FACULDADE ANTONIO MENEGHETTI - AMF
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

MARCELO PUNTEL

ANÁLISE E APLICAÇÃO DE UM MODELO DE POLÍTICA DE ACESSO À INTERNET EM AMBIENTE CORPORATIVO COM SOPHOS XG FIREWALL

RESTINGA SECA/RS
2019

MARCELO PUNTEL

ANÁLISE E APLICAÇÃO DE UM MODELO DE POLÍTICA DE ACESSO À INTERNET EM AMBIENTE CORPORATIVO COM SOPHOS XG FIREWALL

Trabalho de Conclusão de Curso-Monografia, apresentado como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação Curso de Graduação em Sistemas de Informação Faculdade Antonio Meneghetti-AMF.

Orientador: Prof. Esp. José Luiz Rodrigues Filho

RESTINGA SECA/RS
2019

MARCELO PUNTEL

ANÁLISE E APLICAÇÃO DE UM MODELO DE POLÍTICA DE ACESSO À INTERNET EM AMBIENTE CORPORATIVO COM SOPHOS XG FIREWALL

Trabalho de Conclusão de Curso-Monografia, apresentado como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação Curso de Graduação em Sistemas de Informação Faculdade Antonio Meneghetti-AMF.

Orientador: Prof. Esp. José Luiz Rodrigues Filho

COMISSÃO EXAMINADORA

Prof. Esp. José Luiz Rodrigues Filho
Orientador do Trabalho de Conclusão de Curso
Faculdade Antonio Meneghetti

Prof. Msª. Vanice Hentges
Membro da Banca Examinadora
Faculdade Antonio Meneghetti

Prof. Drª. Ana Marli Bulegon
Membro da Banca Examinadora
Faculdade Antonio Meneghetti

Recanto Maestro, 17 de novembro de 2019.

AGRADECIMENTOS

Gostaria de dar início aos meus agradecimentos, primeiramente gostaria de agradecer aos meus pais por me proporcionarem a oportunidade de estar cursando o ensino superior em uma instituição como a Antonio Meneghetti Faculdade e todo o apoio durante este período, meu muito obrigado Nilson Puntel e Erenilda Puntel.

Ao meu orientador, professor e grande amigo José Luiz Rodrigues Filhos, ao qual não mediu esforços para me ajudar, compartilhando seus conhecimentos e contribuindo sempre nessa jornada acadêmica, e profissional, fica a minha imensa gratidão.

A minha namorada Paola Maciel ao qual sempre esteve comigo, me apoiando e me ajudando.

Aos meus professores, que durante toda essa jornada acadêmica, dividiram seus conhecimentos, contribuindo para minha formação.

Aos meus colegas e amigos ao qual dividimos muitas das minhas noites durante esses 5 anos de faculdade.

Aos meus irmãos Márcio e Cátia Puntel, e a todos os meus familiares pelo apoio e carinho, obrigado.

Meu muito obrigado a todos os outros ao qual não foram citados, que colaboraram e colaboram de alguma forma nessa minha jornada acadêmica e profissional!

DEDICATÓRIA

*Dedico este trabalho aos meus pais que em todos os momentos me apoiaram e incentivaram minhas decisões, fornecendo uma base familiar sólida e com liberdade para seguir meu próprio caminho***.**

Epígrafe

“O insucesso é apenas uma oportunidade para recomeçar com mais inteligência”.

Henry Ford.

RESUMO

Os riscos de navegar na internet sem segurança é algo muito importante a se considerar nos dias atuais, tanto para o meio pessoal quanto profissional. Com o avanço da tecnologia e o acesso a qualquer hora ou de qualquer parte do mundo a qualquer tipo de conteúdo, pode trazer altos riscos para integridade dos dados das empresas, pois além de colaboradores utilizarem a internet de forma que não seja produtivo para o negócio, também trazem consigo o risco de terem informações e dados roubados por hackers, a partir de acesso a conteúdos impróprios e ataques de rede. Este trabalho traz como objetivo apresentar como o tempo improdutivo dos colaboradores utilizando a internet no ambiente empresarial é elevado e alertar sobre os perigos das redes de computadores e apresentar o porque é tão importante para uma empresa ou para si, a segurança da informação e seus dados. A pesquisa foi realizada utilizando o case de uma empresa que utiliza a Sophos XG Firewall, onde foram gerados gráficos de acesso e a partir dos dados de monitoramentos coletados implementado uma política de acesso WEB. Os resultados demonstram que o gerenciamento no controle de acesso à internet dos usuários é possível, sendo necessários realizar bloqueios de aplicativos que podem afetar a produtividade do negócio.

Palavras chaves: Firewall; Segurança da Informação; Políticas de acesso; Internet.

ABSTRACT

The risks of surfing the internet without security is very important to consider today, both for the personal and professional environment. With the advancement of technology and access to any type of content anytime or anywhere in the world, can pose high risks to the integrity of business data, as employees use the Internet in a way that is not productive for business. also carry the risk of hacking information and data from access to inappropriate content and network attacks. This paper aims to present how unproductive time employees use the internet in the business environment is high and warn about the dangers of computer networks and present why information security and data is so important for a company or for you. The research was conducted using the case of a company that uses Sophos XG Firewall, where access graphs were generated and from the collected monitoring data implemented a WEB access policy. The results demonstrate that managing Internet users access control is possible, requiring application locks that can affect business productivity.

Keywords: Firewall; Information Security; Access Policies; Internet.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS

XG - Next Generation (Sophos)

P2P - Peer-to-peer

HTTP - Hypertext Transfer Protocol

SSL - Significa Secure Sockets Layer

TCP - Transmission Control Protocol

IP - Internet Protocol

VPN - Virtual Private Network (rede virtual privada)

GB - GIGABYTE

TI - Tecnologia da informação

LAN - Local Area Network (rede local/interna)

WAN - Wide Área NetworK

UDP – User Datagram Protocol

WEB – World Wide Web

SUMÁRIO

1 INTRODUÇÃO

Como vivido no decorrer da história, o mundo tornou-se globalizado, a informação transcorre pelos mais diversos meios de comunicação, o uso de novas tecnologias, assim como modelos de negócios, fez com que facilmente toda e qualquer pessoa tenha acesso à informação em segundos e de qualquer lugar. Vivemos em uma era onde aquele que obtiver a capacidade de manipulação de dados e informação, seja pela sua disponibilidade, confidencialidade ou pela integridade, também terá o poder de manipular resultados, sociedade e negócios.

Nos dias atuais a dependência do acesso à informação através da tecnologia, principalmente pelas empresas quanto ao uso de suas tarefas cotidianas, pois com ela, muitos processos e tarefas são automatizados e feitos com mais velocidade e qualidade, porém junto a todos esses prós a tecnologia traz consigo novos riscos, que podem afetar diretamente nos objetivos, na integridade e lucro das empresas.

Através da disponibilização e do acesso à informação de qualquer lugar, ou seja, sem restrições geográficas ou temporais, traz consigo o aperfeiçoamento de personas não desejadas, por exemplo, hackers. Conforme Blockmon (2018) “um hacker, é qualquer pessoa que utiliza um sistema para acessar sem autorização um outro sistema de dados, ou que deixa o outro sistema indisponível, agindo assim com má intenção.” Um sistema pode permanecer horas inutilizado ou parado por meio de um ataque de invasão de rede ou pelo sequestro de dados.

> Os ataques podem acontecer por diversos motivos, dentre eles os acessos a sites impróprios e infectados por usuários com e sem intenção de acessar, ataques de rede e reconhecimento, onde dados de conhecimentos gerais são coletados, como por exemplo engenharia social e consultas na internet, assim como diversos outros tipos e classificações. (TRIPWIRE, 2019)

Com o intuito de agir diante destes ataques e infecções, surge a necessidade de utilizar uma ferramenta a esta atuação, como por exemplo, um filtro de rede e de pacotes, ao qual é possível monitorar todo o trânsito de dados de origem e destino, assim como a monitoração que segundo Blanchard (2015**)**, “monitorar a rede é necessário, pois o objetivo é manter as informações seguras através de alertas e notificações”. O uso da monitoração também permite que se estabelece parâmetros para este controle, onde também pode ser refletido em políticas de acesso.

Uma política de uso de internet garante que usuários e no caso de ambientes corporativos, colaboradores façam o uso da internet de forma mais eficaz, ou seja, sem perder tempo acessando suas redes sociais ou outros sites considerados improdutivos

para a empresa, que parte desta premissa. Além da otimização na produtividade outro ponto importante ao qual a política de acesso tem controle, é a segurança, que além de limitar o acesso a sites e recursos, também deve incluir etapas que minimizam os riscos causados por vírus, limitando o download para determinado usuário ou dispositivo.

O objetivo do controle de acesso é para passar aos funcionários, uma noção de responsabilidade maior, ao utilizar a internet ao ambiente de trabalho, fazendo com que entenda o valor dos dados possuídos no ambiente empresarial. Entretanto, não deve ser algo cercado por autoritarismo e proibições, pois elas podem ser facilmente burladas. Importante trazer que uma política de uso da internet seja mais uma ferramenta educativa para os colaboradores do que punitiva. (MARQUES, 2019)

Diante das considerações introduzidas acima, é possível questionar: Qual a eficácia da implementação de uma política de acesso à rede e internet em um ambiente corporativo, através de um comparativo entre antes e depois da aplicação de uma política de acesso sugerida?

1.1 PROBLEMA DE PESQUISA

Diante das considerações introduzidas acima, é possível questionar: Qual a eficácia da implementação de uma política de acesso à rede e internet em um ambiente corporativo?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Apresentar a análise e um comparativo do uso de uma política de acesso à rede e internet, em um ambiente corporativo utilizando como base uma ferramenta de filtro de rede, denominada Sophos XG Firewall.

1.2.2 Objetivo Específico

a) Sugerir uma política de uso de acesso à rede e internet utilizando o Sophos XG Firewall.
b) Através de uma política de acesso, manter a integridade, a disponibilidade e a confidencialidade das informações de posse da organização.
c) Apresentar soluções que com a utilização e configuração correta podem ajudar a empresa a atingir os seus objetivos.

d) Apresentar como as políticas de acesso interferem diretamente na produtividade de seus colaboradores.

1.3 JUSTIFICATIVA

A escolha do tema partiu, por um interesse pessoal e profissional do autor, que nos últimos anos se disponibilizou a estudar, se aprofundar e se certificar como arquiteto de segurança na ferramenta Sophos XG Firewall, pois acompanhando diariamente o fluxo de acesso à rede e internet de diversas empresas, nos mais variados segmentos, pode-se vivenciar muitas dificuldades ao qual podem comprometer a integridade dos dados produzidos e oriundos de uma empresa.

Esse trabalho visa estudar, identificar e apresentar alguns pontos onde empresas falham quanto à segurança da informação e o controle de acessos a rede e internet realizados em ambiente de trabalho, assim como chegar a um modelo de gestão para que as empresas possam utilizar de forma mais adequada a tecnologia da informação para impulsionar seus negócios.

2 FUNDAMENTAÇÃO TEÓRICA

2.1. REDE DE COMPUTADORES

As redes de computadores constituem-se de um conjunto de dois ou mais dispositivos interligados com o intuito de compartilhar dados e trocar informações entre si. As redes de computadores estão presentes no dia-a-dia das pessoas, como em empresas de grande porte e médias empresas, escritórios pequenos ou até mesmo em casa. (FRANCISCATTO e col., 2014)

A história das redes de computadores teve início na década de 60, onde a rede telefônica era a rede de comunicação que dominava o mundo. O desenvolvimento de microcomputadores de bom desempenho, com um número menor de requisitos rígidos de temperatura e umidade, permitiu a instalação considerável de poder computacional em diversas localizações, ao invés apenas uma determinada área, porém surgiu a necessidade de unir os mesmos para trocas de informações entre si. (FIGUEIREDO, 2013)

Apesar do custo alto dos computadores na época, com o surgimento da multiprogramação surgiu à necessidade de interligar computadores para que eles compartilham informações entre diferentes usuários e diferentes regiões.

O Departamento de Defesa dos Estados Unidos no final da década de 60, desenvolveu uma rede que interligava computadores. Ela foi chamada de ARPANET (Advanced Research Projects Agency Network). Esta rede serviu, a propósito militares. Era uma forma do governo norte-americano se proteger e garantir a fluência das comunicações.

No final dos anos 80 a ARPANET passou a ser chamada de INTERNET. Ao passar dos anos, muitas aplicações foram criadas, como serviços de Telnet, FTP, E-mail, etc., mas a grande revolução ocorreu em 1990, quando cientistas do CERN (Laboratório de Física na Suíça) criaram o WWW (World Wide Web). O WWW apresenta uma interface gráfica, muito mais amigável que a antiga interface texto. (FERNANDEZ, 2015)

A facilidade de utilizar diversas mídias juntas como texto, imagens, som, vídeo e a característica de se transferir para outra página, em qualquer lugar do mundo, com apenas um botão, tornou a internet acessível para qualquer pessoa, mesmo as que não tinham nenhum conhecimento de informática.

Segundo Andrei L. (2019), no ano de 1996 a internet era utilizada por mais de 15 milhões de usuários, já em 2010 passou para 1,6 bilhões de usuários, em 2019 temos mais de 3,9 bilhões de usuários conectados à internet. Inicialmente a Internet foi uma importante ferramenta para o meio acadêmico, mas hoje ela é essencial para as empresas e corporações.

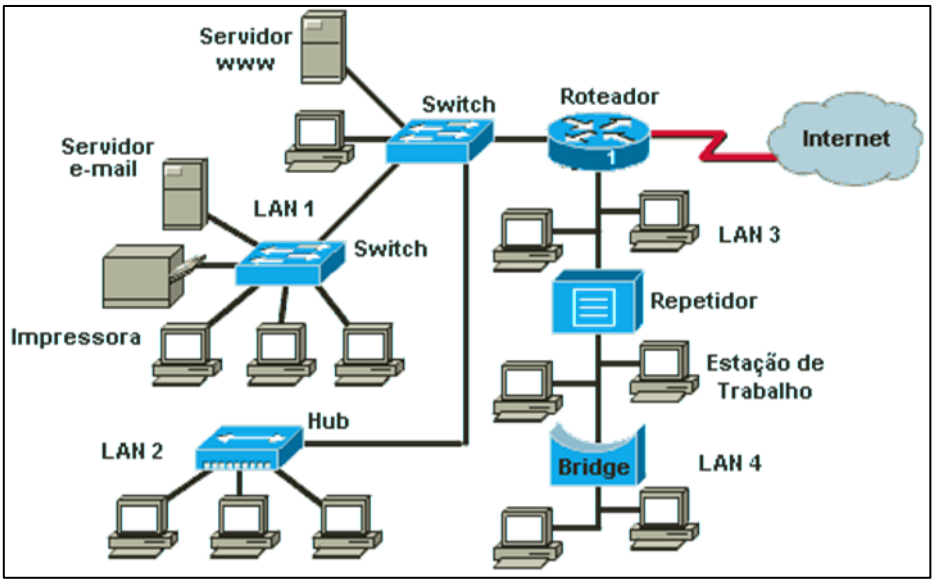
Uma rede de computadores é composta por diversos dispositivos, cada um com sua função, com o intuito de dar funcionalidade e organização e executar a comunicação entre os diferentes dispositivos de uma rede. Ao tratarmos de dispositivos de redes trazemos dois grupos principais: Ativos de rede e Passivos de Rede.

Como traz André Santos (2016), o grupo com componentes passivos é representado por fundamentos responsáveis pela condução dos dados por meio de um meio físico. Os equipamentos que funcionam com sinais e pulsos elétricos e não atuam com uma análise de dados. Dentre eles estão: Cabos Metálicos, Cabos Ópticos, Conectores Painéis de Conexão (Blocos, Patch Panel), Rack de Rede (Parede ou Piso), Voice Panel, e Extensores, etc.

Já dentro do grupo de ativos de rede e são os que analisam e dão ação no modo em como a informação passará pelo dispositivo, afetando diretamente o funcionamento dos sistemas. Estes são os encarregados de garantir a comunicação adequada servidor e clientes. Esses dispositivos garantem uma troca de informação confiável juntamente a

performance desejada pela aplicação. Como alguns exemplos temos Firewall (equipamento), chaveador KVM, conversores de Mídia, servidores, switches, Hubs, Bridges (Pontes), Modems, Roteadores, Placas de Rede; Access Points (Pontos de Acesso), etc. (SANTOS, 2016)

Figura 1: Escopo de rede uma rede de computadores e seus periféricos.



Fonte: Cultura Mix (2011).

2.1.1 Modelo OSI

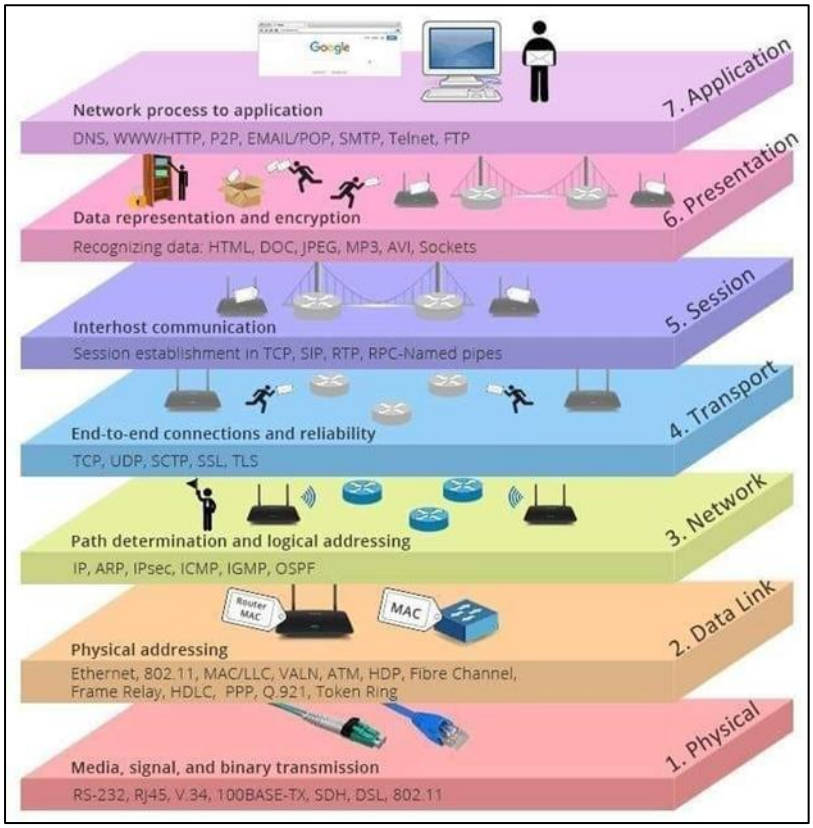
A Organização Internacional de Normalização (ISO) tem como objeto facilitar a padronização do processo e obter a conectividade entre dispositivos de vários fabricantes. Aprovada no início da década de 1980, esse modelo de arquitetura para sistemas abertos, trouxe como objetivo, permitir que máquinas heterogêneas se comunicassem entre si, definindo parâmetros genéricos para a construção das redes de computadores independente. (PINHEIRO, 2004)

Ele divide a comunicação da rede em sete camadas. Nesse modelo, as camadas 1 a 4 são consideradas as camadas inferiores e se preocupam principalmente com a movimentação de dados. As camadas 5 a 7, chamadas de camadas superiores, contêm dados no nível do aplicativo. As redes operam com um princípio básico: "repasse". Cada camada cuida de um trabalho muito específico e passa os dados para a próxima camada. (VENTURA, 2014)

No modelo OSI, o controle é passado de uma camada para a próxima, iniciando na camada de aplicativo (Camada 7) em uma estação e prosseguindo para a camada inferior, passando pelo canal até a próxima estação e fazendo backup da hierarquia. O

modelo OSI assume a tarefa de inter-rede e divide isso no que é chamado de pilha vertical que consiste nas 7 camadas a seguir.

Figura 2: Modelo OSI. Cisco Networks



Fonte: (FELIPPETTI, 2019)

2.1.2 Aplicação (camada 7)

A camada 7, chamada de camada de aplicação é onde tratamos a maioria dos protocolos, pelo simples fato de estar ligada aos usuários e por que cada usuário possui as suas necessidades.

