

Individuelle Praktische Arbeit

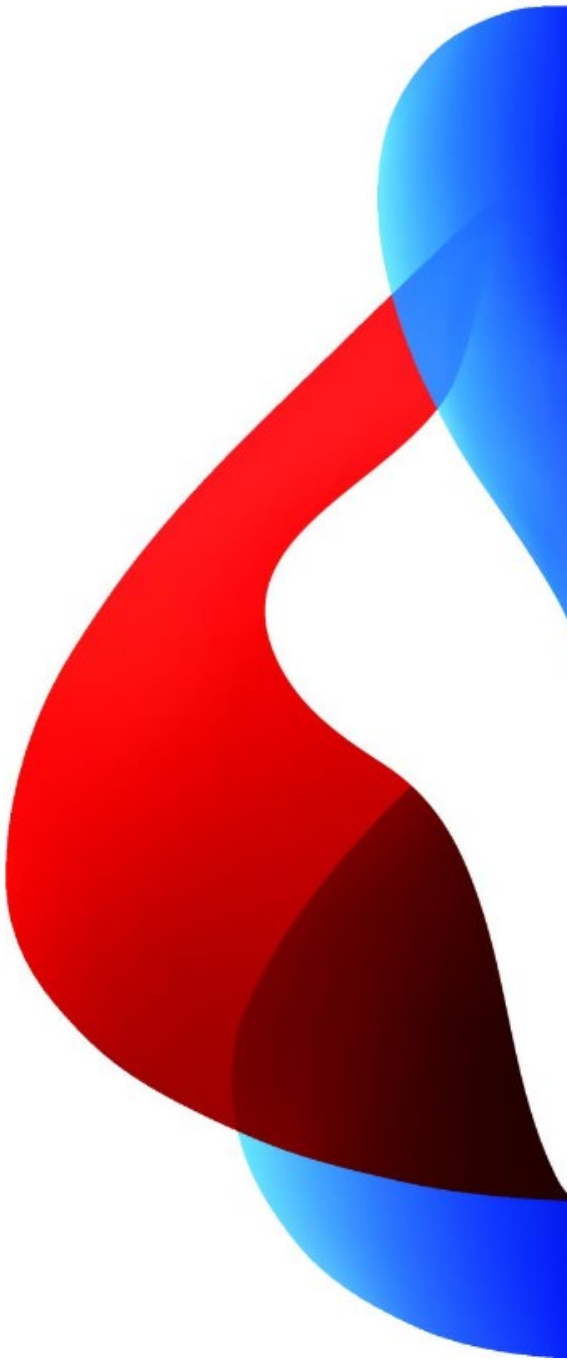
Projektevaluation zur Hybrid-Cloud-Konnektivität mit AWS Site-to-Site VPN

Autor:	Pablo Wynistorf, GHR-POD-NEX-18
Firma und Abteilung:	Swisscom (Schweiz) AG, SBC-MEV-EIT-BDI
Berufsschule:	gibb, Berufsfachschule Bern
Experten:	Cyril Marti (VEX)
	Burak Zendeli (HEX)
	Yunus Cam (NEX)
VF und BB:	Marco Castagna (VF)
	Thomas Albori (BB)
Fachrichtung:	Plattformentwicklung
Projektvorgehensmodell:	HERMES 5.1
Jahrgang:	IPA 2025 Kanton Bern
Ausgabedatum:	04.03.2025

Versionierung

Version	Datum	Autor	Beschreibung / Anpassungen
Vorlage	14.02.2025	Pablo Wynistorf	IPA Dokument Vorlage
0.1	17.02.2025	Pablo Wynistorf	Titelblatt, Zeitplan, Umfeld und Ablauf, Einleitung
0.2	18.02.2025	Pablo Wynistorf	Ist-Situation, Soll-Situation, Projektziele, Auftragsanalyse
0.3	20.02.2025	Pablo Wynistorf	Wahl Projektmanagement Methode, Anforderungen, Abgrenzung, Informationsrecherche, Architektur Konzept
0.4	21.02.2025	Pablo Wynistorf	On-Premises Architekturkonzept, AWS Architekturkonzept, Monitoring-Konzept mit Amazon CloudWatch & SNS-Alarme, BGP-Konzept, VPN-Konzept, Backup-Recovery-Konzept
0.5	24.02.2025	Pablo Wynistorf	Realisierung: On-Premises Umgebung Aufbauen, AWS Umgebung aufbauen
0.6	25.02.2025	Pablo Wynistorf	Realisierung: Aufbau Site-to-Site VPN, Konfiguration BGP
0.7	27.02.2025	Pablo Wynistorf	Realisierung: Konfiguration BGP, Einrichtung Monitoring System
0.8	28.02.2025	Pablo Wynistorf	Realisierung: Testfälle Umsetzung und Dokumentation
0.9	03.03.2025	Pablo Wynistorf	Abschlussberichte
1.0	04.03.2025	Pablo Wynistorf	Kurzfassung, Projektabschluss

Teil 1:
Umfeld und Ablauf



Swisscom (Schweiz) AG
Pablo Wynistorf, GHR-POD-NEX-18
Genfergasse 14
3011 Bern
E-Mail: pablo.wynistorf@swisscom.com

Inhaltsverzeichnis

1 Aufgabenstellung (gemäss PkOrg) 9
1.1 Titel der Arbeit 9
1.2 Ausgangslage 9
1.3 Detaillierte Aufgabenstellung 9
1.4 Mittel und Methoden 10
1.5 Vorkenntnisse 10
1.6 Vorarbeiten 10
1.7 Neue Lerninhalte 11
1.8 Arbeiten in den letzten 6 Monaten 11
2 Deklaration der Firmenstandards 12
2.1 Unternehmensrichtlinien 12
3 Schutzbedarfsanalyse 13
3.1 Swisscom Klassifizierungen 13
3.2 Schutz der Dokumentation 13
3.2.1 Klassifizierung der Dokumentation 13
3.2.2 Schutzmassnahmen für alle IPA-Daten 13
4 Organisation der IPA-Ergebnisse 14
4.1 Datensicherung 14
4.1.1 Wiederherstellung der Daten 15
4.1.2 Versionierung der Dokumente 16
5 Projektmethode 17
5.1 Projektvorgehensmodell 17
5.1.1 Wahl des Projektvorgehensmodells 17
5.1.2 Vergleich verschiedener Projektmanagementmethoden 17
5.1.3 Szenario 18
5.1.4 Phasen 18
5.1.5 Module 20
5.1.6 Meilensteine 20
5.1.7 Phasenfreigaben 21
5.2 Ablauf 23
5.2.1 Arbeitstage 23
5.2.2 IPA-Termine 23
6 IPA Projektaufbauorganisation inkl. Projektrollen 24

6.1 Personen 24
6.1.1 Prüfungskandidat (KAND) 24
6.1.2 Verantwortliche Fachkraft (VF) 24
6.1.3 Hauptexperte (HEX) 24
6.1.4 Nebenexperte (NEX) 25
6.1.5 Berufsbildner (BB) 25
6.2 Rollen 26
6.2.1 Beschreibung der Aufgaben 26
6.3 Organigramm 27
6.4 Rapportierung 28
7 Zeitplan 29
8 Arbeitsjournale 31
8.1 Arbeitsjournal Tag 1 31
8.2 Arbeitsjournal Tag 2 33
8.3 Arbeitsjournal Tag 3 35
8.4 Arbeitsjournal Tag 4 37
8.5 Arbeitsjournal Tag 5 39
8.6 Arbeitsjournal Tag 6 41
8.7 Arbeitsjournal Tag 7 43
8.8 Arbeitsjournal Tag 8 45
8.9 Arbeitsjournal Tag 9 47
8.10 Arbeitsjournal Tag 10 49
9 Abschlussberichte 50
9.1 Vergleich Soll zu finalem Ist 50
9.2 Evaluation der Lösung 51
9.3 Persönliches Fazit 53
9.4 Schlussreflexion 53
10 Kurzfassung des IPA Berichts 55
11 Einleitung 56
12 Initialisierung 57
12.1 Ist-Analyse 57
12.1.1 On-Premises 57
12.1.2 AWS-Seite 57
12.1.3 Netzplan 57
12.2 Soll-Analyse 58
12.2.1 On-Premises 58

12.2.2 AWS-Infrastruktur ... 58
12.2.3 Netzplan ... 59
12.3 Machbarkeitsanalyse (Proof of Concept) ... 60
12.3.1 Technische Realisierbarkeit prüfen ... 60
12.3.2 Mögliche Risiken identifizieren ... 61
12.3.3 Alternativen bewerten ... 61
12.4 Projektziele ... 62
12.4.1 Systemziele (SZ) ... 62
12.4.2 Persönliche Vorgehensweise (VZ) ... 63
12.5 Anforderungen ... 63
12.5.1 Funktionale Anforderungen (FA) ... 63
12.5.2 Nicht funktionale Anforderungen (NFA) ... 63
12.6 Abgrenzungen ... 64
12.7 Informationsrecherche und Grundlagen ... 64
12.7.1 Genutzte Dokumentationen und Quellen ... 64
12.7.2 Erfahrungswerte aus Vorherigen Projekten ... 65
13 Konzept ... 66
13.1 Technische Anforderungen ... 66
13.1.1 Bandbreite ... 66
13.1.2 Standorte ... 66
13.1.3 Verfügbarkeit ... 67
13.1.4 Protokolle ... 67
13.1.5 Sicherheit ... 67
13.2 Gesamte Architektur ... 68
13.2.1 Netzwerkdiagramm ... 68
13.2.2 Definition und Zielsetzung der Architektur ... 68
13.2.3 Netzwerksegmente ... 69
13.3 On-Premises-Architektur ... 70
13.3.1 Komponenten ... 70
13.3.2 OPNsense-Instanzen ... 71
13.4 AWS Architektur ... 73
13.4.1 Komponenten ... 73
13.4.2 AWS Infrastruktur ... 75
13.5 VPN-Konzept ... 76
13.5.1 Architekturübersicht ... 76
13.5.2 VPN-Topologie ... 77

13.6 BGP-Konzept ... 77
13.6.1 Architekturübersicht ... 77
13.6.2 BGP-Topologie ... 78
13.6.3 BGP-Routing-Mechanismen & Failover ... 78
13.7 Monitoring-Konzept ... 79
13.7.1 Architekturübersicht ... 79
13.7.2 Monitoring-Metriken ... 79
13.7.3 Schwellwerte ... 80
13.8 Backup-Recovery-Konzept ... 80
13.8.1 Zielsetzung & Anforderungen ... 80
13.8.2 Backup-Inhalte ... 81
13.8.3 Backup-Strategie & Häufigkeit ... 81
13.9 Testkonzept ... 82
13.9.1 Zielsetzung & Testanforderungen ... 82
13.9.2 Teststrategie & Testverfahren ... 82
13.9.3 Testfälle detailliert ... 83
14 Realisierung ... 87
14.1 On-Premises-Umgebung aufbauen ... 87
14.1.1 Installation der OPNsense Instanzen ... 87
14.1.2 Grundkonfiguration der OPNsense Instanzen ... 99
14.1.3 Updates und Sicherheitsmassnahmen an den OPNsense Instanzen ... 104
14.1.4 Sicherheitsprüfung und Nachweise ... 106
14.1.5 Installation der benötigten OPNsense Plugins ... 108
14.1.6 High-Availability Setup der OPNsense-Instanzen ... 109
14.2 AWS-Umgebung aufbauen ... 121
14.2.1 Erstellung der AWS VPC ... 121
14.2.2 Erstellung der Subnetze in der VPC ... 122
14.2.3 Erstellung der Route Tables ... 124
14.2.4 Definition der AWS Customer Gateways ... 126
14.2.5 Erstellung des AWS Transit Gateways ... 128
14.2.6 Erstellung der AWS Transit Gateway Attachments ... 130
14.2.7 Subnetz-Routing zu Transit Gateway konfigurieren ... 131
14.2.8 Erstellung der beiden AWS Site-to-Site VPN Verbindungen ... 133
14.3 Konfiguration der VPN Verbindung zwischen On-Premises und AWS ... 136
14.3.1 VPN-Konfigurationsdateien herunterladen ... 136
14.3.2 VPN-Verbindung 1 konfigurieren ... 137

14.3.3 VPN-Verbindung 2 konfigurieren ... 145
14.3.4 Konfiguration vom BGP OPNsense Primary ... 147
14.3.5 Konfiguration vom BGP OPNsense Secondary ... 151
14.3.6 Konfiguration der Firewall auf beiden OPNsense Instanzen ... 155
14.4 Erste Connectivity Tests ... 157
14.4.1 On-Premises Testserver Erstellen ... 157
14.4.2 On-Premises Testserver Installieren ... 163
14.4.3 AWS EC2 Testserver Installation ... 171
14.4.4 Verbindungstest durch Pingen der Instanzen ... 174
14.5 Installation der Tunnel Überwachung mittels AWS Cloudwatch und AWS SNS ... 175
14.5.1 AWS SNS Topic erstellen ... 175
14.5.2 CloudWatch Alarm erstellen ... 176
14.6 Testphase ... 178
14.6.1 Testfälle grob mit den Resultaten ... 178
14.6.2 Funktionale Anforderungen mit den Resultaten ... 178
14.6.3 Testfälle detailliert mit Resultat ... 179
14.6.4 Fazit der Tests ... 192
15 Einführung ... 193
15.1 Änderungsprotokoll ... 193
15.2 Dokumentation der Infrastruktur ... 193
16 Verzeichnisse ... 194
16.1 Abbildungsverzeichnis ... 194
16.2 Tabellenverzeichnis ... 198
16.3 Literatur und Quellenverzeichnis ... 200
17 Glossar ... 201
18 Anhang ... 203
18.1 Protokoll vom 1. Expertenbesuch ... 203
18.2 Protokoll vom 2. Expertenbesuch ... 204
18.3 Anhang auf PkOrg ... 205

1 Aufgabenstellung (gemäss PkOrg)

1.1 Titel der Arbeit

Projektevaluation zur Hybrid-Cloud-Konnektivität mit AWS Site-to-Site VPN

1.2 Ausgangslage

In einer zunehmend hybriden IT-Welt bietet Swisscom ihren Kunden neben den eigenen Private-Cloud-Services auch Beratung sowie Professional- und Managed Services für Public-Cloud-Plattformen wie Amazon Web Services (AWS) an. Kunden schätzen die Vorteile der Public Cloud, wie das "Pay-as-you-go"-Modell und die Skalierbarkeit, während sie gleichzeitig bestimmte Workloads weiterhin in ihren eigenen Rechenzentren betreiben. Deshalb gewinnen private Verbindungen zwischen On-Premises-Infrastrukturen und Cloud-Umgebungen zunehmend an Bedeutung. Aufgrund der weit verbreiteten Unterstützung eignet sich ein IPSec-basiertes Site-to-Site-VPN für diese Art der Verbindung.

1.3 Detaillierte Aufgabenstellung

- Nachweis der technischen Machbarkeit einer redundanten Site-to-Site VPN Verbindung zwischen einer On-Premises-Infrastruktur und einem AWS VPC (Virtual Private Cloud) mittels AWS Site-to-Site VPN. Eine redundante AWS Site-to-Site VPN Verbindung besteht aus zwei VPN Verbindungen mit je zwei VPN Tunneln.
- Aufbau eines Monitoring-Systems zur proaktiven Überwachung und Fehlermeldung mittels Amazon CloudWatch und Amazon Simple Notification Service (SNS).
- Bewertung der Zuverlässigkeit und Effizienz der gewählten Lösung.
- Entwicklung einer umfassenden Dokumentation und einer benutzerfreundlichen Anleitung zur Nachahmung der Lösung.

Ziel ist es, eine Lösung zu dokumentieren und zu evaluieren, welche die Konnektivität zwischen einer On-Premises-Infrastruktur und AWS mittels zwei OPNsense-Routern mit redundanten IPSec Site-to-Site VPN-Tunneln und BGP-Routing sicherstellt. Diese Konfiguration basiert auf einer aktiv-aktiv Konfiguration, bei der beide OPNsense-Router jeweils mit eigenem Internetanschluss und öffentlicher IP-Adresse ausgestattet sind, um eine hohe Verfügbarkeit und Ausfallsicherheit zu gewährleisten.

Im Detail umfasst die Aufgabenstellung folgende Punkte:

1) Installation und Konfiguration der Lösung: Die Lösung erfordert eine detaillierte Dokumentation zur Installation und Konfiguration der zwei OPNsense-Router, der redundanten VPN-Tunnel sowie des BGP-Routings. Hierbei wird auf die automatische Fehlererkennung und das Failover zwischen den Routern und VPN-Verbindungen eingegangen. Ziel ist es, sicherzustellen, dass der Verkehr bei einem Ausfall eines Routers oder Tunnels automatisch über den anderen Router bzw. Tunnel geleitet wird.

2) Evaluation der Lösung: Es soll eine Evaluierung erfolgen, wann und in welchen Szenarien diese Lösung sinnvoll ist. Dies umfasst eine Analyse der Redundanz, Verfügbarkeit, Skalierbarkeit und der praktischen Anwendbarkeit, um die Eignung dieser Architektur in verschiedenen betrieblichen Kontexten zu bewerten. Es wird zudem untersucht, unter welchen Bedingungen diese Art der Konnektivität kosteneffizient und zuverlässig ist.

3) Monitoring-System mit CloudWatch und SNS-Alarmen: Ein Monitoring-System wird entwickelt, das mithilfe von Amazon CloudWatch die Zustände der VPN-Tunnel überwacht und im Falle eines Verbindungsverlustes oder Tunnel-Ausfalls einen Alarm über den Amazon Simple Notification Service (SNS) sendet. Dies sorgt für eine zeitnahe Benachrichtigung und ermöglicht schnelles Eingreifen, falls eine VPN-Verbindung instabil wird oder ausfällt.

4) Connectivity-Test zwischen On-Premises und AWS: Ein Connectivity-Test wird durchgeführt, bei dem verschiedene Linux-Instanzen in der On-Premises-Infrastruktur und im AWS VPC getestet werden, indem sie sich gegenseitig anpingen. Ziel dieses Tests ist es, die tatsächliche Funktionsweise der Verbindung zwischen den beiden Umgebungen zu überprüfen und sicherzustellen, dass die redundanten Verbindungen ordnungsgemäss arbeiten.

Die gesamte Lösung wird als Teil einer IPA (Internen Projektarbeit) entwickelt, mit dem Ziel, eine umfassende und leicht verständliche Anleitung zur Einrichtung von AWS Site-to-Site VPN-Verbindungen zu erstellen. Diese soll besonders den Aspekt der Redundanz und der Ausfallsicherheit der Verbindung zwischen On-Premises und AWS betonen, um eine robuste und unterbrechungsfreie Kommunikation zu gewährleisten.

1.4 Mittel und Methoden

Als Projektmanagement-Methode verwendet Pablo Wynistorf HERMES 5.1, eine etablierte und strukturierte Vorgehensweise, die speziell für die Planung und Durchführung von Projekten im IT- und Entwicklungsumfeld entwickelt wurde. HERMES 5.1 bietet klare Rollen, Phasen und Module, die eine transparente und effiziente Projektabwicklung ermöglichen. Diese Methode unterstützt ihn dabei, Ziele präzise zu definieren, Ressourcen effektiv zu nutzen und Risiken frühzeitig zu identifizieren und zu minimieren.

1.5 Vorkenntnisse

Pablo Wynistorf ist AWS Certified Solutions Architect Professional und verfügt über fundierte Kenntnisse in der Arbeit mit AWS-Services. Zusätzlich hat er Erfahrung in der Betreuung von On-Premises-Servern sowie in der Installation und Konfiguration von OPNsense-Systemen. Seine Kombination aus Cloud-Know-how und Praxis in der Verwaltung lokaler IT-Infrastrukturen ermöglicht es ihm, hybride Lösungen effizient umzusetzen.

1.6 Vorarbeiten

Für die Durchführung des Projekts wurden bereits wichtige Vorarbeiten abgeschlossen. Eine Vorlage für die IPA-Dokumentation wurde erstellt, um eine strukturierte und übersichtliche Dokumentation des gesamten Prozesses sicherzustellen. Der AWS-Account ist eingerichtet und einsatzbereit, was die nahtlose Integration und Nutzung der Cloud-Services ermöglicht. Zudem stehen die notwendigen Internetanschlüsse mit öffentlichen IP-Adressen sowie eine Server-Lab-Umgebung bereit. Diese Infrastruktur bildet die Grundlage für die Installation und Konfiguration der OPNsense-Router sowie für die Einrichtung und Evaluierung der Site-to-Site VPN-Verbindungen mit AWS. Mit diesen Vorbereitungen ist die Basis geschaffen, um das Projekt effizient und reibungslos durchzuführen.

1.7 Neue Lerninhalte

Pablo Wynistorf erweitert sein Wissen im Bereich IPsec Site-to-Site VPNs mit BGP, um sichere und hochverfügbare Verbindungen zwischen On-Premises-Infrastrukturen und der Cloud zu realisieren. Der Schwerpunkt liegt dabei auf der Konfiguration von BGP, um dynamisches Routing und automatische Failover-Mechanismen zu ermöglichen. Zusätzlich vertieft er sich in die Einrichtung von Hochverfügbarkeit bei OPNsense-Routern, um sicherzustellen, dass Ausfälle einzelner Geräte oder Verbindungen keine Auswirkungen auf die Netzwerkstabilität haben. Ein weiterer wichtiger Bestandteil ist die umfassende Dokumentation dieser Installationen. Ziel ist es, klar strukturierte Anleitungen zu erstellen, die sowohl technische Details als auch praktische Umsetzungsschritte enthalten. Diese Dokumentationen sollen nicht nur als Referenz für die eigene Arbeit dienen, sondern auch anderen Administratoren die Implementierung solcher Lösungen erleichtern.

1.8 Arbeiten in den letzten 6 Monaten

Pablo Wynistorf arbeitet seit den letzten sechs Monaten bei Swisscom Broadcast im Event ICT Team, das sich auf die Bereitstellung temporärer IT- und Netzwerk-Infrastrukturen für Events spezialisiert. In dieser Rolle konnte er seine Netzwerkkenntnisse, insbesondere im Bereich Routing, vertiefen und in praxisnahen Projekten anwenden. Zuvor hat sich Pablo intensiv mit AWS-Services beschäftigt und dadurch Umfängliches Wissen in Cloud-Technologien aufgebaut. Besonders geprägt wurde sein Wissen durch ein vorheriges Projekt, in dem er sich auf die Konzeption und Umsetzung von Lösungen auf AWS spezialisierte. Seine Teilnahme an den WorldSkills 2024 in Lyon im Bereich Cloud Computing hat sein Know-how weiter gestärkt und ihm umfassende Einblicke in die Arbeit mit modernen Cloud-Technologien gegeben. Diese Erfahrungen machen ihn zu einem vielseitigen Experten, der sowohl in On-Premises- als auch in Cloud-Umgebungen sicher agiert.

2 Deklaration der Firmenstandards

Dieses Kapitel erläutert die internen Standards von Swisscom.

2.1 Unternehmensrichtlinien

Dieses Dokument entspricht bestimmten Firmenstandards hinsichtlich der Gestaltung. Es wurde vollständig in den Schriftarten „TheSans Swisscom“ und „TheSans Swisscom Light“ verfasst. Zudem sind die für Swisscom typischen Farben darin erkennbar, darunter das klassische „Swisscom Navy“.

Im Folgenden sind zwei Darstellungen aus dem internen Brand-Center enthalten, die Informationen zu den charakteristischen Schriftarten und Farben von Swisscom liefern.



Abbildung 1 Swisscom Farben



Abbildung 2 Swisscom Schriften

3 Schutzbedarfsanalyse

Dieser Abschnitt beschreibt den Schutzbedarf der verwendeten Daten für diese IPA.

3.1 Swisscom Klassifizierungen

Die folgende Tabelle gibt einen Überblick über die internen Klassifizierungsstufen von Swisscom. Daten lassen sich in vier verschiedene Level einteilen:

Klassifizierung	Beschreibung
C1 – Public	Allgemeine Informationen über die Swisscom, die öffentlich zugänglich sind.
C2 – General	Informationen, die öffentlich nicht zugänglich sind. Diese sind allerdings für alle Mitarbeiter einsehbar, da sie keine vertraulichen Daten beinhalten.
C3 – Confidential	Vertrauliche Informationen, die nur für auserwählte Gruppen bestimmt sind. Dazu gehören z.B. personenbezogene Daten von Mitarbeitern.
C4 – Strictly Confidential	Streng vertrauliche Daten, die in der Regel nur für wenige Personen bestimmt sind. Diese Daten enthalten geheime Informationen über Mitarbeiter und Kunden, die einer Geheimhaltungspflicht unterstellt sind.

Tabelle 1 Swisscom Klassifizierung

3.2 Schutz der Dokumentation

Dieser Abschnitt behandelt, welcher Klassifizierungsstufe dieses Dokument angehört und was mit allfälligen schützenswerten Daten gemacht wird.

3.2.1 Klassifizierung der Dokumentation

Die Dokumentation dieser IPA umfasst ausschliesslich Daten der Klassifizierungen C1 und C2. Vertrauliche Zugangsdaten werden nur in begrenztem Umfang verwendet, etwa für die konfigurierten OPNsense-VMs oder die Pre-Shared Keys der IPSec-VPN-Verbindungen, die passwortgeschützt eingerichtet sind. Diese Zugangsdaten sind ausschliesslich für diese Umgebung bestimmt und werden nach Abschluss der IPA gelöscht. Sensiblere Zugangsdaten, wie beispielsweise der temporäre Zugriff auf den AWS-Account, sind für diese Arbeit nicht relevant und werden daher nicht dokumentiert. Alle verwendeten und dokumentierten öffentlichen IP-Adressen sind temporär und werden nach Abschluss der IPA nicht mehr im selben Kontext genutzt. Aus diesem Grund werden diese auch in der Dokumentation aufgeführt.

3.2.2 Schutzmassnahmen für alle IPA-Daten

Alle Daten, die durch diese IPA entstehen, werden ausschliesslich auf dem Swisscom internen OneDrive gespeichert. Die entsprechende Ablage kann nur von ausgewählten und befugten Personen eingesehen und bearbeitet werden.

4 Organisation der IPA-Ergebnisse

In diesem Kapitel wird die Organisation der IPA-Ergebnissen dokumentiert.

4.1 Datensicherung

Das nachfolgende Kapitel beschreibt die Vorgehensweise für die Datensicherung der IPA-Dateien. Dieses Konzept stellt sicher, dass keine wichtigen Fortschritte der Arbeit verloren gehen werden.

Die im Rahmen dieser IPA erstellten Dateien werden in der persönlichen OneDrive-Ablage von Swisscom gesichert. Diese Speichermethode gewährleistet eine doppelte Absicherung: Zum einen sind die Daten lokal auf dem Gerät gespeichert, zum anderen existiert bei einem Geräteverlust eine Kopie in der OneDrive-Cloud. Das OneDrive-Verzeichnis ist privat und kann ausschliesslich von autorisierten Personen eingesehen werden.

Folgende Ordnerstruktur wird in der OneDrive-Ablage verwendet:

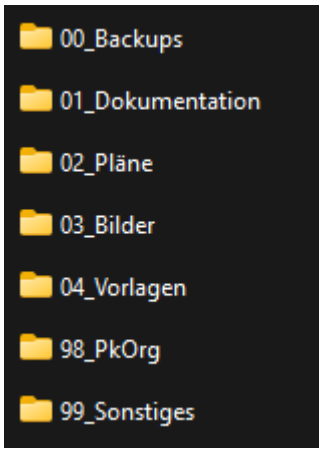


Abbildung 3 IPA Ordnerstruktur

Die Inhalte der Ordner sind folgendermassen definiert:

- **00_Backups**
  - Backup aller erarbeiteten Unterlagen pro Arbeitstag komprimiert als Zip-File.
- **01_Dokumentation**
  - Aktuelle Version der IPA-Dokumentation.
  - IPA-Dokumentenvorgabe
- **02_Pläne**
  - Aktuelle Version des IPA-Zeitplans sowie sonstige Pläne.
- **03_Bilder**
  - Bilder, die für die IPA verwendet wurden.
- **04_Vorlagen**
  - Vorlagen, wie z.B. die Dokumentationsvorlage, die vor IPA-Beginn erstellt wurden.
- **98_PkOrg**
  - Dateien aus PkOrg, wie z.B. der Kriterienkatalog.
- **99_Sonstiges**
  - Sonstige Dateien jeglicher Art.

Als zusätzliche Sicherheitsmassnahme werden am Ende jedes Arbeitstages alle IPA-Dateien als ZIP-Datei auf einer externen SSD gespeichert. Dies bereitet mich für den Fall eines Totalausfalls vor. Dadurch habe ich stets eine Kopie der Dateien vom Vortag, selbst bei einem Datenverlust in der Cloud. Zum Abschluss jedes Tages werden sämtliche IPA-Daten in einen Ordner mit dem jeweiligen Tagesdatum verschoben und anschliessend in eine ZIP-Datei komprimiert. Dies minimiert das Risiko von Datenverlusten und unbeabsichtigten Änderungen an einzelnen Dateien.

Diese Sicherheitskopien haben folgende Ordnerstruktur:



Abbildung 4 IPA Sicherheitskopien

4.1.1 Wiederherstellung der Daten

Durch das tägliche Backup aller Dateien kann jederzeit auf den jeweiligen Stand der verschiedenen Arbeitstage zurückgegriffen werden. Nebst dem ermöglicht es OneDrive, den Versionsverlauf der Dateien anzuschauen. Mit dieser Funktion kann auf Wunsch eine vorherige Version der Dokumentation wiederhergestellt werden:

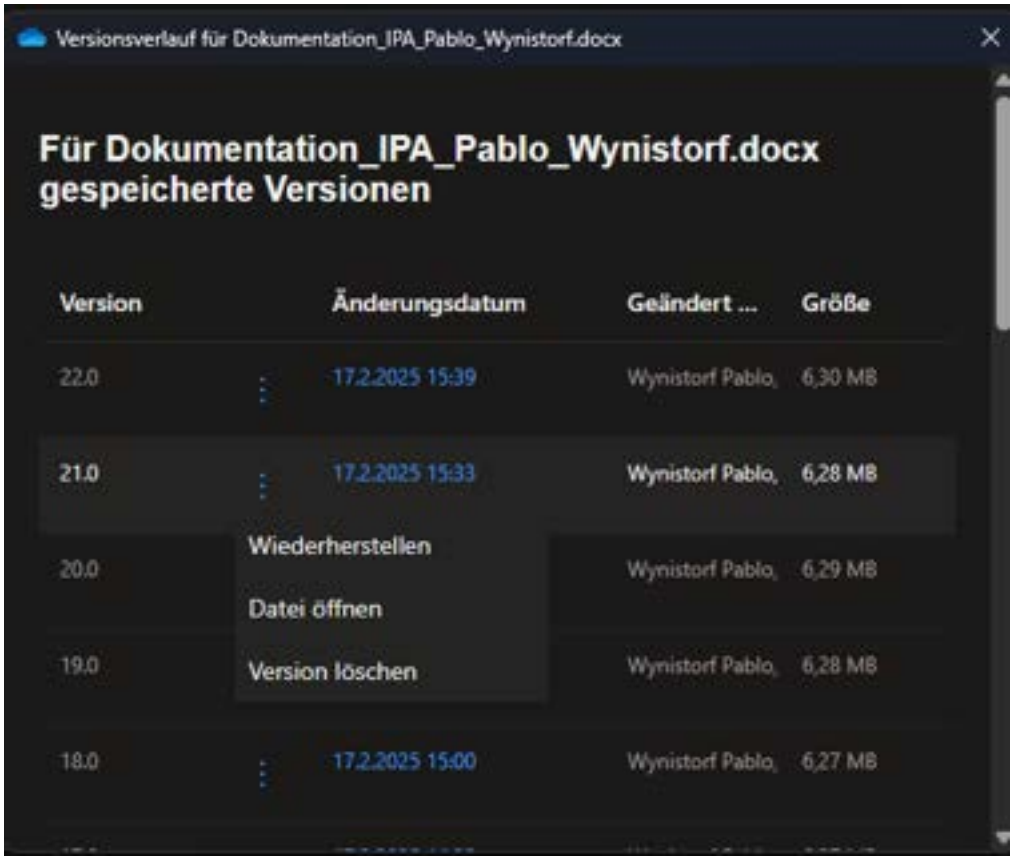


Abbildung 5 Versionsverlauf

4.1.2 Versionierung der Dokumente

Die Dokumentation und der Zeitplan werden regelmässig versioniert. Die ursprüngliche Grundlage der Dokumente wird als «Vorlage» bezeichnet.

Am Ende des ersten Arbeitstages wird die erste Version als 0.1 festgelegt. Anschliessend wird am Ende jedes weiteren Arbeitstages eine neue Version erstellt. Dadurch ergeben sich die folgenden Versionen für den Zeitplan und die Dokumentation:

Version	Bemerkung
Vorlage	Vorlagedokument, welches vor dem IPA Beginn erstellt wurde
0.1	Endversion von Arbeitstag 1
0.2	Endversion von Arbeitstag 2
0.3	Endversion von Arbeitstag 3
0.4	Endversion von Arbeitstag 4
0.5	Endversion von Arbeitstag 5
0.6	Endversion von Arbeitstag 6
0.7	Endversion von Arbeitstag 7
0.8	Endversion von Arbeitstag 8
0.9	Endversion von Arbeitstag 9
1.0	Endversion von Arbeitstag 10

Tabelle 2 Versionstabelle

Die Version 1.0 ist die finale Version der Dokumentation und des Zeitplans. Die IPA-Dokumente werden als Version 1.0 abgegeben.

5 Projektmethode

In diesem Kapitel werden wichtige Punkte über das Projektvorgehen festgehalten.

5.1 Projektvorgehensmodell

Für die Arbeit an diesem Projekt wird die Projektmanagementmethode **HERMES 5.1** verwendet.

5.1.1 Wahl des Projektvorgehensmodells

Die Wahl der Projektmanagement-Methode ist entscheidend für den Erfolg eines Projekts. Für meine IPA habe ich mich für HERMES 5.1 entschieden, da diese Methode eine klare, strukturierte und phasenbasierte Vorgehensweise aufweist. Sie eignet sich besonders gut für IT-Infrastrukturprojekte. Da dieses IPA-Projekt unter anderem den Aufbau und die Evaluation einer neuen IT-Infrastruktur umfasst, erweist sich HERMES 5.1 als eine sinnvolle und passende Wahl. Während der Initialisierungsphase wurde der Auftrag dieses Projekts ausgiebig analysiert und erst im Anschluss wurde die definitive Projektmanagement-Methode ausgewählt. Dazu ist zu erwähnen, dass ich persönlich bereits mehrere Projekte nach den HERMES 5.1-Standards durchgeführt habe und daher über das grösste Vorwissen im Vergleich zu anderen Projektmanagement-Methoden verfüge.

5.1.2 Vergleich verschiedener Projektmanagementmethoden

Methode	Vorteile	Nachteile in Bezug auf dieses IPA-Projekt
Scrum	• Flexibel & wiederholend • Gut für Software-Entwicklung • Klare Rollenverteilung (Product Owner, Scrum Master)	• In gewissen Punkten zu stark auf Software-Entwicklung fokussiert • Funktioniert nicht gut für ein Infrastrukturprojekt • Der Projektablauf passt nicht gut zu Infrastrukturprojekten
Kanban	• Gut geeignet für kontinuierlichen Betrieb • Ideal für Teams mit parallelen Aufgaben • Flexibles und übersichtliches Task-Management	• Meist kein definiertes Endziel • Keine klare Meilenstein-Struktur • Bietet kein Phasenmodell
Wasserfall	• Klare und übersichtliche Phasenstruktur • Gut für Projekte mit klaren Vorgehensweisen	• Ziemlich starr und unflexibel, Änderungen sind eher schwierig • Fortlaufende Anpassungen sind erst am Ende möglich
HERMES 5.1	• Ideal für IT-Infrastrukturprojekte • Klare und nachvollziehbare Phasen • Unterstützte Projektsteuerung durch strikte Rollenverteilung • Klar definierte Projektverantwortlichkeiten	Keine nennenswerten Nachteile für dieses IPA-Projekt

Tabelle 3 Vergleich Projektmethoden

5.1.3 Szenario

Diese IPA ist aus dem Szenario «IT-Infrastruktur» von HERMES 5.1 abgeleitet. Dieses Szenario wurde speziell für die Durchführung von IT-Projekten konzipiert, in denen eine bestehende IT-Infrastruktur erweitert oder optimiert wird, ohne Änderungen an Geschäfts- oder Supportprozessen vornehmen zu müssen.

In diesem Projekt wird die Hybrid-Cloud-Konnektivität zwischen einer bestehenden On-Premises-Infrastruktur und AWS durch eine redundante VPN-Verbindung mit BGP-Routing erweitert. Dafür wird die bestehende Infrastruktur um zwei OPNsense-Router ergänzt, die als zentrale Schnittstelle zwischen der lokalen Umgebung und der AWS-Umgebung dienen. Die Netzwerkintegration erfolgt, ohne dass Änderungen an bestehenden IT-Diensten oder Geschäftsprozessen erforderlich sind.

5.1.4 Phasen

In dieser Arbeit wird das gesamte Phasenmodell von HERMES berücksichtigt. Begonnen hat alles vor IPA-Beginn, mit der konkreten Aufgabenstellung. Diese Deklaration diente als Projekt-Initialisierungsauftrag.

- Aufgrund dieser Aufgabenstellung kann die Initialisierungsphase starten.
- Sobald diese abgeschlossen ist, kann der Auftraggeber die Phasenfreigabe für das Konzept erteilen.
- Wenn die Konzeptphase abgeschlossen wurde, erteilt der Auftraggeber idealerweise die Phasenfreigabe für die Realisierung.
- Nach der erfolgreichen Freigabe zur Einführung kann diese umgesetzt werden.
- Im Anschluss an die Einführungsphase folgt der Projektabschluss.



Abbildung 6 Hermes Phasen

Folgende Tabellen stellen die Projekt- und die persönlichen Meilensteine dar. Die ausführlichen Beschreibungen zu allen Meilensteinen befinden sich in einem späteren Kapitel:

Projekt-Meilenstein	Bedeutung
	Abschluss der Initialisierungsphase → Freigabe für Konzept
	Abschluss der Konzeptphase → Freigabe für Realisierung
	Abschluss der Realisierungsphase → Freigabe für Einführung
	Abschluss der Einführungsphase → Start des IPA-Abschlusses

Tabelle 4 Projekt-Meilensteine

Persönlicher Meilenstein	Bedeutung
	Abschluss des IPA-Starts → Start der Initialisierung
	Abschluss der gesamten Arbeit → Abgabe

Tabelle 5 Persönliche Meilensteine

Folgende Tabelle beschreibt die Standard-HERMES-Phasen:

Projekt-Meilenstein	Bedeutung
Initialisierung	Die Initialisierung schafft eine definierte Ausgangslage für das Projekt und stellt sicher, dass die Projektziele mit den Zielen und Strategien der Organisation abgestimmt sind. Die Projektgrundlagen und der Projektauftrag werden erarbeitet und der Entscheid zur Projektfreigabe wird getroffen.
Konzept	Die in der Initialisierungsphase gewählte Variante wird konkretisiert. Die Ergebnisse werden so detailliert erarbeitet, dass die Projektbeteiligten das Produkt bzw. das IT-System auf einer verlässlichen Grundlage planen, offerieren und realisieren können.
Realisierung	Das Produkt bzw. das IT-System wird realisiert und getestet.
Einführung	Der sichere Übergang vom alten zum neuen Zustand wird gewährleistet. Die Einführungsmassnahmen wie Anwenderschulung etc. werden durchgeführt.

Tabelle 6 Standard HERMES-Phasen

5.1.5 Module

Folgende Module spielen bei dieser Arbeit eine Rolle:

Modul	Beschreibung
Projektsteuerung	• Initialisierung beauftragen und steuern • Projekt steuern
Projektführung	• Projekt planen, führen und in den definierten Rahmenbedingungen mit dem geforderten Ergebnis zum Ziel bringen • Risiken managen • Phasenfreigaben vorbereiten
Testen	• Testkonzept erarbeiten • Testinfrastruktur realisieren • Tests durchführen

Tabelle 7 HERMES-Module

5.1.6 Meilensteine

Die Meilensteine dienen als Orientierungspunkte im Verlauf des Projekts und gelten als abgeschlossen, sobald die zugehörigen Aufgaben erledigt sind.

Die folgende Tabelle zeigt die definierten Meilensteine sowie die darin enthaltenen Aufträge:

Meilenstein	Zu erreichende Aufträge	Bemerkung
1. Projektstart	• Zeitplan erstellen • Titelblatt, Umfeld und Ablauf • Einleitung	Persönlicher Meilenstein
2. Abschluss der Initialisierungsphase	• Ist-Situation • Soll-Situation • Projektziele • Anforderungen • Abgrenzungen	Projekt Meilenstein
3. Abschluss der Konzeptphase	• Architekturkonzept • OPNsense-Router-Konzept • AWS-Infrastrukturkonzept • Monitoring-Konzept • Test-Konzept	Projekt Meilenstein
4. Abschluss der Realisierungsphase	• Installation & Grundkonfiguration der OPNsense-Router und On-Premises-Infrastrukturanpassung MGT-Netz • Einrichtung AWS-Infrastruktur (VPC, Transit Gateway) • Einrichtung der Site-to-Site VPN-Verbindung • Konfiguration von BGP-Routing auf OPNsense & AWS • Einrichtung des Monitoring-Systems mit CloudWatch & SNS-Alarmen	Projekt Meilenstein

	• Test der automatischen Failover-Mechanismen (Router-/Tunnel-Ausfall-Szenarien) • Evaluation der Einsatzszenarien & Vergleich mit Alternativen	
5. Abschluss der Einführungsphase	• Abschlussbericht mit Bewertung der Lösung (Effizienz, Verfügbarkeit, Kosten)	Projekt Meilenstein
6. Projektabschluss	• Erstellung der finalen Projektdokumentation mit Setup-Anleitung • Kurzfassung des IPA-Berichts • Überarbeitung der Dokumentation & Abschlussbericht • Fertigstellung und Abgabe der Arbeit	Persönlicher Meilenstein

Tabelle 8 HERMES Meilensteine

5.1.7 Phasenfreigaben

Bei der Projektmanagementmethode HERMES 5.1 wird für das Voranschreiten zu den nächsten Phasen eine Freigabe benötigt. Dieser Aspekt wird auch in dieser IPA berücksichtigt. Die VF prüft, ob die Kriterien erfüllt werden konnten und somit die nächste Phase freigegeben werden kann. Die Phasenfreigabe wurde jeweils per Mail bestätigt.

Die Nachfolgende Tabelle zeigt die Daten der unterschiedlichen Phasenfreigaben:

Phasenfreigabe für	Wochentag	Datum	Bemerkung
Konzept	Freitag	21.02.2025	Per Mail
Realisierung	Montag	24.02.2025	Per Mail
Einführung	Montag	03.02.2025	Per Mail
Projektabschluss	Dienstag	04.02.2025	Abgabe der IPA

Tabelle 9 Phasenfreigabe

Die Initialisierungsphase wurde nicht speziell freigegeben, da dies bereits mit der Deklaration der detaillierten Aufgabenstellung für diese IPA geschah. Nachdem die konkreten Inhalte der IPA vom Validexperten bestätigt wurden, galt dies automatisch als Freigabe für die Initialisierung.

1. Freigabe Konzeptphase:


[IPA PLW] Freigabe Konzeptphase

Castagna Marco, B2B-ITL-PCL-CLA-2
An: Wynistorf Pablo, GHR-POD-NEX-18

C2 General

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Vielen Dank für das Feedback. | Danke! | Danke für die Rückmeldung! | Feedback

Ciao Pablo

Die Konzeptphase ist aus meiner Sicht ok und abgeschlossen, Du kannst mit der Realisierungsphase weiterfahren.

Merci & Gruess, Marco

Marco Castagna, ICT Architect | Swisscom (Switzerland) Ltd, Enterprise Customers, P.O. Box, CH-3050 Bern |
Phone +41 58 221 40 06 | Mobile +41 79 448 91 78 | marco.castagna@swisscom.com | swisscom.ch/enterprise

Abbildung 7 Freigabe Konzeptphase

2. Freigabe Realisierungsphase


[IPA PLW] Freigabe Realisierungsphase

Castagna Marco, B2B-ITL-PCL-CLA-2
An: Wynistorf Pablo, GHR-POD-NEX-18

C2 General

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Beginnen Sie „Allen antworten" mit: | Danke! | Vielen Dank für das Feedback. | Besten Dank! | Fee

Ciao Pablo

Die Realisierungsphase ist aus meiner Sicht ok und abgeschlossen, Du kannst mit der Einführungsphase weiterfahren.

Merci & Gruess, Marco

Marco Castagna, ICT Architect | Swisscom (Switzerland) Ltd, Enterprise Customers, P.O. Box,
CH-3050 Bern | Phone +41 58 221 40 06 | Mobile +41 79 448 91 78 |
marco.castagna@swisscom.com | swisscom.ch/enterprise

Abbildung 8 Freigabe Realisierungsphase

3. Freigabe Einführungsphase


[IPA PLW] Freigabe Einführungsphase

Castagna Marco, B2B-ITL-PCL-CLA-2
An: Wynistorf Pablo, GHR-POD-NEX-18

C2 General

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Vielen Dank für das Feedback. | Danke! | Danke für die Rückmeldung! | Feedback

Ciao Pablo

Die Einführungsphase ist aus meiner Sicht ok und abgeschlossen, Du kannst zum Projektabschluss übergehen.

Merci & Gruess, Marco

Marco Castagna, ICT Architect | Swisscom (Switzerland) Ltd, Enterprise Customers, P.O. Box,
CH-3050 Bern | Phone +41 58 221 40 06 | Mobile +41 79 448 91 78 |
marco.castagna@swisscom.com | swisscom.ch/enterprise

Abbildung 9 Freigabe Einführungsphase

5.2 Ablauf

In den nachfolgenden Abschnitten werden die Arbeitstage und relevante Termine festgehalten.

5.2.1 Arbeitstage

Arbeitstag	Wochentag	Datum	Ort
1	Montag	17.02.2025	Genfergasse 14, 3011 Bern
2	Dienstag	18.02.2025	Genfergasse 14, 3011 Bern
3	Donnerstag	20.02.2025	Genfergasse 14, 3011 Bern
4	Freitag	21.02.2025	Genfergasse 14, 3011 Bern
5	Montag	24.02.2025	Genfergasse 14, 3011 Bern
6	Dienstag	25.02.2025	Genfergasse 14, 3011 Bern
7	Donnerstag	27.02.2025	Genfergasse 14, 3011 Bern
8	Freitag	28.02.2025	Genfergasse 14, 3011 Bern
9	Montag	03.03.2025	Genfergasse 14, 3011 Bern
10	Dienstag	04.03.2025	Genfergasse 14, 3011 Bern

Tabelle 10 Arbeitstage

5.2.2 IPA-Termine

Termin	Wochentag	Datum	Uhrzeit
IPA Start	Montag	17.02.2025	08:00
Erster Expertenbesuch (Online)	Dienstag	18.02.2025	10:30
Zweiter Expertenbesuch	Freitag	28.02.2025	10:30
Abgabe der IPA	Dienstag	04.03.2025	18:00

Tabelle 11 IPA Termine

6 IPA Projektaufbauorganisation inkl. Projektrollen

In diesem Kapitel sind die involvierten Personen inkl. deren Rolle beschrieben.

6.1 Personen

Es folgen Informationen über die an dieser IPA beteiligten Personen.

6.1.1 Prüfungskandidat (KAND)

Vorname, Name	Pablo Wynistorf
Firma	Swisscom (Schweiz) AG
Strasse	Alte Tiefenaustrasse 6
PLZ, Ort	3050, Bern
Tel. Mobile	
Tel. Geschäft	
E-Mail	pablo.wynistorf@swisscom.com

Tabelle 12 Informationen Kandidat

6.1.2 Verantwortliche Fachkraft (VF)

Vorname, Name	Marco Castagna
Firma	Swisscom (Schweiz) AG
Strasse	Alte Tiefenaustrasse 6
PLZ, Ort	3050, Bern
Tel. Mobile	
Tel. Geschäft	
E-Mail	marco.castagna@swisscom.com

Tabelle 13 Informationen Verantwortliche Fachkraft

6.1.3 Hauptexperte (HEX)

Vorname, Name	Burak Zendeli
Firma	MilenyumSoft GmbH
Strasse	Baarerstrasse 82
PLZ, Ort	6300 Zug
Tel. Mobile	
Tel. Geschäft	-
E-Mail	b.zendeli@milenyumsoft.ch

Tabelle 14 Informationen Hauptexperte

6.1.4 Nebenexperte (NEX)

Vorname, Name	**Yunus Cam**
Firma	trueIT GmbH
Strasse	Hirschmattstrasse 13
PLZ, Ort	6003, Luzern
Tel. Mobile	
Tel. Geschäft	-
E-Mail	cam.yunus@hotmail.com

Tabelle 15 Informationen Nebenexperte

6.1.5 Berufsbildner (BB)

Vorname, Name	**Thomas Albori**
Firma	Swisscom (Schweiz) AG
Strasse	Alte Tiefenaustrasse 6
PLZ, Ort	3050, Bern
Tel. Mobile	
Tel. Geschäft	
E-Mail	thomas.albori@swisscom.com

Tabelle 16 Informationen Berufsbildner

6.2 Rollen

In dieser IPA übernehme ich als Kandidat mehrere Rollen, darunter **Projektleiter**, **Entwickler**, **Testverantwortlicher** und **Tester**.

6.2.1 Beschreibung der Aufgaben

Auftraggeber / Verantwortliche Fachkraft (VF)

- Bestimmt den umzusetzenden Auftrag und dessen Anforderungen
- Unterstützt bei technischen Unklarheiten
- Bewertet die IPA

Hauptexperte (HEX)

- Bewertet die IPA gemeinsam mit VF und NEX, was bedeutet, dass eine enge Zusammenarbeit mit beiden Rollen besteht.
- Kontaktperson für die VF und für den Kandidaten
- Sorgt für eine erfolgreiche Durchführung durch den Kandidaten

Nebenexperte (NEX)

- Bewertet die IPA gemeinsam mit VF und HEX, was bedeutet, dass eine enge Zusammenarbeit mit beiden Rollen besteht.
- Zusätzliche aussenstehende Fachperson

Projektleiter (PL)

- Für die Umsetzung der Vorgaben des VF zuständig
- Administrative Arbeiten, wie z.B. die Erstellung des Zeitplans der Arbeit

Entwickler (DEV)

- Benötigte Konzepte erstellen
- Setzt die Realisierung der Anforderungen und Ziele um

Testverantwortlicher & Tester (TSV)

- Verantwortet die Erstellung der Testkonzepte
- Führt die Tests nach der Realisierung durch

6.3 Organigramm

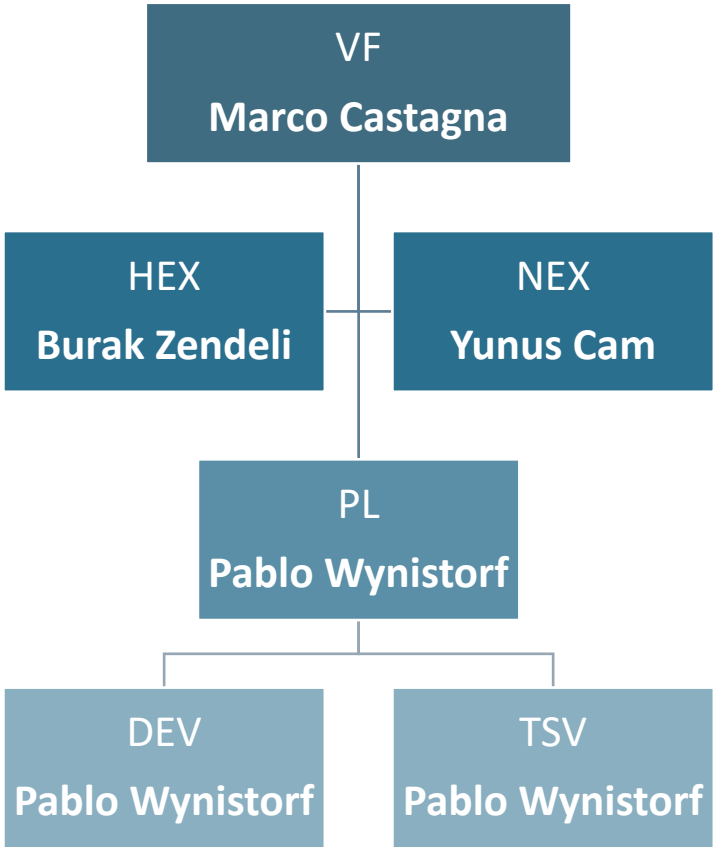


Abbildung 10 Organigramm

Auf diesem Organigramm sind die Abhängigkeiten der Rollen zueinander dargestellt. Marco Castagna ist als verantwortliche Fachkraft (VF) die Person, die die Aufgabenstellung erstellt sowie genaue Anweisungen und Kriterien für den Projektleiter (PL) Pablo Wynistorf definiert.

Der Hauptexperte (HEX) Burak Zendeli bewertet gemeinsam mit dem Nebenexperten (NEX) Yunus Cam und der verantwortlichen Fachkraft (VF) Marco Castagna die Arbeit nach festgelegten Kriterien. Sie fungieren zudem als Unterstützer für den Projektleiter und die verantwortliche Fachkraft.

Der Projektleiter (PL) ist verantwortlich für die Projektmitarbeitenden Entwickler (DEV) und Tester (TSV). Der Entwickler und Tester sprechen nur über den Projektleiter (PL) mit der verantwortlichen Fachkraft (VF) oder dem Haupt- und Nebenexperten.

6.4 Rapportierung

Während der IPA wird täglich ein Arbeitsjournal geführt, um den Fortschritt zu dokumentieren und um Reflexionen aus dem Tag ziehen zu können. Im Arbeitsjournal werden stichwortartig oder in kurzen Sätzen folgende Themen beschrieben:

- Ausgeführte Arbeiten inkl. Soll-Ist-Vergleich nach Zeitplan
- Tagesablauf
- Aufgetretene Probleme
- Hilfestellungen
- Neue Lerninhalte
    - Erfolge?
    - Misserfolge?
    - Herausforderungen?
    - Erkenntnisse?
- Nächste Schritte
- Vergleich mit dem Zeitplan

7 Zeitplan

Die folgenden beiden Abbildungen stellen den finalen Zeitplan dar:

Zeitplan IPA Pablo Wynistorf

Phase	Aktivitäten	Zeit in Stunden		Tag 1 17.02.2025 VM	Tag 1 17.02.2025 NM	Tag 2 18.02.2025 VM	Tag 2 18.02.2025 NM	Tag 3 20.02.2025 VM	Tag 3 20.02.2025 NM	Tag 4 21.02.2025 VM	Tag 4 21.02.2025 NM	Tag 5 24.02.2025 VM	Tag 5 24.02.2025 NM	Tag 6 25.02.2025 VM	Tag 6 25.02.2025 NM	Tag 7 27.02.2025 VM	Tag 7 27.02.2025 NM	Tag 8 28.03.2025 VM	Tag 8 28.03.2025 NM	Tag 9 03.03.2025 VM	Tag 9 03.03.2025 NM	Tag 10 04.03.2025 VM	Tag 10 04.03.2025 NM
IPA-Start & Allgemeines	Zeitplan erstellen & Struktur der Arbeit festlegen	Soll	2.00	1.75	0.25																		
		Ist	2.00	1.75	0.25																		
	Titelblatt, Umfeld & Ablauf der Arbeit definieren	Soll	2.00		1.75	0.25																	
		Ist	2.00		1.75	0.25																	
	Einleitung, Kurzfassung des IPA Berichts, Firmenstandards, Schutzbedarfsanalyse	Soll	1.50			1.50																	
		Ist	1.50			1.50																	
	Organisation der IPA Ergebnisse, IPA Projektorganisation, Projektvorgehen	Soll	1.50				1.50																
		Ist	1.50				1.50																
	Vorbereitung der Projektumgebung	Soll	0.50				0.50																
		Ist	0.50				0.50																
Initialisierung	Soll-Analyse	Soll	2.00			1.75	0.25																
		Ist	2.25			1.75	0.50																
	Ist-Analyse	Soll	1.75				0.75	1.00															
		Ist	2.00				0.75	1.25															
	Projektziele formulieren	Soll	1.00					1.00															
		Ist	1.00					1.00															
	Auftragsanalyse und Wahl einer Projektmethode	Soll	1.75						1.75														
		Ist	2.25						2.00	0.25													
	Anforderungen & Abgrenzungen festlegen	Soll	2.75						1.75	1.00													
		Ist	2.50						1.75	0.75													
	Informationsrecherche	Soll	1.00							1.00													
		Ist	1.00							1.00													
Konzept	Architekturkonzept: Netzwerktopologie	Soll	3.75							2.00	1.75												
		Ist	3.75							2.00	1.75												
	On-Premises Architekturkonzept	Soll	1.75								1.75												
		Ist	1.75								1.75												
	AWS Architekturkonzept	Soll	2.00								2.00												
		Ist	2.25								2.00	0.25											
	Monitoring-Konzept mit Amazon CloudWatch & SNS-Alarme	Soll	1.75									1.75											
		Ist	1.50									1.50											
	Test-Konzept: Connectivity-Tests, Failover-Tests, Performance-Messungen	Soll	2.00									0.25	1.75										
		Ist	2.50									0.25	2.00	0.25									
Realisierung	Installation & Grundkonfiguration der OPNsense-Router und On-Premises Infrastruktur	Soll	3.75										1.75	2.00									
		Ist	4.00										1.50	2.00	0.50								
	Einrichtung AWS Infrastruktur (VPC, Transit Gateway)	Soll	3.75											2.00	1.75								
		Ist	4.50											2.00	2.00	0.50							
	Einrichtung der Site-to-Site VPN-Verbindung	Soll	5.75												2.00	2.00	1.75						
		Ist	5.25												1.50	2.00	1.75						
	Konfiguration von BGP-Routing auf OPNsense & AWS	Soll	5.50														1.75	1.75	2.00				
		Ist	5.75														1.75	1.75	2.00	0.25			
	Durchführung erster Connectivity-Tests	Soll	1.00																	1.00			
		Ist	1.25																	1.00	0.25		
	Einrichtung des Monitoring-Systems mit CloudWatch & SNS-Alarme	Soll	2.75																		2.75		
		Ist	2.75																		2.75		
	Test der automatischen Failover-Mechanismen	Soll	1.75																			1.75	
		Ist	1.75																			1.75	
	Performance-Analyse der VPN-Verbindung	Soll	1.00																				1.00
		Ist	4.75																				2.50
	Feinjustierung der Konfiguration & Troubleshooting	Soll	2.00																				2.00
		Ist	0.50																				0.50
	Evaluation der Einsatzszenarien & Vergleich mit Alternativen	Soll	1.75																				1.75
		Ist	0.50																				0.00

Abbildung 11 Zeitplan 1

Einführung	Abschlussbericht mit Bewertung der Lösung (Effizienz, Verfügbarkeit, Kosten)	Soll	2.75									1.75 1.00	
		Ist	2.00									1.00 1.00	
	Projektreview & Lessons Learned	Soll	2.00									1.00 1.00	
		Ist	2.00									1.00 1.00 (5)	
Abschluss	Erstellung der finalen Projektdokumentation	Soll	3.50									1.00 1.75	0.75
		Ist	3.75									1.00 1.75	1.00
	Kurzfassung des IPA Berichts (Ergebnis)	Soll	1.00										1.00
		Ist	0.25										0.25
	Überarbeitung der Dokumentation & Abschlussbericht	Soll	4.00										2.00 2.00
		Ist	4.50										2.50 2.00
	Fertigstellung und Abgabe der Arbeit	Soll	1.75										1.00 0.75
		Ist	1.75										1.00 0.75 (6)
Administratives	Arbeitsjournal, Zeitplan nachführen & Backups erstellen	Soll	2.50	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
		Ist	2.75	0.25	0.25	0.25	0.50	0.25	0.25	0.25	0.25	0.25	0.25
	Austausch mit Auftraggeber (VF)	Soll	2.50	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
		Ist	2.75	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.50	0.25
	Expertenbesuche	Soll	2.00		1.00						1.00		
		Ist	1.50		1.00						0.50		
Total Vormittag / Nachmittag		Soll											
		Ist											
Total pro Tag		Soll		8.00	8.00	8.00	8.00	8.00	8.00	8.00	8.00	8.00	8.00
		Ist		8.00	8.75	8.00	8.50	8.75	8.00	8.50	8.00	8.00	8.00
Total Insgesamt		Soll		80									
		Ist		82.5									

Soll-Zeit	(blau)
Ist-Zeit	(grün)
Ist-Zeit bei überschreiten der Soll-Zeit	(gelb)
Meeting Soll	(hellorange)
Meeting Ist	(orange)
Persönlicher Meilenstein	X
Projekt-Meilenstein	X

Meilenstein	Abschluss von
1	Projektstart
2	Initialisierungsphase
3	Konzeptphase
4	Realisierungsphase
5	Einführungsphase
6	Projektabschluss

Abbildung 12 Zeitplan 2

8 Arbeitsjournale

In diesem Abschnitt befinden sich die Arbeitsjournale der Arbeitstage.

8.1 Arbeitsjournal Tag 1

Datum	**17.02.2025**		
Ausgeführte Arbeiten	Zeit in Stunden	SOLL	IST
	• Zeitplan erstellen	2h	2h
	• Titelblatt, Umfeld und Ablauf	2h	2h
	• Einleitung, Kurzfassung des IPA Berichts (1. Teil), Firmenstandards, Schutzbedarfsanalyse	1.5h	1.5h
	• Organisation der IPA Ergebnisse, IPA Projektorganisation, Projektvorgehen	1.5h	1.5h
	• Vorbereitung der Projektumgebung	0.5h	0.5h
	• Gespräch mit Auftraggeber	0.25h	0.25h
	• Arbeitsjournal, Zeitplan nachführen & Backups erstellen	0.25h	0.25h
	Total in Stunden	**8h**	**8h**
Tagesablauf	Am Morgen bin ich in die IPA gestartet. Als erstes habe ich mich direkt daran gemacht, den Zeitplan für die IPA zu erstellen. Dank meiner guten IPA-Dokumentationsvorlage konnte ich schnell beginnen, meine im Zeitplan für heute geplanten Aufgaben abzuarbeiten. Danach hatte ich ein kurzes Gespräch mit Marco Castagna (VF). Wir haben über den IPA-Start und den Expertenbesuchstag gesprochen. Alles soweit OK. Die Zeiteinschätzung für die oben genannten Punkte war gut und ich konnte alle Arbeiten bis zum Tagesende erledigen.		
Aufgetretene Probleme	• Excel SUM Funktionen richtig konfigurieren um im Zeitplan eine geordnete Ansicht zu erhalten.		
Hilfestellungen	• Ein Tutorial von Microsoft konnte mir dabei helfen, das Problem zu beheben. • Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.		
Neue Lerninhalte	• Aufbau und Planung einer IPA in Excel Zeitplan		
Reflexion	*Erfolge?* • Ich konnte mir einen sehr guten Überblick über die Arbeit verschaffen • Ich bin perfekt im Zeitplan und konnte alles mir am Morgen Vorgenommene erfolgreich umsetzen.		

	Misserfolge ? • Heute war ein guter Tag, ich hatte keine Misserfolge. *Herausforderungen?* • Die Aufgaben der Arbeit in gute Blöcke aufteilen und die Zeit angemessen einschätzen *Erkenntnisse?* • Es lohnt sich einen guten Zeitplan zu haben, denn dadurch kommt man weniger in den Stress und hat einen guten Überblick auf kommende Arbeiten und die nächsten Schritte
Vergleich Zeitplan	Aktuell bin ich perfekt im Zeitplan. Ich konnte alle mir vorgenommenen Arbeiten erledigen und habe sehr gute Voraussetzungen in den nächsten Arbeitstag zu starten. Dank meines Zeitplans habe ich genau im Blick, was die nächsten Schritte sind.

Tabelle 17 Arbeitsjournal Tag 1

8.2 Arbeitsjournal Tag 2

<table>
<tr><td>Datum</td><td colspan="3">18.02.2025</td></tr>
<tr><td rowspan="9">Ausgeführte Arbeiten</td><td></td><td>SOLL</td><td>IST</td></tr>
<tr><td>• Beschrieb der SOLL-Analyse</td><td>2h</td><td>2.25h</td></tr>
<tr><td>• Beschrieb der IST-Analyse</td><td>1.75h</td><td>2h</td></tr>
<tr><td>• Projektziele Definieren</td><td>1h</td><td>1h</td></tr>
<tr><td>• Auftragsanalyse und Wahl einer Projektmethode</td><td>1.75h</td><td>2h</td></tr>
<tr><td>• Austausch mit Auftraggeber</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>• Erster Expertenbesuch (Online)</td><td>1h</td><td>1h</td></tr>
<tr><td>• Arbeitsjournal, Zeitplan nachführen & Backups erstellen</td><td>0.25h</td><td>0.25</td></tr>
<tr><td>Total in Stunden</td><td>8h</td><td>8.75h</td></tr>
<tr><td>Tagesablauf</td><td colspan="3">Als erstes habe ich die Soll-Analyse ausgefüllt. Um 09:00 hatte ich das Gespräch mit dem Auftraggeber. Alles war soweit gut und wie geplant. Danach konnte ich die Soll-Analyse mit 30 Minuten Verzug fertigstellen. Als nächstes hatte ich den Expertenbesuch der Online statt gefunden hat. Der Ablauf des Meetings war wie folgt:
• Kurze Vorstellungsrunde
• Klärung der Rollen in der IPA
• Sicherstellung der Rollen- und Aufgabenverteilung
• Klärung von Fragen bezüglich einigen Kriterien
• Besprechung Zeitplan
• Besprechung 1. Arbeitsjournal
• Vereinbarung zweiter Besuchstag
• Offene Fragen

Die gesamte Besprechungszeit betrug 50 Minuten. Nach dem Meeting habe ich mich noch ca. 10 Minuten mit dem Auftraggeber über das vergangene Meeting ausgetauscht.

Danach habe am Beschrieb der IST-Analyse weiter gemacht. Nach dem Mittag konnte ich nun auch die IST-Analyse fertigstellen. Bei beiden Analysen habe ich mich Zeitmässig etwas verschätzt. Als nächstes habe ich die Projektziele formuliert. Dies hat gut in die geplante Stunde gepasst. Bis zum Abschluss des Arbeitstages habe ich noch an der Auftragsanalyse und Wahl der Projektmethode gearbeitet. Leider konnte ich diesen Punkt auch noch nicht ganz fertigstellen</td></tr>
<tr><td>Aufgetretene Probleme</td><td colspan="3">• Im Bezug auf technische Probleme ist an diesem Tag nichts aufgetreten
• Ein Problem war aber, dass ich die Zeit der Analysen etwas verschätzt habe, welche mich etwas in Verzug gebracht haben. Ein Teil des Verzuges konnte ich durch längere Arbeitszeit etwas aufholen.</td></tr>
<tr><td>Hilfestellungen</td><td colspan="3">• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.
•</td></tr>
</table>

	• Der Hauptexperte gab mir einige Tipps bezüglich des Arbeitsjournales und der Gliederung des IPA Dokuments
Neue Lerninhalte	• Ich habe einiges über die Projektvorgehensmethode HERMES 5.1 dazugelernt • Ich habe mehr Klarheit über den Verlangten Infrastruktur Aufbau erhalten und welche Services ich einsetzen muss. •
Reflexion	*Erfolge?* • Ich habe immer noch einen guten Überblick über die gesamte Arbeit und was ich zu tun habe. • Der Expertenbesuch hat viele Fragen geklärt und mich noch besser Vorbereitet. *Misserfolge ?* • Ich konnte leider den Abschnitt «Auftragsanalyse und Wahl einer Projektmethode» nicht wie geplant abschliessen. In einem nächsten Projekt würde ich dafür bestimmt mehr Zeit einrechnen. *Herausforderungen?* • Ich hatte Schwierigkeiten die Arbeiten Planmässig abzuschliessen. *Erkenntnisse?* • Ich konnte heute wichtige Puzzleteile zusammenführen was meine allgemeine Sicherheit in der Ausführung der Arbeit verstärkt hat.
Nächste Schritte	Als Nächstes werde ich die «Auftragsanalyse und Wahl einer Projektmethode» abschliessen und die Anforderungen und Abgrenzungen der Arbeit festlegen.
Vergleich Zeitplan	Aktuell bin ich etwas hinter den Zeitplan und muss noch eine Aufgabe von heute am nächsten Arbeitstag fertigstellen. Bin aber ansonsten gut in der Zeit und weiss genau was die nächsten Schritte sind. Ich gehe davon aus, dass ich den Zeitrückstand aufholen kann.

