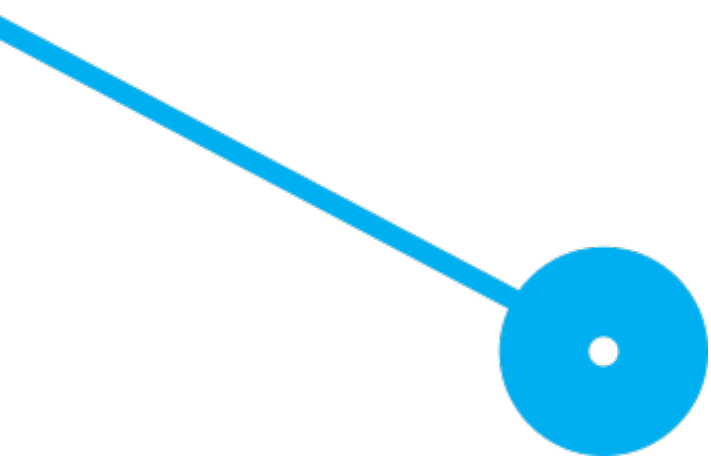
ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

CTeSP CURSO TÉCNICO SUPERIOR PROFISSIONAL

Infraestrutura de Rede Empresarial Segura Open Source

Ryan da Silva Barbosa — 8240758
Igor Gabriel Macedo Araújo — 8240754
Hugo Danial da Silva Correia — 8240532

10 de dezembro de 2025



ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

CTeSP CURSO TÉCNICO SUPERIOR PROFISSIONAL

Infraestrutura de Rede Empresarial Segura Open Source

Ryan da Silva Barbosa — 8240758
Igor Gabriel Macedo Araújo — 8240754
Hugo Danial da Silva Correia — 8240532

Sob Orientação de:

Nuno Figueiredo

Agradecimentos

Gostaríamos de expressar a nossa profunda gratidão a todos aqueles que contribuíram, de forma direta ou indireta, para a concretização deste projeto.

Um agradecimento especial à Professora Marta Martinho e ao Professor Nuno Figueiredo — nossos orientadores — pelo incansável apoio, constante disponibilidade, paciência e valiosa orientação ao longo de todo o desenvolvimento deste trabalho. Suas dedicações e conhecimento foram fundamentais para o sucesso deste projeto.

Às nossas excelentíssimas namoradas, pelo apoio incondicional, compreensão e paciência durante todo este período intenso de trabalho. O vosso suporte emocional foi fundamental para superarmos os desafios deste projeto.

Aos nossos colegas e amigos, pelo companheirismo, partilha de conhecimentos e momentos de reflexão que enriqueceram este percurso académico.

A todos os que, direta ou indiretamente, tornaram possível a realização deste projeto, o nosso mais sincero obrigado.

Os Autores

Resumo

O presente relatótio apresenta o planeamento, implementação e documentação de uma infraestrutura de rede empresarial segura para a organização fictícia FSociety.pt. O projeto, desenvolvido no âmbito da unidade curricular de Administração de Sistemas II, excede os requisitos estabelecidos ao implementar uma arquitetura *Four-Legged Firewall* com quatro zonas de segurança (WAN, LAN, DMZ e VPN), superando o modelo *Three-Legged* proposto inicialmente.

A infraestrutura integra serviços críticos de negócio: Active Directory com Samba AD DC para autenticação centralizada e SSO; Nextcloud como plataforma de colaboração com mais de 65 aplicações; Mailcow como servidor de email com anti-spam baseado em machine learning e validação SPF/DKIM/DMARC (pontuação 10/10 no Mail-Tester); Nginx como reverse proxy centralizado; e OpenVPN com autenticação RADIUS integrada com Active Directory.

A segurança é assegurada através de múltiplas camadas: pfSense com 72 regras de firewall e política *default deny*; CrowdSec como IDS/IPS distribuído em 4 servidores; Cloudflare como WAF e proteção DDoS na edge; e Netdata Cloud para monitorização com análise preditiva baseada em IA.

Os resultados demonstram uma solução empresarial completa, implementada exclusivamente com tecnologias *open source*, que protege os ativos digitais contra ameaças internas e externas. A documentação técnica completa, compreendendo mais de 40 guias de implementação, encontra-se arquivada no Zenodo (DOI: 10.5281/zenodo.17840636), assegurando a reprodutibilidade integral da solução.

Palavras-chave: Segurança de Redes, Four-Legged Firewall, Active Directory, OpenVPN, pfSense

Abstract

This work presents the planning, implementation and documentation of a secure enterprise network infrastructure for the fictitious organization FSociety.pt. The project, developed within the Systems Administration II course, exceeds the established requirements by implementing a *Four-Legged Firewall* architecture with four security zones (WAN, LAN, DMZ and VPN), surpassing the initially proposed *Three-Legged* model.

The infrastructure integrates critical business services: Active Directory with Samba AD DC for centralized authentication and SSO; Nextcloud as a collaboration platform with over 65 applications; Mailcow as an email server with machine learning-based anti-spam and SPF/DKIM/DMARC validation (10/10 score on Mail-Tester); Nginx as a centralized reverse proxy; and OpenVPN with RADIUS authentication integrated with Active Directory.

Security is ensured through multiple layers: pfSense with 72 firewall rules and *default deny* policy; CrowdSec as a distributed IDS/IPS across 4 servers; Cloudflare as WAF and DDoS protection at the edge; and Netdata Cloud for monitoring with AI-based predictive analysis.

The results demonstrate a complete enterprise solution, implemented exclusively with *open source* technologies, that protects digital assets against internal and external threats. The complete technical documentation, comprising over 40 implementation guides, is archived on Zenodo (DOI: 10.5281/zenodo.17840636), ensuring full reproducibility of the solution.

Keywords: Network Security, Four-Legged Firewall, Active Directory, OpenVPN, pfSense

Declaração sobre o uso de Inteligência Artificial

Na elaboração deste relatório foi utilizada Inteligência Artificial generativa. As ferramentas utilizadas foram o Claude (Anthropic) para apoio na estruturação e revisão do texto, esclarecimento de dúvidas técnicas, formatação LaTeX e organização da documentação, e o Gemini (Google Workspace) para geração de diagramas e thumbnails ilustrativos baseados nos resultados dos testes e configurações da infraestrutura. Todo o conteúdo técnico, implementação prática, configurações, testes e decisões de arquitetura foram realizados integralmente pelos autores. Os autores assumem total responsabilidade pelo conteúdo final do trabalho.

Capítulo

Índice

Capítulo

Lista de Figuras

Capítulo

Lista de Tabelas

Capítulo

Listagens de Código

Capítulo

Siglas & Acrónimos

ACL Access Control List (Lista de Controlo de Acesso).

AD Active Directory.

AES Advanced Encryption Standard.

AI Artificial Intelligence (Inteligência Artificial).

API Application Programming Interface.

BIOS Basic Input/Output System.

CAPI Central API.

CARP Common Address Redundancy Protocol.

CDN Content Delivery Network (Rede de Distribuição de Conteúdo).

CLI Command Line Interface (Interface de Linha de Comandos).

CNAME Canonical Name Record.

CPU Central Processing Unit (Unidade Central de Processamento).

CSP Content Security Policy.

CVE Common Vulnerabilities and Exposures.

DC Domain Controller (Controlador de Domínio).

DDNS Dynamic Domain Name System.

DDoS Distributed Denial of Service.

DHCP Dynamic Host Configuration Protocol.

DKIM DomainKeys Identified Mail.

DMARC Domain-based Message Authentication, Reporting and Conformance.

DMZ Demilitarized Zone (Zona Desmilitarizada).

DNS Domain Name System (Sistema de Nomes de Domínio).

DNSBL DNS-based Blackhole List.

DOI Digital Object Identifier.

ESTG Escola Superior de Tecnologia e Gestão.

FQDN Fully Qualified Domain Name.

FTP File Transfer Protocol (Protocolo de Transferência de Ficheiros).

GC Garbage Collection.

GPO Group Policy Object.

GTUBE Generic Test for Unsolicited Bulk Email.

GUI Graphical User Interface (Interface Gráfica).

HA High Availability (Alta Disponibilidade).

HSTS HTTP Strict Transport Security.

HTTP HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto).

HTTPS HyperText Transfer Protocol Secure.

I/O Input/Output (Entrada/Saída).

ICMP Internet Control Message Protocol.

IDS Intrusion Detection System (Sistema de Deteção de Intrusões).

IMAP Internet Message Access Protocol.

IP Internet Protocol (Protocolo de Internet).

IPP Instituto Politécnico do Porto.

IPS Intrusion Prevention System (Sistema de Prevenção de Intrusões).

ISP Internet Service Provider (Fornecedor de Serviços de Internet).

KVM Kernel-based Virtual Machine.

LAN Local Area Network (Rede Local).

LAPI Local API.

LDAP Lightweight Directory Access Protocol.

LXC Linux Containers.

MAC Media Access Control.

MDA Mail Delivery Agent.

ML Machine Learning (Aprendizagem Automática).

MTA Mail Transfer Agent.

MTTD Mean Time To Detect.

MX Mail Exchange.

NAT Network Address Translation.

NFS Network File System.

NTP Network Time Protocol.

OID Object Identifier.

OS Operating System (Sistema Operativo).

OU Organizational Unit (Unidade Organizacional).

OWASP Open Web Application Security Project.

PAM Pluggable Authentication Modules.

PBS Proxmox Backup Server.

POP3 Post Office Protocol version 3.

PTR Pointer Record.

PVE Proxmox Virtual Environment.

RADIUS Remote Authentication Dial-In User Service.

RAID Redundant Array of Independent Disks.

RAM Random Access Memory.

RGPD Regulamento Geral sobre a Proteção de Dados.

RPO Recovery Point Objective.

RTO Recovery Time Objective.

SASL Simple Authentication and Security Layer.

SIEM Security Information and Event Management.

SMB Server Message Block.

SMTP Simple Mail Transfer Protocol.

SPF Sender Policy Framework.

SQL Structured Query Language.

SRV Service Record.

SSD Solid State Drive.

SSH Secure Shell.

SSL Secure Sockets Layer.

SSO Single Sign-On.

TCP Transmission Control Protocol.

TLS Transport Layer Security.

TOTP Time-based One-Time Password.

TTL Time To Live.

UC Unidade Curricular.

UDP User Datagram Protocol.

UID User Identifier.

URL Uniform Resource Locator.

UUID Universally Unique Identifier.

VLAN Virtual Local Area Network.

VM Virtual Machine (Máquina Virtual).

VPN Virtual Private Network (Rede Privada Virtual).

WAF Web Application Firewall.

WAN Wide Area Network (Rede de Área Alargada).

XSS Cross-Site Scripting.

ZSTD Zstandard (algoritmo de compressão).

Capítulo

Glossário

Active Directory Serviço de diretório para gestão centralizada de identidades, autenticação e políticas em redes empresariais. Neste projeto, implementado através do Samba AD DC..

Blocklist Lista de endereços IP ou domínios identificados como maliciosos, utilizada para bloquear tráfego indesejado de forma proativa..

Bouncer Componente do CrowdSec responsável por aplicar decisões de bloqueio. Existem diferentes tipos: Firewall Bouncer (iptables), Nginx Bouncer (Lua) e Cloudflare Bouncer..

CrowdSec Sistema de deteção e prevenção de intrusões open source baseado em análise comportamental e inteligência colaborativa..

Deduplicação Técnica de otimização de armazenamento que elimina cópias duplicadas de dados, armazenando apenas blocos únicos..

Default Deny Política de segurança que bloqueia todo o tráfego por omissão, permitindo apenas o que está explicitamente autorizado por regras..

Defense in Depth Estratégia de segurança que implementa múltiplas camadas de proteção, de modo que a falha de uma camada não comprometa toda a segurança..

Failover Mecanismo de redundância que permite a transferência automática de serviços para um sistema secundário em caso de falha do sistema principal..

Firewall Sistema de segurança de rede que monitoriza e controla o tráfego de entrada e saída com base em regras de segurança predefinidas..

Four-Legged Firewall Arquitetura de firewall com quatro interfaces de rede, cada uma ligada a uma zona de segurança distinta: WAN, LAN, DMZ e VPN..

Greylisting Técnica anti-spam que rejeita temporariamente emails de remetentes desconhecidos, assumindo que servidores legítimos irão reenviar a mensagem..

Hypervisor Software que cria e executa máquinas virtuais, permitindo que múltiplos sistemas operativos partilhem o mesmo hardware físico..

Kerberos Protocolo de autenticação de rede que utiliza criptografia de chave simétrica e tickets para permitir autenticação segura entre cliente e servidor..

Mailcow Solução de servidor de email open source baseada em Docker que integra Postfix, Dovecot, Rspamd, ClamAV e SOGo..

Nextcloud Plataforma de colaboração open source que oferece armazenamento de ficheiros, calendário, contactos e mais de 65 aplicações integradas..

Open Source Software cujo código-fonte está disponível publicamente, podendo ser utilizado, modificado e distribuído livremente..

pfSense Distribuição de firewall e router open source baseada em FreeBSD, com interface web para gestão de regras, VPN, DHCP e outros serviços de rede..

Proxmox VE Plataforma de virtualização open source que combina KVM (máquinas virtuais) e LXC (containers) com gestão via interface web..

Reverse Proxy Servidor intermediário que recebe pedidos de clientes e os encaminha para servidores backend, centralizando funcionalidades como terminação TLS, cache e balanceamento de carga..

Samba AD DC Implementação open source do protocolo Active Directory que permite criar um controlador de domínio compatível com Microsoft AD em sistemas Linux..

Snapshot Cópia instantânea do estado de um sistema ou disco num determinado momento, permitindo backups consistentes sem interrupção de serviço..

Three-Legged Firewall Arquitetura de firewall com três interfaces de rede: uma para a rede externa (WAN), uma para a rede interna (LAN) e uma para a zona desmilitarizada (DMZ)..

Zammad Sistema de helpdesk e tickets open source com interface web moderna, integração de email e suporte a múltiplos canais de comunicação..

1. Introdução

A transformação digital nas organizações modernas trouxe desafios significativos para a administração de sistemas e segurança da informação. Numa era onde os dados representam o ativo mais valioso de qualquer empresa, a implementação de uma infraestrutura de rede segura, resiliente e bem estruturada tornou-se crítica para a continuidade do negócio.

As organizações enfrentam diariamente ameaças cada vez mais sofisticadas — desde tentativas de acesso não autorizado, *malware* e *ransomware*, até ataques de engenharia social e violações de dados (Scarfone & Hoffman, 2009). Simultaneamente, necessitam proporcionar aos colaboradores acesso fluido e seguro aos recursos corporativos, independentemente da localização física, especialmente num contexto onde o trabalho remoto e híbrido se tornou norma.

A segurança da informação não se limita à implementação de tecnologia. Abrange dimensões físicas, técnicas e organizacionais que, quando adequadamente integradas, formam uma defesa em profundidade (*defense in depth*) capaz de proteger contra múltiplos vetores de ataque (National Institute of Standards and Technology, 2020). A arquitetura proposta neste trabalho reflete esta filosofia através da segmentação em múltiplas zonas de segurança, cada uma com políticas e controlos específicos, geridas centralmente por uma solução *firewall* de nível empresarial.

A escolha do pfSense (Netgate, 2024), reconhecido como uma das soluções *open-source* mais robustas para segmentação e proteção de redes, permitiu implementar não apenas filtragem *stateful* de pacotes, mas também funcionalidades avançadas como Virtual Private Network (Rede Privada Virtual) (VPN), Intrusion Detection System (Sistema de Deteção de Intrusões) (IDS)/Intrusion Prevention System (Sistema de Prevenção de Intrusões) (IPS), *traffic shaping* e *logging* detalhado — características essenciais em ambientes corporativos modernos (Kumar & Sharma, 2022).

1.1 Motivação

A motivação para este projeto surge da necessidade de compreender, na prática, como se concebe e implementa uma infraestrutura de TI empresarial que equilibre segurança, funcionalidade e usabilidade. O cenário académico proposto ofereceu a oportunidade de ir além da teoria e enfrentar desafios reais que um administrador de sistemas encontra no mercado de trabalho (Tanenbaum et al., 2021).

Vários fatores específicos motivaram a escolha de expandir o âmbito original do trabalho:

1. **Realismo Empresarial**: As organizações modernas não operam apenas com redes internas isoladas. A necessidade de expor serviços públicos (*websites*, email) e permitir acesso remoto seguro é universal (Kurose & Ross, 2021), justificando a implementação da camada VPN e a segmentação rigorosa através de um *firewall* profissional.

2. **Solução *Firewall Enterprise-Grade***: A escolha do pfSense como núcleo da arquitetura de segurança reflete a realidade do mercado, onde soluções *open-source* como pfSense, OPNsense ou similares são amplamente utilizadas em ambientes empresariais devido à sua robustez, flexibilidade e custo-benefício superior a soluções proprietárias (Netgate, 2024).

3. **Evolução Tecnológica**: A transição de soluções tradicionais (partilhas Server Message Block (SMB) básicas) para plataformas modernas de colaboração (Nextcloud) reflete a realidade do mercado, onde as empresas procuram soluções que ofereçam mais do que simples armazenamento de ficheiros, integrando funcionalidades de colaboração em tempo real e sincronização multi-dispositivo (Nextcloud GmbH, 2024).

4. **Segurança em Camadas**: A implementação de quatro interfaces de rede distintas no pfSense (Wide Area Network (Rede de Área Alargada) (WAN), Local Area Network (Rede Local) (LAN), Demilitarized Zone (Zona Desmilitarizada) (DMZ), VPN) permite explorar conceitos fundamentais como segmentação de rede, princípio do menor privilégio, filtragem *stateful* (Wool, 2010), e defesa em profundidade, essenciais para qualquer profissional de cibersegurança.

5. **Integração de Serviços**: A oportunidade de integrar múltiplos serviços (Active Directory (AD), Lightweight Directory Access Protocol (LDAP), *Email*, *Web*, VPN) protegidos por regras de *firewall* granulares e observar como interagem entre si proporciona uma compreensão holística da administração de sistemas seguros (National Institute of Standards and Technology, 2020; Sermersheim, 2006).

6. **Preparação Profissional**: Este projeto simula um cenário real de consultoria onde um cliente solicita uma infraestrutura completa com segmentação de rede profissional, preparando-nos para as exigências do mercado de trabalho em cibersegurança e administração de sistemas (**kim2021**).

7. **Plataforma de Colaboração Moderna**: A opção pelo Nextcloud em vez de partilhas Samba tradicionais (The Samba Team, 2025) reflete a evolução das necessidades empresariais modernas, onde a colaboração em tempo real, acesso móvel e funcionalidades como calendários partilhados são tão importantes quanto o simples armazenamento de ficheiros (**kurnia2021**). Esta decisão prepara a infraestrutura para cenários de trabalho híbrido e distribuído (**nist800-145**).

8. **Visibilidade e Controlo Centralizado**: A interface *web* do pfSense proporciona visibilidade em tempo real do tráfego de rede (**rfc3954**), permitindo análise de *logs*, monitorização de largura de banda, e ajustes dinâmicos de regras, competências fundamentais para administradores de rede modernos (**pfsensebook2024**).

1.2 Objetivos

Esta secção apresenta o propósito central do projeto e os objetivos específicos que operacionalizam a sua concretização.

1.2.1 Objetivo Geral

Implementar e documentar uma infraestrutura de rede empresarial segura baseada numa arquitetura Three-Legged Firewall, integrando serviços essenciais com políticas de acesso rigorosas e mecanismos de proteção em múltiplas camadas.

Esta arquitetura estabelece zonas de segurança claramente definidas, controladas por uma *firewall* central que atua como ponto único de aplicação de políticas. O pfSense, enquanto *firewall open-source* de nível empresarial, constitui a peça central da solução, orquestrando o tráfego entre zonas e aplicando políticas granulares baseadas no princípio de *defense in depth* (Kumar & Sharma, 2022; Netgate, 2024).

1.2.2 Objetivos Específicos

Os objetivos específicos representam os componentes críticos da infraestrutura, organizados em quatro dimensões: segurança perimetral, gestão de identidades, serviços de infraestrutura e documentação.

Segurança Perimetral e Segmentação

1. **Implementar pfSense como *firewall* central**, configurando quatro interfaces (WAN, LAN, DMZ, VPN) com segmentação rigorosa e filtragem *stateful* (Netgate, 2024).

2. **Configurar regras de *firewall* granulares** seguindo o princípio de *default deny*, onde cada fluxo permitido é explicitamente autorizado, minimizando superfície de ataque e impedindo movimentação lateral (Syed et al., 2022).

3. **Segmentar a rede em quatro zonas** com níveis de confiança distintos:

    - **WAN**: Interface externa, zona não confiável
    - **LAN**: Recursos corporativos sensíveis, confiança elevada
    - **DMZ**: Serviços públicos isolados, confiança intermédia
    - **VPN**: Túnel cifrado para acesso remoto seguro

4. **Registar domínio público com Cloudflare**, implementando Web Application Firewall (WAF), mitigação Distributed Denial of Service (DDoS) e Content Delivery Network (Rede de Distribuição de Conteúdo) (CDN) como camada adicional de proteção antes do perímetro.

Gestão de Identidades e Acesso

5. **Implementar AD Domain Controller (Controlador de Domínio) (DC)** para gestão centralizada de identidades, autenticação unificada e políticas de grupo (The Samba Team, 2025).
6. **Configurar OpenVPN com autenticação Remote Authentication Dial-In User Service (RADIUS)/LDAP**, utilizando certificados digitais e integração com AD para acesso remoto seguro (Netgate, 2024; Stallings, 2016).
7. **Estabelecer políticas de segurança abrangentes**: senhas robustas, Access Control List (Lista de Controlo de Acesso) (ACL) em partilhas de ficheiros, *logging* de auditoria e Network Address Translation (NAT) controlado para serviços DMZ.

Serviços de Infraestrutura

8. **Implementar serviços críticos**: Dynamic Host Configuration Protocol (DHCP) e Domain Name System (Sistema de Nomes de Domínio) (DNS) internos, servidor de ficheiros com Nextcloud (Nextcloud GmbH, 2024), servidor *web* na DMZ, e integração LDAP para Single Sign-On (SSO).
9. **Configurar servidor de *email* corporativo** com Mailcow (mailcow Community, 2024), implementando proteção *anti-spam*, *anti-malware*, e autenticação Sender Policy Framework (SPF)/DomainKeys Identified Mail (DKIM)/Domain-based Message Authentication, Reporting and Conformance (DMARC) (Crocker et al., 2011; Kitterman, 2014; Kucherawy & Zwicky, 2015).

Documentação e Sustentabilidade

10. **Documentar exaustivamente** todos os processos: decisões arquiteturais, configurações, inventário de regras, diagramas de rede, procedimentos operacionais (SOPs) e *runbooks* para resposta a incidentes (**kovelamudi2024**).

Este conjunto de objetivos reflete uma abordagem onde considerações técnicas, de segurança e operacionais são equilibradas para produzir uma solução robusta, escalável e alinhada com as melhores práticas da indústria.

1.3 Importância e Aplicabilidade

A implementação de uma infraestrutura de rede empresarial segura representa um desafio multidisciplinar que integra conhecimentos essenciais para qualquer profissional de tecnologias de informação. Esta secção explora a relevância do projeto em três dimensões: valor académico, aplicabilidade profissional e alinhamento com tendências tecnológicas.

1.3.1 Relevância Académica

O projeto constitui um exercício integrador que mobiliza conhecimentos de múltiplas áreas: redes de computadores (Tanenbaum et al., 2021) (TCP/IP, VLANs, NAT), sistemas operativos (administração Linux/Windows), segurança da informação (Stallings, 2016) (*firewalls*, políticas, defesa em profundidade), e serviços de rede (DNS, DHCP, LDAP, *email*).

Ao contrário de exercícios laboratoriais isolados, este trabalho exige compreensão das interdependências entre componentes e capacidade de tomar decisões arquiteturais fundamentadas. A utilização da pfSense (Netgate, 2024), solução amplamente implementada na indústria, proporciona experiência direta com ferramentas encontradas em ambientes profissionais reais.

1.3.2 Aplicabilidade Profissional

As competências desenvolvidas são diretamente aplicáveis em funções de elevada procura no mercado: administração de sistemas (gestão de infraestruturas, *backup*, disponibilidade), engenharia de segurança (análise de vulnerabilidades, gestão de *firewalls*, resposta a incidentes), administração de redes (segmentação, VPNs, *troubleshooting*) e consultoria (desenho de arquiteturas, implementação de soluções *open-source*).

A experiência prática com soluções *open-source* de nível empresarial constitui diferencial competitivo, demonstrando capacidade de implementar soluções concretas e não apenas conhecimentos teóricos.

1.3.3 Alinhamento com Tendências Tecnológicas

O projeto alinha-se com movimentos que definem o futuro das infraestruturas empresariais:

- **Zero Trust Architecture**: A segmentação rigorosa e o princípio de menor privilégio implementados refletem o paradigma "*never trust, always verify*" (Syed et al., 2022; Weinberg et al., 2024).
- **Open-Source Enterprise**: A adoção empresarial de soluções *open-source* tornou-se norma, desde Linux em servidores até Kubernetes em orquestração.
- **Trabalho Remoto**: A implementação de VPN robusta responde diretamente à realidade de trabalho híbrido pós-pandemia.
- **Conformidade Regulamentar**: Políticas documentadas, controlos de acesso e *logs* de auditoria facilitam cumprimento de RGPD, NIS2, ISO 27002 (International Organization for Standardization, 2022) e NIST (National Institute of Standards and Technology, 2020).

Em síntese, o projeto transcende um exercício técnico, constituindo experiência formativa com relevância académica, aplicabilidade profissional imediata e alinhamento com tendências emergentes.

1.4 Estrutura do Relatório

O presente relatório está organizado em cinco capítulos principais, complementados por anexos técnicos. A documentação detalhada de cada componente encontra-se disponível no repositório do projeto (Barbosa et al., 2025a), arquivado com DOI (Barbosa et al., 2025b), sendo referenciada ao longo do texto.

Capítulo 1 — Introdução: contextualiza o projeto no âmbito da segurança da informação empresarial, apresentando a motivação para a implementação de uma infraestrutura segmentada com *firewall* central. Define os objetivos gerais e específicos, organizados por dimensões (segurança perimetral, gestão de identidades, serviços e documentação), e discute a relevância académica e profissional do trabalho.

