UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Segurança de Tecnologias de Informação: Proposta de implementação de Firewall e Gestão Centralizada de Utilizadores

Caso de estudo:

Universidade Eduardo Mondlane – Faculdade de Engenharia

Autor:

Cossa, Luís António

Supervisor:

Engº Délcio Arnaldo Chadreca

Supervisor na FE:

dr. Xavier Mahumane

Maputo, _____ de 2025

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Segurança de Tecnologias de Informação: Proposta de implementação de Firewall e Gestão Centralizada de Utilizadores

Caso de estudo:

Bloco administrativo da Faculdade de Engenharia da UEM

Autor:

Cossa, Luís António

Supervisor:

_____

Engº Délcio Arnaldo Chadreca, Msc

Supervisor na FE:

_____

dr. Xavier Mahumane

Maputo, _____ de 2025

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

TERMO DE ENTREGA DE RELATÓRIO DO ESTÁGIO PROFISSIONAL

Declaro que o estudante **Luís António Cossa** entregou no dia __/__/2025, às 03 cópias do seu relatório de Estágio Profissional com referência _____, intitulado: Segurança de Tecnologias de Informação: Proposta de implementação de Firewall e Gestão Centralizada de Utilizadores. Caso de Estudo: Bloco Administrativo da Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, __ de _____ de 2025

A chefe da secretaria do DEEL

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, __ de _____ de 2025

O Autor

_____

(Luís António Cossa)

Dedicatória

A todos os que sempre me apoiaram, inspiraram e acreditaram em mim – especialmente aos meus pais, António João Cossa (in memoriam) e Aurora Atanázio Maquenhane – a minha eterna gratidão.

Agradecimentos

Em primeiro lugar agradeço a Deus pela vida, saúde e por ter guiado cada passo da minha trajectória.

Ao meu pai (in memoriam), pela educação e valores que me transmitiu desde tenra idade. Foi e continua a ser o meu modelo de homem íntegro, tendo ensinado-me a enfrentar os desafios da vida com inteligência e dignidade.

À minha mãe, por ser um exemplo de força e por ter contribuído decisivamente para a formação de um homem capaz de enfrentar a vida com autonomia e coragem.

Aos meus segundos pais, Belmote Cossa e Suzália Nhantumbo Cossa, expresso profunda gratidão pelo acolhimento, apoio incondicional e carinho com que sempre me trataram. Graças a vós, nunca precisei de recorrer aos meus pais biológicos para suprir necessidades, mesmo após a minha vinda para Maputo.

Aos meus irmãos Simião, Miguel, Carlos, Atanásio, Isabel, Equinessa, Cristina, João, Eldivanda e Célia Cossa, e à mamã Rute Mavale agradeço pelo exemplo, pelos conselhos e por serem fonte de inspiração constante no meu percurso pessoal e académico.

Ao meu primo e amigo, Emmanuel Muthisse, agradeço pelas partilhas, pelos momentos únicos, pelo incentivo moral e pelo apoio financeiro em momentos cruciais.

Um agradecimento especial ao meu tio Paulo Muthisse, pelas oportunidades profissionais que me tem garantido estabilidade e crescimento, bem como pelas palavras motivadoras sempre que conversamos.

À minha família no seu todo, o meu sincero reconhecimento por serem a minha base, por contribuírem para a minha formação intelectual e humana, e por serem fonte de referências profissionais que me inspiram.

À minha namorada e noiva, a Cátia Ngonhamo, agradeço pela presença constante, pelo amor e por ter estado ao meu lado nos bons e maus momentos.

Aos meus amigos de longa data, Arlindo Pires, Nelson Cossa, Frenk Mundlovo, Raúl Mondlane e Jónia Zandamela agradeço pela amizade sólida e duradoura.

A todos os meus colegas de formação, em particular ao Edson Tamele, Rafael Stoner, Carson Ribeiro, Heronilde Cossa, Alexandre Chavane, Cany Mangue, Domingos Machavane, e em especial a Moisés Maposse, Euclédio Miguel, Ivan Rufino, Gilvaldo Massunguine, Fortunato Jalane e Chaide Pardival agradeço pela amizade construída para além do espaço académico.

Ao corpo docente do curso de licenciatura em Engenharia Informática na Faculdade de Engenharia, o meu agradecimento pelo conhecimento transmitido e pelas metodologias que tornaram a aprendizagem acessível e significativa. Em particular, agradeço ao Engº. Ruben Manhiça, ao Mcs. Vali Issufo, à Engª. Ivone Cipriano, ao Engº. Felizardo Munguambe, ao Engº Albino Cuinhane e, de forma especial, à Engª. Leila Omar, pelo apoio na obtenção do estágio no DTIC.

Ao meu orientador de trabalho de conclusão de curso, o Engº. Délcio Chadreca, agradeço por despertar em mim o interesse pela área de telecomunicações, pela orientação na definição do tema deste trabalho e pela disponibilidade demonstrada ao longo de todo o processo.

Ao meu supervisor de estágio, dr. Xavier Mahumane, pelo acolhimento, pela confiança e por me disponibilizar todos os recursos necessários para o bom desempenho das actividades. Um agradecimento especial ao Sr. Nando e dr. Josué e dra. Cidália, colegas do DTIC, pela orientação prática, pela partilha de conhecimentos e pelo ambiente de camaradagem.

Ao meu superior hierárquico na Khurula&Rios Serviços, Sr. Mário Paulino Ofiço, agradeço pela compreensão, flexibilidade e amizade demonstradas, bem como pelo apoio nos momentos em que precisei conciliar o trabalho com as actividades académicas.

Por fim, agradeço a todos quantos, de forma directa ou indirecta, contribuíram para esta caminhada. A vossa presença e apoio foram determinantes, e sou eternamente grato por isso.

Epígrafe

“Aquele que se empenha a resolver dificuldades, resolve-as antes que elas surjam.”

Sun Tzu

Resumo

A implementação de redes corporativas seguras exige não apenas infraestrutura, mas também uma arquitetura lógica que permita gerir acessos de forma centralizada e controlada. A rede da FEUEM, embora funcional, apresentava fragilidades como ausência de segmentação lógica, gestão manual e descentralizada de acessos, e falta de mecanismos claros para separação de responsabilidades, sobretudo nas zonas administrativas e académicas, onde circulam dados críticos como registos académicos e documentos financeiros.

Este trabalho propõe a implementação de uma solução prática baseada em dois pilares principais: a segmentação da rede por zonas e funções através de VLANs geridas pelo firewall Sophos XGS, e a centralização da autenticação e permissões por meio do Active Directory Domain Services (AD DS) com aplicação de controle de acesso baseado em função (RBAC). A solução foi implementada em ambiente virtualizado com Windows Server 2019 e clientes Windows 10/7, com foco na criação de políticas de grupo (GPOs), partilhas de pastas, e regras de firewall orientadas a grupos de utilizadores autenticados.

A integração entre o Sophos e o AD DS permite não só a aplicação de políticas de acesso à Internet e aos recursos da rede de forma dinâmica, mas também a visibilidade e auditoria por utilizador. A metodologia baseou-se na construção de um ambiente laboratorial funcional, reproduzindo a realidade da FEUEM, com foco em reduzir o trabalho manual e aumentar a segurança lógica da rede sem aumentar custos.

O modelo demonstrou ser viável, escalável e adequado à realidade institucional, servindo de referência prática para outras instituições que desejem evoluir em maturidade de segurança com recursos limitados.

Palavras-chave: Segurança Cibernética, Active Directory Domain Services (AD DS), Controle de Acesso (RBAC), Segmentação de Rede (VLANs), Firewall Sophos XGS, Políticas de Grupo (GPOs), …

Abstract

The implementation of secure corporate networks requires not only physical infrastructure but also a logical architecture that enables centralized and controlled access management. Although functional, FEUEM's network presented several vulnerabilities, such as the lack of logical segmentation, manual and decentralized access management, and absence of clear mechanisms for role separation — especially in academic and administrative zones where critical data such as academic records and financial documents circulate.

This work proposes and implements a practical solution based on two main pillars: network segmentation by zones and roles using VLANs managed by the Sophos XGS firewall, and centralized authentication and permission control using Active Directory Domain Services (AD DS) with Role-Based Access Control (RBAC). The solution was deployed in a virtual lab environment with Windows Server 2019 and Windows 10/7 clients, focusing on the creation of Group Policy Objects (GPOs), shared folders, disk quotas, and firewall rules tied to authenticated user groups.

The integration between Sophos and AD DS enables the enforcement of Internet access policies and resource restrictions dynamically, with user-based visibility and auditing. The methodology involved building a fully functional lab environment that reproduces FEUEM's scenario, aiming to reduce manual administrative tasks while improving logical network security without increasing costs.

The model proved to be viable, scalable, and suitable for institutional realities, serving as a practical reference for other organizations seeking to enhance their security maturity with limited resources.

Keywords: Cybersecurity, Active Directory Domain Services (AD DS), Access Control (RBAC), Network Segmentation (VLANs), Sophos XGS Firewall, Group Policy Objects (GPOs).

ÍNDICE

Lista de figuras

Lista de tabelas

Lista de abreviaturas e acrónimos

TI – Tecnologias de Informação

FE – Faculdade de Engenharia

UEM – Universidade Eduardo Mondlane

QoS – Quality of Service

RGPD – Regulamento Geral sobre Proteção de Dados

RBAC – Role-Based Access Control

LGPD – Lei Geral de Proteção de Dados

TCO – Total Cost Ownership

LDAP – Lightweight Directory Access Protocol

DC – Domain Controller

KDC – Key Distribution Center

RODC – Read-Only DC

GPO – Group Policy Object

OU – Organizational Unit

DC – Domain Controller

GC – Global Catalog

SAML – Security Assertion Markup Language

SSO – Single Sign-On

AD LDS – Active Directory Lightweight Directory Services

LDAP – Lightweight Directory Access Protocol

AD CS – Active Directory Certificate Services

AD RMS – Active Directory Rights Management Services

GDPR – General Data Protection Regulation

IRM – Information Rights Management

TGT – Ticket Grating Ticket

LAPS – Local Administrator Password Solution

RSoP – Resultant Set of Policy

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

W32Time – Windows Time Service

DFS – Distributed File System

VLAN – Virttual Local Area Network

DPI – Deep Packet Inspection

USN – Update Sequence Numbers

NIST – National Institute of Standards and Technology

COBIT – Control Objectives for Information and Related Technologies

EoS – End of Sale

EoL – End of Life

Glossário de termos

- Vulnerabilidades

Fragilidades ou falhas em sistemas, redes ou processos que podem ser exploradas por ameaças para causar danos, acesso não autorizado ou interrupção de serviços.

- Ameaças

Eventos, agentes ou condições que têm o potencial de explorar vulnerabilidades e causar prejuízo aos ativos de informação, como malware, erro humano, falhas técnicas ou desastres naturais.

- Ataques

Ações deliberadas com o objectivo de comprometer a confidencialidade, integridade ou disponibilidade da informação, explorando vulnerabilidades dos sistemas ou redes.

- Incidentes

Ocorrências identificadas que comprometem ou têm o potencial de comprometer a segurança da informação, como acesso não autorizado, falhas de serviço, vazamento de dados ou ações maliciosas.

- Risco

Probabilidade de ocorrência de um incidente de segurança, combinada com o impacto potencial resultante, considerando a existência de vulnerabilidades e ameaças ativas.

- Logs

Registos automáticos de eventos, acessos e ações executadas em sistemas e redes, usados para auditoria, monitoramento, diagnóstico de falhas e investigação de incidentes.

- Porta

Identificador numérico utilizado nos protocolos de rede para distinguir serviços diferentes num mesmo endereço IP, como HTTP (porta 80), HTTPS (porta 443), SSH (porta 22), etc.

- Interface

Ponto de interligação física (como uma porta de rede) ou lógica (como uma interface virtual) que permite a comunicação entre dispositivos ou entre diferentes camadas de software em uma rede.

- Auditoria

Em TI, é o processo de recolha e análise de logs e eventos para verificar se as ações realizadas num sistema estão de acordo com as políticas de segurança e operacionais.

- Token de acesso

Estrutura de dados emitida após autenticação que contém permissões e identificadores de um utilizador; usado para autorizar acessos a sistemas ou recursos.

- Privilégio mínimo

Princípio de segurança segundo o qual os utilizadores devem ter apenas as permissões estritamente necessárias para executar suas funções.

- Segmentação de rede

Técnica que divide a rede em sub-redes (segmentos) isolados logicamente, com o objetivo de melhorar a segurança e o desempenho.

- Inspeção de pacotes

Processo de examinar o conteúdo dos pacotes de dados transmitidos na rede para detectar ameaças ou violações de políticas.

- Conformidade (com normas)

Atendimento a requisitos estabelecidos por normas, leis, regulamentações ou políticas internas. Por exemplo, estar em conformidade com a ISO/IEC 27001 ou RGPD.

- Provisionamento de contas

Processo de criação e configuração automática de contas de utilizadores nos sistemas, conforme políticas da organização.

- Política de segurança

Conjunto de diretrizes e regras que definem como a segurança da informação deve ser gerida e aplicada numa organização.

- Infraestrutura legada (ou sistemas legados)

Sistemas ou equipamentos antigos ainda em funcionamento que podem apresentar limitações de segurança e compatibilidade.

- Quarentena (de rede)

Isolamento automático de dispositivos suspeitos em uma zona controlada da rede, geralmente como resposta a uma ameaça.

- Ataque de força bruta

Técnica de adivinhação de senhas ou chaves criptográficas por tentativa e erro sistemático.

- Proxy reverso

Servidor que intermedeia solicitações externas, direcionando-as para servidores internos específicos, com funções de segurança e balanceamento de carga.

- Controle de banda (QoS)

Mecanismo que permite priorizar o tráfego de rede conforme o tipo de serviço ou aplicação, garantindo melhor desempenho.

- Timeout de sessão

Tempo máximo de inatividade permitido antes de encerrar automaticamente a sessão de um utilizador por razões de segurança.

- Zona Desmilitarizada (DMZ)

Zona intermediária da rede, geralmente entre a internet e a rede interna, usada para hospedar serviços acessíveis externamente, como servidores web ou de e-mail, com isolamento de segurança.

- Multifactor de autenticação (MFA)

Método de autenticação que exige mais de uma forma de verificação (ex.: senha + código SMS).

- Backbone de rede

Infraestrutura principal que interconecta todos os segmentos e equipamentos críticos de uma rede de computadores.

- Rede plana

Arquitetura de rede onde todos os dispositivos estão num único domínio de broadcast, sem segmentação lógica, o que aumenta o risco de propagação de falhas ou ataques.

- Endpoint

Dispositivo que está na "ponta" da rede, como laptops, smartphones ou impressoras, e que pode ser alvo de ameaças ou controlado por políticas de segurança.

- ACL (Access Control List)

Listas que especificam quais utilizadores ou sistemas podem aceder a determinados recursos, e com que permissões.

- Throughtput

Quantidade de dados que pode ser transmitida com sucesso por uma rede ou dispositivo num dado período de tempo (geralmente em Mbps ou Gbps).

- Single Sign-On

Tecnologia que permite a um utilizador aceder a vários sistemas diferentes com uma única autenticação, aumentando a conveniência e a segurança.

- Trunk

Ligação entre switches que transporta tráfego de múltiplas VLANs simultaneamente, utilizando marcações nos quadros Ethernet (ex: IEEE 802.1Q).

1. CAPÍTULO I – INTRODUÇÃO

1.1. Contextualização

A crescente dependência das instituições de ensino superior em infraestruturas digitais trouxe consigo desafios relevantes em termos de gestão e segurança de redes, tornando imperativa a adopção de infraestruturas de rede robustas, escaláveis e seguras. Na Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM), a rede existente evoluiu de forma não planeada, com foco na conectividade básica, mas sem uma arquitetura lógica que contemple segmentação, controlo de acessos centralizado e políticas de segurança orientadas à função dos utilizadores.

Entre as principais fragilidades identificadas estão: a inexistência de separação lógica de departamentos (com tráfego académico, administrativo e técnico a circular numa mesma rede plana), a gestão manual e fragmentada de contas de utilizadores, a ausência de políticas de acesso coerentes entre setores, e a dificuldade em aplicar medidas de segurança que respeitem o princípio do privilégio mínimo.

Este trabalho apresenta o desenvolvimento e implementação de uma solução de segurança de rede baseada na integração entre Active Directory Domain Services (AD DS) e a firewall Sophos XGS. A proposta parte da segmentação da rede em zonas funcionais com VLANs geridas pelo Sophos e da centralização da autenticação e gestão de permissões no AD, com aplicação de políticas de grupo (GPOs), partilhas controladas e regras de firewall baseadas em grupos do domínio. Toda a solução foi implementada e validada em ambiente laboratorial virtualizado, representando de forma realista a rede da FEUEM. O modelo resultante mostra-se viável, replicável e adaptável à realidade de instituições que, como a FEUEM, enfrentam limitações de orçamento, mas possuem recursos tecnológicos subutilizados.

1.2. Descrição do problema

A infraestrutura de rede do bloco administrativo da FEUEM apresenta fragilidades estruturais que comprometem sua segurança, escalabilidade e governança. Actualmente, não existe um mecanismo integrado para a gestão de identidades e de políticas de acesso, o que inviabiliza o controlo centralizado de permissões, autenticação de utilizadores e segmentação de tráfego. Cada estação de trabalho opera com credenciais locais, sem vínculo a um diretório unificado, o que dificulta a rastreabilidade de ações, fragiliza a auditoria e aumenta o risco de uso indevido de contas e elevação não autorizada de privilégios.

Adicionalmente, embora a instituição possua firewalls Sophos XGS 126 (parcialmente instalados) no ambiente de produção, estes encontram-se sem configuração activa, resultando na ausência de segmentação interna da rede e de mecanismos eficazes de inspeção de tráfego, como IDS/IPS. Com todo o tráfego concentrado num único ponto de saída no CIUEM, e sem regras diferenciadas por sector, os departamentos administrativos, académicos e técnicos partilham a mesma infraestrutura lógica, expondo dados sensíveis a vulnerabilidades internas e externas.

A inexistência de documentação formal, procedimentos operacionais padronizados ou políticas de governança tecnológica agrava o cenário, deixando as equipas técnicas sem diretrizes claras para resposta a incidentes, manutenção preventiva ou expansão controlada da infraestrutura. Isso leva à subutilização de recursos existentes e à aplicação fragmentada de soluções pontuais, sem coesão ou continuidade estratégica.

Neste contexto, justifica-se a implementação de um modelo de diretório centralizado com Active Directory Domain Services, a reconfiguração dos equipamentos Sophos XGS para promover segmentação lógica via VLANs e aplicação de políticas de segurança orientadas por função, além da definição de um conjunto mínimo de normas internas de governança. Como defendem (Peterson & Davie, 2011), a integração entre directórios, firewalls de próxima geração e políticas institucionais cria sinergias que permitem maximizar os recursos disponíveis, alinhar-se a boas práticas internacionais de segurança e adaptar-se às exigências específicas de ambientes académicos heterogéneos.

1.3. Motivação

A motivação para este trabalho nasce do fascínio pelas telecomunicações e pela segurança da informação, aliada à convicção de que, mesmo em contextos de recursos limitados, é possível alcançar elevados padrões de governança e proteção de redes. Como estudante e estagiário na Faculdade de Engenharia, especificamente no departamento de tecnologias de informação e comunicação (DTICs), o autor testemunhou acessos não autorizados e falta de monitorização, situações que atrasam processos, expõem dados sensíveis e geram crises evitáveis.

Esse contacto directo com as fragilidades da infra-estrutura despertou o desejo de não apenas cumprir obrigações académicas, mas de deixar um legado que beneficie futuras gerações de estudantes e investigadores. Inspirado pelo princípio de Sun Tzu de resolver problemas antes que surjam, pretende-se implementar soluções que antecipem vulnerabilidades e garantam flexibilidade para atender a exigências futuras. Além do interesse técnico, há um compromisso pessoal em valorizar o esforço dos colegas, proporcionando-lhes ferramentas que facilitem o seu trabalho, e um objectivo institucional de demonstrar que a FE pode ter uma infra-estrutura condizente com a sua missão académica.

1.4. Objectivos

1.4.1. Geral

- Propor a implementação de um mecanismo de segurança Tecnologias de Informação para proteção de dados.

1.4.2. Específicos

- ✓ Revisar e comparar mecanismos de gestão de identidades e segmentação de rede em ambientes acadêmicos.

- ✓ Diagnosticar a infra-estrutura de rede actual, identificando as principais limitações de segurança relacionadas à segmentação, controlo de acessos e gestão de utilizadores.
- ✓ Projetar e implementar a integração AD DS–Sophos XGS com segmentação por zonas funcionais, GPOs e regras de firewall.
- ✓ Validar e documentar a solução mediante testes de conectividade, autenticação e auditoria.

1.5. Metodologia

1.5.1. Pergunta de pesquisa

O presente trabalho de pesquisa propõe responder a seguinte pergunta:

Como implementar um modelo eficaz de governança e segurança de TI em instituições académicas (caso de estudo: FEUEM), integrando AD DS para gestão centralizada de acessos e proteção perimetral, de modo a superar vulnerabilidades em infra-estruturas com recursos limitados e sem substituição completa da rede existente?

1.5.2. Classificação da metodologia

Em relação a metodologia, o presente trabalho de pesquisa pode ser classificado:

a) Quanto à abordagem

Este trabalho de pesquisa segue uma abordagem mista (qualitativa com suporte experimental) que permitirá uma análise robusta e multidimensional do problema de pesquisa. Segundo (Martins, 2006) citado por (Massunguine, 2022), o trabalho não se resume somente em empregar técnicas estatísticas para o tratamento de informações numéricas, mas também, em uma análise dos dados recolhidos de forma a se chegar a um profundo entendimento do problema e com isso poder-se selecionar a solução mais adequada para a resolução do mesmo. A análise qualitativa permitiu compreender o funcionamento actual da rede, identificar as fragilidades estruturais e fundamentar a

proposta de solução. A parte experimental concentrou-se na implementação e validação da solução em ambiente virtualizado.

b) Quanto à natureza

O presente trabalho classifica-se como pesquisa aplicada, com forte orientação prática, pois tem como principal finalidade produzir conhecimento para aplicação prática e concreta na resolução de um problema.

c) Quanto aos objectivos

Os objectivos deste trabalho são, por um lado, exploratórios, pois visam investigar um problema institucional pouco estudado, e, por outro, descritivos, ao documentar e caracterizar a situação actual e o processo de implementação das soluções propostas.

d) Quanto aos procedimentos

Os procedimentos do presente trabalho classificam-se como: Pesquisa bibliográfica, Pesquisa documental e Caso de estudo. A seguir será feita a descrição de cada um dos procedimentos:

- **Pesquisa bibliográfica**

A pesquisa bibliográfica é entendida como um método sistemático de investigação que consiste na revisão e análise de obras publicadas (livros, artigos científicos, teses e documentos técnicos) para fundamentar teoricamente o estudo. No contexto deste trabalho, essa abordagem permite identificar melhores práticas internacionais e adaptá-las à realidade Moçambicana. Sua principal função é contextualizar o problema, evitar redundâncias e embasar as decisões técnicas com evidências consolidadas.

- **Pesquisa documental**

A pesquisa documental caracteriza-se pela análise crítica de registros instituicionais, relatórios técnicos, normativas e arquivos oficiais. É similar à pesquisa bibliográfica, mas diferem pelo facto de a pesquisa bibliográfica utilizar material já elaborado, ou seja, livros e artigos, enquanto que, a pesquisa documental foca-se em documentos primários não publicados comercialmente, ou seja, recorre a fontes mais diversificadas e dispersas

sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, documentos oficiais, cartas, filmes, fotografias, relatórios, etc.

- **Caso de estudo**

O caso de estudo é uma metodologia qualitativa que investiga profundamente um fenômeno específico em seu contexto real. Caracteriza-se como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema, uma pessoa ou uma unidade social. Tem como finalidade conhecer em profundidade o como e o porquê de uma determinada situação que se supõe ser única em muitos aspectos, procurando descobrir o que há de mais essencial e característico. Em suma esta abordagem justifica-se pela necessidade de soluções customizadas que considerem particularidades locais.

1.5.3. Técnicas de coletas de dados

Na realização deste trabalho de pesquisa foram utilizadas as seguintes técnicas de coleta de dados para garantir uma abordagem abrangente e precisa:

- **Observação directa**

A observação directa envolve o registro sistemático das características físicas e operacionais da infra-estrutura durante visitas técnicas. No contexto deste trabalho, esta técnica foi aplicada através de um roteiro estruturado, pois o autor atuou como agente técnico no ambiente, acompanhando e registrando práticas de utilização da rede, identificando falhas, limitações operacionais e pontos críticos de segurança.

- **Entrevistas**

Como técnica qualitativa essencial, as entrevistas informais permitiram capturar as percepções e experiências dos principais actores envolvidos. Foram conduzidas com: (a) membros da DTIC, a equipa responsável pela rede, com o objectivo de obter informações sobre a estrutura lógica actual, dificuldades enfrentadas e expectativas em relação à gestão de acessos e segurança; (b) chefes dos departamentos localizados no bloco administrativo, para entender o impacto das falhas nos processos críticos; e (c)

usuários comuns da rede, como estudantes. O roteiro de entrevistas incluiu perguntas abertas sobre a infra-estrutura de rede da instituição (vide o Anexo 7).

Questionário

Também é uma técnica de investigação, contudo, diferencia-se da entrevista pelo facto das questões elaboradas pelo investigador serem apresentadas de forma escrita ao investigado, normalmente apresentam um número de questões relativamente maior em relação as apresentadas numa entrevista e podem ser respondidas na ausência do investigador.

Foi elaborado um e único questionário contendo perguntas de resposta única (Sim/Não) e abertas, e foi dirigido aos responsáveis pela infra-estrutura de rede corporativa da FEUEM, que é a DTIC. (Vide o anexo 8).

1.6. Estrutura do trabalho

Este trabalho de pesquisa está organizado da seguinte forma:

- Capítulo I – Introdução

Neste capítulo apresenta-se a contextualização, a descrição do problema, a motivação, os objectivos que se pretendem alcançar, são identificadas e descritas as técnicas metodológicas usadas para atender aos objectivos traçados e por fim apresenta-se a estrutura do trabalho.

- Capítulo II – Revisão de literatura

Neste capítulo são descritas e apresentadas as definições mais relevantes em torno do tema do presente trabalho, nomeadamente: Gestão de acessos, Segurança em redes, Monitoramento e Governança de segurança.

- Capítulo III – Caso de estudo

Neste capítulo é feita a apresentação da FEUEM – Faculdade de Engenharia da Universidade Eduardo Mondlane, a descrição da situação actual e os constrangimentos que advém da situação actual.

Capítulo III – Caso de estudo

- Capítulo IV – Proposta de Solução

Após a apresentação clara e precisa do problema, neste caso, os constrangimentos anteriormente identificados na FEUEM, neste capítulo propõe-se e desenvolve-se uma solução para resolver o referido problema.

- Capítulo V – Apresentação e Discussão de Resultados

Neste capítulo, apresenta-se e discute-se em torno dos resultados apresentados no presente trabalho de pesquisa.

- Capítulo VI – Considerações Finais

Neste capítulo, sintetizam-se as principais conclusões do trabalho, confirmando se os objectivos iniciais foram alcançados e analisando criticamente os resultados obtidos. Reflete-se sobre as limitações do estudo e o seu impacto nos achados finais, propondo recomendações para investigações futuras. Destaca-se a contribuição prática e académica do trabalho, encerrando o ciclo de pesquisa com uma avaliação global do percurso realizado. Trata-se de uma análise reflexiva que consolida todo o processo investigativo, sem introduzir novos elementos.

- Bibliografia

Nesta secção são indicadas todas as fontes (obras) consultadas para materializar o presente trabalho de pesquisa assim como para alcançar os objectivos traçados

- Anexos

Nesta secção são apresentados os elementos adicionais que facilitam à compreensão do presente trabalho de pesquisa.

2. REVISÃO DE LITERATURA

2.1. Segurança de informação no ecossistema digital

A crescente dependência das tecnologias digitais para operações organizacionais transformou a segurança da informação num pilar essencial da sustentabilidade institucional. Em ambientes académicos, empresariais e governamentais, a integridade dos dados, a disponibilidade dos sistemas e a confidencialidade das informações são activos estratégicos.

Segundo a (ISO, 2022), a segurança da informação é definida como “a preservação da confidencialidade, integridade e disponibilidade da informação”. Estes três pilares, conhecidos como o triângulo CIA (*Confidentiality, Integrity, Availability*) são a base de qualquer arquitectura de segurança. A seguir são descritas as referidas propriedades para manter um estado de segurança desejado com base em (Fernandes, 2015):

- Confidencialidade é a propriedade que limita o acesso à informação apenas às entidades legítimas, isto é, apenas às entidades autorizadas pelo proprietário da informação;
- Integridade é a propriedade que garante que a informação não sofreu qualquer modificação indevida ao longo do processo de transmissão da mesma;
- Disponibilidade é a propriedade que garante que a informação estará sempre disponível para uso legítimo, ou seja, para uso dos utilizadores autorizados pelo proprietário da informação.

No ecossistema digital, a segurança da informação estende-se à infra-estrutura de redes, aos dispositivos finais, aos utilizadores e às aplicações em nuvem.

A proliferação de ciberameaças, como *ransomware*, *phishing*, exploração de vulnerabilidades e acessos não autorizados, evidenciam a necessidade de estratégias de proteção integradas. A abordagem moderna de segurança requer, portanto, uma

arquitetura de defesa em profundidade, onde múltiplas camadas de proteção (tecnológicas e organizacionais) atuam de forma coordenada para mitigar riscos.

Normas internacionais, como a ISO/IEC 27001**,** COBIT e os frameworks do NIST, oferecem estruturas de referência para a implementação de sistemas de gestão de segurança da informação (SGSI). A ISO 27001, por exemplo, define requisitos para estabelecer políticas de segurança, identificar e tratar riscos, e implementar controlos técnicos e administrativos (ISO, 2022). O NIST, por sua vez, com a série SP 800-53, especifica controlos técnicos detalhados aplicáveis a redes, sistemas operativos, aplicações e utilizadores. Já o COBIT orienta a governação de TI, garantindo que os objectivos estratégicos sejam atingidos por meio da gestão eficaz dos riscos e dos recursos de TI.

Neste contexto, a proteção da infra-estrutura de rede (segurança perimetral) e a gestão de utilizadores (segurança de identidades) não são elementos isolados, mas partes interdependentes de um ecossistema mais amplo. A gestão centralizada de acessos permite reduzir o risco de erros manuais, enquanto as barreiras perimetrais, como firewalls e segmentação de rede, evitam que um incidente comprometa toda a organização.

2.1.1. Gestão Centralizada de Utilizadores

A gestão centralizada de utilizadores consiste em agrupar todas as identidades digitais da organização num único repositório seguro, de forma a simplificar o controlo de acesso e reduzir a duplicação de perfis em múltiplos sistemas. Segundo (Prekas, 2017), esse modelo permite que as credenciais dos utilizadores sejam geridas a partir de um ponto único, facilitando a aplicação de políticas de segurança, como requisitos de complexidade de senhas ou ciclos de vida de conta, e assegurando que quaisquer alterações se reflitam imediatamente em todos os serviços conectados.

