OFPPT – ISTA TAZA

Digitale Infrastruktur – Option Systeme und Netzwerke

Abschlussbericht zum Ausbildungsprojekt:

IMPLEMENTIERUNG EINER SICHEREN UND ÜBERWACHTEN AZURE-INFRASTRUKTUR

Studienjahr: 2025–2026

Regie: Youssef Kachmar – Driss Jhilal; **Betreuung: Majid Lamkadam**

DANKE

Wir möchten allen, die zum Gelingen dieses letzten Ausbildungsprojekts beigetragen haben, unseren aufrichtigen Dank aussprechen.

Zunächst möchten wir Herrn Majid Lamkadam und Frau Meriem Mengad, unseren Betreuern, für ihre Unterstützung, ihre Anleitung und ihre ständige Verfügbarkeit während des gesamten Projekts danken. Ihre Anleitung und Führung waren maßgeblich für die Strukturierung des Projekts, die Bewältigung der aufgetretenen technischen Schwierigkeiten und die Verbesserung der Qualität der erzielten Ergebnisse.

Wir danken außerdem dem Dozententeam von OFPPT – ISTA TAZA sowie allen Ausbildern der Fachrichtung Digitale Infrastruktur – Systeme und Netzwerke für das während unserer Ausbildung vermittelte Wissen und die technischen Fähigkeiten, die die Grundlage dieses Projekts bildeten.

Abschließend möchten wir uns bei allen bedanken, die während der Implementierung dieser Infrastruktur direkt oder indirekt Hilfe oder Unterstützung geleistet haben (Beratung, Tests, Feedback und Ermutigung).

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

WIEDER AUFNEHMEN

Dieser Bericht beschreibt den Entwurf und die Implementierung einer sicheren und überwachten Azure-Infrastruktur, die im Rahmen eines Abschlussprojekts am OFPPT – ISTA TAZA durchgeführt wurde. Hauptziel ist die Bereitstellung einer konsistenten, segmentierten und kontrollierten Cloud-Umgebung, die das Hosting essenzieller Dienste ermöglicht und gleichzeitig Sicherheit, Verfügbarkeit, Nachverfolgbarkeit und Überwachung gewährleistet.

Die Infrastruktur basiert auf einer in mehrere Subnetze segmentierten Netzwerkarchitektur (Active Directory/DNS, Web, Clients, VoIP, Management). Das Routing erfolgt über Azure-Routingtabellen (UDR), die den Datenverkehr über ein pfSense-Gateway leiten, das als zentrale Firewall (LAN/WAN-Filterung, NAT) dient. Sicherer Fernzugriff wird durch OpenVPN mit Zertifikatsverwaltung (CA- und Client-/Server-Zertifikate) gewährleistet.

Die eingesetzten Dienste umfassen einen Webserver, der über HAProxy als Reverse-Proxy betrieben wird, sowie einen Asterisk-basierten VoIP-Dienst, der durch Anruftests mit Zoiper validiert wurde. Zur Sicherheit ist ein IDS/IPS-System mit Suricata zur Erkennung von Netzwerkangriffen (z. B. Nmap-Scans) implementiert. Die Infrastruktur wird schließlich mit Zabbix (Monitoring) und Wazuh (SIEM/HIDS, Warnmeldungen und Schwachstellenanalyse) überwacht und auditiert.

Die erzielten Ergebnisse demonstrieren die Machbarkeit einer sicheren und professionellen Azure-Umgebung, die in der Lage ist, Dienste zu hosten und gleichzeitig vollständige Transparenz über Status, Leistung und Sicherheitsereignisse zu bieten.

ALLGEMEINE EINLEITUNG

Angesichts der rasanten Entwicklung von Cloud-Technologien migrieren Unternehmen ihre Dienste zunehmend auf Plattformen wie Microsoft Azure, um von deren Flexibilität, Skalierbarkeit und Verfügbarkeit zu profitieren. Diese Migration bringt jedoch auch neue Herausforderungen mit sich, insbesondere in Bezug auf Sicherheit, Zugriffsmanagement, Netzwerksegmentierung, Überwachung und Bedrohungserkennung.

Im Rahmen unserer Ausbildung bei OFPPT – ISTA TAZA zielt dieses Abschlussprojekt darauf ab, eine sichere und überwachte Azure-Infrastruktur zu implementieren. Die Hauptidee besteht darin, eine realistische Umgebung zu schaffen, die einer Unternehmensinfrastruktur ähnelt und wesentliche Komponenten wie eine zentrale Firewall, ein VPN, ein Active Directory, einen Webdienst, einen VoIP-Dienst sowie Überwachungs- und Sicherheitstools integriert.

Um diese Ziele zu erreichen, haben wir einen strukturierten Ansatz gewählt:

den Bedarf analysieren und eine Zielarchitektur definieren;
Entwerfen Sie eine klare Netzwerksegmentierung mittels dedizierter Subnetze;
Routingsteuerung mittels UDRs, um den Durchtritt durch das Sicherheitsgateway zu erzwingen;
Dienste (AD/DNS, Web, VoIP) einrichten und deren Funktionsfähigkeit überprüfen;
Stärkung der Sicherheit durch die Integration von Suricata (IDS/IPS);
Überwachung und Transparenz über Zabbix und Wazuh sicherstellen;
um Tests durchzuführen, um die Konformität und Stabilität der Infrastruktur zu bestätigen.
Dieser Bericht ist in Kapitel unterteilt, die nacheinander den Projektrahmen, die Bedarfsanalyse, den detaillierten Infrastrukturentwurf sowie die Phasen Sicherheit/Überwachung und Validierung beschreiben. Ziel ist es, eine vollständige, kohärente und benutzerfreundliche Lösung zu präsentieren und Best Practices in den Bereichen Netzwerk, Sicherheit und Systemadministration im Kontext der Azure-Cloud hervorzuheben.

KAPITEL 1: PROJEKTRAHMEN

Die Bereitstellung einer sicheren Cloud-Infrastruktur erfordert ein umfassendes Verständnis der Geschäftsanforderungen, -beschränkungen und -ziele. In der Praxis muss eine Cloud-Infrastruktur die Verfügbarkeit von Diensten, den Datenschutz, die Zugriffskontrolle und Überwachungsfunktionen gewährleisten, um Vorfälle schnell zu erkennen und zu beheben.

In diesem Kapitel stellen wir den allgemeinen Rahmen des Projekts, den Kontext, in dem es durchgeführt wurde, und die Ziele vor, die wir durch die Implementierung einer sicheren und überwachten Azure-Infrastruktur erreichen wollten.Die

1.1 Projektkontext

In den letzten Jahren hat sich Cloud Computing für viele Unternehmen zu einer strategischen Entscheidung entwickelt. Azure ermöglicht die schnelle Bereitstellung von Ressourcen (Netzwerke, virtuelle Maschinen, Speicher) und bietet gleichzeitig Managed Services, die den Betrieb vereinfachen. Einfache Bereitstellung allein genügt jedoch nicht: Eine Cloud-Infrastruktur muss nach Sicherheitsprinzipien (Segmentierung, Filterung, Verschlüsselung, Protokollierung) und Leistungsprinzipien (kontrolliertes Routing, optimierter Datenverkehr) konzipiert sein.

Im Rahmen unseres Projekts haben wir eine Netzwerkarchitektur auf Azure aufgebaut, die auf Folgendem basiert:

- eine Segmentierung in dedizierte Teilnetze (Dienste, Kunden, Management, VoIP);
- ein pfSense-Sicherheitsgateway, das als zentrale Firewall fungiert;
- sicherer Fernzugriff über OpenVPN;
- essentielle Dienste: Active Directory / DNS, Webserver, VoIP;
- Sicherheits- und Überwachungstools: Suricata, Zabbix, Wazuh.

Ziel ist es, eine konsistente, sichere und überschaubare Umgebung zu schaffen, die es uns ermöglicht, eine moderne „Unternehmensarchitektur“ in der Cloud zu veranschaulichen.

1.2 Projektziele

Das übergeordnete Ziel des Projekts ist die Einrichtung einer sicheren und überwachten Azure-Infrastruktur, die in der Lage ist, Dienste zu hosten und gleichzeitig ein hohes Maß an Kontrolle und Transparenz zu gewährleisten.

Die konkreten Ziele sind:

- Entwerfen Sie eine segmentierte Netzwerkarchitektur (VNet + Subnetze), die an die Rollen der Maschinen angepasst ist;
- Beherrschung des Routings mithilfe von Azure-Routingtabellen (UDR), um das Routing über pfSense zu erzwingen;
- Bereitstellung und Sicherung eines VPN (OpenVPN) für den Fernzugriff;
- Active Directory / DNS für die zentrale Authentifizierung und Clientverwaltung einrichten;
- Veröffentlichung eines Webdienstes über HTTPS mittels eines Reverse-Proxys (HAProxy);
- Implementieren Sie einen VoIP-Dienst (Asterisk) und validieren Sie ihn mit Anrufen über Zoiper;
- Stärkung der Netzwerksicherheit durch ein IDS/IPS (Suricata);
- Überwachung und Protokollierung über Zabbix und Wazuh bereitstellen;
- Die Lösung wird durch eine Reihe technischer Tests validiert.

1.3 Untersuchung der bestehenden Situation

Bevor wir unsere Lösung entwerfen, ist es wichtig, die allgemein üblichen Ansätze zur Sicherung und Überwachung einer Netzwerkinfrastruktur sowie die Einschränkungen zu untersuchen, die sich ergeben, wenn keine strukturierte Architektur implementiert wird.

In vielen Umgebungen beobachten wir:

- Netzwerke mit geringer oder keiner Segmentierung (alle Rechner im selben Subnetz);
- unzureichende oder uneinheitliche Filterung (Regeln werden maschinell angewendet);
- das Fehlen eines sicheren VPN für die Administration;
- ein Mangel an zentralisierten Überwachungsinstrumenten;
- eingeschränkte Transparenz bei Angriffen und Sicherheitsereignissen.

1.3.1 Einschränkungen einer nicht segmentierten Infrastruktur

Wenn sich alle Server und Clients im selben Netzwerk befinden, kann die Kompromittierung eines Rechners (z. B. einer Client-Workstation) die Ausbreitung auf andere kritische Dienste (Active Directory, Web, VoIP) begünstigen. Die fehlende logische Trennung vergrößert die Angriffsfläche und verringert die Kontrolle über den Netzwerkverkehr.

