



Debian server
SSH

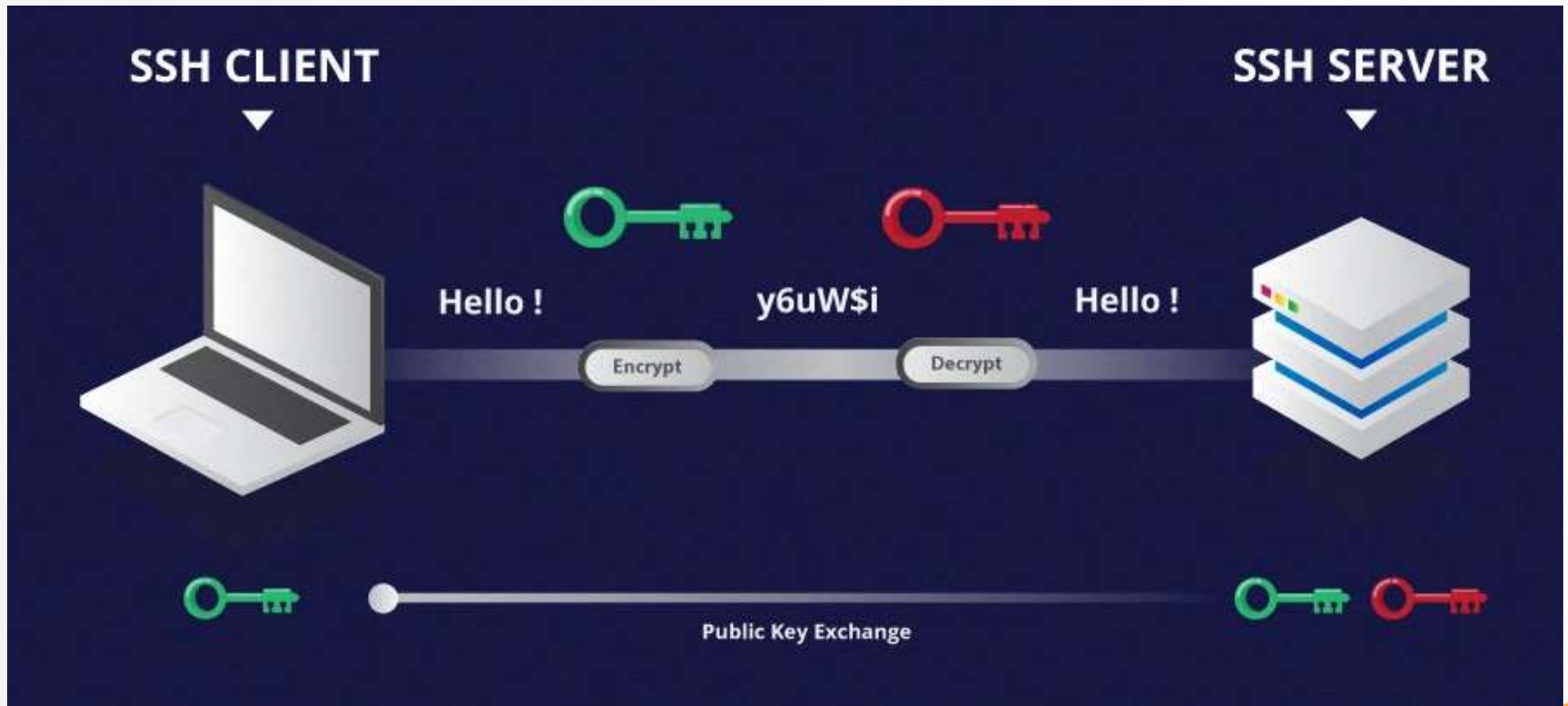
O que é SSH

- Significa *Secure Shell*, é um protocolo de rede criptográfico usado para comunicação e controle remoto e seguros de serviços de rede por meio de uma rede não segura. Substitui o antigo Telnet.
- Ele fornece uma maneira segura de acessar e gerenciar sistemas remotos, no Modelo Cliente/Servidor
- Seu serviço funciona com o protocolo TCP na porta 22 (padrão).

