ANTONIO MENEGHETTI FACULDADE – AMF

CURSO DE SISTEMAS DE INFORMAÇÃO

ANDRÉ REDIN CELLA

APRESENTAÇÃO DA IMPORTÂNCIA DE UM FIREWALL EM AMBIENTE PÚBLICO COM A FERRAMENTA SOPHOS

RESTINGA SÊCA, RS

2018

ANTONIO MENEGHETTI FACULDADE – AMF

CURSO DE SISTEMAS DE INFORMAÇÃO

ANDRÉ REDIN CELLA

APRESENTAÇÃO DA IMPORTÂNCIA DE UM FIREWALL EM AMBIENTE PÚBLICO 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. Esp. José Luiz Rodrigues Filho

RESTINGA SÊCA, RS

2018

FACULDADE ANTONIO MENEGHETTI

André Redin Cella

APRESENTAÇÃO DA IMPORTÂNCIA DE UM FIREWALL EM AMBIENTE PÚBLICO 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. Esp. José Luiz Rodrigues Filho

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

Profª Drª Ana Marli Bulegon
Membro da Banca Examinadora
Antonio Meneghetti Faculdade

Profª Ms. Fábio Prass
Membro da Banca Examinadora
Antonio Meneghetti Faculdade

Restinga Sêca, RS, 28 de novembro de 2018.

AGRADECIMENTOS

Agradeço em primeiro lugar à Deus que iluminou o meu caminho durante esta caminhada.

Aos meus pais que me incentivaram e me apoiaram incondicionalmente todos os anos que estive na faculdade.

A minha namorada Brenda El Hamad Souto, que esteve junto comigo durante essa minha caminhada.

A todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta monografia. Em especial ao meu professor orientador e amigo José Luiz Rodrigues Filho que me auxiliou na elaboração deste trabalho, demonstrando paciência e compreensão, sendo assim de grande importância. E também ao coordenador e professor do curso de Sistemas de Informação, Fabio Prass que sempre me auxiliou e me incentivou para a conclusão do curso.

Aos colegas de curso, que fizeram parte dessa trajetória, dividindo momentos de descontração, estudos, discussões, experiências e conquistas.

Aos meus amigos, que sempre estiveram juntos comigo nas alegrias e nas dificuldades.

A Antonio Meneghetti Faculdade, pela oportunidade de fazer o curso proporcionando um ambiente criativo e amigável.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

“Quando tudo parecer dar errado em sua vida, lembre-se que o avião decola contra o vento, e não a favor dele”.

Henry Ford

RESUMO

A história dos computadores, e mais especificamente das redes de computadores, é uma história que versa não apenas o âmbito tecnológico inerente à constituição destas máquinas, mas também conceções acerca da relação entre o ser humano e o computador e entre os próprios seres humanos. A noção do computador enquanto medium de comunicação e das redes de computadores como uma tecnologia potencialmente emancipadora a um nível humano, social e político foram ideias desenvolvidas paralelamente ao próprio desenvolvimento tecnológico dos computadores ligados em rede. Com o surgimento da internet e posteriormente da banda larga, as conexões e a navegabilidade do usuário tornaram-se cada vez mais rápidas, o que torna necessária a comunicação entre eles para que possam tornar necessária a comunicação entre eles e compartilhar informações e também realizar infinitas tarefas nos mais diferentes segmentos e atividades. Com os benefícios da internet, ter em mãos acesso virtual a quase todo tipo de informação, também chegaram novos tipos de ameaças virtuais. A disseminação dos vírus para sistemas computacionais, o ataque de hackers em qualquer tipo de dispositivo, sem mais limitação geográfica, seja pessoal ou corporativo, estão maiores deste a data de dezembro de 2017, segundo a Karpersky o brasil é, de longe, o país latino-americano mais afetado pela epidemia de ransomware que se propagou em 2017. O país sofreu 55% do total de ataques com este tipo de vírus este ano, quase o dobro da soma do México (23%) e Colômbia (5%). Sendo assim a cada ano o número de ataques cibernéticos via internet aumenta exponencialmente, principalmente através de conexões móveis (celulares, tablets e objetos que conectam a internet). Com este crescente torna-se necessário um meio de controle e mensuração. Desses ataques, as organizações necessitam ter um firewall 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 firewall, 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 firewall 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: Firewall. Internet. Segurança. XG firewall. Ataques cibernéticos.

ABSTRACT

The history of computers, and more particularly computer networks, is a story that is not only a technological support inherent in the performance of these machines but also concepts about the relationship between the human being and the computer and between the main humans. The notion of the computer as a medium of communication and computer networks as a potentially emancipatory technology on a human, social and political level were ideas developed in parallel with the very technological development of networked computers. With the emergence of the internet and later broadband, the connections and the navigability of the user have become increasingly faster, which makes it necessary to communicate among them so that they can make communication between them and share information and also make infinite tasks in different segments and activities. With the benefits of the internet, having virtual access to almost every type of information, new types of virtual threats have also arrived. The spread of viruses to computer systems, hacking attacks on any type of device, with no more geographical limitation, whether personal or corporate, are higher than the date of December 2017, according to Karpersky Brazil is by far, the Latin American country most affected by the ransomware epidemic that spread in 2017. The country suffered 55% of all attacks this year, almost double the sum of Mexico (23%) and Colombia (5%). Thus every year the number of cyber attacks via the internet increases exponentially, mainly through mobile connections (cell phones, tablets and objects that connect the internet). With this growth, a means of control and measurement is necessary. Of these attacks, organizations need to have a firewall set up to reduce virtual threats, as well as visibility into Internet usage and productivity, and improve the availability of the Internet resource in the corporate environment. In this way, the objective is to investigate the benefits brought by an XG firewall tool, in terms of employee performance, increased security, optimization of network usage and user management. This work intends to clarify the functioning of an XG firewall and demonstrate the benefits brought by a unified management tool aimed at protecting networks in a corporate environment by running simulations of attacks and viruses.

Keywords: Firewall. Internet. Safety. XG firewall. Cyber attacks.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

DMZ – *Demilitarized Zone (zona desmilitarizada)*

DNS – *Domain name System* (Sistemas de domínios)

IP – Internet *Protocol*

FTP – *File Transfer Protocol*

UDP – *User Datagram Protocol*

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

TCP – *Transmission Control Protocol/*

TI – Tecnologia da informação

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

XG – *Next Generation (Sophos)*

SUMÁRIO

1 INTRODUÇÃO

Na rede mundial de computadores, que denominamos internet, existe uma infinidade de conteúdo, alguns trazem vários benefícios ao ambiente corporativo, mas existem os que podem afetar esse ambiente. Assim, tendo um firewall 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 (*Uniform Resource Locators*) com malwares similares, podem ser bloqueadas e evitadas com um firewall 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 o uso de uma ferramenta de controle de acesso e mitigação de vulnerabilidades, ou seja, um firewall, operando corretamente a redução de ameaças oferece um ambiente mais puro e disponível, evitando parar as operações da organização, seja ela pública ou privada, diminuindo assim sua capacidade de produção 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

Qual é a necessidade de ter um controle de acessos a mitigação de ataques de rede e internet e também a importância de ter um firewall 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.

1.1.1 Objetivo geral

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.

1.1.2 Objetivos específicos

- Apresentar o conceito de firewalls de nova geração e uma proteção completa da próxima geração com o XG Firewall;
- Mostrar a real importância de um firewall para um negócio;
- Explicar a redução de ameaças virtuais que o ambiente corporativo terá com um firewall;
- Analisar como pode ter um aumento de produtividade e disponibilidade em um ambiente corporativo com um firewall.

1.2 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 mau uso da internet no ambiente de trabalho.

A maioria das organizações sofrem ataques diariamente, onde em alguns casos essas empresas que não possuem nenhum firewall (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 FIREWALL ANTES DO SOPHOS

2.1.1 O que é e como funciona um Firewall

Firewall 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 (TECMUNDO, 2017).

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

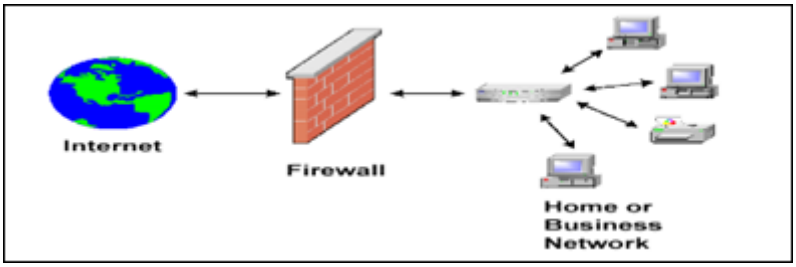


Figura 1: Ilustração de um firewall. Fonte: IMGBUDDY, 2015.

2.1.2 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 (CISCO, 2016).

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 que 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, 2005).

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, 2005).

2.1.3 Firewall Proxy

Proxy é um servidor que centraliza pedidos de um usuário para outros servidores. A figura 2 mostra o procedimento de um proxy ativo.

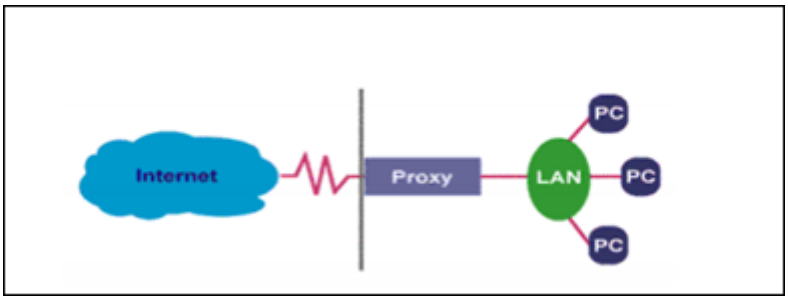


Figura 2: Ilustração de um proxy em funcionamento. Fonte: ORACLE, 2015.

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 TIPOS DE ATAQUES E AMEAÇAS A REDE

2.2.1 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). Exemplos conhecidos incluem o CryptoLocker, CryptoWall, CTBLocker, CoinVault e Bitcryptor.

Segundo a Malwarebytes (2018) 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.

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* (MALWAREBYTES, 2018)

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.

2.2.2 Ataques DDOS

O ataque distribuído de negação de serviço, conhecido como DDoS (*Distributed Denial of Service* em inglês), um computador mestre pode gerenciar até milhões de computadores, chamados de "zumbis".

Segundo a Canaltech (2017), por meio do DDoS, o computador mestre escraviza várias máquinas e as fazem acessar um determinado recurso em um determinado servidor todos no mesmo momento. Assim, todos os zumbis acessam juntamente e de maneira ininterrupta o mesmo recurso de um servidor. Levando em consideração que os servidores web possuem um número limitado de usuários que se podem atender ao mesmo tempo, esse grande número de tráfego impossibilita que o servidor seja capaz de atender a qualquer

pedido. O servidor pode reiniciar ou mesmo ficar travado dependendo do recurso que foi vitimado.

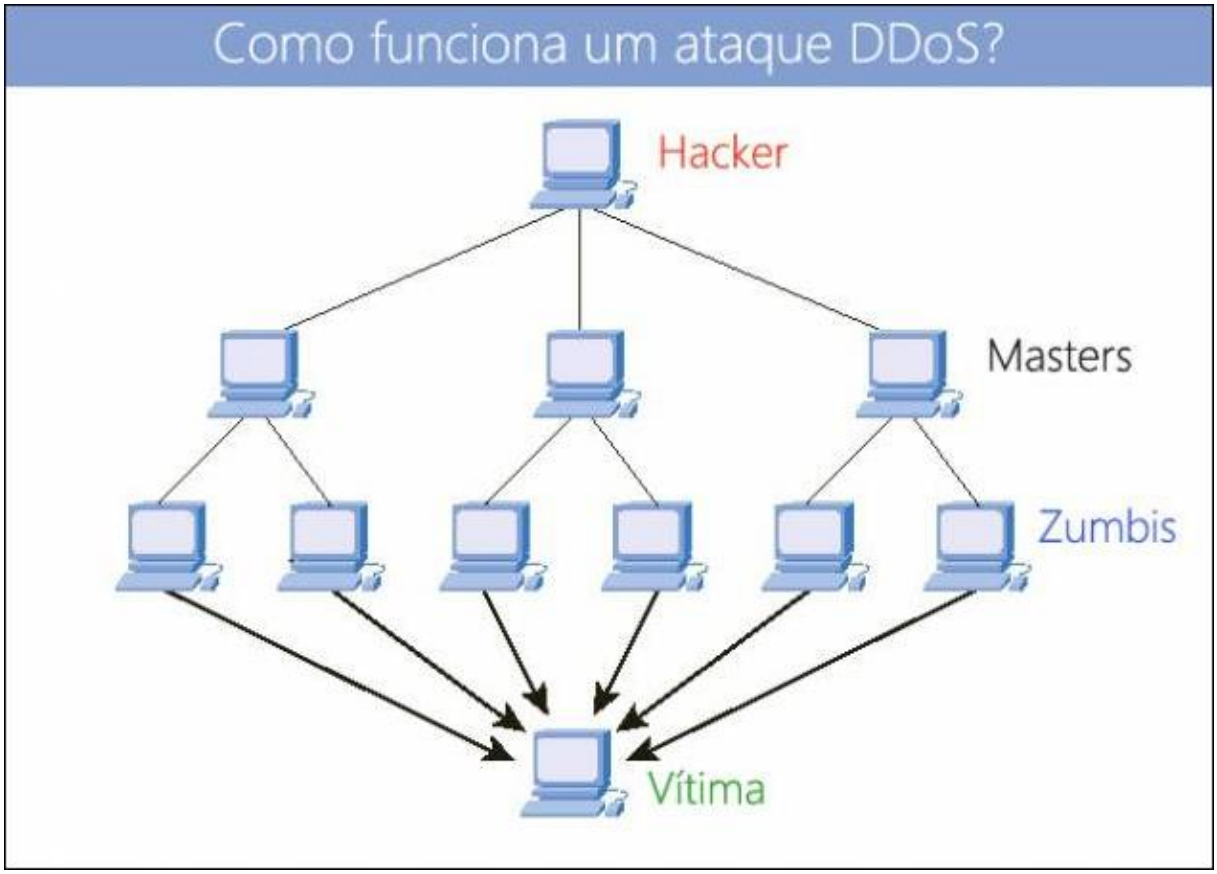


Figura 3: Funcionamento de um ataque DDoS. Fonte: CANALTECH (2017).

Se o computador estiver enviando pacotes sem que o usuário esteja acessando algum serviço na Internet, isso pode ser um indício de que a máquina é um zumbi. Também, a Internet pode ficar lenta mesmo sem a realização de várias tarefas simultâneas na rede (CANALTECH, 2017).

2.2.3 Varredura de portas

Este modo de invasão consiste em enviar pacotes para todas portas TCP e UDP de uma máquina a fim 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. (DUARTE, 2016).

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.

2.2.4 Ping o’ death

Um pacote de ping também pode ser malformado para executar um ataque de negação de serviço, enviando pacotes de ping contínuos para o endereço IP de destino. Um ping contínuo causará estouro de buffer no sistema de destino e fará com que o sistema de destino falhe, e muitas vezes usam o comando CMD “Ping” para verificar principalmente se um servidor ou um gateway está instalado e funcionando. Mas o comando ping também pode ser usado para outras finalidades (SHEKHAR, 2016).

