PROPOSTA DE UM AMBIENTE DE ALTA DISPONIBILIDADE UTILIZANDO *APPLIANCE* DE REDE: *PFSENSE* E *MIKROTIK*[1]

Gustavo Santos Silva
Graduando do 8º período do curso de Sistemas de informação do UNIPAM.
E-mail: gustavosilva@unipmam.edu.br

Fabrício Geraldo Araújo
Professor do curso de Sistemas de Informação do UNIPAM.
E-mail: fabricioa@unipmam.edu.br

RESUMO: A evolução do monitoramento dos sistemas de TI permite uma abordagem equilibrada para manter as coisas em ordem e progresso, ao mesmo tempo que avança na capacitação de práticas recomendadas. É justamente por ser vital/essencial para o negócio de uma empresa, que esse bem traz consigo uma necessidade básica: segurança da informação. Hoje é importante ter uma rede de qualidade e segurança para navegação e utilização dos diversos serviços que nela trafegam. O presente artigo tem como objetivo apresentar um estudo entre dois sistemas pré-configurados ou appliances de rede, o PfSense (baseado na plataforma UNIX FreeBSD) e o RouterOS (Mikrotik, baseado na plataforma LINUX), em dois modelos de redes, seja ele corporativo (privado) ou de acesso público (CyberCafé ou Provedores de Internet com/sem fio). Que poderá ser utilizado para auxiliar administradores de redes e sistemas, em uma escolha mais adequada sobre qual sistema melhor se encaixa no gerenciamento de determinado tipo de rede.
PALAVRAS-CHAVE: Appliances de Rede. PfSense. Mikrotik. Segurança da Informação.

ABSTRACT: The evolution of IT systems monitoring allows a balanced approach to keep things in order and progress, while advancing the training of best practices. It is precisely because it is vital / essential for the business of a company that this good brings with it a basic need: information security. Today it is important to have a network of quality and safety for navigation and use of the various services that travel in it. This article aims to present a study between two preconfigured systems or network appliances, PfSense (based on the UNIX FreeBSD platform) and RouterOS (Mikrotik, based on the LINUX platform), in two models of networks, be it corporate (private) or public access (CyberCafe or Wireless Internet Provider). It can be used to assist network administrators and systems, in a more adequate choice of which system fits best in managing a particular type of network.
KEYWORDS: Network Appliances. PfSense. Mikrotik. Information security.

---

[1] Trabalho apresentado na área temática 1 – Novas tecnologias e ferramentas para gestão empreendedora do XIV Congresso Mineiro de Empreendedorismo, realizado de 5 a 7 de novembro de 2018.

1 INTRODUÇÃO

No final da década de 1960, ainda não era possível substituir os sistemas multitarefas de tempo compartilhado. O gerenciamento de redes de computadores resumia-se em transferir dados de um lado para outro utilizando apenas disquetes, o que comprometia a integridade dos dados por causa das falhas de gravações ou, até mesmo, o transporte e manuseio do disco. Universidades que utilizavam computadores levavam um tempo absurdo para transferir dados de um lado para outro. Hoje, em contrapartida, esse limite é quase infinito, sendo possível enviar e receber grandes quantidades de dados atravessando continentes, não somente paredes como no passado. (WANDERSON, 2012).

Rememorando os tempos anteriores à conveniência do Wi-Fi e à proliferação da virtualização, antes da tecnologia sem fio e da computação em nuvem de hoje, a rede era uma entidade física, em sua maior parte cabeada, controlada por roteadores e switches, com conectividade à Internet através de um backhaul pelo data center. Nesse contexto, VoIP era raro e a conectividade em qualquer lugar – quando havia – era fornecida pela largura de banda de baixa qualidade. Hoje é fundamental criar as condições em que a distância entre o provedor de informações, normalmente um computador (PC), seja a mais curta e direta possível (ADATO, 2015).

No momento em que a Internet passou a ser onipresente no espaço de trabalho, não se estava preparado para esse pico e os problemas para organizar o uso da rede tiveram que ser corrigidos. O mesmo ocorreu quando as pessoas começaram a compartilhar recursos de um montante de novos dispositivos.

Diante da velocidade com que a tecnologia evolui, comparada com ritmo da evolução do conhecimento da humanidade, não há tempo a perder em relação à preparação para gerenciar e monitorar as redes de amanhã.

Porém, quando se passa muito tempo pensando no futuro, e esquece o passado, o presente, e acaba entrando no velho ditado: “aqueles que não podem lembrar o passado, estão condenados a repeti-lo” (SANTAYANA, 1905). Mesmo sendo todas afirmativas intimidantes, a realidade é que as duas coisas não são realmente mutuamente exclusivas.

