FACULDADES INTEGRADAS TORRICELLI

Tecnologia em Redes de Computadores

PIPA – “Projeto Integrado de Pesquisa Acadêmica”

Guarulhos

2010

FACULDADES INTEGRADAS TORRICELLI

Tecnologia em Redes de Computadores

PIPA – Projeto Integrado de Pesquisa Acadêmica em Redes de Computadores das Faculdades Integradas Torricelli, para a conclusão do 4º semestre do curso.

Orientador: Profº Mestre Nelson Aguiar

Guarulhos

2010

SUMÁRIO

1. Resumo 4
2. Introdução 5
3. Consultoria 6
3.1. Proposta e contrato 6
4. Descrição do negocio da empresa 7
4.1. Estrutura organizacional da empresa 7
4.2. Estrutura atual da empresa 7
4.3. Cenário da empresa. 9
4.4. Topologia atual 11
5. Solução 13
5.1.Equipamentos e estações 13
5.2. Sistema operacional - servidor 13
5.2.1. Especificações técnicas dos servidores 13
5.3. Serviços instalados nos servidores 15
5.3.1. Backups 15
5.3.2. Software backup 16
5.3.3.Banco de dados. 16
5.3.4.Aplicação e impressão 17
5.3.5.Serviço de permissão, DNS, email 17
5.3.6. Servidor firewall e proxy 17
5.4. Sistema operacional - desktop 18
5.5. Link de comunicação 18
5.6. VPN 19
5.7. Implementação do Voip 19
5.8. ERP 21
6. Alteração cenário 22
6.1 Topologia externa geral 23
6.2 Topologia interna das unidades 24
7. Tabela ip 25
8. Projeto de segurança de rede 33
8.1. Politica de segurança 33
8.1.1. Contas 33
8.1.2. Senhas 34

8.1.3. Modelo do termo de responsabilidade 35
8.1.4. Firewall 38
8.1.5. Proxy 38
8.1.6. Backup 38
8.1.7. Segurança física 38
8.1.8. Segurança lógica 39
9. Cotação do projeto 40
10. Pesquisa academica 41
10.1. Raid 42
10.1.1. Tecnologia Raid 42
10.1.2. Implementações Raid 43
10.1.3. Niveis de Raid 44
10.2. NAS. 45
10.3. SAN 46
10.4. Segurança em redes TCP/IP 50
10.5. Vpn 50
10.6. Politica de segurança 51
10.6.1. Firewall 52
10.6.2. Filtros 52
10.6.3. Proxy 52
10.6.4. Bastion host 53
10.6.5.DMZ. 53
11.Conclusão 54
12. Bibliografias e referencias 55

1. Resumo

A empresa Viagem Certa do ramo de turismo visa uma adequação em sua estrutura física no setor de tecnologia da informação tendo como objetivo principal a integração de suas novas unidades adquiridas. Através de um projeto elaborado pela consultoria Zinigem será aplicado na área de informática, um conceito de software livre focando a diminuição de custos e também otimizando todo o processo de comunicação da empresa através de tecnologias que proporcionam rapidez e facilidade de uso.

2. Introdução

A implementação de um projeto requer todo o custo material e pessoal para a implementação do mesmo, é necessário na maior parte das vezes a compra de novos equipamentos e a contratação de pessoal especializado para instalação, configuração de equipamentos, servidores e outros equipamentos da rede e o projeto sempre visa corrigir falhas existentes no intuito de diminuir custo.

Esse projeto tem como objetivo através de um trabalho de consultoria apresentar soluções para integração da rede da empresa com foco na comunicação que é de grande importância para uma empresa de turismo.

3. Consultoria

Para desenvolver o projeto de integração de redes a nossa consultoria ZINIGEM foi contratada para elaborar proposta de reestruturação da agência Viagem Certa.

Diante da estrutura atual a ZINIGEM elaborou um projeto de adequação e modernização das tecnologias utilizadas de forma que o funcionamento da agência seja da forma que traga custo baixo e eficiência alta.

A Zinigem se reserva o direito de não se responsabilizar por:

1-Qualquer serviço não especificado nesta proposta.
2- Montagem de ambientes não previstos nesta proposta.

3- Instalação de softwares não previstos nesta proposta.
4-Integração com sistemas ou bases de dados fora do ambiente de desenvolvimento.

5-Solução de problemas técnicos causados por uso incorreto, que venham a gerar problemas no sistema.
6-Serviços de rede elétrica

3.1. Proposta e Contrato

A Zinigem apresentará a proposta com o projeto sobre a reestruturação da agência Viagem Certa, com os custos devidamente especificados de forma clara e concisa.

A Zinigem instalará os serviços e prestará serviço de suporte para que o funcionamento dos sistemas sejam correto e de forma otimizada.

Caso a proposta seja aprovada será apresentado o contrato com todos os termos necessários para realização do projeto.

4. Descrição do negócio da empresa

A empresa de turismo Viagem Certa com sede em São Paulo tendo filiais na cidade do Rio de Janeiro, Belo horizonte, e Curitiba conta atualmente com 104 funcionários (sendo 26 em cada unidade); a empresa que está em um processo de expansão acaba de adquirir mais dois prédios na cidade de Florianópolis e Porto Alegre, que contam com 68 funcionários (34 em cada unidade).

Com as aquisições a nossa empresa de consultoria foi contratada para fazer o processo de integração da rede e verificação de possíveis melhorias em todo o processo.

Atualmente o ramo de turismo é um dos ramos que mais cresce no Brasil, tornado uma área de aspecto fundamental para economia, com essa demanda a Viagem Certa está integrando suas redes para tornar-se uma agência com abrangência nacional.

4.1. Estrutura organizacional da empresa

A estrutura organizacional da Viagem Certa e basicamente à mesma nas unidades de São Paulo, Rio de janeiro, Belo Horizonte e Curitiba e está disposta com os seguintes setores:

-Secretaria, pacotes especiais, passagens internacionais, passagens nacionais, compra e venda financeiro, Rh, dono, diretoria, ti.

Já nos prédios adquiridos em Porto Alegre e Florianópolis está disposta com os seguintes setores:

- secretaria, telemarketing, Venda Passagens nacionais, compra, ti, diretor, Rh, financeiro

4.2. Estrutura atual da empresa

A empresa Viagem Certa tem em sua matriz em São Paulo a centralização dos dados. Os 2 servidores da empresa ficam na matriz, sendo que 1 servidor está trabalhando com o Domínio, Banco de dados e internet e o outro está sendo utilizado para backup.

O sistema operacional do servidor utilizado é o Windows 2003 Server, as máquinas utilizadas tanto na matriz como nas filiais do Rio de Janeiro, Belo Horizonte e Curitiba

são dual core com 2 GB de memória RAM, 250 Gb de HD e também com cd ROM, sendo o sistema operacional o Windows XP.

O antivírus usado em todas as unidades e o AVG FREE.

Na matriz o cabeamento e através de piso falso, já nas filiais o cabeamento é através de canaletas externas.

Para as interligações existe em todas as unidades um roteador e um switch de 48 portas, e a comunicação entre a matriz em São Paulo e o Rio de Janeiro é realizada por um link dedicado da Telefônica de 2MB e as demais filiais se comunicam por Vpn implementada pelo Windows Server 2003.

O banco de dados da empresa é o Microsoft SQL e a empresa não utiliza ERP e sim intranet.

Nos dois prédios adquiridos em Florianópolis e Porto Alegre não há servidor, e as maquinas utilizadas são celeron com 512MB de memória RAM e 120GB de HD.

É utilizado o antivírus AVG FREE.

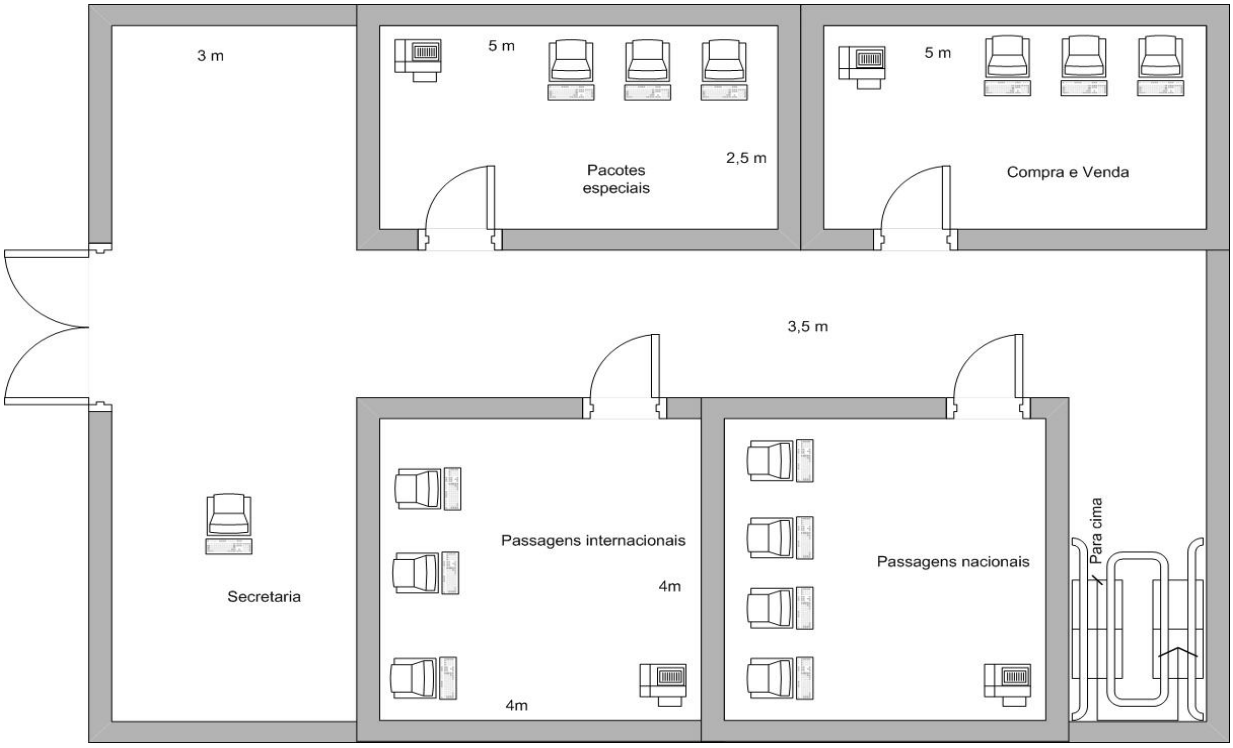
Nessas duas unidades citadas acima o cabeamento é distribuído através de canaletas externas e a comunicação entre elas e feita por um link dedicado de 2 MB da Embratel e em ambas as unidades tem 1 roteador e 1 switch de 48 portas.

Já o Backup é feito em HDs externos que somam 500 GB divididos em 4 HDs que ficam guardados na sala do diretor.