Segundo a Shekhar (2016), se olharmos para o nível básico, então um pacote de ping é geralmente de tamanho de 56 bytes ou 84 bytes (incluindo o cabeçalho IP também). No entanto, um pacote de ping também pode ser feito com até 65536 bytes. Bem, esse é o lado negativo do pacote de ping. Quando aumentamos o tamanho do pacote de ping de forma não natural, formando um pacote de ping malformado para atacar um sistema de computador, esse tipo de ataque é chamado de ataque “Ping da morte”.

Onde abaixo mostrarei a imagem abaixo, isto é apenas para fins educacionais. Não é nada bom, mas você pode usá-lo para aprender.

Figura 4: Comando Ping of Death sendo executado em um sistema Windows.

Salvando o arquivo em .bat e executando, o comando executará muitos pings para o atacado.

2.2.5 SYN Flood

Inundação SYN é um método de ataque DDoS de camada 4 que explora os recursos de conexão TCP de um servidor. Normalmente, o cliente e o servidor estabelecem uma conexão TCP com um acordo de "três vias" (VERISIGN, 2017).

1. O cliente solicita a conexão com o servidor e envia uma mensagem SYN (sincronizar);
2. O servidor reconhece a mensagem SYN e responde com uma mensagem SYN-ACK (sincronizar-reconhecer);
3. O cliente responde com uma ACK (mensagem de reconhecimento), estabelecendo a conexão.

Durante um ataque de inundação SYN, um cliente do agressor enviar várias mensagens SYN ao servidor-alvo. O servidor cria um registro em sua tabela de conexão para cada SYN recebido e responde a todos com uma mensagem SYN-ACK. O agressor pode não enviar uma mensagem ACK, mas muitas vezes falsificar o endereço IP do cliente nos pacotes SYN para que as respostas SYN-ACK do servidor-alvo nunca sejam recebidas. À medida que o agressor continua a enviar mensagens SYN, as tabelas de conexão do servidor-alvo ficam cheias, e o servidor não pode mais responder a nenhuma solicitação de conexão. Com todos seus recursos consumidos, o servidor-alvo não consegue se conectar com clientes legítimos, o que gera uma negação de serviço (VERISIGN, 2017).

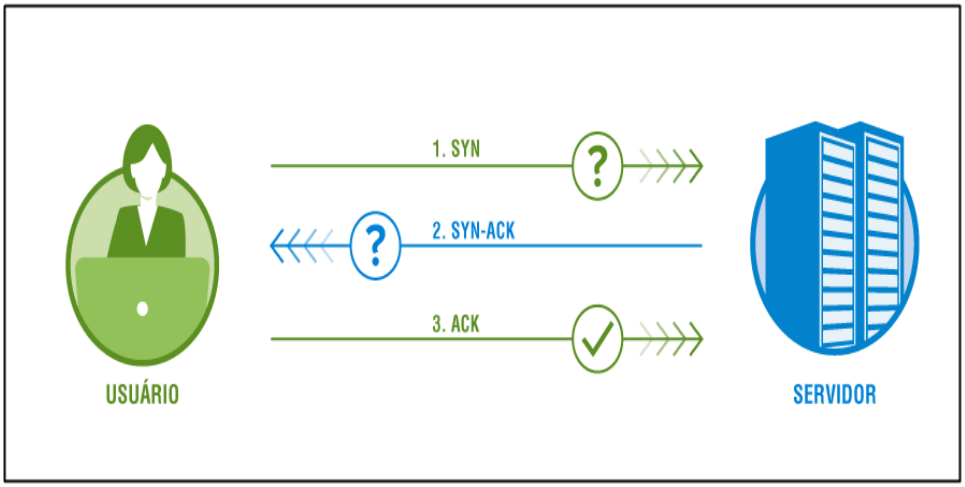


Figura 5: Syn-ACK em operação normal. Fonte: (VERISIGN, 2017).

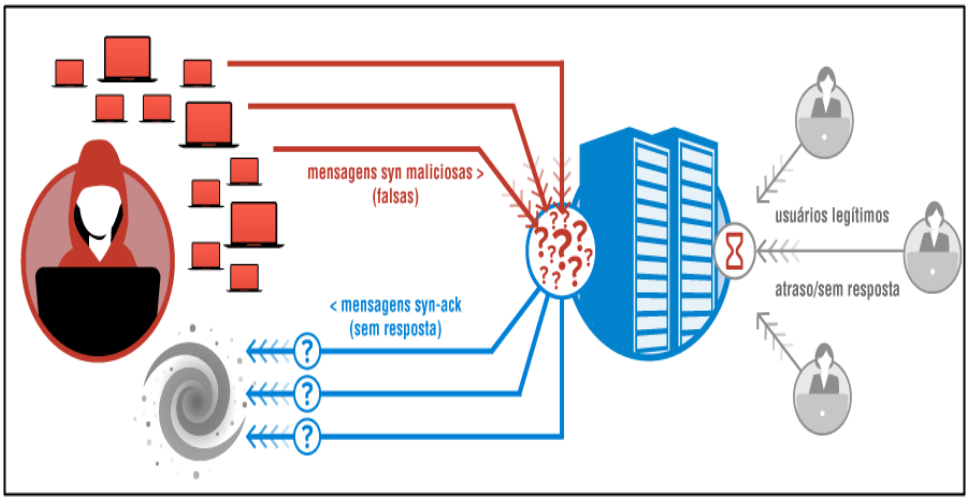


Figura 6: Ilustração Inundação SYN. Fonte: (VERISIGN, 2017).

2.2.6 Sniffing

Sniffing é o processo de monitorar e capturar todos os pacotes que passam por uma determinada rede usando ferramentas de sniffing. É uma forma de “tocar os fios do telefone” e conhecer a conversa. É também chamado de escutas telefônicas aplicadas às redes de computadores (TACIO, 2011)

Há tanta possibilidade de que, se um conjunto de portas de comutação de empresas estiver aberto, um de seus funcionários possa farejar todo o tráfego da rede. Qualquer pessoa

no mesmo local físico pode se conectar à rede usando um cabo Ethernet ou se conectar sem fio a essa rede e farejar o tráfego total (GREYCAMPUS, 2018).

Em outras palavras, o Sniffing permite que você veja todos os tipos de tráfego, protegidos e desprotegidos. Nas condições certas e com os protocolos corretos em vigor, uma parte atacante pode coletar informações que podem ser usadas para novos ataques ou para causar outros problemas para a rede ou o proprietário do sistema (TACIO, 2011).

O que pode ser cheirado?

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

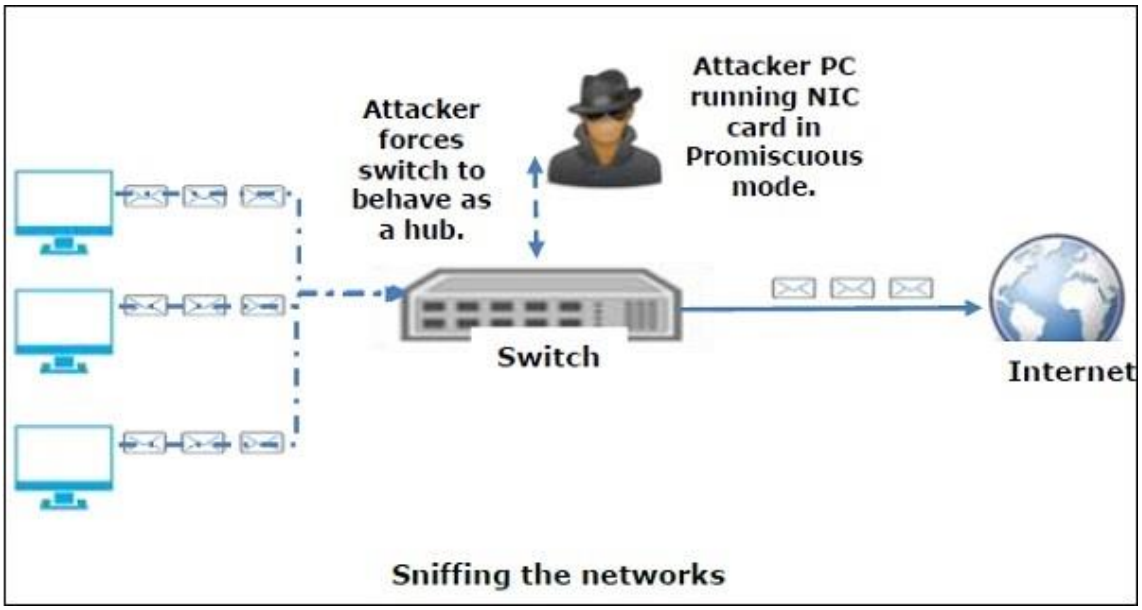


Figura 7: Ilustração de como funciona um ataque Sniffing. Fonte: (MADEIRA, 2018).

Segundo a Verisign um sniffer pode monitorar continuamente todo o tráfego para um computador através da NIC, decodificando as informações encapsuladas nos pacotes de dados. Existem dois tipos de sniffer, o passivo e o ativo.

- **Sniffer Passivo**: No sniffing passivo, o tráfego é bloqueado, mas não é alterado de forma alguma. O sniffing passivo permite apenas escutar. Funciona com dispositivos

Hub. Em um dispositivo de hub, o tráfego é enviado para todas as portas. Em uma rede que usa hubs para conectar sistemas, todos os hosts na rede podem ver o tráfego. Portanto, um invasor pode capturar facilmente o tráfego (VERISIGN, 2018). A boa notícia é que os hubs estão quase obsoletos hoje em dia. A maioria das redes modernas usa switches. Assim, o sniffing passivo não é mais eficaz.

- **Sniffer Ativo**: No sniffing ativo, o tráfego não é apenas bloqueado e monitorado, mas também pode ser alterado de alguma forma, conforme determinado pelo ataque. O sniffing ativo é usado para detectar uma rede baseada em switch. Envolve a injeção de pacotes de resolução de endereços (ARP) em uma rede de destino para inundar a tabela de memória endereçável por conteúdo (CAM). O CAM mantém o controle de qual host está conectado a qual porta (VERISIGN, 2018).

Essas são as técnicas de sniffing que estão ativas são, inundação de MACS, ataques DHCP, envenenamento de DNS, ataques de falsificação, envenenamento ARP. Protocolos como o TCP / IP foram testados e comprovados que nunca foram projetados tendo em mente a segurança e, portanto, não oferecem muita resistência a possíveis intrusos (TACIO, 2011).

2.3 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:

- *Endpoint Protection* – software antivírus para computadores, com definição de políticas para manter os usuários seguros.

- *Rede firewall Essencial* – um *firewall* 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 *firewall* 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.

2.4 XG FIREWALL

XG firewall (*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, firewall de rede, detecção e prevenção de intrusão, filtragem de conteúdo e prevenção de vazamento (SOPHOS, 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.
- Rede pública: onde ficam conectados os computadores que não pertencem à organização, geralmente acessada por visitantes, executivos ou pessoas que vêm ao local para participar de reuniões. Essa divisão proporciona maior controle, políticas de acesso diferentes e aumenta o nível de segurança.

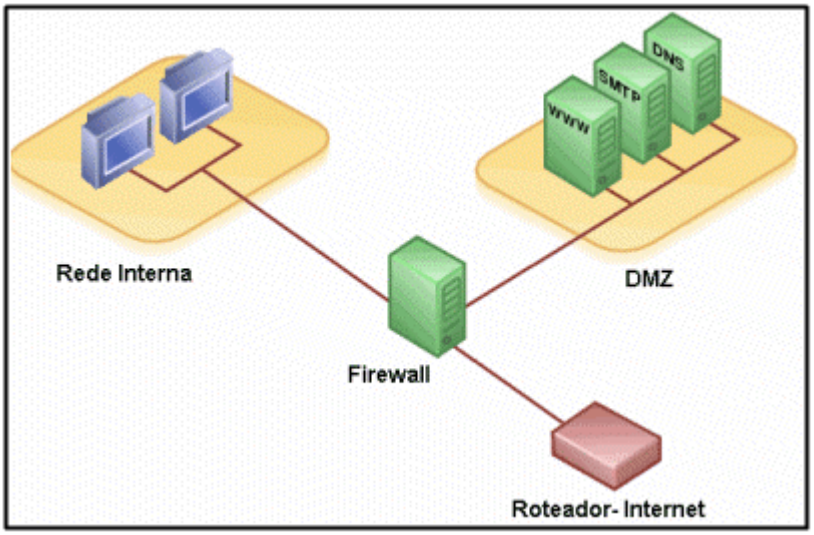


Figura 8: Modelo padrão de divisão de uma rede. Fonte: (MAURÍCIO, 2004).

2.4.1 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 firewall*, um firewall 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.

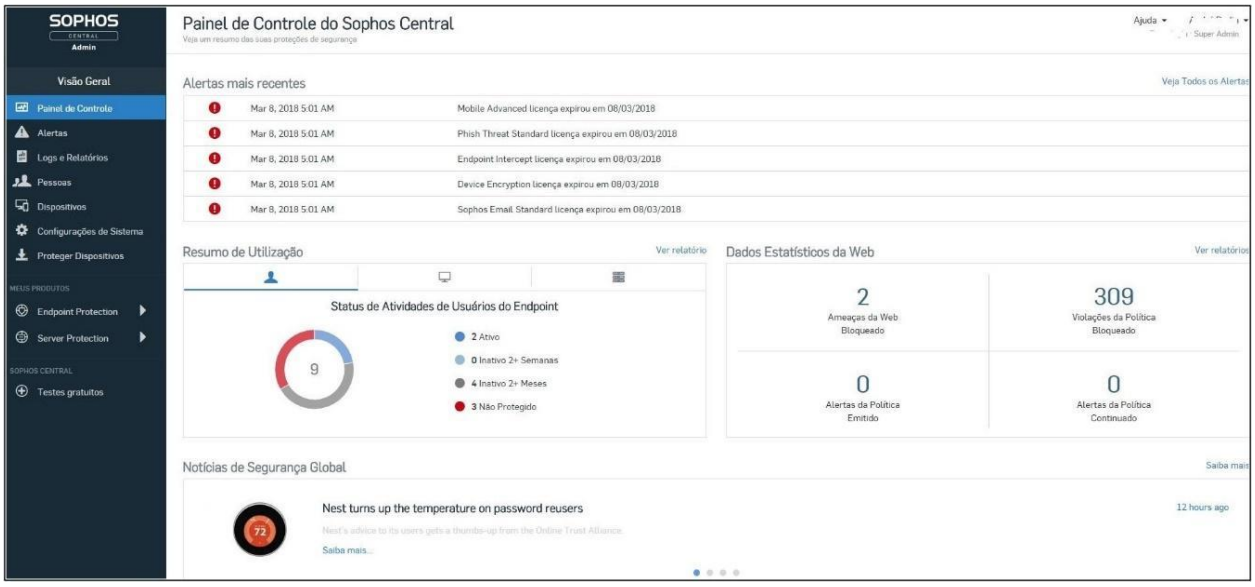


Figura 9: Painel Sophos Endpoint. (Prefeitura Municipal de Faxinal do Soturno - RS, 2018) Fonte: (LOUPEN,2017)

2.4.2 O que um XG firewall pode proporcionar

2.4.2.1 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).

