UC00635 – CONFIGURAR SERVIÇOS DE REDE

Formador: José Ramos

Síntese

O projeto Paca Cloud consistiu na implementação de uma infraestrutura de rede segmentada com LAN, DMZ e Outside, interligadas por uma firewall pfSense. Foram configurados serviços essenciais em Windows Server e Ubuntu Server, com foco na segurança, controlo de acessos e administração de sistemas.

Sérgio Correia / Daniel Santos

Índice

Introdução

No âmbito da unidade curricular, foi desenvolvido o projeto Paca Cloud, cujo objetivo principal consistiu na implementação de uma infraestrutura de rede e serviços completa, funcional e segura, simulando um cenário real de uma organização empresarial.

O projeto envolveu o planeamento e a implementação de uma rede segmentada em rede interna (LAN), zona desmilitarizada (DMZ) e rede externa (Outside), interligadas através de uma firewall pfSense, permitindo aplicar conceitos de segurança, controlo de acessos e separação de serviços críticos. Esta abordagem teve como principal finalidade proteger a rede interna, enquanto disponibiliza serviços ao exterior de forma controlada.

Ao longo do desenvolvimento foram configurados diversos serviços essenciais, com destaque para Active Directory e DHCP em Windows Server 2022, bem como múltiplos serviços em Linux, nomeadamente servidor Web, servidor de Email (Mailcow), FTP e SSH. A infraestrutura foi complementada com a utilização de Docker, reverse proxy com Apache, e a implementação de certificados SSL assinados por uma Autoridade de Certificação interna, garantindo comunicações cifradas e uma identidade digital consistente para os serviços disponibilizados.

O projeto foi desenvolvido em ambiente virtualizado, permitindo testar diferentes cenários, resolver conflitos técnicos e validar a comunicação entre redes e serviços. Durante este processo foram também aplicadas boas práticas de administração de sistemas, automação através de scripts e testes de segurança, de forma a assegurar o correto funcionamento e a robustez da solução final.

Enquadramento do Projeto

O projeto **Paca Cloud** surge no âmbito académico como uma aplicação prática de competências em redes, sistemas operativos, segurança e virtualização, simulando as exigências de um ambiente empresarial real. A solução foca-se na criação de uma infraestrutura que assegura a disponibilidade e escalabilidade de serviços, priorizando a proteção dos dados através de uma arquitetura segmentada. Para tal, o sistema separa a rede interna, dedicada à gestão de recursos e utilizadores, de uma Zona Desmilitarizada (DMZ), onde ficam alojados os serviços expostos ao exterior, como servidores Web e de Email. Todo este tráfego é gerido e filtrado por uma firewall dedicada, que garante o controlo rigoroso dos acessos e a integridade da rede interna face a ameaças externas.

Para além da vertente de redes, o projeto enquadra-se também na área da administração de sistemas, recorrendo a sistemas Windows Server e Linux, à automatização de tarefas através de scripts e à utilização de tecnologias modernas como contentores Docker. Foi ainda dada especial atenção à segurança das comunicações, através da implementação de certificados digitais assinados por uma Autoridade de Certificação interna, garantindo o uso de HTTPS e a confiança dos clientes nos serviços disponibilizados.

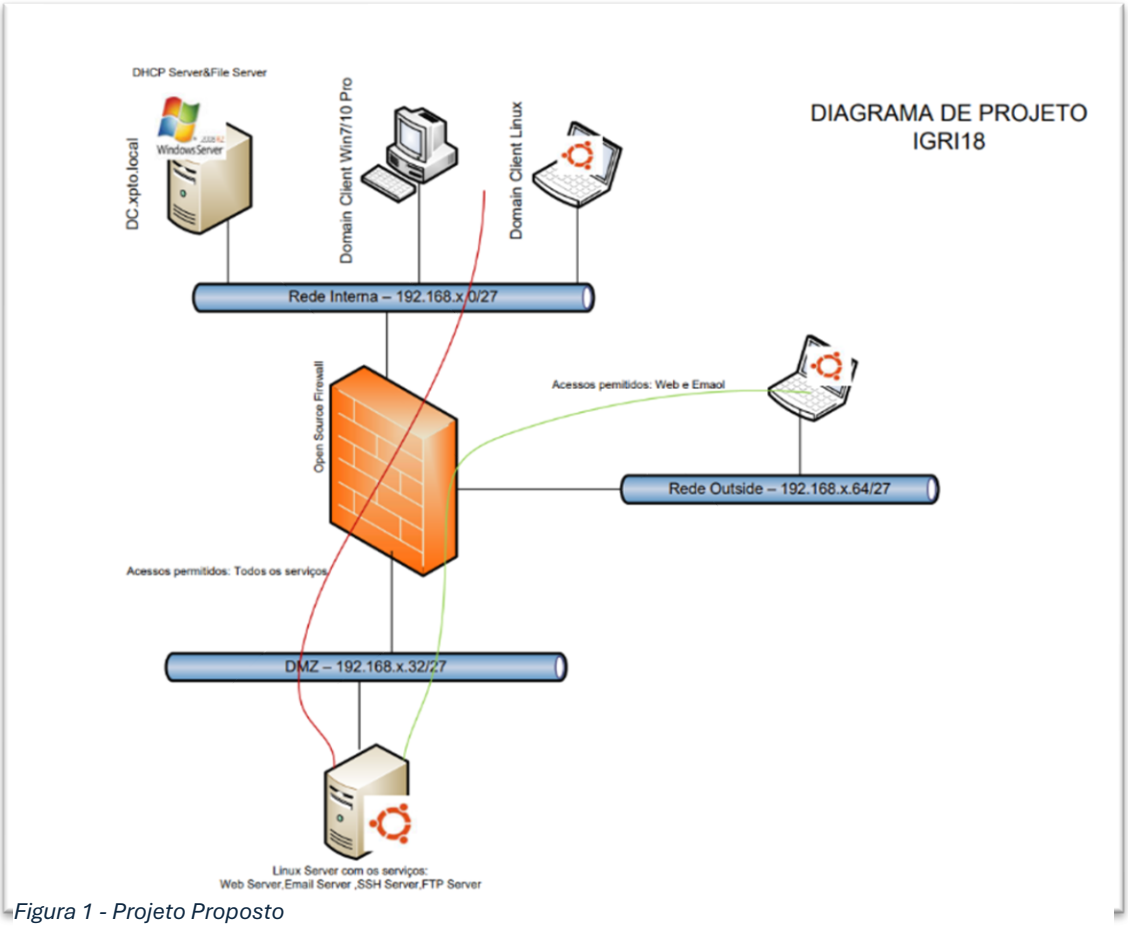

Figura 1 - Projeto Proposto

Objetivos do Projeto

O projeto Paca Cloud teve como objetivo principal a implementação de uma infraestrutura de rede e serviços segura e funcional, simulando um ambiente empresarial real.

De forma específica, pretendeu-se:

- Implementar uma rede segmentada com LAN, DMZ e Outside, utilizando uma firewall pfSense;
- Configurar um servidor Windows Server 2022 com Active Directory, DNS e DHCP;
- Implementar um servidor Linux na DMZ com serviços de Web, Email, FTP e SSH;
- Instalar e configurar o Mailcow com Docker para gestão de correio eletrónico;
- Implementar reverse proxy e certificados SSL assinados por uma CA interna;
- Integrar clientes Linux no domínio Windows;
- Testar a segurança, conectividade e funcionamento dos serviços.

Com este projeto, foi possível consolidar conhecimentos práticos nas áreas de redes, sistemas, segurança e administração de serviços.

Descrição Geral da Infraestrutura

A infraestrutura desenvolvida no projeto Paca Cloud baseia-se numa arquitetura de rede segmentada e centralizada, projetada para garantir segurança, organização e controlo de acessos entre os diferentes componentes do sistema. A solução foi implementada em ambiente virtualizado e estruturada em torno de uma firewall pfSense, que funciona como elemento central de encaminhamento e filtragem de tráfego.

A rede encontra-se dividida em três segmentos principais, cada um com uma função específica:

- Rede Interna (LAN)
- Zona Desmilitarizada (DMZ)
- Rede Externa (Outside)

A interligação entre estes segmentos é assegurada pelo pfSense, que possui múltiplas interfaces de rede configuradas, permitindo isolar os serviços críticos e aplicar regras de segurança adequadas a cada zona.

