DEPARTAMENTO DE CIÊNCIAS E TECNOLOGIAS DA INFORMAÇÃO

Mestrado em Engenharia de Telecomunicações e Informática

Desenvolvimento de produto competitivo para a área de gestão de segurança de dados e aplicações

Márcio Silva Santos

Dissertação submetida como requisito parcial para obtenção do Grau de

Mestre em Engenharia de Telecomunicações e Informática

Orientador:

Doutor Pedro Joaquim Amaro Sebastião, Professor do ISCTE-IUL.

ISCTE-IUL

Dezembro de 2018

Dedicatória

Aos meus pais, Luiz Santos e Sueli Santos que me ensinaram os valores para me tornar um bom cidadão e nunca mediram esforços para proporcionarem o melhor estudo aos seus filhos.

À minha esposa Camila Larangeira que ofereceu apoio incondicional durante todo o decorrer deste mestrado.

Agradecimentos

Ao Professor Doutor Pedro Joaquim Amaro Sebastião, docente do Instituto Universitário de Lisboa, o meu reconhecimento por sua inestimável orientação neste trabalho, apoio na incubação das ideias e transformação em produtos.

Ao Professor Doutor Flávio Luís de Mello, docente da Universidade Federal do Rio de Janeiro, meu orientador no MBA em Tecnologia da Informação, que estimulou e recomendou a este mestrado.

A todos os professores que me acompanharam desde início dos estudos mais básicos, apresentaram as primeiras letras e me levaram aos cálculos mais complexos, contribuíram de alguma forma para a conclusão deste trabalho, ofereço o mais sincero agradecimento.

RESUMO

A segurança informática é tema em constante desenvolvimento. Ameaças cada vez mais sofisticadas exigem das organizações um constante e dispendioso investimento para proteger seus dados e suas informações. Novas leis impactam ainda mais a gestão das tecnologias exigindo que as empresas se adaptem a processos complexos com adoção de tecnologias usualmente de alto custo. O trabalho desenvolvido e apresentado nesta dissertação aborda o desenvolvimento de produtos para segurança de dados e de aplicações, estas últimas com foco especial na componente web, com o uso de tecnologias *open source* e tem como objetivo, compor uma solução com complexidade reduzida e grau de eficiência comparável às soluções proprietárias de mercado, usando metodologias e padrões definidos por organizações e comunidades independentes como o OWASP - *Open Web Application Security Project*. O resultado foi um conjunto de subsistemas de código aberto e inseridos códigos para aperfeiçoamento de funções que integram uma plataforma multicamadas para proteção de dados.

Palavras-chave: Segurança da Informação; Código aberto; Retenção de divisas; Geração de emprego.

ABSTRACT

Computer security is a constantly developing topic. Increasingly sophisticated threats require organizations to constantly and costly invest to protect their data and information. New laws further impact technology management by requiring companies to adapt to complex processes by adopting often-costly technologies. This dissertation addresses the development of products for data security and applications, the latter with special focus on the web component, using open source technologies and aims to compose a solution with reduced complexity and efficiency comparable to proprietary solutions using methodologies and standards defined by independent organizations and communities such as the OWASP - *Open Web Application Security Project*. The result was a set of open source subsystems and embed codes for enhancing functions that integrate a multilayer platform for data protection.

Key-words: Information Security; Open source; Retention of foreign exchange; Job creation.

LISTA DE ACRÓNIMOS

BIND	*Berkeley Internet Name Domain*
BSD	*Berkeley Software Distribution*
BYOD	*Bring Your Own Device*
CRS	*Core Rule Set*
DLP	*Data Loss Prevention*
DNS	*Domain Name System*
DNSBL	*Domain Name System Block List*
DPI	*Deep Packet Inspection*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
IRS	*Imposto sobre Rendimento de pessoas Singulares*
ISC	*Internet Systems Consortium*
LFI	*Local File Inclusion*
MLE	*Machine Learning Engine*
NAT	*Network Address Translation*
NGFW	*Next-Generation Firewall*
OSI	*Open System Interconnection*
OWASP	*Open Web Application Security Project*
PF	*Packet Filtering*
RCE	*Remote Code Execution*
RFI	*Remote File Inclusion*
RGPD	*Regulamento Geral sobre a Proteção de Dados*
RPZ	*Response Policy Zone*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
UE	*União Europeia*
URL	*Uniform Resource Locator*
UTM	*Unified Threat Management*
VPN	*Virtual Private Network*
WAF	*Web Application Firewall*
XSS	Cross-Site Script

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

1. Introdução

Este trabalho é resultado de pesquisas económica, financeira e técnica, complementares, cujo objetivo final é o desenvolvimento de um produto para a gestão e segurança aplicacional e de dados com uso de componentes *open source* que criarão camadas de segurança nos níveis das infraestruturas e aplicações.

O tema escolhido, "Desenvolvimento de produto competitivo para a área de gestão de segurança de dados e aplicações", se deu em função das atuais soluções de segurança de dados compostas por *firewalls*, *web application firewalls* e DNS *firewalls* serem ofertadas a valores relativamente altos e fora do espectro financeiro das pequenas empresas. Neste sentido foi realizada uma pesquisa para listar sistemas de código aberto que pudessem integrar um produto com as características necessárias para proteção de dados. Na sequência do trabalho, foram realizados testes de integração de cada componente de forma a validar o produto final com todas as funcionalidades permitidas pelos sistemas *open source*, resultando numa solução com custo mais baixo comparada a outros produtos já comercializados.

A primeira parte do trabalho caracteriza o problema, a motivação para a realização deste estudo, define o mercado alvo e o produto a ser desenvolvido. Insere conceitos e definições que permitirão compreender a abordagem técnica, econômica e comercial das seções seguintes.

A segunda parte apresenta uma abordagem técnica no âmbito das tecnologias utilizadas para compor o produto final e suas variantes. Com especial foco nas soluções de código aberto com um comparativo técnico a plataformas comerciais. Apresenta ainda diferenciais técnicos entre a solução proposta e produtos proprietários, consolidados no mercado.

A terceira parte aborda os conceitos comerciais e realiza uma análise económica, financeira, agregadas à proposta de um plano de comunicação direcionado ao público identificado na primeira parte deste trabalho, para acompanhar o lançamento do produto e de suas variantes no mercado português.

A quarta parte apresenta um sumário dos diferenciais técnicos e económicos e aponta o produto final como um suporte essencial aos pequenos negócios. A computação suporta atividades heterogêneas; Empresas e pequenos negócios, impulsionados pela redução de

custos na aquisição de soluções de segurança da informação e incremento nos processos de mitigação de ameaças inerentes às tecnologias informáticas, podem focar seus gastos no cerne de suas atividades, promoverem um crescimento interno e darem contributo para um ambiente sustentável, com geração de empregos, manutenção do capital em território português, a fim de promover o bem-estar da sociedade.

1.1.Motivação

Sistemas informáticos convivem constantemente com ameaças digitais. Existe uma vasta linha de soluções que compõem camadas de proteção digital, desde as mais simples aplicações de antivírus, passando por *firewalls* de perímetro até complexos sistemas de correlação de eventos que fazem uso de inteligência artificial para identificar ameaças com base em comportamentos.

Muitas empresas nasceram destas necessidades e oferecem produtos que abrangem cada uma das camadas de acesso à informação. Entretanto, cada um destes níveis de proteção tem um custo agregado relativamente alto e muitas vezes, ao se tratar de pequenas e médias empresas, completamente fora das suas capacidades financeiras.

Medidas governamentais surgem em paralelo aos interesses internos para proteger informações pessoais, tais como o recente Regulamento Europeu de Proteção de Dados (RGPD).

Neste cenário, as empresas se veem cada vez mais obrigadas a investir na segurança da informação para resguardar tanto o seu negócio quanto o ecossistema que as circundam.

Pequenas empresas ou entidades com capital reduzido possuem necessidades semelhantes às grandes corporações no âmbito das transformações digitais. Contudo, não gozam do mesmo potencial financeiro para realizar investimentos tecnológicos para suportar implementações sólidas e fiáveis, sistemas de segurança da informação. Estas empresas, familiares, pequenas e médias são a motivação para a criação de uma plataforma de segurança que permitam aferir um grau de proteção mínimo a um custo aceitável com o menor impacto nos âmbitos financeiros e de processos internos. Não excludentes, empresas que mesmo possuindo capacidade de investimento, podem optar por reduzir os custos em áreas de suporte ao negócio e focarem seus esforços financeiros no cerne de suas atividades, beneficiando-se de um sistema de código aberto.

Em outro aspeto, instituições governamentais podem usufruir de um ambiente de software livre, bem como a manutenção do capital financeiro e intelectual em território nacional, contribuindo para a redução da evasão de divisas e enriquecimento do conhecimento.

Segundo (Miranda, Vieira, & Carelli, 2008), a redução dos gastos com licenciamento é uma das vantagens na adoção de Software Livre pelo Governo. Como a maioria dos softwares de uso corporativo são produzidos por empresas estrangeiras, ressalta ainda que os investimentos têm o capital retido no país que pode ser usado para o desenvolvimento tecnológico, científico e informativo dos servidores públicos. Os gastos economizados podem ser aplicados em formações, treinamentos e programas de disseminação de tecnologias para a sociedade.

Para além dos fatores financeiros a insegurança digital, derivada de eventos amplamente divulgados que se relatam fatos acerca da coleta não autorizada de dados pessoais, movimentos hackers e ameaças como vírus é fator notável para que clientes busquem empresas com investimentos em segurança da informação comprovados e divulgados em boletins públicos que proporcionam uma visão de garantia de serviços e sigilo no tratamento de seus dados.

Já (Ochôa & Pinto, 2018) afirmam que ainda há uma extensa estrada a percorrer para ampliar a segurança dos utentes e consumidores no âmbito da legislação, já inserida no contexto do Regulamento Geral sobre a Proteção de Dados e melhorar os recursos tecnológicos para a criação de um maio seguro de comércio eletrónico tanto para consumidores quanto para as empresas.

Estes fatores motivaram o desenvolvimento deste estudo para oferecer um conjunto de sistemas modulares integrados que compõem uma solução multicamadas para a segurança de dados, seja para o comércio eletrónico ou informações internas, de negócio, críticas para as empresas.

1.2. Objetivos

O principal objetivo deste trabalho desenvolver um produto a partir da integração de sistemas e dispositivos que permitam compor soluções de segurança com especial foco nas plataformas *open source*, capazes de executar atividades de proteção digital de dados e aplicações, destacando as aplicações web.

Na parte I serão abordados os conceitos de segurança da informação. Será realizada a caracterização do perfil de utilização de sistemas informáticos os tipos de dados a serem tratados e a infraestrutura de suporte aos meios informáticos que deve ser protegida. Com base no cenário apresentado, será desenvolvida uma arquitetura de alto nível como proposta para cobrir todos os aspetos de segurança envolvidos.

A parte II pretende dar uma visão das soluções comerciais disponíveis e irá detalhar as soluções técnicas de código aberto capazes de suprir com eficácia os itens de controlo no âmbito da segurança da informação. Pretende-se integrar soluções de código aberto e *software* livre, em hardware desenhado para as funções específicas de modo a obter um produto final de elevado potencial técnico que permita executar as funções essenciais a que se propõe, realizar uma análise técnica das componentes físicas e de sistemas. Na parte final faz-se comparação da solução com plataformas no mercado e indicar aspetos de competitividade nos planos técnico e científico.

A parte III tem como objetivo realizar um estudo financeiro e econômico de soluções comerciais presentes no mercado português para situá-las num cenário comercial, em seguida, inserir uma plataforma de segurança desenhada com soluções abertas e efetuar uma comparação econômica para demonstrar a viabilidade financeira que aliada a um plano de marketing possa criar um produto competitivo a ser inserido no mercado nacional.

A parte IV deverá consolidar os resultados das partes II e III deste trabalho e apresentar o potencial impacto econômico e social que uma solução desenvolvida em Portugal pode oferecer, tais como retenção de divisas, geração de emprego e aumento de renda para promover o bem-estar.

1.3.Materiais e métodos

O desenvolvimento do estudo inicia-se com um levantamento bibliográfico que permitiu definir direções e objetivos específicos para cada parte do trabalho. Na sequência, um ambiente em plataforma virtualizada é implementado para aferição e testes das componentes técnicas de forma a produzir resultados práticos.

A componente técnica apresentada na segunda parte, conta com soluções abertas, de domínio público com adendas de códigos que proporcionam o aumento na qualidade

das atividades a que se propõem. Os parâmetros de qualidade, quantificados, serão destacados nos capítulos em que se façam surgir.

A plataforma foi implementada em um ambiente virtualizado com VMware ESXi, versão 6.0.0 que permite aferir o funcionamento de cada componente e validar o comportamento de tráfego para uma análise de segurança.

Para além de artigos acadêmicos, livros e revistas técnicas, há de se destacar pesquisas de mercado que são fonte rica para a análise de marketing, econômica e financeira. Não podendo excluir o fenômeno das redes sociais, de onde se pode extrair informação sobre o comportamento de mercado dos consumidores e profissionais que também são considerados para a análise da terceira parte do trabalho.

Com base nos temas acima, a quarta parte é fruto de uma análise geral que aponta expectativas de vendas e crescimento de modo a se criar um produto competitivo, com aceitação no mercado e que permita a geração de trabalho de modo direto para o seu desenvolvimento, produção e comercialização, para além dos impactos gerados nos clientes adotantes deste produto beneficiários da redução de custos.

1.4. Principais contribuições

Os produtos listados na análise técnica do capítulo 3 foram inseridos pelo autor, como módulos da solução Cyberlab apresentada no 2º NATO Cyber Defense, Smart Defense Proect's (CD SDP) realizado na sede da Academia Militar em Lisboa em 28 de abril de 2016 (Santos, 2016) e em solução completa, integrada ao Cyberlab apresentado no 3º NATO Cyber Defense, Smart Defense Project's (CD SDP) em 28 de abril de 2017 (Gonçalves & Santos, 2017).

Como principal contribuição, espera-se apresentar um produto, modelado com componentes *open source*, que permita executar as funções primárias de proteção aos dados, respeitando padrões e métricas de qualidade semelhantes aos produtos ofertados por linhas comerciais vigentes no mercado português. Em adição ao contributo principal, o desenvolvimento de um produto com selo português, deve permitir a retenção de capital financeiro em território nacional e disseminar o conhecimento no âmbito dos projetos de implementação, manutenção dos sistemas e suporte. Este trabalho pode ainda ser referência para estudos de implementação de sistemas de código aberto com vista a reduzir o custo total de investimentos em plataformas de segurança.

PARTE I

2. Cenário geral

A informática já faz parte do quotidiano da sociedade atual. Desde a simples emissão de uma fatura eletrônica na compra de um café, a declaração de IRS, exames de saúde e uma lista quase infinita de informações. Os dados dispersos por uma rede complexa carregam informações pessoais, críticas, sigilosas e muitas outras caracterizadas de domínio restrito.

A principal motivação deste trabalho é a criação de um produto acessível a pequenos negócios que permita a transformação digital com segurança. Serão identificados aspetos económicos e de mercado para a criação de um produto que permita oferecer proteção digital com competitividade técnica e financeira.

Todos os sistemas selecionados são de licenciamento aberto e sem despesas recorrentes com renovações ou suporte, o que reduz consideravelmente o custo total de aquisição, conforme será apresentado a seguir. Como abordagem principal, a plataforma foi configurada na nuvem em servidor dedicado, o que permite a flexibilidade para o crescimento e suporte a carga de múltiplos clientes sem a necessidade de grandes investimentos iniciais.

Os sistemas devem permitir ainda serem embarcados em arquiteturas i386/x64. Isto leva a uma vasta gama de hardware disponível no mercado para compor uma solução. Neste sentido, foi realizada uma pesquisa de campo para reconhecer dispositivos de hardware compatíveis com os sistemas pfSense, Ubuntu Linux, CentOS Linux e FreeBSD.

2.1.Dados e informação

Para contextualizar o cenário da segurança, é necessário compreender o que são os dados e a informação.

Em seu artigo intitulado "Dado, Informação, Conhecimento e Competência", (Setzer, 2014) define dado como:

> "[…] uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De facto, as letras são símbolos quantificados […] um dado é necessariamente uma entidade matemática e, desta forma, é puramente sintático.

> Isto significa que os dados podem ser totalmente descritos através de representações formais, estruturais. Sendo ainda quantificados ou quantificáveis, eles podem obviamente ser armazenados em um computador e processados por ele" (Setzer, 2014).

Desta abordagem, entende-se que dado é um elemento bruto, representado matematicamente que sem a correta interpretação não expressa qualquer significado, sendo o dado capaz de conter informação.

O conceito de informação aqui abordado está inserido no âmbito das informações organizacionais e pode ser entendida como dados dentro de um contexto que permitem atribuir um significado, abstraindo-se o simples símbolo matemático e elevando a um entendimento no nível de raciocínio lógico e humano. Outras definições de informação são descritas na literatura acadêmica de forma mais detalhada. Contudo o conceito aqui exposto é mais que suficiente para a compreensão geral deste estudo.

No âmbito da gestão de informação empresarial há outro elemento notável, o conhecimento, que é discutido nos níveis da gestão da informação e que podem servir de base para a classificação da informação.

A informação pode ser classificada com base no seu domínio, ou seja, agrupada conforme o público a quem se destina, a relevância do seu conteúdo e as restrições aplicadas (Administração, 2018). Diversas literaturas citam modelos e segmentações da informação. Este estudo não pretende definir um novo modelo de classificação e dentre as referências pesquisadas, visto que estudos mais recentes não alteraram as definições, (Laureano & Moraes, 2005) apresentam um modelo adequado ao tema central e classificam a informação como:

> **Pública**. Informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital.
>
> **Interna**. O acesso livre a este tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital.
>
> **Confidencial**. Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.

> **Secreta**. Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.
>
> Laureano, M. P., & Moraes, P. S. (2005). p 38-44.

2.2.Presença na Internet

A presença digital é um grande diferencial para qualquer negócio e o consumidor cria a perceção de que um produto que não existe na Internet, não existe em lugar algum (Strutzel, 2015). A grande rede proporciona um meio de comunicação ágil e sem fronteiras. Pequenas empresas são estimuladas a iniciar a sua presença na Internet já durante seu processo de abertura, quando recebem um cupão com validade de um ano para hospedagem gratuita de um *website* e nome no domínio "*.pt"*.

