FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Caio Loredo

IMPACTOS ECONÔMICOS DE *CLUSTER* DE ALTA DISPONIBILIDADE EM REDES CORPORATIVAS

Americana, SP
2024

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Caio Loredo

IMPACTOS ECONÔMICOS DE *CLUSTER* DE ALTA DISPONIBILIDADE EM REDES CORPORATIVAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Especialista Marcus Vinicius Lahr Giraldi

Área de concentração: Tecnologia em Segurança da Informação

Americana, SP

2024

LOREDO, Caio

Impactos econômicos de cluster de alta disponibilidade em redes corporativas. / Caio LOREDO – Americana, 2024.

38f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinicius Lahr Giraldi

1. Intranet – rede de computadores 2. Segurança em sistemas de informação. I. LOREDO, Caio II. GIRALDI, Marcus Vinicius Lahr III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.519Intranet
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Caio Loredo

Impactos Econômicos de Cluster de Alta Disponibilidade em Redes Coorporativas

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação.

Americana, 2 de dezembro de 2024.

Banca Examinadora:

Marcus Vinicius Lahr Giraldi
Especialista
Fatec Americana "Ministro Ralph Biasi"

João Emmanuel D'Alkmin Neves
Doutor
Fatec Americana "Ministro Ralph Biasi"

Benedito Aparecido Cruz
Mestre
Fatec Americana "Ministro Ralph Biasi"

RESUMO

A utilização de um *cluster pfSense*, configurado como *firewall* de borda, em redes corporativas pode ter impactos significativos a economia e a confiabilidade das operações empresariais. O tempo é um recurso valioso, e com a crescente dependência da internet nas operações empresariais, a falta de uma infraestrutura de rede redundante e confiável pode ocasionar várias interrupções nos serviços, gerando prejuízos consideráveis. Este estudo caracteriza-se como uma pesquisa experimental, na qual são analisados e simulados períodos de inatividade em redes corporativas utilizando o *pfSense* como *firewall* de borda, onde os cenários com e sem a implementação de *clusters* são comparados. A análise abrange problemas lógicos, físicos e manutenções programadas. A metodologia inclui análises de estudos de caso e testes práticos conduzidos em um ambiente virtual controlado. A coleta de dados é qualitativa, com o tempo de inatividade como principal indicador. Este documento busca demonstrar a importância da alta disponibilidade em redes corporativas, apresentando configurações que permitem tornar a rede confiável e disponível com o uso de ferramentas de código aberto, como o *pfSense*, transformando a infraestrutura de rede mais compatível com as exigências do mercado profissional atual.

Palavras-chave: *pfSense*, *Cluster*, Alta Disponibilidade

ABSTRACT

The use of a pfSense cluster, configured as an border firewall in corporate networks, can significantly impact the economy and the reliability of business operations. Time is a valuable resource, and with the increasing dependence on the internet in business operations, the lack of a redundant and reliable network infrastructure can cause various service interruptions, resulting in considerable losses. This study is characterized as experimental research, in which periods of downtime in corporate networks using pfSense as a border firewall are analyzed and simulated, comparing scenarios with and without the implementation of clusters. The analysis covers logical, physical problems, and scheduled maintenance. The methodology includes case study analyses and practical tests conducted in a controlled virtual environment. The data collection is qualitative, with downtime as the main indicator. This document aims to demonstrate the importance of high availability in corporate networks, presenting configurations that make the network reliable and available using open-source tools like pfSense, making the network infrastructure more compatible with the current professional market demands.

Keywords: *pfSense, Cluster, Edge Firewall*

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

A evolução tecnológica tem levado as empresas a as suas operações na internet, aumentando a dependência da conectividade e disponibilidade para a execução de suas atividades básicas diárias. Consequentemente, há uma demanda por uma infraestrutura de rede eficiente, junto com uma equipe profissional e equipamentos especializados para diminuir ao máximo o tempo de inatividade, mantendo sempre seus serviços ativos e reduzindo os prejuízos que podem ocorrer com esta nova era tecnológica.

Embora existam diversas formas de garantir a disponibilidade contínua de uma rede, muitas dessas soluções apresentadas no mercado implicam custos altamente significativos. Isso pode fazer com que a gestão de uma empresa hesite em implementar uma rede redundante, deixando a empresa vulnerável a períodos de inatividade.

Atualmente, a grande maioria das redes que possuem um nível mínimo de segurança conta com um equipamento centralizador e gerenciador, como um *firewall*. Esse dispositivo, além de garantir a segurança por meio de análises e bloqueios de tráfego, também é crucial para a conexão interna da rede corporativa. Embora os *firewalls* sejam projetados para estar sempre online, nenhum equipamento é infalível, e falhas inevitavelmente ocorrerão. Nessas situações, quanto tempo de inatividade a empresa pode suportar antes de começar a sofrer prejuízos significativos?

Considerando este contexto, o objetivo deste trabalho é analisar os impactos econômicos da implementação de um *cluster* com o *pfSense* atuando como *firewall* de borda em uma rede corporativa. Serão apresentadas as configurações e o funcionamento do *cluster*, conhecido como HA (*High Availability*) no *pfSense*, além da análise do tempo de inatividade com e sem o *cluster*, incluindo cálculos que demostrem os prejuízos de inatividade de uma empresa.

Destaca-se a alta disponibilidade do *pfSense*, que, mesmo sendo uma ferramenta *open-source*, permite a criação de uma infraestrutura redundante e confiável, profissionalizando a rede, permitindo a sua integração em qualquer rede corporativa ser completamente viável e eficiente.

Este estudo pretende servir como uma fonte de informação para a comunidade acadêmica, abordando sobre um tema relevante e de alta demanda no mercado de

trabalho atual. Além de detalhar as configurações e análises do impacto do *cluster* com o *pfSense*, espera-se também apoiar a comunidade tecnológica em geral, mostrando melhorias de uma infraestrutura já existente, aumentando mais sua confiabilidade e disponibilidade.

A hipótese deste estudo é que a implementação de um *cluster* com o *pfSense* atuando como *firewall* de borda, resultará em uma redução significativa do tempo de inatividade, consequentemente diminuindo os prejuízos financeiros para a empresa, proporcionando uma infraestrutura de rede mais robusta e confiável.

Este trabalho caracteriza-se como uma pesquisa exploratória, na qual serão analisados e simulados períodos de inatividade em redes corporativas, decorrentes de problemas lógicos, físicos e possíveis manutenções na rede que causam interrupções. Os dados serão coletados de forma qualitativa, com o principal indicador sendo o tempo de inatividade das empresas.

1 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem como objetivo apresentar os principais conceitos e termos que sustentam o trabalho realizado, permitindo uma compreensão mais clara do estudo, consolidando o conhecimento prévio disponível e servindo como base para o desenvolvimento do trabalho, além de possibilitar a contextualização do tema dentro da área de estudo.

1.1 *Firewall*

Firewall é um conceito de sistema ativo que contribui para a segurança de redes, ao gerenciar e analisar o tráfego de dados, realizando liberações e/ou bloqueios conforme regras previamente definidas. Geralmente, é implementado em equipamentos estrategicamente posicionados na infraestrutura de rede, com a finalidade de centralizar e controlar o fluxo de comunicações entre redes internas e externas. Sua importância é fundamental nas redes corporativas, onde a integridade e a confidencialidade dos dados são essenciais. Além de suas funções primárias, o *firewall* também auxilia na coleta de informações, facilitando análises e manutenções na infraestrutura corporativa (Gomes, 2023).

Pode-se distinguir dois tipos principais de *firewalls*: o *Stateful* (com estado) e o *Stateless* (sem estado). Essa diferenciação diz respeito à maneira como esses *firewalls* abordam a filtragem do tráfego de dados em uma rede.

O *firewall Stateful* é uma forma avançada de *firewall* que opera com uma tabela de estados, na qual são armazenados dados de conexões previamente estabelecidas. Essa abordagem permite que o *firewall* filtre o tráfego com base nessas informações, reduzindo a necessidade de regras adicionais e proporcionando maior desempenho e segurança a cada requisição. Já o *firewall Stateless* é mais simples em seu funcionamento, tratando cada pacote de dados de forma independente, sem manter registros das conexões estabelecidas. Isso resulta em uma filtragem de tráfego que não leva em consideração as circunstâncias específicas da infraestrutura local (Ostec, 2020).

1.2 pfSense

pfSense é um sistema operacional de código aberto desenvolvido para ser um *firewall* e/ou roteador, criado com base no FreeBSD, que é uma distribuição do *Unix*. Ele permite gerência completa via interface web ou através de linhas de comando pelo terminal *Shell*. (Netgate, 2024).

Devido à sua flexibilidade e interface web intuitiva, o projeto, iniciado em 2004 e atualmente na versão 2.7.2, alcançou um grande número de usuários, formando uma comunidade ativa e colaborativa desde o princípio. Além de oferecer diversos serviços nativos, como regras de *firewall*, servidor DHCP, *OpenVPN*, regras de *NAT*, *failover* e *load balancing*, o *pfSense* possui uma vasta biblioteca de pacotes adicionais oficiais, como *PfBlocker, Squid, SquidGuard, Snort*, entre outros. Esses pacotes aumentam sua versatilidade e potência como um gerenciador de rede (Almeida, 2017).

