# ESCOLA TÉCNICA PROFESSOR MASSUYUKI KAWANO

**TÉCNICO REDES DE COMPUTADORES**

**AMIR FOUAD HAMADE**

**BRUNO SILVINO MACHADO**

**EDUARDO GAVA PEREIRA**

**ERIC MANSANARI CARPANEZI**

**GABRIEL PLAZAZ**


# INTEGRAÇÃO DE SERVIDORES: WINDOWS SERVER E LINUX


**Tupã – SP**

**2016**

# ESCOLA TÉCNICA PROFESSOR MASSUYUKI KAWANO

**TÉCNICO REDES DE COMPUTADORES**


**AMIR FOUAD HAMADE**

**BRUNO SILVINO MACHADO**

**EDUARDO GAVA PEREIRA**

**ERIC MANSANARI CARPANEZI**

**GABRIEL PLAZAZ**


## INTEGRAÇÃO DE SERVIDORES: WINDOWS SERVER E LINUX

Trabalho de conclusão de curso apresentado a ETEC Prof. Massuyuki Kawano. Como requisito parcial para obtenção do titulo de Técnico em Redes De Computadores

Orientador: Anderson Tukiyama Berengue

**Tupã – SP**

**2016**

CENTRO PAULA SOUZA

GOVERNO DO ESTADO SÃO PAULO

# ESCOLA TÉCNICA PROFESSOR MASSUYUKI KAWANO

## TÉCNICO REDES DE COMPUTADORS


**AMIR FOUAD HAMADE**

**BRUNO SILVINO MACHADO**

**EDUARDO GAVA PEREIRA**

**ERIC MANSANARI CARPANEZI**

**GABRIEL PLAZAZ**


## INTEGRAÇÃO DE SERVIDORES: WINDOWS SERVER E LINUX

BANCA EXAMINADORA:

---

Prof. Orientador: Anderson Tukiyama Berengue

---

Prof (a). Avaliador (a)

---

Prof (a). Avaliador (a)

**Resumo**

Trata da integração de dois servidores, com sistemas operacionais distintos para um melhor gerenciamento e segurança dos dados presentes na rede. Segundo o mercado de trabalho vê-se que não são todas as empresas que tem essa integração, algumas tendem a utilizar apenas um que no caso seria mais fácil porem menos seguro, tanto se utilizado de forma com que os dois servidores trabalhem de forma com que o administrador de rede consiga ter um acesso fácil e pratico do servidor, mais sabendo que uma das distribuições é em modo de texto e pode vir a consumir um certo tempo para que seja configurado. De acordo com normas impostas pelo administrador, os servidores que podem ser tanto duas maquinas como uma só, com uso de virtualização (maquinas virtuais) e trabalhem de forma onde todos os usuários da rede possam acessar sites e pastas compartilhadas na rede de forma segura e controlada pelo administrador.

Palavras chave:

- Servidores
- Rede
- Sistemas operacionais

**LISTA DE FIGURAS**

## Sumário

## 1. Introdução

Nos dias atuais, todas as empresas utilizam uma infraestrutura de redes de computadores e muitas utilizam apenas um Sistema Operacional (S.O) para gerenciamento dessa rede. Entretanto é possível integrar dois Sistemas Operacionais (S.O) nesse gerenciamento.

Será implementada uma rede de computador, uma integração de dois servidores com dois sistemas operacionais diferentes trabalhando em conjunto para um gerenciamento de uma infraestrutura de rede de forma fácil e segura, é possível integrar o Windows Server e o Ubunto Server uma integração que visa segurança e compartilhamento de arquivos.

A demanda com serviços Linux (por exemplo, gerenciamento de servidor) no mercado é muito grande, mas por falta de qualificação nessa área, poucos sabem trabalhar com Linux.

## 2. Justificativa

Com o mercado de servidor em alta, e necessário apresentar soluções viáveis aos usuários e à utilização de servidores Linux e a principal forma de unir custo e beneficio. Dessa forma será demonstrado a integração de dois Sistema Operacional (S.O) diferentes para o gerenciamento de uma rede de computadores.

## 3. Objetivo geral

O objetivo e criar uma rede com dois servidores, um Linux e outro Windows para gerenciar a nossa rede wireless e cabeada. Criando um usuário e senha para todos os usuários que utilizam a rede wireless, dessa forma, gerenciar o trafego de informações na rede, mantendo a segurança da rede e gerenciamento de sites inapropriados ou prejudicais a rede.

### 3.1 Objetivo especifico

Criar uma rede com o máximo de proteção para os seus usuários, onde a função do servidor Linux é bloquear sites inapropriados utilizando o serviço de firewall, o (Dynamic Host Configuration Protocol) para gerenciamento de IPs de toda rede, o serviço Linux SARG para apresentação de relatórios e o servidor Windows server 2012 para autenticação do usuário.

## 4. Metodologia

Foi utilizado para montagem desta tese interpretações de artigos tecnológicos, para que se possa chegar ao objetivo que e a implementação dos servidores, as pesquisas sobre os serviços e protocolos utilizados, essas pesquisas partirão do ponto em que e necessário apresentar durante o trabalho conceitos e de serviços e protocolos utilizados na montagem, analisando vários artigos para que assim seja possível a apresentação em ótimo estado do projeto.

## 5. Conceito sobre rede de computadores

As primeiras de redes de computadores foram criados na década de 60, tinha a intenção de mandar arquivos e informações para outro computador, na época era usado para armazenamento de dados em cartões perfurados, era o mais lento, trabalhoso e demorava muito para perfurar os cartões de cartolina com furos que representa os bits.

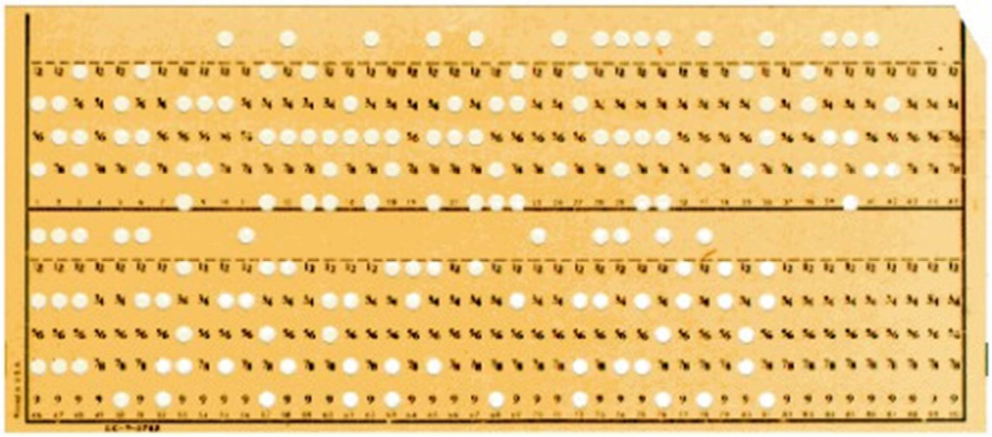


Figura 1 – Cartão perfurado

A Arpanet foi criada entre 1969 a 1972 foi o embrião da Internet, inicialmente com apenas 4 nós, interligados através de link de 50 kbps, usando linhas telefônicas dedicadas para o link de dados. Naquela época 50 kbps em longa distância era uma alta velocidade para a época. As redes domesticas da época era de 110 bps (bits por segundo).