Na camada 7 é onde disponibilizamos a interface onde o usuário tem a integração com as aplicações dos dispositivos, convertendo as diferenças entre diferentes fabricantes para uma tela. Por exemplo, ao transferir arquivos entre diferentes máquinas de diferentes fabricantes, onde pode ter convenções de nomes diferentes, formas diferentes de representar as linhas, etc. (PINHEIRO, 2014)

A transferência de um arquivo entre sistemas distintos requer uma forma de trabalhar com essas diferenças, essa função é realizada na camada de aplicação. Onde o dado é entregue pelo usuário até a camada de aplicação do sistema, e recebe a nomenclatura de SDU (Service Data Unit). Então a camada 7 denominada aplicação

junta a SDU um cabeçalho nomeado de PCI (Protocol Control Information). Então é resultado no PDU (Protocol Data Unit), ao qual corresponde à unidade dos dados especificado a um certo protocolo da camada em questão. (RAZA, 2018)

2.1.3 Apresentação (Camada 6)

A camada de apresentação é a que possui a função mais simples de toda parte do modelo OSI. Na camada de apresentação, ele trata com o processamento de sintaxe dos dados da mensagem, sendo conversões de formato e de criptografia ou descriptografia desejada para prestar suporte a camada de aplicação. (MITCHELL, 2019)

2.1.4 Sessão (Camada 5)

Essa camada tem o trabalho de manter uma comunicação adequada, estabelecendo, gerenciando e encerrando sessões entre dois computadores. Por exemplo, sempre que visitamos qualquer site, nosso computador precisa criar uma sessão com o servidor web deste site. (BAHL, 2018)

2.1.5 Transporte (Camada 4)

A camada de transporte disponibiliza os dados por meio de conexões de rede. O protocolo TCP é o exemplo mais claro de um protocolo da Camada de Transporte. Os diferentes protocolos de transporte podem suportar alto número de recursos opcionais, dentre eles o controle de fluxo, recuperação de erros e o suporte para a retransmissão. (MITHELL, 2019)

2.1.6 Rede (Camada 3)

A camada de rede fornece os meios funcionais e processuais para transferir sequências de dados de comprimento variável de um nó para outro conectado em "redes diferentes". A entrega de mensagens na camada de rede não oferece nenhum protocolo de camada de rede garantido e confiável.

Os protocolos de gerenciamento de camadas que pertencem à camada de rede são:

1. Protocolos de roteamento;
2. Gerenciamento de grupo multicast;
3. Atribuição de endereço da camada de rede.

2.1.7 Link de dados (camada 2)

No modelo OSI, camada 2, os pacotes de dados são codificados e decodificados em bits. Ele fornece conhecimento e gerenciamento de protocolo de transmissão e lida com erros na camada física, controle de fluxo e sincronização de quadros. A camada de enlace de dados é dividida em duas subcamadas: a camada MAC (Media Access Control) e a camada Logical Link Control (LLC). A subcamada MAC controla como um computador na rede obtém acesso aos dados e permissão para transmiti-los. A camada LLC controla a sincronização de quadros, controle de fluxo e verificação de erros. (OLIVEIRA, 2018)

2.1.8 Físico (Camada 1)

O modelo OSI, camada 1, transmite o fluxo de bits - impulso elétrico, luz ou sinal de rádio - através da rede nos níveis elétrico e mecânico. Ele fornece os meios de hardware para enviar e receber dados em uma transportadora, incluindo a definição de cabos, placas e aspectos físicos. Fast Ethernet , RS232 e ATM são protocolos com componentes da camada física. (BEAL, 1999 - 2019)

2.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um dos maiores bens de uma empresa e a evolução da tecnologia está permitindo que essa informação esteja disponível na maioria dos lugares.

Junto a essa informação temos também o risco, pois imagine se o seu e-mail, arquivos e sistema de uma empresa estejam à disposição de pessoas com segundas intenções? Nem sempre os gestores do negócio se preocupam com isso e muitas vezes acreditam que essa situação não deve ocorrer em suas empresas. Conforme destaca Laureano (2005) há o seguinte cenário atual:

> Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

Ainda nesse entendimento LAUREANO (2005) completa:

> As redes de computadores, mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas do que em sistemas fechados, assim como os riscos à privacidade e à integridade da informação. Portanto, é muito importante que mecanismos de

> segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e aos dados desses sistemas.

Como nos preocupamos com a segurança de qualquer outro bem físico de uma pessoa ou organização como carros e imóveis, temos que nos preocupar com o bem intangível que é a informação e que conforme vimos, pode ser inclusive de maior valor que os bens físicos dependendo do negócio da empresa. Para ajudar nesse problema, há uma área da tecnologia da informação especializada no estudo desse assunto, ela é chamada de Segurança da Informação. De acordo com (SÊMOLA, 2003), "podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Para que a segurança da informação possa ser reforçada nas empresas, é preciso atenção aos três pilares que sustentam a segurança em TI: confidencialidade, integridade e disponibilidade.

Cada um desses itens extrema importância para os processos de proteção de dados, sendo essenciais em qualquer política interna de Tecnologia da Informação voltada a garantir que os processos internos fluam corretamente.

2.2.1 Confidencialidade

O princípio de confidencialidade trata que todas as informações são obrigadas a permanecer fora de acesso ou ocultadas para os indivíduos e organizações que não têm permissão de acessá-las. Este princípio traz que é essencial as informações serem somente acessadas pelas pessoas que têm permissão. Portanto, todos os funcionários da empresa ou membros da organização devem estar cientes das responsabilidades que possuem em manter os dados disponíveis a eles confidenciais, tendo isso como parte do seu trabalho.

A confidencialidade é fácil de violar. Por exemplo, se um funcionário de uma organização permitir que alguém tenha um acesso a tela do computador, que no momento pode estar exibindo algumas informações confidenciais, ele pode já ter cometido uma violação da confidencialidade. (ROUSSEY, 2017)

2.2.2 Integridade

A integridade envolve manter a consistência, precisão e confiabilidade dos dados ao longo de todo o ciclo da vida. Os dados não devem ser alterados em trânsito e devem

ser tomadas medidas para garantir que os dados não possam ser alterados por pessoas não autorizadas (por exemplo, em uma quebra de confidencialidade). Essas medidas incluem permissões de arquivo e controles de acesso do usuário. Controle de versão usado para evitar alterações incorretas ou exclusão acidental por usuários autorizados, tornando-se um problema.

Além disso, alguns meios devem estar em vigor para detectar quaisquer alterações nos dados que possam ocorrer como resultado de eventos não humanos causados, como pulso eletromagnético (EMP) ou falhas no servidor. Alguns dados podem incluir soma de verificação, mesmo soma de verificação criptográficas, para verificação da integridade. Backups ou redundâncias devem estar disponíveis para restaurar os dados afetados para o estado correto. (ROUSE, 2014)

2.2.3 Disponibilidade

Para que todo e qualquer sistema, alcance seu objetivo, a informação contida precisa estar disponível quando for necessário o acesso. Isto significa que os todas as funcionalidades utilizadas nos sistemas de computação como os controles de segurança, o armazenamento, o processo de informações e seus canais de comunicação de acesso precisam estar funcionando.

Os sistemas com uma disponibilidade alta buscam estar sempre disponíveis, evitando interrupções no serviço devido a falhas de hardware, atualizações do sistema ou até falta de energia. Garantir a disponibilidade também envolve a prevenção de ataques de negação de serviço. (KEUNG, 2014)

2.3 SÉRIES ISO 27000

A série de padrões ISO/IEC 27000, também chamada de série ISO 27000, é uma série de práticas recomendadas para ajudar as organizações a melhorar a segurança de suas informações.

2.3.1 ISO 27001

Esse é o padrão central da série ISO 27000, contendo os requisitos de implementação para um Sistema de Gestão da Segurança da Informação (SGSI). É um dos pontos mais importantes pois a ISO 27001 é o único padrão da série em que as organizações podem ser auditadas e certificadas. Isso porque ele contém uma visão

geral de tudo que você deve fazer para obter a conformidade, que é expandida em cada um dos seguintes padrões. (IRWIN, 2019)

A ISO 27001 tem como foco proteger a confidencialidade, integridade e disponibilidade da informação de uma organização. Isto é feito identificando quais são os potenciais problemas que podem ocorrer com a informação (avaliação de risco), e então após definir quais necessidades devem ser resolvidas para prevenir que os problemas ocorram (mitigação de risco ou tratamento de risco).

Desta forma, a principal ideia da ISO 27001 é baseada na gestão de riscos: descobrir onde os riscos estão, e então resolvê-los sistematicamente. (LEAL, 2013)

Figura 3: Estrutura do modelo OSI.

Fonte: (LEAL, 2013)

2.3.2 ISO 27002

A ISO/IEC 27002 é um agrupamento de práticas de controle que tem como objetivo auxiliar na aplicação de Sistema de Gestão da Segurança da Informação.

É recomendado que a norma utilize a ISO 27001 em conjunto, mas também pode ser vista de forma independente com o objetivo de aplicar boas práticas. Essa norma é a única da gestão em segurança que existem certificações profissionais.

2.3.3 ISO/IEC 27003

A ISO 27003 contém um conjunto de diretrizes para a implementação do SGSI. Como a norma 27001 disponibiliza apenas os requisitos, a ISO 27003 traz as informações mais detalhada do que se deve ser feito. (PALMA, 2018)

Entre as várias normas da série ISO 27000 as normas acima são as de mais importância, temos também ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27008, ISO/IEC 27009, ISO/IEC 27010, ISO/IEC 27011, entre outras.

2.4 TIPOS DE ATAQUE E AMEAÇAS DE REDE

2.4.1 Hacker e Cracker

Devido a popularização da internet muitos sistemas online, trouxeram consigo vulnerabilidades permitindo que pessoas com elevado conhecimento de determinadas tecnologias pudessem obter acesso a sistemas diretamente conectados à internet. Essas pessoas foram chamadas de hacker, conforme, abordado por Guilherme Marinho:

> [...] significa aquele que se dedica a conhecer e modificar aspectos internos de aplicativos, programas e redes de computadores. Muitos hackers são contratados por grandes empresas para testar seus dispositivos de segurança informática. Já o cracker é aquele que explora as atividades dos sistemas e da tecnologia da informação para a prática de delitos, é o hacker mal-intencionado.

Segundo Caetano (2018), Hackers são programadores com enorme qualificação em determinadas tecnologias, onde tem como objetivo localizar falhas de segurança e acessarem sistemas sem permissão e consentimento dos proprietários.

Os tipos de hackers são delineados de acordo com a intenção, da seguinte maneira:

White Hat (hacker ético): É o Hacker com especialidade em segurança da informação, onde auxiliam as empresas a localizar falhas existentes em seus sistemas. São conhecidos como “hackers do bem”.

Black Hat (hacker mal-intencionado): Os black hats as vulnerabilidades encontradas em sistemas para terem acesso a dados sigilosos, como senha, dados pessoais e dados bancários, etc. São citados por alguns autores como uma subcategoria de crackers. (ARIMURA, 2016)

Gray Hat: Realizam atividades ilegais de hackers para mostrar suas habilidades, em vez de obter ganhos pessoais.

Existem muitos tipos de ataques e ameaças de rede, como o vírus, malwares, corrupção de rede, sobrecarga, etc. Infelizmente, de alguma forma, quaisquer dispositivos que estejam conectados a internet estão vulneráveis à eles. Existem diversas maneiras de evitar cada um deles, e para isso é indispensável saber e entender quais são os tipos de ataques cibernéticos.

2.4.2 Backdoor Ataque

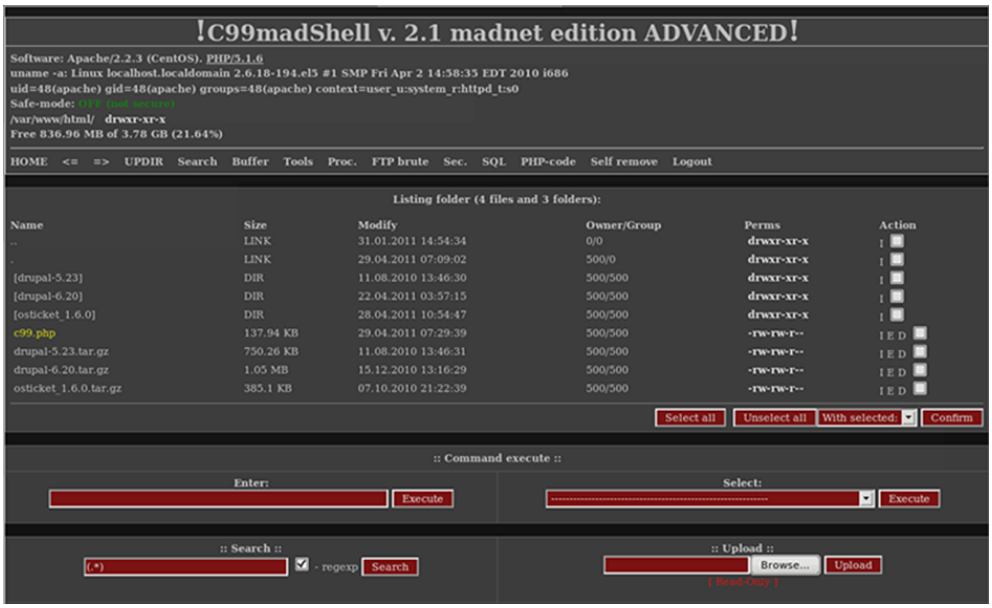
Um backdoor é um tipo de malware que consegue driblar os procedimentos normais de autenticação para acessar um sistema. Através dele, os hackers conseguem emitir comandos do sistema e atualizar o malware, remotamente. Esse acesso remoto é fornecido aos (pelos) recursos de um aplicativo, como banco de dados e servidores de arquivos.

Os hackers aproveitam os componentes vulneráveis de aplicativos da web para executar a instalação do backdoor. Em virtude dos arquivos serem altamente ocultos, torna-se difícil a detecção, uma vez que tenha sido instalado. (IMPERVA)

O backdoors do servidor da web é usado para diversas atividades maliciosas, como:

Roubo de servidor, desconfiguração do site, roubo de dados, entre outros.

Figura 4: Exemplo de um painel backdoor com recursos de execução de comando



Fonte: (IMPERVA)

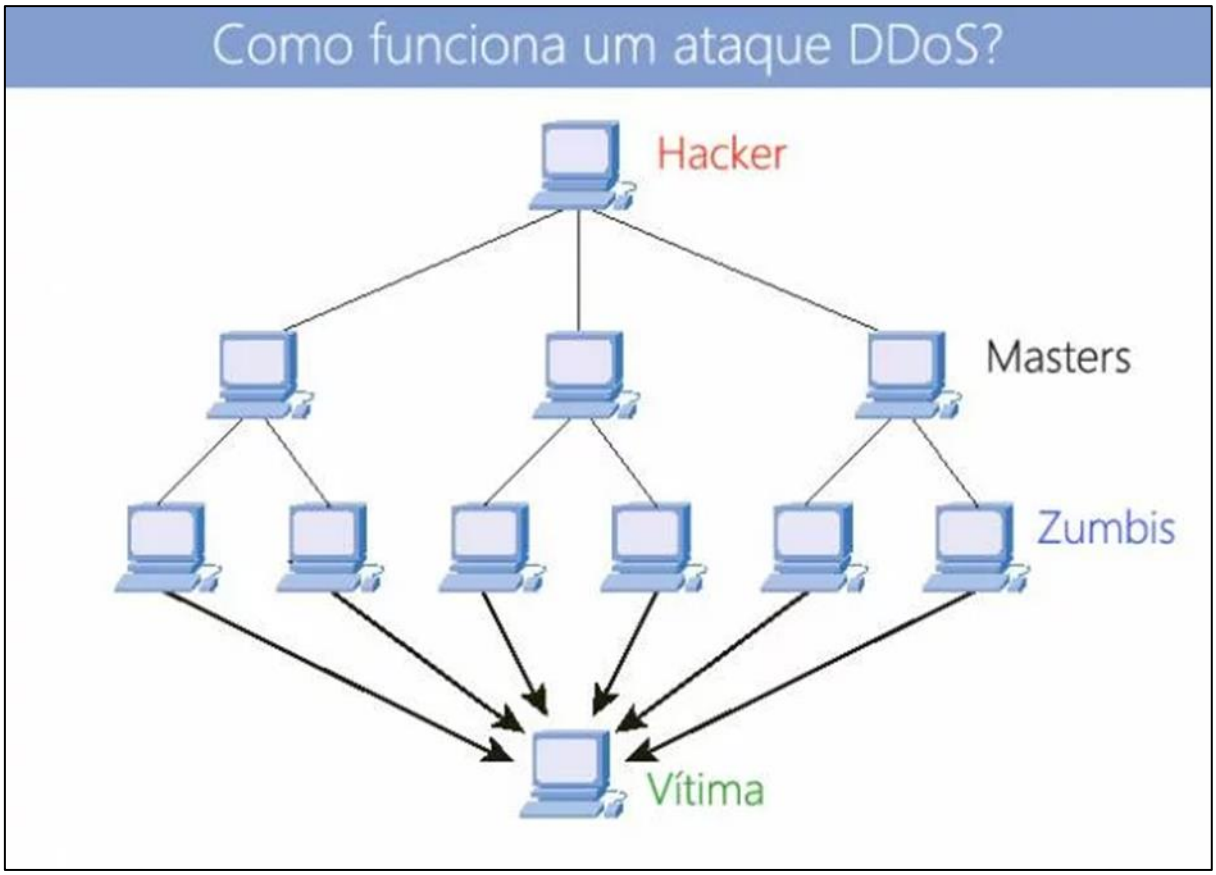
2.4.3 Ataque DDOS

O ataque distribuído de negação de serviço, conhecido como DDos, permite que um computador mestre consiga gerenciar milhões de computadores, chamados de “zumbis”.

Segundo a Canaltech (2017), por meio do DDoS, diversas máquinas são escravizadas e submetidas, ao mesmo tempo, a acessar um determinado recurso em um determinado servidor.

Tendo em vista que há um número limitado de usuários que podem ser acessados ao mesmo tempo nos servidores web, um grande tráfego pode inviabilizar que o servidor atenda a qualquer pedido, fazendo com que ele reinicie ou fique travado.

Figura 5: Funcionamento de um ataque DDoS



Fonte: CANALTECH (2017)

Existem alguns indicadores de que a máquina pode ser um zumbi: a internet lenta, mesmo que não haja a realização de várias tarefas simultâneas na rede; o computador enviando pacotes sem que o usuário acesse algum serviço na internet.

2.4.4 Ransomware

O Ransomware é um tipo de malware que limita o acesso a sistemas ou arquivos, cobrando um valor normalmente em Bitcoin para devolver o acesso. (CARDOSO, 2017). Exemplos conhecidos incluem o WannaCry, CTBLocker, CoinVault, CryptoWall e Bitcryptor.

Segundo a Malwarebytes (2018), o portal No More Ranson contém diversas ferramentas para desbloquear arquivos criptografados por esse tipo de ameaça. O portal foi lançado pela Unidade de Crime de Alta Tecnologia da Polícia Holandesa, European Cybercrime Centre (EC3) da Europol e duas empresas de cibersegurança – a Kaspersky Lab e a Intel Security.

Um utilitário chamado RanSim Ransomware Simulator, consegue simular ataques de Ransomware para verificar as defesas dos dispositivos contra diversas tipos de ameaça ameaças como: LockyVariant, Mover, InsideCryptor, Replacer, Streamer, StrongCryptor, StrongCryptorNet, ThorVariant e WeakCryptor (MALWAREBYTES, 2018). Depois de concluir os testes o RanSim apresenta quais são os arquivos seriam criptografados caso o ataque seja real.

2.4.5 Sniffing

É um processo que, por meio de ferramentas de Sniffing, consegue monitorar e capturar todos os pacotes que passam por uma determinada rede. (TACIO, 2011)

Caso um conjunto de portas de comutação de empresas esteja aberto, há uma grande chance de que seus funcionários conseguem farejar todo o tráfego da rede. Qualquer um pode conectar-se à rede por meio de um cabo Ethernet ou sem fio e farejar o tráfego total, desde que estejam no mesmo local físico. (GREYCAMPUS, 2018)

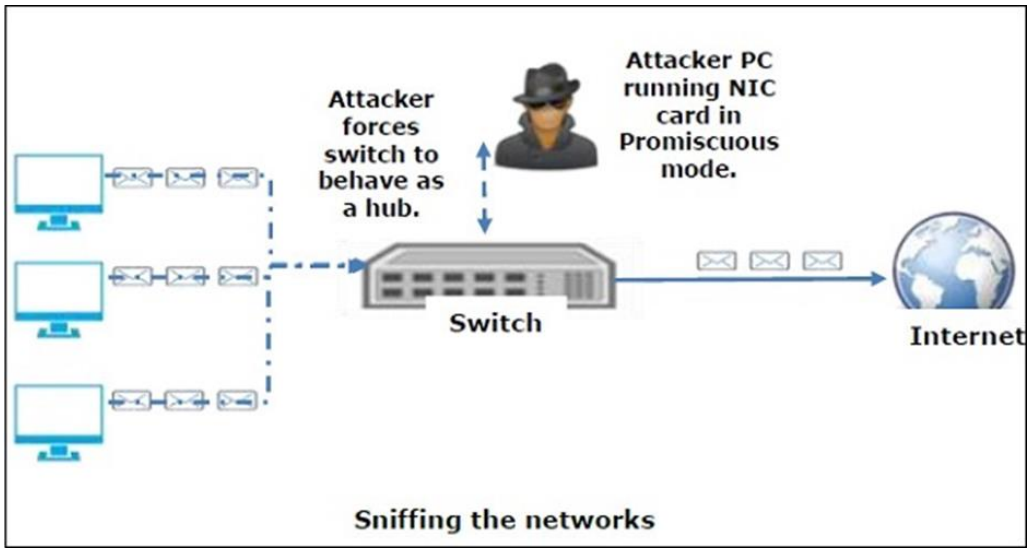
Em outras palavras, o Sniffing consegue visualizar todas as formas de tráfego na rede, sejam eles protegidos ou não. No ambiente correto e com o uso de protocolos verdadeiros em vigor, a parte responsável pelo ataque, é capaz de coletar as informações que serão utilizadas para realização de novos ataques e causar ainda mais problemas para o proprietário do sistema e rede. (TACIO, 2011)

Pode-se farejar as seguintes informações confidenciais de uma rede:

- Tráfego de e-mail
- Senhas FTP
- Tráfegos da Web
- Senhas de Telnet
- Configuração do roteador
- Sessões de chat

● Tráfego de DNS

Figura 6: Ilustração de como funciona um ataque Sniffing



Fonte: (MADEIRA, 2018.

