
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 HAProxy, 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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

- 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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

- 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/política.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

- 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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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*, alteramos a configuração de rede LAN para 192.168.50.1/24 a fim de evitar conflitos de redes.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 1 - Configuração da interface LAN do Firewall

Description	LAN
	Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx
	This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.
MTU	
	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	
	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect)
	Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	192.168.50.1 / 24

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 2 - Alteração da porta padrão 443 para 5080

The screenshot shows the 'webConfigurator' interface. At the top, there is a dark header with the text 'webConfigurator'. Below this, there are several configuration sections:

- Protocol:** Two radio buttons are present. The first is labeled 'HTTP' and is unselected. The second is labeled 'HTTPS (SSL/TLS)' and is selected.
- SSL/TLS Certificate:** A dropdown menu is set to 'webConfigurator default (64e32558cb984)'. Below the dropdown, a note states: 'Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.'
- TCP port:** A text input field contains the value '5080'. Below the field, a note reads: 'Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.'
- Max Processes:** A text input field contains the value '2'. Below the field, a note reads: 'Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.'

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.

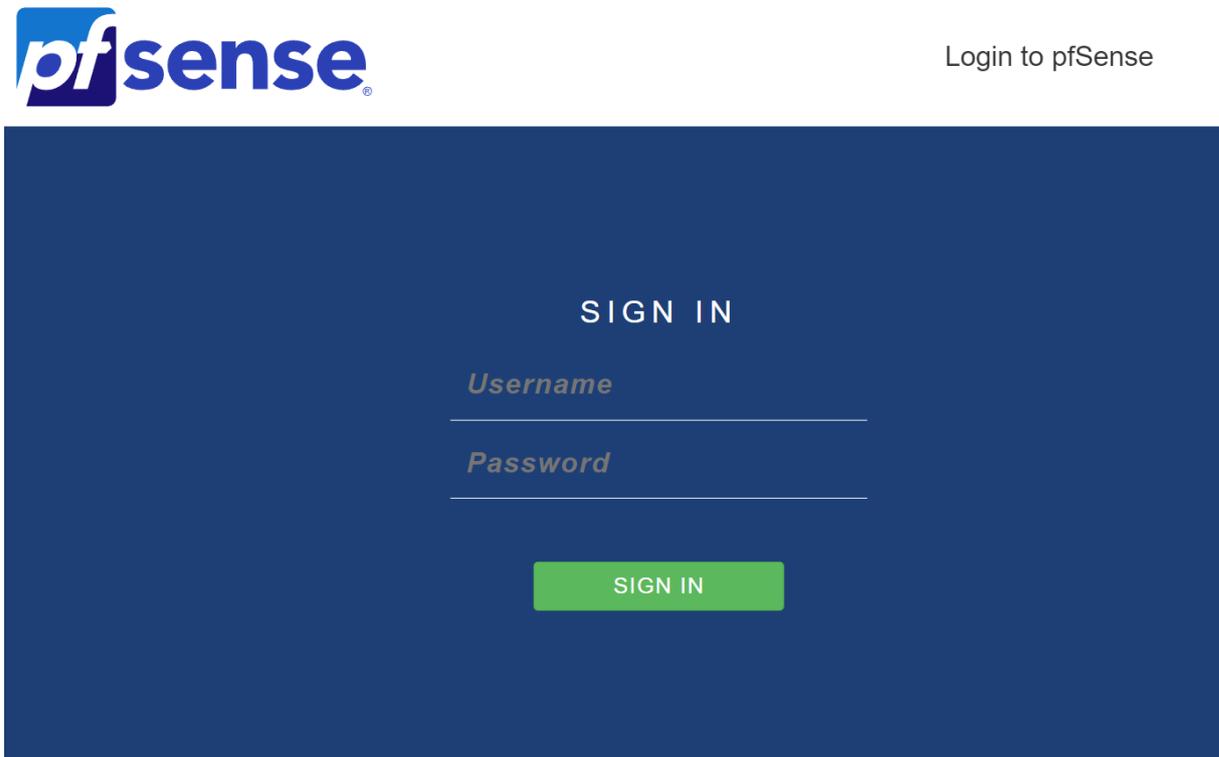
4.2.2 Instalação e Configuração do Pacote Squid no pfSense

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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

