Túneis SSH - Explicado com Exemplos

Existem basicamente duas maneiras de criar um túnel SSH, através do redirecionamento de portas locais ou remota (há também o encaminhamento dinâmico, mas não vamos cobrir isso aqui). A melhor maneira de entender estes é através de um exemplo, vamos começar com o encaminhamento de porta local.

Imagine que você está em uma rede privada que não permite conexões a um servidor específico. Vamos dizer que você está no trabalho e **imgur.com** está sendo bloqueado. Para contornar esta situação, podemos criar um túnel através de um servidor que não está na nossa rede e, portanto, pode acessar Imgur.

```
$ ssh -L 9000:imgur.com:80 user@example.com
```

A chave aqui é -L, que diz que estamos fazendo o encaminhamento de porta local. Em seguida, ele diz que estamos encaminhando nossa porta local 9000 para imgur.com:80, que é a porta padrão para HTTP. Agora abra seu navegador e vá para http://localhost:9000 .

A coisa impressionante sobre túneis SSH é que eles são criptografados. Ninguém vai ver o que sites que você está visitando, eles só verão uma conexão SSH para o seu servidor.

Conectando-se a um banco de dados protegido por um firewall

Outro bom exemplo é se você precisar acessar uma porta no seu servidor que só pode ser acessada a partir de localhost e não remotamente.

Um exemplo aqui é quando você precisa se conectar a um console de banco de dados, que só permite a conexão local por razões de segurança. Vamos dizer que você está executando PostgreSQL no seu servidor, que por padrão escuta na porta 5432 .

```
$ ssh -L 9000:localhost:5432 user@example.com
```

A parte que mudou aqui é o localhost:5432 , que diz para encaminhar ligações a partir do seu porta local 9000 para localhost:5432 em seu servidor. Agora podemos simplesmente conectar ao nosso banco de dados.

```
$ psql -h localhost -p 9000
```

Agora vamos parar aqui por um pouco de explicar o que está realmente acontecendo. No primeiro exemplo, o 9000:imgur.com:80 está realmente dizendo redirecione a minha porta local 9000 para imgur.com na porta 80 Você pode imaginar o SSH em seu servidor, na verdade, fazendo uma conexão (um túnel) entre essas duas portas, uma em sua máquina local, e um no destino alvo.

Se no entanto dizer algo como 9000:localhost:5432 , isso significa localhost partir da perspectiva do servidor, não localhost em sua máquina. Isto redirecionar a minha porta 9000 para a porta 5432 no servidor, porque quando você está no servidor,

localhost significa que o próprio servidor.

Isso pode ser um pouco confuso, mas é importante entender o que a sintaxe significa realmente aqui.

Encaminhamento de Porta Remota

Agora vem a segunda parte deste tutorial, que é o encaminhamento de porta remota. Esta é novamente melhor para explicar com um exemplo.

Digamos que você está desenvolvendo uma aplicação Rails em sua máquina local, e você gostaria de mostrá-lo a um amigo. Infelizmente o seu ISP não lhe fornecer um endereço IP público, por isso não é possível conectar-se a sua máquina diretamente através da internet.

Às vezes isso pode ser resolvido através da configuração de NAT (*Network Address Translation*) no seu roteador, mas isso nem sempre funciona, e isso requer que você altere a configuração do roteador, o que nem sempre é desejável. Esta solução também não funciona quando você não tem acesso de administrador da sua rede.

Para corrigir esse problema, é necessário ter um outro computador, que é acessível ao público e ter acesso SSH a ele. Pode ser qualquer servidor na internet, desde que você pode se conectar a ele. Nós vamos dizer SSH para fazer um túnel que se abre uma nova porta no servidor, e conecta-lo a uma porta local em sua máquina.

```
$ ssh -R 9000:localhost:3000 user@example.com
```

A sintaxe aqui é muito semelhante ao encaminhamento de porta local, com uma única mudança de -L para -R . Mas como com o encaminhamento de porta local, a sintaxe é a mesma.

Primeiro você precisa especificar a porta na qual o servidor remoto vai ouvir, que neste caso é 9000, e ao lado segue localhost para a sua máquina local, e a porta local, que neste caso é 3000 .

Há mais uma coisa que você precisa fazer para permitir isso. SSH não por padrão permitir que máquinas remotas para os portos encaminhadas. Para ativar esta aberta /etc/ssh/sshd_config e adicione a seguinte linha em algum lugar no arquivo de configuração. E reinicie o SSH

```
GatewayPorts yes
```

Após isso, você deve ser capaz de se conectar ao servidor remotamente, mesmo a partir de sua máquina local. A maneira como isso iria funcionar é que você deve primeiro criar um túnel SSH que encaminha o tráfego do servidor na porta 9000 para sua máquina local na porta 3000 . Isto significa que se você se conectar ao servidor na porta 9000 da sua máquina local, você vai realmente fazer um pedido para a sua máquina através do túnel SSH.

Algumas Dicas Finais

Você deve ter notado que cada vez que criar um túnel você obtém um shell. Isso geralmente não é necessário, pois você está apenas tentando criar um túnel. Para evitar isso, podemos executar SSH com as *flags* -nNT, como a seguinte, que fará com que o SSH para não atribuir um tty e só fazer o encaminhamento de porta.

```
$ ssh -nNT -L 9000:imgur.com:80 user@example.com
```

SSH tem um grande número de recursos, por isso eu recomendo que você checkout da página manual em man ssh , que contém ainda mais dicas.