INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA - CÂMPUS CAÇADOR
CURSO DE GRADUAÇÂO EM SISTEMAS DE INFORMAÇÃO

BRUNO DO AMARAL

IMPLEMENTAÇÃO DE UMA REDE DE OPERAÇÃO SEGREGADA

CAÇADOR, 2023.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA - CÂMPUS CAÇADOR
CURSO DE GRADUAÇÂO EM SISTEMAS DE INFORMAÇÃO

BRUNO DO AMARAL

IMPLEMENTAÇÃO DE UMA REDE DE OPERAÇÃO SEGREGADA

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Bacharel em Sistemas de Informação.

Orientador:
Prof. Ma.Andréa Simone Machiavelli Pontes, Msc

Coorientador:
Me.Ademir Goulart, Msc

CAÇADOR, 2023.

Amaral, Bruno
S329i Implementação de uma Rede Operação Segregada /Bruno do Amaral; orientador: Andréa Simone Machiavelli Pontes; coorientador: Ademir Goulart. -- Caçador, SC, 2023.
49f.

Trabalho de Conclusão de Curso (Graduação)-Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, Curso de Sistemas de Informação.
Inclui bibliografias

1. Rede de Computadores. 2. Segurança da Informação. 3. Segregação de Redes. I. Pontes, Andréa Simone Machiavelli. II. Goulart, Ademir. III. Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina. Curso de Sistemas de Informação. IV. Título.

CDD 658.4038

Ficha catalográfica elaborada pela Bibliotecária
Karla Viviane Garcia Moraes – CRB-14/1002

IMPLEMENTAÇÃO DE UMA REDE DE OPERAÇÃO SEGREGADA

BRUNO DO AMARAL

Este Trabalho foi julgado adequado de forma parcial para obtenção do Título de Bacharel em Sistemas de Informação e aprovado na sua forma parcial pela banca examinadora do Curso de Sistemas de Informação do Instituto Federal de Educação Ciência, e Tecnologia de Santa Catarina.

CAÇADOR, 20 de novembro de 2023.

Banca Examinadora:

Documento assinado digitalmente
gov.br
ANDREA SIMONE MACHIAVELLI PONTES
Data: 13/05/2024 10:50:25-0300
Verifique em https://validar.iti.gov.br

Ma.Andréa Simone Machiavelli Pontes, Msc. Msc.

ADEMIR GOULART:19222262034
Digitally signed by ADEMIR GOULART:19222262034
DN: C=BR, O=ICP-Brasil, OU=Presencial, OU=83059667000197, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(em branco), CN=ADEMIR GOULART:19222262034
Reason: I attest to the accuracy and integrity of this document
Location:
Date: 2024.05.14 10:56:25-03'00'
Foxit PDF Reader Version: 2023.2.0

Me.Ademir Goulart, Msc. Msc.

Documento assinado digitalmente
gov.br
RUI BATISTA DOS SANTOS
Data: 09/05/2024 08:31:38-0300
Verifique em https://validar.iti.gov.br

Esp.Rui Batista dos Santos.

Documento assinado digitalmente
gov.br
CARLOS HENRIQUE RADAVELLI
Data: 17/05/2024 13:35:55-0300
Verifique em https://validar.iti.gov.br

Me.Carlos H. Radavelli, Msc.

"Creio firmemente em uma lei de compensação. As verdadeiras recompensas são sempre proporcionais ao esforço e aos sacrifícios feitos". (Nicola Tesla)

AGRADECIMENTOS

Gostaria de expressar minha sincera gratidão aos meus orientadores e à instituição pela orientação e apoio valiosos que me proporcionaram ao longo desta jornada acadêmica. Agradeço pela dedicação em compartilhar seus conhecimentos e experiências, inspirando-me a alcançar todo o meu potencial.

Além disso, estendo minha gratidão à instituição por criar um ambiente propício ao aprendizado e ao desenvolvimento, proporcionando recursos e oportunidades que enriqueceram minha experiência educacional. Sou grato por fazer parte desta comunidade dedicada à busca do conhecimento e ao avanço acadêmico.

Aos meus queridos pais, quero expressar minha mais profunda gratidão por tudo o que vocês fizeram por mim ao longo dos anos. Sua incansável dedicação, amor e apoio inabalável moldaram a pessoa que sou hoje. Agradeço por cada sacrifício que fizeram em prol do meu bem-estar e por cada lição valiosa que me ensinaram.

Gostaria de agradecer também a minha querida esposa, por sua presença constante em minha vida. Seu amor incondicional, apoio incansável e compreensão infinita, têm sido a âncora que me mantém forte. Agradeço por sua paciência nos momentos difíceis e por seus sorrisos que iluminam até os dias mais sombrios. A você só tenho a agradecer.

Agradeço também por cada novo dia, por cada sorriso compartilhado e por cada desafio que me ajuda a crescer. Que a luz de Deus, continue a guiar meus passos e que Sua graça continue a abençoar minha jornada. Amém.

“Aqueles que se sentem satisfeitos sentam-se e nada fazem. Os insatisfeitos são os únicos benfeitores do mundo.” (Walter S. Landor)

RESUMO

Este trabalho de conclusão de curso, teve como objetivo, identificar e solucionar os problemas de uma empresa, que operava com apenas uma rede, o que causava sérios problemas, envolvendo a segurança da informação e segurança operacional do negócio, sendo necessário inicialmente um estudo e levantamento bibliográfico, para por fim realizar a sua aplicação. Durante o desenvolvimento deste trabalho de conclusão de curso, foi identificado que a implementação de uma nova rede segregada para operações foi planejada e executada com êxito, atendendo todas as expectativas e trazendo diversos benefícios significativos para a administração dos sistemas de TI. O aumento operacional foi significativo, uma vez que interrupções de manutenção na rede administrativa anteriormente impactavam negativamente as operações, devido à dependência mútua. Com a introdução de uma nova rede dedicada exclusivamente às operações, as manutenções realizadas na rede administrativa não afetam mais as operações diárias. Além disso, a separação das redes resultou em um desempenho aprimorado para ambas, permitindo um fluxo de dados mais eficiente e uma maior capacidade de tráfego na rede local. A adoção de uma rede segregada, combinada a um ambiente completamente virtualizado, evidencia claramente como a eficiência das equipes de TI e operacionais é aprimorada, proporcionando ambientes mais seguros e ágeis para a execução das atividades diárias. Isso garante a continuidade fluida dos serviços do negócio.

Palavras-chave: Rede de computadores. Segurança. Virtualização. Segregação.

ABSTRACT

This course completion work aimed to identify and solve the problems of a company, which operated with only one network, which caused serious problems, involving information security and operational security of the business, initially requiring a study and bibliographical survey, to finally carry out its application. During the development of this course completion work, it was identified that the implementation of a new segregated network for operations was planned and executed successfully, meeting all expectations and bringing several significant benefits to the administration of IT systems. The operational increase was significant, as maintenance interruptions in the administrative network previously negatively impacted operations due to mutual dependence. With the introduction of a new network dedicated exclusively to operations, maintenance carried out on the administrative network no longer affects daily operations. Additionally, separating the networks resulted in improved performance for both, allowing for more efficient data flow and greater traffic capacity on the local network. The adoption of a segregated network, combined with a completely virtualized environment, clearly shows how the efficiency of IT and operational teams is improved, providing safer and more agile environments for carrying out daily activities. This ensures the smooth continuity of business services.

Keywords: Computer network. Security. virtualization. Segregation.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ARPAnet	*Advanced Research Projects Agency Networks*(Rede da Agência de Pesquisas em Projetos Avançados)
ESXI	*Elastic Sky X integrated*(Plataforma de Virtualização Integrada)
IBM	*International Business Machines.*(Corporação Internacional de Máquinas de Negócios)
ICMP	*Internet Control Message Protocol*(Protocolo de Mensagens de Controle da Internet)
IFSC	Instituto Federal de Santa Catarina
IP	*Internet Protocol*(Protocolo de Internet)
ISP	*Internet Service Provider*(fornecedor de serviços de Internet)
LAN	*Local Area Network*(rede local)
OSI	*Open Systems Interconnection*(Interconexão de Sistemas Abertos)
OSPF	*Open Shortest Path First*(Escolher o caminho mais curto primeiro)
QOS	Qualidade do serviço
TCC	Trabalho de conclusão de Curso
TCP	*Transmission Control Protocol*(Protocolo de Controle de Transmissão)
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*(Protocolo de datagramas de utilizador)
VLAN	*Virtual Local Area Network* (Rede local virtual)
VM	*Virtual Machine* (Máquina Virtual)
WEB	Internet

SUMÁRIO

1 INTRODUÇÃO

Rede de computadores é uma malha que interliga milhares de sistemas computacionais para a transmissão de dados. Também conhecidos como nós, esses dispositivos interconectados enviam, recebem e trocam tráfego de dados, voz e vídeo, graças ao hardware e software que compõe o ambiente. Controle Net Tecnologia (2023)

Um levantamento feito pela Associação Brasileira de Prevenção de Perdas (Abrappe) em setembro de 2018 revelou que o varejo do país perdeu 19,5 bilhões de reais em 2017 por danos em produtos ou furtos. O dado mostra como as companhias podem sofrer grandes perdas por conta da falta de segurança patrimonial, inclusive em setores de indústria e serviços, independentemente do tamanho da empresa.Exame. (2023)

Companhias de pequeno e médio porte, inclusive, devem planejar com cuidado o orçamento de segurança. É preciso investir em soluções que garantam a proteção sem exigir grandes investimentos.Exame. (2023)

A grande maioria das empresas de pequeno porte, nem mesmo investem em equipamentos para sua rede interna, não possuem firewall, e switch normalmente é implementado do tipo não gerenciável. Assim o switch, apenas é usado como uma ponte com o roteador e os demais componentes que serão utilizados na rede.

A segurança de uma rede, envolve vários fatores, sendo um dos principais a vulnerabilidade de uma rede empresarial. Quando não se possui um firewall em sua ponta, para filtrar as informações que trafegam por ela. Quando não se possui esse tipo de proteção, a rede fica, totalmente exposta a ataques maliciosos, roubo de informações e ataques direcionados de todas as partes do mundo.Porém a segurança de uma rede não para na implantação de um *firewall*, para se ter um ambiente mais confiável e seguro, necessita ir além.

A segregação de uma rede, é uma das principais armas, para deixar o ambiente mais seguro, pois separará os ambientes da empresa, por níveis de acesso, deixando muitas vezes a rede separada em três ou até quatro ambientes diferentes. Deixando assim os usuários comuns sem acesso, ou permissão de modificação, em dados mais sigilosos da empresa.

A segregação de redes permite que as organizações isolem diferentes segmentos de rede, limitando o acesso a dados confidenciais e sistemas críticos somente a usuários autorizados. Ao criar barreiras entre os diferentes setores da rede, é possível controlar melhor o tráfego de dados, reduzir o risco de violações de segurança e impedir a propagação de malware.

Além disso, a segregação de redes facilita o cumprimento de regulamentações de privacidade e proteção de dados, como o GDPR (Regulamento Geral sobre a Proteção de Dados) na União Europeia e leis similares em outras regiões do mundo. Ao estabelecer zonas distintas e restringir o acesso a informações confidenciais, as organizações podem garantir a conformidade com os requisitos legais de proteção de dados.

Em suma, a segregação de redes desempenha um papel crítico na preservação da integridade dos dados, na proteção contra ameaças cibernéticas e na garantia da conformidade regulatória. É uma estratégia de segurança indispensável para garantir a resiliência das operações comerciais em um cenário digital cada vez mais complexo e interconectado.

1.1 Justificativa

É de extrema importância manter e garantir que a infraestrutura lógica e física de uma empresa esteja totalmente segura, pelos seguintes motivos:

• Ambiente mais seguro - traz mais confiabilidade para empresa a respeito de suas informações mais sigilosas, até mesmo quanto a suas operações diárias, no caso de empresas que também necessitam de uma comunicação, para o funcionamento de softwares e máquinas, várias empresas, inclusive de grande porte, já foram reféns de ataques maliciosos, através de suas redes.

• Resolução de problemas sem parada geral da rede empresarial - é possível realizar atividades distintas em uma rede segregada, onde a rede que está passando por manutenção, não interferir no funcionamento do restante da rede, trazendo assim otimização e desempenho contínuo nas atividades.

• Princípio do menor privilégio - nessa abordagem de segregação, se trabalha com o princípio do menor privilégio, ou seja tanto funcionários e visitantes na rede da empresa, só tem aceso a ferramentas e informações que sejam estritamente necessários, para suas atividades, e é assim que começa a proteção de uma rede segregada.

• Segmentação de redes por bolhas - antes do conceito de segmentação de redes começar a ser usado, todos os profissionais voltados a segurança de redes, tentavam manter uma grande bolha segura de tudo e de todos, o que tornava a proteção do ambiente, bem mais complicado, na segregação, se cria várias bolhas, ou redes menores, onde cada uma tem a sua determinada função e liberação, podendo muitas vezes não ter nem acesso ao mundo exterior, ”internet”.

