

The logo for IPCA (Instituto Politécnico do Cávado e do Ave) features the letters 'IPCA' in a bold, white, sans-serif font. The 'I' is stylized with vertical bars of varying heights. The logo is set against a teal background that is part of a larger header bar.

**INSTITUTO POLITÉCNICO  
DO CÁVADO E DO AVE  
ESCOLA TÉCNICA  
SUPERIOR PROFISSIONAL**

**Instituto Politécnico do Cávado e do Ave  
Escola Superior de Tecnologia**

**Curso Técnico Superior  
em  
Redes e Segurança Informática**

**Relatório de estágio**

Diogo Miguel Vidal Andrade 16461

Esta página foi propositadamente deixada em branco.

The logo for IPCA (Instituto Politécnico do Cávado e do Ave) features the letters 'IPCA' in a bold, white, sans-serif font. The 'I' is stylized with vertical bars of varying heights. The logo is set against a dark gray square background.

**INSTITUTO POLITÉCNICO  
DO CÁVADO E DO AVE  
ESCOLA TÉCNICA  
SUPERIOR PROFISSIONAL**

**Instituto Politécnico do Cávado e do Ave  
Escola Superior de Tecnologia**

**Curso Técnico Superior  
em  
Rede e Segurança Informática**

**Relatório de Estágio**

Estágio realizado na empresa: Lucemplast, LDA

Diogo Miguel Vidal Andrade

Orientador do IPCA:

José Viamontes Martins

Supervisor da Entidade de Acolhimento:

Sérgio Machado

Esta página foi propositadamente deixada em branco.

## AGRADECIMENTOS

A finalização do presente feito, marca sem dúvida, um momento importante não só na minha vida profissional, mas também na minha vida pessoal. Ao fazer uma retrospectiva de todo o meu percurso de aprendizagem, não é possível preencher por palavras o sentimento de agradecimento que tenho por aqueles que me ajudaram e fizeram parte deste percurso.

Ao IPCA, desde o primeiro momento letivo. Foi marcado pela grande variedade de experiências, a nível educativo, profissional e formativo, adquirindo conhecimentos de excelência e qualidade.

Ao orientador deste estágio, Professor José Manuel Viamontes Martins pela motivação, dedicação, persistência e acompanhamento ao longo deste percurso. Um grande obrigado por me apoiar e acreditar nas minhas competências, fazendo-me acreditar também. Agradeço todos os conhecimentos transmitidos em todos os momentos de aprendizagem.

Ao colega de estágio, que partilhou comigo o estágio curricular. Agradeço pelas experiências e projetos conjuntos, pelo companheirismo e trabalho de equipa.

Aos colegas de curso, que partilharam parte desta caminhada comigo. Agradeço por todas as experiências vividas, amizades realizadas, aprendizagens, projetos em conjunto, por todo o companheirismo e pela partilha de várias opiniões.

Um agradecimento à entidade de acolhimento Lucemplast, Lda, pela boa vontade em formar e acolher um estagiário da minha área, aos seus colaboradores pela maneira como me receberam e trataram, nomeadamente ao supervisor Sérgio Machado pela simpatia e paciência em transmitir os seus conhecimentos e informações necessárias para as tarefas propostas.

Por fim, um obrigado a todos os meus amigos e família que estiveram sempre presentes em todos os momentos da minha vida académica, por todos os momentos que ainda não foram vividos e por toda a paciência que tiveram comigo.

A todos um enorme agradecimento por terem feito parte deste percurso.

## RESUMO

Este relatório é o resultado do estágio curricular e descreve todo o percurso que foi feito no estágio e as tarefas desenvolvidas neste período.

O estágio foi realizado na empresa Lucemplast, Lda, em Soutelo, no concelho de Vila Verde, de 3 de fevereiro a 14 de julho de 2020, com a duração de 840 horas e teve como principais objetivos a aquisição de conhecimentos na área de segurança informática e redes. Ao longo do estágio foram aplicados conhecimentos adquiridos no curso, que auxiliaram na execução das tarefas propostas. Com isto, o estágio curricular fortalece a tomada de iniciativa para a resolução de diversos problemas e tarefas que podem vir a ser feitas ao longo de qualquer percurso, fazendo com que conhecimentos teóricos passem à prática.

O tema deste projeto veio de encontro às necessidades da empresa, pois esta necessitava de um controlo informático maior dentro da própria empresa, conseguindo assim uma maior proteção em todos os aspetos tecnológicos.

O principal objetivo deste projeto é aplicar uma política de segurança à rede da empresa, fazendo com que o tráfego de rede seja filtrado pela firewall e haja um controlo total de acessos à rede. Desta forma é possível controlar os acessos de cada funcionário ou departamento à própria rede/internet, definindo as devidas permissões. Para tal, foi utilizado software Pfsense, um software livre adaptado para assumir o papel de uma firewall. É realizada a descrição desta implementação no presente relatório, detalhando tudo o que foi feito e todos os obstáculos ultrapassados. Antes da utilização deste software, houve tentativas de realizar o projeto em outro software, assim como tentar arranjar outro tipo de soluções para o que era pedido até chegar a um consenso. Foram utilizadas várias técnicas para o atendimento das necessidades da empresa, desde aplicações de controlo de tráfego dentro da própria Pfsense, a um servidor realizado no Windows server para poder simular diversas tarefas.

Finalmente, verificamos que a Pfsense era o software que mais satisfazia as condições necessárias para a realização do projeto.

**Palavras-chave:** Projeto, Software, Firewall, Segurança, Rede, Tráfego, Acessos.

# ABSTRACT

This report is the result of a curricular internship and describes the entire path that has been undertaken and all developed tasks therein.

The curricular internship was done in the company Lucemplast Lda, in Soutelo, in the county of Vila Verde, from February 3<sup>rd</sup> to July 7<sup>th</sup> 2020, with a duration of 840 hours and had as main goals the acquisition of knowledge in computer security and networks. Throughout the internship, knowledge that had been acquired during the course was applied and helped in the execution of the proposed tasks. As such, the curricular internship strengthened the initiative to solve diverse problems and the tasks that can be done in many ways, by making use of theoretical knowledge in practice.

The theme of this project arose company needs, as a greater informatics' control was needed, leading to greater protection in all technological aspects.

The main goal of this project is to apply a security policy to the company network, by filtering the network traffic through a firewall and having full network access control. In this way, it is possible to control the internet access by each worker or department, by defining permissions. For that, Pfsense software was used, a free open source software, adapted to assume the firewall job. The implementation is fully described in this report, detailing everything that has been done and all obstacles overcome. Before the use of this software, another software was used to try to do this project and trying to find other solutions for what was been proposed until a consensus has been reached. Many techniques were used for company needs, from network traffic control applications on the Pfsense, to a Windows server to simulate diverse techniques.

Finally, it was noted that Pfsense was the software that satisfied the necessary conditions to conclude the project.

**Keywords:** Project, Software, Firewall, Security, Network, Traffic, Accesses.

# LISTA DE ABREVIATURAS E SIGLAS

AD - Active Directory;

WS -Windows Server;

VM - Virtual Machine;

IP - Endereço de Protocolo da Internet;

LAN - Local Area Network;

WAN - Wide Area Networks;

GUI - Interface Gráfica;

LTS - Live Time Server;

VPN - Virtual Private Network;

TCP - Transmission Control Protocol;

UDP - User Datagram Protocol;

CIFS - Common Internet File System;

NAT - Network address translation;

ADDS - Active Directory Domain Service;

LDAP - Lightweight Directory Access Protocol;

CP - Captive Portal;

DHCP - Dynamic Host Configuration Protocol;

DNS - Domain Name System;

TLS - Transport Layer Security.



# ÍNDICE GERAL

AGRADECIMENTOS.....	v
RESUMO .....	vi
ABSTRACT.....	vii
LISTA DE ABREVIATURAS E SIGLAS .....	viii
ÍNDICE GERAL .....	ix
ÍNDICE DE FIGURAS.....	xii
INTRODUÇÃO .....	1
CAPÍTULO 1 – ORGANIZAÇÃO DA ENTIDADE DE ACOLHIMENTO DO ESTÁGIO CURRICULAR.....	3
1.1 ESTRUTURA DA ENTIDADE DE ACOLHIMENTO .....	3
1.1.1    MERCADO E CLIENTES .....	4
1.1.2    RESPONSABILIDADE AMBIENTAL.....	4
1.2 SERVIÇOS .....	4
1.2.1 ENGENHARIA DO PRODUTO .....	4
1.2.2 MOLDES/MOLDAÇÃO POR INJEÇÃO.....	4
1.2.3 PINTURA E REVESTIMENTO DA SUPERFÍCIE.....	5
1.2.4 MONTAGEM .....	5
1.2.5 LOGÍSTICA E METEOROLOGIA.....	5
1.3 COMPETÊNCIAS .....	6
1.3.1 GESTÃO DE PROJETOS.....	6
1.3.2 INOVAÇÃO E QUALIDADE.....	6
1.4 PLANEAMENTO DO ESTÁGIO CURRICULAR .....	7
1.5 ESTRUTURA INICIAL DA EMPRESA.....	8
CAPÍTULO 2- FUNÇÕES E TESTES DESEMPENHADOS .....	9
2.1 PRIMEIRAS TENTATIVAS/TESTES .....	9
2.1.1 UBUNTU.....	9
2.1.2 TESTES REALIZADOS COM O UBUNTU .....	10
2.2 PRIMEIRA INSTALAÇÃO DA PFSENSE .....	11
2.3 IPFIRE .....	11
2.3.1 PRINCIPAIS CARACTERÍSTICAS DO IPFIRE:.....	11
2.3.2 TESTES REALIZADOS COM O IPFIRE .....	12
2.3.3 ESTRUTURA DA REDE DO IPFIRE .....	13
2.3.4 O PORQUÊ DE SE TER ESCOLHIDO A PFSENSE.....	14
2.4 SAMBA .....	15
2.4.1 TESTES REALIZADOS COM O SAMBA .....	17

2.4.2 CONFIGURAÇÃO DA FIREWALL.....	17
2.4.3 CRIAÇÃO DE UTILIZADORES E DIRETÓRIOS.....	18
2.4.4 CONFIGURAÇÃO DOS FICHEIROS DE COMPARTILHAMENTO SAMBA .....	20
2.4.5 CONEXÃO AO COMPARTILHAMENTO DE FICHEIROS .....	21
2.4.5.1 LINHA DE COMANDOS .....	21
2.4.5.2 INTERFACE GRÁFICA.....	22
2.4.6 CONEXÃO AO COMPARTILHAMENTO SAMBA PELO WINDOWS .....	24
2.4.7 VANTAGENS E DESVANTAGENS .....	25
2.5 NOVA IMPLEMENTAÇÃO DA PFSense E ESTRUTURA DO SERVIDOR.....	26
2.5.1 ESTRUTURA DE MÁQUINAS VIRTUAIS.....	26
2.5.2. BRIDGE .....	26
2.5.3 NAT .....	27
2.5.4 INTERNAL NETWORK .....	28
2.5.5 HOST ONLY.....	28
2.6 WINDOWS SERVER.....	29
2.6.1 ESTRUTURA DO SERVIDOR .....	30
2.6.2 GRUPOS/UTILIZADORES .....	32
2.7 ACTIVE DIRECTORY .....	33
2.7.1 LDAP.....	34
2.7.2 RADIUS .....	35
2.7.3 LDAP VS RADIUS .....	36
2.8 PFSense .....	37
2.8.1 ESQUEMA DE REDE .....	37
2.8.2 CONSOLA E AMBIENTE GRÁFICO .....	38
2.8.3 PROXY .....	39
2.8.4 FUNÇÕES DO PROXY.....	39
2.8.5 CACHE .....	40
2.8.6 PROXY REVERSO .....	40
2.8.7 SQUID PROXY SERVER .....	41
2.8.8 ESQUEMA DO PROXY E DOS DIFERENTES GRUPOS COM ACESSOS À REDE.....	42
2.8.9 CONFIGURAÇÃO REALIZADA .....	44
2.9 CAPTIVEPORTAL .....	50
2.9.1 VANTAGENS E DESVANTAGENS .....	51
2.9.2 CONFIGURAÇÃO DO CAPTIVE PORTAL NA PFSense.....	52
2.9.2.1 ESQUEMA DO CAPTIVE PORTAL.....	52

2.9.3 TESTES REALIZADOS COM O CAPTIVE PORTAL.....	53
2.10 MONITORIZAÇÃO .....	59
2.10.1 SNORT .....	60
2.10.2 SURICATA .....	60
2.11 VPNS .....	61
2.11.1 ALGUNS EXEMPLOS DE VPNS NO MERCADO.....	63
2.11.2 TIPOS DE VPN.....	63
2.11.2.1 OPEN VPN: .....	63
2.11.2.2 VANTAGENS E DESVANTAGENS DO OPENVPN .....	64
2.11.2.3 PPTP: .....	64
2.11.2.4 VANTAGENS E DESVANTAGENS DO PPTP.....	64
2.11.2.5 L2TP/IPSEC:.....	65
2.11.2.6 VANTAGENS E DESVANTAGENS DO L2TP/IPSEC .....	65
2.11.3 TESTES REALIZADOS COM VPN .....	66
2.11.3.1 VPNS PARA UTILIZADOR LOCAIS.....	66
2.11.3.2 VPN PARA UTILIZADORES DO AD .....	76
2.11.4 ESQUEMA DE REDE DA VPN .....	82
2.12 ENDLESS OS .....	83
2.12.1 UTILIZAÇÃO DESTA DISTRIBUIÇÃO .....	84
2.12.2 VANTAGENS E DESVANTAGENS.....	84
CAPÍTULO 3 OUTRAS TAREFAS DESEMPENHADAS .....	87
3.1 SOFTWARE DE GESTÃO E MANUTENÇÃO .....	87
3.2 PRINCIPAIS FUNCIONALIDADES:.....	87
3.3 TAREFAS DESEMPENHADAS .....	88
PANDEMIA .....	89
CONCLUSÃO.....	90
REFERÊNCIAS.....	91
ANEXOS .....	94

# ÍNDICE DE FIGURAS

Figura 1- Logotipo da empresa.....	3
Figura 2- Esquema de rede inicial da empresa.....	8
Figura 3- Interface Web do IPFire .....	12
Figura 4- Consola do IPFIRE .....	12
Figura 5- Esquema de Rede do Ipfire .....	13
Figura 6- Verificação da ativação do samba .....	17
Figura 7- Rede local do ficheiro de configuração.....	18
Figura 8-Inserir a conta engenharia na base de dados do samba .....	19
Figura 9- Configuração dos utilizadores no ficheiro smb.conf .....	20
Figura 10- Instalar o smbclient.....	21
Figura 11- Aceder ao diretório na consola pelo ip do servidor com o utilizador em questão .....	22
Figura 12- Montar o compartilhamento engenharia .....	22
Figura 13- Aceder ao diretório do servidor ao adicionar uma nova localização de rede no ubuntu .....	22
Figura 14- Credencias da conexão .....	23
Figura 15-Pasta prints criada no diretório do servidor.....	23
Figura 16- Ligação ao servidor ubuntu por um utilizador windows .....	24
Figura 17- Credencias do utilizador ao efetuar a ligação pelo Windows a uma nova rede.....	24
Figura 18- Verificação da pasta prints após a conexão ao servidor .....	25
Figura 19- Estrutura das máquinas virtuais .....	26
Figura 20- Esquema de uma rede Bridge.....	27
Figura 21- Esquema de uma rede NAT .....	27
Figura 22- Esquema de uma rede Interna.....	28
Figura 23- Esquema de uma rede Host Only .....	29
Figura 24- Estrutura do servidor.....	30
Figura 25- DHCP e DNS do Servidor.....	30
Figura 26- Configuração de rede do Servidor .....	31
Figura 27-Ferramentas instaladas no servidor.....	31
Figura 28- Primeira Configuração dos grupos e dos utilizadores no servidor.....	32
Figura 29- Configuração dos Novos Grupos com Acesso e sem acesso.....	33
Figura 30- Esquema de rede da Firewall.....	37
Figura 31- Consola da Pfsense .....	38
Figura 32- Ambiente gráfico da Pfsense e credenciais do utilizador .....	38
Figura 33- Esquema do proxy reverso.....	40
Figura 34- Esquema do proxy e dos grupos definidos .....	42
Figura 35- Configuração da autenticação do proxy na Pfsense .....	44
Figura 36- Configuração da Autenticação do proxy na Pfsense 2 .....	45
Figura 37- Configuração do squid proxy .....	45
Figura 38- Configuração do SquidGuard .....	46
Figura 39- Blacklist .....	46
Figura 40-Download da Blacklist.....	47
Figura 41-Configuração da acl do grupo negado.....	47
Figura 42- Configuração da acl do grupo negado 2 .....	48
Figura 43- Configuração da acl do grupo permitido.....	48
Figura 44- Configuração da acl do grupo permitido 2 .....	49

Figura 45- Rede local do Servidor.....	49
Figura 46- Acesso permitido .....	50
Figura 47- Esquema do Captive Portal .....	52
Figura 48- Interface Guest .....	53
Figura 49- CA e certificado do CaptivePortal .....	53
Figura 50-Host definido no DNS.....	54
Figura 51- Configuração do Captive Portal .....	54
Figura 52- Configuração do Captive Portal 2 .....	55
Figura 53- Configuração da Autenticação do Captive Portal .....	56
Figura 54- Configuração do https login .....	56
Figura 55- Vouchers .....	57
Figura 56- Lista dos códigos do voucher .....	57
Figura 57- Rede do Cliente Ubuntu.....	58
Figura 58- Login no Captive Portal.....	58
Figura 59- Status dos utilizadores conectados ao Captive Portal .....	59
Figura 60- Ca da VPN por utilizadores locais.....	66
Figura 61- Certificado da VPN para utilizadores Locais .....	67
Figura 62- Atributo do Certificado.....	67
Figura 63- Configuração do tipo de servidor da VPN Local .....	68
Figura 64- Adicionar o CA á VPN local .....	68
Figura 65- Adicionar o certificado à VPN Local.....	69
Figura 66- Configuração da VPN Local .....	69
Figura 67- - Continuação da configuração da VPN Local .....	70
Figura 68- Definição da rede local da VPN e da rede do Túnel .....	71
Figura 69- Configuração do DNS e do Domínio.....	72
Figura 70- Regras de Firewall estabelecidas pela VPN .....	72
Figura 71- Criação do Utilizador VPN na firewall.....	73
Figura 72- Definir o certificado do utilizador Local.....	73
Figura 73- Download do ficheiro de configuração da VPN Local .....	74
Figura 74- Login do utilizador Local .....	74
Figura 75- Conexão da VPN local estabelecida.....	75
Figura 76- Ipconfig do cliente para verificar que a rede VPN está conectada .....	75
Figura 77- Utilizador VPNTeste no AD .....	76
Figura 78- Autenticação do servidor à firewall para manutenção de utilizadores .....	77
Figura 79- Continuação da Autenticação do servidor à firewall para manutenção de utilizadores.....	78
Figura 80- Configuração da VPN para utilizadores do AD da Pfsense.....	79
Figura 81- Continuação da configuração da VPN para utilizadores do AD da Pfsense.....	79
Figura 82- Firewall Rules da Wan para permitir o acesso remoto dos utilizadores da VPN .....	80
Figura 83- Download da ferramenta de instalação da VPN.....	80
Figura 84- Login do utilizador na VPN pelo AD.....	81
Figura 85- Conexão estabelecida da VPN pelo AD.....	81
Figura 86- Verificação da conexão VPN na Pfsense.....	81
Figura 87- Esquema de Rede da VPN.....	82
Figura 88- Ativos criados no ValueKeep.....	88

# INTRODUÇÃO

Foram realizadas diversas tentativas em procura da melhor solução para as necessidades da empresa, como não queríamos passar isso em vão, irão ser abordados todos os testes realizados de forma a explicar as opções tomadas e os métodos abordados. Tal como foi dito, optamos que a Pfsense seria a melhor opção para a realização do projeto.

A Pfsense tal como foi dito anteriormente é uma ferramenta de software livre adaptada para assumir o papel de uma firewall.

Uma firewall age como uma parede, impedindo ou bloqueando o acesso a pessoas não autorizadas, também tem a capacidade de controlar todo o tráfego da rede. Existem várias vantagens em implementar este sistema de segurança.

Uma grande vantagem nestes sistemas de software livre é o custo, pois chega a ser mesmo inexistente, podendo tirar partido de praticamente todo o software sem fazer qualquer tipo de pagamento.

Desta forma, o nosso projeto visa conhecer de um modo geral, as capacidades da Pfsense e para que esta pode ser útil a nível profissional.

Neste trabalho de projeto final, é detalhado todo o caminho realizado, desde implementação de um servidor Windows, a divisão de uma rede, a pastas compartilhadas em Linux para a realização de testes entre os utilizadores criados somente para isso, sendo a segurança o foco principal.

Assim, primeiramente é relatado tudo o que é relevante e realizado nas tarefas diárias, sendo apresentados vários objetos distintos, assim como todas as tentativas até chegar ao que achamos ser a melhor opção e ao planeamento do projeto.

Esta página foi propositadamente deixada em branco.

# **CAPÍTULO 1 – ORGANIZAÇÃO DA ENTIDADE DE ACOLHIMENTO DO ESTÁGIO CURRICULAR**

## **1.1 ESTRUTURA DA ENTIDADE DE ACOLHIMENTO**

O presente estágio foi realizado na empresa Lucemplast, Lda, situada na Av. Porto Carreiro 4730-575 Soutelo, Vila Verde, Portugal.

A Lucemplast é o resultado da experiência de 20 anos da sua equipe de gestão técnico-comercial, nomeadamente no mercado de componentes de plástico para indústrias Automóvel, Médica, Elétrico, Eletrónico e de Embalagem.

Esta entidade tem como missão fornecer componentes e serviços de valor acrescentado, excedendo as expectativas dos clientes. Criar valor para os acionistas e colaboradores tendo sempre como objetivo de todos o crescimento sustentado da LUCEMPLAST.

A mesma empresa tem como um dos objetivos a responsabilidade ambiental, aplicando novos métodos produtivos na indústria permitindo reciclar mais de 90% de todos os desperdícios no processo produtivo e reduzir o consumo energético em 30%.

Nesse sentido, a Lucemplast tem preocupação em reduzir emissões de gases de efeito de estufa mediante:

- Desenvolvimento de produtos que ajudem a reduzir o consumo de energia
- Utilização de tecnologias inovadoras em processos de produção que mediante melhor aproveitamento de energia reduzem emissões. (Lucemplast, Empresa, 2020)



**Figura 1- Logotipo da empresa**



### **1.1.1 MERCADO E CLIENTES**

A Lucemplast estará sempre presente em mercados em que o valor acrescentado das suas capacidades seja fator de distinção. A experiência acumulada em mercados como a Indústria Automóvel, Elétrica, Eletrónica e Embalagem é disso prova.

(Lucemplast, Empresa, 2020)

### **1.1.2 RESPONSABILIDADE AMBIENTAL**

Novos métodos produtivos na indústria permitem-nos reciclar mais de 90% de todos os desperdícios no processo produtivo e reduzir o consumo energético em 30%.

A Responsabilidade Ambiental é um pilar muito importante na política da empresa. Nesse sentido, a Lucemplast tem preocupação em reduzir emissões de gases de efeito de estufa.

(Lucemplast, Empresa, 2020)

## **1.2 SERVIÇOS**

### **1.2.1 ENGENHARIA DO PRODUTO**

Com o objetivo de maximizar ganhos de produtividade e competitividade e introduzir o seu capital de conhecimentos nos componentes que produz.

É um serviço que proporciona ao cliente componentes mais fiáveis e competitivos.

A experiência da equipe da Lucemplast na conceção de moldes, moldação por injeção, montagem e tratamentos de superfície é o garante do cumprimento das especificações técnicas do produto. (Lucemplast, Serviços, 2020)

### **1.2.2 MOLDES/MOLDAÇÃO POR INJEÇÃO**

A LUCEMPLAST abrange um range de máquinas até às 500 toneladas. A aposta em máquinas elétricas é um fator diferenciador perante a concorrência. A LUCEMPLAST está no mercado com equipamento que garante a precisão e repetibilidade nos componentes. As características dimensionais e óticas são garantidas pela tecnologia de ponta das máquinas elétricas

A nossa experiência nas máquinas hidráulicas e híbridas leva-nos a apostar nas máquinas 100% elétricas. (Lucemplast, Serviços, 2020)

### **1.2.3 PINTURA E REVESTIMENTO DA SUPERFÍCIE**

A Lucemplast conta com um parceiro em regime de exclusividade, para fornecer aos clientes pintura com proteção UV e proteção a laser. (Lucemplast, Serviços, 2020)

### **1.2.4 MONTAGEM**

Cada projeto com montagem de peças é sempre analisado e desenvolvido um conceito de montagem que garanta a qualidade e fiabilidade pretendidas.

Este conceito obedece a uma criteriosa escolha de métodos e tecnologias, que poderão conter verificações ao componente ou a cada um dos seus elementos este facto será sempre objeto de análise com o cliente. (Lucemplast, Serviços, 2020)

### **1.2.5 LOGÍSTICA E METEOROLOGIA**

Os sistemas logísticos dedicados a cada mercado são selecionados caso a caso.

As entregas de componentes just-in-time nos clientes ou em plataformas logísticas são conceitos utilizados.

A ISO série 9000 define explicitamente a relação entre garantia da qualidade e metrologia, estabelecendo diretrizes para se manter um controle sobre os instrumentos de medição da empresa.

O fator “globalização dos mercados” também põe em prática um de seus principais objetivos, que é traduzir a confiabilidade nos sistemas de medição e garantir que especificações técnicas, regulamentos e normas existentes, proporcionem as mesmas condições de perfeita aceitabilidade na montagem e encaixe de partes de produtos finais, independente de onde sejam produzidas. (Lucemplast, Serviços, 2020)

## **1.3 COMPETÊNCIAS**

### **1.3.1 GESTÃO DE PROJETOS**

O sucesso de um projeto é baseado na experiência do Gestor de Projeto, sociabilidade com os intervenientes e uma liderança clara. Na Lucemplast o gestor de projeto é o responsável pelo fluxo de informação de e para o cliente e fornecedores, garantindo uma clara e objetiva comunicação.

A capacidade de comunicar em várias línguas como o Alemão, Francês, inglês e Português garante uma posição de destaque no mercado Europeu de componentes plásticos.

As novas tecnologias como FTP-Server ou WEB meetings são utilizadas no dia-a-dia da conceção à produção em massa (Lucemplast, Competências, 2020)

### **1.3.2 INOVAÇÃO E QUALIDADE**

A LUCEMPLAST oferece um vasto leque de conhecimentos para suportar todas as fases de desenvolvimento de produto desde Design, Processos e Produção. A constante busca de conhecimento e formação dos colaboradores é um dos pilares para garantir estar na linha da frente da indústria de componentes técnicos. (Lucemplast, Competências, 2020)

## **1.4 PLANEAMENTO DO ESTÁGIO CURRICULAR**

No início do estágio foi efetuada uma apresentação dos colaboradores e a forma como a entidade se organiza, os respetivos departamentos e o que cada setor faz.

Feitas as apresentações, é realizada uma reunião com a minha presença, o supervisor Sérgio Machado, o Orientador José Martins e o colega de estágio Luís.

Com esta reunião foram definidas as atividades a desenvolver ao longo do estágio curricular, desde atividades que podem suceder no dia a dia, assim como o projeto que se pretende realizar.

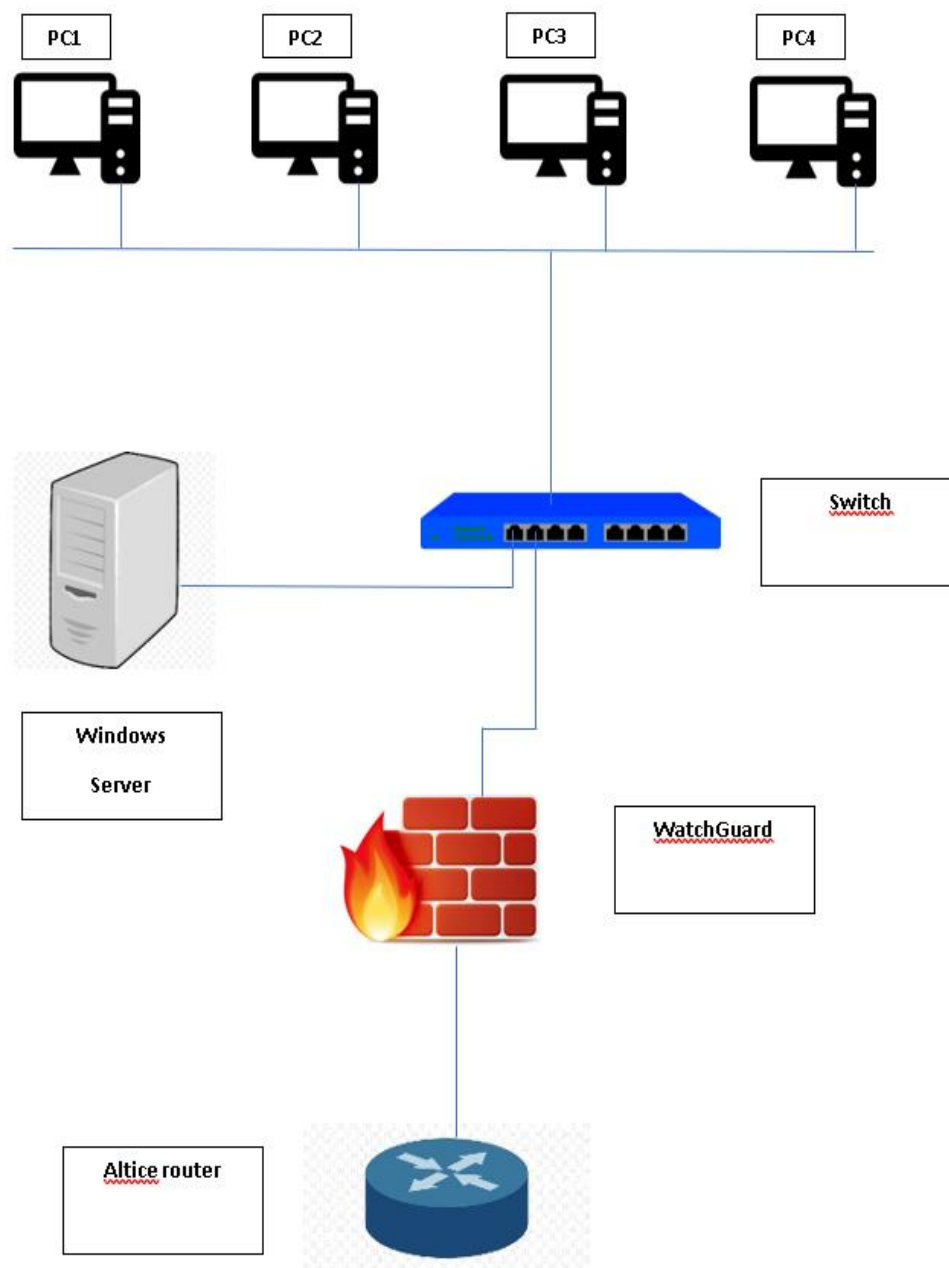
O seguinte projeto tem o objetivo de implementar uma firewall para controlar o tráfego de rede e os acessos dos colaboradores à própria rede.

