UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE TECNOLOGIA

REDES DE COMUNICAÇÃO I

Grupo 6: POP3, POP3 (SSL/TLS) e SMTP

Eric Camille Camargo dos Santos RA: 215419
Gabriel Antônio Lopes de Souza RA: 216070
Gabriel Domingues Ferreira RA: 216207
Gabriel Velasco Fernandes RA: 216507
Giovanni Bassetto RA: 216968
Guilherme Masao Tsuyukubo RA: 217250
Igor da Silva Gouvêa RA: 217956
Isabela Mendes RA: 218123
João Vitor D'Alkimin Basso RA: 218927
Kallynne Yanne Rosa RA: 219525

Limeira - SP
2019

POP 3

POP3 (Post Office Protocol) é um protocolo de configuração de e-mail, ele acessa a caixa de e-mail e **BAIXA** todos os emails da caixa de entrada para o computador que foi configurado. Nesta opção é possível você baixar todos os e-mails (liberando espaço na caixa de e-mail no servidor). Ao utilizar o POP3, não é possível efetuar backup da conta no servidor, pois todos os emails são baixados. O backup dos emails deve ser feito no dispositivo que o utiliza.
POP3 transfere as mensagens, removendo-as do servidor. Deste modo, os e-mails deixam de estar disponíveis através do webmail ou programa de e-mail.

Permite que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas sequencialmente para um computador local. Dessa maneira, o utilizador pode ler as mensagens recebidas, apagá-las, responder-lhes, armazená-las etc.

O funcionamento do protocolo POP3 diz-se *off-line*, uma vez que o processo suportado se baseia nas seguintes etapas:

- É estabelecida uma ligação entre o cliente de e-mail e o servidor onde está a caixa de correio.;
- Todas as mensagens existentes na caixa de correio são transferidas sequencialmente para o computador local;
- As mensagens são apagadas da caixa de correio;
- A ligação com o servidor é terminada;
- O utilizador pode agora ler e processar as suas mensagens (*off-line*).

A característica *off-line* do protocolo POP3 é particularmente útil para utilizadores que se ligam à Internet através de redes públicas comutadas, em que o custo da ligação é proporcional ao tempo de ligação (exemplo: a rede telefônica convencional). Com o POP3, a ligação precisa apenas estar ativa durante a transferência das mensagens, e a leitura e processamento das mensagens pode depois ser efetuada com a ligação inativa.

QUAL É A MELHOR FORMA PARA EU HABILITAR O POP3?

A Brasil Work recomenda habilitar contas de e-mails em POP3 para usuários da empresa que não executam funções gerenciais - Assim, o Dep. de T.I. da empresa pode deixar os Outlook/Thundbird com a senha salva. Desta forma, o funcionários somente utilizarão a caixa de e-mail da empresa, quando estiver fisicamente na empresa.

Esta forma gera **Segurança Jurídica** (uma vez que o funcionário não tem como alegar hora extra) e **Segurança Digital** (o funcionário não saberá a senha do e-mail, assim, não conseguirá abrir a caixa de e-mail em outra ocasião, como não acessará em computadores vulneráveis ou de terceiros).

EXEMPLO PRÁTICO

Para utilizar os emails via POP (ou POP3) é necessário a utilização de um programa de emails. O protocolo POP3 é um protocolo offline no qual, o software de emails conecta-se ao servidor, realiza o download das mensagens e após esse processo, finaliza a conexão.
Esse protocolo tem acesso apenas à Caixa de Entrada, não conseguindo baixar nenhuma outra pasta de sua conta. O acesso via POP baixa as mensagens do servidor e salva as mesmas localmente em seu computador, não deixando uma cópia das mensagens no servidor. Esse tipo de configuração é recomendado para quem precisa acessar os emails em apenas 1 local ou possuem redes com largura de banda baixa.

POP3 (SSL/TSL)

O **Transport Layer Security** (**TLS**), assim como o seu antecessor *Secure Sockets Layer* (**SSL**), é um protocolo de segurança projetado para fornecer segurança nas comunicações sobre uma rede de computadores. Várias versões do protocolo encontram amplo uso em aplicativos como navegação na web, email, mensagens

instantâneas e voz sobre IP (VoIP). Os sites podem usar o TLS para proteger todas as comunicações entre seus servidores e navegadores web.

