SEGURANÇA E SEGMENTAÇÃO DE REDE IMPLEMENTAÇÃO PRÁTICA DE UMA DMZ PARA PROTEÇÃO DE SERVIÇOS EXPOSTOS

1º Sargento – HUGO LEANDRO SUAREZ ABIMORAD
2º Sargento – MARCOS CONCEIÇÃO DE JESUS
2º Sargento – JOSÉ NILSON SILVA DOS SANTOS

RESUMO

A segurança de redes é um dos pilares da infraestrutura de TI, especialmente em ambientes institucionais, onde é necessário proteger dados sensíveis e controlar o acesso a serviços. Nesse sentido, a implementação de uma Zona Desmilitarizada (DMZ) por meio da utilização de uma solução de código aberto como o OPNsense permite isolar serviços expostos à internet, mantendo a integridade da rede interna. Dessa forma, o objetivo é implementar uma infraestrutura de rede segura e segmentada para proteger serviços expostos à internet, utilizando OPNsense para controle de tráfego, regras de firewall, monitoramento avançado (IDS/IPS), VPN para acesso remoto seguro e funcionalidades extras para fortalecimento da segurança da rede, no contexto da Seção de Informática da Escola de Comunicações. A finalidade deste documento é fornecer documentação e catalogação necessárias para a implementação de sistema segmentado de rede por meio de uma estrutura de rede composta por DMZ, LAN e WAN. Além disso, a proposta visa estabelecer práticas padronizadas de segurança e gestão de redes, alinhadas às necessidades operacionais e estratégicas da instituição. A adoção de ferramentas robustas e flexíveis, como o OPNsense, contribui para a elevação do nível de segurança cibernética, mitigando riscos e vulnerabilidades. Por fim, a documentação apresentada servirá como referência técnica para futuras expansões ou ajustes na infraestrutura de rede da Escola de Comunicações.

Palavras-chave: *DMZ, firewall, monitoramento avançado, OPNsense, VPN.*

INTRODUÇÃO

A implementação de uma Zona Desmilitarizada (DMZ) utilizando uma solução robusta e flexível como o OPNsense surge como uma estratégia proativa e eficaz para mitigar os riscos associados à exposição de serviços na internet. Em um contexto onde a segurança cibernética se torna cada vez mais essencial para a continuidade dos negócios e para a proteção de dados sensíveis, a adoção de uma DMZ bem configurada atua como uma camada de segurança intermediária entre a rede interna protegida e a internet pública. Ao isolar os serviços que precisam ser acessíveis externamente, como servidores web, servidores de e-mail ou sistemas de arquivos públicos, a DMZ impede que um ataque bem-sucedido a esses serviços se propague diretamente para a rede interna, onde residem

os dados e sistemas mais críticos de uma organização.

Esse isolamento é fundamental para a implementação de políticas de segurança baseadas no princípio do "privilégio mínimo", garantindo que cada serviço tenha acesso apenas aos recursos estritamente necessários para o seu funcionamento. Além disso, possibilita o estabelecimento de regras de firewall mais específicas e rigorosas, promovendo uma gestão eficiente do tráfego de rede e reduzindo significativamente a superfície de ataque. Dessa forma, a DMZ não apenas dificulta a ação de potenciais invasores, como também facilita a detecção precoce de comportamentos anômalos e tentativas de intrusão.

Este estudo se justifica pela sua relevância em um cenário no qual a segurança cibernética em ambientes institucionais e corporativos muitas vezes não recebe a atenção e o investimento adequados, apesar da sua crescente vulnerabilidade frente ao avanço das ameaças cibernéticas. A rápida evolução de técnicas de ataque, como ransomware, phishing e exploração de vulnerabilidades em sistemas expostos, torna imprescindível que instituições adotem medidas preventivas e estruturais para proteger seus ativos de informação.

A implementação de uma DMZ com OPNsense no âmbito da Seção de Informática da Escola de Comunicações pode servir como um estudo de caso prático e detalhado, demonstrando os benefícios tangíveis de uma arquitetura de segurança bem planejada e implementada. O OPNsense, por ser uma solução open source amplamente reconhecida e com uma vasta gama de recursos de segurança, como firewall, proxy, VPN, IDS/IPS, entre outros, oferece uma plataforma adequada e eficiente para a implementação de políticas de segmentação e proteção de rede.

Adicionalmente, a adoção dessa solução permite à instituição aprimorar seus processos, proporcionando aos usuários envolvidos a oportunidade de vivenciar a aplicação prática de conceitos fundamentais de segurança da informação, redes e administração de sistemas. Esse aspecto pedagógico agrega ainda mais valor ao projeto, ao promover a capacitação de recursos humanos em uma área de conhecimento cada vez mais estratégica.

Por fim, destaca-se que a experiência adquirida com a implementação da DMZ poderá ser replicada e adaptada para outras instituições de ensino ou ambientes corporativos, servindo como referência e incentivo para a adoção de melhores práticas de segurança da informação.

Assim, este trabalho não apenas cumpre um papel técnico, mas também educativo e social, contribuindo para o fortalecimento da cultura de segurança em ambientes institucionais e para a proteção dos dados e serviços essenciais à sociedade contemporânea.

1. IMPORTÂNCIA DA SEGMENTAÇÃO DE REDE: PROTEÇÃO E CONTROLE COM DMZ E OPNSENSE

A crescente dependência de redes de computadores e o aumento de ataques cibernéticos tornam a segurança de rede uma prioridade essencial. Ambientes militares, como a Escola de Comunicações, não estão imunes a essas ameaças. A implementação de uma DMZ com OPNsense busca proteger

serviços expostos e segmentar logicamente a rede para reduzir riscos e aumentar o controle administrativo sobre os fluxos de dados.

FIGURA 1 – OPNsense

Fonte: os autores.

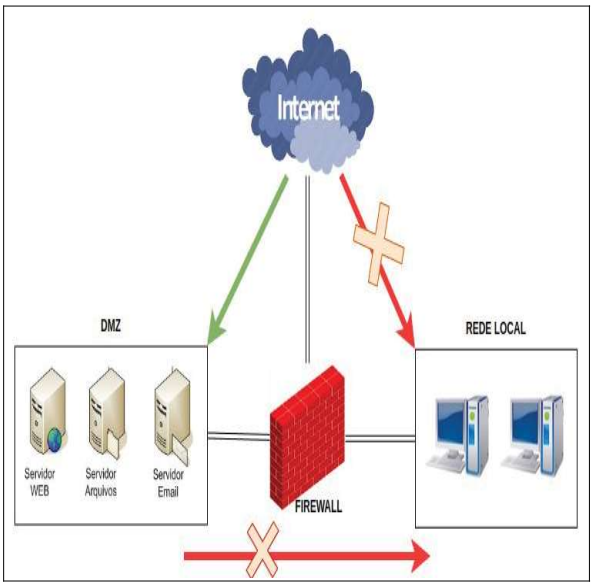
1.1 O QUE É UMA DMZ?

