Fundamentos de Redes de Computadores

Prof.: MSc. Alex Junior Nunes

alex.nunes@unicesumar.edu.br

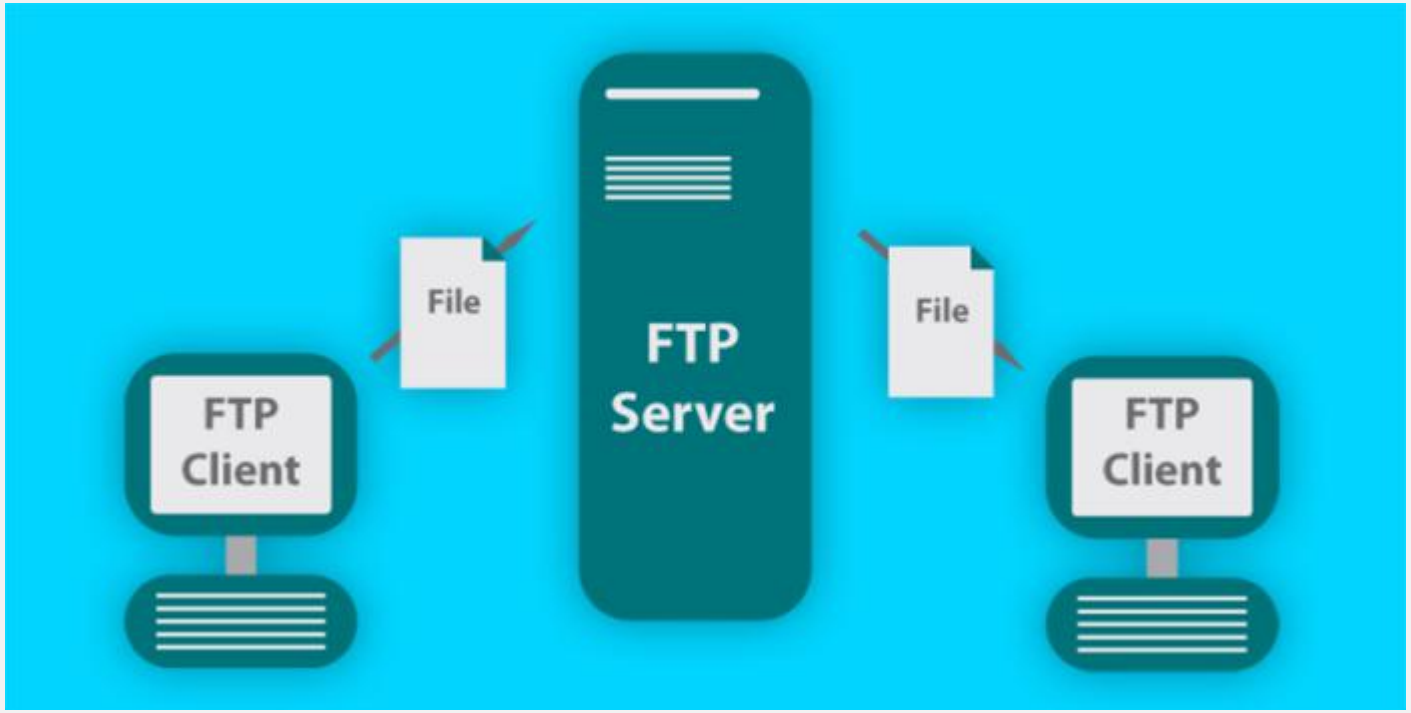
Protocolo FTP

- Sigla para *File Transfer Protocol*
- Protocolo de Transferência de Arquivos
- Ele é basicamente um tipo de conexão que permite a troca de arquivos entre dois computadores conectados à internet
- Também pode ser aplicado em redes locais
- Com isso, você pode enviar qualquer coisa para uma outra máquina ou armazená-los em um servidor FTP, ficando ela sempre disponível para o usuário acessar
- Utiliza o modelo cliente-servidor

Protocolo FTP

- O protocolo é o meio mais antigo de transferir dados entre computadores de uma rede, tendo surgido em 1971
- Ele é considerado inseguro para os padrões de hoje e navegadores modernos estão abandonando o suporte
- Embora seja possível implementar o protocolo SSL (FTPS) para prover conexões mais seguras
- O armazenamento de dados na nuvem é outro modelo cliente/servidor assim como o FTP, com a diferença que os dados não ficam armazenados em um único computador