• Controle de acesso aprimorado - com a implantação de uma rede segregada através de um *firewall*, é possível impor várias políticas de controle internamente, tornando assim o ambiente bem restrito ao que vai trafegar na rede.

• Melhor desempenho - com a segregação da rede , a intranet é divida em vários segmentos distintos e com funções definidas, diminuindo o congestionamento da rede e automaticamente, melhorando o desempenho.

Por isso foi identificado a necessidade de realizar a segregação de redes, de uma empresa de médio porte, que possuí um número de 90 funcionários, e que atualmente conta com apenas uma rede, que é usada para fins adeministrativos e operacionais.

1.2 Definição do Problema

No mundo corporativo empresas de todos os ramos de serviços que possamos imaginar, enfrentam um grande problema, que são os riscos de segurança a informação. Riscos esses que são gerados por vários motivos (roubo de dados, espionagem industrial, *Phishing*, funcionários não especializados, softwares vulneráveis, ataques direcionados, além de vários outros.

O trabalho em questão busca aplicar uma rede segregada para o ambiente de operação. A rede de operação, será destinada, para a comunicação de equipamentos, como controladores lógicos programaveis, rádios, computadores e VMs - *virtual machine*, que estarão operando totalmente segregados da rede de TI(Tecnologia da Informação)/Administrativa da empresa. Trazendo assim, uma rede dedicada para o seu negócio, e outra para questões administrativas, tornando o ambiente muito mais confiável e seguro.

1.3 Objetivo Geral

Implementar uma rede de computadores segregada, destinada a operação de uma empresa de saneamento, localizada no município de caçador de médio porte.

O intuito dessa implementação é deixar o ambiente mais seguro e estável, e menos vulnerável a possíveis invasões hackers e captura de informações.

1.4 Objetivos Específicos

- Definir uma base teórica para conceitos de Rede de Computadores, Segurança da informação e virtualização.
- implementar uma rede de computadores segregada, destinada a operação.
- Construir um ambiente virtualizado, através da ferramenta, *Vmware*, em um servidor físico, para expansão, das redes criadas em segregação.
- Apresentar os resultados através da implementação.

1.5 Estrutura do Trabalho

Este trabalho está dividido, em 5 capítulos. No primeiro capítulo, descrevemos um pouco, sobre a introdução, justificativa, definição do problema, objetivo geral e objetivos específicos do trabalho. No segundo capítulo, realiza-se a fundamentação teórica do trabalho, o capítulo que dá corpo ao assunto levantado para pesquisa. Capitulo três, é onde se menciona os procedimentos metodológicos para o trabalho. No Capítulo quatro, cita-se os resultados prévios e esperados. Capítulo cinco, é onde relata-se as considerações finais desse trabalho.

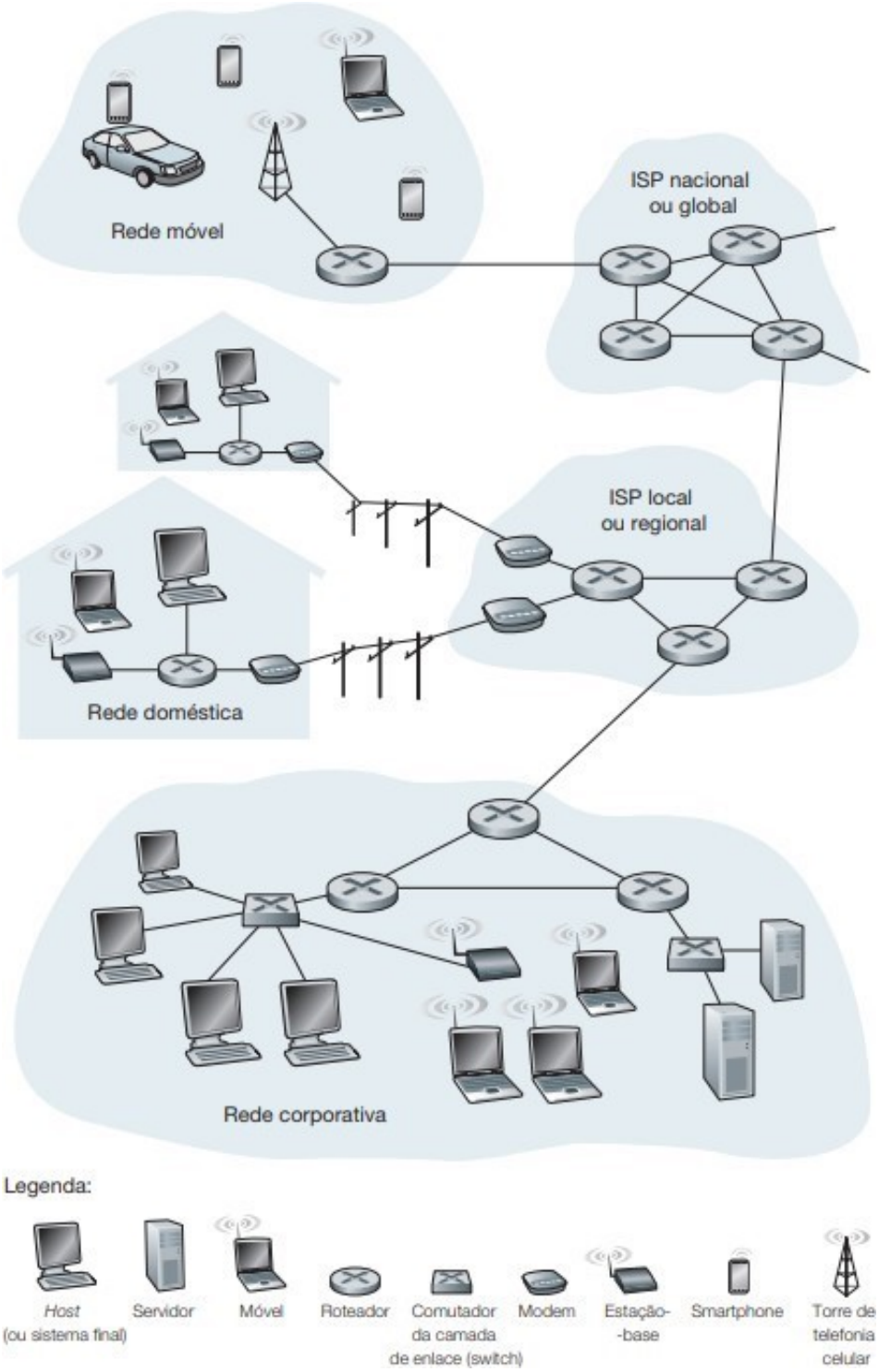
2 FUNDAMENTAÇÃO TEÓRICA

2.1 O que é uma Rede de Computadores e Internet?

Há diversas maneiras de responder a essa questão. Primeiro, podemos descrever detalhadamente os aspectos principais da Internet, ou seja, os componentes de *software* e *hardware* básicos que a formam. Segundo, podemos descrever a Internet em termos de uma infraestrutura de redes que fornece serviços para aplicações distribuídas. Kurose e Ross (2013)

> A Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de computação ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente PCS de mesa, estações de trabalho Linux, e os assim chamados servidores que armazenam e transmitem informações, como páginas da *Web* e mensagens de e-mail. No entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, *webcams*, automóveis, dispositivos de sensoriamento ambiental, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados à rede.
>
> Na verdade, o termo rede de computadores está começando a soar um tanto desatualizado, dados os muitos equipamentos não tradicionais que estão sendo ligados à Internet. No jargão da rede, todos esses equipamentos são denominados hospedeiros ou sistemas finais. Em julho de 2011, havia cerca de 850 milhões de sistemas finais ligados à Internet [ISC, 2012], sem contar os smartphones, laptops e outros dispositivos que são conectados à rede de maneira intermitente. No todo, estima-se que haja 2 bilhões de usuários na Internet [ITU, 2011]. KUROSE; ROSS, 2013,p 330

Figura 1 – Alguns Componentes da Internet



Fonte: Redes de computadores e a internet (2013)

2.1.1 Gerência de Redes

Nos primeiros anos das redes de computadores, quando elas ainda eram usadas como um artefato de pesquisa, e não vista como uma infraestrutura utilizada por milhões de pessoas no seu dia a dia,"gerenciamento de rede"era algo de que nunca se tinha ouvido falar. Se alguém descobrisse que estava com algum problema em sua rede, poderia ser resolvido com alguns testes simples, como um ping, para localizar a fonte de seu problema, e em seguida realizar os ajustes necessários no sistema, reiniciar o software, ou hardware, ou chamar algum amigo para assim fazer.

No ano de 1980, dia 27 de outubro, teve a primeira grande "queda"da ARPAnet (Advanced Research Projects Agency Network, isso muito antes da existência de qualquer ferramenta para gerenciamento de rede.com o passar do tempo essas pequenas redes, foram se transformando em infraestruturas globais, e assim se tornou inevitável a necessidade de ter algum tipo de gerenciamento dessas redes.com isso podemos falar, que temos cinco principais áreas de gerenciamento de rede. Kurose e Ross (2013)

a) Gerenciamento de desempenho: Principais objetivos do gerenciamento de desempenho são, quantificar, medir, informar, analisar e controlar o desempenho, de diferentes componentes da rede,podendo eles ser dispositivos individuais como por exemplo (enlaces, hospedeiros e roteadores).

b) Gerenciamento de Falhas: Registra, detecta e reage às condições de falha da rede, é o tratamento imediato contra falhas transitórias de rede.

c) Gerenciamento de configuração: Permite que o administrador da rede consiga saber quais dispositivos fazer parte da sua rede administrada e quais são suas configurações de *hardware* e *software*.

d) Gerenciamento de contabilização: Tem como principal objetivo, fazer com que o administrador da rede possa especificar, registrar e controlar o acesso de usuários e dispositivos aos recursos da rede.

e) Gerenciamento de Segurança: A principal meta do gerenciamento de segurança é poder controlar o acesso aos recursos, da rede de acordo, com alguma política definida. Rodrigo, Silva (2023)

2.2 Segurança da informação na Rede

Segurança da informação em redes de computadores, pode ser separada quatro pontos principais. Nela o objetivo a ser alcançado é de ter uma comunicação, que possamos ter confiança, sobre a informação que recebemos, ou seja ter certeza de que a comunicação que recebemos de uma ponta, está vindo de fato da fonte em que esperamos, e que essa informação não esteja distorcida. Então pode-se dizer que desses quatro principais pontos pode-se chamá-los:

a) Confidencialidade: Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida, o fato de que determinada mensagem possa ser interceptada, exige com que necessariamente essa mensagem seja cifrada, para assim impedir que o interceptador consiga compreendê-la, nesse aspecto de confidencialidade, é provavelmente, o significado mais comumente percebido na expressão comunicação segura.

b) Autenticação do ponto final: O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida nessa comunicação, confirmar que a outra parte é quem realmente alega ser. Entre seres humanos esse tipo de autenticação se torna mais fácil de se realizar, pois pode-se estar usando essa autenticação através do visual ou da voz. já na computação, se torna um pouco mais complicado. Se recebemos um e-mail de um destinatário conhecido, não temos como afirmar, se realmente do outro lado foi a pessoa, que pensamos ser que enviou o e-mail.

c) Integridade da Mensagem: Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também precisam assegurar de a que o conteúdo da comunicação entre eles não seja alterado, por acidente ou até mesmo má intenção, durante a transmissão.

d) Segurança Operacional: Hoje quase todas as empresas, sejam elas empresas públicas, privadas, universidades, escolas etc. Possuem redes conectadas a internet pública, redes essas que podem ser comprometidas potencialmente por atacantes que ganham acesso a essas redes por meio da internet pública. Os atacantes podem estar realizando ataques de worms nos hospedeiros na rede, e assim adquirir segredos corporativos dessas empresas, mapear configurações de redes internas e lançar ataques. Kurose e Ross (2013)

2.3 Segurança Operacional

A internet não é um local seguro, nela os meliantes estão concentrados por todas as partes, criando todo tipo de destruição. A internet é um local bem hostil, vamos pegar como um exemplo uma empresa e um administrador de rede que a administra, olhando através da perspectiva de um administrador. A rede está divida em dois, contendo os bonzinhos(pessoas que pertencem á organização que administra a rede e que podem acessar os recursos que fazem parte da sua rede), de um modo relativamente livre de restrições, e do outro lado os bandidos, todo o restante. Cujo acessos aos recursos da rede devem ser cuidadosamente inspecionados.

