Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Relatório de migração de Firewall Virtual para Appliance

Elaborador:	Marcelo Aparecido Barbosa Junior
Elaborador:	Ricardo Alexandre da Silva Junior
Orientador:	Edson Gaseta

FACULDADE DE TECNOLOGIA DE AMERICANA

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

S583r SILVA JUNIOR, Ricardo Alexandre da

Relatório de migração de firewall virtual para appliance. / Ricardo Alexandre da Silva Júnior, Marcelo Aparecido Barbosa Júnior. – Americana, 2019.

21f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1 Segurança em sistemas de informação I. BARBOSA JUNIOR, Marcelo Aparecido II. GASETA, Edson Roberto. III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518.5*

Faculdade de Tecnologia de Americana

Marcelo Aparecido Barbosa Junior
Ricardo Alexandre da Silva Junior

Relatório de migração de Firewall Virtual para Appliance

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 12 de junho de 2019.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Mestre em gestão de redes de telecomunicações
Fatec Americana

Eduardo Antônio Vicentini (Membro)
Mestre em Direito
Fatec Americana

Henri Alves Godoy (Membro)
Mestre em Redes de Computadores
Fatec Americana

SUMÁRIO

Lista de figuras

1 OBJETIVO

Este documento foi escrito com o objetivo de demonstrar e relatar o processo de migração de um sistema de segurança virtual para um *appliance* físico. Será descrito o processo de instalação, configuração e migração das regras de *firewall*, relatando ao final do documento as mudanças e os benefícios que foram atingidos com essa migração. Define-se *appliance* como:

> Um *Appliance* para Banco de Dados é um conjunto empacotado ou pré-configurado com *hardware* (servidores, memória, armazenamento e canais de I/O), *software* (sistema operacional, sistema de gerenciamento de banco de dados e software de gerenciamento), serviço e suporte. É vendido como uma unidade com redundância incorporada para alta disponibilidade e posicionado como uma plataforma para uso de SGBD no processamento de transações *online* (OLTP) e/ou data *warehousing* (DW). (GARTNER, 2019).

Atualmente é muito comum encontrar soluções de segurança como essa em empresas de grande e pequeno porte, sendo utilizado principalmente para proteger suas informações de ataques cibernéticos e contra criminosos cibernéticos. Com o crescimento deste tipo de crime, as empresas buscam mais e mais formas de se prevenir contra furto de informações, e o *firewall* é um dos principais aliados nessa luta em tempos onde não se vive mais desconectado do mundo *online*. Segundo Rohr (2016), e Agostini (2017), casos recentes como o furto de informações sigilosas de 29 mil investidores de uma corretora de valores brasileira em 2016 e o furto de dados bancários de milhares de clientes de uma rede global de hotéis em 2015, colocaram o assunto segurança cibernética em pauta em várias ocasiões, deixando outras empresas em estado de alerta e buscando por melhorias para a segurança de suas redes corporativas.

Por trabalhar diretamente na porta de entrada e saída à internet, como se fosse uma portaria de um edifício, o *firewall* é um grande aliado no combate a estes tipos de ataque, pois monitora e gerencia todo o tráfego na rede, filtrando a navegação evitando que usuários acessem coisas indevidas e prevenindo para que qualquer tipo de acesso externo indevido não seja permitido, controlando e protegendo portas e protocolos de rede. Tudo isso contribui com vários fatores, além de aumentar a segurança com relação à navegação, incluindo um maior controle sobre uso de e-mails, prevenindo contra *malwares* nestes, e aumentando a disponibilidade, pois também conta com funcionalidades como prevenção a ataques de negação de serviço.

Ciente de todas essas possibilidades citadas, a empresa se viu com a necessidade da implantação de um sistema de segurança mais robusto e moderno. Este, contando com uma maior variedade de recursos para melhorar o controle da rede, e a eficácia na segurança.

2 DESENVOLVIMENTO

2.1 O que é *firewall*

Firewall é um dos métodos de segurança disponíveis para redes de computadores, e que é amplamente utilizado dentro de qualquer rede, seja ela particular (empresarial ou doméstica), ou até mesmo numa rede pública.

> Os *firewalls* são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. (TANENBAUM, 2003, p. 583).

Forouzan (2007, p. 1021) afirma que "O *firewall* é um dispositivo (normalmente um roteador ou um computador) instalado entre a rede interna de uma organização e o restante da internet. É projetado para encaminhar alguns pacotes e filtrar outros."

Sua configuração consiste em bloquear todas as portas que não forem utilizadas para o tráfego de informações da rede, assim, faz-se a verificação e autorização de todo o tipo de dado que passa pelos computadores, sejam eles a caminho ou saindo da máquina. Desta maneira, se torna muito mais difícil a chance de alguma tentativa de invasão na rede, pois apenas o necessário será autorizado a trafegar, diminuindo as chances de um possível ataque.

Essa ferramenta possibilita a abertura e o fechamento de portas, o *firewall* também gera logs de todo tipo de movimentação que ocorre no tráfego de dados da rede, para que seja feita toda a verificação de atividade no sistema.

De acordo com Brito (2012) para o funcionamento eficaz do *firewall*, se faz necessário o conhecimento da ferramenta de administração do mesmo, da rede em que ele está sendo aplicado, e de conceitos de navegação externa através da Internet. Tendo o domínio de todos estes aspectos, é possível tirar o máximo proveito desse mecanismo de segurança.

De forma geral, existem três tipos de *firewall* utilizados, o *firewall* de filtragem de pacotes, *firewall* de Aplicação e *firewall* de Controle de Estado. Cada um deles trabalha de uma forma diferente, porém todos voltados para o mesmo propósito, a segurança da rede.

Vale lembrar que o *firewall* por si só, não garante totalmente a segurança da rede, porém diminui consideravelmente a chance de uma invasão ou problemas de segurança. Além disso, possibilita a geração de relatórios de tráfego e tentativa de acessos a determinadas aplicações ou portas, o que ajuda bastante no controle da rede.

2.2 Tipos de *firewall* mais utilizados

2.2.1 *Firewall* de filtragem de pacotes ou *packet filtering*

> Um *firewall* pode ser usado como um filtro de pacotes. E pode encaminhar ou bloquear pacotes com base nas informações contidas em cabeçalhos da

> camada de rede ou de transporte: endereços IP de origem e destino, endereços de porta de origem e destino e o tipo de protocolo (TCP ou UDP). Um *firewall* de filtragem de pacotes é um roteador que usa uma tabela de filtragem para decidir quais pacotes devem ser descartados (não encaminhados). (FOROUZAN, 2007, p. 1022).

