FortiGate 旁路流量统计技术说明

版本	1.0
时间	2012 年 4 月
作者	韩晔 (yhan@fortinet.com)
测试版本	FortiOS v4.0 MR3 Patch6， FortiAnalyzer v4.0MR3 Patch 2)
状态	草稿

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

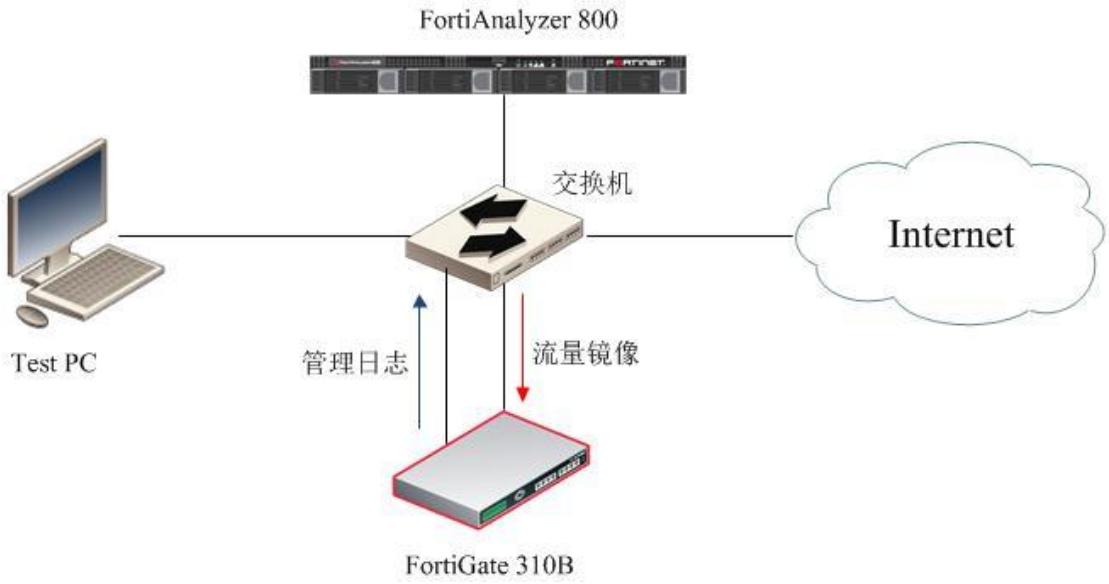
目 录

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

目的

本文的目的是介绍 FortiGate 设备旁路接入网络内，实现对网络流量及各种应用流量的统计，主要实现对 P2P 流量的统计。

测试环境



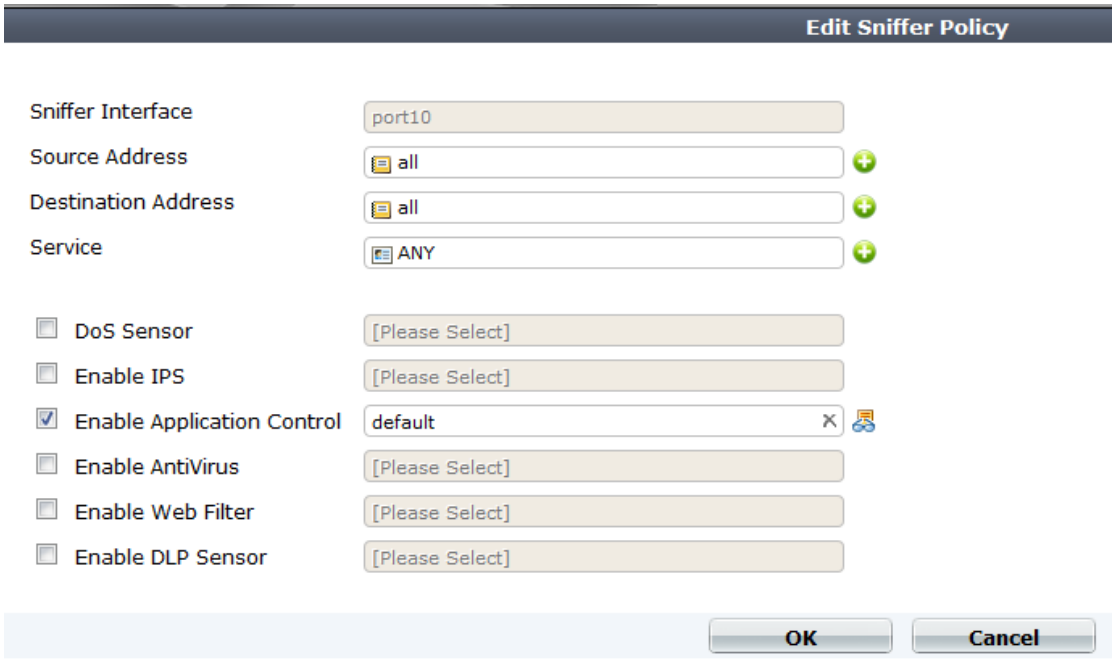
交换机配置镜像接口，把连接 Internet 接口的双向流量镜像到连接 FortiGate 310B 的接口上。FortiGate 310B 的另一个接口也连接在交换机上，用于管理及向 FortiAnalyzer800 上发送日志。测试 PC 通过交换机到连接 Internet。

