ANTONIO MENEGHETTI FACULDADE - AMF

CURSO DE SISTEMAS DE INFORMAÇÃO

ANDRÉ REDIN CELLA

A IMPORTÂNCIA DE UM FIREWALL EM AMBIENTE CORPORATIVO COM A FERRAMENTA SOPHOS

RESTINGA SÊCA/RS

2018

ANDRE REDIN CELLA

A IMPORTÂNCIA DE UM FIREWALL EM AMBIENTE CORPORATIVO COM A FERRAMENTA SOPHOS

Trabalho de Conclusão de Curso-Monografia apresentado como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação, Curso de Graduação em Sistemas de Informação, Faculdade Antonio Meneghetti-AMF.
Orientador: Prof. José Luiz Rodrigues Filho

RESTINGA SÊCA/RS

2018

AGRADECIMENTOS

RESUMO

Com o início da internet banda larga conexões e a navegabilidade do usuário são cada vez mais rápidas o que permite se comunicarem, compartilharem informações e realizar infinitas tarefas diferenciadas. Entretanto, com os benefícios também chegaram novos tipos de ameaças. A disseminação de vírus, os ataques de hackers a todo tipo de computador, seja pessoal ou corporativo, estão maiores do que nunca. Sendo assim a cada ano o número de ataques cibernéticos via internet aumenta drasticamente, principalmente através de conexões móveis (celulares, tablets e objetos que conectam a internet). Para combater esses ataques, as empresas necessitam ter um firewal configurado para reduzir as ameaças virtuais, bem como a visibilidade sobre o uso da internet e produtividade, além de aprimorar a disponibilidade do recurso de internet em ambiente corporativo. Desta forma tem-se por objetivo pesquisar os benefícios trazidos por uma ferramenta XG firewal, em relação ao rendimento por parte dos colaboradores, o aumento da segurança, a otimização do uso da rede e o gerenciamento dos usuários. Este trabalho pretende assim, esclarecer o funcionamento de um XG firewal e demonstrar os benefícios trazidos por uma ferramenta de gerenciamento unificada voltada para a proteção de redes em um ambiente corporativo, executando simulações de ataques e vírus.

Palavras-chave: Firewal, Internet, Segurança ,XG Firewal Ataques cibernéticos.

ABSTRACT

With the coming of broadband internet, connections are getting faster, more accessible for users to browse, communicate, share information, and perform endless differentiated tasks. However, since nothing in life occurs the way we want it, benefits also come with new types of threats. The spread of viruses, hacking attacks on all types of machines, whether personal or corporate, are greater than ever. So every year the number of cyber attacks via the internet increases drastically, mainly through mobile connections (cell phones, tablets and objects that connect the internet). To combat such attacks, companies need to have a well-configured firewall to reduce virtual threats as well as visibility into internet usage and productivity, as well as improve the availability of the Internet resource in a corporate environment, where it aims to research the benefits brought by an XG firewal tool, both in revenue by employees, increased security, optimization of network usage and management of users. This article aims to clarify the operation of an XG firewal and demonstrate the benefits brought by a unified management tool aimed at protecting networks in a corporate environment, running simulations of attacks and viruses.

Keywords: Firewal, Internet, Safety, XG Firewal, Cyber attacks.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

TCP/IP – *Transmission Control Protocol/Internet Protocol*

UTM - *Unified Threat Management* (tratamento unificado de ameaças)

TI – Tecnologia da Informação

Proxy – ferramenta utilizada no controle de acesso à WEB

Spyware – software espião, geralmente com o objetivo de roubar dados

Malware – software mal-intencionado causa danos ao computador

VPN – *Virtual Private Network* (rede virtual privada)

IPS – *Intrusion Prevention System* (sistemas de prevenção de intrusos)

DMZ - *Demilitarized Zone (zona desmilitarizada)*

LAN – *Local Area Network* (rede local/interna)

XG – *Next Generation (Sophos)*

Whatsapp – aplicativo móvel para troca de mensagens de texto e arquivos multimídia.

SUMÁRIO

1 INTRODUÇÃO

Na internet existe uma infinidade de conteúdo, alguns trazem vários benefícios ao ambiente corporativo, mas existem os que podem afetar esse ambiente. Assim, tendo um firewal corporativo configurado de forma satisfatória, ou seja, criando políticas de acesso para usuários, os que falta de experiência ou por agir de má fé acabam acessando conteúdos inadequados. E-mails com anexos maliciosos, ou até *URLs* (Localizador Uniforme de Recursos) com malwares similares, podem ser bloqueadas e evitadas com um firewal corporativo. Sendo assim, o usuário que tentar acessar um endereço bloqueado pelo firewall não conseguirá continuar com a conexão, protegendo seu ambiente e sua estação de trabalho.

Com um firewal funcionando corretamente a redução de ameaças oferece um ambiente mais puro e disponível, evitando parar a empresa em atividade pela ação de vírus e derivados, podendo assim impactar em toda a rede corporativa, prejudicando um número de colaboradores e enormes prejuízos para o negócio.

1.1 PROBLEMA DE PESQUISA

Mostrar como implementar um firewal juntamente com seu antivírus e a importância de ter um firewal bem configurado em sua empresa, para evitar ataques, quedas de internet e congestionamento na rede.

1.2 OBJETIVOS

Para responder o problema apresentado anteriormente, esta pesquisa apresenta os seguintes objetivos.

1.2.1 Objetivo geral

Mostrar como uma infraestrutura de TI (Tecnologia da informação) dentro de um ambiente corporativo pode ser melhorada com o uso da ferramenta Sophos. Fazer uma análise dos resultados obtidos para comprovar sua eficácia e esclarecer como uma rede pode ser melhorada com a utilização dos recursos aplicados de forma consciente, sem falta nem excesso de engenharia.

O trabalho pretende demonstrar que com apenas uma ferramenta unificada é possível fazer o mesmo trabalho que antes era feito por um conjunto de ferramentas para

controlar o acesso de conteúdo web (websites e aplicações específicas) bem como a segurança da rede, executando simulações de ataques e vírus.

1.2.2 Objetivo específicos

- Apresentar o conceito de firewalls de nova geração e centrais unificadas de gerenciamento de ameaças (UTMs) (*Unified Threat Management*).
- Mostrar a real importância de um firewal para um negócio;
- Explicar a redução de ameaças virtuais que o ambiente corporativo terá com um firewal;
- Analisar como pode ter um aumento de produtividade e disponibilidade em um ambiente corporativo com um firewal.

1.3 JUSTIFICATIVA

A escolha do tema partiu de um interesse pessoal com o conhecimento de que várias empresas possuem problemas de segurança de informação, ataques cibernéticos e até mesmo maus uso da internet no ambiente de trabalho.

A maioria das empresas sofrem ataques diariamente, onde em alguns casos essas empresas que não possuem nenhum firewal (no caso empresas pequenas), sendo muito vulnerável para ataques, derrubando seu servidor ou até melhor só roubando informações sem você saber que ele tem acesso a sua rede.

