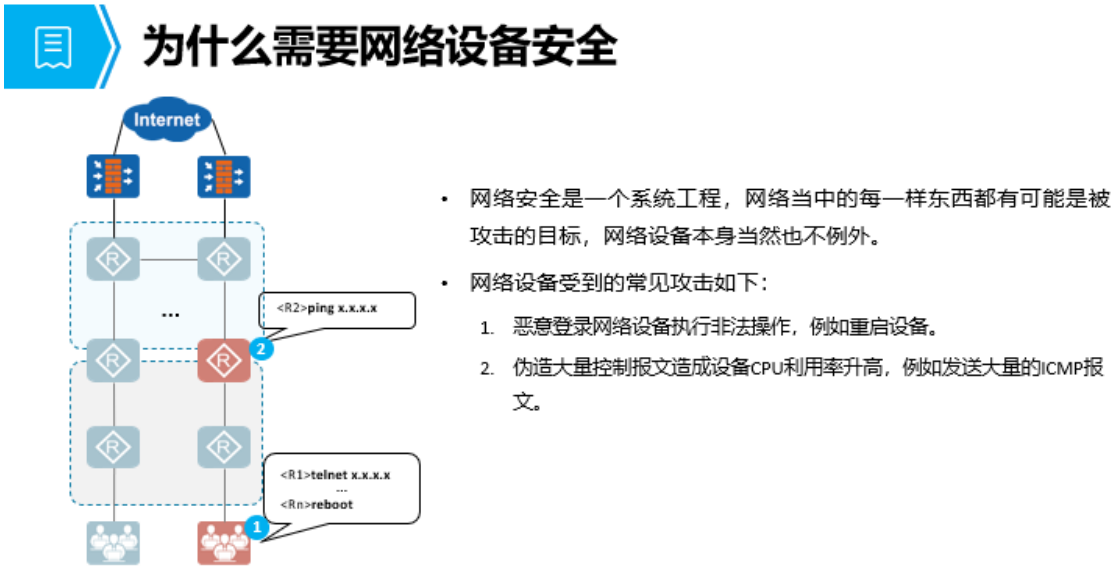
网络设备安全特性

- 由于 IP 网络规模庞大，导致网络设备数量众多、通信协议层出不穷。同时，IP 网络的管理也变得极其复杂，安全性和业务灵活性以及安全性和管理维护便利性之间存在着矛盾。不同技术能力、管理水平的管理人员，对这些矛盾的处理能力也参差不齐。管理员往往追求业务可用性，而忽略了安全防御能力，导致必要的安全措施没有得到妥善的配置，设备本身的安全能力无法发挥。
- 本课程主要介绍常见的网络设备安全加固策略，对一些常见的安全配置进行了举例说明。



常见设备安全加固策略

常见的设备安全加固策略主要可以从以下方面部署：

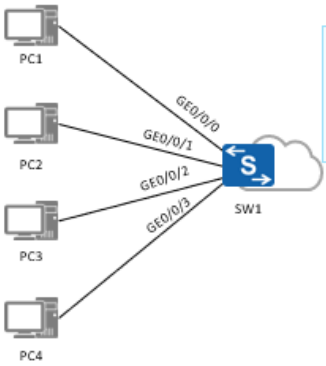
- 关闭不使用的业务和协议端口
- 废弃不安全的访问通道
- 基于可信路径的访问控制
- 本机防攻击

端口关闭 访问通道 URPF 本机防攻击

关闭不使用的业务和协议端口

在分析业务需求的基础上，按照最小授权原则，关闭不使用的业务和协议端口。

- 不使用的物理端口，应该默认配置为关闭，即使插上网线也不能通信
- 不使用的协议端口，应该默认配置为关闭，不对外提供访问。如常见的telnet、FTP、HTTP等端口。




```
<SW1> system-view
[SW1] undo ftp server
Warning: The operation will stop the FTP server. Do you want to continue? [Y/N]:y
Info: Succeeded in closing the FTP server.
[SW1]port-group protgroup1
[SW1-port-group-protgroup1]group-member GigabitEthernet 0/0/4 to GigabitEthernet0/0/48
[SW1-port-group-protgroup1]shutdown
```