Essa realidade mudou, mas, mesmo nos tempos atuais, é de extrema importância sistemas ainda mais avançados, para assim elevar o nível de desenvolvimento tecnológico das redes de computadores. Estes sistemas avançados já são realidade e podem ser utilizados na forma de sistemas pré-configurados. Existem muitas soluções que podem ser aplicadas para proteção e disponibilidade das informações, sendo o *firewall* umas das mais utilizadas pelas empresas.

A meta de qualquer organização de Tecnologia da Informação é garantir que toda a infraestrutura subjacente aos aplicativos esteja funcionando, assim mantendo as três propriedades fundamentais da segurança de informações (confidencialidade, integridade e disponibilidade). Gerenciar e monitorar redes de computadores de forma segura, rápida e eficiente, necessita de ferramentas de monitoramento para alertar sobre problemas ocorridos no ambiente de produção, porém tendências deste monitoramento apontam para uma evolução rumo à análise, à automação e à correção.

A complexidade do ambiente de rede de hoje ressalta o fato de que, embora as lições do passado ainda sejam importantes, um novo conjunto de fundamentos para o monitoramento e gerenciamento de redes é necessário para enfrentar os desafios relativos à administração de rede de hoje. Esses novos fundamentos incluem mapeamento de rede; gerenciamento da tecnologia sem fio; *firewalls* de aplicativos; planejamento de capacidade; informações sobre desempenho dos aplicativos. (ADATO, 2015)

A presente pesquisa é relevante pelo fato de apresentar a utilização de *appliance* de redes, para garantir o acesso a essas informações e para que não ocorra a interrupção nos acessos dos serviços, que podem causar grandes prejuízos financeiros e de imagem à empresa. Sendo a mesma configurada com as seguintes funcionalidades: um *firewall* de alta disponibilidade com tolerância a falhas, um balanceamento de carga, roteamento, dentre outras a serem definidas durante o projeto.

Os resultados dos testes práticos e da teoria pesquisada, permitiu analisar os pontos positivos e negativos, do desempenho de ambos os sistemas em questão. Para que possa auxiliar os administradores de redes, em uma escolha mais adequada, sobre qual sistema melhor se encaixa no gerenciamento e monitoramento de determinado tipo de rede.

Desse modo, os fundamentos de hoje ajudam a moldar os de amanhã, para presenciar as tecnologias do futuro mais complexas e problemas mais complexos.

O presente trabalho teve como objetivo apresentar resultados das duas tecnologias (*PfSense* e *Mikrotik*), baseando-se em requisitos/propostas, utilizando conceitos de segurança da informação, *firewall* e alta disponibilidade. Mesmo que venham apresentar similaridade entre as tecnologias de gerência de serviços básicos de redes, sempre existe algum detalhe que é de vital importância no auxílio aos serviços do administrador, visando a segurança da informação.

Através da implementação de um *appliance* de rede, com alta disponibilidade, buscou-se atingir os seguintes objetivos específicos: conceituar segurança de redes, alta disponibilidade e *firewall*; levantar a relação dos serviços, sites e outras informações necessárias sobre a rotina de trabalho para definir o enlace de Internet e o planejamento das regras de acesso à Internet e servidores; levantar características reais para compor os requisitos de configuração dos ambientes de testes; implementar um ambiente de teste para pôr em prática restrições de acesso às informações; realizar testes de funcionalidades, de disponibilidade e de tolerância a falhas do sistema implantado; pesquisar, testar, analisar e apresentar resultados das duas tecnologias.

2 REFERENCIAL TEÓRICO

O presente referencial teórico contém informações que nortearam a pesquisa. Por meio do embasamento da literatura publicada sobre o tema, deu-se início à busca, à análise e à descrição de um corpo de conhecimento e principalmente da prática, em busca de resposta a uma problemática específica, que no caso se refere à um ambiente com alta disponibilidade, utilizando *appliance* de rede.

Os temas, que foram base para a edificação do presente estudo, encontram-se abaixo.

2.1 NECESSIDADE DE UMA INFRAESTRUTURA SEGURA

Na contemporaneidade, onde tudo está conectado a um "mundo virtual", necessita-se de uma infraestrutura segura, tanto nas instalações físicas, serviços e gestões, que dão suporte a todos os recursos de informática compartilhados em ambientes corporativos. Também é fundamental realizar todas as certificações e testes necessários para ter certeza que a segurança está preservada.

