dynamische Ports in Richtung des Netzes, in dem der Domain Controller liegt, rausgingen und gemäß dem vorliegenden Regelwerk geblockt wurden. [Anhang iii.i.viii](#) Nach intensiver Recherche wurde ersichtlich, dass die Ports von RPC benötigt und freigegeben werden müssen. Um die Theorie zu testen, dass der Fileserver diese braucht, um mit dem DC zu kommunizieren, wurde versuchsweise eine automatische Regel aus der Blockliste angelegt. Dies führte zu einer sofortigen Besserung. Da es allerdings unsicher ist, alle dynamischen Ports freizugeben, wurde nach Anleitung von Microsoft⁴ die Portrange für RPC in der Registry auf 49152-49652 begrenzt. [Anhang v.iv.iii](#) Es wurde bei der Auswahl der Portrange von der Anleitung von Microsoft abgewichen, da innerhalb des vorgeschlagenen Bereichs einige Ports noch von Diensten verwendet werden. Um eine Kollision zu vermeiden, wurden deshalb die ersten der dynamischen Ports gewählt. In der Firewall wurden die entsprechenden Ports freigegeben und die automatisch angelegte Regel gelöscht. [Anhang iii.i.vi](#)

3.6.1 Berechtigungen anpassen

Die Auszubildenden haben innerhalb der Azubi-Testumgebung zwei Netzlaufwerke zur Verfügung, welche über das VPN erreichbar sein sollen. Dabei handelt es sich um einen privaten und einen geteilten Ordner, auf den alle Auszubildenden Zugriff haben. Während der geteilte Ordner über eine Gruppenrichtlinie [Anhang v.iv.i](#) verteilt wird, ist der private Ordner über den Basisordnerpfad eingebunden [Anhang v.iv.ii](#). Dadurch wird ein privater Ordner innerhalb eines freigegebenen Ordners erstellt und beim Anmelden des Nutzers gemapped.

Da beim Zugriff über VPN Zugriff auf den gesamten Fileserver erteilt wird, müssen noch einige Berechtigungen angepasst werden. Die geteilten Laufwerke sind ausgenommen, weil diese aufgrund der Zuordnung über GPOs und Gruppen bereits dementsprechend konfiguriert sind. Aufgrund dessen, dass es sich bei den privaten Ordnern um Unterordner einer Freigabe handelt, muss hier der Zugriff noch reguliert werden. Ansonsten würden die angemeldeten Nutzer Zugriff auf alle privaten Ordner erhalten, was nicht dem Gedanken der Ordner entspricht.

Um die privaten Ordner nur dem angemeldeten Benutzer zugänglich zu machen, muss in den Berechtigungen der Zugriff auf den freigegebenen Ordner \Privat so geändert werden, dass Benutzer, welche Mitglied in der „Domänen-Benutzer“ Gruppe sind, lesenden Zugriff auf \Privat erhalten [Anhang v.iii.ii](#). Dabei ist es wichtig, dass dieser Zugriff nur für \Privat gilt, da alle angelegten Benutzer in dieser Gruppe sind und somit ansonsten lesenden Zugriff auch auf die privaten Unterordner erhalten würden. So können die angemeldeten Benutzer nur ihre eigenen

⁴ Vgl. Microsoft. *Konfigurieren der dynamischen RPC-Portzuweisung für Firewall-Einsatz*. 2025.

Ordner sehen und bearbeiten, da die „Domänen-Benutzer“ Gruppe keinen Zugriff auf diese hat [Anhang v.iii.iii](#).

4 Durchführung von Tests

Damit die Funktionsfähigkeit innerhalb der verschiedenen Netze [\[REDACTED\]](#) gewährleistet ist, werden drei Testszenarien durchgeführt. Ein Test erfolgt im Netz [\[REDACTED\]](#) und einer [\[REDACTED\]](#). Um zu testen, ob das Projektziel erreicht wurde, und um einen Ablauf eines Zugriffs zu simulieren, wird die OpenVPN-Konfiguration von „Musterazubi“ als Windows Installer heruntergeladen.

Diese kann dann mit Hilfe eines USB-Sticks auf den entsprechenden Computer kopiert und installiert werden. Bei der Installation gibt es eine Stelle, an der eine Fehlermeldung generiert wird. Das ist nach der Installation des Clients. Diese Fehlermeldung [Anhang vii.i.i](#) kann ignoriert werden, da im nächsten Schritt automatisch die Konfigurationsdateien eingefügt werden. Nach dem Postinstall kann dann eine Verbindung zum VPN aufgebaut werden. Dafür müssen Benutzername und Passwort eingegeben werden. [Anhang vii.i.ii](#)

Um nach einem erfolgreichen Verbinden mit dem VPN auf den Fileserver zuzugreifen, muss im Explorer in der Pfadleiste \\10.3.15.253 eingegeben werden. Es wird danach direkt die Fehlermeldung angezeigt, dass die Anmeldung fehlgeschlagen ist. Dies liegt daran, dass der Computer versucht sich mit dem angemeldeten Windows-User und der Domäne am Fileserver anzumelden. Es muss also beim Anmelden mit dem VPN-Benutzer die Domäne der Azubi-Testumgebung vorangeschrieben werden [Anhang vii.ii.i](#).

Nach dem Anmelden erscheinen alle freigegebenen Ordner des Fileservers [Anhang vii.ii.ii](#). Dementsprechend erscheint auch bei einem angemeldeten Auszubildenden der Admin-Share, auf welchen diese keinen Zugriff haben [Anhang vii.ii.iii](#). In \Privat wird nur der eigene private Ordner angezeigt, analog zu den gesetzten Berechtigungen [Anhang vii.ii.iv](#).

Der gewählte Benutzer bleibt solange am Fileserver angemeldet, bis sich der Nutzer entweder am Computer abmeldet oder diesen herunterfährt bzw. neu startet.

Alles in allem ist die Testphase gut verlaufen. Die Tests aus [\[REDACTED\]](#) waren beide erfolgreich. Aus dem Netz [\[REDACTED\]](#) kann keine VPN-Verbindung aufgebaut werden [Anhang vii.i.iii](#). Der Grund dafür liegt darin, dass der Internetzugang aus dem [\[REDACTED\]](#) durch einen Drittanbieter erfolgt, bei welchem die OpenVPN-Verbindung abgeblockt wird. Deswegen wird es keine Möglichkeit geben, über die Desktop PCs so auf den Fileserver zuzugreifen. Allerdings ist es über ein Notebook möglich, in dem man sich mit [\[REDACTED\]](#) WLAN verbindet, welches man auch in den Büroräumen empfangen kann.

5 Abschlussphase

5.1 Soll-Ist-Abgleich

Es wurde eine zweite Firewall eingebaut und konfiguriert sowie ein VPN eingerichtet. Eine DMZ ist verfügbar und kann in Zukunft um weitere Dienste erweitert werden. Außerdem wurde eine Anwenderdokumentation erstellt und den Auszubildenden zugänglich gemacht. Die Dokumentation der Azubi-Testumgebung wurde gemäß den vorgenommenen Änderungen angepasst.