Capítulo 2 — Estado da Arte: apresenta uma revisão detalhada sobre infraestruturas de rede empresariais, abordando desde os fundamentos teóricos até às tecnologias e práticas mais recentes na área de administração de sistemas e segurança da informação. Inclui análise de modelos de arquitetura de rede, tecnologias de virtualização, gestão de identidades, segurança perimetral, serviços de colaboração, monitorização, sistemas IDS/IPS e conformidade regulatória.

Capítulo 3 — Metodologia: descreve a abordagem metodológica adotada para a conceção, implementação e validação da infraestrutura. Apresenta os requisitos identificados (obrigatórios e adicionais), os critérios de seleção tecnológica, a arquitetura da solução, o planeamento temporal do projeto e as ferramentas utilizadas ao longo do desenvolvimento.

Capítulo 4 — Implementação da Infraestrutura: documenta a implementação técnica de todos os componentes, organizado nos seguintes eixos:

- **Plataforma de Virtualização**: Configuração do Proxmox Virtual Environment (PVE) e gestão de recursos.
- **Arquitetura de Rede**: Implementação do modelo Four-Legged Firewall com pfSense, incluindo segmentação em zonas (WAN, LAN, DMZ, VPN) e políticas de acesso.
- **Firewall e Segurança Perimetral**: Configuração do pfSense, OpenVPN com autenticação RADIUS, NAT e *port forwarding*.
- **Gestão de Identidades**: Samba AD DC, DNS integrado, DHCP e FreeRADIUS com integração LDAP.
- **Serviços Aplicacionais**: Nextcloud, Zammad, Mailcow, *webserver* Nginx, Cloudflare e CrowdSec.
- **Monitorização**: Netdata Cloud para observabilidade centralizada.
- **Backup e Recuperação**: Proxmox Backup Server (PBS) e backup do AD.

Para detalhes técnicos completos, incluindo comandos e ficheiros de configuração, o leitor é remetido para a documentação no repositório (Barbosa et al., 2025a).

Capítulo 5 — Conclusão: sintetiza as principais conclusões do projeto, avalia o cumprimento dos objetivos estabelecidos (requisitos obrigatórios e funcionalidades de valor acrescentado), apresenta os contributos do trabalho e as competências desenvolvidas, identifica limitações e dificuldades encontradas, e propõe direções para trabalho futuro.

Anexos: incluem documentação complementar de suporte, nomeadamente:

- **Apêndice A — Imagens**: Capturas de ecrã de configurações, incluindo regras de *firewall* por pool VPN, Nextcloud, Zammad, Mailcow e componentes de segurança.
- **Apêndice B — Tabelas**: Requisitos adicionais, requisitos funcionais, requisitos não-funcionais e tecnologias selecionadas.

Esta estruturação procura equilibrar rigor técnico, clareza expositiva e completude documental, permitindo ao leitor acompanhar tanto a fundamentação teórica como a implementação prática da solução proposta.

2. Estado da Arte

Este capítulo apresenta uma revisão detalhada sobre infraestruturas de rede empresariais, abordando desde os fundamentos teóricos até às tecnologias e práticas mais recentes na área de administração de sistemas e segurança da informação. A análise do estado da arte permite compreender as tecnologias, protocolos e melhores práticas utilizadas atualmente na implementação de ambientes corporativos seguros e escaláveis.

2.1 Fundamentos de Infraestruturas de Rede Empresariais

As infraestruturas de rede empresariais constituem a espinha dorsal das organizações modernas, suportando a comunicação, o processamento de dados e a entrega de serviços críticos para o negócio. Esta secção apresenta os conceitos fundamentais e os modelos arquiteturais que sustentam estas infraestruturas.

2.1.1 Modelos de Arquitetura de Rede

A arquitetura de uma rede empresarial pode ser conceptualizada através de diferentes modelos, cada um adequado a contextos específicos de dimensão, requisitos de segurança e complexidade organizacional (Tanenbaum et al., 2021).

O **modelo hierárquico de três camadas** (Three-Tier Architecture), proposto pela Cisco, organiza a rede em camadas de *Core*, *Distribution* e *Access*, proporcionando escalabilidade e facilitando a gestão. A camada *Core* fornece conectividade de alta velocidade entre segmentos, a camada *Distribution* implementa políticas de segurança e routing, e a camada *Access* conecta os dispositivos finais (Kurose & Ross, 2021).

Para organizações de menor dimensão ou com requisitos específicos de segurança, o **modelo de firewall multi-interface** oferece uma alternativa pragmática. Este modelo, também conhecido como *Multi-Legged Firewall*, utiliza um único dispositivo de segurança com múltiplas interfaces para segmentar a rede em zonas de confiança distintas (Scarfone & Hoffman, 2009).

2.1.2 Segmentação de Rede e Zonas de Segurança

A segmentação de rede constitui um princípio fundamental na arquitetura de segurança moderna. Ao dividir a infraestrutura em segmentos isolados, limita-se o impacto de potenciais comprometimentos e reduz-se a superfície de ataque (National Institute of Standards and Technology, 2020).

As zonas de segurança típicas numa infraestrutura empresarial incluem:

- **WAN**: Zona externa não confiável, representando a ligação à Internet ou a redes de terceiros.
- **LAN**: Zona interna de elevada confiança, onde residem os recursos corporativos críticos e as estações de trabalho.
- **DMZ**: Zona de confiança intermédia, destinada a serviços que necessitam de exposição à Internet, como servidores *web* e de correio eletrónico.
- **VPN**: Zona para acesso remoto seguro, permitindo a colaboradores externos acederem aos recursos corporativos através de túneis cifrados.

A implementação de uma arquitetura Four-Legged Firewall, onde um único dispositivo gere quatro ou mais interfaces de rede, proporciona um equilíbrio entre segurança robusta e simplicidade operacional, sendo particularmente adequada para pequenas e médias empresas (Netgate, 2024).

2.1.3 Princípios de Defense in Depth

O conceito de *Defense in Depth* (defesa em profundidade) estabelece que a segurança deve ser implementada em múltiplas camadas independentes, de forma que a falha de um mecanismo não comprometa toda a infraestrutura (National Institute of Standards and Technology, 2020).

Este princípio traduz-se na implementação de controlos em diferentes níveis:

1. **Camada de Perímetro**: Firewalls, sistemas de deteção de intrusões (IDS/IPS), e gateways de aplicação.
2. **Camada de Rede**: Segmentação, Virtual Local Area Networks (VLANs), e políticas de routing.
3. **Camada de Host**: Antivírus, *hardening* do sistema operativo, e controlos de acesso local.
4. **Camada de Aplicação**: Autenticação, autorização, e validação de dados.
5. **Camada de Dados**: Cifração em repouso e em trânsito, políticas de *backup* e recuperação.

A aplicação consistente destes princípios resulta numa postura de segurança resiliente, capaz de resistir a múltiplos vetores de ataque (Stallings, 2016).

2.2 Virtualização e Consolidação de Serviços

A virtualização revolucionou a forma como as infraestruturas de TI são concebidas, implementadas e geridas. Esta secção examina as tecnologias de virtualização disponíveis e os critérios para a sua seleção em contexto empresarial.

2.2.1 Evolução das Plataformas de Virtualização

A virtualização permite executar múltiplos sistemas operativos e aplicações num único servidor físico, através de uma camada de abstração denominada Hypervisor. Esta tecnologia proporciona benefícios significativos em termos de consolidação de recursos, eficiência energética, e agilidade operacional (VMware, Inc., 2024).

Os Hypervisors classificam-se em dois tipos principais. Os Hypervisors de Tipo 1 (ou *bare-metal*) executam diretamente sobre o hardware, oferecendo melhor desempenho e são utilizados em ambientes de produção. Exemplos incluem VMware ESXi, Microsoft Hyper-V, e PVE. Os Hypervisors de Tipo 2 executam sobre um sistema operativo anfitrião, sendo mais adequados para ambientes de desenvolvimento e testes. Exemplos incluem VMware Workstation e Oracle VirtualBox.

2.2.2 Comparação de Soluções de Virtualização

O mercado de virtualização oferece diversas opções, cada uma com características distintas que as tornam adequadas para diferentes contextos:

VMware vSphere/ESXi constitui a solução líder de mercado em ambientes empresariais, oferecendo funcionalidades avançadas como vMotion, DRS (*Distributed Resource Scheduler*), e integração com ecossistemas de *backup* e recuperação de desastres. Contudo, os custos de licenciamento podem ser proibitivos para organizações de menor dimensão (VMware, Inc., 2024).

Microsoft Hyper-V integra-se nativamente com o ecossistema Windows Server, sendo uma opção natural para organizações já investidas em tecnologias Microsoft. A versão gratuita (Hyper-V Server) oferece funcionalidades básicas, enquanto as versões completas requerem licenciamento Windows Server.

PVE emerge como alternativa *open-source* de referência, combinando virtualização Kernel-based Virtual Machine (KVM) com containers Linux Containers (LXC) numa única plataforma. A ausência de custos de licenciamento, aliada a funcionalidades *enterprise* como clustering, *live migration*, e integração com Ceph para armazenamento distribuído, torna-o particularmente atrativo para organizações com competências técnicas internas (Proxmox Server Solutions GmbH, 2024).

A Tabela 2.1 evidencia uma breve comparação entre as plataformas citadas.

Tabela 2.1: Comparação de Plataformas de Virtualização

Critério	VMware ESXi	Hyper-V	Proxmox VE
Licenciamento	Proprietário	Proprietário	Open-source
Custo	Elevado	Moderado	Zero
Interface	vSphere Client	Hyper-V Manager	Web UI
Clustering	Sim (vCenter)	Sim	Sim (nativo)
Live Migration	vMotion	Live Migration	Sim
Containers	Não nativo	Não nativo	LXC nativo
Suporte	Comercial	Comercial	Comunidade/Pago

2.2.3 Containerização vs. Virtualização Tradicional

A containerização, popularizada pelo Docker, oferece uma alternativa leve à virtualização tradicional. Enquanto as máquinas virtuais virtualizam o hardware e executam sistemas operativos completos, os containers partilham o kernel do sistema anfitrião, resultando em menor *overhead* e tempos de arranque mais rápidos (Docker, Inc., 2024).

Esta distinção tem implicações práticas na arquitetura de infraestruturas. Serviços que requerem isolamento completo ou sistemas operativos distintos beneficiam da virtualização tradicional. Aplicações *stateless*, microsserviços, e cargas de trabalho que requerem escalabilidade horizontal são candidatos ideais para containerização.

Plataformas modernas como o PVE permitem combinar ambas as abordagens, executando máquinas virtuais KVM para serviços que requerem isolamento completo (firewalls, domain controllers) e containers LXC para serviços auxiliares com menor *overhead*.

2.3 Gestão de Identidades e Autenticação

A gestão centralizada de identidades constitui um pilar fundamental em infraestruturas empresariais, permitindo autenticação unificada, aplicação consistente de políticas, e auditoria de acessos. Esta secção examina as tecnologias e protocolos que suportam estes requisitos.

2.3.1 Active Directory e Alternativas Open-Source

O **Microsoft AD** estabeleceu-se como o padrão *de facto* para gestão de identidades em ambientes empresariais Windows. O AD combina serviços de diretório LDAP, autenticação Kerberos, e políticas de grupo (Group Policy Object (GPO)) numa solução integrada (The Samba Team, 2025).

Para organizações que procuram alternativas aos custos de licenciamento Microsoft, o **Samba AD DC** oferece uma implementação *open-source* compatível com o protocolo AD. A partir da versão 4.0, o Samba suporta funcionalidades de DC, incluindo autenticação Kerberos, replicação de diretório, e políticas de grupo básicas (The Samba Team, 2025).

A compatibilidade do Samba AD DC com clientes Windows permite cenários híbridos onde estações de trabalho Windows ingressam no domínio e autenticam-se de forma transparente, beneficiando de SSO para recursos de rede.

2.3.2 Protocolos de Autenticação

Os protocolos de autenticação em ambientes empresariais evoluíram para responder a requisitos crescentes de segurança e interoperabilidade:

LDAP fornece acesso padronizado a serviços de diretório, permitindo que aplicações consultem e modifiquem informações de utilizadores, grupos e recursos. A versão segura, LDAPS, adiciona cifração Transport Layer Security (TLS) ao protocolo base (Sermersheim, 2006).

Kerberos implementa autenticação baseada em *tickets*, eliminando a transmissão de passwords pela rede. O protocolo utiliza um Key Distribution Center (KDC) para emitir *tickets* que comprovam a identidade do utilizador perante serviços de rede (MIT Kerberos Consortium, 2023).

RADIUS estende a autenticação centralizada a dispositivos de rede como access points WiFi, switches, e concentradores VPN. A integração de RADIUS com backends LDAP permite autenticação unificada em toda a infraestrutura (Rigney et al., 2000).

2.3.3 Single Sign-On e Federação de Identidades

O SSO permite aos utilizadores autenticarem-se uma única vez e acederem a múltiplos serviços sem necessidade de reintroduzir credenciais. Esta funcionalidade melhora a experiência do utilizador e reduz a proliferação de passwords (Stallings, 2016).

Em ambientes AD, o SSO é implementado nativamente através de Kerberos. Quando um utilizador inicia sessão no domínio, obtém um Ticket-Granting Ticket (TGT) que permite solicitar tickets de serviço para recursos específicos sem nova autenticação.

Para aplicações web e serviços cloud, protocolos de federação como SAML 2.0 e OpenID Connect permitem estender o SSO além das fronteiras da organização, facilitando a integração com fornecedores de serviços externos.

2.4 Segurança Perimetral e Firewalls

O Firewall constitui a primeira linha de defesa numa infraestrutura de rede, controlando o tráfego entre zonas de diferentes níveis de confiança. Esta secção analisa as tecnologias de Firewall disponíveis e os critérios para a sua seleção.

2.4.1 Evolução das Tecnologias de Firewall

As tecnologias de Firewall evoluíram significativamente desde os primeiros filtros de pacotes estáticos. Os **firewalls stateful** mantêm informação sobre o estado das conexões, permitindo decisões mais inteligentes baseadas no contexto da comunicação (Wool, 2010).

Os **Next-Generation Firewalls** (NGFW) integram funcionalidades adicionais como inspeção profunda de pacotes (DPI), prevenção de intrusões (IPS), filtragem de aplicações, e integração com feeds de inteligência de ameaças. Estas funcionalidades permitem políticas baseadas não apenas em endereços Internet Protocol (Protocolo de Internet) (IP) e portas, mas também em aplicações e utilizadores (Palo Alto Networks, 2024).

2.4.2 Soluções Open-Source vs. Comerciais

O mercado de firewalls apresenta opções que variam desde soluções *open-source* gratuitas até appliances comerciais de elevado custo:

pfSense emerge como a solução *open-source* mais popular, baseada em FreeBSD e oferecendo funcionalidades *enterprise* como VPN, IDS/IPS (via Snort ou Suricata), balanceamento de carga, e Failover. A interface web intuitiva e a extensa documentação comunitária facilitam a implementação e gestão (Netgate, 2024).

OPNsense, fork do pfSense, oferece uma alternativa com foco em segurança e atualizações mais frequentes. A interface modernizada e o suporte a plugins através de repositório dedicado atraem utilizadores que valorizam estas características.

Soluções comerciais como Cisco ASA, Fortinet FortiGate, e Palo Alto Networks oferecem suporte profissional, certificações de conformidade, e funcionalidades avançadas de gestão centralizada. Contudo, os custos de aquisição e manutenção podem ser significativos (Cisco Systems, Inc., 2024).

A Tabela 2.2 evidencia uma breve comparação entre as plataformas citadas.

2.4.3 Funcionalidades Essenciais

Um Firewall empresarial moderno deve implementar um conjunto de funcionalidades essenciais para proteção eficaz da infraestrutura:

Filtragem Stateful mantém tabelas de estado das conexões, permitindo distinguir entre tráfego legítimo (respostas a conexões iniciadas internamente) e tentativas de intrusão.

Tabela 2.2: Comparação de Soluções de Firewall

Critério	pfSense	FortiGate	Palo Alto
Licenciamento	Open-source	Proprietário	Proprietário
Custo inicial	Zero	Moderado	Elevado
VPN	OpenVPN, IPsec	FortiClient	GlobalProtect
IDS/IPS	Snort/Suricata	FortiGuard	Threat Prevention
Interface	Web UI	FortiManager	Panorama
Suporte	Comunidade	Comercial	Comercial

NAT permite a tradução de endereços IP, essencial para conservação de endereços públicos e para ocultar a topologia interna da rede.

VPN estabelece túneis cifrados para acesso remoto seguro (client-to-site) ou interligação de escritórios (site-to-site). Protocolos comuns incluem OpenVPN, IPsec, e WireGuard.

IDS/IPS analisa o tráfego em busca de padrões maliciosos, alertando ou bloqueando automaticamente atividades suspeitas.

Traffic Shaping permite priorizar tráfego crítico e limitar largura de banda para aplicações não essenciais, garantindo qualidade de serviço (Kumar & Sharma, 2022).

2.5 Serviços de Colaboração e Armazenamento

A colaboração e partilha de ficheiros constituem requisitos fundamentais em qualquer ambiente empresarial. Esta secção examina as soluções disponíveis para responder a estas necessidades, desde abordagens tradicionais até plataformas cloud modernas.

2.5.1 Evolução das Soluções de Armazenamento

As soluções de armazenamento em rede evoluíram significativamente ao longo das últimas décadas. O protocolo **SMB/CIFS** (Server Message Block / Common Internet File System), originalmente desenvolvido pela Microsoft, estabeleceu-se como padrão para partilha de ficheiros em ambientes Windows. O projeto **Samba** (The Samba Team, 2025) implementa este protocolo em sistemas Unix/Linux, permitindo interoperabilidade com clientes Windows.

Contudo, as partilhas SMB tradicionais apresentam limitações significativas no contexto do trabalho moderno. A dependência de conectividade à rede local, a ausência de funcionalidades de colaboração em tempo real, e as dificuldades de acesso móvel motivaram a evolução para plataformas mais sofisticadas.

2.5.2 Plataformas de Colaboração Modernas

As plataformas de colaboração modernas transcendem o simples armazenamento de ficheiros, oferecendo funcionalidades integradas que respondem às necessidades do trabalho híbrido e distribuído.

Nextcloud (Nextcloud GmbH, 2024) emerge como a alternativa *open-source* mais completa a soluções proprietárias como Google Workspace e Microsoft 365. Para além do armazenamento e sincronização de ficheiros, o Nextcloud oferece: calendários partilhados e contactos (CalDAV/CardDAV), edição colaborativa de documentos (integração com Collabora ou OnlyOffice), videoconferência (Nextcloud Talk), cliente de email integrado, e gestão de projetos através de aplicações como Deck.

A possibilidade de instalação *on-premises* garante controlo total sobre os dados, aspeto particularmente relevante para conformidade com Regulamento Geral sobre a Proteção de Dados (RGPD) e requisitos de soberania digital.

Seafile oferece uma alternativa mais leve, focada especificamente na sincronização de ficheiros com desempenho otimizado para grandes bibliotecas. A arquitetura baseada em blocos permite sincronização eficiente de ficheiros grandes e Deduplicação de dados.

2.5.3 Integração com Serviços de Diretório

A integração das plataformas de colaboração com serviços de diretório empresarial (AD ou LDAP) é essencial para gestão centralizada de utilizadores e aplicação consistente de políticas de acesso.

O Nextcloud suporta integração LDAP/AD através da aplicação "LDAP user and group backend", permitindo que utilizadores do domínio acedam à plataforma com as suas credenciais corporativas. Esta integração suporta mapeamento de grupos AD para grupos Nextcloud, sincronização automática de atributos do utilizador, e quotas diferenciadas por grupo (Nextcloud GmbH, 2024).

2.6 Monitorização e Observabilidade

A monitorização contínua da infraestrutura é essencial para garantir disponibilidade, identificar problemas proativamente, e suportar decisões de capacidade. Esta secção examina as abordagens e ferramentas disponíveis para observabilidade em ambientes empresariais.

2.6.1 Conceitos de Observabilidade

A observabilidade em sistemas de TI refere-se à capacidade de compreender o estado interno de um sistema através das suas saídas externas. Três pilares fundamentais sustentam este conceito (Netdata, Inc., 2024):

Métricas representam medições numéricas ao longo do tempo (séries temporais), como utilização de Central Processing Unit (Unidade Central de Processamento) (CPU), memória disponível, ou latência de rede. Permitem identificar tendências e estabelecer baselines de comportamento normal.

Logs registam eventos discretos com contexto detalhado, essenciais para análise forense e debugging. A agregação centralizada de logs de múltiplos sistemas facilita a correlação de eventos.

Traces acompanham o percurso de uma transação através de múltiplos serviços, particularmente relevantes em arquiteturas de microsserviços para identificar gargalos e pontos de falha.

2.6.2 Ferramentas de Monitorização

O ecossistema de ferramentas de monitorização oferece opções que variam em complexidade, custo, e modelo de deployment:

Nagios e **Zabbix** representam soluções tradicionais, focadas em monitorização baseada em polling e alertas. Embora robustas e amplamente documentadas, requerem configuração extensiva e podem apresentar limitações em ambientes dinâmicos.

Prometheus popularizou o modelo de métricas "pull-based" e o formato de exposição que se tornou padrão em ambientes containerizados. A integração com Grafana proporciona capacidades de visualização avançadas.

Netdata (Netdata, Inc., 2024) distingue-se pela abordagem "zero-configuration", oferecendo milhares de métricas automaticamente descobertas com granularidade de 1 segundo. A versão Cloud adiciona agregação centralizada, alertas inteligentes, e capacidades de Machine Learning (Aprendizagem Automática) (ML) para deteção de anomalias.

2.6.3 Alertas e Resposta a Incidentes

A configuração adequada de alertas é crítica para transformar dados de monitorização em ações. Boas práticas incluem a definição de limiares baseados em baselines históricos em vez de valores absolutos arbitrários, a implementação de *alert fatigue mitigation* através de agregação e supressão inteligente, e o estabelecimento de procedimentos de escalonamento claros com responsabilidades definidas.

A integração de ferramentas de monitorização com sistemas de ticketing e plataformas de comunicação (email, Slack, SMS) garante que alertas críticos chegam às pessoas certas em tempo útil.

2.7 Sistemas de Deteção e Prevenção de Intrusões

A proteção contra ameaças em infraestruturas modernas requer abordagens que vão além do Firewall tradicional, incorporando análise comportamental e inteligência de ameaças colaborativa.

2.7.1 IDS/IPS Tradicionais

Os sistemas de deteção de intrusões (IDS) analisam o tráfego de rede em busca de padrões conhecidos de atividade maliciosa, alertando os administradores quando identificam correspondências. Os sistemas de prevenção (IPS) adicionam a capacidade de bloquear automaticamente o tráfego identificado como malicioso.

Snort, desenvolvido pela Cisco, constitui o motor IDS *open-source* mais amplamente utilizado, com uma base de regras extensa mantida pela comunidade. **Suricata** oferece uma alternativa mais moderna, com suporte nativo a multi-threading e protocolos adicionais.

Ambas as soluções podem ser integradas com firewalls como pfSense, operando em modo inline (IPS) ou passivo (IDS).

2.7.2 Abordagens Colaborativas: CrowdSec

CrowdSec (CrowdSec, 2024) representa uma evolução no paradigma de proteção contra ameaças, combinando deteção local com inteligência colaborativa global. O sistema analisa logs de aplicações e sistemas, identificando comportamentos maliciosos através de cenários configuráveis.

Quando uma ameaça é identificada localmente, a informação é partilhada (de forma anonimizada) com a comunidade CrowdSec, contribuindo para uma Blocklist colaborativa que beneficia todos os participantes. Esta abordagem "crowd-sourced" permite resposta rápida a novas ameaças, mesmo antes de assinaturas tradicionais serem desenvolvidas.

A arquitetura do CrowdSec separa a deteção (agente) da remediação (Bouncers), permitindo integração flexível com diferentes pontos de aplicação: firewalls, Reverse Proxys, ou aplicações específicas.

2.8 Conformidade e Aspetos Regulatórios

A implementação de infraestruturas de TI deve considerar o enquadramento legal e regulatório aplicável, particularmente no que respeita à proteção de dados pessoais. Esta secção examina os principais requisitos e as suas implicações técnicas.

2.8.1 Regulamento Geral sobre a Proteção de Dados (RGPD)

O RGPD (*Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Regulamento Geral sobre a Proteção de Dados)*, 2016), em vigor desde maio de 2018, estabelece o quadro legal para o tratamento de dados pessoais na União Europeia. Os seus princípios fundamentais têm implicações diretas na arquitetura de sistemas de informação:

Minimização de dados: Apenas devem ser recolhidos e tratados os dados estritamente necessários para a finalidade específica.

Limitação da conservação: Os dados devem ser mantidos apenas durante o período necessário, exigindo políticas de retenção e eliminação automatizada.

Integridade e confidencialidade: Medidas técnicas adequadas devem proteger os dados contra acessos não autorizados, incluindo cifração e controlos de acesso.

Responsabilidade demonstrável: As organizações devem ser capazes de demonstrar conformidade através de documentação, auditorias, e registos de atividades de tratamento.

2.8.2 Soberania Digital e Localização de Dados

O conceito de soberania digital ganha relevância crescente, particularmente após decisões judiciais como Schrems II, que invalidou o Privacy Shield para transferências de dados entre a UE e os EUA (*Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II)*, 2020).

A implementação de infraestruturas *on-premises* ou em *clouds* privadas garante controlo total sobre a localização dos dados, eliminando dependências de mecanismos legais complexos como Standard Contractual Clauses (SCCs) para transferências internacionais.

Este aspeto é particularmente relevante para organizações nos setores público, saúde, e financeiro, onde requisitos regulatórios específicos podem impor restrições adicionais à localização e tratamento de dados.

2.8.3 Implicações Técnicas da Conformidade

A conformidade regulatória traduz-se em requisitos técnicos específicos:

- **Logging e auditoria**: Registos detalhados de acessos e operações sobre dados pessoais, com retenção adequada.
- **Cifração**: Proteção de dados em repouso (volumes de armazenamento) e em trânsito (TLS para comunicações).
- **Controlos de acesso**: Implementação do princípio do menor privilégio, com autenticação forte e segregação de funções.
- **Gestão de incidentes**: Procedimentos documentados para resposta a violações de dados, incluindo notificação às autoridades no prazo de 72 horas.
- **Backups e recuperação**: Capacidade de restaurar dados e garantir disponibilidade, com testes periódicos de recuperação.

2.9 Síntese e Tendências Emergentes

A análise do estado da arte revela um ecossistema tecnológico maduro, onde soluções *open-source* atingiram paridade funcional com alternativas comerciais em muitos domínios. Esta realidade abre possibilidades para organizações que procuram equilibrar custos, funcionalidades, e independência tecnológica.