1.3.2 Einschränkungen einer Infrastruktur ohne zentrale Firewall

Ohne ein zentrales Sicherheitsgateway (wie pfSense/Firewall) wird die Datenverkehrskontrolle schwierig. Regeln sind oft verstreut, inkonsistent und schwer zu überprüfen. Dies birgt Risiken:

- unfreiwillige Offenlegung von Dienstleistungen;
- offene, unkontrollierte Ports;
- Schwierigkeiten bei der Anwendung einer einheitlichen Sicherheitsrichtlinie.

1.3.3 Grenzen einer Infrastruktur ohne Überwachung und Erkennung

Ohne Überwachung lassen sich Ausfälle nur schwer vorhersehen und die Leistung nur schwer messen. Ohne IDS/IPS oder SIEM können Angriffe (Scans, Ausnutzungsversuche) unentdeckt bleiben. Im Falle eines Vorfalls verlangsamt das Fehlen zentralisierter Protokolle die Analyse und Reaktion.

1.4 Vorgeschlagene Lösung

Um diese Einschränkungen zu beheben, basiert unsere Lösung auf einer Azure-Architektur, die Folgendes integriert:

- **Netzwerksegmentierung:**Erstellung eines VNet und mehrerer dedizierter Subnetze (AD/DNS, Web, Clients, VoIP, Management).
- **Kontrolliertes Routing:**Implementierung von UDR, um den Datenverkehr über pfSense zu leiten.
- **Zentrale Firewall:**pfSense bietet LAN/WAN-Filterung, NAT und eine zentralisierte Sicherheitsrichtlinie.
- **Sicheres VPN:**OpenVPN mit Zertifikaten (CA + Client-/Serverzertifikate).
- **Sichere Veröffentlichung:**HAProxy, um den Webdienst über HTTPS bereitzustellen.
- **Geschäftsdienstleistungen:**Active Directory/DNS, Webserver, VoIP Asterisk.

- Sicherheit & Überwachung: Suricata (IDS/IPS), Zabbix (Überwachung), Wazuh (SIEM/HIDS).

Dieser Ansatz ermöglicht den Aufbau einer robusten Infrastruktur mit erhöhtem Sicherheitsniveau und vollständiger Transparenz über den Status der Dienste und Sicherheitsereignisse.

KAPITEL 2: BEDARFSANALYSE

In diesem Kapitel stellen wir die Anforderungen für die Implementierung unserer sicheren und überwachten Azure-Infrastruktur vor. Dieser Schritt ermöglicht es uns, die erwarteten Funktionalitäten sowie die nicht-funktionalen Anforderungen (Sicherheit, Leistung, Verfügbarkeit usw.) klar zu definieren, um ein stimmiges Design zu gewährleisten, das den Projektzielen entspricht.

2.1 Funktionale Anforderungen:

- **Netzwerksegmentierung (VNet + Subnetze):**Implementierung mehrerer Subnetze zur Trennung von Rollen (AD/DNS, Web, Clients, VoIP, Management) und zur Reduzierung der Angriffsfläche.
- **Controlled Routing (UDR):**Azure-Routingtabellen definieren, um den Datenverkehr über ein Sicherheitsgateway zu leiten.
- **Central Pare-feu (pfSense):**Anwendung einer Filterrichtlinie (LAN/WAN), NAT-Management, Kontrolle des ein- und ausgehenden Datenverkehrs.
- **Sicherer Fernzugriff (OpenVPN):**Implementierung eines verschlüsselten VPNs, das eine sichere Fernadministration über Zertifikate ermöglicht.
- **Verzeichnis- und Auflösungsdienste (AD DS + DNS):**Zentralisierte Authentifizierung, Verwaltung von Arbeitsstationen und Benutzern sowie interne/externe Namensauflösung über DNS (Weiterleitungen).
- **Veröffentlichung eines Webdienstes über HTTPS:**Kontrollierte Bereitstellung eines Webdienstes über einen Reverse-Proxy (HAProxy) mit sicherem Zugriff.
- **VoIP-Dienst (Asterisk):**Einrichtung eines VoIP-Servers, der die Kommunikation über einen SIP-Client (Zoiper) ermöglicht, einschließlich SIP-Konfiguration und Anrufvalidierung.
- **Einbruchserkennung (Suricata):**Verkehrsüberwachung, Erkennung verdächtiger Aktivitäten (z. B. Nmap-Scan) und Generierung von Warnmeldungen.
- **Überwachung und Transparenz (Zabbix + Wazuh):**Überwachung des Service-/VM-Status und Zentralisierung von Sicherheitsereignissen, Warnungen und Schwachstellen.

2.2 Nichtfunktionale Anforderungen:

- **Sicherheit:**Zugriffsverschlüsselung (VPN), Netzwerkfilterung, Segmentierung, Zertifikate, Protokollierung und Bedrohungserkennung.
- **Verfügbarkeit:**Kritische Dienste (pfSense, AD/DNS, Web, VoIP) müssen stabil erreichbar bleiben.
- **Leistung :** Die Architektur muss unnötige Latenzzeiten begrenzen und ein konsistentes und effizientes Routing gewährleisten.
- **Rückverfolgbarkeit / Prüfung:**Speicherung von Protokollen und Warnmeldungen zur Erleichterung der Vorfallanalyse und der Reaktion auf Angriffe.
- **Wartungsfreundlichkeit:**Klare Konfiguration, Dokumentation und Überwachung ermöglichen eine schnelle Administration und Fehlerbehebung.

KAPITEL 3: INFRASTRUKTURPLANUNG

Nach der Bedarfsanalyse folgt die Designphase. Dieser Schritt umfasst die Definition der Gesamtarchitektur der Azure-Infrastruktur, der Netzwerksegmentierung sowie der Sicherheits- und Überwachungskomponenten, die Schutz und Transparenz der Umgebung gewährleisten.

3.1 Allgemeine Architektur der Lösung:

Die Infrastruktur wird auf Microsoft Azure bereitgestellt und basiert auf folgenden Prinzipien:

- ➔ Virtuelles Netzwerk (VNet): Gruppierung mehrerer dedizierter Subnetze entsprechend der Rolle der Maschinen.
- ➔ pfSense wird als zentrales Sicherheitsgateway (Firewall + NAT + VPN) verwendet.
- ➔ Active Directory / DNS für Identitätsmanagement und Namensauflösung.
- ➔ Webserver, der über HAProxy via HTTPS veröffentlicht wird.
- ➔ Asterisk-basierter VoIP-Dienst mit Validierung über Zoiper.
- ➔ Suricata zur Erkennung von Netzwerkangriffen.
- ➔ Zabbix zur Überwachung von Ressourcen und Diensten.
- ➔ Wazuh für die Protokollerfassung, Sicherheitswarnungen und Schwachstellenerkennung.

Diese Architektur zielt darauf ab, eine klare Trennung der Rollen, eine strikte Kontrolle der Abläufe und eine kontinuierliche Überwachung des Zustands der Infrastruktur zu gewährleisten.

Abbildung 1: Gesamtinfrastrukturtopologie (Azure VNet + Subnetze + Rollen)

3.2 Adressierungsplan und Segmentierung (Subnetze):

Die Subnetzbildung ermöglicht die Isolation kritischer Komponenten und begrenzt die Ausbreitung von Angriffen. Die wichtigsten Subnetze sind:

- ➔ AD/DNS-Subnetz: Beherbergt den Domänencontroller und den DNS-Dienst.
- ➔ Web-Subnetz: beherbergt den Webserver und zugehörige Komponenten.
- ➔ Client-Subnetz: Enthält Client-Rechner (Tests und Domänenintegration).
- ➔ VoIP-Subnetz: Beherbergt den Asterisk-Server und gegebenenfalls SIP-Clients.
- ➔ Subnetzverwaltung: reserviert für Administrations- und Überwachungstools (Zabbix/Wazuh).
- ➔ Die Kommunikation zwischen diesen Subnetzen wird durch Routing und pfSense-Regeln gesteuert.

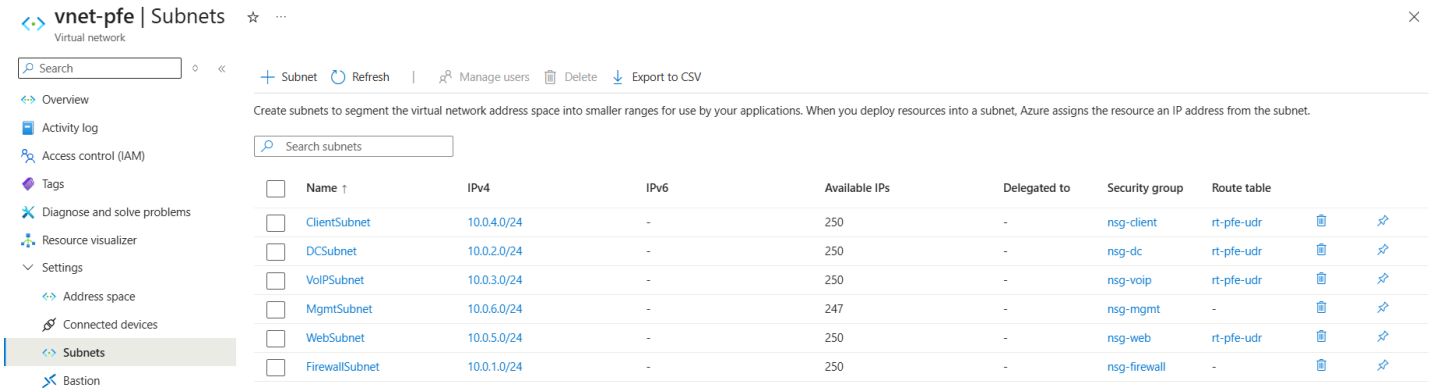

Abbildung 2: Azure-Subnetze (Segmentierung)

Subnet	CIDR	Charge(s) / Workload(s)	IP(s) d'exemple	Objectif
DCSubnet	10.0.2.0/26	Windows Server (AD DS / DNS)	10.0.2.10	Identité + DNS (contrôleur de domaine, résolution interne)
VoIPSubnet	10.0.3.0/26	Asterisk PBX	10.0.3.4	Services SIP / RTP (téléphonie IP)
ClientSubnet	10.0.4.0/24	Client Windows	10.0.4.4	Tests / poste intégré au domaine
WebSubnet	10.0.5.0/24	Serveur Web (ex. Nginx)	10.0.5.10	Application Web interne derrière HAProxy
Management	10.0.6.0/24	Jumpbox, Zabbix, Wazuh	10.0.6.5 10.0.6.6 10.0.6.7	Exploitation / administration / supervision / SIEM

Abbildung 3: Netzwerkadressierungsplan

3.3 Technologische Optionen (pfSense, Azure, OpenVPN usw.)

- **Cloud-Anbieter: Microsoft Azure**

Die Wahl von Microsoft Azure als unsere Infrastructure-as-a-Service-Infrastruktur (IaaS) basiert auf ihrer Zuverlässigkeit, Skalierbarkeit und ihren fortschrittlichen Netzwerkfunktionen. Azure ermöglicht eine detaillierte Segmentierung durch virtuelle Netze (VNets) und Subnetze und bietet vollständige Routing-Kontrolle über benutzerdefinierte Routen (UDRs), was unerlässlich ist, um den Datenverkehr über unsere zentrale Firewall zu leiten.