Devido às suas características e aos serviços disponíveis, somados ao fato de ser uma ferramenta de código aberto, o *pfSense* é amplamente utilizado em redes corporativas de pequenas e médias empresas. Ele pode ser implementado de várias formas, como hospedado em uma máquina virtual, instalado através de uma imagem ISO em uma máquina local ou, em seu uso mais profissional, como um *appliance* (hardware próprio + software), segundo (Severino; Araújo, 2017).

1.3 Alta Disponibilidade

Alta Disponibilidade, também conhecida como HA (*High Availability*), o termo disponibilidade é descrito como o tempo em que um serviço está disponível, utilizável e funcional para realizar suas funções, já a alta disponibilidade é uma qualidade que garante que o serviço esteja quase sempre ativo e apto para quando for requisitado, segundo (Severino; Araújo, 2017 *apud* Heide, 2016). Para um sistema ser considerado de Alta Disponibilidade, é necessário ter configurações especializadas para recuperação e mitigação de falhas, além das disponibilidades comuns oferecidas de fábrica (Reis *et al.,* s.d.) A disponibilidade de um serviço pode ser calculada de maneira simples usando uma fórmula matemática: a Disponibilidade é igual ao tempo total em que o serviço esteve disponível dividido pelo tempo (Ferreira; Santos; Antunes, 2005).

Hoje em dia, com a crescente dependência da internet, muitos serviços demonstram o uso da Alta Disponibilidade, como *Data Centers*, sites, bancos e sistemas críticos como o de saúde, que devem estar acessíveis em qualquer momento (Reis *et al*., s.d.). É possível configurar um sistema de várias formas para obter esta qualidade, como através de redundâncias de equipamentos conhecidas como *clusters*. Quando o equipamento primário enfrenta um problema e fica inativo, o equipamento secundário em perfeito estado assume seu lugar de forma automática, mantendo o serviço ativo. Em geral, essas ferramentas que lidam com falhas e incidentes são simples de configurar para implementar a HA no serviço (Severino; Araújo, 2017).

1.4 *Cluster*

Um *cluster* é definido como uma redundância de dois ou mais computadores ou softwares autônomos, também conhecidos como nós ou nódulos, que trabalham em conjunto para realizar os mesmos processos e serviços. Para o usuário final, essa estrutura parece ser uma única máquina em funcionamento, não percebendo a redundância. Os *clusters* podem operar de duas maneiras, simultânea, onde ambos dividem a carga do serviço, também conhecido como Balanceamento de carga (*Load Balancing*), ou não simultânea, onde um permanece ativo e o outro de forma passiva, pronto para assumir em caso de falha do primário ativo, esta última característica é conhecida como ativo-passivo, ou *cluster* de Alta Disponibilidade (Vieira, 2022).

Os *clusters* são de extrema importância atualmente, pois todos os tipos de sistemas e aplicações buscam estar sempre disponíveis. Eles são amplamente utilizados em serviços críticos onde a Alta Disponibilidade é um requisito necessário (Reis *et al*., s.d.).

O *pfSense* utiliza os protocolos *pfsync* e *CARP* para configurar *clusters* de Alta Disponibilidade. Esses protocolos não só permitem que o servidor secundário se torne o primário em caso de falha, mas também facilitam a replicação de configurações, tornando a rede mais redundante e automática, sem a necessidade de intervenção manual, precisando fazer um retrabalho replicando configurações do *firewall* principal para o secundário (Vieira; Viana, 2020)

2 METODOLOGIA

Este capítulo descreve os métodos, procedimentos e abordagens utilizados para a realização da pesquisa, permitindo compreender o cenário utilizado nos testes experimentais. Além disso, busca proporcionar transparência ao decorrer do experimento, garantindo a validade e a confiabilidade dos resultados obtidos por meio de métodos já consolidados e amplamente utilizados.

2.1 Caracterização de Pesquisa.

Este estudo caracteriza-se como experimental, um método que permite a realização de testes controlados para identificar o melhor resultado. Segundo Button (2012), a pesquisa experimental possui a vantagem de permitir conclusões baseadas em resultados qualitativos, determinando a importância de cada variável. A principal variável analisada neste estudo é o tempo de inatividade, selecionado por sua importância nas operações empresariais. A inatividade da rede indica interrupções na produção, sendo assim, resultando em prejuízos financeiros.

2.1.1 Quanto ao delineamento

A pesquisa foi delineada como um estudo de caso, método que, de acordo com Ventura (2007), permite um entendimento se aprofundando em cenários específicos. Este delineamento é adequado para a coleta e análise de dados qualitativos. O estudo de caso é ideal para este trabalho, pois permite simular cenários virtuais controlados, de uma infraestrutura de rede, e identificar os impactos positivos e negativos da implementação de um *cluster* no *pfSense* como *firewall* de borda.

2.2 Caracterização do lugar e da amostra de pesquisa.

Os testes serão realizados em cenários virtuais utilizando o software gratuito *VirtualBox*. Esta escolha permite a simulação de uma infraestrutura de rede sem a necessidade de dispositivos físicos, proporcionando grande flexibilidade e controle sobre todas as operações, além de que, permite a obtenção de resultados válidos

para implantações reais, sem comprometer a continuidade de operações em cenários empresariais reais.

2.3 Procedimentos para coleta e análise de dados.

Os procedimentos para coleta e análise de dados serão baseados em dois cenários: um com um único *firewall pfSense* como *firewall* de borda e outro com dois *firewalls pfSense* configurados em um *cluster* passivo-ativo. Serão realizadas simulações de problemas que podem ocorrer no cotidiano, como manutenções programadas, problemas de sistema operacional e falhas de hardware.

Nas manutenções programadas, serão realizadas atualizações de software, que exigem reinicializações. Problemas físicos de sistema operacional, como corrupção do sistema operacional, podem necessitar a formatação e reinstalação do *firewall*, além da restauração de backups, se disponíveis. Falhas de hardware, como defeitos em discos, memória RAM ou fontes de alimentação, também serão simuladas, deixando o servidor ocioso até a substituição das peças defeituosas.

Ambos os cenários serão monitorados para medir o tempo de inatividade da rede. Além disso, a produção de dados das empresas será simulada para calcular o impacto econômico da inatividade, associando a quantidade de dados não processados durante os períodos de inatividade, resultando em perda de produtividade e custos associados

2.3.1 Ambiente de coleta de dados

Os dados serão coletados em um laboratório de pesquisa experimental. Neste ambiente, testes controlados permitem manusear variáveis e avaliar sua importância no resultado final. As pesquisas são divididas em dois grupos com cenários semelhantes, onde um grupo permanece igual e o outro passa por alterações, para no final fazer comparações detalhadas, (Fontenelle, s.d). Neste estudo, o ambiente será um laboratório virtual com dois cenários parecidos, diferenciados pela implantação do *cluster* no *pfSense*, onde será coletado e comparado o tempo de inatividade entre ambos.

2.3.2 Técnicas para coleta de dados

Neste estudo, utilizaremos três técnicas de coleta de dados: anotações relevantes, observações registradas e coletas de dados digitais. Essas técnicas foram escolhidas com base no contexto do ambiente de laboratório. Sendo a primeira, a observações registradas, um método tradicional e essencial de coleta de dados, exigem que o pesquisador se aprofunde no cenário de testes, observando e registrando os eventos de forma imediata para análises futuras (Sant Ana; Lemos, 2020). Isso nos permite anotar variáveis mais importantes e significativas para nosso teste, sendo as anotações relevantes, uma outra metodologia chave deste estudo. Além disso, utilizaremos ferramentas digitais para medir nossa principal variável, o tempo de inatividade, realizando testes com *Ping, Traceroute, Tcpdump* e analisando logs fornecidos pelo próprio *pfSense*.

2.3.3 Natureza da análise de dados

Na presente monografia, a natureza da análise de dados será qualitativa. Conforme Gibbs (2009), a análise qualitativa dá a liberdade ao pesquisador tornar-se uma parte crucial do processo de análise, permitindo explorar profundamente o cenário específico e oferecer uma visão pessoal do contexto. A opinião pessoal do pesquisador é fundamental para os resultados dos experimentos, contando que, o pesquisador pode vivenciar tanto a experiência do usuário quanto a do gestor que enfrenta a inatividade da rede sem o *cluster*, comparando com a experiência em um cenário com o *cluster*. Este método permite uma análise mais detalhada e contextualizada dos impactos e dinâmicas envolvidas

3 PROTOCOLOS UTILIZADOS NO HIGH AVALIABILITY

O **pfSense** é um dos poucos softwares gratuitos que disponibilizam a função de alta disponibilidade de forma nativa e confiável. Essa funcionalidade é crucial para garantir a continuidade dos serviços de rede, minimizando interrupções e assegurando que os recursos estejam sempre acessíveis. A configuração é realizada de maneira simples e rápida por meio de sua interface web intuitiva, o que facilita a implantação e o gerenciamento mesmo para administradores com pouca experiência. A ferramenta de alta disponibilidade utiliza três protocolos como base para o seu funcionamento: **CARP**, **XMLRPC** e **pfsync.**

3.1.1 Protocolo XMLRPC

O protocolo XMLRPC é utilizado para manter as configurações do *firewall* sincronizadas com o outro nó do *cluster*. Em outras palavras, ele replica os parâmetros do *firewall* principal (mestre) para o *firewall* secundário (*backup*).