Uma DMZ (sigla para *Demilitarized Zone*, ou "Zona Desmilitarizada") é uma área isolada da rede de uma organização que abriga servidores e serviços acessíveis tanto a partir da rede interna quanto da internet, mas de forma controlada e segura. A implementação de uma rede DMZ tem por função principal proteger a rede interna, criando uma camada adicional de segurança que impede que acessos não autorizados ou ataques comprometam diretamente os sistemas críticos da organização. De acordo com Starllings e Brown (2018):

> "A utilização de uma DMZ permite isolar serviços expostos à internet, reduzindo significativamente o risco de que uma eventual invasão comprometa a rede interna. Além disso, facilita o controle e o monitoramento do tráfego, assegurando que a organização atenda às melhores práticas de segurança da informação" (STALLINGS; BROWN, 2018, p. 412).

A configuração de uma DMZ geralmente envolve o uso de firewalls e outros dispositivos de segurança que regulam rigorosamente o tráfego entre a internet, a DMZ e a rede interna. Dessa forma, mesmo que um servidor localizado na DMZ seja comprometido, o atacante encontrará barreiras adicionais para alcançar sistemas mais sensíveis. Assim, a DMZ se estabelece como um componente essencial em arquiteturas de segurança em rede, especialmente em ambientes que oferecem serviços públicos, como servidores web e de e-mail.

FIGURA 2 - Demilitarized Zone



Fonte: os autores.

1.2 IMPLEMENTAÇÃO DA INFRAESTRUTURA DE REDE

A estrutura proposta foi implementada em ambiente virtualizado utilizando a plataforma Proxmox VE, que permitiu a criação e gerenciamento eficiente de múltiplas máquinas virtuais e interfaces de rede.

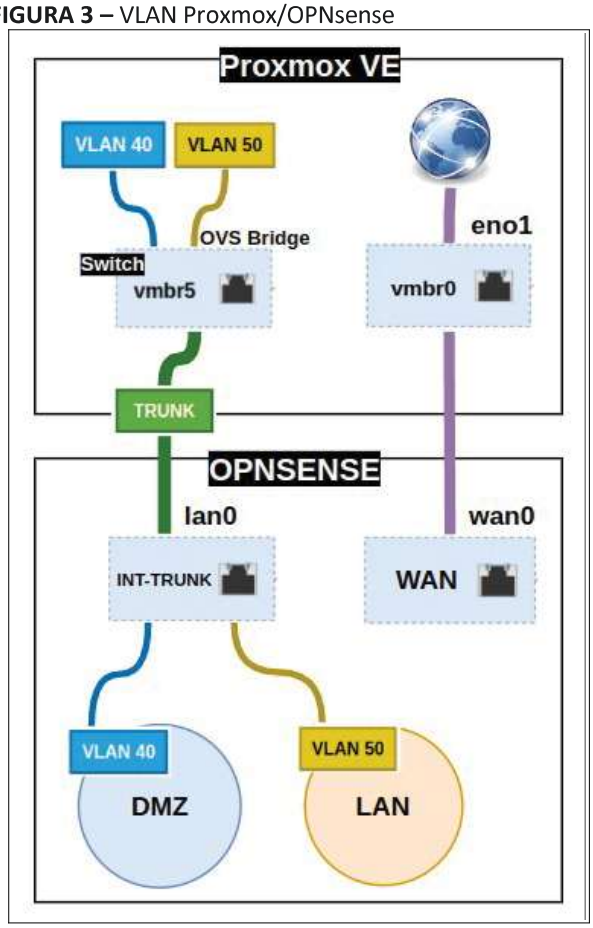
Inicialmente, foram criadas três máquinas virtuais (VMs): a primeira destinada

à instalação do firewall OPNsense, a segunda representando um computador cliente na rede LAN e a terceira configurada como servidor web, localizado na rede DMZ. Em seguida, no Proxmox, foram configuradas duas interfaces de rede distintas. A primeira interface foi configurada como uma bridge, com a função de prover conectividade da internet para a interface WAN do firewall OPNsense. Essa configuração permitiu que a VM do OPNsense tivesse acesso direto à internet, simulando uma interface de borda.

A segunda interface foi configurada especificamente para comportar as VLANs responsáveis pela segmentação das redes internas, por meio da instalação de um plugin adicional que habilita mecanismo semelhante ao funcionamento de um switch, seguindo as boas práticas de segurança e isolamento de domínios. Nesse raciocínio, no ambiente do Proxmox, foram criadas duas VLANs: uma para a rede DMZ e outra para a rede LAN, permitindo a separação lógica entre os serviços expostos à internet e os sistemas internos/rede LAN da organização.

Sequencialmente, no interior do OPNsense, foi configurada a interface WAN, que recebeu a conectividade provida pela bridge configurada no Proxmox. Em seguida, foram criadas e configuradas duas VLANs: uma correspondente à rede DMZ, destinada aos Servidores Web expostos, e outra para a rede LAN, destinada aos computadores clientes. Ambas as VLANs foram associadas à interface VLANSwitch (Int-Trunk) do OPNsense, que está conectada à interface de rede virtual (OVS Bridge) configurada para operar com VLANs no Proxmox, funcionando como um tronco.

FIGURA 3 – VLAN Proxmox/OPNsense



Fonte: os autores.

Essa abordagem permitiu a segmentação eficiente do tráfego de rede, garantindo que as comunicações entre os diferentes domínios fossem controladas de maneira granular através de regras de firewall e políticas de segurança definidas no OPNsense.

Dessa forma, a arquitetura permitiu a criação de um ambiente de rede segmentado e controlado, com o OPNsense atuando como

ponto central de segurança e gerenciamento do tráfego entre as diferentes zonas (WAN, LAN e DMZ). Além disso, a utilização de VLANs para a separação das redes DMZ e LAN reforça a segurança, evitando que eventuais comprometimentos de serviços expostos possam afetar a integridade da rede interna.

