IP Accounting 配置

目 录

第 1 章 ip accounting 概述 1
1.1 ip accounting 应用 1
1.2 ip accounting 的优点 1
1.3 ip accounting 的缺点 1
1.4 ip accounting 术语 1
第 2 章 配置 ip accounting 2
2.1 配置 output-packets 统计 2
2.2 配置 access-violation 统计 3
2.3 配置 precedence 统计 3
2.4 配置 mac 地址统计 4
第 3 章 配置实例 5

第1章 ip accounting 概述

IP accounting 是用来统计网络流量的，相对于 netflow 等流量统计功能，ip accounting 提供的功能更简单，而且可以统计被 ACL 过滤掉的报文，通常部署在小型局域网内。当发生 DOS 等攻击时，可以借助 ip accounting 来判断哪些主机可能正在进行攻击。

ip accounting 是一个非常有用的功能，但不如 netflow 等有名。许多 netflow 的流量统计功能在 ip accounting 中没有，这使得 ip accounting 的应用范围更狭小。但是 ip accounting 也有自己的优势，比如能够非常快捷地获取流量统计的结果。

1.1 ip accounting 应用

以源和目的地址统计正常的转发流量

以源和目的地址统计被 ACL 过滤掉的流量

以 MAC 地址为基础统计流量

以 IP 头部字段的优先级为基础统计流量

1.2 ip accounting的优点

部署简单，可以非常方便地获取当前网络的流量统计信息，并且可以统计被 acl 过滤掉的流量

1.3 ip accounting的缺点

统计太过单一，无法获得流量的详细信息，不适应网络环境多变的情况。

没有超时机制，需要不停地手动删除统计信息，而且也有可能由于流量的表项被全部占用，导致突发流量没有被统计到

1.4 ip accounting 术语

output-packets——经过设备的转发数据

access-violations——被设备 ACL 过滤掉的数据流量

active 数据库——统计 output-packets 或 access-violations 时记录的流量

checkpoint 数据库——当清除统计信息时，output-packet 或 access-violations 流量会被清除至 checkpoint 数据库，原先在 checkpoint 数据库的流被释放到内存中

第2章　配置 ip accounting

2.1　配置output-packets统计

1. 在相应的端口下开启统计功能

只统计源 IP、目的 IP、报文数和字节数，所有流出该端口的流都会被统计，注意只统计转发报文

命令	说明
ip accounting output-packets	统计端口上流出报文的流量

2. 配置统计列表以及相应的 transits 数目

为了减少统计的主机，可以配置主机的统计列表，如果源 IP 地址不在统计列表中，则不统计，除非配置了 Transits 数目不为 0。Transits 流的表项指不满足统计列表的流的表项

命令	说明
ip accounting-list *address netmask*	打开统计的主机列表
ip accounting-transits *num*	配置相应的transits表项数目
show ip accounting transits	显示统计到transits中的流信息
clear ip accounting transits	清除transits中的流信息

3. 配置统计流量的 cache 数目

注意 ip accounting access-violation 和 checkpoint database(后面会讲到)都共享相应的 cache，所以这条命令影响这三者的 cache 数，如果 cache 用完了，后面的流只能被丢弃，并会记录下丢弃了多少报文和字节。

命令	说明
ip accounting-threshold *num*	配置统计流量的cache数目

4. active 数据库和 checkpoint 数据库

统计流的 cache 分为 active database 和 checkpoint database，所有的流都在 active 表项中更新，checkpoint 只是在某一时刻把所有的 active database 移到 checkpoint database 通过 该命令来实现，主要用来观察某一时刻的各个主机的流量有多少

命令	说明
Show ip accounting output-packets	显示所有output-packets的流量统计信息
show ip accounting checkpoint output-packets	显示在checkpoint中output-packets的流量统计信息
show ip accounting checkpoint access-violation	显示在checkpoint中access-violation的流量统计信息
clear ip accounting	将active database 清除到checkpoint，同时清除原先的checkpoint
clear ip accounting checkpoint	清除checkpoint database

2.2 配置access-violation统计

1. 在相应的端口下开启统计被 acl 过滤掉的流

统计所有在该端口下被 acl 过滤掉的流，主要统计源 IP，目的 IP，字节数，报文数以及 ACL name

命令	说明
ip accounting access-violation	统计端口上被acl过滤的流量

2. 显示 access-violation 的 active 数据库

显示从上次清除 active 数据库后统计到得 access-violation 信息

命令	说明
Show ip accounting access-violation	显示所有output-packets的流量统计信息

2.3 配置precedence统计

1. 在相应的端口下开启以 ip 包优先级为基础统计流量的功能

主要统计 8 个优先级的字节数和报文数，不记录 IP 地址和 mac 地址

命令	说明
ip accounting precedence input	对该端口上接收到的包的优先级进行统计
ip accounting precedence output	对该端口上出去的包的优先级进行统计

2. 显示优先级统计的流量信息

命令	说明
show ip accounting precedence	显示所有端口上统计的优先级数据
show ip accounting precedence interface *intf*	显示intf端口上统计的优先级数据

3. 清除优先级统计的流量信息

命令	说明
clear ip accounting precedence	清除所有端口上统计的优先级数据
clear ip accounting precedence interface *intf*	清除intf端口上统计的优先级数据

2.4 配置mac地址统计

1. 在端口上开启 mac 地址统计功能

每个接口都有 512 个表项来记录收到的包，又有 512 个表项来记录发出去的包，对于 input

主要记录源 MAC 地址，字节数和报文数，对于 output 主要记录目的 MAC 地址，字节数和报文数，并且两个都有一个时间戳，用来记录最近收到报文的时间

命令	说明
ip accounting mac-address input	统计该端口收上来的包，并记录源mac地址
ip accounting mac-address output	统计该端口发出去的包，并记录目的mac地址

2. 显示 mac 地址统计的流量信息

命令	说明
show ip accounting mac-address	显示所有端口上统计的mac地址数据
show ip accounting mac-address interface *intf*	显示intf端口上统计的mac地址数据

3. 清除 mac 地址统计的流量信息

命令	说明
clear ip accounting mac-address	清除所有端口上统计的mac地址数据
clear ip accounting mac-address interface *intf*	清除intf端口上统计的mac地址数据

第3章　配置实例

1. 在 f0/0 上配置 output-packets

   Router_config_f0/0#ip accounting output-packets

   Router_config#ip accounting-threshold 1024

2. 在 f0/0 上配置 access-violation

   Router_config_f0/0#ip accounting access-violation

3. 在 f0/0 上配置 precedence 流量统计

   Router_config_f0/0#ip accounting precedence input

   Router_config_f0/0#ip accounting precedence output

4. 在 f0/0 上配置 mac-address 流量统计

   Router_config_f0/0#ip accounting mac-address input

   Router_config_f0/0#ip accounting mac-address output