在SW1上关闭FTP功能，同时关闭多个不使用的端口。

端口关闭 访问通道 URPF 本机防攻击

废弃不安全的访问通道

在业务需求分析的基础上，优先满足业务的访问需求。在同一个访问需求有多种访问通道服务的情况下，废弃不安全的访问通道，而选择安全的访问通道。

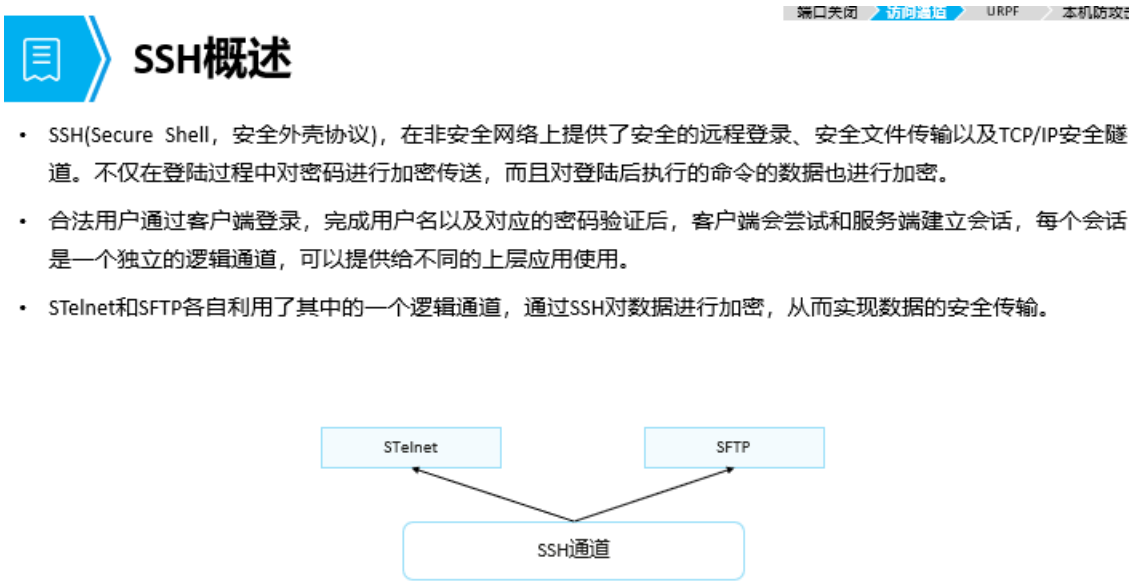
访问需求	不安全的通道	安全的通道
远程登录	Telnet	SSH v2
文件传输	FTP，TFTP	SFTP
网元管理	SNMP v1/v2	SNMP v3
网管登录	HTTP	HTTPS

- 通过命令行、WEB、网管等方式登录设备时，建议采用安全加密的通道 SSH、HTTPS、SNMPv3。
- 设备之间，以及设备和终端之间数据传输，也建议采用加密的数据传输协议 SFTP。

安全的数据访问通道

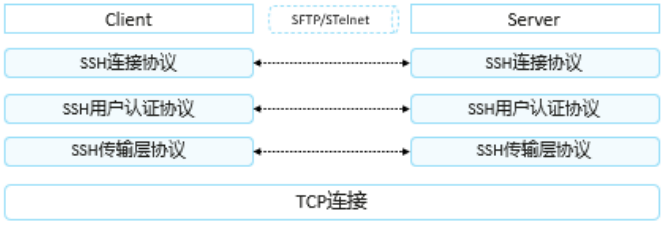
- 为保证设备安全，尽量选择安全的访问通道。
- 设备数据传输安全常见场景及采用协议：

- 用户远程登录：
- Telnet：采用 TCP 协议进行明文传输。
- STelnet：基于 SSH 协议，提供安全的信息保障和强大的认证功能。
- 设备文件操作：
- FTP：支持文件传输以及文件目录的操作，具有授权和认证功能，明文传输数据。
- TFTP：只支持文件传输，不支持授权和认证，明文传输数据。
- SFTP：支持文件传输及文件目录的操作，数据进行了严格加密和完整性保护。



- SSH 协议由 IETF 制订，最新版本是 V2.0，1.3 和 1.5 版本存在安全隐患，已经逐步被淘汰。
- SSH 支持服务端和客户端的双向认证，提供保密性和完整性等安全服务。