1.3 REGRAS DE FIREWALL

Após a implementação da infraestrutura de rede, o próximo passo crucial foi a configuração das regras de firewall no OPNsense. Essas regras são a base da segurança e da segmentação da rede, controlando o fluxo de tráfego entre as diferentes interfaces e VLANs (WAN, LAN e DMZ) de acordo com as boas práticas de segurança. A premissa principal adotada foi a de "privilégio mínimo", ou seja, todo o tráfego não explicitamente permitido é automaticamente bloqueado.

As regras foram aplicadas em cada interface de forma granular, garantindo que apenas as comunicações essenciais e autorizadas pudessem transitar. Para a interface WAN, que é o ponto de contato com a internet, as regras foram extremamente restritivas. Apenas o tráfego de resposta (estados de conexão estabelecidos) e o acesso a serviços específicos expostos na DMZ (como o Servidor Web) foram permitidos, além de regras específicas para VPN, dentre outras. Qualquer tentativa de acesso externo não solicitada ou a portas não autorizadas foi sumariamente bloqueada, mitigando riscos de ataques e varreduras de portas.

Na interface DMZ, foram configuradas regras mais restritivas, permitindo apenas o tráfego indispensável para o funcionamento dos serviços públicos, como acesso externo ao Servidor Web (porta 80 para HTTP e porta 443 para HTTPS) e, em casos específicos, a portas de gerenciamento seguras, quando estritamente necessário.

É importante ressaltar que o acesso da DMZ para a LAN foi rigorosamente proibido, garantindo que, mesmo em caso de comprometimento do Servidor Web na DMZ, a rede interna permaneceria isolada e protegida. Apenas respostas de requisições iniciadas pela LAN à DMZ foram permitidas, seguindo o princípio da comunicação controlada.

Por fim, na interface LAN, as regras de firewall foram elaboradas para permitir o acesso à internet (via interface WAN) e, de forma controlada, o acesso aos serviços específicos hospedados na DMZ. Isso incluiu a navegação web e o acesso a outras aplicações necessárias para os usuários da rede interna. No entanto, o acesso da LAN para a DMZ foi restrito apenas ao que era essencial para o funcionamento dos serviços, evitando a exposição desnecessária e mantendo a segurança da rede interna. A comunicação direta e irrestrita entre a LAN e a DMZ, foi explicitamente negada para evitar vetores de ataque e garantir a integridade do ambiente.

Tabela 1 – Exemplo de Regras de Firewall

Interface	Origem	Destino	Serviço/ Porta	Ação	Descrição
LAN	Rede LAN	Rede DMZ	Any	Negar	Bloquear comunicação entre LAN e DMZ
DMZ	Rede DMZ	Rede LAN	Any	Negar	Impedir tráfego da DMZ para LAN
LAN	Rede LAN	Any	Any	Permitir	Permitir acesso à internet

Fonte: os autores.

A implementação detalhada dessas regras, considerando endereços IP, portas, protocolos e estados de conexão, foi fundamental para estabelecer a segmentação lógica da rede e reforçar a postura de segurança do ambiente, protegendo os serviços expostos e a rede interna contra ameaças cibernéticas.

1.4 PROXY REVERSO

Após a definição das regras de firewall e a segmentação adequada da rede, foi implementado o proxy reverso como uma camada adicional de segurança e gerenciamento dos serviços expostos na DMZ. O proxy reverso atua como intermediário entre os clientes externos e o servidor web localizado na rede DMZ, recebendo as requisições e, após validações, encaminhando-as de forma segura ao destino apropriado.

No contexto desta implementação, o HAProxy, integrado ao OPNsense, foi a solução adotada para desempenhar essa função. A escolha pelo HAProxy se deve à sua robustez, eficiência na manipulação de grandes volumes de tráfego e capacidade de realizar balanceamento de carga, caso necessário, além de oferecer suporte avançado a diversos protocolos e mecanismos de segurança.

A principal função do proxy reverso neste ambiente foi proteger diretamente o servidor web, impedindo que ele fosse exposto diretamente à internet. Com isso, todo o tráfego proveniente da interface WAN chega inicialmente ao HAProxy configurado no OPNsense, onde são aplicadas verificações essenciais, tais como:

- Validação de certificados SSL/TLS, garantindo comunicações seguras via HTTPS.
- Inspeção e filtragem de cabeçalhos HTTP, mitigando tentativas de exploração conhecidas.
- Redirecionamentos ou bloqueios com base em políticas de segurança configuradas.

Além dessas funções, o proxy reverso permite centralizar o gerenciamento de certificados e políticas de segurança, reduzindo a necessidade de configurações complexas diretamente no servidor da DMZ. Dessa forma, o servidor web permanece protegido e isolado, com o OPNsense exercendo um papel de defesa e controle de todas as conexões externas. O uso do proxy reverso também contribui para a performance e a escalabilidade do ambiente, possibilitando, futuramente, a distribuição do tráfego entre múltiplos servidores, caso a demanda de acesso aos serviços públicos aumente. Por fim, ao associar as funções de firewall, segmentação em VLANs e proxy reverso em uma única solução (OPNsense), obteve-se um ambiente coeso, seguro e gerenciável, alinhado com as melhores práticas de segurança da informação.

1.4.1 Aplicação do HAProxy

O HAProxy (High Availability Proxy) é uma solução de software amplamente utilizada para balanceamento de carga (load balancing) e proxy reverso, oferecendo alta disponibilidade, distribuição de tráfego e segurança adicional em ambientes de rede. No contexto do OPNsense, o HAProxy é disponibilizado como um pacote adicional que pode ser instalado e configurado diretamente na interface de administração do firewall, integrando-se de maneira eficiente à estrutura