Além disso, reforça a (NIST, 2020) que a gestão centralizada favorece a implementação de mecanismos de autenticação forte, como autenticação multifactor e a auditoria

unificada de eventos de acesso, uma vez que os registos de autenticação e autorização convergem para um sistema único de logs.

Segundo (Gollman, 2011), centralizar identidades reduz potencial para erros manuais e mitigam riscos de contas órfãs ou acessos indevidos, contribuindo para o princípio do privilégio mínimo.

2.1.1.1. Avaliação de soluções e Critérios técnicos

Ao desenhar a gestão centralizada de identidades, é fundamental comparar soluções que operem em ambientes Windows e Linux de modo integrado. Embora o AD DS seja amplamente utilizado em redes Windows, alternativas open-source, como Samba AD, FreeIPA e OpenLDAP, oferecem funcionalidades semelhantes com custos de licenciamento reduzidos (Gollman, 2011; Harrison, 2018).

Critérios essenciais incluem compatibilidade com Windows, suporte a protocolos padrão e ferramentas administrativas adequadas. A escalabilidade também merece atenção, pois o diretório deve suportar grande volume de contas sem perda de desempenho (Prekas, 2017).

Além disso, é imprescindível cumprir normas como ISO/IEC 27001:2022, que exige auditoria periódica de privilégios de acesso, e adotar diretrizes do NIST SP 800-63 para autenticação digital (ISO, 2022; NIST, 2020). Ferramentas como ITIL reforçam processos formais de criação, modificação e revogação de contas, bem como o monitoramento de eventos de autenticação (Axelos, 2019). A escolha final deve equilibrar segurança, custos, facilidade de integração e garantir redundância, por exemplo, por meio da replicação de controladores de domínio. A seguir é feita a descrição sucinta de cada um dos mecanismos:

1) Samba AD

Figura 2-1: Logotipo do Samba

Fonte: Site Oficial

Segundo (The Samba Team, 2023) o Samba 4.x funciona como controlador de domínio Active Directory (AD DC) desde a versão 4.0 (2012), oferecendo LDAP integrado, suporte a Kerberos (Heimdal ou MIT) e DNS interno para gerir utilizadores, computadores e Group Policy Objects. Permite autenticação única em estações Windows e Linux (via SSSD) e administração pelo RSAT, reproduzindo a experiência do AD Microsoft sem custos de licenciamento.

Apesar de gratuito e eficaz em redes mistas, o Samba AD limita-se historicamente ao nível funcional Windows Server 2008 R2, com suporte experimental a versões mais recentes.

Algumas funcionalidades avançadas de GPO ainda não são totalmente equivalentes às do AD proprietário, exigindo complementar com scripts ou configurações adicionais. Além disso, actualizações do Windows podem afectar incompatibilidades, pelo que é necessário acompanhar os lançamentos do projecto (Tridgell, 2017).

Como enfatiza (The Samba Team, 2023) destina-se a organizações que buscam serviços de domínio compatíveis com Windows sem recorrer a servidores Microsoft, conciliando interoperabilidade e economia.

2) FreeIPA

Figura 2-2: Logotipo Oficial do FreeIPA

Fonte: Site Oficial (https://www.freeipa.org/)

Segundo (Red Hat, Inc, 2022), o FreeIPA (Free Identity, Policy and Audit) é uma solução de código aberto da Red Hat que integra um servidor LDAP (389 Directory Server), um KDC Kerberos (MIT Kerberos), um servidor DNS, uma autoridade certificadora (Dogtag) e serviços de NTP, apresentando-se via interface web e CLI ("ipa").

Essa arquitetura unificada oferece gestão centralizada de utilizadores e grupos, políticas de acesso e Single Sign-On para ambientes Linux/Unix, além de permitir a configuração de trust com AD via Samba para integração em domínios Windows. O FreeIPA valoriza infra-estruturas RHEL/CentOS, simplifica a administração de políticas de segurança e a emissão de certificados TLS, e suporta autenticação multifactor (Tweedale, 2019).

Em contrapartida, está optimizado para Linux e requer configuração avançada de LDAP, Kerberos e DNS, tornando a curva de aprendizagem acentuada; clientes Windows só ingressam no domínio IPA com componentes adicionais, o que pode complexificar a implantação.

3) OpenLDAP

Figura 2-3: Logotipo do OpenLDAP

Fonte: Wikipedia

Segundo (Wahl, Howes, Kille, & Sermershein, 1997), o OpenLDAP é uma implementação open-source do protocolo LDAP, que define como armazenar e consultar dados em diretórios hierárquicos. Seu daemon principal, slapd, atende a requisições LDAP e armazena objectos como utilizadores e grupos, permitindo definir esquemas personalizados (Prevelakis & Spinellis, 2000).

Por ser leve e compatível com vários sistemas operativos, o OpenLDAP adapta-se a cenários que necessitam apenas de um diretório puro, sem sobrecarga de funcionalidades adicionais (Robbins, 2003). No entanto, não possui interface gráfica nativa, exigindo ferramentas externas (por exemplo, phpLDAPadmin) ou uso de comandos CLI para gestão. Além disso, não integra serviços de autenticação forte (Kerberos), autoridade certificadora (CA) ou DNS, tornando necessário configurar esses componentes separadamente para obter um ambiente completo de gestão de identidades (Prevelakis & Spinellis, 2000)

Em suma, o OpenLDAP é ideal quando se busca um diretório flexível e de baixo custo, mas requer complementos externos para oferecer autenticação e políticas de segurança avançadas (Wahl et al., 1997; Robbins, 2003).

4) Active Directory Domain Services (AD DS)

Figura 2-4: Logotipo do Active Directory

Fonte: Figma Resource (https://figmaresource.com/microsoft-active-directory-logo/)

O AD DS é o componente do Active Directory responsável por armazenar o diretório central e autenticar utilizadores e computadores numa rede de domínio Windows. Conforme a (Microsoft Learn, 2025) explica, “o AD DS armazena informações sobre

contas de utilizador, como nomes, senhas, números de telefone etc., e permite que outros utilizadores autorizados da mesma rede acessem essas informações".

Em termos estruturais, o AD organiza estes objectos num armazenamento de dados hierárquico: um domínio contém objectos e políticas, unidades organizacionais agrupam objectos semelhantes, e sites definem agrupamentos físicos. O processo de replicação multi-mestre garante que alterações sejam propagadas a todos os DCs do domínio.

Além disso, o AD integra diretamente mecanismos de controlo de acesso. Ele usa o token de acesso (baseado em SID – identificador de segurança) para autorizar ações de utilizadores e grupos. O AD armazena essas credenciais e controla o acesso a recursos da organização.

O AD também inclui funcionalidades como Catálogo Global para pesquisa rápida de objectos em todo o bosque e esquema para definição de classes de objectos e atributos. Em resumo, o AD DS fornece a base fundamental para autenticação centralizada e gestão de identidades, apoiando a aplicação de políticas corporativas de forma consistente.

a. Controlo de Acesso Baseado em Funções (RBAC)

O modelo RBAC mapeia as funções organizacionais aos direitos de acesso. No RBAC clássico, cada utilizador recebe um ou mais papéis, cada papel tem um conjunto de permissões, e o acesso resultante é a união das permissões dos papéis atribuídos. A (Red Hat, Inc, 2022) define RBAC como "uma maneira de gerenciar o acesso de um usuário a sistemas, redes ou recursos com base na função dele dentro de uma equipa ou empresa".

Em RBAC avançado, pode haver hierarquias de papéis ou restrições de segregação de funções. Em termos de norma, o RBAC corresponde aos controles de acesso da ISO 27001 (Anexo A.9) e NIST SP800-53 (família AC), que preconizam gestão central de contas e privilégio mínimo. A adoção de RBAC em conjunto com AD DS possibilita

delegar permissões por função em vez de gerir cada conta individualmente, simplificando a administração de acessos e reduzindo os erros humanos.

2.1.2. Segurança Perimetral

A segurança de perímetro refere-se às barreiras (físicas ou lógicas) que isolam a rede interna de ameaças externas. Tradicionalmente, o paradigma de "castelo e muralha" dominava: confiava-se que tudo dentro da rede interna era seguro, bastando erguer uma firewall perimetral para controlar o acesso externo.

Nesse modelo clássico, redes públicas e privadas eram separadas por firewalls, e servidores acessíveis ao público eram colocados numa zona desmilitarizada (DMZ), minimizando o risco de intrusão na rede interna. Por exemplo, (Allied Telesis, 2022) descreve uma abordagem típica de três zonas: "zona pública, zona privada e DMZ".

A separação de zonas ajuda a conter compromissos, porque se um servidor num DMZ for invadido, o atacante fica limitado àquele segmento, sem acesso directo ao núcleo interno. Como ilustra o (Hitzel, s.d.), "se um servidor web hospedado dentro da rede interna for comprometido, todos os recursos internos estão em risco; porém no caso de um DMZ, somente os recursos limitados dessa área correm risco, nada na rede interna será afetado (a não ser que haja má-configuração)". Assim, defende-se uma estratégia de defesa em profundidade, segmentando redes e construindo camadas de proteção, em vez de confiar numa única barreira de perímetro.

2.1.2.1. Firewalls

Segundo (Mamede, 2006), quando se cria uma forma de ligação da nossa rede interna à internet, abre-se um canal de troca de tráfego entre estes dois ambientes. Pode se controlar a rede interna de uma organização (ambiente privado), mas é impossível controlar a internet (ambiente público). A zona onde termina a rede interna e começa a rede não controlada chama-se perímetro ou fronteira.

Há o desafio de ter que se implementar mecanismos de segurança, que incluem medidas e tecnologias, que permitam criar segurança ao nível de perímetro de forma a garantir que todo o tráfego desconhecido não consiga acesso à rede interna. O dispositivo que se utiliza para este fim toma o nome de antepara de proteção ou firewall no original em Inglês (Mamede, 2006).

Uma firewall pode ser descrita como um componente de hardware ou software que separa uma rede segura de uma outra não segura.

Aos sistemas de firewall são assim atribuídas as diferentes responsabilidades, como a implementação da política de segurança da empresa no interior da rede protegida, o controlo de acesso, o assegurar a manutenção da privacidade e disponibilizar meios de auditoria. E tudo isto com dois pressupostos básicos que são, segundo (Mamede, 2006):

- Aquilo que não é expressamente permitido, é proibido;
- Aquilo que não é expressamente proibido, é permitido.

De acordo com (Mamede, 2006), o enfoque primário de uma firewall é o controlo de acesso, a diferentes níveis abaixo indicados:

- O controlo de serviços, com a definição de que serviços podem ser acedidos;
- O controlo de redireccionamento, com a definição em que direção pode o serviço ser iniciado e permitido o fluxo;
- O controlo de acessos, com a especificação de que serviços pode um utilizador específico aceder; e
- O controlo de comportamento, definindo como são usados determinados serviços particulares, como o controlo de e-mail para eliminação de spam.

Portanto, uma firewall é um mecanismo de segurança que funciona com base num conjunto bem definido de regras de filtragem de pacotes, que controlam e filtram todas as ligações entre duas ou mais redes, através de um único ponto de acesso, como pode ser visto na figura abaixo. O controlo e a filtragem são feitos com base no tipo de pacote, endereço origem e destino, porta de origem e destino, entre outros parâmetros.

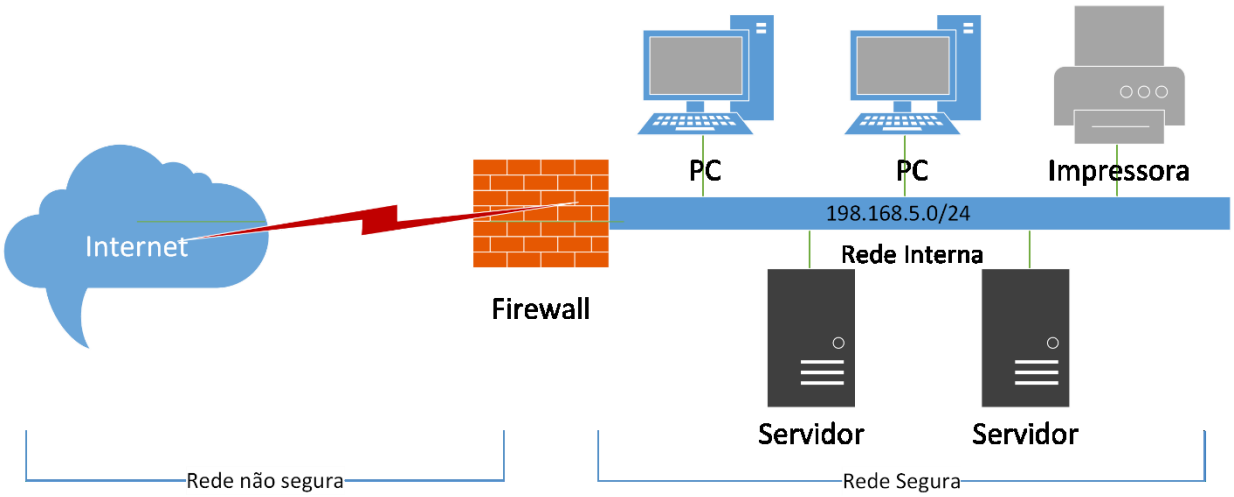


Figura 2-5: Estrutura básica de uma firewall

Fonte: Elaborada pelo autor

Os principais benefícios que se podem ter pelo recurso a este de dispositivos são a proteção contra tráfego indesejado proveniente do exterior da rede e proteção contra a violação da privacidade da rede interna. No entanto, (Mamede, 2006) afirma que, as firewalls não constituem, só por si, a pedra filosofal da segurança de perímetro, até porque eles apresentam alguns riscos, tais como:

- Impacto no desempenho, já que aumentam a latência ao tráfego entre a rede controlada e a internet, na medida em que o mesmo tem de ser analisado;
- Por outro lado, como constituem, ou devem constituir, o único ponto de entrada na rede controlada, se a firewall for comprometida por um atacante, então, toda a rede interna pode ser comprometida;

O (Mamede, 2006) considera que, por vezes é necessário considerar a possibilidade da existência de segmentos na rede com um menor grau de segurança ou proteção para, por exemplo, disponibilizar serviços que pretendemos assegurar ao exterior do perímetro de segurança, mas de forma controlada. Esses segmentos tomam o nome de zonas desmilitarizadas, do inglês demilitarized zone (DMZ). Uma DMZ reside entre uma rede pública como internet e a rede privada, protegida. Todo tráfego que entra ou sai da DMZ é inspecionado pelas regras da firewall, de forma a determinar se o mesmo é ou não permitido.

2.1.2.1.1. Arquitecturas de implementação de firewalls

O (Mamede, 2006) afirma que, existem quatro configurações básicas que podem ser utilizadas como modelos de implementação para a solução de firewall. Porém, antes de detalhar as quatro configurações básicas de firewall, é fundamental entender o conceito de bastião de segurança (Bastion Host).

O bastião representa um ponto crítico na defesa de perímetro, pois agrega o sistema de firewall e demais mecanismos de proteção, funcionando frequentemente como gateway de aplicação ou circuito.

Entre as suas características está a exigência de autenticação adicional para acesso a proxies, que por sua vez podem requerer credenciais próprias. Com esse entendimento, (Mamede, 2006) apresenta quatro modelos arquitecturais para firewalls que contemplam diferentes formas de isolar redes, balancear serviços e maximizar a segurança no ponto de entrada:

1) Filtro de pacotes (Packet-Filtering Boundary Router)

O filtro de pacotes constitui a forma mais antiga de implementação de um sistema de firewall. Na figura abaixo, está representada esta arquitectura, com router, que possui capacidades de filtro de pacotes, posicionado entre a rede segura e a rede publica ou não protegida.

Dada a sua posição, este router é também, por vezes, designado de router de perímetro. Um router com estás funções recorre à utilização de ACL ou listas de controlo de acesso para encaminhar ou descartar os pacotes que chegam até si, garantindo de forma genérica proteção contra ataques provenientes da rede não segura. Esta forma de implementação possui algumas deficiências que são:

- Falta de mecanismos de autenticação forte;
- Complexidade da manutenção da ACL no router;
- Criação de registos de jornal bastante limitados, dificultando a auditoria;

- Se o router for comprometido, o tráfego pode fluir directamente através deste, vindo da Internet, para máquinas da rede interna;

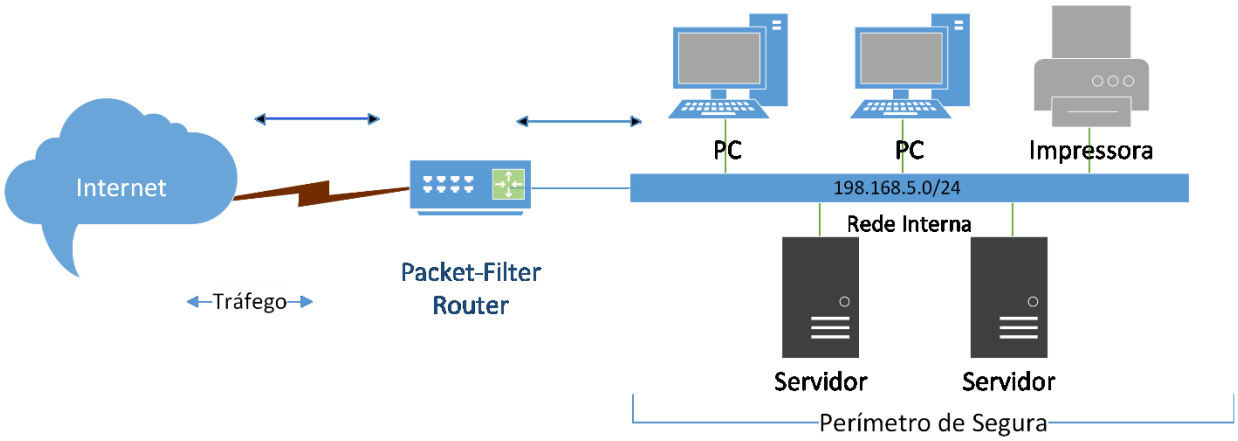


Figura 2-6: Filtro de pacotes

Fonte: Elabora pelo autor

2) Screened Host Firewall (Singled, Dual e Multi home)

Esta arquitectura de firewall utiliza um router filtro de pacotes e um host bastião. É uma arquitectura com um desenho um pouco mais complexo que a outra já referida porque oferece um nível de segurança superior, disponibilizando serviços no nível de rede, com filtro de pacotes, e ao nível aplicacional, como servidor proxy.

Assim, este tipo de sistema firewall é considerado bastante seguro porque exige a um atacante a intrusão em dois sistemas separados antes de conseguir comprometer a rede protegida.

a) Singled-home Bastion Host

Esta arquitectura recorre à utilização de dois sistemas distintos: Um router, que é configurado de forma a seguir duas regras básicas:

1. Para tráfego proveniente da Internet, apenas pacotes destinados ao bastião são permitidos; e

2. Para tráfego proveniente da rede interna, apenas pacotes originados pelo bastião podem passar.

O bastião preenche algumas lacunas apresentadas na arquitectura anterior, com funcionalidades que lhe permitem garantir mecanismos de autenticação forte e de proxy.

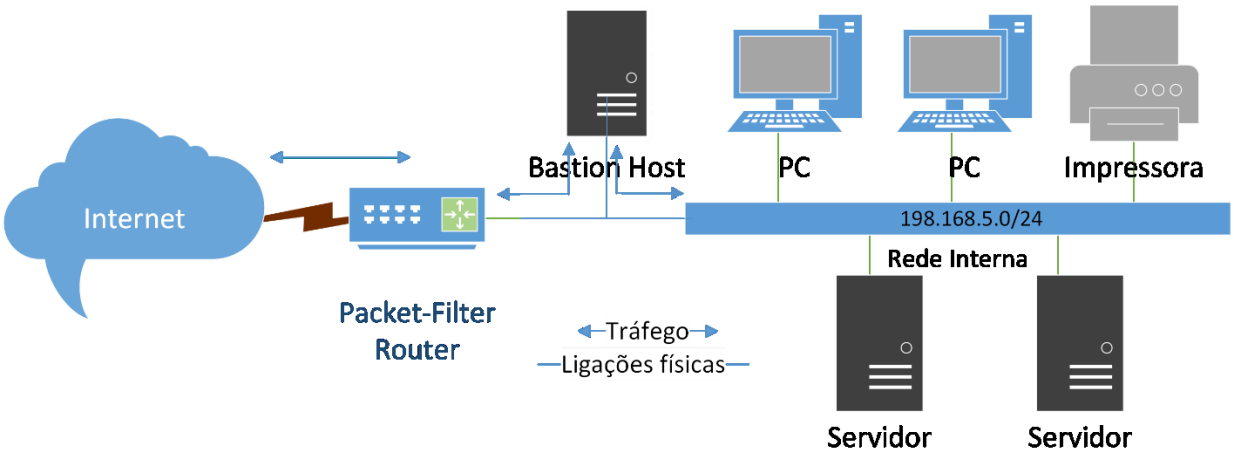


Figura 2-7: Bastion Host Singled-home

Fonte: Elaborada pelo autor

A figura anterior apresenta a arquitectura referida. Salienta-se a possibilidade de definição de uma zona desmilitarizada, com o acesso controlado pelo bastião, como se pode ver na figura abaixo, de forma a possibilitar acessos públicos a determinados serviços como, por exemplo, um servidor web.

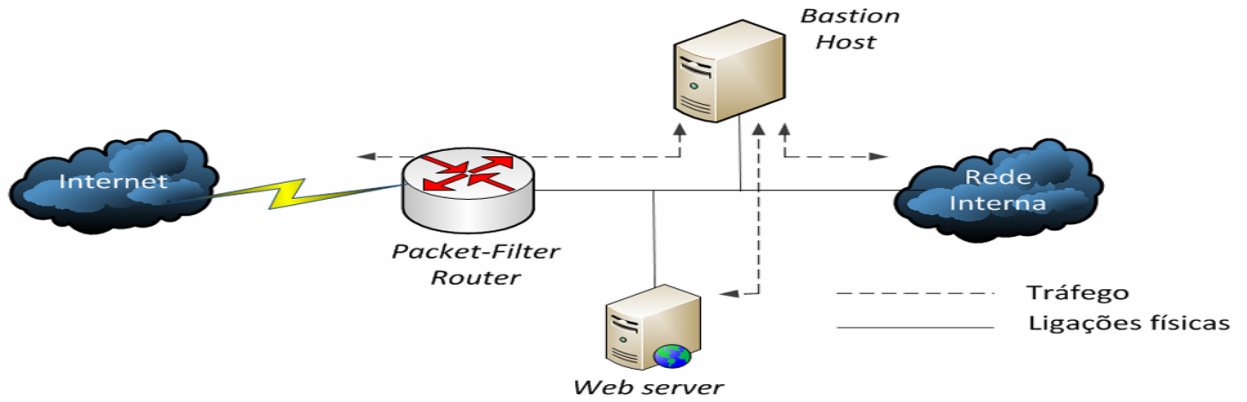


Figura 2-8: Bastion Host Singled-home com DMZ.

Fonte: Adaptado da aula de Firewalls (ASSC, 2021)

b) Dual e Multi-home Bastion Home

A arquitetura dual-homed bastion host é uma evolução do modelo de firewall com filtro de pacotes, oferecendo maior segurança através do isolamento físico entre a rede externa (como a Internet) e a rede interna. Este modelo utiliza um sistema com duas interfaces de rede (NICs), cada uma conectada a uma rede distinta – uma externa e outra interna.

O bastião, nesse caso, atua como intermediário, impedindo que o tráfego externo seja roteado diretamente para a rede interna. Esta configuração, também conhecida como multi-homed bastion host quando possui mais de duas interfaces, reforça a proteção da infra-estrutura ao evitar encaminhamentos directos entre redes, exigindo que todo o tráfego passe por filtros e controlos aplicados pela firewall. O princípio fundamental desta arquitetura é garantir que não exista roteamento directo entre as redes, o que evita a exposição da rede interna a acessos não autorizados.

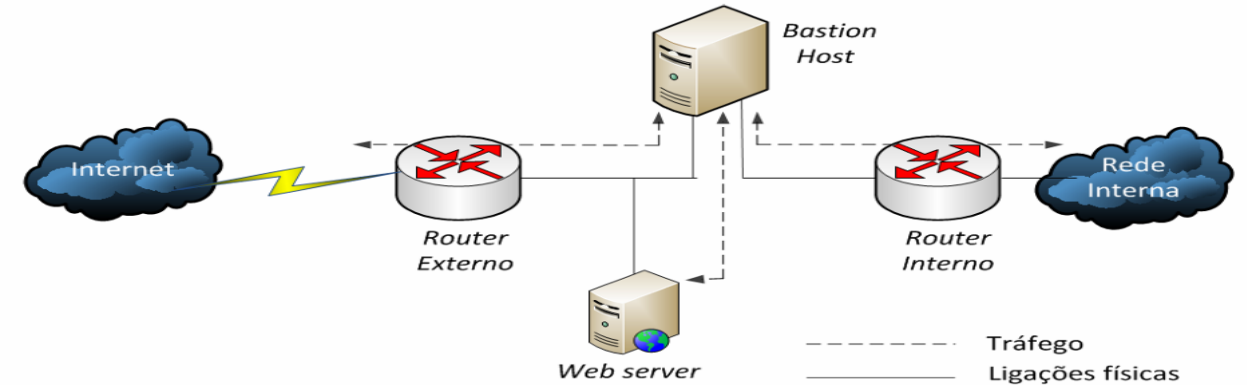


Figura 2-9: Bastion Host Dual-Home

Fonte: Adaptado da aula de Firewalls (ASSC, 2021)

3) Screened Subnet Firewall

A arquitetura Screened Subnet Firewall é considerada uma das mais seguras, pois estabelece uma sub-rede isolada, a DMZ, entre a rede interna protegida e a rede externa não confiável. Esta configuração utiliza dois routers com filtragem de pacotes, posicionando um bastião entre eles. Assim, todo o tráfego que transita pela DMZ é

controlado em três níveis: o router externo bloqueia ataques vindos da Internet, o bastião inspeciona o tráfego na sub-rede, e o router interno restringe o acesso à rede interna.

Mesmo que o bastião seja comprometido, o atacante continua isolado da rede principal, graças à segmentação (Mamede, 2006). A principal desvantagem deste modelo está na sua complexidade de configuração e manutenção.

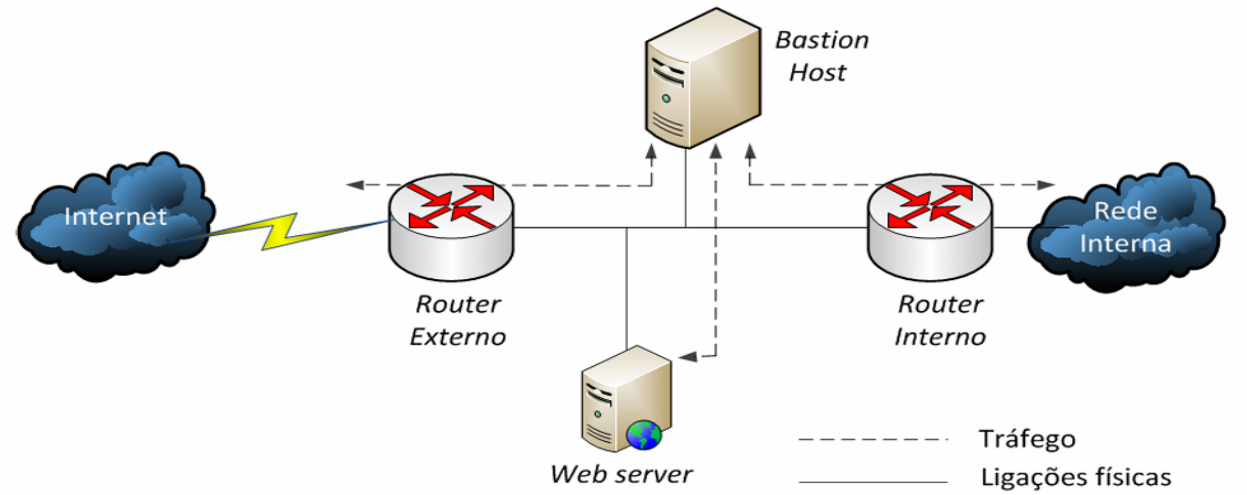


Figura 2-10: Screened subnet Firewall

Fonte: Adaptado da aula de Firewalls (ASSC, 2021)

2.1.2.1.2. Políticas de Firewall

As firewalls desempenham um papel fundamental na segurança das redes ao controlar o tráfego entre diferentes zonas da infra-estrutura digital. Para tal, implementam um conjunto de funcionalidades que vão desde o bloqueio de tráfego indesejado até à autenticação robusta de utilizadores (Stallings & Brown, 2020). Entre os principais mecanismos de proteção oferecidos destacam-se:

- A capacidade de bloquear tráfego não desejado, impedindo acessos não autorizados;
- O redireccionamento de tráfego externo para sistemas internos confiáveis;
- A possibilidade de ocultar sistemas vulneráveis dentro da rede interna;
- A realização de registos (logs) de tráfego entre a rede interna e a externa;

- A ocultação de informações sobre a rede interna, tais como nomes de sistemas, topologia e dispositivos activos;
- A disponibilização de autenticação forte, mais segura do que a geralmente utilizada por aplicações padrão.

Estas funcionalidades permitem aplicar o princípio do privilégio mínimo e reduzir a exposição da infra-estrutura, mas implicam, inevitavelmente, um equilíbrio entre segurança e conveniência. Este equilíbrio é formalizado por meio das políticas de firewall, que definem o comportamento esperado do sistema perante os diversos tipos de tráfego que circulam entre redes com diferentes níveis de confiança (Stallings & Brown, 2020).

Uma política de firewall é implementada através de um conjunto de regras, que devem ser claras, completas e coerentes. A maior parte da administração de uma firewall consiste na definição, revisão e actualização destas regras, conforme as necessidades operacionais e os riscos associados à organização. Exemplos típicos de regras incluem:

- Permitir que todos os IPs internos acedam à Web (porta 80/443);
- Permitir o tráfego de e-mail a partir do servidor interno (porta 25/587/993);
- Bloquear (drop) todo o tráfego que não corresponda às regras autorizadas;
- Permitir tráfego do exterior apenas para o servidor Web público;
- Bloquear todo o tráfego externo não autorizado;
- Registar todas as tentativas de ligação rejeitadas;
- Registar os acessos a servidores web externos.

As regras devem cobrir não só o tráfego de saída da rede interna para a Internet, como também o tráfego entrante proveniente do exterior, garantindo controlo bidirecional. A gestão eficaz destas políticas exige conhecimento técnico e actualização contínua, pois a ameaça digital é dinâmica e em constante evolução.

2.1.2.2. Firewalls de Próxima Geração (NGFW)

As firewalls de próxima geração, do inglês Next-Generation Firewall (NGFW) representam uma evolução das firewalls tradicionais de filtragem por IP e porta, acrescentando inspeção profunda de pacotes e funcionalidades avançadas de segurança. Em vez de limitar-se a analisar apenas os cabeçalhos de rede, um NGFW realiza inspeção profunda de pacotes, identificando protocolos e aplicações mesmo quando utilizam portas não convencionais (Stallings & Brown, 2020).

