Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

UTILIZAÇÃO DE PROXY PARA IMPLEMENTAÇÃO DA ISO 27001

USING PROXY TO IMPLEMENT ISO 27001

Joao Vitor de Oliveira Guimaraes, aluno do curso de Segurança da Informação na FATEC "Ministro Ralph Biasi" Americana, joao.guimaraes5@fatec.sp.gov.br
Orientador: Prof. Ivan Menerval da Silva, ivan.menerval@fatec.sp.gov.br

Ivis Henrique Lopes Gonçalves, aluno do curso de Segurança da Informação na FATEC "Ministro Ralph Biasi" Americana, ivis.goncalves@fatec.sp.gov.br
Orientador: Prof. Ivan Menerval da Silva, ivan.menerval@fatec.sp.gov.br

Resumo

Este artigo aborda a utilização de proxies como uma estratégia eficaz para a implementação da norma ISO 27001, que estabelece requisitos para um Sistema de Gestão da Segurança da Informação (SGSI). A ISO 27001 é fundamental para a proteção de informações sensíveis em organizações. A adoção de proxies, como Squid e HA*Proxy*, pode ajudar na proteção de dados, controle de acesso e monitoramento de tráfego, alinhando-se aos requisitos da ISO 27001. O estudo destaca as principais características dos proxies, seus tipos, vantagens, desvantagens e como eles contribuem para a conformidade com a ISO 27001.

Palavras-chave: ISO 27001, Proxy, Segurança da Informação, SGSI, Conformidade, Monitoramento de Tráfego, Squid, HAProxy.

Abstract

This article addresses the use of proxies as an effective strategy for implementing the ISO 27001 standard, which establishes requirements for an Information Security Management System (ISMS). ISO 27001 is fundamental for protecting sensitive information in organizations. The adoption of proxies, such as Squid and HAProxy, can help with data protection, access control and traffic monitoring, aligning with the requirements of ISO 27001. The study highlights the main characteristics of proxies, their types, advantages, disadvantages and how they contribute to compliance with ISO 27001.

***Keywords**: ISO 27001, Proxy, Information Security, SGSI, Compliance, Traffic Monitoring, Squid, HAProxy.*

1. Introdução

A segurança da informação é um dos pilares fundamentais para a operação de qualquer organização moderna. A norma ISO 27001 fornece um modelo para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão da Segurança da Informação (SGSI). Este artigo tem como objetivo explorar a utilização de proxies como um recurso eficaz para auxiliar na implementação dos requisitos desta norma.

2. Norma ISO 27001:2022

2.1 Definição e Objetivo

A ISO 27001:2022 é uma norma internacional que especifica os requisitos para um SGSI. Seu objetivo é proteger as informações dentro de uma organização, garantindo sua confidencialidade, integridade e disponibilidade. A norma fornece uma abordagem sistemática para a gestão de informações sensíveis, abordando riscos e vulnerabilidades de segurança.

A ISO 27001:2022 é uma norma internacional que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). O SGSI é um conjunto de políticas, procedimentos, processos e controles que visa proteger as informações dentro de uma organização. Ele abrange aspectos como confidencialidade, integridade e disponibilidade dos dados. Em resumo, o SGSI é projetado para gerenciar os riscos e vulnerabilidades de segurança, garantindo que as informações sejam tratadas de forma segura e eficaz.

2.2 Estrutura da ISO 27001:2022

A **ISO 27001:2022** é uma norma que estabelece requisitos para um sistema de gestão de segurança da informação (SGSI). seu objetivo principal é ajudar as organizações a implementarem, monitorarem e melhorarem continuamente os controles de segurança da informação. esses controles abrangem áreas críticas como políticas de segurança, segurança de recursos humanos, controle de acesso, criptografia e segurança física e ambiental. a implementação desses controles é crucial para proteger as informações da organização, mitigar riscos, evitar violações de segurança e garantir a confidencialidade e integridade dos dados.

2.2.1 Controle A.8.15

O Controle 8.15, intitulado "Registros de Eventos", é fundamental para garantir a rastreabilidade e a análise de atividades relevantes para a segurança, permitindo a identificação de incidentes, a investigação de falhas e a demonstração de conformidade com leis e regulamentações.

O Controle 8.15 exige que a organização implemente um processo abrangente para registrar, armazenar, proteger e analisar eventos de segurança da informação. Isso inclui:

- Definição de eventos a serem registrados: Identificar os tipos de eventos que representam riscos à segurança, como tentativas de login falhas, acessos a dados confidenciais, falhas de sistema e violações de dados.
- Implementação de métodos de registro: Utilizar ferramentas adequadas para registrar os eventos, como logs de sistema, arquivos de auditoria ou bancos de dados específicos.
- Estabelecimento de controles de proteção: Implementar medidas para proteger os registros de eventos contra acesso não autorizado, modificação e exclusão.

- Definição de prazos de retenção: Determinar o tempo durante o qual os registros de eventos devem ser armazenados, de acordo com requisitos legais e regulatórios.
- Implementação de procedimentos de análise: Estabelecer processos para analisar os registros de eventos regularmente, buscando identificar atividades anormais, tendências e potenciais ameaças à segurança da informação.

Os proxies podem ser ferramentas valiosas para auxiliar na implementação do Controle 8.15 da ISO 27001:2022. Ao centralizar o tráfego da internet em um único ponto, os proxies facilitam a coleta e o registro de eventos de acesso à internet, como tentativas de login, downloads, uploads e acessos a sites.

2.2.2 Controle A.8.23

O controle 8.23 da ISO 27001:2022, intitulado "Filtragem Web", destaca a importância de implementar medidas para garantir o uso seguro e responsável dos recursos de rede e internet pela organização,sendo seus principais objetivos:

- Proteger a organização contra ameaças cibernéticas: Ao restringir o acesso a websites e conteúdos maliciosos, a organização diminui o risco de ataques cibernéticos, como malware, phishing e ransomware, que podem comprometer a segurança da informação e causar danos financeiros.
- Controlar o uso de recursos de rede: Limitar o acesso a websites e conteúdos não relacionados ao trabalho ajuda a otimizar o uso da banda larga e evitar gargalos na rede, além de aumentar a produtividade dos colaboradores.
- Promover a conformidade com políticas e regulamentações: O controle do acesso à internet garante o cumprimento de políticas internas da organização, leis e regulamentações relacionadas à segurança da informação e à proteção de dados.