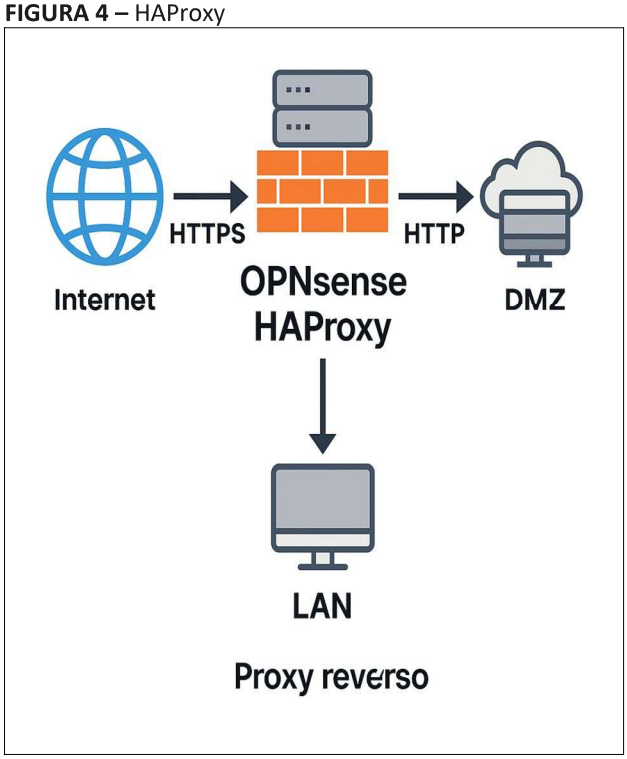
de segurança e segmentação de rede. Sua principal função é atuar como um intermediário entre os clientes que acessam os serviços expostos na internet e os servidores internos, como o servidor web localizado na DMZ. Dessa forma, o HAProxy melhora a gestão de conexões, distribui requisições entre múltiplos servidores, se necessário, e adiciona camadas extras de proteção e mitigação de ataques de negação de serviço (DoS).

Além disso, o uso do HAProxy no OPNsense permite centralizar a publicação de diversos serviços a partir de um único ponto de entrada, aplicando políticas específicas de encaminhamento (frontend e backend), filtros de segurança e autenticações, promovendo uma gestão mais segura e eficiente das conexões externas.

1.4.2 FUNCIONAMENTO do HAProxy

O funcionamento do HAProxy no OPNsense baseia-se na criação de dois componentes principais: frontends e backends. Os frontends são responsáveis por receber as conexões de entrada vindas da internet, definindo quais portas e protocolos serão aceitos, bem como as condições e regras que determinarão como essas conexões devem ser tratadas. Por exemplo, um frontend pode ser configurado para aceitar conexões HTTP e HTTPS, inspecionar cabeçalhos e redirecionar para diferentes servidores dependendo do caminho ou host solicitado. Os backends, por sua vez, são os grupos de servidores internos para os quais as conexões são encaminhadas após passarem pelo frontend. No ambiente implementado, o backend corresponde ao servidor web localizado na rede DMZ, responsável por processar as requisições e enviar as respostas apropriadas aos clientes, sempre mediadas pelo HAProxy.

FIGURA 4 – HAProxy



Fonte: os autores.

Com essa arquitetura, o HAProxy oferece benefícios significativos:

- Segurança: impede que os clientes acessem diretamente os servidores internos, minimizando a exposição.
- Desempenho: distribui cargas de trabalho, podendo direcionar requisições a múltiplos servidores, caso o ambiente seja escalado futuramente.
- Alta disponibilidade: implementa

verificações de saúde (health checks) nos servidores backend, garantindo que apenas serviços operacionais recebam tráfego.

No contexto da estrutura proposta, o HAProxy foi configurado para aceitar conexões HTTPS na interface WAN e, após validação, encaminhá-las ao servidor web na DMZ. Assim, além de reforçar a segurança, essa configuração permite gerenciar certificados SSL/TLS diretamente no OPNsense, centralizando a administração e reduzindo a complexidade nos servidores internos.

2. SURICATA – SISTEMA DE DETECÇÃO E PREVENÇÃO DE INTRUSÕES (IDS/IPS)

O Suricata é um sistema open source de detecção e prevenção de intrusões (IDS/IPS), desenvolvido pela Open Information Security Foundation (OISF). É amplamente adotado em ambientes corporativos por sua eficiência, robustez e escalabilidade na defesa cibernética, atuando na detecção, análise e mitigação de ameaças em redes.

Neste projeto, o Suricata foi implementado com foco na proteção da Zona Desmilitarizada (DMZ), uma área crítica da rede que hospeda serviços acessíveis a partir da Internet, como servidores web, DNS, e-mail e FTP. Por ser constantemente visada por ameaças externas, a DMZ requer monitoramento rigoroso. O Suricata desempenha esse papel aplicando políticas de segurança com base em regras atualizadas, garantindo a detecção e neutralização de tráfego malicioso antes que ele alcance a rede interna.

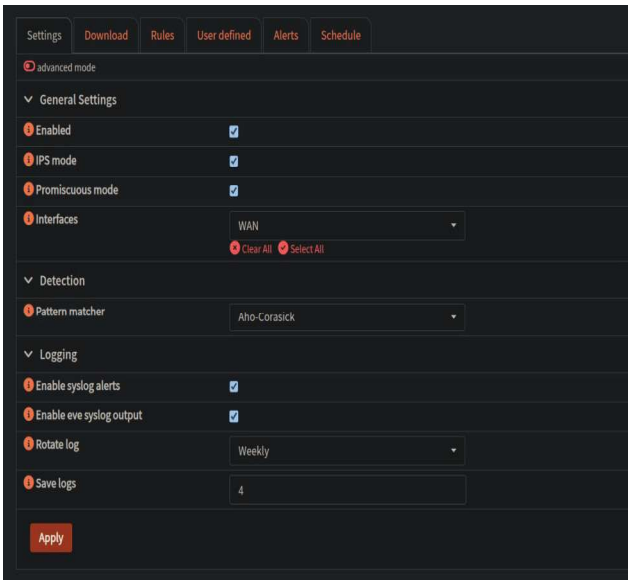
Uma das grandes vantagens do Suricata é sua capacidade de realizar inspeção profunda de pacotes (Deep Packet Inspection - DPI), analisando não apenas os cabeçalhos, mas também o conteúdo das mensagens e protocolos complexos. Isso possibilita identificar comportamentos maliciosos mesmo que ocultos em comunicações aparentemente legítimas. O Suricata suporta DPI para diversos protocolos, incluindo HTTP, TLS/SSL, DNS, FTP, SMB e SSH, tornando-o ideal para ambientes de rede heterogêneos.

O motor de detecção do Suricata é compatível com bases de regras como a Emerging Threats (ET Open e ET Pro), que fornecem assinaturas constantemente atualizadas com base em ameaças reais. Isso o torna altamente eficaz na identificação de ataques emergentes.

O Suricata pode operar em dois modos:

- **IDS (Intrusion Detection System):** monitoramento passivo com geração de alertas.
- **IPS (Intrusion Prevention System):** monitoramento ativo com bloqueio de tráfego malicioso.