O principal proposito da Arpanet foi um desafio de interligar 4 computadores de arquiteturas diferentes, em apenas 3 anos a rede já tinha mais de 30 computadores entre universidades, militares e empresas.

Em 1973 foi o primeiro teste em transmissão de dados via Ethernet pelo laboratório da Xerox onde vários outras tecnologias importantes como a interfase gráfica e o mouse, a transmissão de dados era de 2.94 megabits através de cabos coaxiais permitia mais de 256 estações conectadas. Existem outros padrões que podem ser usado um cabo de fibra óptica, ou mesmo o ar, no caso das redes wireless. Na época a taxa de transmissão de 2.94 megabits do Ethernet original era derivada do clock de 2.94 MHz usado no Xerox Alto, mas foi logo ampliada para 10 megabits dando a origem do padrões Ethernet.

No ano de 1974 surgiu o protocolo de bases TCP/IP protocolo definitivo da ARPANET e da internet do dias atuais usando os recursos como e-mail e o FTP que permite o usuário se conectar e trocar informações e compartilhar arquivos com varias pessoas ao mesmo tempo.

Com o aumento da rede de computadores em 1980 passaram a ser usados nomes de domínio DNS - Domain Name System, domínio usado até hoje na nossa rede atual.

A Internet começou ser acessada mesmo depois da década de 1990, ganhou uma nova dimensão enorme ficou muito popular no mundo todo, mais o acesso era lento via linha discada, mais logo mudarão as conexões para banda larga. Nos dias de hoje quase todo mundo tem um PC com acesso a internet via banda larga com um roteador wireless.

## 5.1 Servidor de redes de computadores

Servidor é basicamente um computador mais potente do que um desktop comum de uso domestico. Ele foi desenvolvido para transmitir informações para outros computadores que estiverem conectados na mesma rede, existem mais de um tipo de servidor, gerenciador de internet e dados que pode ser Windows ou Linux vai da necessidade da empresa. Eles foram desenvolvidos para lidar com cargas de trabalho mais pesadas, eles também oferecem ferramentas de gerenciamento remoto você não precisa esta na frente do servidor para fazer qualquer alteração ou até reiniciar em caso de necessidade mais eles foram desenvolvido para ficar 24 horas ligado, computadores domésticos não consegui ter uma vida útil como um Servidor.

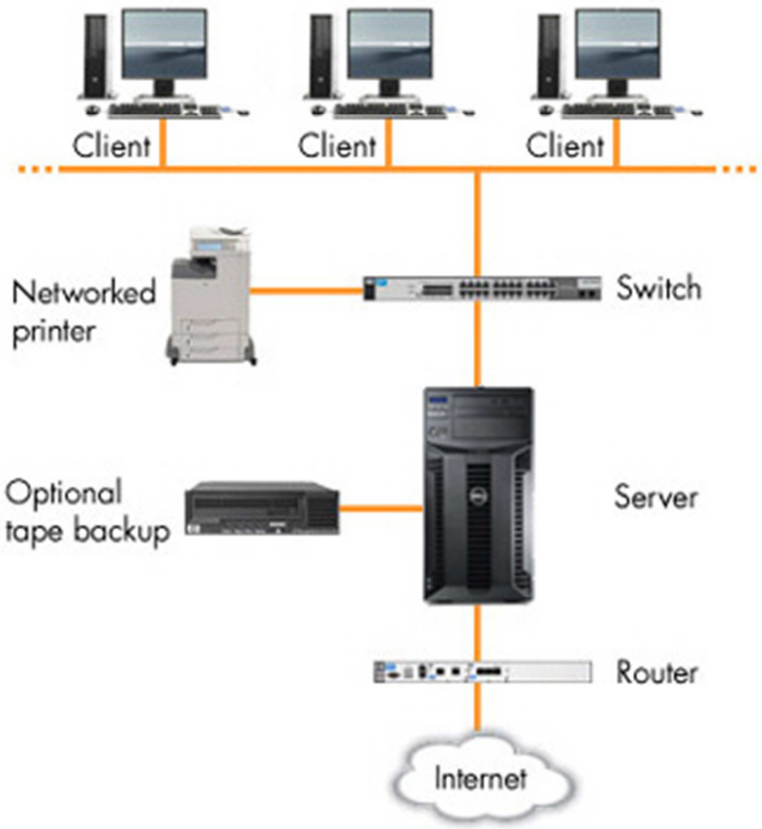



Figura 2 – Exemplo de uma Rede de computadores com servidor

Um servidor pode ajudar a organizar os dados e a proteger seus negócios contra perda ou danos de arquivos. Você pode fazer backup das informações do servidor para um sistema de backup e de recuperação dedicado. Assim, se alguns dos dados importantes de sua empresa forem acidentalmente excluídos, perdidos ou roubados, poderá ter certeza de que seus arquivos estarão seguros no backup e que poderá restaurá-los novamente. Com vários discos rígidos em um servidor e com seus sistemas de backup, você pode ter certeza de que falhas no disco rígido não apagarão seu sistema novamente.

**5.2 Historia do Linux;**

O sistema Linux tem sua origem no Unix, um sistema operacional multitarefa e multiusuário que tem a vantagem de rodar em uma grande variedade de computadores.

Uma grande razão de sucesso é seu equilíbrio entre sua produtividade e portabilidade.

É dividido em 2 partes, a 1ª é o kernel que é o núcleo do sistema responsável pela comunicação com o hardware e o 2ª são os programas e serviços que dependem do kernel para interação.

Um estudante finlandês chamado Linus Torvalds inicia um processo pessoal de aprimoramento do Kernel do Minix um sistema operacional do tipo Unix escrito por Andrew Tannenbaum, chamando esta vertente de Linux como abreviação de Linus´s Minix. Em 5 de outubro 1991, Linus Torvalds anuncia a primeira versão oficial do Linux.