Rede Interna (LAN)

A rede interna corresponde ao segmento principal da organização, com o endereço 192.168.0.0/28, sendo designada como *LAN Segment 1*. Neste segmento encontram-se os sistemas responsáveis pela gestão e autenticação dos utilizadores, bem como os postos de trabalho internos.

Nesta rede estão presentes:

- Um Windows Server 2022, configurado como Domain Controller, com os serviços de Active Directory, DNS e DHCP, associado ao domínio *paca*. *cloud*;
- Um cliente Windows 10, utilizado para testes de autenticação e acesso a serviços;
- Um cliente Linux Mint, integrado no domínio para validação da interoperabilidade entre sistemas.

A atribuição de endereços IP aos clientes é efetuada dinamicamente através de DHCP, com um intervalo definido entre 192.168.0.6 e 192.168.0.13, tendo como gateway o pfSense.

Zona Desmilitarizada (DMZ)

A DMZ corresponde ao segmento destinado à disponibilização de serviços acessíveis externamente, utilizando a rede 192.168.0.16/29, identificada como *LAN Segment 2*. Esta separação permite proteger a rede interna, impedindo acessos diretos a sistemas críticos.

Neste segmento encontra-se um servidor Ubuntu, com endereço IP estático 192.168.0.17, responsável pela execução dos seguintes serviços:

- **Servidor Web;**
- **Servidor de Email (Mailcow);**
- **Servidor FTP;**
- **Serviço SSH para administração remota.**

A colocação destes serviços na DMZ garante que apenas o tráfego estritamente necessário é permitido a partir da rede externa, reduzindo riscos de segurança.

Rede Externa (Outside)

A rede Outside simula o acesso externo à infraestrutura, utilizando o endereço 192.168.0.24/29, identificada como *LAN Segment 3*. Neste segmento encontra-se um cliente Linux Mint, que representa utilizadores externos à organização.

Este cliente é utilizado para testar:

- Acessos aos serviços web e de email;
- Comportamento das regras de firewall;
- Exposição controlada de portas e serviços.

Firewall pfSense

A firewall pfSense (versão 2.7.2) assume o papel central da infraestrutura, funcionando simultaneamente como router, firewall e ponto de controlo de acessos. O sistema encontra-se configurado com várias interfaces de rede, cada uma associada a um dos segmentos definidos, permitindo encaminhar o tráfego e aplicar regras específicas entre LAN, DMZ e Outside.

Esta abordagem garante uma infraestrutura organizada, segura e próxima de um cenário real, permitindo testar e validar políticas de segurança, comunicação entre redes e funcionamento dos serviços implementados.

Planeamento da Rede

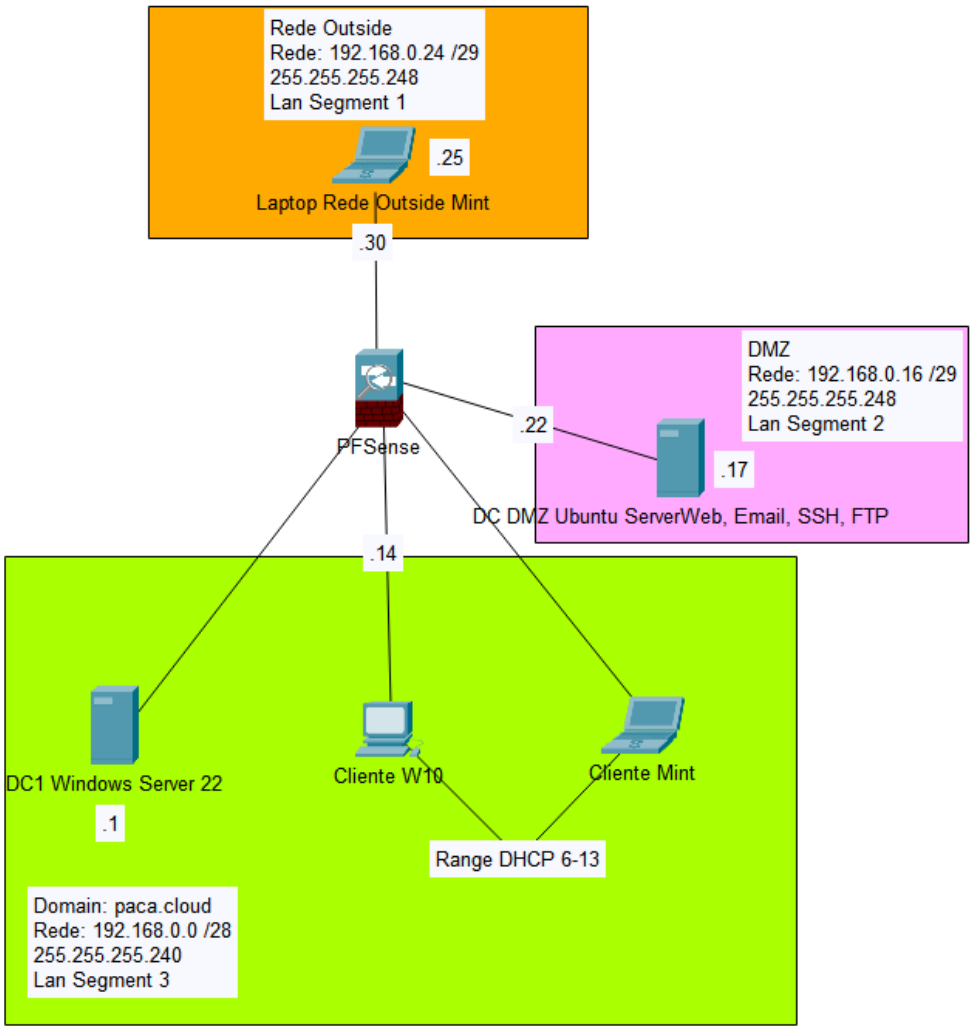

Figura 2 - Packet Tracer Projeto

O planeamento da rede constituiu uma fase fundamental do projeto Paca Cloud, uma vez que todas as configurações posteriores dependem de uma estrutura de rede bem definida, organizada e segura. Antes da implementação dos serviços, foi necessário definir a topologia, a segmentação da rede e o esquema de endereçamento IP, tendo em conta boas práticas de redes e segurança.

Topologia da Rede

A topologia adotada é do tipo estrela hierárquica, tendo a firewall pfSense como elemento central da infraestrutura. Todos os segmentos de rede encontram-se ligados diretamente ao pfSense, que é responsável pelo encaminhamento do tráfego entre redes e pela aplicação das regras de firewall.

Esta abordagem permite:

- Centralizar o controlo de acessos;
- Facilitar a gestão da rede;
- Aumentar a segurança, evitando ligações diretas entre segmentos sem filtragem.

Segmentação da Rede

A rede foi segmentada em três zonas distintas, cada uma com uma função específica, de forma a separar serviços críticos e reduzir riscos de segurança:

- Rede Interna (LAN) – destinada à gestão da infraestrutura e aos utilizadores internos;
- Zona Desmilitarizada (DMZ) – destinada ao alojamento de serviços acessíveis a partir do exterior;
- Rede Externa (Outside) – utilizada para simular acessos externos à organização.

Esta separação permite que os serviços públicos fiquem isolados da rede interna, garantindo que um eventual comprometimento da DMZ não afete diretamente os sistemas internos.

Endereçamento IP e Sub-redes

Foi utilizado endereçamento IPv4 privado, com subnetting adequado ao número de equipamentos existentes em cada segmento, evitando desperdício de endereços e facilitando a gestão da rede.

Rede Interna (LAN)

- Rede: 192.168.0.0/28
- Máscara: 255.255.255.240
- Gateway: 192.168.0.14
- Função: Gestão de utilizadores e equipamentos internos
- Equipamentos:
    - Windows Server 2022 (Domain Controller) – 192.168.0.1
    - Clientes Windows e Linux (IP atribuído por DHCP)
- Range DHCP: 192.168.0.6 a 192.168.0.13

DMZ

- Rede: 192.168.0.16/29
- Máscara: 255.255.255.248
- Gateway: 192.168.0.22
- Função: Serviços acessíveis externamente
- Equipamento:
    - Ubuntu Server – 192.168.0.17 (IP estático)

A utilização de IP estático na DMZ garante estabilidade no acesso aos serviços e simplifica a configuração da firewall e dos certificados SSL.