Es gab während des Projektes einige Probleme, die sich in Zeitrückständen äußerten. Trotz einiger Rückschläge während der Umsetzung konnte der zeitliche Rahmen eingehalten werden. [Anhang ii.ii](#)

Leider ist der Fileserver aus [REDACTED] nicht erreichbar, sondern nur aus dem [REDACTED]. Da der Auslöser des Projekts jedoch der Zugriff während der Berufsschulzeit war, ist das Projekt dennoch ein Erfolg gewesen. Dass der Fileserver aus [REDACTED] nicht erreichbar ist, ist zwar schade, aber nicht problematisch, da es, wie im vorherigen Kapitel genannt, einen Workaround dafür gibt.

Literaturverzeichnis

- Bundesamt für Sicherheit in der Informationstechnik. *BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen"*. 2025. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=13 (Zugriff am 24. 03 2025).
- Electric Sheep Fencing LLC and Rubicon Communications LLC. *pfSense Documentation*. 2024. <https://docs.netgate.com/pfsense/en/latest/>.
- Microsoft. *Konfigurieren der dynamischen RPC-Portzuweisung für Firewall-Einsatz*. 2025. <https://learn.microsoft.com/de-de/troubleshoot/windows-server/networking/configure-rpc-dynamic-port-allocation-with-firewalls> (Zugriff am 06. 03 2025).
- tronet GmbH. *Fortinet FortiGate 60F Firewall*. 2025. https://www.allfirewalls.de/Marken/Fortinet/FortiGate-Firewalls/Entry-Level-Firewalls/fn-fw-60f-Fortinet-FortiGate-60F-Firewall.html?force_sid=3f53dfk5vi3pohktr3ihuvkfsc (Zugriff am 25. 03 2025).

Anlage

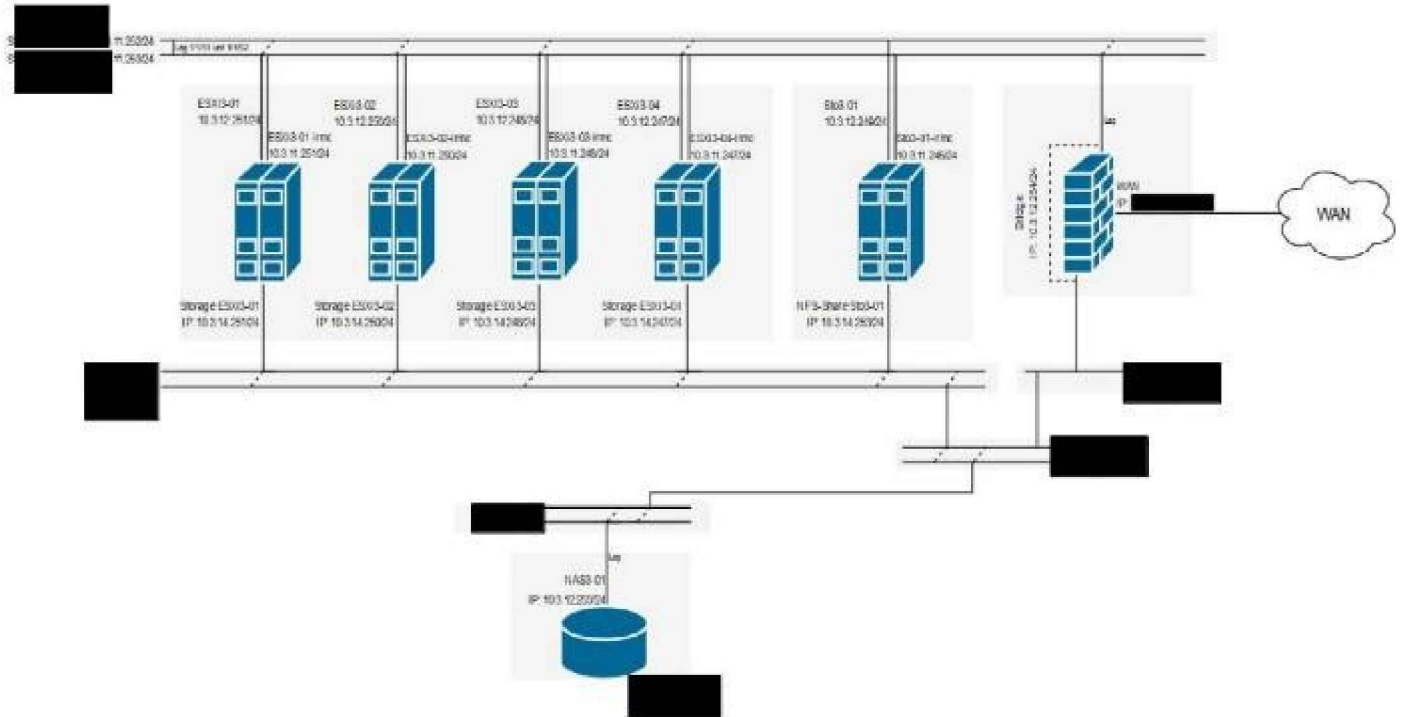
i.	Netzwerkpläne	iv
i.i	Azubi-Testumgebung Ist-Zustand	iv
i.ii	Azubi-Testumgebung Soll-Zustand	iv
i.iii	VLAN-Übersicht	v
i.iv	Verkabelungsplan	v
ii.	Kaufmännisch	vi
ii.i	Gantt-Diagramm	vi
ii.ii	Zeitabgleich	vi
ii.iii	Preis Fortinet Firewall	vii
ii.iv	Rechnung Supermicro	vii
ii.v	Berechnung Wertminderung Supermicro	vii
ii.vi	Kosten eines Arbeitsplatzes 2024	viii
ii.vii	Auskunft Personalabteilung.....	viii
ii.viii	Berechnung Stundenlohn Auszubildende.....	viii
ii.ix	Berechnung Wartungskosten.....	viii

iii.	Firewall - pfSense.....	ix
iii.i	Front-End Firewall.....	ix
iii.i.i	Gateways.....	ix
iii.i.ii	Statische Routen.....	ix
iii.i.iii	WAN-Interface Upstream Gateway	ix
iii.i.iv	WAN-Interface Regeln	ix
iii.i.v	Transfer-Interface IP-Adresse	x
iii.i.vi	DMZ-Interface Regeln.....	x
iii.i.vii	DNS und NTP	x
iii.i.viii	Firewall Logs dynamische Ports.....	xi
iii.ii	Back-End Firewall.....	xi
iii.ii.i	Gateway.....	xi
iii.ii.ii	Transfer-Interface IP-Adresse und Upstream Gateway	xi
iii.ii.iii	DNS- und NTP-Delegation.....	xii
iii.ii.iv	NTP-Einstellungen	xii
iv.	VPN.....	xiii
iv.i	Front-End Firewall CA.....	xiii
iv.ii	OpenVPN-Server-Certificate.....	xiii
iv.iii	OpenVPN-Server.....	xiv
iv.iv	OpenVPN-Server DMZ	xv
iv.v	Gruppe für VPN-User.....	xv
iv.vi	VPN-User anlegen.....	xvi
iv.vii	Clientexport.....	xvi
iv.viii	Clientexport Serverauswahl	xvi
v.	vCenter	xvii
v.i	vSwitch mit Portgruppe	xvii
v.ii	Berechtigung DMZ-Netz.....	xvii
v.iii	Fileserver.....	xvii
v.iii.i	IP Änderung.....	xvii
v.iii.ii	Berechtigung Ordnerfreigabe \Privat	xviii
v.iii.iii	Berechtigungen privater Ordner	xviii
v.iv	Domänen-Controller.....	xix
v.iv.i	GPO geteiltes Laufwerk für Azubis.....	xix
v.iv.ii	Basisordner.....	xix
v.iv.iii	Registry RPC-Portzuweisung begrenzen	xx
vi.	Switches	xx