Segundo a Verisign, todo o tráfego pode ser monitorado continuamente através da NIC, decodificando as informações dos pacotes de dados. Existem dois tipos de Sniffer, o passivo e o ativo.

•Sniffer Passivo: neste tipo de Sniffing o tráfego é bloqueado, mas não sofre alterações. O Sniffing passivo funciona com dispositivos Hub, nos quais o tráfego é enviado para todas as portas.

Diante disso, um invasor é capaz capturar facilmente o tráfego, pois em uma rede que usa hubs para conectar sistemas, todos os hosts na rede podem ver o tráfego. (VERISIGN, 2018)

Hoje, o Sniffing passivo já não é mais eficaz, visto que os hubs já estão quase obsoletos. A maioria das redes modernas utilizam switches.

• Sniffer ativo: nesse tipo de Sniffer, o tráfego não só é bloqueado e monitorado, como também pode ser alterado de alguma maneira, de acordo com o ataque. Ele detecta uma rede baseado em switch, e envolve a injeção de pacotes de resolução de endereços em uma rede de destino para inundar a tabela de memória endereçável por conteúdo. (VERISIGN, 2018)

As técnicas de Sniffing que estão ativas são: inundação de MACS, ataques DHCP, envenenamento de DNS, ataques de falsificação e envenenamento ARP. Os protocolos como TCP/IP não oferecem muita resistência à potenciais intrusos, pois foi

comprovado através de testes que eles nunca foram projetados tendo como base a segurança. (TACIO, 2011)

2.4.6 Varredura de portas

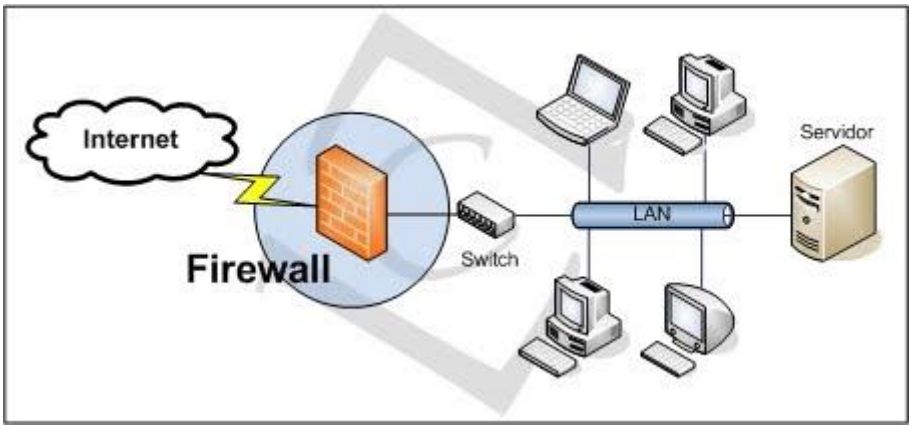
A varredura de portas é um modo de invasão que visa descobrir quais serviços estão sendo executados em forma de escuta, através do envio pacotes para todas as portas TCP e UDP de uma máquina. Sendo assim, é possível estabelecer qual sistema operacional e quais aplicativos estão sendo executados. (DUARTE, 2016)

Quando o administrador tem acesso para configurar os serviços que poderão ser visualizados , o XG Sophos consegue proteger, impedindo esse tipo de ataque.

2.5 Firewall

Um Firewall é uma ferramenta de segurança de redes que distribuído hardware ou software (mais comum) que a partir regras e políticas definidas pelo administrador de ti, verifica o tráfego de rede para analisar quais pacotes de envio ou recepção de dados podem serão aceitas para ser executadas. Traduzido firewall ao português temos como tradução literal de nome "Parede de fogo", e já deixa claro que o firewall se é tipo como uma barreira de defesa contra a rede. O seu objetivo, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejado e permitir somente o que foi definido em suas políticas e regras. (ALECRIM, 2013)

Figura 7: Escopo de um firewall.



Fonte: (CULTURA MIX, 2012)

O firewall garante que nenhum acesso à internet passe por você sem autorização. Apenas acesso definidos a partir de políticas de acesso. Se uma conexão de entrada não corresponder a nenhuma das configurações definidas pelo firewall ou não estiver

associada a um serviço aberto ao mundo externo, o acesso será bloqueado. Dessa forma, evitamos ataques, por exemplo, aqueles em que invasores tentam usar portas abertas para obter acesso a uma rede ou a um computador. (ECOIT, 2019)

Os firewalls são usados para proteger redes domésticas e corporativas. Um sistema típico de firewall filtra todas as informações que chegam pela Internet com destino à sua rede ou sistema de computador. (BEAL, 2014)

Segundo Mitchell Anicas (2015), existem três tipos de firewalls de rede: Firewall de filtragem de pacotes (sem estado), com estado e camada de aplicativo.

Os firewalls de filtragem de pacotes, ou sem estado, funcionam inspecionando pacotes individuais isoladamente. Como tal, eles não têm conhecimento do estado da conexão e só podem permitir ou negar pacotes com base em cabeçalhos de pacotes individuais.

Os firewalls com estado são capazes de determinar o estado da conexão dos pacotes, o que os torna muito mais flexíveis que os firewalls sem estado. Eles trabalham coletando pacotes relacionados até que o estado da conexão possa ser determinado antes que quaisquer regras de firewall sejam aplicadas ao tráfego.

Os firewalls de aplicativos vão um passo além, analisando os dados transmitidos, o que permite que o tráfego de rede seja comparado com as regras de firewall específicas para serviços ou aplicativos individuais. Eles também são conhecidos como firewalls baseados em proxy. (ANICAS, 2015)

Um Firewall em software é uma aplicação de segurança para os computadores. Os computadores de hoje, já vem com um firewall de software instalado por padrão. Utilizam um grupo de regras que fazem o controle do tráfego das informações do aparelho. Estas regras podem ser modificadas, aumentando ou diminuindo ainda mais a segurança do dispositivo. O Firewall pode ser tanto em hardware quanto em software. (BEAL, 2019)

Os firewalls de hardware podem ser adquiridos como um produto independente, mas, mais recentemente, os firewalls de hardware geralmente são encontrados em roteadores de banda larga e devem ser considerados uma parte importante do sistema e da configuração da rede, especialmente para qualquer pessoa em uma conexão de banda larga. Os firewalls de hardware podem ser eficazes com pouca ou nenhuma configuração e podem proteger todas as máquinas em uma rede local. A maioria dos firewalls de hardware terá no mínimo quatro portas de rede para conectar outros

computadores, mas para redes maiores, estão disponíveis soluções de firewall de rede comercial. (ALECRIM, 2019)

Um firewall de hardware usa filtragem de pacotes para examinar o cabeçalho de um pacote e determinar sua origem e destino. Essas informações são comparadas a um conjunto de regras predefinidas ou criadas pelo usuário que determinam se o pacote deve ser encaminhado ou descartado.

Vangie Beal (2019) complementa que como ou em qualquer equipamento eletrônico, um usuário de computador com conhecimentos gerais de computador pode conectar um firewall, ajustar algumas configurações e fazê-lo funcionar. Para garantir que seu firewall esteja configurado para segurança e proteção ideais, os consumidores sem dúvida precisarão aprender os recursos específicos de seu firewall de hardware, como habilitá-los e como testá-lo para garantir que ele faça um bom trabalho de proteger sua rede.

Nem todos os firewalls são criados iguais e, para isso, é importante ler o manual e a documentação que acompanham o seu produto. Além disso, o site do fabricante geralmente fornece uma base de conhecimento.

Para testar a segurança do firewall de hardware, você pode adquirir software de teste de terceiros ou pesquisar na Internet um serviço gratuito de teste de firewall online. O teste do firewall é uma parte importante da manutenção para garantir que seu sistema esteja sempre configurado para a proteção ideal. (TECMUNDO, 2010)

Já os Firewalls de software para usuários domésticos individuais, a opção de firewall mais popular é o firewall de software. Os firewalls de software estão instalados no seu computador (como qualquer software) e você pode personalizá-lo; permitindo a você algum controle sobre seus recursos de função e proteção. Um firewall de software protegerá seu computador de tentativas externas de controlar ou obter acesso ao computador e, dependendo da sua escolha de firewall de software, também poderá fornecer proteção contra os programas de Trojan e worms de email mais comuns. Muitos firewalls de software possuem controles definidos pelo usuário para configurar o compartilhamento seguro de arquivos e impressoras e bloquear aplicativos não seguros de executar no seu sistema. Além disso, os firewalls de software também podem incorporar controles de privacidade, filtragem da Web e muito mais. A desvantagem dos firewalls de software é que eles protegerão apenas o computador em que estão instalados, e não uma rede; portanto, cada computador precisará ter um firewall de software instalado. (TECMUNDO, 2010)

Como os firewalls de hardware, há um grande número de firewalls de software para escolher. Para começar, você pode ler as revisões dos firewalls do software e pesquisar o site do produto para obter algumas informações primeiro. Como o firewall do software sempre estará em execução no computador, anote os recursos do sistema necessários para a execução e as incompatibilidades com o sistema operacional. Um bom firewall de software estará em execução em segundo plano no seu sistema e utiliza uma pequena quantidade de recursos do sistema. É importante monitorar um firewall de software uma vez instalado e baixar as atualizações disponíveis do desenvolvedor. (BEAL, 2010)

2.5.1 Firewalls de próxima Geração - (NGFWs)

Um firewall de próxima geração (NGFW) entra na terceira geração das tecnologias de firewall disponíveis em software ou hardware, onde tem como objetivo barrar ataques de nível mais elevado, aplicando políticas de segurança e acessos, nos níveis de portas e dispositivos.

NGFWs normalmente apresentam funções avançadas, incluindo: conscientização de aplicativos, sistemas integrados de prevenção de intrusões (IPS), conscientização de identidade - controle de usuário e grupo, modos de ponte e roteado, e a capacidade de usar fontes externas de inteligência. (ROUSE, 2018)

Dessas ofertas, a maioria dos firewalls de última geração integra pelo menos três funções básicas: recursos de firewall corporativo, um sistema de prevenção de intrusões (IPS) e controle de aplicativos.

Assim como a introdução da inspeção de estado nos firewalls tradicionais, os NGFWs trazem um contexto adicional ao processo de tomada de decisões do firewall, fornecendo a capacidade de entender os detalhes do tráfego de aplicativos da Web que passam por ele e tomar medidas para bloquear o tráfego que pode explorar vulnerabilidades. (CARRION, 2018)

Os NGFWs combinam muitos dos recursos dos firewalls tradicionais - incluindo filtragem de pacotes, conversão de endereço de rede (NAT) e conversão de endereço de porta (PAT), bloqueio de URL e redes privadas virtuais (VPNs) - com a funcionalidade de qualidade de serviço (QoS) e outros recursos que não são encontrados nos firewalls tradicionais. Isso inclui prevenção de intrusões, inspeção SSL e SSH, inspeção profunda de pacotes e detecção de malware com base na reputação, além de conhecimento do aplicativo.

Esses recursos específicos de aplicativos tem como objetivo impedir o crescente número de ataques de aplicativos que ocorrem nas camadas 4-7 do modelo de rede OSI. (ROUSE, 2018)

Os diferentes recursos dos firewalls de última geração se combinam para criar benefícios exclusivos para os usuários. Os NGFWs geralmente conseguem bloquear o malware antes que ele entre na rede, algo que não era possível anteriormente.

Os NGFWs também estão melhores equipados para lidar com ameaças persistentes avançadas (APTs), porque podem ser integrados aos serviços de inteligência de ameaças. Os NGFWs também podem oferecer uma opção de baixo custo para empresas que tentam melhorar a segurança básica do dispositivo através do uso de reconhecimento de aplicativos, serviços de inspeção, sistemas de proteção e ferramentas de reconhecimento.

Margaret Rouse (2018) acredita que o NGFW e os firewalls tradicionais tenham o objetivo de proteger os ativos de rede e dados de uma organização, eles também têm várias diferenças.

As principais semelhanças incluem a filtragem estática de pacotes para bloquear pacotes no ponto da interface com o tráfego de rede. Ambos também têm a capacidade de fornecer inspeção de pacotes com estado, traduções de endereços de rede e porta, e podem configurar conexões VPN.

Uma das diferenças mais importantes entre os firewalls tradicionais e de última geração é que os NGFWs oferecem uma função de inspeção profunda de pacotes que vai além da inspeção simples de portas e protocolos, inspecionando os dados transportados em pacotes de rede. Outras diferenças importantes são que os NGFWs adicionam inspeção no nível do aplicativo, prevenção de intrusões e a capacidade de atuar nos dados fornecidos pelos serviços de inteligência de ameaças. (CARRION, 2018)

Além disso, os NGFWs estendem a funcionalidade tradicional de firewall do suporte a NAT, PAT e VPN para operar tanto no modo roteado - no qual o firewall se comporta como roteador - quanto no modo transparente - no qual o firewall se comporta como um coletor de informações quando verifica pacotes - enquanto também integra novas tecnologias de gerenciamento de ameaças.

Esses firewalls de última geração (NGFWs) foram criados para uma era diferente. Oito a dez anos atrás, as empresas ainda dependem amplamente da construção de um perímetro em torno da rede para bloquear malware. (ZURIER, 2017)

Chris Rodriguez, analista sênior da indústria na Frost & Sullivan que cobre o mercado de NGFW, afirma que não é mais uma estratégia abrangente.

"Um firewall é apenas um dos muitos sensores que as empresas podem lançar hoje", diz ele. "Um firewall não é um objetivo final. Ele deve trabalhar em conjunto com o gerenciamento de terminais e a análise de ameaças. É aí que as análises de big data e segurança se tornam importantes".

Hoje, as empresas administram redes em ambientes físicos e virtuais e os dados são executados na nuvem. Os funcionários também são mais móveis, portanto, o conceito de construir um fosso ao redor do perímetro não funciona mais. Os funcionários trabalham em todo o mundo, portanto, estão muito além do alcance dos tipos convencionais de firewalls no data center.

"As redes estão constantemente mudando na velocidade da inovação tecnológica", diz Samantha Madrid, chefe de marketing de produtos de segurança de rede da Palo Alto Networks. "É fundamental que sua segurança continue, para que não haja falhas na proteção".

"A automação e a integração são o que realmente é importante aqui", diz Madrid. "E da perspectiva do firewall, as empresas precisam garantir que seus firewalls possam ser executados em ambientes de nuvem pública e privada".

O malware para dispositivos móveis ganhou força e se tornou uma área de maior atenção, de acordo com Don Meyer, chefe de marketing de produtos de data center da Check Point Software Technologies. A plataforma Mobile Threat Prevention da empresa, que detecta aplicativos mal-intencionados em dispositivos iOS e Android, cria os mesmos recursos de detecção e prevenção de ameaças para dispositivos móveis que os NGFWs.

Meyer acredita que, embora os NGFWs ainda sejam relevantes, como eles se integram a outros recursos de detecção de ameaças e gerenciamento de pontos de extremidade faz toda a diferença. O software SandBlast Zero-Day Protection da empresa - que se integra aos seus firewalls - detecta e corrige ataques de dia zero e ameaças persistentes avançadas no nível da CPU, ou na fase de exploração, antes que os autores de malware possam empregar técnicas de evasão. (ZURIER, 2017)

Os firewalls não podem ser tratados como apenas um item da caixa de seleção em uma longa lista de compras de infraestrutura, diz Dave Stuart, diretor de marketing de produtos para segurança de rede da Cisco Systems. Em vez disso, eles precisam oferecer conhecimento contextual sobre infecções em potencial - não apenas alertando a

equipe de TI de que estão vendo ameaças, mas também informando se essas ameaças são prejudiciais. "O setor tem sido bom em proteger ameaças conhecidas. O que é necessário hoje são produtos que possam identificar ameaças desconhecidas", diz Stuart. (ZURIER, 2017)

De acordo com Esdrar Moreira (2016), são 5 itens que os melhores Firewall Corporativos deveriam ter, entre eles estão:

O controle unificado de aplicações, navegação web e usuários é necessário para que uma empresa além de descobrir a quem se destina cada tráfego que passa pela rede, também garanta que somente quem tem autorização, seja ela pessoa ou aplicativo autorizado tenham o acesso aberto ao destino. Por esse motivo é imprescindível que o firewall tenha um controle de gerenciamento unificado das políticas e filtros de acesso, baseados em: aplicações, filtros web e usuários.

Esse recurso permite ao administrador de TI gerenciar todos as políticas em um único lugar, oferecendo ao administrador facilidade e velocidade para criar, filtrar e classificar todas as políticas e regras da segurança da rede.

A camada humana da tecnologia, conta com políticas corporativas atuais que fecham a rede e formem diversas barreiras de segurança nas suas redes, porém diversas vezes esquecem o principal elemento da segurança e também o mais crítico e mais frágil: o humano. Pois a Segurança de uma organização deve ser tão forte quanto seu elo mais fraco – o usuário. (MOREIRA, 2016)

Para ser um bom firewall é preciso controlar os acessos dos usuários na rede, com a tecnologia de controle na camada 8, adicionada a partir de uma necessidade de monitorar e controlar a identidade humana de um usuário como um requisito de segurança em regras de firewall.

A camada 8 da tecnologia trata diretamente a identidade do usuário como uma camada humana em seus protocolos de rede. Permitidos aos gestores a identificar e tomar as devidas ações nas atividades destes usuários no uso da internet, permitindo a elaboração de relatórios específicos e detalhados de suas ações.

A visibilidade instantânea, onde administrador de rede necessita ter rápido acesso a tudo o que acontece com seu firewall, por isso esse equipamento deve exibir status em tempo real de desempenho de seu sistema, serviços, conexões e outros parâmetros.

Os itens precisam ser de fácil entendimento e clicáveis, e a cada clique revelando mais detalhes e informações. O painel principal necessita a fornecer diversas

ferramentas de monitoramento e status de rede para que o administrador utiliza para identificar problemas de forma rápida como: captura de pacotes, o acesso de linha de comando, ping, rotas, etc. (ALECRIM, 2018)

Segurança sincronizada: Hoje em dia os cibercriminosos tem seus ataques cada vez mais direcionados e perigosos do que nunca. Um firewall corporativo necessita estar apto a realizar a proteção do ambiente contra esses ataques e também novos ataques que podem a existir.

Um firewall necessita ter a integração sincronização com um antivírus corporativo. Estes recursos permitem que haja uma troca de informações e um controle mais agudo e detalhado sobre novas ameaças. Essa sincronia, oferece uma nova camada de proteção para a rede e seus dispositivos, fazendo com que o administrador de TI utilize menos tempo para resolver problemas relacionadas à segurança.

Gestão e proteção das redes wireless: Onde cada vez mais os ataques a redes wireless estão acontecendo. São mais de 18000 ataques registrados diariamente. Eles costumam ser executados por links de anúncio online, que direcionam os utilizadores para sites com scripts infectados, e tem como tarefa roubar as informações das vítimas e conseguir acesso remoto aos seus dispositivos. (ZURIER, 2017)

É necessário em um firewall gerenciar e monitorar todas as redes e antenas sem fio de uma empresa, por meio de um controlador na própria interface do firewall. Deve ser permitido ao administrador nesse painel a realizar configurações como: criar redes independentes, até mesmo isolar dispositivos que acessam a rede, e suportar diversos SSIDs por rádio, dentre eles SSIDS ocultos e encriptação. (MOREIRA, 2016)

2.5.2 A Sophos

A Sophos é uma fabricante de hardware e software no ramo da cibersegurança, incluindo entre seus principais produtos firewall XG, antivírus, antispyware, antispam, controle de acesso de rede, software de criptografia e prevenção contra perda de dados para dispositivos, servidores para proteção de e-mail e filtro para gateways de rede.

Fundada em 1985 pelo Dr. Jan Hruska e Dr. Peter Lammer, a Sophos é uma empresa privada com sede em diversos lugares ao redor do mundo entre eles Abingdon, Oxfordshire, Inglaterra e Burlington, Massachusetts, Estados Unidos. A empresa possui também escritórios na Austrália, Benelux, Canadá, França, Alemanha, Áustria, Itália, Japão, Singapura e Espanha. A empresa tem em média mais de 1.800 funcionários

espalhados por todo o mundo. Diferente de outras empresas da área de segurança, a Sophos mantém seu foco sempre no mercado empresarial. (SOPHOS, 2017)

A Sophos atende mais de 100 milhões de usuários em mais de 100 mil empresas, em 150 países. Diante da sua reputação nos quesitos de confiabilidade e inovação a Sophos é uma das empresas líderes quando se trata em Cibersegurança, estando entre as três principais empresas no Quadrante Mágico do Gartner.

