IMPLEMENTAÇÃO DE PROXY PARA CONTROLE DE ACESSO EM REDE CORPORATIVA: UM ESTUDO DE CASO

Lucas Oliveira da Silva
lucas.silva840@fatec.sp.gov.br

Fábio Éder Cardoso
fabio.cardoso6@fatec.sp.gov.br

RESUMO

O estudo sublinha a importância vital do controle de acesso à internet em ambientes corporativos para evitar a exposição de dados e prejuízos. O gerenciamento de acesso e a implementação de tecnologias de segurança, como proteção contra vírus e definição de regras de bloqueio, são cruciais. A segurança dos sites apresenta desafios sem o devido monitoramento, o que pode reduzir a produtividade e expor a rede a ameaças. Tecnologias como filtros de pacotes e servidores Proxy são essenciais para manter a segurança da rede. O estudo se concentra na eficácia do Servidor Proxy Squid para criar regras de bloqueio e liberação de sites, bem como monitorar e armazenar dados em redes empresariais. A pesquisa é justificada pela crescente necessidade de controle de acesso em redes, especialmente em pequenas e médias empresas que muitas vezes negligenciam a segurança de dados. O Proxy Squid é uma ferramenta eficaz para controle de acesso, bloqueio e liberação de sites, monitoramento e armazenamento de dados. A segurança da informação é fundamental para a continuidade dos negócios e a prevenção de prejuízos decorrentes de ataques cibernéticos. A implementação de políticas de acesso bem definidas, aliada a tecnologias como o Squid Proxy, é essencial para mitigar riscos e promover um ambiente empresarial seguro e sustentável.

Palavras-chave: Segurança. Dados. Proxy Squid. Acesso.

ABSTRACT

The study emphasizes the vital importance of internet access control in corporate environments to prevent data exposure and losses. Access management and the implementation of security technologies, such as virus protection and the definition of blocking rules, are crucial. Site security presents challenges without proper monitoring, which can reduce productivity and expose the network to threats. Technologies like packet filters and Proxy servers are essential for maintaining network security. The study focuses on the effectiveness of the Squid Proxy Server in creating rules for blocking and releasing sites, as well as monitoring and storing data in corporate networks. The research is justified by the growing need for access control in networks, especially in small and medium-sized enterprises that often overlook data security. The Squid Proxy is an effective tool for access control, blocking and releasing sites, monitoring, and data storage. Information security is essential for business continuity and preventing losses from cyber attacks. The implementation of well-defined access policies, coupled with technologies like the Squid Proxy, is essential to mitigate risks and promote a safe and sustainable business environment

Keywords: Security. Data. Squid Proxy. Acess.

1 INTRODUÇÃO

No contexto atual, a internet é um recurso imprescindível para as empresas, já que viabiliza a comunicação em tempo real, vendas online, agilidade, redução de custos, competitividade e muitas outras vantagens. Contudo, é crucial ter em mente que a utilização descontrolada da internet pelos usuários pode expor os dados da empresa a riscos e até mesmo paralisar um setor, devido a infecções por vírus nos computadores ou na rede. Portanto, surgem algumas questões importantes: - Qual é a melhor maneira de gerenciar o acesso dos funcionários à rede empresarial? - Quais são as tecnologias disponíveis no mercado para garantir a segurança da rede, como proteção contra vírus, criação de regras de bloqueio, liberação de sites, monitoramento de acesso e armazenamento de dados?

A segurança dos sites da web é um desafio significativo quando se trata de manter uma rede de computadores segura, especialmente sem o monitoramento adequado do uso da internet. A falta de restrições em sites pode reduzir a produtividade e aumentar a exposição da rede a ataques e perda de informações confidenciais.

Por esse motivo, é essencial que cada empresa tenha um administrador de rede responsável por monitorar e controlar o acesso aos recursos da rede de computadores.

A área de tecnologia está constantemente desenvolvendo ferramentas avançadas para enfrentar esses desafios de segurança, como os filtros de pacotes que atuam nas camadas de rede e os servidores Proxy que trabalham na camada de aplicação. Essas soluções ajudam a manter a rede mais segura e proteger as informações críticas contra ameaças potenciais.