Para Pizzolato (2017) é o tipo mais simples que pode ser utilizado, pois ele consiste em configurar no ambiente do *firewall* quais as regras ele deve analisar para autorizar o acesso ou não ao ambiente da rede. Nele existem dois modos para filtragem de pacotes, o estático e o dinâmico.

O estático analisa os pacotes baseando-se nas regras, sem fazer uma análise mais profunda da relação entre uma comunicação iniciada ou qualquer outra, havendo a possibilidade de que não exista resposta para algumas solicitações na rede.

A filtragem dinâmica já trabalha de forma inversa ao estático, proporcionando a criação de regras que se adequam à rede, e permitem que os pacotes trafeguem por ela de acordo com as configurações implementadas, fazendo uma análise do cenário geral em que a regra atua.

2.2.2 *Firewall* de controle de estado ou *stateful inspection*

O *firewall* de controle de estado é considerado a evolução do *firewall* de filtragem dinâmica de pacotes, pois ele tem algumas correções e melhorias com relação a este citado. Basicamente, esse mecanismo de proteção atua fazendo a análise, verificação e comparação dos pacotes que passam por ele.

De acordo com Pizzolato (2017) ele atua fazendo a análise detalhada dos pacotes, buscando sempre fazer uma comparação com o padrão em que a rede opera e a forma com que as conexões costumam ocorrer. Assim, essas informações sempre são utilizadas como parâmetro na verificação. Isso faz com que este tipo de ferramenta seja muito mais maleável que a filtragem de pacotes dinâmica, pois não se baseia simplesmente no fato da porta estar fechada ou não.

Seu diferencial é que é um *firewall* mais avançado e também com uma gama de recursos, pois ele faz o armazenamento do modo com que a rede opera, e adquire conhecimento através dos eventos que ocorrem, para utilização em futuras avaliações. Contando com isso, ele não precisa de muitas intervenções humanas para seu normal funcionamento, o que é uma boa vantagem.

Seu grande problema, está relacionado ao custo de obtenção e utilização, pois apresenta um alto índice de uso de recursos, para aprendizagem e armazenamento de informações. O que pode vir a causar lentidão se não houver um grande poder de processamento onde opera, devido a profunda análise que é feita.

2.3 *Firewall* de aplicação ou a*ppliance firewall*

Para Poloni (2018) o *firewall appliance* consiste em uma forma de proteção que se baseia em um *hardware* que é integrado a administração da rede. Tal característica o torna um pouco mais difícil de implementar e exige maior conhecimento de protocolos de Internet e serviços de rede.

Ele já vem com um software próprio, com configurações definidas pelo fabricante para proteção do ambiente. Essas definições permitem sua modificação, administração e monitoramento. Em resumo é um *firewall* que trabalha fazendo o intermédio entre rede interna e externa.

Uma das maiores vantagens do uso *Appliance Firewall* é que esse tipo de *hardware* já vem de fábrica com toda a estrutura necessária para operar na função de *firewall*, afinal, é um dispositivo desenvolvido para desempenhar o papel de administração e proteção do tráfego de rede.

Este tipo de barreira é considerado uma tecnologia nova, que tende a ser de grande utilização por profissionais da área de Segurança da Informação. Tudo isso devido a sua praticidade e a tecnologia de ponta que são aplicadas nos dispositivos, que permitem uma proteção mais ampla e mecanismos inteligentes que proporcionam resposta automática contra invasões, diminuindo a possibilidade de que falhas na segurança se alastrem por toda a rede.

Um de seus diferenciais é o registro de *logs*, permissão de bloqueio de acesso a determinadas ferramentas (liberação via autenticação de usuário), e também a disponibilidade do *cache* de todas as ações mais utilizadas na rede.

2.4 Cronograma de implementação

Após tomar a decisão de fazer o *upgrade* do sistema de segurança da rede, se fez necessária a criação de um cronograma de implementação, de modo a realizar todo o procedimento de forma organizada e dentro do prazo definido para início das operações do novo *firewall*.

Figura 1 - Cronograma de implementação

Cronograma Migração Firewall							
	10/set	11/set	12/set	13/set	14/set	17/set	18/set
1 - Instalação física do appliance							
2 - Criação das interfaces no firewall							
3 - Criação de IP's virtuais para configuração de NAT							
4 - Configuração dos serviços do Firewall							
5 - Geração do certificado digital para interceptação SSL							
6 - Integração com o Active Directory							
7 - Migração das regras de Firewall							

Fonte: Autoria Própria

Passo a passo da instalação:

- Instalação física do *appliance*: De início, foi feita a acomodação e instalação física do *appliance* no *datacenter* da empresa.
- Criação das interfaces do *firewall*: Logo após a instalação do *appliance*, foram criadas as interfaces do *firewall*.
- Criação dos IP's virtuais para configuração de NAT: Aqui, foram criadas as configurações para roteamento interno da rede, para que os serviços possam ser acessados tanto na rede interna como também na externa.

- Configuração dos serviços do *firewall*: Após toda a configuração inicial ser finalizada, foram configurados todos os serviços em que o *firewall* irá atuar.
- Geração do certificado digital para interceptação SSL: Foi gerado e aplicado o certificado SSL nas estações de trabalho por política de grupo, para que o *firewall* possa ler as informações que trafegam na rede mesmo que as mesmas estejam criptografadas, para assim, analisar e poder buscar possíveis ameaças.
- Integração com o *Active Directory*: Foi feita a integração das regras de *firewall* com o AD para que ele possa relacionar usuários e estações de trabalho. Gerando relatórios mais detalhados sobre o uso da internet.
- Migração das regras de *firewall*: Por fim, após finalizar todo o processo de implementação e migração do novo *appliance*, foram migradas as regras do *firewall* antigo que estava em operação.

2.5 Estrutura lógica

2.5.1 Estrutura lógica antes da migração

Para um melhor entendimento do que foi realizado, será mostrado a seguir como era o ambiente antes da implementação da nova estrutura de rede, e como era seu fluxo de funcionamento.

Na figura 2, é detalhada a infraestrutura lógica da rede antes do trabalho realizado, demonstrando o fluxo iniciando nos *links* de entrada e chegando até o usuário final.