Desde então, muitos programadores e usuários espalhados pelo globo terrestre tem seguido os ideais de Richard Stallman e Linus Torvalds.

### 5.3 Active Directory (AD)

O AD (Active Directory) e um serviço de diretório da Microsoft constantemente usado nos Windows server 2008 e 2012, que são os mais recentes, com o AD é possível gerenciar domínio, DNS, DHCP, arvore ou floresta de domino (arvore e um conjunto de domínios  e a floresta e um conjunto de arvores ).

#### 5.3.1 Domínios

Gerencia o acesso de pastas e contas de usuários cadastrados na lista do AD criando grupos de acesso, por exemplo as pessoas do grupo de pesquisas de uma empresa não podem acessar os diretórios ( pastas) das pessoas de administração mas o diretor da empresa tem acesso total.

#### 5.3.2. Arvores

Conforme Rover (2012), Quando precisa-se criar um segundo domínio , na maioria das vezes por necessidades no processo de segurança tem o que chama-se de domínios filhos. Quando tem um domínio pai com seus filhos, chama-se de arvores de domínio.

Nesse caso e formado uma cadeia de domínios formando uma arvore (pode se comparar com uma arvore genealógica) um domínio dando sequencia a outro ate formar o conjunto

### 5.3.3. Florestas

Como o nome sugeri é um conjunto de arvores de domínio

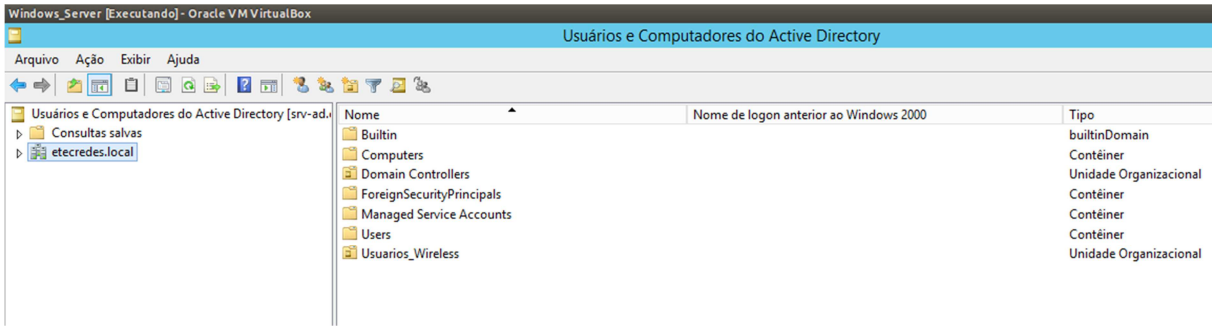



Figura 3 – Exemplo de domínio

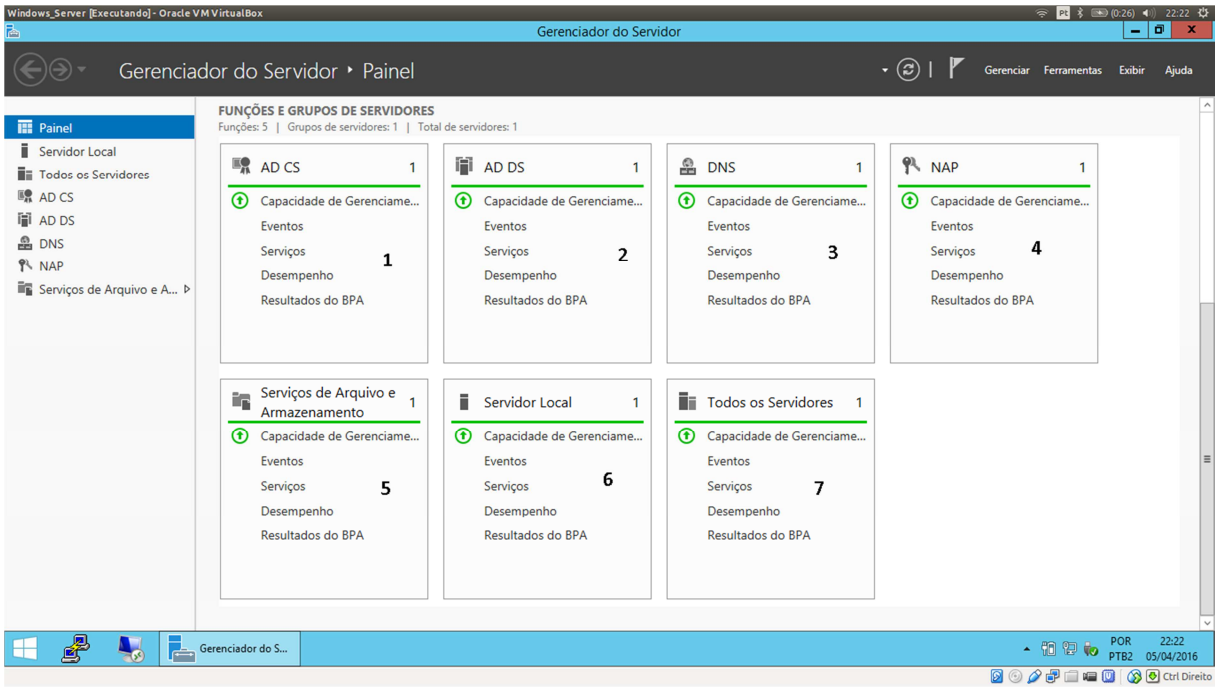



Figura 4 – Serviços utilizados no servidor Windows Server

Descrição dos serviços, conforme numeração da figura 4:

1. Active Directory certificate  services (serviços de certificado do AD)
2. Active Directory domain Controler
3. Active Directory domain name server

4. Network acces protocol controle de acesso
5. Serviço de compartilhamento de acesso
6. Todos serviços locais do servidor
7. Todos os serviços da mesma rede