Tabelle 18 Arbeitsjournal Tag 2

8.3 Arbeitsjournal Tag 3

<table>
<tr><td>Datum</td><td colspan="3">20.02.2025</td></tr>
<tr><td rowspan="8">Ausgeführte Arbeiten</td><td></td><td>SOLL</td><td>IST</td></tr>
<tr><td>• Wahl einer Projektmanagement Methode</td><td>0h</td><td>0.25h</td></tr>
<tr><td>• Austausch mit Auftraggeber</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>• Anforderungen & Abgrenzungen festlegen</td><td>2.75h</td><td>2.5h</td></tr>
<tr><td>• Informationsrecherche</td><td>1h</td><td>1h</td></tr>
<tr><td>• Architekturkonzept: Netzwerktopologie</td><td>3.75h</td><td>3.75h</td></tr>
<tr><td>• Arbeitsjournal, Zeitplan nachführen & Backups erstellen</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>Total in Stunden</td><td>8h</td><td>8h</td></tr>
<tr><td>Tagesablauf</td><td colspan="3">Als Erstes habe ich den Auftrag vom Vortag (Wahl einer Projektmethode abgeschlossen). Dies konnte ich in nur 15 Minuten abschliessen. Danach habe ich mich an die Anforderungen und Abgrenzungen gemacht. In der Zwischenzeit hatte ich noch den täglichen Austausch mit dem Auftraggeber. Danach habe ich mit der Informationsrecherche gestartet, um fehlendes Wissen zu erkennen und auszubauen.

In den Nachmittag bin ich dann mit der Konzeptionierung der Architektur gestartet und habe erste richtige Netzwerkpläne erstellt. Die erste fertige Version habe ich dann mit dem Auftraggeber in einem 10 Minütigen Meeting besprochen. Es gab noch einige kleine Tipps und Verbesserungsvorschläge. Der erste Teil der Konzeptionierung konnte ich rechtzeitig zum Arbeitsplan fertigstellen.</td></tr>
<tr><td>Aufgetretene Probleme</td><td colspan="3">• Heute sind keine nennenswerte Probleme aufgetaucht.</td></tr>
<tr><td>Hilfestellungen</td><td colspan="3">• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.
• Der Auftraggeber gab mir einige Tipps und Verbesserungsvorschläge bezüglich des Netzplans, welche ich anschliessend implementiert habe</td></tr>
<tr><td>Neue Lerninhalte</td><td colspan="3">• Funktionalitäten von Failover-Mechanismen der OPNsense Firewall</td></tr>
<tr><td>Reflexion</td><td colspan="3">Erfolge?

• Fertigstellung «Wahl der Projektmethode»
• Anforderungen & Abgrenzungen abgeschlossen
• Lehrreiche Informationsrecherche
• Abschluss Initialisierung
• Erstes Netzwerkdiagramm Fertiggestellt

Misserfolge ?

• Heute war ein guter Tag, ich hatte keine Misserfolge.</td></tr>
</table>

	Herausforderungen? • Erstellung des Netzwerkdiagramms war nicht ganz einfach und brauchte viel Zeit • Es war nicht ganz einfach die Abgrenzungen zu definieren *Erkenntnisse?* • Ich konnte mir wichtige Informationen aneignen. • Ein ausführlicher Netzplan zu erstellen ist nicht einfach •
Nächste Schritte	Als nächstes werde ich am On-Premises Architekturkonzept arbeiten. Danach werde ich ein Konzept für die AWS Infrastruktur erstellen.
Vergleich Zeitplan	Aktuell bin ich sehr gut im Zeitplan. Konnte den Zeitrückstand vom Vortag wieder einholen. Ich genau was die nächsten Schritte sind.

Tabelle 19 Arbeitsjournal Tag 3

8.4 Arbeitsjournal Tag 4

<table>
<tr><td>Datum</td><td colspan="3">21.02.2025</td></tr>
<tr><td rowspan="9">Ausgeführte Arbeiten</td><td></td><td>SOLL</td><td>IST</td></tr>
<tr><td>• On-Premises Architekturkonzept</td><td>1.75h</td><td>1.75h</td></tr>
<tr><td>• Austausch mit Auftraggeber</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>• AWS Architekturkonzept</td><td>2h</td><td>2.25h</td></tr>
<tr><td>• Monitoring-Konzept mit Amazon CloudWatch & SNS-Alarme</td><td>1.75h</td><td>1.5h</td></tr>
<tr><td>• Test-Konzept: Connectivity-Tests, Failover-Tests, Performance-Messungen</td><td>2h</td><td>2h</td></tr>
<tr><td>• Arbeitsjournal, Zeitplan nachführen & Backups erstellen</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>Total in Stunden</td><td>8h</td><td>8h</td></tr>
<tr><td>Tagesablauf</td><td colspan="3">Als erstes habe ich mit dem On-Premises Architekturkonzept gestartet und konnte dies in der geplanten Zeit fertigstellen. Im Austausch mit dem Auftraggeber haben wird den Zeitplan besprochen. Nach dem Austausch habe ich an der Konzeptionierung der AWS Architektur weitergearbeitet und mit etwas Zeitvorsprung abgeschlossen. Glücklicherweise hatte ich genügend Zeit dafür eingeplant, denn in den Kriterien sind noch Punkte zum Vorschein gekommen, bei denen ich drei weitere Konzepte: VPN-, BGP- und Backup-Recovery Konzept machen sollte. Dies hat mich zeitlich stark gefordert, da diese nicht im Zeitplan mit eingeplant waren. Konnte aber das VPN-Konzept noch bis am Mittag abschliessen.

Das BGP-Konzept konnte ich 15 Minuten nach dem Mittag auch abschliessen. Für das Monitoring Konzept habe ich 1h und 45 Minuten eingeplant. Glücklicherweise konnte ich dieses Konzept nach 1h und 30 Minuten bereits abschliessen. Danach habe ich mit dem Backup-Konzept weiter gemacht. Und Konnte dies nach 30 Minuten abschliessen. In der restlichen Zeit habe ich noch am Test-Konzept gearbeitet. Dieses konnte ich leider bis zum ende des Arbeitstages nicht abschliessen. Werde es am Montag Morgen noch fertigstellen.</td></tr>
<tr><td>Aufgetretene Probleme</td><td colspan="3">• Nicht aufgeführte Konzepte im Zeitplan
• Fertigstellung der Konzept-Phase bis Tagesende</td></tr>
<tr><td>Hilfestellungen</td><td colspan="3">• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.</td></tr>
<tr><td>Neue Lerninhalte</td><td colspan="3">• Das Erarbeiten des BGP-Routing Konzepts konnte einige Unsicherheiten im Bezug auf dieses Projekt aus dem Weg räumen.</td></tr>
<tr><td>Reflexion</td><td colspan="3">Erfolge?

• Abschluss des On-Premises Architekturkonzepts
• Abschluss des AWS Architekturkonzepts
• Abschluss des VPN-Konzepts
• Abschluss des BGP-Konzepts</td></tr>
</table>

	• Abschluss des Backup-Recovery-Konzepts *Misserfolge ?* • Nicht fertigstellen der Konzept-Phase wie geplant bis Tagesende. In einem weiteren Projekt würde ich da auch mehr Zeit einplanen. *Herausforderungen?* • Zeitliche Fertigstellung der falsch geplanten Konzepte *Erkenntnisse?* • Ich hätte bei der Erstellung des Zeitplanes mehr noch auf Kriterien achten sollen. Habe mich damals fast nur auf die Aufgabenstellung konzentriert.
Nächste Schritte	Als nächstes werde ich noch das Test-Konzept fertigstellen. Und somit dann auch die gesamte Konzeptphase abschliessen. Danach werde ich mit der Realisierung und Dokumentation starten.
Vergleich Zeitplan	Aktuell bin ich etwas hinter dem Zeitplan, da ich die nicht bedachten Konzepte fertigstellen musste. Ansonsten bin ich eigentlich gut in der Zeit und werde am nächsten Arbeitstag nach einer kurzen Fertigstellung des Test-Konzepts direkt in die Realisierung starten.

Tabelle 20 Arbeitsjournal Tag 4

8.5 Arbeitsjournal Tag 5

<table>
<tr><td>Datum</td><td colspan="3">24.02.2025</td></tr>
<tr><td rowspan="7">Ausgeführte Arbeiten</td><td></td><td>SOLL</td><td>IST</td></tr>
<tr><td>• Testkonzept fertigstellen</td><td>0</td><td>0.25h</td></tr>
<tr><td>• On-Premises Umgebung Aufbauen</td><td>3.75h</td><td>4h</td></tr>
<tr><td>• Austausch mit Auftraggeber</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>• AWS-Umgebung Aufbauen</td><td>3.75h</td><td>4h</td></tr>
<tr><td>• Arbeitsjournal, Zeitplan nachführen & Backups erstellen</td><td>0.25h</td><td>0.25</td></tr>
<tr><td>Total in Stunden</td><td>8h</td><td>8.5h</td></tr>
<tr><td>Tagesablauf</td><td colspan="3">Als ich morgen in den Tag gestartet bin, musste ich zuerst noch das Testkonzept fertig machen. Dies war aber noch wenig, und konnte dies in 15 Minuten abschliessen.

Danach habe ich direkt angefangen, die On-Premises-Infrastruktur aufzubauen und zu dokumentieren. In der Zwischenzeit hatte ich noch den Austausch mit dem Auftraggeber. Ich hatte ungefähr 15 Minuten länger als geplant, weil das CARP zu Beginn nicht richtig funktionieren wollte, und immer beide OPNsense-Instanzen sich als Master gesehen haben.

Kurz nach dem Mittag konnte ich den für heute geplante Part der On-Premises Infrastruktur abschliessen.

Danach habe ich begonnen die AWS-Infrastruktur aufzubauen und zu dokumentieren. Dabei bin ich zwar auf keine grossen Probleme gestossen, habe aber trotzdem etwas mehr Zeit gebraucht als geplant. Ich werde einen Teil der Infrastruktur am nächsten Arbeitstag fertigstellen müssen, da es mir nicht gereicht hat.</td></tr>
<tr><td>Aufgetretene Probleme</td><td colspan="3">• CARP Protokoll der beiden OPNsense Instanzen richtig konfigurieren, konnte das Problem dann aber mit Hilfe dieses Blogs lösen: https://docs.opnsense.org/manual/hacarp.html
• Dokumentations Layout war nicht einfach zu wählen</td></tr>
<tr><td>Hilfestellungen</td><td colspan="3">• https://docs.opnsense.org/manual/hacarp.html
• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.
• ChatGPT hat mich für die Darstellung der Dokumentation inspiriert.</td></tr>
<tr><td>Neue Lerninhalte</td><td colspan="3">• CARP korrekt einrichten, um IP Konflikte zu vermeiden.</td></tr>
<tr><td>Reflexion</td><td colspan="3">Erfolge?
• Fertigstellung der On-Premises-Infrastruktur und Dokumentation
• Fertigstellung des Testkonzepts

Misserfolge ?
• Heute war ein guter Tag, ich hatte keine Misserfolge.</td></tr>
</table>

	Herausforderungen? • Dokumentation für Installation erstellen • CARP zum laufen kriegen *Erkenntnisse?* • Ich hätte wahrscheinlich mehr Zeit für die Realisierung einplanen sollen. Aktuell bin ich nicht schlecht drin, habe aber schon ein wenig Zeitdruck.
Nächste Schritte	Als nächstes werde ich noch die AWS Umgebung fertig aufbauen und dokumentieren, und dann mit der Einrichtung der Site-to-Site VPN starten.
Vergleich Zeitplan	Aktuell bin ich etwas hinter dem Zeitplan, und muss noch etwas, was für heute geplant war am nächsten Arbeitstag fertigstellen. Denke aber, dass ich die Zeit wieder aufholen kann.

Tabelle 21 Arbeitsjournal Tag 5

8.6 Arbeitsjournal Tag 6

Datum	**25.02.2025**		
Ausgeführte Arbeiten	Zeit in Stunden	SOLL	IST
	• Einrichtung der AWS-Infrastruktur	0h	0.5h
	• Einrichtung der Site-to-Site VPN	5.75h	5.25h
	• Austausch mit Arbeitgeber	0.25h	0.25h
	• BGP Konfiguration	1.75h	1.75h
	• Arbeitsjournal, Zeitplan nachführen & Backups erstellen	0.25h	0.25h
	•		
	Total in Stunden	**8h**	**8h**
Tagesablauf	Als erstes habe ich die Dokumentation für die Realisierung der AWS-Infrastruktur fertig gestellt. Dies hat eine halbe Stunde in Anspruch genommen. Glücklicherweise hatte ich für die Einrichtung der Site-to-Site-VPN sehr viel Zeit eingerechnet. Das hat sich im nachhinein als sehr hilfreich herausgestellt, da ich somit genügend Zeit hatte, die Task vom Vortag abzuschliessen und trotzdem on-time die Task von heute fertigstellen konnte. Nach dem Mittag habe ich dann noch das Gespräch mit dem Auftraggeber gehabt. Wir haben kurz über die nächsten Tasks gesprochen und wie es aktuell so läuft. Später habe ich mit der BGP Konfiguration gestartet. Dort bin ich aktuell on-time und werde es höchstwahrscheinlich wie geplant am nächsten Arbeitstag abschliessen können. Der Arbeitstag hat mit dem Ausfüllen des Arbeitsjournales geendet.		
Aufgetretene Probleme	• Ich hatte kurz kleine Probleme mit dem VPN-Setup, da eine Firewall-Rule noch nicht richtig konfiguriert war. Konnte aber dank dieser Dokumentation das Problem lösen: https://medium.com/@swordfish291/opnsense-firewall-site-to-site-vpn-configuration-to-aws-vpc-6d12c2456ea		
Hilfestellungen	• Folgender Blog hat mir dabei geholfen, das Firewall Problem zu lösen: https://medium.com/@swordfish291/opnsense-firewall-site-to-site-vpn-configuration-to-aws-vpc-6d12c2456ea • Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.		
Neue Lerninhalte	• Ich habe gelernt, wie ich die OPNsense-Firewall richtig konfiguriere, so dass die BGP-Verbindung erfolgreich hergestellt werden kann.		
Reflexion	*Erfolge?* • Erfolgreiche Konfiguration der VPNs • BGP Routing Funktioniert auch bereits, muss morgen noch Dokumentation abschliessen		

	Misserfolge ? • Heute war ein guter Tag, ich hatte keine Misserfolge. *Herausforderungen?* • VPN Setup auf den OPNsense-Instanzen war nicht ganz einfach. *Erkenntnisse?* • Ich habe mehr Zeit für die VPN-Konfiguration eingeplant als effektiv genutzt.
Nächste Schritte	Fertigstellung BGP-Dokumentation Durchführung der ersten Connectivity-Tests
Vergleich Zeitplan	Aktuell bin ich hervorragend im Zeitplan. Ich werde am nächsten Arbeitstag direkt mit den für diesen Tag geplanten Arbeiten starten können.

Tabelle 22 Arbeitsjournal Tag 6

8.7 Arbeitsjournal Tag 7

Datum	**27.02.2025**		
Ausgeführte Arbeiten	Zeit in Stunden	SOLL	IST
	• Realisierung: BGP Routing Setup	3.75h	4h
	• Austausch mit Auftraggeber	0.25h	0.25h
	• Durchführung erster Connectivity Tests	1h	1.25h
	• Realisierung: Monitoring System umsetzen	2.75h	2.75h
	• Arbeitsjournal, Zeitplan nachführen & Backups erstellen	0.25h	0.25h
	•		
	Total in Stunden	**8h**	**8.5h**
Tagesablauf	Als erstes habe ich die Realisierung des BGP Routing Setups weiter verfolgt. Das Routing hat bereits am Vortag funktioniert, jedoch hatte ich immer wider Probleme mit der BGP Routenverteilung. Deshalb habe ich mit der Dokumentation etwa 15 Minuten länger gebraucht als eigentlich geplant. In der Zwischenzeit hatte ich noch das Gespräch mit dem Auftraggeber. Aktuell weiterhin alles OK und in grünen Bereich. Danach habe ich mich an die erste Connectivity Tests gemacht. Dabei habe ich mich auch etwas verschätzt, da ich in diesem Kapitel auch die vier Testserver aufsetzen wollte. Aber wenn man es so betrachtet, konnte ich die Zeit den Umständen entsprechend sehr gut einhalten. Die Connectivity Tests waren nach der Installation der Instanzen erfolgreich. Alle Vorgegebenen Routen und Ziele konnten erreicht werden. Nach den Connectivity Tests habe ich dann noch an der Realisierung des Monitoring Systems gearbeitet. Geplant waren dafür 2.75h, dies war ziemlich grosszügig geschätzt. Ich hatte eine erste laufende Lösung nach nur 2.5h, die restliche Zeit konnte ich aber sehr gut einsetzen um die Dokumentationen der Umsetzung im allgemeinen zu überarbeiten. Als Tagesabschluss habe ich dann noch das Arbeitsjournal ausgefüllt, den Zeitplan nachgeführt und die Backups der IPA-Dateien erstellt.		
Aufgetretene Probleme	• Ich hatte einige Probleme mit der BGP-Routenverteilung. Der Secondary Router hat irgendwie nicht immer alle Routen zu AWS erhalten. Dies sorgte dafür, dass bei einem Ausfall des Primary OPNsense-Routers das Failover nicht funktioniert hätte. Um das Problem zu lösen, bin ich die Konfiguration noch einmal durchgegangen. Dabei habe ich eine Misskonfiguration entdeckt, welche das Problem verursacht hat. Jetzt funktioniert aber alles wieder.		
Hilfestellungen	• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.		
Neue Lerninhalte	• Ich habe einiges über BGP-Troubleshooting gelernt.		

Reflexion	*Erfolge?* • Erfolgreiche Connectivity Tests der VPN-Verbindungen • Erfolgreiche Implementation des Monitoring Systems • Ich konnte das BGP Problem mit der Secondary-OPNSense-Instanz lösen *Misserfolge ?* • Ich hatte für die Realisierung der BGP-Konfiguration länger gebraucht als eigentlich geplant *Herausforderungen?* • Das BGP-Problem hat mich kurzzeitig sehr herausgefordert, da ich nicht wusste was das Problem ist und ob ich es in dieser kurzen Zeit lösen kann. *Erkenntnisse?* • Es lohnt sich meistens mehrmals über Konfigurationen darüber zu schauen, um Fehler zu erkennen und um diese frühzeitig beheben zu können.
Nächste Schritte	Als nächstes werde ich ins Testing übergehen. Und die verschiedenen Testkonzepte durcharbeiten und somit das gesamte Netz analysieren.
Vergleich Zeitplan	Trotz einiger Schwierigkeiten am Morgen konnte ich alles aufholen und bin jetzt mit ein wenig Zeit über dem Soll wieder super im Zeitplan. Am nächsten Arbeitstag kann ich direkt mit den für diesen Tag geplanten Aufgaben starten.

Tabelle 23 Arbeitsjournal Tag 7

8.8 Arbeitsjournal Tag 8

Datum	**28.02.2025**		
Ausgeführte Arbeiten	Zeit in Stunden	SOLL	IST
	• Durchführung der Testfälle	3.75h	3.75h
	• 2. Expertenbesuch	1h	0.5h
	• Austausch mit Auftraggeber	0.25h	0.25h
	• Feinjustierung der Konfiguration & Troubleshooting	1h	1h
	• Evaluation der Einsatzszenarien & Vergleich mit Alternativen	1.75	1h
	• Arbeitsjournal, Zeitplan nachführen & Backups erstellen	0.25h	0.25h
	Total in Stunden		

Tagesablauf	Als erstes habe ich mit der Durchführung der Testfälle gestartet. Der Zeitplan hat eine komische Aufteilung gehabt. Aus diesem Grund habe ich alle Testfälle in eine Task zusammengeführt. Und die eingeplanten Zeiten aller einzelnen Punkte miteinander addiert.
	
	Als nächstes war auch schon der Expertenbesuch.
	
	Dies war der Ablauf des Meetings:
	• Kurzer Rückblick auf die Projektzeit vom Kandidat
	• Vorstellungsrunde mit dem Nebenexperten
	• Dokument gemeinsam durchgegangen
	• Arbeitsjournal angeschaut → Alles OK
	• Zeitplan angeschaut → Alles OK
	• Kurze Infrastruktur Demo
	• Hinweis Präsentation:
	  ○ Präsentation nach Kriterien Machen
	  ○ Nicht zu technisch werden
	• Hinweis Demo:
	  ○ 5-10 Minuten
	• Hinweis Fachgespräch:
	  ○ 6 Fragenkomplexe
	  ○ Maximal 30 Minuten
	  ○ 3-4 Fragen pro Fragenkomplex
	
	Tipps von Experten bezüglich Abgabe:
	• 15 Minuten vor Abgabetermin abgeben
	• IPA Dokumentationskriterien beachten
	
	Fragen an die Experten:
	• Deklaration Verwendung von ChatGPT → Deklaration im Arbeitsjournal
	
	Das Meeting hat nur 30 Minuten statt den geplanten 60 Minuten gedauert. In den restlichen 30 Minuten habe ich das Meeting-Protokoll fertiggestellt. Und einige Punkte in der Dokumentation überarbeitet.		

	Anschliessend hatte ich direkt das Meeting mit dem Auftraggeber. Er hat mir noch einige Tipps bezüglich Abbildungsverzeichnis und Tabellenverzeichnis gegeben. Danach habe ich an den Testfällen weitergearbeitet. Dies hat insgesamt etwas länger gedauert als geplant, da ich es im Zeitplan zeitlich verschätz habe und mehr Testen musste als zu beginn eigentlich gedacht. Konnte alle Testfälle aber bis zum ende des Tages fertigstellen. Dies hat dafür gesorgt, dass ich den letzten Punkt auf dem Zeitplan nicht gestartet habe: Evaluation der Einsatzszenarien & Vergleich mit Alternativen Am ende des Arbeitstages habe ich noch das Arbeitsjournal ausgefüllt und die Backups der IPA-Dateien erstellt.
Aufgetretene Probleme	• Ich hatte eine schlechte Planung im Zeitplan. Darum konnte ich nicht alle für diesen Tag geplanten Aufgaben erledigen.
Hilfestellungen	• Mein Auftraggeber hat mir noch gezeigt wie ich das Tabellenverzeichnis und Abbildungsverzeichnis machen kann. • Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.
Neue Lerninhalte	• Erstellung der Tabellenverzeichnisse und Abbildungsverzeichnisse.
Reflexion	*Erfolge?* • Erfolgreicher Abschluss aller Testfälle. Alle Testfälle waren erfolgreich, und alle Anforderungen wurden erfüllt. *Misserfolge ?* • Der Zeitplan hatte einen Fehler in der Planung, welcher dafür gesorgt hat, dass ich nicht geplanten Aufgaben für den heutigen Tag erledigen konnte. *Herausforderungen?* • Es war nicht ganz einfach den Backup-Recovery Test durchzuführen, da ich zuerst nicht genau wusste, wie ich den erfolgreichen Prozess beweisen konnte. *Erkenntnisse?* • Es wäre definitiv sinnvoll, nach der Konzeptphase den Zeitplan zu überarbeiten, um solche Probleme wie heute zu vermeiden.
Nächste Schritte	Als nächstes werde ich die geplante Aufgabe für heute fertigstellen und danach den Abschlussbericht erstellen.
Vergleich Zeitplan	Nach dem heutigen Tag bin ich etwas hinter dem Zeitplan. Ich denke aber, dass ich es nächste Woche gut aufholen kann, da ich viel Pufferzeit in der Endphase eingeplant habe.

Tabelle 24 Arbeitsjournal Tag 8

8.9 Arbeitsjournal Tag 9

<table>
<tr><td>Datum</td><td colspan="3">03.03.2025</td></tr>
<tr><td rowspan="9">Ausgeführte Arbeiten</td><td>Zeit in Stunden</td><td>SOLL</td><td>IST</td></tr>
<tr><td>• Evaluation der Einsatzszenarien</td><td>0h</td><td>0.5h</td></tr>
<tr><td>• Abschlussberichte</td><td>2.75h</td><td>2h</td></tr>
<tr><td>• Austausch mit Auftraggeber</td><td>0.25h</td><td>0.5h</td></tr>
<tr><td>• Einführung (Änderungsprotokoll, Dokumentation der Infrastruktur)</td><td>2h</td><td>2h</td></tr>
<tr><td>• Erstellung der finalen Projektdokumentation</td><td>2.75h</td><td>2.75h</td></tr>
<tr><td>• Arbeitsjournal, Zeitplan nachführen & Backups erstellen</td><td>0.25h</td><td>0.25h</td></tr>
<tr><td>Total in Stunden</td><td>8h</td><td>8h</td></tr>
<tr><td>Tagesablauf</td><td colspan="3">Als erstes habe ich noch die Aufgabe vom Vortag fertig gemacht. Dabei musste ich kurz die Evaluation der Einsatzszenarien schreiben. Dies konnte ich in ca. 30 Minuten abschliessen. Danach habe ich mit an die Abschlussberichte gemacht. In der Zwischenzeit hatte ich noch das Meeting mit Marco Castagna (VF). Dieses Meeting hat heute etwas länger gedauert als geplant, da wir noch einiges bezüglich der Abgabe besprochen haben. Die Abschlussberichte konnte ich in zwei Stunden abschliessen.

Die Arbeitsaufteilung im Zeitplan war heute erneut wieder etwas komisch. Darum habe ich die Einführung mit dem Änderungsprotokoll auch noch in dieser Zeit erledigt.

Danach habe ich noch die geplante Zeit an der Überarbeitung der IPA-Dokumentation gearbeitet.

Als Tagesabschluss habe ich noch das Arbeitsjournal geschrieben und die Backups erstellt.</td></tr>
<tr><td>Aufgetretene Probleme</td><td colspan="3">• Heute sind keine technischen Probleme aufgetreten.</td></tr>
<tr><td>Hilfestellungen</td><td colspan="3">• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet oder als Inspiration für verständlichere Formulierung verwendet.</td></tr>
<tr><td>Neue Lerninhalte</td><td colspan="3">• Heute habe ich nichts erwähnenswertes gelernt, da der Tag aus viel Fleissarbeit bestanden hat.</td></tr>
<tr><td>Reflexion</td><td colspan="3">Erfolge?

• Ich konnte alle mir vorgenommenen Aufgaben zeitgerecht erfüllen.
• Ich habe kein Abgabestress, da ich sehr gut in der Zeit bin und die meisten Kriterien bereits abgedeckt habe.

Misserfolge ?

• Heute gab es keine grossen Misserfolge.</td></tr>
</table>

	Herausforderungen? • Es war am Anfang etwas herausfordernd, den komisch gegliederten Zeitplan neu für die restlichen Angaben anzupassen und die Aufgaben für den Tag zu definieren. Dies hat aber am ende sehr gut funktioniert. *Erkenntnisse?* • Es wäre definitiv sinnvoll, nach der Konzeptphase den Zeitplan zu überarbeiten, um solche Probleme wie heute zu vermeiden.
Nächste Schritte	Als nächstes werde ich die IPA-Dokumentation überarbeiten und für die Abgabe vorbereiten. Ich möchte die Texte noch auf Rechtschreibung prüfen und korrigieren.
Vergleich Zeitplan	Aktuell bin ich sehr gut im Zeitplan. Ich konnte alle für heute geplanten Punkte fertigstellen und habe gute Voraussetzungen für eine rechtzeitige Fertigstellung der Arbeit.

Tabelle 25 Arbeitsjournal Tag 9

8.10 Arbeitsjournal Tag 10

Datum	**04.03.2025**		
Ausgeführte Arbeiten	Zeit in Stunden	SOLL	IST
	• Erstellung der finalen Projektdokumentation	0.75h	1h
	• Austausch mit dem Auftraggeber	0.25h	0.25h
	• Kurzfassung des IPA Berichts	1h	0.25h
	• Überarbeitung der IPA	4h	4.5h
	• Fertigstellung der Arbeit	1.75h	1.75h
	• Arbeitsjournal, Zeitplan und Backups	0.25h	0.25h
	Total in Stunden	**8h**	**8h**
Tagesablauf	Zuerst habe ich die Projektdokumentation überarbeitet und eine vergessene Sicherheitsprüfung für die Appliance-Installation ergänzt. Danach besprach ich mit Marco Castagna den Projektabschluss und die Abgabe. Zusätzlich half er mir noch dabei, die Darstellung auf gewissen Seiten zu verbessern. Anschliessend stellte ich die Kurzfassung des IPA-Berichts fertig, was weniger Zeit benötigte als geplant. Kurz vor Mittag überprüfte ich die IPA auf Formatierung, Verzeichnisse und Rechtschreibung. Abschliessend füllte ich das Arbeitsjournal aus, finalisierte den Zeitplan und bereitete die IPA für die Abgabe vor.		
Aufgetretene Probleme	• Heute sind keine technischen Probleme aufgetreten.		
Hilfestellungen	• Texte wurden teilweise mithilfe von ChatGPT grammatikalisch überarbeitet.		
Neue Lerninhalte	• Heute habe ich nichts erwähnenswertes gelernt, da der Tag aus viel Fleissarbeit bestanden hat.		
Reflexion	*Erfolge?* • Ich konnte alle mir vorgenommenen Aufgaben zeitgerecht erfüllen. • Ich konnte die IPA rechtzeitig fertigstellen. *Misserfolge ?* • Heute gab es keine grossen Misserfolge. *Herausforderungen?* • Heute hatte ich keine grossen Herausforderungen. *Erkenntnisse?* • Über die gesamte IPA hinweg hatte ich einen sehr guten Zeitplan, der dafür sorgte, dass ich stressfrei arbeiten konnte.		
Nächste Schritte	Abgabe der IPA-Dokumentation und Anhang.		
Vergleich Zeitplan	Die IPA konnte Zeitgerecht fertiggestellt werden.		

Tabelle 26 Arbeitsjournal Tag 10

9 Abschlussberichte

Im nachfolgenden Kapitel sind die Abschlussberichte dieser IPA beschrieben.

9.1 Vergleich Soll zu finalem Ist

Alle definierten und geplanten funktionalen Anforderungen konnten erreicht werden. Somit gelten die geplanten Systemziele als vollständig umgesetzt. Eine Weiterentwicklung ist derzeit nicht erforderlich, da die gesetzten Ziele vollständig erreicht wurden und die Skalierbarkeit durch die gewählte Architektur gewährleistet ist.

Die Hybrid-Cloud-Konnektivität zwischen On-Premises und AWS wurde erfolgreich mittels einer hochverfügbaren VPN-Verbindung hergestellt.

Zielvorgabe (Soll-Zustand)	Tatsächliche Umsetzung (Ist-Zustand)	Erkenntnisse / Optimierungspotenzial
Redundante VPN-Verbindung mit OPNsense	Erfolgreich implementiert mit zwei VPN-Verbindungen über zwei dedizierte Internetanschlüsse	Architektur ist stabil, Failover funktioniert zuverlässig.
BGP-Routing mit Failover-Mechanismus	BGP-Routing eingerichtet, Failover getestet	Failover-Zeiten konnten durch Feintuning optimiert werden.
Monitoring mit CloudWatch & SNS	Erfolgreich umgesetzt, Alarmierungen getestet	Schwellenwerte für Alarme angepasst für bessere Reaktionszeiten.
Connectivity-Test zwischen On-Prem und AWS	Verbindung stabil, Performance-Tests erfolgreich	Die VPN-Geschwindigkeit könnte durch die Verwendung von leistungsstärkeren Internetanschlüssen verbessert werden.
Kostenbewertung und Betriebseffizienz	Lösung entspricht den geplanten Budgetvorgaben.	Langfristige Betriebskosten könnten durch Optimierungen reduziert werden.

Tabelle 27 Vergleich Soll zu finalem Ist

Wichtige Erkenntnisse:

- Die geplante Architektur wurde vollständig umgesetzt, und die Redundanz sorgt für eine hohe Verfügbarkeit.
- BGP-Routing und Failover wurden erfolgreich getestet, wobei kleinere Optimierungen an den Failover-Zeiten vorgenommen wurden.
- Das Monitoring-System erfüllt alle Anforderungen.
- Die Performance der VPN-Verbindung war stabil, und erfüllte die definierten Anforderungen.
- Kosteneffizienz wurde erreicht, jedoch könnten langfristig Optimierungen in der Konfiguration zusätzliche Einsparungen bringen.

Insgesamt erfüllt die implementierte Lösung alle definierten Anforderungen und gewährleistet eine stabile, hochverfügbare und kosteneffiziente Hybrid-Cloud-Konnektivität.

9.2 Evaluation der Lösung

Die implementierte Lösung zur Hybrid-Cloud-Konnektivität mittels AWS Site-to-Site-VPN bietet eine skalierbare und ausfallsichere Möglichkeit zur Anbindung von On-Premises-Infrastrukturen an die Cloud. In folgendem Abschnitt werden mögliche Einsatzszenarien, Effizienz, Verfügbarkeit und die Kosten analysiert.

1. Einsatzmöglichkeiten

Die erarbeitete Lösung eignet sich besonders gut für Unternehmen und Organisationen mit folgenden Anforderungen:

Hybride IT-Architekturen:

- Unternehmen, die sowohl On-Premises-Rechenzentren als auch AWS-Cloud-Ressourcen verwenden.
- Anwendungen, die in einer hybriden Umgebung betrieben werden müssen und einen zuverlässigen und sicheren Datentransfer zwischen On-Premises und AWS erfordern.

Geschäftskritische Anwendungen mit hoher Verfügbarkeit:

- Services, die redundante und ausfallsichere Netzwerkanbindungen benötigen, um eine unterbrechungsfreie Kommunikation zu gewährleisten.

Sichere und private Cloud-Anbindungen:

- Organisationen mit strengen Sicherheitsanforderungen, die öffentliche Internetverbindungen minimieren möchten.
- IPSec-VPN in Kombination mit BGP-Routing ermöglicht eine sichere und dynamische Verbindung mit grossen und komplexen Netzwerken On-Premises sowohl als auch in der Cloud.
- Unternehmen welche eine zentralisierte Netzwerküberwachung von allen Ressourcen über ein einziges Überwachungssystem umsetzen möchten.

Skalierbare und kosteneffiziente Netzwerklösungen:

- Unternehmen, die hohe Kosten für direkte Cloud-Konnektivitätslösungen (z.B. AWS Direct Connect) vermeiden wollen.
- Firmen mit wechselnden Anforderungen, die eine dynamische Skalierung der Verbindungskapazitäten benötigen.

2. Effizienzbewertung

Die Lösung wird anhand der sechs zentralen Aspekte bewertet:

Kriterium	Bewertung	Begründung
Verfügbarkeit	5/5 Sehr hoch	Durch redundante VPN-Tunnel mit BGP-Failover wird eine hohe Verfügbarkeit gewährleistet. Automatisches Routing mittels BGP sichert den kontinuierlichen Datenfluss.
Skalierbarkeit	4/5 Hoch	Die VPN-Architektur kann mit zusätzlichen Tunneln oder Bandbreitenerweiterung skaliert werden. Allerdings ist die Performance von der Internetanbindung abhängig.
Kosten	4/5 Effizient	Die Lösung bietet eine günstigere Alternative zu AWS Direct Connect. Jedoch könnte die Lösung für kleinere Projekte dennoch zu teuer sein.
Sicherheit	5/5 Sehr hoch	Die angewandten Verschlüsselungstechnologien ermöglichen einen sehr sicheren Datenverkehr über die IPSec-VPN-Tunnel.
Redundanz	4/5 Hoch	Die Redundanz zieht sich durch die gesamte Lösung hindurch. Jedoch müsste man für eine wirklich vollständig hochverfügbare Lösung zwei Server verwenden.
Praktische Anwendbarkeit	4/5 Hoch	Die Anwendbarkeit der Lösung ist hoch, da für die Implementierung lediglich grundlegendes Fachwissen in den Bereichen VPN, AWS und BGP erforderlich ist. Weitere spezifische Kenntnisse können schnell erlernt werden. Zudem wird für die Umsetzung keine spezielle oder kostspielige Hardware benötigt, was die Lösung auch für kleinere Unternehmen oder Projekte mit begrenztem Budget attraktiv macht.

Tabelle 28 Effizienzbewertung

3. Schlussfolgerung

Die Hybrid-Cloud-Konnektivität mit AWS Site-to-Site-VPN und BGP-Routing stellt eine effiziente, hochverfügbare und kostengünstige Alternative zu anderen Cloud-Anbindungen dar. Sie ist besonders für Unternehmen mit hybriden IT-Umgebungen und hohen Sicherheitsanforderungen geeignet.

Allerdings sollte in Szenarien mit sehr hohen Bandbreitenanforderungen oder strikten Latenzvorgaben eine Alternative wie AWS Direct Connect evaluiert werden. Für mittelständische Unternehmen oder Projekte mit flexiblen Anforderungen bleibt diese Lösung jedoch eine sehr gute Wahl.

9.3 Persönliches Fazit

Ich bin mit meiner Leistung während der IPA insgesamt sehr zufrieden. Ich konnte die Aufgabe erfolgreich annehmen und die Anforderungen an die Infrastruktur grösstenteils ohne grössere Schwierigkeiten erfüllen. Während der gesamten Arbeit gelang es mir, einen hohen Fokus aufrechtzuerhalten, was mir ermöglichte, die Aufgaben grösstenteils innerhalb des geplanten Zeitrahmens abzuschliessen.

Unsicherheiten bezüglich der Umsetzung hatte ich nur vereinzelt zu Beginn der Arbeit, konnte diese jedoch spätestens nach der Konzeptphase vollständig ablegen. Dies gab mir die nötige Sicherheit, um die Realisierung mit grossem Vertrauen und Struktur durchzuführen.

Mit dem Endergebnis der IPA bin ich sehr zufrieden. Neben den definierten Systemzielen konnten auch meine persönlichen Vorgehensziele erreicht werden. Die HERMES-Phasen wurden wie geplant abgeschlossen und haben sich als sinnvolles Vorgehensmodell für dieses Projekt erwiesen.

Die gesamte Erarbeitung dieser IPA war definitiv eines der umfangreicheren Projekte während meiner Lehrzeit. Zwar hatte ich in vergangenen Projekten bereits ähnliche technische Aufgaben, jedoch war ich noch nie in einem Projekt so stark in die detaillierte Planung und Konzeption eingebunden. Diese Erfahrung hat mich in vielerlei Hinsicht weitergebracht, sowohl fachlich als auch methodisch.

Während der IPA konnte ich wertvolle Erfahrungen in der detaillierten Planung und Konzeption sammeln. Rückblickend würde ich in einem zukünftigen Projekt noch besser versuchen, den Zeitplan in kleinere Blöcke zu unterteilen, um die Vorgehensweise noch klarer zu Beginn des Projekts definiert zu haben. Auch die Dokumentation der einzelnen Projektschritte könnte noch systematischer erfolgen, um eine noch bessere Nachvollziehbarkeit zu gewährleisten. Diese Erkenntnisse werde ich gezielt nutzen, um meine Herangehensweise bei zukünftigen Projekten weiter zu optimieren und zu verbessern.

Ich konnte während der gesamten IPA sehr selbstständig arbeiten, meine eigenen Lösungsansätze entwickeln und diese erfolgreich umsetzen. Insgesamt sehe ich die IPA als eine wertvolle Erfahrung, die mich optimal auf zukünftige Herausforderungen in der IT-Welt vorbereitet hat.

9.4 Schlussreflexion

Ich sehe die absolvierte Arbeit als grossen Erfolg an. Die im Zeitplan geplanten Soll-Zeiten konnten mehrheitlich eingehalten werden. Teilweise waren gewisse Punkte zu grosszügig oder manchmal auch zu knapp bemessen, dies hat sich aber bis zum Ende der Arbeit gut ausgeglichen.

Die Realisierung hat mir persönlich viel Spass gemacht, und ich konnte mich mit einem nicht ganz alltäglichen AWS-Service auseinandersetzen. Dies hat mir neue Erfahrungen mit Hybrid-Cloud-Umgebungen ermöglicht und mein Verständnis für die Konnektivität zwischen On-Premises-Infrastrukturen und der Cloud vertieft. Besonders spannend waren die Einrichtung der VPN-Tunnel sowie die Analyse der Performance und Hochverfügbarkeit.

Obwohl die Infrastruktur nach Abschluss des IPA-Projektes nicht weiterverwendet wird, hat die Umsetzung wertvolle Erkenntnisse geliefert. Die Tests haben gezeigt, dass eine stabile, sichere und performante Verbindung zwischen den Umgebungen realisierbar ist.

Zusammenfassend war dieses Projekt eine wertvolle Erfahrung, die meine technischen und methodischen Fähigkeiten erweitert hat. Ich konnte eigenständig Lösungen entwickeln, Herausforderungen bewältigen und meine Kenntnisse in der Cloud- und Netzwerktechnik weiter ausbauen. Die Arbeit hat mir erneut gezeigt, dass die Hybrid-Cloud ein spannendes und zukunftsweisendes Feld ist, das ich auch in zukünftigen Projekten weiterverfolgen möchte.

Teil 2:
Projekt Dokumentation



Swisscom (Schweiz) AG
Pablo Wynistorf, GHR-POD-NEX-18
Genfergasse 14
3011 Bern
E-Mail: pablo.wynistorf@swisscom.com

10 Kurzfassung des IPA Berichts

Die folgenden Texte dienen zur schnellen Übersicht über die durchgeführte IPA.

Kurze Ausgangssituation

Die bestehende Infrastruktur umfasst nur wenige Komponenten. Dazu gehört eine On-Premises-Umgebung, die auf einem Server in einer Labumgebung im OMU99 (Swisscom-Standort Ostermundigen) basiert. Diese Umgebung wird durch zwei Swisscom-Router ergänzt, die eine redundante FTTH-Internetverbindung bereitstellen.

Auf der AWS-Seite steht zu Beginn der Arbeit lediglich ein leerer AWS-Account mit den erforderlichen Berechtigungen zur Konfiguration der geplanten Services zur Verfügung.

Umsetzung

In der simulierten On-Premises-Umgebung werden zwei OPNsense-VMs eingerichtet. Zur Sicherstellung der Hochverfügbarkeit werden auf den OPNsense-VMs spezifische Konfigurationen vorgenommen.

Im nächsten Schritt werden zwei direkte Site-to-Site-VPN-Verbindungen zwischen AWS in der Region eu-central-1 (Frankfurt) und den beiden OPNsense-Instanzen aufgebaut. Auf jeder OPNsense-Instanz werden zwei VPN-Tunnel konfiguriert:

- Einer der Tunnel läuft im aktiven Modus ("Active").
- Der zweite dient als Backup, um im Fehlerfall automatisch zu übernehmen.

Auf der AWS-Seite wird eine VPC konfiguriert, dass mit einem AWS Transit Gateway verbunden wird. Der Transit Gateway wird mit den beiden Site-to-Site-VPNs verknüpft. Somit dient er als Verbindungsstück zwischen der VPC und den VPN-Endpoints und dem BGP-Peer.

Im Anschluss wird ein BGP-Peering zwischen On-Premises und AWS implementiert. Nach erfolgreicher Konfiguration ermöglicht dieses Setup ein dynamisches Routing zwischen den Netzwerken.

Nach Abschluss der grundlegenden Netzwerkkonfiguration wird ein Monitoring-System eingerichtet, das die Site-to-Site-VPN-Verbindungen überwacht. Im Falle eines Ausfalls wird mithilfe von AWS Simple Notification Service (SNS) eine Benachrichtigung an verantwortliche Personen gesendet.

Abschliessend wird die gesamte Infrastruktur auf ihre Widerstandsfähigkeit getestet. Dabei werden sowohl Geschwindigkeits- als auch Latenzmessungen durchgeführt und sorgfältig dokumentiert.

Ergebnis

Die implementierte Infrastruktur erfüllt die gesetzten Anforderungen und gewährleistet eine stabile, hochverfügbare und sichere Verbindung zwischen der On-Premises-Umgebung und AWS. Die Site-to-Site-VPNs arbeiten zuverlässig im aktiven/Backup-Modus.

Die durchgeführten Performance-Tests bestätigen eine niedrige Latenz sowie eine hohe Stabilität der Verbindung. Zudem stellt das eingerichtete Monitoring-System sicher, dass Ausfälle frühzeitig erkannt und sofortige Benachrichtigungen versendet werden. Damit ist die Infrastruktur optimal für zukünftige Erweiterungen und Anpassungen vorbereitet. Eine mögliche Weiterentwicklung wäre die Integration eines erweiterten Monitorings zur genaueren Analyse von Verbindungsabbrüchen. Aktuell sind aber keine Weiterentwicklungen vorgesehen. Die Architektur bietet zudem Potenzial für eine spätere Skalierung durch zusätzliche VPN-Endpunkte oder alternative Verbindungsoptionen wie AWS Direct Connect.

11 Einleitung

Die vorliegende individuelle praktische Arbeit wird im Rahmen der praktischen Abschlussprüfung zum Informatiker Plattformentwicklung EFZ von Pablo Wynistorf durchgeführt.

Pablo Wynistorf ist Teil des Event-ICT-Teams MEV innerhalb der Swisscom Broadcast AG, einer Tochtergesellschaft der Swisscom (Schweiz) AG. MEV ist auf die Planung und den Betrieb von temporären Netzwerk-Infrastrukturen für Veranstaltungen spezialisiert und bietet zuverlässige Verbindungen für Events jeder Grösse. Zu den Kunden zählen unter anderem die UEFA mit ihren Finalspielen, das jährliche WEF in Davos sowie das Openair Frauenfeld. Das Team implementiert seine ICT-Lösungen sowohl bei nationalen als auch bei internationalen Events.

Das Team setzt verschiedene Monitoring-Lösungen für seine temporären Infrastrukturen ein. Einige davon laufen in On-Premises-Serverumgebungen, während andere, wie z.B. das Grafana-Monitoring, in einer AWS-Cloud-Umgebung betrieben werden.

Aus dieser hybriden Systemlandschaft entstand die Idee einer Hybrid-Cloud-Connectivity-Lösung. Pablo Wynistorf, der durch seine Teilnahme an den WorldSkills 2024 in Lyon umfassende Kenntnisse in AWS-Cloud-Lösungen erworben hat, verfügt über tiefgehendes Wissen über die vielfältigen Möglichkeiten der Cloud.

Daher wurde die Entscheidung getroffen, eine Projektevaluation durchzuführen, um die technische Machbarkeit und den Nutzen dieser Lösung zu untersuchen. Sollte sich das Konzept als vielversprechend erweisen, könnte in einem nächsten Schritt die Planung einer produktiven Umgebung folgen.

Folgende Punkte gehören zu den Themen, die in der Arbeit behandelt werden:

- Hochverfügbare Site-to-Site-VPN-Verbindung von On-Premises zum AWS-Datacenter eu-central-1 (Frankfurt)
- Konfiguration der OPNsense-Firewalls On-Premises
- Konfiguration der AWS Netzwerk Services (VPC, Transit Gateway, Site-to-Site-VPN)
- Konfiguration BGP-Routing On-Premises und AWS
- Monitoring-System zur Überwachung der Site-to-Site-VPN-Verbindung
- Untersuchung zur Performance und Widerstandsfähigkeit
- Dokumentation der gesamten Konfiguration der involvierten Komponenten.

Die daraus resultierenden Mehrwerte sind vielfältig. Durch die Implementierung einer hochverfügbaren Site-to-Site-VPN-Verbindung zwischen der On-Premises-Infrastruktur und AWS wird eine sichere und performante Hybrid-Cloud-Konnektivität gewährleistet. Dies ermöglicht eine nahtlose Integration der bestehenden Monitoring- und Netzwerk-Lösungen in die Cloud-Umgebung, wodurch die Flexibilität und Skalierbarkeit erheblich verbessert werden.

Ein weiteres zentrales Element ist die Dokumentation der Umsetzung, welche es ermöglicht, die gleiche Lösung später in einem produktiven Umfeld zu reproduzieren und den Betrieb der Infrastruktur durch weitere Personen zu gewährleisten.

12 Initialisierung

In der Initialisierungsphase wird die aktuelle Ist-Situation mit der Soll-Situation verglichen und die Anforderungen an das Projekt werden analysiert. Es wird geklärt, welche Ziele, welche funktionalen sowie nicht-funktionalen Anforderungen erreicht werden sollen. Darüber hinaus werden die Schnittstellen beschrieben und eine passende Variante ausgesucht.

12.1 Ist-Analyse

In den nachfolgenden Abschnitten wird die aktuelle Lage, die Ist-Situation, beschrieben.

12.1.1 On-Premises

Die Lab-Infrastruktur für dieses Projekt ist in einem kleinen Serverrack im OMU99, einem Swisscom-Standort in Ostermundigen, untergebracht. Vor Ort umfasst die Infrastruktur einen Dell PowerEdge R630-Server mit installiertem VMware vSphere ESXi sowie zwei Swisscom-Internet-Routern, die beide als Internet-Anbindung dienen.

Beide Internet-Router wurden bereits mit jeweils einem Kabel mit dem Server verbunden. Auf dem Server existieren zwei virtuelle Switches, die jeweils einen der beiden Internet-Anschlüsse als Uplink konfiguriert haben.

Für die Verbindung zum Server gibt es zudem eine separate Managementverbindung, die den Zugriff per VPN ermöglicht. Da dieser Teil der Infrastruktur bereits vorkonfiguriert war und auch nach der Arbeit bestehen bleibt, wird seine Konfiguration hier nicht näher beschrieben.

12.1.2 AWS-Seite

Auf der AWS-Seite ist aktuell noch keine Infrastruktur. Der für das Projekt verwendete AWS-Account wurde bereits erstellt und die nötigen Rechte wurden vor Projektstart zugewiesen. Die Verfügbarkeit der benötigten Services in der gewünschten Region wurde überprüft und bestätigt.

12.1.3 Netzplan

Anbei ist die aktuell vorhandene Infrastruktur On-Premises dargestellt.



Abbildung 13 Netzplan IST-Situation

12.2 Soll-Analyse

Die Soll-Situation beschreibt die angestrebte Infrastruktur nach der Implementierung der neuen Lösung. Ziel ist es, eine Hybrid-Cloud-Konnektivität zwischen der bestehenden On-Premises-Infrastruktur und AWS mittels eines redundanten IPSec-Site-to-Site-VPNs mit BGP-Routing sicherzustellen. Dies gewährleistet hochverfügbare, ausfallsichere und skalierbare Netzwerkverbindungen zwischen den beiden Umgebungen.

12.2.1 On-Premises

Die On-Premises-Infrastruktur bleibt physisch unverändert, jedoch erfolgen einige Veränderungen auf virtueller Ebene:

- Einrichtung von zwei OPNsense-VMs auf dem bestehenden Dell PowerEdge R630-Server.
- Direkte Verbindung zwischen den beiden OPNsense-Instanzen über ein separates Interlink-Interface, um High Availability (HA) und Failover zu ermöglichen.
- Konfiguration des CARP-Protokolls, sodass immer eine der beiden OPNsense-Instanzen als aktiver Router fungiert.
    - Primäre Instanz mit virtueller Router-Adresse (z. B. 192.168.1.1).
    - Sekundäre Instanz übernimmt im Fehlerfall automatisch.
- Konfiguration der beiden Site-to-Site-Verbindungen mit jeweils zwei Tunneln pro Verbindung und OPNsense-Instanz.
- Dynamisches Routing mittels BGP zur automatischen Anpassung an Netzwerkänderungen bei Failover-Mechanismen.

12.2.2 AWS-Infrastruktur

Auf der AWS-Seite werden folgende Komponenten erstellt:

- Zwei redundante VPN-Verbindungen mit je zwei IPSec-VPN-Tunneln für maximale Ausfallsicherheit.
- AWS VPC in der Region eu-central-1 mit Subnetzen in allen Verfügbarkeitszonen.
- AWS Transit Gateway dient als Verbindungsstück zwischen dem AWS VPN-Endpunkt und AWS VPC Netzwerk und als BGP-Peer-Router auf der AWS Seite.
- AWS Customer Gateway als virtuelle Ressourcen-Definition der On-Premises-OPNsense-Instanzen.
- Implementierung eines Monitoring-Systems mit AWS CloudWatch und AWS Simple Notification Service, um Verbindungsstörungen sofort zu erkennen und Benachrichtigungen zu versenden.
- Tests zur Prüfung der Erreichbarkeit der Infrastruktur mittels ICMP-Pings zwischen Linux-Instanzen auf beiden Seiten.

12.2.3 Netzplan

Der detaillierte Netzwerkplan wird erst in der Konzeptphase erstellt. Nach der Konfiguration der OPNsense-Instanzen sollte die On-Premises-Seite ungefähr wie unten dargestellt aussehen. Die VPN-Tunnel sind in diesem Netzplan nicht sichtbar, daher wurde eine zusätzliche AWS-Zeichnung beigefügt, die den gewünschten Soll-Zustand der VPN-Verbindungen veranschaulicht. Bei erfolgreicher Konfiguration sollte der On-Premises-Testserver die Möglichkeit haben, einen Testserver in der AWS VPC über ICMP-Ping zu erreichen.

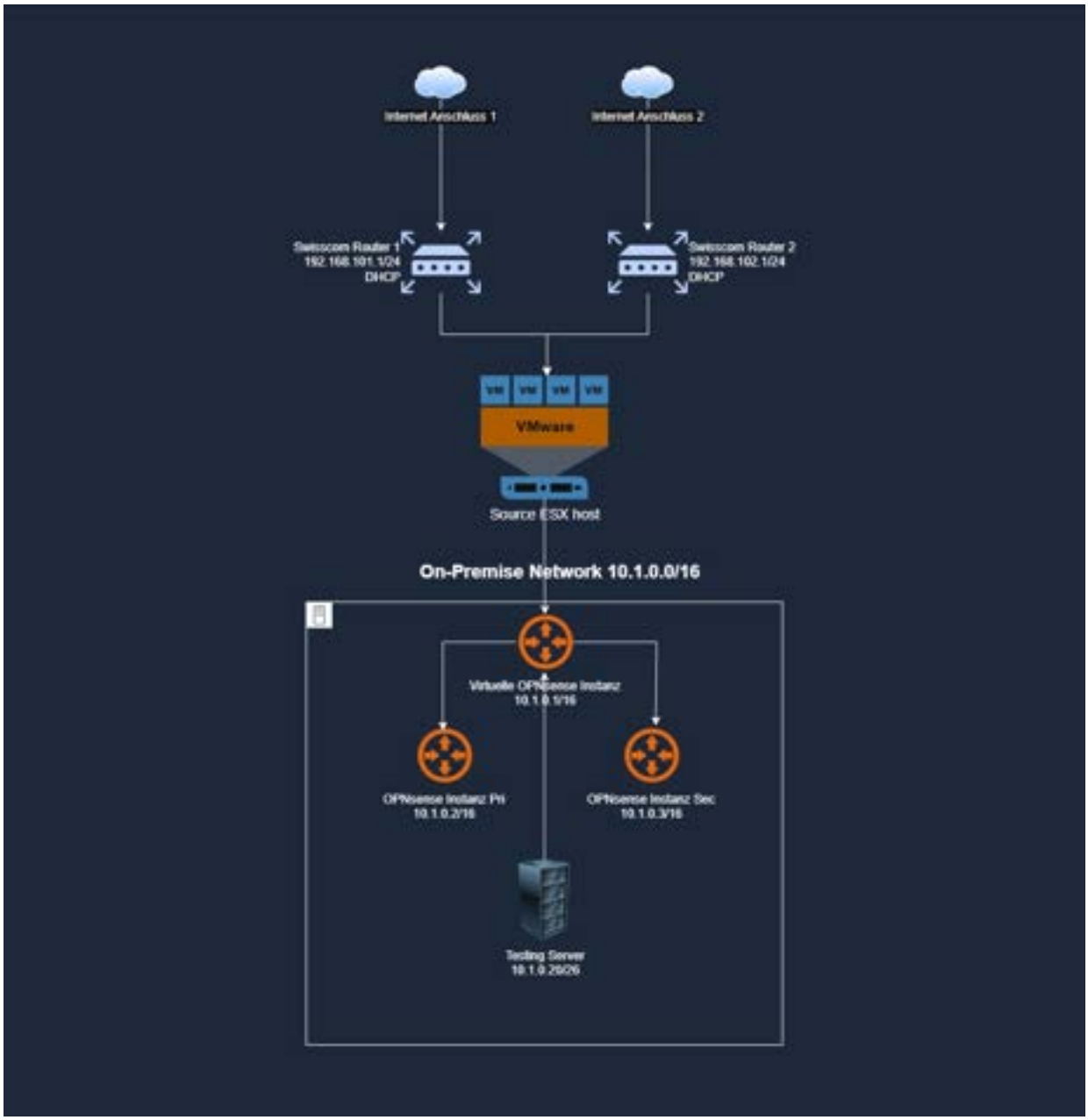
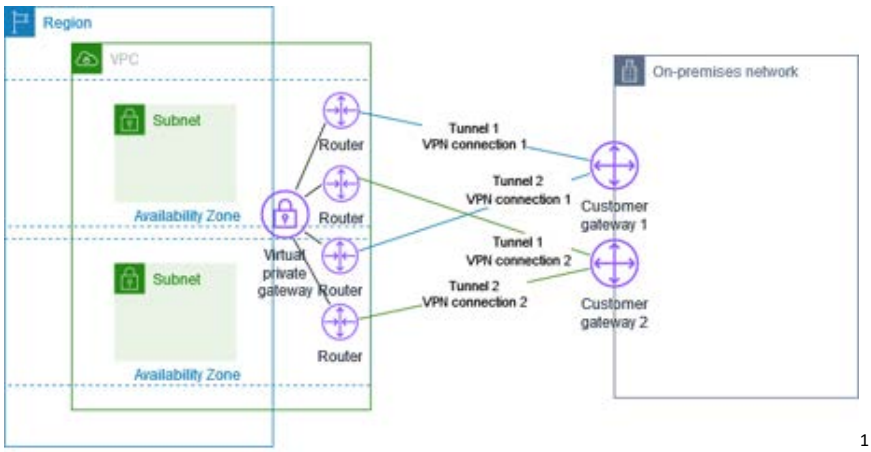


Abbildung 14 Soll-Situation 1

Mit Customer Gateway 1 ist die primäre OPNsense-Instanz gemeint und mit Customer Gateway 2 die sekundäre OPNsense-Instanz.



[1]

Abbildung 15 Soll-Situation 2

12.3 Machbarkeitsanalyse (Proof of Concept)

Dieser Abschnitt beschreibt die Vorgehensweise zur Überprüfung der Machbarkeit der Arbeit.

12.3.1 Technische Realisierbarkeit prüfen

Zur Überprüfung der technischen Realisierbarkeit wurde bereits vor Projektbeginn ein Prototyp der angeforderten Infrastruktur aufgebaut.

Dabei wurden folgende Punkte abgeklärt:

- Erfolgreicher VPN-Verbindungsaufbau
- BGP-Funktionen auf OPNsense-Router
- Hochverfügbarkeitsfunktionen auf OPNsense-Router
- Swisscom Internet Router Connectivity

Aufgrund der erfolgreichen Abklärung der oben genannten Punkte, konnte die Lösung als technisch umsetzbar eingestuft werden. Die endgültige Implementierung muss jedoch sorgfältig konfiguriert und getestet werden.

[1] https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html, Bild kopiert

12.3.2 Mögliche Risiken identifizieren

Risiko	Mögliche Auswirkungen	Gegenmassnahmen
VPN-Störung aufgrund von Problemen mit Swisscom-Routern	Verlust der Konnektivität zu AWS	Redundante VPN-tunnel mit unterschiedlichen Swisscom Routern
Fehlkonfiguration von BGP-Routen	Routing-Probleme & Unerreichbare Netze	Sorgfältige Konfiguration
Hohe Latenz oder Paketverluste	Schlechte Netzwerkperformance	Frühe Performance Tests des Netzwerks
Sicherheitslücken durch falsche Firewall-Regeln	Unautorisierte Zugriffe auf das Netzwerk	Strikte Firewall-Regeln & Principle of least privilege

Tabelle 29 Mögliche Risiken

Durch die Identifikation und Minimierung der Risiken kann sichergestellt werden, dass die Lösung leistungsfähig, sicher und zuverlässig ist.

12.3.3 Alternativen bewerten

Für die Umsetzung der Hybrid-Cloud Connectivity gibt es einige verschiedene Möglichkeiten. Ein paar davon werden in folgender Tabelle analysiert:

Alternative	Vorteile	Nachteile
AWS Direct Connect	• Sehr Stabile & schnelle Verbindung • Professioneller Support	• Hohe Fixkosten • Erfordert langfügigere Planung • Mehr Abhängigkeiten
OpenVPN über EC2	• OpenSource und Flexibel • Kostengünstig	• Schlechtere Performance als IPSec • Nicht geeignet für Hochverfügbarkeit • Kein nativer BGP-Support
Standard IPSec VPN ohne BGP	• Einfache Konfiguration	• Keine automatische Routenanpassungen bei Netzwerkausfällen

Tabelle 30 Alternative Umsetzungsmöglichkeiten

12.4 Projektziele

Folgende Projektziele sollen in der IPA erreicht werden:

12.4.1 Systemziele (SZ)

In der nachfolgenden Tabelle sind die Systemziele ersichtlich:

ID	Systemziel	Beschreibung
SZ1	Installation und Konfiguration der OPNsense-Instanzen	• Bereitstellung und Konfiguration von zwei OPNsense-VMs auf dem bestehenden Server. • Einrichtung des CARP-Protokolls zur automatischen Übernahme durch eine sekundäre Instanz im Fehlerfall. • Anbindung beider OPNsense-Instanzen an einen jeweils dedizierten Internet-Anschluss.
SZ2	Erstellung einer AWS VPC mit erforderlichen Verbindungskomponenten	• Einrichtung einer Virtual Private Cloud (VPC) in AWS mit einem AWS Transit Gateway • Implementierung einer skalierbaren und sicheren Netzwerktopologie zur Unterstützung zukünftiger Erweiterungen.
SZ3	Einrichtung von zwei AWS Site-to-Site-VPN-Verbindungen	• Aufbau und Konfiguration von zwei unabhängigen VPN-Verbindungen mit jeweils zwei Tunneln zur Sicherstellung einer ausfallsicheren Verbindung. • Nutzung von IPSec und BGP für dynamisches Routing und Failover-Mechanismen.
SZ4	Implementierung der BGP-Routing-Unterstützung für dynamisches Routing zwischen AWS und On-Premises	• BGP ASN Konfiguration am AWS Transit Gateway • BGP ASN Konfiguration an beiden OPNsense-Instanzen
SZ5	Einführung eines Monitoring- und Alarmsystems	• Einrichtung von Amazon CloudWatch zur Überwachung der VPN-Verbindungen. • Konfiguration von Amazon SNS für automatische Benachrichtigungen bei Ausfällen.
SZ6	Durchführung eines Connectivity-Tests	• Validierung der Verbindung zwischen On-Premises-Servern und AWS durch ICMP-Ping-Tests. • Sicherstellung der automatischen Routenanpassung bei Tunnel- oder Router-Ausfällen.
SZ7	Dokumentation und Evaluierung der Lösung	• Erstellung einer detaillierten Installations- und Konfigurationsanleitung. • Bewertung der Performance, Skalierbarkeit und Betriebskosten der implementierten Lösung.

Tabelle 31 Systemziele

12.4.2 Persönliche Vorgehensweise (VZ)

In der nachfolgenden Tabelle sind die persönlichen Vorgehensziele ersichtlich:

ID	Vorgehensziel	Beschreibung
VZ1	Initialisierung	Die Initialisierungsphase muss am Mittag von Tag 3 fertig sein.
VZ2	Konzept	Die Konzeptphase muss am Abend von Tag 4 fertig sein.
VZ3	Realisierung	Die Realisierungsphase muss am Abend von Tag 8 fertig sein.
VZ4	Einführung	Die Einführungsphase muss am Nachmittag von Tag 9 fertig sein.
VZ5	Abschluss	Das Projekt muss spätestens bis 18:00 Uhr am Tag 10 fertig sein.

Tabelle 32 Persönliche Vorgehensweise

12.5 Anforderungen

Anbei werden die Anforderungen definiert, die für das Erreichen der Projektziele notwendig sind.

12.5.1 Funktionale Anforderungen (FA)

Folgende Anforderungen werden an die Infrastruktur gestellt.

ID	Anforderung
FA1	Beide OPNsense-Instanzen wurden korrekt installiert und konfiguriert.
FA2	Die Infrastruktur auf der AWS Seite wurde korrekt und nach besten Standards geplant und aufgebaut.
FA3	Die VPN-Verbindung zwischen On-Premises und AWS kann erfolgreich aufgebaut werden.
FA4	Die korrekte BGP-Konfiguration ermöglicht das Routing der verschiedenen Netzen zwischen On-Premises und AWS.
FA5	Das Monitoring-System liefert korrekte Daten und kann bei Ausfällen Mitteilungen an bestimmte Personen senden.
FA6	Die Connectivity-, Failover- und Performancetests liefern Werte innerhalb der definierten Schwellwerten.

Tabelle 33 Funktionale Anforderungen

12.5.2 Nicht funktionale Anforderungen (NFA)

ID	Anforderung
NFA1	Ausführliche Dokumentation für die Installation der Infrastruktur erstellen
NFA2	Evaluation und Einschätzung der vollendeten Lösung

Tabelle 34 Nicht funktionale Anforderungen

12.6 Abgrenzungen

Um die Aufgaben der IPA klarer zu machen, hilft es zu wissen, was bewusst kein Teil der IPA ist und somit abgegrenzt wird.
Folgende Punkte werden während der IPA **nicht** durchgeführt:

- Langfristiger Betrieb und Wartung der vollendeten Lösung
  - Die Infrastruktur wird nach der Demo am Präsentationstag wieder abgebaut.
- Konfiguration von Tiefgehenden IT-Systemen wie z.B. Intrusion Detection Systems
  - Die Implementation von fortgeschrittenen oder tiefgründigeren IT-Systemen ist nicht Teil dieser IPA.
- Implementation eines Monitoring-Systems der On-Premises Infrastruktur
  - Die On-Premises Infrastruktur wird während der IPA nicht mit einem Monitoring-System versehen.
- Langfristige Optimierung des Netzwerks
  - Das Netzwerk wird während der IPA nicht langfristig optimiert.

12.7 Informationsrecherche und Grundlagen

Der Folgende Abschnitt beschreibt die benötige Informationsrecherche, welche für eine erfolgreiche Umsetzung des Projekts notwendig ist.

