Faculdade de Tecnologia de Americana
Curso de Processamento de dados

PROVIMENTO DE UMA REDE DESMILITARIZADA (DMZ)

PAULO SERGIO ROSSETO

Americana, SP
2011

Faculdade de Tecnologia de Americana
Curso de Processamento de dados

PROVIMENTO DE UMA REDE DESMILITARIZADA (DMZ)

PAULO SERGIO ROSSETO

paulo.rosseto@hotmail.com

Estágio em Análise e Projetos de sistemas – ESTANAL, desenvolvido em cumprimento à exigência curricular do Curso de Processamento de Dados da Faculdade de Tecnologia de Americana, sob orientação do Prof. Dr. José Luiz Zem.

Área: Informática

Americana, SP
2011

BANCA EXAMINADORA

Prof. Dr. José Luiz Zem (Orientador)

Prof. Antonio Alfredo Lacerda (Presidente da Banca)

Prof. Rogério Nunes de Freitas (Convidado)

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida.

A minha esposa Rosana e a minha filha Maria Paula, pelo apoio e compreensão, e ao meu orientador José Luiz Zem, pelo apoio, sugestões e acompanhamento na elaboração deste trabalho, sem os quais a conclusão deste não seria possível.

DEDICATÓRIA

Dedico este trabalho a minha esposa Rosana e a minha filha Maria Paula, que sempre apoiaram, ajudaram e me incentivaram nos momentos em que mais precisei.

RESUMO

Este trabalho tem o propósito de demonstrar sobre a importância de uma rede desmilitarizada, a fim de garantir proteção as redes internas de uma empresa ou corporação, para tanto foi realizado um levantamento bibliográfico sobre as redes de computadores, os serviços de rede (web, FTP, e-mail), firewall e a própria DMZ (zona desmilitarizada), efetuado testes confrontando os resultados.

Palavras Chave: demonstrar, rede desmilitarizada, redes internas

ABSTRACT

This work aims to demonstrate the importance of a network demilitarized in order to ensure protection of the internal networks of a company or corporation, for that was based on a literature on computer networks, network services (web, FTP , e-mail), and their own firewall DMZ (demilitarized zone), conducted tests comparing the results.

Keywords: show, demilitarized networks, intranets.

SUMÁRIO

LISTA DE FIGURAS....9

LISTA DE ABREVIATURAS E SIGLAS....10

1 INTRODUÇÃO....11

1.1 OBJETIVOS....11

1.2 JUSTIFICATIVAS....12

1.3 METODOLOGIA....12

2 LEVANTAMENTO BIBLIOGRÁFICO....14

2.1 REDES DE COMPUTADORES....14

2.2 SERVIÇOS DE REDE....15

2.2.1 WEB....16

2.2.2 FTP....17

2.2.3 E-MAIL....18

2.3 FIREWALL....19

2.4 DMZ (Zona Desmilitarizada)....21

3 DESENVOLVIMENTO....24

3.1 TESTES....27

4 CONCLUSÃO....32

5 REFERÊNCIAS BIBLIOGRÁFICAS....33

LISTA DE FIGURAS

Figura 01: Cronograma de trabalho.....13
Figura 02: Sub sistema de comunicação. 14
Figura 03: Sessão FTP.....17
Figura 04: Conexões de controle e dados.....18
Figura 05: Rede DMZ.....22
Figura 06: Rede desmilitarizada.....23
Figura 07: Cenário 01 Sistema de rede típico.....24
Figura 08: Fluxo de comunicação no cenário 01.....25
Figura 09: Cenário 02 Sistema de rede com DMZ.....26
Figura 10: Fluxo de comunicação no cenário 02.....26
Figura 11: Maquina Virtual.....27
Figura 12: Estação interna.....28
Figura 13: Servidor web recebendo pacotes da estação interna.....28
Figura 14: Tráfego da estação.....29
Figura 15: Estação enviando ping.....30
Figura 16: Servidor web recebendo pacotes da estação.....30
Figura 17: Estação interna.....31

LISTA DE ABREVIATURAS E SIGLAS

Web – World Wide Web, sistema de documentos em hipermídia que são interligados e executados na Internet

Ping - é um comando para testar a conectividade entre equipamentos.

LANs - local area network (rede de área local)

WANs - wide area network(rede de longa distância)

DMZ - DeMilitarized Zone (zona desmilitarizada)

FTP - File Transfer Protocol (Protocolo de Transferência de Arquivos)

TCP - Transmission Control Protocol

SMTP - Simple Mail Transfer Protocol

HTTP - Hypertext Transfer Protocol(Protocolo de Transferência de Hipertexto)

1 INTRODUÇÃO

No presente momento, milhões de computadores estão conectados a uma enorme rede de comunicação, espalhados por todo planeta e trocando um grande volume de informações, grande parte delas sem valor algum, e uma boa quantidade, potencialmente perigosa, circulando livremente. Com o crescimento da Internet e do acesso remoto, revelando-se como as grandes portas de entrada e saída, os sistemas ficaram vulneráveis à ataques. Pensando nisso, o uso de firewall e de redes DMZ na interligação entre LANs e WANs tornou-se frequente na proteção de acesso aos servidores, com a separação da rede interna da externa, desempenhando seus papéis de proteção, quando bem configurados.

Todos os requisitos para segurança de uma rede de computadores implicam em que um recurso (seja informação, equipamento, ou outros) somente poderá ser utilizado por quem possua efetivamente o direito de acesso e a maneira prevista. Assim evita-se que uma pessoa não autorizada, sob nenhuma hipótese, possa ter acesso a uma informação à qual ela não tenha direito. Fora isto, é necessário garantir a integridade dos recursos da rede, de modo a impedir danos e minimizar eventuais desastres que possam acontecer. Para tal, é necessário à adoção de regras de segurança.

1.1 OBJETIVOS

Este estudo tem como principal objetivo demonstrar a importância da segurança da rede em uma organização, provendo informações sobre como posicionar uma rede desmilitarizada e evitar por em risco as informações corporativas, utilizando-se de recursos disponíveis com segurança e controle.

Como objetivos secundários tem-se a aquisição de novos conhecimentos, explorar um ambiente de virtualização, para demonstrar uma rede de computadores, através da utilização do software virtualbox, visualizando o processo de

transferência de pacotes em uma rede de computadores, através de simulação, neste caso empregando o software Packet Tracer.

1.2 JUSTIFICATIVAS

Os sistemas corporativos são alvos de constantes ameaças, na mesma proporção que ocorre o crescimento no número de usuários.

A segurança na e da rede é uma preocupação frequente, tendo o desafio de sempre se manter atualizada, explorando os recursos disponíveis para evitar ataques e prejuízos.

Os ataques que produzem grandes problemas para as organizações são aqueles ocorridos a partir da sua própria rede (ataques internos), proveniente de qualquer ponto da rede da organização; a proteção deve ocorrer não somente contra os ataques vindos da rede externa, mas também contra aqueles que podem ser considerados internos.

1.3 METODOLOGIA

A metodologia a ser utilizada consistiu em dividir o estudo em uma série de etapas (mostradas na Figura 01) e consiste no (1) levantamento bibliográfico com ênfase em redes de computadores, serviços de rede, WEB, FTP, firewall e rede DMZ, no (2) desenvolvimento do estudo através de dois cenários e (3) a discussão comparando-se os resultados dos cenários testados. (projeto e implantação, através do packet tracer e virtualbox, respectivamente)

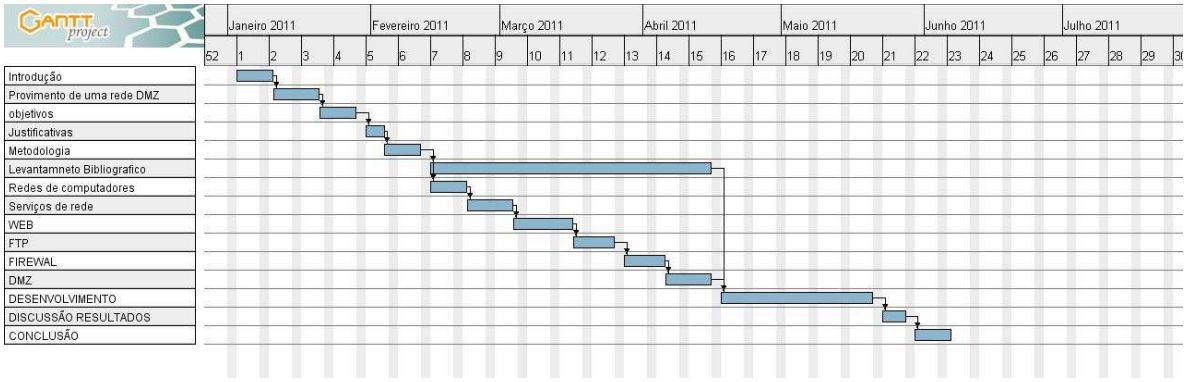

Figura 01: Cronograma de trabalho.

