Revista Perquir*ere*. Patos de Minas, 14(2):124-134, maio/ago. 2017

Implementação de uma infraestrutura de rede abordando *vlans* e utilizando *pfsense* como *firewall* e roteador

Implementation of a net infrastructure, by approaching vlans *and using* pfsense *as firewall and edger router*

Paulo Jacinto Rosa Severino
Graduando do curso de Sistemas de Informação (UNIPAM). e-mail: paulojrs.ti@gmail.com

Fabrício Geraldo Araújo
Professor orientador (UNIPAM). e-mail: fabaraujo23@gmail.com

Resumo: Este artigo é resultado do projeto de implementação de uma infraestrutura de rede numa empresa de contabilidade e consultoria para o agronegócio. O projeto consiste na análise de necessidades da empresa diante da sua política de segurança da informação, implementando uma infraestrutura de rede utilizando como base principal o *firewall pfsense* como roteador de borda, complementando com o recurso de alta disponibilidade, garantindo que o negócio da empresa não venha a ter falhas e indisponibilidade durante o horário de expediente, e visando sempre o mínimo de intermitências no âmbito do trabalho. Esse projeto pode ser aplicado a não somente a esse ramo de atividade, mas em qualquer ambiente onde o parque tecnológico de máquinas tenha um número considerável de estações onde as mesmas necessitem de um gerenciamento.
Palavras-chave: Infraestrutura. Redes. Segurança. Alta disponibilidade.

Abstract: This article is the result of the project of implementation of a network infrastructure in an agribusiness accounting and consulting firm. The project consists of analyzing the needs of the company in the face of its information security policy, implementing a network infrastructure based on the *pfsense* firewall as the edge router, complementing with the high availability feature, ensuring that the company's business does not come to have failures, unavailability during office hours, always aiming at the minimum of intermittency in the scope of work. This project can be applied not only to this branch of activity, but also in any environment where the technological machinery park has a considerable number of stations where they need management.
Keywords: Infrastructure. Networks. Security. High Availability.

---

1. Introdução

As empresas já não utilizam os serviços de TI apenas como suporte de sua estrutura técnica e até mesmo organizacional. Há um crescimento de tendência com o passar dos anos nas empresas que trocam o papel tático de TI por um estratégico para a gestão de negócios e melhoria no apoio a tomada de decisões.

A infraestrutura de TI existe para dar assistência ao negócio, é o alicerce da empresa, e não a própria empresa. Vemos muitos profissionais implantando soluções em suas empresas sem o mínimo impacto de melhoria para o negócio, estão apenas visando a inovação de tecnologia, mas é importante ressaltar que inovação sem aproveitamento não favorecerá a empresa. O departamento de infraestrutura de TI apenas crescerá se a empresa crescer, e por isso, temos que trabalhar a favor do "lucro" da empresa (INFOTECH, 2011).

A infraestrutura de TI está para disponibilizar serviços e/ou recursos, manter serviços existentes, disponíveis para quem os usa, e por último, solucionar problemas dos serviços que auxiliam nos recursos utilizados pelo cliente, seja ele interno ou externo.

Nesse contexto, a proposta deste trabalho foi implementar uma infraestrutura de rede numa empresa de contabilidade e consultoria para o agronegócio, bem como compreender e explicar o funcionando do *firewall*, um *pfsense* como roteador de borda. A infraestrutura de rede que foi implementada pode ser utilizada em qualquer empresa que possui um parque tecnológico de máquinas considerável para a gestão do seu negócio.

Infraestrutura de rede consiste na disposição do cabeamento que suporta qualquer equipamento relacionado à comunicação de dados/voz. Todos os sistemas finais que possuem algum meio de transporte de informação que conduzam informação através de algum meio físico é considerado infraestrutura de rede (PINHEIRO, 2010).

O objetivo geral deste trabalho foi implementar uma infraestrutura de rede completa, desde a análise do atual cenário da empresa em que esta foi implementada, explicar e entender o funcionando do *pfsense* como *firewall* e roteador de borda, num ambiente onde possa ser aplicado o recurso da alta disponibilidade.