12.7.1 Genutzte Dokumentationen und Quellen

Eine Detaillierte und exakte Auflistung aller in dieser Arbeit verwendeten Quellen, befindet sich im Literatur und Quellenverzeichnis am Ende dieses Dokuments. Jedoch werden in nachfolgender Tabelle einige Fachspezifische Quellen für die Umsetzung aufgeführt:

Titel / verwendet für	Quelle
AWS Dokumentationen	https://docs.aws.amazon.com/ Auf dieser Website wurden alle Fachspezifischen Informationen für die Umsetzung der AWS Infrastruktur hergeholt.
OPNsense-Dokumentation	https://docs.opnsense.org/ Auf dieser Website wurden alle fachspezifischen Informationen für die Umsetzung für die Konfiguration der OPNsense-Router hergeholt.
VPN Setup	https://medium.com/@swordfish291/opnsense-firewall-site-to-site-vpn-configuration-to-aws-vpc-6d12c2456ea Diese Webseite wurde zur Konfiguration der Site-to-Site-VPN verwendet.
ChatGPT	https://chatgpt.com/ ChatGPT wurde verwendet, um einige Verständlichkeitsfragen zu beantworten.
OPNsense High Availability Setup	https://www.youtube.com/watch?v=I5n3QXOlxmw Dieses Youtube Video wurde verwendet, um Hochverfügbarkeit für OPNsense zu konfigurieren.

Tabelle 35 Quellen für die Umsetzung

12.7.2 Erfahrungswerte aus Vorherigen Projekten

Da ich seit Beginn meiner Ausbildung mit Netzwerken zu tun habe und mich sehr dafür interessiere, konnte ich in diesem Bereich viel Erfahrung sammeln und verfüge über ein grosses Fachwissen in Bezug auf On-Premises- und Cloud-Networking.

Die Teilnahme an den WorldSkills 2024 in Lyon hat mir dabei geholfen, mein AWS-Wissen zu vertiefen und mehr über die Funktionalitäten von Cloud-Systemen und Netzwerken zu lernen. In den Vorbereitungen auf die WorldSkills habe ich mich über einen längeren Zeitraum intensiv mit VPN-Networking auseinandergesetzt und dabei tiefgehende Kenntnisse in der Konfiguration und Optimierung sicherer Verbindungen erworben.

13 Konzept

In der Konzeptphase werden alle relevanten technischen und organisatorischen Aspekte definiert, die für die erfolgreiche Umsetzung des Projekts erforderlich sind. Dies umfasst die Definition der Anforderungen, Architektur, Netzwerkdesign, Monitoring-Konzept und Testkonzept.

13.1 Technische Anforderungen

In diesem Abschnitt werden alle technischen Rahmenbedingungen definiert, die für die erfolgreiche Implementierung der Hybrid-Cloud-Konnektivität mit AWS Site-to-Site-VPN und BGP-Routing erforderlich sind. Die Anforderungen stellen sicher, dass das Netzwerk leistungsfähig, ausfallsicher und sicher betrieben werden kann.

13.1.1 Bandbreite

Anforderungen an die Netzwerkgeschwindigkeit und die Netzwerkperformance:

- **Netzwerkgeschwindigkeit**:
  - Die redundanten Internetanschlüsse auf der On-Premises Seite haben beide eine Geschwindigkeit von je ca. 600 Mbit/s
  - AWS Site-to-Site VPN unterstützt pro Tunnel maximal 1.25 Gbit/s
  - Konkrete Geschwindigkeitsanforderungen an die VPN-Verbindung wurden nicht definiert. Als Richtwert gilt eine stabile Verbindung mit 100 Mbit/s.
- **Netzwerkperformance**:
  - Exakte Latenzzeitanforderungen wurden nicht gestellt. Als Richtwert wird eine tiefe zweistellige Latzenzzeit gesetzt (z.B. 25ms).
  - Die Latzenzzeit kommt sehr auf die zu zurücklegende Distanz an. In diesem Projekt beträgt die Distanz zwischen den physikalischen Standorten ca. 420 Km.

13.1.2 Standorte

Die physikalischen Standorte sind:

- **On-Premises (Lab in Ostermundigen):**
  - Standort: Swisscom OMU99, Ostermundigen
  - Physische Infrastruktur:
    - Dell PowerEdge R630 Server mit VMs
    - Swisscom Internet Router
- **AWS Seite (eu-central-1):**
  - Standort: Region eu-central-1 in Frankfurt am Main
  - Verwendete Services:
    - AWS VPC
    - AWS Transit Gateway
    - AWS Site-to-Site VPN
    - AWS Simple Notification Service (SNS)
    - AWS CloudWatch
  - Availability Zones:
    - eu-central-1a
    - eu-central-1b
    - eu-central-1c

13.1.3 Verfügbarkeit

Das Ziel ist die Einrichtung einer hochverfügbaren Verbindung zwischen der On-Premises-Infrastruktur und AWS, sodass Netzwerkunterbrechungen durch automatische Failover-Mechanismen minimiert werden.

Folgende Anforderungen werden für die Verfügbarkeit gestellt:

- **Angepeilte Verfügbarkeit:**
  - Alle innerhalb dieser IPA konfigurierten Kernkomponenten sollen insgesamt eine Verfügbarkeit von 99,9% aufweisen.
  - Dies entspricht einer maximalen Ausfallzeit von ca. 8h 45min pro Jahr.

- **Nicht bewertete Verfügbarkeiten:**
  - ISP Verfügbarkeit (Grund: kein professioneller Anschluss, daher kein SLA mit Swisscom)
  - Swisscom Internet Router Verfügbarkeit (Grund: keine hochverfügbaren Geräte)
  - Server Verfügbarkeit (Grund: nicht redundantes System)
  - Stromverfügbarkeit On-Premises (Grund: kein SLA mit Stromanbieter)

Die Infrastruktur gilt als verfügbar, wenn die VPN-Verbindung aktiv ist, und Daten übertragen werden können.

13.1.4 Protokolle

Es werden in dieser Arbeit viele verschiedene Protokolle in unterschiedlichen Kontexten verwendet. Alle verwendeten Protokolle mit deren Funktion werden hier beschrieben:

- **VPN-Protokolle:**
  - IPSec (IKEv2) für eine sichere, verschlüsselte VPN-Verbindung

- **Routing-Protokolle:**
  - BGP (Border Gateway Protocol) für dynamisches Routing
  - AS-Nummern & Peer-Gruppen für redundantes Routing-Setup

- **Hochverfügbarkeits-Protokolle:**
  - CARP (Common Address Redundancy Protocol) für OPNsense-Hochverfügbarkeits-Setup

- **Generelle Protokolle:**
  - TCP (Transmission Control Protocol) für generelle Datenübertragung
  - UDP (User Diagram Protocol) für schnelle Datenübertragung

13.1.5 Sicherheit

Um die Sicherheit der Infrastruktur sicherzustellen, werden folgende Anforderungen gestellt:

- **Firewall-Regeln:**
  - Nur explizit erlaubter Traffic zwischen On-Premises und AWS
  - Principal of least privilege

- **IPSec-Abscherung:**
  - Starke AES-Verschlüsselung

13.2 Gesamte Architektur

Im nachfolgenden Abschnitt wird das exakte Infrastrukturkonzept zuerst zeichnerisch dargestellt und danach beschrieben.

13.2.1 Netzwerkdiagramm

Das folgende Diagramm stellt die gesamte IT-Infrastruktur dar, die für die Hybrid-Cloud-Konnektivität zwischen On-Premises und AWS aufgebaut wird. Es zeigt die einzelnen Komponenten und deren Verbindungen, darunter VPN-Tunnel, Firewall-Instanzen, Internet-Router, Host-Server, Test-Server und die AWS-Netzwerkintegration.

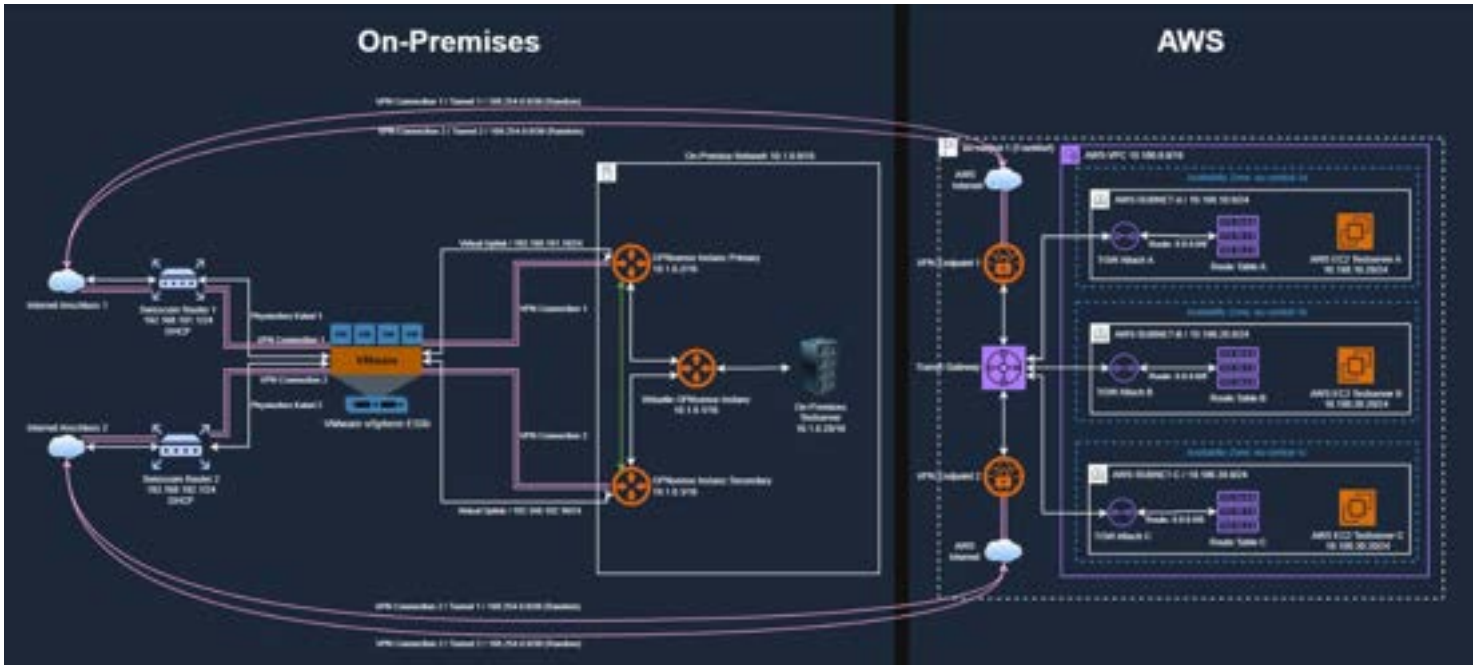


Abbildung 16 Gesamtes Netzwerkdiagramm

13.2.2 Definition und Zielsetzung der Architektur

Das Netzwerk besteht aus zwei Hauptkomponenten.

- **On-Premises Infrastruktur** (links)
  - Physische & virtuelle Netzwerkgeräte in der Lab-Umgebung im OMU99 (Ostermundigen).
  - Zwei unabhängige Internetanschlüsse für Redundanz.
  - Virtualisierte OPNsense-Firewall-Instanzen.
  - Testserver für Connectivity-Tests.
- **AWS-Cloud-Infrastruktur** (rechts)
  - Zwei AWS Site-to-Site-VPN-Endpoints.
  - AWS Transit Gateway mit insgesamt fünf Attachments (3x AWS Subnetze, 2x AWS Site-to-Site VPN Endpoints).
  - VPC mit mehreren Subnetzen & Routing-Tabellen für die Kommunikation.
  - Testserver für Connectivity-Tests.

Das Ziel dieser Architektur ist die hochverfügbare, sichere und skalierbare Anbindung zwischen den beiden Netzwerken über redundante VPN-Tunnel mit BGP-Routing.

13.2.3 Netzwerksegmente

Dieser Abschnitt beschreibt die verschiedenen Netzwerke und wo sie eingesetzt werden.

Name	CIDR Ranges	Beschreibung
On-Premises Internet 1	192.168.101.0/24	DHCP Netzwerk hinter Swisscom Internet Router 1
On-Premises Internet 2	192.168.102.0/24	DHCP Netzwerk hinter Swisscom Internet Router 2
On-Premises Client Netzwerk OPNsense	10.1.0.0/16	Dieses Netzwerk wird das Client Netzwerk der On-Premises Infrastruktur
On-Premises Sync Netzwerk OPNsense	172.16.1.0/30	Dieses Netzwerk besteht nur direkt zwischen der OPNsense Primary und OPNsense-Secondary-Instanz und dient zur Synchronisation und Hochverfügbarkeit.
VPN Tunnel Netzwerke (4x)	169.254.0.0/30 (Random)	Diese Netzwerke sind Transportnetzwerke innerhalb des VPN Tunnels. Die exakte CIDR Range wird von AWS bestimmt und wird erst in der Realisierungsphase festgelegt.
VPC Netzwerk	10.100.0.0/16	Dieses Netzwerk ist die Range für die verschiedenen Subnetze auf AWS.
AWS Subnetz A	10.100.10.0/24	Dieses Netzwerk ist ein Segment aus der VPC Netzwerk CIDR und ist quasi das Client Netzwerk auf der AWS Seite in der Availability Zone A
AWS Subnetz B	10.100.20.0/24	Dieses Netzwerk ist ein Segment aus der VPC Netzwerk CIDR und ist quasi das Client Netzwerk auf der AWS Seite in der Availability Zone B
AWS Subnetz C	10.100.30.0/24	Dieses Netzwerk ist ein Segment aus der VPC Netzwerk CIDR und ist quasi das Client Netzwerk auf der AWS Seite in der Availability Zone C

Tabelle 36 Netzwerksegmente

13.3 On-Premises-Architektur

Dieser Abschnitt beschreibt alle relevanten Komponenten und die IP-Adressierung der On-Premises-Umgebung.

13.3.1 Komponenten

Komponente	Typ	Funktion	IP-Adresse(n)	Schnittstellen / Ports	Hochverfügbarkeit
Swisscom Internet Anschluss 1	Internet Anschluss	Primäre Internetverbindung	-	-	Keine HA
Swisscom Internet Anschluss 2	Internet Anschluss	Primäre Internetverbindung	-	-	Keine HA
Swisscom Internet Router 1	Internet Router	Primärer Internet-Router	**WAN:** 188.63.183.175 **UPLINK LAN:** 192.168.101.1/24	WAN / LAN	Keine HA
Swisscom Internet Router 2	Internet Router	Sekundärer Internet-Router	**WAN**: 178.195.125.21 **UPLINK LAN:** 192.168.102.1/24	WAN / LAN	Keine HA
Dell PowerEdge R630 Server	Host Server	Host Server	**MGMT LAN:** DHCP	LAN	Keine HA
VMware vSphere ESXi	Host Betriebs-system	Betriebssystem	**MGMT LAN:** 10.1.10.100/24	LAN	Keine HA
OPNsense Instanz (Primary)	Firewall / Router	Firewall / Router / VPN Gateway	**UPLINK LAN:** 192.168.101.10/24 **LAN:** 10.1.0.2/16 **SYNC LAN:** 172.16.1.1/30	WAN / LAN	Keine HA
OPNsense Instanz (Secondary)	Firewall / Router	Firewall / Router / VPN Gateway	**UPLINK LAN:** 192.168.102.10/24 **LAN:** 10.1.0.3/16 **SYNC LAN:** 172.16.1.2/30	WAN / LAN	Keine HA

OPNsense Instanz (Virtuell)	Firewall / Router	Firewall / Router	**UPLINK LAN:** 192.168.101.1, 192.168.102.1 **LAN:** 10.1.0.1/16	WAN / LAN	HA Konfiguriert
On-Premises Test Server	Linux Server	Testserver	**LAN:** 10.1.0.20/16	LAN	Keine HA

Tabelle 37 On-Premises Netzwerksegmente

13.3.2 OPNsense-Instanzen

Die OPNsense-Instanzen bilden zusammen den zentralen Baustein der On-Premises Infrastruktur. Sie haben folgende Funktionalitäten:

- Internet Gateway
- Firewall
- On-Premises Client Netzwerk Router
- IPSec-VPN-Funktionalitäten
- BGP-Routing-Funktionalitäten

Die On-Premises Infrastruktur umfasst zwei OPNsense-Instanzen betrieben in Form einer virtuellen Maschine auf dem VMWare vSphere ESXi-Host.

Wichtige Merkmale der Infrastruktur:

- Zwei Instanzen für Hochverfügbarkeit
- CARP (Common Address Redundancy Protocol) für Failover & Redundanz
- IPSec Site-to-Site-VPN-Verbindung mit AWS
- BGP-Routing für dynamisches Routing zu AWS
- Firewall-Regeln zur Kontrolle des Datenverkehrs

Um die OPNsense-Instanzen hochverfügbar zu machen, werden zwei Funktionalitäten von OPNsense in Anspruch genommen. Einerseits wäre da das Feature «HA» mit der die Primary-Instanz über ein dediziertes Sync-Interface den aktuellen Status und die Konfigurationen mit der Secondary-Instanz synchronisieren kann. Über das gleiche Interface wird auch das andere Protokoll/Feature «CARP» (Common Address Redundacy Protocol) konfiguriert, welches sicherstellt, dass immer eine der beiden OPNsense-Instanzen den Default Gateway mit einer virtuellen IP erreichbar macht. Im Normalzustand ist die Primary-Instanz dafür verantwortlich, dass die Default-Gateway-Adresse (10.1.0.1/16) im Netzwerk erreichbar ist. Sollte nun aber die Primary-Instanz ein Problem haben, wird das von der Secondary-Instanz erkannt und diese sorgt dann dafür, dass die Default Gateway Adresse (10.1.0.1/16) im Netzwerk wieder erreichbar ist.

Konfiguration der OPNsense-IP-Adressen:

IP-Typ	Primäre OPNSense (Master)	Sekundäre OPNSense (Backup)	Virtuelle CARP-IP
WAN IP (DHCP von ISP)	Dynamisch	Dynamisch	Keine CARP-IP
LAN Interface	10.1.0.2/16	10.1.0.3/16	10.1.0.1/16 (CARP)
Sync Interface	172.16.1.1/30	172.16.1.2/30	Keine CARP-IP

Tabelle 38 On-Premises OPNsense IP-Adressen

- Das CARP-Protokoll sorgt dafür, dass die virtuelle IP (10.1.0.1) immer von der aktiven Instanz übernommen wird.
- Die sekundäre Instanz synchronisiert den Status mit der primären Instanz über das Sync-Interface (172.16.1.0/30).

Die OPNsense-Instanzen werden auf dem Server als virtuelle Maschinen betrieben. Aus diesem Grund wird in nachfolgender Tabelle die Ressourcenzuweisung aufgeführt:

Instanz	CPU Cores	RAM (GB)	Speicher (GB)	Netzwerkadapter (Virtual Switch)
OPNsense-Primary	6	20	40	FTTH_INTERNET_SW_01, ON-PREM_NET, OPNsense_SYNC_NET
OPNsense-Secondary	6	20	40	FTTH_INTERNET_SW_02, ON-PREM_NET, OPNsense_SYNC_NET

Tabelle 39 On-Premises OPNsense Ressourcenzuweisung

Als Software verwenden die OPNsense-Instanzen die Version: 25.1 «Ultimate Unicorn» Series. Die Instanzen werden mit einem ISO-File installiert.

Folgendes Plugin werden die OPNsense-Instanzen installieren müssen:

- **OS-FRR** (The FRRouting Protocol Suite)

13.4 AWS Architektur

Dieser Abschnitt beschreibt alle relevanten Komponenten und die IP-Adressierung der AWS Umgebung.

13.4.1 Komponenten

Komponente	Typ	Funktion	IP-Adresse(n) / IP-Ranges	Hochverfügbarkeit
AWS VPN Endpoint 1	VPN	Terminierung VPN-Verbindung 1 (Tunnel 1 + 2)	WAN Tunnel 1: WAN Tunnel 2:	HA Konfiguriert
AWS VPN Endpoint 2	VPN	Terminierung VPN-Verbindung 2 (Tunnel 1 + 2)	WAN Tunnel 1: WAN Tunnel 2:	HA Konfiguriert
AWS Transit Gateway	Gateway	Verbindungsstück VPN-Endpoint mit VPC, BGP Router	-	HA Konfiguriert
AWS Transit Gateway Attachment 1 **(VPN Endpoint 1)**	Gateway Attachment	Verbindungsstück VPN-Endpoint 1 mit Transit Gateway	-	HA Konfiguriert
AWS Customer Gateway 1	Ressourcen Definition	Virtuelle Definition des AWS Site-to-Site-VPN Gegenstücks auf der On-Premises-Seite.	WAN: 188.63.183.175	Keine HA
AWS Customer Gateway 2	Ressourcen Definition	Virtuelle Definition des AWS Site-to-Site-VPN Gegenstücks auf der On-Premises-Seite.	WAN: 178.195.125.21	Keine HA
AWS Transit Gateway Attachment 2 **(VPN Endpoint 2)**	Gateway Attachment	Verbindungsstück VPN-Endpoint 2 mit Transit Gateway	-	HA Konfiguriert
AWS Transit Gateway Attachment 3 **(Subnetz A)**	Gateway Attachment	Verbindungsstück Subnetz A mit Transit Gateway	**LAN:** DHCP **Range:** 10.100.10.X/24	HA Konfiguriert
AWS Transit Gateway Attachment 4 **(Subnetz B)**	Gateway Attachment	Verbindungsstück Subnetz B mit Transit Gateway	**LAN:** DHCP **Range:** 10.100.20.X/24	HA Konfiguriert

AWS Transit Gateway Attachment 5 **(Subnetz C)**	Gateway Attachment	Verbindungsstück Subnetz C mit Transit Gateway	**LAN:** DHCP **Range:** 10.100.30.X/24	HA Konfiguriert
AWS VPC	Netzwerk	Virtual Private Cloud Netzwerk	**LAN:** 10.100.0.0/16	HA Konfiguriert
AWS Subnetz A	Subnetz	Virtual Private Cloud Subnetz	**LAN:** 10.100.10.0/24	Keine HA (HA innerhalb der Availability Zone)
AWS Subnetz B	Subnetz	Virtual Private Cloud Subnetz	**LAN:** 10.100.20.0/24	Keine HA (HA innerhalb der Availability Zone)
AWS Subnetz C	Subnetz	Virtual Private Cloud Subnetz	**LAN:** 10.100.30.0/24	Keine HA (HA innerhalb der Availability Zone)
AWS Route Table A	Route Table	Virtual Private Cloud Route Table	-	Keine HA (HA innerhalb der Availability Zone)
AWS Route Table B	Route Table	Virtual Private Cloud Route Table	-	Keine HA (HA innerhalb der Availability Zone)
AWS Route Table C	Route Table	Virtual Private Cloud Route Table	-	Keine HA (HA innerhalb der Availability Zone)
AWS EC2 Test Server A	Linux Server	Testing Server A	**LAN:** 10.100.10.20/24	Keine HA
AWS EC2 Test Server B	Linux Server	Testing Server B	**LAN:** 10.100.20.20/24	Keine HA
AWS Test Server C	Linux Server	Testing Server C	**LAN:** 10.100.30.20/24	Keine HA
AWS CloudWatch Alarms	Monitoring	Monitoring der VPN Tunnel	-	HA Konfiguriert
AWS SNS	Nachrichten-dienst	Senden der Alarme von CloudWatch Alarms	-	HA Konfiguriert

Tabelle 40 AWS-Architektur Komponenten

13.4.2 AWS Infrastruktur

Die AWS Infrastruktur besteht aus mehr zu konfigurierenden Komponenten als die On-Premises-Umgebung. Das Projekt wird auf der AWS-Seite ohne Vorkonfiguration und in einem neuen AWS-Account umgesetzt. Die gesamte Infrastruktur wird in der AWS Region eu-central-1 aufgebaut. Diese Region befindet sich in Frankfurt am Main in Deutschland. Ungefähr 420 Kilometer von der On-Premises Infrastruktur entfernt.

Wichtige Auswahlkriterien für die Region:

- Alle in der Aufgabenstellung geforderten AWS-Services sind verfügbar.
- Geringe Latenz (~15–30 ms) zur On-Premises-Umgebung.
- Hohe Verfügbarkeit durch mehrere Availability Zones (AZs)

Folgende AWS Services kommen in diesem Projekt zum Einsatz:

- **AWS VPC (Virtual Private Cloud)** → Ermöglicht es, komplexe virtuelle Netzwerke in der Cloud zu betreiben.
- **AWS Site-to-Site VPN** → Stellt zwei redundante VPN-Verbindungen zu On-Premises bereit.
- **AWS Transit Gateway** → Wird als zentrale Routing-Schnittstelle zwischen VPN und VPC genutzt.
- **AWS CloudWatch** → Monitoring Service von AWS, welcher es ermöglicht, die VPN Tunnels zu überwachen.
- **AWS SNS (Simple Notification Service)** → Versendet Alarme an verantwortliche Personen, wenn z. B. ein VPN-Tunnel ausfällt.
- **AWS EC2 (Elastic Compute Cloud)** → Auf diesem AWS Service werden die Linux Testserver laufen gelassen.

In der Komponentenliste der AWS-Architektur kann man sehen, welche Komponenten hochverfügbar sein werden. Im Vergleich zu On-Premises muss man bei vielen Services nicht mehr viel konfigurieren, um sie hochverfügbar betreiben zu können, da AWS dies oftmals standardmässig anbietet.

AWS VPCs erstrecken sich über eine gesamte Region und somit auch über alle in dieser Region verfügbaren Availability Zones. Die Region eu-central-1 (Frankfurt) hat drei Availability Zones:

- **eu-central-1a**
- **eu-central-1b**
- **eu-central-1c**

In jeder dieser Availability Zones wird ein Subnetz des VPCs platziert. In jedem Subnetz gibt es ein Routing-Table und ein Attachment des AWS Transit Gateway. Dieser ermöglicht, dass sogar bei einem Ausfall von zwei ganzen Availability Zones immer noch Connectivity zu mindestens einem Testserver besteht. Dies funktioniert nur, da jedes Subnetz in jeder Availability Zone ein AWS Transit Gateway Attachment (Quasi ein Gateway Interface) vom AWS Transit Gateway verbunden hat. Dazu kommt, dass die Route-Tables der einzelnen Subnetze den gesamten Traffic mit der Null-Route (0.0.0.0/0) zum AWS Transit Gateway schicken. Der AWS Transit Gateway routet dann den Traffic automatisch mit BGP über die verfügbaren VPN-Verbindungen zur On-Premises-Umgebung. Diese Null-Route sorgt auch dafür, dass alle AWS EC2 Testserver Internet-Connectivity über die On-Premises-Umgebung erhalten.

13.5 VPN-Konzept

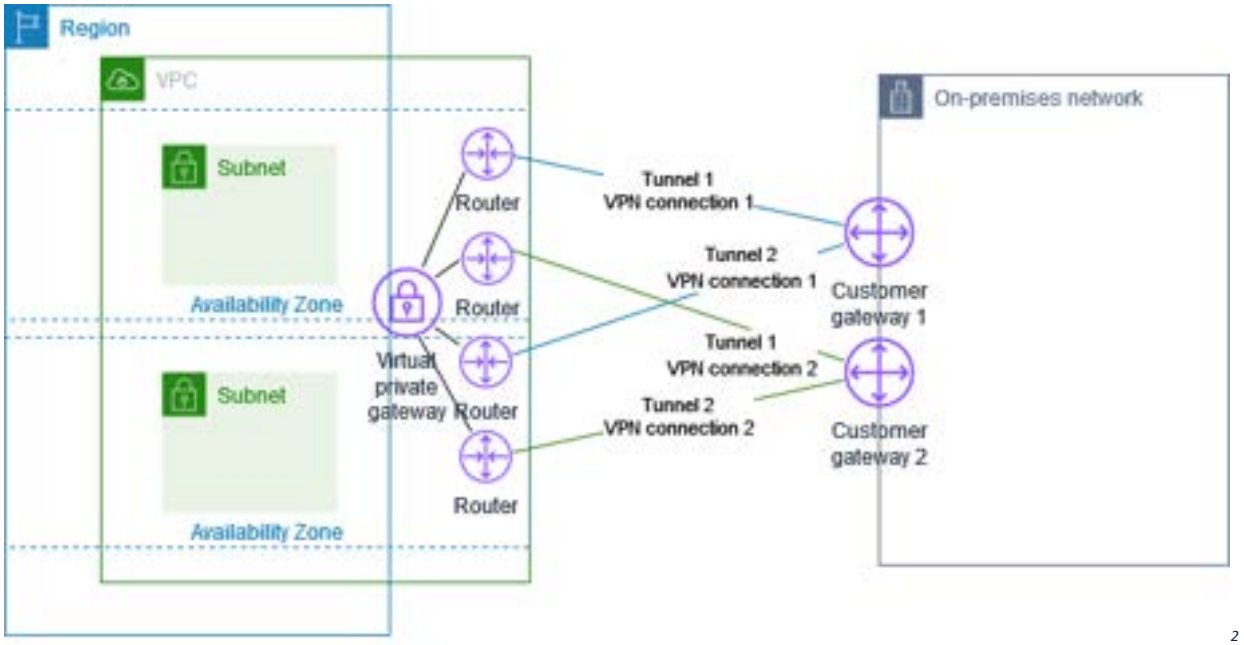
Das nachfolgende Kapitel definiert die Funktionalitäten und Architektur der VPN-Verbindungen.

13.5.1 Architekturübersicht

Das VPN-Konzept basiert auf einer Site-to-Site-VPN-Verbindung zwischen der On-Premises-Umgebung und AWS. Folgende Kernkomponenten bilden die Architektur:

- **On-Premises:**
  - Zwei OPNsense-Firewalls für VPN und Routing
  - Redundante Internetanbindungen
- **AWS:**
  - Ein AWS Transit Gateway als zentrale Routing-Schnittstelle
  - Zwei AWS Site-to-Site VPN-Verbindungen
  - Vier AWS Site-to-Site VPN-Tunnels
  - Fünf AWS Transit Gateway Attachments als Verbindungstücke der AWS Site-to-Site VPN Endpoints mit den VPC Subnetzen.

Folgende Zeichnung ist eine offizielle Zeichnung aus der AWS-Dokumentation, welche die geplante Konfiguration dieser IPA vereinfacht darstellt. Die genauen projektbezogenen VPN-Verbindungen sind auf dem Netzwerkdiagramm im Kapitel «Gesamte Architektur» dargestellt.



[2]

Abbildung 17 VPN-Verbindungs-Architektur

[2] https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html

13.5.2 VPN-Topologie

Die Verbindung zu AWS besteht aus zwei unabhängigen AWS Site-to-Site VPN-Verbindungen mit jeweils zwei parallelen IPSec-Tunneln für Hochverfügbarkeit:

Tunnel	Endpunkt On-Premises	Endpunkt AWS
VPN Verbindung 1, Tunnel 1	OPNsense Instanz Primary	AWS VPN Endpoint 1 Tunnel 1
VPN Verbindung 1, Tunnel 2	OPNsense Instanz Primary	AWS VPN Endpoint 1 Tunnel 2
VPN Verbindung 2, Tunnel 1	OPNsense Instanz Secondary	AWS VPN Endpoint 2 Tunnel 1
VPN Verbindung 2, Tunnel 2	OPNsense Instanz Secondary	AWS VPN Endpoint 2 Tunnel 2

Tabelle 41 VPN-Tunnel-Topologie

Jede OPNsense-Instanz baut ihre eigene IPSec-VPN-Verbindung zu AWS auf. Diese Architektur bietet folgende Vorteile:

- **Redundanz:** Falls ein Tunnel ausfällt, übernimmt der zweite automatisch den Traffic
- **Ausfallsicherheit:** Wenn eine OPNsense-Instanz ein Problem hat, übernimmt die andere Instanz den gesamten VPN-Datenverkehr.

Die VPN-Verbindungen nutzen UDP Port 500 für den Schlüsselaustausch mit dem anderen VPN-Endpunkt und anschliessend UDP Port 4500 für den IPsec-VPN-Datenverkehr. Diese Ports müssen auch On-Premises auf den Swisscom-Internet-Routern als Portweiterleitung zu den OPNsense-Instanzen eingetragen werden.

13.6 BGP-Konzept

Das nachfolgende Kapitel definiert die Funktionalitäten und Architektur des BGP-Routings innerhalb der Hybrid-Cloud-Umgebung. BGP (Border Gateway Protocol) wird verwendet, um dynamisches Routing zwischen der On-Premises-Infrastruktur und AWS durch die VPN-Verbindungen zu ermöglichen.

13.6.1 Architekturübersicht

Das BGP-Routingkonzept basiert auf einer dynamischen Routingstrategie zwischen der On-Premises-Umgebung und AWS, um automatisches Failover, Lastverteilung und effiziente Routensteuerung zu gewährleisten.

Folgende Kernkomponenten bilden die BGP-Architektur:

- **On-Premises:**
  - Zwei OPNsense-Instanzen als BGP-Peer auf On-Premises.
- **AWS:**
  - AWS Transit Gateway als BGP-Peer auf AWS.

13.6.2 BGP-Topologie

Die BGP-Routingstruktur nutzt zwei unabhängige AWS Site-to-Site VPN-Verbindungen, die jeweils zwei parallele IPSec-Tunnel mit BGP-Routing haben.

BGP-Peering-Struktur:

BGP-Session	Endpunkt On-Premises	Endpunkt AWS	AS-Nummern
BGP-Peering-1	OPNsense Instanz Primary	AWS Transit Gateway	65001 ↔ 64512
BGP-Peering-2	OPNsense Instanz Primary	AWS Transit Gateway	65001 ↔ 64512
BGP-Peering-3	OPNsense Instanz Secondary	AWS Transit Gateway	65001 ↔ 64512
BGP-Peering-4	OPNsense Instanz Secondary	AWS Transit Gateway	65001 ↔ 64512

Tabelle 42 BGP-Peering-Struktur

Wichtig zu beachten ist, dass jede OPNsense-Instanz zwei BGP-Peerings zum AWS Transit Gateway aufbaut. Das stellt sicher, dass jeder VPN-Tunnel seine eigene BGP-Session hat.

Die AS-Nummern der jeweiligen Komponenten sind:

- On-Premises verwendet für alle Peerings die private ASN 65001
- AWS Transit Gateway verwendet für alle Peerings die private ASN 64512

13.6.3 BGP-Routing-Mechanismen & Failover

Bei erfolgreicher Konfiguration des BGPs werden die OPNsense-Instanzen und der AWS Transit Gateway den Traffic bei einem Ausfall eines Geräts automatisch auf die verbleibenden Tunnel umleiten. Die Routen der OPNsense-Primary-Instanz werden absichtlich mit einer niedrigeren AS-Path-Länge konfiguriert als die der OPNsense-Secondary-Instanz. Dies stellt sicher, dass der Traffic, wenn verfügbar, immer über die OPNsense Primary-Instanz geht. Falls eine komplette OPNsense-Instanz ausfallen sollte, übernimmt die andere automatisch mit der konfigurierten VPN-Verbindung und BGP-Routen.

13.7 Monitoring-Konzept

Dieses Kapitel beschreibt alle Komponenten und Metriken der Monitoring-Architektur auf AWS.

13.7.1 Architekturübersicht

Die Monitoring-Architektur basiert auf zwei AWS Services.

Die verwendeten AWS Services sind:

- **AWS CloudWatch Alarms** → Überwacht die AWS Site-to-Site-VPN-Tunnels
- **AWS SNS (Simple Notification Service)** → Versendet Alarme an verantwortliche Personen

Folgende Komponenten werden in das Monitoring-System mit einbezogen. Alle anderen hier nicht aufgeführten Komponenten werden nicht überwacht.

Zu überwachende Komponenten:

- **AWS Site-to-Site VPN Connection 1 Tunnel 1 &2**
- **AWS Site-to-Site VPN Connection 2 Tunnel 1 & 2**

Die Aufgabenstellung umfasst ausschliesslich das Monitoring der VPN-Verbindung. Daher wird auf die Überwachung anderer Komponenten verzichtet.

13.7.2 Monitoring-Metriken

Der AWS Service CloudWatch stellt verschiedene Metriken über die VPN-Verbindungen zur Verfügung. Konkret belaufen sich die verfügbaren Metriken auf:

- **Tunnel Data In** → Stellt dar, wie viel Daten (Bytes) über den Tunnel empfangen wurden.
- **Tunnel Data Out** → Stellt dar, wie viel Daten (Bytes) über den Tunnel gesendet wurden.
- **Tunnel State** → Stellt dar, ob der Tunnel Status up (1) oder down (0) ist.

Diese Metriken werden pro Tunnel erhoben. Das bedeutet, die oben genannten Metriken existieren in vier verschiedenen Kontexten. Wichtig zu beachten ist auch, dass die genaue Metrik für den Tunnel State nicht als Up oder Down gekennzeichnet wird, sondern mit 0 für Down und 1 für Up.

13.7.3 Schwellwerte

Um eine Alarmierung möglichst effizient und zuverlässig zu gestalten, muss man die richtigen Schwellwerte definieren, damit bei einem Ausfall das Monitoring früh genug Alarm schlägt.

Die Schwellwerte für dieses Monitoring-System sind in folgender Tabelle definiert.

Komponente	Schwellwert (Up/Down)	Aktion bei Down (0)	Priorität	Dringlichkeit
AWS Site-to-Site VPN Connection 1 Tunnel 1	Up (1) = OK, Down (0) = Alarm	Alarm per AWS SNS	1	Hoch
AWS Site-to-Site VPN Connection 1 Tunnel 2	Up (1) = OK, Down (0) = Alarm	Alarm per AWS SNS	2	Hoch
AWS Site-to-Site VPN Connection 2 Tunnel 1	Up (1) = OK, Down (0) = Alarm	Alarm per AWS SNS	1	Hoch
AWS Site-to-Site VPN Connection 2 Tunnel 2	Up (1) = OK, Down (0) = Alarm	Alarm per AWS SNS	2	Hoch

Tabelle 43 Monitoring Schwellwerte, Aktion, Priorität und Dringlichkeit

Falls ein Tunnel auf Down (0) fällt, sendet AWS CloudWatch Alarms sofort eine Warnung. AWS SNS benachrichtigt die verantwortlichen Personen.

13.8 Backup-Recovery-Konzept

Dieses Kapitel umfasst das Konzept für eine Backup-Recovery-Strategie der On-Premises-Infrastruktur.

13.8.1 Zielsetzung & Anforderungen

Das Ziel dieses Backup & Recovery Konzepts ist die Minimierung von Datenverlusten und Ausfallzeiten der On-Premises-Infrastruktur.

Die Infrastruktur, die Bestandteil dieses Backup- und Recovery-Konzepts ist, umfasst ausschliesslich die beiden OPNsense-Instanzen. Für diese werden zwei unterschiedliche Backup-Methoden angewendet:

Backup-Typ	Beschreibung	Vorteile	Nachteile
Snapshot-Backup	Erstellung eines vollständigen VM-Snapshots	Vollständige Wiederherstellung aller Daten & Konfigurationen	Höherer Speicherbedarf
Konfigurations-Backup (Config-File)	Export aller OPNsense-Konfigurationen	Sehr geringer Speicherbedarf, schnelle Wiederherstellung	Erfordert Neuinstallation bei Systemfehlern

Tabelle 44 Backup-Typen

13.8.2 Backup-Inhalte

Folgende Inhalte werden von den definierten Backup-Bereichen auf der On-Premises-Infrastruktur gesichert:

Backup-Bereich	Datenumfang	Grund für Sicherung
OPNsense-Konfiguration	Config-File (Firewall-Regeln, VPN, BGP)	Sicherstellen, dass alle Netzwerkeinstellungen wiederhergestellt werden können.
VM-Snapshot (OPNsense-VMs)	Vollständige Snapshots der OPNsense-Instanzen	Falls ein kompletter Systemausfall eintritt.

Tabelle 45 Backup-Inhalte

13.8.3 Backup-Strategie & Häufigkeit

Nachfolgendes Kapitel beschreibt die Backup-Intervalle für die verschiedenen Systeme:

Backup-Typ	Methode	Häufigkeit	Aufbewahrung	Sicherer Backup-Speicherort
OPNsense-Konfiguration	Export Config-File (config.xml)	Wöchentlich & vor Änderungen	4 Wochen	Externe Festplatte Offline
VM-Snapshot (OPNsense-VMs)	Manuelles Snapshot-Backup über VMware ESXi	Vor grösseren Änderungen	4 Wochen	WMWare vSphere ESXi Host

Tabelle 46 Backup-Strategie & Häufigkeit

13.9 Testkonzept

Dieses Kapitel definiert das Testkonzept für die gesamte Infrastruktur. Dieses Konzept stellt sicher, dass die gesamte Umgebung reibungslos funktioniert und mögliche Fehlkonfigurationen ausgemacht werden können.

13.9.1 Zielsetzung & Testanforderungen

Das Testkonzept verfolgt folgende Ziele:

- Sicherstellen, dass alle Komponenten der Infrastruktur fehlerfrei funktionieren
- Frühzeitige Erkennung von Konfigurationsfehlern.
- Nachweis der Systemstabilität unter normalen und besonderen Bedingungen.

Testkategorie	Beschreibung
Funktionstests	Sicherstellen, dass Netzwerkkonnektivität, Firewall-Regeln und VPN-Tunnel korrekt arbeiten.
Leistungstests	Test der Systembelastung (z. B. Bandbreite, VPN-Traffic, Latenz).
Failover-Tests	Prüfung der Hochverfügbarkeit durch gezielte Simulation von Ausfällen.
Recovery-Tests	Prüfen ob ein Backup oder Snapshot wiederhergestellt werden kann.

Tabelle 47 Testkategorien

13.9.2 Teststrategie & Testverfahren

Testmethoden für die Infrastruktur:

Testmethode	Ziel	Werkzeuge
Ping & Traceroute	Netzwerkverbindungen überprüfen	ping, traceroute
Bandbreite	Bandbreite der VPN-Verbindung überprüfen	iPerf, speedtest-cli
VPN-Statusprüfung	Funktion der IPSec-Tunnel sicherstellen	OPNsense Status Dashboard, AWS Console
Failover-Simulation (CARP-Test)	Test der Hochverfügbarkeit	Manuelles Deaktivieren der Primary OPNsense
Monitoring Test	Alert Mitteilung bei Ausfall erhalten	AWS CloudWatch, Email

Tabelle 48 Teststrategien & Testverfahren

13.9.3 Testfälle detailliert

Folglich werden alle Testfälle detaillierter beschrieben. Die genauen Beschriebe zu den jeweilig abgedeckten Anforderungen sind in der Initialisierung aufzufinden.

1. Testfall

ID: T1	Abgedeckte Anforderung: FA3, FA4, FA6	Netzwerk-Konnektivitätstest
Testszenario	Mit diesem Testszenario wird überprüft, ob die Netzwerkverbindungen den Vorgaben entsprechend funktionieren.	
Testvoraussetzungen	• Alle Netzwerkgeräte (Switches, Firewalls, Router) gemäss Netzplan müssen eingeschaltet sein • Netzwerkinterfaces müssen nach der Anleitung konfiguriert sein • Alle relevanten IP-Adressen müssen zugewiesen sein.	
Testschritte	1. **Ping-Test:** Führe ping-Befehl vom On-Premises-Testserver zu einem AWS-Testserver durch. **Command:** ping 10.100.10.20 2. **Traceroute-Test:** Überprüfe die Netzwerkpfade mit traceroute oder mtr. **Command:** traceroute 10.100.10.20 5. **BGP-Routing-Test:** Verifiziere die BGP-Routen über OPNsense Dashboard: Routing → Diagnostics → BGP	
Erwartete Resultate	• **Ping-Test:** Alle definierten Ziele sind erreichbar, keine Paketverluste. • **Traceroute:** Der Netzwerkpfad folgt der erwarteten Route gemäss Netzplan ohne unerwartete Hops. • **BGP-Test:** Die erwarteten BGP-Routen gemäss Netzplan sind aktiv und korrekt verteilt.	

Tabelle 49 Testfall 1

2. Testfall

ID: T2	Abgedeckte Anforderung: FA6	VPN-Performance-Test
Testszenario	Dieser Test überprüft, ob die Bandbreite der VPN-Verbindung den Erwartungen entspricht.	
Testvoraussetzungen	• VPN-Tunnel zwischen On-Premises und AWS muss aktiv sein. • Beide Endpunkte müssen über einen iPerf-Server oder Client verfügen. • Kein anderer grosser Datenverkehr sollte während des Tests laufen.	
Testschritte	1. **iPerf-Server auf AWS-Testinstanz starten:** **Command:** iperf -s 2. **iPerf-Client auf On-Premises Testserver ausführen:** **Command**: iperf -c 10.100.10.20 -t 30 3. **Ergebnisse analysieren:** Vergleiche die gemessene Bandbreite mit den erwarteten Werten.	
Erwartete Resultate	• Die gemessene Bandbreite entspricht der erwarteten VPN-Kapazität von 100 Mbit/s Symmetrisch. • Die Latenz ist im definierten Bereich von ca. 25ms	

Tabelle 50 Testfall 2

3. Testfall

ID: T3	Abgedeckte Anforderung: FA1, FA2, FA3	IPSec-Tunnel-Statusprüfung
Testszenario	Sicherstellen, dass die alle VPN-Tunnel zwischen On-Premises und AWS verbunden sind.	
Testvoraussetzungen	• Die VPN-Konfiguration muss nach Anleitung konfiguriert worden sein. • OPNsense- und AWS-VPN-Status-Dashboards müssen zugänglich sein.	
Testschritte	1. **Status der VPN-Tunnel in OPNsense prüfen (Primary und Secondary):** **Navigieren zu:** VPN → IPsec → Status Overview Prüfen, ob alle Tunnel den Status **"Connected"** haben 2. **Status der VPN-Tunnel auf AWS Prüfen:** **Navigieren zu:** AWS Console → VPC → VPN Connections Prüfen, ob alle Tunnel den Status **"UP"** haben	
Erwartete Resultate	Alle vier Tunnel erweisen den Status UP/Connected in beiden Dashboards.	

Tabelle 51 Testfall 3

4. Testfall

ID: T4	Abgedeckte Anforderung: FA1, FA6	Hochverfügbarkeits-Failover-Test
Testszenario	Überprüfung der Hochverfügbarkeit, indem die primäre OPNsense-Instanz deaktiviert wird.	
Testvoraussetzungen	• CARP-Setup mit einer **Primary- und Secondary-OPNsense-Instanz** muss nach Anleitung konfiguriert worden sein. • Der HA-Sync-Status zwischen den Instanzen muss auf «**Synced**» sein.	
Testschritte	1. **Primäre OPNsense-Instanz deaktivieren:** - **Im Dashboard:** Power → Power Off 2. **Sekundäre OPNsense prüfen:** - Status → Unter «Virtual IP» sollte der Status der Backup-Instanz auf **"Master"** wechseln. 3. **VPN-Verbindungen & Routing testen:** - ping zwischen On-Premises & AWS wiederholen. 4. **Nach 5 Minuten primäre Instanz wieder aktivieren:** - Hochfahren der Primary-VM und prüfen, ob sie wieder **Master** wird.	
Erwartete Resultate	• Sekundäre OPNsense übernimmt die virtuelle IP (CARP Failover). • VPN-Tunnel bleibt stabil (keine langen Unterbrechungen). • Firewall- und Routing-Funktionalität bleibt bestehen.	

Tabelle 52 Testfall 4

5. Testfall

ID: T5	Abgedeckte Anforderung: FA5	CloudWatch-Monitoring-Test
Testszenario	Überprüfung, ob Ausfälle über **AWS CloudWatch & E-Mail-Benachrichtigungen** gemeldet werden.	
Testvoraussetzungen	• AWS CloudWatch **Alarm für VPN-Tunnelstatus** muss eingerichtet sein. • AWS SNS muss konfiguriert sein, um **E-Mail-Benachrichtigungen** zu senden. • Ein Admin-Benutzer muss Zugriff auf die Logs haben.	
Testschritte	1. **VPN-Verbindung absichtlich deaktivieren:** - In OPNsense: VPN → IPsec → Status Overview → Disconnect Tunnel. 2. **CloudWatch Dashboard öffnen:** - AWS Console → CloudWatch → Alarms. 3. **Alarm-Status prüfen:** - Alarmstatus muss von **OK → ALARM** wechseln. 4. **E-Mail-Benachrichtigung verifizieren:** - Überprüfung, ob die Alarm-Mail an den Administrator gesendet wurde.	
Erwartete Resultate	• AWS CloudWatch zeigt einen **ALARM** für die unterbrochene VPN-Verbindung. • Eine **E-Mail-Benachrichtigung** wird an die Verantwortlichen gesendet. • Nach Wiederherstellung des Tunnels wechselt der Alarm zurück auf **OK**	

Tabelle 53 Testfall 5

6. Testfall

ID: T6	Abgedeckte Anforderung: IPA Kriterium	Backup-Recovery-Konzept Test
Testszenario	Sicherstellen, dass das Backup-System funktionsfähig ist und eine vollständige Wiederherstellung der gesicherten Daten erfolgreich durchgeführt werden kann.	
Testvoraussetzungen	• Ein aktuelles Backup ist vorhanden. • Zugriff auf das Backup-System und Wiederherstellungssoftware ist sichergestellt. • Eine Testumgebung steht zur Verfügung, um die Wiederherstellung ohne Risiko für die Produktionssysteme durchzuführen.	
Testschritte	**1. Backup-Überprüfung:** - Prüfen, ob das Backup vollständig und aktuell ist. - Sicherstellen, dass alle erforderlichen Dateien enthalten sind. **2. Wiederherstellungsprozess einleiten:** - Backup in einer separaten Testumgebung wiederherstellen. - Prüfen, ob die Wiederherstellung ohne Fehler durchläuft. **3. Integritätsprüfung:** - Vergleich der wiederhergestellten Daten mit den Originaldaten. - Prüfung, ob Konfigurationen und Berechtigungen korrekt wiederhergestellt wurden. **4. Systemtests nach Wiederherstellung:** - Testen, ob alle Dienste und Anwendungen nach der Wiederherstellung ordnungsgemäss funktionieren. - Netzwerkverbindungen und Zugriffe testen.	
Erwartete Resultate	• Das Backup kann erfolgreich wiederhergestellt werden. • Alle Daten sind vollständig und ohne Fehler verfügbar. • Die wiederhergestellten Systeme und Dienste funktionieren wie im Originalzustand. • Falls Fehler auftreten, werden diese dokumentiert und das Backup-System entsprechend optimiert.	

Tabelle 54 Testfall 6

14 Realisierung

Im nachfolgenden Abschnitt der Arbeit ist die Realisierung des gesamten Projekts dokumentiert. Am Ende der Realisierungsphase werden die Testfälle durchgeführt.

14.1 On-Premises-Umgebung aufbauen

Der erste Punkt in der Realisierung ist der Aufbau der On-Premises Umgebung. Also wird jetzt die Installation und Konfiguration der beiden OPNsense Instanzen dokumentiert.

14.1.1 Installation der OPNsense Instanzen

Als erstes müssen die OPNsense Instanzen als VM-Definition im VMware vSphere ESXi erstellt werden.

1. VM-Erstellung starten

- Öffne den **ESXi Host Client**
- Klicke auf **«Create / Register VM»**

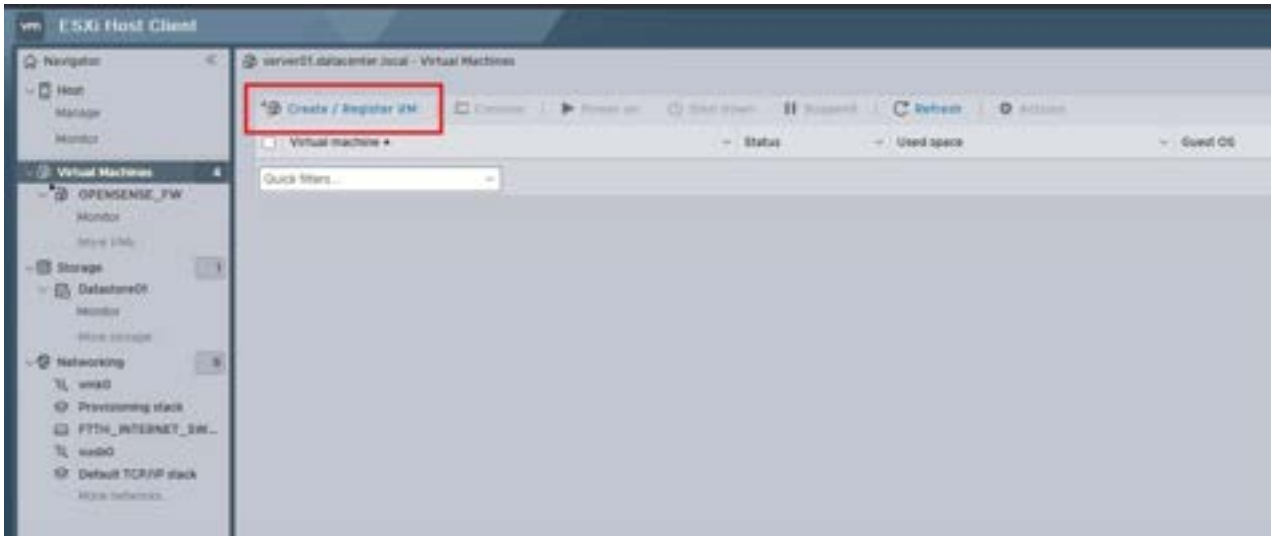


Abbildung 18 VM-Erstellung Starten

2. Wähle «Create a new virtual machine»

- Klicke auf «**Next**»

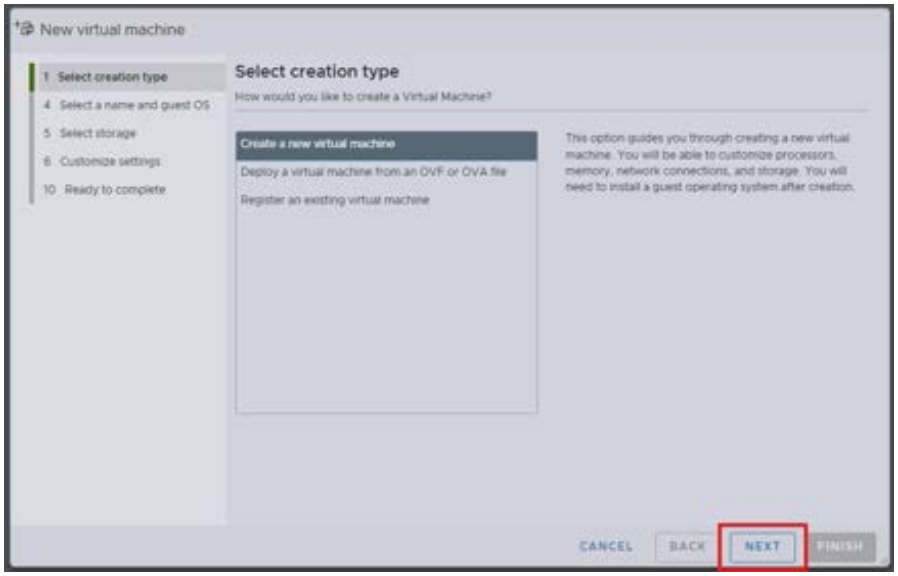


Abbildung 19 Neue virtuelle Maschine

3. Name und Gast-Betriebssystem festlegen

- Gib einen **Namen** für die VM ein
- Wähle die **Kompatibilität** (z. B. ESXi 7.0 U2).
- Setze **Guest OS Family** auf **Other**.
- Wähle als **Guest OS Version FreeBSD 13 oder später (64-bit)**.
- Klicke auf **«Next»**.

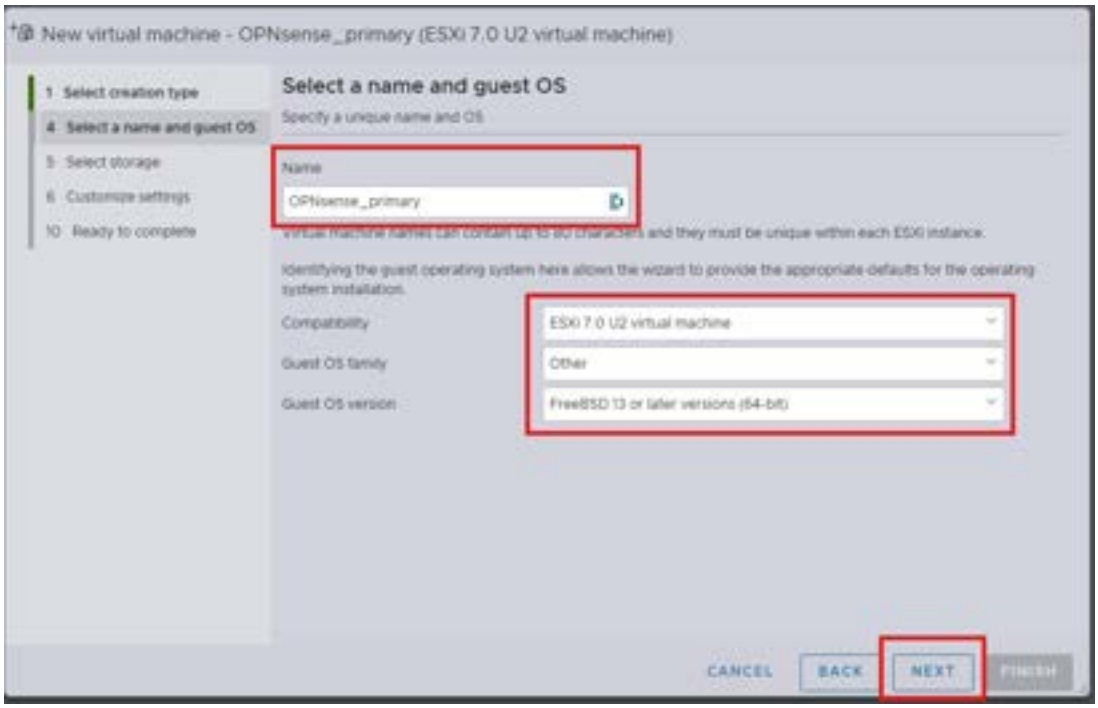


Abbildung 20 Name und Gast-Betriebssystem festlegen

4. Speicherort auswählen

- Wähle den gewünschten **Datastore** für die VM
- Klicke auf **«Next»**.

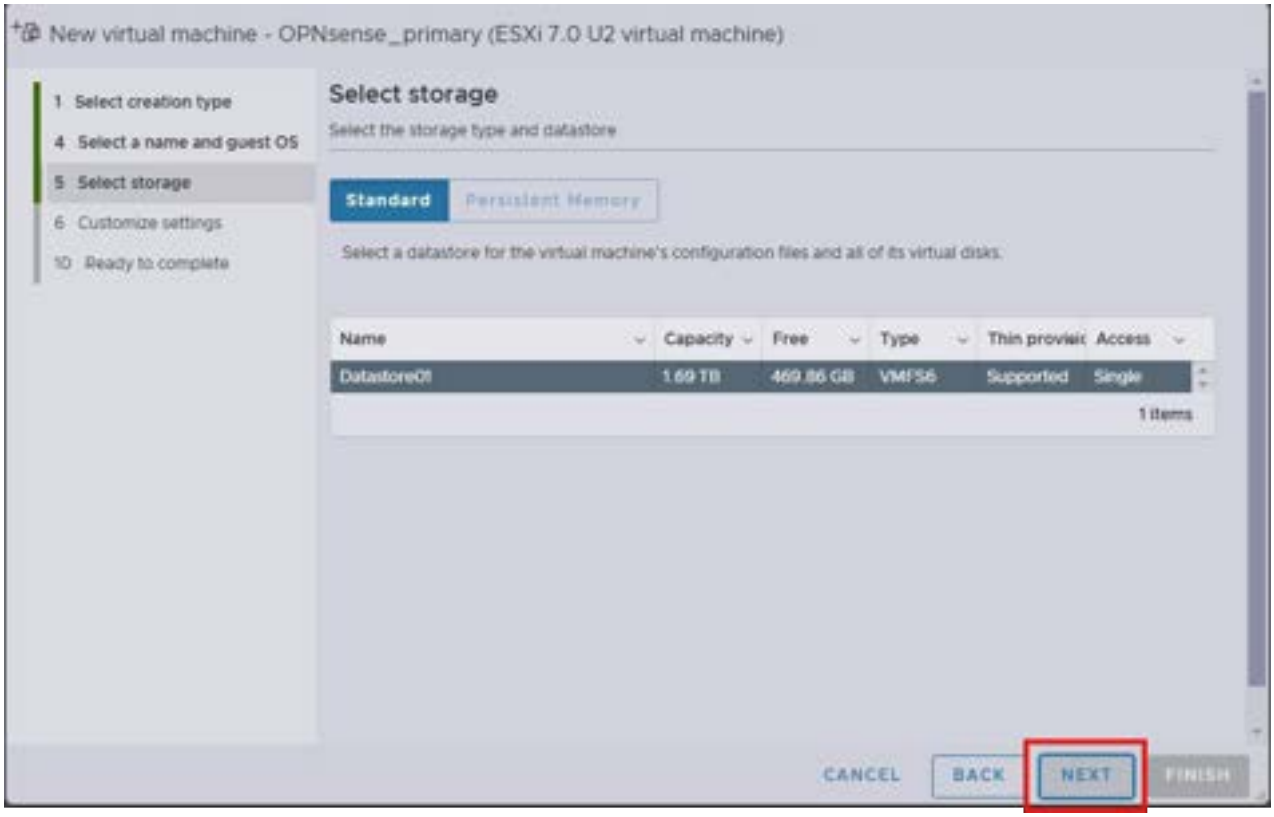


Abbildung 21 Speicherort auswählen

5. Hardware anpassen

- **CPU**: Setze die Anzahl auf **6 Cores**.
- **RAM**: Setze den Speicher auf **20GB**.
- **Festplatte**: Stelle **40GB** ein.
- **Adapter 1:** FTTH_INTERNET_01 (verbunden).
- **Adapter 2:** ON_PREMISES_NET (verbunden).
- **CD/DVD-Laufwerk hinzufügen**.

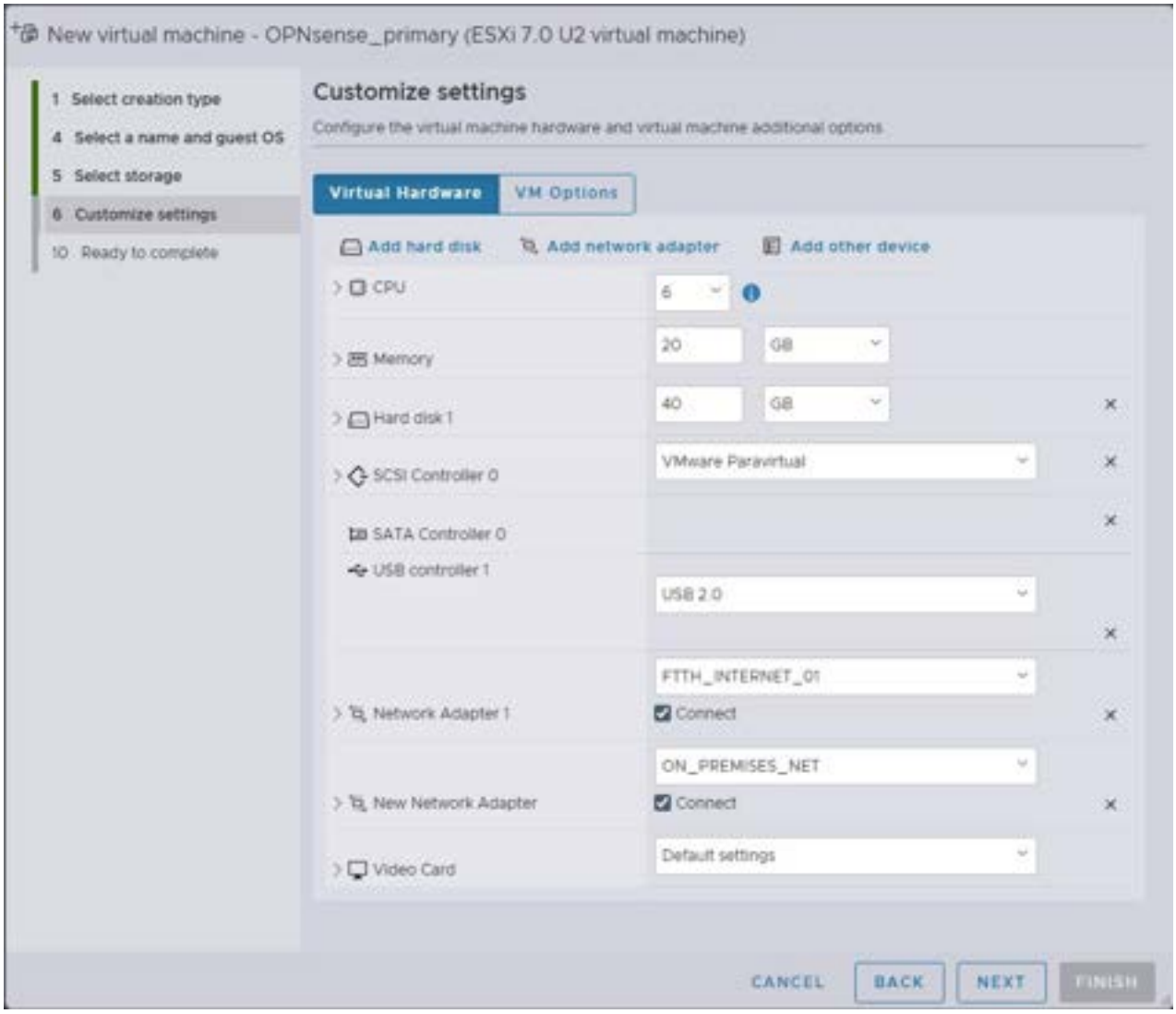


Abbildung 22 Hardware anpassen 1

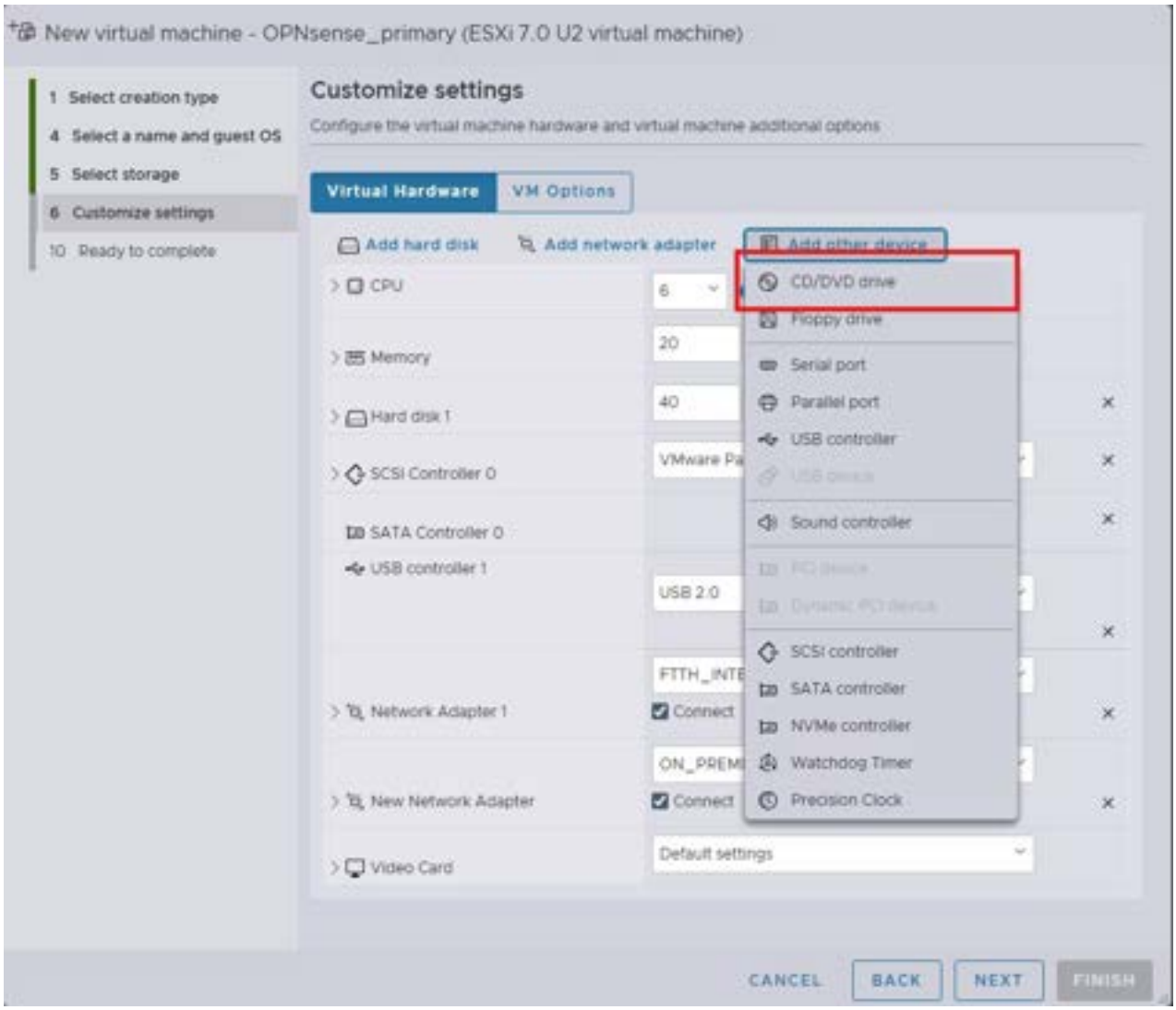


Abbildung 23 Hardware anpassen 2

6. ISO-Image einbinden

- Wähle als **CD/DVD-Laufwerk** die Option **«Datastore ISO file»**.
- Suche das passende **ISO-Image** im Datastore.
- Klicke auf **«Select»**.