SSH协议结构



SSH协议框架中最主要的部分是三个协议：传输层协议、用户认证协议和连接协议。

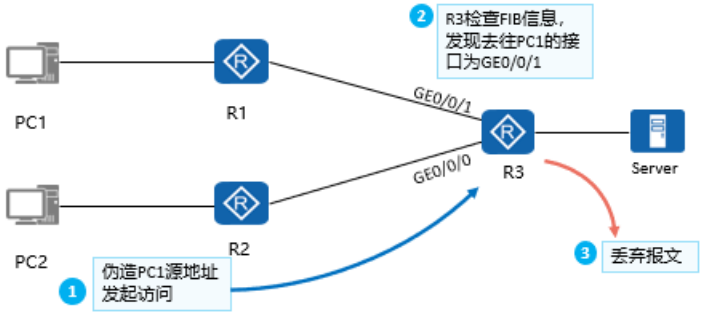
- 传输层协议：提供版本协商，加密算法协商，密钥交换，服务端认证以及信息完整性支持。
- 用户认证协议：为服务器提供客户端的身份鉴别。
- 连接协议：将加密的信息隧道复用为多个逻辑通道，提供给高层的应用协议（STelnet、SFTP）使用；各种高层应用协议可以相对地独立于SSH基本体系之外，并依靠这个基本框架，通过连接协议使用SSH的安全机制。

- SSH 中用到的算法主要有几类：
- 用于数据完整性保护的 MAC 算法，如 hmac-md5、hmac-md5-96 等；
- 用于数据信息加密的算法，如 3des-cbc、aes128-cbc、des-cbc 等；
- 用于产生会话密钥的密钥交换算法，如 diffle-hellman-group-exchange-sha1 等；
- 用于进行数字签名和认证的主机公钥算法，如 RSA、DSA 等；
- RSA（Rivest-Shamir-Adleman）加密算法，一种非对称加密算法。RSA 是 1977 年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。RSA 就是他们三人姓氏开头字母拼在一起组成的。
- DES（Data Encryption Standard）数据加密标准。DES 使用一个 56 比特的密钥。
- 3DES（Triple Data Encryption Standard），是 DES 的一个更安全的变形。它使用 3 条 56 位的密钥对数据进行三次加密。
- DSA（Digital Signature Algorithm）数字签名算法。

- 对称密钥技术：
- 对称密钥加密又叫专用密钥加密，即发送和接收数据的双方必使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括：DES、3DES 等。
- 公开密钥技术：
- 公钥加密算法也称非对称密钥算法，用两对密钥：一个公共密钥和一个专用密钥。用户要保障专用密钥的安全；公共密钥则可以发布出去。公共密钥与专用密钥是有紧密关系的，用公共密钥加密的信息只能用专用密钥解密，反之亦然。由于公钥算法不需要联机密钥服务器，密钥分配协议简单，所以极大简化了密钥管理。除加密功能外，公钥系统还可以提供数字签名。
- 机密性（Confidentiality）：指信息在存储、传输、使用的过程中，不会被泄漏给非授权用户或实体；
- 完整性（Integrity）：指信息在存储、传输、使用的过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；
- 可用性（Availability）：指确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源。

基于可信路径的访问控制

- 可以在设备上部署基于可信路径的访问控制策略，以提升网络的安全性。
- 部署URPF，可以判定某个报文的源地址是否合法，如果该报文的路径与URPF学习的路径不符，丢弃该报文，用URPF可以有效防范IP地址欺骗。



- IP 网络的开放性决定了，只要路由可达，任何人都可以对目标主机进行访问或者攻击。
- 对于某一个主机而言，访问它的客户端的报文历经的路径通常是固定的，尤其是在网络边缘，这种路径的固定特性表现得更加明显。
- URPF（Unicast Reverse Path Forwarding，单播逆向路径转发）分为严格模式和松散模式以及允许匹配缺省路由的方式。其原理是当设备转发 IP 报文时，检查数据报文的源 IP 地址是否合法，检查的原理是根据数据包的源 IP 地址查路由表。
- 对于严格模式：如果报文能匹配明细路由，并且入接口跟匹配路由的出接口一致，则允许报文上送，否则丢弃报文。
- 对于松散模式：如果报文匹配上明细路由，则运行报文上送，否则丢弃报文，不检查接口是否匹配。默认情况下，会认为缺省路由不存在，不会去匹配缺省路由，只有进行了配置时候，才会去匹配缺省路由的。
- 对允许匹配缺省路由的模式，必须和严格模式一起配置，报文匹配明细路由或者缺省路由，并且报文入接口跟匹配路由的出接口一致才上送，否则丢弃。不支持缺省路由与松散模式一起配置，因为这样无法达到防攻击的效果。松散模式和严格