2.9.1 Convergência de Tecnologias

Observa-se uma tendência de convergência entre tecnologias tradicionalmente distintas. Plataformas de virtualização integram containerização (PVE com LXC), firewalls incorporam funcionalidades de IDS/IPS e VPN (pfSense), e plataformas de colaboração oferecem suites completas de produtividade (Nextcloud).

Esta convergência simplifica a arquitetura global, reduzindo o número de componentes a gerir e os pontos de integração entre sistemas.

2.9.2 Zero Trust Architecture

O paradigma *Zero Trust* representa uma mudança fundamental na abordagem à segurança, abandonando o modelo tradicional de perímetro em favor do princípio "never trust, always verify". Em vez de confiar implicitamente em tráfego interno, cada acesso é validado independentemente da origem (Syed et al., 2022; Weinberg et al., 2024).

A implementação de Zero Trust em ambientes empresariais passa pela micro-segmentação de rede (políticas granulares entre todos os segmentos), autenticação contínua (verificação não apenas no login, mas ao longo da sessão), acesso baseado em contexto (considerando dispositivo, localização, e comportamento), e cifração ubíqua (proteção de todas as comunicações, internas e externas).

2.9.3 Automação e Infrastructure as Code

A gestão manual de infraestruturas complexas torna-se insustentável à medida que a escala aumenta. Ferramentas de automação como Ansible, Terraform, e Puppet permitem definir a infraestrutura de forma declarativa, garantindo consistência, reprodutibilidade, e documentação implícita através do código.

A adoção de práticas DevOps/GitOps na gestão de infraestruturas tradicionais representa uma tendência crescente, com benefícios demonstrados em termos de agilidade, redução de erros, e capacidade de recuperação.

Em síntese, o estado da arte apresenta um panorama onde organizações de qualquer dimensão podem implementar infraestruturas robustas, seguras, e funcionalmente completas, combinando tecnologias *open-source* maduras com práticas operacionais modernas. O desafio reside menos na disponibilidade de tecnologia e mais na capacidade de integrar componentes de forma coerente e sustentável.

3. Metodologia

Este capítulo descreve a abordagem metodológica adotada para a conceção, implementação e validação da infraestrutura de rede empresarial FSociety. São apresentados os requisitos identificados (obrigatórios e adicionais), os critérios de seleção tecnológica, o planeamento temporal do projeto, e as ferramentas utilizadas ao longo do desenvolvimento.

3.1 Abordagem Metodológica

O desenvolvimento deste projeto seguiu uma abordagem iterativa e incremental, estruturada em fases que permitiram cumprir os requisitos obrigatórios do enunciado e, progressivamente, adicionar funcionalidades que elevassem a infraestrutura a um nível de maturidade empresarial.

3.1.1 Fases do Projeto

O projeto foi estruturado em cinco fases principais:

1. **Análise e Planeamento**: Interpretação do enunciado, levantamento de requisitos obrigatórios e identificação de oportunidades de melhoria.
2. **Preparação do Ambiente**: Instalação da plataforma de virtualização, criação das redes virtuais (LAN, DMZ, VPN), e provisionamento das máquinas virtuais base.
3. **Implementação Base (Nível 1)**: Configuração dos serviços obrigatórios — DHCP, partilha de ficheiros, Firewall com políticas básicas.
4. **Implementação Avançada (Nível 2 + Extras)**: DMZ com servidor HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto) (HTTP), DNS, evolução para arquitetura Four-Legged Firewall, e implementação de serviços adicionais (email, VPN com RADIUS, monitorização, IDS/IPS).
5. **Validação e Documentação**: Testes de integração, validação de segurança, e elaboração da documentação técnica.

3.1.2 Princípios Orientadores

A implementação foi guiada por cinco princípios fundamentais, derivados de boas práticas da indústria e recomendações de *frameworks* como o NIST SP 800-53 (National Institute of Standards and Technology, 2020):

- **Segmentação Rigorosa**: Isolamento completo entre zonas de confiança distintas (WAN, LAN, DMZ, VPN).
- **Defense in Depth**: Implementação de controlos de segurança em múltiplas camadas independentes.
- **Least Privilege**: Política Default Deny com permissões explícitas mínimas necessárias.
- **Visibilidade Contínua**: Logging centralizado e monitorização em tempo real de todos os componentes.
- **Simplicidade Operacional**: Preferência por soluções com interfaces de gestão intuitivas.

3.1.3 Requisitos Adicionais (Valor Acrescentado)

Para além dos requisitos obrigatórios, a equipa identificou oportunidades de enriquecer a infraestrutura com funcionalidades que aproximassem o projeto de um cenário empresarial real. Estas extensões incluem a evolução para uma arquitetura Four-Legged Firewall, implementação de AD com Samba AD DC, servidor de email completo (Mailcow), plataforma de colaboração (Nextcloud), sistema de deteção de intrusões distribuído (CrowdSec), monitorização centralizada com Artificial Intelligence (Inteligência Artificial) (AI) (Netdata Cloud), entre outros.

A Tabela B.1 no Anexo B apresenta o detalhe completo dos requisitos adicionais implementados e a respetiva justificação.

3.1.4 Requisitos Funcionais

Os requisitos funcionais definem as capacidades que o sistema deve providenciar aos seus utilizadores. Resultam da consolidação dos requisitos obrigatórios do enunciado com as funcionalidades adicionais identificadas pela equipa.

Estes requisitos abrangem seis domínios principais: infraestrutura de rede (segmentação, DHCP, DNS), segurança perimetral (Firewall, IDS/IPS), serviços de rede (HTTP, partilha de ficheiros, email), gestão de identidades (AD/LDAP, SSO), acesso remoto (VPN com RADIUS), e operações (monitorização, backup).

A Tabela B.2 no Anexo B apresenta os requisitos funcionais organizados por domínio, identificando a origem de cada um (enunciado, extra, ou misto).

3.1.5 Requisitos Não-Funcionais

Os requisitos não-funcionais estabelecem critérios de qualidade e restrições técnicas transversais à implementação. Definem as características que o sistema deve exibir independentemente das funcionalidades específicas.

Os principais requisitos não-funcionais abrangem: **segurança** (tráfego entre zonas via Firewall, TLS 1.2+, políticas de passwords), **desempenho** (latência LDAP < 100ms, overhead de monitorização < 3%), **disponibilidade** (> 99% para serviços críticos), **escalabilidade** (suporte até 200 utilizadores), **manutenibilidade** (documentação completa e versionada), e **conformidade** (RGPD, soluções *open-source*).

A Tabela B.3 no Anexo B detalha os requisitos não-funcionais por categoria.

3.2 Seleção de Tecnologias

A seleção das tecnologias seguiu um processo estruturado, priorizando soluções *open-source* que satisfizessem tanto os requisitos obrigatórios como os adicionais.

3.2.1 Critérios de Avaliação

As alternativas foram avaliadas segundo cinco critérios:

1. **Adequação Funcional**: Capacidade de satisfazer os requisitos.
2. **Maturidade**: Estabilidade, comunidade e documentação.
3. **Custo**: Licenciamento e operação.
4. **Integração**: Compatibilidade com restantes componentes.
5. **Competências**: Alinhamento com conhecimentos da equipa.

3.2.2 Tecnologias Selecionadas

Com base nos critérios definidos, foram selecionadas tecnologias *open-source* maduras e com comunidades ativas. As principais escolhas incluem: **PVE** para virtualização (interface web completa, KVM+LXC, custo zero), **pfSense** como Firewall (documentação extensa, suporte OpenVPN e RADIUS), **Samba AD DC** para gestão de identidades (compatibilidade Windows, LDAP/Kerberos nativo), **Nextcloud** como plataforma de colaboração (65+ aplicações, integração LDAP), **Mailcow** para email (arquitetura Docker, Rspamd com ML), e **Netdata Cloud** para monitorização (zero-config, granularidade de 1 segundo, AI Insights).

A Tabela B.4 no Anexo B apresenta o resumo completo das tecnologias escolhidas para cada componente da infraestrutura e a respetiva justificação.

3.2.3 Justificação da Arquitetura Four-Legged

O enunciado especificava uma arquitetura Three-Legged Firewall com três zonas: WAN, LAN e DMZ. A equipa optou por estender para Four-Legged Firewall, adicionando uma quarta zona dedicada a VPN.

Esta decisão justifica-se pelos seguintes motivos:

- **Isolamento de Utilizadores Remotos**: Clientes VPN não acedem diretamente à LAN, passando por regras de Firewall específicas.
- **Políticas Granulares**: Possibilidade de definir acessos diferenciados por departamento (TI, Gestores, Financeiro, Comercial).
- **Auditoria**: Tráfego VPN claramente identificável nos logs e na monitorização.
- **Segurança Acrescida**: Compromisso de credenciais VPN não implica acesso direto à rede interna.

3.3 Arquitetura da Solução

Com base nos requisitos identificados e nas tecnologias selecionadas, foi definida a arquitetura lógica e física da infraestrutura. O desenho privilegia a segmentação rigorosa entre zonas de confiança distintas, implementando o modelo Four-Legged Firewall onde todo o tráfego entre segmentos atravessa obrigatoriamente o Firewall central.

3.3.1 Topologia de Rede

A arquitetura implementada organiza a infraestrutura em quatro zonas de segurança, cada uma com políticas de acesso e níveis de confiança diferenciados:

- **WAN** (192.168.31.0/24): Interface externa ligada ao router, zona não confiável com exposição direta à Internet.
- **LAN** (192.168.1.0/24): Rede interna de alta confiança, alojando os serviços críticos — DC, servidor de ficheiros e PBS.
- **DMZ** (10.0.0.0/24): Zona desmilitarizada para serviços expostos à Internet, nomeadamente servidor de email, webserver e Reverse Proxy, isolados da rede interna.
- **VPN** (10.8.0.0/24 + 10.9.0.0/24): Redes dedicadas para utilizadores remotos autenticados, com pools de endereços hierárquicos atribuídos por grupo departamental no AD.

3.3.2 Inventário de Sistemas

A infraestrutura é composta por seis máquinas virtuais executadas sobre PVE. Os recursos apresentados na Tabela 3.1 representam os limites máximos configurados para cada Virtual Machine (Máquina Virtual) (VM); o PVE implementa gestão dinâmica de recursos através de *ballooning* de memória e partilha de CPU, permitindo que recursos não utilizados por uma VM sejam temporariamente alocados a outras com maior carga, otimizando a utilização do hardware físico disponível.

Tabela 3.1: Inventário de Máquinas Virtuais

VM	Função	Zona	vCPU	RAM	Disco
pfSense	Firewall/VPN	Multi	2	2 GB	42 GB
dc.fsociety.pt	AD/DNS/DHCP/RADIUS	LAN	1	1.4 GB	24 GB
files.fsociety.pt	Nextcloud/Zammad	LAN	4	2 GB	50 GB
pbs.fsociety.pt	Backup Server	LAN	2	2 GB	200 GB
mail.fsociety.pt	Mailcow	DMZ	2	6 GB	100 GB
web.fsociety.pt	Reverse Proxy	DMZ	2	1 GB	20 GB
Total			**13**	**14.4 GB**	**436 GB**

3.3.3 Modelo de Segurança em Camadas

A arquitetura implementa o princípio de *Defense in Depth* através de controlos de segurança em quatro camadas independentes. Esta abordagem garante que a falha ou comprometimento de uma camada não resulta em acesso direto aos recursos protegidos, exigindo que um atacante ultrapasse múltiplas barreiras sucessivas.

1. **Edge**: Cloudflare atua como primeira linha de defesa para serviços web públicos, providenciando WAF, mitigação DDoS e terminação TLS.
2. **Perímetro**: pfSense implementa filtragem stateful, NAT e terminação VPN, controlando todo o tráfego entre zonas de segurança.
3. **Host**: CrowdSec opera em cada servidor como IDS/IPS comportamental, partilhando inteligência de ameaças com a comunidade global.
4. **Aplicação**: Autenticação centralizada via LDAP/Kerberos, validação de email (SPF/DKIM/DMARC) e cifração TLS em todas as comunicações.

3.4 Planeamento Temporal

O desenvolvimento decorreu ao longo de aproximadamente 12 semanas como evidenciado na Tabela 3.2, organizadas de forma a cumprir primeiro os requisitos obrigatórios e depois os adicionais, e por fim, validar e documentar todo o projeto.

Tabela 3.2: Cronograma do Projeto

Fase	Semanas	Atividades
Planeamento	1–2	Análise do enunciado, definição de arquitetura, seleção de tecnologias
Ambiente Base	3–4	Proxmox VE, redes virtuais (vmbr0/1/DMZ), VMs base
Nível 1 (Obrigatório)	5–7	pfSense, DHCP, DNS, partilha de ficheiros, firewall básico
Nível 2 (Obrigatório)	8–9	DMZ, servidor HTTP, políticas avançadas de firewall
Extras	10–11	Samba AD, Mailcow, Nextcloud, CrowdSec, Netdata, VPN/RADIUS
Validação	12	Testes, documentação, relatório

3.5 Ferramentas e Ambiente de Trabalho

O desenvolvimento do projeto exigiu a utilização de diversas ferramentas para gestão de código, documentação, comunicação e elaboração do relatório. Esta secção descreve as ferramentas adotadas, a estratégia de documentação seguida e a metodologia de validação aplicada.

3.5.1 Ferramentas Utilizadas

A seleção das ferramentas de desenvolvimento privilegiou soluções gratuitas, colaborativas e adequadas ao contexto académico, permitindo o trabalho simultâneo dos três elementos da equipa.

- **Controlo de Versões**: Git com repositório GitHub para versionamento de configurações, scripts e documentação, permitindo histórico completo de alterações e colaboração assíncrona.
- **Documentação Técnica**: MkDocs com tema Material para documentação estruturada e pesquisável, publicada automaticamente via GitHub Pages.
- **Diagramas**: Draw.io para criação de diagramas de arquitetura de rede, fluxos de dados e topologias.
- **Relatório**: LaTeX com classe ESTG e `biblatex-apa` para formatação académica e gestão de referências bibliográficas conforme norma APA 7.ª edição.
- **Comunicação**: Discord para coordenação diária da equipa, partilha de progresso e resolução de problemas em tempo real.

3.5.2 Estratégia de Documentação

A extensão e complexidade da infraestrutura implementada tornaram impraticável a inclusão de todos os detalhes técnicos no corpo do relatório académico. Optou-se por uma abordagem em dois níveis: o relatório foca-se na análise, justificação de decisões e apresentação de resultados, enquanto a documentação técnica detalhada (guias passo-a-passo, ficheiros de configuração, comandos e procedimentos de troubleshooting) foi mantida no repositório GitHub.

Esta separação permite que o relatório mantenha um foco académico adequado, ao mesmo tempo que disponibiliza documentação técnica completa e reprodutível para quem pretenda replicar ou adaptar a infraestrutura.

A documentação completa está disponível em:

- **GitHub Pages**: https://ryantech00.github.io/fsociety-infrastructure/
- **Zenodo** (arquivo permanente com Digital Object Identifier (DOI)): 10.5281/zenodo.17840636 (Barbosa et al., 2025b)

3.5.3 Metodologia de Validação

A validação da infraestrutura seguiu uma abordagem sistemática e progressiva, garantindo que cada componente funciona corretamente de forma isolada antes de testar a sua integração com os restantes. Esta metodologia permite identificar e corrigir problemas de forma localizada, reduzindo a complexidade do diagnóstico.

1. **Testes Unitários**: Verificação individual de cada serviço após configuração — resolução DNS, autenticação LDAP, conectividade de rede, emissão de certificados TLS.
2. **Testes de Integração**: Validação de fluxos completos envolvendo múltiplos componentes (ex: login VPN → autenticação RADIUS → validação AD → atribuição de IP por grupo → acesso a recursos na LAN).
3. **Testes de Segurança**: Validação externa das configurações de segurança através de ferramentas reconhecidas — SSL Labs para cifração TLS (classificação A+), Mail-Tester para autenticação de email (pontuação 10/10), verificação de regras de Firewall e políticas de acesso.

Os resultados detalhados dos testes e validações são apresentados no Capítulo **??**.

4. Implementação da Infraestrutura

Este capítulo descreve a implementação da infraestrutura de rede empresarial FSociety, detalhando as decisões técnicas tomadas, as configurações realizadas e os desafios encontrados. A apresentação segue a ordem de implementação, respeitando as dependências entre componentes identificadas na metodologia.

Para cada componente, é apresentada uma justificação breve da abordagem adotada, as configurações principais implementadas e os pontos de integração com os restantes serviços. Os guias de instalação passo-a-passo, ficheiros de configuração completos e procedimentos de troubleshooting encontram-se na documentação técnica disponível no repositório do projeto (Barbosa et al., 2025b).

4.1 Plataforma de Virtualização

A infraestrutura física é composta por um único servidor que aloja todas as máquinas virtuais através da plataforma PVE, evidenciado na Figura 4.1. Esta secção descreve a configuração do Hypervisor e a preparação do ambiente de virtualização.

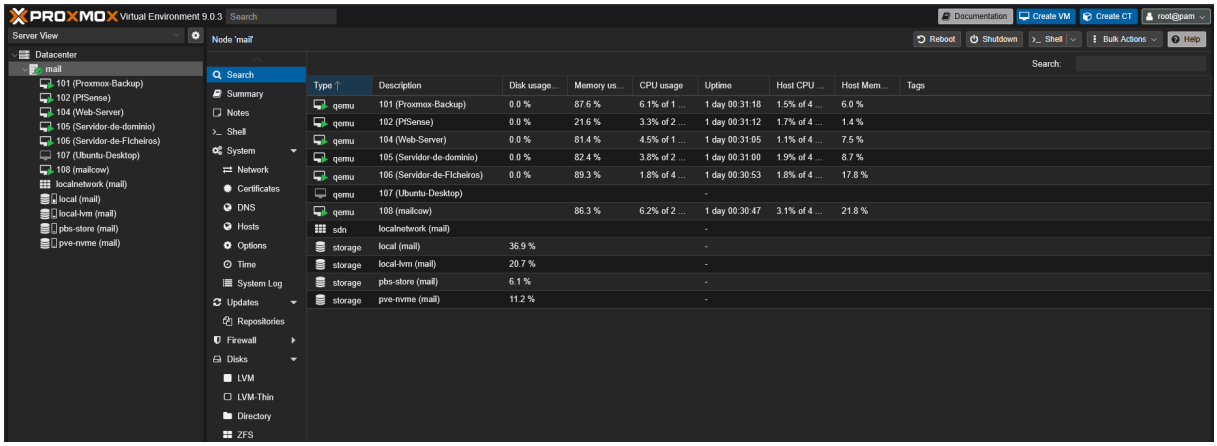


Figura 4.1: Interface Proxmox VE: inventário de VMs e monitorização de recursos com alocação dinâmica via *ballooning*.

4.1.1 Proxmox VE

O PVE foi instalado na versão 9.x sobre o hardware disponível, um portátil convertido em servidor com processador Intel Core i5-7300HQ (4 cores), 16 GB de Random Access Memory (RAM) DDR4 e armazenamento híbrido composto por um HDD de 1 TB e um Solid State Drive (SSD) NVMe de 224 GB.

Configuração de Storage

A estratégia de armazenamento implementada separa as cargas de trabalho por criticidade e requisitos de desempenho:

- **pve-nvme** (NVMe 224 GB): Aloja as VMs críticas que requerem baixa latência de Input/Output (Entrada/Saída) (I/O) — pfSense (Firewall) e DC. A utilização de storage NVMe para estas VMs garante tempos de resposta consistentes para operações de Firewall e autenticação.
- **local-lvm** (HDD 1 TB): Aloja as restantes VMs e backups locais. O maior espaço disponível permite alojar VMs com requisitos de armazenamento mais elevados, como o servidor de email (100 GB) e o PBS (200 GB).

Configuração de Rede

Foram criadas três *bridges* virtuais no Proxmox para suportar a segmentação de rede definida na arquitetura:

Tabela 4.1: Bridges Virtuais do Proxmox

Bridge	Interface	Função	Rede
vmbr0	enp2s0	WAN (Internet)	192.168.31.0/24
vmbr1	—	LAN (Interna)	192.168.1.0/24
vmbr2	—	DMZ	10.0.0.0/24

A bridge `vmbr0` está associada à interface física com acesso à Internet, enquanto `vmbr1` e `vmbr2` são bridges internas sem interface física associada, isolando completamente as redes LAN e DMZ do mundo exterior. Todo o tráfego entre estas redes passa obrigatoriamente pelo pfSense.

Gestão de Recursos

O PVE implementa gestão dinâmica de recursos através de dois mecanismos:

- **Memory Ballooning**: Permite que memória não utilizada por uma VM seja temporariamente disponibilizada a outras com maior carga. Cada VM tem configurado um valor mínimo de memória garantida e um máximo que pode atingir quando há recursos disponíveis.
- **CPU Shares**: Os 4 cores físicos são partilhados entre as VMs através de um sistema de pesos. Em situações de contenção, as VMs críticas (pfSense, DC) têm prioridade sobre as restantes.

Esta abordagem permite alocar nominalmente mais recursos do que os fisicamente disponíveis (overcommitment), confiando no facto de que nem todas as VMs necessitam dos recursos máximos simultaneamente.

4.2 Arquitetura de Rede

A segurança de infraestruturas modernas depende de arquitetura de rede segmentada. A necessidade de expor serviços (email, *web*) à *Internet* mantendo recursos internos protegidos exigiu implementação do modelo Four-Legged Firewall via pfSense (Netgate, 2024).

A documentação técnica detalhada da configuração do pfSense, incluindo todas as regras de Firewall, aliases e configurações NAT, encontra-se disponível no repositório do projeto (Barbosa et al., 2025a).

4.2.1 Princípios de Design

A implementação seguiu cinco princípios: **(1)** Segmentação rigorosa com isolamento entre zonas; **(2)** *Defense in depth* com múltiplas camadas de controlo; **(3)** *Least privilege* com Default Deny (Syed et al., 2022); **(4)** Visibilidade através de *logging* centralizado no pfSense; **(5)** Simplicidade operacional via interface *web*.

4.2.2 Segmentação em Quatro Zonas

A rede foi segmentada em quatro zonas com níveis de confiança distintos:

WAN (192.168.31.100/24) Interface externa com gateway 192.168.31.1. Em ambiente de produção, este endereço seria substituído por IP público. Todo o tráfego entrante é filtrado: bloqueio por *default*, permissão apenas de respostas a conexões internas (*stateful*) (Kumar & Sharma, 2022), e *port forwarding* seletivo para DMZ (HTTP/HyperText Transfer Protocol Secure (HTTPS), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP)).

LAN (192.168.1.0/24) Rede corporativa com recursos críticos: DC Samba AD DC (The Samba Team, 2025) com DNS/DHCP/FreeRADIUS (192.168.1.10), PBS (192.168.1.30), servidor de ficheiros com Nextcloud (Nextcloud GmbH, 2024) (192.168.1.40), e estações de trabalho (DHCP 192.168.1.100–200). Acesso total à *Internet* via NAT, acesso controlado à DMZ, bloqueio de tráfego entrante não solicitado.

DMZ (10.0.0.0/24) Zona de confiança baixa para serviços públicos: servidor de email Mailcow (10.0.0.20) com Postfix, Dovecot, Rspamd e SOGo integrados, e *webserver* com Reverse Proxy Nginx (10.0.0.30). Conexões DMZ↛LAN bloqueadas por omissão, com exceções específicas para integração LDAP com o DC; acesso *Internet* restrito a portas necessárias (SMTP, HTTP/HTTPS, DNS).

VPN (10.8.0.0/24 e 10.9.0.0/24) Dois túneis cifrados (Stallings, 2016) para acesso remoto:

- **OpenVPN Server RADIUS** (User Datagram Protocol (UDP) 1195, 10.8.0.0/24): Servidor principal com autenticação RADIUS integrada ao AD. Endereços atribuídos dinamicamente por grupo AD: TI (10.8.0.10–59), Gestores (10.8.0.60–109), Financeiro (10.8.0.110–159), Comercial (10.8.0.160–209), VPN_Users (10.8.0.210–254).
- **OpenVPN Server Local** (UDP 1194, 10.9.0.0/24): Servidor de backup com autenticação local, utilizado em cenários de emergência quando o DC não está disponível.

Acesso à LAN controlado por grupo através de aliases no pfSense; regras hierárquicas garantem que TI tem acesso total enquanto outros departamentos têm acesso restrito aos recursos necessários.

4.2.3 Plano de Endereçamento

A Tabela 4.2 consolida o plano de endereçamento IP atualizado, refletindo a arquitetura implementada.

4.2.4 Camada de Proteção Externa: Cloudflare

Implementou-se Cloudflare como primeira linha de defesa para serviços *web*, posicionado entre a *Internet* e o pfSense, como evidenciado na Figura 4.2.

Esta camada proporciona WAF, mitigação DDoS, CDN e gestão de certificados Secure Sockets Layer (SSL)/TLS para registos HTTP/HTTPS, enquanto protocolos que requerem conexão direta (SMTP/IMAP, OpenVPN) mantêm resolução DNS-only.

Tabela 4.2: Plano de Endereçamento IP da Infraestrutura FSociety

Zona	Servidor	IP	Serviços
Firewall	pfSense WAN	192. 168.31.100	Gateway externo
	pfSense LAN	192. 168.1.1	Gateway LAN
	pfSense DMZ	10.0. 0.1	Gateway DMZ
	pfSense VPN1	10. 8.0.1	OpenVPN RADIUS
	pfSense VPN2	10.9.0.1	OpenVPN Local
LAN	dc. fsociety.pt	192.168.1.10	AD, DNS, DHCP, RADIUS
	pbs.fsociety. pt	192. 168.1.30	Proxmox Backup
	files.fsociety. pt	192. 168.1.40	Nextcloud
	Clientes DHCP	192.168.1. 100–200	Estações de trabalho
DMZ	mail.fsociety. pt	10. 0.0.20	Mailcow (Email)
	web.fsociety.pt	10.0.0.30	Nginx (Reverse Proxy)
VPN	Pool TI	10. 8.0.10–59	Acesso total
	Pool Gestores	10.8.0.60–109	LAN + DMZ + Internet
	Pool Financeiro	10.8. 0.110–159	DC + Internet
	Pool Comercial	10.8. 0.160–209	DC + Internet
	Pool RH/Users	10.8.0.210–254	Mail + Web + Internet

4.3 Firewall e Segurança Perimetral

O pfSense constitui o elemento central da arquitetura de segurança, implementando o modelo Four-Legged Firewall onde todo o tráfego entre zonas distintas é inspecionado e filtrado.