É importante ressaltar que nem todas as configurações são replicadas; por exemplo, as configurações das interfaces não são sincronizadas. Para o funcionamento correto do XMLRPC, alguns pontos devem ser observados. Primeiramente, as interfaces de rede devem ser configuradas de maneira idêntica nos dois nós do *cluster*. Recomenda-se que as interfaces sejam do mesmo tipo e modelo, evitando misturar diferentes tipos de hardware. Isso é essencial para evitar problemas em serviços como DHCP ou até mesmo em regras de *firewall*, que podem não funcionar corretamente se houver discrepâncias nas interfaces de rede.

Outro requisito essencial é que a sincronização seja realizada por meio de um usuário com privilégios de administrador. Além disso, a porta do gerenciador *web* deve ser a mesma em ambos os dispositivos pfSense para garantir o funcionamento adequado.

3.1.2 Protocolo CARP

O protocolo CARP (*Common Address Redundancy Protocol*), ou Protocolo Comum de Redundância de Endereço em português, é um protocolo de redundância desenvolvido pelo projeto OpenBSD. Embora existam outros protocolos com soluções semelhantes, o CARP foi criado para evitar problemas de patentes com a Cisco, que já está em disputa sobre seu protocolo nativo HSRP *(Hot Standby Router Protocol*) com o VRRP (*Virtual Router Redundancy Protocol*) (Netgate, 2021).

O CARP é utilizado na configuração de *clusters* de alta disponibilidade do pfSense, atuando como intermediário entre dois *firewalls* através de um VIP (Virtual IP). O *firewall* primário envia um sinal *multicast* indicando seu funcionamento normal. O *firewall* secundário (*backup*) permanece inativo enquanto o principal opera normalmente. Quando o *firewall* principal para de enviar este sinal, o secundário assume o papel de primário, tornando-se o *gateway* principal da rede. Isso garante que o usuário final não perceba nenhuma alteração na disponibilidade, nem mesmo a queda do *firewall* principal (Flores; Trentin; Teixeira, 2019).

O CARP tem requisitos e limitações específicos. Sua configuração requer no mínimo três endereços IP: um para cada *firewall* e um terceiro para o IP virtual do CARP. Podem ocorrer conflitos com outros protocolos de redundância, como VRRP e HSRP. Por usar comunicação *multicast*, é crucial verificar se os switches intermediários não interferem na propagação desses pacotes. A *Netgate* adverte contra o acesso à interface web de gerenciamento do pfSense através do IP virtual do CARP, pois isso pode resultar na aplicação de configurações no dispositivo errado (Netgate, 2021).

3.1.3 Protocolo pfSync

E por fim, o protocolo pfsync opera com sincronização de maneira semelhante ao XMLRPC; entretanto, a diferença fundamental é que o pfsync sincroniza os estados das conexões entre os dois nós do *cluster*, em vez das configurações de *firewall*. Como o *firewall* secundário tem conhecimento das conexões por meio do pfsync, quando o nó principal fica fora do ar, o secundário mantém as conexões ativas, de modo que o usuário final não percebe a troca efetuada pelo *cluster*.

O funcionamento do pfsync ocorre através de multicast na rede, enviando os estados das conexões utilizando o protocolo **pfsync**. Ao chegar na interface de sincronização do outro dispositivo **pfSense**, eles estabelecem comunicação para importar esses estados. Também é possível configurar um endereço IP de destino para forçar o uso de *unicast* para o endereço correto, evitando assim o tráfego de multicast na rede. É necessário assegurar que não haja nenhum bloqueio por regras de *firewall*, para que o **pfsync** funcione corretamente. É ideal que as interfaces sejam idênticas nos dois nós do *cluster*, para evitar problemas de sincronização e garantir que a alta disponibilidade opere de forma adequada. (Netgate, 2021).

4 Prejuízo por *Downtime*

Downtime, ou tempo de inatividade, é um termo utilizado para referenciar o período em que uma rede ou sistema fica inoperante, infringindo um dos pilares da segurança da informação: a disponibilidade. Quanto maior o tempo de inatividade, mais significativos são os danos causados à empresa, resultando em custos associados ao *downtime*. Esses custos podem variar desde a interrupção da continuidade da produção, prejuízos à imagem da organização transmitindo ao mercado a percepção de incapacidade de atender às demandas até penalidades legais ou indenizações, caso haja obrigações legais de manter altos níveis de disponibilidade (Ferrigolo, 2020)

4.1 Tempo de inatividade médio nas empresas

Segundo uma pesquisa realizada pela Acronis, empresa renomada no mercado de cibersegurança, o tempo de inatividade das empresas está aumentando. Em 2021, 60,8% das empresas sofreram com inatividade, e no ano seguinte, 2022, esse percentual aumentou para 76%, representando um aumento de 25% em relação ao ano anterior (Acronis, 2022).

Pesquisas indicam que o tempo de inatividade de uma empresa pode chegar a cerca de 80 horas ao final do ano, somando todas as interrupções de minutos ou horas

que ocorrem ao longo desse período. A Gartner, empresa de consultoria e pesquisa, revelou que grandes corporações podem alcançar até 87 horas de inatividade por ano (Zdnet, 2014). Em outra pesquisa relacionada ao tema, a Dun & Bradstreet indica que, entre as empresas da Fortune 500, 59% sofrem no mínimo 1,6 horas de inatividade por mês, totalizando anualmente até 83,2 horas (Evolven, 2021)

4.2 Como calcular o *Downtime*

O cálculo do custo de *downtime* não possui uma fórmula precisa e concreta, pois envolve fatores intangíveis, como danos à imagem da empresa e insatisfação dos funcionários que sofrem com interrupções de processos devido a falhas. No entanto, é possível estimar de forma simplificada a receita perdida durante o tempo de inatividade. Para isso, obtém-se a receita anual da empresa e divide-se por 52 semanas, número de semanas que compõem um ano, obtendo-se a receita média semanal. Em seguida, para determinar a receita por hora, divide-se a receita semanal por 40, que corresponde ao número típico de horas de trabalho em uma semana (8 horas diárias em 5 dias úteis).

Exemplo:

- R$15 milhões de receita anual / 52 semanas = R$288.461,54 de receita média semanal
- R$288.461,54 / 40 horas por semana = R$7.211,54 de receita média por hora

Conforme o exemplo acima, a empresa perderia aproximadamente R$7.211,54 em receita para cada hora de inatividade. Esse cálculo fornece uma estimativa básica do impacto financeiro direto, embora não contabilize os custos indiretos e intangíveis associados ao *downtime* (Encomputers, 2024).

5 Cenário de teste

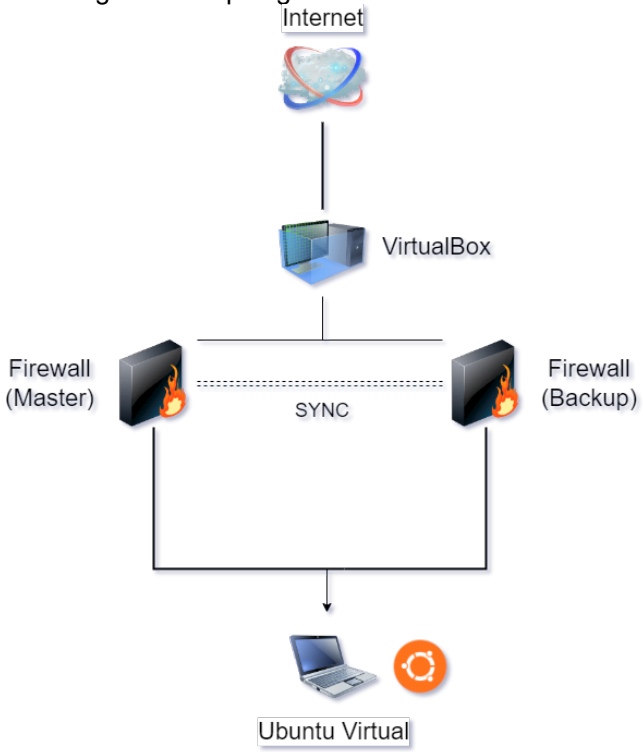
Neste tópico, será descrito, com detalhes, o ambiente utilizado, incluindo informações técnicas e relevantes. O cenário de teste foi planejado para simular condições reais, de modo a permitir uma análise detalhada e confiável dos resultados obtidos, além de possibilitar a comparação entre os dois cenários avaliados no teste realizado.

5.1 Descrição do cenário

No presente teste, serão realizadas comparações entre dois cenários distintos: um que utiliza a Alta Disponibilidade do pfSense e outro que não utiliza. Em ambos os cenários, será utilizada uma máquina virtual com o sistema operacional Ubuntu, na qual simularemos o comportamento do usuário final. Serão também utilizadas ferramentas, como o ping, para medir o tempo de inatividade.

Para a realização dos testes, foi utilizada a ferramenta *open source* VirtualBox, permitindo a virtualização dos laboratórios de teste, conforme a figura 1 descreve a topologia do ambiente.

Figura 1 - Topologia do ambiente de testes



Fonte: elaborado pelo autor.