Protocolo FTP



Protocolo SSL

- O protocolo SSL (*Secure Sockets Layer*) foi desenvolvido pela Netscape Communications Corporation
- Esse protocolo assegura que os dados transferidos entre um cliente e um servidor permaneçam privados
- Esse protocolo permite que o cliente autentique a identidade do servidor

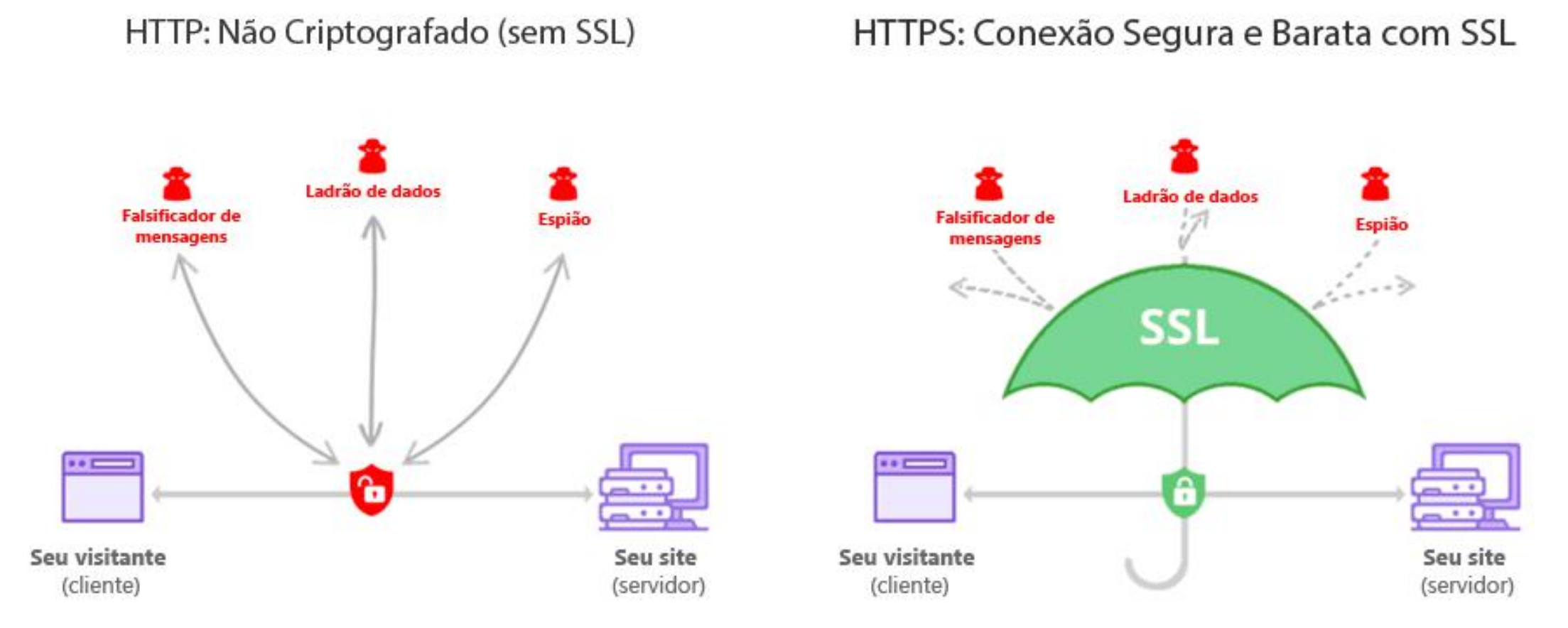
Protocolo SSL

- Quando seu servidor tiver um certificado digital, navegadores ativados para SSL poderão se comunicar com segurança com seu servidor, usando SSL
- Com SSL, você pode facilmente estabelecer um site da Web com segurança ativada na Internet ou em sua intranet privada
- Um navegador que não suporte HTTP através de SSL não pode solicitar URLs utilizando HTTPS
- Os navegadores não SSL não permitem apresentação de formulários que requerem comunicações seguras