Para além disso, estes dispositivos integram num único equipamento funcionalidades como controlo de aplicações, permitindo bloquear programas indesejados, IPS, VPN, filtragem web/URL e gestão de identidades (ligando-se a diretórios de utilizadores), simplificando a arquitetura de segurança (Stallings & Brown, 2020).

Na prática, os administradores posicionam NGFWs para criar zonas de segurança mais granuladas (por exemplo, separar uma zona administrativa de outra de utilizadores) ou manter o clássico esquema de três zonas (externa, desmilitarizada e interna), mas com maiores níveis de controlo em cada segmento.

De modo geral, o NGFW combina funções de múltiplos equipamentos de segurança: o módulo IDS/IPS integrado analisa o tráfego em tempo real para detectar e impedir ataques, enquanto o filtro web bloqueia sítios maliciosos com base nas políticas da organização. Esta convergência de capacidades facilita a gestão, pois concentra várias camadas de defesa num só ponto.

Contudo, importa ter em atenção o desempenho: a ativação simultânea de mecanismos como antivírus, IPS e controlo de aplicações pode reduzir significativamente a vazão (throughput) se o hardware não estiver devidamente dimensionado (Stallings & Brown, 2020).

2.1.2.3. Segmentação com VLANs e Roteamento Inter-VLAN

A segmentação com VLANs consiste em dividir um único switch físico em várias redes lógicas distintas, cada uma funcionando como um domínio de broadcast isolado. Assim,

um dispositivo numa VLAN só vê o tráfego dos seus membros, melhorando a segurança ao limitar a visibilidade do tráfego a utilizadores autorizados (Odom, 2019).

Para implementar, atribuem-se portas específicas do switch a cada VLAN conforme departamentos ou funções, e estabelecem-se ligações “trunk” que transportam múltiplas VLANs entre switches.

A comunicação entre VLANs exige um roteador inter-VLAN ou um switch de camada 3 com subinterfaces VLAN, permitindo o encaminhamento de tráfego entre sub-redes distintas enquanto se aplicam políticas de firewall ou listas de controlo de acesso (ACLs) para regular quais as VLANs que comunicam entre si (Hucaby, McQuerry, & Jansen, 2009).

Em conjunto, VLANs e roteamento inter-VLAN criam uma rede multicamadas onde cada segmento é isolado, comunicando-se apenas por caminhos autorizados, o que reduz significativamente o risco de propagação lateral de ataques (Odom, 2019).

2.1.2.4. IDS/IPS

Os sistemas de detecção e prevenção de intrusões (IDS/IPS) monitoram o tráfego de rede em busca de padrões maliciosos.

Um IDS (Intrusion Detection System) é passivo, ou seja, ele observa o tráfego, compara com assinaturas ou comportamentos conhecidos e emite alertas caso algo suspeito seja detectado. Já um IPS (Intrusion Prevention System) é activo, além de alertar, pode bloquear tráfego e encerrar conexões automaticamente ao identificar uma ameaça.

Muitas firewalls modernos incluem módulos de IDS/IPS, criando uma barreira adicional contra exploits e malware.

- Incidência de alertas em IDS/IPS

De acordo com Stitiawan et al. (2011) citado por (Massunguine, 2022), os sistemas IDS e IPS geram alertas baseados em tráfego de rede ou actividade do sistema. Cada alerta pode ser classificado como:

Verdadeiro Positivo	Verdadeiro Negativo
Falso Positivo	Falso Negativo

Tabela 1: Tipologia de alertas em IDS/IPS

Fonte: Elaborado pelo autor

- **Verdadeiro Positivo:** um ataque real detectado correctamente;
- **Falso Positivo:** um alerta indicando ataque quando, na verdade, o tráfego é benigno;
- **Verdadeiro Negativo:** tráfego benigno correctamente ignorado;
- **Falso Negativo:** um ataque real que passa sem ser detectado.

Os falsos positivos e falsos negativos são erros comuns em sistemas de segurança, como IDS/IPS. Um falso positivo ocorre quando um ataque é sinalizado indevidamente, enquanto um falso negativo representa uma falha grave, pois um ataque real passa despercebido.

Na segurança de redes, falsos positivos podem sobrecarregar os analistas e causar "fadiga de alerta", desviando atenção de ameaças reais, ao passo que falsos negativos aumentam o risco de comprometimento da infra-estrutura (Stallings & Brown, 2020). Estes erros têm impacto operacional significativo, incluindo desperdício de recursos, interrupções desnecessárias e danos reputacionais no caso de ataques não detectados.

2.1.3. Integração com Diretórios e Políticas de Segurança

Para garantir um controlo de acesso mais preciso, os mecanismos de segurança perimetral podem ser integrados a diretórios corporativos e políticas centralizadas de autenticação. Neste cenário, os protocolos AAA (Authentication, Authorization e Accounting, respectivamente) assumem um papel essencial. Segundo (Stallings & Brown, 2020), o modelo AAA envolve três funções principais: a autenticação, que verifica a identidade digital do utilizador; a autorização, que assegura que o utilizador autenticado acede apenas aos recursos permitidos; e a auditoria (ou contabilização), que regista informações sobre a utilização dos recursos.

Ao integrar-se com diretórios centrais como o Active Directory ou o OpenLDAP, os protocolos AAA tornam-se a ponte entre a infra-estrutura de utilizadores e os dispositivos de segurança da rede. Isso permite a aplicação de políticas uniformes de autorização e o registo centralizado de acessos e tentativas de ligação, reforçando assim a rastreabilidade e a conformidade normativa (Stallings & Brown, 2020; Cisco Systems, 2021).

2.2. Governança de TI

A Governança de Tecnologia da Informação (TI) corresponde a um conjunto de estruturas, processos e políticas que visam alinhar a gestão tecnológica aos objectivos estratégicos da organização, assegurando a conformidade, o controlo de riscos e a criação de valor (Weill & Ross, 2004).

No contexto da segurança da informação, a governança estabelece diretrizes fundamentais: define quem decide, quais são as responsabilidades e como os resultados são auditados (ISACA, 2018).

Entre os principais referenciais internacionais, destaca-se o COBIT (Control Objectives for Information and Related Technologies), mantido pela ISACA, que fornece orientações para alinhar a TI ao negócio, através de objectivos de controlo, métricas de desempenho e boas práticas de gestão de riscos e conformidade (ISACA, 2018). Já a norma ISO/IEC

38500 estabelece princípios de boa governança corporativa de TI, recomendados ao nível do conselho de administração, reforçando o uso responsável, eficaz e aceitável da tecnologia nas organizações (ISO, 2022).

Na prática, a governança traduz-se na definição de políticas de acesso, atribuição de papéis e fiscalização de controlos técnicos, sendo operacionalizada por mecanismos como Active Directory, firewalls ou VLANs, que implementam tecnicamente as diretrizes estratégicas (ISO, 2022). Por exemplo, o controlo de identidades e a auditoria de acessos, exigências comuns na certificação ISO/IEC 27001, são concretizados através de diretórios como o AD, FreeIPA ou OpenLDAP, que permitem criar, rever e eliminar contas segundo processos formais (ISO, 2022). Da mesma forma, firewalls e segmentações de rede (como VLANs) reforçam a confidencialidade e a integridade das comunicações internas, cumprindo requisitos definidos nas normas ISO e COBIT.

3. CAPÍTULO III – CASO DE ESTUDO

3.1. Faculdade de Engenharia da Universidade Eduardo Mondlane

A Faculdade de Engenharia é uma unidade orgânica da Universidade Eduardo Mondlane, dotada de autonomia pedagógica e científica no âmbito dos cursos que ministra e de autonomia administrativa, patrimonial e financeira relativamente aos seus próprios recursos dentro dos limites legais. Goza igualmente de autonomia regulamentar e disciplinar dentro dos limites legais.

Foi fundada em 1962 com uma estrutura de chefia centralizada, com cada curso associado a um departamento específico. Logo após a independência, os departamentos assumiram o estatuto de faculdade com um corpo directivo não centralizado, mas com uma coordenação inter-faculdade. Esta estrutura permaneceu até 1980, quando de novo foi mudada (a estrutura) para a situação de 1962. Na altura, em 1962, existiam quatro cursos nomeadamente: Engenharia Civil, Engenharia Eletrotécnica, Engenharia Mecânica e Engenharia Química. No início, os cursos duravam seis anos, sendo os três primeiros anos virados para matérias gerais-básicas e os últimos três anos para disciplinas de Engenharia incluindo disciplinas de gestão.

Em 1970 a duração dos cursos foi encurtada para cinco anos, com os dois primeiros anos virados para matérias gerais- básicas e os últimos dois para matérias de Engenharia. As horas de ensino foram estendidas e as disciplinas tornaram-se tipicamente semestrais, ao contrário de anuais como eram em 1962. Dois novos cursos foram introduzidos em 1970 Engenharia de Minas e Engenharia Metalúrgica. Estes novos cursos não duraram muito visto serem de longa duração (5 e 8 anos respectivamente). Atualmente, a faculdade é composta por dez departamentos, sendo cinco deles académicos e os outros cinco, não académicos:

Departamentos académicos

- Engenharia Civil (DECI);
- Engenharia Eletrotécnica (DEEL);

- Engenharia Mecânica (DEMA);
- Engenharia Química (DEQUI);
- Cadeiras Gerais (DCG).

Não académicos

- Departamento de Património e Manutenção (DPM);
- Departamento do Registo Académico (DRA);
- Departamento de Tecnologias de Informação e Comunicação (DTIC);
- Departamento de Administração e Finanças (DAF);
- Departamento de Informação e Biblioteca (DIB);

É composta também por três centros, nomeadamente:

- Centro de Estudos de Engenharia – Unidade de Produção (CEE-UP);
- Centro de Electrónica e Instrumentação;
- Centros de Regional de Excelência em Estudos de Engenharia e Tecnologia de Petróleo e Gás (CSOGET).

No conjunto dos seus departamentos, a FEUEM oferece oito cursos de licenciatura, nas áreas de:

- Engenharia Civil;
- Engenharia Eléctrica;
- Engenharia Electrónica;
- Engenharia Informática;
- Engenharia Mecânica;
- Engenharia de Gestão Industrial;
- Engenharia Química e;
- Engenharia do Ambiente.

E oferece também cursos de Pós-Graduação:

- Mestrado em Hidráulica e Recursos Hídricos;
- Mestrado em Tecnologia de Alimentos;
- Mestrado em Engenharia de Petróleo;

- Curso preparatório para o Mestrado em Engenharia de Petróleo;
- Curso de Especialização em Segurança no Trabalho.

Os departamentos académicos estão todos separados por edifícios, mas os não académicos (exceptuando o DIB) todos fazem parte de um único edifício denominado Bloco Administrativo.

I.1.1. Visão, Missão, Objectivos e Valores

I. Visão

Ser uma referência nacional, regional e internacional na formação, treinamento e investigação em engenharia.

II. Missão

Desenvolver competências e conhecimentos científicos na área de engenharia e contribuir na formação do homem.

III. Objectivos

- Providenciar uma educação padrão à sociedade e conhecimento científico internacional;
- Providenciar compreensão da importância da tecnologia em áreas como economia, ecologia e sociedade no geral.

IV. Valores

- Liberdade académica;
- Ética e Imparcialidade;
- Responsabilidade;
- Confiança;

- Proatividade;
- Colegialidade;
- Engajamento Social e Comunitário;
- Autonomia Institucional.

3.1.2. Estrutura orgânica

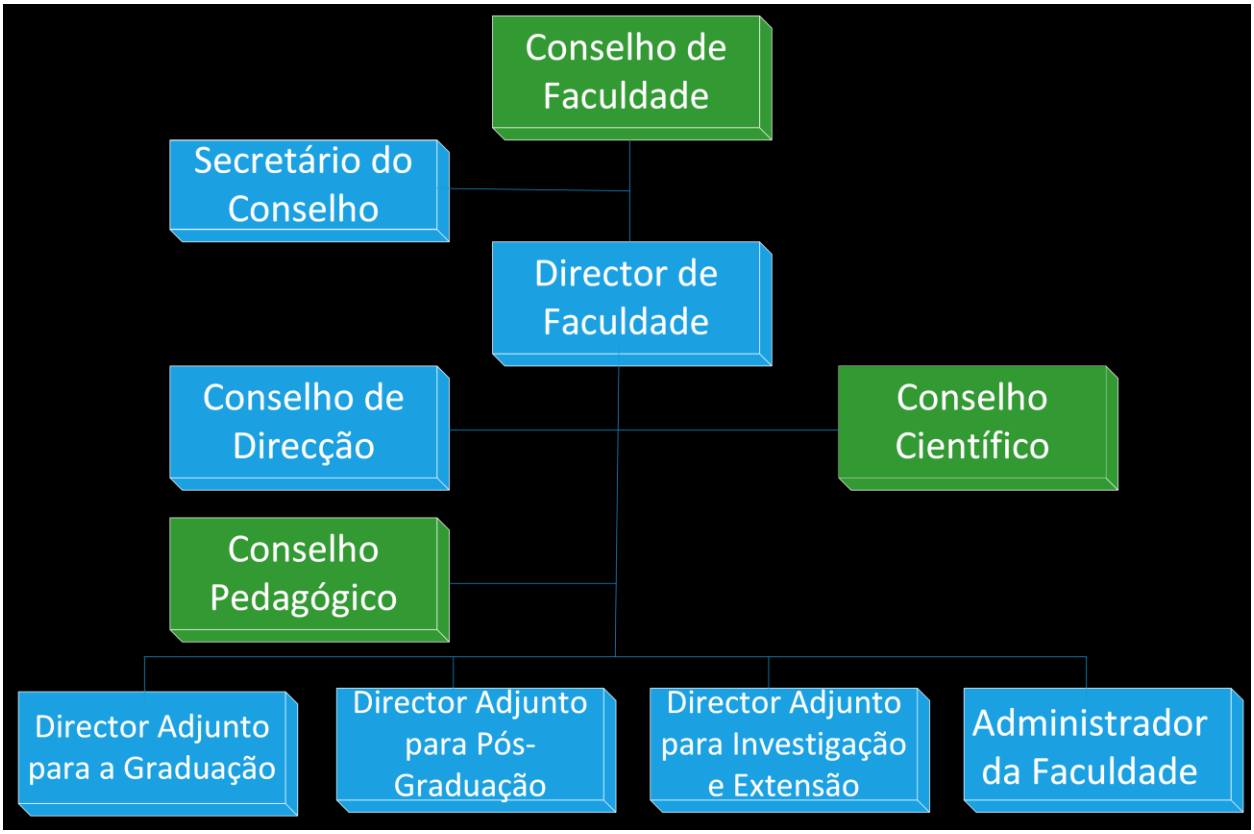


Figura 3-1: Organograma da Faculdade de Engenharia da UEM

Fonte: Adaptada pelo autor

3.1.3. Bloco administrativo

O bloco administrativo da FEUEM abriga majoritariamente departamentos não académicos (exceto o DIB) e o Centro de Estudos de Engenharia – Unidade de Produção (CEE-UP). Embora seja reconhecido como uma unidade administrativa, este bloco também comporta salas de aula para estudantes de Engenharia Civil (regime laboral e pós-laboral), gabinetes de diretores e um laboratório técnico, o que o torna uma estrutura híbrida.

Assim, o bloco representa um caso de estudo singular, onde convivem três realidades operacionais distintas sob uma única infraestrutura de rede:

- Administração institucional sensível, como a DAF e a DRA;
- Ensino especializado, no âmbito dos cursos de Engenharia Civil;
- Produção técnica, representada pelo CEE-UP.

Essa sobreposição de perfis (administrativo, académico e de produção) numa rede plana e sem segmentação viola o princípio do menor privilégio, criando um cenário realista e desafiador para testar modelos de segmentação, controlo de acessos e governança de TI em ambientes multifuncionais.

Inventário resumido dos componentes (activos) mapeados:

- 1 Switch Layer 3 – Actua como ponto central de roteamento básico entre redes;
- 8 Switches Layer 2 – Distribuem rede local, sem funcionalidades de gestão;
- 17 Pontos de Acesso Wi-Fi – Criam cobertura sem fio, com controlo limitado;
- 28 Estações de trabalho (PCs) e 5 Impressoras partilhadas.

A ligação à Internet é fornecida pelo CIUEM, que funciona como provedor de acesso (ISP) da faculdade. No entanto, a única firewall activa encontra-se no CIUEM, e o bloco administrativo recebe conectividade a partir de um Switch L3 situado na sala de servidores do edifício do DEEL (o backbone da rede da instituição).

3.1.4. Constragimentos

Com base no diagnóstico efectuado, a infraestrutura actual da rede do bloco administrativo apresenta constrangimentos técnicos e operacionais que comprometem tanto a segurança quanto a eficiência de serviços críticos. Abaixo estão listadas as limitações identificadas:

a. Infra-estrutura física despadronizada

- Cablagem heterogênea: há mistura de cabos CAT5e e CAT6, o que impacta negativamente a velocidade e estabilidade das ligações.
- Switches não geridos: os 8 switches Layer 2 operam de forma passiva, sem suporte a VLANs ou políticas de controlo (ACLs).
- Subutilização de recursos: 10 firewalls Sophos XGS 126 com licença ativa estão disponíveis, mas não foram implantadas nem configuradas.

b. Gestão de acessos ineficiente

- Autenticação descentralizada: cada computador utiliza contas locais (administrador e utilizador padrão), sem qualquer integração a um diretório central. As credenciais são muitas vezes partilhadas, dificultando a rastreabilidade.
- Partilhas descontroladas: pastas e impressoras são partilhadas informalmente, sem políticas de segurança claras.

Ausência de:

- Permissões baseadas em função (RBAC) para aceder a documentos sensíveis;
- Cotas de armazenamento ou políticas de uso em partilhas;
- Logs de acesso ou histórico de modificações em arquivos críticos.

c. Segurança perimetral insuficiente

- Dependência total do CIUEM: toda a proteção da rede depende de uma única firewall remota, localizada fora do bloco.

- Falta de segmentação: os departamentos operam numa única rede plana (domínio de broadcast único), o que favorece a propagação de ameaças.
- Políticas inexistentes: não há filtragem de conteúdos, nem priorização de tráfego (QoS), nem bloqueios personalizados.

d. Governança frágil

- Documentação desatualizada ou ausente: não há mapeamento recente da topologia ou dos ativos.
- Procedimentos não padronizados: a resposta a incidentes é reativa e baseada em conhecimento informal dos técnicos.

3.1.4.1. Riscos associados

Através dos problemas identificados, podem ser listados os seguintes riscos associados:

Constrangimento	Riscos imediatos	Impacto potencial	Norma violada
Rede plana não segmentada	Propagação de malware entre departamentos	Paralisação de serviços críticos	NIST SP 800-53 (SC-7)
Falta de AD DS	Acessos não autorizados a dados sensíveis	Violação de RGPD e perda de credibilidade institucional	ISSO/IEC 27001 (A.9.2.3)
Switches não geridos	Impossibilidade de implementar VLANs ou QoS	Degradação de desempenho em serviços prioritários	CIS Controls v8 (12.1)
Firewalls não activados	Exposição a ataques internos ou	Roubo de dados académicos ou	ITIL 4 (HVIT.5)

	externos	financeiros	
Redes Wi-Fi abertas	Ataques de intermediário (Man-in-the-Middle)	Interceptação de credenciais ou dados sem trânsito	OWASP IoT Top 10 (M3)

Tabela 2: Riscos associados aos constrangimentos

Fonte: Elaborada pelo autor

Estes constrangimentos são particularmente preocupantes no bloco administrativo devido à:

i. Concentração de dados sensíveis;
ii. Diversidade de usuários;
iii. E dependência de sistemas legados que não evoluíram com as necessidades de segurança.

4. CAPÍTULO IV – PROPOSTA DE SOLUÇÃO

4.1. Análise de soluções para gestão centralizada

Para resolver os problemas de gestão de acessos e segurança, diversas abordagens são propostas na literatura especializada, cada uma com vantagens e limitações que devem ser avaliadas conforme o contexto institucional.

Para a realização da presente análise comparativa, foram consideradas as soluções OpenLDAP, FreeIPA, AD e Samba e de seguida foram definidos critérios (vide a tabela 2), que foram escolhidos de acordo com os seguintes aspectos em torno de sistemas de Gestão Centralizada, alinhadas a boas práticas (ITIL 4 e ISO 27001):

- Custo e licenciamento;
- Funcionalidades essenciais

De forma geral, o que diz respeito às funcionalidades essenciais a observar para a implementação de um sistema de gestão centralizada é: controle de acesso granular, integração, interoperabilidade, logs centralizados, complexidade, escalabilidade, conformidade com normas, tolerância a falhas, suporte técnico e comunidade e custo total de propriedade (TCO).

Contudo, para o presente trabalho foram considerados relevantes os seguintes critérios: Controle de acesso granular (RBAC), integração, Conformidade com normas, Suporte técnico, complexidade e escalabilidade.

Apresentados os aspectos que motivaram a escolha de cada um dos critérios, agora será feita a sua descrição segundo ITIL 4 (Axelos, 2019):

- **Controle de Acesso Granular**

Sistema de permissões que atribui direitos de acesso baseados em funções organizacionais (RBAC). Sua função principal é implementar o princípio do menor privilégio, limitando acessos apenas ao estritamente necessário. Como solução centralizada, é fundamental para garantir segurança de dados, conformidade com

regulamentações (LGPD e ISO 27001) e auditoria eficiente de acessos em ambientes com múltiplos usuários.

- **Integração com Sistemas Existentes**

Capacidade de interoperabilidade com a infra-estrutura tecnológica já implementada na instituição. Permite sincronização automática de dados entre sistemas diversos (acadêmicos, administrativos, de autenticação e etc). Na gestão centralizada, elimina silos de informação, reduz custos operacionais e melhora a eficiência ao evitar redundâncias e inconsistências nos dados institucionais.

- **Conformidade com Normas**

Refere-se a adequação a padrões e regulamentações internacionais de segurança e gestão de TI (ISO 27001 e ITIL). Garante que os processos implementados sejam auditáveis, padronizados e alinhados com melhores práticas do setor. Para instituições de ensino, assegura proteção de dados sensíveis, mitigação de riscos legais e sustentabilidade da solução a longo prazo.

- **Suporte Técnico**

Disponibilidade de assistência especializada para resolução de problemas e manutenção do sistema. Inclui suporte contratual, comunitário ou interno. Em ambientes centralizados, é crucial para garantir continuidade operacional, especialmente em sistemas críticos, onde o tempo de inatividade gera impactos significativos.

- **Complexidade**

Grau de dificuldade para implementação, configuração e manutenção da solução. Deve ser balanceada com a capacidade técnica da equipe e recursos disponíveis. Sistemas excessivamente complexos podem comprometer a adoção efetiva e aumentar custos ocultos de capacitação e suporte.

- **Escalabilidade**

É a capacidade da solução de expandir seu desempenho e capacidade conforme o crescimento da demanda institucional. Em ambientes educacionais, onde o número de

usuários e serviços tende a aumentar, garante que a infra-estrutura não precise ser substituída prematuramente, protegendo o investimento inicial.

- **Custos (Iniciais e Totais de Propriedade)**

São o investimento financeiro necessário para aquisição, implementação e operação contínua da solução. O TCO (Total Cost of Ownership ou Custo Total de Propriedade, em português) deve considerar licenças, hardware, treinamento, manutenção e custos de oportunidade. Para instituições de ensino, a análise precisa equilibrar orçamentos limitados com necessidades de longo prazo, evitando soluções com baixo custo inicial, mas com altas despesas operacionais.

Após o a descrição dos critérios considerados relevantes, segundo ITIL 4, segue abaixo a tabela comparativa. Na tabela abaixo, os critérios são valorados como: Alto (atende plenamente aos requisitos da FEUEM), Médio (requer adaptações ou tem limitações) e Baixo (não atende ou exige mudanças radicais), com exceção do critério custo que assume valores: grátis ou **comercial**.

Critérios	**Solução**			
	AD	**OpenLDAP**	**FreeIPA (Red Hat)**	**Samba**
Controle de acesso (RBAC)	Alto	Médio	Alto	Médio
Integração	Alto	Baixo	Médio	Médio
Conformidade	Alto	Médio	Alto	Médio
Suporte Técnico	Alto	Baixo	Alto	Baixo
Complexidade	Alto	Baixo	Médio	Médio
Escalabilidade	Alto	Médio	Alto	Médio
Custo	Comercial	Grátis	Grátis	Grátis

Tabela 3: Análise comparativa de soluções de GC

Fonte: Elaborada pelo autor

As cores representam a avaliação em relação a valoração de cada critério de acordo com os objectivos que se pretendem alcançar, nomeadamente o vermelho para Mau, amarelo para Normal e verde para Bom.

	Mau	Normal	Bom
AD DS	0	1	6
OpenLDAP	3	3	1
FreeIPA	0	2	5
Samba	1	5	1

Tabela 4: Resumo da análise comparativa

Fonte: Elaborada pelo autor

Pela análise comparativa apresentada, chegou-se à conclusão de que a solução que atende integralmente aos requisitos atuais da infra-estrutura de rede corporativa da Faculdade de Engenharia da Universidade Eduardo Mondlane é Active Directory da Microsoft, com desempenho alto em 6 dos 7 critérios relevantes.

Desta forma, o autor propõe a sua implementação.

A seleção da solução ideal foi guiada por três critérios fundamentais, ordenados por impacto directo na operacionalidade e segurança da infra-estrutura, respectivamente: (1) integração com sistemas existentes, (2) controle de acesso granular e (3) complexidade (implementação e uso).

A integração com sistemas existentes emergiu como critério primordial porque a eficácia de qualquer solução de gestão centralizada depende de sua capacidade de comunicar-se nativamente com a infra-estrutura atual – toda infra-estrutura atual da faculdade usa o sistema operacional Windows.

O controle de acesso granular foi elevado à segunda posição pelo seu papel crítico na proteção de dados académicos e financeiros, alinhando-se ao RGPD.

A complexidade, embora menos determinante que os anteriores, foi decisiva para descartar opções que precisassem de capacitação extensiva da equipa do DTIC.

Embora o custo-benefício seja um critério universal, a sua aplicação favoreceu o AD DS devido ao contexto institucional único: licenças existentes (a instituição já possui licenças do Windows Server 2022) e expertise em Windows – é o sistema operacional dominante, ou seja, em uso. Soluções teoricamente mais baratas como OpenLDAP teriam um TCO superior quando considerados treinamentos e desenvolvimento.

4.2. Análise de soluções para segurança perimetral

A segurança perimetral é um pilar crítico no modelo proposto, complementando a gestão centralizada de acessos via Active Directory. A ausência de uma firewall dedicado no bloco administrativo cria vulnerabilidades graves, como: tráfego não filtrado entre departamentos, exposição a ataques externos e a falta de monitorização proactiva.

Contudo, diferentemente da análise realizada para a gestão centralizada (onde múltiplas soluções foram comparadas), não se justifica uma avaliação comparativa de firewalls, pois a instituição já possui equipamentos Sophos XGS 126 licenciados e prontos para implantação.

Esta decisão baseia-se em dois princípios fundamentais:

i. Viabilidade económica imediata

As firewalls Sophos XGS já foram adquiridos, eliminando custos de aquisição, portanto, não há necessidade de investimento adicional em hardware e licenças.

ii. Adequação técnica corporativa

O Sophos XGS é uma firewall de última geração (Next-Generation Firewall – NGFW) com funcionalidades essenciais para o contexto académico:

- Segmentação de rede via VLANs (isolamento lógico entre departamentos);
- Inspeção profunda de pacotes (DPI) e deteção de intrusões (IDS/IPS);
- Filtragem de aplicações (e.: bloquear streaming em redes administrativas);

- Integração nativa com Active Directory (políticas baseadas em grupos de utilizadores).

Soluções que podem ser consideradas alternativas como FortiGate e Palo Alto, não trariam benefícios adicionais significativos para as necessidades específicas da instituição. Uma análise comparativa tradicional (Sophos XGS vs. FortiGate vs. Palo Alto) prolongaria desnecessariamente o trabalho, ou seja, seria redundante.

Com essa observação, a segurança perimetral será garantida através da implementação das firewalls Sophos XGS já disponíveis. A integração com o Active Directory assegurará um modelo unificado de governança e segurança, tornando a rede administrativa resiliente a ameaças internas e externas.

4.3. Descrição da solução proposta

4.3.1. Active Directory (AD)

O Active Directory é um serviço de diretório da Microsoft, integrado no Windows Server, concebido para gerir redes corporativas de forma centralizada. Atua como uma base de dados hierárquica que armazena informações sobre utilizadores, computadores, grupos e políticas, facilitando a administração e a autenticação em ambientes de rede.

O AD utiliza protocolos como LDAP, Kerberos e DNS, permitindo autenticar e autorizar acessos, aplicar políticas de segurança e gerir software. Inicialmente denominado apenas Active Directory, a partir do Windows Server 2008 passou a ser conhecido como Active Directory Domain Services (AD DS), mantendo-se como componente essencial para a gestão segura e eficiente de redes empresariais.

4.3.1.1. Componentes do Active Directory

Segundo (Francis, 2021), os componentes do Active Directory podem ser divididos em duas categorias: Componentes lógicos e componentes físicos.

a) Componentes lógicos

Os componentes lógicos definem como os dados são estruturados, gerenciados e organizados. Esses componentes lógicos ajudam a organizar usuários, computadores e outros recursos de forma a facilitar o gerenciamento e a escalabilidade em grandes ambientes. Dentre muitos que existem, os principais que vão ser abordados são: Domínio, Árvore de domínio, Floresta e Unidade Organizacional.

