UNIVERSIDADE CATÓLICA DE BRASÍLIA

PRÓ-REITORIA DE GRADUAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

Bacharelado em Ciência da Computação e Sistemas de Informação

CRIAÇÃO DE UM CORREIO ELETRÔNICO CORPORATIVO COM POSTFIX

Autores: Davi Eduardo R. Domingues
Luiz Carlos G. P. C. Branco
Rafael Bispo Silva
Orientador: MSc. Eduardo Lobo

BRASÍLIA 2007

DAVI EDUARDO R. DOMINGUES

LUIZ CARLOS G. P. C. BRANCO

RAFAEL BISPO SILVA

CRIAÇÃO DE UM SERVIDOR DE CORREIO ELETRÔNICO CORPORATIVO COM POSTFIX

Monografia apresentada ao Programa de Graduação da Universidade Católica de Brasília, como requisito para obtenção do Título de Bacharelado em Ciência da Computação.

Orientador: MSc. Eduardo Lobo

Brasília

2007

TERMO DE APROVAÇÃO

Dissertação defendida e aprovada como requisito parcial para obtenção do Título de Bacharel em Ciência da Computação, defendida e aprovada, em 05 de dezembro de 2007, pela banca examinadora constituída por:

Professor Eduardo Lobo – Orientador do Projeto

Professor Mário de Oliveira Braga Filho – Membro Interno

Professor Giovanni – Membro Interno

Brasília
UCB

Dedico este trabalho primeiramente a Deus que me deu a vida e paciência para chegar a este nível de estudo que me encontro. Em especial a minha mãe que acreditou em mim, aos bons valores que me ensinou e pelo apoio a toda minha vida acadêmica e me compreendeu pelos momentos de ausência ao seu lado.

Davi Eduardo R. Domingues

Dedico a minha família que sempre acreditou em mim, também aos meus grandes amigos e aos grandes amigos que se foram, aqueles que nos deixam saudades e uma vontade de continuar seus trabalhos.

Luiz Carlos G. P. C. Branco

Gostaria de agradecer e dedicar esse trabalho primeiramente a minha família e a todos que torceram positivamente para essa minha grande conquista, obrigado Deus por permitir essa grande vitória na minha vida, obrigado aos meus pais que são grandes responsáveis por essa etapa e obrigado a todos os meus amigos que sempre estiveram comigo, me apoiando em todas as dificuldades encontradas.

Rafael Bispo Silva

Agradecemos ao orientador Prof. MSc Eduardo Lobo pelo acompanhamento, sugestões e discussões ao logo desse projeto.

"Uma mente que se abre a uma nova idéia nunca mais voltará a seu tamanho original."

Albert Einstein

RESUMO

Atualmente o uso do *e-mail* ultrapassou o exercício básico da utilização da Internet ao ponto de fazer parte da vida das pessoas. O uso desse serviço abrange desde a troca de diálogos informais, até mensagens corporativas diariamente acessadas para negócios, marcar reuniões e enviar informações sigilosas.

No entanto, a popularização deste serviço também possibilita que usuários, com más intenções, acessem um grande contingente de informações valiosas e pertinentes. Por esse motivo, faz-se necessário a produção de um e-mail seguro, garantindo assim, princípios básicos da segurança da informação, como: disponibilidade, integridade e confiabilidade.

O modelo de e-mail seguro que será descrito pretende ser um padrão que atenda às necessidades do mercado, mostrando as possibilidades existentes para a implementação segura e prática no ambiente da Universidade Católica de Brasília, bem como em qualquer outro ambiente corporativo.

PALAVRAS-CHAVE: E-mail, Segurança, Ferramentas livres, NBR ISO/IEC 17799, Spam.

ABSTRACT

Currently, the usage of the *e-mail* exceeded the basic utilization of the Internet, but also it is part of people's life. The usage of this tool embraces since the exchange of informal notes, until corporative messages that are daily accessed to solve business, mark reunions and send sigil information.

Meanwhile, the popularization of this service also permits that users, with bad intentions, access a great contingent of relevant information. By this reason, is needful the production of a safe e-mail, that guarantee the essential needs of information security, like: availability, integrity and reliability.

The model of safe e-mail that is going to be described in this paper intends to be a standard that accomplish the necessity of the market, showing possibilities to a practical and safe implementation at Universidade Católica de Brasília, also to any other corporative environment.

Keywords: E-mail, Security, Free tools, NBR ISO/IEC 17799, Spam.

SUMÁRIO

ÍNDICE DE FIGURAS

1. INTRODUÇÃO

A informática é um instrumento cada vez mais utilizado para realizar os trabalhos de forma fácil, eficiente e rápida. A rede é o que interliga esse universo de conexões e recursos que, disponibilizados ao mundo, muitas vezes representam o próprio negócio das organizações. Isso faz com que essa flexibilidade e facilidade de uso resultem em uma produtividade maior e na criação de novos serviços e produtos.

Por outro lado, essa facilidade aumenta o uso desses serviços, tornando-os mais críticos e vitais. Com isso, as empresas e profissionais devem se empenhar mais para diminuir os riscos e falhas, para que não aconteça interrupção desses serviços, e se houver, que exista um plano de contingência para que o serviço seja restabelecido no menor tempo possível.

Como falar da Era da Informação sem falar da necessidade de utilização de serviços de e-mail em uma empresa e do quanto essa utilização pode ser importante e decisiva no mundo dos negócios. Para que seja possível esta interação com o mundo dos e-mails, as empresas optam por algumas soluções, como: a terceirização do serviço de e-mail por uma empresa especializada, a compra de um software de serviço de e-mail proprietário, ou até mesmo, a construção de um servidor de e-mail através da junção de algumas ferramentas livres.

Um dos pontos atrativos do e-mail é que se trata de um meio informal e rápido de se comunicar com colegas, clientes e fornecedores. Mas o e-mail também propõe seus desafios. Seu uso criou algumas questões comerciais, de segurança e jurídicas, das quais é necessário ter consciência. Este projeto propõe informar ao usuário sobre os usos e abusos do e-mail no trabalho. Conhecendo-os, poderão evitar problemas.

A proposta dessa monografia é montar um servidor de e-mail robusto, que esteja de acordo com o nível de qualidade que a Universidade Católica de Brasília utiliza neste tipo de serviço, utilizando-se de software livre, além de seguir boas práticas e normas em vigor, proporcionando um aumento da segurança das informações contidas nas mensagens de correio eletrônico.

2. OBJETIVOS

Esse projeto tem por finalidade pesquisar uma solução adequada para montar um servidor de e-mail corporativo para a Universidade Católica de Brasília. Para isso será instalado soluções gratuitas, que possuem uma ideologia de códigos abertos que facilitaram a compreensão do funcionamento e um aprendizado teórico e prático de tudo o que for utilizado, explorar as funcionalidades e recursos dessas soluções e proporcionar a integração com outros tipos de soluções, sejam elas proprietárias ou não.

2.1. Objetivo Geral

O objetivo global é: aprofundar o conhecimento necessário para a implementação de um servidor de e-mail corporativo, para explorar os conceitos, requisitos estruturais necessários, as limitações e escalabilidades possíveis. Definir os protocolos e serviços que podem ser agregados para completar um pacote de solução, respeitando as normas de cada produto utilizado. Resumindo: abranger os tópicos teóricos e práticos na implementação de uma solução de e-mail robusta.

2.2. Objetivos Específicos

O projeto tem como intenção alcançar os seguintes objetivos:

- Conhecer os protocolos associados ao serviço de e-mail;
- Pesquisar os aspectos jurídicos existentes no uso de e-mail em corporações;
- Testar métodos e implementações de segurança sobre os protocolos;
- Estudar as diversas ferramentas de webmail e escolher a mais adequada para a UCB;
- Implementar o serviço de lista de distribuição.
- Testar o desempenho da maquina hospedeira do serviço de e-mail.

3. CRONOGRAMA PREVISTO E REALIZADO

Para a implementação do projeto é necessário realizar e cumprir o cronograma com fidelidade e presteza, a fim de mitigar e contingenciar possíveis problemas.

O desenvolvimento do projeto ocorreu de acordo com as seguintes etapas:	*Fevereiro*	*Março*	*Abril*	*Maio*	*Junho*	*Julho*	*Agosto*	*Setembro*	*Outubro*	*Novembro*	*Dezembro*
Estudar os conceitos de E-Mail	P	P R									
Levantar as ferramentas de E-Mail existentes	P	P R	P								
Levantar requisitos para a solução de E-Mail	P	P	P R								
Instalação da ferramenta escolhida: o Postfix	P	P	P	P	P R	P R					
Levantar as soluções disponíveis para Postfix					P R	P R	P R	P R			
Implementar a solução de E-Mail								P R	P R	P R	P R
Teste de validação da solução								P	P R	P R	P R
Elaboração da monografia	P	P R	P R	P R	P R	P R	P R	P R	P R	P R	P R

P = Etapas previstas R = Etapas realizadas.

Tabela 1 – Cronograma das atividades previstas e realizadas.

4. PROPOSTA DO ESTUDO

Apresentar um projeto de construção de e-mail, baseado em software livre, estudando os tipos de soluções existentes atualmente no mercado. Escolher e aprofundar os conhecimentos sobre estas soluções, bem como os recursos disponíveis.

Após todo conhecimento obtido, criar uma solução que atenda à necessidade dos alunos da pós-graduação da Universidade Católica de Brasília, das direções dos cursos e de alguns setores da instituição que utilizam os serviços de correio ou de lista de distribuição.

4.1. Descrição da Pesquisa

Proposta de uma solução corporativa de e-mail utilizando software livre. Inicialmente, serão feitas buscas e estudos em referências bibliográficas relacionadas ao assunto. Em seguida, serão selecionadas e testadas ferramentas livres, candidatas a utilização como solução. Por último, deverá ser apresentada a solução.

Por meio de um estudo bibliográfico, serão estudadas e analisadas as diferenças dos principais MTA's gratuitos, de código aberto, existentes no mercado que possibilitam o desenvolvimento de novas funcionalidades de forma simples e eficaz..

4.2. Resultados Esperados

Espera-se com o projeto ampliar os conhecimentos sobre instalação, gerenciamento, vantagens e recursos de um MTA, utilizando software livre, tornando possível apresentar, em laboratório, uma solução para a Universidade Católica de Brasília.

4.3. Restrições da Pesquisa Proposta

Mesmo a Instituição já possuindo uma solução proprietária, a premissa é a utilização de software livre, pois, além da vantagem de não existir custos adicionais ao trabalho, a utilização de uma solução livre e de código aberto agrega valores acadêmicos e incentiva direta e indiretamente a pesquisa.

Considerando que o foco é um serviço para uso amplo, tanto para utilização dentro da Universidade, quanto para quaisquer outros interessados, serão estudados os recursos que se apliquem a usos gerais.

4.4. Interessados e Beneficiados

A Universidade Católica de Brasília, que implementará a solução apresentada e customizada para seu uso próprio; estudantes que tenham interesse sobre o assunto; empresas que queiram uma solução corporativa bem projetada e estudada; administradores de redes; consultores; todos aqueles que tenham cenários semelhantes; pessoas que estejam interessadas

no estudo sobre e-mail e interessados em colocar uma solução profissional onde exista a necessidade de um serviço de e-mail seguro e confiável.

4.5. Recursos Necessários

De acordo com as informações, obtidas no levantamento de requisitos junto ao cliente, sobre o que é importante ser monitorado, levantam-se os seguintes recursos necessários para montagem do ambiente de testes.

4.5.1. Recursos de Hardware

Montar um laboratório composto por 4 computadores: A figura da página 19 representa a topologia da rede utilizada como laboratório.

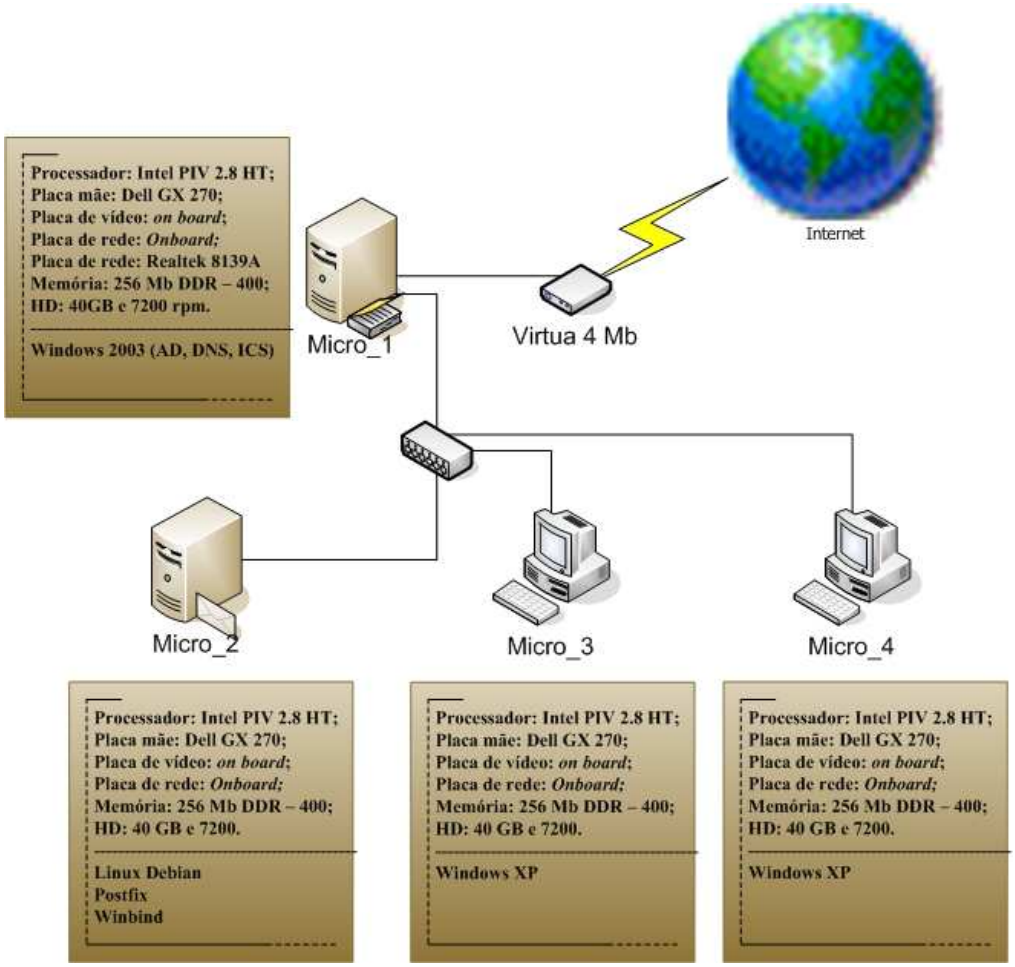

Figura 1 – Topologia da rede utilizada no desenvolvimento

4.5.2. Recursos de Software

Será montado um servidor de E-mail. Para isso será necessário um servidor de nome de domínio – DNS (*Domain Name System*) devidamente configurado, IPs válidos ou seja, o básico operacional de uma rede existente.

Conforme indicado na Figura 1, após análise de alguns sistemas operacionais, dentre eles *RedHat*, *RedHat Enterprise*, *Fedora*, foi um consenso utilizar o Sistema operacional Linux Debian, por apresentar melhor desempenho e possuir um código totalmente aberto, para servidor de e-mail será utilizado o Postfix, juntamente com os pacotes abaixo:

Softwares Utilizados	
Softwares	**Versão**
Sistema Operacional Debian	4.0
Servidor Web Apache	2.2.3
Autenticador Winbind	3.0.24
Servidor de E-mail Postfix	2.4
Compilador Perl	5.8.8
Filtro de Conteúdo SpamAssassin	3.1.7-deb
Servidor POP CourierPOP	0.57.1
Servidor IMAP CourierIMAP	4.2.1
Servidor Listas de distrib. MailMan	2.1.9

Tabela 2 - Softwares utilizados

4.5.3. Recursos Físicos

Para os testes de implantação do projeto será utilizado os servidores da Figura 1. Após os testes o projeto será implementado em um servidor de máquinas virtuais da Universidade Católica de Brasília, em Debian, com 4 GB de memória e 4 processadores Pentium III 800MHZ simultâneos.

Com isso existirá um laboratório próprio, sem restrições de acesso e físicas para o desenvolvimento do projeto, sendo assim o ambiente de testes será montado num laboratório de testes da Diretoria de Tecnologia da Informação – DTI-UCB.

4.6. Relação Custo Benefício

Já que será usada uma solução baseada em software livre, os custos serão apenas nas horas de trabalho dos alunos em desenvolver o projeto. Haverá como benefício o aprimoramento intelectual dos envolvidos no projeto. A Universidade Católica de Brasília poderá beneficiar-se utilizando a solução proposta e customizada fornecendo e-mails para os alunos que fazem a pós-graduação melhorando, também, a questão de segurança da rede da instituição que terá suas contas de e-mail dos alunos na base Active Directory já existente, além de que receberá mais um subsídio para novas pesquisas.

5. CORREIO ELETRÔNICO

> *"O correio eletrônico é um dos serviços mais elementares e mais importantes disponíveis na Internet. Basicamente, o correio eletrônico é a troca de mensagens (cartas), memorandos etc. em formato eletrônico) que um usuário da Internet pode mandar para outro usuário."* [**DAMSKI,1996**].

A utilização do correio eletrônico corporativo tem se tornado uma ferramenta muito importante para cada organização. As empresas crescem a cada dia e isso implica na expansão de suas redes e no aumento de tráfego de e-mail. Com esse incremento os serviços por sua vez tornam-se mais críticos, mais valiosos e mais importantes, aumentando também a necessidade de segurança nas mensagens. Mas para garantir a continuidade de um serviço é necessário antes definir os estágios nele existentes e o que cada um especificamente faz, ou seja, tudo que é necessário para garantir que uma mensagem saia de um ponto A e chegue a um ponto B.

5.1. Breve Histórico

Por volta de 1965, surgiu a correspondência eletrônica, com a simples missão de trocar mensagens entre usuários de computadores de grande porte. Devido a sua eficiência, logo se transformou em um método que permitia diferentes usuários em diferentes computadores trocar mensagens. Assim surgiu o *e-mail* (eletronic mail), com o sistema AUTODIN (*Automatic Digital Network*), criado em 1966 com uso exclusivo para a força militar americana.

Um dos grandes contibuintes para o progresso e popularização, não somente do e-mail mas da Internet foi a rede de computadores ARPANET (*Advanced Research Projects Agency Network* -Agência de Pesquisas Avançadas em Projetos de Rede) ela foi a primeira a utilizar comutação de pacotes.

O uso do sinal @, que significa *"at"* ("proveniente") para separar os nomes do usuário e o da empresa foi definido pelo programador Ray Tomlinson, funcionário da empresa contratada pelo Departamento de Desesa dos Estados Unidos em 1968 para implantar a ARPANET,, em 1971.

5.2. O que é?

É um sistema que necessita de uma conexão cliente/servidor (podendo ser uma conexão GPRS, ou Wi-Fi) e não necessita obrigatóriamente da internet, é baseado no protocolo SMTP (Simple Message Transfer Protocol - Protocolo Simples de Transferência de Mensagens) e permite criar, enviar e receber mensagens entre usuários dentro de uma empresa ou entre empresas e organizações

O correio eletrônico possui um tempo de entrega de mensagens baixo, questões de minutos para atravessar diversos países. Nenhum outro sistema de correspondência, seja ela correio, sedex, fedex, não consegue se comparar a esse serviço. A troca de mensagens é tão rápida que se o destinatário estiver usando computador quando o remetente envia a mensagem, ele pode receber a mensagem quase que instantâneamente e pode responder esta no mesmo instante do recebimento da mensagem.

Esse serviço oferece praticidade, rapidez e baixos custos para troca de informações sobre negócios, principalmente pela simplicidade em seus recursos on-line ou em rede local, independentemente da cidade, país ou região em que o usuário se encontra.

O conceito de E-mail não está relacionado somente a troca de informações entre apenas duas pessoas, existe a possibilidade de uma mesma mensagem ser direcionada a uma lista de endereços. Através desse recurso criaram-se as famosas listas de discussão e publicações eletrônicas.

O corpo da maioria das mensagens eletrônicas geralmente é formado por texto, mas o e-mail também é muito utilizado para troca de mensagens com conteúdos diversos anexados, tais como: imagens, vídeos, sons, dentre outros arquivos codificados. Levando-se em consideração o cenário de Correio Eletrônico Corporativo, o usuário da organização deve tomar cuidado com o tipo de arquivo enviado, pois existem políticas que restringem alguns tipos de conteúdos que não são permitidos no ambiente de trabalho da Instituição, o que pode acarretar em problemas para o funcionário como processos, suspensões e até mesmo demissão por justa causa.

5.3. Como usar?

O uso do Correio Eletrônico corporativo é basicamente a principal aplicação utilizada para a comunicação entre os funcionários de uma empresa.

Usando um micro é possível montar um Servidor de Correio Interno e Externo para sua empresa, como as maiorias das empresas fazem.

A vantagem é que o Servidor ficará internamente em sua empresa, e a troca de correio entre seus funcionários internos não necessitará do acesso à Internet, evitando tráfego desnecessário. A outra vantagem é que o número de caixas postais e o tamanho não necessitam ser limitados, desde que o disco rígido local do servidor suporte o volume de informações.

Um fator importante que deve ser levado em consideração é a sigilosidade das informações contidas no servidor de e-mail: em hipótese alguma poderão ser disponibilizadas para pessoas estranhas à Universidade. Por se tratar de uma instituição (UCB), existem pesquisadores de várias áreas na universidade desenvolvendo diversos trabalhos, na qual uma das informações enviadas por e-mail deve seguir os padrões de integridade, confidencialidade e disponibilidade, se houver vazamento da informação pode prejudicar o pesquisador e/ou a pesquisa, e ajudar um intruso a postar a tal pesquisa que era de outro pesquisador.

Com relação à usabilidade do correio eletrônico o usuário pode enviar e receber mensagens pela Internet; basta esse tipo de acesso estar liberado pelo administrador de rede.

Existem vários programas disponíveis para correio eletrônico, tanto no sentido de servidores quanto de clientes. Dependendo do programa utilizado muda-se a forma de acessá-lo: pode ser um programa a parte, ou o próprio servidor pode ter a opção de disponibilizar uma interface de acesso remota, como o da Universidade Católica de Brasília, que disponibiliza um webmail integrado ao browser (***mail.ucb.br***).