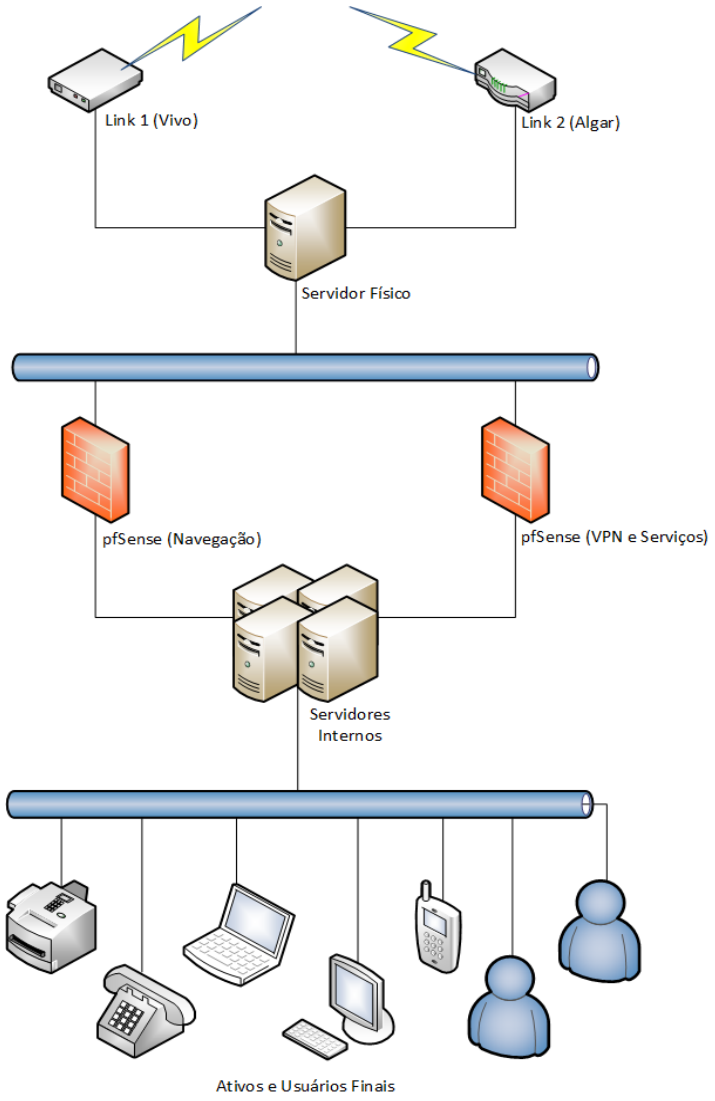
A estrutura possui dois *links* de navegação, um *link* “sujo” para navegação comum como acesso à internet, e um *link* dedicado, que possui uma garantia de disponibilidade maior e um prazo de SLA menor, utilizado para publicação de serviços externos como servidores de *e-mail* e VPN.

Os dois *links* chegam direto ao servidor físico, que possui um sistema operacional para virtualização e é administrado remotamente. Dentro do servidor está configurado um vSwitch que é responsável pela comunicação entre máquinas virtuais e para deixar o ambiente preparado em caso de um novo servidor físico ser adicionado, sendo assim possível administrá-los centralizadamente e unificando os dois ambientes.

Existem dois *firewalls* virtuais configurados, um sendo o *gateway* principal contendo todas as regras de acesso à internet, liberação de portas de entrada e saída, onde é gerado os relatórios de acesso à internet e também onde está configurado o proxy da rede. O segundo *firewall* funciona como *gateway* de VPN, onde este serviço está configurado, e também é o *gateway* dos servidores *web* e de *e-mail*, pois é por este *firewall* que a conexão é direcionada para o *link* dedicado.

Além dos servidores *web* e de *e-mail*, existem os servidores de *Active Directory*, banco de dados, servidor de arquivos, servidor de imagem, etc., que utilizam o primeiro *firewall* como gateway principal, e mais abaixo no fluxo estão todos os ativos de rede e os usuários, que podem se comunicar com a rede por qualquer um desses ativos.

Figura 2 - Estrutura antiga da rede



Fonte: Autoria Própria

2.5.2 Estrutura lógica após migração

Na figura 3, é ilustrado o ambiente após a instalação do novo *appliance*, demonstrando a diferença no fluxo de rede do ambiente.

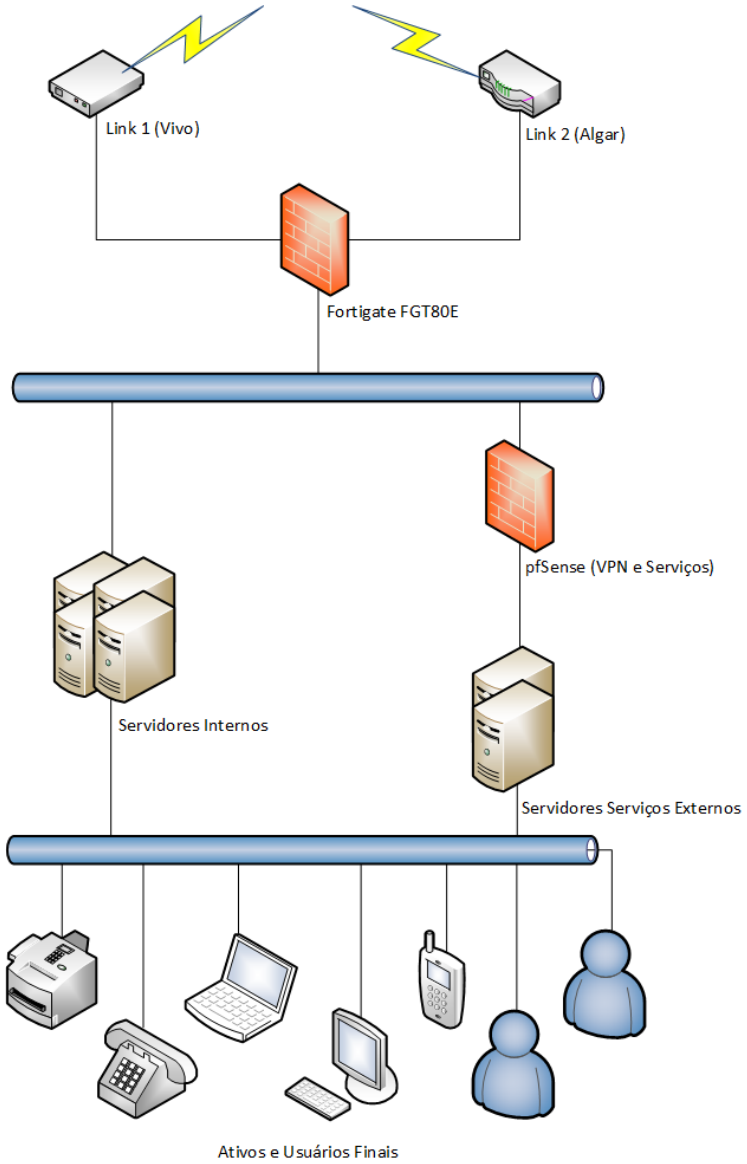
A estrutura conta com dois *links* de navegação, um comum e um dedicado, e todo o tráfego realizado, de entrada e saída, passa antes pelo *firewall* principal, onde é feita toda a filtragem de pacotes.