Para tanto, ficaram definidos outros objetivos específicos, que têm como finalidade relacionar várias ferramentas utilizadas pela TI, caracterizando toda a infraestrutura da empresa, entre os quais podemos citar:

- Instalar o servidor de autenticação espelhado fisicamente (redundância);
- Instalar o servidor de arquivos com redundância física, configuração de permissão dos usuários a diretórios mapeados pela rede;
- Implantar o *firewall pfsense* como roteador de borda;
- Fazer a estrutura de *backup* interna e externa;
- Entender o funcionamento e implementação de *vlans* para segmentação de departamentos e de *broadcast*;
- Entender o funcionamento e demonstração de roteamento utilizando *pfsense*;
- Fazer a documentação de toda a infraestrutura de rede e seus respectivos diagramas;
- Ter alta disponibilidade de autenticação, *firewall*, arquivos.

Desta forma, este estudo pretendeu promover a integração de diversas ferramentas que possam ser implementadas em qualquer empresa que necessite de uma TI para contribuir com o seu desenvolvimento e crescimento no mercado. Além disso, o projeto teve como foco final também mostrar para as empresas o quanto é importante o investimento em TI, mostrando seus benefícios, vantagens, e qual será o retorno que a mesma terá depois de um tempo, agregando valor ao seu negócio.

O processo de implementação de uma infraestrutura de rede numa empresa é de suma importância para uma melhor gestão dos ativos de *hardware* e *software*, pois uma infraestrutura bem montada, organizada, passa mais segurança, confiabilidade, integridade, tanto para usuários internos, quanto para externos que utilizam os serviços da empresa que passam pela área de TI.

Nesse contexto, a adoção de medidas para essa implementação pode solucionar, por exemplo, problemas relacionados à perda de arquivos, à disponibilidade e integridade de informações em servidores, à segurança de rede no que se diz respeito a conexões de entrada e saída na empresa e à facilidade de comunicação entre matriz e filiais através de um túnel privado de informações trocadas pelas mesmas.

Dessa forma, é possível obter uma análise precisa e detalhada de todos os requisitos, e nesse sentido, um mapeamento individual de cada setor da empresa e de sua relação com a TI, bem como o estágio atual da mesma podem auxiliar para uma implementação concisa e segura de uma infraestrutura de rede completa.

2. Referencial teórico

Nesta seção são apresentados os conceitos referentes ao processo de desenvolvimento do trabalho.

2.1. Infraestrutura de rede

Infraestrutura de rede consiste na disposição do cabeamento que suporta qualquer equipamento relacionado à comunicação de dados/voz. Todos os sistemas finais que possuem algum meio de transporte de informação que conduzam informação através de algum meio físico é considerado infraestrutura de rede (PINHEIRO, 2010). Refere-se aos recursos de *hardware* e *software* de toda uma rede que permitem a conectividade de rede, comunicação, operações e gestão de uma rede corporativa. Infraestrutura de rede fornece o caminho e os serviços de comunicação entre os usuários, processos, aplicações, serviços e rede externa, a *internet*.

Uma infraestrutura de rede, geralmente, é parte da infraestrutura de TI encontrada na maioria dos ambientes de TI corporativos. A infraestrutura de rede inteira está interligada, e pode ser usada para comunicações internas, externas ou ambos os casos. Uma estrutura típica de rede é dividida entre *hardware* de rede, *softwares* e protocolos de rede e serviços de rede.

O *hardware* de rede pode ser compreendido por roteadores, comutadores ou *switches*, placas de redes, pontos de acesso sem fio, cabos de par trançados. Já na parte lógica, os softwares de redes geralmente são compreendidos por operações e gerenciamento de rede, sistemas operacionais, *firewall*, aplicativos de segurança de rede. Por último, os serviços de rede que são oferecidos por terceiros, como DSL, links dedicados ponto a ponto entre o provedor de serviços e o cliente final, protocolos de comunicação, endereçamento IP.

2.1. Segurança da informação

Segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações assegurando integridade, disponibilidade, não repúdio, autenticidade e confidencialidade. Esses elementos constituem os cinco pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiabilidade em sistemas de informações (SILVA FILHO, 2004).

