xxx

统计时间：2018-08-06 02:00:00 - 2018-08-13 02:00:00

生成时间：2018-08-13 11:01:46

目录

[1. 安全威胁概览](#_Toc1)

[1.1. 核心资产安全概览](#_Toc2)

[1.2. 主机安全概览](#_Toc3)

[1.3. 外部攻击源地理位置分布](#_Toc4)

[1.4. 威胁概览](#_Toc5)

[1.4.1. 威胁趋势分析](#_Toc6)

[1.4.2. 威胁类型分布](#_Toc7)

[1.4.3. 威胁协议分布](#_Toc8)

[1.4.4. 威胁检测引擎分布](#_Toc9)

[1.4.5. 威胁严重程度分布](#_Toc10)

[1.4.6. 威胁源排名](#_Toc11)

[2. 安全风险详情](#_Toc12)

[2.1. 核心资产安全分析](#_Toc13)

[2.2. 主机安全分析](#_Toc14)

[2.2.1. 10.180.186.123发现威胁分析](#_Toc15)

[2.2.2. 10.180.203.27发现威胁分析](#_Toc16)

[2.2.3. 10.180.0.161发现威胁分析](#_Toc17)

[2.2.4. 224.0.1.2发现威胁分析](#_Toc18)

[2.2.5. 1.207.63.153发现威胁分析](#_Toc19)

[2.2.6. 116.23.46.194发现威胁分析](#_Toc20)

[2.2.7. 103.69.68.86发现威胁分析](#_Toc21)

[2.2.8. 180.101.45.88发现威胁分析](#_Toc22)

[2.2.9. 10.180.185.23发现威胁分析](#_Toc23)

[2.2.10. 119.191.145.227发现威胁分析](#_Toc24)

[3. 威胁类型汇总](#_Toc25)

[3.1. 拒绝服务](#_Toc26)

[3.1.1. 拒绝服务趋势](#_Toc27)

[3.1.2. 拒绝服务主要影响IP](#_Toc28)

[3.1.3. 拒绝服务主要来源](#_Toc29)

[3.1.4. 拒绝服务类型排名](#_Toc30)

[4. 网络流量概览](#_Toc31)

[5. 网络流量详情](#_Toc32)

[5.1. 应用流量分析](#_Toc33)

[5.1.1. 热门高风险应用排名](#_Toc34)

[5.1.2. 应用类别排名](#_Toc35)

[5.1.3. 应用子类别排名](#_Toc36)

[5.1.4. 应用风险等级分布](#_Toc37)

[5.1.5. 应用技术分布](#_Toc38)

[5.2. IP流量分析](#_Toc39)

[5.2.1. 用户流量排名](#_Toc40)

[5.2.2. IP流量排名](#_Toc41)

[5.2.3. 流量地区分布](#_Toc42)

[5.3. 接口流量分析](#_Toc43)

[5.4. 安全域流量分析](#_Toc44)

[5.5. 策略流量分析](#_Toc45)

[6. URL内容概览](#_Toc46)

[7. URL访问详情](#_Toc47)

[7.1. 最活跃的用户排名](#_Toc48)

[7.2. 热门URL类别访问排名](#_Toc49)

[7.3. 热门URL访问排名](#_Toc50)

[8. 系统运行状况](#_Toc51)

[8.1. 系统资源利用率](#_Toc52)

[8.1.1. CPU利用率趋势](#_Toc53)

[8.1.2. 内存利用率趋势](#_Toc54)

[8.1.3. 磁盘空间利用率趋势](#_Toc55)

[8.2. 系统温度](#_Toc56)

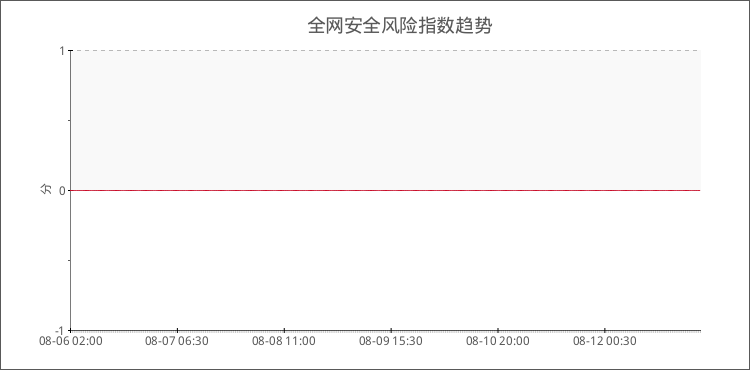
[8.2.1. CPU温度趋势](#_Toc57)

[8.2.2. 机箱温度趋势](#_Toc58)

# 1. 安全威胁概览

2018-08-06至2018-08-13期间，全网安全风险指数平均为1分（越低越好），共检测到威胁事件108次，平均每天发现15次，其中中威胁事件108次，主要涉及10.180.186.123，10.180.203.27，10.180.0.161等主机，主要的威胁类型包括拒绝服务等。核心资产和主机面临的攻击不多，现有攻击风险能够有效的防护。

统计期间，评分最高的时段为2018-08-06 02:00:00至2018-08-06 02:30:00，分数为0，趋势图如下：

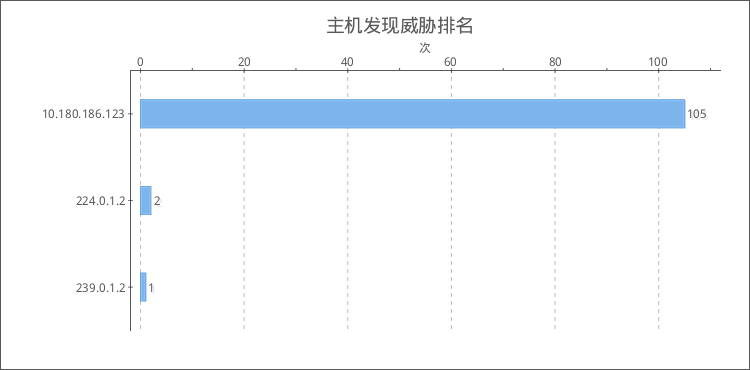


## 1.1. 核心资产安全概览

暂无符合条件的数据

## 1.2. 主机安全概览

统计期间，主机共发现威胁108次，其中10.180.186.123占比97.22%，224.0.1.2占比1.85%，239.0.1.2占比0.93%。具体的排名如下：



发现威胁最多的主机(IP)详情如下：

|  |  |  |  |
| --- | --- | --- | --- |
| # | 主机 | 威胁类型(次) | 百分比 |
| 1 | 10.180.186.123 | 拒绝服务(105) | 97.22% |
| 2 | 224.0.1.2 | 拒绝服务(2) | 1.85% |
| 3 | 239.0.1.2 | 拒绝服务(1) | 0.93% |

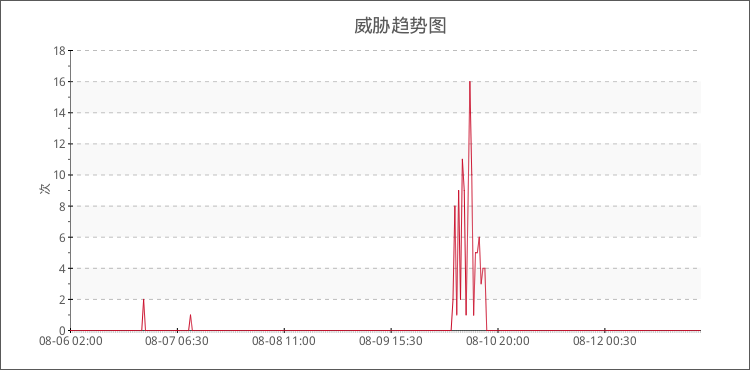
## 1.3. 外部攻击源地理位置分布

暂无符合条件的数据

## 1.4. 威胁概览

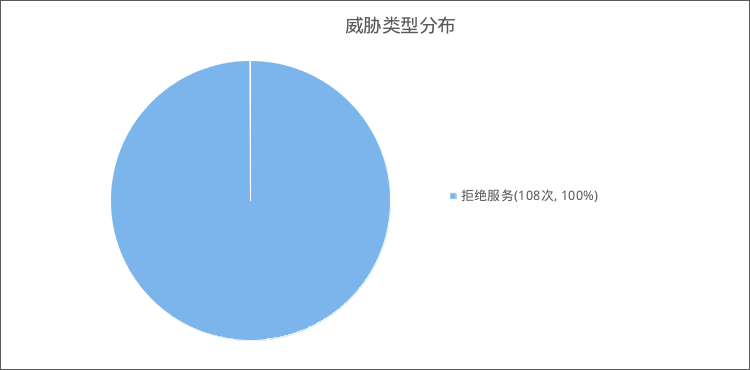
### 1.4.1. 威胁趋势分析

统计期间共发现108次威胁，平均每30分钟发现0.32次，发现最频繁的时段为 2018-08-10 12:30:00 到 2018-08-10 13:00:00，共发现威胁16次。