O ideal é deixar a estrutura pronta e adequada para estar de acordo com as necessidades e o crescimento da organização. Conectividade, segurança e produtividade precisam de sua devida importância. Os principais benefícios de uma infra em TI compreendem a facilidade de troca de informações por toda organização, redução de instabilidades e eliminação de barreiras de comunicação seja interfuncional ou interpessoal.

2.2 DEFINIÇÃO DE INFORMAÇÃO

A informação é um ativo essencial para os negócios de uma corporação e para quem depende desses dados, seja para processos relacionados a sistemas, redes e pessoais, na qual existe sob diversas formas (impressa, escrita em papel, armazenada eletronicamente e etc), possuindo diversos valores e importância (DALLABONA, 2013). Informação nunca é demais, e quem depende dela, sabe a necessidade para melhor tomar decisões, traçar metas, definir estratégias, comunicar-se, referenciar um fato/fenômeno, adquirir conhecimento ou qualquer outra ação que envolva uma organização (seja pública ou particular) ou uma pessoa em particular. Logo, é necessário haver uma forma que possibilite a segurança das informações. Afinal, ninguém quer perder algo tão importante assim.

2.3 DEFINIÇÃO DE SEGURANÇA DA INFORMAÇÃO

A segurança se traduz efetivamente em minimizar a vulnerabilidade de bens, recursos e sistemas em si, sobre falhas ou fraquezas, que podem ser explorados para se ter acesso a um ou mais dados que a mesma contém, garantindo a continuidade do negócio, a minimização de riscos e a maximização do retorno sobre investimentos e as oportunidades do negócio. Além disso, é uma área do conhecimento que se dedica à proteção dos ativos contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (DALLABONA, 2013)

2.4 OS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A informação necessita de um sistema de gestão de segurança, que preserve a confidencialidade, integridade e disponibilidade da mesma. A integridade é garantir exatidão e completeza da informação e dos métodos de processo, para que a

informação não seja corrompida, falsificada, roubada ou destruída. A disponibilidade é garantir que a informação e os ativos estejam sempre disponíveis, é assegurar o êxito da leitura, do trânsito e do armazenamento da mesma. A confidencialidade é garantir que a informação seja acessível somente por pessoas autorizadas, assegurando o valor da mesma e evitando divulgações indevidas. (TRIBUNAL DE CONTAS DA UNIÃO, 2012)

2.5 *FIREWALL*

Firewall ou, tradução mais próxima, "parede corta-fogo" é uma barreira para evitar a propagação de ações indevidas. É definido como sendo um filtro de tráfego de rede, podendo ser um dispositivo, arranjo ou *software*, que impõe limite de acesso à rede. O *firewall* na maioria das vezes está localizado entre a rede local e a rede externa, mas pode ser necessário o uso do mesmo internamente à rede, com o objetivo de isolar e proteger sub-redes umas das outras. (ALECRIM, 2013)

Uma forma análoga para se entender o que é *firewall* pode ser a apresentada por Tanenbaum (2003, p. 583) que materializa que *firewall*

> [...] 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. Nas redes, é possível usar o mesmo artifício: uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou de entrada da empresa é feito através de uma ponte levadiça eletrônica (*firewall*) [...].

No início dos anos 90, surgiram os primeiros *firewalls* que trabalharam com segurança de redes, que consistiam em pequenos conjuntos de regras bastante efetivos, porém limitados, como, por exemplo: rede A pode fazer acesso à rede B, porém a rede C não pode realizar acessos à rede A e B. A segunda geração *firewalls* trouxe um grande salto evolutivo, que foi à interface de gerencia de regras, além de utilizar filtros, pacotes e aplicativos.

Atualmente existem várias soluções muito mais modernas para *firewalls*. Sendo por exemplo, o *RouterOS* da *Mikrotik* e o *PfSense* soluções de *software firewall.*

2.6 ROTEAMENTO

Roteamento é uma das funções da camada de rede principal, que roteai pacotes de origem para a máquina de destino, ou seja, é o intermediador da comunicação entre dois dispositivos que estejam em redes distintas. (WANDERSON, 2012)

2.7 ALTA DISPONIBILIDADE

Alta disponibilidade é a capacidade de um sistema funcionar sem interrupções por longo período de tempo, sendo o equilíbrio entre as ações de proteção e o custo de inatividade, tendo como suas principais características a disponibilidade, o sistema tolerante a falhas e a redundância. A alta disponibilidade previne prejuízos, uma vez

que o serviço ou sistema funcionará plenamente. (RUIZ, 2000)

A alta disponibilidade está relacionada a provimento de serviços que não podem parar, independente de falhas de energia, equipamentos, conectividade ou outras adversidades, para não causar prejuízos. Um atributo ou uma métrica importante para tais sistemas é a disponibilidade, ao qual atribui um nível de tolerância para indisponibilidades. Essa métrica faz referência a respeito do que a empresa faz para manter o serviço disponível, sendo um cálculo com um grande número de variáveis, que resulta em um número em formato % (percentual), informando a estabilidade no último período de aferição desse sistema.