2.4.2.2 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*.

2.4.2.3 Relatórios (*reports*)

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.

2.4.2.4 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. (TRIPLAIT, 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 firewall, 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.

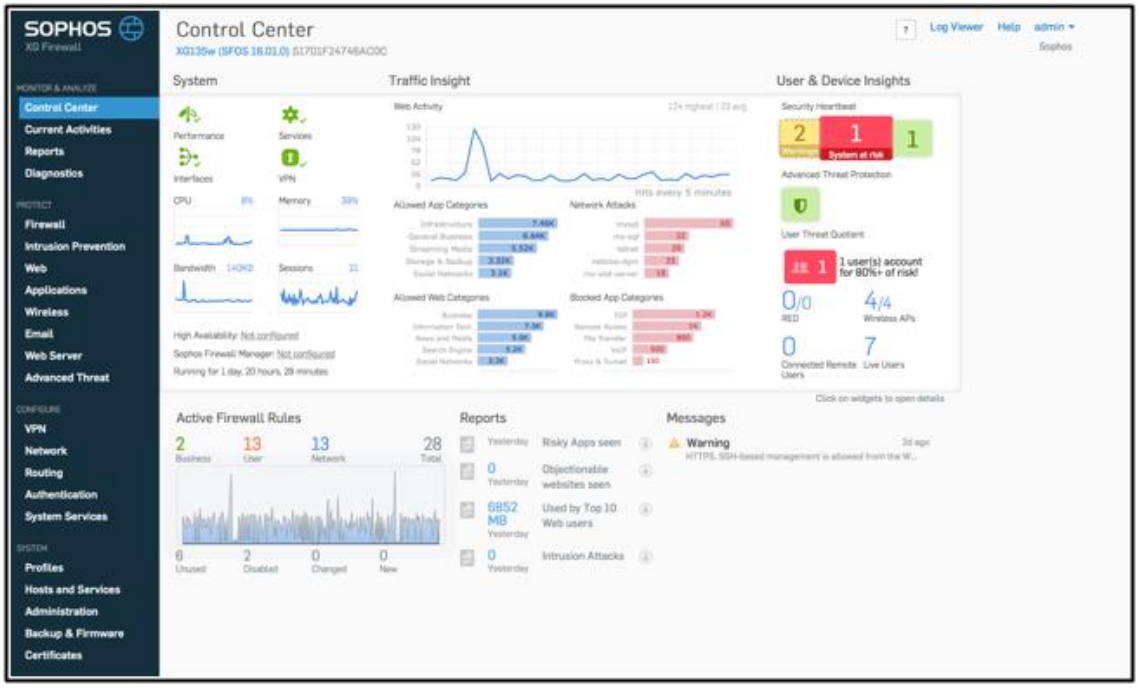


Figura 10: Painel principal Sophos Acessado pela Web. Fonte: (LOUPEN, 2017).

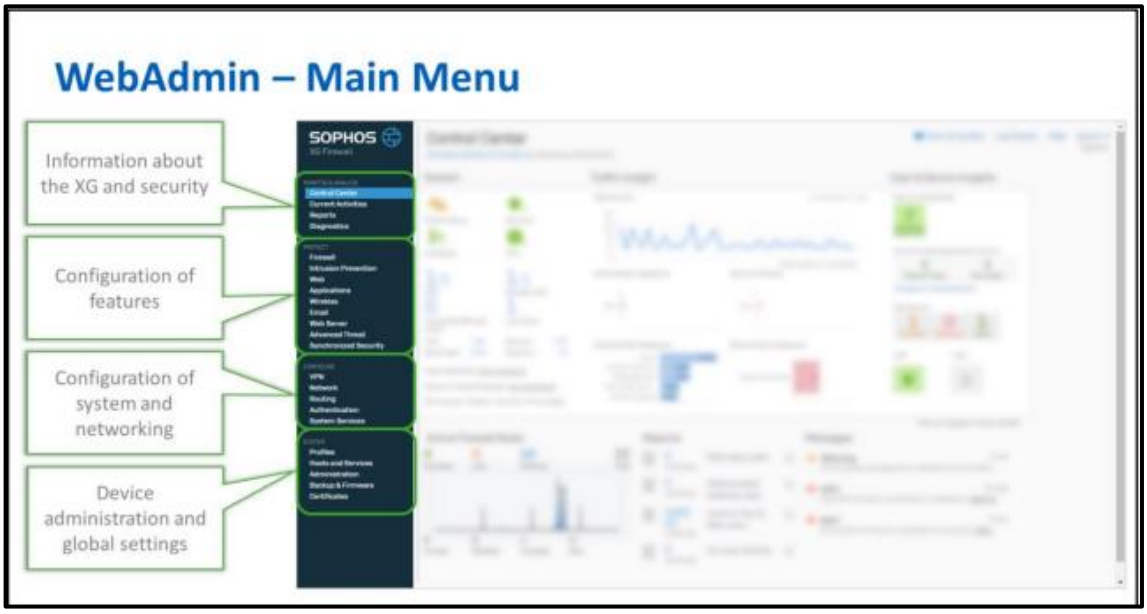


Figura 11: Menu Principal. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Além de ter vários itens que podem ser clicados dentro do centro de controle, o método principal de navegar na interface WebAdmin do firewall XG é o menu principal no lado esquerdo da tela. Aqui encontramos vários links que nos permitirão navegar muito rapidamente entre os diferentes módulos do XG Firewall. Um rápido resumo dos principais tópicos inclui:

A seção monitorar e analisar, que contém links para informações e descobertas relacionadas a usuários e o dispositivo. Podemos monitorar o comportamento do usuário e os recursos do sistema nessa área. O grupo Protect inclui links que nos permitem configurar muitas das políticas e módulos que será usado para proteger a rede. De políticas básicas de firewall a proteção avançada contra ameaças e filtragem de web e aplicativos, todos os módulos de proteção podem ser encontrados dentro.

Na seção configurar, encontramos vários links para serviços fornecidos pelo XG relacionados a rede, autenticação e conectividade. VPNs e roteamento são encontrados aqui, bem como autenticação de serviço de diretório e opções de log.

O grupo final, a seção Sistema, contém várias definições e opções do sistema operacional. Coisas como definições de cronograma e cotas de tráfego, assim como definições de ser encontrado dentro, mas também a Autoridade de Certificação XGs e banco de dados são acessíveis a partir deste grupo. Para completar, importantes opções administrativas, como licenciamento e opções de backup a configuração e atualização do firmware também são encontradas aqui.

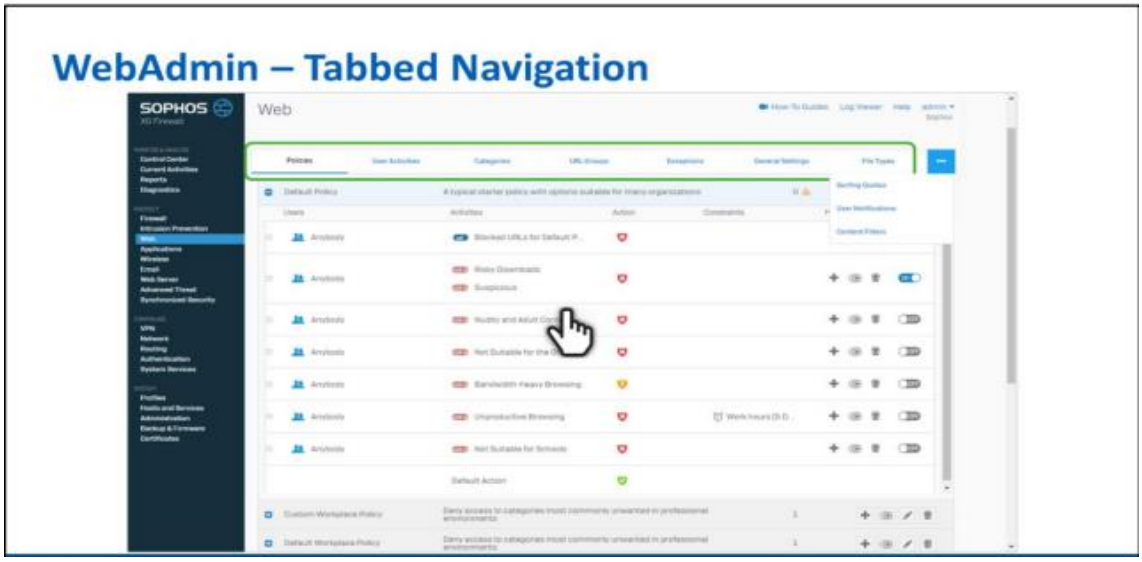


Figura 12: Configurações Web. Fonte: (SOPHOS CERTIFIED ENGINEER,2018).

Depois de selecionar um tópico na área do menu principal, como Web encontrado em PROTECT, você pode achar que existem itens de menu adicionais na forma de um layout com guias no topo a tela. Esses links de navegação com guias podem ser usados para alternar entre as diferentes seções do tópico principal selecionado. Se a tela não for larga o suficiente para mostrar todos os itens do menu, será exibido no final da linha com guias (SOPHOS CERTIFIED ENGINEER, 2018).

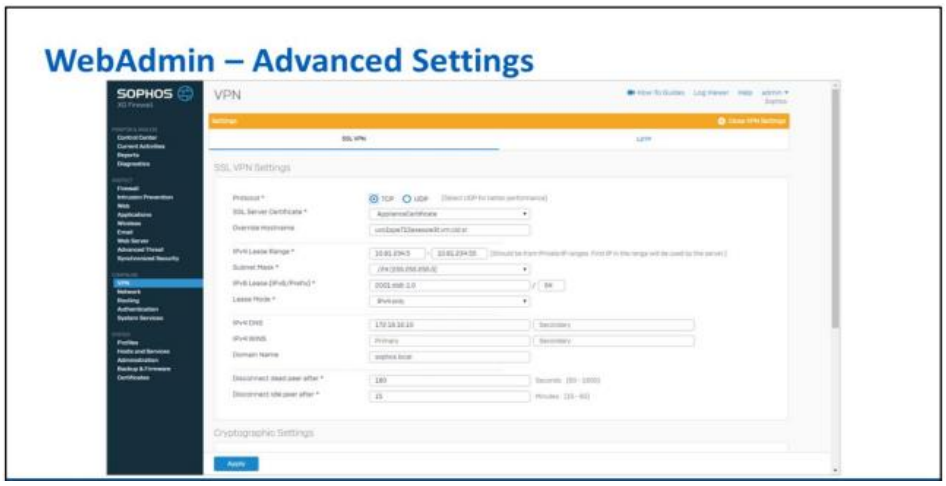


Figura 13: Parte de configuração de VPN. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Segundo (LAMMER, 2017) encontrados em Relatórios e telas de VPN são opções adicionais como mostrar configurações de VPN ou mostrar configurações de relatórios que permitem ao administrador acessar algumas opções menos usadas relacionadas a relatórios ou configuração de VPN. Como pode ser visto aqui, quando a opção de menu no canto superior direito é clicada, a tela irá alternar para as opções adicionais e essa tela de configurações especiais pode ser identificada pela barra de título amarela na parte superior da página.

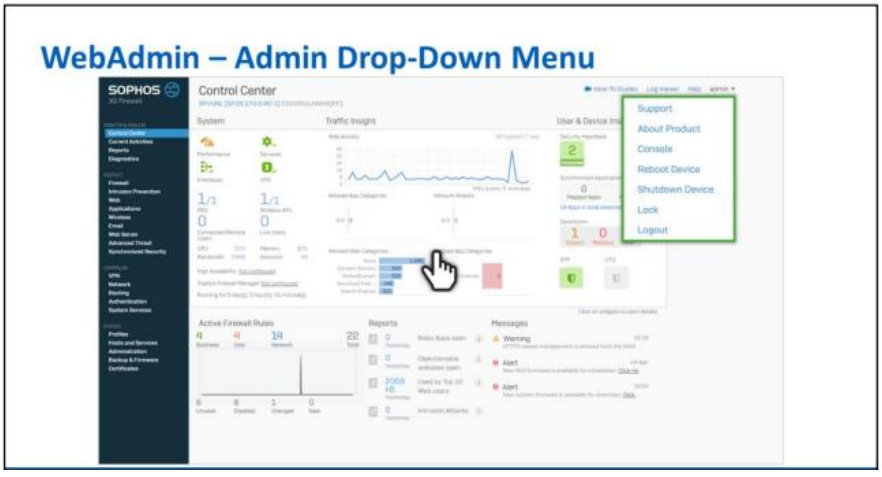


Figura 14: Menu de Ajuda Sophos. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Encontrado ao lado do item de menu de ajuda está o menu admin. Este menu contém uma lista de opções muito úteis, incluindo um link para o site de suporte técnico Sophos, uma janela do console para inserir comandos CLI no firewall XG, opções para reinicializar, desligar, bloquear ou efetuar logout do firewall XG e até mesmo um maneira de iniciar o assistente de inicialização que foi oferecido durante a instalação inicial do firewall XG (SOPHOS CERTIFIED ENGINEER, 2018).

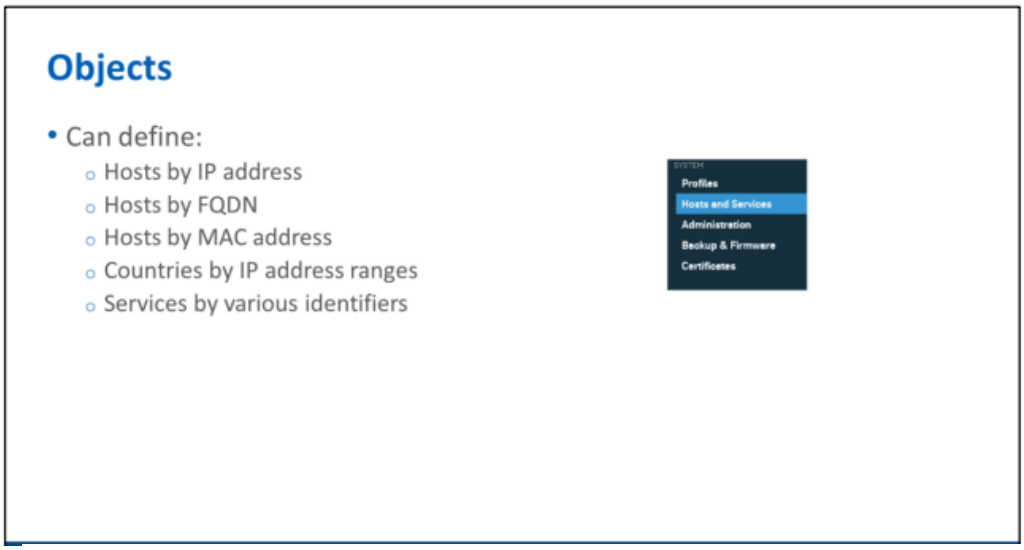


Figura 15: Objetos de definição. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

O Sophos XG Firewall é um sistema orientado a objetos que permite aos administradores criar objetos reutilizáveis que podem representar hosts, serviços, redes ou até mesmo países inteiros SOPHOS, 2016. Esses objetos podem ser usados em várias regras em todo o XG Firewall e fornecer uma visão visual das várias regras e políticas criadas. Esses mesmos objetos também facilitam a implementação de alterações na configuração da rede. Se um objeto for modificado, todas as regras que usam esse objeto também serão atualizadas com a nova configuração.