- **Firewall und zentraler Router: pfSense**

PfSense, basierend auf FreeBSD, wurde als Network Virtual Appliance (NVA) zur Zentralisierung von Routing und Sicherheit ausgewählt. Es handelt sich um eine äußerst leistungsstarke Open-Source-Lösung der Enterprise-Klasse. Aus Kostengründen und aufgrund seines großen Funktionsumfangs wurde fSense gegenüber nativen Azure-Firewalls (wie der Azure Firewall) bevorzugt: Routing, VPN und Proxying sind nativ integriert, und wichtige Zusatzpakete (HAProxy, Suricata) werden unterstützt.

- **Identitäts- und DNS-Verwaltung: Windows Server Active Directory (AD DS)**

Begründung: Active Directory ist nach wie vor der unbestrittene Branchenstandard für die zentrale Identitäts- und Zugriffsverwaltung (IAM). In Verbindung mit dem eigenen DNS-Dienst ermöglicht es die nahtlose Namensauflösung im lokalen Netzwerk und erleichtert die Anwendung von Sicherheitsrichtlinien (GPOs) auf Clientrechnern.

- **Sicherer Fernzugriff: OpenVPN**

Begründung: Für den Fernzugriff auf Arbeits- und Verwaltungsaufgaben wurde OpenVPN aufgrund seiner einfachen Bereitstellung hinter restriktiven Firewalls (es arbeitet über einen einzigen UDP/TCP-Port) und seiner robusten Sicherheit mittels SSL/TLS gegenüber IPsec bevorzugt. Die native Integration in pfSense, einschließlich der Verwaltung einer lokalen Public-Key-Infrastruktur (PKI), erleichterte die Auswahl erheblich.

- **Voice over IP (VoIP): Asterisk**

Begründung: Asterisk ist das weltweit führende Open-Source-Framework zur Entwicklung von Kommunikationsanwendungen. Es wurde aufgrund seiner kostenlosen Verfügbarkeit, Stabilität und vollständigen Kompatibilität mit dem Standard-SIP-Protokoll ausgewählt, wodurch die Einrichtung einer internen Telefonanlage (IP-PBX) ermöglicht wird, die vollständig unabhängig von externen Anbietern ist.

- **Web-Publishing und Proxy: HAProxy und Nginx**

Begründung: Um interne Dienste sicher im Internet bereitzustellen, wurde Nginx aufgrund seiner geringen Größe und hohen Leistungsfähigkeit als Webserver gewählt. Zum Schutz dient HAProxy (auf pfSense bereitgestellt) als Reverse-Proxy. Diese Vorgehensweise ermöglicht die zentrale Zertifikatsverwaltung (SSL-Offloading) und verbirgt die tatsächliche IP-Adresse der internen Webserver.

- **Sicherheit und Überwachung (Suricata, Zabbix, Wazuh)**

Suricata (IDS/IPS): Bevorzugt aufgrund seiner Multithread-Verarbeitungsfähigkeit, die eine effiziente Einbruchserkennung gewährleistet, ohne den Netzwerkfluss auf pfSense zu verlangsamen.
Zabbix: Aufgrund seines sehr flexiblen Templatesystems wurde es für die Überwachung der Verfügbarkeit und der Hardware-Ressourcen ausgewählt.
Wazuh (SIEM/HIDS): Ausgewählt aufgrund seiner Fähigkeit, Protokolle in Echtzeit zu analysieren, Schwachstellen zu erkennen und die Einhaltung von Vorschriften sicherzustellen, wodurch ein vollständiges und quelloffenes Security Control Center (SOC) angeboten wird.

KAPITEL 4: IMPLEMENTIERUNG UND EINSATZ

4.1 Azure-Netzwerkbereitstellung und -Routing (UDR)

Um eine zentrale Sicherheit zu gewährleisten, haben wir in der Azure-Umgebung benutzerdefinierte Routingtabellen, sogenannte User Defined Routes (UDRs), implementiert. Diese Tabellen erzwingen,

dass der gesamte ausgehende Datenverkehr aus den verschiedenen Subnetzen zur Überprüfung und Filterung die pfSense-Firewall passiert. Diese Konfiguration verhindert nicht nur den direkten Internetzugang von Rechnern in sensiblen Subnetzen, sondern ermöglicht auch eine detaillierte Steuerung des netzwerkübergreifenden Datenverkehrs. Dadurch wird die Firewall zum zentralen logischen Kontrollpunkt unserer Infrastruktur.

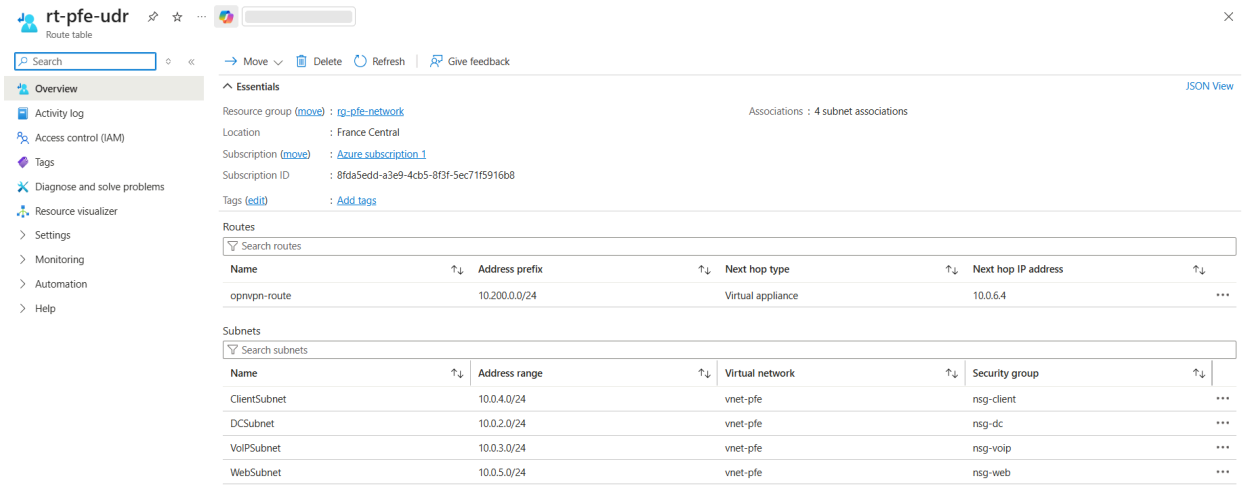

Abbildung 4: Azure-Routingtabelle (UDR)

4.2 Zentrale Firewall-Konfiguration (pfSense)

Die pfSense-Firewall, das Herzstück unserer Sicherheitsarchitektur, fungiert als obligatorisches Gateway für die gesamte Kommunikation. Ihre Konfiguration umfasste die strikte Definition von Filterregeln zwischen dem internen Netzwerk (LAN) und dem externen Netzwerk (WAN). Sie verwaltet zudem das NAT-Routing, um die Veröffentlichung bestimmter essenzieller Dienste und den Internetzugang von Arbeitsstationen selektiv zu ermöglichen. Die Implementierung dieser zentralen Sicherheitsrichtlinie reduziert die direkte Gefährdung interner Systeme erheblich und gewährleistet die Einhaltung des Prinzips der minimalen Berechtigungen.

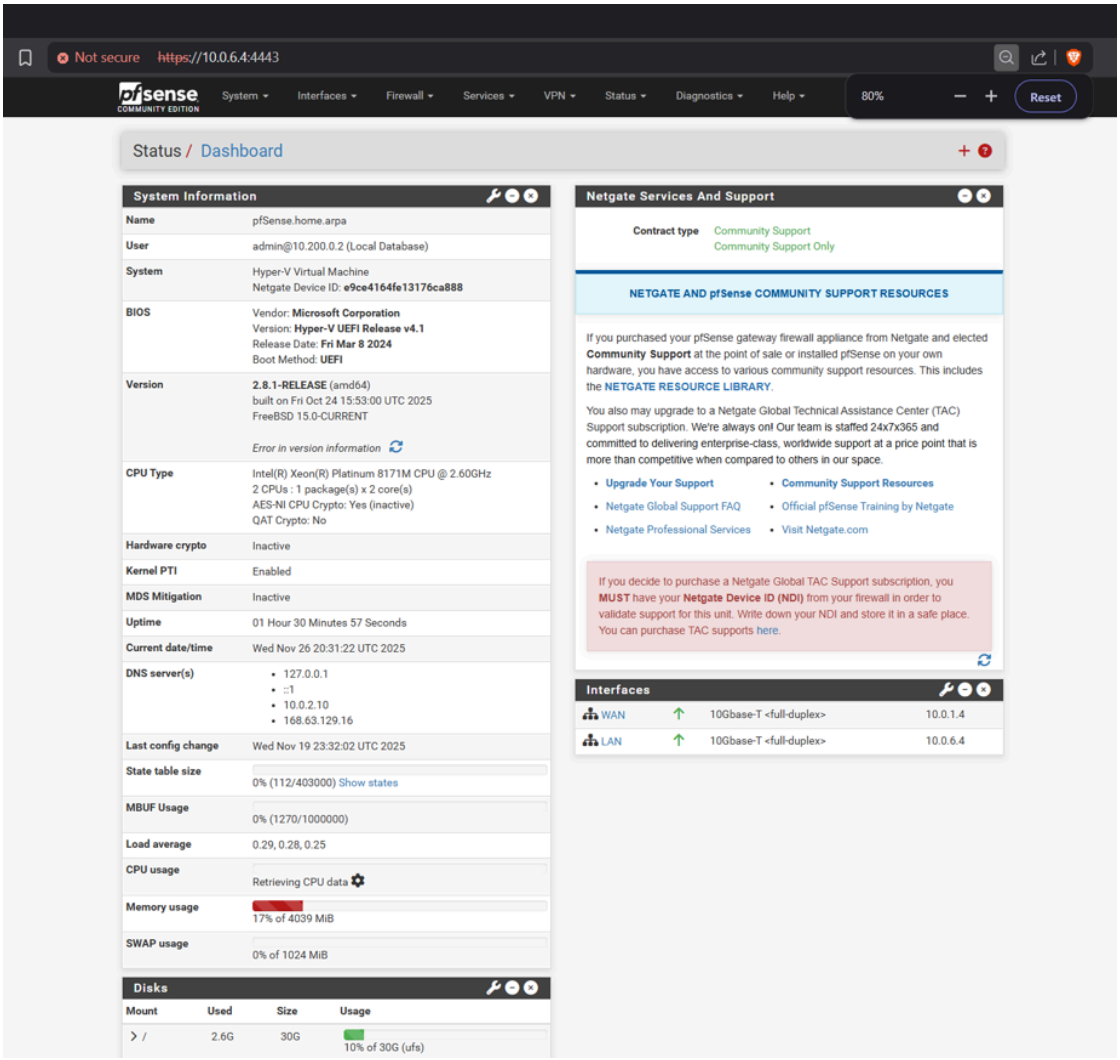

Abbildung 5: pfSense-Dashboard (Gateway)