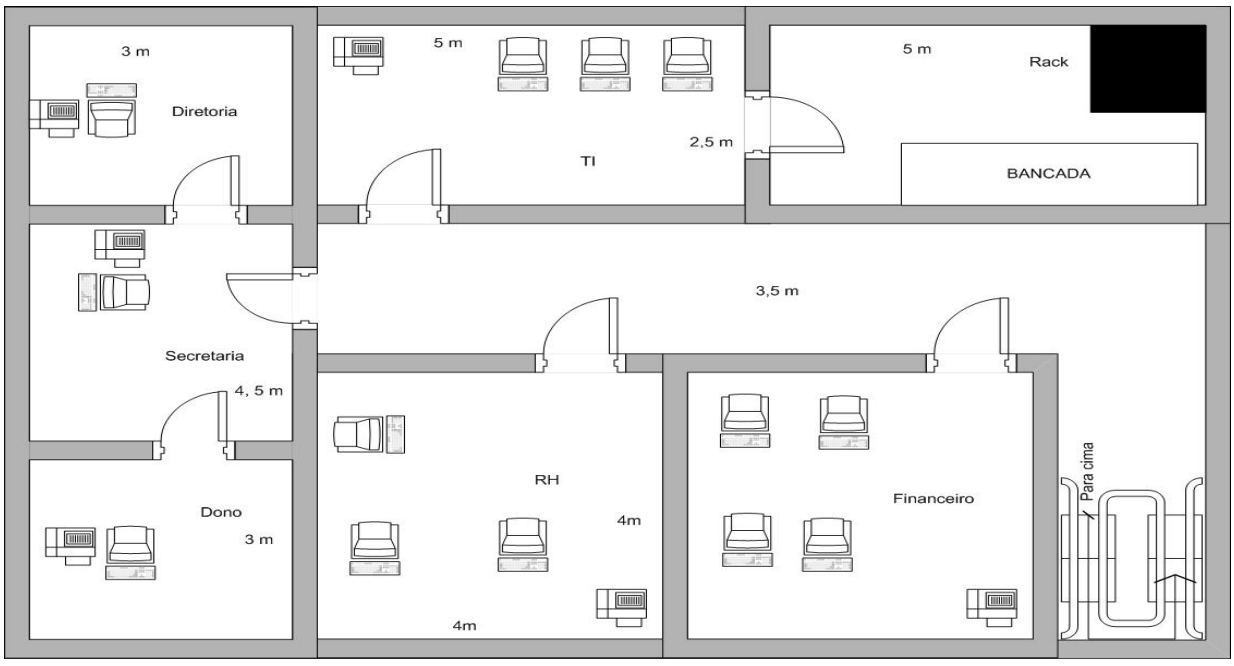
4.3. Cenário da Empresa

Unidades São Paulo, Rio de Janeiro, Belo horizonte e Curitiba.