Para enviar um e-mail deve-se estar atento aos campos a serem preenchidos corretamente:

- **Mail To (Para):** Esse campo diz respeito à pessoa para o qual se quer enviar uma mensagem.
- **Cc (Com cópia):** Pode-se utilizar esse campo se quiser enviar mensagem com cópia para mais alguém.
- **Cco (Com cópia oculta):** Funciona como a opção acima, com a diferença que o usuário que esta no “Mail To” não sabe que esse outro usuário estará recebendo uma cópia.
- **Subject (Assunto):** Representa o conteúdo da mensagem, para o remetente e destinatário(s) saber do se trata.
- **Corpo da mensagem (Data ou Body):** Está é a mensagem propriamente dita, o que é escrito para alguém.
- **Anexos (attachment)**: É usado para anexar arquivos, como documentos textos, planilhas, vídeos, mp3.

5.4. MTA

O termo MTA (*Mail Transfer Agent*), também conhecido como agente de transporte de e-mail, é na verdade o servidor de e-mail ou aquele que é responsavel por enviar ou receber os e-mails provenientes de outros dominios, se responsabilizando pelas transferências de mensagens de correio eletrônico entre um host e outro. Como mostra a **Erro! Fonte de referência não encontrada.**, cada MTA têm a função de transferir mensagens para outros MTAS. Mesmo o destino sendo local ou Internet. Existem muitos tipos de MTAs, alguns exemplos são: Sendmail, Qmail, Exim, Postfix e Courier.

MTA	Maturidade	Segurança	Performance	Instalação	Documentação	Utilitários para análise. de Logs
Qmail	Médio	Alto / Muito Alto	Alto	Médio / Dificil	Muita	Sim
Sendmail	Alto	**Baixo**	**Baixo**	Fácil	Muita	Sim
Postfix	Médio	Alto	Alto	Fácil / Médio	Médio / Muito	Sim
Exim	Médio	**Médio / Baixo**	Médio	Médio	Muito	Sim
Courier	**Baixo**	Médio	Médio	Médio	**Baixo**	**Não**

Tabela 3 – Comparativo de MTAs.

Fonte: http://lifewithqmail.org/lwq.html#comparison ,http://homepages.tesco.net/~J.deBoynePollard/Reviews/UnixMTSes/ e http://www.geocities.com/mailsoftware42/**.**

O sendmail é um agente de transporte de E-mail mais conhecido. Baseado em Free BSD, sua função básica é aceitar mensagens a partir de um agente MUA (*Mail User Agent*) e entregá-las ao servidor apropriado, também aceita conexões de rede e entrega as mensagens em caixas de mensagens locais.

O Qmail é outro agente de transporte de e-mail, criado para ser mais seguro que o Sendmail. Por ele seguir fielmente as RFC'S chega a ser ao mesmo tempo enxuto e complexo. A vantagem desse tipo de codificação é que ainda na primeira versão só foram encontrados 02 Bugs e ainda existe um prêmio de $500,00 para quem encontrar uma vulnerabilidade em sua última versão, o anuncio do prêmio pode ser visto em http://cr.yp.to/qmail/guarantee.

O Exim, outro exemplo de MTA, foi desenvolvido na Universidade de Cambridge. É menos conhecido que o sendmail e o qmail, mas também possui grande flexibilidade e suporte

a spam, antivírus, entre outros. Em alguns sistemas operacionais ele vem por padrão em seus pacotes como o Debian.

Após a análise desse material, os únicos aceitos, com desempenho e segurança alta, são o Postfix e o Qmail. Após uma observação do comparativo entre os MTAS, identifica-se o Postfix como ferramenta de e-mail mais pertinente ao estudo. Este será adotado por ter uma série de requisitos que atendem às necessidades do projeto, aliado ao fato de ser uma ferramenta modular, permitindo a implantação de uma série de funcionalidades que são de fato úteis ao sistema.

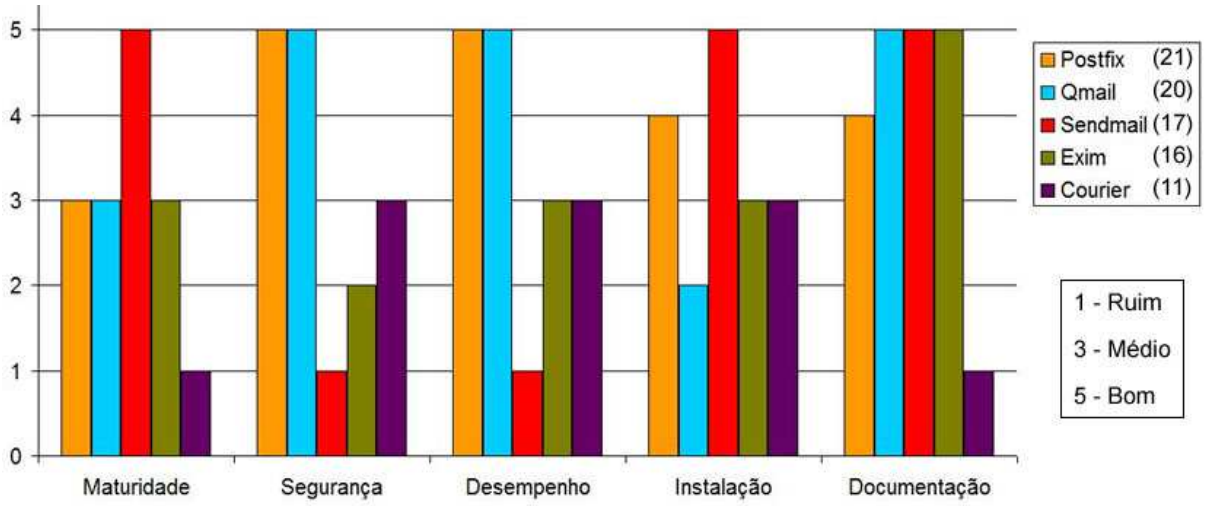

Figura 2 – Comparativo entre os 5 maiores MTAS livres

5.5. MUA

O MTA faz seu trabalho por de forma invisível para o usuário, enquanto o mesmo interage com o MUA, ou seja, MUA é o software que faz a interface com o usuário. Enquanto para o usuário final um MTA pode ser transparente o MUA é sim o grande responsável pelo manuseio das mensagens, é o caso de softwares como Mutt, Microsoft Outlook, Outlook Express, Eudora Light ou página de webmail).

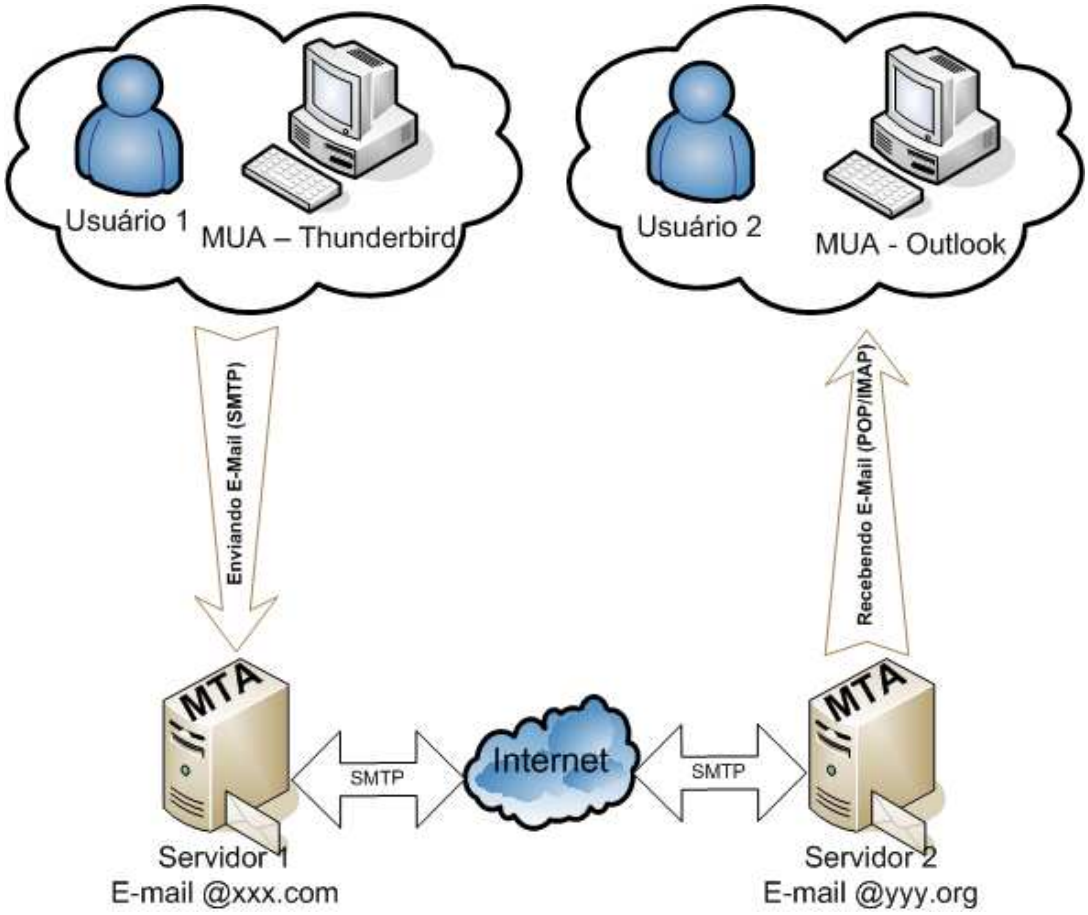

Figura 3 – Relação do MUA e MTA

5.6. Mailbox e Maildir

Existem dois tipos de armazenamento de mensagem no servidor, cada um com suas particularidades.

O Padrão mailbox é o mais simples, ele consiste na seguinte idéia:

- Todas as caixas são armazenadas no mesmo diretório;
- Dentro desse diretório são criados arquivos, cada um com o nome de uma caixa postal. Cada nova mensagem de uma caixa postal é gravada no final do arquivo de dessa caixa.
- O arquivo é apagado após o usuário baixar localmente todas as mensagens do servidor.

O Padrão Maildir é o mais simples, ele consiste na seguinte idéia:

- Não armazenar todas as mensagens em apenas um arquivo, pois aumentaria o risco de uma perda caso o arquivo se corrompesse, destruindo toda uma caixa postal e não somente uma mensagem. Pensando nisso padrão Maildir trabalha com uma estrutura de pastas da seguinte forma: Cria varias pastas (para mensagens não lidas, mensagens lidas e mensagens apagadas). Dentro de cada pasta, cada arquivo é uma mensagem.
- A medida que cada mensagem é lida, ela é transferida da pasta de mensagens não lidas para a pasta de lidas. Assim, se uma conexão é interrompida enquanto o usuário baixava suas mensagens, quando o usuário voltar a baixar, ele continuará da ultima mensagem baixada.

6. BANCO DE DADOS

A estrutura de banco de dados é extremamente importante no que diz respeito à segurança do MTA, o fato de usuários estarem gravados em um banco de armazenamento de dados não significa que essas contas tenham permissão para logarem no servidor, e em se tratando de contas locais, quando se fala em mais de 2 mil usuários a performance é comprometida.

Foram abordadas as duas soluções mais usadas no mercado, um banco MYSQL (software livre de gerenciamento de banco de dados) no próprio servidor Postfix, e uma autenticação LDAP (*Lightweight Directory Access Protocol*) onde o Postfix pode autenticar o usuário em outra base (como Windows, por exemplo). Isso permite que os usuários usufruam mais opções de serviços independente da plataforma. Obviamente existem outras soluções, porém serão abordadas as mais comuns.

6.1. MySQL

O MySQL é um software livre de gerenciamento de banco de dados baseado em linguagem SQL como interface. Possui uma excelente portabilidade, excelente desempenho e estabilidade e é pouco exigente quanto a recursos de hardware.

Foi considerado em 2005, pela SQL Magazine (Edição 23) como um dos bancos de dados mais populares do mundo, dentre os mais famosos usuários desse banco estão: NASA, Banco Bradesco, HP, Nokia, Sony, Banco Federal dos Estados Unidos da América, Alcatel, Cisco Systems, entre outros.

A solução de Postfix e MySQL permite ao Postfix acessar uma ou múltiplas bases de dados MySQL, essa técnica cria uma escalabilidade e segurança enorme, como na figura abaixo.

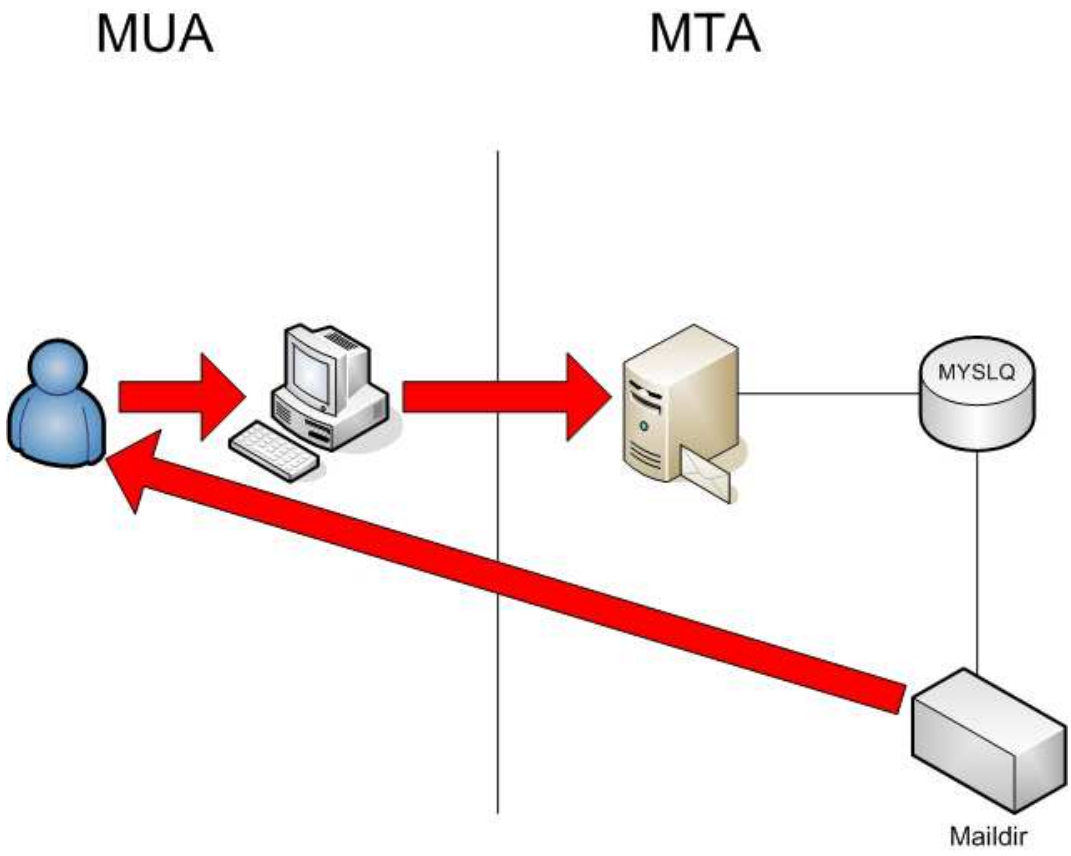

Figura 4 - Envio de e-mail entre MUA e MTA utilizando MYSQL

Infelizmente, a solução oficial disponível no site do Postfix propõe o uso do banco apenas para autenticação, argumentando a vantagem de não ser necessário criar milhares de contas, com isso é possível autenticar um número imenso de usuários, mas não soma em

solução com a base de mensagens de usuários como é visto na Figura 5 abaixo, que ainda deverá ser armazenada no servidor Postfix.

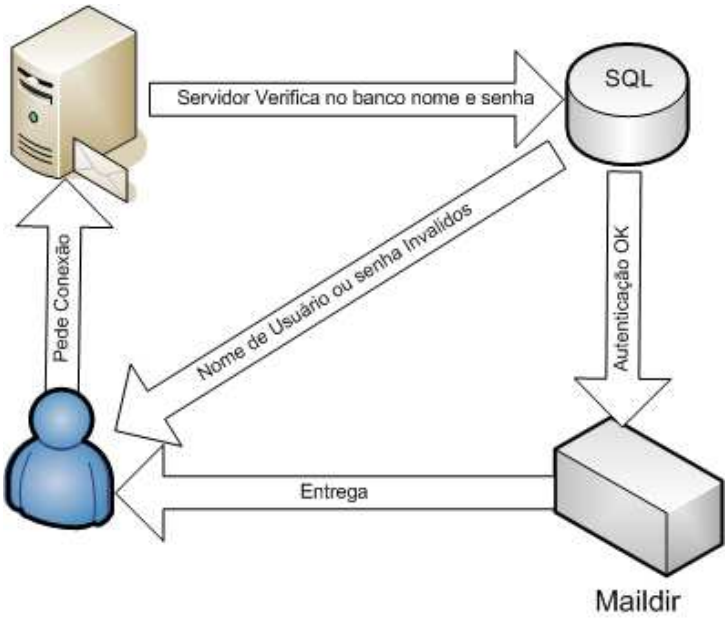

Figura 5 – Processo de autenticação no SQL

6.2. LDAP

Segundo Theisen (2005) *"LDAP significa Lightweight Directory Access Protocol, ou seja, Protocolo de Leve Acesso a Diretórios. Como o nome sugere, é um protocolo leve para acessar serviços de diretório. O LDAP roda em cima do protocolo TCP/IP ou outras conexões de transferência de serviços."*

A utilização do LDAP, hoje em dia, tende a se basear nos nomes já existentes do sistema DNS, na estruturação dos níveis mais básicos de hierarquia. Mais profundamente, podem aparecer estruturas representando pessoas, unidades organizacionais, impressoras, documentos, grupos de pessoas ou qualquer outra coisa que represente um nó.

Postfix pode usar um diretório LDAP como fonte para várias pesquisas, de acordo com a Figura 6. Isto permite manter informações sobre os serviços de e-mail em base de dados que serão replicadas na rede, com um bom controle de acesso.

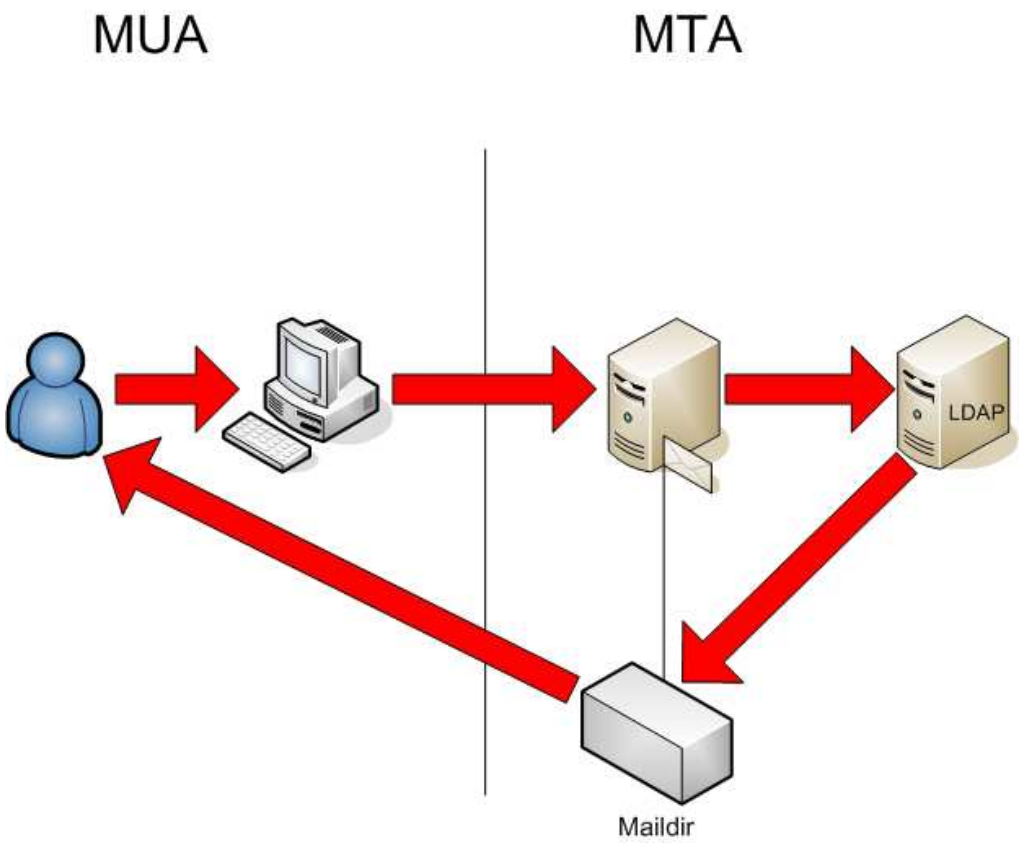

Figura 6 - Envio de e-mail entre MUA e MTA utilizando LDAP

Postfix pode usar uma base de diretório LDAP para autenticar os usuários de e-mail, não armazenando essas contas localmente no servidor. É possível possuir múltiplos servidores

de e-mail e outros serviços e servidores acessando estas mesmas informações simultaneamente sem degradar a estrutura que o LDAP fornece.

A base de dados LDAP mais conhecida e utilizada hoje é a do fabricante de softwares proprietário Microsoft. Apesar disto a solução Postfix acessa qualquer base LDAP agregada ainda sendo um software gratuito, como mostrado abaixo.

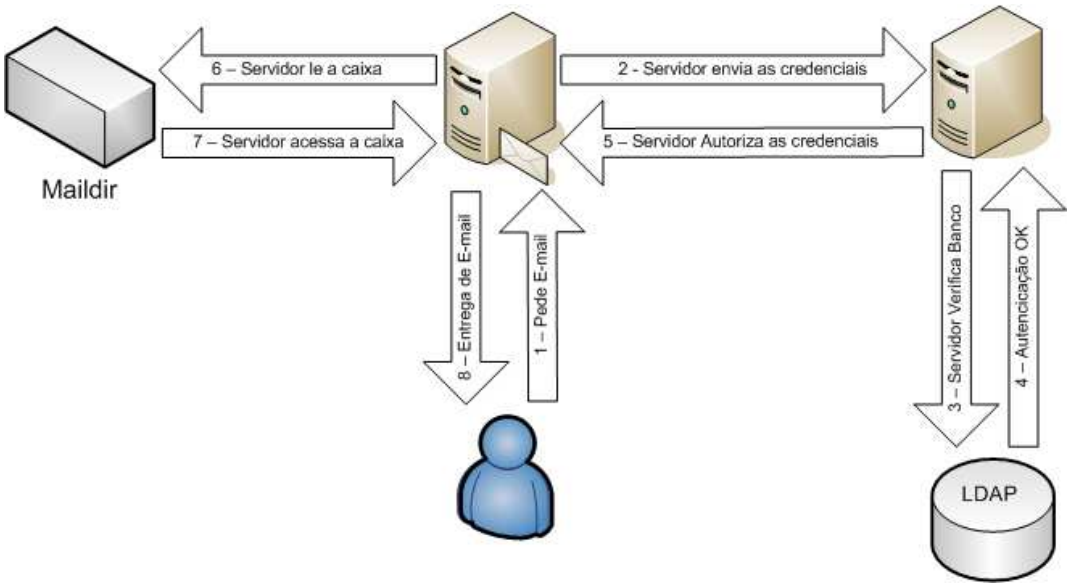

Figura 7 – Processo de autenticação na base LDAP.

