



Redes de computadores

# SSH

Secure Socket Shell



# Introdução

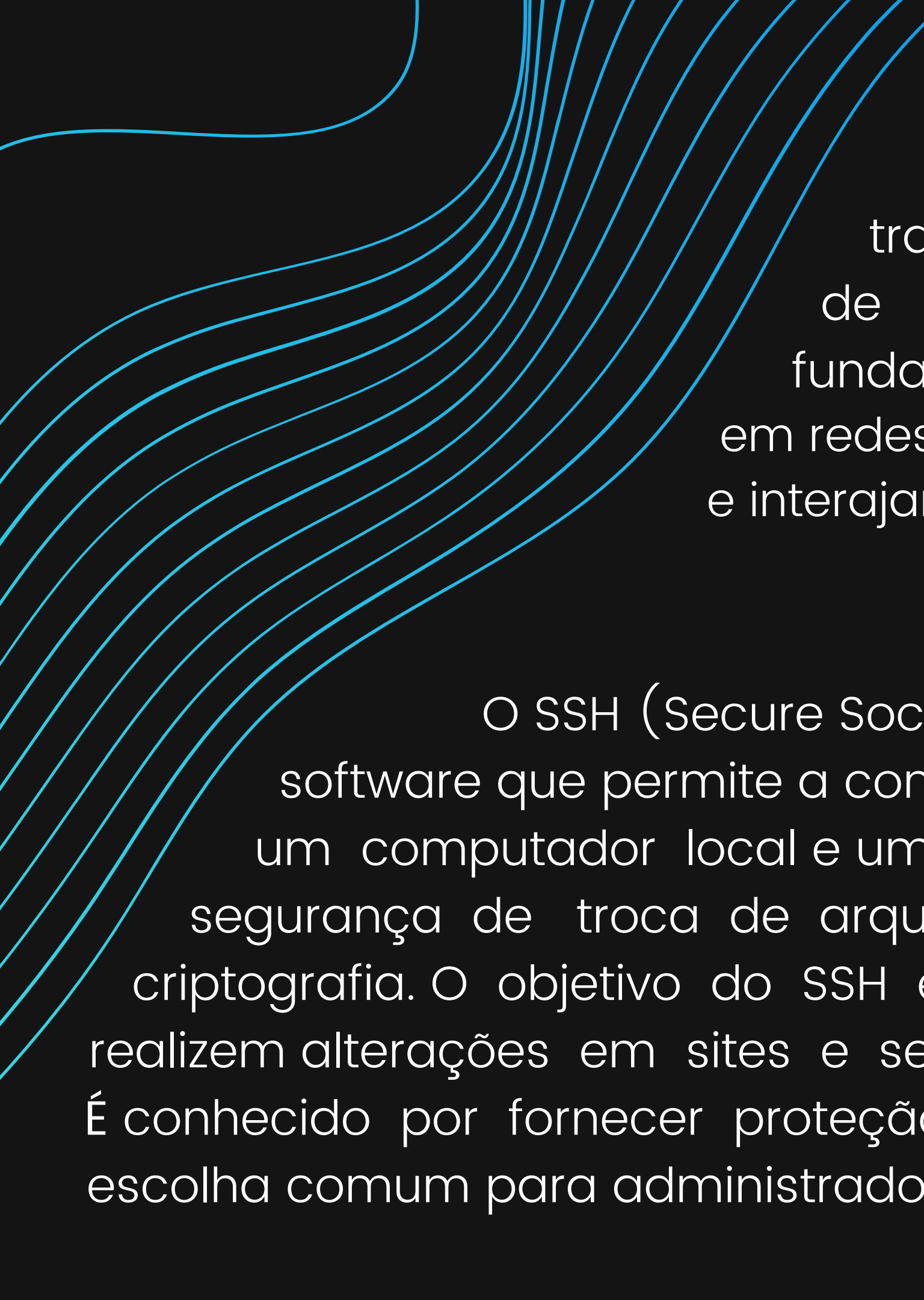


Nesta apresentação serão introduzidos os conhecimentos básicos sobre o protocolo de SSH na disciplina de Redes de Computadores.