Em redes de computadores, quando o tráfego que entra e sai de uma rede passa por inspeção de segurança, é registrado, descartado ou transmitido. Esse tipo de trabalho é realizado, por mecanismos operacionais conhecidos como *firewalls*, sistemas de detecção de invasão e sistemas de prevenção de invasão. Kurose e Ross (2013)

2.4 *Firewall*

Um *Firewall* é a combinação de um *hardware* com um *software*, que serve para isolar uma rede interna de uma organização do restante da internet, permite que alguns pacotes passem, e bloqueiam outros. Um *firewall* permite que seu administrador de rede tenha controle sobre o acesso entre o mundo externo e os recursos internos de sua rede. Também serve para gerenciar o fluxo de tráfego para esses recursos, pode-se dizer que o *firewall* possuí três objetivos principais:

• Todo tráfego de fora para dentro, e vice e versa, passa pelo *firewall*, o *firewall* pode ser colocado em um único ponto da rede, assim como ele pode passar por mais camadas, que é o caso de grandes organizações.

• Somente o tráfego autorizado, como definido na política local de segurança, poderá passar, com todo o tráfego que entra e sai da rede organizacional, passando pelo *firewall*, este pode limitar o acesso a tráfego autorizado.

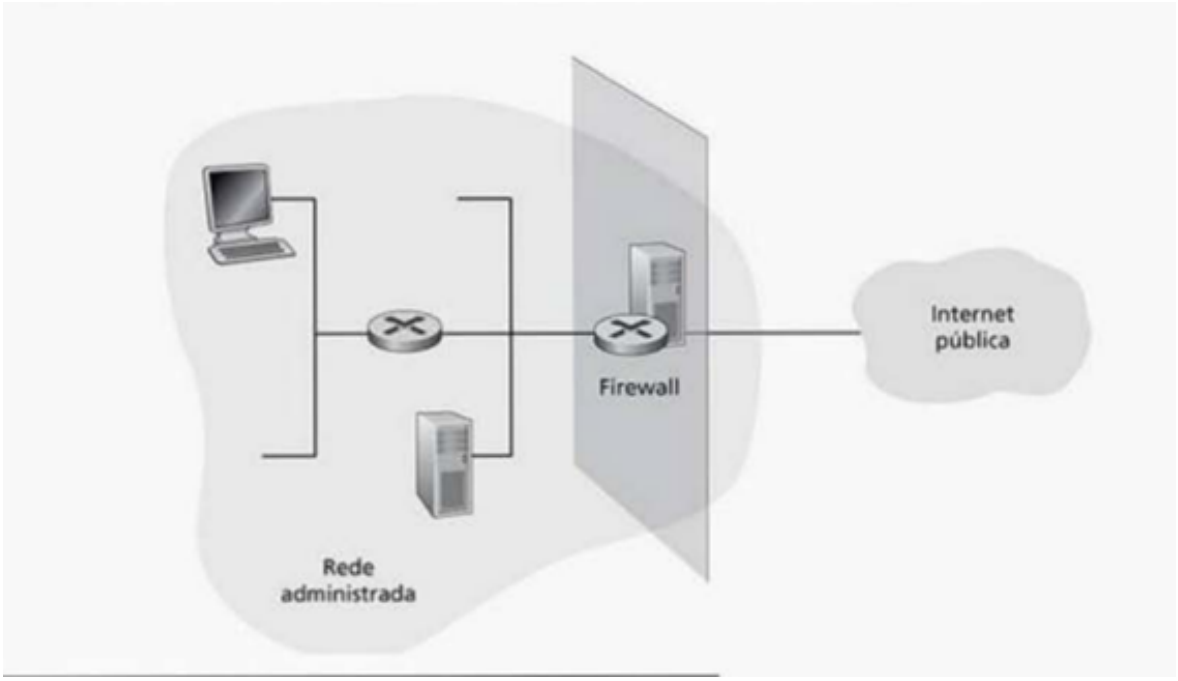
• O *firewall* em si é imune a penetração, o próprio *firewall* é um mecanismo conectado à rede, se não instalado e configurado da forma correta, ele pode ser comprometedor, podendo assim oferecer apenas uma falsa sensação de segurança(que é pior do que não ter nenhum *firewall*). Kurose e Ross (2013)

2.4.1 Filtros de Pacotes Tradicionais

Como mostra a figura 2, uma organização normalmente tem um roteador de borda que conecta sua rede interna com seu ISP (e dali com a internet pública, mais ampla). Todo tráfego que sai ou que entra na rede interna passa por esse roteador e é nesse roteador que ocorre a filtragem de pacotes.

Um filtro de pacote examina cada datagrama que está sozinho, determinando se o datagrama deve passar ou ficar baseado nas regras especificas do administrador. normalmente as decisões de filtragem são baseadas em: Endereço IP de origem e de destino e tipos de protocolo no campo do datagrama *IP*: *TCP*, *UDP*, *ICMP*, *OSPF* e etc.Kurose e Ross (2013)

Figura 2 – Filtro de Pacotes



Fonte:Redes de computadores e a Internet (2013)

2.5 O que é um Switch de Rede?

Um switch de rede é um dispositivo de hardware utilizado em redes de computadores para encaminhar pacotes de dados entre dispositivos dentro da mesma rede local LAN *Local Area Network*. Ele opera na camada 2 (camada de enlace de dados) ou na camada 3 (camada de rede) do modelo OSI *Open Systems Interconnection* e é projetado para melhorar a eficiência e o desempenho das comunicações em rede.

O principal objetivo de um switch de rede é direcionar o tráfego de dados de forma eficiente, enviando pacotes de dados apenas para o destino correto, em vez de para todos os dispositivos conectados à rede, como ocorre em um hub. Isso reduz o congestionamento da rede e melhora a segurança, uma vez que os dados são transmitidos apenas para o dispositivo de destino pretendido.

Os switches de rede podem variar em termos de capacidade, velocidade de transmissão, número de portas e recursos adicionais, como recursos de gerenciamento de tráfego, segurança e QoS (Qualidade de Serviço). Eles são amplamente utilizados em ambientes comerciais e domésticos para criar redes locais confiáveis e eficientes, permitindo a conexão e a comunicação entre vários dispositivos, como computadores, impressoras, servidores e outros dispositivos de rede.Aruba Networks (2023)

2.5.1 Por que Switchs de Rede?

Os switches de rede são essenciais para facilitar a comunicação eficiente e confiável entre dispositivos em uma rede local. Eles oferecem várias vantagens importantes em comparação com tecnologias mais antigas, como hubs. Algumas das razões pelas quais os switches de rede são amplamente usados incluem:

a) Segmentação de rede: Os switches de rede permitem a segmentação eficiente de uma rede em sub-redes menores. Isso pode ajudar a reduzir o tráfego e melhorar o desempenho geral da rede, especialmente em redes maiores.

b) Aumento de velocidade: Eles oferecem velocidades mais rápidas de transferência de dados em comparação com hubs, pois são capazes de transmitir dados diretamente para o dispositivo de destino, sem afetar outros dispositivos na rede.

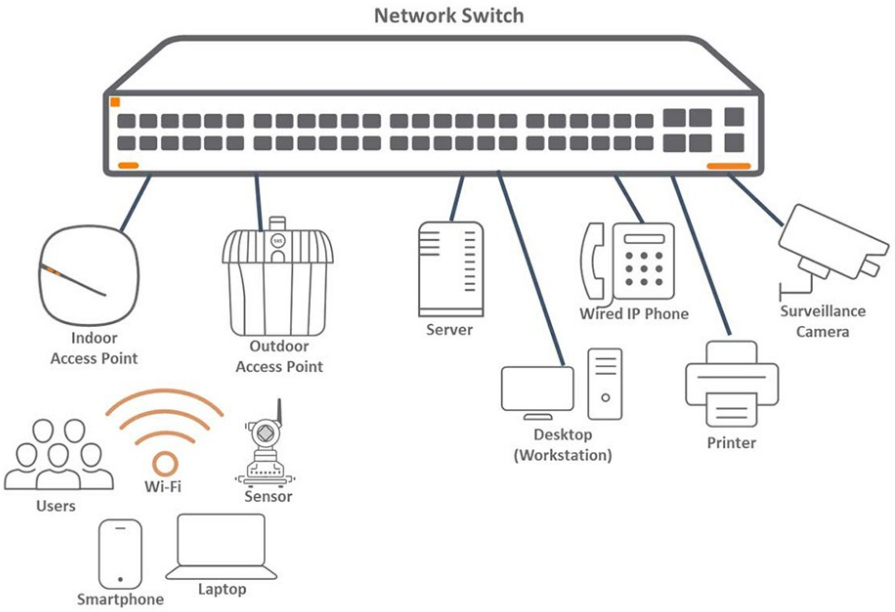
c) Maior Segurança: Os switches de rede oferecem maior segurança, pois direcionam o tráfego de rede apenas para os dispositivos de destino pretendidos. Isso é essencial para redes corporativas e de negócios, onde a segurança dos dados é uma prioridade.

d) Maior Eficiência: Eles melhoram a eficiência da rede ao minimizar colisões de pacotes e otimizar a largura de banda disponível. Isso resulta em uma melhor utilização dos recursos de rede e uma experiência mais rápida para os usuários.

e) Recursos de Gerenciamento: Muitos switches de rede oferecem recursos de gerenciamento avançados, permitindo o monitoramento e o controle detalhados do tráfego de rede. Isso é crucial para redes maiores, onde é necessária uma supervisão cuidadosa para garantir o desempenho ideal da rede.

Um Switch traz muitos beneficios e pode ser utilizado, para várias aplicações em uma rede, servindo até mesmo para dividir a rede, em várias subredes, ou até mesmo, para transmitir outras redes, através do uso de VLANs. Aruba Networks (2023)

Figura 3 – Network Switch

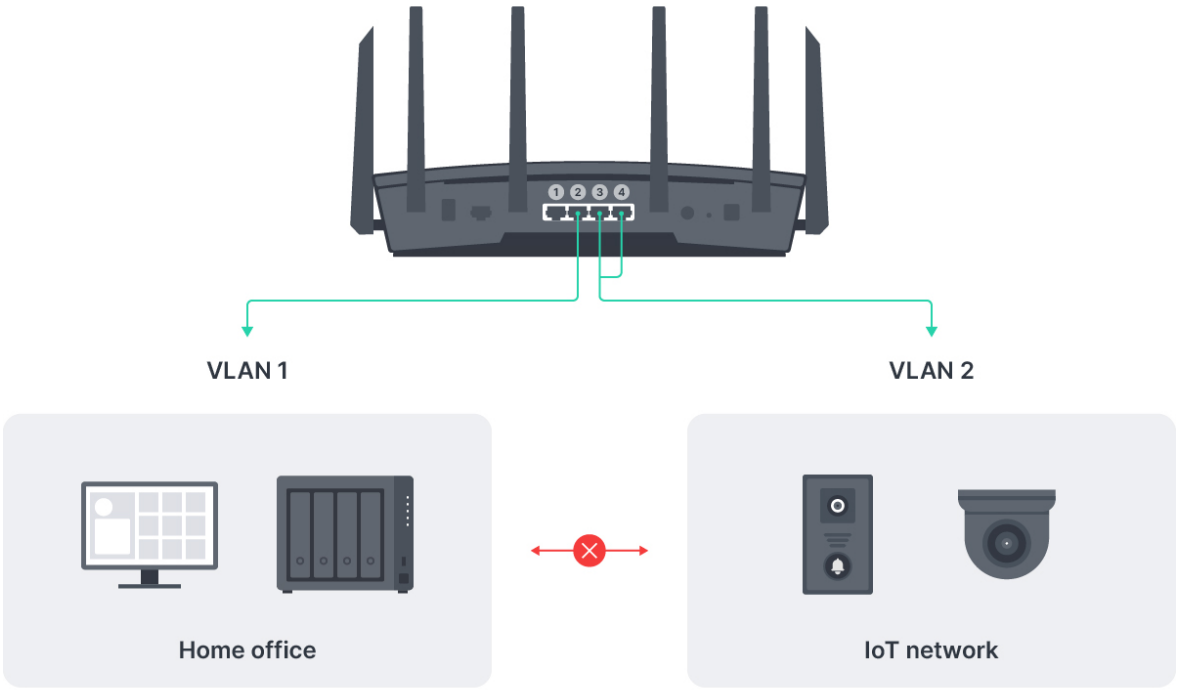


Fonte:https://www.arubanetworks.com

2.6 O que é uma VLAN?

A Virtual Local Area Network(VLAN) é uma rede independente que visa se conectar e se comunicar com redes fisícas, através de domíminios broadcast. É uma separação lógica que serve para melhorar a administração, desempenho e segurança da rede.Tecnoblog (2023)

Figura 4 – VLAN



Fonte:https://kb.synology.com

2.6.1 Para que serve uma VLAN?

As VLANs desempenham um papel crucial na segmentação e organização de redes, facilitando o gerenciamento e a segurança de uma rede de maneira eficaz. Elas fornecem uma abordagem flexível e escalonável para o gerenciamento de tráfego e recursos em ambientes de rede complexos.