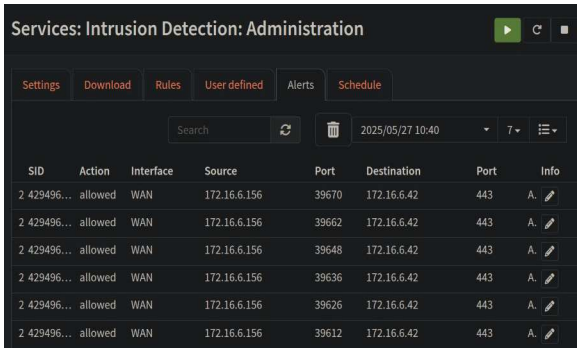
FIGURA 5 – Configuração de monitoramento.
Fonte: os autores.



Essa flexibilidade permite ajustá-lo de acordo com a política de segurança e o nível de intervenção desejado.

Comparado a ferramentas como Snort, Zeek e OSSEC, o Suricata se destaca por oferecer **multithreading nativo**, utilizando múltiplos núcleos de CPU simultaneamente. Isso proporciona um desempenho superior, especialmente em redes com alto volume de tráfego, como em datacenters e ISPs.

FIGURA 6 – Detecção gerada no alerta.



Fonte: os autores.

Outro diferencial relevante é o suporte à decodificação de sessões TLS — quando legalmente possível — permitindo a inspeção de tráfego criptografado, o que é uma limitação em muitas ferramentas de segurança tradicionais. Além disso, o Suricata realiza análise baseada em fluxo de aplicação, possibilitando uma visão contextual das comunicações e reduzindo falsos positivos.

A integração com o **OPNsense**, uma plataforma de firewall baseada em FreeBSD, amplia ainda mais seu potencial. A interface gráfica do OPNsense permite configurar regras personalizadas, visualizar alertas em tempo real, gerar relatórios e atuar rapidamente diante de incidentes, otimizando o trabalho da equipe de segurança.

2.1 Principais vantagens do Suricata:

- Código aberto com suporte ativo da comunidade.
- Processamento multithread para alto desempenho.
- Análise DPI de protocolos variados.
- Compatibilidade com regras ET Open e ET Pro.
- Integração com interface gráfica via OPNsense.
- Geração de alertas e bloqueio em tempo real.
- Inspeção de tráfego criptografado e análise contextual.
- Escalabilidade para redes de diferentes tamanhos.

Em suma, o Suricata é uma ferramenta moderna e eficaz para a defesa proativa da rede, especialmente útil na proteção da DMZ. Combinado ao OPNsense, forma uma solução poderosa, ada

3. OPENVPN – CONEXÃO SEGURA PARA ACESSO REMOTO À DMZ

O OpenVPN é uma solução de rede privada virtual (VPN) de código aberto, amplamente reconhecida por sua robustez, confiabilidade e elevada flexibilidade de configuração. Desde sua criação, o OpenVPN tem se consolidado como uma das tecnologias mais utilizadas para acesso remoto seguro, tanto em ambientes corporativos quanto em redes acadêmicas e governamentais.

Desenvolvido com foco em segurança e

desempenho, o OpenVPN permite a criação de túneis criptografados para conectar redes e dispositivos por meio da Internet, garantindo a confidencialidade e integridade dos dados.

Neste projeto, o OpenVPN é utilizado para fornecer acesso remoto seguro à Zona Desmilitarizada (DMZ) da organização, onde ficam serviços como web, DNS, e-mail e banco de dados replicado. O uso do túnel criptografado evita a exposição direta desses serviços, protegendo contra interceptações e ataques do tipo *man-in-the-middle*, ao garantir que apenas usuários autenticados acessem os recursos da DMZ.

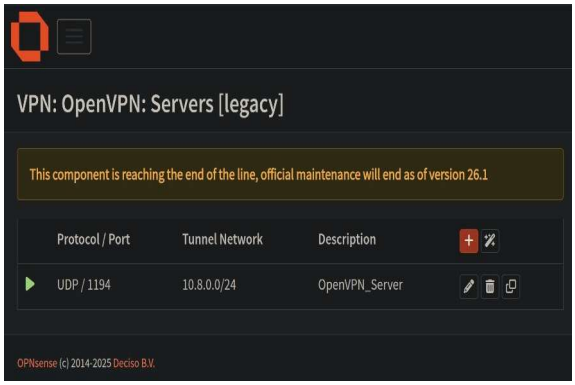


FIGURA 7 – Criação do server.
Fonte: os autores.

A solução permite autenticação por usuário e senha, certificados digitais individuais ou uma combinação de ambos (autenticação mútua), o que assegura que somente usuários autorizados tenham acesso. Além disso, a capacidade de registrar conexões, atividades e eventos dentro da VPN oferece auditabilidade completa, um requisito fundamental em conformidade com normas de segurança da informação, como a ISO/IEC 27001.

O OpenVPN utiliza a biblioteca criptográfica OpenSSL, oferecendo suporte a chaves RSA (2048–4096 bits), certificados X.509 e algoritmos modernos como AES-256-CBC/GCM, com HMAC-SHA256 para integridade e autenticação.

Integrado ao OPNsense, permite configurar autenticação de dois fatores (2FA), reforçando a segurança com um token adicional além da senha.

3.1 Comparação com Outras Soluções de VPN.

Ao ser comparado com outras tecnologias de VPN, como IPSec, L2TP/IPSec e WireGuard, o OpenVPN destaca-se por um equilíbrio ideal entre segurança, compatibilidade, estabilidade e facilidade de implantação:

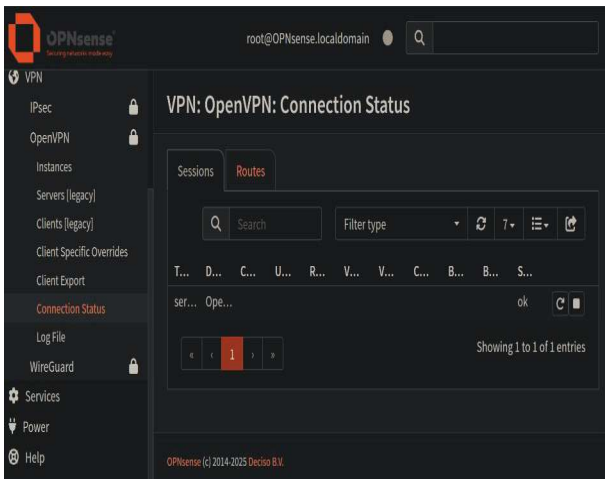
- WireGuard, embora mais moderno e com código mais enxuto, ainda enfrenta limitações de compatibilidade, principalmente com firewalls e appliances mais conservadores. Sua arquitetura baseada em chaves pré-compartilhadas também pode limitar sua aplicabilidade em grandes ambientes corporativos.