O intuito deste trabalho é facilitar o entendimento de como essa ferramenta de segurança unificada funciona, quais os benefícios trazidos, como são aplicados filtros, bloqueios, regras para acesso a aplicações web, bem como mostrar o resultado final por meio de gráficos que possam comprovar seus benefícios.

2 ABORDAGEM TEÓRICA

Esta seção tem por objetivo abordar os tópicos de interesse do corrente trabalho, os quais são importantes para desenvolver os objetivos do trabalho, tanto para a pesquisa quanto para o produto.

2.1 Sophos

A Sophos é uma desenvolvedora e fornecedora de software e de hardware de segurança, incluindo antivírus, *antispyware*, antispam, controle de acesso de rede, software de criptografia e prevenção de perda de dados para *desktops*, servidores para proteção de sistemas de e-mail e filtragem para *gateways* de rede.

Fundada em 1985 pelo Dr. Peter Lammer e o Dr. Jan Hruska, Sophos é uma empresa privada e sediada em Abingdon, Oxfordshire, Inglaterra e Burlington, Massachusetts, Estados Unidos. A empresa tem subsidiárias e escritórios na Austrália, Benelux, Canadá, França, Alemanha, Áustria, Itália, Japão, Singapura e Espanha. A empresa tem aproximadamente 1.800 funcionários em todo o mundo. Ao contrário de outras empresas de segurança, a Sophos não produz antivírus e soluções antispam para usuários domésticos, mantendo seu foco sempre no mercado empresarial (SOPHOS, 2017).

O console de gerenciamento tem *interface* pela Web permite o gerenciamento simples e consolida toda a estrutura de segurança: Alguns módulos que o produto oferece (BASSO, 2015):

- *Endpoint Protection* – software antivírus para computadores, com definição de políticas para manter os usuários seguros.
- *Rede Firewal Essencial* – um *firewal* para impedir ataques que levam à perda ou roubo de dados, infecções e outros incidentes que custam tempo e dinheiro. Os recursos de proteção do *firewal* são projetados para simplificar a entrada de dados e controle de tráfego de saída.
- *Rede de Proteção* - permite a configuração flexível de site para site e de acesso remoto VPN, protege contra-ataques de negação de serviço, *worms* e de ataques de hackers sofisticados com exploits através de uma proteção contra intrusão de forma totalmente integrada.
- *Email Protection* – protege o e-mail corporativo de *spams* e vírus.

- *Web Shield* – permite aplicar um filtro de navegação web para proteger os trabalhadores contra as ameaças da Web e controlar a forma como gastam seu tempo online.
- *Proteção de servidor Web* – protege o seus servidores e aplicações web contra-ataques sofisticados, perda de dados, entre outros.
- *Wireless Protection* – Torna as redes sem fio mais segura e confiável.
- *Clientes VPN* – criar um acesso facilitado para se conectar a uma VPN.

2.1.2 O que é e como funciona um firewall

Firewal é basicamente o que há entre o nosso computador e a internet. É um software capaz de gerenciar regras de entrada ou saída. As regras nele configuradas são as regras que podem permitir ou negar a entrada ou saída de protocolos, categorias de conteúdo ou endereços IP (*Internet Protocol*) válidos ou inválidos (MICROSSOFT, 2017).

O Firewal segue as regras e configurações determinadas e realizadas pelo administrador de redes, determinando assim as políticas de segurança que o firewal irá tomar, onde será instalado após o link da internet, ele podendo ser montado de acordo com a figura abaixo.

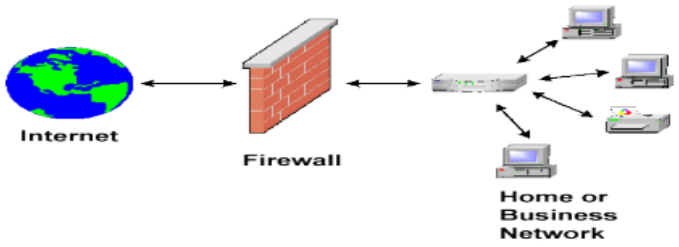

Figura 1 - Ilustração de um Firewall.
Fonte: IMGBUDDY, 2015.

2.1.3 Redes e Endereços IP

Endereço de IP válido significa um endereço IP da grande internet, onde a empresa ou residência do usuário possui um IP somente para ela. Como ter um IP "próprio" tem um custo adicional, pois o número de endereços IP não é infinito, normalmente os provedores ou operadoras de internet entregam o acesso web para os clientes através de um IP inválido (FEY, 2007).

Essa entrega só é possível através da criação de uma sub-rede, assim, o IP válido normalmente é configurado em um servidor e todos os demais computadores da sub-rede acessam a internet através dele. (CISCO, 2016)

Podemos dizer quem um firewall é um muro em que toda informação de uma rede local deve passar antes de entrar ou sair. Comum em todo computador, o firewall tem objetivo de aplicar uma política de segurança, filtrando o que entra e o que sai, proporcionando assim segurança para o usuário. (FELIPE, 2007)

No momento em que um firewall verifica toda informação que passa por ele (entra ou sai do computador para a rede), automaticamente fecha-se o cerco contra invasões. Ele fecha todas as portas de acesso, que são onde os serviços comunicam-se. A partir desse ponto, somente esses computadores e portas autorizadas são os que podem ter comunicação (MORIMOTO, 2006)

Na prática obviamente um firewall não bloqueia todas as portas de comunicação, pois assim um computador perderia a sua utilidade.
Também há o firewall que é instalado em cada computador, este, comumente é chamado de firewall pessoal.

É importante esclarecer que o uso de um firewall não é garantia de proteção completa, sendo assim, prevenção, uso de software antivírus e bom senso sempre são medidas bem-vindas quando falamos em segurança. (MORIMOTO, 2006)

2.1.4 Firewal Proxy

Proxy é um servidor que centraliza pedidos de um usuário para outros servidores. A figura 3 mostra o procedimento de um proxy ativo.

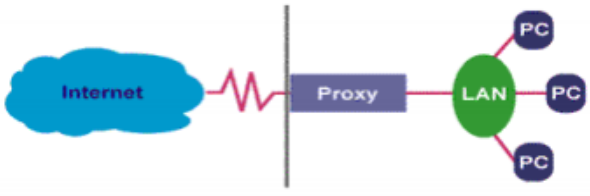

Figura 2 - Ilustração de um proxy em funcionamento.
Fonte: ORACLE, 2015.

O proxy serve como um filtro. Todas os pedidos passam pelo servidor proxy, que tem a função de analisar o que o usuário está pedindo, redirecionando até o destino ou não.

2.2 XG Firewal

XG Firewal (*Next Generation*) é um termo de segurança de informações que se refere a uma única solução de segurança, e normalmente é um único dispositivo de segurança que oferece várias funções de segurança em um único ponto na rede.

Normalmente, um dispositivo de UTM inclui funções como: antivírus, antispyware, antispam, firewal de rede, detecção e prevenção de intrusão, filtragem de conteúdo e prevenção de vazamento (KASPERKY, 2017).

