ESTUDO DE CASO: MIGRAÇÃO DA REDE DE COMPUTADORES EM UMA INDÚSTRIA PETROQUÍMICA

CASE STUDY: COMPUTER NETWORK MIGRATION IN A PETROCHEMICAL INDUSTRY

Fabio Fonseca Barbosa Gomes[1]
Celso Barreto da Silva[2]

RESUMO

As redes de computadores são importantes recursos utilizados pelas organizações na atualidade, pois essa tecnologia ajuda a empresa na transmissão das informações, servindo como base para a utilização de sistemas organizacionais e é utilizada como forma de comunicação com o mundo, facilitando a transmissão de informações e o crescimento de produtividade das empresas. Este artigo tem como principal objetivo, mostrar a migração do projeto de rede de uma Indústria Petroquímica, abordando os problemas que atingiam a rede antes, como foram às soluções foram geradas e a realização de estudos de satisfação dos usuários mediante um questionário na empresa. Este trabalho foi resultado da participação e observação de todo o projeto de rede da Indústria Petroquímica, realizado por colaboradores da Indústria Petroquímica e das empresas parceiras. Foi realizada uma pesquisa visando saber o que o usuário achou da migração da rede e descobrir quais foram os serviços da rede que se tiveram um melhor desempenho. Os resultados demonstram que o novo projeto de rede é bastante superior ao anterior, tanto em termos de desempenho, quanto em tolerância às falhas. Com a nova rede instalada a empresa poderá ganhar em termos de desempenho e em produtividade.

Palavras-Chave: Redes de computadores, migração, VPN.

ABSTRACT

[1] Mestre em Sistemas e Computação E-mail: fabiofbg@gmail.com
[2] Especialista em Metodologia para Ensino Superior E-mail: profcelsobarreto@hotmail.com

Computer networks are important resources that are used by organizations today, as this technology helps the company in the transmission of information, serving as a basis for the use of important organizational systems and is used as a way of communicating with the world, facilitating the transmission information and, consequently, the productivity growth of companies. This article has as main objective, to show the migration of the network project of a Petrochemical Industry, addressing the problems that reached the network before, how the solutions were generated and the accomplishment of user satisfaction studies through a questionnaire in the company. This work was the result of the participation and observation of the entire Petrochemical Industry network project, carried out by employees of the Petrochemical Industry and partner companies. Research was carried out in order to find out what the user thought of the network migration and to find out which network services had the best performance. The results demonstrate that the new network design is far superior to the previous one, both in terms of performance and fault tolerance. With the new network installed, the company will be able to gain in terms of performance and productivity, which makes it more competitive in the market.

Keywords: *Computers Network, migration, VPN*

INTRODUÇÃO

Com o crescimento cada vez maior dos recursos tecnológicos existentes e da velocidade em que as informações devem ser lidas e processadas, torna-se necessário para as organizações a contratação de colaboradores da área de tecnologia da informação (TI) que sejam capacitadas e treinadas. Além disso, são necessários equipamentos modernos e redes com alta disponibilidade, tolerantes a falhas, seguras e sem lentidão.

As empresas estão constantemente se atualizando para chegar a essa situação, pois elas sabem que se ficarem atrás de outras empresas do mesmo ramo poderá perder produtividade, qualidade e não conseguirão baratear os custos de produção de seus produtos, consequentemente perderão o seu bem mais precioso, o cliente. Neste sentido, uma Indústria Petroquímica percebeu que a sua rede de computadores estava sofrendo com muita lentidão, tempos de resposta muito altos para um determinado serviço que o nível de segurança da mesma não era o ideal. Devido a este fato, ela passou por um processo de migração da sua rede de computadores. Este processo resultou numa solução de rede capaz de fazer com que a informação chegue ao usuário de forma mais rápida e segura, evitando que problemas maiores acontecessem no futuro.

A topologia antes existente na organização não estava bem distribuída, dentre as quatro redes existentes nas cidades do Rio de Janeiro - RJ, São Paulo - SP, Sorocaba - SP e Camaçari - BA. Uma primeira decisão foi o aumento do *link* da Internet em Camaçari, mudanças nas redes de Sorocaba e São Paulo, a instalação um *link* alternativo para evitar que a rede pare quando o *link* principal falhar, outro fato importante foi a implantação de um novo *firewall* que irá monitorar toda a rede, gerando segurança dos dados vindos da Internet.

O objetivo deste trabalho é mostrar como aconteceu a migração da estrutura de rede dessa Indústria Petroquímica, quais as dificuldades e soluções foram encontradas para resolver esses problemas, considerando o prazo estabelecido pelo coordenador e por uma empresa parceira. No desenvolvimento desta monografia, foi feito um levantamento das melhores políticas para o projeto de rede e um estudo de caso da implantação de melhorias na rede de computadores da Indústria Petroquímica e o resultado das melhorias foi realizado via um questionário respondido pelos usuários.

Inicialmente serão estudados conceitos básicos de VPN (*Virtual Private Network* - Rede Privada Virtual), *Multiprotocol Label Switching* (MPLS) e de projetos de rede. Na etapa da mudança, a migração do endereço IP (*Internet Protocol* - Protocolo Internet) foi feita de forma gradual em todas as redes, Camaçari ficando por último por ter a rede mais complexa, nesse momento, instalado o novo *firewall* denominado Cisco Adaptive Secure Appliance (ASA).