4.3.1 pfSense

O pfSense CE 2.8.1 foi instalado numa VM com 2 vCPUs, 2 GB de RAM e 42 GB de disco no storage NVMe. A VM possui quatro interfaces de rede virtuais, cada uma ligada a uma bridge diferente ou a uma interface OpenVPN.

Configuração de Interfaces

Tabela 4.3: Interfaces do pfSense

Interface	Nome	Endereço IP	Bridge	Função
vtnet0	WAN	192.168.31.100/24	vmbr0	Acesso Internet
vtnet1	LAN	192.168.1.1/24	vmbr1	Gateway LAN
vtnet2	DMZ	10.0.0.1/24	vmbr2	Gateway DMZ
ovpns1/2	VPN	10.8.0.1 / 10.9.0.1	—	Túneis OpenVPN

Política de Firewall

A política de Firewall implementada segue o princípio Default Deny: todo o tráfego é bloqueado por omissão, sendo explicitamente permitido apenas o necessário para o funcionamento dos serviços. Foram configuradas aproximadamente 100 regras distribuídas pelas quatro interfaces.

A demonstração completa da navegação pelas regras configuradas nas interfaces WAN, LAN, DMZ e OpenVPN está disponível em vídeo[1] e no Anexo A.18.

As regras estão organizadas por interface de origem, seguindo a lógica de que o tráfego é filtrado à entrada. Os principais fluxos permitidos incluem:

- **LAN → WAN**: Acesso à Internet para atualizações e serviços externos.
- **LAN → DMZ**: Acesso a serviços na DMZ (email, web) pelos utilizadores internos.
- **DMZ → LAN**: Apenas queries DNS e LDAP ao DC (portas 53, 389, 636).
- **VPN → LAN**: Acesso diferenciado por grupo AD, controlado através de aliases que mapeiam pools de IP a departamentos.
- **WAN → DMZ**: Port forwards para serviços públicos (HTTPS 443, SMTP 25/587, IMAP 993).

Aliases e Organização

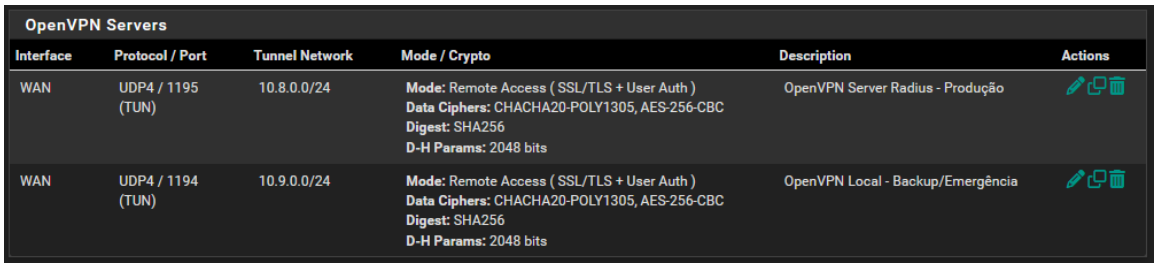
Para facilitar a gestão das regras, foram criados 34 aliases organizados por categoria:

- **Redes**: LAN_NET, DMZ_NET, VPN_RADIUS_NET, VPN_LOCAL_NET
- **Servidores**: DC_Server, Mail_Server, Web_Server, Files_Server
- **Portas**: DNS_Ports, LDAP_Ports, Mail_Ports, Web_Ports
- **Grupos VPN**: VPN_TI, VPN_Gestores, VPN_Financeiro, VPN_Comercial, VPN_RH/USERS

A utilização de aliases permite alterar endereços IP ou portas num único local, propagando automaticamente a alteração para todas as regras que os referenciam.

4.3.2 OpenVPN com Autenticação RADIUS

Foram implementados dois servidores OpenVPN no pfSense, conforme evidencia a Figura 4.3, oferecendo redundância e flexibilidade na autenticação.



OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1195 (TUN)	10.8.0.0/24	**Mode:** Remote Access (SSL/TLS + User Auth) **Data Ciphers:** CHACHA20-POLY1305, AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits	OpenVPN Server Radius - Produção	
WAN	UDP4 / 1194 (TUN)	10.9.0.0/24	**Mode:** Remote Access (SSL/TLS + User Auth) **Data Ciphers:** CHACHA20-POLY1305, AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits	OpenVPN Local - Backup/Emergência	

Figura 4.3: Servidores OpenVPN configurados no pfSense

O servidor RADIUS é o principal, autenticando utilizadores contra o AD através do FreeRADIUS instalado no DC. Esta integração permite:

- **Credenciais únicas**: Utilizadores autenticam-se com as mesmas credenciais do domínio.

[1] Demonstração das regras de firewall (vídeo)

- **Pools hierárquicos**: O FreeRADIUS atribui IPs de ranges específicos conforme o grupo AD do utilizador, permitindo regras de Firewall diferenciadas por departamento.
- **Accounting**: Registo centralizado de sessões VPN para auditoria e conformidade.

O servidor Local serve como backup para situações em que o DC esteja indisponível, permitindo acesso de emergência a administradores.

RADIUS Accounting Daemon

Para além da autenticação, foi desenvolvido um daemon de contabilização que implementa o protocolo RADIUS Accounting conforme definido no RFC 2866 (Rigney, 2000). Este script, executado continuamente no pfSense, monitoriza o ficheiro de status do OpenVPN e envia pacotes de accounting para o FreeRADIUS.

A demonstração do funcionamento do daemon está disponível em vídeo[2] e no Anexo A.19.

O daemon implementa três tipos de eventos:

- **Acct-Start**: Enviado quando um cliente estabelece conexão, registando username, IP atribuído e timestamp de início.
- **Acct-Interim-Update**: Enviado a cada 30 segundos com estatísticas atualizadas de bytes transferidos e duração da sessão.
- **Acct-Stop**: Enviado quando o cliente desconecta, registando os totais finais de tráfego e duração.

O Listing 4.1 apresenta um excerto do daemon que ilustra a função de envio de pacotes RADIUS Accounting.

```
#!/bin/sh
# OpenVPN RADIUS Accounting Daemon
# Implementa RADIUS Accounting (RFC 2866) para OpenVPN no pfSense
# Autor: Hugo Correia | Projeto: FSociety.pt - ESTG/IPP
RADIUS_SERVER="192.168.1.10"
RADIUS_ACCT_PORT="1813"
NAS_IDENTIFIER="pfSense-OpenVPN"
INTERIM_INTERVAL=30
send_radius_accounting() {
    USERNAME="$1"
    SESSION_ID="$2"
    ACCT_STATUS_TYPE="$3"  # Start, Interim-Update, Stop
    FRAMED_IP="$4"
    BYTES_IN="${5:-0}"
    BYTES_OUT="${6:-0}"
    SESSION_TIME="${7:-0}"

    # Criar ficheiro com atributos RADIUS
    cat > "${TEMP_FILE}" <<EOF
User-Name = "${USERNAME}"
Acct-Session-Id = "${SESSION_ID}"
Acct-Status-Type = ${ACCT_STATUS_TYPE}
NAS-IP-Address = ${NAS_IP}
Framed-IP-Address = ${FRAMED_IP}
Acct-Input-Octets = ${BYTES_IN}
Acct-Output-Octets = ${BYTES_OUT}
Acct-Session-Time = ${SESSION_TIME}
EOF

    # Enviar para servidor RADIUS
    radclient "${RADIUS_SERVER}:${RADIUS_ACCT_PORT}" \
```

[2] Demonstração do RADIUS Accounting Daemon (vídeo)

```
        acct "${RADIUS_SECRET}" < "${TEMP_FILE}"
}
```

Listagem 4.1: Excerto do OpenVPN RADIUS Accounting Daemon

Esta funcionalidade permite responder a requisitos de auditoria e conformidade, nomeadamente:

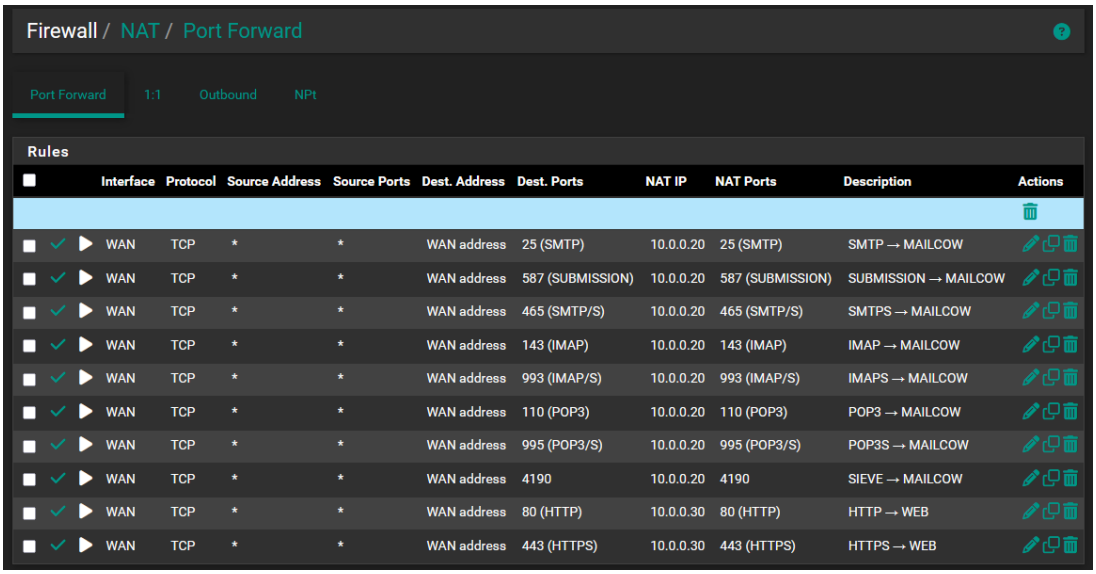
- **Auditoria de acessos**: Registo completo de quem acedeu, quando e durante quanto tempo.
- **Análise de consumo**: Estatísticas de tráfego por utilizador para identificação de anomalias.
- **Compliance**: Rastreabilidade exigida pelo RGPD e normas como ISO 27001.

Os logs de accounting são armazenados no DC em `/var/log/freeradius/radacct/`, organizados por data e IP de origem (NAS). O script completo está disponível na documentação técnica do projeto (Barbosa et al., 2025b) (em docs/03-pfsense/scripts/accounting-daemon.sh).

4.3.3 NAT e Port Forwarding

O pfSense implementa NAT para permitir que as redes internas acedam à Internet através do IP público (via Cloudflare) e port forwarding para expor serviços da DMZ.

A Figura 4.4 apresenta a configuração de port forwarding implementada, incluindo os serviços de email (SMTP, IMAP, POP3, Sieve) redirecionados para o Mailcow (10.0.0.20) e os serviços web (HTTP/HTTPS) redirecionados para o webserver (10.0.0.30).



	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
	WAN	TCP	*	*	WAN address	25 (SMTP)	10.0.0.20	25 (SMTP)	SMTP → MAILCOW	
	WAN	TCP	*	*	WAN address	587 (SUBMISSION)	10.0.0.20	587 (SUBMISSION)	SUBMISSION → MAILCOW	
	WAN	TCP	*	*	WAN address	465 (SMTP/S)	10.0.0.20	465 (SMTP/S)	SMTPS → MAILCOW	
	WAN	TCP	*	*	WAN address	143 (IMAP)	10.0.0.20	143 (IMAP)	IMAP → MAILCOW	
	WAN	TCP	*	*	WAN address	993 (IMAP/S)	10.0.0.20	993 (IMAP/S)	IMAPS → MAILCOW	
	WAN	TCP	*	*	WAN address	110 (POP3)	10.0.0.20	110 (POP3)	POP3 → MAILCOW	
	WAN	TCP	*	*	WAN address	995 (POP3/S)	10.0.0.20	995 (POP3/S)	POP3S → MAILCOW	
	WAN	TCP	*	*	WAN address	4190	10.0.0.20	4190	SIEVE → MAILCOW	
	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.30	80 (HTTP)	HTTP → WEB	
	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.0.0.30	443 (HTTPS)	HTTPS → WEB	

Figura 4.4: Configuração de NAT e Port Forwarding no pfSense

Na prática, o tráfego HTTPS e email passa primeiro pelo Cloudflare (proxy e WAF), que depois encaminha para o IP público do router, sendo este redirecionado para o pfSense via port forward no router doméstico.

4.4 Gestão de Identidades

O DC constitui o serviço central de autenticação e autorização, implementando AD através do Samba AD DC. Esta secção descreve a configuração do domínio e dos serviços associados.

4.4.1 Samba Active Directory Domain Controller

O Samba AD DC 4.x foi provisionado numa VM Ubuntu Server 24.04 LTS com 1 vCPU, 1.4 GB de RAM e 24 GB de disco no storage NVMe. A escolha do NVMe justifica-se pela criticidade do serviço de autenticação, onde a latência de I/O impacta diretamente o tempo de login dos utilizadores.

Informação do Domínio

Tabela 4.4: Parâmetros do Domínio Active Directory

Parâmetro	Valor
Realm Kerberos	FSOCIETY.PT
Nome NetBIOS	FSOCIETY
FQDN do DC	dc.fsociety.pt
Endereço IP	192.168.1.10
Nível Funcional	Windows 2008 R2
DNS Backend	SAMBA_INTERNAL

A utilização do DNS interno do Samba simplifica a gestão ao manter os registos DNS essenciais para o AD (Service Record (SRV), A, Pointer Record (PTR)) sincronizados automaticamente com a base de dados LDAP.

Estrutura Organizacional

Foi definida uma estrutura de Organizational Unit (Unidade Organizacional)s (OUs) que reflete a organização departamental da empresa fictícia:

```
DC=fsociety,DC=pt
  OU=FSociety
      OU=Utilizadores
          OU=TI
          OU=Gestores
          OU=Financeiro
|   |       OU=RH
          OU=Comercial
      OU=Grupos
      OU=Computadores
      OU=Service Accounts
  CN=Users (built-in)
```

Esta estrutura permite aplicar políticas diferenciadas por departamento e facilita a gestão de permissões através de grupos de segurança.

Service Accounts

Para integração com os diversos serviços, foram criadas contas de serviço para queries LDAP:

- **svc_ldap**: Utilizada pelo Nextcloud e Mailcow para queries LDAP. Possui apenas permissão de leitura sobre os objetos de utilizadores e grupos.

O FreeRADIUS utiliza atualmente a conta Administrator para bind LDAP, uma abordagem funcional para ambiente de desenvolvimento. Em produção, recomenda-se a criação de uma service account dedicada (e.g., `svc_radius`) com permissões mínimas, seguindo o princípio do menor privilégio.

A Figura 4.5 permite aceder à demonstração da estrutura do AD implementado com Samba AD DC, incluindo as OUs departamentais, os 19 utilizadores criados, os 6 grupos de segurança e os respetivos membros.

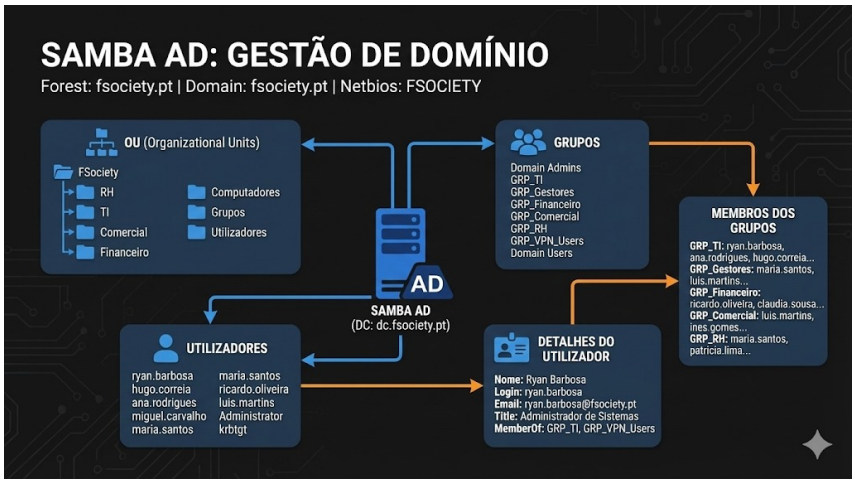


Figura 4.5: Demonstração da estrutura do Samba Active Directory (clique para ver vídeo)

Fluxos de Autenticação

O DC atua como ponto central de autenticação para todos os serviços da infraestrutura, utilizando diferentes protocolos conforme a zona de rede e o tipo de cliente. A Figura 4.6 ilustra os três fluxos principais implementados.

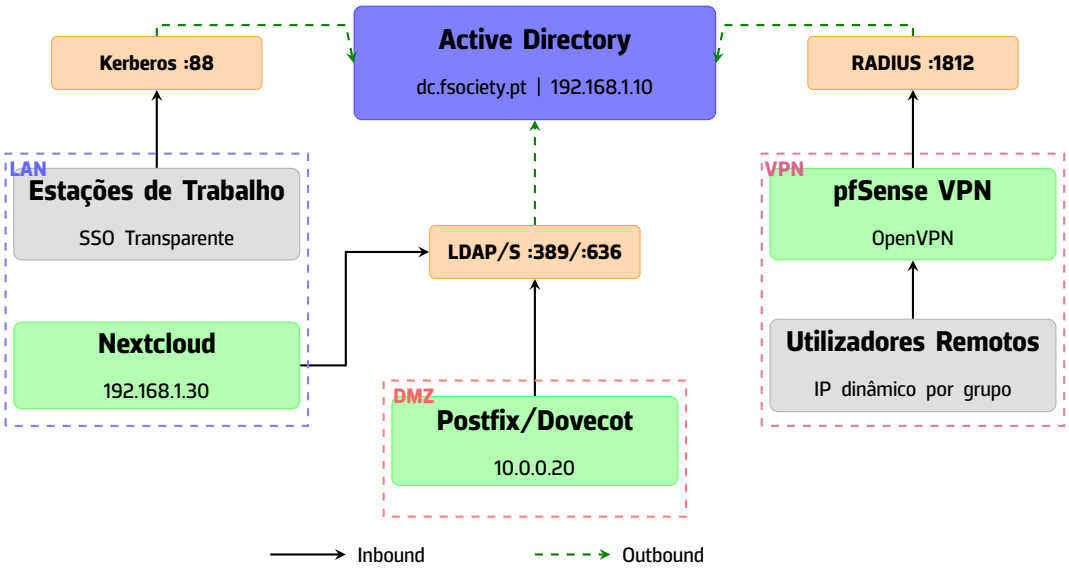


Figura 4.6: Fluxos de autenticação centralizados no controlador de domínio.

Os três protocolos de autenticação utilizados respondem a requisitos distintos:

- **Kerberos** (porta 88): Utilizado pelas estações de trabalho na LAN para autenticação transparente (SSO). Após o login inicial, o utilizador obtém um *Ticket Granting Ticket* (TGT) que permite acesso aos recursos do domínio sem reintroduzir credenciais.
- **LDAP/LDAPS** (portas 389/636): Utilizado pelos serviços aplicacionais (Nextcloud, Mailcow) para validação de credenciais e consulta de atributos de utilizadores e grupos. As comunicações são cifradas via TLS (LDAPS) ou STARTTLS.

- **RADIUS** (porta 1812): Utilizado pelo pfSense para autenticação de utilizadores VPN. O FreeRADIUS atua como intermediário, validando credenciais contra o LDAP do AD e retornando atributos específicos (como o IP a atribuir) baseados no grupo do utilizador.

Esta arquitetura centralizada garante que todas as alterações de credenciais ou permissões são imediatamente refletidas em todos os serviços, eliminando a necessidade de gestão de contas duplicadas e reduzindo o risco de credenciais órfãs.

4.4.2 DNS Integrado

O servidor DNS do Samba gere as zonas necessárias para o funcionamento do domínio e resolução de nomes interna:

- **fsociety.pt** (forward): Registos A para todos os servidores, registos Mail Exchange (MX) para email, registos TXT para SPF/DKIM/DMARC.
- **1.168.192.in-addr.arpa** (reverse): Resolução inversa da LAN.
- **0.0.10.in-addr.arpa** (reverse): Resolução inversa da DMZ.
- **_msdcs.fsociety.pt**: Registos SRV para localização de serviços AD (LDAP, Kerberos, Global Catalog).

O DNS forwarder está configurado para 192.168.1.1 (pfSense), que por sua vez utiliza o DNS do Cloudflare (1.1.1.1) para resolução externa.

A Figura 4.7 permite aceder à demonstração da configuração DNS integrado do Samba AD DC AD, incluindo as 4 zonas DNS (forward e reverse), registos A, PTR, SRV para localização de serviços AD (LDAP, Kerberos), registos MX e TXT (SPF/DMARC), computadores no domínio e teste do forwarder.

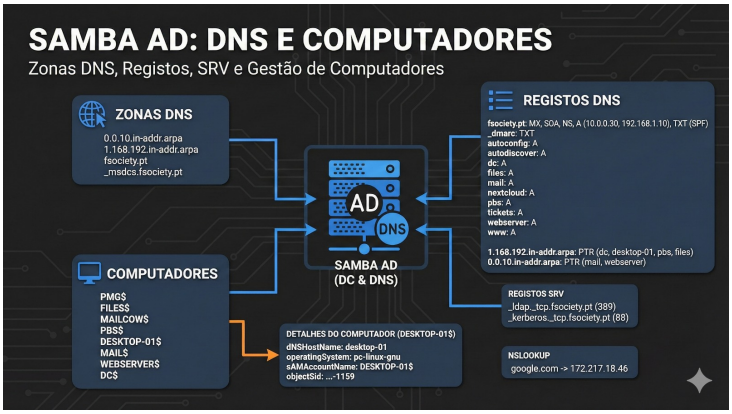


Figura 4.7: Demonstração do DNS Integrado do Samba AD (clique para ver o resultado)

4.4.3 DHCP Server

O ISC DHCP Server foi configurado para atribuição dinâmica de IPs na rede LAN, com o seguinte esquema de endereçamento:

Tabela 4.5: Esquema de Endereçamento DHCP

Range	Utilização
192.168.1.1 – 192.168.1.9	Infraestrutura de rede
192.168.1.10 – 192.168.1.29	Servidores (reservas estáticas)
192.168.1.30 – 192.168.1.49	Estações de trabalho fixas
192.168.1.100 – 192.168.1.200	Pool DHCP dinâmico

Os servidores possuem reservas DHCP baseadas em Media Access Control (MAC) address, garantindo IPs consistentes mesmo em caso de reinstalação.

4.4.4 FreeRADIUS com Integração LDAP

O FreeRADIUS 3.x foi instalado no DC para providenciar autenticação RADIUS integrada com o AD. Esta integração permite que o OpenVPN no pfSense autentique utilizadores contra o AD.

Fluxo de Autenticação

A Figura 4.8 ilustra o fluxo completo de autenticação de um utilizador VPN, desde o envio das credenciais até à atribuição do IP correspondente ao seu grupo departamental no AD.

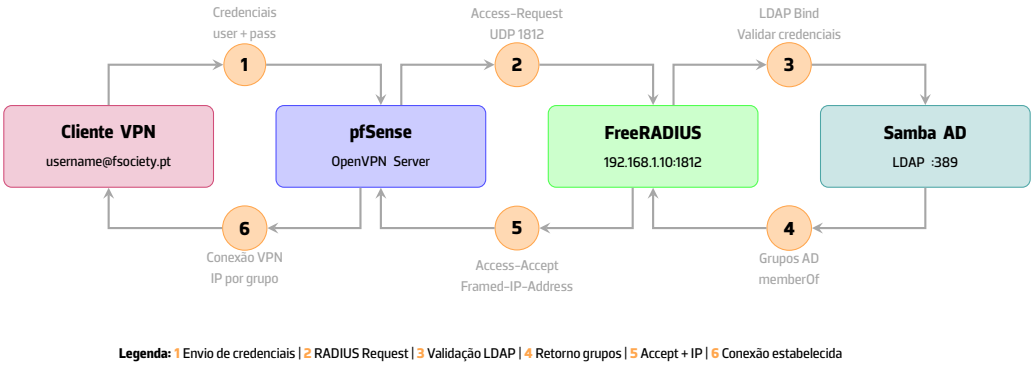


Figura 4.8: Fluxo de autenticação VPN com RADIUS e Active Directory

Validação da Autenticação

A Figura 4.9 demonstra o teste de autenticação RADIUS realizado através do pfSense. O utilizador `ryan.barbosa` foi autenticado com sucesso contra o AD, sendo corretamente identificado como membro do grupo `GRP_TI`.

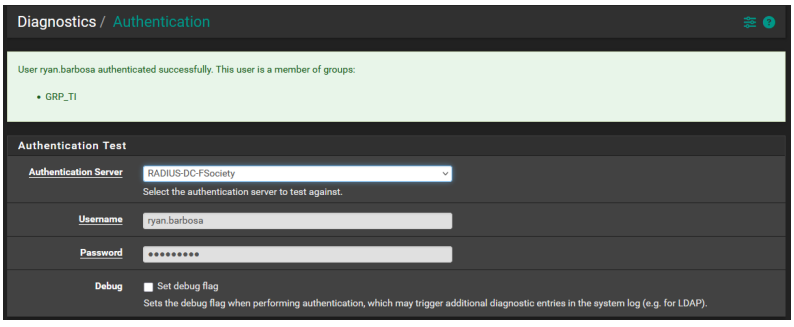


Figura 4.9: Teste de autenticação RADIUS no pfSense com integração AD

Pools de IP por Grupo

A configuração do FreeRADIUS mapeia grupos AD a ranges de IP específicos:

Tabela 4.6: Mapeamento Grupos AD – Pools VPN

Grupo AD	Pool de IPs	Alias pfSense
GRP_TI	10.8.0.10 – 10.8.0.59	VPN_TI
GRP_Gestores	10.8.0.60 – 10.8.0.109	VPN_Gestores
GRP_Financeiro	10.8.0.110 – 10.8.0.159	VPN_Financeiro
GRP_Comercial	10.8.0.160 – 10.8.0.209	VPN_Comercial
GRP_RH	10.8.0.210 – 10.8.0.254	VPN_RH/Users

Esta abordagem permite aplicar políticas de Firewall diferenciadas: por exemplo, apenas o grupo TI tem acesso Secure Shell (SSH) aos servidores, enquanto o grupo Comercial apenas acede ao Nextcloud e ao email via Reverse Proxy e nunca contactando diretamente o servidor de emails, conforme ilustra a Figura A.1 presente no Anexo A.

