DESTAQUES ACADÊMICOS
UNIVATES | CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
Revista Destaques Acadêmicos, Lajeado, v. 11, n. 4, 2019. ISSN 2176-3070
DOI: http://dx.doi.org/10.22410/issn.2176-3070.v11i4a2019.2385
http://www.univates.br/revistas

FIREWALL DE PRÓXIMA GERAÇÃO - FORTINET

Mateus Fachinelli[1], Edson Moacir Ahlert[2]

Resumo: Desde a criação das redes de computadores sempre foi essencial podermos gerenciá-las e mantê-las seguras, a fim de ter um ambiente protegido e livre de qualquer tipo de ameaça. Este artigo tem como objetivo apresentar a tecnologia de *firewall* de próxima geração (NGFW) implantado no grupo Tramontina, em relação aos seus antecessores, descrevendo e demonstrando algumas das suas principais características por meio de um cenário de testes, baseado nas mesmas implementações e configurações feitas no grupo Tramontina, e então discutir e analisar quais as diferenças e recursos de segurança que essa nova tecnologia proporcionou para a empresa. A solução de *firewall* adotada pela empresa é proprietária da empresa Fortinet e o trabalho demonstra, por meio dos resultados analisados, que o *firewall* de próxima geração, em relação ao utilizado anteriormente no grupo Tramontina, de filtragem de pacotes, veio para agregar funções a tecnologia de *firewall* de estado, ampliando a segurança de redes e facilitando a vida dos administradores de redes em ambientes corporativos.

Palavras-chave: Redes de computadores, Segurança da informação, *Firewall*.

1. INTRODUÇÃO

Quando falamos em segurança, estamos falando de um conceito amplo, mas que basicamente consiste em preservar a confidencialidade, a integridade e a disponibilidade da informação. O que se espera é que as informações não sejam acessadas por pessoas não autorizadas, que estejam em local adequado e disponíveis no momento desejado.

As questões relacionadas à segurança da informação têm ganhado destaque e tomado tempo nas reuniões estratégicas e orçamentárias das empresas, esse fato se dá devido ao avanço das tecnologias, dos recursos on-line e também da evolução das ameaças digitais.

Hoje nas empresas, o *firewall* tornou-se ferramenta indispensável. Ele nada mais é do que um ativo colocado em uma localização estratégica dentro da

1 Curso Superior de Tecnologia em Redes de Computadores. mfachinelli@universo.univates.br

2 Mestre em Ambiente e Desenvolvimento. Professor da Univates. edsonahlert@univates.br

topologia de rede, por onde todo tráfego, obrigatoriamente, deve passar para poder chegar em determinado destino. Sua função é realizar a segurança de toda comunicação entre as redes existentes, como a passagem de determinados tráfegos, portas, determinar o que pode entrar e sair em termos de pacotes e informações de rede, quem pode acessar determinada rede, permitindo assim um controle maior sobre o ambiente.

Com esse progresso surgiu um desafio aos métodos de controle mais tradicionais, exemplificados aqui pelo *stateful firewall*. Este, age basicamente sobre portas de conexão, sem a capacidade de um controle mais preciso (qual tipo de aplicação está passando pela conexão) ou até mesmo vazamento de informações através de extensões de arquivos ou conteúdo que seja controlado para fora da rede da empresa.

Firewalls tradicionais não conseguiram evoluir com o avanço das ameaças e não foram capazes de inspecionar os pacotes de redes de forma granular e inteligente (identificando ataques, ameaças e aplicações), incapazes de diferenciar os tipos de tráfego que estão passando por ele. Para essas tarefas, surgiu o *firewall* da próxima geração (NGFW), que tem funções de segurança avançadas para o controle de uso dos recursos e detecção de ameaças sem gerar latência ou lentidão na rede (MANECA, 2015).

Existem algumas semelhanças entre estes dois tipos de *firewalls* (*stateful* e NGFW). O objetivo deles é proteger a rede na qual estão implementados, efetuando o controle dos acessos de forma autorizada, de acordo com cada política definida, possuindo também recursos de conexão VPN a fim de garantir a segurança dos dados enviados e recebidos e o controle de portas e protocolos para comunicação interna ou externa (MANECA, 2015).

Segundo MANECA (2015), a grande diferença está nas integrações que o NGFW possui, onde em um mesmo equipamento ou máquina virtual, é possível ter recursos como o IDS (Sistema de detecção de intrusão), IPS (Sistema de Prevenção a intrusão), controle de aplicação, filtragem web, antivírus, controle de estações e *QoS* (controle de banda). Devido a essas capacidades, o NGFW se torna uma ferramenta de uso imprescindível para a proteção dos recursos disponíveis em uma empresa.

O uso deste tipo de *firewall* deve ser controlado para garantir a integridade lógica dos dados e física dos equipamentos, na era da mobilidade onde é possível levar um notebook, tablet, etc, para fora da rede da empresa, é gerado um desafio para as soluções tradicionais, sendo necessário um ambiente/sistema/aplicação que se estenda além das fronteiras da rede corporativa.

Com um *firewall* de próxima geração é possível utilizar políticas de proteção por cliente e localização. Desta maneira, quando um ativo de propriedade da empresa deixa a rede da corporação que é protegida e vai para um ambiente comum, ativa-se uma proteção nesse equipamento, com regras pré-estabelecidas no NGFW.

O objetivo deste trabalho é apresentar a tecnologia de NGFW, solução da Fortinet implementada em todas as unidades da empresa Tramontina, de Carlos Barbosa/RS, exceto no exterior. Os testes para demonstrar as características da ferramenta, foram feitos a partir de um ambiente mais simplificado, mas com as mesmas funções implementadas na empresa, como detecção de ameaças, filtro de conteúdo, controle de aplicação, prevenção a perda de dados e inspeção SSL.

2. TECNOLOGIAS DE *FIREWALL*

Para ajudar os administradores a manter seu ambiente seguro, vamos iniciar falando sobre técnicas e soluções de *firewall*, que ajudam a garantir a segurança do ambiente de TI. *Firewall* é uma combinação de hardware e software que isola a rede interna de uma empresa da Internet em geral, permitindo que alguns pacotes passem e outros sejam bloqueados, possibilitando que o administrador da rede tenha total acesso sobre o sistema que gerencia.

Um *firewall* possui três objetivos principais, que são: ser imune à penetração, controlar todo o tráfego de entrada e de saída e ser o único caminho de entrada/saída dos dados de uma rede. O termo *firewall* faz uma analogia à barreira física a prova de fogo colocada entre duas estruturas para prevenir que o fogo passe de uma para a outra (KUROSE; ROSS, 2010).