Utilizar ferramentas/metodologias de gerenciamento para monitorar tais indicadores, é uma prática muito comum. Uma designação muito utilizada, até mesmo em contratos de fornecimento de serviços, é o SLA (*Service Level Agreement* ou Nível de Acordo de Serviço), que abrange tolerância à falhas, performance, prioridade e incidência de erros, e apresenta o % de disponibilidade do sistema. Envolvendo inúmeros aspectos, desde equipamentos até a satisfação do cliente.

2.8 TOLERÂNCIA A FALHAS

Técnica utilizada para descobrir, mascarar e tolerar falhas em sistemas computacionais. A aplicação dessa técnica tende a garantir o bom funcionamento, confiança e disponibilidade do sistema.

2.9 FATORES QUE COMPROMETEM À SEGURANÇA DE UM REDE

Explorar as vulnerabilidades é uma das melhores formas de se encontrar as condições favoráveis para ataques. A segurança absoluta ou perfeita é uma utopia, e os fatores que comprometem a segurança de uma rede variam em relação a suas particularidades, pois cada Instituição/Organização é um caso. No entanto, existem alguns fatores gerais comuns em todos os casos, independente da arquitetura organizacional, que são chamados de: segurança em camada física (dizem respeito à estrutura física, localização, energia elétrica, cabeamento e ativos de *hardware*); segurança em camada lógica (dizem respeito à *firewall*, segregação de redes, registro do usuário, identificação e autenticação do usuário, antivírus, *backup*, serviços de rede, monitoramento); e segurança em camada humana (dizem respeito à segurança dos recursos humanos, documentação de procedimentos, conscientização, educação e treinamento). (DALLABONA, 2013)

2.10 *PFSENSE*

Pfsense é um sistema pré-configurado, também conhecido como *appliance* de rede, que é um sistema operacional *open source* baseado em *FreeBSD* utilizado como *firewall* e roteador. (WANDERSON, 2012)

O projeto *PfSense* foi concebido em meados de setembro de 2004 por Chris Buechler e Scott Ullrich. Chris foi um colaborador assíduo de códigos por muito tempo do projeto m0n0wall. O m0n0wall tem basicamente as mesmas pretensões técnicas do

Pfsense, mas desde o seu surgimento até o fim de seu desenvolvimento, seu foco foi em appliances.

A desvantagem do m0n0wall foi de ser um sistema contido em si e voltado para dispositivos que pudessem rodá-lo diretamente da memória principal. Não é possível instalá-lo em um sistema de arquivos comum em um disco rígido, por exemplo. Daí muitas funções desejáveis para sistemas mais complexos (VPN, suporte a modems 3G, autenticação de usuários, proxy, IDS, etc.) não podem ser razoavelmente implementadas nele.

Diante de tal cenário, Chris Buechler e Scott Ullrich resolveram criar um projeto baseado em todas as funcionalidades existentes no m0n0wall, porém com melhorias na interface web de configuração e uma aproximação com as versões mais recentes do FreeBSD (sistema base). O sistema conquistou usuários por ser extremamente organizado e agregar uma série de funcionalidades com fácil acesso, permitindo à um leigo que tenha conhecimentos básicos de redes, instalar e gerenciar um sistema *PfSense*.

PfSense e suas qualidades: gratuito; pequeno e leve; fácil utilização; estável; seguro; robusto; recursos de filtragem; pacotes diversificados; tráfego dinâmico; cluster; completo.

2.11 *MIKROTIK*

Empresa da Letônia, fundada em 1995, fabricante de equipamentos para redes de computadores, sendo muito utilizados por provedores de banda larga e empresas dos mais variados segmentos, cuja função principal é estabilidade e versatilidade. Com o sistema operacional baseado em Linux, chamado *Mikrotik RouterOS*, concatena diversas funcionalidades de redes em um simples roteador, deixando-o bem poderoso. (WANDERSON, 2012)

O RouterOS é um sistema operacional “carrier class”, licenciado, stand-alone baseado no kernel Linux v2.6, caracterizado pelas inúmeras funcionalidades, robustez, estabilidade e facilidade de uso. O sistema pode ser instalado em PC embarcado (exemplo: Routerboard) ou PC comum.