7. PROTOCOLOS

Fernando Albuquerque define protocolo como *"um conjunto de regras e convenções precisamente definidas que possibilita a comunicação através de uma rede de computadores."*. **[ALBUQUERQUE, 2001]**

Protocolo é um serviço de rede que, por uma normatização utiliza uma porta específica do TCP ou UDP.

Em uma rede de comunicação TCP/IP (Transfer Control Potocol/ Internet Protocol) cada serviço utiliza um protocolo para a comunicação de dados e interligação em rede e cada protocolo é responsável por serviços específicos.

7.1. SMTP

"A Internet é considerada como a maior solução de correio eletrônico. Os gateways da Internet conectam as organizações participantes. Ao contrário das

> *organizações privadas ou comerciais, não existe uma única autoridade ou gerenciamento da Internet. Mas mesmo assim, existe uma padronizaçãp no SMTP, alem de gatways da Internet para praticamente qualquer sistema de correio eletrônico prúblico e privado."* **[ALBUQUERQUE,1995]**

O SMTP (*Simple Mail Transfer Protocol*) é o protocolo básico e também o mais importante para um servidor de e-mail, primeiramente porque quando se pensa em um bom funcionamento e uma boa comunicação entre servidores, ele é o protocolo que garante esses fatores, pois é o responsável em enviar mensagens entre servidores e é também usado pelo cliente para enviar mensagens. Definido em 1982, foi projetado como um protocolo especifico para envio de e-mails baseado em texto simples, usa por padrão a porta 25 do TCP tanto para comunicação aberta quanto em TLS (*Transport Layer Security*) ou SSL (*Secure Sockets Layer*), um dos primeiros servidores que utilizaram SMTP foi o Sendmail.

O SMTP possui uma larga quantidade de implementações que permitem que ele seja bastante robusto. Entretanto, muitos consideram que alguns serviços: como anti-spam, blacklists, antivírus e filtros de conteúdos são muito importantes para ser deixado de lado quando o protocolo foi desenvolvido pela primeira vez. Portanto falar do SMTP é falar apenas do seu funcionamento básico, quaisquer outras implementações, apesar de serem possíveis, não estão definidas em nenhuma norma como serviço básico do SMTP. O objetivo do SMTP é transferir e-mails de forma real e eficiente. Uma importante característica do SMTP é sua capacidade de transportar mensagens através de redes, função essa chamada de "SMTP Mail Relaying". Usando o processo de SMTP, pode-se transferir mensagens para outros pedaços da mesma rede ou para outras redes por um relay ou por processos de gateway de ambas as redes.

Desse modo, uma mensagem de correio passa por grande números de relays e gateways para sair do remetente e chegar ao seu destinatario. Os comandos de SMTP são gerados pelo cliente SMTP e enviados para o servidor SMTP. O SMTP envia mensagens de respostas do servidor SMTP para o cliente SMTP sobre esses comandos, essas respostas servem como confirmação de que a comunicação está sendo feita corretamente. Em outras palavras, a transferência de mensagens pode ocorrer através de conexões simples entre o remetente original e o seu destino final, ou pode ocorrer uma série de saltos entre sistemas. Neste caso, a responsabilidade formal da mensagem ocorre: o protocolo requer que o servidor aceite a responsabilidade pela sua entrega de mensagem ou reporte uma falha caso aconteça.

Quando a mesma mensagem é enviada para múltiplos destinatários, o protocolo faz a transmissão apenas de uma cópia do conteúdo para todos os destinatários do mesmo domínio.

O SMTP transporta um objeto de correio. Um objeto de correio contém um envelope e um conteúdo. Um envelope SMTP é enviado com uma série de cabeçalhos de protocolos SMTP's. Neles consistem: o remetente, um ou mais endereços destinatários e material de extensão a mais.

7.1.1. Tipos de SMTP: Originator, Delivery e Sistemas de Gateway

Esta especificação faz a distinção entre quatro tipos de sistemas de SMTP, baseado na regra que estes sistemas estão transmitindo e-mails.

Considerando a Figura 8, onde o usuario Bispo, que trabalha na empresa1, deseja mandar um e-mail para Meedhos, que trabalha na empresa2. O desenho abaixo ilustra alguns tipos de SMTPs envolvidos:

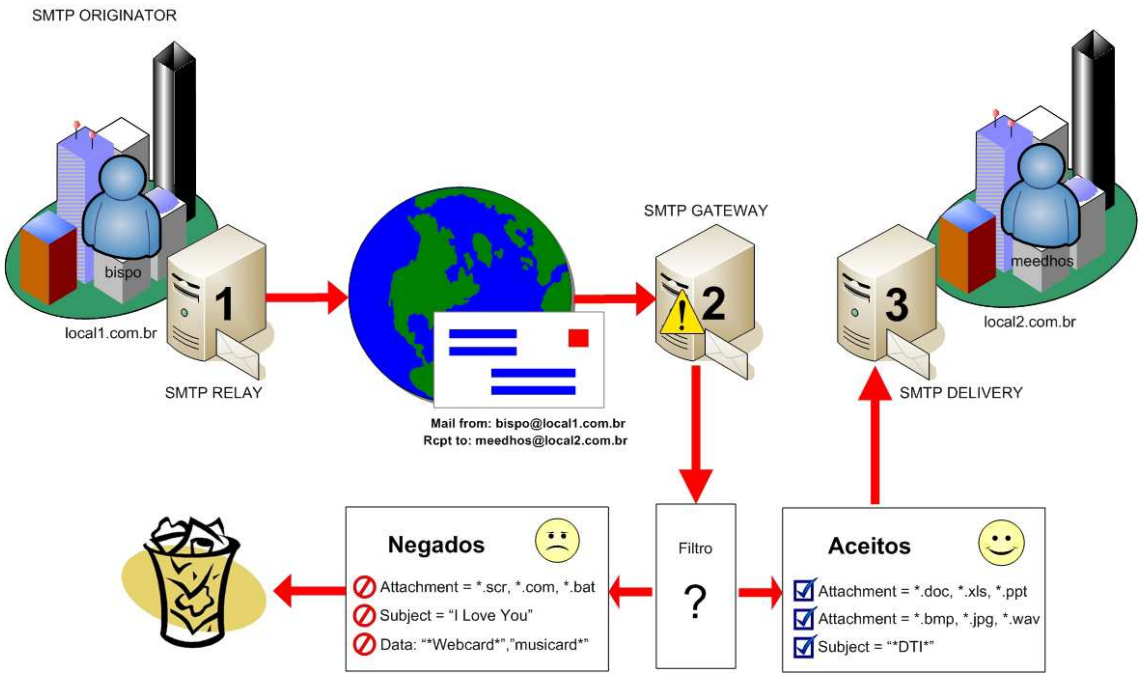

Figura 8 - Exemplo de envio de mensagem com smtp relay, Gateway, delivery

O SMTP ORIGINATOR: envia mensagem para a Internet ou para um serviço de transporte, no desenho acima, o usuário bispo, da empresa local1, está agindo como um SMTP ORIGINATOR.

Um sistema SMTP DELIVERY é um dos que recebe e-mail do ambiente de serviço de transporte e o envia para o MUA ou deposita num local onde o MUA acessará depois, no desenho acima o servidor 3 está sendo o SMTP DELIVERY.

O SMTP RELAY recebe e-mails de um cliente SMTP e o transmite sem modificações do conteúdo da mensagem para outro servidor SMTP para futuro relay ou delivery, o servidor 1, acima, é a demonstração de um SMTP RELAY.

Um sistema SMTP GATEWAY recebe correspondências do cliente de um ambiente e envia para o servidor que está em outro ambiente, fazendo um filtro e barrando o conteúdo que não é bem vindo. No caso acima o servidor 2 está fazendo o serviço de SMTP GATEWAY e bloqueando os conteúdos que não são do interesse da empresa2.

Caso o SMTP GATEWAY decida que uma mensagem deve ser bloqueada ele pode tomar uma série de ações, como por exemplo, responder ao remetente dizendo que a mensagem não pode ser entregue, armazenar a mensagem numa pasta de “Bad Mail” ou simplesmente apagar a mensagem para não gastar processamento e nem ocupar o seu disco.

7.2. POP3

O POP3 (*Post Office Protocol version 3*) funciona muito bem devido à sua simplicidade e robustez para usuários com uma conta de correio eletrônico e por isso a maioria dos servidores de e-mail oferece este protocolo para uso. Ele pode perfeitamente trabalhar em modo “off-line” onde o cliente faz o download de suas mensagens para sua máquina local removendo-as do servidor, isso é uma vantagem respeitosa com relação aos outros protocolos, por outro lado, ele seria inviável, por exemplo, para um empresário ou executivo que tem a necessidade de viajar muito e está a cada dia em um local diferente, como no trabalho, em casa, em outro país ou região, já que estando em diferentes locais, suas mensagens ficariam espalhas em várias máquinas, algumas delas nem pertencendo ao usuário.

O POP3 veio para resolver o problema do uso de e-mails, através de máquinas que não ficam conectadas permanentemente. Seu funcionamento está descrito de acordo com a RFC 1939 (*Post Office Protocol- Version 3*) Este protocolo permite que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas para um computador local. Esse protocolo permite que as estações acessem essas caixas dinamicamente, de uma maneira útil. Com isso, o usuário pode ler as mensagens recebidas, apagá-las, respondê-las ou armazená-las.

É muito interessante, o usuário poder gerenciar suas mensagens do correio eletrônico para sua maquina local, este meio se dá utilizando MUA (Mail User Agent), a partir de programas específicos como o Outlook Express, dentre outros.

O funcionamento do protocolo POP3 se dá da seguinte forma: É estabelecida uma conexão TCP (porta 110) entre o servidor MTA e a aplicação cliente de e-mail que deseja fazer o uso do serviço. No estabelecimento da conexão o servidor envia uma saudação. Logo, são trocados (na ordem da Figura 9) comandos e respostas.

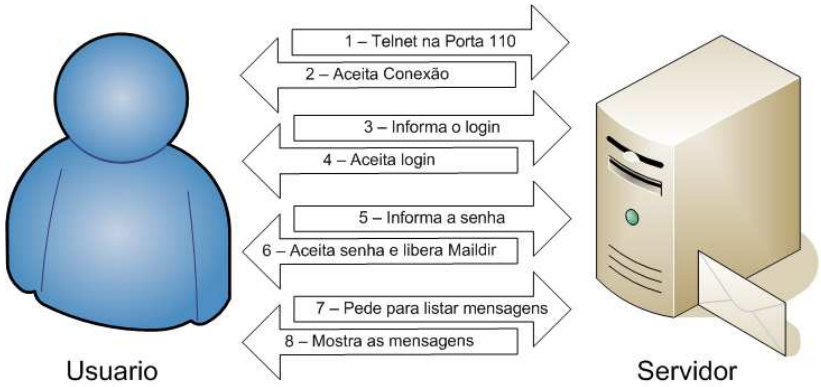

Figura 9 - Representa o envio de mensagens usando o POP3

O usuário tem que se autenticar. Em seguida, as mensagens existentes na caixa são baixadas para o micro do cliente ou, caso o usuário queira ele pode optar por deixar cópia das mensagens no servidor. Em seguida a conexão é encerrada, com isso o usuário poderá ler todas as suas mensagens off-line, sem que a máquina esteja ligada a uma rede local ou Internet (ADSL, Discada ou outros).

Com o POP3, a ligação na rede local ou Internet precisa estar ligada só durante a transferência das mensagens, e a leitura e o processamento das mensagens possa depois ser feitos posteriormente sem nenhum custo, com relação à conexão web.

O servidor define dois tipos de respostas que consiste em um indicador de status, uma palavra-chave e informações adicionais. Todas as respostas terminam com um par de <CRLF>.

As mensagens de status são: +OK para respostas positivas. -ERR para respostas negativas. As respostas podem conter múltiplas linhas. Cada linha termina com um <CRLF> . A última linha consiste de um código decimal 046 que equivale ao caractere (**.**) seguido de um par de <CRLF>. Existem alguns estados que o cliente se encontra: **Authorization**; **Transaction**; **update**.

O estado de autorização se trata do login do usuário. O estado de transação se trata da coleta de mensagens de correio eletrônico do usuário e com a marcação das mensagens para exclusão da caixa de correio. Por exemplo, quando envia um comando “telnet”: ***telnet mail.zoo.ucb.br 110***. Na qual o ***mail.zoo.ucb.br*** é o DNS do servidor. O telnet estabelece uma

conexão TCP na porta 110. Ao enviar esse comando, há uma resposta de “+OK”, quer dizer que a conexão foi estabelecida. O estado de update se trata de comandos de atualização.

7.3. IMAP

O protocolo IMAP (*Internet Message Access Protocol*) foi desenvolvido na Universidade de Stanford em 1986. É um protocolo de gerenciamento de correio eletrônico para manipulação de mensagens entre cliente e servidor de e-mails que necessita do padrão de armazenamento de mensagens Maildir. Este protocolo possui familiaridades e evuluções ao protocolo POP3, como foi introduzido mais recentemente ele possui funcionalidades e recursos superiores ao POP3.

Com muita freqüência, quem utiliza o correio eletrônico da Internet necessita ter acesso remoto à sua caixa de correio. Esta é a situação mais comum, uma vez essas pessoas normalmente usam o seu computador para acesso ao e-mail armazenado em qualquer servidor. Esta situação também abrange usuários que fazem uso de vários computadores para acesso ao e-mail, como no seu local de trabalho, *Lan house*, em casa, entre outros.

Com o IMAP, o usuário envia pedidos e faz consultas no servidor, se autenticando e acessando apenas o cabeçalho de suas mensagens, ele permite copiar o conteúdo de alguma mensagem (mas ele não move do servidor para o micro local) ou até mandar apagá-las no servidor. Ele também tem recursos para manipulação, por exemplo, criar nova pasta, remover pastas, criar uma assinatura. Outra vantagem é que o usuário pode ter acesso à caixa postal ou agendamentos compartilhados entre usuários membros de um grupo de trabalho.

As grandes vantagens do IMAP é a velocidade, se no POP um cliente precisa, por exemplo, da décima quinta mensagem, ele necessariamente tem que baixar as primeiras 15 para chegar onde ele quer, no IMAP ele lê apenas o cabeçalho de cada mensagem (que é extremamente menor) e escolhe diretamente qual mensagem deseja descarregar no momento.

A última versão do protocolo é o IMAPv4, definido pela RFC 2060 – Internet Message Access Protocol – Version 4rev1, é orientado à conexão e utiliza a porta TCP 143.

Ele possui muitos recursos, pode-se ativar ou desativar marcadores de características da mensagem, que podem ser definidas pelo usuário.

O IMAP possui também algumas características, como:

- O tamanho do armazenamento das mensagens é definido pelo administrador do servidor do correio eletrônico, que fornecerá um limite de armazenamento atribuído para cada usuário.
- O usuário tem sempre que estar conectado a Internet ou numa rede local todo o tempo, para o acesso das novas mensagens ou das mensagens que ele possua apenas o cabeçalho.

Com relação ao acesso as mensagens eletrônicas. São três as formas possíveis de se trabalhar com correio eletrônico remotamente [segundo o documento da RFC 1733 – Distributed Eletronic Mail Models In IMAP4]: "on-line", "offline" e "disconnected".

- On-line - as mensagens e pastas ficam armazenadas no servidor. Neste modo o usuário manipula remotamente através de um programa cliente de correio eletrônico, sendo possível adicionar, apagar, renomear ou mover pastas, ativar marcações em mensagens, receber, parte de mensagens, de acordo com a seleção escolhida.
- Offline - É o modo de acesso mais conhecido e mais antigo, para manipulação remota de mensagens. Como já foi descrito acima, neste modo o programa transfere o pacote de novas mensagens do servidor para o computador do usuário e as apaga da sua origem, passando então, todo o processamento de mensagens para o computador local do usuário, inclusive as informações sobre o "status" das mensagens passam a ser mantidas pelo programa cliente.
- Disconnected - É comumente confundido com o modo "offline" de acesso. Há diferença é que o programa do usuário faz uma cópia em cache (memória RAM) das suas mensagens e desconecta-se do servidor, ou seja, o usuário fica com copias no servidor e na sua máquina local.

O modo “offline” do IMAP é ideal para o usuário que vai sempre utilizar o mesmo computador para acessar suas mensagens e é similar ao protocolo POP3. Esse modo de operação "offline" também permite a opção de deixar as mensagens originais no servidor após terem sido copiadas para o computador do usuário. Mas este meio de acesso ainda não é muito bom com relação aos outros modos, pois os outros dois, tanto o "on-line" quanto o "disconnected" utilizam melhor os recursos do IMAP, além da otimização da transmissão.

O que interessa é que o usuário tem como acessar, remotamente, sua caixa postal e suas pastas armazenadas em um servidor, de modo uniforme, a partir de diferentes computadores em momentos diferentes sem depender de protocolos de sistemas de arquivos que não estão disponíveis em todas as plataformas e que podem trazer diversos tipos de problemas no acesso simultâneo a um mesmo arquivo ou pasta.

7.3.1. IMAP e Segurança

Com relação ao contexto de segurança, já foi encontrado vulnerabilidades em certas implementações do servidor IMAP em diversas plataformas.

Aos que queiram implementar o IMAP, é recomendável obter e instalar a versão mais recente, para evitar falhas de segurança das versões anteriores do servidor. A última versão, produzida pela Universidade de Washington para sistemas UNIX apresenta correções de potenciais falhas de segurança presentes em versões anteriores. A Tabela 4 mostra um comparativo entre os protocolos IMAP e POP3

Característica	**POP3**	**IMAP**
Onde o protocolo está definido?	RFC 1939	RFC 2060
Porta TCP a ser usada?	110	143
Onde está armazenado o e-mail?	PC do usuário	Servidor
Onde é lido e-mail?	Off-line	On-line
Tempo de conexão exigido?	Pequeno	Grande
Utilização de recursos do servidor?	Mínima	Intensa
Várias caixas de mailboxes?	Não	Sim
Quem guarda cópias das mailboxes?	Usuário	ISP
Bom para usuários em trânsito?	Não	Sim
Controle de usuário sobre o download?	Pequeno	Grande
Downloads de mensagens parciais?	Não	Sim
Quotas de disco constituem um problema?	Não	Possível, após algum tempo
Implementação simples?	Sim	Não
Suporte difundido?	Sim	Crescendo

Tabela 4 - Comparação entre os protocolos IMAP e POP3

Fonte: TANENBAUM, Andrew S. Computer networks

7.4. NNTP

O NNTP (*Network News Transfer Protocol*) é o protocolo usado por usuários de notícia do USENET e por clientes (leitores) e é definido pela RFC 977. Como exemplo vale citar o servidor de NEWS da Microsoft. Especifica o modo de distribuição, busca, recuperação e postagem de mensagens usando um sistema de transmissão de notícias numa comunidade ARPA na Internet.

Usenet (*Unix User Network*) é um meio de comunicação onde as pessoas trocam mensagens de textos (Artigos) em fóruns. Estes fóruns geralmente vêm agrupados por assuntos, assim o usuário recebe apenas as mensagens que lhe interessa. As mensagens postadas nos *newsgroups* não são transmitidas diretamente, quando um artigo é postado ele é retransmitido por uma enorme rede de servidores que disponibilizam esse serviço e estão interligados.

Esse serviço surgiu em meados dos anos 80, os computadores que participavam dessa rede na época se comunicavam através de conexões discadas através do protocolo chamado UUCP, que era um protocolo de transferência de arquivos, muito usado na era pré-Internet em sistemas de correio eletrônico, onde os servidores se conectavam à rede via modem, suas conexões eram muito caras, muitas vezes era necessário discar separadamente para vários computadores, daí o fato de sua conexão não ser contínua como na Internet de hoje. Com a popularização da Internet nas décadas de 80 e 90 o sistema passou a funcionar quase que completamente baseado no protocolo NNTP esse é um protocolo da família de protocolos TCP/IP. A maioria das máquinas que fazem parte da rede Usenet são conectadas através do programa chamado INN que é hoje o servidor mais utilizado para esse tipo de serviço. O protocolo do NNTP existe na camada de aplicação do modelo de OSI.

O NNTP utiliza a porta 119 do TCP; O NNTP com SSL utiliza a porta 563 do TCP.

7.5. Protocolo SSL

O SSL é um protocolo que criptografa um protocolo já existente. Routo define que criptografar é *"basicamente objetiva esconder informações sigilosas de pessoas desautorizadas a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia."* **[TERADA,2000].**

Criptografia é o método que se utiliza de regras para codificar um texto, ou imagem, para que o conteúdo seja compreensível à leitura apenas usando as regras para decodificar novamente o texto, garantindo a integridade, segurança e sigilo dos dados.

O protocolo SSL foi criado pela Netscape Corporation, com o objetivo de proporcionar mecanismos de autenticação e segurança entre duas aplicações que se comunicam por algum tipo de protocolo de comunicação, por exemplo, o TCP/IP. A função do SSL foi concebida pela necessidade de se ter um sigilo dos dados que trafegam na rede e garantir a autenticação eletrônica como nas transações bancárias, dentre outras aplicações. Sua versão mais recente é a 3.0.

Desde sua criação, o protocolo SSL vem se tornando padrão a cada dia, porém a implementação básica somente com técnicas de criptografia do próprio protocolo SSL, já não é suficiente para garantir uma boa segurança nos negócios on-line. Com isso, surgiram novos mecanismos que podem ser adicionados na configuração do mesmo, que ajudam na segurança do protocolo.

Como foi projetado para trabalhar com protocolos confiáveis, o SSL roda sobre o protocolo TCP, que é o principal protocolo de transporte da Internet, onde o cliente e o servidor podem se autenticar.

Neste sentido, Largura (2000) define que a proposta desse protocolo "é permitir a autenticação de servidores, encriptação de dados, integridade de mensagens e, como opção, a autenticação do cliente, operando nas comunicações entre aplicativos de forma interoperável." [**LARGURA,2000**]

7.5.1. Características do SSL:

O protocolo de segurança SSL(Secure Socket Layer) segundo Largura*(2000) " é um protocolo de comunicação que implementa um duto seguro para comunicação de aplicações na Internet, de forma transparente e independente da plataforma."* [**LARGURA,2000**]

O SSL usa a criptografia simétrica o que garante a segurança dos dados transmitidos, evitando assim, possíveis ataques para que os dados não sejam modificados, chegando aos destinos intactos. Este protocolo faz isso, utilizando o MAC (*Message Authentication Code*) que garante a integridade das mensagens, além disso, o protocolo utiliza autenticação entre cliente/servidor.