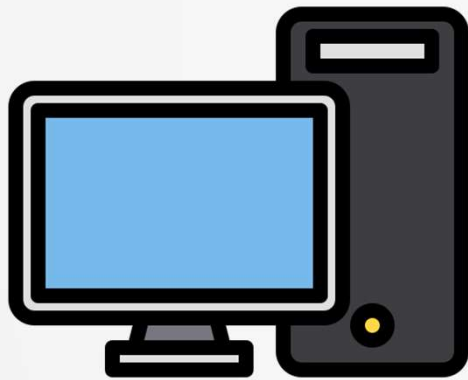
SSH - Características

- **Criptografia:** Criptografa todos os dados transmitidos pela rede, incluindo nomes de usuário, senhas e os próprios dados em transferência.
- **Autenticação:** O SSH usa vários métodos de autenticação de usuário, incluindo senhas, criptografia de chave pública e autenticação de vários fatores.
- **Comunicação Segura:** Fornece canais de comunicação seguros por meio dos quais os usuários podem acessar sistemas remotos. Isso inclui sessões de terminal, transferências de arquivos.
- **Redirecionamento de Porta:** O SSH suporta redirecionamento de porta local e remoto, o que permite que os usuários criem túneis para conexões de rede por meio de uma sessão SSH.
- **Gerenciamento de Chaves:** Chaves SSH são frequentemente usadas para autenticação. Os usuários geram um par de chaves (pública e privada), e a chave pública é armazenada no servidor remoto, enquanto a chave privada é mantida em segurança.
- **Compatibilidade:** O SSH é amplamente suportado em vários sistemas operacionais, incluindo Linux, Unix, macOS e Windows.
- **Melhores Práticas de Segurança:** Para garantir a segurança do SSH, é importante seguir as melhores práticas, como desabilitar a autenticação baseada em senha, atualizar regularmente o software SSH e configurar firewalls para restringir o acesso SSH a endereços IP confiáveis.

Como Funciona?

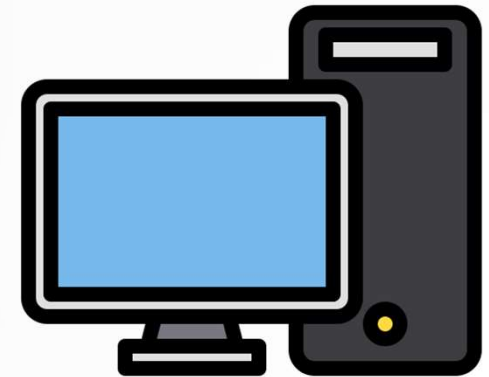
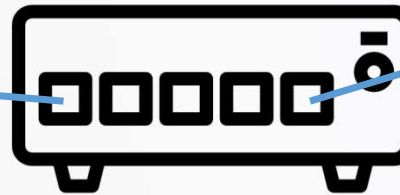


Cenário para teste



- VM Linux Debian 12
- Ip: 192.168.0.1 (rede Interna)
- SSH configurado

- Rede virtual
- Interfaces modo rede interna



- VM Windows (7/10)
- Ip: 192.168.0.5 (rede Interna)
- Executando Putty

Instalando e configurando o SSH no Debian

- Verificação do SSH no Debian. Por padrão o SSH vem no formato cliente, precisamos configurá-lo para ser SSH servidor.

- `# vim /etc/ssh/ssh_config`

```
aluno@debian: ~  
# This is the ssh client system-wide configuration file. See  
# ssh_config(5) for more information. This file provides defaults for  
# users, and the values can be changed in per-user configuration files  
# or on the command line.  
  
# Configuration data is parsed as follows:  
# 1. command line options  
# 2. user-specific file  
# 3. system-wide file  
# Any configuration value is only changed the first time it is set.  
# Thus, host-specific definitions should be at the beginning of the  
# configuration file, and defaults at the end.  
  
# Site-wide defaults for some commonly used options. For a comprehensive  
# list of available options, their meanings and defaults, please see the  
# ssh_config(5) man page.  
  
Include /etc/ssh/ssh_config.d/*.conf  
  
Host *  
# ForwardAgent no  
# ForwardX11 no  
"/etc/ssh/ssh_config" 53L, 1650B
```


Instalando o SSH no Debian

- É possível instalar somente com o comando:

- `#apt install ssh`

- Ou

- `#apt install openssh-server`

- Com as 2 opções será identificado a necessidade dos mesmos pacotes.

```
root@debian:/# apt install ssh
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
O seguinte pacote foi instalado automaticamente e já não é necessário:
  linux-image-6.1.0-9-amd64
Utilize 'apt autoremove' para o remover.
The following additional packages will be installed:
  openssh-server openssh-sftp-server runit-helper
Pacotes sugeridos:
  molly-guard monkeysphere ssh-askpass ufw
Os NOVOS pacotes a seguir serão instalados:
  openssh-server openssh-sftp-server runit-helper ssh
0 pacotes atualizados, 4 pacotes novos instalados, 0 a serem removidos e 0 não a
tualizados.
É preciso baixar 700 kB de arquivos.
Depois desta operação, 2.400 kB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n]
```