A primeira ação tomada durante a implantação da ferramenta no ambiente é dividir a rede, sempre observando o escopo do projeto e respeitando a disponibilidade do ambiente de trabalho, para que a migração de ferramenta gere o menor impacto possível.

Dividir uma rede significa separá-la por partes, de acordo com a necessidade de desempenho, nível de acesso ou segurança em padrões pré-estabelecidos. Nesse ambiente, a rede de computadores foi dividida em três: DMZ, LAN e rede pública.

DMZ: também conhecida como Zona Desmilitarizada. Fica localizada entre uma rede interna e uma rede externa (intranet e internet). Na forma ideal, é destinada aos servidores, assim é possível fazer com que o IP da rede externa seja redirecionado ao servidor da rede interna (que está na zona DMZ) para rodar os serviços web.

LAN: é onde ficam todos os demais computadores da rede, rodam sistemas, acessam à internet e fazem acesso aos servidores que ficam na DMZ para a execução dos sistemas de gestão.

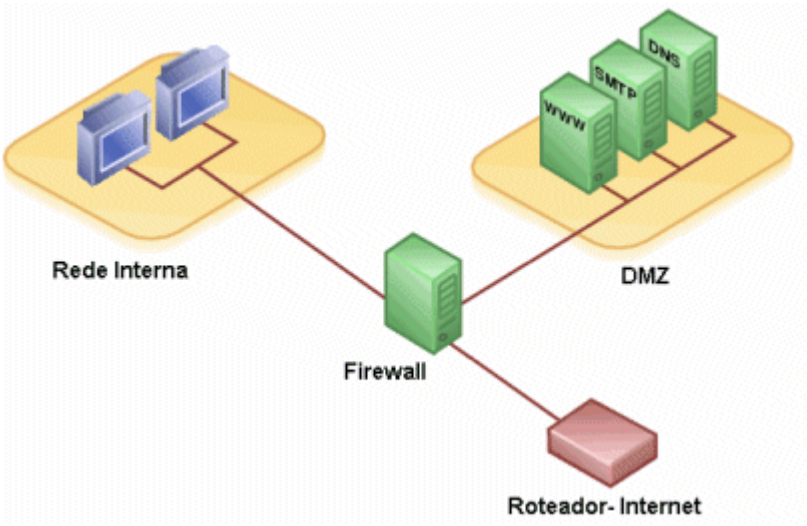

Figura 3 - Modelo padrão de divisão de uma rede.
Fonte: (MAURICIO, 2004)

Rede pública: onde ficam conectados os computadores que não pertencem à organização, geralmente acessada por visitantes, executivos ou pessoas que vem ao local para participar de reuniões. Essa divisão proporciona maior controle, políticas de acesso diferentes e aumenta o nível de segurança.

2.2.1 Sophos Endpoint Protection

Endpoint é uma solução completa para bloquear vírus e proteger seus dados em um único responsável. Ao correlacionar indicadores de ameaças, o Sophos Endpoint pode bloquear exploits, URLs perigosas, aplicativos potencialmente indesejados e códigos maliciosos. Onde quer que seus usuários estejam, Sophos Endpoint é uma solução rápida, eficaz e completa para segurança de seus equipamentos. Desenhado para o mercado corporativo, permite o controle de todas suas funcionalidades em um console (INFOLINK, 2018)

A proteção Endpoint possui as seguintes composições.

- *Proteção Web*, atualizações periódicas de ameaças e listas de URLs maliciosas protegem os usuários contra novas ameaças que surgem a todo momento.
- *Cliente Firewal*, um firewal cliente, gerenciado centralmente, protege seus ativos e bloqueia *worms* e hackers, impedindo invasões.
- *Filtragem de Navegação*, caso deseje você pode também utilizar a Filtragem de Navegação embutida no Sophos Endpoint. Podem ser definidas políticas inteligentes de navegação para 14 principais categorias de sites diretamente no console.
- *Controle de Dispositivos,* a implementação de políticas de uso de dispositivos de armazenamento removível permite uma maior gerência dos dados que entram e saem de sua empresa e reduz a possibilidade de infecção de equipamentos.
- *Prevenção a Intrusão,* o agente analisa em tempo real o comportamento de seus ativos aumentando ainda mais a segurança de suas máquinas, servidores e rede. Esta análise é realizada com um impacto mínimo na performance do equipamento.

- *Criptografia de Disco*, a criptografia *SafeGuard* protege os dados em seus computadores e mídias removíveis. A perda de um notebook não representará mais uma possível fonte de vazamento de informações, pois os dados somente serão acessados com o fornecimento da senha.
- *Controle de Acesso à Rede*, o NAC detecta problemas de configuração, tais como antivírus desatualizados, firewall desativados, sistemas operacionais ou aplicações vulneráveis antes de permitir o acesso destes equipamentos à sua rede. Com esta ferramenta são garantidas as *compliance* de sua política de segurança.
- *Controle de Dados Confidenciais (DLP),* endurece seus servidores e aplicações web para protegê-los contra ataques modernos e perda de dados.

Logo abaixo uma imagem do seu Painel de Controle.

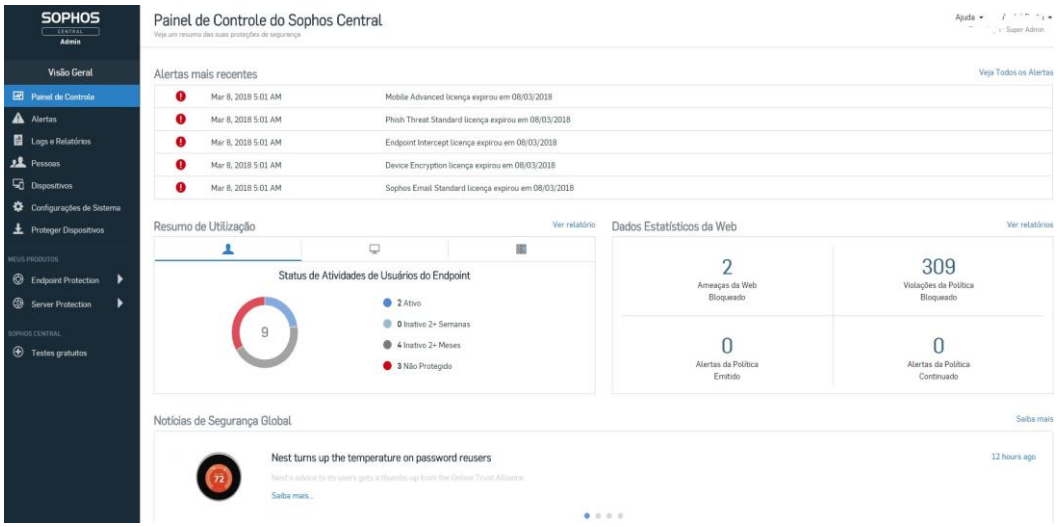

Figura 4 - Painel Sophos Endpoint.
(Prefeitura Municipal de Faxinal do Soturno – RS 2018)

2.2.2 O que um XG firewal pode lhe proporcionar

Filtro de aplicações (*application filter*):

Um filtro de aplicação que serve para que possamos "filtrar" todo tipo de aplicação web. É um método de permitir ou interromper o acesso à determinada categoria ou aplicação de forma coletiva (grupo de aplicativos) ou em específico (somente uma aplicação).