### 1.4.2. 威胁类型分布

统计期间，本设备共发现1种威胁类型，其中拒绝服务占比100%。具体的分布图如下：



排名靠前的威胁类型详情如下：

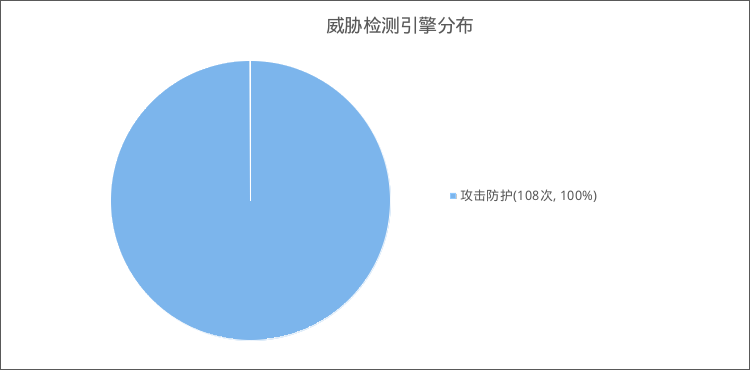
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | 威胁类型 | 威胁子类型 | 次 | 百分比 |
| 1 | 拒绝服务 | DDOS洪范(108) | 108 | 100% |

### 1.4.3. 威胁协议分布

暂无符合条件的数据

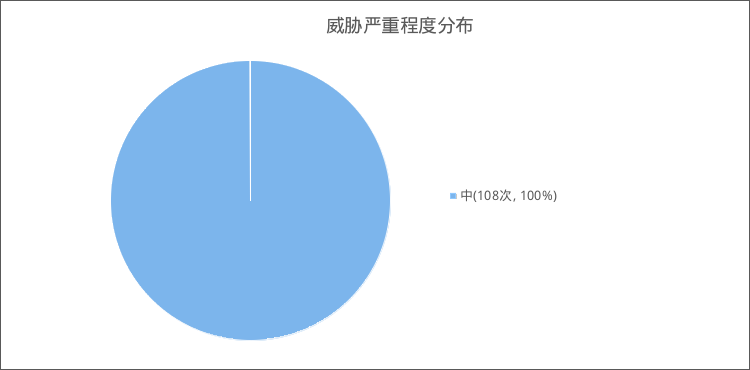
### 1.4.4. 威胁检测引擎分布

统计期间，本设备共发现1种检测引擎，其中攻击防护占比100%。具体的分布图如下：



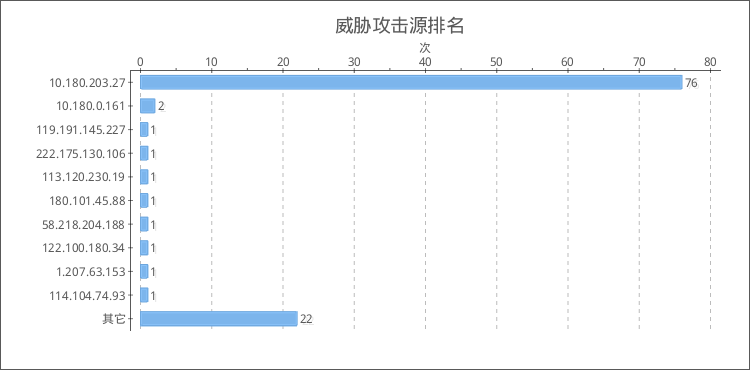
### 1.4.5. 威胁严重程度分布

统计期间，本设备共发现1种严重程度，其中中占比100%。具体的分布图如下：



### 1.4.6. 威胁源排名

统计期间，本设备共发现32种威胁源，其中10.180.203.27占比70.37%，10.180.0.161占比1.85%，119.191.145.227占比0.93%。具体的排名如下：



发现攻击最多的主机(IP)详情如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 威胁源 | 次 | 威胁目的(次) | 威胁类型(次) | 威胁名称(次) | 百分比 |
| 1 | 10.180.203.27 | 76 | 10.180.186.123(76) | DDOS洪范(76) | icmp-flood(76) | 70.37% |
| 2 | 10.180.0.161 | 2 | 224.0.1.2(1), 239.0.1.2(1) | DDOS洪范(2) | icmp-flood(2) | 1.85% |
| 3 | 119.191.145.227 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 4 | 222.175.130.106 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 5 | 113.120.230.19 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 6 | 180.101.45.88 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 7 | 58.218.204.188 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 8 | 122.100.180.34 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 9 | 1.207.63.153 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 10 | 114.104.74.93 | 1 | 10.180.186.123(1) | DDOS洪范(1) | icmp-flood(1) | 0.93% |
| 11 | 其它 | 22 |  |  |  | 20.37% |

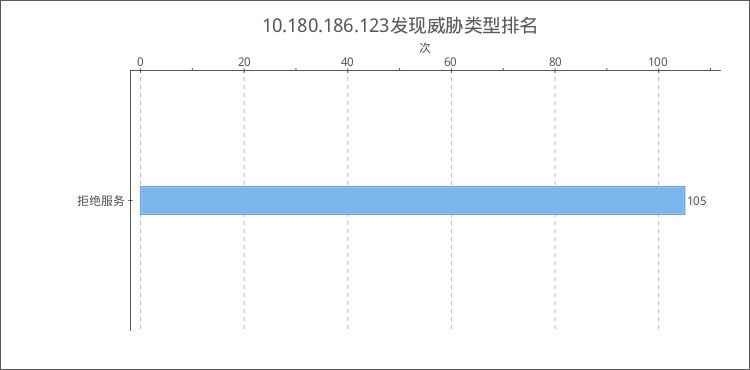
# 2. 安全风险详情

## 2.1. 核心资产安全分析

## 2.2. 主机安全分析

### 2.2.1. 10.180.186.123发现威胁分析

统计期间，10.180.186.123共发现威胁105次，其中拒绝服务占比100%。具体的排名如下：

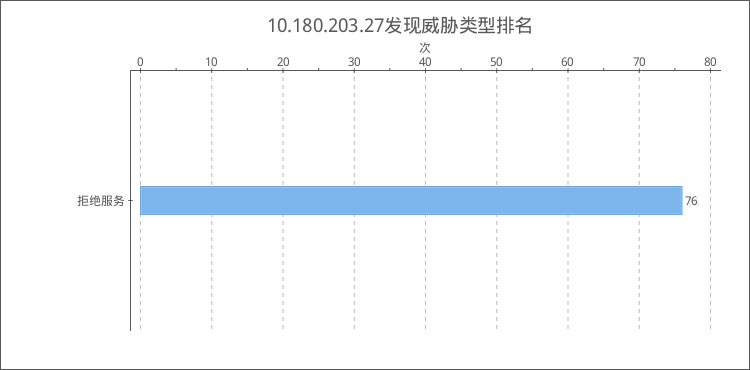


对10.180.186.123发起攻击的IP地址详情如下

|  |  |  |  |
| --- | --- | --- | --- |
| # | 攻击源 | 威胁类型(次) | 百分比 |
| 1 | 10.180.203.27 | 拒绝服务(76) | 72.38% |
| 2 | 1.207.63.153 | 拒绝服务(1) | 0.95% |
| 3 | 27.154.76.91 | 拒绝服务(1) | 0.95% |
| 4 | 45.115.243.159 | 拒绝服务(1) | 0.95% |
| 5 | 58.218.204.188 | 拒绝服务(1) | 0.95% |
| 6 | 60.213.119.60 | 拒绝服务(1) | 0.95% |
| 7 | 61.164.72.218 | 拒绝服务(1) | 0.95% |
| 8 | 103.69.68.86 | 拒绝服务(1) | 0.95% |
| 9 | 111.8.51.2 | 拒绝服务(1) | 0.95% |
| 10 | 111.8.89.57 | 拒绝服务(1) | 0.95% |
| 11 | 其它 |  | 19.05% |

### 2.2.2. 10.180.203.27发现威胁分析

统计期间，10.180.203.27共发现威胁76次，其中拒绝服务占比100%。具体的排名如下：

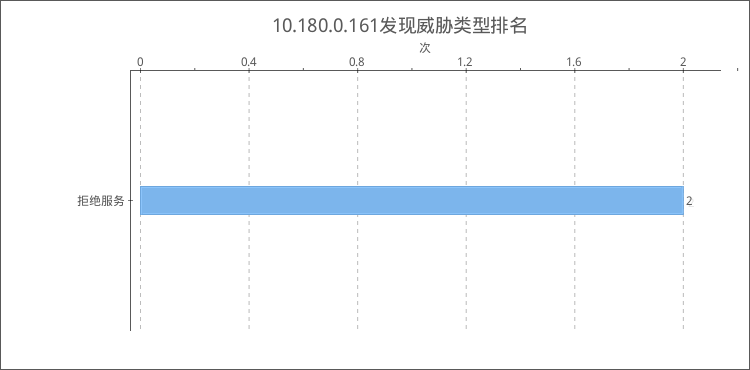


对10.180.203.27发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.3. 10.180.0.161发现威胁分析