Os servidores menos críticos e que não necessitam de conexão com a internet em tempo integral tem como *gateway* o *firewall* principal, porém existem regras que impedem o acesso direto aos servidores para aumentar a segurança, e os servidores

de VPN e *e-mail* passam primeiramente pelo segundo *firewall* onde estão todas as configurações de roteamento das VPNs e IP's dedicados.

Ao final do fluxo, estão os ativos e os usuários finais, que agora são identificados individualmente pelo *firewall* por conta da integração realizada com o servidor de *Active Directory*. Nenhuma alteração nas configurações de rede dos ativos foi necessária pois as configurações são todas distribuídas por DHCP e o mesmo também passa rotas customizadas para utilização das VPNs, utilizando somente um *gateway* principal.

Figura 3 - Nova estrutura da rede



Fonte: Autoria Própria

3 RESULTADOS

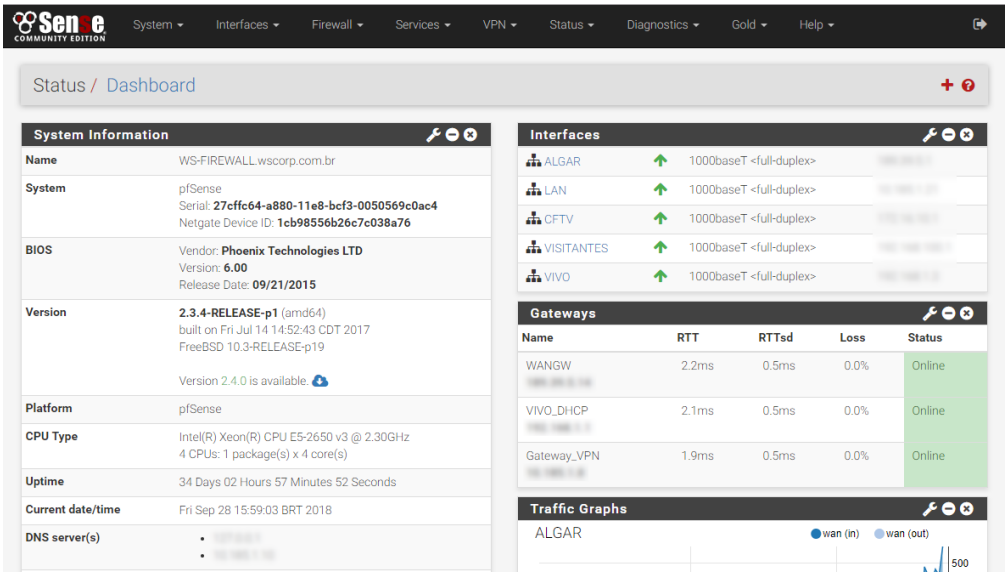
Neste tópico será apresentada a comparação das configurações da ferramenta *pfSense* e *FortiGate*.

3.1 *Dashboard*

Dashboard é a tela principal do *firewall*, onde informações vitais do sistema são apresentadas.

A tela principal do *pfSense,* como visto na figura 4, possui algumas informações mais básicas, como nome, tipo de sistema, versões e configurações de *hardware*. Possui também algumas informações sobre as interfaces do *firewall* e *gateway*, contemplando os *gateways* e as configurações de IP.

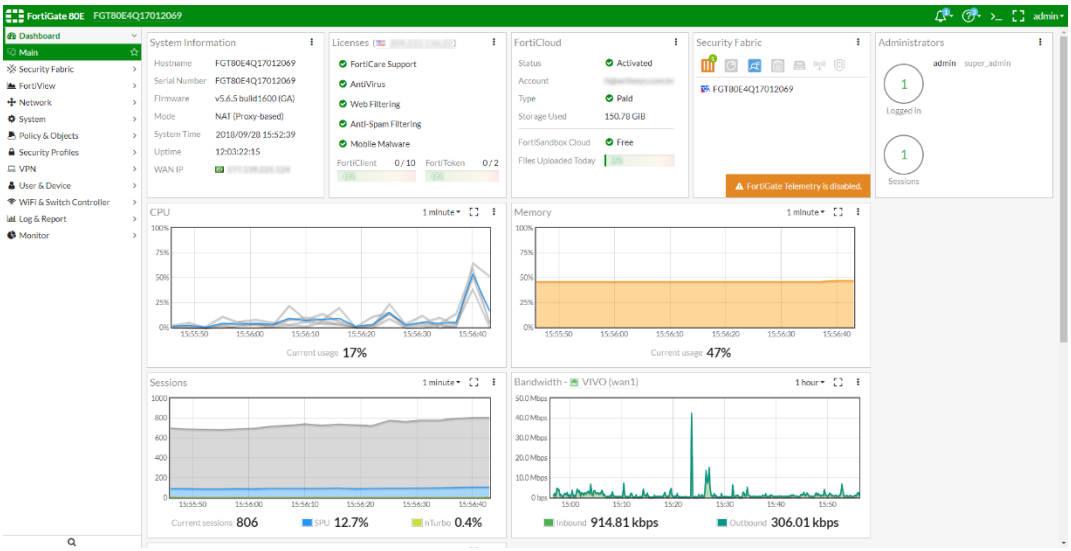
Figura 4 - *Dashboard pfSense*



Fonte: Autoria Própria

A tela principal do *Fortigate,* conforme figura 5, contém algumas informações mais detalhadas, como os tipos de serviço que estão ativos, usuários que estão conectados no sistema, informações sobre licenciamento e consumo de hardware e das interfaces de rede em tempo real.