模式互斥，只能配置一种模式。

本机防攻击

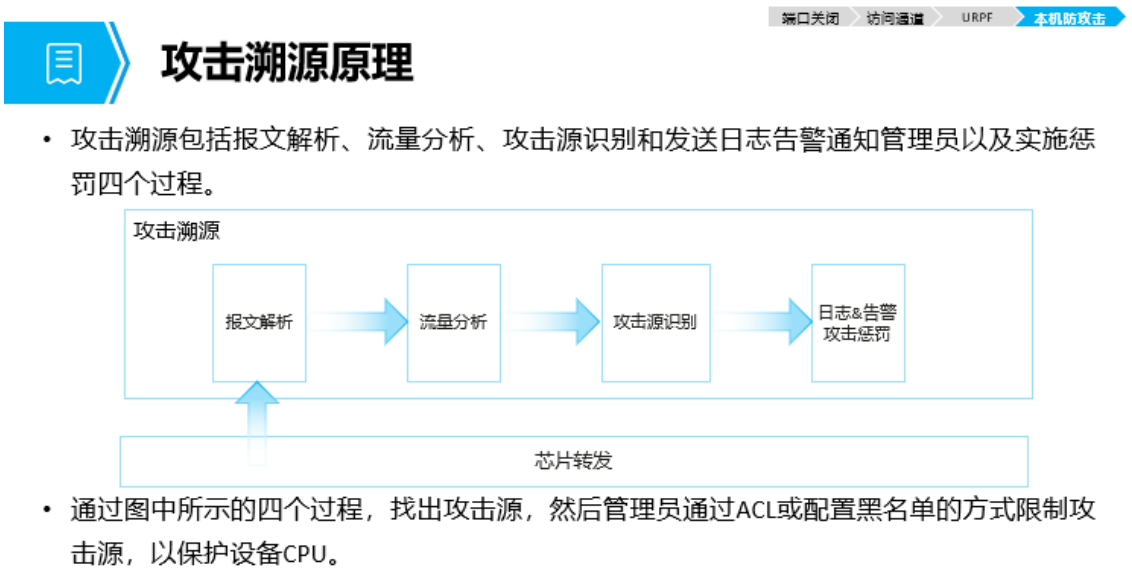
- 在网络中，存在着大量针对 CPU 的恶意攻击报文以及需要正常上送 CPU 的各类报文。针对 CPU 的恶意攻击报文会导致 CPU 长时间繁忙的处理攻击报文，从而引发其他业务的断续甚至系统的中断；大量正常的报文也会导致 CPU 占用率过高，性能下降，从而影响正常的业务。
- 为了保护 CPU，保证 CPU 对正常业务的处理和响应，设备提供了本机防攻击功能。本机防攻击针对的是上送 CPU 的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。
- 本机防攻击包括 CPU 防攻击和攻击溯源两部分。
- CPU 防攻击针对上送 CPU 的报文进行限制和约束，使单位时间内上送 CPU 报文的数量限制在一定的范围之内，从而保护 CPU 的安全，保证 CPU 对业务的正常处理。
- 攻击溯源针对 DoS（Denial of Service，拒绝服务）攻击进行防御。设备通过对上送 CPU 的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再对这些攻击报文根据报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。

CPU 防攻击

- 多级安全机制，保证设备的安全，实现了对设备的分级保护。设备通过以下策略实现对设备的分级保护：
- 第一级：通过黑名单来过滤上送 CPU 的非法报文。
- 第二级：CPCAR（Control Plane Committed Access Ra

te）。对上送 CPU 的报文按照协议类型进行速率限制，保证每种协议上送 CPU 的报文不会过多。

- 第三级：对上送 CPU 的报文，按照协议优先级进行调度，保证优先级高的协议先得到处理。
- 第四级：对上送 CPU 的报文统一限速，对超过统一限速值的报文随机丢弃，保证整体上送 CPU 的报文不会过多，保护 CPU 安全。
- 动态链路保护功能的 CPU 报文限速，是指当设备检测到 SSH Session 数据、Telnet Session 数据、HTTP Session 数据、FTP Session 数据以及 BGP Session 数据建立时，会启动对此 Session 的动态链路保护功能，后续上送报文如匹配此 Session 特征信息，此类数据将会享受高速率上送的权利，由此保证了此 Session 相关业务的运行可靠性、稳定性。



SSH基本配置 (1)