统计期间，10.180.0.161共发现威胁2次，其中拒绝服务占比100%。具体的排名如下：

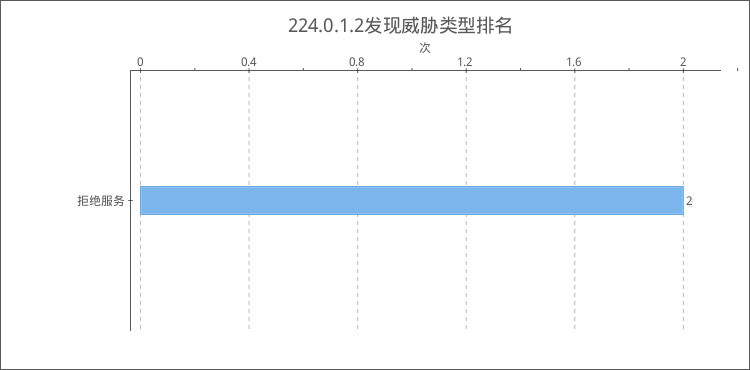


对10.180.0.161发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.4. 224.0.1.2发现威胁分析

统计期间，224.0.1.2共发现威胁2次，其中拒绝服务占比100%。具体的排名如下：

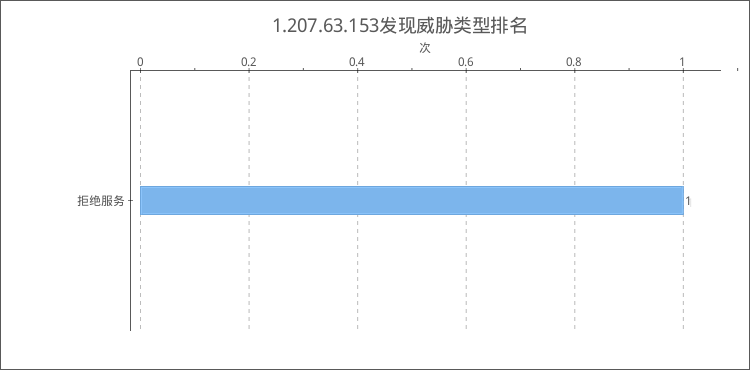


对224.0.1.2发起攻击的IP地址详情如下

|  |  |  |  |
| --- | --- | --- | --- |
| # | 攻击源 | 威胁类型(次) | 百分比 |
| 1 | 10.180.0.161 | 拒绝服务(1) | 50% |
| 2 | 10.180.185.23 | 拒绝服务(1) | 50% |

### 2.2.5. 1.207.63.153发现威胁分析

统计期间，1.207.63.153共发现威胁1次，其中拒绝服务占比100%。具体的排名如下：

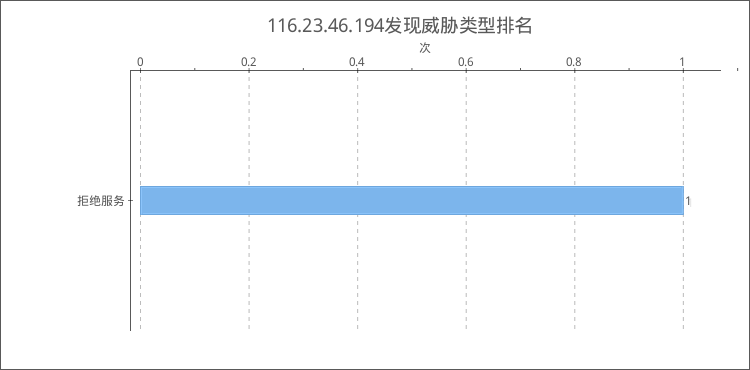


对1.207.63.153发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.6. 116.23.46.194发现威胁分析

统计期间，116.23.46.194共发现威胁1次，其中拒绝服务占比100%。具体的排名如下：

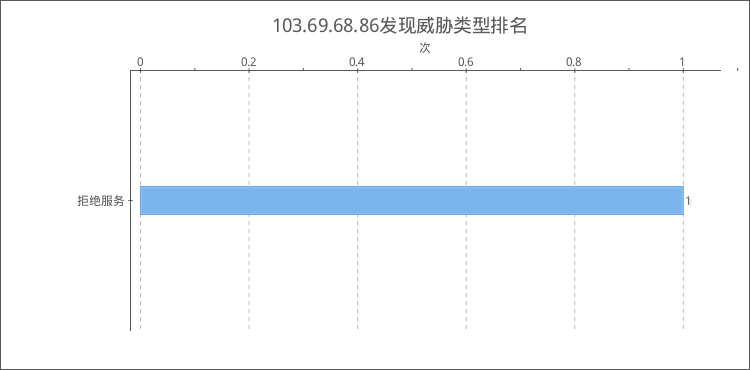


对116.23.46.194发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.7. 103.69.68.86发现威胁分析

统计期间，103.69.68.86共发现威胁1次，其中拒绝服务占比100%。具体的排名如下：

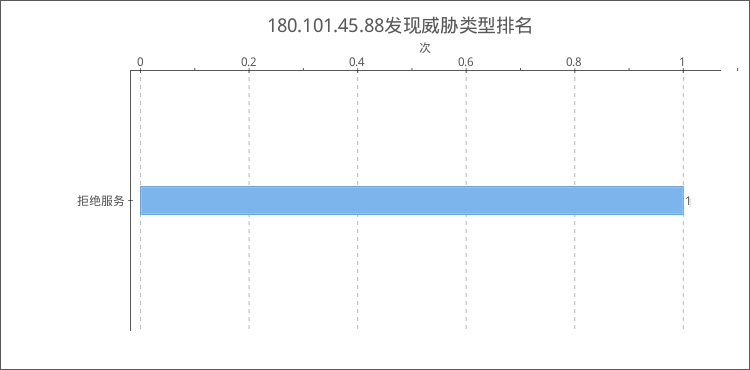


对103.69.68.86发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.8. 180.101.45.88发现威胁分析

统计期间，180.101.45.88共发现威胁1次，其中拒绝服务占比100%。具体的排名如下：

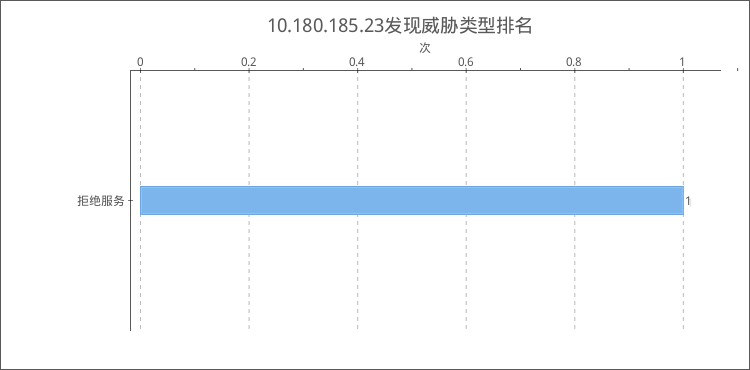


对180.101.45.88发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.9. 10.180.185.23发现威胁分析

统计期间，10.180.185.23共发现威胁1次，其中拒绝服务占比100%。具体的排名如下：

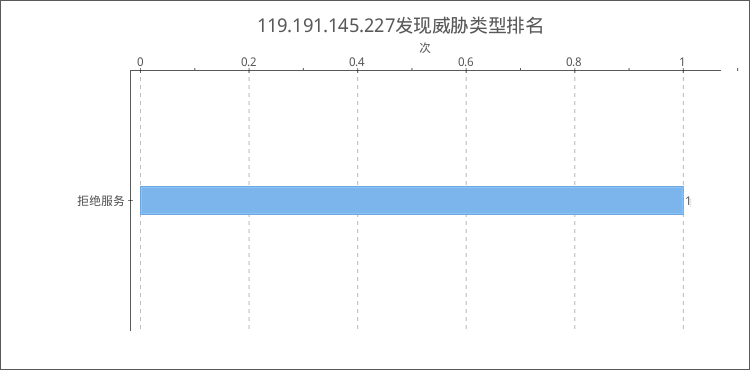


对10.180.185.23发起攻击的IP地址详情如下

暂无符合条件的数据

### 2.2.10. 119.191.145.227发现威胁分析

统计期间，119.191.145.227共发现威胁1次，其中拒绝服务占比100%。具体的排名如下：



对119.191.145.227发起攻击的IP地址详情如下

暂无符合条件的数据

# 3. 威胁类型汇总

## 3.1. 拒绝服务

描述

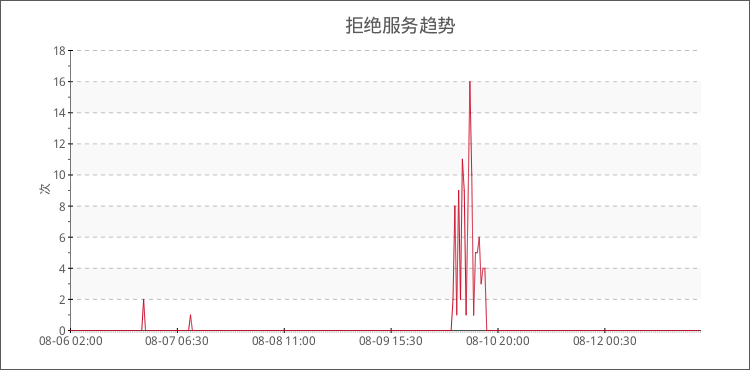
DoS/DDoS攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。这种攻击会导致资源的匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快都无法避免这种攻击带来的后果。