4.5 Serviços Aplicacionais

Esta secção descreve a implementação dos serviços aplicacionais que suportam as operações da organização: plataforma de colaboração, servidor de email e Reverse Proxy.

4.5.1 Nextcloud

O Nextcloud 32.x foi instalado no servidor de ficheiros (192.168.1.40) como plataforma central de colaboração, substituindo a tradicional partilha SMB por uma suite completa de produtividade.

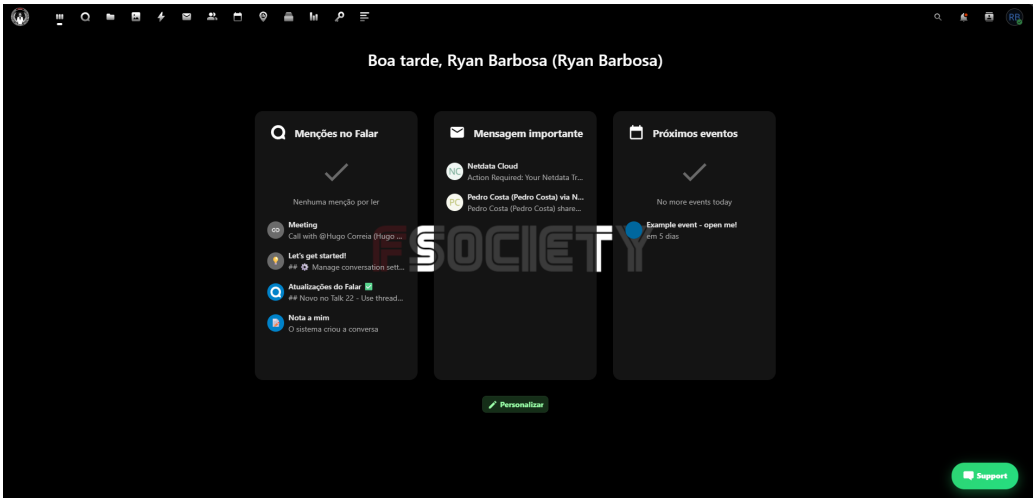


Figura 4.10: Dashboard principal do Nextcloud

O Nextcloud foi selecionado em detrimento de uma simples partilha de ficheiros SMB pelos seguintes motivos:

- **Funcionalidades integradas**: Calendário, contactos, tarefas, notas, videoconferência (Talk), e edição colaborativa de documentos conforme apresentado na Figura A.2 no Anexo A.
- **Acesso web**: Utilizadores podem aceder a ficheiros de qualquer dispositivo com browser, autenticando via VPN.

- **Sincronização**: Clientes desktop e mobile permitem sincronização automática de ficheiros.
- **Integração LDAP**: Autenticação centralizada com o AD, sincronização automática de utilizadores e grupos.

As Figuras A.2 e A.3 no Anexo A apresentam, respetivamente, as aplicações instaladas e a configuração da integração LDAP.

Integração LDAP

A integração com o AD foi configurada através da aplicação *LDAP user and group backend*, permitindo:

- Autenticação de 19 utilizadores do domínio
- Sincronização de 6 grupos de segurança
- Quotas diferenciadas por grupo (TI: ilimitado, outros: 5 GB)
- Provisionamento automático de contas no primeiro login

Aplicações Instaladas

Foram instaladas mais de 65 aplicações para estender as funcionalidades base, organizadas nas seguintes categorias:

- **Produtividade**: Calendar, Contacts, Deck (kanban), Tasks, Notes, Forms, Polls
- **Colaboração**: Talk (videoconferência), Mail, Group Folders, Circles
- **Segurança**: Two-Factor Time-based One-Time Password (TOTP), Suspicious Login (ML), Brute-force Protection
- **Integração**: Collabora Online (edição Office), External Storage, LDAP backend

4.5.2 Zammad

O Zammad 6.5.2 foi instalado no servidor de ficheiros (192.168.1.40) como sistema de gestão de tickets e suporte interno. A plataforma está integrada com o AD para autenticação centralizada e acessível apenas na rede interna através do endereço `tickets.fsociety.pt`.

Integração com Nextcloud

O Zammad foi integrado no ecossistema de produtividade através de um widget de suporte no dashboard do Nextcloud visivelmente evidenciado na Figura 4.10. Esta integração permite que os utilizadores acedam ao suporte técnico sem sair da plataforma principal de trabalho, reduzindo a fricção no processo de abertura de pedidos.

Fluxo de Tickets

O processo de suporte segue um fluxo estruturado em quatro fases:

1. **Abertura do Pedido**: O utilizador, autenticado no Nextcloud, clica no ícone de suporte visível no dashboard. É apresentada uma interface de chat onde pode descrever o problema.
2. **Fila de Espera**: O pedido entra na fila de atendimento visível para os agentes de suporte (equipas TI e RH). O utilizador aguarda que um agente aceite o atendimento.

3. **Atendimento**: Um agente aceita o ticket, iniciando uma sessão de chat em tempo real com o utilizador. Durante o atendimento, o agente pode solicitar informações adicionais, partilhar instruções ou escalar o problema.

4. **Encerramento**: Após resolução, o agente encerra o chat e cria formalmente o ticket no sistema, associando o email do utilizador. O sistema envia automaticamente um email de confirmação com o resumo do atendimento e o número do ticket para referência futura.

A Figura A.5 no Anexo A ilustra as quatro fases do fluxo de atendimento.

Benefícios da Solução

A implementação do Zammad integrado com o Nextcloud proporciona:

- **Rastreabilidade**: Todos os pedidos ficam registados com histórico completo de interações.
- **Notificação automática**: Utilizadores recebem confirmação por email sem intervenção manual.
- **Autenticação única**: Integração LDAP elimina necessidade de credenciais separadas.
- **Métricas**: Dashboards de tempo médio de resposta, tickets por categoria e desempenho dos agentes.

4.5.3 Servidor de Email (Mailcow)

O Mailcow Dockerized foi implementado na DMZ (10.0.0.20) como solução completa de email corporativo. A escolha do Mailcow justifica-se pela sua natureza. O Mailcow integra todos os componentes necessários numa arquitetura containerizada: Mail Transfer Agent (MTA) (Postfix), Mail Delivery Agent (MDA) (Dovecot), webmail (SOGo), anti-spam (Rspamd) e antivírus (ClamAV), eliminando a necessidade de múltiplos servidores ou soluções complementares.

Arquitetura de Containers

A arquitetura Docker do Mailcow compreende 18 containers que colaboram para fornecer todos os serviços de email. A Figura A.6 no Anexo A ilustra a arquitetura completa.

A Tabela 4.7 apresenta os componentes principais e as suas funções.

Tabela 4.7: Componentes do Mailcow

Componente	Função	Tecnologia
MTA	Envio/receção de email	Postfix
MDA	Entrega e armazenamento	Dovecot
Anti-spam	Filtragem de spam	Rspamd (ML)
Antivírus	Deteção de malware	ClamAV
Webmail	Interface web	SOGo
Admin	Gestão	Mailcow UI

Integração LDAP

O Mailcow foi configurado para sincronizar automaticamente com o AD, eliminando a necessidade de gestão duplicada de contas:

- **Sincronização automática**: A cada 15 minutos, o Mailcow consulta o AD via LDAPS (porta 636) e cria mailboxes para novos utilizadores.
- **Filtro de importação**: Apenas utilizadores com o atributo `mail` preenchido e pertencentes ao grupo GRP_VPN_Users são importados, excluindo contas de serviço e sistema.
- **Autenticação**: O bind LDAP é realizado através da conta de serviço `svc_ldap`, com permissões de leitura apenas.

A Figura A.7 no Anexo A apresenta a configuração LDAP no painel de administração.

Segurança Anti-Spam

O Rspamd atua como motor de filtragem anti-spam, utilizando múltiplas técnicas de deteção:

- **Filtros Bayesianos**: Aprendizagem automática baseada em emails classificados como spam ou legítimos pelos utilizadores. A integração com Redis permite armazenar estatísticas de classificação (BAYES_SPAM e BAYES_HAM) de forma persistente.
- **Greylisting**: Rejeição temporária de emails de remetentes desconhecidos, eficaz contra spambots que não reenviam.
- **DNS-based Blackhole List (DNSBL)**: Consulta a listas negras de IPs conhecidos por enviar spam.
- **ClamAV**: Análise antivírus de anexos em tempo real.

A validação do sistema foi realizada através do teste Generic Test for Unsolicited Bulk Email (GTUBE), que consiste no envio de um email contendo a string padrão de teste anti-spam. Conforme ilustrado na Figura A.8 presente no Anexo A, o sistema identificou e bloqueou corretamente a mensagem de teste, demonstrando o funcionamento adequado da filtragem.

As estatísticas do Rspamd, recolhidas durante o período de testes, indicam o processamento de 39 mensagens com a seguinte distribuição: 63% sem ação necessária (tráfego legítimo), 28% submetidas a Greylisting, e 9% rejeitadas como spam. O backend Redis regista atualmente 9 ocorrências classificadas como spam e 2 como ham nos filtros bayesianos, valores que refletem o período inicial de treino do sistema.

Autenticação de Email

Foram implementados os três mecanismos de autenticação recomendados para garantir a entregabilidade e prevenir spoofing:

- **SPF**: Registo TXT no DNS especificando os servidores autorizados a enviar email pelo domínio fsociety.pt.
- **DKIM**: Assinatura criptográfica RSA de 2048 bits aplicada a todas as mensagens enviadas, com chave pública publicada no DNS.
- **DMARC**: Política de tratamento de mensagens que falham SPF/DKIM, configurada em modo `quarantine` com relatórios enviados para análise.

A configuração foi validada externamente através do serviço Mail-Tester, obtendo a pontuação máxima de 10/10[3], conforme ilustrado na Figura 4.11.

[3] Resultado disponível em: https://www.mail-tester.com/test-2e3vyl3cx

Figura 4.11: Resultado do teste de autenticação no Mail-Tester (10/10)

Relay SMTP Externo

Devido às limitações inerentes a uma ligação doméstica — IP dinâmico e porta 25 frequentemente bloqueada por Internet Service Provider (Fornecedor de Serviços de Internet)s (ISPs) — foi implementada uma estratégia híbrida para o fluxo de email:

- **Envio (Outbound)**: Configurado o SMTP2GO como relay externo. O Mailcow autentica-se no SMTP2GO que, por sua vez, entrega os emails a partir de IPs com reputação estabelecida.
- **Receção (Inbound)**: Os registos MX apontam para o Cloudflare, que atua como proxy e encaminha o tráfego para o IP dinâmico através do túnel configurado. Esta abordagem também proporciona proteção contra ataques DDoS direcionados ao servidor de email.

Webmail e Clientes

O SOGo fornece uma interface webmail completa acessível em `mail.fsociety.pt`, incluindo:

- Calendário partilhado com suporte a convites
- Gestão de contactos com sincronização
- ActiveSync para dispositivos móveis iOS e Android
- Autodiscover/Autoconfig para configuração automática de clientes

A Figura A.9 no Anexo A apresenta a interface do webmail SOGo. E a Figura A.10 no Anexo A evidencia que a configuração automática foi validada utilizando o Mozilla Thunderbird em dispositivo móvel Android.

4.5.4 Webserver e Reverse Proxy

O servidor web (10.0.0.30), localizado na DMZ, executa Nginx como Reverse Proxy para todos os serviços web da infraestrutura. Esta abordagem centraliza a terminação TLS, a gestão de certificados e a aplicação de políticas de segurança num único ponto de entrada, seguindo o princípio de defesa em profundidade.

Arquitetura de Segurança

A configuração do Nginx implementa múltiplas camadas de proteção. Ao nível global, são aplicados security headers que previnem ataques comuns como clickjacking (X-Frame-Options), MIME-type sniffing (X-Content-Type-Options) e Cross-Site Scripting (XSS) (X-XSS-Protection). O rate limiting está configurado com três zonas distintas: limite geral de 50 requisições por segundo por IP, limite específico para endpoints de autenticação de 5 requisições por minuto, e limite de 1000 conexões simultâneas por IP.

A integração com CrowdSec proporciona proteção adicional através de três Bouncers complementares. O Firewall Bouncer (v0.0.34) opera ao nível de iptables, bloqueando IPs maliciosos antes de atingirem o Nginx. O Nginx Lua Bouncer (v1.1.3) executa verificações ao nível da aplicação, permitindo páginas de bloqueio personalizadas. O Cloudflare Bouncer (v0.3.0) sincroniza decisões de bloqueio com o WAF na edge, mitigando ataques antes de chegarem à infraestrutura.

Virtual Hosts Configurados

A Tabela 4.8 apresenta os seis virtual hosts configurados, cada um com funcionalidades específicas de segurança adaptadas ao serviço correspondente.

Tabela 4.8: Virtual Hosts do Nginx com funcionalidades de segurança

Domínio	Backend	Serviço	Funcionalidades
fsociety.pt	10.0.0.30	Website	HSTS, CSP
nextcloud.fsociety.pt	192.168.1.40:443	Nextcloud	Geo-access control
mail.fsociety.pt	10.0.0.20:443	Mailcow	WebSocket support
tickets.fsociety.pt	192.168.1.40:3000	Zammad	Acesso restrito
autoconfig.fsociety.pt	10.0.0.20	Email config	Thunderbird/Outlook
autodiscover.fsociety.pt	10.0.0.20	Autodiscover	Microsoft Exchange

O virtual host do Nextcloud implementa geo-access control, permitindo acesso completo apenas a partir de redes internas (LAN/VPN), enquanto utilizadores externos acedem apenas à aplicação de email. Esta configuração utiliza os módulos geo e map do Nginx para decisões de acesso baseadas no IP de origem.

Certificados SSL/TLS e Proteção Cloudflare

A terminação TLS utiliza certificados wildcard Let's Encrypt obtidos através de validação DNS via Cloudflare. O certificado cobre todos os subdomínios (*.fsociety.pt) e o domínio base, com renovação automática configurada via certbot. A configuração SSL implementa apenas TLS 1.2 e 1.3, com cipher suites modernas e parâmetros Diffie-Hellman de 4096 bits.

O domínio está configurado com proxy Cloudflare ativo em modo Full (Strict), garantindo encriptação end-to-end com validação de certificados. As funcionalidades de segurança ativas incluem WAF com regras Open Web Application Security Project (OWASP) geridas, proteção DDoS nas camadas 3, 4 e 7, Bot Fight Mode para bloqueio automático de bots maliciosos, e HTTP Strict Transport Security (HSTS) forçado ao nível da edge.

4.5.5 Cloudflare

O Cloudflare atua como primeira linha de defesa para todos os serviços web expostos à Internet, providenciando proteção WAF com filtragem de pedidos maliciosos, mitigação DDoS através da absorção de ataques volumétricos antes de atingirem a infraestrutura, CDN com cache de conteúdo estático, e gestão automática de certificados SSL/TLS.

O modo de proxy está configurado como *Full (Strict)*, garantindo cifração end-to-end tanto entre cliente-Cloudflare como Cloudflare-origem. A configuração DNS implementada encontra-se detalhada no Anexo A.11.

A configuração inclui registos A para os serviços principais (fsociety.pt, nextcloud, webmail, www) com proxy ativo, registos Canonical Name Record (CNAME) para autoconfig e autodiscover do email, e registos TXT para autenticação de email (SPF, DKIM, DMARC). Os registos MX, SRV e TLSA complementam a configuração do servidor de email, garantindo conformidade com as melhores práticas de entrega e segurança.

4.5.6 CrowdSec

O CrowdSec foi implementado em todos os servidores como sistema de deteção e prevenção de intrusões baseado em análise comportamental e inteligência colaborativa.

Arquitetura Distribuída

A implementação segue uma arquitetura distribuída com agentes CrowdSec instalados em cada servidor, todos registados no IP público 188.81.65.191 e ligados à Central API (CAPI) para partilha de inteligência. O dashboard com os quatro servidores monitorizados é apresentado no Anexo A.12.

A Tabela 4.9 detalha a configuração de cada servidor.

Tabela 4.9: Configuração CrowdSec por servidor

Servidor	Scenarios	Alerts	Bouncers	Blocklists
Web Server	56	149	3	1
File Server	55	0	1	1
Domain Server	11	0	1	1
Mailcow	10	0	1	1

O Web Server, por ser o ponto de entrada principal exposto à Internet, concentra a maioria dos alertas (149) e dispõe de três componentes de remediação: Firewall Bouncer (iptables), Nginx Lua Bouncer, e Cloudflare Bouncer. Os restantes servidores, protegidos pelo Firewall perimetral, apresentam zero alertas diretos mas mantêm cenários de deteção ativos para proteção contra ameaças internas.

As métricas detalhadas de ataques prevenidos e tráfego malicioso descartado são apresentadas nos Anexos A.13 e A.14.

4.6 Monitorização

A operação de infraestruturas distribuídas exige visibilidade contínua sobre o estado de múltiplos sistemas heterogéneos. Para responder a este desafio, foi implementado o Netdata Cloud como plataforma de monitorização em tempo real dos servidores da infraestrutura.

4.6.1 Netdata Cloud

O Netdata foi selecionado pela facilidade de implementação (deployment inferior a 5 minutos por servidor), granularidade temporal de 1 segundo que permite deteção de anomalias transientes, auto-descoberta de mais de 800 tipos de serviços, e overhead reduzido (1–3% CPU, 150MB RAM). O tier gratuito disponibiliza dashboard centralizado com retenção de 14 dias, adequado ao contexto académico do projeto.

Arquitetura de Monitorização

O Netdata Cloud agrega métricas de seis servidores: PVE (Hypervisor), pfSense (Firewall), DC, Servidor de Ficheiros, Servidor de Email e Webserver. Para cada servidor, são recolhidas automaticamente métricas de sistema (CPU, memória, disco, rede), serviços específicos (Samba, Postfix, Nginx,

Docker) e aplicações (PostgreSQL, Redis, mail servers). O dashboard centralizado é apresentado no Anexo A.16.

Sistema de Alertas

Foram configurados alertas para condições críticas incluindo CPU acima de 90% durante mais de 5 minutos, memória acima de 95%, disco acima de 90%, serviços críticos em estado *down*, e latência de rede anormal. As notificações são enviadas por email e através da aplicação móvel nativa (iOS/Android), reduzindo o Mean Time To Detect (MTTD) de potenciais horas para segundos, conforme ilustrado no Anexo **??**.

AI Insights

O módulo de AI integrado proporciona capacidades de observabilidade proativa: deteção de anomalias antes de se tornarem críticas, correlação de eventos entre diferentes servidores, predição de tendências de utilização, e análise automatizada de root cause. Durante a validação, a AI analisou 168 horas de métricas agregadas e identificou padrões como memory exhaustion e I/O spikes coordenados, gerando recomendações específicas de mitigação. Os relatórios completos da análise AI estão disponíveis no repositório do projeto[4].

4.7 Backup e Recuperação

A estratégia de backup implementada visa garantir a recuperação da infraestrutura em caso de falha, com Recovery Point Objective (RPO) de 24 horas e Recovery Time Objective (RTO) inferior a 1 hora para serviços críticos.

4.7.1 Proxmox Backup Server

O PBS foi instalado numa VM dedicada (VMID 101, 192.168.1.30) com datastore de 850 GB para backups. A integração nativa com o PVE simplifica a gestão e permite funcionalidades avançadas como Deduplicação chunk-based com economia de 60–80% de espaço, cifração Advanced Encryption Standard (AES)-256 dos backups em repouso, verificação automática de integridade através de checksums, e backups em modo Snapshot sem downtime das VMs.

Agendamento

A Tabela 4.10 apresenta os backup jobs configurados.

Tabela 4.10: Agendamento de Backups no PBS

VMID	VM	Horário	Modo	Compressão
102	pfSense	02:00	Snapshot	zstd
104	Web-Server	02:30	Snapshot	zstd
105	Servidor de Domínio	02:30	Snapshot	zstd
106	Servidor de Ficheiros	02:30	Snapshot	zstd
108	Mailcow	02:30	Snapshot	zstd

[4] https://github.com/RyanTech00/fsociety-infrastructure/blob/main/docs/10-monitorizacao-centralizada/ai-reports/

Os backups são executados durante a madrugada para minimizar impacto no desempenho, com o pfSense isolado às 02:00 e os restantes servidores agrupados às 02:30. A compressão Zstandard (algoritmo de compressão) (ZSTD) oferece bom equilíbrio entre taxa de compressão e performance.

Políticas de Retenção

A política de retenção configurada mantém 7 backups diários, 4 semanais e 6 mensais, implementada através de prune-jobs automáticos. O Garbage Collection (GC) executa semanalmente para libertar espaço de chunks órfãos. A documentação detalhada está disponível no repositório do projeto[5].

4.7.2 Backup do Active Directory

Para além do backup completo da VM, o Samba AD DC possui backup dedicado da base de dados LDAP através do comando `samba-tool domain backup offline`, executado diariamente com retenção de 7 dias.

```
#!/bin/bash
# Backup diario do Samba AD
BACKUP_DIR="/backup/samba-ad/daily"
DATE=$(date +%Y%m%d)
samba-tool domain backup offline \
    --targetdir=$BACKUP_DIR \
    --configfile=/etc/samba/smb.conf
# Manter apenas ultimos 7 dias
find $BACKUP_DIR -name "*.tar.bz2" -mtime +7 -delete
```

Listagem 4.2: Script de Backup do Samba AD

Este backup permite restaurar apenas a base de dados do AD sem necessidade de restaurar a VM completa.

4.8 Síntese da Implementação

A implementação da infraestrutura FSociety resultou num ambiente funcional que cumpre todos os requisitos obrigatórios do enunciado e implementa funcionalidades adicionais de valor acrescentado.

4.8.1 Cumprimento dos Requisitos

A Tabela **??** resume o estado de cumprimento dos requisitos obrigatórios do enunciado.

4.8.2 Valor Acrescentado

Para além dos requisitos obrigatórios, a implementação inclui funcionalidades que aproximam a infraestrutura de um ambiente empresarial de produção:

- **Four-Legged Firewall**: Zona VPN dedicada com políticas granulares por departamento.
- **AD**: Gestão centralizada de identidades com SSO para todos os serviços.

[5] https://github.com/RyanTech00/fsociety-infrastructure/tree/main/docs/07-proxmox-backup

- **Servidor de Email**: Mailcow com anti-spam baseado em ML, integração LDAP e validação SPF/DKIM/DMARC (pontuação 10/10 no Mail-Tester).
- **Plataforma de Colaboração**: Nextcloud com mais de 65 aplicações integradas, substituindo a simples partilha SMB.
- **IDS/IPS Distribuído**: CrowdSec em 4 servidores com mais de 130 cenários de deteção e Blocklists colaborativas.
- **Proteção Edge**: Cloudflare com WAF, mitigação DDoS nas camadas 3/4/7 e CDN global.
- **Monitorização Inteligente**: Netdata Cloud com análise preditiva baseada em ML.
- **VPN com RADIUS**: Autenticação integrada com AD e pools de endereços hierárquicos por grupo.
- **Backup Centralizado**: PBS com Deduplicação, cifração e verificação automática de integridade.

4.8.3 Documentação Técnica

A documentação técnica completa, incluindo guias de instalação passo a passo, ficheiros de configuração, scripts de automação e procedimentos de troubleshooting, está disponível publicamente:

- **Repositório GitHub**: https://github.com/RyanTech00/fsociety-infrastructure
- **GitHub Pages**: https://ryantech00.github.io/fsociety-infrastructure/
- **Arquivo Zenodo**: DOI 10.5281/zenodo.17840636 (Barbosa et al., 2025b)

A documentação compreende mais de 40 páginas de guias técnicos organizados por componente, cobrindo todos os aspetos da implementação.

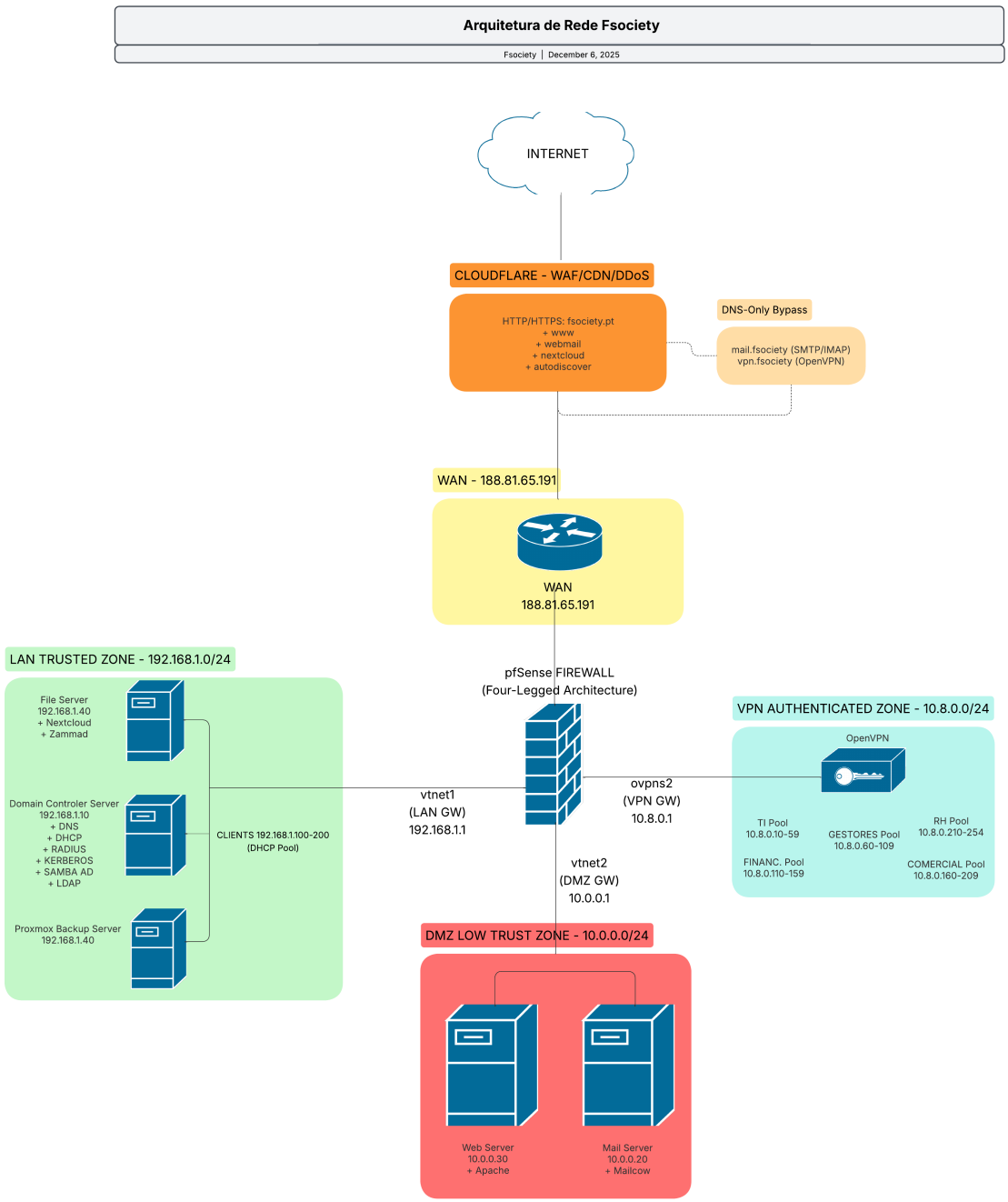


Figura 4.2: Arquitetura de Rede FSociety com Cloudflare

5. Conclusão

Este capítulo encerra o relatório apresentando uma síntese do trabalho desenvolvido. Afere-se o grau de cumprimento dos objetivos traçados, tendo em conta as contribuições técnicas, bem como as limitações inerentes ao escopo do projeto. Por fim, são delineadas perspetivas de evolução e trabalhos futuros que visam a continuidade e o aperfeiçoamento da solução implementada.