Objetos são criados nos Hosts e Serviços, que são encontrados sob o cabeçalho SYSTEM. Muitos administradores passam pelo processo de criação de vários objetos ao configurar o firewall Sophos XG. Muitas vezes, existem vários hosts e serviços que eles sabem que precisarão criar regras, bem como redes, como as VLANs, que não estão diretamente conectadas ao dispositivo. Se esses itens forem conhecidos com antecedência, eles poderão ser criados antes que quaisquer regras ou políticas sejam adicionadas e possam economizar tempo e confusão

Abaixo vamos mostrar os tipos de objetos e suas opções.

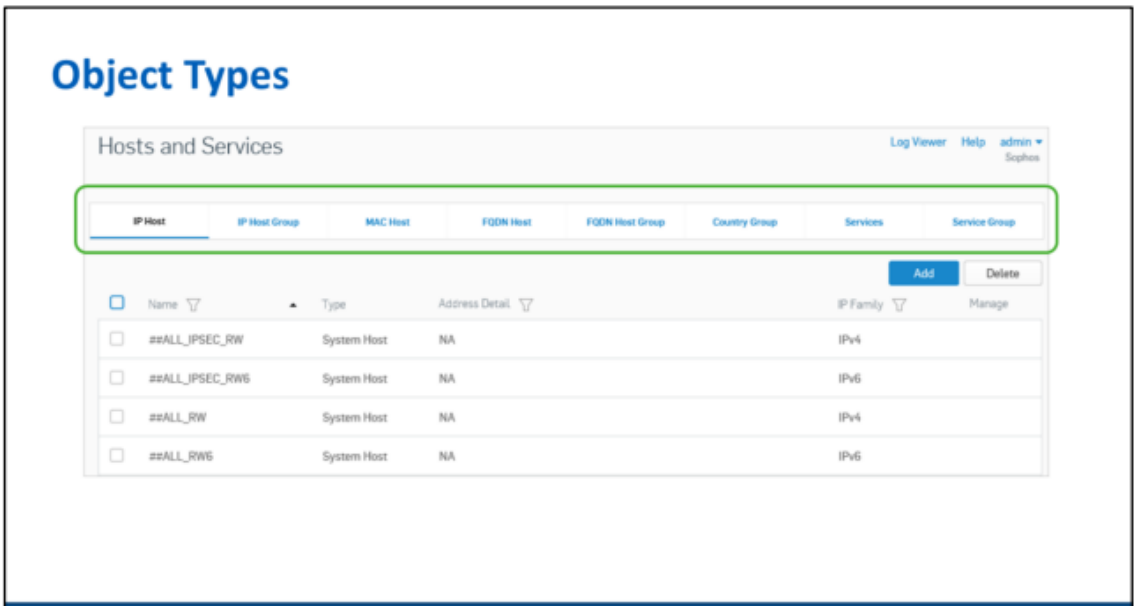


Figura 16: Hosts e serviços. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Em Hosts e Serviços, há várias opções para criar diferentes tipos de objetos, cada um dos quais pode ser encontrado nas guias da barra de menus superior do grupo de menus Hosts e Serviços (LAMMER, 2016)

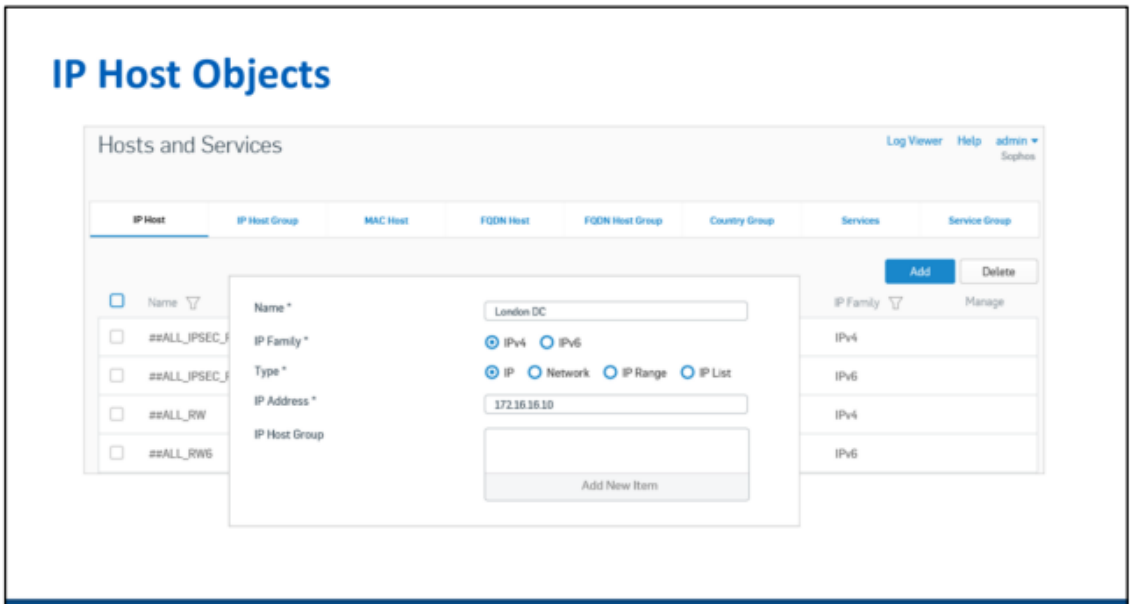


Figura 17: IP Hosts. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Hosts IP são objetos que podem representar um único host de rede, um grupo de hosts ou uma rede inteira. Eles são criados a partir da seção Host IP, clicando no botão Adicionar no canto superior direito da tela. Na próxima tela, atribua um nome ao novo objeto, selecione se ele é um objeto IPv4 ou IPv6 e o tipo de objeto de rede que será (SOPHOS CERTIFIED ENGINEER,2018).

Um objeto IP é para um único endereço, um objeto Rede nos permite usar uma máscara de sub-rede para definir o alcance da rede, a opção Faixa IP permite a entrada de um endereço IP inicial e final e a Lista IP permite a entrada individual Endereços IP separados por vírgulas (SOPHOS CERTIFIED ENGINEER, 2018).

Ao criar qualquer um dos tipos de objeto que não seja uma Lista de IPs, há também a opção de adicioná-lo a um Grupo de Host IP. Essa é uma maneira conveniente de agrupar vários objetos IP para facilitar a criação de regras e políticas.

Figura 18: FQDN Hosts. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Um host FQDN nos permite criar objetos de nome de domínio totalmente qualificados que podem ser agrupados em um grupo de hosts FQDN. Semelhante aos Hosts IP, clique no botão Adicionar na guia Host FQDN e preencha as informações necessárias (SOPHOS CERTIFIED ENGINEER, 2018)

Dê ao objeto um nome que ajudará você a identificá-lo ao ser adicionado a uma política. Digite o nome de domínio totalmente qualificado para o objeto, e, opcionalmente, adicione o Host FQDN a um ou mais grupos para que possa ser usado mais facilmente em políticas grandes.

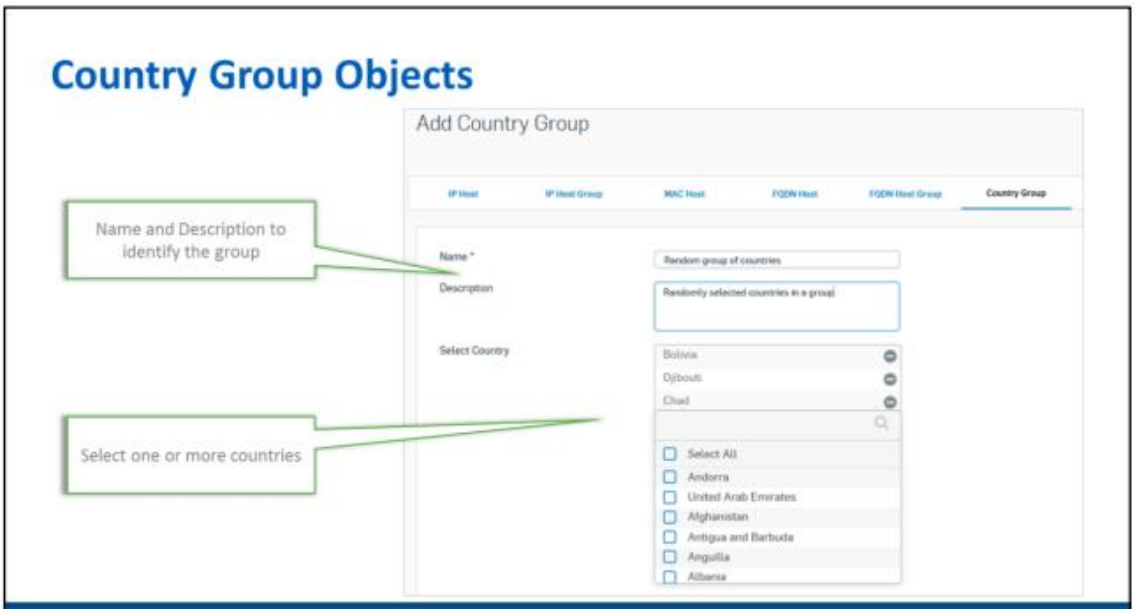


Figura 19: Grupo de Países. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Um Grupo de países é uma lista de intervalos de IPs categorizados pelo que é atribuído a países específicos por um grupo conhecido como ICANN. Essas listas são mantidas pela Sophos e vários grupos maiores pré-definidos estão prontos e aguardando o uso no XG Firewall. Naturalmente, um administrador pode criar seus próprios grupos personalizados ou modificar os supergrupos existentes que acompanham o dispositivo (SOPHOS CERTIFIED ENGINEER, 2018)

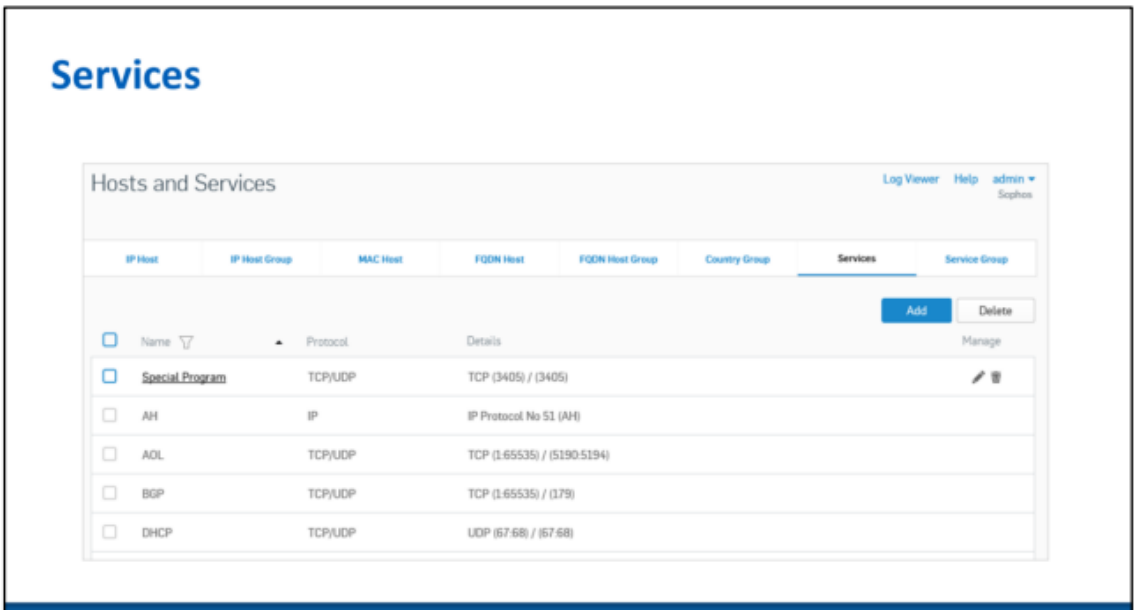


Figura 20: Serviços. Fonte (SOPHOS CERTIFIED ENGINEER,2018).

Existem muitos objetos de serviço pré-criados no XG Firewall para protocolos comuns, como DHCP, HTTPS, SMTP e muitos outros. Naturalmente, não poderíamos incluir todas as definições de serviço para cada aplicativo existente, para que os administradores tenham a capacidade de criar suas próprias definições (LAMMER, 2016)

Os serviços são criados clicando no botão Adicionar no canto superior direito ou os objetos de serviço que foram criados por um administrador podem ser editados clicando no nome ou no ícone de lápis, no entanto os serviços pré-existentes que acompanham o dispositivo não podem ser modificados. Objetos criados pelo usuário aparecerão acima de qualquer objeto de serviço pré-existente (SOPHOS CERTIFIED ENGINEER, 2018)

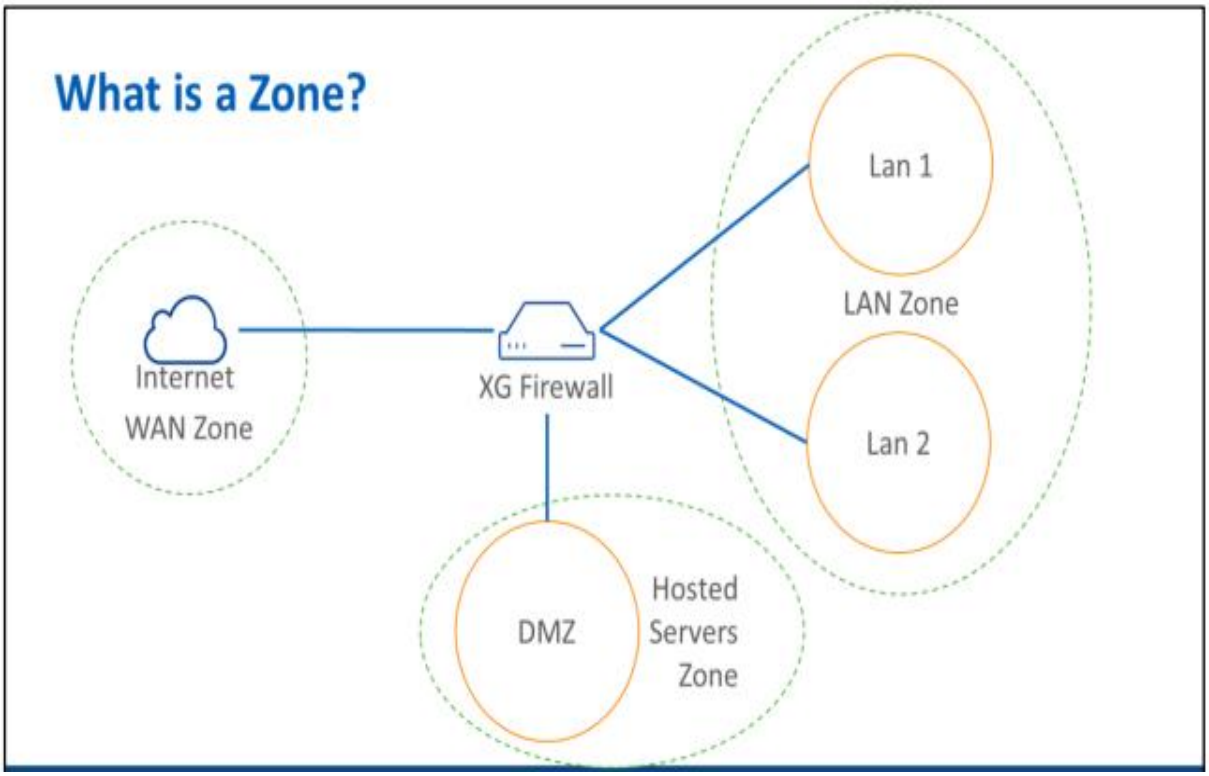


Figura 21: Zonas de distribuição. Fonte: (SOPHOS CERTIFIED ENGINEER, 2018).