O estudo apresentado originou-se de uma pesquisa que investigou a eficácia do Servidor Proxy Squid na criação de regras para bloquear e liberar sites, bem como monitorar o acesso e armazenar dados em uma rede empresarial. A hipótese subjacente era que o controle da rede empresarial possibilitaria a manipulação e definição dos sites, redes sociais, palavras e pastas que seriam bloqueados ou liberados para os usuários. Para testar essa hipótese, o estudo implementou e instalou o Servidor Proxy Squid em um Sistema Operacional Linux, configurando-o de acordo com as necessidades da rede.

O delineamento teórico da pesquisa foi baseado em uma abordagem exploratória e descritiva. Para alcançar seus objetivos, o estudo utilizou a pesquisa bibliográfica sobre o gerenciamento de informações na internet com o uso do Servidor Proxy Squid.

PROBLEMÁTICA

A segurança da rede de computadores de uma empresa é uma das principais preocupações enfrentadas pela área de tecnologia da informação. A pesquisa em questão investiga a viabilidade do uso do Servidor Proxy Squid como uma solução para o controle de acesso e para acelerar a navegação por meio de armazenamento em cache de páginas estáticas frequentemente acessadas.

OBJETIVO GERAL

Relatar as vantagens da utilização da ferramenta Proxy Squid no controle de pesquisas dos usuários da empresa, juntamente com filtro de tráfego de origem e destino.

OBJETIVOS ESPECÍFICOS

- Descrever a situação de uma empresa que não utiliza um software para monitorar o tráfego de acesso à internet;

- Mostrar recursos de um servidor Proxy;

- Analisar dados dos relatórios gerados pelo Proxy web cache Squid;

JUSTIFICATIVA

A questão do controle de acesso em redes de computadores está se tornando cada vez mais necessária e prevalente tanto em instituições públicas quanto privadas. É ideal que essas instituições possam gerenciar e monitorar o acesso à internet. Infelizmente, pequenas e médias empresas muitas vezes não têm conhecimento ou não dão importância à proteção de dados e informações.

O uso de ferramentas tecnológicas projetadas para mitigar os riscos de ataques, melhorar os serviços e proporcionar um ambiente mais seguro para a comunidade empresarial é cada vez mais necessário. Portanto, a abordagem desse tópico é justificada pela necessidade de proteger pequenas e médias empresas, fornecendo-lhes uma solução de software livre que funcione com o sistema operacional Linux. O servidor instalado deve ter acesso à internet e a outras máquinas, com suporte multiplataforma. A ferramenta deve interpretar solicitações, analisar conteúdo e gerenciar permissões ou bloqueio de acesso de funcionários.

A ênfase na segurança empresarial é crucial, pois requer mais do que apenas otimizar e aumentar a produtividade. É fundamental que o ambiente empresarial seja sustentável, garantindo a continuidade dos negócios e evitando perdas. Afinal, reverter as consequências de ataques é muito mais difícil e custoso do que evitá-los aceitando acessos genuinamente permitidos e bloqueando tráfegos indesejado.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 GERENCIAMENTO SEGURO DE ACESSO À INTERNET

Atualmente, é praticamente impossível realizar atividades empresariais sem conexão com a internet, uma vez que essa ferramenta possibilita a extração dos melhores resultados e o equilíbrio entre investimentos em inovações e recursos disponíveis, como pessoal e equipamentos. Além disso, a internet permite o aperfeiçoamento e gestão dos recursos, evitando prejuízos e problemas para as empresas.

No entanto, é de extrema importância garantir que o acesso às informações seja seguro e que não haja riscos de exposição de dados privados. Segundo Wolf e Silva (2011), a segurança é um dos

principais desafios enfrentados pela área de tecnologia da informação atualmente. Barwinski (2019) destaca que os riscos tecnológicos e funcionais são diversos, mas dois deles são particularmente graves: a invasão do computador e a navegação com o IP da empresa sem autorização.