2. REDE PRIVADA VIRTUAL

Segundo Chin (1998), as *Virtual Private Networks* ou Redes Privadas Virtuais, conhecidas como VPN são canais de comunicação privados e criptografados entre dois pontos autorizados (usuários remotos e uma rede corporativa) através da internet, esse canal é seguro. O foco principal deste tipo de comunicação é a economia e a segurança, pois a VPN é utilizada através da Internet, que é insegura principalmente quando se transmite sobre informações sigilosas da organização através da VPN, por esse motivo os dados são criptografados evitando, assim, que caiam nas mãos de usuários maliciosos. (LEAL e FILHO, 2021).

Segundo Chin (1998), a VPN é dividida em três principais aplicações:

a) Acesso remoto via Internet: Para que este tipo de conexão ocorra basta que o cliente tenha um provedor de Internet, assim que ele se conectar a rede mundial de computadores, o software da VPN que está instalado no seu micro, irá criar uma conexão remota com a rede corporativa, assim o usuário passa a ter os recursos da rede, a partir de onde ele estiver.

b) Acesso remoto de LAN via Internet: Com a VPN, é possível que duas ou mais LAN possam ser conectadas através da Internet, para que isso seja possível, é necessário apenas um *link* dedicado entre as LAN, com isso, organizações que possuam matriz e filiais em cidades distantes, podem se conectar na mesma rede.

c) Conexão de computadores numa *intranet*: Cada departamento está em um local diferente e para que esses dados possam ser compartilhados surge o servidor VPN, que interconectam essas estações formando uma LAN.

Para que as VPN sejam seguras e possam ser utilizadas rotineiramente pelas organizações é necessário serem cumpridas determinadas etapas de segurança, a

VPN precisa ter: autenticação dos usuários, criptografia, ocultamento do endereço da VPN, gerenciamento de chaves de forma que devam ser mantidas em sigilo entre as pessoas envolvidas na VPN e é importante que a VPN tenha suporte a múltiplos protocolos e não fique presa apenas ao IP (KUROSE e ROSS, 2021).

A tecnologia VPN funciona por meio de um protocolo de tunelamento, esse protocolo tem a capacidade de compactar e criptografar (caso o pacote seja interceptado no meio do caminho, não será possível lê-lo) o pacote dentro de seu protocolo e enviá-lo através da internet para o ponto final de onde existe a chave para descriptografar o pacote no formato original (LEAL e FILHO, 2021) (CRIST, 2015).

Os protocolos da VPN são divididos em duas camadas: protocolos de enlace e protocolos da rede. Os protocolos de enlace visam o principal o transporte dos protocolos IP e outros, o transporte é feito como forma de encapsulamento. Os protocolos de rede são aqueles que encapsulam os pacotes IP com um cabeçalho adicional do mesmo protocolo, antes de enviá-los para a rede. O protocolo que faz isso é chamado de IPSec (*Internet Protocol Secure* - Protocolo Internet Seguro), que procura o aumento da segurança dos pacotes IP, este protocolo será absorvido pela nova tecnologia denominada Internet IPv6 (Internet *Protocol version* 6 – Protocolo Internet Versão 6) (CHIN, 1998) e (KUROSE e ROSS, 2021).

4. *MULTIPROTOCOL LABEL SWIWTCHING*

Segundo Torre *et al.* (2021), o MPLS (*Multiprotocol Label Switching* – Multiprotocolo de Troca de Rótulos) é uma tecnologia que surgiu com o objetivo principal de capacitar diversos serviços que funcionem com segurança de forma paralela numa infraestrutura compartilhada na rede, concentrando diversos tipos de serviços, incrementando a qualidade de serviços.

Esta tecnologia possui a capacidade de chaveamento e comutação de fluxo de dados de forma eficiente, com isso diminui a capacidade de processamento dos equipamentos de rede, além de ligar tecnologias de rede diferentes com uma Eficiência maior. Os métodos de engenharia de tráfego que utilizavam MPLS surgiram na década de 1990 e o MPLS foi sendo fundido por novos protocolos pela IETF, gerando interesse de organizações que viram no MPLS uma tecnologia nova que estava além dos domínios da engenharia de tráfego (KUROSE e ROSS, 2021).

Segundo Torre *et al.* (2021) existem duas maneiras de roteamento, o roteamento convencional e o MPLS, em um roteamento tradicional, à medida que um pacote chega a um roteador, ele tem um algoritmo de roteamento que escolhe o próximo roteador ao qual ele deverá enviar aquele pacote. Ao utilizar o MPLS, as rotas são otimizadas, os roteadores já sabem antecipadamente para qual caminho irão mandar o pacote, antes mesmo de ele chegar.

Para ter esse conhecimento, os roteadores usam um rótulo, conhecido como *label,* que informa para qual caminho aquele pacote deve seguir. Esta característica reduz o uso do processamento dos roteadores que não precisam mais calcular para qual roteador o pacote deverá ser enviado. Isso traz vantagens em relação ao roteamento tradicional são elas: o QoS (*Quality of Service* – Qualidade de Serviço) e a Engenharia de tráfego (LEAL, 2004).