Uma abordagem comummente usada por pequenas empresas é a contração direta do serviço de provedores especializados para a hospedagem do seu site. Outra, não tão diferente, é o uso de blogs e outras ferramentas com vastas possibilidades gratuitas para a comunicação e vendas de seus produtos. Algumas mais focadas possuem seus próprios servidores de páginas que integram microssistemas de gestão de clientes e vendas.

Independente do tipo de cliente, uma arquitetura de infraestrutura é base para que os sistemas sejam publicados na Internet. Esta arquitetura tem um desenho de alto nível conforme a figura abaixo:

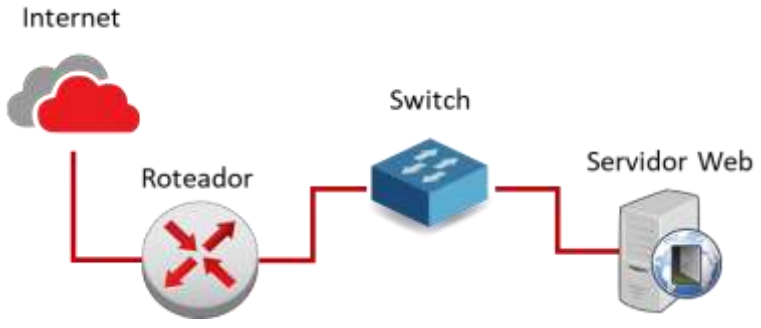

Figura 1 - Diagrama alto nível

O diagrama da Figura 1 apresenta as conexões básicas desde o acesso proveniente da infraestrutura de um operador de telecomunicações, que chega ao cliente através de um

equipamento roteador de tráfego, conectado a um comutador e este ao servidor de páginas (Amaral, 2012). Os dados, transportam as informações por este caminho e precisam ser protegidos de forma a garantir as premissas básicas da segurança da informação (Galegale, Fontes, & Galegale, 2017):

Acessibilidade: É necessário garantir que estes dados sejam acessíveis quando são necessários para que o negócio tenha continuidade e não sofra perdas em seus processos;

Confidencialidade: É necessário garantir que os dados sejam acedidos pelo público devidamente segmentado conforme a classificação da informação que este dado transporta.

Integridade: É necessário garantir que a informação constante nos dados não foi alterada ou corrompida de forma intencional ou não.

2.3. Arquitetura e premissas

Algumas componentes de rede foram desenvolvidas para atuarem na segurança dos dados aplicacionais e aqui serão destacadas as soluções de proteção a ambientes web.

O diagrama da Figura 2 apresenta o desenho genérico de uma infraestrutura protegida (Maurício, Alvarenga, Rubinstein, & Duarte, 2017). Os detalhes de cada componente, funcionalidades e modo de operação serão abordados na segunda parte deste trabalho.

Figura 2 - Infraestrutura protegida - Visão geral

Os roteadores via de regra são fornecidos e geridos pelo operador. Embora níveis de proteção possam ser aplicados nesta componente, a sua componente de defesa é superficial (Szewczyk & Macdonald, 2017) e não é objeto de trabalho desta dissertação.

Os produtos propostos devem atender às normas e metodologias de segurança reconhecidas no mercado, como OWASP – Open Web Application Security Project e ISO 27000[1].

Como premissa, a solução deve conter tanto quanto possível, soluções de código aberto, sem que cause qualquer prejuízo à qualidade esperada do produto final e comparadas a soluções proprietárias que serão analisadas no decorrer deste trabalho.

A arquitetura em alto nível proposta para a solução final é apresentada no diagrama de blocos da Figura 3:

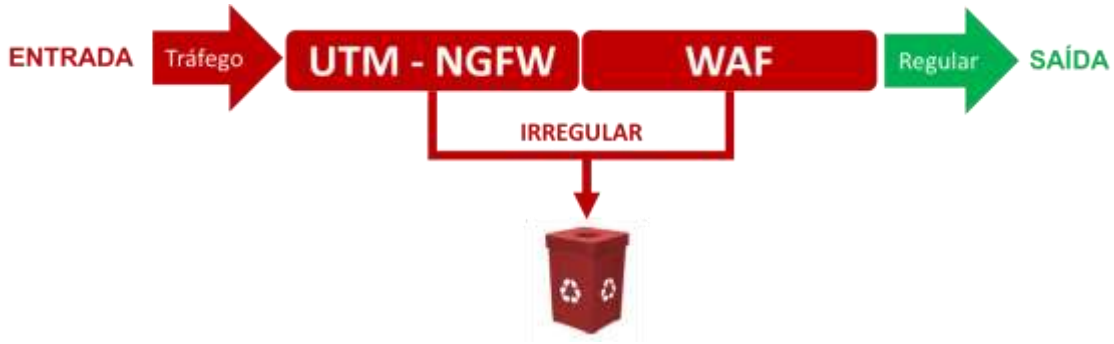

Figura 3 - Arquitetura proposta

O tráfego de entrada, que representa a requisição de acesso a um recurso provido pela empresa, é entregue a cada uma das componentes de forma sequencial. As requisições são analisadas e ações são tomadas com base em assinaturas, tipos de tráfego, classificações de acesso entre outras políticas a serem definidas com base nos modelos de negócio de cada cliente. Um tráfego identificado como irregular pode ser descartado ou simplesmente acionar um processo de alerta. O tráfego regular é enviado ao destino para acesso aos dados.

O desenho expõe um tráfego de entrada, inicialmente desconhecido e entregue à primeira componente UTM/NGFW[2] que corresponde à primeira camada de proteção e opera de forma independente das demais camadas. Na sequência, o tráfego aprovado é entregue a componente WAF[3] que atua nos níveis aplicacionais.

[1] A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade. Fonte: https://www.27001.pt/

[2] Firewall UTM/NGFW são dispositivos de software e hardware que permitem o controlo de tráfego entre redes distintas.

[3] WAF – Web Application Firewall. Executa funções de firewall no nível das aplicações. Diferente dos Firewalls UTM/NGFW, um WAF atua como um servidor intermediário que analisa o tráfego aplicacional.

Esta arquitetura permite oferecer um nível de proteção desde o acesso mais básico até à camada de aplicação acedida por um utilizador que insere dados pessoais, aferindo um nível de controlo e monitoração mínimos para atender aos padrões da indústria de segurança (Galegale, Fontes, & Galegale, 2017).

Cada componente é um módulo que pode operar de forma independente ou integrado para oferecer camadas de proteção contíguas que quando agregadas aumentam a capacidade de defesa da infraestrutura do cliente.

PARTE II

3. Análise técnica

A seguir serão descritas em detalhes as componentes das soluções de *firewall, web application firewall e DNS firewall* com suas subcomponentes, apresentando modelos de implementação descritos nos documentos oficiais de cada subsistema e métodos de integração dos módulos que permitirão o tráfego de dados ser inspecionado em uma arquitetura que oferece camadas de proteção sequenciais.

3.1.Firewall

Redes são um conjunto de elementos que permite a comunicação entre dispositivos (Bungart, 2018). A segmentação das redes é uma técnica para separar o tráfego para grupos de dispositivos que visa garantir a segurança dos dados e melhor capacidade na troca de informações (Mathew & Prabhu, 2017).

Uma firewall é um ativo de software ou hardware que tem como função específica, controlar o tráfego entre segmentos de rede com base em regras e políticas de acesso (Kumar S. N., 2015) e (Khan, 2017).

Para compreender melhor, a Figura 4 mostra o diagrama de uma firewall entre as redes externas e as zonas protegidas. O controlo pode ser aplicado entre qualquer zona onde a firewall tenha uma conexão de rede.

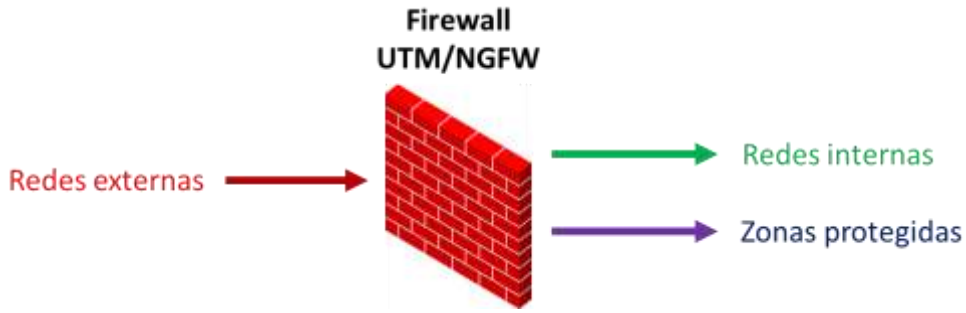

Figura 4 - Zonas protegidas e redes externas

Neste exemplo, apresentam-se os segmentos de redes externas, nomenclatura usual para as redes fora do domínio de controlo da organização. Este segmento é onde comumente estão conectados os dispositivos de interconexão com a Internet, redes de parceiros, clientes e outras conexões nas quais a organização não tem controlo. A firewall de

perímetro é instalada neste ponto da rede para controlar as interações entre o meio externo e as zonas internas.

Redes internas são segmentos de comunicação controlados pela organização, onde o fluxo de dados pode ser monitorizado, restringido ou liberado conforme as necessidades e regras do negócio.

Aqui, segmentamos em duas camadas:

- Redes internas: redes de acesso às informações, onde estão dispostos os dispositivos dos colaboradores, equipamentos de uso comercial, terminais de automação entre outros.
- Zonas protegidas: segmentos de rede onde são armazenadas as informações críticas para o negócio e que contem dados classificados, exigentes a um processo de controlo de acesso, implementando níveis de controlo até mesmo para as redes internas, sob domínio e gestão da organização.

3.1.1. Tipos de firewall

Há essencialmente 3 tipos de firewalls que atuam em diferentes camadas do modelo OSI (Kumar S. N., 2015) e (Sharma & Parekh, 2017):

- Packet filtering
- Gateway de circuito
- Stateful Inspection

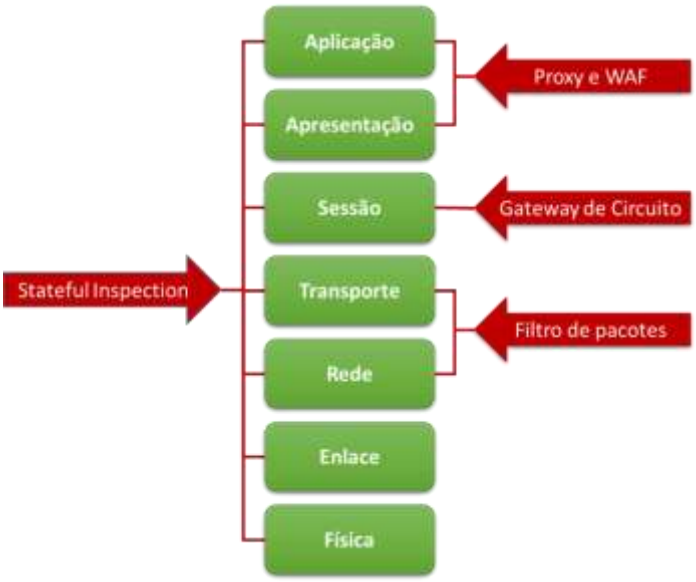

Figura 5 - Tipos de firewall e o modelo OSI

A Figura 5 exibe as camadas do modelo OSI em que estão inseridos os conceitos de cada tipo de firewall.

3.1.1.1. Packet Filtering

Na firewall de filtragem de pacotes, PF (Packet Filtering), é aplicado um controlo a partir de regras pré-definidas pelo gestor da aplicação. O pacote é analisado com base nas regras e a ação sobre seu tráfego é executada (Kumar S. N., 2015) e (Sharma & Parekh, 2017).

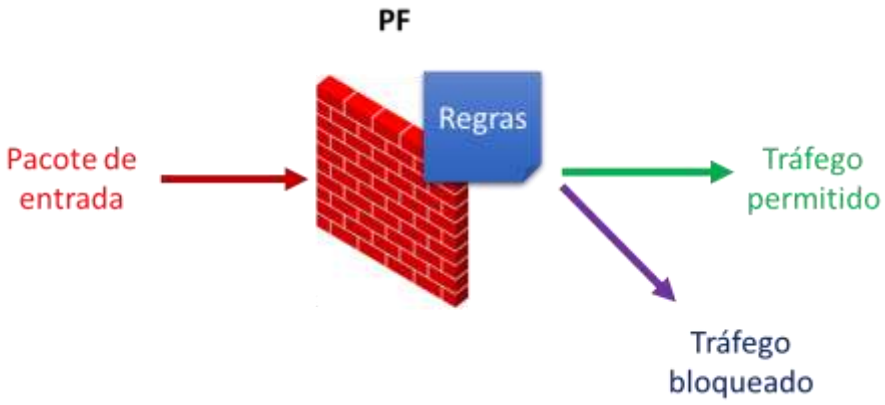

Figura 6 - Filtro de pacotes

Como exemplo, o acesso proveniente de uma rede externa como a Internet a um servidor Web instalado numa zona protegida requer que a firewall permita o tráfego no porto 80, onde são executados os serviços de publicação de páginas sob o protocolo *http*. Neste cenário, é necessária a configuração de uma regra específica na firewall para que o tráfego proveniente das redes externas com requisições de acesso às páginas web hospedadas no servidor, tenha a prévia autorização de passagem pela firewall no porto 80.

Os demais portos e acessos devem ser bloqueados pela firewall, reduzindo assim, o número de requisições e tráfego de origem externa a circular pelas componentes internas.

3.1.1.2. Proxy, gateways aplicacionais e de circuitos

As *firewalls* que atuam como *proxy* ou *gateways*, servem como intermediários na comunicação entre o cliente e o serviço final. As duas partes nunca interagem diretamente (Kumar S. N., 2015) e (Sharma & Parekh, 2017).

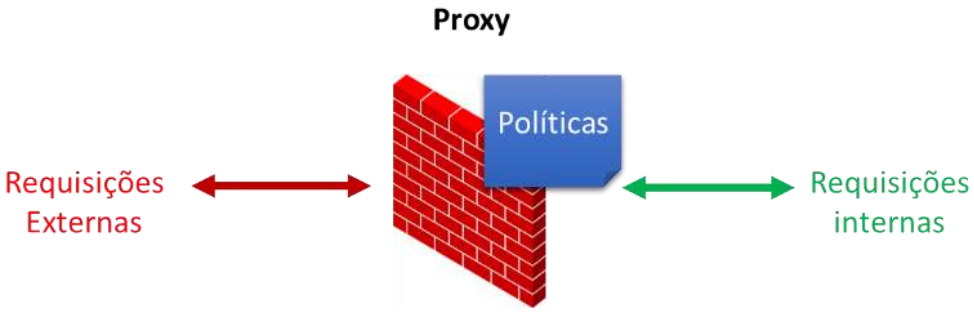

Figura 7 – Proxy

Um servidor *proxy* responde às requisições de um segmento de rede em nome do serviço protegido por esta componente.

No exemplo do item anterior, uma requisição externa a um serviço Web é direcionada ao servidor interno apenas no porto específico para a publicação dos conteúdos. Já com o uso de um *proxy*, a requisição é direcionada apenas à firewall que responde ao cliente em nome do servidor Web e como se fosse o próprio servidor. Desta forma, as requisições externas nunca chegam diretamente ao servidor Web. A comunicação com o servidor web é feita apenas pelo proxy e não mais diretamente por um redireccionamento do cliente.

3.1.1.3. Stateful Inspection

As *firewalls* de inspeção de estado analisam o tráfego para validar o estado das conexões de forma mais inteligente e profunda, verificando as sete camadas do modelo OSI e construindo uma tabela de estado. Esta tabela é usada no processo de decisão para validação de um pacote (Kumar S. N., 2015) e (Sharma & Parekh, 2017).

Nos exemplos apresentados, uma regra de firewall permite que um computador externo se conecte a um servidor Web instalado numa zona protegida. A firewall registará as informações de conexão. É então esperada a resposta do servidor, que analisada pela firewall tem o tráfego de retorno para a rede externa permitido sem a necessidade da criação e uma regra específica para a resposta do servidor. Conexões que não tem seu início baseados numa regra pré-definida, são bloqueadas ou alertadas pela firewall.

3.1.2. Firewall proposto

Para compor o produto final, a camada de firewall proposta deve atender aos requisitos previamente identificados de ser um sistema de código aberto, sem custos recorrentes de licenciamento e ser suportado em plataformas x86/amd64.

A solução de software de firewall proposta para ser integrada ao produto final é o pfSense®, distribuído sob a licença BSD, sem custos de licenciamento e incorpora os tipos de *firewlall* PF, *Proxy* e *Stateful Inspection*. O pfSense também acumula as funcionalidades UTM (*Unified Threat Management*) sendo também uma plataforma NGFW (*Next-Generation Firewall*).

Adicionalmente o pfSense conta com serviço de consultoria e suporte da empresa que o mantém, a Netgate, que pode ser contratado diretamente pelos clientes que buscam maiores garantias na sua operação.

Um UTM - *Unified Threat Management* é um sistema que centraliza em uma única plataforma, as características de filtragem de pacotes (PF), NAT, VPN, proxy web, antivírus, IDS/IPS e inspeção profunda de pacote (DPI) (Dwivedi & Rahul, 2017). A desvantagem deste tipo de sistema é que por estarem centralizadas, todas as funções partilham dos mesmos recursos o que pode causar um alto consumo de processamento, memória e disco do hardware em que está instalado.

Para resolver este problema, a indústria desenvolveu as plataformas NGFW que retiram alguns recursos dos UTM e os tornam mais especializados.

O pfSense é modular e pode conter tantas funcionalidades quanto necessárias, tanto de UTM como NGFW, para o controlo de uma infraestrutura sem a necessidade de ter todas habilitadas em simultâneo, o que permite uma gestão de recursos mais aprimorada. A Figura 8 apresenta a tela principal do sistema que contem grades de monitorização dos serviços que permitem o controlo do estado da plataforma.