O protocolo TLS visa principalmente fornecer privacidade e integridade de dados entre dois ou mais aplicativos de computador que se comunicam. Quando protegidos por TLS, conexões entre um cliente (por exemplo, um navegador da Web) e um servidor (por exemplo, wikipedia.org) devem ter uma ou mais das seguintes propriedades:

- A conexão é *privada* (ou *segura*) porque a criptografia simétrica é usada para criptografar os dados transmitidos. As chaves para essa criptografia simétrica são geradas exclusivamente para cada conexão e são baseadas em um segredo compartilhado que foi negociado no início da sessão . O servidor e o cliente negociam os detalhes de qual algoritmo de criptografia e chaves criptográficas usar antes que o primeiro byte de dados seja transmitido. A negociação de um segredo compartilhado é segura (o segredo negociado não está disponível para bisbilhoteiros e não pode ser obtido, mesmo por um invasor que se coloque no meio da conexão) e confiável (nenhum invasor pode modificar as comunicações durante a negociação sem ser detectou).
- A identidade das partes em comunicação pode ser autenticada usando criptografia de chave pública. Essa autenticação pode ser opcional, mas geralmente é necessária para pelo menos uma das partes (geralmente o servidor).
- A conexão é confiável porque cada mensagem transmitida inclui uma verificação de integridade de mensagem usando um código de autenticação de mensagem para evitar perda não detectada ou alteração dos dados durante a transmissão.

Além das propriedades acima, a configuração cuidadosa do TLS pode fornecer propriedades adicionais relacionadas à privacidade, como sigilo de encaminhamento, garantindo que qualquer divulgação futura de chaves de

criptografia não possa ser usada para descriptografar as comunicações TLS registradas no passado.

Tentativas foram feitas para subverter aspectos da segurança das comunicações que o TLS procura fornecer, e o protocolo foi revisado várias vezes para lidar com essas ameaças de segurança. Os desenvolvedores de navegadores da Web também revisaram seus produtos para se defenderem de potenciais pontos fracos de segurança depois que eles foram descobertos.

O protocolo TLS compreende duas camadas: o registro TLS e os protocolos de handshake TLS. O TLS é um padrão proposto pela IETF (Internet Engineering Task Force), definido pela primeira vez em 1999, e a versão atual é o TLS 1.3 definido no RFC 8446 (agosto de 2018). O TLS baseia-se nas especificações SSL anteriores (1994, 1995, 1996) desenvolvidas pela Netscape Communications para adicionar o protocolo HTTPS ao navegador da Web Navigator.

DESCRIÇÃO

O protocolo SSL provê a privacidade e a integridade de dados entre duas aplicações que comuniquem pela internet. Isso ocorre por intermédio da autenticação das partes envolvidas e da cifragem dos dados transmitidos entre as partes. Ainda, esse protocolo ajuda a prevenir que intermediários entre as duas extremidades das comunicações obtenham acesso indevido ou falsifiquem os dados que estão sendo transmitidos.

FUNCIONAMENTO

O servidor do site que está sendo acessado envia uma chave pública ao browser, usada por este para enviar uma chamada secreta, criada aleatoriamente. Desta forma, fica estabelecida a troca de dados criptografados entre dois computadores.

Baseia-se no protocolo TCP da suíte TCP/IP e utiliza-se do conceito introduzido por Diffie-Hellman nos anos 70 (criptografia de chave pública) e Phil Zimmermann (criador do conceito PGP).

HISTÓRIA E DESENVOLVIMENTO

A primeira versão foi desenvolvida pela Netscape em 1994. O SSL versão 3.0 foi lançado em 1996, e serviu posteriormente de base para o desenvolvimento do TLS versão 1.0, um protocolo padronizado da IETF originalmente definido pelo RFC 2246. Grandes instituições financeiras como Visa, Mastercard, American Express, dentre outras, aprovaram o SSL para comércio eletrônico seguro na Internet.

O SSL opera de forma modular, possui *design* extensível e apresenta compatibilidade entre pares com versões diferentes do mesmo.

O SSL executa a autenticação das 2 partes envolvidas nas comunicações (cliente e servidor) baseando-se em certificados digitais.

SMTP

O QUE É SMTP?

A sigla SMTP significa *Simple Mail Transfer Protocol* (Protocolo de Transferência de Correio Simples), o processo por trás do fluxo de e-mail na Internet, usado na arquitetura Internet TCP/IP. Foi padronizado em Agosto de 1982 por Jonathan B. Postel.

Esse é um padrão utilizado com eficiência na transferência de e-mails pela internet, definido na RFC 821. Ele é compatível com as grandes plataformas de e-mail utilizadas atualmente, como o Gmail, o Hotmail e o Outlook. O SMTP é um protocolo apenas de envio, sendo necessário um outro protocolo, como o POP3, para completar a transferência da mensagem eletrônica. Assim, o POP3 — ou outro protocolo com função similar — atua como servidor de entrada e o SMTP atua como servidor de saída.

SMTP é, portanto, uma solução que controla o transporte e a entrega de mensagens enviadas pela internet.

Ele é baseado em linhas de comunicação simples, que garantem o envio de e-mails de forma segura.

SMTP E E-MAILS TRANSACIONAIS

Os e-mails transacionais são essenciais para uma boa estratégia de marketing digital. Eles contribuem para manter o diálogo aberto entre empresa e consumidor, porque são um tipo de resposta automática para determinadas ações feitas no seu site, e-commerce ou portal. Por exemplo, cada vez que um usuário faz o download de um *e-book*, ele pode receber um e-mail fornecendo mais informações sobre o assunto, oferecendo ajuda ou ainda solicitando a opinião do cliente. Também podem ser programados e-mails de boas-vindas sempre que alguém se cadastra no seu site.