As etapas necessárias para o desenvolvimento do estudo são:

Levantamento Bibliográfico: realizado através de pesquisas em livros de redes de computadores, livros de sistemas operacionais, monografias e internet, com duração total de 45 dias.

Redes de computadores: elaborado através de rede de pesquisas em livros, sobre redes de computadores, com duração de 6 dias.

Serviços de rede: realizado com embasamento nos livros de redes de computadores, com duração de 8 dias.

WEB: realizado através de pesquisas em livros de redes de computadores, livros de sistemas operacionais, com duração de 9 dias.

FTP: elaborado através de pesquisas em livros de redes de computadores, livros de sistemas operacionais, com duração de 7 dias.

FIREWAL: eladorado através de pesquisas em livros de redes de computadores, livros de sistemas operacionais, com duração de 7 dias.

DMZ: realizado através de pesquisas em livros de redes de computadores, livros de sistemas operacionais, com duração de 8 dias.

Desenvolvimento: realizado através do software virtual Box e Packet Tracer, simulando em dois ambientes, cenário 1 e cenário 2, com duração de 25 dias.

2 LEVANTAMENTO BIBLIOGRÁFICO

O levantamento aqui apresentado aborda questões relativas a redes de computadores, serviços de redes, WEB, FTP, firewall e a rede DMZ (desmilitarizada).

2.1 REDES DE COMPUTADORES

Uma rede de computadores tem como objetivos básicos prover a comunicação confiável entre os vários sistemas de informação, melhorar o fluxo e o acesso às informações, bem como agilizar a tomada de decisões administrativas facilitando a comunicação entre seus usuários, [TANENBAUM, 2003].

Uma rede de computadores é formada por um conjunto de módulos processadores (MPs) capazes de trocar informações e compartilhar recursos, interligados por um sub-sistema de comunicação,[Zem, 2011].

Já o sub-sistema de comunicação, como mostra a Figura 02, irá constituir-se de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com a finalidade de organizar a comunicação (protocolos), [Zem, 2011].

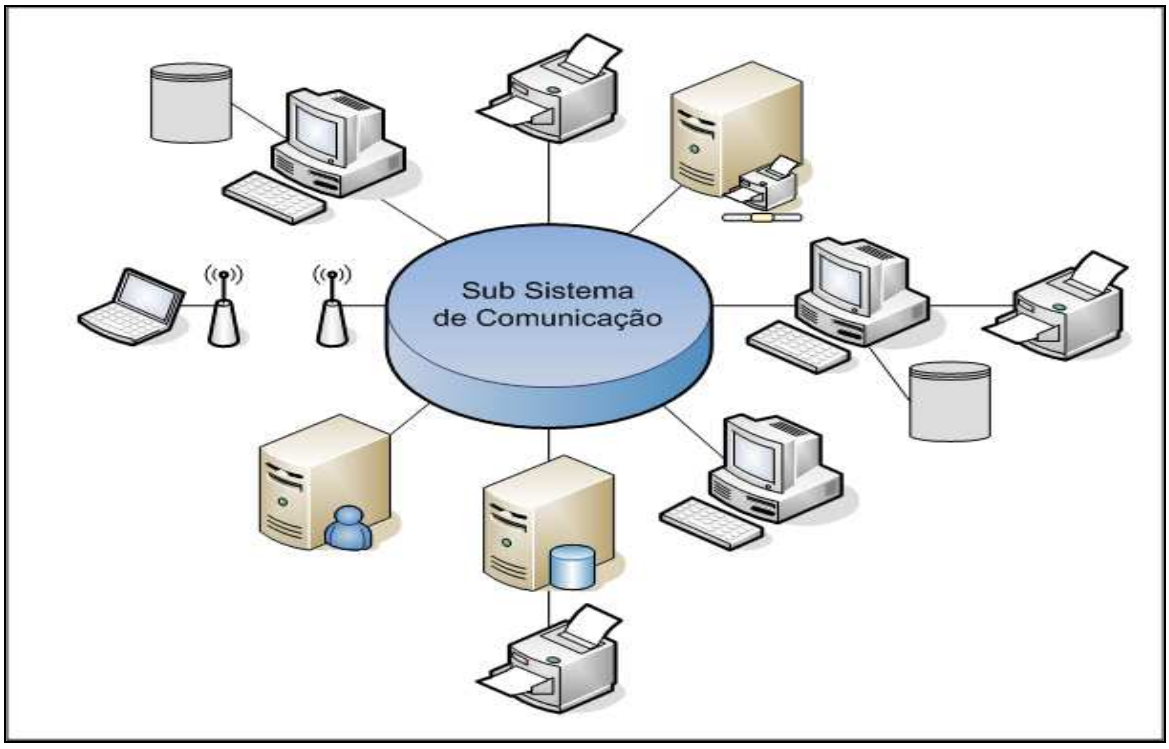

Figura 02: Sub sistema de comunicação.

As redes locais surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo.

Segundo TANENBAUM (1994).“Objetivo é a redução de custo, uma vez que computadores de pequeno porte, os mais utilizados atualmente na construção de modelos de redes, têm uma relação custo/desempenho muito melhor do que os computadores de grande porte. Isto se explica pelo fato de que um mainframe, apesar de ser aproximadamente dez vezes mais rápido do que o mais rápido microprocessador de um chip custa muitas vezes mais. Esse desequilíbrio levou muitos projetistas de sistemas a construírem redes constituídas de computadores pessoais potentes, havendo um por usuário, com os dados guardados em uma ou mais máquinas servidoras de arquivos. Esse último objetivo leva à existência de redes com muitos computadores localizados em um mesmo prédio, sendo esse tipo de estrutura conhecida como rede local”.

2.2 SERVIÇOS DE REDE

A rede mundial de computadores surgiu de um sistema chamado Arpanet, criado em 1969, nos Estados Unidos. Os projetistas que a desenvolveram trabalharam para criar uma rede de comunicações sem coordenação central, para assim, superar o tradicional ”modelo pirâmide”, isto é, modelo no qual diversos computadores trabalham ligados, necessariamente, a um único computador central. Pretendia–se evitar, desta forma, que uma eventual falha ou destruição do ponto central anulasse todo o sistema de comunicação. Num primeiro momento, foram interligados apenas quatro pontos, mas as conexões cresceram rapidamente, principalmente nos meios universitários, e, em 1981, quando começou a ser chamada de Internet, já era uma rede com cerca de duzentas unidades interligadas. Dessa época em diante, com o aparecimento dos microcomputadores e uma série de serviços relativamente baratos e fáceis de usar, a rede se expandiu.

2.2.1 WEB

A Web (também conhecida como WWW ou World Wide Web) é a estrutura arquitetônica que permite o acesso a documentos vinculados e espalhados por milhares de máquinas na Internet. Sua popularidade se deve à interface gráfica, que é de fácil utilização para principiantes e pelo oferecimento de uma imensa variedade de informações sobre quase todos os assuntos.

É um ambiente que permite publicar informações e disponibilizações para qualquer pessoa. A Web permite que seus usuários publiquem textos, imagens, sons e outros recursos de linguagem. Os ambientes criados com esses recursos são chamados ambientes multimídia e só surgiram depois de a Web ser criada, porque antes a Internet não comportava forma gráficas, apenas textos.

Tim Berners-Lee (o mentor e criador da WWW) teve a ideia de ligar a funcionalidade do hipertexto com a Internet e assim formar uma rede que ajudasse os físicos do Cern (Organização Europeia para Pesquisa Nuclear) a partilhar todas as informações armazenadas em computador nos laboratórios da instituição. Através de um sistema de hipertexto, desenvolvido por ele em 1988, os pesquisadores acessavam mundialmente os resultados dos colegas.

O impulso decisivo, só viria após o Cern abrir a Web ao público e renunciar ao pagamento de licenças ou a um patenteamento da invenção de Tim Berners-Lee. O triunfo da rede, porém, aconteceu fora do Cern.

Para que novos ambientes multimídia pudessem ser facilmente utilizados , criou–se em 1993, o programa Mosaic, que se tornou conhecido como “navegador”; atualmente os navegadores mais conhecidos são Internet Explorer e o Mozilla Firefox.

O navegador permitiu “unir” a Internet e a Web e ampliou o uso da rede que, até aquele momento, era utilizada quase exclusivamente por universidades e empresas.

O navegador levou a Internet e a Web à uma imensa quantidade de usuários, pois tornou possível que cada usuário usasse seu computador pessoal, instalado em casa. Em outras palavras, o navegador transformou a Internet no poderoso instrumento de comunicação que conhecemos hoje.

A Internet representa tanto uma coleção de comunidades como uma coleção de tecnologias, e seu sucesso é amplamente atribuído à satisfação das

necessidades básicas da comunidade e à utilização efetiva da comunidade na expansão da sua infra-estrutura.

2.2.2 FTP

A sigla **FTP** significa *File Transfer Protocol* (Protocolo de Transferência de Arquivos) e é uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na Internet. O protocolo FTP oferece muitos recursos além da função de transferência propriamente dita.

