Redes de Computadores II

Aula 12 - Correio Eletrônico – Parte II

Apresentação

Nesta aula, você aprenderá que além do protocolo de envio de e-mails estudado na aula passada, chamado de SMTP, outros protocolos também estão envolvidos no serviço de correio eletrônico, como o POP3 e o IMAP. Além disso, veremos programas relacionados a este tipo de serviço, tais como servidores e clientes de e-mail.

Objetivos

Ao final desta aula, você será capaz de:

- Entender os possíveis formatos (*mailbox* ou *maildir*) utilizados para armazenar as mensagens dos usuários em um servidor de e-mail.
- Entender como o usuário pode ler as mensagens recebidas que estão armazenadas no servidor.
- Compreender o que é um *webmail* e como ele funciona.
- Relacionar quais programas adicionais são usados em conjunto com o servidor de e-mail.

Autenticação para Envio de E-mail

Na aula anterior, estudamos o funcionamento do protocolo SMTP para envio de mensagens eletrônicas. Por padrão, o SMTP não requer autenticação para envio de mensagens, ou seja, você não precisa informar um usuário e senha para poder enviar e-mails. Isso gera dois grandes problemas.

O primeiro problema que pode ocorrer devido à falta de autenticação é que um usuário pode enviar e-mail em nome de outro, e isso pode ter sérias consequências.

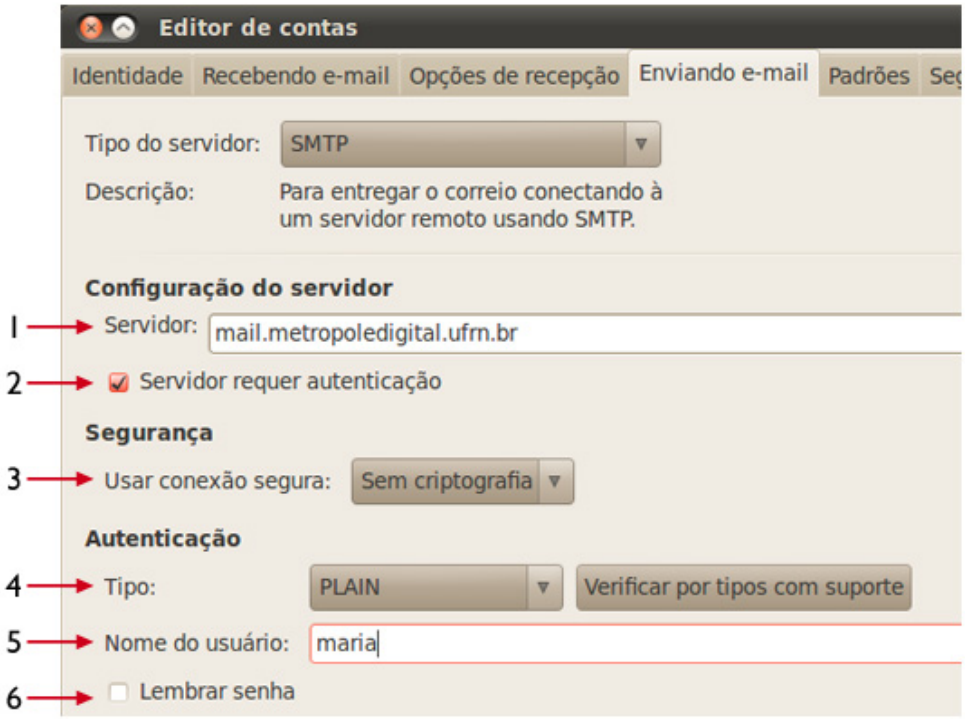
O outro problema é que máquinas com vírus na sua rede podem conectar no seu servidor automaticamente e enviar e-mails. Além de sobrecarregar o servidor e a rede, isso vai gerar um transtorno enorme para os usuários, pois quem recebe a mensagem pode achar que a pessoa constando como remetente do e-mail realmente enviou a mensagem. Além disso, existem vírus que obtêm partes de arquivos da máquina do usuário e os enviam nas mensagens, podendo tornar públicas informações pessoais do usuário.