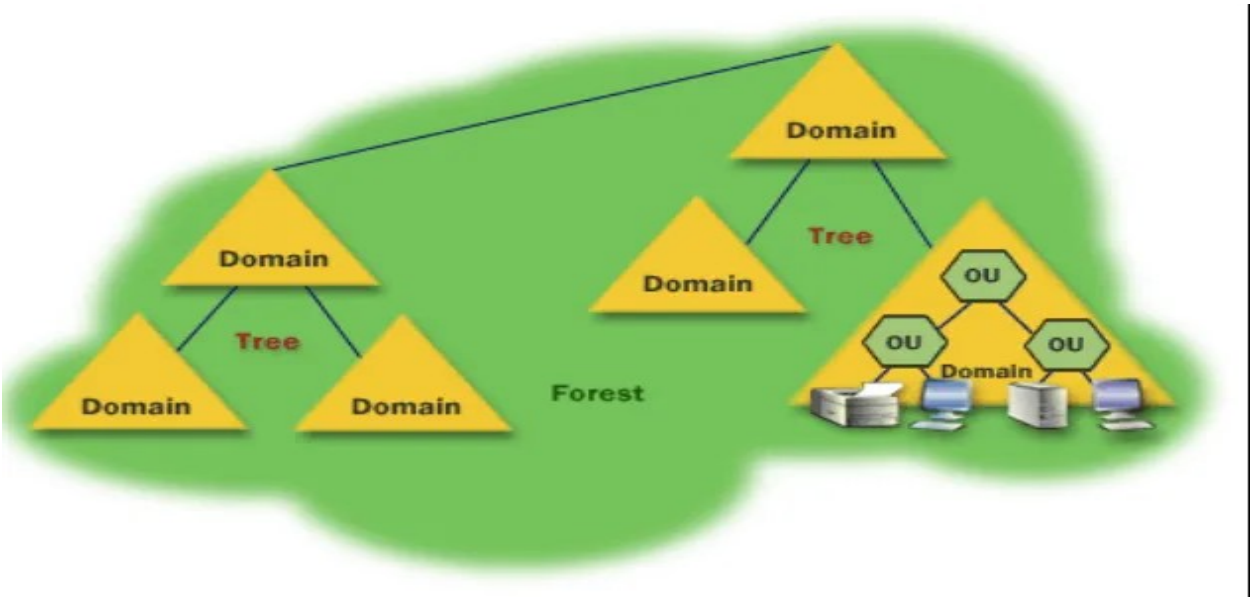


Figura 4-1: Componentes Lógicos de AD DS

Fonte: Adaptado de Wikipedia

- Floresta (Forest)

A floresta constitui a unidade lógica de mais alto nível na arquitectura do Active Directory Domain Services (AD DS), agregando uma ou mais árvores de domínios inter-relacionadas por relações de confiança transitivas. Representa um limite de segurança e partilha um esquema comum (schema), que define a estrutura dos objectos e os atributos permitidos. Um componente essencial da floresta é o Catálogo Global, responsável por armazenar uma réplica parcial e indexada de todos os objectos da floresta, possibilitando pesquisas rápidas e eficientes entre domínios distintos. As florestas são particularmente relevantes em contextos de integração organizacional

(como fusões e aquisições) ou quando se impõe a separação de ambientes com requisitos de segurança autónomos.

- Domínio (Domain)

Um domínio constitui a unidade lógica fundamental, operando como um contentor hierárquico que agrega objectos, tais como utilizadores, computadores e grupos, sob um único espaço de nomes DNS. Este estabelece um limite administrativo e de segurança, no qual se aplicam políticas de grupo e configurações de forma centralizada e consistente.

Cada domínio é identificado por um nome DNS exclusivo (por exemplo, engenharia.uem.mz) e é gerido por um ou mais controladores de domínio, responsáveis por armazenar a base de dados do diretório (NTDS.dit) e por processar autenticações e autorizações. Em ambientes de grande escala, a criação de múltiplos domínios permite a segmentação lógica da infra-estrutura, promovendo uma gestão descentralizada e mais granular por equipas administrativas distintas.

- Árvore de Domínio (Domain Tree)

Uma árvore de domínios é uma estrutura hierárquica composta por múltiplos domínios interligados que partilham um espaço de nomes DNS contíguo. A partir de um domínio raiz (por exemplo, engenharia.uem.mz), podem ser criados subdomínios como ***dtic.engenharia.uem.mz*** ou ***deel.engenharia.uem.mz***, mantendo uma organização lógica coerente. Os domínios pertencentes à mesma árvore estabelecem relações de confiança transitivas, permitindo o acesso autenticado entre domínios sem requerer novas credenciais. Esta topologia suporta a escalabilidade da infra-estrutura de diretório, assegurando a integridade da gestão centralizada e o isolamento administrativo quando necessário.

- Unidades Organizacionais (Organizational Units)

As OUs constituem elementos hierárquicos dentro de um domínio Active Directory, utilizados para agrupar logicamente objectos relacionados, como utilizadores, computadores e grupos, com o objectivo de simplificar a gestão administrativa. Permitem a delegação granular de permissões e a aplicação segmentada de Políticas de Grupo (GPOs), ajustadas a contextos funcionais distintos, como departamentos ou funções específicas. Por exemplo, uma OU dedicada ao departamento Financeiro pode ter definições de segurança mais restritivas face a uma OU destinada a utilizadores genéricos. A concepção da hierarquia de OUs deve obedecer a critérios de clareza e eficiência operacional, evitando estruturas excessivamente complexas que comprometam a escalabilidade e a manutenção administrativa.

b) Componentes físicos

Os componentes físicos referem-se à infra-estrutura que garante que o serviço de diretório opere com eficiência em uma rede. Esses componentes se preocupam com a forma como o Active Directory é distribuído e replicado em vários locais. São três componentes que se discutirão, segundo o (Francis, 2021).

- Controlador de Domínio (Domain Controller)

O controlador de domínio é o servidor responsável por alojar o serviço AD DS, mantendo uma cópia da base de dados do diretório (NTDS.dit) e desempenhando funções críticas de autenticação, autorização e aplicação de políticas de grupo.

Internamente, integra o Kerberos KDC, que gere a emissão de tickets para autenticação segura, e mecanismos de replicação multimestre que asseguram a consistência dos dados entre múltiplos DCs no domínio. Em cenários de segurança diferenciada, pode-se utilizar um RODC, que permite autenticação local com uma réplica parcial e não modificável do diretório, ideal para ambientes remotos ou sucursais com restrições operacionais e maior exposição ao risco.

- Catálogo Global (Global Catalog)

O Catálogo Global é um serviço essencial que optimiza consultas em ambientes com múltiplos domínios, armazenando atributos-chave de todos os objectos na floresta. Além disso, o GC desempenha um papel crucial durante o processo de início de sessão, especialmente em florestas com vários domínios, garantindo que os utilizadores sejam autenticados rapidamente mesmo quando os seus dados estão distribuídos.

- Sites e Sub-redes

São representações de localizações físicas de rede que optimizam o tráfego de replicação (dados são replicados primeiro dentro do mesmo site) e autenticação local (utilizadores autenticam-se no DC mais próximo).

4.3.1.2. Serviços do Active Directory

Os serviços controlam grande parte da actividade que ocorre no seu ambiente de TI. Em particular, eles garantem que cada pessoa seja quem afirma ser (autenticação), geralmente verificando o ID de usuário e a senha inseridos, e permitem que acessem apenas os dados que têm permissão para usar (autorização).

Segundo (Francis, 2021), os serviços principais do AD são:

1) **Serviços de Domínio do Active Directory (AD DS)**

Os AD DS constituem o componente central de gestão de identidades, autenticação e autorização em infra-estruturas Windows. Funcionando como controlador de domínio, o AD DS autentica utilizadores utilizando preferencialmente o protocolo Kerberos e, de forma legada, o NTLM, emitindo um token de segurança com os identificadores de utilizador (SID) e respectivos grupos para controlo de acesso.

A base de dados NTDS.dit armazena os objectos do directório, e as GPOs permitem a imposição centralizada de configurações de segurança e restrições operacionais a nível de domínio. A integração com DNS é essencial, uma vez que registos SRV suportam a descoberta automática de serviços críticos, como controladores de domínio. Em ambientes mais complexos, o AD DS pode ser estendido com Active Directory Certificate Services (AD CS), para emissão de certificados digitais, e Active Directory Federation Services (AD FS), para autenticação federada entre domínios ou organizações.

2) Serviços de Diretório Leve do Active Directory (AD LDS)

É uma implementação independente e modular do AD, projectada especificamente para cenários onde aplicações exigem serviços de diretório leves, mas não requerem a complexidade de um domínio completo do AD DS, ou seja, é um serviço de diretório leve e autónomo, ideal para aplicações que não requerem a infra-estrutura completa do AD DS. Oferece esquema personalizável, múltiplas instâncias e isolamento de segurança, sendo usado em sistemas de RH, portais web ou migrações híbridas. Não substitui o AD DS, mas complementa-o em cenários específicos

3) Serviços de Certificados do Active Directory (AD CS)

É um pilar crítico da infra-estrutura de segurança do AD, permitindo que organizações implementem infra-estruturas de chave pública (PKI) integradas ao seu ambiente de rede. O AD DS vai além da simples emissão de certificados: ele estabelece um framework de confiança hierárquica, onde autoridades certificadoras (CAs) emitem credenciais digitais que validam identidades, protegem comunicações e garantem a integridade de dados.

Em linhas gerais, é a solução da Microsoft para PKI integrada ao AD DS, emitindo certificados digitais que autenticam utilizadores, encriptam dados e validam integridade. Centraliza a gestão de CAs, elimina dependência de senhas e suporta cenários como acesso seguro, assinatura digital e encriptação de discos.

4) Serviços de Federação do Active Directory (AD FS)

É um serviço de federação de identidades que permite Single Sign-On (SSO) entre organizações e aplicações heterogéneas, funcionando como um intermediário de confiança (trust broker) entre Identity Providers (IdPs) e Relying Parties (RPs).

Em resumo, é o serviço da Microsoft para SSO federado, permitindo que utilizadores autenticados no AD DS acedam a recursos externos sem reinserir credenciais. Baseia-se em protocolos como SAML e OAuth, garantindo segurança e interoperabilidade. Ideal para ambientes híbridos e colaborações interorganizacionais.

5) Serviços de Gestão de Direitos do Active Directory (AD RMS)

É uma solução de proteção de dados que vai além da simples encriptação, permitindo às organizações aplicar políticas de uso persistentes a documentos confidenciais, mesmo após estes deixarem a rede corporativa. Opera através de um modelo de gestão de direitos de informação (IRM) baseado em certificados e licenças, garantindo que apenas utilizadores autorizados possam aceder, editar, imprimir ou partilhar ficheiros sensíveis. Integra-se ao AD CS para autenticação baseada em certificados e é essencial para cumprir regulamentos como o GDPR. Não substitui encriptação tradicional, mas complementa-a com controlo granular de utilização.

Segundo (Francis, 2021), o AD DS é a espinha dorsal da infra-estrutura de TI em organizações que utilizam tecnologias Microsoft, fornecendo funcionalidades essenciais como: Autenticação e autorização centralizada (via Kerberos e NTLM), GPOs para controle de configurações, Replicação distribuída para alta disponibilidade e Estrutura hierárquica (domínios, OUs e Objectos). A seguir far-se-à uma descrição sucinta de cada uma delas:

- **Autenticação e Autorização Centralizada (Kerberos e NTLM)**

O AD DS implementa autenticação centralizada baseada principalmente em Kerberos, complementado pelo legado NTLM. O Kerberos utiliza um sistema de tickets, emitidos

pelo KDC, que evita o envio de credenciais em texto claro e permite autenticação mútua, delegação segura e proteção contra replay attacks (Francis, 2021).

O utilizador recebe um TGT, válido por tempo limitado, que é trocado por Service Tickets (STs) ao aceder a recursos específicos. Já o NTLM, considerado obsoleto e vulnerável a ataques como Pass-the-Hash, deve ser desativado sempre que possível, conforme recomenda Francis, para evitar riscos de segurança desnecessários.

- **Políticas de Grupo para Gestão Centralizada**

De acordo com (Francis, 2021), as Políticas de Grupo (Group Policy Objects – GPOs) constituem o principal mecanismo para assegurar a conformidade normativa e a padronização de configurações em ambientes Microsoft Windows.

Cada GPO pode agregar milhares de definições organizadas em dois blocos funcionais: Configuração do Computador, aplicada na fase de arranque do sistema, e Configuração do Utilizador, aplicada no momento da autenticação. Entre os casos de uso avançado destacam-se:

- Segurança reforçada, com a aplicação de políticas como o Local Administrator Password Solution (LAPS) para rotação automática e segura de senhas locais;
- Gestão de aplicações, através de mecanismos como AppLocker ou Software Restriction Policies (SRP), que permitem controlo granular sobre a execução de software;
- Integração em ambientes híbridos, onde as GPOs são estendidas a dispositivos fora do domínio local através de soluções como o Microsoft Intune.

Contudo, a utilização intensiva de GPOs está sujeita à complexidade acumulada, especialmente em domínios com múltiplas Unidades Organizacionais (OUs) e heranças sobrepostas. Conflitos de políticas podem surgir e exigir o uso de ferramentas como Resultant Set of Policy (RSoP) ou GPResult para análise de aplicação efectiva. Para mitigar estes riscos, recomenda-se a adoção de uma estrutura hierárquica de OUs bem definida, aliada à documentação sistemática de cada GPO por meio de comentários técnicos descritivos.

- **Replicação Distribuída para Resiliência Operacional**

O mecanismo de replicação do AD DS é analisado por Francis como "um equilíbrio cuidadoso entre consistência imediata e tolerância a falhas". A replicação multi-master permite que qualquer DC aceite alterações, que são depois propagadas através de um sistema sofisticado que inclui: Actualização de Sequência de Números – identificadores únicos para cada alteração, Propagation dampening – prevenção de loops de replicação e Compressão RPC – optimização para ligações WAN. É importante frisar que a topologia de sites, deve refletir a estrutura física da rede.

- **Arquitectura Hierárquica (Domínios, OUs e Objectos)**

Francis descreve a estrutura do AD DS como "um sistema orgânico que deve espelhar a organização que serve", apresentando um modelo de design com cinco princípios:

i. Princípio do Menor Privilégio: delegação granular usando OUs;
ii. Modelo de Segurança Baseado em Funções (RBAC): grupos aninhados com nomes padronizados;
iii. Separação de Serviços: OUs dedicadas para servidores (Tiering Model);
iv. Documentação Dinâmica: atributos personalizados para metadados;
v. Preparação para Expansão: espaço de nomes DNS planeado para o crescimento.

A beleza do AD DS está na sua flexibilidade, pode ser tão simples ou complexo quanto a organização exigir, mas sempre requer planeamento antecipado meticuloso.

2.1.2.2. Características do AD

As suas características abrangem desde autenticação segura até à organização hierárquica de recursos, tornando-o essencial para infra-estruturas de TI modernas. Abaixo, estão apresentadas de forma resumida, as suas características principais com exemplos e contextos adicionais:

Características	Descrição
Gestão Centralizada	Centraliza usuários, computadores e recursos, simplificando a administração.
Autenticação e Autorização	Verifica credenciais e controla o acesso a recursos com base em permissões.
Estrutura Hierárquica	Organiza em florestas, árvores, domínios e UOs para gestão eficiente.
Banco de Dados	Armazena informações sobre objectos, adequados para grandes organizações.
Escalabilidade	Gerencia milhões de objectos, adequados para grandes organizações.
Segurança	Aplica políticas de segurança, como senhas complexas e autenticação multifactor.
Integração	Integra-se com serviços Microsoft e terceiros, como Exchange Server.
Flexibilidade	Esquema extensível para adicionar propriedades e valores personalizados.
Replicação	Replicação multi-master garantida em múltiplos domínios de domínio.
Catálogo Global	Contém informações de todos os objectos, facilitando buscas em múltiplos domínios.
Mecanismo de Consulta e Índice	Permite publicar e localizar objectos e propriedades por aplicações e usuários.
Administração Baseada em Políticas	Usa políticas de grupo para gerenciar redes complexas de maneira uniforme.

Tabela 5: Características de AD DS

Fonte: Elaborada pelo autor

4.3.2. Firewall Sophos XGS

O Sophos XGS 126 é uma firewall de próxima geração (NGFW) desenvolvido pela Sophos, uma empresa líder em soluções de cibersegurança. Vai além das funções tradicionais de filtragem de tráfego, incorporando capacidades avançadas como inspeção profunda de pacotes (DPI), sistema de prevenção de intrusões (IPS), controlo de aplicações, inteligência de ameaças e descriptografia TLS. É projectado para pequenas e médias empresas (PMEs) e escritórios de filiais, este dispositivo combina alto desempenho com funcionalidades avançadas de segurança, incluindo inspeção de tráfego criptografado, prevenção de intrusões e suporte a SD-WAN. É ideal para redes com 50 a 100 utilizadores, oferecendo proteção robusta contra ameaças cibernéticas modernas.

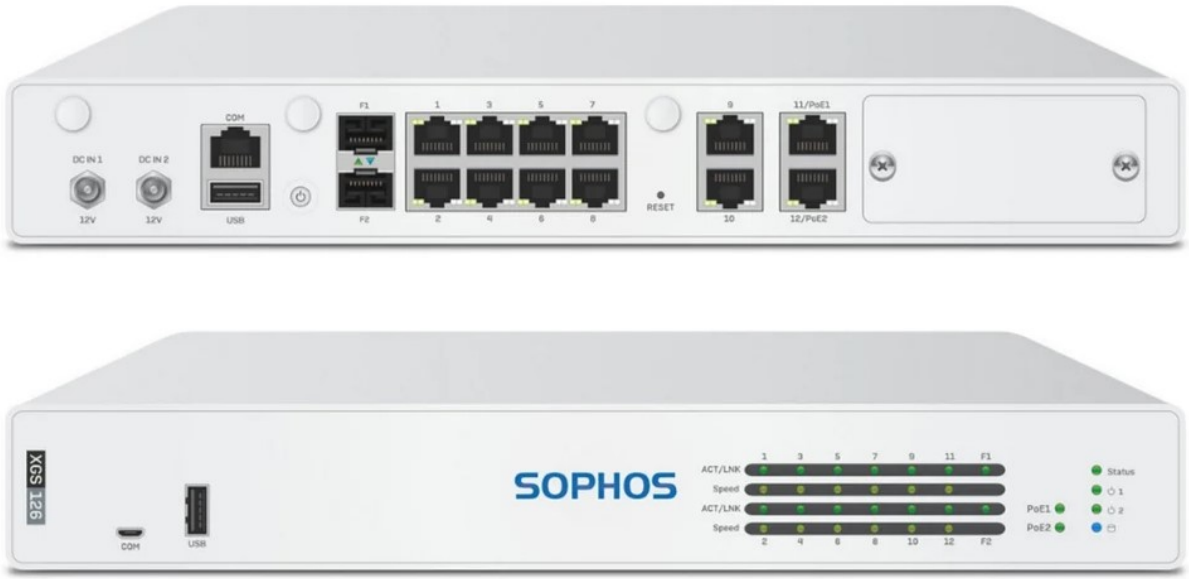


Figura 4-2: Hardware de Firewall Sophos XGS 126

Fonte: Ajustado do site https://www.indiamart.com/proddetail/firewall-sophos-xgs-126

a) Ciclo de vida

Fim de Venda (EOS): é a data em que se para de vender o produto ou vende-se somente enquanto durar o estoque. A Sophos anunciou oficialmente o fim de vendas para todos os aparelhos da 1ª geração, incluindo o XGS 126, em 14 de Abril de 2025.

Fase de Suporte Após EOS (Post-EoS): é o período em que não se vende mais o produto, mas ele ainda conta com suporte completo. Ao final desta fase, os clientes devem planejar a atualização para um modelo mais recente. A partir de 15 de Abril de 2025 até 30 de Setembro de 2030, o XGS 126 continua recebendo suporte técnico, atualizações de firmware e RMA normalmente, mesmo não estando mais à venda.

Renovação Final é a última oportunidade para solicitar assinaturas de renovação. A renovação final padrão é um ano antes da data de fim de vida útil.

Fim de Vida Útil (EoL): ocorre quando o suporte ao produto termina. Os clientes não devem usar o produto após o EOL. A data final de vida útil do XGS 126 (fim de suporte, atualizações e RMA) está prevista para 30 de Setembro de 2030.

A sophos tem feito actualizações de firmware do Sophos XGS (SFOS) para o modelo 126, desde o lançamento da linha XGS em 2017, versão SFOS17.0.0 GA até as versões recentes como SFOS 21.0 MR1 – aprimoramentos de VPN IPSec/SSL, correções críticas de estabilidade aos 31/03/2025 e SFOS21.5 GA – integração com NDR Essentials, melhorias na proteção DNS aos 02/06/2025.

b) Modelo de licenciamento

O sophos inclui uma licença básica, que é necessária para todos os firewalls virtuais e de hardware. A seguir são descritas as funcionalidades que cada pacote oferece.

Pacote	Funcionalidades
Base (grátis)	Sistema de Rede e SD-WAN, Proteção e Desempenho, VPN e Emissão de relatórios.

Standard Protection	Base, Proteção de Rede, Proteção Web e Apoio reforçado
Xstream Protection	Base, Standard Protection, Proteção de Dia Zero (sandaboxing), Proteção de DNS e Orquestração central.
Epic Protection	Adiciona proteção de E-mail e de Servidor Web .

Tabela 6: Tipos de pacotes de licenciamento do Sophos XGS 126

Fonte: Elaborada pelo autor

4.3.2.1. Características

O Sophos XGS possui as seguintes características:

- Factor de forma: desktop, compacto e ideal para ambiente de escritório;
- Slots (Portas máximas): 14/1 (14 portas no total);
- Wi-Fi: suporta Wi-Fi 5 (802.11ac), com opção para um segundo módulo Wi-Fi;
- Componentes substituíveis: inclui opções para segundo suprimento de energia, módulos 3G/4G/5G e Wi-Fi;
- Eficiência energética: embora seja um modelo de primeira geração, a linha XGS prioriza a eficiência energética, possibilitando, 30W (ocioso) / 59W (pico), fonte externa com opção redundante.

O Sophos XGS 126 é equipado pelos seguintes componentes:

Categoria	Descrição
Arquitetura de Hardware	Processador dual: 2.6GHz dual-core AMD Ryzen Embedded R1600 com Xstream Flow Processor para uma relação custo-desempenho superior.
Conectividade	12 portas Ethernet 1 Gbps (2 com PoE+ 30W); 2 portas SFP 1 Gbps (fibra); 1 USB 2.0 (frente);

	1 USB 3.0 (traseiro); 1 Micro-USB (gerenciamento); Suporte a FTTH/FTTP ou modem VDSL opcional.
Redundância	Opção para segunda fonte de alimentação (2 portas de fonte), garantindo confiabilidade.
Módulos opcionais	Wi-Fi integrado; Segundo módulo de rádio Wi-Fi; Conectividade celular (3G/4G/5G).
Tecnologia	Processadores Xstream Flow para aceleração de tráfego e inspeção TLS eficiente.
Armazenamento	SSD 64 GB dedicado para logs e quarentena de ameaças.

Tabela 7: Descrição de componentes de hardware do Sophos 126

Fonte: Elaborada pelo autor

4.3.2.2. Funcionalidades

As suas funcionalidades são vastas, sendo algumas disponibilizadas de acordo com o tipo de licença em uso. Para o projecto corrente que é licenciamento básico, tem-se:

a) Firewall (Stateful Inpection): inspeção de pacotes em estado (stateful), permitindo criar regras de filtragem de tráfego entre interfaces e zonas;
b) NAT: permite traduzir endereços IP internos para IPs públicos e vice-versa. Suporta SNAT, DNAT e Full NAT;
c) Roteamento: suporte a roteamento estático e dinâmico (OSPF, BGP, RIP), para gerenciar o tráfego entre sub-redes.
d) VPN (IPsec, SSL, L2TP): túneis seguros site-to-site e acesso remoto: IPsec, SSL VPN e L2TP;

e) IDS/IPS: módulo básico de detenção e bloqueio de ameaças em camada de rede, baseado em assinaturas fornecidas pela SophosLabs;
f) DoS/DDoS Protection: proteção contra ataques de negação de serviço, identificando e limitando tráfego malicioso de alto volume;
g) Autenticação de usuários: integração com Active Directory, LDAP, RADIUS e TACACS+, permitindo aplicar políticas de acesso por identidade de usuário/grupo;
h) Failover e Balanceamento de Links: suporte a múltiplas conexões WAN com failover automático e balanceamento de carga para manter alta disponibilidade;
i) SD-WAN (básico): capacidade de roteamento inteligente entre links WAN, com balanceamento de carga e failover baseado em latência/jitter;
j) VLANS (802.1Q Taagging): criação e gerenciamento de VLANs: interfaces virtuais, atribuição de IP/DHCP, e aplicação de regras de firewall entre VLANs e zonas.
k) Logs e Relatórios Básicos: armazenamento local de logs, relatórios gerados na GUI para análise de eventos, tráfego e alertas simples.
l) Administração via Web Interface: interface gráfica (GUI) para configuração, monitoramento e visualização de status em tempo real.
m) CLI (Linha de comando): acesso via SSH para administração avançada e execução de comandos de diagnóstico/configuração.

Todas as funcionalidades acima estão disponíveis sem custo adicional na Base License.

4.3.2.3. Desempenho (Throughput e Métricas)

Os valores de desempenho referem-se às capacidades de hardware do Sophos XGS 126, mas nem todas podem ser alcançados usando apenas a licença básica. A licença não “desliga” ou limita esse desempenho, ela apenas garante ou retira o acesso à funcionalidade.

Métrica	Valor Aproximado	Observação
Firewall Throughput	10500 Mbps	Desempenho máximo para filtragem stateful de tráfego não criptografado.
Firewall IMIX	5250 Mbps	Throughput em ambiente realista (mistura de tamanhos de pacotes e protocolos).
IPS Throughput	3250 Mbps	Taxa de inspeção IPS ativo (assinaturas básicas), visto que o módulo IDS/IPS faz parte da Base License.
IPsec VPN Throughput	5500 Mbps	Velocidade máxima de túneis IPsec site-to-site ou remoto, sem encapsulamento extra para inspeção avançada.
TLS Inspection Throughput	800 Mbps	Inspeção de tráfego TLS/SSL (decriptação e inspeção IPS simples). Nota: não inclui verificação de malware dentro de sessões TLS.

Tabela 8: Métricas de desenpenho do Sophos XGS

Fonte: Elaborada pelo autor

4.3.2.4. Arquitetectura

Segundo a documentação oficial, o Sophos XGS 126 é uma firewall baseado em zona. Quando se fala de zonas no Sophos XGS Firewall, refere-se a um grupo lógico de redes onde o tráfego se origina ou se destina. Cada interface está associada a uma única zona, o que significa que o tráfego pode ser gerenciado entre as zonas, em vez de por interface ou rede, simplificando a configuração, vide a figura 14.

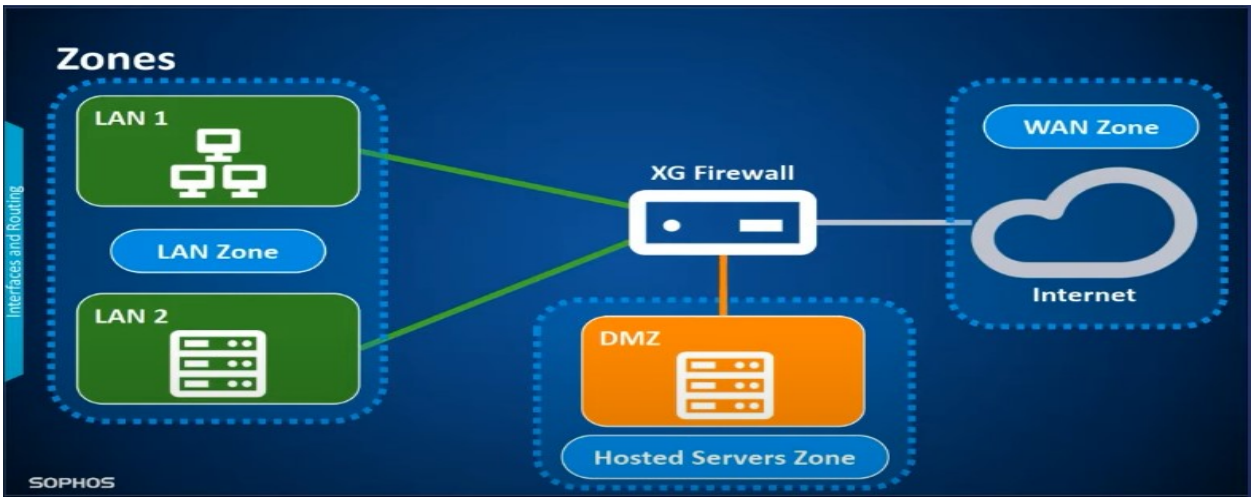


Figura 4-3: Representação de zonas no Sophos XGS

Fonte: Fagner Nascimento
(https://youtu.be/cTcNP-uaP6s?list=PLDmzUqrUykTn_zpuYglnyc5ekyoPDxuEZ)

As interfaces e zonas não são equivalentes; várias interfaces podem ser associadas a uma zona e cada zona pode ser composta por várias redes. Por padrão não existe comunicação directa entre as zonas a não ser que o administrador da rede permita isso através de regras de firewall.

4.3.3. Integração com Active Directory

A integração com o Active Directory Domain Services (AD DS) no Sophos XGS é nativa, ou seja, o dispositivo já inclui internamente um conector LDAP/LDAPS capaz de estabelecer comunicação directa com o domínio.

Basta configurar, na interface administrativa, o endereço do controlador de domínio (host e porta) e informar as credenciais de uma conta de leitura do AD. A partir desse momento, o XGS sincroniza automaticamente usuários, grupos de segurança e unidades organizacionais, permitindo que as políticas de firewall, filtro de conteúdo web e VPN sejam definidas com base em identidades ou grupos do diretório.

Além disso, o Sophos XGS oferece, de forma integrada, mecanismos de Single Sign-On, como o Agentless SSO ou o SSO Agent, que correlacionam o login do Windows ao

endereço IP da estação de trabalho, sem a necessidade de solicitações de autenticação adicionais. Dessa forma, toda a configuração é realizada por meio do próprio firmware, sem requerer componentes externos ou desenvolvimento de scripts, o que simplifica a implantação e garante uma experiência transparente ao usuário.

4.4. Desenvolvimento da solução proposta

4.4.1. Descrição do cenário proposto para o cenário de implementação

A solução visa suprir as necessidades de isolamento de tráfego, autenticação centralizada, controlo de acessos e governança da rede do bloco administrativo da FEUEM. Para isso, adota-se uma arquitetura segmentada em três zonas funcionais (Gestão, Administrativa e Académica/Pública), interligadas pela firewall Sophos XGS e integradas a um servidor Windows Server 2019 rodando o AD DS. Para testar a solução e consequentemente convencer a direção a direção a tomar uma possível decisão sobre a utilização da mesma é proposto o cenário da figura 15. O objetivo é, num ambiente de laboratório virtualizado, demonstrar de forma realista como a FEUEM pode:

- Manter o AD DS como fonte única de identidade;
- Controlar quem faz o quê, onde e quando, via grupos RBAC;
- Impor políticas de acesso à Internet e aos recursos internos com base em função de usuário;
- Facilitar auditoria e redução de trabalho manual.

4.4.2. Estrutura Física e Lógica

1) Firewall Sophos XGS

- eth0 (WAN): ligado ao CIUEM/DEEL para Internet.
- eth1 (Gestao – VLAN 99): 192.168.99.1/27 – DC e consoles de administração.
- eth2 (Administrativa – VLANs 10, 20, 30, 40): gateways .1 e slash 27 em cada sub-interface.

- eth3 (Académica/Publica – VLAN 50 e 88): 192.168.50.1/24 e 192.168.99.1/27.

Switches virtuais no VirtualBox em modo “Rede Interna” (`Gestao´, `Administrativa´ e ´Academica_Publica`) simulam o tagging 802.1Q.

Servidor AD DS (ServBA_AD) em VLAN 99, IP estático 192.168.99.10/27 e DNS configurados para oferecer registros dinâmicos.