Embora o FTP seja projetado para ser usado por programas, a maioria das operações também fornece uma interface interativa que permite às pessoas interagirem com servidores remotos.

O FTP permite que o cliente especifique o tipo e a representação dos dados armazenados, exige que os clientes se autorizem através de um nome de *login* e uma senha para com o servidor antes de requisitar transferência do arquivo. O servidor recusa acesso à clientes que não forneça um *login* e senha válidos.

Em uma sessão FTP típica Figura 03, o usuário, de um hospedeiro (o local), deseja transferir arquivos de, ou para, um hospedeiro remoto. Para acessar sua conta remota, ele deve fornecer uma identificação e uma senha, sendo que após essas informações de autorização, pode transferir livremente arquivos do sistema local de arquivos para o sistema remoto e vice-versa.

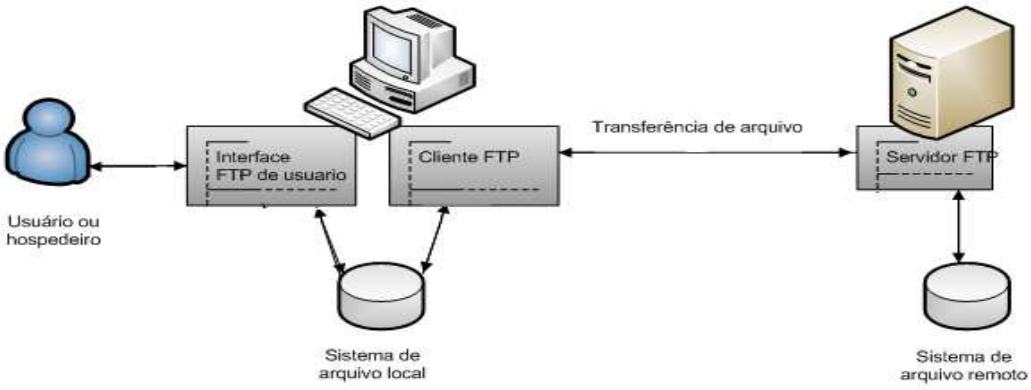

Figura 03: Sessão FTP

O FTP usa duas conexões TCP (Transmission Control Protocol) paralelas para transferir um arquivo, uma conexão de controle e uma conexão de dados. A

primeira é usada para enviar informação de controle entre os dois hospedeiros, como identificação de usuário, senha, comandos para manipular arquivos e diretórios. Já conexão de dados é usada para efetivamente enviar ou receber os conteúdos dos arquivos. Como o FTP usa uma conexão de controle separada, diz-se que ele envia suas informações de controle “fora da banda”. As conexões de controle e dados do FTP estão ilustradas na Figura 04.

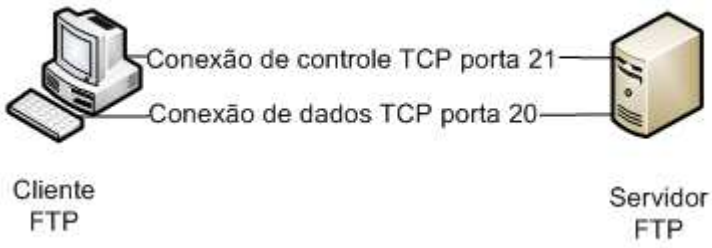

Figura 04: Conexões de controle e dados

As conexões e os processos de transferência de dados que as utilizam são criados dinamicamente, quando necessário, mas a conexão de controle persiste durante toda uma sessão. Uma vez que a conexão de controle termina, a sessão é encerrada e o software em ambos os lados encerram todos os processos de transferência de dados.

Além de transferir comandos do usuário para o servidor, o FTP usa conexão de controle para permitir que os processos de controle do cliente e do servidor coordenem o uso das portas do protocolo TCP dinamicamente atribuídas e a criação dos processos de transferencia de dados que usam essas portas.

2.2.3 E-MAIL

E-mail é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo e-mail é aplicado tanto aos sistemas que utilizam a Internet e são baseados no protocolo SMTP, como aqueles sistemas conhecidos como intranets, que permitem a troca de mensagens dentro de uma empresa ou organização e são, normalmente, baseados em protocolos proprietários.

O correio eletrônico tornou-se bastante popular devido a sua grande facilidade em cobrir grandes distâncias geográficas. Pessoas que estão em diferentes

continentes podem se comunicar, desde que possuam computadores ou qualquer outro dispositivo, com tal funcionalidade, conectados à Internet. Eles podem enviar e receber mensagens a qualquer hora e para qualquer parte do mundo.

Observa-se que o correio eletrônico deixa de ser apenas um meio de troca de mensagens entre pessoas para se tornar um grande fator na produtividade das empresas. Grandes empresas usam cada vez mais o correio eletrônico para desempenhar papéis decisivos em suas decisões. Já a intranet pode ser usada para tornar a comunicação de funcionários com outros grupos mais fácil e rapida, eliminando o envio de mensagens em massa e outras indesejadas.

As aplicações de correio eletrônico normalmente oferecem ao usuário uma série de facilidades. A maior parte delas fornece um editor de textos embutido e a possibilidade do envio de arquivos anexados a correspondência. Além disso, a maioria das aplicações permite o envio de correspondências para um único destinatário ou para mais de uma pessoa, ou ainda para um grupo selecionado de pessoas.

Embora não tenha sido desenvolvida como uma ferramenta de trabalho cooperativo, os serviços de correio eletrônico adaptaram-se muito bem ao ambiente de grupos de trabalho onde se tornaram indispensáveis nas organizações, agilizando processos, democratizando o acesso as informações e diminuindo os custos. Esta é uma das formas mais usadas para o estabelecimento de comunicações por computador.

2.3 FIREWALL

Firewall nada mais é do que uma ferramenta que trabalha como mecanismo de proteção entre redes, liberando ou bloqueando a comunicação.

Especificamente, o *firewall* é uma ferramenta que age em "defesa" dos computadores e das redes de computadores, controlando os acessos ao sistema por meio de regras e a filtragem de dados. Em redes de computadores os administradores tem como vantagem, uma maior proteção contra invasões e, além disso, eles não necessitam instalá-lo em cada máquina, apesar de ser possível, mas apenas em um, aquele que servirá toda rede.

Firewall é uma das ferramentas mais importantes quando se fala em segurança de computadores. O uso de informações e sistemas é cada vez maior, e sua proteção requer a aplicação de ferramentas e conceitos de segurança eficientes. Atualmente o *firewall* é uma ferramenta necessária para qualquer computador, independente do seu uso ou tipo de trabalho.

O *firewall* tem como objetivo conceder acesso a dados e conteúdos autorizado. Ele é resultante de junção de *hardware* e *software*, porém no ambiente doméstico geralmente é implementado por software.

O funcionamento do *firewall* irá depender da ferramenta, aplicação e programador. Existem dois tipos de *firewall*, o de filtragem de pacotes e o de controle de aplicações. Não é possível compará-los para se saber qual o melhor, uma vez que cada um é destinado para um determinado fim, tornando a comparação não aplicável.

A filtragem de pacotes é bastante usada em redes pequenas, ou de porte médio. Através de algumas regras estabelecidas, esse tipo de firewall determina quais endereços e dados podem estabelecer comunicação e/ou transmitir/receber dados. Diversos serviços podem ser liberados por completo e outros já são bloqueados por padrão, por oferecerem maior riscos (como softwares de mensangens instantâneas). O maior problema desse tipo de *firewall*, é que as regras utilizadas podem ser muito complexas e causar queda no desempenho da rede ou então não serem eficazes o suficiente.

Este tipo de *firewall* restringe-se a atuar nas camadas do TCP/IP, decidindo quais pacotes de dados podem passar ou não por ele. Essas escolhas são feitas a partir de regras baseadas nas informações do endereço IP remoto, além da porta usada. Quando configurado corretamente, esse tipo de *firewall* permite que somente "computadores conhecidos troquem determinadas informações entre si e tenham acesso a determinados recursos".

Este tipo de *firewall*, também é capaz de avaliar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível.

Já os *firewalls* de aplicação geralmente são instalados nos computadores servidores e são conhecidos como “*Proxy*”. Este tipo não permite comunicação direta entre a rede e a Internet, mas tudo deve passar por ele, que atua como um

intermediador. O *proxy* efetua a comunicação de ambos lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de firewall é bem mais complexo, porém bastante seguro, pois todas as aplicações necessitam passar *proxy*. Caso isso não ocorra, a aplicação simplesmente não funciona.

O *firewall* de aplicação permite o acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre uma rede e outra rede). Sendo possível, inclusive, contar com recursos de registro em log e ferramentas de auditoria. Tais características deixam claro que este tipo de *firewall* é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

Abaixo são apresentadas três boas razões [InfoWester, 2004] para se usar um firewall:

1 - Auxiliar a bloquear sua rede ou seu computador para que não seja acessado sem autorização. Sendo assim, é possível evitar que informações sejam liberadas ou que sistemas tenham seu funcionamento prejudicado por ação de hackers;

2 - É um dos maiores aliados no combate à vírus e cavalos-de-tróia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso à programas não autorizados;

3 - Nas redes corporativas, é possível evitar que usuários utilizem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram.