5.2 Descrição técnica

5.2.1 Faixa de Rede

A faixa de rede dos *firewalls* foi definida da seguinte forma: Faixa de Rede**:** 192.168.0.0/24

5.2.2 *Firewall* 1

O *Firewall* 1 está configurado com duas interfaces de rede:

- **Placa de Rede 1 (em0):** Modo bridge (WAN) Endereço IP: Desativada **Placa de Rede 2 (em1):** Modo bridge (LAN)
- **Endereço IP:** 192.168.0.250
- **Placa de Rede 3 (em2):** Modo rede interna (intnet) (OPT_1)
- **Endereço IP:** 192.168.50.254 (Servidor DHCP ativo)
- **Versão do pfSense:** 2.7.2 (versão mais recente até o momento da documentação)
- **IP Virtual CARP (LAN):** 192.168.0.252
- **IP Virtual CARP (OPT1):** 192.168.50.253

5.2.3 *Firewall* 2

O *Firewall* 2 possui uma configuração semelhante ao *Firewall* 1, com as seguintes especificações:

- **Placa de Rede 1 (em0):** Modo bridge (WAN) Endereço IP: Desativada
- **Placa de Rede 2 (em1):** Modo bridge (LAN)
- **Endereço IP:** 192.168.0.251
- **Placa de Rede 3 (em2):** Modo rede interna (intnet) (OPT_1)
- **Endereço IP:** 192.168.50.252 (Servidor DHCP ativo)
- **Versão do pfSense:** 2.7.2 (versão mais recente até o momento da documentação)
- **IP Virtual CARP (LAN):** 192.168.0.252
- **IP Virtual CARP (OPT1):** 192.168.50.253

5.2.4 Configuração do Servidor DHCP

Ambos os *firewalls* utilizam o ISC DHCP com a seguinte configuração de *subnet*:

- **Subnet:** 192.168.50.0/24
- **Faixa de Endereços DHCP (*Pool Range*):** 192.168.50.10 - 192.168.50.11 (Apenas um IP é alocado, visto que o laboratório possui apenas uma máquina)
- **Servidores DNS:** 8.8.8.8, 9.9.9.9
- ***Gateway*:** 192.168.50.253

5.2.5 Máquina Ubuntu

A máquina Ubuntu utilizada neste ambiente de rede possui as seguintes configurações:

- **Versão do Ubuntu:** 22.04.3 LTS
- **Placa de Rede:** enp0s3, configurada em modo rede interna (intnet)
- **Endereço IP:** 192.168.50.10/24
- **Servidores DNS:** 8.8.8.8, 9.9.9.9
- ***Gateway*:** 192.168.50.253

5.3 Descrição da Empresa

Para a simulação dos cenários de falha, será considerada uma empresa fictícia do setor de *e-commerce*, cuja operação é totalmente dependente da internet para a geração de receita. A empresa possui uma receita média anual de R$ 8 milhões e conta com 20 funcionários. Todos os sites e sistemas de vendas da empresa estão hospedados em sua infraestrutura local, o que torna a dependência de uma rede funcional essencial para o andamento de suas atividades diárias, como vendas, cadastros de clientes e outras demandas operacionais.

5.4 Cálculos e custos do cenário

Conforme visto pela forma de calcular a perda de receita, utilizaremos estes números para nossos cenários:

- R$8 milhões de receita anual / 52 semanas = R$153.846,15 de receita média semanal
- R$153.846,15 / 40 horas por semana = R$3.846,15 de receita média por hora
- R$3.846,15 / 60 minutos = R$64,10 por minuto
- R$64,10 / 60 segundos = R$1,07 por segundo

De acordo com estudos sobre as especificações da funcionalidade de alta disponibilidade do pfSense, um dos requisitos para seu funcionamento correto é que as interfaces de rede sejam idênticas em ambos os nós do *cluster*. Para o nosso cenário de testes, utilizaremos os *firewalls* adquiridos na forma de *appliances* idênticos, assegurando essa equivalência na configuração. Além disso, esses equipamentos são mais adequados para redes corporativas, oferecendo maior profissionalismo e confiabilidade. Atualmente, o equipamento *Appliance* pfSense *Firewall* Intel J4125, com 8 GB de RAM e SSD de 128 GB, possui um valor de mercado aproximado de R$ 1.450,00. Considerando a necessidade de dois dispositivos para implementação da redundância, o custo total será de R$ 2.900,00**.**

5.5 Motivo da escolha ser pfSense neste cenário

A maioria das empresas que valorizam a segurança da informação utiliza *firewalls* para gerenciar suas redes. Uma escolha comum no mercado são as soluções *open-source* gratuitas. Contudo, por ser o último ponto de conexão da rede interna com a internet, o *firewall* acumula outras funções além da proteção dos dados, como o roteamento e a manutenção da disponibilidade da rede. Dessa forma, caso o equipamento de roteamento fique inativo, toda a rede interna fica indisponível para o acesso à internet, uma vez que o *firewall* atua como a ponte entre a rede interna e a externa.

Uma ferramenta de código aberto e gratuita bastante utilizada pelo mercado é o pfSense, que desempenha o papel de *firewall* e roteador, sendo comumente utilizado na borda da rede, como o último ponto de acesso. Ele pode ser implementado

em qualquer equipamento, como desktops e servidores, mas também é comercializado na forma de *appliance*, um dispositivo compacto que já vem com o sistema operacional integrado. Os benefícios do *appliance* incluem otimização para redes corporativas, menor acúmulo de resíduos, melhor resfriamento, maior durabilidade e, consequentemente, foco na continuidade da rede devido à sua maior confiabilidade.

5.6 Simulações de inatividades na rede

Para este estudo, serão simulados três possíveis cenários de falhas relacionadas ao *firewall* pfSense de borda, que são comuns no ambiente corporativo e podem impactar significativamente a continuidade dos serviços de rede. Os cenários propostos têm como objetivo avaliar o tempo de inatividade e comparar o uso da ferramenta Alta Disponibilidade.

5.6.1 Simulação de Reboot do *Firewall* pós-atualização

No primeiro cenário, será simulada uma reinicialização simples do *firewall*, causada por uma atualização de *software* que exige um *reboot* do sistema para a aplicação das modificações. Este cenário é comum, pois o pfSense é atualizado continuamente, além de existirem outras correções pelo pacote *System_Patches* que realizam atualizações de pacotes específicos, onde ao final é necessário reiniciar o sistema. Esse processo pode levar de 2 a 10 minutos de tempo de inatividade do *firewall* de borda, dependendo das características de cada rede.

5.6.2 Problema no Sistema Operacional

No segundo cenário, será simulado um problema no sistema operacional do *firewall*, resultando em uma corrupção do sistema que impede o funcionamento do dispositivo. Esse tipo de problema requer habilidades técnicas, pois é necessário realizar a restauração do sistema operacional por meio de uma nova imagem de inicialização. Geralmente, este problema demanda uma resposta imediata da equipe

de TI responsável e, considerando a existência de um backup, o tempo de inatividade para normalizar a rede fica em torno de 2 horas.

5.6.3 Troca de Equipamento

No terceiro cenário, será abordada a falha mais crítica, onde o equipamento que hospeda o *firewall* sofre danos críticos, tornando necessária a substituição ou manutenção do *appliance*. Embora seja uma situação mais rara, ela pode ocorrer, especialmente em locais com condições inadequadas, como ambientes quentes ou sujos, que aumentam a chance de falhas físicas devido à falta de cuidados técnicos. Neste cenário, o tempo de inatividade estimado é de um dia, considerando a recuperação dos arquivos e a aquisição de um novo dispositivo até a normalização completa dos serviços de rede.

6 Testes realizados

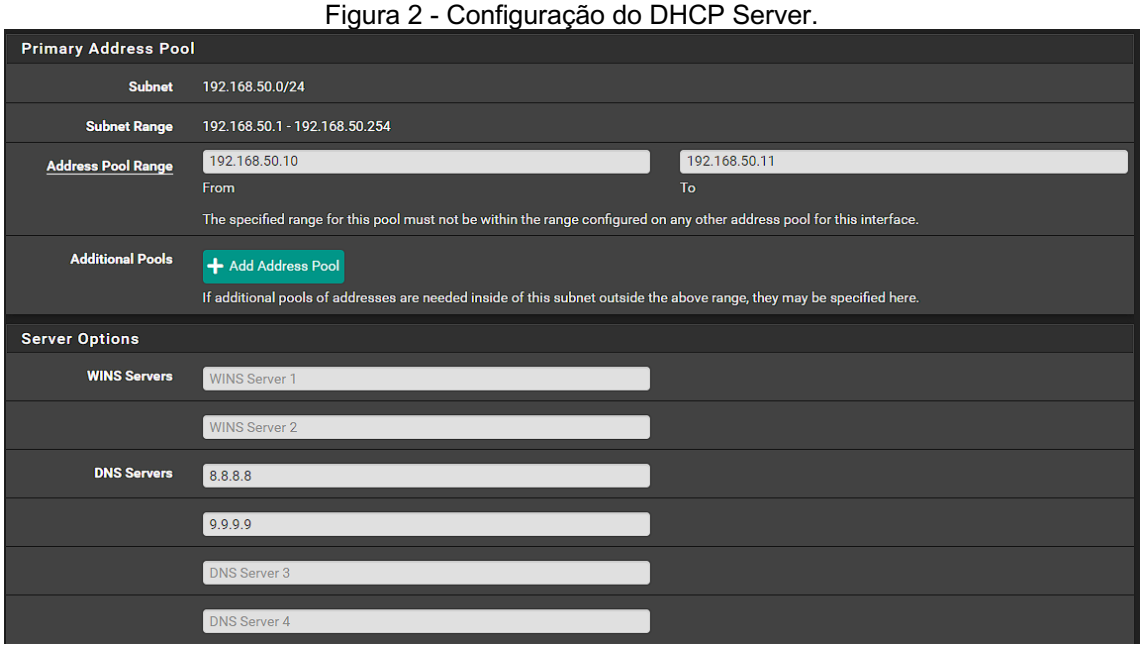
Neste capítulo serão apresentadas todas as configurações e os testes realizados, bem como seus respectivos resultados. Além disso, será realizada uma comparação entre os resultados obtidos, destacando os valores econômicos da empresa fictícia e evidenciando os prejuízos apresentados.