Rede Externa (Outside)

- Rede: 192.168.0.24/29
- Máscara: 255.255.255.248
- Gateway: 192.168.0.30
- Função: Simulação de clientes externos
- Equipamento:
    - Laptop Linux Mint – 192.168.0.25

Este segmento foi utilizado para validar o acesso externo aos serviços e testar as regras de segurança implementadas.

Justificação das Opções Tomadas

As opções de planeamento adotadas tiveram como base os seguintes critérios:

- Segurança, através da separação clara entre redes;
- Escalabilidade, permitindo adicionar novos serviços ou clientes;
- Organização, com sub-redes bem definidas;
- Realismo, aproximando o projeto de um cenário empresarial real.

O planeamento da rede permitiu criar uma base sólida para a implementação dos serviços, garantindo um funcionamento correto, seguro e fácil de gerir.

Descrição dos Equipamentos Utilizados

Para a implementação do projeto Paca Cloud foram utilizados vários equipamentos virtuais, cada um com uma função específica dentro da infraestrutura. Todos os sistemas foram configurados em ambiente virtualizado, permitindo simular um cenário real de uma organização empresarial e facilitar os testes e validações.

Firewall / Router – pfSense

A firewall pfSense (versão 2.7.2) foi utilizada como elemento central da infraestrutura de rede. Este equipamento desempenha simultaneamente as funções de router, firewall e gateway entre os diferentes segmentos da rede.

O pfSense encontra-se configurado com várias interfaces de rede, associadas à LAN, DMZ e Outside, sendo responsável por:

- **Encaminhar o tráfego entre redes;**
- **Aplicar regras de firewall e controlo de acessos;**
- **Garantir a separação e segurança entre os diferentes segmentos.**

A sua utilização permitiu implementar políticas de segurança realistas, aproximando o projeto de um ambiente profissional.

Servidor Windows – Windows Server 2022

Foi utilizado um Windows Server 2022, designado como DC1, localizado na rede interna (LAN), com as seguintes funções:

- **Domain Controller (Active Directory);**
- **Servidor DNS;**
- **Servidor DHCP.**

Este servidor é responsável pela gestão centralizada de utilizadores, computadores e autenticação no domínio paca. cloud.
O serviço DHCP permite a atribuição automática de endereços IP aos clientes internos, enquanto o DNS garante a correta resolução de nomes dentro da infraestrutura.

Servidor Linux – Ubuntu Server (DMZ)

Na zona desmilitarizada (DMZ) foi instalado um Ubuntu Server, com endereço IP estático, responsável pela disponibilização dos serviços acessíveis ao exterior.

Neste servidor foram configurados:

- **Servidor Web (Apache);**
- **Servidor de Email (Mailcow, utilizando Docker);**
- **Servidor FTP;**
- **Serviço SSH para administração remota segura.**

Este equipamento assume um papel crítico no projeto, sendo isolado da rede interna por razões de segurança, de forma a reduzir o impacto de possíveis acessos não autorizados.

Clientes Windows e Linux

Para testes e validação da infraestrutura foram utilizados vários sistemas cliente:

- **Cliente Windows 10**
  Utilizado para testar a integração no domínio, autenticação de utilizadores e acesso aos serviços internos.
- **Cliente Linux Mint (LAN)**
  Integrado no domínio Windows, permitindo validar a interoperabilidade entre sistemas Linux e Active Directory.
- **Cliente Linux Mint (Outside)**
  Utilizado para simular acessos externos à infraestrutura, testando o acesso aos serviços web e de email, bem como o comportamento das regras de firewall.

A utilização destes equipamentos permitiu validar o correto funcionamento da infraestrutura, testar diferentes cenários de acesso e garantir que os serviços implementados respondem conforme o planeado, tanto a nível funcional como de segurança.

Configuração da PFSense

A Firewall pfSense foi o componente central da infraestrutura do projeto Paca Cloud, sendo responsável pelo encaminhamento do tráfego, separação de redes e aplicação das políticas de segurança entre os diferentes segmentos da rede.

A sua configuração foi realizada após o planeamento da rede, garantindo que cada interface estivesse corretamente associada à respetiva sub-rede e que apenas o tráfego autorizado fosse permitido.

Configuração das Interfaces

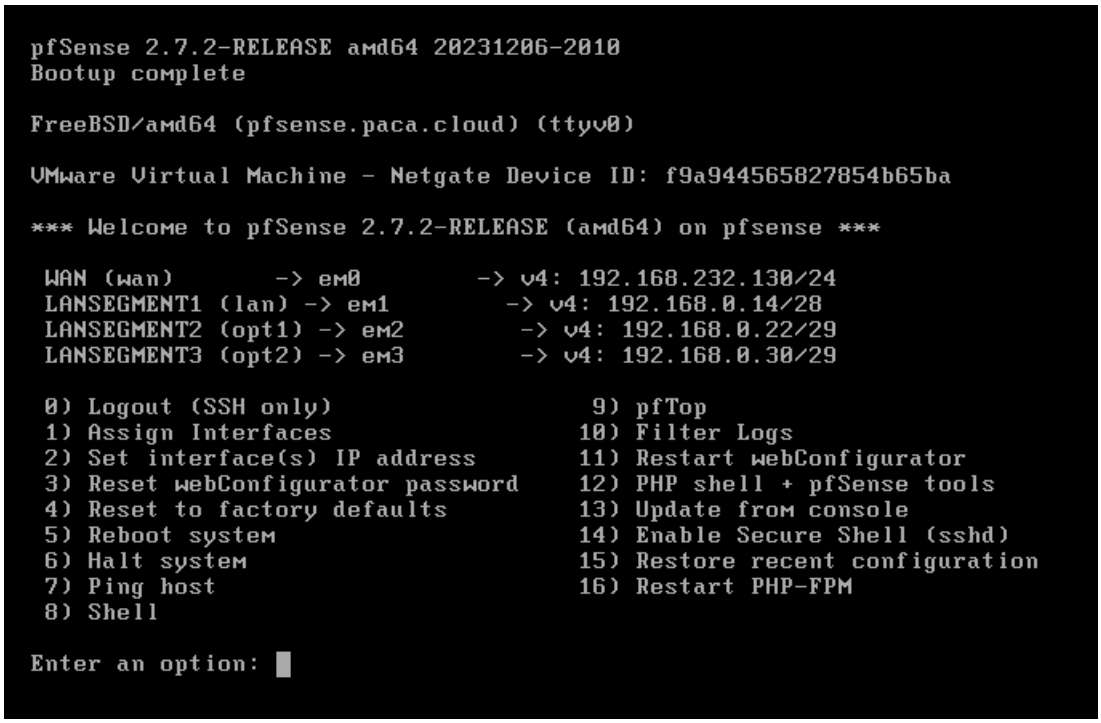

Figura 3 - Interfaces da PFSense

O pfSense foi configurado com múltiplas interfaces de rede, cada uma associada a um segmento específico da infraestrutura:

LAN (LANSEGMENT1)

- **Endereço IP:** 192.168.0.14/28

DMZ (LANSEGMENT2 / OPT1)

- **Endereço IP:** 192.168.0.22/29

Outside (LANSEGMENT3 / OPT2)

- **Endereço IP:** 192.168.0.30/29

Encaminhamento e Função de Gateway

O pfSense foi configurado para funcionar como gateway padrão para todos os dispositivos das diferentes redes. Desta forma:

- Os clientes da LAN utilizam o pfSense para aceder à DMZ e à rede Outside;
- Os serviços da DMZ comunicam com outras redes apenas através das regras definidas;
- A rede Outside não possui acesso direto à rede interna.

Esta abordagem garante que todo o tráfego inter-redes passa obrigatoriamente pela firewall, permitindo controlo total da comunicação.

Regras de Firewall

Figura 4- Aliases das Ports

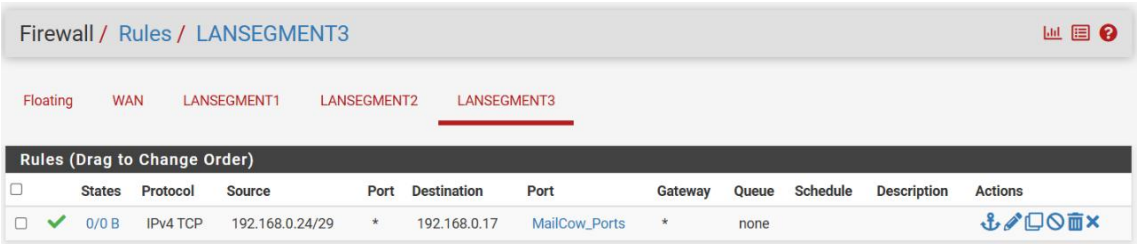

Figura 5 - Firewall Rules

Foram definidas regras de firewall específicas para controlar o tráfego entre os diferentes segmentos da rede, seguindo o princípio do menor privilégio.