Embora a utilização de programas antivírus nas máquinas e certificados digitais nos e-mails (que você vai estudar na disciplina de segurança) possam resolver esses problemas, a exigência de autenticação para o envio de e-mails reduz bastante esses tipos de problemas.

> A recomendação é que todo servidor de e-mail exija autenticação dos usuários para envio de e-mails.

A configuração dos programas clientes de e-mails no que diz respeito ao envio consiste basicamente em informar: o endereço do servidor de e-mail, o nome do usuário, e o tipo de autenticação (incluindo o tipo de criptografia). A Figura 1 mostra a tela para configuração desses parâmetros no programa.

Figura 01 - Configuração para envio de mensagens usando SMTP no programa Evolution.



Em 1 é informado o servidor ao qual esse cliente vai conectar para enviar suas mensagens. Normalmente é o servidor da empresa onde o usuário trabalha (ou do seu provedor).

Para ativar a autenticação, deve-se marcar o *checkbox* em 2.

Em 3 é definido se será utilizada criptografia. Veja que é possível utilizar autenticação sem criptografia, mas isso é altamente desaconselhado, porque permite que sua senha seja facilmente capturada por algum *hacker* espionando a rede. Quando se ativa criptografia, normalmente as opções são SSL ou TLS. O valor deve ser o mesmo usado pelo seu servidor de e-mail. O mesmo se aplica ao tipo de autenticação utilizado.

Finalmente, deve-se informar o nome do usuário em 5.

Procure não marcar a opção para gravar sua senha. Se por um lado isso é bom, porque reduz o número de vezes que você vai digitar sua senha, por outro, reduz a segurança e facilita que outras pessoas se passem por você.

Veja aqui a explicação em vídeo sobre a autenticação para envio de e-mail:

Vídeo 01 - Autenticação

Atividade 1

1. A autenticação é sempre requerida para enviar uma mensagem?
2. Qual o problema de usar autenticação sem criptografia?

Relay

Na seção **Enviando uma mensagem**, ao descrevermos como uma mensagem é processada do cliente de e-mail até chegar ao destino, dissemos, no passo 2, que um servidor de e-mail ao receber uma mensagem que não é para ele, vai reencaminhá-la para o servidor de destino correto.

Embora ele precise ter esse comportamento para tudo funcionar bem, isso abre um precedente para uma situação perigosa: qualquer máquina da Internet pode conectar neste servidor de e-mail e enviar mensagens para qualquer outro destino. Isso se chama *Relay*.

Os servidores que aceitam fazer *relay* de qualquer máquina que lhe enviem mensagens são frequentemente usados para atacarem outros servidores.

Portanto, você precisa controlar quem pode fazer *relay* através do seu servidor. Isso pode ser feito de duas formas:

- Fazendo a liberação pelos endereços IP das máquinas clientes. Essa técnica é usada para liberar as máquinas de dentro da rede da sua empresa.

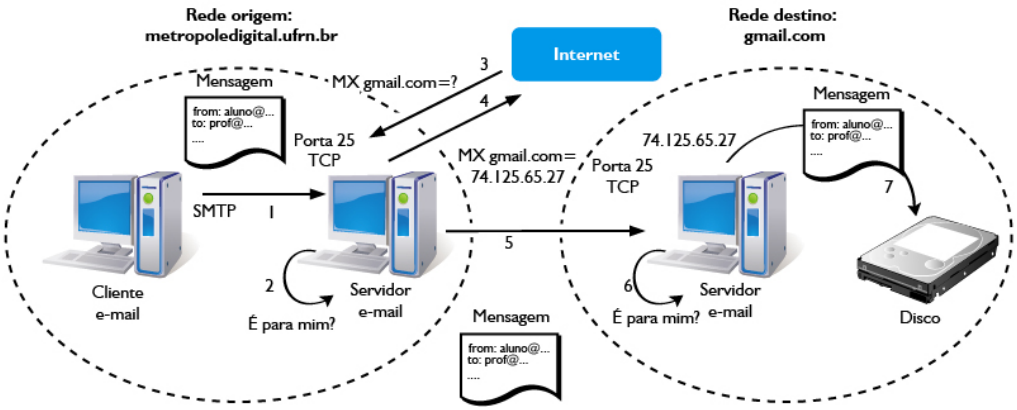
- Liberando o *relay* para todos os usuários que conseguem se autenticar com sucesso no seu servidor. Desse modo, você tem como saber que ele é um usuário autêntico da sua empresa.