Na Engenharia de tráfego, o MPLS tem a capacidade de utilizar o IGP (*Interior Gateway Protocol* – Protocolo de Entrada Interior) como maneira de facilitador para a engenharia de tráfego, com isso ele tem a informação sobre a rota que o pacote deve seguir. A rota é obtida através de algoritmos de roteamento do IP tradicional, o MPLS pode, também, utilizar as diversas informações inseridas no cabeçalho IP para definir uma rota.

O MPLS necessita que sejam indicadas rotas explícitas para atingir um determinado nível de qualidade de serviço. O tratamento de roteamento é feito de duas maneiras, a rede MPLS pode gerar múltiplos caminhos alternativos e a segunda maneira é a utilização do rótulo pelo MPLS para indicar o caminho necessário da rota (GOLDANI, 2005).

5. PROJETO DE REDE

Segundo Pinheiro (2004), atualmente é muito comum serem feitos projetos de rede por via de informações imprecisas, com isso o produto ou serviço formado não terá a qualidade esperada. Para que isso não aconteça é necessário utilizar uma metodologia de projetos especificada em documentos e dados reais da organização. Para que a metodologia seja realizada é necessário o uso de ferramentas que façam a avaliação dos problemas e, depois, o projeto deverá propor a solução desses problemas com técnicas, procedimentos e conceitos (PETERSON e DAVIE, 2011).

A metodologia de Birkner (2003) é dividida em seis etapas distintas, demonstradas abaixo:

a) Analisar requisitos: Deve-se verificar o custo-benefício da rede e levar em conta as novas tendências da tecnologia, que trazem novos aplicativos que consomem mais a banda, devido a esses motivos, deve-se levar em conta entrevistas com usuários e estudos para projetar a rede que consiga utilizar a capacidade de banda de maneira mais objetiva possível, visando o desempenho da mesma.

b) Desenvolver a estrutura de interconexão de redes: Nessa etapa é desenvolvida uma topologia de toda a rede, esta topologia é dividida em três camadas: núcleo (camada em que estão localizados os enlaces para pontos remotos, que ligam um grupo de redes a uma WAN empresarial, por exemplo), distribuição (camada onde é formada a topologia geral da rede as políticas implementadas para o funcionamento da mesma) e acesso (fornecimento de acessos da rede para o usuário final), cada camada realiza uma função específica para a rede, esse método de camadas transforma a rede de computadores em uma rede altamente flexível e escalável.

c) Estabelecer convenções de endereçamento e nomes: convenções para desenvolvimento de um esquema geral de nomes de interfaces de rede e de endereços IP como forma de facilitar o gerenciamento da rede no futuro.

d) Especificar *hardware*: Etapa onde são definidos os *hardwares* que serão utilizados na rede, o ideal é sempre utilizar os *hardwares* mais atualizados disponíveis no mercado, pois a tecnologia é atualizada de forma rápida e em pouco temo os equipamentos se tornarão obsoletos.

e) Empregar recursos: Etapa na qual são definidos recursos de *proxy,* filas, forma de tráfego, QoS, dentre outros que serão utilizadas na rede.

f) Implementar, monitorar e gerenciar a rede: esta etapa é a última, mas o ciclo nunca termina, pois, a tecnologia está em constante crescimento e em mudanças, vai chegar a um determinado ponto que o administrador terá que atualizar seu parque de *hardware* ou utilizar alguma nova tecnologia na rede. Nestes casos, o ciclo começa, volta-se para a etapa de especificação do *hardware* para passar novamente pela etapa empregar recursos e depois voltar para a etapa de gerenciamento. (BIRKNER, 2003), (SOUSA, 2009).

6. ESTUDO DE CASO: MIGRAÇÃO DA REDE DE COMPUTADORES EM UMA INDÚSTRIA PETROQUÍMICA

A Indústria Petroquímica fica localizada no Polo Petroquímico de Camaçari (BA). Na matriz, a infraestrutura da TI é formada por quarenta micros, dezessete *notebooks*, nove servidores, um *cluster* (formado por três *switchs*, dois servidores XSeries 366M, um *storage* DS4300 e um servidor XSeries 346M), no qual funciona a aplicação mais importante da empresa, o SAP R/3, este sistema é responsável pela execução de todas as tarefas administrativas dos funcionários da empresa e é onde estão armazenadas todas as informações da organização.

Nos outros pontos, a empresa possui: dois servidores, cinco *notebooks* e vinte micros em Sorocaba (SP), um servidor, três *notebooks* e cinco micros no Rio de Janeiro (RJ) e um servidor, um *notebook* e dez micros em São Paulo (SP). Toda a organização possui setenta e quatro microcomputadores, vinte e quatro *switchs*, treze servidores, quatro roteadores, vinte e cinco *notebooks*.

O cabeamento de rede da organização é constituído de cabos par-trançado, fibras ópticas, com objetivo de conectar a infraestrutura do SAP R/3 (que tem seu *cluster* funcionando exclusivamente com fibras ópticas de 1Gb) e a rede industrial da organização. Além dessas duas tecnologias, a empresa também possui *Wi-Fi* no ambiente organizacional.