Existem várias maneiras de definir uma zona de rede, alguns dizem que é uma área de administração para a qual você pode exercer controle. Outra definição é um grupo lógico ou físico de redes e hosts em um ambiente (INFOLINK, 2018). Para o firewall XG, uma zona é uma área da qual o tráfego se origina ou é destinado a, em outras palavras, são as portas físicas ou interfaces virtuais pelas quais o tráfego entrará e sairá do firewall.

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 (SOPHOS CERTIFIED ENGINEER, 2018)

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

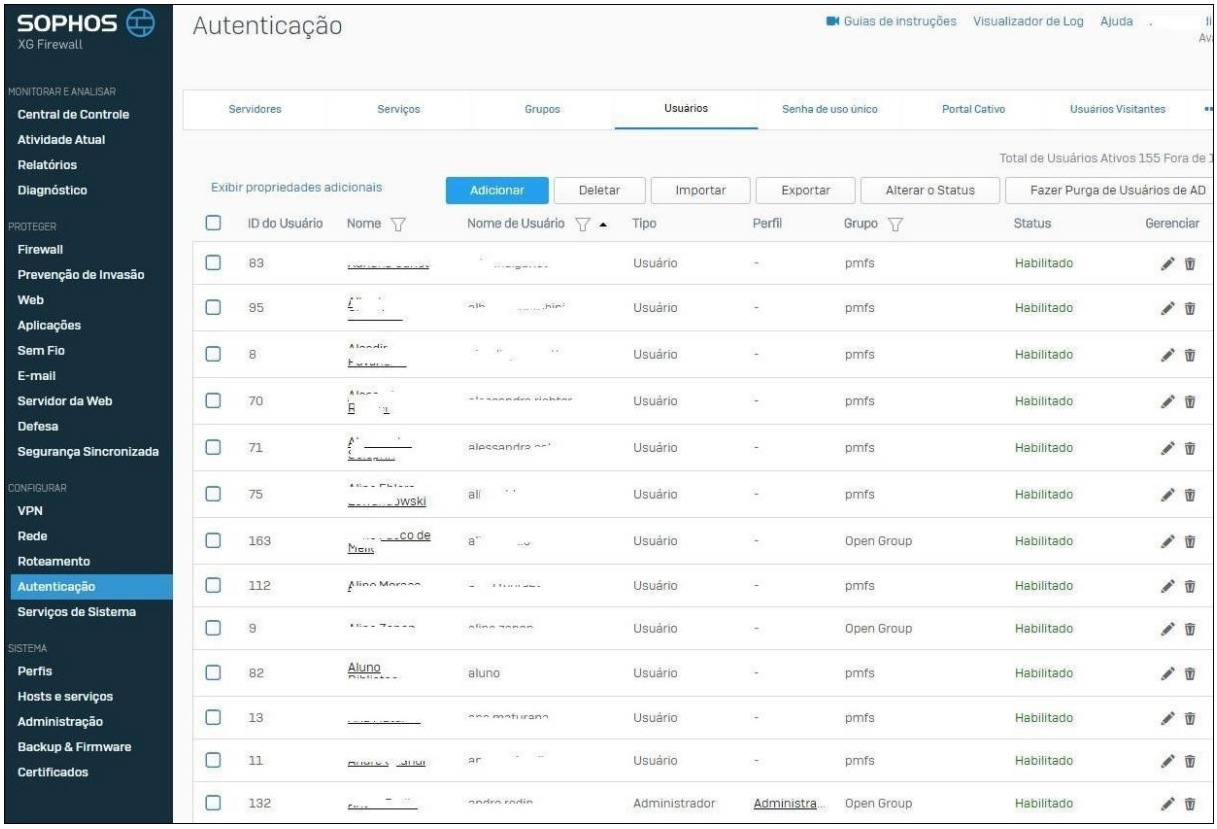


Figura 22: Parte de Autenticação. (Painel Sophos – Prefeitura Municipal de Faxinal do Soturno – RS,2018)

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.

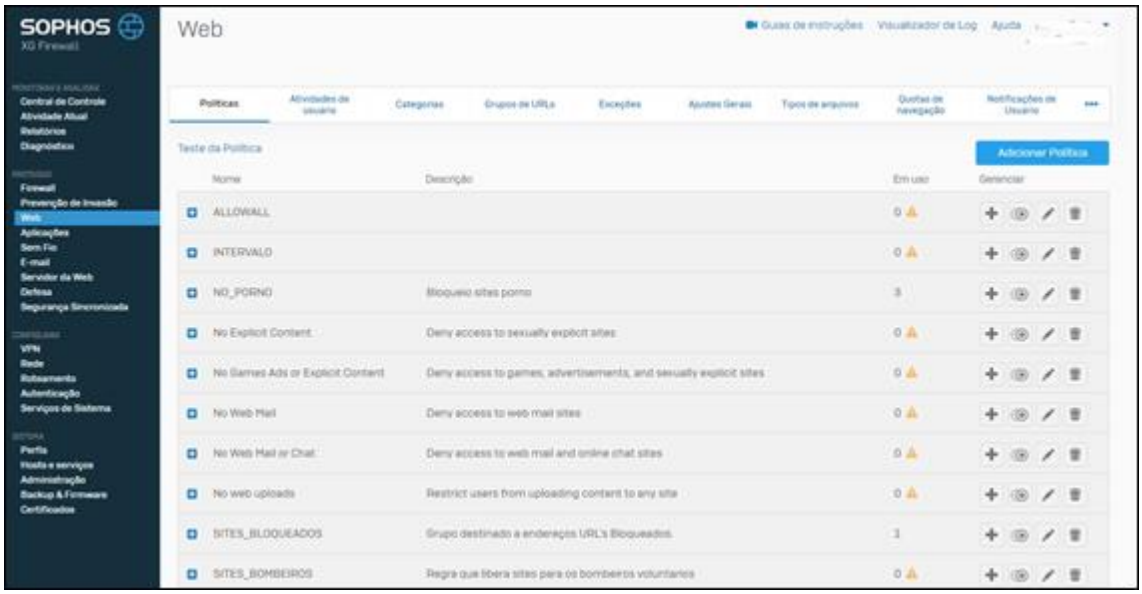


Figura 23: Aplicações Web. (Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018)

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.

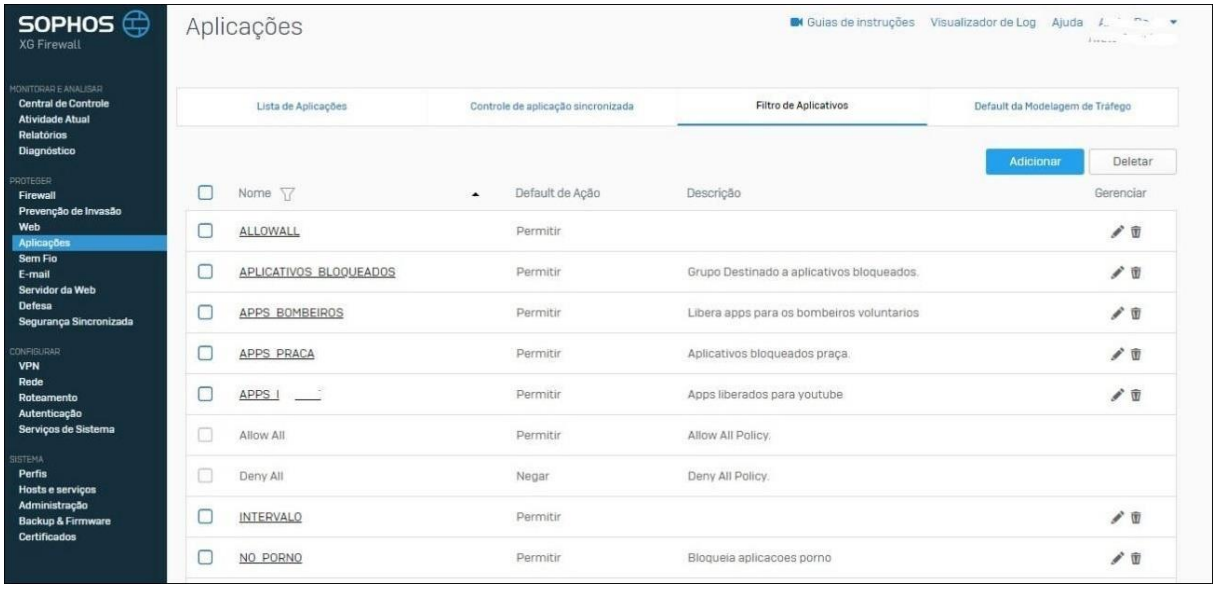


Figura 24: Políticas de Aplicação. (Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018)

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.

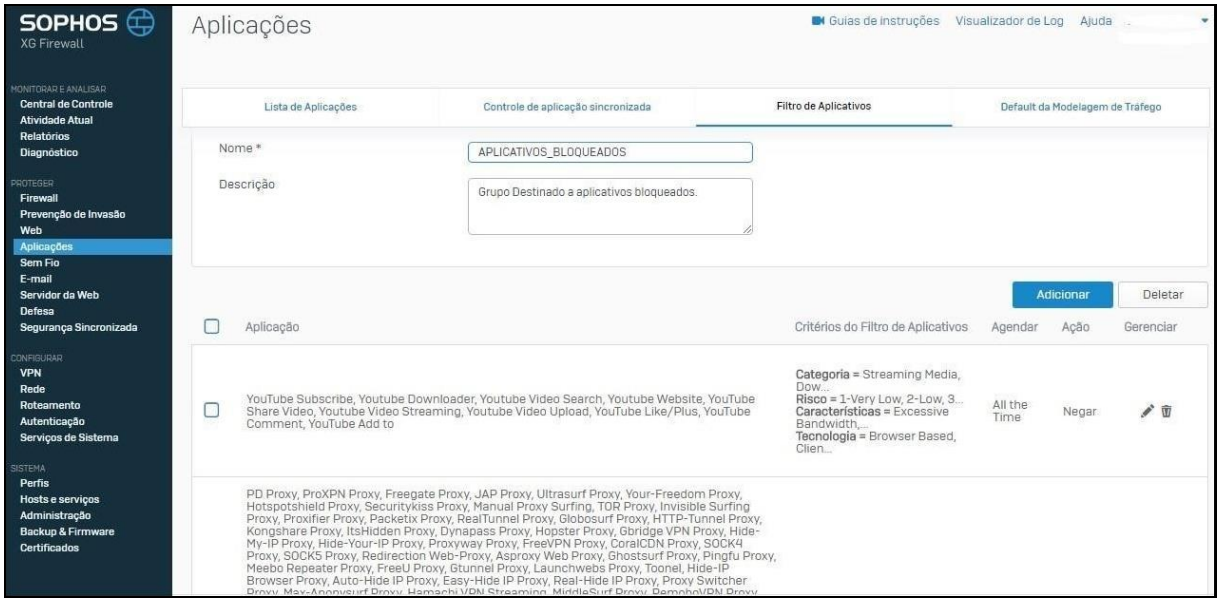


Figura 25: Interior das Políticas de Aplicação. (Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018).

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

2.5 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 (TRIPLAIT, 2017).

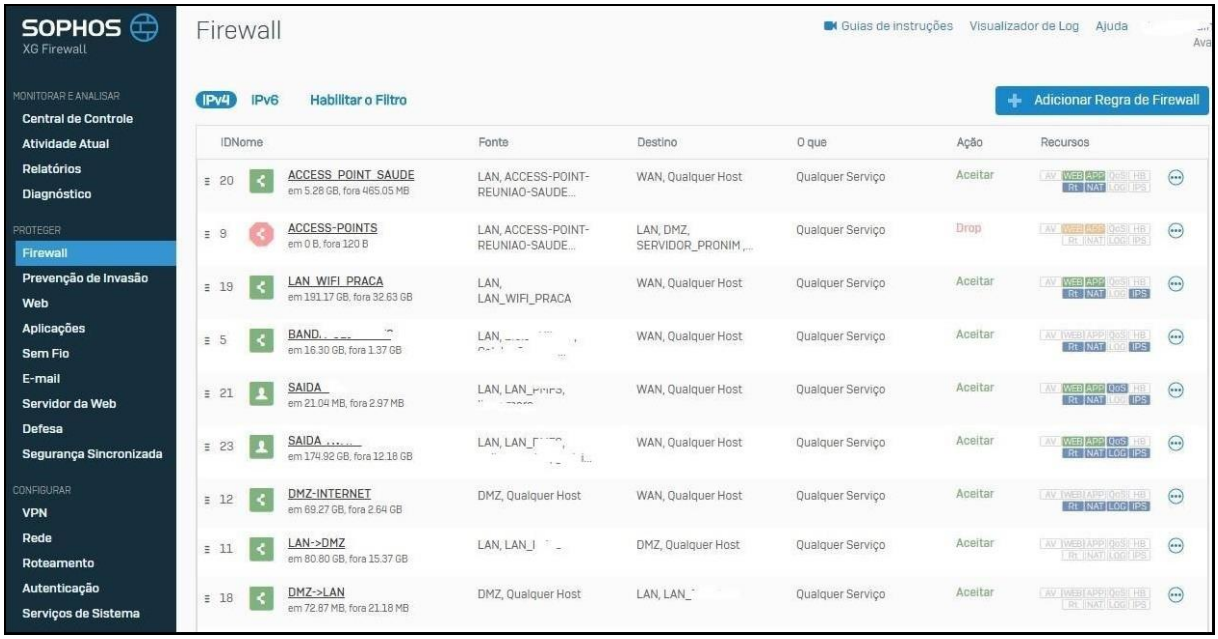


Figura 26: Regras de firewall. (Painel Sophos Prefeitura Municipal de Faxinal do Soturno - RS 2018)

2.6 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) (TRIPLAIT, 2017)

Todo esse processo tem que passar pelo *firewall* da zona WAN para LAN. A figura 27 ajudas a entender melhor o processo de redirecionamento:

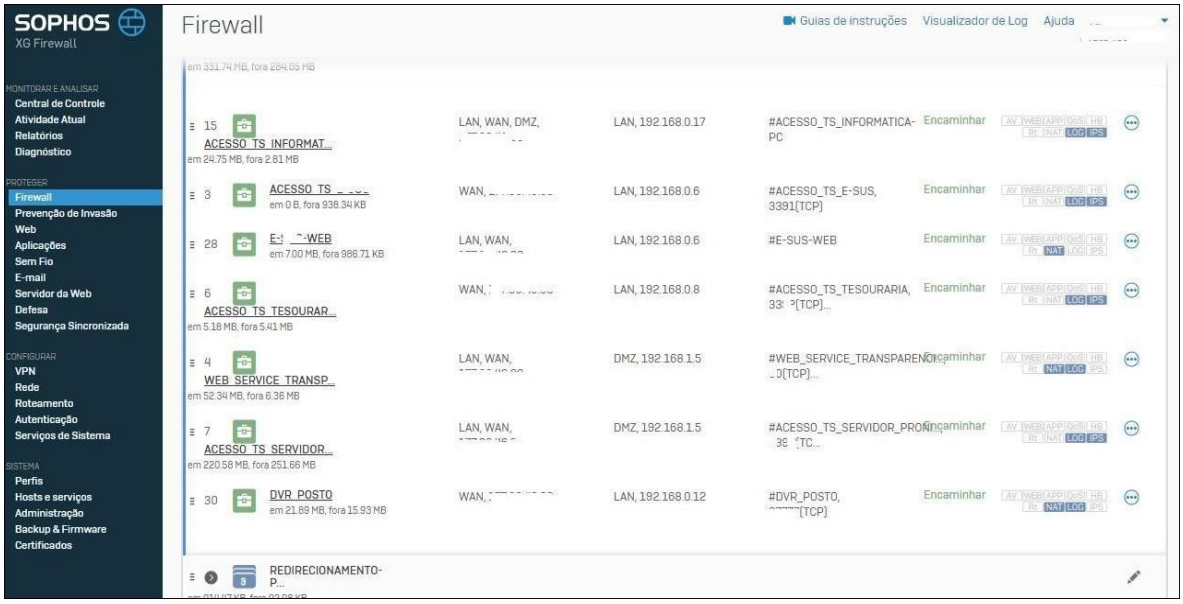


Figura 27: Redirecionamento firewall. (Painel Sophos Prefeitura Municipal de Faxinal do Soturno – RS 2018)

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 28 vemos como é feita a simulação.