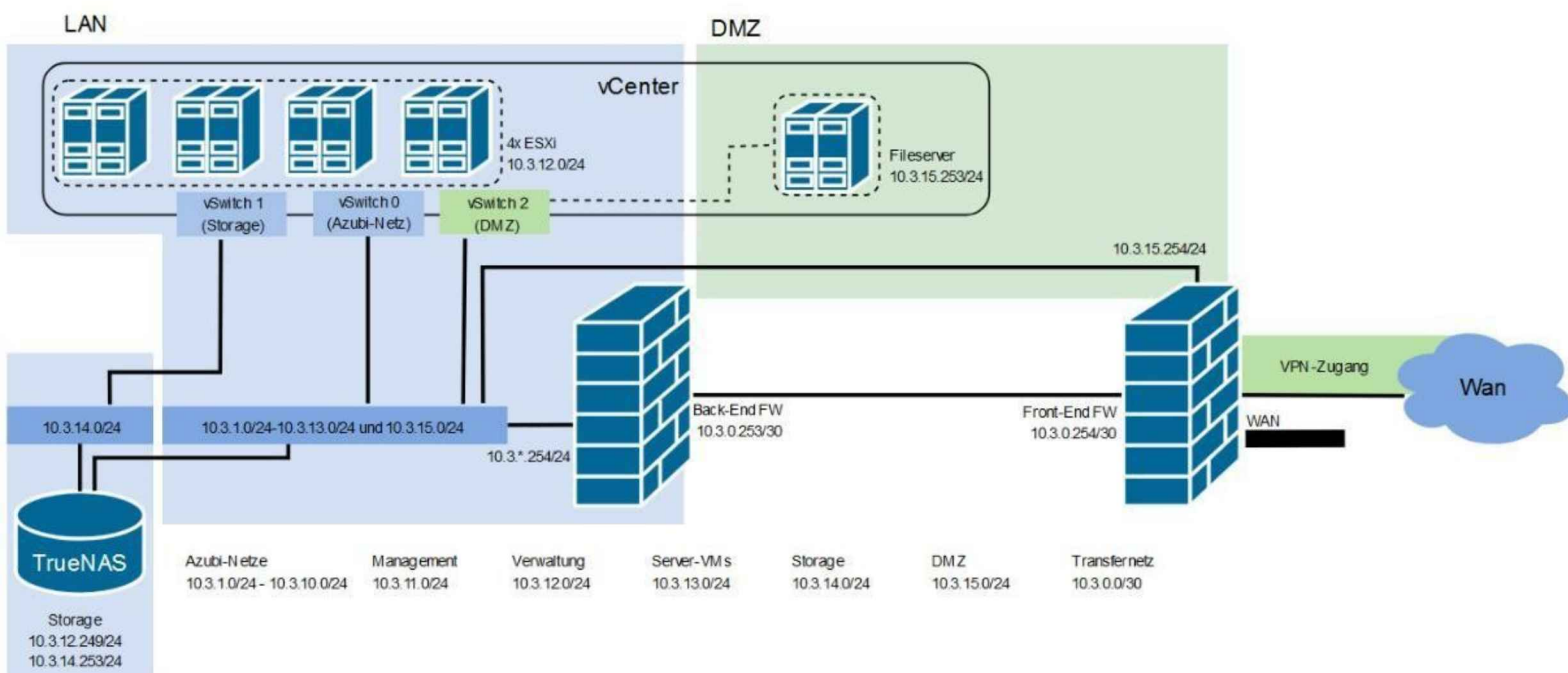
vi.i	Port Konfiguration	XX
vii.	Anwendung	XX
vii.i	VPN	XX
vii.i.i	Fehlermeldung Installation	XX
vii.i.ii	Anmeldung VPN.....	xxi
vii.i.iii	Verwaltungs-Netz VPN-Verbindung	xxi
vii.ii	Fileserver.....	xxi
vii.ii.i	Anmeldung am Fileserver	xxi
vii.ii.ii	Freigegebene Ordner.....	xxii
vii.ii.iii	Zugriffsverweigerung Admin-Share.....	xxii
vii.ii.iv	Ansicht \Privat	xxii
viii.	Dokumentationen.....	xxiii
viii.i	Anwenderdokumentation	xxiii
viii.ii	Betriebsdokumentation	xxiii