A VLAN possui algumas vantagens como:

a) Maior flexibilidade de conexão de rede: A tecnologia VLAN integra diversos locais, redes e usuários para criar um ambiente de rede virtual, proporcionando a mesma conveniência, flexibilidade e eficiência de uma LAN local. A implementação de VLAN pode diminuir a complexidade de realocar ou modificar a localização das estações de trabalho, o que é especialmente vantajoso para empresas com requisitos operacionais sujeitos a mudanças constantes.

b) Controle a transmissão na rede: As VLANs oferecem um recurso de firewall que impede a propagação excessiva de transmissões na rede de switches. Ao utilizar VLANs, uma porta de switch ou um usuário pode ser designado a um grupo específico de VLAN, que pode estar presente em um único switch ou em vários switches. As transmissões dentro de uma VLAN não são enviadas para fora dela, garantindo maior isolamento e segurança. Da mesma forma, as portas adjacentes não recebem transmissões de broadcast originadas em outras VLANs.

c) Melhore a segurança da rede: Uma VLAN atua como um domínio de transmissão segregado, fornecendo isolamento entre diferentes segmentos da rede. Essa separação aprimora a eficiência do uso da rede, ao mesmo tempo que garante maior segurança e confidencialidade dos dados transmitidos. Considerando que dados sensíveis e críticos são frequentemente compartilhados na rede local (LAN), é essencial protegê-los com medidas de segurança, como controle de acesso. Uma abordagem eficaz e simples de implementar é a segmentação da rede em diversos grupos de transmissão separados, nos quais o administrador da rede pode restringir o número de usuários na VLAN e proibir o acesso a aplicativos sem permissão. As portas de comutação podem ser agrupadas com base no tipo de aplicativo e privilégios de acesso, enquanto as VLANs de segurança são geralmente designadas para aplicativos e recursos restritos.Fibermall (2023)

2.7 Virtualização

Com toda a popularidade que as máquinas virtuais ganharam nos últimos anos, as pessoas acabam esquecendo, que elas na verdade, são muito antigas, no início dos anos 1960, a IBM realizou duas experiências com *hipervisores* desenvolvidos independentemente: SIMMON e CP-40, o CP-40 foi um projeto de pesquisa, e logo depois virou o CP-67, para assim iniciar o programa de controle do CP/CMS, um sistema operacional de máquina virtual para o IBM *System/360 Model 67*. e a partir desse modelo, foi reimplementado, por outras vezes,e lançado como VM/370 para a série *System/370* no ano de 1972.Andrew e Boss (2016)

> É impossível escrever um capítulo sobre virtualização sem se referir ao trabalho e terminologia deles. Como se sabe, a conhecida arquitetura x86 que também surgiu na década de 1970 não atendeu a essas exigências por décadas. Ela não foi a única. Quase todas as arquiteturas desde o surgimento dos computadores de grande porte também falharam no teste.ANDREW; BOSS, 2016,p. 327).

As máquinas virtuais, oferecem soluções interessantes para determinados problemas, que há muito tempo incomoda os usuários. Especialmente para os usuários que trabalham com código aberto, como por exemplo: instalar novos programas e aplicativos.

O problema é que várias dessas aplicações dependem de outras bibliotecas e aplicações, que em si são dependentes de uma grande variedade de outros pacotes de *software*, e assim por diante. Além de que, pode haver dependências em versões particulares dos compiladores, linguagens de scripts e do sistema operacional. Agora com a opção das máquinas virtuais, um desenvolvedor de software, poderá construir cuidadosamente uma máquina virtual, carregá-la com o sistema operacional exigido, códigos de aplicação, compiladores e bibliotecas e congelar a unidade inteira, deixando a pronta para executar. Sendo assim essa imagem de máquina virtual, pode ser alocada em algum CD-Rom, Pendrive, website, rede interna para que as pessoas possam baixá-la. Andrew e Boss (2016)

2.8 Ferramentas de Virtualização

2.8.1 Virtual BOX

O Virtual Box, é um produto de virtualização x86 e ADM64/Intel64, tanto para uso doméstico, quanto para uso corporativo, ele não é apenas um produto extremamente rico em recursos e de alto desempenho para clientes corporativos, mais se trata da única ferramenta de solução profissional disponível gratuitamente como *software* de código aberto. Atualmente ele é executado em hosts Windows, Linux, macOS(NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, windows 8, Windows 10), DOS/Windows 3.x, Linux(2.4, 2.6, 3.x e 4.x), solaris e OpenSolaris, OS/2e OpenBSD. Figura 2, apresenta a interface inicial do Virtual Box.Oracle VM VirtualBox (2023)

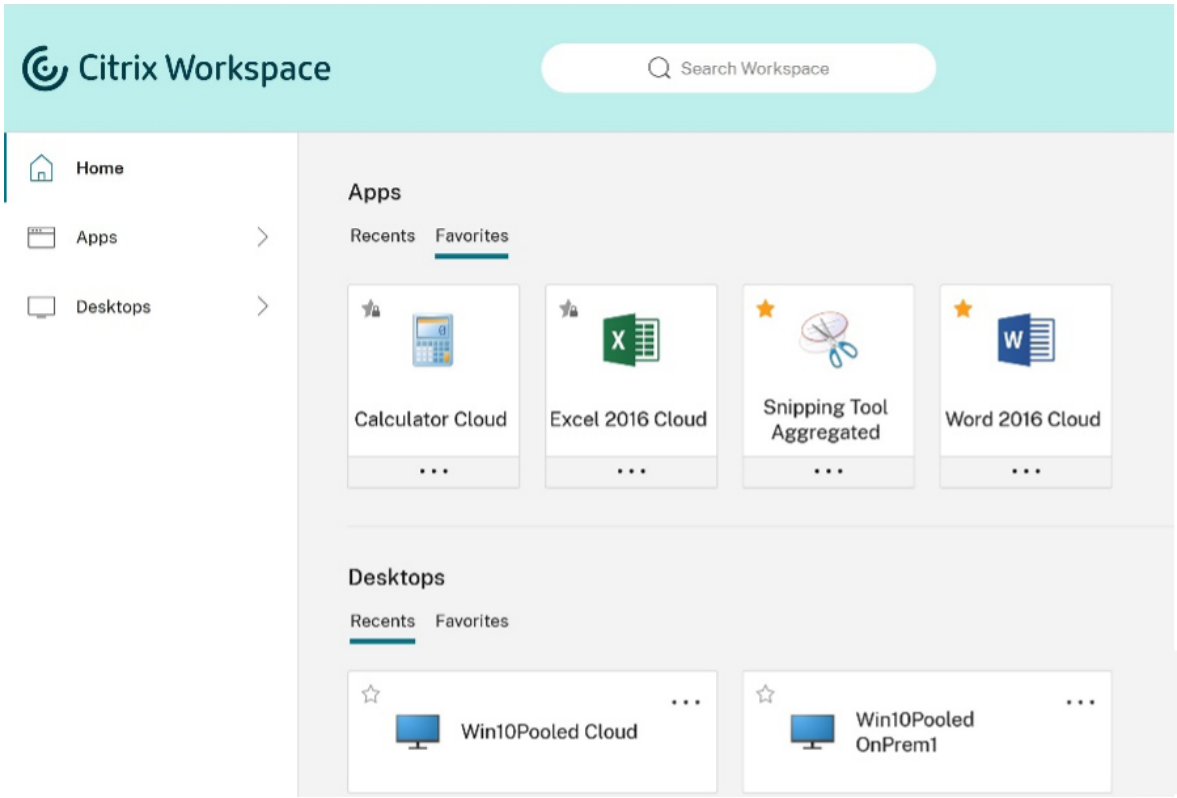
Figura 5 – Virtual Box

Fonte: osxdaily.com

2.8.2 Citrix Workspace

O Citrix Workspace está alimentando a transformação digital, usando os espaços de trabalho, centrados totalmente nas pessoas que oferecem a experiência certa para o usuário certo, e na hora certa, sempre. A ferramenta consegue equilíbrio, flexibilidade e uma experiência, diferente para as pessoas conseguirem ser mais produtivas e com a segurança exigida pela TI. Com o *Workspace* pode-se criar seus desktops, virtuais , e permitir que as pessoas trabalhem de qualquer lugar, e com um recurso que não precisem ser tão potente, mais que contenham apenas uma boa conexão com a internet, é uma excelente opção para empresas que queiram utilizar o recurso como meio de trabalho para a criação de máquinas virtuais. Na figura 4, apresentadado a interface Citrix.Citrix Systems, Inc (2023)

Figura 6 – Citrix Workspace

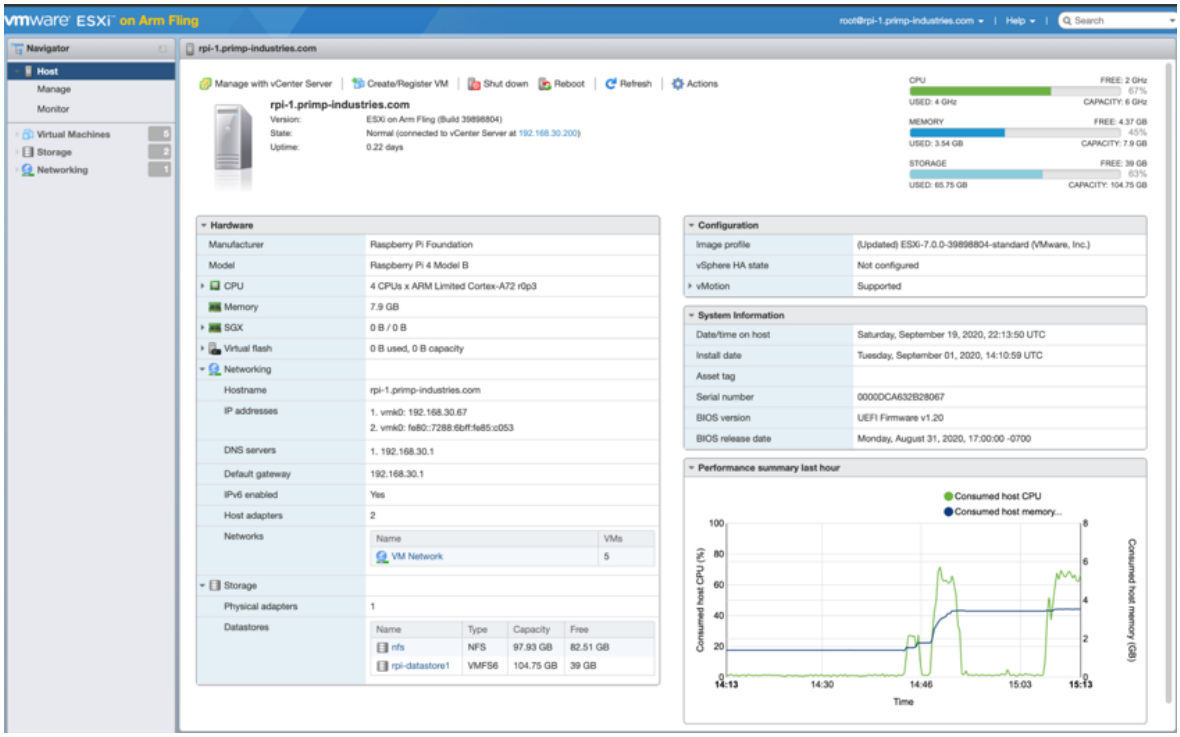


Fonte: docs.citrix.com

2.8.3 VMware ESXi

O Vmware ESXi é um *hypervisor* que é instalado diretamente no servidor físico, ele possui controle e acesso, direto aos recursos da máquina física, ele particiona o *hardware* com eficiência para consolidar aplicativos e reduzir custos, é a ferramenta líder do setor em eficiência na arquitetura, conseguindo um alto padrão de confiabilidade, com desempenho e um ótimo suporte. No presente trabalho a escolha pela ferramenta, foi feita pelos benefícios que ela pode trazer, como consolidar o hardware para uma maior utilização de sua capacidade, aumentar o desempenho para oferecer vantagem competitiva, simplificar a administração da TI por meio do gerenciamento centralizado e também minimizar os recursos de hardware necessários para executar o *hypervisor*, o que no final trás uma melhor eficiência. Figura 05, mostra a interface principal do Vmware.VMware, Inc (2023)

Figura 7 – Vmware ESXI



Fonte: flings.vmware.com

3 PROCEDIMENTOS METODOLÓGICOS

Apresentação da metodologia utilizada para o trabalho, procedimentos realizados, além dos resultados finais do trabalho de conclusão.

3.1 Metodologia de pesquisa

Este trabalho de conclusão de curso foi feito através de uma pesquisa aplicada e se divide em algumas etapas: início, levantamento, pesquisa bibliográfica, construção e aplicação.

> A pesquisa aplicada concentra-se em torno dos problemas presentes nas atividades das instituições, organizações, grupos ou atores sociais. Está empenhada na elaboração de diagnósticos, identificação de problemas e busca de soluções. Respondem a uma demanda formulada por “clientes, atores sociais ou instituições”.THIOLLENT,2009,p. 39).