2) Configuração do AD DS

- Instalação do papel AD DS e promoção a controlador de domínio *engenharia.uem.mz* (ServBA_AD).
- Zonas DNS directa e reversa criadas (*engenharia.uem.mz* e *99.168.192.in-addr.arpa*), testadas com nslookup.
- DHCP Server no Sophos para cada zona, apontando DNS para 192.168.99.10 e registrando novos hosts no DNS do AD.

As OUs foram definidas em dois grupos principais com base na estrutura funcional e operacional da instituição, considerando escalabilidade, integração com a firewall e a dinâmica de utilização dos recursos. A estrutura proposta é a seguinte:

- Usuarios: OU principal para utilizadores (pessoas).
    - IT: técnicos informáticos, ou seja, a equipa do DTIC.
    - Docentes: contas do corpo docente, com políticas específicas e acesso interzonal autorizado (académico e administrativo).
    - Estudantes: destinada a contas genéricas por laboratório ou por turma, com validade temporária e aplicação de políticas restritivas.
    - Departamentos: administrativos subdivididos por sectores funcionais.
        - CEE: Centro de Estudos de Engenharia.
        - DAF: Departamento Administrativo e Financeiro.
        - DRA: Departamento de Registo Académico.

- Computadores: OU principal para equipamentos
    - Servidores
    - IT: computadores da equipa do DTIC
    - LabInfo: computadores dos laboratórios
    - Administrativos: computadores da administração

Grupos de segurança no AD:

- G_Docentes – acesso geral de docentes a recursos académicos e internet. Membros típicos: todos os docentes.
- G_Directores – GPOs ou permissões específicas para directores. Membros típicos: Docentes com cargo de direção.
- G_Técnicos_TI – permissões administrativas no AD e rede. Membros típicos: Pessoal do DTIC.
- G_Staff_DAF – acesso a sistema, partilhas ou serviços financeiros. Membros típicos: pessoal do departamento de finanças.
- G_Staff_CEE – acesso a documentos e sistemas de projectos ou produção. Membros típicos: pessoal da UP.
- G_Staff_DRA – acesso a sistema de gestão académica e registros. Membros típicos: pessoal do registo académico, incluindo secretarias.
- G_Acesso_Internet – controlo de acesso a Internet via firewall. Membros típicos: todos os usuários com permissão web.
- G_Instalação_Software – permissão para instalar aplicações ou atualizações via GPO. Membros típicos: pessoal de TI e Directores, se aplicável.
- G_LabInfo_Users – contas genéricas dos laboratórios de informática; restrições severas, sem instalação de aplicações oriundos da internet. Membros típicos: Estudantes.

Nesses grupos são associados os usuários, o que permite aplicar GPOs e regras de firewall por grupo.

3) Regras de Firewall por VLAN/Zona

A política de firewall proposta baseia-se em princípios de segmentação lógica, privilégio mínimo e controlo de acessos por função, considerando as especificidades de cada zona da rede. O objetivo é permitir apenas os fluxos de comunicação necessários ao funcionamento seguro e eficiente das atividades da instituição, evitando exposições desnecessárias entre departamentos ou utilizadores.

a) Zona de Gestão

Esta zona é dedicada à infraestrutura técnica, incluindo servidores de domínio, DNS, DHCP, ficheiros e máquinas da equipa do DTIC. Por ser o núcleo da gestão da rede, deve ter acesso completo às demais zonas para fins de manutenção e administração.

Regras propostas:

- Permitir comunicação total com todas as outras zonas, exclusivamente a partir de máquinas autenticadas.
- Permitir acesso exclusivo à interface administrativa da firewall (ex.: porta 4444/HTTPS e SSH).
- Bloquear qualquer tentativa de acesso não autenticado oriunda de zonas externas.

b) Zona Administrativa

Compreende os departamentos de apoio institucional, como a Direção de Registo Académico (DRA), o Departamento Administrativo e Financeiro (DAF) e o Centro de Estudos de Engenharia (CEE). Estas áreas necessitam de acesso aos servidores da zona de gestão, bem como à internet para atividades operacionais.

Regras propostas:

- Permitir comunicação com os servidores da zona de gestão (DNS, autenticação, partilhas).

- Impedir comunicação lateral entre departamentos, mantendo o isolamento intra-zona.
- Permitir acesso à internet mediante autenticação por grupo (ex.: acesso mais amplo para chefias, acesso restrito para técnicos administrativos).
- Bloquear o acesso a zonas académicas e públicas, exceto quando justificado por função (ex.: docentes com dupla afiliação).

c) Zona Académica

Destinada a salas de aula e laboratórios de informática, esta zona é usada por docentes e estudantes. Os docentes devem autenticar-se com suas credenciais e ter acesso controlado a partilhas, recursos internos e à internet. Já os estudantes, devido à alta rotatividade, utilizam contas genéricas por laboratório ou turma, com validade temporária e políticas altamente restritivas.

Regras propostas:

- Permitir autenticação ao domínio e acesso controlado a partilhas pedagógicas.
- Para docentes, permitir acesso à internet com permissões ajustadas à função.

Para estudantes:

- Utilizar contas genéricas com acesso apenas ao essencial.
- Aplicar filtros de conteúdo e restrições de horário/navegação.
- Bloquear completamente o acesso a zonas administrativas e de gestão.

d) Zona Pública

Na prática esta zona está integrada na zona académica, ela é voltada para acesso Wi-Fi aberto, visitantes ou eventos, e não está vinculada diretamente a nenhum grupo do domínio. A segurança aqui é tratada com prioridade máxima, considerando a natureza aberta do acesso.

Regras propostas:

- Permitir exclusivamente o acesso à internet.
- Aplicar limitação de largura de banda e tempo de sessão por dispositivo.
- Bloquear totalmente o acesso a qualquer zona interna da rede.
- Monitorar a navegação por IP, com aplicação de políticas de contenção.

A modelagem proposta serve de base lógica para a aplicação de políticas técnicas na firewall e na configuração do Active Directory, conforme detalhado na etapa de implementação.

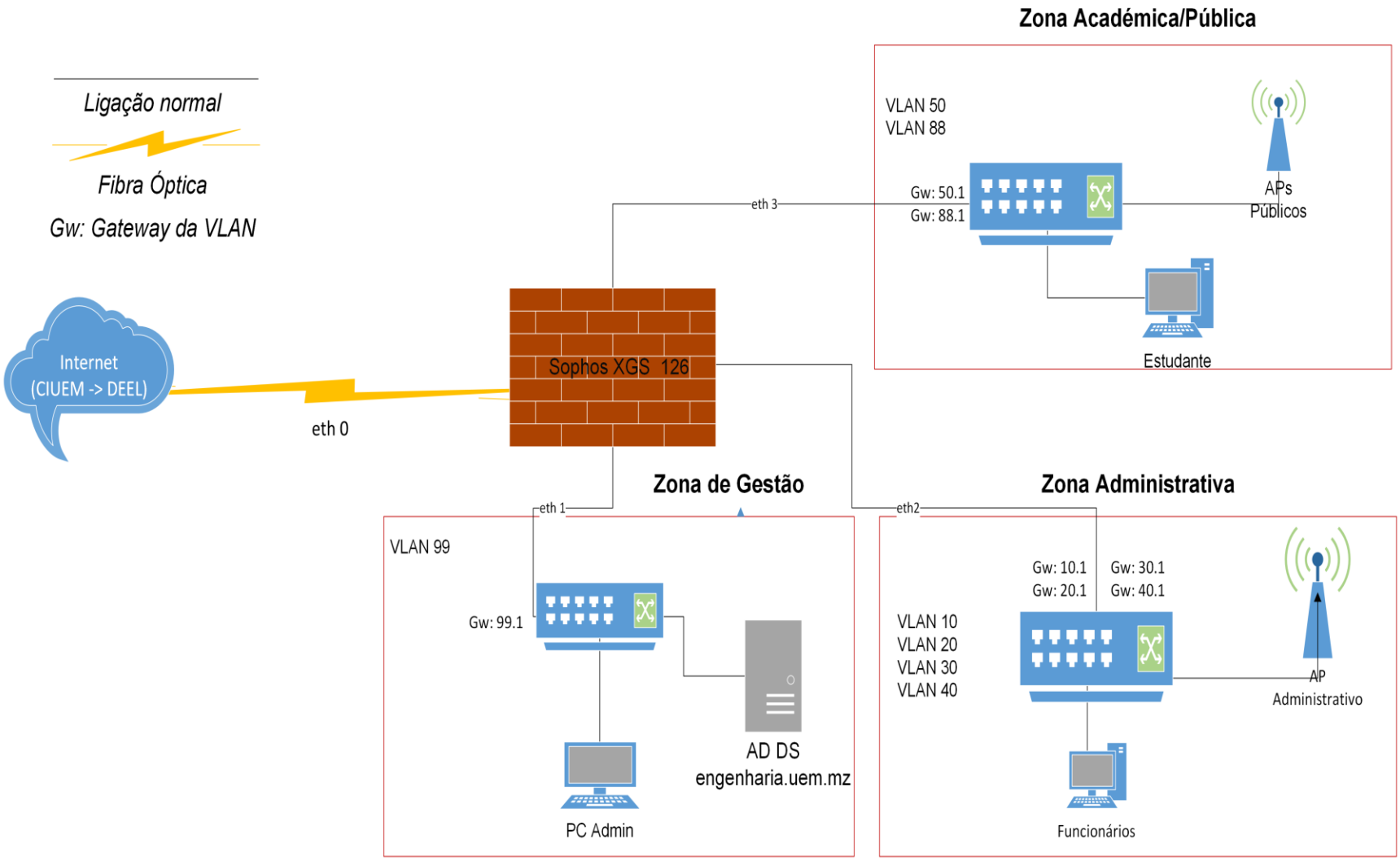


Figura 4-4: Cenário proposto para a solução

Fonte: elaborado pelo autor

3. CAPÍTULO V – APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

3.1. Revisão de literatura

A literatura analisada destaca a importância da segmentação lógica de redes, da gestão centralizada de utilizadores e da aplicação de políticas de acesso com base em função como pilares fundamentais da segurança em ambientes corporativos.

Destacou-se a importância da criação de zonas funcionais separadas por VLANs, que permitem isolar tráfego, reduzir a propagação de ameaças e aplicar regras específicas de firewall conforme a natureza da comunicação.

Autores como (Peterson & Davie, 2011) e (Tanenbaum & Wetherall, 2014) defendem o uso de VLANs para isolar tráfegos entre sectores e limitar a propagação de ameaças. A gestão centralizada por meio do AD DS é apontada como prática essencial para consolidar autenticação, controle de permissões e aplicação de políticas por grupo.

Também é destacada a adoção do modelo RBAC (Role-Based Access Control), que associa permissões a grupos organizados por função, simplificando o controlo de acesso e promovendo alinhamento com a estrutura hierárquica e operacional da instituição.

A integração entre firewalls de próxima geração e serviços de directório permite aplicar políticas com base na identidade do utilizador, ampliando a capacidade de controlo e auditoria sobre os acessos. Esses fundamentos orientaram a estruturação da solução proposta.

3.2. Análise dos Resultados

A solução desenvolvida, baseada na segmentação da rede com VLANs (mas na prática, por zonas), na gestão centralizada com AD DS e na aplicação de políticas com firewall Sophos XGS, mostrou-se tecnicamente viável e alinhada com as boas práticas apontadas pela literatura.

A segmentação permitiu isolar logicamente três zonas principais da rede: Gestão, Administrativa, Académica/Pública. Cada zona recebeu regras de acesso específicas, reduzindo o risco de propagação de ameaças e permitindo controle granular do tráfego.

Departamentos administrativos, por exemplo, foram isolados entre si, e os acessos à zona de gestão ficaram restritos à equipa técnica.

A estrutura das OUs criada no AD reflectiu a organização funcional da instituição. Técnicos, docentes e administrativos foram organizados conforme suas responsabilidades, com aplicação de GPOs específicas. Para os estudantes, devido à alta rotatividade, adotaram-se contas genéricas por laboratório, associadas a políticas restritivas. Esta abordagem simplificou a gestão de identidades, evitando sobrecarga administrativa.

A integração do Sophos XGS com o AD DS via LDAP seguro e STAS permitiu aplicar regras de firewall com base em grupos do domínio, conforme a função do utilizador. Isso tornou possível controlar o acesso à internet e a recursos internos de forma dinâmica, segura e auditável. A firewall passou a identificar os utilizadores por nome de login e a aplicar filtros automaticamente, o que reforçou a governança da rede.

Adicionalmente, políticas como o bloqueio de acesso à interface da firewall fora da zona de gestão e o isolamento total da zona pública (Wi-Fi) foram aplicadas para reforçar o perímetro de segurança. A zona pública ficou restrita apenas à navegação na internet, com controle de banda e sem qualquer acesso aos recursos internos.

Os testes realizados comprovaram a eficácia da solução: os clientes ingressaram no domínio com sucesso, as políticas de grupo foram aplicadas conforme o grupo do utilizador, os utilizadores autenticados puderam ser visualizados em tempo real na firewall, mas os acessos à internet filtrados por perfil apresentaram dificuldades por conta do ambiente utilizado.

De modo geral, a solução demonstrou que é possível elevar o nível de organização e segurança da rede utilizando os recursos já disponíveis, quando aplicados com base em princípios técnicos sólidos e adaptados à realidade organizacional.

4. CAPÍTULO VI – CONSIDERAÇÕES FINAIS

Conclusão

Este trabalho apresentou uma solução de segurança para a rede do bloco administrativo da Faculdade de Engenharia da Universidade Eduardo Mondlane, baseada na integração entre o Active Directory Domain Services e a firewall Sophos XGS. A proposta visou organizar logicamente a rede, centralizar a gestão de utilizadores e aplicar políticas de acesso conforme a função de cada grupo.

A análise da rede existente evidenciou a falta de segmentação, controle de acessos e autenticação unificada. Com base nisso, foi implementado um modelo de rede segmentada por zonas (gestão, administrativa, académica/pública), com regras de firewall e políticas de grupo aplicadas por identidade.

A solução foi testada num ambiente virtualizado, demonstrando sua viabilidade técnica e aderência às boas práticas recomendadas na literatura. Os resultados confirmam que é possível aumentar o controlo, a segurança e a organização da rede com tecnologias já disponíveis, preparando o ambiente para futuras melhorias.

Recomendações

- Implementação de autenticação multifactor (MFA)

Para fortalecer a segurança da autenticação, especialmente para acessos administrativos ao AD DS, firewall, serviços web e acesso remoto, recomenda-se a activação de autenticação multifactor, pelo menos para utilizadores críticos.

- Planeamento estratégico da infra-estrutura de rede

Todas as alterações ou expansões devem estar integradas num plano de infra-estrutura bem definido, com análise de impacto técnico e alinhamento com os objectivos institucionais. As soluções devem ir além da resolução imediata de falhas, sendo sustentáveis a médio e longo prazo.

- Criação de um sistema de documentação contínuo

Toda alteração na rede, nas políticas ou nos sistemas deve ser devidamente registada. Recomenda-se manter um repositório técnico actualizado, acessível apenas a técnicos autorizados, garantindo continuidade administrativa mesmo em casos de substituição de pessoal.

- Implementação de um gestor de senhas institucional

As credenciais de sistemas críticos devem ser armazenadas de forma segura, com uso de um gestor de senhas cifrado. É igualmente recomendada a definição de uma política obrigatória de renovação periódica de senhas.

- Listagem e disponibilização local de software académico

Recomenda-se a criação de um repositório interno que contenha os softwares mais utilizados na faculdade (ex.: MATLAB, AutoCAD, Code::Blocks, Visual g, Cisco Packet Tracer, NetBeans, etc.), evitando que os estudantes acedam à Internet para descarregar aplicações.

- Expansão da solução para outros blocos e departamentos

A proposta deve ser replicada nos restantes edifícios da faculdade, como a direção, laboratórios e espaços académicos, promovendo uniformização, melhor controlo e centralização da gestão da rede.

- Formação contínua da equipa técnica

A capacidade técnica do DTIC é vital para a continuidade da solução. Recomenda-se a realização regular de formações sobre administração de firewalls, servidores, políticas de grupo, segurança e resposta a incidentes.

- Auditorias internas e simulações de incidentes

A equipa técnica deve realizar auditorias de segurança e simulações controladas de falhas ou ataques para testar a resiliência dos sistemas e a eficácia das políticas aplicadas.

Constrangimentos

Durante a realização do presente trabalho enfrentou-se os seguintes desafios:

- Conciliar as actividades de estágio e trabalho com o desenvolvimento da pesquisa revelou-se um dos principais desafios, exigindo uma gestão rigorosa do tempo e priorização contínua de tarefas, em detrimento de análises mais extensas e testes práticos mais prolongados;
- Falta de acesso integral à documentação técnica da infraestrutura actual da faculdade, o que obrigou à recolha empírica de informações junto da equipa técnica, atrasando o mapeamento exato da topologia original; entre outros.
- Dispor de computador de poucas capacidades para suprir com os requisitos necessários para configurar o ambiente virtual e realizar os testes, mantendo um desempenho desejável, o que causou a morosidade e condicionou a conclusão total dos objectivos.

Apesar desses desafios, o trabalho foi concluído com sucesso e os objectivos inicialmente propostos foram cumpridos, com algumas excepções no último.

BIBLIOGRAFIA

REFERÊNCIAS BIBLIOFRÁFICAS

1. Allied Telesis. (s.d. de Novembro de 2022). *Product information for 1GbE UTM Firewalls*. Obtido de site oficial da Allied Telesis: https://www.alliedtelesis.com/sites/default/files/file/2022-11/ati-utm-ds.pdf
2. Axelos. (2019). *ITIL Foundation: ITIL 4 Edition* (1st ed.). London: The Stationery Office (TSO).
3. Cisco Systems. (2021). *Cisco APIC Security Configuration Guide, Release 5.1(x): TACACS+, RADIUS, LDAP, RSA, SML,and DUO.* San José, CA: Cisco Systems.
4. Francis, D. (2021). *Mastering Active Directory* (3rd ed.). Birmingham: Packt Publishing Ltd. Obtido de https://books.google.co.mz/books?hl=pt-PT&lr=&id=xVBSEAAAQBAJ&oi=fnd&pg=PP1&dq=Active+Directory&ots=2YUucdolZC&sig=3acGNaJeBZaM0KzkS_xCW3irnfw&redir_esc=y#v=onepage&q=Active%20Directory&f=false
5. Gollman, D. (2011). *Computer Security* (3.ª ed.). Chichester, Reino Unido: John Wiley & Sons Ltd.
6. Harrison, G. (2018). *Enterprise Directory Services: A Technical Guide to LDAP and Active Directory.* Sebastopol, CA, EUA: O'Reilly Media.
7. Hitzel, B. (s.d.). *Network Design: Dual ISP, DMZ, adn the Network Edge.* Unknowen: Network Defense Blog.
8. Hucaby, D., McQuerry, S., & Jansen, D. (2009). *Cisco LAN Switching Configuration Handbook* (2nd ed.). Indianapolis: Cisco Press.
9. ISACA. (2018). *COBIT 2019 Framework: Governance and Management Objectives.* Schaumburg, IL: ISACA.

10. ISO. (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems* (3rd ed.). Genebra: ISO.

11. Mamede, H. S. (2006). *Segurança Informática nas Organizações.* Lisboa, Portugal: FCA.

12. Massunguine, G. P. (15 de Agosto de 2022). Segurança Cibernética: Proposta de Implementação de uma Plataforma SIEM. *Repositório da UEM.* Obtido de Site da UEM.

13. Microsoft Learn. (17 de 03 de 2025). *Windows Server*. Obtido de Microsoft Learn: https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services

14. NIST. (2020). *NIST Special Publication 800-63: Digital Identity Guidelines.* Gaithersburg, MD, EUA: NIST.

15. Odom, W. (2019). *CCNA 200-301 Official Cert Guide, Volume 1.* Indianapolis: Cisco Press.

16. Peterson, L. L., & Davie, B. S. (2011). Computer Netwoks a systems approach. Em L. L. Peterson, & B. S. Davie, *Computer Netwoks a systems approach* (5th ed., p. 920). Burlington: Morgan Kaufmann.

17. Prekas, J. (2017). *Mastering Identity and Access Management with Azure Active Directory.* Birmingham, Reino Unido: Apress.

18. Prevelakis, V., & Spinellis, D. (2000). *OpenLDAP Administration Cookbook.* Boston, MA: Addison-Wesley.

19. Red Hat, Inc. (2022). *Documentation*. Obtido de Red Hat: https://www.freeipa.org/docs/

20. Robbins, F. (2003). *Understanding and Deploying LDAP Directory Services* (2.ª ed.). Boston, MA: Addison-Wesley Professional.

21. Stallings, W., & Brown, L. (2020). *Computer Security: Principles and Practice* (4th ed.). Boston: Pearson.

22. The Samba Team. (s.d. de s.d. de 2023). *Setting up Samba as an Active Directory Domain Controller*. Obtido de Wiki do Samba.

23. Tridgell, A. (2017). *Managing Samba*. Obtido de Managing Samba: https://linuxclass.heinz.cmu.edu/doc/Open-Source-books/Samba-3-by-example.pdf

24. Tweedale, F. (19 de 07 de 2019). *Designing revocation self-service for FreeIPA.* Obtido de Fraser's IdM Blog: https://frasertweedale.github.io/blog-redhat/posts/2019-07-19-designing-revocation-self-service-for-freeipa/

25. Wahl, M., Howes, T., Kille, S., & Sermershein, J. (1997). *LDAP: Promaning Directory-Enabled Applications with Lightweight Directory Access Protocol* (2.ª ed.). Indianapolis, IN: Que Press.

26. Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.* Boston, Massachusetts, EUA: Harvard Business School Press.

ANEXOS

Anexo 1: Especificações do Host e das Máquinas Virtuais

Sistema Operativo	Windows 10 Pro, 22H2
Arquitectura do Sistema	64-bit
Processador	Intel® Core™ i5 – 6200U @2.30GHz ~2.40GHz
RAM	16 GB
Hard Disk Drive (HDD)	500 GB + 1 TB

Tabela A 0-1: Especificações do Host

Sistema Operativo	Sophos Firewall Operating System (SFOS)
Versão	SFOS 21.5.0 GA Build 171
Arquitectura do sistema	64-bit
RAM	4 GB
Processadores	1
Hard Disk Drive (HDD)	96 GB
Network Adapters	Adapter 1: Internal Network, “Gestão” (192.168.99.1/27)
	Adapter 2: NAT
	Adapter 3: Internal Network, “Administrativa” (192.168.10.1/27)
	Adapter 4: Internal Network, “Academica_Publica” (192.168.50.1/24)

Tabela A 0-2: Especificações da VM Sophos

Sistema Operativo	Windows 10
Arquitectura	64-bit
Processadores	2
RAM	4 GB
Hard Drive Disk (HDD)	50 GB
Network Adapters	Adapter 1: Internal Network, “Gestao” (192.168.99.10/27)
	Adapter 2: NAT

Tabela A 0-3: Especificações da VM com Servidor (AD DS)

Sistema Operativo	Windows 10
Arquitectura do sistema	64-bit
RAM	2 GB
Processadores	1
Hard Disk Drive (HDD)	50 GB

Network Adaptadores	Adapater 1: Internal Network, “Administrativa” (192.168.10.1/27)

Tabela A 0-4: Especificações da VM do usuário na zona Administrativa

Sistema Operativo	Windows 7
Arquitectura do sistema	64-bit
RAM	2 GB
Processadores	2
Hard Disk Drive (HDD)	32 GB
Adaptador	Adapter 1: Internal Network, “Academica_Publica” (192.168.50.1/27)

Tabela A 0-5: Especificações da VM do usuário na zona Academica/Publica

Anexo 3: AD DS – Instalação e Configuração

Este anexo apresenta as etapas realizadas para instalar e configurar o Active Directory Domain Services (AD DS) no Windows Server 2019, promovendo o servidor a controlador de domínio e criando a base da estrutura de autenticação da rede. Apesar do papel relevante, a instalação do Windows Server 2019 não será documentada.

3.1. Instalação do papel AD DS

Acesso ao “Add Roles and Features Wizard” pelo Server Manager.

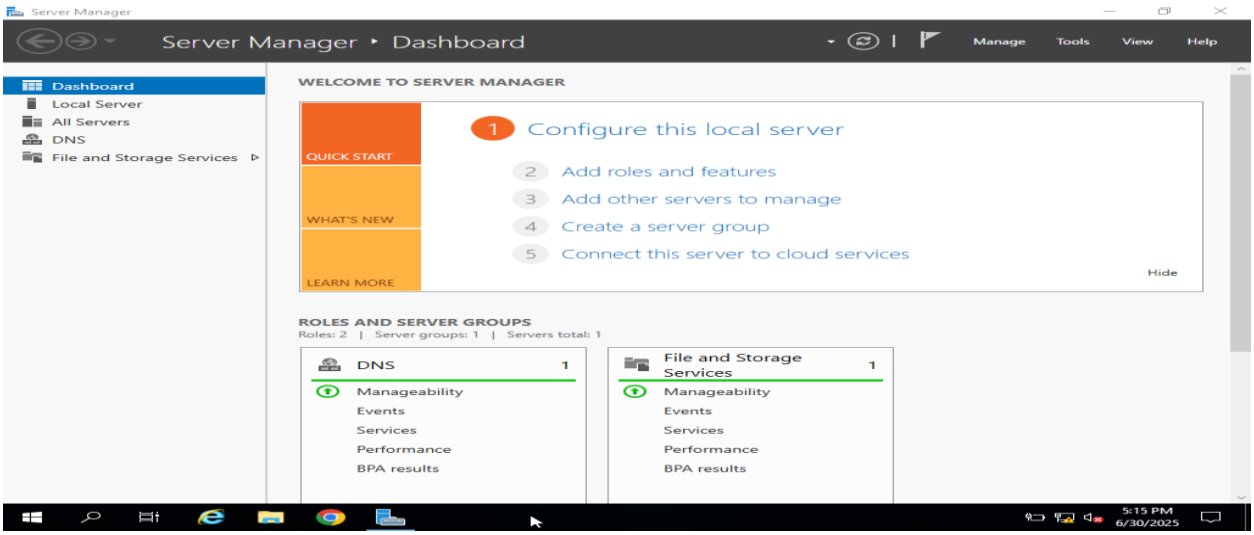


Figura A 1: Inicio da instalação dos serviços de domínio via assistente gráfico

Seleção do papel “Active Directory Domain Services”. Depois clicar “Next” até etapa de intalação.

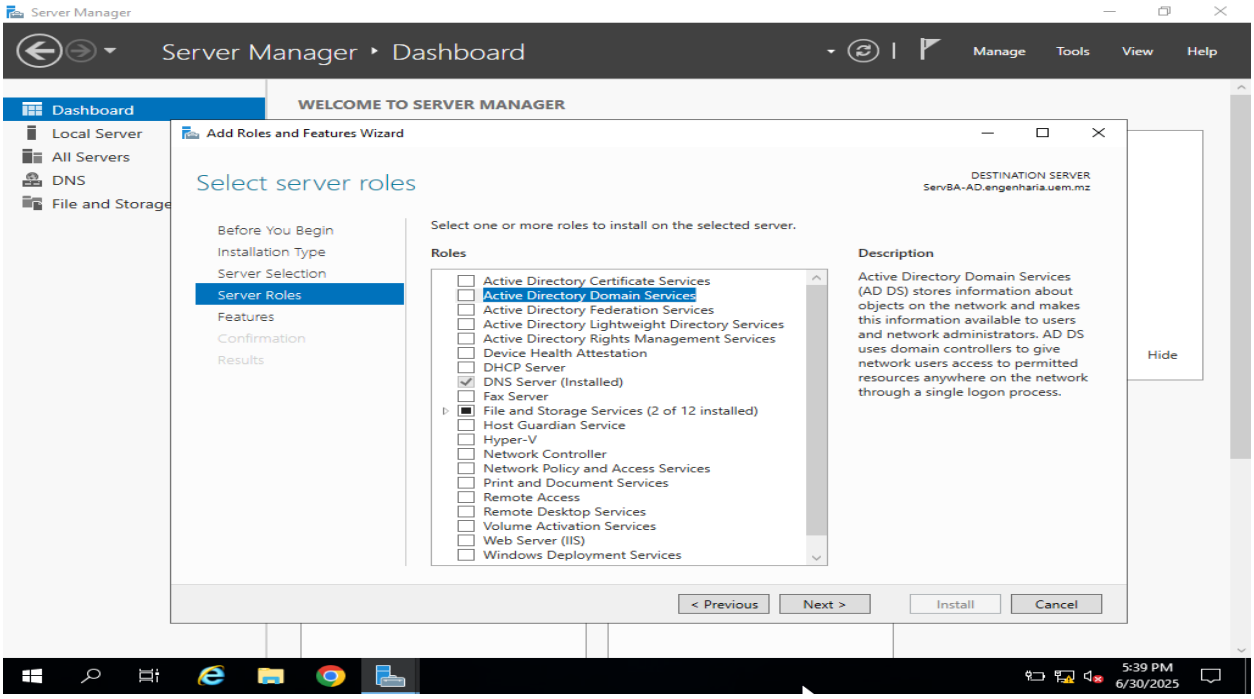


Figura A 2: Marcação da função AD DS entre os papéis disponíveis no servidor

3.2. Promoção do servidor a controlador de domínio

Clicar na opção “Promote this server to a domain controller”

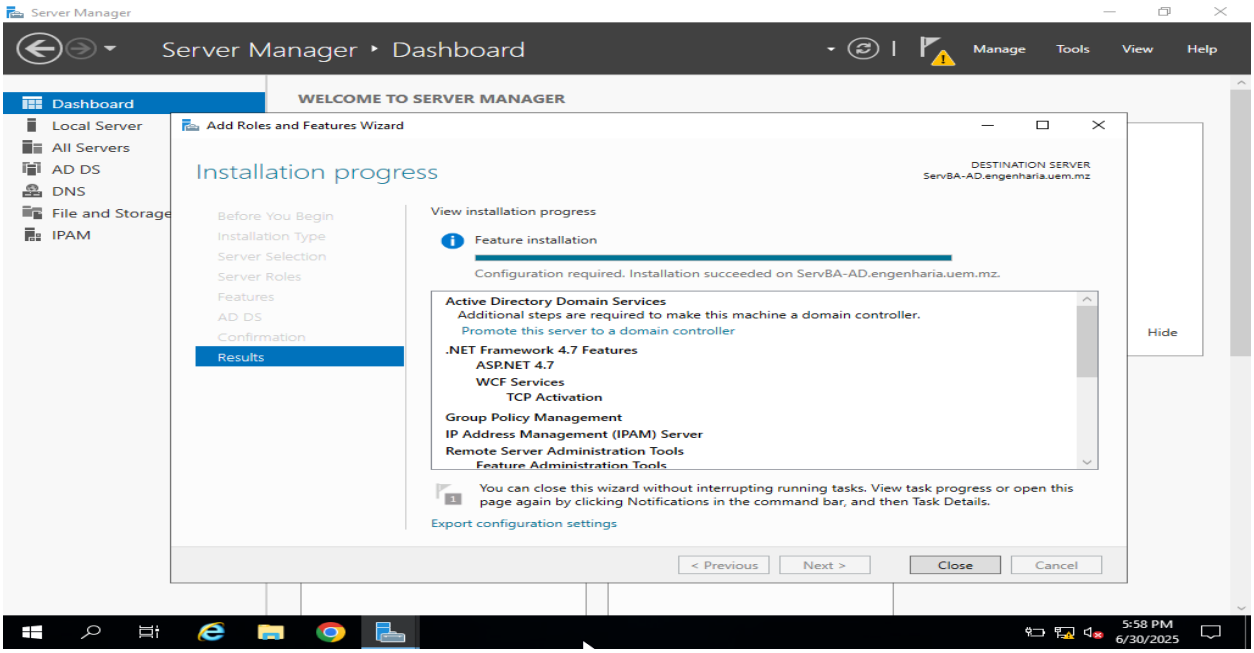


Figura A 3: Ação tomada após instalar o papel AD DS, para iniciar a promoção do servidor