Creating config file /etc/ssh/sshd_config with new version

```
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:D2QSYsuPuYXH50LvURQaoVpptoQnX0GTo/ej8LiJTjk root@debian (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:mcwvUd1cpbxY9RunWwBR6GzFvEzqX89ZcKa0hV8qLZ0 root@debian (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:am00andFGy0Kfwl1bvR7RdViPNjS6X4tCJj6AlHuzio root@debian (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.servi
ce.
```

Verificando o status do serviço SSH

- `#systemctl status sshd`

```
root@debian:/# systemctl status sshd
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Sat 2023-09-23 19:11:15 -03; 5min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 3302 (sshd)
    Tasks: 1 (limit: 2286)
   Memory: 1.5M
      CPU: 48ms
   CGroup: /system.slice/ssh.service
           └─3302 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

set 23 19:11:15 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell
set 23 19:11:15 debian sshd[3302]: Server listening on 0.0.0.0 port 22.
set 23 19:11:15 debian sshd[3302]: Server listening on :: port 22.
set 23 19:11:15 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell s
lines 1-16/16 (END)
```


Configurando o SSH

- Por padrão o usuário root é bloqueado.
- Vamos habilitar o acesso ao usuário root.
- Editando o arquivo de configuração:
- `#vim /etc/ssh/sshd_config`
- Após é necessário reiniciar o serviço SSH.
- `#systemctl restart sshd`

```
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

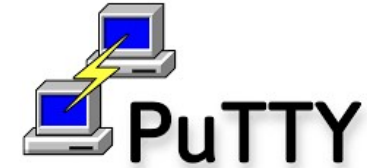
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
-- INSCRIÇÃO --
```

33,20

23%

Cliente SSH Putty



- É um software de emulação de terminal grátis e de código livre, utiliza o protocolo SSH para o acesso remoto a servidores via shell seguro.
- Permite download de arquivos via SFTP (SSH File Transfer Protocol), e a criação de “túneis” cifrados entre servidor/cliente.
- Download:
- <https://www.putty.org/>

MSI (‘Windows Installer’)

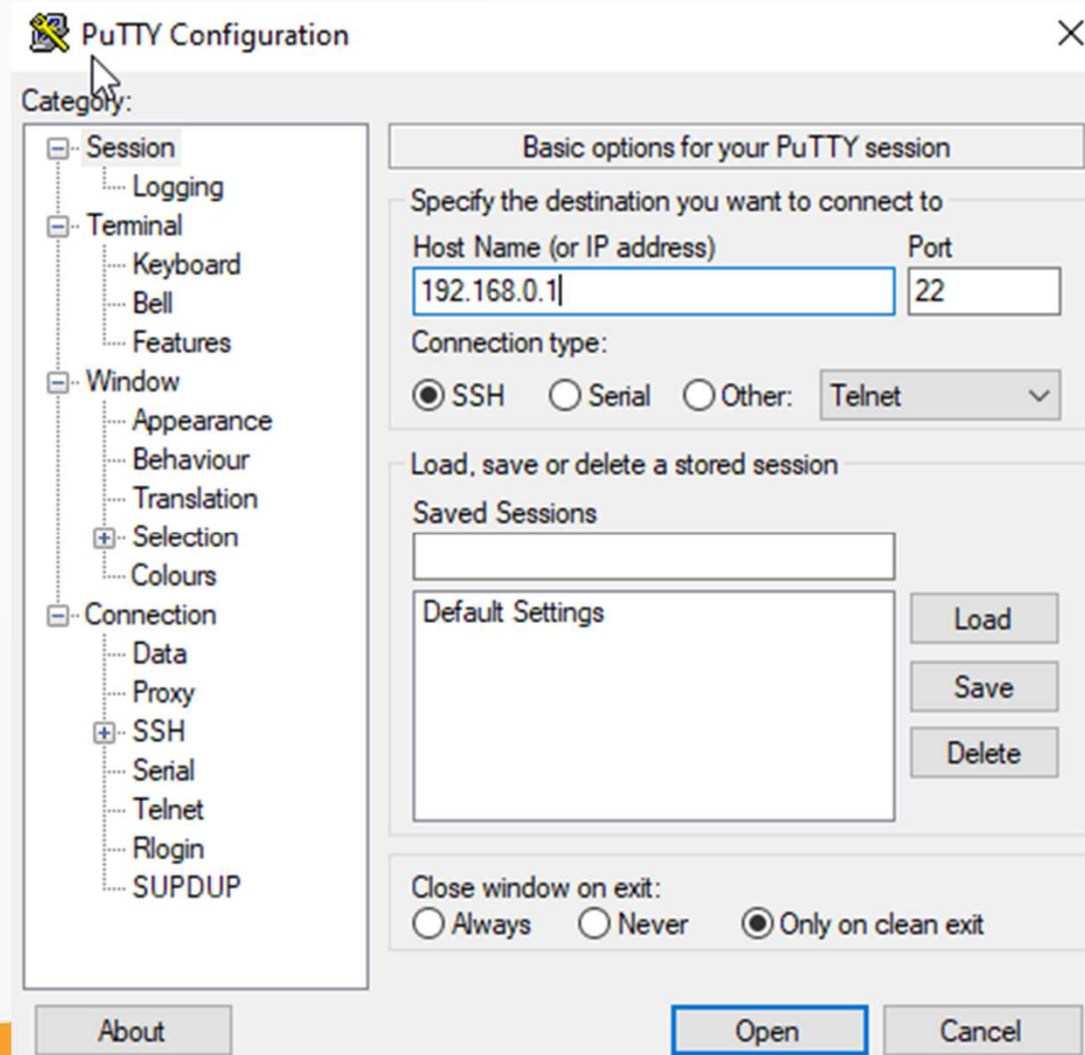
64-bit x86: [putty-64bit-0.79-installer.msi](https://www.putty.org/putty-64bit-0.79-installer.msi)