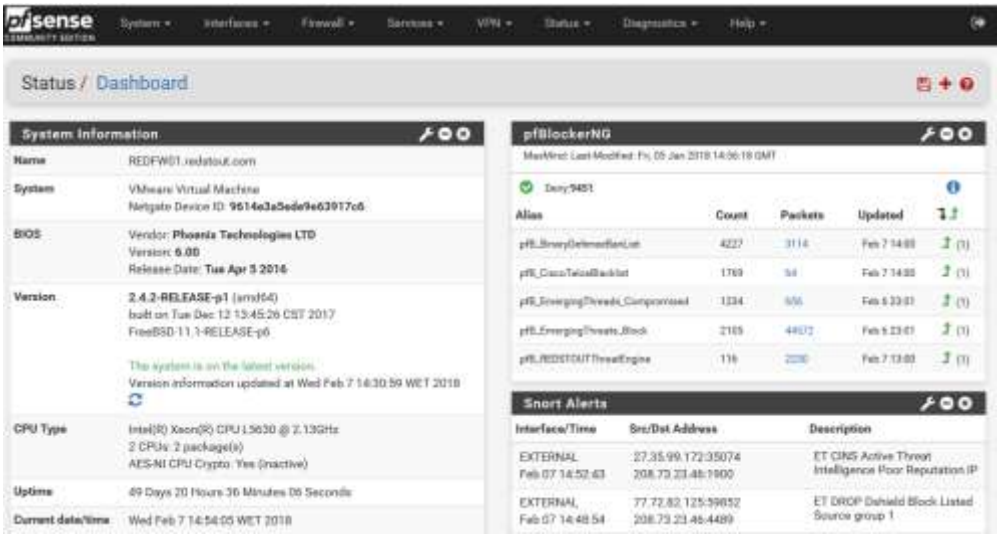

Figura 8 - Dashboard pfSense

Como módulos adicionais, foram integrados para controle do tráfego de saída, o Squid® Proxy Server que controlará os acessos de clientes localizados nas zonas protegidas, o pacote SquidGuard® que permite a criação de listas de acesso para controlar o tráfego dos utilizadores, o motor de antivírus ClamAV®, usado para deteção de *malwares*, *trojans*, vírus e outras ameaças.

Para o controlo do tráfego de entrada é mantido o Squid® Proxy Server que pode atuar como proxy reverso e publicar serviços das redes protegidas para o exterior, a plataforma pfBlockerNG® que trata o tráfego com base em listas de ameaças, endereços, reputação, usa as listas DNSBL (*Domain Name System Block List*) e a plataforma de IDS/IPS Snort®.

3.1.3. Arquitetura firewall

A arquitetura de firewall é a primeira camada do produto final. Esta camada não é um bloco único e indivisível. Possui subcamadas de proteção, ressaltando que maiores níveis de proteção são alcançados com um maior número de camadas habilitadas. Contudo, análises detalhadas das necessidades de cada cliente deverão ser levantadas como requisitos para definição de quais serviços internos da firewall deverão ser ativados para oferecer o melhor nível de proteção e desempenho.

A arquitetura proposta para a solução de firewall é apresentada no diagrama da Figura 9.

Figura 9 - Firewall - Arquitetura proposta

Aqui temos representados os tráfegos de entrada e saída, bem como um fluxo de tráfego regular e espúrio.

O tráfego de entrada refere-se às requisições de redes externas a dados e informações armazenadas em redes protegidas, tal qual o tráfego ao servidor Web exemplificado anteriormente. A partir de uma requisição de entrada que chega à firewall, as funções UTM/NGFW inspecionam os pacotes com base nas regras, listas e motores automatizados de inspeção para validar a origem e fiabilidade da requisição. Caso alguma das componentes de análise encontre distorções face ao comportamento esperado da requisição, a conexão é bloqueada e os pacotes descartados, sem atingirem o seu destino final.

O tráfego de saída refere-se a requisições internas a serviços localizados em redes externas e deve igualmente ser tratado para evitar que tais requisições estabeleçam sessões de comunicação com nós de rede contendo potenciais ameaças à infraestrutura e mais importante, aos dados e informações.

3.1.4. Soluções de mercado

O produto proposto neste trabalho possui similares já consolidados no mercado. Contudo as soluções disponíveis devem ser adquiridas a custos relativamente altos e, como citado nos capítulos anteriores, a proposta é de compor módulos integrados que forneçam os serviços de proteção de dados a custos reduzidos.

Com vista a validar a solução de firewall proposta, é necessária a comparação técnica da solução proposta a outras plataformas de mercado. Este processo pode validar a arquitetura de firewall ao confrontá-la com produtos de mérito já reconhecido.

Como plataformas de segurança devem manter-se tão atualizadas quanto possível, a revisão e comparativos das soluções de mercado frente ao pfSense® se iniciou no âmbito de relatórios publicados por entidades de pesquisa tais como Gartner® e Forrester Research®. Contudo, estas entidades não alimentam uma base com muitas plataformas *open source*, salvo algumas exceções, focando-se nos produtos comerciais. Durante a pesquisa das fontes de informação, chegou-se ao sítio da web *IT Central Station*[4] que realiza pesquisas recorrentes com o parecer de utilizadores e que não apresentou restrição em suas bases de pesquisa entre *firewalls* abertos e comerciais.

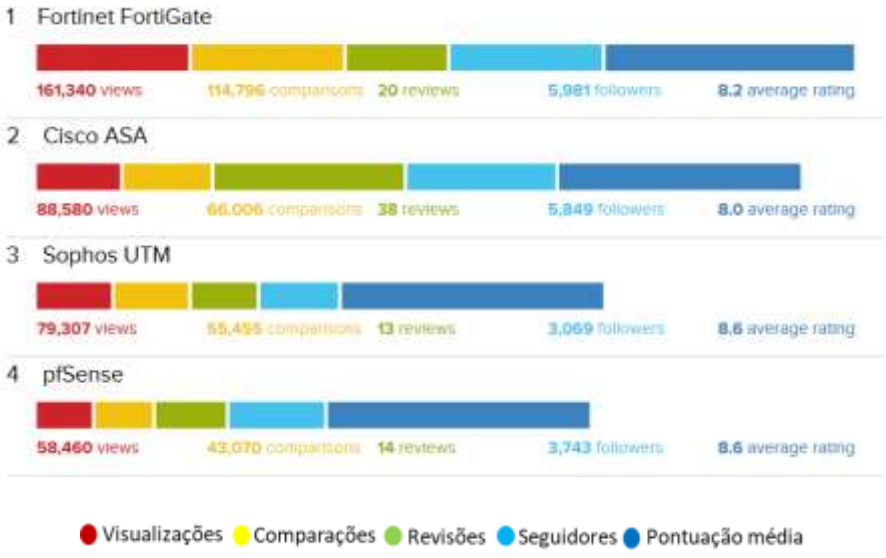

Figura 10 - Top Firewall Solutions[5]

Com base no relatório publicado pela *IT Central Station*, foram selecionadas as plataformas listadas na Figura 10, para a elaboração de uma tabela de funcionalidades.

A lista de características técnicas apresentadas na Tabela 1, não consideram todas as funcionalidades de cada produto usado no quadro de comparação, mas apenas as mais relevantes para a definição do produto final deste trabalho e que são comuns a todos.

[4] https://www.itcentralstation.com oferece uma pesquisa de crowdsourcing sobre tecnologias de TI e é usado como alternativa ao Gartner e ao Forresnter Research. Nota do autor.
[5] Gráfico extraído do documento "Firewalls Buyer's Guide and Reviews – January 2018". Disponível em http://www.itcentralstation.com

Tabela 1 – Funcionalidades extraídas dos datasheets[6]

	pfSense	Cisco ASA	Fortigate	Sophos UTM
Packet Filtering	Sim	Sim	Sim	Sim
VLAN Support	Sim	Sim	Sim	Sim
NAT Support	Sim	Sim	Sim	Sim
Stateful Inspection	Sim	Sim	Sim	Sim
pfBlockerNG	Sim	Sim**	Sim**	Não
Traffic Shaper	Sim	Sim	Sim	Sim
IDS/IPS	Sim	Sim	Sim	Sim
Filtro de conteúdo	Sim	Sim	Sim	Sim
Alta Disponibilidade	Sim	Sim	Sim	Sim
Suporte IPv6	Sim	Sim	Sim	Sim
VPN				
Ipsec	Sim	Sim	Sim	Sim
L2TP	Sim	Não	Sim	Sim
PPTP	Não	Não	Não	Sim
OpenVPN	Sim	Sim*	Sim*	Sim*
Web VPN	Não	Sim	Sim	Sim

* Suporte a SSL VPN
** Utiliza recursos próprios para implementar funcionalidades semelhantes

3.1.5. Diferenciais

Há de se destacarem 3 pontos importantes em que o pfSense se apresenta como uma plataforma diferenciada às demais analisadas:

3.1.5.1. Intrusion Detection and Prevention System

IDS/IPS são soluções que analisam o tráfego com base em assinaturas e identificam potenciais ameaças. O IDS, *Intrusion Detection System* é um sistema de alarmística que identifica potenciais ameaças e tentativas de intrusão, alertando aos engenheiros de rede acerca da natureza do tráfego malicioso. O IPS, *Intrusion Prevention System* é a evolução do sistema IDS, que permite a execução de ações previamente configuradas para bloquear uma ameaça no momento em que ela é identificada, de forma automatizada (Choi & Allison, 2017) e (Park & Ahn, 2017).

Uma solução de IDS/IPS implementada no pfSense é o Snort, a mesma usada pela companhia Cisco Systems, adquirida da Sourcefire, em sua linha de *firewalls*. As assinaturas podem ser disponibilizadas pela comunidade ou adquiridas na própria Sourcefire.

O pfSense permite a visualização das ameaças detetadas pelo Snort no seu painel de monitorização exibido na Figura 11, que exibe em tempo real as potenciais ameaças e

[6] Fonte: Datasheets dos fabricantes.

tentativas de conexão com a zona protegida. Os alertas são exibidos em numa lista e ações podem ser tomadas diretamente em cada registo, como bloquear o tipo de trêfego ou inseri-lo numa *whitelist* para liberação do fluxo de dados.

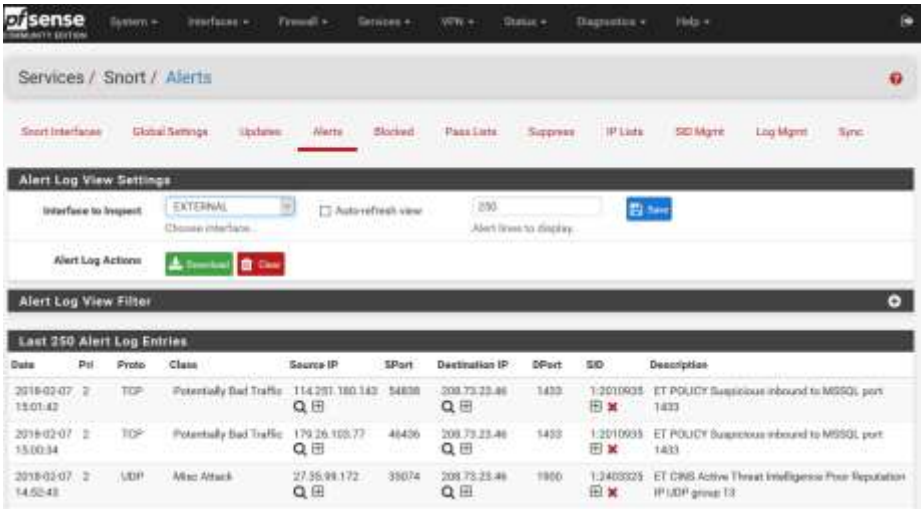

Figura 11 - Alertas Snort

O Snort é de implementação simples, bastando ativar o pacote na lista de funcionalidades disponíveis no pfSense. Pode fazer uso de listas de uso público e gratuitas bem como listas proprietárias, que exigem um valor de assinatura recorrente para seu acesso e utilização.

Em alternativa ao Snort, o pfSense possui suporte aos pacotes do Suricata, solução de IDS/IPS *open source*, tal qual o Snort, faz uso de assinaturas, com dois pontos a destacar que o diferencia do Snort:

- Mutithreading

  Diferente do Snort, o Suricata foi desenvolvido com suporte ao *multithreading*. Isto quer dizer que pode fazer uso de múltiplos *cores* em simultâneo, aumentado a sua capacidade de resposta a redes com maior tráfego (Park & Ahn, 2017).

- Integração Dragonfly MLE

> O Dragonly MLE (Machine Learnig Engine) é um mecanismo de análise de streaming, programável para deteção de ameaças à rede, construído no Redis[7], uma ferramenta de armazenamento de dados na memória, e no LuaJIT[8], uma linguagem de script. O MLE fornece uma estrutura para operacionalizar algoritmos de deteção de anomalias, pesquisas de inteligência de ameaças e previsões de aprendizado de máquina com modelos treinados. Foi projetado para funcionar em conjunto com um mecanismo de inspeção profunda de pacotes, como o Suricata.
>
> A sua implementação é objeto de estudo em comunidades de desenvolvimento de plataformas *open source* e foi considerado neste trabalho com a implementação de um protótipo em conjunto com o Suricata. Como modelo de base para o este trabalho, consideram-se os produtos em desenvolvimento OPNids, uma implementação do Suricata com o DragonflyMLE (OPNids, 2018) e Counterflow AI, uma implementação de algoritmos de Machine Learning para análise de tráfego de dados em redes de pacotes (CounterFlow AI, 2018).

O produto proposto pode conter o Snort ou Suricata integrados no pfSense ou ofertar implementação separada da componente Suricata sobre um sistema operativo Linux ou FreeBSD para a integração com a componente de aprendizagem automática Dragonfly MLE.

Para o cenário composto de duas implementações em separado (pfSense + Suricata/DragonflyMLE) é necessária a análise de tráfego do cliente, a definição dos algoritmos de análise e uma etapa de aprendizagem onde devem ser coletadas amostras de tráfego para compor os grupos de treinamento e avaliação dos comportamentos de rede.

Os algoritmos de aprendizagem automática permitem criar um modelo de comportamento esperado para o tráfego de rede com base na avaliação do comportamento num período de aprendizagem, oferecendo uma linha de comparação a fim de predizer o modelo de tráfego e executar ações quando o comportamento real difere do tráfego previsto.

[7] Redis é um sistema de código aberto para armazenamento de estrutura de dados na memória, usado como banco de dados, cache e message broker. Tradução livre do autor. Fonte: https://redis.io/

[8] Lua é uma linguagem de programação poderosa, dinâmica e leve. Tradução livre do autor. Fonte: http://luajit.org/luajit.html

A implementação do Dragonfly MLE é realizada em conjunto com o Suricata. O sistema IDS/IPS analisa o tráfego e gera alertas e mensagens com base em suas assinaturas. Estas mensagens são então analisadas pelo Dragonfly MLE que executa as ações com base nos comportamentos esperados (OPNids, 2018).

Os eventos de rede e de deteção de intrusão gerados pelo IDS/IPS são enviados aos algoritmos de aprendizagem automática que inserem um atraso no tempo de resposta face ao evento identificado. Isto quer dizer que ações serão executadas pelo algoritmo com um atraso em relação ao tráfego de rede sinalizado num evento. Este atraso está diretamente relacionado à capacidade de processamento disponível ao motor que executa os algoritmos. Sendo assim, recomenda-se a implementação em separado de outras componentes para evitar a perda de pacotes ou a passagem de tráfego não analisado para as redes protegidas.

3.1.5.1.1. Exemplo prático

É útil saber quantas conexões exclusivas estão sendo feitas por um determinado *host*. Quando combinado com os bytes enviados por cada nó, o número de conexões únicas e exclusivas pode ser usado para entender a diversidade de destinos e conexões que cada nó estabelece num determinado período e traçar um perfil de tráfego típico para a rede, criando um modelo de base para alarmes e identificação de comportamentos.

Para contar o número de conexões distintas realizadas por cada *host*, os ativos de rede devem manter uma lista de endereços IP exclusivos acedidos. Ou seja, a conexão iniciada pelo *host* A para o *host* B é registada como uma entrada na tabela; a conexão iniciada pelo *host* B para o *host* A corresponde a um novo e único registo na mesma tabela. Para o exemplo em questão vamos considerar apenas os endereços IP de cada *host*, mas a tabela contempla ainda os portos de início e terminação de cada conexão.

O número de entradas é definido por um arranjo onde o resultado de conexões é expressado pela função:

Número de conexões = H! / H-2!

Onde H é o número de *hosts* combinados dois a dois com dependência da ordem em que a conexão é estabelecida.

Assim, considerando uma rede com 100 nós, se cada nó estiver conectado a todos os outros nós nessa mesma organização, haverá 100! / (100-2)! = 9900 conexões possíveis.

Conforme visto na Figura 12Figura 12 - Número de conexões por hosts, para um aumento de 50 nós de rede o número de conexões é de 22350 e a função do arranjo que determina o número de conexões apresenta uma curva de crescimento que exige uma capacidade de análise de alto desempenho para soluções de inspeção de tráfego tradicionais.

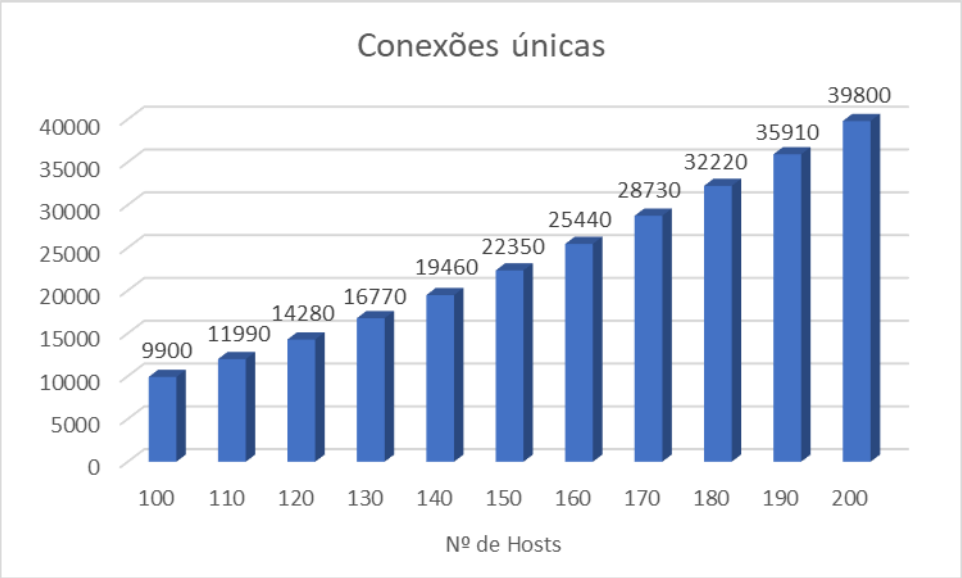

Figura 12 - Número de conexões por hosts

O cálculo dinâmico destas conexões, embora não complexo, exige recursos constantes de processamento e memória. Para otimizar a função de cálculo, o MLE introduz o algoritmo HyperLogLog para estimar o número de itens distintos em um conjunto (neste caso, o número de conexões distintas) dentro de uma percentagem de erro do número verdadeiro.