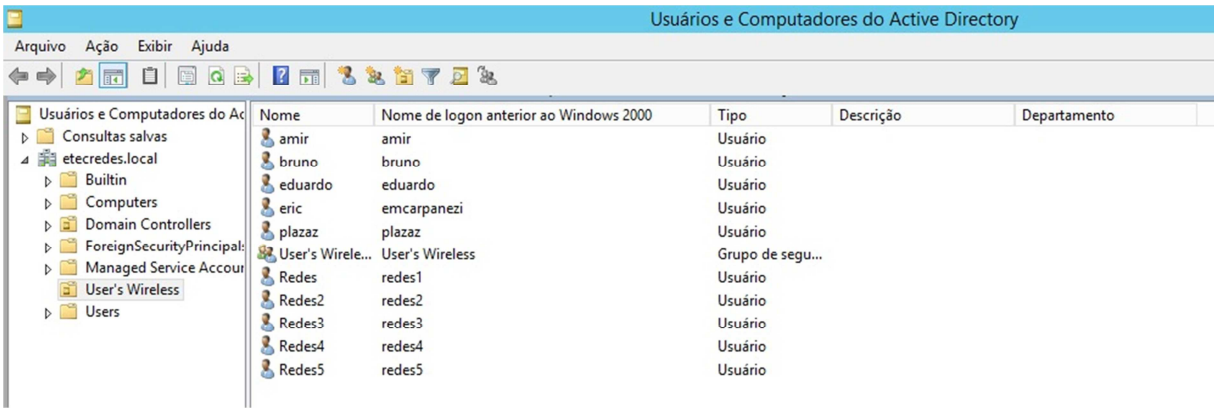



Figura 5 – Usuários e Grupos do AD.

### 5.4 Secure Shell (SSH)

O Ssh e uma ferramenta de acesso remoto para distribuição Linux, que permite um acesso de forma segura fazendo uso da criptografia assimétrica (que utiliza um par de chaves ao invés de apenas uma chave ) ,os pacotes enviados pelo acesso ,permitindo assim uma certa tranquilidade de não ser ouvido se caso aja uma escuta[1] na rede.

A instalação na plataforma Ubuntu do Linux é da seguinte forma:

$sudo apt-get install openssh-server

O arquivo de configuração pode ser encontrado no seguinte diretório, /etc/ssh/sshd_config, partindo da raiz padrão “/”.

Exemplo software que utiliza essa estrutura: O Putty.

[1] Escuta na rede: é quando há um programa malicioso em busca de informações privilegiadas e sigilosas.

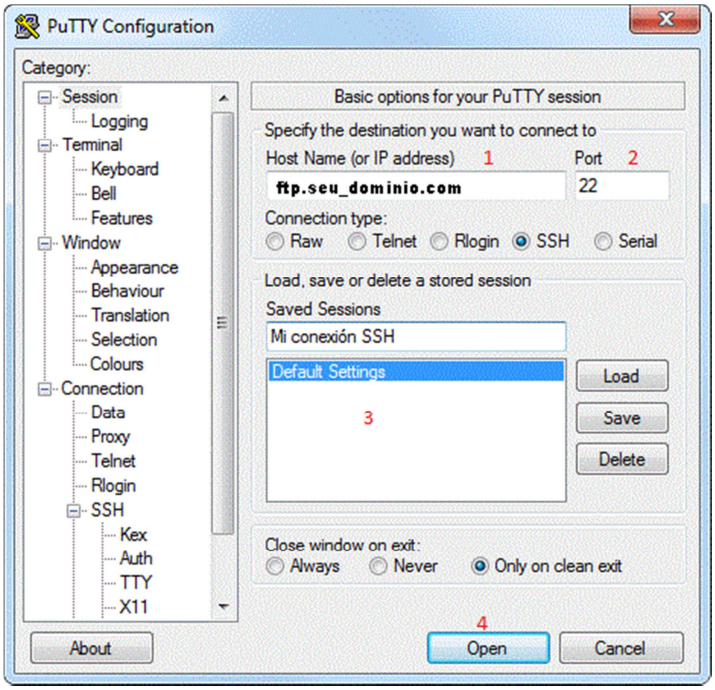



Figura 6 - tela de login do Putty

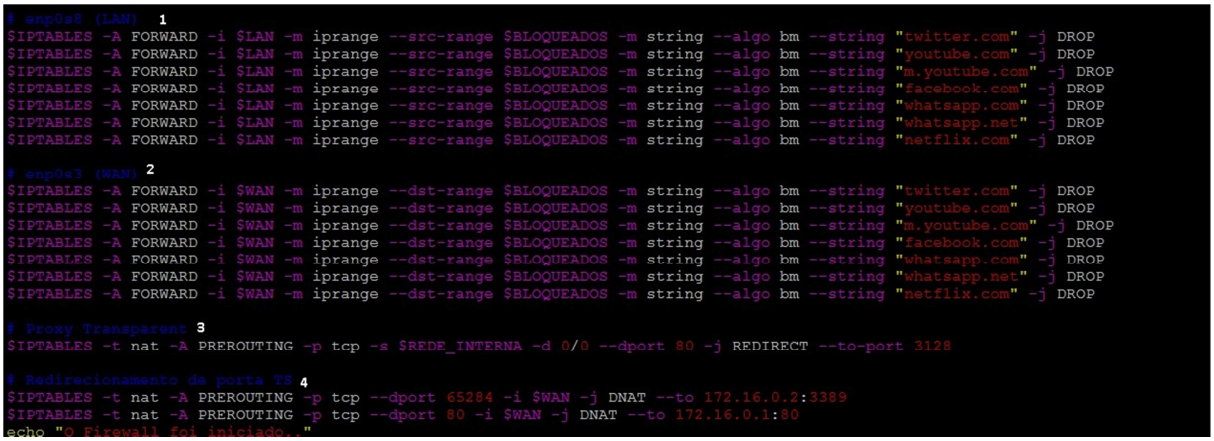
Descrição dos campos da figura 6:

1. Espaço onde e colocado o IP ou nome de domínio
2. Espaço onde e colocada a porta
3. Configurações de tela do putty
4. Iniciador de conexão com servidor

## 5.5 FIREWALL

O Firewall é um Software ou Hardware de segurança que tem como objetivo analisar os dados da rede e determinar o que pode ou não trafegar na rede, ou seja, o firewall basicamente funciona como um bloqueio de dados indesejados e liberação de acesso.