Figura 5 - *Dashboard Fortigate*

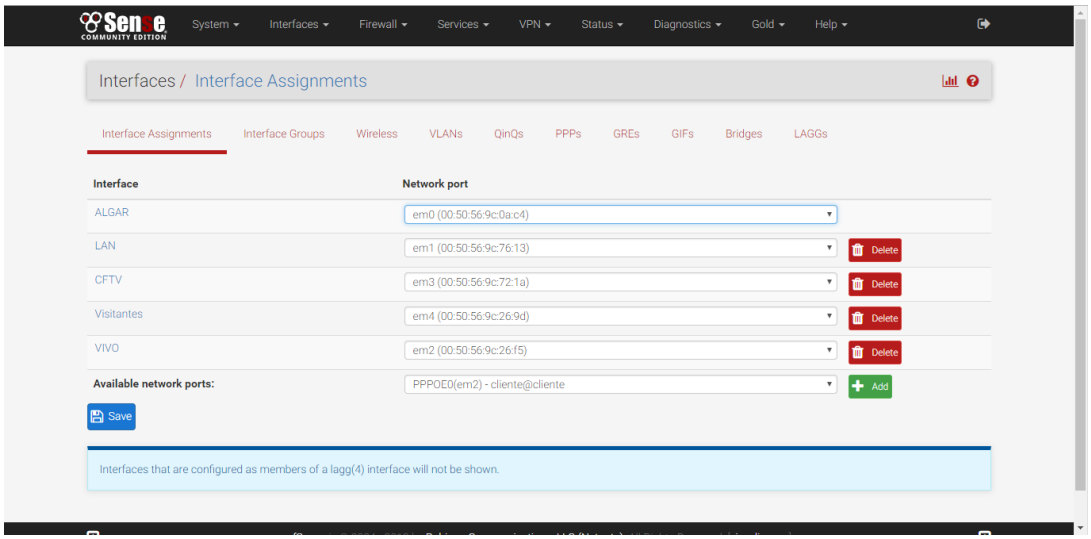


Fonte: Autoria Própria

3.2 Interfaces

Na tela de interfaces, conforme figura 6, é possível encontrar a configuração das interfaces que estão em uso no sistema, assim como sua nomenclatura e MAC *Address*. No *pfSense* a tela é bem simples, contando apenas com o básico, como o nome da interface, sua nomenclatura e o MAC *Address*, e por ser um *firewall* virtual, não possui a visualização das portas de rede físicas.

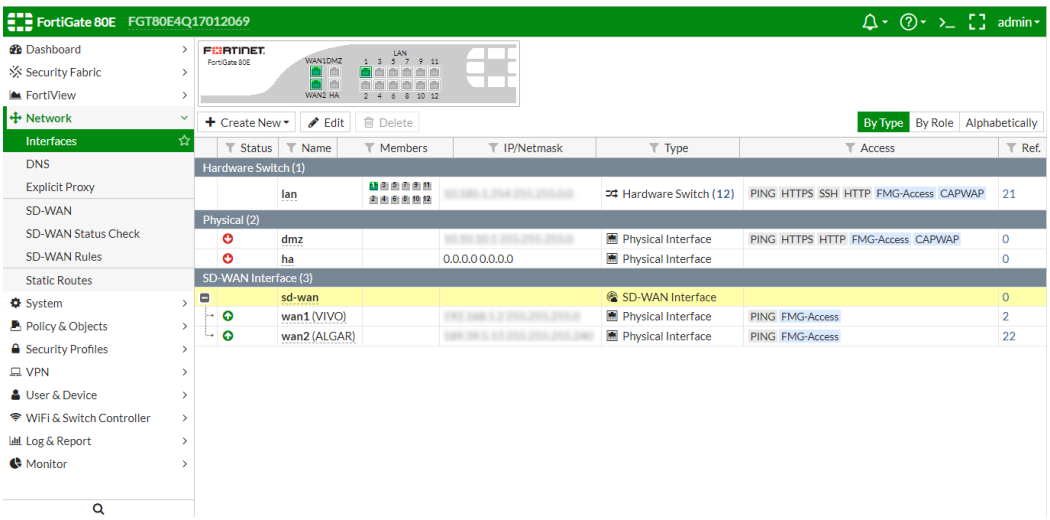
Figura 6 - Interfaces *pfSense*



Fonte: Autoria Própria

No *Fortigate*, como visto na figura 7, temos algumas informações mais importantes nas interfaces, como nome e status da interface, o tipo de interface, quais tipos de acesso estão liberados, o IP de cada interface, em quantas regras ela está referenciada e também nos dá uma visão das portas físicas do *firewall*.

Figura 7 - Interfaces *Fortigate*

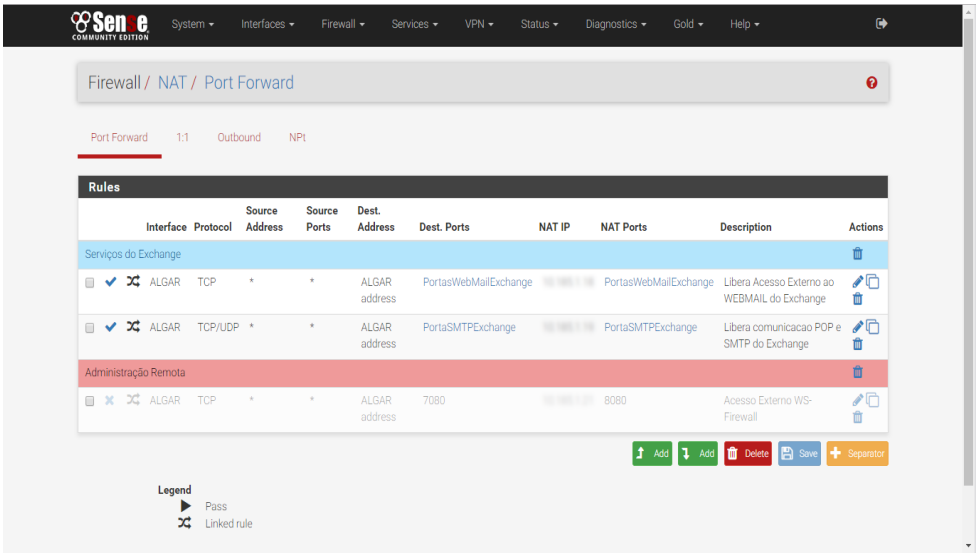


Fonte: Autoria Própria

3.3 NAT

Na tela de NAT (*Network Address Translation*), conforme figura 8, é onde se tem as configurações de roteamento interno para publicação de serviços externamente para que se possa ser feito o acesso ao serviço de fora da rede privada.