64-bit Arm: [putty-arm64-0.79-installer.msi](https://www.putty.org/putty-arm64-0.79-installer.msi)

32-bit x86: [putty-0.79-installer.msi](https://www.putty.org/putty-0.79-installer.msi)

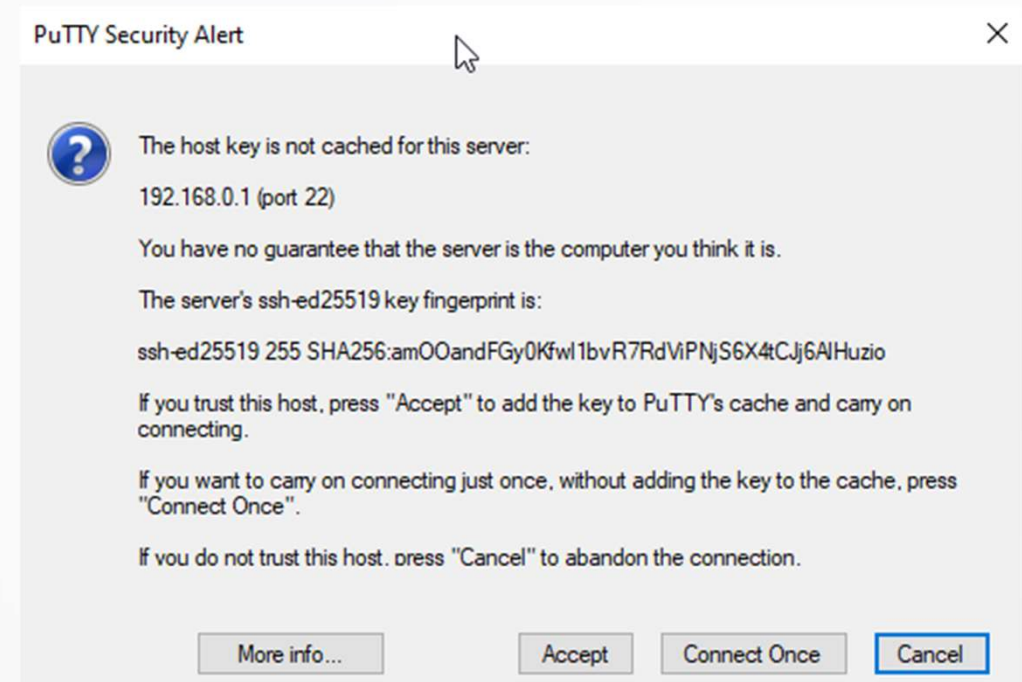
Máquina cliente Windows - Putty

- Acessando o servidor Debian pelo Windows utilizando o Putty.



Máquina cliente Windows - Putty

- Esse alerta de segurança significa a primeira conexão, a pergunta é se confiamos no Servidor SSH.
- Ao clicar em *Accept* é adicionado a chave pública que o servidor enviou.



Máquina cliente Windows - Putty

- Digite o nome do usuário, no caso, root e a senha.



```
192.168.0.1 - PuTTY
login as: root
root@192.168.0.1's password:
Linux debian 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~#
```