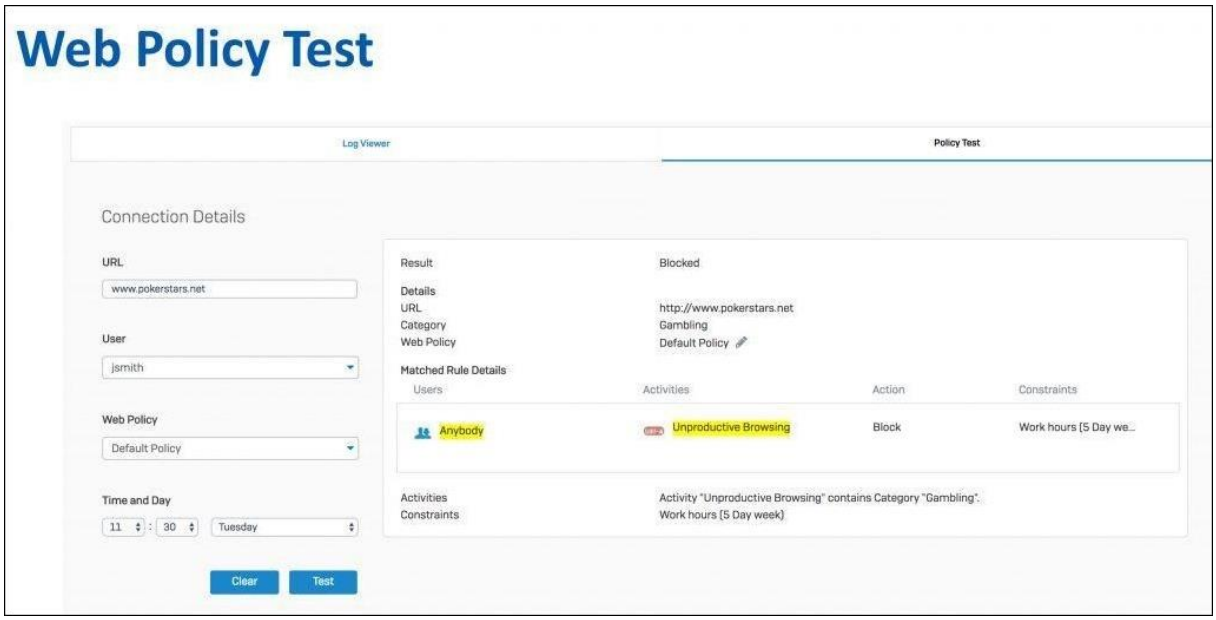


Figura 28: Simulação e testes de Regras de firewall. Fonte: TRIPLAIT, 2017

2.6 Relatórios

Não há a obrigatoriedade de uso de servidor externo para logs e relatórios. Você consegue emitir os relatórios direto na caixa da Sophos. Como os dados ficam dentro do próprio equipamento, pode-se gerar relatórios atualizados em questão de poucos minutos. Não há a necessidade de aguardar horas para popular os dados. Onde tem opção de escolher a data de início e data final dos relatórios, gerar relatórios de aplicações, ameaças, VPN, e-mails e conformidade.

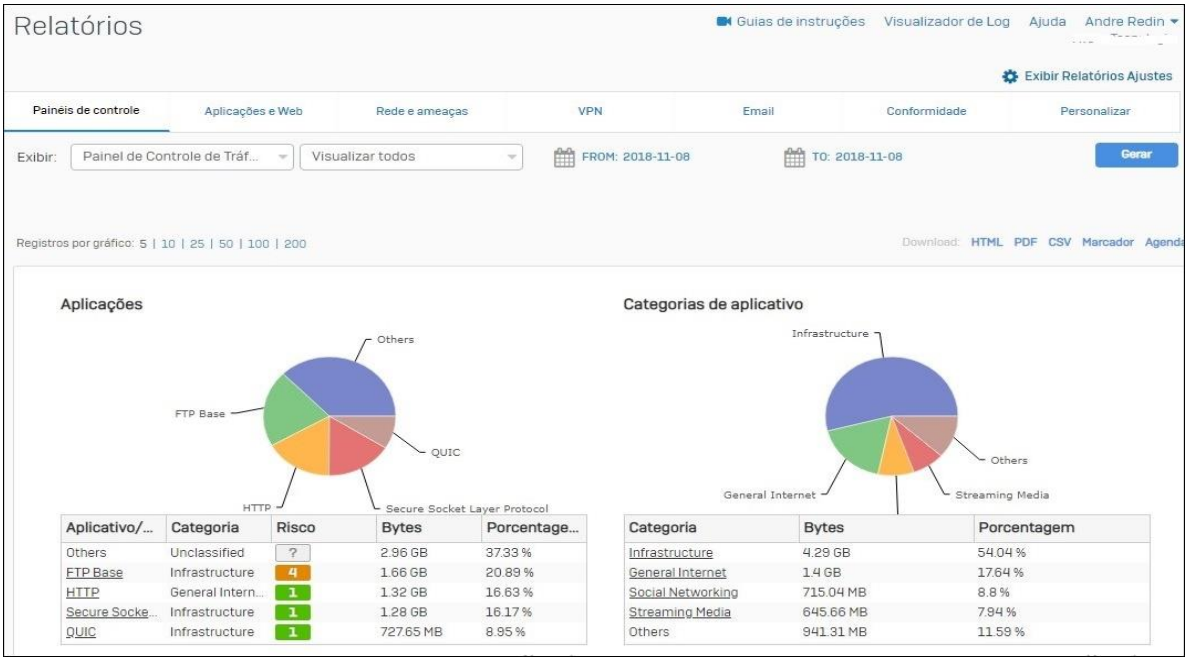


Figura 29: Gerador de Relatório.

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, 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 na Prefeitura Municipal de Faxinal do Soturno, o qual é uma técnica de investigação composta por questões apresentadas por escrito às pessoas, com o propósito de obter determinadas informações (GIL, 1999). 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. 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.

A Sophos é líder no quadrante mágico da plataforma de proteção para Endpoint, o relatório Gartner elogia o ntercept X por sua capacidade de proteger contra o ransomware. Quando a tecnologia CryptoGuard incluída no Intercept X detecta tentativas de criptografia maliciosas, ele para o ataque e retorna os arquivos afetados para seu estado seguro (NEWS SOPHOS, 2018).

O [1]Gartner também destaca as capacidades anti-exploit do Intercept X. Intercept X tem mais de 25 diferentes técnicas de anti-exploit e também contra o adversário ativo.

As líderes são empresas com o nível mais avançado de desenvolvimento tecnológico. Elas normalmente encontram-se na ponta do mercado, com maior capacidade de implementar novidades, aplicações mais definidas e um conjunto de serviços bem estabelecido. Além disso, elas também costumam ditar as regras de um segmento e apresentar as novidades para os próximos anos (MOREIRA, 2018).

Abaixo uma imagem do quadrante mágico do Gartner, mostrando o Sophos como líderes junto com Symantec e Trend Micro.

Figura 30: Gráfico de Gartner

[1]A Gartner desenvolve tecnologias relacionadas a introspecção necessária para seus clientes tomarem suas decisões todos os dias. (GARTNER, 2018)

4 RESULTADOS

Foi constatada uma considerável queda tráfego internet que antes era desperdiçado com o acesso a aplicações e páginas não produtivas tais como: vídeos, jogos on-line, músicas e rádios. Além da diminuição do tráfego internet obtido através dos filtros web e de aplicação, o XG Firewall 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.

Abaixo foram obtidos os seguintes gráficos que a ferramenta de relatório utilizada por esse fabricante no período de 01/08/2018 até 01/10/2018.

Os gráficos foram retirados da Prefeitura Municipal de Faxinal do Soturno, onde o mesmo utiliza o XG Sophos com o modelo de hardware XG 125 (SFOS 17.0.8 MR-8).

- Usuários que mais consumiram banda;
- Categorias de Web Sites mais acessadas;
- Aplicações mais bloqueadas;
- Países em que as pesquisas foram mais destinadas;
- Ataques de invasão;

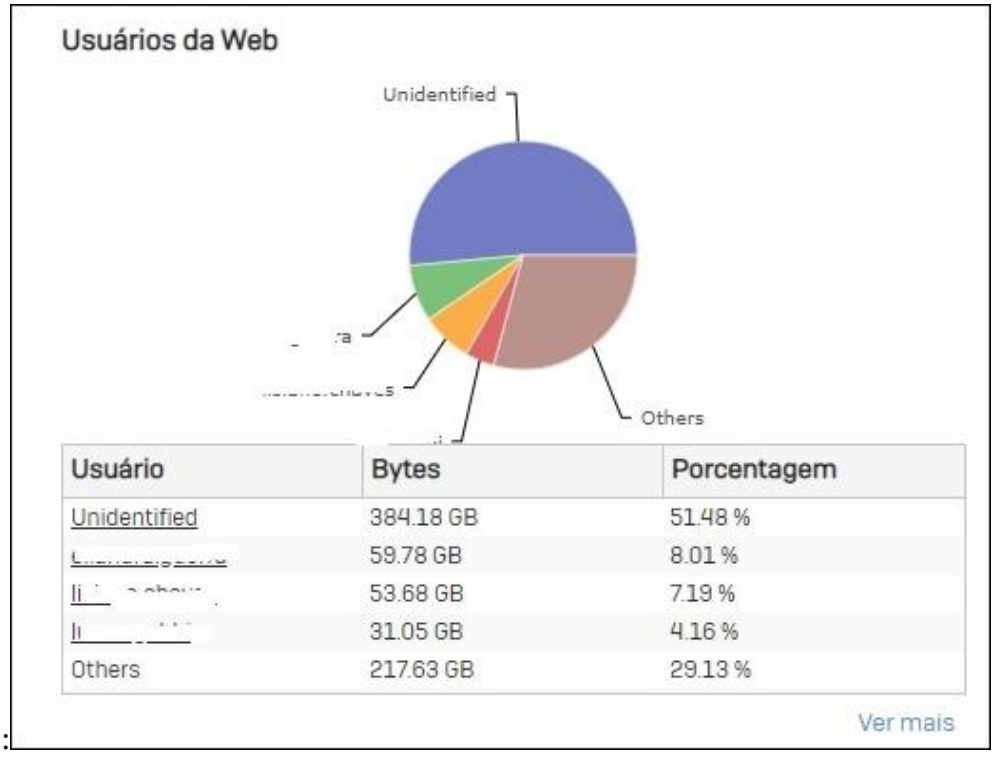


Figura 31: Usuários que mais consumiram banda.

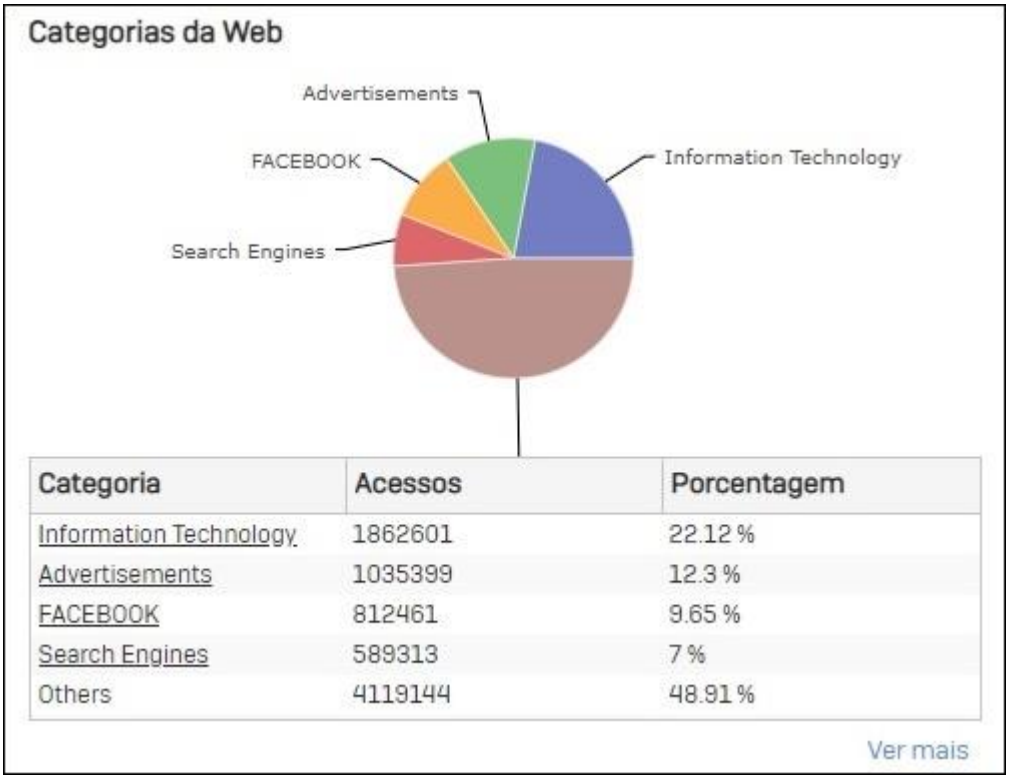


Figura 32: Categorias de Web mais acessadas.

