# CHECK POINT 04 – 2º SEMESTRE

## Encaminhamento de porta SSH

O encaminhamento de porta SSH, ou tunelamento SSH, é uma técnica de r**ede segura em que dados são trocados entre dispositivos** — como uma máquina local e remota — usando uma conexão SSH.

SSH (Secure Shell) é um protocolo de comunicação de rede que usa criptografia para habilitar conexões remotas e criptografadas de e para dispositivos, permitindo que **dois computadores compartilhem dados e se comuniquem com segurança em redes não seguras.** Ao criptografar dados, o encaminhamento de porta SSH aprimora a segurança transmitida pelo túnel e os **protege de possíveis interceptações ou espionagens.** É um recurso poderoso frequentemente usado por **administradores de sistema, desenvolvedores e usuários que precisam de acesso seguro** a recursos em diferentes redes ou para contornar restrições de rede.

### Existem três tipos de encaminhamento de porta SSH:

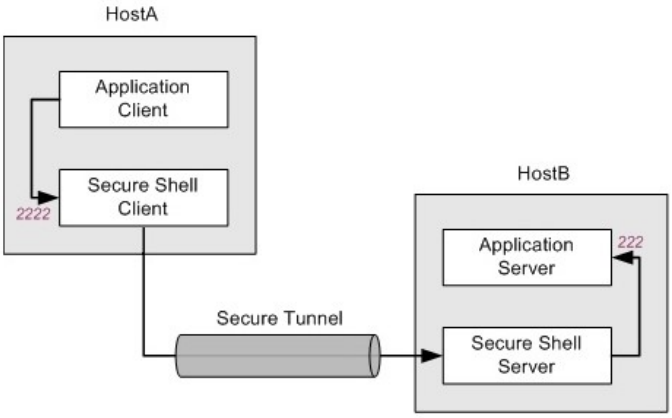
**1. Encaminhamento de porta local (VOCÊ <-- CLIENTE):** redireciona o tráfego de uma porta local na máquina cliente para uma porta especificada em um servidor remoto por meio de uma conexão SSH.

**2. Encaminhamento de porta remota (VOCÊ --> CLIENTE):** redireciona o tráfego de uma porta no servidor remoto para uma porta especificada na máquina cliente.

**3. Encaminhamento de porta dinâmico:** cria um proxy SOCKS na máquina cliente, permitindo o encaminhamento de tráfego de vários aplicativos por meio da conexão SSH.

Exploraremos o **encaminhamento de porta local** neste Check Point. Primeiro, vamos entender como o encaminhamento de porta funciona e como executá-lo.

# Encaminhamento de porta local




Quando um usuário precisa acessar um recurso ou serviço localizado em um servidor remoto, mas não consegue fazê-lo diretamente devido a configurações de firewall, configurações de rede ou limitações de rede privada, o encaminhamento de porta local é utilizado.

Isso envolve usar um SSH para estabelecer um túnel seguro entre uma máquina local (o cliente) e um servidor remoto. Ele permite que os usuários acessem serviços ou recursos no servidor de destino que, de outra forma, seriam inacessíveis devido a configurações de firewall ou limitações de rede.

Para estabelecer o encaminhamento de porta local, o usuário inicia uma conexão SSH com o servidor remoto com a -L opção seguida pelas especificações de encaminhamento. A sintaxe para configurar o encaminhamento de porta local é:

**ssh -L 8080:192.168.1.100:80 user@remote_server**

## Por que o encaminhamento de portas é importante?

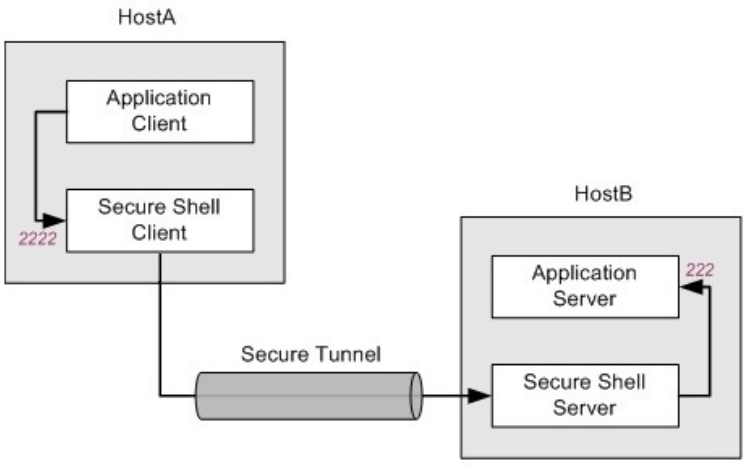
O encaminhamento de porta é crucial quando se trata de rede e obtenção de acesso a recursos dentro de redes privadas . A seguir estão algumas das principais razões para a importância do encaminhamento de porta:

**Acessando serviços de fora da rede local:** O encaminhamento de porta permite que usuários ou dispositivos externos da Internet acessem serviços, aplicativos ou recursos hospedados em dispositivos dentro de uma rede privada.
**Execução de aplicativos especializados:** o encaminhamento de porta garante que os aplicativos possam enviar e receber dados pelas portas necessárias, permitindo que funcionem corretamente.

**Jogos e conexões ponto a ponto:** os jogadores geralmente utilizam o encaminhamento de porta para hospedar servidores de jogos ou participar de jogos multijogador, permitindo conexões de entrada por meio de portas específicas.
**Habilitando gerenciamento e controle remotos:** Facilita o gerenciamento remoto de dispositivos como câmeras, dispositivos IoT ou sistemas de armazenamento conectado à rede (NAS) dentro da rede local.
**Segurança e controle:** permite a abertura seletiva de portas, garantindo que apenas serviços ou aplicativos específicos sejam acessíveis, reduzindo assim o risco de acesso não autorizado.
**Flexibilidade na configuração de rede:** o encaminhamento de porta oferece flexibilidade na configuração de rede, permitindo que os usuários personalizem como o tráfego de entrada é direcionado e quais dispositivos ou serviços podem ser acessados de fora da rede local.

## ATIVIDADE A SER REALIZADA:

Na configuração mostrada abaixo, o cliente do aplicativo e o cliente Secure Shell são executados no HostA. O servidor Secure Shell e o servidor do aplicativo são executados no HostB. Todos os dados enviados para a porta 2222 no HostA são encaminhados para a porta 222 no HostB. Nesse arranjo, todos os dados em trânsito são criptografados com segurança. O comando a seguir (no qual localhost identifica o endereço de loopback no HostB) configura isso:




**ssh -L listening_port:app_host:hostport user@sshserver**

**1. Realize um laboratório onde contenha dois host: cliente e servidor (1 pt)**

**Cliente:**
eth0: 192.168.10.20

**Servidor:**

enp0s3: 192.168.10.10

Servidor apache na porta 80 e 8080 (ou python3);
Servidor ssh 22;

**2. Exibir dois sites a escolha do aluno: (1 pt)**

site A: na porta 80
Site B: na porta 8080

**3. Acesso: (2 pts)**

Cliente acessa o site na porta 80 sem o ssh;
Cliente acesso o site na porta 8080 **após ativar** o encaminhamento de porta local através do ssh na porta 2222.

**4. Prints das seguintes telas: (3 pts)**

1. Configuração das placas de redes do cliente e servidor;
2. Arquivo de configuração do servidor da porta 80,
3. Arquivo de configuração do servidor na porta 8080;
4. Arquivo de configuração e conexão ssh (dica: sshd_config);
5. Comunicação entre as placas de redes;
6. Portas abertas do servidor;
7. Site do servidor acessado através do cliente na porta 80;
8. Site do servidor acessado através do cliente na porta 8080 acessado no localhost.

**5. Pitch de 15 segundos (NO MÁXIMO) gravando as telas do CLIENTE E SERVIDOR funcionando o acesso local do security shell, contendo: (2 pts)**

**1. Sem ativar a porta local do ssh:**
   a. Tela do cliente conectando o site A na porta 80;
   b. Tela do cliente conectando o site B na porta 8080;

**2. Ativando a porta local do ssh:**
   a. Ativação do encaminhamento de porta 8080;
   b. Tela do cliente conectando o site A na porta 80;
   c. Tela do cliente conectando o site B na porta 8080;

**6. Entrega do arquivo compactado (.rar ou .zip) com nome: turma_rm_aluno_sobrenome.pdf contendo os seguintes arquivos: (1 pt)**

a) um arquivo com nome: turma_rm_aluno_nome_sobrenome.pdf
b) um pitch com nome: pitch_turma_rm_aluno_sobrenemo.pdf de 10 segundos gravando a tela do cliente e do servidor;

**EXEMPLO:** 4SIA_1388_JOAO_SILVArar (e dentro do .rar: 4SIA_1388_JOAO_SILVA.pdf e 4SIA_1388_JOAO_SILVA.mov (OU OUTRA EXTENSÃO)

## observação: o Check Point será em dupla