LAN -> DMZ

- Permissão de acesso aos serviços da DMZ;
- Utilizado para administração, testes e manutenção dos serviços.

LAN -> Outside

- Tráfego permitido conforme necessário;
- Utilizado para simular acesso externo a partir da rede interna.

Outside -> DMZ

- Apenas permitidos os serviços essenciais, nomeadamente:
    - HTTP / HTTPS (Web)
    - Serviços de Email (SMTP, Submission, IMAPS)
- Outras portas permanecem bloqueadas.

Outside -> LAN

- Totalmente bloqueado, impedindo acessos diretos à rede interna.

DMZ -> LAN

- Tráfego restrito ao estritamente necessário;
- Apenas respostas a pedidos iniciados pela LAN são permitidas.

Testes de Segurança e Validação

Para validar a correta aplicação das regras de firewall, foram realizados testes a partir da rede Outside, utilizando ferramentas de análise de portas, como o Nmap. Estes testes permitiram confirmar que:

- Apenas as portas de serviços públicos se encontravam acessíveis;
- A porta de administração SSH não estava exposta externamente;
- A rede interna permanecia protegida contra acessos não autorizados.

Os resultados obtidos confirmaram que as regras de firewall estavam corretamente implementadas e que a segmentação da rede funcionava conforme o planeado.

A configuração do pfSense revelou-se essencial para garantir uma infraestrutura segura, organizada e funcional, permitindo a disponibilização controlada de serviços ao exterior sem comprometer a segurança da rede interna.

Configuração da Rede Interna (LAN)

A rede interna (LAN) constitui o núcleo da infraestrutura do projeto Paca Cloud, sendo responsável pela gestão de utilizadores, autenticação, resolução de nomes e atribuição de endereços IP.

Configuração de Rede

A LAN utiliza o endereçamento 192.168.0.0/28, estando associada à interface LAN do pfSense, que atua como gateway padrão para todos os equipamentos internos, com o endereço 192.168.0.14.

Todos os dispositivos da rede interna comunicam entre si através deste segmento e recorrem ao pfSense para aceder a outras redes, nomeadamente à DMZ e à rede Outside, sempre de acordo com as regras de firewall definidas.

Active Directory e Domain Controller

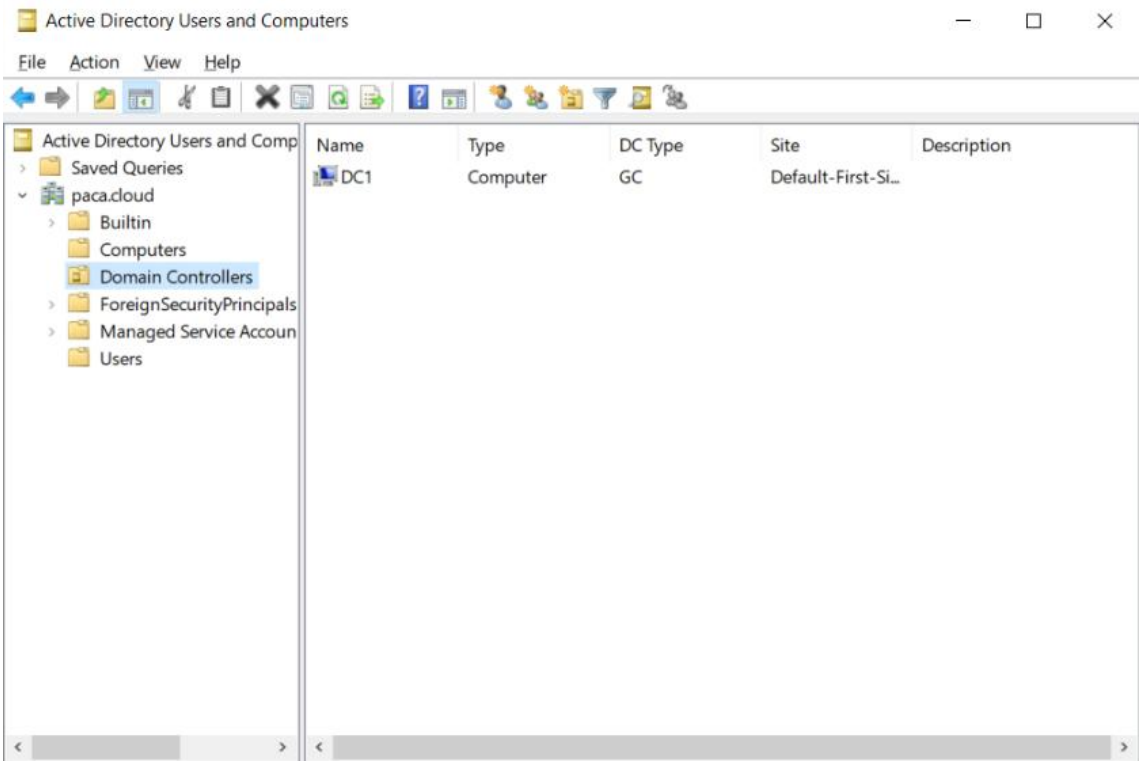

Figura 6 - DC1

Na rede interna foi instalado um Windows Server 2022, configurado como Domain Controller (DC1), responsável pela gestão centralizada do domínio paca.cloud.

O Active Directory permite:

- Criar e gerir utilizadores e grupos;
- Controlar permissões e políticas de segurança;
- Centralizar a autenticação dos sistemas Windows e Linux integrados no domínio.

Esta configuração facilita a administração da infraestrutura e aproxima o projeto de um cenário empresarial real.

Serviço DNS

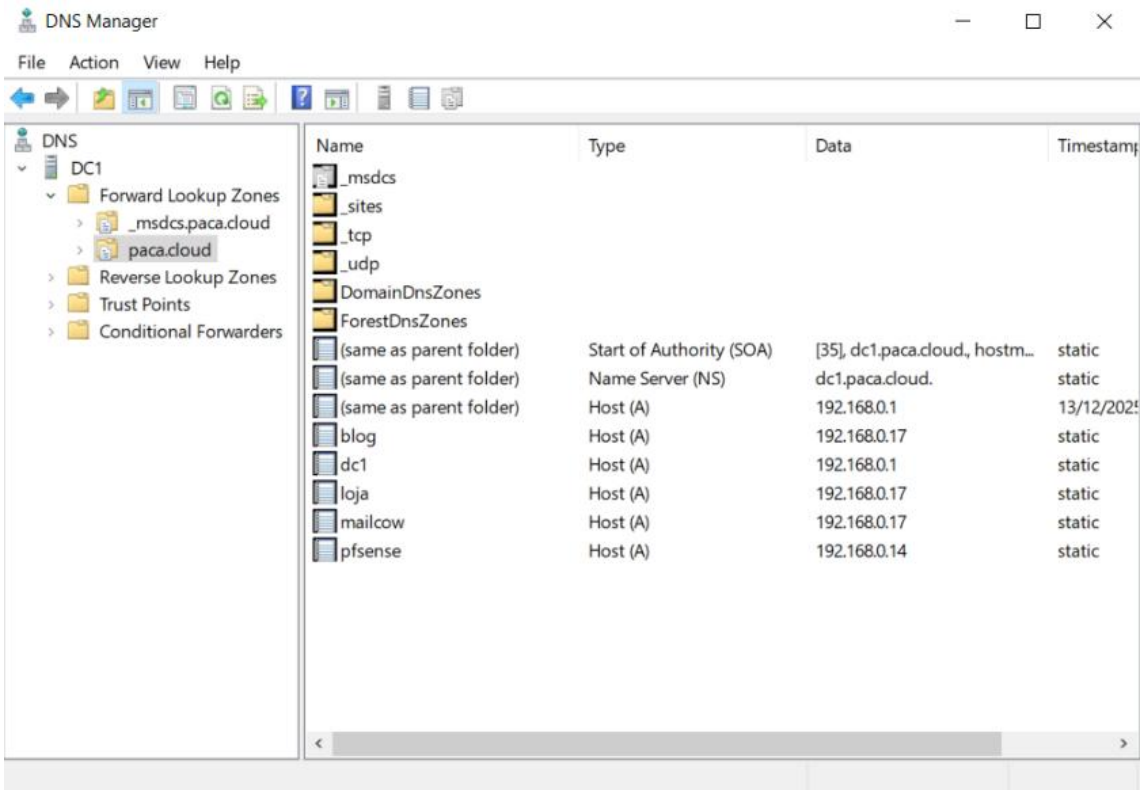

Figura 7 - DNS

O servidor Windows desempenha também a função de servidor DNS, sendo responsável pela resolução de nomes dentro do domínio paca.cloud.