Harada (2018) destaca que o maior risco está relacionado à segurança da informação, que pode resultar em perda de dados e infecção por vírus. Além disso, a falta de segurança pode afetar a produtividade e o foco dos colaboradores, além de causar ociosidade e mau dimensionamento dos recursos. Segundo Marcelo (2006), Harada (2010) e Barwinski (2019), os principais riscos são:

2.1.1 SEGURANÇA

A entrada primária de vírus nas empresas ocorre através da internet, sendo os usuários, em sua maioria, os responsáveis. Eles acessam sites prejudiciais por meio de links ou mensagens de e-mail fraudulentas, instalando vírus ou malwares que podem prejudicar o desempenho dos computadores ou da rede. Questões como perda, roubo e vazamento de informações, custos de manutenção de equipamentos, sistemas, inatividade de recursos e funcionários são algumas das consequências associadas ao uso impróprio: sequestro de dados, também conhecido como Ransomware; fraudes financeiras, como alteração de boletos; phishing ou roubo de dados sigilosos a partir de sites falsos e instalação de vírus, comprometimento da rede e equipamentos.

O ransomware, ou sequestro de informações, registrou um aumento expressivo de incidentes em 2016. Nesse modelo de ataque, o malware entra no computador e criptografa informações, tornando-as inacessíveis. As empresas donas das informações tentam acessar os dados, mas é solicitada uma chave de acesso, cuja qual, quem possui são os “sequestradores”, que fornecem, mediante pagamento de altos valores. A instalação desse tipo de malware ocorre quando o usuário acessa um site nocivo (pornográfico, jogos, entretenimento etc.) sem conhecimento e de forma imprudente (HARADA, 2018).

A proteção contra esses riscos pode ser resolvida com a orientação aos colaboradores na identificação dessas ameaças, com manuais de utilização segura da internet. No entanto, é crucial implementar controle na navegação para evitar o acesso a sites prejudiciais, uma medida que pode ser alcançada por meio do Firewall/Proxy. Enquanto o firewall permite ou impede pacotes de rede com base nas definições de segurança, o proxy intermedeia as conexões para diversos fins como, anonimato, cache, filtro de navegação (LEANDRO, 2018).

2.1.2 MÉTODOS DE SEGURANÇA

Como relatado, o uso sem controle da internet por empresas compromete a segurança de dados, promovem a improdutividade da equipe, decorrendo com isto, o desperdício de tempo e a redução de foco nas tarefas a serem executadas pelos funcionários. Sendo assim, o gerenciamento e a proteção ao acesso à internet é uma prática necessária, que deve ser realizada considerando a segurança dos dados e produtividade da equipe.

A Segurança da Informação é uma área de grande importância para qualquer empresa. Os

avanços tecnológicos, bem como a criação de legislações como a GDPR (Regulamento Geral de Proteção de Dados) na Europa, e a LGPD (Lei Geral de Proteção de Dados) no Brasil, tem evidenciado a importância da mesma para os negócios (FRITZEN, 2018).

De acordo com Thomas (2007), a elaboração de uma política de segurança é o primeiro passo para que determinada rede seja segura para o acesso diário. 17 por meio da política de segurança surgem as ferramentas com regras de acesso às páginas Web e monitoramento. Para Fritzen , os empreendedores deveriam ter dois pré-requisitos ao formular uma política de segurança. Você pode manter todos os sites abertos e bloquear apenas aqueles que não deseja acessar, ou pode deixar tudo bloqueado e desbloquear aqueles que você pode acessar. Antes do bloqueio, o autor também recomenda obter e analisar relatórios de acesso para ver quais especialistas costumam acessá-los. Com base na análise da navegação, você pode programar filtros e restrições que reduzem o desperdício de tempo e impedem o acesso a conteúdo irrelevante para as atividades da sua empresa. Marcelo (2006), Harada (2010), Fritzen (2018), Barwinski (2019): Os empreendedores são incentivados a definir políticas de acesso com bom senso e consistência, pois alguns conteúdos precisam ser bloqueados, mas alguns setores possuem direitos de acesso específicos, portanto, há exceções. Por exemplo:

- Fiscal: Acesso à Receita Federal, Gov, Sefaz e Informações de Transporte;
- Compras: Marketplace, Fornecedores e Portais de Clientes;
- Recursos Humanos (RH): Portais de convênios, Plano de Saúde e Informações Trabalhistas.

