

如何利用ASA发现DDOS攻击以及应急预案

目录

[案例分析网络拓扑结构](#)

[目的](#)

[地址规划](#)

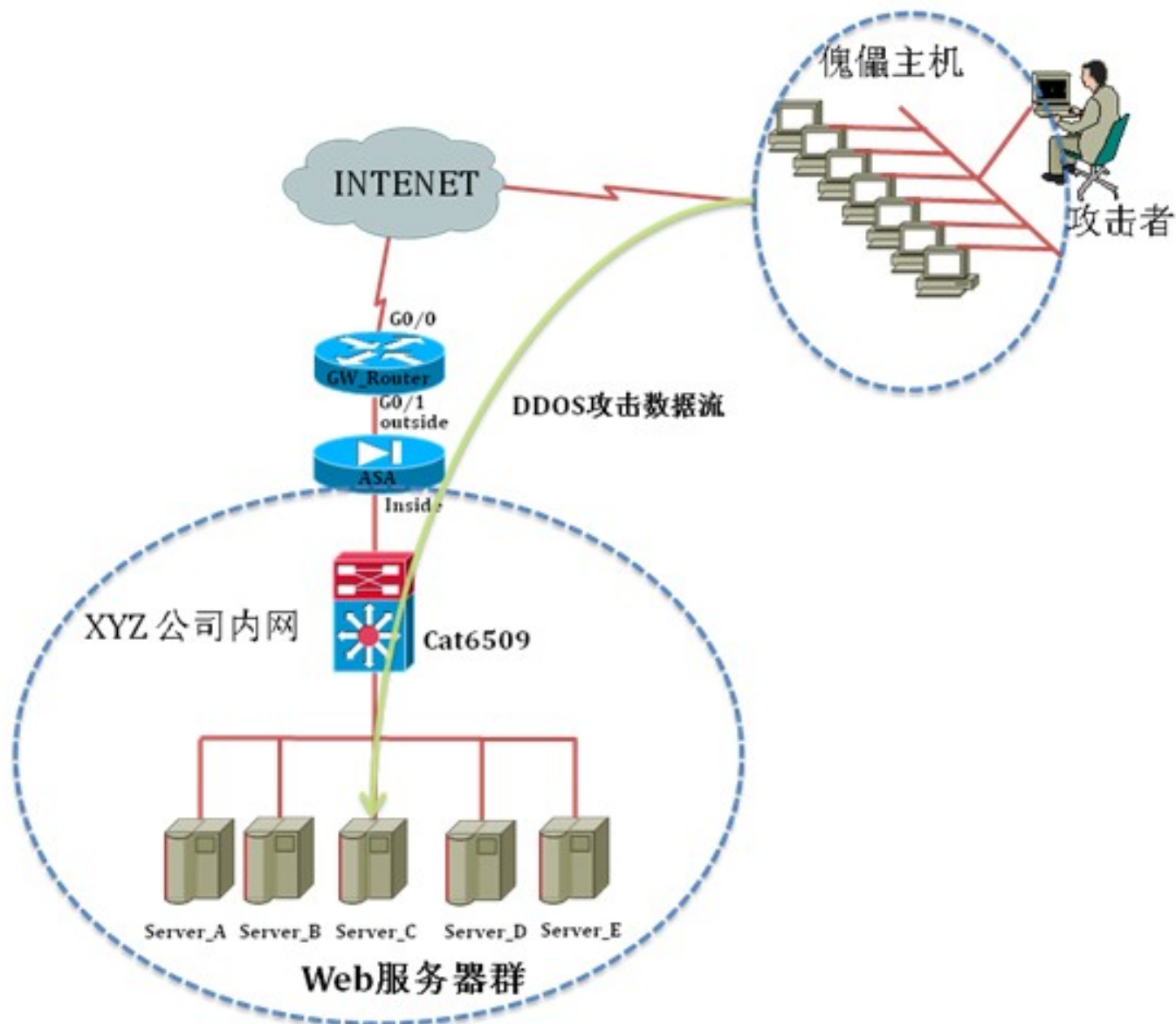
[案例描述](#)