3.1.1 Início

Foi realizado uma pesquisa bibliográfica para ter uma base de conhecimentos e aplicações disponíveis para segurança de redes, onde foi notado que existem vários, equipamentos , e softwares para se fazer a segregação e virtualização de uma rede.

Após a pesquisa, foi conversado com alguns profissionais das áreas de telecom e cybersegurança, onde foi discutido com duas pessoas responsáveis pelas comunicação da infraestrutura de redes de suas empresas, e também com uma pessoa, responsável por toda infraestrutura de uma empresa de locação de servidores, virtualizados na nuvem, essa conversa teve o intuito de discutir as formas em que poderia ser feito, para atender a demanda do projeto e da empresa. A discussão realizada com os profissionais , chegou ao consenso de estar implementando a separação total das redes, deixando a rede administrativa totalmente separada do ambiente de automação e operação.

3.1.2 Levantamento

No decorrer do projeto, se fez uma nova pesquisa bibliográfica para fixar uma base de conceitos em redes, segurança, infraestrutura, e softwares, para virtualização do ambiente, de servidores e computadores, o motivo foi verificar os conceitos necessários para aplicação do projeto e possuir um suporte acadêmico.

A partir dessa parte, foi elaborado um escopo para definir como seria feito. Por fim, após pesquisas e definições do escopo do projeto, foi realizado a implementação para demonstração de tudo que foi proposto no projeto.

3.1.3 Construção

Seguindo as etapas, foi executado o processo de configuração de uma nova rede no firewall, seguindo para o ambiente de infraestrutura com switch e servidor, e chegando pôr fim a rede lógica dos servidores virtualizados.

3.1.4 Entrega

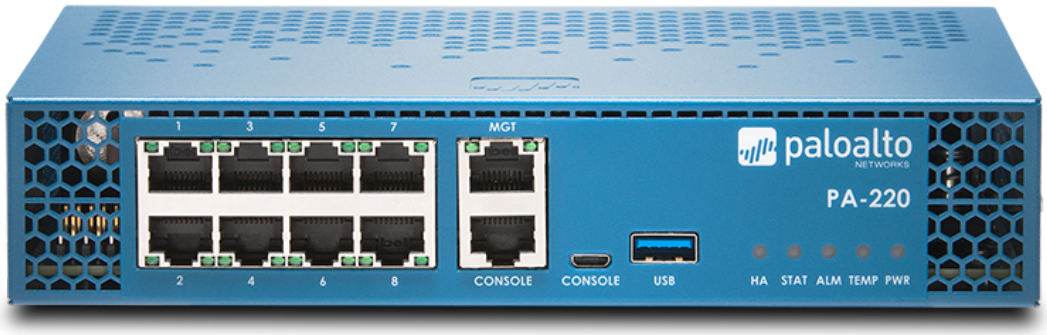
O trabalho teve como objetivo fazer a entrega do projeto proposto implementado, e por fim mostrar a rede pronta e totalmente segregada, da rede de administração, deixando o ambiente mais seguro e funcional para o negócio.

A segurança da informação é crucial para uma empresa, principalmente se tratando de dados e informações privilegiadas, toda empresa deve investir para ter um ambiente seguro e confiável, trazendo assim mais segurança para o seu negócio, um ambiente segregado, traz muito mais segurança e confiabilidade para uma empresa, seja do setor público ou privado.

3.2 Implantação e Segregação da Rede

Seguindo as etapas do projeto, foi realizada a criação de uma nova rede, no software de gerenciamento do firewall, Palo Alto PA-220. continuando as demais configurações, nos demais equipamentos da rede, como switch e servidor virtualizado.

Figura 8 – Palo Alto PA 220

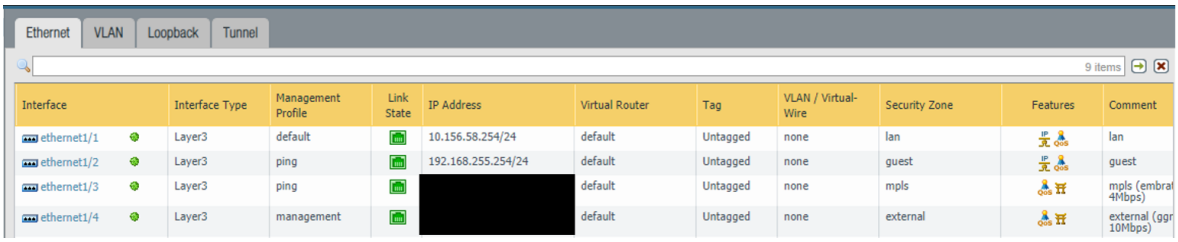


Fonte:https://www.paloguard.com/

3.2.1 Redes externas e administrativas

A criação das novas faixas de redes, foram criadas no software de gerenciamento do firewall da marca Palo Alto, modelo PA 220, o firewall mencionado, já se encontrava em operação, contendo a rede administrativa lan, uma rede guest, e também as entradas de internet local, external e MPLS, conforme apresentado na Figura 08.

Figura 9 – Redes externas e administrativa

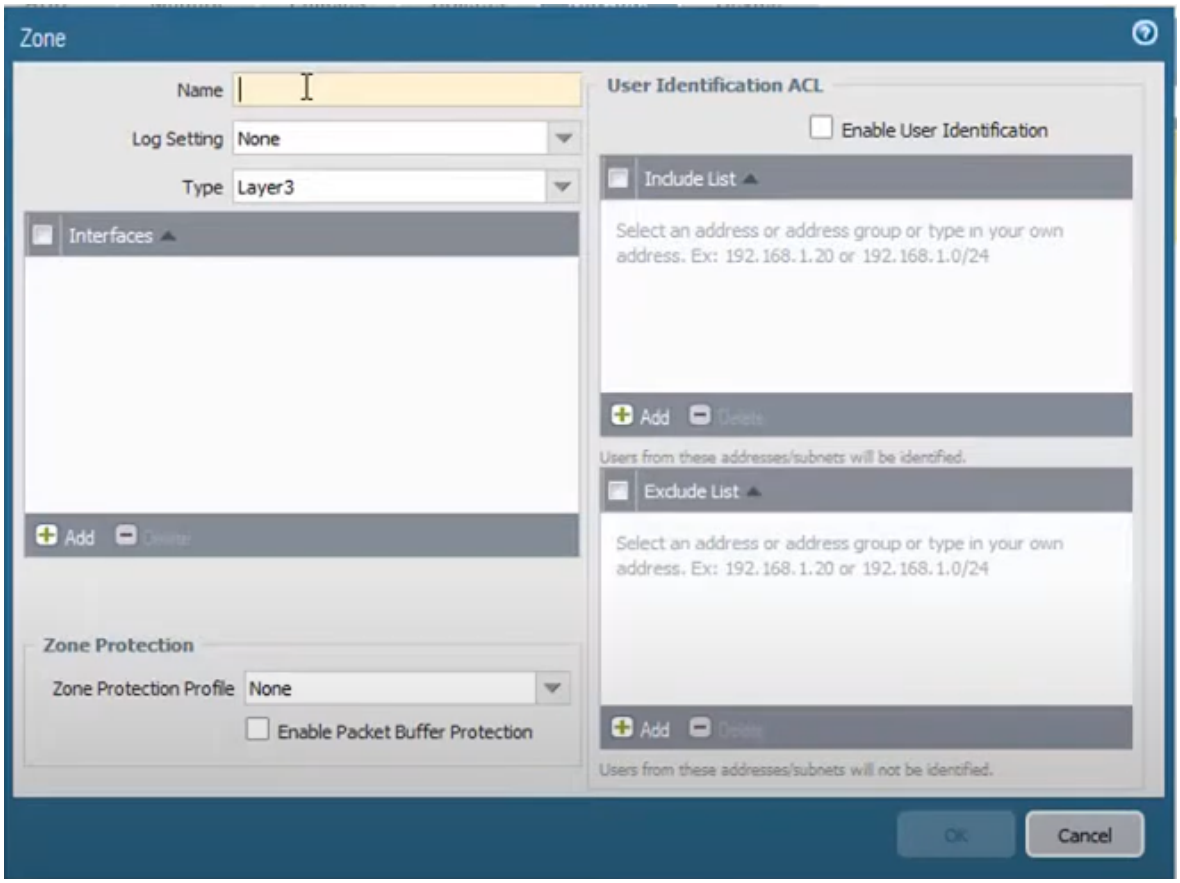


Fonte:Própria (2023)

3.2.2 Criando uma zone para interface de rede no Firewall

Para realizar a segregação de uma rede, é necessária a criação de novas interfaces no gerenciamento do firewall, para isso, foi necessário acessar no painel de navegação do firewall, a opção de zones, onde foi criada a zone da nova interface, conforme mostra nas Figura 09.

Figura 10 – Zone



Fonte:Própria (2023)

3.2.3 Criando novas interfaces de rede no Firewall

Após criação de uma nova zone, foi realizado a configuração das novas interfaces. na Figura 08, temos o mapeamento realizado de cada faixa de IP, com a sua exclusiva finalidade de utilização.

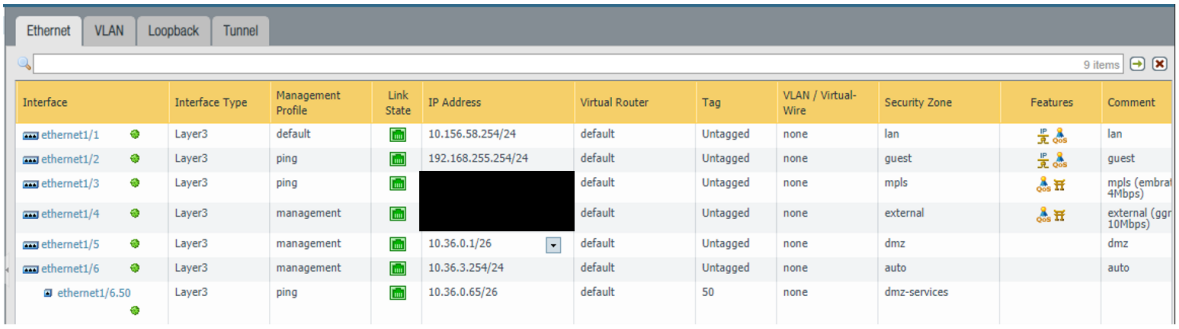
Figura 11 – Faixa IP e suas Finalidades

FINALIDADE	ENDEREÇO IPV4/CIDR	VLAN	Gateway
DMZ	10.36.0.1/26	49	10.36.0.1 (port 1/5)
DMZ de serviços (AD, WSUS, Backup.)	10.36.0.65/26	50	10.36.0.65 (port 1/6)
PLCs, Máquinas virtuais, computadores	10.36.3.254/24	55	10.36.3.254 (port 1/6)

Fonte:Própria (2023)

A lógica representada na Figura 10 acíma, foi implementada, através da criação de novas interfaces, no firewall Palo Alto, ficando a rede DMZ com faixa de IP 10.36.0.1/26, com conexão exclusiva na porta ethernet 5 do firewall, e as redes 10.36.0.65/26 e 10.36.3.254/24, compartilhando a porta ethernet 6 do firewall, sendo a rede 10.36.0.65, sendo utilizada exclusivamente através de uma VLAN.