4.3 Einrichten des Fernzugriffs (OpenVPN)

Um die sichere Administration der Umgebung von außerhalb des Netzwerks zu gewährleisten, wurde ein OpenVPN-Server direkt auf pfSense implementiert. Die Absicherung dieses Tunnels basiert auf der Einrichtung einer lokalen Zertifizierungsstelle (CA), die für die Ausstellung und Validierung von Zertifikaten für Server und Clients zuständig ist. Diese Lösung ermöglicht Administratoren einen verschlüsselten und stark authentifizierten Zugriff auf interne Netzwerke (insbesondere das Management-Subnetz), ohne die Administrationsschnittstellen kritischer Server öffentlich im Internet zugänglich machen zu müssen.

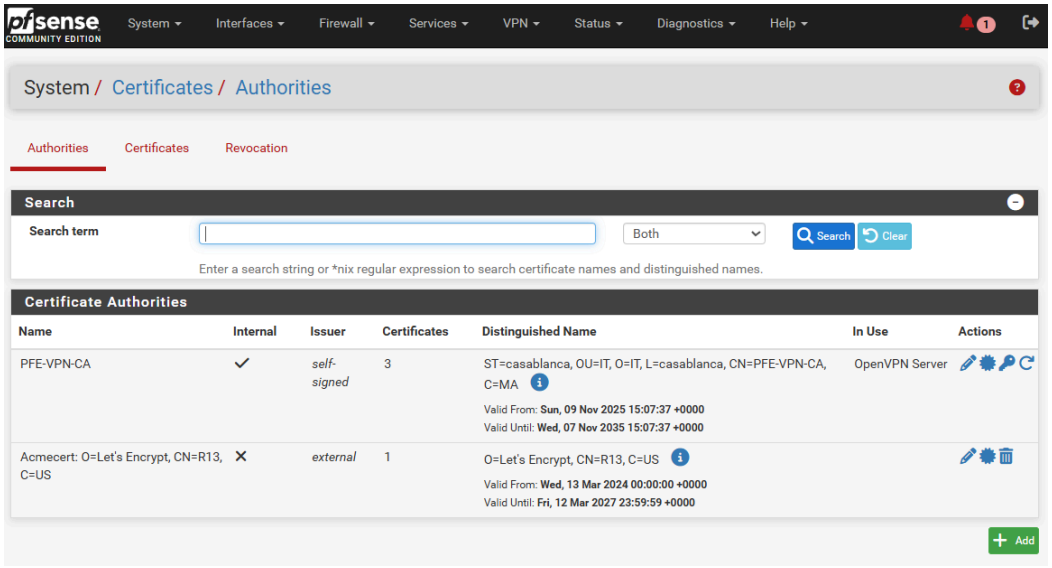

Abbildung 6: OpenVPN-Zertifizierungsstelle (CA)

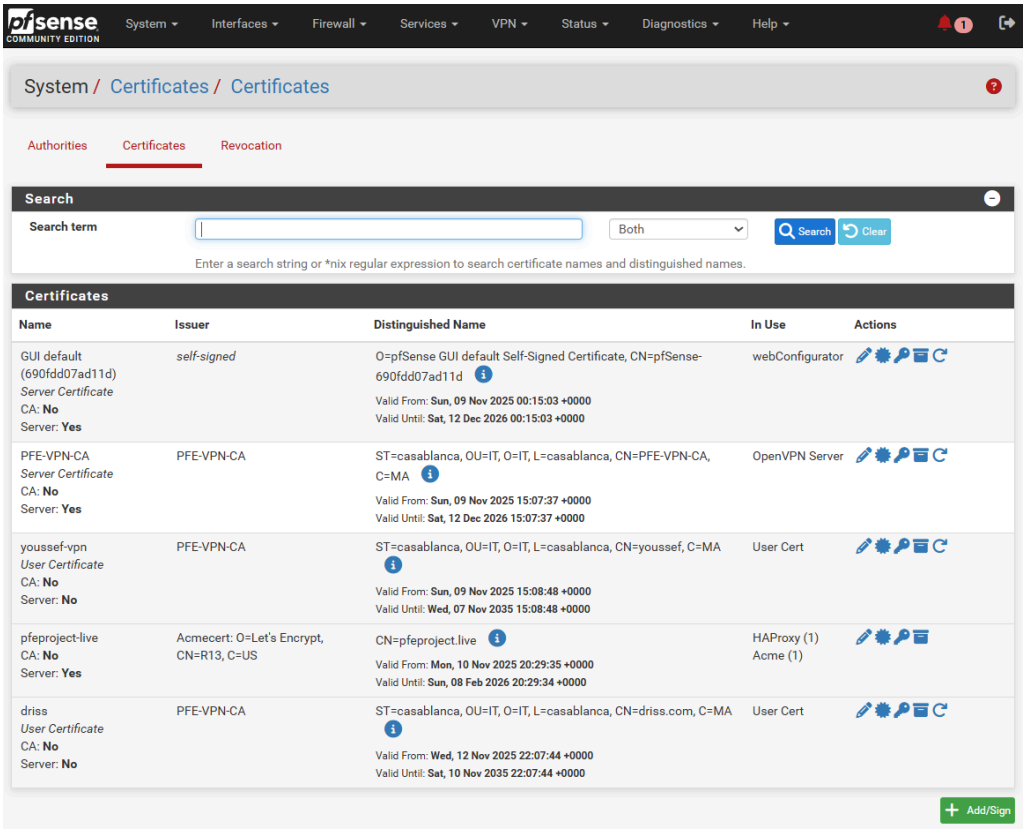

Abbildung 7: OpenVPN-Zertifikate (Benutzer/Server)

4.4 Active Directory & DNS

Zur zentralen Authentifizierung und Administration des Netzwerks wurde ein Windows Server-Domänencontroller bereitgestellt. Dieser übernimmt die Benutzerverwaltung, Sicherheitsgruppen und die Anwendung grundlegender Richtlinien. Parallel dazu wurde der DNS-Dienst für die interne Namensauflösung konfiguriert. Für externe Anfragen wurden DNS-Weiterleitungen implementiert. Dadurch können lokale Rechner auf das Internet zugreifen, während die vollständige Kontrolle über die Namensauflösungsanfragen erhalten bleibt.

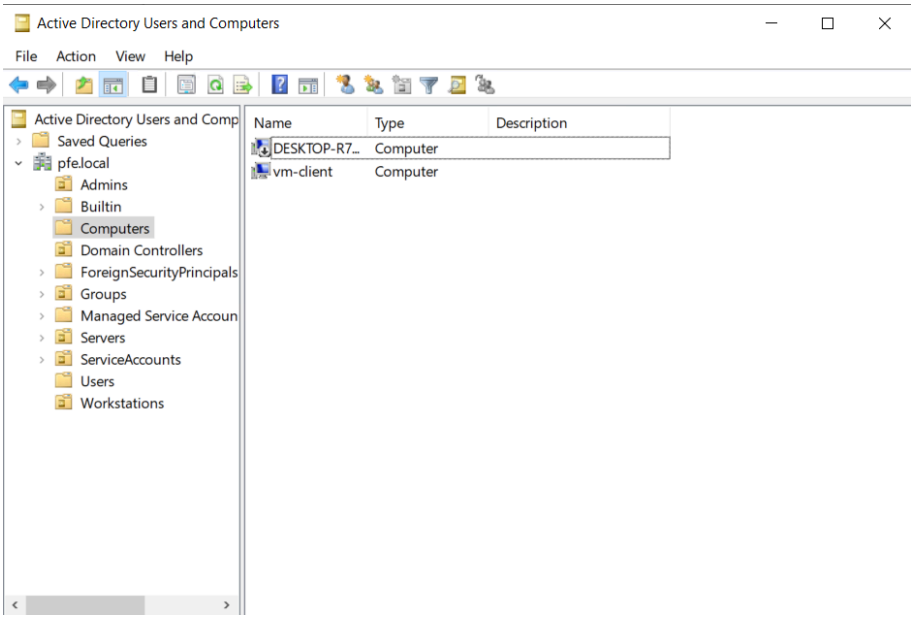

Abbildung 8: Active Directory-Computer

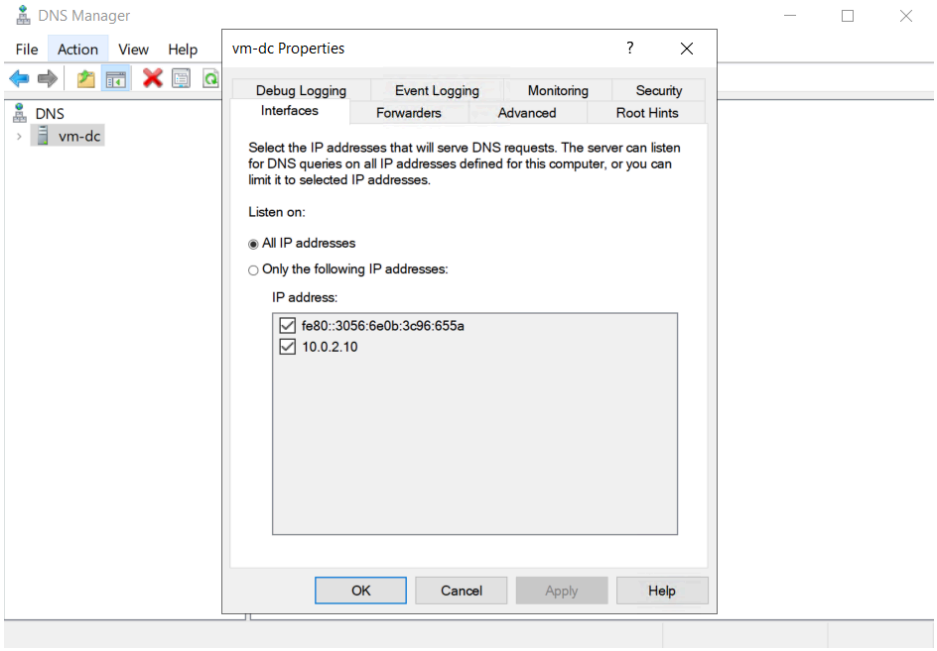

Abbildung 9: Schnittstellen DNS (AD/DNS)