Nesse sentido, esses pilares, juntamente com mecanismos de proteção, têm por objetivo prover suporte a restauração de sistemas de informações, adicionando-lhes capacidades, detecção, reação e proteção. O estabelecimento de um programa de segurança da informação em sua empresa deve passar sempre por ações que norteiem esses princípios. Tal modelo deve estar amparado por um sistema de gestão de segurança da informação que precisa ser planejado e organizado, implementado, mantido e monitorado (MAIA, 2013).

2.2. *Pfsense*

PfSense é um sistema operacional de código aberto baseado em *Unix FreeBSD*, adaptado para ser usado como um firewall e/ou roteador. Ele teve o seu lançamento em 2004 e hoje a sua versão mais atual é a 3.2. É um projeto popular colaborativo com mais de 1 milhão de downloads desde seu início, possuindo uma grande comunidade que apoia o projeto, fazendo implementações e melhoria no seu código fonte.

O *pfsense* pode ser instalado em pequenas redes domésticas para proteger um único computador ou em grandes empresas, universidades, dentre outras organizações, protegendo e administrando milhares de dispositivos de rede.

Hoje o *pfsense* pode ser considerado um serviço UTM, *Unified Threat Management*, ou Central Unificada de Gerenciamento de Ameaças, apesar de não ser muito popularizado na forma *appliance* (*hardware* + *software*). Porém, seus serviços são abrangentes no quesito segurança de redes, sendo uma evolução do firewall tradicional, pois une a execução de vários serviços tais como VPN, balanceamento de carga, regras de NAT, regras de firewall, geração de chaves RSA, monitoramento de tráfego, etc. (ANDRADE, 2013).

2.3. Alta disponibilidade

Segundo Heidi (2016), em computação, a disponibilidade é um termo usado para descrever o período de tempo quando um serviço está disponível, assim como o tempo requerido por um sistema para responder a um pedido feito por um utilizador. Alta disponibilidade é uma qualidade de um sistema ou componente que assegura um elevado nível de desempenho operacional durante um determinado período de tempo.

A disponibilidade é muitas vezes expressa como uma porcentagem que indica a quantidade de tempo de funcionamento que é esperada a partir de um sistema ou componente específico num determinado período de tempo, em que um valor de 100% indica que o sistema nunca falha. Por exemplo, um sistema que garanta 99% de disponibilidade no período de um ano pode ter até 3,65 dias de tempo de inatividade (1%).

Esses valores são calculados com base em vários fatores, incluindo ambos os períodos de manutenção programadas e não programadas, bem como o tempo para se recuperar a partir de uma possível falha do sistema. Funções de alta disponibilidade como um mecanismo de resposta de falha de infraestrutura conceitualmente é bastante simples, mas normalmente requer algum software ou configuração previamente feita para tal efeito.

2.4. *Vlan*

Uma *vlan* é uma rede local que agrupa um conjunto de máquinas de maneira lógica e não física propriamente dita, utilizando equipamentos de rede como cabos, switches, entre outros (PILLOU, 2016).

Com efeito, numa rede local a comunicação entre as diferentes máquinas é governada pela arquitetura física. Graças às *vlans* é possível livrar-se das limitações da arquitetura física (constrangimentos geográficos, restrições de endereçamento, etc.), definindo uma segmentação lógica (*software*) baseada num agrupamento de máquinas usando endereços MAC, números de porta, protocolos, etc.

3. Metodologia

O presente trabalho teve como base a implementação de uma infraestrutura de rede numa empresa de contabilidade e consultoria para o agronegócio. A metodologia de desenvolvimento utilizada na construção do projeto pode ser aplicada a qualquer empresa que necessite de uma infraestrutura de rede.