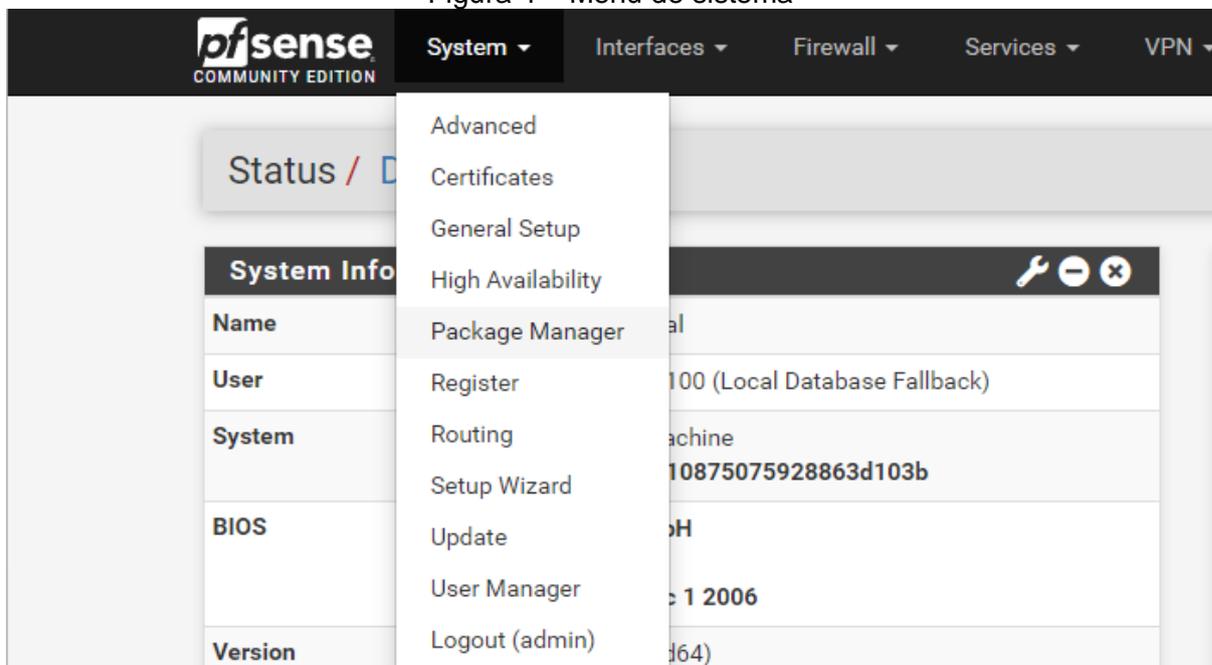


Fonte: Autoria Propria

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 4 – Menu de sistema



Fonte: Autoria propria

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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 5 – Pacotes Disponíveis

The screenshot shows the pfSense Package Manager interface. The breadcrumb trail is "System / Package Manager / Available Packages". There are two tabs: "Installed Packages" and "Available Packages", with the latter being selected. A search bar is present with a search term field, a dropdown menu set to "Both", and "Search" and "Clear" buttons. Below the search bar, a table lists available packages:

Name	Version	Description	Action
acme	0.8_1	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install
apcupsd	0.3.92_1	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN	+ Install

Fonte: Autoria propria

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

Figura 6 – Pesquisa do pacote Squid

The screenshot shows the pfSense Package Manager interface with the search term "squid" entered. The search results table is as follows:

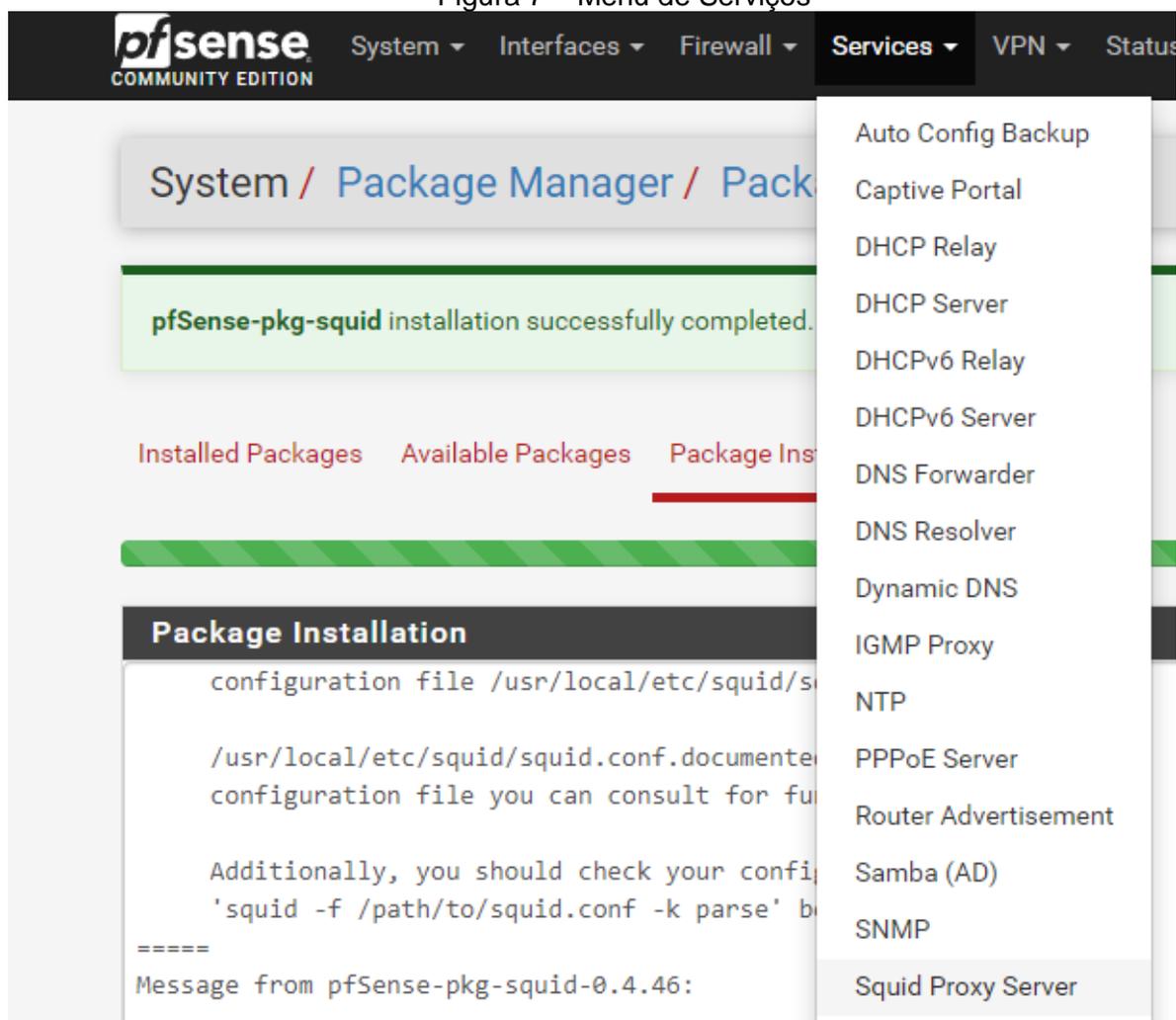
Name	Version	Description	Action
Lightsquid	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
squid	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	+ Install
squidGuard	1.16.19	High performance web proxy URL filter.	+ Install

Fonte: Autoria propria

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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: Aatoria 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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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

The image shows the 'Squid General Settings' configuration page. The settings are as follows:

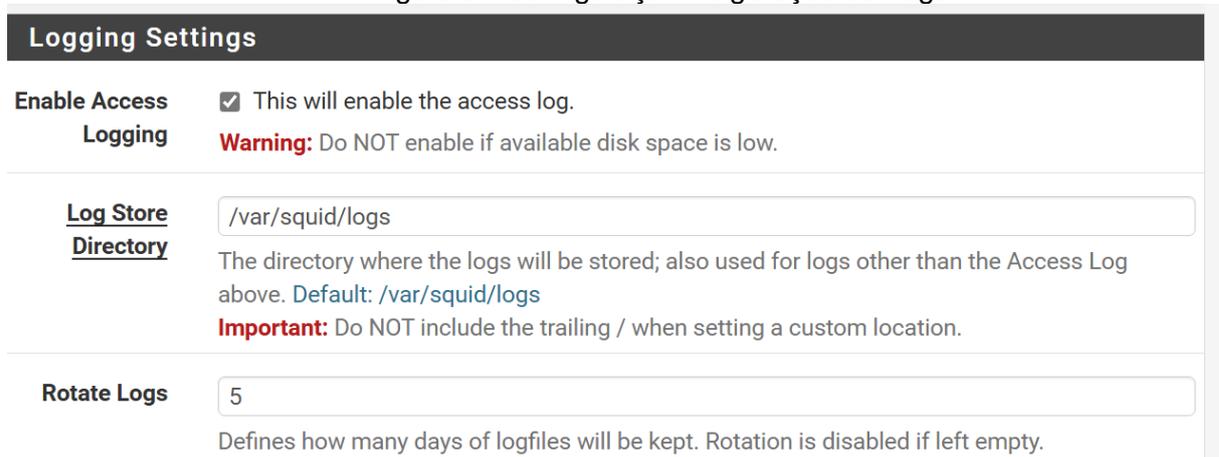
- Enable Squid Proxy:** Check to enable the Squid proxy. **Important:** If unchecked, ALL Squid services will be disabled and stopped.
- Keep Settings/Data:** If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. **Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
- Listen IP Version:** IPv4. Select the IP version Squid will use to select addresses for accepting client connections.
- CARP Status VIP:** none. Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. **Important:** Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.
- Proxy Interface(s):** WAN, LAN, OPT1_TESTE, loopback. The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
- Outgoing Network Interface:** Default (auto). The interface the proxy server will use for outgoing connections.
- Proxy Port:** 3128. This is the port the proxy server will listen on. Default: 3128.
- ICP Port:** (empty). This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
- Allow Users on Interface:** If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 9 - Configuração de geração de Logs