É utilizado para bloquear e liberar o tráfego de dados na rede, mas bloquear tudo não é interessante, por isso existem as regras para liberar aplicativos e sites. Abaixo a configuração utilizada em um servidor Linux.



```
# enp0s8 (LAN)  1
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "twitter.com" -j DROP
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "youtube.com" -j DROP
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "m.youtube.com" -j DROP
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "facebook.com" -j DROP
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "whatsapp.com" -j DROP
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "whatsapp.net" -j DROP
$IPTABLES -A FORWARD -i $LAN -m iprange --src-range $BLOQUEADOS -m string --algo bm --string "netflix.com" -j DROP

# enp0s3 (WAN) 2
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "twitter.com" -j DROP
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "youtube.com" -j DROP
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "m.youtube.com" -j DROP
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "facebook.com" -j DROP
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "whatsapp.com" -j DROP
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "whatsapp.net" -j DROP
$IPTABLES -A FORWARD -i $WAN -m iprange --dst-range $BLOQUEADOS -m string --algo bm --string "netflix.com" -j DROP

# Proxy Transparent 3
$IPTABLES -t nat -A PREROUTING -p tcp -s $REDE_INTERNA -d 0/0 --dport 80 -j REDIRECT --to-port 3128

# Redirecionamento de porta TS 4
$IPTABLES -t nat -A PREROUTING -p tcp --dport 65284 -i $WAN -j DNAT --to 172.16.0.2:3389
$IPTABLES -t nat -A PREROUTING -p tcp --dport 80 -i $WAN -j DNAT --to 172.16.0.1:80
echo "O Firewall foi iniciado.."
```

Figura 7 – Configuração do Firewall

Descrição das configurações do firewall

1. Linha onde são bloqueados os pacotes de rede enp0s8 (LAN)
2. Linha onde são bloqueados os pacotes de rede enp0s3 (WAN)
3. Proxy Transparente
4. Redirecionamento de Portas

Conforme Machado (2012), Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final.

O Firewall funciona de acordo com as regras estabelecidas pelo gerente da rede de acordo com sua politica de segurança de rede.

### *5.5.1 IPTABLES*

O IPTables serve para administrar as regras e filtrar pacotes de redes de computador, funciona comparando as regras existentes em seus arquivos de configuração. Dessa forma um pacote tem ou não permissão para passar ou não para rede de computador.

É utilizado para redirecionar portas, redirecionar servidores e serviços. Pode criar regras para bloquear usuários na rede, bloquear serviços e acesso por determinados IPs.

As CHAIN ou correntes da tabela filter INPUT, OUTPUT, FORWARD, na tabela nat PREROUTING, OUTPUT, POSTROUTING, e na tabela mangle PREROUTING E OUTPUT

INPUT – E ela quem faz a filtragem de pacotes cujo destino e o firewall

OUTPUT – E responsável por estabelecer as regras para a filtragem dos pacotes que são originados pelo firewall

FORWARD – Comporta as regras que farão filtragem dos pacotes que passarão pelo firewall

PREROUTING – Responsável por definir as regras de roteamento antes que o pacote seja enviado

POSTROUTING – Responsável por regras especificas de roteamento depois do pacote ter passado pelas demais chains