Criação de um novo domínio na nova floresta: engenharia.uem.mz

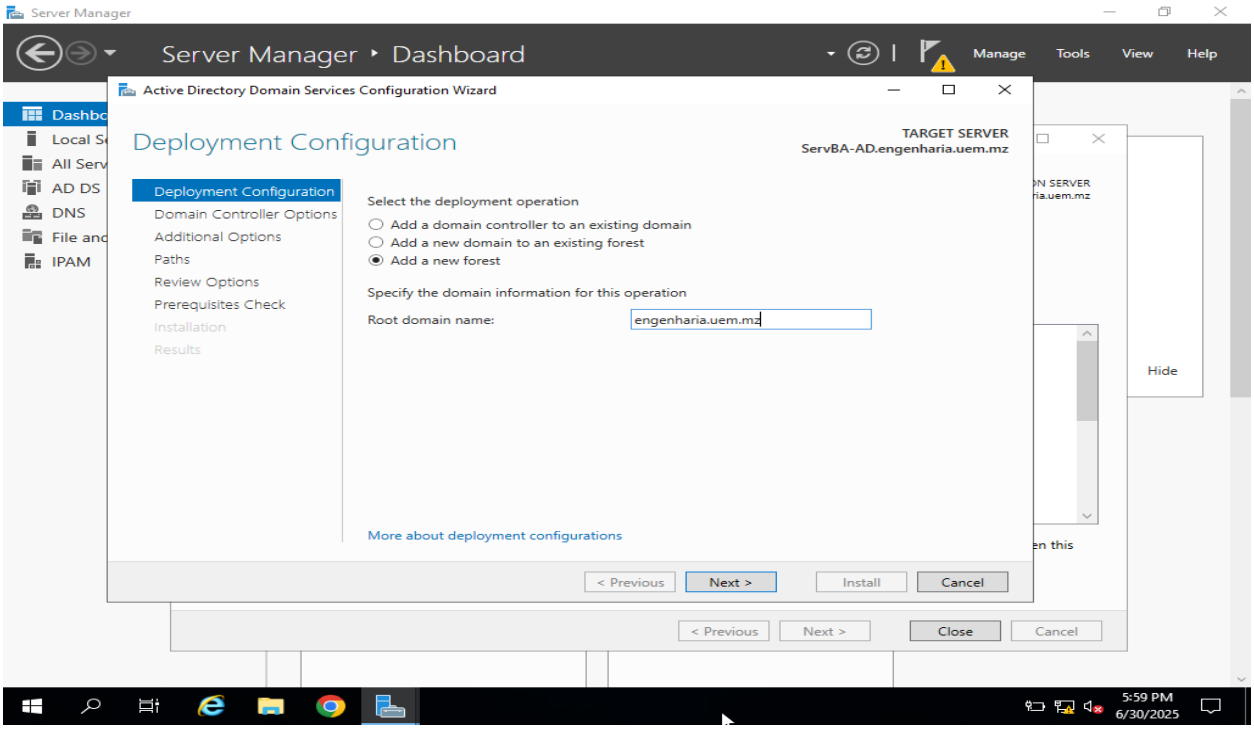


Figura A 4: Definição do nome de domínio principal para o ambiente da FEUEM

Definição da senha do DSRM (Directory Services Restore Mode)

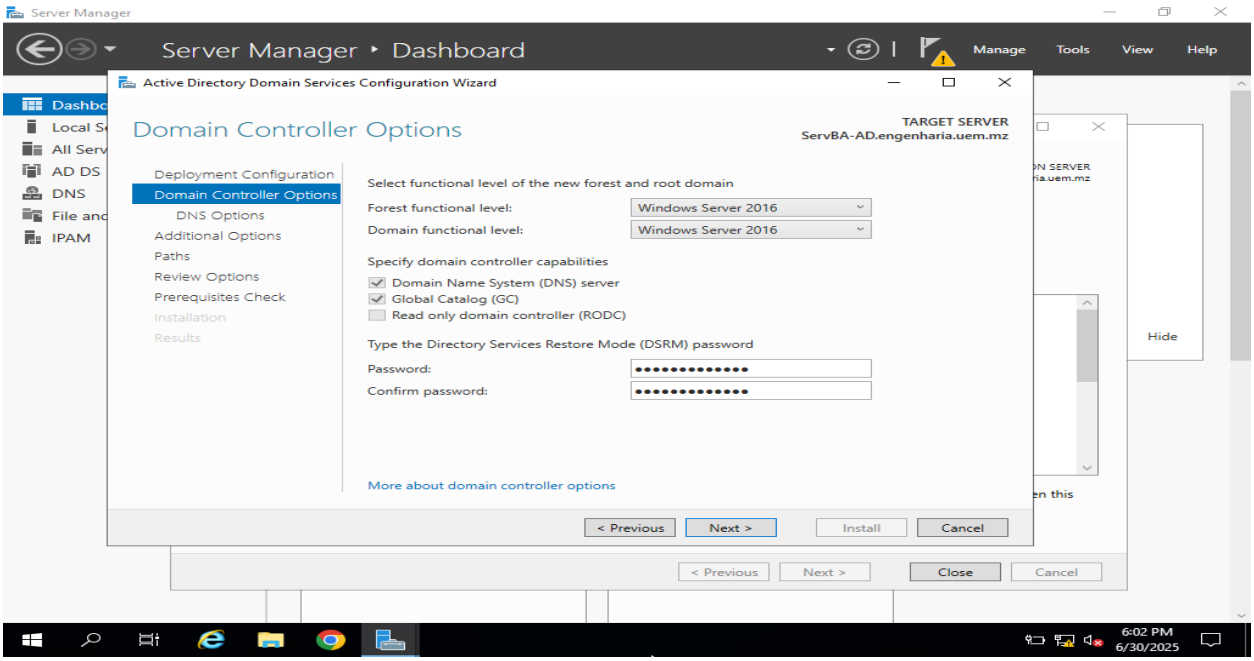


Figura A 5: Configuração da senha para recuperação do serviço de diretório em casos críticos.

3.3. Conclusão e reinício: Resumo da instalação de pré-requisitos.

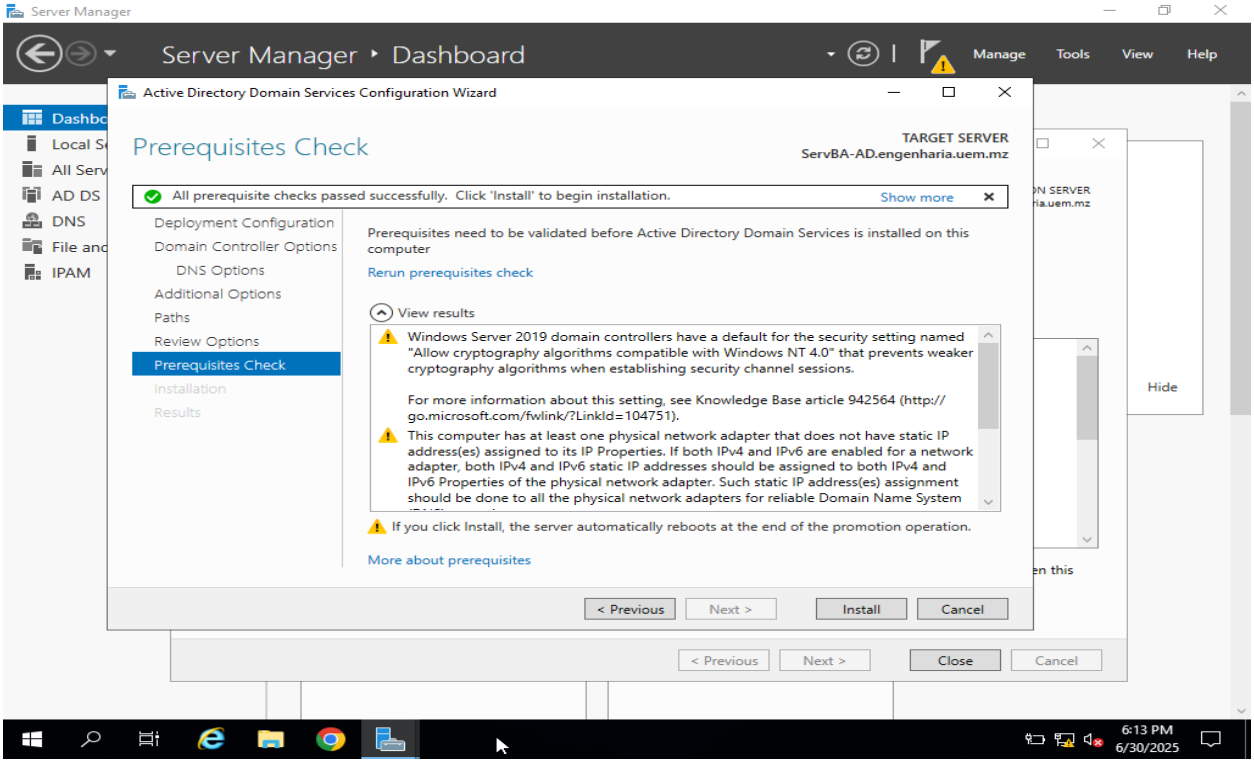


Figura A 6: Confirmação das opções escolhidas antes de iniciar a promoção.

Após a instalação e configuração, o servidor irá reiniciar automaticamente.

3.4. Validação do domínio e funcionalidades: Exibição do domínio criado e abertura da consola “Active Directory Users and Computers” a partir da aba “Tools”.

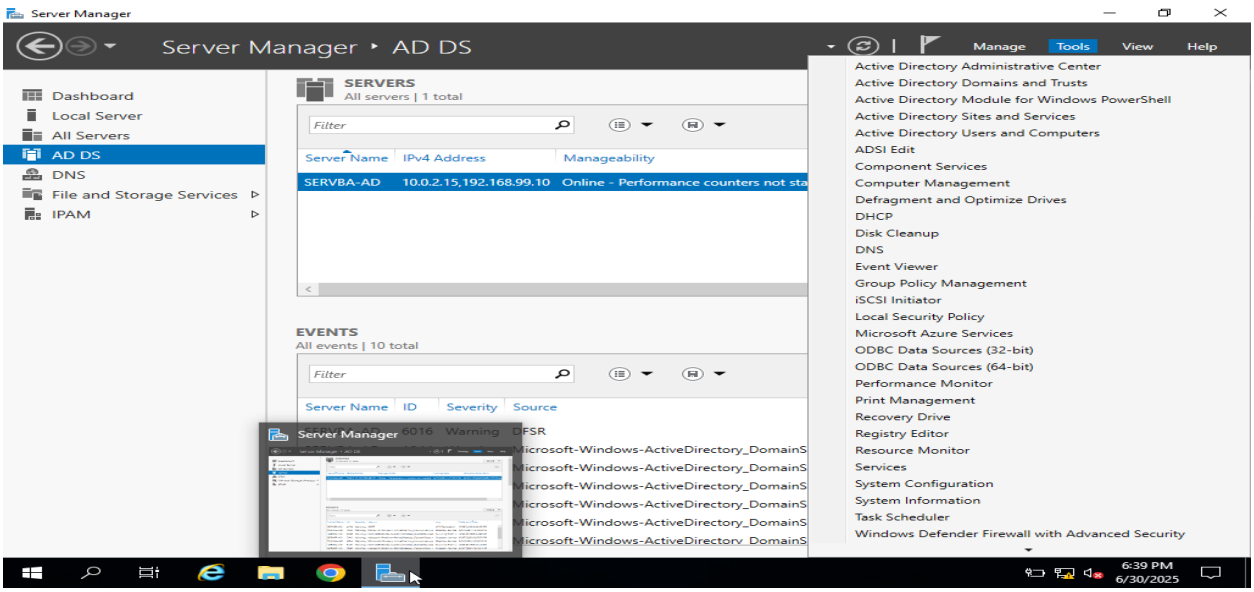


Figura A 7: Validação da promoção bem sucedida ao permitir gestão de objectos do domínio

Terminado com sucesso a fase anterior, deve-se verificar a zona de pesquisa directa e reversa no DNS. Incluir o serviço DNS saudável, é um pré-requisito crítico para o AD DS e para integração com o Sophos XGS. A zona reversa foi criada para permitir resolução inversa (IP para nome), essencial para integração com o STAS/Sophos.

Para verificar se existe a zona e se não existir, criar: no “Server Manager” clica na aba “Tools” -> “DNS” -> expandir o Server -> “Reverse Loookup Zone”. Caso esteja vazio (sem nenhum registro), clica com mouse direito sobre a zona e “New Zone” -> preencha com o IP da sub-rede (x.x.x) -> “Next” -> “Finish”. Depois abra o cmd para iniciar a criação dos registros, insira o comando **ipconfig /registerdns**, pouco tempo depois os registros terão sido criados.

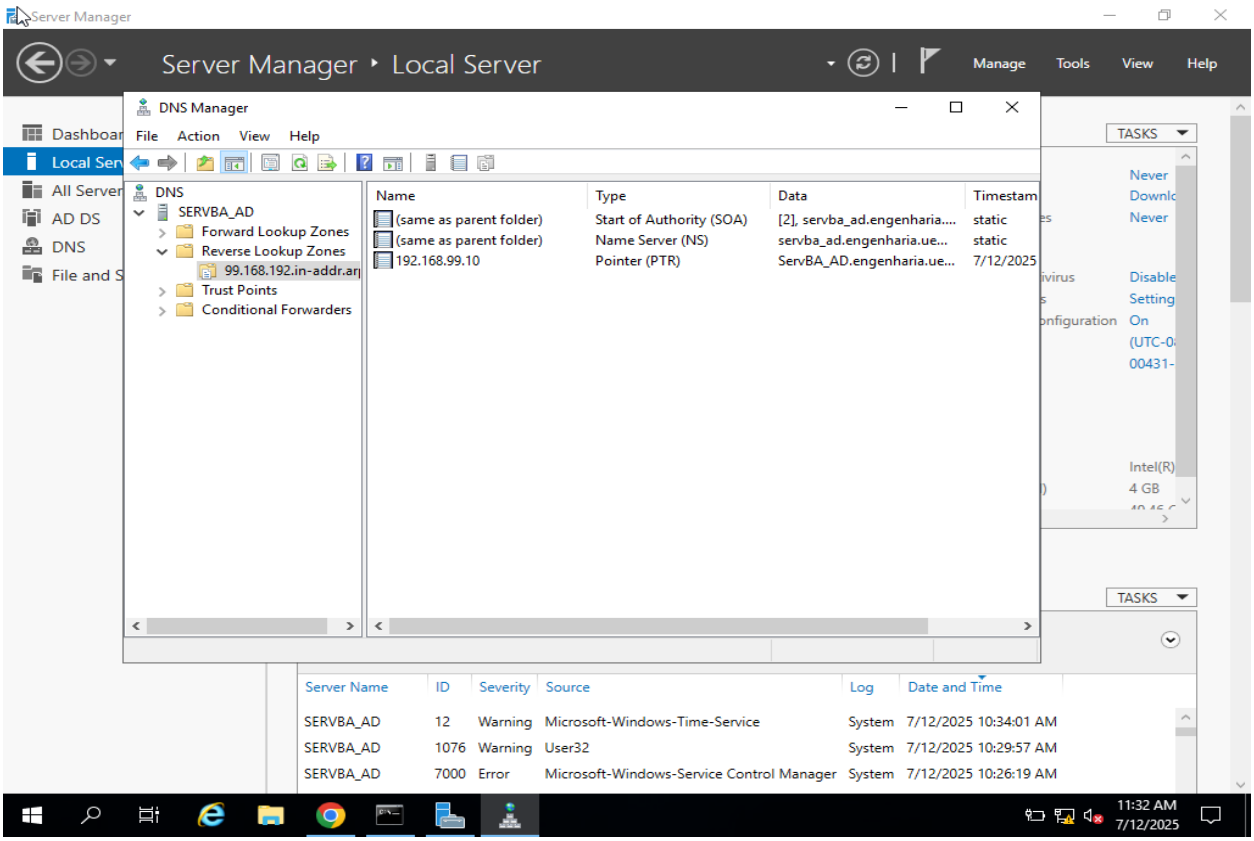


Figura A 8: Zona de pesquisa directa e reversa no DNS.

Anexo 4: Organização de OUs, Grupos e Utilizadores no AD DS

Este anexo apresenta a estrutura organizacional criada no Active Directory para representar a hierarquia funcional da FEUEM. A organização lógica em Unidades Organizacionais visa permitir a aplicação de políticas de grupo, partilha de recursos e regras de firewall com base no papel de cada utilizador.

4.1. Criação da estrutura de OUs

No Server Manager, clica no “Tools”, depois no “Active Directory Users and Computers” e depois é expandir conforme demonstrado na fig A 9.

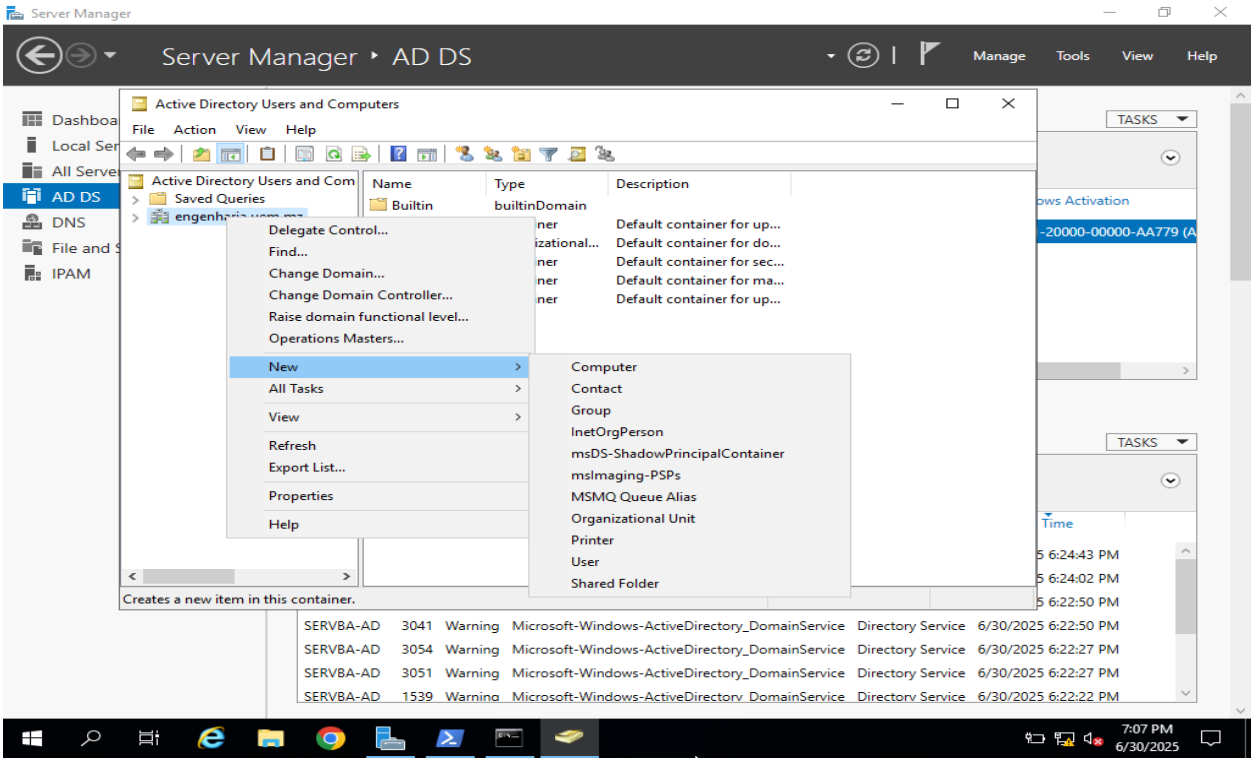


Figura A 9: Caminho de criação de elementos do domínio.

Estrutura de OUs criada no domínio engenharia.uem.mz

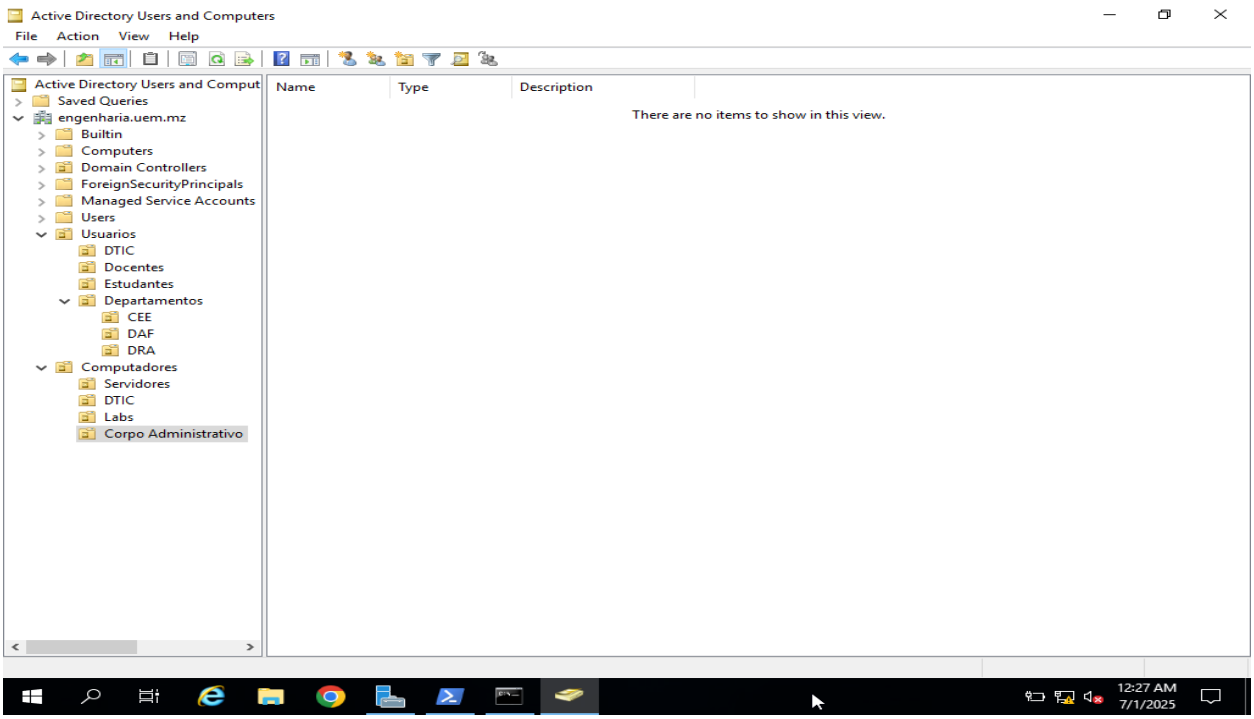


Figura A 10: Segmentação dos utilizadores de acordo com a função e classificação dos equipamentos de rede por local de uso.

Para a criação de usuários e grupos segue-se os mesmos passos, bastando clicar no New “User” ou “Group”. Os usuários e grupos foram criados na OU a qual pertencem de acordo com a sua função. Os usuários foram adicionados aos seus respectivos grupos funcionais.

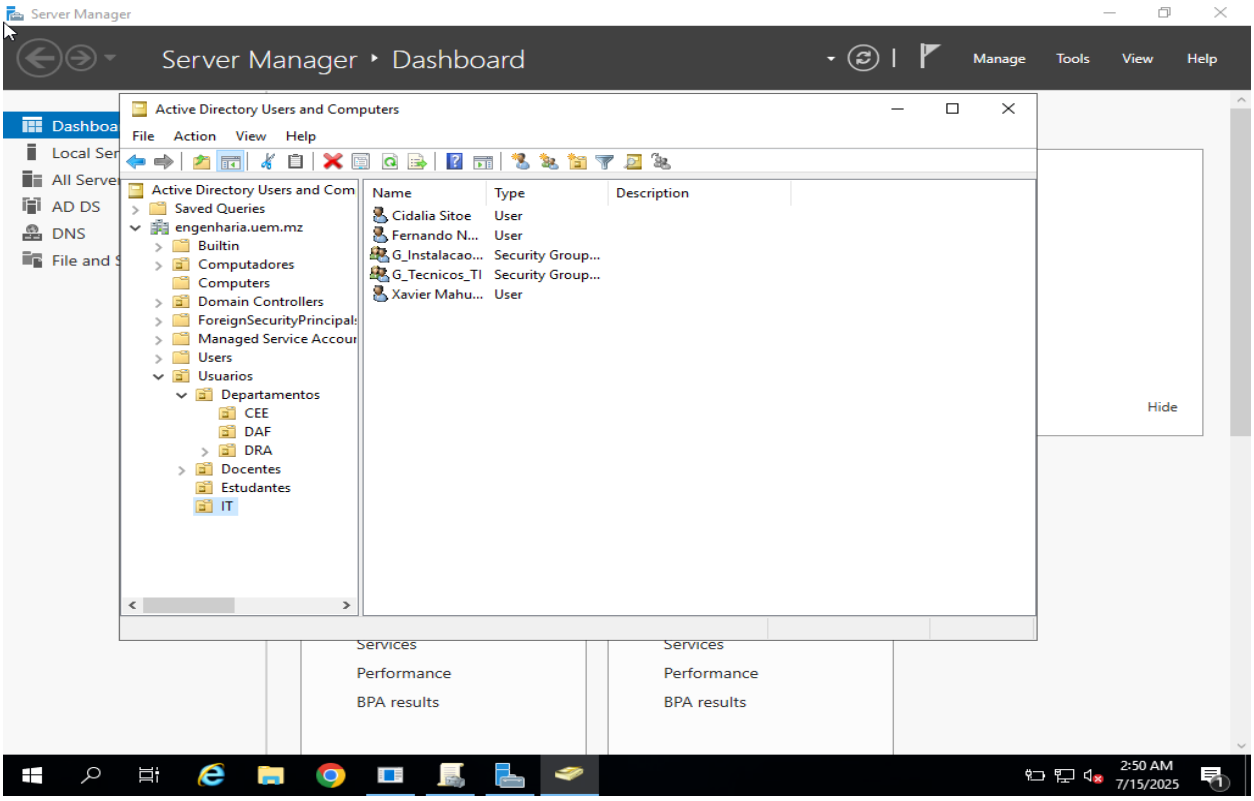


Figura A 11: Organização das OUs, Usuários e Grupos por função

Anexo 5: Políticas de Grupo (GPOs) aplicadas

Este anexo documenta a aplicação de políticas de grupo (GPOs) no domínio *engenharia.uem.mz*, com base na organização por Unidades Organizacionais (OUs) e grupos de segurança. As GPOs foram aplicadas com foco na restrição de funcionalidades, padronização do ambiente de trabalho e reforço da segurança, respeitando as necessidades operacionais de cada grupo de utilizadores.

5.1. Visão geral das GPOs

Para a criação de GPO, clica nas teclas Inicial + R e digita o comando “gpmc.msc”. Ao apresentar a tela, expande o “Forest:” -> “Domains”, depois clicar no domínio e então verá as OUs criadas. Depois clica com o mouse direito sobre a OU que pretende criar nele a política e clica no “Create GPO in this domain, and Link it here…”

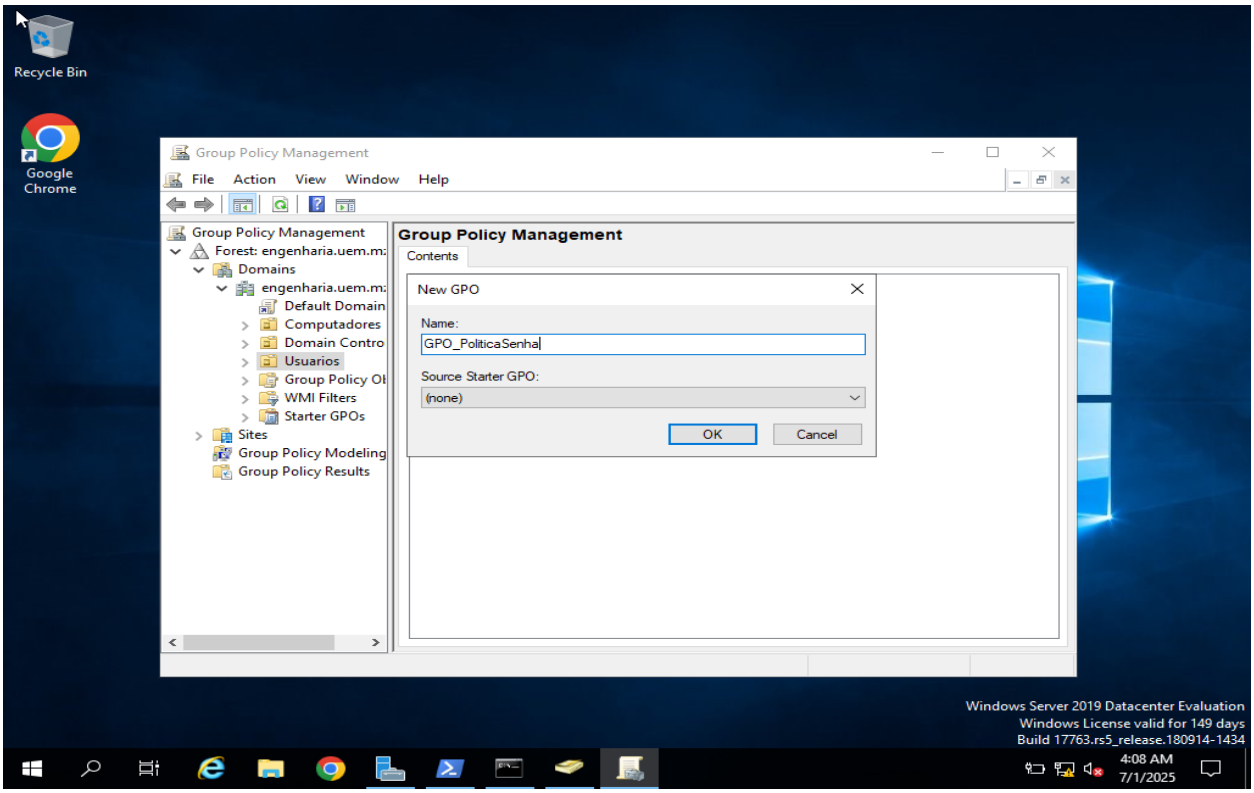


Figura A 12: Exemplo de criação de GPO de política de senhas que será abranger a todos usuários

Após a criação da GPO, pressione sobre ela com o mouse direito e clica em “Edit”. Siga a expansão feita na figura A 12.