São definidas as ideias que se pretendem e a própria estrutura de projeto.

É também abordada, a criação de duas VPN's, capazes de conectar o cliente através de casa ao seu posto de trabalho.

O tráfego externo também é preciso ter em atenção, por isso foi pedido que clientes visitantes se conectem a uma rede diferente da dos colaboradores, com um sistema de login efetuado na internet.

## 1.5 ESTRUTURA INICIAL DA EMPRESA



**Figura 2- Esquema de rede inicial da empresa**

Esta Figura 2 retrata a estrutura de rede da empresa, onde a rede que vem do altice router é filtrada pela WatchGuard, que por sua vez está ligada a um switch que faz ligação com o servidor e com os respetivos utilizadores.

# **CAPÍTULO 2- FUNÇÕES E TESTES DESEMPENHADOS**

## **2.1 PRIMEIRAS TENTATIVAS/TESTES**

### **2.1.1 UBUNTU**

O Ubuntu é uma distribuição linux, um sistema operativo open source. Pode ser utilizado tanto para uso pessoal, como para servidor, o ubuntu server.

Acaba por ser um sistema operativo bem intuitivo para qualquer pessoa, e isento de qualquer pagamento. (Perens, 2020)

O Ubuntu é construído sobre a arquitetura Debian, outro sistema operativo de software livre, tendo versões de cada sistema operativo para diferentes dispositivos. Este sistema lança updates de 6 em 6 meses, e cada e cada lançamento recebe suporte gratuito por nove meses com todo o tipo de correções que são necessárias fazer, como correções de segurança, bugs, etc.

O primeiro lançamento foi em 2004. Em 8 de julho de 2005, Mark Shuttleworth e a Canonical Ltd anunciaram a criação da Ubuntu Foundation. A finalidade da fundação é garantir apoio e desenvolvimento a todas as versões posteriores.

Em 12 de março de 2009, o Ubuntu anunciou o suporte de desenvolvedores para plataformas de gerenciamento de nuvem de terceiros.

Desde o Ubuntu 17.10, o GNOME 3 é a GUI padrão do Ubuntu Desktop, enquanto o Unity ainda é o padrão em versões mais antigas, incluindo todas as versões atuais do LTS. A versão Ubuntu GNOME foi descontinuada após a versão padrão adotar este ambiente de desktop e os esforços de desenvolvimento foram combinados.

## **2.1.2 TESTES REALIZADOS COM O UBUNTU**

Primeiramente, como recebemos um computador em que a formatação do mesmo era necessária, assim como a instalação de um sistema operativo na mesma, foi optado por instalar o Ubuntu por diferentes razões, tal como o facto de ser um sistema gratuito e de já ter sido usado em ambiente escolar.

Feita a instalação do sistema operativo, começamos a pesquisar como desenvolver o projeto e o que era necessário para a criação do mesmo.

Rapidamente foi chegado à conclusão de que, para uma fase inicial de testes não valia a pena ter instalado o Ubuntu na máquina, porque era necessário simular um ambiente completo de rede, assim como toda a sua estrutura por detrás.

Com isto, foi instalado uma versão windows10 na máquina para podermos simular o projeto num ambiente virtual.

Posteriormente em ambiente virtual foi instalado uma máquina ubuntu onde fizemos diversos testes.

Maioritariamente o uso deste sistema operativo foi para testes de conexão para com o sistema Windows, tendo em conta que muitas das máquinas na empresa têm sistema operativo Linux.

## **2.2 PRIMEIRA INSTALAÇÃO DA PFSense**

Houve inicialmente uma instalação da Pfsense, onde foi definida uma estrutura de rede e desenvolvido algum trabalho de investigação. Como a estrutura final ainda não estava definida e pelo facto de a configuração da Pfsense ser um bocado complexa, estudou-se outras possibilidades, nomeadamente o IpFire.

## **2.3 IPFIRE**

É uma distribuição linux que funciona como uma firewall dedicada com a capacidade de fazer de router, tendo um sistema de configuração web e consola.

Inicialmente foi desenvolvido sobre o IPCOP, outro sistema idêntico, em que engenheiros ou desenvolvedores de software pegaram na fonte desse código e desenvolveram o Ipfire por cima desse código, fazendo alterações e começando a desenvolver o IpFire.

Esta distribuição tem múltiplas opções de configuração na interface web, permite implementar facilmente serviços de firewall, proxy, file server, VPN e outros serviços de rede capazes de satisfazer as necessidades do utilizador.

O IPFire pode ser instalado numa máquina ou executado a partir de um CD, ou dispositivo de armazenamento USB.

É direccionado para redes de dados de empresas ou para redes domésticas. (Pinto, 2020)

### **2.3.1 PRINCIPAIS CARACTERÍSTICAS DO IPFIRE:**

- Serviços de Firewall;
- Serviços de Web Proxy;
- Serviços de VPN;
- Pode funcionar como Sistema de Detecção de Intrusão;
- Integração com redes wireless; (Pinto, 2020)



### 2.3.2 TESTES REALIZADOS COM O IPFIRE

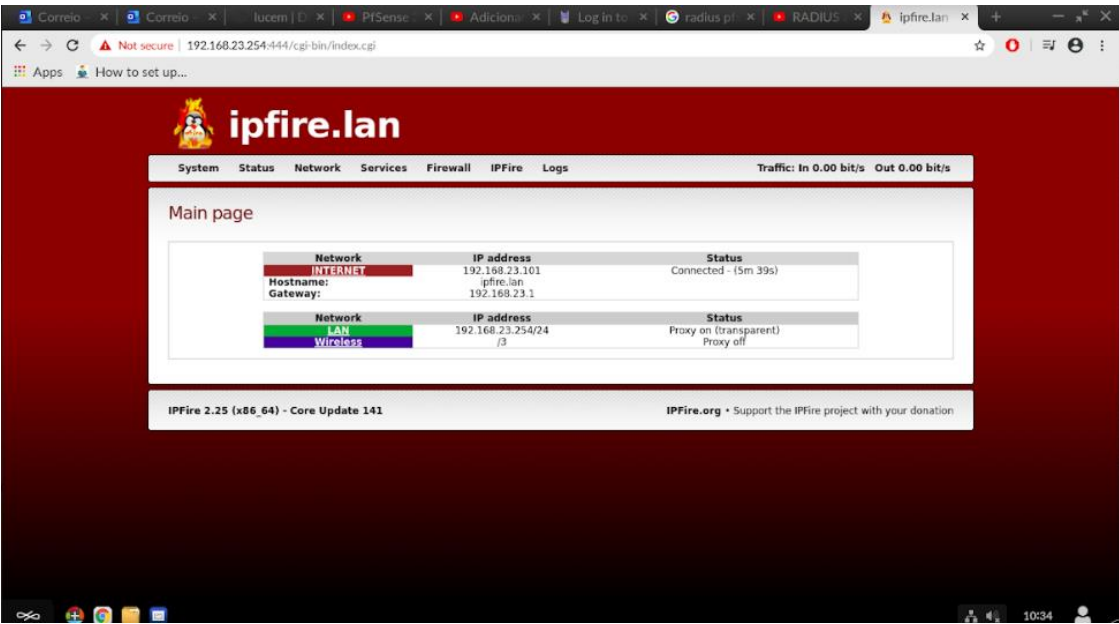


Figura 3- Interface Web do IPFire

Na figura 3, é possível verificar o ambiente gráfico do IPFIRE, onde está demonstrada a configuração da rede.

```
IPFire v2.25 - www.ipfire.org
=====
ipfire.lan running on Linux 4.14.154-ipfire x86_64
green0  Link encap:Ethernet HWaddr 08:00:27:BC:8B:A6
        inet addr:192.168.23.254 Bcast:192.168.23.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:3762 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3332 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:651824 (636.5 Kb) TX bytes:1649105 (1.5 Mb)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:4006 errors:0 dropped:0 overruns:0 frame:0
        TX packets:4006 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:220445 (215.2 Kb) TX bytes:220445 (215.2 Kb)

red0    Link encap:Ethernet HWaddr 08:00:27:66:FE:BB
        inet addr:192.168.23.101 Bcast:192.168.23.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MTU:1500 Metric:1
        RX packets:236 errors:0 dropped:0 overruns:0 frame:0
        TX packets:141 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:38712 (37.8 Kb) TX bytes:17524 (17.1 Kb)

root@ipfire ~]#
```

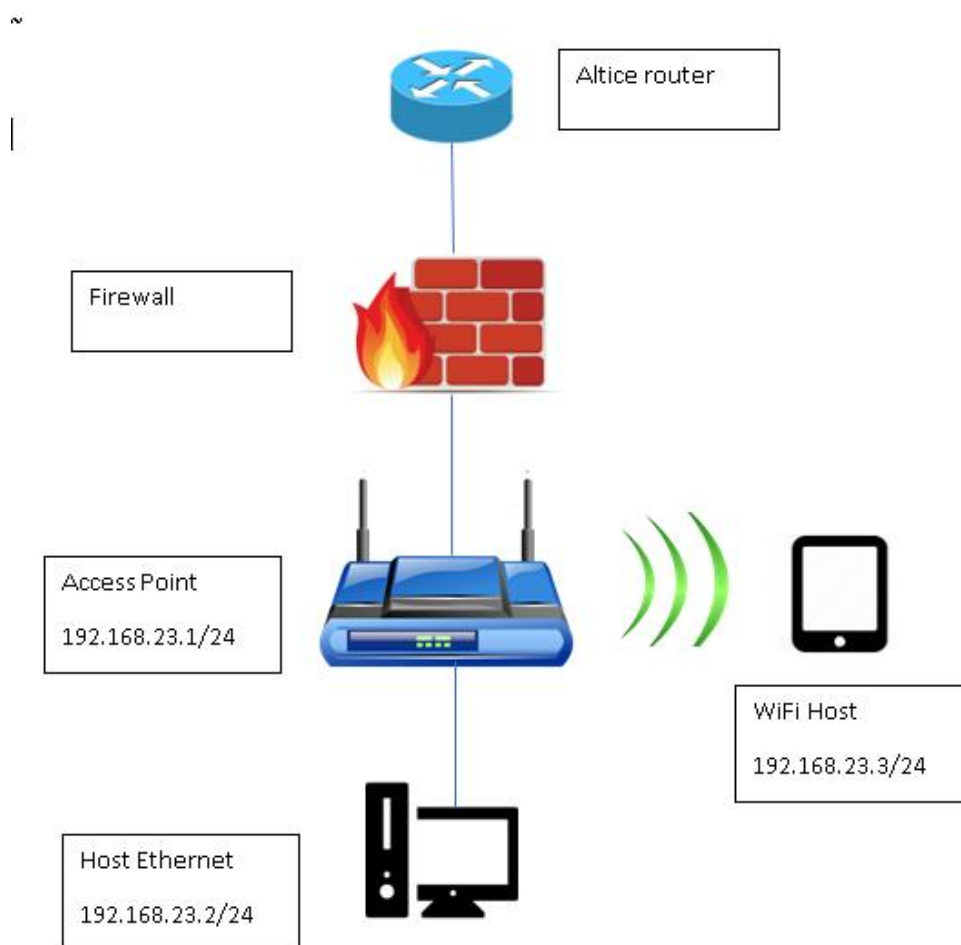
Figura 4- Consola do IPFIRE

Tal como se pode verificar na figura 4, foram definidas 3 placas, a green0 para a rede LAN com o ip 192.168.23.254, a lo como rede local 127.0.0.1 e a red0 como WAN com o ip 192.168.23.101, a servir de router para a LAN.

O ip da LAN foi definido dentro da mesma rede que a WAN para que fosse possível que todos os computadores comunicarem entre si.

Reforço que, a ideia de trabalhar com este tipo de firewall foi tentar criar um ambiente de servidor entre máquinas ubuntu e Windows. Surgiu com uma oportunidade para aprender conhecimentos e estudar novas hipóteses, uma vez que a escolha do software ainda não estava acertada.

### 2.3.3 ESTRUTURA DA REDE DO IPFIRE



**Figura 5- Esquema de Rede do Ipfire**

A Figura 5, representa como estava definido o laboratório de rede quando foi experimentado o IPFIRE. Esta Figura retrata que existe uma rede proveniente do router altice, que é filtrada por uma firewall, que neste caso é o IPFIRE, que está conectada a um access point com dois hosts conectados, com uma rede de 192.168.23.0/24. O IP do access point representa o gateway da rede.

## 2.3.4 O PORQUÊ DE SE TER ESCOLHIDO A PFSENSE

Estes dois sistemas têm os seus prós e contras, tendo os dois capacidade para executar a função principal da sua instalação, que é a segurança do utilizador.

Uma das grandes vantagens do IpFire é mesmo ser intuitivo e mais básico do que a Pfsense, tendo muito menos opções e um menu bastante mais fácil de manusear.

A segurança e a performance destes dois, é um fator relevante e positivo, tendo os dois capacidades de performance bastante semelhantes, a Pfsense acaba por reter relativamente mais memória em uso do que o IpFire, como têm os dois a capacidade de se instalar diferentes packages de segurança acabam por ser sistemas muito seguros.

Uma desvantagem do IpFire é o sistema de suporte, pois a Pfsense é bastante mais popular e tem um suporte de investigação e de fóruns bastante mais alargado do que o IpFire, por outro lado o IpFire tem uma Wikipédia própria com muita informação relevante para o utilizador.

A nível de ferramentas o sistema de pacotes da Pfsense também é mais alargado, permitindo mais opções de instalação de diversos pacotes.

A principal razão de se ter optado pela Pfsense para implementação final, foi pelo simples facto de achar que é uma plataforma mais complexa, mais bem constituída e acima de tudo mais profissional do que o Ipfire.

Como grande conclusão posso dizer que tudo depende do uso que o utilizador que dar, se o utilizador estiver à procura de uma solução que seja de fácil configuração e está numa fase inicial de aprendizagem, é recomendável a instalação do IpFire.

Por outro lado, se o utilizador procura uma solução mais profissional e mais complexa a Pfsense é a melhor opção. (Becher, 2020)

## 2.4 SAMBA

É um software grátis capaz de fornecer serviços de arquivo e impressão para várias plataformas, como diversas versões do Windows e Linux.

Pode ser integrado num servidor com um controlador de domínio ou mesmo um membro do domínio.

Este software suporta o Server Message Block (SMB) protocolo, com este protocolo o Samba permite que computadores corram o Unix, comunicando com o mesmo protocolo de rede que o Windows aparecendo na rede windows como perspectiva de cliente windows.

Um servidor Samba oferece os seguintes serviços:

- Compartilhar uma ou mais árvores de diretório;
- Compartilhar uma ou mais árvores do sistema de arquivos distribuídos;
- Compartilhar impressoras instaladas no servidor entre clientes Windows na rede;
- Ajudar os clientes na navegação na rede;
- Autenticar clientes que efetuam login em um domínio do Windows;
- Fornecer ou ajudar com a resolução do servidor de nomes do Windows Internet Name Service(WINS).

O Samba também inclui ferramentas que permitem aos utilizadores de um sistema Unix aceder pastas que os sistemas Windows e servidores Samba oferecem na rede.

Foi desenvolvido por Andrew Tridgell em 1991, usado inicialmente rastrear pacotes e analisar redes.

Apenas em 2003, o Samba ganhou a habilidade de se juntar a um active directory, embora como membro e não como controlador de domínio.

Em 2006 foi lançada a primeira tentativa de fazer com que o samba conseguisse ser um controlador de domínio, mas foi uma tentativa falhada.

A partir daqui foram adicionadas mudanças relativas a problemas de segurança, e diferentes tipos de suporte.

Em dezembro de 2012, o Samba passa a conseguir ser um controlador de domínio do Active directory, podendo participar totalmente num active directory windows.

Depois disto, foram lançados diversos updates com o objetivo de melhorar o software, seja a nível de desempenho ou suporte, estando atualmente na versão 4.12.

A implementação deste software, foi para adquirir novos conhecimentos e tentar criar um servidor de partilha de ficheiros entre um servidor ubuntu e uma máquina Windows.

## 2.4.1 TESTES REALIZADOS COM O SAMBA

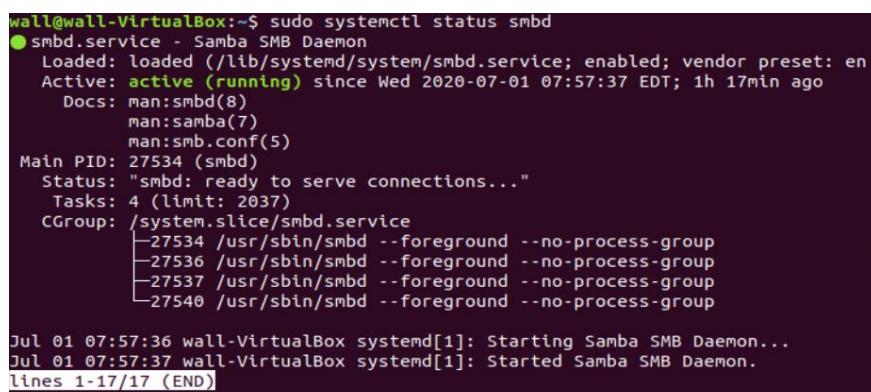
Depois de instaladas as máquinas virtuais, a ideia de utilizar este software passa por conseguir criar um servidor de partilha de ficheiros através de uma máquina Linux, em que um utilizador Windows consiga aceder a esse mesmo servidor.

Estando no terminal do Ubuntu a primeira coisa a fazer é digitar o comando de instalação do samba, com o comando “sudo apt install samba”.

Também é recomendado fazer updates à máquina antes de instalar o software.

Para fazer a atualizações basta digitar na consola sudo apt update e consequentemente sudo apt upgrade.

Feita a instalação da aplicação é possível verificar o estado do servidor, para ver se o mesmo está ativo, tal como indica a Figura 6.



```
wall@wall-VirtualBox:~$ sudo systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: en
   Active: active (running) since Wed 2020-07-01 07:57:37 EDT; 1h 17min ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
   Main PID: 27534 (smbd)
   Status: "smbd: ready to serve connections..."
     Tasks: 4 (limit: 2037)
    CGroup: /system.slice/smbd.service
            └─27534 /usr/sbin/smbd --foreground --no-process-group
              └─27536 /usr/sbin/smbd --foreground --no-process-group
                └─27537 /usr/sbin/smbd --foreground --no-process-group
                  └─27540 /usr/sbin/smbd --foreground --no-process-group

Jul 01 07:57:36 wall-VirtualBox systemd[1]: Starting Samba SMB Daemon...
Jul 01 07:57:37 wall-VirtualBox systemd[1]: Started Samba SMB Daemon.
lines 1-17/17 (END)
```

Figura 6- Verificação da ativação do samba

## 2.4.2 CONFIGURAÇÃO DA FIREWALL

Verificado o estado do servidor, é necessário abrir as portas tcp e udp.

Feito isto é necessário partir para o ficheiro de configuração do servidor, com o comando “sudo nano /etc/samba/smb.conf”. É importante verificar se o ficheiro está em standalone server, tal como mostra a Figura 7.

Como neste caso é necessário restringir o acesso ao servidor apenas à rede local é aplicado o seguinte comando.

```
#### Networking ####  
  
# The specific set of interfaces / networks to bind to  
# This can be either the interface name or an IP address/netmask;  
# interface names are normally preferred  
; interfaces = 127.0.0.0/8 eth0  
  
# Only bind to the named interfaces and/or networks; you must use the  
# 'interfaces' option above to use this.  
# It is recommended that you enable this feature if your Samba machine is  
# not protected by a firewall or is a firewall itself. However, this  
# option cannot handle dynamic or non-broadcast interfaces correctly.  
; bind interfaces only = yes
```

**Figura 7- Rede local do ficheiro de configuração**

Realizadas estas configurações é necessário reiniciar o servidor para serem aplicadas as alterações, para isso basta digitar “sudo systemctl restart smbd” e “sudo systemctl restart nmbd”.

Para melhor manutenção e flexibilidade é melhor criar um diretório onde vai ser guardado todo o tipo de configurações aplicadas, em vez de serem usados os diretórios padrão.

### **2.4.3 CRIAÇÃO DE UTILIZADORES E DIRETÓRIOS**

Foi criado um diretório denominado samba para poder ser feita a gestão dos utilizadores e dos respetivos grupos, com o comando “sudo mkdir /samba”.

Foi criado um grupo para controlar todos os utilizadores que vão ser inseridos no diretório samba, para efetuar a seguinte operação foi utilizado o comando “sudo chgrp samba share/samba”.

Com o grupo criado passa-se para a criação do utilizador que vai ter permissão para aceder à partilha de ficheiros e um utilizador admin que vai ficar responsável por todos os processos realizados no servidor.

Elaborados o diretório e o grupo, foi criado um utilizador, com o nome de engenharia dentro do diretório samba. Para a realização desta operação foi utilizado o comando “sudo useradd -M -d /samba/engenharia -s /usr/sbin/nologin -G sambashare engenharia”.

As letras descritas no comando representam o seguinte:

-M criar o diretório manualmente.

-d /samba/engenharia – define o diretório inicial do utilizador to /samba/engenharia.

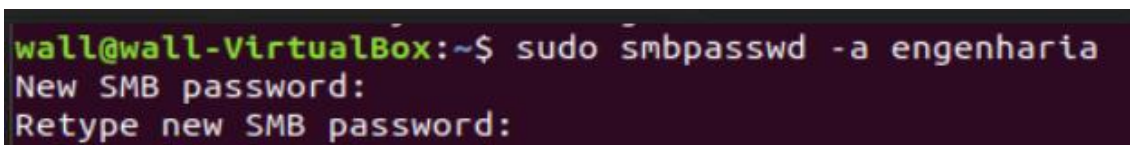
-s /usr/sbin/nologin – desativar o acesso ao Shell para este utilizador.

-G sambashare – adicionar um utilizador ao grupo sambashare.

Adicionado o utilizador, foi criado o diretório do próprio utilizador e inserido no grupo sambashare como administrador. O comando “sudo mkdir /samba/engenharia” é responsável por criadi o diretório, o comando “sudo chown engenharia:sambashare /samba/engenharia” é que ira passar o dono do diretório para o utilizador engenharia.

É necessário adicionar o bit setgid ao diretório /samba/engenharia, para que os arquivos recém-criados neste diretório herdem o grupo do diretório pai. Dessa forma, não importa qual utilizador crie um arquivo, o arquivo terá o proprietário do grupo de sambashare . Por exemplo, se o administrador que está a configurar não definir as permissões do diretório para 2770 e o utilizador sadmin criar um arquivo, o utilizador engenharia não poderá ler / gravar neste arquivo. O comando “sudo chmod 2770 /samba/engenharia” vai definir as permissões do diretório.

Seguidamente, é necessário inserir a conta do utilizador engenharia na base de dados Samba, configurando a senha do utilizador, como mostra a Figura 8.



```
wall@wall-VirtualBox:~$ sudo smbpasswd -a engenharia
New SMB password:
Retype new SMB password:
```

**Figura 8-Inserir a conta engenharia na base de dados do samba**

Definida a senha é necessário ativar a conta, “ sudo smbpasswd -e engenharia”, onde a letra “e” é responsável por ativar o utilizador.



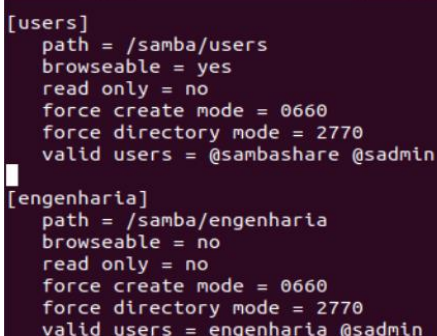
Criado o utilizador engenharia, é necessário criar um utilizador e um grupo com permissões de administração. Posteriormente qualquer utilizador que seja necessário se tornar administrador, basta adicionar o utilizador a este grupo. Para a seguinte tarefa foi inserido o comando “sudo useradd -M /samba/users -s /usr/sbin/nologin -G sambashare sadmin”

Realizada a criação do grupo e do utilizador de administração, é necessário definir uma palavra passe e ativar a conta, “sudo smbpasswd -a sadmin” e “sudo smbpasswd -e sadmin”. Feita a ativação da conta sadmin, foi criado o diretório de partilha denominado users.

Criado o diretório de utilizadores é necessário definir o administrador do diretório, que foi dado consequentemente ao utilizador sadmin ao grupo sambashare. Não só é necessário um administrador para o grupo assim como o tipo de permissões que outros utilizadores têm perante este diretório, logo foi definido as permissões de ler/escrever do grupo sambashare perante o diretório samba/users. O comando “sudo chown sadmin:sambashare /samba/users” é o que atribui o administrador do diretório, o comando “sudo chmod 2770 /samba/users” é o que defini os moderadores.

## 2.4.4 CONFIGURAÇÃO DOS FICHEIROS DE COMPARTILHAMENTO SAMBA

Diretamente no ficheiro de configuração é adicionado o utilizador assim como as suas permissões, tal como se pode verificar na Figura 9.



```
[users]
  path = /samba/users
  browseable = yes
  read only = no
  force create mode = 0660
  force directory mode = 2770
  valid users = @sambashare @sadmin

[engenharia]
  path = /samba/engenharia
  browseable = no
  read only = no
  force create mode = 0660
  force directory mode = 2770
  valid users = engenharia @sadmin
```

**Figura 9- Configuração dos utilizadores no ficheiro smb.conf**

As opções têm os seguintes significados:

-[Users e engenharia] - Os nomes dos partilhaamentos que vão ser usados para fazer login.

-Path - O caminho para o compartilhamento.

- Browseable - Se o compartilhamento deve ser listado na lista de compartilhamentos disponíveis. Ao definir para “no” outros utilizadores não conseguirão ver o compartilhamento.

-Read only - se os utilizadores especificados na lista de valid users podem gravar neste compartilhamento.

-Force create mode - Define as permissões para os arquivos recém-criados neste compartilhamento.

-Force directory mode - Define as permissões para os diretórios recém-criados neste compartilhamento.

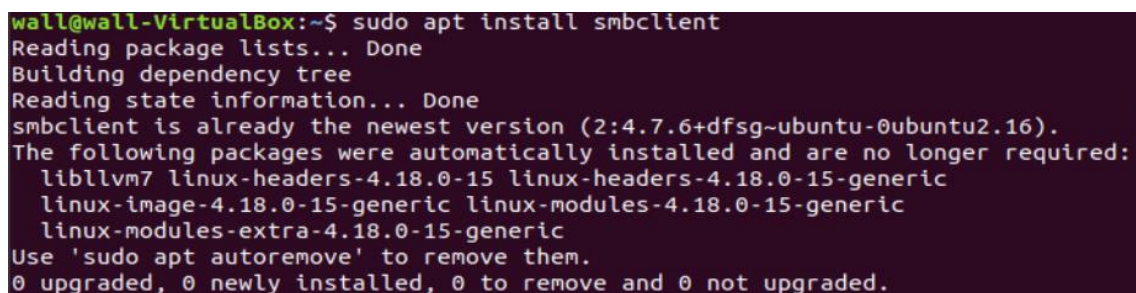
-Valid users - Uma lista de utilizadores e grupos que têm permissão para aceder o compartilhamento. Os grupos são prefixados com o símbolo @ .

Realizadas estas configurações o restart do servidor é essencial.

## 2.4.5 CONEXÃO AO COMPARTILHAMENTO DE FICHEIROS

### 2.4.5.1 LINHA DE COMANDOS

Os utilizadores Linux podem aceder ao samba share através da linha de comandos, utilizando o gestor de arquivos ou montar o compartilhamento Samba. Para permitir este acesso é necessário a instalação de uma ferramenta chamada “smbclient” , que faz com que seja possível aceder ao Samba pela linha de comandos, tal como mostra a Figura 10.



```
wall@wall-VirtualBox:~$ sudo apt install smbclient
Reading package lists... Done
Building dependency tree
Reading state information... Done
smbclient is already the newest version (2:4.7.6+dfsg~ubuntu-0ubuntu2.16).
The following packages were automatically installed and are no longer required:
  libllvm7 linux-headers-4.18.0-15 linux-headers-4.18.0-15-generic
  linux-image-4.18.0-15-generic linux-modules-4.18.0-15-generic
  linux-modules-extra-4.18.0-15-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

**Figura 10- Instalar o smbclient**

Feita a instalação da ferramenta, para aceder ao diretório basta digitar o ip definido e o utilizador. Inserido estes dados o utilizador está conectado à linha de comandos do servidor, tal como descreve a Figura 11.