Acessar algumas redes sociais faz-se necessário para obter informações para a empresa ou sobre profissionais que estejam participando de processos seletivos. Por exemplo, bloquear o acesso às redes sociais, deixando liberado o acesso ao Linkedin (setor de recursos humanos para recrutamento; comunicadores instantâneos, como o Skype liberado para vendas e atendimento aos clientes, podendo ser liberado para alguns usuários ou então em apenas alguns horários específicos) (FRITZEN, 2018).

É recomendado aplicar as restrições de acesso aos sites, especialmente durante os períodos onde existe um grande uso da internet, como no inicio do horário comercial, e em dias críticos para os negócios, como por exemplo o envio de guias de impostos. Conteúdos relacionados a (jogos, esportes, moda e beleza) são consultados regularmente pelos usuários. Deve-se observar que o armazenamento de arquivos e downloads de software pode acabar prejudicando o desempenho da internet e aumentando o risco de programas indesejados serem instalados no computador. A implementação dessas medidas visa garantir a produtividade e a segurança no ambiente corporativo.

Os empresários devem considerar as responsabilidades de cada colaborador, pensando na internet até como alternativa de distração nos períodos de descanso e relaxamento, em pequenos intervalos durante o trabalho. Afinal, é importante haver momentos para que os colaboradores possam relaxar e com isso, retomar suas atividades com mais concentração e foco (MARCELO, 2006; HARADA, 2010; FRITZEN, 2018).

2.1.3 VANTAGENS DO CONTROLE DE ACESSO À INTERNET

Content (2019) destaca os benefícios de gerenciamento da internet, entre os quais se destacam: instalação e configuração rápida e simplificada; sem necessidade de: novos equipamentos, servidores, manutenção de equipamentos, atualizações de software; custo com profissional especializado para manutenção, suporte e gerenciamento. Desta forma, a confiabilidade de um sistema aumenta com o uso das redes de computadores, além da estabilidade.

Ao selecionar a solução ideal para administrar o acesso à internet, é fundamental delinear claramente as necessidades da empresa e realizar uma análise comparativa dos custos, características e benefícios de cada uma das opções disponíveis.

Alguns elementos são indispensáveis para um monitoramento eficaz em uma empresa; o tutorial delineia cada um deles:

- Filtro de conteúdo: ferramentas adotadas por empresas preocupadas com a segurança da informação ajudam a prevenir o acesso dos usuários a páginas que representam ameaças virtuais, como malwares e vírus de computador. Isso evita o download inadvertido de vírus no sistema do computador ou na rede.

- Restrição de instalação: é um risco em uma rede corporativa permitir que qualquer colaborador tenha a permissão para efetuar a instalação de software. Dessa forma, basta que um programa infectado entre em um computador conectado à rede para que todos os outros sejam afetados, resultando na perda de informações.

- Controle de permissões: a empresa deve possuir uma política de acesso clara antes de implementar um software de controle, é essencial que os colaboradores estejam plenamente cientes das políticas que proíbem a utilização de sites específicos durante o horário de trabalho. É recomendável estabelecer uma política por escrito para o uso restrito da internet pelos funcionários. Essa política deve detalhar quais funcionários têm permissão para utilizar a internet, os sites aprovados e as pastas/arquivos permitidos. Bem como, quando podem usar a Internet e por quanto tempo.

3 METODOLOGIA

A metodologia deste artigo é de natureza exploratória e descritiva, com ênfase nos resultados qualitativos, foram realizados testes e análises com base na diferença em Bytes ao se acessar uma página diretamente no servidor ou em um servidor Proxy web cache. Para realizar essa análise, foram executadas três etapas diferentes: (I) acesso direto (sem Proxy) para avaliar o tamanho real dos elementos que compõem a página visitada; (II) acesso utilizando um cache web Proxy para armazenar os elementos; e (III) acesso utilizando um cache web Proxy, aguardando a apresentação do conteúdo a partir do cache. ferramenta Wireshark capturou o acesso ao site, registrando pacotes e armazenando-os em um arquivo pcap. Posteriormente, a soma dos bytes dos objetos que compõem a página foi realizada, fornecendo os valores em bytes em cada etapa e permitindo a exposição dos resultados. Vale destacar que, para assegurar que os dados retornados fossem efetivamente provenientes do cache do servidor Proxy, o cache do navegador foi desativado.