Para o desenvolvimento foram utilizadas as seguintes ferramentas:

- *Hyper V*: provê a infraestrutura de software e as ferramentas de gerenciamento básico que você pode utilizar para criar e gerenciar um ambiente de virtualização de servidores.
- *Debian*: distribuição *Linux* geralmente voltada para a implantação de servidores.
- *Crashplan*: *software* de *backup* pessoal e para empresas em que o principal foco é o versionamento em nuvem.
- *Diaw*: criação dos diagramas da infraestrutura de rede.
- *Windows Server 2012*: Sistema operacional da Microsoft, com soluções para infraestrutura e virtualização.
- *Samba4*: pacote de software *Linux* que nos possibilita ter um controlador de domínio e um servidor de arquivos completo.
- *PfSense*: sistema operacional de código aberto baseado em *Unix FreeBSD* adaptado para ser usado como um firewall e/ou roteador

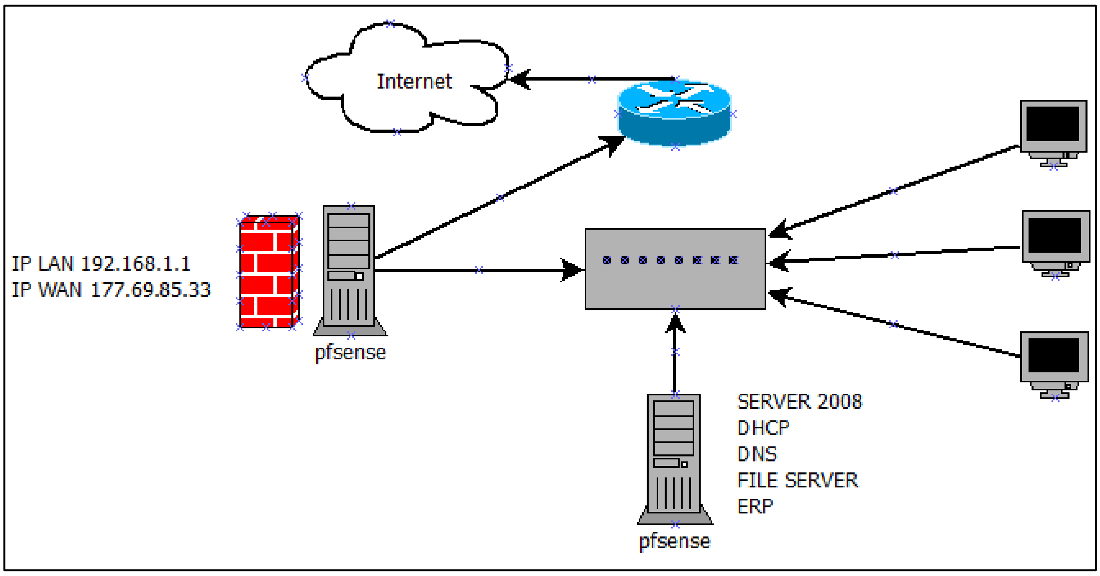
Como suporte para levantamento das informações perante a empresa para o desenvolvimento do projeto, foi utilizada a coleta de informações via e-mail, atendimentos realizados pela TI no período do primeiro trimestre de 2016, e reuniões com a diretoria e a TI para se ter conhecimento dos problemas atuais e principalmente das necessidades que a empresa tinha com relação a segurança, disponibilidade e integridade de suas informações.

4. Desenvolvimento e resultados

Num primeiro momento foi necessária a realização de mapeamento de toda a atual infraestrutura de rede da empresa, através de diagramas e análise de como os processos vinham sendo utilizados pela equipe e pelos colaboradores da empresa.

Os procedimentos iniciais se basearam em inicialmente fazer um diagrama do estado atual da rede da matriz, como se pode ver na Figura 1, precedendo de um levantamento de requisitos do que necessariamente é composta a infraestrutura de TI da empresa atualmente.

Figura 1. Diagrama de rede da matriz



Fonte: Dados do trabalho, 2016.

No cenário em que a empresa se encontrava, percebeu-se a necessidade de melhoria em diversos serviços, principalmente no que diz respeito ao gerenciamento de recursos que reduzem a inoperabilidade de servidores, sistemas e demais serviços oferecidos pela empresa aos seus clientes.

