



SSH

SSH (Secure Shell, ou Shell Seguro) é um servidor de acesso remoto com implementação nativa de criptografia.

Permite o uso de criptografia assimétrica ou simétrica, sendo que a primeira permite uma forma de identificar o host de acesso, garantindo sua autenticidade.

É uma alternativa muito interessante ao Telnet.

O SSH permite criar túneis criptografados para outros serviços (o mais comum é o X-Windows, mas existem vários outros).

Também permite a transferência de arquivos, podendo ser utilizado como uma alternativa ao FTP, em certas funções.

Porta padrão: 22



SSH – Instalação

No Debian (e na maioria das distribuições), estando o pacote OpenSSH instalado, basta iniciar o serviço sshd:

- `invoke-rc.d sshd start`

Para instalar o servidor:

- `apt-get install openssh-server`

Observação: iniciar o serviço permite a conexão baseado em usuário X senha com criptografia simétrica.

O uso de criptografia assimétrica exige a geração do par de chaves (pública e privada).



SSH – Acesso

- **No Linux:**

Utilize o comando **ssh** (no exemplo abaixo, com criptografia simétrica)

```
ssh usuario@nome_ou_ip_servidor
```

- **No Windows:**

O Windows não possui um programa nativo para acesso ao SSH. Utiliza-se vários aplicativos (alguns deles gratuitos). Uma sugestão é o PUTTY.

- Após o login, o uso é semelhante a estar fisicamente à frente da máquina. A depender do cliente utilizado, pode haver alguma limitação.



SSH – Transferência de Arquivos

- **No Linux:**

Utilize o comando **scp** (no exemplo abaixo, com criptografia simétrica)

```
scp arquivo_origem arquivo_destino
```

sendo que o host acesso é sempre referenciado como `usuario@nome_ou_ip_servidor:/pasta/arquivo`

- **No Windows:**

O Windows não possui um programa nativo para transferência de arquivos via SSH. Utiliza-se vários aplicativos (alguns deles gratuitos). Uma sugestão é o WINSCP2.