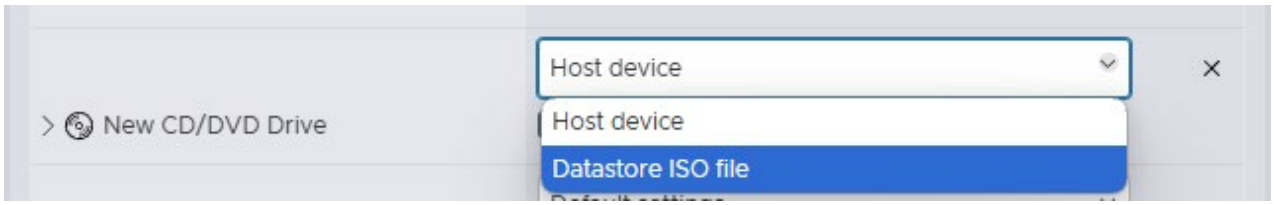


Abbildung 24 ISO-Image einbinden 1

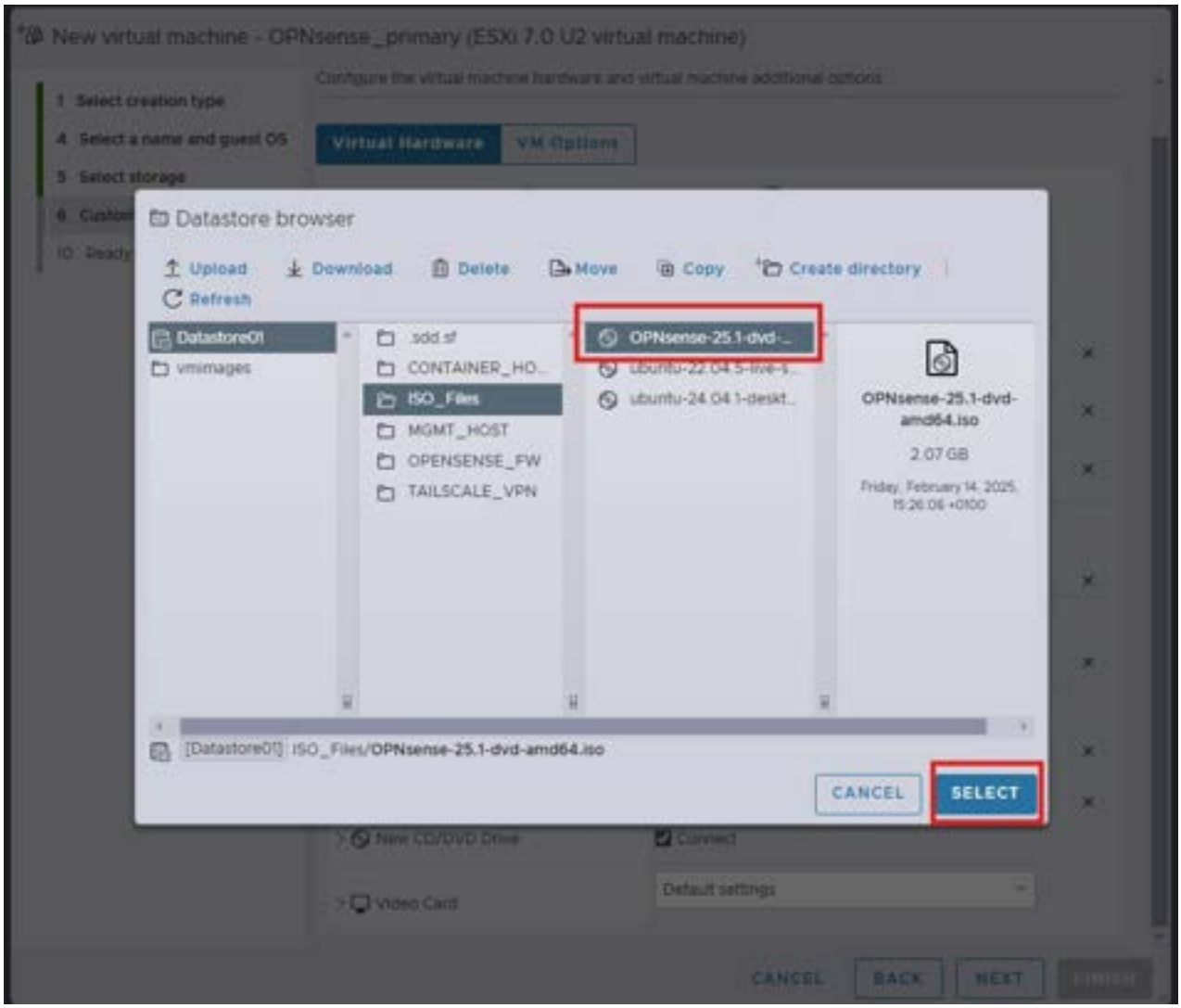


Abbildung 25 ISO-Image einbinden 2

7. Überprüfung und Abschluss

- Überprüfe alle **Einstellungen**
- Klicke auf «**Finish»**, um die VM zu erstellen

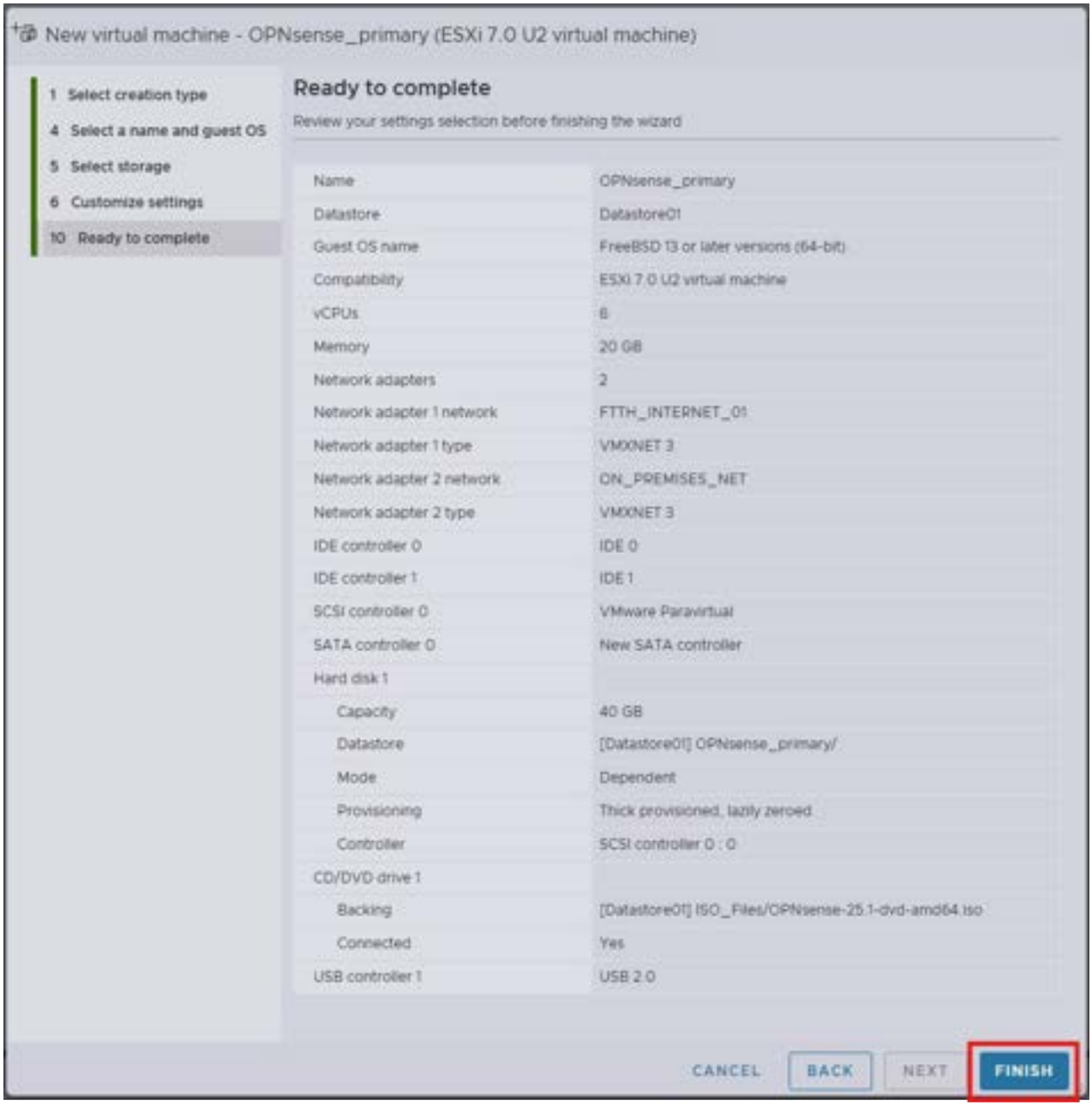


Abbildung 26 Überprüfung und Abschluss

Es sollte dann ungefähr so aussehen. Nun muss der gleiche Prozess für die Secondary-Instanz erneut durchlaufen werden. **Da die Konfiguration grundsätzlich identisch ist, wird dieser Schritt nicht nochmals dokumentiert.**



Abbildung 27 Erfolgreiche Konfiguration OPNsense Primary

Wichtig: Es ist zu beachten, dass sich die Netzwerkadapter von der Primary Instanz vor allem im Bezug auf den Uplink Adapter unterscheiden.

Danach sollte es ungefähr so aussehen:



Abbildung 28 Erfolgreiche Konfiguration beide OPNsense-Instanzen

8. VM einschalten

- Wähle die erstellte VM (OPNsense_primary) aus.
- Klicke auf **«Power on»**, um die VM zu starten.



Abbildung 29 VM einschalten

9. Bootvorgang von ISO starten

- Die VM bootet von der eingelegten **OPNsense-ISO-Datei**.
- Es erscheint ein Anmeldebildschirm mit **Live-Umgebung**.
- Melde dich als «installer» an, um die Installation zu starten.

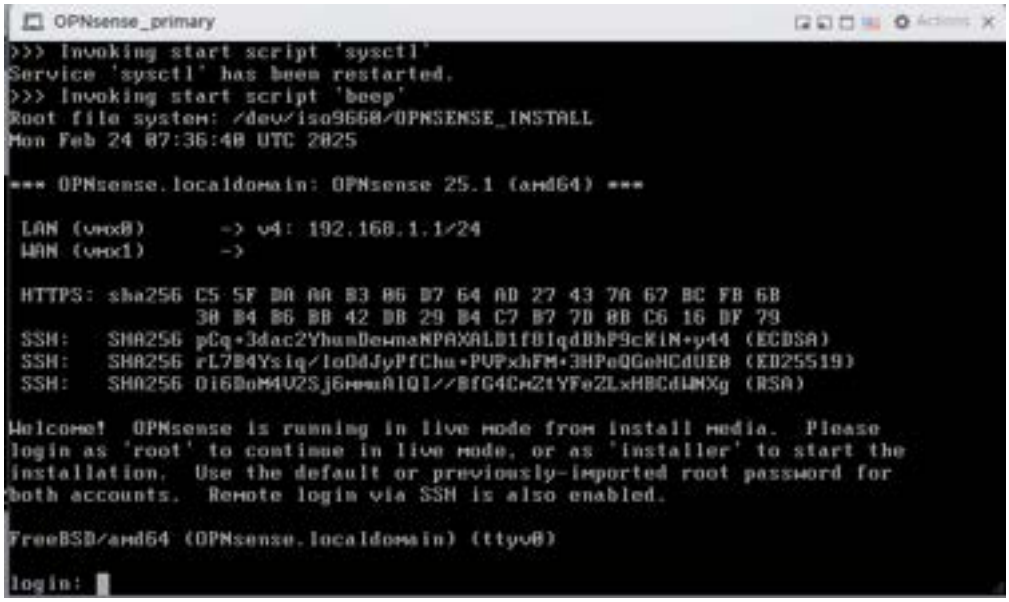


Abbildung 30 Bootvorgang von ISO starten

10. Tastaturlayout auswählen

- Wähle das gewünschte **Keyboard-Layout** (z. B. Swiss-German).
- Bestätige mit **«Select»**.

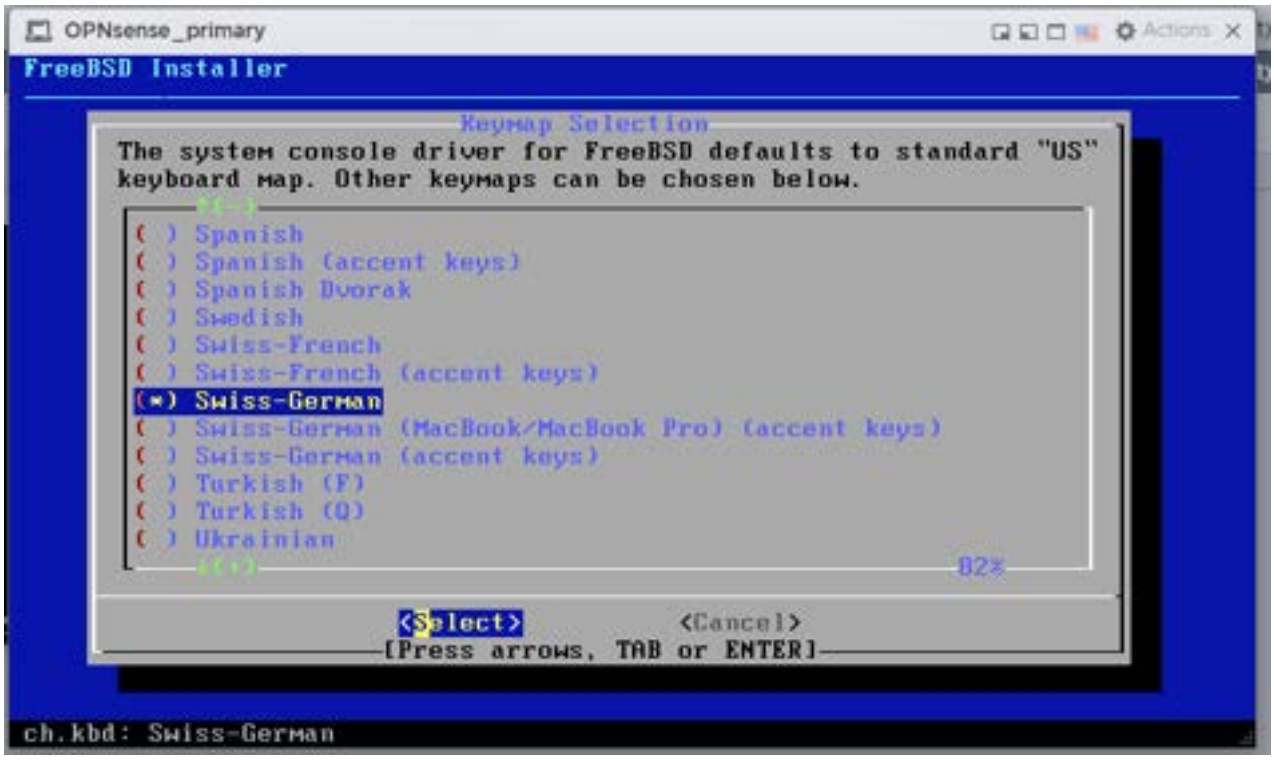


Abbildung 31 Tastaturlayout auswählen

11. Installationsmodus wählen

- Wähle **«Install (ZFS)»**, um ZFS als Dateisystem zu nutzen.



Abbildung 32 Installationsmodus wählen

12. ZFS-Storage-Konfiguration

- Wähle den **Speichertyp** für ZFS (z. B. Stripe - No Redundancy).
- Stripe bedeutet maximale Speicherkapazität, aber keine Redundanz.

Es wird keine Redundanz benötigt, da der Datenspeicher des Servers bereits auf einem RAID basiert.



Abbildung 33 ZFS-Storage-Konfiguration

13. Festplatte für Installation auswählen

- Wähle die **VMware Virtual Disk (da0)** als Installationsziel.
- Bestätige mit **«OK»**.

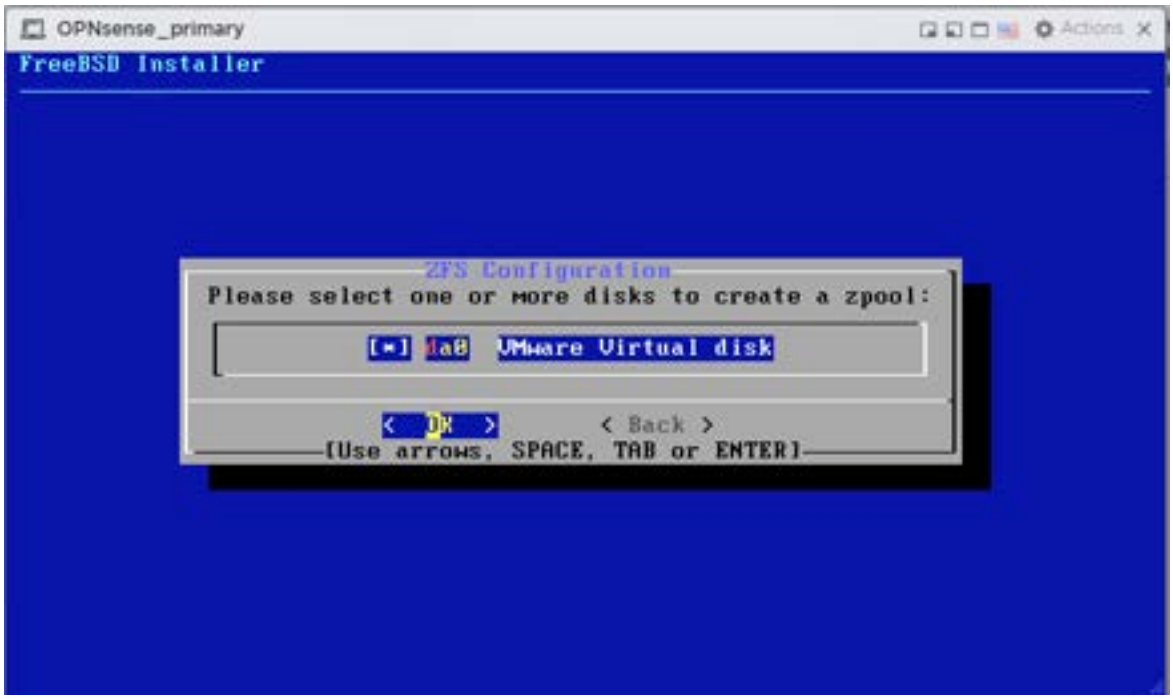


Abbildung 34 Festplatte für Installation auswählen

14. Installation starten

- Der Installer beginnt das System zu **clonen** und auf die Festplatte zu schreiben.
- Warte, bis der Vorgang abgeschlossen ist.

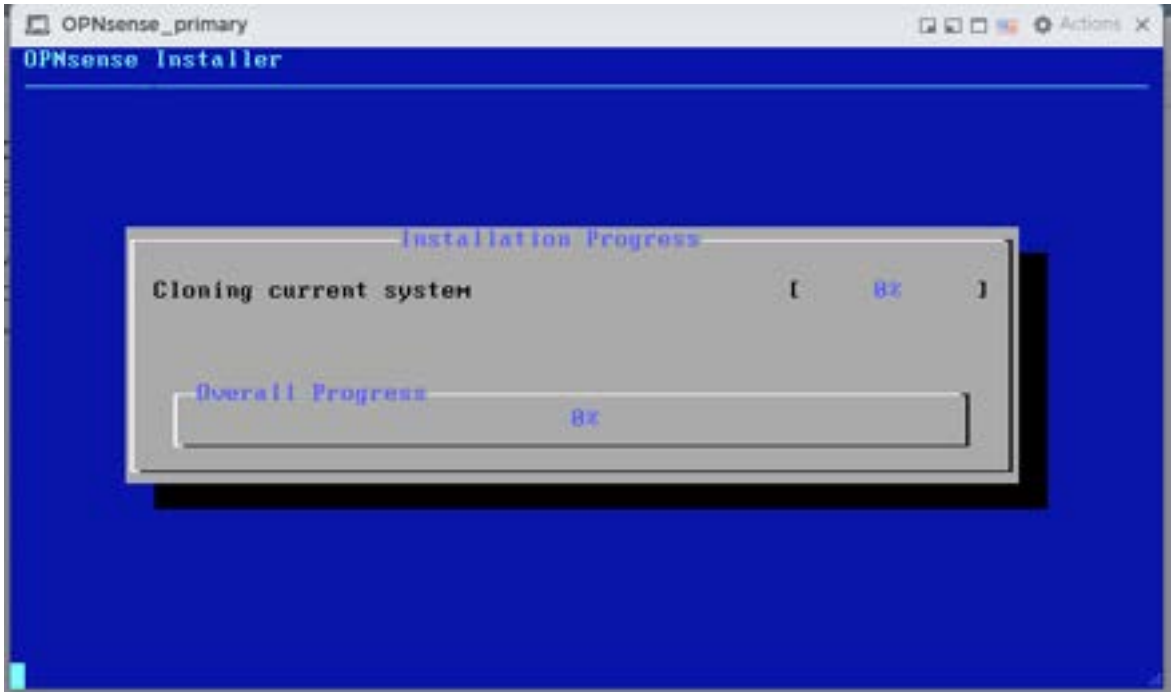


Abbildung 35 Installation starten

15. Finale Konfiguration

- Ändere das **Root-Passwort**
- Bestätige mit **«Complete Install»**, um die Installation abzuschliessen.



Abbildung 36 Finale Konfiguration

14.1.2 Grundkonfiguration der OPNsense Instanzen

Nachdem die Instanzen nun erfolgreich installiert sind, muss man noch die Netzwerk-Adapter korrekt zuweisen und richtig konfigurieren.

1. Grundlegende Konfigurationsübersicht

- Nach dem Start der VM wird die **OPNsense CLI-Menü** angezeigt
- Es können verschiedene Konfigurationen durchgeführt werden, z. B. Netzwerkschnittstellen zuweisen, IP-Adressen setzen oder Firewall-Logs einsehen.

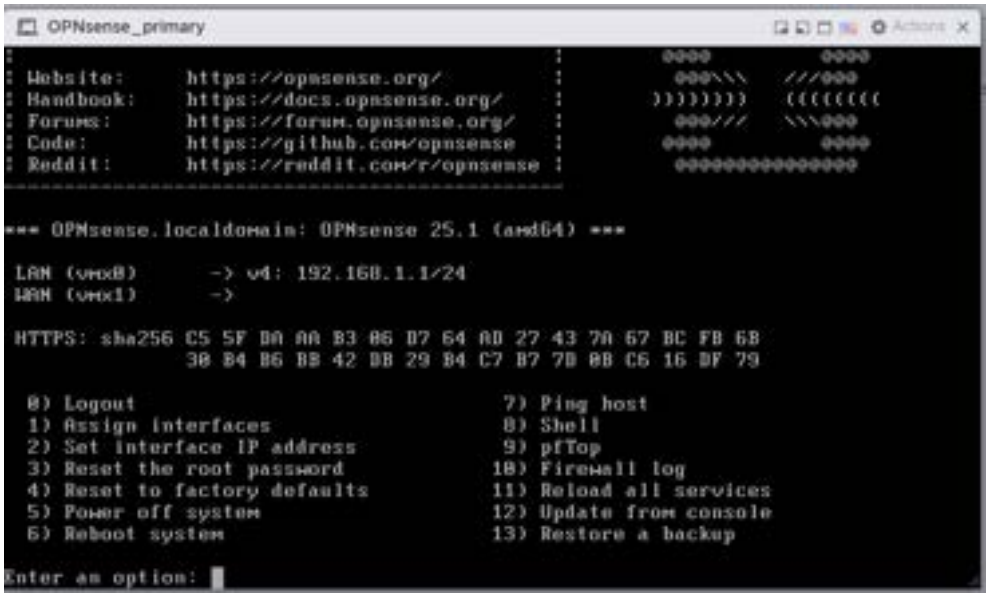


Abbildung 37 Grundlegende Konfigurationsübersicht

2. Netzwerkschnittstellen zuweisen

- Wähle **Option 1**: **«Assign interfaces»**.
- VLANs und LAGG (Link Aggregation) werden nicht benötigt (N für Nein eingeben).
- Verfügbare Netzwerkschnittstellen (vmx0, vmx1) werden aufgelistet.

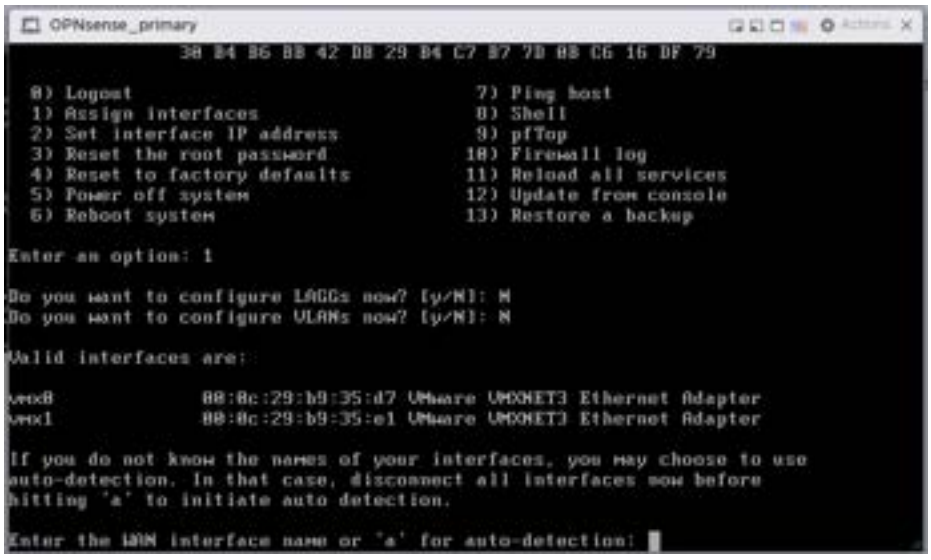


Abbildung 38 Netzwerkschnittstellen zuweisen

3. WAN- und LAN-Interfaces festlegen

- **WAN-Interface** → vmx0
- **LAN-Interface** → vmx1
- Bestätige die Zuweisung mit y.

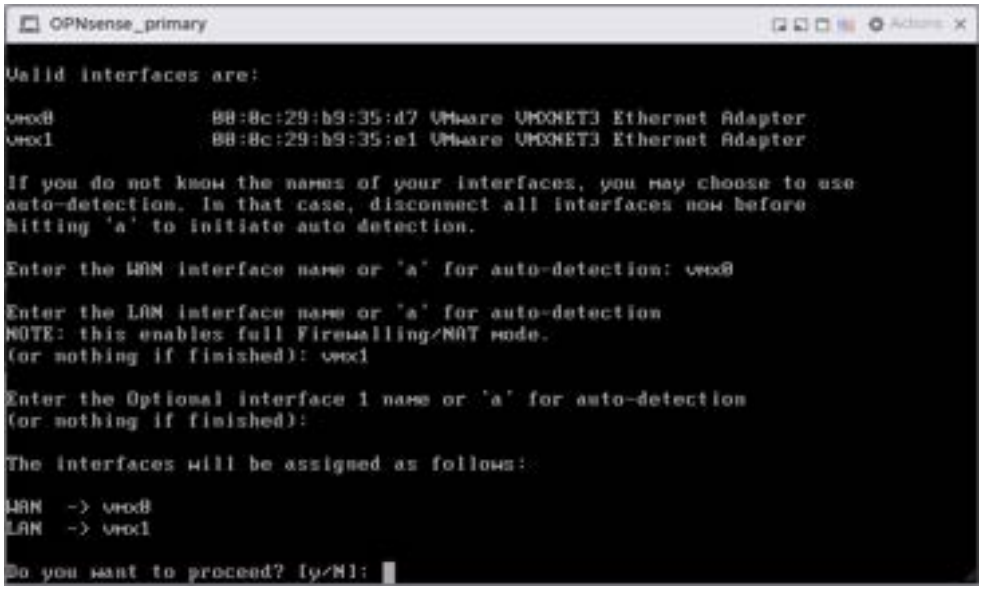


Abbildung 39 WAN- und LAN-Interfaces festlegen

4. Netzwerkkonfiguration prüfen

- Nach dem Neustart der Netzwerkdienste wird die neue IP-Konfiguration angezeigt:
  - **LAN**: 192.168.1.1/24
  - **WAN**: Bezieht eine IP per DHCP

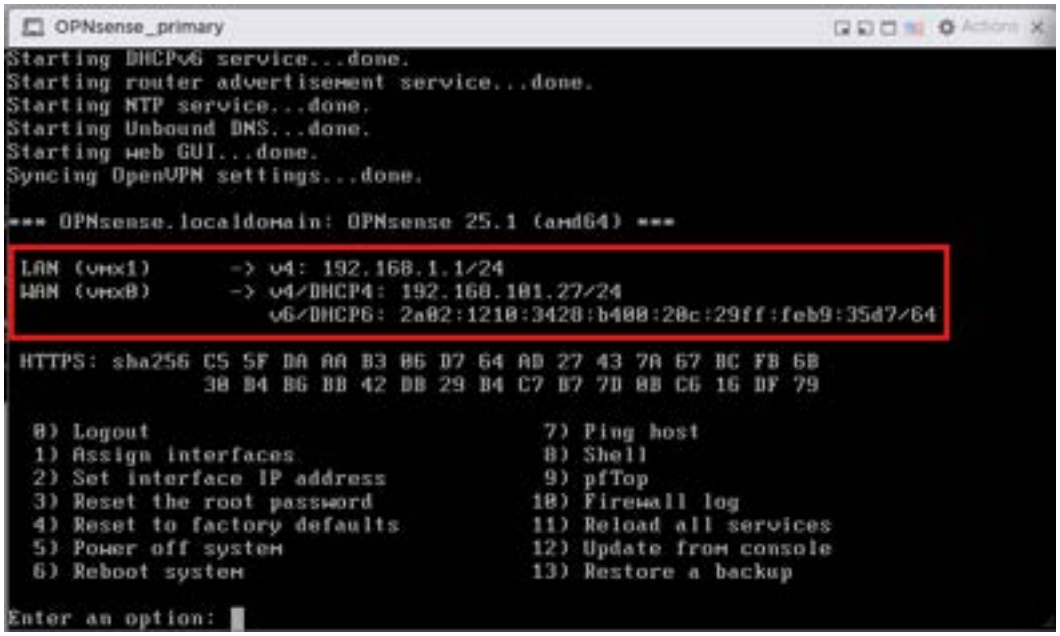


Abbildung 40 Netzwerkkonfiguration prüfen

5. LAN-IP-Adresse ändern

- Wähle **Option 2**: **«Set interface IP address”**.
- Wähle **«LAN»** und setze eine statische IP-Adresse

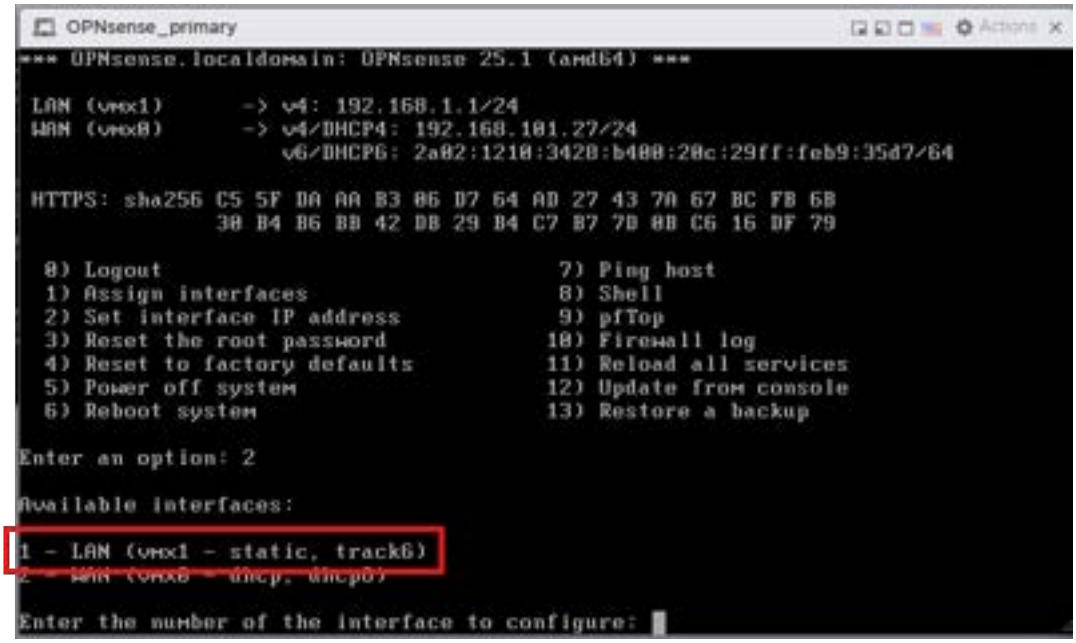


Abbildung 41 LAN-IP-Adresse ändern

6. WAN-IP-Adresse ändern

- Wähle **Option 2**: **«Set interface IP address»**.
- Wähle **«WAN»** und setze eine statische IP-Adresse.

Nach erfolgreicher Konfiguration sollte es wie folgt aussehen. Die gleichen Konfigurationsschritte müssen nun auch auf der Secondary-OPNsense-Instanz durchgeführt werden, wobei dort die IP-Adressen aus dem Konzept verwendet werden sollten.

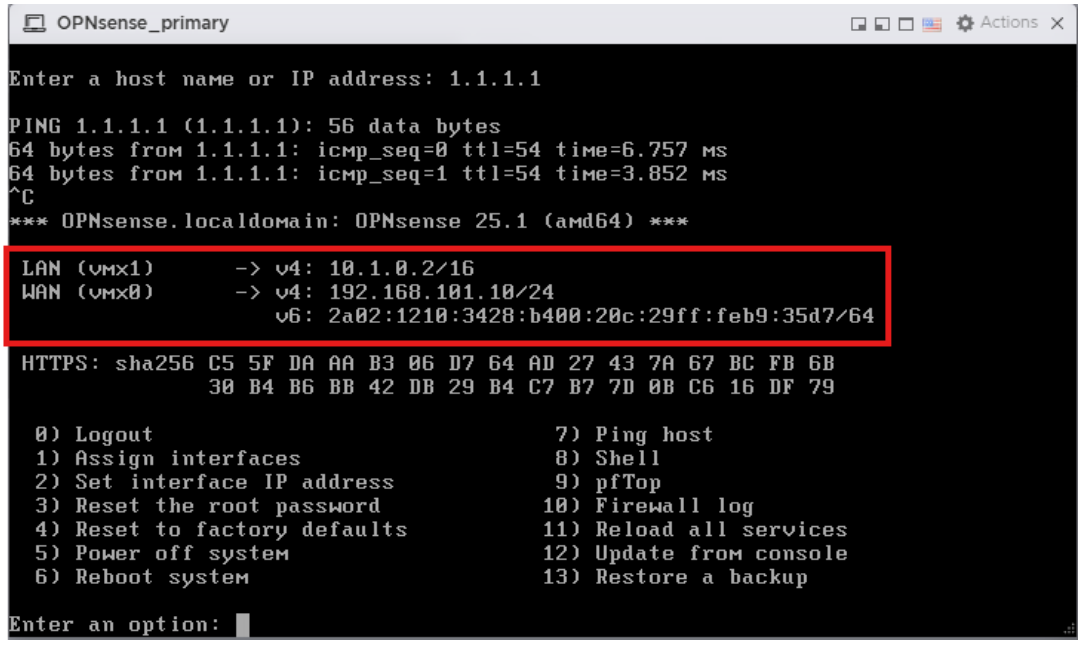


Abbildung 42 WAN-IP-Adresse ändern

7. Zugriff auf das OPNsense-Webinterface

- Öffne einen Browser und gehe zu:
  - https://10.1.0.2
  - https://10.1.0.3
- Melde dich mit den Anmeldedaten an
  - **Benutzername**: root
  - **Passwort**: (Bei der Installation gesetzt).



Abbildung 43 Zugriff auf das OPNsense-Webinterface

8. Erstkonfiguration-Wizard durchlaufen

- Setze Hostnamen und DNS-Server (z. B. 1.1.1.1 und 8.8.8.8).
- Nach Abschluss ist OPNsense einsatzbereit.



Abbildung 44 Erstkonfiguration-Wizard durchlaufen 1



Abbildung 45 Erstkonfiguration-Wizard durchlaufen 2

Wenn alle zuvor genannten Schritte erfolgreich durchgeführt wurden, kann davon ausgegangen werden, dass sämtliche Komponenten der OPNsense-Instanz korrekt installiert, konfiguriert und betriebsbereit sind. Durch die vollständige Implementierung der beschriebenen Installations- und Konfigurationsmassnahmen sind alle notwendigen Systemkomponenten vorhanden und ordnungsgemäss integriert. Dies gewährleistet, dass die Appliance in ihrer vorgesehenen Umgebung fehlerfrei funktioniert und die definierten Anforderungen erfüllt.

14.1.3 Updates und Sicherheitsmassnahmen an den OPNsense Instanzen

Im nächsten Kapitel werden die Updates und Sicherheitseinstellungen beschrieben. Bei Neuinstallationen ist es wichtig, das System als aller erstes auf die neuste Version zu bringen, um Schwachstellen und Sicherheitslücken zu vermeiden. Nach erfolgreichem Update ist die OPNsense-Instanz auf dem neusten Stand und hält den aktuellen Bedrohungen stand.

1. Zum Firmware-Status navigieren

- Im OPNsense-Webinterface gehe zu **Firmware > Status**.



Abbildung 46 Zum Firmware-Status navigieren

2. Nach Update suchen

- Klicke auf **«Check for updates»**, um die neuesten Updates zu prüfen.

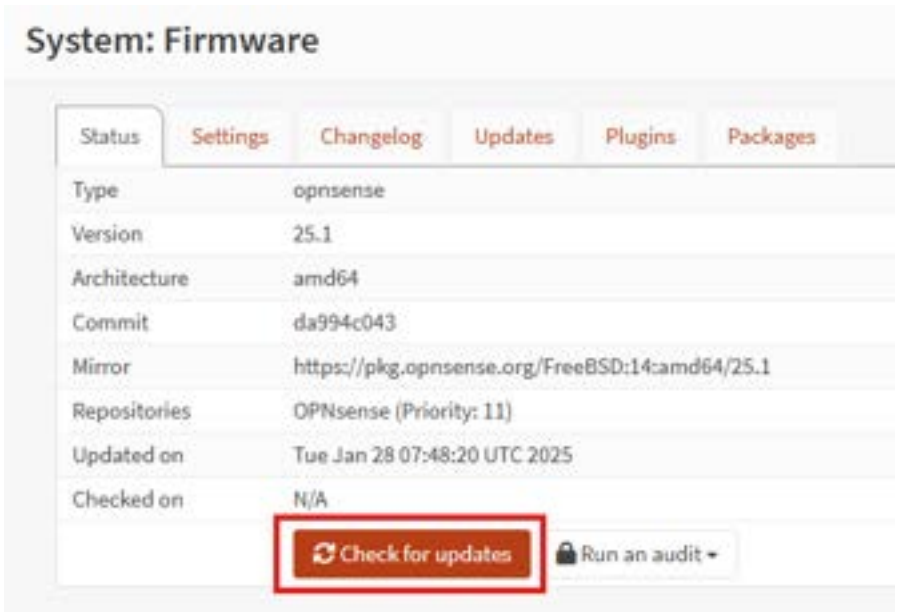


Abbildung 47 Nach Update suchen

3. Verfügbare Updates anzeigen

- Eine Liste der **verfügbaren Updates** wird angezeigt.
- Klicke auf **«Update»**, um alle Pakete auf die neuesten Versionen zu aktualisieren.

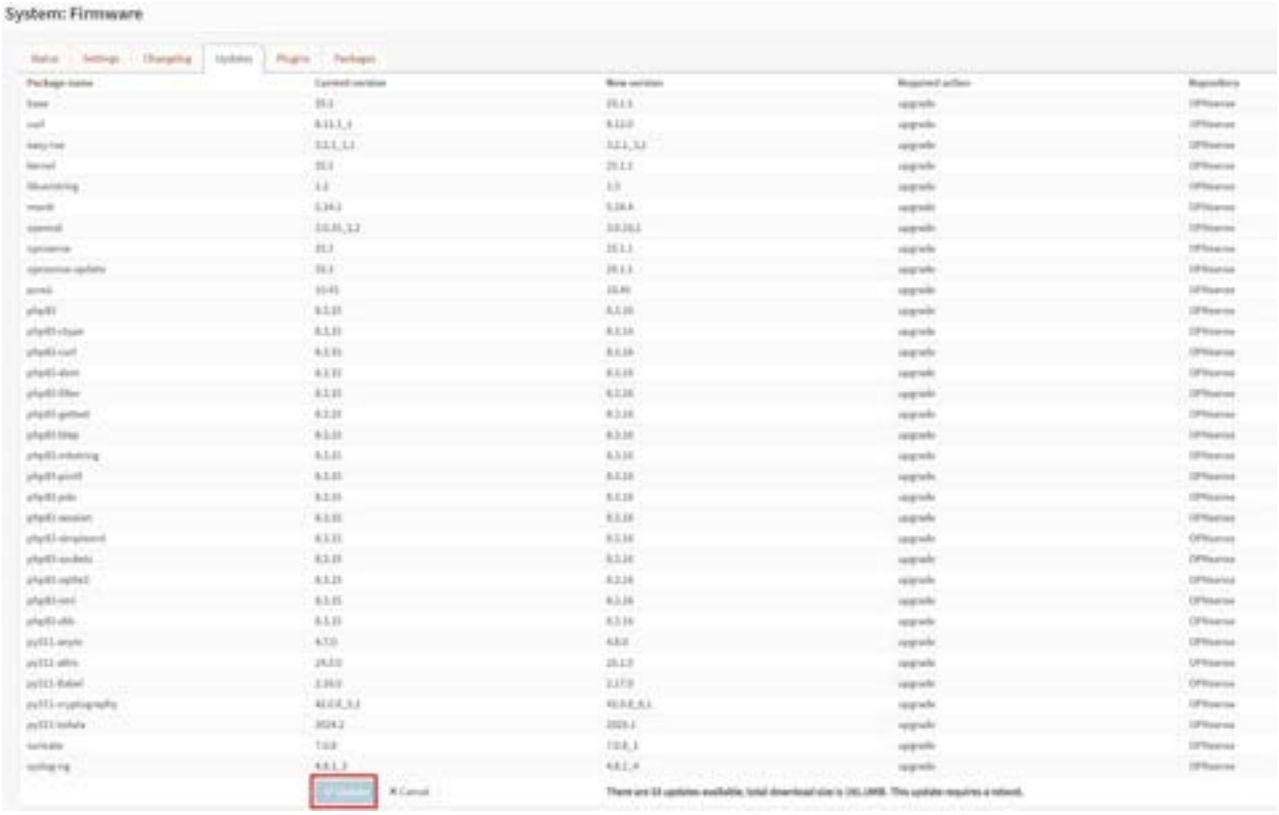


Abbildung 48 Verfügbare Updates anzeigen

4. Neustart erforderlich

- Nach dem Update erscheint eine Meldung, dass die Firewall **automatisch neu startet**.
- Klicke auf **«OK»**, um den Neustart zu bestätigen.

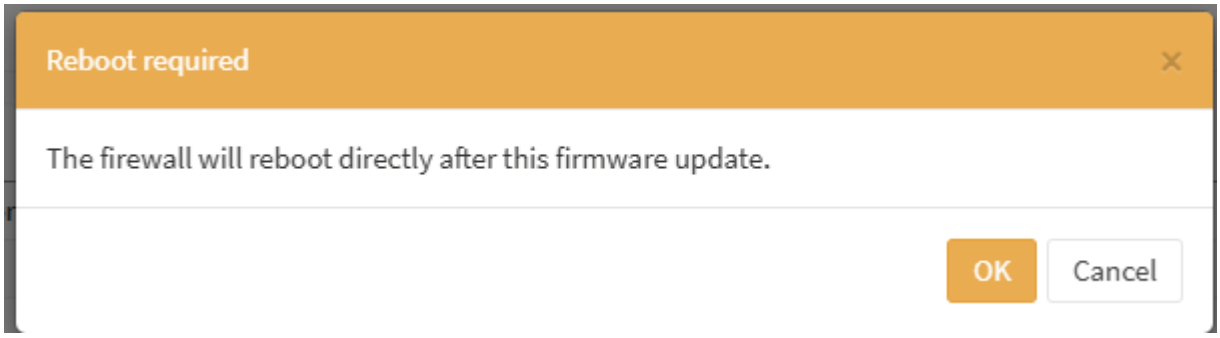


Abbildung 49 Neustart erforderlich

14.1.4 Sicherheitsprüfung und Nachweise

Zur Überprüfung der Sicherheit wurden verschiedene Tests durchgeführt:

- **Firewall-Regel-Test (Manueller Test)**
  - **Ziel:** Prüfen, ob unerwünschter Datenverkehr blockiert wird.
  - **Vorgehen**:
    - Versuche von einem nicht autorisierten Gerät (z. B. deinem persönlichen PC) eine Verbindung zur OPNsense-Instanz herzustellen (z. B. per `ping`, SSH oder http auf das WAN-Interface).
    - Falls die Verbindung blockiert wird → Firewall funktioniert korrekt.
    - Falls die Verbindung durchkommt → Firewall-Regeln überprüfen und anpassen.

```
PS C:\Users\pwyni> ping 192.168.101.10

Ping wird ausgeführt für 192.168.101.10 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 192.168.101.10:
    Pakete: Gesendet = 2, Empfangen = 0, Verloren = 2
    (100% Verlust),
STRG-C
PS C:\Users\pwyni> ping 192.168.102.10

Ping wird ausgeführt für 192.168.102.10 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 192.168.102.10:
    Pakete: Gesendet = 2, Empfangen = 0, Verloren = 2
    (100% Verlust),
```

Abbildung 50 Sicherheitsprüfungsnachweis 1

- **Benutzerrechte und Zugriffsprüfung**
  - **Ziel:** Sicherstellen, dass nur berechtigte Nutzer Zugriff haben.
  - **Vorgehen**:
    - Logge dich mit einem Administrator-Account ein und überprüfe die aktiven Benutzer und ihre Berechtigungen.
    - Falls keine weiteren Benutzer existieren → Sicherheit passt.
    - Falls weitere Benutzer existieren→ Berechtigungen anpassen.

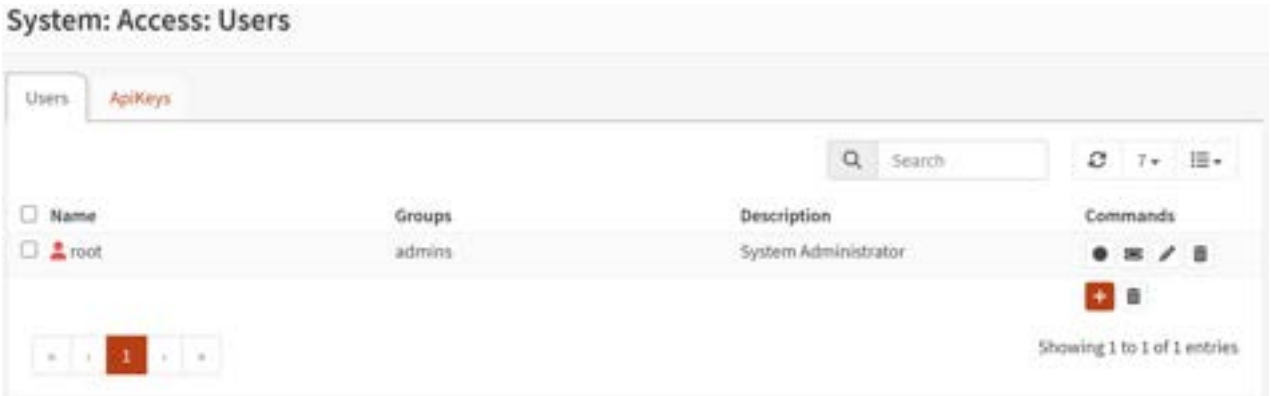


Abbildung 51 Sicherheitsprüfungsnachweis 2

- **Externer Port-Scan mit Online-Tools**
  - **Ziel:** Sicherstellen, dass nur notwendige Ports offen sind.
  - **Vorgehen:**
    - Gehe auf eine Website wie **portchecker.de** oder **Pentest-Tools** und führe einen Port-Scan deiner öffentlichen IP durch.
    - Falls nur benötigte Ports offen sind (z. B. für VPN 500, 4500) → Sicherheit ist gewährleistet.
    - Falls unerwartete Ports offen sind → Firewall-Regeln anpassen

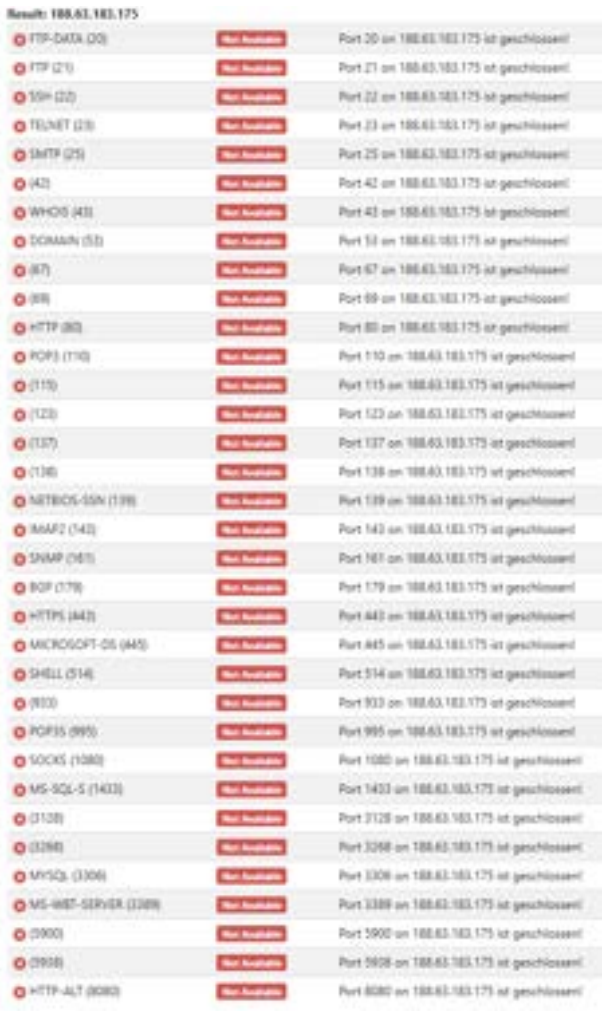


Abbildung 52 Sicherheitsprüfungsnachweis 3

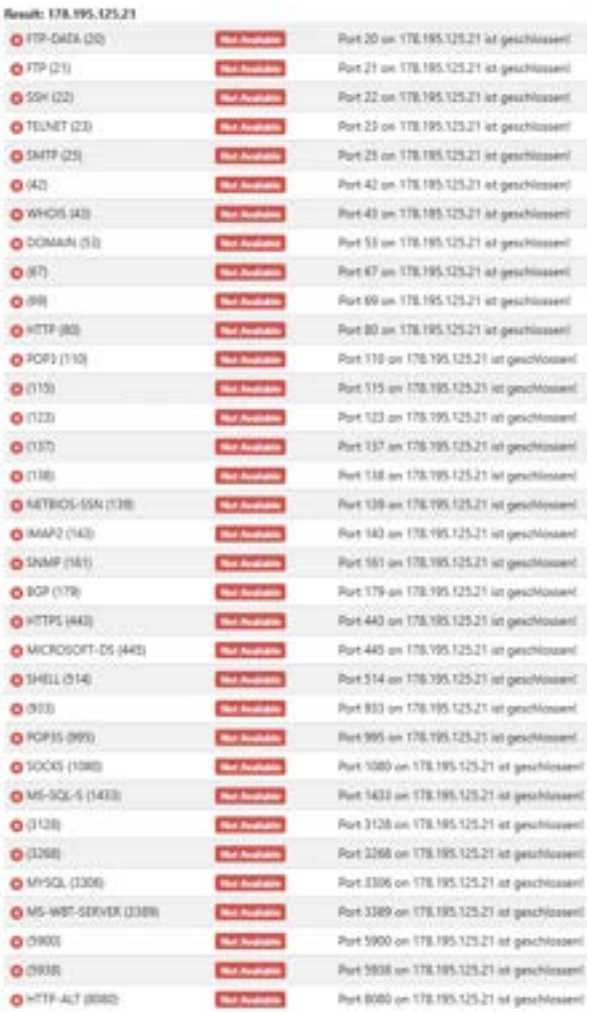


Abbildung 53 Sicherheitsprüfungsnachweis 4

14.1.5 Installation der benötigten OPNsense Plugins

Da OPNsense in der Grundversion kein BGP unterstützt, muss zunächst ein Plugin installiert werden.

1. Zum Plugin-Menü navigieren

- Öffne das OPNsense-Webinterface.
- Gehe zu **System > Firmware > Plugins**.

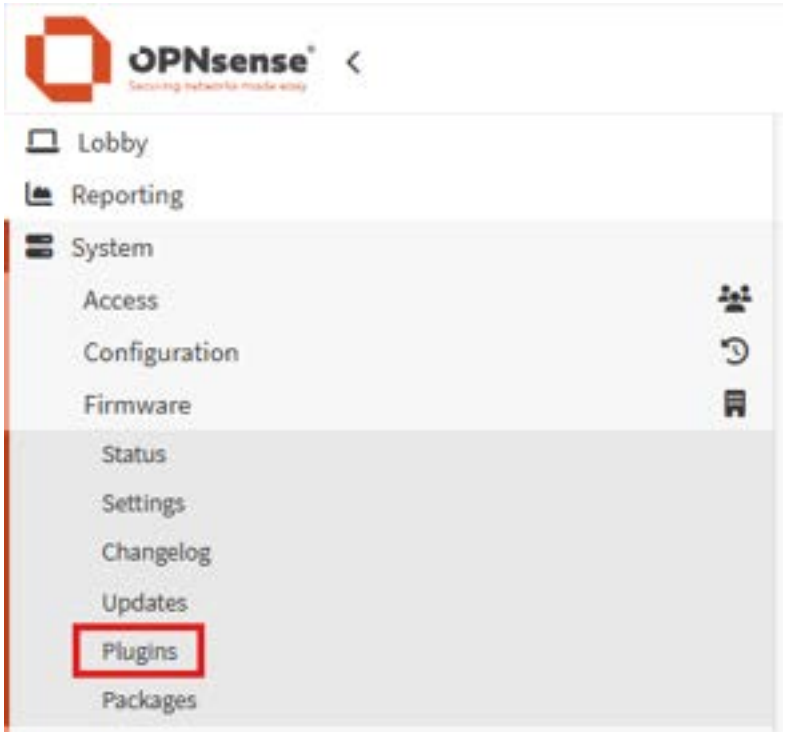


Abbildung 54 Zum Plugin-Menü navigieren

2. Plugin suchen

- Im Suchfeld os-frr eingeben, um das **FRR-Routing-Plugin** zu finden.

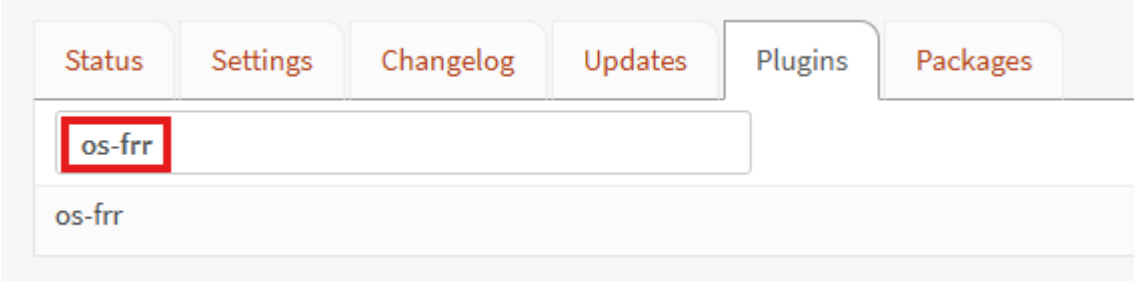


Abbildung 55 Plugin suchen

3. Plugin Installation starten

- Klicke auf das **«+»-Symbol**, um die Installation zu starten.
- Warte, bis die Installation abgeschlossen ist.

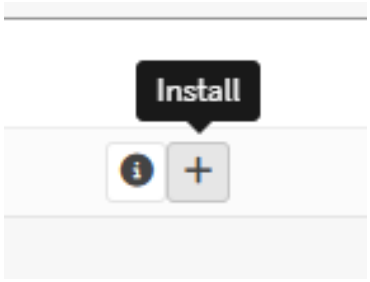


Abbildung 56 Plugin Installation starten

4. Routing-Menü aktivieren

- Nach der Installation erscheint der neue **Routing-Menüpunkt** im Hauptmenü.
- Enthält **RIP, OSPF, OSPFv3, BGP, BFD, STATIC** und **Diagnose-Tools**.



Abbildung 57 Routing-Menü aktivieren

14.1.6 High-Availability Setup der OPNsense-Instanzen

Damit die VPN-Verbindung hochverfügbar betrieben werden kann, muss zunächst ein neuer Virtual Switch auf dem VMware vSphere ESXi erstellt werden.

1. Neuen virtuellen Switch erstellen

- Navigiere in ESXi zu **Networking > Virtual switches**.
- Klicke auf **«Add standard virtual switch»**.
- Setze den Namen des Switches auf **opnsense_sync**.
- Stelle sicher, dass **Promiscuous Mode, MAC-Adressänderungen und Gefälschte Übertragungen auf «Accept»** gesetzt sind.
- Klicke auf **«Add»**.

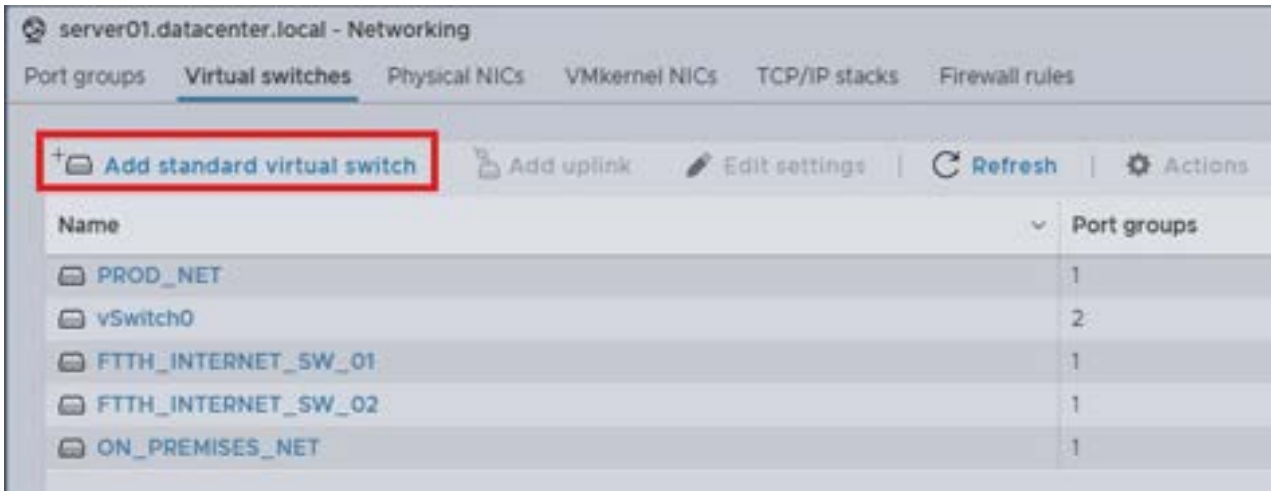


Abbildung 58 Neuen virtuellen Switch erstellen 1

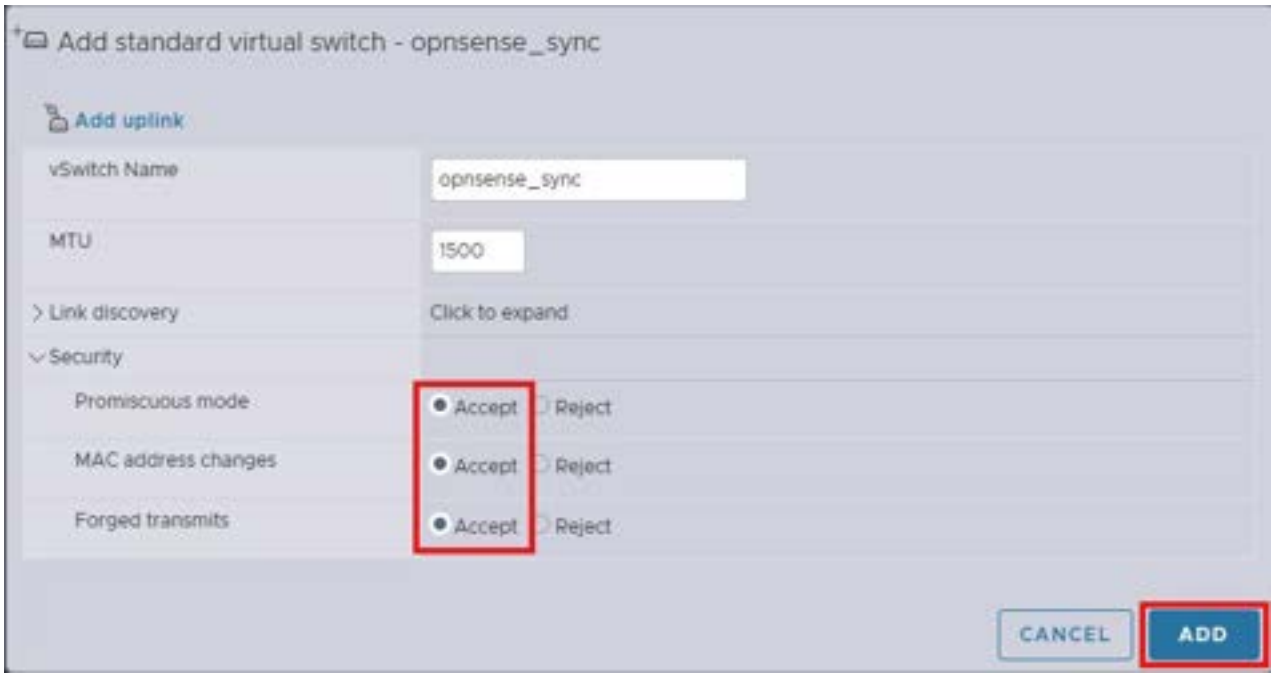


Abbildung 59 Neuen virtuellen Switch erstellen 2

2. Portgruppe für den Synchronisations-Switch erstellen

- Erstelle eine neue **Portgruppe** mit dem Namen **opnsense_sync_net**.
- Weise sie dem virtuellen Switch **opnsense_sync** zu.
- Klicke auf **«Add»**.

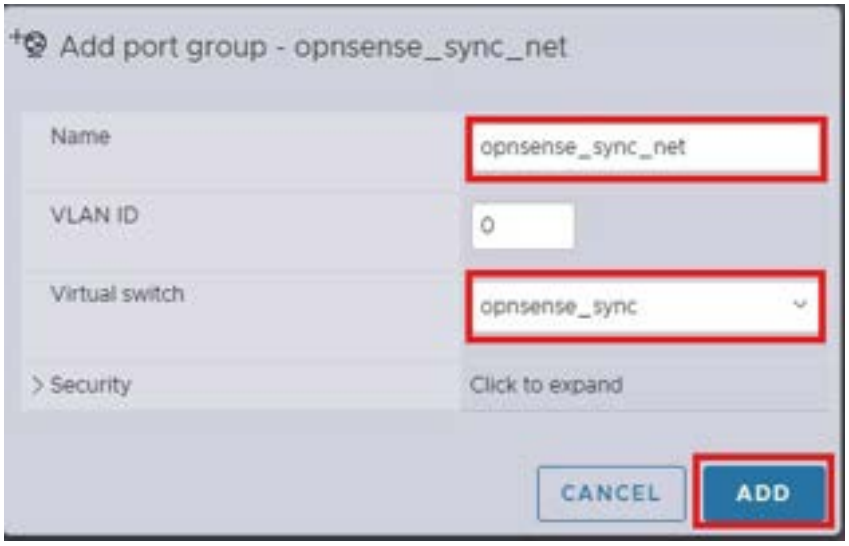


Abbildung 60 Portgruppe für den Synchronisations-Switch erstellen

3. Netzwerkadapter den OPNsense-VMs hinzufügen

- Öffne die **Einstellungen der OPNsense-VMs**.
- Klicke auf **«Add network adapter»** und wähle **opnsense_sync_net** als Netzwerk.
- Aktiviere **«Connect»** und speichere die Änderungen mit **«Save»**.
- Das wars mit der Konfiguration auf dem ESXi

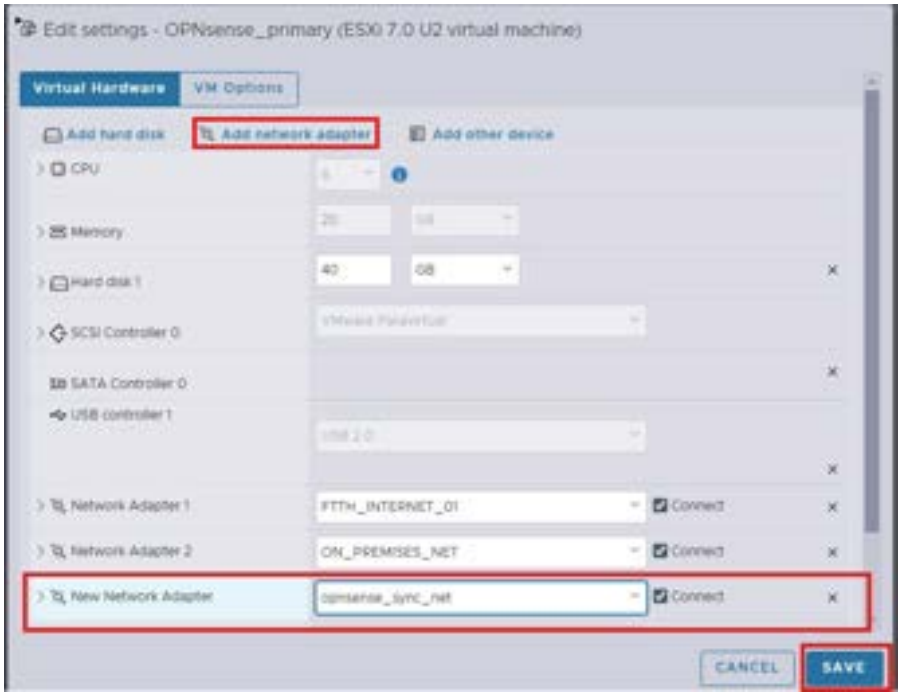


Abbildung 61 Netzwerkadapter den OPNsense-VMs hinzufügen

4. Interface in OPNsense zuweisen

- Im OPNsense-Webinterface navigiere zu **Interfaces > Assignments**.
- Füge das neue Interface **vmx2** hinzu und benenne es als **OPNSENSE_SYNC**.
- Klicke auf **«Add»** und dann **«Save»**.