```
wall@wall-VirtualBox:~$ smbclient //192.168.23.109/engenharia -U engenharia
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\engenharia's password:
Try "help" to get a list of possible commands.
smb: \>
```

**Figura 11- Aceder ao diretório na consola pelo ip do servidor com o utilizador em questão**

Outra maneira de conectar é através da montagem do compartilhamento Samba. Para isto é necessária uma ferramenta chamada cifs. Instalada a ferramenta é preciso criar o ponto de montagem, com o comando “sudo mkdir /mnt/smbmount”

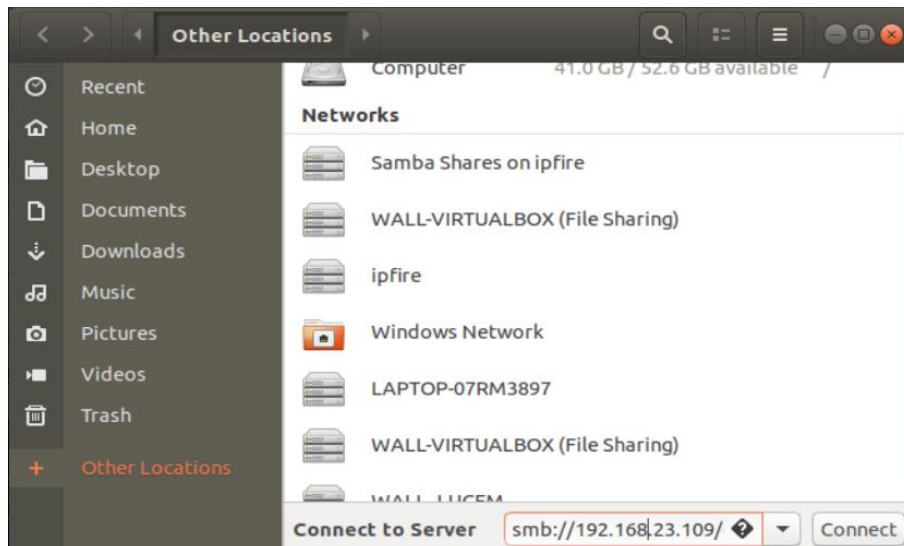
Criado o ponto de montagem, é montado o compartilhamento engenharia neste caso, é preciso inserir o ip definido, o utilizador e a password, tal como se verifica na Figura 12.