Veja aqui a explicação em vídeo sobre relay.

Vídeo 02 - Relay

Formato para Gravação dos E-mails em Disco

Figura 02 - Envio de e-mail para prof@gmail.com usando SMTP.



Se você olhar a Figura 2 vai ver que o último passo (passo 7) no envio de um e-mail é gravá-lo no disco do servidor de e-mail onde o usuário destinatário da mensagem está cadastrado. Como dissemos, isso é feito por um programa a parte de servidor de e-mail.

Dois programas muito usados para essa finalidade são o *procmail* e o *maildrop*.

Mais importante do que o programa que se usa é o formato como eles gravam as mensagens no disco. Existem basicamente dois formatos.

O formato mais antigo se chama *mbox* e consiste em ter um arquivo por usuário, onde cada arquivo armazena todas as mensagens de cada usuário. Tipicamente nos sistemas Linux, esses arquivos estão na pasta /var/spool/mail. Dentro dessa pasta existe um arquivo para cada usuário, e o nome do arquivo é igual ao nome do usuário. Supondo que em um servidor existam os usuários Maria, Pedro e Carlos, então também vão existir os arquivos *maria, pedro e carlos* nessa pasta. A Figura 3 mostra o esquema do *mbox*.

Figura 03 - Mensagens armazenadas no modelo mbox.

Embora esse esquema seja mais simples de entender, ele possui sérios problemas em termos de desempenho.

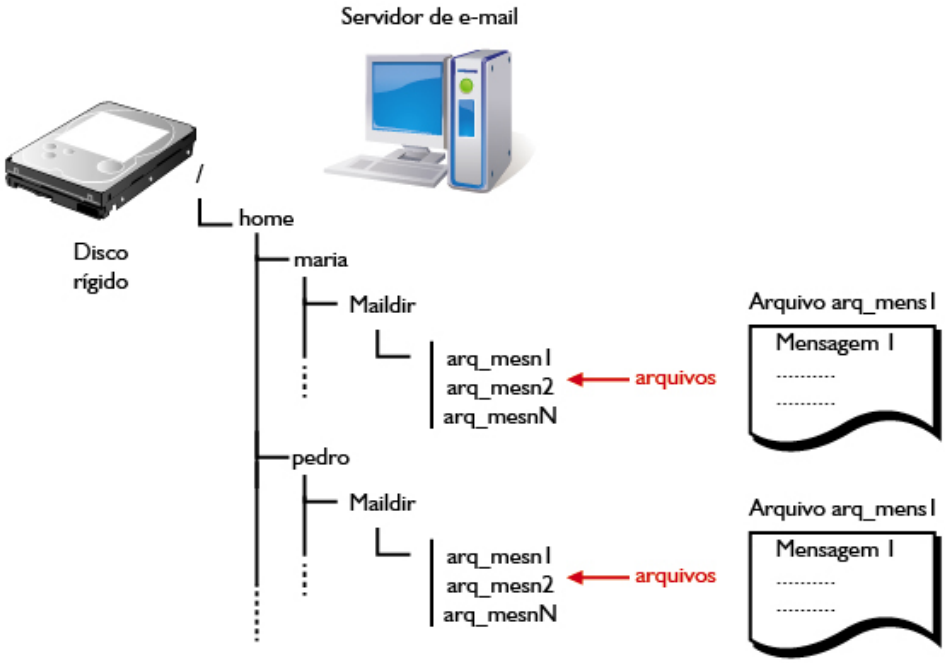
Como todas as mensagens do usuário estão dentro do mesmo arquivo, ele só suporta uma operação por vez (incluir mensagem, excluir etc.). Portanto, enquanto uma nova mensagem estiver chegando, por exemplo, o usuário não poderia estar apagando uma mensagem existente. Além disso, apagar uma mensagem é uma operação custosa porque todo o arquivo precisa ser reorganizado.