Protocolo SSL

SSL	TLS
Seu significado é “camada de segurança de soquete”.	Seu significado é “segurança da camada de transporte".
A Netscape desenvolveu a primeira versão do SSL em 1995.	A primeira versão do TLS foi desenvolvida pela Internet Engineering Taskforce (IETF) em 1999.
SSL é um protocolo criptográfico que usa conexões explícitas para estabelecer uma comunicação segura entre o servidor e o usuário.	O TLS também é um protocolo criptográfico, porém que fornece comunicação segura entre servidor e usuário por meio de conexões implícitas, sendo considerado, assim, o sucessor do SSL.
Teve um total de três versões lançadas: SSL 1.0, 2.0 e 3.0.	Possui quatro versões lançadas: TLS 1.0, 1.1, 1.2 e 1.3.
Todas as versões foram consideradas vulneráveis e descontinuadas.	O TLS 1.0 e 1.1 foram considerados obsoletos em março de 2020. O TLS 1.2 é a versão que mais tem sido implantada até então.

Protocolo SSL



Protocolo SMTP

- O *Simple Mail Transfer Protocol* (SMTP) é um protocolo usado no envio e recebimento de e-mail
- O SMTP é baseado na implementação do protocolo do início de 1971: o protocolo da caixa de correio e o programa SNDMSG
- Somente em 1980, Jon Postel propôs um Mail Transfer Protocol e até hoje continua sendo um dos protocolos mais populares em uso no mundo inteiro

Protocolo SMTP

- No entanto, como é limitado em sua capacidade de enfileirar mensagens na extremidade de recebimento
- Geralmente é usado com um dos dois outros protocolos
  - POP3
  - IMAP
- Que permitem que o usuário salve as mensagens em uma caixa de correio do servidor e faça o download delas periodicamente do servidor

Protocolo SMTP

Em outras palavras, os usuários geralmente usam um programa que usa SMTP para enviar e-mail e POP3 ou IMAP para receber e-mail

Para o consumidor normal, o protocolo SMTP permanece praticamente invisível, uma vez que o respectivo programa de e-mail o executa em segundo plano

No entanto, o SMTP foi projetado para ser um protocolo orientado a conexões com base em texto, deixando dessa forma desprotegida para interceptação de mensagens e fraudes.

Protocolo POP

- Post Office Protocol (POP)
- Com o POP, é possível configurar uma máquina como um ponto de recebimento de e-mail.
- O POP fornece uma maneira simples e padronizada para os usuários acessarem caixas de correio e baixarem mensagens para seus computadores
- O POP permite que a caixa de correio de um usuário resida em um host remoto, mas permite que o usuário recupere as mensagens da caixa de correio remota sob demanda

Protocolo POP

- Como tal, o POP é orientado pelo usuário, já que o e-mail não é transferido até que seja solicitado
- Após a transferência, o usuário pode ler e-mails no sistema local sempre que for conveniente
- As respostas são retransmitidas para o servidor POP usando o SMTP
- Existem duas versões de POP: o POP2 e o POP3