A aplicação deste algoritmo tem como objetivo executar a leitura do *streaming* gerado pelo IDS/IPS e gerar uma contagem aproximada das conexões únicas realizadas por cada *host*, armazenar um *hash* da contagem em um espaço restrito da memória sem a criação de extensas tabelas de conexões, o que permite acesso a informação de forma ágil e com baixo consumo dos recursos de processamento. O HyperLoLog é um algoritmo de *streaming* que executa este tipo de contagem com fatores de aproximação e margens de erro a reduzir com o aumento do número de elementos distintos (Allen, et al., 2018).

O HyperLogLog usa várias funções de *hashing* para mapear cada nova conexão reportada pelo Suricata usando uma estratégia de categorização. O *hashing* armazena a informação do número de conexões simultâneas e é usado por outros módulos nas análises de tráfego e comportamento. Desta forma, reduz-se a necessidade de consultas ou mesmo dispensa-se a criação de extensas tabelas para o registo das conexões, reduzindo a carga de processamento e memória.

A margem de erro varia conforme a quantidade de entradas registadas. Quanto maior o número de entradas registadas, menor será a margem de erro em relação a contagem real. De acordo com (Flajolet, Fusy, Gandouet, & Meunier, 2015), a margem de erro é de cerca de ±7% para 256 registos, ±3% para 1024 registos e ± 0.5% para 65536 registos.

Figura 13 - Margem de erro – HyperLogLog

A Figura 13 apresenta uma curva decrescente que indica menores taxas de erro para maiores volumes medidos. Isto vai de acordo com a ideia de uso de tabelas para redes com poucas entradas de *hosts* e o uso dos algoritmos de contagem para redes com maiores números de *hosts*.

A otimização deste processo permite o dimensionamento de plataformas de hardware menores e com custo mais acessível, sem a perda de qualidade e capacidade do tratamento do tráfego de dados.

O Dragonfly MLE é uma aplicação desenhada para a integração com ferramentas de inspeção de tráfego (CounterFlow AI, 2018). Embora seja possível a sua integração com o Snort, para efeitos deste trabalho, foi realizada uma bateria de testes com o Suricata, por ter melhor documentado os procedimentos de integração com os módulos

de aprendizagem automática do Dragonfly MLE. Contudo a aplicação deste módulo ainda requer um estudo adicional para a quantificação dos resultados, visto que no ambiente de testes virtualizado, desenhado para a idealização do produto final deste trabalho, encontram-se recursos limitados de memória e processamento que não permitem a simulação de altos números de conexões para minimizar a margem de erros prevista no estudo de (Flajolet, Fusy, Gandouet, & Meunier, 2015).

3.1.5.2. Snorby

Todas as tarefas de identificação de intrusão são executadas por processos automatizados. É de extrema importância obter uma visualização detalhada dos eventos para a identificação, análise e correção de falhas. Entretanto, o pfSense possui apenas uma tela de visualização dos eventos que não oferece um painel de alarmes e filtros adequados à operação dos sistemas (Snorby, 2018).

Como adicional no controle das informações geradas pelo Snort ou Suricata, foi instalada, em servidor independente, a plataforma de coleta de informações Snorby, específica para tratamento de dados provenientes de sistemas de deteção/prevenção de intrusos (Dietrich, 2015).

O Snorby exibe de forma simples e intuitiva os alertas gerados pelo IDS/IPS e contadores de registos que permitem a identificação dos eventos por seu grau de severidade e recorrência num período.

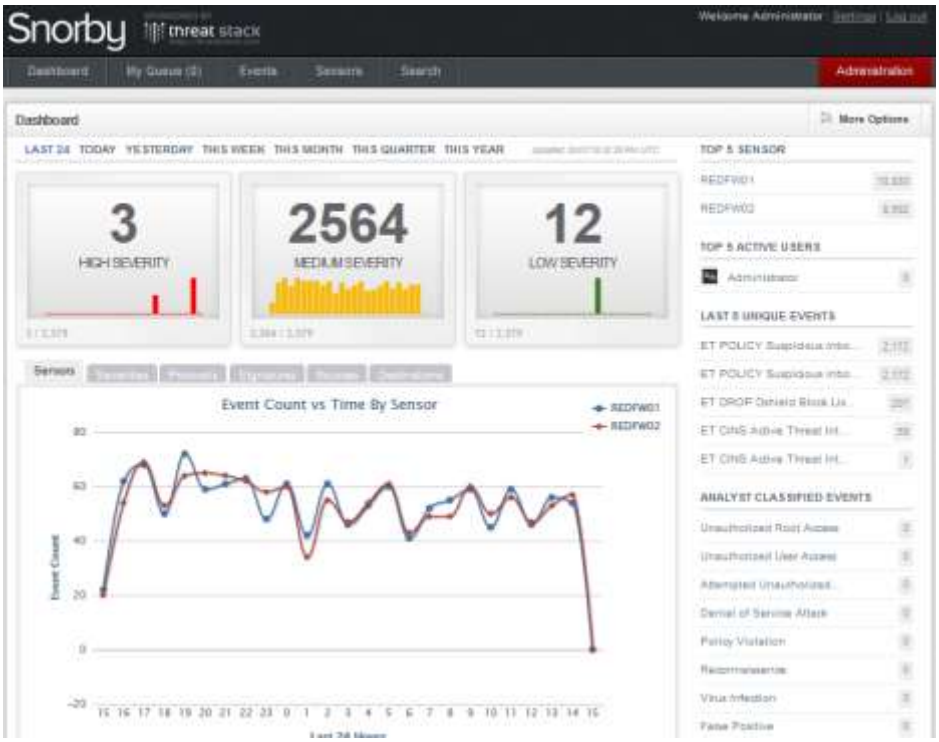

Figura 14 - Snorby - Tela principal

A Figura 14, exibe a tela principal do Snorby e nela pode-se observar a contagem de alertar e seu grau de severidade. A apresentação simples em um painel intuitivo permite a tomada de ações rápidas para o controlo de eventos críticos de segurança. Este tipo de painel não é nativo do pfSense, pelo que se recomenda o uso de ferramentas auxiliares para obter um melhor resultado de visualização de eventos.

Figura 15 - Snorby - Lista de eventos

Estatísticas de eventos relacionados a assinaturas específicas são geradas, conforme visto na Figura 15, o que permite a identificação de vulnerabilidades ou falhas na configuração de sistemas. É importante manter uma constante monitorização sobre os eventos para mitigar falhas e corrigir os problemas, prevenindo assim a ocorrência de eventos catastróficos com perda de informação.

Figura 16 - Snorby - Assinaturas mais frequentes

Por se basear em assinaturas, é importante ainda observar quais métodos são mais frequentemente identificados pelo sistema a fim de promover a correção ou revisão de arquitetura com foco a mitigar a fraqueza no ambiente do cliente. A ferramenta permite visualizar os eventos recorrentes com maior incidência de casos conforme apresentado na Figura 16.

É de se prever que ao elevar o grau de maturidade da infraestrutura do cliente com base nas informações e ações corretivas e de prevenção suportadas pelo Snorby, que o número de eventos e alarmes tenha a tendência em diminuir. Contudo, é importante salientar que a atividade de monitorização e melhoria deve fazer parte de um ciclo constante num processo de avaliação e mudança dos sistemas com foco em segurança.

3.1.5.3. Antivírus

O motor antivírus integrado ao proxy do pfSsense é o ClamAV, *open source* que tem o apoio da Cisco Systems. Esta componente pode ser aplicada no nó de rede de interconexão com redes externas a fim de mitigar a intrusão de aplicações maliciosas como vírus, malwares e trojans.

O serviço proxy implementado no pfSense pode integrar o motor do ClamAV de forma transparente ao utilizador, ofertando uma subcamada de proteção na firewall.

No ambiente de testes, foi implementado o Squid Proxy com uma lista simples de controlos de acesso e como teste, foi realizado o acesso a partir de uma estação de trabalho protegida pelo serviço de proxy e antivírus, com a tentativa de download do ficheiro eicar.txt[9]. A ferramenta de antivírus identificou o conteúdo com base em suas

[9] EICAR é um grupo europeu para a segurança da informação que disponibiliza ficheiros de testes que contem assinaturas de malwares. http://www.eicar.org

assinaturas e efetuou o bloqueio da sua transferência impedindo a infiltração de um ficheiro malicioso, conforme visto na Figura 17:

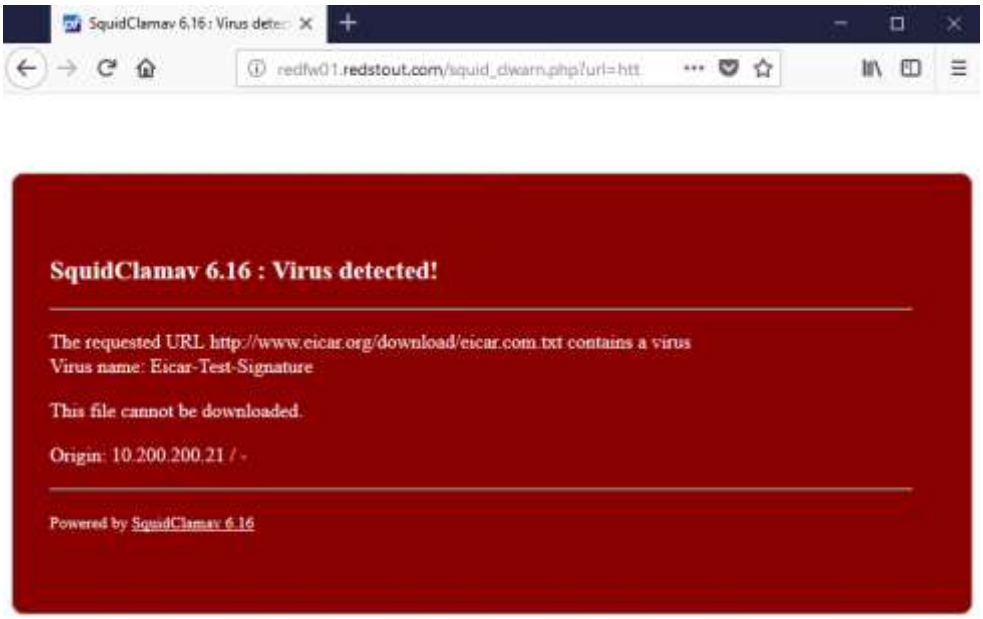

Figura 17 - Tela de bloqueio do motor antivírus

3.1.5.4. Filtro de conteúdo

Filtros de conteúdo são subsistemas comumente incorporados à *firewalls* mas também apresentados em plataformas independentes para suportarem maior carga e análise de tráfego. Têm como objetivo, identificar conteúdos de páginas web e executar ações de bloqueio, alertas e registos de acesso dos utilizadores.

Segundo (Kumar & Kumar, 2014), dispositivos de segurança de rede consistem em uma ou mais funções de segurança, incluindo firewall, sistemas de prevenção e deteção de intrusões (IPS/IDS), prevenção de perda de dados (DLP) e funções de filtragem de segurança.

A solução de controlo de conteúdo é aplicada no módulo de proxy através do Squid Guard, uma ferramenta de controlo que faz uso de listas de acesso para organizar os grupos e perfis de websites e aplicar políticas baseadas em conteúdo com suporte a listas de classificação de uso livre.

Figura 18 - Exemplo de configuração de políticas por grupos

A ferramenta Squid Guard, permite com base em listas, especificar ações conforme o conteúdo identificado nos acessos. O exemplo da Figura 18, apresenta o bloqueio de sites de encontros e drogas em seus conteúdos. Permite o acesso a sites de downloads.

Conteúdos bloqueados podem emitir alertas diretamente aos utilizadores para informar acerca dos motivos que levaram ao bloqueio de sua navegação (Figura 19). As páginas podem ser personalizadas com mensagens de conscientização para promover a educação no uso dos recursos corporativos.

Figura 19 - Tela de bloqueio de website por conteúdo

3.1.5.5. Bloqueio por listas de endereços

Algumas companhias elaboram e publicam listas contendo endereços IP identificados como originadores de ameaças tais como *malwares*, vírus e *trojans*. Dentre estas, destacam-se a Talos[10], Binary Defense[11] e Proofpoint (EmergingThreats)[12].

O pfSense integra o módulo pfBlocker, um subsistema de controlo de acessos que usa listas de referência, geolocalização e nomes de domínio para controlar o tráfego entre redes. Como diferencial técnico competitivo, o pfBlockerNG permite a leitura em

[10] https://www.talosintelligence.com/
[11] https://www.binarydefense.com/
[12] https://www.proofpoint.com

tempo real destas listas e a criação de regras dinâmicas que usam as informações online para o processo de decisão sobre o fluxo de pacotes.

Para reduzir o processamento, leitura e escrita destas listas, foi desenvolvido um script, inserido no ANEXO I, que deve ser executado de forma automatizada e periódica em um servidor web para a disponibilização de uma lista única e centralizada que permite a consolidação das informações de diversas listas publicadas na Internet num único, simples e organizado ficheiro em formato texto; na sequência, a lista é publicada num *host* virtual web acessível pelo pfSense que periodicamente atualiza a lista interna a ser usada pelo pfBlockerNG.

Isto oferece ao cliente a soma das análises de domínio público sobre endereços que possam comprometer seu negócio.

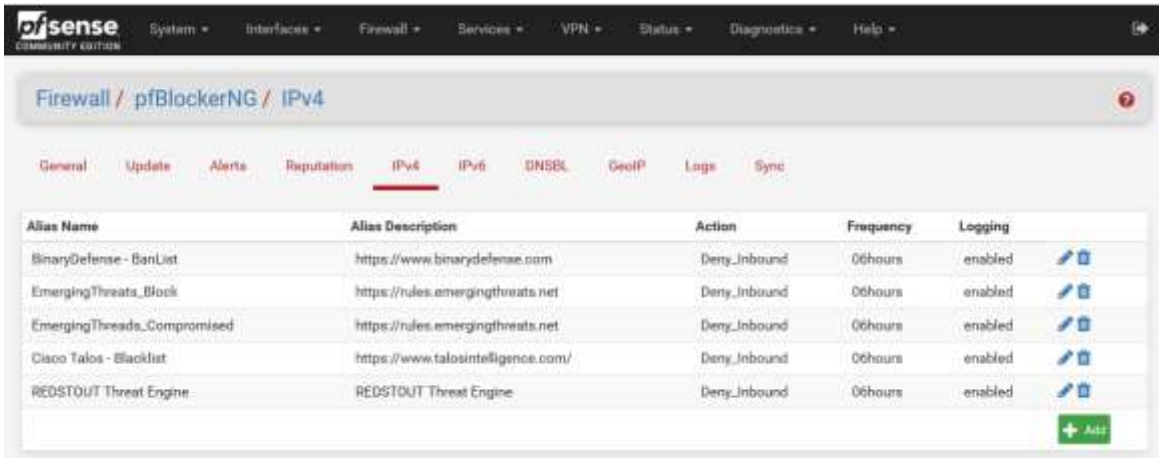

Figura 20 - Tela de configuração das listas no pfBlockerNG

A configuração do pfBlocker no ambiente de teste configurado para este trabalho contemplou a criação de uma lista única baseada em quatro listas públicas, conforme visto na Figura 20. O ficheiro parcial contendo a lista utilizada nos experimentos é apresentado no ANEXO II.

3.1.6. Comparativo

Há uma série de funcionalidades presentes em todas as soluções que são base para a definição de uma firewall do tipo UTM/NGFW, tais como o *Packet Filtering*, *Proxy*, *Stateful Inspection*, antivírus, entre outras. Outros módulos internos, opcionais, são desenhados e implementados conforme a necessidade e foco de mercado, como

exemplo o pfBlockerNG, nome de um sistema integrado ao pfSense que tem funcionalidades semelhantes em componentes proprietárias de outras marcas.

Face aos itens em comum de cada solução que caracterizam os produtos selecionados para o comparativo como uma firewall UTM/NGFW, o pfSense não apresenta quaisquer restrições que reduzam a sua capacidade de operação no aspeto funcional em relação às outras plataformas.

3.2. Web Application Firewall

Firewalls UTM/NGFW, IDS e IPS conseguem proteger ambientes de TI de diversos ataques. Entretanto, para ataques do tipo SQL *Injection*, *Cross site Scripting* (XSS), *Local File Inclusion* (LFI), *Remote File Inclusion* (RFI), *Remote Code Execution* (RCE), *PHP Code Injection*, *Application Denial of Service* entre outros, essas ferramentas não são eficazes. Surge então a necessidade do uso de uma plataforma de segurança que consiga mitigar estas ameaças.

Um WAF (*Web Application Firewall*) é um *gateway* aplicacional que atua nos níveis 6 e 7 do modelo de referência OSI. Um WAF observa o conteúdo da aplicação e consegue identificar ameaças e ataques específicos com base em assinaturas e comportamentos (Nico, Funk, & Cappo, 2018).

Por atuarem no nível aplicacional, esta componente de segurança analisa os pacotes HTTP e HTTPS que têm como destino o servidor web que hospeda as aplicações.

O diagrama da Figura 22 apresenta a arquitetura com o fluxo de tráfego a entrar pela *firewall* UTM/NGFW, o protocolo http/https em duas formas: legítimo/regular e ilegítimo/irregular. O tráfego não HTTP/HTTPS é analisado e tratado na componente de Firewall UTM/NGFW (pfSense).