Térreo

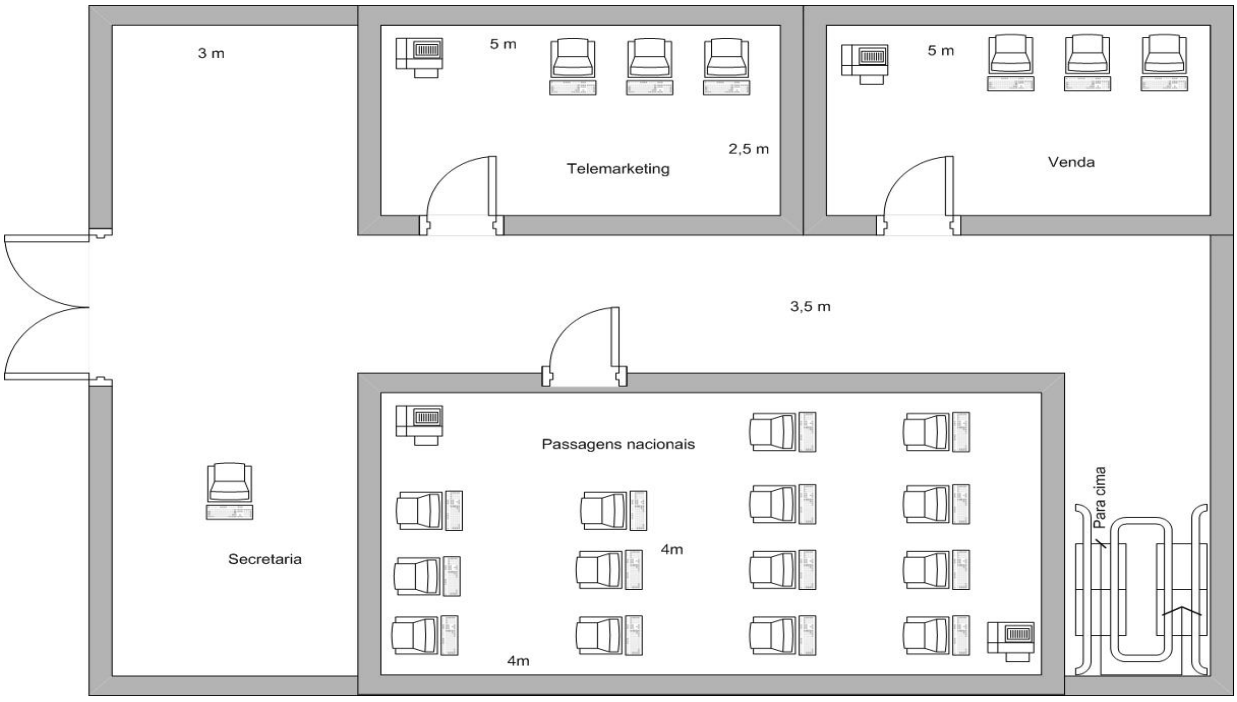


1º Andar

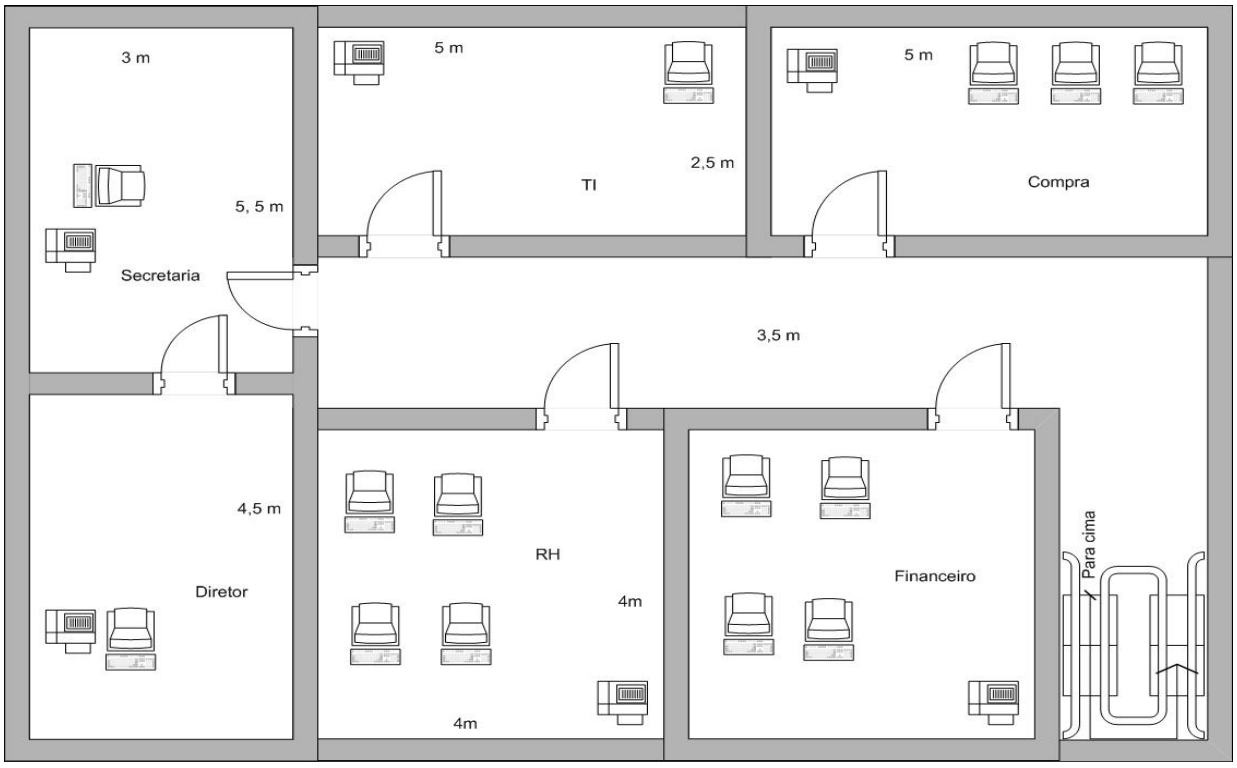


Unidades de Florianópolis e Porto alegre

Térreo

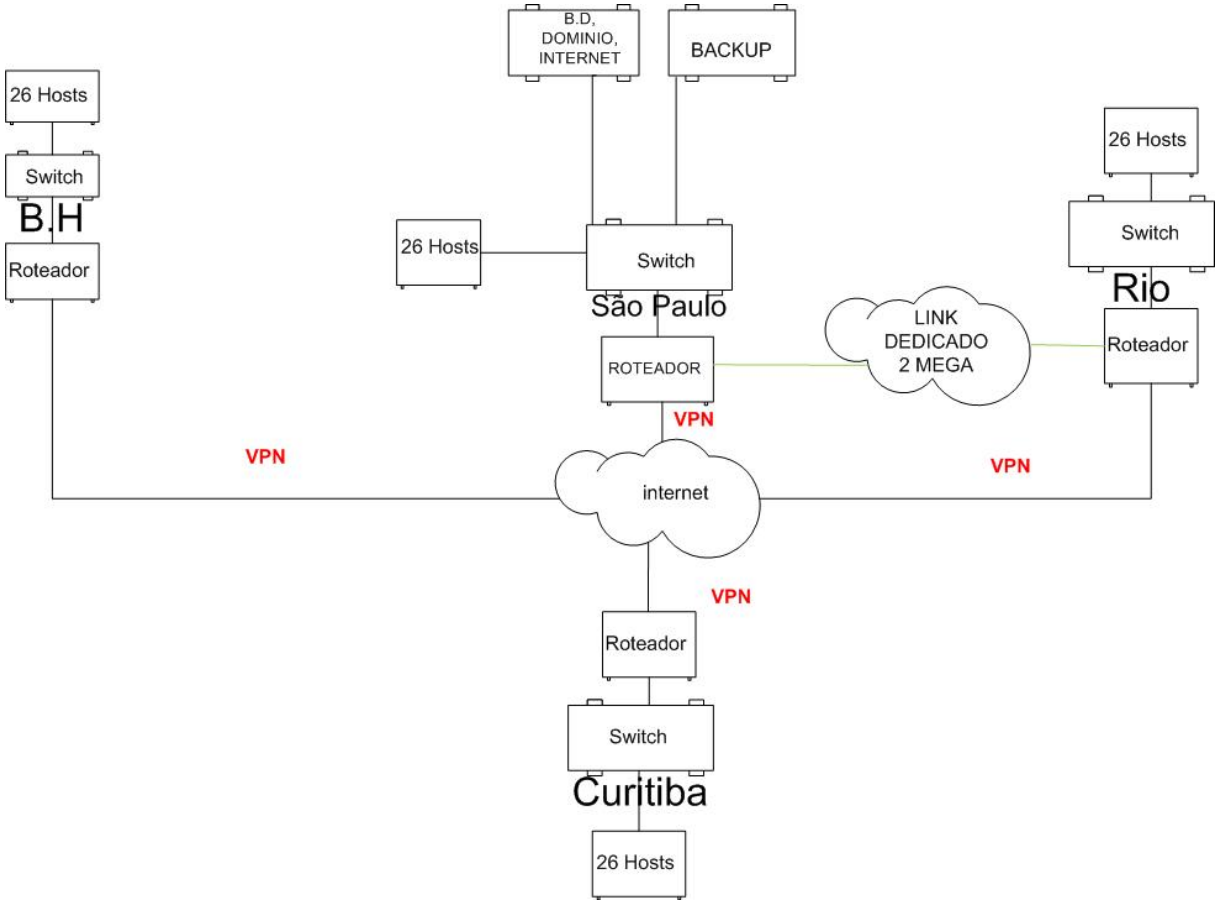


1ºandar

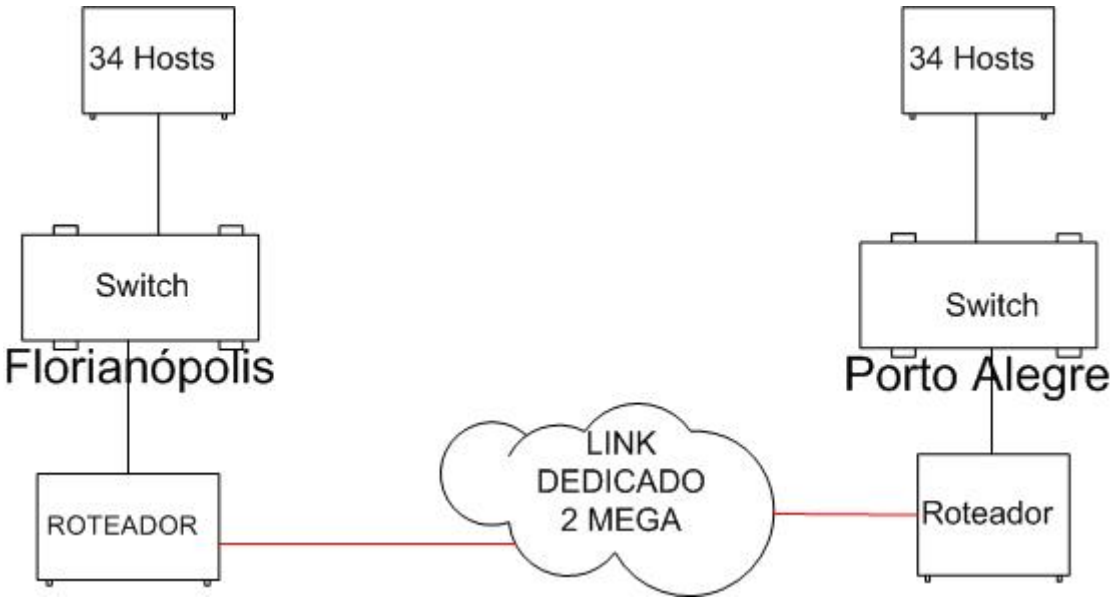


4.4. Topologia Atual

Unidades São Paulo, Rio de Janeiro, Belo Horizonte e Curitiba



Unidades Florianópolis e Porto Alegre



5. Solução

5.1. Equipamentos e estações

- Sugerimos a compra de 10 servidores (sendo 2 para cada filial) e na matriz serão mantidos os 2 servidores atuais.
- Também será solicitado a compra de 5 nobreaks (sendo 1 para cada filial), pois apenas a matriz tem nobreak.
- Sugerimos a compra de 3 hds externos, 6 racks e 172 aparelhos ip para voip.
- Os hosts em todas as unidades serão mantidas nas configurações atuais de seus hardwares.
- Em todas as unidades sugerimos a instalação de ar condicionado na sala da T.i.
- Sugerimos a compra de 6 switches para implementar os telefones voips e 6 roteadores para aplicar a dmz.
- As impressoras serão trocadas pelo fato de não terem entrada de rede, e serão sugeridas a compra de 48 impressoras e 6 multifuncionais.
- O cabeamento das unidades será mantido.

5.2. Sistema Operacional - Servidor

O sistema operacional dos servidores sugerimos a utilização do Fedora 12 pelo fato de necessitarmos de soluções em gerenciamento de arquivos na Rede.

Com o Fedora, os serviços na matriz estarão distribuídos em 2 servidores, sendo 1 servidor com maior processamento para a utilização do banco de dados sendo implementado RAID 5 com 3 hds de 1TB cada um, e o outro com menor processamento sendo utilizado para os demais serviços.

Novas regras, relatórios e controle de acesso também serão implementados com os Grupos de usuários, cada grupo com suas permissões.

5.2.1.Especificações técnicas dos servidores

Na matriz em São Paulo indicaremos 2 servidores:

1º Servidor:

Dell t610 11g

Processador xeon quad core

8 Gb de RAM

3 hds 1 tera cada sata ii

Placa de rede gigabit

5 pcie Generation 2

Raid físico

Interno

PERC H700 (6 Gbit/s) com 512 MB de cache não volátil

Externo

PERC H800 (6 Gbit/s) com 512 MB de cache não volátil

Fonte

Duas psus de 570 W (Energy Smart) redundantes e de conexão automática ou duas psus de 870 W (alta saída)

DISPONIBILIDADE

ECC; memória DDR3; discos rígidos de conexão automática; fontes de alimentação redundantes opcionais; placas de rede de porta dupla incorporadas com suporte para failover e balanceamento de carga; controlador de placa auxiliar integrado PERC6/i opcional com cache alimentado por bateria; sistema de resfriamento redundante; chassi acessível sem ferramentas; suporte para cluster SAS e fibre channel; validado para SAN Dell/EMC

2º Servidor:

Dell t110

Processador xeon quad core

RAM 6Gb

2 hds 500 Gb cada

Fonte

Duas psus de 570 w (energy smart) redundantes e de conexão automática ou duas psus de 870 w (alta saída)

Placa de rede gigabit

Controladores raid

Controladores internos:

SAS 6/iR PERC S100 (baseado em software)

PERC S300 (baseado em software)

Controladores externos:

HBA SAS de 6 Gbit/s

SAS 5/E

HBA PCIe SCSI LSI2032

Em todas as demais unidades serão utilizados servidores com a configuração igual ao 2º servidor de São Paulo demonstrado acima, este servidor utiliza raid 1.

5.3. Serviços instalados no Servidor

A seguir teremos as definições básicas dos serviços que serão utilizados para a realização do projeto.

5.3.1. Backups

O backup dos dados da empresa será feito em duas etapas:

- Backup Centralizado. Todos os dias, após o expediente, os dados administrativos das filiais serão enviados e centralizados na matriz, já os demais dados será feito o backup de 3 em 3 dias. O backup central será feito em horário agendado pelo software open source bacula.

Estes dados serão gravados no servidor da matriz e o Backup através do software bacula será feito em hds externos.

Os Backups serão do tipo incremental, onde serão gravados apenas os arquivos que foram alterados depois do último backup. Os horários dos backups serão determinados de acordo com o melhor momento para que este não interfira no desempenho da Rede.

5.3.2. Software Backup

As informações de uma empresa compõem seu ativo mais valioso e podem ser perdidas acidentalmente, seja por falha física, ou por falha humana, a qualquer momento, por isso sugerimos o uso de um software livre Bacula para centralização de backup.

Vantagens de um sistema de Backup Centralizado (viabilizado pelo Bacula):

- Economia do espaço subutilizado.
- Facilidade na administração, correção de erros, troca e controle de mídias.
-Economia de hardware (storages).
- Maior agilidade (time sharing).
- Facilidade no restore (catálogo único)

Quaisquer bancos de dados relacionais com uma única base de código podem utilizar bancos de dados livres ou proprietários como catálogos de metadados do Bacula.

5.3.3. Banco de Dados

O banco de dados será reestruturado, e utilizaremos o MySQL opensource. Este Banco de dados será acessado pelos principais aplicativos utilizados na empresa. Para ser acessado, o usuário precisará de uma conta com permissão, assim como o os serviços de arquivos.

O banco de dados ficará centralizado na matriz, através de configuração ip via vpn às demais filiais serão integradas ao banco de dados e assim ao fazer o login no erp, à filial em questão terá disponíveis os dados necessários para seu pleno funcionamento. Como exemplo seria configurado assim:

São Paulo - Matriz

Rio – filial 1, Belo horizonte – filial 2, Curitiba – filial 3, Florianópolis – filial 4, Porto Alegre – filial 5

5.3.4. Aplicação e impressão

Os serviços de aplicação conterão todos os principais programas utilizados pela empresa. O serviço utilizado para gerenciamento dos aplicativos será o do próprio sistema operacional, Fedora 12 de acordo com as permissões de acesso de cada usuário. O próprio Fedora 12 irá controlar também as impressões, através de seu serviço de impressão de acordo com as permissões nele configurado.

5.3.5. Serviços de permissão de usuário, DNS, e-mail.

Para todos esses serviços será utilizado quotas de usuário e domínio de resolução de nomes por setores, devidamente configurado para um desempenho correto e otimizado.

5.3.6. Servidor Firewall e Proxy

Para a segurança da empresa instalaremos os servidores de Firewall e Proxy.

Para que isso seja possível será implementado também os serviços de Firewall e Proxy que podem ser configurados controles de pacotes na rede que será permitido ou não, dependendo do grupo o qual um usuário está vinculado. Para isso será instalado como proteção um servidor de Firewall, Proxy com o serviço (software) Squid e o Firewall Iptables.

Squid é um ProxyCache de alta performance para clientes Web, suportando protocolos FTP e HTTP. O Squid mantém meta dados e especialmente objetos armazenados em sua memória RAM, cacheia buscas de DNS e implementa cache negativo de Requests falhos, suporta SSL, listas de acesso complexas e login completo. Por utilizar o Internet Cache Protocol, o Squid pode ser configurado para trabalhar de forma hierárquica ou mista para melhor aproveitamento da banda.