[排错工具](#)

[如何利用ASA发现并应急处理DDOS攻击](#)

[案例结果](#)

案例分析网络拓扑结构



目的

在阅读完本案例后，可以利用ASA发现并应急处理TCP 泛洪类的DDOS攻击。

地址规划

Server C

真实地址是10.1.1.50

地址转换后的地址是192.168.1.50

案例描述

在一个周一的早上，XYZ公司的网络管理员突然接到员工报障，反映打开位于Web服务器群的Server_C网页很慢甚至无法打开。接到报障后XYZ公司的管理员马上检查路由器的相关信息，除了入口流量大以外，在路由器侧没有任何异常，此时该管理员将目光投向了ASA。

排错工具

- 1) ASDM
- 2) Show 命令

如何利用ASA发现并应急处理DDOS攻击

- 1) 通过ASDM发现每秒的TCP连接数突增。



2) 利用 show perfmon 命令检查连接状态，发现每秒的TCP连接数高达2059个，半开连接数量则是1092个每秒。从公司的日常记录看，此时这两个连接数量属于不正常的范围。

```

ASA-5510# show perfmon

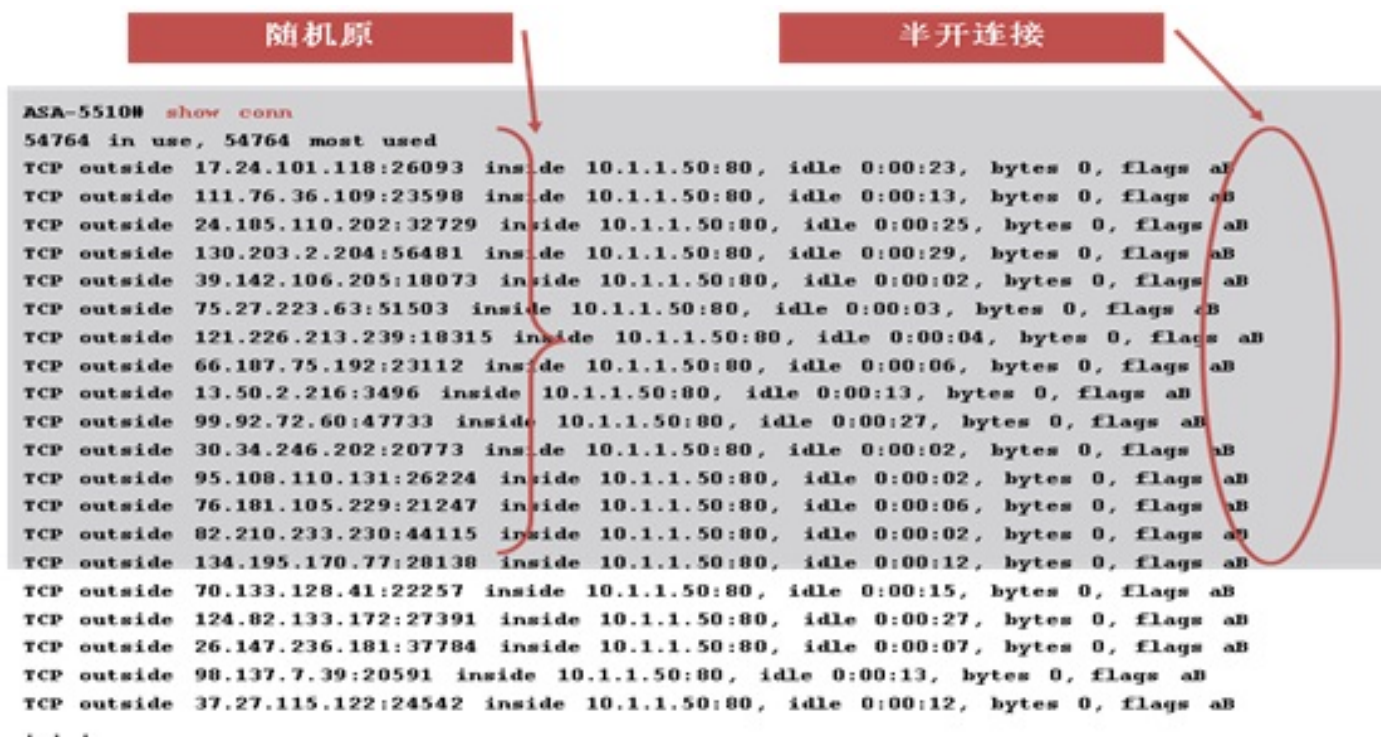
PERFMON STATS:
Xlates          0/s          0/s
Connections     2059/s       299/s
TCP Conns       2059/s       299/s
UDP Conns       0/s          0/s
URL Access      0/s          0/s
URL Server Req  0/s          0/s
TCP Fixup       0/s          0/s
TCP Intercept Established Conns 0/s          0/s
TCP Intercept Attempts 0/s          0/s
TCP Embryonic Conns Timeout 1092/s       4/s
HTTP Fixup      0/s          0/s
FTP Fixup       0/s          0/s
AAA Authen      0/s          0/s
AAA Author      0/s          0/s
AAA Account     0/s          0/s

VALID CONNS RATE in TCP INTERCEPT:
Current         Average
N/A             95.00%

ASA-5510#