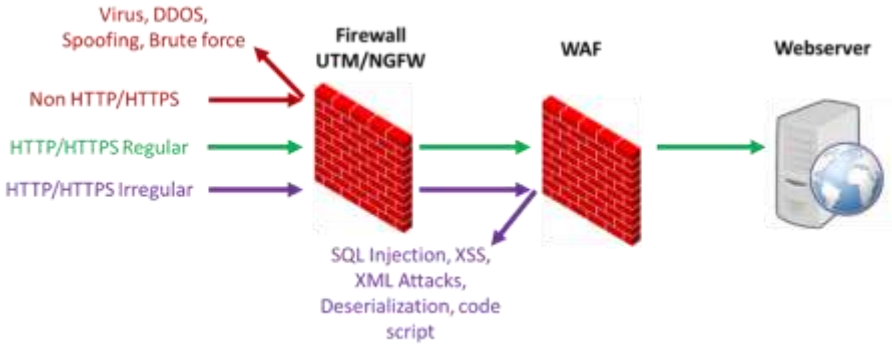

Figura 21 - Arquitetura UTM/NGFW e WAF

Como componente de segurança aplicacional, foi selecionada a solução WAF *open source* ModSecurity® que pode ser instalada em sistemas operativos Linux e conta com assinaturas de padrões de tráfego e ameaças aplicacionais publicadas por organizações independentes como o OWASP[13].

3.2.1. Assinaturas, padrões e metodologias

As assinaturas emitidas pela OWASP podem ser integradas em soluções WAF de diversos fornecedores, inclusive *open source* através do projeto OWASP ModSecurity Core Rule Set[14]. O OWASP publica periodicamente o OWASP TOP 10, lista com as 10 categorias de riscos aplicacionais mais recentes que são usadas pela maioria dos sistemas de WAF. A plataforma ModSecurity pode ainda lançar o motor antivírus ClamAV para inspecionar o envio de ficheiro ao servidor web. Esta componente é habilitada com um script LUA apresentado no ANEXO III.

3.2.2. Modos de operação

A solução WAF pode ser implementada em 3 diferentes modos de operação (Prasad & Rao, 2017):

Proxy reverso – Não há conexão direta entre o requisitante e o servidor web. Neste modo os pacotes podem ser inspecionados, modificados e bloqueados.

Proxy transparente – As requisições são enviadas diretamente ao IP do servidor web e o WAF pode inspecionar, modificar e bloquear o tráfego.

Proteção offline – O WAF atua apenas como monitor do trafego entre o requisitante e o servidor web. O tráfego é redirecionado para o WAF, sem interferências na comunicação cliente servidor.

3.2.3. Publicação de sites e SSL

No modo Proxy Reverso, o website é publicado pelo WAF, isolando o servidor web de qualquer conexão externa direta. O certificado digital garante a conexão criptografada

[13] O OWASP (*Open Web Application Security Project), em português* Projeto Aberto de Segurança em Aplicações Web é uma comunidade que estuda, elabora e divulga metodologias e recursos de análise aplicacional.
[14] https://coreruleset.org/

entre o utilizador e os dados aplicacionais. Como o tráfego precisa ser inspecionado pela componente WAF, há essencialmente dois modos de conseguirmos efetuar a análise:

SSL Inspection – A inspeção de certificado utiliza apenas o certificado do servidor web para desencriptar o tráfego, a fim de analisá-lo por violações de políticas. Se não houver violações, permite que o tráfego criptografado existente continue sem interrupção.

Figura 22 - SSL Inspection

Neste modo, o servidor web mantém a criptografia desde a origem dos dados aplicacionais até o cliente. Isto pode ser exigido em algumas aplicações ou motivado por legislações de proteção a dados.

SSL offload – Neste modo, o certificado SSL é atribuído no WAF que mantem uma conexão criptografada com o cliente, abre os pacotes, inspeciona, aplica as políticas de segurança e encaminha as requisições em protocolo aberto (http) para o servidor web protegido.

Como vantagem deste método há de se perceber que o processo de criptografia dos pacotes não está mais no servidor web e fica agora na componente WAF. A aplicação web opera assim, em um ambiente com menos carga de processamento, podendo dar foco à aplicação e não mais à segurança.

Figura 23 - SSL Offload

3.2.4. Arquitetura proposta

A arquitetura desenhada para a solução de *web application firewall* apresentada no diagrama da Figura 24 implementa subcamadas de proteção que contem a inspeção de certificados e tráfego criptografado, perfis de aplicações criados com base em uma aprendizagem realizada com amostras de tráfego, assinaturas de tráfego e a correlação de eventos.

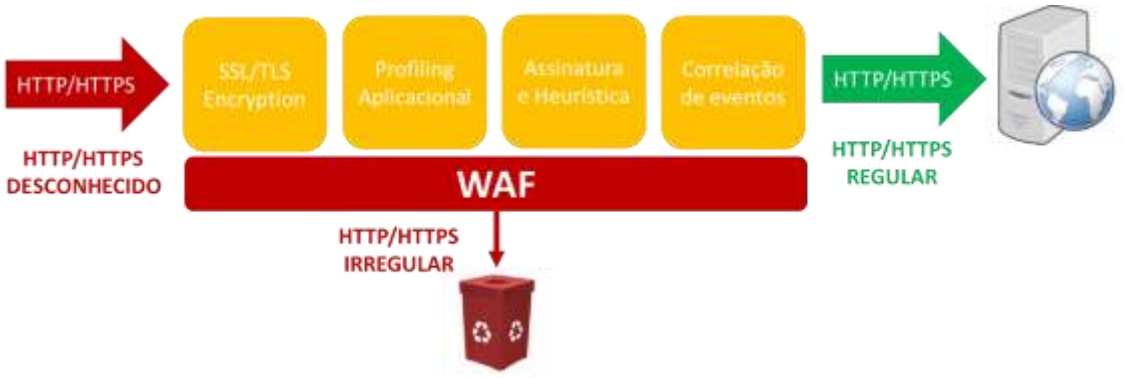

Figura 24 - WAF - Arquitetura proposta

Após o tratamento pelas subcamadas, o tráfego espúrio é descartado e o tráfego regular é encaminhado ao seu destino, sem alterações. O tráfego bloqueado pode gerar alertas para os utilizadores e administradores dos sistemas a fim de validarem o conteúdo bloqueado.

3.2.5. Soluções de mercado

Com vista a validar a solução de *web application firewall* proposta, recorreu-se à comunidade do IT Central Station para o levantamento e classificação das plataformas de WAF mais relevantes do mercado. Dentre as plataformas publicadas no sítio da web, destacam-se o Cloudflare e o Imperva Incapsula, soluções líderes e baseadas na nuvem que são usadas para análise comparativa.

3.2.6. Comparativo

Em um estudo publicado pelo *Zero Science Lab*[15], intitulado "CloudFlare vs Incapsula vs ModSecurity", (Petrushevski, Krstic, & Cabrera, 2013) apresentaram os resultados comparativos de testes executados nas três plataformas citadas em seu título. Os

[15] Zero Science Lab é um laboratório de pesquisa e desenvolvimento de segurança da informação. Fundada em 2007 pelo pesquisador de segurança, Gjoko Krstic. Fonte: https://www.zeroscience.mk/en/about/

números foram transcritos na Tabela 2 e expressam os números absolutos aferidos nos testes de proteção a aplicações web.

Tabela 2 - Comparativo WAF

Fonte: Zero Science Lab

	Cloudflare	ModSecurity	Incapsula
SQL Injection			
Blocked	0	54	53
Passed	54	0	1
Total		54	
XSS			
Blocked	0	46	43
Passed	46	0	3
Total		46	
LFI/RFI			
Blocked	0	21	19
Passed	23	2	4
Total		23	

Para além dos valores aferidos nos testes, a componente ModSecurity permite trazer a Core Rule Set, que é conjunto de regras genéricas de deteção de ataques para uso com o ModSecurity ou *firewalls* de aplicativos da Web compatíveis. O próprio projeto OWASP refere-se às regras como sendo "OWASP ModSecurity Core Rule Set"[16], desenhada para uso com o ModSecurity.

A integração ao projeto OWASP é um grande fator diferencial para a seleção do ModSecurity. Isto aliado aos resultados dos testes apontam o ModSecurity como uma plataforma fiável para compor a solução de WAF, implementada em servidor separado da firewall e que pode atuar em linha com o tráfego previamente inspecionado pela primeira camada de proteção, constituindo assim, a segunda camada do produto final deste trabalho.

3.3.Domain Name System Firewall

O ISC – *Internet Systems Consortium*[17] é uma organização fundada em 1994 com objetivo de manter e distribuir o sistema de nomes de domínio BIND. Atua ainda na orientação de padrões para o serviço DNS.

[16] https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project
[17] https://www.isc.org/

Uma vasta lista de aplicações e recursos na web utiliza o Sistema de Nomes de Domínio como base para identificar *hosts* e serviços. Tal qual as aplicações legítimas, as ameaças digitais podem fazer uso do DNS para identificar alvos e desencadear ataques cibernéticos. Neste sentido o ISC desenvolveu o conceito RPZ - *Response Policy Zone*, uma componente que permite implementar no serviço DNS uma política de consulta com verificação de listas antes da consulta pública ou interna a uma base de nomes. Isto permite atuar no controlo da requisição para evitar o contato direto do cliente com os destinos maliciosos.

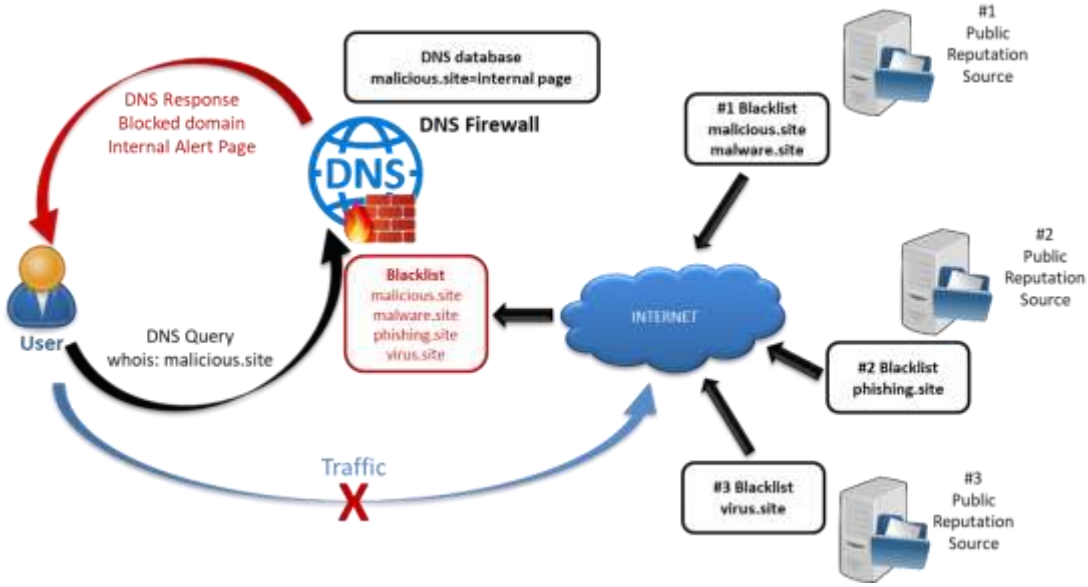

Figura 25 - Fluxo de dados - DNS Firewall

Uma firewall DNS é um servidor DNS que intercepta seletivamente a resolução de DNS para ativos de rede maliciosos conhecidos (ISC, 2018). A intercetação pode reescrever uma resposta do DNS para direcionar o requisitante para um destino seguro na web ou simplesmente não dar visibilidade aos ativos de rede maliciosos por parte dos clientes de rede, conforme apresentado no fluxo de requisições DNS da Figura 25.

Para além de proteger os dispositivos da infraestrutura interna, este tipo de solução oferece uma camada de proteção mesmo fora do perímetro de segurança da firewall UTM/NGFW. Isto porque as consultas DNS podem ser direcionadas sempre ao DNS Firewall que por uma ação de desinformação não permitirá aos clientes terem o conhecimento dos destinos listados em suas bases de dados de ameaças. Isto é especialmente importante para as empresas que adotam o conceito BYOD, "*Traga seu*

próprio dispositivo (BYOD), que permite que os funcionários carreguem seus dispositivos pessoais com eles para executar tarefas de trabalho conectando-se à rede e aos recursos corporativos."[18] (Herrera, Ron, & Rabadão, 2017).

A implementação da solução de DNS firewall é uma camada adicional de proteção não integrada à arquitetura final do produto, mas que oferta maior capacidade na identificação e mitigação de ameaças e riscos digitais.

3.4. Arquitetura final proposta

A plataforma proposta possui duas componentes básicas:

- Firewall UTM/NGFW
- WAF (Web Application Firewall)

A arquitetura difere quanto ao sentido do tráfego. Isto porque o tráfego proveniente das redes externas é inicialmente desconhecido e necessita de uma profunda análise e inspeção para permitir os acessos a recursos internos. A zona externa é o maior ponto de ameaça para as informações, visto que o movimento dos dados para esta zona representa o maior risco de exfiltração de informações e deve ser minuciosamente controlado.

No sentido oposto, temos o tráfego originado numa zona controlada, mas que representa também, riscos de perda de dados, pois da mesma maneira, embora originado nas redes internas, tem como destino zonas externas fora do controlo da organização.

Com isto temos um produto final cuja arquitetura para o tráfego de entrada é mostrada na Figura 26.

O tráfego de entrada é entregue na componente de Firewall UTM/NGFW, tratado pelos módulos: pfBlockerNG, *Packet Filtering* e IDS/IPS (Snort/Suricata). Na sequência a componente de WAF recebe os pacotes e valida o endereço de destino, desencripta o tráfego SSL, verifica o comportamento com base nas assinaturas da Core Rule Set, executa o motor antivírus ClamAV e finalmente acede ao serviço web hospedado no servidor protegido.

[18] Tradução livre do autor: *There are many trends in today's technology, one of those is known as "Bring Your Own Device (BYOD)," which allows workers to carry their personal devices with them to perform work tasks by connecting to the network and corporate resources*.

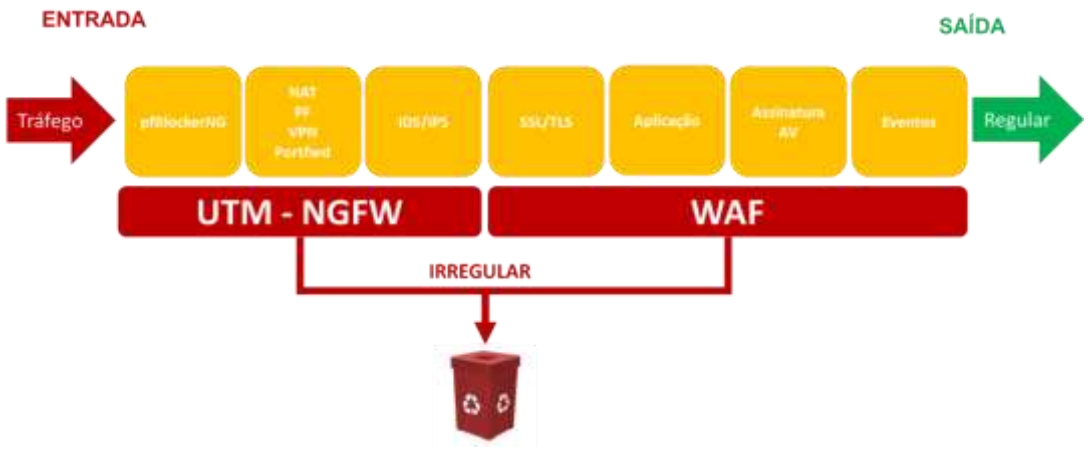

Figura 26 - Arquitetura - tráfego de entrada

O tráfego de saída partilha de controlos com o tráfego de entrada, nomeadamente o pfBlockerNG, IDS/IPS, NAT e PF, componentes implementados exclusivamente na firewall. Adicionalmente, o tráfego de saída ainda conta com o URL Filtering que fornece limitações de acesso conforme o tipo de conteúdo a ser acedido.

Conforme visto na Figura 27, o controlo do tráfego de saída, originado nas redes internas, a arquitetura mostra-se levemente invertida, sem contar com a componente de WAF.

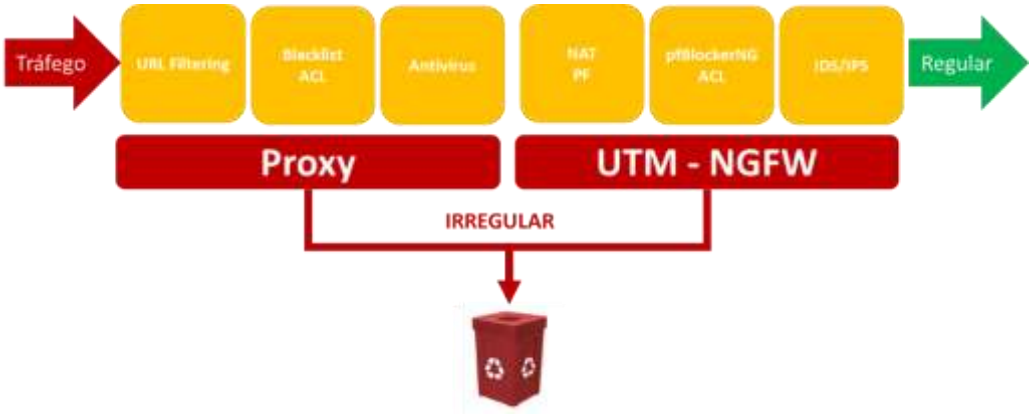

Figura 27 - Arquitetura - Tráfego de saída

A Tabela 3, lista os itens integrantes da solução de firewall e WAF definidos no desenho da arquitetura exposto na Figura 26 e Figura 27 .

Tabela 3 - Componentes e módulos

pfSense	Módulos
	pfBlockerNG
	Snort
	Squid Proxy Server
	Squid Reverse Proxy
	SquidGuard Proxy Filter
ModSecurity	**Módulos**
	apache2
	libapache2-modsecurity
	modsec-clamscan.lua
Snorby	
	Opcional

A componente de Firewall DNS deve ser considerada de forma independente à solução Firewall UTM/NGFW e WAF e deve ser vista como uma camada de proteção adicional com vista a reduzir os acessos a conteúdos maliciosos.

3.5. Conclusão – Parte II

No âmbito técnico, a plataforma composta pelo pfSense e seus módulos aliada ao ModSecurity implementado em servidor à parte é uma linha de defesa adequada para a proteção de perímetro a modelos de negócio que necessitem ter seus dados publicados na Internet. Por se tratar de uma plataforma modular, cada uma das componentes pode ser integrada de forma independente a uma infraestrutura heterogênea.