É um protocolo independente de qualquer outro protocolo, ou seja, roda em qualquer protocolo de transporte. Além do mais possui outras características como: interoperabilidade, extensibilidade e eficiência, ou seja, é muito úteis nas mais sensíveis transmissões de informação, como dados pessoais e números de cartão de crédito.

O protocolo SSL se incorpora em quatro mecanismos de segurança, são eles: autenticação (identificação da fonte dos dados), integridade (garantia de alteração de dados), criptografia (garantia de privacidade) e troca de chaves criptográficas (aumento da segurança).

7.5.2. Como é realizada a conexão cliente/servidor

O cliente realiza uma conexão a uma página protegida pelo protocolo SSL, em seguida o servidor envia uma solicitação para iniciar a sessão segura. Caso o navegador suporte SSL, retorna uma resposta. Com isso, o cliente (browser) e o servidor trocam informações seguras. A resposta do navegador define o ID da sessão, os algoritmos de criptografia e os métodos de compactação que suporta. Nas informações de segurança fornecidas pelo browser, o servidor faz sua seleção e a comunica ao browser. O servidor e o *browser*, em seguida, trocam certificados digitais utilizando a infra-estrutura de chaves publicas (PKI) e autoridade certificadora (CA). O servidor também especifica uma chave pública ("chave de sessão") apropriada para o algoritmo de criptografia anteriormente selecionado. O *browser* pode, então, usar a chave pública para criptografar informações enviadas ao servidor, e o servidor pode usar sua chave privada para descriptografar essas mensagens. Depois que o servidor e o browser estão de acordo sobre a organização da segurança, as informações podem ser transmitidas entre os dois com segurança.

8. SPAM

Com o passar dos anos, o uso da Internet e do correio eletrônico se tornou um dos principais meios de comunicação, e com isso veio alguns desagrados. Desde o seu surgimento, no qual se tornou um dos principais problemas da comunicação eletrônica no geral. Esse conceito está relacionado ao spam.

O conceito de spam quer dizer o uso do correio eletrônico para mandar mensagens não-solicitadas a uma pessoa, ou grande quantidade delas. Geralmente o conteúdo destas

mensagens, normalmente não oferece utilidade nenhuma para quem os recebe, e o envio descontrolado acaba congestionando os servidores de e-mails corporativos, como também dos provedores de acesso a e-mails. Muitas vezes, esse transtorno pode fazer, até mesmo, que o serviço de e-mail pare de funcionar por um tempo indeterminado, fazendo o administrador da rede trabalhar várias horas.

Quando se fala em spam, logo vem o termo correio eletrônico, que é a forma mais comum de enviar esse desconforto. Spammers utilizam programas que facilitam a obtenção de endereços de pessoas e acaba enviando a uma grande quantidade de pessoas.

Entretanto, existem vários métodos diferentes para um spammer obter uma lista de endereços. Um dos procedimentos mais comuns é utilizar programas que executam varreduras em ambientes corporativos, já que numa corporação possui um número elevado de endereços disponíveis.

8.1. Origem

Segundo a RFC 2635 (*DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings*), o termo spam deu origem na Inglaterra durante a segunda guerra mundial, devido a uma marca de carne suína enlatada chamada SPAM, que foi associado ao envio de mensagens não-solicitadas. Essa marca foi um dos alimentos eliminados na cidade, levando as pessoas a enjoarem da tal marca, dando início ao contexto spam.

Um exemplo disso foi, um casal discutindo com uma garçonete em um restaurante a respeito da quantidade de SPAM presente nos pratos. A discussão faz com que um grupo de vikings presentes no restaurante comece a cantar: "SPAM, amado SPAM, glorioso SPAM, maravilhoso SPAM".

Uma das definições da palavra spam significa Sending and Posting Advertisement in Mass (Enviar e postar publicidade em massa). A segunda significa Shit Posing As Mail (porcaria fingindo ser correspondência).

O primeiro registro oficial de uma mensagem eletrônica não solicitada enviada em massa ocorreu no CTTS (*Compatible Time-Sharing System*) do MIT (*Massachusetts Institute of Technology*). O sistema, criado em 1961, consistia em um computador que podia ser acessado por múltiplos usuários através de diferentes terminais. Pouco tempo depois de sua criação, Tom Van Vleck e Noel Morris implementaram o programa CTSS MAIL que permitia que usuários se comunicassem através de mensagens.

Com a criação da ARPANET, algum tempo depois, a rede de computadores da Internet, e do sistema de correio eletrônico, começou a observar o problema do envio de mensagens não-solicitadas, assunto que chegou a ser descrito em 1975, na RFC 706. Em 1978 ocorreu o primeiro registro de uma mensagem não solicitada enviada em massa através do correio eletrônico.

Na época a ARPANET era considerada somente de uso exclusivo para assuntos do governo Norte-Americano, a questão do spam não foi considerada de grande importância. Hoje em dia, muitos órgãos consideram o spamming como um dos maiores problemas da Internet. Antes, acreditava-se que as conseqüências do spam eram pequenas e não justificavam a criação de um sistema de controle que pudesse julgar tal mensagem como sendo spam.

Foi na rede Usenet, o maior sistema de grupos de notícias e listas de discussão da época, que o uso do termo spam se popularizou na década de 1990, que depois disso começaram a pensar nesse termo com mais cautela, e posteriormente em alguma forma de bloquear esse tipo de mensagem.

Com a popularização da Internet, o envio de mensagens não-solicitadas passou a crescer nos correios eletrônicos, em parte estimulado pela existência dos programas para envio automático de mensagens, e se expandiu rapidamente para os outros meios disponíveis, não somente no correio eletrônicos, outros como paginas oferendo produtos grátis, páginas pornográficas, entre outros. Os spams são classificados em:

- Hoaxex (Boatos): Histórias falsas com intenção de alarmar ou iludir aos que lêem com o objetivo de divulgar para o maior número de pessoas;
- Chain letters (Correntes): Mensagens que prometem benefícios (sorte, riqueza) para as pessoas que reenviar esta mensagem para um número X de pessoas, inclusive com pequenas ameaças do que pode acontecer se a mensagem não for enviada;
- Propagandas: divulgam algum tipo de produtos ou serviços, como medicamentos, ervas naturais, softwares, diplomas, cassinos, produtos eróticos, entre outros;
- Scam (Golpes): oferecem ofertas de ganho de dinheiro fácil (e normalmente uma quantia alta) trabalhando em casa, empréstimos, pedindo uma pequena quantia para começar esse “negócio”, muitas vezes tentam simular uma

mensagem confidencial. Quando o usuário paga a quantia de entrada o usuário simplesmente perde o dinheiro.

- Phishing (Estelionato): são mensagens que assumem o disfarce de “spam comercial”, ou simulam mensagens comuns (como comunicados de uma organização ou mensagens pessoais) fazendo com que o destinatário acredite e envie dados pessoais, como preenchimento de formulários, esses cadastros são usados para fazer compras on-line, abrir contas bancárias, entre outros.

8.2. Questões sociais, econômicas e políticas

No meio social, existe algumas organizações de combate ao *spam*, na qual criticam a tal prática se baseando no espaço em que essas mensagens ocupam, no tempo em que levam para enviarem. Porém, existem outras organizaões que são a favor do envio **spam**, não somente dos spammers, mas organizações que disponibilizam produtos anti-spam.

Um grande número de mensagens não-solicitadas são do tipo maliciosa, que fazem com que o uso do spamming seja visto negativamente. Vendo isso, a DMA (*Direct Marketing Association*) propôs uma definição de *spam* que se restringia somente a esse tipo de mensagem. Mesmo assim, qualquer tipo de mensagem não-solicitada é considerada como incômodo aos usuários, pois, o alto volume de **spam** recebido por qualquer usuário pode aumentar a cada dia, se o usuário não tiver nenhum controle desse tipo de mensagem.

Existe um consenso entre estatísticos e economistas de que, apesar do baixo custo de envio, o lucro resultante do spamming não é suficientemente compensador, dado o incômodo que ele pode causar aos clientes. Em outras palavras, os spammers realmente beneficiados pela prática são aqueles cujo propósito tende ao ilícito.

Uma comparação entre a publicidade e o **spam** costuma ser contra-argumentada através da definição de **spam** e da relação deste com os meios de envio. A diferença entre o *spammer* e os anunciantes de publicidade, é que o spammer não tem custo nenhum com relação ao provedor de envio, pois alguns provedores declaram ser prejudicados pelo ato de envio de **spam**, e os anunciantes pagam pelos serviços prestados às emisoras de televisão como propagandas, comerciais dentre outros.

De acordo com um estudo realizado pela Spam Filter Review, 40% de todas as mensagens de e-mail transmitidas no ano de 2003 foram **spam**, um valor que exige dos provedores de e-mail um grande espaço de armazenamento em disco e além do mais a

transmissão desse tipo de mensagem. Sendo assim, as empresas começaram a investir em filtros anti-spam para bloquear mensagens não-solicitadas.

Para os usuários de correio eletrônico corporativo, o **spam** representa uma perda de tempo que reduz sua produtividade na empresa, o que ocasiona custos não somente à organização, mas também para o lado do funcionário que recebe a mensagem. Porém, do ponto de vista do **spammer**, essa prática muitas vezes pode ser lucrativa, no caso de algumas dessas mensagens enviadas pode resultar em venda de algum produto, ou algum tipo de fraude, no qual compensa o tempo que perde para enviar a mensagem.

No Brasil não existem leis que tratam especificamente da prática de *spamming*. Mesmo se houvesse não há como identificar, localizar e punir os spammers infratores, que geralmente tem um nome e endereço eletrônico falsos.

Os Estados Unidos possui uma lei federal (*can-spam act of 2003)*, que tem o objetivo de regularizar o envio de mensagens eletrônicas comerciais no território norte-americano, visando punição aos infratores e fraudadores. Essa lei faz com que as mensagens comerciais tenham cabeçalho válido, identificando endereço eletrônico do remetente, que contenha também, o assunto como um texto que não impeça o receptor de identificar a mensagem incluindo algum tipo de mecanismo para o destinatário poder interromper o envio desse tipo de mensagem a qualquer momento, no caso dele não querer receber mais nenhuma mensagem daquele gênero.

8.3. Técnicas dos spammers

A maioria dos usuários de correio eletrônico hoje em dia consegue identificar quando uma mensagem é **spam**, por isso, os *spammers* devenvolvem a cada dia novas práticas para confundir o destinatário. Utilizando-se de métodos cada vez mais elaborados para atrair a atenção do usuário e enganá-lo.

Outra técnica utilizada por *spammers*, é a alteração do texto, das palavras e do conteúdo das mensagens**,** que tem por finalidade enganar os programas que filtram as mensagens e definem como **spam** ou não.

8.4. Técnicas dos anti-spammers

Um das principais técnicas utilizadas para barrar **spam** é o uso de filtros de conteúdo. Estes programas fazem uma análise do texto da mensagem não-solicitada com a finalidade de saber se ela é ou não **spam.** Quando uma mensagem é classificada com **spam**, pode ser removida ou transferida automaticamente para uma pasta dentro do e-mail do cliente (dentro uma pasta *"Lixo Eletrônico"*, por exemplo). Este tipo de serviço é bastante eficiente, porém, tem a desvantagem de julgar como **spam** uma mensagem que pode ser normal.

Outra técnica usada para controlar o nível de **spam** é esconder endereços de correio eletrônico por camuflagem. Alguns interpretadores de textos que fazem varreduras na Internet em busca de endereços eletrônicos podem ser enganados pela criptografia, como por exemplo trocar a palavra "@" por "at", descaracterizando os endereços de e-mail.

8.4.1. Controle de Conteúdo

Atualmente existem várias técnicas de bloqueio de spam que se baseia na análise do conteúdo da mensagem, reconhecendo padrões do conteúdo que buscam identificar se o e-mail pode conter um vírus ou se tem características comuns aos Spams, como é possível analisar na figura abaixo Tais filtros podem ser usados em conjunto com o MTA, MDA, ou ainda no aplicativo do usuário.

As mensagens que supostamente pode ter algum tipo de anomalia podem ter quatro destinos:

1º - Rejeita e devolve a mensagem;
2º - Aceita e apaga a mensagem;
3º - Aceita e coloca em quarentena;
4º - Entrega a mensagem ao destinatário

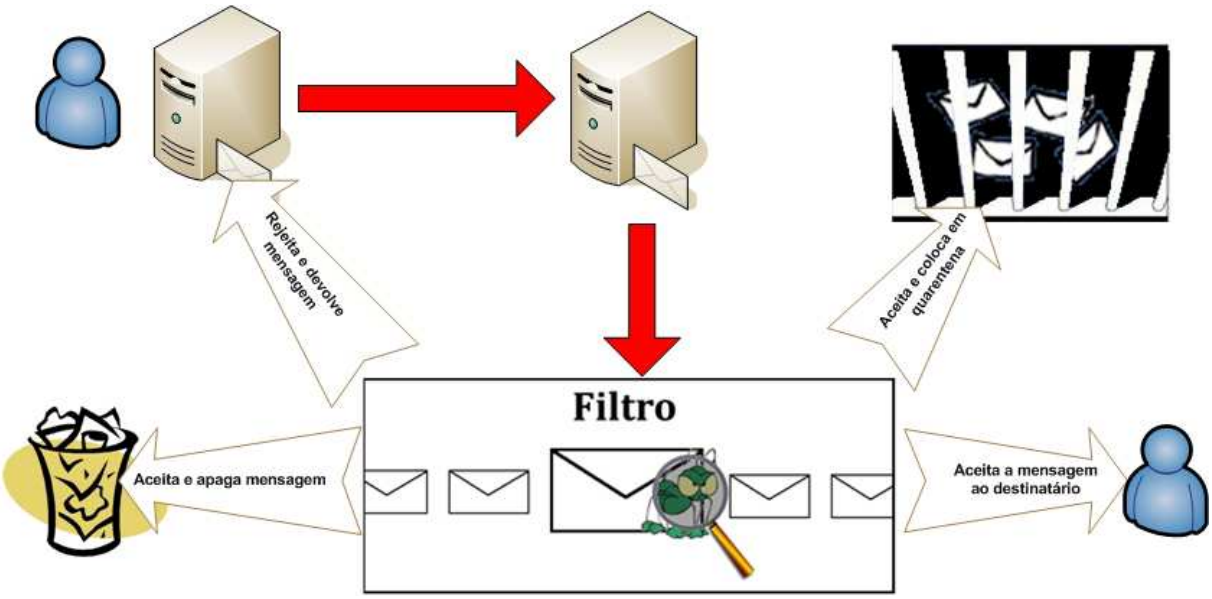

Figura 10 - A mensagem ao passando pelo filtro de conteúdo

8.4.2. Filtros Bayesianos anti-spam

Os filtros bayesianos anti-spam verificam o conteúdo da mensagem e avaliam a possibilidade dela ser spam, em função de uma base de conhecimento já armazenada. É necessário fazer regras para o filtro, para que ele forme a base de dados, injetando mensagens boas e ruins, ou seja, fazer realmente um treinamento dessas mensagens, que pode ser contínuo e concomitante com a operação regular. Um filtro bastante popular de reconhecimento de spam é o SpamAssassin, que será detalhado com mais precisão no item 12.4.

Os mesmos programas usados para desmontar mensagens para antivírus podem acionar filtros anti-spam. Ao contrário dos antivírus, porém, o foco desses filtros é muito mais o texto da mensagem do que os anexos.

Para colocar um filtro funcionando e se adaptando ao caráter mutável do **spam** é necessário que haja um treinamento contínuo, com devida identificação dos **spams** que não foram classificados e das mensagens que não são **spam** e que foram rotuladas como sendo **spam.** Para realizar o controle de mensagens, há um consumo de recursos computacionais muito elevados, mas muito menor com relação ao antivírus, mas mesmo assim pode ser comprometedor em servidores que possuem tráfego alto na rede.

É aconselhável não descartar qualquer mensagem marcada como **spam**, colocando-a em quarentena, já que os **filtros bayesianos** podem acarretar falsos positivos. Tal problema ser agravado, no caso da base de dados com que ele toma a decisão estiver em um outro idioma ou simplesmente desatualizada.

Deve-se estar atento, também, no caso de estes filtros poderem ser enganados por **spammers** que injetam "ruídos" em suas mensagens, ou seja, além do texto do **spam** são introduzidas palavras aleatórias, palavras com outro idioma, letras. Podendo gerar um resultado insignificante na análise estatística das ocorrências de palavras. Uma outra técnica utilizada para desviar **filtros bayesianos** é a utilização de "ASCII arte" e imagens.

8.4.3. Antivírus

No grande mercado da tecnologia da informação existem várias opções de antivírus que podem ser utilizados em conjunto com MTAs, sendo que algumas destas opções é a utilização de software livre, nessa solução apresentada utiliza-se o *Clamav*. A maioria deles possui mecanismos de atualização automática, já que a criação de novos vírus é bastante intensa e exige atualizações diárias, ou até mesmo mais freqüentes, das assinaturas dos antivírus.

Os programas antivírus não lidam diretamente com arquivos comprimidos ou no formato usual dos e-mails. Deste modo, antes do conteúdo da mensagem ser analisado pelo antivírus é necessário desmontar a mensagem e possivelmente descomprimir os anexos. Um programa muito comum para realizar estas tarefas é o *Amavis*, que também será utilizado na solução proposta para implementação.

É aconselhável passar as mensagens ao antivírus depois que foram avaliadas por técnicas como o uso do *Amavis*. Com isso, a passarem por esse tipo de trabalho de desmontagem, e do uso de antivírus com os MTAs, o processamento da máquina e da memória do servidor vai ao um nível bastante alto, em relação ao nível normal.

No MTA Postfix o controle de conteúdo pode ser divido em duas partes:

1. Ferramentas embutidas: Essas ferramentas têm a finalidade de resolver problemas mais simples. Essas ferramentas possuem dois tipos de controle:

a. ***Restrictions:*** Supervisiona o diálogo SMTP aceitando ou rejeitando mensagens baseado no remetente (*mail from*), destinatário (*rcpt*), IP ou *hostname*.
b. ***Checks:*** Examina o conteúdo da mensagem, verificando cabeçalho, corpo da mensagem, anexos e cabeçalhos de mensagens anexadas. Apesar de ter um funcionamento relativamente simples, o administrador deve tomar cuidado com a complexidade das expressões regulares utilizadas. Em geral é utilizado para bloquear mensagens originadas de certos tipos de programas, e com determinados títulos (*subject*), e também tipos de anexos considerados muito maliciosos.

2. Ferramentas externas: Tem a finalidade de lidar com problemas mais complexos. Esse tipo de ferramenta atua onde o controle de cabeçalho e corpo da mensagem já não consegue atuar, em geral efetuam varredura procurando por vírus ou *worms*, detectam spam. Os *daemons pipe, smtp* e *lmtp* podem delegar a filtragem de mensagens a aplicações externas. Em geral instala-se o programa *amavisd-new* como um intermediário entre os *daemons* citados e as ferramentas de Anti-spam (por exemplo: Spamassassin) ou antivírus.

A quem for implementar uma solução de controle de conteúdo não pode esquecer-se de estar atento de que uma filtragem ideal não é atingida em um primeiro momento. Deve ser implementada e testada aos poucos, colocando-se poucas restrições, testá-las e somente após colocar a implementação efetivamente em uso. Levando em conta, a questão dos falsos positivos e falsos negativos. No primeiro pode-se rejeitar e-mail que a princípio não deveriam estar sendo rejeitados, e no segundo caso ocorre o inverso.

O Postfix possui um parâmetro *warn_if_reject* que é extremamente útil para avaliar o impacto de uma regra de rejeição, permitindo que o *log* registre a mensagem que seria rejeitada. Deste modo pode-se avaliar o impacto de determinada regra sem descartar mensagens que podem ser verdadeiras, ou seja, falso negativo.

8.4.4. Bloqueio de anexos

O bloqueio de anexos é automático, e já bloqueia a mensagem dependendo do tipo de arquivo enviado pelo receptor (até mesmo de pessoas conhecidas da própria lista de contatos), como muitos cavalos de tróia e vírus que afetam sistemas Windows são enviados, por exemplo, em arquivos executáveis (.exe) ou associados a certos aplicativos, como screen savers (.scr), (.lnk), (.bat), alguns administradores procuram bloquear mensagens com determinados arquivos anexados.

As informações que são obtidas através do cabeçalho MIME, têm a função de apoiar no bloqueio das mensagens com base no tipo ou no nome do arquivo. Os tipos dos anexos são dados pelo campo Content-Type, e os nomes dos arquivos pelo atributo ’name’ deste campo.

Na prática, no entanto, esta técnica pode bloquear anexos que não são maliciosos, mas que estão entre os tipos proibidos, e pode deixar passar anexos que aparentemente não são hostis, como é o caso de imagens que exploram falhas no software usado para exibi-las.

Os antivírus podem ser eficazes na detecção de códigos maliciosos, porém, os filtros de conteúdo podem consumir muitos recursos e produzir falsos positivos, podendo dificultar a identificação dos spams.

9. LISTAS NEGRAS E LISTAS BRANCAS

As *"Blacklist"* (listas negras) são listas de remetentes conhecidos de spam, e as *"Whitelists"* (listas brancas) são remetentes conhecidos de e-mails que possam ser classificados como spam, mas que contém informações desejadas.

Além das *"Blacklists"* e *"Whitelists"* definidas pelo administrador, os usuários podem criar *"Blacklists"* e *"Whitelists"* pessoais para aumentar a personalização e a precisão do seu filtro de Spam.

9.1. Blacklists (listas negras)

As listas negras, conhecidas como blacklist, definem o local onde o administrador irá incluir os e-mails de quem não deseja receber mensagens.

É uma lista contendo os endereços IP de máquinas que enviam *spams*. Assim, verificam se os endereços IP dos remetentes das mensagens recebidas estão presentes na lista e, caso positivo, a mensagem é descartada e deletada. Não é atoa, quando as pessoas dizem que alguém está na sua lista negra.

A eficácia da lista negra pode ser medida pela rapidez de atualização de seus endereços IPs. Assim que se detecta uma máquina que está enviando *spams*, o seu endereço IP deve ser inserido na lista e assim que a máquina deixa de enviar o endereço IP deve ser retirado. É comum uma máquina ser infectada e passar a ser um zumbi que envia *spams* e seu endereço entrar na lista negra. Uma vez a máquina sendo desinfectada o endereço deve ser retirada da lista negra, pois, caso contrario, todas as mensagens enviadas continuarão a ser classificadas como *spams*.

9.2. Whitelists (listas brancas)

As listas brancas, conhecidas como *"Whitelist"*, é a lista onde estão seus contatos autorizados a enviar mensagens para você sem ter que ficar passando pelo anti-spam, lembrando que a qualquer momento ele poderá ser excluído desta lista e ser cadastrado na blacklist.

