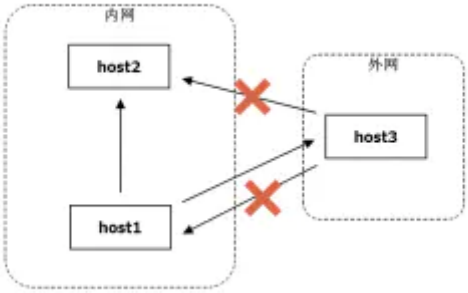
SSH远程端口转发

Author: hxzd55681896



image

假设，host1和host2位于内网，host3位于外网，host1可以连接host3和host2，但host3不能连接host1和host2。我们要做的是，通过位于内网的host1，让host3来连接host2，也就是实现所谓的**“内网穿透”**。

主机密钥生成

公钥具有特定的 ACL 要求，在 Windows 上，这些要求等同于仅允许管理员和 System 进行访问。 首次使用 sshd 时，将自动生成主机的密钥对。

重要

首先需要安装 OpenSSH 服务器。 请参阅 OpenSSH 入门。

默认情况下，sshd 服务设置为手动启动。 若要在每次重新启动服务器时启动它，请从服务器上提升的 PowerShell 提示符运行以下命令：

PowerShell复制

```
# Set the sshd service to be started automatically
Get-Service -Name sshd | Set-Service -StartupType Automatic

# Now start the sshd service
Start-Service sshd
```

由于没有与 sshd 服务关联的用户，因此主机密钥存储在 C:\ProgramData\ssh 下。

用户密钥生成

若要使用基于密钥的身份验证，首先需要为客户端生成公钥/私钥对。 ssh-keygen.exe 用于生成密钥文件，并且可以指定算法 DSA、RSA、ECDSA 或 Ed25519。 如果未指定算法，则使用 RSA。 应使用强算法和密钥长度，例如此示例中的 Ed25519。

若要使用 Ed25519 算法生成密钥文件，请从客户端上的 PowerShell 或 cmd 提示符运行以下命令：

PowerShell复制

```
ssh-keygen -t ed25519
```

这应当会显示以下内容（其中，“username”将替代为你的用户名）：

复制

```
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\username\.ssh\id_ed25519):
```

你可以按 Enter 来接受默认值，或指定要在其中生成密钥的路径和/或文件名。 此时，系统会提示你使用密码来加密你的私钥文件。 这可为空，但不建议这样做。 将密码与密钥文件一起使用来提供双因素身份验证。 在此示例中，我们将密码留空。

复制

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\username\.ssh\id_ed25519.
Your public key has been saved in C:\Users\username\.ssh\id_ed25519.pub.
The key fingerprint is:
SHA256:OIzc1yE7joL2Bzy8!gSOj8eGK7bYaH1FmF3sDuMeSj8 username@server@LOCAL-
HOSTNAME

The key's randomart image is:
+--[ED25519 256]--+
|        .        |
|         o       |
|    . + + .      |
|   o B * = .     |
|   o= B S .      |
|   .=B O o       |
|  + =+% o        |
| *oo.O.E         |
|+.o+=o. .        |
+----[SHA256]-----+
```

现在，指定位置已有一个公共/专用 Ed25519 密钥对。 .pub 文件是公钥，没有扩展名的文件是私钥：

复制

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/3/2021   2:55 PM            464 ed25519
-a----         6/3/2021   2:55 PM            103 ed25519.pub
```

请记住，私钥文件等效于密码，应当采用与保护密码相同的方式来保护它。 为了实现此目的，请使用 ssh-agent 来将私钥安全地存储在与你的 Windows 登录关联的 Windows 安全上下文中。 为执行该操作，请以管理员身份启动 ssh-agent 服务并使用 ssh-add 来存储私钥。

PowerShell复制

```
# By default the ssh-agent service is disabled. Allow it to be manually started
for the next step to work.
# Make sure you're running as an Administrator.
Get-Service ssh-agent | Set-Service -StartupType Manual

# Start the service
Start-Service ssh-agent

# This should return a status of Running
Get-Service ssh-agent

# Now load your key files into ssh-agent
ssh-add ~\.ssh\id_ed25519
```

完成这些步骤后，每当从此客户端进行身份验证需要使用私钥时，ssh-agent 都会自动检索本地私钥，并将其传递到你的 SSH 客户端。

重要

强烈建议你将私钥备份到一个安全位置，将其添加到 ssh-agent，然后将其从本地系统中删除。 如果使用了强算法（例如此示例中的 Ed25519），则无法从代理中检索私钥。 如果你失去了对私钥的访问权限，则必须在你与之交互的所有系统上创建一个新的密钥对并更新公钥。

部署公钥

若要使用上面创建的用户密钥，需要将公钥 (~.ssh\id_ed25519.pub) 的内容放置在服务器上的一个文本文件中，其名称和位置取决于用户帐户是本地管理员组的成员还是标准用户帐户。

