INSTITUTO SUPERIOR DE CIÊNCIAS DE EDUCAÇÃO DA HUÍLA

ISCED-HUÍLA

Melhoria da Segurança da Rede de Computadores no Instituto Superior de Ciências da Educação da Huíla

Autores: Alcides Paulo Cassanga

Lino Carlos Mendonça Guelepete

LUBANGO

2023

INSTITUTO SUPERIOR DE CIÊNCIAS DE EDUCAÇÃO DA HUÍLA

ISCED-HUÍLA

Melhoria da Segurança da Rede de Computadores no Instituto Superior de Ciências da Educação da Huíla

Trabalho apresentado para a obtenção do Grau de Licenciado em Informática Educativa

Autores: Alcides Paulo Cassanga

Lino Carlos Mendonça Guelepete

Tutor: Tomás Lucas Selombo, Msc.

LUBANGO

2023

INSTITUTO SUPERIOR DE CIÊNCIAS DE EDUCAÇÃO DA HUÍLA

ISCED-HUÍLA

DECLARAÇÃO DE AUTORIA DO TRABALHO DE LICENCIATURA

Temos consciência que a cópia ou o plágio, além de poderem gerar responsabilidade civil, criminal e disciplinar, bem como reprovação ou a retirada do grau, constituem uma grave violação da ética académica.

Nesta base, eu ALCIDES PAULO CASSANGA e LINO CARLOS MENDONÇA GUELEPETE, estudantes finalistas do Instituto Superior de Ciências de Educação da Huíla (ISCED-Huíla) do curso de Informática Educativa, do Departamento de Ciências Exactas, declaramos, por nossa honra, ter elaborado este trabalho, só e somente com o auxílio da bibliografia que tivemos acesso e dos conhecimentos adquiridos durante a nossa carreira estudantil e profissional.

Lubango, aos 31 de Maio de 2023

O Autor

_____

O Autor

_____

Dedicatória

A minha amada esposa Tina e as minhas queridas filhas Alcidiane e Agnes, por serem motivo da minha alegria. Aos meus pais João Eusébio Cassanga e Maria Fernanda Augusta por desde cedo terem se preocupado em colocar-me na escola, por me amarem e muito contribuíram para a minha formação. Aos meus irmãos pelo apoio incondicional.

Alcides Paulo Cassanga

A minha querida avó, Maria Tchilombo por acreditar em mim, me amar e apoiar incondicionalmente. Ao meu querido tio Francisco Pelé e a minhas mães Florentina Mendonça e Juliana Tchilombo pelo apoio e incentivo dado ao longo da minha caminhada estudantil. A minha amada esposa Eva e os meus queridos filhos Almir e Luna, por despertarem em mim a força, dedicação e vontade de vencer. Em memória da minha amada e eterna mãe Rosa Selestina Tchilombo Mendonça que muito me amou.

Lino Carlos Mendonça Guelepete

Agradecimentos

A Deus pai todo poderoso, pelos seus dons despertados em nós por meio de Jesus Cristo, em particular o dom da Vida, Saúde, Sabedoria e Ciência.

Ao professor **Tomás Lucas Selombo**, pelos conhecimentos transmitidos no decorrer do curso, mostrou ser um óptimo e excelente profissional, além de contribuir com a orientação deste projecto, por ter depositado sua confiança no nosso potencial para a realização do mesmo, pelo apoio, dedicação, bem como pelos conselhos sábios e motivadores que nos transmitiu, ao longo desta nossa jornada estudantil e não só muito obrigado por tudo.

Agradecemos aos nossos pais e avós por não terem poupado esforços para que hoje chegássemos até aqui, aos nossos irmãos, tios, primos, sobrinhos e amigos que acreditaram em nós nos nossos feitos.

As nossas amadas esposas, pelo amor, carinho e paciência que têm dedicado a nós e por estarem connosco nos bons e maus momentos.

Ao corpo docente, direcção e coordenação do curso de Informática Educativa, em particular o Professor **Salomão Pena**, que não mediram esforços para oferecer um ensino diversificado, e que contribuiu para aquisição de experiência e qualificação profissional.

Agradecemos ao pessoal do Departamento de Tecnologia de Informação e Comunicação do ISCED-Huíla que muito ajudaram para a realização do projecto, e a todos os nossos colegas, e todos que de uma maneira directa ou indirecta contribuíram para que este sonho se tornasse realidade.

Resumo

As instituições de ensino são de grande importância para assegurar o desenvolvimento de um país. Por isso, torna-se necessário que os entes académicos, administrativos e tecnológicos sejam constantemente aprimorados para garantir o sucesso das actividades das respectivas instituições. O Instituto Superior de Ciências de Educação da Huíla em particular, tem elencado o desafio constante de melhoria do seu ambiente tecnológico, fundamentalmente no que concerne às tecnologias de comunicação, como forma de facilitar a partilha de informações entre todos actores do processo de ensino e aprendizagem. Entretanto, a troca de informações sem uma segurança adequada pode se tornar perigosa e consequentemente atrair terceiros interessados em roubar tais dados e infectar redes, acarretando em perdas substanciais. Este trabalho de investigou a questão: como melhorar a segurança a nível da rede de computadores do Instituto Superior de Ciências da Educação da Huíla? E teve como objectivo geral de investigação, implementar mecanismos de segurança a nível da rede de computadores do ISCED-Huíla. Trata-se de uma pesquisa tipo quantitativa aplicada, na qual se utilizou como método de projecto de rede o Bottom-up, que permitiu fazer uma abordagem mais detalhada de cada parte do de projecto de sistema. A pesquisa foi desenvolvida no contexto Instituto Superior de Ciências da Educação da Huíla dando sequência da proposta defendida por Valeriano Sunda (2021). A recolha de dados foi realizada utilizando inquérito por questionário, na qual participaram quatro (4) funcionários responsáveis pela gestão da rede, e quinze (15) trabalhadores administrativos utilizadores da rede de computadores da instituição. Após o diagnóstico e feito a triangulação com a parte teórica do estudo, identificou-se a necessidade de implementação de mecanismos de segurança na rede de computadores da instituição. Com a percepção deste problema, optou-se por buscar proteger a rede através da implementação da tecnologia pfSense. Concluiu-se que com a implementação do pfSense houve melhorias significativas na segurança da rede de computadores, com realce na autenticação de usuários na rede via email institucional, regras de firewall e web cache.

Palavras-Chaves: Redes de Computadores, Mecanismos de Segurança, Tecnologia pfSense, Instituições de ensino Superior.

Abstract

Educational institutions are of great importance to ensure the development of a country. Therefore, it is necessary that the academic, administrative and technological entities are constantly improved to guarantee the success of the activities of the respective institutions. The Higher Institute of Educational Sciences in Huíla, in particular, has listed the constant challenge of improving its technological environment, fundamentally with regard to communication technologies as a way of facilitating the sharing of information between all actors in the teaching and learning process. However, exchanging information without adequate security can become dangerous and consequently attract third parties interested in stealing such data and infecting networks, resulting in substantial losses. This research has as an investigation question how to improve security at the computer network level of the Higher Institute of Education Sciences of Huíla? and its general objective was to implement security mechanisms at the level of the ISCED-Huíla computer network. This is an applied quantitative research, in which Bottom-up was used as a network method, which allowed a more detailed approach to each part of the system project. The research was developed in the context of the Instituto Superior de Ciências da Educação da Huíla, following the proposal defended by Valeriano Sunda (2021). Data collection was carried out after completing the surveys, in which four (4) employees responsible for managing the network and fifteen (15) administrative workers who used the institution's computer network participated. After the diagnosis and the triangulation with the theoretical part of the study, the need to implement security measures in the institution's computer network was identified. With the perception of this problem, it was decided to seek to protect the network through the implementation of pfSense technology. With the implementation of pfSense there were significant improvements in computer network security, with emphasis on user authentication on the network via institutional email, firewall rules and web cache.

Keywords: Computer Networks, Security Mechanisms, pfSense Technology, Higher Education Institutions.

Índice

Índice de figuras

Índice de tabelas

Índice de gráficos

Lista de abreviaturas

ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
APD	Agência de Protecção de Dados
ARP	Address Resolution Protocol
AS	Authentication Server
ATM	Asynchronous Transfer Mode
BSD	Berkeley Software Distribution
CD	Compact disc
CIA	Confidentiality, integrity e availability
CID	Centro de Informação e Documentação
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial of servisse
DVD	Digital Versatile Disc
D-NAT	Destination Network Address Translation
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HIDS	Host-based intrusion detection system
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
LAN	Local Area Network
LEDs	light-emitting diode
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
OSI	Open Systems Interconnection
PC	Computador Pessoal

PoE	Power Over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RARP	Reverse Address Resolution Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
S-NAT	Source Network Address Translation
TCP	Transmission Control Protocol
TI	Tecnologia de Informação
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide area network
WLAN	Wireless Local Area Network
WWW	World Wide Web

Introdução

Introdução

Durante as primeiras décadas, as redes de computadores eram utilizadas principalmente por pesquisadores universitários e funcionários de empresas, tendo um uso basicamente formado por compartilhamento de impressoras e troca de mensagens electrónicas. Neste cenário, a preocupação com segurança era quase nula. Porém, com o avanço e o aumento da utilização da tecnologia, veio a necessidade em pensar na segurança da rede de computadores e a protecção dos activos que ali se encontram (Tanenbaum & Feamster, 2021)

Com o crescimento das comunicações entre as redes de computadores, faz-se necessário a utilização de mecanismos de prevenção de ataques e furtos de informações, seja ela no servidor interno ou na internet. As pessoas e grupos, acobertados pela distância e anonimato, tentam burlar a segurança dos sistemas informatizados das organizações no intuito de extrair benefícios indevidos da exploração da bem chamada informação.

Diante desse contexto, as informações quanto aos dados pessoais para variadas actividades, tais como: identificação, classificação, autorização e tantas outras, transformou num elemento essencial para o mercado e, sobretudo, para que a pessoa consiga se mover, com autonomia e liberdade, nos corredores denominado sociedade da informação (Barbosa, et al, 2021).

E assim, surge o conceito de segurança da informação sendo definida como área de conhecimento dedicada à protecção de dados contra acessos não autorizados, alterações indevidas ou indisponibilidade (Sêmola, 2014). Conforme descrito pela Lei de Protecção de Dados Pessoais (2011), a segurança da informação protege as informações registradas, sem importar onde estejam situadas: impressas em papel, discos rígidos dos computadores ou na memória das pessoas.

Para se implantar um projecto de segurança da informação em uma organização é necessário antes de tudo definir as políticas, mecanismos de segurança, e procedimentos, ferramentas de protecção e autenticação, e a sua associação custo benefício. Determinar o nível de segurança é fundamental. Este nível de segurança deve assegurar que cada colaborador só poderá aceder ao conteúdo que lhe é

permitido e que faz parte do seu trabalho e não poderá aceder a um dado que for de outro departamento que não tenha nenhuma associação com as funções na qual desempenha.

Uma política de segurança corresponde a um conjunto de regras, que especificam o que pode e o que não pode ser feito, geralmente aplicada a uma rede local de computadores (principalmente em uma rede corporativa – ambiente de trabalho), bem como as penalidades as quais estão sujeitos os utilizadores que dela não cumprem (Macedo et al, 2018).

Dentro do escopo de segurança da informação, existem diferentes tipos de ameaças e ataques, e as intrusões podem ser consideradas um destes tipos de ameaças. Um exemplo de intrusão é um adversário obter acesso não autorizado a dados sensíveis, burlando protecções de controle de acesso do sistema (Stallings & Brown, 2017).

Assim, Maschio (2017) diz que a utilização de um firewall é uma acção simples a ser adoptada, implicando toda a política de rede, onde o principal objectivo é prevenir e monitorar os acessos não autorizados. Em geral, um firewall é um “muro” entre a rede local e a externa, onde se filtra todos os pacotes de dados, aplicações, proxy de rede, e tráfego das informações.

Maschio (2017), complementa ainda que não é suficiente utilizar apenas uma medida de segurança, e como a necessidade de actuar na área de segurança é cada vez maior, adoptar o sistema pfSense como firewall se torna uma boa escolha, pois trata-se de uma alternativa totalmente gratuita. O pfSense, baseia-se num no sistema operacional FreeBSD, assumindo e herdando do mesmo as estratégias de segurança, e adicionando funções de filtro e roteamento.

Antecedentes do tema

O tema em estudo é bastante pertinente, pois alguns autores já abordaram sobre temas relacionados ao mesmo. Assim, citam-se alguns trabalhos de fim do curso:

Ezequiel Tchimissi elaborado em 2018, no seu trabalho de fim do curso com o tema “Implementação de Mecanismos de Segurança e Desempenho na Rede de

Computadores do Instituto Superior de Ciências de Educação da Huíla". Para o autor, a instituição em estudo possui já uma infra-estrutura de redes de computadores. Porém o autor apresenta algumas dificuldades na rede, uma vez que, a maior parte das dificuldades constatadas estavam voltadas para problemas de segurança e desempenho da rede. Então o autor recomenda a implementação de firewall para melhorar a segurança, o desempenho e protecção do controlo de tráfego da rede. O trabalho desenvolvido foi, de certa forma, aproveitado, pois na rede proposta foi utilizado um Firewall, padronizando a configuração para diversos elementos da rede.

Destacamos ainda o autor Faustino Sita Sunda no seu trabalho elaborado em 2021 com o tema "Proposta de implementação de Mecanismos de Segurança na Rede de Computadores do ISCED-Huíla", cujo o objectivo geral foi Implementar Mecanismos de Segurança e Desempenho na Rede de Computadores do Instituto Superior de Ciências de Educação da Huíla. O mesmo faz uma abordagem sobre os principais mecanismos de segurança a se ter em conta na instituição propondo serviços integrados de autenticação Radius Firewall e proxy que pode contribuir bastante no processo de segurança da rede de computadores. Assim, o seu trabalho serviu de guia para a realização do projecto em estudo.

Justificação da investigação

A relevância do tema prende-se pelo facto do mesmo ser actual e pelo vasto interesse que suscita na revolução do mundo de TI (Tecnologia de Informação), pois, com o avanço da tecnologia tem-se registrado também vários e muitos ataques cibernéticos, que vão desde invasões e sequestros de dados.

O processo de implementação de uma infra-estrutura de rede numa empresa é de suma importância para uma melhor gestão dos activos de hardware e software, uma infra-estrutura bem montada, organizada, passa mais segurança, confiabilidade, tanto para utilizadores internos, tanto como externos que utilizam os serviços da empresa que passam pela área de TI.

A instituição, objecto de estudo, encontra-se na província da Huíla, no Município do Lubango, é uma instituição de ensino que alberga cerca de treze (13) cursos, e as

mesmas distribuídas em diferentes repartições, é composta ainda por várias secções, como o DAAC, o Herbário, Secretaria Geral, Sala do Director, Departamento de Tecnologias de Informação e Comunicação entre outros. A mesma, actualmente já dispõe de uma Rede de Computadores, dividida em vários segmentos físicos e lógicos, porém o firewall configurado, tem apresentado vários constrangimentos, desde a latência e invasões de dados.

Frente a isso, este trabalho procurou melhorar a segurança a nível da segurança da rede de computadores do Instituto Superior de Ciências da Educação da Huíla utilizando o software livre pfSense que desempenha um papel de firewall.

Desenho teórico

Questão de investigação

Como melhorar a segurança a nível da rede de computadores do Instituto Superior de Ciências da Educação da Huíla?

Objectivos de investigação

Objectivo geral

O presente trabalho tem como objectivo geral o seguinte:

- Implementar mecanismos de segurança a nível da rede de computadores do ISCED-Huíla.

Objectivos específicos

De modo a alcançar o objectivo principal aqui proposto, houve a necessidade de determinar os seguintes objectivos específicos:

- Diagnosticar o ambiente de segurança da informação /electrónica no ISCED-Huíla;
- Fundamentar teoricamente sobre a importância da protecção de sistemas e redes de computadores, e consequente protecção dos activos das organizações;

- Modelar o projecto da rede de computadores;
- Configurar os mecanismos de segurança em servidores e na rede local do ISCED-Huíla.

Desenho metodológico

Metodologia empregue

Pretendendo alcançar os objectivos traçados, levou-nos a uma opção metodológica que se apega nos aspectos aplicada quantitativas. Segundo Gil (2017), a pesquisa aplicada abrange estudos elaborados com a finalidade de resolver problemas identificados no âmbito das sociedades em que os pesquisadores vivem tendo como objectivo principal gerir conhecimento para aplicação prática e imediata.

Segundo Bickman & Rog (2008), esta metodologia tem duas fases principais - planejamento e execução e quatro estágios embutidos neles. Na fase de planejamento, o pesquisador define o escopo da pesquisa e desenvolve um plano de pesquisa abrangente. Durante a segunda fase, o pesquisador implementa e monitora o plano (desenho, recolha e análise de dados e procedimentos de gerenciamento), seguido de relatórios e actividades de acompanhamento.

População e Amostra

Para Afonso e Nunes (2019), a população é o grupo de todos os elementos que se pretende estudar e que possuem uma característica comum. Alvarenga (2012) diz que a população é formada pelo conjunto de pessoas ou casos que integra a comunidade a ser estudada.

Assim, para a realização deste projecto, considera-se como população indivíduos pertencentes ao quadro de funcionários do ISCED-Huíla responsáveis pelo gestão, monitoramento e manutenção da rede de computadores, e os trabalhadores administrativos da Instituição utilizadores da rede de computadores da instituição, que constitui um total de cinquenta (50).

Técnicas de Amostragem

De modo que as diferentes respostas ou opiniões possíveis na presente pesquisa possam aparecer de forma proporcional e representativa utilizou-se a técnica de

amostragem não probabilística intencional. Segundo Alchemer (2023), a amostragem intencional é um método de amostragem não probabilística em que os elementos seleccionados para a amostra são escolhidos ao critério do pesquisador. Neste tipo de amostragem os pesquisadores geralmente acreditam que podem obter uma amostra representativa utilizando um bom julgamento, o que resultará na economia de tempo e dinheiro. Foi utilizada essa técnica de maneira que trabalhássemos com os funcionários que mantivessem disponíveis a responder os inquéritos.

Assim sendo, a amostra foi constituída por quatro (4) funcionários responsáveis pela gestão da rede, e quinze (15) trabalhadores administrativos utilizadores da rede de computadores da instituição.

Métodos e Técnicas de Investigação

Métodos

Para se cumprir com os objectivos traçados na presente pesquisa houve a necessidade de se utilizar os seguintes métodos:

Método para projecto de rede

Bottom-up – O método Bottom-up é uma abordagem de projecto de sistema em que as partes de um sistema são definidas em detalhes. Ela inclui inicialmente o projecto das partes mais fundamentais que são então combinadas para fazer o módulo de nível superior. Esta integração de submódulos e módulos no módulo de nível superior é repetidamente executada até que o algoritmo completo requerido seja obtido. Nesta investigação tendo em conta o facto de já existir uma estrutura de rede instalada optou-se pela metodologia bottom-up que inicia com o projecto físico da rede, permitindo reaproveitar o que já existe (recursos e equipamentos) com o mínimo custo possível.

Técnicas de Recolha de dados

Análise documental – Nesta etapa, fez-se estudo dos documentos relacionados com a investigação em causa, retirando dos mesmos evidências que fundamentam as afirmações da pesquisa, particularmente o problema proposto, de forma a propor

uma orientação qualificada. Para além de obras de escritores renomados na segurança de Informática e Informação, foram ainda analisados os seguintes documentos: Lei 22/11 de 17 Junho - Protecção de Dados Pessoais, Lei 7/17 de 16 Fevereiro - Protecção das Redes e Sistemas Informáticos.

Observação – Segundo Conceito (2020), a observação consiste na medição ou examinação e no registro dos factos observáveis. A observação deve ser realizada tendo em conta os objectivos que se pretendem alcançar na investigação, de maneira a não deixar que as opiniões, os sentimentos e as emoções influenciem no trabalho científico. A observação também é considerada uma técnica de recolha de dados para conseguir informações sob determinados aspectos da realidade. Esta técnica foi utilizada na recolha de dados durante as visitas efectuadas ao local onde foi realizado o estudo.