Infelizmente, os firewalls não são uma cura definitiva para os males de segurança na Internet. Existem diversas tarefas que os firewalls não realizam, tais como a garantir a integridade dos dados, ou a autenticidade da origem dos dados, nem o sigilo dos mesmos, também não garantem proteção contra ameaças internas.

2.4 DMZ (Zona Desmilitarizada)

DMZ, em segurança da informação, é uma sigla para de *DeMilitarized Zone* ou "zona desmilitarizada", em português. Também conhecida como Rede de Perímetro, a DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet como mostra a Figura 05.

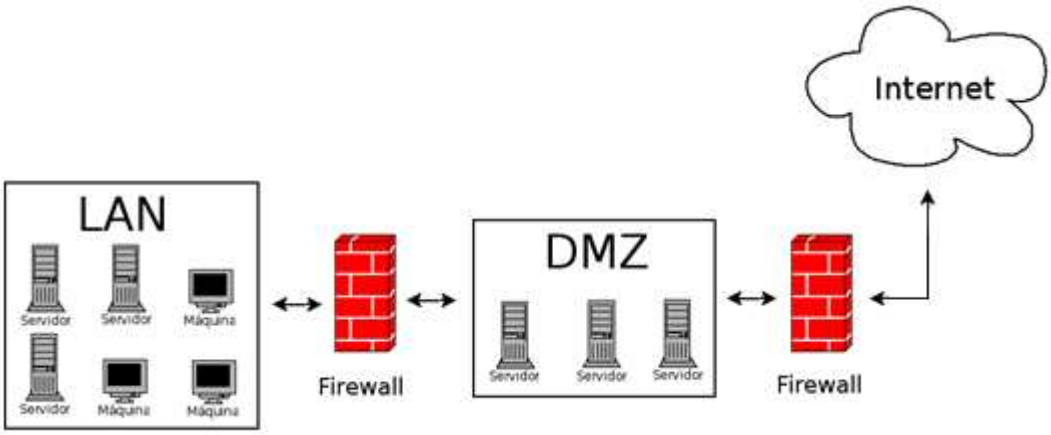

Figura 05: Rede DMZ

A função de uma DMZ é manter todos os serviços que possuem ou permitem acesso externo (tais como servidores HTTP, FTP, de correio eletrônico, etc.) separados da rede local, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um invasor. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter nenhuma forma de acesso à rede local.

A configuração é realizada através do uso de equipamentos de *firewall*, que realizarão o controle de acesso entre a rede local, a Internet e a DMZ (ou, em um modelo genérico, entre as duas redes a serem separadas e a DMZ). Os equipamentos na DMZ podem estar em um segmento de rede dedicado ou compartilhar um segmento único da rede, porém neste último caso devem ser configuradas redes virtuais distintas dentro do equipamento, também chamadas de VLANs (ou seja, redes diferentes que não se "enxergam" dentro de uma mesma rede física).

A DMZ pode ser um segmento ou segmentos de rede, parcialmente protegida, que está entre uma rede protegida e uma desprotegida e que contém serviços e informações. Nela podem existir regras de acesso específico e sistemas de defesa de perímetro simulando uma rede protegida para induzir os possíveis invasores para armadilhas virtuais, assim tentando localizar a origem do ataque. A Figura 06 representa uma DMZ.

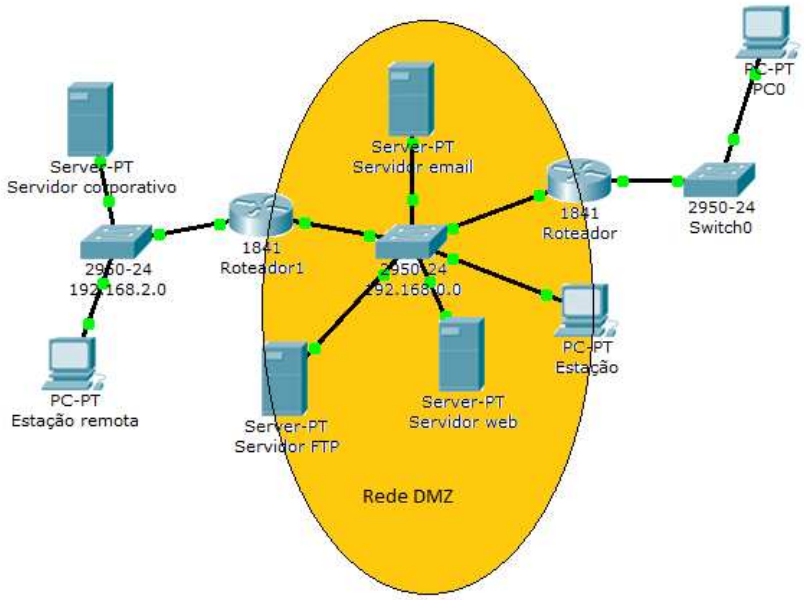

Figura 06: Rede desmilitarizada

3 DESENVOLVIMENTO

Atualmente as empresas e organizações tem um sistema típico de redes de computadores, com uma configuração onde a rede externa tem acesso a rede interna ficando, assim exposta à ataques com grande potencial de danos ao sistema.

A idéia do trabalho é implementar uma rede desmilitarizada para que os computadores da rede externa não acesse a rede interna.

O desenvolvimento foi realizado no ambiente virtual através dos softwares Virtualbox e Packet Tracer. Foram implementados dois cenários sendo em um deles caracterizando o sistema típico das empresas, como é possível observar na Figura 07.

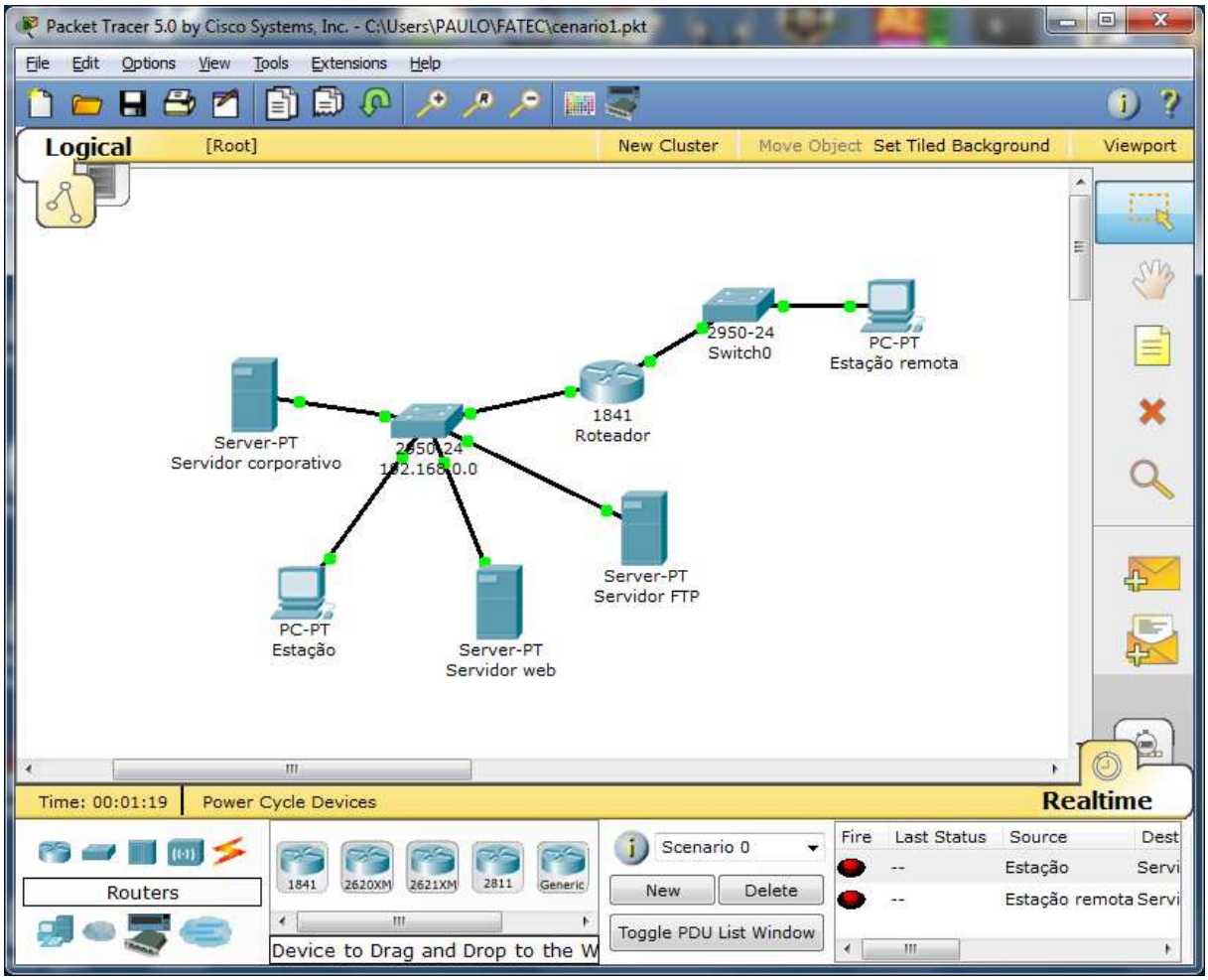

Figura 07: Cenário 01 Sistema de rede típico.