- Conscientizar os colaboradores sobre os riscos cibernéticos: Treinamentos e campanhas de conscientização ajudam a educar os colaboradores sobre os perigos da internet e como se proteger online, minimizando o risco de erros humanos que possam comprometer a segurança da informação.

A utilização de um servidor *Proxy* se configura como uma ferramenta valiosa na implementação do controle 8.23 da ISO 27001:2022, que trata do uso seguro de recursos de rede e internet. Através do *Proxy*, é possível filtrar conteúdos maliciosos e inadequados, monitorar e controlar o acesso à internet, implementar medidas de autenticação e autorização robustas, criptografar dados e otimizar o desempenho da rede.

3. Proxies e sua Utilização

3.1 O que é um *Proxy*?

> Segundo James Kurose (2010) "Um *Proxy* atua como um intermediário entre um cliente e um servidor, aceitando solicitações de conexão, encaminhando essas solicitações ao servidor correspondente e, em seguida, retornando a resposta do servidor ao cliente" (KUROSE; ROSS, 2010, p. 145).

Portanto, o *Proxy* atua como um controlador de acesso, decidindo quem pode trafegar dados externamente. Ele verifica credenciais, verifica permissões e garante que apenas os autorizados tenham acesso aos recursos online. Além disso, o *Proxy* é um filtrador de conteúdo, vasculhando as informações que passam através dele. Ele examina cada pacote de dado, analisando-os e verificando se o conteúdo que está sendo acessado está em sua lista de controle de acesso, como por exemplo: domínios suspeitos e conteúdo potencialmente perigoso, definidos de acordo com sua escolha e necessidade/politica.

3.2 Tipos de Proxies

Existem vários tipos de proxies, cada um com funcionalidades específicas, mas os principais utilizados são:

Proxy HTTP/HTTPS: Utilizado para filtrar e monitorar tráfego web.

Proxy Reverso: Posicionado entre uma rede interna e a internet, ele distribui o tráfego de entrada entre múltiplos servidores.

3.3 Exemplos de serviços de proxies utilizados

3.3.1 *Squid*

Segundo Joel Jaeggli, engenheiro de rede e um dos autores do livro "*Squid: The Definitive Guide*":

"*Squid* é um *Proxy* de cache que melhora o desempenho da navegação na web armazenando em cache páginas frequentemente solicitadas, reduzindo assim a largura de banda e melhorando os tempos de resposta" (JAEGGLI. Joel, 2004, p. 23). Em termos técnicos, o *Squid* implementa os protocolos HTTP, HTTPS, FTP, entre outros, permitindo que os clientes solicitem recursos da web por meio dele. Quando um cliente faz uma solicitação pela primeira vez, o *Squid* encaminha essa solicitação para o servidor web correspondente e armazena uma cópia do conteúdo em seu cache local. Nas solicitações subsequentes para o mesmo conteúdo, o *Squid* pode fornecer o recurso diretamente do cache, evitando assim a necessidade de acessar o servidor web novamente. Isso resulta em tempos de resposta mais rápidos e uma redução no tráfego de rede.

Além do armazenamento em cache, o *Squid* oferece uma variedade de recursos de segurança, incluindo autenticação de usuário, controle de acesso baseado em regras, filtragem de conteúdo e suporte a criptografia SSL/TLS. Esses recursos ajudam a proteger a rede contra ameaças, como acesso não autorizado, ataques de negação de serviço e conteúdo malicioso.

3.3.2 HAProxy

Segundo o site da *LogicMonitor* (2024):

" *HAProxy* é uma solução de *Proxy*, *Proxy* reverso e balanceamento de carga de código aberto para aplicações baseadas em HTTP e TCP. O balanceamento de carga é uma técnica para encaminhar tráfego para servidores com base em regras definidas durante a configuração. Essas regras podem sempre procurar o servidor com o menor tráfego ou simplesmente instruir o *Proxy* a enviar conexões para servidores diferentes em rodízio." (LOGICMONITOR, 2024).

Do ponto de vista técnico, o *HAProxy* atua como um ponto de entrada para o tráfego de rede, recebendo solicitações de clientes e roteando-as para os servidores de destino com base em uma variedade de critérios, como carga do servidor, saúde, geolocalização e algoritmos de balanceamento de carga configuráveis.

Uma das características mais notáveis do *HAProxy* é sua capacidade de suportar grandes volumes de tráfego simultâneo com baixa latência e alta disponibilidade. Ele é conhecido por sua eficiência e escalabilidade, sendo capaz de lidar com milhões de conexões por segundo em hardware relativamente modesto.

3.4 Vantagens e Desvantagens dos Tipos de Proxy

Cada tipo de *Proxy* deve ser selecionado, estudado e implementado de acordo com as necessidades específicas da empresa. É fundamental compreender as

vantagens e desvantagens de cada tipo de *Proxy* para garantir que ele atenda aos requisitos de segurança, desempenho e funcionalidade da rede. Além disso, é importante considerar aspectos como escalabilidade, compatibilidade com os sistemas existentes e facilidade de gerenciamento. Uma escolha bem-informada garantirá que o *Proxy* escolhido seja uma adição valiosa à infraestrutura de rede da empresa.

3.4.1 Vantagens e Desvantagens do *Proxy* HTTP/HTTPS

Vantagens:

- Controle de acesso a informações sensíveis: Os proxies podem ser configurados para controlar o acesso a determinados recursos da rede, garantindo que apenas usuários autorizados possam acessar informações sensíveis.
- Monitoramento de tráfego: Os proxies podem ser usados para monitorar e registrar o tráfego de rede, o que pode ser útil para identificar possíveis ameaças à segurança da informação e investigar incidentes de segurança.
- Filtragem de conteúdo: Os proxies podem ser configurados para filtrar o tráfego de rede com base em políticas de segurança estabelecidas, bloqueando o acesso a sites maliciosos ou não autorizados.

Desvantagens:

- Complexidade de configuração: Configurar e gerenciar proxies HTTP/HTTPS pode ser complexo e exigir conhecimentos técnicos especializados, especialmente para implementações em larga escala.
- Impacto na velocidade e desempenho: O uso de proxies pode introduzir latência e afetar o desempenho da rede, especialmente se os proxies estiverem sobrecarregados ou mal configurados.