```
wall@wall-VirtualBox:~$ sudo mount -t cifs -o username=engenharia //192.168.23.109/engenharia /mnt/smbmount
Password for engenharia@//192.168.23.109/engenharia: *****
```

**Figura 12- Montar o compartilhamento engenharia**

## 2.4.5.2 INTERFACE GRÁFICA

Para aceder através da interface gráfica, fui aos ficheiros Linux, outras localizações e inseri o caminho do diretório do servidor, tal como demonstra a Figura 13.



**Figura 13- Aceder ao diretório do servidor ao adicionar uma nova localização de rede no ubuntu**

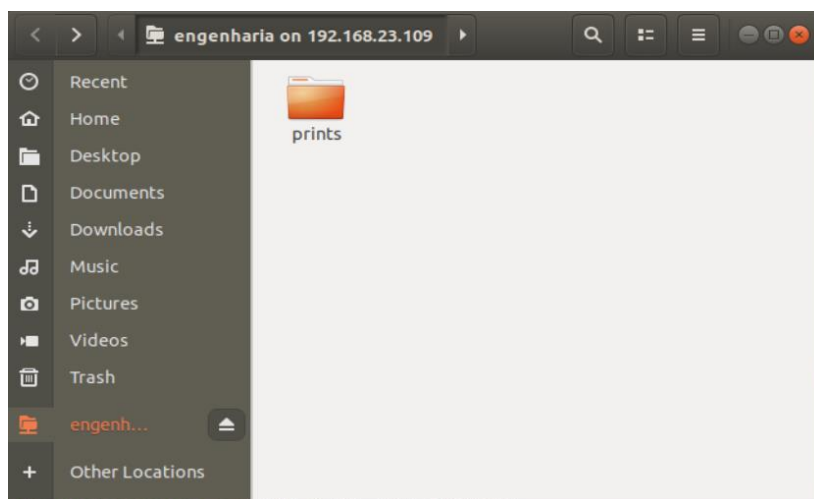
Seguidamente é pedido o utilizador e password, como se pode verificar na Figura 14.



**Figura 14- Credencias da conexão**

Depois de inserido o utilizador é possível aceder à partilha de ficheiros.

Neste caso foi criada uma pasta chamada prints apenas para testar e foram inseridas duas imagens, como se pode verificar na Figura 15.



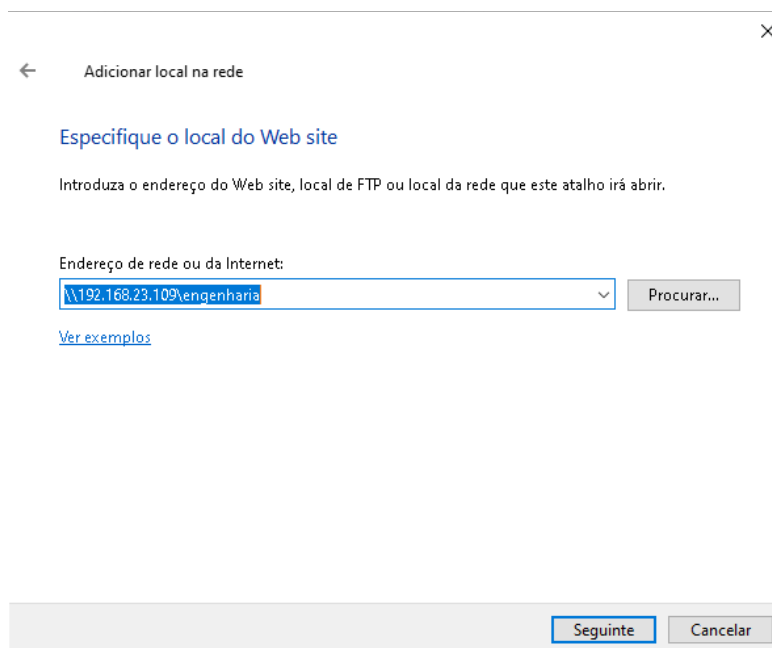
**Figura 15-Pasta prints criada no diretório do servidor**

Realizada esta configuração, foi testada a conexão ao servidor samba através um utilizador Windows.

## 2.4.6 CONEXÃO AO COMPARTILHAMENTO SAMBA PELO WINDOWS

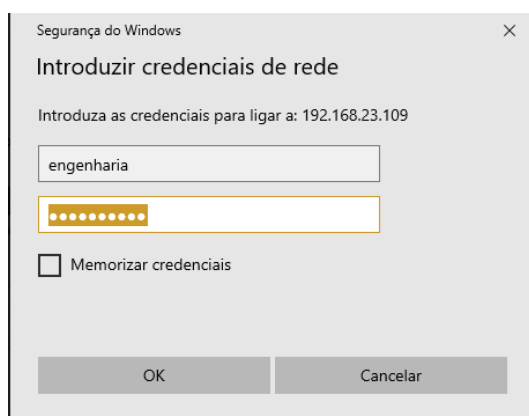
Qualquer utilizador windows consegue se conectar ao Samba, para isso basta ir ao “explorador de ficheiros”, “este computador”, clicar no lado direito do rato e escolher um “local de rede personalizado”.

Posto isto basta inserir o ip do servidor e o nome do diretório, como retrata a Figura 16.



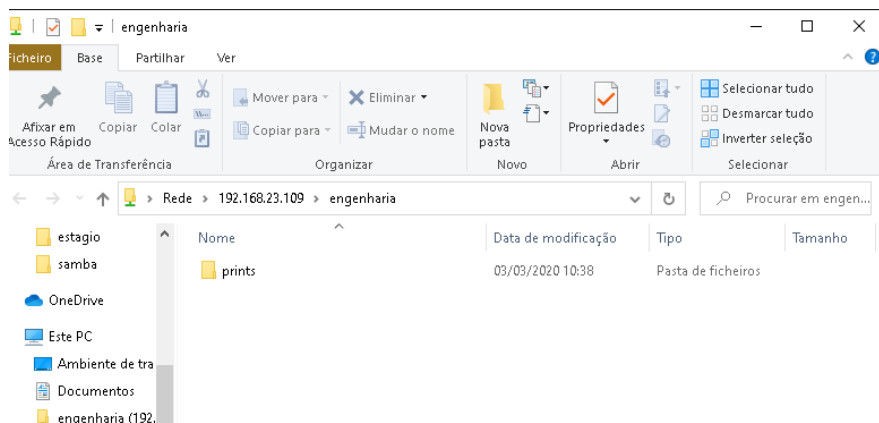
**Figura 16- Ligação ao servidor ubuntu por um utilizador windows**

Depois de clicar em seguinte, são pedidas as credenciais do utilizador, como mostra a Figura 17.



**Figura 17- Credencias do utilizador ao efetuar a ligação pelo Windows a uma nova rede**

Depois de conectado, é possível verificar através da Figura 18 que a mesma pasta prints está lá.



**Figura 18- Verificação da pasta prints após a conexão ao servidor**

## 2.4.7 VANTAGENS E DESVANTAGENS

A grande desvantagem deste software é a segurança, tendo já sido descobertos certos bugs e até mesmo algumas vulnerabilidades capazes de meter a segurança do utilizador em risco, assim como informações relevantes que estejam armazenadas.

Uma das vantagens é que permite que diferentes sistemas operativos consigam trocar ficheiros entre si.

Outras das vantagens é, se dois sistemas operativos estiveram interligados pelo samba e um deles ficar vulnerável a hackers, mas não quer dizer que o outro sistema fique vulnerável (rohitphulsunge, 2020).

A interface gráfica assim como a sua configuração é outro ponto negativo em relação ao Windows server, pois têm uma configuração muito menos intuitiva e uma interface gráfica muito menos complexa.

Claro que outro ponto a ter em conta é o facto de o Samba ser um software gratuito.

Não é compatível com todos os sistemas windows.

## 2.5 NOVA IMPLEMENTAÇÃO DA PFSENSE E ESTRUTURA DO SERVIDOR

### 2.5.1 ESTRUTURA DE MÁQUINAS VIRTUAIS

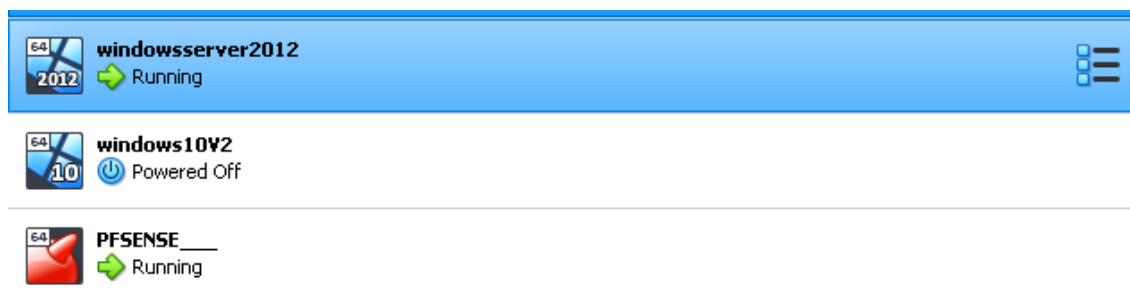


Figura 19- Estrutura das máquinas virtuais

Tal como é possível ver na Figura 19, foram criadas 3 máquinas virtuais, uma máquina Pfsense, uma para o servidor e outra para o cliente.

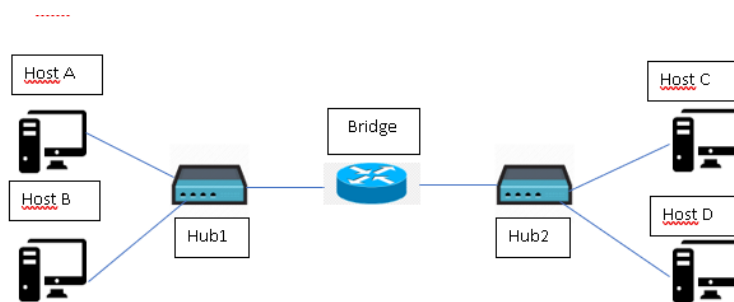
Foram definidas, uma placa NAT que iria servir de router e uma placa de Rede interna para a interligar a firewall com o servidor, posteriormente essa placa em NAT passou a Bridge.

Tanto o servidor e máquina cliente tinham a placa de Rede Interna para que estivesse tudo dentro da mesma rede. Posteriormente foi criada uma máquina cliente ubuntu para servir de utilizador na rede Guest.

### 2.5.2. BRIDGE

Uma **ponte**, ou **bridge**, é um dispositivo de rede que cria uma rede agregada a partir de várias redes de comunicações ou vários segmentos de rede. A operação de uma bridge é diferente daquela de um router, que permite que várias redes diferentes se comuniquem independentemente, permanecendo distintas entre si. No modelo OSI as pontes operam nas duas primeiras camadas abaixo da camada de rede, ou camada 3. (Bhardwaj, 2020)

Basicamente uma rede bridge é responsável por encaminhar os pacotes de rede para o host de destino.

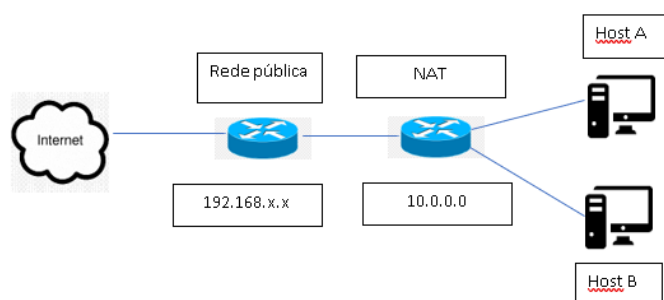


**Figura 20- Esquema de uma rede Bridge**

Na Figura 20, dá para perceber bem o papel da Bridge, por exemplo, se o Host A quiser comunicar com o Host C, o Host A vai enviar o quadro com o endereço MAC de destino do Host C para a Bridge. Esta vai inspecionar o quadro e vai encaminhar para o dispositivo de rede em que o Host C está.

### 2.5.3 NAT

Uma rede NAT é desenhada para conservação de endereços ip. Isto permite que redes privadas usem endereços ip não registados para se conectar à internet. A NAT funciona num router, normalmente conectando duas redes, e traduz o endereço privado da rede privada para um endereço público, antes dos pacotes serem encaminhados para outra rede. NAT permite que um único dispositivo, como um router, funcione como um agente entre a internet (rede publica) e a rede local (rede privada), o que significa que apenas um único ip é necessário para representar um grupo de computadores para qualquer coisa fora da rede. Na Figura 21, dá para entender como uma rede NAT funciona, onde o host A e o host B estão ligados a uma rede privada antes de se conectarem a uma rede pública. (rvigil, 2020)



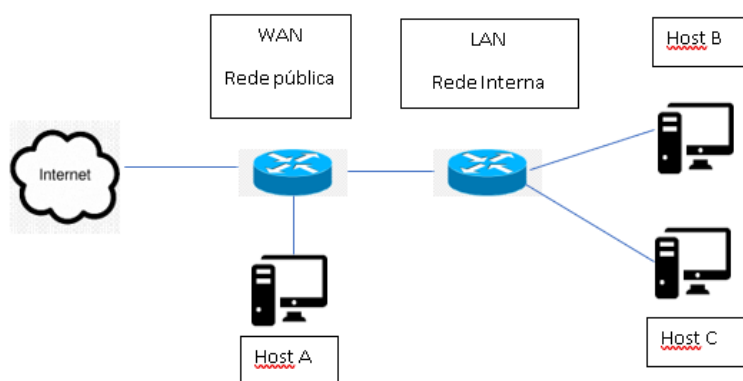
**Figura 21- Esquema de uma rede NAT**



## 2.5.4 INTERNAL NETWORK

Tal como o próprio nome indica, Internal Network, é uma rede interna. Este tipo de redes é geralmente utilizado para redes LAN. Esta rede está sempre associada a outro tipo de dispositivos de rede para ter internet. Neste modo, a comunicação entre as máquinas dentro da rede interna fica escondida da rede do host, pois é criada uma rede privada à parte da rede do host. Uma das grandes vantagens que esta rede oferece é a segurança, justamente pelo facto de os pacotes transmitidos entre as máquinas não serem capturados pela rede do host. (Valiante, 2020)

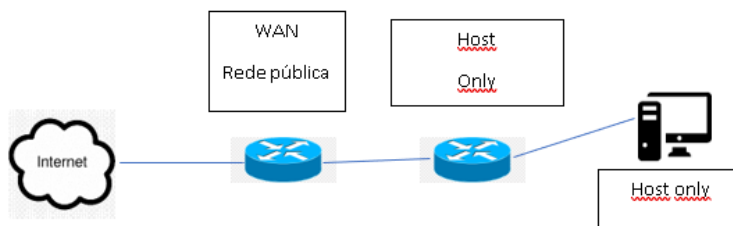
A Figura 22 retrata um esquema de uma rede interna, onde demonstra que uma rede interna, ao contrário de uma rede NAT não é um agente de rede. Os Hosts da rede interna vão poder comunicar entre si sem qualquer influência da rede pública, ao estar conectados a uma rede completamente diferente da pública.



**Figura 22- Esquema de uma rede Interna**

## 2.5.5 HOST ONLY

Esta rede funciona como a Internal Network, mas apenas com a diferença que é destinada a um único Host. Para cada host é necessária uma placa de rede diferente.



**Figura 23- Esquema de uma rede Host Only**

A Figura 23 demonstra um esquema referente a uma rede em que há uma interface host only, em que é definida uma rede isolada para um utilizador.

## 2.6 WINDOWS SERVER

O Windows Server é um grupo de sistemas operativos projetados pela Microsoft que oferece suporte à gestão, armazenamento de dados, aplicativos e comunicações em nível empresarial. As versões anteriores do Windows Server focavam na estabilidade, segurança, rede e várias melhorias no sistema de arquivos. Outras melhorias também incluíram melhorias nas tecnologias de implantação, bem como maior suporte de hardware. O Windows Server 2012 R2 é a versão mais recente do Windows Server e se concentra na computação em nuvem.

Este sistema tem um software de servidor, que inclui diversas ferramentas para as necessidades do cliente, inclusive o próprio cliente é que escolhe quais quer instalar.

As razões pela escolha deste sistema operativo foram, bastante intuitiva, ser um sistema bastante profissional e ser um sistema que a empresa já tinha implementado.

Foi optado o Windows Server 2012 pelo facto de já terem sido realizadas tarefas curriculares em ambiente escolar. (Rouse, 2020)

## 2.6.1 ESTRUTURA DO SERVIDOR

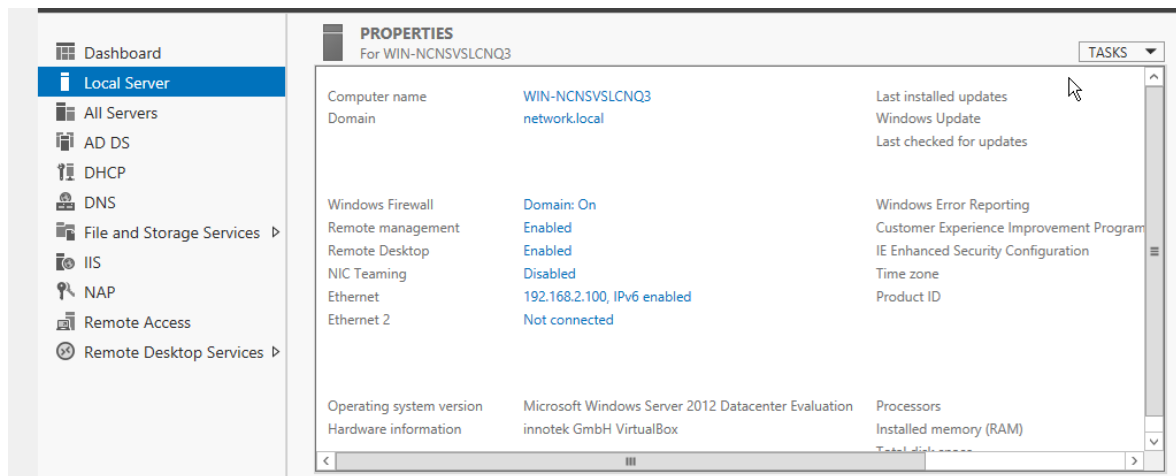


Figura 24- Estrutura do servidor

Tal como se pode verificar na Figura 24, foi definido o domínio network.local e o próprio ip do servidor de acordo com a rede da firewall.

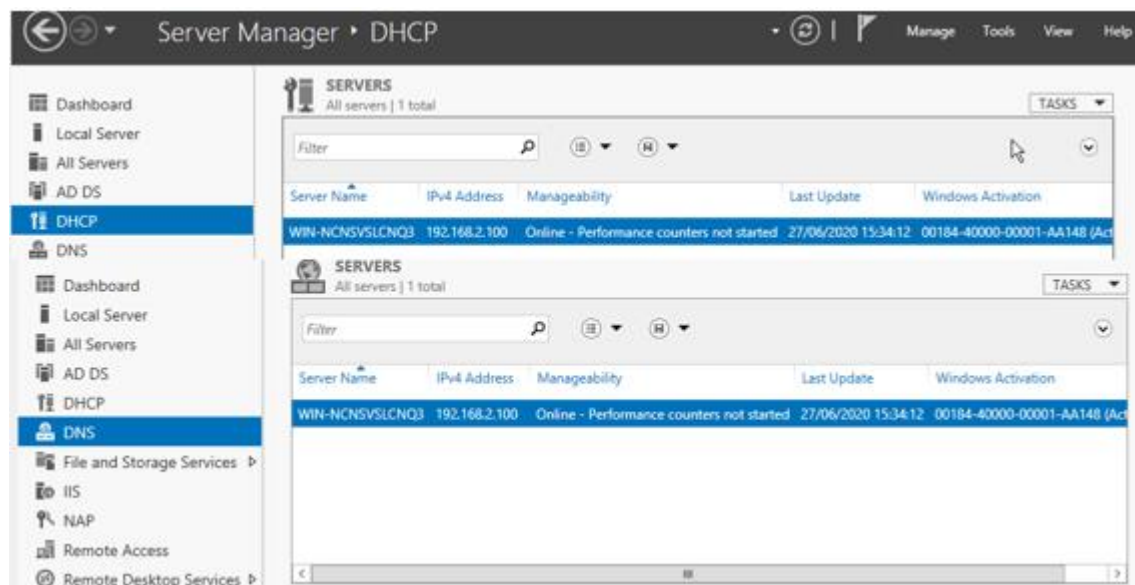
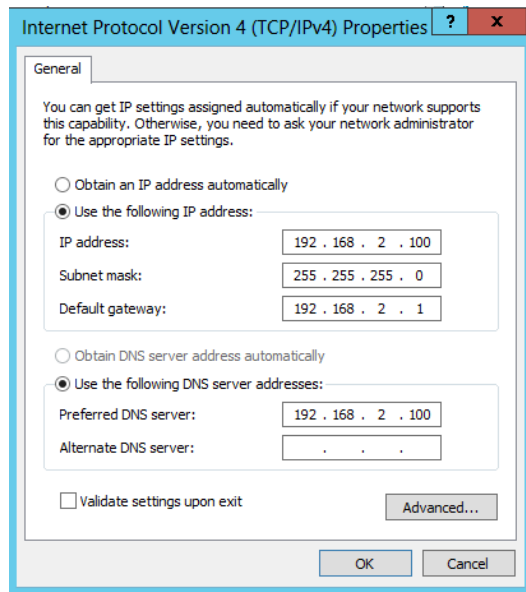


Figura 25- DHCP e DNS do Servidor

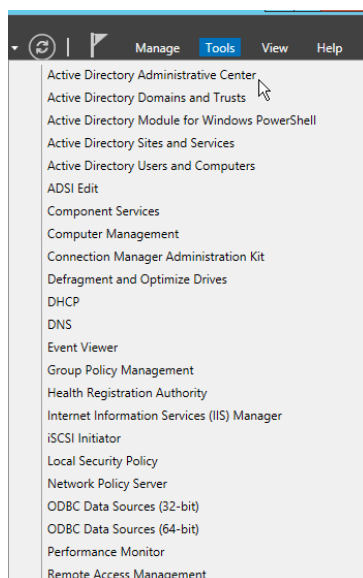
Como a rede foi diretamente definida na placa da máquina, o DHCP e o DNS ficaram automaticamente com o ip definido, tal como demonstra a Figura 25.



**Figura 26- Configuração de rede do Servidor**

A Figura 26 descreve que o ip do servidor ficou definido como 192.168.2.100, a máscara /24 e o gateway definido na firewall.

Foram adicionadas bastantes ferramentas caso fosse necessário o uso das mesmas, muitas destas ferramentas são essências para qualquer cliente que esteja a pensar instalar este sistema, tais como, todas as ferramentas do active directory, DHCP, DNS, adsi edit entre outras, como demonstra a Figura 27.



**Figura 27-Ferramentas instaladas no servidor**

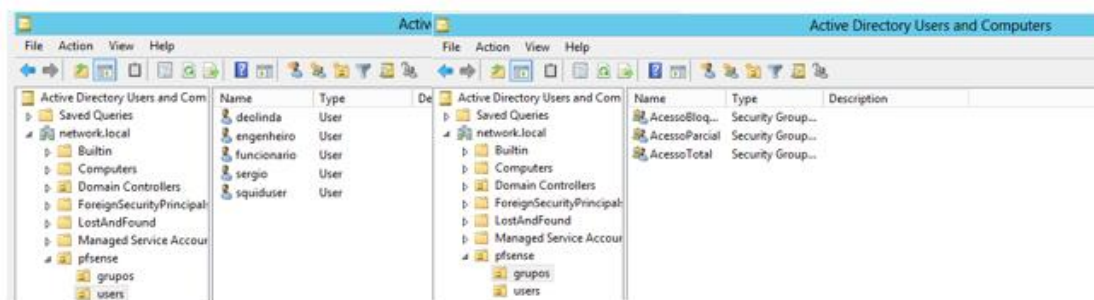
## 2.6.2 GRUPOS/UTILIZADORES

Foram criados vários utilizadores para testes, de primeiro momento foi criado uma unidade organizacional para dividir os utilizadores da Pfsense.

Dentro desta unidade podemos verificar que foram criadas outras duas unidades organizacionais, uma chamada grupos e outra users.

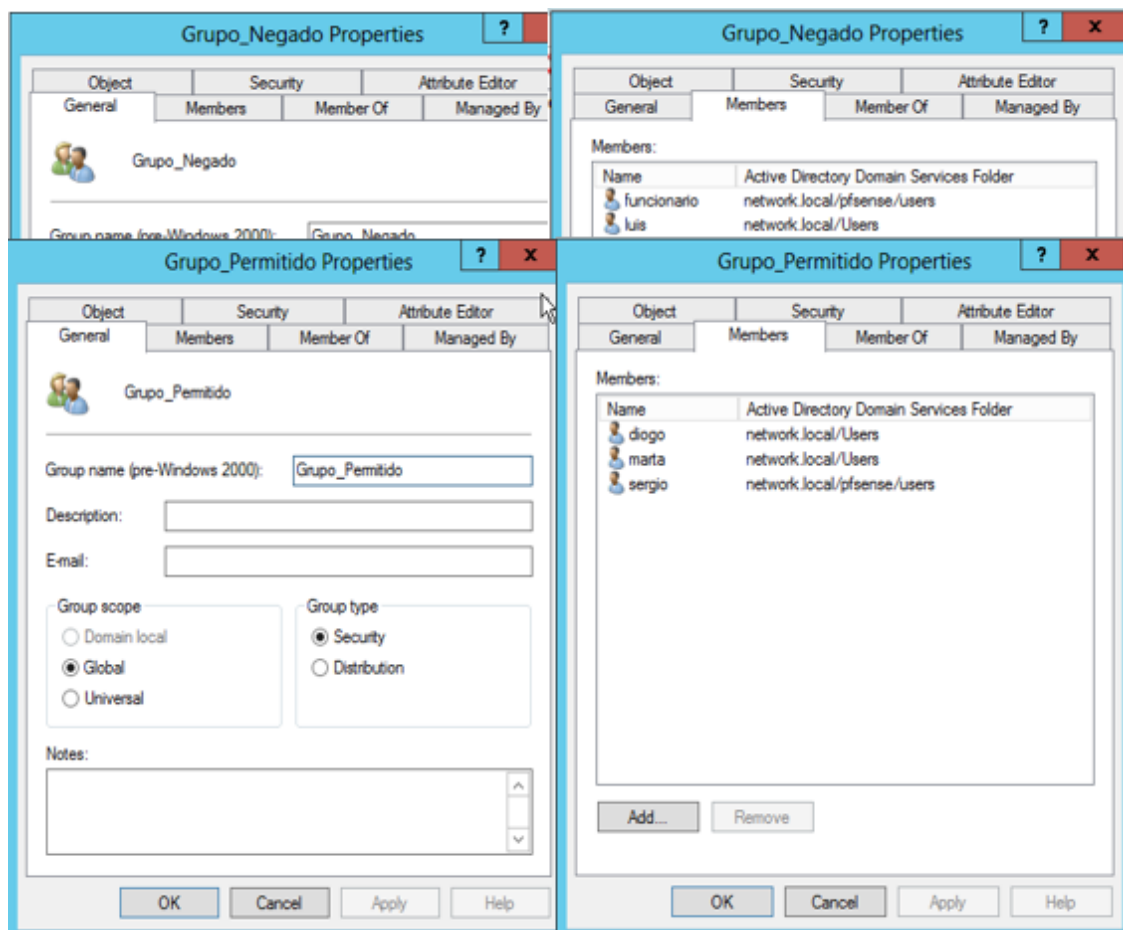
Estas duas unidades tinham o intuito de dividir os utilizadores por grupos com os respetivos acessos de cada um.

Chegou a tentar ser implementado deste ponto de vista, mas como os caminhos dos nomes já estavam demasiado longos, foi optado por juntar todos os utilizadores no grupo de utilizadores predefinido pelo ws, tal como mostra a Figura 28.



**Figura 28- Primeira Configuração dos grupos e dos utilizadores no servidor**

Posto isto foram criados dois grupos, o Grupo Negado e o Permitido, estes 2 grupos tinham o papel de separar os utilizadores com acesso à internet dos sem acesso. De certa forma ficou mais simples em relação à maneira anterior. A criação dos referentes grupos é demonstrada na Figura 29.



**Figura 29- Configuração dos Novos Grupos com Acesso e sem acesso**

Dentro do Grupo Negado foram adicionados apenas 2 utilizadores para não terem qualquer acesso à rede. Já no Grupo Permitted, foram adicionados 3 utilizadores, com o intuito de ter um acesso total à rede.

## 2.7 ACTIVE DIRECTORY

O active directory é um produto da Microsoft, que contém alguns serviços executados no Windows server, em que estes são responsáveis por gerir permissões e acessos à rede.

O AD armazena dados como objetos. Um objecto representa um utilizador, um grupo ou um dispositivo. Estes objetos são categorizados por nome e atributos. Por exemplo, um nome de utilizador pode incluir uma cadeia de nomes, junto com as informações associadas ao utilizador.

O principal serviço do AD é o Active Directory Domain Service (ADDS), que é responsável por armazenar informações de diretório e lidar com a ligação do utilizador com o domínio.

O ADDS verifica o acesso quando um utilizador entra num dispositivo ou tenta se conectar a um servidor através de uma rede.

Dentro dos serviços do AD, existe ainda um serviço chamado “Active Directory Lightweight Directory Services”, que guarda os dados do diretório num banco de dados utilizando o protocolo LDAP (Lightweight Directory Access Protocol).

### **2.7.1 LDAP**

Ldap é um protocolo de aplicação usado para aceder e manter serviços de diretório numa rede. Este guarda vários objetos, como nomes do utilizador, palavras passes, etc, dentro dos serviços de diretório e partilha esses dados e objetos pela rede.

Um servidor LDAP contém o diretório de utilizadores em uma árvore de diretórios LDAP. Clientes LDAP que desejam obter informações sobre entradas na árvore ou faça modificações nessas entradas, entre em contato com o servidor. Esses servidores podem ser replicados para permitir acesso mais rápido e confiável ao diretório em uma rede. Servidores LDAP podem armazenar vários atributos do utilizador, como números de telefone, e-mails e locais, além de informações de autenticação. Isso oferece aos administradores de rede flexibilidade ao implementar serviços como login único.

Por norma o LDAP usa como portas padrões as 389 e 636. Este protocolo também é responsável por conectar um serviço AD à firewall. (DeMeyer, 2020)

## 2.7.2 RADIUS

Radius ou “Remote Access Dial-In User Service” é uma ferramenta criada para autenticar identidades de utilizadores na infraestrutura da rede geralmente de um diretório, como o Active Directory. Da mesma forma que o LDAP, o Radius serve como um protocolo e como um software. (DeMeyer, 2020)

Isto quer dizer que o Radius pode armazenar identidades de utilizadores para fins de autenticação, mas o trabalho de realizar essas autenticações é de um serviço do AD.

O principal uso do Radius é centralizar autenticações para muitos diferentes tipos de equipamentos de rede. Estes dispositivos podem incluir “wireless access points”, switches, VPNs, routers, entre outros. Essencialmente o Radius fornece uma maneira de garantir a segurança na rede através da autenticação de utilizadores ser feita pelo seu próprio conjunto de credenciais, sem utilizar credencias de rede compartilhadas como o acesso ao Wifi ou VPN.

O facto de o Radius existir há mais de 20 anos faz com que este trabalhe com vários equipamentos. Pode ser utilizado em várias situações, desde capus universitários a infraestruturas corporativas, onde existem muitos utilizadores diferentes e uma grande quantidade de equipamentos de rede.

Se cada utilizador tivesse de ter uma infinidade de informações de login para cada rede Wi-fi ou VPN, seria claramente uma experiência aborrecida para o utilizador pois iria consumir muito tempo. O Radius vem de certa forma facilitar esse problema, ao centralizar o processo de autenticação para que os utilizadores tenham um conjunto de credenciais para uma grande variedade de redes, equipamentos de rede e infraestrutura.

Por norma usa o UDP 1645 ou UDP 1812 como porta padrão.



### 2.7.3 LDAP VS RADIUS

Existem algumas diferenças na maneira como estes protocolos operam, o que faz com que haja diferenças de segurança e tráfego.

A maneira de interagir com a rede é diferente, o LDAP usa o protocolo TCP e o Radius usa o UDP. A conexão pelo TCP é confiável, mas a sobrecarga da rede é maior. O UDP minimiza essas despesas gerais da rede e a conexão não é tão confiável como a do TCP.

Se a velocidade é prioridade, o RADIUS é a melhor opção, o LDAP requer várias transações de pedidos entre o cliente e o servidor, o que faz com que seja mais lento, ao usar um mecanismo de cache para armazenar informações do utilizador faz com que o Radius seja mais rápido.

Por definição padrão, os pacotes Radius não possuem criptografia diferente daquele que contém a senha, logo há uma chance de vazamento de informações confidenciais e, portanto, as administrações precisam de mecanismos de segurança adicionais. Enquanto que no protocolo TCP, a criptografia é aplicável em todas as transferências. (DeMeyer, 2020)

Por outro lado, o LDAP ainda não suporta a autenticação multifactor. Existem vários serviços de nível empresarial disponíveis, mas o requisito de recursos é demasiado alto. Esses serviços podem usar outros protocolos, incluindo o RADIUS.

É por isso que existem tantas empresas a usar o LDAP e RADIUS em conjunto.

Gerir o RADIUS não é uma tarefa fácil, pois tem mais funcionalidades e é de maior complexidade. O RADIUS usa vários protocolos para comunicação e a solução de problemas se torna um pouco complicada. Como o LDAP oferece uma autenticação básica com o mínimo de hardware e uma interface fácil de usar, a carga de manutenção é mínima e não há tanto estresse para os administradores.

Em resumo, as funções básicas de ambos os protocolos são as mesmas, a autenticação.

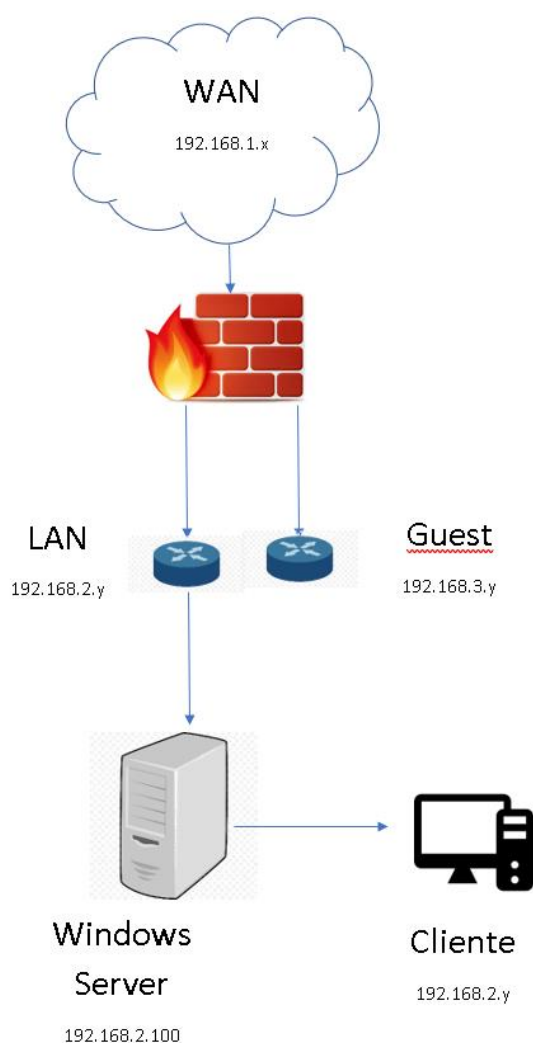
O LDAP é ideal para serviços de login únicos, é facilmente criptografado e extremamente simples de configurar e integrar com a rede.

O Radius permite flexibilidade nos serviços e é aplicável a todos os serviços de rede, mas a configuração é complexa o que faz com que seja mais demorada.

O LDAP é perfeito para pequenas aplicações e autenticações simples, o RADIUS é direcionado para uma autenticação complexa e avançada. (Herrmann, 2020)

## 2.8 PFSENSE

### 2.8.1 ESQUEMA DE REDE



**Figura 30- Esquema de rede da Firewall**

A Figura 30 mostra o esquema rede definido na firewall, onde existe uma rede WAN que tem a função de rede pública, que por sua vez é filtrada pela firewall PfSense. Dentro desta firewall ainda existem outras duas redes, uma referente à LAN e outra à rede Guest. A rede LAN está conectada ao servidor, onde existe um cliente conectado ao domínio do servidor.

## 2.8.2 CONSOLA E AMBIENTE GRÁFICO

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: c176fb2b827d0bbf6c1a
*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.103/24
                v6/DHCP6: 2001:8a0:f4cd:2101:a00:27ff:fe2e:4bf
3/64
LAN (lan)      -> em1      -> v4: 192.168.2.1/24
GUESTWIFI (opt1) -> em2      -> v4: 192.168.4.200/24
OPT2 (opt2)    -> ovps1     -> v4: 192.168.10.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Figura 31- Consola da Pfsense

A Figura 31 retrata a configuração da Pfsense, onde foram adicionadas as redes de 3 placas, uma rede WAN que está a fazer de router, a interface desta Wan foi mudada de Nat para bridge para poder estabelecer conexão VPN, outra que está a servir de LAN, que neste caso vai servir para os utilizadores do WS, e outra rede diferente mas que é controlada na mesma pela firewall, que vai ter o papel de rede Guest.

Para configurar estas redes fui à primeira opção e escolhi as interfaces que necessitava, de seguida defini apenas o ip de cada uma delas na opção 2.

Através da opção “Filter Logs” consegue-se verificar quem fez o login na firewall.

A Figura 32 descreve o ambiente gráfico da Pfsense, que corresponde ao ip do gateway da LAN, onde o administrador tem de fazer o login para poder entrar dentro da firewall.

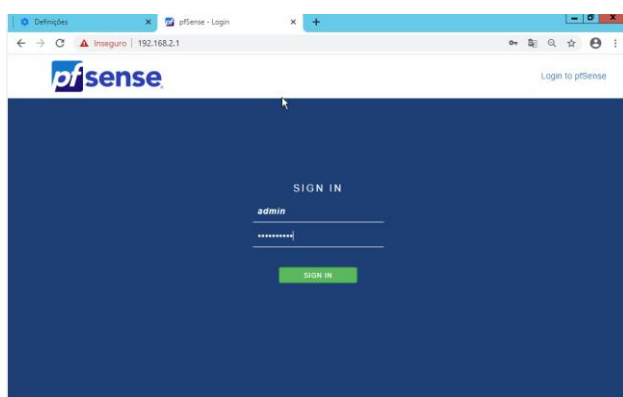


Figura 32- Ambiente gráfico da Pfsense e credenciais do utilizador

### 2.8.3 PROXY

Um proxy é um servidor que age como um intermediário para requisições dos clientes, solicitando recursos de outros servidores. Um cliente conecta-se a um servidor proxy, fazendo a solicitação de algum serviço, como uma página web, conexão, ou outros recursos disponíveis, o proxy avalia a situação e controla a acessibilidade do cliente. Os serviços proxy foram inventados para adicionar estrutura e encapsulamento aos sistemas distribuídos. Esses servidores têm uma série de usos, como filtrar conteúdo, providenciar anonimato, entre outros. Com um serviço proxy web, qualquer operação que o cliente pretenda desempenhar na internet, é realizada uma solicitação ao proxy para este avaliar a situação do cliente relativamente às suas permissões efetuadas na configuração do proxy, para ver se o mesmo pode aceder ao serviço que pretende aceder ou não, caso a requisição seja bem sucedida, o proxy deixa o cliente aceder, senão é impedido.

O servidor proxy surgiu da necessidade de conectar uma rede local (ou LAN) à Internet através de um computador da rede que compartilha a sua conexão com as demais máquinas. O proxy é aquele que permite que outras máquinas tenham acesso externo.

Depois deste implementado no servidor, qualquer utilizador necessita de ter o proxy do seu computador devidamente configurado para aceder à rede. (Pinto, 2020)

### 2.8.4 FUNÇÕES DO PROXY

**Controlo de acesso** – É possível para os administradores do servidor proxy permitir que determinados utilizadores tenham, ou não, acesso à Internet através de restrições aplicadas ao login do próprio utilizador ou aos endereços IP, dando ao ambiente uma camada extra de proteção.

**Filtro de conteúdo** – O servidor também permite que determinados sites sejam, ou não, acedidos. Entre as regras que podem ser aplicadas estão as destinadas ao bloqueio de sites específicos, podendo chegar ao bloqueio de categorias inteiras.

## 2.8.5 CACHE

Os webs proxies podem fazer a função de cache, fazendo com que após o acesso a uma página, o proxy armazena o seu conteúdo no sistema. Desta forma é economizado o próprio uso da internet e tempo, devido a já estar na memória é mais fácil e rápido aceder ao site pretendido e o proxy não precisa de receber solicitação para depois responder ao pedido. (Pinto, 2020)

## 2.8.6 PROXY REVERSO

No caso do proxy reverso, as origens das requisições estão na Internet e tentam aceder a um servidor dentro do ambiente. A Figura 33 retrata como funciona um proxy reverso.



**Figura 33- Esquema do proxy reverso**

Os proxies reversos são normalmente usados para tratar requisições destinadas a servidores que alojam páginas da Internet.

## 2.8.7 SQUID PROXY SERVER

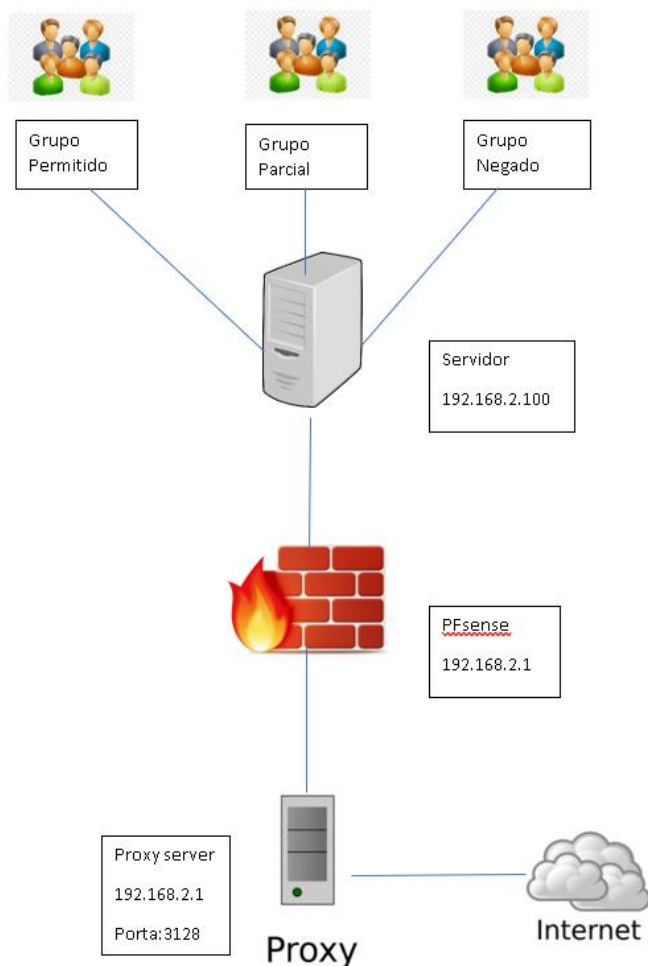
Squid é principalmente um proxy de encaminhamento usado para controle de acesso do cliente. O Squid é um aplicativo de servidor de cache de proxy completo, que fornece serviços de proxy e cache para HTTP (Hyper Text Transport Protocol), FTP (File Transfer Protocol) e outros protocolos de rede populares.

O Squid é usado por centenas de provedores de Internet em todo o mundo para fornecer aos seus utilizadores o melhor acesso possível à internet. O Squid otimiza o fluxo de dados entre cliente e o servidor para melhorar o desempenho e armazena em cache o conteúdo usado com frequência para economizar largura de banda.

Milhares de sites na Internet usam o Squid para aumentar drasticamente a entrega de conteúdo. O mesmo pode reduzir a carga do servidor e melhorar as velocidades de entrega para os clientes.

O Squid tem algumas funcionalidades que permitem tornar as conexões anônimas, tais como desabilitar ou alterar campos específicos do cabeçalho dos pedidos HTTP do cliente. Se isto é feito e como, é controlado pela pessoa que administra a máquina que corre o Squid, as pessoas que requisitam páginas numa rede que usa Squid de forma transparente podem não saber que esta informação será registada.

## 2.8.8 ESQUEMA DO PROXY E DOS DIFERENTES GRUPOS COM ACESSOS À REDE



**Figura 34- Esquema do proxy e dos grupos definidos**

A Figura 34, demonstra a estrutura de rede que ficou definida, desde os grupos de utilizadores definidos, à conexão do servidor com a firewall, onde é possível verificar que qualquer utilizador para se conectar à internet tem de estar ligado ao proxy.

A restrição de acessos ficou definida em 3 grupos diferentes, o grupo permitido, o grupo parcial e o grupo negado.

No grupo permitido, os utilizadores têm um acesso total à internet, tendo por base permissões extras relativamente aos outros funcionários para poder resolver qualquer tipo de situação, sendo o grupo constituído por um número reduzido de utilizadores.

Já no grupo parcial, os utilizadores, os mesmos têm um acesso à internet com opções reduzidas ou mesmo sites limitados. Podendo fazer praticamente qualquer tipo de investigação na internet, mas nada que fuga muito relativamente ao seu trabalho. Este grupo acabou por não ficar definido.

Relativamente ao grupo negado, estes utilizadores não têm qualquer tipo de acesso à internet, tendo por base funções na empresa que não necessitam do acesso à rede.

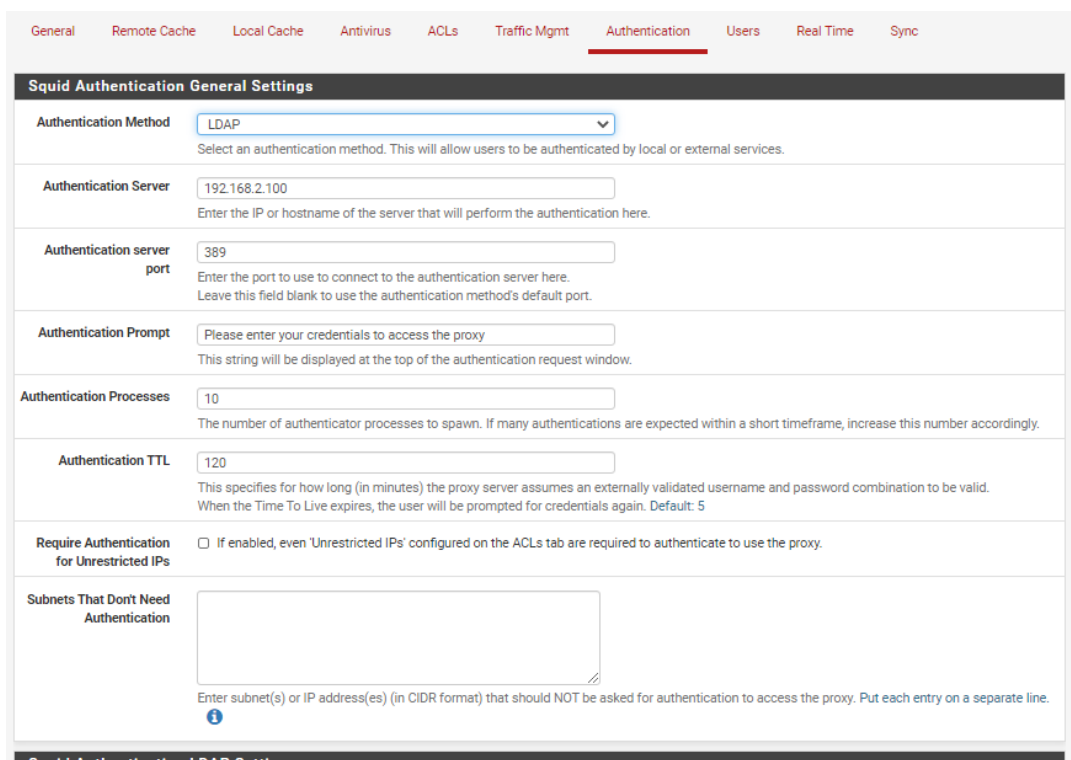


## 2.8.9 CONFIGURAÇÃO REALIZADA

Primeiro de tudo foi instalado o squid proxy e o squid guard na Pfsense.

Já na configuração do Squid proxy foi selecionado a opção autenticação LDAP, onde é configurado tudo relativamente à conexão entre a firewall e o AD.

Tal como se pode verificar na Figura 35 é definido o ip do servidor, em seguida a porta do servidor, que é a porta 389 definida por padrão para conexões LDAP e usa o protocolo TCP, conseqüentemente o número de processos de autenticação e o tempo que o utilizador pode ficar conectado sem serem pedidas as credenciais outra vez. (Moraes, 2020)



The screenshot displays the 'Squid Authentication General Settings' page in the PfSense web interface. The 'Authentication' tab is selected in the top navigation bar. The settings are as follows:

- Authentication Method:** LDAP (selected from a dropdown menu). Description: Select an authentication method. This will allow users to be authenticated by local or external services.
- Authentication Server:** 192.168.2.100. Description: Enter the IP or hostname of the server that will perform the authentication here.
- Authentication server port:** 389. Description: Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.
- Authentication Prompt:** Please enter your credentials to access the proxy. Description: This string will be displayed at the top of the authentication request window.
- Authentication Processes:** 10. Description: The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.
- Authentication TTL:** 120. Description: This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5.
- Require Authentication for Unrestricted IPs:** ☐. Description: If enabled, even 'Unrestricted IPs' configured on the ACLs tab are required to authenticate to use the proxy.
- Subnets That Don't Need Authentication:** (Empty text area). Description: Enter subnet(s) or IP address(es) (in CIDR format) that should NOT be asked for authentication to access the proxy. Put each entry on a separate line.

The bottom of the page shows the start of the 'Squid Authentication LDAP Settings' section.