1. 使能设备的SSH服务器功能。

```
[Huawei] stelnet server enable
```

2. 配置SSH用户的认证方式。

```
[Huawei] ssh user user-name authentication-type { password | rsa | password-rsa | all }
```

当用户使用RSA认证方式时，需要在SSH服务器上输入SSH客户端生成的密钥中的公钥部分。这样当客户端登录服务器时，自己的私钥如果与输入的公钥匹配成功，则认证通过。

3. 配置SSH服务器基于SSH客户端生成的密钥中的公钥部分。

```
[Huawei] rsa peer-public-key key-name [ encoding-type { der | openssh | pem } ]
[Huawei-rsa-public-key] public-key-code begin
```

输入的公钥必须是按公钥格式编码的十六进制字符串，由支持SSH客户端生成。

4. 退出公共密钥编辑视图；退出公共密钥视图，回到系统视图。

```
[Huawei-rsa-key-code] public-key-code end
[Huawei-rsa-public-key] peer-public-key end
```

SSH基本配置 (2)

1. 为SSH用户分配RSA公钥。

```
[Huawei] ssh user user-name assign { rsa-key | ecc-key } key-name
```

2. 生成本地RSA主机密钥对和服务器密钥对。

```
[Huawei] rsa local-key-pair create
```

如果RSA密钥已经存在，则系统将提示用户确认是否替换原有密钥；执行此命令后，会提示您输入主机密钥的位数。服务器密钥对的位数与主机密钥对的位数至少相差128位。服务器密钥对和主机密钥对的最小长度为512位，最大长度为2048位，缺省长度为2048位。

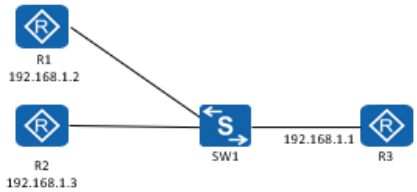
3. 使能SSH客户端首次认证功能。

```
[Huawei] ssh client first-time enable
```

当SSH客户端首次访问SSH服务器，而SSH客户端没有配置SSH服务器端的公钥时，用户可以选择使能SSH客户端首次认证继续访问该SSH服务器，并在SSH客户端保存该主机公钥；当SSH客户端下次访问该SSH服务器时，就以保存的主机公钥来认证该SSH服务器。

SSH配置示例

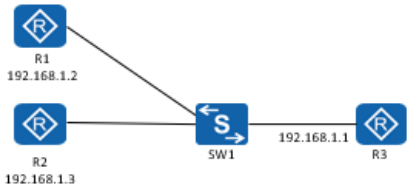
- 用户希望安全的远程登录设备，因此配置STelnet方式进行远程的安全登录。
- 在R3上配置两个登录用户client001和client002，R1使用client001通过password认证方式登录R3，R2使用client002通过RSA认证方式登录R3。配置安全策略，保证只有R1和R2才能登录设备。



配置步骤：

1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

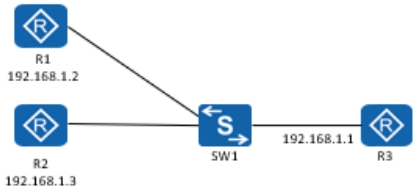
SSH配置命令 (1)



1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

```
[R3] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist. Confirm to replace them? (y/n):y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating
keys... .....+++ ....+++ .....
.....++++++++ .....++++++++
```

SSH配置命令 (2)



1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

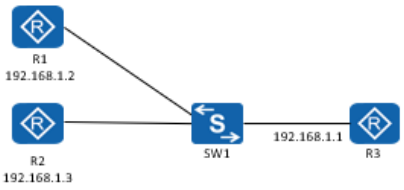
```
[R3] user-interface vty 0 4
[R3-ui-vty0-4] authentication-mode aaa
[R3-ui-vty0-4] protocol inbound ssh
[R3-ui-vty0-4] quit
[R3] aaa
[R3-aaa] local-user client001 password irreversible-cipher Huawei@123
[R3-aaa] local-user client001 privilege level 3
[R3-aaa] local-user client002 password irreversible-cipher Huawei@123
[R3-aaa] local-user client002 privilege level 3
[R3-aaa] quit
[R3] ssh user client001 authentication-type password
[R3] ssh user client002 authentication-type rsa
```

```
[R3] stelnet server enable
```

```
[R3] aaa
[R3-aaa] local-user client001 service-type ssh
[R3-aaa] local-user client002 service-type ssh
[R3-aaa] quit
```

```
[R3] ssh server port 1025
```