设备配置

FortiGate 设备配置

FortiGate 开启 Sniffer policy，并开启 Application control 功能，对所有应用进行监控。

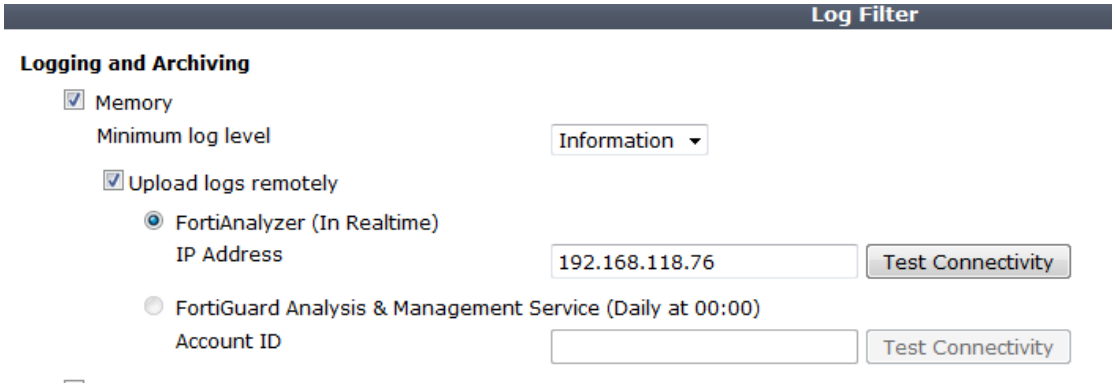
北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255



在命令行下开启流量日志功能，如下：

```
config firewall sniff-interface-policy
    edit 1
        set interface "port10"
            set srcaddr "all"
            set dstaddr "all"
            set service "ANY"
        set logtraffic enable
        set application-list-status enable
        set application-list "default"
    next
```