As soluções criadas pela Sophos permitem que a empresa proteja a sua infraestrutura de rede, como computadores e servidores virtuais, do tráfego web mal intencionado, aos serviços de e-mail utilizados em aparelhos móveis, onde todos os dados de uma empresa podem ser mantidas longe de risco devido às ferramentas de alta performance e com atualizações regulares, oferecidas pela Sophos para estar sempre se protegendo contra novos tipos de ataques, e malware.

Nos dias atuais Sophos contém uma lista grande de clientes. Empresas de diversos setores fazem utilização das ferramentas de segurança digital oferecidas pela empresa fundada em Oxford, no Reino Unido. Entre os principais clientes estão: Pixar; Under Armour; Ford; Toshiba. (SOPHOS, 2017)

Tendo em vista que as soluções utilizadas pelas corporações mencionadas acima, são completas. Onde permite aos gestores implementar programadamente e gerir regras de firewall para a segurança de forma simplificada com um controle máximo e um baixo custo. Desse modo o negócio pode contar com um ambiente robusto e sempre confiável. (GIMENES, 2018)

2.5.3 Sophos XG Firewall

Para a realização deste experimento foi utilizado a ferramenta Sophos XG firewall, ao qual é um termo que se refere a uma única solução com diversos recursos embutidos. (SOPHOS, 2017)

O XG Firewall disponibiliza um gerenciamento completo e em tempo real da sua rede, e sua segurança, de forma que fique fácil o entendimento, oferecendo relatórios de acesso e quem os acessa e também qual o perigo que aquele tipo de acesso traz a sua rede. Apresenta um sistema um gerenciamento completo no controle de conteúdo a ser acessado dentro da empresa, que com apenas alguns cliques é possível bloquear ou liberar acesso a determinados sites.

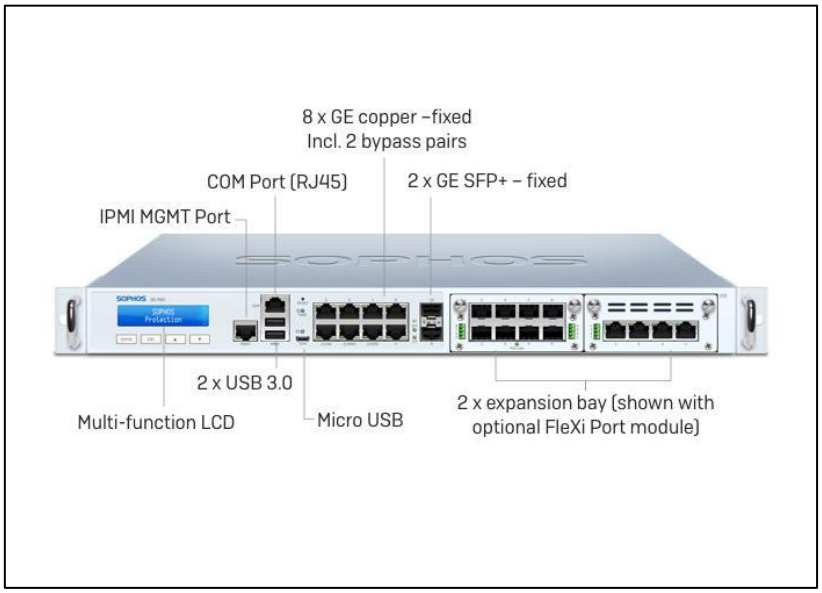
Dentre suas ferramentas de segurança, temos como principais o Sistema de Prevenção de Intrusão (IPS), que analisa o tráfego de tudo que é acessado dentro da rede

com o intuito de localizar e bloquear as explorações das vulnerabilidades do sistema. Outra ferramenta principal oferecida pelo Firewall XG é o Advanced Threat Protection (ATP), com o objetivo de capturar e identificar os dispositivos da rede comprometidas por ameaças avançadas que tenham passado dispersos pela segurança da rede, que ao detectar o tráfego com o perfil de tentativas de invasão, ou estações que tentam o mesmo notifica o administrador e realiza o bloqueio. (SOPHOS, 2017)

O firewall conta também com o serviço de VPN de diversas maneiras, disponibilizando conexões de clientes como aplicativos de conexão SSL, e também interligações entre unidades (IPSec). Junto a isso traz consigo um serviço de autenticação de rede, com integração com diversos servidores de autenticação como Active Directory.

A solução da Sophos é oferecida tanto e hardware como software, abaixo temos uma imagem de um dos modelos do Sophos XG Firewall

Figura 8: Modelo de Firewall Sophos XG 230 (SOPHOS)



Fonte: (SOPHOS, 2019)

2.5.4 Política de acesso

Uma política de uso da internet fornece aos funcionários regras e diretrizes sobre o uso apropriado dos equipamentos de acesso à internet no âmbito empresarial. Ter essa política em prática ajuda a proteger o negócio e o funcionário, pois o funcionário estará ciente de que a navegação em determinados sites ou o download de determinados arquivos é proibida e que a política deve ser respeitada ou que pode ter sérias

repercussões, levando a trazer maiores riscos de segurança para os negócios como resultado de negligência do funcionário. (GFI, 2015)

Com uma política de acesso mal definida os usuários podem ceder o acesso a rede a hackers com intenção de roubar e destruir os dados da empresa, fazendo com que o impacto no negócio seja de alto risco, pois uma empresa com seus dados vazados ou roubados além de multas ficam inoperantes deixando de produzir, causando um grande impacto no resultado final.

Para definir o que será bloqueado e o que será liberado para acesso na rede, deve se realizar uma análise nos conteúdos acessados pelas equipes, definindo a partir dessas diretrizes quais são os tipos de serviços e conteúdos necessários para as atividades na empresa, e quais fazem com que os usuários ficam dispersos. Antes de começar a bloquear os conteúdos é necessário identificar o que os colaboradores costumam acessar, e então a partir dessa análise definir as políticas de acesso à internet, para evitar que os bloqueios interfiram na produção das tarefas dos usuários.

Para definir uma política de acesso é necessário entender a coerência, pois há tipos de conteúdo que devem ser bloqueados inevitavelmente, mas de outro lado, temos alguns sites que precisam estar acessíveis a algumas pessoas, dependendo de setores, cargos ou horários específicos, de acordo claro com a responsabilidade de cada usuário, e também para um descanso e relaxamento durante intervalo dos usuários. (CEG INFORMATICA, 2019)

3 MÉTODO

Do ponto de vista de sua natureza, esta é uma pesquisa aplicada, que tem como proposta produzir conhecimentos e aplicar seus resultados para contribuir com a solução de um problema encontrado na realidade. (BARROS; LEHFELD, 2000, p.78)

Trata-se de uma pesquisa qualitativa, que tem como finalidade determinar conceitos e teorias de forma expressiva, utilizar adequadamente as técnicas de coleta de dados e analisar de forma específica e contextualizada todo o material pesquisado. (MINAYO, 2008)

Já na visão de seus objetivos, esta pesquisa caracteriza-se por uma pesquisa experimental, pois nela “determinamos um objeto de estudo, selecionamos as variáveis que seriam capazes de influenciá-lo, definimos as formas de controle e de observação dos efeitos que a variável produz no objeto”. (PRODANOV; FREITAS, 2013)

Para realizar essa pesquisa foi utilizado a ferramenta o XG firewall (Next Generation) da Sophos. O Sophos XG firewall oferece um gerenciamento completo e em tempo real de tudo que passa dentro de sua rede. Ele conta com acesso a relatórios em tempo real, podendo tomar diversas ações ao que está passando na sua rede. Este firewall possui um sistema de gerenciamento de políticas de acesso bem dinâmico e de fácil entendimento, o qual é possível bloquear e liberar acesso a qualquer tipo de conteúdo web.

Diante dos recursos providos por esta ferramenta, foram realizados comparativos em uma empresa X, com o intuito de visualizar a diferença do consumo de internet antes e depois das implementações de segurança e políticas de acesso no Firewall, sendo monitorado quais foram as aplicações e as categorias de acesso mais acessadas durante os dois períodos aplicados. No primeiro momento o Firewall ficou apenas em modo gateway do modo que possui todo o gerenciamento da rede, porém sem a aplicação de polícias de acesso, apenas monitorando e recolhendo as informações do que se era acessado, sem haver a implementação de nenhuma política de acesso.

Em um segundo momento foi aplicado às políticas de acesso, bloqueando sites como Facebook, Instagram, jogos online e outros conteúdos que não eram considerados produtivos para o horário e local de trabalho, apenas deixando liberado conteúdos categorizados como improdutivos para usuários específicos. A análise dos dados foi realizada utilizando o relatório desta ferramenta, onde foi realizado a comparação de quais foram os acessos antes e depois da aplicação de políticas de acesso no Firewall.

As políticas de acesso foram definidas a partir da apresentação de um primeiro relatório aos decisores da empresa, ao qual o firewall foi aplicado, tendo realizado os bloqueios e liberações conforme o indicado pelos mesmos.

3.1 ESTUDO DE CASO

Esse estudo foi realizado diante de um ambiente em produção de uma empresa, com mais de 15 unidades utilizando o firewall como gateway de navegação principal, com um número médio de 80 usuários utilizando simultaneamente.

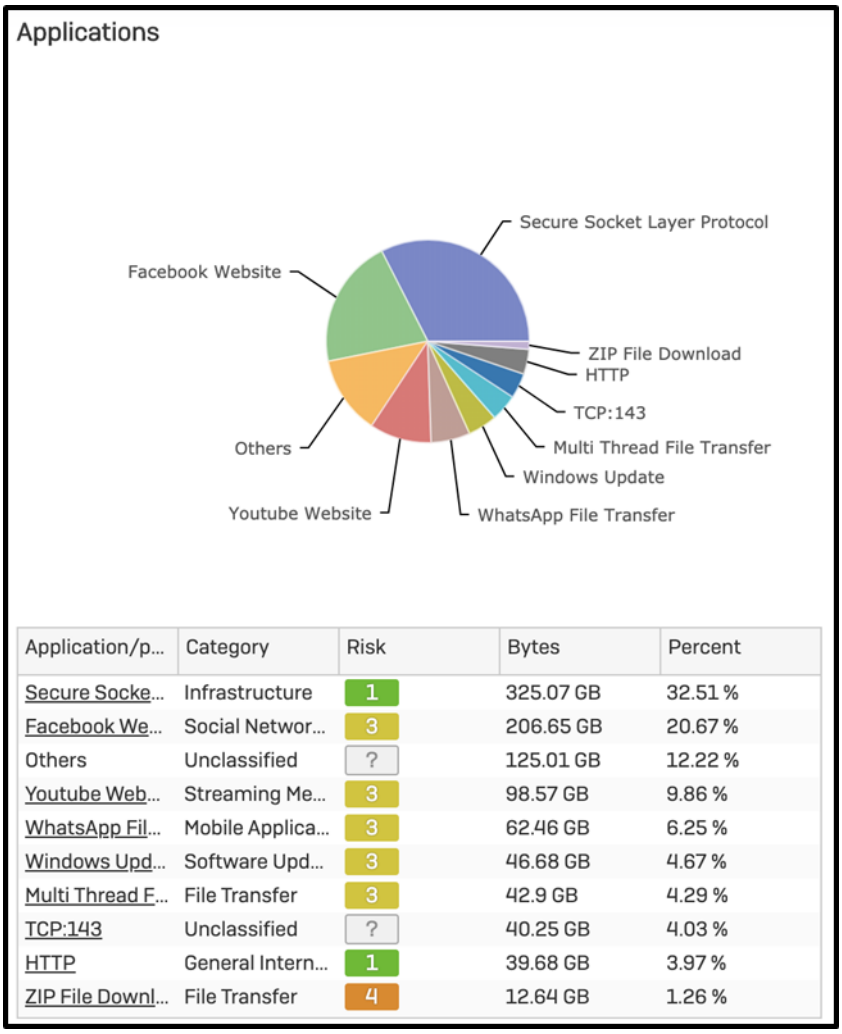
Neste primeiro relatório iremos visualizar o período de coleta de informações do equipamento, apenas monitorando tudo que era acessado no ambiente, para apresentar um relatório aos decisores do negócio e a partir das indicações, trabalhar em uma política de acesso, que não interfira no trabalho e produção dos colaboradores, e

também para trazer segurança e integridade para a rede e seus usuários, utilizando boas práticas de TI.

O relatório foi utilizado a partir da ferramenta de firewall da empresa Sophos, o XG Firewall, modelo XG 135 rev.3, versão 19.5 mr. 7.

Abaixo podemos visualizar os relatórios de acesso antes das políticas de acesso serem aplicadas na rede:

Gráfico 1: Aplicações mais acessadas antes da implementação da política de acesso

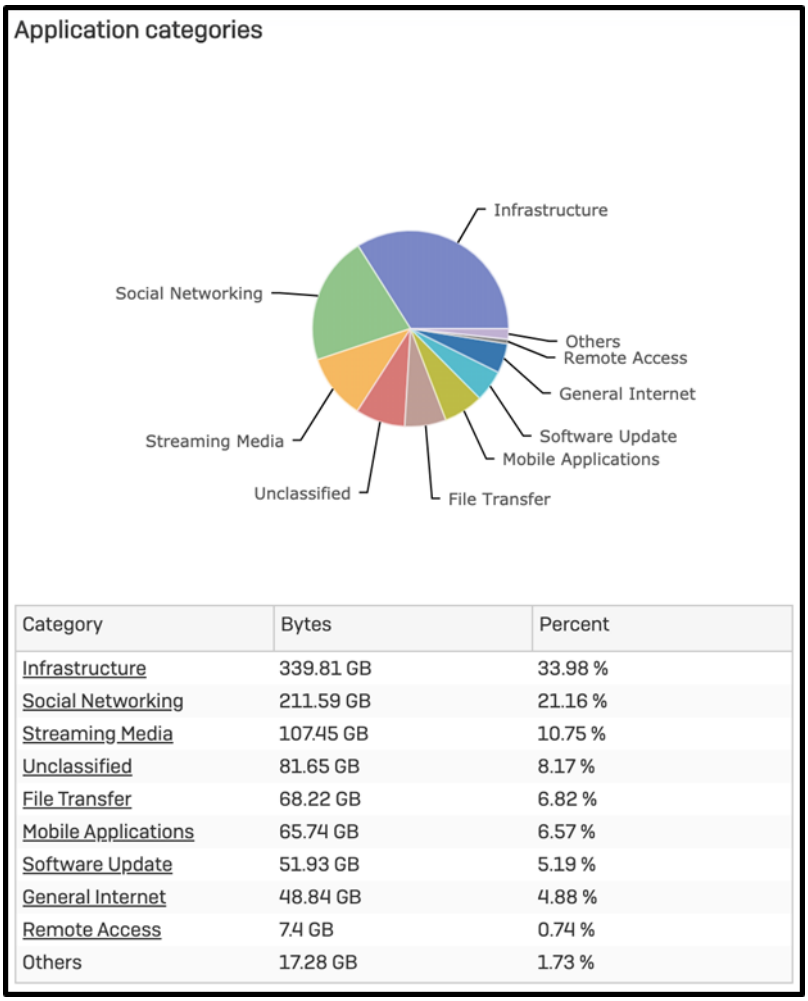


Application/p...	Category	Risk	Bytes	Percent
Secure Socke...	Infrastructure	1	325.07 GB	32.51 %
Facebook We...	Social Networ...	3	206.65 GB	20.67 %
Others	Unclassified	?	125.01 GB	12.22 %
Youtube Web...	Streaming Me...	3	98.57 GB	9.86 %
WhatsApp Fil...	Mobile Applica...	3	62.46 GB	6.25 %
Windows Upd...	Software Upd...	3	46.68 GB	4.67 %
Multi Thread F...	File Transfer	3	42.9 GB	4.29 %
TCP:143	Unclassified	?	40.25 GB	4.03 %
HTTP	General Intern...	1	39.68 GB	3.97 %
ZIP File Downl...	File Transfer	4	12.64 GB	1.26 %

Fonte: Elaborada pelo autor

Neste gráfico, é possível visualizar as aplicações mais acessadas, onde podemos verificar que temos como aplicação mais acessada o protocolo Secure Socket Layer (SSL), em seguida temos o Facebook com mais de 200 GB de acesso, seguido de Youtube, Transferência de arquivo de Whatsapp, e atualização do windows.

Gráfico 2: Categorias de aplicação mais acessadas antes da implementação da política de acesso

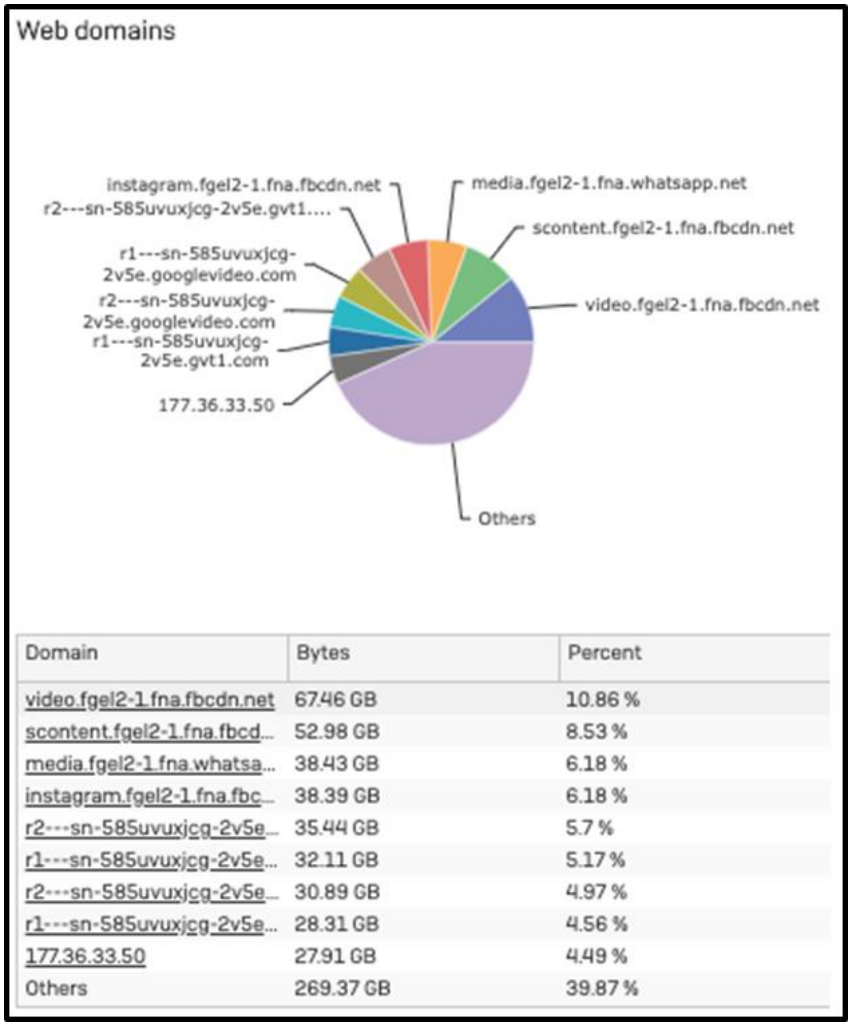


Category	Bytes	Percent
Infrastructure	339.81 GB	33.98 %
Social Networking	211.59 GB	21.16 %
Streaming Media	107.45 GB	10.75 %
Unclassified	81.65 GB	8.17 %
File Transfer	68.22 GB	6.82 %
Mobile Applications	65.74 GB	6.57 %
Software Update	51.93 GB	5.19 %
General Internet	48.84 GB	4.88 %
Remote Access	7.4 GB	0.74 %
Others	17.28 GB	1.73 %

Fonte: Elaborada pelo autor

Neste outro gráfico, é possível visualizar as categorias de aplicação mais acessadas, onde temos como categoria mais acessada infraestrutura, em seguida redes sociais com 211 GB de acesso, em seguida streaming media, Transferência de arquivo, em seguida aplicações móveis.

