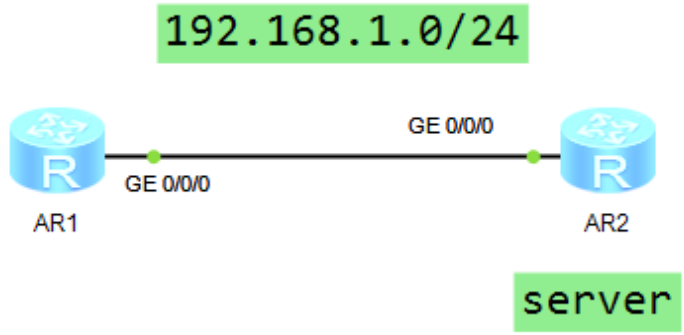
HCIP-Datacom 分解实验 - 网络设备安全

臧家林制作

网络设备安全实验 1： SSH



SSH ： Secure Shell 是一个网络安全协议，基本于 TCP 协议 22 端口传输数据，通过对网络数据的加密，使其能够在一个不安全的网络环境中，提供安全的远程登录和其他安全网络服务。

SSH 协议支持对报文加密传输，而非明文会传送。因此，在跨越互联网的远程登录管理中，建议你使用 SSH 协议，内网使用 telnet 协议。

RSA 公开密钥密码体制。所谓的公开密钥密码体制就是使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

配置 SSH 服务端

开启 SSH 服务器功能 ，
SSH 用户使用 password 方式验证，需要在 SSH 服务器端生成本 RSA 密钥

R2：
stelnet server enable

rsa local-key-pair create

配置完成后，可以查看本地密钥对中的公钥部分信息

```
[R2]dis rsa local-key-pair public

=============================================
==========
Time of Key pair created: 2020-09-20
09:07:15-08:00
Key name: Host
Key type: RSA encryption Key
=============================================
==========
Key code:
3047
  0240
        C5CFF6E8 A978C3AF 241196F2 DFD7482D
618F91DD
        AECD8FA9 5092125B FB3CDF3B D0028106
```

1BE63C0C
        227D8091 D0DEAF00 3B519495 DB52D9AC
2219F409
        7F9B1CCD

配置 VTY 用户界面，AAA 授权验证方式 ，设置只支持 SSH 协议，设备自动禁止 telnet

user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
aaa
local-user huawei password cipher huawei
local-user huawei service-type ssh
local-user huawei privilege level 3
q

新建 SSH 用户，指定认证方式为 password
ssh user huawei authentication-type password

配置完成后，查看服务器配置和用户配置
[R2]dis ssh user-information

```
------------------------------------------------------------------
 Username                    Auth-type
User-public-key-name
------------------------------------------------------------------
 huawei                        password
null
```

```
-----------------------------------------
--------------------

[R2]dis ssh server status
 SSH version
:1.99
 SSH connection timeout
:60 seconds
 SSH server key generating interval    :0
hours
 SSH Authentication retries
:3 times
 SFTP Server
:Disable
 Stelnet server
:Enable
```

配置 SSH 客户端

客户端需要开启 SSH 首次认证功能

R1：

ssh client first-time enable

stelnet 192.168.1.2

```
[R1]stelnet 192.168.1.2
Please input the username:huawei
Trying 192.168.1.2 ...
Press CTRL+K to abort
Connected to 192.168.1.2 ...
The server is not authenticated. Continue
to access it? (y/n)[n]:y
```

```
Save the server's public key? (y/n)[n]:y
The server's public key will be saved with
the name 192.168.1.2. Please wait...

Enter password:
<R2>sy
```

第一次登录需要对 RSA 进行检查，第二次登录就简单

```
[R1]stelnet 192.168.1.2
Please input the username:huawei
Trying 192.168.1.2 ...
Press CTRL+K to abort
Connected to 192.168.1.2 ...
Enter password:
------------------------------------------
-------
    User last login information:
------------------------------------------
-------
    Access Type: SSH
    IP-Address : 192.168.1.1 ssh
```

查看 SSH 服务器端的当前会话连接信息

```
[R2]dis ssh server session

------------------------------------------
------------------------
 Conn      Ver      Encry          State
Auth-type                Username
```

```
-----------------------------------------------------------------------
 VTY 0    2.0      AES                 run
password                    huawei

-----------------------------------------------------------------------
```