配置日志发送到 FortiAnalyzer

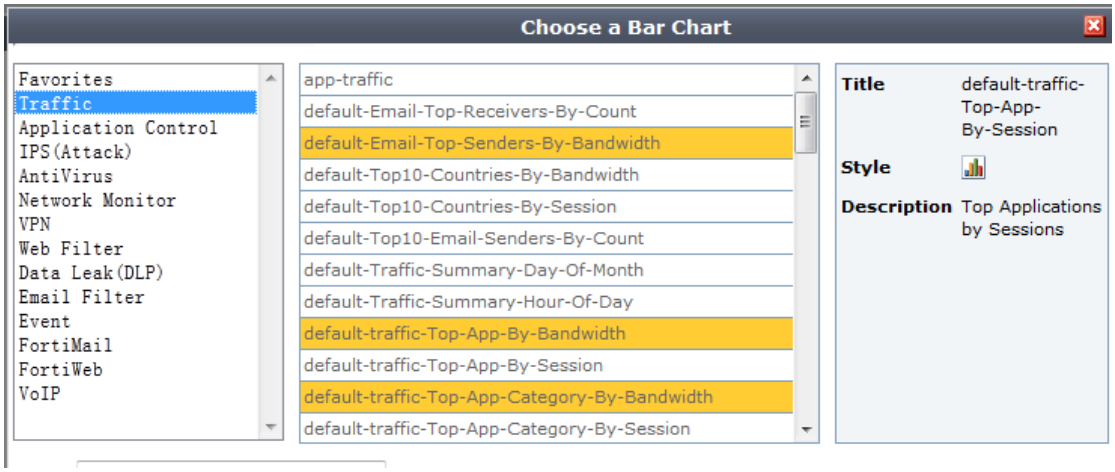


应用流量统计

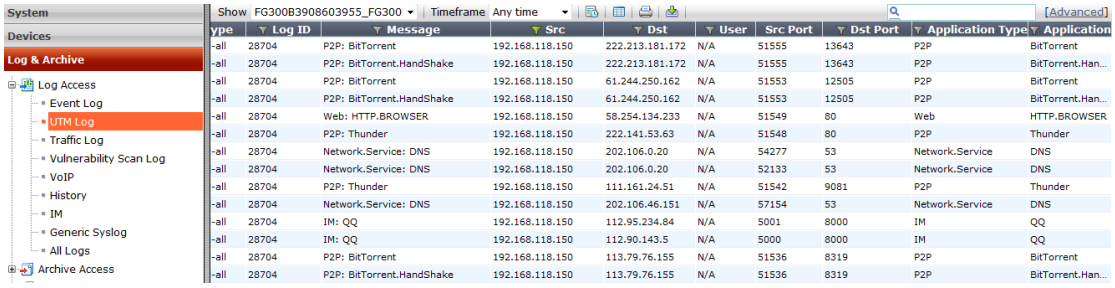
北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

FortiAnalyzer 配置

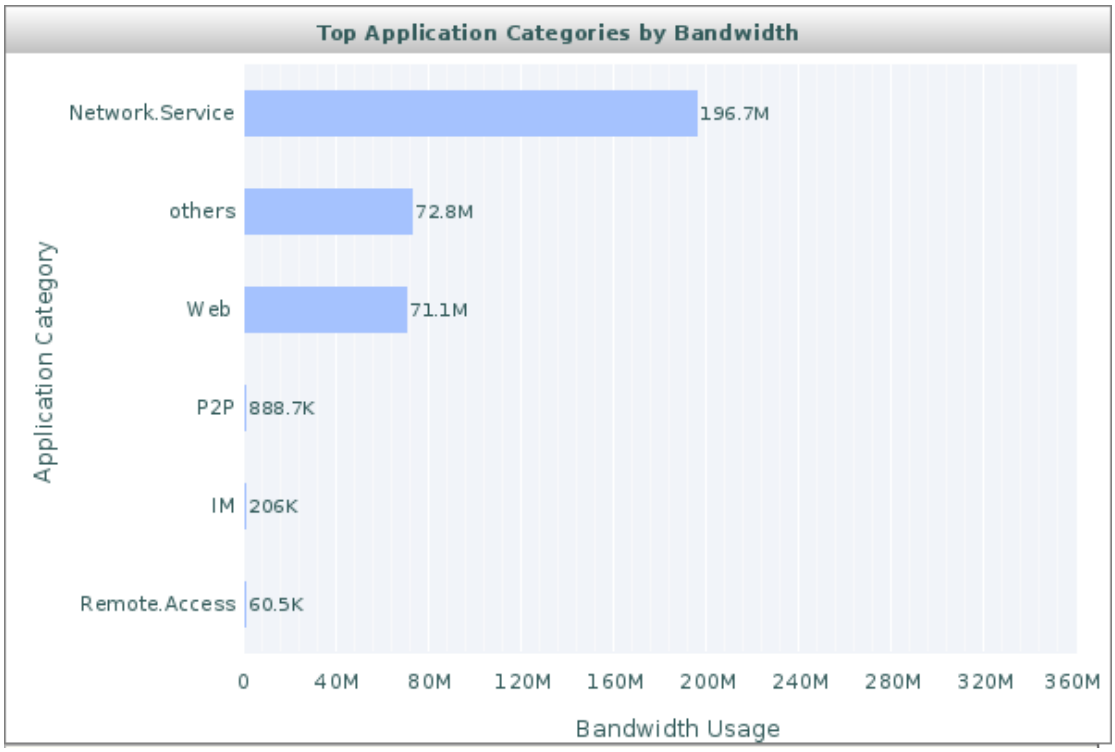
FortiAnalyzer 开启 Local Datasheet，并配置相关流量统计报表：