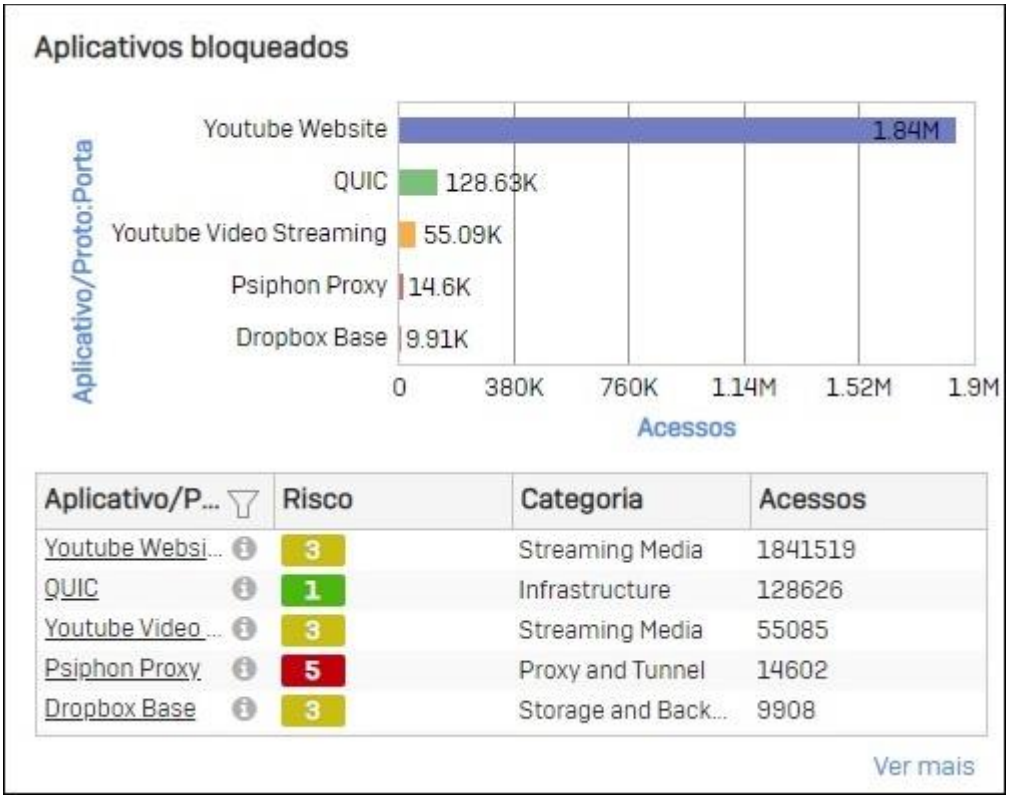
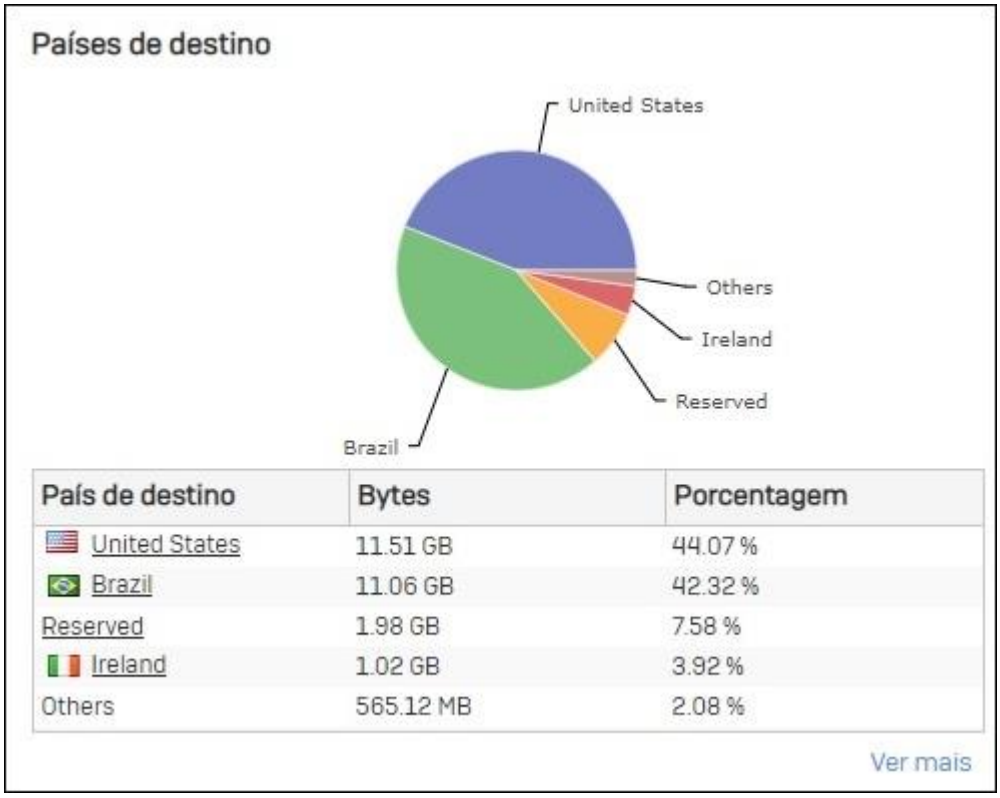


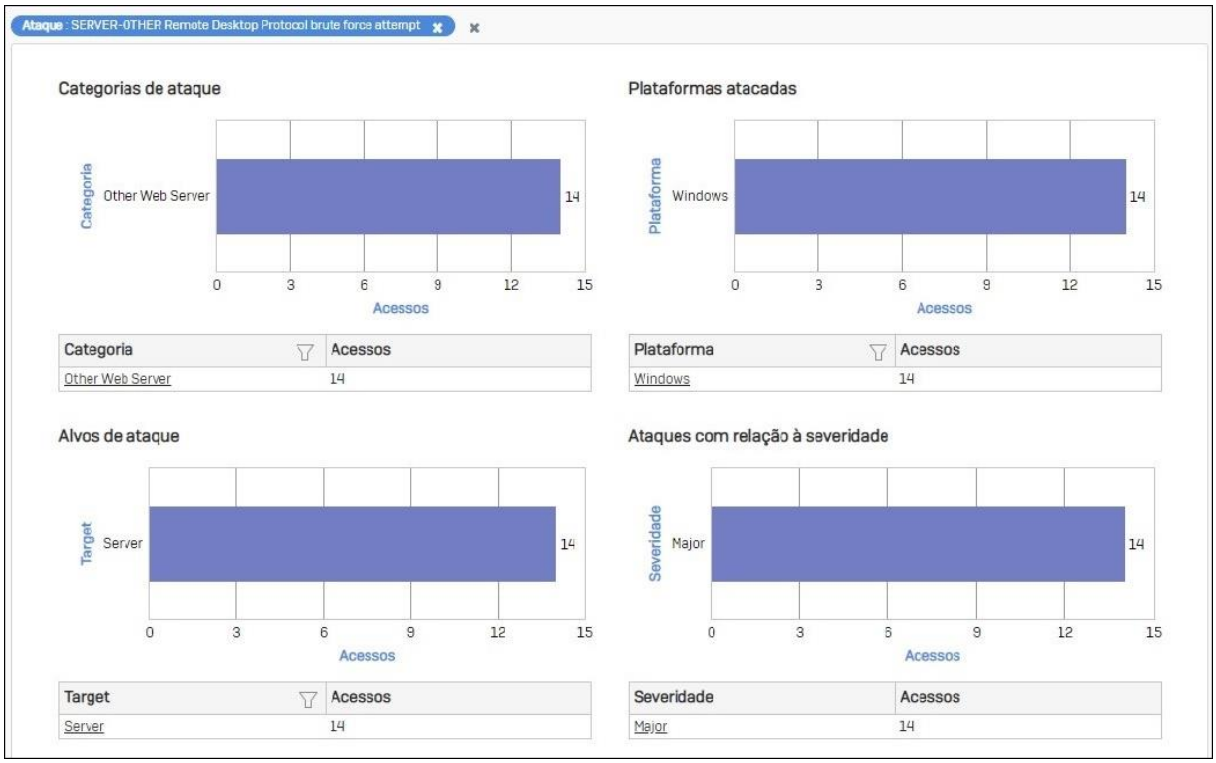
Figura 33: Aplicações mais bloqueadas.



País de destino	Bytes	Porcentagem
United States	11.51 GB	44.07 %
Brazil	11.06 GB	42.32 %
Reserved	1.98 GB	7.58 %
Ireland	1.02 GB	3.92 %
Others	565.12 MB	2.08 %

Ver mais

Figura 34: Países que tiveram as pesquisas mais destinadas.



Categoria	Acessos
Other Web Server	14

Plataforma	Acessos
Windows	14

Target	Acessos
Server	14

Severidade	Acessos
Major	14

Figura 35: Parte 1 Ataques de Invasão

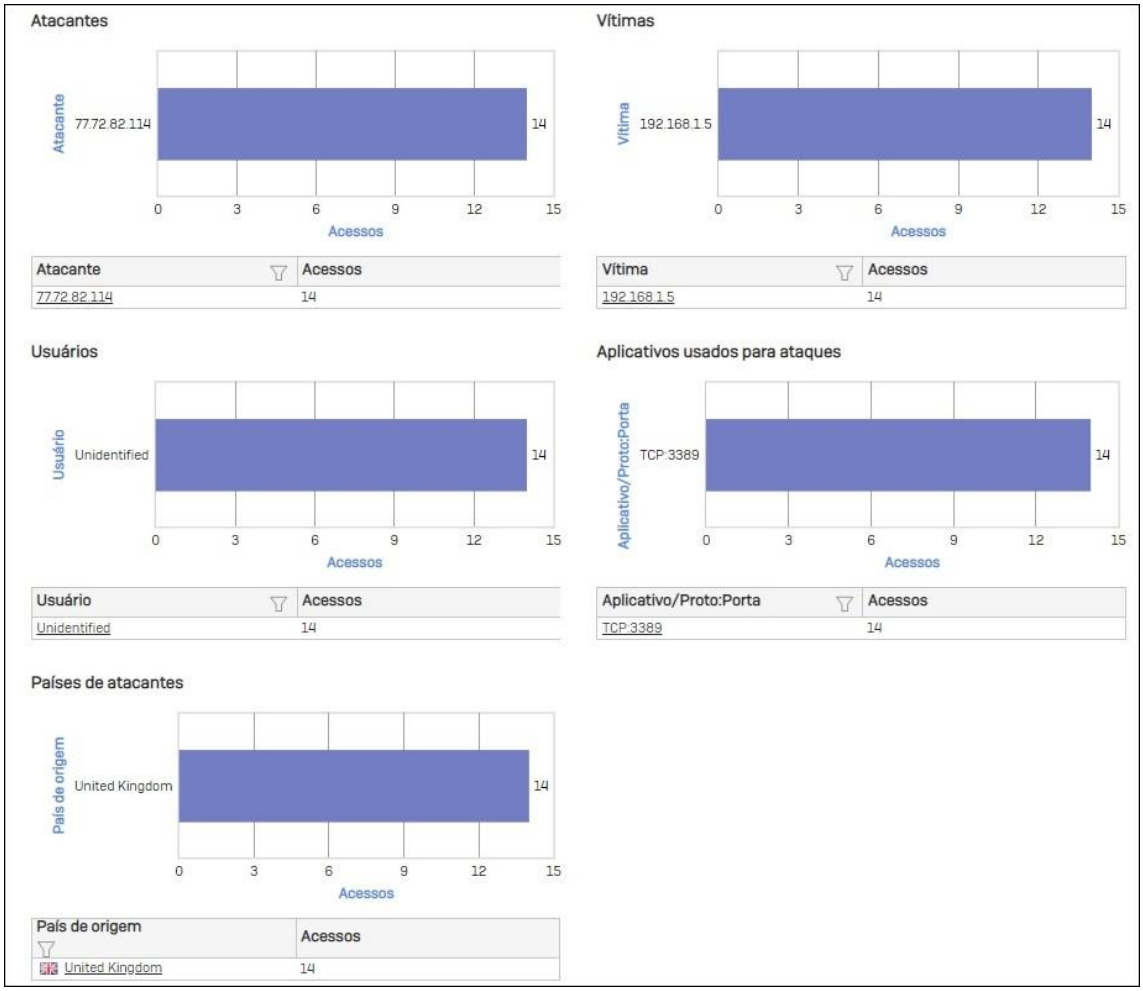


Figura 36: Parte 2 Ataques de Invasão.

A figura 37 é um gráfico da Zona de WAN: Total de Upload/Download de Transferência de Dados, com alto consumo em cima de um link de 15Mb/s, que era utilizado sem regras de bloqueios e acessos (imagem obtida através do monitoramento de gráficos do sistema SOPHOS).

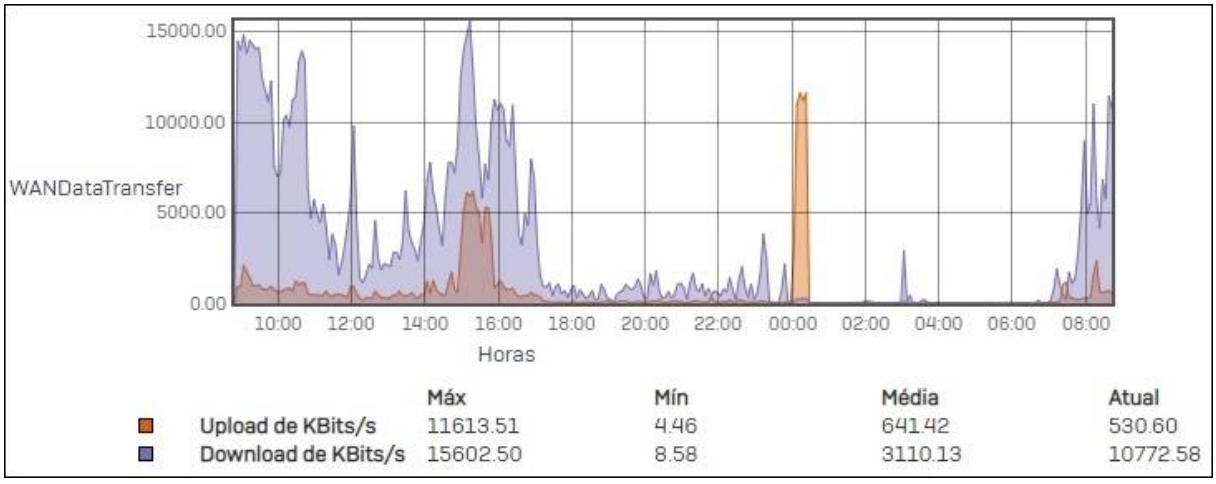


Figura 37: Gráfico de Alto Consumo.

A figura 38 é um gráfico representando queda de tráfego (imagem obtida através do monitoramento de gráficos do sistema SOPHOS).