Figura 35- Configuração da autenticação do proxy na Pfsense

De seguida é configurado conforme ilustra Figura 36 a versão do LDAP, o modo de transporte, o utilizador que vai fazer a conexão do proxy com o AD, a password desse mesmo utilizador, seguidamente o domínio do servidor, o nome conforme é atribuído e o modo de procura que este vai utilizar.

**Squid Authentication LDAP Settings**

LDAP version: 3  
Select LDAP protocol version.

Transport: TCP - Standard  
If 'SSL Encrypted' or 'TCP - STARTTLS' is selected, the CA certificate of the LDAP server must be trusted by the Operating System Trust Store. This is automatic for certificates signed by globally trusted CAs such as Let's Encrypt; self-signed CAs can optionally be added to the Trust Store on pfSense 2.5.

LDAP Server User DN: CN=Administrator,CN=Users,DC=network,DC=local  
Enter the user DN to use to connect to the LDAP server here.

LDAP Password: .....  
Enter the password to use to connect to the LDAP server here.

LDAP Base Domain: DC=network,DC=local  
Enter the base domain of the LDAP server here.

LDAP Username DN Attribute: sAMAccountName  
Enter LDAP username DN attribute here.

LDAP Search Filter: (&(objectClass=person)(sAMAccountName=%s))  
Enter LDAP search filter here.

LDAP not follow referrals: ☐ Do not follow referrals.

**Squid Authentication RADIUS Settings**

RADIUS Secret: .....  
Enter the RADIUS secret for RADIUS authentication here.

[Save](#)

Figura 36- Configuração da Autenticação do proxy na PfSense 2

Tal como demonstra a Figura 37, nas configurações gerais, apenas foi ativado, o proxy, o modo de guardar as configurações, para o caso de haver algum problema as configurações manterem-se, a porta do proxy, permitir a navegação dos utilizadores na interface, foi verificada também a opção para resolver ipv4 DNS primeiro, caso haja algum problema a aceder a sites https. A presente configuração está disposta em anexo um.

**Squid General Settings**

Enable Squid Proxy: ☒ Check to enable the Squid proxy.  
**Important:** If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data: ☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.  
**Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version: IPv4  
Select the IP version Squid will use to select addresses for accepting client connections.

Proxy interface(s): LAN  
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Proxy Port: 3128  
This is the port the proxy server will listen on. Default: 3128

ICP Port: .....  
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.  
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface: ☒ If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.  
There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal: This feature was removed - see Bug #5594 for details!

Resolve DNS IPv4 First: ☒ Enable this to force DNS IPv4 lookup first.  
This option is very useful if you have problems accessing HTTPS sites.

[Save](#)

Figura 37- Configuração do squid proxy

No SquidGuard, na parte das configurações gerais, foram também postos, o utilizador responsável pela conexão do proxy com o AD e a sua password correspondente, foi verificada a opção de “enable log” com o intuito de se configurar os ACLS Groups, tal como demonstra a Figura 38.

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

**General Options**

Enable ☒ Check this option to enable squidGuard.  
**Important:** Please set up at least one category on the 'Target Categories' tab before enabling. See [this link](#) for details.  
 The Save button at the bottom of this page must be clicked to save configuration changes.  
 To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STARTED**

**LDAP Options**

Enable LDAP Filter ☒ Enable options for setup ldap connection to create filters with ldap search

LDAP DN   
 Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password   
 Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z][a-zA-Z0-9/\_\.\|\%|\+]?=8]

Strip NT domain name ☐ Strip NT domain name component from user names (/ or \ separated).

Strip Kerberos Realm ☐ Strip Kerberos Realm component from user names (@ separated).

LDAP Version

**Logging options**

Enable GUI log ☐ Check this option to log the access to the Proxy Filter GUI.

Enable log ☒ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

Enable log rotation ☐ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

**Figura 38- Configuração do SquidGuard**

De Seguida é verificada a opção de escolher uma blacklist, uma lista com diversos parâmetros para o administrador definir se o utilizador tem acesso ou não, foi escolhida uma das mais populares blacklist's atualmente, depois de selecionar esta foi necessário efetuar o download da mesma, tal como é possível verificar na Figura 39.

**Miscellaneous**

Clean Advertising ☐ Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

**Blacklist options**

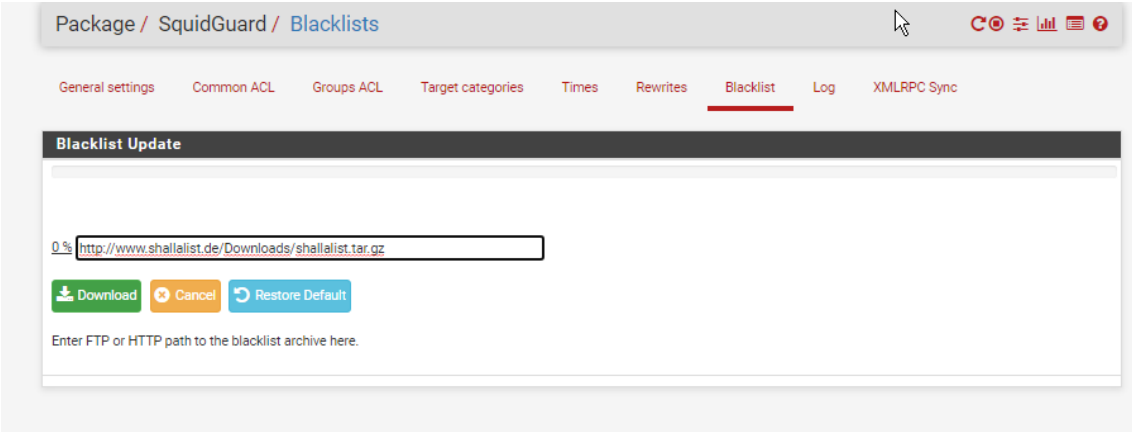
Blacklist ☒ Check this option to enable blacklist  
 Do NOT enable this on NanoBSD installs!

Blacklist proxy   
 Blacklist upload proxy - enter here, or leave blank.  
 Format: host[:port login:pass] . Default proxy port 1080.  
 Example: '192.168.0.1:8080 user:pass'

Blacklist URL   
 Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfSense (/tmp/blacklist.tar.gz).

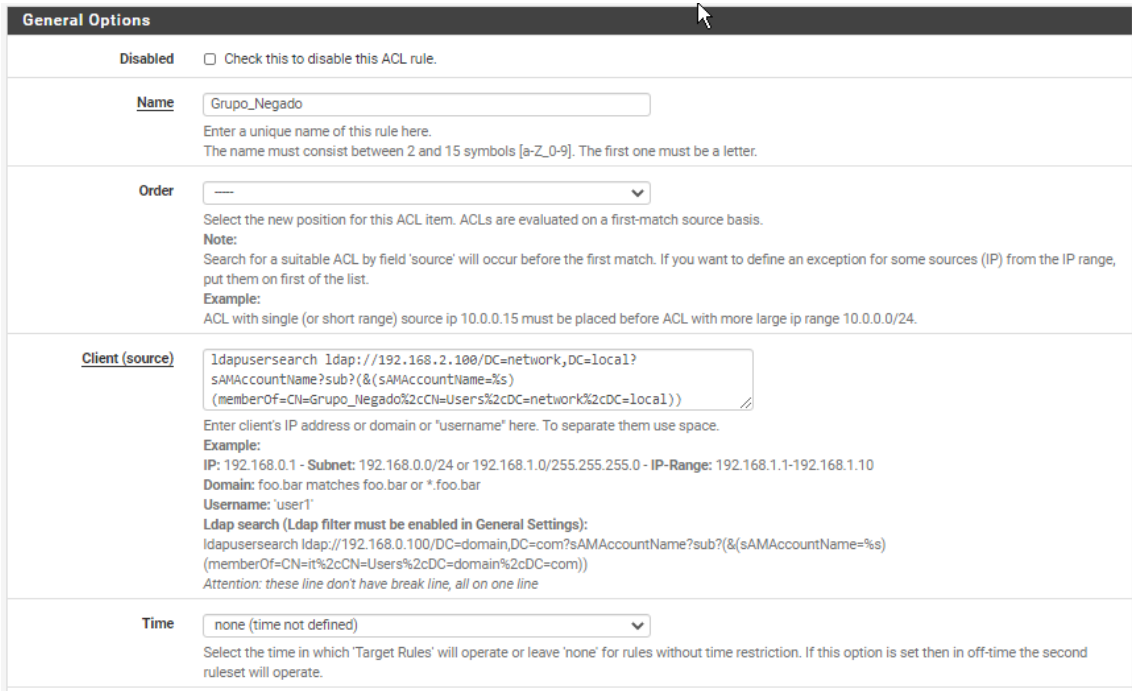
**Figura 39- Blacklist**

Para efetuar o download da blacklist apenas foi necessário inserir o link correspondente à blacklist e fazer o download, tal como mostra a Figura 40.



**Figura 40-Download da Blacklist**

Tal como demonstra Figura 41, de seguida foram feitas as configurações necessárias nos Groups ACL, onde foi configurado de acordo com os grupos e utilizadores adicionados no Windows server. É especificado o nome do grupo, neste caso é Grupo Negado, de seguida o caminho de configuração do grupo, onde é introduzido o ip, o domínio e a especificação do grupo e do modo de procura. A presente configuração está disposta em anexo dois.



**Figura 41-Configuração da acl do grupo negado**

De acordo com a blacklist instalada, o número de opções varia, mas como neste caso como o objetivo é proibir qualquer acesso do utilizador à internet é dado deny a todas as opções por definição. Neste caso o redireccionamento é definido para o site do ipca apenas por uma questão de testes. Pode ainda ser definido o site para que o utilizador é redirecionado. A Figura 42 demonstra a configuração descrita.

Target Rules List			
[URL_BL_webphone]	access	[URL_BL_webphone]	access
[URL_BL_webradio]	access	[URL_BL_webradio]	access
[URL_BL_webtv]	access	[URL_BL_webtv]	access
Default access [all]	deny	Default access [all]	deny

Figura 42- Configuração da acl do grupo negado 2

No grupo Permitido a configuração é a mesma, mas com o caminho especificado para os o grupo em questão. O target Rules neste caso como é para o utilizador ter um acesso total á rede é definido “allow” para todas a opções por definição, tal como demonstra a Figura 43.

**General Options**

☒ Check this to disable this ACL rule.

**Name**: Grupo\_Permitido

**Order**: 1

**Client (source)**: ldapsearch ldap://192.168.2.100/DC=network,DC=local?sAMAccountName?sub?(&(sAMAccountName=\*))

**Time**: none (time not defined)

**Target Rules**: all

Figura 43- Configuração da acl do grupo permitido

Foi ainda definido a modo de redirecionamento da página, como int error page, os outros também são válidos, foi ainda definido a mensagem que aparece, as outras opções não foram definidas pois não era necessário para o caso em questão. Configuração demonstrada em Figura 44.

[URL, BL, WEURLIST]	access	[URL, BL, WEURLIST]	access
[blk_BL_webphone]	access	[blk_BL_webphone]	access
[blk_BL_webradio]	access	[blk_BL_webradio]	access
[blk_BL_webtv]	access	[blk_BL_webtv]	access
Default access [all]	allow	Default access [all]	allow

**Do not allow IP-Addresses in URL**

☐ To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

**Redirect mode**

int error page (enter error message)

Select redirect mode here.  
Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.  
Options: [ext url err page](#) , [ext url redirect](#) , [ext url as 'move'](#) , [ext url as 'found'](#).

**Redirect**

permitido

Enter the external redirection URL, error message or size (bytes) here.

**Use SafeSearch engine**

☐ To protect your children from adult content you can use the protected mode of search engines.  
At the moment it is supported by Google, Yandex, Yahoo, DuckDuckGo, Qwant, Rambler, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.  
Note: This option overrides 'Rewrite' setting.

**Rewrite**

none (rewrite not defined)

Enter the rewrite condition name for this rule or leave it blank.

**Rewrite for off-time**

none (rewrite not defined)

Enter the rewrite condition name for this rule or leave it blank.

**Description**

Grupo\_Permitido

You may enter any description here for your reference.

**Log**

☐ Check this option to enable logging for this ACL.

Save

Figura 44- Configuração da acl do grupo permitido 2

De seguida foi adicionado o proxy nas configurações do browser, com o ip do gateway e porta do servidor, como mostra a Figura 45.

Internet Properties

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☒ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

☒ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.2.1 Port: 3128 Advanced

☐ Bypass proxy server for local addresses

OK

Cancel

Figura 45- Rede local do Servidor

Adicionado o proxy, o login é automaticamente pedido ao tentar aceder à internet.

Como se pode verificar na Figura 46, a implementação do proxy é bem sucedida, com um redireccionamento para o ip do gateway com a porta 3128, geralmente a porta usada pelo servidor do proxy. Caso o utilizador tenha permissão o acesso é permitido, caso o utilizador não tenha permissão o acesso é negado.

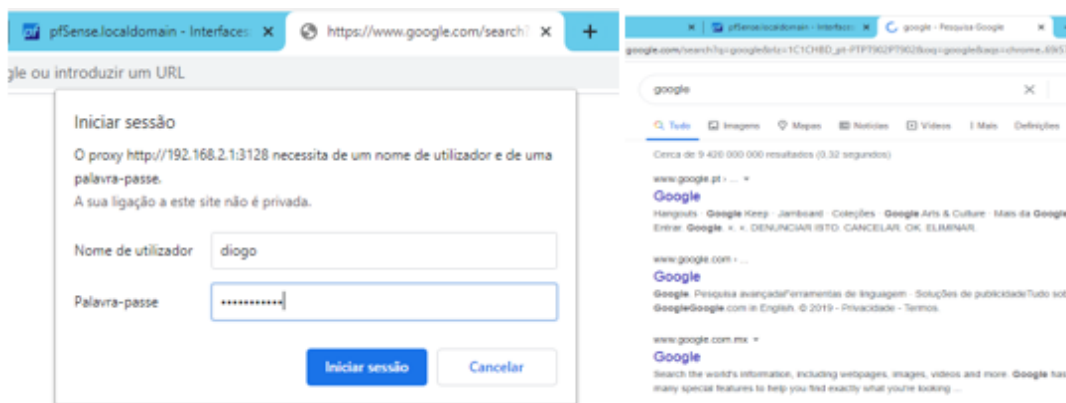


Figura 46- Acesso permitido

## 2.9 CAPTIVEPORTAL

O Captive Portal é um software que bloqueia o acesso do cliente à internet até uma verificação do cliente ser estabelecida. O cliente que se está a conectar a uma rede é redirecionado para uma página web para efetuar uma verificação.

Este tipo de verificação pode ser efetuado através de várias maneiras, as maneiras mais aplicadas são, ou por login do utilizador ou através de um voucher.

O uso mais comum do Captive Portal é para redes Wi-fi ou para autenticação adicional, na maioria das vezes é utilizado para controlar o acesso de visitantes à rede.

A configuração deste software é maioritariamente definida de maneira a que o utilizador visitante tenha um acesso parcial à rede, incluindo que a ligação do mesmo termine passado algum tempo, nunca sendo controlada pelo utilizador, este método é muito implementado em hotéis, aeroportos, centros comerciais, etc.

Deste modo os acessos dos visitantes são controlados assim como toda a sua ligação à rede, tornando a rede mais segura e que não haja possíveis intrusos na rede.

Existem várias maneiras de configurar este software, tudo vai depender da maneira que está implementado e da sua função.

É possível fazer com que certos mac-addresses ou mesmo alguns ip's passem pela autenticação do portal.

A página de login pode ser configurada e customizada pelo responsável da configuração da mesma, podendo tornar por exemplo mais apelativa a página web. (Rouse, 2020)

### **2.9.1 VANTAGENS E DESVANTAGENS**

O facto de visitantes estarem conectados numa rede diferente dos administradores ou mesmo operadores faz com que a rede fique muito mais segura e protege informações valiosas da empresa.

Uma das grandes desvantagens é a segurança do utilizador na rede, como a maioria das vezes este tipo de método é implementado numa rede pública, o acesso do utilizador à rede acaba por estar bastante exposto a eventuais hackers que possam estar na rede. O aconselhado neste tipo de casos é mesmo o cliente ter noção que está numa rede pública e não aceder a informações relevantes dentro da rede.

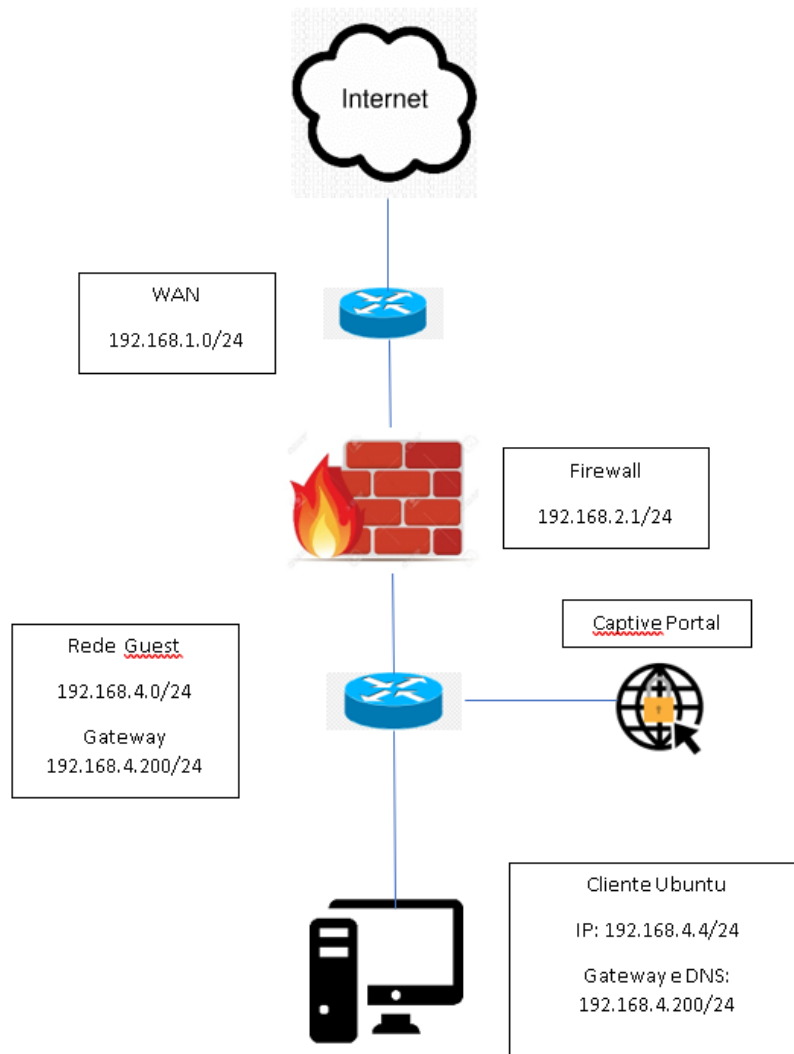
Limitar a largura de banda é crucial para equilibrar a carga de rede, impedindo que utilizadores usem muitos recursos da rede, como fazer grandes downloads ou mesmo alguns streaming de vídeo em HD.

O uso fácil é outro ponto a ter em vista, o utilizador não precisa de preencher qualquer tipo de formulário ou algum tipo de informação massiva e complexa, apenas precisa de fazer o login no portal. (HOFFMAN-ANDREWS, 2020)



## 2.9.2 CONFIGURAÇÃO DO CAPTIVE PORTAL NA PFSENSE

### 2.9.2.1 ESQUEMA DO CAPTIVE PORTAL



**Figura 47- Esquema do Captive Portal**

A Figura 47, demonstra como ficou definida a rede guest dentro da firewall, onde se verifica que existe uma rede WAN que faz partilha de rede para a rede local da firewall, que está conectada e é responsável por filtrar a rede guest, que tem um cliente ubuntu conectado, com o gateway e o DNS definido da rede.

## 2.9.3 TESTES REALIZADOS COM O CAPTIVE PORTAL

Como era necessária uma rede destinada aos utilizadores guest e um sistema de controlo desses mesmos utilizadores, foi configurada uma interface em Bridge, mas com um ip fixo, que neste caso a rede optada foi a 192.168.4.0/24.

Depois de adicionada a interface à máquina da PfSense, ativação da mesma pode ser através da consola ou mesmo pela interface gráfica, onde é definido o ip do gateway e se é pretendido ativar o DHCP para a rede em questão, como demonstra a Figura 48.

The image shows two screenshots of the PfSense web interface. The top screenshot is the 'General Configuration' page for an interface named 'GuestWifi'. It includes fields for 'Enable' (checked), 'Description' (GuestWifi), 'IPv4 Configuration Type' (Static IPv4), 'IPv6 Configuration Type' (None), 'MAC Address' (blank), 'MTU' (blank), 'MSS' (blank), and 'Speed and Duplex' (Default). The bottom screenshot is the 'Static IPv4 Configuration' page, showing the 'IPv4 Address' set to 192.168.4.200 with a subnet mask of 24.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	GuestWifi <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="xxxxxxxxxxxx"/> <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xx:xx or leave blank.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.</small>
Speed and Duplex	Default (no preference, typically autoselect) <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small>

Static IPv4 Configuration	
IPv4 Address	192.168.4.200 / 24

Figura 48- Interface Guest

Ativada a placa, é necessário a criação de uma autoridade certificadora, assim como o seu respetivo certificado, como se pode verificar na Figura 49.

The image shows two screenshots of the Captive Portal configuration. The top screenshot shows the 'CAPTIVECA' self-signed certificate with details: ST=Braga, OU=lucemplast, O=lucemplast, L=Braga, CN=CAPTIVECA, C=PT. The bottom screenshot shows the 'lucemplast.captive.com' server certificate with details: CAPTIVECA, ST=Braga, OU=lucemplast, O=lucemplast, L=Braga, CN=lucemplast.captive.com, C=PT.

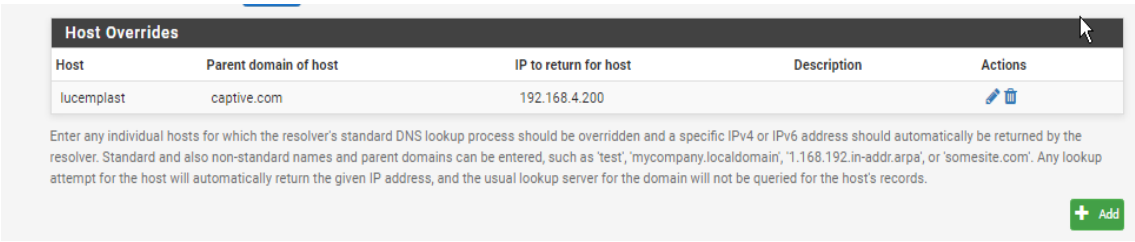
CA	Self-Signed	Details
CAPTIVECA	self-signed	ST=Braga, OU=lucemplast, O=lucemplast, L=Braga, CN=CAPTIVECA, C=PT

Server Certificate	CA	Details
lucemplast.captive.com	CAPTIVECA	ST=Braga, OU=lucemplast, O=lucemplast, L=Braga, CN=lucemplast.captive.com, C=PT

Figura 49- CA e certificado do CaptivePortal

O certificado, foi criado com nome que irá representar o domínio da página de login do captive portal, justamente para o cliente aceder pelo domínio e não pelo ip.

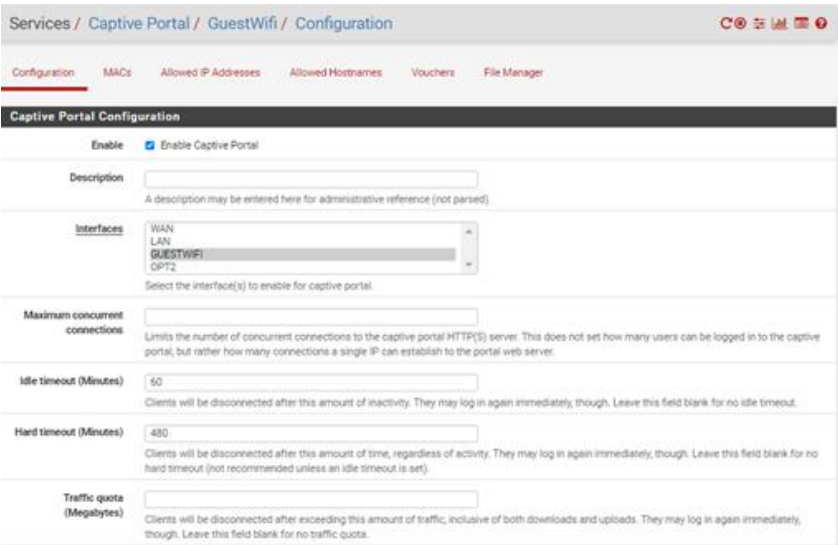
Para que o ip do gateway da rede guest fosse associado ao domínio estabelecido no certificado, é necessário ativar o DNS Resolver e definir um host, para que o ip seja retornado para o host com o domínio definido, como demonstra Figura 50.



**Figura 50-Host definido no DNS**


Feitos estes passos, a configuração do captive portal está pronta a ser realizada, em services encontra-se o serviço do captive portal já instalado na PfSense.

Sucessivamente, a configuração foi feita da seguinte maneira, começando pela ativação do serviço, é definida a placa em questão, é possível definir o número máximo de conexões que um ip consegue estabelecer ao serviço, o tempo definido por um período de inatividade do cliente, que neste caso foi selecionado um tempo de 60 minutos, é ainda selecionado um tempo que force a desconexão do utilizador, que optou-se por ficar um período de 480 minutos, um total de 8 horas. É também possível definir quantos megabytes os clientes conectados conseguem ter, de certa forma isto ajuda a melhorar o tráfego de rede, assim como a controlar a atividade que os utilizadores têm na internet, a presente configuração é demonstrada na Figura 51.



**Figura 51- Configuração do Captive Portal**

Foi verificada a opção de existir uma janela popup de logout para que eventualmente o utilizador queira fazer logout. Pode ser definido um link de pré autenticação, assim como um link para depois do utilizador se conectar. Filtragem por macs também é uma das possibilidades do captive portal, onde são definidos os macs que têm acesso ou mesmo os bloqueados. Por definição, existe um tipo de login da netgate, mas é possível configurar uma página html de raiz e inserir na configuração do captive portal. Foram inseridas ainda duas imagens, uma de fundo e uma de logotipo, apenas para dar outro ar ao portal configurado. Na Figura 52 é possível verificar os campos de configuração.

 Logout popup window ☒ Enable logout popup window  
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

---

Pre-authentication redirect URL   
Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal don't know where to redirect them. This field will be accessible through \$PORTAL\_REDIRECTURLS variable in captiveportal's HTML pages.

---

After authentication Redirection URL   
Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

---

Blocked MAC address redirect URL   
Blocked MAC addresses will be redirected to this URL when attempting access.

---

Concurrent user logins ☐ Disable Concurrent user logins  
If enabled only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.

---

MAC filtering ☐ Disable MAC filtering  
If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

---

Pass-through MAC Auto Entry ☐ Enable Pass-through MAC automatic additions  
When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the [MAC tab](#) or send a POST from another system. If this is enabled, the logout window will not be shown.

---

Per-user bandwidth restriction ☐ Enable per-user bandwidth restriction

---

Use custom captive portal page ☐ Enable to use a custom captive portal login page  
If set a portal.html page must be created and uploaded. If unchecked the default template will be used

**Figura 52- Configuração do Captive Portal 2**

O método de autenticação é outra opção a configurar, pois esta pode ser pelo AD, por utilizadores locais ou por vouchers. Para uma primeira fase de testes é recomendável o uso de um utilizador local. Tal como mostra a Figura 53.

**Authentication**

**Authentication Method** Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

**Authentication Server** AD  
Local Database

You can add a remote authentication server in the [User Manager](#).  
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

**Secondary authentication Server** AD  
Local Database

You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs.  
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

**Reauthenticate Users** ☐ Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

**Local Authentication Privileges** ☒ Allow only users/groups with "Captive portal login" privilege set

**Figura 53- Configuração da Autenticação do Captive Portal**

Por último, é escolhida a opção de permitir o login pelo https para tornar a conexão mais segura, pedindo o server https, assim como o certificado que foi definido, como mostra a Figura 54.

**HTTPS Options**

**Login** ☒ Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

**HTTPS server name** lucemplast.captive.com

This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

**SSL Certificate** lucemplast.captive.com

If no certificates are defined, one may be defined here: [System > Cert. Manager](#)

**HTTPS Forwards** ☐ Disable HTTPS Forwards

If this option is set, attempts to connect to SSL/HTTPS (Port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

[Save](#)

**Figura 54- Configuração do https login**

Além da capacidade de o login no portal ser feito por um utilizador local criado na firewall, foi adicionado outro método de conexão, o voucher, que nada mais é que um código gerado na hora para o utilizador se poder conectar. É uma das opções mais viáveis para conseguir definir o tempo que os utilizadores conseguem se conectar a uma determinada rede, podendo definir vários tipos de vouchers, com um número abrangido de utilizadores, para que cada utilizador tenha o seu próprio código.







→ ↻ ⚠ Não seguro | 192.168.3.1/services\_captiveportal\_vouchers.php?zone=guestwifi


**pfsense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / GuestWifi / Vouchers

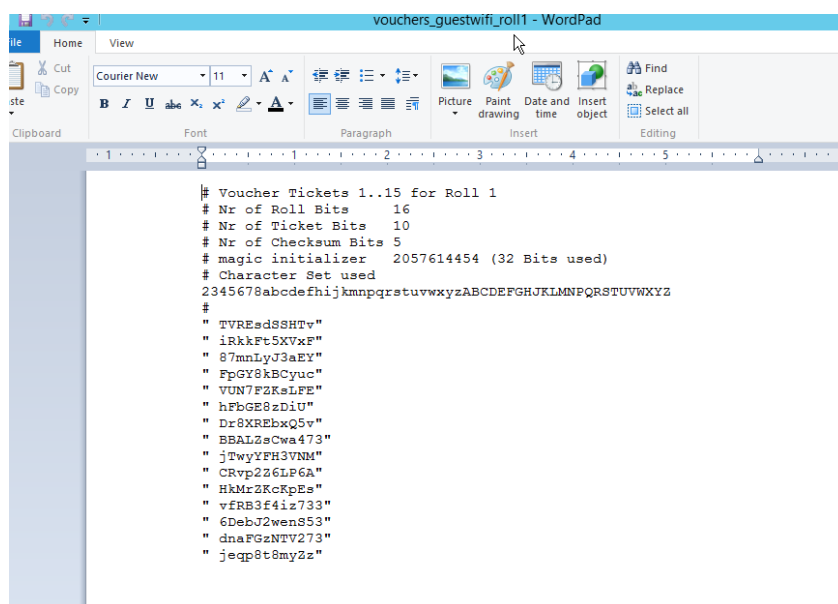
Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers File Manager

**Voucher Rolls**

Roll #	Minutes/Ticket	# of Tickets	Comment	Actions
0	120	15	Voucher de 2 horas para reunioes	  
1	480	15	Voucher para 8 horas	  

 Add

Para receber os códigos pretendidos basta o administrador fazer o download do ficheiro do voucher pretendido.



Basta fornecer qualquer um dos seguintes códigos exemplificados na Figura 56, para que o utilizador se conecte ao portal.

57

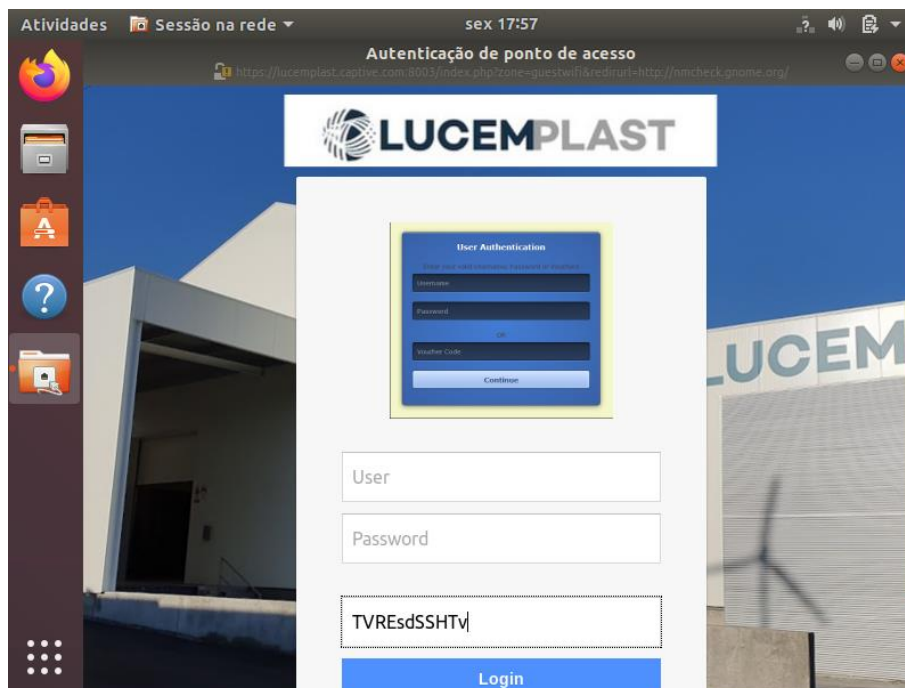
iria tomar e o ip do gateway da interface, da mesma forma foi inserido o DNS, tal como descreve a Figura 57.



The screenshot shows the 'Com fios' (Wired) network settings window for an IPv4 connection. The 'Método IPv4' (IPv4 Method) is set to 'Manual'. Under 'Endereços' (Addresses), the IP address is 192.168.4.4, the netmask is 255.255.255.0, and the gateway is 192.168.4.200. The 'DNS' section shows the DNS server set to 192.168.4.200, with the 'Automático' (Automatic) toggle switched on. The window has tabs for 'Detalhes', 'Identidade', 'IPv4', 'IPv6', and 'Segurança'.

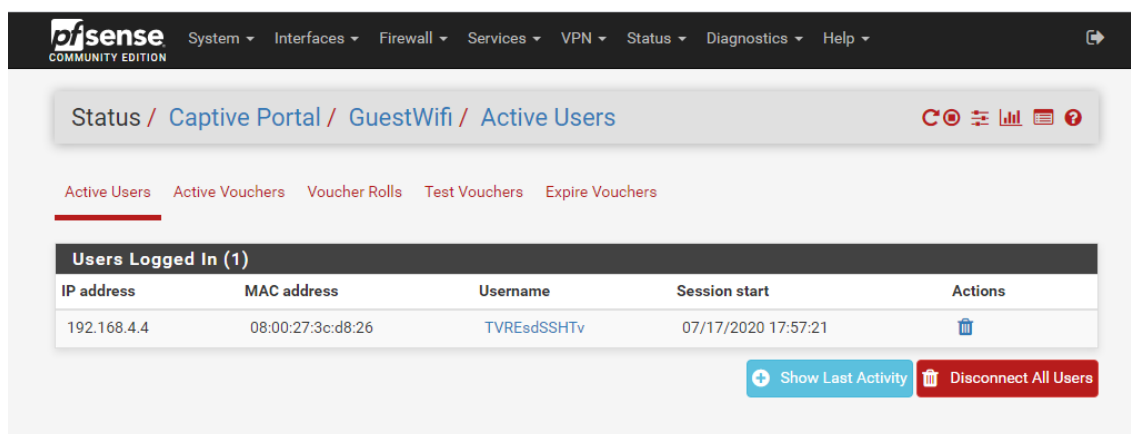
**Figura 57- Rede do Cliente Ubuntu**

Após a máquina estar definida na rede em questão, é acionada uma aplicação de rede do ubuntu em que mostra que é necessário efetuar uma ligação à rede para poder ter acesso à mesma. É ainda possível visualizar que o site é o definido no DNS e o portal é o que foi configurado. Para testar o acesso foi introduzido um dos códigos gerados pelo voucher, como mostra a Figura 58.



**Figura 58- Login no Captive Portal**

Efetuada o login o cliente já tem acesso à internet, podendo realizar qualquer operação desejada. É de salientar que o administrador da rede consegue visualizar todas as conexões efetuadas ao portal, assim como o ip que foi atribuído, o mac adress e a hora que está conectado, podendo desconectar o utilizador a qualquer momento, como mostra a Figura 59.



**Figura 59- Status dos utilizadores conectados ao Captive Portal**

## 2.10 MONITORIZAÇÃO

A monitorização do utilizador é uma função que é bastante pretendida pelas empresas, atualmente cada vez mais o rastreio de tudo o que o utilizador faz no tempo de útil de trabalho é bastante convencional e pretendido.

Existem várias ferramentas para monitorizar todo o tipo de tráfego na rede. A Pfsense por si só já tem um próprio sistema de logs para controlar toda a autenticação efetuada na rede. Como a Pfsense permite instalar certos pacotes de diversas ferramentas, é possível utilizar várias ferramentas de monitorização.

Este tipo de ferramentas pode ser usado para detetar vários tipos de ataques na rede assim como possíveis intrusos.



### **2.10.1 SNORT**

É uma ferramenta open source de prevenção de intrusões de rede, desenvolvido inicialmente em 1998 por Martin Roesch, fundador da Sorcefire. Este sistema é capaz de realizar uma análise em tempo real de todo o tráfego de rede, como ips, sites pesquisados, logins e todo o tipo de informação que o utilizador faça na internet.

A vantagem do Snort é a tecnologia nele presente faz com que ameaças urgentes sejam detetadas com bastante rapidez. Como por exemplo, o snort foi uma das ferramentas capazes de detetar uma vulnerabilidade no Equifax depois de um dia ter sido anunciada a ameaça a que esta estava exposta.

Uma das desvantagens é o facto de esta ferramenta ter sido desenvolvida há mais de 20 anos, estando capacitada para correr em infraestruturas antigas. Tornando muitas vezes difícil de detetar ameaças muito complexas e de alta velocidade.

Muitas das complicações surgiram com o IPV6 e do multi- threading, que veio a melhorar a velocidade dos processos. (Delfino, 2020) (Morgan, 2020)

### **2.10.2 SURICATA**

Este software foi introduzido em 2009, com a finalidade de conhecer vulnerabilidades de infraestruturas modernas.

O Suricata, assim como o Snort, também é baseado em regras, mas este tem introduzido multi-threading, que fornece a capacidade de processar mais regras em redes mais rápidas, com volumes de tráfego maiores, no mesmo hardware.

