O SSH é executado sobre o conjunto de protocolos TCP/IP, do qual grande parte da internet depende.TCP significa protocolo de controle de transmissão e IP significa protocolo de internet . O TCP/IP combina esses dois protocolos para formatar, rotear e entregar pacotes. O IP indica, entre outras informações, para qual endereço de IP um pacote deve ir (pense em um endereço de correspondência), enquanto o TCP indica para qual porta um pacote deve ir em cada endereço de IP (pense no andar de um prédio ou no número de um apartamento).

O TCP é um protocolo de camada de transporte: ele se preocupa com o transporte e a entrega de pacotes. Normalmente, protocolos adicionais são usados sobre o TCP/IP para colocar os dados transmitidos em um formato que o aplicativo possa usar. O SSH é um desses protocolos. (Outros exemplos incluem HTTP, FTP e SMTP).

**1. Escolha de um cliente SSH**

O primeiro passo para acessar o **SSH** é utilizar um cliente ou ferramenta **SSH**, como as que comentamos no tópico anterior. Lembre-se que existem várias opções disponíveis, dependendo do sistema operacional que você utiliza.

**2. Obtenção dos dados de conexão**

Para acessar um servidor via **SSH**, você precisará dos seguintes dados:

- Endereço IP ou domínio do servidor que deseja acessar.
- Nome de usuário no servidor remoto.
- Senha ou chave **SSH** privada para autenticação.

**3. Conectando ao servidor via linha de comando**

Se você estiver em um ambiente de terminal (Linux), basta usar o seguinte comando: ssh usuario@servidor

Onde:

- Usuário é o nome de usuário no servidor remoto.
- Servidor é o endereço IP ou domínio do servidor ao qual você está se conectando.

Por exemplo, para conectar como "admin" em um servidor com IP "192.168.1.100", você usaria: ssh admin@192.168.1.100

**4. Autenticação**

Após executar o comando, o terminal solicitará sua senha ou, se configurado, fará a autenticação utilizando a chave **SSH** privada.

Se for a sua primeira conexão com o servidor, você verá uma mensagem perguntando se deseja continuar com a conexão. Nesse caso, basta digitar "yes" para prosseguir.

**5. Mantendo a conexão segura**

Após acessar o servidor via **SSH**, certifique-se de seguir boas práticas de segurança:

- ❿ Não compartilhe suas credenciais de acesso.
- ❿ Use **chaves SSH** em vez de senhas sempre que possível.
- ❿ Configure autenticação multifator (MFA) se disponível.

O **SSH** oferece uma maneira eficaz e segura de acessar servidores remotamente, permitindo executar comandos, fazer alterações no sistema e gerenciar arquivos com facilidade.