Inquérito por Questionário – De acordo com Santos e Henriques (2021), é um instrumento de recolha de informação sobre uma população, a sua aplicação exige que se garanta um número de inquiridos que viabilize a análise estatística. Neste tipo de instrumento de dados é bastante comum encontramos questões abertas e fechadas. As perguntas abertas permitem respostas mais ricas e variadas, por sua vez, as perguntas fechadas possibilitam fazer o tratamento e análise de dados de maneira simplificada. Este método foi utilizado para obter as opiniões dos funcionários sobre o real contexto da rede de computadores do ISCED – Huíla, e detectar as principais dificuldades que têm encontrado com os problemas de segurança na rede.

Método de Análise de dados

Estatística - descritiva – Este método pode ser visto como uma representação sintetizada de algum processo complexo, o mesmo, foi criado de modo facilitar a análise quantitativa das as variantes envolvidas em um processo de investigação (Neogrid, 2022). Com este método fez-se a análise das frequências absolutas e relativas.

Estrutura do trabalho

Para além da introdução o trabalho em causa está estruturado da seguinte forma:

- Capítulo I – Neste capítulo é apresentado a fundamentação teórica sobre Mecanismos de Segurança de redes de computadores em ambientes corporativos, bem como os principais conceitos de diferentes autores em volta do assunto de modo a se obter um melhor entendimento acerca do tema em causa, assim como as principais tecnologias utilizadas para alcançar os objectivos propostos no trabalho.

- Capítulo II – Na abordagem deste capítulo, foca-se naquilo que é o nosso propósito, a visão geral da segurança e desempenho da rede de computadores do ISCED-Huíla.

- Conclusões e Sugestões – Fez-se um levantamento crítico dos resultados mostrados anteriormente, em função da fundamentação teórica. Como também, as principais dificuldades, conquistas e desafios ainda presentes são citados, a fim de criar um caminho que possa ser seguido também por outros pesquisadores.

- Bibliografia – Neste tópico foram apresentadas as fontes das ideias dos diferentes autores citados no projecto.

- Apêndice e Anexos – Permitiu abordar e ilustrar as configurações de cada medida de segurança implementada no projecto.

Capítulo I - Fundamentação teórica

Capítulo I - Fundamentação teórica

1.1. Conceitos gerais de redes de computadores

As redes de computadores e sistemas de comunicação, actualmente, são uma das tecnologias que mais crescem e têm atraído diversos estudos para essa área, bem como surgem-se muitas profissões que utilizam dessas ferramentas para seu êxito operacional.

Uma rede de computadores compreende na interconexão de dois ou mais computadores e dispositivos adicionais ligados por meio de recursos de comunicação, geograficamente distribuídos, permitindo deste modo, a troca de dados entre estas unidades e optimizando recursos de hardware e software.

De acordo com Tanenbaum e Woodhull (2021) o hardware é a parte física do computador, a qual inclui placas de circuito impresso, teclado, mouse, monitor, entre outros. E de acordo com Pressman e Maxim (2019) o software é um conjunto de instruções que quando executadas permitem a manipulação de dados e informações de forma impressa e também virtual.

1.1.1. Protocolos de redes de computadores

Os protocolos de rede determinam o formato e a ordem das mensagens trocadas entre duas ou mais entidades que se comunicam, bem como as acções realizadas na transmissão e recepção de uma mensagem ou qualquer outro evento (Kurose & Ross, 2015).

A arquitectura TCP-IP, possui quatro camadas com funções bem definidas: aplicação, transporte, Internet e a camada de acesso. Cada uma dessas camadas oferece uma gama de protocolos.

Camada de Aplicação – É nesta camada onde é feita a comunicação entre os aplicativos e o protocolo de transporte. Nela podemos encontram vários protocolos, sendo os mais conhecidos o HTTP, HTTPS, SSH, SMTP, FTP, SNMP, SIP e DNS (Redes, 2020). A camada de aplicação comunica-se com a camada de transporte através de uma porta. As portas são numeradas e as aplicações padrão utilizam sempre uma mesma porta.

Camada de Transporte – Esta é a terceira camada do Modelo TCP/IP, é responsável pela comunicação lógica dos diferentes dispositivos de uma rede. Nesta camada é feita a captação dos dados enviados pela camada de aplicação, e posteriormente esses mesmos dados são transformados em pacotes, e repassados para a camada de Internet (Fazenda, 2016).

Camada de Internet – Realiza transferência e roteamento de pacotes entre dispositivos da inter-rede. Há vários protocolos que podem operar nesta camada: IP, ICMP, ARP e RARP (Junior, 2017).

Camada de acesso a rede – Segundo Macedo, et al (2018), a camada de acesso a rede não é uma camada propriamente dita, mas uma interface entre os hosts e os enlaces de transmissão. Nesta camada faz-se o endereçamento físico entre os dispositivos através do MAC, o controlo de fluxo e a detenção e correcção de erros.

Internet Protocol (IP) – é o principal protocolo de comunicação utilizado para transmissão de dados chamados datagramas (pacotes) através de uma rede interna utilizando o Internet Protocol Suite. É responsável pelo roteamento de pacotes através dos limites da rede onde é o principal protocolo para estabelecer a Internet. Segundo Tanenbaum (2021), a principal característica desse protocolo é que a transmissão é efectuada sem a necessidade de uma conexão entre máquina fonte máquina destino, sendo baseada no envio de datagrama que podem passar por muitas redes intermediárias até chegarem ao destino. Um datagrama IP consiste de um cabeçalho e uma área de dados.

TCP – É um dos principais protocolos da Internet Protocol Suite e um dos dois componentes originais do conjunto, complementando o IP, portanto, todo o conjunto é comumente referindo como TCP/IP.

UDP – É um protocolo simples da camada de transporte, ele permite que a aplicação escreva um datagrama encapsulado num pacote IPv4 ou IPv6, e enviar ao destino. Mas não há qualquer tipo de garantia que o pacote irá chegar ou não.

SNMP – Existente na arquitectura TCP/IP é o grande responsável pelo gestão de uma rede, operando na camada de aplicação. O SNMP define e administra a forma de execução dos intercâmbios de informações de gestão.

DNS – Esse protocolo é um recurso utilizado em redes TCP-IP, responsável por localizar e traduzir para números IP os endereços dos sites que digitamos nos navegadores. Como exemplo www.google.com (Costa, 2022).

HTTP - É o protocolo mais utilizado para aceder aos conteúdos das páginas web. Por exemplo ao aceder a uma página web na internet o explorador web envia um pedido HTTP relativo a uma determinada página.

DHCP – Este protocolo tem a função de gerar e administrar endereços IP em uma rede de computadores. Ao actuar junto a um servidor DHCP devidamente configurado, o mesmo permite distribuir endereços IP, máscaras de sub-redes, gateway padrões, entre outras configurações, para os diferentes dispositivos que podem compor uma rede de computadores (Macedo, et al, 2018).

FTP – É um protocolo cliente-servidor responsável pela transmissão e transferência rápida de arquivos (também conhecidos como ficheiros), sendo assim um dos protocolos mais utilizadas na Internet.

SSL – A principal tarefa do SSL é manipular a compactação e a criptografia. Quando o HTTP é usado sobre SSL, ele se denomina HTTPS (Secure HTTP), embora seja o protocolo HTTP padrão, ele está disponível em uma nova porta (443) (Tanenbaum & Feamster, 2021).

SSH – É um protocolo de rede criptográfico para operação de serviços de rede que permite a comunicação e compartilhamento de dados de dispositivos na mesma ou em diferentes redes. Um exemplo de aplicação conhecido é para login remoto de utilizadores a sistemas de computadores.

1.1.2. Serviços de rede

Segundo Informatique-Mania (2022), os serviços de rede podem ser entendidos como um conjunto de equipamentos e softwares conectados uns aos outros por meio de dispositivos físicos ou sem fio. Geralmente, esses serviços são ferramentas carregados em segundo plano, e fornecem funcionalidades para rede interna e externa. Alguns desses serviços bem conhecidos que foram utilizados no projecto são os seguintes: Web cache e Proxy.

Web cache – Este serviço encontra-se entre um servidor web, e um ou mais clientes HTTP. Este serviço tem a responsabilidade analisar (e na maioria das vezes, fazer uma cópia) das requisições HTTP (páginas HTML, imagens e outros arquivos) (Novo, 2015). Na presente pesquisa foi configurado esse serviço no intuito de deixar a rede mais optimizada no acesso a determinados sites a um tempo útil.

Proxy Systems – Os servidores de serviço proxy são particularizados em aproveitamentos ou programas servidores que se executa um firewall. Os mesmos pegam a solicitação e exigência dos utilizadores para o serviço da internet, examina-se as solicitações serão acatadas dentro do anexo de regras preestabelecidas e logo passam ou não a solicitação adiante para o serviço característico solicitado. Neste projecto foi utilizado este serviço como mediador entre o utilizador da rede interna e a internet. Geralmente esse servidor é utilizado de modo transparente para o utilizador, evitando assim alguma intervenção de configuração nas máquinas dos utilizadores, sendo subtil, porém actuando assim como filtro de pacotes (Severino & Araújo, 2016).

1.1.3. Virtual Local Area Network

As VLANs, são redes locais virtuais que possibilitam uma maior flexibilidade nas estruturas de empresas, onde uma rede física não precisar ser alterada para atender mudanças organizacionais, somente a sua configuração virtual (Tanenbaum & Feamster, 2021).

De acordo com Kurose e Ross (2015), as VLANs apareceram com o objectivo de resolver algumas dificuldades:

- **Carência de isolamento do tráfego –** Com a utilização de VLANs, torna-se admissível limitar o tráfego de broadcast (por exemplo, gráficos carregando mensagens DHCP) na rede, desta forma, além de aprimorar o desempenho da LAN, aperfeiçoaria questões de privacidade e segurança. Por exemplo, em uma universidade, estudantes poderiam utilizar um software analisador de pacotes para capturar informações trafegadas nos departamentos administrativos da instituição.

- **Utilização ineficiente de switches –** Por exemplo, para dividir em três grupos uma LAN com 30 computadores, conectados a um switch sem suporte a VLANs, seriam necessários três switches.
- **Gestão de utilizadores –** Por exemplo, em uma LAN, dividida em grupos que utilizando switches sem suporte a VLANs, caso um funcionário mude de grupo, seria necessário alterar o cabo de rede de switch. Problema que não existiria em switches com VLANs, pois seria necessário somente alterar as configurações nos softwares de gestão das VLANs.

As principais implementações de VLAN são: VLAN baseada em porta, a qual opera em switches da camada dois (2) do modelo OSI, VLAN baseada em IP, utilizando a camada três (3) do modelo OSI, e VLAN baseada em MAC que permite que os pacotes não marcados de entrada sejam atribuídos à LAN virtual (Williams, 2023).

Assim, Anlix (2021) e Williams (2023) destacam as seguintes as vantagens da utilização das VLANs na segurança e desempenho da rede:

- Redução do tráfego;
- Redução de custos de configuração;
- Redução o número de dispositivos para determinada topologia de rede;
- Maior segurança e facilidade de administração e isolamento de utilizadores;
- Pode simplificar e facilitar a gestão de dispositivos;
- VLAN remove o limite físico.

1.1.4. Qualidade de Serviço

De acordo com as definições da Cisco (2009), QoS refere a capacidade de uma rede para proporcionar o melhor serviço ao tráfego de rede seleccionado sobre as várias tecnologias subjacentes. QoS é um conjunto de mecanismos ou tecnologias que permitem que aplicativos requisitem e recebam níveis de tarefas previsíveis em termos de capacidade de throughput de dados (largura de banda), variações de latência jitter e retardo.

Os recursos QoS fornecem um serviço de rede melhor e mais previsível através dos seguintes métodos: Ajuste de largura de banda dedicada; gestão das

características de perda de pacotes; gestão da capacidade da rede para evitar congestionamento; definição e modelação de prioridades de tráfego na rede.

1.2. Aspectos gerais sobre segurança de Redes de Computadores.

Nos dias actuais a informação é um activo de elevado valor para as empresas e demais organizações. Ela requer cuidados especiais, e deve estar protegido obrigatoriamente de acessos não autorizados.

Segundo a APD (2022), a segurança da informação é um conjunto de acções e mecanismos que visam alcançar a preservação da Confidencialidade, Integridade e Disponibilidade da Informação (CID).

A segurança de redes é baseada em métodos e processos que permitem proteger um dado e que a mesma seja acessível somente para quem de facto deve ter acesso. Stallings (2019) menciona que, a definição de segurança de redes está voltada para “três objectivos principais que são o coração da segurança de computadores”. Estes objectivos são normalmente chamados de tríade CIA (do acrónimo em inglês para confidentiality, integrity e availability). Estes conceitos são validos para a segurança tanto para os dados quanto para serviços de computação realizados. Ainda podem ser citados a autenticidade e o não repúdio da informação.

1.2.1. Pilares fundamentais de segurança

Segundo a ISO/IEC 27000 (2018) e Stallings (2019), segurança da redes de computadores bem como a segurança da informação compreende a três pilares fundamentais: a preservação da confidencialidade, integridade e disponibilidade da informação.

- Confidencialidade – Este pilar consiste em salvaguardar os limites autorizados sobre acesso e divulgação das informações, bem como os mecanismos para proteger a privacidade das entidades e das informações privadas." Uma perda de confidencialidade seria a divulgação não autorizada de informação.
- Integridade – Este princípio, tem haver com a prevenção dos dados contra a sua alteração, manipulação ou destruição inapropriada, incluindo a irretratabilidade e autenticidade da mesma. Uma perda de integridade seria a modificação ou destruição não autorizada de informação.

- Disponibilidade – Assegurar acesso e uso rápido e confiável da informação. Uma perda de disponibilidade é a perda de acesso ou de uso da informação ou sistema de informação.

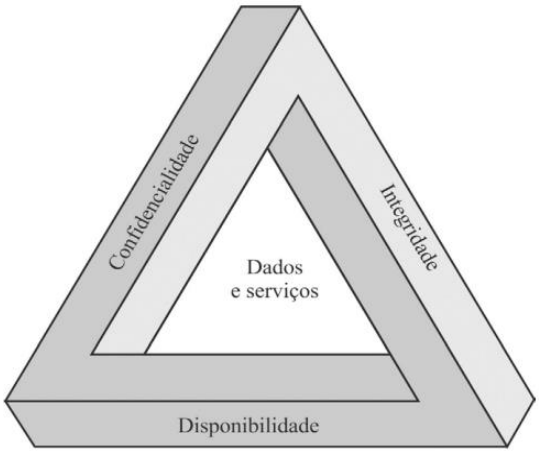


Figura 1 – Tríade de requisitos de segurança
Fonte: Stallings (2019).

Embora o emprego da tríade CIA para definir os objectivos da segurança esteja bem estabelecido, Stallings (2019) percebe que conceitos adicionais são necessários para apresentar um quadro completo. Abaixo são mencionados esses conceitos:

- Autenticidade: Este princípio é projectado para estabelecer a validade de uma transmissão de uma mensagem ou a origem de uma mensagem, verificando se a propriedade é genuína e confiável. Isso significa verificar que os utilizadores são quem dizem ser e, além disso, que cada entrada no sistema vem de uma fonte confiável.
- Responsabilização/Legalidade: é o aspecto que garante que nenhuma informação pode ser resultado de qualquer acção em desconformidade com a lei. Com o avanço da tecnologia pode-se perceber que não existem sistemas totalmente seguros, assim, surge a ideia de responsabilizar indivíduos ou organizações que violam a segurança de um determinado sistema. De maneira averiguar as infracções de segurança, é necessário o sistema manterem registros de suas actividades para posteriormente permitir a analise forense.

1.2.2. Vulnerabilidades, ameaças e ataques

Com o passar do tempo e aumento da necessidade de se utilizar a Internet dentro das organizações, começaram a ocorrer outras preocupações. A utilização da Internet trouxe novas vulnerabilidades na rede interna. Para além das preocupações existentes com espionagem comercial, fraudes, erros e acidentes, as organizações também necessitam também se preocupar com os hackers, invasões, vírus e outras ameaças que penetram através desta nova porta de acesso (Martins, Silveira, & Santos, 2017).

Vulnerabilidade – Conforme a definição da ISO/IEC 27000 (2018), vulnerabilidade é uma fraqueza de um activo ou de controle que pode ser explorada por uma ou mais ameaças. Em um ambiente de rede existem diversas dessas fraquezas umas que já foram identificadas e corrigidas, outras que foram somente identificadas e possivelmente outra quantidade igual ou superior que ainda nem foi descoberta.

Ameaças – Segundo Pedra (2022), ameaças são factores ou acções capazes de interferir e causar danos à integridade, à confidencialidade, à autenticidade e à disponibilidades de dados e informações sobre a Organização. Ela pode ser vista como um risco, esse risco pode ser uma pessoa, um dispositivo defeituoso, ou um evento que venha a explorar a vulnerabilidade do sistema.

Conforme a norma ISO 27005 (2022) existem diversas formas de ameaças à questão da segurança nas empresas e organizações, tanto por causas de origem ambiental (natural) como por falhas humanas intencionais ou acidentais, como por exemplo, falhas de energia, sabotagem, vandalismo, roubo e incêndio, entre outras.

Ataques – Ataque é um acto inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de fugir dos serviços de segurança e violar a política de segurança de um sistema. A política de Segurança pode ser entendida como um conjunto de boas práticas que devem ser seguidos por todos os membros internos e externos que tem acesso aos dados da rede, das informações da instituição e não só (Stallings, Criptografia e Segurança de Redes: Princípios e Práticas, 2019). Essa prática tem o objectivo de padronizar e aumentar a segurança das informações de uma empresa e evitar possíveis problemas na corrupção dos dados trafegados na rede.

Stallings (2019) considera os ataques em activos e passivos: Os ataques passivos procuram descobrir ou utilizar informações do sistema, mas não afectam, nem interferem no funcionamento dos recursos do sistema a ser atacado. Por sua vez, um ataque activo tenta alterar recursos do sistema ou afectar sua operação.

Tabela 1 - Alguns tipos de Ataques e suas camadas de actuação

Camada TCP-IP	Categoria do Ataque	Componentes de Segurança
Aplicação	Exploração	Confidencialidade/Autenticidade
Rede	Usuário para super usuário	Confidencialidade/Autenticidade
Transporte	Negação de serviço	Disponibilidade
Host Rede	Remoto para usuário	Confidencialidade/Autenticidade

Fonte: Adaptado de (Tchimissi, 2018).

1.2.3. Métodos e técnicas de ataques

Existem vários tipos de ataques que diferem pela forma como são feitos e pelo objectivo. Os mesmos podem utilizar o método manual, onde o alvo é escolhido cuidadosamente e o objectivo é bem definido antes de ser escolhida a técnica de ataque, ou automáticos, esses tipos de ataque não necessitam de intervenção humana para serem efectivados, podendo ser activados através de scripts ou software específico. Dentre estes ataques podemos destacar:

1) **BackDoor** – A função de um backdoor é permitir algum tipo de acesso ilegal ao sistema alvo. Os backDoor são projectados de modo a não só manter o acesso do atacante ao sistema invadido, mas como também para criar um novo canal de acesso (isso acontece principalmente com a ajuda de utilizadores internos).
2) **Password Guessing Attack** – Este tipo de ataques ocorre quando um utilizador não autorizado, tenta repetidamente aceder a um computador ou rede tentando adivinhar nomes de utilizadores e palavra-chave.
3) **DoS** – São tipos de ataques que pretendem esgotar os recursos da máquina ou torná-la inacessível a um determinado utilizador ou máquina. Esse tipo de ataque é muito utilizado para atacar servidores de hospedagem de sites na Internet.
4) **DDoS** – É um tipo de ataque de negação. actualmente ele vem se difundido entre a comunidade hacker e se tornando um dos tipos de ataque de negação

mais utilizados, principalmente por possuir uma arquitectura de ataque que dificulta e muita das vezes impossibilita a identificação da origem do ataque.