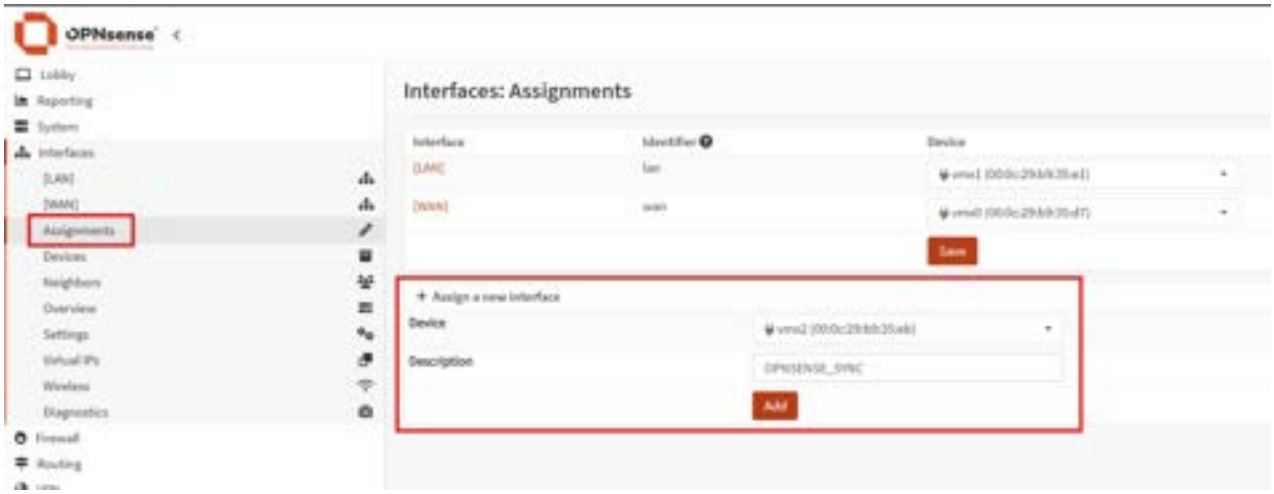


Abbildung 62 Interface in OPNsense zuweisen

5. Schnittstellenkonfiguration prüfen

- Nach der Zuweisung erscheint das Interface als **opt1**.
- Wenn es so aussieht, hat alles funktioniert



Abbildung 63 Schnittstellenkonfiguration prüfen

6. OPNsense Sync-Netzwerk konfigurieren

- **Interface aktivieren**: Gehe zu **Interfaces > OPNsense_SYNC**.
- Setze **«Enable Interface»** und wähle **Static IPv4**.
- Vergib die **IP-Adresse 172.16.1.1/30** auf der Primary-Instanz und die **IP-Adresse 172.16.1.2/30** auf der Secondary-Instanz
- Speichere die Änderungen.

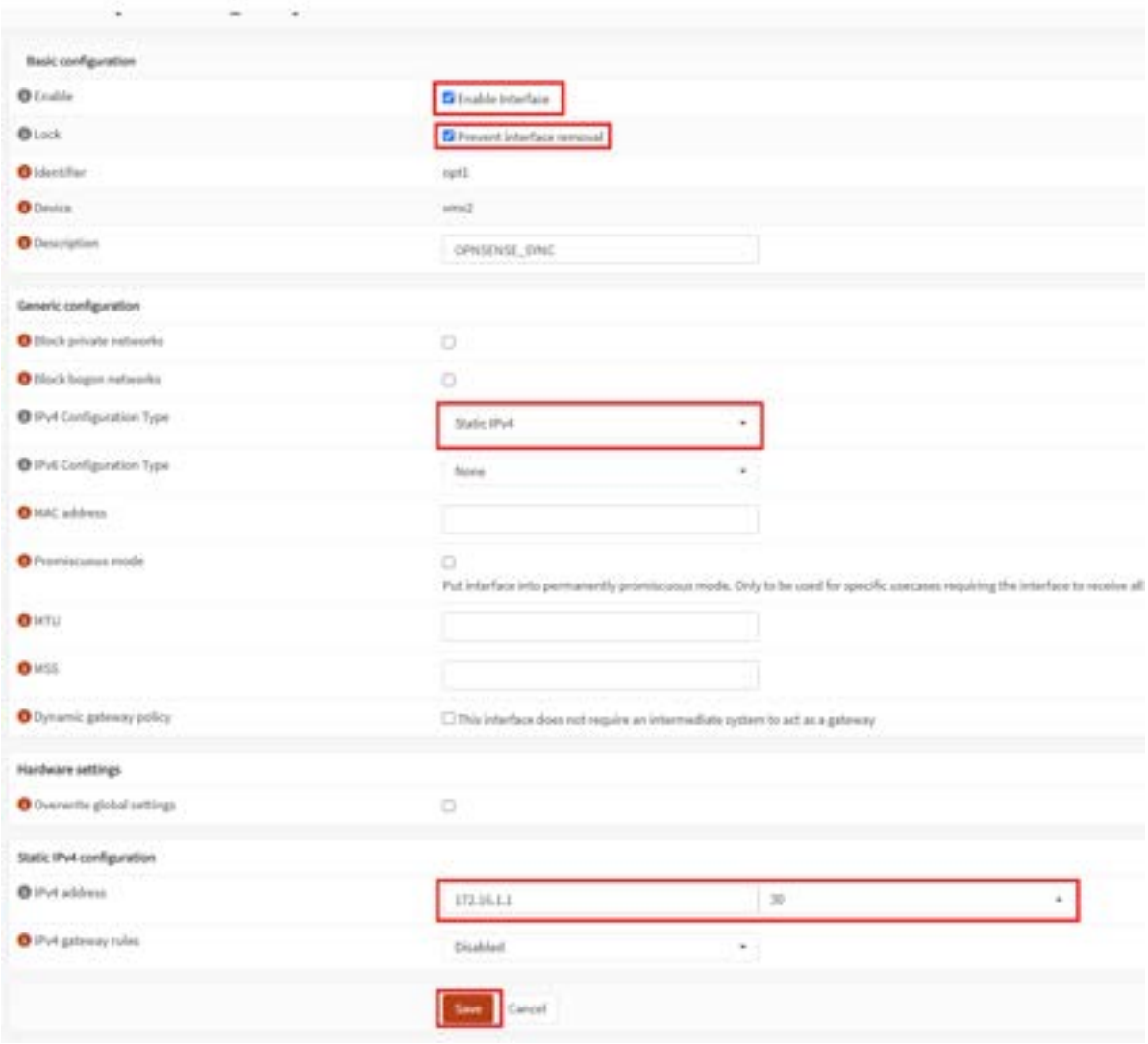


Abbildung 64 OPNsense Sync-Netzwerk konfigurieren

7. Firewall-Regeln für OPNsense Sync

- Gehe zu **Firewall > Rules > OPNsense_SYNC**.

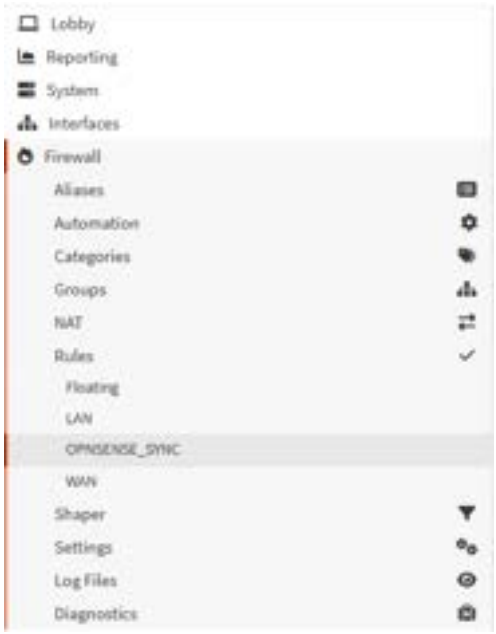


Abbildung 65 Firewall-Regeln für OPNsense Sync 1

- Erstelle eine Regel mit:
  - **Action**: Pass
  - **Interface**: OPNsense_SYNC
  - **TCP/IP Version**: IPv4
  - **Protocol**: Any
  - **Source**: Any
  - **Destination**: Any
- Speichere und übernehme die Regel.
- Erstelle diese Regel auf beiden OPNsense-Instanzen

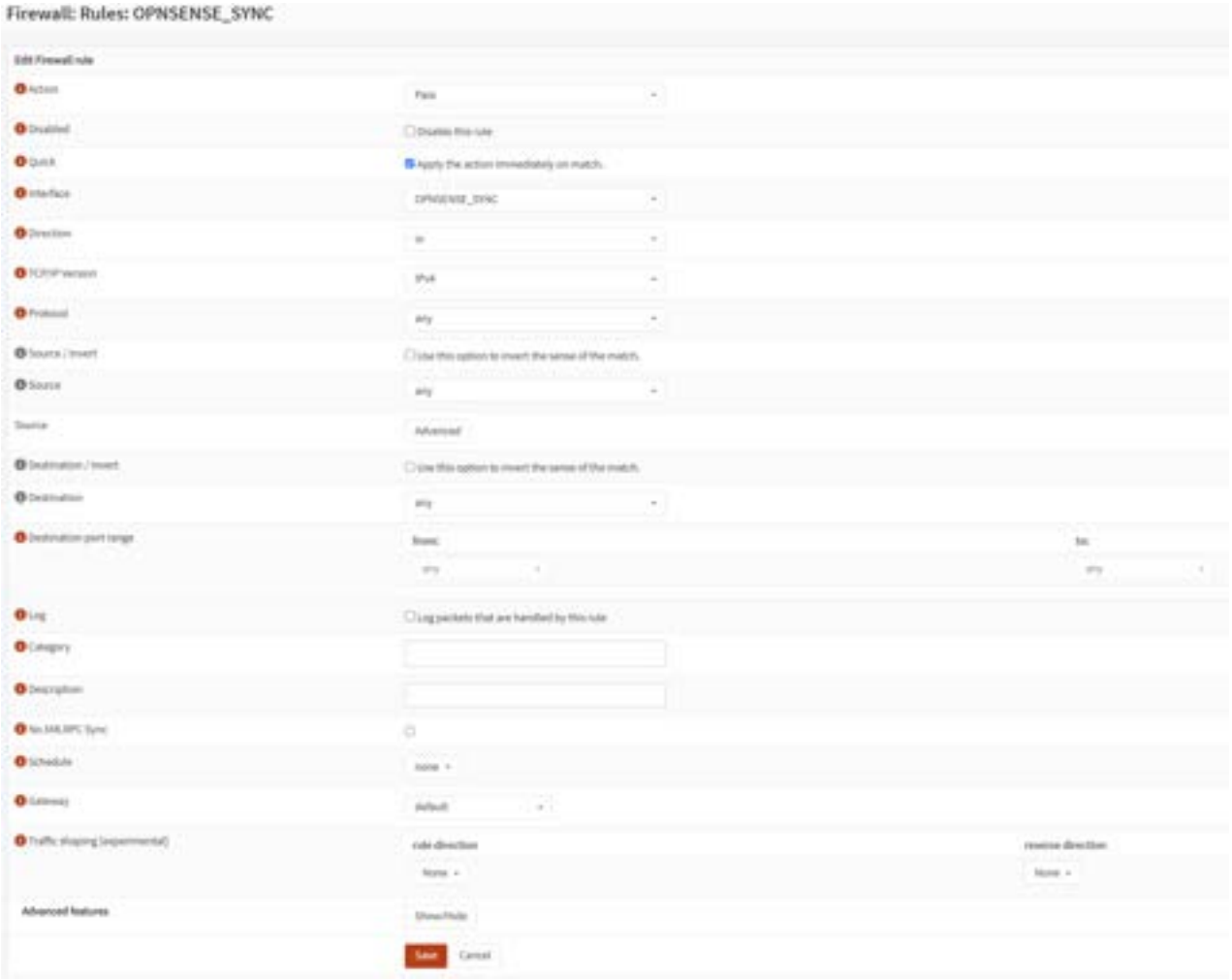


Abbildung 66 Firewall-Regeln für OPNsense Sync 2

8. Firewall-Regel überprüfen

- Pinge die **Peer-IP 172.16.1.2** im **Diagnostics > Ping** Menü.
- Wenn erfolgreich, ist die Verbindung zwischen den Firewalls bereit für die Hochverfügbarkeits-Konfiguration.



Abbildung 67 Firewall-Regel überprüfen

9. High Availability einrichten

- Navigiere zu **System > High Availability > Settings**.
- Setze **Synchronize all states via** auf **OPNsense_SYNC**.
- Trage die **Peer IP (172.16.1.2)** und **Anmeldedaten (root / Passwort)** ein.
- Wähle **Services zur Synchronisation**
  - DHCPD
  - Virtual IP
- Speichere die Konfiguration.

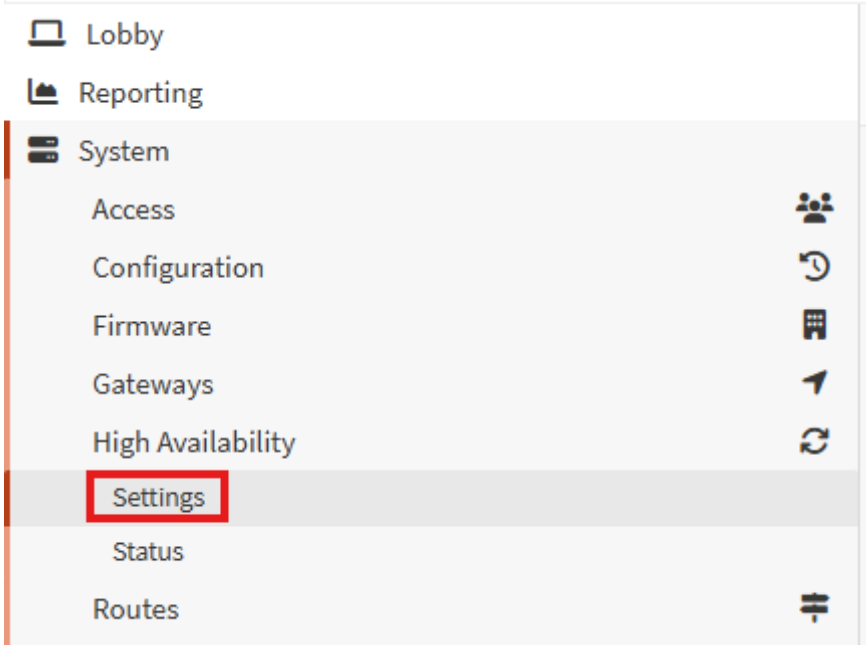


Abbildung 68 High Availability einrichten 1

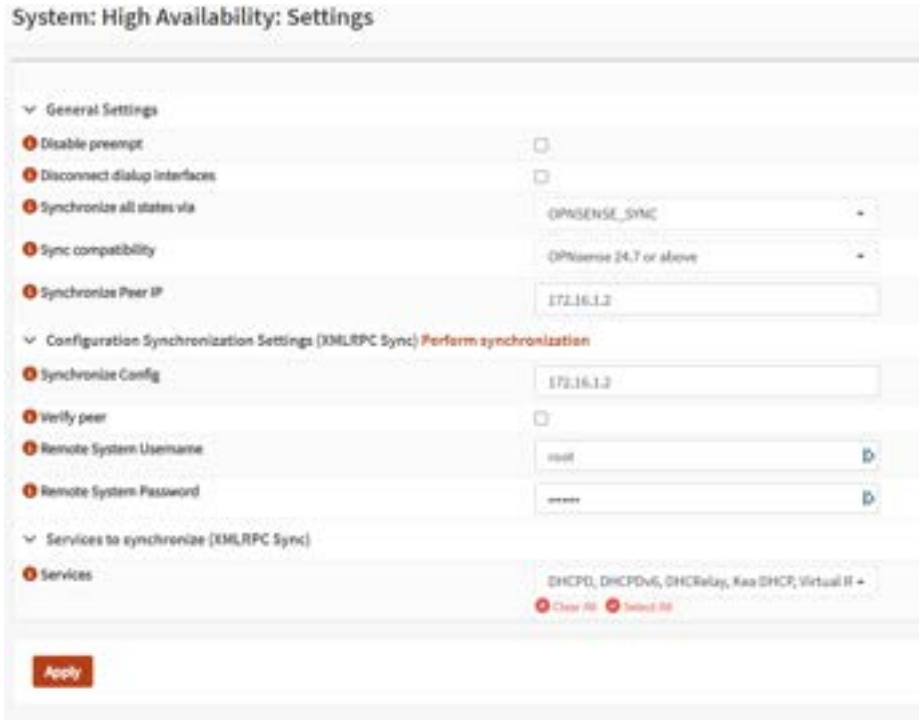


Abbildung 69 High Availability einrichten 2

Auf der Primary Instanz muss man nun die folgenden Konfigurationen vornehmen:

- **Synchronize all states via** → Stellt sicher, dass die Konfigurationen über das neu erstellte Sync-Interface synchronisiert werden
- **Synchronize Peer IP** → Definiert die IP wo die Konfiguration hin synchronisiert werden sollte
- **Synchronize Config** → Definiert die IP wo die Konfiguration hin synchronisiert werden sollte
- **Remote System Username** → Username der Secondary OPNsense Instanz
- **Remote System Password** → Passwort der Secondary OPNsense Instanz
- **Services** → Definiert welche Services synchronisiert werden sollen.

Wichtig: Diese Konfiguration muss man nur auf der Primary Instanz vornehmen.

10. Synchronisationsstatus prüfen

- Gehe zu **System > High Availability > Status**, um sicherzustellen, dass die Dienste synchronisiert werden.



Abbildung 70 Synchronisationsstatus prüfen

11. CARP Virtuelle IPs einrichten

- Gehe zu **Interfaces > Virtual IPs > Settings.**

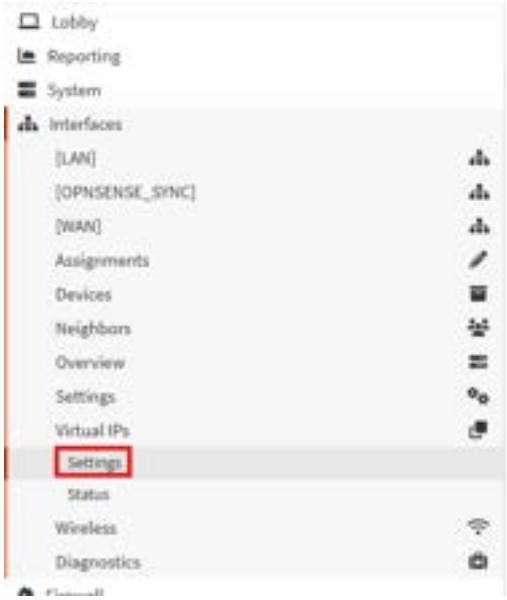


Abbildung 71 CARP Virtuelle IPs einrichten

- Erstelle eine neue virtuelle IP mit folgenden Parametern:
  - **Mode**: CARP
  - **Interface**: LAN
  - **Netzwerk/Adresse**: 10.1.0.1/16
  - **Peer (IPv4)**: Backup-Host (z. B. 10.1.0.3 für Master, 10.1.0.2 für Backup)
  - **VHID Group**: 1
  - **Advbase**: 1
  - **Advskew**: 0 (Primary), 100 (Secondary)
  - **Passwort** setzen.

OPNsense Primary:

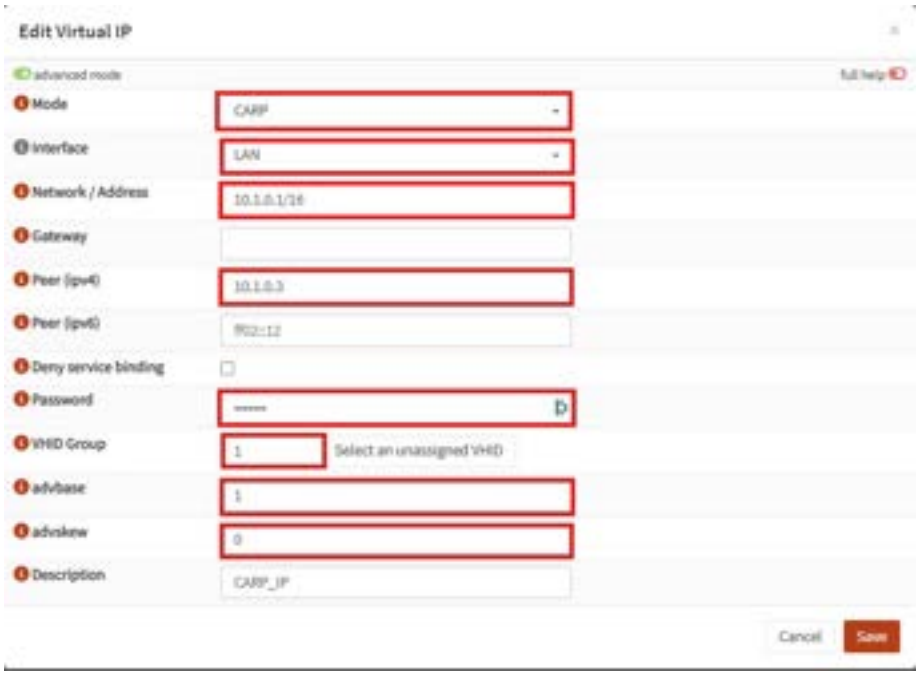


Abbildung 72 CARP Virtuelle IPs einrichten OPNsense Primary

OPNsense Secondary:

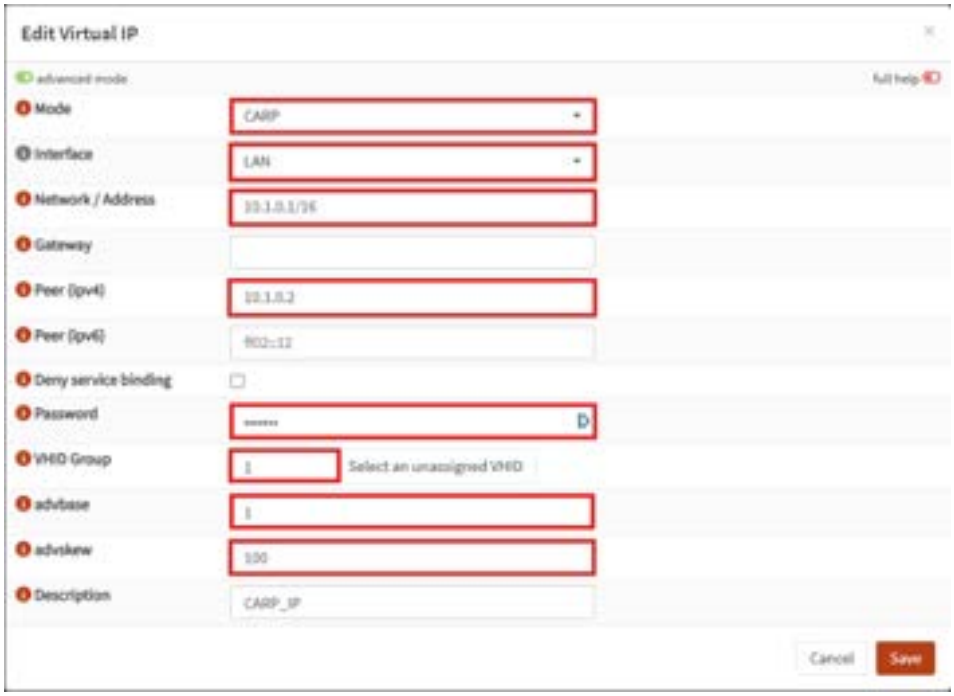


Abbildung 73 CARP Virtuelle IPs einrichten OPNsense Secondary

Diese Konfiguration muss auf beiden Instanzen gemacht werden.

12. Test der Failover-Funktion

- Auf der **Status Seite** kann man dann sehen, ob es funktioniert hat.
- Beim Primary sollte «**Master**» stehen.
- Beim Secondary sollte «**Backup**» stehen.
- Die IP: **10.1.0.1** sollte nun über den Browser erreichbar sein



Abbildung 74 Test der Failover-Funktion 1



Abbildung 75 Test der Failover-Funktion 2

Wenn das alles funktioniert hat, ist **CARP** erfolgreich eingerichtet.

14.2 AWS-Umgebung aufbauen

In diesem Kapitel wird die AWS-Umgebung Schritt für Schritt aufgebaut.

14.2.1 Erstellung der AWS VPC

Als erstes muss man das VPC im AWS Account erstellen. Dafür muss man zunächst in die VPC Konsole in der Region eu-central-1 navigieren.

1. Navigiere zu AWS VPC Dashboard

- Gehe zur AWS-Konsole und öffne das **VPC Dashboard**.
- Klicke auf **«Create VPC»**.



Abbildung 76 Navigiere zu AWS VPC Dashboard

2. VPC-Einstellungen konfigurieren

- **Name:** AWS-VPC
- **IPv4 CIDR:** 10.100.0.0/16
- **IPv6 CIDR:** Keine IPv6-Unterstützung
- **Tenancy:** Standard (Default)
- Klicke auf **«Create VPC»**.

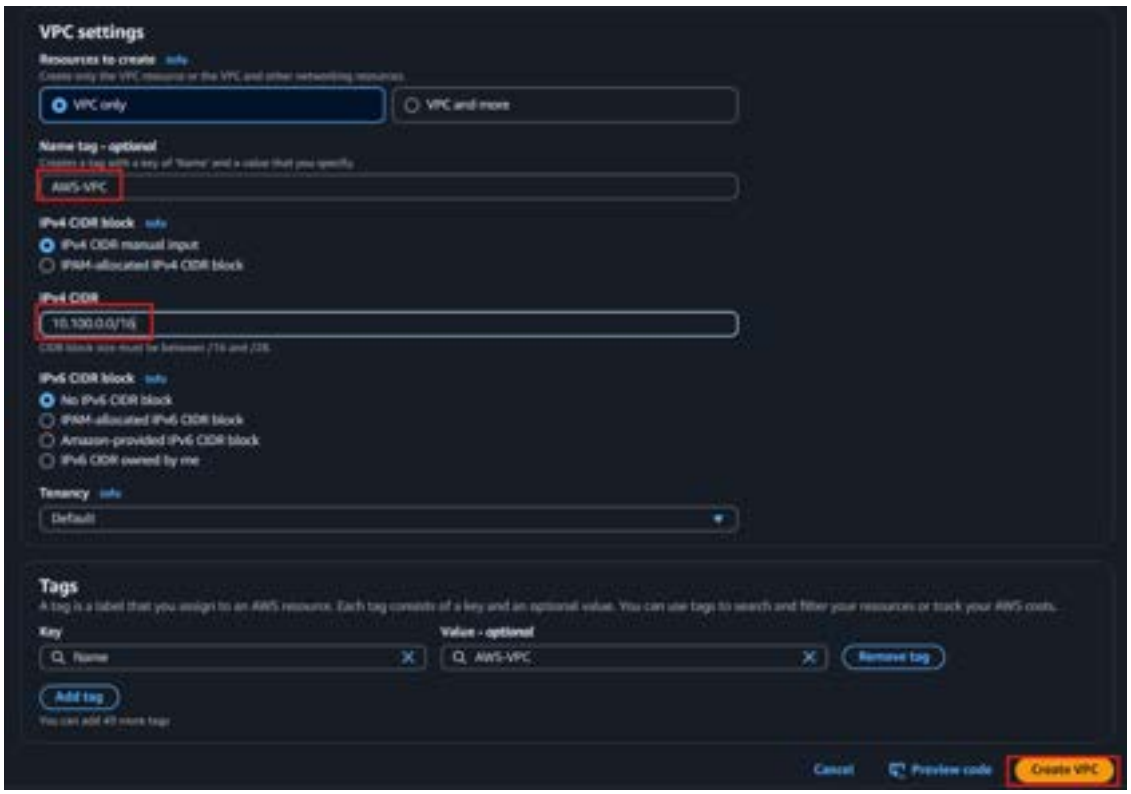


Abbildung 77 VPC-Einstellungen konfigurieren

14.2.2 Erstellung der Subnetze in der VPC

Nachdem man die VPC erstellt hat, kann man nun die Subnetze erstellen.

1. Subnetz A (eu-central-1a)

- **Subnetzname:** AWS-SUBNET-A
- **Availability Zone:** eu-central-1a
- **CIDR:** 10.100.10.0/24
- Klicke auf **«Create subnet»**.



Abbildung 78 Subnetz A (eu-central-1a)

2. Subnetz B (eu-central-1b)

- **Subnetzname:** AWS-SUBNET-B
- **Availability Zone:** eu-central-1b
- **CIDR:** 10.100.20.0/24
- Klicke auf **«Create subnet»**.

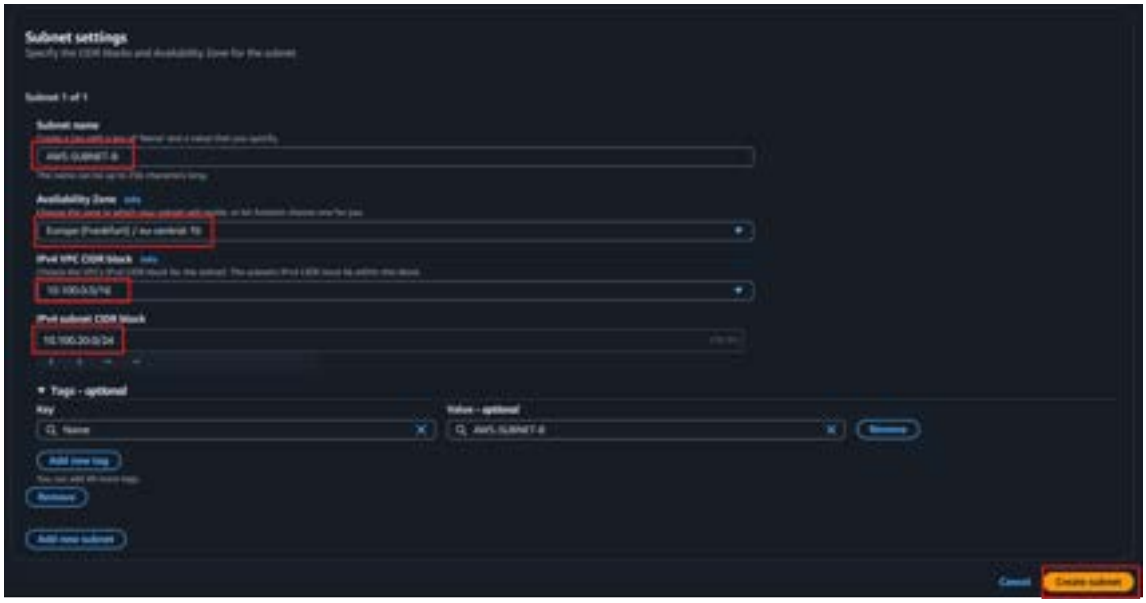


Abbildung 79 Subnetz B (eu-central-1b)

3. Subnetz C (eu-central-1c)

- **Subnetzname:** AWS-SUBNET-C
- **Availability Zone:** eu-central-1c
- **CIDR:** 10.100.30.0/24
- Klicke auf **«Create subnet»**.

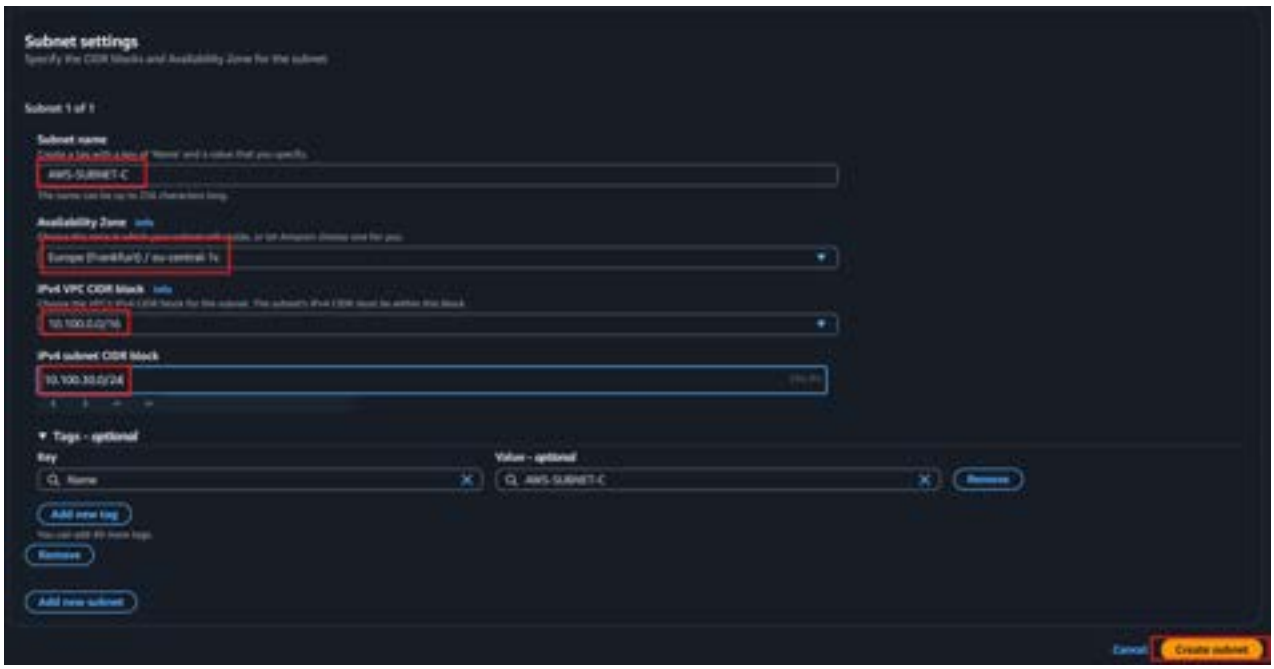


Abbildung 80 Subnetz C (eu-central-1c)

4. Subnetz Konfiguration überprüfen

- **Ergebnis:** Alle Subnetze sollten im VPC-Dashboard mit Status «Available» erscheinen.



Abbildung 81 Subnetz Konfiguration überprüfen

14.2.3 Erstellung der Route Tables

Um ein Hochverfügbares Netzwerk in AWS sicherstellen zu können, braucht es ein dediziertes Route Table für jedes Subnetz.

1. Navigiere zu Route Tables

- Gehe zu **«Route tables»** im VPC-Dashboard.
- Klicke auf **«Create route table»**.



Abbildung 82 Navigiere zu Route Tables

2. Route Table erstellen

- **Name:** AWS-SUBNET-A-RT / AWS-SUBNET-B-RT / AWS-SUBNET-C-RT
- **VPC:** Wähle AWS-VPC
- Klicke auf **«Create route table»**



Abbildung 83 Route Table erstellen

3. Routing-Tabelle mit Subnetzen verbinden

- Öffne die erstellte Routing-Tabelle.
- Gehe zum Tab **«Subnet associations»**.
- Klicke auf **«Edit subnet associations»**.
- Wähle das entsprechende Subnetz aus und speichere die Änderungen.

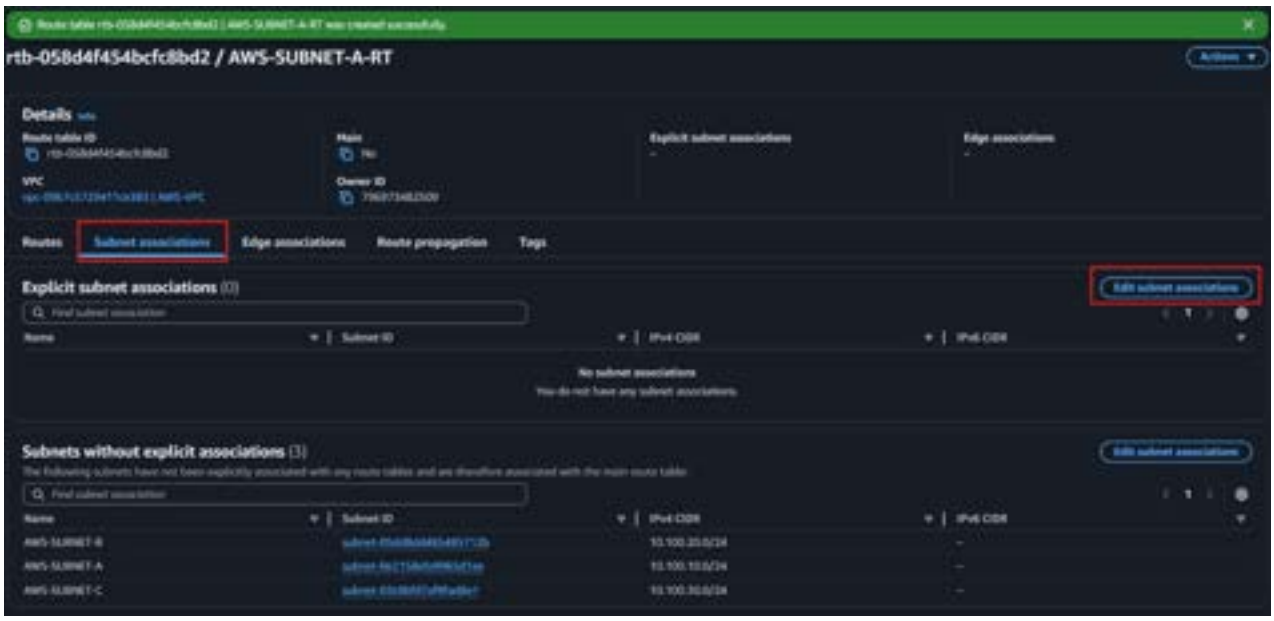


Abbildung 84 Routing-Tabelle mit Subnetzen verbinden 1



Abbildung 85 Routing-Tabelle mit Subnetzen verbinden 2

Diese Schritte muss man dann noch für die anderen beiden Routing-Tabellen wiederholen.

4. Konfiguration überprüfen

- Die neue erstellen Routing-Tabellen sollten nun alle mit dem entsprechenden Subnetz verbunden sein



Abbildung 86 Konfiguration überprüfen

14.2.4 Definition der AWS Customer Gateways

In diesem Teil erstellt man die AWS Customer Gateways. Diese Customer Gateways dienen als Ressourcen Definition des On-Premises Teils der Infrastruktur.

1. Navigiere zu Customer Gateways

- Gehe zu **«Customer Gateways»** im VPC-Dashboard unter «**Virtual private network (VPN)**»



Abbildung 87 Navigiere zu Customer Gateways

2. Erstellen des Primären Customer Gateways

Das nachfolgende Bild zeigt die Eingabemaske für das Erstellen eines **Customer Gateways**.
Fülle folgende Felder aus:

- **Name tag**: on-premises-opnsense-primary-cgw
- **BGP ASN**: 65001 (Wert für AS-Nummer des Customer Gateways)
- **P-Adresse**: 188.63.183.175 (externe IP der primären OPNsense-Firewall)
- **Device** (optional): opnsense-primary
- Klicke auf **Create customer gateway**.

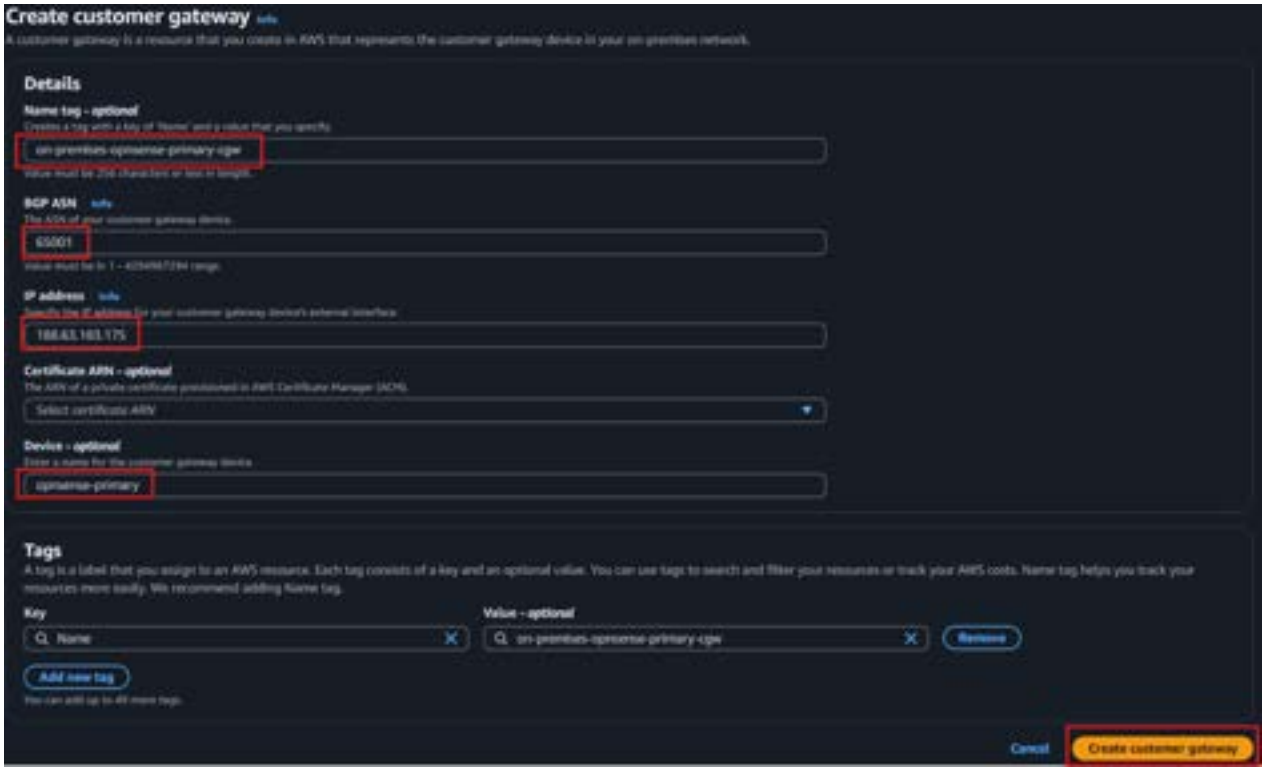


Abbildung 88 Erstellen des Primären Customer Gateways

3. Erstellen des Sekundären Customer Gateways

Das dritte Bild zeigt die Erstellung des **sekundären Customer Gateways**.
Fülle folgende Werte aus:

- **Name tag**: on-premises-opnsense-secondary-cgw
- **BGP ASN**: 65001
- **IP-Adresse**: 178.195.125.21 (externe IP der sekundären OPNsense-Firewall)
- **Device** (optional): opnsense-secondary
- Klicke auf **Create customer gateway**.

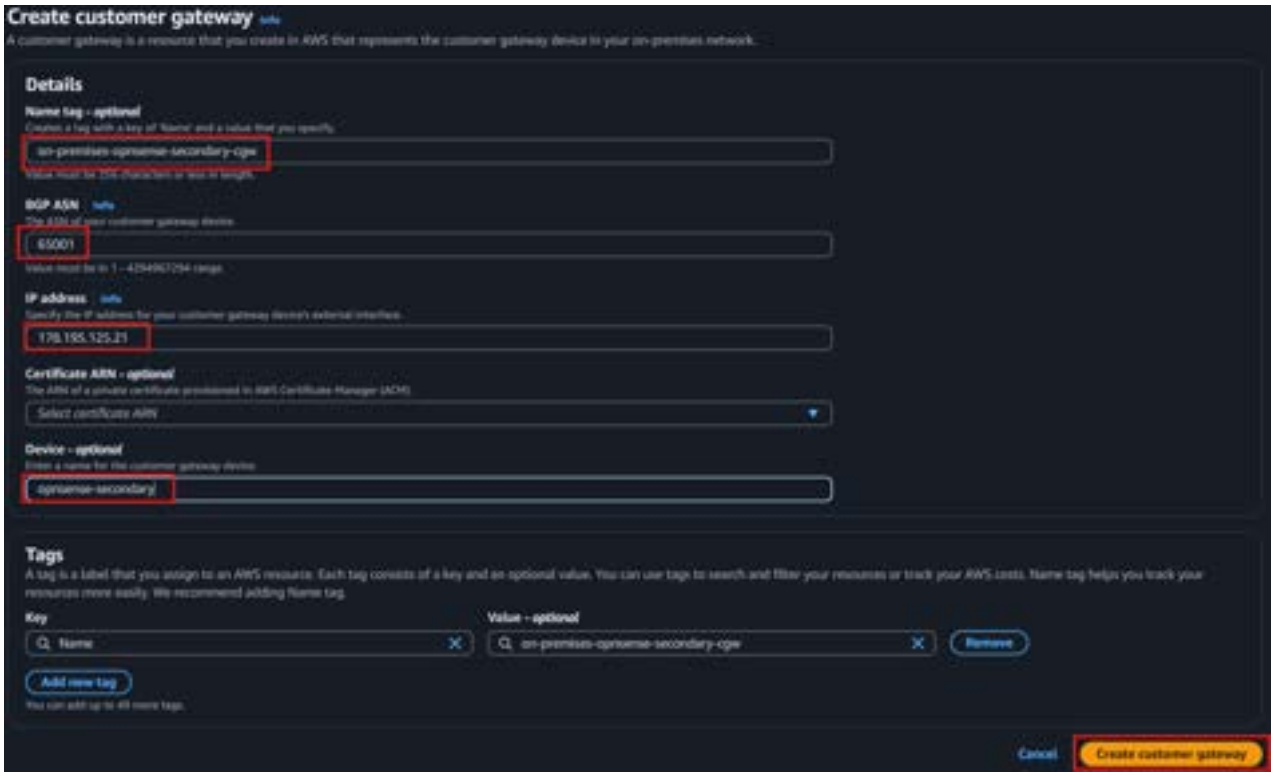


Abbildung 89 Erstellen des Sekundären Customer Gateways

4. Konfiguration überprüfen

- Die neu erstellten Customer Gateways sollten nun in etwa so aussehen



Abbildung 90 Konfiguration überprüfen

14.2.5 Erstellung des AWS Transit Gateways

In diesem Kapitel wird beschrieben wie man den Transit Gateway erstellt.

1. Navigiere zu AWS Transit Gateway

- Gehe zu **«Transit Gateways»** im VPC-Dashboard unter «**Transit gateways**



Abbildung 91 Navigiere zu AWS Transit Gateway

2. Transit Gateway erstellen

- Klicke auf **Create Transit Gateway**.
- **Name tag**: aws-transit-gw (Optional, aber nützlich für eine bessere Übersicht)
- **Amazon side Autonomous System Number (ASN)**: 64512 (Dies ist eine private ASN, die für BGP-Routing verwendet werden kann.)
- **Optionen aktivieren**:
  - **DNS Support** → Erlaubt die Namensauflösung zwischen VPCs.
  - **Security Group Referencing Support** → Erlaubt Sicherheitsgruppen zwischen VPCs.
  - **VPN ECMP Support** → Ermöglicht gleichzeitige Nutzung mehrerer VPN-Verbindungen
  - **Default Route Table Association** → Standard-Routentabelle für verbundene VPCs.
  - **Default Route Table Propagation** → Automatische Weitergabe von Routing-Informationen.
- **Cross-Account-Sharing Optionen konfigurieren**
  - **Auto accept shared attachments**
- Klicke auf «**Transit Gateway erstellen»**

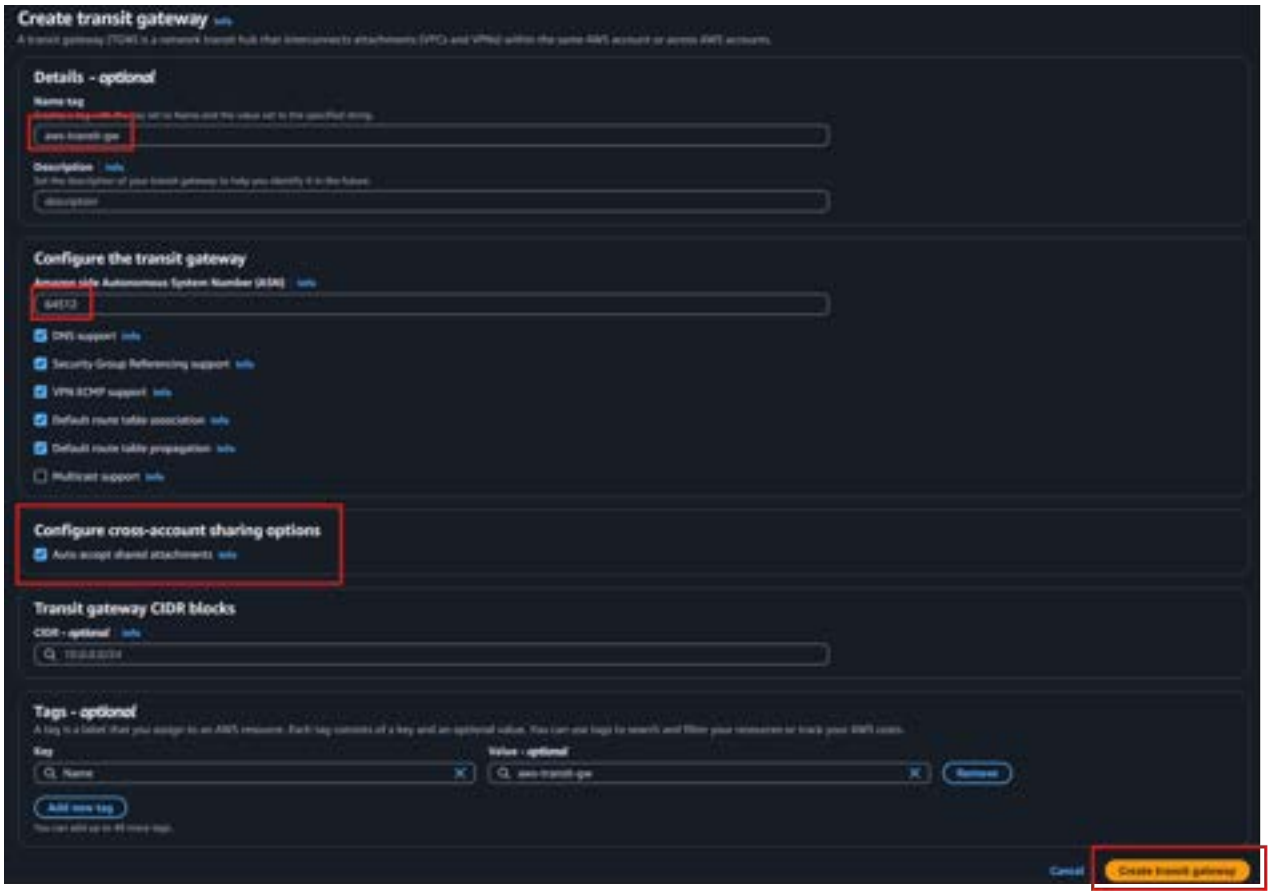


Abbildung 92 Transit Gateway erstellen

3. Konfiguration überprüfen

- Transit Gateway State «**Available**» sollte im Dashboard ersichtlich sein.



Abbildung 93 Konfiguration überprüfen

14.2.6 Erstellung der AWS Transit Gateway Attachments

1. Gehe zur AWS Transit Gateway Konsole

- Öffne die **VPC-Konsole** in AWS.
- Wähle **Transit Gateway Attachments** aus dem Menü.

2. Transit Gateway Attachment erstellen

- Klicke auf **Create Transit Gateway Attachment**.

3. Details für das Attachment eingeben

- **Name tag**: aws-transit-gw-subnets-attachment (Optional, aber hilfreich für eine bessere Übersicht)
- **Transit Gateway ID**: (Das Transit Gateway, mit dem die VPC verbunden wird.)
- **ttachment type**: VPC
  (Da es sich um eine Verbindung zwischen VPC und TGW handelt.)

4. VPC Attachment konfigurieren

- **VPC ID**: (Die VPC, die mit dem Transit Gateway verbunden wird.)
- **Subnet IDs**:
  - **eu-central-1a**
  - **eu-central-1b**
  - **eu-central-1c**
- **Optionen aktivieren:**
  - **DNS Support** → Erlaubt DNS-Auflösung zwischen VPCs
  - **Security Group Referencing Support** → Ermöglicht den Zugriff auf Sicherheitsgruppen zwischen VPCs.

5. Transit Gateway Attachment erstellen

- Klicke auf **Create transit gateway attachment**, um die Verbindung bereitzustellen.

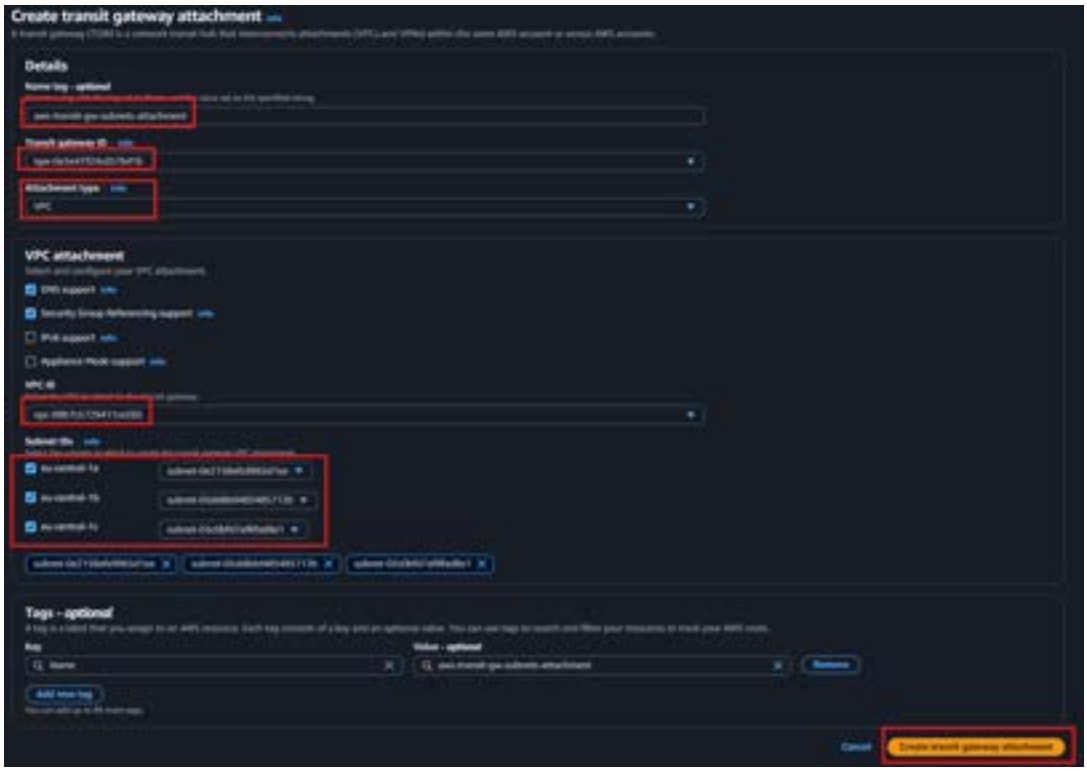


Abbildung 94 Transit Gateway Attachment erstellen

6. Konfiguration überprüfen

- Transit Gateway Attachment State «**Available**» sollte im Dashboard ersichtlich sein.



Abbildung 95 Konfiguration überprüfen

14.2.7 Subnetz-Routing zu Transit Gateway konfigurieren

In diesem Kapitel wird beschrieben, wie man die Routing Tabellen erstellt, welche routing zum Transit Gateway ermöglichen.

1. Navigiere zu Route Tables

- Gehe zu **«Route tables»** im VPC-Dashboard.
- Klicke auf **«Create route table»**.



Abbildung 96 Navigiere zu Route Tables

2. Routen bearbeiten

- Wähle eine nach der anderen der drei Routen aus
  - **AWS-SUBNET-A-RT**
  - **AWS-SUBNET-B-RT**
  - **AWS-SUBNET-C-RT**
- Klicke auf **«Routes»**
- Danach auf **«Edit Routes»**

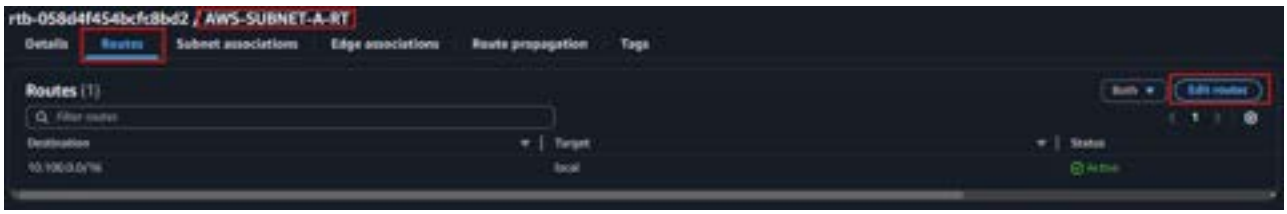


Abbildung 97 Routen bearbeiten 1

- Füge auf jedem der drei Route Tables diese Route hinzu
  - **0.0.0.0/0 → Transit Gateway**
- Klicke **«Save Changes»**

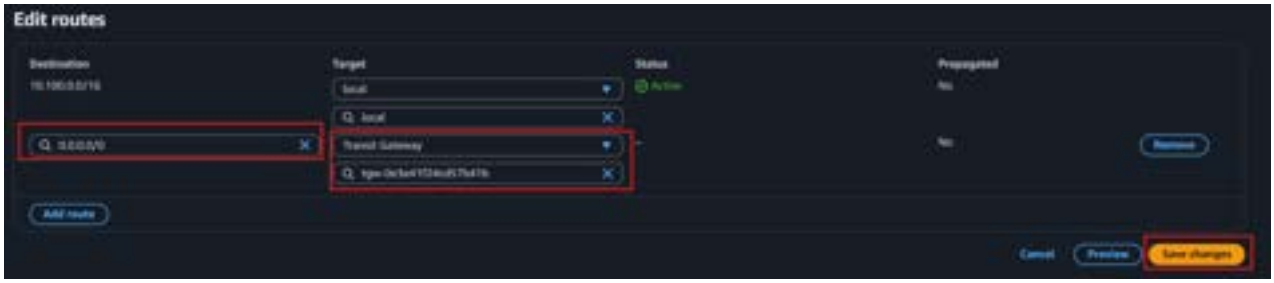


Abbildung 98 Routen bearbeiten 2

3. Konfiguration überprüfen

- Die Routen sollten für alle Route-Tables folgendermassen aussehen.



Abbildung 99 Routen Konfiguration überprüfen

14.2.8 Erstellung der beiden AWS Site-to-Site VPN Verbindungen

In diesem Kapitel wird beschrieben, wie man die AWS Site-to-Site VPN-Verbindungen erstellt.

1. Navigiere zu Site-to-Site VPN Connections

- Gehe zu **«Site-to-Site VPN connections»** im VPC-Dashboard unter «**Virtual private network (VPN)**»

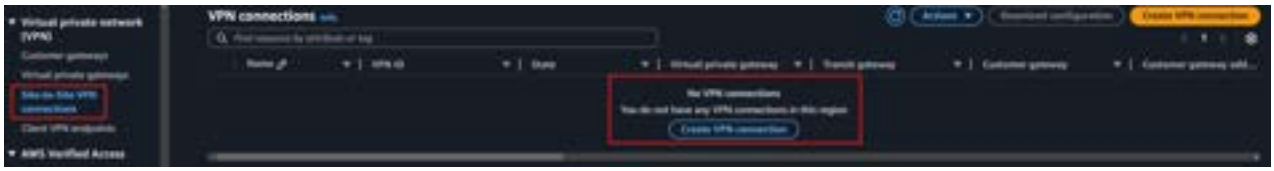


Abbildung 100 Navigiere zu Site-to-Site VPN Connections

2. Erstellen der primären Site-to-Site VPN Verbindung

Das nachfolgende Bild zeigt die Eingabemaske für das Erstellen einer AWS Site-to-Site VPN Verbindung. Fülle folgende Felder aus:

- **Name tag:** vpn-connection-1
- **Target gateway type:** Transit Gateway
- **Customer Gateway:** Wähle den Primary Customer Gateway aus
- **Routing Options:** Dynamic (BGP)
- **Tunnel inside IP version:** IPv4
- **Local IPv4 network CIDR:** 0.0.0.0/0
- **Remote IPv4 network CIDR:** 0.0.0.0/0
- **Outside IP address type:** Publicpv4
- Klicke auf «**Create VPN connection»**

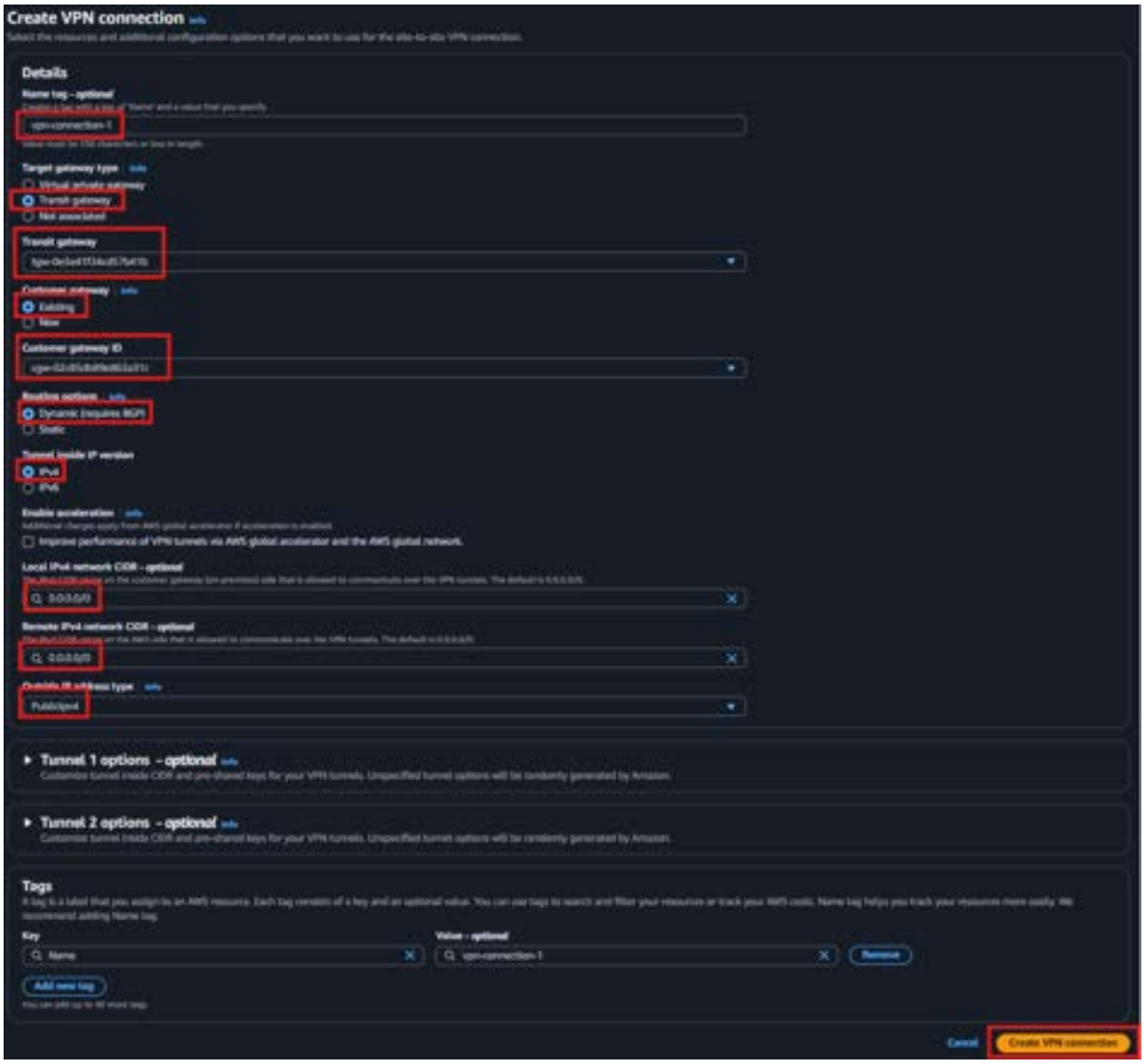


Abbildung 101 Erstellen der primären Site-to-Site VPN Verbindung

3. Erstellen der sekundären Site-to-Site VPN Verbindung

Das nachfolgende Bild zeigt die Eingabemaske für das Erstellen einer AWS Site-to-Site VPN Verbindung. Fülle folgende Felder aus:

- **Name tag:** vpn-connection-2
- **Target gateway type:** Transit Gateway
- **Customer Gateway:** Wähle den Secondary Customer Gateway aus
- **Routing Options:** Dynamic (BGP)
- **Tunnel inside IP version:** IPv4
- **Local IPv4 network CIDR:** 0.0.0.0/0
- **Remote IPv4 network CIDR:** 0.0.0.0/0
- **Outside IP address type:** Publicpv4
- Klicke auf «**Create VPN connection**»

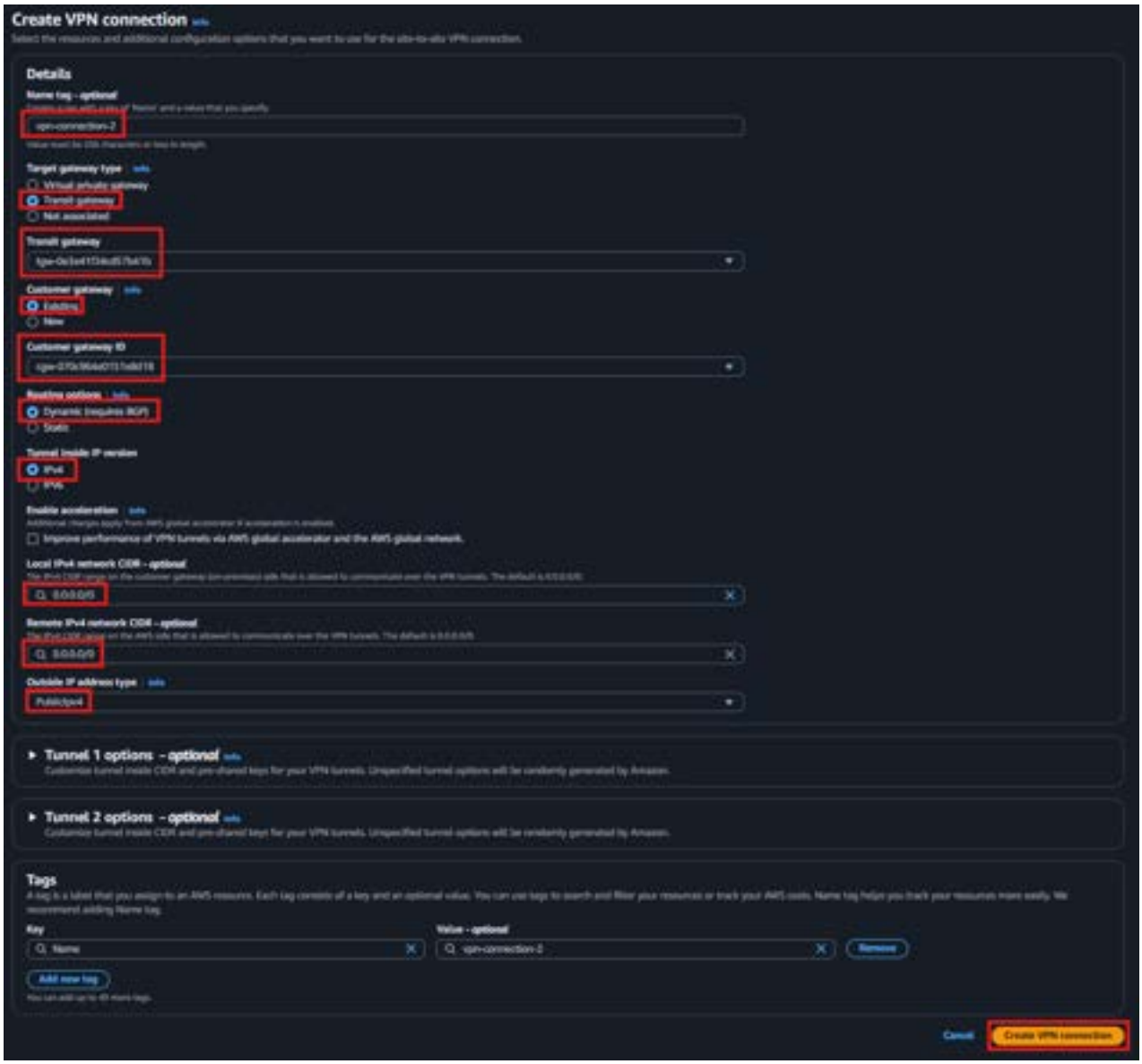


Abbildung 102 Erstellen der sekundären Site-to-Site VPN Verbindung

14.3 Konfiguration der VPN Verbindung zwischen On-Premises und AWS

Diese Anleitung beschreibt die Konfiguration einer Site-to-Site-VPN-Verbindung zwischen einer On-Premises-Umgebung (OPNsense) und AWS unter Verwendung von IPSec-VPN mit IKEv2.