- Riscos de segurança adicionais: Se não forem configurados corretamente, os proxies podem representar um ponto único de falha na segurança da rede e serem alvos de ataques cibernéticos.

3.4.2 Vantagens e Desvantagens do *Proxy* Reverso

Vantagens:

- Segurança: Um dos principais benefícios do *Proxy* reverso é a melhoria da segurança. Ele atua como uma camada de proteção entre os clientes externos e os servidores internos, ocultando a infraestrutura de servidor interna e protegendo-a contra ataques diretos.
- Balanceamento de carga: O *Proxy* reverso pode distribuir o tráfego de entrada entre vários servidores internos, ajudando a melhorar o desempenho e a disponibilidade do serviço. Isso é particularmente útil em ambientes com alto volume de tráfego ou onde a escalabilidade é uma preocupação.
- Criptografia SSL/TLS: O *Proxy* reverso pode atuar como um ponto de terminação SSL/TLS, criptografando e descriptografando o tráfego entre os clientes externos e os servidores internos. Isso simplifica a implantação de certificados SSL/TLS e melhora a segurança das comunicações.
- Cache de conteúdo: Alguns proxies reversos têm a capacidade de armazenar em cache conteúdo estático, como imagens e arquivos CSS, reduzindo a carga nos servidores internos e melhorando o tempo de resposta para os usuários finais.
- Flexibilidade na configuração de roteamento: O *Proxy* reverso permite que os administradores de rede configurem regras de roteamento flexíveis com base em diferentes critérios, como URL, cabeçalhos HTTP ou endereço IP de origem, direcionando o tráfego para servidores internos específicos com base nessas regras.

Desvantagens:

- Complexidade de configuração: Configurar e manter um *Proxy* reverso pode ser complexo, especialmente em ambientes com infraestruturas distribuídas e diversas tecnologias.
- Ponto único de falha: Se o *Proxy* reverso falhar, todos os serviços dependentes dele podem se tornar inacessíveis. Portanto, é crucial implementar medidas de redundância e alta disponibilidade para mitigar esse risco.
- Overhead de desempenho: O uso de um *Proxy* reverso pode introduzir algum overhead de desempenho devido ao processamento adicional necessário para rotear e manipular o tráfego de entrada.
- Custo: Implementar e manter um *Proxy* reverso pode ser caro, especialmente se forem necessários hardware e software especializados para suportar os requisitos de desempenho e segurança.
- Dificuldades de depuração: Em ambientes complexos, pode ser desafiador diagnosticar e resolver problemas de conectividade ou desempenho que envolvem o *Proxy* reverso, devido à sua posição intermediária entre os clientes externos e os servidores internos.

4. Implementação da ISO 27001 com o uso de Proxies

4.1 Monitoramento e Auditoria

Os proxies podem ser utilizados para monitorar e registrar todo o tráfego de rede, permitindo auditorias eficazes e a identificação de comportamentos suspeitos ou não conformes com as políticas de segurança da informação definidas

4.2 Estudos de Caso

Em diversos contextos organizacionais, a implementação de proxies tem sido adotada como parte integrante das estratégias de segurança da informação. Estudos de caso revelam que a adoção de proxies, em conformidade com as diretrizes estabelecidas pela Norma ISO/IEC 27001, tem conduzido a melhorias significativas tanto na proteção dos dados quanto na aderência aos requisitos normativos.

Neste trabalho, será apresentado um estudo de caso no qual será configurado o *Proxy* Squid no PFsense para fins de demonstração. A escolha desta configuração específica visa ilustrar de forma prática como a implementação de proxies pode contribuir para a segurança e conformidade das organizações.

4.2.1 Implementação do Firewall Pfsense

O PFsense é uma solução robusta de firewall, conhecida por sua confiabilidade e flexibilidade. Baseado no sistema operacional FreeBSD, o PFsense oferece uma ampla gama de recursos de segurança, desde firewall de próxima geração até VPN e filtragem de conteúdo. Sua interface de usuário intuitiva torna a configuração e o gerenciamento do firewall acessíveis mesmo para usuários com menos experiência técnica.

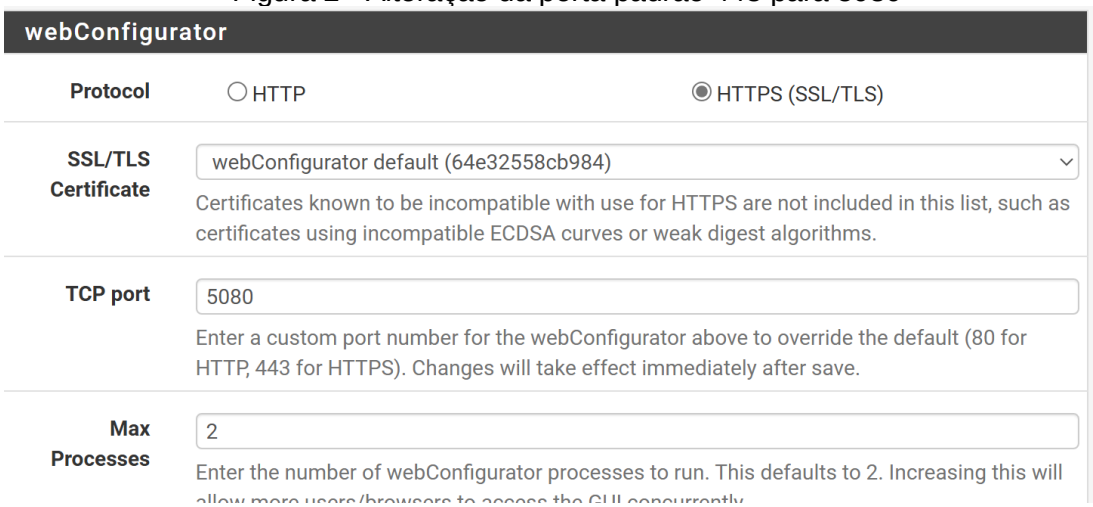
Nesta implementação específica do PFsense, alteraramos a configuração de rede LAN para 192.168.50.1/24 a fim de evitar conflitos de redes.

Figura 1 - Configuração da interface LAN do Firewall

Fonte: Autoria própria

Focamos em fortalecer a segurança da rede ao alterar a porta de acesso padrão para 5080, esta simples modificação ajuda a mitigar potenciais ataques de força bruta, tornando mais difícil para invasores encontrarem e explorarem a interface de administração do firewall.