i. Netzwerkläne

i.i Azubi-Testumgebung Ist-Zustand



i.ii Azubi-Testumgebung Soll-Zustand

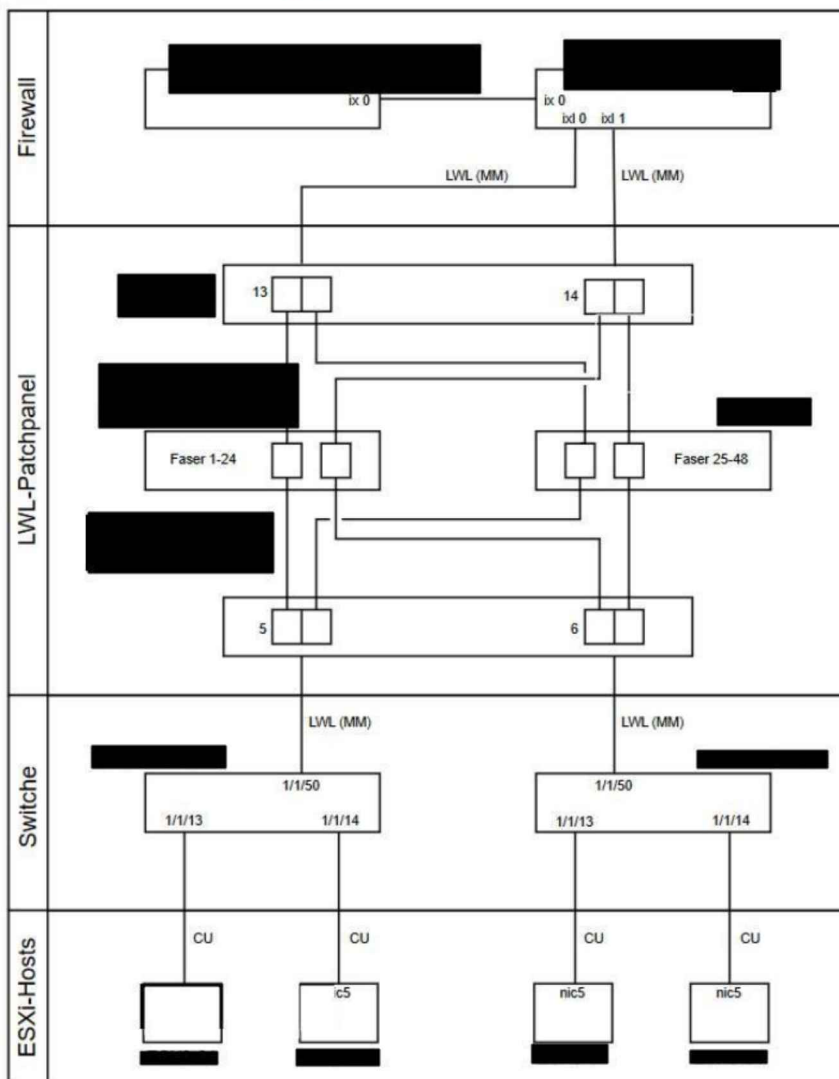


i.iii VLAN-Übersicht

Name	VLAN-ID	Subnetz	Netzmaske	Gateway	Hinweis
Azubi-Netze	1001-1010	10.3.1.0 – 10.3.10.0	255.255.255.0 (/24)	10.3.1.254 – 10.3.10.254	Testnetze
Management	1011	10.3.11.0	255.255.255.0 (/24)	10.3.11.254	Mgmt, vCenter
Verwaltung	1012	10.3.12.0	255.255.255.0 (/24)	10.3.12.254	ESXi, TrueNas, Backup
Server-VMs	1013	10.3.13.0	255.255.255.0 (/24)	10.3.13.254	TS, FS, DC
Storage	1014	10.3.14.0	255.255.255.0 (/24)	10.3.14.254	Storage
DMZ	1015	10.3.15.0	255.255.255.0 (/24)	10.3.15.254	DMZ
Transfernetz	-	10.3.0.252	255.255.255.252 (/30)	-	Transfernetz

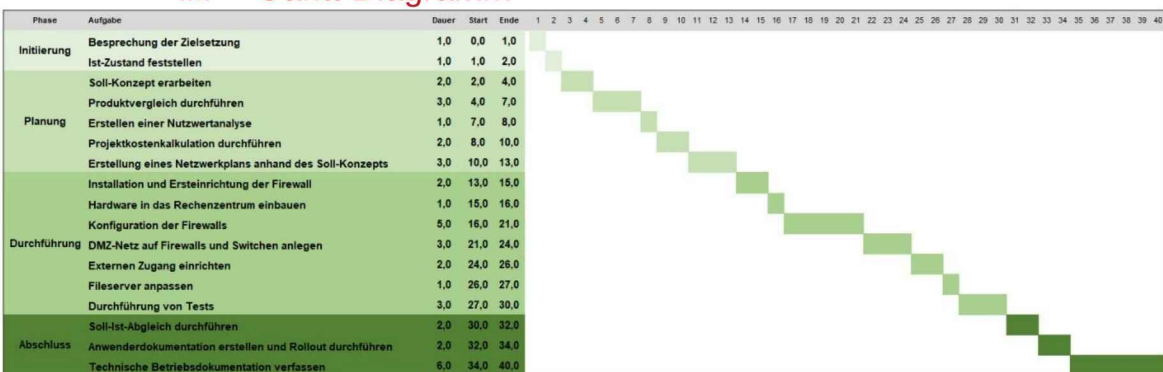
Hinweis: drittes Oktett = letzten 2 Zahlen der VLAN-ID und zweites Oktett = Standort Nummer

i.iv Verkabelungsplan



ii. Kaufmännisch

ii.i Gantt-Diagramm



ii.ii Zeitabgleich

Phase	Aktivität	geplante Zeit	tatsächliche Zeit
Initiierung	Besprechung der Zielsetzung	1	1
	Ist-Zustand feststellen	1	1
Planung	Soll-Konzept erarbeiten	2	2
	Produktvergleich durchführen	3	3
	Erstellen einer Nutzwertanalyse	1	1
	Projektkostenkalkulation Durchführung	2	2
	Erstellung eines Netzwerkplans anhand des Soll-Konzepts	3	3
Durchführung	Installation und Ersteinrichtung der Firewall	2	2
	Hardware in das Rechenzentrum einbauen	1	1,5
	Konfigurieren der Firewalls	5	4,5
	DMZ-Netz auf Firewalls und Switchen anlegen	3	3
	Externen Zugang einrichten	2	2
	Fileserver anpassen	1	2
	Durchführen von Tests	3	2
	Soll-Ist-Abgleich durchführen	2	2
Abschluss	Anwenderdokumentation erstellen und Rollout durchführen	2	2
	Technische Betriebsdokumentation verfassen	6	6
		40	40

ii.iii Preis Fortinet Firewall

Wird oft zusammen gekauft



Gesamtpreis: **825,00 €***

[Auswahl in den Warenkorb](#)

- ☒ **DIESER ARTIKEL: Fortinet FortiGate 60F Firewall – 693,00 €***
Desktop-Hardware-Firewall für kleine bis mittelgroße Betriebe
- ☐ allfirewalls Einrichtungsservice für Ihre Fortinet FortiGate Firewall, 4 Stunden – 600,00 €*
Fachgerechte Einrichtung und Inbetriebnahme Ihrer FortiGate-Firewall durch einen zertifizierten allfirewalls-Spezialisten für Netzwerksicherheit
- ☐ Fortinet FortiCare Premium Support für FortiGate 60F Firewall, Lizenz verlängern oder erstmalig kaufen, 1 Jahr – 138,00 €*
Firmware-Updates, 24x7-Herstellerschutz und Vorabaustausch defekter Hardware mit Versand am nächsten Tag
- ☒ **Rackmount.IT Rack Mount Kit für FortiGate 60E / 61E / 60F / 61F / 70F / 71F / 70G / 71G – 132,00 €***
Montageset zum Einbau in ein 19-Zoll-Server-Rack
- ☐ DrayTek Vigor 167 SuperVectoring ADSL-/VDSL Modem (Annex A+B) – 98,00 €*
SuperVectoring Modem mit Unterstützung aller ADSL-/VDSL-Varianten inkl. Vectoring und Annex-A/B/J/Q/M

ii.iv Rechnung Supermicro

HCM Computer GmbH · Nadorster Straße 162 · 26123 Oldenburg

HCM

HCM Computer GmbH
Nadorster Straße 162
D-26123 Oldenburg
Tel.: +49 441 97156-0
Fax: +49 441 97156-49
E-Mail: info@HCM-Computer.de
Internet: www.HCM-Computer.de

Kunden Nr.: [REDACTED]

Rechnung [REDACTED] Seite - 1 - 07.03.2022

Pos	Artikel	Bezeichnung	Menge	Preis EUR	Gesamt EUR	Ust
01	99-10002	Supermicro Barebone SuperServer SYS-E300-4D PCS3625416 1389675-22222 E242344X1002541	1,0 Stk	824,80	824,80	19%
02	99-10002	KINGSTON KVR26N1958/8 8GB PCS4170380 98614-24222	1,0 Stk	35,70	35,70	19%
03	99-10002	INTEL 545e SSD 128GB M2 PCS4833948 23974-24222 BTLA80320LHK128I BTLA80320MLG128I	2,0 Stk	41,20	82,40	19%
Übertrag					942,90	

Rechnung [REDACTED] Seite - 2 - 07.03.2022

Pos	Artikel	Bezeichnung	Menge	Preis EUR	Gesamt EUR	Ust
Übertrag						942,90
04	99-10002	SUPERMICRO RACKMOUNT KIT MCP-290-30002-0B PCS4809088 482032-3322	1,0 Stk	68,80	68,80	19%
05	99-10002	INTEL Ethernet Converged Network Adapter E10G428TDABLK 1389675-3322 c37D74E68793002	1,0 Stk	318,40	318,40	19%
06	99-10002	Supermicro RiscCard RSC-RR1U-E8 PCS1379425 1389675-3322 VR2155018043	1,0 Stk	26,40	26,40	19%
Lieferdatum: 07.03.2022					Endsumme	1.356,50 EUR
					+MwSt 19.0%	257,74 EUR
					Bruttoendbetrag	1.614,24 EUR

Alle Angaben ohne Gewähr. Es gelten ausschließlich unsere AGB.
Die Ware bleibt bis zur vollständigen Bezahlung unser Eigentum,
auch wenn sie verarbeitet bzw. eingebaut wurden. Sämtliche Lieferungen
erfolgen unter dem verlängerten Eigentumsvorbehalt.