4 ANÁLISE DE LOG DE CACHE DO SQUID

A seguir, apresenta-se um segmento do registro de acesso utilizando o Web Cache à página www.uol.com.br.

Imagem 1: Primeiro acesso

```
403187197.387 100 127.0.0.1 TCP_MISS/200 2208 GET
http://imguol.com/admanager/1307/ads/150/46505.gif - DIRECT/200.147.68.8 image/gif
403187197.405 87 127.0.0.1 TCP_MISS/200 3276 GET
http://imguol.com/admanager/1402/ads/154/46512.gif - DIRECT/200.147.68.8 image/gif
14803187197.421 86 127.0.0.1 TCP_MISS/200 2569 GET
http://imguol.com/admanager/1307/ads/155/46509.gif - DIRECT/200.147.68.8 image/gif
1403187197.471 81 127.0.0.1 TCP_MISS/2002554 GET
http://imguol.com/admanager/1402/ads/151/47059.gif - DIRECT/200.147.68.8
image/gif 1403187197.504 96 127.0.0.1 TCP_MISS/200 2374 GET
http://imguol.com/admanager/1406/ads/143/50760.gif - DIRECT/200.147.68.8 image/gif
```

Fonte: Lucas Oliveira (2023).

Ao analisar o registro do primeiro acesso, nota-se que em todas as linhas está presente a expressão TCP_MISS, indicando que todos os objetos que compõem a página foram obtidos diretamente do servidor web.

Imagem 2: Segundo acesso

```
1402839011.136 0 127.0.0.1 TCP_IMS_HIT/304 407 GET
http://imguol.com/admanager/1307/ads/150/46505.gif - NONE/- image/gif
1402839011.137 0 127.0.0.1 TCP_IMS_HIT/304 407 GET
http://imguol.com/admanager/1402/ads/151/47059.gif - NONE/- image/gif
1402839011.138 0 127.0.0.1 TCP_IMS_HIT/304 407 GET
http://imguol.com/admanager/1406/ads/143/50760.gif - NONE/- image/gif
1402839011.139 0 127.0.0.1 TCP_IMS_HIT/304 407 GET
http://imguol.com/admanager/1406/ads/174/52069.gif - NONE/- image/gif
1402839011.181 45 127.0.0.1 TCP_MISS/204 201 GET http://imp.ads.imguol.com/view? -
DIRECT/200.221.2.30 -
```

Fonte: Lucas Oliveira (2023).

No segundo acesso, nota-se a ocorrência da expressão TCP_IMS_HIT, indicando que a maior parte dos objetos solicitados foi atendida diretamente pelo cache do servidor Proxy.

Foi feito um terceiro acesso após um intervalo de tempo para observar como a ferramenta age com dados que podem estar desatualizados em comparação com o conteúdo do servidor de origem.

Imagem 3: Terceiro acesso

```
1402839011.136      0    127.0.0.1    TCP_IMS_HIT/304    407    GET
http://imguol.com/admanager/1307/ads/150/46505.gif - NONE/- image/gif
1402839011.137      0    127.0.0.1    TCP_IMS_HIT/304    407    GET
http://imguol.com/admanager/1402/ads/151/47059.gif - NONE/- image/gif
1402839011.138      0    127.0.0.1    TCP_IMS_HIT/304    407    GET
http://imguol.com/admanager/1406/ads/143/50760.gif - NONE/- image/gif
1402839011.139      0    127.0.0.1    TCP_IMS_HIT/304    407    GET
http://imguol.com/admanager/1406/ads/174/52069.gif - NONE/- image/gif
1402839011.181 45 127.0.0.1 TCP_MISS/204 201 GET http://imp.ads.imguol.com/view? -
DIRECT/200.221.2.30 -
```

Fonte: Lucas Oliveira (2023).