6.1 Configurações

Afim de mostrar as configurações realizadas para o experimento, foi retirado capturas de telas das máquinas envolvidas.

A figura 2 revela as configurações do DHCP Server, onde só deixamos um endereço de IP livre, pois nosso cenário contém apenas uma máquina, essa configuração é replicada igualmente para os dois *firewalls*.

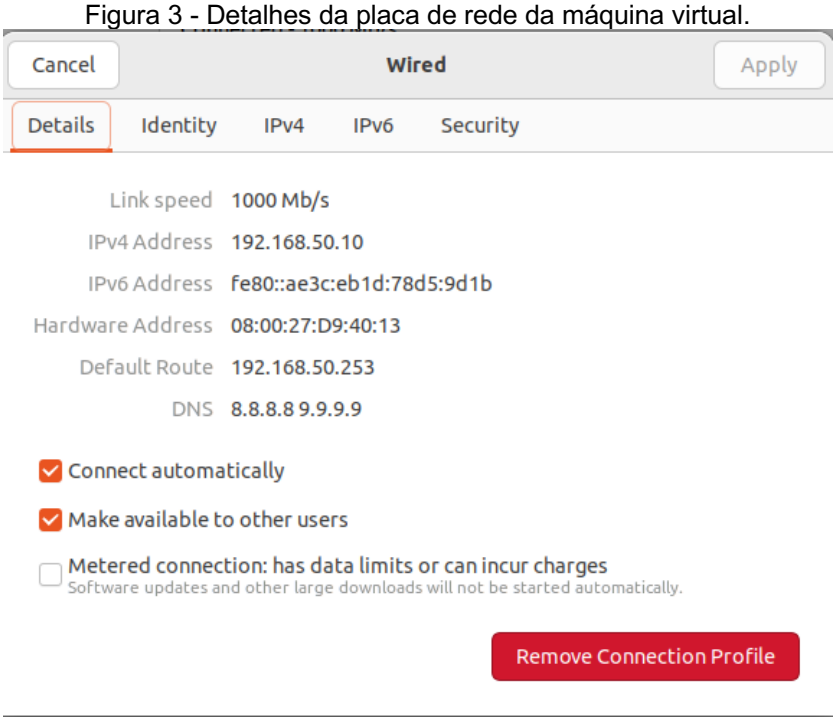
Figura 2 - Configuração do DHCP Server.



Fonte: elaborado pelo autor.

A figura 3 mostra todos os detalhes da placa de rede do Ubuntu, a máquina utilizada no cenário, como velocidade, endereços *IPs*, e *MAC Address*, além de revelar o *gateway* e o DNS adquirido através do DHCP Server.

Figura 3 - Detalhes da placa de rede da máquina virtual.



Fonte: elaborado pelo autor.

6.2 Testes de conexões

Para verificar se o computador está conectado na internet corretamente, é utilizado duas ferramentas do Linux, o *ping* para um destino conhecido, como o do Google conforme mostra a figura 4.

Figura 4 - Teste de ping para o destino google.com

```
caio@caio-VirtualBox:~$ ping google.com -c 5 -4
PING  (172.217.29.142) 56(84) bytes of data.
64 bytes from gru10s01-in-f142.1e100.net (172.217.29.142): icmp_seq=1 ttl=115 time=19.7 ms
64 bytes from pngrua-ad-in-f14.1e100.net (172.217.29.142): icmp_seq=2 ttl=115 time=19.8 ms
64 bytes from gru10s01-in-f142.1e100.net (172.217.29.142): icmp_seq=3 ttl=115 time=21.8 ms
64 bytes from gru10s01-in-f142.1e100.net (172.217.29.142): icmp_seq=4 ttl=115 time=20.6 ms
64 bytes from pngrua-ad-in-f14.1e100.net (172.217.29.142): icmp_seq=5 ttl=115 time=21.5 ms

---  ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 19.653/20.689/21.807/0.869 ms
caio@caio-VirtualBox:~$
```

Fonte: elaborado pelo autor.

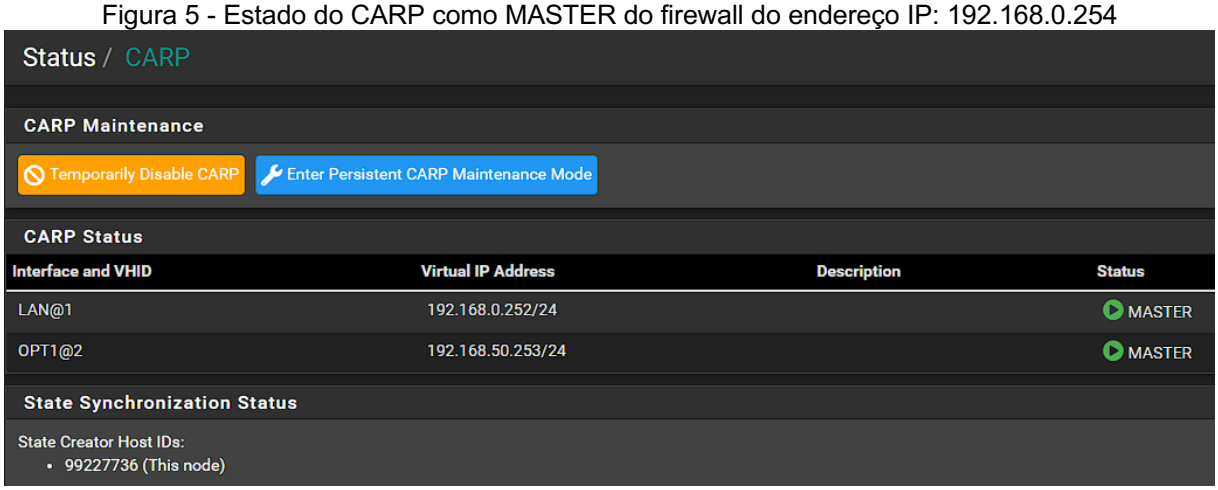
Conforme identificado na figura 4, é possível confirmar que o computador está conectado na internet, pois eles tem a resposta esperada do teste realizado.

6.3 Estado do CARP nos *firewalls*

Foi capturado o estado atual do CARP nos *firewalls*, identificando o primário e o secundário, que nas fotos são *MASTER* e *BACKUP* respectivamente.

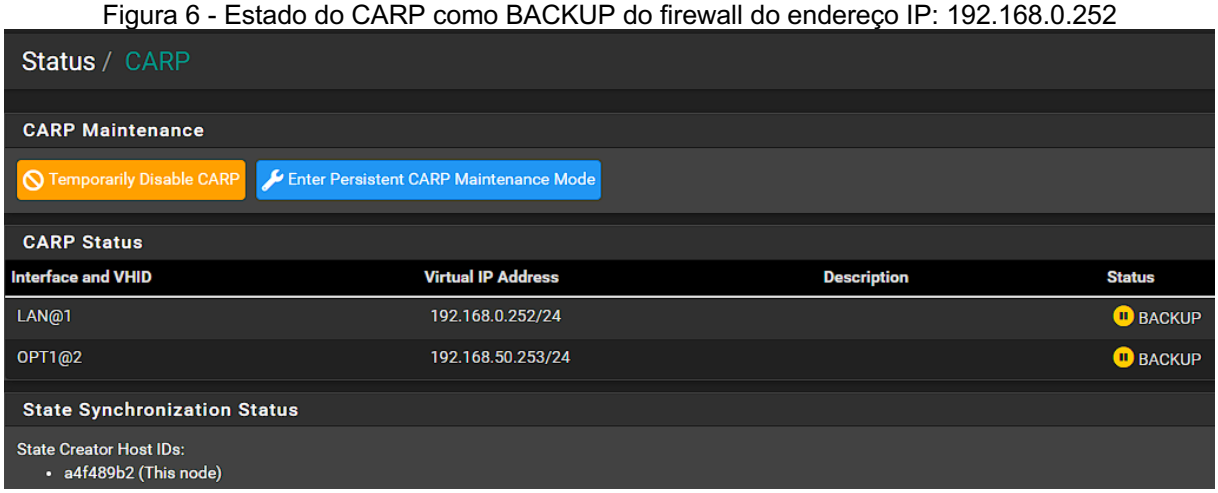
Na Figura 5 é apresentada a captura de tela do firewall principal, mostrando o status do protocolo CARP, no qual ele é identificado como "*MASTER*" nas duas interfaces configuradas com o protocolo (LAN e OPT1). Já na Figura 6 é exibida a mesma tela, porém referente ao *firewall* secundário, evidenciando o status das interfaces como "*BACKUP*".