- IPSec, por sua vez, é extremamente seguro e padronizado, mas apresenta uma complexidade significativa na configuração, especialmente em ambientes com NAT ou múltiplos firewalls. Além disso, frequentemente requer ajustes finos de política de tráfego e regras de encapsulamento, o que torna sua manutenção mais trabalhosa.

- O OpenVPN, em contraste, é altamente amigável a NATs e firewalls, podendo operar sobre as portas TCP

ou UDP na 443, o que lhe permite disfarçar o tráfego VPN como HTTPS padrão, evitando bloqueios mesmo em redes altamente restritivas. Essa característica o torna ideal para uso em ambientes corporativos, educacionais, hotéis, aeroportos e conexões internacionais, onde firewalls agressivos podem impedir conexões convencionais de VPN.

FIGURA 8 – Status de conexão.



Fonte: os autores.

Quando integrado ao OPNsense, o OpenVPN ganha ainda mais funcionalidades através de uma interface web intuitiva e poderosa. Administradores podem:

- Criar e revogar certificados de forma centralizada;
- Monitorar conexões em tempo real, com detalhes como IP de origem, tempo de conexão e quantidade de dados transferidos;
- Definir políticas de acesso específicas por grupo ou por usuário;
- Implementar ACLs (Access Control Lists) que limitam o acesso do usuário VPN a determinados segmentos de rede;
- Automatizar o bloqueio de conexões suspeitas ou com tentativas de autenticação maliciosas.

Essa abordagem promove controle granular sobre quem acessa a DMZ, quando, e com que permissões, atendendo tanto a requisitos de segurança como aos princípios de mínimo privilégio e segmentação de rede.

Vantagens do OpenVPN:

- Criptografia forte baseada em bibliotecas auditadas e reconhecidas (OpenSSL);
- Suporte a múltiplos métodos de autenticação: senha, certificado, 2FA, etc.;
- Compatibilidade multiplataforma: Windows, Linux, macOS, Android, iOS;
- Fácil integração com OPNsense, permitindo gestão centralizada e intuitiva;
- Operação confiável por trás de firewalls e NATs, inclusive em ambientes com bloqueios de rede agressivos;
- Possibilidade de registro e auditoria de acessos, com logs detalhados;
- Capacidade de restrição de acesso por sub-rede, endereço IP, horário ou perfil de usuário;
- Escalável, ideal tanto para pequenas equipes como para grandes corporações com centenas de usuários

remotos.

Em suma, a utilização do OpenVPN neste projeto representa uma solução segura, flexível e de fácil manutenção para acesso remoto à DMZ, possibilitando que administradores, desenvolvedores ou parceiros externos trabalhem de qualquer local com conectividade segura, sem comprometer a integridade e a confidencialidade da infraestrutura interna.

Sua combinação com o OPNsense transforma o ambiente em um ponto de controle centralizado, seguro e eficiente, essencial para qualquer estratégia moderna de segurança de rede.

4. APLICAÇÃO DE QOS (QUALITY OF SERVICE) COM OPNSENSE PARA CONTROLE E PRIORIZAÇÃO DE TRÁFEGO

Com o uso crescente de redes para múltiplas aplicações (VoIP, vídeo, sistemas corporativos), o desempenho adequado é essencial, mesmo sob alta demanda. A Qualidade de Serviço (QoS) surge como estratégia vital para controlar o tráfego, distribuindo recursos de forma eficiente.

QoS gerencia e prioriza o tráfego de rede, garantindo desempenho para aplicações críticas de baixa latência, como VoIP e streaming. Permite definir políticas para diferenciar pacotes com base em prioridade, tipo de serviço ou consumo de largura de banda.

As regras de QoS visam: (1) priorizar serviços críticos em congestionamentos; (2) limitar banda de aplicações não essenciais, evitando prejuízos à rede; e (3) controlar pacotes, distribuindo banda eficientemente para estabilidade da rede.

Na prática, as regras QoS usam: "pipes" para limites de banda; "queues" para níveis de prioridade; e "regras de filtragem" para associar definições a pacotes específicos (IP, porta, protocolo).

Por exemplo, em uma OM, o tráfego de sistemas corporativos na LAN pode ter prioridade máxima. Vídeos ou redes sociais teriam prioridade inferior ou banda limitada. Isso garante a eficiência dos serviços essenciais, mesmo com rede saturada.

Regras de QoS são fundamentais para redes modernas. Elas permitem priorizar, limitar e controlar o tráfego, mantendo a integridade e desempenho de aplicações críticas e evitando desperdício de recursos. Em qualquer ambiente com muitos usuários, QoS é uma prática recomendada para estabilidade e satisfação do usuário.

5. ANÁLISE DE LOGS E RELATÓRIOS NO OPNSENSE PARA AUDITORIA E AJUSTES

Em ambientes de rede modernos, a análise de logs e relatórios é uma prática essencial para a segurança, auditoria e desempenho operacional. Ferramentas de gerenciamento de rede, como o OPNsense — um firewall e roteador de código aberto baseado em FreeBSD — oferecem recursos robustos para registro, monitoramento e geração de relatórios.

A análise sistemática desses dados permite a identificação de anomalias, ajustes de configuração e tomada de decisões informadas, tornando-se um componente indispensável para a administração eficiente da infraestrutura de rede.

5.1 Registro Detalhado de Eventos: Firewall, VPN, Proxy Reverso e IDS/IPS

O primeiro passo para uma análise eficaz no OPNsense consiste em configurar o registro detalhado dos eventos ocorridos nos principais serviços da rede. Isso inclui:

- Firewall: Registro de tentativas de conexões permitidas e bloqueadas, origem e destino de pacotes, interfaces utilizadas, entre outros. Isso permite identificar possíveis ameaças, acessos não autorizados e gargalos de tráfego.
- VPN (OpenVPN ou IPsec): Monitoramento de conexões estabelecidas, falhas de autenticação e tempo de sessão. Esses logs são fundamentais para verificar a confiabilidade e disponibilidade do serviço para usuários remotos.
- Proxy Reverso (HAProxy): Armazenamento de informações sobre requisições HTTP/HTTPS encaminhadas para servidores internos, ajudando a detectar falhas de roteamento, quedas de serviço e possíveis tentativas de ataque.
- IDS/IPS (como o Suricata): Detecção e prevenção de intrusões, registrando alertas sobre assinaturas maliciosas, exploração de vulnerabilidades e tráfego suspeito.