5.1 Síntese do Trabalho Desenvolvido

O presente projeto assumiu como desígnio o desenvolvimento e validação de uma infraestrutura de rede empresarial segura, integralmente baseada em tecnologias de código aberto, para a empresa fictícia FSociety.pt. A solução arquitetada materializou-se sobre a plataforma de virtualização PVE, orquestrando componentes de referência como pfSense (firewall), Samba AD DC (gestão de identidades), Mailcow (email), Nextcloud (colaboração) e CrowdSec (deteção de intrusões).

A implementação decorreu num ambiente virtualizado doméstico, obedecendo rigorosamente aos princípios da segurança em profundidade (*defense in depth*) através de uma arquitetura Four-Legged Firewall com segmentação em zonas de confiança diferenciadas: WAN, LAN, DMZ e VPN.

Os resultados empíricos validam a hipótese de partida: o ecossistema *open source* atingiu um patamar de maturidade que permite não só igualar a fiabilidade operacional das soluções comerciais, como oferecer maior controlo, auditabilidade e flexibilidade na gestão da infraestrutura.

5.2 Aferição do Cumprimento dos Objetivos

Esta secção apresenta uma análise do cumprimento dos requisitos estabelecidos no enunciado do trabalho prático. Para cada requisito proposto, avalia-se o grau de concretização alcançado.

5.2.1 Requisitos Obrigatórios

A Tabela 5.1 apresenta o mapeamento entre os requisitos do enunciado e a sua implementação no projeto.

Tabela 5.1: Cumprimento dos requisitos do enunciado

Requisito	Nível	Estado
Implementação de Rede Interna (Desktop Cliente)	1	✓
Implementação de Servidor interno DHCP	1	✓
Implementação de Servidor com partilha de ficheiros	1	✓
Implementação de Firewall com políticas de segurança	1	✓
DMZ: Implementação de Servidor HTTP	2	✓
Outros Serviços (DNS, Rotas, ...)	2	✓
Rede interna e DMZ protegidas por Firewalls	2	✓
Arquitetura Three-Legged Firewall	Final	✓*

* Implementado como Four-Legged Firewall, excedendo o requisito.

5.2.2 Funcionalidades de Valor Acrescentado

Para além dos requisitos obrigatórios, foram implementadas funcionalidades adicionais que demonstram competências avançadas em administração de sistemas:

- **Four-Legged Firewall**: Zona VPN isolada com pools de IP hierárquicos por grupo departamental e autenticação RADIUS integrada com AD.
- **Servidor de Email Empresarial**: Mailcow com anti-spam baseado em ML, integração LDAP e validação SPF/DKIM/DMARC, obtendo pontuação máxima (10/10) no Mail-Tester.
- **Plataforma de Colaboração**: Nextcloud com mais de 65 aplicações integradas, substituindo soluções de partilha de ficheiros tradicionais.
- **IDS/IPS Distribuído**: CrowdSec em 4 servidores com mais de 130 cenários de deteção e Blocklists colaborativas, complementado por proteção edge via Cloudflare WAF.
- **Monitorização Inteligente**: Netdata Cloud com AI Insights para deteção de anomalias e análise preditiva.
- **Backup Centralizado**: PBS com Deduplicação, cifração AES-256 e verificação automática de integridade.

5.3 Contributos do Trabalho

O projeto aporta valor em múltiplas dimensões:

- **Técnica**: Disponibiliza uma arquitetura de referência completa baseada em tecnologias *open source*, provando que é possível implementar uma infraestrutura empresarial robusta sem dependência de soluções proprietárias.
- **Pedagógica**: O material produzido serve como recurso didático para o ensino de administração de sistemas, segurança de redes e virtualização.
- **Documental**: A disponibilização pública de mais de 40 documentos técnicos, scripts de automação e ficheiros de configuração assegura que a implementação pode ser replicada por terceiros.

5.4 Competências Desenvolvidas

A realização deste projeto permitiu desenvolver e consolidar competências técnicas em múltiplas áreas: virtualização com gestão de Hypervisors PVE; segurança de redes com configuração de firewalls stateful e segmentação por zonas; gestão de identidades com administração de AD e integração LDAP; protocolos de autenticação incluindo Kerberos e RADIUS; serviços de email com configuração de MTA/MDA e autenticação SPF/DKIM/DMARC; scripting e automação com desenvolvimento de daemons em Bash; e produção de documentação técnica estruturada com arquivo académico.

5.5 Limitações e Dificuldades

A honestidade intelectual obriga ao reconhecimento das limitações do projeto:

- **Recursos de Hardware**: A implementação em ambiente doméstico com hardware limitado (16 GB RAM, CPU mobile) exigiu otimizações agressivas na alocação de recursos das VMs.
- **IP Dinâmico**: A ausência de IP público fixo obrigou à implementação de Dynamic Domain Name System (DDNS) via Cloudflare e relay SMTP externo para envio de emails.
- **Porta 25 Bloqueada**: O bloqueio da porta SMTP pelo ISP impediu a receção direta de emails, resolvido através de proxy via Cloudflare.
- **Alta Disponibilidade**: A implementação num único nó físico constitui um ponto único de falha, não permitindo demonstrar cenários de Failover e clustering essenciais em ambientes de produção.

5.6 Trabalho Futuro

Considerando que a infraestrutura base já se encontra funcional e integrada, as perspetivas de evolução focam-se na resiliência e automação:

- **Alta Disponibilidade**: Implementação de cluster Proxmox com múltiplos nós e pfSense em configuração Common Address Redundancy Protocol (CARP) para Failover.
- **Infrastructure as Code**: Adoção de Ansible e Terraform para provisionamento automatizado e gestão de configurações.
- **Containerização**: Migração de serviços adicionais para containers Docker/Kubernetes, aumentando flexibilidade e escalabilidade.
- **Security Information and Event Management (SIEM)**: Implementação de solução centralizada de gestão de eventos de segurança (Wazuh ou ELK Stack) para correlação de logs.
- **Disaster Recovery**: Implementação de site secundário com replicação de dados e procedimentos documentados de recuperação.

5.7 Considerações Finais

O presente trabalho encerra-se com a convicção de que a infraestrutura desenvolvida ultrapassa o estatuto de mero exercício académico, constituindo uma prova de conceito funcional e robusta. A arquitetura Four-Legged Firewall com defesa em profundidade, combinada com gestão centralizada de identidades e monitorização contínua, constitui uma base sólida para ambientes de produção.

A disponibilização pública de toda a documentação técnica — em https://ryantech00.github.io/fsociety-infrastructure/ e arquivada com DOI 10.5281/zenodo.17840636 (Barbosa et al., 2025b) — assegura a perenidade e a reprodutibilidade do projeto pela comunidade.

Demonstrou-se assim que, através da orquestração de tecnologias *open source*, é possível implementar uma infraestrutura empresarial completa e segura. O trabalho desenvolvido excedeu os requisitos mínimos estabelecidos no enunciado, demonstrando iniciativa na exploração de tecnologias complementares e capacidade de integração de múltiplos sistemas numa arquitetura coesa. As competências adquiridas são diretamente aplicáveis em contextos profissionais de administração de sistemas e cibersegurança.

Capítulo

Referências

Barbosa, R., Correia, H., & Araújo, I. (2025a). *FSociety Infrastructure — Repositório GitHub*. Acedido em dezembro 7, 2025, de https://github.com/RyanTech00/fsociety-infrastructure.

Barbosa, R., Correia, H., & Araújo, I. (2025b, dezembro). FSociety Infrastructure: Enterprise Network with Four-Legged Firewall (Version 1.1.0). https://doi.org/10.5281/zenodo.17840636.

Cisco Systems, Inc. (2024). *Cisco ASA Series General Operations CLI Configuration Guide*. Acedido em dezembro 7, 2025, de https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

Crocker, D., Hansen, T., & Kucherawy, M. (2011). *DomainKeys Identified Mail (DKIM) Signatures* (RFC N.º 6376). Internet Engineering Task Force. https://doi.org/10.17487/RFC6376.

CrowdSec. (2024). *CrowdSec Documentation*. Acedido em dezembro 7, 2025, de https://docs.crowdsec.net/.

Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II). Acedido em dezembro 7, 2025, de https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

Docker, Inc. (2024). *Docker Documentation*. Acedido em dezembro 7, 2025, de https://docs.docker.com/.

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC N.º 27002:2022). International Organization for Standardization. Acedido em dezembro 7, 2025, de https://www.iso.org/standard/75652.html.

Kitterman, S. (2014). *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1* (RFC N.º 7208). Internet Engineering Task Force. https://doi.org/10.17487/RFC7208.

Kucherawy, M., & Zwicky, E. (2015). *Domain-based Message Authentication, Reporting, and Conformance (DMARC)* (RFC N.º 7489). Internet Engineering Task Force. https://doi.org/10.17487/RFC7489.

Kumar, R., & Sharma, R. (2022). A Survey on Firewall Technologies and Their Performance Analysis. *Journal of Network and Computer Applications*, *198*, 103287. https://doi.org/10.1016/j.jnca.2021.103287.

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8ª ed.). Pearson.

mailcow Community. (2024). *mailcow: dockerized Documentation*. Acedido em dezembro 7, 2025, de https://docs.mailcow.email/.

MIT Kerberos Consortium. (2023). *Kerberos: The Network Authentication Protocol*. Acedido em dezembro 7, 2025, de https://web.mit.edu/kerberos/.

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication N.º 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5.

Netdata, Inc. (2024). *Netdata Documentation*. Acedido em dezembro 7, 2025, de https://learn.netdata.cloud/.

Netgate. (2024). *pfSense Documentation*. Acedido em dezembro 7, 2025, de https://docs.netgate.com/pfsense/en/latest/.

Nextcloud GmbH. (2024). *Nextcloud Administration Manual*. Acedido em dezembro 7, 2025, de https://docs.nextcloud.com/server/latest/admin_manual/.

Palo Alto Networks. (2024). *PAN-OS Administrator's Guide*. Acedido em dezembro 7, 2025, de https://docs.paloaltonetworks.com/pan-os.

Proxmox Server Solutions GmbH. (2024). *Proxmox VE Administration Guide*. Acedido em dezembro 7, 2025, de https://pve.proxmox.com/pve-docs/pve-admin-guide.html.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Regulamento Geral sobre a Proteção de Dados). Acedido em dezembro 7, 2025, de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679.

Rigney, C. (2000, junho). *RADIUS Accounting* (RFC N.º 2866). Internet Engineering Task Force. https://doi.org/10.17487/RFC2866.

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2000). *Remote Authentication Dial In User Service (RADIUS)* (RFC N.º 2865). Internet Engineering Task Force. https://doi.org/10.17487/RFC2865.

Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy* (NIST Special Publication N.º 800-41 Rev. 1). National Institute of Standards e Technology. https://doi.org/10.6028/NIST.SP.800-41r1.

Sermersheim, J. (2006). *Lightweight Directory Access Protocol (LDAP): The Protocol* (RFC N.º 4511). Internet Engineering Task Force. https://doi.org/10.17487/RFC4511.

Stallings, W. (2016). *Network Security Essentials: Applications and Standards* (6ª ed.). Pearson.

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679.

Tanenbaum, A. S., Feamster, N., & Wetherall, D. J. (2021). *Computer Networks* (6ª ed.). Pearson.

The Samba Team. (2025). *Setting up Samba as an Active Directory Domain Controller*. Acedido em dezembro 7, 2025, de https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller.

VMware, Inc. (2024). *vSphere Documentation*. Acedido em dezembro 7, 2025, de https://docs.vmware.com/en/VMware-vSphere/index.html.

Weinberg, R., Zisser, Y., Aviv, R., & Wool, A. (2024). From Perimeter to Zero Trust: A Systematic Review of Network Security Paradigm Shifts. *Computers & Security*, *137*, 103602. https://doi.org/10.1016/j.cose.2023.103602.

Wool, A. (2010). Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese. *IEEE Internet Computing*, *14*(4), 58–65. https://doi.org/10.1109/MIC.2010.29.

Capítulo

Certificação de Integridade

A integridade deste documento encontra-se certificada através de registo na blockchain Bitcoin via protocolo OpenTimestamps. Esta certificação proporciona:

- **Prova de existência**: Demonstra que o documento existia numa data específica, sem possibilidade de antedatação;
- **Integridade garantida**: Qualquer alteração ao conteúdo, por mínima que seja, invalida o hash registado;
- **Imutabilidade**: O registo na blockchain Bitcoin é permanente e não pode ser modificado ou removido;
- **Verificação independente**: Qualquer pessoa pode validar a autenticidade do documento sem depender de terceiros.

O ficheiro de prova (`.ots`) e o hash SHA-256 do documento estão disponíveis no repositório do projeto, permitindo a verificação de que o conteúdo não foi alterado desde a data de submissão.

Verificação:

Para verificar a integridade do documento:

1. Descarregar o ficheiro `.ots` do repositório GitHub;
2. Executar: `ots verify Relatorio-FSociety-ASII-2025.pdf`;
3. Ou verificar online em: https://opentimestamps.org.

Repositório: https://github.com/RyanTech00/fsociety-infrastructure

Arquivo Zenodo: https://doi.org/10.5281/zenodo.17840636

A. Imagens

Este anexo apresenta imagens complementares cuja dimensão ou nível de detalhe não justificava a sua inclusão no corpo principal do relatório. As figuras estão organizadas por componente da infraestrutura, fornecendo evidências visuais das configurações implementadas.

A.1 Regras de Firewall por Pool VPN

A segmentação do acesso VPN por departamento é implementada através de regras de Firewall específicas no pfSense. Cada pool de endereços IP (TI, Gestores, Financeiro, Comercial, RH) possui regras diferenciadas que determinam quais recursos da LAN e DMZ podem ser acedidos.

A Figura A.1 apresenta a configuração completa destas regras, evidenciando o princípio de *least privilege* onde, por exemplo, o grupo Comercial apenas acede ao Nextcloud e email via Reverse Proxy, enquanto o grupo TI possui acesso SSH aos servidores.

NÍVEL 1: ADMINISTRAÇÃO (ACESSO TOTAL)									
✓	33/169.22 MiB	IPv4 TCP	Alias_VPN_TI	*	*	*	*	none	[L1-Admin] TI → Acesso Total
NÍVEL 2: GESTÃO									
✓	0/0 B	IPv4 TCP	Alias_VPN_Gestores	*	LAN_NET	*	*	none	[L2-Gestao] Gestores → LAN completa
✓	0/0 B	IPv4 TCP	Alias_VPN_Gestores	*	DMZ_NET	*	*	none	[L2-Gestao] Gestores → DMZ completa
✓		IPv4 TCP	Alias_VPN_Gestores	*	*	*	*	none	[L2-Gestao] Gestores → Internet
NÍVEL 3: DEPARTAMENTOS (FINANCEIRO + COMERCIAL)									
✓		IPv4 TCP	Alias_VPN_Financeiro	*	HOST_DC	445 (MS DS)	*	none	[L3-Dept] Financeiro → File Server (SMB)
✓	0/0 B	IPv4 TCP/UDP	Alias_VPN_Financeiro	*	HOST_DC	53 (DNS)	*	none	[L3-Dept] Financeiro → DNS
✓		IPv4 TCP	Alias_VPN_Financeiro	*	*	80 (HTTP)	*	none	[L3-Dept] Financeiro → Internet (HTTP)
✓		IPv4 TCP	Alias_VPN_Financeiro	*	*	443 (HTTPS)	*	none	[L3-Dept] Financeiro → Internet (HTTPS)
✓		IPv4 UDP	Alias_VPN_Financeiro	*	*	123 (NTP)	*	none	[L3-Dept] Financeiro → NTP
✓		IPv4 TCP	Alias_VPN_Comercial	*	HOST_DC	445 (MS DS)	*	none	[L3-Dept] Comercial → File Server (SMB)
✓	0/0 B	IPv4 TCP/UDP	Alias_VPN_Comercial	*	HOST_DC	53 (DNS)	*	none	[L3-Dept] Comercial → DNS
✓		IPv4 TCP	Alias_VPN_Comercial	*	*	80 (HTTP)	*	none	[L3-Dept] Comercial → Internet (HTTP)
✓		IPv4 TCP	Alias_VPN_Comercial	*	*	443 (HTTPS)	*	none	[L3-Dept] Comercial → Internet (HTTPS)
✓		IPv4 UDP	Alias_VPN_Comercial	*	*	123 (NTP)	*	none	[L3-Dept] Comercial → NTP

Figura A.1: Regras de firewall para os pools VPN por departamento

A.2 Nextcloud

O Nextcloud foi configurado como plataforma central de colaboração, substituindo a tradicional partilha SMB por uma suite completa de produtividade. A integração com o AD permite autenticação centralizada e sincronização automática de utilizadores e grupos.

A Figura A.2 apresenta o conjunto de mais de 65 aplicações instaladas, organizadas por categoria: produtividade (Calendar, Contacts, Deck, Tasks, Notes), colaboração (Talk, Mail, Group Folders), segurança (Two-Factor TOTP, Suspicious Login) e integração (Collabora Online, LDAP backend).

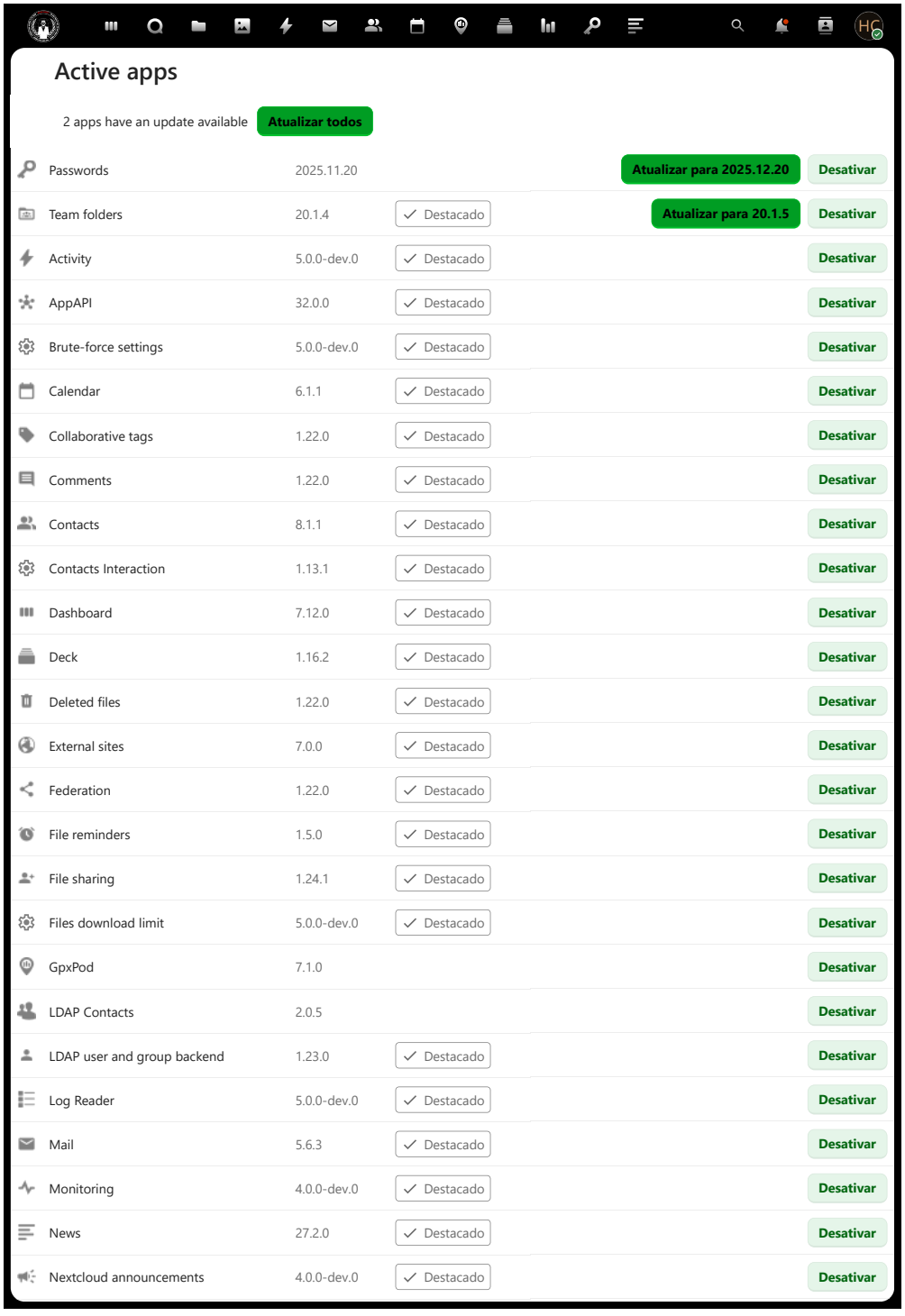


Figura A.2: Aplicações instaladas no Nextcloud (65+ apps)

A Figura A.3 ilustra a configuração do backend LDAP que permite ao Nextcloud autenticar utilizadores contra o AD. Os parâmetros incluem o servidor LDAP (192.168.1.10), a porta LDAPS (636), o filtro de utilizadores e o mapeamento de atributos.

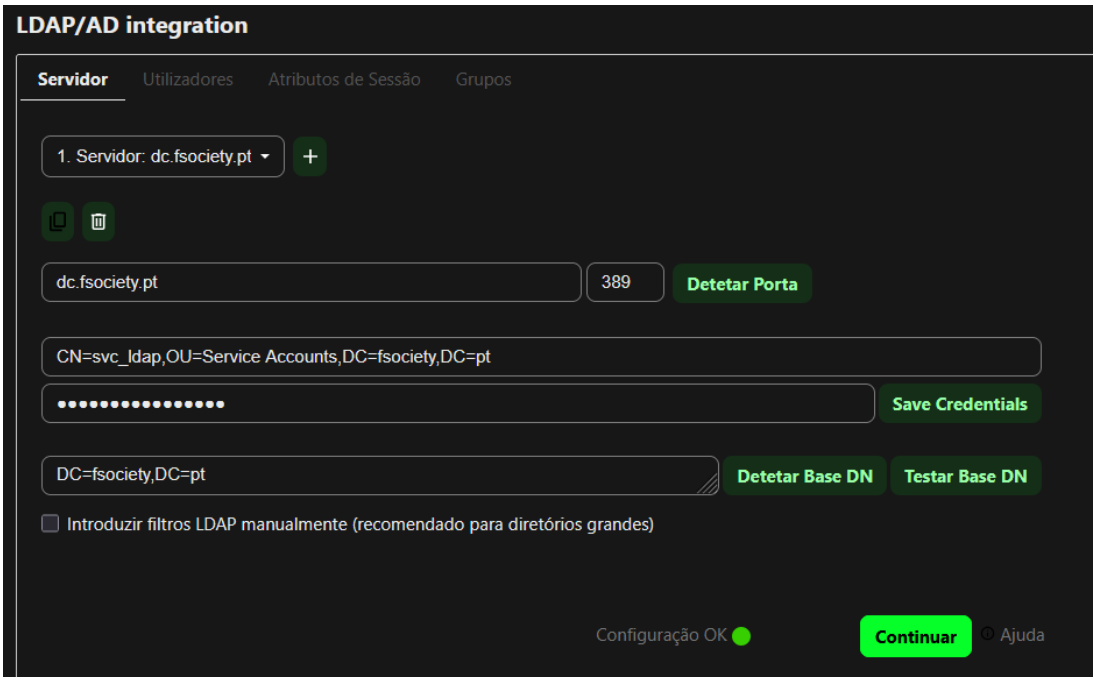


Figura A.3: Configuração da integração LDAP com Active Directory

A Figura A.4 apresenta os 19 utilizadores sincronizados automaticamente do AD, demonstrando o funcionamento do provisionamento automático de contas no primeiro login.

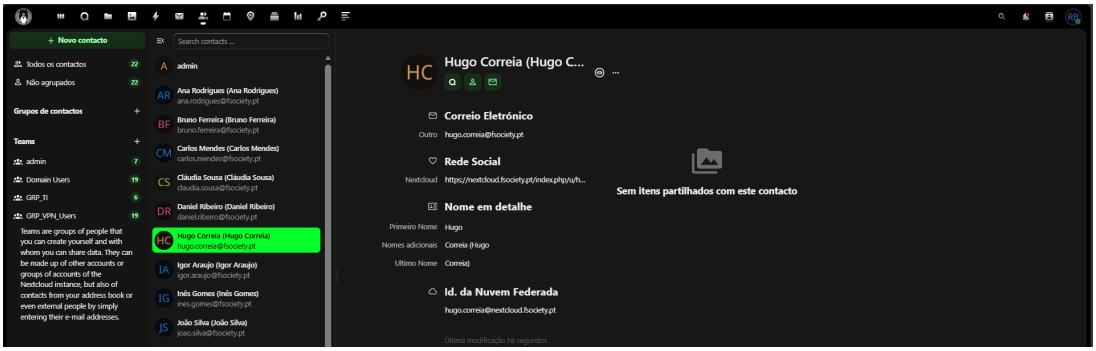


Figura A.4: Utilizadores sincronizados do Active Directory

A.3 Zammad – Sistema de Tickets

O Zammad foi integrado no ecossistema de produtividade através de um widget de suporte no dashboard do Nextcloud. Esta integração permite que os utilizadores acedam ao suporte técnico sem sair da plataforma principal de trabalho.

