基于 NetFlow 网络流量异常的分析

Analysis of Network Flux Abnormity Based on NetFlow

朱 敏　（浙江大学校园网络中心 杭州 310027）

摘要：本文介绍了用 NetFlow 对网络异常流量的特征进行了深入的分析，并提出了如何在网络层面对网络异常流量采取防护措施。

关键词：NetFlow　流量　路由器

1　引言

随着计算机网络技术的迅速发展和应用，人们对计算机网络的依赖也不断增强，网络的重要性及其对社会的影响也越来越大。与此同时，网络上形形色色的异常流量也随之而来，影响到互联网的正常运行，威胁用户主机的安全和正常使用。

2 NetFlow 概述

2.1　工作原理

NetFlow 是一种数据交换，它利用标准的交换模式处理数据流的第一个 IP 包，生成 NetFlow? 缓存，随后同样的数据基于缓存信息在同一个数据流中进行传输，不再匹配相关的访问控制等策略，NetFlow 缓存同时包含了随后数据流的统计信息。一个 NetFlow 流定义为在一个源 IP 地址和目的 IP 地址之间传输单向数据包流，且所有数据包具有共同的传输层源、目的端口号。

2.2　数据的格式说明及采集

本文的数据分析都是基于这种格式。

源地址|目的地址|源自治域|目的自治域|流入接口号|流出接口号|源端口|目的端口|协议类型|包数量|字节数|流数量，如：

31. *. *. 88|31. *. *. 200|55918|Others|8|12|3529|126|6|7|190|1

NetFlow 数据也可在路由器上直接查看，下面是采集的网络流量数据：

210. *. *. 88|205. *. *. 33|Others|localas|7|3|1280|80|80|11|60|1

gsr #att 2

LC – Slot2 ship cache flow

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts

Gi2/1 212. *. *. 210 PO4/2 211. *. *. 209 05 08CD 178D 2

Gi2/1 31. *. *. 12 Null 33. *. *. 225 10 0315 038B 1

由路由器直接输出的 Neflow 数据，也可采用类似的方法分析。NetFlow 的支持情况与路由器类型、板卡类型、IOS 版本、IOS 授权都有关系，不是在所有的情况下都能使用，使用时还需要考虑软、硬件配置情况。

3　异常流量的 NetFlow 分析

3.1　异常流量的种类

(1) 拒绝服务攻击(DoS)。DoS 攻击使用大量的数据流量攻击网络设备和其接入的服务器，使网络设备和服务器的性能下降、占用大量网络带宽、消耗系统资源，影响其它相关用户流量的正常通信，导致网络服务不能用，最终使整个网络瘫痪。如 DoS 可利用 TCP 协议的缺陷，通过 SYN 打开 TCP 连接，占用系统资源，使合法用户被排斥而不能建立正常的 TCP 连接。下面是一个典型的 DoS SYN 攻击 NetFlow 数据案例，该例中多个伪造的源 IP 同时向一个目的 IP 发起 TCP SYN 攻击。

119. *.212.200|211. *. *.60|Others|53261|2|3|1122|8000|6|1|60|1

103. *.88.50|211. *. *.60|Others|53261|2|3|2567|8000|6|1|60|1

21. *.13.92|211. *. *.60|Others|53261|2|3|6580|8000|6|1|60|1

由于 Internet 协议本身存在的缺陷,IP 包中的源地址是可以伪造的,目前有很多 DoS 工具可以伪装源地址,使攻击源主机不易追踪。

(2) 分布式拒绝服务攻击(DDoS)。DDoS 把 DoS 又进了一步,从互联网上的多个地点制造网络流量,使整个攻击行动更为巨大,分布式拒绝服务攻击可以协调多台计算机上的进程发起攻击,使被攻击目标因过载而崩溃。下面是一个典型的 DDoS 攻击 NetFlow 数据案例,该例中多个 IP 同时向一个 IP 发起 UDP 攻击。

31. *. *.50|39. *. *.200|85393|as9|3|8|15269|3216| 17|1596|8621390|1

51. *. *.120|39. *. *.200|85182|Others|3|8|56271|65280|17|16|71688|1

212. *. *.186|39. *. *.200|85633|as9|3|8|35167|33521|17|7101|2012168|1

(3) 蠕虫病毒流量。蠕虫病毒的传播也会对网络产生影响。Red? Code、冲击波、振荡波等病毒不但会对用户主机造成影响,而且还会对网络的正常运行构成危害,因为这些病毒具有扫描网络,主动传播病毒的能力,大量占用系统资源和带宽。下面是一个振荡波病毒 NetFlow 数据案例,该例中一个 IP 同时向随机生成的多个 IP 发起 445 端口的 TCP 连接请求,相当于对网络发起 DoS 攻击。

31. *. *. *|117. *. *.56|Others|Others|2|3|1133|445|6|1|60|1

31. *. *. *|65. *. *.90|Others|Others|2|3|8000|445|6|1|60|1

31. *. *. *|10. *. *.136|Others|Others|2|3|8000|445|6|1|60|1

3.2 异常流量的流向分析

异常流量可分为三种。第一、外网对内网的攻击,第二、内网对外网的攻击,第三、内网对内网的攻击。不同异常流量的流向,需要采取不同的防护和处理策略,下面是这三种情况 NetFlow 数据案例。210 开头的地址为内网地址。