```

3) 利用show conn命令察看不正常连接的具体信息，例如源/目的地址以及源/目的端口。在本案例中发现随机的源地址和端口去访问相同的目的地10.1.1.50的80端口，并且这些TCP的连接都是半开连接属于TCP SYN泛洪攻击。



The screenshot shows the output of the 'show conn' command on an ASA-5510H device. The output lists 20 TCP connections, all in an 'idle' state. Each connection originates from a different random source IP address and port on the 'outside' interface and is destined for the 'inside' interface at 10.1.1.50:80. The flags for all connections are 'aB', indicating they are half-open (SYN received). Two red boxes at the top of the image highlight the '随机原' (Random Source) and '半开连接' (Half-open connection) aspects. A red oval on the right side of the output highlights the flags 'aB' for several connections.

```
ASA-5510H show conn
54764 in use, 54764 most used
TCP outside 17.24.101.118:26093 inside 10.1.1.50:80, idle 0:00:23, bytes 0, flags aB
TCP outside 111.76.36.109:23598 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 24.185.110.202:32729 inside 10.1.1.50:80, idle 0:00:25, bytes 0, flags aB
TCP outside 130.203.2.204:56481 inside 10.1.1.50:80, idle 0:00:29, bytes 0, flags aB
TCP outside 39.142.106.205:18073 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 75.27.223.63:51503 inside 10.1.1.50:80, idle 0:00:03, bytes 0, flags aB
TCP outside 121.226.213.239:18315 inside 10.1.1.50:80, idle 0:00:04, bytes 0, flags aB
TCP outside 66.187.75.192:23112 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 13.50.2.216:3496 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 99.92.72.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
TCP outside 30.34.246.202:20773 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 95.108.110.131:26224 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 76.181.105.229:21247 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 82.210.233.230:44115 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 134.195.170.77:28138 inside 10.1.1.50:80, idle 0:00:12, bytes 0, flags aB
TCP outside 70.133.128.41:22257 inside 10.1.1.50:80, idle 0:00:15, bytes 0, flags aB
TCP outside 124.82.133.172:27391 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
TCP outside 26.147.236.181:37784 inside 10.1.1.50:80, idle 0:00:07, bytes 0, flags aB
TCP outside 98.137.7.39:20591 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 37.27.115.122:24542 inside 10.1.1.50:80, idle 0:00:12, bytes 0, flags aB
. . .
```