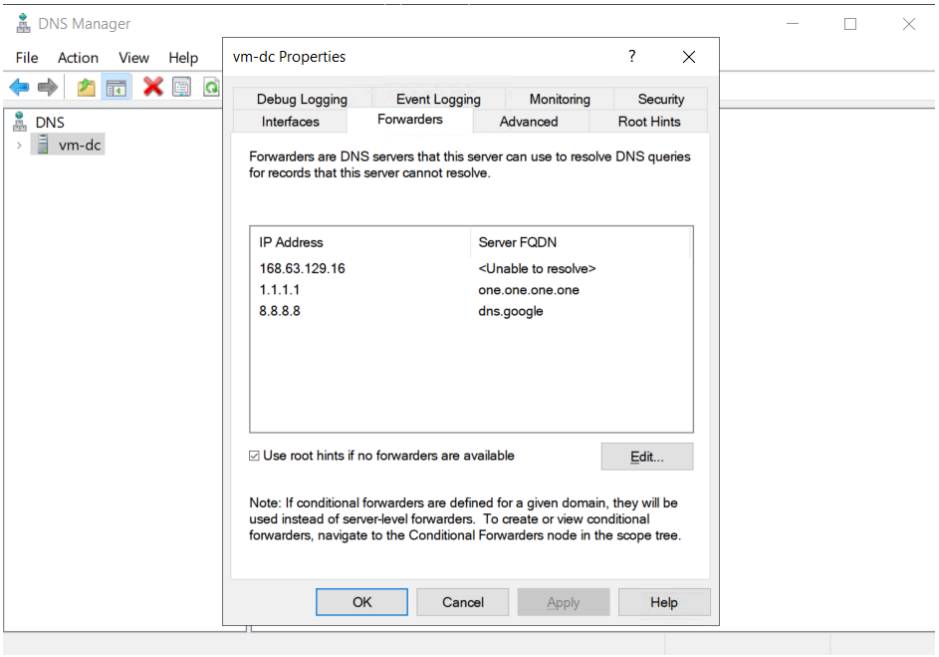

Abbildung 10: DNS-Weiterleitungen

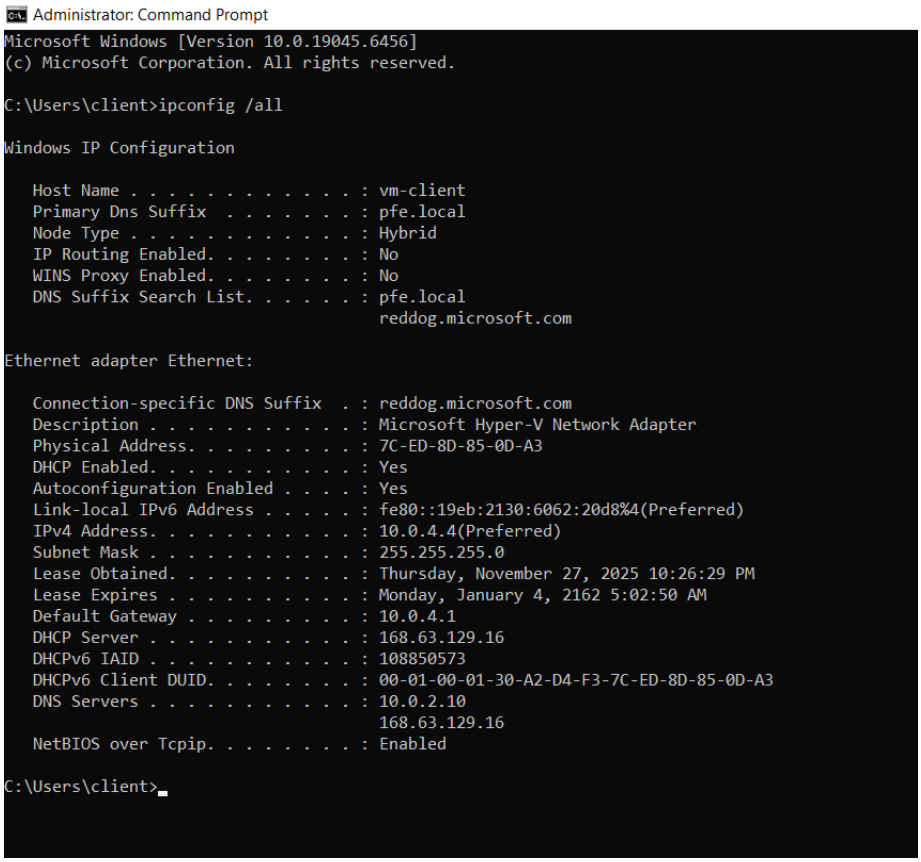

Abbildung 11: Client-IP-Konfiguration (DNS + Domäne)

4,5Sichere Webveröffentlichung (HAProxy + HTTPS)

Unser interner Webdienst wurde mithilfe der HAProxy-Komponente, die als Reverse-Proxy fungierte, nach außen hin zugänglich gemacht. Diese Methode zentralisiert den Zugriff auf den Dienst über einen einzigen Zugangspunkt und bietet eine zusätzliche Schutzebene, indem sie die tatsächliche interne Netzwerktopologie verschleiert. Darüber hinaus wurde der Zugriff auf die Website durch die Verknüpfung mit einem Domainnamen gesichert, wodurch die verschlüsselte Kommunikation durch HTTPS gewährleistet wurde.

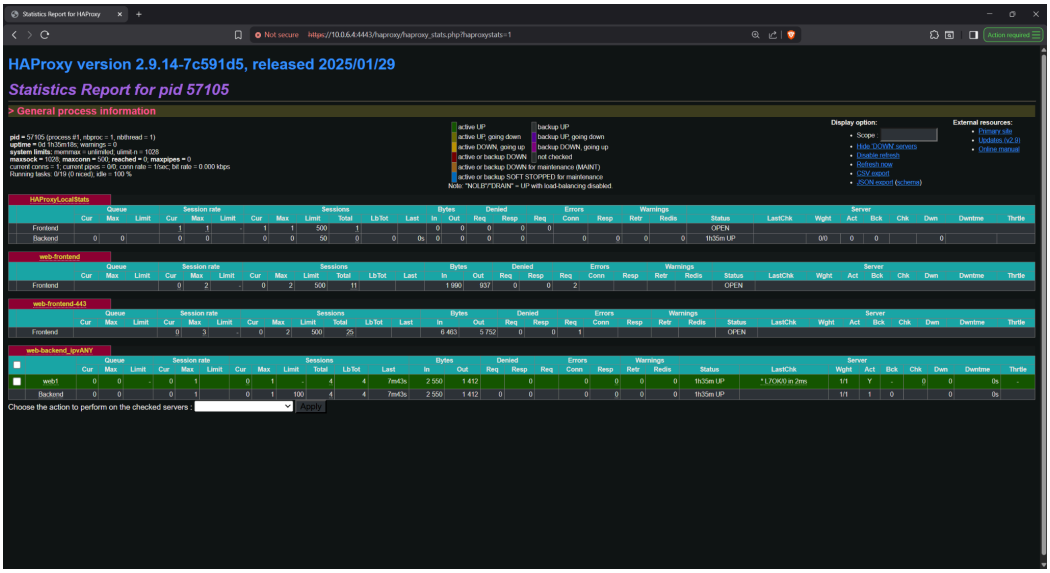

Abbildung 12: HAProxy (Reverse-Proxy)-Statistiken

4.6 VoIP-Dienste (Asterisk + Zoiper)

Für die VoIP-Implementierung wurde ein Asterisk-Server bereitgestellt und konfiguriert, um die Erstellung von SIP-Konten und den Verbindungsaufbau zu orchestrieren. Da der VoIP-Server hinter der Firewall gehostet wird, wurde besonderes Augenmerk auf die Routing-Konfiguration gelegt. In pfSense wurden spezifische „NAT Outbound“-Regeln definiert, um striktes Port-Rewriting zu verhindern und so ein reibungsloses, bidirektionales und unterbrechungsfreies Audio-Streaming (RTP-Protokoll) zu gewährleisten. Anschließend wurden Validierungen mit dem Zoiper-Softwareclient durchgeführt.

```
voip@vm-voip:/etc/asterisk$ sudo cat extensions.conf
[phones]

exten => 1001,1,Dial(SIP/youssef,20)
 same => n,Voicemail(1001@default,u)
 same => n,Hangup()

exten => 1002,1,Dial(SIP/driss,20)
 same => n,Voicemail(1002@default,u)
 same => n,Hangup()

exten => 500,1,Goto(ivr-menu,s,1)
voip@vm-voip:/etc/asterisk$
```

Abbildung 13: Asterisk – Konfiguration des Wählplans (extensions.conf)

```
voip@vm-voip:/etc/asterisk$ sudo cat sip.conf
[general]
context=default
bindport=5060
bindaddr=0.0.0.0
disallow=all
allow=ulaw,alaw
nat=yes

[youssef]
type=friend
secret=youssef.123
host=dynamic
context=phones

[driss]
type=friend
secret=driss.123
host=dynamic
context=phones

voip@vm-voip:/etc/asterisk$
```

Abbildung 14: Asterisk – SIP-Konfiguration von Accounts (sip.conf)