管理员用户（有系统管理员级别的用户，一般都是）

公钥 (~.ssh\id_ed25519.pub) 的内容需放置在服务器上的一个名为 `administrators_authorized_keys` 的文本文件中，该文件位于 \。 OpenSSH 客户端包括了 scp 来帮助实现此目的，这是一个安全的文件传输实用工具。 此文件上的 ACL 需要配置为仅允许访问管理员和系统。

以下示例将公钥复制到服务器并配置 ACL（其中“username”替换为你的用户名）。 最初，对于服务器，需要使用用户帐户的密码。

备注

此示例演示了创建 `administrators_authorized_keys file` 的步骤。 如果多次运行，则每次都会覆盖此文件。 若要为多个管理用户添加公钥，需将此文件附加到每个公钥。

PowerShell复制

```
# Make sure that the .ssh directory exists in your server's user account home
folder
ssh user1@domain1@contoso.com mkdir C:\ProgramData\ssh\

# Use scp to copy the public key file generated previously on your client to the
authorized_keys file on your server
scp C:\Users\username\.ssh\id_ed25519.pub
user1@domain1@contoso.com:C:\ProgramData\ssh\administrators_authorized_keys

# Appropriately ACL the authorized_keys file on your server
ssh --% user1@domain1@contoso.com icacls.exe
"C:\ProgramData\ssh\administrators_authorized_keys" /inheritance:r /grant
"Administrators:F" /grant "SYSTEM:F"

-----------------------------------------------------
如果是linux执行命令，注意：路径中的分格符号 \ 要变为  /
上述第三条命令等价于在服务器上执行  icacls.exe
"C:\ProgramData\ssh\administrators_authorized_keys" /inheritance:r /grant
"Administrators:F" /grant "SYSTEM:F"
```

这些步骤完成了对 Windows 上的 OpenSSH 使用基于密钥的身份验证所需的配置。 完成此项后，用户可以从具有私钥的任何客户端连接到 sshd 主机。

启动并配置 OpenSSH 服务器

若要启动并配置 OpenSSH 服务器来开启使用，请以管理员身份打开 PowerShell，然后运行以下命令来启动 `sshd service`：

PowerShell复制

```
# Start the sshd service
Start-Service sshd

# OPTIONAL but recommended:
Set-Service -Name sshd -StartupType 'Automatic'

# Confirm the Firewall rule is configured. It should be created automatically by
setup. Run the following to verify
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction
SilentlyContinue | Select-Object Name, Enabled)) {
    Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not exist, creating
it..."
    New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName 'OpenSSH
Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -
LocalPort 22
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and
exists."
}
```

client

连接到 OpenSSH 服务器

安装后，可从使用 PowerShell 安装了 OpenSSH 客户端的 Windows 10 或 Windows Server 2019 设备连接到 OpenSSH 服务器，如下所示。 请务必以管理员身份运行 PowerShell：

PowerShell复制

```
ssh username@servername
```

连接后，会收到如下所示的消息：

复制

```
The authenticity of host 'servername (10.00.00.001)' can't be established.
ECDSA key fingerprint is SHA256:(<a large string>).
Are you sure you want to continue connecting (yes/no)?
```

选择“是”后，该服务器会添加到包含 Windows 客户端上的已知 SSH 主机的列表中。

系统此时会提示你输入密码。 作为安全预防措施，密码在键入的过程中不会显示。

连接后，你将看到 Windows 命令行界面提示符：

反向代理

```
ssh -R 2222:localhost:22 user3@host3
```

效果

从外网登录到内网32575@DESKTOP-PA8G1ES

```
(base) PS C:\Windows\system32> ssh -p 2222 32575@localhost
The authenticity of host '[localhost]:2222 ([127.0.0.1]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:+iCgxt/qCueJFMnsIaFBPIZHvPQBTgYtMWoE2Or8BUg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ECDSA) to the list of known
hosts.
32575@localhost's password:
Microsoft Windows [版本 10.0.19045.2251]
Microsoft Windows [版本 10.0.19045.2251]
(c) Microsoft Corporation。保留所有权利。

32575@DESKTOP-PA8G1ES C:\Users\32575>
32575@DESKTOP-PA8G1ES C:\Users\32575>wmic
wmic:root\cli>memorychip get capacity
Capacity
17179869184
```

```
17179869184
17179869184
17179869184
```

server

侦听

```
ssh -p 2222 user1@localhost
```

可选

自动重连

autossh与ssh用法类似，只要将ssh命令替换成autossh命令即可，如下所示：

```
autossh -M 2345 -NTR 2222:localhost:22 user3@host3
```

其中，-M参数指定了**autossh监听的端口**，注意这里与其转发的端口要区分开。

另外，-N表示禁止执行远程命令，-T表示禁止分配伪终端，这两个参数结合起来表示SSH连接不允许用户交互执行远程操作，只能用来传数据，从而保证了远程主机的安全。

reference

SSH端口转发实现内网穿透 - 简书 (jianshu.com)

适用于 Windows 的 OpenSSH 密钥管理 | Microsoft Learn