Figura 12 – Novas Interfaces



Fonte:Própria (2023)

3.3 Configuração das novas camadas de redes no Switch

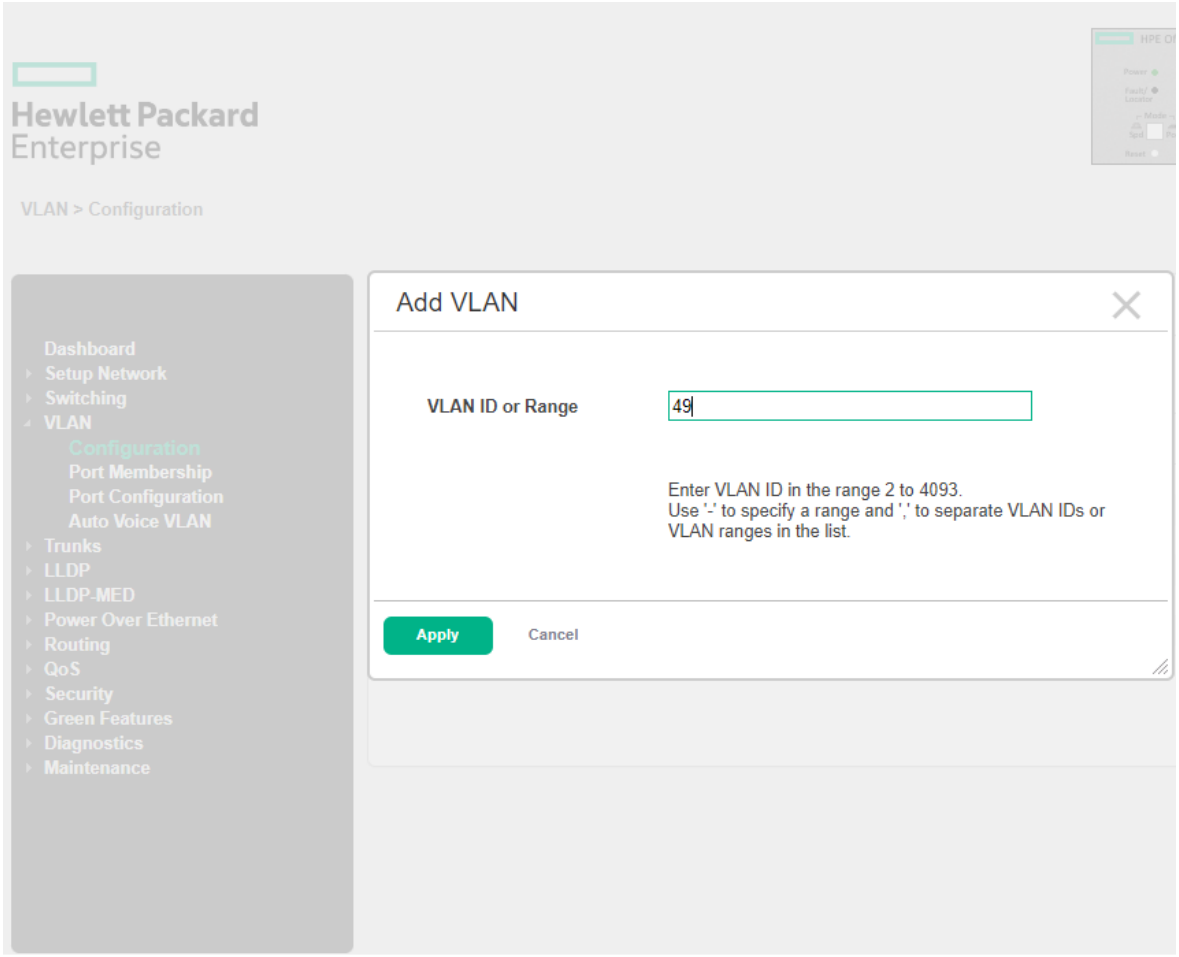
Após finalização da criação das novas interfaces de redes no firewall, onde foi realizada a criação de três novas camadas de redes. foi realizado a configuração também nos demais equipamentos de comunicação, iniciando-se pelo switch core HPE OfficeConnect Switch 1920S 24G 2SFP PPoE+ (185W) JL384A, que é responsável por todo roteamento das redes configuradas no firewall.

Figura 13 – HPE 1920S 24G JL384A

Fonte:https://www.finktecnologia.com.br/

Esse switch está com seu IP fixo 10.156.58.1, configurado na rede administrativa, para que ele conseguisse transmitir as demais interfaces novas criadas no firewall, foi necessário realizar a configuração através de VLANs, cada rede criada possui uma VLAN, com isso foi configurado na aba de VLANs do Switch, todas as VLANs correspondentes as novas redes.

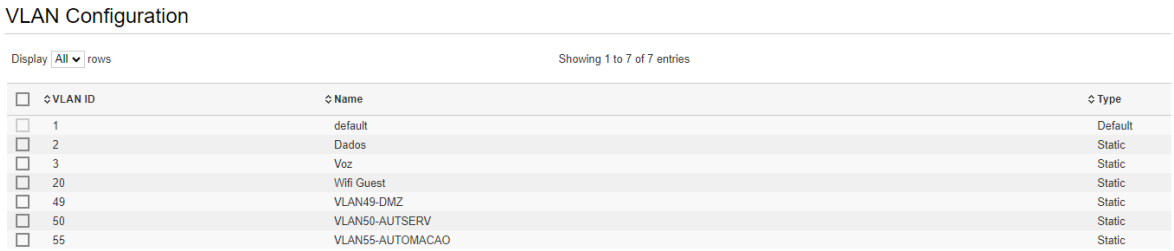
Figura 14 – Configuração de VLAN



Fonte:Própria (2023)

Após a criação das três VLANs, referentes as interfaces criadas no firewall, o Switch ficou com todas as VLANs inclusas, da mesma maneira que se encontra no firewall.

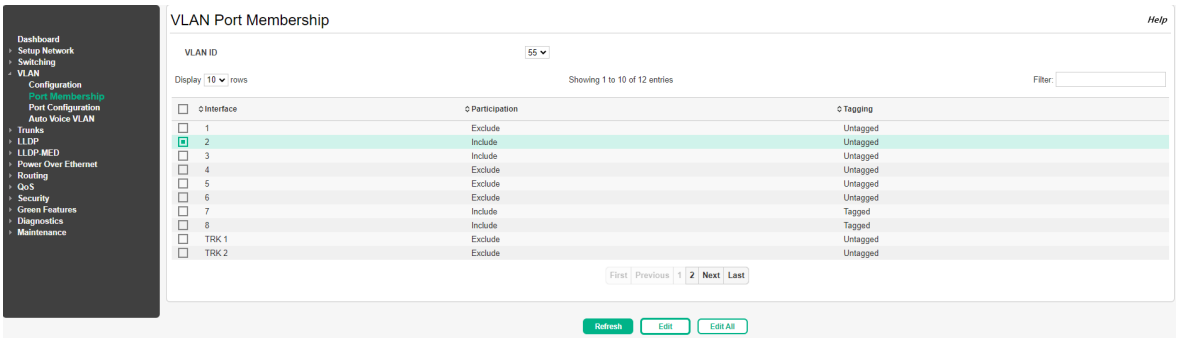
Figura 15 – Configuração de VLANs



Fonte:Própria (2023)

Depois de incluídas nas configurações do Switch, foi necessário realizar a distribuição das VLANs em cada porta necessária. para isso foi preciso acessar a aba de VLAN>Port Membership, e incluí-las nas portas necessárias.

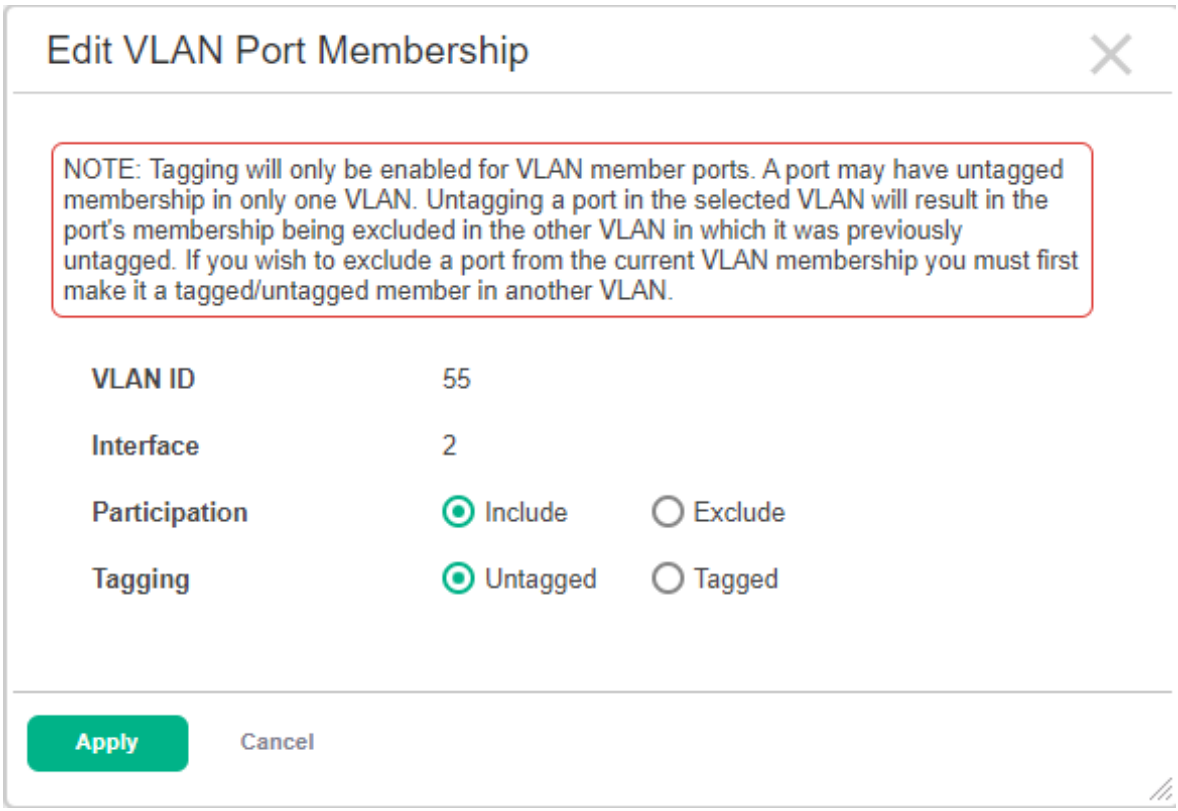
Figura 16 – Configuração de VLANs por portas



Fonte:Própria (2023)

Selecionando a porta em que deve possuir a configuração da VLAN, e adicionando-a.

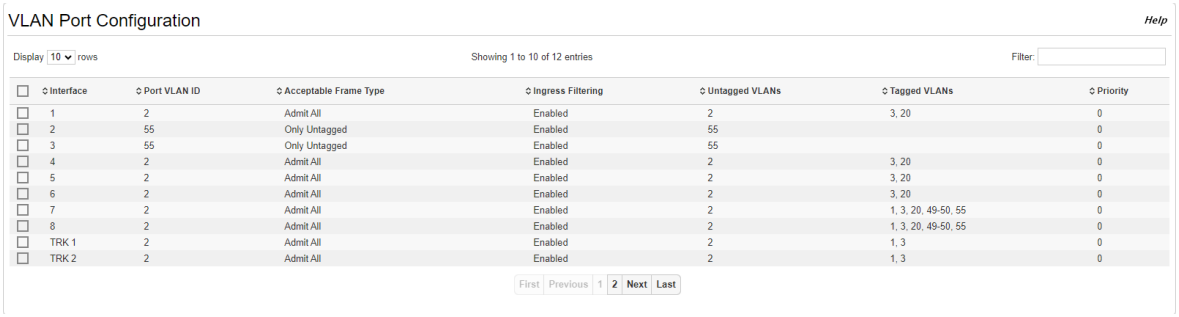
Figura 17 – Aplicando a VLAN as portas



Fonte:Própria (2023)

Por fim, após aplicação das VLANs nas portas necessárias, pode-se confirmar a configuração das portas, voltando ao painel de navegação do switch, e selecionar o caminho VLAN>Port Configuration, configuração final das portas indicadas na Figura 14.

Figura 18 – Configuração final das portas do Switch



Fonte:Própria (2023)

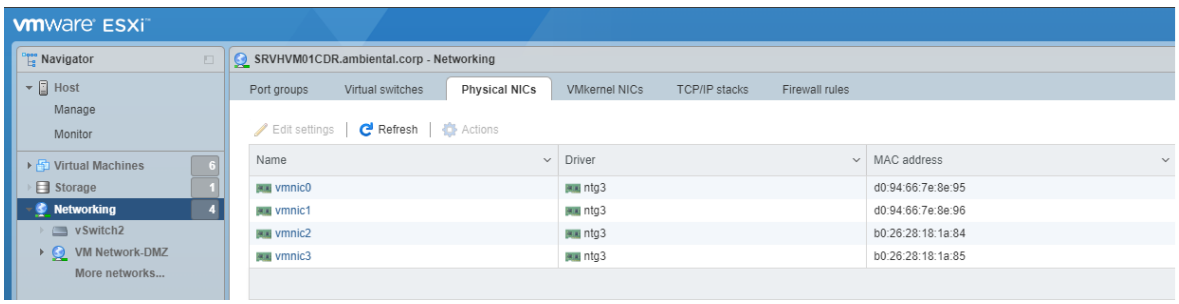
3.4 Configuração das novas camadas de redes no Servidor VMware

Seguindo para o terceiro passo de configuração das novas interfaces de rede, as mesmas serão configuradas também no servidor de virtualização do VMwhere ESXI 7.03, ele é o sistema operacional, onde ficarão alocadas as VMs que faram uso, dessas novas redes.

3.4.1 Configuran rede e vlans

O primeiro passo na instação de qualquer nova rede no VMware, é conferir e ter a certeza, de qual porta física do seu servidor será utilizada nessa conexão, nesse caso a Figura 18, mostra quais portas possuem no servidor fisíco, nessa demonstração, foi utilizada a porta com nome de vmnic3.