Gráfico 3: Domínios da web mais acessadas antes da implementação da política de acesso

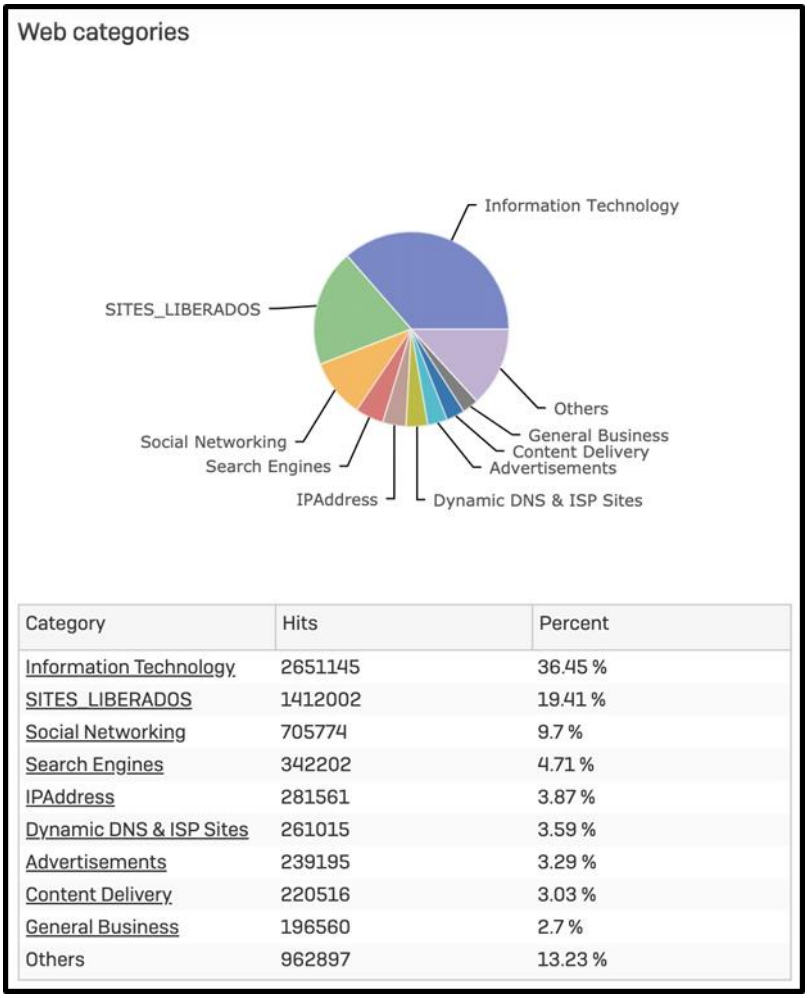


Domain	Bytes	Percent
video.fgel2-1.fna.fbcdn.net	67.46 GB	10.86 %
scontent.fgel2-1.fna.fbcd...	52.98 GB	8.53 %
media.fgel2-1.fna.whatsa...	38.43 GB	6.18 %
instagram.fgel2-1.fna.fbc...	38.39 GB	6.18 %
r2---sn-585uvuxjcg-2v5e...	35.44 GB	5.7 %
r1---sn-585uvuxjcg-2v5e...	32.11 GB	5.17 %
r2---sn-585uvuxjcg-2v5e...	30.89 GB	4.97 %
r1---sn-585uvuxjcg-2v5e...	28.31 GB	4.56 %
177.36.33.50	27.91 GB	4.49 %
Others	269.37 GB	39.87 %

Fonte: Elaborada pelo autor

No gráfico acima é possível visualizar os domínios de acesso Web com maior número, entre eles temos domínios do Facebook, Instagram e Whatsapp.

Gráfico 4: Categorias da web mais acessadas antes da implementação da política de acesso

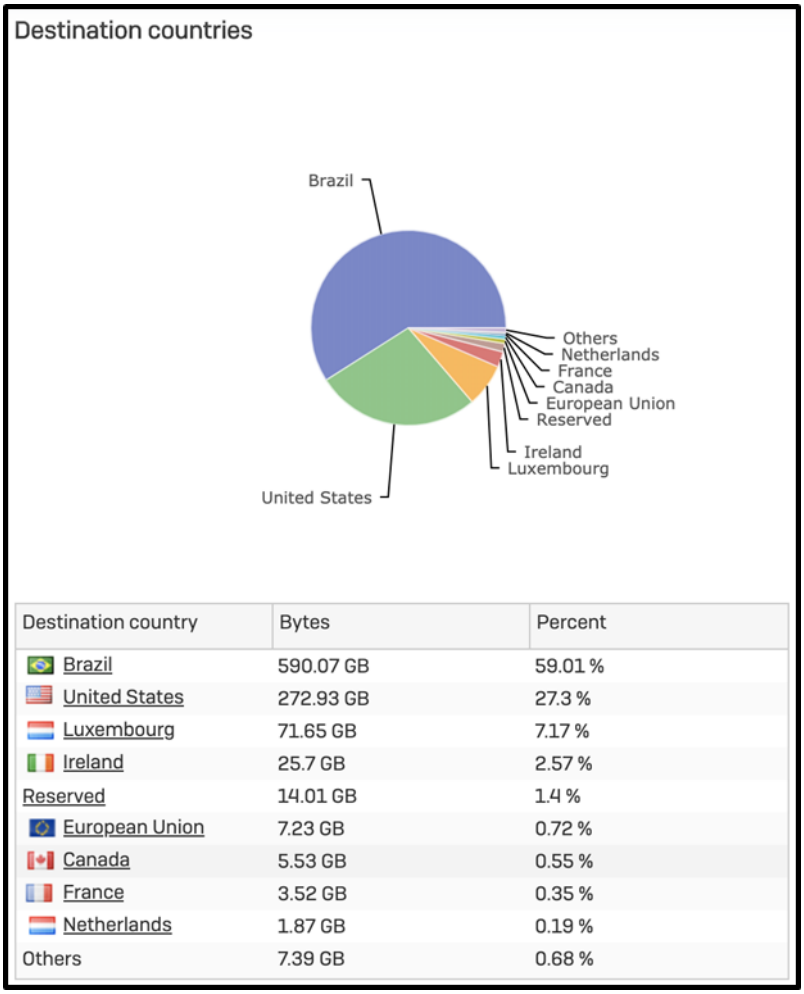


Category	Hits	Percent
Information Technology	2651145	36.45 %
SITES_LIBERADOS	1412002	19.41 %
Social Networking	705774	9.7 %
Search Engines	342202	4.71 %
IPAddress	281561	3.87 %
Dynamic DNS & ISP Sites	261015	3.59 %
Advertisements	239195	3.29 %
Content Delivery	220516	3.03 %
General Business	196560	2.7 %
Others	962897	13.23 %

Fonte: Elaborada pelo autor

No gráfico acima podemos visualizar as categorias de web mais acessadas, como principal categoria com mais de 35% de acesso temos a tecnologia da informação, em seguida sites liberados, como bancos e governo, seguido por redes sociais e mecanismos de busca.

Gráfico 5: Países mais acessados antes da implementação da política de acesso

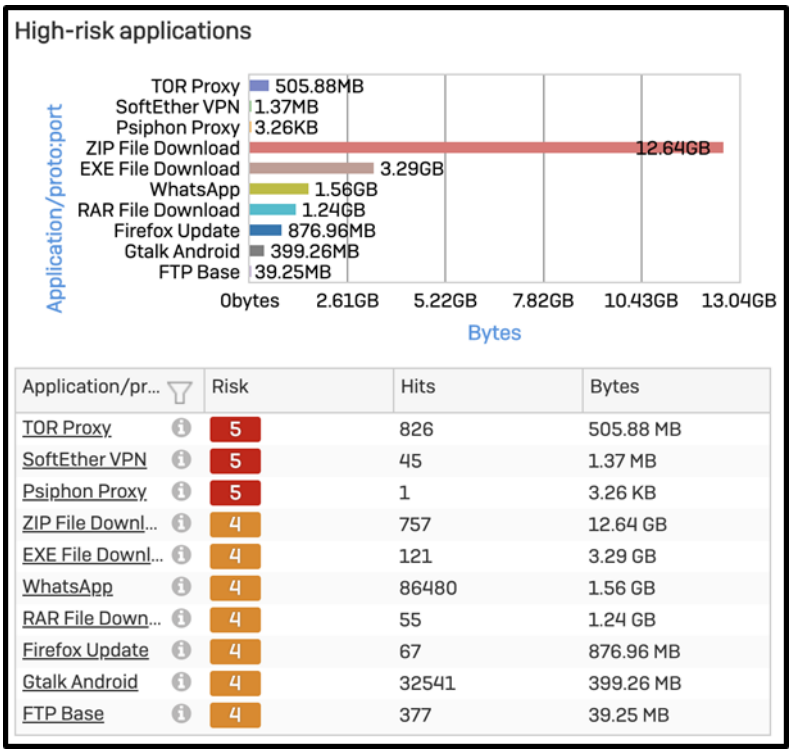


Destination country	Bytes	Percent
Brazil	590.07 GB	59.01 %
United States	272.93 GB	27.3 %
Luxembourg	71.65 GB	7.17 %
Ireland	25.7 GB	2.57 %
Reserved	14.01 GB	1.4 %
European Union	7.23 GB	0.72 %
Canada	5.53 GB	0.55 %
France	3.52 GB	0.35 %
Netherlands	1.87 GB	0.19 %
Others	7.39 GB	0.68 %

Fonte: Elaborada pelo autor

Neste outro gráfico é possível visualizar os países de destinos com maior número de acesso, tendo como principal país o Brasil, seguido pelos Estados Unidos e Luxemburgo.

Figura 9: Aplicações de alto risco

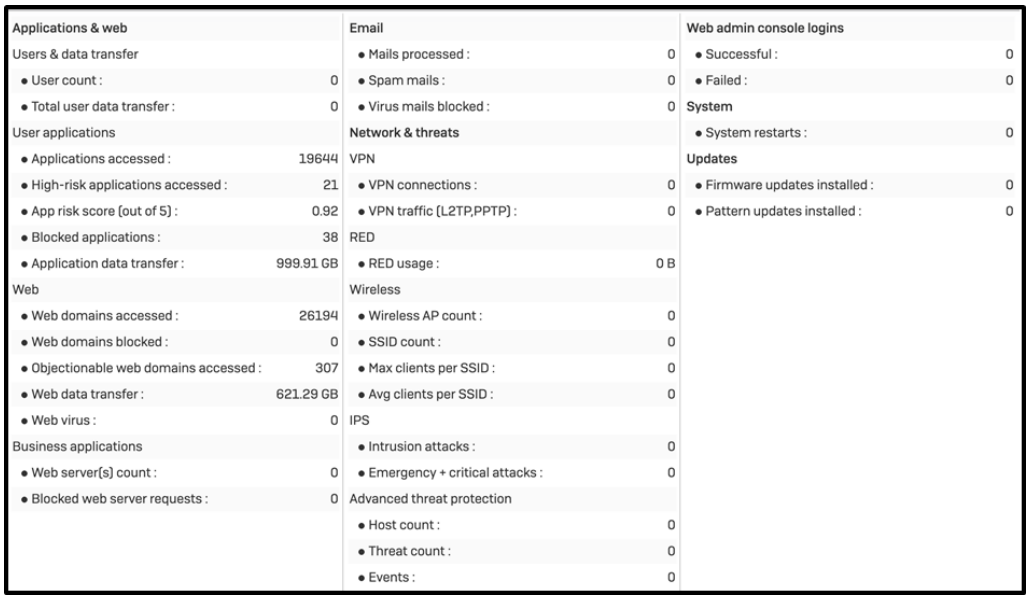


Application/pr...	Risk	Hits	Bytes
TOR Proxy	5	826	505.88 MB
SoftEther VPN	5	45	1.37 MB
Psiphon Proxy	5	1	3.26 KB
ZIP File Downl...	4	757	12.64 GB
EXE File Downl...	4	121	3.29 GB
WhatsApp	4	86480	1.56 GB
RAR File Down...	4	55	1.24 GB
Firefox Update	4	67	876.96 MB
Gtalk Android	4	32541	399.26 MB
FTP Base	4	377	39.25 MB

Fonte: Elaborada pelo autor

Esse gráfico traz as aplicações acessadas com maior risco para a rede, tendo o Proxy TOR como principal seguido de SoftEtcher VPN, Psiphon Prox, Download de arquivos zip, e de arquivos executáveis.

Figura 10: Relatório geral de acesso da rede



Applications & web		Email		Web admin console logins	
Users & data transfer		• Mails processed :	0	• Successful :	0
• User count :	0	• Spam mails :	0	• Failed :	0
• Total user data transfer :	0	• Virus mails blocked :	0	System	
User applications		Network & threats		• System restarts :	0
• Applications accessed :	19644	VPN		Updates	
• High-risk applications accessed :	21	• VPN connections :	0	• Firmware updates installed :	0
• App risk score (out of 5) :	0.92	• VPN traffic (L2TP,PPTP) :	0	• Pattern updates installed :	0
• Blocked applications :	38	RED			
• Application data transfer :	999.91 GB	• RED usage :	0 B		
Web		Wireless			
• Web domains accessed :	26194	• Wireless AP count :	0		
• Web domains blocked :	0	• SSID count :	0		
• Objectionable web domains accessed :	307	• Max clients per SSID :	0		
• Web data transfer :	621.29 GB	• Avg clients per SSID :	0		
• Web virus :	0	IPS			
Business applications		• Intrusion attacks :	0		
• Web server(s) count :	0	• Emergency + critical attacks :	0		
• Blocked web server requests :	0	Advanced threat protection			
		• Host count :	0		
		• Threat count :	0		
		• Events :	0		

Fonte: Elaborada pelo autor

Este relatório apresenta de forma resumida todas as informações sobre o que foi trafegado na rede, durante o período. Onde é possível verificar mais 999 GB de tráfego em transferência de dados em aplicações web, ainda 26194 domínios web acessado e 621 GB de transferência web.

Após a análise dos gráficos anteriores, e o levantamento do conteúdo acessado na rede, foi criado um modelo de política de acesso WEB para o ambiente empresarial, visando bloquear, o que for de conteúdo não produtivo para o negócio, seguido por decisões dos gestores da empresa, ao qual se foi coletado os dados.

O modelo de política WEB aplicada nesse ambiente foi o seguinte:

Este relatório apresenta de forma resumida todas as informações sobre o que foi trafegado na rede, durante o período. Onde é possível verificar mais 999 GB de tráfego em transferência de dados em aplicações web, ainda 26194 domínios web acessado e 621 GB de transferência web.

Após a análise dos gráficos anteriores, e o levantamento do conteúdo acessado na rede, foi criado um modelo de política de acesso WEB para o ambiente empresarial, visando bloquear, o que for considerado não produtivo, seguido por decisões dos gestores da empresa, onde os dados foram coletados.

Tomando como base a documentação do fabricante Sophos, o filtro de conteúdo web e suas respectivas descrições, onde foram utilizadas para sugerir uma política de acesso web. SOPHOS (2019)

Modelo de política WEB aplicada no ambiente descrito neste trabalho:

Categoria	**Descrição**	**Origem**	**Período**	**Protocolo**	**Ação**
Serviços Financeiros	Inclui site de bancos, e transações financeiras	Todos	Sempre	HTTP & HTTPS	Permitir
Governo	Inclui sites do governo	Todos	Sempre	HTTP & HTTPS	Permitir
Crime ativo	Inclui sites para instruir ou dar conselhos sobre a realização de atos ilegais;	Todos	Sempre	HTTP & HTTPS	Negar
Entretenimento	Inclui sites rádios, televisão, músicas e revistas	Todos	Sempre	HTTP & HTTPS	Negar
Jogos de azar	Inclui sites de jogos de azar on-line ou sites de loteria	Todos	Sempre	HTTP & HTTPS	Negar
Jogos	Sites para jogar ou baixar jogos	Todos	Sempre	HTTP & HTTPS	Negar
Hacking	Sites que fornecem instruções sobre atividades ilegais	Todos	Sempre	HTTP & HTTPS	Negar
Pirataria Intelectual	Sites de compartilhamento de conteúdos piratas	Todos	Sempre	HTTP & HTTPS	Negar
Áudio ao vivo	Sites com áudio ao vivo	Todos	Sempre	HTTP & HTTPS	Negar
Maconha	Sites com conteúdos relacionados a maconha	Todos	Sempre	HTTP & HTTPS	Negar

News	Sites de notícias em geral	Todos	Sempre	HTTP & HTTPS	Negar
Nudismo	Sites com conteúdos de nudismo	Todos	Sempre	HTTP & HTTPS	Negar
Peer to Peer & Torrents	Clientes de compartilhamento de arquivos peer-to-peer	Todos	Sempre	HTTP & HTTPS	Negar
Caça e pesca	Sites relacionados a caça e pesca	Todos	Sempre	HTTP & HTTPS	Negar
Plágio	Sites destinados a conteúdos de plágio	Todos	Sempre	HTTP & HTTPS	Negar
Pro suicídio e auto-dane	Sites que provém de suicídio e automutilação	Todos	Sempre	HTTP & HTTPS	Negar
Educação sexual	Sites relacionados à discussão sobre o uso da pílula	Todos	Sempre	HTTP & HTTPS	Negar
Sexualidade explícita	Sites para produtos adultos e brinquedos sexuais	Todos	Sempre	HTTP & HTTPS	Negar
Esportes	Sites destinados a materiais e conteúdos esportivos	Todos	Sempre	HTTP & HTTPS	Negar
Spyware e Malware	Sites com conteúdos categorizados como infectados	Todos	Sempre	HTTP & HTTPS	Negar

Fonte: Elaborada pelo autor

Junto ao modelo de política WEB mencionado anteriormente, também foi criado um modelo de política de acesso a aplicações, conforme a necessidade da empresa.

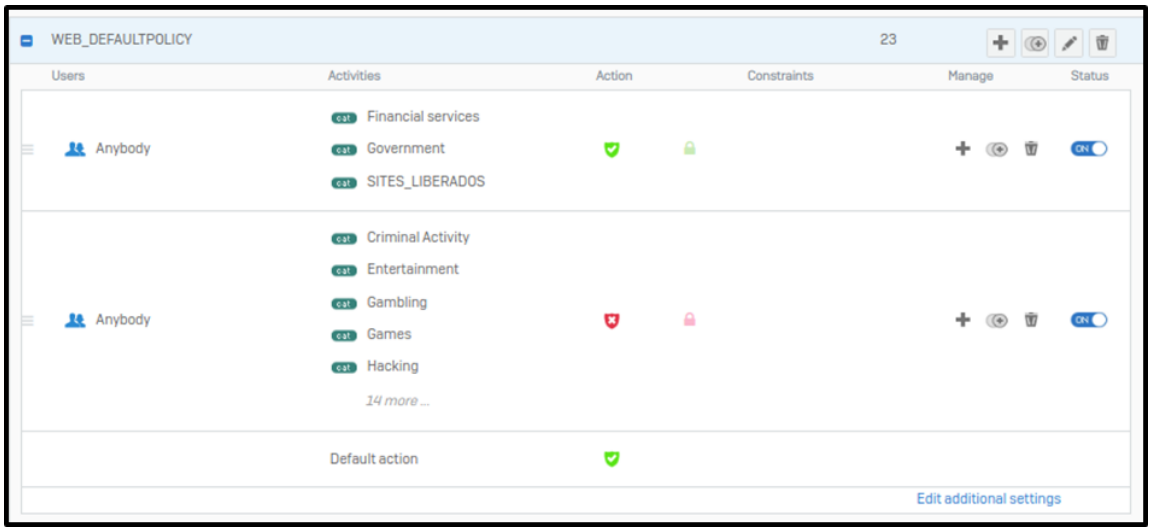
Categoria	Descrição	Quem	Período	Ação
Streaming Media	Aplicações que utilizam player para vídeos e músicas, como spotify, Netflix	Todos	Sempre	Negar
Yahoo	Aplicações do Yahoo	Todos	Sempre	Permitir
Youtube	Aplicações do Youtube	Todos	Sempre	Negar
Redes Sociais	Aplicações de redes sociais como facebook, instagram, twitter	Todos	Sempre	Negar
Jogos	Aplicações de jogos, como free fire, 8ball, entre outros	Todos	Sempre	Negar
Proxy e Túnel	Aplicações de VPN e proxy, para desvio de conexões	Todos	Sempre	Negar
P2P	Aplicações de alto risco para a rede como o torrent	Todos	Sempre	Negar

Fonte: Elaborada pelo autor

Após a coleta dessas informações foram realizadas as aplicações das políticas de acesso, definidas juntamente com os decisores da empresa. Após perceber o alto tráfego de acesso à internet, para conteúdos não produtivos do ponto de vista do negócio, foram realizados os seguintes bloqueio de acesso.