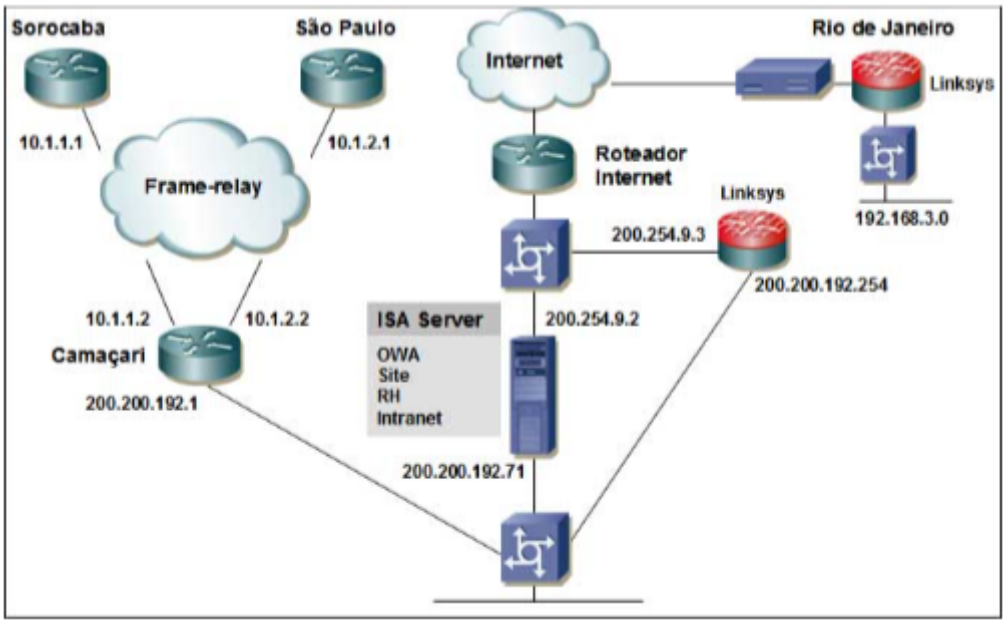
A topologia de rede era suscetível a perda de comunicação entre o *link* do Rio de Janeiro e a matriz em Camaçari, pois estas eram duas redes distintas, cuja conexão era feita mediante uma linha ADSL, que ligava Camaçari para o Rio de Janeiro através de um roteador/modem com conexão ADSL. Com isso, a gestão da empresa, que fica no Rio de Janeiro, tinha que operar de outras maneiras para manter o contato com a rede principal da Indústria Petroquímica, que era formada pelas redes de Sorocaba, São Paulo e Camaçari.

Outro problema era o uso da tecnologia VoIP (voz sobre IP), que não funcionava a contento, gerando falhas. Uma das principais era na utilização do canal de voz da VPN, geralmente havia perda de sinal, o que comprometia a comunicação entre as filiais e a matriz. Um problema constante era a lentidão da velocidade da rede, foi relatado através de diversas Ordens de Serviço de Informática (OSI).

Alguns usuários utilizavam acesso discado à Internet para realizar transações bancárias da empresa. Na figura 1, a estrutura de rede estava interligada por

frame-relay, as redes de Sorocaba e São Paulo estavam interligadas com Camaçari. O *link* de Internet (Embratel - Camaçari) era de 50Mb e era administrado pela Embratel, a rede interna de Camaçari era de 5Mb.