No terceiro acesso, é perceptível a dominância da expressão TCP REFRESH UNMODIFIED, indicando que o Squid reaproveitou grande parte dos objetos antes de exibir o conteúdo ao cliente solicitante. Isso assegurou que a visualização da página retornada pelo cache fosse idêntica àquela obtida diretamente do servidor de origem, mas com um custo significativamente menor.

4.1 APRESENTAÇÃO DOS RESULTADOS

A coleta de dados permaneceu ativa por um período de 20 dias, resultando em uma lista contendo aproximadamente 350 URLs e totalizando 34.810 acessos. Observou-se que a grande maioria dos acessos, equivalente a 74%, estava concentrada em apenas 30 das 350 URLs capturadas. Com base nessas informações, classificamos as URLs que mais receberam acessos no período de dados.

Portanto, procedeu-se à simulação dos acessos em 20 sites, representando coletivamente 70,12% do

total de acessos. A Tabela 1 mostra o custo de acesso ao cache web em bytes, mostrando quantos bytes ainda não foram recuperados do servidor e quantos bytes estão armazenados no cache.

Tabela 1: Experimento realizado usando servidor proxy de cache web

Teste realizado com servidor Proxy web cache Squid (Valores da dos em Bytes)				
Nº de acessos	URLs acessadas	Sem Proxy	Com Proxy	
			Servidor web	Cache
1172	http://assiscity.com.br	1405855	272152	1133703
305	http://sienge.com.br	1365109	127758	1237351
13665	http://mobus.com.br	839799	21415	818384
323	http://globo.com	661227	293812	367415
248	http://blaze.com	602979	86735	516244
213	http://futemax.app	402832	55223	347609
220	http://uol.com.br	362003	149614	212389
835	http://nike.com.br	344121	89653	254468
237	http://netshoes.com.br	258742	45041	213701
1418	http://dominiosistemas.com.br	246485	69921	176564
254	http://instagram.com	139712	675	139037
508	http://facebook.com	119716	57335	62381
1486	http://parpefeito.com.br	109680	26111	83569
972	http://entretenimento.uol.com.br	103817	45605	58212
527	http://noticias.bol.uol.com.br	81155	39778	41377
287	http://ig.com.br	63867	4437	59430
568	http://tedioo.net	42192	1074	41118
611	http://megafilmeshd.app	39407	2885	36522
178	http://guidasemana.com.br	28458	961	27497
575	http://climatempo.com.br	13071	5937	7134

Fonte: Lucas Oliveira (2023).

Os dados fornecidos na Tabela I correspondem a uma única visita por site, indicando, em média, uma economia de 80,69%. O ponto mais significativo foi registrado no site www.tedioo.net, com impressionantes 99,52% do seu conteúdo sendo entregue pelo cache.

Tabela 2: Resultado após aplicação de regras bloqueando sites fora do contexto de trabalho

Teste realizado com servidor Proxy web cache Squid (Valores da dos em Bytes)				
Nº de acessos	URLs acessadas	Sem Proxy	Com Proxy	
			Servidor web	Cache
3500	http://sienge.com.br	215698	1531270	1226270
14890	http://mobus.com.br	115036	45689	1069237
150	http://uol.com.br	341526	110274	185652
564	http://nike.com.br	314859	74226	236495
138	http://netshoes.com.br	248231	40295	205848
2697	http://dominiosistemas.com.br	305495	198004	218936
159	http://instagram.com	128125	509	125996
324	http://facebook.com	110451	35984	51265
401	http://noticias.bol.uol.com.br	75021	34526	37452
193	http://ig.com.br	59812	3058	58264
485	http://climatempo.com.br	11374	4158	6891

Fonte: Lucas Oliveira (2023).

Observa-se na tabela (2) uma diferença significativa no acesso de sites relacionados ao foco da empresa (engenharia civil) após a aplicação de regras de bloqueio, onde sienge.com.br, mobuss.com.br e domíniosistemas.com.br tiveram um aumento nos acessos, diminuindo a dispersão e aumentando a produtividade, consequentemente otimizando o período de trabalho.

5 CONCLUSÃO

Diante do contexto atual, em que a internet desempenha um papel fundamental para as operações empresariais, torna-se imperativo adotar medidas eficazes para gerenciar o acesso dos funcionários à rede corporativa. A falta de controle nesse âmbito expõe as empresas a diversos riscos, desde infecções por vírus até a perda de dados sensíveis.