Figura 8 - NAT *pfSense*

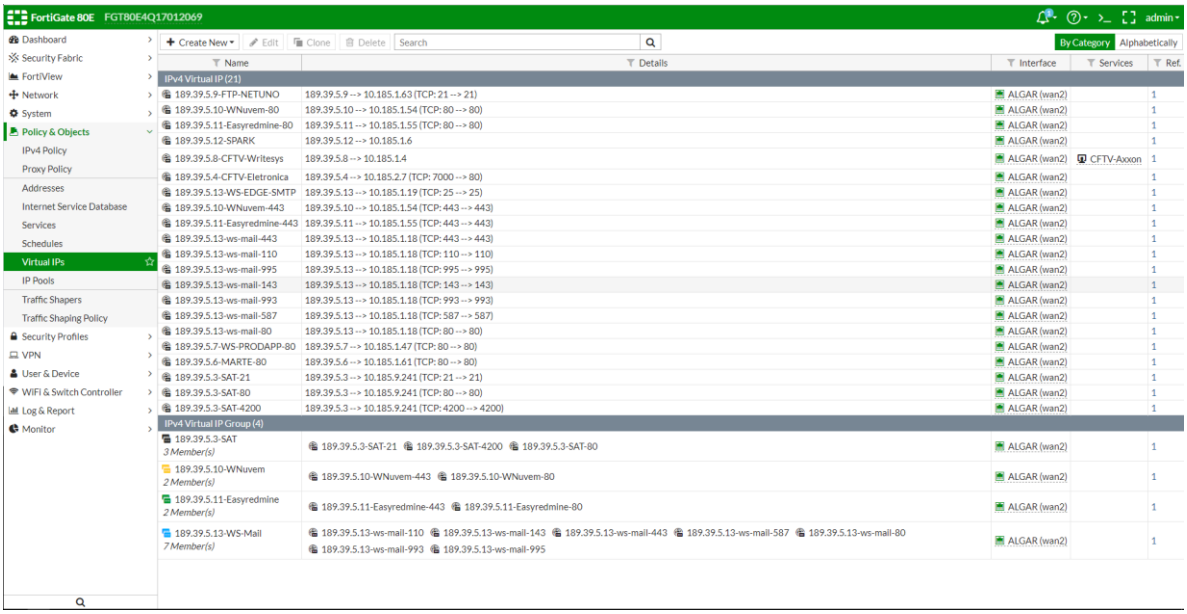


Fonte: Autoria Própria

No *pfSense* temos uma tela básica com a interface, os protocolos sendo utilizados pelo serviço, endereços e portas de origem e também os endereços e portas de destino.

No *Fortigate* a visão é mais limpa e ampla, como visto na figura 9, porém o conteúdo é basicamente idêntico, contemplando o nome e endereço IP do serviço, a rota interna que deverá ser feita, qual interface será utilizada para receber a conexão e as portas liberadas para acesso, assim como em quantas regras cada NAT está referenciado.

Figura 9 - NAT *Fortigate*

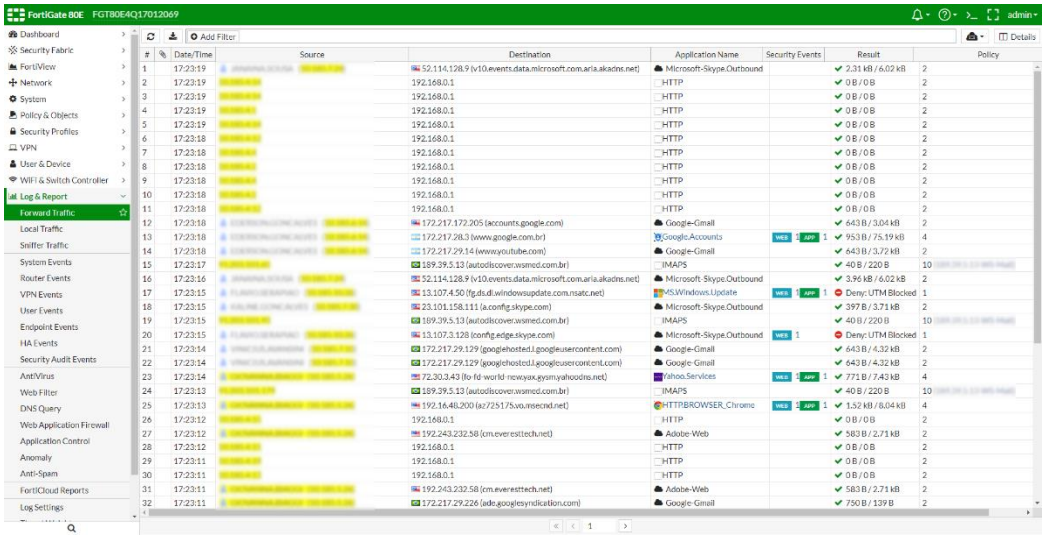


Fonte: Autoria Própria

3.4 Relatório de tráfego de rede

Na figura 10, está o relatório de tráfego de rede onde é possível acompanhar todos os acessos que estão sendo realizados em tempo real, contemplando o nome dos usuários, seus respectivos IPs, o destino qual estão acessando, o tipo de aplicação, quais regras de *firewall* estão sendo aplicadas e o resultado (se o tráfego foi permitido ou negado).