SSH配置命令 (3)

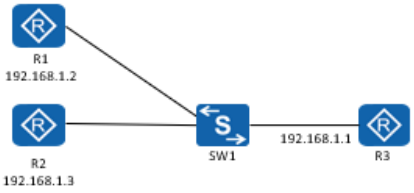


1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

```
# 在R2生成客户端的本地密钥对。
[R2] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n):y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys... ..........................................................................
+++ ....+++ ..........................++++++++ ..............++++++++
```

- 本页及后续两页是为了实现用户 client002 登录 R3。

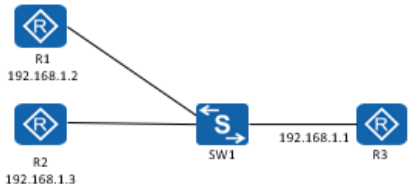
SSH配置命令 (4)



1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

```
# 查看R2生成的RSA密钥对的公钥部分。
[R2] display rsa local-key-pair public
Key code: 30820109 02820100 CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B
A3A48594 69517096 35626F55 E4FAF0EB FDA2B9E9 5E417B2B E09F38B0 D26FCA73
FE2E3FC4 DFBEC8CF 4ED0C909 E8D975E6 FFC73C81 D13FE71E 759DC805 B0F0E877
4FC9288E BE1E197C 2A7186B0 B56F5573 3A5EA588 29C63E3B 20D56233 8E63278D
F941734F 6B359C69 BBAE5A52 EB842179 04B4204D 5DB31D72 97F0C085 DA771F66
0AAADC28 D264CEB9 5BADA92C CDE9F116 D6D99C48 CEBA3A1D 868B053A
32941D85 CCAA9796 A4B55760 0A8108ED DB45DA12 F61634C9 59431600 341FEDEF
5379D565 A8D1953D DEA018A2 72F99FFC 63DE04BF 2A6219BD DF13D705
27D63DEF 83D556BC 5B44D983 8D5EA126 C1EB71CB 0203 010001
 ============================================================
Time of Key pair created: 2012-08-06 17:17:44+00:00 Key name: Server Key type: RSA
encryption Key ============================================================
Key code: 3067 0260 DF8AFF3C 28213B94 2292852E E98657EE 11DE5AF4 8A176878
CDD4BD31 55E05735 3080F367 A83A9034 47D534CA 81250C1D 35401DC3 464E9E5F
A50202CF A7AD09CD AC3F531C A763F0A0 4C8E51B9 18755400 76AF4A78 225C92C3
01FE0DFF 06908363 0203 010001
```

SSH配置命令 (5)

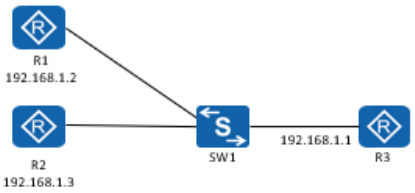


1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

将R2上产生的RSA公钥配置到服务器端（上页display命令显示信息中黑体部分即为客户端产生的RSA公钥，将其拷贝粘贴至服务器端）。
[R3] **rsa peer-public-key rsakey001**
[R3-rsa-public-key] **public-key-code begin**
[R3-rsa-key-code] **30820109**
[R3-rsa-key-code] **02820100**
[R3-rsa-key-code] **CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B**
[R3-rsa-key-code] ……
[R3-rsa-key-code] **010001**
[R3-rsa-key-code] **public-key-code end**
[R3-rsa-public-key] **peer-public-key end**

在R3上为SSH用户client002绑定STelnet客户端的RSA公钥。
[R3] **ssh user client002 assign rsa-key rsakey001**

SSH配置验证



1. 在R3生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在R3配置SSH用户client001和client002。
3. 在R3开启STelnet服务功能。
4. 在R3配置SSH用户client001和client002的服务方式为STelnet。
5. 在R3配置SSH服务器的端口号，有效防止攻击者对SSH服务标准端口的访问，确保安全性。
6. 用户client001和client002分别以STelnet方式实现登录R3。

[R1] **ssh client first-time enable**
[R1] **stelnet 192.168.1.1 1025**
Please input the username:**client001**
Trying 192.168.1.1 …
Press CTRL+K to abort
Connected to 192.168.1.1 …
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 192.168.1.1. Please wait… Enter password:
<R3> # 显示登录成功