A componente informacional Snorby tem uma função muito específica e deve ser considerada sempre que o Snort/Suricata ou outra solução de IDS/IPS for utilizada.

Para uma proteção mais abrangente, a extrapolar o perímetro digital proporcionado pela componente de Firewall UTM/NGFW, o DNS Firewall é essencial, pois oferece uma camada de defesa inicial, além-fronteiras, que mitiga ataques que utilizem os serviços de nomes para identificação dos *hosts* e serviços maliciosos. Adicionalmente, o Firewall DNS reduz a carga e impactos nas componentes de Firewall UTM/NGFW por reduzir o número de acessos provenientes de ambientes que hospedam ameaças.

3.6. Trabalho futuro – Parte II

Como trabalho futuro, pretende-se desenvolver a integração plena com o Dragonfly MLE de modo a obter uma interface gráfica para a implementação dos algoritmos e

acompanhamento do processo de aprendizagem de máquina. Propõe-se ainda a validação da integração do Dragonfly MLE com o Snort.

Como adicional e expansão dos campos de estudo deste trabalho, propõe-se a avaliação do Tensorflow, uma biblioteca de aprendizagem automática, de código aberto, desenvolvido por pesquisadores e engenheiros da *Google Brain Team* bem como outras bibliotecas de aprendizagem automática que possam fornecer códigos e algoritmos com o objetivo de reduzir a carga de processamento e memória das *appliances* físicas ou virtuais, para o melhor uso dos recursos computacionais aplicados ao produto final.

PARTE III

4. Análise económica e de mercado

Na sequência da análise técnica dos produtos apresentados na Parte II deste trabalho, serão identificados aspetos económicos e de mercado para a criação de um produto que permita oferecer proteção digital com competitividade técnica e financeira, garantindo a sustentabilidade nas suas várias vertentes.

A principal motivação deste trabalho é a criação de um produto acessível a pequenos negócios que permita a transformação digital com segurança. Serão identificados aspetos económicos e de mercado para a criação de um produto que permita oferecer proteção digital com competitividade técnica e financeira.

Todos os sistemas selecionados são de licenciamento aberto e sem despesas recorrentes com renovações ou suporte, o que reduz consideravelmente o custo total de aquisição (Miranda, Vieira, & Carelli, 2008), apresentado em detalhe a seguir. Como abordagem principal, a plataforma foi configurada na nuvem em servidor dedicado, o que permite a flexibilidade para o crescimento e suporte a carga de múltiplos clientes sem a necessidade de grandes investimentos iniciais.

Os sistemas permitem ainda serem integrados em arquiteturas i386/x64, isto leva a uma vasta gama de hardware disponível no mercado para compor uma solução. Neste sentido, foi realizada uma pesquisa de campo para reconhecer dispositivos de hardware compatíveis com os sistemas pfSense, Ubuntu Linux, CentOS Linux e FreeBSD.

O objetivo deste estudo é a criação de um produto competitivo. A competitividade, palavra chave, se apresenta sob dois conceitos para o desenvolvimento de um produto que proporcione aceitação de mercado:

- Qualidade técnica do produto
- Custo total de uso e propriedade

4.1. Custo total de uso e propriedade

O custo total de uso e propriedade é uma avaliação de indicadores financeiros que definem o valor de um bem. No âmbito do produto proposto neste trabalho, o custo total

inclui a aquisição, gestão e suporte de hardware e software, custo de inatividade e outras perdas de produtividade.

A implementação das componentes deve ser tratada como um projeto que por definição "*é um conjunto de atividades temporárias, realizadas em grupo, destinadas a produzir um produto, serviço ou resultado únicos.*" (Project Management Institute, s.d.).

Assim, avaliações de custos das componentes de hardware e software somadas aos serviços, formação e consultoria devem ser consideradas para a definição do custo total de uso e propriedade do objeto deste estudo.

4.2. Capital humano

A primeira componente a ser considerada na análise financeira deste projeto é o custo do capital humano, visto que a implementação no cliente final é tratada como um projeto e seus custos associados vão muito além da simples aquisição de um hardware, mas deve ser composta por custos de serviços de preparação do ambiente físico, como instalações elétricas e de rede de dados para a interconexão dos equipamentos, instalação física dos servidores e das configurações dos sistemas de segurança (Santos M. A., 2018).

A solução requer para sua implementação a atuação de 3 tipos de profissionais (PORDATA, 2018):

- **Profissional com formação média**

Recurso humano com qualificação mínima para a instalação de equipamentos em ambientes tecnológicos, cablagem, instalações elétricas e itens afins.

- **Profissional qualificado**

Recurso humano com educação de nível superior nas áreas das Engenharias Informática, Telecomunicações ou afins.

- **Profissional altamente qualificado**

Recursos humano para além das qualificações acima citadas, que possua formação e/ou conhecimentos específicos nas tecnologias constituintes dos sistemas de Firewall UTM/NGFW, WAF e DNS Firewall. Deve ser um profissional com capacidade de

assimilar novas tecnologias, prover suporte ao corpo técnico e apto a passar conhecimento. Recomenda-se níveis de metrado ou doutoramento.

4.2.1. Fonte de dados

O portal PORDATA – Base de Dados Portugal Contemporâneo, mantido pela Fundação Francisco Manuel dos Santos, recolhe, organiza, sistematiza e divulga informações sobre múltiplas áreas da sociedade, para Portugal (PORDATA, 2018). Dentre as informações constantes no seu portal, podem ser acedidos dados referentes aos valores salariais mensais médios praticados na economia portuguesa, ver Tabela 4Tabela 4 - Média salarial em Portugal.

Tabela 4 - Média salarial em Portugal

Fonte: https://www.pordata.pt

Ano	Remuneração base média	Ganho médio
2014	909,50 €	1 093,20 €
2015	913,90 €	1 096,70 €
2016	924,90 €	1 107,90 €

Os valores referidos na Tabela 4 - Média salarial em Portugal, serão considerados para o cálculo do custo dos profissionais de formação média e que atuarão de forma direta em atividades que envolvem a fixação de *appliances* físicas em bastidores, a organização da cablagem e tarefas diversas necessárias para a implementação em ambiente do cliente. Os profissionais precisam ter formação mínima nas áreas técnicas com conhecimentos e experiência na instalação de bastidores e ativos de rede.

A solução proposta para a implementação na nuvem e configuração das *appliances* físicas requer profissionais com qualificação mínima em sistemas e redes o que nos faz considerar valores mais específicos que compreendam mão-de-obra qualificada. A mesma fonte permite-nos consultar e aferir valores médios para profissionais qualificados, conforme observado na Tabela 5, distribuídos ao longo dos anos de 2014, 2015 e 2016.

Tabela 5 - Média salarial em Portugal - Profissionais qualificados

Fonte: https://www.pordata.pt

Ano	Profissionais altamente qualificados	Profissionais qualificados
2014	2 025,00 €	1 615,70 €
2015	2 007,50 €	1 604,90 €
2016	2 001,90 €	1 572,70 €

4.2.2. Valor hora

A definição de valores em diferentes períodos para o capital humano é importante nesta etapa do projeto, pois permite a flexibilidade no sentido de fracionar a carga de trabalho para estabelecer um valor estimado mais próximo do real (Santos M. A., 2018).

Com os valores salariais publicados até o ano de 2016, foi aplicado um fator de correção médio, calculado pela diferença entre os 3 anos listados para em seguida, definir os valores salariais expectáveis para o ano de 2018.

Tabela 6 - Valor mensal, diário e hora

Período	Profissionais altamente qualificados	Profissionais qualificados	Profissionais de nível médio
Mensal (22 dias)	2.048,10 €	1.658,70 €	1.222,60 €
Diário (8h/dia)	93,10 €	75,40 €	55,57 €
Hora	11,64 €	9,42 €	6,95 €

O valor médio mensal foi ainda redimensionado para aferir um valor de custo de mão de obra com base em dias e horas. Estes números podem ser usados na alocação de recursos nos projetos de implementação que suportarão a criação de um plano orçamentário a ser apresentado para o cliente final.

4.3.Produtos e parceiros

A implementação de cada componente requer o mapeamento de parceiros e produtos para criar uma composição que integre o serviço a ser ofertado para o cliente final com as partes de sistemas descritas nos capítulos anteriores.

4.3.1. Implementação na nuvem

A implementação de uma arquitetura em nuvem oferece benefícios de custos e flexibilidade para o dimensionamento de equipamentos para atenderem a diversas

cargas de tráfego. A configuração de elementos para a composição da plataforma na nuvem prevê a parceria com provedores de hospedagem de serviços.

Segundo (Diniz, Costa, & Medeiros, 2017), dentre outras, as principais vantagens da implementação de soluções na nuvem são a redução de investimentos em infraestruturas e com pessoal especializado. Isto permite criar um cenário mais acessível para empresas com menor potencial de investimentos.

Dentre os maiores provedores, destacam-se a Amazon Cloud Services, Rackspace, Google Cloud e Microsoft Azure (Dignan, 2018) que possuem ofertas de servidores com características e compatibilidade para suportar a implementação dos serviços na nuvem. O reconhecimento de mercado adquirido ao longo do tempo e da demonstração da qualidade destes fornecedores é fator a ser considerado para a inclusão de suas marcas na análise financeira. Contudo, o projeto em questão pretende desenvolver novos produtos, valorizar especialmente o mercado português, reter capital e conhecimento no espaço nacional. Assim, foram considerados para a análise financeira, apenas fornecedores nacionais e em alternativa, fornecedores no espaço comum europeu, cuja oferta esteja alinhada com os perfis da componente técnica.

A Tabela 7, apresenta as configurações exigidas para um servidor dedicado na nuvem. Os valores de cada componente computacional foram atribuídos com base comparativa ao modelo XG-1537 U, linha média da Netgate[19], fabricante de produtos com suporte oficial ao pfSense.

Tabela 7 - Requisitos mínimos para servidor dedicado[20]

Requisitos mínimos	
CPU	
Clock: 1.7 GHz	Cores: 8
RAM	
8 GB ECC 2133	
Storage	
SSD: 256 GB	SATA: 1 TB

4.3.1.1. Oferta em Portugal

Em breve pesquisa de mercado, foram identificados 4 fornecedores com oferta de produtos qualificados para compor a solução técnica:

[19] https://www.netgate.com/solutions/pfsense/xg-1537-1u.html
[20] Valores obtidos com base comparativa das configurações do produto Netgate XG-1537.

- **OVH** é um provedor de serviços de hospedagem, multinacional com unidades na Europa.
    - Produto EG-16

        CPU: Intel Xeon E3-1230v6 - 4/8t - 3.5GHz /3.9GHz

        RAM: 16GB DDR4 ECC 2400MHz

        Discos: RaidSoft 2x4TB
- **EVS Portugal** é um provedor de serviços de Internet com ofertas de servidores dedicados.
    - Produto I7-2600

        CPU: Intel Core i7- 2600 or 3770

        RAM: 16GB

        Discos: HDD 2X 3TB SATA
- A empresa **.Rede** (leia-se Ponto Rede), tem sede no concelho de Aveiro que oferece serviços de hosting, servidores virtuais e dedicados.
    - Produto: .Rede D1

        CPU: Processador Core i7

        RAM: 12GB

        Discos: HDD 2000GB
- A **Iberweb** é uma empresa fornecedores de serviços de datacenter pertencente ao grupo Lusologia, com sede na cidade de Braga em Portugal.
    - Produto: STAR 2

        CPU: Intel Xeon Quad-CoreE3-1270v3 3.5GHz 8MB

        RAM:16GB - KingstonDDR3 1600MHz ECC

        Discos: 2 X 1 TB RAID 1 - Western Digital SATA III

Foram obtidos os custos fixos mensais em Euros, listados na Tabela 8, associados a cada produto na nuvem[21]:

Tabela 8 - Custos fixos mensais - Servidores dedicados

Fornecedor	Modelo	Valor/mês
OVH	EG-16	64,99 €
EVS Portugal	I7-2600	69,99 €
.Rede	.Rede D1	120,00 €
Iberweb	STAR 2	139,00 €

[21] Valores dispostos nos sites dos fornecedores em 28/08/2018.

4.3.1.2. Capital humano – Solução na nuvem

Com base na implementação de um laboratório na nuvem, estima-se o consumo em horas de trabalho conforme exposto na Tabela 9. Esta estimativa inclui o item de "Configurações Básicas" que contem os ajustes de endereçamento IP, atribuição de utilizadores para acesso administrativo, ajustes de hora, *hostname* e instalação dos pacotes de proxy, antivírus e pfBlocker com configuração das listas de reputação de endereços IP.

Configurações adicionais devem ser validadas em trabalho interno em cada cliente a fim de coletar informações sobre serviços específicos que devem ter seus acessos protegidos e garantidos pelas plataformas de segurança.

Tabela 9 - Esforço - Implementação na nuvem

Solução na nuvem			
Item	**Profissionais altamente qualificados**	**Profissionais qualificados**	**Profissionais de nível médio**
Sistema Operativo	-	1,0	-
Configurações Básicas	-	1,0	-
Coleta de dados do cliente	2,0	2,0	-
Implementação de regras	1,0	4,0	-
Testes	1,0	3,0	-
Migração	1,0	1,0	-
Produção	1,0	1,0	-
Tempo de implementação (h)	**6,0**	**13,0**	**0,0**
Custo da Hora (Euros)	11,64	9,42	6,95
Custo Total (Euros)	**69,8**	**122,5**	**0,0**

4.3.2. Implementação em hardware específico

Como alternativa à implementação na nuvem e com vista a atender necessidades de clientes que por quaisquer motivos não possam ter seus dados dispostos fora de seu próprio ambiente ou para a garantia de maior desempenho, foi desenhada a implementação dos sistemas em hardware específico.

4.3.2.1. Hardware

Item essencial neste modelo de negócio, apontou para a necessidade de integração de hardware especializado com suporte aos sistemas operativos FreeBSD, Ubuntu e CentOS Linux. Neste contexto, fez-se a integração com dispositivos produzidos no

espaço comum europeu, visto que não foram encontrados fabricantes em território nacional português.

Adotando os limites mínimos computacionais da solução na nuvem, foi realizado o trabalho de obter-se as cotações de preços para hardware com requisitos mínimos de CPU 2.7 GHz, memória RAM a 8 GB e disco 128 GB SSD ou 1 TB SATA.

O espaço europeu não ofereceu muitas alternativas, sendo apenas um fabricante apontado nas consultas com um produto adequado e certificado para os sistemas de código aberto e com o requisito de produzir um *hardware* genuinamente europeu.

A DECISO[22], empresa com sede na Holanda produz uma *appliance* com tecnologia alemã e oferta linhas de produtos para pequenos escritórios até soluções mais robustas com suporte a conexões de 10 Gbps. No âmbito técnico, as appliances produzidas pela DECISO apresentam-se como opção de hardware a ser integrado no produto final deste trabalho. Para além das características técnicas, o facto de ser uma empresa baseada na Holanda, permite manter o capital financeiro dentro do espaço europeu.

Figura 28 - Appliance 1 U - DEC4610 – Deciso

Com vista a manter um padrão de compatibilidade entre as especificações das componentes integradas na nuvem, e para efeitos deste estudo considera-se apenas a appliance DEC4610, equipamento de média capacidade, com preço de lista na ordem de 1799,00 Euros[23].

A appliance conta com um processador Quad Core Intel Xeon de 3,3 GHz, com 8 GB de memória RAM e disco duro de 128 GB SSD.

[22] https://www.deciso.com/ - Designed & Made in The Netherland
[23] Fonte: https://www.deciso.com/product-catalog/dec4610/

4.3.2.2. Capital humano – Solução em hardware dedicado

O esforço assemelha-se ao dedicado para a solução na nuvem, adicionadas as componentes de testes e instalação física do *hardware*. Estima-se o consumo em horas de trabalho conforme exposto na Tabela 10, com base nas informações do portal PORDATA e nas projeções de horas de trabalho para a execução de cada tarefa. Esta estimativa, em consonância com a implementação na nuvem, contempla o item de "Configurações Básicas" que contem os ajustes de endereçamento IP, atribuição de utilizadores para acesso administrativo, ajustes de hora, *hostname* e instalação dos pacotes de proxy, antivírus e pfBlocker com configuração das listas de reputação de endereços IP.

Tabela 10 - Esforço - Implementação em hardware dedicado

Solução on premises			
Item	**Profissionais altamente qualificados**	**Profissionais qualificados**	**Profissionais de nível médio**
Sistema Operativo	-	1,0	-
Configurações Básicas	-	1,0	-
Validação do ambiente	-	1,0	1,0
Teste energia elétrica	-	-	1,0
Cablagem	-	-	1,0
Instalação física	-	-	1,0
Testes de acesso	-	1,0	1,0
Coleta de dados do cliente	2,0	2,0	-
Implementação de regras	1,0	4,0	-
Testes	1,0	3,0	-
Migração	1,0	1,0	-
Produção	1,0	1,0	-
Tempo de implementação (h)	**6,0**	**15,0**	**5,0**
Custo da Hora (Euros)	11,64	9,42	6,95
Custo Total (Euros)	**69,8**	**141,4**	**34,7**

4.4. Mercado e concorrência

Uma avaliação da concorrência é essencial para definir a estratégia de abordagem do mercado alvo (Hass, 2017). Por se tratar tipicamente de soluções integradas de código aberto, a inteligência e diferencial da solução proposta neste trabalho estão no modelo de integração, características especificas de códigos escritos à medida para a coleta e tratamento de dados púbicos que aferem maior qualidade aos motores de análise automatizada das componentes de Firewall UTM/NGFW, DNS Firewall e Web

Application Firewall. No âmbito financeiro, a solução apresenta-se como alternativa a plataformas de propriedade fechada, de alto custo.

4.4.1. Mercado alvo

O produto tem como alvo o mercado de pequenas e médias empresas que não possuem amplitude financeira para a aquisição de serviços de segurança de alto custo e recursos humanos para atuar em soluções complexas de segurança da informação. A solução busca ainda beneficiar o governo, onde busca inserir componentes de menor custo para reduzir os gastos públicos.

Adicionalmente, em qualquer nível de serviço, as componentes técnicas permitem a redução de riscos digitais de forma semelhante a soluções proprietárias e empresas que possuem a necessidade de implementação de múltiplas camadas de proteção que podem se beneficiar na adoção de diferentes tecnologias para proverem um nível de proteção mais avançado e heterogêneo.