Figura 5 - Estado do CARP como MASTER do firewall do endereço IP: 192.168.0.254



Fonte: elaborado pelo autor.

Figura 6 - Estado do CARP como BACKUP do firewall do endereço IP: 192.168.0.252



Fonte: elaborado pelo autor.

6.4 **Cenário 1:** Simulação de Reboot do *Firewall* pós-atualização (Com a Alta Disponibilidade configurada)

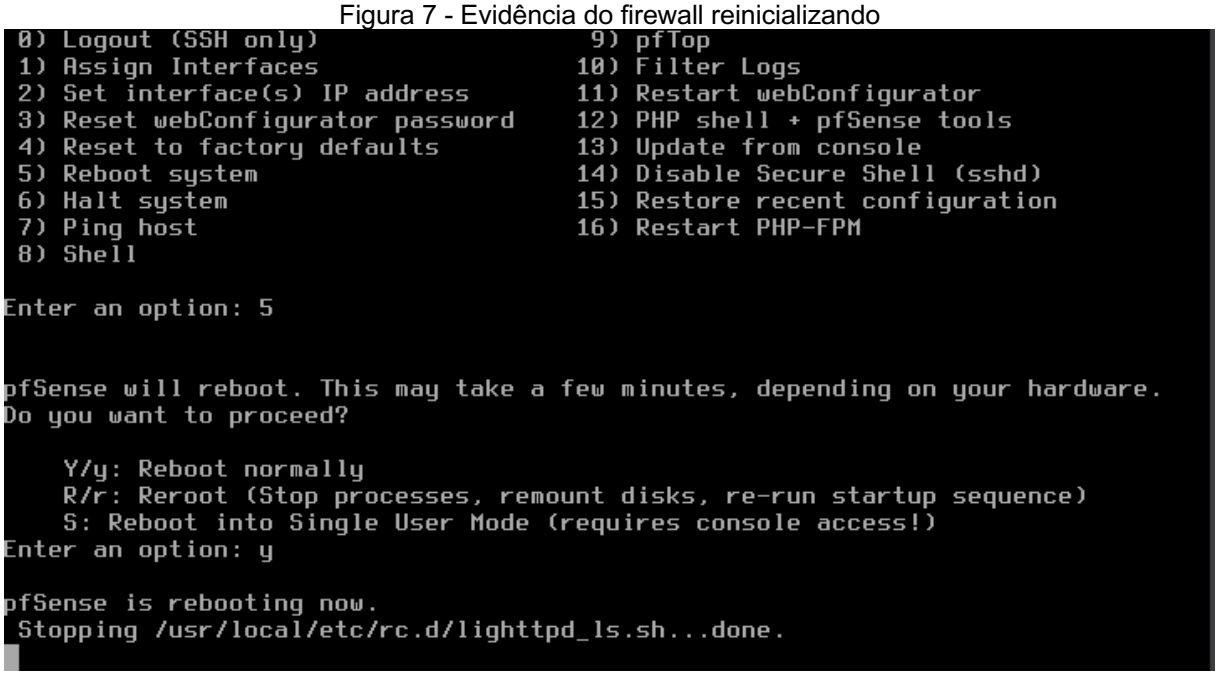
Para este cenário utilizaremos a ferramenta *ping* com registros de data e horas, redirecionando em um arquivo de texto para analisar futuramente e evitar perder registros importantes, para isso utilizaremos o comando:

- *ping google.com | ts '[%Y-%m-%d %H:%M:%S]' > cenario1/firewall_reboot_HA_log.txt*

Esse comando vai monitorar a conectividade com google.com e registrar a saída de data e horas no arquivo *cenario1/firewall_reboot_log.txt*, neste teste será possível verificar os tempos quando teve respostas, mostrando conexão ativa, e o tempo onde não teve comunicação.

Na figura 7, mostra a opção 5 do *firewall "Reboot System*" sendo utilizada, para fazer uma reinicialização segura, igual ocorre em uma atualização.

Figura 7 - Evidência do firewall reinicializando



Fonte: elaborado pelo autor.

A figura 8 comprova o funcionamento do CARP, em segundos após o desligamento do *Firewall* principal, o secundário já aparece como "*Master*", evitando a descontinuidade dos processos da rede, sem identificação de oscilação para o usuário final.

Figura 8 - Firewall secundário virando “Master” após desligamento do primário

Fonte: elaborado pelo autor.

Podemos ver com mais detalhes esse funcionamento através de uma captura de pacote do protocolo CARP, para esse resultado, utilizamos uma ferramenta de captura de pacote conhecida como *tcpdump*, utilizando o comando:

- *tcpdump -i enp0s3 -n proto 112*

Na figura 9, observa-se que, até a linha destacada em rosa, o *firewall* principal (IP 192.168.50.254) era o responsável pelo envio dos pacotes CARP. No entanto, às 22 horas, 33 minutos e 50 segundos, ele interrompe o envio desses pacotes, o que leva o *firewall* secundário a interpretar que o dispositivo principal está inativo. Consequentemente, o *firewall* secundário (IP 192.168.50.252) assume a função de principal às 22 horas, 33 minutos e 54 segundos, resultando em um período de apenas 4 segundos de inatividade.

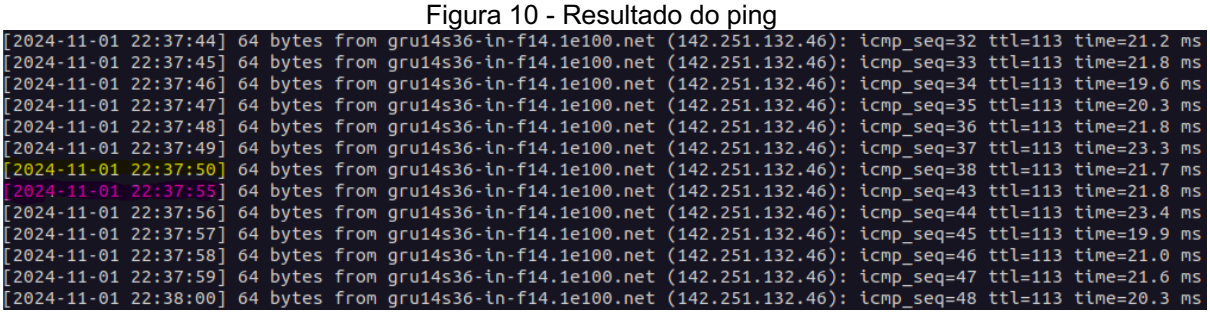
Figura 9 - Funcionamento do CARP

```
22:37:44.659353 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:45.681653 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:46.748620 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:47.777258 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:48.797973 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:49.841376 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:50.881503 IP 192.168.50.254 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s, length 36
22:37:54.281966 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
22:37:55.682382 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
22:37:57.082310 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
22:37:58.476789 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
22:37:59.902094 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
22:38:01.298713 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
22:38:02.741638 IP 192.168.50.252 > 224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 100, authtype none, intvl 1s, length 36
```

Fonte: elaborado pelo autor.

O resultado apresentado na figura 10 comprova, mais uma vez, o funcionamento da alta disponibilidade. Observa-se, com destaque em amarelo, que as respostas cessam após as 22 horas, 37 minutos e 50 segundos, exatamente no momento em que o *firewall* principal interrompe o envio de pacotes CARP. Na linha destacada em rosa, as respostas são retomadas às 22 horas, 37 minutos e 55 segundos, demonstrando um período de inatividade de apenas 5 segundos, imperceptível para o usuário final.

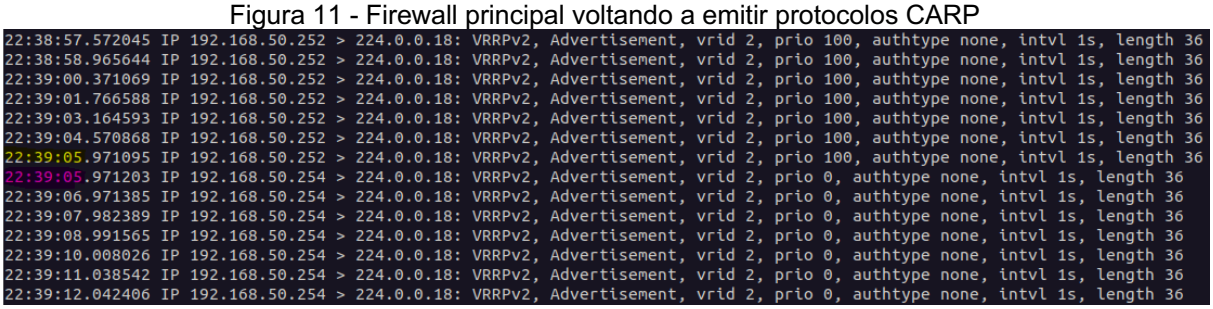
Figura 10 - Resultado do ping



Fonte: elaborado pelo autor.

Após a conclusão do processo de reinicialização do *firewall* primário, ele retoma o envio de pacotes CARP. Assim, o *firewall* secundário, que estava ativo até então, detecta a reativação do *firewall* principal e permite que ele reassuma o controle, conforme ilustrado na figura 11.