Para um bloqueio para o acesso geral de todos os colaboradores foram criadas as seguintes políticas WEB:

Figura 11: Política de acesso WEB Sophos XG



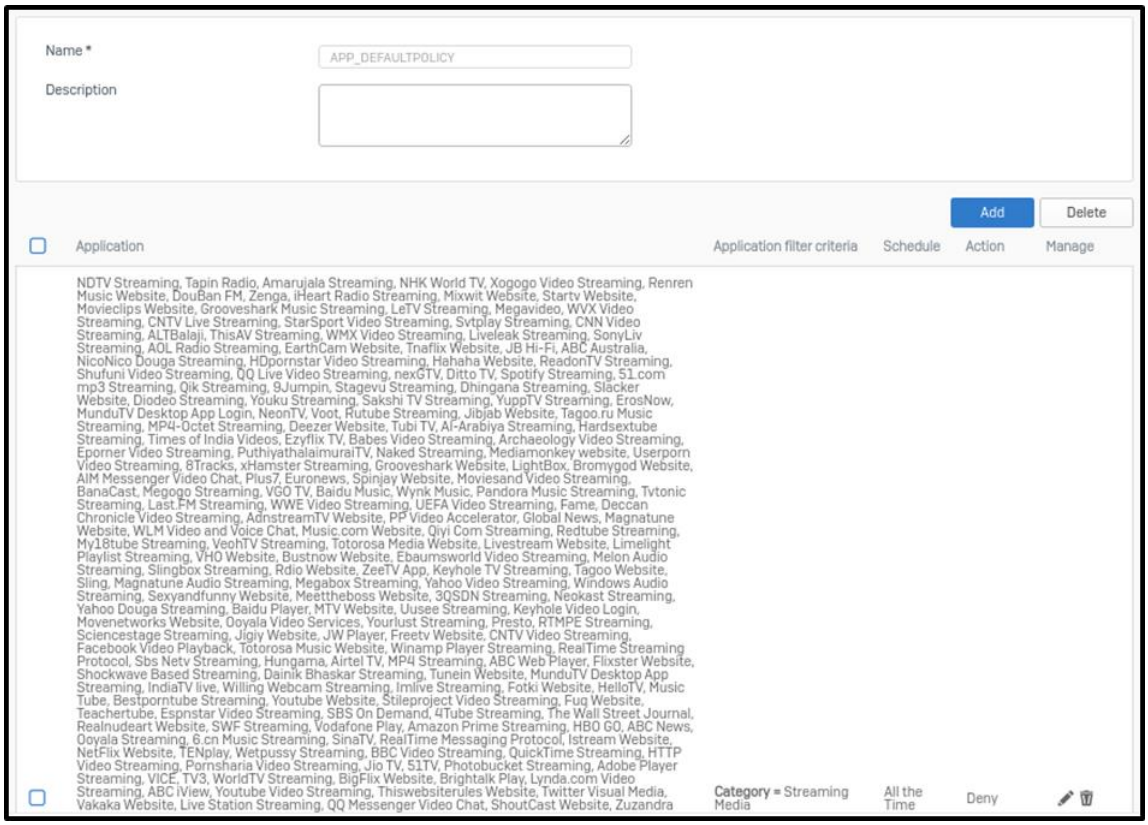
Fonte: Elaborada pelo autor

Nessa primeira política de acesso geral aos colaboradores, foram definidos a liberação das categorias de serviços financeiros, governos, e SITES_LIBERADOS como o site da própria empresa, serviços de frete ao qual é utilizado no ambiente empresarial, entre outros sites que foram definidos como importantes no negócio.

Após a liberação destes foram realizados os bloqueios das seguintes categorias, crime ativo, entretenimento, jogos de azar, jogos, hacking, pirataria intelectual, áudio ao vivo, maconha, notícias, nudismo, P2P e torrents, phishing e fraude, educação sexual, sexo explícito, esportes, spyware e malware, SITES_BLOQUEADOS como clicRBS e facebook. E como política padrão as demais categorias web foram permitidas pelo firewall.

Realizada a política de acesso WEB, a todos os usuários da rede, foi definido também uma política de aplicação para o mesmo, o qual pode se verificar abaixo:

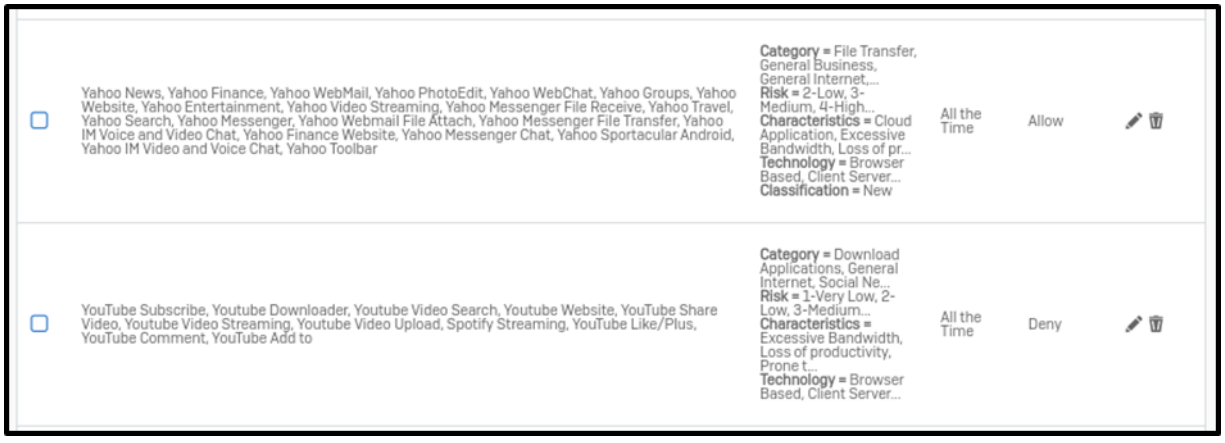
Figura 12: Política de acesso a aplicações (Straming Media)



Fonte: Elaborada pelo autor

Uma das categorias de aplicação ao qual foram bloqueadas foi a categoria de streaming de media, ao qual encontra-se players de vídeo e áudio, como Youtube.

Figura 13: Política de acesso a aplicações (Youtube, Yahoo)



Fonte: Elaborada pelo autor

Após foi realizado a liberação do Yahoo, ao qual é categorizado em geral como rede social, porém conta com serviço de E-mail e era de utilização da empresa. Foi realizado também o bloqueio geral do Youtube.

Figura 14: Política de acesso a aplicações (Redes Sociais)

Fonte: Elaborada pelo autor

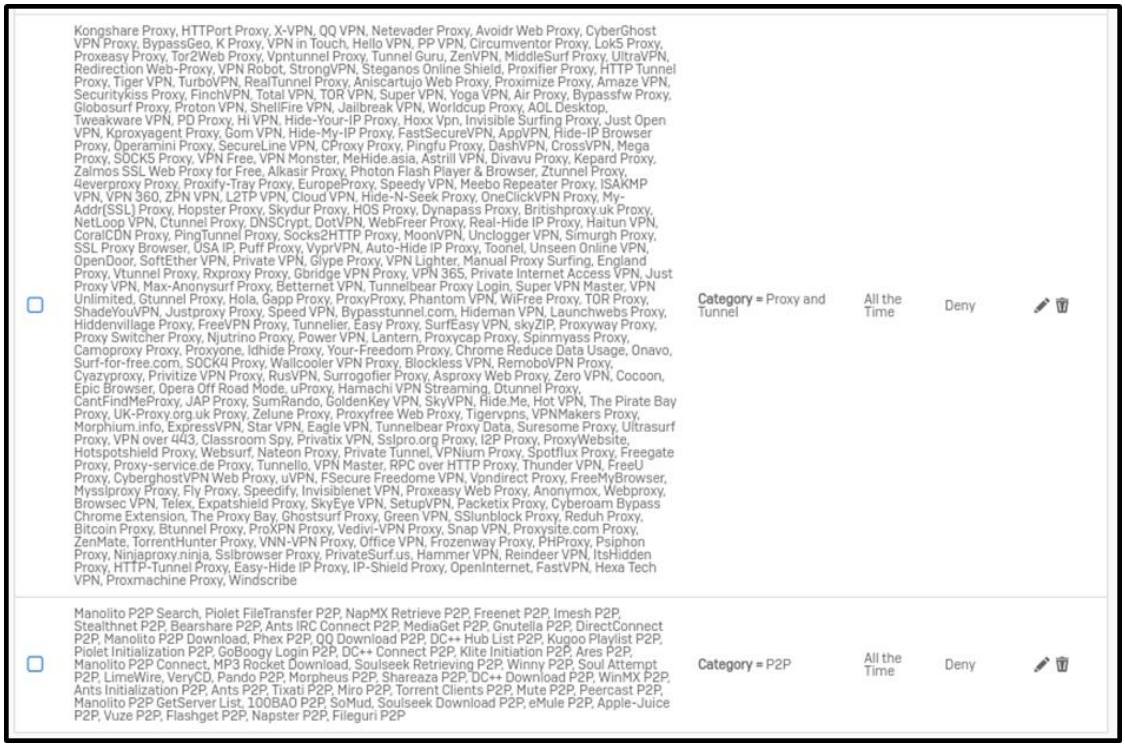
Foi bloqueado a categorias de redes sociais, dentro dela encontra-se, Facebook, Instagram, LinkedIn, Twitter, entre outras.

Figura 15: Política de acesso a aplicações (Jogos)

Fonte: Elaborada pelo autor

A categoria de jogos também foi bloqueada para o acesso em geral, dentre os jogos nessa categoria encontram-se Free Fire, Xbox Live, jogos do Facebook.

Figura 16: Política de acesso a aplicações (Proxy e Túnel, P2P)



Fonte: Elaborada pelo autor

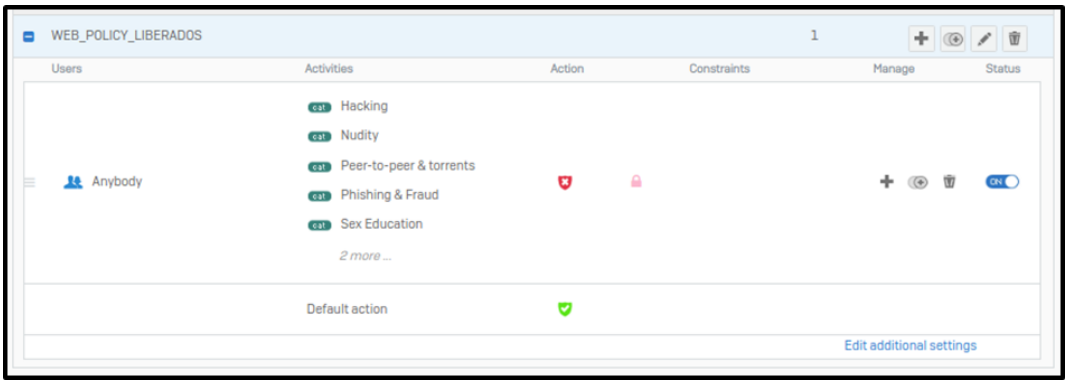
E por último foi realizado o bloqueio das categorias de proxy e túnel, ao qual encontram-se VPNs para desviar o tráfego para a internet, e a categoria de P2P, ao qual pode trazer risco a segurança e integridade da rede.

As políticas mencionadas acima foram definidas para os usuários em rede e geral, porém conforme a necessidade da empresa, foram feitas liberações a determinados IPs, com direito a acesso liberado a internet como iremos mostrar nas configurações abaixo.

A política de IPs liberados foi solicitada pelo departamento de ti da empresa e seus gestores, ao qual possui um número de 20 IPs sem restrições de acesso, a conteúdos que foram definidos acima para a rede em geral, dentre os IPs definidos estão os dispositivos dos gestores da empresa, e do departamento de TI, e para colaboradores com cargo de gerência.

Para os dispositivos liberados foram criadas as seguintes políticas de acesso WEB:

Figura 17: Política de acesso web liberados

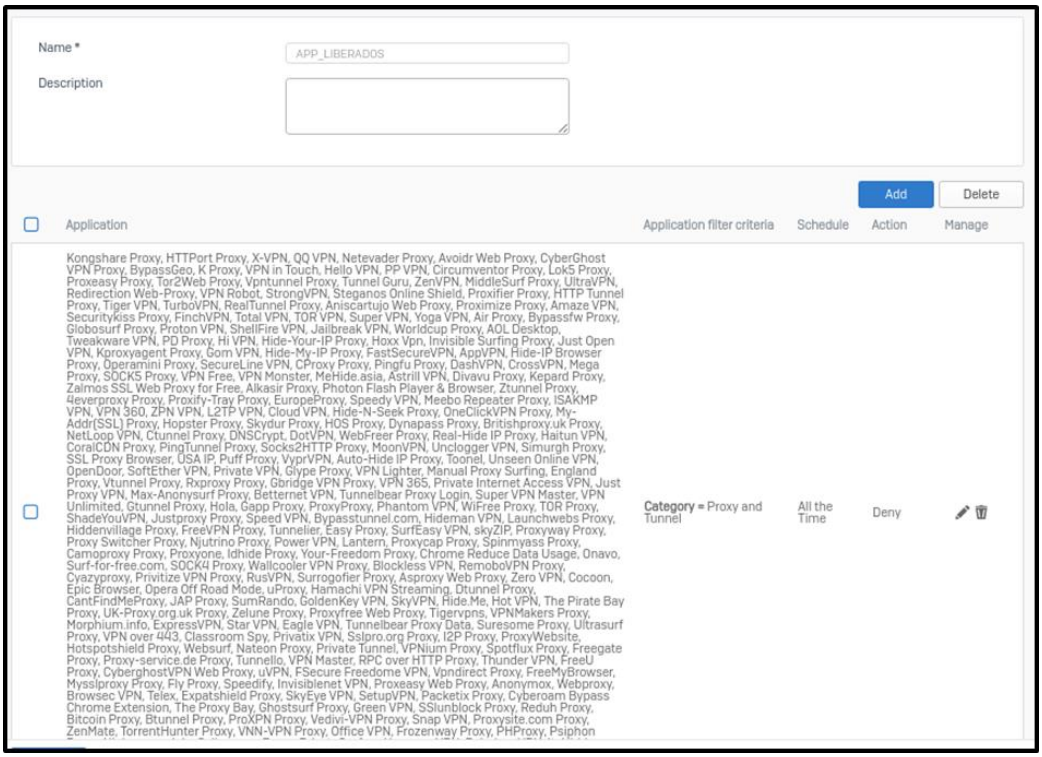


Fonte: Elaborada pelo autor

Foram bloqueadas as seguintes categorias, para os dispositivos liberados, Hacking, nudismo, P2P e Torrent, Phishing e fraude educação sexual, sexo explícito, Spyware e Malware. Mesmo os dispositivos sendo solicitados para ter liberação total foi mantido uma política de acesso para manter a segurança e a integridade da rede bloqueando acesso a conteúdos que são por onde temos os maiores números de infecções de rede.

Para os mesmos dispositivos liberados, foi definida também uma política de aplicação, como podemos verificar abaixo:

Figura 18: Política de acesso a aplicações (Proxy e Túnel)



Fonte: Elaborada pelo autor

Foi realizado o bloqueio da categoria proxy e túnel, para evitar desvios de conexões, e manter a navegação principal pelo firewall.

Figura 19: Política de acesso a aplicações (P2P)

Fonte: Elaborada pelo autor

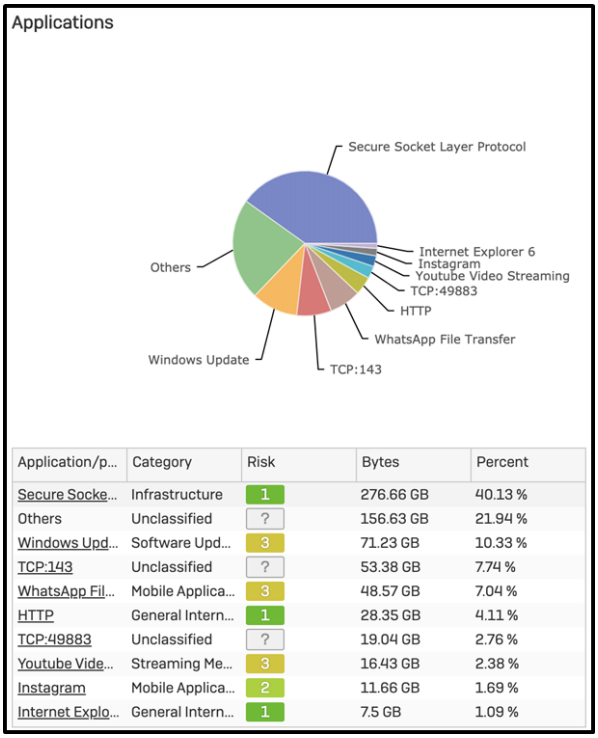
Outra categoria bloqueada foi a categoria de P2P onde se encontram aplicações como Torrent que pode trazer riscos para a rede da empresa.

Sendo aplicadas as políticas mencionadas acima a seus respectivos usuários foi notável a diferença do que era acessado antes e depois, das aplicações das políticas como poderemos verificar em seguida.

4 RESULTADOS E DISCUSSÃO

Após a aplicação das políticas de acesso, foi extraído um novo relatório do que foi acessado de dentro da empresa, onde foi possível identificar uma enorme queda no acesso de conteúdo considerado improdutivo para a empresa, vamos analisar os gráficos abaixo:

Gráfico 6: Aplicações mais acessadas após a implementação da política de acesso

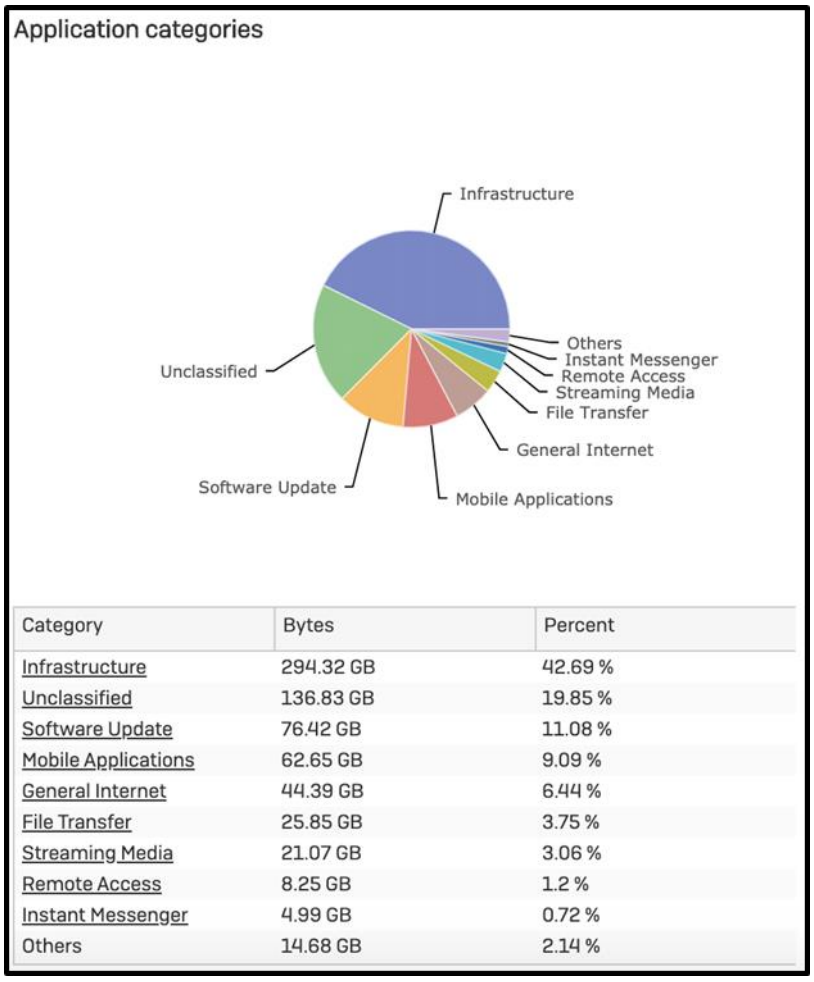


Application/p...	Category	Risk	Bytes	Percent
Secure Socke...	Infrastructure	1	276.66 GB	40.13 %
Others	Unclassified	?	156.63 GB	21.94 %
Windows Upd...	Software Upd...	3	71.23 GB	10.33 %
TCP:143	Unclassified	?	53.38 GB	7.74 %
WhatsApp Fil...	Mobile Applica...	3	48.57 GB	7.04 %
HTTP	General Intern...	1	28.35 GB	4.11 %
TCP:49883	Unclassified	?	19.04 GB	2.76 %
Youtube Vide...	Streaming Me...	3	16.43 GB	2.38 %
Instagram	Mobile Applica...	2	11.66 GB	1.69 %
Internet Explo...	General Intern...	1	7.5 GB	1.09 %

Fonte: Elaborada pelo autor

Esse primeiro gráfico traz as aplicações mais acessadas após a implementação das políticas de acesso, no gráfico anterior tínhamos o Facebook com mais de 200 GB de acesso, ao qual no momento não é nem listado no gráfico, Youtube no gráfico anterior estava com um consumo de 98 GB, após a aplicação das políticas o mesmo diminui para 16 GB, onde é notável a diminuição também do quanto foi trafegado na rede, pois limitando o acesso a determinados sites, o consumo também diminuiu.