A *Mikrotik* iniciou a fabricação do seu próprio hardware em 2002, embarcado com seu sistema RouterOS de arquitetura x86 e *Hardwares Appliances Embedded* (módulos Appliance com o sistema embarcado) popularmente chamado de RouterBoard. Incluindo alguns modelos para fibra, além de placas e acessórios diversos. Os vários modelos de hardware conseguem atender à vários tipos de ambientes. Desde um ponto de acesso em um hotel até um roteador de borda em um datacenter.

3 METODOLOGIA

Foi realizado um estudo bibliográfico sobre alta disponibilidade, segurança da informação e rede de computadores, que está sendo utilizado neste trabalho para entendimento e para apresentar propostas de ambientes de rede de computadores. Também foram estudadas tecnologias de sistemas operacionais de rede, denominados

sistemas pré-configurados ou *appliances* de rede.

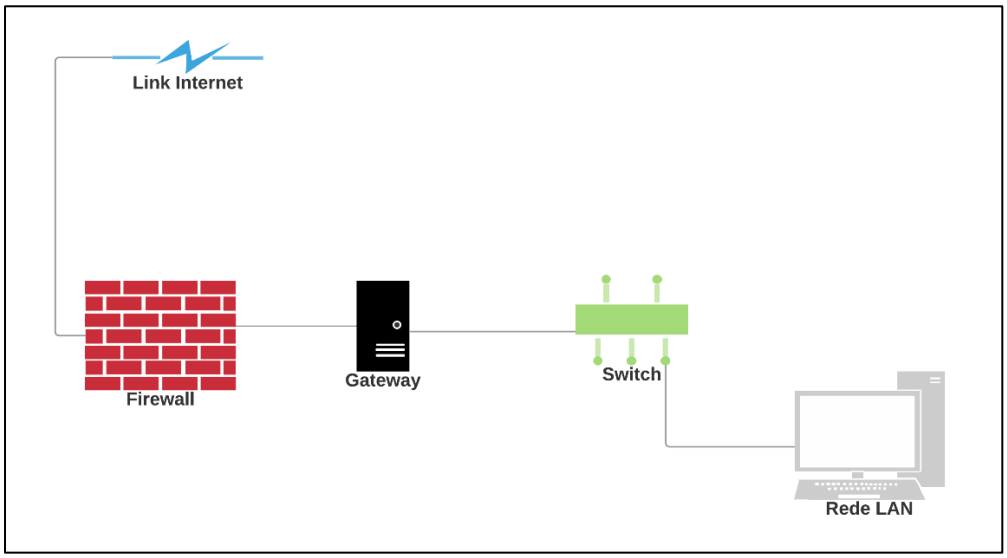
Os estudos que contribuíram com a concretização desta pesquisa foram incorporados em ambos os sistemas de *appliances* de rede: *PfSense* e *Mikrotik*. Contudo foram realizados testes em dois tipos diferentes de infraestrutura de rede: uma rede corporativa (visando fornecer acesso aos funcionários de uma instituição), e um provedor *wi-fi* (fornecendo acesso à Internet para usuários domésticos).

4 DESENVOLVIMENTO E RESULTADOS

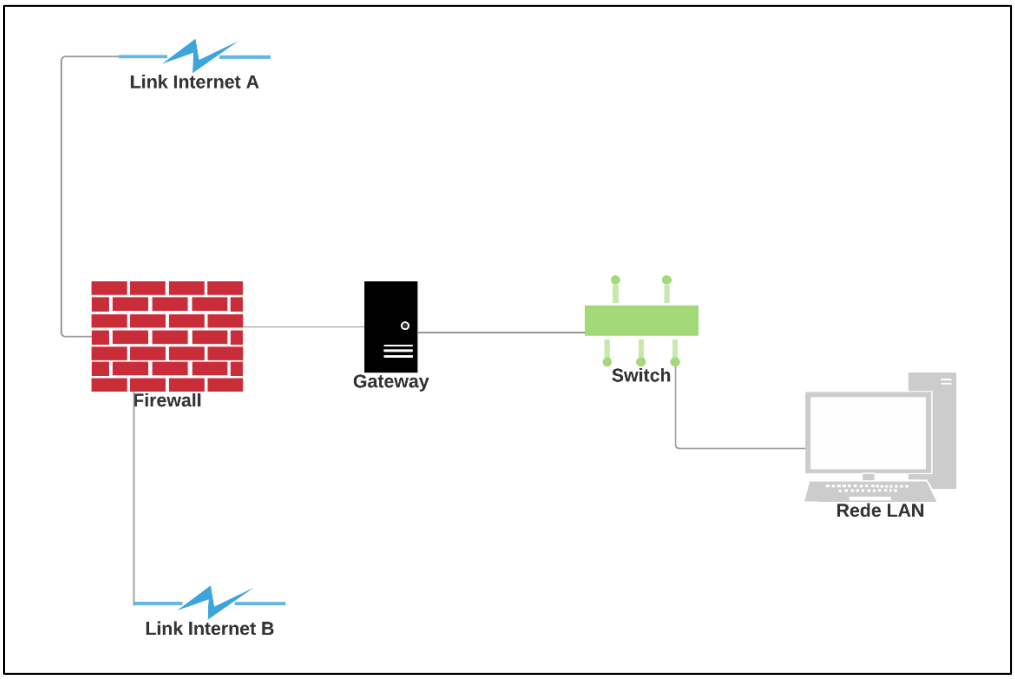
Esta seção tem como objetivo apresentar o desenvolvimento do que foi obtido na metodologia, evidenciando as etapas seguidas pelo autor e os resultados obtidos, a fim de identificar os pontos positivos.