A funcionalidade de um *firewall* pode ser simples, como a implementação de um roteador que aplica um filtro de pacotes, ou complexa como um *gateway*, que combina funções de filtros de pacotes e Proxy na camada de aplicação. As primeiras arquiteturas de *firewall* isolavam as redes em um nível lógico, mas na atualidade existem basicamente os sistemas de segurança baseados em Filtro de Pacotes, *Firewall* de Aplicação e Inspeção de Estados.

O *Packet filtering* (filtragem de pacotes) é baseado em uma lista de regras criadas pelo administrador da estrutura de rede, verifica apenas o cabeçalho das camadas de rede e de transporte, podendo ser *stateless* (filtragem estática) ou *stateful* (filtragem dinâmica). A checagem referente as permissões dos acessos de cada usuário são feitas a partir destas regras e trabalham a partir destes dois princípios: Aceitar tudo que não está explicitamente negado ou negar tudo que não está explicitamente autorizado (HOYER; MEIRELLES; PROTECTOR, 2013).

Já o *Firewall* de aplicação ou *proxy* de serviços trata-se de uma solução que atua de forma intermediária entre um computador e a rede destino. Esta solução necessita de um hardware potente, pois trabalha com um número grande de solicitações, opção interessante quando o assunto é segurança, pois a comunicação entre a origem e destino não acontece diretamente. Trabalha como um cache para os endereços que são mais acessados, com isso a navegação web se torna mais rápida, determinados acessos são apenas liberados mediante autenticação do usuário e também é capaz de registrar o tráfego de dados em

log para posteriormente fazer uma análise sobre tais (HOYER; MEIRELLES; PROTECTOR, 2013).

Por fim, o *Stateful inspection (inspeção de estados)* analisam todo o tráfego de dados para encontrar estados, isto é, alguns padrões aceitáveis por suas regras e que, a princípio, devem continuar sendo usados para manter a comunicação. Estas informações são então mantidas pelo *firewall* e usadas como parâmetro para o tráfego subsequente, para evitar pacotes ilegítimos (HOYER; MEIRELLES; PROTECTOR, 2013).

Segundo Scarfone e Hoffman (2009), a inspeção *stateful* melhora as funções de filtros de pacotes, monitorando o estado de conexões e bloqueando pacotes que desviam do estado esperado. Isto é possível através da incorporação de uma maior consciência da camada de transporte. Tal como acontece com a filtragem de pacotes, a inspeção *stateful* intercepta pacotes na camada de rede e inspeciona-os para ver se eles são permitidos por uma regra de *firewall* existente, mas ao contrário da filtragem de pacotes, a inspeção *stateful* acompanha cada conexão com uma tabela de estado.

Arquiteturas mais atuais de *Firewall*s são conhecidos como NGFW ou *firewall* da próxima geração. Segundo Gaaserud (2013), *firewalls* NGFW integram funcionalidades de todas as gerações de *firewalls* e sistemas de detecção de intrusão em um único produto, prometendo alto *throughput*, funcionalidades *all-in-one*, interface de gerenciamento única, aparência sólida e organizada, menor custo de propriedade, melhor controle, visibilidade, segurança, redução da complexidade do conjunto de regras e inspeção de tráfego criptografado.

Um *firewall* da nova geração deve ser o sucessor dos *firewalls stateful* e *port-based*, consolidando uma série de capacidades (features) de segurança, em uma única plataforma. Enquanto mantém as capacidades de *firewall*, adiciona funções de segurança como proteção e prevenção a intrusão, reputação e filtragem de *malwares*, assim como controle de aplicações e usuários (GAASERUD, 2013).

Para Gartner (2017), os NGFW são *firewalls* de inspeção de pacote em profundidade que vão além da inspeção de porta e protocolo e atuam em nível de inspeção de aplicativo, prevenção de intrusão e trazem inteligência de fora do *firewall*. Um NGFW não deve ser confundido com um sistema de prevenção de intrusão de rede (IPS) independente, que inclui um *firewall* embarcado, ou um *firewall* e IPS no mesmo equipamento, sem que estejam intimamente integrados.

Para Palmer (2014), um NGFW deve ter uma mistura das capacidades das primeiras gerações de *firewalls* de rede e de um IIPS e, ao mesmo tempo fornecer uma inspeção mais extensiva de forma a dar uma maior visibilidade do tráfego. Um NGFW deve atender não somente as demandas de conexão básicas, como identificação e controle de portas e protocolos, mas também se

adequar às regras de negócio e segurança da empresa, provendo assim, além da conectividade, uma segurança para o ambiente.

3. NGFW FORTINET

Existem diversas ferramentas de *firewall* de próxima geração disponíveis no mercado, todas atendendo à sua maneira ao que foi descrito acima. Para o ambiente da empresa Tramontina foi escolhido o NGFW da Fortinet chamado Fortigate. Foi realizado um estudo de caso utilizando um ambiente de testes simplificado em relação a estrutura do grupo Tramontina, cujos testes foram executados objetivando analisar algumas funções deste produto. Antes de passar para a explicação destas, serão esclarecidas as partes que compõem o *firewall* de próxima geração da Fortinet.

O sistema operacional utilizado pelo Fortigate é baseado em Linux, tendo o kernel sido customizado pelo fabricante. Ele é o responsável por entregar todos os recursos disponíveis do equipamento de uma maneira fácil e intuitiva, eliminando as configurações de menor utilização e mantendo uma interface clara e simples.

Segundo a Fortinet (2018), o sistema trabalha em conjunto com a rede de segurança do fabricante que foi citada acima, utilizando a inteligência entregue pela mesma para desempenhar as funções de segurança, tais como: *Intrusion Prevention, Application Control, Web Filtering, Antispam, Antivírus, Firewall, Data Leak Prevention, SSL Inspection*, entre outros.

Além das funções relacionadas à segurança existem também as relativas a conectividade, uma vez que este NGFW é capaz de exercer diversas funções relacionadas a serviços de rede, tais como (Fortinet, 2018): VPN IPSec e SSL, Serviço de Autenticação, DHCP e DNS Server, Switch, Roteador, Tradução de Endereços (NAT), Alta Disponibilidade e Tolerância a Falhas, Controlador Wireless e registro de Logs.