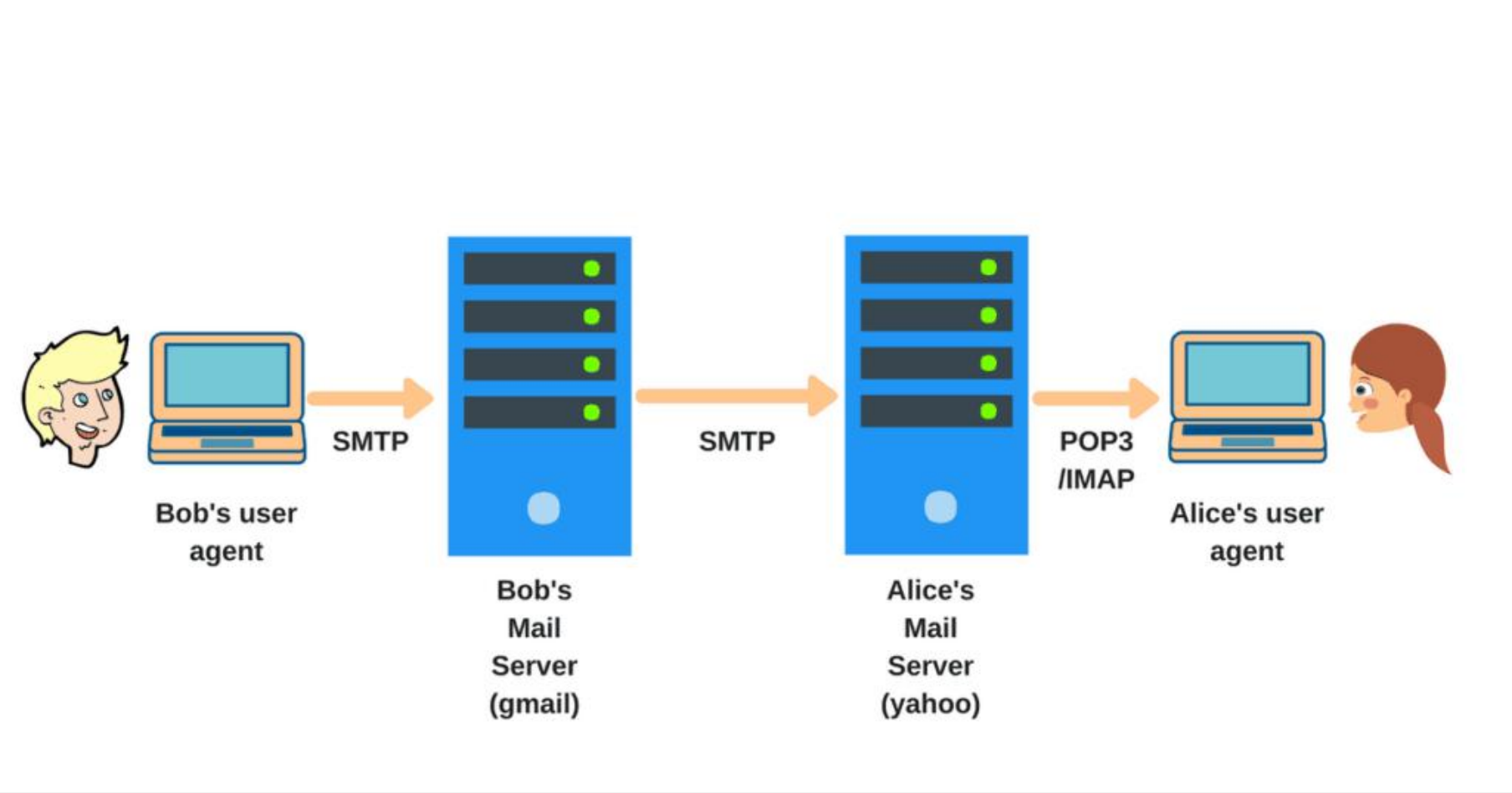
Protocolo IMAP

- Internet Message Access Protocol (IMAP)
- Usado para acessar e-mails no servidor da web remoto a partir do cliente local
- O IMAP pode ser considerado como um servidor de arquivos remoto
- A principal diferença dele o do SMTP é a função que eles desempenham
- SMTP é o protocolo para envio de e-mail, seja do cliente ou entre servidores, para propagar a mensagem ao destino pretendido