Gráfico 7: Categorias de aplicação mais acessadas após a implementação da política de acesso

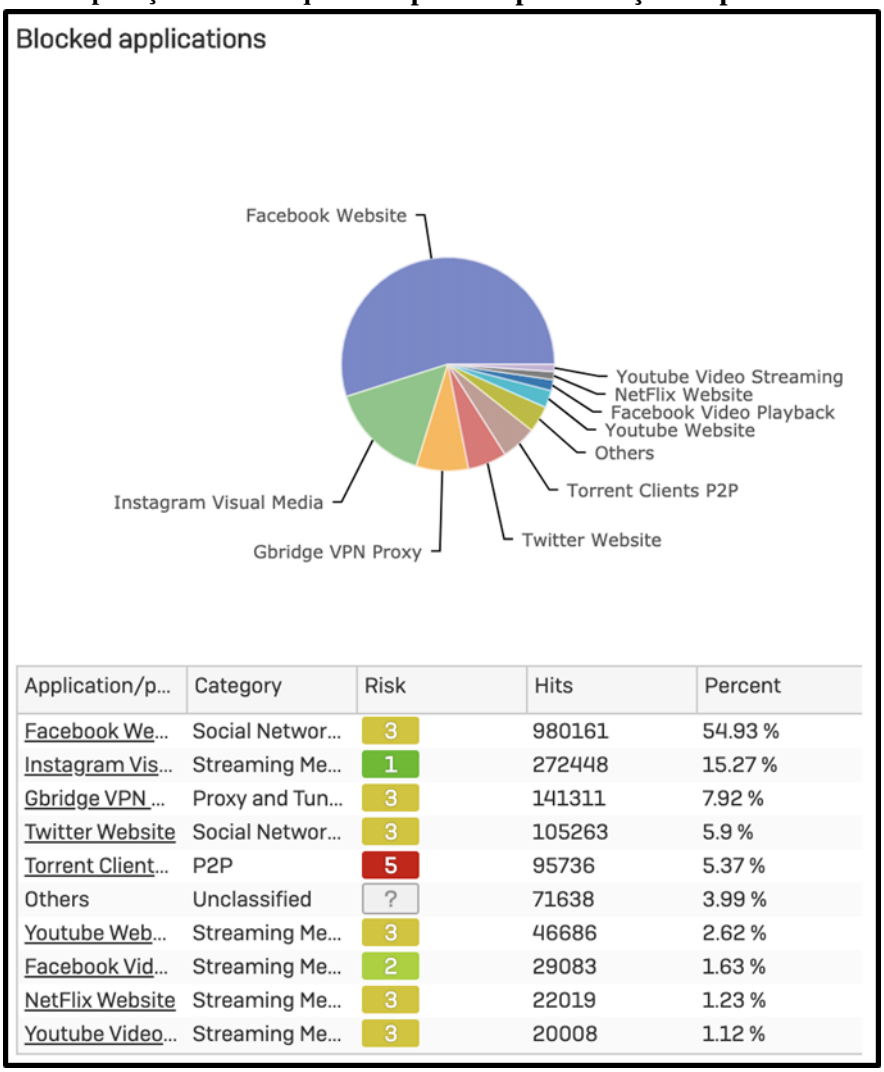


Category	Bytes	Percent
Infrastructure	294.32 GB	42.69 %
Unclassified	136.83 GB	19.85 %
Software Update	76.42 GB	11.08 %
Mobile Applications	62.65 GB	9.09 %
General Internet	44.39 GB	6.44 %
File Transfer	25.85 GB	3.75 %
Streaming Media	21.07 GB	3.06 %
Remote Access	8.25 GB	1.2 %
Instant Messenger	4.99 GB	0.72 %
Others	14.68 GB	2.14 %

Fonte: Elaborada pelo autor

Neste outro gráfico verificamos as categorias de aplicação mais acessadas, após a implementação das políticas de acesso, à categoria de infraestrutura continua como líder de acesso, e diferente do relatório anterior ao qual as redes sociais era a segunda categoria mais acessada com mais 200 GB de acessado, a mesma categoria, nem lista entre as top 10 categorias de acesso.

Gráfico 8: Aplicações mais bloqueadas após a implementação da política de acesso

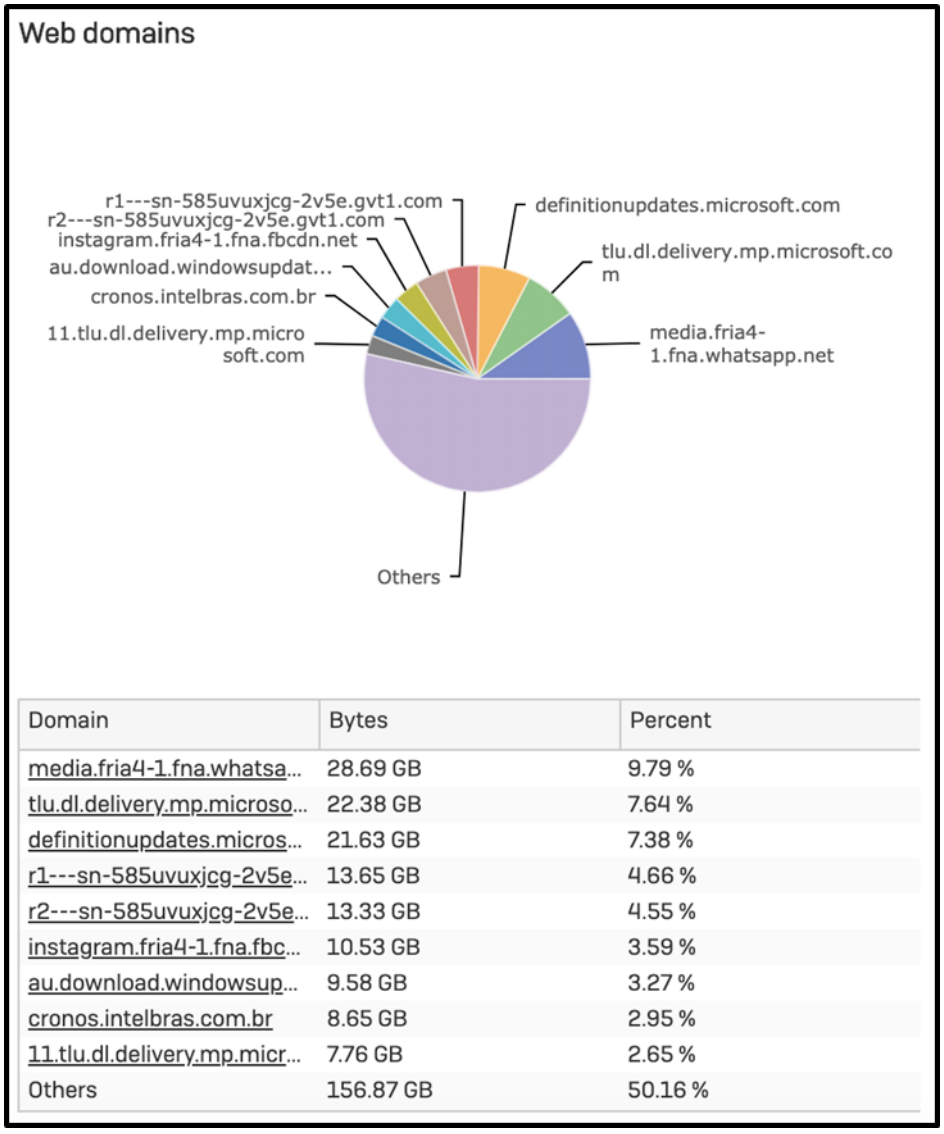


Application/p...	Category	Risk	Hits	Percent
Facebook We...	Social Networ...	3	980161	54.93 %
Instagram Vis...	Streaming Me...	1	272448	15.27 %
Gbridge VPN ...	Proxy and Tun...	3	141311	7.92 %
Twitter Website	Social Networ...	3	105263	5.9 %
Torrent Client...	P2P	5	95736	5.37 %
Others	Unclassified	?	71638	3.99 %
Youtube Web...	Streaming Me...	3	46686	2.62 %
Facebook Vid...	Streaming Me...	2	29083	1.63 %
NetFlix Website	Streaming Me...	3	22019	1.23 %
Youtube Video...	Streaming Me...	3	20008	1.12 %

Fonte: Elaborada pelo autor

Neste gráfico é possível visualizar as aplicações mais bloqueadas na rede, dentre a principal categoria encontram-se o Facebook, com mais de 50% do que é bloqueado, seguido de Instagram, Gbridge VPN e Twitter.

Gráfico 9: Domínios da web mais acessados após a implementação da política de acesso

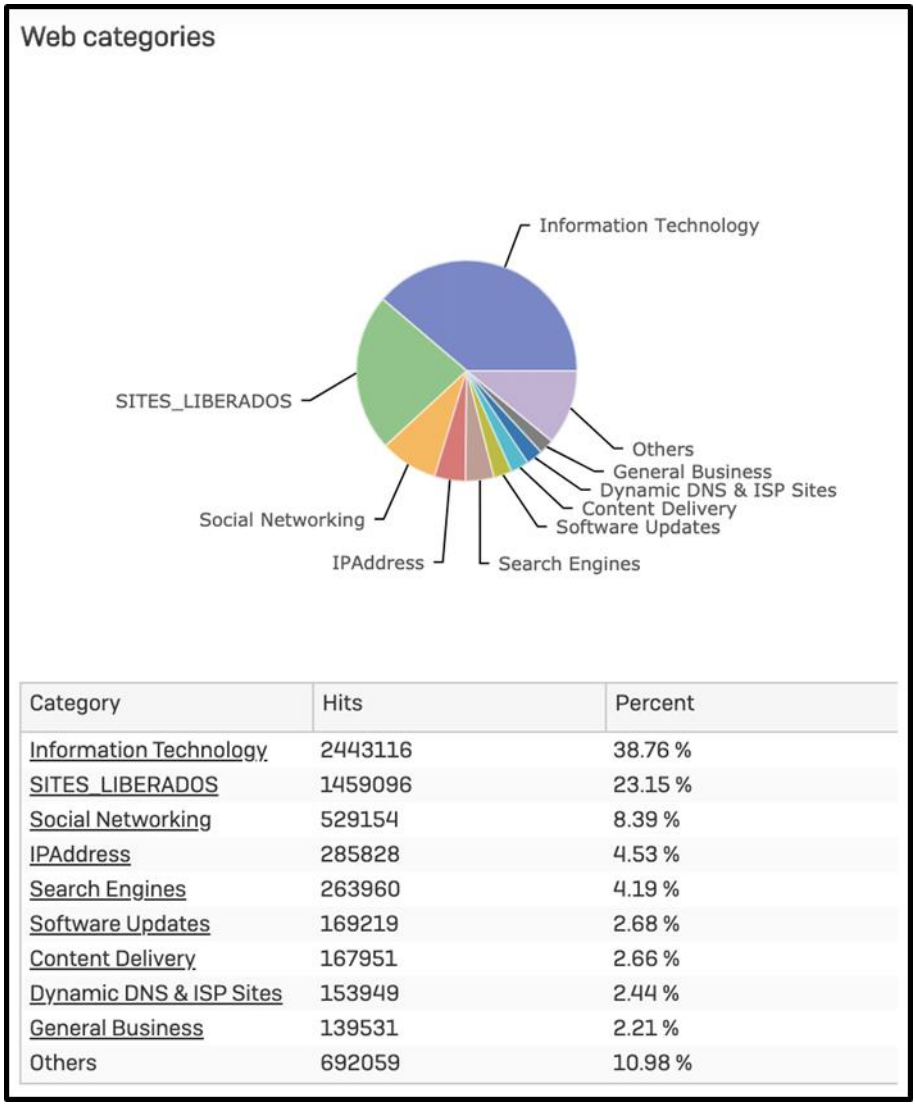


Domain	Bytes	Percent
media.fria4-1.fna.whatsa...	28.69 GB	9.79 %
tlu.dl.delivery.mp.microso...	22.38 GB	7.64 %
definitionupdates.micros...	21.63 GB	7.38 %
r1---sn-585uvuxjcg-2v5e...	13.65 GB	4.66 %
r2---sn-585uvuxjcg-2v5e...	13.33 GB	4.55 %
instagram.fria4-1.fna.fbc...	10.53 GB	3.59 %
au.download.windowsup...	9.58 GB	3.27 %
cronos.intelbras.com.br	8.65 GB	2.95 %
11.tlu.dl.delivery.mp.micr...	7.76 GB	2.65 %
Others	156.87 GB	50.16 %

Fonte: Elaborada pelo autor

Este gráfico traz os domínios da Web mais acessados após a implementação da política de acesso, como é possível visualizar o domínio com mais acesso é as atualizações da Microsoft, tendo também uma enorme redução no acesso aos domínios de Instagram, Facebook e Whatsapp.

Gráfico 10: Categorias da web mais acessada após a implementação da política de acesso

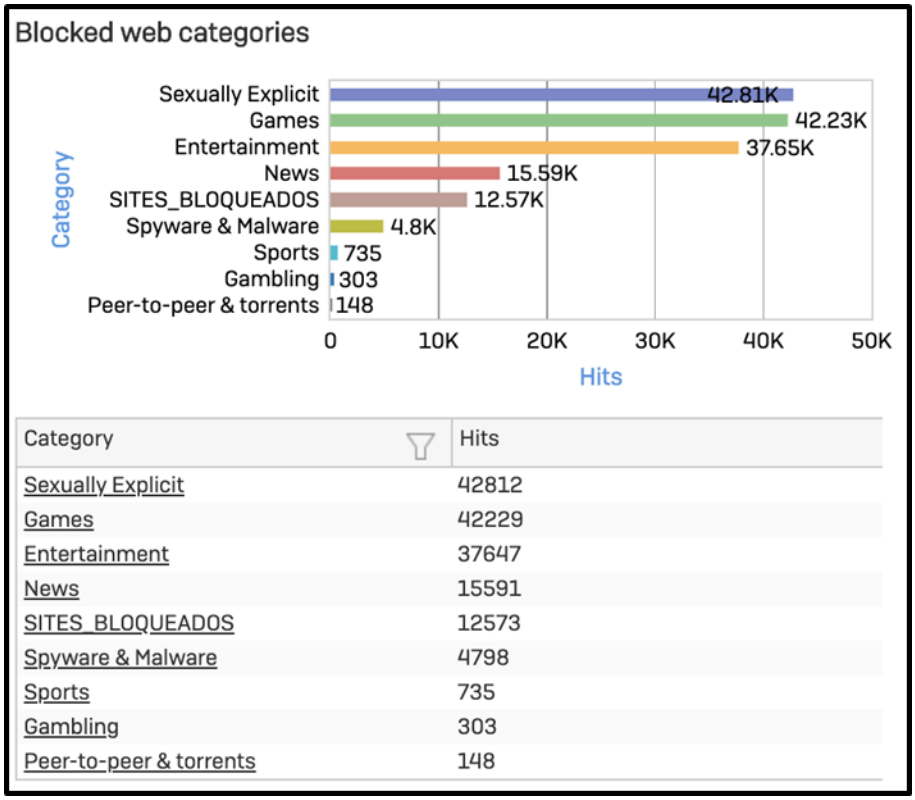


Category	Hits	Percent
Information Technology	2443116	38.76 %
SITES_LIBERADOS	1459096	23.15 %
Social Networking	529154	8.39 %
IPAddress	285828	4.53 %
Search Engines	263960	4.19 %
Software Updates	169219	2.68 %
Content Delivery	167951	2.66 %
Dynamic DNS & ISP Sites	153949	2.44 %
General Business	139531	2.21 %
Others	692059	10.98 %

Fonte: Elaborada pelo autor

As categorias da web mais acessada após a implementação da política de acesso como Tecnologia da Informação com 38,76% dos acessos, seguido dos SITES_LIBERADOS com 23,15%, e Redes Sociais com 8,39% dos acessos.

Figura 20: Categorias WEB bloqueadas

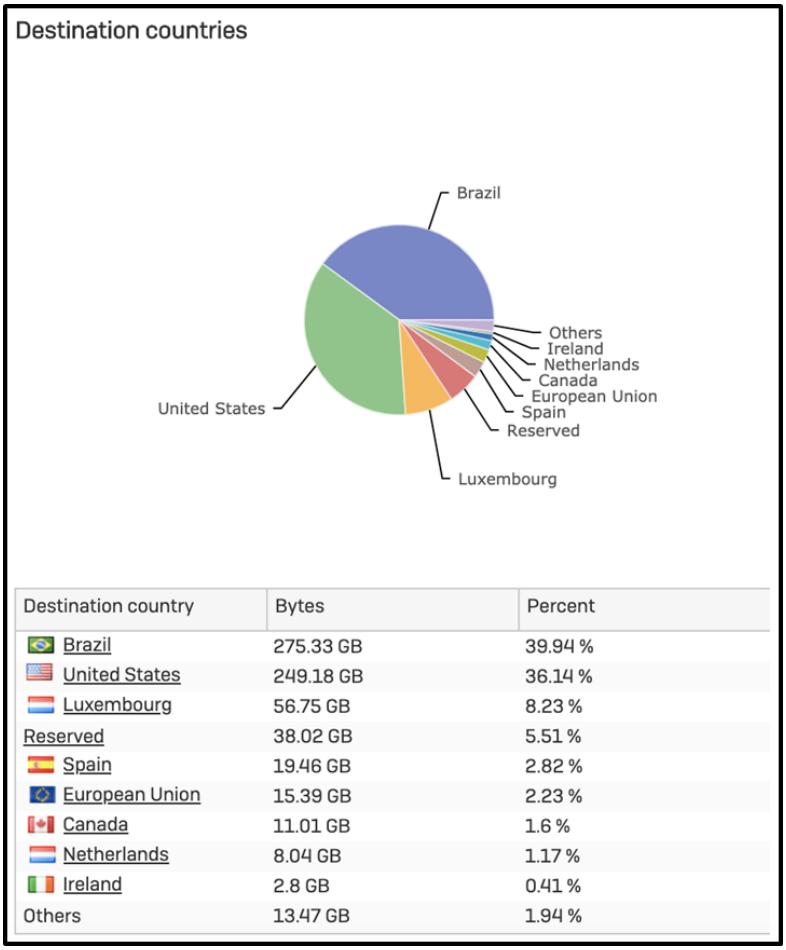


Category	Hits
Sexually Explicit	42812
Games	42229
Entertainment	37647
News	15591
SITES_BLOQUEADOS	12573
Spyware & Malware	4798
Sports	735
Gambling	303
Peer-to-peer & torrents	148

Fonte: Elaborada pelo autor

No gráfico acima podemos visualizar as categorias da web mais bloqueadas pelo firewall, ao qual encontram-se categorias como sexo explícito, jogos, entretenimento, jogos de azar, esportes, P2P e Torrent.

Gráfico 11: Países com mais acesso após a implementação da política de acesso

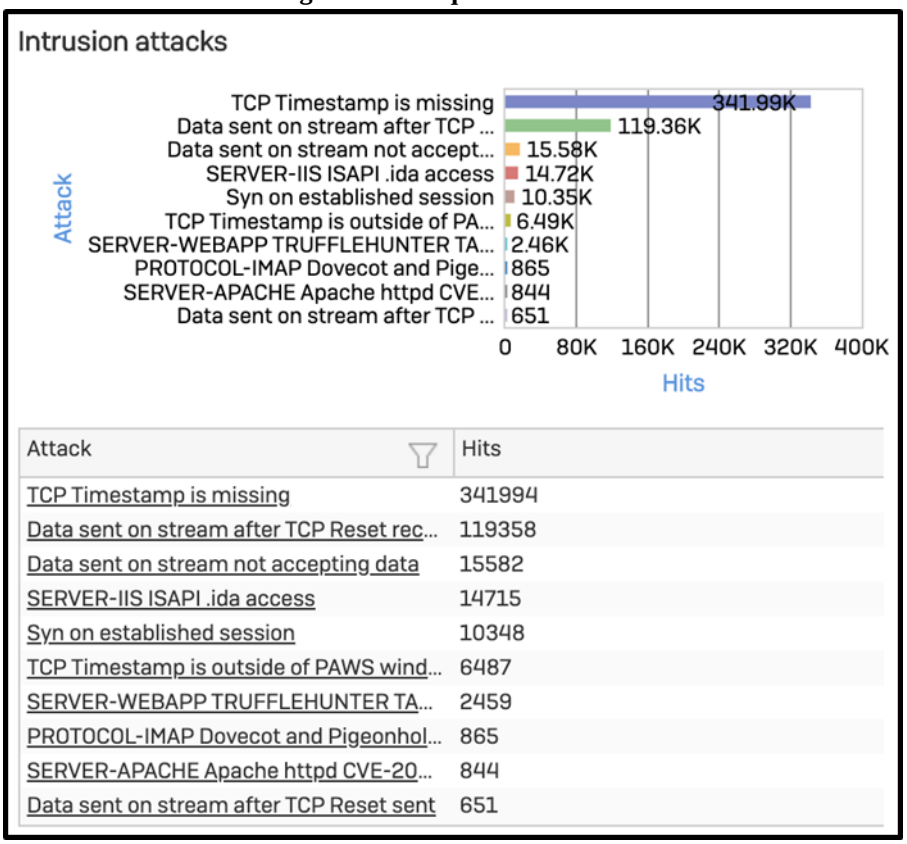


Destination country	Bytes	Percent
Brazil	275.33 GB	39.94 %
United States	249.18 GB	36.14 %
Luxembourg	56.75 GB	8.23 %
Reserved	38.02 GB	5.51 %
Spain	19.46 GB	2.82 %
European Union	15.39 GB	2.23 %
Canada	11.01 GB	1.6 %
Netherlands	8.04 GB	1.17 %
Ireland	2.8 GB	0.41 %
Others	13.47 GB	1.94 %

Fonte: Elaborada pelo autor

Este gráfico apresenta os países mais acessados, onde temos o Brasil com 275,33 GB de tráfego comparado ao primeiro cenário temos uma redução de mais de 300GB de acesso após a implementação das políticas, seguido de Estados Unidos com 249,18 GB de tráfego e Luxemburgo com 56,75 GB, e Espanha com 19,46 GB.

Figura 21: Ataques de intrusão



Attack	Hits
TCP Timestamp is missing	341994
Data sent on stream after TCP Reset rec...	119358
Data sent on stream not accepting data	15582
SERVER-IIS ISAPI .ida access	14715
Syn on established session	10348
TCP Timestamp is outside of PAWS wind...	6487
SERVER-WEBAPP TRUFFLEHUNTER TA...	2459
PROTOCOL-IMAP Dovecot and Pigeonhol...	865
SERVER-APACHE Apache httpd CVE-20...	844
Data sent on stream after TCP Reset sent	651

Fonte: Elaborada pelo autor

Neste gráfico podemos visualizar os ataques de intrusão realizados na rede durante o período, como podemos visualizar no gráfico temos diversas tentativas de ataque onde todos são identificados e barrados pelo firewall, esses ataques ocorrem por motivos de acessos externos, tentativa de roubo de informações, acessos a sites vulneráveis e infectados.