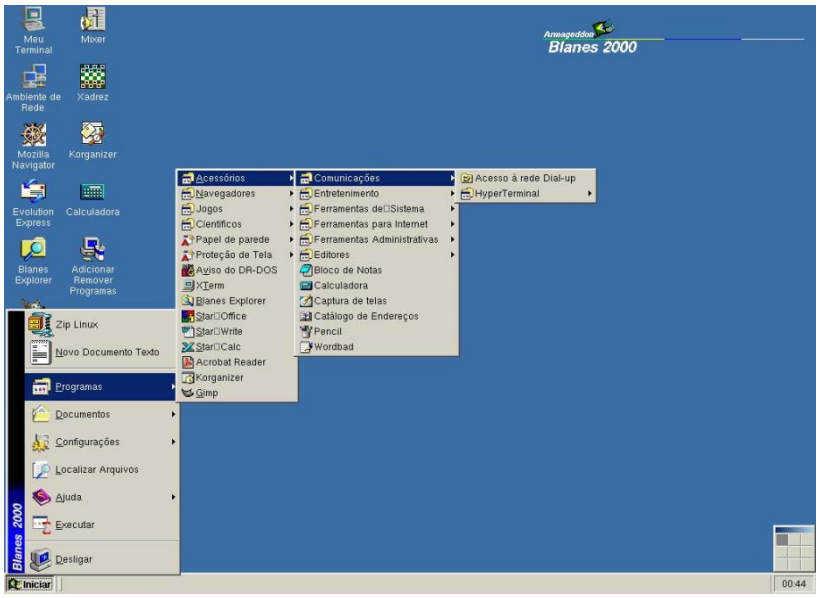
5.4. Sistema Operacional – Desktops

Nas maquinas em todas as unidades serão instalados o sistema operacional Debian com o gerenciador de janela Blane.

Com esse sistema instalado que se caracteriza pelo fato de não necessitar de maquinas com hardware super potentes, por esse motivo continuaremos com as maquinas existentes em todas as unidades.

O fato de o Debian com o gerenciador de janela Blane ter uma aparência amigável aos usuários também foi um dos motivos preponderantes para sua escolha.

Abaixo imagem da tela do Debian com visual semelhante ao Windows 2000:



5.5. Link de comunicação

A conexão entre a matriz em São Paulo e a filial do Rio de janeiro continuará sendo feita através de um link dedicado devido ser as unidades que mais geram fluxo de dados.

As filiais de Belo horizonte e Curitiba continuarão se comunicando com a matriz através de Vpn.

As duas unidades adquiridas em Porto Alegre e Florianópolis se conectaram com a matriz em São Paulo através de VPN e o link dedicado entre as unidades não será mais utilizado provendo economia.

Sugerimos a compra da solução adsl da Embratel de 20 MB para a internet nas unidades, sendo o link de 2mb existente utilizado para redundância.

5.6. VPN

O software a ser implementado para este serviço será o software livre muito utilizado no mercado que é o OPENVPN que permite autenticação dos usuários, maior segurança e criptografia de dados.

Para a implementação da Vpn é utilizado o roteador:

Cisco RV042 Dual WAN VPN Router

• Duas conexões WAN para balanceamento de carga e redundância de conexão
• Ethernet switch
• Funcão DMZ
• Built-in 4 portas 10/100
• Total IPsec VPN capacidades para até 50 conexões remotas
• Advanced firewall de inspeção de pacotes ajuda a manter sua rede segura
• DMZ zone, Ghost zone.

5.7. Implementação do Voip

O Voip será implantado com 26 pontos na matriz e 26 pontos nas filiais de Belo Horizonte, Rio de Janeiro e Curitiba, já nas unidades de Florianópolis e Porto Alegre serão implementados 34 pontos.

O Software utilizado será o Asterisk de código aberto, que implementa em software os recursos encontrados em um PABX convencional, utilizando tecnologia de Voip.

O Asterisk apresenta as seguintes vantagens:

• Interligar ramais entre sua matriz e filiais;

• Transferência de chamadas;

• Conferência;

• Gravar a conversa;

• Ramal Virtual: todos os usuários podem utilizar suas contas em qualquer lugar, para receber chamadas;

• Call balance (serviço de chamadas não atendidas);

Serão utilizados telefones Ips para a comunicação, o modelo será:

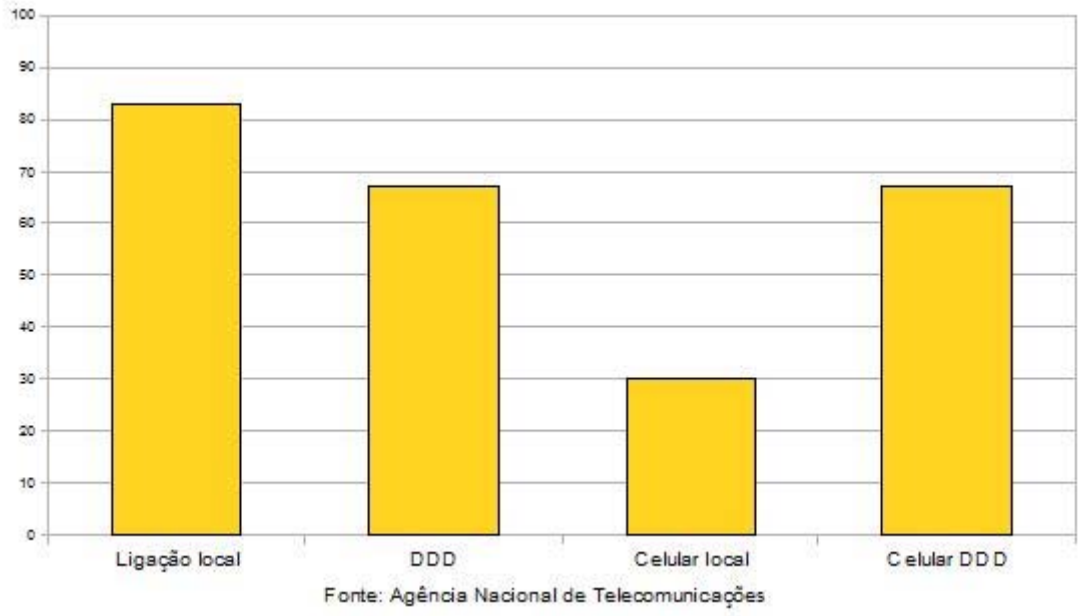
Telefone Grafite Force Lineu

O telefone híbrido - fixo e internet - para chamadas sem uso de computador

• Telefone híbrido para chamadas pela rede fixa e pela internet;
• Não é necessário o uso de um computador nem de programas instalados para funcionar;
• Multilinhas para até 6 contas SIP (VoIP);
• Identificador de chamadas (CLIP);
• Display e teclado iluminados;
• Agenda para até 100 registros;

Serão contratado um pacote da empresa Vono de 1300 minutos para ligação para fora das unidades.

O Voip traz uma grande redução de custos, veja tabela abaixo:



Fonte: Agência Nacional de Telecomunicações

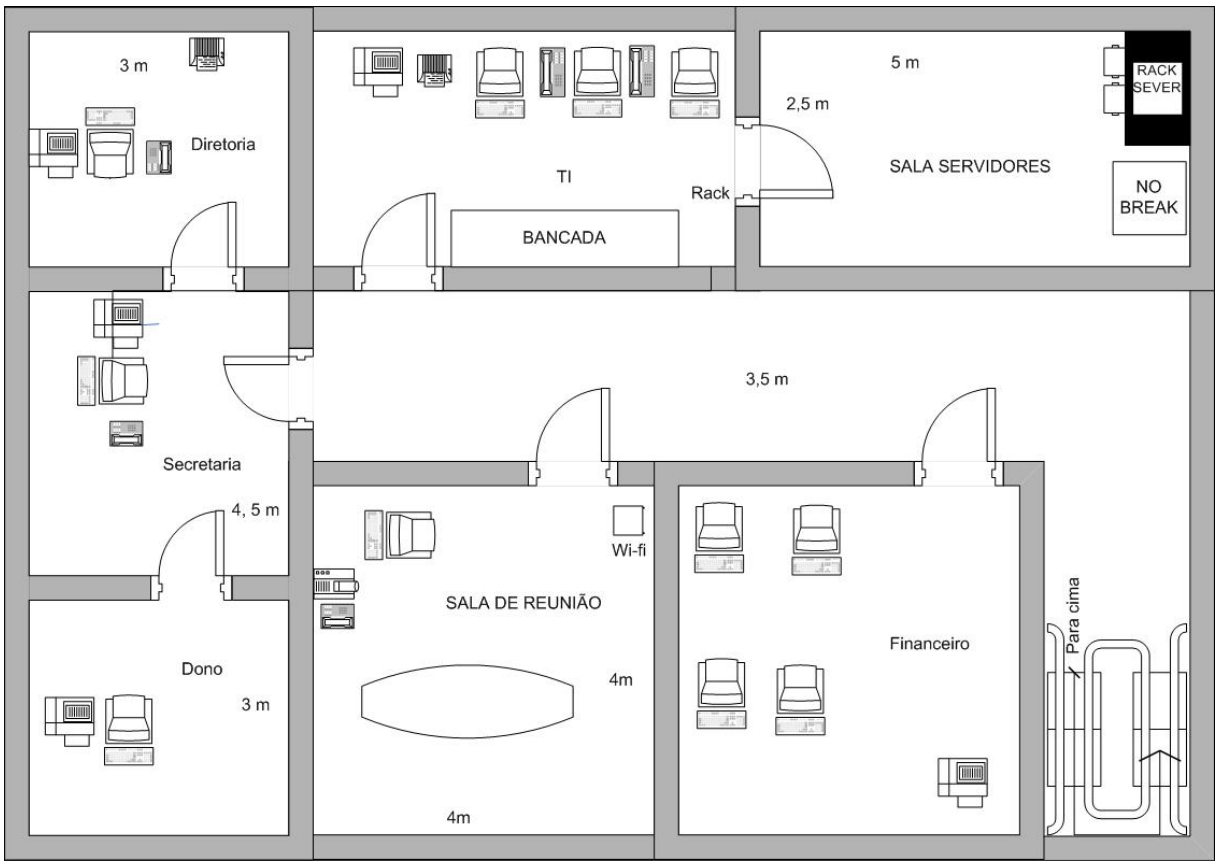
5.8. ERP

Para gerenciar e integrar os processos de gestão da empresa sugerimos a solução Open ERP, pois é dinâmica, racional e eficiente, e prepara a companhia para administrar processos e recursos na busca de integração de informações. A adoção da solução Open ERP elimina o uso de interfaces manuais e a redundância de atividades, proporcionando integração de diversos departamentos, automatização e armazenamento de todas as informações de negócios.

Estaremos utilizando os módulos de RH, financeiro, administrativo e compras e vendas.