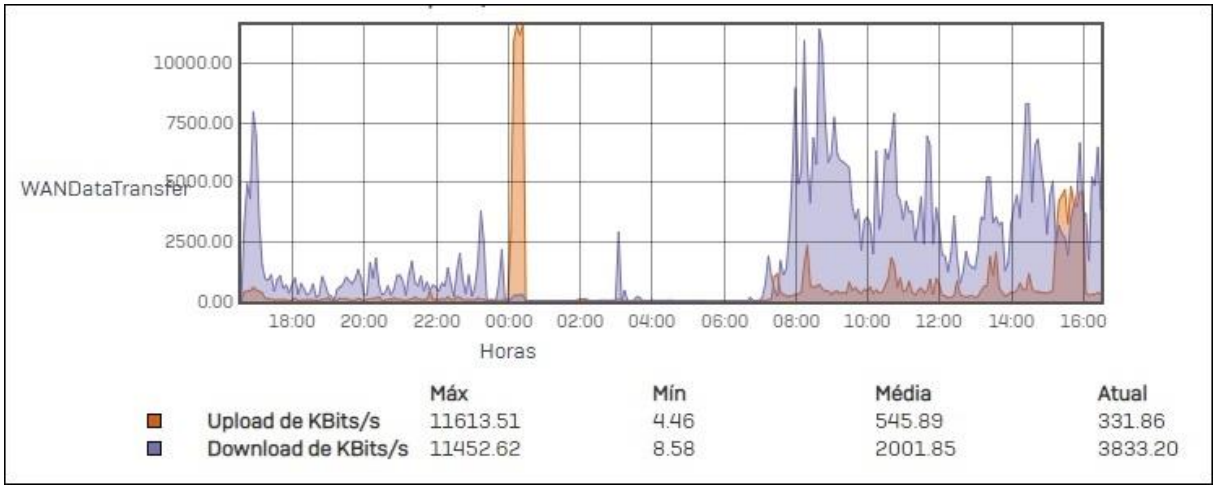


Figura 38: Queda de Tráfego

A figura 39 representa a ferramenta XG Firewall da marca SOPHOS modelo XG 125W *(appliance)* que é objeto dessa pesquisa acadêmica.

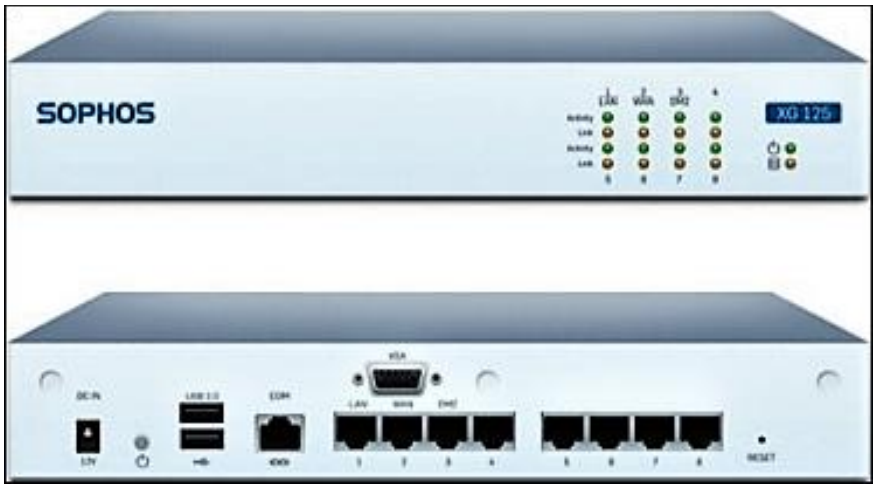


Figura 39: XG 125W (appliance). Fonte: (TRUSTVISION, 2018).

5 CONSIDERAÇÕES FINAIS

Com esse trabalho de pesquisa podemos considerar que o XG SOPHOS possivelmente é uma das melhores soluções presentes no mercado para gerenciar ambientes corporativos. Ele conta com todos os itens necessários para uma proteção do seu ambiente acoplados em um só software, garantindo a eficiência e a facilidade de gerir com ele.

Utilizando o XG SOPHOS vemos como fica mais fácil para um gestor de TI, criar e gerenciar políticas de acesso, redirecionamentos, consultar relatórios de consumo, páginas mais acessadas além de evitar que pessoas não autorizadas usem a conexão do ambiente para acesso à internet.

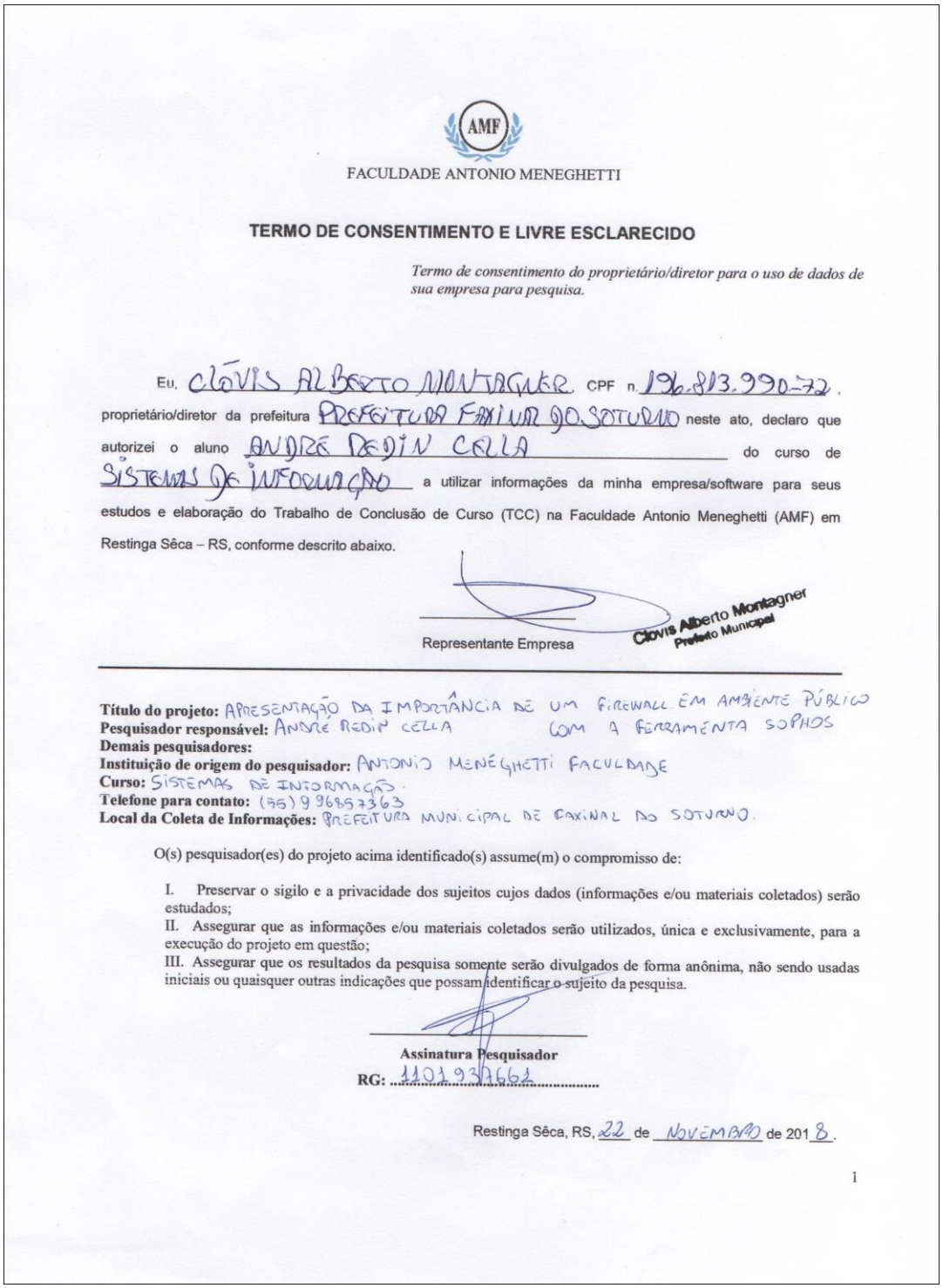
Possui uma interface simples de ser manejada, muita eficiência em seus resultados. Para ter uma a mais proteção para seu ambiente corporativo, uma opção para isso é o Endpoint Protection, seu próprio antivírus, onde ele também possui um painel web para controle de políticas e para manter os usuários mais seguros.

Foi coletado o depoimento do Prefeito Municipal de Faxinal do Soturno, Clovis Alberto Montagner e também de alguns servidores públicos sobre o XG Sophos que é utilizado na prefeitura, onde foi feito através de uma pergunta dissertativa.

O que você acha sobre as políticas de bloqueio do firewall implantada na prefeitura, onde são bloqueadas redes sociais, vídeos e sites pornográficos? Responda em um breve parágrafo.

“Acredito ser de suma importância, uma vez que além de proteger os equipamentos da ameaça de algum vírus, entendo que não é apropriado o uso dos computadores para esses fins no local e horário de trabalho, e infelizmente as pessoas não tem o bom senso de não utilizarem esses sites o que faz necessário o bloqueio. ”

“Vejo que segurança em todos os aspectos da nossa vida é importante. No que diz respeito às informações dentro das organizações este tema toma uma relevância maior. Diria imprescindível para a organização. Tornam o trabalho mais sério, buscam maior compromisso e comprometimento dos colaboradores, tempo melhor aproveitado. ”



FACULDADE ANTONIO MENEGHETTI

TERMO DE CONSENTIMENTO E LIVRE ESCLARECIDO

Termo de consentimento do proprietário/diretor para o uso de dados de sua empresa para pesquisa.

Eu, CLÓVIS ALBERTO MONTAGNER, CPF n. 196.813.990-72, proprietário/diretor da prefeitura PREFEITURA PAIXÃO DO SOTURNO neste ato, declaro que autorizei o aluno ANDRÉ REDIN CELLA do curso de SISTEMAS DE INFORMAÇÃO a utilizar informações da minha empresa/software para seus estudos e elaboração do Trabalho de Conclusão de Curso (TCC) na Faculdade Antonio Meneghetti (AMF) em Restinga Sêca – RS, conforme descrito abaixo.

Representante Empresa

Clóvis Alberto Montagner
Prefeito Municipal

Título do projeto: APRESENTAÇÃO DA IMPORTÂNCIA DE UM FIREWALL EM AMBIENTE PÚBLICO COM A FERRAMENTA SOPHOS
Pesquisador responsável: ANDRÉ REDIN CELLA
Demais pesquisadores:
Instituição de origem do pesquisador: ANTONIO MENEGHETTI FACULDADE
Curso: SISTEMAS DE INFORMAÇÃO.
Telefone para contato: (55) 996857363
Local da Coleta de Informações: PREFEITURA MUNICIPAL DE PAIXÃO DO SOTURNO.

O(s) pesquisador(es) do projeto acima identificado(s) assume(m) o compromisso de:

I. Preservar o sigilo e a privacidade dos sujeitos cujos dados (informações e/ou materiais coletados) serão estudados;
II. Assegurar que as informações e/ou materiais coletados serão utilizados, única e exclusivamente, para a execução do projeto em questão;
III. Assegurar que os resultados da pesquisa somente serão divulgados de forma anônima, não sendo usadas iniciais ou quaisquer outras indicações que possam identificar o sujeito da pesquisa.

Assinatura Pesquisador
RG: 1101937661

Restinga Sêca, RS, 22 de NOVEMBRO de 2018.

1

Figura 40: Termo de Consentimento e Livre Esclarecido.

REFERÊNCIAS

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.

CANALTECH. Ataque DDoS. [2017]. Disponível em: <https://canaltech.com.br/produtos/O-que-e-DoS-eDDDoS/>. Acesso em: 15-12-2017

CISCO, **TCP-IP ROUTING**, 2006. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13788-3.html>. Acesso em: 15-12-2017

CISCO, **Redes e Ips** 2017, Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13788-3.html >. Acesso em: 15-12-2017

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

INFOLINK, **Sophos Endpoint**. 2018. Disponível em <https://www.infolink.com.br/sophos-endpoint/>. Acesso em: 15-12-2017

MALWAREBYTES. Tudo sobre ransomware. **Malwarebytes**, [201-?]. Disponível em: <https://br.malwarebytes.com/ransomware/>. Acesso em: 10-05-2018

MELIM, Miguel. Poisining, Man-in-the-middle attack (MITM) e Sniffing. **Madeira Computing**, [2018]. Disponível em: < https://www.madeira-computing.pt/contacts/>. Acesso em: 10-05-2018

MOREIRA, Esdras. Descubra agora o que é o quadrante mágico do Gartner. **Introduce TI**, 1 mar. 2018. Disponível em: <http://introduceti.com.br/blog/quadrante-magico-do-gartner-2018/>. Acesso em:15-06-2018

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

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, **Sobre a Sophos** 2017. Disponível em: <http://www.solucoes-sophos.com.br/sobre-a-sophos>. Acesso em: 15-06-2018

SOPHOS, **XG SOPHOS**, 2017 Disponível em: <https://www.m3corp.com.br/sophos/sophos-utm-2> Acesso em: 15-06-2018

SOPHOS CERTIFIED ENGINEER. **Module 2**: getting started with XG Firewall. Disponível em: <https://v6.SOPHOS CERTIFIED ENGINEER.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: 24-07-2018

SHEKHAR, Amar. How to perform ping of death attack using CMD and notepad (just for learning). **Fossbytes**, jun. 10, 2016. Disponível em: <https://fossbytes.com/perform-ping-of-death-attack-using-cmd-just-for-learning/>. Acesso em: 24-07-2018

TRIPLAIT. Serviço de Firewall UTM gerenciado da Tripla powered by Sophos. **Triplait**, 2017a. Disponível em: <http://triplait.com/firewall-como-servico> . Acesso em: 24-07-2018

TRIPLAIT, Novas funcionalidades do firewall Sophos XG V17.**Triplait**, 2017b. Disponível em < https://triplait.com/novas-funcionalidades-do-firewall-sophos-xg-v17/#.WzEhBadKjGg/>. Acesso em: 28-07-2018

VERISIGN. Serviços de segurança: ataque de inundação SYN. Verisign, [2017]. Disponível em: <https://www.verisign.com/pt_BR/security-services/ddos-protection/syn-flood/index.xhtml>. Acesso em: 15-08-2018

MORIMOTO. Appliance, [2005]. Disponível em: <http://www.hardware.com.br/termos/appliance>. Acesso em: 20-06-2017

CISCO. Redes e Endereços IP's. [2016]. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13788-3.html>. Acesso em 15-08-2017

TRUSTVISION. XG 125W. [2018]. Disponível em: <http://www.trustvision.pt/pt/produtos/redes-de-voz-e-dados/firewalls/sophos-xg-125/6/30/191>. Acesso em 08-10-2018

DUARTE. Varredura de portas. [2016]. Disponível em: <https://www.gta.ufrj.br/grad/16_2/2016VARPORT/>. Acesso em 10-03-2018

TACIO. Sniffing. [2011]. Disponível em: <http://www.mundodoshackers.com.br/top-5-os-melhores-sniffers-gratuitos>. Acesso em 21-05-2018

MAURICIO. Modelo Padrão de uma Divisão de rede. [2004]. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php>. Acesso em 04-04-2017

Bär.Simulador de testes e regras de Firewall. [2018]. Disponível em: <https://triplait.com/novas-funcionalidades-do-firewall-sophos-xg-v17/#.W-7oUjhKiUk>. Acesso em 06-06-2018

NEWSOPHOS. Gráfico de Gartner. [2018]. Disponível em: <https://news.sophos.com/pt-br/2018/02/02/a-sophos-e-lider-no-quadrante-magico-da-plataforma-de-protecao-para-endpoint/>. Acesso em 19-07-2018

LAMMER. Co-fundadior. [1985]. Disponível em: <http://rjnetwork.com.br/blog/?p=1891>. Acesso em 19-07-2018

LOUPEN. Painel Sophos. [2017]. Disponível em: <http://loupen.com.br/pt/sophos/network/secure-web>. Acesso em 10-12-2017

GREYCAMPUS. Sniffing. [2018]. Disponível em: <https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types>. Acesso em 22-08-2018