Figura 2 - Alteração da porta padrão 443 para 5080



Fonte: Autoria própria

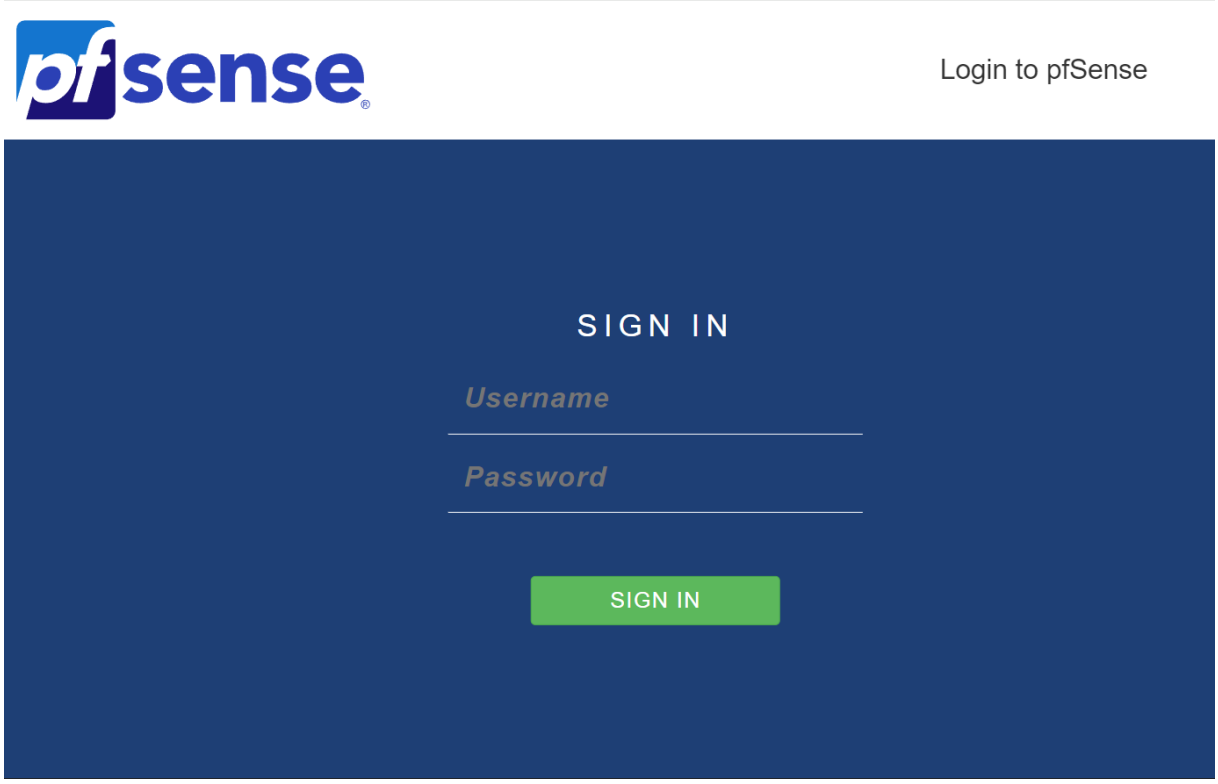
Além disso, para aprimorar ainda mais a funcionalidade do PFsense, foi instalado o pacote Squid. O Squid é um servidor *Proxy* de alto desempenho que oferece caching de conteúdo, filtragem de URLs e controle de acesso à Internet. Com o Squid integrado ao PFsense, os administradores podem otimizar o uso da largura de banda, acelerar o acesso a sites frequentemente visitados e aplicar políticas de segurança adicionais, como bloqueio de sites maliciosos ou não autorizados.

4.2.2 Instalação e Configuração do Pacote Squid no pfSense

O Squid foi escolhido devido à sua reputação de fácil configuração e sua robusta capacidade de filtragem. Essas características o tornam uma escolha popular para servidores de *Proxy* em redes corporativas e de internet, onde a gestão eficiente do tráfego e a aplicação de políticas de segurança são essenciais. Sua flexibilidade e ampla gama de recursos fazem dele uma ferramenta versátil para atender às diversas necessidades de filtragem e controle de acesso em ambientes de rede.

O primeiro passo para a configuração do Squid é o acesso ao Gerenciador de Pacotes do pfSense. Para isso, é necessário acessar o IP configurado da interface LAN na porta 192.168.50.1:5080.