Figura 19 – Portas fisícas

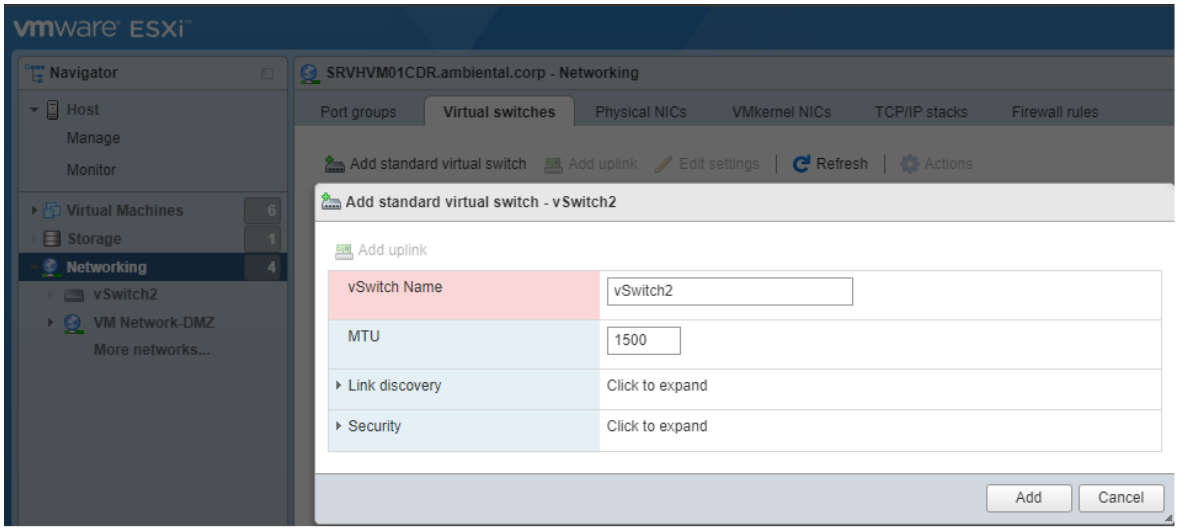


Fonte:Própria (2023)

3.4.2 Criando um virtual Switch

Depois de realizada a conferência de qual porta fisíca será utilizada para sequência da configuração, é necessária a criação de um virtual switch, ele serve para direcionamento da porta fisíca, que ficará vinculada a ele na configuração.

Figura 20 – Virtual Switch

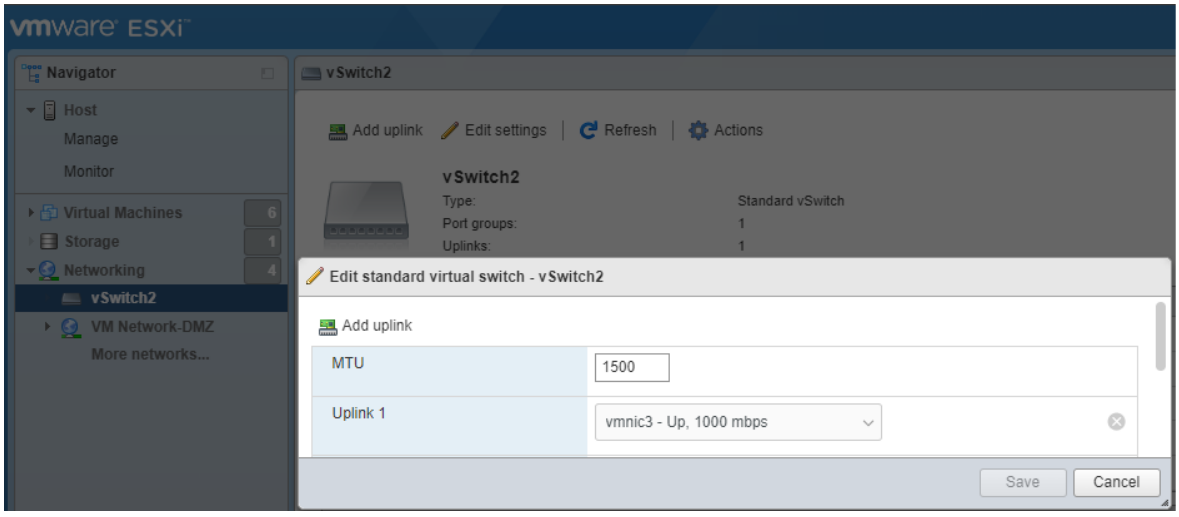


Fonte:Própria (2023)

3.4.3 Adicionando uma Vmnic ao Virtual Switch

Depois de criado o virtual Switch, foi vinculado a ele uma das portas físicas, que para essa implementação, foi a vmnic3, o virtual switch, não se limita a apenas uma placa de rede, pode-se vincular outras placas a um mesmo virtual switch, para esse projeto, foi adicionado apenas uma das portas.

Figura 21 – Adicionando uma vmnic ao Virtual Switch

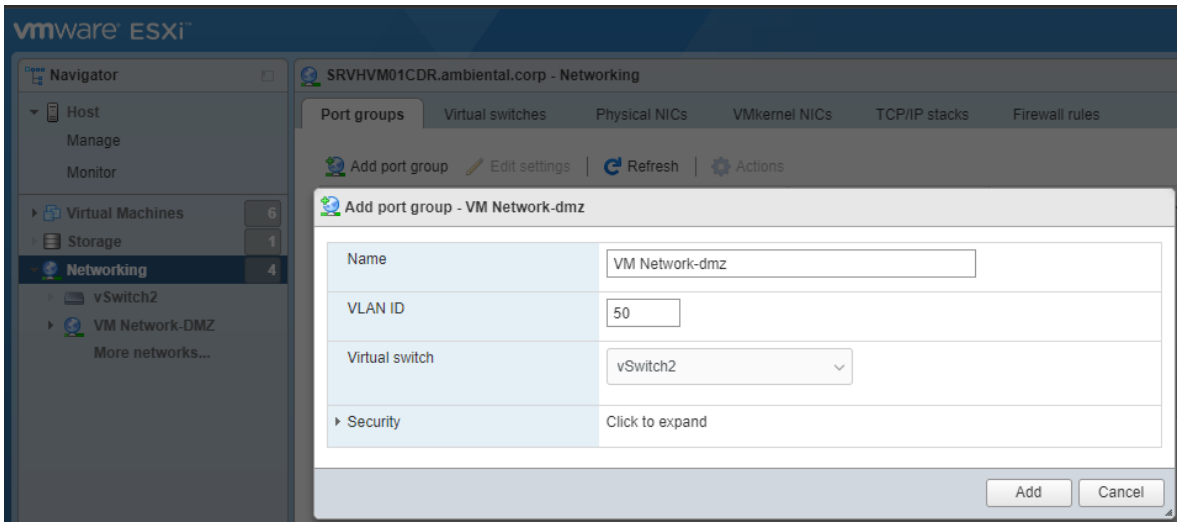


Fonte:Própria (2023)

3.4.4 Adicionando uma Port Group

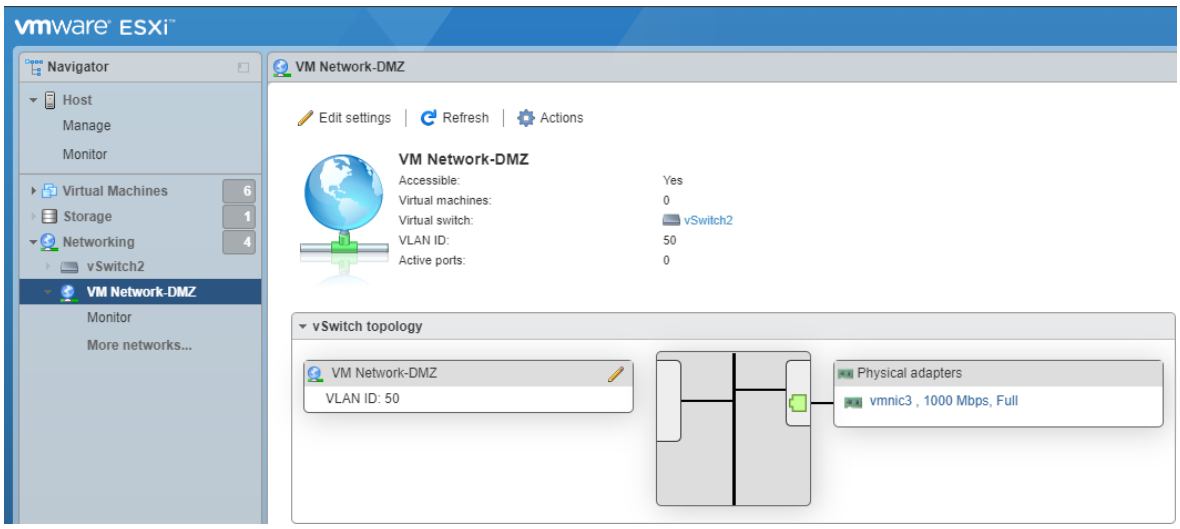
A port group(grupo de porta), é o local onde pode ser inserído as VLANs, que são necessárias para configuração do ambiente, para adicionar uma nova port group, é necessário que seja selecionado um dos virtual switch criados, e caso seja necessário também adicionar uma VLAN, na Figura 21, pode-se observar como ficou a configuração dessa port group.

Figura 22 – Adicionando uma Port Group



Fonte:Própria (2023)

Figura 23 – Port Group criada e configurada

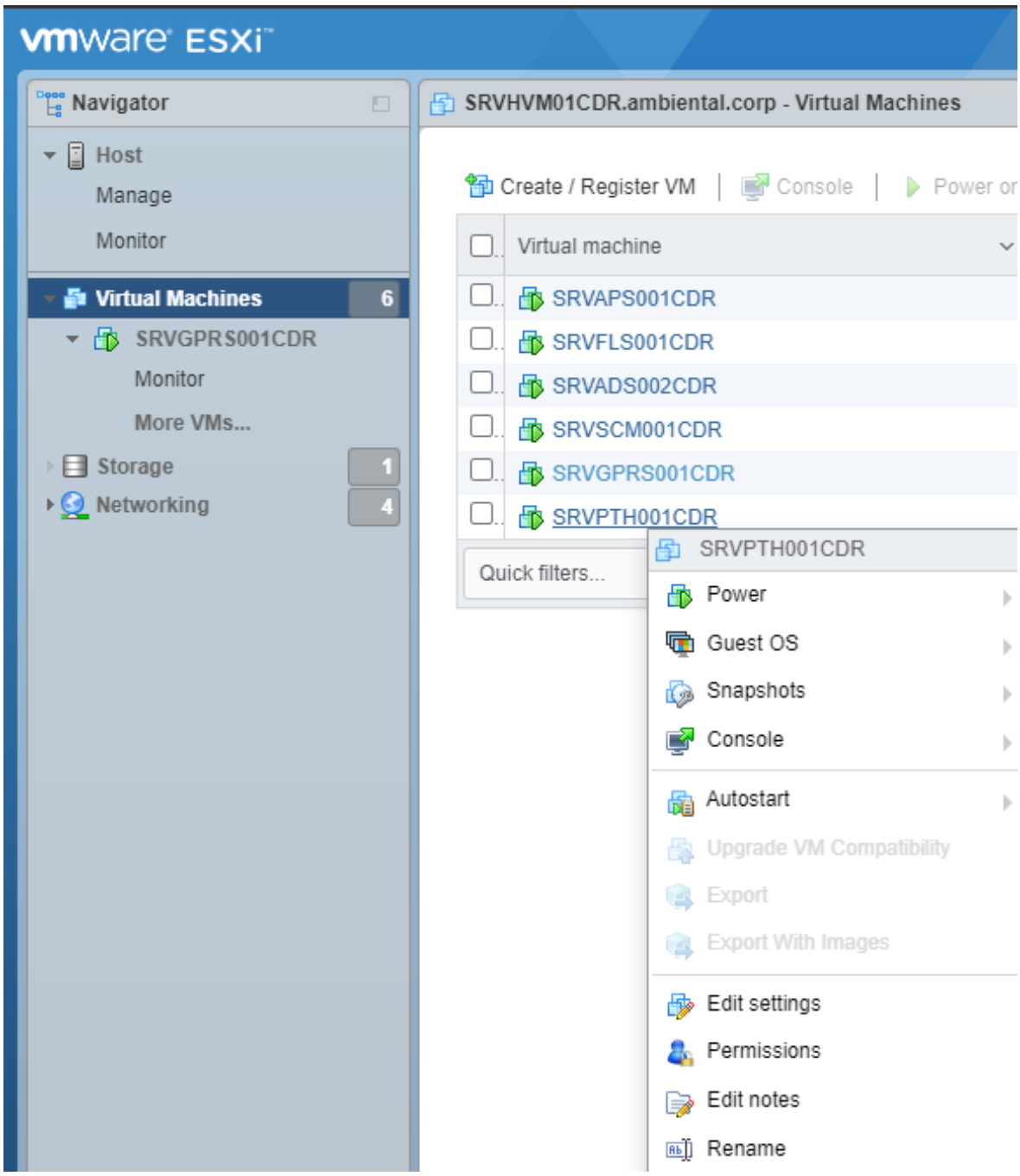


Fonte:Própria (2023)