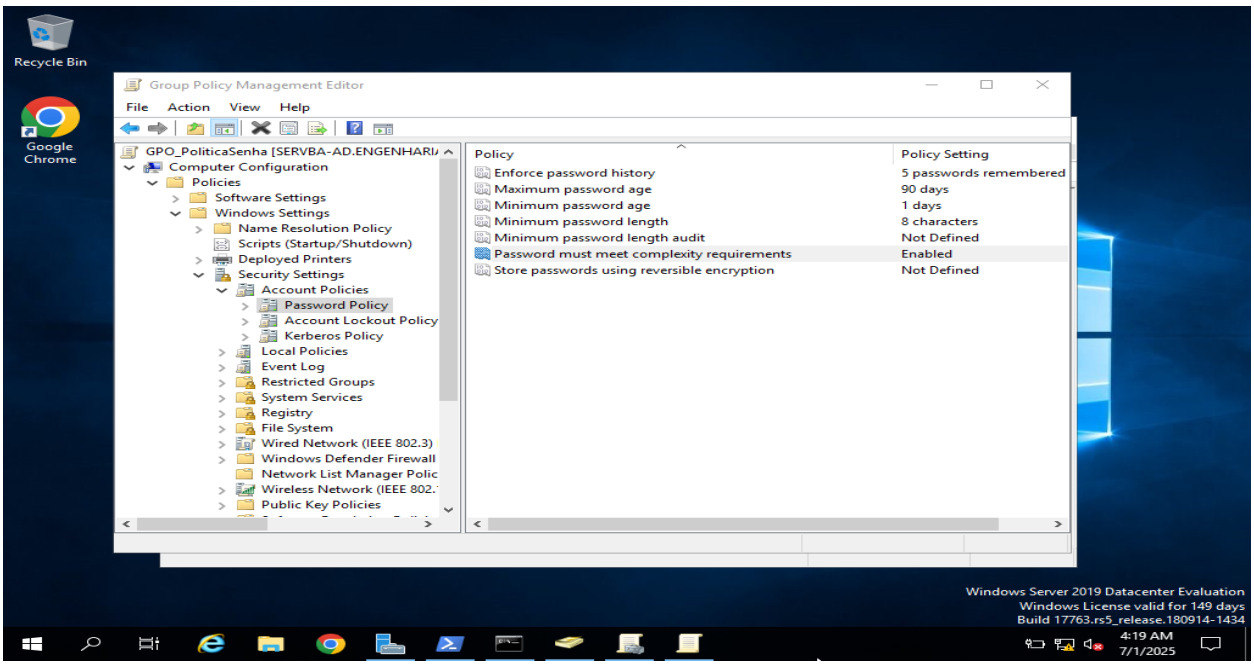


Figura A 13: Definição da política de senhas para todos usuários.

Para as GPOs direcionada a certo(s) grupo(s), faz-se a delegação do grupo em causa. Após ter cria a GPO, pressione com mouse esquerdo e vá na aba “Delegation” -> “Advanced” -> remover o “Auhenticated User” -> “Add”, pesquise e selecione o grupo, habilitar as permissões “Read” e “Apply group policy” e OK.

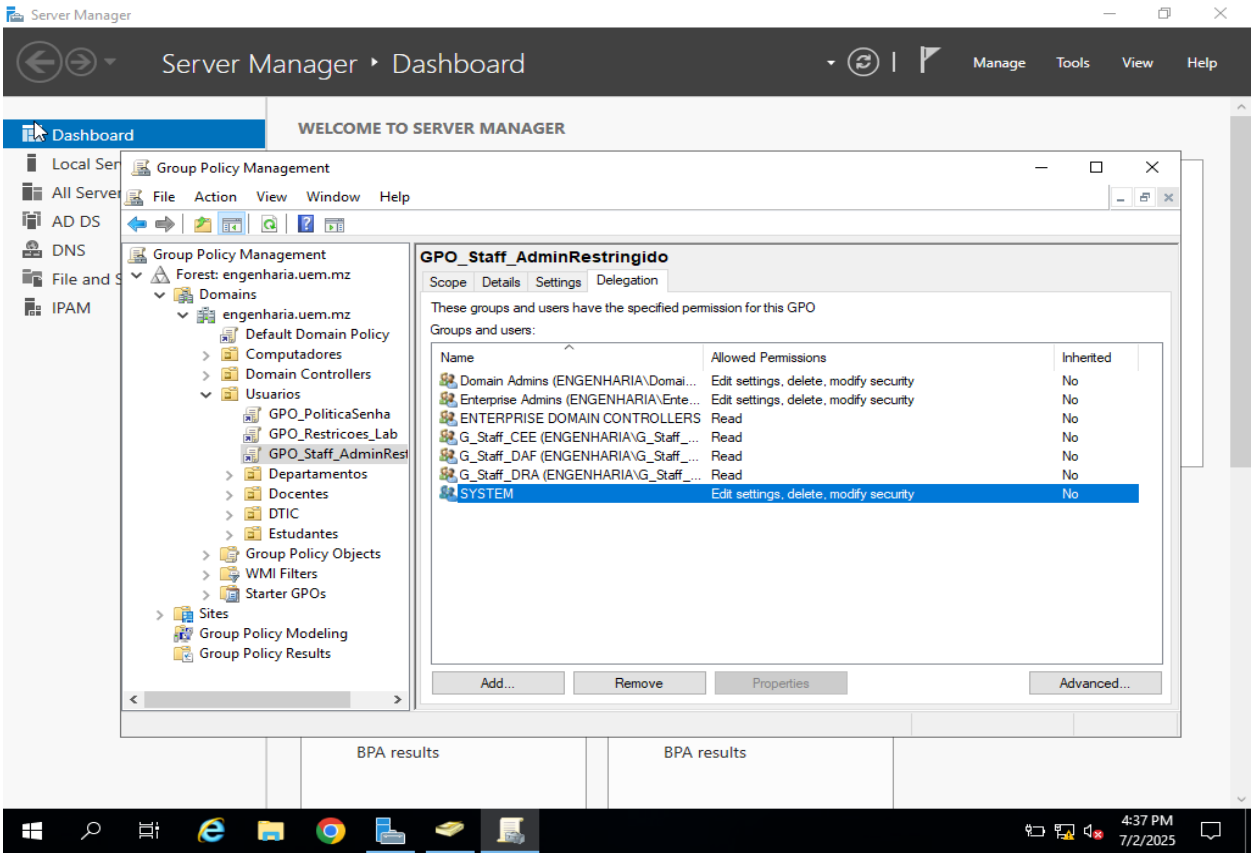


Figura A 14: Delegação de grupo para uma política de grupo.

Depois de definir e configurar todas as políticas necessárias, é preciso validá-las e testá-las nas máquinas de clientes que se encontram no domínio, através do comando **gpupdate /force** e em seguida **gpresult /r,** no cmd. O primeiro comando actualiza as políticas na máquina cliente e o segundo apresenta para qual GPO foi aplicada, que o cliente é abrangido.

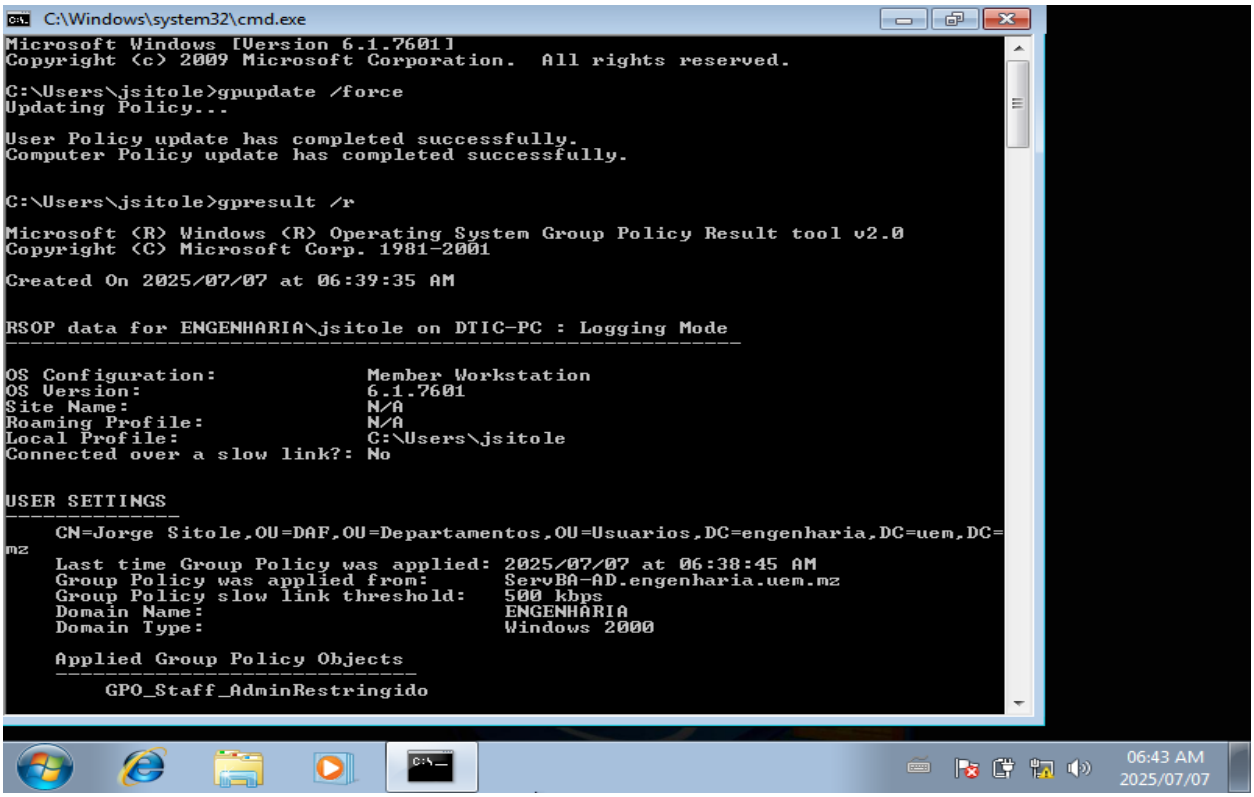


Figura A 15: Aplicação das políticas.

O autor criou várias políticas de grupo, mas por uma questão de gestão do espaço, não poderá demonstrar o passo a passo de cada.

Após confirmar que está tudo operacional com o AD DS, partiu-se para o Sophos XGS.

Anexo 6: Instalação de Firewall Sophos XGS

Baixar o a imagem ISO no site oficial. Abrir o gerenciador VirtualBox, criar a máquina e depois ir ao Setup fazer duplo click, logo aparecerá no VirtualBox. Executar “Start”, vai abrir consola e primeiramente a senha é: admin.

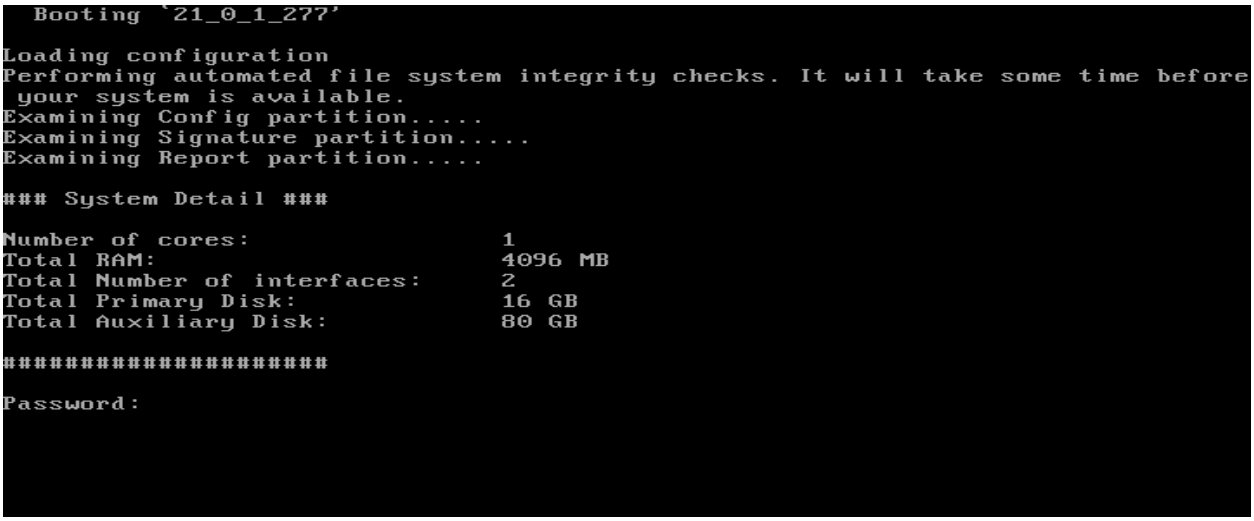


Figura 0-1: Tela inicial login via console.

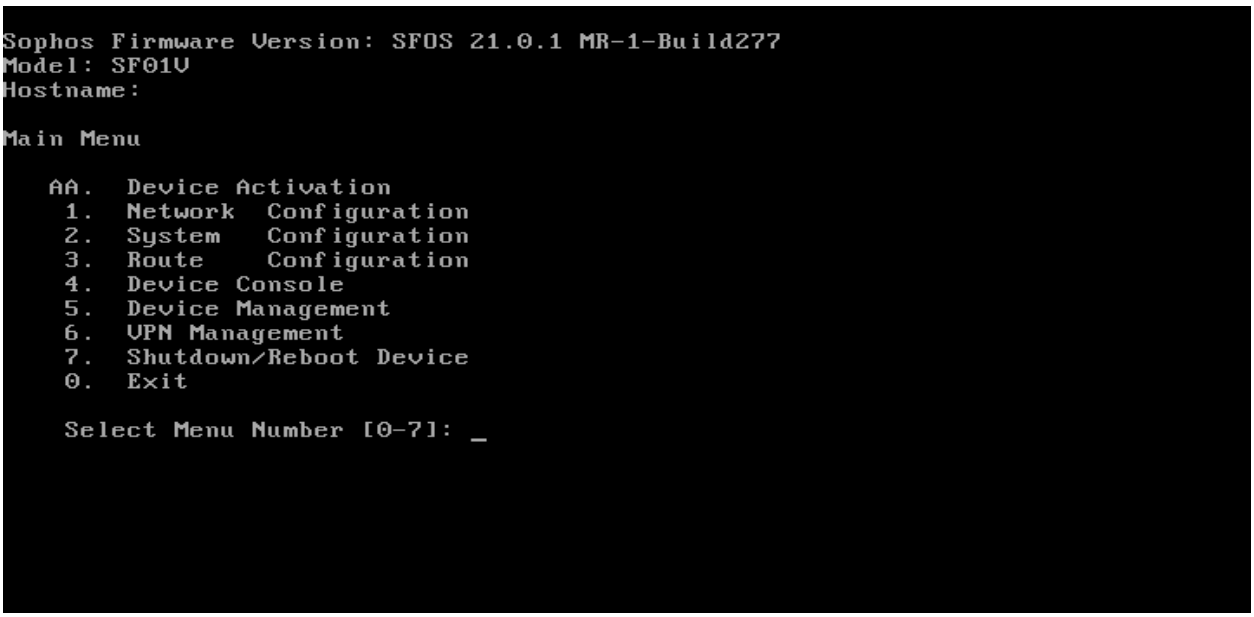


Figura 0-2: Menu inicial para configurações

Ao ter chegado aqui, abra o navegaor (de preferência Chrome) com uma máquina que esteja na mesma rede e insira o endereço https://172.16.16.16:4444, avançar.

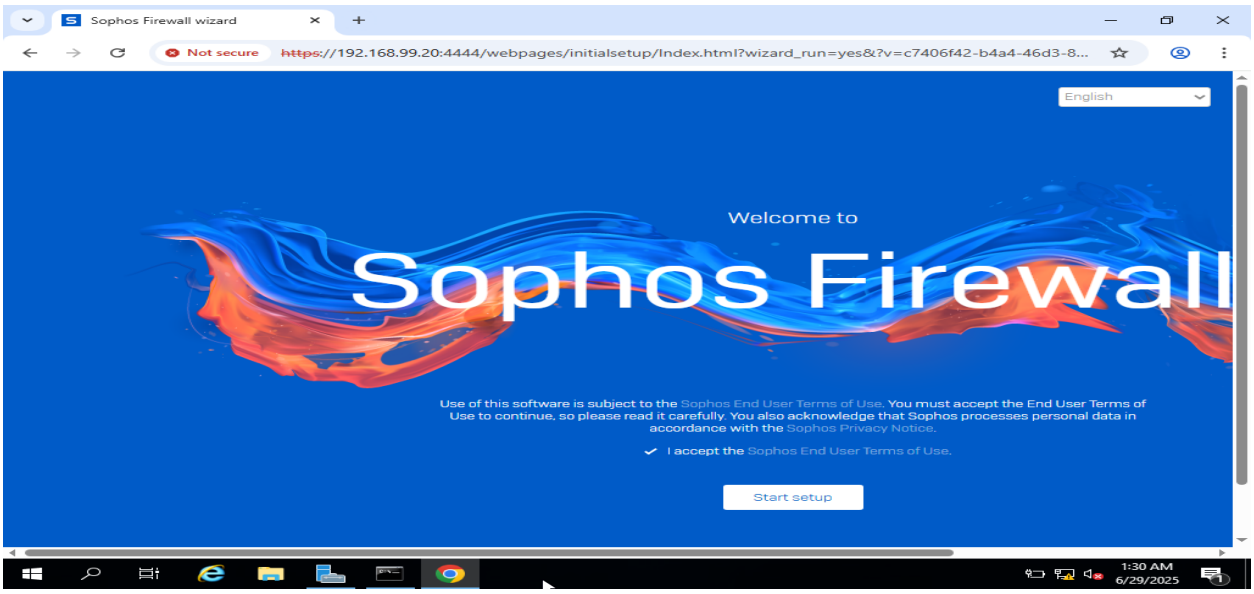


Figura 0-3: Tela inicial antes das configurações.

Prosseguir com a configuração básica, preenchendo credenciais, ao chegar na etapa de preenchimento da licença, selecione “I do not want to register now”, depois “Continue”.

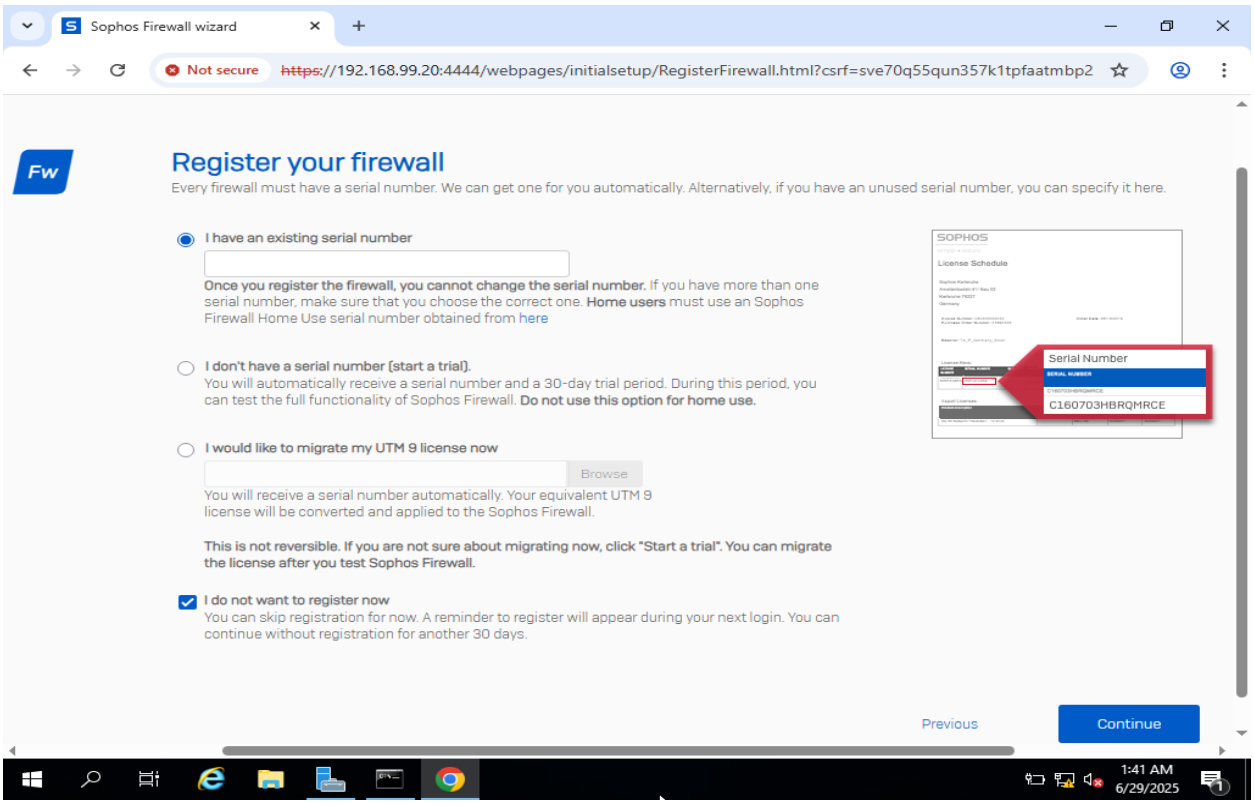


Figura 0-4: Registro de licença

Finalizada a instalação, insere-se as credenciais definidas. O username é “admin”.

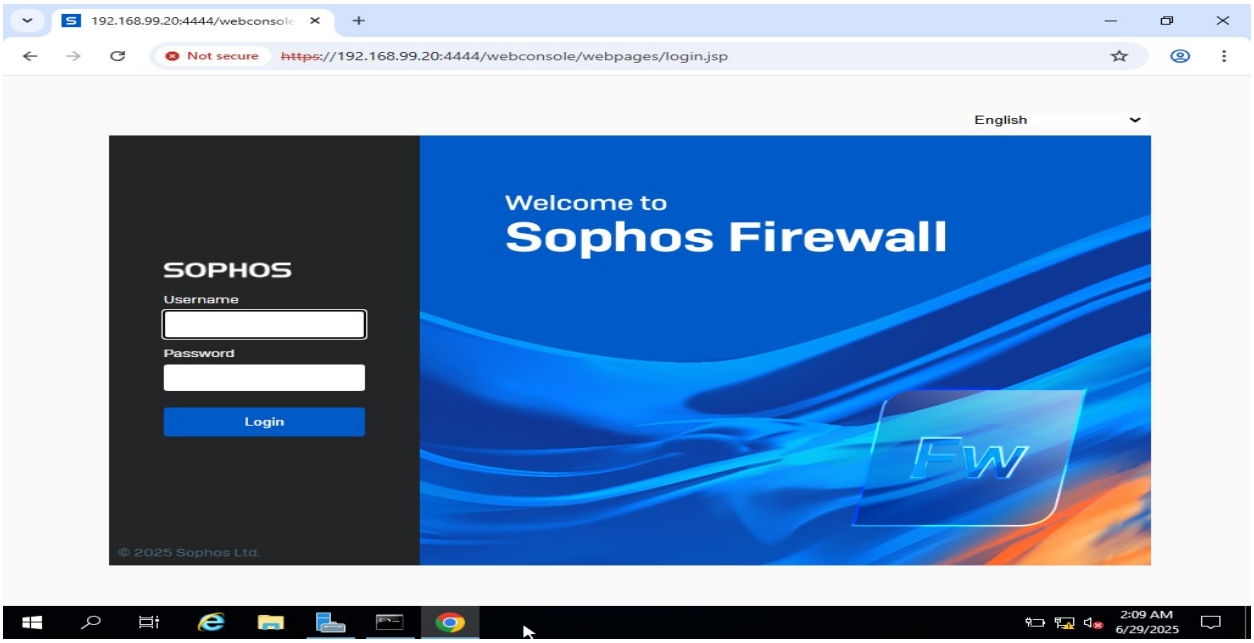


Figura 0-5: Tela de login

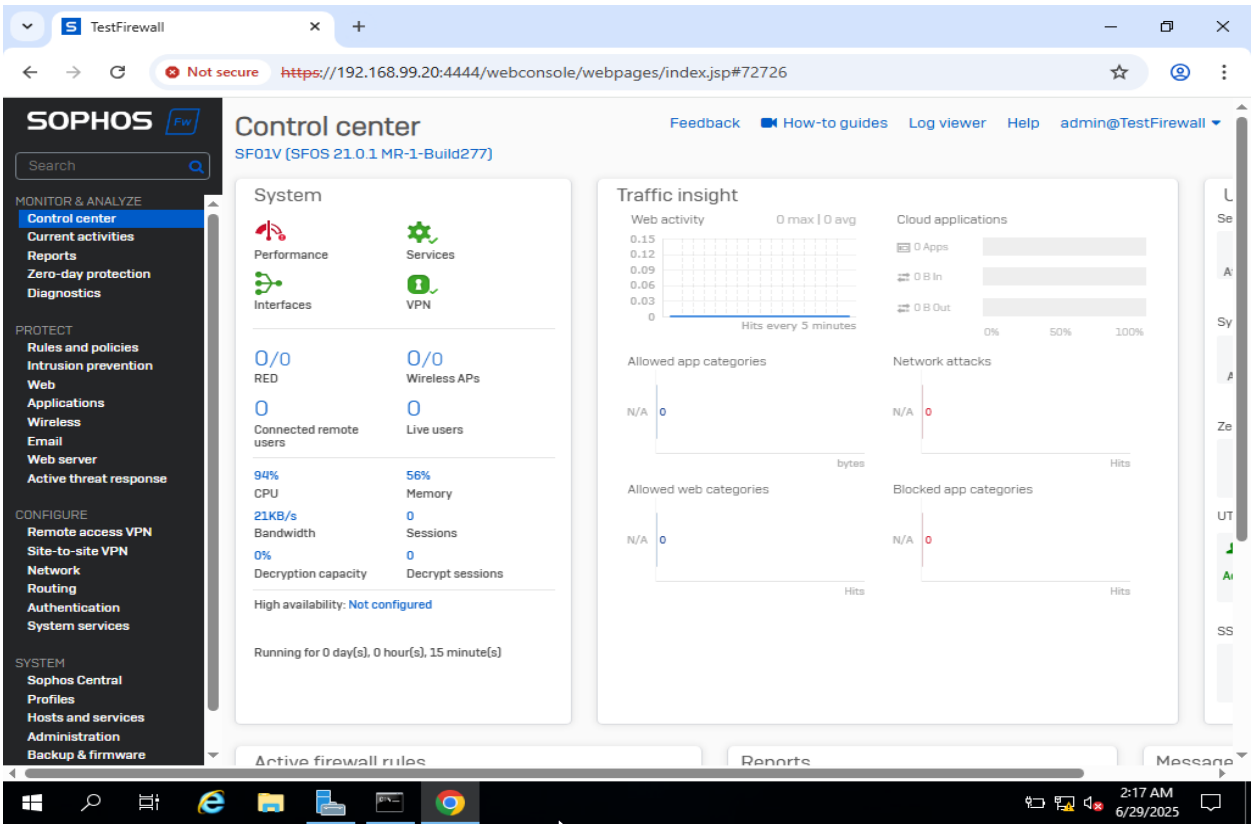


Figura 0-6: Painel central do Sophos

Anexo 7: Integração Sophos + AD DS

Para a integração do AD DS, primeiro é preciso verificar a comunicação entre o servidor e o Sophos e se o protocolo LDAP escuta a partir da porta 389.

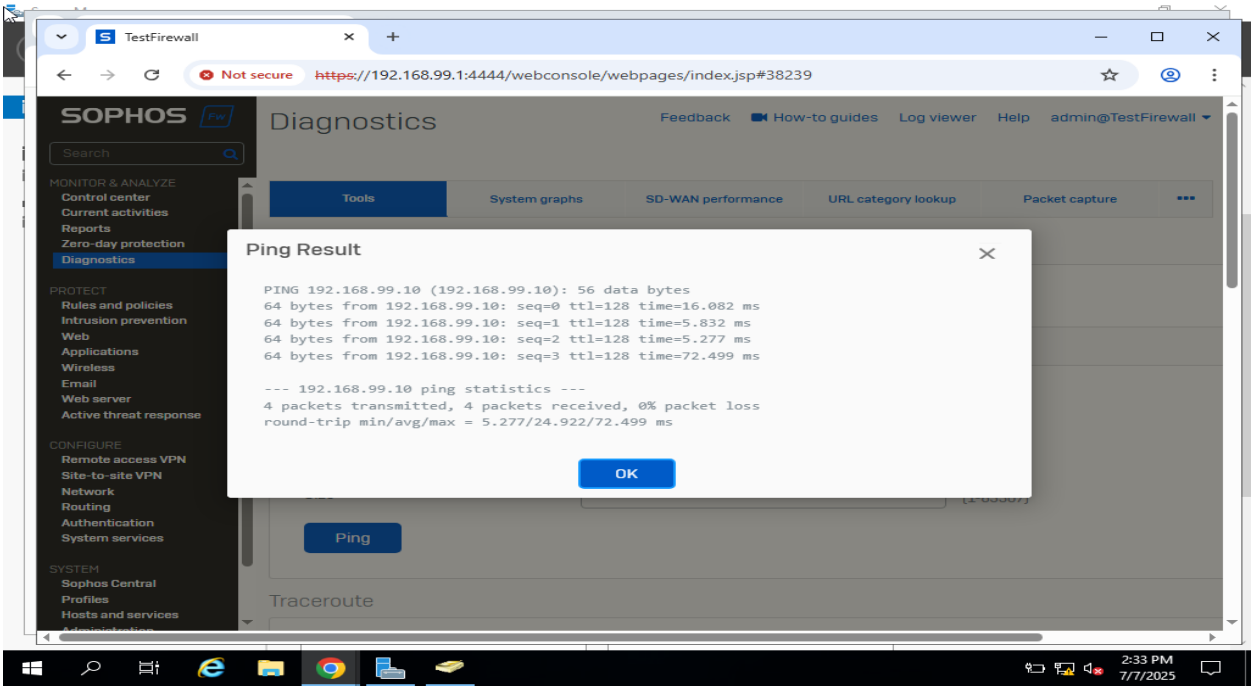


Figura 0-7: Teste de conectividade Sophos e o Servidor

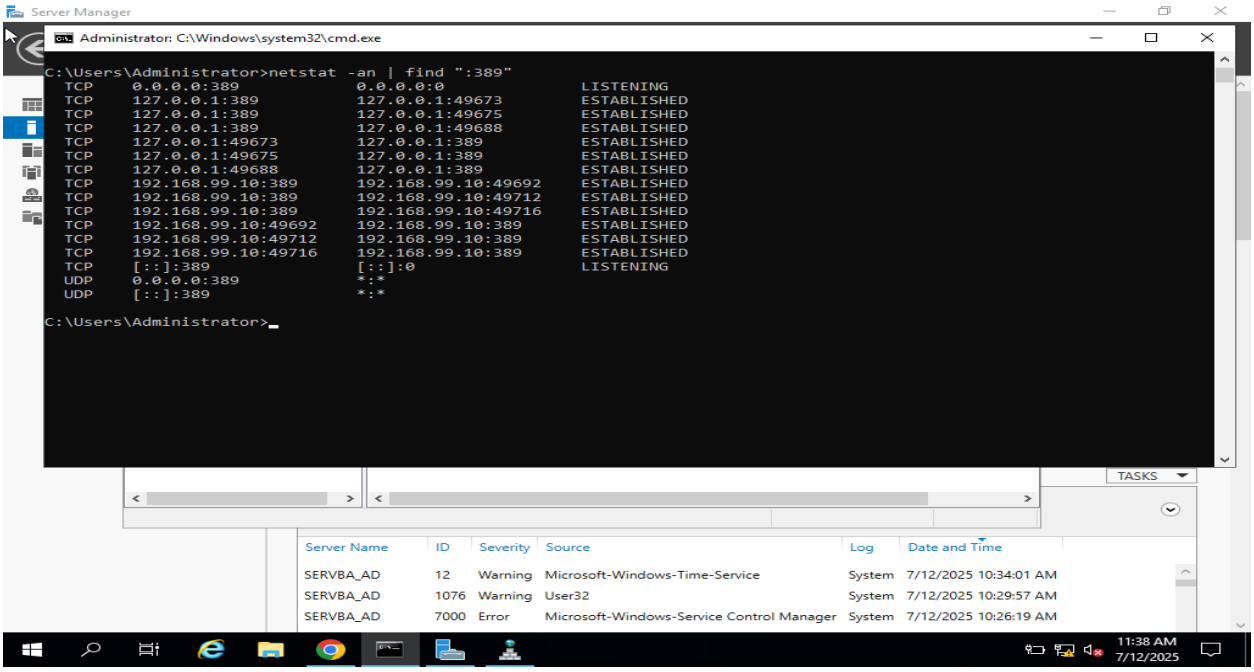


Figura 0-8: Teste de disponibilidade do protocolo LDAP

Após o sucesso dos testes acima, prossegue-se na integração do AD DS. Na administração web do Sophos, vai em “Configure” -> “Authentication” -> “Server” -> “Add Server” e prosseguir com o preenchimento dos campos.