Dentro do sistema, a política de *firewall* é dividida em basicamente três estruturas (Fortinet, 2018):

- A primeira, contendo as opções relacionadas às interfaces de origem e destino, endereços IP, usuário ou grupo de usuários de origem (para fins de autenticação), endereço de IP de destino, tipo de serviço ou serviços (protocolos e portas). Adicionalmente, pode ser configurado um horário para o funcionamento, útil quando se faz necessária alguma liberação específica para uma rotina (ex: Backup). Por último, há a opção de habilitar ou não a tradução de endereços (NAT).
- A segunda estrutura diz respeito às configurações dinâmicas, onde são aplicados os perfis de segurança que foram criados, sendo permitido apenas um perfil por módulo de segurança.

- A última estrutura diz respeito a questão de Logs que a política irá produzir, sendo possível registrar apenas os que forem relacionados à segurança (segunda estrutura), ou então de toda a política, mostrando informações de rede da conexão (Exemplo: Portas e protocolos).

As etapas que compõem o processo de inspeção dos pacotes são importantes, visto que para tratamento de tráfego de rede, com o objetivo de controle, é necessário existir uma ordem que organize as etapas de cada verificação para evitar o uso desnecessário de recursos e possíveis erros de validação. O fluxo de inspeção inicia no recebimento do pacote pela interface de rede, o mesmo irá passar por etapas que tem como fim, verificar se esse pacote terá sua conexão liberada ou bloqueada de acordo com o que foi definido pela configuração do NGFW (Fortinet, 2018).

Como pode ser visto na Figura 1, após a entrada do pacote na fase de ingresso é iniciada uma verificação de endereço IP de origem e destino para validar se o mesmo é válido dentro desta rede, em seguida o pacote passa por uma verificação de DoS (*Denial-of-Service*), para validar se não existe nenhuma tentativa de realizar um ataque de inundação (*Flood*) ou escaneamento de portas, logo é feita a checagem de integridade do pacote e validação do roteamento do mesmo.

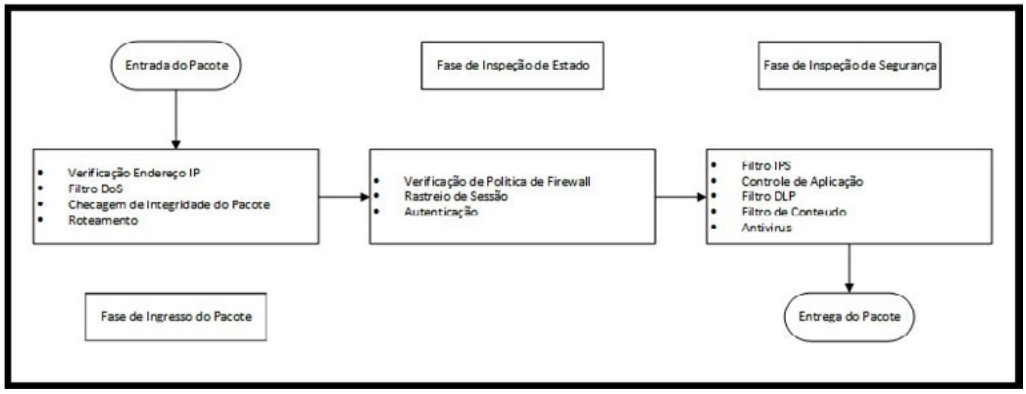
Logo após todas estas etapas terem sido concluídas com sucesso é iniciada a fase de inspeção de estado, nela em primeiro lugar ocorre a tentativa de encontrar uma política de *firewall* que corresponda ao tráfego que está tentando conexão, caso aconteça, se inicia um rastreio de sessão para validar se já existe alguma sessão ativa relacionada, após é verificada a necessidade de autenticação.

Dando sequência, assim que a fase de inspeção de estado estiver concluída com sucesso, se inicia a fase de inspeção de segurança, nela são verificados os itens configurados na política de *firewall* que tem características dinâmicas, começando pela validação de IPS, é realizada uma busca por padrões no tráfego que se assemelham ao comportamento de um ataque ou exploração de vulnerabilidade.

Após é feito o controle de aplicação, da mesma maneira que o IPS, porém buscando o comportamento das aplicações, em seguida é realizado a verificação da prevenção a perda de dados (DLP), tentando encontrar no tráfego se existe alguma extensão de arquivo ou conteúdo que seja controlado, após esta etapa, se inicia o filtro de conteúdo a fim de verificar se o acesso que está ocorrendo é permitido ou não, por último vem a validação do antivírus, para prevenir que arquivos maliciosos entrem no ambiente.

Após todas essas etapas certificarem que o tráfego é válido, é realizada a entrega do pacote, caso aconteça uma falha ou uma negação em qualquer uma das fases é realizado um descarte do pacote, não permitindo que o mesmo prossiga para as próximas etapas.

Figura 1 - Fluxograma de inspeção



Fonte: Dos autores (2018).

4. PROCEDIMENTOS METODOLÓGICOS

Este estudo, quanto aos objetivos é exploratório, por proporcionar maior familiaridade com o problema e quanto aos procedimentos técnicos é bibliográfica, pois é baseada em material já elaborado, constituído principalmente de livros e artigos científicos (GIL, 2008).