Dentre os fatores importantes deste trabalho, alta disponibilidade, baixo investimento e ROI (*Return On Investimet*) são os principais para sua elaboração.

No presente projeto, as configurações incorporadas nos *appliances*, os modelos de rede bases para os testes e a especificação dos componentes necessários, foram definidos e seguem, respectivamente, abaixo.



Fonte: O autor (2018)



Fonte: O autor (2018)

Os materiais utilizados para compor a topologia de rede foram:

Equipamento	Nome	Descrição	Sistema Operacional	Placas de Rede
PC01	Contabilidade	CPU: AMD Athlon™ XP1600+ RAM: 1GB HD: 40GB	Slackware 14.2 – 32 bits	*3COM 3c905C-TX *Realtek RTL8169
PC02	Diretoria	CPU: RAM: 256MB DIMM HD: 40GB	Slackware 14.2 – 32 bits	*VIA VT6105
PC03	Servidor	CPU: AMD Athlon X2 RAM: 8GB HD: 160GB	Pfsense / Mikrotik RouterOS	
PC04	Servidor	CPU: AMD Athlon™ XP1600+ RAM: 1GB HD: 160GB	Pfsense / Mikrotik RouterOS	*VIA VT6105 *D-LINK DGE-530T
PC05	Vendas	CPU: AMD Athlon™ XP1600+ RAM: 1GB HD: 40GB	Slackware 14.2 – 32 bits	*VIA VT6105 *D-LINK DGE-530T *3COM 3c905C-TX *INTEL CORPORATION 82557/8/9/01 ETHERNET PRO 100
PC06	Estoque	CPU: AMD Athlon™ XP1600+ RAM: 1GB HD: 20GB	Slackware 14.2 – 32 bits	*VIA VT6105 *3COM 3c920B-EMB *NVIDIA GEFORCE ETHERNET
SWITCH	Switch	HP JE009A V1910-48G, 48 portas 1Gbit 4 X SFP	-	-

Fonte: O autor (2018)

As configurações e os serviços incorporados nos *appliances* abrange os seguintes itens:

- Identificar e atribuir interfaces WAN, LAN e DMZ;
- SSH;
- DNS;
- NTP;
- SNMP;
- Aliases;
- Dashboard personalizado;
- Regras IPTABLES;
- Agendamento;
- VPN;
- VIPS;
- Gateway;
- Captive Portal;
- NAT;
- Port Fowarding;
- Controle de MAC por IP;
- Controle de banda (Loadbalance, tratar portas e limitar conexões por clientes);
- Proxy e Squid;
- Disponibilidade de nodo (heartbeat e VRRP);
- Monitoramento e registro em tempo real.

As instalações dos sistemas operacionais de rede utilizados foram da seguinte forma:

- Sistema Operacional de Rede 1 - PfSense: imagem obtida no site https://www.pfsense.org.br/, na seção de downloads, sendo possível escolher a versão para a instalação, com arquitetura a i386 (32 bit) ou amd64 (64 bit) ou netgate ADI, e para instalação em *pendrive* ou *live* CD. Depois de gravada a imagem, o CD funciona como um *live* CD, ou seja, todo o sistema *PfSense* já está previamente carregado e pronto para uso ao se iniciar o servidor a partir do CD ROM. Logo, pode-se seguir os passos da instalação. A versão do *PfSense* instalada foi a 2.4.3. Após a instalação exibe-se a tela padrão do sistema com algumas informações iniciais e com seu menu.
- Sistema Operacional de Rede 2 – Mikrotik RouterOS: imagem obtida no site https://mikrotik.com/, na seção de software, sendo possível escolher a versão para a instalação, com diversas opções de arquitetura para a instalação em diversos dispositivos compatíveis e/ou homologados. Depois de gravada a imagem, o CD funciona como um *live* CD, ou seja, todo o sistema *Mikrotik RouterOS* já está previamente carregado e pronto para uso ao se iniciar o servidor a partir do CD ROM. Logo pode-se seguir os passos da instalação. A versão do *RouterOS* instalada foi a 6.43.2. Após a instalação exibe-se a tela padrão do sistema com algumas informações iniciais e com seu menu.