常见的DoS攻击有：Smurf攻击、TearDrop攻击、缓冲区溢出攻击等等；常见的DDoS攻击有TCP Syn Flood攻击、TCP ACK Flood攻击、ICMP Flood攻击、HTTP CC攻击、DNS反射攻击等。

要避免系统免受DoS攻击，网络管理员要积极谨慎地维护系统，确保无安全隐患和漏洞；而针对第三点的恶意攻击方式则需要安装防火墙等安全设备过滤DDoS攻击，同时应当定期查看安全设备的日志，及时发现对系统的安全威胁行为。

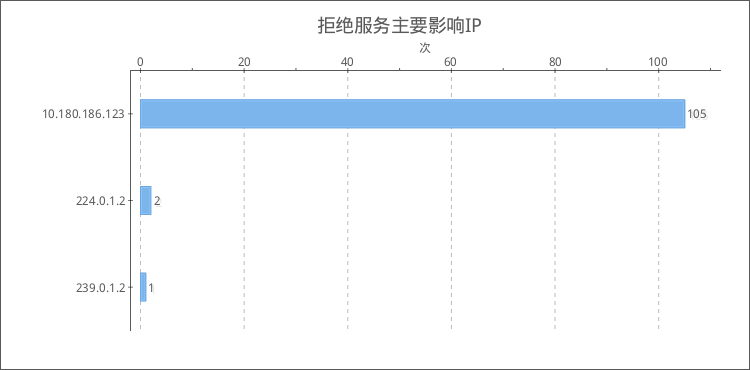
### 3.1.1. 拒绝服务趋势

统计期间共发现108次拒绝服务，平均每30分钟发现0.32次，发现最频繁的时段为 2018-08-10 12:30:00 到 2018-08-10 13:00:00，共发现威胁16次。



### 3.1.2. 拒绝服务主要影响IP

统计期间，本设备共发现3种威胁目的，其中10.180.186.123占比97.22%，224.0.1.2占比1.85%，239.0.1.2占比0.93%。具体的排名如下：

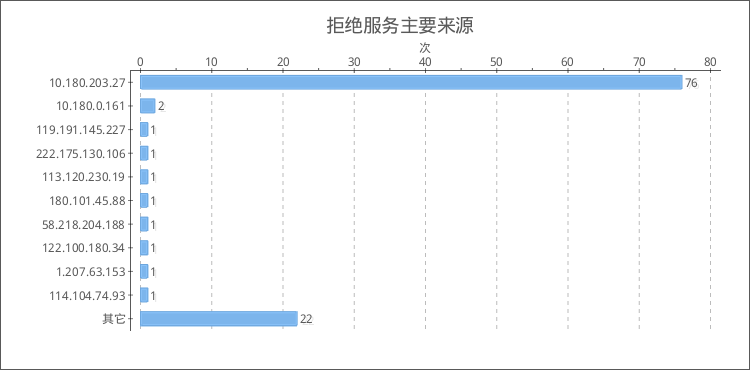


发现威胁最多的主机(IP)详情如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | 威胁目的 | 次 | 威胁源(次) | 威胁名称(次) |
| 1 | 10.180.186.123 | 105 | 10.180.203.27(76), 123.233.173.232(1), 115.205.89.53(1), 202.103.12.18(1), 61.164.72.218(1), 124.135.63.238(1), 1.207.63.153(1), 115.236.38.240(1), 218.93.208.250(1), 103.69.68.86(1) | icmp-flood(105) |
| 2 | 224.0.1.2 | 2 | 10.180.0.161(1), 10.180.185.23(1) | icmp-flood(2) |
| 3 | 239.0.1.2 | 1 | 10.180.0.161(1) | icmp-flood(1) |

### 3.1.3. 拒绝服务主要来源

统计期间，本设备共发现32种威胁源，其中10.180.203.27占比70.37%，10.180.0.161占比1.85%，119.191.145.227占比0.93%。具体的排名如下：

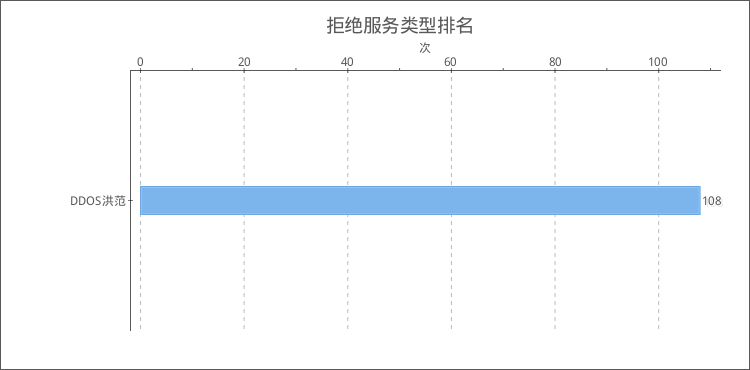


发现攻击最多的主机(IP)详情如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 威胁源 | 次 | 威胁目的(次) | 威胁名称(次) | 百分比 |
| 1 | 10.180.203.27 | 76 | 10.180.186.123(76) | icmp-flood(76) | 70.37% |
| 2 | 10.180.0.161 | 2 | 224.0.1.2(1), 239.0.1.2(1) | icmp-flood(2) | 1.85% |
| 3 | 119.191.145.227 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 4 | 222.175.130.106 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 5 | 113.120.230.19 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 6 | 180.101.45.88 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 7 | 58.218.204.188 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 8 | 122.100.180.34 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 9 | 1.207.63.153 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 10 | 114.104.74.93 | 1 | 10.180.186.123(1) | icmp-flood(1) | 0.93% |
| 11 | 其它 | 22 |  |  | 20.37% |

### 3.1.4. 拒绝服务类型排名

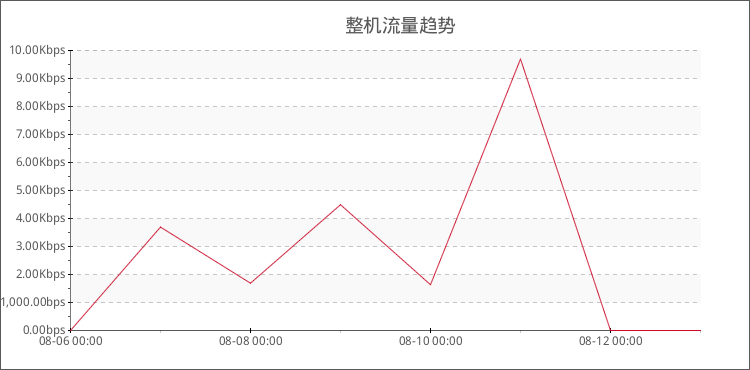
统计期间，本设备共发现1种威胁类型，其中DDOS洪范占比100%。具体的排名如下：



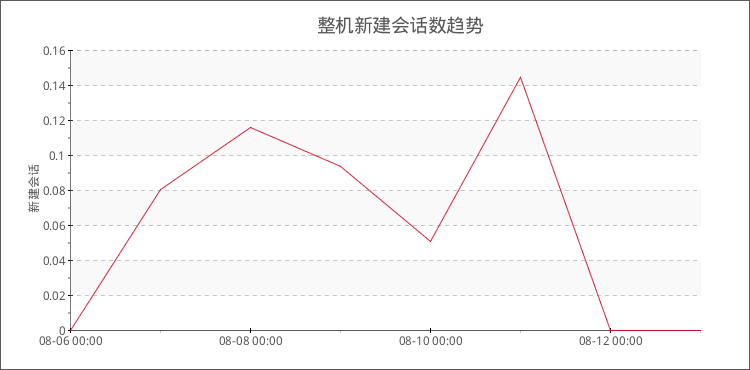
# 4. 网络流量概览

2018-08-06至2018-08-13期间，共发生流量218.42MB，其中下行流量166.10MB，上行流量52.31MB。平均每天31.20MB。主要涉及吉吉影音，BT，腾讯网等应用。排名靠前的源IP为0.0.0.0，192.168.7.32，目的IP为0.0.0.0，222.173.105.218，138.75.154.42；源国家为N\A，目的国家为中国，美国，新加坡；出安全域为trust，入安全域为trust；出接口为ethernet0/0，入接口为ethernet0/1；策略为1。