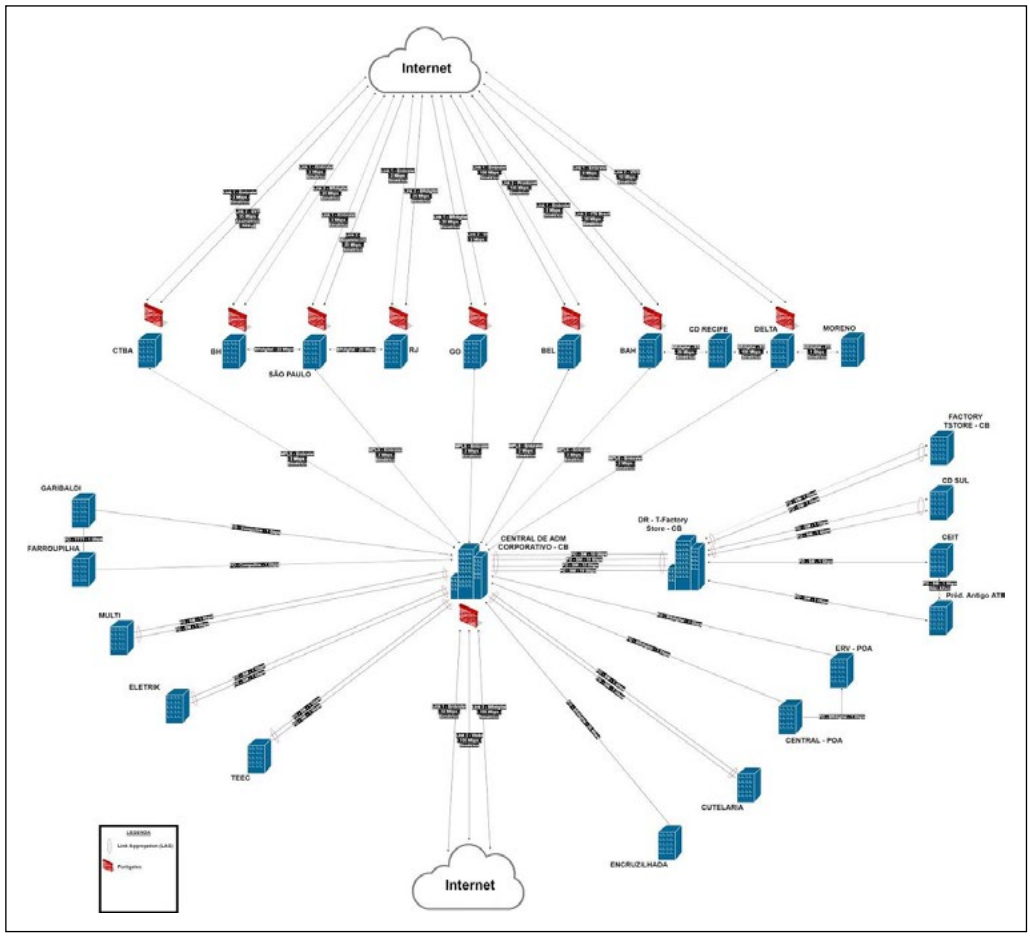
Neste capítulo é feita a apresentação da empresa Tramontina, que serviu para demonstração da comparação e testes dos *firewalls*, em relação a solução utilizada anteriormente e a nova solução da Fortigate implementada entre 2017 e 2018. Em seguida são apresentados os cenários de testes que foram utilizados para demonstração das funcionalidades do NGFW da Fortinet e posterior análise dos resultados.

A Tramontina é reconhecida como referência de qualidade em mais de 120 países. Sua marca se apoia na inovação, no design, na tecnologia e no valor do capital humano para cumprir uma missão indelegável: gerar valor ao consumidor nas mais diversas fronteiras, culturas, épocas e ocasiões. Os mais de 8 mil funcionários que atuam nas fábricas e demais unidades operacionais e comerciais são uma das forças que movem essa marca (TRAMONTINA, 2018).

A estrutura de TI da empresa, conforme a figura 2 demonstra, está organizada da seguinte maneira: Cada fábrica ou CD (Centro de Distribuição) possui sua sala de equipamentos onde chegam dois links de Internet, um da Embratel e um outro de uma operadora local. Os dois links são conectados diretamente aos dois Fortigates que trabalham em *cluster*. A comunicação com a matriz se dá através de um link MPLS da própria Embratel, com exceção das empresas que estão situadas em Carlos Barbosa, Garibaldi e Farroupilha, que estão conectadas por fibra óptica através de duas rotas distintas. As demais lojas (TStore) situadas no Brasil e no exterior, fábricas e CDs que também estão

no exterior, possuem comunicação através do serviço OpenVPN e não possuem o Fortigate nelas. O *firewall* utilizado nelas é um *packet filtering* (Iptables).

Figura 2 - Estrutura do grupo Tramontina no Brasil



Fonte: Dos autores (2018).

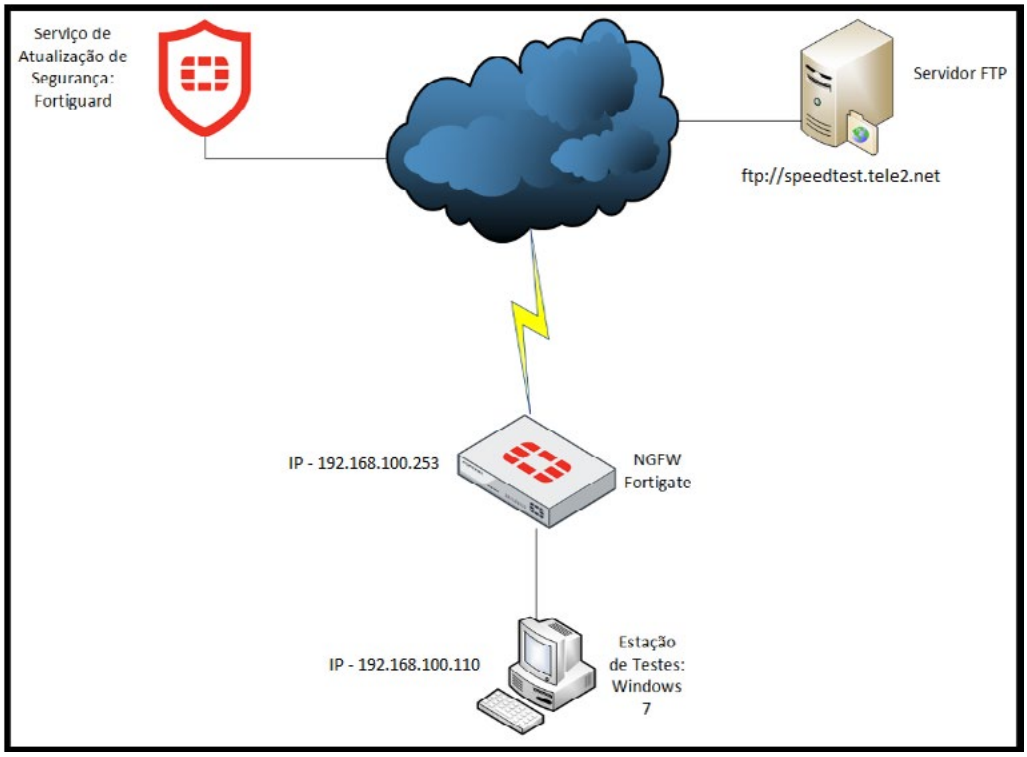
A implementação feita do NGFW da Fortinet no grupo Tramontina iniciou-se pela matriz, em dezembro de 2017, onde permaneceu por um tempo no ambiente para que pudéssemos acompanhar o funcionamento da ferramenta e consequentemente tratarmos e prevermos os problemas que teríamos nas demais unidades. Após isso, os equipamentos das demais unidades foram configurados em Carlos Barbosa e encaminhados para os locais. Estes foram implantados sempre com o acompanhamento da empresa terceira fornecedora da solução até a conclusão do projeto em agosto de 2018.