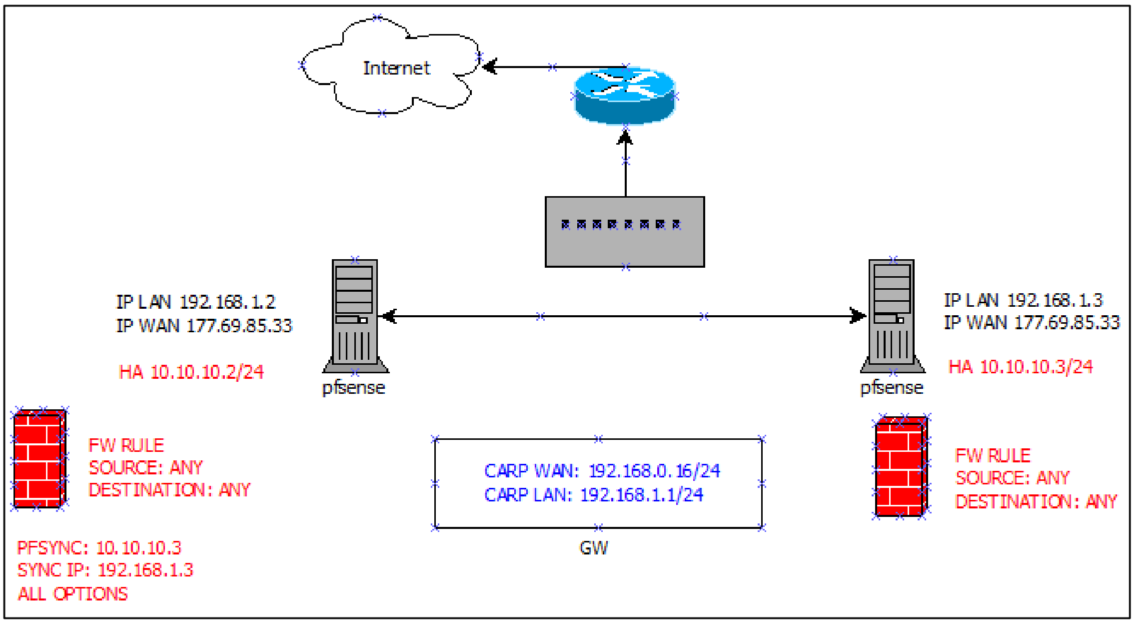
Visto que a empresa tem em sua carta de clientes 92% deles fora da cidade de

Patos de Minas, a mesma utiliza-se de recursos de conexão remota para que os colaboradores possam acessar o servidor dos clientes em questão para o recolhimento de informações, documentos, análise de dados e balancetes contábeis. Foi identificado um certo risco em que a mesma se encontrava por não contar com alta disponibilidade em seus recursos de rede.

A primeira questão abordada para a implementação foi a implantação do *firewall Pfsense:* em reunião com a equipe de TI, entendeu-se que esta era uma solução bem recomendada no mercado, sendo reconhecida no mesmo patamar de soluções comerciais como o *Sonic Wall* da *Dell*, *Fortigate* da *Fortinet*, entre outras soluções de segurança. Além disso, não geraria custos com licença de *software*, sendo o UTM uma *open source*, além de possuir uma comunidade amplamente colaborativa no desenvolvimento de seu código fonte.

O *Pfsense* é uma ferramenta robusta, pois une a execução de vários serviços tais como VPN, balanceamento de carga, regras de NAT, regras de firewall, monitoramento de tráfego suspeito, bloqueio de conteúdo impróprio, essas que seriam imposições da empresa para se adequar à política de segurança da informação desenvolvida pela mesma. Pode-se observar, na Figura 2, o diagrama da implementação do *firewall* mostrando o recurso de alta disponibilidade, caso o mesmo venha a ocasionar alguma falha.