A Figura A.5 ilustra as quatro fases do fluxo de atendimento: abertura do pedido através do ícone de suporte, interação via chat com o agente, criação formal do ticket pelo agente, e envio automático de email de confirmação ao utilizador com o número do ticket para referência futura.

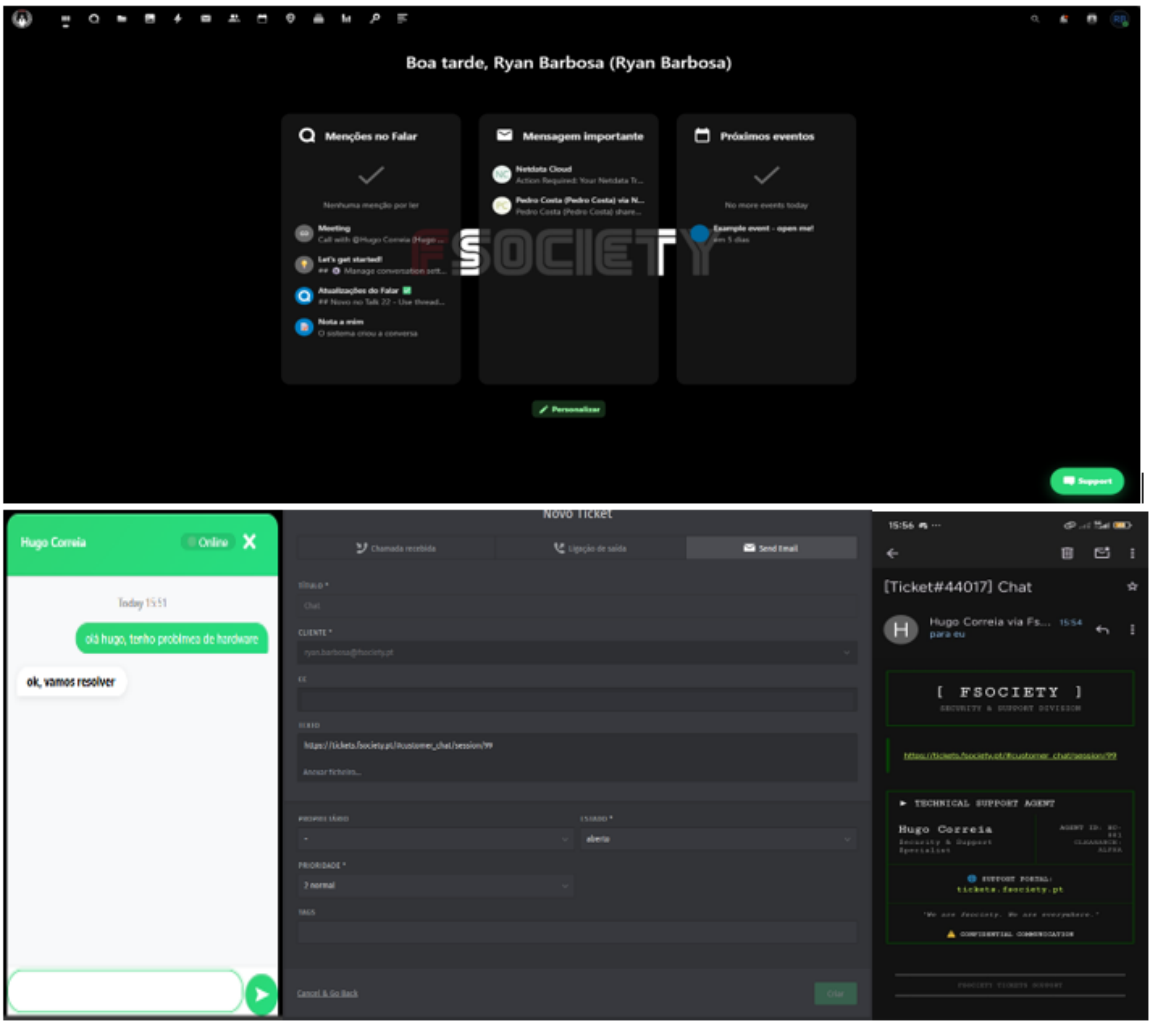


Figura A.5: Fluxo de atendimento no Zammad: (1) ícone de suporte no dashboard Nextcloud, (2) chat de suporte com agente, (3) criação do ticket pelo agente, (4) email de confirmação enviado ao utilizador

A.4 Mailcow – Servidor de Email

O Mailcow constitui a solução de email empresarial implementada na DMZ, integrando todos os componentes necessários numa arquitetura containerizada: MTA (Postfix), MDA (Dovecot), webmail (SOGo), anti-spam (Rspamd) e antivírus (ClamAV).

A Figura A.6 representa a arquitetura completa do servidor de email e as suas integrações com os restantes componentes da infraestrutura, incluindo o fluxo de mensagens inbound e outbound.

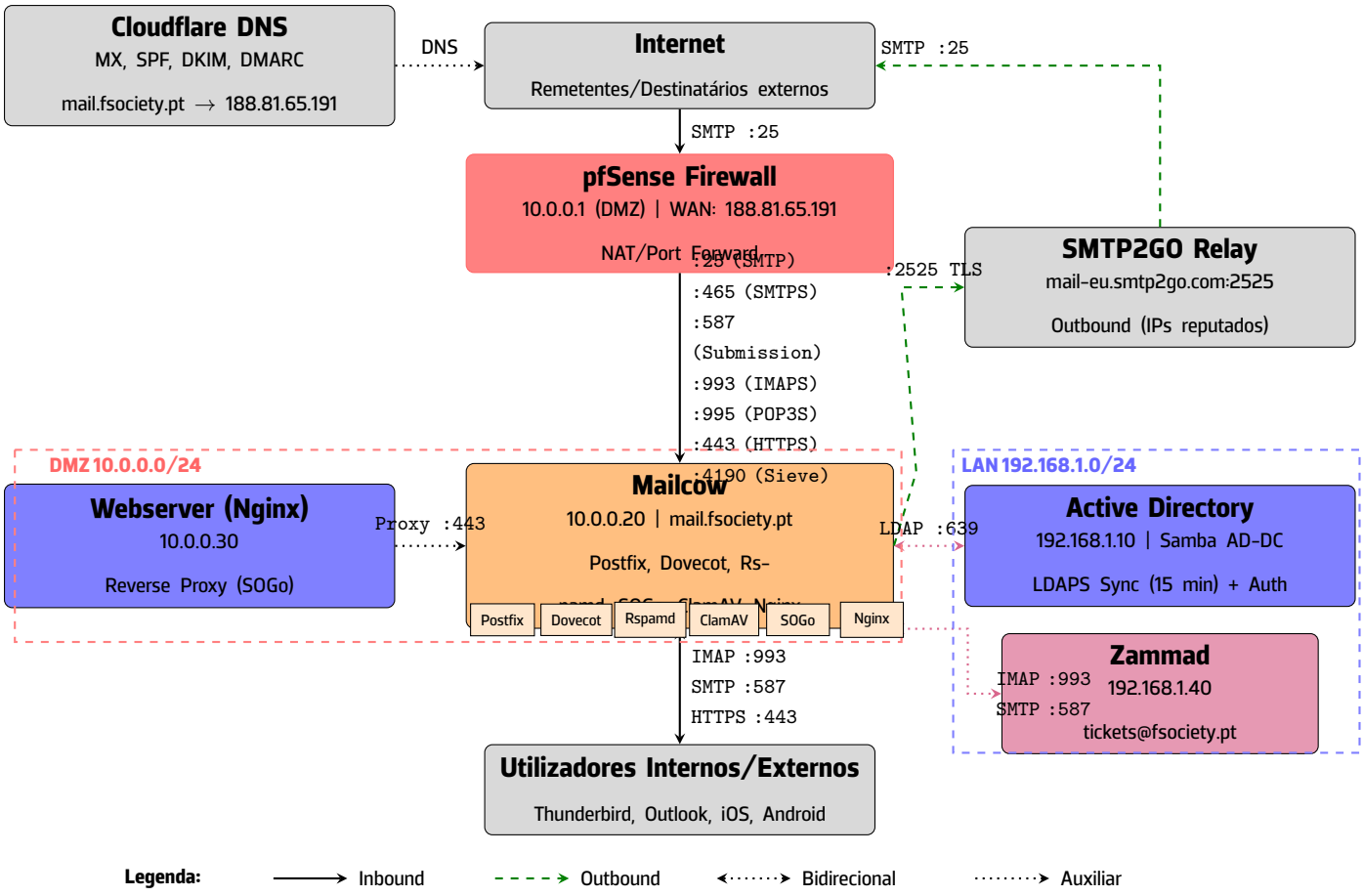


Figura A.6: Arquitetura do sistema de correio eletrónico Mailcow com integrações

A Figura A.7 apresenta a configuração do Identity Provider LDAP no painel de administração do Mailcow. A sincronização com o AD ocorre a cada 15 minutos, criando automaticamente mailboxes para novos utilizadores que possuam o atributo `mail` preenchido.

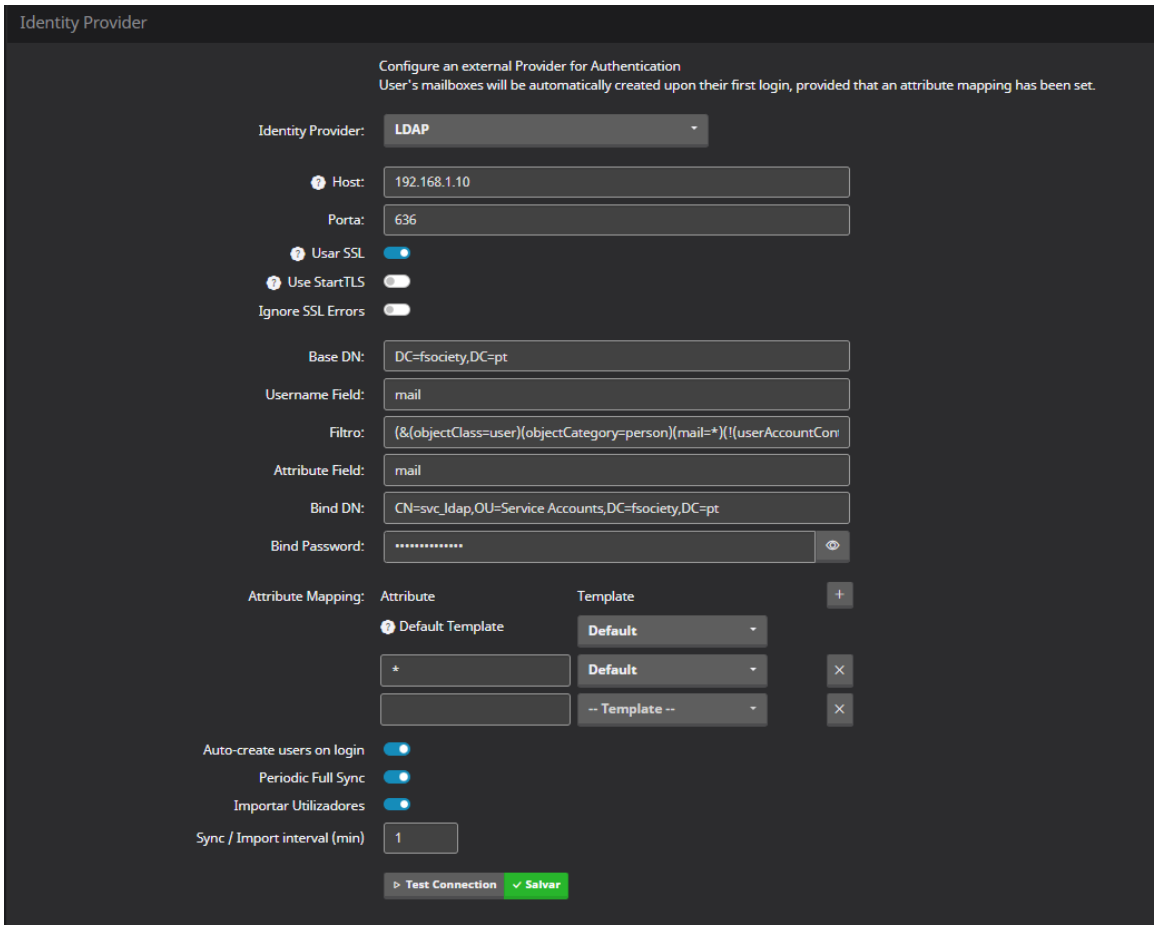


Figura A.7: Configuração da integração LDAP com Active Directory no Mailcow

A Figura A.8 demonstra a validação do sistema anti-spam Rspamd através do teste GTUBE. A mensagem de teste foi corretamente identificada e bloqueada, confirmando o funcionamento adequado da filtragem. São também visíveis as estatísticas de processamento: 63% sem ação necessária, 28% submetidas a Greylisting, e 9% rejeitadas como spam.

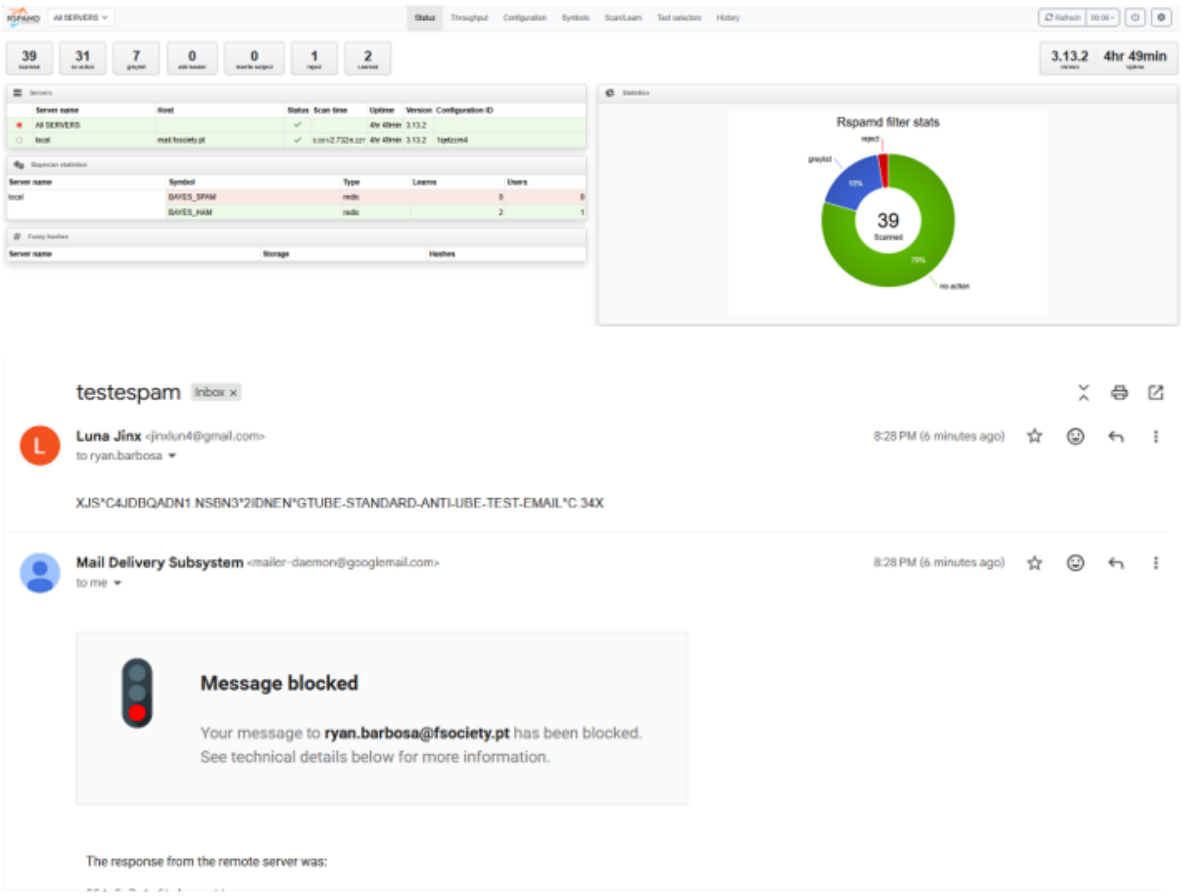


Figura A.8: Validação do sistema anti-spam Rspamd através do teste GTUBE

A Figura A.9 apresenta a interface do webmail SOGo, acessível em `mail.fsociety.pt`. A interface inclui caixa de entrada com pré-visualização de mensagens, acesso ao calendário partilhado e gestão de contactos com sincronização via ActiveSync.

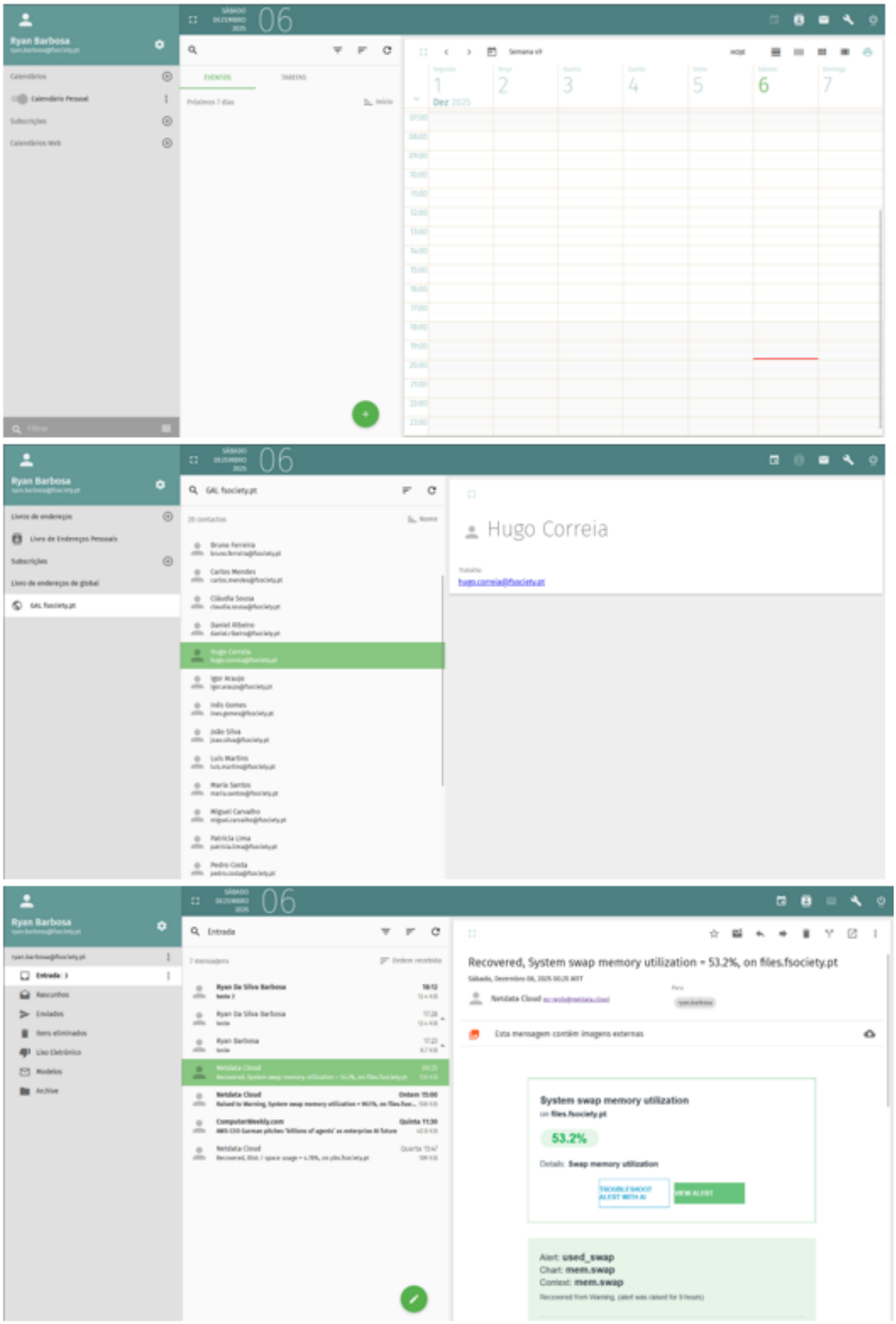


Figura A.9: Interface SOGo webmail com caixa de entrada, calendário e contactos

A Figura A.10 evidencia o funcionamento do protocolo Autodiscover, que permite a configuração automática de clientes de email. O utilizador apenas

inseriu o endereço de email e palavra-passe, sendo os parâmetros IMAP e SMTP detetados automaticamente através dos registos DNS autoconfig e autodiscover.

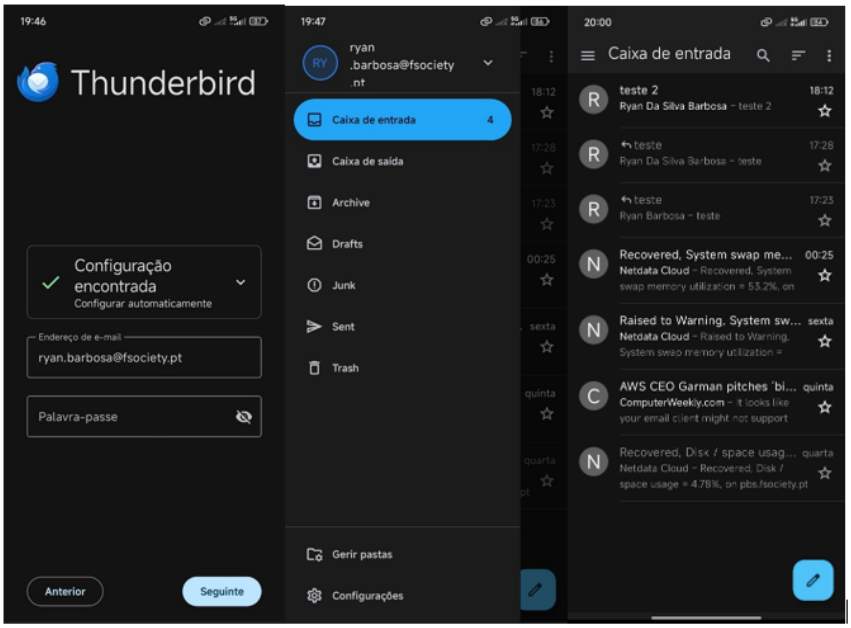


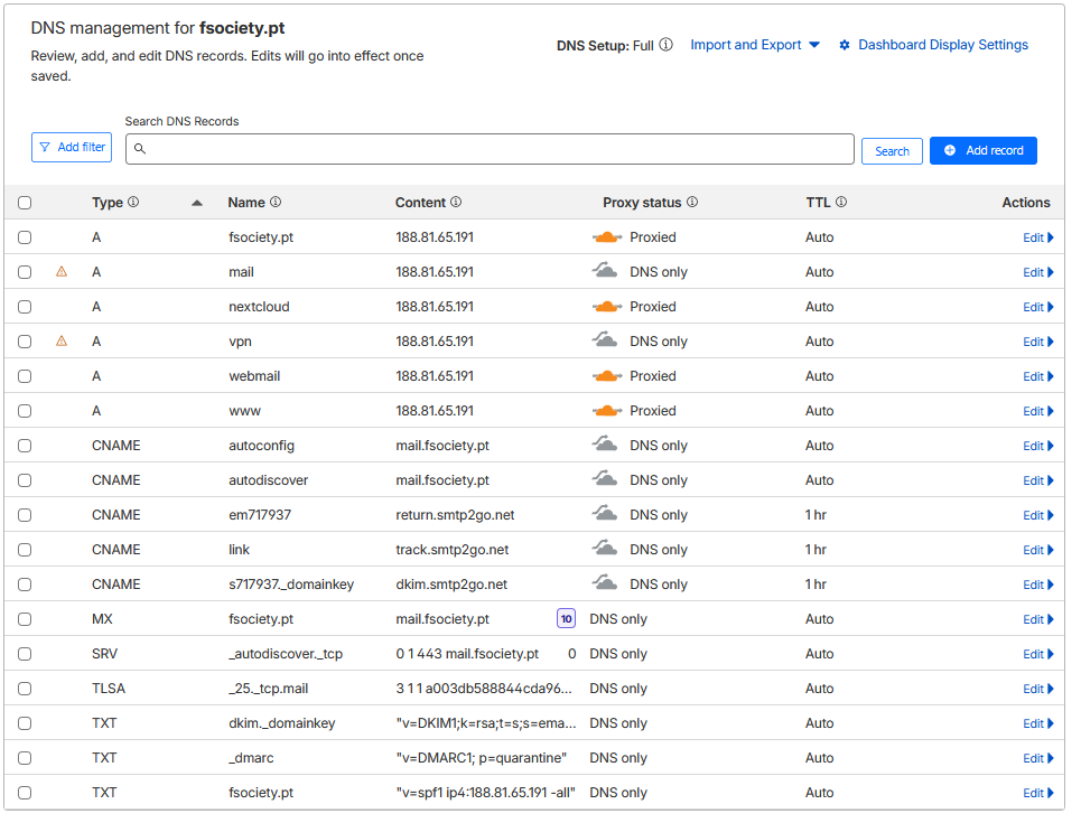
Figura A.10: Configuração automática no Mozilla Thunderbird via Autodiscover

A.5 Segurança

Esta secção apresenta as evidências visuais das configurações de segurança implementadas, incluindo DNS no Cloudflare, IDS/IPS distribuído com CrowdSec, e monitorização centralizada com Netdata Cloud.

A.5.1 Cloudflare DNS

A Figura A.11 apresenta a configuração DNS no Cloudflare para o domínio fsociety.pt. Os registos incluem entradas A para os serviços principais com proxy ativo, registos CNAME para autodiscovery do email, registos MX para receção de email, e registos TXT para autenticação (SPF, DKIM, DMARC).