Normalmente, a lista branca é gerenciada e mantida pelo administrador da rede, podendo ser implementada através de DNS, listas de domínios e IPs. Esse tipo de lista é na verdade uma lista de exceções às regras de bloqueio por listas negras.

10. FALSO POSITIVO / FALSO NEGATIVO

A questão do falso positivo e falso negativo são termos que estão relacionados ao **spam,** ou seja, SPAMs aprovados (falso negativos) e mensagens "boas" reprovadas (falso positivo).

Um falso positivo é um erro no qual o anti-spam ou antivírus reporta (barra) que um arquivo ou mensagem está contaminado, quando na verdade essa mensagem está livre de vírus ou spam.

Um falso negativo é um erro mediante o qual o antivírus ou anti-spam falha, na identificação desse arquivo, deixando passar um conteúdo contaminado.

As taxas de falso positivos e falso negativos num sistema anti-spam são de suma importância no uso do correio eletrônico, os falso-positivos que corresponde à taxa de mensagens legítimas classificadas como spam, e os falsos negativos, que é a taxa de spam classificadas como legítimas. Em geral, a taxa de falso positivo tem um grande impacto, pois classificar como *spam* e filtrar uma mensagem legítima podem gerar grandes transtornos, prejuízos financeiros e atrasos no processo de comunicação.

O falso negativo tem um impacto menor, pois o usuário perderá apenas um determinado tempo abrindo e lendo os *spams* para depois apagá-los. Outro aspecto importante de um sistema anti-*spam* é a sua interferência com o usuário. Quanto maior o nível de interação com o usuário, mais complexo o sistema se torna, dificultando que um usuário simples venha a adquirir o sistema, ou seja, um usuário que não é da área da TI.

11. ASPECTOS JURÍDICOS

Uma Empresa que deseja implementar o serviço de e-mail corporativo, deve antes de mais nada se preocupar com os possíveis problemas que este tipo de serviço pode gerar. Não somente problemas técnicos no serviço de e-mail mas também judiciais.

É cada vez maior o número de empresas preocupadas com a segurança das informações ameaçadas muitas vezes pelo uso indevido do e-mail e da Internet, ferramentas de suma importância no dia a dia do trabalho.

Com o aumento e facilidade da Internet houve um rápido crescimento na utilização dos instrumentos eletrônicos. Porém, esse meio representa um novo conceito sem precedentes. Sendo assim, não existe, ainda, uma normatização e sim diversas opiniões a respeito.

"A informática pode servir ao Direito como objeto e como meio. Com isso surgem novos campos de estudos na área jurídica num trabalho de se procurar determinar a aplicabilidade e infuência da nova tecnologia". **[SILVA,2003]**

Já que a legislação ainda não está adaptada para a arquitetura e os serviços de rede, não existe uma norma especifica. Assim, a lei fica entre a privacidade do cidadão e o direito da empresa sobre a correspondência de e-mail.

Diante disso, algumas empresas tomam medidas e ações para coibir o mau uso por funcionário, muitas vezes consideradas arbitrárias na visão de alguns especialistas.

Essa situação deve preocupar não só as pessoas físicas, mas também as pessoas jurídicas. No caso de usuários domésticos ou profissionais, a razão é clara, que é preservar o sigilo de suas informações. Portanto, as empresas têm o dever de assegurar o sigilo, porque as regulamentações setoriais de cada mercado têm recentemente imposto deveres de Segurança da Informação que se não forem respeitados, sujeitam a empresa e os seus gestores a multas, indenizações, suspensão de atividades on-line, e até mesmo sanções penais.

O grande problema quando se fala em aspectos jurídicos sobre o e-mail é que a maioria das empressa só se dá conta da gravidade e seriedade que a falta de uma definição política de acesso pode causar quando ocorrem sérios danos a organização.

Logo não pode ser abordado o que deve ser feito e sim levantadas as opiniões e justificativas dos especialistas para que seja possível uma análise e interpretação e criação de um regimento interno.

"É extremamente difícil analisar qual a melhor solução a adotar. Os questionamentos são muitos, inúmeros aspectos devem ser analizados, sendo assim, a escolha mais apropriada é levar em conta a realidade da organização" **[FILHO,1999].**

Preocupadas com o uso indevido do e-mail, roubo de informações sigilosas e até mesmo degradação da imagem de sua organização, as empresas cada vez mais procuram fiscalizar o e-mail de seus colaboradores, prova disto está em um estudo da American Management Association, realizado no ano de 2001, mostrando que mais de ¾ das maiores empresas dos Estados Unidos utilizam ferramentas de monitoramento eletônico, 77%, realizam essa prática em seus empregados ao menos ocasionalmente, outro estudo realizando também pema American Management Associetion em 2005, aponta que 26% das empresas americanas tem despedido trabaladores por uso indevido de internet e 25% tem denunciado seus empregados por desvio de e-mails contendo informações sigilosas.

"Hodiernamente, surge a necessidade de delinear a fronteira entre o direito à intimidade do empregado e o poder de direção do empregador, por tratar-se de tema atual, de extrema importância e ainda insuficientemente abordado pelo ordenamento jurídico pátrio, onde não se encontram diretrizes específicas para a regulamentação dos procedimentos de fiscalização dos correios eletrônicos no ambiente de trabalho." **[MELO,2005]**

11.1. Modalidades da Fiscalização Eletrônica

Ao se analizar a fiscalização e o monitoramento eletrônico em uma corporação vale ressaltar que a fiscalização das mensagens de correio eletrônico, de forma a não se pesquisar o conteúdo das informações presentes nas mensagens, mas somente observá-las quanto a presença de vírus de computador, é legal e de consenso geral de todos os especialistas, Bruno Herrlein afirma que essa prtática *"é indiscutivelmente possível, lícita e até necessária, em virtude do atual fluxo de programas destrutivos na Internet."* **[MELO,2005].**

Quanto essa fiscalização ultrapassa o carater preservatório do ambiente informativo da empresa e essa fiscalização segue uma linha de observação do conteúdo das mensagens as opiniões entram em conflitos, Carla Rodrigues defende que:

"O sigilo das correspondências constitui uma garantia constitucional prevista no artigo 5º, XII. Correspondência é uma troca de informações entre pessoas ausentes, que pode ser

feita por cartas, bilhetes e agora por computador. O e-mail nada mais é do que uma correspondência enviada pela Internet." **[CASTRO,2003]**

Diante disto é essencial que se realize uma separação da fiscalização do correio eletrônico em duas possibilidades, a fiscalização do correio eletrônico profissional e a fiscalização do correio eletrônico pessoal acessado no ambiente de trabalho.

11.2. Fiscalização do Correio Eletrônico Pessoal em Ambiente de Trabalho

O correio eletrônico pessoal pertence exclusivamente ao empregado. É por meio deste correio que o indivíduo se comunica para tratar de assuntos, na maioria das vezes, pessoais.

Alguns doutrinadores entendem que, quando esse e-mail particular é acessado em um ambiente corporativo o mesmo torna-se passível de fiscalização da empresa. O advogado e professor da Universidade Estadual Paulista Júlio de Mesquita Filho, UNESP, Mauro César Martins de Souza justifica a fiscalização afirmando que:

> *"O correio eletrônico é uma ferramenta de trabalho dada pelo empregador ao empregado para realização do trabalho, portanto sobre ele incide o poder de direção do empregador e conseqüentemente o direito do mesmo fiscalizar seu uso pelo funcionário. Os endereços eletrônicos gratuitos e ou particulares, desde que acessados no local de trabalho, enquadram-se, em tese, no mesmo caso."*

Diversas opiniões de profissionais a respeito tendem a acreditar que o *e-mail* particular acessado, utilizando os recursos físicos e equipamentos da empresa, torna-se passivel de fiscalização, já que durante o horário de trabalho o empregado deve ter sua atenção voltada exclusivamente aos afazeres do ofício para o qual foi contratado a executar. Portanto, a consulta particular de e-mail, bem como a navegação de páginas que não tenham relação com seu trabalho configura o não cumprimento de suas obrigações, motivo para rescisão do contrato de trabalho por justa causa. Contrário a essa idéia, *Mário Antônio Lobato de Paiva* acredita que, no que diz respeito a um e-mail particular do trabalhador, *"é evidente que qualquer intromissão do mesmo poderá ser considerada uma violação a direitos constitucionais de cidadão"*. Porém o mesmo doutrinador ressalta que a impossibilidade jurídica não impede que a empresa proíba ou restrinja a utilização do correio pessoal durante sua jornada de trabalho.

Segundo o colunista da "Revista do Direito Privado", Marcus Paredes: na edição de número 9, no artigo "Violação da privacidade na Internet", entende que no que concerne o e-

mail pessoal, a investigação de dados é ato criminoso tipificado no artigo 1º da Lei 9.296/96, mesmo quando realizada nas comunicações internas da empresa (por meio de Intranet), e, portanto, *"não há justificativa juridicamente aceitável que autorize a violação de e-mails particulares do empregado, pois vulnera a intimidade e a privacidade como direitos da personalidade, além de incidir numa conduta criminosa"*. Tendo em vista o caráter *particular* do correio eletrônico pessoal e o fato de que este é, exclusivamente de propriedade do próprio trabalhador, e esse recurso não foi cedido pela empresa, a violação do correio pessoal, configura invasão de privacidade, onde quer que seja acessado, sendo que os danos sofridos por tal ato passíveis de reparações judiciais.

Vale lembrar que o uso do correio eletrônico particular em ambiente corporativo deve ser admitido pelo empregador/empresa, de forma não abusiva e justificada através dos recursos de comunicações disponíveis na empresa contratante, já que não há possibilidade de impor o desligamento completo e total do empregado em seu ambiente de trabalho. Entretanto, cabe ressaltar que há a possibilidade legítima da empresa de proibir o acesso ao correio eletrônico pessoal por meio das suas ferramentas de trabalho fornecidas.

Nesse contexto, Marco Antônio Lobato de Paiva, orienta que:

> *"é aconselhável ao empregador utilizar-se da possibilidade de impedir o acesso a sites impróprios, bem como a transmissão de imagens por e-mail, ou então criar normas internas proibindo ao empregado a utilização da internet para fins não condizentes com assuntos relacionados à empresa, ou inseri-las até mesmo nos contratos de trabalho, a fim de justificar eventual rescisão da relação empregatícia e evitar possíveis demandas judiciais de parte a parte"*. **[Paiva,2002]**

11.3. Fiscalização do Correio Eletrônico Corporativo

Dentre as justificativas que as empresas utilizam para a fiscalização do correio eletrônico profissional estão: preservação da imagem da empresa e a garantia do melhor desempenho de seus funcionários no horário de trabalho, através da disponibilização do e-mail como ferramenta exclusiva de trabalho, essa fiscalização do correio eletrônico profissional tem que obedecer a certos requisitos.

Essa observação deve ser possível em caráter cautelador e não como espião da privacidade do empregado, esse controle deve acontecer sob ciência do funcionário ou ordem

judicial específica para afastar a possibilidade de rescisão indireta do contrato de trabalho e indenizações.

Segundo Mário Antônio Lobato de Paiva, a fiscalização do correio eletrônico profissional é uma garantida à empresa,

> "*desde que comprove realmente que a fiscalização do correio eletrônico serviu para o fim a que se destina sem maiores intervenções que pudessem revestir-se de ilegalidade e lesão a direitos*" **[Paiva,2002]**,

Diante do exposto, a verificação do e-mail (profissional) sem maiores justificativas pode ser considerada lesiva aos direitos do trabalhador. A empresa deve deixar claro contratualmente tais condições no ato da contratação do funcionário ou estabelecer políticas internas de fácil acesso embora todas essas precauções não sejam garantias absolutas diante das inúmeras possibilidades de cada caso.

Dentre a quantidade de opiniões, o Juiz do Trabalho Luiz Alberto de Vargas, considera lícita a fiscalização do correio eletrônico profissional, desde que: dentro da empresa se estabeleça uma política de acesso transparente, que conscientize o empregado que seus e-mails poderão ser monitorados, que a empresa advirta os empregados de que todas as mensagens, de qualquer tipo, inclusive as protegidas por senhas, estão potencialmente disponíveis para o conhecimento da empresa; e que não se pratique o monitoramento sem clara finalidade específica.

12. SOFTWARES

Para a realização da Proposta, foram utilizados softwares exclusivamente livres, pois um dos propósitos desse trabalho é demonstrar o poder e robustez desse tipo de ferramenta e que para se ter um serviço de correio eletrônico rápido e eficiente, não é preciso grandes investimentos, abaixo serão descritos os softwares utilizados nessa pesquisa.

12.1. Sistema Operacional (Debian Linux 4.0)

O projeto Debian foi criado em agosto de 1993, com filosofia de uma distribuição aberta e é a única distribuição que permite ao desenvolvedor trabalhar e contribuir em qualquer parte do seu código, é o único que não age como uma entidade comercial, possui uma constituição, um contrato social e documentos com políticas para organizar o projeto. A Debian também é a única distribuição que é micro-empacotada, usando informações detalhadas de dependência de pacotes para garantir a consistência do sistema em atualizações.

O Debian adota um rico conjunto de políticas e procedimentos para empacotamento e distribuição de software, mantendo assim um alto padrão de qualidade. Backups são automatizados através de ferramentas e a documentação detalha todos os elementos chaves do Debian de uma forma aberta e visível.

12.2. Servidor de Páginas Apache

O Apache surgiu no NCSA (*National Center of Supercomputing Applications*,) é o mais conhecido e usado servidor de páginas na atualidade. Os motivos incluem sua excelente performance, segurança, compatibilidade com diversas plataformas , além de ser uma ferramenta gratuita. É compatível com o protocolo HTTP versão 1.1. Suas funcionalidades são mantidas através de uma estrutura de módulos, podendo inclusive o usuário escrever seus próprios módulos, utilizando a API do software.

Quando um site é acessado, há um servidor por trás daquele endereço, que disponibiliza todos os recursos e as páginas disponíveis para acesso. Assim, quando um usuário envia um e-mail através de um formulário, faz uma compra on-line, por exemplo, um servidor de páginas é responsável por processar essas informações.

Resumidamente, um servidor de páginas é um computador que processa solicitações HTTP, que é o protocolo padrão da Web. Quando se usa um navegador de Internet (Mozilla ou Internet Explorer, por exemplo), para acessar um site, este faz as solicitações ao servidor de página através de HTTP ou HTTPS para receber o conteúdo correspondente.

O servidor web Apache passou a liderar, pela primeira vez, o ranking de servidores web SSL. Segundo a NetCraft (http://www.netcraft.com), empresa inglesa de serviços de Internet que fornece serviços de segurança e que realiza pesquisa e análises de muitos aspectos do mundo on-line (entre suas áreas de especialização estão análise de servidores web), o software agora possui 44% dos servidores web seguros da Internet, contra 43.8% do Microsoft IIS, a Figura 11 mostra o gráfico com os dados retirados da NetCraft.

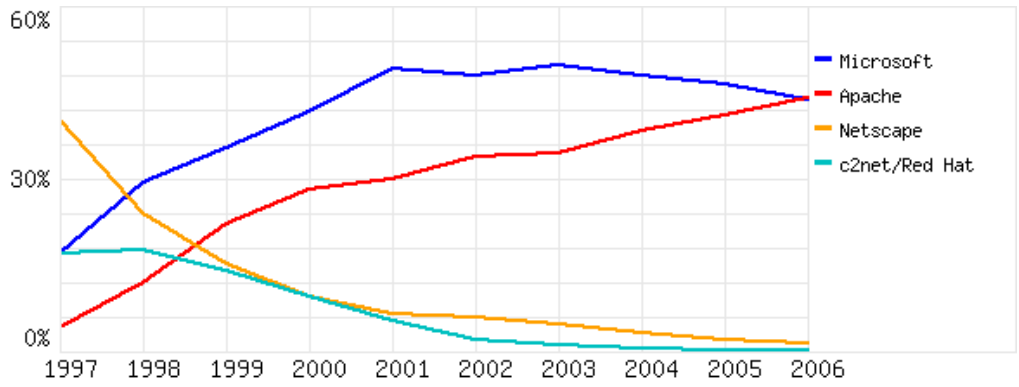

Figura 11 - Ranking dos servidores de páginas.

http://news.netcraft.com/archives/2006/04/26/apache_now_the_leader_in_ssl_servers.html

12.3. Postfix Versão 2.1.5-9

O termo Postfix é um agente de transporte de e-mails, que faz o transporte das mensagens de um MUA para um servidor com SMTP. Postfix é o MTA padrão do *Conectiva Linux* e será visto a seguir como implementá-lo e configurá-lo.

O Postfix é um dos melhores MTA's, que envolve desempenho, robustez, e segurança, por isso o estudo em implementar essa solução. Além do mais, o Postfix é capaz de emular várias funções de outro MTA, que é o Sendmail.

Outro fato do Postfix ser um MTA bastante robusto, é a construção modular, que facilita a manutenção do código na qual permite a implementação de novas funcionalidades e melhorias para o MTA.

Para instalar o Postfix no Linux Debian na qual foi abordado essa distribuição do projeto em questão é muito fácil, ele funciona através de uma maneira muito segura, essa segurança é adicionada em seus próprios arquivos de configurações padrão. Essa configuração básica é segura e completa o suficiente a ponto de não ser necessário realizar modificações para tal. Mas o Postfix vai além, mesmo que um software tenha segurança e configurações suficientes ele nunca será perfeito para todos os usuários, se o mesmo necessitar modificar seu Postfix, sua estrutura de sintaxe s bem como suas opções são facilmente alteradas e depois executadas de uma forma pouco traumática, e mais, a palicação do PostFix foi desenvolvida de forma modular, o qual cada modulo é executado com o mínimo nível de privilégios necessários. Quando resolveram desenvolver o PostFix foi pensando em segurança que o fizeram.

O desempenho do Postfix é impressionante já que suas tarefas são focadas nos núcleos do transporte de e-mail, ele não tenta reinventar a roda com funcionalidades que outras aplicações já fazem o Postfix lhe dá os meios para se conectar em aplicações externas em uma tarefa depende de transporte de mensagens externamente.

Postfix usa todo o seu poder no Unix para fazer seu trabalho, sua grande interação com o sistema operacional permite que não apenas seja mais fácil o acesso a aplicações externas, mas também ele provê um grande desempenho.

12.4. SpamAssassin

Spamassassin é um analisador de mail, com uma quantidade enorme de critérios desenvolvidos para classificar mensagens como spam (ou não-spam). Configurando sua conta de mail para seu uso, é possível desviar da caixa postal muito do lixo indesejado.

O Spamassassin é um programa Perl distribuído sob a mesma licença dual GPL (Licença Pública Geral do GNU). Isto permite distribuir o SpamAssassin através do CPAN (Comprehensive Perl Archive Network - Rede de Arquivamento Abrangente do Perl). E também reusar código da CPAN sem nenhum problema legal.

O funcionamento do SpamAssassin é muito simples, seu algorítimo opera aplicando inúmeros testes diferentes aos e-mails que ele analisa. Existem testes para e-mails em HTML, verifica se a mensagem de e-mail contém frases usadas com freqüência em Spam, se a mensagem afirma não ser Spam de acordo com certas leis e normas, se ele contém uma quantidade pouco usual de pontos de exclamação e de interrogação.

À medida em que a aplicação vai fazendo testes, vai pontuando a mensagem que está sendo verificada. O usuário pode especificar a quantidade de pontos que cada teste vale, através de um arquivo de configuração em ASCII. A identificação do SPAM é feita somando-se os pontos da mensagem, se a soma dos pontos ultrapassa um certo valor, o SpamAssassin considera que a mensagem se trata de um e-mail SPAM, vale lembrar que o usuário também pode definir essa pontuação, afinal se trata de software livre.

Baseado neste contexto, o SpamAssassin insere marcadores no cabeçalho que informam o resultado dos testes. Se o usuário quiser, os e-mails de Spam passam a ter o valor "e;text/plain", ou "texto simples", no campo Content-Type, ou "tipo de conteúdo", o que torna muito mais fácil verificar o resultado dos testes. O SpamAssassin pode também inserir um relatório de teste mais detalhado no começo do e-mail, para que um usuário possa claramente ver porque um e-mail foi considerado Spam.

O maior risco de se usar SpamAssassin é claramente a possibilidade de "falso positivos": mensagens normais de e-mail classificadas como Spam. Portanto, o usuário deve se policiar e examinar regularmente a pasta em que as mensagens consideradas Spam são armazenadas a fim de evitar perda de alguma mensagem interessante ao usuário, e com isso corrigir resultados falso-positivos.

Outra característica da aplicação é a possibilidade de se baixar o nível de sensibilidade, o que vai aumentar a quantidade de Spam não detectado. Para o administrador

do SpamAssassin, a tarefa mais difícil é encontrar o ponto de equilíbrio necessário na sensibilidade das regras.

suporte a listas negras on-line é uma funcionalidade importante, a referência a listas negras de DNS, fontes e "relays" conhecidos de Spam são também suportados.

Pode-se destacar como um ponto fraco dessa aplicação o fato dele ter sido desenvolvido para usuários experientes e ainda não possui uma interface gráfica para o usuário.

12.4.1. Courier-Pop

O Courier provê o serviço de pop de maneira rápida e estável, é instalado no Sistema Operacional como um simples e consistente framework, seu código fonte pode ser compilado para a maioria dos sistemas operacionais baseados em LINUX, e para maioria de derivações de Kernel para BSD. Também pode ser compilado para SOLARIS e AIX, como uma pequena ajuda de ferramentas adicionais da SUN ou IBM para o respectivo Sistema Operacional.

O Courier Pop pode prover os serviços de e-mail para o sistema de contas padrão, também provê serviços de e-mail para contas virtuais, acessadas por banco de dados de autenticação via LDAP e MYSQL, acessa base de e-mails tanto no padrão mailbox quanto maildir.

12.5. Courier-Imap

O courier-imap é rápido, escalavél e para uso em servidores críticos de grandes empresas usando Maildir. Muitos provedores de serviços de E-mail usam o courier-imap para gerenciar milhares de contas de E-mail de forma simples, com o recurso de imap e pop3 Proxy, o courier-imap tem praticamente uma infinita escalabilidade horizontal, ou seja, é possível adicionar uma quantidade de servidores paralelos para somar base de dados de usuários.

Na configuração de Proxy, um grupo de servidores courier, faz conexões Pop e Imap para seus clientes e quando recebe os pedidos desses clientes os encaminha para o servidor que guarda aquele Mailbox de usuário, estabelecendo uma conexão Proxy ao servidor de maneira simples e transparente. Da mesma forma, as contas de e-mail podem ser movidas

entre diferentes Servidores para melhor dimensionar o uso de recursos. A única limitação prática do courier-imap é na viabilidade da rede e na quantidade de banda.