Appliance:

Uma appliance pode ser traduzida na forma mais genérica como "ferramenta". Na informática, as appliances são máquinas (computadores) pré-configurados para executar um trabalho específico. Normalmente as appliances são voltadas para aplicações de automação, caixas registradoras ou de firewall.

Segundo MORIMOTO (2014) pode ser montada em um gabinete específico, e o hardware deve ser o mais parecido possível com um eletrodoméstico, ao contrário do que pode parecer, nem sempre são dispositivos difíceis de construir. Pelo contrário, às vezes é um computador comum que foi montado em um gabinete diferente acoplado a um leitor de código de barras ou o que for necessário para executar suas tarefas.

Um exemplo claro que a maioria conhece são os computadores de caixas dos grandes supermercados, estes são *appliances*.

Reports (relatórios):

Relatórios são sempre importantes no momento da tomada de decisão, às vezes as empresas, por incrível que pareça trocam de sistema simplesmente porque o utilizado não atendia a obtenção de resultados mostrados em relatórios. Afinal, nada melhor que podermos tirar um relatório para demonstrar a eficiência de um trabalho ou ferramenta, comprovando que o trabalho desenvolvido está sendo feito da forma mais eficiente (MORIMOTO, 2014)

Mais adiante veremos como o Sophos é executado e compreendido até mesmo por um usuário mais leigo.

Balanço de carga (*load balance*):

Uma capacidade muito interessante de um XG é trabalhar com balanço de carga. Ela funciona da seguinte forma: é possível ter dois ou mais links de internet trabalhando em conjunto. (TRIPAIT, 2017)

Cada um desses links no balanço de carga pode ter ou seu "peso" configurado, ou seja, o link de maior velocidade geralmente é configurado com um peso maior para ele.

Na prática, isso quer dizer que quanto maior a carga configurada para determinado link, mais tráfego irá chegar à rede por ele.

Para compreender melhor, podemos imaginar o seguinte cenário: No momento em que esse link começa a ficar lento (no limite do tráfego fornecido pelo provedor) automaticamente os computadores na rede do firewal, passam a navegar pelo link alternativo, sem qualquer impacto na navegação web do usuário final. Ainda há a opção de fazer com que usuários ou computadores naveguem por um link específico. Exemplo: no departamento financeiro os computadores usam um link de 15Mbps e no RH usam o link de 10Mb.

A imagem abaixo representa o painel principal da interface web da ferramenta, onde podemos visualizar os detalhes sobre consumo de recursos (processador e memória), bem como regras de firewalls ativas, relatórios, mensagens de alertas e o tráfego na rede, também avisando se o Sophos está configurado corretamente.

Figura 5 - *Painel Sophos Principal Acessado pela Web.*
Fonte: (LOUPEN,2017)

Na parte de autenticação de usuários por padrão os usuários utilizam o nome e o sobrenome com sua própria senha. O objetivo de criar cada usuário é para poder gerenciar o que for acessado pelos mesmos na web, aplicações, relatórios de acesso e consumo de banda, todos esses dados ficam armazenados no disco do equipamento.

Onde veremos na imagem abaixo como funciona a criação de usuários.

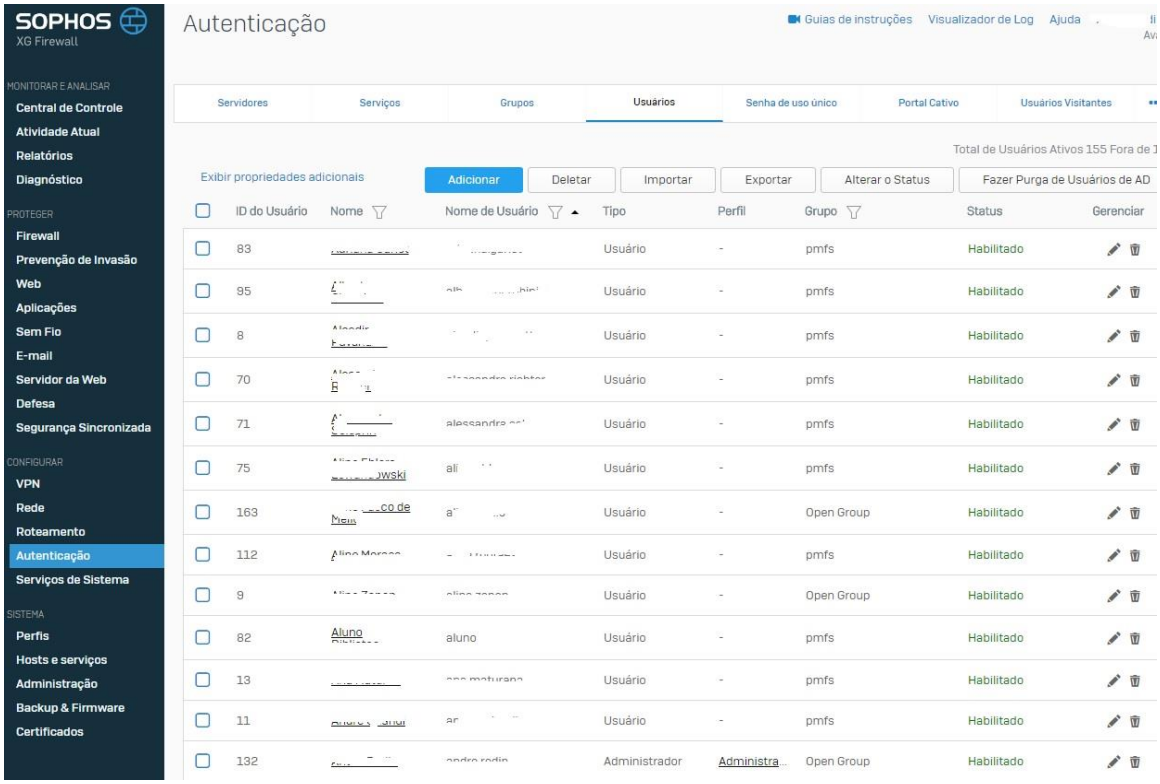

Figura 6 - Parte de Autenticação.
(Painel Sophos - Prefeitura Municipal de Faxinal do Soturno - RS 2018)

Com os usuários criados a configuração parte para as políticas do filtro web. Onde as políticas são criadas com as suas devidas categorias, ou seja, dentro de cada política existem categorias de páginas web. Estas categorias são oriundas de uma lista de classificação. Exemplo: entretenimento, comércio, redes sociais, conteúdo adulto.