Com base na estrutura de rede do grupo Tramontina e nas funções em que esses Fortigates exercem em todas as unidades do grupo, a estrutura

da Figura 3 foi montada para o cenário de testes utilizada neste trabalho. Ela conta com uma estação de trabalho utilizando o sistema operacional Microsoft Windows 7, de onde partiram todos os testes, um NGFW físico configurado como *gateway* da rede interna fazendo a ligação da estação de testes com o link de internet, este link fará a conexão com o que chamamos aqui de rede externa. Na rede externa existe um servidor de FTP de testes, na qual será utilizado durante os testes para validação de um dos módulos.

Na rede externa se encontra também o FortiGuard (serviço de atualização do fabricante), o qual tem uma conexão ativa com o NGFW a fim de mantê-lo sempre em conforme com as últimas atualizações de segurança disponibilizadas.

Figura 3 - Topologia da rede para testes com o NGFW



Fonte: Dos autores (2018).

A estrutura lógica foi montada da seguinte maneira, pensando nos testes que foram executados durante a próxima etapa:

- Perfil de antivírus inspecionando os protocolos HTTP, SMTP, POP3, IMAP, MAP e FTP.

- Perfil de filtro de conteúdo web, impedindo o acesso a sites categorizados como sendo "Conteúdo Adulto".
- Perfil de controle de aplicação, impedindo a utilização de aplicações relacionadas a armazenamento de dados em nuvem (*Cloud Storage*).
- Perfil de prevenção a vazamento de dados, impedindo que sejam enviados ou recebidos arquivos do tipo JSP e DOCX.
- Perfil de inspeção SSL que atuará como um MITM (*man-in-the-middle*), para que as conexões criptografadas possam ser inspecionadas.

Utilizando a estrutura de testes apresentada acima, foram criados cenários, dividindo os mesmos por função de segurança, onde em cada cenário foram testadas individualmente a fim de garantir que uma função de segurança não interfira no funcionamento da outra e para conferir se o funcionamento das mesmas acontece conforme o esperado.

Aqui são apresentados os cenários de testes que foram criados, para cada um dos mesmos foram analisados os resultados de acordo com testes feitos durante esta etapa.

- O primeiro cenário é composto pelo teste de Inspeção SSL. Este foi realizado analisando as informações que o navegador na estação de testes gerou, uma vez que o mesmo mostra se a conexão a sites HTTPS está sendo inspecionada por algum dispositivo que não seja uma Unidade Certificadora válida (CA) ou que não esteja configurada para ser confiável. Foram duas etapas, uma utilizando o navegador sem nenhuma configuração externa ou customização e outra instalando o Certificado de CA do NGFW para que a inspeção ocorra de maneira transparente.
- O segundo cenário, foi o de teste do módulo de Antivírus. Para este foi utilizado o site www.eicar.org que reside na rede externa e disponibiliza um arquivo para testes de detecção, este arquivo foi baixado duas vezes, a primeira utilizando o protocolo HTTP e a segunda o HTTPS, a fim de validar a detecção do motor de Antivírus para ambas as conexões.
- O cenário de teste seguinte foi o do módulo de filtragem de conteúdo web, realizando a tentativa de acesso a sites na rede externa que foram categorizados como "Conteúdo Adulto" pelo fabricante, estes foram www.badoo.com.br e www.taurusarmas.com.br.
- No próximo cenário foi utilizado o módulo de Controle de Aplicações. Este teste consistiu em utilizar o aplicativo do Google Drive instalado no computador para verificar se o mesmo consegue se comunicar com o serviço de armazenamento de dados que fica na rede externa e uma tentativa de comunicação com a mesma aplicação via navegador.

- Este último cenário foi o de prevenção a vazamento de dados, o DLP. Para realizar o teste deste módulo, foi feito o upload de um arquivo JSP para o site www.4shared.com e o upload de um arquivo DOC e um DOCX para um servidor FTP de teste, ftp://speedtest.tele2.net, onde ambos se encontram na rede externa.

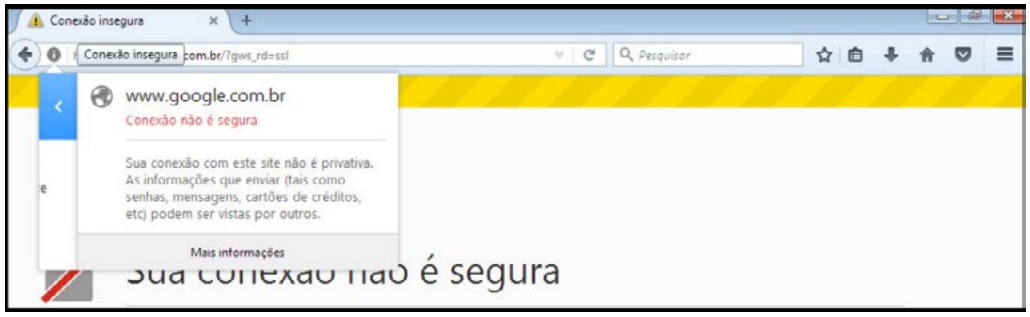
5. RESULTADOS E DISCUSSÃO

Após a configuração dos cenários propostos e testes realizados, foram obtidos os resultados a seguir, mostrando se o módulo funcionou ou não e contendo uma análise sobre as informações resultantes.

5.1 Cenário 01 - Inspeção SSL

Após executar o primeiro teste de inspeção SSL, foi obtido como resultado um alerta do navegador informando "Sua conexão não é segura", conforme Figura 4, que ocorreu devido ao mesmo não conhecer a unidade certificadora do NGFW como válida.

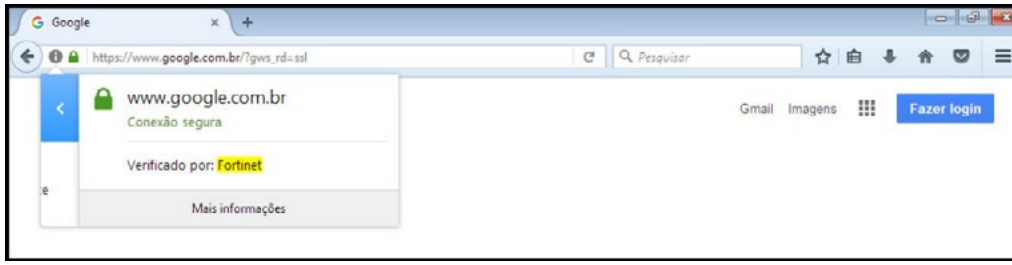
Figura 4 - Erro de conexão segura



Fonte: Dos autores (2018).

No segundo teste, com o certificado de autoridade já instalado como confiável, não houve erro, ao verificar as informações da conexão é possível ver quem inspecionou a mesma, no caso Fortinet (Figura 5).

Figura 5 - Inspeção válida



Fonte: Dos autores (2018).

