**山东海事局海上船舶异常行为自动监测项目**

**网络环境测试报告**

**一、测试条件**

工具： tcpdump

netcat

NetAssist

python脚本

服务器：198.15.20.100（青岛）

198.15.20.102（青岛）

​台位： 198.15.108.109（威海）

198.15.108.79（威海）

198.15.19.39（VPN）

**二、测试记录**

1、测试列表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 编号 | 发送端IP | 发送PORT | 接收端IP | 接收PORT | 发送报文数 | 接收报文数 | 是否阻断 |
| 1 | 198.15.108.109  威海 | 6881 | 198.15.20.102  青岛 | 6880 | 50 | 15 | 是 |
| 2 | 6882 | 6880 | 50 | 15 | 是 |
| 3 | 6883 | 6880 | 50 | 15 | 是 |
| 4 | 6883 | 6881 | 50 | 15 | 是 |
| 5 | 6881 | 6881 | 50 | 15 | 是 |
| 6 | 6882 | 6880 | 50 | 15 | 是 |
| 7 | 198.15.108.109  威海 | 6881 | 198.15.19.39  VPN | 6881 | 30 | 15 | 是 |
| 8 | 198.15.19.39  VPN | 6882 | 198.15.108.109  威海 | 6882 | 30 | 15 | 是 |
| 9 | 198.15.20.102  青岛 | 6883 | 198.15.19.39  VPN | 6883 | 30 | 30 | 否 |
| 10 | 198.15.19.39  VPN | 6881 | 198.15.20.102  青岛 | 6881 | 30 | 15 | 是 |
| 11 | 198.15.20.102  青岛 | 6882 | 198.15.108.109  威海 | 6882 | 30 | 15 | 是 |
| 12 | 198.15.20.102  青岛 | 6881 | 198.15.108.109  威海 | 6881 | 30 | 30 | 否 |
| 13 | 198.15.108.79  威海 | 6881 | 198.15.108.109  威海 | 6881 | 30 | 30 | 否 |
| 14 | 198.15.108.109  威海 | 6882 | 198.15.108.79  威海 | 6882 | 30 | 30 | 否 |
| 15 | 198.15.20.100  青岛 | 6881 | 198.15.20.102  青岛 | 6881 | 30 | 30 | 否 |
| 16 | 198.15.20.102  青岛 | 6882 | 198.15.20.100  青岛 | 6882 | 30 | 30 | 否 |