Um formato bem mais eficiente é armazenar cada mensagem em um arquivo separado dentro de uma pasta no diretório *home* do usuário. Isso aumenta o paralelismo, pois permite que diversas operações sejam realizadas em várias mensagens diferentes simultaneamente.

Por exemplo, enquanto chega uma nova mensagem (um novo arquivo é criado), uma mensagem existente pode ser excluída (basta apagar o arquivo referente a ela). Além disso, a exclusão de uma mensagem é um processo extremamente simples e rápido, pois consiste apenas em apagar um arquivo.

Normalmente, a pasta criada no diretório do usuário se chama *Maildir*. A Figura 4 mostra o esquema do Maildir. Observe que cada mensagem é um arquivo dentro da pasta Maildir do usuário.

Figura 04 - Mensagens armazenadas no formato *Maildir*.



Veja aqui a explicação em vídeo sobre os formatos para armazenamento dos e-mails em disco.

Vídeo 03 - Armazenamento

Atividade 02

1. Em qual pasta ficam as mensagens dos usuários quando utilizamos mbox?
2. Como as mensagens são armazenadas quando utilizamos *Maildir*?
3. Por que o formato mbox não suporta o recebimento de um novo e-mail enquanto o usuário estiver apagando uma mensagem existente?

Lendo os E-mails Recebidos

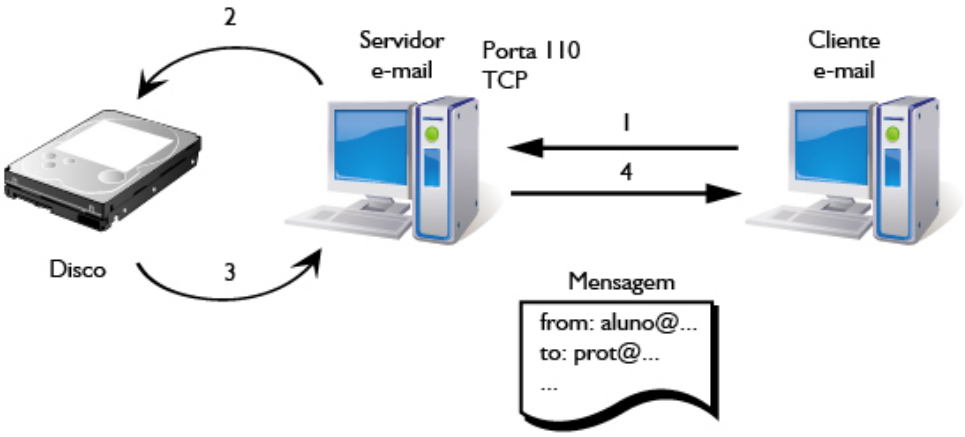
Uma vez que os e-mails sejam recebidos pelo servidor e sejam gravados no disco, você provavelmente vai querer lê-los. Isso é feito usando outro protocolo independente do SMTP. Os dois protocolos mais utilizados são o POP3 e o IMAP, sendo que este último vem sendo cada vez mais utilizado.

Diferentemente do envio de mensagens, onde a autenticação era uma tarefa opcional, para recuperar os e-mails do servidor a autenticação é obrigatória. Idealmente ela deve ser utilizada em conjunto com criptografia para proteger a sua senha enquanto ela estiver sendo transmitida pela rede.

A Figura 5 mostra como um cliente pode recuperar uma mensagem do servidor. No caso, é mostrada a porta 110, que é a porta do POP3, mas o IMAP também poderia ser utilizado.

As setas de 1 a 4 indicam a ordem em que as tarefas são realizadas. Veja que o cliente envia uma requisição para o servidor, que obtém a mensagem do disco e depois a envia de volta ao cliente.