Figura 1: Topologia do Cenário Anterior



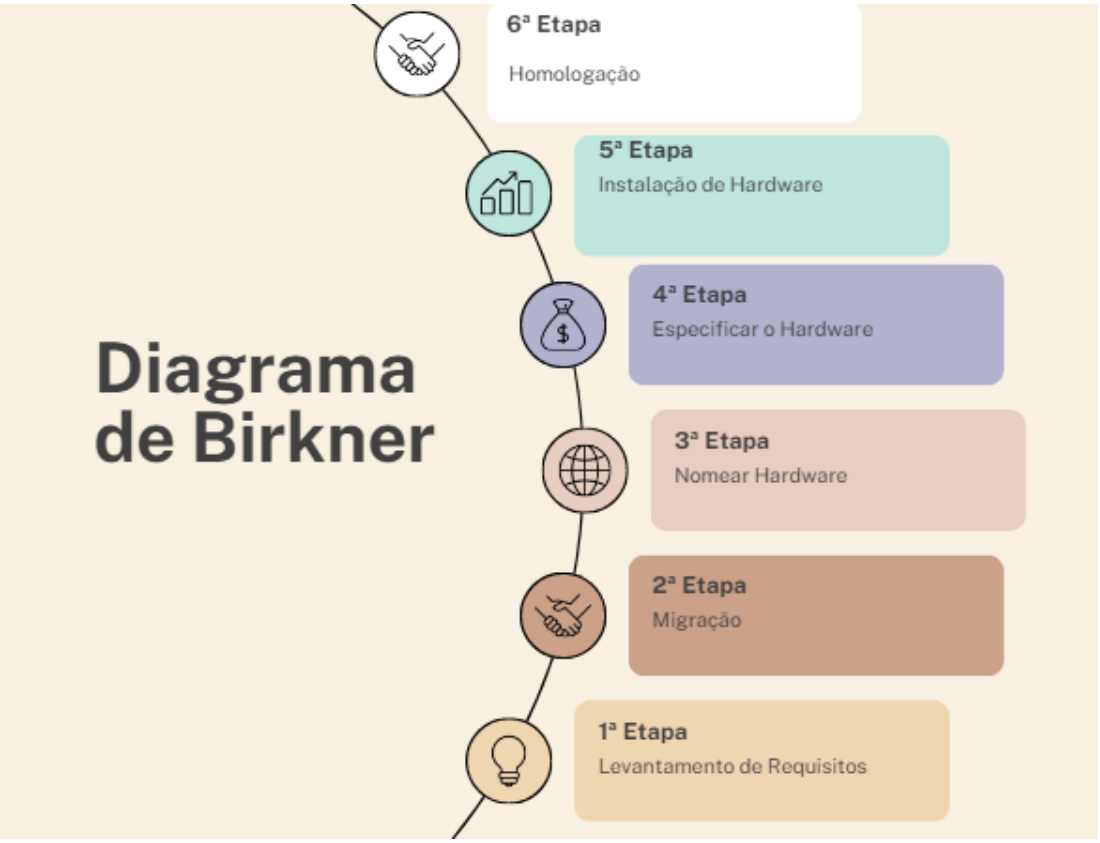
Fonte: Autoria Própria

6.1 PROCESSO DE MIGRAÇÃO

Para realizar a migração, a empresa de consultoria criou um cronograma que definia as etapas em que as mudanças seriam realizadas. Uma empresa fornecedora de internet foi contratada para gerenciar o novo *link* Internet de 100Mb que a conectaria com a rede de Camaçari e um link alternativo de 50Mb, que a conectaria com a rede de Camaçari, caso o link principal falhasse, como um provedor ela possui um *firewall* que protege a nova rede ao se conectar com a Internet. Além do cronograma, a empresa de consultoria disponibilizou relatórios de atendimento técnico (RAT), no qual está todo o detalhamento sobre cada serviço realizado pela organização em parceria com a Indústria Petroquímica e que serviu de base para o levantamento de informações sobre a migração de rede, que será apresentada a seguir.

Muitas das etapas que serão mostradas neste trabalho são baseadas na metodologia de projeto de rede usada por Birkner (2003), elas podem ser visualizadas na figura 2.

Figura 2: Diagrama de Birkner



Fonte: Birkner (2003)

Conforme pode ser visto na figura 1, percebe-se que a metodologia de Biikner está dividida em: (i) levantamento de informações (1ª etapa); (ii) migração (2ª etapa); (iii) nomear hardware (3ª etapa); (iv) especificar o hardware (4ª etapa); (v) instalar o hardware (5ªetapa) e, (vi) homologação (sexta etapa).

Para a realização da 1ª etapa foi necessário realizar duas tarefas:

a) Análise de Requisitos: levantamento das informações pertinentes à rede, número de usuários, equipamentos, rede dentre outros. Foi necessário listar os servidores de cada ponto para mapear os equipamentos que estavam com o IP configurado manualmente, para detectar os equipamentos que não iriam ter a migração de IP dinâmico. Esses equipamentos são cruciais, pois devem manter seus IP fixos, visto que são servidores importantes e, com um IP dinâmico, muitas configurações podem ser comprometidas.

Na organização, existem aplicações que se conectam à rede usando o IP do servidor, ao invés de se conectar pelo nome. Por isso foi necessário identificar quais aplicativos se comportavam dessa maneira, como o caso do ERP SAP R/3. Após essa fase, foi feito um levantamento lógico da rede. Com isso, era necessário saber as configurações que estavam no *firewall* da empresa, bem como saber que regras ele estava gerenciando. Outro ponto importante é saber quais eram os endereços IP públicos que este *firewall* estava gerenciando para corrigir pelos novos IP privados.

b) Testes: Fase na qual são realizados testes de desempenho da rede entre as filiais e a matriz. Era importante saber quais eram os controladores de domínio (descobriu-se que eles estavam no servidor 2 e no servidor 1) e as informações sobre quais dados estavam sendo replicados entre os servidores da rede. Quando um usuário era criado no Active Directory de Sorocaba, por exemplo, a replicação demorava para chegar a todas as redes.
Na comunicação entre Camaçari e Rio de Janeiro também havia o mesmo problema. Isso foi resultado de má configuração dos servidores, o que causava lentidão na rede devido ao excesso de pacotes.