O DNS interno permite:

- Resolver nomes de máquinas e serviços da rede;
- Garantir o correto funcionamento do Active Directory;
- Facilitar o acesso aos serviços através de nomes de domínio, em vez de endereços IP.

Serviço DHCP

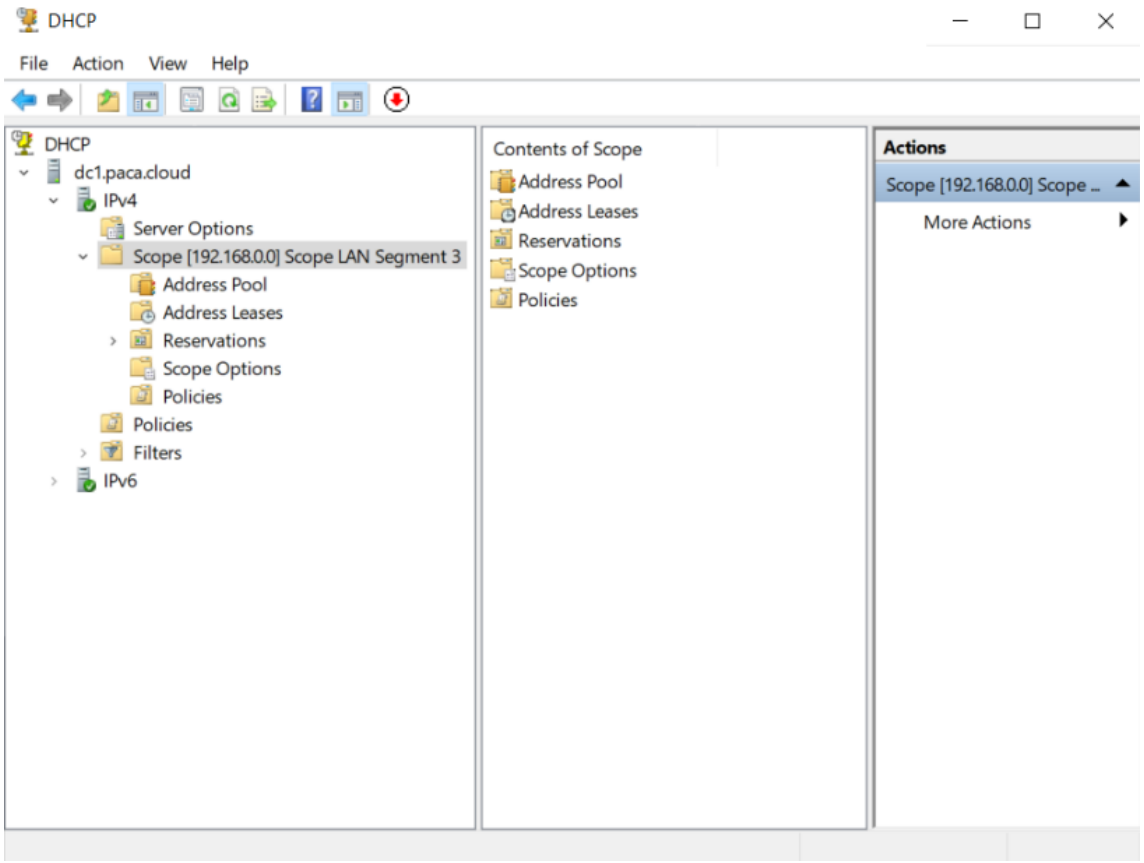

Figura 8 - DHCP

O serviço DHCP foi configurado no Windows Server 2022 para automatizar a atribuição de endereços IP aos clientes da rede interna.

As principais configurações do DHCP são:

- **Scope:** 192.168.0.6 a 192.168.0.13
- **Gateway:** 192.168.0.14 (pfSense)
- **DNS:** Endereço IP do Domain Controller

Esta abordagem permite reduzir erros de configuração manual, facilitar a gestão da rede e garantir que todos os clientes recebem parâmetros de rede corretos.

Configuração do DMZ

A DMZ foi configurada com o objetivo de alojar os serviços acessíveis a partir da rede externa, garantindo simultaneamente a proteção da rede interna. Esta abordagem permite expor serviços públicos sem comprometer os sistemas críticos da organização.

A DMZ encontra-se associada à sub-rede 192.168.0.16/29 e é interligada às restantes redes através da firewall pfSense, que controla todo o tráfego de entrada e saída.

Configuração de Rede do Servidor DMZ

Na DMZ foi instalado um Ubuntu Server, configurado com endereço IP estático, de forma a garantir estabilidade no acesso aos serviços e facilitar a aplicação das regras de firewall e dos certificados SSL.

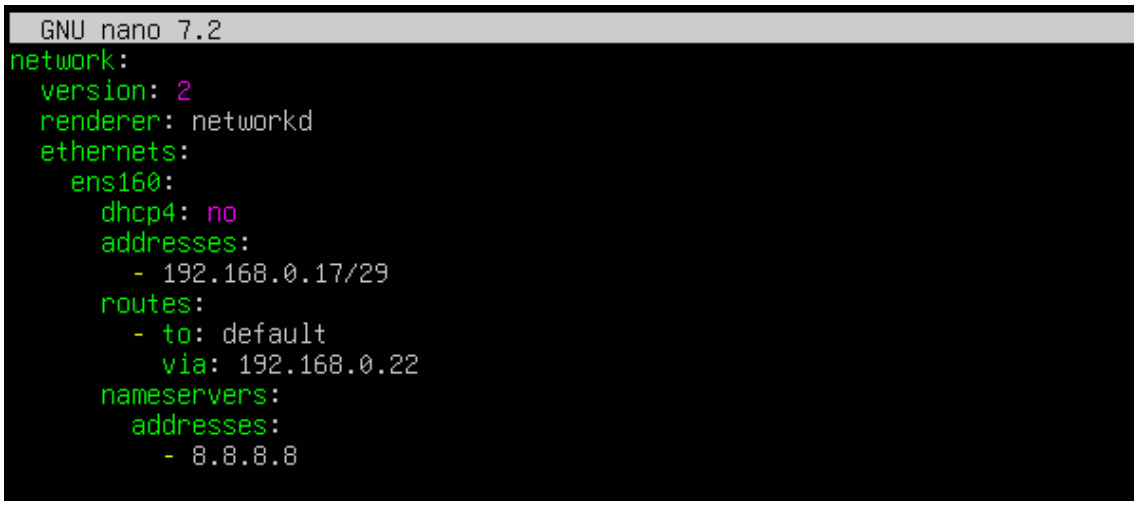

Figura 9 - Netplan do Ubuntu Server

Configuração principal:

- **Sistema Operativo:** Ubuntu Server
- **Endereço IP:** 192.168.0.17
- **Máscara:** 255.255.255.248 (/29)
- **Gateway:** 192.168.0.22 (pfSense)
- **DNS:** Servidor Windows (DC1)

A utilização de IP estático é essencial neste tipo de servidor, uma vez que os serviços públicos dependem de um endereço fixo para funcionamento correto.

Serviços Disponibilizados na DMZ

O servidor Ubuntu na DMZ foi responsável pela disponibilização de vários serviços críticos, todos acessíveis de forma controlada a partir da rede externa.

Os serviços implementados foram:

- **Servidor Web**, responsável pelo alojamento de websites e interfaces web dos serviços, através do uso de um Script;
- **Servidor de Email**, utilizando a plataforma **Mailcow**, executada em contentores Docker, através do uso de um Script;
- **Servidor FTP**, para transferência de ficheiros, através do uso de um Script;
- **Serviço SSH**, utilizado para administração remota segura do servidor, através do uso de um Script.