5) **Spoofing** – Um ataque de spoofing é quando uma pessoa personaliza um dispositivo ou uma rede com finalidade de atacar uma rede, roubar dados, distribuir vírus para ter controle de acesso aos hosts, assim podendo realizar os diferentes tipos de ataque de spoofing, IP, DNS e ARP (Dupaul, 2016).
6) **Wardriving** – O objectivo do Wardriving é de mapear as redes sem fios sem segurança para utilização ou também para identificar as redes sem fios e realizar ataques para obter informações de pessoas ou de uma empresa.
7) **Engenharia Socia**l – Este tipo de ataque refere-se à manipulação psicológica de pessoas para a execução de acções ou divulgar informações confidenciais. Na engenharia social geralmente são exploradas algumas vulnerabilidades emocionais das vítimas, tais como a curiosidade, preguiça, solidariedade, vaidade e a ansiedade (Wikipédia, 2023).
8) **Malwares –** Malware nada mais é que uma denominação para as inúmeras classificações de vírus. Alguns malwares mais conhecidos são: Vírus de computador, trojan ou cavalo de tróia e ransomware.

1.3. Mecanismos de segurança em redes locais

Apesar de todos os benefícios proporcionados pelas redes de computadores, ao interligar máquinas em rede, estas ficam mais vulneráveis a ataques, necessitando de cuidados específicos no que diz respeito a “protecção da informação” que ali trafega, no intuito de evitar que estes dados possam ser alterados, destruídos ou roubados. Existem algumas maneiras utilizadas por administradores de redes para proteger sites e redes, como: VPN - permite estabelecer uma conexão de rede protegida ao utilizar redes públicas; NAT - Sob o ponto de vista da segurança o NAT pode esconder os endereços dos equipamentos da rede interna e, consequentemente, sua topologia de rede, dificultando os eventuais ataques externos (Nakamura & Geus, 2007); Contas e Senhas - Em sistemas computacionais, as senhas são muito utilizadas para permitir a autenticação de utilizadores e conceder-lhes privilégios especiais ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema; Criptografia - A criptografia é um mecanismo de segurança mais eficaz actualmente, podendo ser entendido

como a modificação de uma informação em outra, deixando-a ilegível para pessoas não autorizadas, para obter essas transformações na mensagem, faz-se a utilização de algoritmos predefinidos e uma chave secreta, que codifica a mensagem em outra e depois é decodificada quando chega ao seu destino com a chave secreta, dessa maneira, procurar-se-á garantir a privacidade e a integridade, impossibilitando que terceiros possam ler a mensagem original ou mesmo alterá-la. A criptografia pode ser simétrica e assimétrica: - Criptografia Simétrica (chave secreta) e Criptografia Assimétrica (chave pública); Assinatura digital - Este processo garante que a mensagem realmente veio do remetente, confirmando sua autenticidade, este método utiliza técnicas de criptografia, dessa maneira, garante também a integridade e o não repúdio, que tem como característica provar quem foi o emissor da mensagem. Basicamente, seu mecanismo gera um resumo criptografado da mensagem utilizando algoritmos complexos, minimizando a mensagem em tamanhos menores, que é denominado hashing ou checagem; Certificado digital - Para obtenção de uma assinatura digital, é necessária uma Autoridade Certificadora (AC) que faça esse serviço, tendo como função averiguar a identidade de um utilizador e agregar a ele uma chave. O certificado digital tem por função atestar a integridade dos negócios, garantindo a legitimidade da operação realizada na Internet, funciona como se fosse um documento usado na Internet para assegurar sua identidade; Autenticação - A autenticação é o acto de verificar se as informações fornecidas são provenientes de uma fonte confiável, ou seja, se o solicitante estiver com o certificado correcto e o mesmo não foi realizado alterações ele é autenticado na rede, software ou página web (Bezerra, 2012); Autorização – É uma espécie de permissão, onde o utilizador só poderá aceder aquele recurso ou informação a qual eu concedi a permissão, sendo permissão de somente leitura, ou escrita e/ou as duas permissões (Conceito, 2013). A autorização de acesso à rede é concedida ou negada com base nas políticas implicadas no ambiente de trabalho ou residencial (Microsoft, 2022); Backups - É uma cópia de todos os dados importantes de uma determinada máquina cliente ou servidor que são armazenados em diferentes dispositivos de armazenamento para que possam ser recuperados em caso de alguma fala na máquina cliente ou servidor. É aconselhável realizar o backup dos dados com determinada frequência tendo em conta as políticas de segurança da Organização. As backups podem ser

feitas em diferentes formas locais, como, um disco rígido externo, um pendrive, CD ou DVD, nuvem, entre outras (Significados, 2011) e (Computer-Hope, 2023); Ferramentas Anti-malwares - são softwares que permitem detectar, proteger os dispositivos contra e remover softwares maliciosos. Alguns exemplos de anti-malwares são os seguintes: Avast, Kaspersky, Norton Antivírus e o IObit Malware Fighter.

1.3.1. Firewall

Para controlar o tráfego de uma rede, ferramentas como Firewall são as aplicações mais utilizadas. Firewall é um conjunto de hardware e software que tem por objectivo manter uma rede interna protegida da Internet (rede externa).

De acordo com Stallings (2019), o firewall serve como uma maneira segura de ligar a rede interna de uma organização com a Internet. O firewall é um sistema que pode ser implementado na rede em forma de hardware específico ou softwares.

Stallings (2019), cita quatro técnicas gerais utilizada pelos firewall para controle de acesso e política de segurança de uma rede: - Controle de serviço: Define os serviços que podem entrar e sair da rede interna para a Internet; - Controle de direcção: Define em qual direcção as solicitações de serviço podem iniciar e passar pelo firewall; - Controle de utilizador: Define o controle de acesso a serviços conforme os utilizadores que o estão acedendo; - Controle de comportamento: Define como determinados serviços são utilizados dentro da rede. Ele possui três princípios básicos: todo tráfego, tanto de dentro para fora quanto de fora para dentro, da rede deve passar por ele; o tráfego autorizado é o único que poderá passar por ele sem ser bloqueado; o Firewall deve ser impenetrável (Kurose & Ross, 2015).

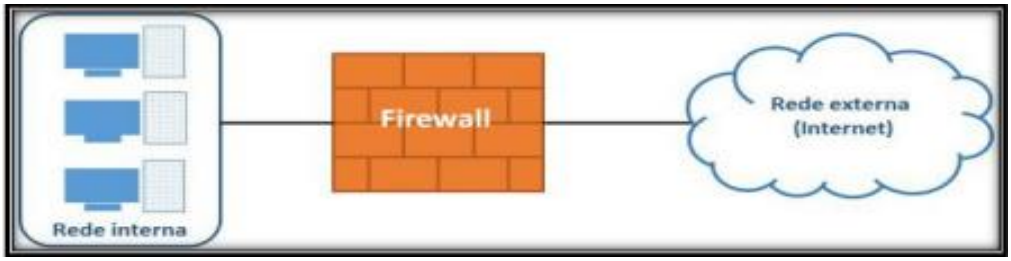


Figura 2 – Estrutura de Firewall.

Fonte: Adaptado de Alecrim (2013)

Para Gray (2016), uma das vantagens de uma firewall é que ele protege contra-ataques e invasões provenientes de redes não conhecidas ou não confiáveis. Uma das principais desvantagens de uma firewall é que ele não é capaz de proteger contra-ataques provenientes da própria rede interna (Maste, 2010).

1.3.1.1. Tipos de firewall

De acordo com Algar-Telecom (2018), actualmente temos três tipos de firewall: filtro de pacotes, filtro de pacotes com base no estado da conexão e filtros de pacotes na camada de aplicação.

Os filtros de pacotes funcionam permitindo ou eliminando pacotes com base em seus endereços de origem ou destino, ou nos números de porta. As decisões são tomadas com base no conteúdo do pacote que o Firewall está recebendo ou enviando. Por exemplo, todos os computadores de uma rede local podem aceder páginas na Internet (origem): rede LAN, (destino): Internet, aceita: protocolo HTTP porta 80, onde os roteadores são exemplos de Firewall de filtro de pacotes.

O Firewall com filtro de pacotes com base no estado da conexão (stateful packet Filter) baseia suas acções utilizando dois elementos: dados contidos no cabeçalho do pacote e na tabela de estados, que armazena informações do estado de todas as conexões que estão trafegando através do Firewall e usa estas informações, em conjunto com as regras definidas pelo administrador, na hora de tomar a decisão de permitir ou não a passagem de um determinado pacote. Como exemplo podemos citar o protocolo FTP (Kashefi, Kassiri, & Shahidinejad, 2013).

O Firewall com filtro de pacotes com base no estado da conexão consegue analisar todo o tráfego da conexão FTP, identificando qual o tipo de transferência que será utilizada (activa ou passiva) e quais as portas que serão utilizadas para estabelecer a conexão. Sendo assim, todas as vezes que o Firewall identifica que uma transferência de arquivos estará sendo realizada, é acrescentado uma entrada na tabela de estados, permitindo que a conexão seja estabelecida. As informações ficam armazenadas na tabela somente enquanto a transferência do arquivo é realizada.

Os Firewall com filtros na camada de aplicação são mais complexos, pois utilizam um código especial para filtrar a aplicação desejada. Por exemplo, os Firewall com filtros na camada de aplicação podem identificar vírus anexos às mensagens (e-mails) que estão chegando ou saindo do seu ambiente computacional. Outro recurso disponível neste tipo de Firewall são os registros de todo o conteúdo do tráfego enviado ou recebido (Kashefi, Kassiri, & Shahidinejad, 2013).

1.3.1.2. Arquitectura de firewall

Diversas arquitecturas podem ser empregadas para a implantação de Firewall em uma rede. A opção por uma delas obedece a uma série de factores, incluindo a estrutura lógica da rede a ser protegida, custo, funcionalidades pretendidas e requisitos tecnológicos dos Firewall.

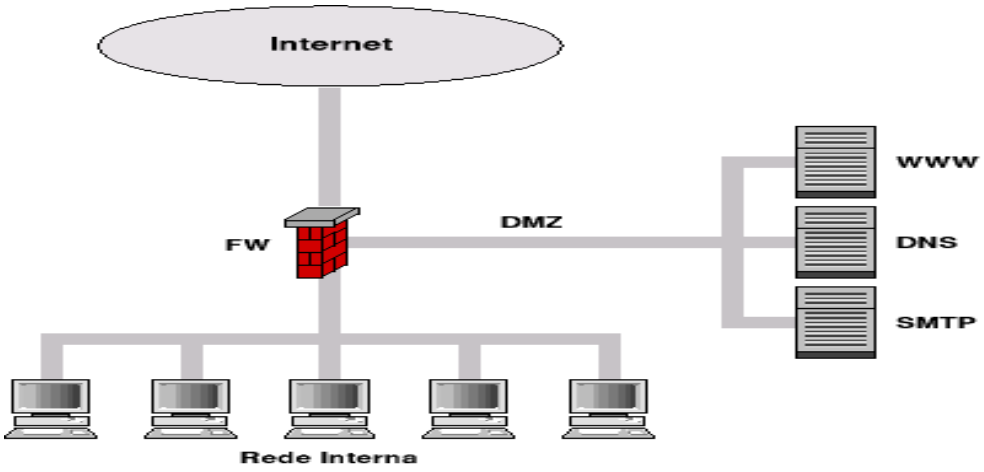


Figura 3 – Exemplo de um Firewall simples.
Fonte: (Cert br, 2003).

O firewall não pode assegurar que a rede está protegida, pois como lida apenas com entrada e saída de dados, ele não pode proteger a rede de outros ataques provindos da rede interna ou da Internet. Um exemplo que pode ser citado é o ataque de negação de serviços (Tanenbaum & Feamster, 2021). Para a protecção da rede contra outros tipos de ataques é necessária a implantação de sistemas de detecção e prevenção de intrusos e analise de comportamento da rede.

1.3.2. Servidores de autenticação

Em ambientes corporativos a utilização de servidores se tornou um investimento frequente e necessário nas últimas décadas. Segundo Servidor de Autenticação (Authentication Server – AS) - Um servidor de autenticação permite autenticar utilizadores (e também máquinas). É responsável por receber um pedido de autenticação de um utilizador e verificar se a identidade deste utilizador é autêntica. Numa rede de dados é muito usual existirem servidores de autenticação de forma a que os utilizadores apenas tenham acesso aos recursos mediante a introdução de credenciais (utilizador + password). O servidor RADIUS e o LDAP, são exemplos claros desses tipos de servidores:

RADIUS - É um protocolo para confirmação, habitualmente utilizado em provedores de internet juntamente a redes sem fio. É um protocolo tratado na [RFC2865], definido nela como sendo desenvolvido para a realização de autenticação, autorização e encaminhamento de informações de configuração entre uma rede de acesso compartilhado, que deseja autenticar as suas ligações, e um servidor de autenticação (Silva, 2010). LDAP - É um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para aceder e manter serviços de informação de directório distribuído sobre uma rede de Protocolo da Internet (IP). Podem fornecer qualquer conjunto de registros organizado, geralmente com uma estrutura hierárquica, como um directório de e-mail corporativo. Uma utilização comum do LDAP é fornecer um "logon único" onde uma senha para um utilizador é compartilhada entre muitos serviços, como a aplicação de um código de login da companhia para páginas web (de forma que a equipe loga apenas uma vez aos computadores da companhia e então são automaticamente logadas na intranet da companhia).

1.3.3. Sistemas de detecção e prevenção de intrusão

Para se evitar ataques que não são bloqueados pelas regras de firewall, é necessário manter aplicações de segurança e de gestão para monitorar a saúde da rede e prevenir possíveis danos causados por esses ataques. Assim faz-se necessário manter as redes seguras através dos Sistemas Detectores e de Prevenção de intrusão. Intrusão é um conjunto de acções que buscam

comprometer a integridade, confidencialidade ou disponibilidade de um recurso computacional. Já o acto de detectar acções que podem comprometer a integridade, confidencialidade ou disponibilidade de um recurso computacional pode ser denominado detecção de intrusão.

De acordo com Fares (2021) o IDS é uma solução que pode identificar uma invasão da rede com intenções maliciosas ou pode apenas detectar um utilizador não autorizado conectado à rede de dados. Esse sistema é capaz de identificar e analisar os dados que trafegarem pela rede mediante a observação de pacotes que possuem padrões predefinidos e podem actuar em tratativas para soluções de possıveis invasões na rede.

O Sistema de Prevenção de Intrusão (IPS) actua na prevenção de invasões nas redes de comunicação. Trata-se de uma ferramenta que possibilita tomar decisões de intervenções na rede, podendo realizar bloqueios de tráfego malicioso. Esta ferramenta se baseia em conteúdo de aplicações e não apenas nos endereços IPs ou em portas, como é feito pelo firewall (Fares, 2021).

Os IDS estão constituídos tipicamente por: Sensores que geram eventos e alarmes de segurança, Consola que controla os sensores, monitorando os eventos e alertas e motor que utiliza as regras de segurança para gerar os alertas a partir dos eventos de segurança.

Principais características de um IDS

Para a escolha de um sistema de IDS adequado temos de ter em conta algumas Características importantes que o sistema deve ter: Simplicidade de configuração, simplicidade de administração, independência de operação, tolerância a falhas, segurança. baixo impacto no funcionamento do sistema/infra-estrutura, analisar padrões e não detectável resistente a erros de monitorização.

Classificação dos IDS

Conforme Nassaro (2012), os Sistemas de Detecção de Intrusão podem ser divididos em três (3) categorias:

a) **IDS baseado em Host (HIDS)** – A análise é feita apenas com base em um computador específico da rede normalmente o servidor principal e o levantamento das informações é feito por um software específico ou através de dados de eventos do sistema. Os HIDS chegam a ser mais eficientes em detectar ataques de origem interna e menos eficientes para detectar ameaças de origem externa.
b) **IDS baseado em Rede (NIDS)** – A análise é feita em toda a rede e de maneira mais detalhada. As informações são monitoradas por vários sensores espalhados pela rede e sistemas que monitoram a fundo pilhas de protocolos e cabeçalhos de pacotes que trafegam na rede. Eles são geralmente posicionados em locais estratégicos da infra-estrutura da rede;
c) **IDS híbridos –** É utilizado para a junção de sistemas baseados em Host e sistemas baseados em Redes. Essa união dos dois tipos de sistemas de detecção aumenta o controle e segurança da rede.

Segundo Patel et al (2010), os IDS/IPS são inseridos como a última linha de defesa dentro de uma arquitectura computacional, o que os torna de grande importância, possibilitando inferir sobre a legitimidade de acções realizadas e possuindo comportamento pró-activo em situações de ataque.

1.3.3.1. Ferramentas IDS/IPS

Com a impossibilidade de testar todas as ferramentas disponíveis, a escolha feita teve como base as ferramentas de IDS/IPS mais comuns disponíveis online e que reuniam um conjunto de características que necessitamos, como o facto de ser uma ferramenta open-source e a necessidade de as ferramentas reunirem características diferentes de forma a poderem ser testadas as várias vertentes na detecção de intrusões. Dentre os pogramas de IDS, desctacam-se, ainda: O Snort, O Suricata, Ossec, AntiSniff, TripWire, Vallhala

O Snort é um sistema de detecção e prevenção de invasões de rede, agindo como um filtro, ele é capaz de realizar analises nos pacotes que estão trafegando em redes IP em tempo real. Neste projecto em particular utilizou-se o Snort para poder detectar e prevenir as possíveis intrusões. Pois, este sistema permite realizar analises em protocolos de redes, busca de conteúdo automático para actualização

de regras, além de ser utilizado para detectar uma variedade de ataques (Snort, 2022).

1.4. Sistemas de gestão de redes

Ipcop - É um software livre, licenciado sob a Licença BSD, baseado no sistema operacional FreeBSD, personalizado para trabalhar como Firewall. Porém, suas funcionalidades vão muito além das de um simples Firewall, podendo exercer o papel de roteador, trabalhar com VPN's, Sistemas de Detecção de intrusão, e muito mais.

ENDIAN FIREWALL – Fundada em Appiano, Itália, no ano de 2003, por uma equipe de especialistas em redes e entusiastas do Linux, o objectivo da empresa Endian logo ficou explícito: desenvolver um sistema de gestão unificado de ameaças de código aberto mais potente e com uso facilitado que o mercado já ofereceu (Endian, 2022).

Mikrotik RouterOS – É um sistema operacional desenvolvido e mantido pela Mikrotik, uma empresa fundada em 1995, sediada em Riga, capital da Letónia. O Mikrotik RouterOS é um sistema dedicado a realizar gestão e controle de redes de computadores. Para isso, dispõe de diversos recursos, como por exemplo, roteamento de redes de computadores, controle e filtro de tráfego e conteúdo e sistema de protecção para estas redes (Mikrotik, 2015).

PfSense – O pfSense é uma ferramenta que faz a conexão de vários instrumentos que fazem parte de uma área da rede e sua segurança. É um Sistema Operacional fundamentado no FreeBSD, que deriva do UNIX. O pfSense é uma compilação que traz vários serviços consigo. Como por exemplo, o firewall, proxy, domínio de acessos de utilizadores entre outras funcionalidades. O uso dele promove a gestão e a segurança de rede, tanto pelo fio quanto como a rede wireless.

1.5. Tecnologias utilizadas no projecto

PfSense é uma distribuição linux, licenciada sob BSD licence, que tem por base o sistema operacional FreeBSD, tendo sido adaptado para assumir o papel de uma firewall e/ou roteador de rede, totalmente gerenciado por uma interface web fácil de usar (Netgate, 2022).

A utilização de uma máquina com sistema operacional pfSense visa manter o foco na segurança e administração da rede, actuando activamente como um firewall e roteador. Além disso, a ferramenta é flexível, pois inclui uma longa lista de recursos relacionados e um sistema de pacotes, permitindo a expansão de serviços sem acrescentar novas vulnerabilidades para o sistema. Outra facilidade do pfSense é o backup das configurações, o que torna a administração muito mais fácil e segura, isso quando o backup das configurações é feito regularmente.

De acordo com a configuração e/ou as necessidades, a ferramenta pode assumir o papel de: VLANs, Firewall, LAN ou WAN Router, Ponto de Acesso Wireless, Proxy Server, Serviços específicos, tais como VPN Appliance, sniffer Appliance, Servidor DHCP Appliance, Servidor DNS Appliance, IDS/IPS e muito mais.