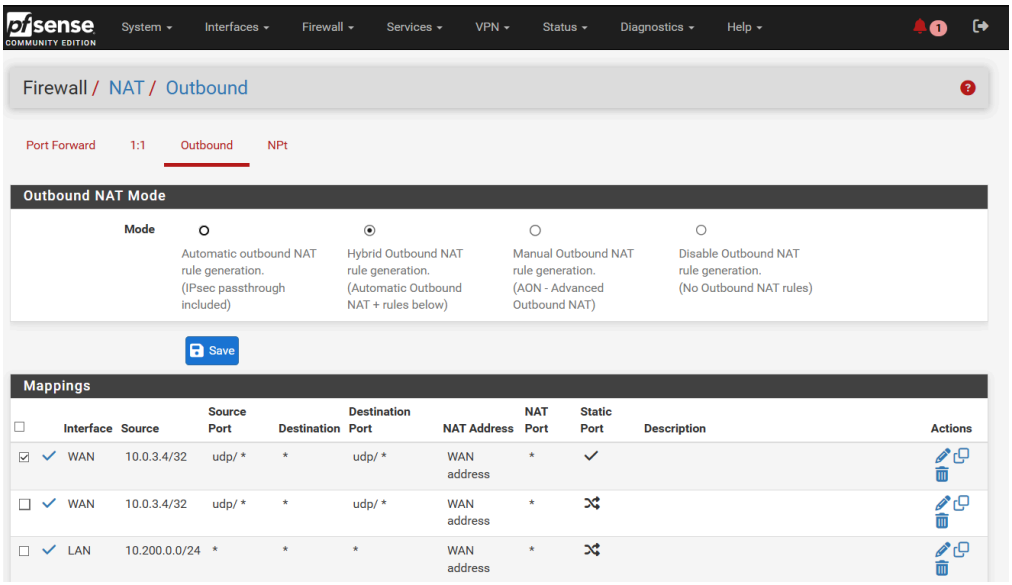

Abbildung 15: Ausgehende NAT-Regeln

KAPITEL 5: SICHERHEIT UND AUFSICHT

Nach Abschluss der Entwurfsphase und der operativen Bereitstellung der verschiedenen Dienste ist die Sicherung und Überwachung der Infrastruktur ein entscheidender Schritt im Projekt. Ziel dieses Kapitels ist es, die implementierten Mechanismen zur strengen Kontrolle des Netzwerkverkehrs, zur proaktiven Erkennung verdächtigen Verhaltens, zur Zentralisierung von Sicherheitsereignissen und zur Gewährleistung der Echtzeitüberwachung des Systemzustands vorzustellen.

5.1 Netzwerkfilterung und Sicherheitsrichtlinie (pfSense)

pfSense dient als zentrale Steuerungsstelle. Die angewandte Richtlinie basiert auf Folgendem:

- Autorisierung nur der notwendigen Datenflüsse (Prinzip der minimalen Berechtigungen);
- Die klare Trennung zwischen internem Datenverkehr (LAN) und externem Datenverkehr (WAN);
- Die Umsetzung der NAT-Regeln für die Veröffentlichung wesentlicher Dienste;
- Begrenzung der Exposition gegenüber internen Maschinen.

Dieser Ansatz trägt dazu bei, die Angriffsfläche zu verringern und den Zugriff besser zu kontrollieren.

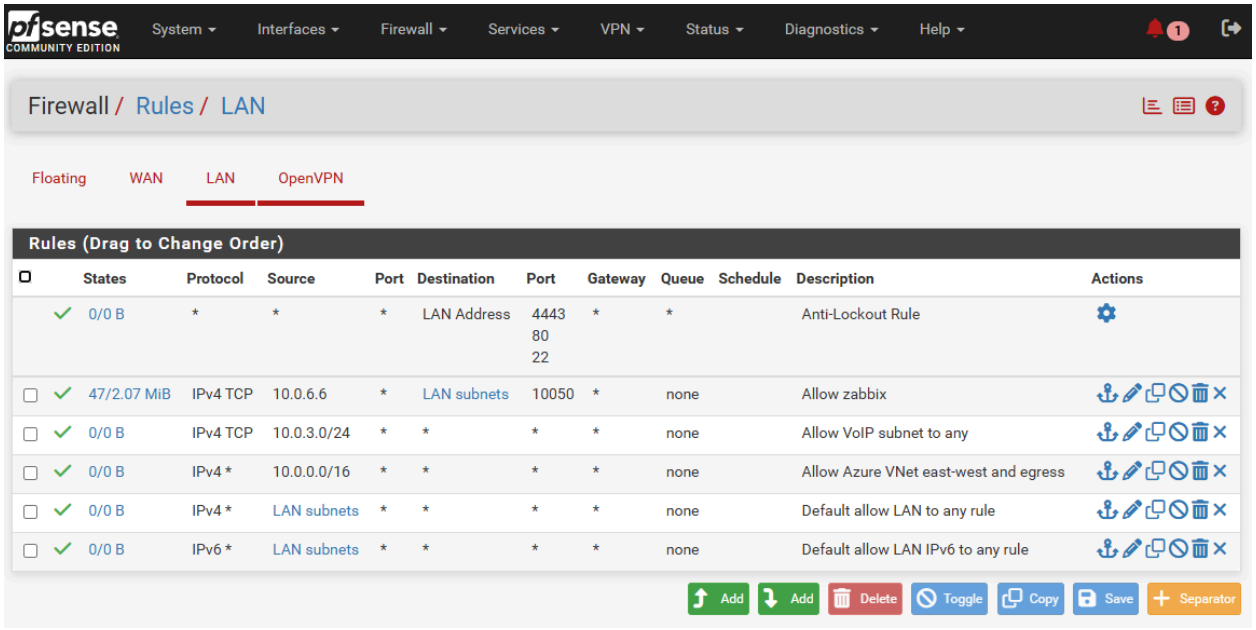

Abbildung 16: pfSense – LAN-Firewall-Regeln

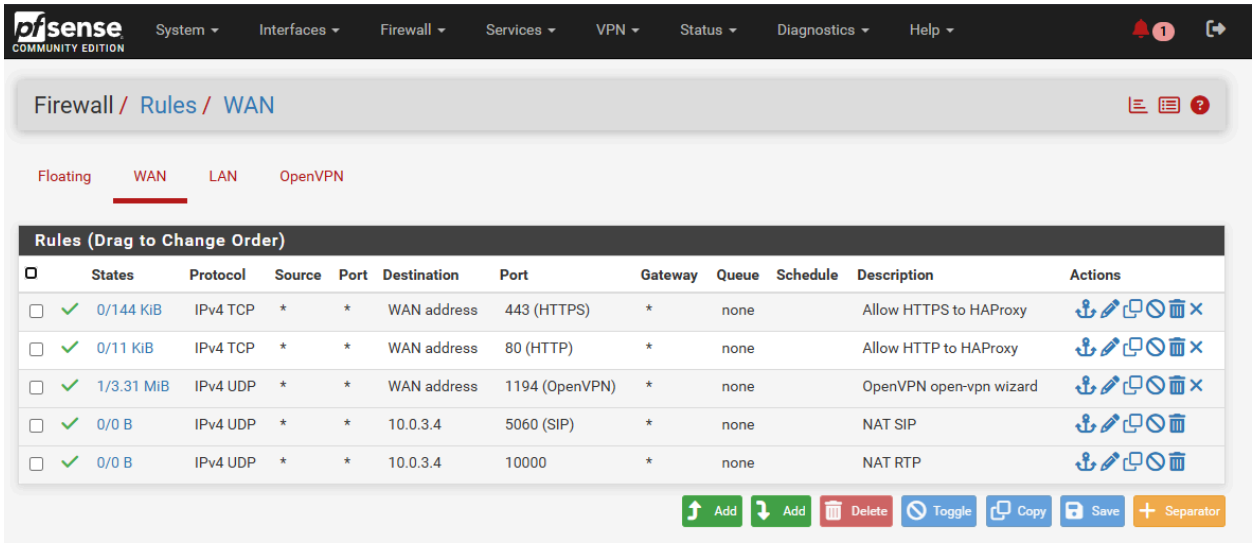

Abbildung 17: pfSense – WAN-Firewall-Regeln

5.2 Sicheres VPN (OpenVPN):

Der Fernzugriff auf die Infrastruktur zu administrativen Zwecken erfolgt ausschließlich über einen VPN-Tunnel. Dieser Mechanismus gewährleistet durch robuste Verschlüsselung absolute Vertraulichkeit der Kommunikation. Die Administratorauthentifizierung wird durch digitale Zertifikate verstärkt, wodurch unbefugter Zugriff verhindert wird. Dieses Sicherheitsgateway ermöglicht kontrollierten Zugriff auf interne Netzwerke (einschließlich des Management-Subnetzes) und somit eine vollständig

transparente Administration der Umgebung, ohne sensible Dienste jemals über öffentliche Ports bereitzustellen.

5.3 Netzwerk-Intrusion-Detection (Suricata):

Um unserer Firewall eine dynamische Sicherheitsebene hinzuzufügen, wurde das Suricata Intrusion Detection and Prevention System (IDS/IPS) integriert. Dessen Aufgabe ist die kontinuierliche Analyse des Netzwerkverkehrs, um Signaturen bekannter Angriffe oder ungewöhnliches Verhalten, wie beispielsweise bösartige Portscans, zu erkennen. Wird eine Bedrohung identifiziert, generiert Suricata detaillierte Warnmeldungen und kann die Quell-IP-Adressen proaktiv blockieren. Dies trägt zu einer schnellen und automatisierten Reaktion auf Vorfälle bei.