O potencial de risco pode ser observado na Figura 08 onde os pacotes destinados aos servidores tem acesso à rede interna, deixando a rede interna vulnerável ao ataque de um invasor.

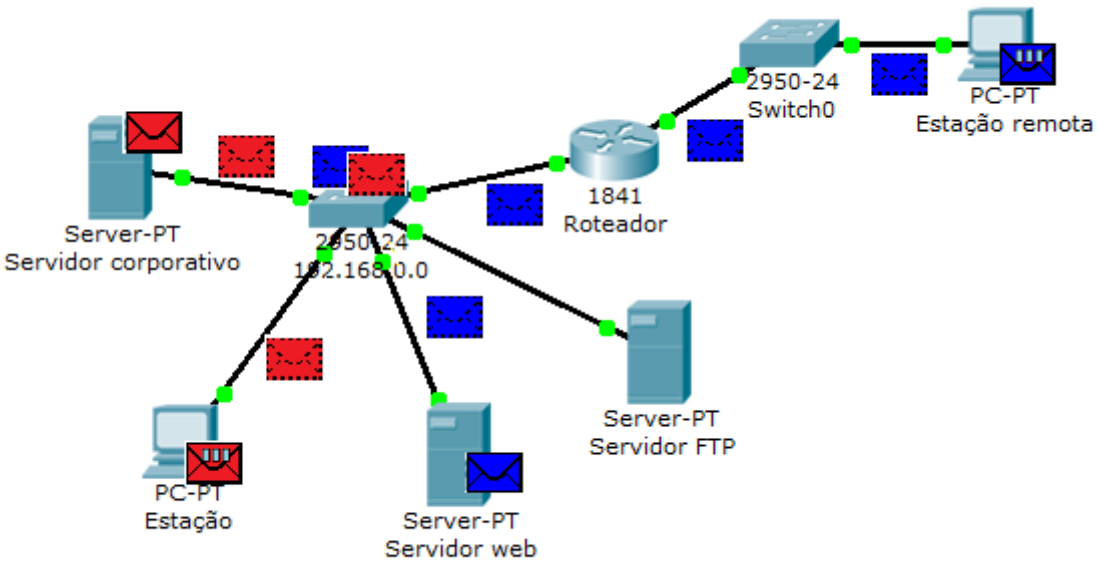

Figura 08: Fluxo de comunicação no cenário 01

No segundo cenário, como mostra a Figura 09, a rede interna foi separada da rede externa, ficando protegida pela configuração de uma rede desmilitarizada, diminuindo assim o potencial de dano causado por um ataque de um invasor.

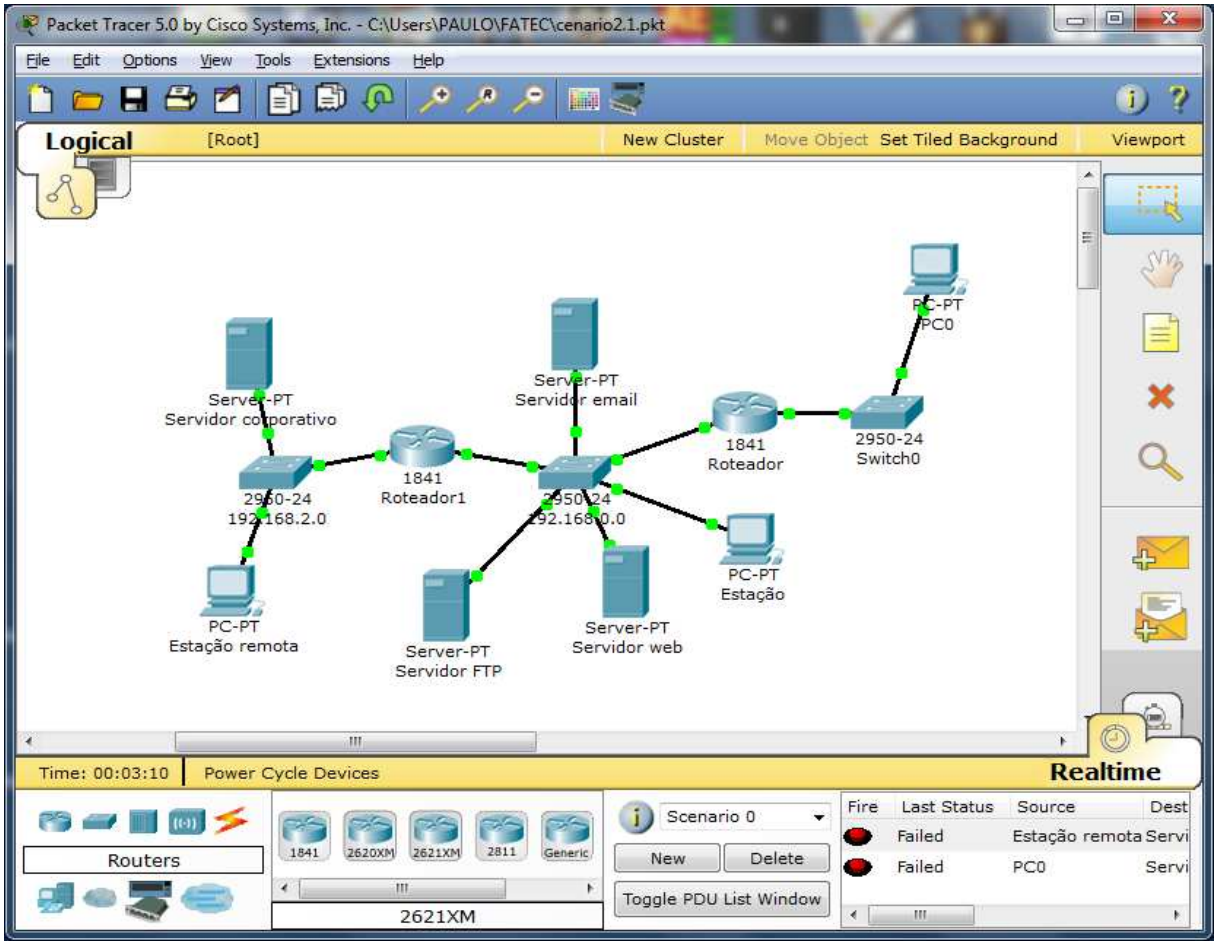

Figura 09: Cenário 02 Sistema de rede com DMZ

Na Figura 10 é possível observar que os pacotes vão para o seu endereçamento correto, não passando pela rede interna.

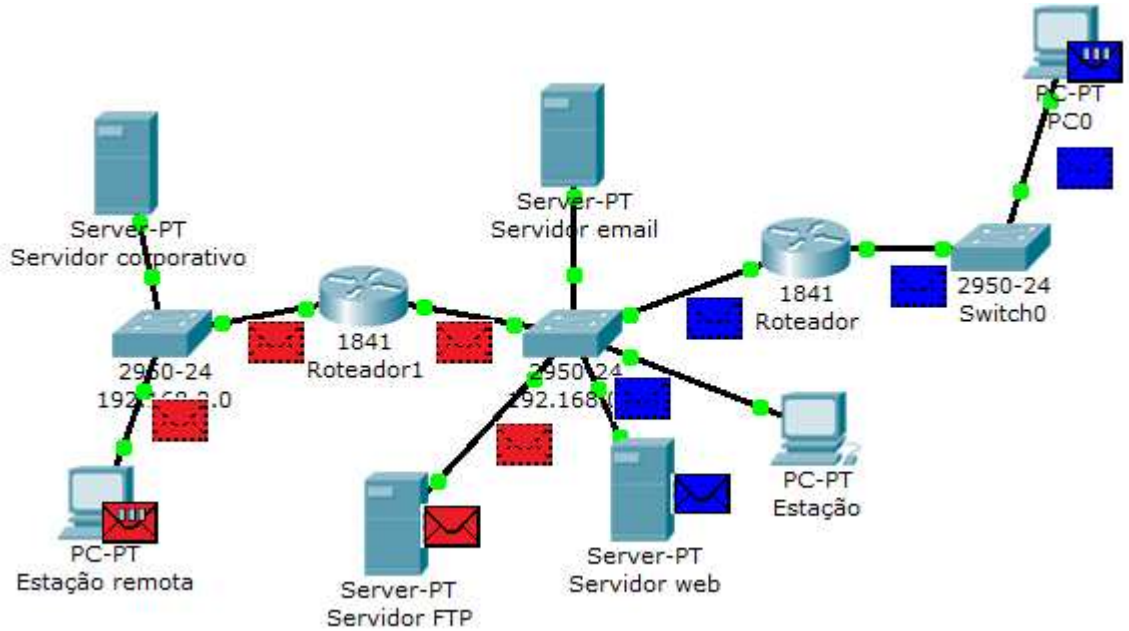

Figura 10: Fluxo de comunicação no cenário 02.