Toda administração do pfSense é feita após a instalação via navegador na rede local. Instalou-se, e configurou-se além da solução de NAT que é padrão, os seguintes módulos: VLANs, Squid, SquidGuard – para controle de conteúdo. Lightsquid, Captive Portal e SNORT. Todos esses módulos são instalados directamente do modulo Web de gestão do pfSense que permite a escolha destes e de outros pacotes com a instalação automatizada. Com esse conjunto de módulos, garantimos a mínima segurança necessária para o acesso à internet.

Utilizou-se também o GSuite, PaperCut e Microsotf-Vision, sendo o GSuite para a gestão das contas para autenticação, e o PaperCut para monitorar e controlar a impressão pela rede de maneira segura e o Visio que serviu para a criação dos diagramas presentes no trabalho.

1.6. Metodologias de projectos de redes de computadores

A estruturação de um projecto de redes de computadores requer um método sistemático e iterativo, pois envolve a integração de muitos e sofisticados componentes. Além disso, o levantamento de todos os requisitos comerciais e técnicos são essenciais para o sucesso do projecto. A análise de requisitos ou engenharia de requisitos é um aspecto importante na gestão de projectos, de forma projectar e implementar melhor as estratégias de segurança dentro de uma rede

corporativa. A análise de requisitos é fundamental para o desenvolvimento do sistema, ela determina o sucesso ou o fracasso do projecto (Quiterio, 2006).

Uma metodologia deve ser estruturada no sentido de incluir um projecto lógico antes de constituir um projecto físico e abordar os requisitos dos utilizadores do sistema antes de considerar outras variáveis. Deve ser interactiva, ou seja, novas informações devem entrar progressivamente no projecto, à medida que se conhece melhor os requisitos dos utilizadores, a fim de corrigir desvios e eventuais falhas (Pinheiro, 2008).

Segundo Oppenheimer (2010), dentre os diferentes tipos de metodologias de projectos de rede existentes temos a citar: Metodologia top-down, Metodologia bottom-up e Metodologia middle Out.

A **Metodologia top-down** é um método utilizado no projecto de redes de computadores que inicia o seu desenvolvimento por meio da camada mais alta do modelo de referência OSI (Open Systems Interconnection), enfocando o levantamento das aplicações, os fluxos de dados e os tipos de serviços necessários para o transporte de dados, em detrimento da selecção dos equipamentos (switches, roteadores, firewall, balanceadores de carga, entre outros) e das tecnologias de cabeamento e interconexão que serão utilizadas (Oppenheimer , 2010).

Nesta investigação tendo em conta o facto de já existir uma estrutura de rede instalada durante a fase de construção do edifício optou-se pela metodologia bottom-up que inicia com o projecto físico da rede, permitindo reaproveitar o que já existe (recursos e equipamentos) com o mínimo custo possível.

A abordagem **bottom-up** (de baixo para cima) funciona de maneira oposta à abordagem top-down. Inicialmente, inclui o projecto das partes mais fundamentais que são então combinadas para fazer o módulo de nível superior. Esta integração de submódulos e módulos no módulo de nível superior é repetidamente executada até que o algoritmo completo requerido seja obtido. Segundo Oppenheimer (2010), esta metodologia descreve o projecto de rede nos seguintes passos:

- **Identificação das necessidades** – Nesta primeira fase, são analisados os objectivos comerciais e técnicos do projecto, enumerando suas principais contradições e dificuldades. Outrossim são identificados o ambiente legado e os principais fluxos de dados que serão encaminhados pela rede de computadores;
- **Projecto físico de rede** – Nesta etapa, são efectivamente seleccionados os dispositivos e as tecnologias para as redes locais e as redes geograficamente distribuídas;
- **Projecto lógico de rede** – Define as topologias de rede, a padronização de nomes e a hierarquia de endereços IP que serão empregadas na concepção do modelo lógico. Este passo detalhará as configurações das soluções e funcionalidades adoptadas para a segurança e a gestão adequada da rede;
- **Testes e optimização** – Serão planejados os testes de validação e os critérios de aceitação. Também serão descritas tecnologias para optimização da infra-estrutura.

Capítulo II - Projecto e implementação dos mecanismos de segurança na rede de computadores do ISCED-Huíla

Capítulo II - Projecto e implementação dos mecanismos de segurança na rede de computadores do ISCED-Huíla

2.1. Caracterização da rede existente

O levantamento da situação da rede existente anteriormente foi elaborado através de visitas realizadas aos edifícios que compõem o ISCED-HUÍLA. Os dados obtidos nesta pesquisa foram adquiridos com a ajuda do administrador da rede.

A topologia utilizada pela instituição é a estrela estendida. Este tipo de topologia possui um nó central, onde se encontra actualmente um roteador principal, por ele está ligado o switch de distribuição. Por este switch de distribuição estão ligados mais switches de acesso para os outros edifícios, um servidor de aplicativos e configurados alguns serviços, tudo isto localizados no segundo andar do edifício principal.

Através de informações obtidas junto ao responsável pela administração da rede e com a ajuda do software Microsoft Visio foi traçada o modelo lógico da rede anterior. Nela são mostrados os equipamentos de rede, o servidor, switch de distribuição, bem como os de acesso e os roteadores. Os switchs utilizados são gerenciáveis de camada dois (2), como é caso do switch principal de marca Cisco com vinte e quatro (24) portas FastEthernet e duas GigabitEthernet, de camada dois (2) gerenciáveis, suportando VLAN. O Router Principal utilizado é de marca Cisco, esse roteador oferece variadas funcionalidades, como aceleração de criptografia de hardware incorporada, slots de processador de sinal digital (DSP) com capacidade de voz e vídeo, firewall opcional, prevenção de intrusão e muito mais. A instituição é constituída por três (3) edifícios, que são interligados por fibra óptica multimodo, nos switches de acesso situados no edifício principal.

Detectou-se que a instituição tem dificuldades em restringir acessos a determinados sites durante o horário de trabalho para cada departamento por falta de segmentação da mesma. Os pontos de acesso muitas das vezes são acedidos por qualquer individuo na instituição sem um controlo adequado. Não existe um limitador de download na rede, e isso faz com que alguns utilizadores consomam

mais banda que os outros. As UPS encontram-se com as baterias gastas fazendo com que os servidores desliguem sempre que há uma queda de energia.

Caracterização da Topologia Lógica Existente.

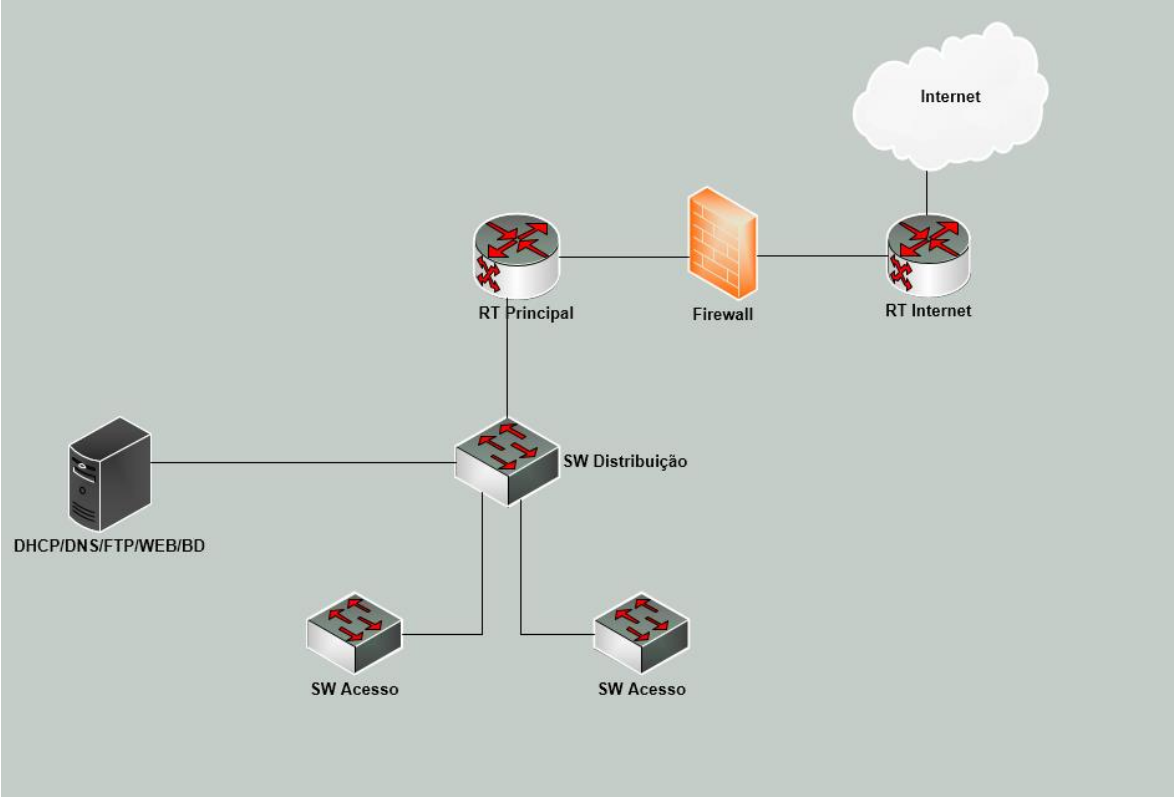


Figura 4 - Demonstração da Rede Existente

A figura acima ilustra o tipo de rede existente anteriormente. Nessa estrutura se contava apenas com um link de internet, existia apenas uma sub-rede para toda a instituição o que tornava bastante difícil para os gestores da rede mo momento de controlar o tráfego e gerenciar os usuários conectados na rede. A mesma infra-estrutura contava com o Ipcop como seu firewall de filtragem de pacotes, porém a mesma apresentava muitos constrangimentos com relação a segurança na rede, dificuldade na gestão de conteúdos, dificuldades na gestão de intrusão, falta de autenticação nos diferentes pontos de acesso, o que fazia com que qualquer utilizador tivesse acesso a rede de maneira deliberada sem muito controlo. Para além disso esse software foi descontinuado em 2018, não havendo assim novas actualizações de segurança.

Depois de uma análise da situação actual da rede do ISCED –Huíla, e mediante as pesquisas feitas no local, constatou-se os seguintes pontos fortes e fracos:

Pontos fortes:

1- Existência de uma rede devidamente estruturada;

2- Existência de tecnologias de rede tais como: computadores, impressoras, armário, switches, roteadores, cabos, tomadas de rede e painel de ligação;

3- Existência de um proxy.

Pontos Fracos:

1- Falta de uma política clara de gestão de segurança informática;

2- Inexistência de um sistema de autenticação de utilizadores nas redes wireless;

3- Falta de equipamentos de vigilância electrónica;

4- Défice de técnicos para a gerência da rede;

5- Falta de segmentação da rede por meio de VLANs na rede;

6- Défice nas regras de firewall para bloqueios de sites indesejados;

7- Falta de detectores de intrusão na rede;

8- Falta de servidor de impressão.

Todos esses pontos fracos supracitados trazem um monte de consequências negativas para instituição. Com a ausência de políticas claras de gestão de segurança informática pode trazer vários aspectos negativos para a instituição, como é o caso do aumento de riscos de violações de segurança, como acesso não autorizado, falta de conscientização e treinamento, protecção inadequada de dados sensíveis, dificuldade na resposta a incidentes, não conformidade com regulamentações e perda de confiança dos clientes. A inexistência de um sistema de autenticação de utilizadores pode levar a acesso não autorizado. Os equipamentos de vigilância electrónica vêm se tornando cada vez mais essenciais para o monitoramento das actividades na rede, e a sua inexistência acarreta um monte de consequências negativas dificuldades no controlo sobre o desempenho da rede. É fundamental ter pessoal qualificado na instituição para garantir a gestão eficaz e segura da rede, pois a falta de técnicos pode levar a uma baixa eficiência operacional e maior tempo de resposta a problemas. A ausência de IDS pode levar a explorações de vulnerabilidades não detectadas, perda de dados, danos à

reputação, interrupção de serviços. Com a falta de segmentação da rede na instituição, torna-se muito difícil para os técnicos gerenciar o tráfego e aplicar políticas de segurança.

2.2. Apresentação e análise de dados

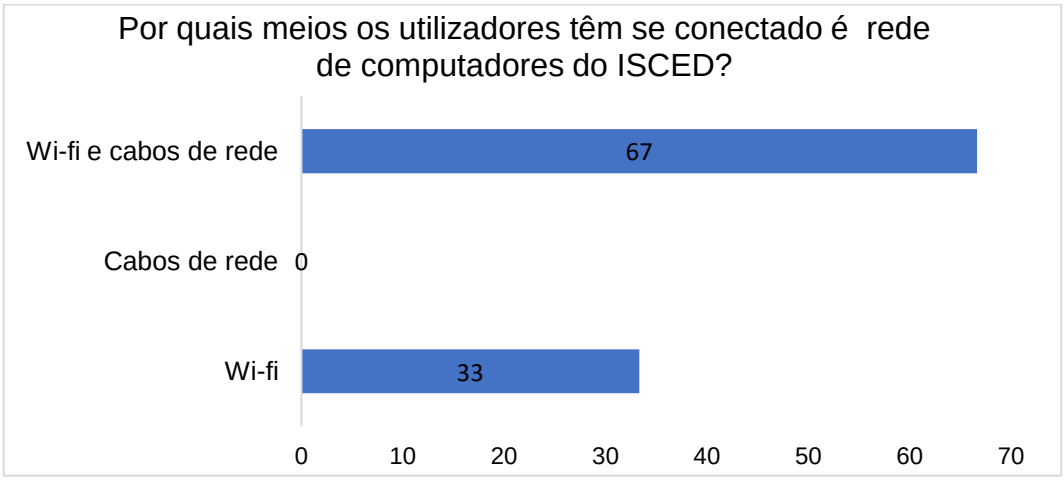
2.2.1. Resultado do diagnóstico

Para a representação dos dados utilizou-se os gráficos de barra, uma vez que os inquiridos poderiam escolher mais de uma opção como resposta. Por conseguinte o gráfico de barra é utilizado em geral para representar dados de uma tabela de frequência referentes a uma variável qualitativa, ou seja, quando estamos perante uma distribuição de dados não uniforme pode-se optar pela utilização do gráfico de barras. Com base no inquérito aplicado, para melhor percepção dos problemas acima citados, cujo os resultados obtidos, passamos apresentar:

2.2.1.1. Resultado dos inquéritos aplicados aos gestores da rede

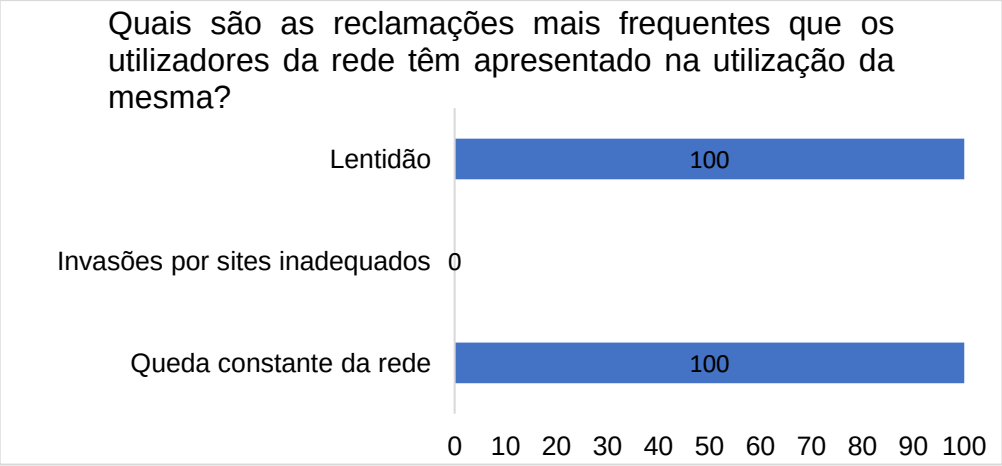
O inquérito feito aos gestores da rede constou seis questões de múltipla escola, com o objectivo de avaliar o desempenho da rede do ISCED-HUILA.

Gráfico 1 - Referente à questão nº 1, feita aos Gestores da Rede



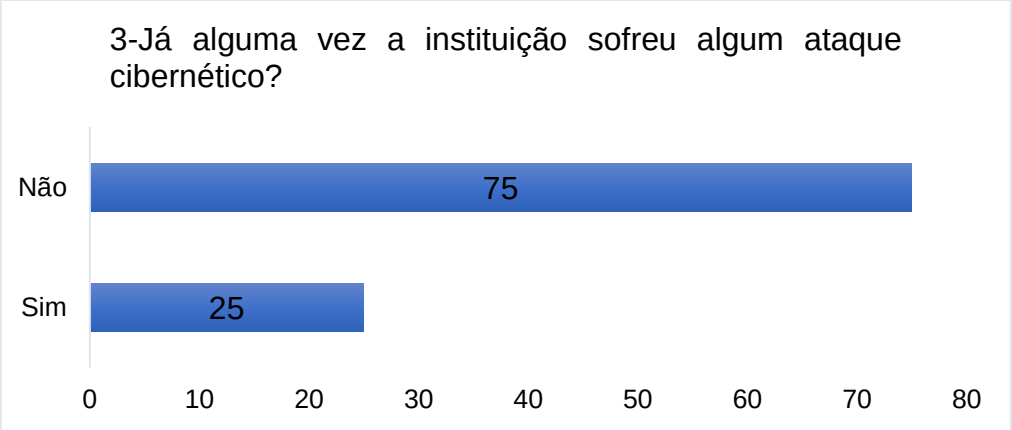
Essa questão colocou-se aos gestores da rede do ISCED, com o objectivo de saber como os utilizadores acedem a rede de computadores. Como se pode observar no gráfico 1, 67% dos inquiridos responderam Wifi e Cabos, e 33% responderam Wi-fi apenas. Geralmente as redes cabeadas oferecem maior qualidade e menos interferência no sinal e mais segurança do tráfego de informações.

Gráfico 2 - Referente à questão nº 2, feita aos Gestores da Rede



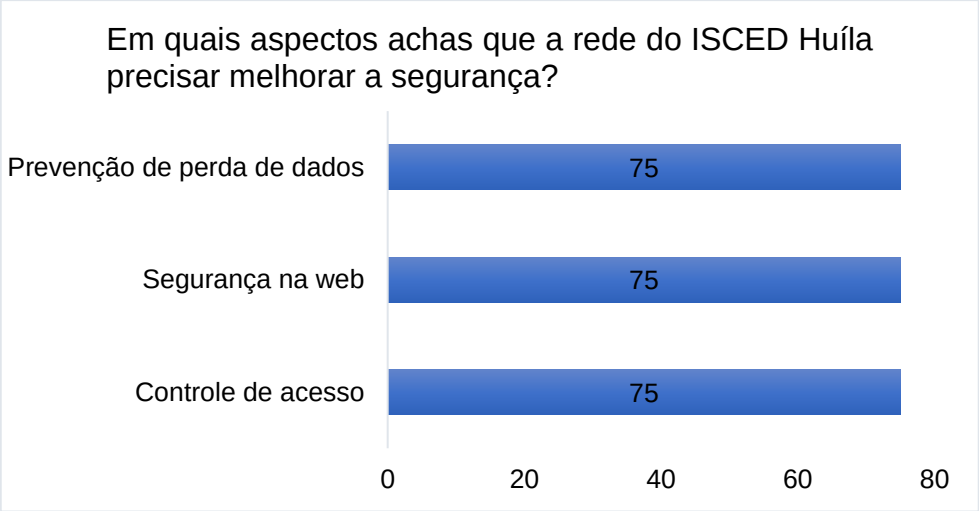
Essa questão foi colocada aos gestores da rede do ISCED, com o intuito de identificar as reclamações constantes que os utilizadores da rede têm apresentado na utilização da rede. Como se pode observar no gráfico 2, 100% dos inquiridos responderam lentidão e queda constante da rede. Geralmente um dos grandes problemas na rede é a latência, isso acontece por vários motivos, como falta de Web Cash na rede, largura de banda má distribuída, e má configuração dos equipamentos.

Gráfico 3 - Referente à questão nº 3, feita aos Gestores da Rede



Essa questão foi colocada aos gestores da rede do ISCED, com o objectivo de saber se a Instituição já alguma vez sofreu algum ataque cibernético. Como se pode observar no gráfico 3, 75% dos inquiridos responderam não e 25% respondeu sim. Se bem-sucedidos, os ataques cibernéticos podem prejudicar as empresas. Eles podem causar tempo de inactividade valioso, perda ou manipulação de dados e perda de dinheiro por meio de resgates.