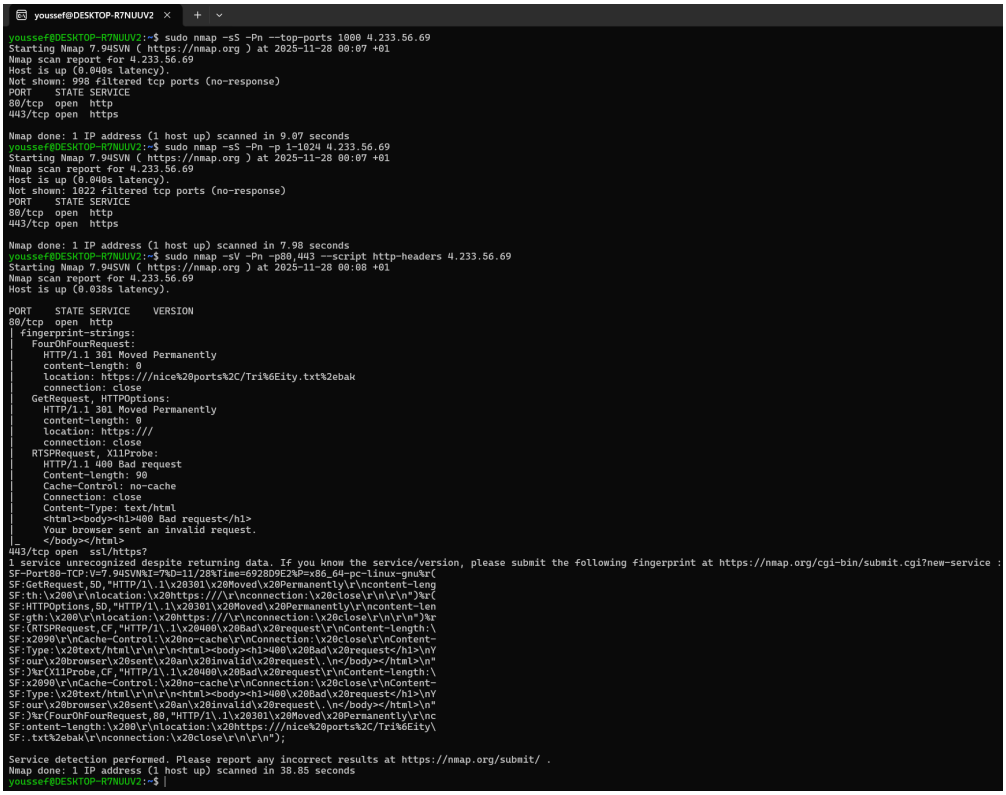

Abbildung 18: Suricata – Nmap-Erkennung

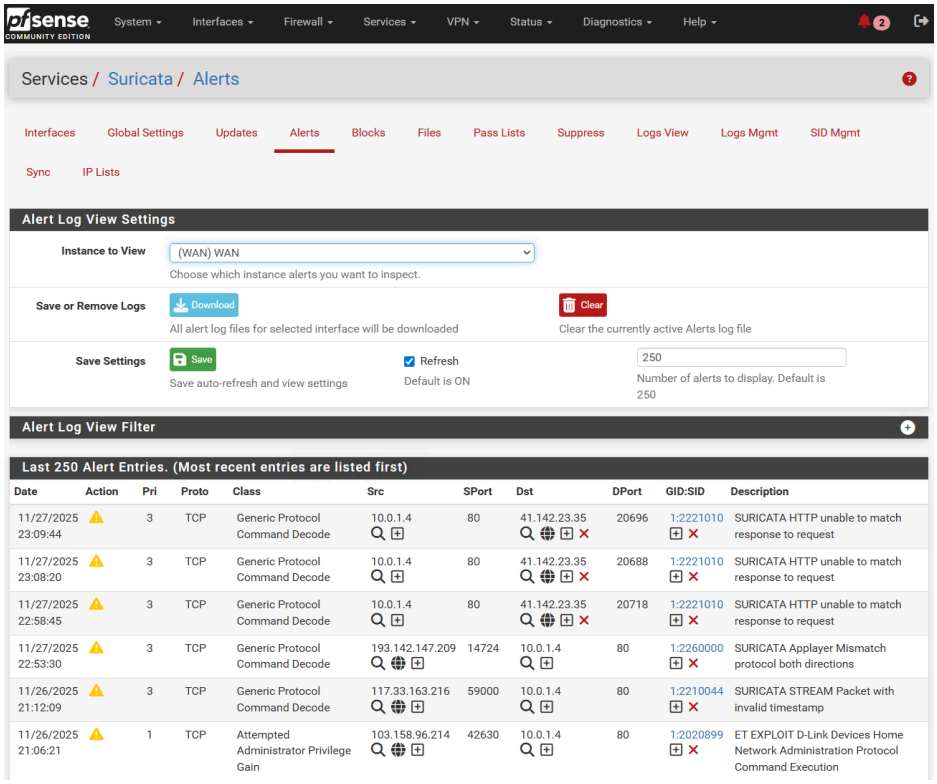

Abbildung 19: Erdmännchen – Warnungen

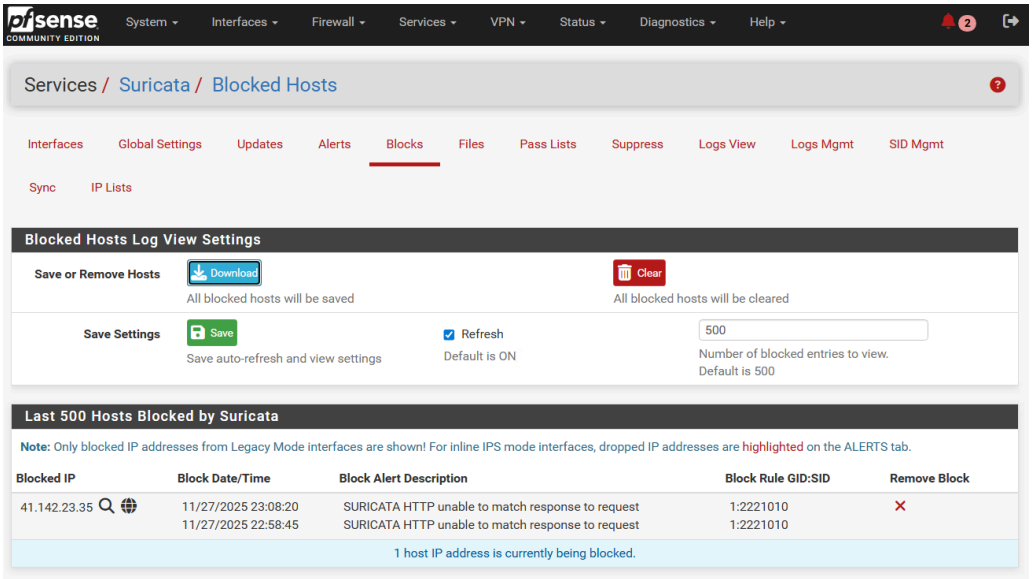

Abbildung 20: Suricata – Blockierte IP-Adressen (Blockierte Hosts)

5.4 Aufsicht (Zabbix)

Um den Betrieb der Infrastruktur sicherzustellen, wurde die Zabbix-Lösung implementiert. Dieses technische Überwachungstool ermöglicht die Echtzeit-Überwachung des Systemzustands und der Serviceverfügbarkeit. Es überwacht kontinuierlich die Auslastung von Hardware-Ressourcen wie CPU, RAM und Festplattenspeicher. Über zentrale Dashboards können Administratoren Anomalien wie Überlastungen oder Serviceausfälle sofort erkennen und so eine schnelle Fehlerbehebung gewährleisten.

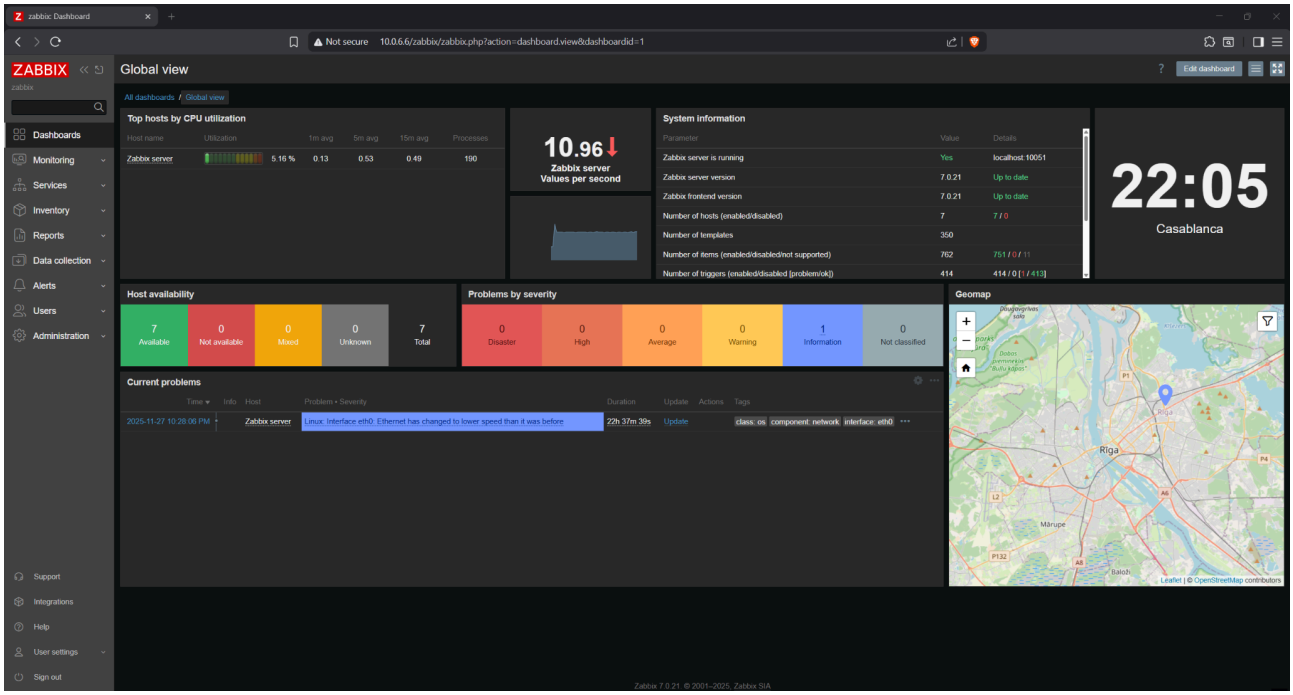

Abbildung 21: Zabbix-Dashboard

5.5 SIEM / HIDS (Wazuh)

Zusätzlich zur rein technischen Überwachung wurde die Wazuh-Plattform zur zentralen Verwaltung von Sicherheitsereignissen implementiert. Wazuh erfasst und analysiert Systemprotokolle in Echtzeit und bietet so detaillierte Einblicke in die Aktivitäten der auf verschiedenen virtuellen Maschinen bereitgestellten Agenten. Die Plattform zeichnet sich durch die Erkennung von Anomalien, die Eskalation kritischer Sicherheitswarnungen und die kontinuierliche Analyse von Konfigurationsschwachstellen aus und erleichtert dadurch Sicherheitsaudits und die Nachverfolgbarkeit der Azure-Umgebung erheblich.