3.1 TESTES

Os testes foram realizados nas máquinas virtuais criadas no Virtualbox, onde foram criados os servidores e estações como mostra a Figura 11, afim de simular uma situação real na rede de uma corporação.

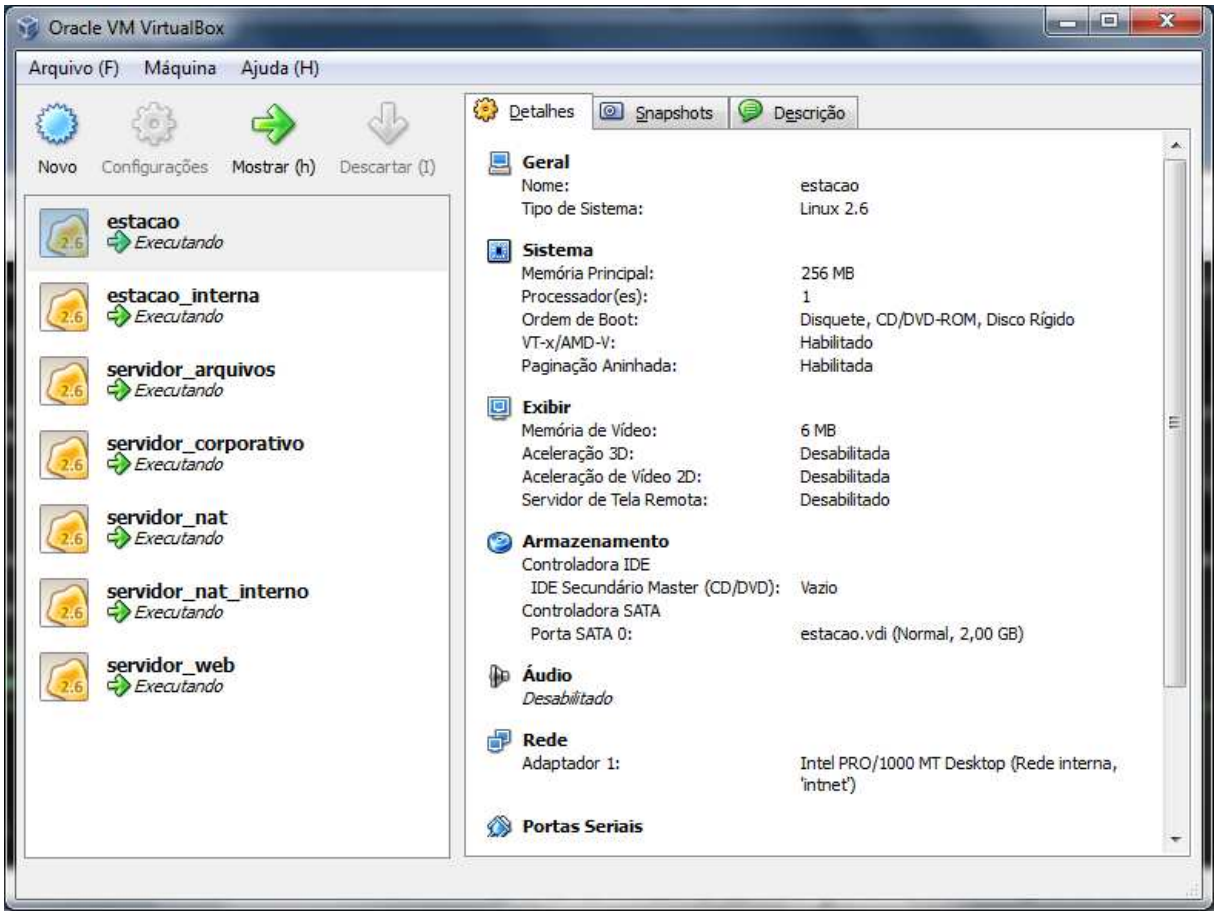

Figura 11: Maquina Virtual

O teste foi realizado com um *ping*, comando para verificar a conexão entre equipamentos. Neste caso os pacotes saíram da estação interna para o servidor web que, encontrando ativo o equipamento solicitado, foi devolvida uma resposta ao computador solicitante, como mostra a Figura 12.

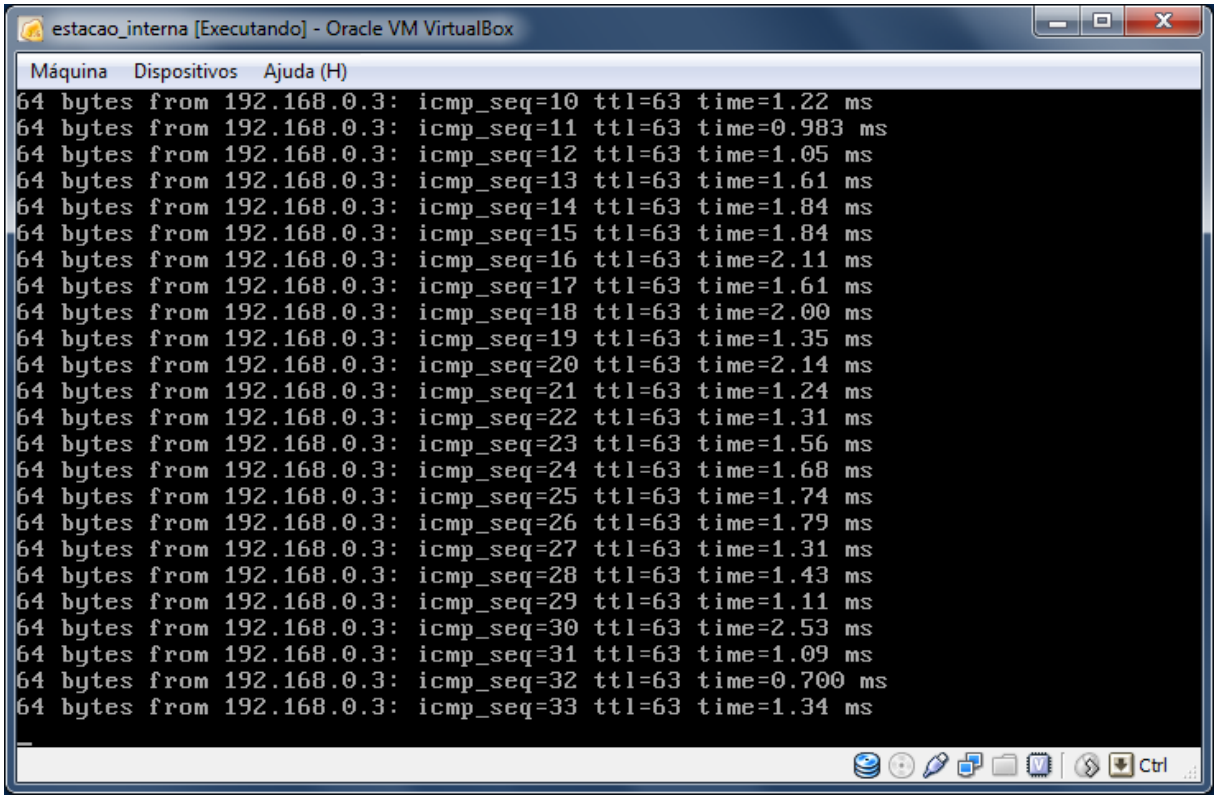

Figura 12: Estação interna

O servidor web foi o equipamento que recebeu os pacotes enviados pelo computador solicitante. (Figura 13)