Geovanna Teresa Felix

---

2313275



Os protocolos de rede são conjuntos de regras e convenções que governam a comunicação e a transferência de dados entre dispositivos em uma rede de computadores. Eles desempenham um papel fundamental na garantia da comunicação eficaz e segura em redes, permitindo que dispositivos diferentes compreendam e interajam uns com os outros.

O SSH (Secure Socket Shell) é um protocolo de rede e um programa de software que permite a comunicação segura entre dois dispositivos, geralmente um computador local e um servidor remoto. É um dos protocolos específicos de segurança de troca de arquivos entre cliente e servidor de internet, usando criptografia. O objetivo do SSH é permitir que desenvolvedores ou outros usuários realizem alterações em sites e servidores utilizando uma conexão simples e segura. É conhecido por fornecer proteção contra ameaças de segurança, tornando-o uma escolha comum para administradores de sistemas.

# Para que serve?

O SSH é uma ferramenta fundamental para proteger comunicações e acesso a computadores em redes, tornando os acessos e as transferências de dados mais seguras.

- **Acesso Remoto:** O SSH permite controlar um computador à distância de forma segura, útil para administrar servidores ou computadores remotos.
- **Transferência de Arquivos:** Pode ser usado para mover arquivos de uma máquina para outra de maneira segura.
- **Encaminhamento de Portas:** Ajuda a acessar serviços em computadores remotos de maneira segura.
- **Tunelamento de Tráfego:** Protege suas comunicações ao navegar em redes públicas, como redes Wi-Fi em cafés.
- **Autenticação Segura:** Garante que apenas pessoas autorizadas possam acessar sistemas remotos.  
**Segurança de Senhas:** Protege contra tentativas de adivinhar senhas.
- **Segurança de Dados:** Mantém suas informações seguras e confidenciais durante a transmissão.



# Como funciona

## Autenticação:

O processo começa com a autenticação do cliente no servidor. Isso envolve o envio das credenciais, como nome de usuário e senha, ou chaves de autenticação SSH. O uso de chaves SSH é mais seguro do que senhas, pois não são transmitidas pela rede.

## Troca de chaves:

Após a autenticação inicial, o servidor e o cliente iniciam uma troca de chaves para estabelecer uma conexão segura. Isso envolve a negociação de algoritmos criptográficos, como algoritmos de criptografia, hashes e métodos de autenticação.

## Criação de um canal seguro:

Uma vez que a troca de chaves é bem-sucedida, o SSH estabelece um canal seguro entre o cliente e o servidor. Todo o tráfego de dados que passa por esse canal é criptografado, protegendo as informações de terceiros.

## Comandos e transferência de dados:

O cliente SSH pode agora enviar comandos ou realizar transferências de arquivos para o servidor através do canal seguro. Tudo o que é transmitido é criptografado e protegido.

## Encerramento da sessão:

Quando a sessão é encerrada, os canais seguros são desativados e a conexão é encerrada.

SSH CLIENT



Hello!



f7#E+r



Hello!

SSH SERVER



Criptografado

Descriptografado

# Quais portas utiliza?

## TCP / UDP?

Utiliza o **protocolo TCP** para estabelecer conexões seguras.

A porta padrão para conexões SSH é a **porta 22**.

Portanto, as conexões SSH o correm via TCP na porta 22 por padrão.

Embora o padrão seja na porta 22, é possível configurar o SSH para ouvir em portas diferentes se necessário.

O SSH não usa o protocolo UDP para suas conexões padrão.

# Conectividade de rede

---

Os sistemas que desejam usar o SSH devem estar conectados à mesma rede ou à internet.