Figura 10 – Relatório tráfego de rede

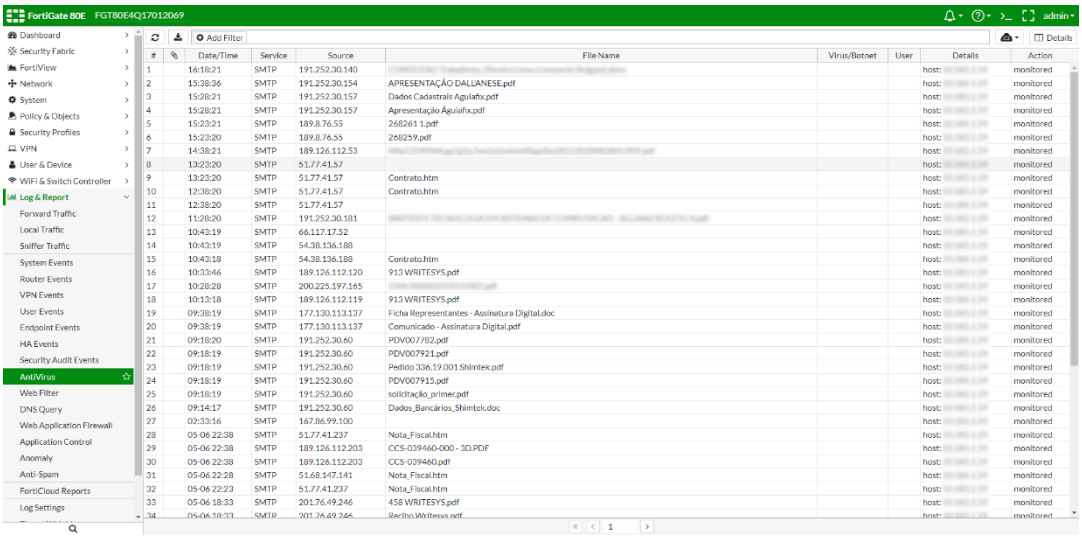


Fonte: Autoria Própria

3.5 Relatório de antivírus

Na figura 11, está um exemplo do relatório de antivírus gerado pelo *firewall Fortigate* onde possibilita, em tempo real, acompanhar todos os arquivos que chegam e que são enviados, contemplando informações como o serviço, a origem, o *host* por qual o arquivo o passou e a ação (se foi apenas monitorado ou se existe alguma ameaça). Caso o arquivo esteja infectado, o relatório exibe qual o tipo de vírus existente no arquivo e para qual usuário ele foi enviado.

Figura 11 – Relatório antivírus

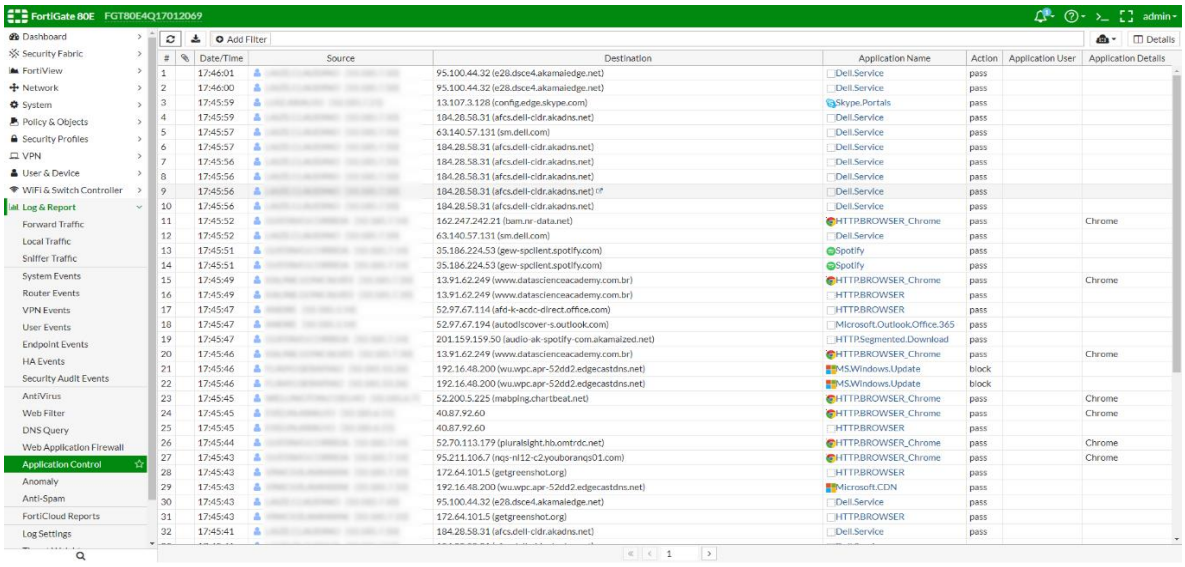


Fonte: Autoria Própria

3.6 Relatório de controle de aplicação

No relatório de controle de aplicação é possível acompanhar quais aplicações estão sendo usadas no momento, contemplando informações como origem, destino, o nome da aplicação e a ação (se foi permitido o tráfego ou se foi negado), como pode ser visto na figura 12.