A 2ª etapa foi dividida em três fases:

a) Roteadores: Foi realizada a troca dos endereços IP, fora do horário de expediente, para evitar que os usuários ficassem sem acesso externo. Foram adicionadas novas rotas na tabela do roteador para incrementar o desempenho da rede
b) Testes: Foi utilizado um microcomputador com um IP dinâmico para que fossem realizados os testes com aplicativos (abria-se o programa no aplicativo cliente do SAP e sistemas internos utilizados pela Indústria Petroquímica, para verificar o desempenho da conexão entre a máquina cliente com o IP dinâmico e o servidor), conexão com a Internet e servidores de impressão, essa tarefa foi realizada pelo estagiário de suporte e o teste de acesso SAP foi realizado pelo analista de sistemas, não houve problemas.
c) Migração entre os pontos: Inicialmente, foram trocados os IP dos microcomputadores através de DHCP (protocolo que torna a atribuição de endereços IP automática). Alguns deles precisaram ser configurados manualmente

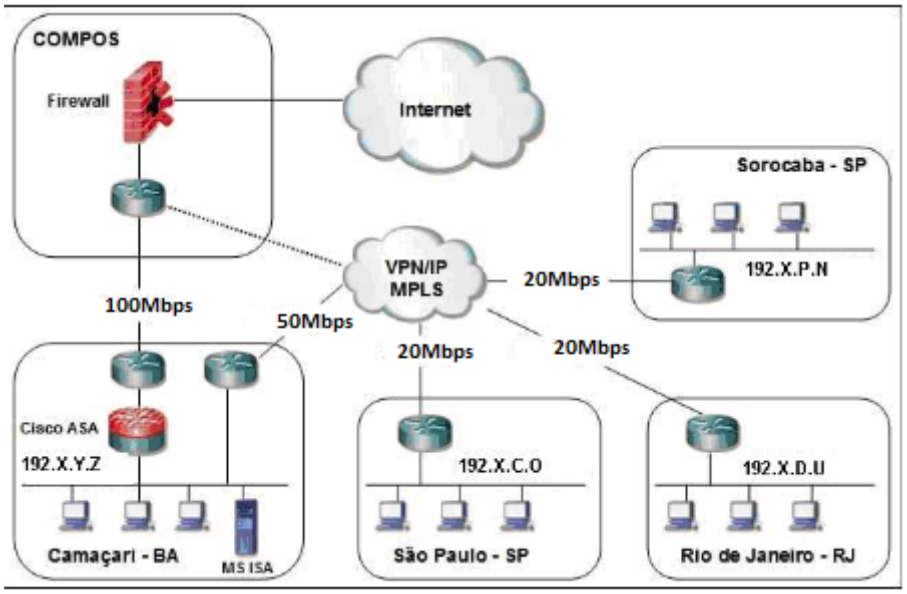
para que o IP dinâmico pudesse ser atribuído, a migração foi feita com sucesso e levou cerca de 6 horas.

Visando aumentar a segurança e o controle dos sites acessados pelos usuários, foi realizada a 5ª etapa da metodologia de Birkner (2003): instalação de equipamentos. Para isso, foi instalado um *firewall* físico denominado Cisco ASA para incrementar a segurança da rede. Outro ponto importante foi a desinstalação do roteador com conexão ADSL, visto que a rede do Rio de Janeiro foi integrada à rede corporativa. O *software* de *firewall utilizado na configuração anterior, passou a ser* usado em conjunto com o Cisco ASA. Cada rede da empresa passou a possuir uma faixa específica de IP. Nas filiais, a mudança de IP foi tranquila e não houve problemas.
O Cisco ASA possibilita a conexão VPN entre as redes da empresa, com isso foi configurado a VPN com segurança MPLS entre a matriz e as filiais, aumentando segurança na transmissão das informações. Desta maneira, o canal de voz será criptografado de maneira que uma ligação entre Camaçari e Rio de Janeiro, por exemplo, não tenha nenhum tipo de invasão por parte de usuários maliciosos da Internet.
Finalmente chegou-se a etapa de homologação, em que realizados testes finais de todos os tipos e não houve problemas detectados. Com isso, a rede corporativa foi declarada apta para voltar ao expediente normal, sem problemas de comunicação entre *hosts* e servidores.

6.2 CENÁRIO POSTERIOR

Depois das mudanças a topologia de rede passou a ficou mais unida, muito mais estável (o ponto do Rio de Janeiro agora faz parte da rede e os pontos de São Paulo e Sorocaba também estão ligados diretamente a rede de Camaçari, através da VPN, eliminando a necessidade do *frame-relay*) e segura (a empresa possui três *firewalls*, o ISA Server, Cisco ASA, o firewall do provedor utilizado na Empresa fornecedora de internet e ainda tem uma rede alternativa, para o caso da rede principal falhar). A figura 3 exibe como ficou a nova topologia de rede da organização.

Figura 3: Cenário posterior



Fonte: Autoria própria

As redes foram interligadas mediante uma VPN com segurança MPLS, a Embratel possui o link principal da Internet, conectado com a Empresa fornecedora de internet, a Empresa fornecedora de internet trabalha como um provedor de acesso da Indústria Petroquímica na Internet, portanto o link Internet Empresa fornecedora de internet /Camaçari é de 100 Mbps.

Caso ocorra alguma falha no *link* Internet principal, é ativado um link alternativo entre a Empresa fornecedora de internet e a Indústria Petroquímica que utiliza a VPN, nesse link alternativo, a velocidade de banda é de 50Mb. Sorocaba passou a ficar com a velocidade de rede de 20Mb, São Paulo com 20Mb, Rio de Janeiro com 20Mb e Camaçari com 50Mb.