3.4.5 Utilizando Port group em uma VM

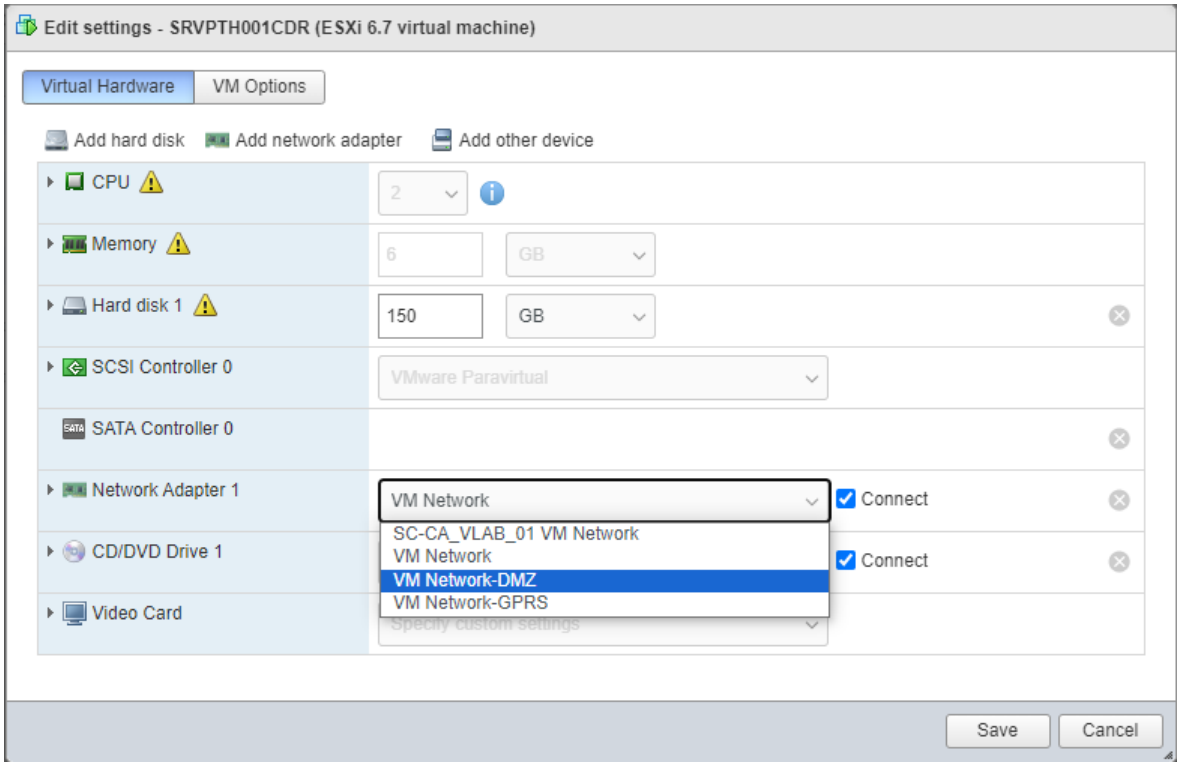
Depois que finalizar toda a criação da nova rede, ela fica disponível para uso. para adiciona-la a uma VM já criada, é necessário voltar a página de navegação do vmware, selecionar a opção virtual machines, aparecerá uma lista contendo todas as VMs criadas no vmware, para poder editar as configurações de uma delas, é necessário clicar com o botão direito em cima da VM desejada, e selecionar a opção edit settings(editar configuração), conforme a Figura 23.

Figura 24 – Utilizando Port group em uma VM



Fonte:Própria (2023)

Figura 25 – Lista de Port Groups para uso

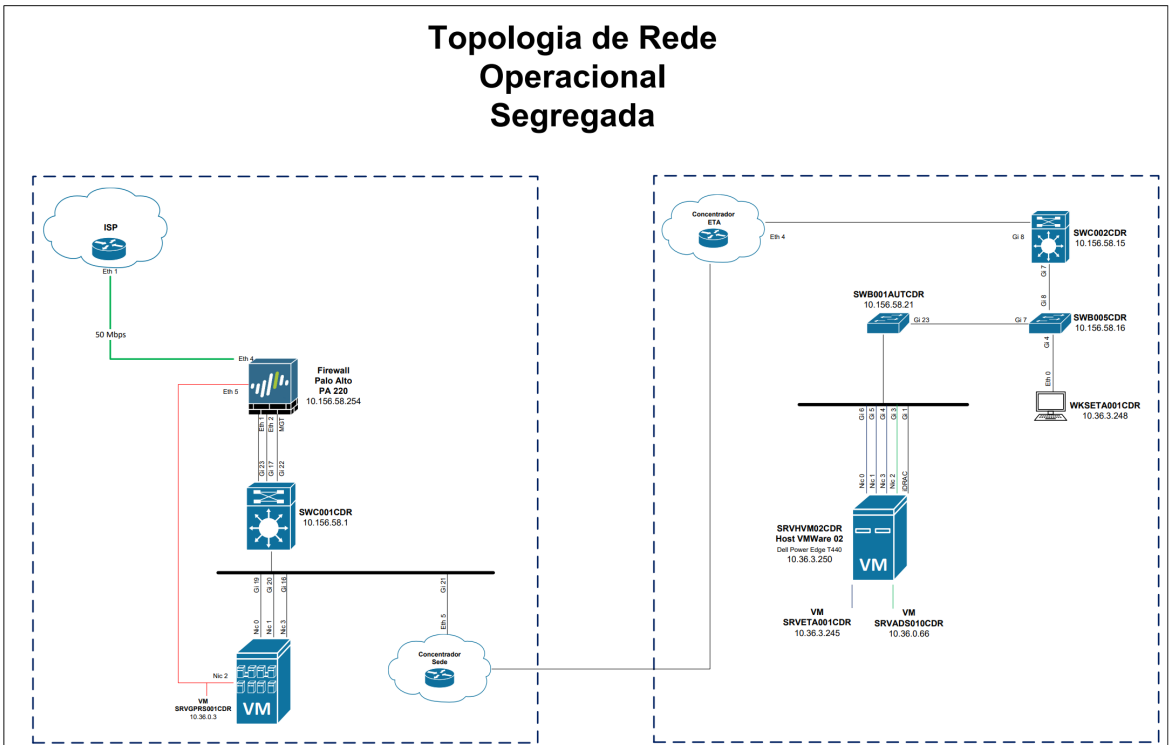


Fonte:Própria (2023)

3.5 Topologia de rede operacional segregada

Após a criação e configuração das novas interfaces, passando por todos os equipamentos necessários(firewall, switch, servidor virtualizado), foi criada a topologia lógica da rede operacional, utilizando o software visio da microsoft. deste modo, pode-se observar a topologia da rede operacional segregada na Figura 22, abaixo.

Figura 26 – Topologia de rede operacional segregada



Fonte:Própria (2023)

4 RESULTADOS E DISCUSSÕES

Neste trabalho de conclusão de curso, tem abaixo descrito, o resultado esperado, com base no levantamento de dados, levantando as maiores necessidades e ajustes para o sucesso da implementação do projeto final.

4.1 Detalhes dos resultados e discussões

A segurança da informação e das redes de operação é uma área vital na proteção de dados e sistemas críticos contra ameaças cibernéticas. Ambos os campos têm a importante tarefa de garantir a confidencialidade, integridade e disponibilidade das informações e sistemas essenciais para o funcionamento contínuo de uma organização.

A segregação de redes é essencial para fortalecer a postura de segurança cibernética de uma organização, proteger dados sensíveis e garantir a conformidade com regulamentações de privacidade e segurança de dados. É uma prática de segurança proativa que ajuda a minimizar os riscos e a proteger a infraestrutura de rede de potenciais ameaças e violações de segurança.

A implantação de uma rede operacional segregada, adiciona uma confiabilidade muito grande a área operacional, permitindo com que possíveis ataques, manutenções ou quedas de rendimento da rede administrativa, não gerem impacto para a operação. Após a implantação, a empresa experimentou melhorias significativas em sua eficiência operacional e segurança cibernética. A segregação das duas redes permitiu um controle mais preciso sobre o fluxo de dados e o acesso a recursos críticos, resultando em uma redução substancial na superfície de ataque e uma diminuição significativa no risco de violações de segurança.

Além disso, a separação das redes permitiu que os sistemas operacionais críticos funcionassem com mais eficiência e confiabilidade, minimizando as interrupções causadas por potenciais ameaças de segurança. Isso resultou em uma melhoria geral na produtividade e no desempenho, permitindo que a empresa se concentrasse em suas operações principais.

5 CONCLUSÃO

Realizar o trabalho de conclusão de curso é uma jornada repleta de desafios e recompensas gratificantes. Desde a seleção de um tema relevante e envolvente até a coleta e análise de dados, cada etapa do processo apresenta desafios únicos que exigem perseverança e dedicação. O enfrentamento de obstáculos como prazos apertados, aprofundamento de pesquisa e garantia de precisão metodológica pode testar os limites de um estudante, mas cada superação contribui para um crescimento pessoal e profissional significativo.

Ao implementar a segregação de redes, separando os ambientes de administração e operação da empresa, foi possível melhorar e identificar, pequenos detalhes, que antes da execução do trabalho, não foram encontrados, essa implementação resultou em ótimos resultados, elevando o nível de confiança das informações, e trazendo maior segurança operacional no dia a dia. Os diversos benefícios que essa implementação traz, torna ainda mais notável, o fato de que, esse assunto deve ser levado muito a sério, e ser implementado para todas as empresas e instituições de pequeno, médio e grande porte.

Ao estabelecer segmentos distintos e isolados dentro de uma infraestrutura de rede, as empresas podem reduzir significativamente a superfície de ataque, minimizando a propagação de ameaças e garantindo a proteção de dados confidenciais e sistemas críticos. Isso não apenas protege a integridade das operações, mas também fortalece a confiança dos clientes e parceiros na capacidade da empresa de proteger suas informações sensíveis.

Essa implementação ressalta a importância das empresas estarem constantemente concentradas em adotar novas tecnologias, seja por meio de softwares, equipamentos ou investimento em habilidades de equipe. A atualização tecnológica é crucial e pode ter um impacto significativo no cotidiano das empresas, diferenciando aquelas que a aplicam no mercado.

REFERÊNCIAS

ANDREW, T.; BOSS, H. *Sistemas Operacionais Modernos*. 4. ed. [S.l.]: Pearson Education do Brasil Ltda, 2016. 325-331 p. 25, 26

ARUBA NETWORKS. *O que é um switch de rede?* 2023. Disponível em: https://www.arubanetworks.com/br/faq/o-que-e-um-switch-de-rede/#:~:text=Um%20switch%20de%20rede%20(geralmente,para%20o%20dispositivo%20de%20destino. Acesso em: 05 october 2023. 22, 23

CITRIX SYSTEMS, INC. *5 formas que o Citrix Workspace coloca a experiência dosusuários em primeirolugar*. 2023. Disponível em: https://www.citrix.com/content/dam/citrix/pt-br/documents/ebook/5-ways-citrix-workspace-puts-user-experience-first.pdf. Acesso em: 12 may 2023. 28

CONTROLE NET TECNOLOGIA. *O que é rede de computadores?* 2023. Disponível em: https://www.controle.net/faq/rede-de-computadores. Acesso em: 28 june 2023. 12

EXAME. *5 problemas de segurança que podem ser resolvidos com tecnologia*. 2023. Disponível em: https://exame.com/tecnologia/5-problemas-de-seguranca-que-podem-ser-resolvidos-com-tecnologia/. Acesso em: 28 june 2023. 12

FIBERMALL. *VLAN: O que é e como funciona?* 2023. Disponível em: https://www.fibermall.com/pt/blog/what-is-vlan-and-how-it-work.htm. 25

KUROSE, J.; ROSS. ***Redes de Computadores e a Internet: uma abordagem top-down***. 6. ed. [S.l.]: Pearson Education do Brasil Ltda, 2013. 330-336 p. 16, 18, 19, 20, 21

ORACLE VM VIRTUALBOX. *Oracle VM VirtualBox*. 2023. Disponível em: https://www.virtualbox.org. Acesso em: 10 may 2023. 27

RODRIGO, SILVA. *APLICAÇÃO DE UMA METODOLOGIA PARA SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES COM A UTILIZAÇÃO DE SOFTWARE LIVRE COM BASE NA NBR ISO/IEC 27002:2005: ESTUDO DE CASO EM UMA EMPRESA DE MEDIO PORTE DA REGIÃO DE CARATINGA*. 2023. Disponível em: https://dspace.doctum.edu.br/handle/123456789/843. Acesso em: 02 may 2023. 18

TECNOBLOG. *O que é uma VLAN?* 2023. Disponível em: https://tecnoblog.net/responde/o-que-e-vlan/. Acesso em: 10 october 2023. 24

THIOLLENT, M. *Metodologia de Pesquisa-ação*. [S.l.]: São Paulo: Saraiva, 2009. 39 p. 30

VMWARE, INC. *VMware ESXI*. 2023. Disponível em: https://www.vmware.com/br/products/esxi-and-esx.html. Acesso em: 15 may 2023. 29

APÊNDICES

ANEXOS