14.3.1 VPN-Konfigurationsdateien herunterladen

1. Navigiere zu Site-to-Site VPN Connections

- Gehe zu **«Site-to-Site VPN connections»** im VPC-Dashboard unter «**Virtual private network (VPN)**»

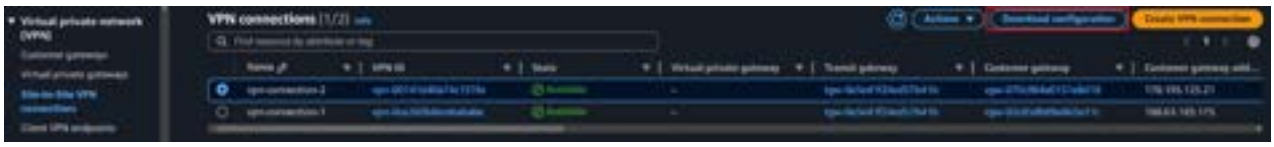


Abbildung 103 Navigiere zu Site-to-Site VPN Connections

2. VPN-Konfigurationsdateien herunterladen

- Wähle eine Verbindung nach der anderen aus und klicke auf **«Download Configuration»**
- Im daraufhin erscheinenden Fenster konfiguriere folgende Optionen:
  - **Vendor**: Generic
  - **Platform**: Generic
  - **Software**: Vendor Agnostic
  - **IKE-Version**: ikev2
- Klicke auf **Download**, um die VPN-Konfigurationsdatei herunterzuladen.

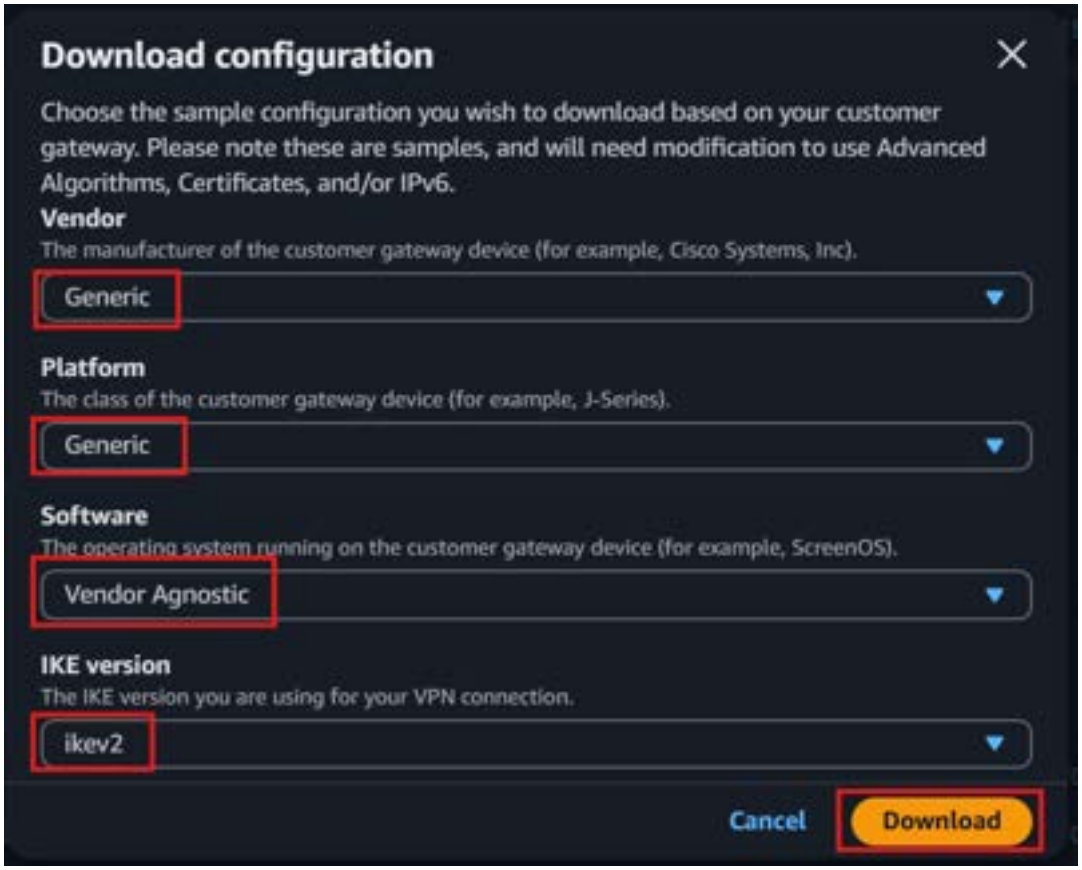


Abbildung 104 VPN-Konfigurationsdateien herunterladen

14.3.2 VPN-Verbindung 1 konfigurieren

In diesem Abschnitt werden die Site-to-Site VPN Tunnels auf der Primary OPNsense Instanz eingerichtet.

1. VPN-Tunnel-Eintrag erstellen

- Navigiere in der OPNsense Web-GUI zu **VPN > IPsec > Tunnel Settings (legacy)**.
- Klicke auf das **Plus-Symbol** in der Sektion «Phase 1», um eine neue VPN-Verbindung hinzuzufügen.

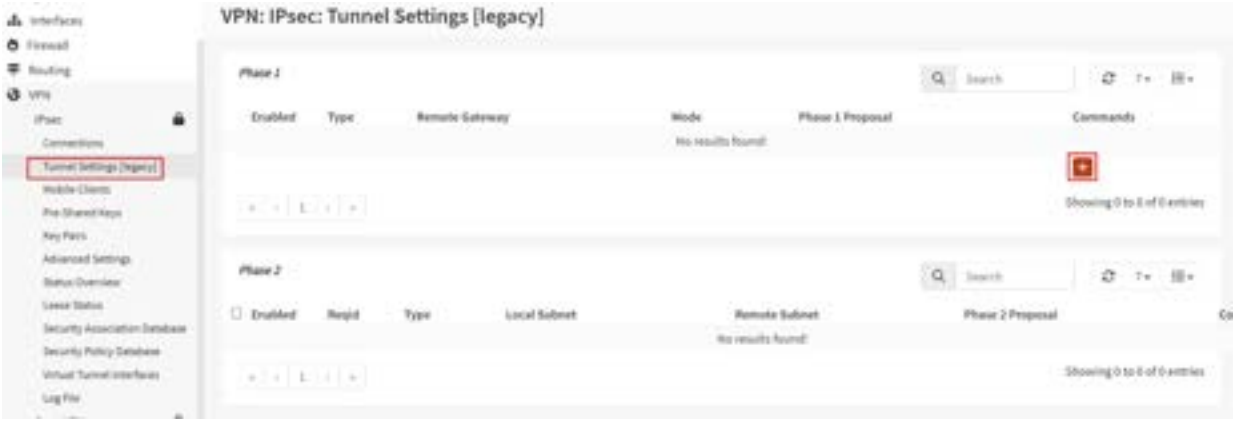


Abbildung 105 VPN-Tunnel-Eintrag erstellen

2. Tunnel 1 Phase 1 Konfigurieren

- **Connection method:** Start immediate
- **Key Exchange version:** V2
- **Internet Protocol:** IPv4
- **Remote Gateway:** Trage die externe IP-Adresse des AWS VPN-Endpunkts ein
- **Description:** vpn-connection-1-tunnel-1
- **Authentication method:** Mutual PSK
- **Pre-Shared Key:** Kopiere den von AWS bereitgestellten **Pre-Shared Key**.
- **Encryption algorithm:** AES 256
- **Hash algorithm:** SHA256
- **DH key group:** 24 (2048 bits)
- **Dead Peer Detection:** Aktivieren und folgende Werte setzen:
  - 10 seconds
  - 3 retries
  - Default
- Klicke auf **Save**, um die Phase 1 Einstellungen zu speichern.

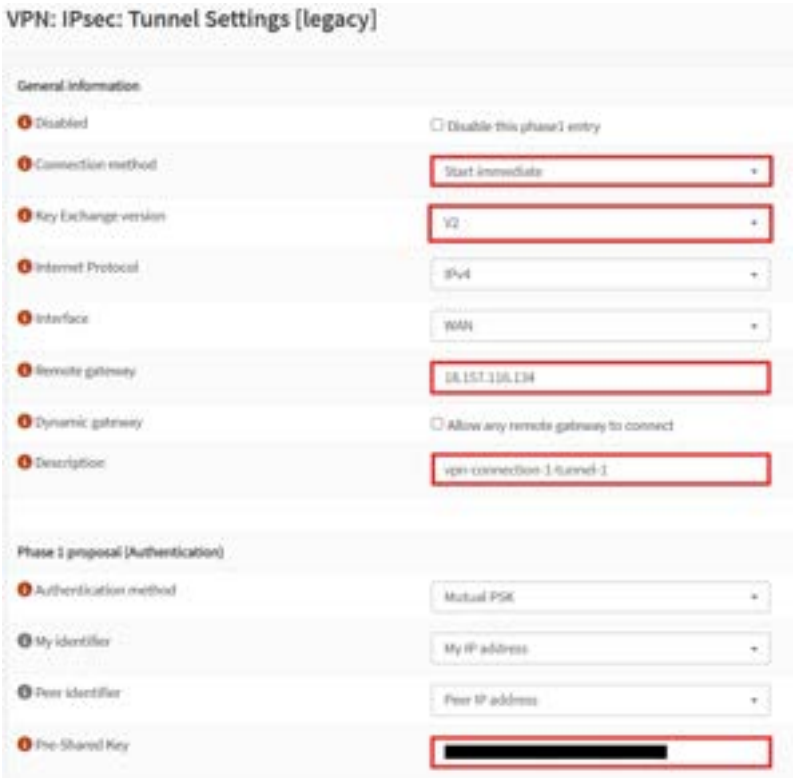


Abbildung 106 Tunnel 1 Phase 1 Konfigurieren 1

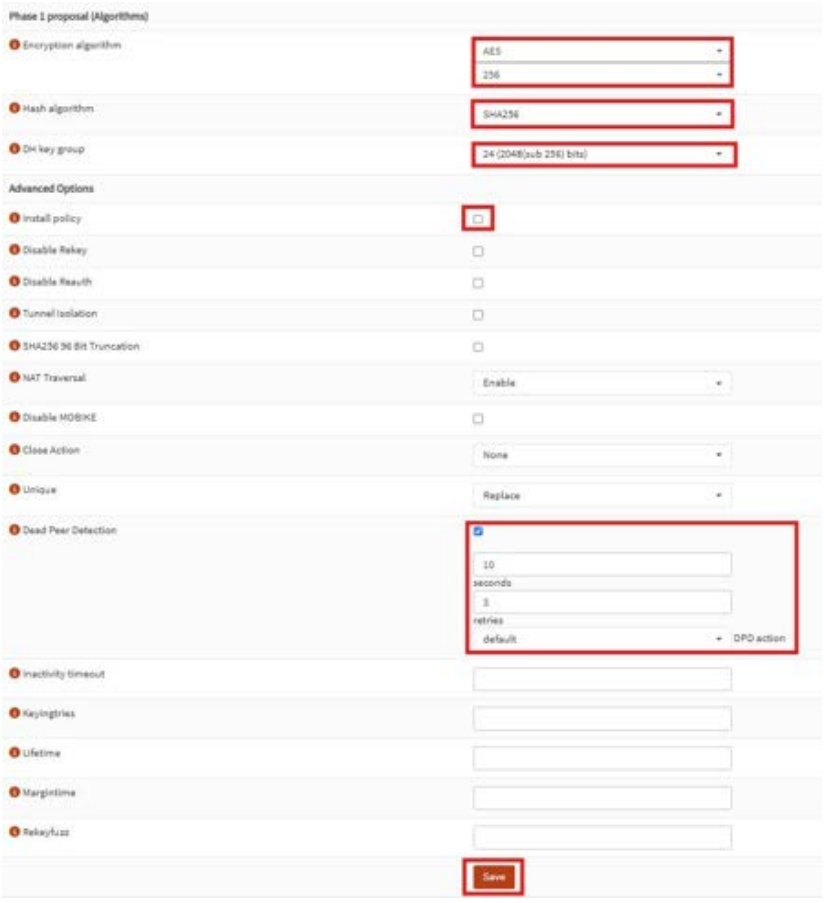


Abbildung 107 Tunnel 1 Phase 1 Konfigurieren 2

3. Tunnel 1 Phase 2 Konfigurieren

- **Mode:** Route-based
- **Description:** vpn-connection-1-tunnel-1-p2
- **Local Address:** 169.254.184.18 (von AWS bereitgestellte Tunnel-IP)
- **Remote Address:** 169.254.184.17 (AWS-Seite des Tunnels)
- **Protocol:** ESP
- **Encryption algorithm:** AES256
- **Hash algorithm:** SHA256
- **PFS key group:** 24 (2048 bits)
- **Install Policy deaktivieren**
- **Lifetime:** 3600 seconds
- Klicke auf **Save**, um die Phase 2 Einstellungen zu speichern.



Abbildung 108 Tunnel 1 Phase 2 Konfigurieren 1

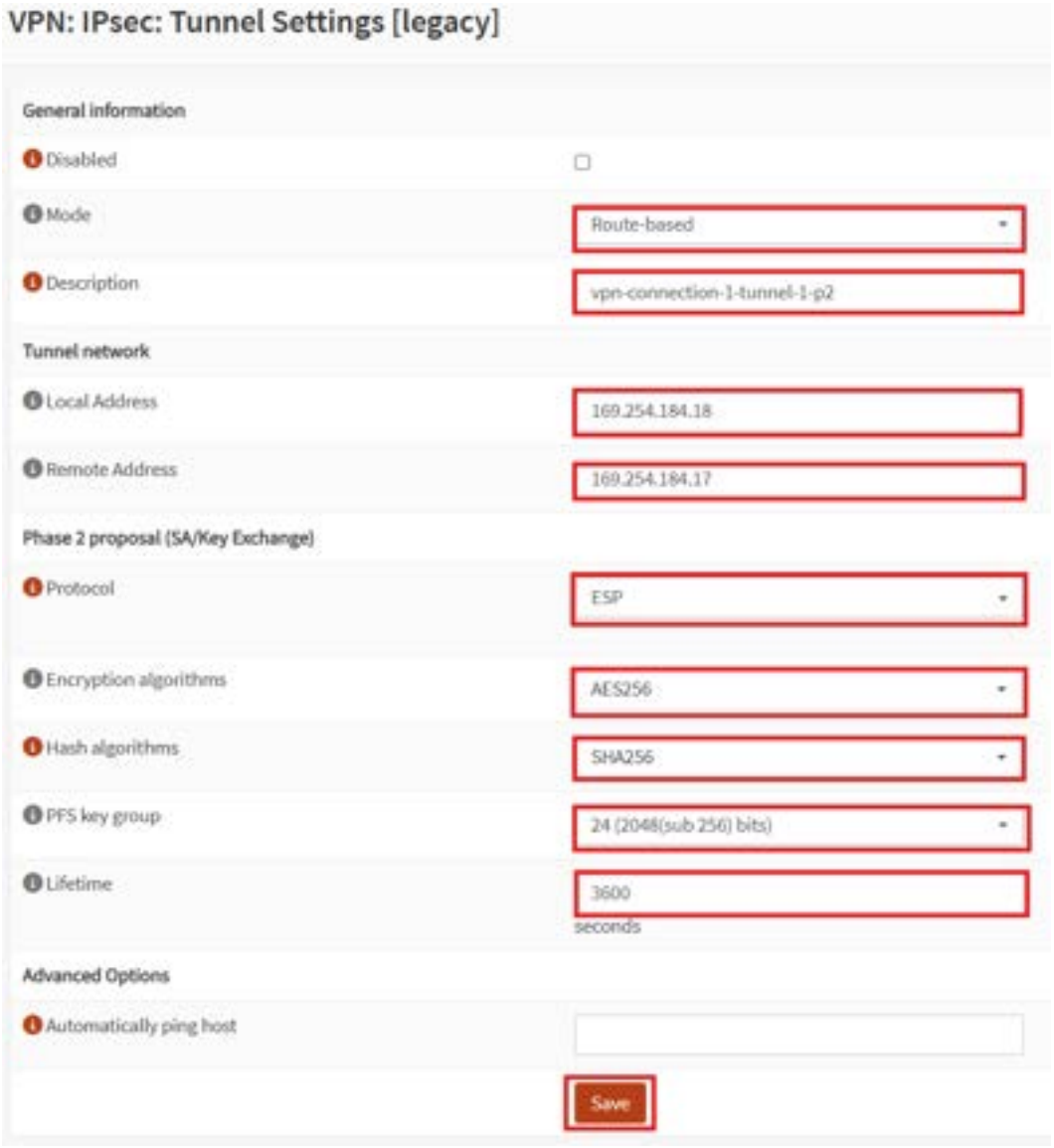


Abbildung 109 Tunnel 1 Phase 2 Konfigurieren 2

4. Tunnel 2 Phase 1 Konfigurieren

- **Connection method:** Start immediate
- **Key Exchange version:** V2
- **Internet Protocol:** IPv4
- **Remote Gateway:** Trage die externe IP-Adresse des AWS VPN-Endpunkts ein
- **Description:** vpn-connection-1-tunnel-2
- **Authentication method:** Mutual PSK
- **Pre-Shared Key:** Kopiere den von AWS bereitgestellten **Pre-Shared Key**.
- **Encryption algorithm:** AES 256
- **Hash algorithm:** SHA256
- **DH key group:** 24 (2048 bits)
- **Dead Peer Detection:** Aktivieren und folgende Werte setzen:
  - 10 seconds
  - 3 retries
  - Default
- Klicke auf **Save**, um die Phase 1 Einstellungen zu speichern.

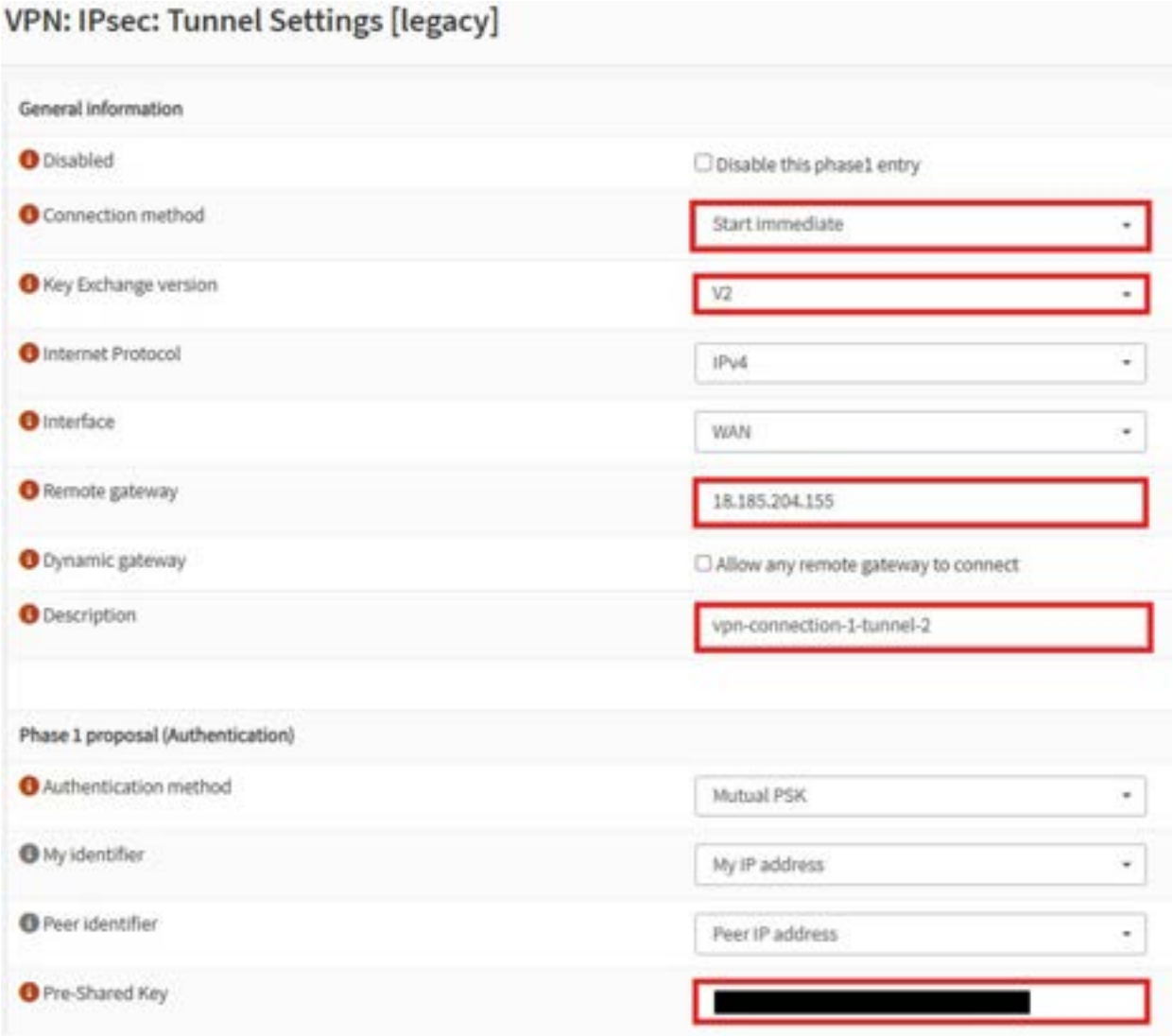


Abbildung 110 Tunnel 2 Phase 1 Konfigurieren 1

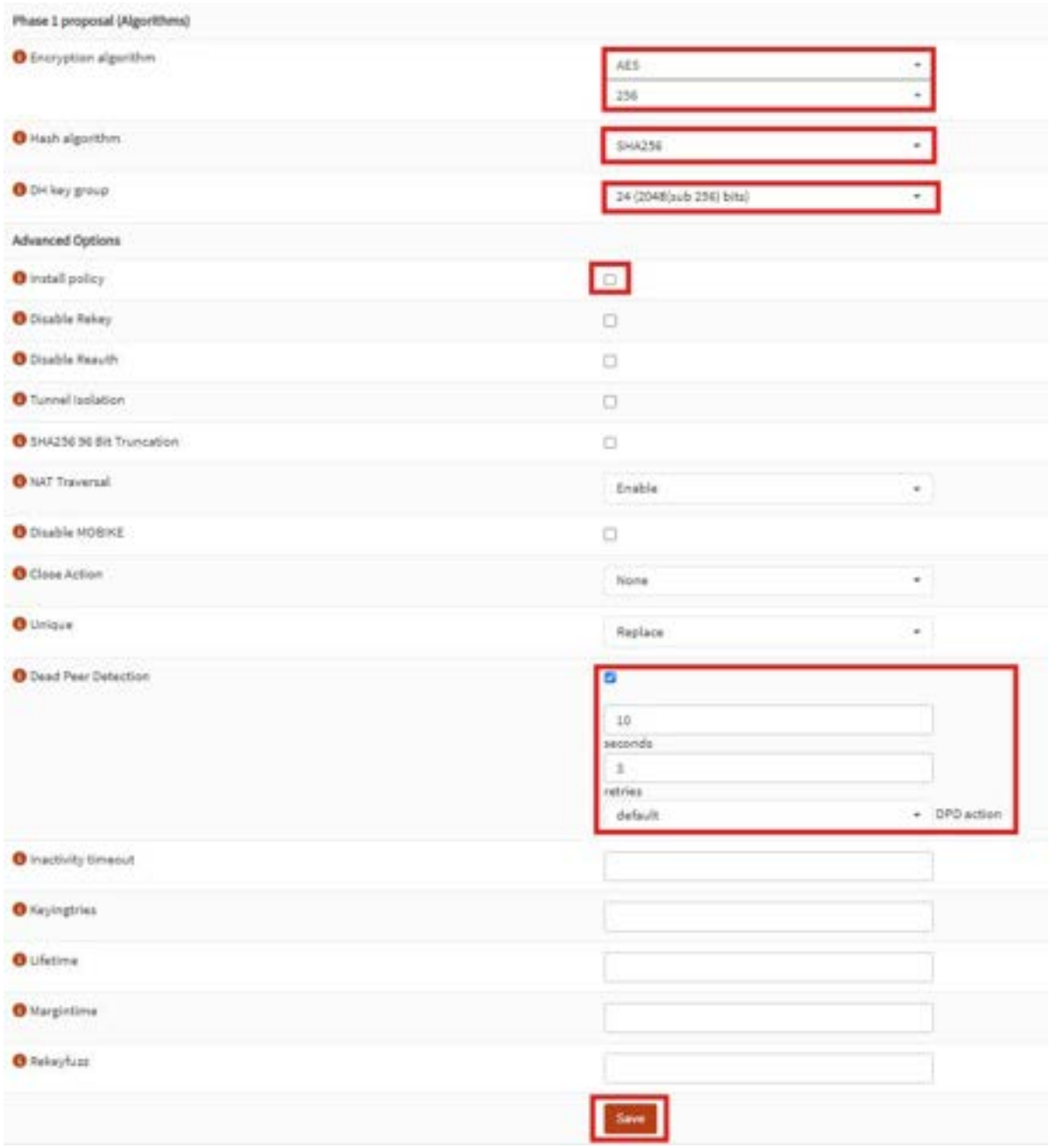


Abbildung 111 Tunnel 2 Phase 1 Konfigurieren 2

5. Tunnel 2 Phase 2 Konfigurieren

- **Mode:** Route-based
- **Description:** vpn-connection-1-tunnel-1-p2
- **Local Address:** 169.254.184.18 (von AWS bereitgestellte Tunnel-IP)
- **Remote Address:** 169.254.184.17 (AWS-Seite des Tunnels)
- **Protocol:** ESP
- **Encryption algorithm:** AES256
- **Hash algorithm:** SHA256
- **PFS key group:** 24 (2048 bits)
- **Install Policy deaktivieren**
- **Lifetime:** 3600 seconds
- Klicke auf **Save**, um die Phase 2 Einstellungen zu speichern.

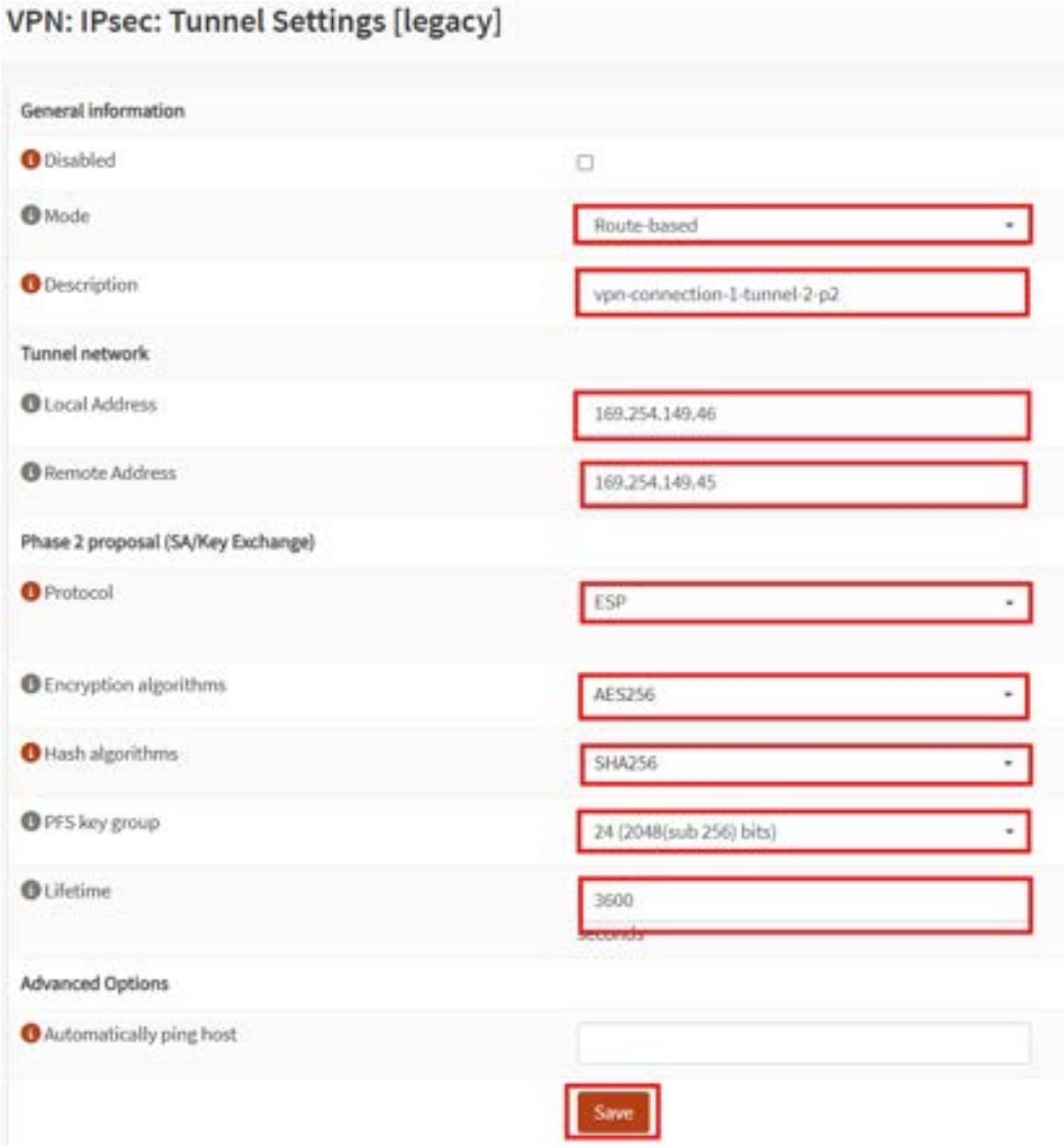


Abbildung 112 Tunnel 2 Phase 2 Konfigurieren

6. Konfiguration überprüfen

- Öffne die **OPNsense Web-GUI**.
- Gehe zu **VPN > IPsec > Status Overview**.
- Die Konfiguration sollte in etwa wie auf den Bild gezeigt aussehen.
- Wichtig ist der State: **INSTALLED**



Abbildung 113 VPN Konfiguration überprüfen

14.3.3 VPN-Verbindung 2 konfigurieren

In diesem Abschnitt werden die Site-to-Site-VPN Tunnels auf der Secondary-OPNsense-Instanz eingerichtet.

Hinweis zur fehlenden Bilddokumentation für VPN-Verbindung 2

Da die Konfiguration der zweiten VPN-Verbindung **exakt** der ersten VPN-Verbindung entspricht, abgesehen von den spezifischen IP-Adressen und Namen der VPN-Tunnel, wurden **keine neuen Screenshots** erstellt.

1. VPN-Tunnel-Eintrag erstellen

- Navigiere in der OPNsense Web-GUI zu **VPN > IPsec > Tunnel Settings (legacy)**.
- Klicke auf das **Plus-Symbol** in der Sektion «Phase 1», um eine neue VPN-Verbindung hinzuzufügen.

2. Tunnel 1 Phase 1 Konfigurieren

- **Connection method:** Start immediate
- **Key Exchange version:** V2
- **Internet Protocol:** IPv4
- **Remote Gateway:** Trage die externe IP-Adresse des AWS VPN-Endpunkts ein
- **Description:** vpn-connection-2-tunnel-1
- **Authentication method:** Mutual PSK
- **Pre-Shared Key:** Kopiere den von AWS bereitgestellten **Pre-Shared Key**.
- **Encryption algorithm:** AES 256
- **Hash algorithm:** SHA256
- **DH key group:** 24 (2048 bits)
- **Dead Peer Detection:** Aktivieren und folgende Werte setzen:
  - 10 seconds
  - 3 retries
  - Default
- Klicke auf **Save**, um die Phase 1 Einstellungen zu speichern.

3. Tunnel 1 Phase 2 Konfigurieren

- **Mode:** Route-based
- **Description:** vpn-connection-2-tunnel-1-p2
- **Local Address:** 169.254.186.118 (von AWS bereitgestellte Tunnel-IP)
- **Remote Address:** 169.254.186.117 (AWS-Seite des Tunnels)
- **Protocol:** ESP
- **Encryption algorithm:** AES256
- **Hash algorithm:** SHA256
- **PFS key group:** 24 (2048 bits)
- **Install Policy deaktivieren**
- **Lifetime:** 3600 seconds
- Klicke auf **Save**, um die Phase 2 Einstellungen zu speichern.

4. Tunnel 2 Phase 1 Konfigurieren

- **Connection method:** Start immediate
- **Key Exchange version:** V2
- **Internet Protocol:** IPv4
- **Remote Gateway:** Trage die externe IP-Adresse des AWS VPN-Endpunkts ein
- **Description:** vpn-connection-2-tunnel-2
- **Authentication method:** Mutual PSK
- **Pre-Shared Key:** Kopiere den von AWS bereitgestellten **Pre-Shared Key**.
- **Encryption algorithm:** AES256
- **Hash algorithm:** SHA256
- **PFS key group:** 24 (2048 bits)
- **Dead Peer Detection:** Aktivieren und folgende Werte setzen:
  - 10 seconds
  - 3 retries
  - Default
- Klicke auf **Save**, um die Phase 1 Einstellungen zu speichern.

5. Tunnel 2 Phase 2 Konfigurieren

- **Mode:** Route-based
- **Description:** vpn-connection-2-tunnel-2-p2
- **Local Address:** 169.254.137.98 (von AWS bereitgestellte Tunnel-IP)
- **Remote Address:** 169.254.137.97 (AWS-Seite des Tunnels)
- **Protocol:** ESP
- **Encryption algorithm:** AES256
- **Hash algorithm:** SHA256
- **PFS key group:** 24 (2048 bits)
- **Install Policy deaktivieren**
- **Lifetime:** 3600 seconds
- Klicke auf **Save**, um die Phase 2 Einstellungen zu speichern.

6. Konfiguration überprüfen

- Öffne die **OPNsense Web-GUI**.
- Gehe zu **VPN > IPsec > Status Overview**.
- Die Konfiguration sollte in etwa wie auf den Bild gezeigt aussehen.
- Wichtig ist der State: **INSTALLED**



Abbildung 114 IPsec Konfiguration überprüfen

14.3.4 Konfiguration vom BGP OPNsense Primary

Diese Anleitung beschreibt, wie BGP (Border Gateway Protocol) in OPNsense konfiguriert wird, um eine Verbindung mit AWS Transit Gateway über Site-to-Site VPN herzustellen.

1. BGP Aktivieren und Grundkonfiguration

- Navigiere zu **Routing > BGP**.
- Aktiviere BGP durch das Setzen des Häkchens bei **Enable**.
- Setze die **BGP AS Number** auf **65001** (interne ASN für das On-Premises-Netzwerk).
- Trage unter **Network** das Netzwerk **0.0.0.0/0** ein, um die Standard Route anzukündigen.
- Klicke auf **Apply**, um die Änderungen zu übernehmen.

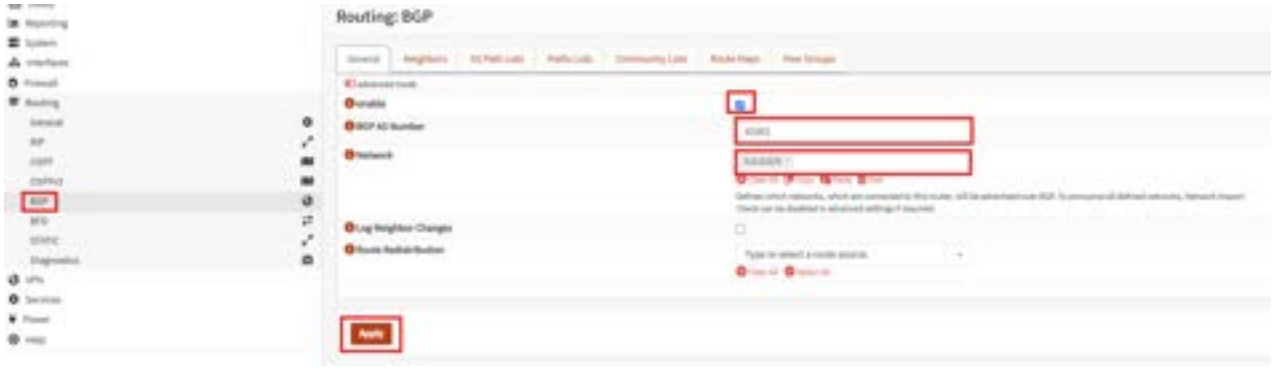


Abbildung 115 BGP Aktivieren und Grundkonfiguration

2. BGP Neighbors hinzufügen

- Wechsle zum Tab **Neighbors** und klicke auf das **Plus-Symbol**, um einen neuen BGP-Nachbarn hinzuzufügen.
- Tunnel 1 Neighbor-Konfiguration:
  - **Description:** aws-transit-gateway-tunnel-1
  - **Peer-IP:** 169.254.184.17 (AWS-Seite des VPN-Tunnels 1)
  - **Remote AS:** 64512 (AWS ASN)
  - **Update-Source Interface:** vpnconnection1tunnel1
  - **Hold Down Time:** 30
  - Klicke auf **Save**, um die Einstellungen zu speichern.
- Tunnel 2 Neighbor-Konfiguration:
  - **Description:** aws-transit-gateway-tunnel-2
  - **Peer-IP:** 169.254.149.45 (AWS-Seite des VPN-Tunnels 2)
  - **Remote AS:** 64512 (AWS ASN)
  - **Update-Source Interface:** vpnconnection1tunnel2
  - **Hold Down Time:** 30
  - Klicke auf **Save**, um die Einstellungen zu speichern.
- Nach dem Speichern der beiden Neighbor-Einträge klicke erneut auf **Apply**, um die Änderungen zu aktivieren.



Abbildung 116 BGP Neighbors hinzufügen 1

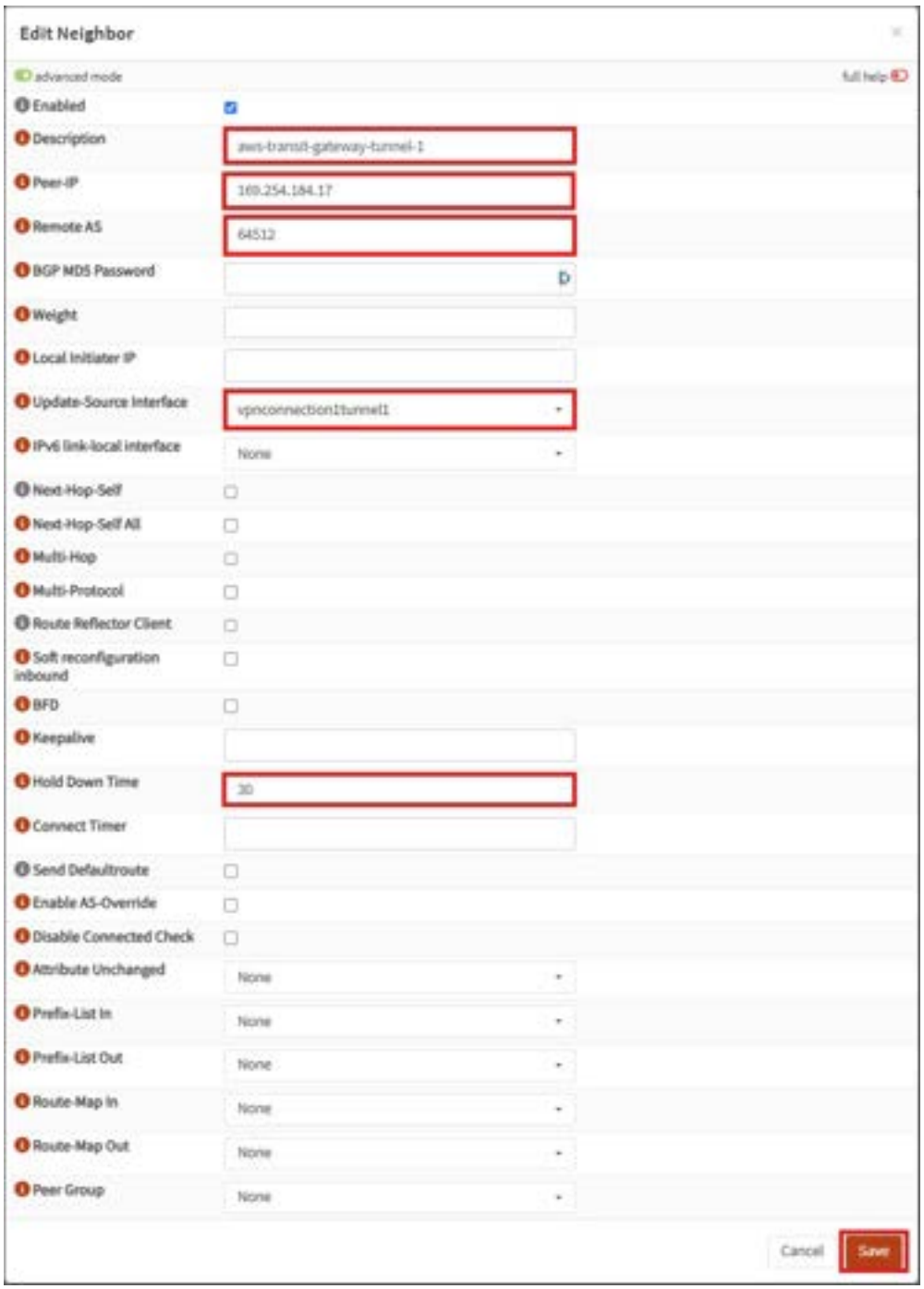


Abbildung 117 BGP Neighbors hinzufügen 2

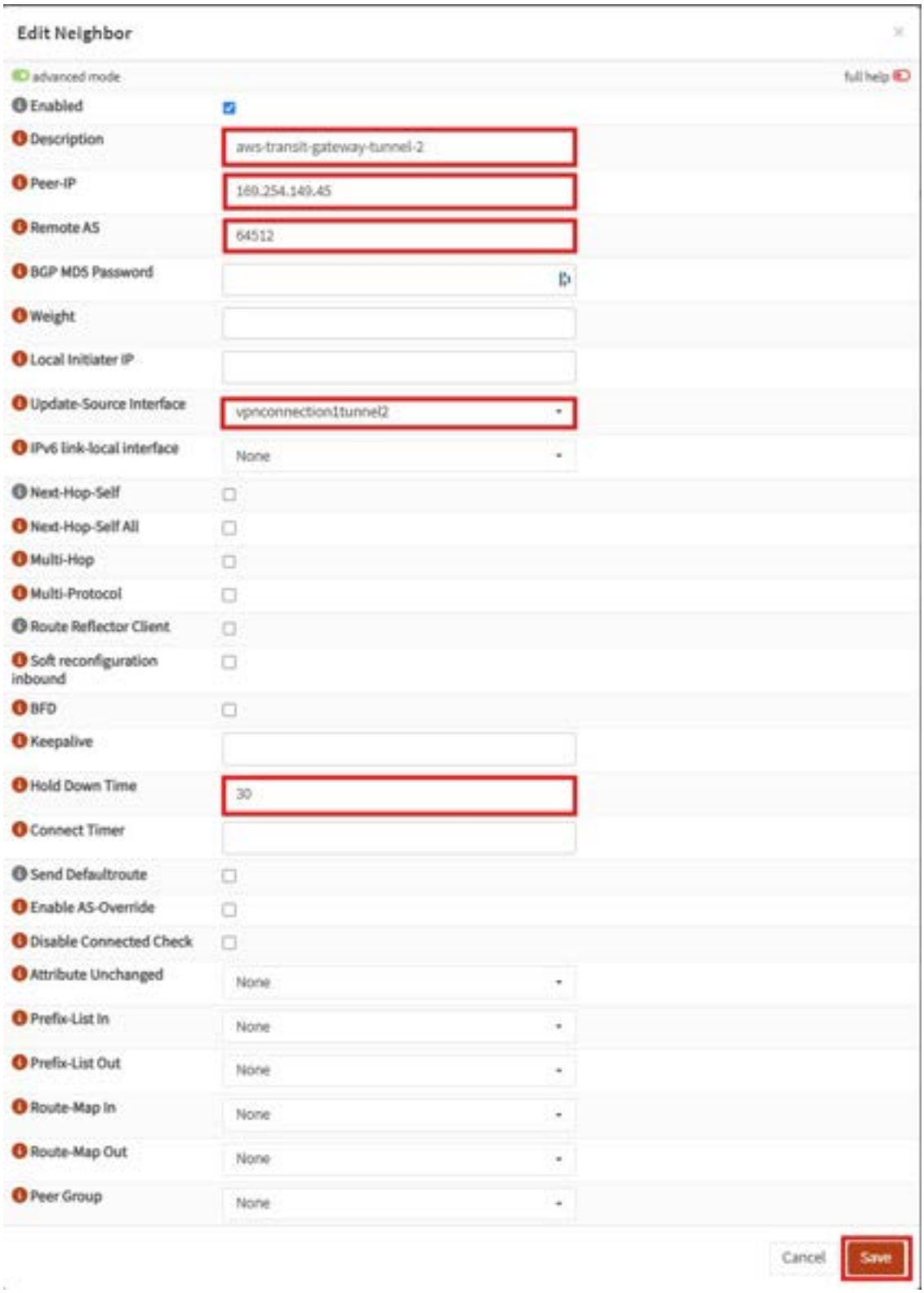


Abbildung 118 BGP Neighbors hinzufügen 3

3. Überprüfung der Konfiguration

- Navigiere zu **Routing > BGP > Routing Diagnostics**.
- Wechsle zum Tab **IPv4 Routing Table**, um die erlernten Routen anzuzeigen.
- Hier sollten nun die AWS Transit Gateway-Peers mit den Next-Hop-Adressen (169.254.184.17 und 169.254.149.45) sichtbar sein.
- Prüfe, ob die Routing-Einträge für das AWS VPC-Netzwerk (z. B. 10.100.0.0/16) korrekt übernommen wurden.



Abbildung 119 Überprüfung der BGP Konfiguration

14.3.5 Konfiguration vom BGP OPNsense Secondary

Diese Anleitung beschreibt, wie BGP (Border Gateway Protocol) in OPNsense konfiguriert wird, um eine Verbindung mit AWS Transit Gateway über Site-to-Site VPN herzustellen.

1. BGP Aktivieren und Grundkonfiguration

- Navigiere zu **Routing > BGP**.
- Aktiviere BGP durch das Setzen des Häkchens bei **Enable**.
- Setze die **BGP AS Number** auf **65001** (interne ASN für das On-Premises-Netzwerk).
- Trage unter **Network** das Netzwerk **0.0.0.0/0** ein, um die Standard Route anzukündigen.
- Klicke auf **Apply**, um die Änderungen zu übernehmen.



Abbildung 120 BGP Aktivieren und Grundkonfiguration

2. BGP Neighbors hinzufügen

- Wechsle zum Tab **Neighbors** und klicke auf das **Plus-Symbol**, um einen neuen BGP-Nachbarn hinzuzufügen.
- Tunnel 1 Neighbor-Konfiguration:
  - **Description:** aws-transit-gateway-tunnel-1
  - **Peer-IP:** 169.254.186.117 (AWS-Seite des VPN-Tunnels 1)
  - **Remote AS:** 64512 (AWS ASN)
  - **Update-Source Interface:** vpnconnection2tunnel1
  - **Hold Down Time:** 30
  - Klicke auf **Save**, um die Einstellungen zu speichern.
- Tunnel 2 Neighbor-Konfiguration:
  - **Description:** aws-transit-gateway-tunnel-2
  - **Peer-IP:** 169.254.137.97 (AWS-Seite des VPN-Tunnels 2)
  - **Remote AS:** 64512 (AWS ASN)
  - **Update-Source Interface:** vpnconnection2tunnel2
  - **Hold Down Time:** 30
  - Klicke auf **Save**, um die Einstellungen zu speichern.
- Nach dem Speichern der beiden Neighbor-Einträge klicke erneut auf **Apply**, um die Änderungen zu aktivieren.



Abbildung 121 BGP Neighbors hinzufügen 1

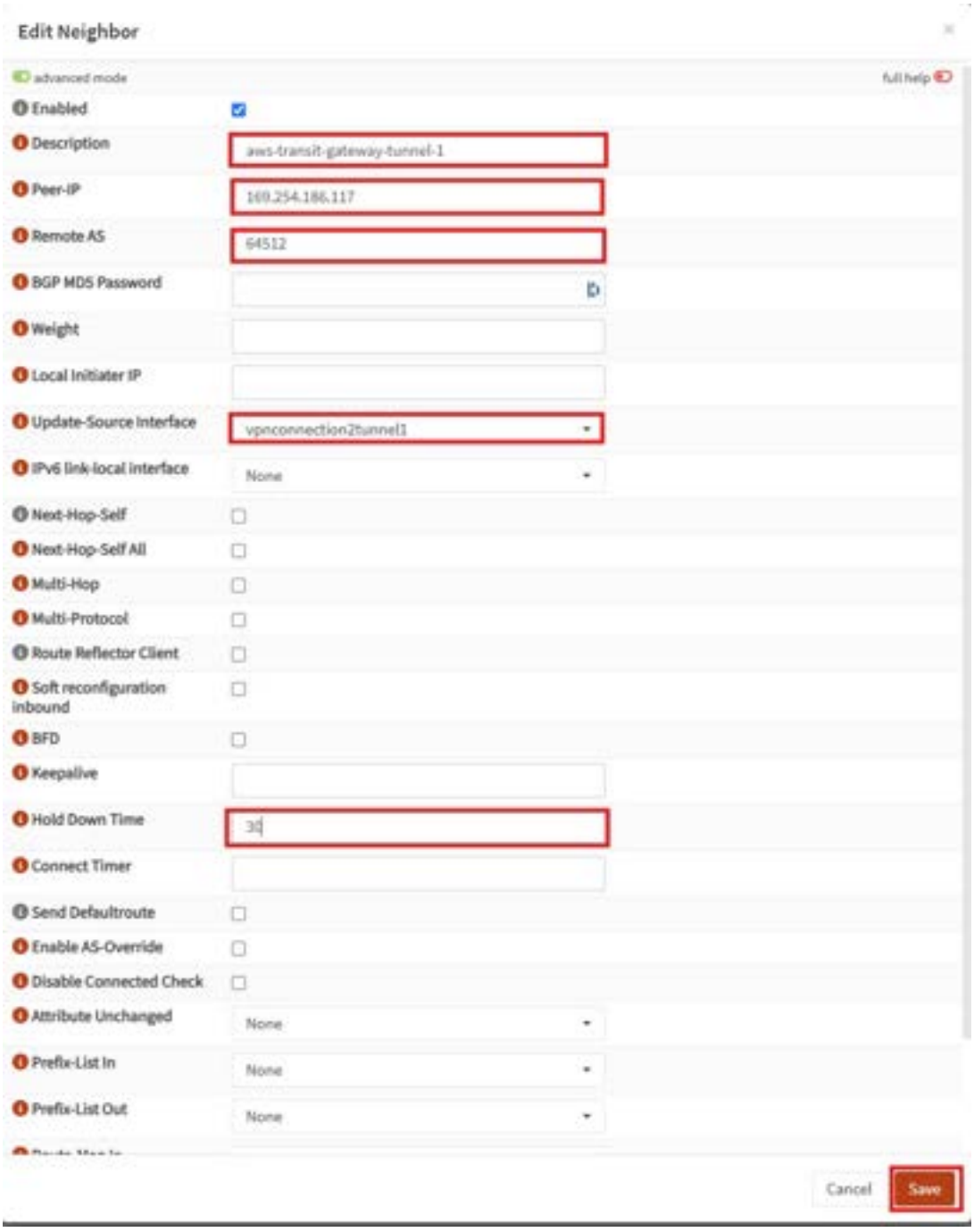


Abbildung 122 BGP Neighbors hinzufügen 2

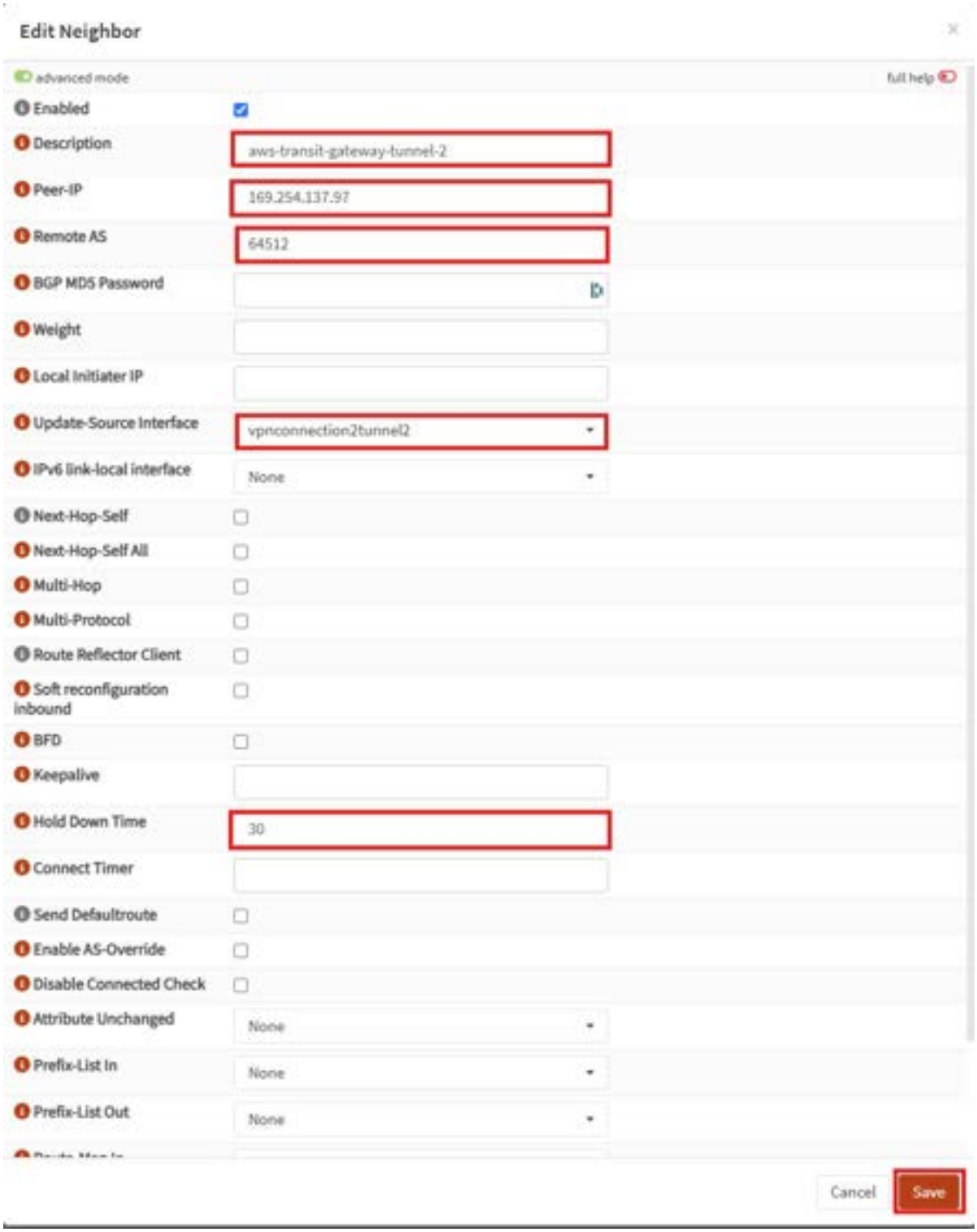


Abbildung 123 BGP Neighbors hinzufügen 3

3. Überprüfung der Konfiguration

- Navigiere zu **Routing > BGP > Routing Diagnostics**.
- Wechsle zum Tab **IPv4 Routing Table**, um die erlernten Routen anzuzeigen.
- Hier sollten nun die AWS Transit Gateway-Peers mit den Next-Hop-Adressen (169.254.184.17 und 169.254.149.45) sichtbar sein.
- Prüfe, ob die Routing-Einträge für das AWS VPC-Netzwerk (z. B. 10.100.0.0/16) korrekt übernommen wurden.

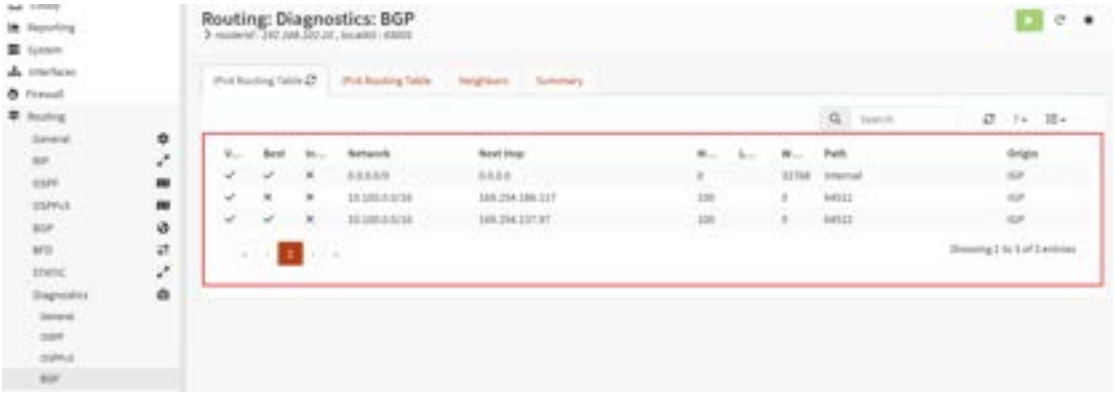


Abbildung 124 Überprüfung der BGP-Konfiguration

14.3.6 Konfiguration der Firewall auf beiden OPNsense Instanzen

In diesem Kapitel wird die Konfiguration der Firewall beschrieben, damit die Kommnikation zwischen On-premises und AWS erlaubt wird.

WICHTIG: Diese Konfiguration muss auf beiden (Primary und Secondary) Instanzen durchgeführt werden.

1. Neue Firewall Regel hinzufügen

- Navigiere in der OPNsense Web-GUI zu **Firewall > Rules > IPsec**.
- Klicke auf das **Plus-Symbol (+)**, um eine neue Regel hinzuzufügen.



Abbildung 125 Neue Firewall Regel hinzufügen

2. Firewall Regel konfigurieren

- Setze folgende Werte in der **Edit Firewall Rule**-Maske:
  - **Action:** Pass (Erlaubt den Datenverkehr)
  - **Quick:** Aktivieren (Anweisung wird sofort angewendet)
  - **Interface:** IPsec
  - **Direction:** in (eingehender Datenverkehr)
  - **TCP/IP Version:** IPv4
  - **Protocol:** any (beliebige Protokolle)
  - Source:
    - **Typ:** Single host or Network
    - **Wert:** 10.100.0.0/16 (Beispiel: VPC-Netzwerk)
  - **Destination:** any (beliebiges Ziel)
  - **Destination port range:** any (beliebiger Port)
- Scrolle nach unten und klicke auf **Save**, um die Regel zu speichern.

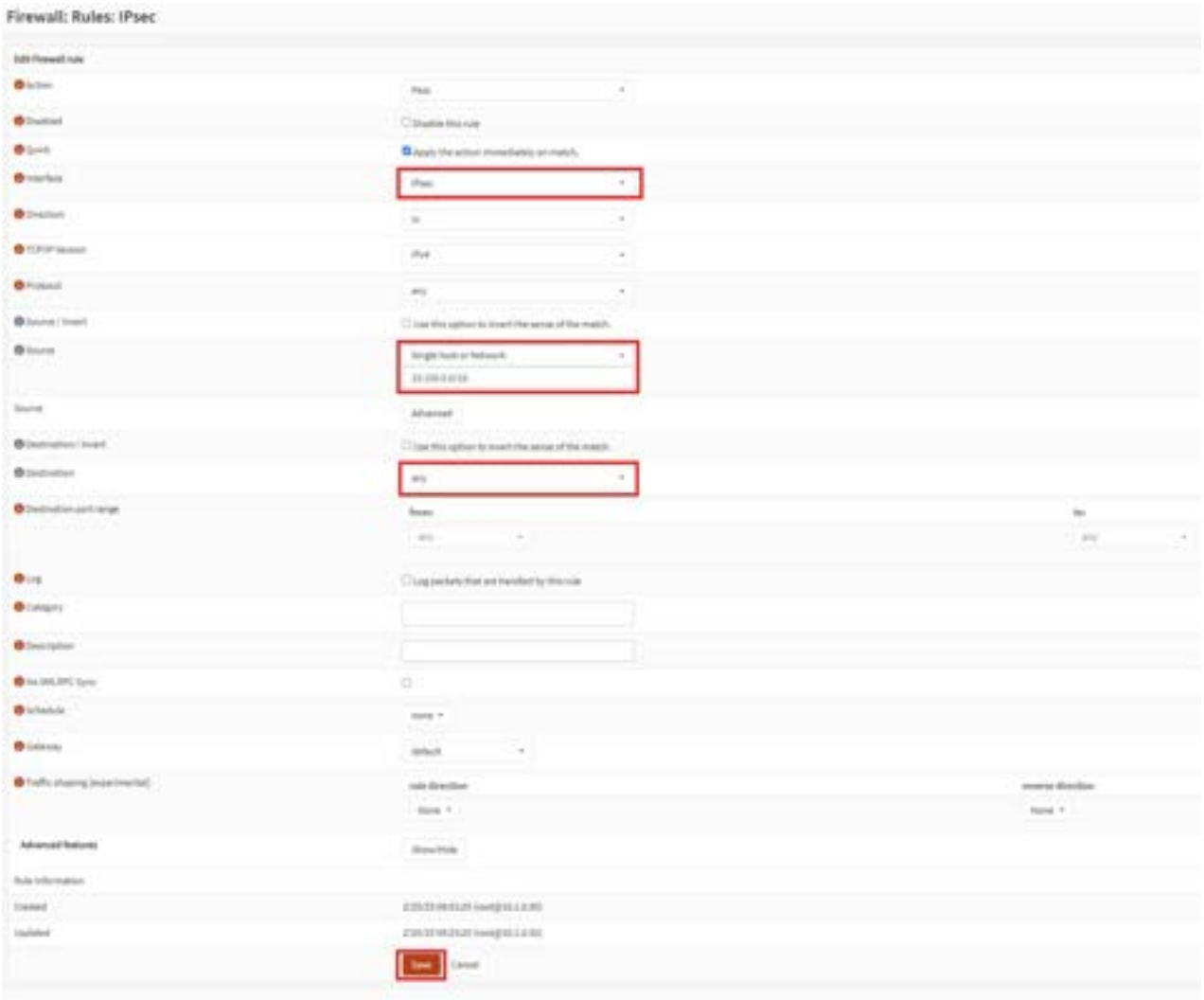


Abbildung 126 Firewall Regel konfigurieren

3. Konfiguration überprüfen

Die Regel sollte nun wie auf der nächsten Darstellung aussehen.