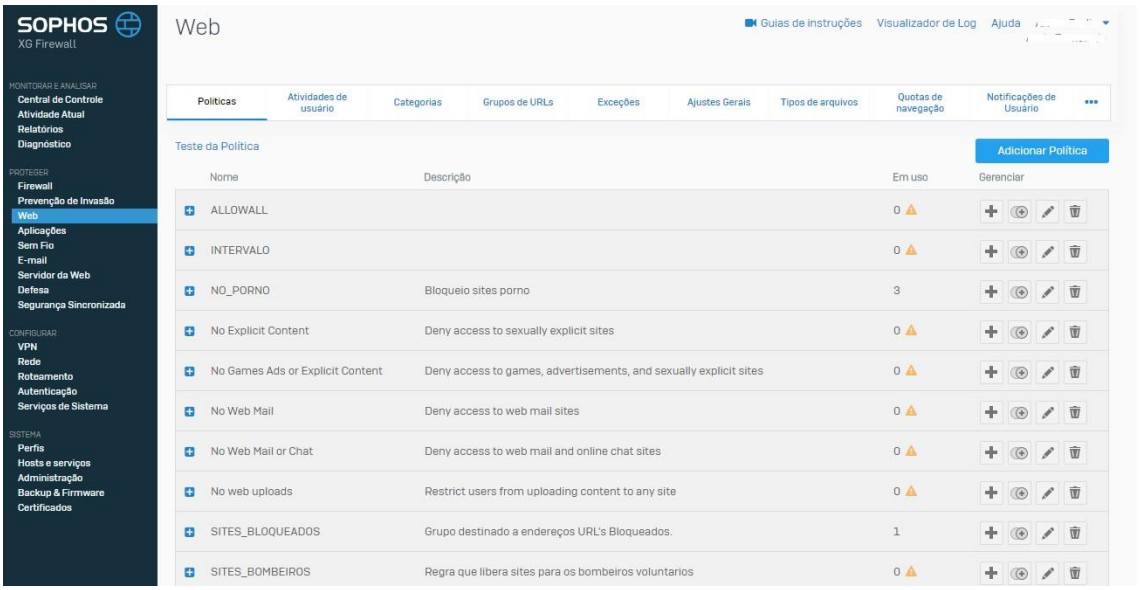

Figura 7 – Aplicações Web.
(Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018)

Estas políticas de acesso web são gerenciáveis no que diz respeito às suas categorias inclusive, é possível criarmos categorias específicas com o endereço dos sites desejados, o sistema faz isso através de endereços de domínio ou palavras-chave.

O Sophos, ainda contribui para monitoramento em tempo real da quantidade de usuários autenticados, horário, tentativas de ataque externa, vírus na rede e transferência de download/upload. Além do mais, podem ser feitos bloqueios por endereço físico (MAC), criar rede virtual privada (VPN) bem como redirecionamento de portas para acesso remoto externo aos servidores.

É importante destacar que as políticas de aplicação com suas devidas categorias podem ser customizadas, porém as categorias de aplicação não podem. Na figura 8 representamos as políticas de aplicação, que foram criadas.

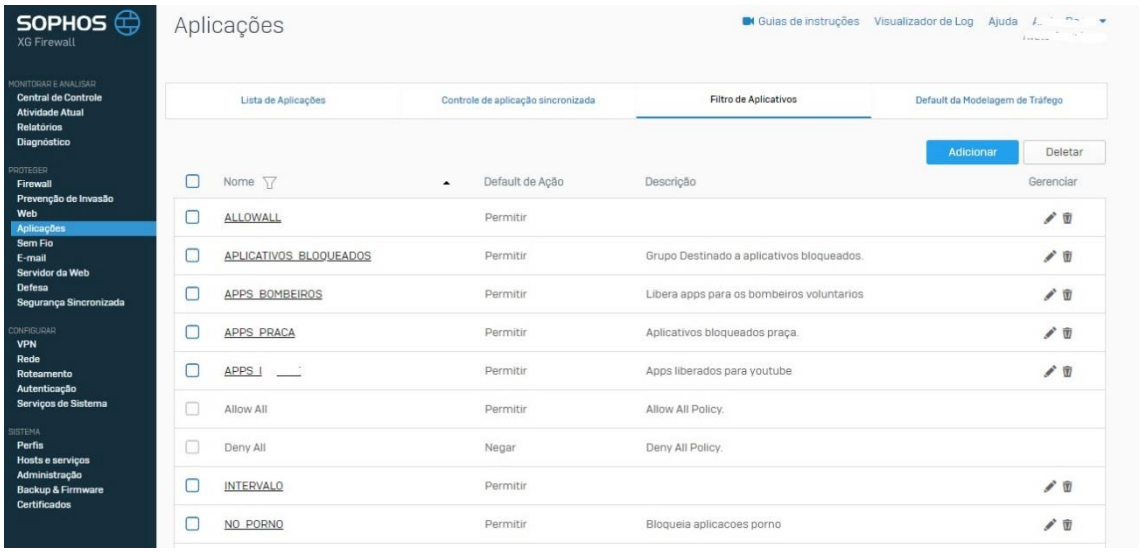

Figura 8 - Políticas de Aplicação.
(Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018)

Pode ser visualizado o que foi adicionado dentro da política de acesso à aplicação "APLICATIVOS_BLOQUEADOS". Onde na figura abaixo verá aplicativos e tipos de arquivos que foram bloqueados.

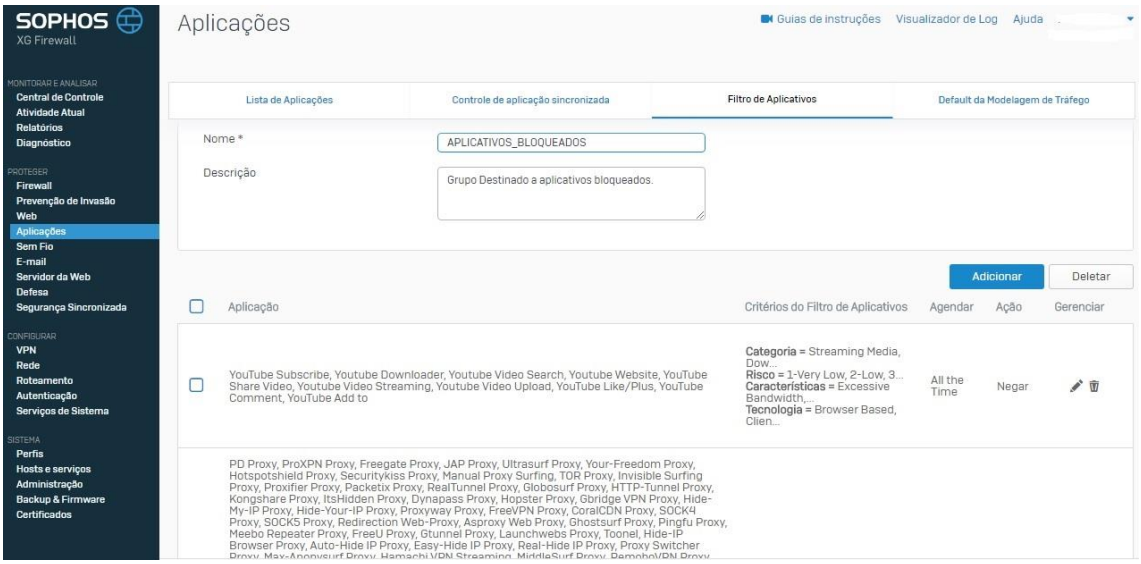

Figura 9 - Interior das Políticas de Aplicação.
(Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018)

Conforme podemos observar na imagem acima, foram bloqueadas as categorias de *streaming* e *proxys*.