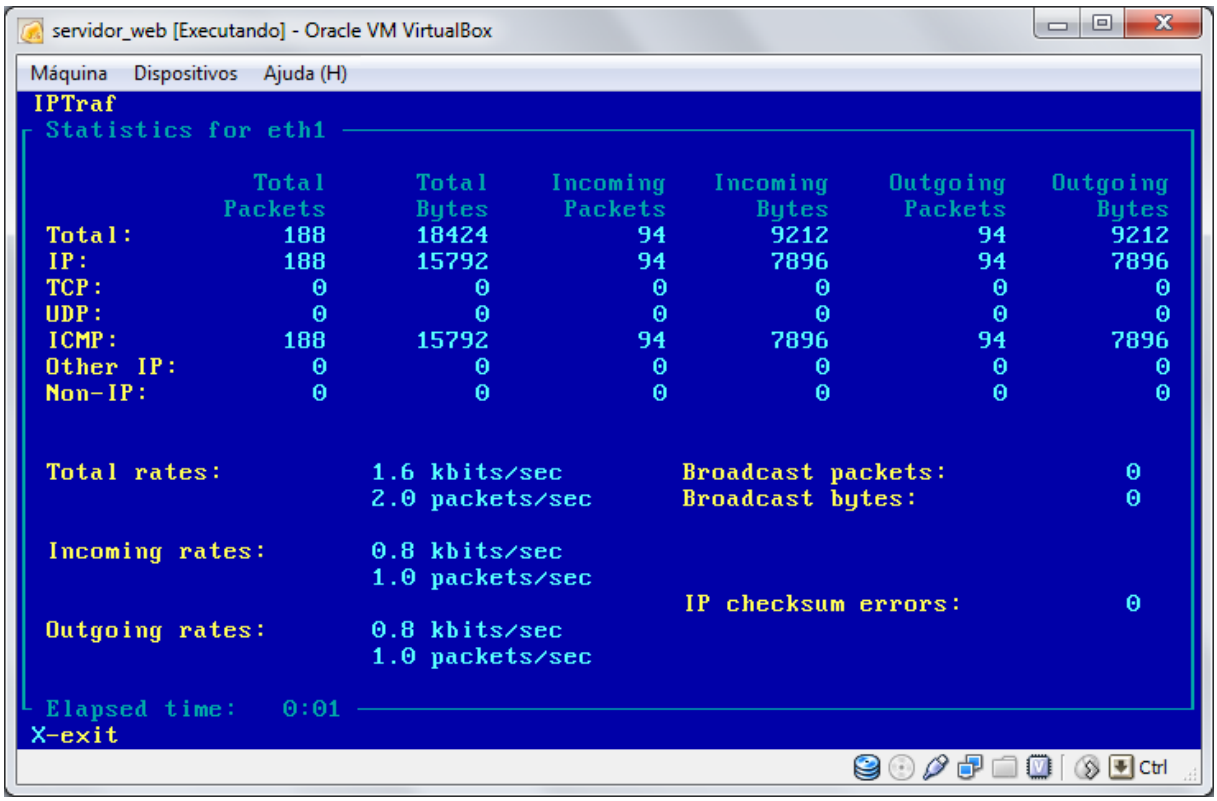

Figura 13: Servidor web recebendo pacotes da estação interna

Como é possível observar a estação localizada na rede externa não recebeu o tráfego dos pacotes endereçados entre a estação interna e o servidor web. (Figura 14)

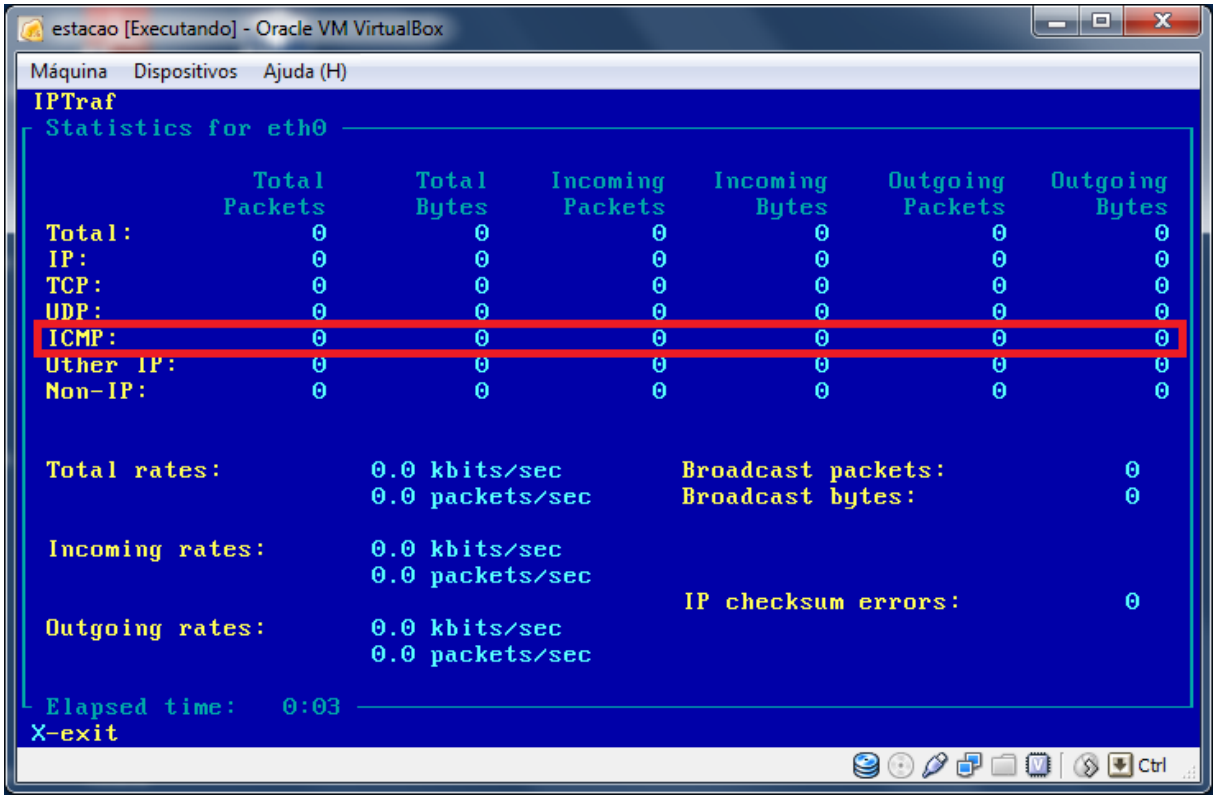

Figura 14: Tráfego da estação

Para fazer a confirmação de que a rede desmilitarizada realmente funciona em ambos sentidos, foi invertido o sentido dos pacotes. O teste foi realizado com um *ping* da estação externa para o servidor web, como mostra a Figura 15. O comando com saída da estação, encontra o servidor web e retorna a resposta a estação que, no caso, foi o computador solicitante.

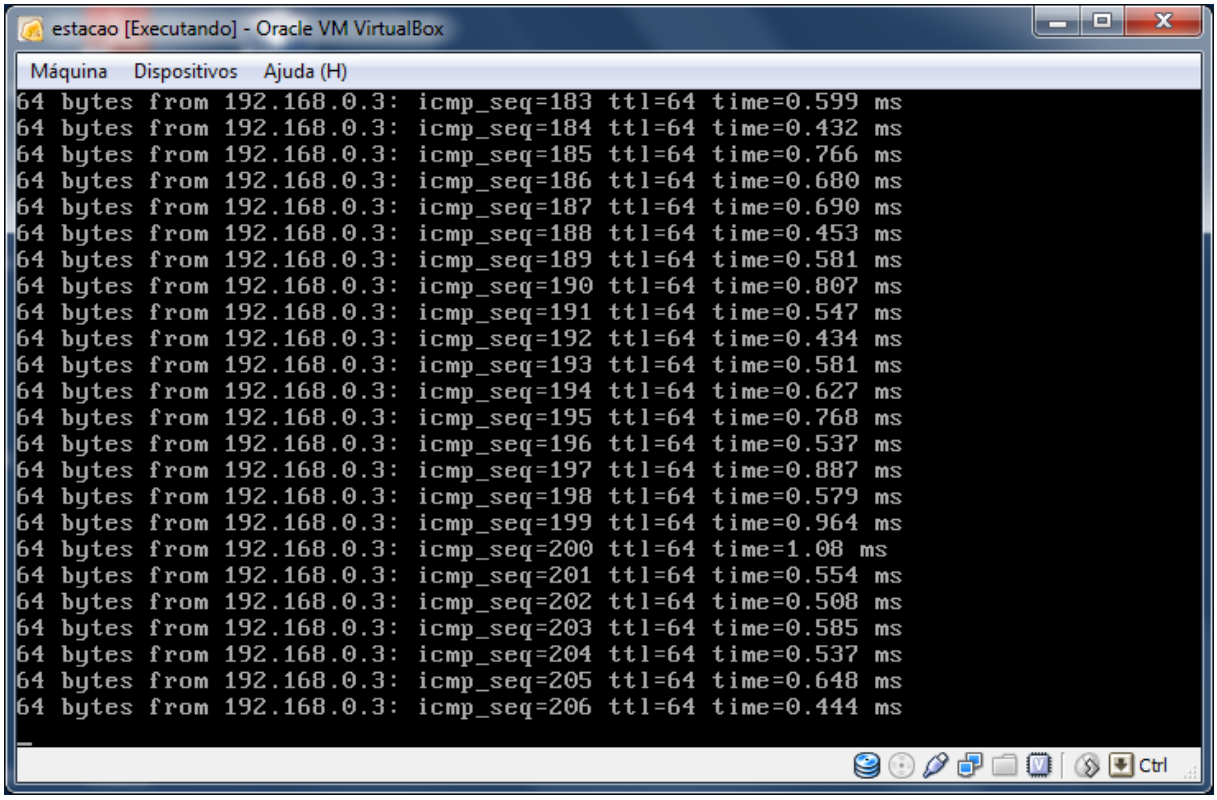

Figura 15: Estação enviando ping

Na Figura 16, o servidor web recebe os pacotes enviados pela estação externa.