4.4.2. Produtos concorrentes

Diversos produtos assemelham-se à solução proposta de *Firewall* e WAF. A seleção de concorrentes para a comparação foi realizada com base na classificação feita pelo grupo IT Central Station que considera de forma agnóstica todas as plataformas de segurança e publica opiniões de profissionais inseridos no mercado de trabalho. Para este estudo, foram selecionados os 3 primeiros classificados no relatório de *Firewall* publicado em março de 2018. Para a componente de *Web Application Firewall*, foram selecionados o Imperva Incapsula e o Cloudflare, presentes no relatório de (Petrushevski, Krstic, & Cabrera, 2013). Foi ainda inserido o produto da empresa Sucuri[24], que tem semelhanças técnicas marcantes com a proposta deste trabalho e está presente nos relatórios do grupo IT Central Station, publicação mais recente e que também cita os produtos Imperva e Cloudflare como líderes no segmento de proteção a aplicações web.

4.4.2.1. Firewall

A análise da componente de *firewall* é realizada apenas no modelo embarcado em *hardware*. Isto pelo facto de que os produtos concorrentes não ofertam soluções de *firewall* na nuvem e não apresentam bases para uma comparação neste nível. Embora

[24] https://sucuri.net/

haja produtos de *firewall* na nuvem, estes são comercializados fora do espaço europeu o que não faz interceção de mercado com o alvo que se pretende atingir com este trabalho.

Deste cenário pode-se extrair o entendimento de que para além do comparativo a seguir, a solução proposta neste trabalho apresenta um produto diferenciado por permitir a implementação da componente de *firewall* na nuvem com vista a controlar o tráfego seja por listas de acesso, regras e serviços ou pela concentração de conexões VPN em um ambiente externo à rede do cliente, mas sob sua administração.

Para esta componente destacam-se as principais marcas de mercado, conforme o relatório do IT Central Station:

1. Cisco
2. Fortinet
3. Sophos

Para efeitos deste estudo, consideramos os custos de mão de obra idênticos para a implementação de todas as soluções. Assim, o diferencial encontra-se essencialmente nos produtos comercializados.

A Tabela 11 apresenta os custos apurados de cada plataforma e o custo total de aquisição projetado para 1 ano, 2 anos e 5 anos. Os valores foram obtidos a partir dos preços de lista dos produtos em sites dos fabricantes, parceiros e revendas.

Tabela 11 - TCO Firewall[25]

Firewall					
Produto	**Período**	**Cisco 5516-X**	**Sophos XG 210**	**Fortigate 100D**	**Hardware**
Appliance	-	2.120,00 €	1.250,54 €	1.165,44 €	1.799,00 €
Suporte	1 ano	2.053,72 €	-	295,00 €	-
IPS/Antivirus/Webfiltering/ Antispam	1 ano	-	2.941,00 €	1.038,00 €	-
TCO	**1 ano**	**4.173,72 €**	**4.191,54 €**	**2.498,44 €**	**1.799,00 €**
	2 anos	6.227,44 €	7.132,54	3.831,44	1.799,00 €
	5 anos	12.388,60 €	15.955,54	7.830,44	1.799,00 €

O custo total de propriedade de um sistema de código aberto não afere valores recorrentes de licenciamento e suporte. Isto reduz consideravelmente o valor final de aquisição e mais notável ainda quando diluído ao longo do tempo.

[25] Custos das Appliances obtido em www.amazon.com. Custo das componentes Cisco 5516-x obtido em http://www.kernelsoftware.com/products/catalog/cisco.html. Custo das componentes Fortigate 100D obtido em http://www.avfirewalls.com/FortiGate-100D.asp. Custo das componentes Sophos XG 210 obtido em https://www.enterpriseav.com/XG-210.asp. Custo da componente de Hardare da solução proposta obtido em https://www.deciso.com/product-catalog/dec4610/.

4.4.2.2. Web Application Firewall

A componente de WAF pode ser integrada em uma *appliance* física para ser instalada na infraestrutura do cliente. Contudo, os produtos utilizados para comparação com base no relatório de (Petrushevski, Krstic, & Cabrera, 2013), e do grupo IT Central Station, ofertam soluções na *cloud*, sendo a Sucuri e Cloud Flare, empresas com produtos exclusivamente neste modelo de oferta. Dentro desta perspetiva, serão abordadas apenas as soluções implementadas na nuvem:

1. Cloudflare
2. Imperva Incapsula
3. Sucuri

Tabela 12 - TCO WAF[26]

WAF					
Produto	**Período**	**Cloudflare**	**Imperva incapsula**	**Sucuri**	**Cloud**
Hosting	1 mês	200,00 €	299,00 €	299,00 €	120,00 €
TCO	**1 mês**	**200,00 €**	**299,00 €**	**299,00 €**	**120,00 €**
	12 meses	2.400,00	3.588,00	3.588,00	1.440,00 €
	60 meses	12.000,00	17.940,00	17.940,00	7.200,00 €

4.4.3. Investimentos e retorno

O plano de investimento prevê valores em separado para cada componente a fim de fornecer um produto final contendo todos os módulos propostos no capítulo 3.

Os custos iniciais de um projeto contemplam a aquisição de uma *appliance* física e os valores apurados de mão de obra para a implementação de todas as soluções em hardware dedicado, conforme visto na Tabela 13.

[26] Custos obtidos nos sites dos fabricantes Cloudflare, Imperva e Sucuri. Comparativo Cloud com base nos valores mencionados na Tabela 8 - Custos fixos mensais - Servidores dedicados.

Tabela 13 - Custo total de implementação[27]

Produto em hardware dedicado				
	Unidade	Quantidade	Valor unitário	Valor total
Aquisição da Appliance	Unidade	1	1.799,00 €	1.799,00 €
Profissional altamente qualificado	Hora	6	11,64	69,84
Profissional qualificado	Hora	13	9,42	122,46
Profissional de nível médio	Hora	4	6,95	27,8
Custo total				**2.019,10 €**
Mais valia	**25%**			**504,78 €**
Custo final ao cliente				**2.523,88 €**
Custo final ao cliente + IVA	**23%**			**3.104,37 €**

O custo total de um projeto de implementação é estimado em 2.019,10 Euros. A margem de retorno no projeto é estimada em 25% o que determina um custo final ao cliente na ordem de 2.523,68 a acrescer o IVA em vigor.

O baixo custo de um projeto individual dispensa cálculos rebuscados para a projeção de fluxos de pagamento, pelo que os valores aferidos serão contabilizados em apenas duas frações, sendo a primeira na entrega do hardware ao cliente e a segunda no fecho do projeto, estimado em 5 dias de duração.

4.4.4. Concorrência empresarial

A Associação de Empresas de Software Open Source Portuguesas, ESOP[28], é a organização em Portugal que agrega as empresas com ofertas de código aberto. Em seu rol de associados, lista apenas a Eurotux[29], situada no distrito de Braga, como companhia fornecedora de serviços de infraestrutura e segurança a possuir um produto semelhante ao proposto neste trabalho.

Isto alerta para o facto de que o mercado português, embora tenha presença de empresas de código aberto, possui carência em provedores de serviços qualificados para suportarem soluções de infraestrutura e segurança.

[27] Valores consolidados das tabelas 6, 9 e 10.

[28] A ESOP é uma associação empresarial que representa as empresas portuguesas que se dedicam ao desenvolvimento de software e à prestação de serviços baseados em tecnologias Open Source. Fonte: http://www.esop.pt/sobre-a-esop/#a-nossa-missao

[29] A Eurotux Informática S.A. é uma empresa especializada em planeamento, integração e implementação de sistemas informáticos, oferecendo soluções de tecnologias de informação construídas à medida das necessidades dos clientes. Fonte: https://eurotux.com/empresa

4.5. Conclusão - Parte III

Face aos dados de mercado e a composição financeira da plataforma, conclui-se que o sistema de segurança composto pelas componentes de firewall, WAF e DNS Firewall podem ser adquiridos a preços competitivos confrontados com a concorrência de sistemas de código fechado. Estudos de viabilidade técnica e financeira podem beneficiar com a inserção dos sistemas abertos em seus processos de seleção, de modo a criar uma linha de referência para comparativos tecnológicos agnósticos, sem a interferência do marketing das grandes marcas.

4.6. Limitações e trabalho futuro – Parte III

Esta etapa teve como limitações a utilização de limitados fornecedores de serviço para efeitos comparativos de custos. Parte destas limitações são naturais do mercado, por não encontrarmos empresas portuguesas e mesmo europeias a fornecerem produtos nacionais ou regionais.

Como trabalho futuro propõe-se a elaboração de um plano de marketing com vista a segmentar o mercado alvo dos produtos de segurança da informação e a adequação técnica e financeira do produto final ao consumidor alvo detetado ao fim deste plano. Na sequência, espera-se prosseguir a elaboração de um plano de negócios completo que permita a avaliação financeira e viabilidade de projeto para a criação de um produto competitivo em todos os aspetos comerciais.

PARTE IV

5. Impacto socioeconómico

Em julho de 2014, o governo português firmou com a União Europeia, um acordo de parceria denominado Portugal 2020[30] que está alinhado com os objetivos da União Europeia, denominado Estratégia Europa 2020[31]. Este acordo tem a atuação de 5 fundos europeus estruturais e de investimento e visa desenvolver áreas de interesse comum entre Portugal e EU com objetivos claros e específicos.

> "Estímulo à produção de bens e serviços transacionáveis; Incremento das exportações; Transferência de resultados do sistema científico para o tecido produtivo […] Promoção do desenvolvimento sustentável, numa óptica de eficiência no uso dos recursos; Reforço da coesão territorial, particularmente nas cidades e em zonas de baixa densidade; Racionalização, modernização e capacitação da Administração Pública […]." (Comissão Européia & República Portuguesa, 2014).

5.1. Estratégia Europa 2020 e Portugal 2020

A Estratégia Europa 2020 possui metas que são usadas como referências pelos governos nacionais da UE para definirem suas próprias metas nacionais (Estratégia Europa 2020, s.d.). O programa Portugal 2020 desdobra estas metas para objetivos regionais e prioriza as ações com base nas medições da Estratégia Europa 2020, publicadas em relatórios intercalares pelo Eurostat[32]. Dentre as prioridades da Estratégia Europa 2020/Portugal 2020, destacam-se para o âmbito deste trabalho o "Crescimento inteligente" e "Crescimento inclusivo"[33].

[30] Trata-se do ACORDO DE PARCERIA adotado entre Portugal e a Comissão Europeia, que reúne a atuação dos 5 Fundos Europeus Estruturais e de Investimento, entre 2014 e 2020. Fonte: https://www.portugal2020.pt/Portal2020

[31] A estratégia Europa 2020 é a estratégia da UE para o crescimento e o emprego. Fonte: https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_pt

[32] Eurostat é uma organização estatística da União Europeia.

[33] Fonte: https://www.portugal2020.pt/Portal2020/o-que-e-o-portugal2020

5.1.1. Crescimento inteligente

A prioridade Crescimento Inteligente (Estratégia Europa 2020, s.d.) possui 3 objetivos primários:

1. Reforçar a investigação, o desenvolvimento tecnológico e a inovação;
2. Melhorar o acesso às tecnologias da informação e da comunicação, bem como a sua utilização e qualidade;
3. Reforçar a competitividade das pequenas e médias empresas e dos sectores agrícola, das pescas e da aquacultura.

A solução proposta neste trabalho permite atingir os 3 objetivos em questão. Ao desenvolver em território nacional um produto com base de código livre, complementado por desenvolvimento de código em Portugal e integrado em hardware genuinamente europeu, é inserido na primeira prioridade citada anteriormente, ao reforçar a investigação, o desenvolvimento tecnológico e a inovação.

Ao produzir uma solução com custo consideravelmente reduzido comparativamente aos produtos de mercado, permite mais fácil aquisição por pequenas empresas, auxiliando os indicadores para a melhoria do acesso às tecnologias da informação e da comunicação, bem como a sua utilização e qualidade.

Ao permitir o acesso a soluções de tecnologia de forma facilitada para empresas pequenas e médias, contribui diretamente para reforçar a competitividade das pequenas e médias empresas.

Neste contexto, a proposta de produto a ser desenvolvida em Portugal permite cumprir com os 3 objetivos primários previstos no Programa Portugal 2020 para a prioridade "Crescimento inteligente".

5.1.2. Crescimento inclusivo

A prioridade Crescimento Inclusivo (Estratégia Europa 2020, s.d.) possui 4 objetivos primários:

1. Promover o emprego e apoiar a mobilidade laboral;
2. Promover a inclusão social e combater a pobreza;
3. Investir no ensino, nas competências e na aprendizagem ao longo da vida;
4. Reforçar a capacidade institucional e uma administração pública eficiente.

A proposta de um produto competitivo inclui o desenvolvimento e produção em território nacional, desta forma insere-se ao abrigo do objetivo de promover emprego.

O desenvolvimento do produto ainda prevê a geração de emprego e qualificação de capital humano para o suporte das tecnologias, sendo assim, potencial fomentador e investidor para a formação de recursos humanos.

A tecnologia da informação é suporte para diversas atividades nos níveis privados e público. São mais que conhecidos e estudados os benefícios dos investimentos em tecnologias que permitem agilizar processos e muitas vezes automatizar de forma completa, permitindo a órgão públicos fornecerem serviço com mais qualidade à sociedade. Neste contexto, a solução técnica proposta neste trabalho permite aos organismos do estado implementarem sistemas de segurança com melhor proveito financeiro, reduzindo gastos públicos e reter o capital dos investimentos em território nacional, reduzindo a expatriação de euros para outras unidades da EU e mesmo fora dela, como nas aquisições de produtos dos EUA, que representam a maioria das propriedades tecnológicas na área da informática.

5.2. Conclusão – Parte IV

O desenvolvimento de um produto em território nacional beneficia toda uma cadeia produtiva com notável impacto social. Além destes benefícios, auxilia nos indicadores de sucesso das metas propostas para Portugal no âmbito da União Europeia, gera valor, retém capital e insere o país como desenvolvedor e produtor de tecnologia.

O desenvolvimento deste produto reforça os indicadores para os objetivos do Portugal 2020, por construir uma solução de segurança a um custo notavelmente reduzido, facilitando a sua inserção em cidades e zonas de baixa densidade e consequente menor volume financeiro seja de mercado ou investimentos públicos.

5.3. Limitações e trabalho futuro – Parte IV

Esta etapa do trabalho foi limitada à pesquisa bibliográfica no âmbito do Acordo de parceria 2014-2020. Não contemplou iniciativas de governo separadas do documento em questão.

Como trabalho futuro propõe-se o levantamento de fontes e recursos de investimento que beneficiem zonas regionais para a inserção do produto para cumprimento dos

objetivos estratégicos do Portugal 2020 com especial foco para a "Transferência de resultados do sistema científico para o tecido produtivo", visando a implementação de unidades de produção, suporte e manutenção de serviços de modo a difundir a tecnologia no país.

6. Conclusões

6.1. Considerações finais

Este trabalho foi desenvolvido no âmbito académico. Aspetos comerciais, parcerias de negócio e incentivos fiscais não foram considerados para a definição de custos.

No âmbito técnico a solução proposta atende a requisitos essenciais de segurança que permitem inseri-la no contexto empresarial privado ou público, com aspetos inovadores face a outras analisadas. A solução de firewall, composta pelo *pfSense* é um produto consolidado, com implementações e casos de uso já validados por empresas, incluindo infraestruturas críticas. O ModSecurity é padrão de facto para soluções de WAF, sendo apresentado no sítio da web www.owasp.org. A solução ModSecurity Core Rule Set é solução nativa do ModSecurity que contem um conjunto de regras que implementam o OWASP Top 10, usado por diversos fabricantes. A solução de DNS Firewall é uma implementação de políticas de resposta do BIND DNS, publicado pelo ISC – Internet Systems Consortium, com base em listas de reputação públicas.

O aspeto financeiro é fator marcante na solução do produto que afirma a característica competitiva do mesmo face a soluções de mercado. O custo de hardware apresenta-se semelhante. Contudo, o suporte, atualizações e custos advindos de renovações não são considerados, o que torna a solução proposta no trabalho apresentado nesta dissertação, financeiramente mais atraente e rentável quando comparada com qualquer outra analisada.

Em termos de mercado, Portugal apresenta potencial para a adoção de soluções abertas. Porém, há ainda poucos fornecedores e empresas que suportam softwares e sistemas de código livre. Ainda assim, há casos de sucesso como a Caixa Mágica (empresa portuguesa que desenvolveu uma distribuição Linux) que, desde o ano 2000 tem recebido subsequentes prémios pelo seu produto.

A inserção de um produto nacional nas tecnologias deve ser vista como estratégia para o mercado português, uma vez que os benefícios socioeconómicos são plenamente atingidos quando se retém capital ao produzir em território nacional, ativando a economia ao contratar mão de obra local para a produção e também incentiva o ensino ao fomentar a formação e qualificação de pessoal para o suporte tecnológico.

Todo este cenário consolida a criação de um produto competitivo de elevado valor para o mercado que suporta a segurança da informação e proteção de dados.

6.2. Limitações

Este trabalho foi limitado ao âmbito técnico dos sistemas propostos no capítulo 3 com ensaios práticos realizados em ambiente virtualizado. Isto limita os resultados técnicos à plataforma de virtualização, permitindo apresentar uma proposta de trabalho futuro detalhada na secção seguinte.

A componente financeira apresentada no capítulo 4 foi limitada aos produtos e parcerias listadas na parte III desta dissertação.

6.3. Trabalho futuro

Experiências em hardwares dedicados devem ser observados em complemento a este trabalho. As plataformas virtuais permitiram a validação das funções, mas limitaram o âmbito da capacidade de conexões simultâneas para os testes funcionais da componente de IDS/IPS.

As análises deste trabalho apontaram para a necessidade de estudos mais detalhados face a carência de capital humano que pode ser fator impeditivo para inserir a produção e implementação do produto final em zonas menos favorecidas, onde um trabalho prévio de qualificação profissional deve ser iniciado para suportar o todo o ciclo produtivo e manutenção dos sistemas. O estudo pode ainda ser potencializado com uma avaliação sobre a regionalização da produção e interiorização no espaço geográfico português, levando conhecimento, emprego e receita a zonas desfavorecidas, como fruto da criação do ambiente produtivo em regiões com incentivos para a mobilidade empresarial.