Figura 22: Resumo do relatório geral de tudo que foi trafegado na rede

Applications & web	
Users & data transfer	
• User count :	23
• Total user data transfer :	438.1 MB
User applications	
• Applications accessed :	15563
• High-risk applications accessed :	24
• App risk score (out of 5) :	0.52
• Blocked applications :	85
• Application data transfer :	689.44 GB
Web	
• Web domains accessed :	28129
• Web domains blocked :	913
• Objectionable web domains accessed :	169
• Web data transfer :	293.08 GB
• Web virus :	0
Business applications	
• Web server(s) count :	0
• Blocked web server requests :	0

Email	
• Mails processed :	19
• Spam mails :	0
• Virus mails blocked :	0
Network & threats	
VPN	
• VPN connections :	13
• VPN traffic (L2TP,PPTP) :	0 B
RED	
• RED usage :	0 B
Wireless	
• Wireless AP count :	0
• SSID count :	0
• Max clients per SSID :	0
• Avg clients per SSID :	0
IPS	
• Intrusion attacks :	513326
• Emergency + critical attacks :	3399
Advanced threat protection	
• Host count :	0
• Threat count :	0
• Events :	0

Web admin console logins	
• Successful :	34
• Failed :	0
System	
• System restarts :	0
Updates	
• Firmware updates installed :	0
• Pattern updates installed :	166

Fonte: Elaborada pelo autor

Essa tabela apresenta o relatório geral após a implementação das políticas de acesso e nele podemos visualizar uma enorme redução na transferência de dados de aplicação onde tínhamos no primeiro ambiente 999,91 GB onde reduziu para 689,44 GB. Na transferência de dados WEB, de 621,29 GB o consumo diminui para 293,08 GB de tráfego. Também medimos a quantidade de login dos usuários administradores, conexões VPN, número de ataques, número de domínios e aplicações acessadas.

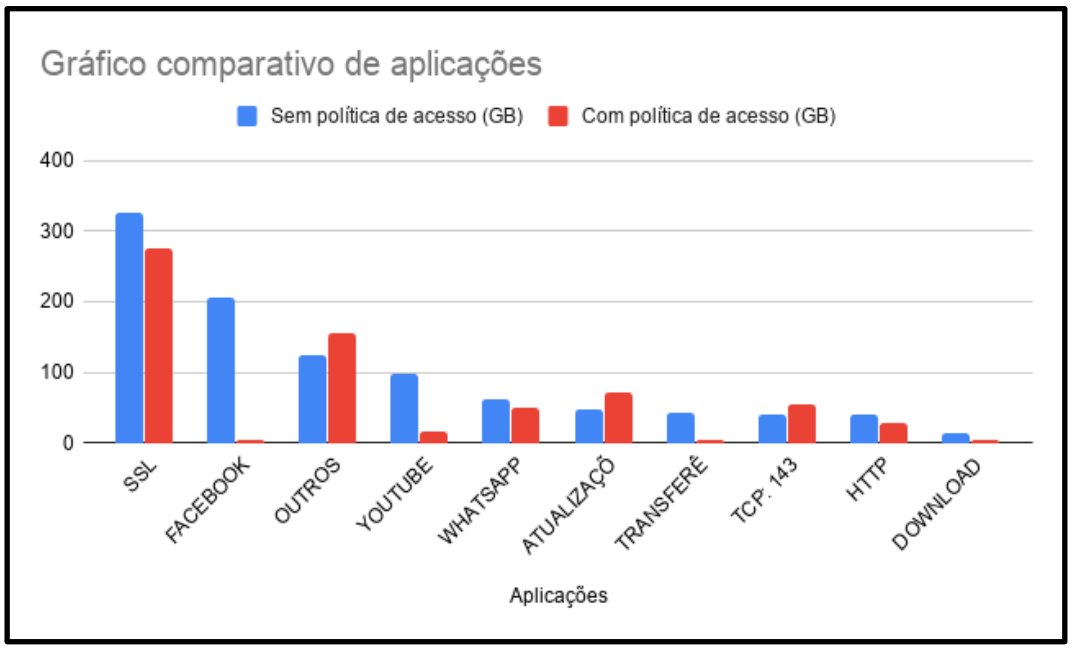
5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo: a) Sugerir uma política de uso de acesso a rede e internet utilizando o Sophos XG Firewall; b) Através de uma política de acesso, manter a integridade, a disponibilidade e a confidencialidade das informações de posse da organização; c) Apresentar soluções que com a utilização e configuração correta podem ajudar a empresa a atingir os seus objetivos; d) Apresentar como as políticas de acesso interferem diretamente na produtividade de seus colaboradores.

Através desse estudo de caso onde foi sugerido e aplicado a um ambiente corporativo uma política de acesso à rede e internet, onde foram feitos bloqueios de conteúdo classificados como improdutivos, e de alto risco para a rede. Como podemos visualizar no Gráfico de nº 1 Aplicações mais acessadas antes da implementação da política de acesso, onde o acesso a conteúdo ao qual não era considerado e classificado como produtivo tinha alto número de acessos. Nos gráficos abaixo está uma

comparação entre os acessos à internet antes e após a implementação das políticas de acesso sugeridas, onde podemos observar uma grande redução de acessos à conteúdos considerados e classificados como improdutivos para o ambiente empresarial, onde além de termos um alto consumo de tráfego de rede incluindo rende interna e externa, ou seja, internet da empresa deixando o acesso consideravelmente mais lento, com base na análise de tráfego como um todo. Possivelmente inviabilizando a realização de tarefas do dia-a-dia dos colaboradores quando falamos em produtividade.

Gráfico 12: Gráfico comparativo das aplicações

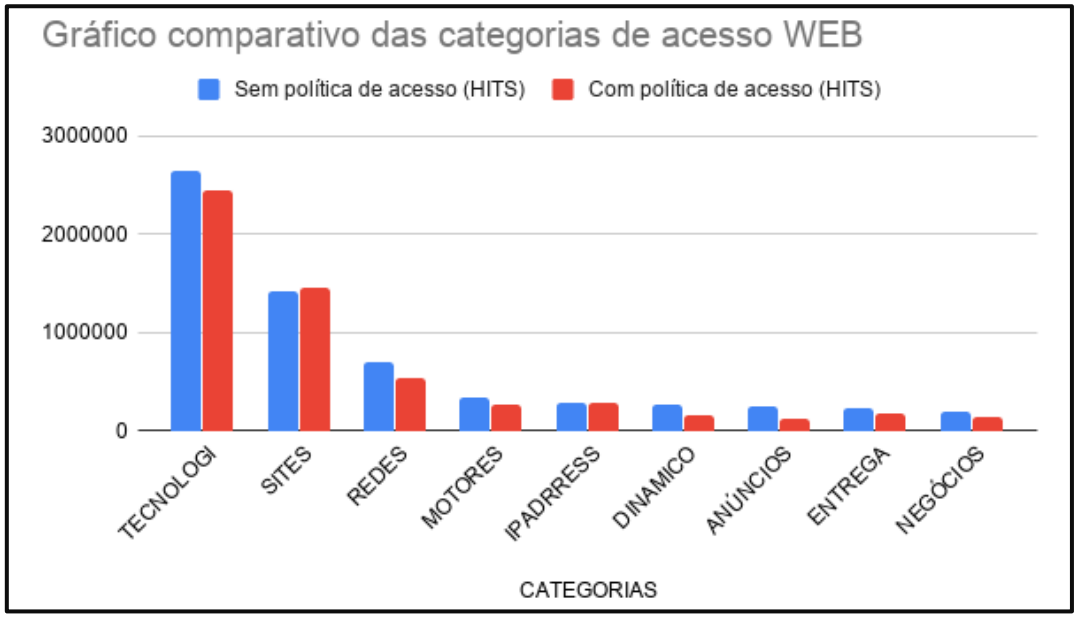


Fonte: Elaborada pelo autor

Neste primeiro gráfico é possível visualizar um comparativo do tráfego da rede, através do filtro de aplicações implementada em ambos os cenários, ou seja, como as políticas de acesso sugeridas aplicadas e sem a política. Podemos verificar uma queda na utilização do Facebook, onde tínhamos 206,65 GB de tráfego e após o uso da política reduziu para 2,79 GB. O Youtube de 98,57 GB de tráfego reduziu para 16,43 GB, o protocolo SSL anteriormente a aplicação das políticas consumiu 325,07 GB e após a implementação passou para 276,66. Transferência de arquivos de WhatsApp consumia 62,46 GB e diminuiu para 48,57 GB, as atualizações do Windows de 36,68 GB aumentou para 71,23 GB. As transferência de arquivos Multi-thread de 42,6 GB diminui para 4,72 GB, o protocolo TCP: 143 de 40,25 GB aumentou para 53,51 GB, já o protocolo HTTP diminuiu de 39,68 GB para 28,35 GB, e a última aplicação download de arquivos ZIP de 12,64 GB de tráfego reduziu para 4,4 GB.

Se for observado somente as 10 aplicações citadas acima, temos uma redução de tráfego de dados na rede de 336,42 GB em 16 dias.

Gráfico 13: Gráfico comparativo entre as categorias de acesso WEB



Fonte: Elaborada pelo autor

No gráfico acima onde observamos as categorias de acesso WEB mais acessadas nos dois ambientes, onde o acesso a categoria da Tecnologia da Informação era de 2651145 acessos e passou para 2443116 acessos, já os SITES_LIBERADOS de 1412002 passou para 1459096 acessos, às Redes Sociais de 705774 acessos diminuiu para 529154, a categoria de Motores de Busca de 342202 acessos passou para 263960, a categoria de anúncios de 239195 reduziu para 123002 acessos, outra categoria de Entrega de Conteúdo de 220516 passou para 167951 acessos, e como a última categoria, Negócios em geral que de 196560 acessos diminuiu para 139531.

Através de um comparativo desenvolvido e apresentado neste trabalho foi possível observar que a utilização do método proposto, traz grandes benefícios para o âmbito empresarial, pois além de limitar os usuários a terem acesso somente a conteúdos permitidos, também reduz o tráfego de rede na infraestrutura de tecnologia da empresa, deixando assim a rede menos sobrecarregada, ou seja, menos GB desnecessariamente filtrados, o que traz uma boa performance operacional aos colaboradores diante da realização de suas tarefas, sem travamentos e/ou infecções de vírus, malware e ataques à rede e dispositivos.

Como é possível visualizar na figura nº 21, que traz as 10 categorias web mais bloqueadas, acompanhamos inúmeras tentativas barradas pelo Sophos XG firewall nas

categorias que trazem risco para rede, como Spyware e Malware, sexo explícito, P2P e Torrents. Já no outro gráfico de nº 8 , o gráfico das aplicações mais bloqueadas traz o Facebook, com mais de 50% dos bloqueios, seguido de Instagram, Gbridge, Twitter e Torrent.

A ferramenta de segurança Sophos XG Firewall, selecionada para a implantação no ambiente descrito acima, se mostrou totalmente estável, e fiel, em todos os momentos que foi utilizado e todos recursos necessários estiveram disponíveis, sendo confirmada como uma boa opção para implementação de políticas de acesso e segurança. Vale lembrar que esta foi uma política de acesso arquitetada como modelo para o ambiente descrito neste trabalho, ou seja, para cada ambiente é necessário estudar a melhor política de acesso a se aplicar, pois além de limitar o acesso a sites e manter a segurança, a política de acesso tem como objetivo também, melhorar a performance da rede da empresa, para que os usuários possam utilizar um ambiente confiável, íntegro e sempre disponível.

Portanto concluo que a pesquisa proposta neste trabalho, foi fielmente aplicada e os resultados apresentados.

REFERÊNCIAS

ALECRIM, Emerson. **O que é firewall? - Conceito, tipos e arquiteturas.** Infowester. Disponível em: <https://www.infowester.com/firewall.php/>. Acesso em: 15 março 2019.

ANDREI L. **História da Internet.** Agos. 2019. Disponível em: <https://www.weblink.com.br/blog/historia-da-internet/> Acesso em 25 agosto 2019.

ANICAS, Mitchell. **O que é um firewall e como funciona?** Agosto 2015. Disponível em: <https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work>. Acesso em: 20 de julho 2019.

ARIMURA, Mayumi. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros.** jun. 2016. Disponível em:

<https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros> Acesso em: 31 outubro. 2019.

BAHL, Madhav. **Camadas do modelo OSI.** Abr. 2018. Disponível em: <https://medium.com/learn-with-the-lean-programmer/osi-model-layers-explained-ee1d430581f > Acesso em: 23 agosto 2019.

BEAL, Vangie. **Firewall.** Seção ponto de vista. Disponível em: <https://www.webopedia.com/TERM/F/firewall.html>. Acesso em: 20 jul. 2019.

BEAL, Vangie. **A diferença entre firewall de hardware e software.** Jun. 2010. Disponível em: <https://www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp>. Acesso em: 20 de julho 2019.

BEAL, Vangie. **As 7 camadas do modelo OSI.** abr. 2019. Disponível em: <https://www.webopedia.com/quick_ref/OSI_Layers.asp>. Acesso em: 03 agosto 2019.

BLANCHARD, Chad. **A importância do monitoramento de rede.** Out. 2015. Disponível em: < https://itnow.net/the-importance-of-network-monitoring/>. Acesso: em 1 novembro 2019.

BLOCKMON, Raymond. **O que é um hacker? - Definição e Visão Geral.** mar. 2018. Disponível em: < https://study.com/academy/lesson/what-is-a-hacker-definition-lesson-quiz.html > Acesso em 22 outubro 2019.

CAETANO, Érica. **"O que é hacker?"**; Brasil Escola. Disponível em: <https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm >. Acesso em 16 de novembro de 2019.

CANALTECH. **O que é DoS e DDoS.** CANALTECH. Disponível em: <https://canaltech.com.br/produtos/O-que-e-DoS-e-DDoS/ > Acesso em 1 nov. 2019.

CARRION, Izabella. **Próxima geração de firewalls.** 2018. Disponível em: <https://ostec.blog/seguranca-perimetro/next-generation-firewall> Acesso em: 20 de outubro 2019.

CBRONLINE. **O que é Sophos?** Nov. 2010. Disponível em: <https://www.cbronline.com/what-is/what-is-sophos/#2> Acesso em: 27 junho 2019.

CEG. **Segurança: Controle de acesso à internet nas empresas.** Jun. 2019. Disponível em: <http://cegconsultoria.com.br/controle/ > Acesso em: 13 novembro 2019.

DUARTE. **Varredura de portas.** 2016. Disponível em: < https://www.gta.ufrj.br/grad/16_2/2016VARPORT/> Acesso em: abril 2019.

ECOIT. **O que é firewall e qual seu papel na manutenção da segurança.** Seção ponto de vista. Disponível em: <https://ecoit.com.br/o-que-e-firewall/>. Acesso em: 12 maio 2019.

FIGUEIREDO, Iria. **História das redes de computadores**. mar. 2013. Disponível em: <https://www.oficinadanet.com.br/post/10123-historia-das-redes-de-computadores> Acesso em: 10 agosto 2019.

FILIPPETTI, Marco. **Modelo OSI um diagrama funcional.** Mar. 2019. Disponível em: <http://blog.ccna.com.br/2019/03/20/modelo-osi-um-diagrama-funcional/> Acesso em: 27 agosto 2019.

GIMENES, Mauricio. **Sophos o que é?** Fev. 2018. Disponível em: <https://introduceti.com.br/blog/o-que-e-sophos/>. Acesso em: 03 agosto 2019.

GFI. **Exemplo de política de uso de internet.** Disponível em: <https://www.gfi.com/pages/sample-internet-usage-policy> Acesso em: 7 outubro 2019.

IMPERVA. **O que é um ataque de backdoor.** IMPERVA. Disponível em: <https://www.imperva.com/learn/application-security/backdoor-shell-attack/ > Acesso: 1 novembro 2019.

IRWIN, Luke. **O que é a série de padrões ISO 27000?** Out. 2019. Disponível em: <https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards>. Acesso em: 3 novembro 2019.

KEUNG, Yau. **Princípios básicos da segurança.** mar. 2014. Disponível em: <https://www.omicsonline.org/open-access/basic-principle-of-information-security-2168-9695.1000e120.php?aid=25302> Acesso em: 30 agosto 2019.

LEAL, Rhand. **O que é a iso 27001?** Disponível em: <https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/ > Acesso em 3 nov. 2019.

MALWAREBYTES. **Ransomware.** 2018. Disponível em: < https://br.malwarebytes.com/ransomware/>. Acesso em 1 novembro 2019.

MARINHO, Guilherme. **hackers, crackers e o direito-penal.** 2016. Disponível em: <https://grmadv.jusbrasil.com.br/artigos/407334629/hackers-crackers-e-o-direito-penal> Acesso em: 31 outubro 2019.

MARQUES, Marcus. **Criando uma Política Interna de Acesso à Internet na Organização**. abr. 2017. Disponível em: <http://marcusmarques.com.br/gestao-de-pessoas/criando-politica-interna-acesso-internet-organizacao/ >. Acesso em: 22 outubro 2019.

MELIM, Miguel. **DHCP Snooping, IP Source, ARP Inspection | Defesa MITM.** Madeira. Disponível em: < https://www.madeira-computing.pt/contacts/ > Acesso em 1 novembro 2019.

MITCHELL, Bradley. **As camadas do modelo OSI ilustradas.** 2019. Disponível em: <https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017 > Acesso em: 25 novembro 2019.

MOREIRA, Esdras. **Os 5 itens que os melhores firewalls corporativos devem ter.** dez. 2016. Disponível em: <https://introduceti.com.br/blog/os-5-itens-que-os-melhores-firewalls-corporativos-devem-ter>. Acesso em: 03 agosto 2019.

OLIVEIRA, Yuri. **O modelo OSI e suas camadas**. jan, 2018. Disponível em: <https://www.alura.com.br/artigos/conhecendo-o-modelo-osi >. Acesso em: 30 agosto 2019.

PALMA, Fernando. **As normas da família ISO 27000.** dez, 2018. Disponível em: <https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html>. Acesso em 1 novembro 2019.

RAZA, Muhammad. **Modelo OSI e suas 7 camadas.** Jun. 2018. Disponível em: <https://www.bmc.com/blogs/osi-model-7-layers/> Acesso em: 27 agosto 2019.

ROUSE, Margaret. **Firewall de próxima geração (NGFW)**. Disponível em: <https://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW>Acesso em 20 julho 2019.

ROUSE, Margaret. **Confidencialidade, integridade e disponibilidade (tríade da CIA).** Disponível em: <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> Acesso em: 30 agosto 2019.

ROUSSEY, Benjamin. **O que são princípios de segurança da informação?** dez. 2017. Disponível em: <https://www.ostechnical.com/information-security-principles/> Acesso em 30 agosto 2019

SANTOS, Andre. **Principais dispositivos de uma rede de computadores.** set. 2016. Disponível em: <https://www.uniaogeek.com.br/principais-dispositivos-de-uma-rede-de-computadores-p1/> Acesso em: 20 agosto 2019.

SANTOS, José. **O Modelo OSI**. Nov. 2004. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php> Acesso em 20 agosto 2019.

SOPHOS CERTIFIED ENGINEER. **Module 2: getting started with XG Firewall**. Disponível em: <https://v6.netexam.com/Courses5/11017/89889/117762/251138/12_11_2017_7_01_07_AM/ET802-v17.0.0-Getting-Started-XG-Firewall-Engineer.pdf>. Acesso em: 01 novembro 2019.

SOPHOS. **Lista de categorias de Gateway da Web.** Disponível em: <https://community.sophos.com/kb/en-us/123333>. Acesso em: 12 novembro 2019.

TACIO, Paulo. **OS Melhores sniffers gratuitos.** Fev, 2011. Disponível em: <http://www.mundodoshackers.com.br/top-5-os-melhores-sniffers-gratuitos> Acesso em 1 novembro 2019.

TRIPLAIT. **Novas funcionalidades do firewall Sophos XG V17.Triplait, 2017b**. Disponível em: < https://triplait.com/novas-funcionalidades-do-firewall-sophos-xgv17/#.WzEhBadKjGg />. Acesso em: 28 outubro 2019.

VENTURA, Plinio. **O modelo OSI e suas 7 camadas.** mai. 2014. DIsponível para em: <https://www.ateomomento.com.br/o-modelo-osi-e-suas-7-camadas/> Acesso em: 25 agosto 2019.

VERISIGN. **Proteção DDoS.** 2018. Disponível em: <https://www.verisign.com/pt_BR/security-services/ddos-protection/syn-flood/index.xhtml> Acesso em: março 2019.

ZURIER, Steve. **Os tipos mais recentes de firewalls mesclam NGFW e recursos de análise de ameaças.** Disponível em**:** <https://searchnetworking.techtarget.com/feature/Latest-types-of-firewalls-merge-NGFW-and-threat-analysis-features > Acesso em: 23 julho 2019.