2.3 Aplicando os Filtros do XG Sophos

Até agora foi visto como funcionam os filtros web e de aplicação. Más para eles funcionarem precisa ser efetivado os bloqueios no firewall.

No firewall irá permitir ou negar as regras criadas pelo administrador da rede. Dentro do XG existem regras que podem ser parametrizadas para cada zona de rede, tanto quanto (LAN, WAN, DMZ). Os bloqueios de acesso para a maioria dos casos realizados no tráfego da zona LAN para WAN. Abaixo algumas regras de Firewall, por exemplo a LAN ter acesso a DMZ.

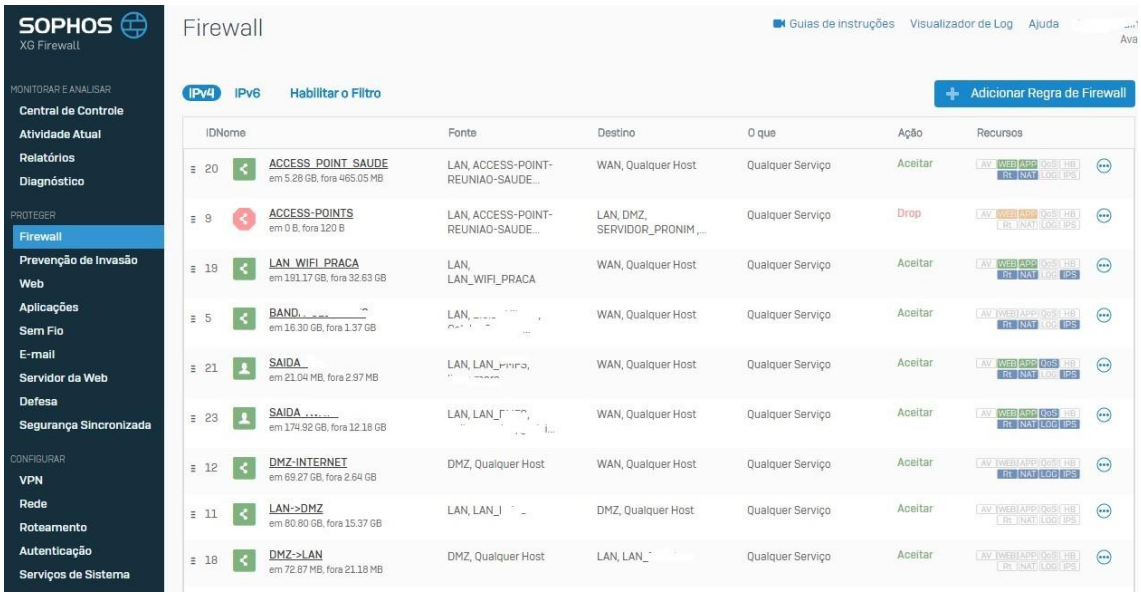

Figura 10 - Regras de Firewall.
(Painel Sophos Prefeitura Municipal de Faxinal do Soturno *- RS 2018)*

2.4 Redirecionamentos

Como a necessidade de acesso externo através dos serviços de área de trabalho remota do Windows, foram criados os redirecionamentos. Um redirecionamento funciona da seguinte forma: ao informar o endereço IP da rede WAN e sua devida porta no assistente de conexão de área de trabalho remota, ele irá fazer uma busca na rede à procura da porta especificada liberada para acesso, então ele passa para a interna que por sua vez possui um IP interno (da rede LAN).

Todo esse processo tem que passar pelo firewall da zona WAN para LAN. A figura 11 ajudas a entender melhor o processo de redirecionamento:

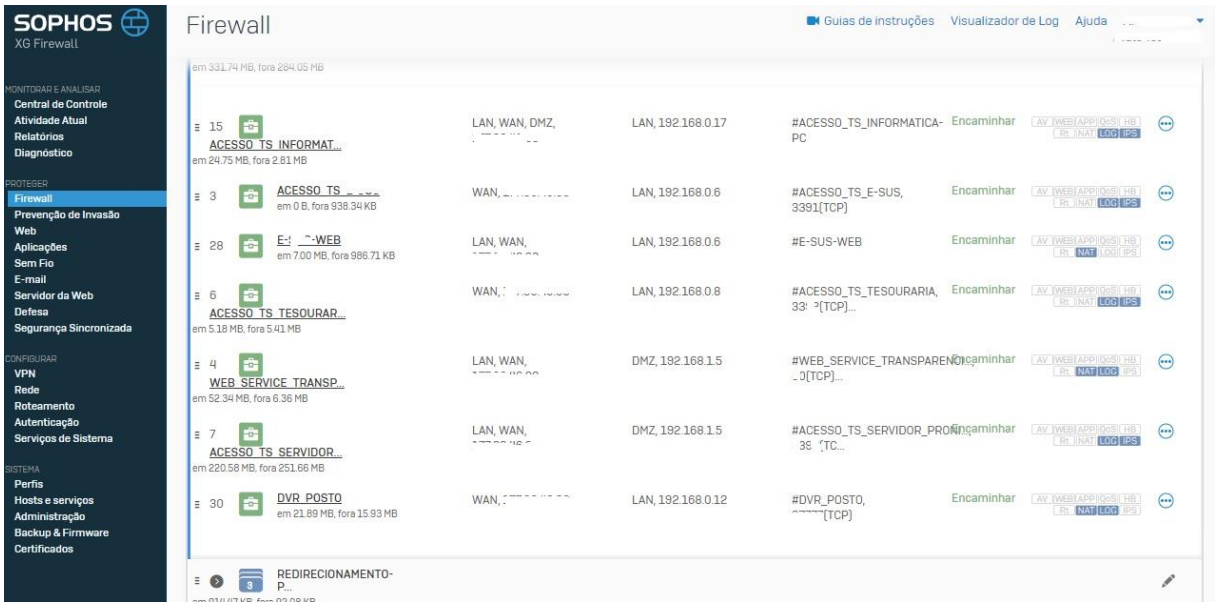

Figura 11 - Redirecionamento Firewall.
(Painel Sophos Prefeitura Municipal de Faxinal do Soturno – RS 2018)

2.5 Simulador e Teste de Regras e Políticas de Firewall

O simulador de teste de regras e de firewall lhe permite simulação instantânea e sem algum esforço de regras de firewall e política de filtragem da web com base no usuário, protocolo, fonte, destino e hora do dia. Esta ferramenta fornece uma maneira rápida e fácil de verificar que uma política ou regra está funcionando como esperado e pode ser uma valiosa ferramenta de solução de problemas no caso de usuários ou o tráfego está sendo inesperadamente bloqueado. (Bär, 2017)

Os resultados do teste de simulação de política ou de regras indicam se o tráfego é permitido ou bloqueado e identifica a regra ou a política da web que está a reger o tráfego. (Bär, 2017), na figura 12 vemos como é feita a simulação.