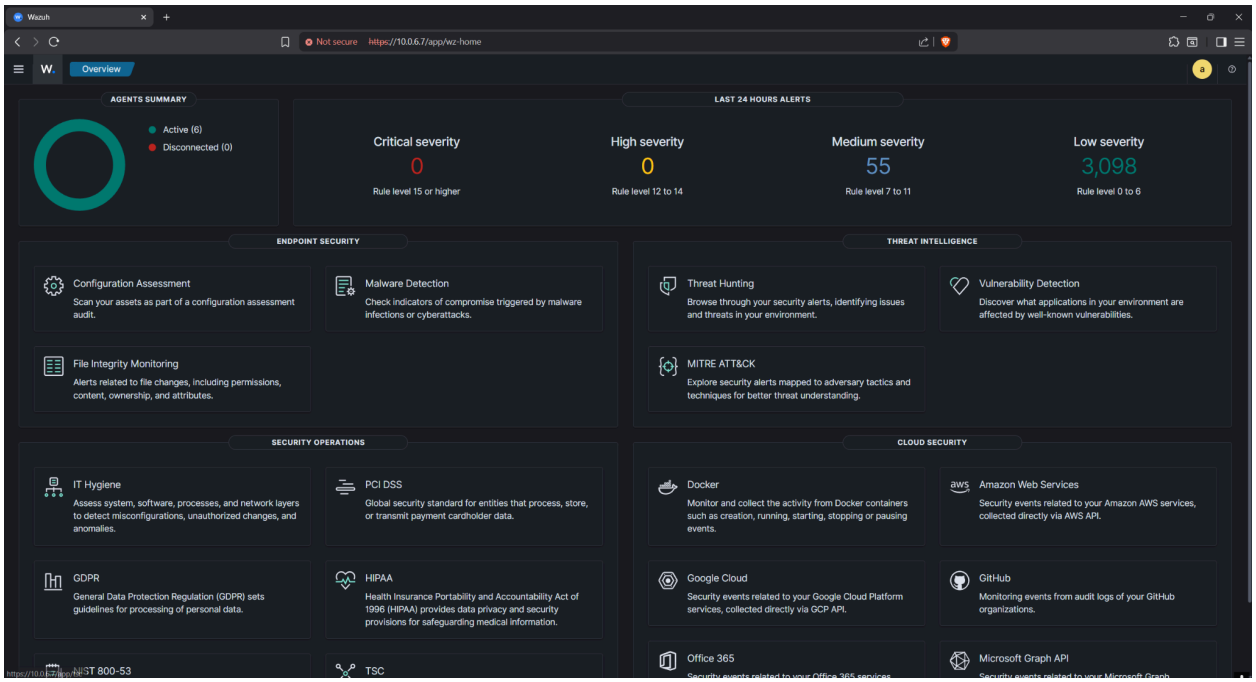

Abbildung 22: Wazuh-Dashboard

5.6 Tests und Validierung

Die letzte Phase unseres Projekts bestand aus der Prüfung der Infrastruktur durch eine Reihe strenger Tests, um zu bestätigen, dass die Implementierungen die anfänglichen Anforderungen erfüllten. Ziel war es, zu überprüfen, ob jede Komponente konsistent mit dem Rest des Systems interagierte.

5.6.1 Netzwerk- und VPN-Validierung

Zunächst überprüften wir die Netzwerksicherheit, indem wir die Kommunikation zwischen den Subnetzen testeten und die strikte Anwendung der Routing-Tabellen (UDR) validierten, indem wir den Datenverkehr über pfSense leiteten. Der Fernzugriff wurde ebenfalls validiert, indem wir eine Verbindung von einer externen Workstation via OpenVPN simulierten und so die korrekte Funktion der zertifikatsbasierten Authentifizierung sowie den Zugriff auf das interne Managementnetzwerk bestätigten.

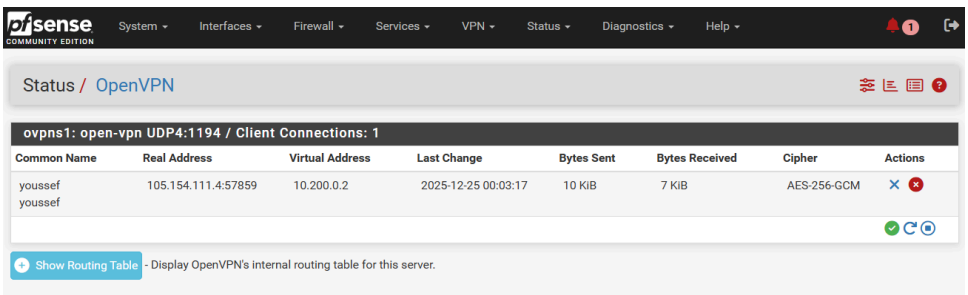

Abbildung 23: OpenVPN – Client-Verbindungsstatus

5.6.2 Validierung von Geschäftsdiensten (Web und VoIP)

Die gehosteten Dienste wurden Praxistests unterzogen. Der Webdienst wurde über einen externen Browser aufgerufen, um das korrekte Routing durch den HAProxy-Reverse-Proxy, die korrekte Namensauflösung und den HTTPS-Verkehrsschutz zu bestätigen. Im Bereich der Telefonie zeigten SIP-Aufzeichnungs- und eingehende/ausgehende Anruftests mit dem Zoiper-Client die einwandfreie Stabilität des Audiostreams und die korrekte NAT-Konfiguration auf Firewall-Ebene.

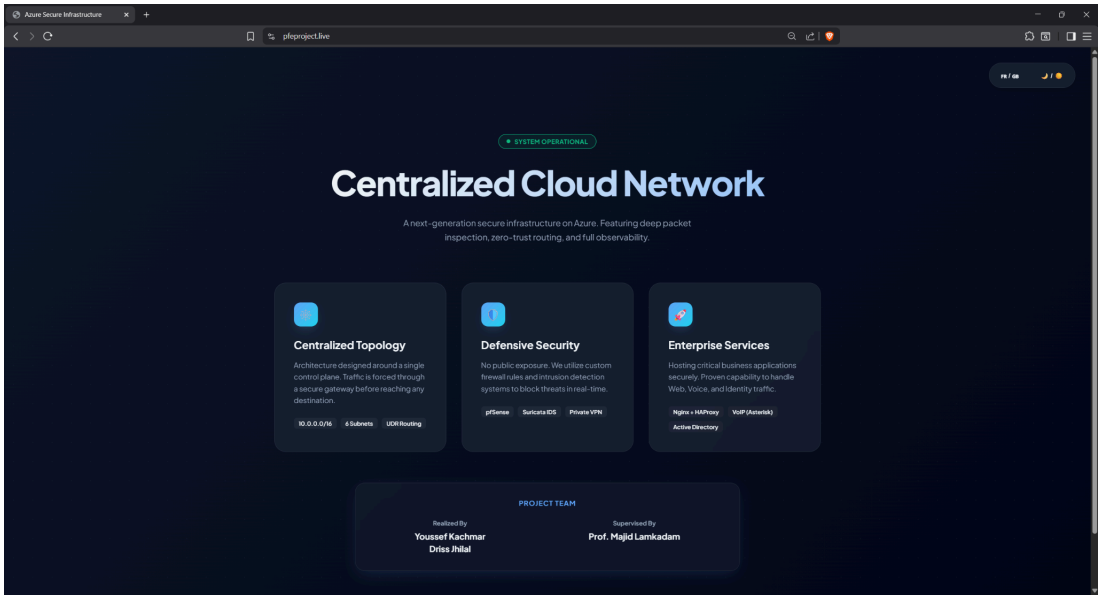

Abbildung 24: Website, die über einen Domainnamen erreichbar ist

5.6.3 Sicherheitsvalidierung und -überwachung

Abschließend wurde die Robustheit der Umgebung durch gezielte Portscans (mittels Nmap) von extern überprüft. Diese Simulationen bestätigten die Effektivität von Suricata, das die entsprechenden Warnmeldungen generierte und die IP-Sperrregeln anwendete. Gleichzeitig verifizierten wir, dass Zabbix und Wazuh diese Sicherheitsereignisse und Lastmetriken korrekt und in Echtzeit in ihren Dashboards meldeten und somit die vollständige Funktionsfähigkeit und Sicherheit unserer Architektur bestätigten.

ALLGEMEINE SCHLUSSFOLGERUNG

Dieses Abschlussprojekt umfasste die Konzeption, Bereitstellung und Validierung einer sicheren und überwachten Cloud-Infrastruktur auf Microsoft Azure, die die Anforderungen einer modernen Unternehmensumgebung vollständig erfüllt. Die implementierte Lösung basiert auf einer streng segmentierten Netzwerkarchitektur, in der das Routing über benutzerdefinierte Routingtabellen (UDRs) gesteuert wird, um den Datenverkehr über unsere zentrale pfSense-Firewall zu leiten. Letztere bewies ihre Effektivität durch die Zentralisierung von Filterung, Netzwerkadressübersetzung (NAT) und Fernzugriff über einen verschlüsselten VPN-Tunnel.

Neben der Netzwerkinfrastruktur wurden wichtige Geschäftsdienste erfolgreich implementiert. Die Integration von Active Directory und DNS ermöglichte ein zentralisiertes Identitätsmanagement. Die Veröffentlichung eines Webdienstes über den HAProxy-Reverse-Proxy (über HTTPS) und die Implementierung einer VoIP-Telefonanlage (Asterisk) demonstrierten die Fähigkeit der Architektur, kritische Dienste sicher zu hosten. Im Bereich der Verteidigung wurde der Schutz vor Eindringlingen durch die Kombination der Firewall mit dem Suricata IDS/IPS deutlich verbessert. Die Integration von Zabbix- und Wazuh-Lösungen ermöglichte schließlich eine vollständige Echtzeit-Transparenz des Ressourcenzustands und von Sicherheitsereignissen und erleichterte somit Audits und die Reaktion auf Sicherheitsvorfälle.
Die in den Spezifikationen festgelegten Ziele wurden somit vollständig erreicht. Die Infrastruktur ist nun funktionsfähig und hochsicher, und die durchgeführten Tests bestätigen die allgemeine Stimmigkeit der getroffenen technologischen Entscheidungen.

Entwicklungsperspektiven

Diese Infrastruktur bietet zwar eine solide und betriebsbereite Grundlage und veranschaulicht Best Practices im Cloud Computing und der Cybersicherheit, doch lassen sich einige Verbesserungen in Betracht ziehen, um sie weiter auszubauen. In einer groß angelegten Produktionsumgebung wäre es vorteilhaft, Hochverfügbarkeitsmechanismen (Redundanz) für kritische Komponenten wie Firewall und Domänencontroller zu integrieren. Darüber hinaus würden eine erweiterte Systemhärtung und die Implementierung einer regelmäßigen Datensicherungsstrategie mit einem Notfallwiederherstellungsplan (Disaster Recovery Plan, DRP) die allgemeine Ausfallsicherheit erhöhen. Schließlich würde die vollständige Automatisierung der Bereitstellung mithilfe von Infrastructure-as-Code-Tools (wie Terraform oder Ansible) die Bereitstellung dieser Umgebung in Zukunft standardisieren und beschleunigen.

BIBLIOGRAPHIE & WEBOGRAPHIE

Microsoft Azure:https://azure.microsoft.com/

pfSense :https://www.pfsense.org/

OpenVPN:https://openvpn.net/

HAProxy:https://www.haproxy.org/

NGINX:https://nginx.org/

Sternchen:https://www.asterisk.org/

Zoiper :https://www.zoiper.com/

Erdmännchen:https://suricata.io/

Zabbix:https://www.zabbix.com/

Wazuh:https://wazuh.com/

RFC 1918 :https://datatracker.ietf.org/doc/html/rfc1918