Figura 2. Diagrama de HA do firewall Pfsense



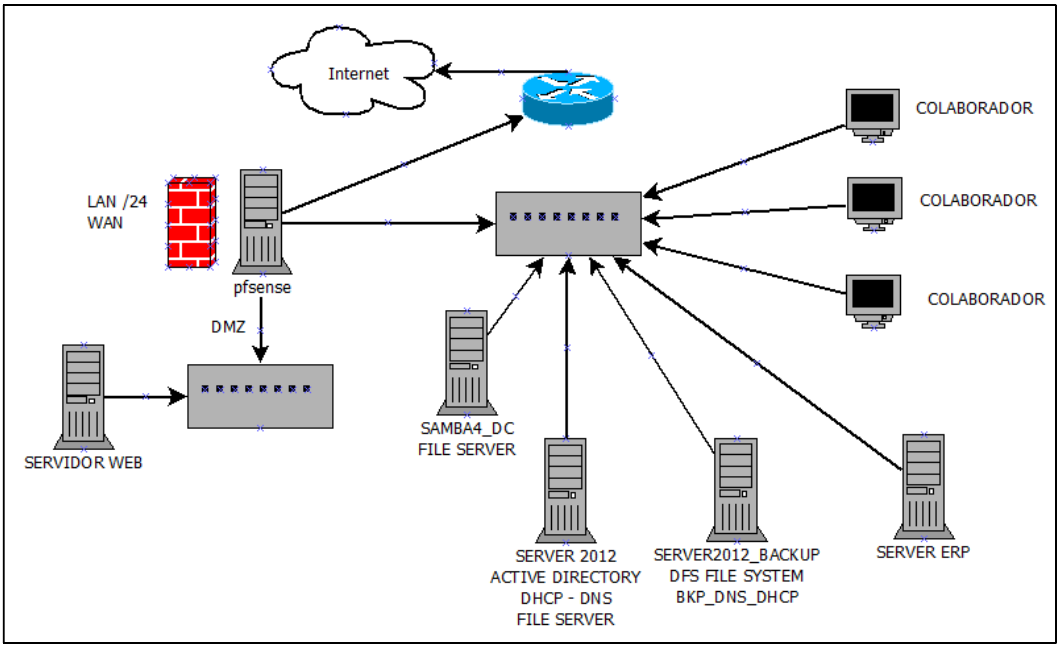
Fonte: Dados do trabalho, 2016.

Outro ponto a ser observar bem foi uma melhor análise do tráfego de rede através dos pacotes que o *Pfsense* oferece, utilizando o *squid* e o *squidguard*. Isso possibilitou que relatórios de conteúdo acessado fossem analisados pela coordenação da empresa e que fossem repassados para a TI os ajustes necessários para filtros de bloqueio por grupo de usuários, melhorando assim a navegação da internet em que conteúdo com gasto excessivo de banda sem utilidade foi bloqueado.

Ao utilizar o pacote *snort*, que é uma aplicação que pode ser instalada em conjunto com o *firewall*, tendo a função de fazer detecção de intrusões na rede, foi possível fazer a análise de tráfego em tempo real e o registro de pacotes. Foi observado que muitos pacotes estavam sendo enviados para as portas UDP 3389 e 3489, respectivamente serviços de RDP *Terminal Server* e servidor STUN utilizado no PABX da empresa. Ao fazer esses bloqueios, percebeu-se uma melhora relatada pelos usuários na performance do VOIP nas chamadas entre as unidades da empresa.

Um dos problemas que a empresa tinha era a alta dependência de somente um servidor Windows Server 2008, fazendo funções mais do que sua capacidade podia suportar, além de estar sendo usado por diversas funções, tornando-o sobrecarregado. Para sanar esse problema, foram separadas as funções de cada servidor em específico, fazendo-se a distribuição correta, ficando cada serviço necessário em seu respectivo servidor, como se pode observar na Figura 3.