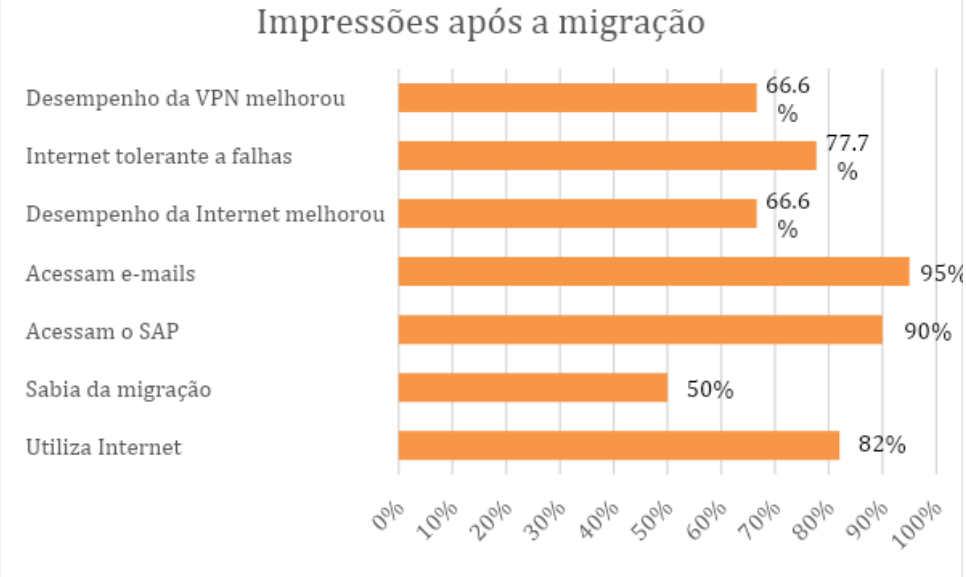
O *link* de Internet da empresa é usado voltado para a produtividade, ou seja, a empresa não permite o uso de *softwares* de bate-papo, *downloads* por meio de FTP, sites de *broadcast* (*sites* de *streaming* de vídeos, como o YouTube) e *sites* impróprios como de jogos, comunidades ou de conteúdo adulto.

Foi implantada a tecnologia WebVPN, com isso, o usuário pode acessar a rede da empresa sem precisar ter um aplicativo de acesso a VPN instalado no seu microcomputador, essa tecnologia também possui o protocolo IPSec. A telefonia sofreu diversas melhorias depois da reorganização da rede da empresa, com isso a velocidade da Internet dobrou de 50Mb para 100Mb, consequentemente, a

qualidade das ligações feitas através do VoIP (Voz sob IP) melhorou, eliminando o problema dos cortes.

O problema de replicação do Active Directory e do Exchange (compartilhamento de agenda) entre os diversos pontos da organização foi resolvido, com a configuração correta dos servidores, o acesso ao ERP SAP se tornou mais rápido nos pontos do Rio de Janeiro, Sorocaba e São Paulo, as aplicações se tornaram mais seguras ao serem acessadas de fora da organização. Após a implantação, foi realizado uma pesquisa por perguntas em um questionário para atender a um universo de vinte colaboradores da empresa e, os resultados podem ser vistos na figura 4.

Figura 4: Resultado da pesquisa



Fonte: Autoria própria

Conforme pode-se ver na figura, foi descoberto que 82% acessam a Internet; metade sabia da migração; 90% acessam SAP e 95% e-mails; 66,6% acham que o desempenho da Internet melhorou; 77,7% acham a Internet mais tolerante a falhas; 66,6% acham que o desempenho da VPN melhorou e apenas 5 usuários, de 18 que usam SAP, acham que ele melhorou.

CONSIDERAÇÕES FINAIS

É de extrema importância que as organizações mantenham as suas redes de computadores seguras, com qualidade e escaláveis, pois a organização sempre

tende a crescer e se faz necessário que sua rede de computadores possa crescer em conjunto.

Dessa forma, as informações estarão seguras e a qualidade da rede de computadores será a melhor alta possível. Esse conjunto de fatores irá tornar os usuários mais satisfeitos, consequentemente, tornará a empresa mais competitiva no mercado. Além disso, os sistemas de informação da empresa irão funcionar da forma mais produtiva possível, gerando mais lucratividade.

O objetivo geral foi atingido, realizado um estudo de caso na Indústria Petroquímica para a migração da rede. Os objetivos específicos foram atingidos e descobriu-se que o SAP não apresentou mudanças com a migração da topologia de rede, pois ele utiliza uma tecnologia diferenciada (os servidores do SAP se comunicam na velocidade de 1Gb, enquanto os *switchs* da organização na totalidade trabalha em 10/100) e os equipamentos de rede da Indústria Petroquímica precisam ser modificados para que este ERP ganhe em desempenho. Para que isto fosse realizado seria necessária uma nova abordagem na estrutura de rede interna da empresa totalmente nova, com uma velocidade de tráfego interna maior que 100Mb, o que seria um alto investimento e a sugestão para um novo trabalho acadêmico, caso essa mudança possa ocorrer no futuro.