As iniciativas do Portugal 2020 podem ser uma forte alavanca para a criação de empresas com base nos produtos de código aberto e uma análise apurada dos cenários de investimento deve ser realizada em complemento a este trabalho.

Referências

Dwivedi, R., & Rahul, N. S. (2017). Evaluating Unified Threat Management Products for Enterprise Networks. *SURYA-THE ENERGY MANAGEMENT RESEARCH JOURNAL, 3*(4), 6-18.

Laureano, M. P., & Moraes, P. S. (2005). SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO. *Revista Economia & Tecnologia, 8*, 38-44.

Administração, F. E. (2018). Classificação de Informações e Dados Abertos. *Acesso à infromação*. Brasília, Brasil: Escola Nacional de Administração Pública.

Alencar, M. A. (2010). *Fundamentos de redes de computadores.* Manaus: CETAM.

Allen, J., Nori, H., Ohrimenko, O., Ding, B., Kulkarni, J., & Yekhanin, S. (2 de Julho de 2018). An Algorithmic Framework For Differentially Private Data Analysis on Trusted Processors. Cornell University Library.

Amaral, A. F. (2012). *Redes de Computadores.* Colatina: Instituto Federal do Espírito Santo.

Bungart, J. W. (2018). *Redes de computadores: Fundamentos e protocolos.* São Paulo, Brasil: SENAI-SP.

Chiranjeeva Rao, N., & Shankha De, C. (2017). Study of User Behaviour for Firewall Configuration. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 387-389.

Choi, Y. B., & Allison, G. D. (25 de 03 de 2017). Intrusion Prevention And Detection in Small to Medium-Sized Enterprises. *Association for Information Systems*. AIS Electronic Library (AISeL).

Cisco Systems. (7 de Junho de 2017). *Cisco ASA 5585-X Stateful Firewall Data Sheet.* Obtido em 18 de Março de 2018, de Cisco: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-730903.html

Comissão Européia, & República Portuguesa. (Julho de 2014). Acordo de parceria 2014-2020. Obtido de https://www.portugal2020.pt/Portal2020/Media/Default/docs/C_2014_5513_PT_ACTE_f.pdf

CounterFlow AI, I. (Agosto de 2018). *CounterFlow AI*. Obtido em 11 de Agosto de 2018, de CounterFlow AI: https://www.counterflow.ai/

Dietrich, N. (16 de 12 de 2015). *Snort 2.9.8.x on Ubuntu 12, 14, and 15 with Barnyard2, PulledPork, and Snorby.* Obtido de DSPACE: http://lib.hpu.edu.vn/bitstream/handle/123456789/21431/0024_Snort_2.9.8.x_on_Ubuntu_12_14_15.pdf

Dignan, L. (11 de 12 de 2018). *Top cloud providers 2018: How AWS, Microsoft, Google, IBM, Oracle, Alibaba stack up*. Obtido em 28 de 07 de 2018, de ZDNet:

https://www.zdnet.com/article/top-cloud-providers-2018-how-aws-microsoft-google-ibm-oracle-alibaba-stack-up/

Diniz, I. d., Costa, L. d., & Medeiros, M. M. (Abril de 2017). Utilização da computação em nuvem no poder legislativo: percepções dos gestores e entraves ao uso. *Revista Brasileira de Políticas Públicas*, pp. 255-275.

Ekaterina, D., & Otsetova, A. (2017). OPEN SOURCE RULES FOR REAL-TIME PROTECTION OF WEB SERVER. *International Journal of Advanced Research in IT and Engineering*, 13-21.

Estratégia Europa 2020. (s.d.). Obtido em 01 de Agosto de 2018, de Comissão Europeia: https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_pt

Filho, E. L. (2008). Arquitetura de alta disponibilidade para firewall e IPS baseada em SCTP. Uberlândia, Brasil: Universidade Federal de Uberlândia.

Flajolet, P., Fusy, É., Gandouet, O., & Meunier, F. (17 de Agosto de 2015). HyperLogLog: the analysis of a near-optimal cardinality estimation algorithm. *Conference on Analysis of Algorithms, AofA*, (pp. 137-156). França.

Fortinet. (7 de Junho de 2017). *Fortigate Datasheet.* Obtido em 16 de Janeiro de 2018, de Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_100D_Series.pdf

Galegale, N. V., Fontes, E. G., & Galegale, B. P. (2017). Uma contribuição para a segurança da informação: Um estudo de casos múltiplos com organizações brasileiras. *Perspectivas em Ciência da Informação*, (pp. 75-97).

Glenn, N. (2018). *Estados Unidos da América Patente Nº US 2018 / 0013792 A1.*

Gonçalves, F., & Santos, M. S. (27 de Abril de 2017). *Apresentações.* Obtido em 30 de Março de 2018, de Academia Militar: https://academiamilitar.pt/images/site_images/Eventos/3rd_Conference/Day_2/Cyber_Defence_Training_Enviroment_-_Francisco_Goncalves_Novabase_IMS-Axians.pdf

Hass, D. (Junho de 2017). INTELIGÊNCIA COMPETITIVA: ANÁLISE DA CONCORRÊNCIA PARA PRECIFICAÇÃO DE OPERAÇÕES DE CRÉDITO NO MERCADO FINANCEIRO. Lajeado, Brasil: CENTRO UNIVERSITÁRIO UNIVATES.

Herrera, A. V., Ron, M., & Rabadão, C. (2017). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI).* Lisbon.

ISC. (Janeiro de 2018). *DNS Firewall solution for BIND*. Obtido de ISC: https://www.isc.org/rpz/

IT Central Station. (2018). *Firewalls - Buyer's Guide and Reviews - March 2018.* New York: IT Cenrtral Station.

IT Central Station. (2018). *Web Application Security - Buyer's Guide and Reviews - March 2018.* New York: IT Central Station.

Khan, M. (2017). COMPUTER SECURITY IN THE HUMAN LIFE. *International Journal of Computer Science, 6, 1*, 35-42. Saudi Arabia.

Kumar, G., & Kumar, K. (2014). Network security – an updated perspective. *Systems Science & Control Engineering: An Open Access*, pp. 325-334.

Kumar, S. N. (2015). Review on Network Security and Cryptography. *International Transaction of Electrical and Computer Engineers System, 3*(1), 1-11. doi:10.12691/iteces-3-1-1

Mathew, I. A., & Prabhu, D. B. (2017). A STUDY ON VIRTUAL LOCAL AREA NETWORK (VLAN) AND INTER-VLAN ROUTING. *4*, 43-45. ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697.

Maurício, L. A., Alvarenga, I. D., Rubinstein, M. G., & Duarte, O. M. (2017). Uma Arquitetura de Virtualização de Funções de Rede para Proteção Automática e Eficiente contra Ataques. Sociedade Brasileira de Computação.

Miranda, V. V., Vieira, C. C., & Carelli, F. C. (Dezembro de 2008). O uso de Software Livre no Serviço Federal de Processamento de Dados. *Cadernos UniFOA*.

Mota, A. G., Nunes, J. P., Inácio, P. L., Barroso, C. D., Ferreira, M. A., & Oliveira, L. (2015). *Finanças nas empresas.* Lisboa: Edições Sílabo.

Nico, E., Funk, R., & Cappo, C. (2018). Anomaly-based Web Application Firewall using HTTP-specific features and One-Class SVM. *Universidad Nacional de Asunción*. Paraguay: Facultad Politecnica.

Ochôa, P., & Pinto, L. G. (2018). Transformação digital e competências digitais: estratégias de gestão e literacia. *Literacia, Media e Cidadania - Livro de Atas do 4.º Congresso.* Braga: Centro de Estudos de Comunicação e Sociedade (CECS).

OPNids. (Julho de 2018). *OPNids*. Obtido em 13 de Julho de 2018, de OPNids: https://www.opnids.io/

Paço, S. R., & Ramos, M. C. (2018). EMPREENDEDORISMO EM PORTUGAL DE IMIGRANTES DE PAÍSES FORA DA UNIÃO EUROPEIA. *Holos*, 365-385.

Park, W., & Ahn, S. (2017). Performance Comparison and Detection Analysis in Snort and Suricata Environment. *Wireless Pers Commun*, 241-252. New York, EUA: Springer Science+Business Media. doi:10.1007/s11277-016-3209-9

Petrushevski, S., Krstic, G., & Cabrera, H. (2013). *CloudFlare vs Incapsula vs ModSecurity - Comparative penetration testing analysis report v2.0.* Zero Science Lab. Obtido de https://www.zeroscience.mk/files/wafreport2013.pdf

PORDATA. (2018). *PORDATA*. Obtido de PORDATA: https://www.pordata.pt/

Prasad, D. R., & Rao, G. (2017). Combating Cross-Site Scripting Assaults without Proprietary Software. *International Journal of Applied Engineering Research*, 6788-6796.

Project Management Institute. (s.d.). *WhatIs Project Management*. Obtido em 09 de Agosto de 2018, de Project Management Institute: https://brasil.pmi.org/brazil/AboutUs/WhatIsProjectManagement.aspx

Ridha, M. A., & Memen Akbar, R. (2018). SQL Injection and Cross Site Scripting Prevention using OWASP ModSecurity Web Application Firewall. *JOIV - International Journal Of Informatics Visualization*, 286-292.

Sagar, D., Kukreja, S., Brahma, J., Tyagi, S., & Jain, P. (2018). STUDYING OPEN SOURCE VULNERABILITY SCANNERS FOR VULNERABILITIES IN WEB APPLICATIONS. *IIOAB Journal*, 43-49.

Santos, M. A. (2018). *CONTABILIDADE DE CUSTOS.* Salvador: UFBA, Faculdade de Ciências Contábeis; Superintendência de Educação a Distância.

Santos, M. S. (26 de Abril de 2016). *Apresentações.* Obtido em 30 de Março de 2018, de Academia Militar: https://academiamilitar.pt/images/CDSDP2016/Apresentacoes/3.Parallel-Session_Marcio-Silva-Santos.pdf

Sengupta, S., & Gupta, N. (18 de April de 2017). FIREWALL FOR INTERNET OF THINGS. New Delhi, India: Indraprastha Institute of Information Technology.

Setzer, V. W. (2014). *Os Meios Eletrônicos e a Educação: Uma Visão alternativa.* São Paulo: Escrituras.

Sharma, R., & Parekh, C. (May-June de 2017). Firewalls: A Study and Its Classification. *International Journal of Advanced Research in Computer Science, 8*, 1979-1984. IJARCS.

Snorby. (2018). *Snorby*. Obtido de Github: https://github.com/Snorby/snorby

Sophos. (Janeiro de 2018). *Sophos UTM Feature List.* Obtido de Sophos: https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-utm-feature-list-dsna.ashx

Strutzel, T. (2015). *Presença Digital - Estratégias Eficazes para Posicionar sua Marca Pessoal ou Corporativa.* Rio de Janeiro: Alta Books.

Szewczyk, P., & Macdonald, R. (12 de 2017). Broadband Router Security: History, Challenges and Future Implications. *Journal of Digital Forensics, Security and Law, 12(4)*. Journal of Digital Forensics, Security and Law. doi:https://doi.org/10.15394/jdfsl.2017.1444

Tensorflow. (setembro de 2018). Obtido em 12 de Julho de 2018, de Tensorflow: https://www.tensorflow.org/

Yadav, P. B. (23 de Abril de 2014). Web Application Vulnerabilities. *Helsinki Metropolia University of Applied Sciences*. Helsinki, Finlândia.

ANEXO I – Script de criação da lista pfBlockerNG

```
#!/bin/sh
# redlist.sh
# Script de criação da lista de endereços

# Download das listas públicas
mkdir /usr/src/lista
cd /usr/src/lista

# CISCO TALOS
wget https://www.talosintelligence.com/documents/ip-blacklist

# EMERGINTHREADS
wget https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
wget https://rules.emergingthreats.net/blockrules/compromised-ips.txt

# BINARY DEFENSE
wget https://www.binarydefense.com/banlist.txt

# Criar merge temporário e ordenar crescente
cat emerging-Block-IPs.txt compromised-ips.txt banlist.txt ip-blacklist | sort > listtemp.txt

# Apagar linhas vazias
sudo sed -i '/^$/d' listtemp.txt

# Apagar linhas iniciadas por #
sudo sed -i '/#/d' listtemp.txt

# Eliminar linhas duplicadas
sort listtemp.txt | uniq > list.txt

# Copiar arquivo temporário para o servidor web e apagar temporários
mv list.txt /var/www/list.txt
rm *
```

ANEXO II – Modelo do ficheiro de Endereços IP comprometidos

```
####################################
#                                  #
#   Wed Feb  7 15:42:32 WET 2018   #
#                                  #
####################################
####################################
#                                  #
#     Redstout Threat IP list      #
#                                  #
#          redstout.com            #
#                                  #
#    This feed is free for use     #
#                                  #
####################################
####################################
101.100.137.199
101.109.140.169
101.109.97.253
101.140.56.70
101.15.35.62
101.187.28.8
101.192.0.0/14
101.200.81.187
101.202.0.0/16
101.203.128.0/19
101.228.30.30
101.231.189.62
101.231.211.131
101.231.245.166
101.231.34.100
101.231.60.122
101.236.59.24
101.236.62.2
101.24.124.221
101.248.0.0/15
101.248.146.204
101.251.197.238
101.251.72.148
101.252.0.0/15
101.254.149.223
101.254.150.144
101.254.150.236
101.254.150.46
101.255.66.147
101.25.67.46
101.36.81.98
101.51.29.54
101.52.131.65
101.66.0.23
101.68.67.178
101.69.248.38
101.71.29.235
101.78.196.27
101.81.194.157
101.81.29.12
101.88.233.111
101.89.136.208
```

ANEXO III - modsec-clamscan.lua

```
#!/usr/bin/lua
--[[
  This script can be used to inspect uploaded files for viruses
  via ClamAV. To implement, use with the following ModSecurity rule:
  SecRule FILES_TMPNAMES "@inspectFile /opt/modsecurity/bin/modsec-
clamscan.lua" "phase:2,t:none,log,deny"
  Author: Angelo Conforti (based on Josh Amishav-Zlatin code)
  Requires the clamav-server and clamav-scanner

  If you use SELinux on RHEL base distro:
  setsebool -P antivirus_can_scan_system 1

  And remember that CentOS ClamAV distribution has some issue
  with permission in the "default" configuration. Use Debian and
  you'll be happy :)
  This program is free software: you can redistribute it and/or modify
  it under the terms of the GNU General Public License as published by
  the Free Software Foundation, either version 3 of the License, or
  (at your option) any later version.
  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
  GNU General Public License for more details.
  You should have received a copy of the GNU General Public License
  along with this program.  If not, see <http://www.gnu.org/licenses/>.
]]--


function fsize(filename)
  file = io.open(filename,"r")
  local current = file:seek()
  local size = file:seek("end")
  file:seek("set",current)
  file:close()
  return size
end

function main(filename)
  -- Configure paths
  local clamdscan  = "/usr/bin/clamdscan"
  local clamscan  = "/usr/bin/clamscan"

  -- failoverOnClamdFailure: failover to clamscan if clamdscan report an error
  local failoverOnClamdFailure = true

  -- fail (and block) if clamdscan (and clamscan) fails
  local failOnError = false
```

```
  -- local var
  local agent = "clamdscan"

  -- Skip empty items because if clamd is not working and you
  -- use the clamscan agent an empty file can take about 12 secs
  -- to be analyzed
  if fsize(filename) == 0 then
    m.log(1, "[scanav skipped, file " .. filename .." size is zero]")
    return nil
  end

  -- The system command we want to call with fdpass flag to
  -- do not incur in a permission issue
  local cmd = clamdscan .. " --fdpass --stdout --no-summary"

  -- Run the command and get the output
  local f = io.popen(cmd .. " " .. filename .. " || true")
  local l = f:read("*a")
  f:close()

  -- Check the output for the FOUND or ERROR strings which indicate
  -- an issue we want to block access on
  local isVuln = string.find(l, "FOUND")
  local isError = string.find(l, "ERROR")

  -- If clamdscan fails and you want failover to the traditional clamscan...
  if isError and failoverOnClamdFailure then
    -- Try to use the clamscan program
    m.log(1, "[clamdscan fails (" .. l .. "), failover to clamscan]")
    agent = "clamscan"
    cmd = clamscan .. " --stdout --no-summary"
    f = io.popen(cmd .. " " .. filename .. " || true")
    l = f:read("*a")
    f:close()
    isVuln = string.find(l, "FOUND")
    isError = string.find(l, "ERROR")
  end

  if isVuln then
    m.log(1, "[" .. agent .. " scanner message: " .. l .. "]")
    return "Virus Detected"
  elseif isError and failOnError then
    -- is a error (not a virus) a failure event?
    m.log(1, "[" .. agent .. " scanner message: " .. l .. "]")
    return "Error Detected"
  else
    return nil
  end
end
```

ANEXO IV – XG-1537 1U – Technical specifications

CPU	Intel "Xeon-DE" D-1537, 1.7 GHz FCBGA 1667 supported SoC
CPU Cores	8
Memory Options	8GB DDR4 UDIMM
Storage Options	256GB M.2 SSD 2x 150GB 2.5" SSD RAID 1
Network Interfaces	Dual LAN via Intel® i350-AM2 1 Gigabit Ethernet Dual LAN via SoC 10GbE SFP+ Virtual Machine Device Queues reduce I/O overhead Supports 10GbE (SFP+), 100BASE-TX, and 1000BASE-T (RJ45) 1x Realtek RTL8201N PHY (dedicated IPMI)
Network Expansion Options	4-Port Intel GbE 2-port Chelsio SFP+ Expansion
USB Ports	2x 3.0 ports
Console Port	VGA
Max Active Connections	8 Million
Power	200W Internal Power Supply, 100~240V, 50-60Hz, 2.6 Amp Max
Case	Standard 19" 1U rack mount
Dimensions	17.2" (437mm) x 1.7" (43mm) x 9.85" (250mm)
Cooling	Active
Operating Temperature	0°C to 60°C (32°F to 140°F)
Hardware Warranty	12 months
Certifications	CE Emission, FCC, RoHS, UL
Power Consumption	20W (idle)
Support Options	Professional, Enterprise, and Enterprise Plus