[R2] **ssh client first-time enable**
[R2] **stelnet 192.168.1.1 1025**
Please input the username:**client002**
Trying 192.168.1.1 … Press CTRL+K to abort Connected to 192.168.1.1 …
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 192.168.1.1. Please wait…
<R3> # 显示登录成功

本机防攻击基本配置 (1)

1. 创建防攻击策略并进入防攻击策略视图。

   [Huawei] **cpu-defend policy** *policy-name*

2. 配置黑名单。

   [Huawei-cpu-defend-policy-test] **blacklist** *blacklist-id* **acl** *acl-number*

   如果某个防攻击策略要配置多个黑名单，该防攻击策略的黑名单群中不允许出现二层ACL和基本ACL、二层ACL和高级ACL以及三种ACL同时使用的情况。

3. 配置上送CPU报文的限制速率。

   [Huawei-cpu-defend-policy-test] **packet-type** *packet-type* **rate-limit** *rate-value*

   如果设备收到某种协议类型的攻击报文或大量上送CPU的正常报文，可以在防攻击策略中对该协议类型的报文进行限速，使该协议类型的报文限制在一个较小的速率范围内，减少对CPU处理正常业务的影响。

4. 配置上送CPU报文中指定协议类型报文的优先级。

   [Huawei-cpu-defend-policy-test] **packet-type** *packet-type* **priority** *priority-level*

本机防攻击基本配置 (2)

1. 使能动态链路保护功能。

   [Huawei-cpu-defend-policy-test] **cpu-defend application-apperceive** [**ssh** | **telnet** | **bgp** | **ftp** | **http**] **enable**

   缺省情况下，对于SSH协议、Telnet协议、SSHv6协议、Telnetv6协议、FTP协议、BGP协议和HTTP协议，已使能动态链路保护功能。

2. 使能攻击溯源功能。

   [Huawei-cpu-defend-policy-test] **auto-defend enable**

3. 配置攻击溯源检查阈值。

   [Huawei-cpu-defend-policy-test] **auto-defend threshold** *threshold*

4. 使能攻击溯源事件上报功能。

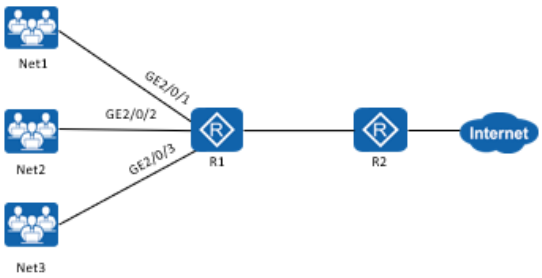
   [Huawei-cpu-defend-policy-test] **auto-defend alarm enable**

5. 应用防攻击策略。

   [Huawei] **cpu-defend-policy** *policy-name* [**global** | **slot** *slot-id*]

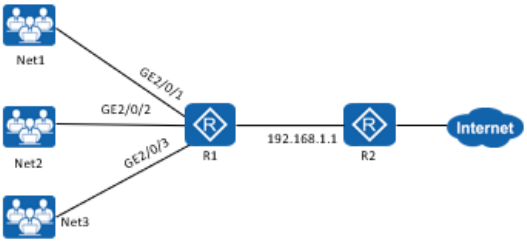
- 缺省情况下，SSH 报文、Telnet 报文、SSHv6 报文、Telnetv6 报文、HTTP 报文、BGP 报文的动态链路保护功能的限制速率是 512pps，FTP 报文的动态链路保护功能的限制速率是 1024pps。

本机防攻击配置示例



- 如图所示，位于不同局域网的用户通过R1访问Internet。为分析R1受攻击情况，需要配置攻击溯源检查功能记录攻击源信息。管理员发现存在以下现象：
  - 通过攻击溯源检查功能分析可知，Net1中的某个用户经常会发生攻击行为。
  - R1收到大量的ARP Request报文，影响CPU的正常工作。
  - R1无法提供FTP服务。
  - 局域网用户通过DHCP方式动态获取IP地址，但R1未优先处理上送CPU的DHCP报文。
  - R1收到大量的Telnet报文。
- 管理员希望通过在R1进行配置，以便解决上述问题。

本机防攻击配置命令 (1)