6. Alteração cenário

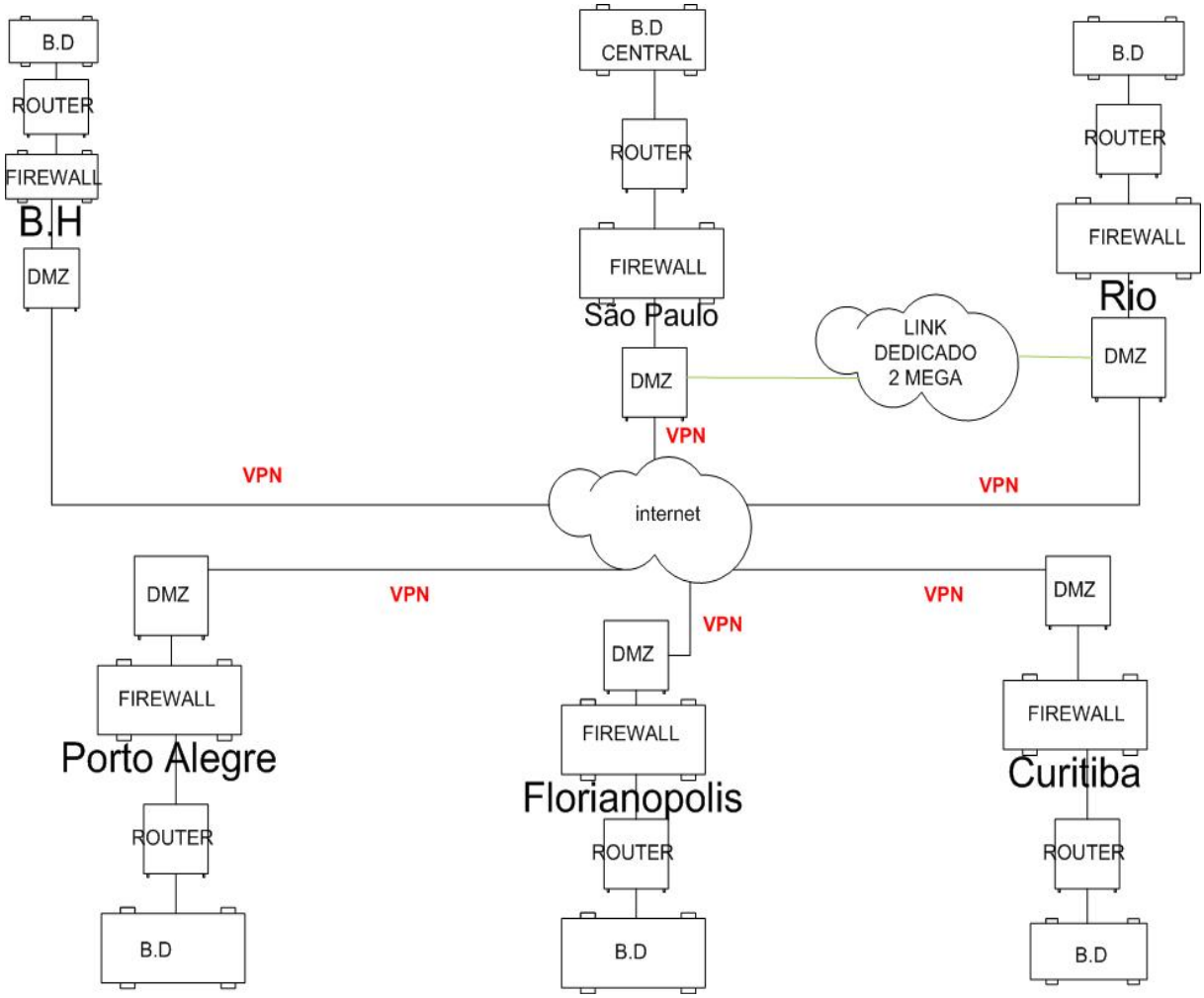
Abaixo está demonstrado a alteração do cenário das filiais em seu 1º andar.



Nessa alteração o RH que está nas filiais é substituído por uma sala de reunião que terá a disposição internet wi- fi e um projetor para auxiliar nas atividades recorrentes.

O Rh portanto ficará situado apenas na matriz.

6.1 Topologias externa geral



6.2 Topologia interna das unidades

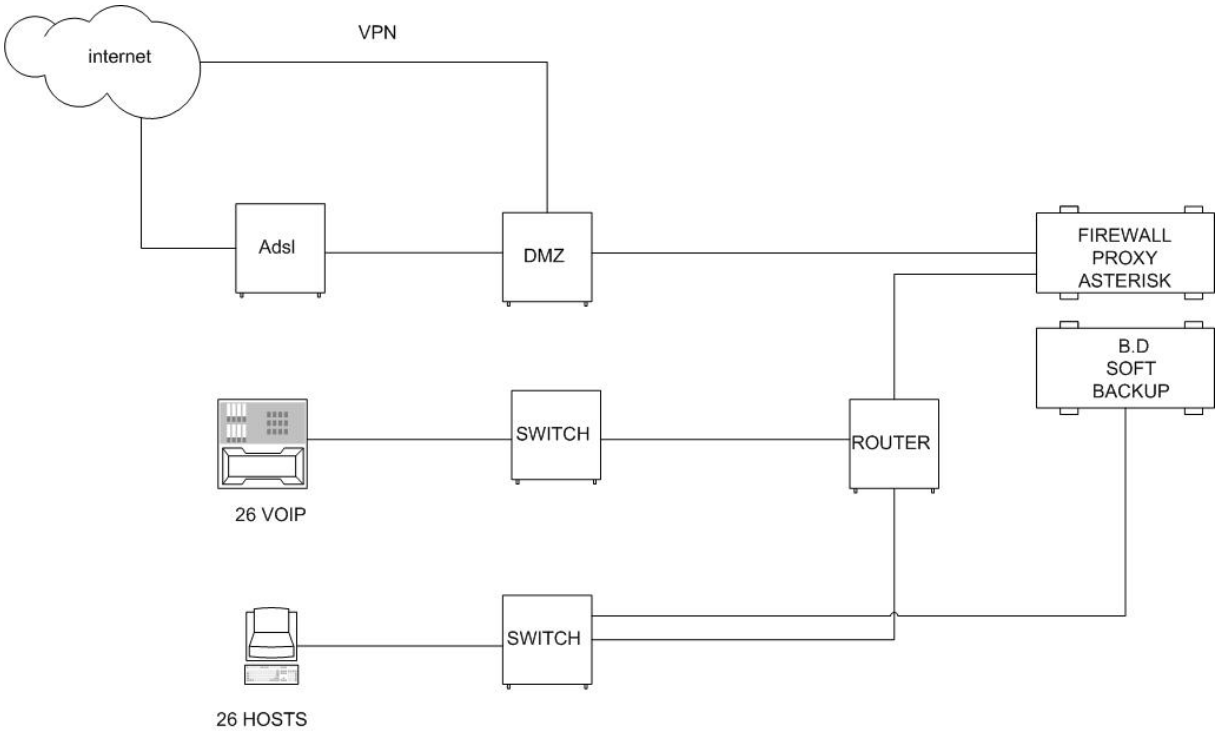


Tabela IP

Matriz

rede: 200.0.0.0

broadcast: 200.0.0.255

gateway: 200.0.0.254

máscara: 255.255.255.0

Servidor Firewall Proxy Dns

ip: 200.0.0.1

Servidor Banco de dados

ip: 200.0.0.2

Diretoria

host: diretoria

200.0.0.6

impressora

200.0.0.253

Secretaria diretoria

host: sec_dir

200.0.0.7

impressora

200.0.0.252

Dono

host: dono

200.0.0.8

impressora

200.0.0.251

T.I

host: infra_01

200.0.0.3

host: infra_02

200.0.0.4

host: helpdesk

200.0.0.5

impressora

200.0.0.250

R.H

host: rh_01

200.0.0.9

host: rh_02

200.0.0.10

host: rh_03

200.0.0.11

impressora

200.0.0.499

Financeiro

host: fin_01

200.0.0.12

host: fin_02

200.0.0.13

host:fin_03

200.0.0.14

host:fin_04

200.0.0.15

impressora

200.0.0.498

Secretaria geral

host: sec_geral

200.0.0.15

Pacotes especiais

host: especial_01

200.0.0.16

host: especial_02

200.0.0.17

host: especial_03

200.0.0.18

impressora

200.0.0.247

Compra e Venda

host: comp_01

200.0.0.19

host: comp_02

200.0.0.20

host: comp_03

200.0.0.21

impressora

200.0.0.246

Passagens internacionais

host: inte_01

200.0.0.22

host: inte_02

200.0.0.23

host: inte_03

200.0.0.24

impressora

200.0.0.245

Passagens nacionais

host: naci_01

200.0.0.25

host: naci_02

200.0.0.26

host: naci_03

200.0.0.27

host: naci_04

200.0.0.28

impressora

200.0.0.244

Filial

rede: 201.0.0.0

broadcast: 201.0.0.255

gateway: 201.0.0.254

máscara: 255.255.255.0

Servidor firewall proxy dns

ip: 201.0.0.1

Servidor Banco de dados

ip: 201.0.0.2

Diretoria

host: diretoria

201.0.0.6

impressora

201.0.0.253

Secretaria diretoria

host: sec_dir

200.0.0.7

impressora

201.0.0.252

Dono

host: dono

200.0.0.8

impressora

201.0.0.251

T.I

host: infra_01

201.0.0.3

host: infra_02

201.0.0.4

host: helpdesk

201.0.0.5

impressora

201.0.0.250

Sala de reunião

host: reunião

201.0.0.9

Financeiro

host: fin_01

201.0.0.10

host: fin_02

201.0.0.11

host:fin_03

201.0.0.12

host:fin_04

201.0.0.13

impressora

201.0.0.249

Secretaria geral

host: sec_geral

201.0.0.14

Pacotes especiais

host: especial_01

201.0.0.15

host: especial_02

201.0.0.16

host: especial_03

201.0.0.17

impressora

201.0.0.248

Compra e Venda

host: comp_01

201.0.0.18

host: comp_02

201.0.0.19

host: comp_03

201.0.0.20

impressora

201.0.0.247

Passagens internacionais

host: inte_01

201.0.0.21

host: inte_02

201.0.0.22

host: inte_03

201.0.0.23

impressora

201.0.0.246

Passagens nacionais

host: naci_01

201.0.0.24

host: naci_02

201.0.0.25

host: naci_03

201.0.0.26

host: naci_04

201.0.0.27

impressora

201.0.0.245

As outras filiais serão as redes em 202.0.0.0, 203.0.0.0, 204.0.0.0 e 205.0.0.0

por questões de segurança foi designado ips de numeração mais alta.

8. Projeto de segurança da rede

Um projeto de segurança requer todo um estudo, pois é cada vez mais comum o ataque as empresas em busca de dados relevantes que possam ser utilizados de forma a prejudicar o desempenho da rede.

A proteção tem que ser de forma uniforme, pois além de se proteger de ataques de hackers, ataques externos ou mesmo internos não estaremos implementando um boa política de segurança se deixarmos qualquer pessoa acessar nossa rede ou mesmo fazer uso indevido de serviços indesejados ou fazer mau uso dos recursos.

8.1. Política de segurança

Serão estabelecidas as seguintes políticas de segurança para os funcionários da agência Viagem Certa.

O uso da conta e senha de autenticação é obrigatório para que o funcionário tenha acesso à rede e aos recursos computacionais.