Figura 3. Diagrama de rede da matriz



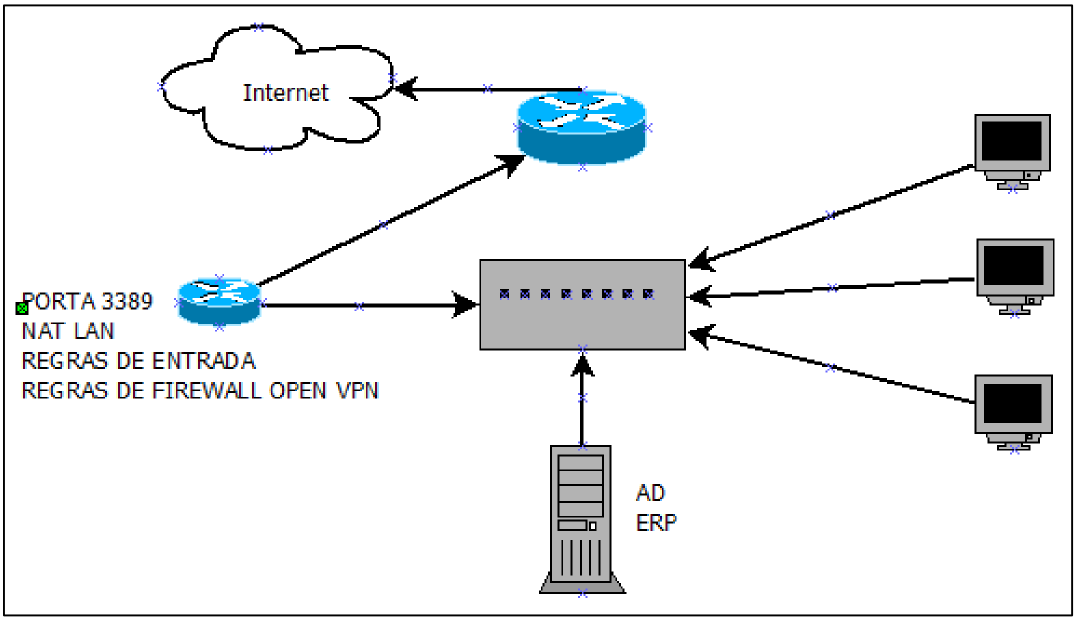
Fonte: Dados do trabalho, 2016.

Antes da implantação do *firewall pfsense*, o acesso era feito totalmente liberado, utilizando-se o protocolo RDP via conexão de área de trabalho remota rodando sobre a porta 3389, onde a mesma não possuía nenhuma regra de entrada, ocasionando problemas pelo vírus *ransomware,* que foi um problema encontrado durante a implementação deste projeto.

Ransomware é um tipo de *malware* que restringe o acesso ao sistema e até mesmo ao computador infectado, e cobra um valor de "resgate" para que o acesso seja reestabelecido. O *ransomware* visto durante o projeto foi do tipo *Cryptolocker*, que compacta os arquivos no computador da vítima em um pacote criptografado em 256 bits.

A resolução deste problema foi através da criação de um túnel VPN entre o cliente externo e o servidor de autenticação, juntamente com o servidor de ERP da empresa que oferece *software* como *SAAS* para os mesmos. Pode-se observar na Figura 4 o diagrama de como agora é feito o acesso do cliente externo.

Figura 4. Diagrama de conexão do cliente externo



Fonte: Dados do trabalho, 2016.

Além dos diagramas e implantações que foram feitas, como se pode observar, para uma melhor gestão do negócio da empresa, juntamente com a TI, diversas melhorias e implementações foram feitas visando a disponibilidade dos serviços, a integridade e a segurança das informações:

- Servidor de autenticação espelhado fisicamente (redundância);
- Servidor de arquivos com redundância física, configuração de permissão dos usuários à diretórios mapeados pela rede;
- Implantação do *firewall pfsense* como roteador de borda;
- Estrutura de *backup* interna e externa com versionamento de arquivos em nuvem;
- Separação de departamentos utilizando *vlans* para segmentação de *broadcast*, diminuindo tráfego desnecessário de rede isolando a comunicação com outros setores;

- Documentação de toda a infraestrutura de rede e seus respectivos diagramas, através de documentos de instruções e manuais;
- Alta disponibilidade do servidor de autenticação *Active Directory*;
- Implantação do servidor DHCP e DNS;
- Servidor *Debian* com o pacote do Samba 4 fazendo a função de Controlador de Domínio;
- Replicação de arquivos utilizando DFS;
- Bloqueio de sites utilizando o *squid* e *squidguard* gerando relatórios de acesso, tráfego de internet gasto pelos usuários;
- VPN Cliente Servidor para o acesso dos clientes externos, VPN *Site to Site* para acesso dos clientes internos.