Esta ferramenta também incorporou a linguagem de script Lua, que forneceu maior flexibilidade para criar regras que identificam condições que seriam difíceis ou impossíveis com uma regra de Snort herdada. Em termos simples, isso permite que os utilizadores adaptem o Suricata às ameaças complexas que comumente enfrentam a empresa.

As desvantagens do Suricata é a sua instalação ser relativamente mais complexa e a comunidade ser relativamente menor em comparação com a do Snort. Para um trabalho futuro é aconselhável a instalação desta ferramenta. (Mott, 2020)

### **2.10.3 LIGHSQUID**

É um sistema de analisador de logs leve e rápido para o proxy Squid, analisa logs e é capaz de gerar relatórios html todos os dias se necessário, conseguindo resumir toda a atividade associada ao proxy.

Tal como já foi dito uma das vantagens desta ferramenta é ser leve e rápida, tornando-se mais adequada para sistemas menos desenvolvidos e com menos capacidade. É também de salientar que esta ferramenta tem um sistema de cache configurável e que por definição apenas guarda logs durante 5 semanas, para controlar o espaço em uso do disco. Estas configurações podem ser alteradas manualmente pelo administrador. (Kear, 2020)

## **2.11 VPNS**

VPN, ou Virtual Private Network, permite ao utilizador criar uma conexão privada e segura a outra rede através de uma rede pública.

Inicialmente as VPNs foram criadas para conectar redes de negócios com segurança através da internet ou permitir o acesso a uma rede comercial em casa.

Este tipo de conexão tem vários benéficos e um deles é o acesso remoto a recursos de rede local através de outra rede. (HOFFMAN, 2020)

Muitas vezes efetuar qualquer tipo de transação ou operação em uma rede WI-FI não segura, pode implicar expor certos tipos de dados privados. Uma rede virtual privada só traz benefícios a uma pessoa que se preocupa com a privacidade e segurança online.

Quando uma pessoa está conectada a uma rede publica Wi-Fi como uma rede de um café, ou aeroporto, qualquer tipo de operação relacionada com contas bancárias ou mesmo emails, não deve ser realizada, mas se por acaso acontecer a melhor maneira é através de um serviço VPN, para que os dados não fiquem vulneráveis a outras pessoas que estejam conectadas na mesma rede pública.

As VPNS criam um túnel de dados entre a rede local e a outra rede a que está conectada, permitindo mesmo que a conexão seja feita através de outro país ou região. Esta vantagem faz com que um certo tipo de liberdade online e conseguir aceder a certos tipos de aplicativos ou sites que não tem acesso na sua rede local.

Uma VPN faz também com que o histórico de navegação ou qualquer tipo de pesquisa realizada naquela rede seja oculta, fazendo com que atividade seja associada ao endereço IP do servidor VPN, assim como a própria localização do utilizador.

Existem diversos tipos de serviços VPN espalhados pela internet, sendo a maioria não gratuitos.

Um serviço deste tipo deve ser escolhido de acordo com as necessidades do utilizador. Uma vez que a privacidade do utilizador é prioridade máxima é necessário ter em atenção o tipo de serviço e fiabilidade do mesmo. Muitas vezes certos tipos de serviço podem ter políticas definidas para conseguir rastrear as atividades do utilizador, fazendo com que todo o tipo de operações que o utilizador pensa que estão a ser seguras estejam a ser registadas online.

Outro fator a ter em conta é se a própria conexão não restringe o limite de dados da largura de banda, pois pode acontecer o utilizador não usufruir da mesma largura de banda que tinha sem estar a usar a VPN. A localização também é uma circunstância que a pessoa deve ter em conta, pois o ping pode ser um fator influenciável nas necessidades do utilizador. Quanto mais longe for a localização mais lenta pode ficar a conexão à internet podendo limitar o trabalho do utilizador.

A quantidade de dispositivos que podem estar conectados à VPN também é um princípio a tomar atenção, pois de acordo com o que o utilizador pretende, se necessita de utilizar vários dispositivos ao mesmo tempo ou não.

O preço do serviço também é uma medida a ter em consideração, pois existem vários tipos de serviços e opções no mercado. Tal como foi dito anteriormente muitos dos serviços não são gratuitos, mas também pode depender do tempo de utilização que o utilizador pretende e do efeito para que é. Se for para uma necessidade empresarial ou mesmo uma necessidade que seja muito confidencial é melhor utilizar um serviço a pagar traz sempre mais vantagens e outro tipo de suporte. (Gervais, 2020)

### **2.11.1 ALGUNS EXEMPLOS DE VPNS NO MERCADO**

Norton Secure VPN, PureVPN, IPVanish , CyberGhost, NordVPN, ExpressVPN, etc.

O sistema operacional também é um fator muito relevante, pois nem todos os serviços são compatíveis com todos os sistemas operativos.

Ps: ping- é um utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos internos ou a própria conexão à internet. Sendo uma ferramenta fundamental para verificar o estado da rede.

### **2.11.2 TIPOS DE VPN**

Existem diversas topologias de VPNS, todas têm o objetivo de proteger a ligação do utilizador, mas muitas têm funcionalidades diferentes. Apenas irei falar de algumas topologias, mais concretamente das que tive oportunidade de trabalhar. (Daniels, 2020)

#### **2.11.2.1 OPEN VPN:**

É um servidor e cliente VPN open source compatível com vários sistemas operacionais e várias plataformas, incluindo o software em que foi desenvolvido o projeto, a Pfsense. Esta topologia pode também ser usada para configurações de VPN de acesso remoto site a site. Nada mais é que um software especificamente desenvolvido para VPNS. Atualmente é o protocolo VPN mais popular, não só devido a ter uma criptografia forte e de alta qualidade, mas também por ser de fácil configuração.

### **2.11.2.2 VANTAGENS E DESVANTAGENS DO OPENVPN**

Muito seguro.

Suportado por muitos softwares e praticamente todos os provedores de VPN modernos.

Suportado por quase todos os sistemas operacionais.

Amplamente testado e fiscalizado.

Às vezes necessita de software adicional.

### **2.11.2.3 PPTP:**

O point-to-point tunneling protocol, é um dos protocolos mais antigos do mercado. Chegando a ser o primeiro protocolo VPN a ser suportado pelo Windows.

A NSA (Agência de Segurança Nacional) estudou este protocolo e detetou várias falhas de segurança neste protocolo. A falta de criptografia de alto nível, foi um dos grandes motivos para este protocolo não ser considerado o mais seguro. Porém este protocolo é bastante rápido. Certas firewalls tentam bloquear os utilizadores de VPNS e os utilizadores PPTP são facilmente reconhecidos, tornando o protocolo nada eficiente.

### **2.11.2.4 VANTAGENS E DESVANTAGENS DO PPTP**

Muito rápido.

Simples e fácil de usar.

É compatível com praticamente todos os sistemas operacionais.

Oferece apenas uma criptografia básica.

Fácil de ser reconhecido e bloqueado por firewalls e similares.

Hackers geralmente exploraram as falhas de segurança do PPTP.

### **2.11.2.5 L2TP/IPSEC:**

Layer 2 Tunneling Protocol (L2TP) é um protocolo de encapsulamento usado para criar o chamado “túnel-VPN”, por onde os dados são transportados, no entanto, o L2TP em si não criptografa nenhum dado. É por isso que em praticamente todos os casos o L2TP é combinado com o protocolo IPSEC para criptografar os dados. Daí surge o nome L2TP/IPSEC.

IPSec (Internet Protocol Security) cuida da criptografia ponta-a-ponta dos dados no túnel L2TP.

Uma das desvantagens deste protocolo é que algumas firewalls bloqueiam também os utilizadores deste protocolo. Isto acontece porque o L2TP utiliza porta UDP 500 e alguns sites bloqueiam esta porta. Em relação à velocidade, o L2TP/IPSEC em si tem um bom desempenho, no entanto tem uma conexão mais lenta que o OPENVPN.

### **2.11.2.6 VANTAGENS E DESVANTAGENS DO L2TP/IPSEC**

Criptografia melhor que o PPTP.

Compatível com a maioria dos sistemas operacionais.

Mais lento que o OpenVPN.

De acordo com Snowden, a NSA explorou as vulnerabilidades na segurança deste protocolo. Este protocolo pode ser bloqueado por alguns firewalls.

Para terminar, ficou bem saliente a importância de um serviço VPN nas operações que um utilizador pode desempenhar e a segurança que as mesmas devem ter. Todos os protocolos e serviços VPNS têm as suas vantagens e desvantagens, tudo depende das necessidades do utilizador tal como foi referido. O OpenVPN é a melhor solução na maioria dos casos, se por alguma razão não for necessária a instalação deste serviço o IPSec é sempre uma boa opção.

## 2.11.3 TESTES REALIZADOS COM VPN

### 2.11.3.1 VPNS PARA UTILIZADOR LOCAIS

Por uma questão de praticar e testar, foi primeiramente definida uma VPN para utilizadores diretamente criados na firewall, com o objetivo de aperfeiçoar os conhecimentos para eventualmente passar para uma VPN com utilizadores diretamente conectados ao Active directory. (chrislazari, 2020)

Primeiramente foram criados um CA o e respetivo certificado correspondente, conforme Figura 60.

CAS Certificates Certificate Revocation

**Create / Edit CA**

**Descriptive name** PFSense\_RootCA

**Method** Create an internal Certificate Authority

**Internal Certificate Authority**

**Key length (bits)** 2048

**Digest Algorithm** sha256  
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

**Lifetime (days)** 3650

**Common Name** PFSense\_RootCA

The following certificate authority subject components are optional and may be left blank.

**Country Code** PT

**State or Province** Braga

**City** Braga

**Organization** Lucemplast

**Organizational Unit** Lucemplast

**Figura 60- Ca da VPN por utilizadores locais**

Tal como se pode verificar, foi definido, o método do certificado que neste caso é interno, o tamanho da chave, o algoritmo da chave que neste caso é o sha256 que vai servir de criptografia para a hash, o tempo que o CA dura, o nome que vai ficar conhecido pelo certificado, a abreviação do país, a organização e a cidade, tal como mostra a Figura 61.

CA's Certificates Certificate Revocation

### Add/Sign a New Certificate

**Method** Create an Internal Certificate

**Descriptive name** VPNServer\_Cert

### Internal Certificate

**Certificate authority** PFSense\_RootCA

**Key length** 2048

**Digest Algorithm** sha256  
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

**Lifetime (days)** 3650

**Common Name** VPNServer\_Cert

The following certificate subject components are optional and may be left blank.

**Country Code** PT

**State or Province** Braga

**City** Braga

**Organization** Lucemplast

**Organizational Unit** Lucemplast

**Figura 61- Certificado da VPN para utilizadores Locais**

Neste caso o tipo de certificado é definido como servidor para que mais que um utilizador se consiga ligar ao mesmo certificado, tal como mostra a Figura 62.

**Figura 62- Atributo do Certificado**

### Certificate Attributes

**Attribute Notes** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.  
For Internal Certificates, these attributes are added directly to the certificate as shown.

**Certificate Type** Server Certificate  
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

**Alternative Names** FQDN or Hostname  
Type Value  
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add + Add

Save

Para a criação da openVPN foi implementada uma wizard para utilizadores locais com as respetivas configurações, como demonstra a Figura 63.



Wizard / OpenVPN Remote Access Server Setup /

### OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

#### Select an Authentication Backend Type

Type of Server:

NOTE: If unsure, leave this set to "Local User Access."

[» Next](#)

**Figura 63- Configuração do tipo de servidor da VPN Local**

É selecionado o CA a que se destina, caso seja conveniente é possível criar um novo diretamente na wizard, ao selecionar a opção “Add new CA”, tal como mostra a Figura 64.

Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Step 5 of 11

### Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

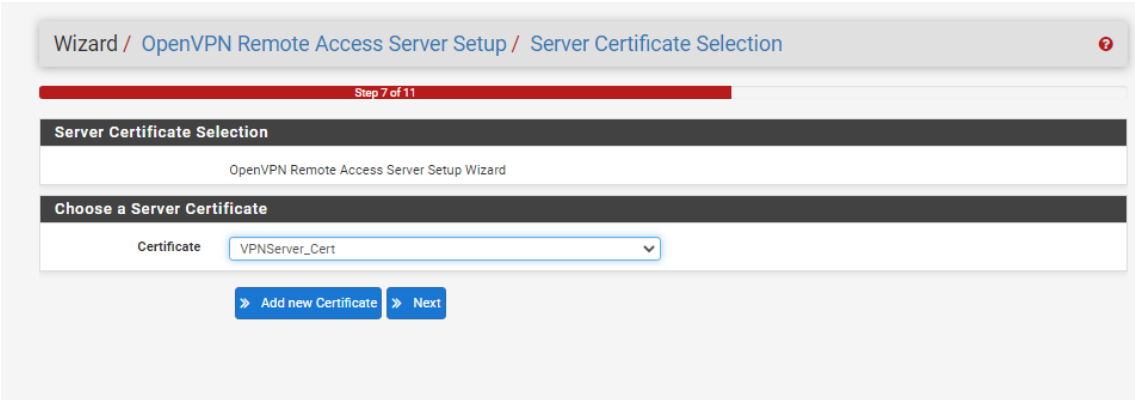
#### Choose a Certificate Authority (CA)

Certificate Authority:

[» Add new CA](#) [» Next](#)

**Figura 64- Adicionar o CA á VPN local**

De seguida é selecionado o certificado pretendido, que também é possível criar diretamente na wizard, como demonstra a Figura 65.

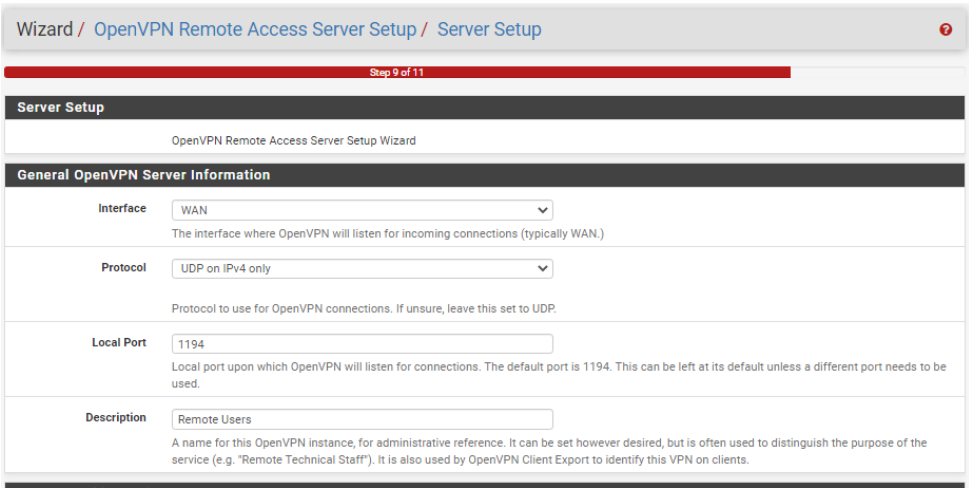


**Figura 65- Adicionar o certificado à VPN Local**

Estabelecidos o certificado e autoridade do certificado, é definida a configuração do servidor da openVPN ,com o tipo de interface desejada, que neste caso é pela WAN que os utilizadores vão comunicar entre si, o protocolo UDP, que vai ser o responsável pelo transporte de pacotes, a porta que vai permitir a conexão e o respetivo nome.

O protocolo definido, o UDP, apenas foi selecionado, porque para este caso era o mais conveniente para uma fase inicial de testes, onde apenas a conexão é prioridade e não tanto a informação que passa.

Num trabalho futuro, é recomendável o uso do protocolo TCP para uma conexão mais segura e fiável. A configuração realizada é possível verificar na Figura 66.



**Figura 66- Configuração da VPN Local**

Dentro da configuração do servidor da VPN, é necessário definir as definições de criptografia, que neste caso é definido que haja uma autenticação tls e seja gerada uma nova chave para cada conexão, como demonstra a Figura 67.

O protocolo tls vai ser responsável pela criptografia dos dados enviados pela internet, de modo a garantir segurança ao utilizador conectado.

**Cryptographic Settings**

**TLS Authentication** ☒ Enable authentication of TLS packets.

**Generate TLS Key** ☒ Automatically generate a shared TLS authentication key.

**TLS Shared Key**  Paste in a shared TLS key if one has already been generated.

**DH Parameters Length** 2048 bit  
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.

**Encryption Algorithm** AES-256-CBC (256 bit key, 128 bit block)  
The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.

**Auth Digest Algorithm** SHA256 (256-bit)  
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.

**Hardware Crypto** No Hardware Crypto Acceleration  
The hardware cryptographic accelerator to use for this VPN connection, if any.

**Figura 67- - Continuação da configuração da VPN Local**

O Que é o tlls?

O TLS é um protocolo criptográfico que fornece segurança de ponta a ponta dos dados enviados pela Internet. É principalmente para os utilizadores através de seu uso na navegação segura na Web e, em particular, no ícone de cadeado que aparece nos navegadores da Web quando uma sessão segura é estabelecida, uma ligação https. No entanto, também pode e deve ser usado para outras aplicações, como email, transferência de arquivos, vídeo / audioconferência, mensagens instantâneas e voz sobre IP, além de serviços de Internet como DNS e NTP. (internetsociety, 2020)

Como o TLS funciona?

O TLS usa uma combinação de criptografia simétrica e assimétrica, pois isso oferece um bom compromisso entre desempenho e segurança ao transmitir dados com segurança.

Com a criptografia simétrica, os dados são criptografados e descriptografados com uma chave secreta conhecida pelo remetente e pelo destinatário; tipicamente 128, mas de preferência 256 bits de comprimento (agora, menos de 80 bits é considerado inseguro).

A criptografia simétrica é eficiente em termos de computação, mas ter uma chave secreta comum significa que ela precisa de ser compartilhada de maneira segura.

A criptografia assimétrica usa pares de chaves - uma chave pública e uma chave privada. A chave pública está matematicamente relacionada à chave privada, mas, com o comprimento suficiente da chave, é impraticável computacionalmente derivar a chave privada da chave pública. Isso permite que a chave pública do destinatário seja usada pelo remetente para criptografar os dados que eles desejam enviar a eles, mas esses dados só podem ser descriptografados com a chave privada do destinatário.

É também selecionado o algoritmo de encriptação entre as duas redes, este é selecionado dependente do hardware em questão, por norma existe um predefinido, mas é possível mudar para um mais compatível com a máquina que é utilizada.

Caso seja necessário, é possível ainda adicionar um processo de aceleração na encriptação do hardware.

Na configuração do túnel é definida a rede responsável pela conexão do servidor com o cliente, que tem de ser uma rede diferente de qualquer rede que já esteja definida na firewall. Foi verificada a opção do “Redirect Gateway” para forçar a que todo o tráfego de dados seja gerado pelo túnel criado. É necessário selecionar a rede local definida, que normalmente é a rede LAN, que neste caso era a 192.168.2.0/24, é estabelecido o número de conexões que se podem conectar, o tipo de algoritmo que vai encriptar os dados pelo túnel, que neste caso foi definido por definição o OpenVPN. Era possível ainda permitir uma conexão entre os clientes no próprio servidor OpenVPN e assim permitir que o mesmo nome seja utilizado para várias conexões. A Figura 68 demonstra a configuração realizada.

Tunnel Settings	
Tunnel Network	<div>192.168.10.0/24</div> <div>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</div>
Redirect Gateway	<div><input checked="" type="checkbox"/></div> <div>Force all client generated traffic through the tunnel.</div>
Local Network	<div>192.168.2.0/24</div> <div>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</div>
Concurrent Connections	<div>15</div> <div>Specify the maximum number of clients allowed to concurrently connect to this server.</div>
Compression	<div>Omit Preference (Use OpenVPN Default)</div> <div>Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</div>
Type-of-Service	<div><input type="checkbox"/></div> <div>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</div>
Inter-Client Communication	<div><input type="checkbox"/></div> <div>Allow communication between clients connected to this server.</div>
Duplicate Connections	<div><input type="checkbox"/></div> <div>Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.</div>

Figura 68- Definição da rede local da VPN e da rede do Túnel

Dentro das definições do cliente foi definido o domínio do servidor assim como o DNS estabelecido pela firewall, como mostra a Figura 69.

The image shows two sections of a web interface for OpenVPN client configuration. The top section, titled "Client Settings", has a "Dynamic IP" checkbox checked with the text "Allow connected clients to retain their connections if their IP address changes." Below it, the "Topology" dropdown is set to "Subnet - One IP address per client in a common subnet", with explanatory text about IP address allocation. The bottom section, titled "Advanced Client Settings", includes "DNS Default Domain" (checked, value: "network.local"), "DNS Server enable" (checked, with text "Provide a DNS server list to clients. Addresses may be IPv4 or IPv6."), and "DNS Server 1" (value: "192.168.2.1").

Figura 69- Configuração do DNS e do Domínio

Por fim, é criada uma firewall rule para cada interface que irá ser utilizada para a conexão da VPN, que neste caso é a interface WAN que vai servir de rede pública e a OpenVPN para a o túnel. Estas regras vão permitir as conexões entre o cliente e o servidor em qualquer parte, assim como o tráfego gerado passe pelo túnel. A Figura 70 mostra criação das regras abordadas.

The image shows a "Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration" screen, labeled "Step 10 of 11". It contains two main sections: "Traffic from clients to server" and "Traffic from clients through VPN". In the first section, a "Firewall Rule" checkbox is checked with the description "Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet." In the second section, an "OpenVPN rule" checkbox is checked with the description "Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel." A "Next" button is at the bottom.

Figura 70- Regras de Firewall estabelecidas pela VPN

Realizadas as configurações é necessário criar um utilizador responsável para esta conexão e a ferramenta que irá permitir fazer o download do ficheiro configurado. A ferramenta utilizada para o download vai ser a openVPN cliente export utility. Para proceder a este download basta pesquisar a ferramenta diretamente no “Package Mannager” da Pfsense.

Procedendo à criação do utilizador, no campo “User Mannager”, foi criado um utilizador denominado VPN e definida uma palavra-passe. Era possível ainda definir os privilégios deste utilizador dentro interface gráfica da firewall, tal como demonstra a Figura 71.

The screenshot shows the 'Edit' page for a user in the Pfsense User Manager interface. The breadcrumb trail is 'System / User Manager / Users / Edit'. The 'Users' tab is selected. The 'User Properties' section includes the following fields:

- Defined by:** USER
- Disabled:** ☐ This user cannot login
- Username:** VPN
- Password:** Two masked password fields.
- Full name:** VPN
- Expiration date:** A date picker field with a note: 'Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY'.
- Custom Settings:** ☐ Use individual customized GUI options and dashboard layout for this user.
- Group membership:** A dropdown menu showing 'admins'.
- Certificate:** ☒ Click to create a user certificate

At the bottom of the group membership section, there are buttons: 'Move to "Member of" list' and 'Move to "Not member of" list'. A note below states: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.'

**Figura 71- Criação do Utilizador VPN na firewall**

É estabelecido o certificado, assim como o tempo de vida e o tamanho da chave, tal como mostra a Figura 72.

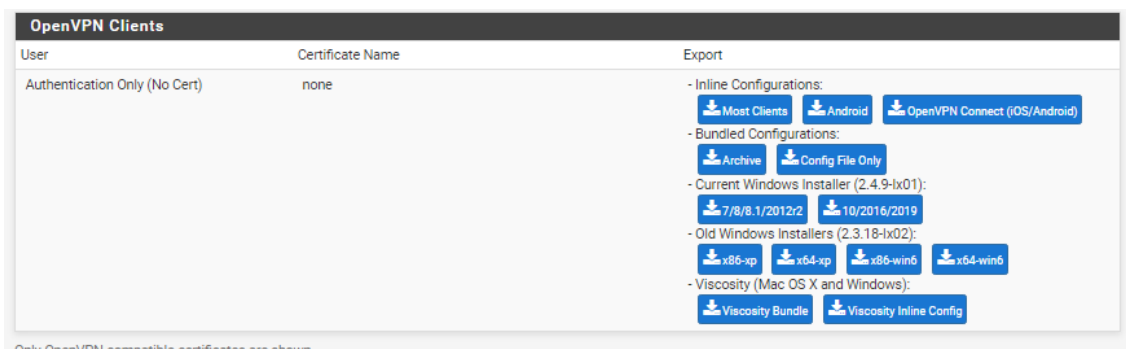
The screenshot shows the 'Create Certificate for User' page in the Pfsense interface. The fields are as follows:

- Descriptive name:** VPN\_User\_Cert
- Certificate authority:** PFSense\_RootCA
- Key length:** 2048 bits. A note below states: 'The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](http://keylength.com).'
- Lifetime:** 3650
- Keys:**
  - Authorized SSH Keys:** A large text area for entering authorized SSH keys.
  - IPsec Pre-Shared Key:** A text field for entering the IPsec pre-shared key.

A 'Save' button is located at the bottom of the page.

**Figura 72- Definir o certificado do utilizador Local**

Instalado o “open VPN client export utility”, apenas basta efetuar o download para o cliente destinado, tal como é possível verificar na Figura 73.

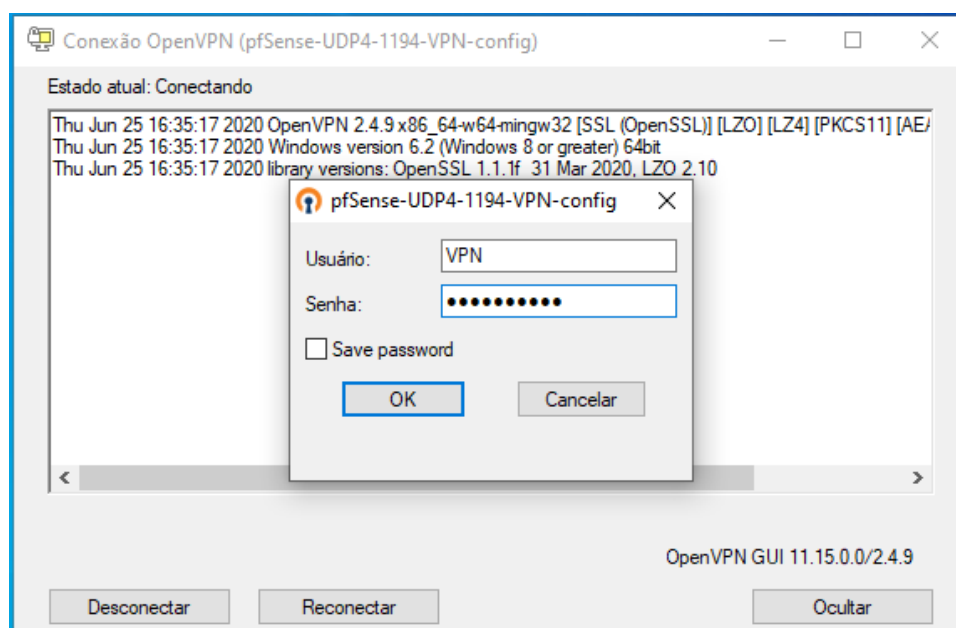


**Figura 73- Download do ficheiro de configuração da VPN Local**

Dependendo do sistema operativo do cliente, é possível realizar o download do ficheiro. Neste caso o cliente testado tem o Windows 10 como sistema operativo.

Realizado o download do ficheiro no cliente, procede-se a instalação da aplicação, em que apenas é necessário dar permissão para instalar, uma vez que o ficheiro de download já vem com a configuração definida.

Com a instalação bem sucedida, para o cliente se conectar ao serviço VPN é pedido as credenciais do utilizador, que são as do utilizador criado na firewall, tal como mostra a Figura 74.



**Figura 74- Login do utilizador Local**

Tal como se pode visualizar, a conexão foi bem estabelecida, onde é possível verificar o certificado estabelecido, a rede wan responsável por estabelecer o servidor e o cliente, e o ip que ficou definido na rede a que se conectou, neste caso o 192.168.10.2, como mostra a Figura 75.

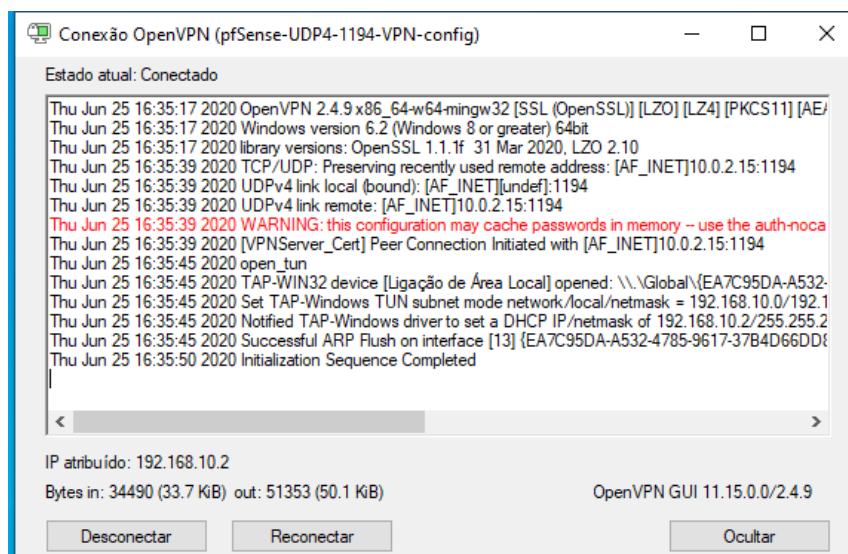


Figura 75- Conexão da VPN local estabelecida

A Figura 76, mostra o comando “ipconfig”, realizado no cliente que está conectado à VPN, onde é possível mais uma vez, verificar que a rede a que o cliente se conectou foi a rede estabelecida na configuração do túnel da VPN.

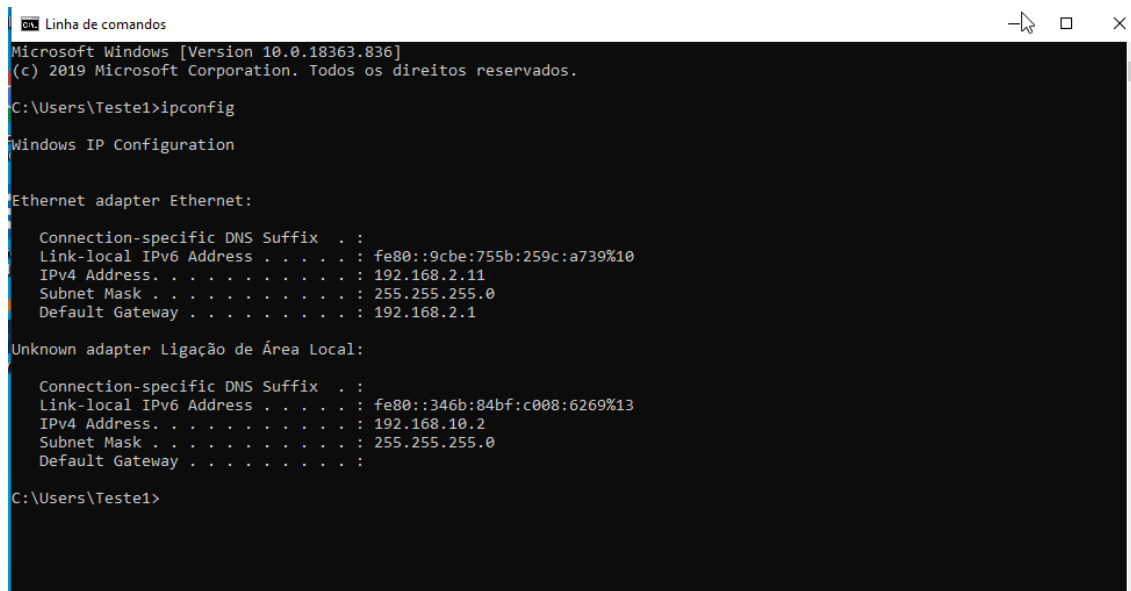


Figura 76- Ipconfig do cliente para verificar que a rede VPN está conectada



### 2.11.3.2 VPN PARA UTILIZADORES DO AD

Testadas as configurações da VPN para utilizadores locais, passou-se para conexões através do Active Directory. (Vorkbaard, 2020)

Primeiramente foi criada uma Unidade Organizacional (OU) denominada VPN, para todos os utilizadores que fossem a fazer uma possível conexão, a criação da OU não é uma questão relevante para a conexão funcionar, apenas foi criada por uma questão de organização, também era possível a criação de um grupo para distinguir os utilizadores.

Dentro da “OU” VPN foi criado um utilizador “VPNTeste”, que irá ser responsável por dois fatores, um deles irá ser a conexão do AD com a firewall para uma gestão dos utilizadores e neste caso também irá servir para a ligação ao servidor OpenVPN. A Figura 77 demonstra a criação do utilizador VpnTeste na Unidade Organizacional VPN.

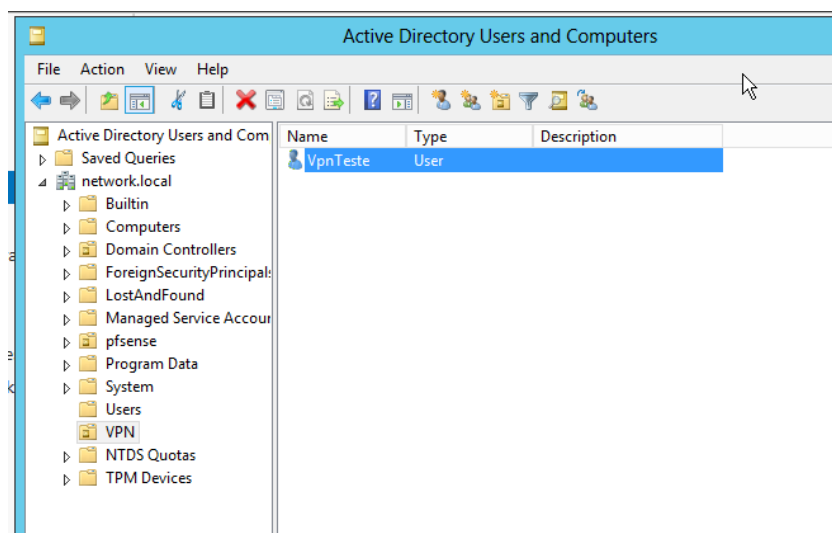


Figura 77- Utilizador VPNTeste no AD

Criado o utilizador no servidor, é necessário prosseguir para a configuração e autenticação de utilizadores do AD com a firewall. É necessário criar um CA e um certificado para esta conexão, tal como foi efetuado na VPN para utilizadores locais.

Tal como se pode verificar na Figura 78, é necessário seleccionar o tipo de conexão que irá ser estabelecida entre o AD e a firewall, que neste caso em concreto é o LDAP, o ip definido é o ip do servidor, a porta 389 é a utilizada por um serviço LDAP, o TCP como protocolo de transporte, esta conexão é para manutenção de utilizadores.