12.6. MailMan (listas)

O Mailman é um gerenciador de listas de discussão ou distribuição de e-mail. É desenvolvido na sua maior parte em Python (é uma linguagem de programação interpretada, interativa, dinamicamente tipada, orientada a objetos) com um pouco de código C para segurança. O mailman é integra com a interface Web, tornando fácil o gerenciamento de usuários, moderadores de lista e gerenciadores. Ele suporta arquivamento de mensagens, processamento automático da fila, filtro de conteúdo, filtro de Spam e muitas outras funcionalidades.

Vantagens do Mailman

- Criação de listas via WEB;
- Suporte a nomes reais dos membros;
- Acesso dos usuários através de senhas individuais;
- Suporte a moderação de mensagens;
- Filtro baseado em expressões regulares;
- Melhor gerência de membros, inclusive com buscas;
- Reorganização das páginas administrativas;
- Suporte a grupos moderados;
- Nova arquitetura para entrega de mensagens, removendo a dependência de agendamentos melhorando o tempo de resposta e a escalabilidade;
- Novos controles de privacidade e moderação;
- Convites;
- Auto-Respostas;
- Usuários podem mudar algumas opções globais de entrega para todas as listas de seu site incluindo, senhas, statos de envio, nomes reais entre outros;
- Possui administração baseado em WEB, inscrição e desinscrição também via WEB;
- Uma página customizada para cada lista criada;
- Opções privadas por listas ex: membros, arquivar mensagens;
-Suporte a domínios virtuais;

- Entrega de e-mails em alta performance com arquitetura completamente escalável;

Seu site é www.list.org. Entre alguns dos seus muitos usuários estão Apple Computer, Dell Computers, The XFree86 Project, SourceForge.net, Massachusetts Institute of Technology, RedHat, Samba, KDE Project, Python.Org, Zope.org e GNOME.Org - uma lista mais completa se encontra em http://www.list.org/inthenews.html.

12.7. SquirrelMail

SquirrelMail é uma ferramenta de webmail, ou seja, uma interface da *world wide web*, que permite ao usuário ler e escrever e-mails pelo navegador, não sendo necessário ao usuário ter algum programa de leitura e envio de mensagens, logo, não é preciso ter um MUA.

O programa de webmail utilizado para o projeto foi o SquirrelMail, que é um WebMail Escrito em PHP, o que torna suas páginas completamente personalizáveis, ele possui suporte aos protocolos IMAP e SMTP, todas as páginas são mostradas em HTML puro para uma maior compatibilidade entre os browsers e requer poucos recursos

Squirrelmail possui as funcionalidades mais importantes de um cliente de e-mail, incluindo um suporte forte a criptografia, catálogo de endereços e gerência de pastas.

A origem do projeto surgiu da necessidade das empresas em acessar o e-mail e o catálogo de endereços de modo remoto, uma interface web é ideal para este tipo de solução, pois qualquer um com acesso a Internet conseguirá usufruir de suas mensagens de qualquer lugar.

O squirrelmail é estável suficiente para ser usado em qualquer empresa, na verdade ele é usado em vários sistemas em todo mundo facilitando milhares de usuários por sistema.

A interface utilizada no projeto é um pouco diferenciada da original, ela é um plugin que ambientaliza o webmail com a aparência do Microsoft Outlook, essa versão pode ser obtida através do seguinte endereço: http://sourceforge.net/projects/squirreloutlook. A intenção é deixar a interface com o mesmo design das Figura 12.e Figura 13.

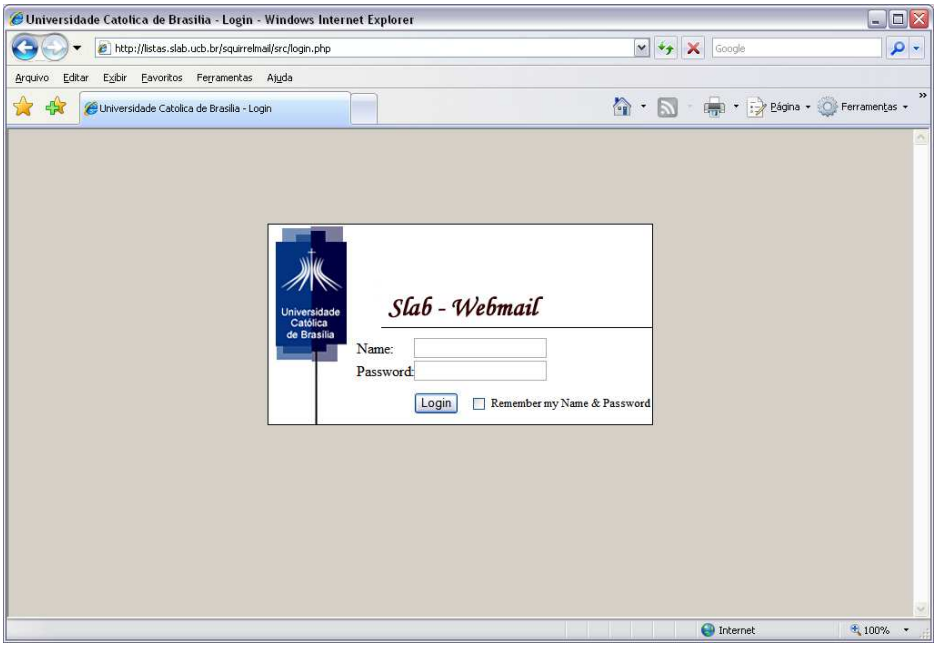

Figura 12 - Tela de login do webmail

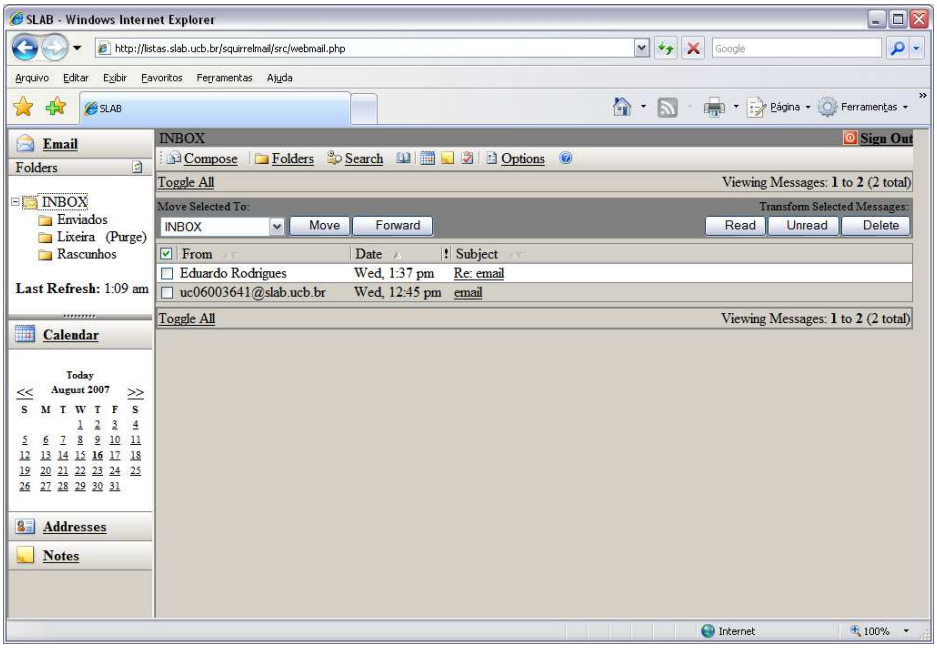

Figura 13 - Tela da interface de webmail para o usuário

13. POLÍTICA DO USO DO E-MAIL

Hoje, a maioria das empresas não possui uma política interna que delimite para quais finalidades seus usuários devem utilizar o recurso de e-mail e com isso o usuário possa utilizar o e-mail corporativo corretamente, não enviando arquivos de vídeos, imagens, dentre outros, na qual não são para uso da instituição. Por isso na solução que foi montada, não foi escrito uma política de uso do e-mail na corporação e sim abordado que, para implementar a solução, é necessário fazer uma política, ficando assim, a critério de quem adquirir.

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento das contas de e-mail, isso para a organização que deseja implementar essa política. Lembrando que para uma solução corporativa é necessário respeitar as normas da ISO/IEC 17799.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio público que foge do controle da equipe técnica da área de TI da equipe que implanta a solução de e-mail. As mensagens podem estar sujeitas a demora e serviços realmente não confiáveis.

Grande parte da comunicação do dia-a-dia passa através de e-mails. Mas é importante também lembrar que grande parte das pragas (spam) eletrônicas atuais chega por esse meio. Os vírus atuais são mandados automaticamente, isso significa que um e-mail de um cliente, parceiro ou amigo não foi mandado necessariamente pelo mesmo.

13.1. Algumas Regras Gerais

a) O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, freqüência ou tamanho das mensagens;

b) O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los, se for solicitada a interrupção do envio a solicitação deve ser acatada e o envio não devera acontecer;

c) É proibido o envio de grande quantidade de mensagens de e-mail (*spam)* que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;

d) É proibido reenviar ou de qualquer forma propagar mensagens em cadeia independentemente da vontade do destinatário de receber tais mensagens;

e) Evite mandar e-mail para mais de 10 (dez) pessoas de uma única vez, é proibido o envio de e-mail mal- intencionado, tais como *mail bombing5* ou sobrecarregar um usuário, site ou servidor com e- mail muito extenso ou numerosas partes de e- mail;

f) Caso a corporação contratante julgue necessário haverá bloqueios:

1. De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

2. De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

g) É proibido o forjar qualquer das informações do cabeçalho do remetente;

h) Não é permitido má utilização da linguagem em respostas aos e-mails comerciais, como abreviações de palavras, uso de gírias;

i) É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;

j) A cota máxima de e-mails armazenados no servidor não deve ultrapassar os 200 Megabytes;

l) Pode-se utilizar o webmail ou programa, Outlook Express, Microsoft Outlook 2003 ou outro software homologado pelo departamento técnico, para ser o cliente de e-mail, utilizando a configuração dos protocolos citados neste trabalho, ex: POP, IMAP;

m) Para certificar-se que a mensagem foi recebida pelo destinatário, deve-se, se necessário, utilizar procedimentos de controles extras para verificar a chegada da mensagem, devem ser solicitadas notificações de “recebimento” e “leitura”;

n) Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos, e alguns casos até mesmo de pessoas da lista todos;

o) Não abra arquivos anexados com as extensões **.bat**, **.exe**, **.src**, **.lnk** e **.com** se não tiver certeza absoluta que solicitou este e-mail;

p) Desconfie de todos e-mails com assuntos estranhos ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: Virus.Win32.Grum.A (*chega com o título "Internet Explorer 7 Downloads" e com o remetente "admin@microsoft.com" e oferece um download disfarçado de Internet Explorer Beta2 (IE7.exe) que na verdade é um vírus*),

um outro chega como convite para ver um cartão virtual e instala um *trojan*: Cartão virtual de Segredinho, entre outros;

q) Evite anexos muito grandes;

13.2. Regras para Funcionários da Corporação

a) Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito a corporação contratante, não podendo tornar-se público;

b) Não utilize o e-mail da corporação para fins pessoais;

c) É obrigatória a utilização de assinatura nos e-mails, seguindo padrão a ser estabelecido pela corporação contratante, de acordo com cada setor da instituição.

14. TESTES DE DESEMPENHO

Foram realizados testes de desempenho utilizando uma ferramenta de benchmark gratuita específica para testes de desempenho em servidores de e-mails chamada Postal. Com ela pode-se manipular uma série de variáveis (memória, número de usuários, quantidade de mensagens enviadas por minuto, dentre outros) e com isso é possível verificar como o servidor se comporta, para isto, essa ferramenta permite uma simulação prática de envio de e-mails, após definirmos o tamanho das mensagens, quantidade de conexões por minuto e os usuários que receberão os e-mails, esse software dispara mensagens continuamente gerando relatório de erros e informações, como número de conexões, quantidade de erros e o tamanho dos pacotes enviados.

14.1. Metodologia

Atualmente, existem vários softwares de *benchmarks* que avaliam o desempenho de servidores de e-mail. Porém, não foi verificado nenhum conjunto de regras ou mesmo uma única metodologia a ser seguida para se avaliar e testar corretamente o desempenho destes. Com base nessa premissa, procurou-se propor uma metodologia de testes que produziram resultados suficientes para ser possível executar uma analise conclusiva sobre a performance do servidor de e-mail aumentando sua carga de usuários e sua memória disponível, analisando

a porcentagem de uso de processador e memória RAM e a quantidade de mensagens enviadas bem como a quantidade em megabytes processada pelo servidor.

14.2. Comparativo de desempenho

Para definir o nível de hardware necessário para obter um desempenho satisfatório, foi analisada a situação dos e-mails utilizados na Universidade Católica de Brasília. Existem cerca de 2.262 contas de e-mail criadas e ativas, algumas dessas contas possuem mais de um endereço SMTP, como por exemplo usuario@ucb.br , usuario@pos.ucb.br , usuario@catolica.edu.br e usuario@ubec.edu.br. Logo existem aproximadamente 4.000 e-mails.

Essas informações servem de embasamento inicial para definir e avaliar o desempenho do Postifix instalado.

Em uma pesquisa realizada foi observado que a Universidade Católica de Brasília possui cerca de 2.000 alunos cursando a Pós-gradaduação dentre eles especialistas, mestrandos e doutorandos A solução levantada no projeto deverá atender a essa quantidade de contas de forma eficaz e com desempenho necessário, esse desempenho será embasado nas contas de E-mail administrativas da Católica, no item 14.2.1 demonstraremos a contextualização real do servidor Exchange da UCB;

14.2.1. Ambiente Exchange Windows

Para executar um teste conclusivo, é necessário compreender o fluxo de mensagens do servidor atual da Universidade Católica de Brasília e assim saber quais as necessidades o novo servidor deverá atender, para isso serão levantados alguns requistos funcionais do servidor de e-mail, que são:

- Quantas mensagens cada usuário possui;
- Quantos megas cada usuário ocupa no servidor;
- Quanto de disco é necessário no servidor para suportar essa quantidade de usuários;
- Quantas conexões são feitas por minuto num servidor com esse número de usuários.

Com os seguintes itens levantados, será possível descrever a configuração de hardware necessária para atender o projeto.

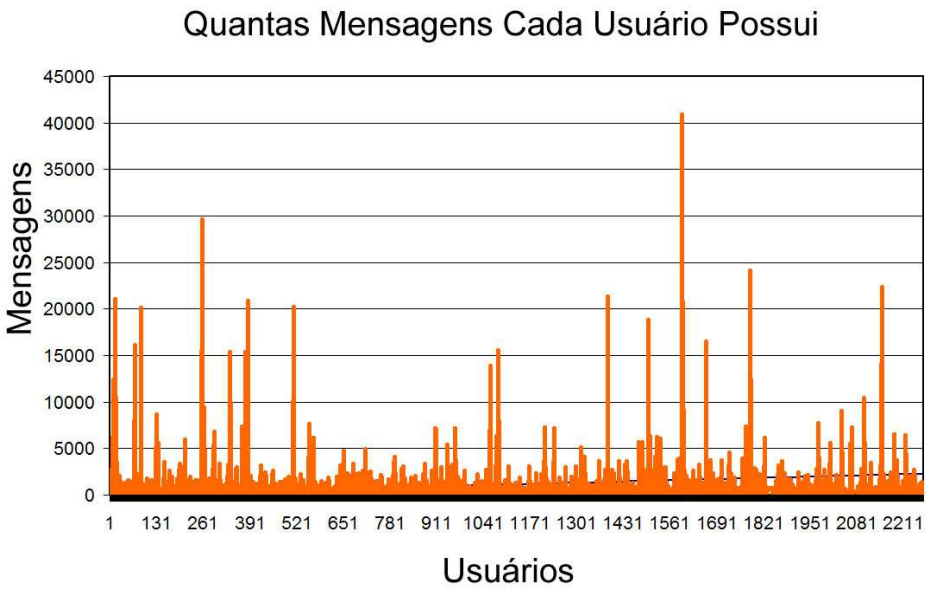

Figura 14 - Quantidade de Mensagens por Usuário na UCB

No servidor da Universidade Católica de Brasília, nem todos os usuários possuem restrinção de cotas, sendo assim os últimos usuários da Figura 15 (a partir do usuário 2161) não são aplicados à analise.

Figura 15 - Tamanho da caixa de e-mail de cada usuário

A cota estipulada na UCB é de 200 megas, já no novo servidor será de 100 megas. Analisando a Figura 15 entende-se que metade dos usuários, se possuísem uma cota de 100 megas, não consegiriam ter a quantidade e-mails que ocupam hoje, e o uso de disco do servidor consequentemente seria menor.

Percebe-se então, na Figura 16, que se não existissem as exessões na UCB a partir do usuário 2161, um disco de 150 Gigabytes atenderia, considerando o fato da cota ser estipulada em 100 megas e a análise do parágrafo anterior, cerca de 30% de disco poderia ser economizado, logo um disco de 120 Gigabyte seria suficiente.

Um fato relevante é que, apesar da cota de 200 megas na UCB, todos os usuários ocupam um total de 225 Gigabytes no servidor de e-mail, já que poucos usam o espaço em disco do servidor para guardar as mensagens.

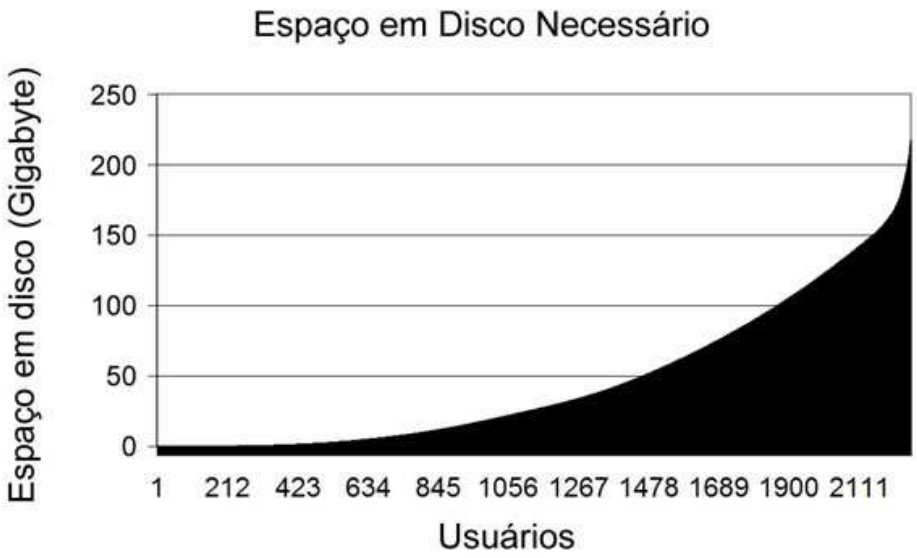

Figura 16 - Espaço em disco utilizado para E-Mail na UCB

Os dados da Figura 14; Figura 15 e Figura 16 foram retiradas da ferramenta *"Exchange System Manager"* como mostra a Figura 17.

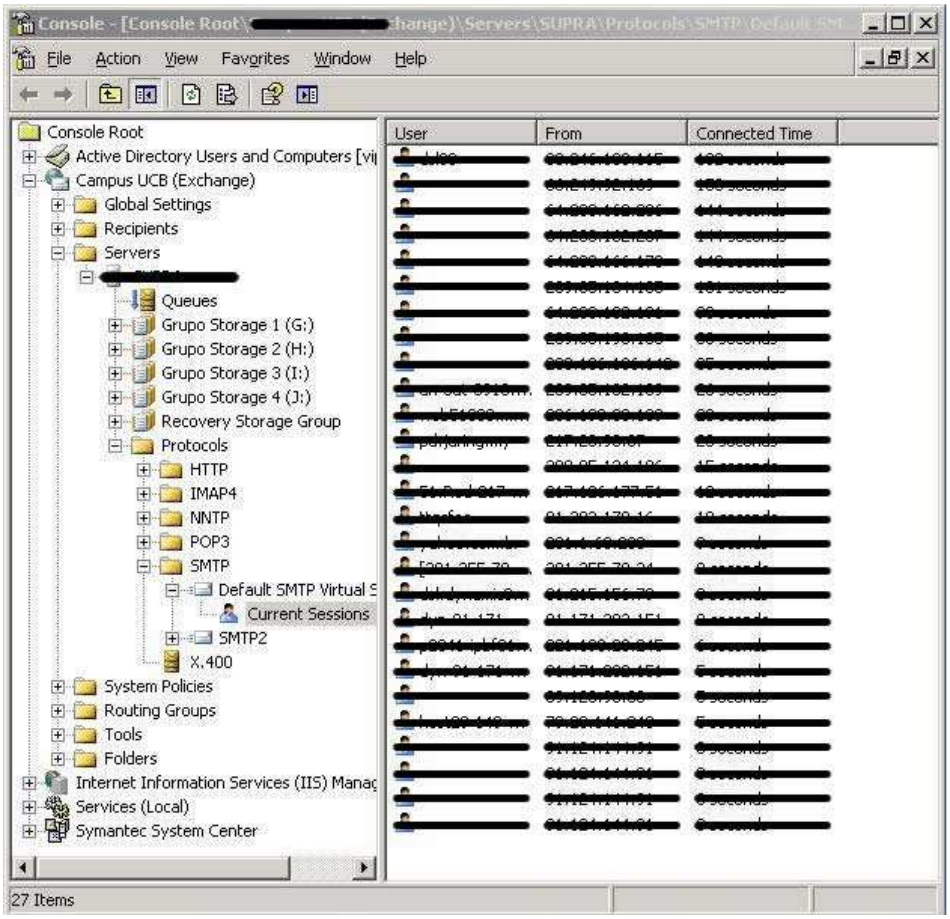

Figura 17 - Console de Gerência do Servidor de e-mail da UCB

Com essa ferramenta, também foi possível extrair o número de conexões SMTP durante um intervalo de tempo, será importante para cruzar a relação: quantidade de usuários/quantidade de mensagens enviadas e recebidas por minuto, criar uma projeção de quantas conexões existirão no servidor para um numero “x” de alunos, com essa perspectiva serão feitos testes no postfix até que encontre um valor de hardware que atenda as necessidades estabelecidas. A Figura 18 demostra o número de mensagens e de dados no servidor da UCB.