Todos estes serviços foram configurados tendo em conta as regras de firewall definidas no pfSense, garantindo que apenas as portas estritamente necessárias se encontram acessíveis a partir da rede Outside.

Utilização de Docker no Servidor DMZ

Para a implementação do serviço de email foi utilizada a tecnologia Docker, que permite isolar os diferentes componentes do Mailcow em contentores independentes.

A utilização de Docker trouxe várias vantagens:

- Melhor organização dos serviços;
- Facilidade de manutenção e atualização;
- Isolamento entre aplicações;
- Maior estabilidade do sistema.

Os contentores foram geridos através do Docker Compose, permitindo iniciar, parar e monitorizar os serviços de forma centralizada.

Segurança da DMZ

A segurança da DMZ foi uma preocupação constante ao longo do projeto. Para tal, foram adotadas as seguintes medidas:

- Isolamento total da DMZ em relação à rede interna;
- Acesso controlado através de regras de firewall;
- Exposição apenas das portas necessárias aos serviços públicos;
- Utilização de certificados SSL para cifrar as comunicações;
- Restrição do acesso SSH a redes específicas.

Estas medidas garantem que, mesmo em caso de comprometimento de um serviço da DMZ, o impacto na restante infraestrutura é minimizado.

A correta configuração da DMZ permitiu disponibilizar serviços ao exterior de forma segura, organizada e controlada, mantendo a integridade e a proteção da rede interna, cumprindo assim um dos principais objetivos do projeto.

Configuração dos Serviços no Servidor Linux

O servidor Ubuntu Server, localizado na DMZ, foi configurado para disponibilizar vários serviços essenciais acessíveis a partir da rede externa, mantendo sempre elevados níveis de segurança e controlo. Este servidor assume um papel central na infraestrutura, concentrando os serviços de web, email, transferência de ficheiros e administração remota.

Servidor Web

O Apache foi utilizado como servidor web principal, sendo responsável pelo alojamento de diferentes serviços e aplicações web. No servidor foram configurados vários Virtual Hosts, permitindo a coexistência de múltiplos sites e serviços no mesmo sistema.

Entre os serviços alojados destacam-se:

- **WordPress**, utilizado como plataforma de gestão de conteúdos;
- **PrestaShop**, utilizado como loja online;
- Interface web de acesso aos serviços associados.

Cada serviço encontra-se associado ao respetivo nome de domínio, facilitando o acesso e a gestão dos conteúdos.

Servidor de Email (Mailcow)

O serviço de correio eletrónico foi implementado através da plataforma Mailcow, recorrendo a Docker para a gestão dos diferentes componentes do sistema de email.

A instalação do Mailcow envolveu:

- Preparação do sistema e resolução de conflitos de portas;
- Instalação do Docker e Docker Compose;
- Clonagem do repositório oficial do Mailcow;
- Geração do ficheiro de configuração com definição do domínio;
- Inicialização e monitorização dos contentores.

A utilização de contentores permitiu isolar os serviços de email, garantindo maior estabilidade, facilidade de manutenção e organização do sistema.

Reverse Proxy

De forma a permitir a coexistência do servidor web e do Mailcow no mesmo sistema, foi implementado um reverse proxy com Apache.

Nesta configuração:

- O Mailcow opera em portas internas alternativas;
- O Apache recebe os pedidos externos nas portas 80 e 443;
- O tráfego é redirecionado internamente para os serviços corretos com base no domínio solicitado.

Esta abordagem permitiu centralizar a gestão do tráfego web e simplificar a exposição dos serviços ao exterior.

Certificados SSL e Segurança HTTPS

Para garantir a segurança das comunicações, foram implementados certificados SSL assinados por uma Autoridade de Certificação (CA) interna, criada no Windows Server.

Os certificados foram gerados com suporte para Subject Alternative Name (SAN), garantindo compatibilidade com browsers modernos. Cada serviço web utiliza o seu próprio certificado, corretamente configurado nos Virtual Hosts do Apache.

Adicionalmente, foi configurado o redirecionamento automático de HTTP para HTTPS, assegurando que todas as comunicações são cifradas.

Servidor FTP

O servidor FTP foi configurado para permitir a transferência controlada de ficheiros, sendo utilizado principalmente para fins administrativos e de manutenção.

As principais medidas aplicadas incluem:

- Acesso restrito a utilizadores autorizados;
- Separação de permissões de leitura e escrita;
- Integração com as regras de firewall, limitando o acesso externo.

Serviço SSH

O serviço SSH foi configurado para permitir a administração remota segura do servidor Linux.

As principais medidas de segurança adotadas foram:

- Restrição do acesso SSH a redes específicas;
- Controlo das portas expostas externamente;
- Utilização do SSH apenas para tarefas administrativas.

A correta configuração dos serviços no servidor Linux permitiu disponibilizar uma solução funcional, segura e organizada, garantindo o acesso controlado aos serviços públicos e mantendo a integridade da infraestrutura interna.

Políticas de Segurança Implementadas

A segurança foi um dos aspetos centrais do projeto Paca Cloud, tendo sido adotadas várias políticas e medidas de proteção ao longo de toda a infraestrutura, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos sistemas e serviços.

Estas políticas foram aplicadas a diferentes níveis: rede, sistemas, serviços e comunicações, seguindo boas práticas de segurança em ambientes empresariais.

Segmentação da Rede

A principal política de segurança implementada foi a segmentação da rede, através da separação em três zonas distintas:

- **LAN** – rede interna e protegida;
- **DMZ** – serviços expostos ao exterior;
- **Outside** – simulação de rede externa.

Esta separação impede acessos diretos da rede externa à rede interna, reduzindo significativamente o impacto de eventuais ataques ou compromissos de serviços públicos.

Regras de Firewall e Controlo de Acessos

A firewall pfSense foi configurada segundo o princípio do menor privilégio, permitindo apenas o tráfego estritamente necessário entre as diferentes redes.

Foram implementadas as seguintes políticas:

- Bloqueio total de acessos da Outside para a LAN;
- Permissão apenas das portas essenciais da Outside para a DMZ (Web e Email);
- Restrição do acesso SSH, não expondo a porta de administração externamente;
- Controlo rigoroso do tráfego entre LAN e DMZ.

Estas regras garantem que apenas os serviços públicos ficam acessíveis externamente, mantendo a rede interna protegida.

Segurança dos Serviços Web

Os serviços web foram protegidos através da utilização de certificados SSL, garantindo comunicações cifradas via HTTPS.

As principais medidas aplicadas foram:

- Implementação de certificados assinados por uma Autoridade de Certificação interna;
- Utilização de certificados com Subject Alternative Name (SAN);
- Redirecionamento automático de HTTP para HTTPS;
- Correção de conteúdos mistos em aplicações como WordPress e PrestaShop.

Estas medidas evitam alertas de segurança nos browsers e protegem os dados trocados entre clientes e servidores.

Segurança do Serviço de Email

O serviço de email, implementado com Mailcow, foi configurado com foco na segurança e isolamento:

- Execução dos serviços em contentores Docker, isolando-os do sistema base;
- Exposição apenas das portas necessárias ao funcionamento do email;
- Utilização de certificados SSL para serviços SMTP, IMAP e Webmail;
- Monitorização do estado dos contentores.

Esta abordagem reduz a superfície de ataque e facilita a gestão segura do serviço.

Segurança no Acesso Remoto

O acesso remoto ao servidor Linux foi efetuado exclusivamente através de SSH, com as seguintes medidas:

- Restrição do acesso a redes específicas;
- Não exposição da porta SSH à rede externa;
- Utilização do SSH apenas para administração.

Estas medidas reduzem o risco de acessos não autorizados ao sistema.

Testes de Segurança

Para validar as políticas de segurança implementadas, foram realizados testes a partir da rede Outside, recorrendo à ferramenta Nmap.

Estes testes permitiram confirmar que:

- Apenas as portas dos serviços públicos se encontravam acessíveis;
- A porta SSH não estava exposta externamente;
- A rede interna permanecia inacessível a partir da rede externa.

Os resultados obtidos demonstraram que as políticas de segurança estavam corretamente aplicadas e funcionais.

As políticas de segurança implementadas permitiram criar uma infraestrutura robusta, organizada e segura, garantindo a proteção dos sistemas internos e a disponibilização controlada dos serviços ao exterior, cumprindo os objetivos definidos para o projeto.