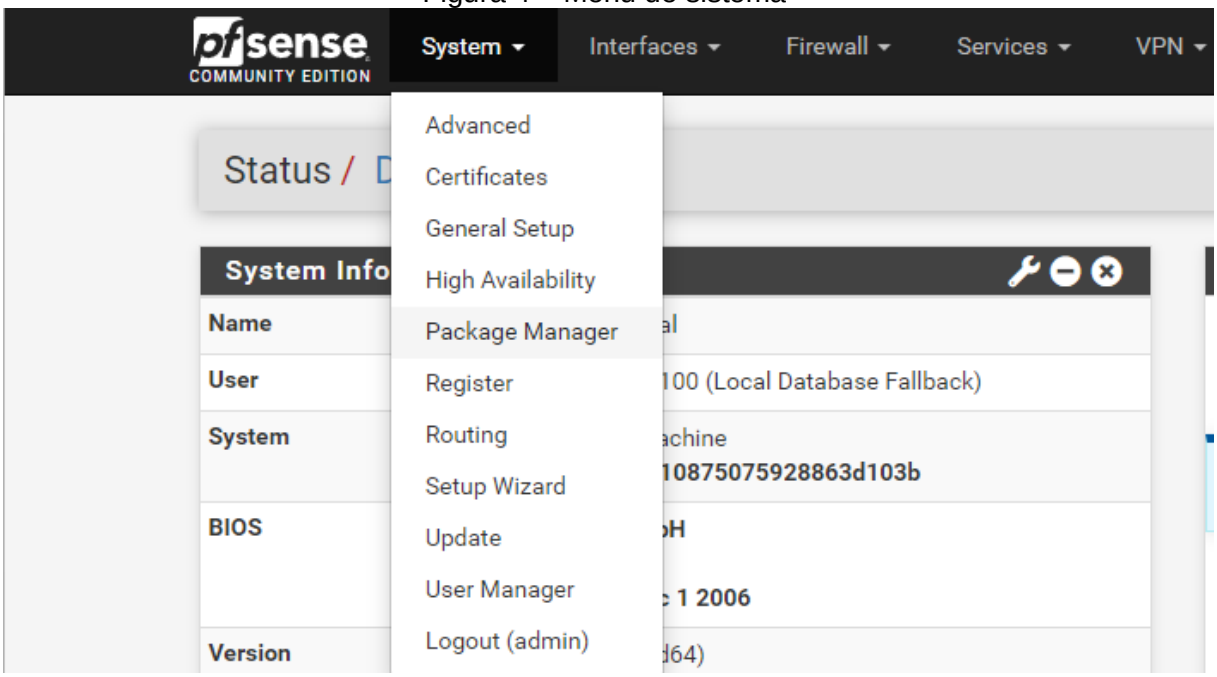
Figura 3 – Tela de login



Fonte: Autoria Propria

É necessário realizar o login com um usuário com permissão para instalação de pacotes, nesse caso utilizamos o usuário admin padrão do PFsense porém com a senha alterada.

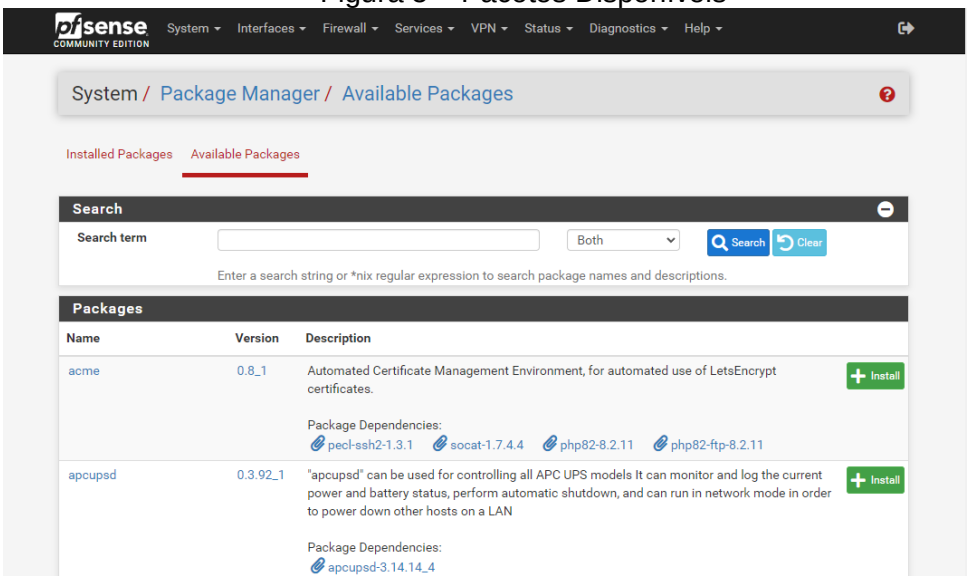
Figura 4 – Menu de sistema



Fonte: Autoria propria

No menu superior, navegue para Sistema → Gerenciador de Pacotes → Pacotes Disponíveis.

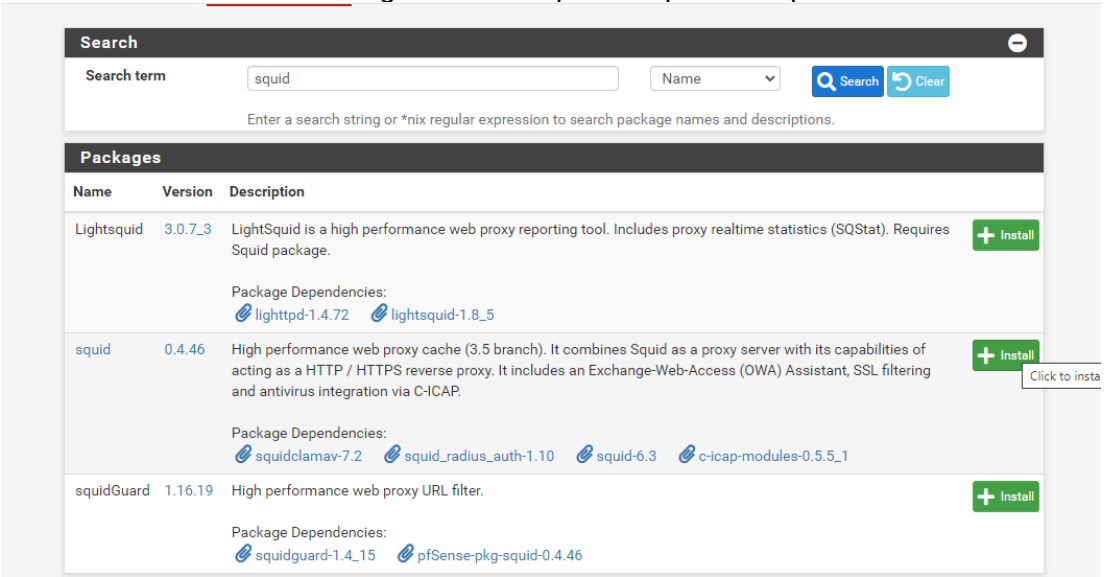
Figura 5 – Pacotes Disponíveis



Fonte: Autoria propria

Em seguida, pesquise pelo pacote Squid e instale-o.