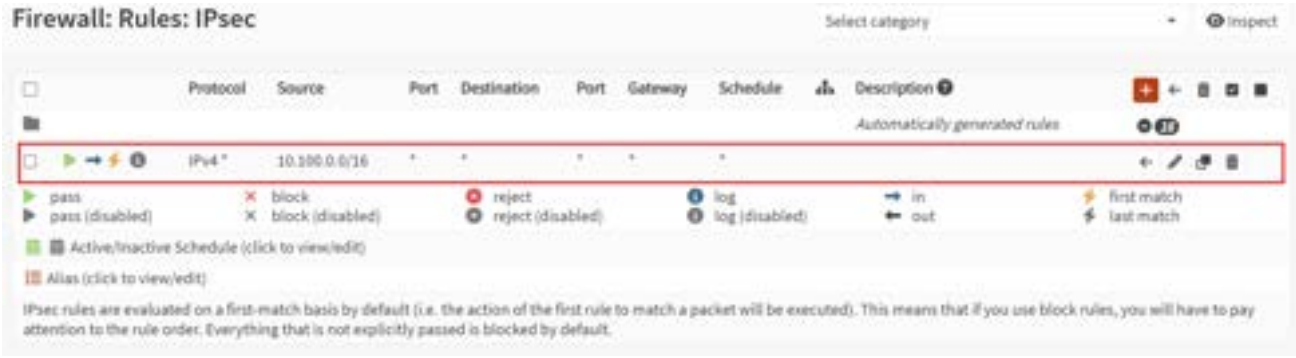


Abbildung 127 Firewall Rule-Konfiguration überprüfen

14.4 Erste Connectivity Tests

14.4.1 On-Premises Testserver Erstellen

1. VM-Erstellung starten

- Öffne den **ESXi Host Client**
- Klicke auf **«Create / Register VM»**

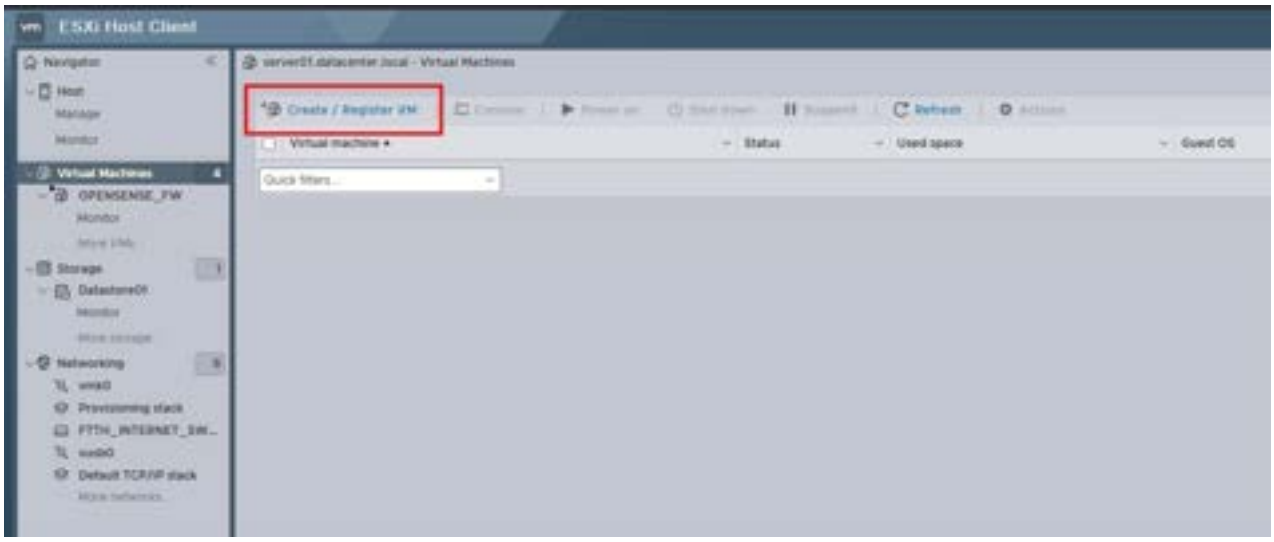


Abbildung 128 VM-Erstellung starten

2. Wähle «Create a new virtual machine»

- Klicke auf «**Next**»

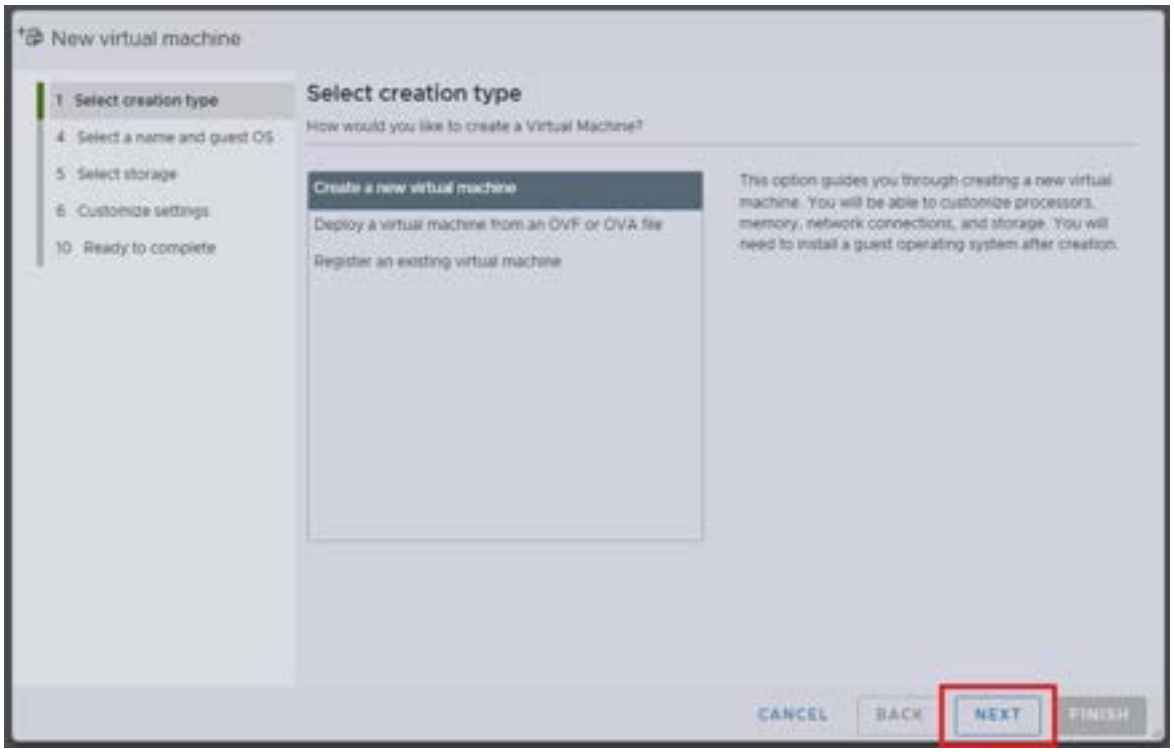


Abbildung 129 Wähle «Create a new virtual machine»

3. Name und Gast-Betriebssystem festlegen

- Gib einen **Namen** für die VM ein
- Wähle die **Kompatibilität** (z. B. ESXi 7.0 U2).
- Setze **Guest OS Family** auf **Linux**.
- Wähle als **Guest OS Version Ubuntu Linux (64-bit)**
- Klicke auf **«Next»**.

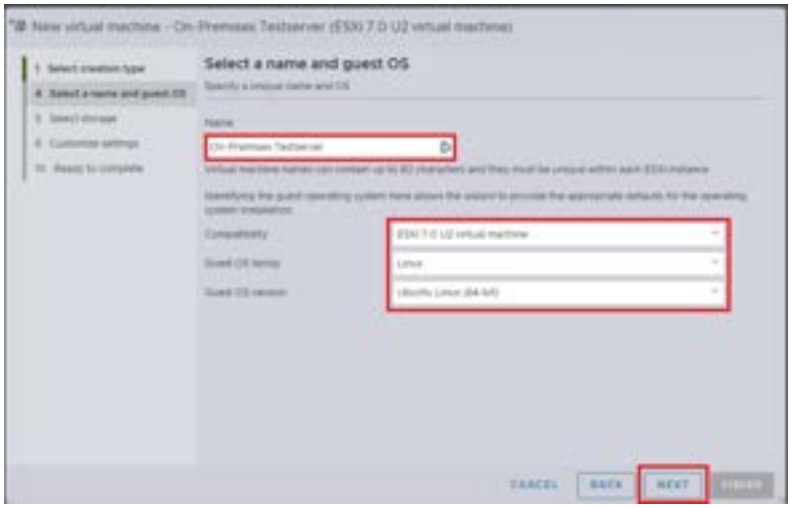


Abbildung 130 Name und Gast-Betriebssystem festlegen

4. Speicherort auswählen

- Wähle den gewünschten **Datastore** für die VM
- Klicke auf **«Next»**.

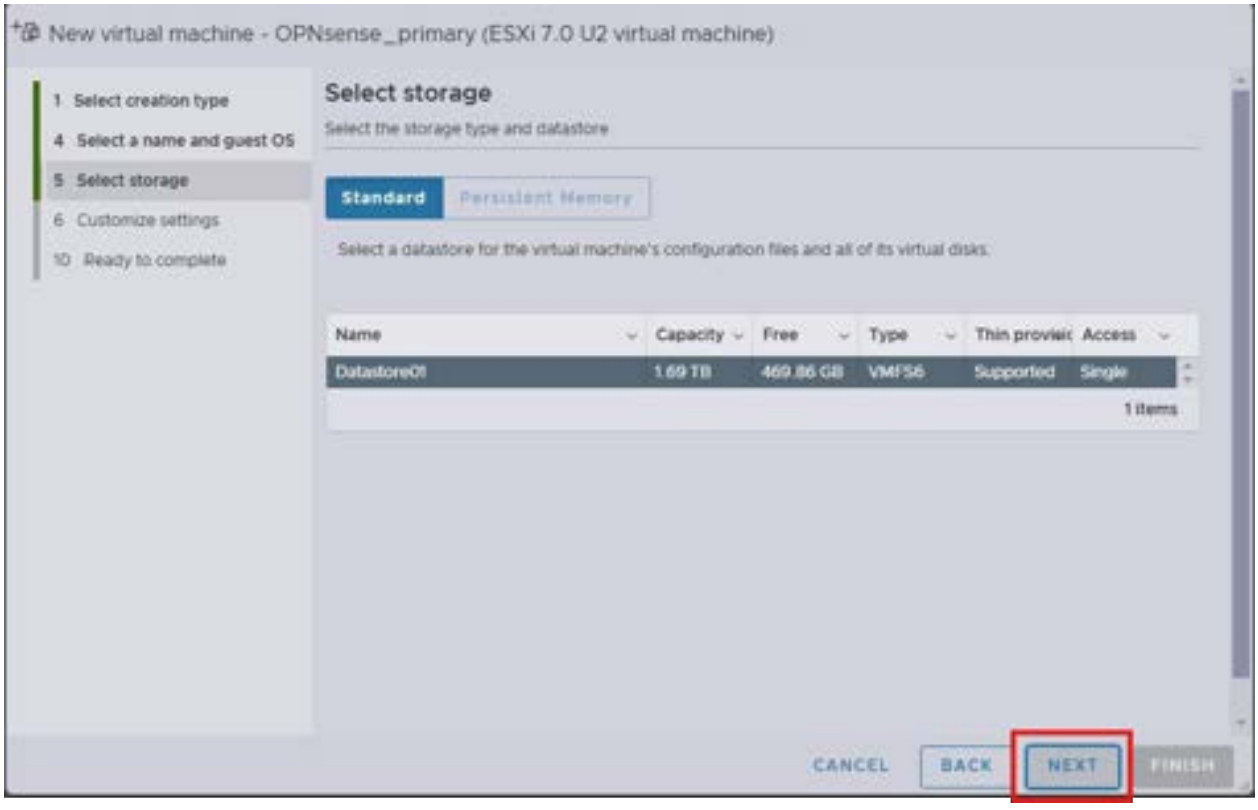


Abbildung 131 Speicherort auswählen

5. Hardware anpassen

- **CPU**: Setze die Anzahl auf **2 Cores**.
- **RAM**: Setze den Speicher auf **6GB**.
- **Festplatte**: Stelle **25GB** ein.
- **Adapter 1:** ON_PREMISES_NET (verbunden).
- **CD/DVD-Laufwerk hinzufügen**.

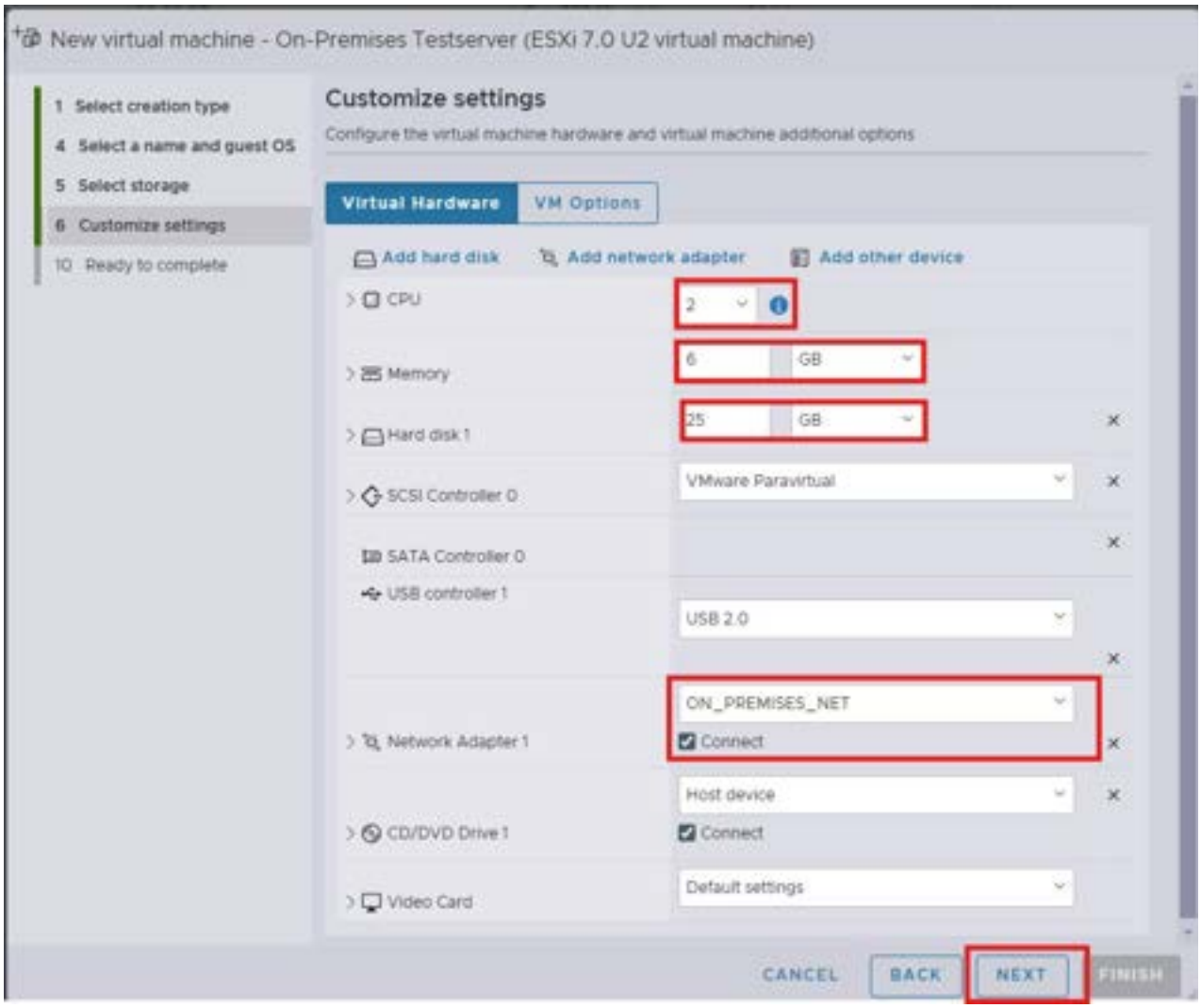


Abbildung 132 Hardware anpassen 1

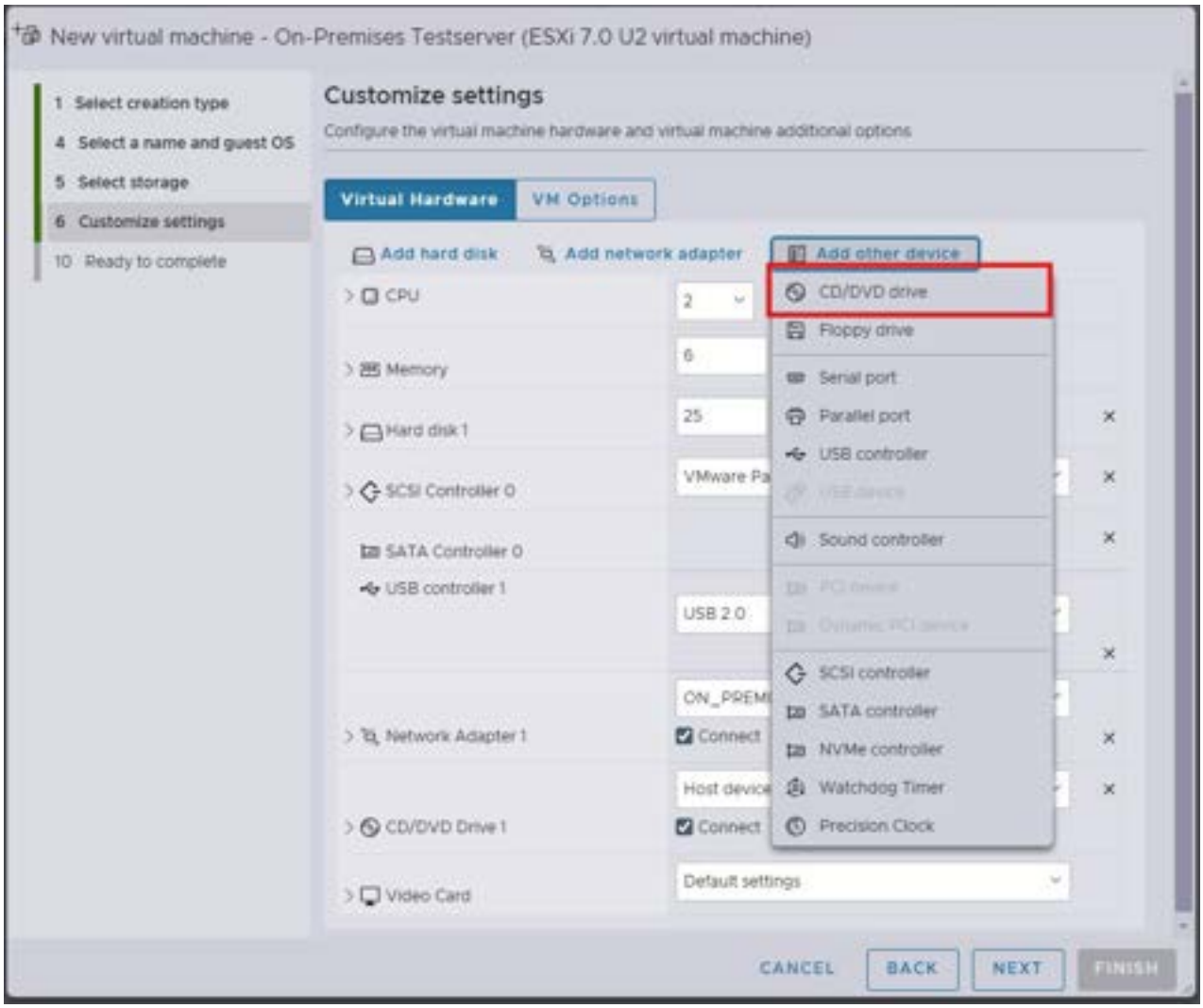


Abbildung 133 Hardware anpassen 2

6. ISO-Image einbinden

- Wähle als **CD/DVD-Laufwerk** die Option **«Datastore ISO file»**.
- Suche das passende **ISO-Image** im Datastore.
- Klicke auf **«Select»**.

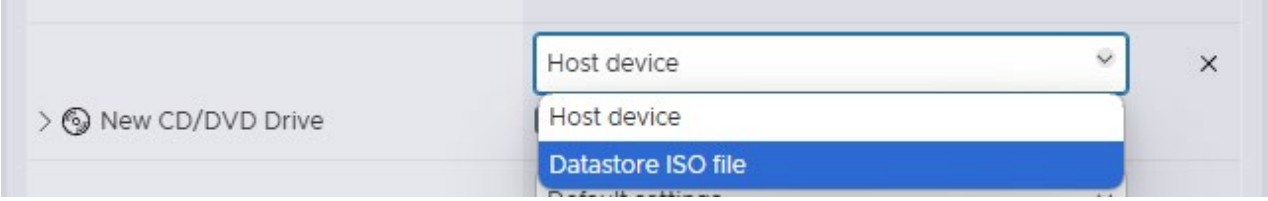


Abbildung 134 ISO-Image einbinden 1

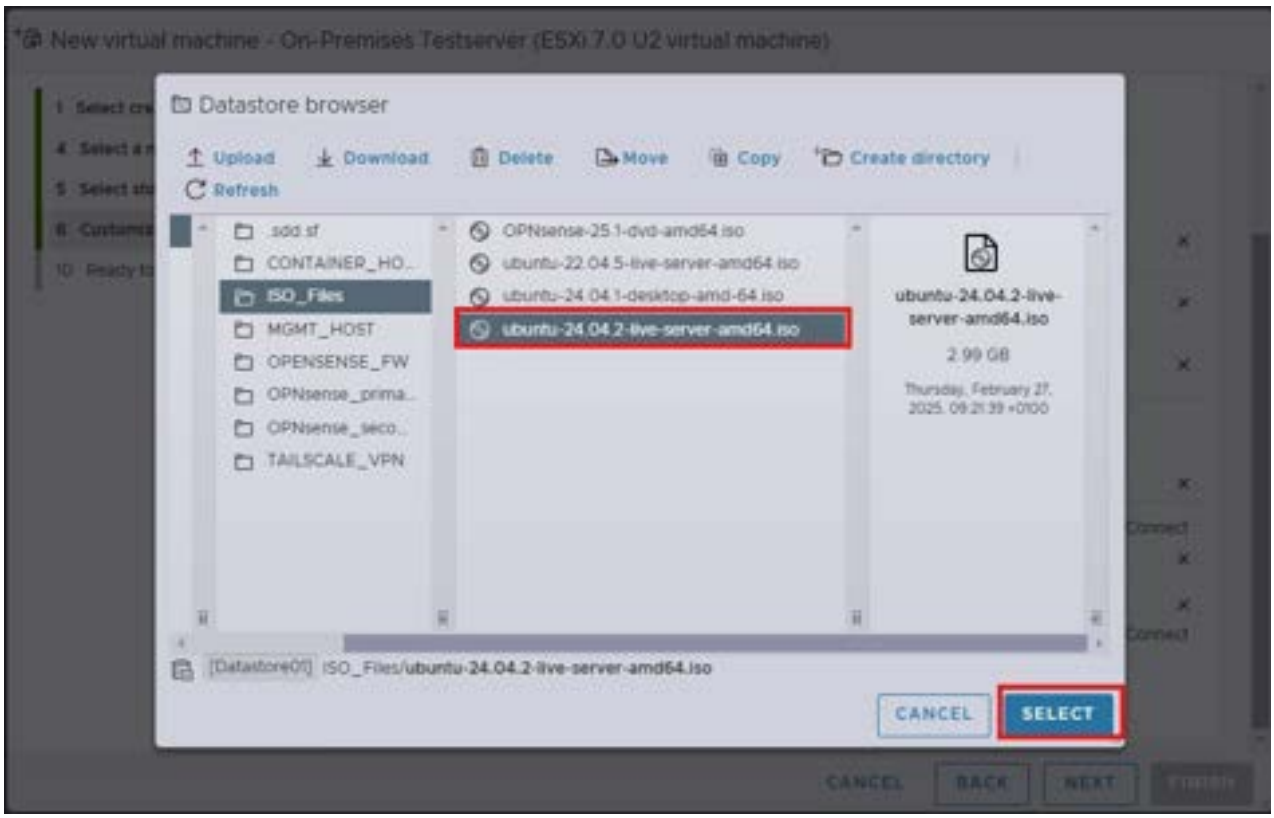


Abbildung 135 ISO-Image einbinden 2

7. Überprüfung und Abschluss

- Überprüfe alle **Einstellungen**
- Klicke auf «**Finish»**, um die VM zu erstellen

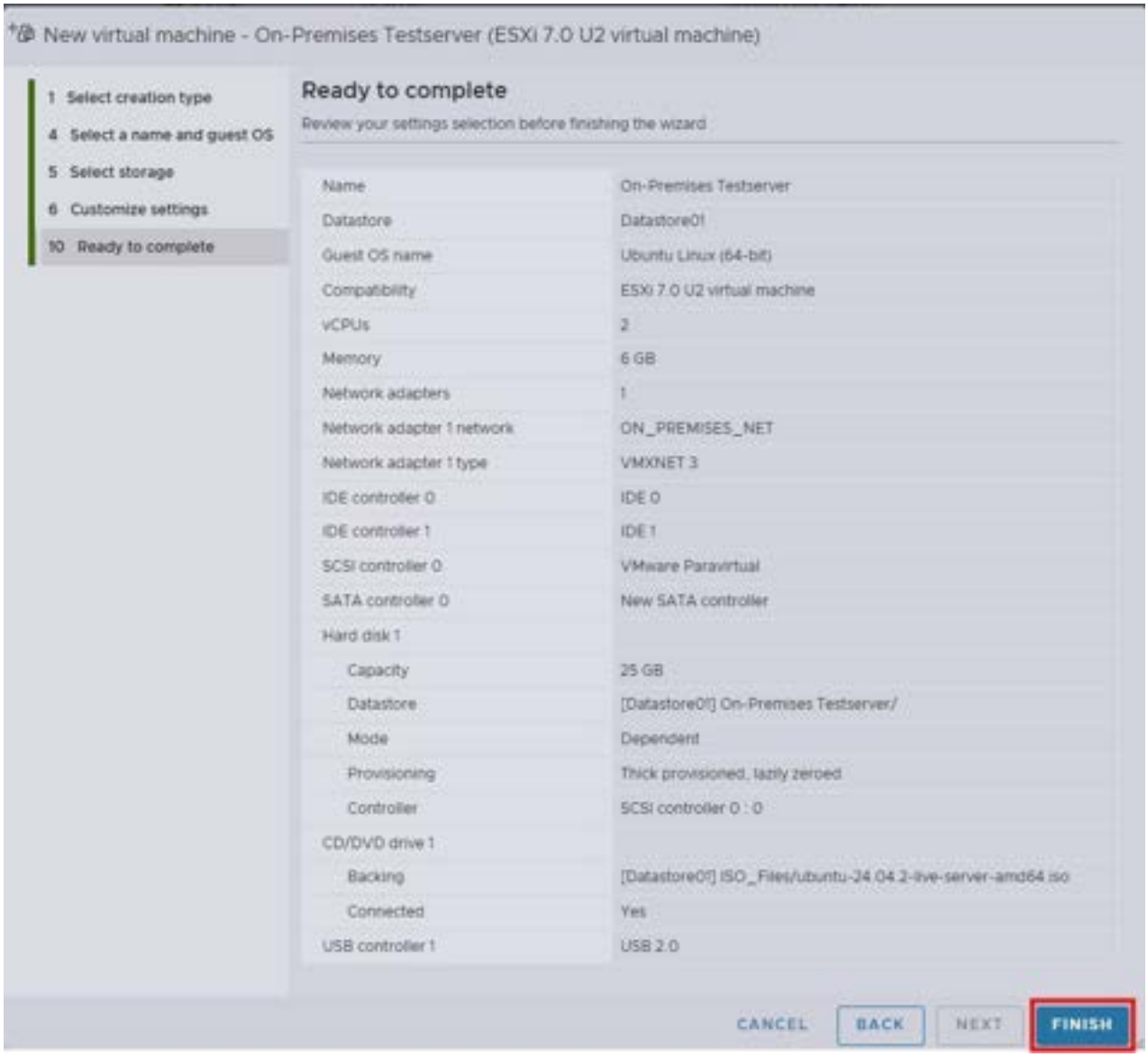


Abbildung 136 Überprüfung und Abschluss

8. VM einschalten

- Wähle die erstellte VM (OPNsense_primary) aus.
- Klicke auf **«Power on»**, um die VM zu starten.

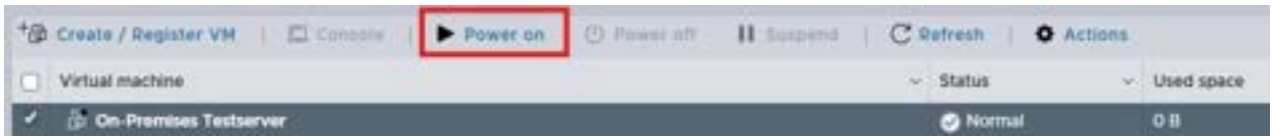


Abbildung 137 VM einschalten

14.4.2 On-Premises Testserver Installieren

1. Sprache auswählen

- Nach dem Start des Installationsmediums erscheint das **Sprachauswahl-Menü**.
- Mit den **Pfeiltasten** durch die Liste navigieren.
- **«English»** auswählen und mit **Enter** bestätigen.

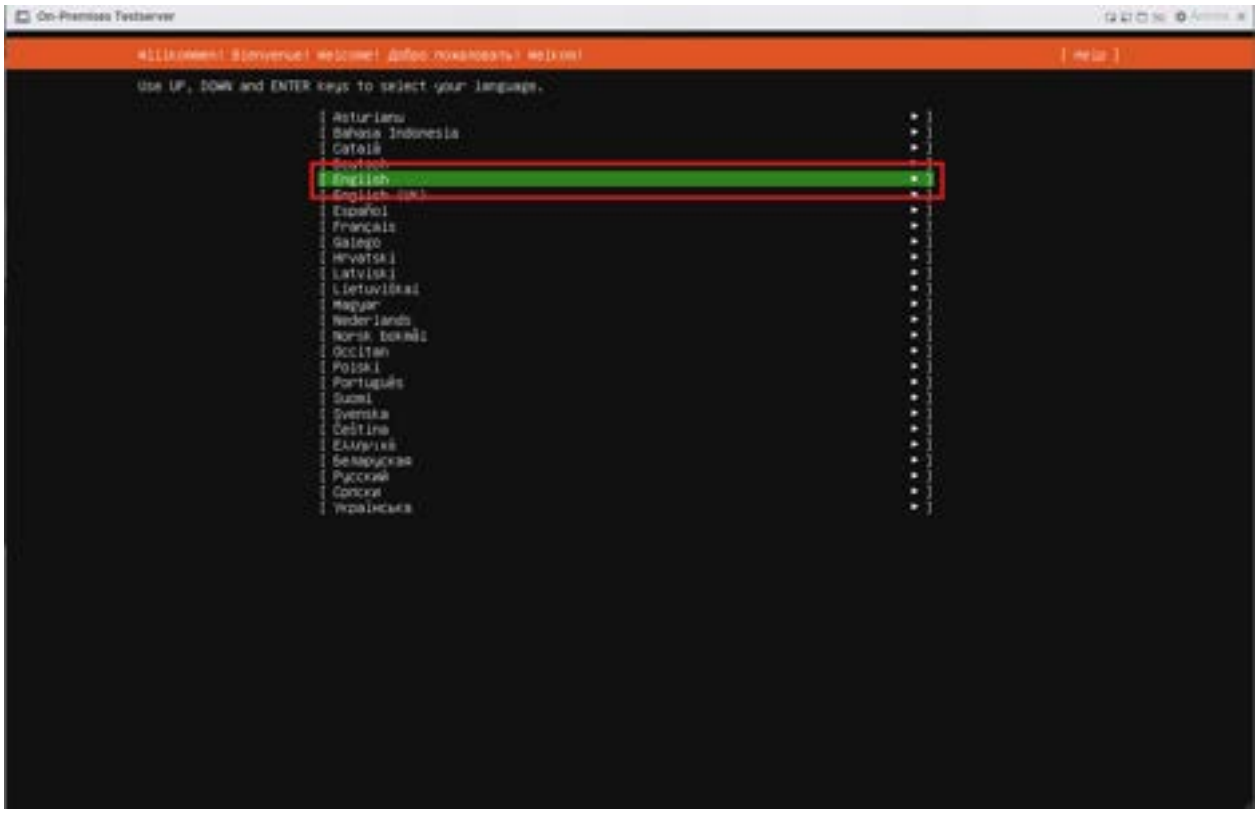


Abbildung 138 Sprache auswählen

2. Tastaturlayout festlegen

- Das **Tastatur-Layout** bestimmen.
- Die Voreinstellung ist auf **US-English**, dies kann geändert werden.
- In diesem Fall wird **«Switzerland»** als Layout gewählt.
- Mit **«Done»** bestätigen.

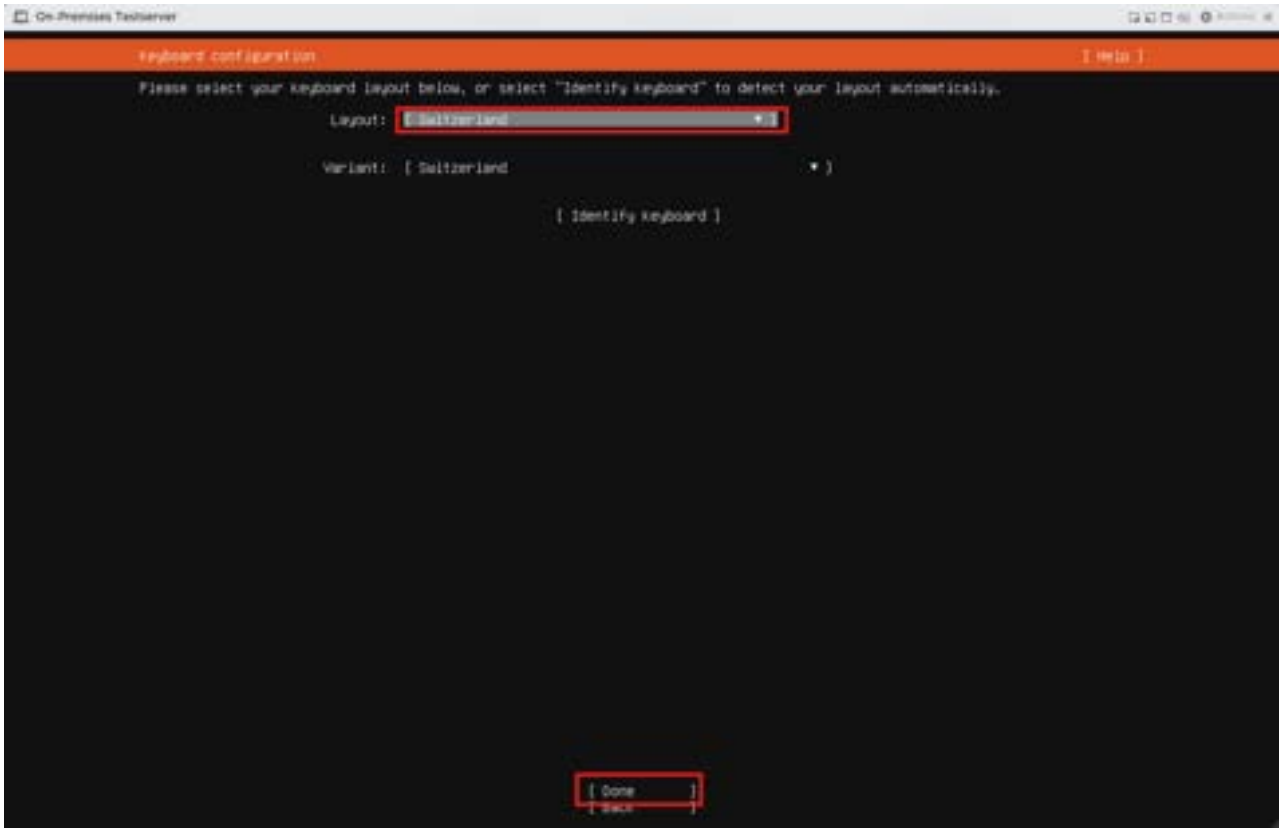


Abbildung 139 Tastaturlayout festlegen

3. Installationsart wählen

- Standardmässig ist **«Ubuntu Server»** vorausgewählt.
- Die Option **«Search for third-party drivers»** kann ignoriert werden.
- Mit **«Done»** fortfahren.

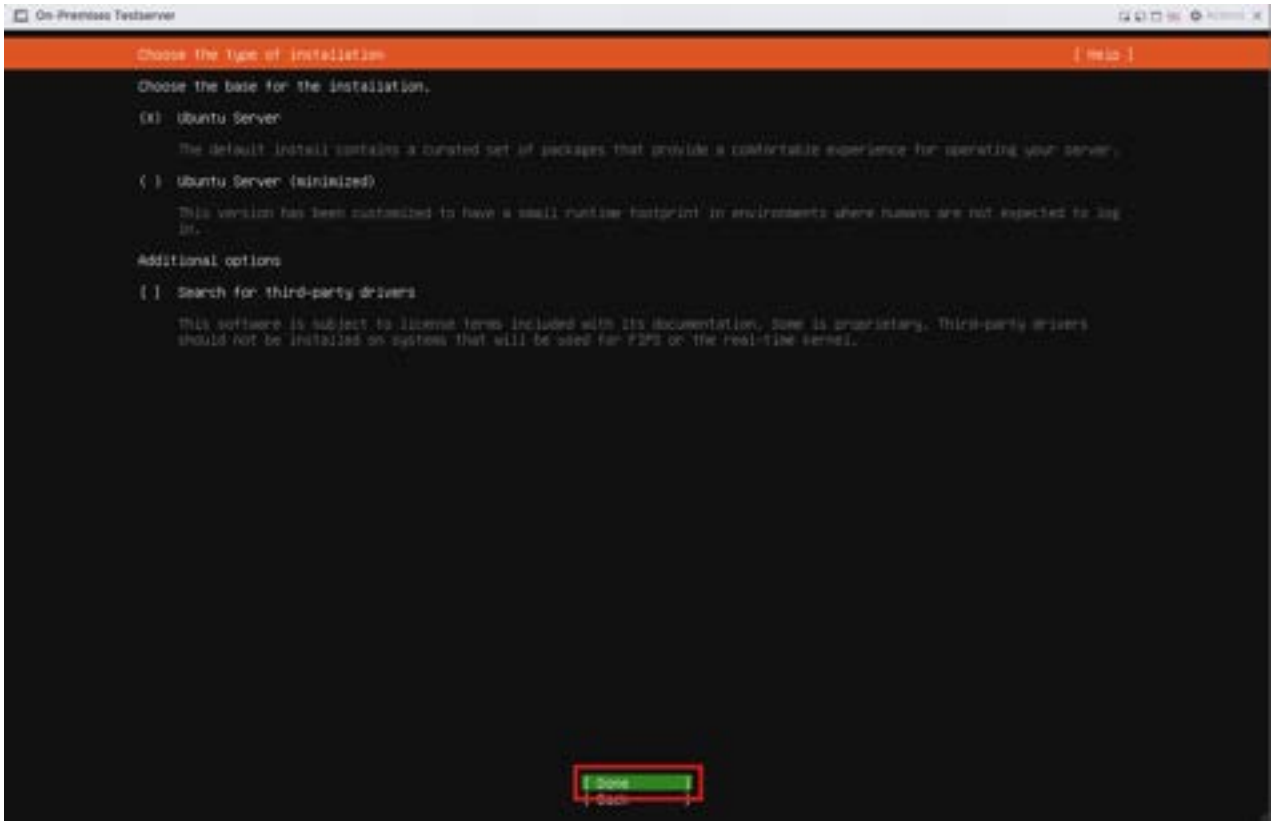


Abbildung 140 Installationsart wählen

4. Netzwerkkonfiguration

- Eine Netzwerkschnittstelle konfigurieren.
- **„IPv4 Method“ auf „Manual“ setzen**.
- Die Netzwerkeinstellungen eingeben:
  - **Subnet**: `10.1.0.0/16`
  - **Address**: `10.1.0.20`
  - **Gateway**: `10.1.0.1`
  - **Name Server**: `1.1.1.1, 8.8.8.8`
- Mit **„Save“** bestätigen.
- Danach mit **„Done“** fortfahren.

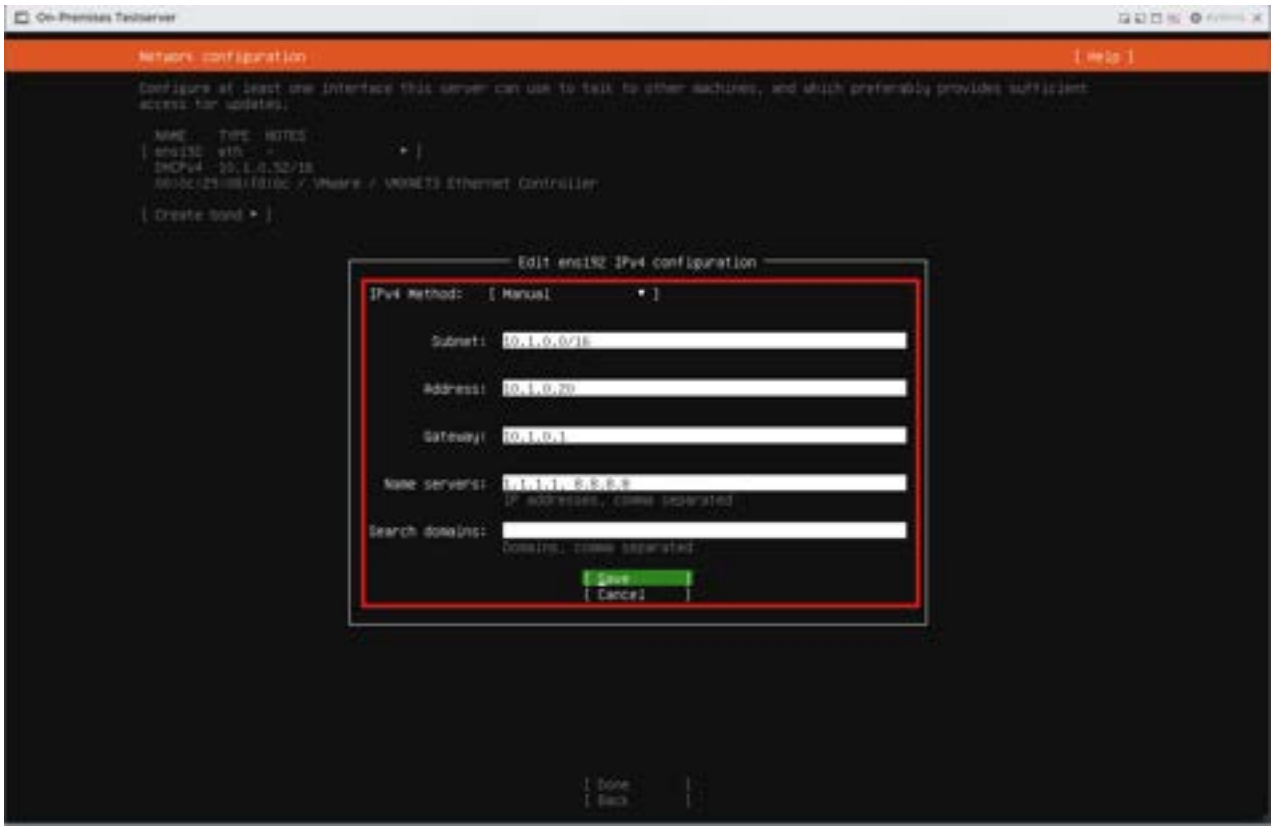


Abbildung 141 Netzwerkkonfiguration

5. Festplattenpartitionierung

- Standardmässig ist **«Use an entire disk»** gewählt.
- Mit **«Done»** bestätigen.
- Eine **Bestätigung für das Löschen der Partitionen** wird verlangt.
- **«Continue»** wählen.

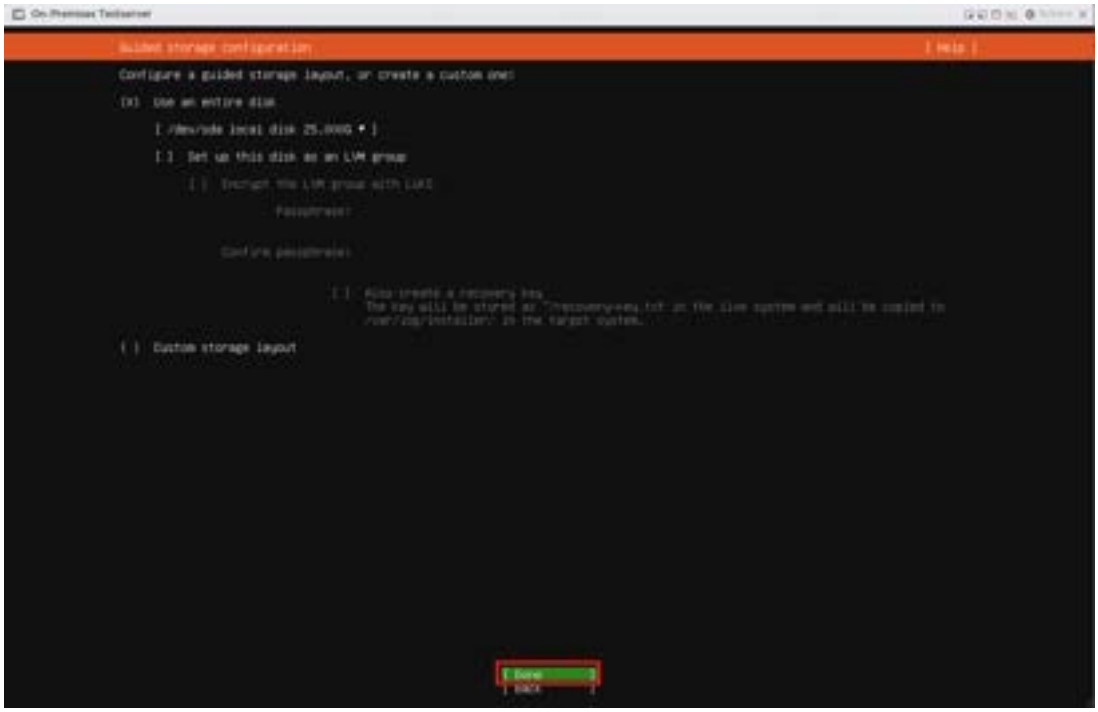


Abbildung 142 Festplattenpartitionierung 1

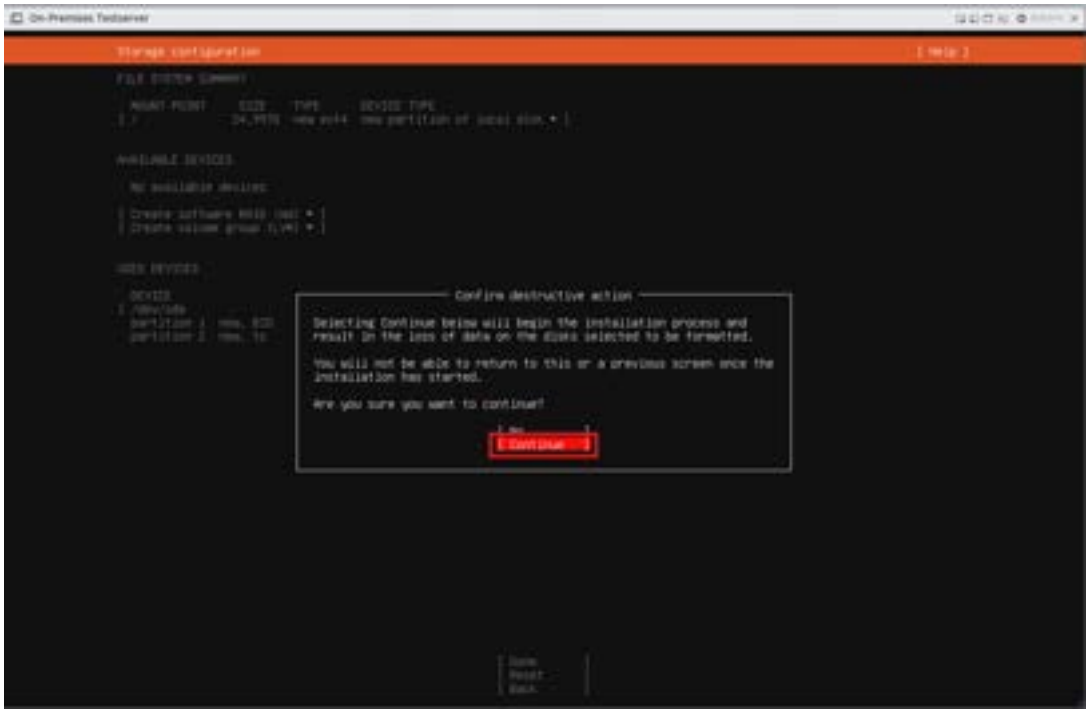


Abbildung 143 Festplattenpartitionierung 2

6. Benutzerkonto einrichten

- **Name:** On-premises Testserver
- **Servername:** testserver
- **Benutzername:** test
- **Passwort:** Ein sicheres Passwort festlegen.
- Mit **«Done»** speichern.

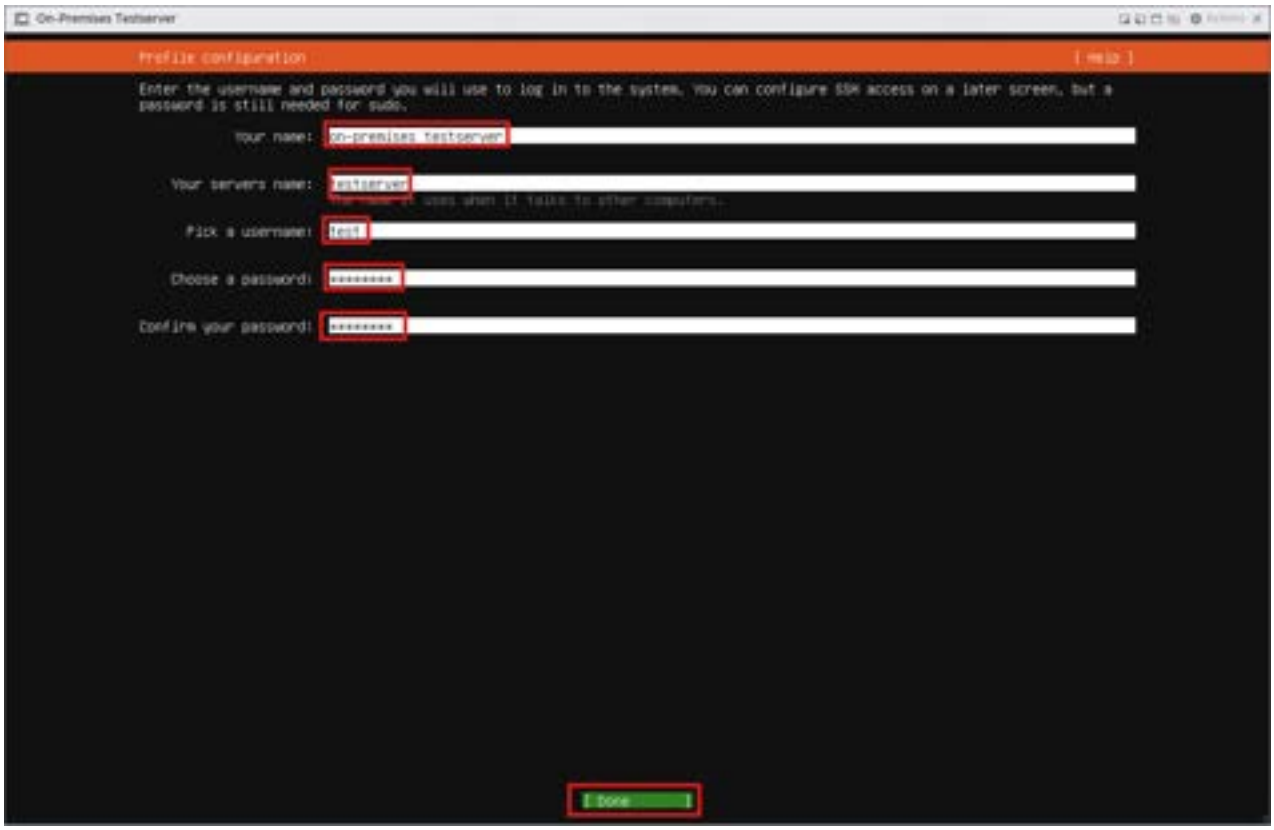


Abbildung 144 Benutzerkonto einrichten

7. SSH-Server installieren

- Die Option **«Install OpenSSH Server»** aktivieren.
- Mit **«Done»** bestätigen.

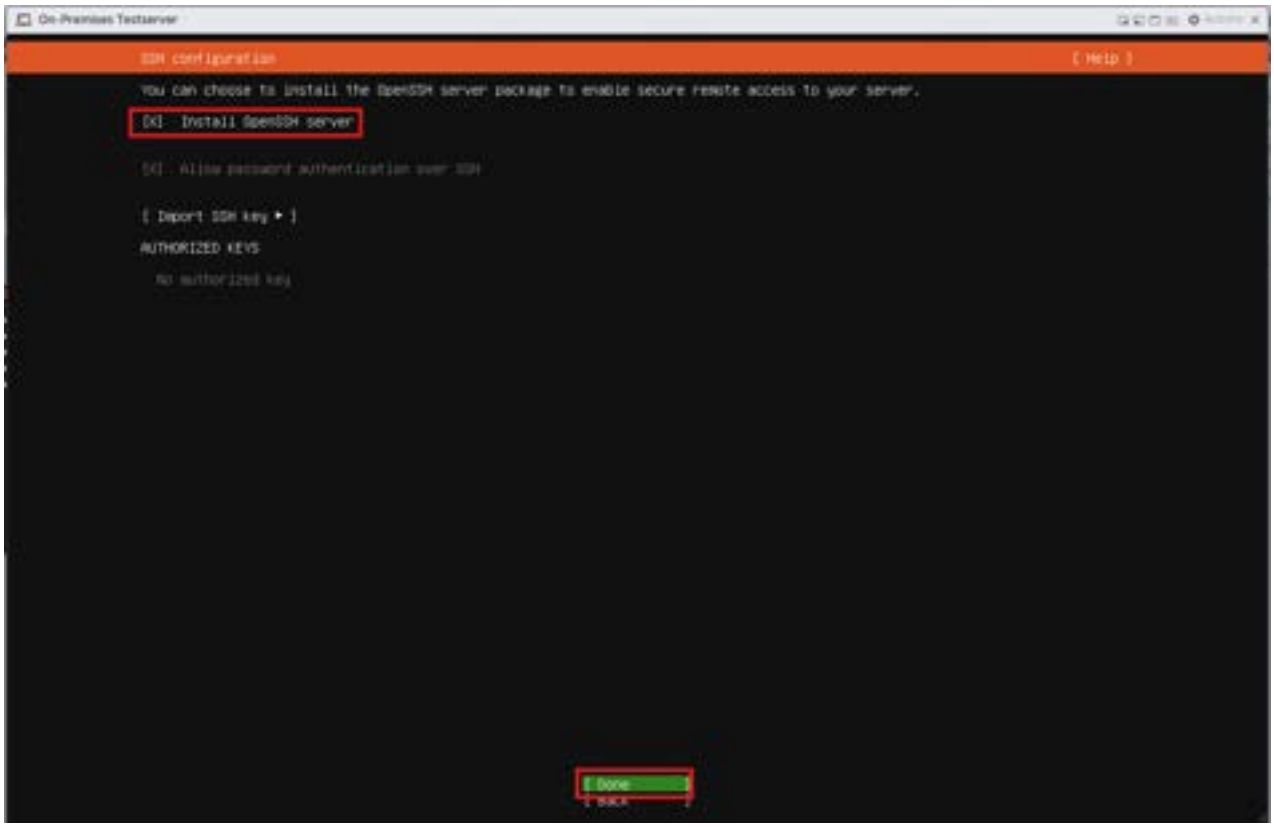


Abbildung 145 SSH-Server installieren

8. Update Ubuntu Server

Nach der Installation:

- Login auf dem neuen Server
- **Command**:
  - sudo apt update && sudo apt upgrade -y
- Danach ist das System auf dem neuesten Stand.

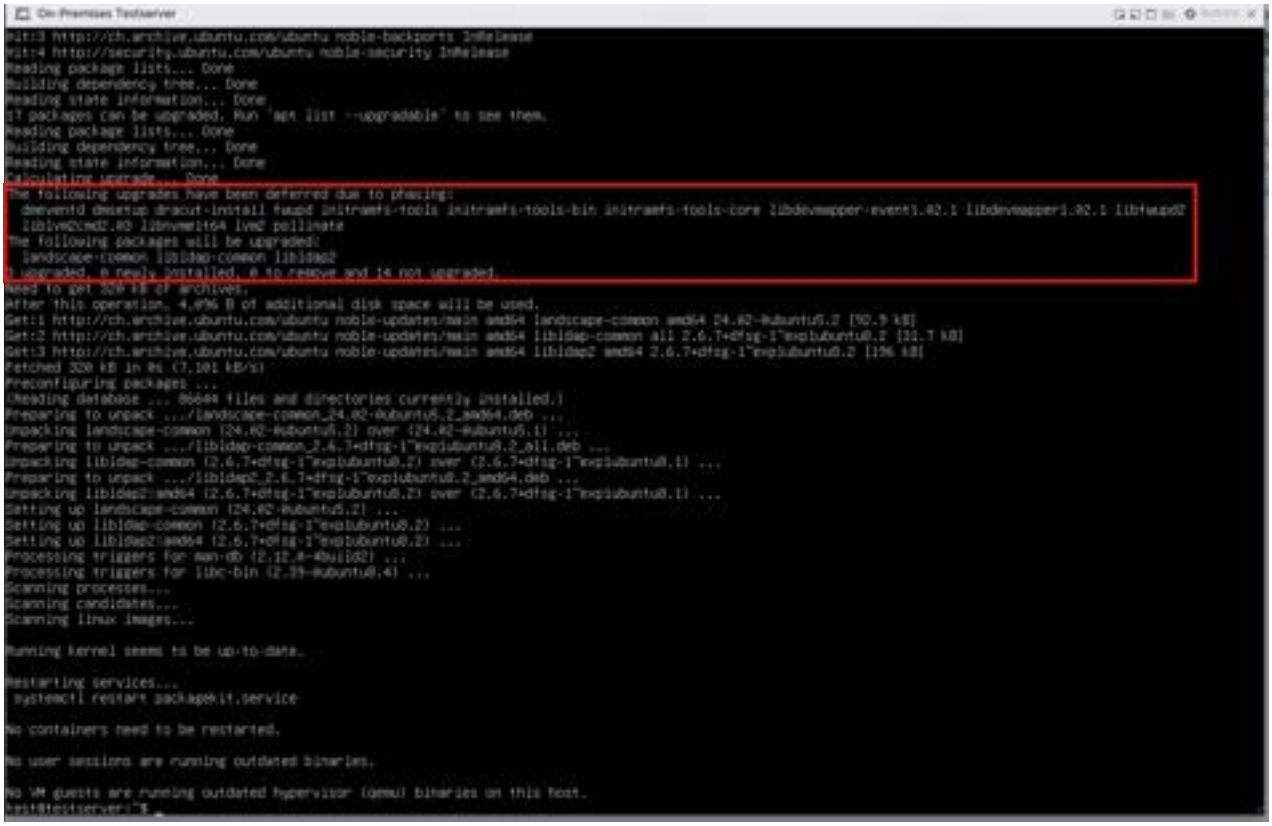


Abbildung 146 Update Ubuntu Server

9. Installation der Testing-Tools

- Installiere alle relevanten Test-Tools:
  - sudo apt install -y net-tools iperf3 traceroute speedtest-cli
- Damit ist die Installation des **On-Premises Testservers** abgeschlossen.

14.4.3 AWS EC2 Testserver Installation

1. Navigiere zu AWS EC2 Dashboard

- Gehe zur AWS-Konsole und öffne das **EC2 Dashboard**
- Klicke auf **«Launch Instance»**.



Abbildung 147 Navigiere zu AWS EC2 Dashboard

2. EC2-Einstellungen konfigurieren

- **Name:** AWS EC2 Testserver A
- **Application and OS Images:** Ubuntu 24.04 LTS
- **Instance Type:** t3.micro
- **Key pair name:** ssh-key
- **VPC:** AWS-VPC
- **Subnet:** AWS-SUBNET-A
- **Auto-assign public IP:** Disable
- **Firewall:** Create security group
  - **Security group name:** aws-ec2-testserver-a
  - **Description:** Security group for Testserver in AZ A
  - **Inbound Security Group Rules:**
    - **Type:** All Traffic
    - **Source type:** Custom
    - **Source:** 10.100.0.0/16, 10.1.0.0/16
- **Advanced network configuration:**
  - **Primary IP:** 10.100.10.20
- **Configure storage:** 25 GB
- Klicke auf **«Launch Instance»**.

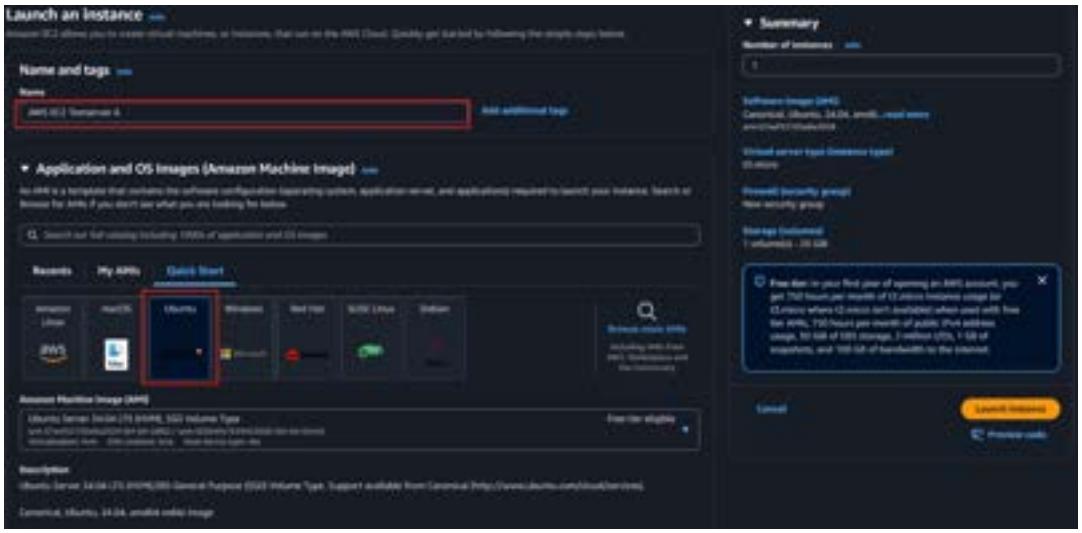


Abbildung 148 EC2-Einstellungen konfigurieren 1

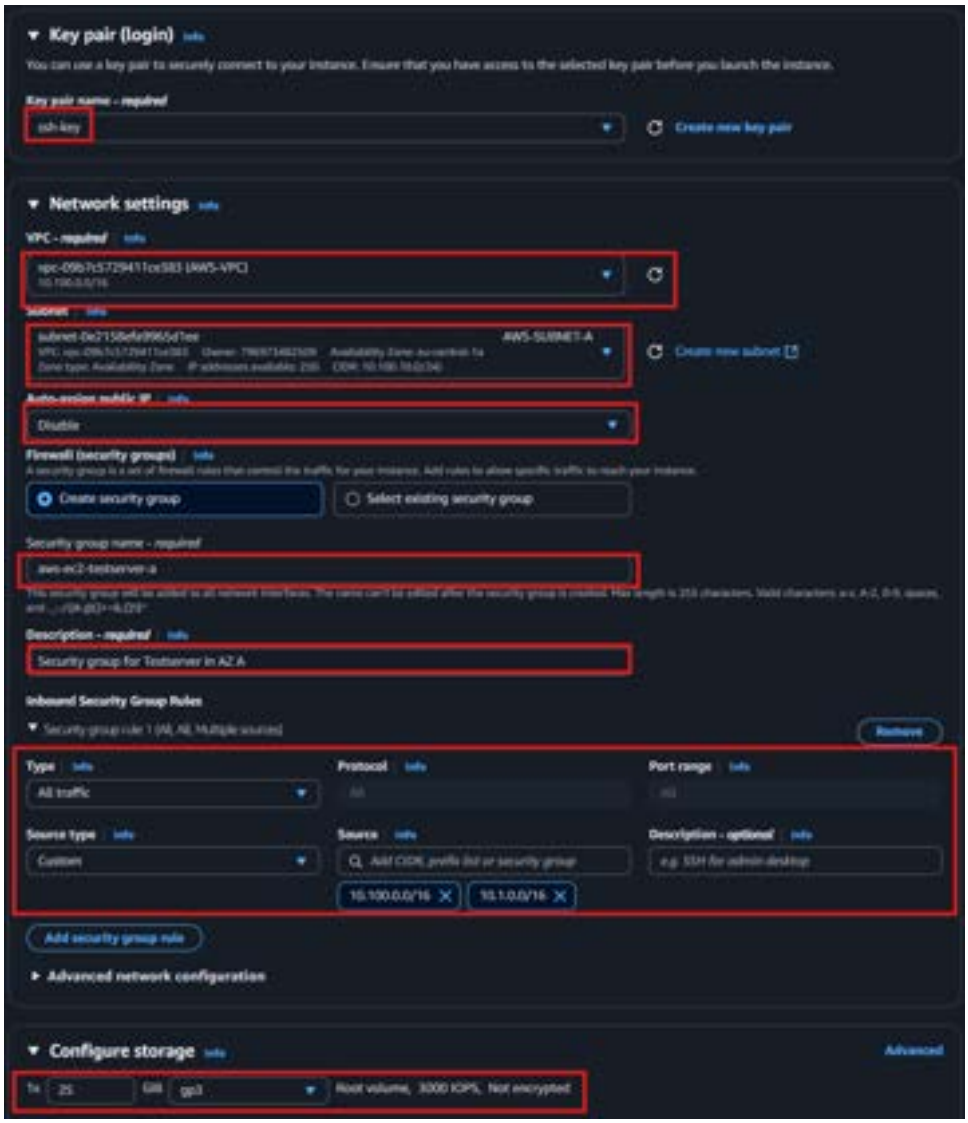


Abbildung 149 EC2-Einstellungen konfigurieren 2

Wichtig: Erstelle zwei weitere Testserver mit folgenden Parametern.

AWS EC2 Testserver B:

- **Name:** AWS EC2 Testserver B
- **Application and OS Images:** Ubuntu 24.04 LTS
- **Instance Type:** t3.micro
- **Key pair name:** ssh-key
- **VPC:** AWS-VPC
- **Subnet:** AWS-SUBNET-B
- **Auto-assign public IP:** Disable
- **Firewall:** Create security group
    - **Security group name:** aws-ec2-testserver-b
    - **Description:** Security group for Testserver in AZ B
    - **Inbound Security Group Rules:**
        - **Type:** All Traffic
        - **Source type:** Custom
        - **Source:** 10.100.0.0/16, 10.1.0.0/16
- **Advanced network configuration:**
    - **Primary IP:** 10.100.20.20
- **Configure storage:** 25 GB
- Klicke auf **«Launch Instance»**.

AWS EC2 Testserver C:

- **Name:** AWS EC2 Testserver C
- **Application and OS Images:** Ubuntu 24.04 LTS
- **Instance Type:** t3.micro
- **Key pair name:** ssh-key
- **VPC:** AWS-VPC
- **Subnet:** AWS-SUBNET-C
- **Auto-assign public IP:** Disable
- **Firewall:** Create security group
    - **Security group name:** aws-ec2-testserver-C
    - **Description:** Security group for Testserver in AZ C
    - **Inbound Security Group Rules:**
        - **Type:** All Traffic
        - **Source type:** Custom
        - **Source:** 10.100.0.0/16, 10.1.0.0/16
- **Advanced network configuration:**
    - **Primary IP:** 10.100.30.20
- **Configure storage:** 25 GB
- Klicke auf **«Launch Instance»**.

3. Konfiguration überprüfen

- Wenn alles korrekt konfiguriert wurde, sollte im EC2 Dashboard nun diese drei EC2-Instanzen angezeigt werden

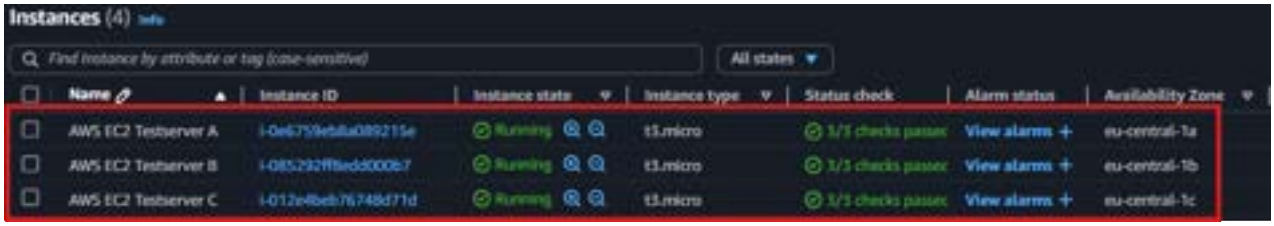


Abbildung 150 Konfiguration überprüfen

14.4.4 Verbindungstest durch Pingen der Instanzen

Nach der Einrichtung der VPN-Verbindung sollte die Erreichbarkeit getestet werden.