Zahlbar rein netto bis spätestens **21.03.2022**

Ware geprüft: _____ Ware erhalten: _____

ii.v Berechnung Wertminderung Supermicro

Nutzdauer der Supermicro ist durchschnittlich 6 Jahre bzw. 72 Monate

Anschaffung März 2022, ergibt ein Alter von 35 Monaten bei Projektbeginn

Wertminderung/Abschreibung pro Monat $1.614,24 \text{ €} / 72 = 22,42 \text{ €}$ pro Monat

Wertverlust $22,42 \text{ €} * 35 = 784,70 \text{ €}$

Wert bei Projektbeginn $1.614,24 \text{ €} - 784,70 \text{ €} = 829,54 \text{ €}$

ii.vi Kosten eines Arbeitsplatzes 2024

Kosten eines Arbeitsplatzes 2024						
Beschäftigte						
	beitrags- geber- Personal- kosten	gemeinkosten 20 %	Sachkosten	IT-Kosten	KeAP (p.a.)	KeAP (p. Std.) 1.590 Std./p.a.
	52.090 €	10.418 €	6.250 €	3.450 €	72.208 €	45,41
	55.084 €	11.017 €	6.250 €	3.450 €	75.801 €	47,67
	58.023 €	11.604 €	6.250 €	3.450 €	79.327 €	49,89
	59.666 €	11.933 €	6.250 €	3.450 €	81.299 €	51,13
	60.021 €	12.004 €	6.250 €	3.450 €	81.725 €	51,40
	62.239 €	12.448 €	6.250 €	3.450 €	84.387 €	53,07
	71.150 €	14.290 €	6.250 €	3.450 €	95.080 €	59,80
	72.659 €	14.532 €	6.250 €	3.450 €	96.891 €	60,94
	75.705 €	15.141 €	6.250 €	3.450 €	100.546 €	63,24
	81.191 €	16.238 €	6.250 €	3.450 €	107.129 €	67,38
	87.233 €	17.446 €	6.250 €	3.450 €	114.379 €	71,94
	99.696 €	19.939 €	6.250 €	3.450 €	129.335 €	81,34
	98.392 €	19.678 €	6.250 €	3.450 €	127.770 €	80,36
	109.249 €	21.850 €	6.250 €	3.450 €	140.799 €	88,55
	116.324 €	23.265 €	6.250 €	3.450 €	149.289 €	93,89

ii.vii Auskunft Personalabteilung

in 2024 beliefen sich die Personalkosten für Auszubildende im Ausbildungsberuf Fachinformatiker für Systemintegration auf rund 21.000 € jährlich, wenn diese sich zu Beginn des Jahres 2024 im 2. Ausbildungsjahr befanden und zum 01.08. in das 3. Ausbildungsjahr wechselten.
Für Auszubildende im Ausbildungsberuf Fachinformatiker für Systemintegration sind in 2024 Personalkosten von rund 20.100 € jährlich entstanden, wenn diese sich zu Beginn des Jahres 2024 im 1. Ausbildungsjahr befanden und zum 01.08. in das 2. Ausbildungsjahr wechselten.

ii.viii Berechnung Stundenlohn Auszubildende

Durchschnittliche Arbeitgeber-Personalkosten belaufen sich auf 21.000 € laut Anhang ii.vii

Verwaltungsgemeinkosten 20% $21.000 \text{ €} \cdot 0,2 = 4.200 \text{ €}$

Sach- und IT-Kosten können dem Anhang ii.vi entnommen werden

KeAP (p.a.) $21.000 \text{ €} + 4.200 \text{ €} + 6.250 \text{ €} + 3.450 \text{ €} = 34.900 \text{ €}$

Stundenlohn $34.900 \text{ €} / 1.590 = 21,95 \text{ €}$

ii.ix Berechnung Wartungskosten

Geschätzte Wartungszeit pro Jahr 10 Stunden

Stundenlohn Auszubildender drittes Lehrjahr 21,95 €

Wartungskosten im Jahr $10 \cdot 21,95 \text{ €} = 219,50 \text{ €}$

Wartungskosten im Monat $219,50 \text{ €} / 12 = 18,29 \text{ €}$

iii. Firewall - pfSense

iii.i Front-End Firewall

iii.i.i Gateways

Gateways

	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>		Default (IPv4)	WAN			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Transfernetz	TRANSFER	10.3.0.253	10.3.0.253		

Save

Add

Default gateway

Default gateway IPv4

Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6

Automatic

Select a gateway or failover gateway group to use as the default gateway.

iii.i.ii Statische Routen

Static Routes					
	Network	Gateway	Interface	Description	Actions
✓	10.0.0.0/8	Transfernetz - 10.3.0.253	TRANSFER		  
✓	192.168.0.0/16	Transfernetz - 10.3.0.253	TRANSFER		  

iii.i.iii WAN-Interface Upstream Gateway

Static IPv4 Configuration

IPv4 Address

/ 27

IPv4 Upstream gateway

Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

iii.i.iv WAN-Interface Regeln

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/41 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/824.60 MiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN Remote Access	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/2.50 MiB	IPv4 UDP	*	*	WAN address	1195	*	none		OpenVPN Remote Access DMZ	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP		*	WAN address	443 (HTTPS)	*	none			

iii.i.v Transfer-Interface IP-Adresse

Static IPv4 Configuration

IPv4 Address

10.3.0.254

/ 30
















IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

iii.i.vi DMZ-Interface Regeln

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 32/170.20 MiB	IPv4 TCP/UDP	10.3.15.253	*	10.3.13.0/24	AD	*	none			  
<input type="checkbox"/>	✓ 7/73 KiB	IPv4 TCP/UDP	10.3.15.253	*	10.3.13.0/24	49152 - 49652	*	none		RPC Ports	  
<input type="checkbox"/>	✓ 2/3.79 MiB	IPv4 TCP/UDP	10.3.15.0/24	*	10.3.13.0/24	Services	*	none			  
<input type="checkbox"/>	✓ 0/708 B	IPv4 ICMP echoes	DMZ subnets	*	10.3.13.0/24	*	*	none			  
<input type="checkbox"/>	✓ 6/767.21 MiB	IPv4 TCP/UDP	DMZ subnets	*	! RFC_1918	ZugangInternet	*	none			  

Firewall Aliases Ports				
Name	Type	Values	Description	Actions
AD	Port(s)	389, 445, 135, 88		  
Services	Port(s)	53, 123		  
ZugangInternet	Port(s)	443, 80, 21		  

iii.i.vii DNS und NTP

DNS Server Settings

DNS Servers

1.1.1.1

cloudflare-dns.com

none

Address

Hostname

Gateway

Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

Add DNS Server

+ Add DNS Server

DNS Server Override

☐ Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server

If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

DNS Resolution Behavior

Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)

By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

Localization

Timezone

Europe/Berlin

Select a geographic region name (Continent/Location) to determine the timezone for the firewall.
Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.

