网络设备安全特性

一、为什么需要网络设备安全

1、随着IP网络的不断发展，运行的协议越来越多，传输的数据越来越丰富，网络安全是一个系统工程，网络当中的每一样东西都有可能是被攻击的目标

2、在保障网络可用性与管理性的同时，往往忽略掉网络设备自身的安全性

3、因此需要在没有防火墙的保护下，提高网络设备自身的安全性，抗打击性

4、网络设备受到的常见攻击如下：

4.1、恶意登录网络设备执行非法操作，例如重启设备

4.2、伪造大量控制报文造成设备CPU利用率升高，如：发送大量的ICMP报文

二、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：

1、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

1.1、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

1.2、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
```

2、废弃不安全的访问通道【例如：Telnet（TCP的23号端口）使用明文的方式发送数据，易被网络攻击者截获】

2.1、在业务需求分析的基础上，优先满足业务的访问需求

2.2、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

2.3、通过命令行（CLI）、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

2.4、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

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

2.5、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：

2.5.1、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

2.5.2、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

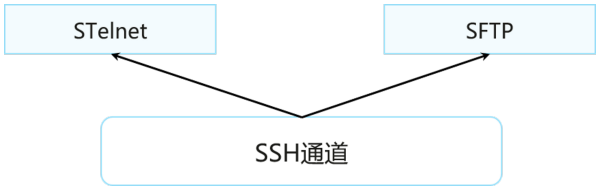
SFTP：支持文件传输及文件目录的操作，数据进行了严格加密和完整性保护

2.6、SSH概述

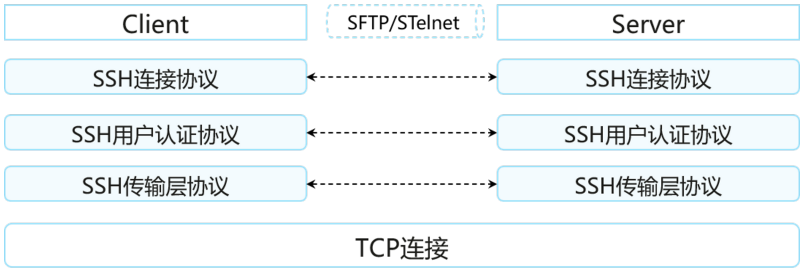
2.6.1、SSH【Secure Shell | 安全外壳协议】，在非安全网络上提供了安全的远程登录、安全文件传输以及TCP/IP安全隧道。不仅在登陆过程中对密码进行加密传送，而且对登陆后执行的命令的数据也进行加密

2.6.2、合法用户通过客户端登录，完成用户名以及对应的密码验证后，客户端会尝试和服务端建立会话，每个会话是一个独立的逻辑通道，可以

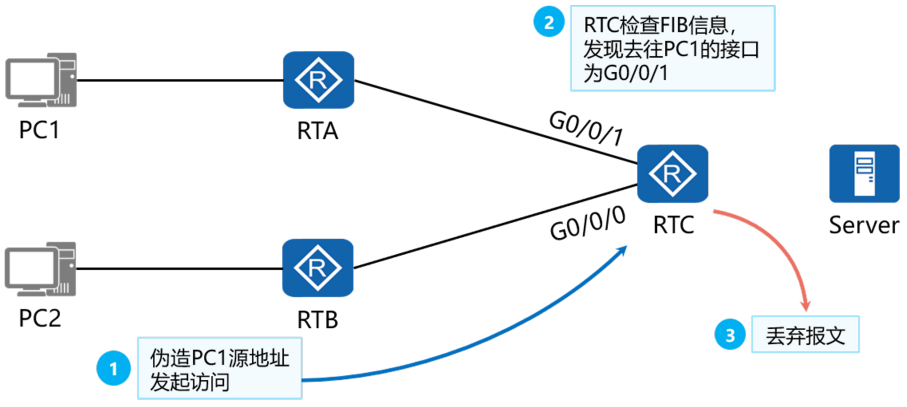
提供给不同的上层应用使用
2.6.3、STelnet和SFTP各自利用了其中的一个逻辑通道，通过SSH对数据进行加密，从而实现数据的安全传输
注：SSH协议由IETF制订，最新版本是v2.0；v1.3和v1.5版本存在安全隐患，已经逐步被淘汰；SSH支持服务端和客户端的双向认证，提供保密性和完整性等安全服务



2.6.4、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
a、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
b、用户认证协议：为服务器提供客户端的身份鉴别
c、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
注：SSH中用到的算法主要有几类：
注1、用于数据信息加密的算法，如：des-cbc（56bit密钥）、3des-cbc（使用3条56位的密钥对数据进行三次加密）、aes128-cbc等
注2、用于密钥交换的算法，如：diffle-hellman-group-exchange-sha1等
注3、用于数据完整性保护的MAC算法，如：hmac-md5、hmac-md5-96等
注4、用于进行数字签名和认证的主机公钥算法，如RSA、DSA（数字签名算法）等



3、基于可信路径的访问控制
3.1、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
3.2、部署URPF【Unicast Reverse Path Forwarding | 单播逆向路径转发】，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



3.3、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
3.4、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
3.5、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
3.5.1、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
3.5.2、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

3.6、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

4、本机防攻击

4.1、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，从而引发其它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

4.2、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

4.3、本机防攻击包括【CPU防攻击】和【攻击溯源】两部分：

4.3.1、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

4.3.2、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

5、CPU防攻击

5.1、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 Rate】，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

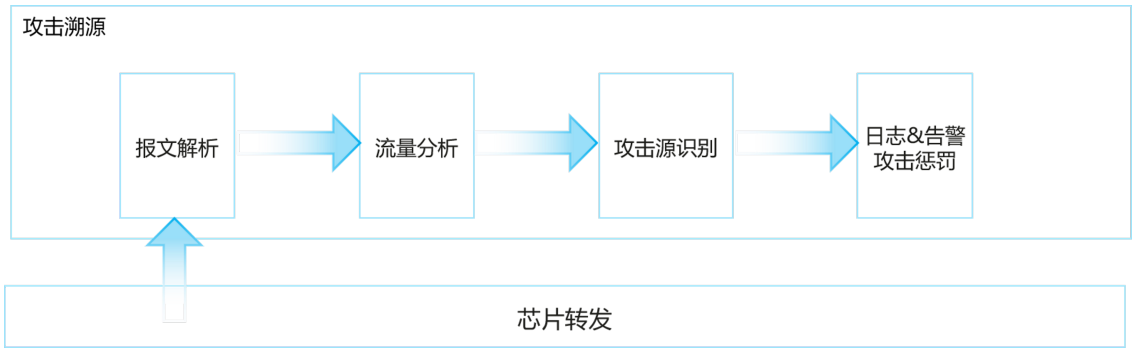
第三级：对上送CPU的报文，按照协议优先级进行调度，保证优先级高的协议先得到处理

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

6、攻击溯源原理

攻击溯源包括报文解析、流量分析、攻击源识别和发送日志告警通知管理员以及实施惩罚四个过程



通过上述所示的四个过程找出攻击源，然后管理员通过ACL或配置黑名单的方式限制攻击源，以保护设备CPU

三、SSH与本机防攻击的配置

详细配置见实验手册