Os testes aplicados após as configurações nos servidores, com foco na conexão ou acesso a rede e os downloads, foram:

1º: servidor mestre e o servidor escravo, ambos ligados;

2º: servidor mestre é desligado e o servidor escravo assume a rede;

3º: servidor mestre é religado e reassume a rede e o servidor escravo continua ligado;

Para a realização dos testes foram aplicados os seguintes processos:

- Testar as configurações de IP com comando de rede PING;

- Verificar conectividade com a internet;
- Testar DNS;
- Verificar velocidade de conexão com os hosts e server;
- Testar o funcionamento do SSH acessando os hosts da rede via protocolo SSH;
- Forçar situações negativas sobre a rede (indisponibilidade de algum serviço da rede, como um exemplo);
- Gerar stress na rede, analisar os pacotes e coletar os dados (utilizando softwares, como por exemplo o *iperf*);
- Testar a rede com os protocolos RSTP, STP e MSTP;

Analisando as características de cada um dos sistemas estudados, foi possível identificar os benefícios de cada *appliance* de rede nos ambientes testados. Considerando que os testes foram realizados no Laboratório de Redes e Sistemas do UNIPAM – LRSU, localizado no 2º piso do bloco G, sala 209, do Centro Universitário de Patos de Minas – FEPAM/UNIPAM. Cujo laboratório deu total apoio e disponibilizou todos os equipamentos necessários, para que fosse possível implementar as infraestruturas de rede do projeto.

Inicialmente as duas redes, tanto a pública quanto a corporativa, utilizavam como sistema de gerência dos recursos das redes, o *RouterOS*.

Na rede de acesso corporativa o *link* foi ficando saturado, o que atrapalhou a acessar os sites e *e-mails*, realizar downloads e assistir *streaming*. O *PfSense* foi então implementado e através das análises comparativas, foi observado um melhor aproveitamento do *link* com o novo sistema, na gestão da rede. Não foi utilizado um controle de banda efetivo nesse modelo de rede. Porém, com o controle de conteúdo (como por exemplo: bloqueio de conteúdos de download; bloqueio de sites), resolveu-se à deficiência do tráfego da rede corporativa, com redução do *Throughput* (taxa de transmissão) do *link* de internet. Para tal resultado, foi utilizado o módulo *SquidGuard*, para filtrar conteúdos pesados, e o módulo *Squid-Proxy*, para armazenar conteúdos já acessados pelos usuários na rede.

Na rede de acesso público, aconteceu o contrário. Baseando-se nas implementações e nos testes realizados na rede anterior, o *PfSense* não foi capaz de realizar o controle de banda de usuário individual, de forma eficaz e necessária ao modelo de rede. Neste caso, o controle de banda é considerado o ponto chave, por se tratar de venda de serviço preestabelecido, na qual o usuário adquire tal serviço e paga o valor baseado na velocidade contratada. Foi então implementado o *RouterOS*, que proporcionou um controle de qualidade e precisão, entre todas as conexões ativas no *link* de Internet.

Ficou claro que na rede corporativa não era necessário um controle de banda efetivo, mas sim, de um controle efetivo de todo o conteúdo que era acessado. Isso pelo fato de que funcionários passam boa parte do tempo acessando sites de downloads, sites de entretenimento, redes sociais, sites de *streaming*, e etc. Fazendo com que o *throughput* do *link* fique saturado e atrapalhe os funcionários que realmente precisa acessar informações relevantes e necessárias para executar os seus serviços. Já na rede pública, fica claro o contrário, há necessidade de um controle de banda efetivo por usuário. Porém pode-se manter o *RouterOS* como sistema principal deste modelo de rede, e acrescentar um servidor *PfSense* paralelo, para gerenciar o

cache efetivo, através do serviço de *proxy-cache*, dando apoio ao *link* de Internet, evitando que requisições fossem buscadas sempre direto na internet. Aumentando assim a sensação de velocidade para o usuário final e evitando possíveis saturações do *link*. Mas esse acréscimo de servidor não foi realizado neste trabalho, é uma futura implementação, um próximo passo para abranger a pesquisa nos temas estudados.