Timeservers

2.pfsense.pool.ntp.org

Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

Language

English

Choose a language for the webConfigurator

iii.i.viii Firewall Logs dynamische Ports

11:52:14	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55865	10.3.13.253:49669	TCP:S
11:52:10	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55865	10.3.13.253:49669	TCP:S
11:52:08	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55865	10.3.13.253:49669	TCP:SEC
11:52:07	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55865	10.3.13.253:49669	TCP:SEC
11:52:05	WAN	Default deny rule IPv4 (1000000103)	57.129.64.219:39447	[REDACTED]:2577	TCP:S
11:52:01	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55862	10.3.13.253:65024	TCP:S
11:51:59	WAN	Default deny rule IPv4 (1000000103)	64.62.197.229:55545	[REDACTED]:800	TCP:S
11:51:52	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55862	10.3.13.253:65024	TCP:S
11:51:49	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55862	10.3.13.253:65024	TCP:S
11:51:47	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55862	10.3.13.253:65024	TCP:SEC
11:51:46	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55862	10.3.13.253:65024	TCP:SEC
11:51:46	WAN	Default deny rule IPv4 (1000000103)	103.156.210.15:42559	[REDACTED]:3627	TCP:S
11:51:40	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55860	10.3.13.253:49669	TCP:S
11:51:31	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55860	10.3.13.253:49669	TCP:S
11:51:27	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55860	10.3.13.253:49669	TCP:S
11:51:26	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55860	10.3.13.253:49669	TCP:SEC
11:51:25	DMZ	Default deny rule IPv4 (1000000103)	10.3.15.253:55860	10.3.13.253:49669	TCP:SEC

iii.ii Back-End Firewall

iii.ii.i Gateway

Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
Transfernetz	Default (IPv4)	TRANSFER	10.3.0.254	10.3.0.254		

Save
 Add

Default gateway

Default gateway IPv4

Transfernetz

Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6

Automatic

Select a gateway or failover gateway group to use as the default gateway.

iii.ii.ii Transfer-Interface IP-Adresse und Upstream Gateway

Static IPv4 Configuration

IPv4 Address

10.3.0.253

/ 30

IPv4 Upstream gateway

Transfernetz - 10.3.0.254

Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
 On local area network interfaces the upstream gateway should be "none".
 Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.
 Gateways can be managed by [clicking here](#).

iii.ii.iii DNS- und NTP-Delegation

DNS Server Settings	
DNS Servers	<div><div>10.3.0.254</div><div>Address</div><div>Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.</div></div> <div><div></div><div>Hostname</div><div>Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).</div></div>
Add DNS Server	<div>+ Add DNS Server</div>
DNS Server Override	<div><input type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server</div> <div>If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.</div>
DNS Resolution Behavior	<div><div>Use remote DNS Servers, ignore local DNS</div><div>By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.</div></div>
Localization	
Timezone	<div><div>Europe/Berlin</div><div>Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.</div></div>
Timeservers	<div><div>10.3.0.254</div><div>Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!</div></div>
Language	<div><div>English</div><div>Choose a language for the webConfigurator</div></div>

iii.ii.iv NTP-Einstellungen

NTP Server Configuration	
Enable	<div><input checked="" type="checkbox"/> Enable NTP Server</div> <div>You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.</div>
Interface	<div><div>ADMIN BRIDGE1012 TRANSFER Localhost</div><div>Interfaces without an IP address will not be shown. Selecting no interfaces will listen on all interfaces with a wildcard. Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.</div></div>
Time Servers	<div><div>10.3.0.254</div><div><input checked="" type="checkbox"/> Prefer <input type="checkbox"/> No Select <div>Server</div></div><div>Type</div></div>

iv. VPN

iv.i Front-End Firewall CA

Create / Edit CA	
Descriptive name	<input type="text" value="pfsense-Azubi-wan-ca"/> <small>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.</small>
Method	<input type="text" value="Import an existing Certificate Authority"/>
Trust Store	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store <small>When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.</small>
Randomize Serial	<input type="checkbox"/> Use random serial numbers when signing certificates <small>When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.</small>

Existing Certificate Authority	
Certificate data	<div><div>-----BEGIN CERTIFICATE-----</div><div></div></div> <small>Paste a certificate in X.509 PEM format here.</small>
Certificate Private Key (optional)	<div><div>-----BEGIN PRIVATE KEY-----</div><div></div></div> <small>Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).</small>
Next Certificate Serial	<input type="text" value="8"/> <small>Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.</small>

iv.ii OpenVPN-Server-Certificate

Add/Sign a New Certificate	
Method	<input type="text" value="Create an internal Certificate"/>
Descriptive name	<input type="text" value="OpenVPN-Server-Cert"/> <small>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.</small>

Internal Certificate	
Certificate authority	<input type="text" value="pfsense-Azubi-wan-ca"/>
Key type	<input type="text" value="RSA"/>
	<input type="text" value="4096"/> <small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>
Digest Algorithm	<input type="text" value="sha256"/> <small>The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.</small>

Certificate Attributes	
Attribute Notes	<p>The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.</p> <p>For Internal Certificates, these attributes are added directly to the certificate as shown.</p>
Certificate Type	<input type="text" value="Server Certificate"/> <small>Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.</small>

iv.iii OpenVPN-Server

Peer Certificate Authority	pfsense-Azubi-wan-ca
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP
Server certificate	OpenVPN-Server-Cert (Server: Yes, CA: pfsense-Azubi-wan-ca, In Use)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.	
DH Parameter Length	4096 bit
Diffie-Hellman (DH) parameter set used for key exchange.	

Strict User-CN Matching	<input checked="" type="checkbox"/> Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.	
Client Certificate Key Usage Validation	<input checked="" type="checkbox"/> Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").	

Mode Configuration

Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Device mode	tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)	

Tunnel Settings

IPv4 Tunnel Network	10.3.16.0/28
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.	
A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.	

Client Settings

Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet – One IP address per client in a common subnet
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".	

Ping settings

Inactive	3600
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.	

Advanced Configuration

Custom options	<div>push "route 10.3.0.0 255.255.0.0" </div> <div>Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"</div>
Username as Common Name	<input checked="" type="checkbox"/> Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

iv.iv OpenVPN-Server DMZ

Local port

1195

The port used by OpenVPN to receive client connections.

