

用cisco命令确定和跟踪DOS攻击源 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/251/2021_2022__E7_94_A8cisco_E5_91_c101_251056.htm

今天ISP所面临的最大的挑战之一是跟踪和阻止denial of service (DoSattacks)。对付DoS attack有三个步骤：intrusion detection，source tracking，and blocking. 本命令是针对source tracking. 1、配置举例：本例说明怎样在路由器上所有line cards/port adapters，为了让每

块line card or port adapter收集到主机 100.10.0.1 (被攻击的机器) 的数据流。两分钟后生成 log日志。记录在log的数据包和流每60秒向GRP/RSP 导出以方便察看。Router# configure

```
interfaceRouter(config)# ip source-track 100.10.0.1Router(config)# ip source-track syslog-interval 2Router(config)# ip source-track export-interval 60
```

显示到达源端口的攻击包的源地址及流量

```
Router# show ip source-track
```

Address	SrcIF	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	PO2/0	0	0	0	0
192.168.9.9	PO1/2	131M	511M	1538	6192
192.168.9.9	PO2/0	144G	3134M	6619923	143909

显示所有攻击源

条目：2、Cisco IOS feature 配置 TCP Intercept (防止 Denial-of-Service Attacks) 配置路由器以保护服务器免收 TCP SYN-flooding attacks. 以下配置定义了一个扩展access list 101，保护192.168.1.0/24网段的服务器：

```
Router# show ip source-track summary
```

Address	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	0	0	0	0
100.10.1.1	131M	511M	1538	6192
192.168.9.9	146G	3178M	6711866	145908

show tcp intercept connections 显示不完全和已建TCP连接

100Test 下载频道开通，各类考试题目直接下载。详细请访问

www.100test.com