2、具体案例

（1）威海局198.15.108.109台位向山东局服务器198.15.20.102服务器发送UDP报文，发送15条后被阻断

图1 威海局发送端

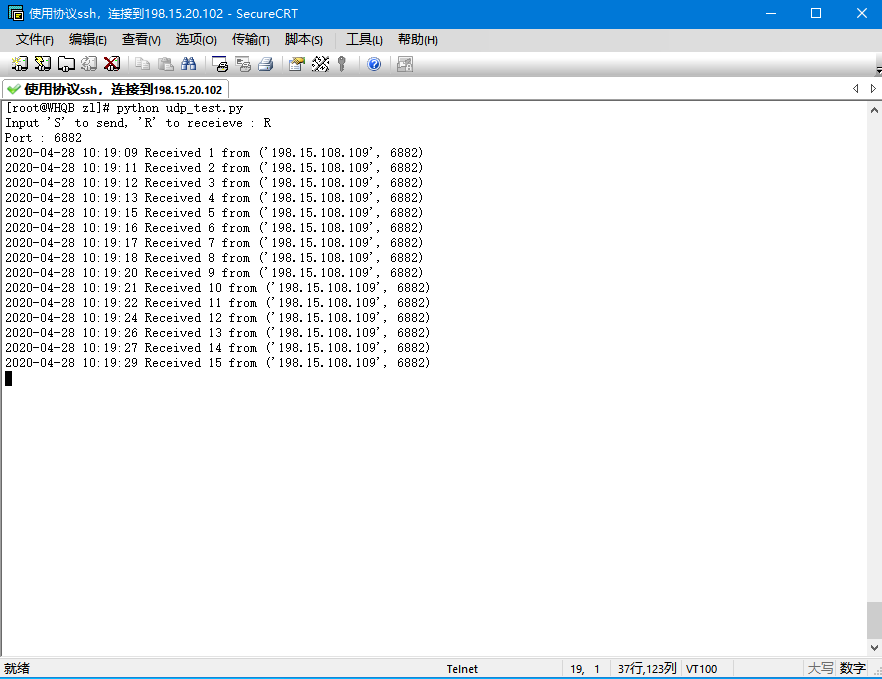


图2 山东局接收端

（2）山东局服务器198.15.20.102服务器向威海局198.15.108.109台位发送UDP报文，发送15条后被阻断

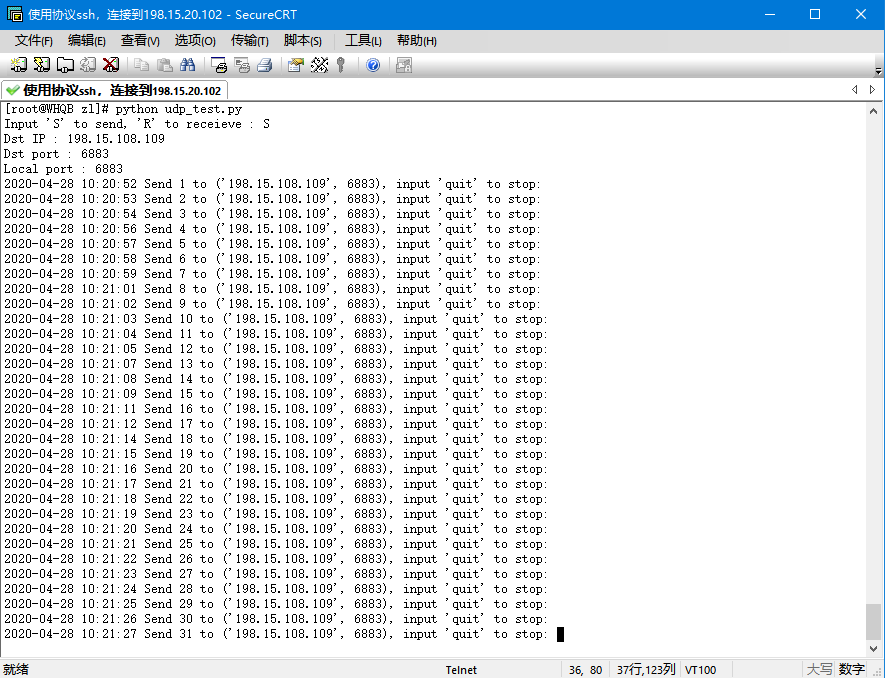


图3 山东局发送端

图4 威海局接收端

（3）VPN 198.15.19.39台位向山东局198.15.20.102服务器发送UDP报文，发送15条后被阻断

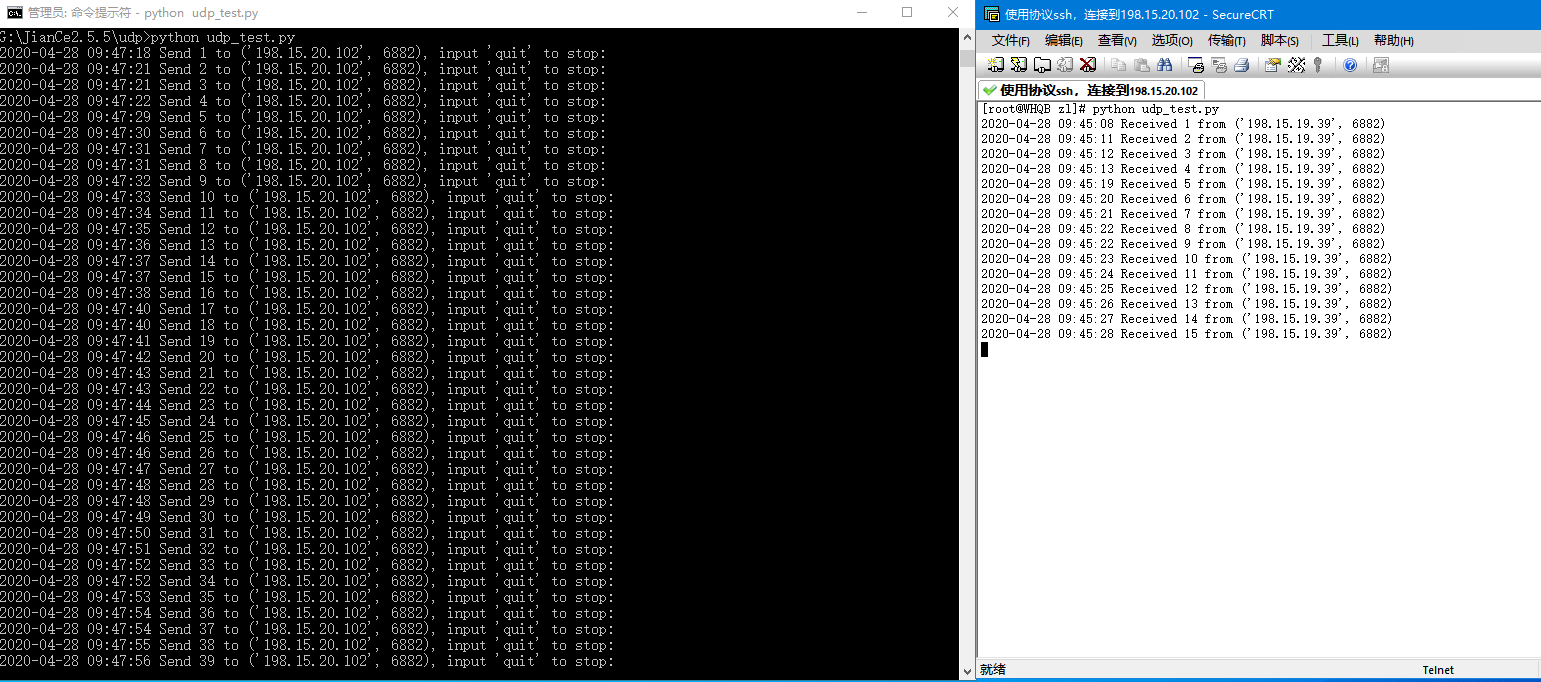