Testes e Validação do Projeto

Após a implementação de toda a infraestrutura, foram realizados vários testes de funcionamento e segurança, com o objetivo de validar se a solução desenvolvida cumpria os requisitos definidos e se todos os serviços operavam corretamente nos diferentes cenários de acesso.

Os testes foram efetuados a partir das três zonas da rede (LAN, DMZ e Outside), permitindo verificar a comunicação entre redes, o acesso aos serviços e a eficácia das regras de segurança implementadas.

Testes de Conectividade

Foram realizados testes de conectividade básica para validar a comunicação entre os diferentes equipamentos e segmentos da rede, recorrendo a comandos como ping e verificação de resolução de nomes.

Estes testes permitiram confirmar que:

- Os dispositivos da LAN comunicam corretamente entre si;
- Existe conectividade entre a LAN e a DMZ, de acordo com as regras definidas;
- A resolução de nomes DNS funciona corretamente dentro do domínio paca.cloud;
- A comunicação entre redes ocorre sempre através da firewall pfSense.

Testes aos Serviços

Foram realizados testes específicos a cada serviço configurado no servidor Linux da DMZ:

- **Servidor Web**
  Foi testado o acesso aos websites (WordPress, PrestaShop e serviços associados) a partir da rede interna e da rede externa, confirmando o correto carregamento das páginas através de HTTPS.
- **Servidor de Email**
  Foi validado o acesso ao webmail do Mailcow, bem como o funcionamento dos serviços SMTP e IMAP, confirmando o envio e receção de mensagens.
- **Servidor FTP**
  Foram realizados testes de autenticação e transferência de ficheiros, validando as permissões de leitura e escrita configuradas.
- **Serviço SSH**
  Foi testado o acesso SSH a partir das redes autorizadas, confirmando que o serviço se encontra funcional e devidamente protegido.

Testes de Segurança

Para validar as políticas de segurança e as regras de firewall implementadas, foram realizados testes a partir da rede Outside, utilizando a ferramenta Nmap para análise de portas.

Estes testes permitiram verificar que:

- Apenas as portas dos serviços públicos se encontram acessíveis a partir do exterior;
- A porta de administração SSH não está exposta externamente;
- A rede interna não é acessível a partir da rede Outside;
- As regras de firewall do pfSense estão corretamente aplicadas.

Adicionalmente, foi confirmada a correta utilização de **certificados SSL**, não sendo apresentados avisos de segurança nos browsers ao aceder aos serviços web.

Resultados Obtidos

Os testes realizados demonstraram que:

- A infraestrutura funciona de forma estável e consistente;
- Os serviços estão corretamente configurados e acessíveis apenas quando autorizado;
- As políticas de segurança implementadas são eficazes;
- A segmentação da rede cumpre o seu objetivo de proteção da rede interna.

Desta forma, pode-se concluir que o projeto foi validado com sucesso, cumprindo os objetivos definidos e apresentando um comportamento adequado em termos de funcionamento e segurança.

Teste de Email

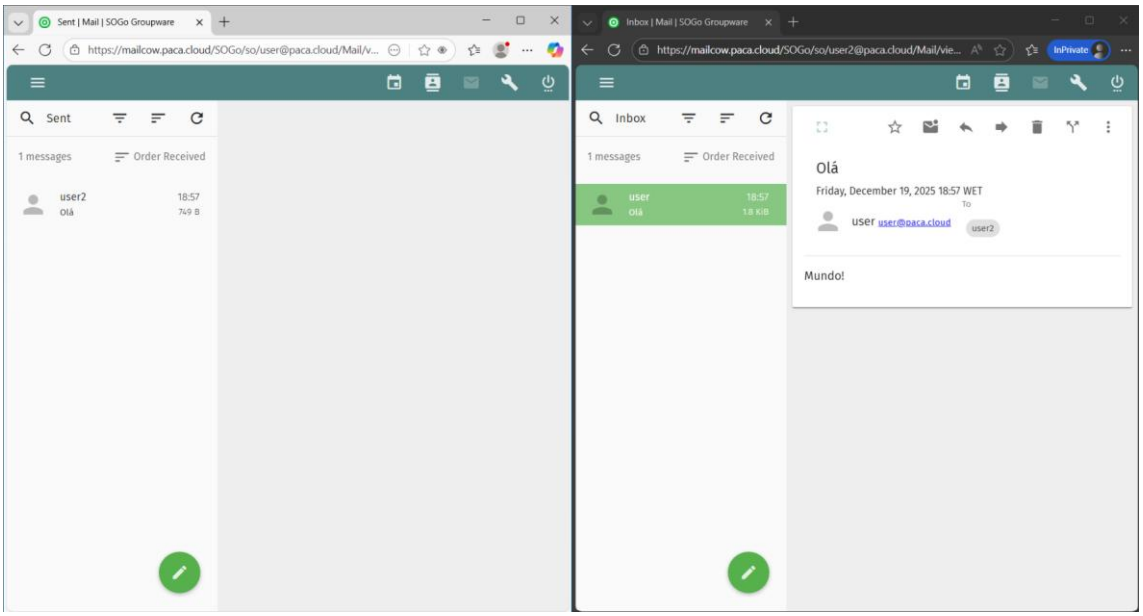

Figura 10 - Teste de Email

Como visto, ambos os *users* conseguem comunicar um com o outro.

Web

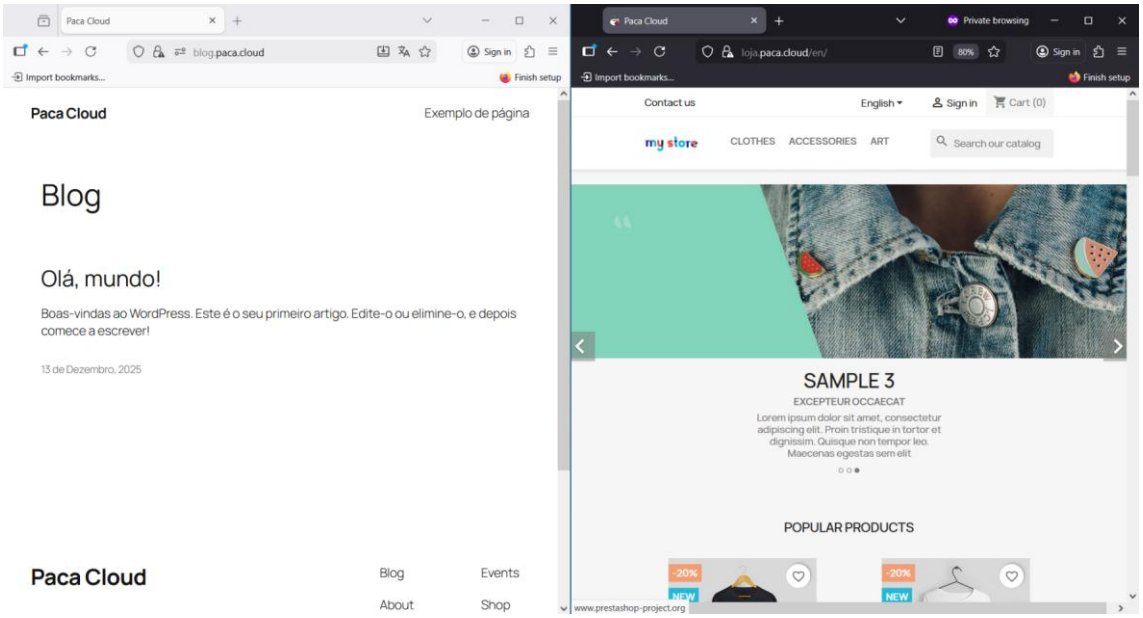

Figura 11- Teste de Web

Como visto, temos ambas as CMS configurada e funcionais.