A configuração detalhada dos logs permite que os eventos sejam armazenados de forma cronológica e estruturada, facilitando a investigação de incidentes e a realização de auditorias completas.

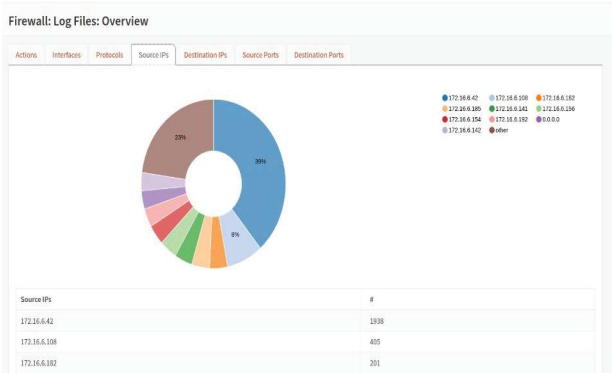
5.2 Criação de Painéis de Monitoramento

Para dar suporte à análise visual e em tempo real dos dados registrados, é recomendada a criação de painéis de monitoramento personalizados. O OPNsense oferece:

- Visualização gráfica do tráfego por interface, IP, porta ou protocolo;
- Acompanhamento em tempo real de alertas de segurança (IDS/IPS);
- Identificação de padrões de uso da banda e picos de tráfego;
- Detecção de comportamentos fora do esperado ou de possíveis ataques.

Esses painéis tornam a gestão da rede mais proativa, auxiliando o administrador na tomada de decisões rápidas com base em dados confiáveis.

FIGURA 9 – Overview



Fonte: os autores.

5.3 Geração de Relatórios Periódicos: Segurança e Performance da DMZ.

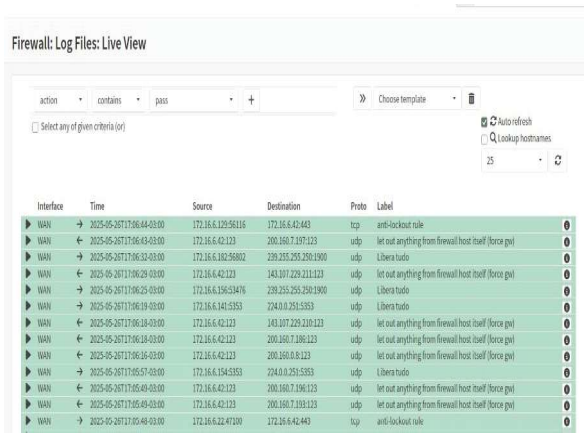
A geração periódica de relatórios é fundamental para manter um histórico organizado das atividades da rede e para embasar ajustes de configuração. Em ambientes que utilizam uma zona desmilitarizada (DMZ), é ainda mais importante acompanhar indicadores de segurança e desempenho, considerando que essa rede expõe serviços públicos (como servidores web e de e-mail) à internet.

Relatórios periódicos devem incluir:

- Volume de tráfego recebido e enviado pela DMZ;
- Tentativas de acesso não autorizado ou escaneamentos de porta;
- Alertas gerados pelo IDS/IPS relacionados à DMZ;
- Tempo de resposta e disponibilidade dos serviços publicados.

Esses dados podem ser compilados automaticamente pelo OPNsense ou exportados para ferramentas especializadas, permitindo uma visão clara do comportamento da rede ao longo do tempo e facilitando a tomada de decisões corretivas ou preventivas.

FIGURA 10 – Live View



Fonte: os autores.

CONCLUSÃO

A implementação de uma Zona Desmilitarizada (DMZ) com o firewall OPNsense revela-se uma estratégia crucial para aprimorar a segurança da informação em ambientes de rede, com um estudo de caso prático na Seção de Informática da Escola de Comunicações. A premissa central é a criação de uma camada de segurança intermediária entre a rede interna (LAN) e a internet (WAN), isolando serviços públicos e mitigando o risco de ataques que, se bem-sucedidos na DMZ, não se propagariam diretamente para a rede interna.

O estudo enfatiza o princípio do privilégio mínimo, onde o tráfego não explicitamente permitido é automaticamente bloqueado. Isso é alcançado através de regras de firewall rigorosamente configuradas no OPNsense para as interfaces WAN, DMZ e LAN, controlando o fluxo de dados em todas as direções.

A WAN, por exemplo, permite apenas tráfego essencial como respostas de conexões iniciadas internamente e acesso a serviços específicos na DMZ, bloqueando o restante. Na DMZ, o tráfego é restrito ao necessário para a operação dos serviços expostos (como HTTP/HTTPS para o servidor web), com comunicação direta para a LAN rigidamente proibida. A LAN, por sua vez, tem acesso controlado à internet e aos serviços da DMZ.

A infraestrutura de rede foi virtualizada no Proxmox VE, permitindo a criação eficiente de máquinas virtuais para o OPNsense, clientes LAN e servidores web na DMZ. A segmentação lógica é reforçada pelo uso de VLANs (Virtual LANs) para a DMZ e a LAN, garantindo isolamento e controle granular do tráfego.

Para uma segurança aprofundada, o artigo descreve a implementação de um Proxy Reverso (HAProxy) no OPNsense. O HAProxy atua como intermediário para os serviços da DMZ, inspecionando e filtrando o tráfego antes

de encaminhá-lo aos servidores, centralizando o gerenciamento de certificados SSL/TLS e oferecendo proteção contra ataques diretos.

Um componente vital para a detecção e prevenção de ameaças é o Suricata, um Sistema de Detecção e Prevenção de Intrusões (IDS/IPS) de código aberto, também integrado ao OPNsense. O Suricata realiza Análise Profunda de Pacotes (DPI) na DMZ, utilizando bases de regras atualizadas para identificar e, no modo IPS, bloquear tráfego malicioso em tempo real, inclusive em comunicações criptografadas (TLS).

Para acesso remoto seguro, o OpenVPN é empregado, permitindo que usuários autenticados acessem a DMZ através de túneis criptografados, protegendo a confidencialidade e integridade dos dados e evitando a exposição direta dos serviços. O OPNsense gerencia centralizadamente as conexões OpenVPN, certificados e políticas de acesso.

Além disso, o artigo aborda a aplicação de Qualidade de Serviço (QoS) no OPNsense para controle e priorização do tráfego, garantindo desempenho adequado para aplicações críticas mesmo sob alta demanda. Por fim, a análise de logs e relatórios no OPNsense é destacada como fundamental para auditoria, detecção de anomalias e ajustes contínuos da configuração de segurança.