The screenshot shows a web interface for configuring an authentication server. The breadcrumb trail is 'System / User Manager / Authentication Servers / Edit'. There are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers', with 'Authentication Servers' being the active tab. The main content area is titled 'Server Settings' and contains the following fields:

- Descriptive name:** Active Directory
- Type:** LDAP (dropdown menu)
- LDAP Server Settings:**
  - Hostname or IP address:** 192.168.2.100 (with a note: 'NOTE: When using SSL or STARTTLS, this hostname MUST match the Common Name (CN) of the LDAP server's SSL Certificate.')
  - Port value:** 389
  - Transport:** TCP - Standard (dropdown menu)
  - Peer Certificate Authority:** VPN\_CA (with a note: 'This option is used if 'SSL Encrypted' or 'TCP - STARTTLS' options are chosen. It must match with the CA in the AD otherwise problems will arise.')
  - Protocol version:** 3 (dropdown menu)
  - Server Timeout:** 25 (with a note: 'Timeout for LDAP operations (seconds)')
  - Search scope:** Level (dropdown menu)
    - Entire Subtree:** (dropdown menu)
    - Base DN:** DC=network,DC=local

**Figura 78- Autenticação do servidor à firewall para manutenção de utilizadores**

É ainda definido o domínio do servidor, o caminho da OU VPN e as credenciais do utilizador em questão. O samAccountName é o tipo de nome atribuído ao utilizador para clientes do servidor, é possível verificar este nome com a ferramenta ADSI do Windows server. O nome de grupo que é do tipo CN, que representa “common name”, “memberOf” retrata o atributo definido no LDAP para o caminho do cliente, o “posixGroup” é um tipo de classe de objeto para um grupo de dados do LDAP, que é selecionado por definição. A Figura 79 demonstra a configuração realizada.

<b>Authentication containers</b>	<input type="text" value="OU=VPN,DC=network,DC=local"/> <input type="button" value="Select a container"/>
	<small>Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers</small>
<b>Extended query</b>	<input type="checkbox"/> Enable extended query
<b>Bind anonymous</b>	<input type="checkbox"/> Use anonymous binds to resolve distinguished names
<b>Bind credentials</b>	<input type="text" value="VpnTeste"/> <input type="password" value="*****"/>
<b>User naming attribute</b>	<input type="text" value="samAccountName"/>
<b>Group naming attribute</b>	<input type="text" value="cn"/>
<b>Group member attribute</b>	<input type="text" value="memberOf"/>
<b>RFC 2307 Groups</b>	<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership <small>RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).</small>
<b>Group Object Class</b>	<input type="text" value="posixGroup"/> <small>Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".</small>
<b>UTF8 Encode</b>	<input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server. <small>Required to support international characters, but may not be supported by every LDAP server.</small>
<b>Username Alterations</b>	<input type="checkbox"/> Do not strip away parts of the username after the @ symbol <small>e.g. user@host becomes user when unchecked.</small>

**Figura 79- Continuação da Autenticação do servidor à firewall para manutenção de utilizadores**

Criado o utilizador e estabelecida a conexão, é necessário proceder para a configuração da VPN. Nesta é necessário definir uma wizard do tipo LDAP responsável pela criação do servidor OpenVPN. (Stefan, 2020)

Na seguinte configuração é selecionado o tipo de servidor, o “Remote Access (User Auth)”, que apenas serve para acesso remoto, num ambiente de testes é uma opção fiável, caso seja implementada num ambiente real, é adequado mudar para um servidor “Remote Access + Tls” de modo a estabelecer uma conexão mais segura, onde é necessário instalar o certificado de cada utilizador e o do servidor, por definição este modo de servidor já é o selecionado. O protocolo utilizado, o UDP apenas em IPV4 para não permitir conexões pelo IPV6, relembro que para uma maior segurança de pacotes o protocolo TCP é o ideal. O tipo de túnel que irá ser configurado, a rede WAN, que irá ser responsável por fazer a conexão da rede do servidor VPN com o cliente, a porta 1194 que é a porta utilizada pelo OpenVPN para receber conexões dos clientes e uma descrição para o administrador perceber do que se trata. A Figura 80 demonstra a configuração realizada no servidor de VPN.

**Pfsense** COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

### General Information

**Disabled** ☐ Disable this server  
Set this option to disable this server without removing it from the list.

**Server mode** Remote Access ( User Auth ) ▾

**Backend for authentication** Active Directory ▾  
Local Database ▾

**Protocol** UDP on IPv4 only ▾

**Device mode** tun - Layer 3 Tunnel Mode ▾  
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

**Interface** WAN ▾  
The interface or Virtual IP address where OpenVPN will receive client connections.

**Local port** 1194  
The port used by OpenVPN to receive client connections.

**Description** VPN  
A description may be entered here for administrative reference (not parsed).

**Figura 80- Configuração da VPN para utilizadores do AD da PfSense**

O protocolo responsável pela encriptação dos dados entre as duas redes estabelecidas é o TLS, para garantir segurança nos dados enviados pela internet, tal como já foi referido. A rede definida foi exatamente a mesma que na criação da VPN local, com o túnel na rede 192.168.10.0/24 e a rede Local como 192.168.2.0/24 que corresponde à rede LAN. É também definido o domínio e o DNS do servidor para que os utilizadores consigam aceder ao servidor, tal como mostra a Figura 81.

**Duplicate Connection** ☐ Allow multiple concurrent connections from clients using the same Common Name.  
(This is not generally recommended, but may be needed for some scenarios.)

### Client Settings

**Dynamic IP** ☒ Allow connected clients to retain their connections if their IP address changes.

**Topology** Subnet - One IP address per client in a common subnet ▾  
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.  
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

### Advanced Client Settings

**DNS Default Domain** ☒ Provide a default domain name to clients

**DNS Default Domain** network.local

**DNS Server enable** ☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

**DNS Server 1** 192.168.2.1

**Figura 81- Continuação da configuração da VPN para utilizadores do AD da PfSense**

Feitas as configurações, são criadas duas firewall rules tal como na VPNLocal, onde é dada a permissão para que os utilizadores consigam passar pela rede wan justamente pela porta 1194 e com o protocolo UDP, como mostra a Figura 82.

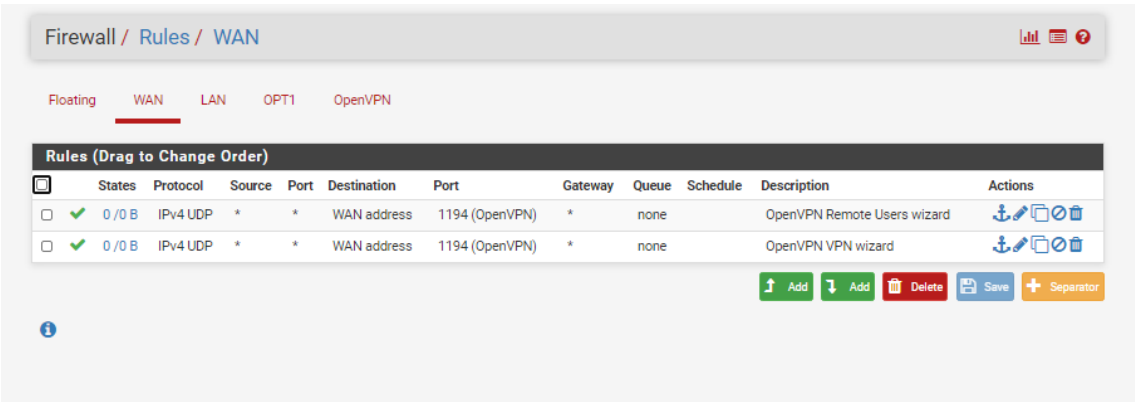


Figura 82- Firewall Rules da Wan para permitir o acesso remoto dos utilizadores da VPN

Realizadas todas as configurações, é necessário mais uma vez fazer o dowload da configuração para o sistema desejado, através da ferramenta cliente export, como mostra a Figura 83.

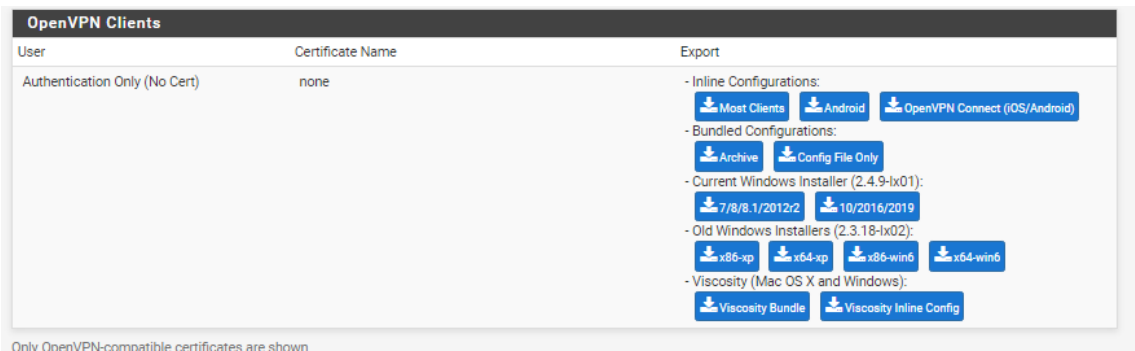
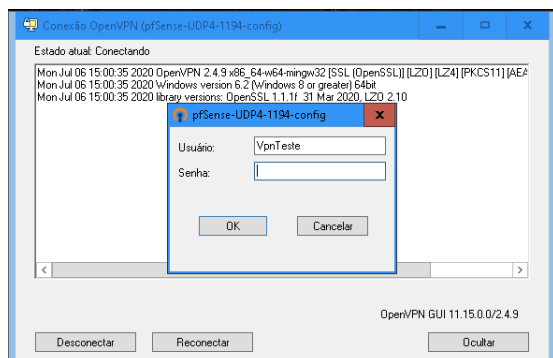


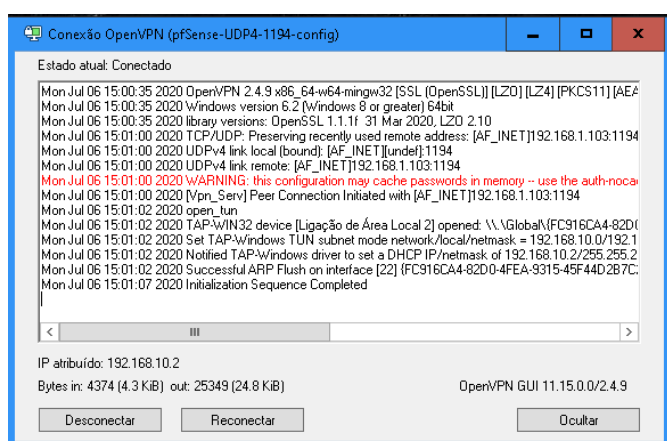
Figura 83- Download da ferramenta de instalação da VPN

Instalada a openVPN com a configuração desejada, é pedido ao cliente que insira as credenciais do utilizador definido, tal como demonstra a Figura 84.



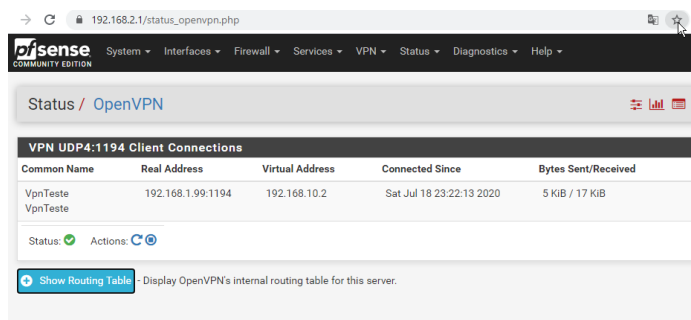
**Figura 84- Login do utilizador na VPN pelo AD**

Apenas utilizadores criados na OU definida no servidor irão ter acesso à VPN, qualquer utilizador que não esteja inserido nessa OU a conexão não vai ser estabelecida. A Figura 85, mostra a conexão bem sucedida pelo utilizador, onde o cliente acede à rede Wan pela rede do túnel definido.



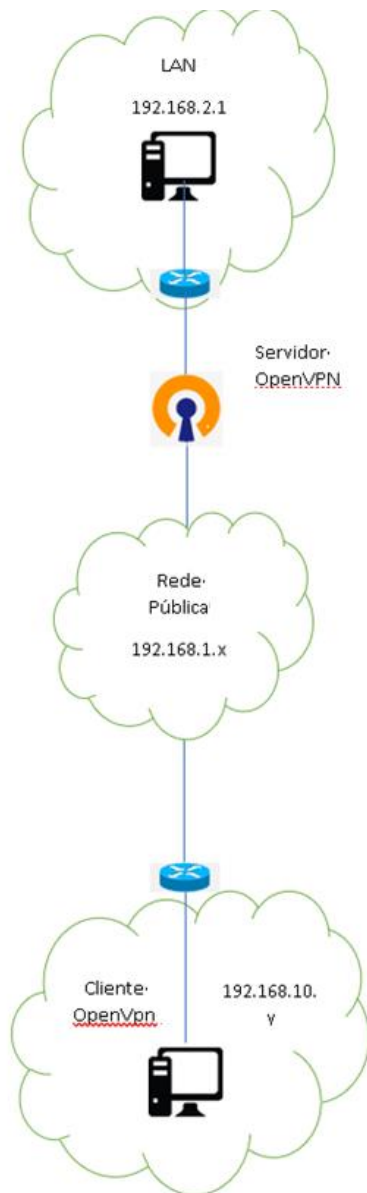
**Figura 85- Conexão estabelecida da VPN pelo AD**

É possível verificar a conexão através dos status da OpenVPN na Pfsense, tal como mostra a Figura 86.



**Figura 86- Verificação da conexão VPN na Pfsense**

#### 2.11.4 ESQUEMA DE REDE DA VPN



**Figura 87- Esquema de Rede da VPN**

O esquema referente à Figura 87, retrata como a vpn foi estabelecida na firewall, onde a rede LAN, que corresponde à rede principal da firewall, tem um servidor VPN instalado dentro dessa rede, que vai ser responsável por encaminhar a rede do cliente por um túnel de rede, neste caso com rede 192.168.10.0/24, ligado à rede WAN. A comunicação das duas redes, a da LAN e do cliente, vai ser feita pela rede WAN, que funciona como um IP público.

## 2.12 ENDLESS OS

É um sistema operativo baseado em linux que proporciona uma utilização simples ao utilizador.

Este sistema vem com mais de 100 aplicações gratuitas sem ser necessário o acesso à internet.

Tal como já foi referido este sistema operativo é feito com o propósito de ser simples de usar para qualquer pessoa, seja com experiência em computadores ou não.

O download deste sistema operativo é totalmente gratuito e todas as atualizações são automáticas.

Esta distribuição tem um ambiente de trabalho baseado em Gnome3.

O EndlessOs tem uma interface muito parecida com a do android, tornando mais apelativo e interativo a utilização deste sistema.

Tem uma plataforma específica denominada de AppCenter com centenas de aplicações disponíveis e milhares de artigos Wikipédia.

Embora não se possa fazer qualquer instalação de alguma aplicação que esteja fora do AppCenter. (Sohail, 2020)

Endless é uma empresa americana de informação tecnológica que desenvolve o sistema operativo EndlessOs e todo o sistema de hardware necessário.

Esta empresa foi fundada em maio de 2011 em São Francisco, Califórnia por Matthew Dalio e Marcelo Sampaio.

Nos primeiros 3 anos a empresa realizou projetos de pesquisa em Rocinha, uma favela no Rio de Janeiro, com a intenção de se expandir.

Em abril de 2015, a empresa foi lançada para o público em geral por meio de uma campanha na plataforma de crowdfunding Kickstarter (uma corporação de benefício ao público com uma plataforma focada na criatividade).



Em novembro de 2015, a Endless começou a vender computadores nas lojas da Claro na Guatemala. Antes disso, o produto estava sendo vendido em quiosques próprios. Janeiro de 2016 marcou o lançamento do Endless Mini.

A primeira versão pública foi o Endless OS 2.1.0 em julho de 2014. Em meados de dezembro de 2017, o Endless OS 3.3.6 foi lançado. A versão mais recente do Endless OS é 3.7.7, lançada em 10 de fevereiro de 2020.

### **2.12.1 UTILIZAÇÃO DESTA DISTRIBUIÇÃO**

A empresa optou por utilizar este sistema operativo em muitas das suas máquinas de trabalho, pelo simples facto de ficar uma solução muito mais económica, do que estar a ter de comprar serviços para todas as máquinas.

Uma vez que as distribuições linux são grátis e muitas das máquinas são touch, quando foi encontrada uma distribuição com uma interface android foi juntar 2 em 1.

### **2.12.2 VANTAGENS E DESVANTAGENS**

Ser grátis é sem dúvida uma vantagem para com outro tipo de sistemas operativos.

O facto de ser simples de usar e mesmo muito interativa para o utilizador também é uma vantagem.

Nem sempre são encontradas aplicações com suporte para este sistema operativo.

As drives de certos tipos de hardware têm de ser manualmente instaladas e algumas nem são mesmo compatíveis.

Ser um sistema de código aberto também permite que exista alguma liberdade ao utilizador de pesquisar, modificar ou estudar

o código fonte para qualquer finalidade.

A nível de suporte de pesquisa para este sistema operativo em concreto também há pouca documentação.

Ter bastantes aplicações grátis

O EndlessOs é algo realmente diferente da maioria das distribuições Linux. Não é para os entusiastas comuns do Linux, mas sim para países em desenvolvimento, pessoas sem acesso à Internet e pessoas que não desejam ou precisam do controle ou poder normal oferecido pela maioria das distribuições . Com sua experiência no estilo Android, é bastante simples, fácil de usar. (Marsh, 2020) (Sohail, 2020)

Esta página foi propositadamente deixada em branco.

## **CAPÍTULO 3 OUTRAS TAREFAS DESEMPENHADAS**

### **3.1 SOFTWARE DE GESTÃO E MANUTENÇÃO**

O Valuekeep é uma solução de software de gestão da manutenção que simplifica o planeamento, agiliza a execução e aumenta o controlo das ações realizadas quer pelas equipas internas, quer pelos técnicos subcontratados.

Na minha opinião, trata-se de um software em cloud capaz de guardar e simular todo o tipo de dados referente a um processo de manutenção, desde gestão de ativos, gestão de manutenção, etc. e gestão das mesmas.

Basta um equipamento com ligação à internet para aceder ao sistema e gerir rapidamente os processos de manutenção. Ao aderir à solução acede a um serviço completo que lhe garante também a manutenção e atualização contínua do sistema.

### **3.2 PRINCIPAIS FUNCIONALIDADES:**

-Máxima acessibilidade

Uma vez que não é preciso fazer a instalação do software basta ter um dispositivo com acesso à internet para poder controlar o sistema.

-Reporte de trabalho a partir de qualquer dispositivo móvel

A partir de qualquer dispositivo com acesso à internet os técnicos podem reportar qualquer tipo de operação executada, desde registo de avarias, identificação de sintomas, causas e ações a desenvolver, registo do tempo de mão-de-obra consumido, ect.

-Profundidade de controlo de custos

Com esta solução também é possível encontrar uma estrutura detalhada dos gastos de cada intervenção, desde as despesas com mão de obra, deslocações, etc.

-Rapidez e eficiência na gestão administrativa da manutenção

Com isto as operações são aceleradas e a fluidez dos processos é promovida, desde o cadastro, caracterização e localização dos objetos de Manutenção; passando pelo planeamento, e controlo de execução das intervenções.

-Informação analítica preciosa para a tomada de decisão

A informação de gestão disponibilizada permite avaliar, com elevado grau de precisão, a disponibilidade dos ativos ao longo do tempo.

### 3.3 TAREFAS DESEMPENHADAS

Foram desenvolvidos conhecimentos a nível de manutenção e gestão de tarefas e artigos assim como todos os processos relativos ao software, desde criação de ativos, criação de tarefas, planos de manutenção, ocorrências, etc, tal como mostra as Figura 88 .

Estes conhecimentos e aplicação de diversas tarefas no software fizeram com que eu ficasse uma pessoa instruída e capaz de trabalhar neste software.

Por motivos de segurança e proteção de dados não foram tirados prints ao trabalho realizado neste software. Para além das imagens mostradas, foram criados outros tipos de dados no software.

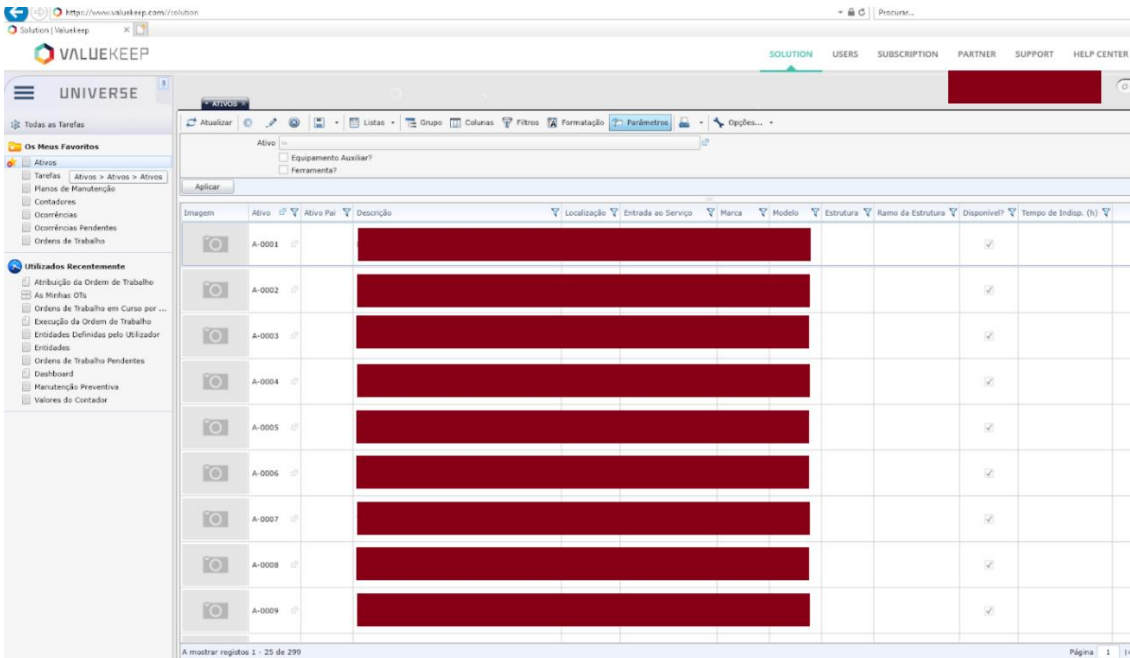


Imagem	Ativo	Ativo Pai	Descrição	Localização	Entrada ao Serviço	Marca	Modelo	Estrutura	Ramo da Estrutura	Disponível?	Tempo de Indisp. (h)
	A-0001									✓	
	A-0002									✓	
	A-0003									✓	
	A-0004									✓	
	A-0005									✓	
	A-0006									✓	
	A-0007									✓	
	A-0008									✓	
	A-0009									✓	

Figura 88- Ativos criados no ValueKeep

## PANDEMIA

Com a pandemia, eu e o meu colega de estágio, vimo-nos obrigados a vir para casa durante um período por uma questão de segurança.

Conseguimos manter sempre contacto com a empresa, ficando estipulado o teletrabalho durante este período.

Neste período foi desenvolvido bastante trabalho de pesquisa referente ao projeto.

Apesar de termos estado em teletrabalho, posso afirmar que a pandemia só veio a provocar desvantagens no estágio, isto porque perdi algumas atividades presenciais importantes que só vinham a ajudar no meu desenvolvimento profissional. Desde tarefas mínimas, a acompanhar futuros projetos na empresa que estavam a ser desenvolvidos na altura. Foi ainda criado um ambiente de laboratório, pois era um necessário uma máquina capaz de aguentar todo o laboratório implementando e ainda a partilha de acra para uma possível reunião.

Após um tempo em teletrabalho, garantiu-se que existiam as condições e as medidas necessárias para voltar ao trabalho presencial.

## CONCLUSÃO

A implementação de uma firewall/sistema de controlo de tráfego de rede é bastante útil para controlar os acessos à internet dos funcionários, ou mesmo dos acessos de fora e tudo o que se passa na rede. Não só por estes fatores, mas também para manter a empresa muito mais segura a nível informático.

O estágio foi muito gratificante, pois representou de certa forma o meu primeiro contacto relativamente à área de segurança informática no mundo empresarial. Durante estes meses, pude trabalhar numa área que me agrada bastante e desenvolver conhecimentos de diferentes pontos da informática, a nível de controlo e proteção de rede, de gestão de um servidor, de VPNs, de partilha de ficheiros entre diferentes sistemas operativos, entre outros conhecimentos que contribuíram para o meu desenvolvimento profissional. Ao longo deste percurso foram ultrapassadas diversas dificuldades, com a tentativa de ir ao máximo ao encontro do que era pedido. Foram desenvolvidas capacidades de trabalho, métodos de organização e sobretudo o fortalecimento da vontade de superação.

A segurança informática sempre foi uma área que me fascinou e que sempre tive curiosidade de aprender, contudo sei que não se trata de uma área fácil e que está em constante evolução, mas só me motiva a aprender e a saber mais.

O facto de se ter escolhido um software que eu não tinha muito conhecimento, fez com que houvesse um trabalho de pesquisa a fundo sobre este software e de várias maneiras de realizar diversos problemas.

Ainda relativamente à Pfsense foram encontradas algumas limitações durante o desenvolvimento do projeto, uma delas foi na configuração de uma página de login no captive portal, pois o código de desenvolvimento web nem sempre era detetado corretamente limitando a criação da página.

Ao mesmo tempo que as o projeto era implementado, também houve o cuidado de se perceber que podia ter sido realizado de diferentes maneiras, como por exemplo o controlo de tráfego ser feito todo pelo captive portal.

De futuro pode ser aplicado o protocolo Wpad, que é o protocolo responsável pela deteção automática de proxy nos browsers, fazendo com que os utilizadores possam sair e entrar sem ter de estar sempre a dar login. Outra configuração importante é definir no router o ip da VPN e as portas de tcp e udp para que possa existir uma conexão de qualquer ponto do mapa.

## REFERÊNCIAS

- Becher, J. (Acedido em maio de 2020). Obtido de <https://jimiz.net/2014/11/ipfire-pfsense-firewall-review/>
- Bhardwaj, R. (Acedido em maio de 2020). *what-is-a-network-bridge*. Obtido de networkinterview.com: <https://networkinterview.com/what-is-a-network-bridge/>
- chrislazari. (Acedido em junho de 2020). *pfsense-setting-up-openvpn-on-pfsense-2-4*. Obtido de chrislazari.com: <https://chrislazari.com/pfsense-setting-up-openvpn-on-pfsense-2-4/>
- Daniels, N. (Acedido em junho de 2020). *informacoes-sobre-vpn/protocolos-vpn*. Obtido de vpnoverview.com: <https://vpnoverview.com/pt/informacoes-sobre-vpn/protocolos-vpn/>
- Delfino, P. (Acedido em maio de 2020). Obtido de <https://e-tinet.com/linux/snort-monitor-redes/>
- DeMeyer, Z. (Acedido em maio de 2020). *ldap-vs-radius#cookie-accept*. Obtido de jumpcloud.com: <https://jumpcloud.com/blog/ldap-vs-radius#cookie-accept>
- DomiStyle. (Acedido em maio de 2020). Obtido de [https://www.reddit.com/r/homelab/comments/577rfl/ipfire\\_vs\\_pfsense/](https://www.reddit.com/r/homelab/comments/577rfl/ipfire_vs_pfsense/)
- Gervais, J. (Acedido em junho de 2020). *internetsecurity-privacy-what-is-a-vpn.html*. Obtido de norton.com: <https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html>
- GUPTA, K. (Acedido em maio de 2020). *Freelancinggig*. Obtido de how-do-radius-and-ldap-differ: <https://www.freelancinggig.com/blog/2019/05/13/how-do-radius-and-ldap-differ/>
- Herrmann, B. (Acedido em maio de 2020). *Understanding When to Use LDAP or RADIUS*. Obtido de selinc.com: [https://cdn.selinc.com/assets/Literature/Publications/Application%20Notes/AN2015-08\\_20150817.pdf?v=20150916-200419](https://cdn.selinc.com/assets/Literature/Publications/Application%20Notes/AN2015-08_20150817.pdf?v=20150916-200419)
- HOFFMAN, C. (Acedido em junho de 2020). *htg-explains-what-is-a-vpn*. Obtido de howtogeek.com: <https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/>
- HOFFMAN-ANDREWS, G. G. (Acedido em junho de 2020). */how-captive-portals-interfere-wireless-security-and-privacy*. Obtido de eff.org: <https://www.eff.org/deeplinks/2017/08/how-captive-portals-interfere-wireless-security-and-privacy>
- internetsociety. (Acedido em junho de 2020). *deploy360/tls/basics/*. Obtido de internetsociety.org: <https://www.internetsociety.org/deploy360/tls/basics/>
- Kear, S. (Acedido em maio de 2020). *Monitoring-Internet-Usage-With-LightSquid-and-pfSense*. Obtido de turbofuture.com: <https://turbofuture.com/computers/Monitoring-Internet-Usage-With-LightSquid-and-pfSense>
- KnowITFree. (Acedido em junho de 2020). *How to setup captive portal and vouchers in pfsense 2.3.3*. Obtido de youtube.com: <https://www.youtube.com/watch?v=oG3cbekjlz0>
- linuxize. (Acedido em abril de 2020). *how-to-install-and-configure-samba-on-ubuntu-18-04*. Obtido de linuxize.com: <https://linuxize.com/post/how-to-install-and-configure-samba-on-ubuntu-18-04/>



Lucemplast. (Acedido em abril de 2020). *Competências*. Obtido de Lucemplast:  
<http://www.lucemplast.com/page2.html#counters6-1g>

Lucemplast. (Acedido em abril de 2020). *Empresa*. Obtido de Lucemplast:  
<http://www.lucemplast.com/page1.html#counters5-10>

LUCEMPLAST. (Acedido em abril de 2020). *LUCEMPLAST*. Obtido de LUCEMPLAST.COM:  
<HTTP://WWW.LUCEMPLAST.COM/>

Lucemplast. (Acedido em abril de 2020). *Serviços*. Obtido de Lucemplast:  
<http://www.lucemplast.com/page3.html#header6-1j>

Marsh, J. (Acedido em junho de 2020). *linux-advantages-disadvantages-open-source-technology/*. Obtido de storagecraft.com: <https://blog.storagecraft.com/linux-advantages-disadvantages-open-source-technology/>

Moraes, M. (Acedido em maio de 2020). *squid-com-autenticacao-local-squidguard-com-categorias-no-pfsense*. Obtido de mmoraessolucoes.com:  
<http://mmoraessolucoes.com.br/2016/09/07/squid-com-autenticacao-local-squidguard-com-categorias-no-pfsense/>

Morgan, T. (Acedido em maio de 2020). *snort-suricata-bro-ids*. Obtido de bricata.com:  
<https://bricata.com/blog/snort-suricata-bro-ids/>

Mott, J. (Acedido em maio de 2020). *what-is-suricata-ids*. Obtido de bricata.com:  
<https://bricata.com/blog/what-is-suricata-ids/>

Perens, B. (Acedido em abril de 2020). *help*. Obtido de ubuntu.com:  
<https://help.ubuntu.com/lts/installation-guide/s390x/ch01s01.html>

Pinheiro, L. (Acedido em junho de 2020). *LAB - pfSense 2.3 Wifi Guest Captiva Portal User+Voucher*. Obtido de youtube.com:  
<https://www.youtube.com/watch?v=QwQbvRWbPo8&t=182s>

Pinto, P. (Acedido em abril de 2020). Obtido de <https://pplware.sapo.pt/linux/ipfire-a-distribuicao-linux-gratis-para-criar-routers-e-firewalls/>

Pinto, P. (Acedido em maio de 2020). Obtido de <https://pplware.sapo.pt/internet/saiba-o-que-e-um-proxy-e-para-que-serve-para-o-bem-e-para-o-mal/>

rohitphulsunge. (Acedido em maio de 2020). *samba-server-configuration*. Obtido de slideshare.net: <https://www.slideshare.net/rohitphulsunge/samba-server-configuration>

Rouse, M. (Acedido em junho de 2020). Obtido de <https://searchmobilecomputing.techtarget.com/definition/captive-portal>

Rouse, M. (Acedido em maio de 2020). Obtido de <https://searchwindowsserver.techtarget.com/definition/Microsoft-Windows-Server-OS-operating-system>

rtunity. (Acedido em junho de 2020). *PfSense 2.4.3 Squid Active Directory Authentication - pfSense Part 12*. Obtido de youtube.com: <https://www.youtube.com/watch?v=XFxu-5L4Bug&list=LL-RlDa9K2tmXPx4Q5ap-1g&index=3&t=192s>

rvigil. (Acedido em maio de 2020). *network-address-translation-nat/26704-nat-faq-00.html*. Obtido de cisco.com: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html>

samba. (Acedido em abril de 2020). *samba*. Obtido de samba.org: <https://www.samba.org/>

Sohail. (Acedido em junho de 2020). *endless-os-32-review-the-offline-distro*. Obtido de linuxandubuntu.com: <http://www.linuxandubuntu.com/home/endless-os-32-review-the-offline-distro>

Stefan. (Acedido em junho de 2020). *openvpn-with-ldap-authentication-on-pfsense-2-0-rc1*. Obtido de stefcho.eu: <https://blog.stefcho.eu/openvpn-with-ldap-authentication-on-pfsense-2-0-rc1/>

techotopia. (Acedido em abril de 2020). *The History Of Ubuntu*. Obtido de techotopia.com: [https://www.techotopia.com/index.php/The\\_History\\_of\\_Ubuntu\\_Linux](https://www.techotopia.com/index.php/The_History_of_Ubuntu_Linux)

ubuntu. (Acedido em junho de 2020). *proxy-servers-squid*. Obtido de ubuntu.com: <https://ubuntu.com/server/docs/proxy-servers-squid>

Valiante, F. (Acedido em maio de 2020). *configuracoes-de-rede-maquina-virtual*. Obtido de <http://prof.valiante.info/disciplinas/hardware/maquinas-virtuais-e-containers/configuracoes-de-rede-maquina-virtual>

valuekeep. (Acedido em junho de 2020). *valuekeep*. Obtido de ciben.pt: <https://www.ciben.pt/solucoes/valuekeep/>

Vorkbaard, K. (Acedido em maio de 2020). *set-up-openvpn-on-pfsense-with-user-certificates-and-active-directory-authentication*. Obtido de vorkbaard.nl: <https://vorkbaard.nl/set-up-openvpn-on-pfsense-with-user-certificates-and-active-directory-authentication/>

## **ANEXOS**

## Anexo 1- Proxy config