1. Terminal oder SSH-Sitzung öffnen

- Falls noch nicht eingeloggt, mit SSH auf eine der Instanzen verbinden:
  - ssh test@10.1.0.20

2. Ping-Befehl ausführen

- Die AWS Instanzen anpingen:
  - ping -c 4 10.100.10.20
  - ping -c 4 10.100.20.20
  - ping -c 4 10.100.30.20

3. Ergebnisse überprüfen

- Falls die Verbindung funktioniert, sollte eine erfolgreiche Ping-Antwort erscheinen.
- Dies sollte ungefähr so aussehen:

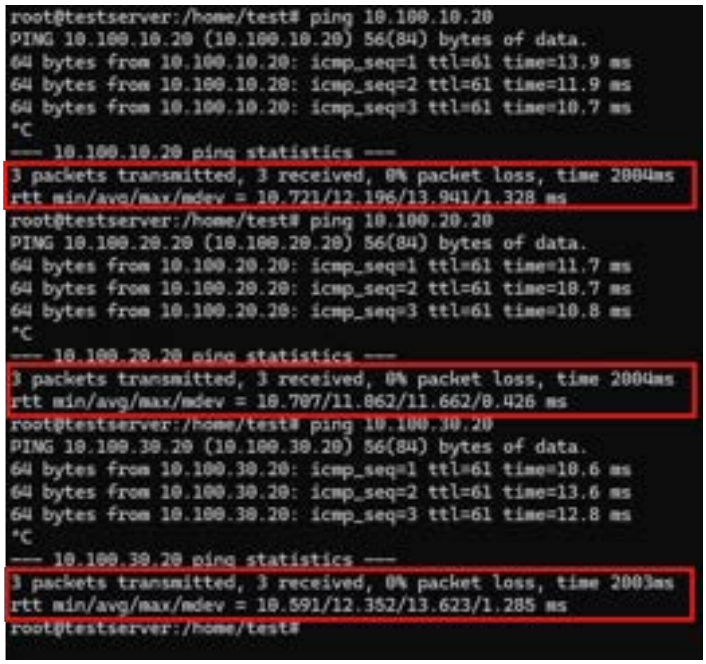


Abbildung 151 Ergebnisse überprüfen

14.5 Installation der Tunnel Überwachung mittels AWS Cloudwatch und AWS SNS

Nachdem die Site-to-Site-VPN-Verbindung erfolgreich eingerichtet wurde, ist es wichtig, deren Verfügbarkeit und Status zu überwachen. Dies kann mit AWS CloudWatch und AWS Simple Notification Service (SNS) erfolgen. In diesem Kapitel wird beschrieben, wie eine Tunnel-Überwachung eingerichtet wird, die bei Problemen automatisch eine Benachrichtigung versendet.

14.5.1 AWS SNS Topic erstellen

Jetzt wird in AWS SNS eine Gruppe erstellt, welche die Empfänger der jeweiligen Alarmen enthält.

1. AWS Management Console öffnen

- Navigiere zu SNS: **AWS Console > Simple Notification Service > Topics**
- Wähle : **«Create topic»**

Abbildung 152 AWS Management Console öffnen SNS

2. SNS Topic erstellen

- Wähle den Type: **«Standard»** aus
- Gebe einen Namen für das Topic ein:
  - **AWS-VPN-Monitoring**
- Danach Klicke: **«Create topic»**

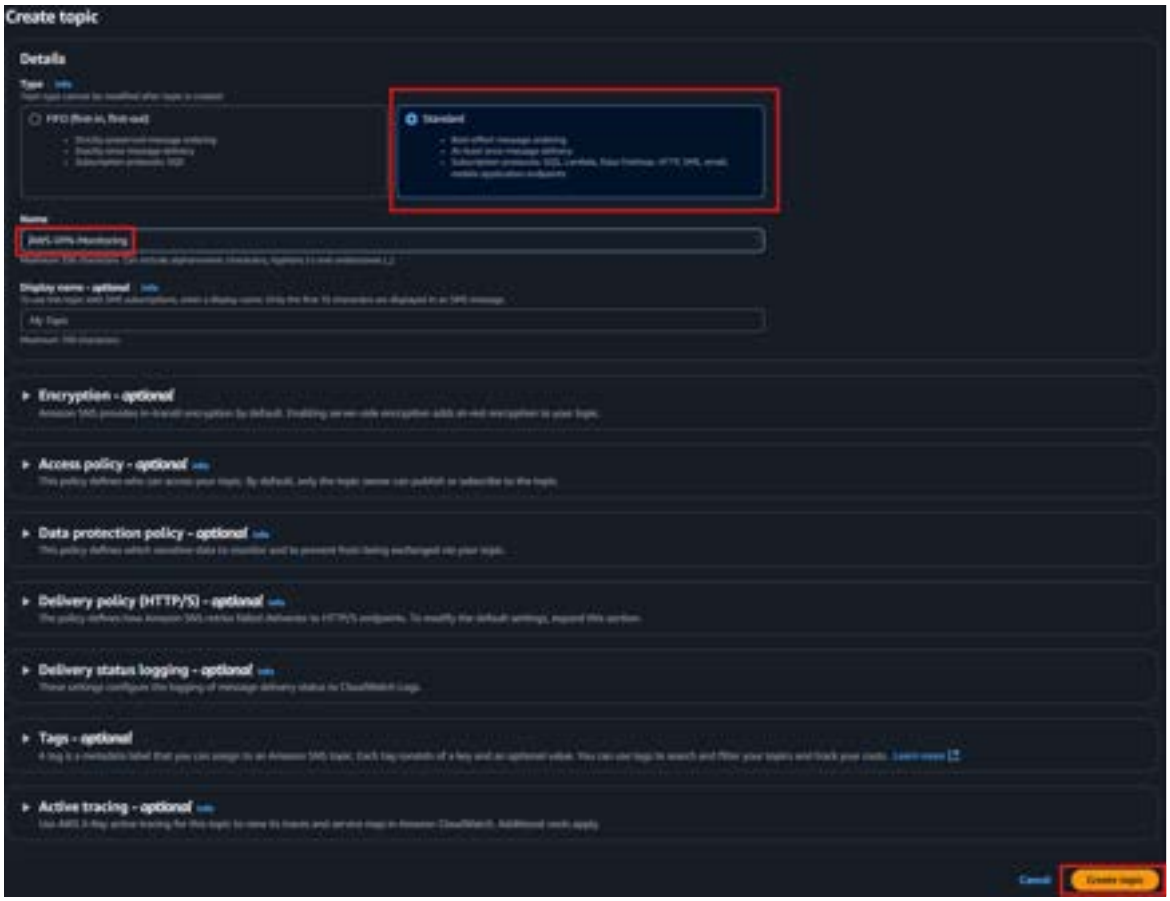


Abbildung 153 SNS Topic erstellen

3. SNS Subscription erstellen

- Klicke auf: **«Create subscription»**
- Wähle das Protocol: **«Email»**
- Gib eine Email Adresse an
- Klicke auf: **«Create Subscription**
- Bestätige die E-Mail aus dem Postfach



Abbildung 154 SNS Subscription erstellen

14.5.2 CloudWatch Alarm erstellen

Jetzt wird ein **Alarm** erstellt, der eine Benachrichtigung sendet, wenn der VPN-Tunnel ausfällt.

1. Navigiere zu CloudWatch > Alarms

- Klicke auf **Create Alarm** (Alarm erstellen).

2. Metrik auswählen

- Klicke auf **Select metric** und wähle:
  - VPN > VPN Connection Metrics
  - Wähle eine Metrik mit dem Namen **TunnelState** für die entsprechende VPN-Verbindung aus

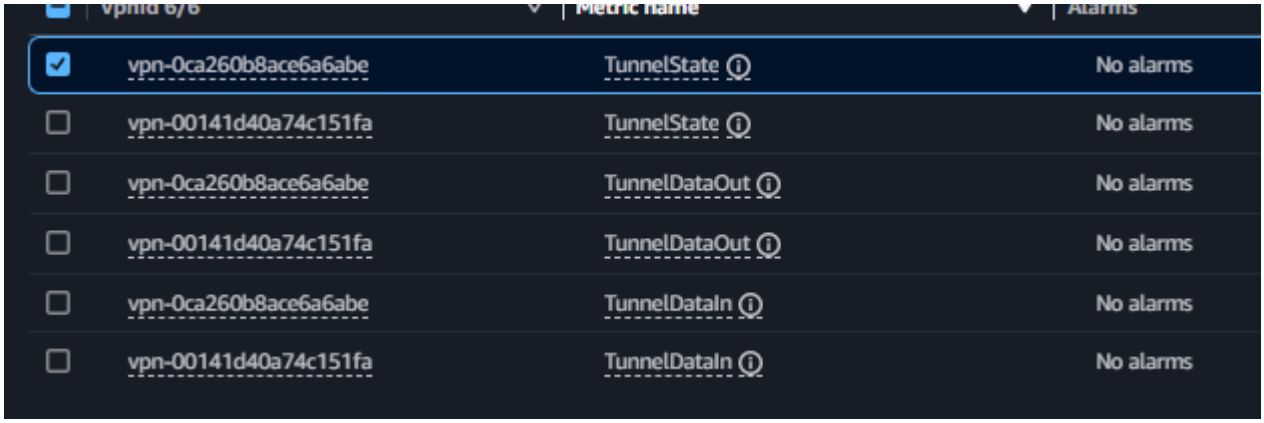


Abbildung 155 Metrik auswählen

3. Definiere die Alarm-Konditionen

Setze folgende werte:

- Metric name: **TunnelState**
- Wähle als VpnId jeweils die ID der jeweiligen VPN-Verbindung
- Statistic: **Maximum**
- Periode: **10 Sekunden**
- Threshhold type: **Static**
- Whenever TunnelState is lower than: **0.9**
- Alarm state Trigger: **In Alarm**
- Send notification to: **AWS-VPN-Monitoring**
- Alarm Name: **VPN-Verbindung-1 Alarm**
- Alarm description: **VPN-Verbindung 1 hat aktuell Probleme**
- Klicke: **«Create alarm»**

Wiederhole diese Schritte für den Alarm der zweiten VPN-Verbindung.

Wenn alles richtig konfiguriert wurde, sollte es nun so aussehen:



Abbildung 156 CloudWatch Alarms überprüfen

Und sobald eine VPN-Verbindung nicht mehr laufen sollte, wird so ein E-Mail gesendet:

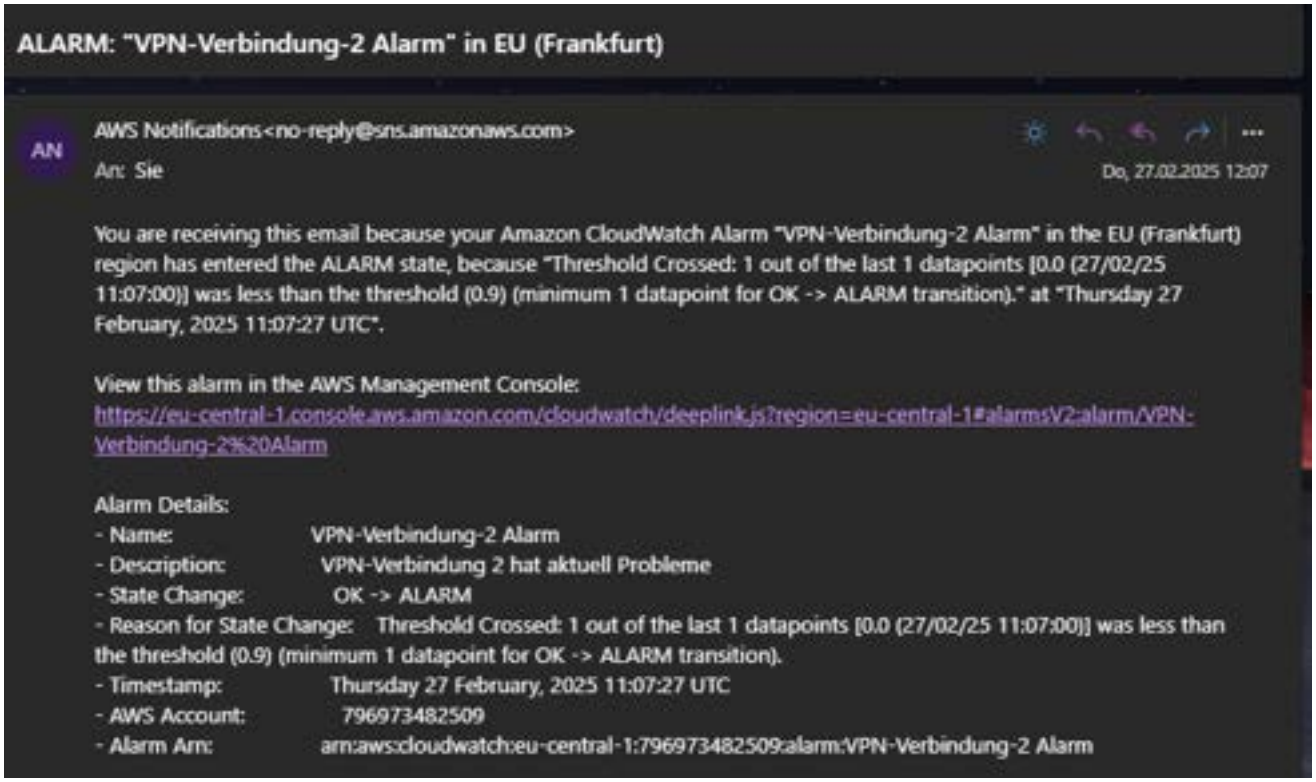


Abbildung 157 CloudWatch Alarm E-Mail

14.6 Testphase

In folgenden Abschnitten wird die durchgeführte Testphase beschrieben.
Bei der Durchführung der Tests wurde dem definierten Test-Konzept gefolgt.
Es gab keine Abweichungen zu den geplanten Tests.

14.6.1 Testfälle grob mit den Resultaten

Folgende Tabelle stellt alle Testfälle inklusive des jeweiligen Resultats dar:

ID	Testfall	Erfolgreich?
T1	**Netzwerk-Konnektivitätstest**	**JA**
T2	**VPN-Performance-Test**	**JA**
T3	**IPSec-Tunnel-Statusprüfung**	**JA**
T4	**Hochverfügbarkeits-Failover-Test**	**JA**
T5	**CloudWatch-Monitoring-Test**	**JA**
T6	**Backup-Recovery-Konzept Test**	**JA**

Tabelle 55 Testfälle grob mit Resultaten

14.6.2 Funktionale Anforderungen mit den Resultaten

Folgende Tabelle zeigt die funktionalen Anforderungen und ob diese erfüllt wurden oder nicht:

ID	Testfall	Erfolgreich?
FA1	Beide OPNsense Instanzen wurden korrekt installiert und konfiguriert.	**JA**
FA2	Die Infrastruktur auf der AWS Seite wurde korrekt und nach besten Standards geplant und aufgebaut.	**JA**
FA3	Die VPN Verbindung zwischen On-Premises und AWS kann erfolgreich aufgebaut werden.	**JA**
FA4	Die korrekte BGP Konfiguration ermöglicht das Routing der verschiedenen Netzen zwischen On-Premises und AWS.	**JA**
FA5	Das Monitoring System liefert korrekte Daten und kann bei Ausfällen Mitteilungen an bestimmte Personen senden.	**JA**
FA6	Die Connectivity-, Failover- und Performancetests liefern Werte innerhalb der definierten Schwellwerten.	**JA**

Tabelle 56 Funktionale Anforderungen mit Resulaten

14.6.3 Testfälle detailliert mit Resultat

In diesem Abschnitt werden alle Resultate durchgeführten Tests inklusive der Beweise zu den Ergebnissen beschrieben:

1. Testfall

ID: T1	Abgedeckte Anforderung: FA3, FA4, FA6	Netzwerk-Konnektivitätstest
Tester	Pablo Wynistorf	
Datum	28.02.2025	
Testszenario	Mit diesem Testszenario wird überprüft, ob die Netzwerkverbindungen den Vorgaben entsprechend funktionieren.	
Testvoraussetzungen	• Alle Netzwerkgeräte (Switches, Firewalls, Router) gemäss Netzplan müssen eingeschaltet sein • Netzwerkinterfaces müssen nach der Anleitung konfiguriert sein Alle relevanten IP-Adressen müssen zugewiesen sein.	
Testmethode	Manuelles Testen	
Testschritte	1. **Ping-Test:** Führe ping-Befehl vom On-Premises-Testserver zu einem AWS-Testserver durch. **Command:** ○ ping 10.100.10.20 ○ ping 10.100.20.20 ○ ping 10.100.30.20 2. **Traceroute-Test:** Überprüfe die Netzwerkpfade mit traceroute oder mtr. **Command:** ○ traceroute 10.100.10.20 ○ traceroute 10.100.20.20 ○ traceroute 10.100.30.20 5. **BGP-Routing-Test:** Verifiziere die BGP-Routen über OPNsense Dashboard: Routing → Diagnostics → BGP	
Erwartete Resultate	• **Ping-Test:** Alle definierten Ziele sind erreichbar, keine Paketverluste. • **Traceroute:** Der Netzwerkpfad folgt der erwarteten Route gemäss Netzplan ohne unerwartete Hops. • **BGP-Test:** Die erwarteten BGP-Routen gemäss Netzplan sind aktiv und korrekt verteilt.	

Tatsächliche Resultate

- **Ping-Test:**

Alle im Testfall erwähnten IP-Adressen konnten erfolgreich erreicht werden.

```
test@testserver:~$ ping 10.100.10.20
PING 10.100.10.20 (10.100.10.20) 56(84) bytes of data.
64 bytes from 10.100.10.20: icmp_seq=1 ttl=61 time=10.9 ms
64 bytes from 10.100.10.20: icmp_seq=2 ttl=61 time=10.5 ms
64 bytes from 10.100.10.20: icmp_seq=3 ttl=61 time=10.6 ms
^C
--- 10.100.10.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 10.484/10.643/10.862/0.159 ms
test@testserver:~$ ping 10.100.20.20
PING 10.100.20.20 (10.100.20.20) 56(84) bytes of data.
64 bytes from 10.100.20.20: icmp_seq=1 ttl=61 time=10.6 ms
64 bytes from 10.100.20.20: icmp_seq=2 ttl=61 time=9.62 ms
64 bytes from 10.100.20.20: icmp_seq=3 ttl=61 time=9.82 ms
^C
--- 10.100.20.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 9.623/10.011/10.591/0.417 ms
test@testserver:~$ ping 10.100.30.20
PING 10.100.30.20 (10.100.30.20) 56(84) bytes of data.
64 bytes from 10.100.30.20: icmp_seq=1 ttl=61 time=11.3 ms
64 bytes from 10.100.30.20: icmp_seq=2 ttl=61 time=11.1 ms
64 bytes from 10.100.30.20: icmp_seq=3 ttl=61 time=10.9 ms
^C
--- 10.100.30.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 10.919/11.101/11.319/0.165 ms
test@testserver:~$
```

Abbildung 158 Testfall 1 Ergebnis 1

- **Traceroute-Test:**

Der Traceroute-Test ergab zu allen drei Instanzen das erwartete Resultat. Es sind keine unerwarteten Hops aufgetaucht.

```
test@testserver:~$ traceroute 10.100.10.20
traceroute to 10.100.10.20 (10.100.10.20), 30 hops max, 60 byte packets
 1  10.1.0.2 (10.1.0.2)  0.130 ms  0.086 ms  0.051 ms
 2  * * *
 3  * 10.100.10.20 (10.100.10.20)  11.687 ms *
test@testserver:~$ traceroute 10.100.20.20
traceroute to 10.100.20.20 (10.100.20.20), 30 hops max, 60 byte packets
 1  10.1.0.2 (10.1.0.2)  0.088 ms  0.063 ms  0.045 ms
 2  * * *
 3  * * *
 4  * * 10.100.20.20 (10.100.20.20)  11.694 ms
test@testserver:~$ traceroute 10.100.30.20
traceroute to 10.100.30.20 (10.100.30.20), 30 hops max, 60 byte packets
 1  10.1.0.2 (10.1.0.2)  0.093 ms  0.080 ms  0.070 ms
 2  * * *
 3  10.100.30.20 (10.100.30.20)  11.178 ms *  11.108 ms
test@testserver:~$
```

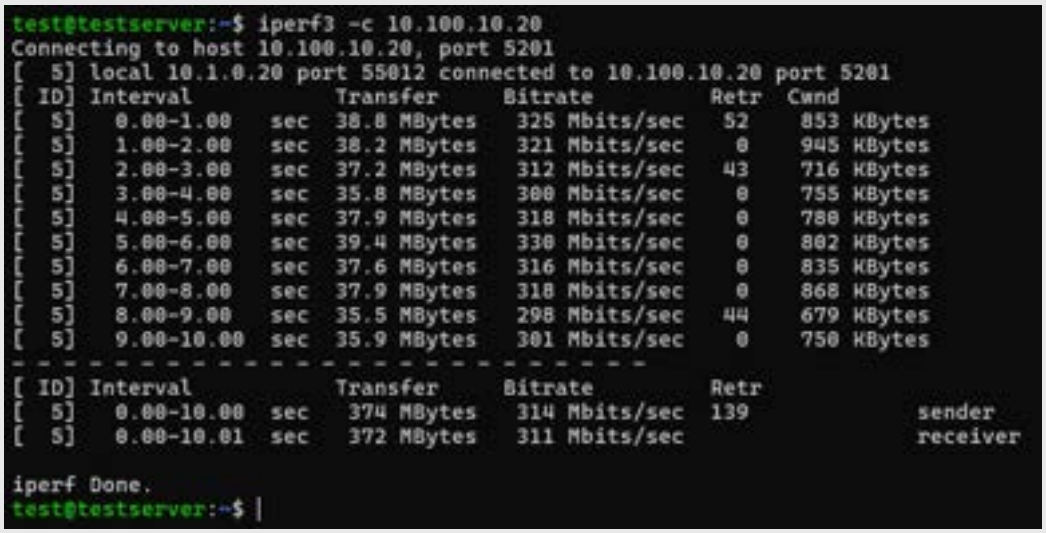
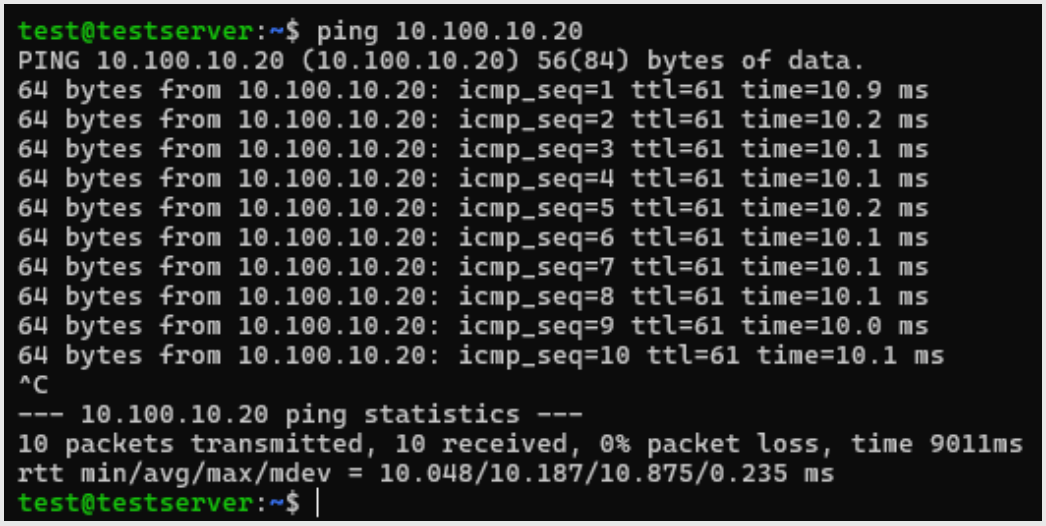
Abbildung 159 Testfall 1 Ergebnis 2

	• **BGP-Test:** Im OPNsense Dashboard konnte man sehen, dass alle Routen zu AWS korrekt erhalten wurden.  *Abbildung 160 Testfall 1 Ergebnis 3*  *Abbildung 161 Testfall 1 Ergebnis 4*
Massnahmen und Empfehlungen	Da in diesem Testfall alle Punkte erreicht wurden, sind keine weitern Konfigurationsmassnahmen erforderlich.

Swisscom (Schweiz) AG
Pablo Wynistorf, GHR-POD-NEX-18
Genfergasse 14
3011 Bern
E-Mail: pablo.wynistorf@swisscom.com

2. Testfall

ID: T2	Abgedeckte Anforderung: FA6	VPN-Performance-Test
Tester	Pablo Wynistorf	
Datum	28.02.2025	
Testszenario	Dieser Test überprüft, ob die Bandbreite der VPN-Verbindung den Erwartungen entspricht.	
Testvoraussetzungen	• VPN-Tunnel zwischen On-Premises und AWS muss aktiv sein. • Beide Endpunkte müssen über einen iPerf-Server oder Client verfügen. Kein anderer grosser Datenverkehr sollte während des Tests laufen.	
Testmethode	Manuelles Testen	
Testschritte	1. **iPerf-Server auf AWS-Testinstanz starten:** **Command:** iperf -s 2. **Performence-Test auf On-Premises Testserver ausführen:** **Command**: ○ iperf -c 10.100.10.20 ○ ping 10.100.10.20 3. **Ergebnisse analysieren:** Vergleiche die gemessene Bandbreite mit den erwarteten Werten.	
Erwartete Resultate	• Die gemessene Bandbreite entspricht der erwarteten VPN-Kapazität von 100 Mbit/s. • Die Latenz ist im definierten Bereich von ca. 25ms	
Tatsächliche Resultate	Der Performance Test hat sich als erfolgreich herausgestellt. Die erwartete Bandbreite von 100 Mbit/s wurde sehr gut erreicht. Die durchschnittliche Geschwindigkeit beläuft sich auf 314 Mbit/s. Dies ist fast dreimal so schnell wie als Anforderung gestellt wurde. Auch der Laten-Test war erfolgreich. Als Anforderung verlangt war der Bereich um ca. 25ms. Die durchschnittliche Latenzzeit war bei 10.2ms. Dies ist die hälfte der Latenz welche in den Anforderungen gestellt wurde.	

	Geschwindigkeits-Test:  *Abbildung 162 Testfall 2 Ergebnis 1* Latenz-Test:  *Abbildung 163 Testfall 2 Ergebnis 2*
Massnahmen und Empfehlungen	Da in diesem Testfall alle Punkte erreicht wurden, sind keine weitern Konfigurationsmassnahmen erforderlich.

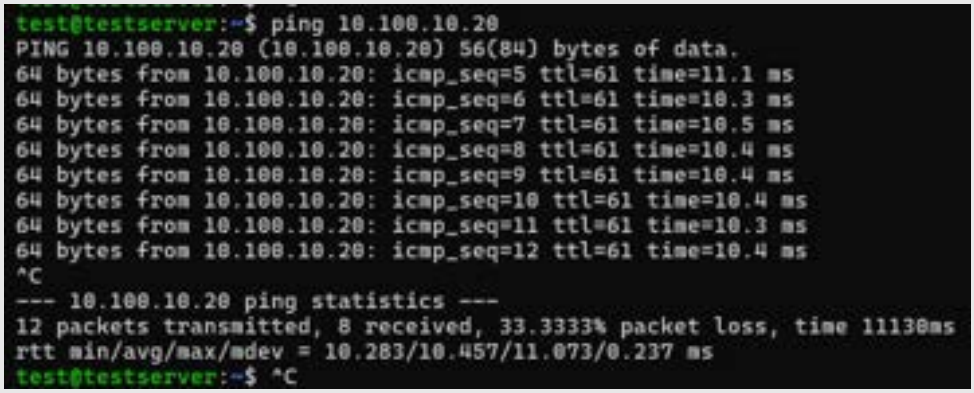
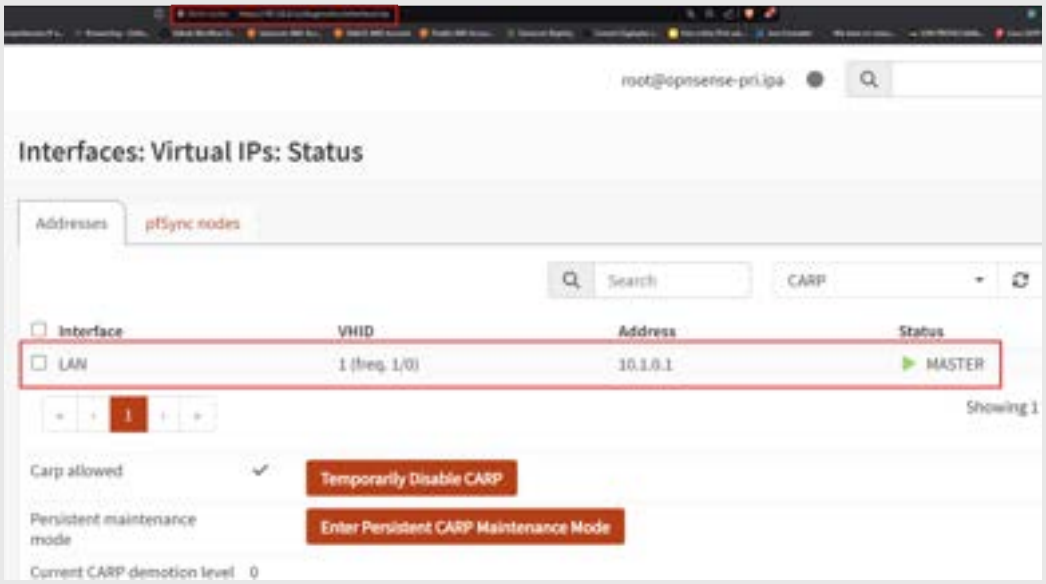
3. Testfall

ID: T3	Abgedeckte Anforderung: FA1, FA2, FA3	IPSec-Tunnel-Statusprüfung
Tester	Pablo Wynistorf	
Datum	28.02.2025	
Testszenario	Sicherstellen, dass die alle VPN-Tunnel zwischen On-Premises und AWS verbunden sind.	
Testvoraussetzungen	• Die VPN-Konfiguration muss nach Anleitung konfiguriert worden sein. OPNsense- und AWS-VPN-Status-Dashboards müssen zugänglich sein.	
Testmethode	Manuelles Testen	
Testschritte	1. **Status der VPN-Tunnel in OPNsense prüfen (Primary und Secondary):** **Navigieren zu:** VPN → IPsec → Status Overview Prüfen, ob alle Tunnel den Status **"Connected"** haben 2. **Status der VPN-Tunnel auf AWS Prüfen:** **Navigieren zu:** AWS Console → VPC → VPN Connections Prüfen, ob alle Tunnel den Status **"UP"** haben	
Erwartete Resultate	Alle vier Tunnel erweisen den Status UP/Connected in beiden Dashboards.	
Tatsächliche Resultate	Alle vier Tunnel sind wie erwartet UP/Connected. Sowie im OPNsense Dashboard als auch im AWS Dashboard. On-Premises VPN-Verbindung 1:  *Abbildung 164 Testfall 3 Ergebnis 1* On-Premises VPN-Verbindung 2:  *Abbildung 165 Testfall 3 Ergebnis 2*	

	AWS VPN-Verbindung 1:  *Abbildung 166 Testfall 3 Ergebnis 3* AWS VPN-Verbindung 2:  *Abbildung 167 Testfall 3 Ergebnis 4*
Massnahmen und Empfehlungen	Da in diesem Testfall alle Punkte erreicht wurden, sind keine weitern Konfigurationsmassnahmen erforderlich.

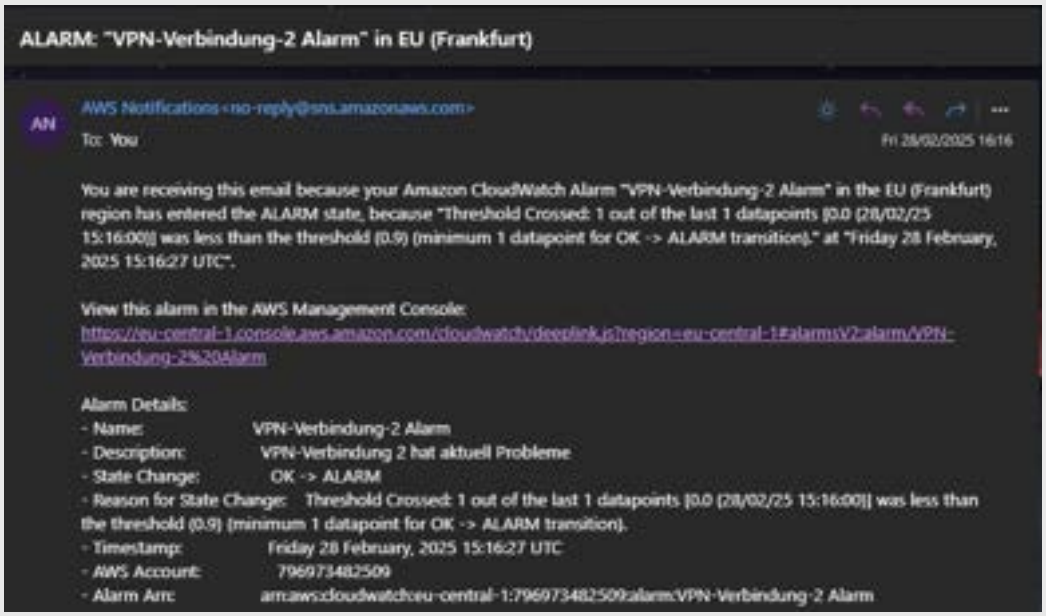
4. Testfall

ID: T4	Abgedeckte Anforderung: FA1, FA6	Hochverfügbarkeits-Failover-Test
Tester	Pablo Wynistorf	
Datum	28.02.2025	
Testszenario	Überprüfung der Hochverfügbarkeit, indem die primäre OPNsense-Instanz deaktiviert wird.	
Testvoraussetzungen	• CARP-Setup mit einer **Primary- und Secondary-OPNsense-Instanz** muss nach Anleitung konfiguriert worden sein. Der HA-Sync-Status zwischen den Instanzen muss auf «**Synced**» sein.	
Testmethode	Manuelles Testen	
Testschritte	1. **Primäre OPNsense-Instanz deaktivieren:** - **Im Dashboard:** Power → Power Off 2. **Sekundäre OPNsense prüfen:** - Status → Unter «Virtual IP» sollte der Status der Backup-Instanz auf **"Master"** wechseln. 3. **VPN-Verbindungen & Routing testen:** - ping zwischen On-Premises & AWS wiederholen. 4. **Nach 5 Minuten primäre Instanz wieder aktivieren:** - Hochfahren der Primary-VM und prüfen, ob sie wieder **Master** wird.	
Erwartete Resultate	• Sekundäre OPNsense übernimmt die virtuelle IP (CARP Failover). • VPN-Tunnel bleibt stabil (keine langen Unterbrechungen). • Firewall- und Routing-Funktionalität bleibt bestehen.	
Tatsächliche Resultate	Dieser Testfall war erfolgreich. Das CARP erkannte den Ausfall der Primary-OPNsense Instanz und konnte sofort die Secondary-OPNsense Instanz zum Master ernennen.  *Abbildung 168 Testfall 4 Ergebnis 1*	

	Die Konnektivität war nach nur ein paar wenigen Sekunden wieder vorhanden und die Testserver konnten sich gegenseitig Pingen.  *Abbildung 169 Testfall 4 Ergebnis 2* Die Primary-OPNsense-Instanz wurde nach dem erneuten Hochfahren wieder als «Master» erkannt.  *Abbildung 170 Testfall 4 Ergebnis 3*
Massnahmen und Empfehlungen	Da in diesem Testfall alle Punkte erreicht wurden, sind keine weitern Konfigurationsmassnahmen erforderlich.

5. Testfall

ID: T5	Abgedeckte Anforderung: FA5	CloudWatch-Monitoring-Test
Tester	Pablo Wynistorf	
Datum	28.02.2025	
Testszenario	Überprüfung, ob Ausfälle über **AWS CloudWatch & E-Mail-Benachrichtigungen** gemeldet werden.	
Testvoraussetzungen	• AWS CloudWatch **Alarm für VPN-Tunnelstatus** muss eingerichtet sein. • AWS SNS muss konfiguriert sein, um **E-Mail-Benachrichtigungen** zu senden. Ein Admin-Benutzer muss Zugriff auf die Logs haben.	
Testmethode	Manuelles Testen	
Testschritte	1. **VPN-Verbindung absichtlich deaktivieren:** - In OPNsense: VPN → IPsec → Status Overview → Disconnect Tunnel. 2. **CloudWatch Dashboard öffnen:** - AWS Console → CloudWatch → Alarms. 3. **Alarm-Status prüfen:** - Alarmstatus muss von **OK → ALARM** wechseln. 4. **E-Mail-Benachrichtigung verifizieren:** - Überprüfung, ob die Alarm-Mail an den Administrator gesendet wurde.	
Erwartete Resultate	• AWS CloudWatch zeigt einen **ALARM** für die unterbrochene VPN-Verbindung. • Eine **E-Mail-Benachrichtigung** wird an die Verantwortlichen gesendet. • Nach Wiederherstellung des Tunnels wechselt der Alarm zurück auf **OK**	
Tatsächliche Resultate	Der Testfall war erfolgreich. Alle erwarteten Resultate wurden erfüllt. CloudWatch zeigt einen Alarm für die Unterbrochene VPN-Verbindung:  *Abbildung 171 Testfall 5 Ergebnis 1*	

	Auch eine Alarm-E-Mail wurde an verantwortliche Personen gesendet.  *Abbildung 172 Testfall 5 Ergebnis 2* Nach dem Wiederherstellen der VPN-Verbindung wurde der Alarm wieder auf OK gesetzt.  *Abbildung 173 Testfall 5 Ergebnis 3*
Massnahmen und Empfehlungen	Da in diesem Testfall alle Punkte erreicht wurden, sind keine weitern Konfigurationsmassnahmen erforderlich.

6. Testfall

ID: T6	Abgedeckte Anforderung: IPA Kriterium	Backup-Recovery-Konzept Test
Tester	Pablo Wynistorf	
Datum	28.02.2025	
Testszenario	Sicherstellen, dass das Backup-System funktionsfähig ist und eine vollständige Wiederherstellung der gesicherten Daten erfolgreich durchgeführt werden kann.	
Testvoraussetzungen	• Ein aktuelles Backup ist vorhanden. • Zugriff auf das Backup-System und Wiederherstellungssoftware ist sichergestellt. Eine Testumgebung steht zur Verfügung, um die Wiederherstellung ohne Risiko für die Produktionssysteme durchzuführen.	
Testmethode	Manuelles Testen	
Testschritte	**1. Backup-Überprüfung:** - Prüfen, ob das Backup vollständig und aktuell ist. **2. Wiederherstellungsprozess einleiten:** - Backup in einer separaten Testumgebung wiederherstellen. - Prüfen, ob die Wiederherstellung ohne Fehler durchläuft. **3. Integritätsprüfung:** - Vergleich der wiederhergestellten Daten mit den Originaldaten. - Prüfung, ob Konfigurationen und Berechtigungen korrekt wiederhergestellt wurden. **4. Systemtests nach Wiederherstellung:** - Testen, ob alle Dienste und Anwendungen nach der Wiederherstellung ordnungsgemäss funktionieren. - Netzwerkverbindungen und Zugriffe testen.	
Erwartete Resultate	• Das Backup kann erfolgreich wiederhergestellt werden. • Alle Daten sind vollständig und ohne Fehler verfügbar. • Die wiederhergestellten Systeme und Dienste funktionieren wie im Originalzustand. Falls Fehler auftreten, werden diese dokumentiert und das Backup-System entsprechend optimiert.	
Tatsächliche Resultate	Der Testfall war erfolgreich. Das Backup konnte erfolgreich wiederhergestellt werden. Auf der Secondary-OPNsense-Instanz wurde der Hostname geändert. Danach habe ich das Backup wiederhergestellt und der Hostname wurde wiederhergestellt.	

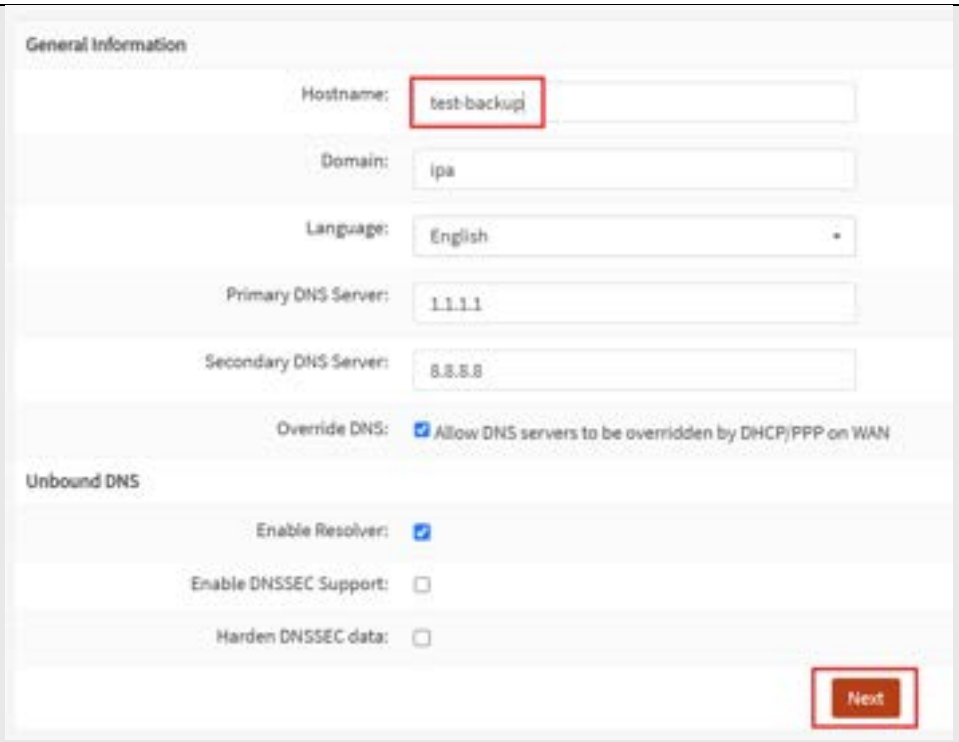


Abbildung 174 Testfall 6 Ergebnis 1

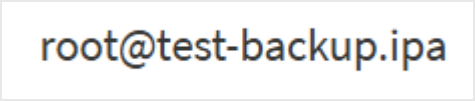


Abbildung 175 Testfall 6 Ergebnis 2

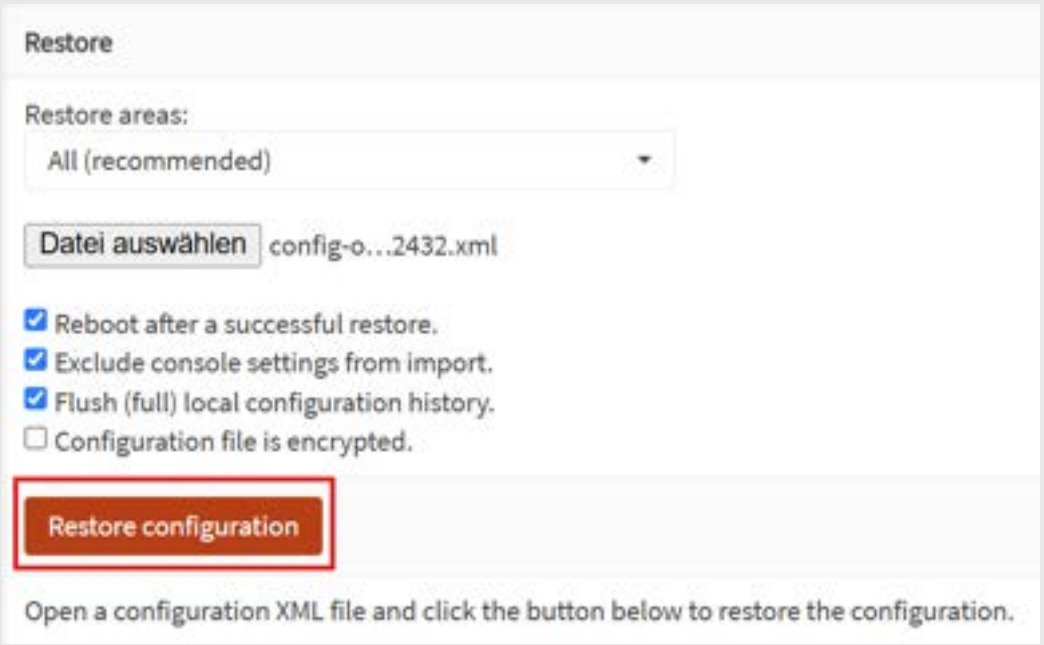
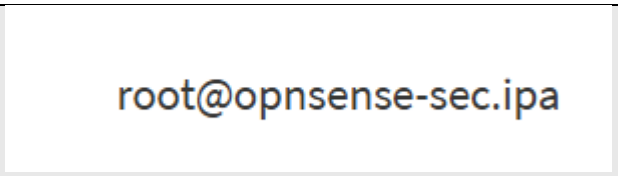


Abbildung 176 Testfall 6 Ergebnis 3

	 *Abbildung 177 Testfall 6 Ergebnis 4*
Massnahmen und Empfehlungen	Da in diesem Testfall alle Punkte erreicht wurden, sind keine weitern Konfigurationsmassnahmen erforderlich.

14.6.4 Fazit der Tests

Alle definierten Testfälle konnten erfolgreich durchgeführt werden und erfüllten oder übertrafen die gesetzten Erfolgskriterien. Da damit sämtliche Anforderungen an die Infrastruktur abgedeckt sind, ergibt sich kein weiterer Handlungs- oder Optimierungsbedarf.

15 Einführung

Die folgenden Schritte werden gemäss der geplanten Vorgehensweise zur Evaluierung und Dokumentation der umgesetzten Lösung durchgeführt. Da es sich um eine neu entwickelte Lösung handelt und kein bestehendes System ersetzt wurde, liegt der Fokus auf der Überprüfung der Implementierung, der Bewertung der erreichten Ziele und der Sicherstellung der Betriebsfähigkeit.

15.1 Änderungsprotokoll

Da kein bestehendes System migriert oder erweitert wurde, entfällt ein klassisches Änderungsprotokoll. Stattdessen wird eine Zusammenfassung der implementierten Lösung bereitgestellt, die die wichtigsten Merkmale und Neuerungen beschreibt:

Was wurde umgesetzt?

- Eine Hybrid-Cloud-Konnektivität wurde mittels AWS Site-to-Site VPN und OPNsense-Firewalls hergestellt.
- Das Netzwerk wurde mit BGP-Routing und automatischem Failover für hohe Verfügbarkeit konzipiert.
- Ein Monitoring-System mit CloudWatch und SNS-Alarmierung wurde integriert, um Netzwerkausfälle proaktiv zu erkennen.

Hat die neue Infrastruktur Auswirkungen auf bestehende Systeme?

- Nein, da es sich um eine komplett neue Implementierung handelt, gibt es keine direkten Auswirkungen auf bestehende Netzwerkkomponenten.
- Die Lösung wurde eigenständig aufgebaut und könnte in bestehende Umgebungen integriert werden.

15.2 Dokumentation der Infrastruktur

Die Installation der entwickelten Lösung wurde vollständig dokumentiert, um eine nachvollziehbare und reproduzierbare Implementierung sicherzustellen. Dies umfasst:

- Netzwerkdiagramme zur Veranschaulichung der Verbindung zwischen On-Premises und AWS.
- Konfigurationsanleitungen für die VPN-Tunnel, Firewall-Regeln und Routing-Mechanismen.
- Monitoring-Konzepte zur Sicherstellung der Betriebsfähigkeit.
- Test-Konzepte zur Überprüfung der verschiedenen Systeme

Mit dieser Dokumentation ist gewährleistet, dass die Infrastruktur wartbar, erweiterbar und gut verständlich ist.

16 Verzeichnisse

16.1 Abbildungsverzeichnis

Abbildung 1 Swisscom Farben 12
Abbildung 2 Swisscom Schriften 12
Abbildung 3 IPA Ordnerstruktur 14
Abbildung 4 IPA Sicherheitskopien 15
Abbildung 5 Versionsverlauf 15
Abbildung 6 Hermes Phasen 18
Abbildung 7 Freigabe Konzeptphase 22
Abbildung 8 Freigabe Realisierungsphase 22
Abbildung 9 Freigabe Einführungsphase 22
Abbildung 10 Organigramm 27
Abbildung 11 Zeitplan 1 29
Abbildung 12 Zeitplan 2 30
Abbildung 13 Netzplan IST-Situation 57
Abbildung 14 Soll-Situation 1 59
Abbildung 15 Soll-Situation 2 60
Abbildung 16 Gesamtes Netzwerkdiagramm 68
Abbildung 17 VPN-Verbindungs-Architektur 76
Abbildung 18 VM-Erstellung Starten 87
Abbildung 19 Neue virtuelle Maschine 88
Abbildung 20 Name und Gast-Betriebssystem festlegen 88
Abbildung 21 Speicherort auswählen 89
Abbildung 22 Hardware anpassen 1 90
Abbildung 23 Hardware anpassen 2 91
Abbildung 24 ISO-Image einbinden 1 91
Abbildung 25 ISO-Image einbinden 2 92
Abbildung 26 Überprüfung und Abschluss 93
Abbildung 27 Erfolgreiche Konfiguration OPNsense Primary 94
Abbildung 28 Erfolgreiche Konfiguration beide OPNsense-Instanzen 94
Abbildung 29 VM einschalten 94
Abbildung 30 Bootvorgang von ISO starten 95
Abbildung 31 Tastaturlayout auswählen 95
Abbildung 32 Installationsmodus wählen 96
Abbildung 33 ZFS-Storage-Konfiguration 97
Abbildung 34 Festplatte für Installation auswählen 97
Abbildung 35 Installation starten 98
Abbildung 36 Finale Konfiguration 98
Abbildung 37 Grundlegende Konfigurationsübersicht 99
Abbildung 38 Netzwerkschnittstellen zuweisen 99
Abbildung 39 WAN- und LAN-Interfaces festlegen 100
Abbildung 40 Netzwerkkonfiguration prüfen 100
Abbildung 41 LAN-IP-Adresse ändern 101
Abbildung 42 WAN-IP-Adresse ändern 101
Abbildung 43 Zugriff auf das OPNsense-Webinterface 102
Abbildung 44 Erstkonfiguration-Wizard durchlaufen 1 102
Abbildung 45 Erstkonfiguration-Wizard durchlaufen 2 103
Abbildung 46 Zum Firmware-Status navigieren 104
Abbildung 47 Nach Update suchen 104

Abbildung 48 Verfügbare Updates anzeigen 105
Abbildung 49 Neustart erforderlich 105
Abbildung 50 Sicherheitsprüfungsnachweis 1 106
Abbildung 51 Sicherheitsprüfungsnachweis 2 106
Abbildung 52 Sicherheitsprüfungsnachweis 3 107
Abbildung 53 Sicherheitsprüfungsnachweis 4 107
Abbildung 54 Zum Plugin-Menü navigieren 108
Abbildung 55 Plugin suchen 108
Abbildung 56 Plugin Installation starten 109
Abbildung 57 Routing-Menü aktivieren 109
Abbildung 58 Neuen virtuellen Switch erstellen 1 110
Abbildung 59 Neuen virtuellen Switch erstellen 2 110
Abbildung 60 Portgruppe für den Synchronisations-Switch erstellen 111
Abbildung 61 Netzwerkadapter den OPNsense-VMs hinzufügen 111
Abbildung 62 Interface in OPNsense zuweisen 112
Abbildung 63 Schnittstellenkonfiguration prüfen 112
Abbildung 64 OPNsense Sync-Netzwerk konfigurieren 113
Abbildung 65 Firewall-Regeln für OPNsense Sync 1 114
Abbildung 66 Firewall-Regeln für OPNsense Sync 2 115
Abbildung 67 Firewall-Regel überprüfen 115
Abbildung 68 High Availability einrichten 1 116
Abbildung 69 High Availability einrichten 2 116
Abbildung 70 Synchronisationsstatus prüfen 117
Abbildung 71 CARP Virtuelle IPs einrichten 118
Abbildung 72 CARP Virtuelle IPs einrichten OPNsense Primary 119
Abbildung 73 CARP Virtuelle IPs einrichten OPNsense Secondary 119
Abbildung 74 Test der Failover-Funktion 1 120
Abbildung 75 Test der Failover-Funktion 2 120
Abbildung 76 Navigiere zu AWS VPC Dashboard 121
Abbildung 77 VPC-Einstellungen konfigurieren 121
Abbildung 78 Subnetz A (eu-central-1a) 122
Abbildung 79 Subnetz B (eu-central-1b) 122
Abbildung 80 Subnetz C (eu-central-1c) 123
Abbildung 81 Subnetz Konfiguration überprüfen 123
Abbildung 82 Navigiere zu Route Tables 124
Abbildung 83 Route Table erstellen 124
Abbildung 84 Routing-Tabelle mit Subnetzen verbinden 1 125
Abbildung 85 Routing-Tabelle mit Subnetzen verbinden 2 125
Abbildung 86 Konfiguration überprüfen 125
Abbildung 87 Navigiere zu Customer Gateways 126
Abbildung 88 Erstellen des Primären Customer Gateways 126
Abbildung 89 Erstellen des Sekundären Customer Gateways 127
Abbildung 90 Konfiguration überprüfen 127
Abbildung 91 Navigiere zu AWS Transit Gateway 128
Abbildung 92 Transit Gateway erstellen 129
Abbildung 93 Konfiguration überprüfen 129
Abbildung 94 Transit Gateway Attachment erstellen 130
Abbildung 95 Konfiguration überprüfen 131
Abbildung 96 Navigiere zu Route Tables 131
Abbildung 97 Routen bearbeiten 1 131

Abbildung 98 Routen bearbeiten 2 132
Abbildung 99 Routen Konfiguration überprüfen 132
Abbildung 100 Navigiere zu Site-to-Site VPN Connections 133
Abbildung 101 Erstellen der primären Site-to-Site VPN Verbindung 134
Abbildung 102 Erstellen der sekundären Site-to-Site VPN Verbindung 135
Abbildung 103 Navigiere zu Site-to-Site VPN Connections 136
Abbildung 104 VPN-Konfigurationsdateien herunterladen 136
Abbildung 105 VPN-Tunnel-Eintrag erstellen 137
Abbildung 106 Tunnel 1 Phase 1 Konfigurieren 1 138
Abbildung 107 Tunnel 1 Phase 1 Konfigurieren 2 138
Abbildung 108 Tunnel 1 Phase 2 Konfigurieren 1 139
Abbildung 109 Tunnel 1 Phase 2 Konfigurieren 2 140
Abbildung 110 Tunnel 2 Phase 1 Konfigurieren 1 141
Abbildung 111 Tunnel 2 Phase 1 Konfigurieren 2 142
Abbildung 112 Tunnel 2 Phase 2 Konfigurieren 143
Abbildung 113 VPN Konfiguration überprüfen 144
Abbildung 114 IPsec Konfiguration überprüfen 146
Abbildung 115 BGP Aktivieren und Grundkonfiguration 147
Abbildung 116 BGP Neighbors hinzufügen 1 148
Abbildung 117 BGP Neighbors hinzufügen 2 148
Abbildung 118 BGP Neighbors hinzufügen 3 149
Abbildung 119 Überprüfung der BGP Konfiguration 150
Abbildung 120 BGP Aktivieren und Grundkonfiguration 151
Abbildung 121 BGP Neighbors hinzufügen 1 152
Abbildung 122 BGP Neighbors hinzufügen 2 152
Abbildung 123 BGP Neighbors hinzufügen 3 153
Abbildung 124 Überprüfung der BGP-Konfiguration 154
Abbildung 125 Neue Firewall Regel hinzufügen 155
Abbildung 126 Firewall Regel konfigurieren 156
Abbildung 127 Firewall Rule-Konfiguration überprüfen 156
Abbildung 128 VM-Erstellung starten 157
Abbildung 129 Wähle «Create a new virtual machine» 157
Abbildung 130 Name und Gast-Betriebssystem festlegen 158
Abbildung 131 Speicherort auswählen 158
Abbildung 132 Hardware anpassen 1 159
Abbildung 133 Hardware anpassen 2 160
Abbildung 134 ISO-Image einbinden 1 161
Abbildung 135 ISO-Image einbinden 2 161
Abbildung 136 Überprüfung und Abschluss 162
Abbildung 137 VM einschalten 162
Abbildung 138 Sprache auswählen 163
Abbildung 139 Tastaturlayout festlegen 164
Abbildung 140 Installationsart wählen 165
Abbildung 141 Netzwerkkonfiguration 166
Abbildung 142 Festplattenpartitionierung 1 167
Abbildung 143 Festplattenpartitionierung 2 167
Abbildung 144 Benutzerkonto einrichten 168
Abbildung 145 SSH-Server installieren 169
Abbildung 146 Update Ubuntu Server 170
Abbildung 147 Navigiere zu AWS EC2 Dashboard 171

Abbildung 148 EC2-Einstellungen konfigurieren 1 172
Abbildung 149 EC2-Einstellungen konfigurieren 2 172
Abbildung 150 Konfiguration überprüfen 174
Abbildung 151 Ergebnisse überprüfen 174
Abbildung 152 AWS Management Console öffnen SNS 175
Abbildung 153 SNS Topic erstellen 175
Abbildung 154 SNS Subscription erstellen 176
Abbildung 155 Metrik auswählen 176
Abbildung 156 CloudWatch Alarms überprüfen 177
Abbildung 157 CloudWatch Alarm E-Mail 177
Abbildung 158 Testfall 1 Ergebnis 1 180
Abbildung 159 Testfall 1 Ergebnis 2 180
Abbildung 160 Testfall 1 Ergebnis 3 181
Abbildung 161 Testfall 1 Ergebnis 4 181
Abbildung 162 Testfall 2 Ergebnis 1 183
Abbildung 163 Testfall 2 Ergebnis 2 183
Abbildung 164 Testfall 3 Ergebnis 1 184
Abbildung 165 Testfall 3 Ergebnis 2 184
Abbildung 166 Testfall 3 Ergebnis 3 185
Abbildung 167 Testfall 3 Ergebnis 4 185
Abbildung 168 Testfall 4 Ergebnis 1 186
Abbildung 169 Testfall 4 Ergebnis 2 187
Abbildung 170 Testfall 4 Ergebnis 3 187
Abbildung 171 Testfall 5 Ergebnis 1 188
Abbildung 172 Testfall 5 Ergebnis 2 189
Abbildung 173 Testfall 5 Ergebnis 3 189
Abbildung 174 Testfall 6 Ergebnis 1 191
Abbildung 175 Testfall 6 Ergebnis 2 191
Abbildung 176 Testfall 6 Ergebnis 3 191
Abbildung 177 Testfall 6 Ergebnis 4 192

16.2 Tabellenverzeichnis

Tabelle 1 Swisscom Klassifizierung 13
Tabelle 2 Versionstabelle 16
Tabelle 3 Vergleich Projektmethoden 17
Tabelle 4 Projekt-Meilensteine 19
Tabelle 5 Persönliche Meilensteine 19
Tabelle 6 Standard HERMES-Phasen 19
Tabelle 7 HERMES-Module 20
Tabelle 8 HERMES Meilensteine 21
Tabelle 9 Phasenfreigabe 21
Tabelle 10 Arbeitstage 23
Tabelle 11 IPA Termine 23
Tabelle 12 Informationen Kandidat 24
Tabelle 13 Informationen Verantwortliche Fachkraft 24
Tabelle 14 Informationen Hauptexperte 24
Tabelle 15 Informationen Nebenexperte 25
Tabelle 16 Informationen Berufsbildner 25
Tabelle 17 Arbeitsjournal Tag 1 32
Tabelle 18 Arbeitsjournal Tag 2 34
Tabelle 19 Arbeitsjournal Tag 3 36
Tabelle 20 Arbeitsjournal Tag 4 38
Tabelle 21 Arbeitsjournal Tag 5 40
Tabelle 22 Arbeitsjournal Tag 6 42
Tabelle 23 Arbeitsjournal Tag 7 44
Tabelle 24 Arbeitsjournal Tag 8 46
Tabelle 25 Arbeitsjournal Tag 9 48
Tabelle 26 Arbeitsjournal Tag 10 49
Tabelle 27 Vergleich Soll zu finalem Ist 50
Tabelle 28 Effizienzbewertung 52
Tabelle 29 Mögliche Risiken 61
Tabelle 30 Alternative Umsetzungsmöglichkeiten 61
Tabelle 31 Systemziele 62
Tabelle 32 Persönliche Vorgehensweise 63
Tabelle 33 Funktionale Anforderungen 63
Tabelle 34 Nicht funktionale Anforderungen 63
Tabelle 35 Quellen für die Umsetzung 64
Tabelle 36 Netzwerksegmente 69
Tabelle 37 On-Premises Netzwerksegmente 71
Tabelle 38 On-Premises OPNsense IP-Adressen 72
Tabelle 39 On-Premises OPNsense Ressourcenzuweisung 72
Tabelle 40 AWS-Architektur Komponenten 74
Tabelle 41 VPN-Tunnel-Topologie 77
Tabelle 42 BGP-Peering-Struktur 78
Tabelle 43 Monitoring Schwellwerte, Aktion, Priorität und Dringlichkeit 80
Tabelle 44 Backup-Typen 80
Tabelle 45 Backup-Inhalte 81
Tabelle 46 Backup-Strategie & Häufigkeit 81
Tabelle 47 Testkategorien 82
Tabelle 48 Teststrategien & Testverfahren 82

Tabelle 49 Testfall 1 83
Tabelle 50 Testfall 2 84
Tabelle 51 Testfall 3 84
Tabelle 52 Testfall 4 85
Tabelle 53 Testfall 5 85
Tabelle 54 Testfall 6 86
Tabelle 57 Testfälle grob mit Resultaten 178
Tabelle 58 Funktionale Anforderungen mit Resulaten 178
Tabelle 59 Literatur & Quellenverzeichnis 200
Tabelle 60 Glossar 202
Tabelle 61 Protokoll vom 1. Expertenbesuch 203
Tabelle 62 Protokoll vom 2. Expertenbesuch 204

16.3 Literatur und Quellenverzeichnis

Titel / verwendet für	Quelle	Zugriffsdatum
Unternehmensrichtlinien / Bilder zu Richtlinien	https://brand.swisscom.com/ Zugriff auf Webseite per Default nur für Swisscom Interne. Falls Zugriff erwünscht ist, kann dieser im Login Fenster angefragt werden.	17.02.2025
Swisscom Klassifizierungen / Informationen zu Klassifizierungen	https://wiki.swisscom.com/pages/releaseview.action?pageId=279447410 Zugriff auf Webseite nur für Swisscom Interne.	17.02.2025
Szenario / Informationen zu HERMES Szenario	https://www.hermes.admin.ch/hermes5/de/projektmanagement/verstehen/szenarien.html	18.02.2025
Phasen und Meilensteine / Informationen zu HERMES Phasen	https://www.hermes.admin.ch/hermes5/de/projektmanagement/verstehen/phasen-und-meilensteine.html	18.02.2025
Module / Informationen zu HERMES Modulen	https://www.hermes.admin.ch/hermes5/de/projektmanagement/verstehen/module.html	18.02.2025
Projektmetode	https://de.smartsheet.com/agile-vs-scrum-vs-waterfall-vs-kanban	20.02.2025
AWS Dokumentationen	https://docs.aws.amazon.com/ Von dieser Website stammen alle Fachspezifischen Informationen für die Umsetzung der AWS Infrastruktur.	20.02.2025 – 27.02.2025
OPNsense Dokumentation	https://docs.opnsense.org/ Von dieser Website stammen alle Fachspezifischen Informationen für die Einrichtung und Konfiguration der OPNsense Router.	20.02.2025 – 27.02.2025
VPN Setup	https://medium.com/@swordfish291/opnsense-firewall-site-to-site-vpn-configuration-to-aws-vpc-6d12c2456ea Diese Webseite wurde zur Konfiguration der Site-to-Site VPN verwendet.	20.02.2025 – 27.02.2025
ChatGPT	https://chatgpt.com/ ChatGPT wurde verwendet um einige Verständlichkeitsfragen zu beantworten und Texte grammatikalisch zu überarbeiten.	Täglich
OPNsense High Availability Setup	https://www.youtube.com/watch?v=I5n3QXOlxmw Dieses YouTube Video wurde verwendet um Hochverfügbarkeit für OPNsense zu konfigurieren.	20.02.2025 – 24.02.2025

Tabelle 57 Literatur & Quellenverzeichnis

17 Glossar

Begriff	Erläuterung
AES	Advanced Encryption Standard
AS	Autonomus System
ASN	Autonomous System Number
AWS	Amazon Web Services
BB	Berufsbildner
BGP	Border Gateway Protocol
CARP	Common Address Redundancy Protocol
CIDR	Classless Inter-Domain Routing
DHCP	Domain Host Control Protocol
EC2	Elastic Compute Cloud
Gbit/s	Gigabits per second
GHR-POD-NEX-18	Lehrlingsabteilung Swisscom
HA	High Availability
HEX	Hauptexperte
ICMP	Internet Control Message Protocol
IPA	Individuelle Praktische Arbeit
IPSec	VPN Protokoll
LAN	Local Area Network
Mbit/s	Megabits per second
MGMT	Management
NEX	Nebenexperte
OMU99	Swisscom Standort
OPNsense	OPNsense Firewall
SBC-MEV-EIT-BDI	Abteilung in Swisscom Broadcast
SNS	Simple Notification Service
SSD	Solid State Drive
TCP	Transmission Control Protocol
VEX	Validexperte
VF	Verantwortliche Fachkraft

VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAN	White Area Network

Tabelle 58 Glossar

18 Anhang

18.1 Protokoll vom 1. Expertenbesuch

Datum	18.02.2025
Teilnehmer	HEX, VF, KAND
Ort	Online (Microsoft Teams Meeting)
Protokoll	Der Ablauf des Meetings war wie folgt: • Kurze Vorstellungsrunde • Klärung der Rollen in der IPA • Sicherstellung der Rollen- und Aufgabenverteilung. • Klärung von Fragen bezüglich einigen Kriterien • Besprechung Zeitplan • Besprechung 1. Arbeitsjournal • Vereinbarung zweiter Besuchstag • Offene Fragen Die gesamte Besprechungszeit betrug 50 Minuten. Nach dem Meeting habe ich mich noch ca. 10 Minuten mit dem Auftraggeber über das vergangene Meeting ausgetauscht.

Tabelle 59 Protokoll vom 1. Expertenbesuch

18.2 Protokoll vom 2. Expertenbesuch

Datum	28.02.2025
Teilnehmer	HEX, NEX, VF, KAND
Ort	Online (Microsoft Teams Meeting)

Protokoll	Der Ablauf des Meetings war wie folgt:
	• Kurzer Rückblick auf die Projektzeit vom Kandidat
	• Vorstellungsrunde mit dem Nebenexperten
	• Dokument gemeinsam durchgegangen
	• Arbeitsjournal angeschaut → Alles OK
	• Zeitplan angeschaut → Alles OK
	• Kurze Infrastruktur Demo
	• Hinweis Präsentation
	  - Präsentation nach Kriterien Machen
	  - Nicht zu technisch werden
	• Hinweis Demo
	  - 5-10 Minuten
	• Hinweis Fachgespräch
	  - 6 Fragenkomplexe
	  - Maximal 30 Minuten
	  - 3-4 Fragen pro Fragenkomplex
	
	Tipps von Experten bezüglich Abgabe:
	• 15 Minuten vor Abgabetermin abgeben
	• IPA Dokumentationskriterien beachten
	
	Fragen an die Experten:
	• Deklaration Verwendung von ChatGPT → Deklaration im Arbeitsjournal und Quellenverzeichnis

Tabelle 60 Protokoll vom 2. Expertenbesuch

18.3 Anhang auf PkOrg

Im Dokumenten Anhang auf PkOrg wurden folgende Dateien in Form einer ZIP Datei hochgeladen:

- Technischer Netzplan
- VPN-Konfigurationsdatei (vertrauliche Informationen wurden zensiert)
- OPNsense-Config-Backups (vertrauliche Informationen wurden zensiert)
- Zeitplan