Com o SMTP, é possível potencializar essas ações de marketing, automatizar tarefas e implementar as respostas automáticas em diferentes sistemas externos.

FUNCIONAMENTO

A lógica de trabalho é quase a mesma utilizada pelo correio convencional, sendo que o SMTP atua praticamente como o carteiro (intermediário na comunicação entre cliente e servidor). Após serem capturadas, as mensagens são enviadas para ele que, em seguida, encaminha os e-mails aos destinatários finais.

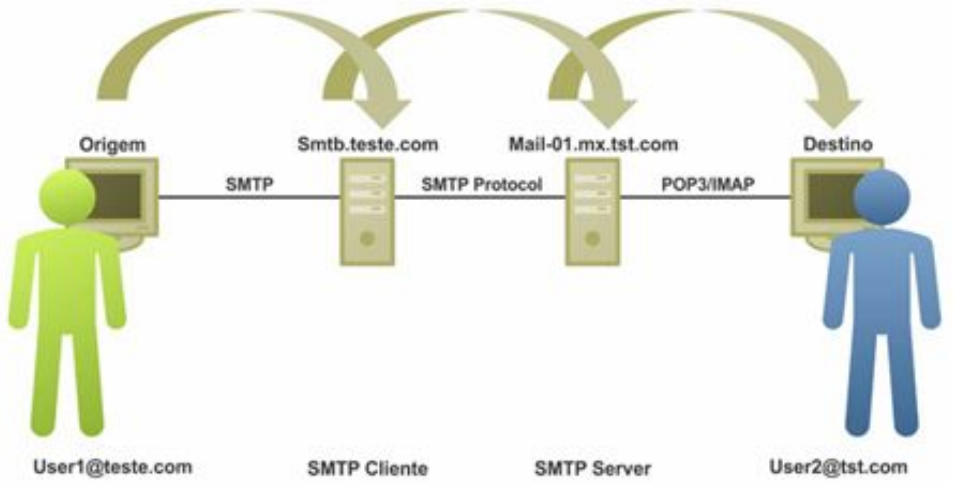
Cada e-mail tem o endereço do remetente (por exemplo, remetente@email.com.br) e o destinatário está no campo “Para” (por exemplo, destinatario@email.com.br). Quando um e-mail é enviado, o provedor de e-mail se conecta ao servidor SMTP do serviço de e-mail do remetente. O provedor transmite o endereço do remetente, o endereço do destinatário e o conteúdo da mensagem. Assim, o servidor SMTP trabalha para localizar o paradeiro do destinatário. Usando o ID de e-mail do destinatário, ele localiza o nome do domínio.

Cada nome de domínio representa um endereço da web exclusivo, que são os endereços de protocolo da Internet (IP). O servidor SMTP, em seguida, contata o servidor onde o registro é mantido: o servidor DNS, que envia de volta o endereço para o servidor SMTP. O servidor SMTP passa, então, a enviar o e-mail para o servidor SMTP do serviço de e-mail do destinatário. Esse servidor SMTP, por sua

vez, verifica e confirma o e-mail endereçado e o entrega à sua contraparte, através do servidor POP3 ou do servidor IMAP.

f

Exemplo de funcionamento:



Um e-mail é enviado da origem “User1@teste.com” passando pelo servidor Cliente “Smtp.teste.com” através do protocolo SMTP que por sua vez irá direcioná-lo ao servidor SMTP “Mail-01.mx.tst.com” que vai recebê-lo e disponibilizá-lo para o destinatário “user2@tst.com”, que terá duas opções para ler este e-mail, através do protocolo POP ou do IMAP.

SEGURANÇA E SPAM

Uma das limitações do SMTP é que ele não tem nenhum método para autenticar a conta de e-mail que está enviando a mensagem, sendo assim é possível utilizar este protocolo para enviar spam com certa “facilidade”.

A princípio o protocolo SMTP utilizava como padrão as portas 25 ou 465 (conexão criptografada) para conexão, porém a partir de 2013 os provedores de internet e as operadoras do Brasil passaram a bloquear a porta 25, e começaram a usar a porta 587 para diminuir a quantidade de SPAM.

Para melhorar a segurança do protocolo foi criada uma extensão chamada SMTP-AUTH que se torna cada vez mais popular entre os usuários. Se você utiliza

uma CMS como WordPress por exemplo, existem plugins que facilitam muito a implementação desta extensão.

Existem provedores de hospedagem (assim como a SECNET) que não permitem o envio de e-mails sem autenticação, justamente para não sofrer com spam e manter a boa reputação dos servidores de envio.

DIFERENÇA ENTRE POP E SMTP

POP é um protocolo padrão da Internet para recebimento de e-mail, que **baixa** as mensagens do servidor para a sua máquina, smartphone ou tablet. **SMTP** é o protocolo para **envio** de e-mail.