```
192.168.2.1/squidGuard/squidguard_log.php

# This file is automatically generated by pfSense
# Do not edit manually !

http_port 192.168.2.1:3128
icp_port 0
digest_generation off
dns_v4_first on
pid_filename /var/run/squid/squid.pid
cache_effective_user squid
cache_effective_group proxy
error_default_language pt
icon_directory /usr/local/etc/squid/icons
visible_hostname proxy
cache_mgr admin@localhost
access_log /var/squid/logs/access.log
cache_log /var/squid/logs/cache.log
cache_store_log none
netdb_filename /var/squid/logs/netdb.state
pinger_enable on
pinger_program /usr/local/libexec/squid/pinger

logfile_rotate 5
debug_options rotate=5
shutdown_lifetime 3 seconds
# Allow local network(s) on interface(s)
acl localnet src 192.168.2.0/24
forwarded_for on
httpd_suppress_version_string on
uri_whitespace strip

acl dynamic urlpath_regex cgi-bin ?
cache deny dynamic
```

```

cache_mem 64 MB
maximum_object_size_in_memory 256 KB
memory_replacement_policy heap GDSF
cache_replacement_policy heap LFUDA
minimum_object_size 0 KB
maximum_object_size 4 MB
cache_dir ufs /var/squid/cache 500 16 256
offline_mode off
cache_swap_low 90
cache_swap_high 95
cache_allow all
# Add any of your own refresh_pattern entries above these.
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|?) 0 0% 0
refresh_pattern . 0 20% 4320

#Remote proxies

# Setup some default acls
# ACLs all, manager, localhost, and to_localhost are predefined.
acl allsrc src all
acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901 3128 3129 1025-65535
acl sslports port 443 563

acl purge method PURGE
acl connect method CONNECT

# Define protocols used for redirects
acl HTTP proto HTTP
acl HTTPS proto HTTPS
http_access allow manager localhost

```

```
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !safeports
http_access deny CONNECT !sslports

# Always allow localhost connections
http_access allow localhost

request_body_max_size 0 KB
delay_pools 1
delay_class 1 2
delay_parameters 1 -1/-1 -1/-1
delay_initial_bucket_level 100
delay_access 1 allow allsrc

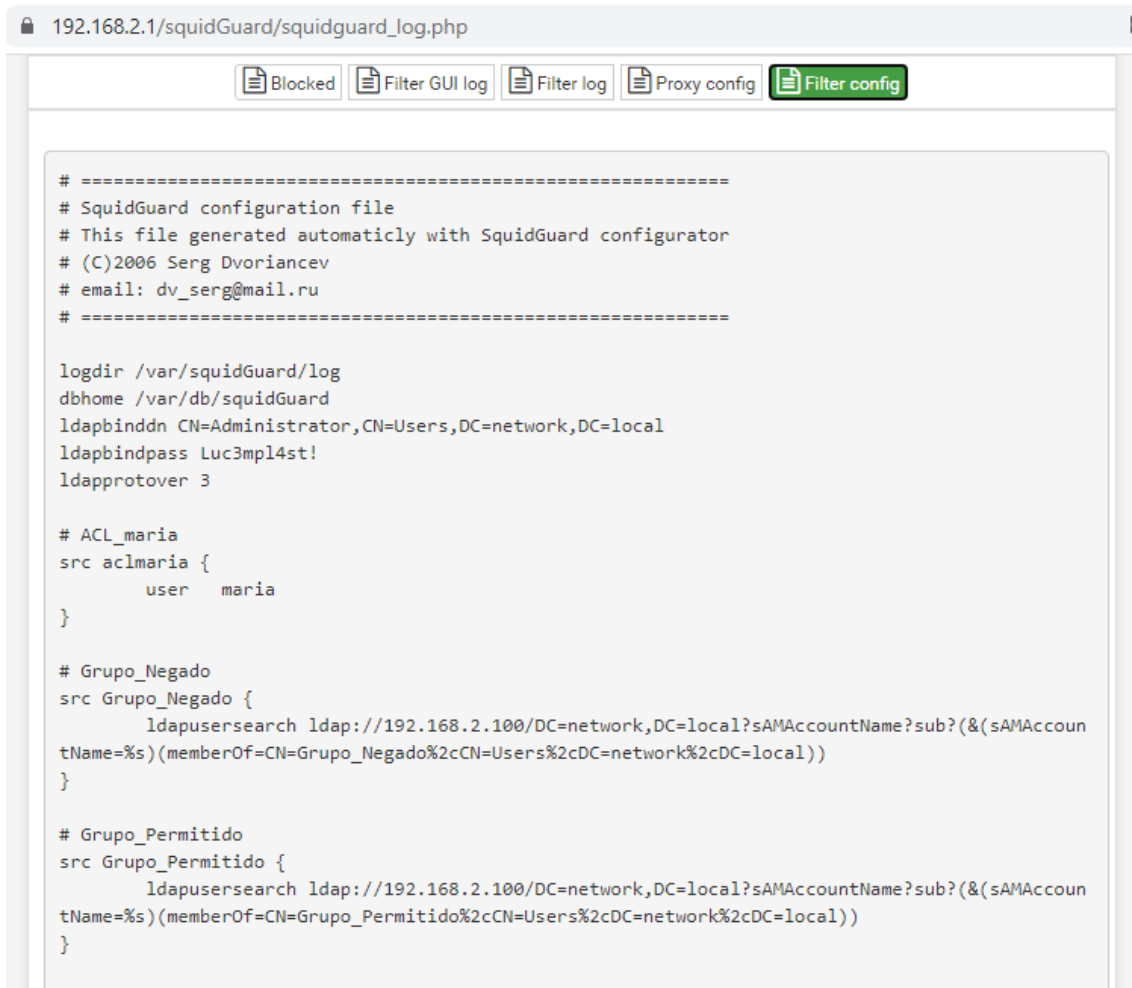
# Reverse Proxy settings

# Package Integration
url_rewrite_program /usr/local/bin/squidGuard -c /usr/local/etc/squidGuard/squidGuard.conf
url_rewrite_bypass off
url_rewrite_children 16 startup=8 idle=4 concurrency=0

# Custom options before auth

auth_param basic program /usr/local/libexec/squid/basic_ldap_auth -v 3 -b 'DC=network,DC=local'
-D 'CN=Administrator,CN=Users,DC=network,DC=local' -w 'Luc3mpl4st!' -f '(&(objectClass=person)
(sAMAccountName=%s))' -u 'sAMAccountName' -P -H 'ldap://192.168.2.100:389'
auth_param basic children 10
auth_param basic realm Please enter your credentials to access the proxy
auth_param basic credentialsttl 120 minutes
acl password proxy_auth REQUIRED
```

## Anexo 2- Configuração de Filtro



The screenshot shows a web browser window with the address bar displaying `192.168.2.1/squidGuard/squidguard_log.php`. The page has a navigation bar with five buttons: `Blocked`, `Filter GUI log`, `Filter log`, `Proxy config`, and `Filter config` (which is highlighted in green). The main content area displays the SquidGuard configuration file in a monospaced font. The configuration includes comments about the file's origin, log directory, database home, LDAP settings, and ACL definitions for `ACL_maria`, `Grupo_Negado`, and `Grupo_Permitido`.

```
# =====
# SquidGuard configuration file
# This file generated automaticly with SquidGuard configurator
# (C)2006 Serg Dvoriancev
# email: dv_serg@mail.ru
# =====

logdir /var/squidGuard/log
dbhome /var/db/squidGuard
ldapbinddn CN=Administrator,CN=Users,DC=network,DC=local
ldapbindpass Luc3mpl4st!
ldapprotover 3

# ACL_maria
src aclmaria {
    user    maria
}

# Grupo_Negado
src Grupo_Negado {
    ldapusersearch ldap://192.168.2.100/DC=network,DC=local?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=Grupo_Negado%2cCN=Users%2cDC=network%2cDC=local))
}

# Grupo_Permitido
src Grupo_Permitido {
    ldapusersearch ldap://192.168.2.100/DC=network,DC=local?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=Grupo_Permitido%2cCN=Users%2cDC=network%2cDC=local))
}
```

```

#
dest blk_BL_adv {
    domainlist blk_BL_adv/domains
    urllist blk_BL_adv/urls
    log block.log
}

#
dest blk_BL_aggressive {
    domainlist blk_BL_aggressive/domains
    urllist blk_BL_aggressive/urls
    log block.log
}

#
dest blk_BL_alcohol {
    domainlist blk_BL_alcohol/domains
    urllist blk_BL_alcohol/urls
    log block.log
}

#
dest blk_BL_anonvpn {
    domainlist blk_BL_anonvpn/domains
    urllist blk_BL_anonvpn/urls
    log block.log
}

#
dest blk_BL_automobile_bikes {
    domainlist blk_BL_automobile_bikes/domains
    urllist blk_BL_automobile_bikes/urls
    log block.log
}

```

```

dest blk_BL_automobile_boats {
    domainlist blk_BL_automobile_boats/domains
    urllist blk_BL_automobile_boats/urls
    log block.log
}

#
dest blk_BL_automobile_cars {
    domainlist blk_BL_automobile_cars/domains
    urllist blk_BL_automobile_cars/urls
    log block.log
}

#
dest blk_BL_automobile_planes {
    domainlist blk_BL_automobile_planes/domains
    urllist blk_BL_automobile_planes/urls
    log block.log
}

#
dest blk_BL_chat {
    domainlist blk_BL_chat/domains
    urllist blk_BL_chat/urls
    log block.log
}

#
dest blk_BL_costtraps {
    domainlist blk_BL_costtraps/domains
    urllist blk_BL_costtraps/urls
    log block.log
}

```



```
#
dest blk_BL_dating {
    domainlist blk_BL_dating/domains
    urllist blk_BL_dating/urls
    log block.log
}

#
dest blk_BL_downloads {
    domainlist blk_BL_downloads/domains
    urllist blk_BL_downloads/urls
    log block.log
}

#
dest blk_BL_drugs {
    domainlist blk_BL_drugs/domains
    urllist blk_BL_drugs/urls
    log block.log
}

#
dest blk_BL_dynamic {
    domainlist blk_BL_dynamic/domains
    urllist blk_BL_dynamic/urls
    log block.log
}

#
dest blk_BL_education_schools {
    domainlist blk_BL_education_schools/domains
    urllist blk_BL_education_schools/urls
    log block.log
}

#
```

```
#
dest blk_BL_finance_banking {
    domainlist blk_BL_finance_banking/domains
    urllist blk_BL_finance_banking/urls
    log block.log
}

#
dest blk_BL_finance_insurance {
    domainlist blk_BL_finance_insurance/domains
    urllist blk_BL_finance_insurance/urls
    log block.log
}

#
dest blk_BL_finance_moneylending {
    domainlist blk_BL_finance_moneylending/domains
    urllist blk_BL_finance_moneylending/urls
    log block.log
}

#
dest blk_BL_finance_other {
    domainlist blk_BL_finance_other/domains
    urllist blk_BL_finance_other/urls
    log block.log
}

#
dest blk_BL_finance_realestate {
    domainlist blk_BL_finance_realestate/domains
    urllist blk_BL_finance_realestate/urls
    log block.log
}

#
dest blk_BL_finance_trading {
    domainlist blk_BL_finance_trading/domains
    urllist blk_BL_finance_trading/urls
    log block.log
}

}
```

```
#
dest blk_BL_fortunetelling {
    domainlist blk_BL_fortunetelling/domains
    urllist blk_BL_fortunetelling/urls
    log block.log
}

#
dest blk_BL_forum {
    domainlist blk_BL_forum/domains
    urllist blk_BL_forum/urls
    log block.log
}

#
dest blk_BL_gamble {
    domainlist blk_BL_gamble/domains
    urllist blk_BL_gamble/urls
    log block.log
}

#
dest blk_BL_government {
    domainlist blk_BL_government/domains
    urllist blk_BL_government/urls
    log block.log
}

#
dest blk_BL_hacking {
    domainlist blk_BL_hacking/domains
    urllist blk_BL_hacking/urls
    log block.log
}

#
dest blk_BL_hobby_cooking {
    domainlist blk_BL_hobby_cooking/domains
    urllist blk_BL_hobby_cooking/urls
    log block.log
}
}
```

```

dest blk_BL_hobby_games-misc {
    domainlist blk_BL_hobby_games-misc/domains
    urllist blk_BL_hobby_games-misc/urls
    log block.log
}

#
dest blk_BL_hobby_games-online {
    domainlist blk_BL_hobby_games-online/domains
    urllist blk_BL_hobby_games-online/urls
    log block.log
}

#
dest blk_BL_hobby_gardening {
    domainlist blk_BL_hobby_gardening/domains
    urllist blk_BL_hobby_gardening/urls
    log block.log
}

#
dest blk_BL_hobby_pets {
    domainlist blk_BL_hobby_pets/domains
    urllist blk_BL_hobby_pets/urls
    log block.log
}

#
dest blk_BL_homestyle {
    domainlist blk_BL_homestyle/domains
    urllist blk_BL_homestyle/urls
    log block.log
}

#
dest blk_BL_hospitals {
    domainlist blk_BL_hospitals/domains
    urllist blk_BL_hospitals/urls
    log block.log
}
}
```

```

dest blk_BL_imagehosting {
    domainlist blk_BL_imagehosting/domains
    urllist blk_BL_imagehosting/urls
    log block.log
}

#
dest blk_BL_isp {
    domainlist blk_BL_isp/domains
    urllist blk_BL_isp/urls
    log block.log
}

#
dest blk_BL_jobsearch {
    domainlist blk_BL_jobsearch/domains
    urllist blk_BL_jobsearch/urls
    log block.log
}

#
dest blk_BL_library {
    domainlist blk_BL_library/domains
    urllist blk_BL_library/urls
    log block.log
}

#
dest blk_BL_military {
    domainlist blk_BL_military/domains
    urllist blk_BL_military/urls
    log block.log
}

#
dest blk_BL_models {
    domainlist blk_BL_models/domains
    urllist blk_BL_models/urls
    log block.log
}

```

```

#
dest blk_BL_movies {
    domainlist blk_BL_movies/domains
    urllist blk_BL_movies/urls
    log block.log
}

#
dest blk_BL_music {
    domainlist blk_BL_music/domains
    urllist blk_BL_music/urls
    log block.log
}

#
dest blk_BL_news {
    domainlist blk_BL_news/domains
    urllist blk_BL_news/urls
    log block.log
}

#
dest blk_BL_podcasts {
    domainlist blk_BL_podcasts/domains
    urllist blk_BL_podcasts/urls
    log block.log
}

#
dest blk_BL_politics {
    domainlist blk_BL_politics/domains
    urllist blk_BL_politics/urls
    log block.log
}

#
dest blk_BL_porn {
    domainlist blk_BL_porn/domains
    urllist blk_BL_porn/urls
    log block.log
}

```

```

#
dest blk_BL_radiotv {
    domainlist blk_BL_radiotv/domains
    urllist blk_BL_radiotv/urls
    log block.log
}

#
dest blk_BL_recreation_humor {
    domainlist blk_BL_recreation_humor/domains
    urllist blk_BL_recreation_humor/urls
    log block.log
}

#
dest blk_BL_recreation_martialarts {
    domainlist blk_BL_recreation_martialarts/domains
    urllist blk_BL_recreation_martialarts/urls
    log block.log
}

#
dest blk_BL_recreation_restaurants {
    domainlist blk_BL_recreation_restaurants/domains
    urllist blk_BL_recreation_restaurants/urls
    log block.log
}

#
dest blk_BL_recreation_sports {
    domainlist blk_BL_recreation_sports/domains
    urllist blk_BL_recreation_sports/urls
    log block.log
}

#
dest blk_BL_recreation_travel {
    domainlist blk_BL_recreation_travel/domains
    urllist blk_BL_recreation_travel/urls
    log block.log
}

```

```

#
dest blk_BL_recreation_wellness {
    domainlist blk_BL_recreation_wellness/domains
    urllist blk_BL_recreation_wellness/urls
    log block.log
}

#
dest blk_BL_redirector {
    domainlist blk_BL_redirector/domains
    urllist blk_BL_redirector/urls
    log block.log
}

#
dest blk_BL_religion {
    domainlist blk_BL_religion/domains
    urllist blk_BL_religion/urls
    log block.log
}

#
dest blk_BL_remotecontrol {
    domainlist blk_BL_remotecontrol/domains
    urllist blk_BL_remotecontrol/urls
    log block.log
}

#
dest blk_BL_ringtones {
    domainlist blk_BL_ringtones/domains
    urllist blk_BL_ringtones/urls
    log block.log
}

#
dest blk_BL_science_astronomy {
    domainlist blk_BL_science_astronomy/domains
    urllist blk_BL_science_astronomy/urls
    log block.log
}

```

```

dest blk_BL_science_chemistry {
    domainlist blk_BL_science_chemistry/domains
    urllist blk_BL_science_chemistry/urls
    log block.log
}

#
dest blk_BL_searchengines {
    domainlist blk_BL_searchengines/domains
    urllist blk_BL_searchengines/urls
    log block.log
}

#
dest blk_BL_sex_education {
    domainlist blk_BL_sex_education/domains
    urllist blk_BL_sex_education/urls
    log block.log
}

#
dest blk_BL_sex_lingerie {
    domainlist blk_BL_sex_lingerie/domains
    urllist blk_BL_sex_lingerie/urls
    log block.log
}

#
dest blk_BL_shopping {
    domainlist blk_BL_shopping/domains
    urllist blk_BL_shopping/urls
    log block.log
}

#
dest blk_BL_socialnet {
    domainlist blk_BL_socialnet/domains
    urllist blk_BL_socialnet/urls
    log block.log
}

```

```

#
dest blk_BL_spyware {
    domainlist blk_BL_spyware/domains
    urllist blk_BL_spyware/urls
    log block.log
}

#
dest blk_BL_tracker {
    domainlist blk_BL_tracker/domains
    urllist blk_BL_tracker/urls
    log block.log
}

#
dest blk_BL_updatesites {
    domainlist blk_BL_updatesites/domains
    urllist blk_BL_updatesites/urls
    log block.log
}

#
dest blk_BL_urlshortener {
    domainlist blk_BL_urlshortener/domains
    urllist blk_BL_urlshortener/urls
    log block.log
}

#
dest blk_BL_violence {
    domainlist blk_BL_violence/domains
    urllist blk_BL_violence/urls
    log block.log
}

#
dest blk_BL_warez {
    domainlist blk_BL_warez/domains
    urllist blk_BL_warez/urls
    log block.log
}

```

```
#
dest blk_BL_weapons {
    [domainlist blk_BL_weapons/domains
    urllist blk_BL_weapons/urls
    log block.log
}

#
dest blk_BL_webmail {
    domainlist blk_BL_webmail/domains
    urllist blk_BL_webmail/urls
    log block.log
}

#
dest blk_BL_webphone {
    domainlist blk_BL_webphone/domains
    urllist blk_BL_webphone/urls
    log block.log
}

#
dest blk_BL_webradio {
    domainlist blk_BL_webradio/domains
    urllist blk_BL_webradio/urls
    log block.log
}

#
dest blk_BL_webtv {
    domainlist blk_BL_webtv/domains
    urllist blk_BL_webtv/urls
    log block.log
}

#
rew safesearch {
    s@(google../search?.*q=.*)*@r&safe=active@i
    s@(google../images.*q=.*)*@r&safe=active@i
    s@(google../groups.*q=.*)*@r&safe=active@i
    s@(google../news.*q=.*)*@r&safe=active@i

```

```

s@(yandex../yandex.*text=.*)*@r&fyandex=1@i
s@(search.yahoo../search.*p=.*)*@r&vm=r&v=1@i
s@(search.live../.*q=.*)*@r&adlt=strict@i
s@(search.msn../.*q=.*)*@r&adlt=strict@i
s@(bing../.*q=.*)*@r&adlt=strict@i
s@(duckduckgo../.*q=.*)*@r&kp=1@i
s@(rambler../.*query=.*)*@r&adult=family@i
s@(qwant../.*q=.*)*@r&s=2@i
log block.log
}

#
acl {
    # ACL_maria
    aclmaria {
        pass !blk_BL_porn all
        redirect http://192.168.2.1:80/sgerror.php?url=403%20pagina%20bloqueada&a=%a&n=%n&i=%i&s=%s&t=%t&u=%u
    }
    # Grupo_Negado
    Grupo_Negado {
        pass none
        redirect https://ipca.pt/
    }
    # Grupo_Permitido
    Grupo_Permitido {
        pass none
        redirect http://192.168.2.1:80/sgerror.php?url=403%20permitido&a=%a&n=%n&i=%i&s=%s&t=%t&u=%u
    }
    #
    default {
        pass all
        redirect http://192.168.2.1:80/sgerror.php?url=403%20&a=%a&n=%n&i=%i&s=%s&t=%t&u=%u
    }
}

```