Tunnel Settings

IPv4 Tunnel Network

172.16.0.0/28

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

Advanced Configuration

Custom options

```
push "route 10.3.15.0 255.255.255.0"
```

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

iv.v Gruppe für VPN-User

Assigned Privileges		
Name	Description	Action
WebCfg - System: User Password Manager	Allow access to the 'System: User Password Manager' page.	
		 Add

iv.vi VPN-User anlegen

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	Musterazubi
Password	*****
Full name	
User's full name, for administrative information only	
Expiration date	
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY	
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	admins
Not member of	vpn_users
Move to "Member of" list Move to "Not member of" list	
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

Create Certificate for User	
Descriptive name	Musterazubi-OpenVPN-DMZ-Cert
Certificate authority	pfsense-Azubi-wan-ca
Key type	RSA
	2048
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
Digest Algorithm	sha256
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
Lifetime	3650

iv.vii Clientexport

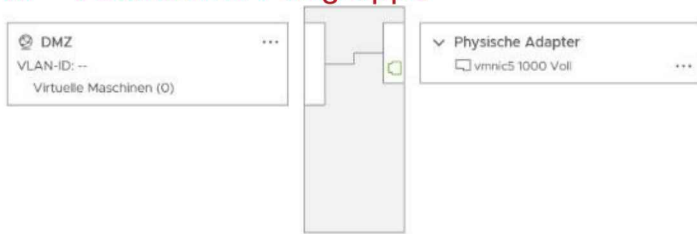
OpenVPN Clients		
User	Certificate Name	Export
Musterazubi	Musterazubi-OpenVPN-DMZ-Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Mac Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Android Config File Only - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none"> 64-bit 32-bit - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none"> 10/2014/2019 7/8/6.1/2013/2015 - Viscosity (Mac OS X and Windows) <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config

iv.viii Clientexport Serverauswahl

OpenVPN Server	
Remote Access Server	OpenVPN-RemoteAccess UDP4:1194
Client Connection Behavior	OpenVPN-RemoteAccess UDP4:1194
	OpenVPN-RemoteAccess-DMZ UDP4:1195

v. vCenter

v.i vSwitch mit Portgruppe



v.ii Berechtigung DMZ-Netz

Rolle ändern | DMZ [X]

Domäne: VSPHERE.LOCAL

Benutzer/Gruppe: Auszubildende

Rolle: **Kein Zugriff**

☐ An untergeordnete Objekte weitergeben

ABBRECHEN OK

v.iii Fileserver

v.iii.i IP Änderung

Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4) [X]

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

☐ IP-Adresse automatisch beziehen

☒ Folgende IP-Adresse verwenden:

IP-Adresse: 10 . 3 . 15 . 253

Subnetzmaske: 255 . 255 . 255 . 0

Standardgateway: 10 . 3 . 15 . 254

☐ DNS-Serveradresse automatisch beziehen

☒ Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server: 10 . 3 . 13 . 253

Alternativer DNS-Server: 10 . 3 . 13 . 252

☐ Einstellungen beim Beenden überprüfen

Erweitert...

OK Abbrechen

v.iii.ii Berechtigung Ordnerfreigabe \Privat

Berechtigungseintrag für "Privat"

Prinzipal: Domänen-Benutzer (Domänen-Benutzer) [Prinzipal auswählen](#)

Typ: Zulassen

Anwenden auf: Nur diesen Ordner

Grundlegende Berechtigungen: [Erweiterte Berechtigungen anzeigen](#)

- ☐ Vollzugriff
- ☐ Ändern
- ☐ Lesen, Ausführen
- ☐ Ordnerinhalt anzeigen
- ☒ Lesen
- ☐ Schreiben
- ☐ Spezielle Berechtigungen

☐ Berechtigungen nur für Objekte und/oder Container in diesem Container übernehmen [Alle löschen](#)

Fügen Sie eine Bedingung zum Beschränken des Zugriffs hinzu. Dem Prinzipal werden die angegebenen Berechtigungen nur gewährt, wenn die Bedingungen erfüllt werden.

[Bedingung hinzufügen](#)

OK Abbrechen

v.iii.iii Berechtigungen privater Ordner

Eigenschaften von Musterazubi

Vorgängerversionen Anpassen Klassifizierung

Allgemein Freigabe Sicherheit

Objektname: D:\Privat\Musterazubi

Gruppen- oder Benutzernamen:

- krueger (krueger@...)
- Muster Azubi (Musterazubi@...)
- Domänen-Admins (Domänen-Admins)
- Administratoren (Administratoren)

Klicken Sie auf "Bearbeiten", um die Berechtigungen zu ändern. [Bearbeiten...](#)

Berechtigungen für "Muster Azubi"

	Zulassen	Verweigern
Vollzugriff	✓	
Ändern	✓	
Lesen, Ausführen	✓	
Ordnerinhalt anzeigen	✓	
Lesen	✓	
Schreiben	✓	
Spezielle Berechtigungen		

Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen. [Erweitert](#)

OK Abbrechen Übernehmen

v.iv Domänen-Controller

v.iv.i GPO geteiltes Laufwerk für Azubis

u_Shared Laufwerk anzeigen

Bereich Details Einstellungen Delegation

Laufwerkzuordnungen

Laufwerkzuordnung (Laufwerk: S) Ausblenden

S: (Reihenfolge: 1) Ausblenden

Allgemein Ausblenden

Aktion	Aktualisieren
Letter	S
Ort	\\[redacted] Shared
Verbindung wiederherstellen	Aktiviert
Beschriften als	Shared
Erste verfügbare Option verwenden	Deaktiviert
Laufwerk aus-/einblenden	Keine Änderung
Alle Laufwerke aus-/einblenden	Keine Änderung

Gemeinsam Ausblenden

Optionen

Bei Fehler keine Elemente mehr für diese Erweiterung verarbeiten	Nein
Im Sicherheitskontext des angemeldeten Benutzers ausführen (Benutzerrichtlinienoption)	Ja
Element entfernen, wenn es nicht mehr angewendet wird	Nein
Nur einmalig anwenden	Nein

Zielgruppenadressierung auf Elementebene: Sicherheitsgruppe

Attribut	Wert
bool	AND
not	0
name	\\[redacted]o_Shared
sid	[redacted]
userContext	1
primaryGroup	0
localGroup	0

Zielgruppenadressierung auf Elementebene: Sicherheitsgruppe

Attribut	Wert
bool	OR
not	0
name	\\[redacted]nv_Shared
sid	[redacted]
userContext	1
primaryGroup	0
localGroup	0

v.iv.ii Basisordner

Eigenschaften von Muster Azubi

Mitglied von Einwählen Umgebung Sitzungen
Remoteüberwachung Remotedesktopdienste-Profil COM+
Allgemein Adresse Konto Profil Rufnummern Organisation

Benutzerprofil

Profilpfad:

Anmeldeskript:

Basisordner

☐ Lokaler Pfad:

☒ Verbinden von: P: Mit:

OK Abbrechen Übernehmen Hilfe

v.iv.iii Registry RPC-Portzuweisung begrenzen

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Internet			
	Name	Typ	Daten
> NET Framework Setup	(Standard)	REG_SZ	(Wert nicht festgelegt)
> NetSh	Ports	REG_MULTI_SZ	49152-49652
> Network	PortsInternetAvailable	REG_SZ	Y
> NetworkController	UseInternetPorts	REG_SZ	Y
> Non-Driver Signing			
> Notepad			

vi. Switche

vi.i Port Konfiguration

```
Last login: 2025-03-03 09:00:06 from 172.26.0.2
User "admin" has logged in 1 time in the past 30 days
# config
(config)# vlan 1015
(config-vlan-1015)# name DMZ
(config-vlan-1015)# exit
(config)# int 1/1/13-1/1/14
(config-if-<1/1/13-1/1/14># vlan access 1015
(config-if-<1/1/13-1/1/14># no shutdown
(config-if-<1/1/13-1/1/14># exit
(config)# int 1/1/50
(config-if)# vlan access 1015
(config-if)# no shutdown
(config-if)# exit
(config)# exit
# write memory
Copying configuration: [Success]
```