Em sua essência, implantação da estrutura de rede apresenta uma solução técnica robusta e escalável, mas também serve como um estudo de caso prático e uma ferramenta educativa, promovendo a capacitação em segurança da informação e incentivando a adoção de melhores práticas em outros ambientes. O objetivo é fortalecer a cultura de segurança e proteger dados e serviços essenciais em um cenário de ameaças cibernéticas em constante evolução.

A flexibilidade inerente ao OPNsense, como uma solução de código aberto, foi um diferencial notável nesta implementação. Sua arquitetura modular permitiu a integração de funcionalidades cruciais como o HAProxy e o Suricata, transformando um firewall em um ecossistema de segurança multifuncional.

Essa capacidade de consolidar múltiplos serviços de segurança em uma única plataforma simplifica a gestão, reduz a complexidade operacional e otimiza os recursos, um fator de grande importância em ambientes onde orçamentos e pessoal são limitados. A liberdade de customização oferecida pelo OPNsense também permitiu que as políticas de segurança fossem ajustadas precisamente às necessidades da Escola de Comunicações, garantindo um nível de proteção sob medida, algo que soluções proprietárias muitas vezes não permitem sem custos adicionais elevados.

O caráter prático deste estudo de caso vai além da mera demonstração técnica; ele sublinha o potencial da virtualização com Proxmox VE como base para a construção de infraestruturas de rede seguras e dinâmicas. A agilidade na criação, teste e modificação de ambientes de rede isolados, graças às máquinas virtuais e às VLANs, é um trunfo inestimável tanto para o desenvolvimento seguro quanto para a capacitação.

Essa abordagem virtualizada não apenas facilitou a implementação da DMZ e de suas camadas de segurança, mas também criou um laboratório vivo, onde conceitos complexos de rede e segurança podem ser explorados e compreendidos de forma prática, preparando futuros profissionais para os desafios reais do mercado de trabalho. A capacidade de replicar essa infraestrutura em diferentes contextos, com adaptações mínimas, reforça o valor da metodologia empregada.

A robustez da solução é ainda mais acentuada pela integração do OpenVPN para acesso remoto. Em um mundo cada vez mais conectado e com a crescente demanda por trabalho e estudo remoto, a capacidade de acessar recursos de rede de forma segura é imperativa.

O OpenVPN, com sua criptografia robusta e flexibilidade de autenticação, garante que apenas usuários autorizados e autenticados acessem a DMZ, protegendo os serviços expostos de acessos indevidos mesmo em trânsito pela internet. Essa funcionalidade não apenas amplia a acessibilidade dos serviços da DMZ para administradores e usuários específicos, mas o faz com um nível de confiança que é crucial para manter a integridade da rede, minimizando o risco de vazamento de informações ou comprometimento através de canais remotos.

Finalmente, a ênfase na análise de logs e relatórios ressalta a importância de uma postura proativa em segurança da informação. A simples implementação de tecnologias não é suficiente; é a capacidade de monitorar, auditar e reagir que realmente fortalece a defesa de uma rede.

Os recursos de logging detalhado e a geração de relatórios no OPNsense, aliada à visualização em painéis de monitoramento, transformam grandes volumes de dados em informações acionáveis. Isso permite que os administradores identifiquem tendências, detectem anomalias e respondam rapidamente a incidentes, ajustando as regras de firewall e outras configurações de segurança em tempo real. Essa vigilância contínua é a espinha dorsal de um ciclo de melhoria contínua da segurança, garantindo que a infraestrutura permaneça resiliente frente às ameaças cibernéticas em constante evolução.

ABSTRACT

Network security is one of the pillars of IT infrastructure, especially in institutional environments, where it is necessary to protect sensitive data and control access to services. In this sense, the implementation of a Demilitarized Zone (DMZ) through the use of an ope source solution such as OPNsense allows isolating services exposed to the Internet, maintaining the integrity of the internal network. Thus, the objective is to implement a secure and segmented network infrastructure to protect services exposed to the Internet, using OPNsense for traffic control, firewall rules, advanced monitoring (IDS/IPS), VPN for secure remote access and additional features to strengthen network security, in the context of the Computer Science Sectio of the School of Communications. The purpose of this document is to provide the documentation and cataloging necessary for the implementation of a segmented network system through a network structure composed of DMZ, LAN and WAN. In addition, the proposal aims to establish standardized network security and management practices, aligned with the operational and strategic needs of the institution. The adoption of robust and flexible tools, such as OPNsense, contributes to raising the level of cybersecurity, mitigating risks and vulnerabilities. Finally, the documentation presented will serve as a technical reference for future expansions or adjustments to the School of Communications' network

infrastructure.

***Keywords**: DMZ, firewall, advanced monitoring, OPNsense, VPN.*

REFERÊNCIAS

STEWART, James Michael. **CompTIA Security+ Guide to Network Security Fundamentals**. 7. ed. Boston: Cengage Learning, 2021.

STALLINGS, William; BROWN, Lawrie. **Segurança de Redes: Princípios e Práticas**. 6. ed. São Paulo: Pearson, 2018.

SOUSA, Luis F.; GOUVEIA, Nelson; PINTO, Luís. **Segurança em Redes de Computadores: Conceitos, Técnicas e Boas Práticas**. FCA - Editora de Informática, 2020.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Comunicação de Dados e Redes de Computadores**. 5. ed. McGraw-Hill Education, 2013.

PEREIRA, Alexandre; GOMES, Rodrigo. **Segurança da Informação e Cibersegurança**. Novatec Editora, 2022.

HAProxy Technologies. **HAProxy Documentation**. Disponível em: https://www.haproxy.com/documentation/. Acesso em: 28 maio 2025.

Open Information Security Foundation (OISF). Suricata Documentation. Disponível em: **Proofpoint.** ET Open Rules – Emerging Threats. Disponível em: ttps://rules.emergingthreats.net/open/suricata/rules/

OPNsense. Documentation. Disponível em: https://suricata.io/documentation/

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de Computadores.** 5. ed. São Paulo: Pearson, 2011.

OpenVPN Technologies Inc. OpenVPN Official Documentation. 2024. Disponível em: https://openvpn.net/vpn-server-resources/

OPNsense Documentation. VPN: OpenVPN Configuration and Management. 2025. Disponível em: https://docs.opnsense.org/manual/how-tos/sslvpn_client.html.