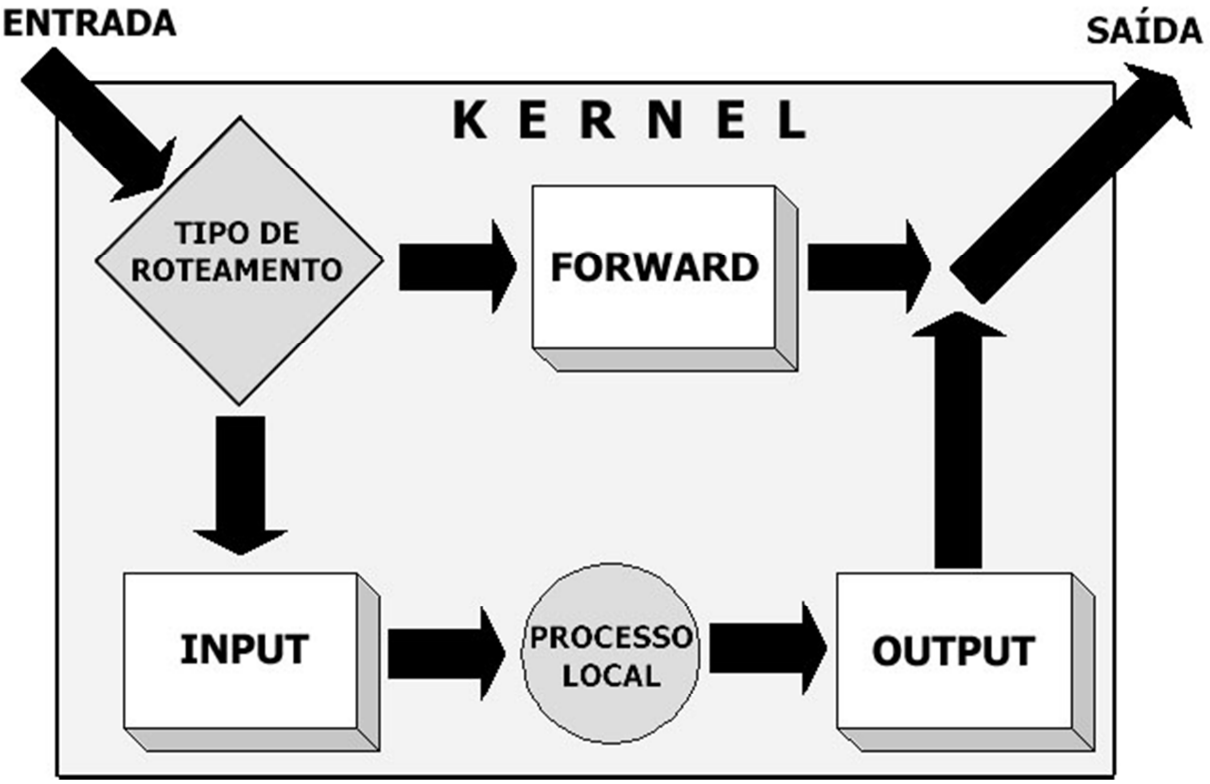



Figura 8- exemplo da tabela filter

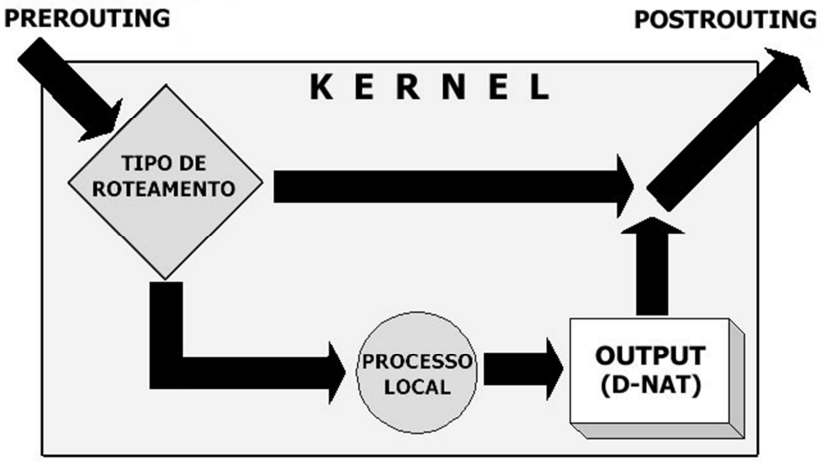



Figura 9-exemplo da tabela NAT

```
root@srv-tcc: /etc/squid3

$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state INVALID -j DROP

echo "O Firewall Foi iniciado..."
}

fw_stop()
{
## Voltando Politica Padrao "ACCEPT" , Removendo regras existentes nas chains INPUT-FORWARD-OUTPUT
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT

$IPTABLES -F
$IPTABLES -X
$IPTABLES -t nat -F

## Parando Roteamento
echo 0 > /proc/sys/net/ipv4/ip_forward

echo "O Firewall foi Parado"
}

fw_usage()
{
echo "$0 (start | stop | restart | clear)"
echo
echo "start      - Ativa o Firewall"
echo "stop       - Desativa o Firewall"
echo "restart    - Reativa o Firewall"
echo "clear      - Limpa o Firewall"
}

fw_clear()
{

#_Limpa as regras existentes nas chains INPUT-FORWARD-OUTPUT
$IPTABLES -F
$IPTABLES -X

#_Limpa as regras existentes na Tablea NAT
$IPTABLES -t nat -F

echo "As Regas do Firewall foram Limpas..."
}

case $1 in

        start)
          fw_start;
        ;;
```

Figura 10 – Configurações do Firewall

Na figura 8 pode – se visualizar as configurações de filtros utilizadas no servidor Linux.

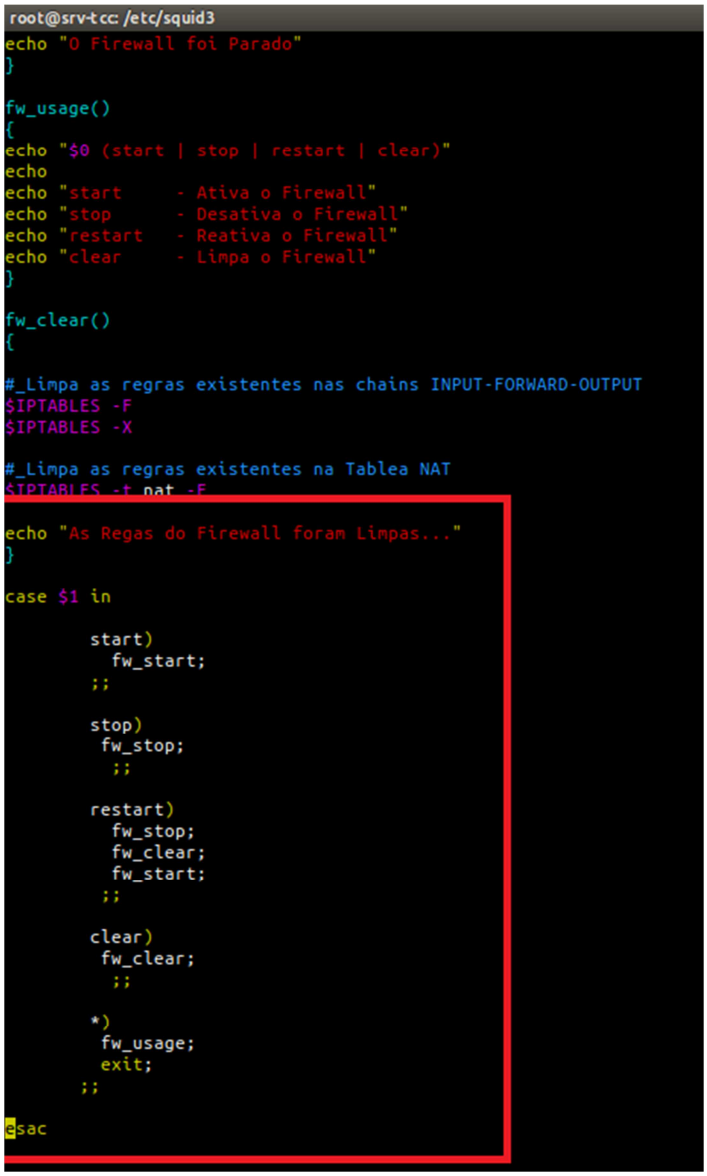



Figura 11 – Configuração do Firewall (start, stop, clear e restart)

Na figura 9 é mostrado as linhas do scrip de configuração do firewall com os comandos de start, stop, restart e clear e os comandos executados quando se digita firewall (nome da palavra) exemplo firewall restart ele ira restartar o firewall

## ***5.6 SQUID***

É um serviço Proxy que tem o papel de fazer a intermediação dos acessos da rede de computadores. Podendo fazer alguns bloqueio através de palavras, extensões, sites, rede local, horários de acesso e controle de banda. O proxy é carregado junto com o Kernel do Sistema Operacional, por esse motivo, não se tem uma demora para os pacotes chegar ao destino final, compatível com a maioria dos Sistemas GNU[2], porem o Squid não trabalha com portas Seguras “HTTPS” somente com http, ftp entre outros.