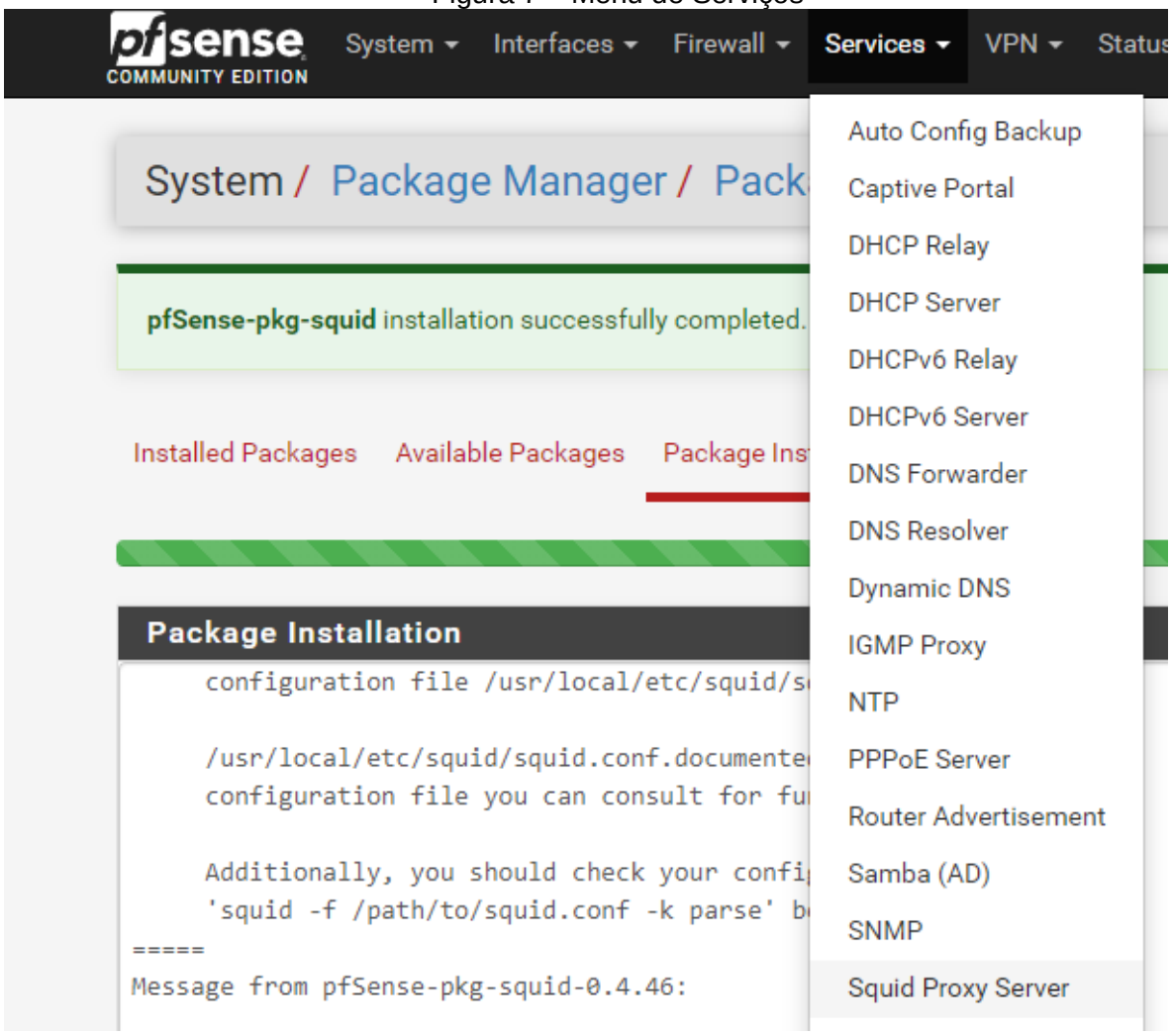
Figura 6 – Pesquisa do pacote Squid



Fonte: Autoria propria

Depois de realizada a instalação do pacote Squid, é necessário proceder com a configuração. Para isso, vá em Serviços → Squid *Proxy* Server

Figura 7 – Menu de Serviços

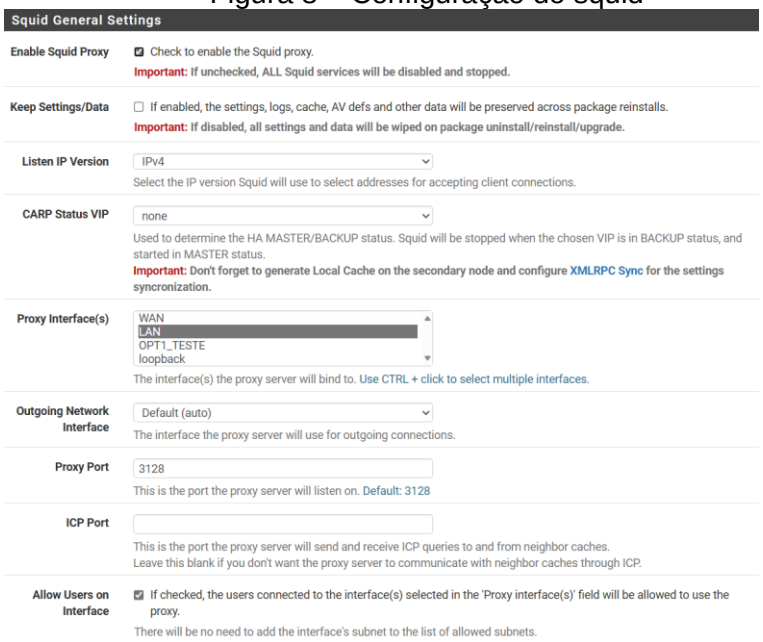


Fonte: Autoria propria

Nas configurações do Squid ativamos a checkbox para que o serviço inicie, utilizamos apenas ele em IPv4 por conta de ainda ser o ambiente mais comum nas empresas, selecionamos para que ele fosse ativo na interface LAN que é a nossa rede interna além de deixar como padrão a porta 3128 de funcionamento do serviço, depois

disso ativamos a opção "Allow Users on Interface" que permite a rede 192.168.50.0/24 de navegar no *Proxy* sem criar uma regra de liberação separada para no squid.