图5 VPN发送端

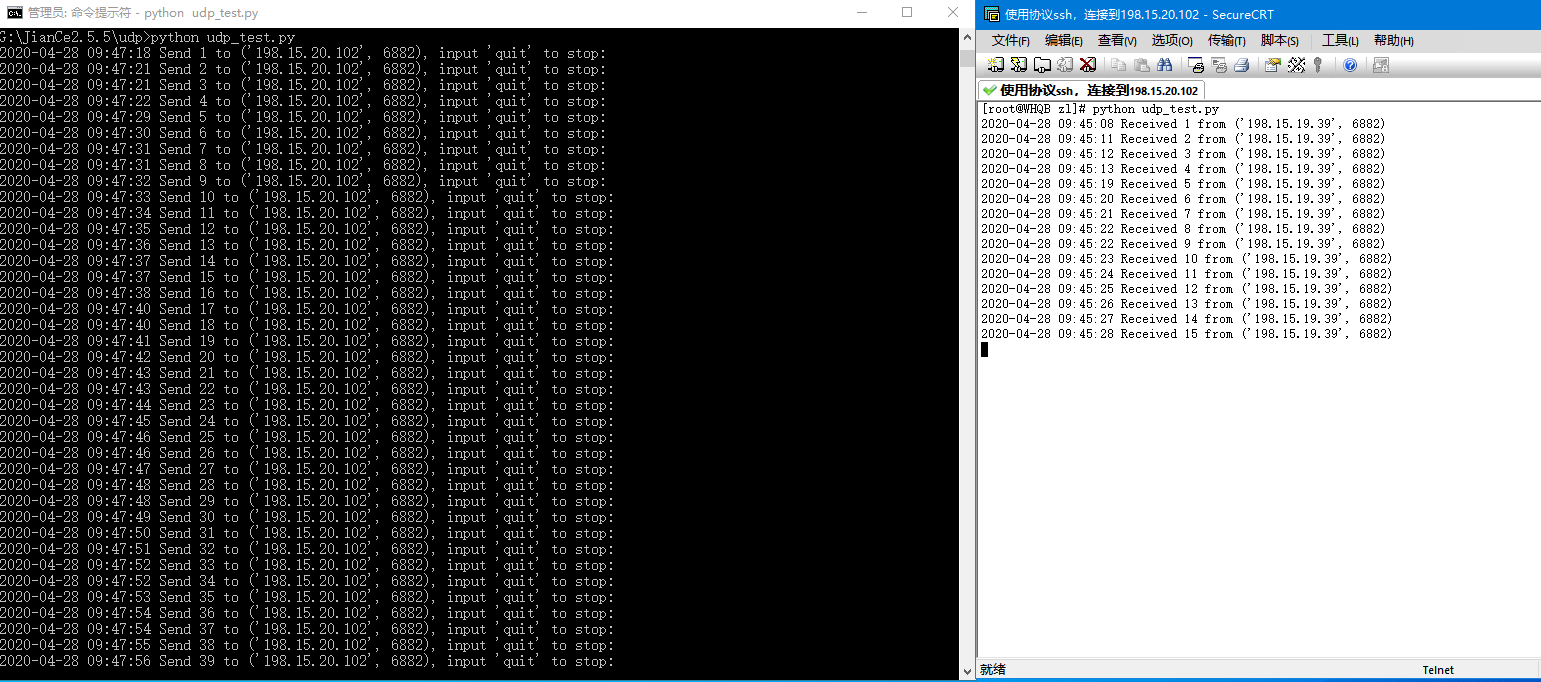


图6 山东局接收端

（4）VPN 198.15.19.39台位向威海局198.15.108.109台位发送UDP报文，发送15条后被阻断

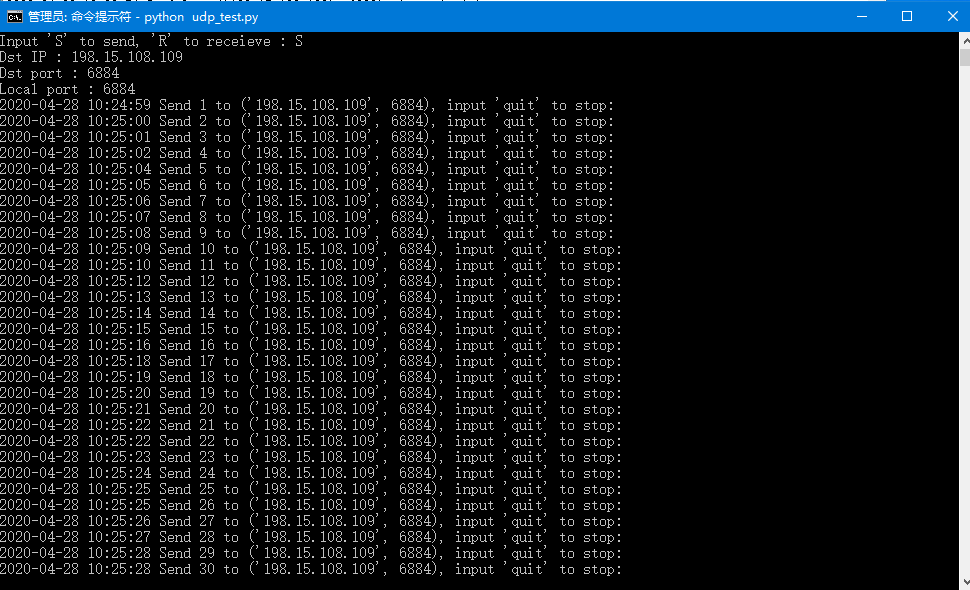


图7 VPN发送端

图8 威海局接收端

**三、测试结果描述**

1、威海局台位向山东局服务器发送UDP报文，每秒1条连续发送15条后被阻断，冷却约两分钟后恢复

2、VPN台位向山东局服务器发送UDP报文，每秒1条连续发送15条后被阻断，冷却约两分钟后恢复

3、威海局台位向VPN台位发送UDP报文，每秒1条连续发送15条后被阻断，冷却约两分钟后恢复

4、VPN台位向威海局台位发送UDP报文，每秒1条连续发送15条后被阻断，冷却约两分钟后恢复

5、UDP被阻断后，尝试更改发送或接收方端口，报文发送畅通，连续发送15条后被阻断

6、山东局服务器向威海局台位发送UDP报文，每秒1条连续发送，偶尔被阻断，部分情况可连续发送

7、山东局服务器向VPN台位发送UDP报文，每秒1条连续发送，偶尔被阻断，部分情况可连续发送

8、山东局内部两台服务器互发UDP报文，每秒1条连续发送，不会被阻断可连续发送

9、威海局内部两台台位互发UDP报文，每秒1条连续发送，不会被阻断可连续发送

**四、疑似问题**

山东局服务器、交换机、防火墙等设备，可能被设置了某种安全策略，在收到密集UDP报文时会临时中断点对点UDP收发。山东局向外发送UDP报文时偶尔会触发该策略，但不必然出现。山东局内部服务器、威海局内部台位之间发送UDP报文不会触发该策略。