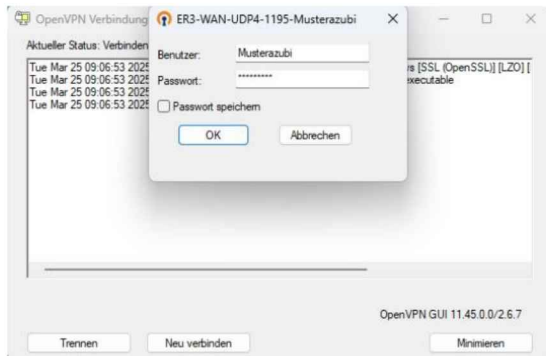
vii. Anwendung

vii.i VPN

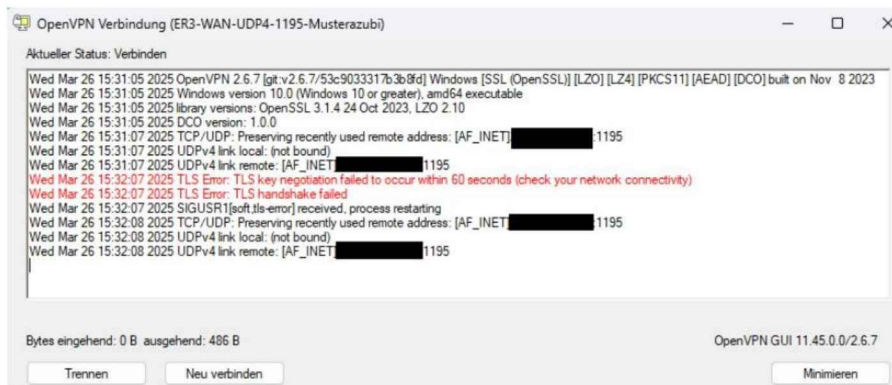
vii.i.i Fehlermeldung Installation



vii.i.ii Anmeldung VPN

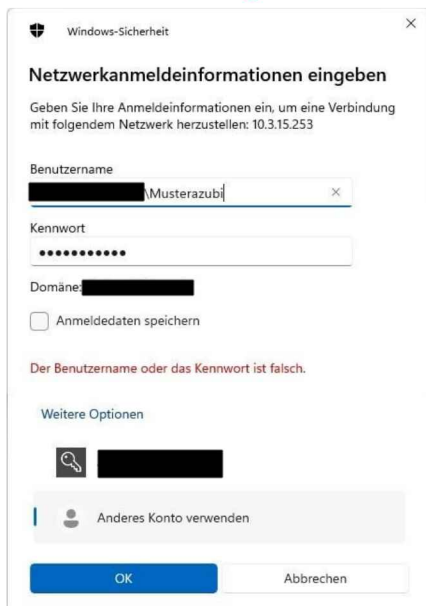


vii.i.iii Verwaltungs-Netz VPN-Verbindung



vii.ii Fileserver

vii.ii.i Anmeldung am Fileserver



vii.ii.ii Freigegebene Ordner



vii.ii.iii Zugriffsverweigerung Admin-Share



vii.ii.iv Ansicht \Privat



viii. Dokumentationen

viii.i Anwenderdokumentation

Zugriff auf den Fileserver der Azubi-Testumgebung über VPN

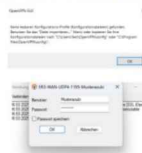
Du kannst Dich nicht am Fileserver anmelden, wenn Du bereits in einem anderen VPN bist oder Du Dich im [REDACTED] befindest!

OpenVPN Installation

Der Installer mit Konfigurationsdatei ist im Anhang der E-Mail. Bei der Installation kann alles einfach bestätigt werden.

Diese Fehlermeldung entsteht, da der neu installierte OpenVPN Client direkt auf Konfigurationsdateien prüft und keine findet, da diese erst im Postinstall eingefügt werden. Die Fehlermeldung kann also ignoriert werden.

Nach der Installation kann man sich mit seinem Benutzer am VPN anmelden. Benutzer und Passwort hast Du ebenfalls in der Mail erhalten.



Passwort ändern

Nach der ersten Anmeldung solltest Du einmal dein Passwort ändern. Das machst Du, indem du in einem Browser Deiner Wahl <https://10.3.15.254> eingibst. Dadurch kommst du zur Oberfläche der pSense und kannst Dich dort mit deinem Benutzer anmelden und Dein Passwort ändern.



Am Fileserver anmelden

Um Dich am Fileserver anzumelden öffnest Du den Explorer und gibst in die Pfadleiste? Die IP-Adresse des Fileservers ein 10.3.15.253.

Es wird eine Fehlermeldung erscheinen, die sagt, dass die Anmeldung fehlergeschlagen ist. Das liegt daran, dass der Computer versucht sich mit dem derzeit angemeldeten Windows Benutzer anzumelden, was nicht geht.

Du musst also im Anmeldefenster die Domäne der Azubi-Testumgebung eintragen, um dich anzumelden.



FYI:

- Wenn Du eine neue VPN-Verbindung bekommst, um zu administrieren, dann musst Du diese unter C:\Program Files\OpenVPN\config einfügen. Du kannst die anderen Konfigurationen ruhig im Ordner lassen. Du kannst Dich beim Verbinden dann für eine der beiden Konfigurationen entscheiden.
- Sobald Du Dich vom Computer abmeldest oder ihn herunterfährst, musst Du Dich am Fileserver neu anmelden.
- Du wirst nach einer Stunde Inaktivität automatisch vom VPN getrennt.

viii.ii Betriebsdokumentation

Einrichten eines VPN-Users

User anlegen

Auf der Oberfläche der pSense unter **System > User Manager > Add** können neue Benutzer angelegt werden.

Die Benennung der User besteht nur aus dem Nachnamen. Falls es doppelte Nachnamen gibt, wird am Ende des Namens jeweils ein weiterer Buchstabe des Vornamens angehängt. Ebenfalls muss ein Passwort vergeben und der User in die Gruppe vpn_users aufgenommen werden.

Jeder User benötigt ein Zertifikat für die VPN-Verbindung, welches erstellt werden muss.

Beim Erstellen des Benutzers kann initial ein Zertifikat angelegt werden. Die Einstellungen können so belassen werden.



Der Deskriptive Name der Zertifikate sieht wie folgt aus:

Musterazubi-OpenVPN-DMZ-Cert

User Zertifikat anpassen

Wenn der Azubi in das dritte Lehrjahr kommt, dann muss sein Zertifikat angepasst werden. Dazu wird im Deskriptiven Namen einfach das „DMZ“ entfernt.

So ist immer ersichtlich, welcher Azubi nur auf den Fileserver darf und welcher administrativ tätig ist.

VPN Konfiguration exportieren

Damit der Azubi das VPN nutzen kann, muss die Konfiguration exportiert werden. Das geht unter **VPN > OpenVPN > Client Export**.

Es muss darauf geachtet werden, dass der richtige VPN-Server ausgewählt ist. Für Konfigurationen für die DMZ und für Administrationsarbeiten.



Anhand der Namen des VPN-Servers ist festzustellen, welcher Server für welche Zwecke ausgewählt werden muss.

Wenn ein Azubi das erste Mal eine VPN-Verbindung erhält und noch kein OpenVPN auf dem betreffenden Gerät installiert ist, muss der **Windows Installer** ausgewählt werden, in welchem Installer und Konfigurationsdateien enthalten sind.

Wenn sich die Berechtigung des Azubis ändert, muss die **Bundles Konfigurations Archive** Option gewählt werden. Dort enthalten sind nur die Konfigurationsdateien.