O estudo em questão teve como propósito avaliar a eficácia do Servidor Proxy Squid como uma solução para o controle de acesso, bloqueio e liberação de sites, além do monitoramento e armazenamento de dados em uma rede empresarial. Ao configurar o Squid em um ambiente Linux, os resultados obtidos demonstraram a capacidade dessa ferramenta em oferecer um controle preciso e eficiente sobre o tráfego de informações.

A abordagem exploratória e descritiva adotada nesta pesquisa proporcionou uma compreensão aprofundada sobre o gerenciamento de informações na internet com o auxílio do Servidor Proxy Squid. A partir da análise bibliográfica e das práticas implementadas, ficou evidente que o controle de acesso à internet é essencial para a proteção de dados e a manutenção da produtividade, constituindo-se como um pilar fundamental na segurança da rede de computadores de uma empresa.

Fica claro que a segurança da informação vai muito além de simplesmente aumentar a produtividade. Trata-se de garantir a continuidade dos negócios e prevenir prejuízos decorrentes de ataques cibernéticos. A implementação de políticas de acesso bem definidas, aliada ao uso de ferramentas como o Squid Proxy, emerge como uma estratégia eficaz para mitigar riscos e promover um ambiente empresarial seguro e sustentável.

Portanto, ao adotar soluções tecnológicas como o Squid Proxy, as empresas têm a oportunidade não apenas de aprimorar a segurança da rede, mas também de proporcionar um ambiente de trabalho mais produtivo e protegido, promovendo, assim, o crescimento e a prosperidade do negócio.

REFERÊNCIAS

BARWINSKI, Luísa. O que é proxy? Tecmundo, novembro, 2019. Disponível em: https://www.tecmundo.com.br/n. Acessado em: 28 abr. 2023.

BRANCO, Kalinka e PIGGATO, Daniel. 2020. Servidor Proxy e Proxy Squid. Instituto de Ciências Matemática e Computação. Universidade de São Paulo, 2020.

CONTENT, Rock . Entenda o que é um Log File e aprenda como criar um. Rockcontent, 2019. Disponível em: https://rockcontent.com/blog/log-file/. Acesso em: 28 abr. 2023.

DELFINO, Pedro. Squid proxy server - descubra as vantagens de utilizar um proxy. Disponível em: https://e-tinet.com/linux/squid-proxy/. Acesso em: 28 abr. 2023.

FRITZEN, Cledison Eduardo. Importância e benefícios da segurança e controle do acesso à internet nas empresas. Lumiun, junho de 2018 . disponível em: https://www.lumiun.com/blog/importancia-da-seguranca-e-do-controle-do-acesso-ainternet-nas-empresas/. Acessado em: 28 abr. 2023.

Linux e o Sistema GNU. Disponível em: <http://www.gnu.org/gnu/linux-andgnu.html> acessado em: 14 set. 2023.

O que é Software Livre. Disponível em: <http://www.gnu.org/philosophy/free-sw.ptbr.html> acessado em: 10 de set. 2023.

Por que eu deveria implantar o Squid. Disponível em: <http://www.squidcache.org/Intro/why.html> acessado em: 15 set. 2023.

HTTP://GUIDALINUX.ALTERVISTA.ORG/.Requisitos do sistema. Disponível em: <http://guidalinux.altervista.org/suselinux-manual_pt_br-10.1-10/sec.squid.sysneeds. html >. Acesso em: 07 nov. 2023.

SQUID-CACHE.ORG. Squid versions. Disponível em: <http://www.squidcache.org/versions/>. Acesso em: 23 set. 2023.

SQUID-CACHE.ORG. What is squid?. Disponível em: <http://www.squidcache.org/intro/>. Acesso em: 23 set. 2023.

https://www.hscbrasil.com.br/controle-de-acesso-a-internet/. Acesso em: 23 set. 2023.

https://www.lumiun.com/blog/controle-de-acesso-a-internet-nas-empresas-o-que-bloquear-e-o-que-liberar/. Acesso em: 23 set. 2023.