Teste de FTP

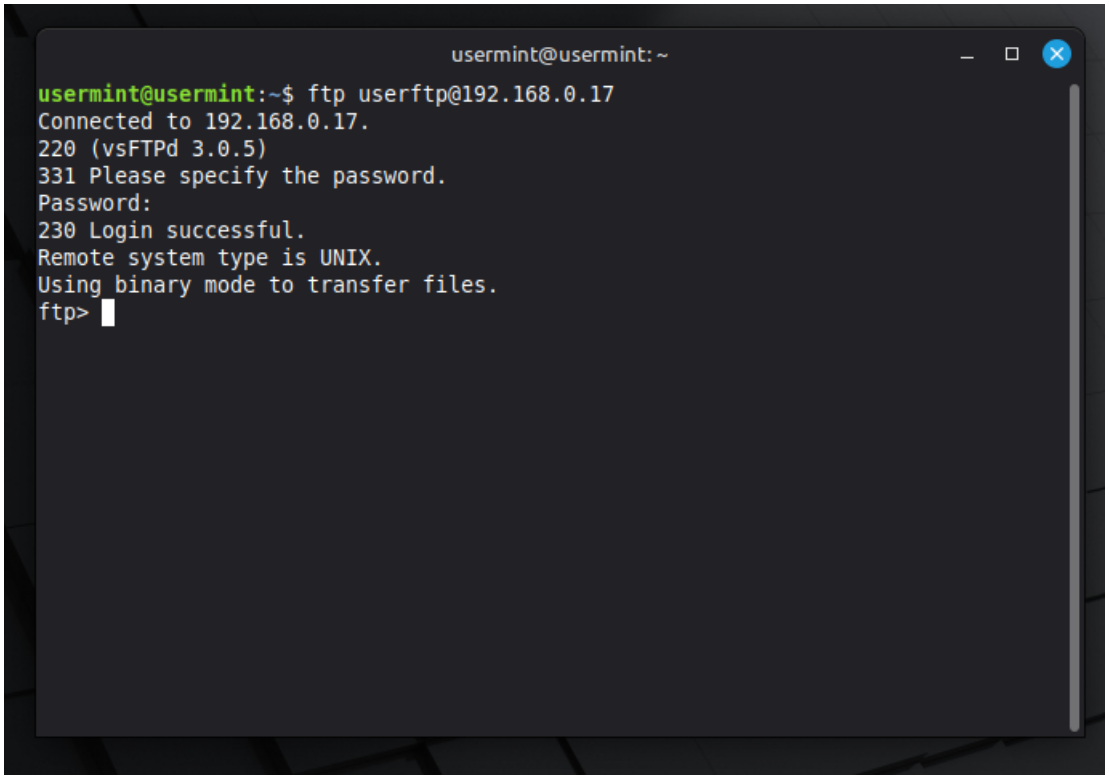

Figura 12 - Teste de FTP

Confirmação de FTP com sucesso, a partir do Mint presente na nossa LAN Segment 3.

Teste de SSH

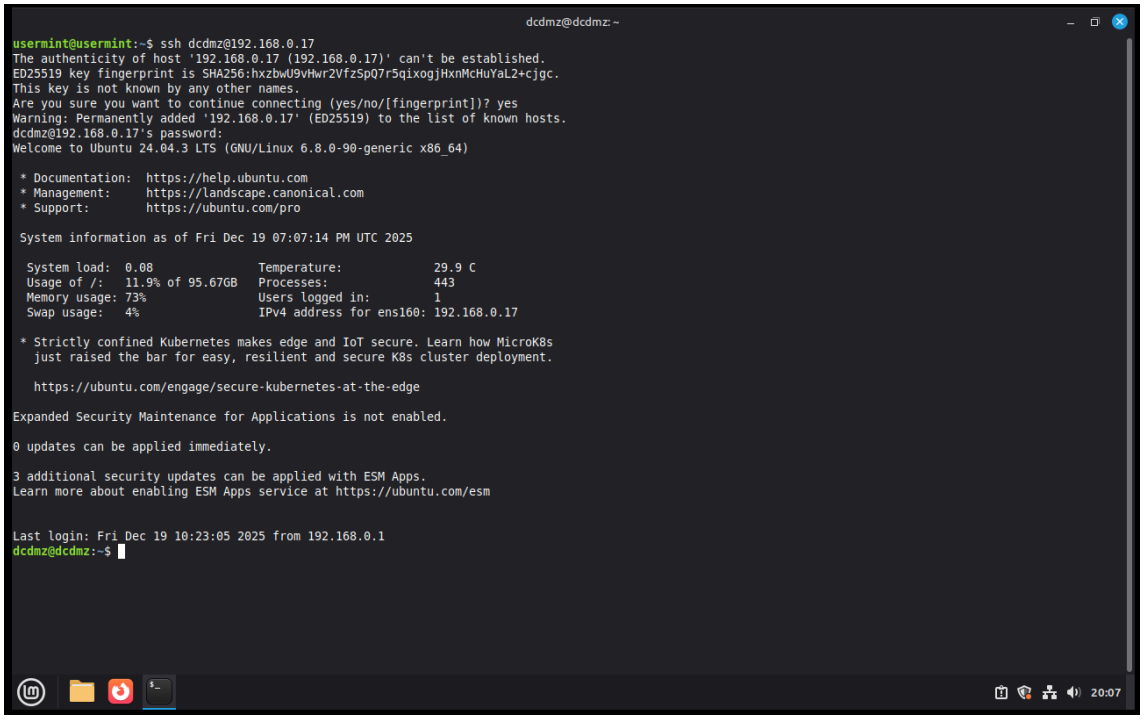

Figura 13 - Teste de SSH

Teste realizado com sucesso, como visto no *print*, a partir do Mint presente na nossa LAN Segment 3.

Dificuldades Encontradas

Uma das principais dificuldades surgiu na instalação do Mailcow, devido a conflitos de portas com serviços já existentes no sistema, nomeadamente o Apache a utilizar as portas 80 e 443. Esta situação foi resolvida através da reconfiguração do Mailcow para portas internas alternativas e da utilização de um reverse proxy.

Foram também encontradas dificuldades na configuração da firewall pfSense, onde um erro na definição das portas inicialmente impediu o acesso a alguns serviços a partir da rede externa. Após correção das regras e realização de testes, o problema foi resolvido.

Adicionalmente, a configuração dos certificados SSL apresentou alguns desafios, relacionados com erros de validação nos browsers, que foram solucionados através da correta geração de certificados com suporte para Subject Alternative Name (SAN).

Apesar destas dificuldades, todas foram ultrapassadas com sucesso, contribuindo para uma melhor compreensão prática dos conceitos de redes, segurança e administração de sistemas.

Conclusão

Com a realização do projeto Paca Cloud, foi possível implementar com sucesso uma infraestrutura de rede e serviços completa, funcional e segura, cumprindo os objetivos definidos no âmbito da unidade curricular IGRI18.

Ao longo do projeto foram aplicados conhecimentos práticos de planeamento de redes, segmentação em LAN, DMZ e Outside, configuração de firewalls, bem como administração de sistemas Windows e Linux. A utilização da firewall pfSense permitiu garantir um controlo rigoroso do tráfego entre redes, protegendo a rede interna e assegurando a disponibilização controlada de serviços ao exterior.

A configuração do Windows Server 2022 como Domain Controller possibilitou a gestão centralizada de utilizadores, DNS e DHCP, enquanto o servidor Ubuntu Server, localizado na DMZ, permitiu a implementação de serviços essenciais como Web, Email, FTP e SSH. A utilização de tecnologias modernas, como Docker para o Mailcow e reverse proxy com Apache, contribuiu para uma infraestrutura mais organizada, escalável e próxima de um cenário real.

Foi também dada especial atenção à segurança, através da implementação de certificados SSL assinados por uma Autoridade de Certificação interna, da aplicação de políticas de firewall restritivas e da realização de testes de segurança com ferramentas de análise de portas. Os testes realizados demonstraram que a infraestrutura funciona corretamente, garantindo tanto a funcionalidade dos serviços como a proteção da rede interna.

Em suma, o projeto permitiu consolidar conhecimentos teóricos e práticos nas áreas de redes, sistemas, segurança e serviços, proporcionando uma experiência realista e relevante para a futura integração em contextos profissionais. Os resultados obtidos comprovam o sucesso da implementação e a adequação das soluções adotadas.

Acessos

Wordpress

URL (Admin): https://blog.paca.cloud/wp-admin (Mint – Browser: Firefox)

User: sergioc@paca.cloud

Password: Formacao2025

Prestashop

URL (Admin): https://loja.paca.cloud/admin2734dqrdxwv1i8bu51g

User: sergioc@paca.cloud

Password: Formacao2025

Mint (User)

User: usermint

Password: 1234

Outside Mint

User: usermint

Password: 1234

DC

User: PACA@Administrator

Password: Formacao2025

DMZ

User: dcdmz

Password: 1234

PFSense

User: Admin

Password: Formacao2025

MailCow (Admin)

URL (Admin): https://mailcow/admin (Mint – Browser: Firefox)

User: admin

Password: moohoo