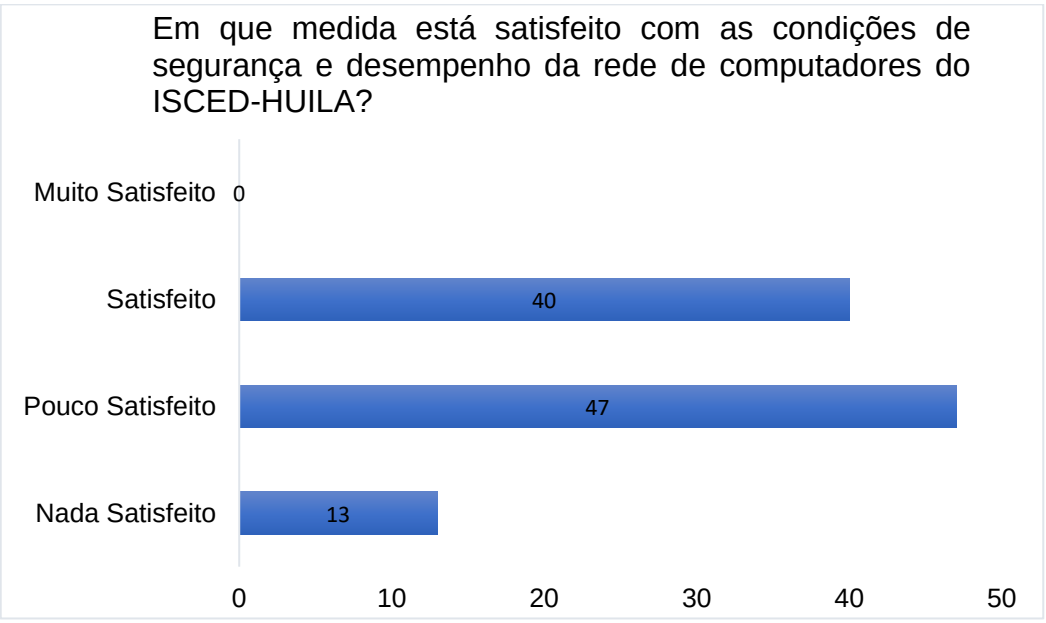
Gráfico 4 - Referente à questão nº 4, feita aos Gestores da Rede



Essa questão foi colocada aos gestores da rede do ISCED-Huíla, com o objectivo de saber em quais aspectos a rede do ISCED-Huíla precisar melhor na segurança? Como se pode observar no gráfico 4, 75% dos inquiridos responderam Prevenção de perda de dados, Segurança da Web e controle de acesso. Controlar quem deve e não deve aceder a rede de computadores de uma organização não é uma tarefa fácil. O controlo de acesso (NAC), garante que apenas utilizadores autenticados e dispositivos autorizados e em conformidade com as políticas de segurança possam

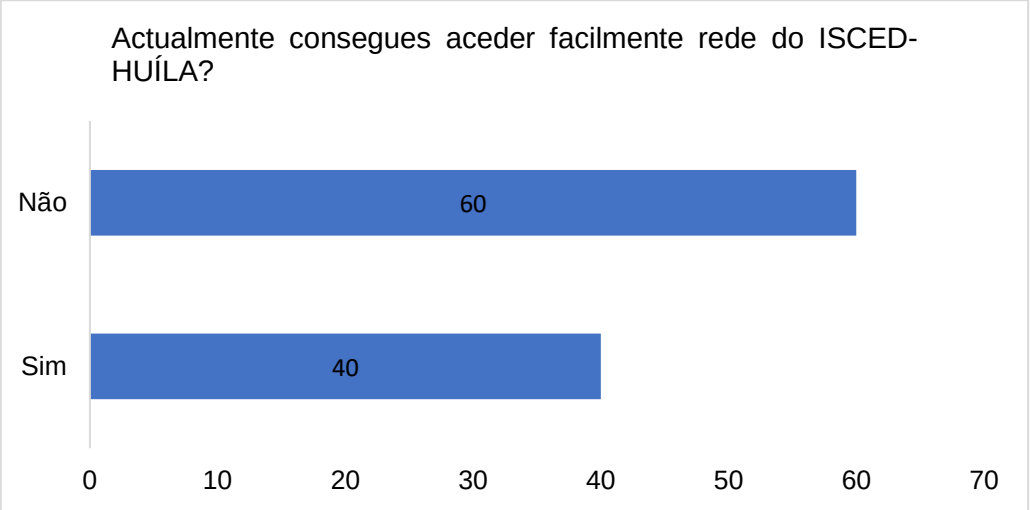
2.2.1.2. Resultado dos Inquéritos aplicados aos Funcionários Administrativos

Gráfico 5 - Referente à questão nº 1, feita aos Funcionários Administrativos



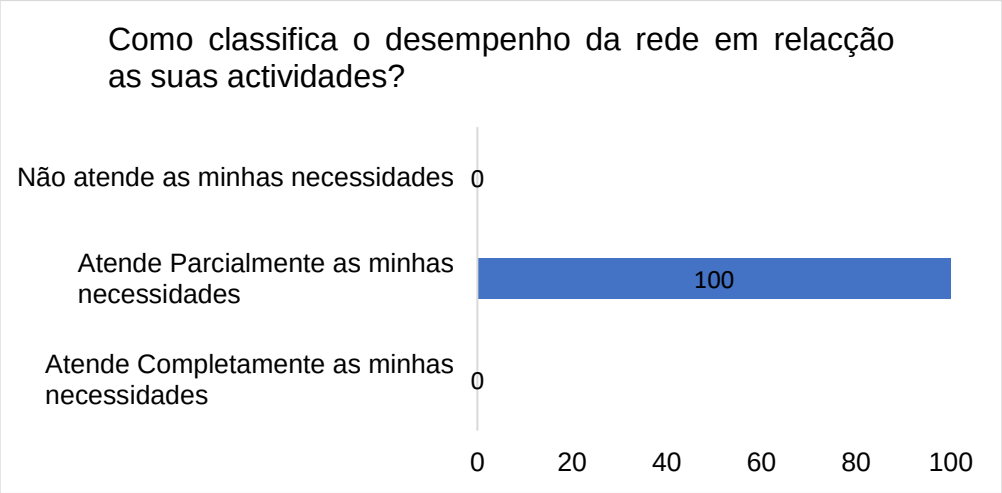
Essa questão colocou-se aos funcionários administrativos do ISCED-HUÍLA, com o objectivo de descobrir em que medida estão satisfeitos com as condições de segurança e desempenho da rede de computador. Como se pode observar no gráfico 5, 40% dos inquiridos responderam satisfeitos, 47% satisfeitos e 13% responderam nada satisfeito.

Gráfico 6 - Referente à questão nº 2, feita aos Funcionários Administrativos



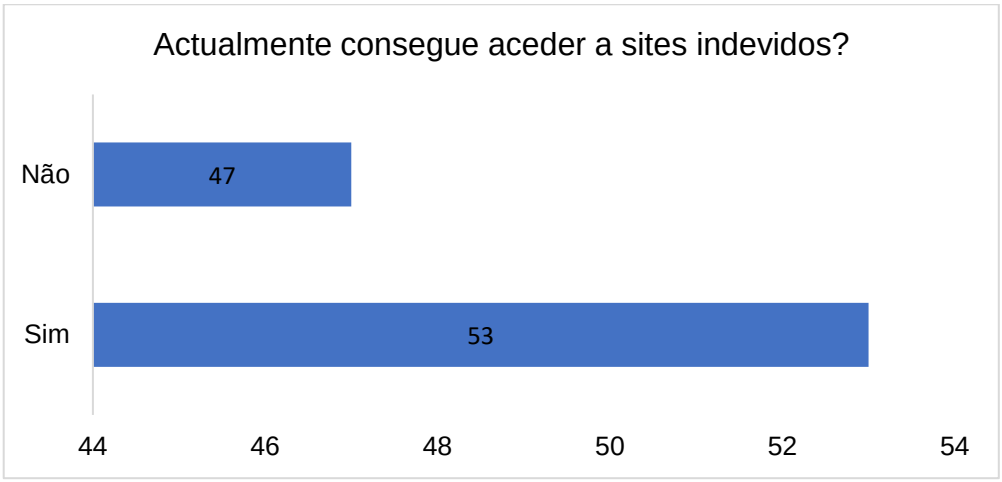
Essa questão colocou-se aos funcionários administrativos do ISCED-HUÍLA, com o objectivo de saber se se consegue aceder facilmente a rede da instituição. Como se pode observar no gráfico 6, 60% dos inquiridos responderam não, ao passo que 40% sim. Em redes corporativas se deve ter bastante atenção se os utilizadores conseguem ou não ter fácil acesso a mesma. Muitas das vezes quando não se tem em conta este pormenor, o utilizador acaba não utilizando os serviços oferecidos pela rede, tornando assim o ambiente de trabalho pouco produtivo quando esses dependem do acesso a rede para a realização das tarefas. Então, faz-se necessário criar condições de acesso a rede de maneira que a manter a sua disponibilidade.

Gráfico 7 - Referente à questão nº 3, feita aos Funcionários Administrativos



Essa questão foi colocada aos funcionários administrativos do ISCED-HUÍLA, com o objectivo de classificar o desempenho da rede em relação as realizações das tarefas. Como se pode observar no gráfico 7, 100% dos inquiridos responderam que atende parcialmente as suas necessidades.

Gráfico 8 - Referente à questão nº 4, feita aos Funcionários Administrativos



Essa questão foi colocada aos funcionários administrativos do ISCED-HUÍLA, com o objectivo de saber se conseguem aceder a sites indevidos. Como se pode observar no gráfico 8, 47% dos inquiridos responderam que não, e 53% responderam que sim. Esse facto é uma prova real de que a firewall não está a funcionar correctamente ou não foi correctamente configurada.

2.3. Mecanismos e funcionalidades Implementadas para a Segurança da Rede de Computadores

Hoje em dia, cada vez mais em infra-estruturas de redes necessitam de ser implementadas planos de segurança. Mesmo em redes de pequena dimensão, torna-se indispensável a utilização de ferramentas de segurança. A segurança de redes procura minimizar os problemas associados ao acesso não autorizado a recursos da rede.

Em relação aos sites de internet, utilizamos o servidor Proxy que contem regras simplificadas e bloqueios a sites indesejados e controle de portas, evitando que a rede da Instituição seja invadida por pessoas de má fé.

Após a configuração do servidor estabeleceu-se limitação através do Firewall por meio de regras de entrada e regras de saídas, garantindo que a comunicação entre outros departamentos de VLANs diferentes seja feita com maior controlo e segurança, estabeleceu-se ainda o sistema de backup automático da informação de modo a evitar perdas de dados em consequência de mau funcionamento.

É importante salientar que mesmo com essas práticas de segurança, ainda existem diversas possibilidades para que as pessoas más intencionadas consigam extrair informações sensíveis da instituição.

Portanto para a implementação de mecanismos de segurança da rede da instituição em estudo fez-se necessário uma interligação entre as Firewall e IDS onde o firewall tipicamente foi o responsável pelas filtragens de entradas e saídas na rede escolhendo os pacotes que podem ou não passar dependendo das suas características, enquanto que os sistemas IDS têm a função de reconhecer potenciais ataques em tempo real, através da análise de todos os processos e padrões de todo o comportamento de uma intrusão, para tal, o sistema IDS deve ser capaz de monitorizar e analisar todo tráfego da rede do ISCED-HUILA, podendo desta forma reconhecer padrões de ataques ou comportamento anormal logo pode se concluir que a diferença entre estes dois sistemas de protecção pensando que o Firewall sendo o gradeamento de uma casa e o sistema IDS sendo o alarme da mesma casa.

2.3.1. Políticas e procedimentos

Para Moreira (2017), uma organização que se baseia em meios digitais para realizar o seu trabalho, precisa lidar com o crescimento da estrutura de TI para que essas acções tenham êxito, o componente principal que deve ser priorizado é a segurança, com o objectivo de evitar problemas como o comprometimento dos activos, para tanto, é necessário que se tenha uma política de segurança planejada e cumprida por todos os entes da organização. Uma política de segurança é um conjunto de regras e práticas geralmente escritos que especificam e regulam como um sistema ou organização fornece serviços de segurança para proteger recursos sensíveis e críticos do sistema, contra ameaças e como lidar com situações quando elas ocorrem (Stallings & Brown, 2017).

O Centro de Informática possui políticas e procedimentos que devem ser seguidos por todos aqueles que têm um papel importante na manutenção da infra-estrutura informática, que são os seguintes:

- Cada novo equipamento que se pretenda ligar à rede necessita de ter o seu Mac-Address registado;
- Todas as tomadas de rede necessitam de registro para serem utilizadas;
- Nenhum equipamento de rede pode estar registado em duas tomadas;
- Todos os servidores que tenham um serviço disponibilizado para o exterior não podem ter outro dispositivo de rede para acesso à rede interna;
- Não é permitida a criação de pontos de acesso wireless com ligação à rede do ISCED – HUÍLA sem autenticação hotspot;
- Não é permitido acesso a rede wifi a mais de um dispositivo simultaneamente com o mesmo utilizador ou credenciais;
- Detectar e prevenir ameaças de segurança cibernética.

2.3.2. Requisitos de negócio e técnicos

Tendo em conta as fraquezas (vulnerabilidades) identificadas na rede do ISCED-Huíla e as políticas definidas, foram então formulados um conjunto de requisitos de negócio e técnicos, que são apresentados na seguinte tabela.

Tabela 2 - Requisitos de negócio e técnico

REQUISITOS DO NEGÓCIO	REQUISITOS TÉCNICOS
Garantia de funcionamento e disponibilidade do acesso a Internet.	Mais de um Link Internet de operadoras diferentes
Limitação e liberação de acesso a alguns sites.	Servidor proxy para filtrar conteúdos indesejáveis à política da Instituição.
Cópia de segurança das transacções realizadas para rápida recuperação.	Servidores de backup e softwares especializados em recuperação.
Monitoramento e Controlo de Intrusão	IDS SNORT
Garantir a segurança das informações trafegadas na rede.	Firewall contra intrusos, utilizando o mesmo servidor proxy para acesso a Internet
Limitações de downloads	Servidor Proxy
Acesso ao hotspot	Autenticação LDAP Google com hotspot no Captive Portal
Controlo das Impressoras	Servidor de Impressão PaperCut
Garantir a segurança física da instituição	Câmaras de vigilância e centrais de alarme

Fonte: Autores

Como se pode observar na tabela não está focado no modelo físico, pois o trabalho é continuidade do projecto de Faustino Sita Sunda, no seu trabalho de fim do curso elaborado em 2021. Para o autor, a instituição em estudo possui já uma infra-estrutura de redes de computadores. Depois de comprovado por nós, decidimos não detalhar novamente sobre o projecto físico da rede.

2.3.3. Projecto lógico da rede

Para a reestruturação da rede foram considerados quatro pontos principais: Roteador de Internet, Firewall (pfSense), Switch principal e pontos acesso.

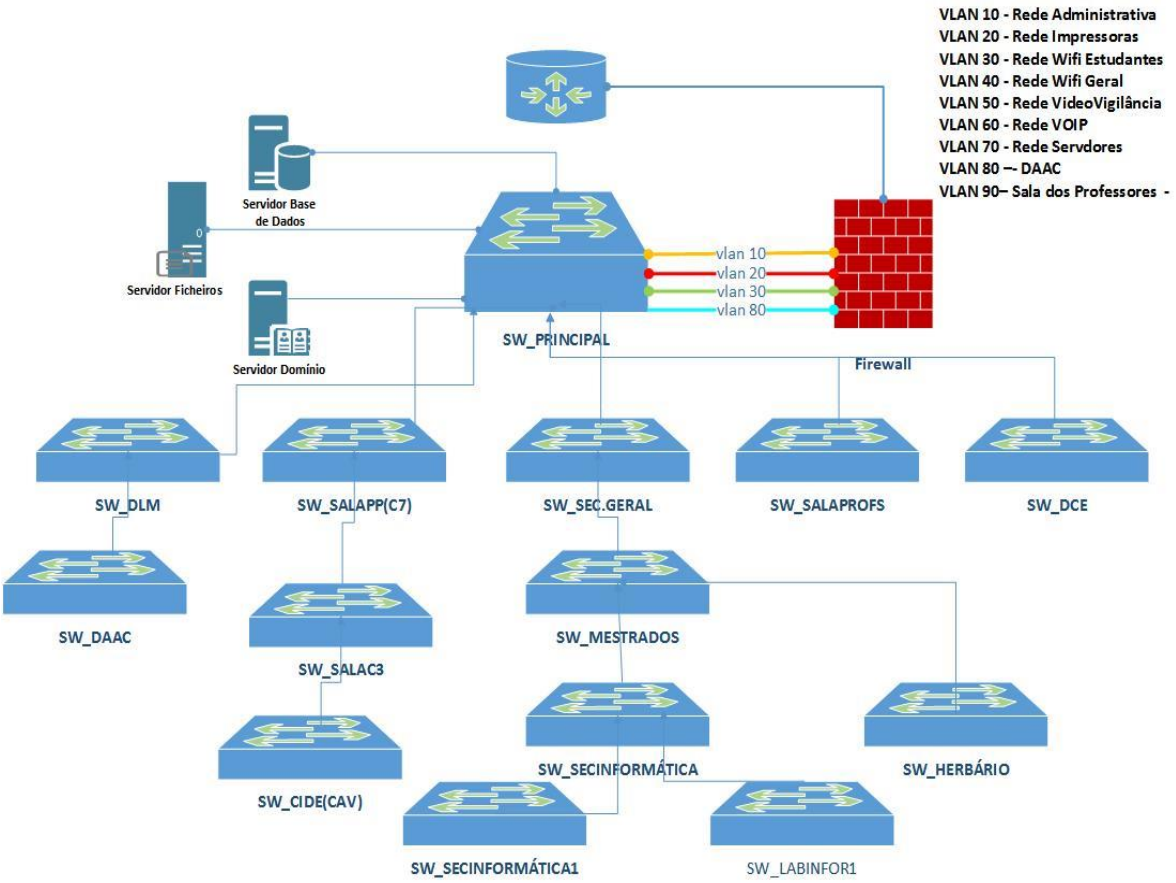


Figura 5 - Arquitectura Lógica da Rede

Fonte: Autores

Como vemos a figura acima, o Roteador de internet que é o primeiro ponto, tem a responsabilidade de efectuar o acesso tanto ao exterior (Internet) como ao interior (pontos de distribuição), através de equipamentos activos como roteador principal e switches. O segundo ponto, é o Firewall (pfSense), que permitiu fazer a gestão da rede interna. Com este Firewall foi possível configurar-se vários serviços, como o servidor DHCP, Proxy Transparente, controlo e distribuição de banda, ponto de acesso com autenticação via LDAP utilizando como servidor o GSuite, entre outros. No terceiro ponto encontra-se o Switch principal, sendo ela a camada de distribuição. Neste ponto fez-se a segmentação da rede através da criação de VLANs, que permite a comunicação entre o âmbito local e o roteador principal, através dos switches localizados na instituição. Por fim, o quarto ponto é a camada de acesso. A função principal do ponto de acesso é de interligar cada posto de trabalho com os equipamentos de rede das Rack. Houve-se a necessidade de se configurar as VLANs no intuito de segmentar a rede de forma a se ter maior controlo

sobre a mesma. As VLANs permitem que um grupo de dispositivos disponíveis em várias redes sejam combinados em uma rede lógica.

A topologia física a adoptada foi a estrela construída em cabo UTP cat6 desde as Rack até as tomadas RJ-45 e em fibra óptica para interligar as Rack de outros edifícios e a Rack principal. Essa nova topologia traz consigo melhorias de segurança significativa em relação a topologia anterior. Diferente da topologia anterior em que o Ipcop era a única camada de segurança, essa topologia conta agora com duas camadas de segurança, tanto a nível do roteador onde fez-se a configuração do roteamos e algumas regras de NAT, quanto a nível do Firewall pfSense que é responsável pelo endereçamento lógico, filtragem de pacotes e conteúdos na internet. O pfSense oferece recursos avançados de segurança.