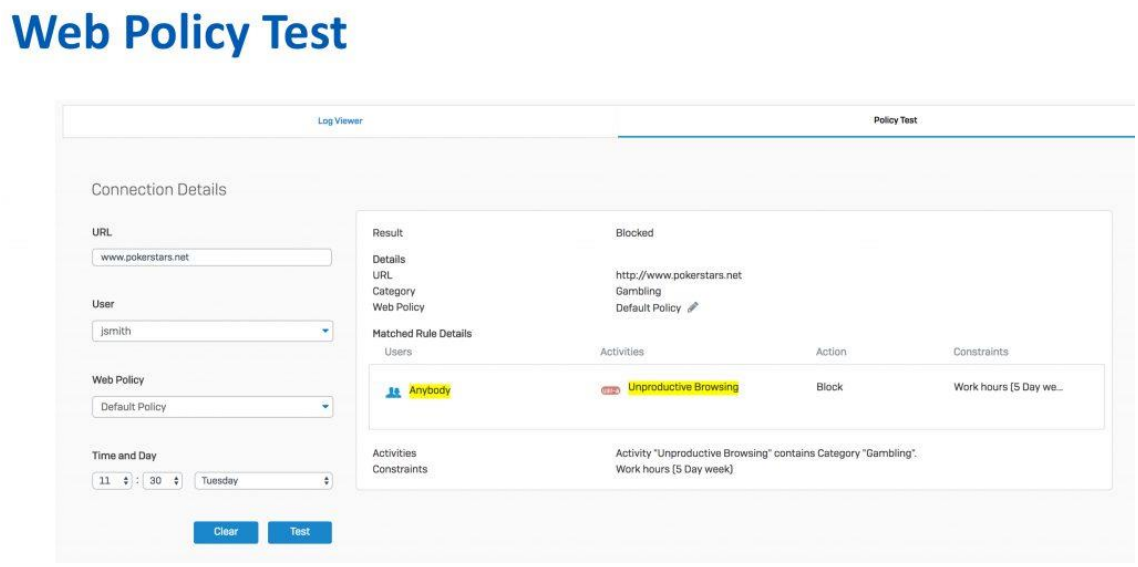

Figura 12 - Simulação e testes de Regras de Firewall. Fonte: TRIPAIT, 2018

3 METODOLOGIA

3.1 METODOLOGIA DE PESQUISA

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 quantitativa-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)

A coleta de dados foi realizada através da aplicação de um questionário, o qual é uma técnica de investigação composta por questões apresentadas por escrito às pessoas, com o propósito de obter determinadas informações (GIL, 1999). Neste questionário foram abordadas questões fechadas, de múltipla escolha e abertas. As questões fechadas são as que se pede aos respondentes para que escolham uma alternativa dentre as questões apresentadas em uma lista. As questões abertas são utilizadas para que os respondentes

se sintam à vontade de escrever com suas próprias palavras, sem se limitarem a escolha entre alternativas definidas pelo autor. (GIL, 1999)

3.2 PORQUE O SOPHOS XG FIREWALL

O Sophos foi escolhido por ser completo para um ambiente de infraestrutura de TI, onde abaixo será citado alguns requisitos que foi levantado.

- *Facilidade de manejo*: as configurações são fáceis de serem manuseadas, contento um *template* ágil. Até mesmo as configurações de regras de bloqueio, limite de banda, podem ser feitas pelo usuário final.
- *Escalabilidade*: com os tempos de hoje, a tendência é sempre aumentar de número de usuários na rede, e a ferramenta consegue suportar bastante carga sem perda de qualidade.
- *Confiabilidade*: por possuir o hardware próprio não haveria preocupação com falhas físicas e muito menos gastos com compra de peças para mantê-lo funcionando.
- *Idioma*: não à limitação no idioma do Sophos, contendo dês da linguagem global (Inglês) até mesmo o português brasileiro.
- *Baseia-se em identidade*: onde a administração dos bloqueios e permissões não fossem efetuados apenas pelo IP do computador, mas por usuário e senha também. Assim torna-se mais fácil a visualização dos *logs* e relatórios. Esse controle através da criação de usuário e senha nos permite que sejam criados grupos de usuário e torna a manipulação das regras mais fácil, esse controle chamado de baseado em identidade.
- *Camada 7 do modelo OSI*: também chamada de *layer 7*. Esta é a camada de aplicação. Corresponde às aplicações (programas) na parte mais elevada da camada OSI, onde é feita a interação entre o computador e o usuário da aplicação. Esta camada também especifica qual protocolo a aplicação utiliza para que aconteça a comunicação. Sete são as do modelo OSI, sendo elas: física, enlace, rede, transporte, sessão, apresentação e aplicação. O conceito da sétima camada de rede é a ferramenta ter capacidade de bloquear uma aplicação específica sem interferir nas demais. (VENTURA, 2014) Exemplo: conseguir bloquear somente o bate papo de uma rede social como o *Facebook*,

ou bloquear somente a transferência de conteúdo multimídia em uma aplicação como o *WhatsApp*. Isto proporciona proteção avançada e com controle por aplicação.

- *Relatórios*: a ferramenta gera relatórios detalhados de acesso, consumo de banda de forma individual e geral. Esses relatórios detalhados baseados em identidade é uma forma de inteligência embarcada que nos ajudam na tomada de decisão, de qual conteúdo bloquear ou liberar, quais os riscos oferecidos pelos acessos, quais os países em que foram realizadas mais buscas.
- *Tráfego*: a ferramenta suporta um alto tráfego de banda junto com as políticas de bloqueio que passa por ela. E está preparada para futuras ampliações sem precisar de alterações ou redimensionamentos.

3.3 PHISH THEART (EXPLICAÇÃO DO ZÉ)

3.4 RANSOMWARE

Ransomware é um tipo de malware que restringe o acesso ao sistema ou certos arquivos e cobra um valor de "resgate" para que o acesso possa ser restabelecido (CARDOSO, 2017)

Ferramentas para desbloquear arquivos criptografados por este tipo de ameaça também estão disponíveis no portal *No More Ransom*. 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*.

3.4.1 RANSIM RANSOMWARE SIMULATOR

O *RanSim Ransomware* Simulator, é um utilitário que simula um ataque de ransomware para testar as defesas do seu PC contra 10 diferentes ameaças: *InsideCryptor*, *LockyVariant*, Mover, *Replacer*, *Streamer*, *StrongCryptor*, *StrongCryptorNet*, *ThorVariant* e *WeakCryptor*.

O utilitário não modifica nenhum arquivo do usuário e é perfeitamente seguro. Depois da conclusão dos testes, ele mostrará quais arquivos teriam sido criptografados se fosse um ataque verdadeiro.