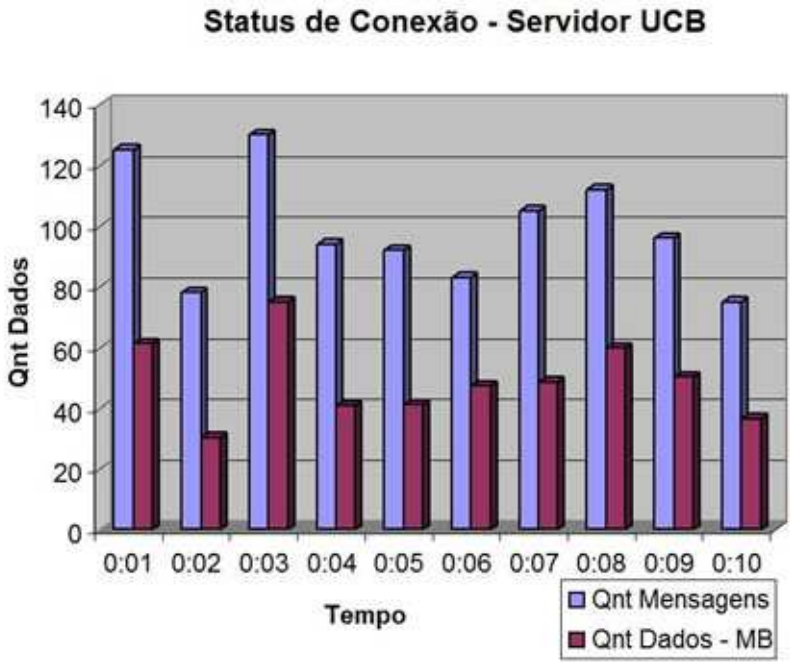

Figura 18 - Numero de Conexões no Servidor da UCB

14.2.2. Ambiente de Testes de Desempenho

- Cenário: Servidor com 256 MB de RAM enviando 50 mensagens por conexão com mensagens variando de 1K a 1024K e disparos de mensagens para **100 usuários** simultaneamente.

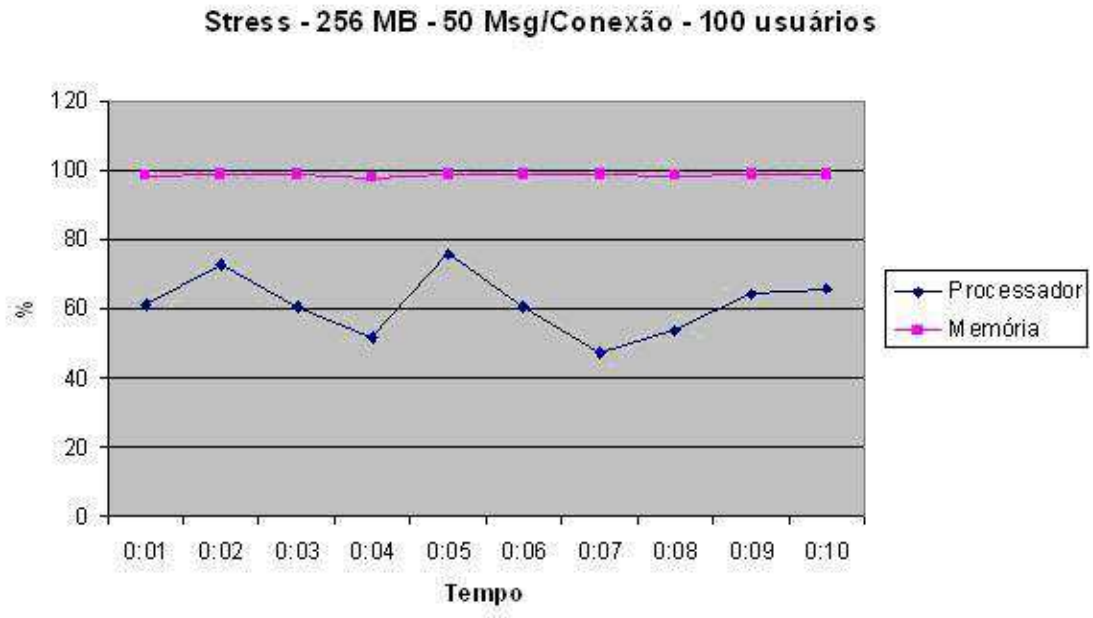

Figura 19 - Desempenho do MTA com 256 de memória RAM

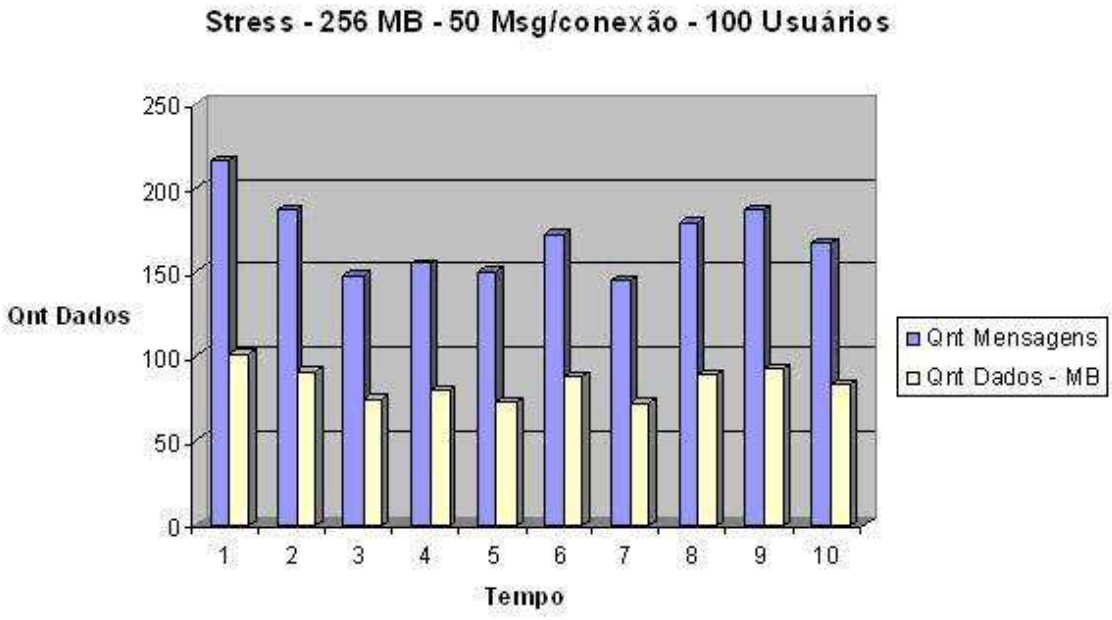

Figura 20 - Numero e tamanho de mensagens enviadas com 256 megas de RAM

Neste teste de desempenho, foi observado que a quantidade de mensagens que o MTA Postfix suportou, com apenas 256 de memória RAM, está de acordo com o necessário para suportar a quantidade de usuários proposto, como observado na Figura 14.

14.3. Conclusão do Teste

Pôde-se perceber que o Postfix é uma ferramenta robusta, basta observar nos gráficos que, mesmo com pouca memória, o número de mensagens enviadas simultaneamente foi satisfatório e a quantidade de erros foi zero. Só foram percebidos erros quando foi aumentado o número de mensagens para 1000 por minuto com 100 usuários simultâneos, levando em consideração que esses números são muito elevados para um servidor de correio eletrônico, usando como referência o próprio servidor de e-mail da UCB. Para se obter um serviço de qualidade com Postfix para um número elevado de usuários (maior que 1000) será necessário:

- Um servidor pentium 4 2.8 Ghz com tecnologia Hyperthread ou superior (pois este foi o modelo usado no projeto);
- 1GB de memória RAM ou mais;
- Dois discos SATA de 300 Gigabytes em RAID 1.

Com isso, acredita-se que o serviço estará completamente estável e suportando uma previsão de expansão na quantidade de usuários.

15. TRABALHOS FUTUROS

Recomenda-implementar e integração de Anti-Vírus e a emissão de certificado digital no servidor de e-mail, pois o objetivo desse certificado é atribuir maior segurança nas transações de mensagens eletrônicas, permitindo a identificação das partes envolvidas, bem como sua integridade e a confidencialidade dos documentos e dados das mensagens.

Foi detectado a necessidade de se criar uma interface gráfica para administração do administrador e do usuário.

Foi também diagnosticado a falta de uma interface gráfica para analisar e gerenciar o SpamAssassin que pode ser feita no futuro.

Por fim, deveria se criar uma pólitica de uso do serviço de e-mail para a Universidade Católica de Brasília.

16. CONCLUSÃO

O correio eletrônico já se tornou parte integrante de nossas vidas, na maioria das empresas o serviço de e-mail é um ativo indispensável para o funcionamento da Empresa, parar o correio eletrônico é parar a empresa, algo que nos faz refletir “Como conseguimos viver tanto tempo sem ele?”

A proposta era montar um servidor de e-mail robusto, com a utilização software livre, buscando o aumento da segurança e a diminuição nos custos do projeto, pesquisar uma solução adequada para montar um servidor de e-mail corporativo para a Universidade Católica de Brasília era o principal desafio. Após várias pesquisas concluiu-se que o Postfix é um dos melhores MTA’s, principalmente no quesito desempenho, robustez, e segurança, sua construção modular, facilita a manutenção do código na qual permite a implementação de novas funcionalidades e melhorias por isso a decisão de implementar essa solução.

Felizmente houve sucesso e foi possível montar o servidor de e-mail totalmente gratuito em plataforma Linux. Embora a árdua tarefa estivesse concluída, o grupo se deparou com um novo desafio. Simultaneamente ao desenvolvimento e popularização da Internet, ocorreu o crescimento de um fenômeno que, desde seu surgimento, se tornou um dos principais problemas da comunicação eletrônica em geral: o envio em massa de mensagens não-solicitadas. Esse fenômeno ficou conhecido como Spams.

A construção de um servidor de e-mail sem a utilização de uma ferramenta Anti-Spam era completamente inviável, isso ficou nítido já que por dia o servidor de e-mails estava recebendo cerca de 40 mensagens não solicitadas para cada usuário.

Este trabalho atingiu a meta proposta, pois baseado nas referências teóricas ele sugere uma implementação segura de correio eletrônico livre, oferecendo orientações sobre como fazê-lo e como proceder diante de algumas situações e especificando o que deve ser realizado para atingir o sucesso na prática.

Conforme a metodologia definida, a norma proposta foi elaborada, abordando os seguintes assuntos: Estudar a teoria e as diferenças entre os MTA’s, conhecer os protocolos associados ao serviço de e-mail; pesquisar os aspectos jurídicos existentes no uso de e-mail em corporações, testar métodos e implementações de segurança sobre os protocolos; Estudar as ferramentas de webmail para aplicar uma na prática, Implementar o serviço de lista de distribuição.

Vale salientar que o sucesso desta pesquisa se deu graças ao conhecimento adequado de pessoas mais experientes, como o do orientador deste projeto, que foi de fundamental importância para o aproveitamento deste trabalho, com sua vasta experiência na área de tecnologia, soube guiar e direcionar para que fosse possível alcançar o sucesso e, com certeza, permanecerá como experiência valiosa na vida dos integrantes deste projeto, devido a sua dedicação em auxiliar seus alunos a alcançar as metas propostas.

17. BIBLIOGRAFIA

[1] ALBERTO SALLES, Carlos. Rede de Computadores. Protocolos: SSH, TELNET, POP3, IMAP. Disponível em: <http://www.filmsub.com/carlos/docs/redes_protocolos.pdf>.Acesso em: 07 mar. 2007.

[2] ALBUQUERQUE, Fernando. “Mensagens sem Extravio”. Revista Connections. Nº 45, Fevereiro 1995 , PP.38-39.

[3] ALBUQUERQUE, Fernando. Tcp/ip internet: Programação de sistemas distribuídos html, javascript e java. 2001. Rio de Janeiro: Axcel Books, 2001.

[4] AMAVIS. AMaViS - a mail virus scanner. Disponível em: <http://www.amavis.org>. Acesso em: 21 ago. 2007.

[5] AMERICA MEDIA- Guia de Referência – “E-mail – Lidando com correio eletrônico”.

[6] [AMA]American Management Association – Management Training and Professional Development Seminars. Disponível em: <http://www.amanet.org/>. Acesso em 07/12/2007.

[7] ALECRIM, Emerson. Conhecendo o Servidor Apache (HTTP Server Project). São Paulo, 2006. Disponível em: <http://www.infowester.com/servapach.php>. Acesso em: 08 jun. 2007.

[8] APACHE, The Apache Software Foundation, Disponível em: <http://www.apache.org/>. Acesso em: 15 ago. 2007.

[9] PHIPPS, Colin. Apache Now the Leader in SSL Servers. 2006. Disponível em: <http://news.netcraft.com/archives/2006/04/26/apache_now_the_leader_in_ssl_servers.html>. Acesso em: 10 mar. 2007.

[10] CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

[11] BALBONI, Mariana. CERT.br (2007). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança. Cartilha de Seguranca para Internet, versao 3.1 / CERT.br – Sao Paulo: Comite Gestor da Internet no Brasil, 2006.

[12] CLAMAV. ClamAV - Clan Antivirus. Disponível em: <http://www.clamav.net>. Acesso em: 21 ago. 2007.

[13] JOSE CARLOS B;VALENTE,ANDRE DE S M. Internet: Guia do usuário brasileiro. São Paulo: Makron Books, 1996. 183p ISBN 85-346-0538-6

[14] ELIAS, Vinicius Graciano; Servidor de E-mail - Postfix/Amavisd-new/SpamAssassin/ClamAV. Disponível em: <http://www.ginux.ufla.br/documentacao/monografias/mono-ViniciusElias.pdf>. Acesso em: 17 fev. 2007.

[15] Enciclopédia e-mail, Correio eletrônico, 2007. Disponível em: <http://www.arikah.net/enciclopedia-portuguese/E-mail>. Acesso em: 04 maio. 2007.

[16] FILHO, Jaimy Teixeira Filho. “Intranet, Groupware, Internet e os processos de Qualidade”. Informal Informática. 1999.

[17] HILDEBRANDT, Ralf . “The Book Of Postfix: state-of-the-art message transport”. Ralf Hildebrandt and Patric Koetter, San Francisco 2005.

[18] HSBC. Uma curta história dos vírus. Disponível em: <http://www.hsbc.com.br/common/seguranca/artigo-seguranca-historia-virus.shtml>. Acesso em: 10 mar. 2007.

[19] RFC 2060. Internet Message Access Protocol - Version 4rev1, 1996. Disponível em: <http://www.ietf.org/rfc/rfc2060.txt>. Acesso em: 04 maio 2007.

[20] RFC 3501.Internet Message Access Protocol - Version 4rev1, 2003. Disponível em: <http://www.isi.edu/in-notes/rfc3501.txt>. Acesso em: 04 maio 2007.

[21] RFC 2821. Simple Mail Transfer Protocol. Disponível em: <http://www.ietf.org/rfc/rfc2821.txt?number=2821>. Acesso em: 04 maio 2007.

[22] KOJM, Tomasz. Clamav User Manual, 2002-2007. Disponível em: <http://www.clamav.net/doc/latest/html/>. Acesso em: 10 mar. 2007.

[23] LARGURA, Luiz Aristides Rios Largura. Monografia sobre SSL para o Curso de Extensão “Segurança em Redes de Computadores. 2000.

[24] LIMA, Amanda, et. al. Protocolos: MIME, SMTP, POP3, IMAP Redes de computadores, Pernambuco, v.1, n. 12, 2006. Disponível em: <http://www.dei.unicap.br/~almir/rc2/apresentacao/rc/smtp/smtp.doc>.
Acesso em: 07 mar. 2007.

[25] MACHADO, Junior. Webmail Squirrelmail, 2007. Disponível em: <http://www.vivaolinux.com.br/dicas/verDica.php?codigo=8700>.
Acesso em: 16 ago. 2007.

[26] MÁXIMO, Marco A. S. Montando um servidor de e-mail completo com Postfix. LOCAL, v.1 n. 12, 2003. Disponível em:
http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=526
Acess em: 07 mar. 2007.

[27] MELO, Bruno Herrlein Correia de. Aspectos jurídicos da fiscalização do correio eletrônico no ambiente de trabalho, 2005. Disponível em: <http://jus2.uol.com.br/doutrina/> acessado em 06/12/07

[28] MTA’s. Open Source Mail Server Comparison. Disponível em: <http://www.geocities.com/mailsoftware42/>. Acesso em: 17 fev. 2007.

[29] MYSQL. The world's most popular open source database. Disponível em:

<http://www.mysql.com>. Acesso em: 10 mar. 2007.

[30] NARCISO, Marcelo Gonçalves. Instalação de Antivírus na Servidora de Mail: Uma Opção para Impedir Ataques de Vírus Anexados a E-mail. Campinas-SP. Outubro, 2001. Disponível em: <http://www.cnptia.embrapa.br/modules/tinycontent3/content/2001/INSTRTECNICAS4int.pdf>. Acesso em: 20 ago. 2007.

[31] Norma ABNT NBR ISO/IEC 17799. Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação. Segunda Edição, 2005.

[32] PAIVA, Marco Antônio Lobato de. O monitoramento do correio eletrônico no ambiente de trabalho, “Direito e Tecnologias da Informação”, 2002.

[33] PEREIRA, Carla Rosely, et. al. Protocolo POP3. Redes de computadores, Brasília, v.1, n. 09, 2003. Disponível em: <http://www.iesplan.br/~augustus/S2_03_redes2/trabalho_01/POP3/Protocolo_POP3.pdf>. Acesso em: 07 mar. 2007.

[34] POSTFIX. Postfix Documentation, 2007. Disponível em: <http://www.postfix.org/>. Acesso em 10 mar. 2007.

[35] ROCHA LIMA, William. Qtrap barrando SPAM por palavras. Disponível em: <http://www.dicas-l.com.br/dicas-l/20060719.php>. Acesso em: 04 maio 2007.

[36] SHIRKY, Clay. Internet: Guia de acesso por correio eletrônico / tradução Cláudio Costa. – Rio de Janeiro, 1994.

[37] SILVA, Rita de Cássia Lopes da Silva. Direito Penal e Sistema Informático – Ciência do Direito Penal Contemporânea V. 4, 2003

[38] SPAM. Técnicas de mitigação para administradores de redes, Spam e fraudes por e-mail. 2006. Disponível em: <http://www.cert.br/docs/palestras/certbr-ssi2006-2.pdf>. Acesso em: 23 fev. 2007.

[39] SQL Magazine. The Smart Guide to Building World-class Applications. Disponível em: <http://www.sqlmag.com/>. Acesso em: 10 jun. 2007.

[40] SQUIRRELMAIL. SquirrelMail webmail for nuts, 2007. Disponível em: <http://www.squirrelmail.org>. Acesso em: 16 ago. 2007.

[41] TANENBAUM, Andrew S. Computer networks. 2. ed. New Jersey: Printice Hall, 1989. 658 p.

[42] TERADA, Routo. Segurança de dados: Criptografia em redes de computador. São Paulo: Edgard Blücher, 2000.

[43] THEISEN, Marcone Luis. 2005, Portal LDAP Brasil, disponível em: <http://www.ldap.org.br/>. Acesso em: 06 dez. 2007.

[44] TISSIATO NAKAMURA, Emilio. Segurança de Redes – Em ambientes corporativos. New Jersey: Upper Saddle River, 1999. p. 29

[45] WIKIPEDIA, a enciclopédia livre, 2007. E-Mail. Disponível em: <http://pt.wikipedia.org/wiki/E-mail>. Acesso em: 17 fev. 2007.

[46] [35]WIKIPEDIA, a enciclopédia livre, 2007. SAGE. Disponível em: <http://en.wikipedia.org/wiki/Semi_Automatic_Ground_Environment>. Acesso em: 20 nov. 2007.

[47] WIKIPEDIA, a enciclopédia livre, 2007. Simple Mail Transfer Protocol. Disponível em: <http://pt.wikipedia.org/wiki/E-mail>. Acesso em: 19 fev. 2007.

[48] CAMARGO, Franciso.2004. O spam se tornou um grande vilão para as empresas. Disponivel em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=403&pagenumber=0&idiom=0>. Acesso em 07 dez. 2007.

[49] TEIXEIRA, Renata Cicilini. 2004. Vamos combater o spam? - Parte 2. Disponivel em: <http://www.modulo.com.br:80/pt/page_i.jsp?page=3&catid=2&objid=402&pagenumber=0&idiom=0>. Acesoo em 07 dez. 2007.

[50] FERREIRA, Ana Amélia de Castro. 2003. Correio Eletrônico Corporativo - Aspectos Jurídicos. Disponivel em: <http://www.modulo.com.br:80/pt/page_i.jsp?page=3&catid=2&objid=359&pagenumber=0&idiom=0>. Acesso em 04 jun. 2007

GLOSSÁRIO:

Active Directory: Serviço de diretório do fabricante Microsoft baseado em LDAP, armazena informações sobre objetos de uma rede de computadores e disponibiliza essas informações aos administradores da rede.

Antivírus: Software feitos para detectar e eliminar vírus de computador.

Anti-spam: Programas feitos para detectar e eliminar algum tipo de spam.

ARPANET: Advanced Research Projects Agency Network. Rede de computadores à base de comutação de pacotes criada antes da Internet nos anos de 1969.

Autenticar: processo de validar as credenciais de uma pessoa ou dispositivo. A autenticação requer que a pessoa, processo ou dispositivo faça uma requisição fornecendo uma credencial que prove que ela é quem diz ser.

AUTODIN: Automatic Digital Network. Sistema que tem a função de prover troca de mensagens para o correio militar americano, pode ter sido o primeiro a permitir que mensagens eletrônicas fossem transferidas entre computadores diferentes.

Autoridade certificadora (CA): Emitem certificados para as Autoridades de Certificação Intermediárias ou para o Cliente.

Autorização: Processo de garantir a uma pessoa ou dispositivo acesso a certas informações, serviços ou funcionalidades. A autorização é derivada da identidade da pessoa, processo ou dispositivo ao requerer acesso, o que é verificado através da autenticação.

Backup: Copia de segurança dos dados de um dispositivo para outro, como medida de precaução no caso de haver alguma falha com o dispositivo original.

Benchmarks: Processo de teste e comparação de desempenho serviço.

Blacklist: Lista de remetentes conhecidos classificados como não confiáveis.

Browser: Programa de computador usado para localizar e visualizar documentos via web em HTML, permitindo a navegação no ambiente WWW. Os browsers mais utilizados são a Internet Explorer e o Mozilla Firefox.

Certificado digital: Software que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido, é muito utilizado em sites de bancos. No caso, do e-mail o certificado vai verificar quem é quem, se a mensagem é realmente de quem enviou.

Chain letters: Mensagens que prometem benefícios (sorte, riqueza) para as pessoas que reenviar esta mensagem para um número X de pessoas.

Confiabilidade: Garantia de não existência de acessos não-autorizados as informações.

Controle de Conteúdo: Técnicas de bloqueio de spam que se baseia na análise do conteúdo da mensagem.

Criptografia: É o estudo ou análise de métodos de codificação e decodificação usada para proteger informações. As técnicas de criptografia podem ser usadas para permitir e garantir a confidencialidade, integridade e autenticação dos dados.