2.3.3.1. Tabela de endereçamento

A nível do endereçamento a rede contava com apenas uma subrede para todas as máquinas, isso era um problema, pois os gestores da rede tinham bastante dificuldade em fazer a gestão e controlo das máquinas que se ligavam a rede. Actualmente para mitigar esse problema criaram-se várias VLANs e para VLAN foi atribuída uma subrede diferente.

Tabela 3 - Tabela de endereçamento

Designação	VLAN ID	Endereço de Rede	Pool DHCP	Máscara
AdminG	VLAN 10	192.168.10.0	196.168.10.1 – 250	255.255.255.0
Impressoras	VLAN 20	192.168.20.0	196.168.20.1 – 50	255.255.255.240
Wifi-Estudantes	VLAN 30	192.168.30.0	196.168.30.1 – 50	255.255.255.192
Wifi-Geral	VLAN 40	192.168.40.0	196.168.40.1 – 120	255.255.255.128
Videovigilância	VLAN 50	192.168.10.0	196.168.50.1 – 50	255.255.255.192
VoIP	VLAN 60	192.168.60.0	196.168.60.1 – 50	255.255.255.192
Servidores	VLAN 70	192.168.70.0	196.168.70.1 – 30	255.255.255.192
DAAC	VLAN 80	192.168.80.0	196.168.80.1 – 20	255.255.255.240
Sala dos Professores	VLAN 90	192.168.90.0	196.168.90.1 – 20	255.255.255.240

Fonte: Autores

Como se pode ver na tabela temos 9 (nove) VLANs implementadas. Foram utilizadas máscaras de classe C de tamanho variável, em função da quantidade de host necessárias para cada VLAN. Com exceção da VLAN 70 dos Servidores onde a atribuição do IP foi manual para os clientes, nas demais VLANs o endereçamento destas redes ficou a cargo de um servidor DHCP, para atribuição dinâmica dos endereços das máquinas clientes.

2.3.4. Configuração e soluções implementadas

Nesta fase serão apresentadas considerações sobre a implementação do projecto, onde foram utilizadas as seguintes técnicas e ferramentas:

- **PfSense** é uma distribuição linux, licenciada sob BSD licence, que tem por base o sistema operacional FreeBSD, tendo sido adaptado para assumir o papel de uma firewall e/ou roteador de rede, totalmente gerenciado por uma interface web fácil de usar (Netgate, 2022).

Escolheu-se esse sistema por ser um Firewall completo, que oferecendo recursos avançados de segurança, como filtragem de pacotes, detenção de Intrusão, prevenção de ataques, QoS, balanceamento de link, controle de acesso baseado em regras de Firewall, suporte a uma variedade de protocolos de rede. É gratuito, não possui custo de licenciamento, as conexões simultâneas são ilimitadas. Além disso oferece aos administradores da rede uma variedade de recursos de monitoramento de rede, como monitoramento de tráfego, largura de banda e monitoramento de sistemas de forma eficaz e segura. Outra razão que nos levou a escolher esse Firewall é facilidade de se fazer o backup das configurações, o que torna a administração muito mais fácil e segura, isso quando o backup das configurações é feito regularmente. Toda administração do pfSense é feita após a instalação via navegador na rede local. Instalou-se, e configurou-se além da solução de NAT que é padrão, os seguintes módulos:

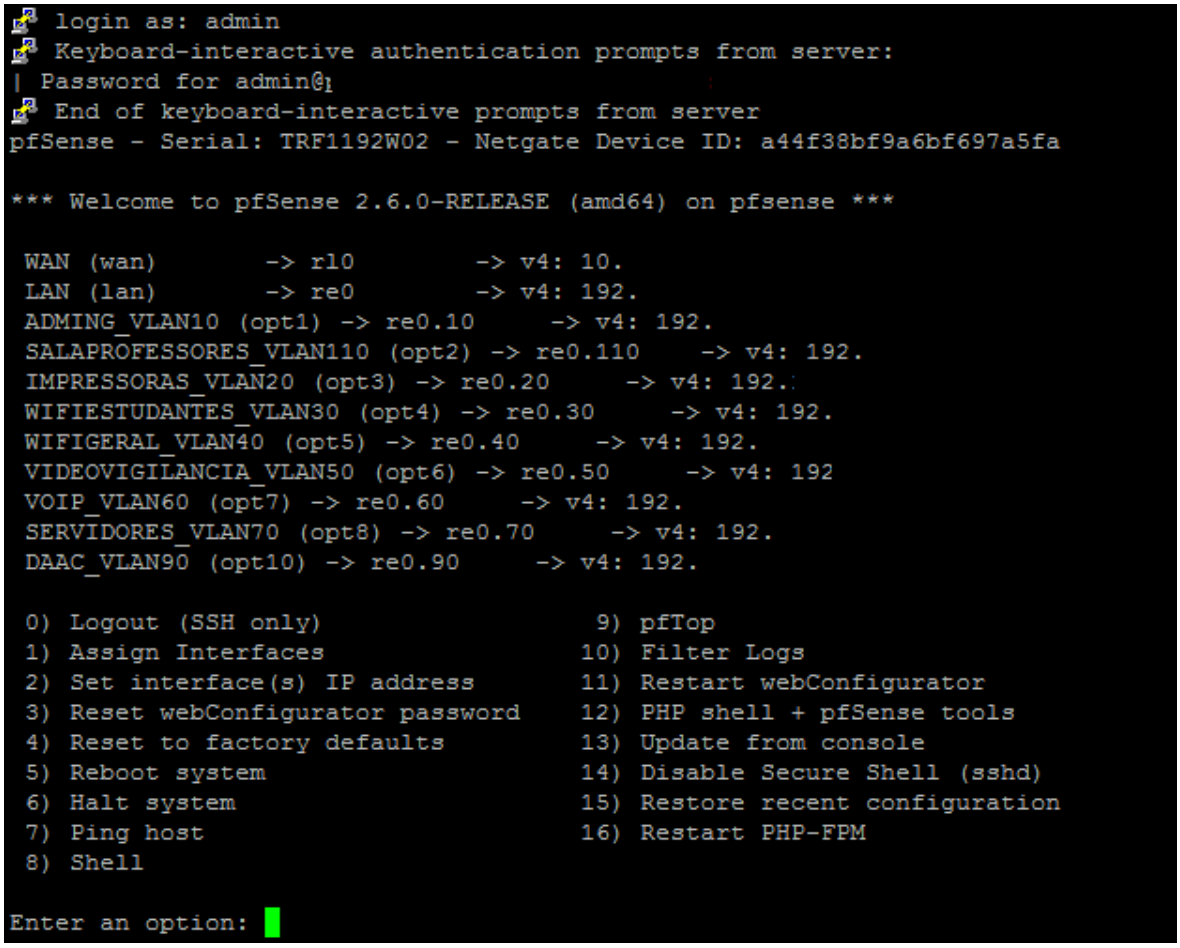


Figura 6 - Tela de gestão do pfSense

Por padrão, o webconfigurator só é acessível a partir da interface LAN. Pode ser configurado para ser acessível também na interface WAN, mas para a configuração inicial precisamos de uma maneira de acessá-la a partir da interface LAN. Na configuração inicial, o certificado SSL do webconfigurator é um certificado autoassinado padrão, então você precisa informar seu navegador para aceitar este certificado não confiável para exibir a página de login e autenticar com credenciais padrão (nome de usuário=admin e senha=pfsense).

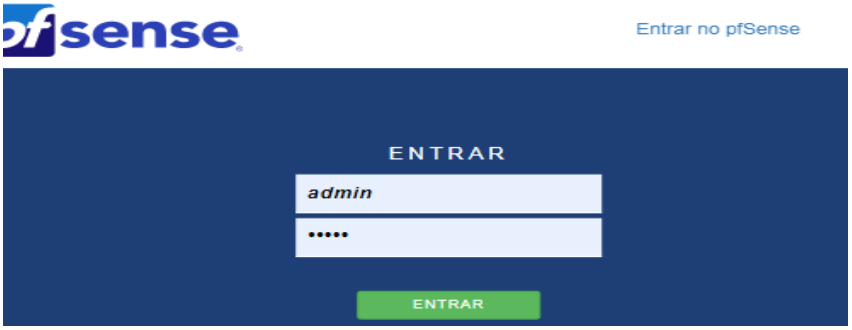


Figura 7 - Tela de Login do pfSense

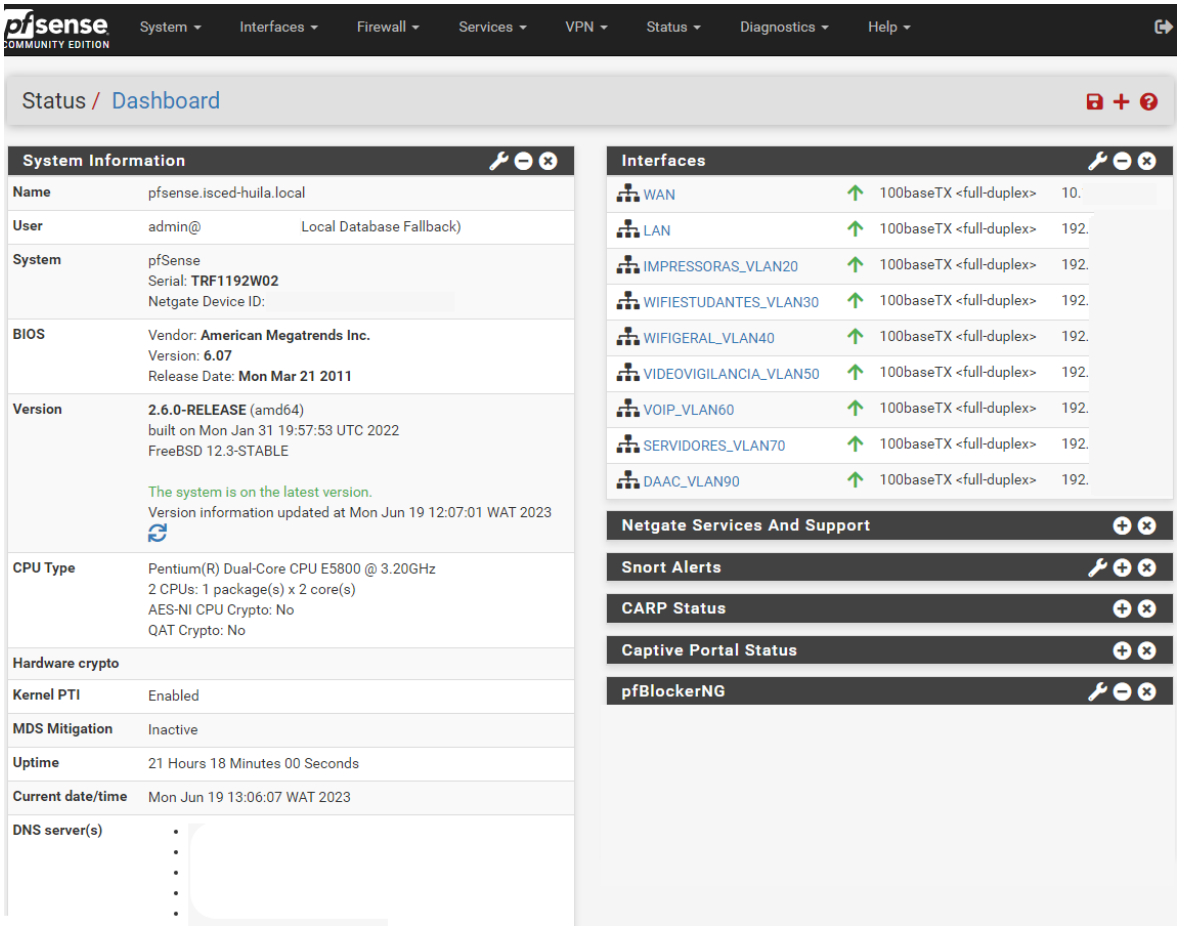


Figura 8 - Dashboard do pfSense

Como se pode notar na figura 10, a interface Web do pfSense é dividida em vários menus de configuração com variados serviços, abaixo são mencionadas algumas funcionalidades desses menus implementadas no projecto:

- **Segmentação da Rede** – Para segmentar a rede de forma lógica criou-se VLANs permitindo assim restrições próprias para cada sub-rede. Além de criar a VLAN no switch da camada. Também se criou um gateway para cada VLAN na camada 3 na firewall pfSense.

Figura 9 - VLANs e seus endereçamentos

Tal como vimos anteriormente a configuração de VLANs no switch fez-se necessário configurar as mesmas no pfSense, de maneira a fazer o endereçamento de IP do mesmo. A figura 9 mostra as interfaces activas no pfSense e seus IPs.

- **Autenticação de utilizadores e servidor de autenticação –** A autenticação é importante porque permite que as organizações mantenham suas redes seguras, permitindo que apenas utilizadores (ou processos) autenticados acedem seus recursos protegidos, que podem incluir sistemas de computador, redes, bancos de dados, sites e outros aplicativos ou serviços baseados em rede. Assim sendo configurou-se o captive portal de modo a solicitar os utilizadores da rede a se autenticarem antes de conceder acesso à Internet. O Captive portal necessita de um servidor de autenticação para gerir os utilizadores. Daí que se teve que recorrer à utilização das contas do GSuite do ISCED-HUILA, permitindo que cada utilizador se autentique com o seu email e senha institucional. O GSuite um serviço oferecido pelo Google o qual possui vários produtos que podem ser facilmente personalizados de forma independente com o nome de domínio do cliente. Ele oferece vários aplicativos da web com recursos similares aos de pacotes de escritório tradicionais, inclusive Gmail, Hangouts, Google Agenda, Drive, Docs, Planilhas, Apresentações, Groups, News, Play, Sites e Vault.

Assim sendo foi necessário configurar um cliente LDAP do Google de modo que gerasse o certificado e credenciais para acesso aos emails do GSuite do ISCED-HUILA.

Feito isso fez-se a integração do Cliente LDAP do GSuite com o pfSense importando o certificado gerado pelo cliente LDAP do GSuite no pfSense, depois fez-se a criptografia SSL entre o cliente remoto e o servidor local através do programa STunnel e criou-se uma base de consulta LDAP no pfSense.

Para se ter acesso a tela de login do captive portal, o utilizador tem de se conectar a rede sem fio e tentar abrir uma página Web, o captive portal intercepta a tentativa de acesso e, redirecciona o utilizador para uma tela de autenticação.

Figura 10 - Tela de autenticação do Captive Portal

Após a autenticação, o utilizador já pode navegar na internet sem nenhum problema. De lembrar que o acesso à Internet só será liberado se o utilizador possuir login e senha válidos

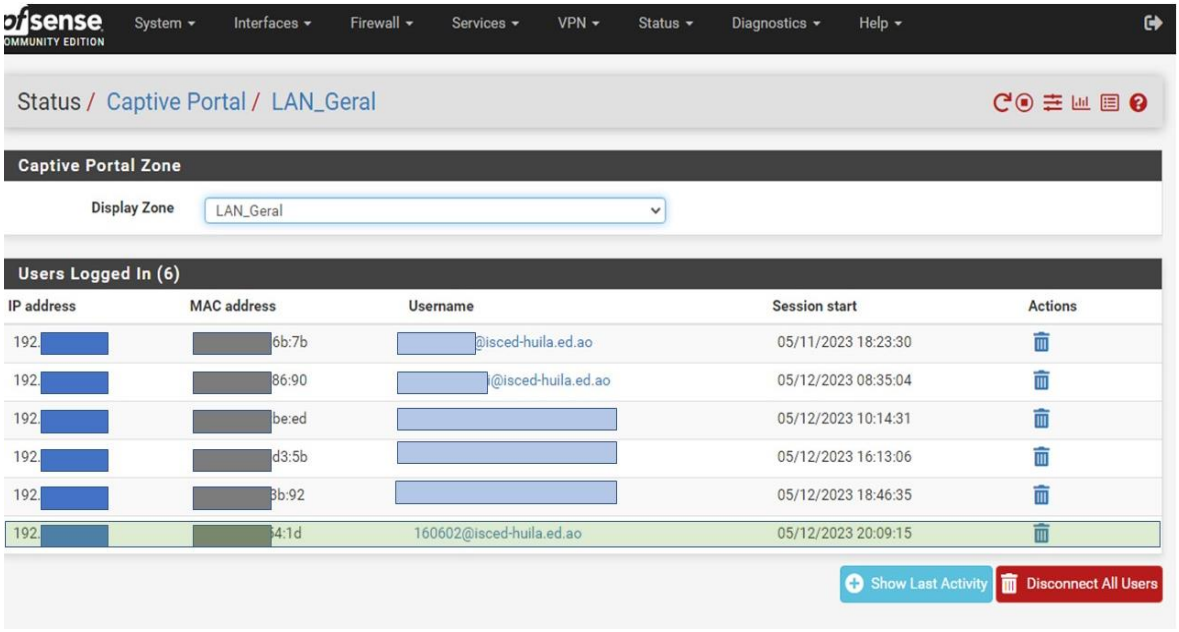


Figura 11 - Status do Captive Portal

Como se pode notar na figura acima, a autenticação correu devidamente permitindo ter maior controlo sobre quem está ligado na internet.

- **Proxy, WebCache –** Configurou-se o proxy de modo a fazer a filtragem de todos os conteúdos acedidos pelos utilizadores fora da rede. Para isso configurou-se o Squid, SquidGuard e LithSquid, essas ferramentas podem ser baixadas directamente no pfSense na lista de pacotes. Antes das demais configurações do Squid tem que se ter em atenção o WebCache, então foi configurado o WebCache no intuito de fazer cópias das requisições das páginas e arquivos consultados pelos utilizadores na web, tornando a rede mais rápida.

No Squid configurou-se o proxy no modo transparente que além de fazer o cache da conexão permite a fim de que possamos auditar e controlar o conteúdo que será entregue aos utilizadores.

Hard Disk Cache, foi definido tamanho do cache que será guardado no disco, no caso do projecto implementado foi de 30000MB; - Cache System, Local onde são guardados os arquivos de cache. Deixou-se o mesmo no directório /var/squid/cache por padrão; - Memory Cache Size, definiu-se aqui o tamanho de memória do sistema para colocar os arquivos cacheados, em geral é recomendado no máximo 50% da memória instalada; Minimum Object Size, definiu-se o volume mínimo dos arquivos armazenados em cache; Maximum Object Size - Permanece a dimensão

máximo de arquivos guardados em cache.; Maximum Object Size in RAM - define a quantidade máxima de objectos guardados dentro da memória Ram do servidor.

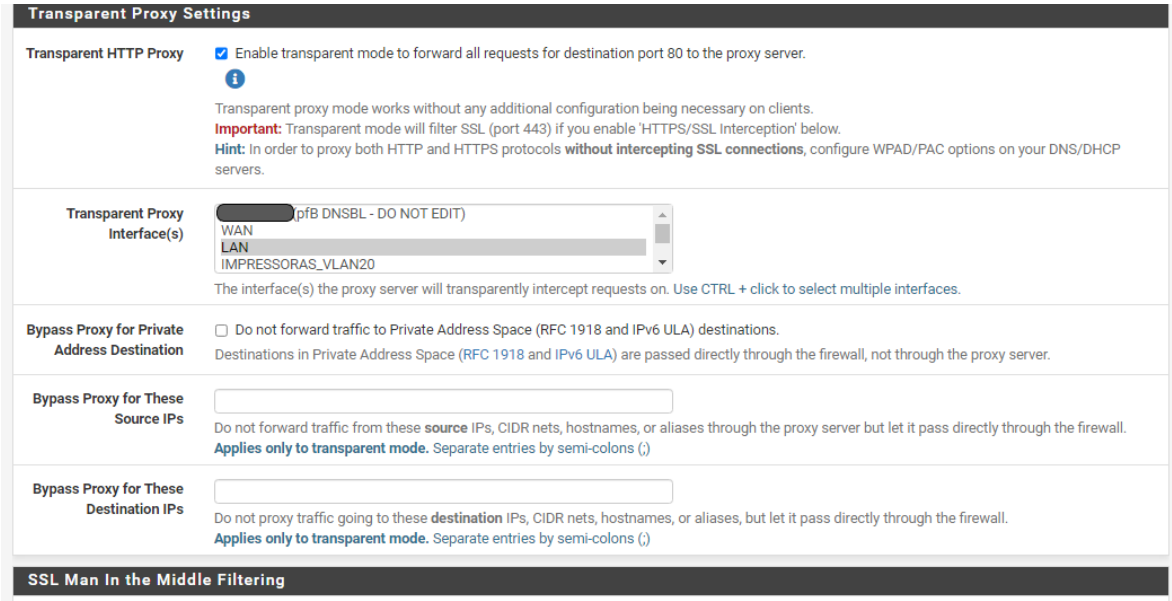


Figura 12 - Configuração do Proxy transparente

- **Bloqueio de URL –** Para o controle de conteúdo utilizou-se o SquidGuard, dessa maneira fica mais fácil permitir ou bloquear o conteúdo que pode ser trafegado na rede do ISCED-HUILA. Utilizou-se uma blacklist que permitiu dar permissões e bloqueios de sites por categorias. Para mais detalhes de configuração.