Figura 05 - Recuperando os e-mails do servidor



POP x IMAP

É importante saber as principais diferenças do POP3 para o IMAP para que você possa decidir qual utilizar.

O POP3 foi criado em uma época em que as conexões de Internet eram muito precárias. Utilizava-se principalmente acesso discado, que tem um custo elevado, e com isso as pessoas procuravam ficar conectadas por pouco tempo para reduzir os custos financeiros com a conta telefônica. Assim sendo, o POP3 foi projetado para baixar as mensagens do servidor para a máquina local e permitir sua leitura *off-line*, ou seja, com o usuário desconectado.

No cenário atual, onde as pessoas usam diferentes computadores isso tende a ser um problema. Além do mais, as conexões de Internet possuem melhores velocidades e tipicamente os usuários usam conexões dedicadas, ficando conectados quanto tempo desejarem, sem que isso aumente seu custo.

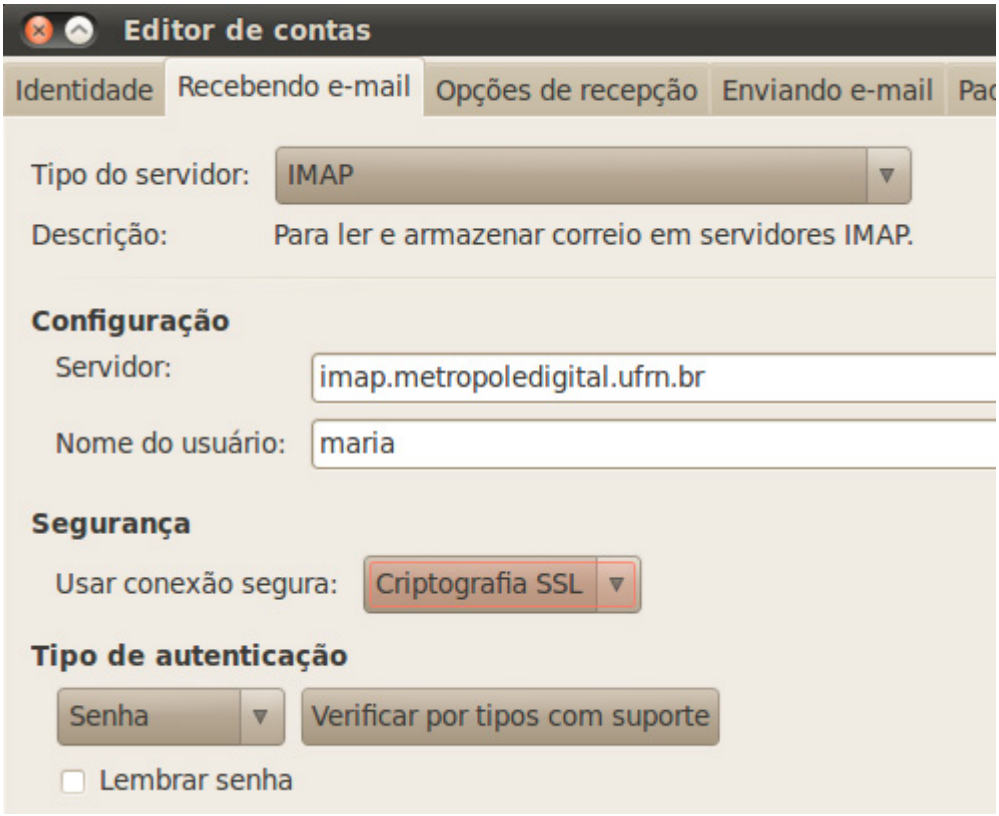
Foi criado então um protocolo chamado IMAP, que é voltado para aproveitar esse novo cenário. O IMAP procura deixar as mensagens no servidor, só trazendo uma cópia para sua máquina das que você pretende ler no momento.

De qualquer modo, s mensagens ficam sempre armazenadas no servidor, permitindo que você as leia de qualquer lugar. O IMAP possui diversas outras vantagens, como permitir que várias pessoas acessem uma conta de e-mail ao

mesmo tempo, permitindo o compartilhamento de caixas postais. Por tudo isso, o IMAP é o protocolo mais utilizado atualmente.