Figura 12 – Relatório controle de aplicação

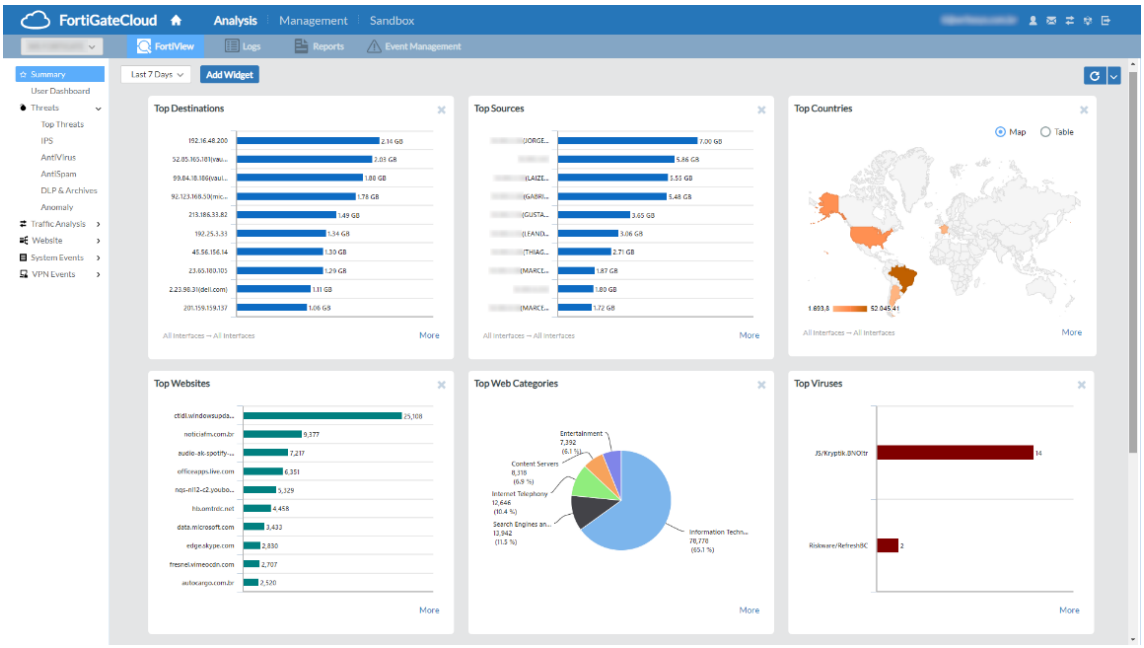


Fonte: Autoria Própria

3.7 Relatórios *FortiCloud*

O *FortiCloud* é um serviço que foi adquirido em conjunto para armazenamento em nuvem dos relatórios gerados pelo *firewall*. Esse serviço armazena todos os registros na nuvem pelo prazo de 1 ano para que seja possível visualizar relatórios de acesso, controle de aplicação, antivírus e também estatísticas do *firewall* de um determinado período. O *dashboard* do *FortiCloud*, conforme figura 13, exibe gráficos dinâmicos para uma rápida visualização do tráfego na rede dos últimos 7 dias. Um clique em um dos gráficos ou em algum item do gráfico exibe uma informação bem mais detalhada dos dados.

Figura 13 – Relatório *FortiCloud*



Fonte: Autoria Própria

4 CONCLUSÃO

Como especificado anteriormente no projeto, o processo de migração do *firewall* virtual para *appliance* demandou uma grande mobilização interna para que tudo pudesse ocorrer em conformidade, pois, para sua implantação, tiveram que ser aplicadas todas as precauções iniciais quanto a organização, como por exemplo a realização de reuniões para discutir possíveis problemas da migração, montagem de um cronograma de implementação e a escolha do *appliance* ideal para a infraestrutura.

Após a definição destas questões fundamentais, se fez necessário todo o processo de migração do *firewall* em si, envolvendo toda a parte da criação das interfaces, criação de IPs para configuração de NAT, serviços, geração do certificado SSL, integração com *Active Directory*, etc. Todos esses processos tiveram que ser executados com base no cronograma que foi apresentado, e foram atentamente realizados seguindo os parâmetros de segurança adequados, utilizando um ambiente em paralelo para realização das configurações e sempre trabalhando com cópias dos arquivos do *firewall* antigo que estava em atividade. Além da aplicação de testes durante cada alteração.

Desta forma, foi possível realizar a migração com o máximo de êxito, e com o aproveitamento adequado do novo equipamento de segurança, pois como especificado no relatório, a infraestrutura de rede apresentou muito mais segurança e estabilidade, pois deixou os servidores e equipamentos da empresa menos vulneráveis e trabalhando com um fluxo de dados mais adequado.

Uma das grandes vantagens de ter sido realizada a migração foi o maior detalhamento nos relatórios gerados, podendo acompanhar de uma forma mais ampla o que acontece na rede em tempo real e, junto com a inspeção SSL, é possível saber tudo o que acontece e quando acontece, quem foi o responsável, da onde veio e para onde foi, e também é possível saber até mesmo se algum arquivo estava infectado e qual o tipo de *malware* que o arquivo continha. Outra grande vantagem foi a redundância de *links*, que após a migração foi possível ser feita de uma forma mais estável pois os dois *links* chegam diretamente no *firewall*, facilitando o gerenciamento por conter uma porta dedicada para cada *link*.

Após o início das operações com o novo *firewall*, notou-se uma nítida vantagem com relação ao anterior, pois além dos benefícios que foram adquiridos no desempenho e segurança, devido ao tipo de tecnologia e o suporte proporcionado, foi percebida uma grande diferença com relação a quantidade de recursos disponíveis para o monitoramento da segurança do ambiente e ferramentas para aplicação de novos recursos e restrições para a rede, com o objetivo de aumentar ainda mais o nível de controle e segurança.

REFERÊNCIAS BIBLIOGRÁFICAS:

AGOSTINI, Renata. **Hackers roubam dados de 29 mil clientes da corretora XP investimentos**. [*S. l.*], 23 jan. 2017. Disponível em: https://www1.folha.uol.com.br/mercado/2017/01/1852499-hackers-roubam-dados-de-29-mil-clientes-da-corretora-xp-investimentos.shtml?utm_source=blog&utm_campaign=rc_blogpost. Acesso em: 29 abr. 2019.

ALERTA SECURITY. **Tipos de *firewall* e suas especificações.** [*S. l.*], 2015. Disponível em: https://alertasecurity.com.br/downloads/ebook/TIPOS-DE-FIREWALL-E-SUAS-ESPECIFICA%C3%87%C3%95ES.pdf. Acesso em: 29 abr. 2019.

BRITO, Edivaldo. **O que é *firewall*?**. [*S. l.*], 30 jun. 2016. Disponível em: https://www.techtudo.com.br/artigos/noticia/2012/10/como-funciona-o-firewall.html. Acesso em: 29 abr. 2019.

FOROUZAN, Behrouz. **Comunicação de dados e redes de computadores**. Porto Alegre - RS: AMGH, 2007.

GARTNER. ***Database appliances***. [*S. l.*], 2016. Disponível em: https://blogs.gartner.com/it-glossary/database-appliances/. Acesso em: 29 abr. 2019.

HAUTSCH, Oliver. **Como funciona o *firewall*?** [*S. l.*], 6 jan. 2010. Disponível em: https://www.tecmundo.com.br/seguranca/3329-como-funciona-o-firewall-.htm. Acesso em: 29 abr. 2019.

PIZZOLATO, Rafael. **Quais os tipos de *firewall* e suas diferenças?** [*S. l.*], 2 abr. 2018. Disponível em: https://blog.starti.com.br/tipos-de-firewall/. Acesso em: 29 abr. 2019.

POLONI, Brayan. ***Firewall appliance*: saiba tudo sobre o tema**. [*S. l.*], 15 ago. 2018. Disponível em: http://introduceti.com.br/blog/firewall-appliance-saiba-tudo-sobre-o-tema/. Acesso em: 29 abr. 2019.

ROHR, Altieres. **Vírus roubou dados de cartões de crédito em hotel de SP**. [*S. l.*], 19 jan. 2016. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/virus-roubou-dados-de-cartoes-de-credito-em-hotel-de-sp-revela-hyatt.html?utm_source=blog&utm_campaign=rc_blogpost. Acesso em: 29 abr. 2019.

TANENBAUM, Andrew Stuart. **Redes de Computadores**. Rio de Janeiro - RJ: Elsevier, 2003.