5.2 Cenário 02 - Antivírus

Conforme proposto pelo cenário, seguem os resultados do teste utilizando a conexão HTTP (Figura 6) e HTTPS (Figura 7). Nas duas tentativas de download do arquivo de testes, o módulo de antivírus foi efetivo, bloqueando a conexão e impedindo a infecção.

Figura 6 - Download com HTTP

Fonte: Dos autores (2018).

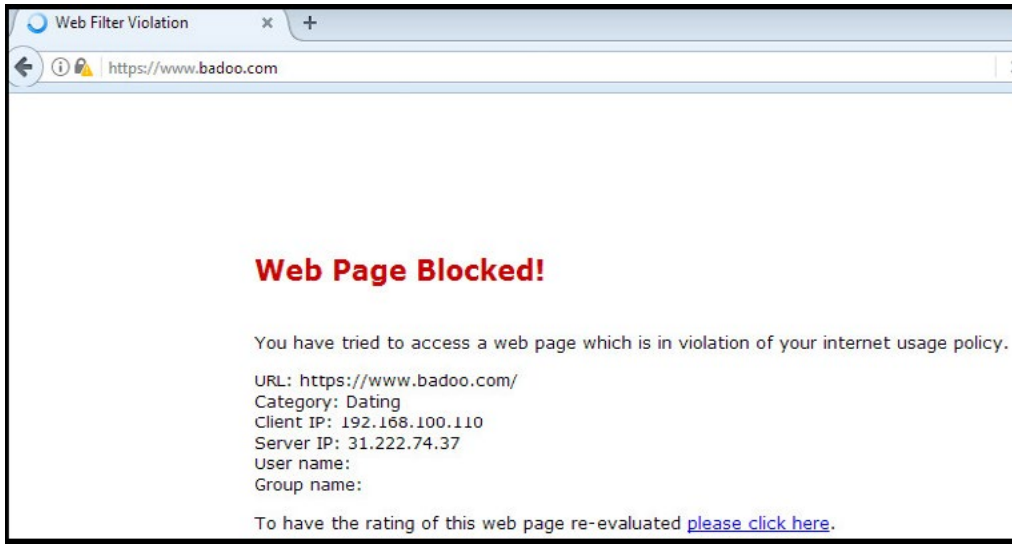
Figura 7 - Download com HTTPS

Fonte: Dos autores (2018).

5.3 Cenário 03 - Filtro de Conteúdo Web

De acordo com o que foi posto pelo cenário, foram realizados dois testes, tentando o acesso a sites que foram categorizados como "Conteúdo Adulto". O primeiro ao site www.badoo.com.br, como mostra a Figura 8 e o segundo ao www.taurusarmas.com.br (Figura 9).

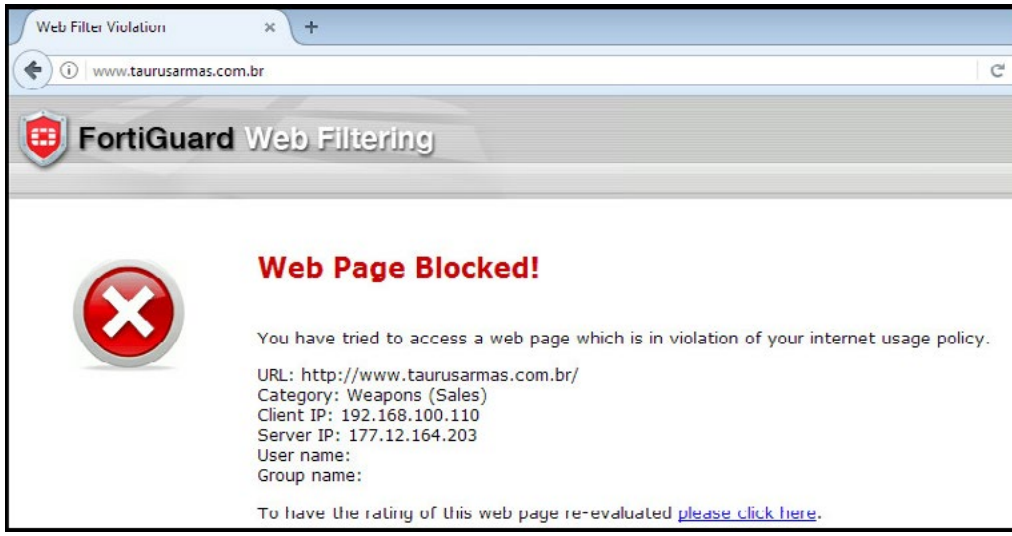
Figura 8 - Acesso site de rede social



Fonte: Dos autores (2018).

Neste caso, o filtro de conteúdo web inspeciona a URL que está sendo acessada e a verifica junto à base de dados do fabricante, caso a mesma pertença a uma categoria que não foi permitida durante a configuração do módulo, a sessão é interrompida e é apresentada uma mensagem contendo os dados do bloqueio. Esta mensagem pode ser customizada pelo administrador do NGFW.

Figura 9 - Acesso site de armas

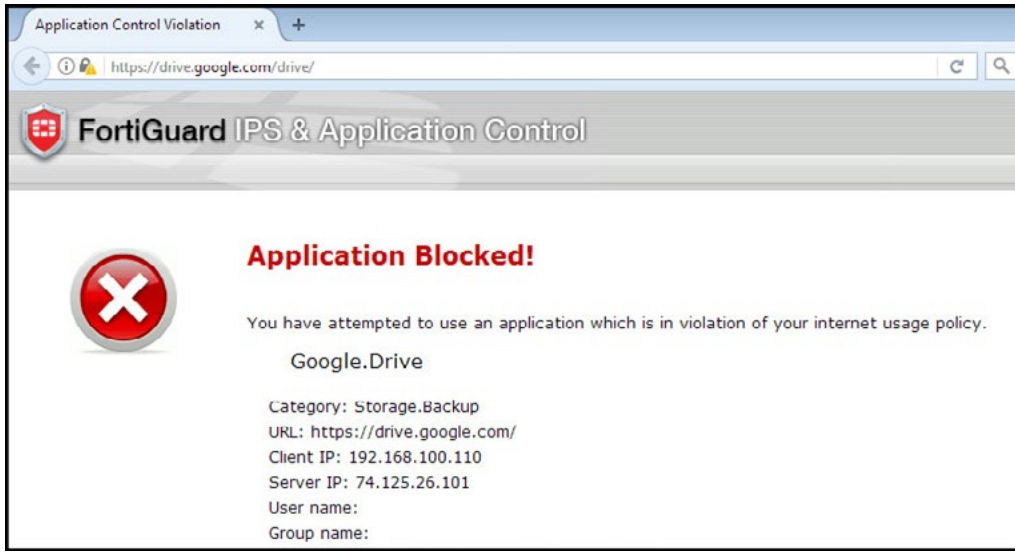


Fonte: Dos autores (2018).