# Porta SSH aberta

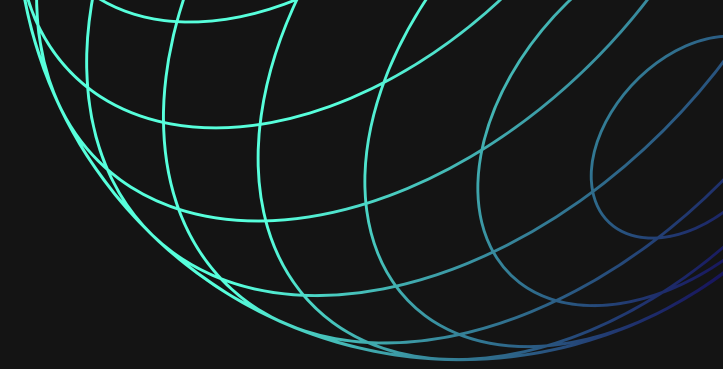
---

O servidor deve estar configurado para ouvir em uma porta específica que deve estar aberta/acessível. Ou seja, não deve haver bloqueios de firewall ou restrições de porta que impeçam a comunicação na porta SSH.

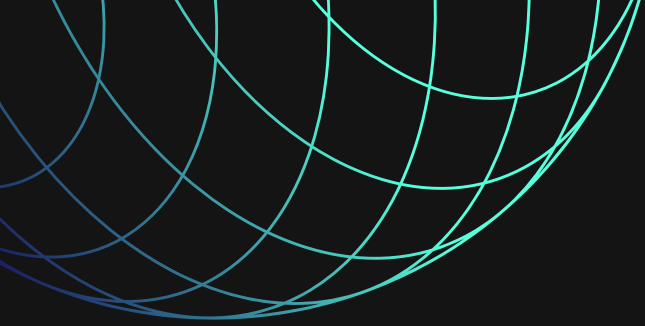
# Endereços IP e DNS

---

Os sistemas precisam de endereços IP corretamente configurados e funcionando. Se estiver usando nomes de host em vez de endereços IP, o DNS deve estar configurado corretamente para resolver os nomes de host em endereços IP.







## Roteamento

---

A rede deve permitir o roteamento adequado entre o cliente SSH e o servidor SSH. Isso é especialmente importante se o cliente e o servidor estiverem em redes diferentes.

## Configuração de firewall

---

Os firewalls em ambas as extremidades (cliente e servidor) permitam o tráfego na porta SSH.. Isso inclui firewalls em sistemas locais e firewalls de rede.

## Acesso de rede

---

Os sistemas devem ter permissão para se conectar uns aos outros por meio da rede. Isso envolve a configuração apropriada de permissões de rede, políticas de segurança e autenticação, incluindo a configuração de chaves SSH ou senhas para autenticação.

# Aplicações

Esses são apenas alguns exemplos de como o SSH é amplamente utilizado em uma variedade de aplicações para garantir a segurança da comunicação e autenticação em ambientes de rede.

## Acesso remoto a servidores

O processo começa com a autenticação do cliente no servidor. Isso envolve o envio das credenciais, como nome de usuário e senha, ou chaves de autenticação SSH. O uso de chaves SSH é mais seguro do que senhas, pois não são transmitidas pela rede.

## Túneis SSH

Os túneis SSH permitem que o tráfego de rede seja encapsulado em uma conexão SSH segura, o que é útil para proteger comunicações de dados sensíveis, contornar firewalls ou acessar recursos de rede remotamente.

## Acesso a dispositivos IoT

O SSH é usado para acessar e gerenciar dispositivos da Internet das Coisas (IoT) que suportam o protocolo.

## Transferência de arquivos segura

É frequentemente usado para transferência de arquivos segura, substituindo protocolos menos seguros, como o FTP. O SFTP é um exemplo disso, permitindo a transferência de arquivos criptografados sobre uma conexão SSH.

## Acesso a bancos de dados

Muitas vezes, o SSH é usado para acesso seguro a bancos de dados remotos, permitindo a administração e consulta de bancos de dados de maneira segura.

## Gerenciamento de dispositivos de rede

Dispositivos de rede, como roteadores e switches, podem ser configurados e gerenciados por meio de conexões SSH seguras.

An abstract graphic consisting of numerous thin, flowing teal lines that originate from the top left and curve across the top of the slide, creating a sense of movement and depth.

# Ficou alguma dúvida?

Fique a vontade para perguntar