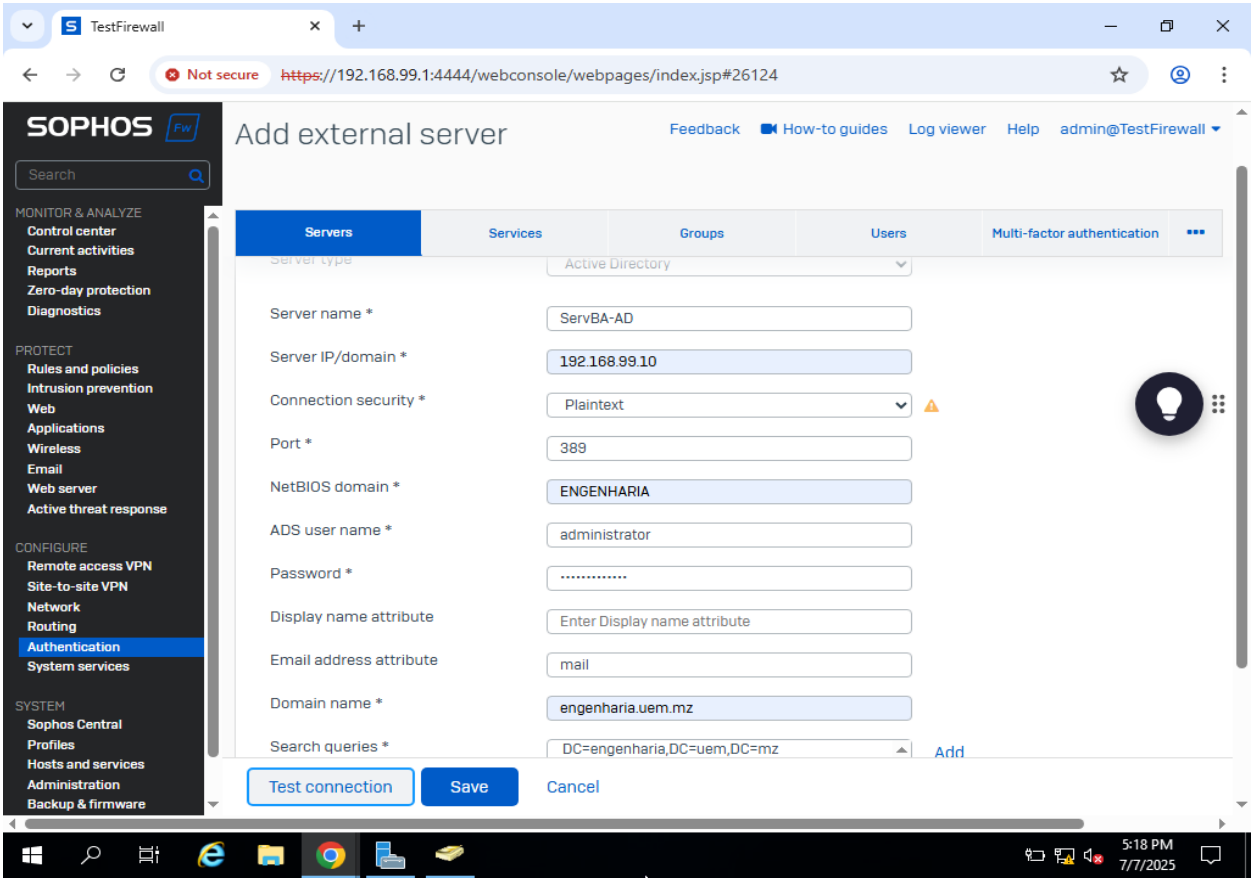


Figura 0-9: Sessão de informar o Sophos sobre o AD

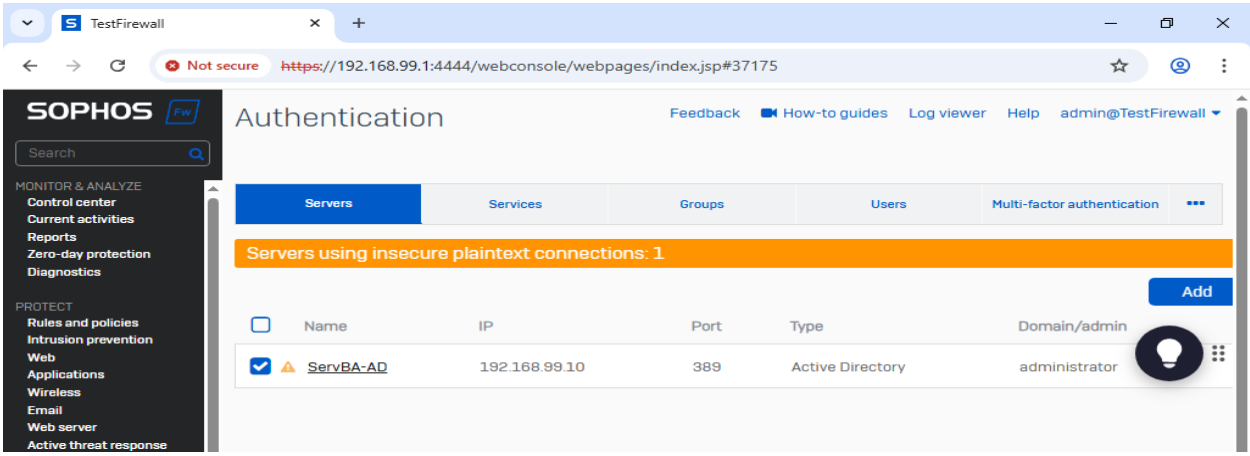


Figura 0-10: Confirmação da integração com sucesso

Como o Sophos e o Servidor já estão integrados, agora é só habilitar que o método de autenticação na firewall para acesso a internet e rede interna seja pelo servidor.

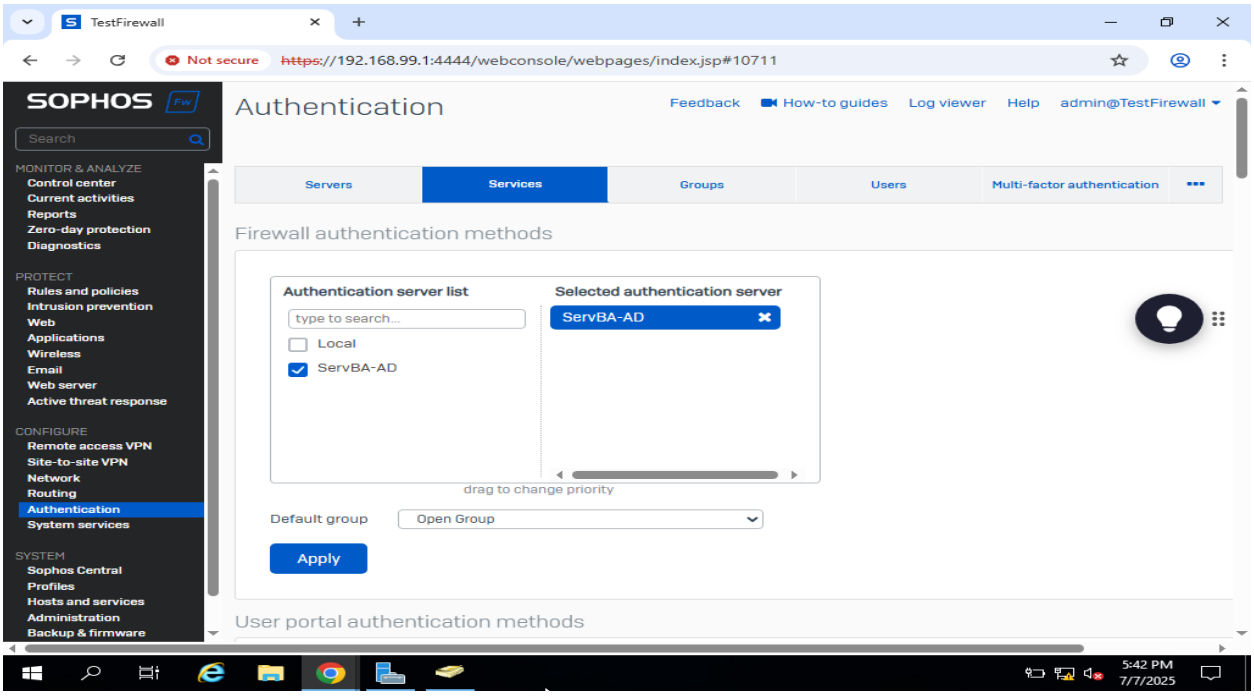


Figura 0-11: Método de acesso a internet e rede interna

Para a criação de VLANs ou configuração de interfaces físicas, é necessário que primeiro se crie as zonas, as quais vai abrigar as interfaces ou sub-interfaces.

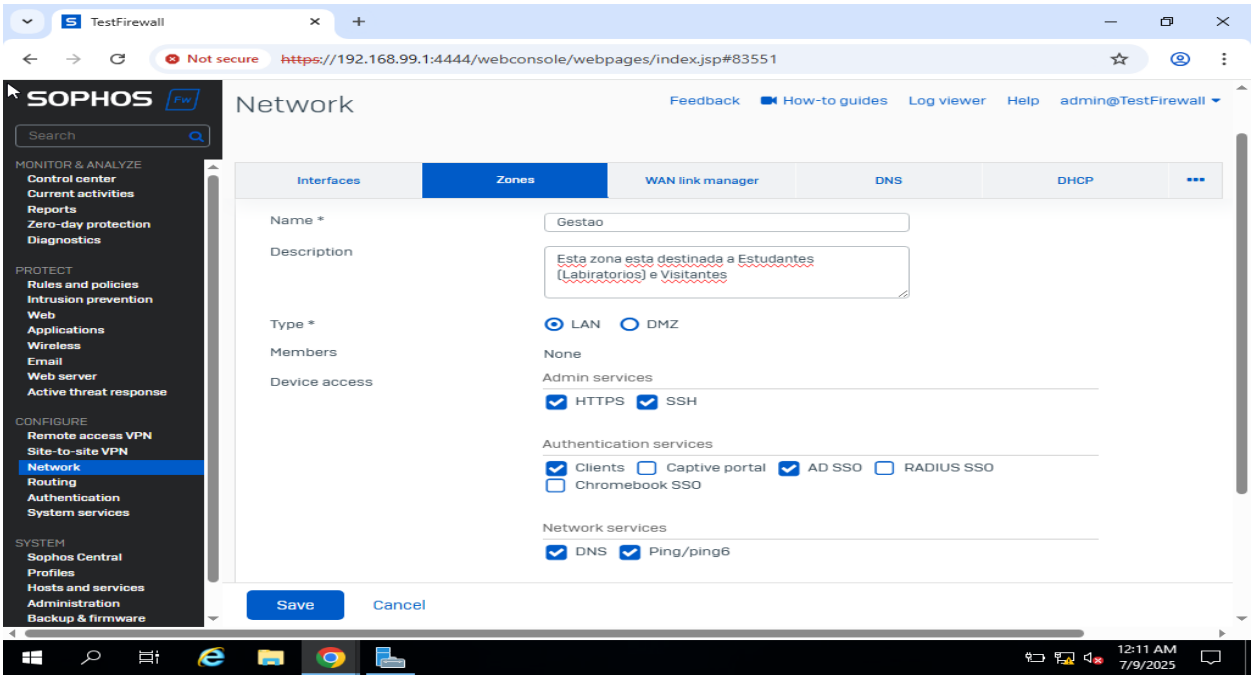


Figura 0-12: Criação da zona Gestao

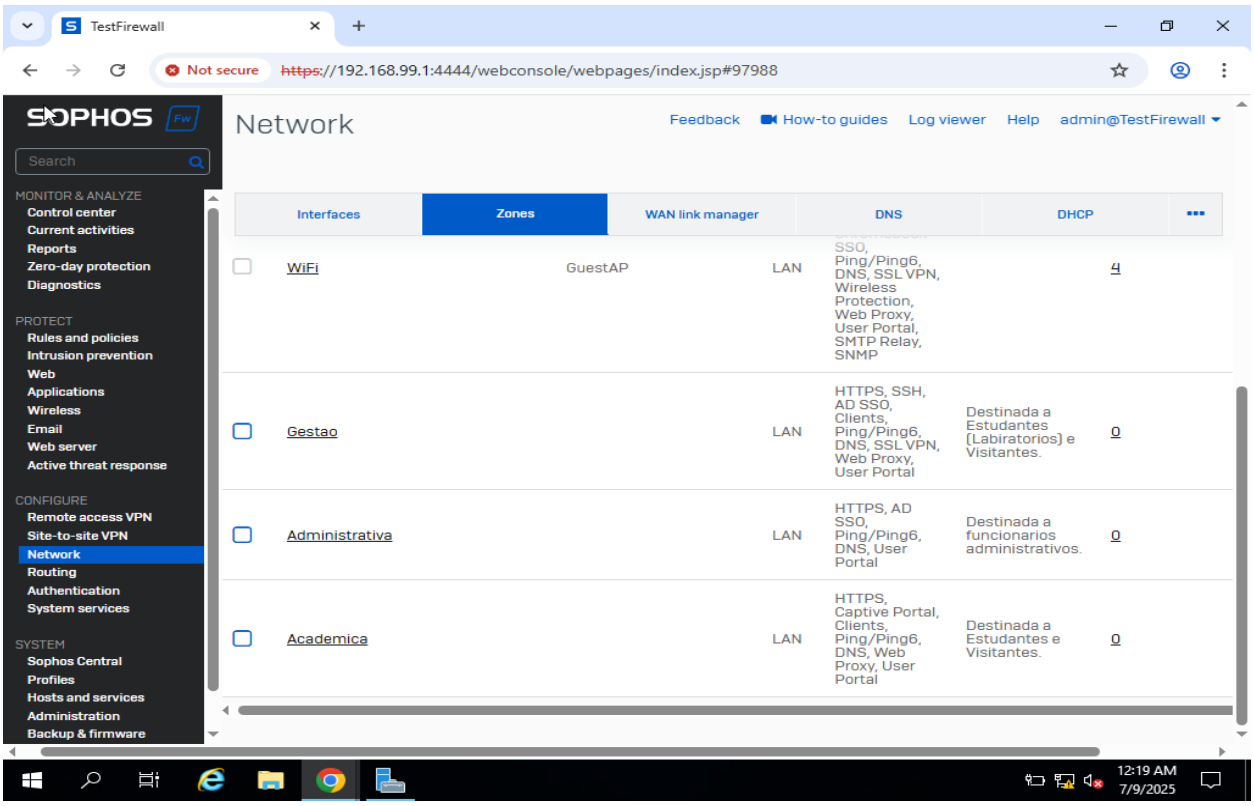


Figura 0-13: Três zonas e seus serviços

Para a criação de VLANs segue-se o mesmo roteiro que a configuração de interfaces físicas.

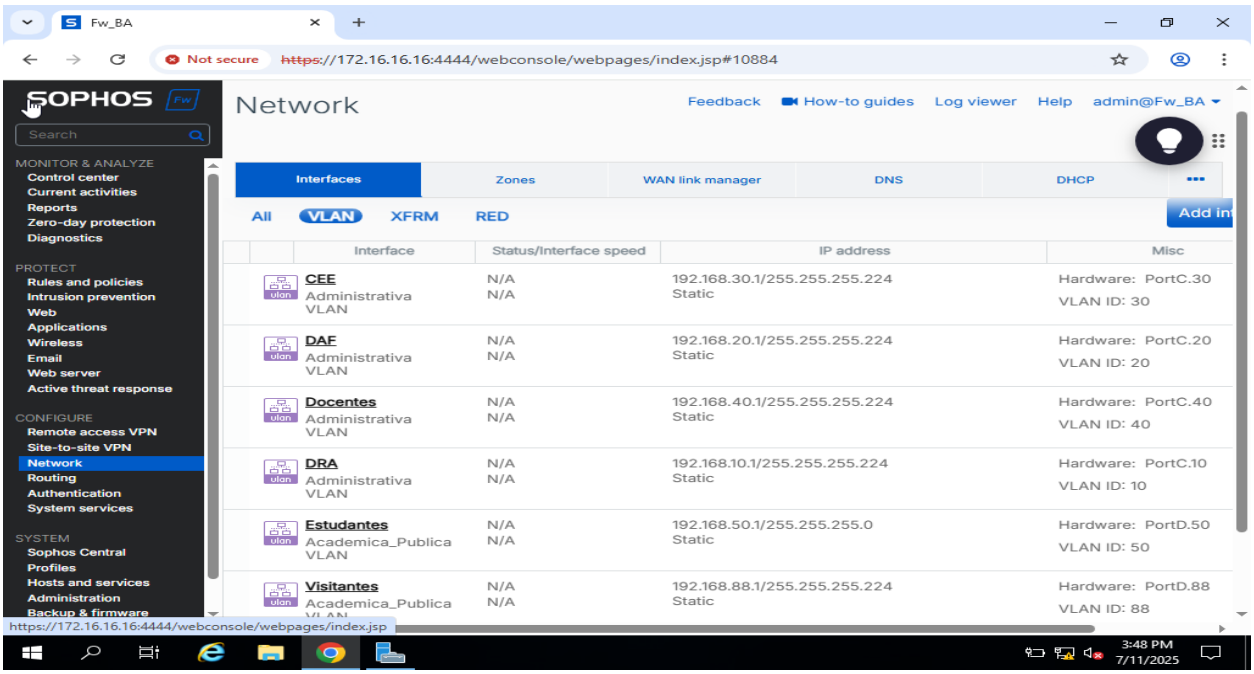


Figura 0-14: VLANs criadas e atribuidas a zonas e interface fisica

Há necessidade de configurar e habilitar o DHCP por cada sub-rede.

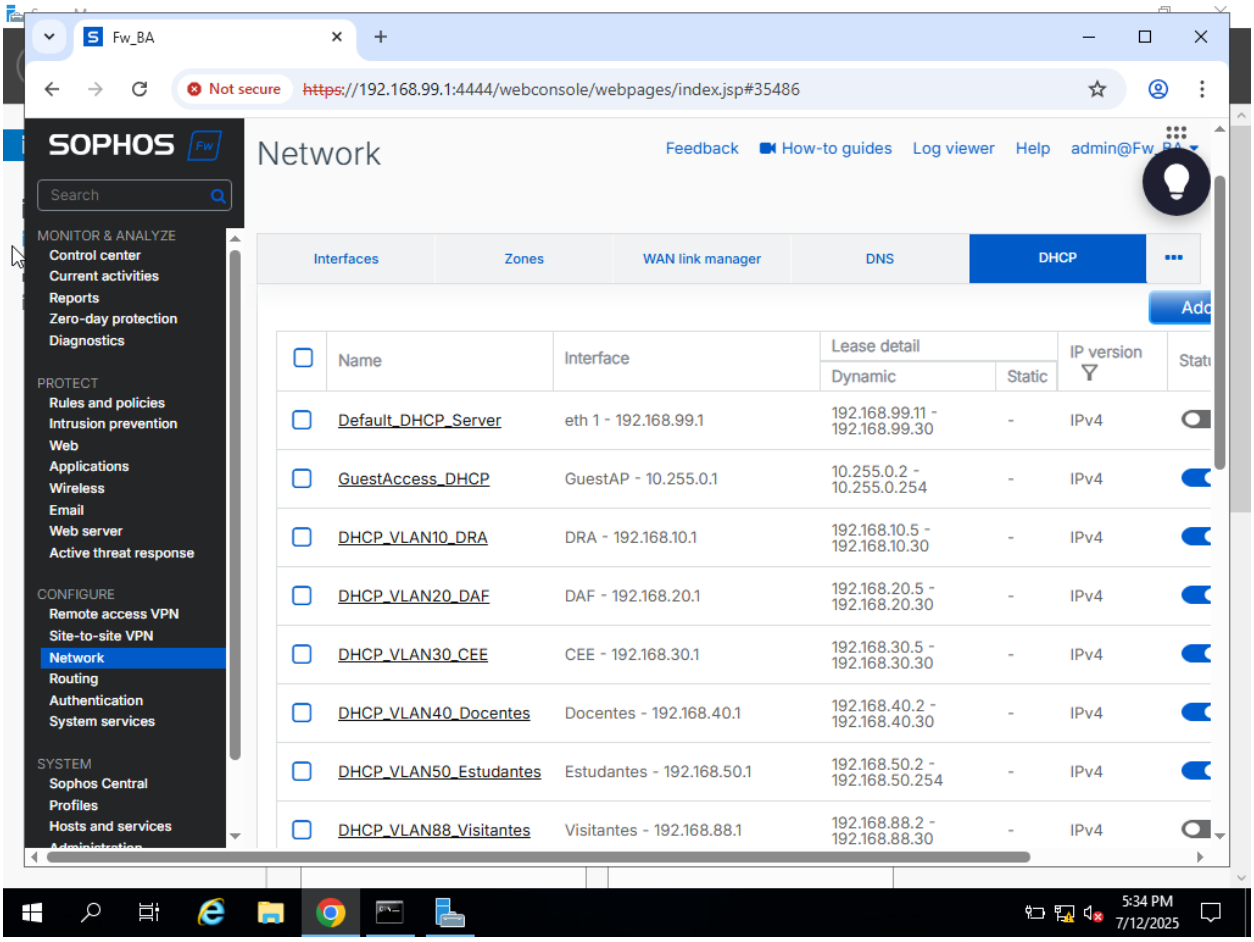


Figura 0-15: DHCP por sub-rede

Anexo 8: Guião da entrevista

Universidade Eduardo Mondlane

Faculdade De Engenharia

Departamento de Engenharia Electrotécnica

Guião da entrevista

1. Quais são os principais activos de rede existentes na infra-estrutura (ex.: servidores, firewalls, switches, access points, etc.)?
2. Como está estruturada a segmentação da rede? Existem VLANs definidas por departamentos ou funções?
3. Quantos blocos de endereçamento IP estão em uso? Os endereços são geridos por DHCP ou estáticos?
4. Quantas estações de trabalho existem no bloco administrativo e como estão organizadas (por departamentos, pisos, funções)?
5. Existem mecanismos de segurança actualmente implementados para proteger a infra-estrutura contra ameaças?
6. Quais são os meios utilizados pelos colaboradores para a partilha de ficheiros e troca de informação no âmbito do trabalho?
   - Pastas partilhadas na rede
   - Pen drives
   - E-mail institucional
   - Aplicações como Whatsapp ou outras
7. As estações de trabalho estão integradas num domínio centralizado? Como é feito o controlo de acesso dos utilizadores?

Anexo 9: Guião do questionário

Universidade Eduardo Mondlane

Faculdade De Engenharia

Departamento de Engenharia Electrotécnica

Guião do questionário

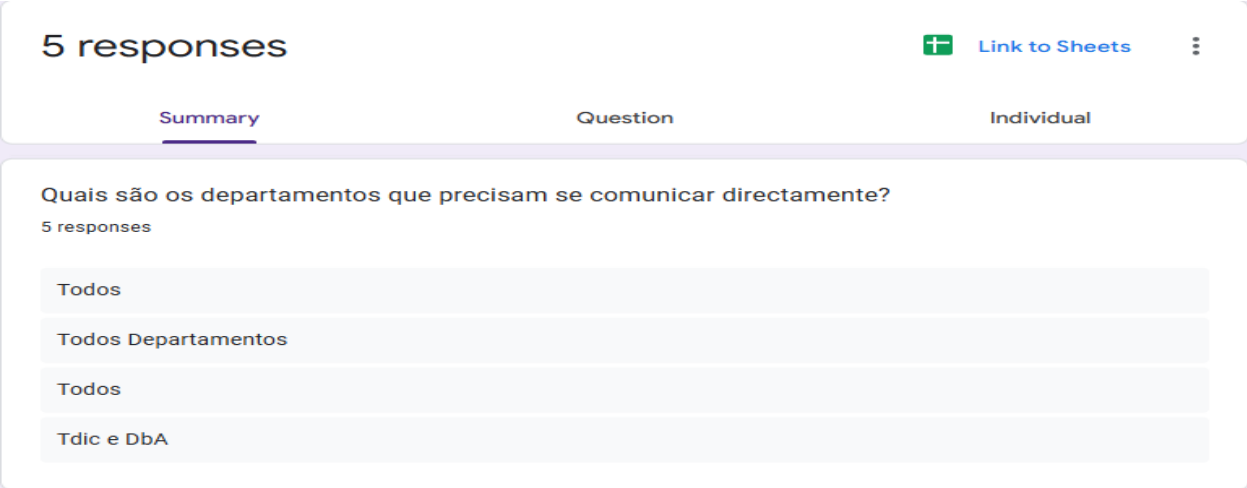
NB: Este questionário contém questões abertas e de resposta única. As que tem * são de carácter obrigatório.

1. Quais são os departamentos que precisam se comunicar directamente? *
2. Há restrições de acesso entre sectores (Ex.: RH não deve acessar redes do DAF)? *
3. Se na pergunta acima respondeu SIM, quais são esses sectores?
4. Quais serviços críticos dependem da rede? *
5. Existem políticas de backup de configurações? *
6. Como têm tido conhecimento sobre incidentes na infra-estrutura de rede?
7. Como são tratados incidentes de segurança? *
8. Quais aplicações apresentam mais problemas?
9. Já sofreu com lentidão em períodos específicos? *

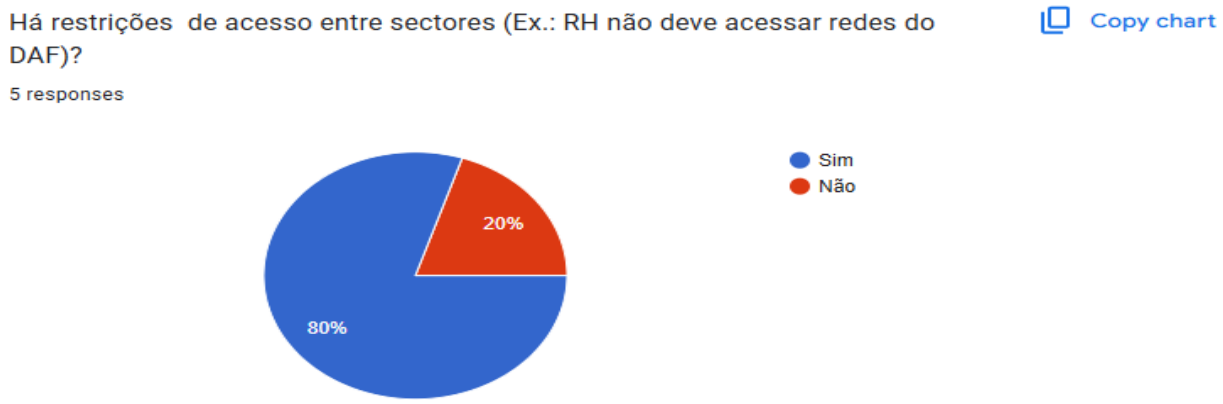
Como o questionário foi elaborado no google forms e enviado o link para o grupo de Whatsapp dos colaboradores do DTIC, partilho anexos das respostas obtidas.

Respostas:

1.



2.



3.

Se na pergunta acima respondeu SIM, quais são esses sectores?

4 responses

São Os Departamentos, porque a rede esta segmentada

A infraestrutura da Huawei no Deel nao consegue se comunicar com os APs nos outros Departamentos como Cadeiras Gerais

A rede esta segmentada

Hshehs

4.

Quais serviços críticos dependem da rede?

5 responses

E-mail's , impresssão e outros

Registo Academico e Daf

Registo Académico, DAF, Secretarias dos Departamentos Académicos, Direcção

DAF, DRA,

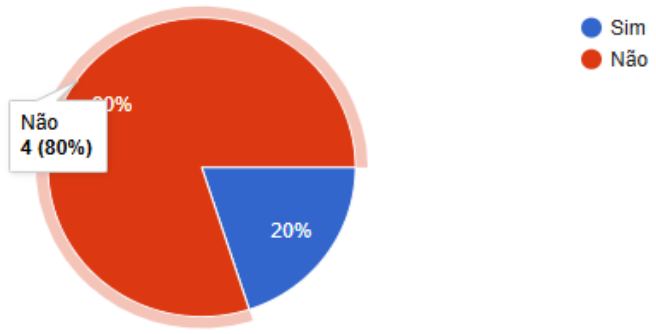
Jsjehs

5.

Existem políticas de Backup de configurações?

Copy chart

5 responses



6.

Como têm tido o conhecimento sobre incidentes na infraestrutura de rede?

5 responses

- Não Posso responder, porque a Ciuem é que faz a interveção nesses casos
- Quando somos reportados pelo usuarios
- Através de informações fornecidas pelos usuários
- Sem Informacao
- Hshehsh

7.

Como são tratados incidentes de segurança?

5 responses

- Está na respossablidade da Ciuem
- Ainda nao temos uma policitca de seguranca, as vezes procuramos ajuda no Centro de Informatica da UEM
- Backups regulares, senhas de acesso
- A Ciuem é que tem feito interveção
- Hshshshs

8.

Quais aplicações apresentam mais problemas?

4 responses

- Os sistemas Operativos
- Siga
- Sistema Operacional
- Hshshsh

9.

Já sofreu com lentidão em períodos específicos?

Copy chart

5 responses