5 CONCLUSÃO

O desenvolvimento do presente trabalho possibilitou o estudo de um conjunto de ferramentas e suas integrações, para implementação de sistemas em alta disponibilidade, com certa facilidade. Além de colocar em prática aprendizados adquiridos durante o curso em diversas matérias, como: linguagem e comunicação; organização e arquitetura de computadores; engenharia de software II; redes de computadores e telecomunicações I e II; análises de sistemas; auditoria e segurança de sistemas; tópicos especiais II; dentre outros.

A crescente procura por soluções em alta disponibilidade, está se tornando cada vez mais comum no mercado, devido ao crescimento de sites de e-commerce, de sites de relacionamento, da quantidade de acessos à serviços da internet, de sistemas ERP, de bancos de dados que trabalham em regime de missão-crítica, e dentre outros. Exigindo assim, sistemas onde a conectividade não pare, não fique indisponível, não apresente perde de desempenho e que garanta a segurança dos dados.

Nenhum modelo de segurança pode: resolver todos os problemas; cuidar dos problemas de gerenciamento; prevê proteção perfeita e não pode prevenir todos os incidentes. Mas pode impedir às ameaças advindas tanto de pessoas de fora da Instituição/Organização, quanto às pessoas internas, se tornem incidentes que danifiquem seriamente o ambiente de trabalho, deixe fora de operação determinado sistema ou que cause danos à imagem da Instituição/Organização. Transformando as invasões em momentos raros, breves e com baixo ônus, porém não se pode evitá-las completamente.

Tornam-se necessárias, ações para descobrir os pontos vulneráveis e a partir de aí avaliar os riscos e impactos e providenciar soluções para prevenção de forma eficaz. Porém muitas das vezes o preço é alto para prevenir e as empresas não dão o devido valor a esta questão. Portanto, o melhor a se fazer é reduzir ao máximo quaisquer riscos às informações, mantendo a integridade e a disponibilidade dos sistemas. Sendo importante implementar uma análise de riscos, a definição da Política de Segurança e um plano de contingência.

Dada à importância do assunto, a escolha de um sistema depende muito do modelo, dos requisitos e da infraestrutura da rede a ser gerenciada. Ambos sistemas possuem suas peculiaridades, variando de acordo com a implementação realizada. O *PfSense* mostrou melhor desempenho no gerenciamento da rede corporativa. Já o *Mikrotik RouterOS* mostrou-se melhor desempenho gerenciando a rede pública. Porém é possível afirmar que o *PfSense* pode muito bem complementar o *RouterOS*, e vice-versa.

Com isso, o artigo encontra-se adequadamente direcionado com o âmbito de receber melhorias, continuar crescendo ao longo do tempo e abranger ainda mais a

pesquisa. Nesse sentido, é necessário a implementação do *PfSense* complementando o *RouterOS* e vice-versa, que não foram realizados neste trabalho.

REFERÊNCIAS

ADATO, Leon, 2015. **A evolução da infraestrutura de rede** – Parte 01. Disponível em: <https://imasters.com.br/tecnologia/redes-e-servidores/a-evolucao-da-infrarede-parte-01/>. Acesso em: 23/fev./2017.

ALECRIM, Emerson, 2013. **O que é firewall?** – Conceito, tipos e arquiteturas. Disponível em: <https://www.infowester.com/firewall.php>. Acesso: 05/mar/2017.

DALLABONA, Nilson Sergio, 2013. **SEGURANÇA DA INFORMAÇÃO:** Uma proposta para projeto de rede baseada em software livre. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2416/1/CT_GESER_IV_2014_07.pdf>. Acesso: 24/fev./2017.

RUIZ, A. **Alta Disponibilidade em Servidores Linux.** Revista do Linux, v. 6, fev. 2000. Disponível em: <http://labbi.uesc.br/apostilas/revista_do_linux/006/alta.html>. Acesso em: 24/fev./2017.

SANTAYANA, George. **Life of Reason.** Vol. 1, 1905.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Amsterdam: Campus, 2003.

TRIBUNAL DE CONTAS DA UNIÃO, Brasil, 2012. **Boas práticas em segurança da informação / Tribunal de Contas da União.** 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação. Disponível em: <http://www4.planalto.gov.br/cgd//assuntos/publicacoes/2511466.pdf>. Acesso: 05/mar/2017.

WANDERSON, 2012. **Estudo comparativo entre o PfSense e o RouterOS em dois modelos de rede.** Disponível em: <http://tecnologoderedes.blogspot.com.br/2012/06/artigo-tcc-estudo-comparativo-entre-o.html>. Acesso em: 23/fev./2017.