As senhas são de caráter pessoal e intrasferível, nenhum funcionário poderá fornecer a sua senha de acesso a terceiros para que tenham acesso à rede, caso isto aconteça o funcionário deverá sofrer uma penalidade de acordo com as normas da empresa.

Cada funcionário deverá efetuar o logoff da maquina em que estiver trabalhando após terminar a sua tarefa.

O acesso a sites indevidos e conteúdos inapropriados são proibidos, como jogos on-line, bate papo (exceto o setor de marketing e vendas), sites com conteúdo pornográficos, e páginas de origem duvidosas.

Os usuários deverão trocar suas senhas caso haja desconfiança que a sua senha tenha sido descoberta ou reportar ao administrador da rede.

8.1.1. Contas

Por questão de segurança e bom funcionamento da rede fica incumbido à total responsabilidade do administrador e funcionários de informática a criação e gerenciamento das contas de usuários.

Serão criadas contas de usuários baseadas no setor em que usuário trabalha.

As contas de funcionários da empresa serão criadas com os sobrenomes de cada funcionário seguido das iniciais do nome completo, caso haja funcionários com sobrenomes e iniciais idênticas serão acrescidas uma numeração em ordem crescente.

Os usuários terão que assinar um termo de responsabilidade de acesso e ficarem cientes de que estão sendo monitorados.

Para funcionários que forem demitidos serão bloqueadas as suas contas no ato da demissão.

As contas dos funcionários licenciados serão periodicamente suspensas até que o funcionário retorne ao trabalho de forma efetiva.

8.1.2. Senhas

As senhas por padrão deverão ter um mínimo de 6 caracteres. Será aconselhado o não uso de senha de fácil dedução como data de nascimento, CPF, número do celular, etc.

A atribuição de senhas para os funcionários ficará a critério dos funcionários a digitação de sua senha pessoal, mas seguindo o padrão da empresa, usando números, letras maiúsculas e minúsculas.

Abaixo o termo de responsabilidade sobre uso da rede corporativa, sobre sigilo de logins e senhas.

8.1.3. Modelo do termo de responsabilidade

TERMO DE RESPONSABILIDADE

Política de Uso da rede corporativa, computadores, Internet e/ou utilização de e-mails corporativos.

Eu, __________

Setor: _____**Função**: _____

CPF: _____ **Identidade**: _____

Matricula: _____ **Ramal**:_____

User ID da rede corporativa: _____, **Declaro haver solicitado acesso a rede corporativa, computadores, Internet e/ou utilização de e-mail e me comprometendo a:**

a) Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege o acesso a rede corporativa, computadores, Internet e/ou utilização de e-mail;

b) Utilizar a caixa postal (e-mail) colocada a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege o acesso a rede corporativa, computadores, Internet e/ou utilização de e-mail;

c) Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

d) Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

e) Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador, bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

f) Não revelar minha senha de acesso a rede corporativa, computadores, Internet e/ou de minha caixa postal (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

g) Responder, em todas as instâncias, pelas conseqüências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro, ainda, estar plenamente esclarecido e consciente que:

1) Não é permitida a navegação em sites pornográficos, defensores do uso drogas, de Pedofilia ou sites de cunho racistas e similares;

2) É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade das informações contidas em minha caixa postal (e-mail), devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas no sistema de correio, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

3) O acesso à informação de minha caixa postal (e-mail) não me garante direito sobre ela, nem me confere autoridade para liberar acesso a outras pessoas, pois se constitui informações pertencentes da Agência Viagem Certa uma vez que faço uso para melhor desempenhar minhas atividades administrativas;

4) Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos por meio do uso de minha caixa postal (e-mail) ao qual tenho acesso para outros servidores não envolvidos nos trabalhos executados;

5) Devo alterar minha senha, sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

6) Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

7) Cumprir e fazer cumprir os dispositivos da Política Corporativa de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade.

Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional a revelação de segredo do qual me apropriei em razão do cargo. Sendo crime contra a administração

Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que habilitado;

Constitui infração funcional e penal enviar ou facilitar o envio por terceiros de e-mails falsos, ficando o infrator sujeito a punição com a demissão, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-A e 313-B, do Código Penal Brasileiro (Decreto-Lei 2.848, de 1940).

Declaro, **nesta data,** ***ter ciência e estar de acordo*** **com os procedimentos acima descritos**, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

_____ _____

(nome do usuário / Matricula / CPF)

_____ _____

(Administrador de NTI / Matricula / CPF)

Este documento deve ser assinado em 02 (duas) vias – 1ª via arquivo CPD, 2ª Via usuário.

8.1.4. Firewall

O firewall irá aplicar os controles exigidos pela política de segurança da empresa. Além de fazer o controle de acesso, interligando de forma segura as redes garantido o controle, a verificação e log dos pacotes entre ambas.

8.1.5. Proxy

Juntamente com o firewall, instalaremos o Proxy, que atua como intermediário entre a rede interna da Agência Viagem Certa e a internet. Ele interrompe a conexão entre o host da LAN e da internet, estabelecendo duas novas conexões.

Uma entre o host da LAN e ele próprio e outra entre ele e a internet, fazendo a checagem se ele pode fazer ou não o forward dos pacotes. Em caso negativo ele descarta a conexão. Com o Proxy a rede da Agência Viagem Certa terá um ganho de desempenho no acesso à internet, uma vez que o Proxy possui um cache e cada vez que uma pessoa acessa uma página ele guarda o conteúdo desta para posteriores acessos.

Outro ganho é com a relação à segurança, pois com o Proxy nós restringiremos página de conteúdos impróprios do tipo páginas de sexo, pornografia, bate papo, entre outros.

8.1.6. Backup

O Backup é um fator fundamental na segurança, pois é necessário ter a cópia das informações importantes em dispositivos adicionais e em locais seguros para garantir a continuidade do negócio em caso de desastres e falhas técnicas nos equipamentos.

Para a realização do Backup será destacado um funcionário da T.I, que terá a tarefa de realizar o backup e armazená lo.

8.1.7. Segurança Física

Não será permitida a entrada de pessoas não autorizadas na sala da T.I, que terá porta de aço e leitor de biometria par ter acesso ao ambiente citado.

Será de uso restrito aos administradores de redes o acesso aos livros de ocorrência.

Será mantida em local seguro e confiável toda a documentação relacionada ao projeto da rede que poderá ser visto apenas por pessoas autorizadas.

Equipes de segurança patrimonial devem ser avisadas sempre sobre pessoas que trabalham a noite, principalmente usando computadores. Quando acharem necessários, de vem questionar tais funcionários. Outro ponto é adotar critérios rigorosos para a contratação de empresas terceirizadas.

Manter fora da empresa em local seguro as copias de Backup para evitar que em caso de incêndio ou outro tipo desastre natural, os dados não se percam.

8.1.8. Segurança Lógica

Desabilitar os login remotos durante a noite e fins de semana (FTP, telnet)

Desabilitar contas de usuários que saíram de férias.

Estabelecer como parte do procedimento de demissão a desativação da conta.

Não permitir que funcionários instalem hardware.

Para determinadas contas, estabelecer dias e horas de uso.

Desabilitar as portas abertas, e hardware não utilizado.

9. Cotação do projeto

Cotação do projeto				
DESCRIÇÃO	MODELO	QUANTIDADE	VALOR UNIT.	VALOR TOTAL
AR CONDICIONADO	LG LT-C60BDLAO	6	R$ 6.000,00	R$ 36.000,00
APARELHOS TELEFONICOS	Force line	172	R$ 62,00	R$ 10.664,00
BACKUP	Bacula	6	FREE	
BANCO DE DADOS	Mysql	6	FREE	
DBA		1	R$ 24.000,00	R$ 24.000,00
ERP	Open erp	6	FREE	
HDS EXTERNOS	Samsung	3	R$ 139,00	R$ 417,00
IMPRESSORA	HP e120n	48	R$ 355,00	R$ 17.040,00
TRANCA BIOMETRIA	Digital Ekoo	1	R$ 900,00	R$ 900,00
MÃO DE OBRA		1	R$ 90.000,00	R$ 90.000,00
MULTIFUNCIONAL	laserjet e120n	6	R$ 500,00	R$ 3.000,00
NOBREAK	Smart-ups 7500w	5	R$6.000,00	R$ 30.000.00
PACOTE DE TELEFONIA	Vono 1300m	7	R$ 150,00	R$ 1.050,00
PORTA DE AÇO		1	R$ 4.000,00	R$ 4.000,00
PROJETOR	EPSON	5	R$ 800,00	R$ 4.000,00
RACK	42U VENTILADO	6	R$ 1.800,00	R$ 10.800,00
ROTEDOAR CISCO	RV042	6	R$ 460,00	R$ 2.760,00
S.O	FEDORA/DEBIAN	12/172	FREE	
SERVIDOR DELL	Dell t610 11g	1	R$ 5.198,00	R$ 5.198,00
SERVIDOR DELL	Dell t110	6	R$ 4.000,00	R$ 4.000,00
SWITCH	CISCO	6	R$ 649,00	R$ 3.894,00
SOLUÇÃO EMBRATEL	ADSL	6	R$ 355,00	R$ 2.130,00
VPN	OPENVPN	6	FREE	
TOTAL				R$ 250.655,00

PESQUISA ACADÊMICA

10.1. RAID

O termo RAID significa "Redundant Array of Inexpensive Disks", indicando justamente o uso de Hds padronizados e baratos como "blocos de montagem" para a criação de sistemas que se comportam como um único disco rígido, maior, mais rápido e/ou mais confiável do que suas peças individuais.

A tecnologia RAID desenvolve a forma de agrupar dois ou mais discos de forma que apareçam como um só dispositivo no sistema operativo que os aloja. Isto é, um RAID combina numa só unidade lógica vários discos, desta forma, o sistema operativo em vez de ver vários discos rígidos diferentes, vê apenas um.

O objetivo desta tecnologia é aumentar o rendimento e o nível de proteção de dados.

10.1.1. Tecnologia Raid

Há alturas em que se enchem de dados, ficam sem espaço livre e, portanto perdem a capacidade de armazenar mais informação e com isto o seu propósito. Outras vezes simplesmente deixam de funcionar.

Entre todos os componentes que se encontram nos nossos equipamentos o disco rígido é o que mais sofre. Temos que ter em conta que se trata de um dispositivo que gira a mais ou menos 10 mil voltas por minuto e isso durante horas e horas. O disco rígido será por isso mesmo geralmente é o primeiro a danificar-se e o primeiro na tornar-se pequeno, e se isto for pouco, além disso, é o elemento mais lento, devido a ser o único que incorpora uma parte mecânica.

A tecnologia RAID trata de melhorar todos estes problemas e em geral, se desenhado corretamente, consegue-o.

O sistema RAID proporciona uma série de vantagens frente aos discos rígidos convencionais:

O rendimento geral aumenta uma vez que os discos que formam um sistema RAID podem funcionar de forma paralela.

Oferece tolerância às falhas e níveis de rendimento mais altos que um disco rígido único ou que um grupo de discos independente.