5.4 Cenário 04 - Controle de Aplicações

Este teste aborda a análise das aplicações pelo *Payload*, independente da porta ou protocolo, para tal foi realizado um teste de acesso ao site drive. google.com através do navegador web. A figura 10 mostra que a página foi bloqueada, resultando em uma mensagem no próprio navegador.

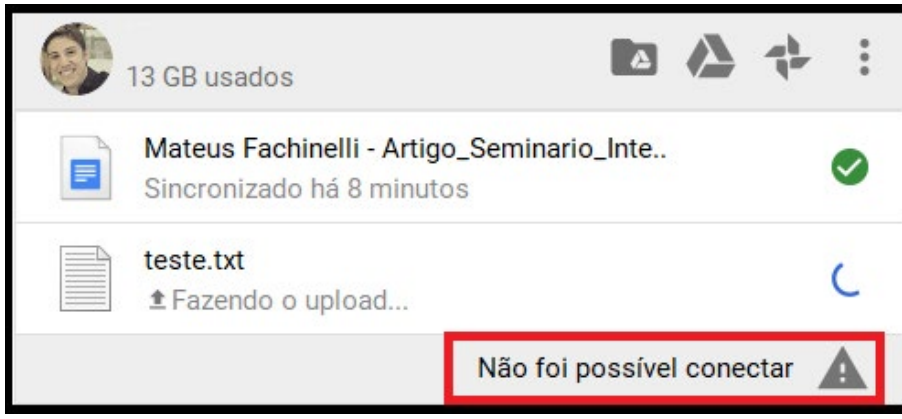
Figura 10 - Acesso Armazenamento em Nuvem Web



Fonte: Dos autores (2018).

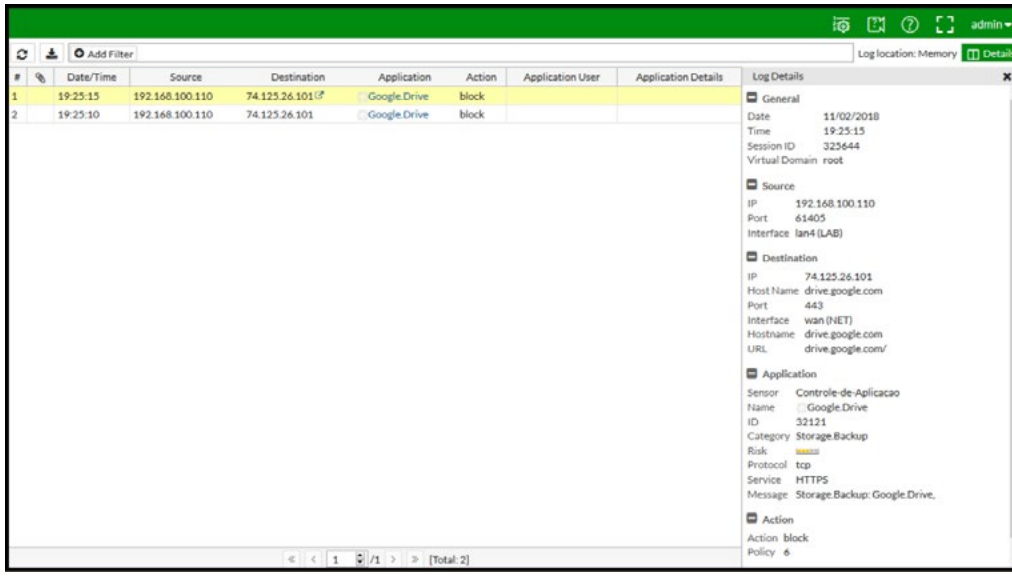
Também foi realizada a tentativa de acesso ao mesmo serviço utilizando a aplicação instalado na estação Windows (Figura 11), nesta pode se verificar que aconteceu um erro de conexão devido a mesma restrição de acesso, porém o bloqueio só pode ser validado verificando o Log de Aplicação (Figura 12).

Figura 11 - Aplicação tentando conectar com armazenamento em nuvem



Fonte: Dos autores (2018).

Figura 12 - Log de Bloqueio tentativa de conexão



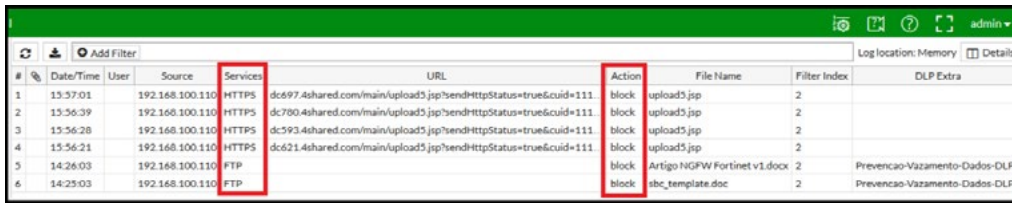
Fonte: Dos autores (2018).

5.5 Cenário 05 - Prevenção a Vazamento de Dados

Neste experimento é possível verificar o funcionamento do módulo de DLP que trabalha inspecionando os pacotes de rede em busca dos padrões configurados. O primeiro teste foi a tentativa de Upload de um arquivo JSP para o serviço de armazenamento de dados em nuvem (www.4shared.com), onde ocorreu um erro na conexão impedindo que o arquivo fosse enviado. Para podermos ter certeza de que o bloqueio foi efetivo, é possível conferir no Log (Figura 13) mostrando uma tentativa de envio de uma extensão não autorizada.

Além do teste com o arquivo JSP, foram realizados mais dois, utilizando um servidor FTP de teste, um arquivo no formato .DOC e outro .DOCX, onde também o bloqueio ocorreu exibindo uma mensagem de erro no próprio cliente de conexão FTP.

Figura 13 - Log bloqueio de Upload



Fonte: Dos autores (2018).

Em relação à solução anterior de *firewall* existente no grupo Tramontina, na qual era composta por um *firewall packet filtering* (*iptables* com interface gráfica), uma ferramenta de proxy e um NAC (Network Access Control) para cada unidade, pode-se comparar na Tabela 1 as diferenças apresentadas em relação à solução anterior com a solução atual da Fortinet.

A estrutura de rede do grupo Tramontina permaneceu a mesma, sendo que antes havia um servidor proxy e outro que era o *firewall* da empresa, já hoje, há apenas um *appliance* que abrange essas funções, dentre outras, configurados em *cluster*.