(FALTA IMAGEM DO ENDPOINT REALIZANDO O BLOQUEIO)

3.5 ATAQUES DDOS (FALAR COM O ZÉ)

3.6 TIPOS DE ATAQUES E COMO O XG SOPHOS PROTEGE-SE

3.6.1 Varredura de portas

Este modo de invasão consiste em enviar pacotes para todas portas TCP e UDP de uma máquina afim de descobrir os serviços que estarão sendo executados em estado de escuta. Sendo assim consegue-se determinar qual sistema operacional e quais aplicativos estão sendo executados. (STALLIVIERY, 2011)

Para proteção de caso o XG Sophos impede esse tipo de ataque quando o administrador tem acesso para configurar quais serviços poderão ser visualizados para qualquer programa de varredura.

3.6.2 Roteamento dirigido

Na maioria das vezes a validação de um serviço ou usuário é feito com base no endereço IP da máquina que está se conectando. Com o uso de pacotes direcionados, um atacante pode enviar pacotes para as máquinas da rede interna como se fossem enviados de uma máquina confiável. Desta forma, o atacante consegue estabelecer uma conexão válida para uma máquina da rede interna com os mesmos direitos se estivesse se conectando a partir de outra máquina. (STALLIVIERY, 2011)

Este tipo de ataque é particularmente perigoso em serviços que utilizam apenas endereços IP para fazer a validação de usuários. Um firewall impede este tipo de ataque na medida em que permite que o administrador o configure para recusar todos os pacotes direcionados. (STALLIVEIRY,2011)

Onde a XG Sophos não utiliza somente endereços IP’s para validações, utilizam autenticações.

3.6.3 Ping of Death (POD)

O tamanho de um pacote IPv4 formado corretamente, incluindo o cabeçalho IP, é de 65.535 bytes, incluindo um tamanho total de carga útil de 84 bytes. Muitos sistemas de computadores históricos simplesmente não conseguiam lidar com pacotes maiores, e travariam se recebessem um. Esse bug foi facilmente explorado nas primeiras implementações de TCP / IP em uma ampla gama de

sistemas operacionais, incluindo Windows, Mac, Unix, Linux, bem como dispositivos de rede, como impressoras e roteadores. (IMPERVA, 2018)

Como o envio de um pacote de ping com mais de 65.535 bytes viola o Protocolo da Internet, os invasores geralmente enviam pacotes malformados em fragmentos. Quando o sistema de destino tenta remontar os fragmentos e acaba com um pacote superdimensionado, o estouro de memória pode ocorrer e levar a vários problemas no sistema, incluindo travamento. (IMPERVA, 2018)

Os ataques Ping of Death foram particularmente eficazes porque a identidade do atacante pode ser facilmente falsificada. Além disso, um atacante do Ping of Death não precisaria de nenhum conhecimento detalhado da máquina que estava atacando, exceto pelo seu endereço IP. (IMPERVA, 2018)

(IMPERVA,2018) É digno de nota que esta vulnerabilidade, embora melhor reconhecida por sua exploração por ataques Pingo f Death, pode realmente ser explorada por qualquer coisa que envie um datagrama IP - ICMP, TCP, UDP e IPX.

Para evitar ataques Ping of Deatch a XG Sophos bloqueia mensagens de ping ICMP completamente em seus firewalls.

A Sophos impede este ataque na medida em que ele armazena e monta todos os fragmentos de pacotes IP recebidos, quando um pacote inválido é detectado, ele é descartado.

3.6.4 SYN Flood

3.6.5 Sniffing

4 XG Sophos operando com EndPoint Protection (PRECISA FAZER UM LAB COM O ZÉ)

5 **RESULTADOS**

Referências

BEYTECK, **A importancia de um firewall.** 2015 Disponível em : < https://beytech.com.br/2015/10/21/voce-sabe-a-importancia-de-um-firewall/ >

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social.** 5. Ed. São Paulo: Atlas, 1999.

OSTEC, **Firewall Corporativo**. 2017 Disponível em : < https://blog.ostec.com.br/seguranca-perimetro/firewall-corporativo-importancia-negocio.

KAUARK, Fabiana da Silva; MANHÃES, Fernanda Castro; MEDEIROS, Carlos Henrique. Metodologia da Pesquisa: Um guia prático. Bahia: Via Litterarum Editora, 2010.

MINAYO, Maria Cecília de Souza. O desafio do conhecimento. 11 ed. São Paulo: Hucitec, 2008.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2007.

BSPI, **Firewall Nova Geração** 2017. Disponível em: < http://www.bspi.pt/notiacutecias/utm-e-firewall-de-nova-gerao-conhea-as-diferenas >

PROJETO REDES, **Redes de Perimetro** 2018. Disponível em : < http://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php >.

SOPHOS, **Sobre a Sophos** 2017. Disponível em : http://www.solucoes-sophos.com.br/sobre-a-sophos>.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do Trabalho Científico:** Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2 ed. Novo Hamburgo: Universidade Feevale, 2013.

SOPHOS, **XG SOPHOS**, 2017 Disponível em : < https://www.m3corp.com.br/sophos/sophos-utm-2/ > .

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento.** 11 ed. São Paulo: Hucitec, 2008.

CISCO, **Redes e Ips** 2017, Disponível em : < https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13788-3.html >

GEOCITIES, **Comunicação de Dados**, 2007. Disponível em < http://www.geocities.ws/ndionata/EGIII/material-extra/Comunicacao_de_dados.pdf>.

TRIPLAIT, **Firewall como serviço**, 2017. Disponível em: < http://triplait.com/firewall-como-servico/>.

BARROS, Aidil Jesus Paes; LEHFELD, Neide Aparecida de Souza. **Fundamentos de Metodologia: Um Guia para a Iniciação Científica.** 2 Ed. São Paulo: Makron Books, 2000.

CISCO, **TCP-IP ROUTING**, 2006. Disponível em https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13788-3.html.

INFOLINK, **Sophos Endpoint**, 2018. Disponível em < https://www.infolink.com.br/sophos-endpoint/>.

STREMA, **Sophos Endpoint**, 2018. Disponível em < http://www.strema.com.br/sophos-endpoint/ >.

R7, **Ransomware Simulator**, 2017. Disponível em < http://noticias.r7.com/blogs/seguranca-digital/ransim-ransomware-simulator-v1-1-0-7-20170814 />.

SOPHOS, **Phish Threat**, 2018. Disponível em < https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-phish-threat-datasheet.aspx />.

INCAPSULA, **Ping of Death**, 2018. Disponível em < https://www.incapsula.com/ddos/attack-glossary/ping-of-death.html/>.

MICREIROS, **Técnicas de Invasão**, 2018. Disponível em < http://micreiros.com/tecnicas-de-invasao-entendendo-para-se-proteger/>.

TRIPLAIT, **Novas Funcionalidades Sophos**, 2017. Disponível em < https://triplait.com/novas-funcionalidades-do-firewall-sophos-xg-v17/#.WzEhBadKjGg/>.

TECHTUDO, **Ransomware**, 2017. Disponível em: http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html/>

ATEOMOMENTO, **Modelo OSI**, 2014. Disponível em: <http://www.ateomomento.com.br/o-modelo-osi-e-suas-7-camadas/>