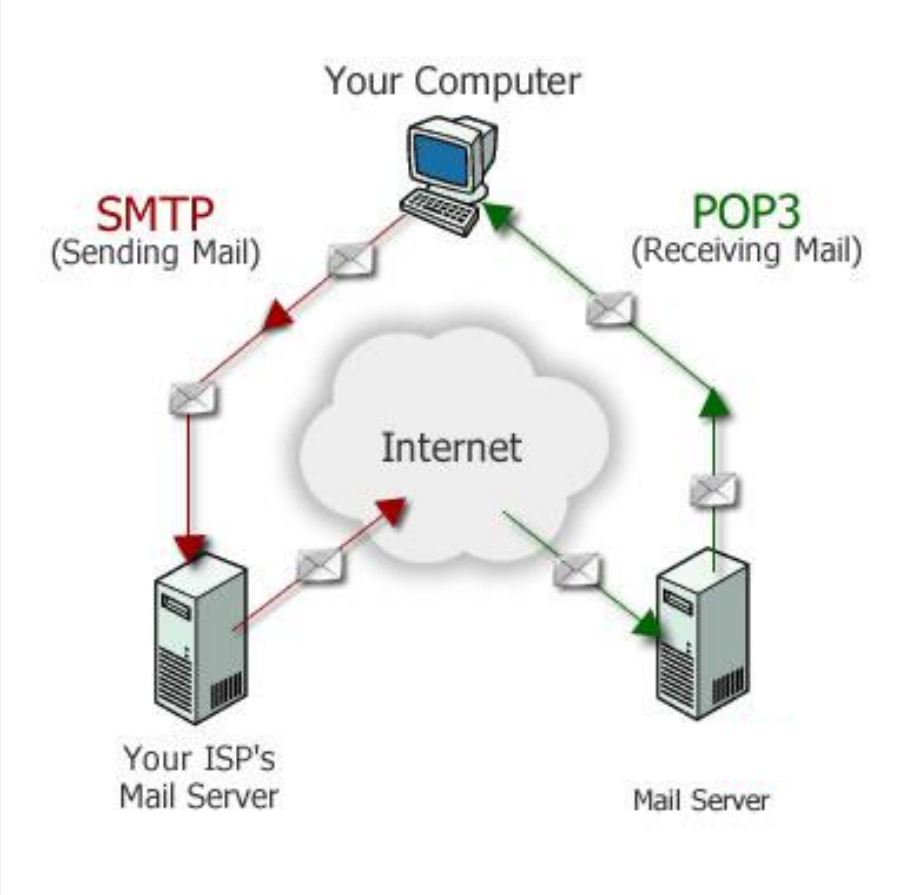
Protocolo IMAP

- Em comparação, o IMAP é um protocolo que lida com o gerenciamento e a recuperação de mensagens de e-mail do servidor
- Então, se você estiver usando e-mail, provavelmente está usando os dois protocolos, mesmo que não saiba
- O IMAP oferece ao usuário mais recursos, retendo e-mails no servidor e organizando-os em pastas
- Além disso, permite o acesso simultâneo por vários clientes
- Portanto, é bastante adequado para acessar seu e-mail a partir de diferentes dispositivos e locais

Protocolos de e-mail



Protocolos de e-mail



Protocolo Telnet

- Telnet é um protocolo de rede na Internet ou redes locais para proporcionar uma facilidade de comunicação baseada em texto interativo bidirecional usando uma conexão de **terminal virtual**
- Os dados do usuário são intercalados em banda com informações de controle Telnet em um byte de conexão 8-bit de dados orientado sobre o Transmission Control Protocol (TCP)

Protocolo Telnet

- O protocolo Telnet é um protocolo standard de Internet que permite a interface de terminais e de aplicações através da Internet
- Este protocolo fornece as regras básicas para permitir ligar um cliente (sistema composto de uma afixação e um teclado) a um intérprete de comando (do lado do servidor)
- O Telnet existe há mais de 40 anos, muito antes de aparecer a Internet

Protocolo Telnet

- Este sistema de transmissão de dados foi inventado pelas Forças Armadas Americanas para transmissão de dados entre bases militares
- Foi disponibilizado ao público em 1977, tendo sido os radioamadores os primeiros a aproveitá-lo

Protocolo SSH

- O SSH é um protocolo que garante que cliente e servidor remoto troquem informações de maneira segura e dinâmica
- O processo é capaz de criptografar os arquivos enviados ao diretório do servidor, garantindo que alterações e o envio de dados sejam realizados da melhor forma

Protocolo SSH

- *Secure Shell* (SSH)
- É um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura
- O melhor exemplo de aplicação conhecido é para login remoto de utilizadores a sistemas de computadores