Quadro 1 - *Firewall* tradicional vs NGFW

Features	***Solução anterior***	**NGFW**
FW / VPN	Suporta	Suporta
IPS	Não suporta	Suporta
AV	Não suporta	Suporta
Web Filtering	Parcial	Suporta
Application Control	Não suporta	Detalhada
E-mail Security	Não suporta	Suporta
DLP	Não suporta	Suporta
Proxy	Não transparente	Transparente
Throughput and Performance	Baixa	Alta
Traffic Filtering(port, IP, Address and protocol based)	Suporta	Suporta
NAT	Suporta	Suporta
Working Layer	*Layer* 2 até *layer* 4	*Layer* 2 até *layer* 7
Dep Inspection	Não suporta	Suporta
Inspection SSL	Não suporta	Suporta
QoS	Não suporta	Suporta
Integration with AD (Active Directory)	Não suporta	Suporta
Reporting	Padrão	Customizáveis, detalhamento das informações

Fonte: Dos autores (2018).

6. CONSIDERAÇÕES FINAIS

Este trabalho teve por objetivo apresentar a tecnologia de *firewall* de próxima geração da Fortinet, implementado no grupo Tramontina, expondo

as principais características que definem um NGFW e comparando com a ferramenta de *firewall* utilizada anteriormente no grupo através de testes e pesquisa bibliográfica. Foi realizado também um embasamento por meio de referências públicas a respeito do *firewall* de estado (*stateful firewall*), com o intuito de apresentar onde o mesmo consegue atuar dentro de uma infraestrutura de comunicação e quais são suas capacidades.

Foram criados cinco cenários de testes modelados de maneira que pudessem apresentar de forma simples e clara a ação de cada função de segurança escolhida para compor o estudo de caso. Nesses cenários foram realizados testes para validar o funcionamento do NGFW perante situações de uso comum relacionadas ao acesso à internet para navegação em sites e realização de downloads ou uploads de arquivos.

Após a realização dos testes pode-se perceber que a aplicação das políticas configuradas nos cenários para controle de uso de recursos na internet foi eficaz, não permitindo que acessos a sites bloqueados, download de arquivos maliciosos ou upload de extensões controladas acontecesse, além de realizar a inspeção de conexões criptografadas.

Em relação a solução de *firewall* anteriormente utilizada na Tramontina, pode-se destacar algumas das funções da ferramenta que facilitam o controle e gerência de toda a rede de dados do grupo pela ferramenta. Dentre elas, análise detalhada do tráfego passante entre suas interfaces, controle sobre aplicações (*layer* 7), controle de banda por aplicação, usuário, inspeção de conteúdo criptografado, autenticação de usuários via FSSO (Fortinet Single Sign-On), acesso à relatórios personalizáveis entre outras.

Por fim, pode-se observar ao término deste trabalho, que cada vez mais os *firewalls* de próxima geração se tornam necessários para a proteção de recursos em qualquer tipo e tamanho de empresa e que essa geração não veio sobrepondo os *firewalls* tradicionais (*stateful firewall*), mas sim absorvendo as capacidades de controle estático e adicionando novas funções que trabalham de maneira dinâmica para que seja possível acompanhar a expansão das tecnologias e recursos que são disponibilizados no mundo digital todos os dias e que vá além, sendo também capaz de barrar ameaças que crescem ao mesmo passo.

REFERÊNCIAS

BRODBECK, Cassio. ***Firewall***: Mecanismos de filtragem stateless e stateful. 2017. Disponível em: <http://blog.ostec.com.br/seguranca-perimetro/*firewall*-stateful-stateless>. Acesso em: 28 jul. 2018.

FILHO, Sócrates. ***Firewall***. 2009. Disponível em: <http://waltercunha.com/blog/index.php/2009/09/18/*firewall*-conceitos/>. Acesso em: 22 jul. 2018.

FORTINET. **FortiGate: Next Generation *Firewall* (NGFW)**. 2018. Disponível em : <https://www.fortinet.com/products/next-generation-*firewall*.htm>. Acesso em: 09 out. 2018

GAASERUD, Aslak. **Towards an unified policy for Next-Generation *Firewall*s**: Creating a high-level language for NGFWs. 2013. 114 f. Dissertação (Mestrado) - Curso de Informática, Informatica, University Of Oslo, Oslo, 2013. Disponível em: <https://www.duo.uio.no/handle/10852/37441>. Acesso em: 08 ago. 2018.

GARTNER. **Next-Generation *Firewall*s (NGFWs)**. Disponível em: <http://www.gartner.com/it-glossary/next-generation-*firewall*s-ngfws>. Acesso em: 11 ago. 2018.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

HOFFMAN, Stefanie. **Fortinet Blog. Security 101**: Next Generation *Firewall* (NGFW). 2013. Disponível em: <https://www.fortinet.com/post/security-101-next-generation-*firewall*-ngfw>. Acesso em: 28 ago. 2018.

HOYER, Erika; MEIRELLES, Pedro; PROTECTOR, Renan. ***Firewall***. 2013. Disponível em: <https://www.gta.ufrj.br/grad/13_1/*firewall*/index.html>. Acesso em: 21 jul. 2018.

KUROSE, J. F.; Ross, K. W. **Redes de Computadores e a Internet**: uma abordagem topdown. 5. Ed. São Paulo: Addison Wesley, 2010.

MANECA, Miguel António Moreira Boavida. ***Firewall*s**: A Próxima Geração. Disponível em: <http://repositorio.ul.pt/bitstream/10451/23557/1/ulfc118229_tm_Miguel_Maneca.pdf>. Acesso em: 01 ago. 2018.

MILLER, Lawrence C. **Next-Generation *Firewall*s**: For Dummies. 2. ed. Hoboken: John Wiley & Sons, Inc., 2016. 77 p.

PALMER, Tony. **McAfee Next Generation *Firewall***: Examining Next Generation Network Security. 2014. Disponível em: <http://research.esg-global.com/reportaction/123400149/TOC>. Acesso em: 12 ago. 2018.

SCARFONE, Karen A., HOFFMAN, Paul. **Guidelines on *Firewall*s and *Firewall* Policy**: Recommendations of the National Institute of Standards and Technology. 2009. Disponível em: <https://www.nist.gov/publications/guidelines-*firewall*s-and-*firewall*-policy>. Acesso em: 04 ago. 2018.

TRAMONTINA. **História da Tramontina**, 2018. Disponível em: <https://www.tramontina.com.br/sobre/historia>. Acesso em: 30 nov. 2018.