1. **配置黑名单，将Net1网段中的攻击者（0001-c0a8-0102）列入黑名单，阻止其接入网络。**
2. 配置ARP Request报文上送CPU的速率限制，使ARP Request报文限制在一个较小的速率范围内，减少对CPU处理正常业务的影响。
3. 配置FTP协议的动态链路保护功能，保证R1正常提供FTP功能。
4. 配置协议优先级，对DHCP Client报文设置较高的优先级，保证R1优先处理上送CPU的DHCP Client报文。
5. 关闭R1的Telnet服务器功能，使R1丢弃收到的Telnet报文。

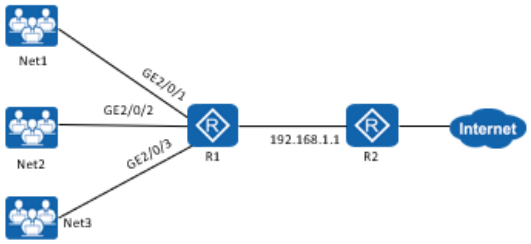
```
# 配置黑名单使用的ACL。
[R1] acl number 4001
[R1-acl-L2-4001] rule 5 permit source-mac 0001-c0a8-0102
[R1-acl-L2-4001] quit
```

```
# 创建防攻击策略。
[R1] cpu-defend policy devicesafety
```

```
# 配置攻击溯源检查功能。
[R1-cpu-defend-policy-devicesafety] auto-defend enable
[R1-cpu-defend-policy-devicesafety] auto-defend threshold 50
```

```
# 配置黑名单。
[R1-cpu-defend-policy-devicesafety] blacklist 1 acl 4001
```

本机防攻击配置命令 (2)



1. 配置黑名单，将Net1网段中的攻击者（0001-c0a8-0102）列入黑名单，阻止其接入网络。
2. 配置ARP Request报文上送CPU的速率限制，使ARP Request报文限制在一个较小的速率范围内，减少对CPU处理正常业务的影响。
3. 配置FTP协议的动态链路保护功能，保证R1正常提供FTP功能。
4. 配置协议优先级，对DHCP Client报文设置较高的优先级，保证R1优先处理上送CPU的DHCP Client报文。
5. 关闭R1的Telnet服务器功能，使R1丢弃收到的Telnet报文。

```
# 配置ARP Request报文上送CPU的速率限制。
[R1-cpu-defend-policy-devicesafety] packet-type arp-request rate-limit 64
```

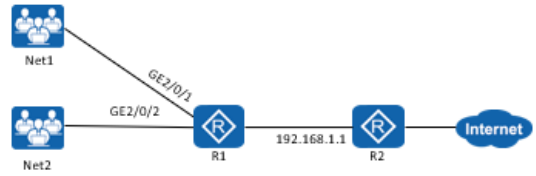
```
# 配置FTP协议动态链路保护功能的速率限制值。
[R1-cpu-defend-policy-devicesafety] application-apperceive packet-type ftp rate-limit 2000
# 使能FTP协议动态链路保护功能。
[R1] cpu-defend application-apperceive ftp enable
```

```
# 应用防攻击策略。
[R1] cpu-defend-policy devicesafety
```

```
# 关闭telnet server功能。
[R1] undo telnet server enable
```

- 应用层联动不需要使能，只要关闭 Router 的 Telnet 服务器功能，Router 会丢弃收到的 Telnet 报文。

本机防攻击配置验证




```
# 查看上送到主控板的报文的统计信息，丢弃的报文表明设备对arp-request进行了速率限制。
<R1> display cpu-defend statistics
```

Packet Type	Pass Packets	Drop Packets
8021X	0	0
arp-miss	5	0
arp-reply	8090	0
arp-request	1446576	127773
bfd	0	0
bgp	0	0
bgp4plus	0	0
dhcp-client	879	0
dhcp-server	0	0

```
# 查看配置的防攻击策略的信息。
[R1] display cpu-defend policy devicesafety
Related slot   : <0>
.....
Slot<0>        : Success
Configuration :
        Blacklist 1 ACL number                : 4001
        Packet-type arp-request rate-limit    : 64(pps)
        Packet-type dhcp-client priority      : 3
        Rate-limit all-packets                : 2000(pps)(default)
        Application-apperceive packet-type ftp  : 2000(pps)
        Application-apperceive packet-type tftp : 2000(pps)
```

思考题：

- （判断题）当远程登录设备时，采用 Stelnet 的方式比 Telnet 的方式更加安全，因为 Stelnet 的方式登录采用 TCP 封装，而 Telnet 的方式登录设备采用 UDP 封装。
- （判断题）本机防攻击包括 CPU 防攻击和攻击溯源两部分。

答案：

- 错
- 对
-