统计期间，平均带宽为2.65Kbps，峰值带宽为9.70Kbps，发生在2018-08-11 00:00:00到2018-08-12 00:00:00。



统计期间，平均新建会话数为0.06，峰值为0.1447，发生在2018-08-11 00:00:00到2018-08-12 00:00:00。

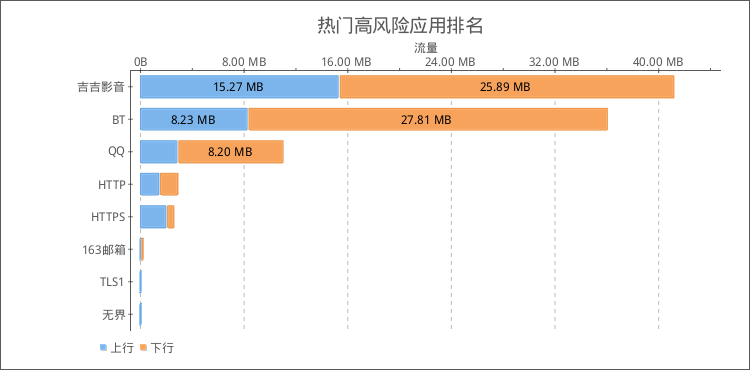


# 5. 网络流量详情

## 5.1. 应用流量分析

### 5.1.1. 热门高风险应用排名

统计期间，本设备共发生应用流量93.79MB，排名如下：

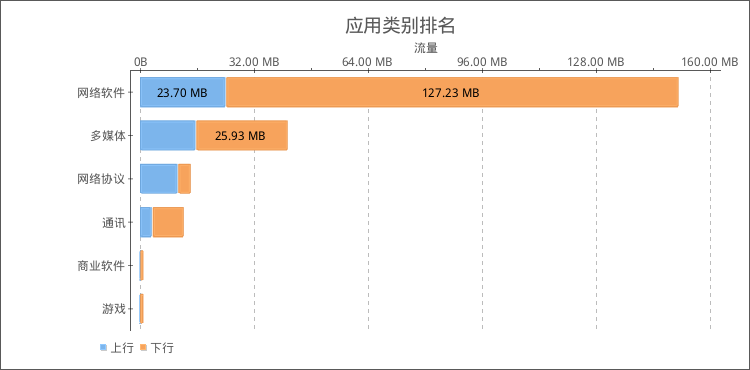


发生流量最多的应用详情如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | 应用 | 总流量 | 上行 | 下行 | 源IP(总流量 /上行 /下行) |
| 1 | 吉吉影音 | 41.16MB | 15.27MB | 25.89MB | 192.168.7.32(41.16MB/15.27MB/25.89MB) |
| 2 | BT | 36.04MB | 8.23MB | 27.81MB | 192.168.7.32(36.04MB/8.23MB/27.81MB) |
| 3 | QQ | 11.01MB | 2.82MB | 8.20MB | 0.0.0.0(7.64MB/1.97MB/5.67MB), 192.168.7.32(3.38MB/871.05KB/2.53MB) |
| 4 | HTTP | 2.86MB | 1.40MB | 1.46MB | 0.0.0.0(2.21MB/1.10MB/1.12MB), 192.168.7.32(664.29KB/309.24KB/355.05KB) |
| 5 | HTTPS | 2.56MB | 1.95MB | 628.69KB | 0.0.0.0(2.17MB/1.60MB/589.75KB), 192.168.7.32(397.05KB/358.11KB/38.94KB) |
| 6 | 163邮箱 | 155.49KB | 17.24KB | 138.25KB | 0.0.0.0(155.49KB/17.24KB/138.25KB) |
| 7 | TLS1 | 5.75KB | 5.75KB | 0.00B | 0.0.0.0(5.75KB/5.75KB/0.00B) |
| 8 | 无界 | 388.00B | 388.00B | 0.00B | 192.168.7.32(388.00B/388.00B/0.00B) |

### 5.1.2. 应用类别排名

统计期间，本设备共发生应用类别流量218.42MB，排名如下：

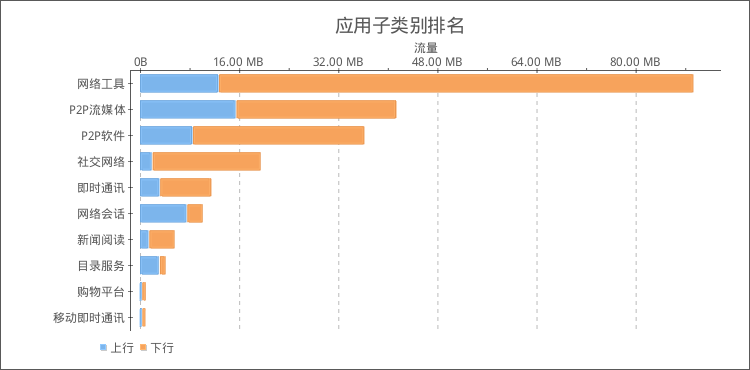


发生流量最多的应用类别详情如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | 应用类别 | 总流量 | 上行 | 下行 |
| 1 | 网络软件 | 150.93MB | 23.70MB | 127.23MB |
| 2 | 多媒体 | 41.23MB | 15.30MB | 25.93MB |
| 3 | 网络协议 | 13.99MB | 10.24MB | 3.75MB |
| 4 | 通讯 | 12.04MB | 3.05MB | 9.00MB |
| 5 | 商业软件 | 155.49KB | 17.24KB | 138.25KB |
| 6 | 游戏 | 73.01KB | 15.07KB | 57.95KB |

### 5.1.3. 应用子类别排名

统计期间，本设备共发生应用子类别流量217.99MB，排名如下：

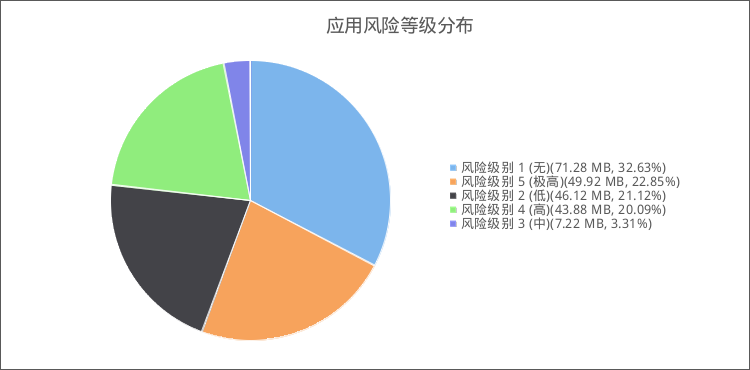


发生流量最多的应用子类别详情如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | 应用子类别 | 总流量 | 上行 | 下行 |
| 1 | 网络工具 | 89.17MB | 12.43MB | 76.73MB |
| 2 | P2P流媒体 | 41.16MB | 15.27MB | 25.89MB |
| 3 | P2P软件 | 36.04MB | 8.23MB | 27.81MB |
| 4 | 社交网络 | 19.34MB | 1.74MB | 17.60MB |
| 5 | 即时通讯 | 11.33MB | 2.96MB | 8.37MB |
| 6 | 网络会话 | 9.99MB | 7.34MB | 2.65MB |
| 7 | 新闻阅读 | 5.45MB | 1.20MB | 4.24MB |
| 8 | 目录服务 | 4.00MB | 2.90MB | 1.10MB |
| 9 | 购物平台 | 819.61KB | 72.29KB | 747.32KB |
| 10 | 移动即时通讯 | 733.36KB | 87.41KB | 645.95KB |

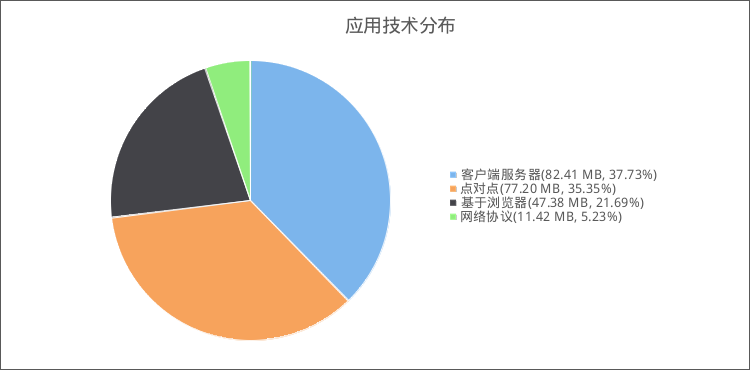
### 5.1.4. 应用风险等级分布

统计期间，本设备共发现5种风险等级，其中风险级别 1 (无)占比32.63%，风险级别 5 (极高)占比22.85%，风险级别 2 (低)占比21.12%。具体的分布图如下：