Ainda que em princípio, estas matrizes de discos sejam consideradas complexas e relativamente orientadas para sistemas de armazenamento especializados, hoje em dia são fáceis de utilizar e a sua presença é mais comum, sobretudo em aplicações do tipo cliente/servidor.

Dependendo do nível de RAID que se escolha, se um dos discos do conjunto falha, a unidade continua a funcionar, sem perda de tempo ou dados. A reconstrução dos dados do disco que falhou faz-se de forma automática sem intervenção humana.

No caso de alguns sistemas operativos a regeneração dos dados faz-se a partir do software, ainda que nestes sistemas se possam usar controladores RAID que se regeneram automaticamente.

Ainda que esta tolerância a erros dos sistemas os torne imunes a falhas e relaxe os administradores que muitas vezes utilizam a implementação de um sistema RAID como alternativa às cópias de segurança. Uma boa política de cópias de segurança não deixa de ser necessário ao utilizar um sistema RAID.

O fato de que um sistema RAID previna certo tipo de falhas não evita que possam prevenir que a fonte de alimentação sofra um pico de tensão que faça arder os discos como uma fogueira. Também não protege a informação de outros fatores perigosos como incêndios, inundações, etc.

10.1.2. Implementações RAID

Um sistema RAID pode configurar-se e gerir-se mediante hardware ou software. Além disso, existem sistemas híbridos. Daqui vêm às expressões “RAID por Hardware” e “RAID por Software”.

Um “RAID or Hardware” requer que o equipamento tenha pelo menos uma controladora RAID específica seja como placa de expansão independente ou integrada na própria placa base do equipamento. Esta placa gerencia a administração dos discos e efetua cálculos de paridade.

Num sistema “RAID por Software” os discos são conectados a uma controladora de discos convencional, seja IDE, SATA, SCSI, SAS ou Fibra Channel.

Nos sistemas híbridos, o RAID é montado numa caixa externa específica que por sua vez se conecta ao sistema principal mediante conexões SCSI, ISCSI ou Fibra Channel. Em alguns sistemas, como NAS o RAID é completamente autônomo, conectando-se ao resto do sistema mediante a rede.

10.1.3. Níveis de RAID

Na sua origem a especificação RAID sugeria certas combinações diferentes de discos, ao que se chamava “níveis de RAID”. A cada uma dava-se-lhe um número RAID0, RAID1, RAID2, etc. Com o passar do tempo a tecnologia expandiu-se e apareceram diferentes implementações e métodos, alguns deles muito distintos dos originais, ainda que se tenha conservado o costume de chamá-los por números. Isto pode levar a alguma confusão dado que um conjunto RAID5, por exemplo, pode ser totalmente diferente de outro RAID5.

A definição RAID em si mesma pode não ser clara já que o uso do termo “redundante” poderia fazer duvidar que um RAID 0 seja realmente um RAID. Em geral, entende-se que qualquer sistema que utilize os conceitos básicos da tecnologia RAID de combinar espaço físico no disco para melhorar a sua prestação é um sistema RAID.

Tipos de níveis de RAID

Mais Comuns	Originais	Anidados	Proprietários
RAID 0	RAID 0	RAID 0+1	Dupla Paridade
RAID 1	RAID 1	RAID 1+0	RAID 1.5
RAID 5	RAID 2	RAID 30	RAID 7
	RAID 3	RAID 100	RAIDS ou RAID de paridade
	RAID 4	RAID 50	Matrix RAID
	RAID 5		Linux MDRAID 10
	RAID 6		IBM ServeRAID1E
	JBOD		RAID Z
	RAID 5E		
	RAD 6E		

10.2. NAS

(Network-attached storage) é o nome dado a dispositivos de armazenamento dedicados que podem ser conectados diretamente a uma rede local provendo aos demais computadores da rede facilidades de acesso e armazenamento de dados centralizados.

O conceito de NAS difere de um servidor de arquivos tradicional. O dispositivo NAS é um computador dedicado a uma função específica O sistema operacional e demais softwares provêem quase que exclusivamente a funcionalidade de armazenamento e acesso a dados. Os protocolos tipicamente suportados incluem o NFS (popular em ambiente UNIX) ou o CIFS/SMB (Common Internet File System/Server Message Block) usado em ambiente Windows, além do bom e velho FTP. Em termos de armazenamento físico, uma unidade NAS típica contem um ou mais discos. Os modelos mais sofisticados suportam redundância organizando os discos em arrays RAID.

Um dispositivo NAS usa hardware especificamente desenvolvido para a função de NAS, com um sistema operacional embarcado. Mas também pode ser implementado por computadores de prateleira rodando softwares especialmente configurados para as funções de NAS. Até a Microsoft possui uma versão de Windows Server voltada para implementação de soluções NAS: o Windows Storage Server 2003.

Equipamentos NAS vem sendo usados pelo mundo corporativo por algum tempo. Mais recentemente, com a redução do custo destes dispositivos e a popularização de redes domésticas e redes em pequenos escritórios, diversos produtos NAS surgiram para estes mercados. O mercado potencial emergente para dispositivos NAS é o mercado de usuários pessoais, com grande quantidade de dados multimídia. O preço de dispositivos deste tipo tem caído bastante, viabilizando o acesso aos recursos de NAS por um custo ligeiramente mais alto do que um disco externo. Estes dispositivos NAS de uso doméstico são baseados em processadores baratos rodando uma versão embarcada de Linux. Alem do baixo custo, têm baixo consumo de energia. A instalação é relativamente simples e a configuração se dá por uma interface Web.

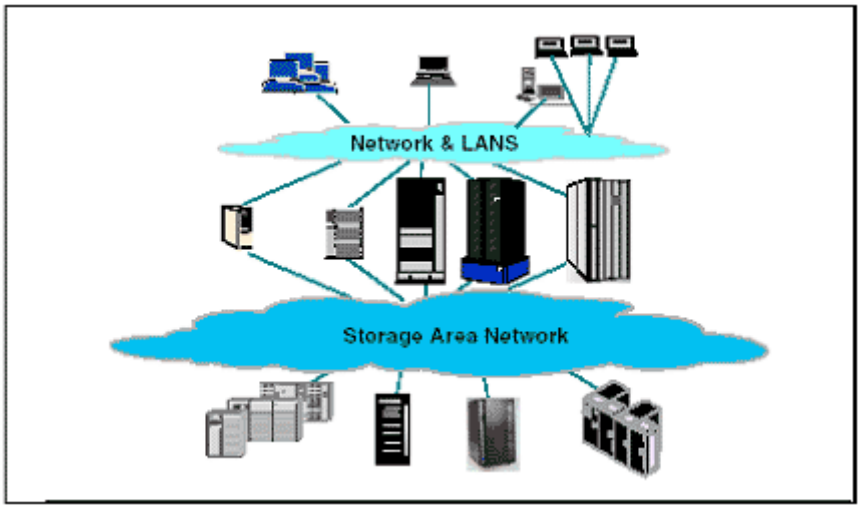
Também existem pacotes open source para implementação de soluções caseiras de NAS, utilizando equipamentos de prateleira mais antigos e de menor consumo. Os mais conhecidos são o FreeNas (baseado em FreeBSD), o NASLite e o Openfiler.

10.3. SAN (Storage Area Network)

A SAN poderia ser definido como uma rede de alta velocidade, comparada à LAN (Local Area Network), que permite o estabelecimento de conexões diretas entre os dispositivos de armazenamento e processadores (servidores) centralizados à extensão suportada pela distância das fibras óticas. A SAN pode ser vista como uma extensão do conceito que permite que os dispositivos de armazenamento sejam compartilhados entre servidores e interconectados entre si. Uma SAN pode ser compartilhada entre servidores ou dedicada a um servidor local ou remoto. As interfaces de SAN podem ser:

- ESCON (Enterprise Systems Connection)
- SCSI (Small Computer Systems Interface)
- SSA (Serial Storage Architecture)
- HIPPI (High Performance Parallel Interface)
- FC (Fibre Channel)
- Qualquer outra nova interface emergente

A figura abaixo mostra uma visão geral de uma SAN conectando vários servidores a vários sistemas de armazenamento:



SANs criam novos métodos de conexão de armazenamento aos servidores. Estes novos métodos prometem uma notável melhora em performance e disponibilidade. SANs são usadas para conectar conjuntos de armazenamento compartilhados a vários servidores, e são usadas por servidores em ambiente de cluster para fail over. Elas podem interconectar discos ou fitas de mainframe a servidores ou clientes de rede e podem criar caminhos paralelos de dados para ambientes de computação e de alta largura de banda. A SAN é uma outra rede que difere das redes tradicionais, porque foi concebida a partir de interfaces de armazenamento.

Além disso, a SAN pode ser usada para contornar os conhecidos gargalos de rede, pois suporta diretamente altas velocidades de transferência de dados entre os servidores e dispositivos de armazenamento nas seguintes formas:

Servidor para storage: é o modelo tradicional de interação com os dispositivos de armazenamento e cuja vantagem é que um mesmo dispositivo de armazenamento pode ser acessado serial ou concorrentemente por múltiplos servidores.

Servidor para servidor: no qual a SAN pode ser usada para alta velocidade e comunicações de alto volume entre servidores.

Storage para storage: permite a movimentação dos dados sem intervenção do servidor, liberando o processador para outras atividades. Por exemplo: um disco pode realizar o backup de dados para uma fita sem a intervenção do servidor ou um espelhamento de dispositivo remoto através da SAN.

O uso de Sãs gera uma melhora de performance das aplicações, por exemplo, permitindo que o dado enviado diretamente do dispositivo de origem ao dispositivo de destino não requeira intervenção do servidor. As Sãs também habilitam novas arquiteturas de rede nas quais vários computadores (host) acessam vários dispositivos de armazenamento conectados na mesma rede. Conheça outros benefícios que o uso da SAN pode oferecer às empresas:

Mais disponibilidade: armazenamento independente de aplicações acessíveis através de caminhos alternativos de dados.

Alta performance: os dados são descarregados do servidor e movidos para uma rede independente.

Armazenamento centralizado e consolidado: gerenciamento mais simples, escalabilidade, flexibilidade e disponibilidade.

Transferência e armazenamento: cópia remota de dados habilitada para proteção contra falhas e desastres.

Gerenciamento centralizado mais simplificado: a imagem simples do meio de armazenamento simplifica o gerenciamento.

Assim, os ambientes de SAN são uma rede de armazenamento de alta velocidade gerenciada centralmente, que consiste de vários fabricantes de sistemas de armazenamento, software de gerenciamento de armazenamento, servidores de aplicação e hardware de rede que permitem a sua empresa explorar da melhor forma o valor da informação do seu negócio, e ainda ganhar em produtividade e performance protegendo seus investimentos em TI.