A Figura 6 mostra a tela de configuração de um cliente de e-mail (Evolution) no que diz respeito à parte de leitura dos e-mails. Veja que basicamente são os mesmos parâmetros que configuramos para o envio de e-mail, com a principal diferença de que não há como desabilitar a autenticação, uma vez que ela é obrigatória para a leitura.

Figura 06 - Configuração de cliente de e-mail para leitura das mensagens.



Veja aqui a explicação em vídeo sobre a recuperação dos e-mails do servidor

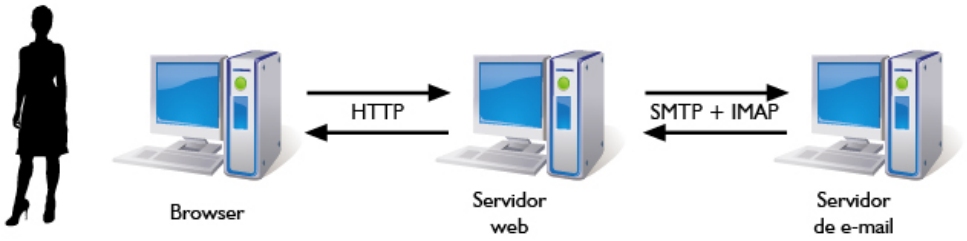
Vídeo 04 - POP x IMAP

Webmail

No início desta aula já falamos que cada vez mais as pessoas estão deixando de usar programas clientes de e-mail, como o *Outlook*, o *Thunderbird*, entre outros, para acessarem seus e-mails através da Web.

Vamos voltar rapidamente a este assunto, agora que você já viu quais protocolos fazem parte de um serviço de correio eletrônico, apenas para mostrar um esquema de como esses protocolos se encaixam no modelo do Webmail. A Figura 7 mostra esse esquema.

Figura 07 - Webmail.



Observe que o usuário utiliza apenas um browser/navegador e que este browser se comunica apenas com o servidor Web. Portanto, nessa etapa só se faz uso do protocolo HTTP.

As páginas do servidor Web, entretanto, são geradas dinamicamente, para que possam conter as mensagens dos usuários. Para isso, o servidor Web se comunica com o servidor de e-mail utilizando o protocolo IMAP (ou POP3). Quando o usuário deseja enviar uma mensagem, o servidor web se comunica com o servidor de e-mail usando o protocolo SMTP.

Nem sempre os programas de envio e recebimento de e-mail são instalados na mesma máquina. Para melhorar o desempenho, algumas empresas instalam um (ou vários) servidor(es) para envio das mensagens (SMTP), outro(s) para recuperação/leitura (IMAP), e ainda outro(s) para servir como Webmail. Naturalmente, este tipo de arranjo requer uma configuração bem mais complexa dos servidores e está fora do escopo de nossa aula.

Veja aqui a explicação em vídeo sobre Webmail.

Vídeo 05 - Webmails

Vídeo 06 - Webmails

Atividade 03

1. Qual a principal vantagem em utilizar um Webmail ao invés de um programa cliente de e-mail convencional?
2. É necessária autenticação para recuperar um e-mail do servidor?
3. Qual a principal diferença entre o POP3 e o IMAP?