112. *. *.152|210. *. *.31|Others|71356|2|3|80000|8000|6|1|60|1

210. *. *.69|117. *. *.120|55216|as3|2|8|19561|102|17|1|62|1

210. *. *.70|210. *. *.110|Others|localas|80|3|1320|445|6|1|60|1

3.3 异常流量的数据包类型

(1) TCP SYN Flood(60 字节)

10. *.51.3|2. *.21.160|59329|as9|3|2|1000|18|6|1|60|1

从 NetFlow 采集的数据可见,此异常流量的典型特征是数据包协议类型为 6(TCP),数据流大小为 60 字节(通常为 TCP 的 SYN 连接请求)。

(2) ICMP Flood

2. *.65.1|1. *.81.88|as12|53122|3|2|1|1|1|1|146173|300239168|1

从 NetFlow 采集的数据可见,此异常流量的典型特征是数据包协议类型为 1(ICMP),单个数据流字节数达 300M 字节。

(3) UDP Flood

*. *.35.22|117. *.66.155|55326|Others|6|30|1322|1322|17|198|288958|1

*. *.23.167|32. *.198.100|55326|Others|6|30|923|113|17|1|88|1

从 NetFlow 采集的数据可见,此异常流量的典型特征是数据包协议类型为 17(UDP),数据流有大有小。

3.4 异常流量的源、目的端口分析

异常流量的源端口通常会随机生成,而目的端口一般固定在一个或几个端口,因此可对异常流量进行过滤或限制。目的端口为 UDP? 5169:如:

217. *. *.166|133.121.150.66|Others|localas|71|6|2591|445|6|2|100|1

217. *. *.166|100.168.100.121|Others|localas|71|6|5129|445|6|2|100|1

217. *. *.166|170.195.30.60|Others|localas|71|6|1188|445|6|2|100|1

217. *. *.200|162. *.100.31|Others|Others|13|9|

8000|5169|17|1|28|1
217. *. *. 200|162. *. 100. 32|Others|Others|13|9|
8000|5169|17|2|68|2
217. *. *. 200|162. *. 100. 33|Others|Others|13|9|
8000|5169|17|3|108|3

3.5 异常流量产生的后果

异常流量对网络的影响主要表现在这二个方面，第一、占用系统资源(CPU、内存等)，使网络不能提供正常的服务，第二、占用带宽使网络拥塞，造成丢包、时延增大，严重时可导致网络瘫痪。

4 利用 NetFlow 处理防范网络异常流量

4.1 判断异常流量的流向

目前大多数的网络设备只提供物理端口流入量的 NetFlow 数据，因此在采集异常流量 NetFlow 数据之前，先要判断异常流量的流向，然后选择合适的物理端口去采集数据。流量监控管理软件是判断异常流量流向的有效工具，通过流量大小变化的监控，可以发现异常流量，特别是大流量的异常流量的流向，从而进一步找到异常流量的源、目标接入设备端口和源、目的地址。

4.2 NetFlow 数据采集分析

异常流量的流向判断后，可选择合适的网络设备端口，进行 Neflow 配置，采集该端口流入量的 NetFlow 数据。以下是在 Cisco? GSR 路由器 GigabitEthernet10/0 端口上对 NetFlow 的配置。通过该配置把流入到 GigabitEthernet10/0 的 NetFlow 数据送到 NetFlow 采集器 *. *. *. 51，采样间隔为 100:1。

```
ip flow - expor source Loopback0
ip flow - export destination *. *. *. 51 9995
ip flow - sampling - mode packet - interval 100
interface GigabitEthernet10/0
ip route - cache flow sampled
```

4.3 异常流量的处理方法

(1) 切断连接。在知道异常流量源地址且该源地址设备可控的情况下，切断异常流量源设备的物理连接。

(2) 静态空路由过滤。在知道异常流量目标地址的情况下，可用静态路由把异常流量的目标地址指向空(Null)，这种过滤不消耗路由器系统资源，同时也过滤了对目标地址的正常访问，配置如下：

```
ip route 205. *. *. 2 255. 255. 255. 255 Null 0
```

对于多路由器的网络，还需增加相关动态路由配置，保证过滤在全网上生效。

(3) 过滤。利用 ACL(Access Control List)过滤能灵活地对源、目的 IP 地址、协议类型、端口号等各种方式过滤，但存在消耗网络设备系统资源的副作用，下面是利用 ACL 过滤 UDP 1434 端口的配置。

```
access - list 101 deny udp any any eq 1434
access - list 101 permit ip any any
```

(4) 异常流量限定。利用路由器 CAR 功能，可将异常流量限定在一定的范围，但这种过滤存在消耗路由器系统资源的副作用，下面是利用 CAR 限制 UDP 1434 端口流量的配置。此配置限定 UDP 1434 端口的流量为 10Kbps。

```
Router# (config) access - list 150 deny udp any any eq 1434
Router# (config) access - list 150 permit ip any any
Router# (config) interface fastEthernet 0/0
Router# (config - if) rate - limit input access - group rate - limit 150 10000 1500 20000
conform - action drop exceed - action drop
```

5 结束语

处理分析网络异常流量还有许多其它的方法，如利用 IDS、协议分析仪、网络设备的 ip? accounting 等功能来处理异常流量，但这些方法效率低、对网络设备性能有影响、数据不易采集等等。利用 NetFlow 分析网络异常流量因其方便、快捷、高效的特点，成为互联网安全管理的重要手段，特别是在较大的网络管理中，更能体现出其独特的优势。

参考文献

1 http://www. bluedon. com/bluedo621/search/newsdisplay4. asp id = 2479&sort = 4.