The screenshot shows the 'Logging Settings' configuration page for Squid. It includes three main sections: 'Enable Access Logging', 'Log Store Directory', and 'Rotate Logs'. The 'Enable Access Logging' section has a checked checkbox and a warning about disk space. The 'Log Store Directory' section has a text input field containing '/var/squid/logs' and explanatory text. The 'Rotate Logs' section has a text input field containing '5' and explanatory text.

Logging Settings	
Enable Access Logging	<input checked="" type="checkbox"/> This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	<input type="text" value="/var/squid/logs"/> The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs	<input type="text" value="5"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 10 – Configurando Proxy no Computador

Fonte: Autoria própria

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 própria

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.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Figura 12 - Configuração de bloqueio

Blacklist

```
*g1*  
*facebook*  
*youtube*
```

Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

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

The screenshot shows the Squid proxy interface with the 'Real Time' tab selected. The 'Filtering' section shows 'Max lines' set to 10 and 'String filter' set to 'TCP_DENIED'. Below, the 'Squid Access Table' displays a log of denied access attempts.

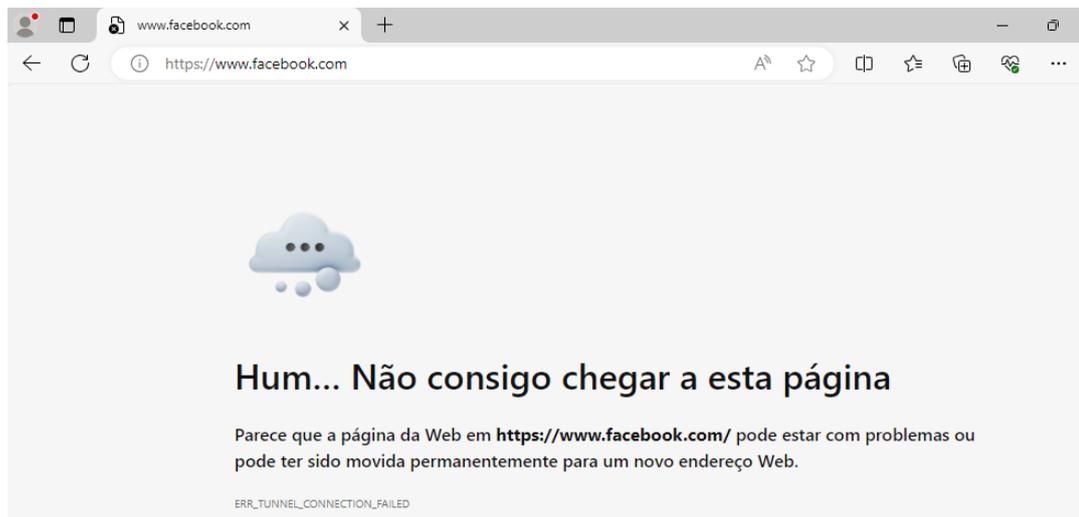
Date	IP	Status	Address	User	Destination
05.06.2024 00:51:40	192.168.50.13	TCP_DENIED/403	www.facebook.com:443	-	-
05.06.2024 00:51:40	192.168.50.13	TCP_DENIED/403	www.facebook.com:443	-	-
05.06.2024 00:51:35	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:35	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:35	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:35	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:34	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:33	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:33	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-
05.06.2024 00:51:33	192.168.50.13	TCP_DENIED/403	www.youtube.com:443	-	-

Fonte: Autoria propria

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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

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.