Programas Adicionais

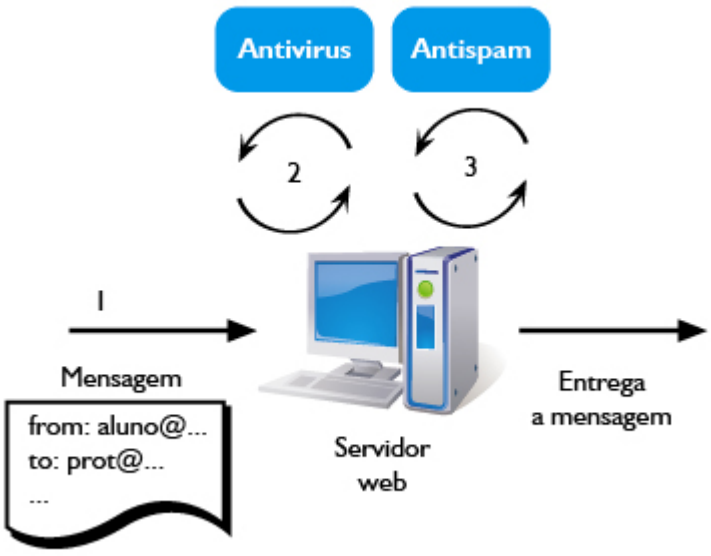
Já vimos que o servidor de e-mail faz uso de um programa adicional para gravar as mensagens no disco. Nesta seção, veremos que ele utiliza também alguns outros programas adicionais. Esses programas são necessários para resolver dois problemas principais que afetam os servidores de e-mail, que são SPAM e vírus.

Provavelmente, você já sabe que SPAMS são mensagens indesejadas enviadas tipicamente para um número elevado de pessoas. Todos os servidores de e-mails recebem um número bastante elevado de spams e precisam filtrá-los para que eles não cheguem até os usuários.

Quando o e-mail surgiu, as mensagens eram formadas basicamente por texto. Atualmente, as coisas mudaram bastante, e cada vez mais as mensagens carregam junto com o texto, diversos tipos de arquivos, desde imagens, vídeos, e programas. Isso tem facilitado enormemente a propagação de vírus nas redes.

Como o servidor de e-mail é a porta de entrada (e saída) de todas as mensagens de uma empresa, nada mais natural do que executar um programa de antivírus junto ao servidor de e-mail para que ele analise todas as mensagens que passam por ele.

Figura 08 - Webmail.



Desse modo, um servidor de e-mail sempre é utilizado em conjunto com programas antivírus e antispam. Conforme mostrado na Figura 8, o servidor de e-mail ao receber uma mensagem, a repassa para os programas de antispam e antivírus (a ordem pode ser diferente da mostrada).

Esses programas analisam a mensagem e a devolvem para o servidor de e-mail identificando se ela é um spam ou se possui vírus. O servidor de e-mail toma a ação predeterminada pelo administrador da máquina, que nesses casos tipicamente seria descartar a mensagem.

Tenha muito cuidado para que seu servidor de e-mail não fique enviando mensagens de spam ou contendo vírus. Existem entidades que mantêm um cadastro de servidores que se comportam desta forma. Esses cadastros são chamados de *listas negras*, e é comum que os servidores da Internet sejam configurados para não aceitarem mensagens de servidores incluídos nessa listas.

Veja aqui uma explicação em vídeo sobre esses programas adicionais.

Vídeo 07 - Programas Adicionais

Resumo

Nesta aula você concluiu seu aprendizado em relação a um dos serviços mais importantes e fundamentais da Internet: o e-mail. Você aprendeu que as mensagens podem ser armazenadas utilizando o formato *mbox* ou *Maildir*, sendo este último o preferido. Também viu que existem dois protocolos (POP3 e IMAP) que o usuário pode utilizar para ler as mensagens recebidas e armazenadas no servidor. Finalmente, você aprendeu que um servidor de e-mail sempre utiliza alguns programas auxiliares para verificar a existência de vírus nos e-mails, ou se uma mensagem é *spam*.

Autoavaliação

1. Qual dos dois protocolos, IMAP ou POP3, é mais utilizado atualmente e por quê?
2. Quais as vantagens em se exigir autenticação para envio de mensagens?
3. Quais as duas formas de controlar quem pode fazer relay em um servidor de e-mail?

Referências

FOROUZAN, B. **Comunicação de Dados e Redes de Computadores**. 3. ed. Rio de Janeiro: Bookman, 2006.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 5. ed. São Paulo: Addison Wesley, 2010.

MORIMOTO, C. **Redes e Servidores Linux**. 2. ed. São Paulo: GDH Press e Sul Editores, 2006.

WETHERALL, D.; TANENBAUM, A. S. **Redes de computadores**. 5. ed. Rio de Janeiro: Editora Pearson, 2011.