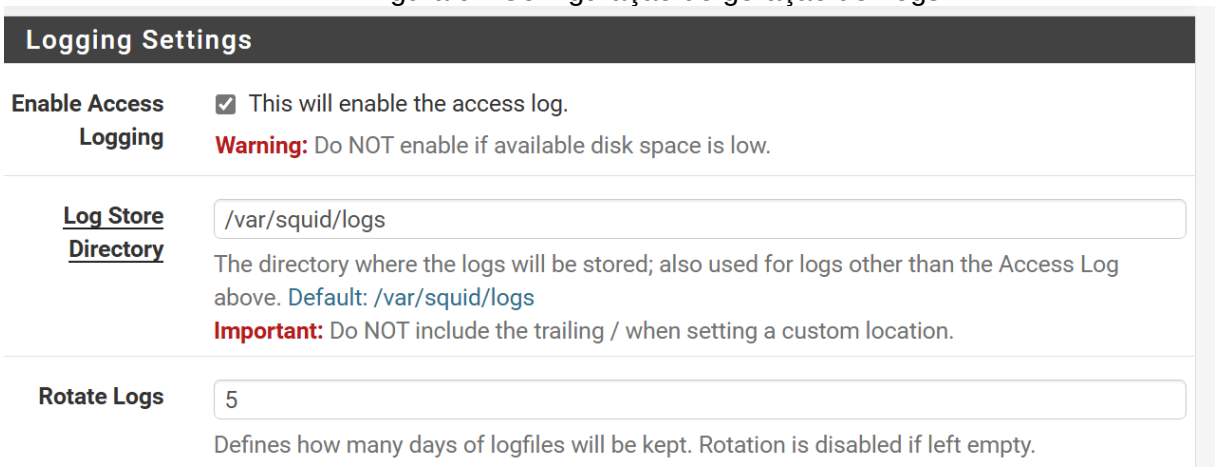
Figura 8 – Configuração do squid



Fonte: Autoria propria

Nas configurações de logs realizamos a ativação e deixamos o caminho de armazenagem de logs no padrão do Squid, definimos para que os logs fossem rotacionados cada 5 dias simulando uma empresa que trabalha segunda a sexta apenas.

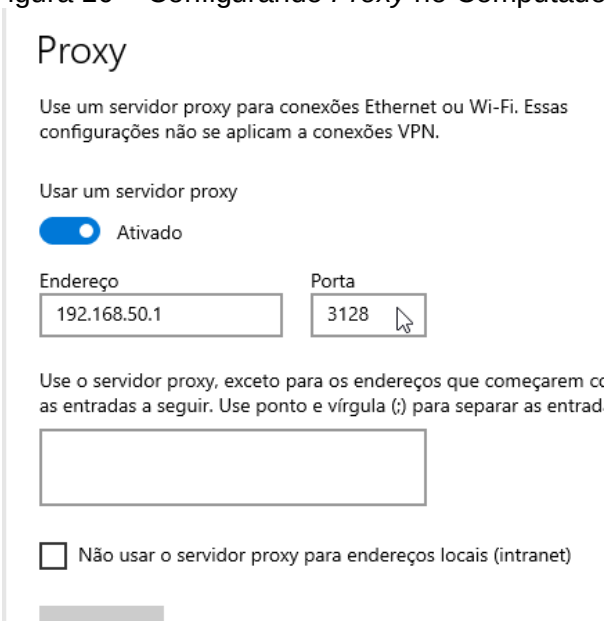
Figura 9 - Configuração de geração de Logs



Fonte: Autoria propria

Após realizar a configuração, no menu de pesquisa do Windows, procure por "*Proxy*" e selecione a primeira opção. Em "Usar um servidor de *Proxy*", coloque no campo "Endereço" o valor 192.168.50.1 e na "Porta" o valor 3128.

Figura 10 – Configurando *Proxy* no Computador



Fonte: Autoria propria

Com a configuração realizada, já é possível visualizar em Serviços → Squid *Proxy* Server → Real Time.

Figura 11 – Logs de Acesso

Squid Access Table

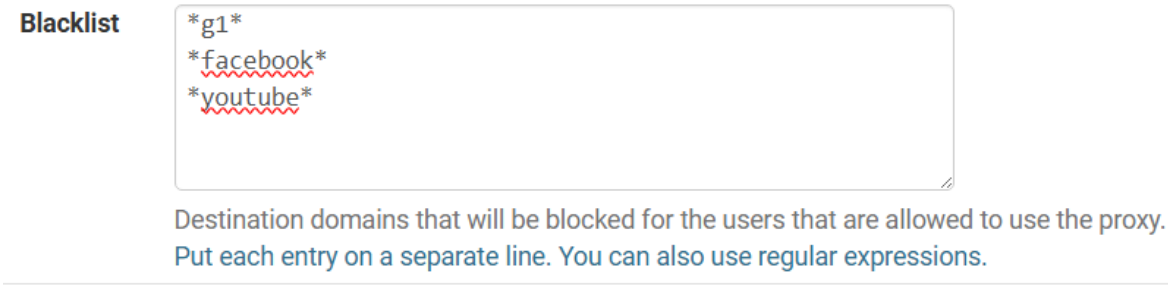
Squid - Access Logs

Date	IP	Status	Address	User	Destination
05.06.2024 00:43:59	192.168.50.13	TCP_TUNNEL/200	prg.smartadserver.com:443	-	216.22.16.0
05.06.2024 00:43:59	192.168.50.13	TCP_TUNNEL/200	ib.adnxs.com:443	-	68.67.178.10
05.06.2024 00:43:59	192.168.50.13	TCP_TUNNEL/200	bidder.criteo.com:443	-	74.119.117.6
05.06.2024 00:43:58	192.168.50.13	TCP_TUNNEL/200	tpsc-ue1.doubleverify.com:443	-	34.117.228.201
05.06.2024 00:43:53	192.168.50.13	TCP_TUNNEL/200	simage4.pubmatic.com:443	-	104.36.113.111
05.06.2024 00:43:53	192.168.50.13	TCP_TUNNEL/200	tps.doubleverify.com:443	-	34.117.228.201
05.06.2024 00:43:53	192.168.50.13	TCP_TUNNEL/200	tpsc-ue1.doubleverify.com:443	-	34.117.228.201
05.06.2024 00:43:53	192.168.50.13	TCP_TUNNEL/200	tpsc-ue1.doubleverify.com:443	-	34.117.228.201
05.06.2024 00:43:39	192.168.50.13	TCP_TUNNEL/200	r.clarity.ms:443	-	20.119.174.243
05.06.2024 00:43:38	192.168.50.13	TCP_TUNNEL/200	tpsc-ue1.doubleverify.com:443	-	34.117.228.201

Fonte: Autoria propria

Para configurar os bloqueios, vá em Serviços → Squid *Proxy* Server → ACLs. Na seção Blacklist, foram bloqueadas, como exemplo, quaisquer URLs que contenham "g1", "facebook" ou "youtube". conforme demonstrado nas imagens abaixo.