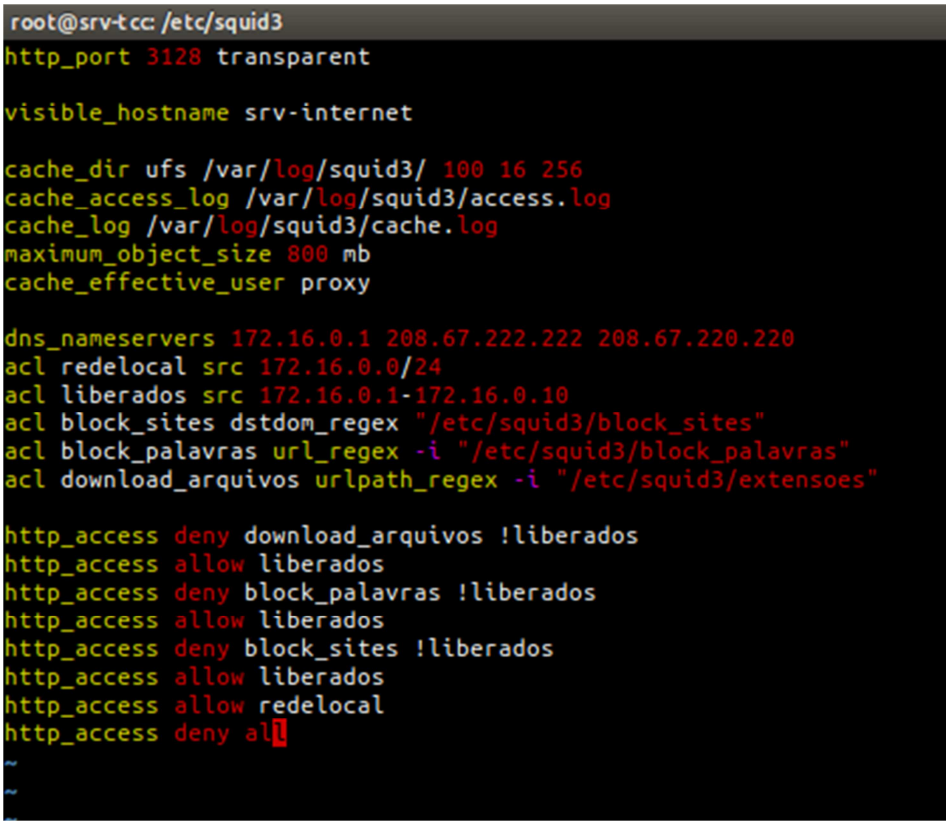



Figura 12 – Configuração do Squid

### 5.7 Domain Name Serve (DNS)

O DNS tem função de atribuir um nome a um IP para que sua localização seja mais fácil através de palavras, ao colocar um endereço (link) legível no navegador,

[2] GNU – distribuição do Sistema Operacional Linux

ele vai entra em contato com o servidor de DNS e faz a conversão para numero IP do computador a ser acessado.

Exemplos: www.vivaolinux.com.br IP: 162.144.34.3

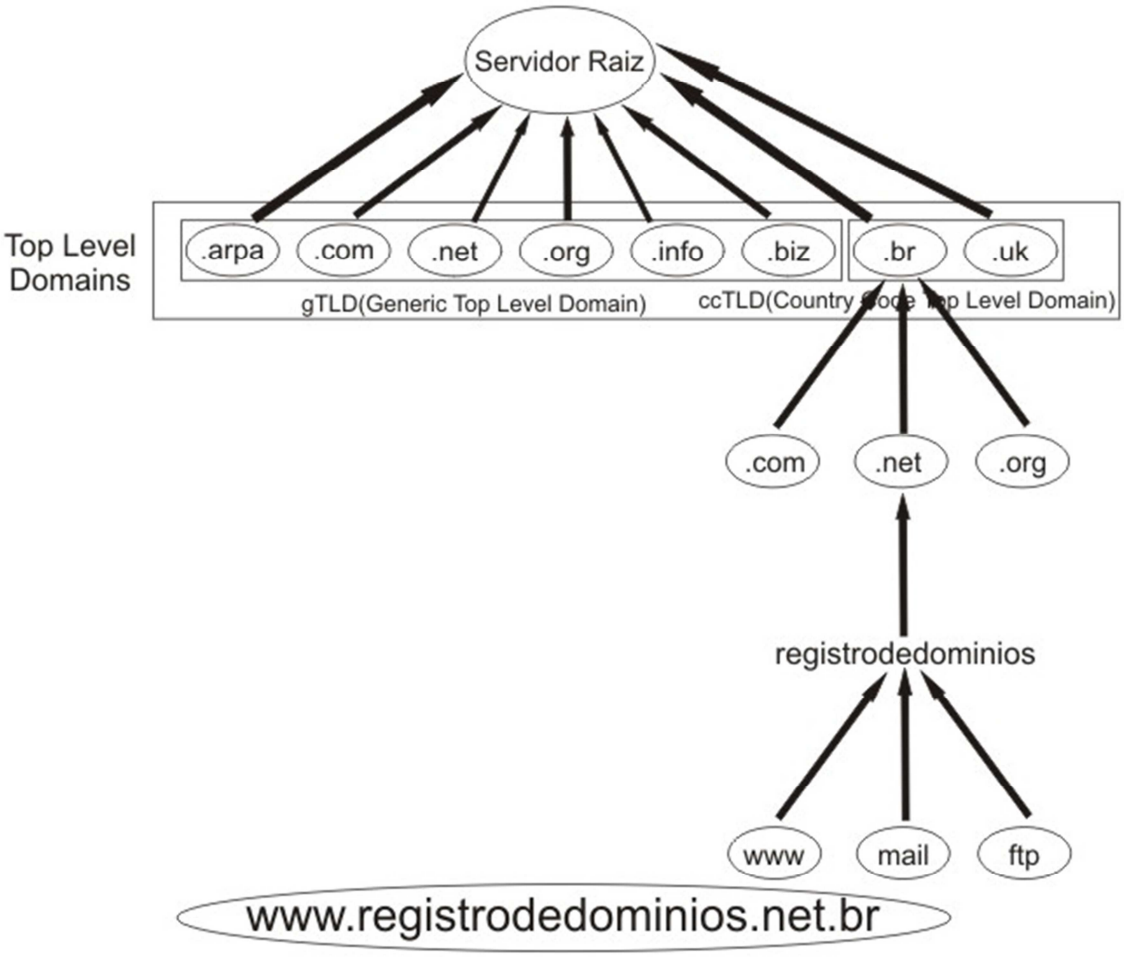



Figura 13 – Representação do DNS

A figura 11 mostra as arvores de domínio de acordo com sua hierarquia.

O DNS foi introduzido originalmente nos estados unidos são utilizados alguns no fim do nome de domínio que se referem a entidades governamentais como .gov por exemplo.

Nos países a mudança dentre os nomes de domínio também como .br no brasil cada pais tem o seu fim diferente como localização nacional.

## 5.8 Dynamic Host Configuration Protocol (DHCP)

Conforme PAULA PEREIRA (2009), DHCP é um protocolo configuração Dinâmica de Endereços de Rede, é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente.

Quando e feita uma solicitação pela maquina cliente o servidor manda um pacote contendo as informações dispostas no DHCP, o Gateway da rede, o nome de domínio e o IP dentro da faixa disponível.

O DHCP tem três formas de funcionamento Automática, dinâmica e manual

- Automática – o DHCP automático e o que libera IP conforme as maquinas clientes vão se conectando a rede de acordo com a faixa imposta pelo gerente de rede
- Dinâmica – muito parecida com a automática porem os IPs são fornecidos por um período de tempo que e dito pelo gerente de rede
- Manual – a forma manual e quando o gerente aloca um IP a uma maquina pelo seu MAC (Media Access Control) como um CPF da maquina todas tem e não pode ser mudado então e alocado um IP especifico por MAC para que aquele MAC tenha sempre aquele IP.
- MAC: É o endereço de controle de acesso da sua placa de rede. É um endereço único, como se fosse um CPF do computador,12 dígitos hexadecimais.