DNS management for **fsociety.pt**

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ Import and Export Dashboard Display Settings

Search DNS Records

Add filter | Search | Add record

	Type ⓘ	Name ⓘ	Content ⓘ	Proxy status ⓘ	TTL ⓘ	Actions
	A	fsociety.pt	188.81.65.191	Proxied	Auto	Edit
⚠	A	mail	188.81.65.191	DNS only	Auto	Edit
	A	nextcloud	188.81.65.191	Proxied	Auto	Edit
⚠	A	vpn	188.81.65.191	DNS only	Auto	Edit
	A	webmail	188.81.65.191	Proxied	Auto	Edit
	A	www	188.81.65.191	Proxied	Auto	Edit
	CNAME	autoconfig	mail.fsociety.pt	DNS only	Auto	Edit
	CNAME	autodiscover	mail.fsociety.pt	DNS only	Auto	Edit
	CNAME	em717937	return.smtp2go.net	DNS only	1 hr	Edit
	CNAME	link	track.smtp2go.net	DNS only	1 hr	Edit
	CNAME	s717937._domainkey	dkim.smtp2go.net	DNS only	1 hr	Edit
	MX	fsociety.pt	mail.fsociety.pt 10	DNS only	Auto	Edit
	SRV	_autodiscover._tcp	0 1 443 mail.fsociety.pt 0	DNS only	Auto	Edit
	TLSA	_25._tcp.mail	3 1 1 a003db588844cda96...	DNS only	Auto	Edit
	TXT	dkim._domainkey	"v=DKIM1;k=rsa;t=s;s=ema...	DNS only	Auto	Edit
	TXT	_dmarc	"v=DMARC1; p=quarantine"	DNS only	Auto	Edit
	TXT	fsociety.pt	"v=spf1 ip4:188.81.65.191 -all"	DNS only	Auto	Edit

Figura A.11: Configuração DNS no Cloudflare para o domínio fsociety.pt

A.5.2 CrowdSec – IDS/IPS Distribuído

O CrowdSec foi implementado em quatro servidores da infraestrutura como sistema de deteção e prevenção de intrusões baseado em análise comportamental e inteligência colaborativa.

A Figura A.12 apresenta o dashboard com os quatro servidores monitorizados, todos registados no IP público e ligados à CAPI para partilha de inteligência de ameaças com a comunidade global.

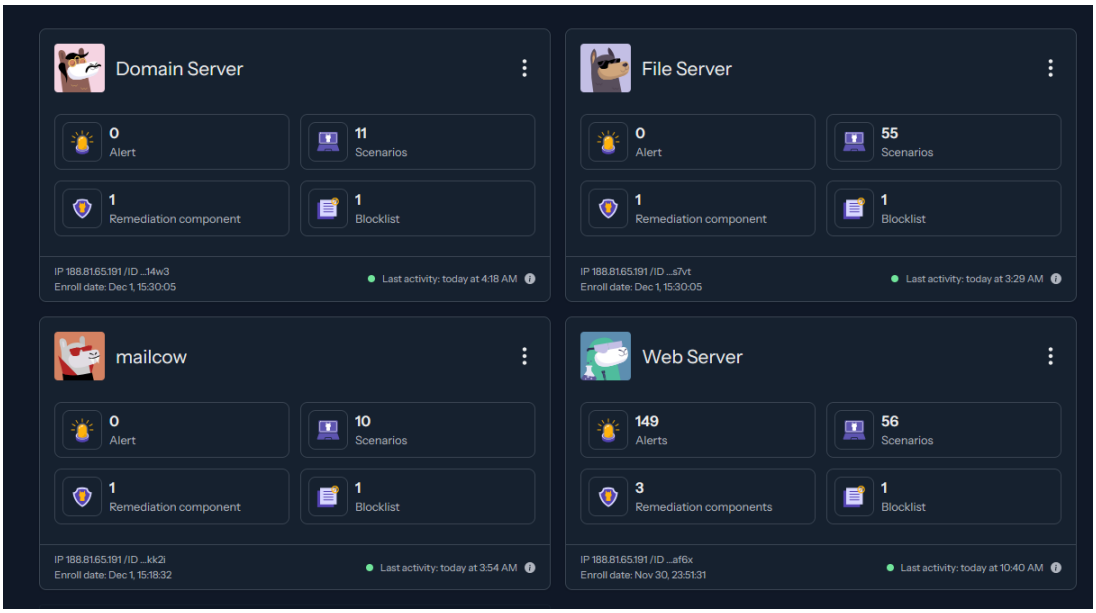


Figura A.12: Dashboard CrowdSec com os quatro servidores monitorizados

A Figura A.13 ilustra a distribuição de intenções maliciosas detetadas pelo CrowdSec durante o período de operação, categorizadas por tipo de ataque (brute-force, scanning, exploitation).

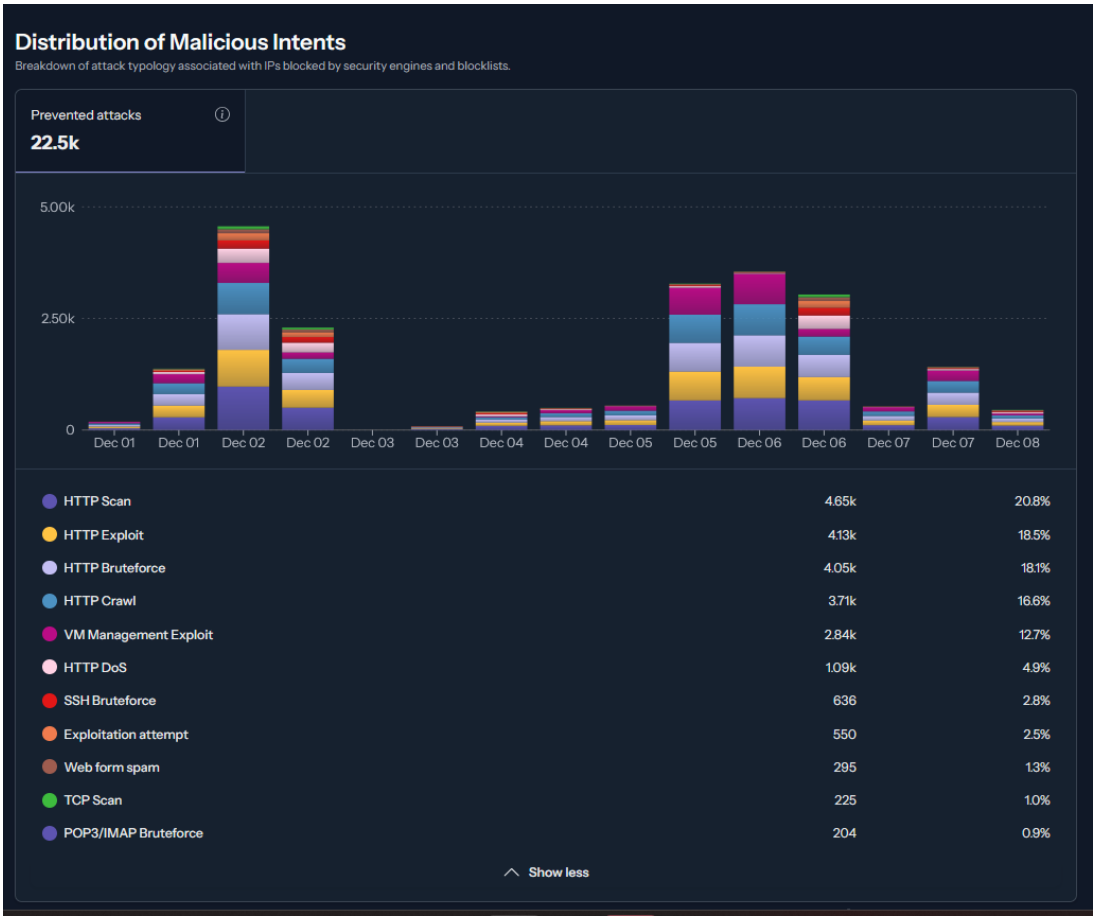


Figura A.13: Distribuição de intenções maliciosas detetadas pelo CrowdSec

A Figura A.14 apresenta as métricas de tráfego malicioso descartado pelos Bouncers, demonstrando a eficácia da remediação automática em bloquear

ataques antes de atingirem os serviços protegidos.

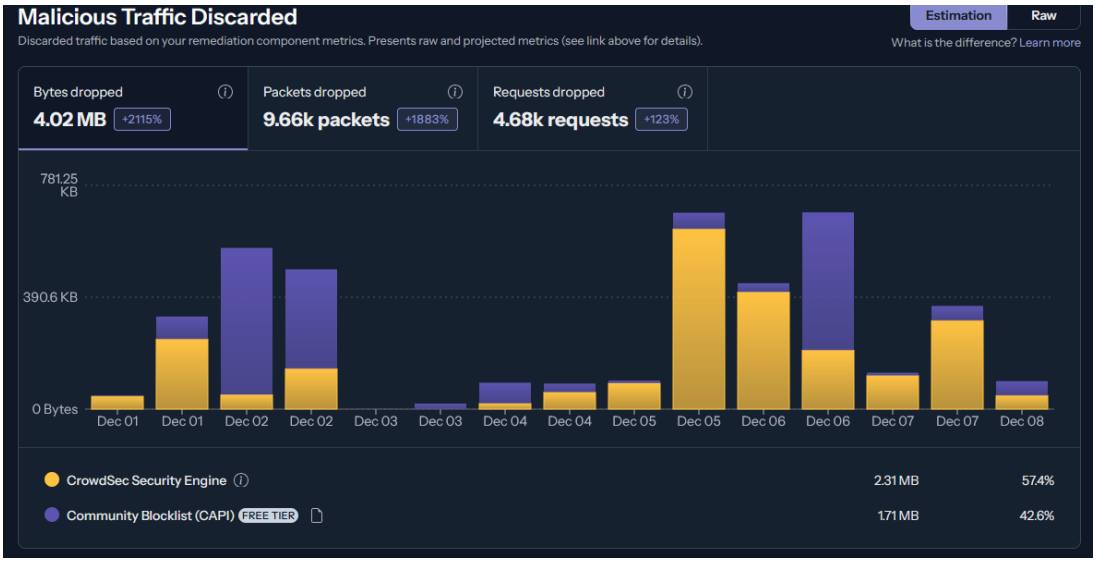


Figura A.14: Tráfego malicioso descartado pelo CrowdSec

A Figura A.15 quantifica os recursos poupados através da remediação CrowdSec, incluindo largura de banda não consumida por tráfego malicioso e tempo de processamento evitado nos servidores.

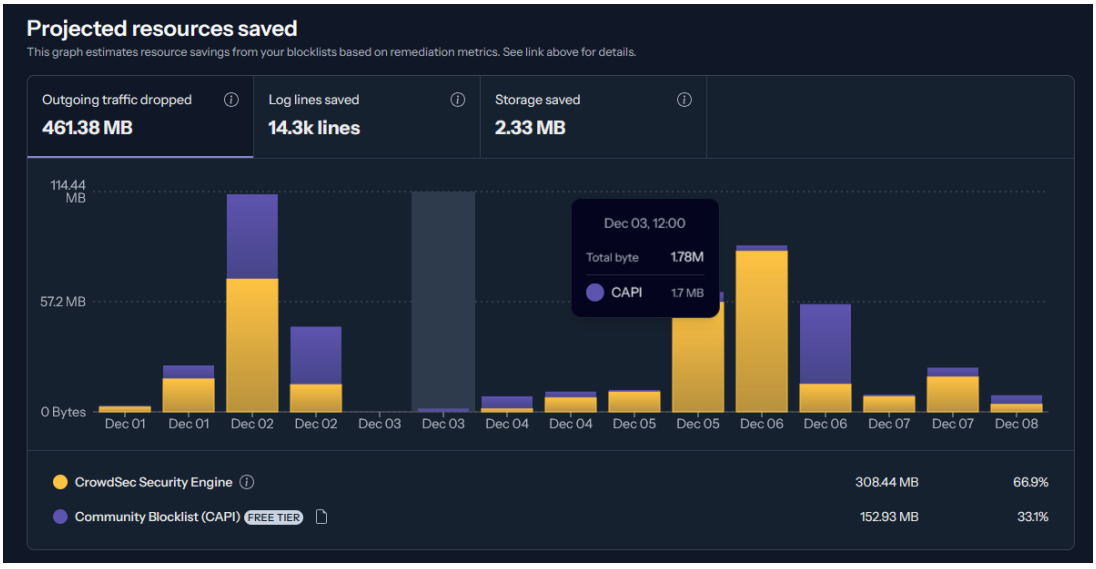


Figura A.15: Recursos poupados através da remediação CrowdSec

A.5.3 Netdata Cloud – Monitorização

O Netdata Cloud agrega métricas de seis servidores com granularidade de 1 segundo, providenciando visibilidade contínua sobre o estado da infraestrutura.

A Figura A.16 apresenta o dashboard centralizado com visão agregada dos servidores monitorizados: PVE, pfSense, DC, Servidor de Ficheiros, Servidor de Email e Webserver.

Figura A.16: Dashboard Netdata Cloud com visão agregada dos 6 servidores

A Figura A.17 demonstra o sistema de alertas configurado, que reduz o MTTD de potenciais horas para segundos. As notificações são enviadas por email com relatório detalhado de saúde da infraestrutura e através da aplicação móvel nativa para alertas em tempo real.

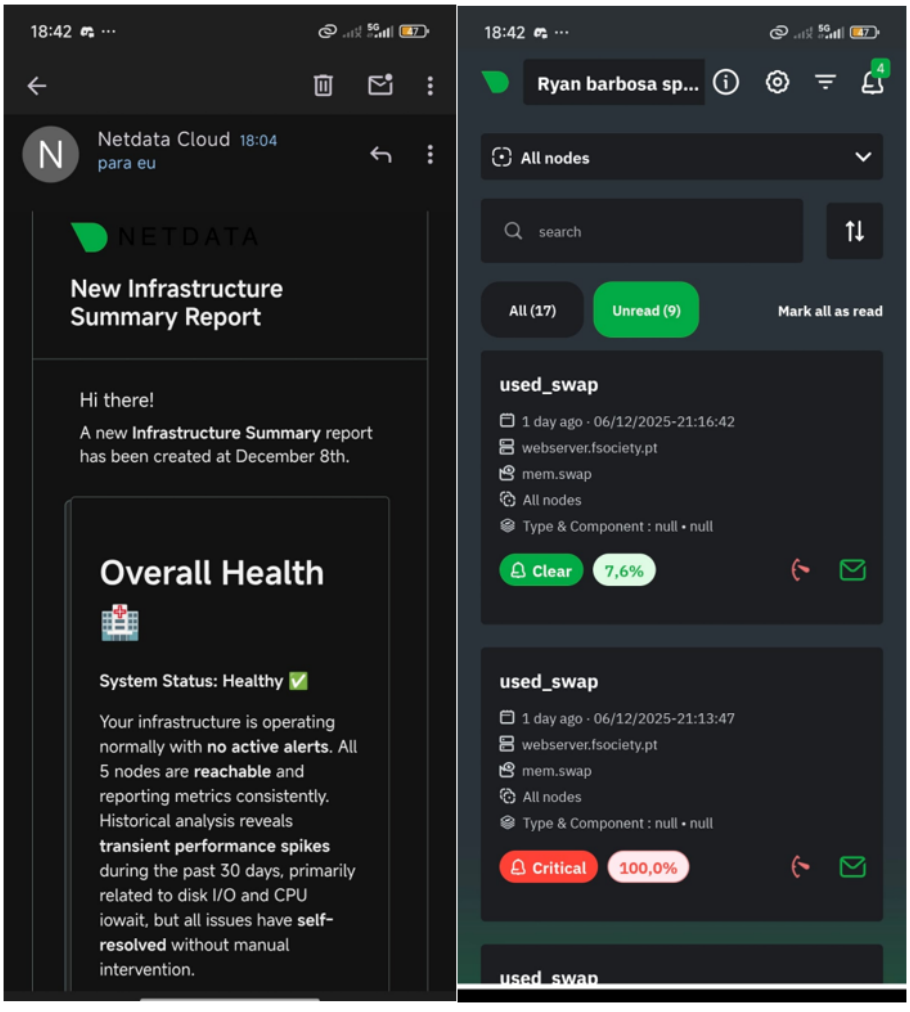


Figura A.17: Sistema de alertas Netdata: notificação por email e aplicação móvel

A.6 Demonstrações em Vídeo

Configurações extensas que não são adequadamente representadas em capturas de ecrã estáticas foram documentadas em formato de vídeo. Os vídeos estão disponíveis no repositório do projeto e podem ser acedidos através das hiperligações nas figuras abaixo.

A.6.1 Regras de Firewall

A Figura A.18 permite aceder à demonstração completa da navegação pelas aproximadamente 100 regras de Firewall configuradas no pfSense, distribuídas pelas interfaces WAN, LAN, DMZ e OpenVPN. O vídeo evidencia a organização hierárquica das regras e o princípio Default Deny implementado.

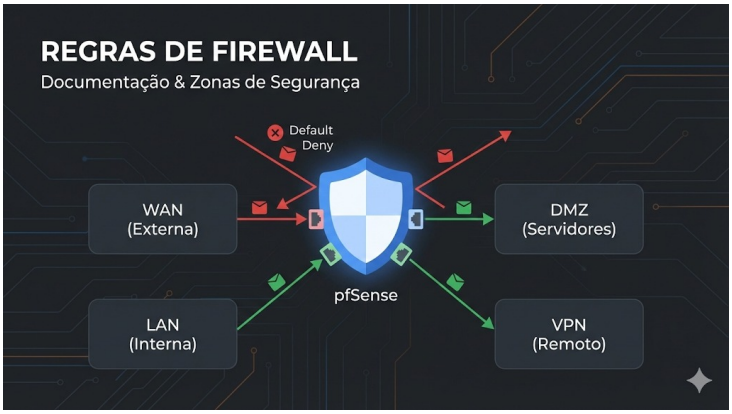


Figura A.18: Demonstração das regras de firewall do pfSense (clique para ver vídeo)

A.6.2 RADIUS Accounting Daemon

A Figura A.19 permite aceder à demonstração do daemon de contabilização RADIUS, que regista sessões VPN incluindo eventos de início, atualização e fim de sessão, bem como estatísticas de tráfego por utilizador.

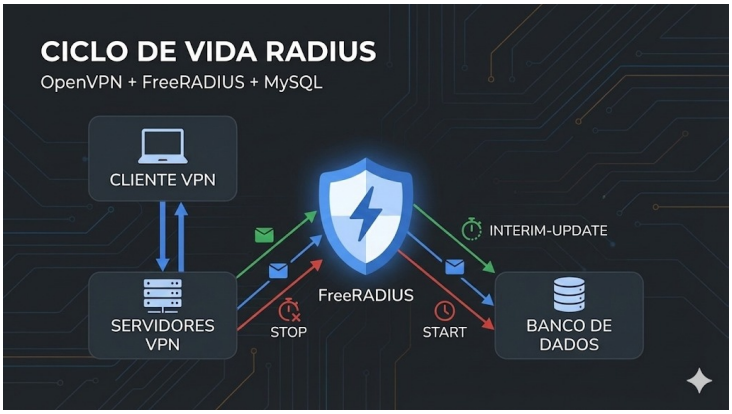


Figura A.19: Demonstração do RADIUS Accounting Daemon (clique para ver vídeo)

B. Tabelas

Este anexo apresenta as tabelas detalhadas referenciadas ao longo do relatório, cujas dimensões ou nível de detalhe não justificavam a sua inclusão no corpo principal do documento. As tabelas estão organizadas por temática, abrangendo requisitos do projeto e seleção tecnológica.

B.1 Requisitos Adicionais

Para além dos requisitos obrigatórios definidos no enunciado do trabalho prático, a equipa identificou oportunidades de enriquecer a infraestrutura com funcionalidades que aproximassem o projeto de um cenário empresarial real. Estas extensões demonstram competências avançadas em administração de sistemas e foram implementadas após a conclusão dos requisitos base.

A Tabela B.1 apresenta o detalhe completo dos requisitos adicionais implementados, incluindo a evolução para arquitetura Four-Legged Firewall, implementação de AD com Samba AD DC, servidor de email (Mailcow), plataforma de colaboração (Nextcloud), IDS/IPS distribuído (CrowdSec), e monitorização com AI (Netdata Cloud). Para cada requisito é apresentada a respetiva justificação técnica e valor acrescentado.

B.2 Requisitos Funcionais

Os requisitos funcionais definem as capacidades que o sistema deve providenciar aos seus utilizadores. Resultam da consolidação dos requisitos obrigatórios do enunciado com as funcionalidades adicionais identificadas pela equipa, abrangendo seis domínios principais: infraestrutura de rede (segmentação, DHCP, DNS), segurança perimetral (Firewall, IDS/IPS), serviços de rede (HTTP, partilha de ficheiros, email), gestão de identidades (AD/LDAP, SSO), acesso remoto (VPN com RADIUS), e operações (monitorização, backup).

A Tabela B.2 consolida todos os requisitos funcionais organizados por domínio, identificando a origem de cada um: requisito do enunciado, funcionalidade extra implementada pela equipa, ou requisito misto que combina ambas as fontes.

B.3 Requisitos Não-Funcionais

Os requisitos não-funcionais estabelecem critérios de qualidade e restrições técnicas transversais à implementação, definindo as características que o sistema deve exibir independentemente das funcionalidades específicas. Estes requisitos são fundamentais para garantir que a infraestrutura opera de forma segura, eficiente e em conformidade com as normas aplicáveis.

A Tabela B.3 detalha os requisitos não-funcionais organizados por categoria: segurança (tráfego entre zonas via Firewall, TLS 1.2+, políticas de passwords), desempenho (latência LDAP < 100ms, overhead de monitorização < 3%), disponibilidade (> 99% para serviços críticos), escalabilidade (suporte até 200 utilizadores), manutenibilidade (documentação completa e versionada), e conformidade (RGPD, soluções *open-source*).

Tabela B.1: Requisitos Adicionais Implementados

Componente	Descrição
Four-Legged Firewall	Extensão da arquitetura para incluir zona VPN dedicada (10.8.0.0/24 e 10.9.0.0/24), permitindo isolamento e políticas específicas para acesso remoto
Active Directory	Evolução de simples partilha de ficheiros para gestão centralizada de identidades com Samba AD DC, incluindo LDAP, Kerberos e GPO
Autenticação VPN/RADIUS	Integração OpenVPN com FreeRADIUS e Active Directory, com pools de IP hierárquicos por grupo departamental
Servidor de Email	Implementação de Mailcow na DMZ com Postfix, Dovecot, Rspamd, integração LDAP e validação SPF/DKIM/DMARC
Plataforma de Colaboração	Nextcloud com 65+ aplicações, substituindo simples partilha SMB por suite completa de produtividade
IDS/IPS Distribuído	CrowdSec em todos os servidores com 57+ cenários de deteção e blocklists colaborativas (70k IPs)
Proteção Edge	Cloudflare como camada WAF/CDN para serviços web públicos, com mitigação DDoS e TLS gerido
Monitorização Avançada	Netdata Cloud com agregação de 6 servidores, granularidade de 1 segundo e AI Insights para análise preditiva
Backup Centralizado	Proxmox Backup Server com deduplicação, cifração e verificação automática de integridade
Sistema de Tickets	Zammad integrado com LDAP para gestão de incidentes e suporte interno

B.4 Tecnologias Selecionadas

A seleção das tecnologias seguiu um processo estruturado, priorizando soluções *open-source* maduras e com comunidades ativas. As alternativas foram avaliadas segundo cinco critérios: adequação funcional, maturidade e estabilidade, custo de licenciamento e operação, compatibilidade com restantes componentes, e alinhamento com as competências da equipa.

A Tabela B.4 apresenta o resumo completo das tecnologias escolhidas para cada componente da infraestrutura — PVE para virtualização, pfSense como Firewall, Samba AD DC para gestão de identidades, Nextcloud para colaboração, Mailcow para email, e Netdata Cloud para monitorização — incluindo a justificação técnica de cada escolha e as alternativas consideradas.

Tabela B.2: Requisitos Funcionais por Domínio

Domínio	**Requisitos**	**Origem**
Infraestrutura de Rede	Segmentação em zonas distintas (LAN, DMZ, VPN); servidor DHCP para atribuição automática de IPs; servidor DNS para resolução interna e externa	Enunciado
Segurança Perimetral	Firewall com políticas *default deny*; proteção da rede interna e DMZ; IDS/IPS distribuído em todos os servidores	Misto
Serviços de Rede	Servidor HTTP na DMZ; partilha de ficheiros na LAN; servidor de email com anti-spam e antivírus	Misto
Gestão de Identidades	Autenticação centralizada via AD/LDAP; *Single Sign-On* para todos os serviços; integração com VPN via RADIUS	Extra
Acesso Remoto	VPN com autenticação integrada no Active Directory; permissões diferenciadas por departamento através de pools IP hierárquicos	Extra
Operações	Monitorização centralizada com alertas automáticos; backup automatizado com verificação de integridade; sistema de tickets para gestão de incidentes	Extra

Tabela B.3: Requisitos Não-Funcionais por Categoria

Categoria	**Requisitos**
Segurança	Todo o tráfego entre zonas deve passar pelo firewall central; comunicações externas devem utilizar cifração TLS 1.2 ou superior; passwords devem cumprir política de complexidade definida no Active Directory
Desempenho	Latência de autenticação LDAP inferior a 100ms; overhead de monitorização inferior a 3% de CPU por servidor
Disponibilidade	Serviços críticos (firewall, AD, DNS) devem ter disponibilidade superior a 99%
Escalabilidade	Arquitetura deve suportar crescimento até 200 utilizadores sem alterações estruturais
Manutenibilidade	Documentação completa de todas as configurações; versionamento de configurações em repositório Git; guias de troubleshooting para cada componente
Conformidade	Sistema deve cumprir requisitos básicos do RGPD (dados em território controlado, direito ao esquecimento); utilização exclusiva de soluções *open-source* para eliminar custos de licenciamento

Tabela B.4: Tecnologias Selecionadas por Componente

Componente	**Tecnologia**	**Justificação**
Virtualização	Proxmox VE 8.x	Interface web completa, suporte KVM+LXC, custo zero, integração nativa com Proxmox Backup Server
Firewall	pfSense CE 2.8.x	Maturidade comprovada, documentação extensa, suporte robusto a OpenVPN com autenticação RADIUS
Active Directory	Samba AD DC 4.x	Compatibilidade com clientes Windows, LDAP/Kerberos nativo, sem custos de licenciamento
DHCP/DNS	Samba + ISC DHCP	Integração nativa com AD, suporte a DNS dinâmico, gestão centralizada
Partilha Ficheiros	Nextcloud 32.x	Suite completa de colaboração, 65+ aplicações, integração LDAP robusta
Servidor HTTP	Nginx	Alta performance, reverse proxy, integração nativa com Let's Encrypt
Servidor Email	Mailcow	Arquitetura Docker simplificada, Rspamd com machine learning, integração LDAP
VPN	OpenVPN	Integração RADIUS nativa, clientes multiplataforma, configuração flexível
IDS/IPS	CrowdSec	Abordagem colaborativa, baixo overhead, deployment multi-servidor simplificado
Monitorização	Netdata Cloud	Zero-config, granularidade 1 segundo, AI Insights para análise preditiva
Backup	Proxmox Backup Server	Deduplicação eficiente, cifração, integração nativa com Proxmox VE