Figura 11 - Firewall principal voltando a emitir protocolos CARP

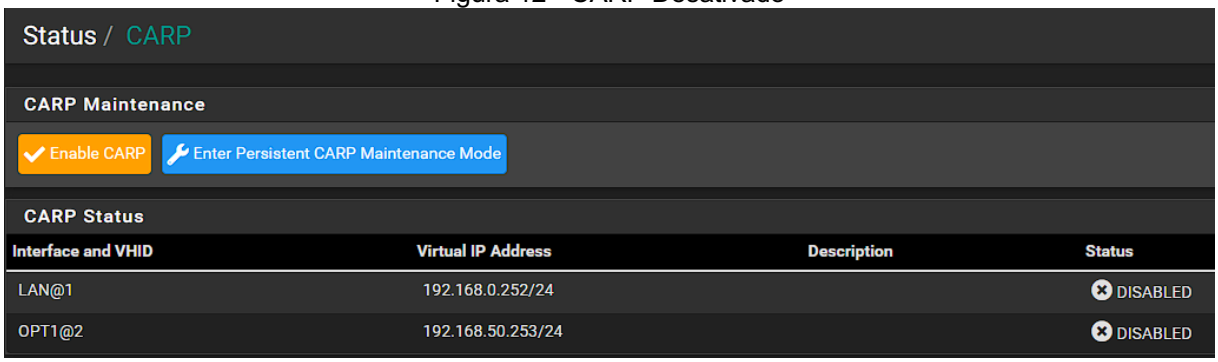


Fonte: elaborado pelo autor.

6.5 **Cenário 1:** Simulação de *Reboot* do *Firewall* pós-atualização (Sem a Alta Disponibilidade configurada)

Para fazermos os testes neste novo cenário, não utilizaremos a ferramenta de Alta Disponibilidade para mostrarmos o tempo de inatividade sem o uso dela, para isso é necessário desativarmos principalmente o CARP nos dois pfSense, conforme ilustrado na Figura 12 o status como *"DISABLED"*

Figura 12 - CARP Desativado



Fonte: elaborado pelo autor.

Para evitar erros no roteamento da máquina, e manter ela conectada na internet, iremos apontar o *gateway* para o Endereço de IP direto para a interface de rede do *firewall*, no caso 192.168.50.254, ficará como o *gateway* da máquina neste teste, mostrado na Figura 13 através do comando Linux *"route –n"*

Figura 13 - Rota nova da máquina

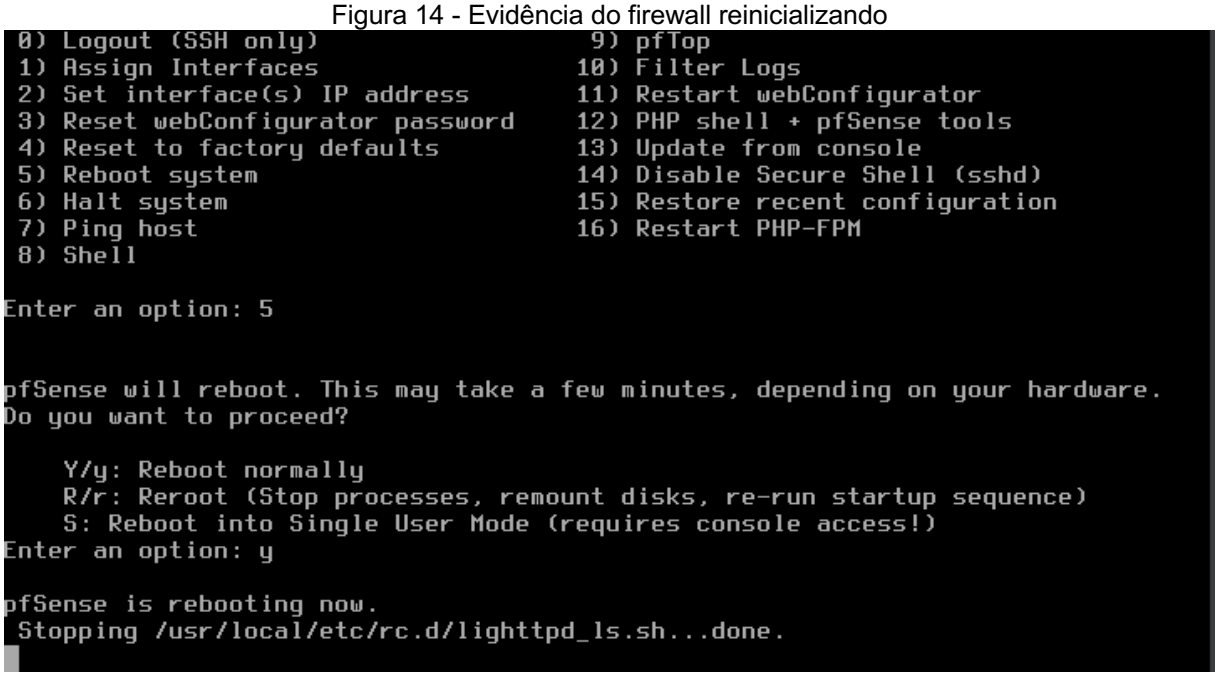
```
caio@caio-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.50.254  0.0.0.0         UG    100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
192.168.50.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
```

Fonte: elaborado pelo autor.

O teste será realizado de forma simplificada, sem a utilização de configurações complexas ou redundantes, simulando um cenário mais direto. Para registrar as respostas e medir o tempo de inatividade da rede, será empregado o comando *ping*, igual no teste passado.

Na figura 14, mostra novamente a opção 5 do *firewall* “*Reboot System*” sendo utilizada, para fazer uma reinicialização segura, igual ocorre em uma atualização.

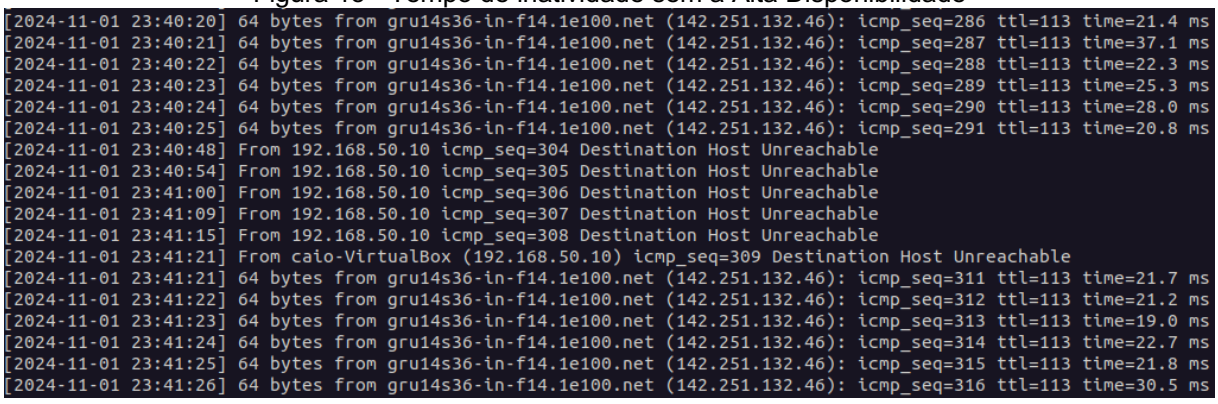
Figura 14 - Evidência do firewall reinicializando



Fonte: elaborado pelo autor.

Conforme indicado na Figura 15, observa-se que, às 23 horas, 40 minutos e 25 segundos, o dispositivo para de receber respostas ao comando *ping* de forma adequada, voltando a receber as respostas corretas às 23 horas, 41 minutos e 21 segundos. Esse intervalo de 56 segundos de inatividade é totalmente perceptível para o usuário final.

Figura 15 - Tempo de inatividade sem a Alta Disponibilidade



Fonte: elaborado pelo autor.

Conforme analisado nos logs de resposta dos *pings*, no cenário com o *cluster* de alta disponibilidade, a inatividade da rede foi de apenas cinco segundos, o que não é perceptível para o usuário final. Já no cenário sem redundância, o tempo de inatividade em um simples reinício do sistema chega a 56 segundos. Essa oscilação é perceptível ao usuário final, pois resulta no fechamento das conexões, tornando necessário o estabelecimento de novas conexões para normalizar o funcionamento.

O tempo de inicialização do *firewall* é uma variável, dependente do hardware utilizado e das configurações aplicadas; quanto maior o volume de informações configuradas no *firewall*, maior será o tempo de inicialização. Em geral, esse período varia de 1 a 5 minutos.

Considerando que, nesse intervalo de reinicialização, as conexões serão encerradas, resultando em quase um minuto de inatividade, aplicaremos a fórmula para calcular o impacto financeiro devido à perda de receita. Utilizando os dados da empresa no cenário sem Alta Disponibilidade (HA), a estimativa de perda de receita é dada por:

- R$1,07 por segundo x 56 segundos de inatividade = **R$59,92 reais de prejuízo**

6.6 **Cenário 2:** Problema no Sistema Operacional

Diante de um problema no sistema operacional, é possível considerar o cenário anterior para análise. Conforme observado, em um ambiente configurado com um *cluster* de alta disponibilidade, a inatividade de um dos nós do *cluster* não afeta a experiência do usuário final, independentemente da duração dessa inatividade. Mesmo em casos onde a rede permanece inativa por até 2 horas em um dos nós, o usuário não percebe oscilações, mantendo as operações ininterruptas.