DAP: *Directory Access Protocol*. Protocolo de acesso de diretório para atualizar e pesquisar diretórios rodando sobre TCP/IP. Anterior ao protocolo LDAP.

Delay: Tempo de atraso de um sinal em circuitos eletronicos ou em transmissões de arquivos, ou seja, um retardo de sinais.

Disponibilidade: Determina que os recursos estejam disponíveis para acessos autorizados, sempre que solicitados.

DMA: *Direct Marketing Association*. Permite que certos dispositivos de hardware num computador acedam a memória do sistema para leitura e escrita independentemente da CPU.

DNS: *Domain Name System*: Sistema de gerenciamento de nomes. O DNS traduz nomes para os endereços IP e endereços IP para nomes dentro de uma rede.

Download: Transferência de arquivos ou dados de um computador remoto para um micro local.

Estado de transação: Coleta de mensagens de correio eletrônico do usuário e com a marcação das mensagens para exclusão da caixa de correio.

Exim: Agente de transporte de e-mail, desenvolvido na Universidade de Cambridge, possui grande flexibilidade e suporte a spam, antivírus, entre outros.

Falsos negativos: Mensagens maliciosas bloqueadas como mensagens corretas.

Falsos positivos: Mensagens corretas bloqueadas como mensagens maliciosas.

Filtros Bayesianos: Tipo de filtragem que se baseia em estatísticas de identificação e controle de spam, são os mais eficientes da atualidade.

FTP: *File Transfer Protocol*. É um protocolo de transferência de arquivos com acessos remotos.

Gateway: Equipamento interligado a várias redes, permitindo a passagem de pacotes de uma rede para outra.

Hardware: Conjunto de componentes físicos de um computador.

Hoaxex: Histórias falsas com intenção de alarmar ou iludir aos que lêem com o objetivo de divulgar para o maior número de pessoas.

Host: Qualquer computador conectado a uma rede.

HTTP: *Hyper Text Transfer Protocol*. Protocolo padrão de Internet que permite a transferência de dados na Web entre os servidores e clientes.

HTML: *Hyper Text Markup Language*. Linguagem padrão utilizada para construir os documentos web (websites).

IMAP: *Internet Message Access Protocol*. Protocolo de gerenciamento de correio eletrônico com funções mais elaboradas em relação ao POP3.

Integridade: Garantia sobre a autenticidade e da não alteração ou remoção de informações.

Interface: Dispositivo físico ou lógico que estabelece a adaptação entre dois sistemas independentes.

Internet: Rede mundial baseada no protocolo TCP/IP com vários computadores interligados.

Internet: Rede mundial de computadores interconectados.

IP: *Internet Protocol*: Protocolo da Internet. É este protocolo que identifica, localiza e estabelece conexão entre computadores ligados à rede.

ISO/IEC 17799: Norma de Segurança da Informação que contêm um conjunto de recomendações de boas práticas.

Kernel: Núcleo do sistema operacional, responsável por gerenciar os recursos deste sistema.

LDAP: *Lightweight Directory Access Protocol*. Protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP e segue o modelo baseado em árvore de nós, cada um consistindo de um conjunto de atributos com seus respectivos valores.

Listas de discussão: É um programa que reúne vários endereços de correio eletrônico de pessoas interessadas em um assunto específico. Este programa redistribui a todos os e-mails que tenham sido passados por qualquer um dos participantes da lista.

Linux: Sistema com código aberto baseado em Unix.

MAC: *Message Authentication Code*. Garante a integridade das mensagens, utiliza autenticação entre cliente/servidor.

Mailbox: Padrão de armazenamento de mensagens baseado em um arquivo por usuário.

Maildir: Padrão de armazenamento de mensagens baseado em um arquivo por mensagem.

MailMan: Gerenciador de listas de discussão ou distribuição de e-mail.

Máquinas virtuais: Serviço que simula outros computadores, podem ser criados vários computadores virtuais dentro do mesmo serviço/servidor.

MIME: *Multipurpose Internet Mail Extensions.* Extensões Multi função para Mensagens de Internet. Norma da Internet para o formato das mensagens de correio eletrônico.

Modelo OSI: Interoperabilidade entre computadores d diferentes fabricantes. Usado para facilitar a interconexão de sistemas de computadores à arquitetura ISO (International Standards Organization).

Modem: Dispositivo eletrônico que modula um sinal digital em uma onda analógica, utilizando a linha telefônica para que um computador consiga comunicação de dados.

MTA: *Mail Transfer Agent*. Programa responsável por transferências de mensagens entre uns servidores.

MUA: *Mail User Agent*. Aplicação ou programa utilizado pelo usuário para compor, enviar e ler mensagens.

MYSQL: Software livre de gerenciamento de banco de dados baseado na linguagem SQL como interface.

NNTP: *Network News Transfer Protocol.* Protocolo usado por usuários de notícia do usenet e por clientes (leitores) e é definido pela RFC 977.

Pacote: Unidade de dados de protocolo de transmissão em uma rede. Muito conhecido também como datagrama.

Phishing: Mensagens que assumem o disfarce de “spam comercial”, ou simulam mensagens comuns fazendo com que o destinatário acredite e envie dados pessoais.

Plataforma: Padrão de um sistema operacional ou de um computador. Podendo ser plataforma Windows, Linux, dentre outras.

POP: *Post Office Protocol*. Protocolo utilizado no acesso remoto a uma caixa de correio eletrônico.

Postfix: Agente de transporte de e-mails de grande modularidade e uso no mercado.

Privacidade: O controle que os clientes possuem na coleta, uso e distribuição de suas informações pessoais.

Protocolo: Padrão que especifica o formato de dados e regras a serem seguidas, especifica como um programa deve preparar os dados para serem enviados para o estado seguinte do processo de comunicação.

Provedor: Empresa que provê acesso aos serviços de Internet aos seus clientes através da manutenção de uma central de linhas telefônicas exclusivas ligadas aos seus servidores de serviços Internet.

Publicações eletrônicas: Conjunto de informações eletrônicas colocadas (publicadas) na rede.

Qmail: Agente de transporte de e-mail Unix criado para ser mais seguro que o Sendmail.

Relay: Configuração que define quem quais remetentes terão acesso a enviar e-mails sem filtros.

RFC: *Request For Comments*. Série de documentos com os padrões de protocolos de Internet.

Scam: Oferecem ofertas de ganho de dinheiro fácil trabalhando em casa, empréstimos, pedindo uma pequena quantia para começar esse "negócio", muitas vezes tentam simular uma mensagem confidencial.

Sendmail: Agente de transporte de e-mail baseado em BSD.

Servidor: Computador que possui um hardware robusto e redundante, usado para fornecer serviços a uma rede, serviços de e-mail, dns, ldap, dentre outros.

Servidor Apache: Servidor web livre, sendo um dos melhores servidores web disponíveis.

SMTP: *Simple Mail Transfer Protocol*. Protocolo padrão para envio de e-mail entre os MTA's através da Internet.

SMTP DELIVERY: SMTP que recebe e-mail do ambiente de serviço de transporte e o envia para o MUA ou deposita num local onde o MUA acessará depois

SMTP GATEWAY: SMTP que recebe correspondências do cliente de um ambiente e envia para o servidor que está em outro ambiente, fazendo um filtro e barrando o conteúdo que não é bem vindo.

SMTP ORIGINATOR: Cliente que origina mensagem, inicia o tráfego SMTP.

SMTP RELAY: SMTP que recebe e-mails de um cliente SMTP e o transmite sem modificações do conteúdo da mensagem para outro servidor SMTP para futuro relay ou delivery.

Software livre: Software com distribuição gratuita, podendo ser estudado, modificado e melhorado.

Spam: Toda e qualquer mensagem não solicitada.

SpamAssassin: Analisador de e-mail, com filtro para classificar mensagens como spam ou não-spam.

Spammer: Pessoas que utilizam programas que facilitam a obtenção de endereços de pessoas e acaba enviando spam para uma grande quantidade de pessoas.

SQL: *Structured Query Language*. Linguagem de pesquisa declarativa para banco de dados relacional é um padrão de linguagem de banco de dados.

SquirrelMail: Software de webmail escrito em PHP, o que torna suas páginas completamente personalizáveis, ele possui suporte aos protocolos IMAP e SMTP.

SSL: *Secure Sockets Layer*. Protocolo que roda em cima de qualquer protocolo de transporte, usa criptografia simétrica que provê comunicação segura na Internet para serviços como e-mail, navegação por página, proporcionando autenticação e segurança.

TCP/IP: *Transfer Control Protocol/Internet Protocol*. Protocolo de transporte voltado para a conexão, que permite uma transmissão bidirecional completa (full duplex) de dados entre duas entidades, freqüentemente entre um aplicativo cliente e um servidor.

TLS: *Transport Layer Security*. Protocolo de criptografia usado para prover comunicação segura.

Topologia da rede: Modelo/Desenho da rede, podendo ser este relativo a parte física ou lógica.

Trashing: Ato de enviar múltiplas mensagens com o objetivo de deslocar as mensagens de outros usuários para fora da tela, era conhecido flooding (inundação).

Unix: Sistema operacional multi-usuário utilizado em serviços críticos.

Usabilidade: Extensão na qual um produto pode ser usado por usuários específicos para alcançar objetivos específicos com efetividade, eficiência e satisfação em um contexto de uso específico.

Usenet: *Unix User Networt*. É um local onde os usuários postam mensagens de texto chamadas de artigos em fóruns que são agrupados por assunto chamados de grupos de notícias.

Vírus: Código malicioso, escrito com a intenção de se espalhar, degradar e causar danos ao hardware, software ou aos dados.

Vulnerabilidade: Qualquer fraqueza que pode ser explorada, causando perda ou danos.

Webmail: É uma interface que permite acessar e-mails por um site web.

Whitelist: Lista de remetentes conhecidos classificados como confiáveis.

ANEXOS

I. ANEXOS

I.I. Instalação Kerberos

Validação dos acessos com o AD

Comandos:

 # apt-get install krb5-config krb5-user

O arquivo ***/etc/krb5.conf*** deve ser configurado com o conteúdo:

```
[libdefaults]
        default_realm = DOMINIO.COM.BR

[realms]
        DOMINIO.COM.BR = {
                kdc = dc.dominio.com.br
                }

[domain_realm]
        .kerberos.server = DOMINIO.COM.BR

[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log

[appdefaults]
        pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
                }
```

```
```

 # kinit administrator@DOMINIO.COM.BR

Deve retornar:

 # klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@DOMINIO.COM.BR

Valid starting Expires Service principal
03/08/07 10:41:29 03/08/07 20:41:29 krbtgt/DOMINIO.COM.BR@DOMINIO.COM.BR

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached

I.II. Instalação SAMBA

Para se comunicar e autenticar com uma base de usuário Microsoft Windows é preciso ter um servidor *Samba* instalado no equipamento para ingressar o servidor no domínio e, assim, ser possivel autenticar os usuários:

 # apt-get install samba samba-common winbind

Depois se edita o */etc/samba/smb.conf* da seguinte forma

```
[global]
unix charset = ISO-8859-1
workgroup = DOMINIO
netbios name = MAIL
server string = Mail
```

```
        load printers = no
        log file = /var/log/samba/log.%m
        max log size = 500
        realm = dominio.com.br
        security = ads
        auth methods = winbind
        password server = *
        winbind separator = +
        encrypt passwords = Yes
        winbind cache time = 10
        winbind enum users = Yes
        winbind enum groups = Yes
        winbind use default domain = Yes
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        socket options = TCP_NODELAY SO_RCVBUF=8192
SO_SNDBUF=8192
        local master = no
        os level = 233
        domain master = no
        preferred master = no
        domain logons = no
        wins server = 172.16.0.20
        dns proxy = no
        ldap ssl = no
        template shell = /bin/bash
        template homedir = /home/%D/%U
```

Reinicie o samba e winbind com o comando:

 # /etc/init.d/samba restart

 # /etc/init.d/winbind restart

Coloque o servidor no domínio:

 # net ads join -U administrator -S dominio.com.br

E reinicie o samba novamente:

 # /etc/init.d/samba restart

 # /etc/init.d/winbind restart

Faça um teste com wbinfo:

 # wbinfo –u

I.III. NSSWITCH

Edite o arquivo /etc/nsswitch.conf substituindo as linhas:

passwd: compat
group: compat

Por:

passwd: compat winbind
group: compat winbind

O arquivo vai ficar da seguinte forma:

```
passwd:         compat winbind
group:          compat winbind
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Teste a configuração:

 # getent passwd
 # getent group

APACHE

Instale o apache com suporte a ssl:

 # apt-get install apache-ssl apache-common apache2-utils php4

Crie um atalho para */etc/apache-ssl*:

 # ln -s /etc/apache-ssl /etc/apach

Criando certificado
Caso não existam, crie os diretórios:

 # mkdir ssl.crl ssl.crt ssl.csr ssl.key ssl.prm

Configure a permissão:

 # chmod 755 ssl.crl ssl.crt ssl.csr ssl.key ssl.prm

Dentro de /etc/apache, crie os certificados:

 # openssl genrsa -out ssl.key/dominio.com.br.key 102
 # openssl req -new -key ssl.key/dominio.com.br.key -out ssl.csr/dominio.com.br.csr

Preencha os dados –

 # openssl x509 -req -days 365 -in ssl.csr/dominio.com.br.csr -signkey ssl.key/dominio.com.br.key -out ssl.crt/dominio.com.br.crt

Comente a linha no httpd.conf:

SSLCertificateFile /etc/apache-ssl/apache.pem

Ficando:

#SSLCertificateFile /etc/apache-ssl/apache.pem

Insira as linhas:

SSLCertificateFile /etc/apache/ssl.crt/dominio.com.br.cr
SSLCertificateKeyFile /etc/apache/ssl.key/dominio.com.br.key

Reinicie o apache-ssl:

/etc/init.d/apache-ssl restart

I.IV. Instalação do PostFix

Instale o *Postfix* e o suporte a TLS:

 # apt-get install postfix postfix-tls

Edite o */etc/postfix/main.cf*

#Configuração do servidor

smtpd_banner = DOMINIO
biff = no
append_dot_mydomain = no

```
delay_warning_time = 2h
command_time_limit = 1h
myhostname = dominiomail.dominio.com.br
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydomain = dominio.com.br
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain, $mydomain
relay_domains = $mydestination
relayhost =
recipient_delimiter = +
fallback_transport = /usr/bin/maildrop
inet_interfaces = all
debug_peer_level = 9
disable_vrfy_command = yes
message_size_limit = 5120000
home_mailbox = Maildir/
mail_spool_directory = /mail/
mynetworks = 127.0.0.0/8 172.16.0.0/16

# SSL config
smtpd_use_tls = yes
smtpd_tls_auth_only = no
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/dominio.com.br.key
smtpd_tls_cert_file = /etc/postfix/ssl/dominio.com.br.crt
smtpd_tls_CAfile = /etc/postfix/ssl/sap.sp2.gov.br.csr
smtpd_tls_loglevel = 9
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

# SASL smtp-auth
```

smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_application_name = smtpd
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes
smtpd_tls_auth_only = no
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination

Copie os certificados criados para o apache no */etc/postfix/ssl*:

#mkdir /etc/postfix/ssl
#cp /etc/apache/ssl.csr/dominio.com.br.csr /etc/postfix/ssl
#cp /etc/apache/ssl.crt/dominio.com.br.crt /etc/postfix/ssl
#cp /etc/apache/ssl.key/dominio.com.br.key /etc/postfix/ssl
#chmod 400 /etc/postfix/ssl/*

Crie um link simbólico do diretório de mail para um diretório com o nome do domínio do AD dntro de /home:

 # ln -s /mail /home/DOMINIO

Reinicie o Postfix:

 # /etc/init.d/postfix restart

I.V. Instalando SASL 2

Instale os pacotes do sasl2:

 # apt-get install libsasl2-modules sasl2-bin

Crie o arquivo */etc/postfix/sasl/smtpd.conf* com

pwcheck_method: saslauth

mech_list: plain logi

Edite o arquivo */etc/default/saslauthd*:

 # START=no

por:

START=yes

Crie o arquivo */etc/pam.d/smtp* com:

```
#%PAM-1.0
auth    required     pam_winbind.so
account required     pam_winbind.so
```

Edite o */etc/postfix/master.cf* substituindo as linhas:

```
smtp      inet  n       -       -       -       -       smtpd
```

por:

```
smtp      inet  n       -       n       -       -       smtpd
```

I.VI. Instalação Courier

Instale os pacotes necessários:

 # apt-get install courier-base courier-pop courier-pop-ssl courier-ssl courier Imap courier-authdaemon

Edite o conteúdo dos arquivos */etc/pam.d/imap* e */etc/pam.d/pop3* com:

```
#%PAM-1.0
```

```
auth    required     pam_winbind.so
account required     pam_winbind.so
```

I.VII. Script de Usuários

```
#!/bin/bash

DOMINIO=`wbinfo --own-domain`
mkdir -p /home/$DOMINIO/$1
maildirmake /home/$DOMINIO/$1/Maildir
chown -R $1 /home/$DOMINIO/$1
```

I.VIII. Instalando Spamassassin

Instale o Spamassassin com:

apt-get install spamassassin

Edite a configuração para iniciar o spamassassin:

vi /etc/default/spamassassin

Substitua:

 # Change to one to enable spamd
ENABLED=0

Por:

 # Change to one to enable spamd
ENABLED=1

Inicie o serviço do Spamassassin:

/etc/init.d/spamassassin start

I.IX. Instalando o WebMail

Vamos usar uma versão modificada do Squirrelmail, se trata deum Squirrelmail com uma skin parecida com o Outlook

Baixe o pacote do Squirrelmail Outlook skin theme em:

http://sourceforge.net/projects/squirreloutlook

Nesse exemplo foi usado a versão 1.0.2_1. Descompacte os arquivos dentro de /var/www/ e configure o squirrelmail:

```
# tar -zxvf squirreloutlook-1.0.2_1.tar.gz
# mv squirreloutlook-1.0.2_1 /var/www/squirrelmail
# cd /var/www/squirrelmail/config
# chmod +x conf.pl
# ./conf.pl
```

Edite as opções de acordo com o exibido abaixo:

SquirrelMail Configuration : Read: config.php (1.4.0)

Main Menu --

1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on

S Save data

Q Quit

Command >>

No 1º menu deve ser editado o dado sobre a organização, siga abaixo:

SquirrelMail Configuration : Read: config.php (1.4.0)

Organization Preferences

1. Organization Name : Secretaria da Administração Penitenciária
2. Organization Logo : ../images/logo.png
3. Org. Logo Width/Height : (239/51)
4. Organization Title : Secretaria da Administração Penitenciária
5. Signout Page :
6. Top Frame : _top
7. Provider link : http://www.squirrelmail.org/
8. Provider name : Secretaria da Administração Penitenciária

R Return to Main Menu

C Turn color on

S Save data

Q Quit

Command >>

No 2º menu deve-se editar as configurações do servidor como loopback e domínio:

SquirrelMail Configuration : Read: config.php (1.4.0)

Server Settings

General

---

1. Domain : dominio.com.br
2. Invert Time : false
3. Sendmail or SMTP : SMTP

A. Update IMAP Settings : 127.0.0.1:143 (courier)
B. Update SMTP Settings : 127.0.0.1:25

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >>

O 3º menu trata das opções de pastas de usuários, edite o trash folder, sent folder e draft folder conforme abaixo para palavras em português, farão diferença na interface do webmail.

SquirrelMail Configuration : Read: config.php (1.4.0)

Folder Defaults

1. Default Folder Prefix :
2. Show Folder Prefix Option : false
3. Trash Folder : INBOX.Lixeira
4. Sent Folder : INBOX.Enviados
5. Drafts Folder : INBOX.Rascunhos
6. By default, move to trash : true
7. By default, move to sent : true
8. By default, save as draft : true
9. List Special Folders First : true
10. Show Special Folders Color : true
11. Auto Expunge : true
12. Default Sub. of INBOX : true
13. Show 'Contain Sub.' Option : false
14. Default Unseen Notify : 2

15. Default Unseen Type : 1
16. Auto Create Special Folders : true
17. Folder Delete Bypasses Trash : false
18. Enable /NoSelect folder fix : false

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >>

O 4º menu trata dos diretórios onde ficarão os anexos dos usuários,

SquirrelMail Configuration : Read: config.php (1.4.0)

General Options

1. Data Directory : /var/sqmdata/
2. Attachment Directory : /var/sqmdata/anexos/
3. Directory Hash Level : 0
4. Default Left Size : 160
5. Usernames in Lowercase : false
6. Allow use of priority : true
7. Hide SM attributions : true
8. Allow use of receipts : true
9. Allow editing of identity : true
   Allow editing of name : true
   Remove username from header : false
10. Allow server thread sort : false
11. Allow server-side sorting : false
12. Allow server charset search : true
13. Enable UID support : true
14. PHP session name : SQMSESSID
15. Location base :

R Return to Main Menu

C Turn color on

S Save data

Q Quit

Command >>

No 5º, 6º e 7º menu não precisa editar nada!

O 8º menu trada das questões de plugins do squirrelmail, edite-o conforme o exemplo abaixo:

Plugins

Installed Plugins

1. calendar
2. delete_move_next
3. abook_take
4. newmail
5. notes
6. todo
7. html_mail
8. login_auto
9. compatibility
10. squirrelspell
11. smallcal
12. check_quota

Available Plugins:

13. administrator
14. askuserinfo
15. bug_report
16. filters
17. forced_prefs
18. fortune

19. info
20. listcommands
21. mail_fetch
22. message_details
23. newuser_wiz
24. preview_pane
25. sent_subfolders
26. spamcop
27. translate
28. vkeyboard

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >>

O 9º menu trata das questões de address book, não nos serve neste exemplo:
SquirrelMail Configuration : Read: config.php (1.4.0)

Database
1. DSN for Address Book :
2. Table for Address Book : address

3. DSN for Preferences :
4. Table for Preferences : userprefs
5. Field for username : user
6. Field for prefs key : prefkey
7. Field for prefs value : prefval

8. DSN for Global Address Book :
9. Table for Global Address Book : global_abook
10. Allow writing into Global Address Book : false

11. Allow listing of Global Address Book : false

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >>

O 10º menu trata da língua nativa do squirrelmail, mude a opção 1 para pt_BR:

SquirrelMail Configuration : Read: config.php (1.4.0)

Language preferences
1. Default Language : pt_BR
2. Default Charset : iso-8859-1
3. Enable lossy encoding : false

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >>

Fora do menu de configuração, mova o diretório data para /var/sqmdata e crie o diretório de anexos:

 # mv data /var/sqmdata
 # mkdir -p /var/sqmdata/anexos
 # chown -R www-data.www-data /var/sqmdata