Na imagem acima mostra a blacklist e nela definiu-se várias regras, com destaque a regra de bloqueio de sites adultos (pornográficos), malware entre outros.

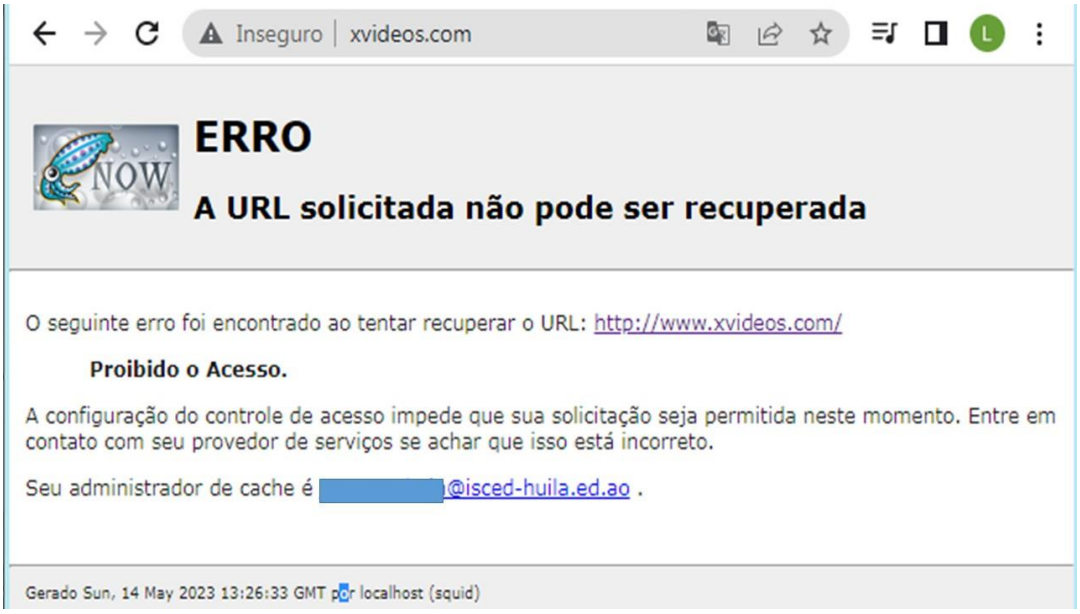


Figura 13 - Página de bloqueio

A figura cima mostra o bloqueio realizado pelo Squid a um site adulto.

- **Outras regras de permissão de entrada e saída de dados –** O pfSense é um UTM robusta. Ela dispõe de várias soluções de segurança para uma determinada rede, assim, para além do Squid, foram configuradas regras de firewall e NAT que permitem controlar o tráfego da rede do ISCED-HUILA.

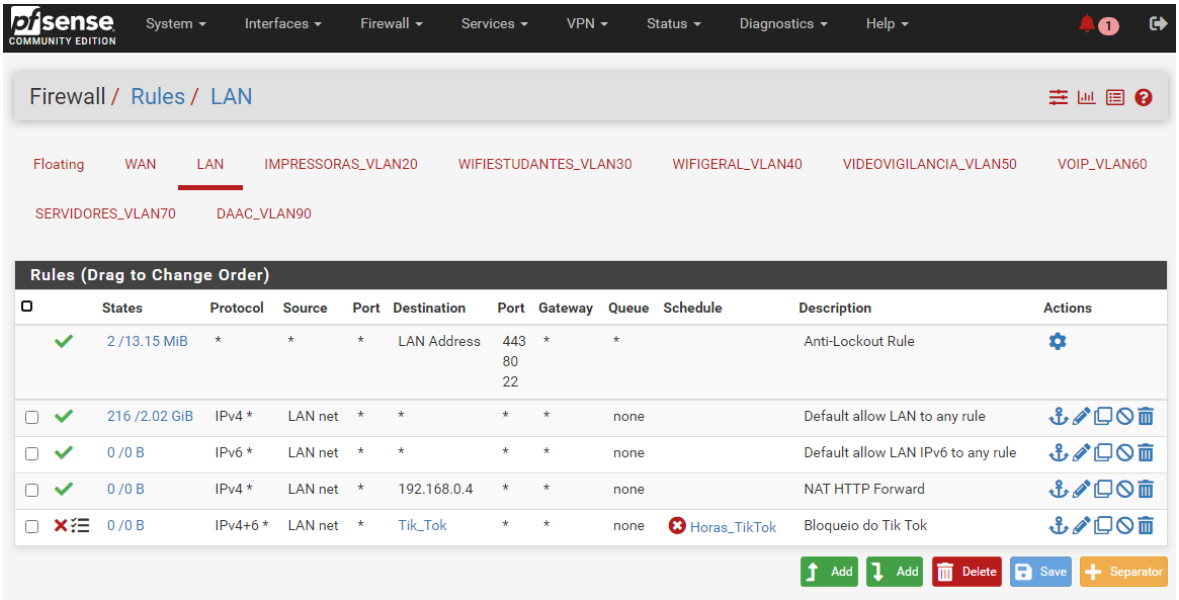


Figura 14 - Regras de firewall

Como se pode ver na figura acima tem-se algumas regras configuradas, como a regra de bloqueio do tiktok, e criou-se também o Port Forward para se ter acesso a secretaria virtual do ISCED-HUILA a partir da internet.

1ª regra - A primeira regra é para o firewall pfSense sendo um padrão que permite o acesso através do SSH para configuração em modo texto, ou através da porta 80, que permite a configuração via browser; 2ª regra - A segunda regra é para a LAN, liberando para saída (nada entra a não ser que uma resposta foi solicitada) na internet tudo que vem dele, é uma regra padrão; 3ª regra - A terceira regra é para a LAN, liberando para saída (nada entra a não ser que uma resposta foi solicitada) na internet tudo que vem dele, é uma regra padrão, para IPv4; 4ª regra - Essa regra é o Port Forward para se ter acesso a secretaria virtual do ISCED-HUILA a partir da internet; 5ª regra - A quinta regra bloqueia todo tráfego da rede LAN para o tik tok.

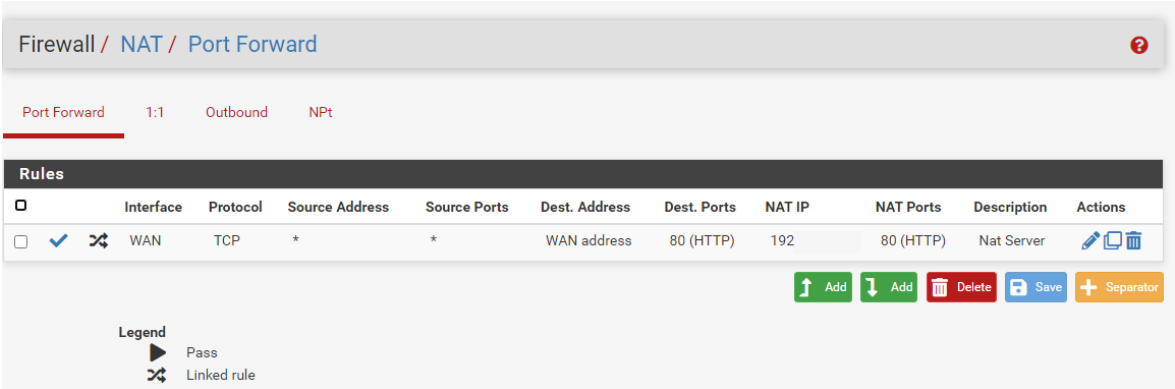


Figura 15 - Port Forward para acesso a secretaria virtual

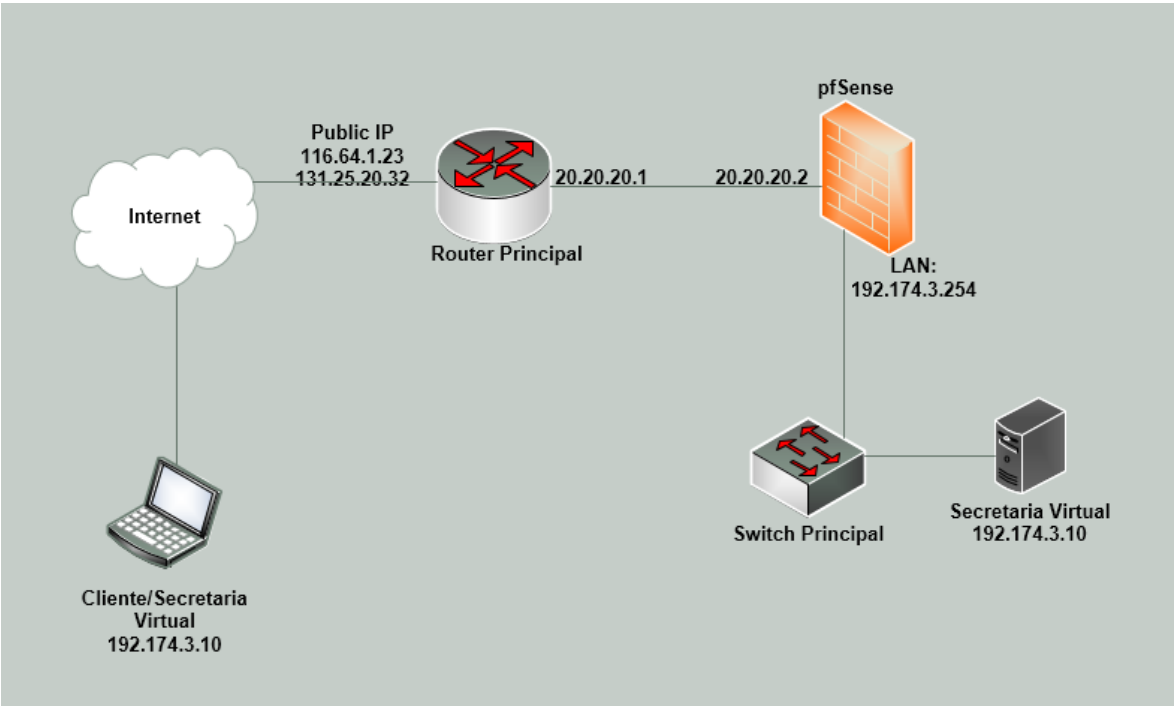
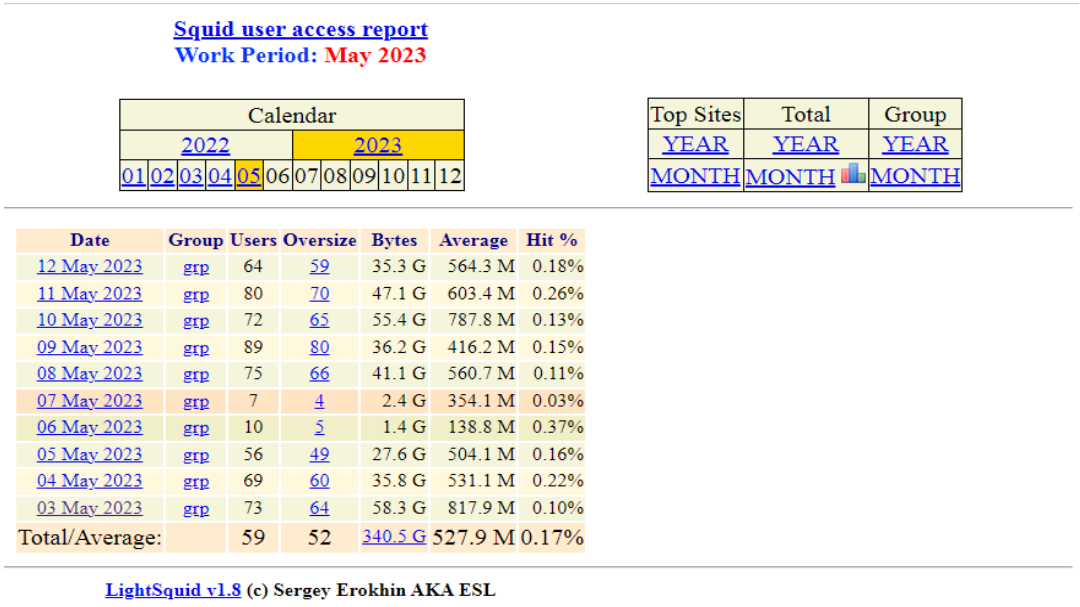


Figura 16 - Diagrama lógico do PortForward

A imagem acima ilustra a portforward configurado para se ter acesso a secretaria virtual a partir da internet. Assim, foi necessário configurar essa regra no firewall pfSense como vemos na figura 15 e 16, e ainda houve-se a necessidade de se configurar uma regra Nat no router.

- **Auditoria por relatório de acesso aos sites** – Para auditoria dos sites acedidos utilizou-se o LightSquid. Essa ferramenta gera relatórios de todos os sites acedidos por cada utilizador na rede.



Squid user access report
Work Period: May 2023

Calendar											
2022				2023							
01	02	03	04	05	06	07	08	09	10	11	12

Top Sites	Total	Group
YEAR	YEAR	YEAR
MONTH	MONTH	MONTH

Date	Group	Users	Oversize	Bytes	Average	Hit %
12 May 2023	grp	64	59	35.3 G	564.3 M	0.18%
11 May 2023	grp	80	70	47.1 G	603.4 M	0.26%
10 May 2023	grp	72	65	55.4 G	787.8 M	0.13%
09 May 2023	grp	89	80	36.2 G	416.2 M	0.15%
08 May 2023	grp	75	66	41.1 G	560.7 M	0.11%
07 May 2023	grp	7	4	2.4 G	354.1 M	0.03%
06 May 2023	grp	10	5	1.4 G	138.8 M	0.37%
05 May 2023	grp	56	49	27.6 G	504.1 M	0.16%
04 May 2023	grp	69	60	35.8 G	531.1 M	0.22%
03 May 2023	grp	73	64	58.3 G	817.9 M	0.10%
Total/Average:		59	52	340.5 G	527.9 M	0.17%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Figura 17 - Relatório geral

Nas figuras acima pode-se ver a tabela geral com os dias, e na outra podemos ver os sites acedidos por um determinado utilizador. O pfSense filtra todos os tráfegos da rede, e optimiza o acompanhamento das actividades dos utilizadores em geral, e esses relatórios podem ser recolhidos ao final do mês, posteriormente podem ser solicitados para análise e nas auditorias.

- **Detecção e prevenção de Intrusão** – Para além das regras de firewall e filtragem de conteúdos, utilizou-se também o SNORT, para detectar e prevenir a rede contra intrusões. O Snort é um sistema de detecção de intrusões baseado na rede. É um IDS baseado em assinaturas que utiliza regras para verificar a existência de pacotes com informações que possam indiciar a ocorrência de um ataque. Regras essas que consistem num conjunto de requisitos que gerariam um alerta

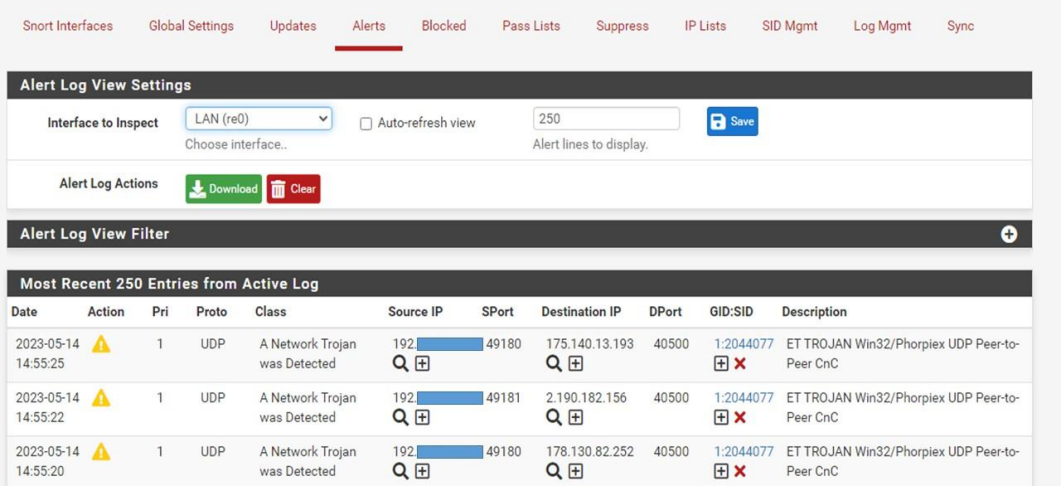


Figura 18 - Alertas de intrusão no Snort

Como vemos na figura acima, o Snort está gerando alerta sobre algumas possíveis tentativas de ataque.

- **Backup -** O software pfSense faz um backup interno a cada alteração quando configurados no modo automático, Porém preferiu-se optar em fazer backup manuais, e é tida como a melhor prática backup (Netgate, 2022). O processo de backup é bastante simples e indolor, os administradores devem criar o hábito de baixar um backup de vez em quando e mantê-lo em local seguro**.**
- **Controlo de Impressão –** Para monitorar e controlar a impressão pela rede de maneira segura utilizou-se o PaperCut. Que permitiu que numa primeira fase os professores do ISCED-HUILA fizessem as suas impressões de forma controlada.

O PaperCut é um Software que permite fazer gestão e monitoramento de operações de impressão de uma organização, possibilitando assim a redução e o desperdício, com uma experiência de impressão segura e fácil (PaperCut, 2023).

Para tal fez-se a integração dos GSuite com o PaperCut de modo a sincronizar os emails dos professores ao Servidor de impressão.

Essa integração foi feita através do LDAP, tal como a sincronização GSuite com pfSense, também foi necessário criar um cliente no GSuite para o Servidor de Impressão.

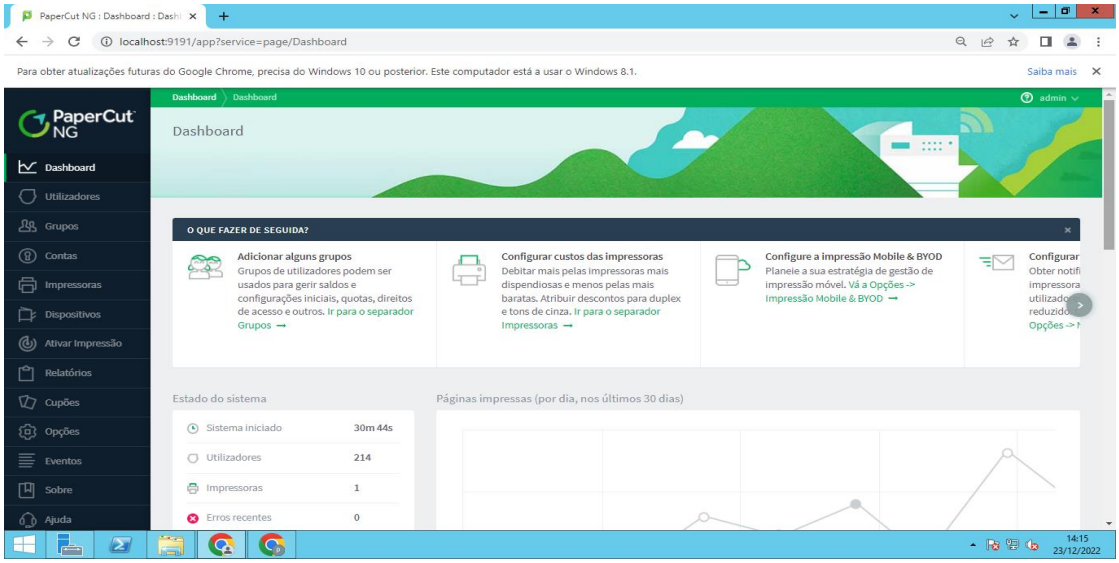


Figura 19 - Ambiente de gestão do PaperCut

Esse servidor permite definir quotas de impressão por utilizadores. A impressora deve estar ligada à rede e registada no Servidor, no nosso caso foi registada num dos servidores Windows da Instituição.