Por outro lado, em um ambiente sem a configuração de alta disponibilidade, um problema dessa natureza resultaria em uma interrupção total para o usuário até que o dispositivo retomasse o funcionamento correto, ocasionando a perda de todas as conexões ativas e a permanência offline por 2 horas. No contexto de uma empresa de e-commerce, essa indisponibilidade implica na interrupção dos sites da empresa pelo mesmo período, o que afeta diretamente sua receita. Com base nesse cenário, é possível calcular o impacto financeiro da inatividade:

- R$3.846,15 de receita média por hora x 2 horas de inatividade = **R$7692,30 reais de prejuízo**

6.7 **Cenário 3:** Troca de Equipamento

Neste cenário, em que é necessário adquirir um novo dispositivo, a rede permanecerá inativa por 24 horas (1 dia) até que o novo equipamento esteja instalado e configurado e normalizado as atividades. Em um ambiente configurado com um *cluster* de alta disponibilidade, a substituição de um dos dispositivos não causaria impacto para o usuário final, mantendo a rede ativa e as operações ininterruptas, mantendo todos os sites da empresa em total funcionamento. No entanto, sem a configuração de um *cluster*, essa aquisição resultará na completa inatividade da rede durante o período de instalação do novo *firewall*, fazendo com que todas as conexões sejam perdidas e que o sistema permaneça offline por 24 horas.

- R$3.846,15 de receita média por hora x 24 horas de inatividade = **R$ 92.307,60 reais de prejuízo**

7 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo avaliar os impactos econômicos da implementação de um *cluster* de Alta Disponibilidade no *firewall* de borda em uma rede corporativa. Utilizando como exemplo uma empresa fictícia de comércio eletrônico de médio porte, foram simuladas possíveis quedas e períodos de inatividade devido a falhas no *firewall*, calculando os prejuízos na receita da empresa e comparando dois cenários: um com o *cluster* configurado e outro sem.

Os resultados da comparação demonstraram que, no cenário sem a configuração do *cluster*, a perda de receita é significativamente maior em relação ao cenário com o *cluster* implementado. O único custo adicional para a configuração do *cluster* é a aquisição de um dispositivo de *firewall* extra com os mesmos módulos de rede do principal. No entanto, o investimento é recuperado em menos de uma hora de inatividade evitada, permitindo concluir que a implementação da Alta Disponibilidade com o pfSense é totalmente viável economicamente em empresas que dependem da internet para seus processos e geração de receita.

Embora o *cluster* seja uma ferramenta essencial para garantir a redundância na rede, pode ser insuficiente para manter a empresa online pelo máximo de tempo possível. Portanto, é de suma importância considerar outros tipos de redundância, como redundância de links de internet (*failover*), balanceadores de carga (*load balancing*) e ferramentas cruciais para a recuperação de desastres, como *backups*.

Conclui-se que a implementação de um *cluster* de Alta Disponibilidade no pfSense, atuando como *firewall* de borda em redes corporativas onde a geração de receita depende da disponibilidade da infraestrutura local, apresenta impactos consideravelmente positivos. A solução demonstra eficácia em casos de falhas no dispositivo do *firewall*, de modo que o usuário final não percebe a inatividade do dispositivo principal da rede, garantindo a continuidade dos serviços e minimizando prejuízos.

REFERÊNCIAS

ACRONIS. ***Acronis Cyber Protection Week Global Report 2022***. 2022. Disponível em: https://dl.acronis.com/u/rc/Acronis-Cyber-Protection-Week-Global-Report-2022.pdf.

ALMEIDA, Fernando Oliveira. ***Implantação e análise da ferramenta PFsense como firewall em uma empresa de médio porte baseado na ISO 27001***. Caratinga: Faculdades Integradas de Caratinga, 2017. Disponível em: https://dspace.doctum.edu.br/bitstream/123456789/399/1/TCC%20FERNANDO%20OLIVEIRA%20DE%20ALMEIDA.pdf.

BUTTON, Sérgio Tonini. ***Metodologia para Planejamento Experimental e Análise de Resultados.*** Campinas: Universidade Estadual de Campinas, Faculdade de Engenharia Mecânica, 2012. Disponível em: https://www.fem.unicamp.br/~sergio1/pos-graduacao/IM317/apostila2012.pdf.

ENCOMPUTERS. ***Small Business Cost of Downtime*****.** 2024. Disponível em: https://www.encomputers.com/2024/03/small-business-cost-of-downtime/#toggle-id-1.

EVOLVEN. ***Downtime, Outages and Failures – Understanding Their True Costs*****.** 2021. Disponível em: https://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html.

FERREIRA, Filipa; SANTOS, Nélia; ANTUNES, Mário. ***Clusters de alta disponibilidade – uma abordagem Open Source***. Leiria: Escola Superior de Tecnologia e Gestão de Leiria, Instituto Politécnico de Leiria, 2005. Disponível em: https://www.dcc.fc.up.pt/~mantunes/papers/Eng2005_1.pdf.

FERRIGOLO, Ronei Martins. ***O Custo do Downtime***. Disponível em: https://anaiscbc.emnuvens.com.br/anais/article/view/2927/2927.

FLORES, Fábio Brotto; TRETIN, Marco Antônio; TEIXEIRA, Adriano Canabarro. ***Protocolo CARP: Aplicação de Redundância em Firewall: Análise do CARP como Alternativa a Ataque do Tipo DoS***. Disponível em: https://41jaiio.sadio.org.ar/sites/default/files/1_AST_2012.pdf.

FONTENELLE, André. ***Metodologia científica: Como definir os tipos de pesquisa do seu TCC?*** Disponível em: https://andrefontenelle.com.br/tipos-de-pesquisa/. Acesso em: 1 jun. 2024.

GIBBS, Graham. ***Análise de Dados Qualitativos***. Tradução de Roberto Cataldo Costa. 1. ed. Porto Alegre: Bookman, 2009.

GOMES, José Rodrigo da Fonseca***. Segurança de redes de computadores: um estudo sobre o Endian Firewall***. Goiânia: Pontifícia Universidade Católica de Goiás, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/6739/2/tcc%20final%20Rodrigo.pdf.

NETGATE. ***About pfSense. pfSense***. Disponível em: https://www.pfsense.org/about-pfsense/. Acesso em: 20 mai. 2024.

NETGATE. ***Documentação Oficial do pfSense: High Availability*****.** Disponível em: https://docs.netgate.com/pfsense/en/latest/highavailability/index.html#carp-overview.

OSTEC. ***Firewall definição: Aprimore seus conhecimentos sobre segurança***. OSTEC Blog. 2020. Disponível em: https://ostec.blog/seguranca-perimetro/*firewall*-definicao/.

PORTILHO, Tiago Teixeira. ***Proposta de Reestruturação da Rede Lógica de Endereços IPv4 do HUSM com Ênfase na Segurança de Redes*****. 2018**. Disponível em: https://www.ufsm.br/app/uploads/sites/495/2018/12/TCC_Tiago_Portilho.pdf.

REIS, Adrieli Cristiane de Freitas; SOARES JÚNIOR, Claudio Gonçalves; FERREIRA, Jorge Felipe da Silva; ALMEIDA, Júlio César Parra de; SILVA, Matheus Marcondes da; GAVINIER, Sabrina Aparecida dos Santos. ***Cluster de alta disponibilidade***. Guaratinguetá, SP: Faculdade de Tecnologia de Guaratinguetá (FATEC-GT), s.d.

SEVERINO, Paulo Jacinto Rosa; ARAÚJO, Fabrício Geraldo. ***Importância da pesquisa científica***. Revista Perquirere, Patos de Minas, v. 14, n. 2, p. 124-134, maio/ago. 2017. Disponível em: https://revistas.unipam.edu.br/index.php/perquirere/article/view/3371/903.

VENTURA, Magda Maria. ***O Estudo de Caso como Modalidade de Pesquisa***. Revista SOCERJ, 2007, v. 20, n. 5, p. 383-386, set./out. Disponível em: http://sociedades.cardiol.br/socerj/revista/2007_05/a2007_v20_n05_art10.pdf.

VIEIRA, Omar Junio Antunes; VIANA, José Corrêa. ***Comparação da alta disponibilidade implementada no PfSense e no Mikrotik***. Revista Perquirere, Patos de Minas, v. 17, n. 2, p. 228, maio/ago. 2020. Disponível em: https://revistas.unipam.edu.br/index.php/perquirere/article/view/2027/629.

VIEIRA, Samuel Antonio. ***Cluster de alta disponibilidade com balanceamento de carga em máquinas virtuais: gerenciando banco de dados MariaDB com Galera Cluster***. Tatuí, SP: Faculdade de Tecnologia – Centro Paula Souza, 2022. Disponível em: https://sol.sbc.org.br/index.php/latinoware/article/view/22972/22799

ZDNET. ***Average large corporation experiences 87 hours of network downtime a year*****.** 2014. Disponível em: https://www.zdnet.com/article/average-large-corporation-experiences-87-hours-of-network-downtime-a-year/.