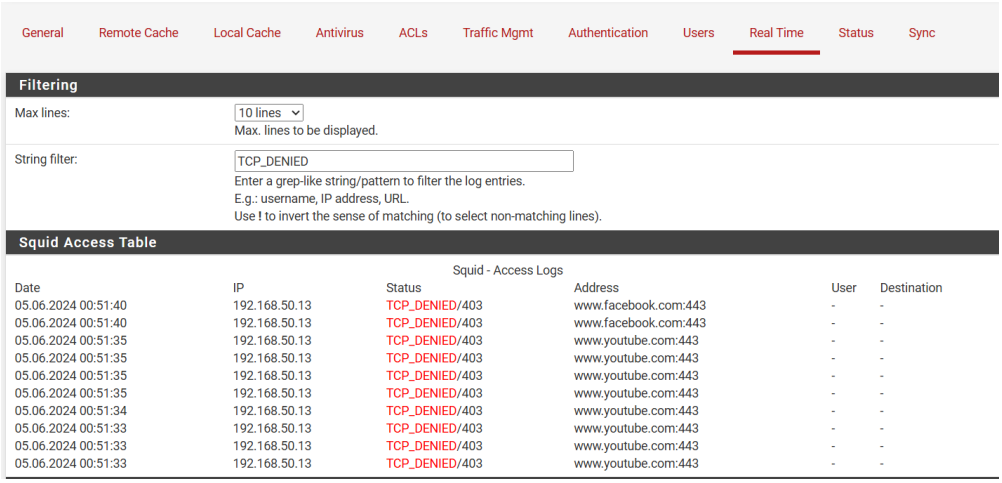
Figura 12 - Configuração de bloqueio



Fonte: Autoria propria

Dessa forma, sempre que for acessado algo com essas palavras, nos acessos em tempo real aparecerá como TCP_DENIED.

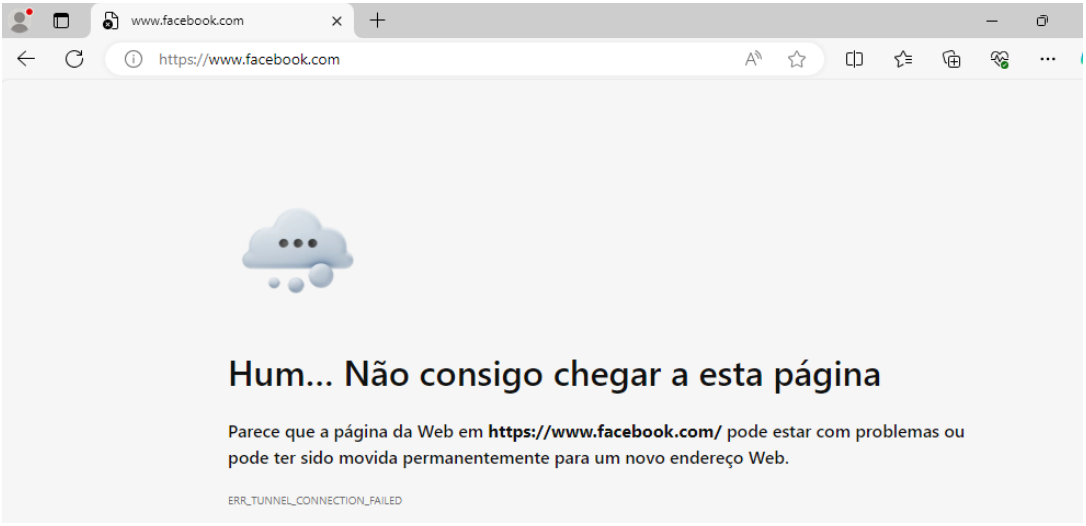
Figura 13 – Logs de bloqueio



Fonte: Autoria propria

No computador do usuário será apresentado um problema de rede e que por conta disso não foi possível acessar a página.

Figura 14 – Bloqueio no computador



Fonte: Autoria propria

5. Considerações Finais

A implementação de proxies é uma ferramenta poderosa na estratégia de conformidade com a ISO 27001. Eles oferecem múltiplos benefícios em termos de segurança, privacidade e controle de acesso, que são essenciais para a proteção de informações sensíveis, pois reduz os riscos de segurança e vulnerabilidades uma vez que bloqueia o acesso a conteúdo não autorizado, além de promover um registro de informações essenciais para melhorias e análises em caso de incidentes.

Após a definição de qual tipo de *Proxy* será utilizado em seu cenário é importante considerar os desafios e custos associados à sua implementação, manutenção, compatibilidade e escalabilidade.

Visando a estabilidade da ferramenta, a implementação de proxies deve ser acompanhada de medidas de redundância para reduzir riscos de falhas do sistema.

Com uma abordagem cuidadosa e bem planejada aplicando compromisso com as melhores práticas de segurança da informação e considerando o grau de complexidade de implantação juntamente ao nível técnico necessário para manter a

ferramenta em funcionamento adequado com a ciência de que quanto maior sua estrutura maior será sua complexidade, os proxies podem contribuir positivamente para um ambiente de segurança da informação trazendo robustez e conformidade com os padrões internacionais.

Referências

HAProxy Technologies. ***HAProxy Documentation***. Disponível em: http://www.haproxy.org/#docs. Acesso em: 15 fev. 2024.

ISMS Online. ISO 27001 Annex A: 8.23 Web Filtering 2022. Disponível em: https://www.isms.online/iso-27001/annex-a/8-23-web-filtering-2022/. Acesso em: 13 fev. 2024.

ISMS Online. ISO 27001 Annex A: 8.15 Logging 2022. Disponível em: https://www.isms.online/iso-27001/annex-a/8-15-logging-2022/. Acesso em: 13 fev.2024

JAEGGLI, Joel. *Squid: The Definitive Guide*. 1. ed. São Francisco: O'Reilly Media, 2004.

LOGICMONITOR. What is HAProxy and what is it used for. Disponível em: https://www.logicmonitor.com/blog/what-is-haproxy-and-what-is-it-used-for. Acesso em: 6 jun. 2024.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 8. ed. São Paulo: Pearson, 2021.

SQUID INTERNET CACHE. ***Squid: Optimising Web Delivery***. Disponível em: http://www.squid-cache.org/Doc/. Acesso em: 3 mar. 2024.

VARDHMAN,Raj; DEFENSOR, Girlie. ***What Is a Reverse Proxy? [All You Need To Know]***. Disponível em: https://techjury.net/blog/what-is-a-reverse-proxy/. Acesso em: 15 fev. 2024.