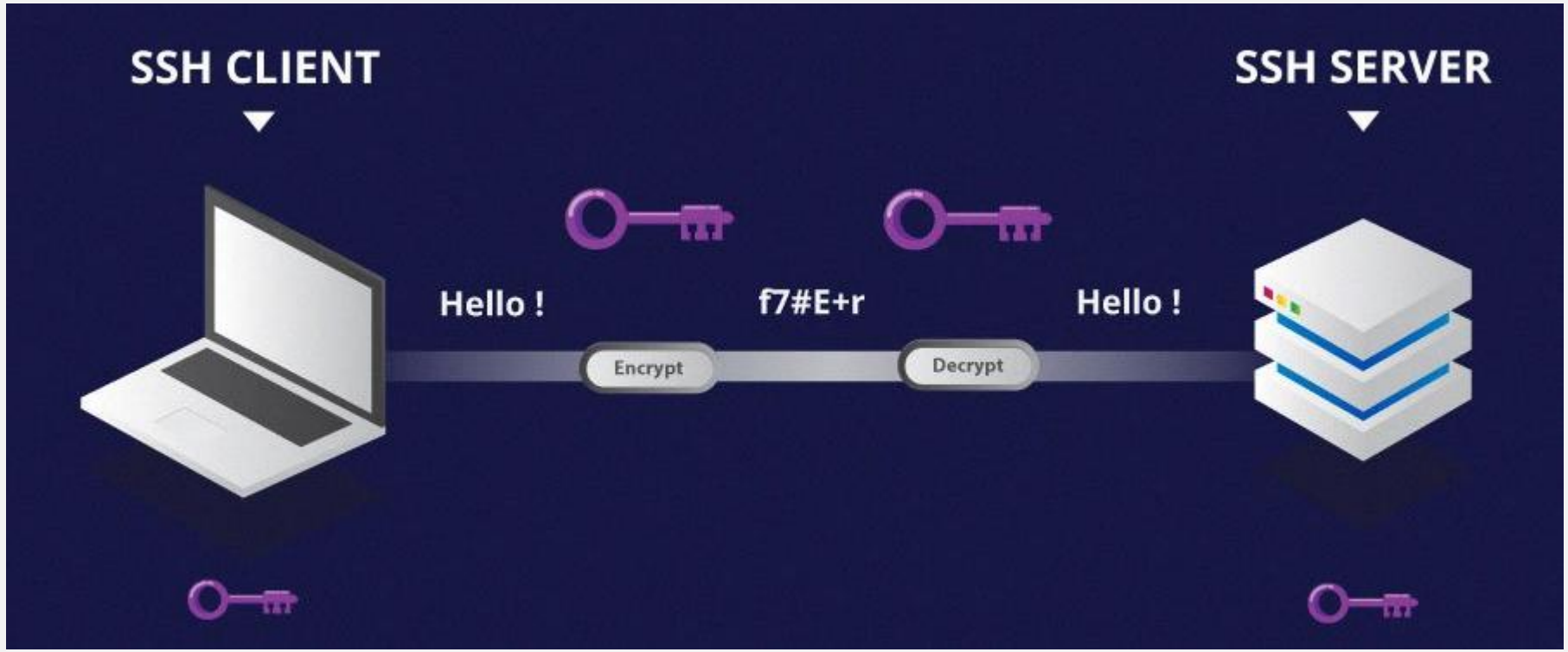
Protocolo SSH

- O SSH fornece um canal seguro sobre uma rede insegura em uma arquitetura cliente-servidor, conectando uma aplicação cliente SSH com um servidor SSH
- Aplicações comuns incluem login em linha de comando remoto e execução remota de comandos, mas qualquer serviço de rede pode ser protegido com SSH
- A especificação do protocolo distingue entre duas versões maiores, referidas como SSH-1 e SSH-2
- A aplicação mais visível do protocolo é para acesso a contas shell em sistemas operacionais do tipo Unix, mas também verifica-se algum uso limitado no Windows

Protocolo SSH

- O SSH foi projetado como um substituto para o Telnet e para protocolos de shell remotos inseguros como os protocolos Berkeley rlogin, rsh e rexec
- Estes protocolos enviam informações, especialmente senhas, em texto simples, tornando-os suscetíveis à interceptação e divulgação usando análise de pacotes
- A criptografia usada pelo SSH objetiva fornecer confidencialidade e integridade de dados sobre uma rede insegura, como a Internet, apesar dos arquivos vazados por Edward Snowden indicarem que a Agência de Segurança Nacional pode algumas vezes descriptografar o SSH, permitindo-os ler o conteúdo de sessões SSH

Protocolo SSH



Protocolo SSH