5. Conclusão

O trabalho realizado possibilitou a justificativa da implementação da infraestrutura de rede da empresa. O desenvolvimento deste projeto propiciará à TI um autoconhecimento do que é realizado, uma melhor gestão e organização de toda a infraestrutura de rede referente à estrutura de recursos e também aos processos utilizados.

A principal dificuldade encontrada durante o desenvolvimento do projeto foi a falta de dados e informações em relação aos processos que eram efetuados pelo setor de TI. A falta dessas informações durante o projeto teve grande impacto nos resultados obtidos, pois gerou a necessidade de ter toda a documentação do que foi desenvolvido e de todos os processos realizados pela TI, como forma de continuidade dos serviços, não ficando sob dependência de nenhum colaborador o conhecimento sobre determinada ferramenta ou serviço prestado.

Como trabalho futuro, será feita a implantação do Gerenciamento de Incidentes e de Problemas, juntamente com um sistema de Help Desk e monitoramento, abrangendo uma base de dados de erros conhecidos, para um melhor atendimento da equipe de suporte perante os clientes externos e internos. Espera-se a implantação gradativa desses serviços, após análise e feedback da aplicação dos processos iniciais e dos demais processos, com o intuito da melhoria gradativa e contínua dos serviços prestados pela equipe de TI da empresa.

Existem estudos que mostram que, se uma empresa hoje investe em TI, ela leva mais ou menos 5 anos para ter o retorno sobre esse investimento. Com esse projeto, demonstramos exatamente esse retorno e o quanto é importante as empresas focarem nesse investimento.

O fato é que os gestores com poder de decisão sobre investimentos em TI precisam saber o que a empresa ganha como retorno do capital investido em um projeto. As decisões precisam estar baseadas em números e benefícios tangíveis, que possam ser mensurados. Medidas quantificáveis e métricas é que vão esclarecer se a iniciativa é significativa para a melhoria da empresa. O ROI tem, portanto, o papel de provar às partes interessadas, sejam diretores técnicos, sejam gestores executivos, que fazer um determinado investimento em um projeto de TI pode trazer benefícios para o seu negócio.

Após a implantação da infraestrutura em todo ambiente de produção, espera-se que a alta disponibilidade dos serviços contribua para a mínima interrupção possível do negócio da empresa. Com um ambiente de tecnologia dinâmico e gerenciado, você reduz o custo operacional, mantém sua empresa funcionando, sua equipe se comunicando e consequentemente diminui em escala quase zero a indisponibilidade de seus serviços oferecidos perante aos seus clientes.

Referências

ANDRADE, Márcio. *Conhecendo e configurando o PfSense*. 2015. Disponível em: <http://sejalivre.org/conhecendo-configurando-pfsense/>. Acesso em: 14 fev. 2016.

DAVID, Daves. *Configuring Vlans*. 2007. Disponível em: <http://searchnetworking.techtarget.com/Configuring-VLANs/>. Acesso em: 28 fev. 2016.

FILHO, Antônio Silva. *Segurança da Informação*. 2010. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm/>. Acesso em: 04 fev. 2016.

INFOTECH. *Conceito de Infraestrutura de TI*. 2011. Disponível em: <https://infotechsolucoes.wordpress.com/2011/03/25/conceito-de-infraestrutura-de-ti//>. Acesso em: 28 fev. 2016.

MAIA, Marco. *Segurança da informação*. 2015. Disponível em: <http://segurancadainformacao.modulo.com.br/seguranca-da-informacao >. Acesso em: 24 fev. 2016.

PINHEIRO, José. *Conceitos de Infraestrutura*. 2010. Disponível em: http://www.projetoderedes.com.br/aulas/ugb_infraestrutura/UGB_aula1_Conceitos_de_Infraestrutura.pdf/>. Acesso em: 04 set. 2016.

PILLOU, Jean. *Vlan – Redes Virtuais*. 2016. Disponível em: <http://br.ccm.net/contents/289-vlan-redes-virtuais/>. Acesso em: 12 nov. 2016.

HEIDI, Erika. *Alta disponibilidade de Infraestrutura de Redes*. 2016. Disponível em: <https://www.digitalocean.com/community/tutorials/what-is-high-availability/>. Acesso em: 26 fev. 2016.