### 5.1.5. 应用技术分布

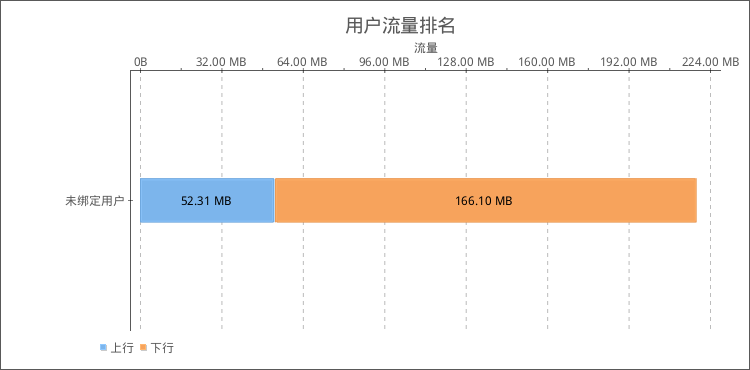
统计期间，本设备共发现4种应用技术，其中客户端服务器占比37.73%，点对点占比35.35%，基于浏览器占比21.69%。具体的分布图如下：



## 5.2. IP流量分析

### 5.2.1. 用户流量排名

统计期间，本设备共发现1种源用户，其中未绑定用户占比100%。具体的排名如下：

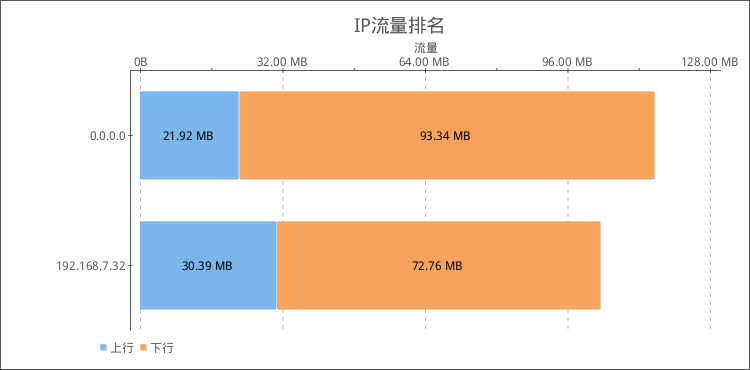


发生流量最多的源用户详情如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 用户 | 总流量 | 上行 | 下行 | 目的IP(总流量 /上行 /下行) | 应用 (总流量 /上行 /下行) |
| 1 | 未绑定用户 | 218.42MB | 52.31MB | 166.10MB | 0.0.0.0(115.26MB/21.92MB/93.34MB), 222.173.105.218(10.23MB/256.60KB/9.98MB), 138.75.154.42(8.09MB/350.82KB/7.75MB), 138.75.151.14(6.71MB/163.46KB/6.55MB), 61.48.181.75(4.33MB/398.03KB/3.94MB), 119.165.189.5(4.08MB/2.75MB/1.33MB), 1.26.180.119(3.61MB/227.96KB/3.39MB), 23.75.13.233(3.35MB/222.41KB/3.13MB), 103.235.46.82(2.00MB/1.08MB/943.30KB), 49.77.46.94(1.89MB/938.51KB/997.19KB) | 吉吉影音(41.16MB/15.27MB/25.89MB), BT(36.04MB/8.23MB/27.81MB), 腾讯网(31.84MB/2.49MB/29.35MB), 网易网(22.61MB/2.30MB/20.31MB), 搜狗网(19.05MB/1.59MB/17.46MB), 百度网(13.14MB/2.06MB/11.08MB), QQ(11.01MB/2.82MB/8.20MB), 百度地图(9.50MB/4.49MB/5.01MB), 阿里云(5.75MB/229.62KB/5.52MB), 网易新闻(5.31MB/1.19MB/4.12MB) |

### 5.2.2. IP流量排名

统计期间，本设备共发现2种源IP，其中0.0.0.0占比52.77%，192.168.7.32占比47.23%。具体的排名如下：

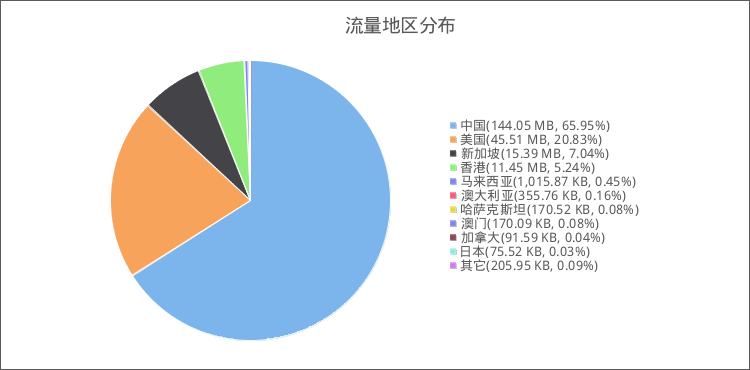


发生流量最多的源IP详情如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | 源IP | 总流量 | 上行 | 下行 | 目的IP(总流量 /上行 /下行) | 应用 (总流量 /上行 /下行) |
| 1 | 0.0.0.0 | 115.26MB | 21.92MB | 93.34MB | 0.0.0.0(115.26MB/21.92MB/93.34MB) | 腾讯网(23.79MB/1.91MB/21.88MB), 网易网(22.61MB/2.30MB/20.31MB), 百度网(13.14MB/2.06MB/11.08MB), 搜狗网(12.52MB/1.12MB/11.40MB), 百度地图(7.72MB/3.61MB/4.11MB), QQ(7.64MB/1.97MB/5.67MB), 阿里云(5.75MB/229.62KB/5.52MB), 网易新闻(4.82MB/946.16KB/3.90MB), DNS(3.49MB/2.61MB/901.46KB), HTTP(2.21MB/1.10MB/1.12MB) |
| 2 | 192.168.7.32 | 103.15MB | 30.39MB | 72.76MB | 222.173.105.218(10.23MB/256.60KB/9.98MB), 138.75.154.42(8.09MB/350.82KB/7.75MB), 138.75.151.14(6.71MB/163.46KB/6.55MB), 61.48.181.75(4.33MB/398.03KB/3.94MB), 119.165.189.5(4.08MB/2.75MB/1.33MB), 1.26.180.119(3.61MB/227.96KB/3.39MB), 23.75.13.233(3.35MB/222.41KB/3.13MB), 103.235.46.82(2.00MB/1.08MB/943.30KB), 49.77.46.94(1.89MB/938.51KB/997.19KB), 27.214.49.59(1.87MB/768.98KB/1.12MB) | 吉吉影音(41.16MB/15.27MB/25.89MB), BT(36.04MB/8.23MB/27.81MB), 腾讯网(8.04MB/583.76KB/7.47MB), 搜狗网(6.53MB/482.44KB/6.06MB), QQ(3.38MB/871.05KB/2.53MB), TCP-ANY(2.66MB/2.41MB/261.75KB), 百度地图(1.79MB/904.89KB/925.35KB), HTTP(664.29KB/309.24KB/355.05KB), DNS(517.05KB/295.93KB/221.12KB), 网易新闻(494.44KB/267.47KB/226.98KB) |