O estudo de caso da Indústria Petroquímica possibilitou muitas mudanças na estrutura de redes de computadores da empresa, além de proporcionar mais desempenho e qualidade na transmissão dos dados. Todos os gráficos gerados, com exceção dos dados gerados através do questionário, foram cedidos pela organização e através deles pode-se verificar que a rede está se mantendo constante e está sendo utilizada por uma faixa de banda razoável.

Mesmo com a instalação do Cisco ASA, ainda é necessário que a organização invista em novos equipamentos de rede, como *switches* e conversores mais atualizados e de maior qualidade, para que a banda de rede possa ser mais bem gerenciada e controlada. Não foi possível mensurar a rede antes da migração da estrutura porque a empresa não possuía nenhum tipo de ferramenta que pudesse gerar gráficos da rede, o estudo do cenário anterior e seus problemas, foram baseados nas reclamações de usuários e diversos atendimentos de suporte na área

de redes e de telefonia, onde os usuários se queixavam constantemente das falhas no VoIP e da rede estar extremamente lenta.

Seria interessante para novos trabalhos e pesquisas na área, estudar a rede depois do investimento em novos equipamentos de rede, mais confiáveis e de fácil gestão, outro tema interessante para ser realizado na empresa seria um estudo da segurança da informação como forma de verificação da utilização do usuário na rede e formas de controlar a banda de rede, no sentido de respeitar as políticas de segurança e das normas de sites impróprios mantidos pela organização.

Um problema crítico detectado com a migração de rede foi a dependência de um provedor de acesso. A estrutura anterior não tinha nenhum provedor, possuindo acesso direto com a Embratel, ela se comprometia a fazer manutenção constante e otimizada. Com essa nova estrutura, a Empresa fornecedora de internet passou a receber o link da Embratel, tratá-lo e repassá-lo para a Indústria Petroquímica, caso aconteça um problema na Empresa fornecedora de internet, como uma queda de energia, por exemplo, a rede da Indústria Petroquímica e de todos os clientes da Empresa fornecedora de internet também irão falhar.

Também é necessário configurar o Cisco ASA como forma de não permitir que os usuários possam efetuar downloads ou acessar sites de *broadcast*, pois esses sites ajudam a consumir o *link* Internet da rede corporativa. A equipe de migração de rede não realizou uma análise das cargas e fluxos de dados dos servidores visando estimativa de equipamentos e bandas de acesso, se esse levantamento tivesse sido feito, provavelmente a rede não precisaria ter um aumento de banda e sim um controle maior dos acessos dos usuários na Internet.

É necessária uma análise do tráfego da rede para uma possível diminuição da taxa de transmissão através da implantação de uma política de segurança eficaz, com isso deverá ser possível diminuir o tráfego de dados economizando na velocidade da banda.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURA E SIGLAS

IP *Internet Protocol (Protocolo Internet)*

MPLS *Multiprotocol Label Switching* (Multiprotocolo de Troca de Rótulos)

TIC *Tecnologia da informação e comunicação.*

TI *Tecnologia da Informação.*

VPN *Virtual Private Network (Rede Privada Virtual)*

REFERÊNCIAS

BIRKNER, Matthew H. Projeto de Interconexão de Redes Cisco Internetwork Design - CID, Makron Books, São Paulo, 2003.

CHIN, Liou Kuo. Rede Privada Virtual - VPN, 1998. Disponível em: < http://www.rnp.br/newsgen/9811/vpn.html>. Acesso em: 16 jun. 2023.

CRIST, Eric F. Mastering OpenVPN, Packt Publishing, 2015.

GOLDANI, Carlos Alberto. Multiprotocol Label Switching (MPLS). Univert Brasil Certificadora. São Paulo, 2005.

KUROSE, J. F. ROSS, K. W. Redes de Computadores e a Internet: uma abordagem top-down. 8ª edição. Addison Wesley. São Paulo, 2021.

LEAL, Marco Aurélio de Araújo, QoS - Qualidade dos Serviços em TCP/IP. UFLA, Lavras, 2004.

LEAL, Matheus Carvalho e PEREIRA FILHO, Marcelo Renato do Carmo. 2021. A Importância da Vpn (Virtual Private Network) Durante a Pandemia COVID 19: Uma Revisão de Literatura in Facit Business and Technological Journal.

PETERSON, Larry L. e DAVIE, Bruce S. Redes de Computadores – Uma Abordagem de Sistemas, 2011

PINHEIRO, José Maurício Santos, Caracterizando a Rede Existente Para Um Novo Projeto. 2006 <http://www.projetoderedes.com.br/artigos/artigo_caracterizando_a_rede_existente.php> Acesso em: 16 jun. 2023.

PINHEIRO, José Maurício Santos, Metodologia de Projetos, um Desafio. 2004 < http://www.projetoderedes.com.br/artigos/artigo_metodologia_projetos.php> Acesso em: 15 fev. 2020.

SOUSA, Lindeberg Barros. Projetos e implementação de redes: Fundamentos, Soluções, Arquiteturas e Planejamento. Érica, Rio de Janeiro, 2009.

TORRE, Daniel Iglesias; PALIZA, Félix Álvarez; FLEITES, Arelis Ramos. Combinación de mecanismos MPLS en una arquitectura SDN. (2021) Telemática