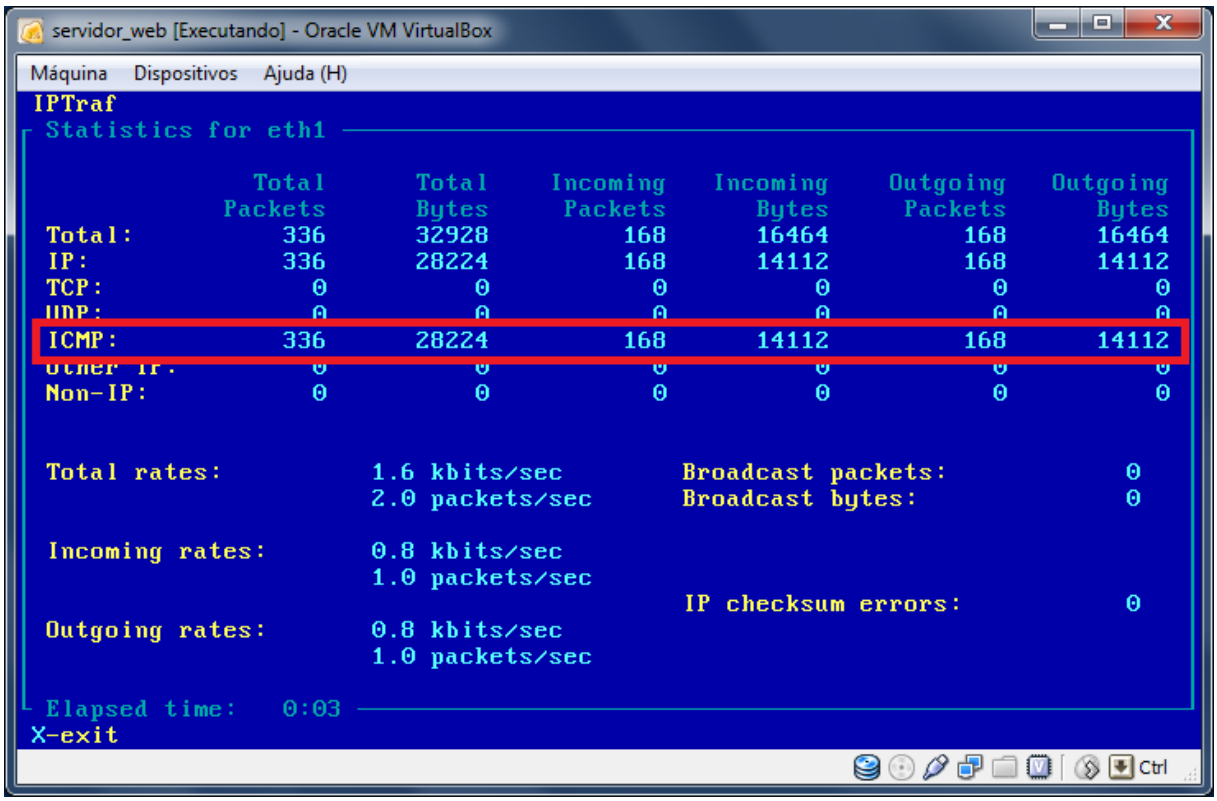

Figura 16: Servidor web recebendo pacotes da estação

A estação interna, Figura 17, que esta localizada na rede interna também não recebeu o tráfego dos pacotes endereçados entre a estação e o servidor web. (Figura 17)

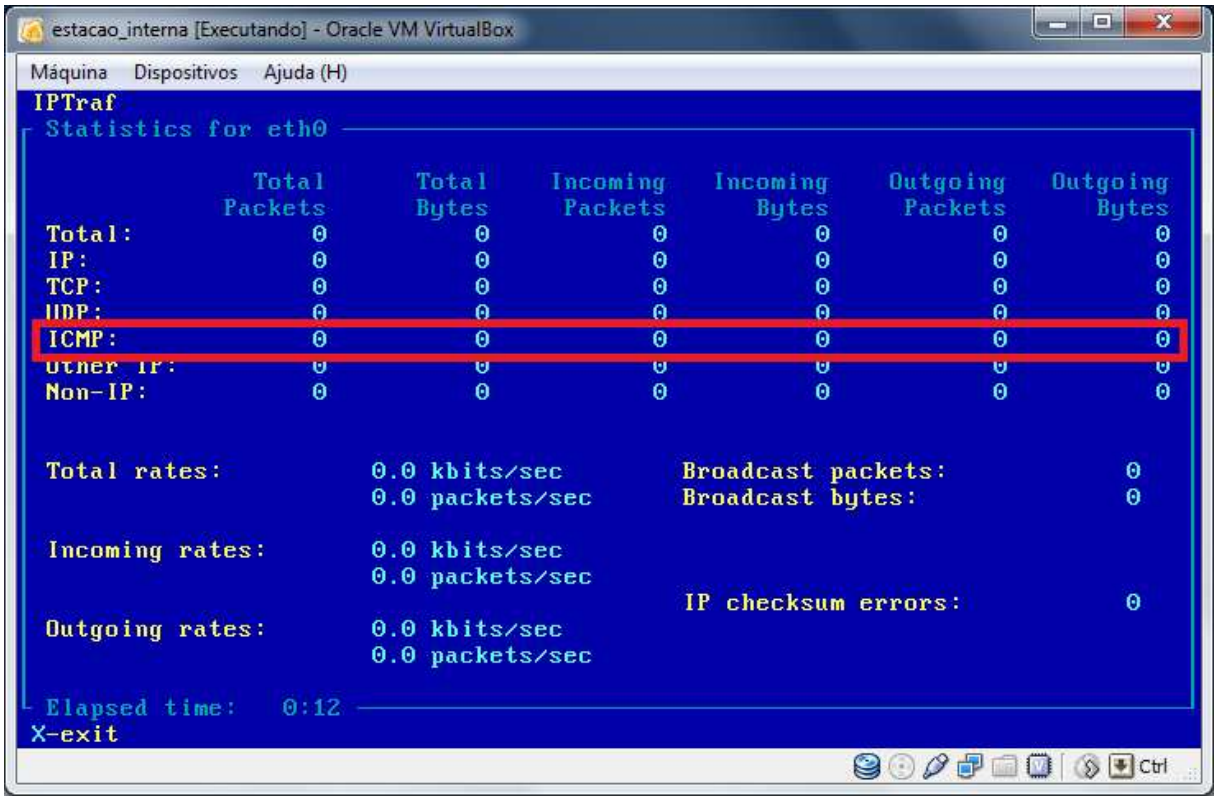

Figura 17: Estação interna

4 CONCLUSÃO

Com base nos dados obtidos, conclui-se que a implantação de uma rede desmilitarizada entre a rede interna e a rede externa de uma corporação, efetivamente “isola” a rede interna da web através de uma rede virtual distinta.

Os resultados observados após a implantação da rede desmilitarizada foi que o tráfego da rede interna e rede externa ficou restrito entre os equipamentos solicitantes e os equipamentos de destino.

Não ocorreu tráfego de pacotes em outros equipamentos a não ser os solicitados e destinados pelos pacotes, sendo assim, os resultados obtidos na execução dos testes foram satisfatórios para a confirmação do estudo realizado, atingindo plenamente o objetivo esperado do projeto desenvolvido.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

TANENBAUM, A. Redes de Computadores – Tradução da 4º edição. Rio de Janeiro: Elsevier Editora LTDA, 2003.

KUROSE, J. Redes de Computadores e a Internet: Uma abordagem top down 5º Ed. São Paulo: Addison-Wesley, 2010.

COMER, D. E. Interligação de Redes com TCP/IP – Tradução da 5º edição. Rio de Janeiro: Elsevier Editora LTDA, 2006.

SOARES, L. F.G., LEMOS, G., COLCHER, S. Redes de Computadores: das LANs, MANs e WANs às Redes ATM 2° Ed. Rio de Janeiro: Cam pus, 1995.

STALLINGS, W. Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas - Tradução da 5º edição. Rio de Janeiro: Campus, 2005.

http://sites.google.com/site/jlzemfatec/trc_tsi_noturno. Acesso em: 12 de fevereiro de 2011. 23h30.

http://www.infowester.com/firewall.php. Acesso em: 18 de fevereiro de 2011. 22h55.

Software Virtualbox disponível em: http://www.virtualbox.org. Acesso em: 20 de fevereiro de 2011. 22h48.

Informações sobre o software Packet Tracer Disponível em: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html. Acesso em 24 de fevereiro de 2011. 22h50.

SANTOS JUNIOR, A. L. dos. Quem Mexeu no Meu Sistema?: Segurança em Sistemas de Informação. Rio de Janeiro: Brasport, 2008. p.71-73.

PINHEIRO, J. M. S. Redes de Perímetro: Zona Desmilitarizada – DMZ. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php. Acesso em: 02 de maio de 2011. 22h43.