在 UTM 日志中，可以看到有大量的 P2P 日志，如下图：

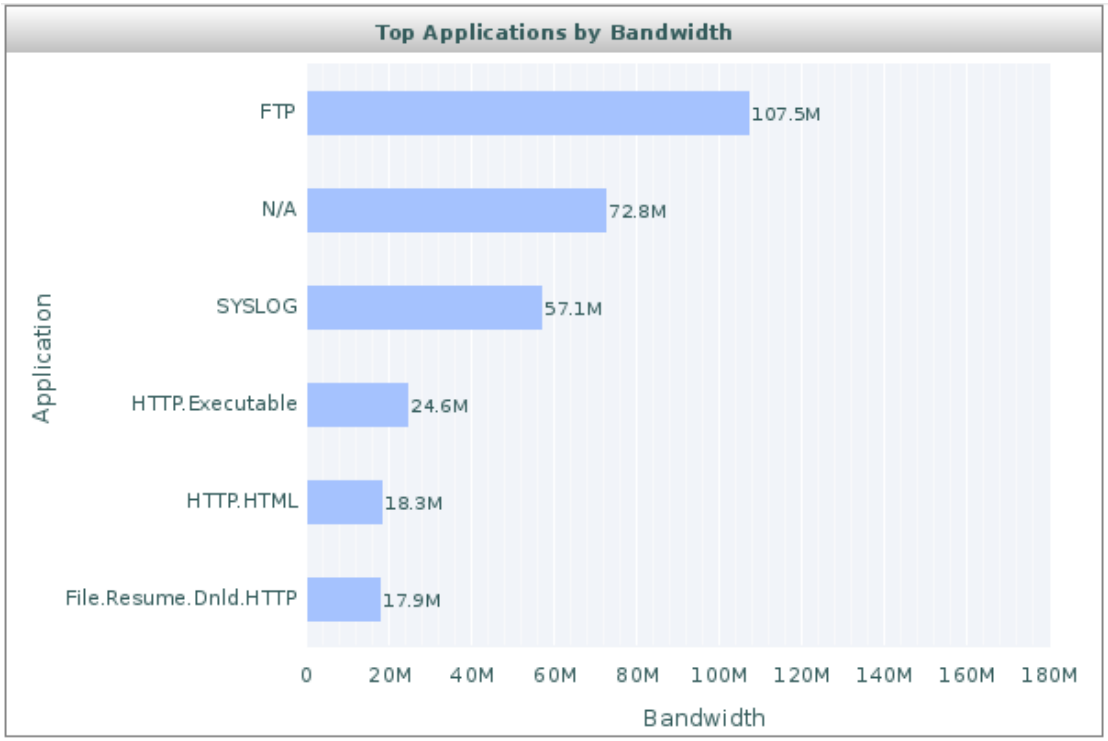


但在生成的应用分类流量统计报表中，只有少量的 P2P 流量。



北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

在生成的应用流量统计报表中，没有任何一种 P2P 流量。



原因分析

FortiAnalyzer 在对应用流量进行统计时，与 UTM log 中的内容无关，是根据 Traffic log 中的 Application 相关字段来确定应用类型，并统计流量。

在 UTM 日志中，可以看到针对一个目的 IP 地址的 BT 下载记录，如下图：

Message	Src	Dst	User	Src Port	Dst Port	Application Type	Application
P2P: BitTorrent	192.168.118.152	114.228.20.240	N/A	52684	12465	P2P	BitTorrent
P2P: BitTorrent.HandShake	192.168.118.152	114.228.20.240	N/A	52684	12465	P2P	BitTorrent.Han...

可以看到，同一下载生成两条日志，分别是 BitTorrent 和 BitTorrent.HandShake

而在流量日志中搜索该目的 IP 的日志记录，如下图：

Type	Level	Status	Src	Dst	Sent	Application	Application Type	Received	Applicat
traffic		√	192.168.118.152	114.228.20.240	68 B	BitTorrent.HandShake	N/A	0 B	P2P

在流量日志中，只看到一条日志，是与 BitTorrent.HandShake 相关的，且流量非常小。从 FortiGuard 上可以查到 BitTorrent.HandShake 的介绍：“This indicates an attempt to access BitTorrent.”因此，在流量日志中，只记录了 BT 下载握手的过程，而流量传输的过程没有记录。

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

[1]其它网络流量统计

使用 FTP 下载一个约 40M 的文件，FortiAnalyzer 上记录的日志如下图所示：

Src	Dst	Sent	Application	Application Type	Received	Application
192.168.118.182	192.168.118.254	1 B	FTP	N/A	38.2 MB	Network.Service
192.168.118.182	192.168.118.254	102 B	FTP	N/A	349 B	Network.Service

可以准确记录流量。

使用 HTTP 下载一个约 18M 的文件，FortiAnalyzer 上记录的日志如下图所示：

Src	Dst	Sent	Application	Application Type	Received	Application Cate
192.168.118.182	192.168.118.38	311 B	HTTP.Compress	N/A	18.0 MB	Web
192.168.118.182	192.168.118.38	128 B	ICMP	N/A	128 B	Network.Service

可以准确记录流量。

[1]

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255