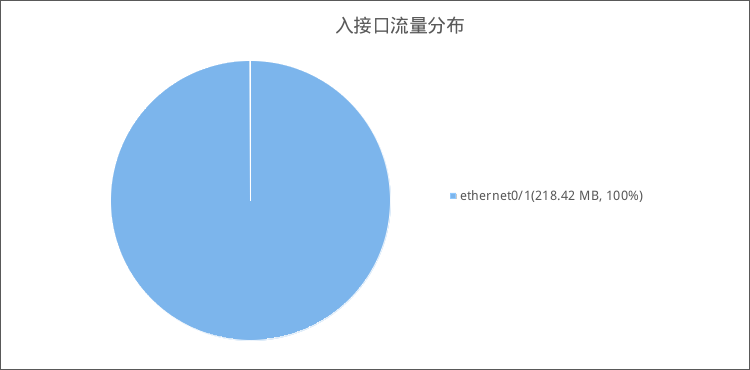
### 5.2.3. 流量地区分布

统计期间，本设备共发现33种国家/地区，其中中国占比65.95%，美国占比20.83%，新加坡占比7.04%。具体的分布图如下：

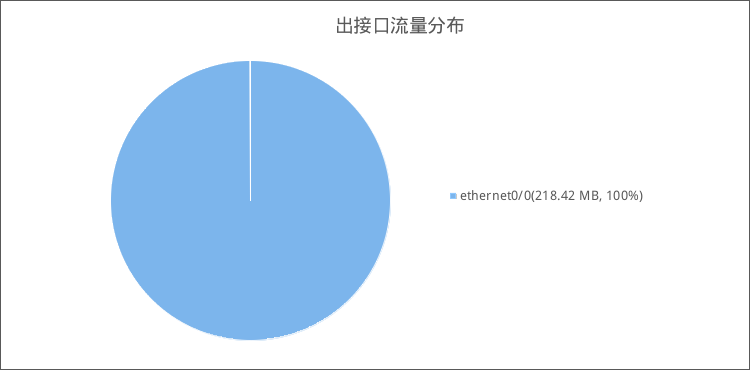


## 5.3. 接口流量分析

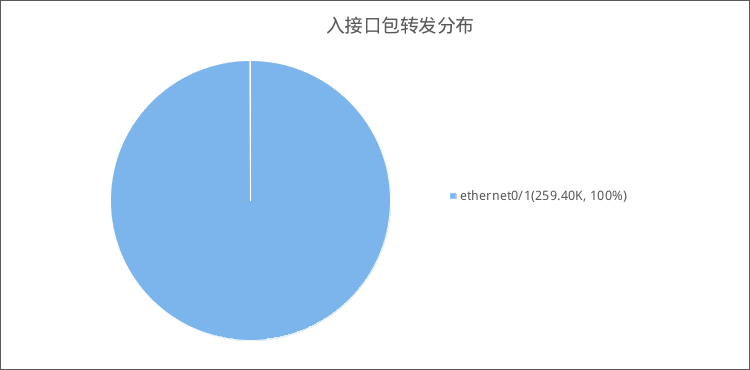
统计期间，本设备共发生入接口流量218.42MB，其中ethernet0/1占比100%。具体的分布图如下：



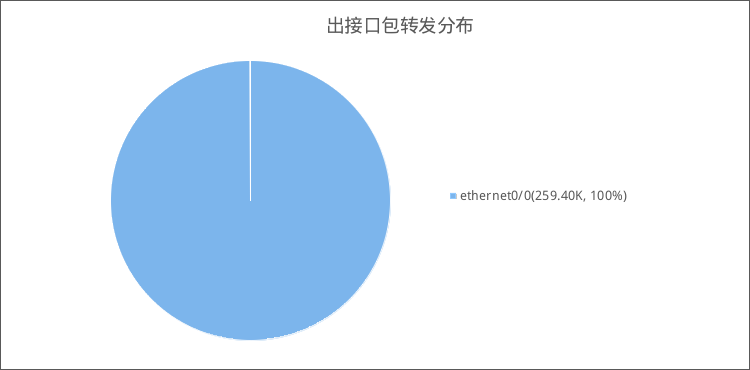
统计期间，本设备共发生出接口流量218.42MB，其中ethernet0/0占比100%。具体的分布图如下：



统计期间，本设备共发生入接口数据包259.40K，其中ethernet0/1占比100%。具体的分布图如下：

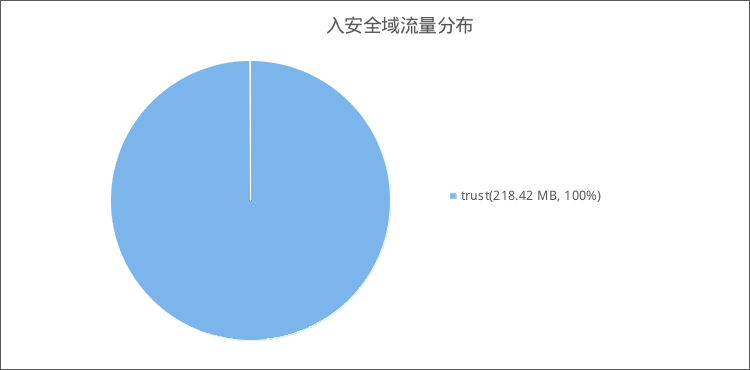


统计期间，本设备共发生出接口数据包259.40K，其中ethernet0/0占比100%。具体的分布图如下：

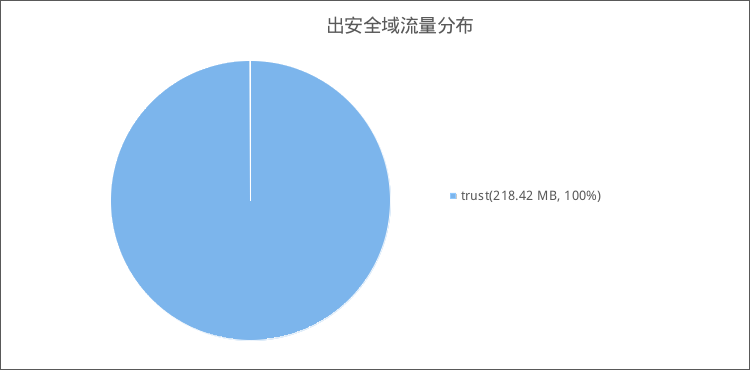


## 5.4. 安全域流量分析

统计期间，本设备共发生入安全域流量218.42MB，其中trust占比100%。具体的分布图如下：

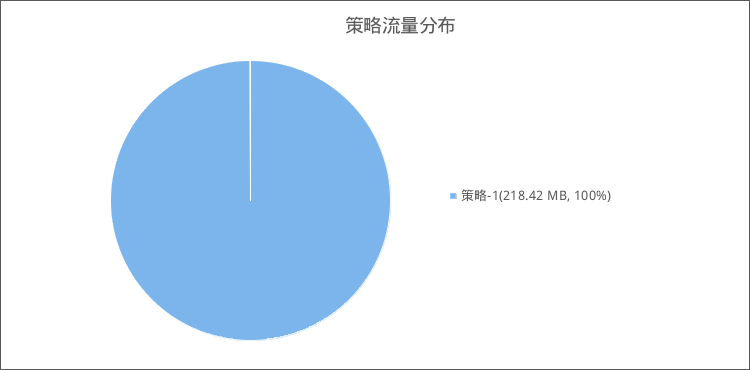


统计期间，本设备共发生出安全域流量218.42MB，其中trust占比100%。具体的分布图如下：



## 5.5. 策略流量分析

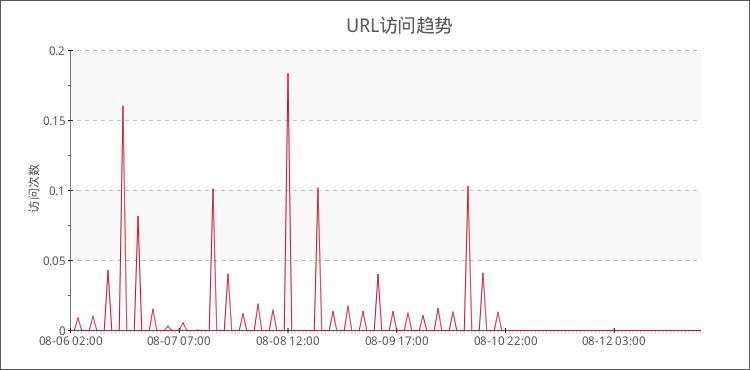
统计期间，本设备共发生策略流量218.42MB，其中策略-1占比100%。具体的分布图如下：



# 6. URL内容概览

2018-08-06至2018-08-13期间，用户共访问URL 3989 次，平均每天 570 次，共涉及 123 条URL。其中未分类URL访问最为频繁，用户经常访问的URL包括d3g.qq.com，pinghot.qq.com，cms-bucket.nosdn.127.net等。访问URL最活跃的用户包括192.168.7.32等。

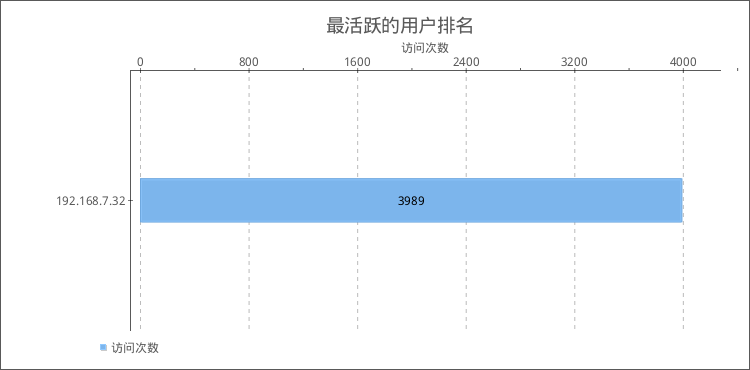
统计期间，平均每秒访问URL 0.01 次，峰值为 0.18 次，发生在2018-08-08 12:00:00到2018-08-08 13:00:00。