Toda SAN tem como bloco de montagem Hás tradicionais, que são ligados a uma unidade controladora (que se encarrega do acesso aos dados, RAID e outras funções) e é ligada a um servidor através de uma interface dedicada, que pode ser tanto uma interface Libre Channel quanto uma interface de rede Gigabit Ethernet ou 10Giga bit Ethernet (usando o iSCSI). O servidor se encarrega então de distribuir os dados para os clientes da rede ou fornecê-los para aplicativos específicos, como no caso de um cluster de servidores web, que utilizam a SAN para armazenar um grande banco de dados usado para atender às requisições dos clientes.

Além da maior capacidade de armazenamento e de recursos de redundância, a principal diferença de uma SAN e um NAS ou um servidor de arquivos tradicional é que o SAN se comporta como se fosse uma única unidade de armazenamento, que o servidor pode acessar diretamente, de forma transparente. Ou seja, é como se você conectasse um único HD de 100 TB (por exemplo) no servidor, diferente de um NAS, que se comporta como um servidor de arquivos e pode ser acessado simultaneamente por vários clientes.

Apesar disso, na grande maioria dos casos, o objetivo de usar uma SAN não é simplesmente obter um grande espaço de armazenamento, mas sim obter ganhos de desempenho e de confiabilidade para aplicações críticas. Imagine o caso de um cluster de servidores responsáveis pelo site de um grande portal. As páginas são montadas a partir de um enorme banco de dados, armazenado na SAN, que é acessado de forma conjunta por todos os servidores do cluster. As unidades de armazenamento combinam um grande número de HDs em RAID, o que as torna capazes de atender a um grande volume de requisições por segundo, o que permite atender aos muitos visitantes simultâneos. Além do desempenho e do

armazenamento centralizado, temos também a questão da redundância, que garante que o sistema funcione de forma contínua, sobrevivendo a falhas em componentes diversos.

Os componentes básicos de uma SAN são um ou storage racks (as unidades de armazenamento, com os arrays de discos), um switch Fibre Channel, os cabos e o servidor ao qual a SAN é conectada. Apesar disso, é comum o uso de dois switchs e dois servidores, de forma a oferecer um sistema redundante (o segundo servidor fica a postos para assumir o lugar o primeiro em caso de falha).

A principal vantagem do uso de uma SAN é que o sistema pode ser expandido conforme necessário, incluindo mais storage racks e mais switchs. Os diferentes arrays podem então ser acessados por diferentes servidores e, dependendo da configuração, até mesmo serem configurados para se comportarem como uma única unidade, com as capacidades somadas. Se dinheiro não for problema, é possível atingir facilmente a marca de 100 terabytes de espaço de armazenamento, com direito a um sistema de redundância completo.

O grande problema é mesmo a questão do custo, já que um SAN completa pode facilmente superar a marca dos US$ 50.000, em preços do exterior. Isso faz com que elas fiquem restritas a ambientes onde as vantagens compensam o maior custo. Para pequenas redes, servidores com diversos HDs (configurados como um array RAID) acabam sendo a melhor opção, já que podem oferecer um espaço de armazenamento similar ao de uma pequena SAN (embora com um desempenho e confiabilidade inferiores) a uma fração do custo.

10.4. Segurança em redes TCP/IP

10.5. VPN

VPN (Virtual Private network), ou rede virtualmente privada, como o próprio nome exprime, disponibiliza através de uma rede pública um caminho que se comporta como uma linha privativa para conectar dois equipamentos ou redes que querem se comunicar entre si.

Esse caminho simula ser privativo, sem compartilhamento, de forma a dar segurança à conexão. Desta forma podemos utilizar a infra-estrutura da internet para uma comunicação que se comporta como uma linha privativa.

Os dados que trafegam por esse caminho (também chamado de “túnel”) são criptografados de forma que teoricamente somente o transmissor e o receptor conseguem entendê-los, por isso a segurança e o sentimento de que o canal de comunicação funciona como se fosse privativo.

Podemos assim interligar redes locais distantes entre si, utilizando a internet com meio de transmissão, fazendo com que a interligação entre as redes comporte-se como uma rede privada (não compartilhada por estranhos às redes da empresa). A vantagem desse tipo de solução é que uma empresa pode montar uma rede corporativa com baixo investimento em canais de comunicação, utilizando a internet como meio de comunicação de seus dados.

Uma VPN permite assim uma comunicação entre computadores e redes distantes entre si, utilizando uma rede pública de comunicação de dados, coma segurança que as redes privadas com LPs dedicadas fornecem.

O conceito de VPN é criar um túnel privativo lógico virtual entre dois pontos, com criptografia dos dados entre a origem e o destino final (criptografia end-to-end), de forma que ninguém possa interceptar os dados ao longo do caminho. Soluções Vpn podem ser implantadas em firewalls da rede.

A vantagem do uso de VPNs por uma empresa é principalmente a é principalmente a econômica, pois não utiliza links dedicados LPs nem redes de pacotes como frame-relay ou x. 25 para conectar redes remotas. Utiliza neste caso internet, por meio de um provedor, a custo menor e com um alcance mundial.

A VPN utiliza protocolos que fazem a criptografia dos dados antes de transmiti-los, de forma a fornecer segurança na transmissão dos dados contra intrusos. Os protocolos de segurança e criptografia mais utilizados são:

Os protocolos de segurança e criptografia mais utilizados são:

- IPSEC (Internet Protocol Security)
- L2TP (Layer 2 Tunneling Protocol)
- L2F(Layer 2 Forwarding)
- PPTP (Point to Point Tunneling Protocol)

10.6. Política de segurança

A segurança em redes TCP/IP possui outros componentes que devem ser considerados no projeto de redes. O planejamento da segurança de uma rede nasce no projeto, em que as necessidades de segurança da empresa devem ser analisadas.

O desenvolvimento de uma política de segurança é à base da segurança da informação em uma empresa. Alguns padrões e normas internacionais de segurança foram desenvolvidos por organizações normatizadoras como a ISSO (International Standars Organization) e a BS (british Standard), como a isso 17799 e a BS7799.

A política de segurança é desenvolvida considerando – se aspectos físicos e lógicos. A segurança física é aquela que envolve aspectos como prevenção contra falhas de equipamentos, incêndios, acesso de pessoas a locais restritos, enchentes, desastre naturais, acidentes, roubo e demais aspectos físicos. A segurança lógica envolve aspectos de prevenção contra interceptação e modificação de informações, sigilo no tráfego dos dados na rede, alterações de softwares, invasões em sistemas , acessos não autorizados a informações e demais aspectos relacionados ao acesso e manipulação dos dados da empresa.

O uso e o controle de senhas de acesso e criptografia de dados fazem parte de uma política de segurança, assim com o uso de firewall.

10.6.1. Firewall

É uma aplicação que faz a filtragem dos pacotes, por meio de seus endereços IP e de seus ports TCP, evitando que determinados ports e endereços sejam acessados. Desta forma, endereços e aplicações são bloqueados para acesso pelos usuários. Em uma política de segurança definimos quais endereços e aplicações serão bloqueados.

O firewall é formado de vários componentes como filtros (bloqueio de endereços), Proxy (bloqueio de aplicações), bastion host (equipamento usado para acesso externo, isolado da rede interna) e zonas deslimilirarizadas (zonas de isolamento entre a rede externa e a interna).

Controla e isola o tráfego entre duas redes, em especial a internet, para proteger redes corporativas de ataques e fornecer segurança à rede que tem informações e recursos que não devem estar disponíveis aos usuários de outras redes. O firewall pode ser implementado em roteadores, configurando regras de filtragem que permitem ou descartam pacotes de acordo com regras definidas.

10.6.2. Filtros

De acordo com as regras de filtragem estabelecidas, as aplicações d filtragem estabelecidas, as aplicações de filtragem do firewall encaminham ou bloqueiam e descartam pacotes de acordo com os endereços IP ou ports dos campos de controles dos pacotes IP ou TCP.

O filtro de pacotes opera nas camadas de rede e transporte do TCP/IP. Filtrando pacotes com base no endereço IP de origem. Endereço IP de destino, porta da aplicação de origem e porta da aplicação de destino.

10.6.3. Proxy

São aplicações que atuam como interface ou gateway entre duas redes, permitindo ou negando as requisições dos usuários para acesso a outros sistemas e redes. O usuário primeiramente se conecta ao servidor onde está a aplicação Proxy que então reencaminha para área externa, caso o usuário esteja autorizado.

10.6.4. Bastion host

Nesses equipamentos são instalados os sistemas e informações disponibilizados para acesso de usuários pela internet. Ou seja, os dados da empresa que estarão disponíveis na internet ficam em um equipamento apartado da rede interna da empresa, de forma que se houver alguma invasão e alterações das bases de dados desses equipamentos, elas não alterarão os dados da rede interna da empresa que estão em outros servidores internamente na empresa e fora do acesso externo.

10.6.5. DMZ (DeMilitarized Zone ou perimeter network)

É uma área de rede que fica entre a rede externa (Internet, por exemplo) e a rede interna que deve ser protegida. Caso ocorra algum problema ou ataque a um dos equipamentos dentro dessa área, não afeta a rede interna da empresa que continuará segura e fora do alcance dos ataques externos.

A função de uma Dmz é manter todos os serviços que possuem acesso externo (tais como servidores HTTP, FTP, etc.) separados da rede local, limitando assim o potencial risco de danos caso haja uma invasão.

Um ponto fundamental é que os computadores da DMZ não tenham acesso nenhum à rede local, essa configuração será feita através de um firewall que vai realizar o controle de acesso entre a rede local, a internet e a DMZ.

11. Conclusão

Esse projeto apresentado pela Consultoria Zinigem visou implementar na empresa de turismo “Viagem certa” a estruturação necessária para a união de 2 unidades adquiridas pela empresa, com intuito de que essa união além de proporcionar redução de custo traga facilidade de comunicação com todas as unidades da empresa.

A comunicação entre as unidades é um fator decisivo, pois a informação é importante para a definição dos pacotes e roteiros de viagens.

Implementando tecnologias atuais para que a comunicação ocorra de forma rápida e segura sendo esse o principal foco do projeto.

Portanto o projeto realizado mostra na visão da empresa Zinigem as melhorias necessárias para que a empresa “viagem Certa” esteja dentro das normas e padrões tanto na parte física e lógica da rede, proporcionando a interligação de todas as unidades da empresa com agilidade através da otimização dos equipamentos e softwares.

12. Bibliografias e Referências

MORIMOTO**,** Carlos E. Hardware, o Guia Definitivo. Editora GDH Press e Sul Editores,2007.

Sousa, L.B. TCP/IP Básico e conectividade em redes. 4º edição.Editora Érica,2008.

Vieira, F.M. Trabalhando em Redes. Editora Érica,2002

http://www.cisco.com/web/BR/index.html

http://www.dell.com.br

http://www.bacula.org

http://www.projetofedora.org

http://www.vivaolinux.com.br

http://www.debian.org

http://www.guiadohardware.net

http://www.asterisk.org

http://www.openvpn.net

http:/www.openerpbrasil.org

http://www.forceline.com.br

http://www.5ti.com.br

http://www.lg.com.br

http://www.mysql.com