O DHCP é protocolo configuração Dinâmica de Endereços de Rede, um serviço que permite a distribuição de IP para os computadores e outros aparelhos. O DHCP foi criado para facilitar o endereçamento de IP e evitar conflito, se o DHCP for mal configurado no servidor ou roteador pode gerar conflito na rede.

# 6 Implementação prática dos servidores Windows Server e Linux

Será implementado 2 servidores, sendo 1 Windows Server Data Center R2 x64 e Ubuntu Server LTS x86, fazer com que todos que estiverem conectado a

nossa rede passar por um servidor de Internet, fazendo assim uma conexão mais rápida e segura para todos os usuários da rede.

O Servidor Windows Server vai ser usado para fazer autenticação de usuários, será instalado alguns serviços do tipo, AD (Active Directory),Serviço de Certificado do Active Directory, e o NAP (Proteção de Acesso a Rede),

O Active Directory será usado para criação dos “Usuários” e “Grupos” da nossa rede,

O Serviço de Certificado do Active Directory será usado para fazer a autenticação via RADIUS.

O NAP será usado para fazer com que o roteador ou AP (Access Point), consiga ter uma comunicação com o servidor e autenticando cada usuário registrado no Active Directory.

O servidor Ubuntu será usado para fazer a comunicação com a Internet, serão instalados alguns serviços para um gerenciamento adequado, do tipo como: DHCP,SQUID,SARG,NTOP,FAIL2BAN,APACHE,APACHE2UTILS.

O serviço de DHCP é usado para fazer com que todos que estiverem na rede recebam 1 endereço IP.

O serviço Squid é um proxy usado para fazer bloqueios na rede local, o mesmo serviço e usado como servidor de cache.

O Serviço SARG é bastante utilizado para ter relatórios do que foi acessado no squid, mostrando IP do usuário, sites acessados, se foi permitido ou bloqueado.

O Serviço NTOP é usado para ter um controle de banda, sabendo quando a sua rede esta usando no momento ou dias anteriores.

O Serviço FAIL2BAN é usado para bloquear ataques de Força Bruta, do tipo ssh.

O Serviço APACHE é usado para levantar alguma pagina de internet no servidor.

O Serviço APACHE2-UTILS é usado para proteger paginas de serviços locais.

O Servidor Ubuntu responsável pelo tratamento da internet bloqueando alguns sites no Proxy (squid) e no Firewall (iptables), Fazendo uma conexão mais rápida e segura, gerando logs de acesso de serviços e sites, Com o FAIL2BAN

Consigo bloquear 2 tentativas de acesso ao serviço SSH com usuário e senha Invalida ele bloqueia o endereço IP da Pessoas por 2 Horas

Fazendo com que todos que estiverem conectado a rede sera forçado a passar pelo proxy, fazendo a intermediação dos acesso local, bloqueando alguns Sites, Palavras e Extensões de arquivos para Download, exceto alguns IP's que estão liberados.

O Windows Server será bastante utilizado quando os clientes forem conectar na rede Wireless, Ao solicitar a conexão Wireless será solicitado Usuário e Senha, estes usuários e senha que for solicitado, são gerenciados pelo Active Directory, será solicitado algum tipo de certificado, com o serviço “Certificado do Active Directory”, consegue fazer com que ele não obrigue o usuário final a especificar o certificado.

Ao Colocar o “Usuário” e “Senha” será mandado a solicitação pro Servidor Windows ele ira fazer a validação de seu usuário e senha, caso o usuário e senha esteja correto será atribuído um endereço IP pro Dispositivo ou Notebook etc, caso esteja incorreta não terá acesso a rede, fazendo com que o Servidor Windows Gere relatório para fazer quando o usuários Logou ou não consegui acessar por motivos de Usuário e Senha

Será disponibilizado Usuário e Senha para que possa conectar e testar a rede.

# 7 Conclusão

Com uma integração de dois servidores e possível melhorar o gerenciamento da rede com segurança e agilidade para técnicos e usuários. O objetivo de criar uma rede cabeada e wireless segura foi atingido com a utilização dos serviços citados no trabalho

Com a rede em funcionamento e implementando a virtualização de servidores é possível reduzir os gastos com hardware para servidores e dessa forma mantem a qualidade do serviço fornecido para o gerenciamento dos computadores e da rede de computadores, mas é necessário ter um hardware compatível para virtualização.

Atualmente é raro ver esse tipo de integração, pois muitos não possuem conhecimento para implementar essa estruturação de servidores de forma correta para o gerenciamento da rede de computadores,

Sendo assim, esse Projeto visa renovar as redes empresariais de Pequeno e Médio Porte.

# 8 Referencias

Carlos.E Morimoto (11/04/2008) http://www.hardware.com.br/tutoriais/historia-redes/ .Acesso em (10/05/2016)

Equipe Microsoft https://technet.microsoft.com/pt-br/windowsserver/dd448603.aspx Acesso Em **(**10/04/2016)

Equipe Microsoft https://technet.microsoft.com/pt-br/library/hh831683.aspx Acesso Em (10/04/2016)

Equipe Dell http://www.dell.com/learn/br/pt/brbsdt1/sb360/what-is-a-server Acesso Em (24/042016)

Emerson Alecrim (19/02/2013) http://www.infowester.com/firewall.php Acesso Em (11/04/2016)

Vinicius Muniz (1/11/2014) http://viniciusmuniz.com/o-que-e-iptables-para-que-server-como-usar/ Acesso Em (28/03/2016)

Gleydson Mazioli da Silva (05/09/2010) http://www.guiafoca.org/cgs/guia/avancado/ch-fw-iptables.html Acesso Em (28/03/2016)

Jonathan D. Machado (21/06/2012) http://m.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm Acesso Em (12/04/2016)

Ana Paula Pereira (12/05/2009) http://m.tecmundo.com.br/2079-o-que-e-dhcp-.htm Acesso Em (22/03/2016)

Carlos E. Morimoto (26/08/2006) http://www.hardware.com.br/tutoriais/dominando-ssh/ Acesso Em (15/04/2016)

Marinho Rover (Junho 2012) https://technet.microsoft.com/pt-br/library/jj206711.aspx Acesso Em (19/04/2016)

Italo Diego Teotonio (27/02/2010) https://www.vivaolinux.com.br/artigo/Squid-Configuracao-basica-funcional-e-limpa Acesso Em (27/05/2016)