- **Link redundante** – A instituição contava apenas com um link de internet, e esse link muitas das vezes esse mesmo link se encontra indisponível por várias razões técnicas impedindo no bom funcionamento da instituição por falta de Internet. Assim foi contratado mais um link de internet de uma outra operadora no intuito de assegurar a disponibilidade de acesso da internet. Foi ainda configurado o Router principal para fazer o balanceamento entre esses dois links.

```
RT_PRINCIPAL#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.1       unassigned      YES unset  up                    up
GigabitEthernet0/0.200     105.[redacted]  YES NVRAM  up                    up
GigabitEthernet0/0.300     10.[redacted]   YES NVRAM  up                    up
GigabitEthernet0/1         unassigned      YES NVRAM  down                  down
GigabitEthernet0/2         154.[redacted]  YES NVRAM  down                  down
GigabitEthernet0/2.200     unassigned      YES unset  down                  down
GigabitEthernet0/2.300     unassigned      YES unset  down                  down
SM1/0                      unassigned      YES NVRAM  administratively down down
SM1/1                      unassigned      YES unset  administratively down down
Loopback0                  1.1.1.1         YES NVRAM  up                    up
NVI0                       1.1.1.1         YES unset  up                    up
Vlan1                      unassigned      YES unset  down                  down
```

Figura 20 - Configuração das Interfaces no Router Principal

Na figura acima mostra as interfaces configuradas, sendo GigabitEthernet0/2 para o link de Internet da Operadora 1, GigabitEthernet0/0.200 para o link de Internet da Operadora 2 e GigabitEthernet0/0.100 para a rede local. Na interface GigabitEthernet0/0 foi houve-se a necessidade de se configurar duas subinterfaces pelo facto da GigabitEthernet0/1 apresentar alguns problemas. Para que o Router se comunicasse com o Firewall(pfSense) foi necessário configurar-se o roteamento.

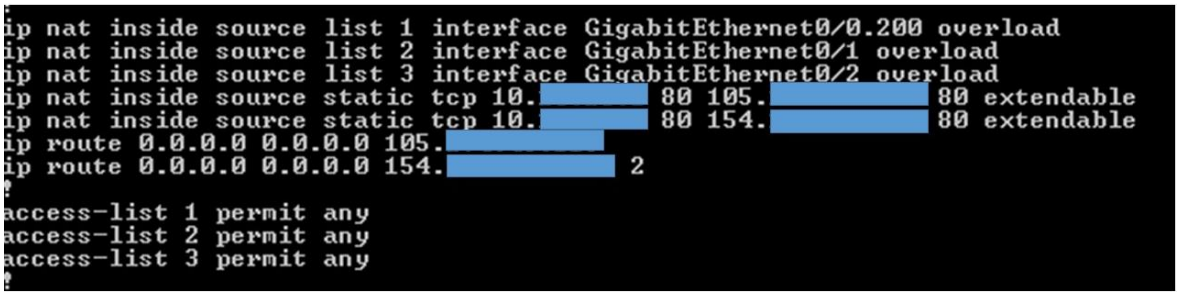


Figura 21 - Configuração de NAT e Rotas no Router Principal

Atendendo que a nossa rede possui dois links de internet de provedores diferentes, foi necessário criar duas rotas estáticas que permitiu a troca de pacotes entre os hosts.

Conclusões e Sugestões

Conclusão

Os resultados do diagnóstico feito ao ISCED-Huila, no âmbito da segurança em redes, demonstrou a existência de muitas vulnerabilidades e ameaças não controladas à rede e aos dados dos utilizadores.

Durante a realização deste projecto foram abordados vários temas e subtemas que nos permitiram entender melhor sobre a necessidade dos diferentes conceitos de segurança da informação e conceitos sobre rede de computadores, e das referências consultadas dos vários autores, foram unânimes de que a segurança informática é fundamental para a protecção de dados em uma rede corporativa.

Para implementação de mecanismos de segurança foi utilizado o software pfSense, SNORT IDS, SQUID, isto é, para a gestão dos serviços necessários para a nova estrutura de rede da instituição, pois além de ser uma ferramenta gratuita, ele possui recursos integrados, como: Captive Portal, VLANs, firewall, proxy, DNS cache, servidor DHCP, recursos estes, necessários para a solução dos problemas apresentados.

A implementação da firewall (pfSense), mostra que há melhoria na infra-estrutura de segurança acrescentando a ela uma segunda camada de filtros. Com a configuração das regras do firewall é possível bloquear por completo as conexões externas da rede.

Dessas melhorias destacam-se o acesso à Internet de forma livre, com uma autenticação para o acesso à rede para os computadores em cada departamento, controle da banda, bloqueios de sites indesejáveis, redução de limites de downloads, quer seja na rede LAN e WAN, bloqueio dados de entrada que possam conter um ataque de hacker, ocultação de informações sobre a rede interna, fazendo com que pareça que todo o tráfego de saída seja proveniente do Firewall e não da rede, denominado Network Address Translation (NAT), filtrar o tráfego de saída criando um limite de downloads para não sobrecarregar a rede, e bloqueio por completo das conexões externas da rede através das regras de firewall.

Sugestões

Sugerimos que se pague a licença do PaperCut de forma a usufruir dos variados serviços disponibilizados por essa ferramenta. Pois assim, a instituição terá uma gestão sobre as actividades de impressão, principalmente os gastos realizados pelos seus funcionários.

Como perspectiva de actividades futuras dando continuidade ao processo de análise de resultados deste trabalho, pretende-se adicionar novos recursos a segurança da infra-estrutura, como por exemplo o suporte a videovigilância.

Sugerimos ainda que sejam mediatizados aos funcionários da instituição que têm tido acesso a rede de computadores seminários relacionados com temas relacionados à segurança de redes de computadores, pois desta maneira o pessoal terá melhor atenção com as actividades realizadas dentro da instituição

Referências Bibliográficas

Bibliografia

Alchemer. (2023). Purposive Sampling 101. Acesso em 15 de Junho de 2023, disponível em Alchemer: https://www.alchemer.com/resources/blog/purposive-sampling-101/

Alecrim, E. (2013). O que é firewall? - Conceito, tipos e arquiteturas. Acesso em 18 de Maio de 2022, disponível em Info Wester: http://www.infowester.com/firewall.php

Alvarenga, E. M. (2012). Metodologia da Investigação quantitativa e qualitativa: Normas técnicas de apresentação de trabalhos científicos. 2ª. (C. Amarilhas, Trad.) Paraguay.

Anlix. (2021). Pontos positivos da VLAN. Acesso em 15 de Dezembro de 2022, disponível em Anlix: https://anlix.io/vlan-redes-virtuais-facilitam-trafego-e-agilizam-conexao/

Barbosa, J. S., & et al. (2021). A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional (Vol. 10). Fonte: https://rsdjournal.org/index.php/rsd/article/download/12557/11384/167309

Bezerra, A. (2012). Evitando Hackers. Rio de Janeiro: Ciência Moderna.

Bickman, L., & Rog, D. J. (2008). Applied Research Design: A Practical Approach. Fonte: https://www.sagepub.com/sites/default/files/upm-binaries/23770_Ch1.pdf

Cert br. (2003). Práticas de Segurança para Administradores de Redes Internet. Acesso em 17 de Janeiro de 2023, disponível em Cert br: https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html

Cisco. (2009). QoS Frequently Asked Questions. Acesso em 8 de Fevereiro de 2023, disponível em Cisco: https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html

Computer-Hope. (2023). What is backup? Fonte: Computer Hope: https://www.computerhope.com/jargon/b/backup.htm

Conceito. (2013). Conceito de autorização. Acesso em 10 de Maio de 2022, disponível em Conceito de: https://conceito.de/autorizacao

Conceito. (2020). Conceito de observação. Acesso em 3 de Novembro de 2022, disponível em Conceito de: https://conceito.de/observacao

Costa, M. B. (2022). O que é DNS? | Trocá-lo pode ser a solução. Acesso em 17 de Novembro de 2022, disponível em Canaltech: https://canaltech.com.br/internet/o-que-e-dns/

Dupaul, N. (2016). Spoofing Attack: IP, DNS & ARP.

Endian. (2022). Secure - Monitor - Analyze. Acesso em 2022, disponível em Endian : https://www.endian.com/company/about-endian/

Fares, A. A. (2021). Proposta De Integração De Um Sistema De Detecção De Intrusão (Ids) Entre Uma Rede Sdn E Uma Honeynet. Dissertação De Mestrado Profissional Em Engenharia Elétrica Na Universidade De Brasilia. Brasília.

Fazenda, A. (2016). Principais Protocolos da Internet. Fonte: https://pt.slideshare.net/AlessandroFazenda/principais-protocolos-da-internet-61296389

Gil, A. C. (2017). Como elaborar projetos de pesquisa (6ª ed.). São Paulo: Atlas.

Informatique-Mania. (4 de Novembro de 2022). Serviço de rede: o que são, para que servem e quais existem atualmente? Acesso em 4 de Novembro de 2023, disponível em Informatique-Mania: https://www.informatique-mania.com/pt/linformatique/service-reseau/

ISO/IEC 27000. (2018). Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação. Fonte: Plataforma de Navegação Online (OBP): https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Junior, A. (2017). Resumo Alguns Protocolos de Rede. Fonte: Academia edu: http://www.academia.edu/31537255/Resumo_Alguns_Protocolos_de_Rede

Kashefi, I., Kassiri, M., & Shahidinejad, A. (2013). A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities.

International Journal of Engineering Research and Applications (IJERA) (Vol. 7).

Kurose, J. F., & Ross, K. W. (2015). Redes de computadores e a Internet: uma abordagem top-down. (6 ed.). USA: Pearson.

Macedo, R. T., Francicatto, R., Cunha, G. B., & Bertolini, C. (2018). Redes de Computadores (1ª ed.). Santa Maria, Brasil.

Martins, L. H., Silveira, S. R., & Santos, F. B. (2017). Gerenciamento e Controle por Autenticação para Acesso à Estrutura de Rede de Computadores da Prefeitura Municipal de Palmeira das Missões – RS. Palmeira das Missões: UFSM. Fonte: http://repositorio.ufsm.br/handle/1/12905

Maschio, B. H. (2017). Segurança De Infraestrutura Com pfSense. Projeto de pesquisa apresentado ao curso de ciência da computação como requisito à obtenção do Certificado de Conclusão. Instituto Municipal de Ensino Superior de Assis – IMESA, São Paulo.

Maste, S. (2010). Vantagens e Desvantagens do Firewall. Acesso em 17 de Maio de 2022, disponível em forumeiros: http://habbosal.forumeiros.com/t1132-vantagens-e-desvantagens-do-firewall

Microsoft. (2022). Autorização de acesso de rede. Fonte: Microsoft: https://technet.microsoft.com/pt-br/library/cc732787%28v=ws.10%29.aspx

Mikrotik. (2015). Fonte: Mikrotik: http://www.mikrotik.com/

Nakamura, E. T., & Geus, P. L. (2007). Segurança de redes: em ambientes cooperativos. São Paulo: Novatec Editora Ltda. Fonte: https://books.google.com.br/books?id=AamSIJuLc34C

Nassaro, D. (2012). Sistemas de Detecção e Protecção Contra Invasões a Ambientes informatizados – IDS e IPS. Brasília: Segurança Digital.

Neogrid. (2022). Método estatístico: o que é como se aplica à cadeia de suprimentos. Fonte: Neogrid: https://neogrid.com/br/blog/metodo-estatistico-como-se-aplica-cadeia-de-suprimentos

Netgate. (2022). The pfSense Documentation. Acesso em 28 de Maio de 2020, disponível em https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-documentation.pdf

Networkpro. (2020). Curso gratuito - pfSenseCORE - Aula 2 - Instalação do pfSense + UFS x ZFS. Acesso em 20 de Dezembro de 2021, disponível em Youtube: https://www.youtube.com/watch?v=YsTLUHhFykg&list=PL3Sj98RICiBGJnypyKjfkQdGxxDbXgh3l&index=17

Oppenheimer , P. (2010). Top-Down Network design. Indianapolis, USA: Cisco Press.

PaperCut. (2023). PaperCut: Print Management. Fonte: PaperCut: https://www.papercut.com/

Pedra, D. (2022). O que é uma ameaça em segurança da informação? Como calcular o seu impacto? Acesso em 18 de Janeiro de 2023, disponível em Siteware: https://www.siteware.com.br/seguranca/o-que-e-uma-ameaca-em-seguranca-da-informacao/

Pressman, R. S., & Maxim, B. R. (2019). Software Engineering: A Practitioner's Approach (9ª ed.). USA. Fonte: https://dokumen.pub/qdownload/software-engineering-a-practitioners-approach-9nbsped-1260548007-9781260548006.html

Quiterio, A. P. (2006). Engenharia de software/analise de requisitos. Fonte: InfoEscola: https://www.infoescola.com/engenharia-de-software/analise-de-requisitos/

Redes, E. S. (2020). Arquitetura TCP/IP: conceitos básicos. Fonte: Escola Superior de Redes: https://esr.rnp.br/administracao-e-projeto-de-redes/arquitetura-tcp-ip/

República, D. d. (2011). Lei nº. 22/11. Lei de Protecção de Dados Pessoais. (I Série - N.º 114). Angola. Fonte: https://www.apd.ao/fotos/frontend_1/editor2/110617_lei_22-11_de_17_junho-proteccao_dados_pessoais.pdf

República, D. d. (2017). Lei 7/17 de 16 Fevereiro - Protecção das Redes e Sistemas Informáticos. (I Série - N.º 27). Angola.

Santos, J. R., & Henriques, S. (2021). Inquérito por questionário: contributos de conceção e utilização em contextos educativos. Portugal: Universidade Aberta. Fonte: https://repositorioaberto.uab.pt/handle/10400.2/10696

Sêmola, M. (2014). Gestão da segurança da informação (Vol. 2). Rio de Janeiro: Elsevier Brasil.

Severino, P. J., & Araújo, F. G. (2016). Implementação De Uma Infraestrutura De Rede Abordando Vlans, Utilizando Pfsense No Roteamento. 1. UNIPAM.

Significados. (2011). Backup. Fonte: Significados: https://www.significados.com.br/backup/

Snort. (2022). Snort. Acesso em Abril de 2022, disponível em Snort: snort.org

Stallings, W. (2019). Criptografia e Segurança de Redes: Princípios e Práticas (8 ed.). Pearson.

Stallings, W., & Brown, L. (2017). Segurança de Computadores: PrincÍpios e Práticas. Rio de Janeiro: Elsevier.

Sunda, F. S. (2021). Implementação de medidas de Segurança na Rede de Computadores do ISCED-Huíla. TCC à obtenção do título de Engenheiro. Lubango: ISPI.

Tanenbaum, A., & Feamster, N. (2021). Redes de Computadores (6ª ed.). São Paulo: Bookman.

Tchimissi, E. (2018). Implementação de Medidas de Segurança e Desempenho na Rede de Computadores do Instituto Superior de Ciências de Educação da Huíla. TCC de Licenciatura. Lubango: ISCED-HUÍLA.

Wikipédia. (2023). Engenharia social (segurança). Acesso em 26 de Janeiro de 2023, disponível em Wikipédia: pt.wikipedia.org/wiki/Engenharia_social_(segurança)

Williams, L. (2023). What is VLAN? Types, Advantages, Example. Fonte: Guru99: https://www.guru99.com/vlan-definition-types-advantages.html#10

Anexos

Anexo 1

Instituto Superior de Ciências de Educação da Huíla

Curso: Informática Educativa

Inquérito aos administradores da rede de computadores do Instituto Superior de Ciências de Educação da Huíla (ISCED-Huíla, Lubango).

Trabalho de Licenciatura a ser desenvolvido por Alcides Paulo Cassanga e Lino Carlos Mendonça Guelepete, estudantes do 4º ano do curso de Informática Educativa do ISCED HUÍLA, com o tema "**Melhoria da Segurança da Rede de Computadores no Instituto Superior de Ciências da Educação da Huíla".** Este inquérito tem como objectivo a recolha de informações, para diagnosticar medidas de segurança e desempenho na rede de computadores do ISCED-Huíla, e sugerir o melhoramento com implementação de mecanismos de segurança a utilizar.

Comprometemo-nos a respeitar o anonimato e a confidencialidade dos dados, apenas para estudos académicos, pelo que a identidade será sempre salvaguardada. Agradecemos a vossa colaboração.

Identificação do Inquirido

Função/Categoria_____

Questionário

A informação é o activo mais importante de uma instituição, e precisa ser protegida de maneira a assegurar a sua integridade, disponibilidade e confidencialidade.

Assinale com um X

1) **Por quais meios os utilizadores têm se conectado é rede de computadores do ISCED-Huíla?**
   a) Wi-fi ☐
   b) Cabos de rede ☐
   c) Wi-fi e cabos de rede ☐

2) **Quais são as reclamações constantes que os utilizadores da rede têm apresentado na utilização da mesma?**
   a) Queda constante da rede ☐
   b) Invasões por sites inadequados ☐
   c) Lentidão. ☐

3) **Já alguma vez a instituição sofreu algum ataque cibernético?**
   a) Sim ☐
   b) Não ☐

4) **Em quais aspectos achas que a rede do ISCED Huíla precisar melhor na segurança?**
   a) Controle de acesso ☐
   b) Segurança na web ☐
   c) Prevenção de perda de dados ☐

5) **Tem havido extravio de equipamentos na instituição?**
   a) Sim ☐
   b) Não ☐

6) **Acha viável a utilização de camaras de vigilância para monitorar a instituição?**

a) Sim ☐

b) Não ☐

Muito obrigado!

Anexo 2

Instituto Superior de Ciências de Educação da Huíla

Curso: Informática Educativa

Inquérito aos Funcionários Administrativos do Instituto Superior de Ciências de Educação da Huíla (ISCED-Huíla, Lubango).

Trabalho de Licenciatura a ser desenvolvido por Alcides Paulo Cassanga e Lino Carlos Mendonça Guelepete, estudantes do 4º ano do curso de Informática Educativa do ISCED HUÍLA, com o tema "**Melhoria da Segurança da Rede de Computadores no Instituto Superior de Ciências da Educação da Huíla".** Este inquérito tem como objectivo a recolha de informações, para diagnosticar medidas de segurança e desempenho na rede de computadores do ISCED-Huíla, e sugerir o melhoramento com implementação de mecanismos de segurança a utilizar.

Comprometemo-nos a respeitar o anonimato e a confidencialidade dos dados, apenas para estudos académicos, pelo que a identidade será sempre salvaguardada. Agradecemos a vossa colaboração.

Identificação do Inquirido

Função/Categoria_____

Questionário

A informação é o activo mais importante de uma instituição, e precisa ser protegida de maneira a assegurar a sua integridade, disponibilidade e confidencialidade.

Assinale com um X

1) **Em que medida está satisfeito com as condições de segurança e desempenho da rede de computadores do ISCED-HUILA?**
   a) Muito satisfeito ☐
   b) Satisfeito ☐
   c) Pouco satisfeito ☐
   d) Pouco satisfeito ☐

2) **Actualmente consegues aceder facilmente rede do ISCED-HUÍLA??**
   a) Não ☐
   b) Sim ☐

3) **Como classifica o desempenho da rede em relação as suas actividades?**
   a) Não atende as minhas necessidades ☐
   b) Atende parcialmente as minhas necessidades ☐
   c) Atende completamente as minhas necessidades ☐

4) **Actualmente consegue aceder a sites indevidos??**
   a) Sim ☐
   b) Não ☐

Muito obrigado!