# 7. URL访问详情

## 7.1. 最活跃的用户排名

统计期间，本设备共发现1种用户，其中192.168.7.32占比100%。具体的排名如下：

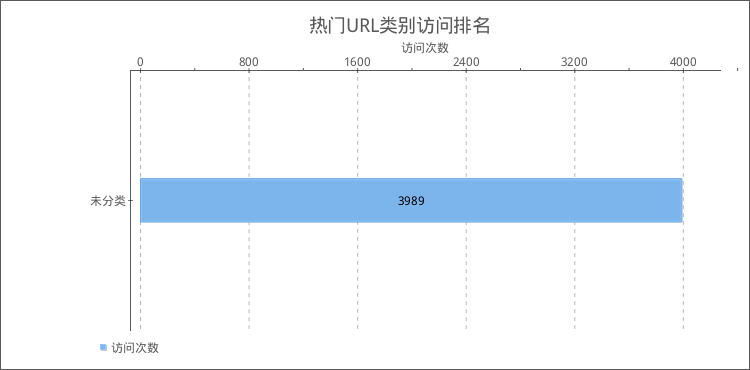


访问最多的用户详情如下：

|  |  |  |  |
| --- | --- | --- | --- |
| # | 用户 | 访问次数 | URL/访问次数 |
| 1 | 192.168.7.32 | 3989 | d3g.qq.com(782), pinghot.qq.com(632), cms-bucket.nosdn.127.net(559), temp.163.com(501), ping.pinyin.sogou.com(182), pub.idqqimg.com(176), config.pinyin.sogou.com(154), info.pinyin.sogou.com(126), pic-bucket.nosdn.127.net(91), p3p.sogou.com(65) |

## 7.2. 热门URL类别访问排名

统计期间，本设备共发现1种URL类别，其中未分类占比100%。具体的排名如下：

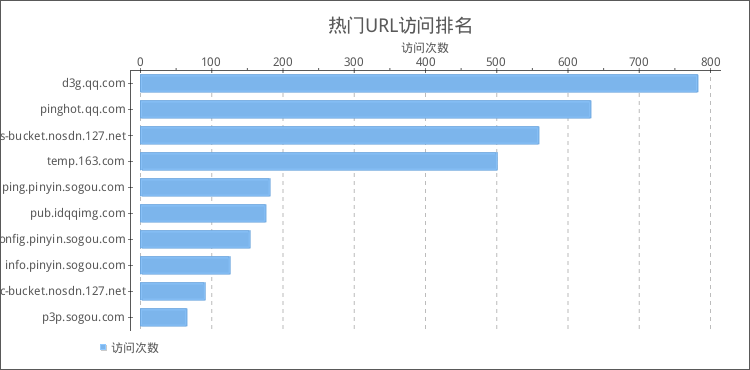


访问最多的URL类别详情如下：

|  |  |  |  |
| --- | --- | --- | --- |
| # | URL类别 | 访问次数 | 用户(IP)/访问次数 |
| 1 | 未分类 | 3989 | 192.168.7.32(3989) |

## 7.3. 热门URL访问排名

统计期间，本设备共发现10种URL，其中d3g.qq.com占比23.93%，pinghot.qq.com占比19.34%，cms-bucket.nosdn.127.net占比17.11%。具体的排名如下：



访问最多的URL详情如下：

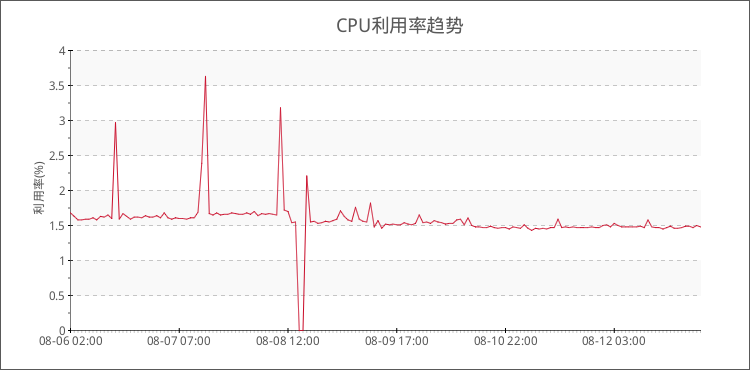
|  |  |  |  |
| --- | --- | --- | --- |
| # | URL | 访问次数 | 用户(IP)/访问次数 |
| 1 | d3g.qq.com | 782 | 192.168.7.32(782) |
| 2 | pinghot.qq.com | 632 | 192.168.7.32(632) |
| 3 | cms-bucket.nosdn.127.net | 559 | 192.168.7.32(559) |
| 4 | temp.163.com | 501 | 192.168.7.32(501) |
| 5 | ping.pinyin.sogou.com | 182 | 192.168.7.32(182) |
| 6 | pub.idqqimg.com | 176 | 192.168.7.32(176) |
| 7 | config.pinyin.sogou.com | 154 | 192.168.7.32(154) |
| 8 | info.pinyin.sogou.com | 126 | 192.168.7.32(126) |
| 9 | pic-bucket.nosdn.127.net | 91 | 192.168.7.32(91) |
| 10 | p3p.sogou.com | 65 | 192.168.7.32(65) |

# 8. 系统运行状况

## 8.1. 系统资源利用率

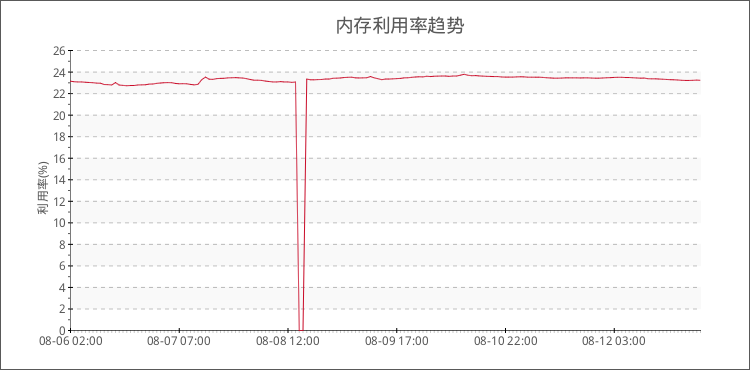
### 8.1.1. CPU利用率趋势

统计期间，平均利用率为1.58，峰值利用率为3.63，发生在2018-08-07 14:00:00到2018-08-07 15:00:00。



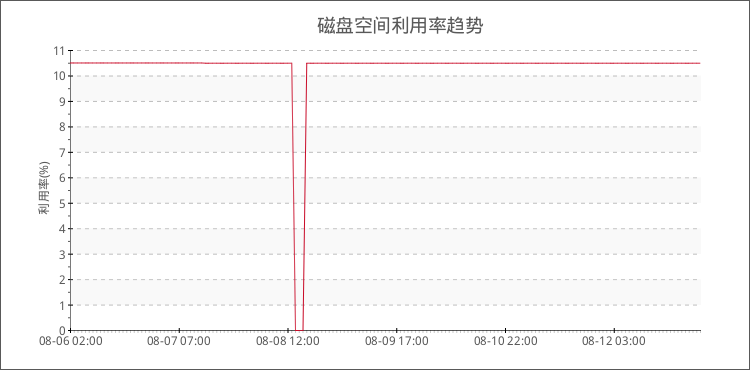
### 8.1.2. 内存利用率趋势

统计期间，平均利用率为23.05，峰值利用率为23.79，发生在2018-08-10 11:00:00到2018-08-10 12:00:00。



### 8.1.3. 磁盘空间利用率趋势

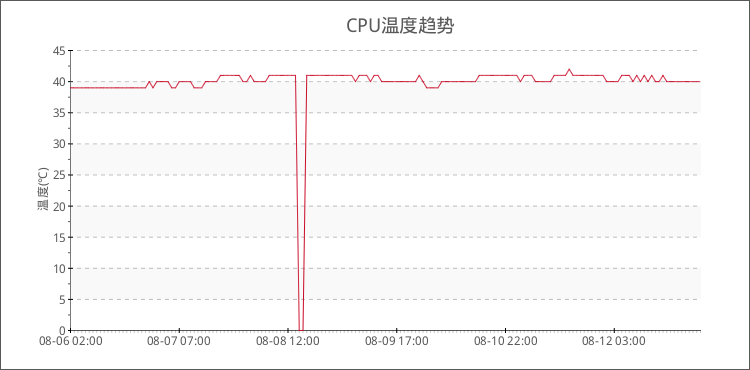
统计期间，平均利用率为10.32，峰值利用率为10.51，发生在2018-08-06 02:00:00到2018-08-06 03:00:00。



## 8.2. 系统温度

### 8.2.1. CPU温度趋势

统计期间，平均温度为39.76，峰值温度为42，发生在2018-08-11 15:00:00到2018-08-11 16:00:00。



### 8.2.2. 机箱温度趋势

统计期间，平均温度为43.49，峰值温度为45，发生在2018-08-07 18:00:00到2018-08-07 19:00:00。