4) 利用ASDM发现半开 (TCP SYN 泛洪) 攻击存在，并且连接数量突增。



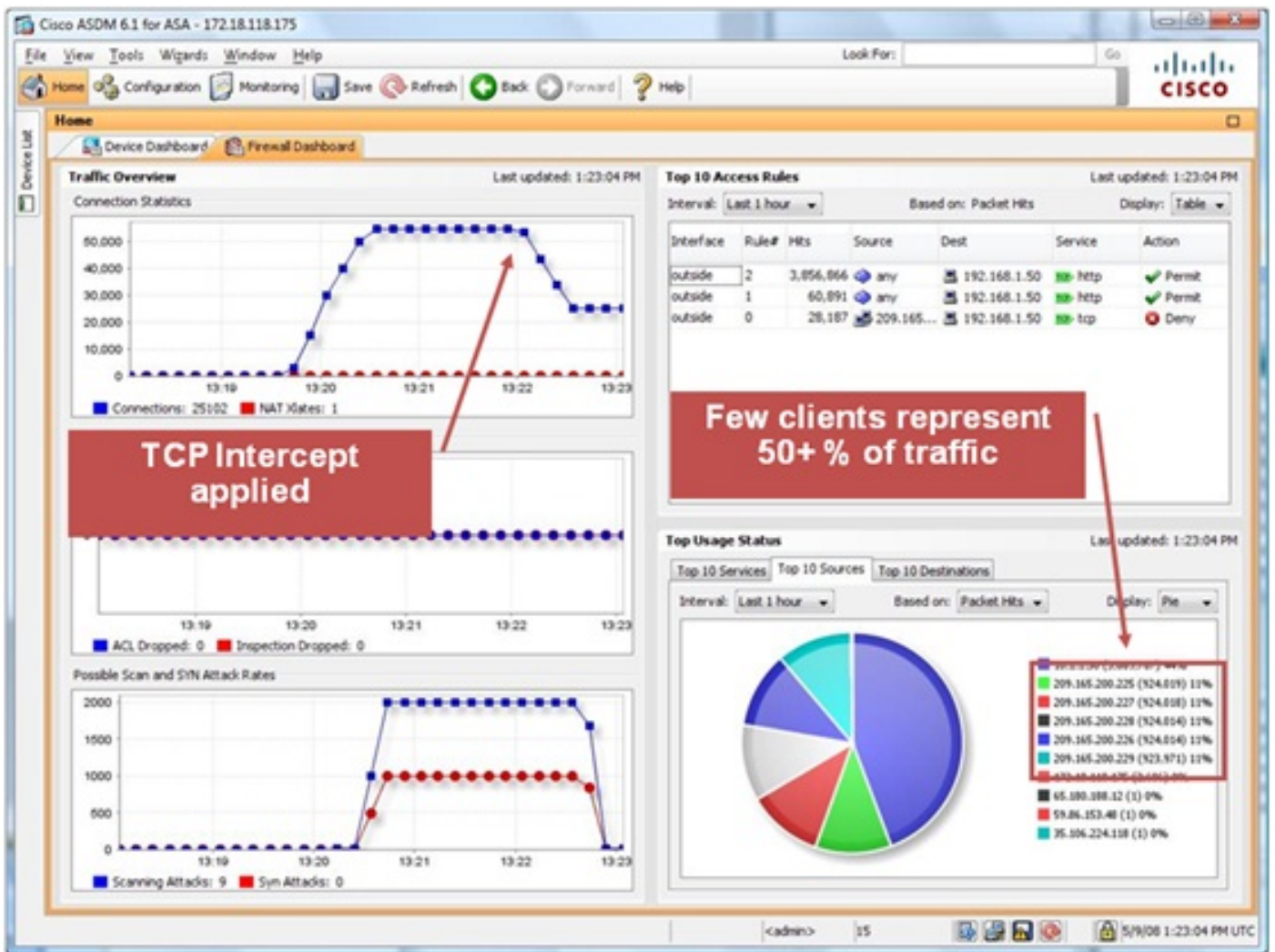
5) 利用TCP Intercept机制应急处理TCP的半开连接攻击。利用ACL及Class-Map来分类流量，在Policy-Map下限制最大的半开连接数，在本案例中为100。

```

access-list 140 extended permit tcp any host 192.168.1.50 eq www
!
class-map protect
  description Protect web server from attacks
  match access-list 140
!
policy-map interface_policy
  class protect
    set connection embryonic-conn-max 100
!
service-policy interface_policy interface outside

```

6) 利用ASDM检查，是否TCP intercept机制起效。由此可见连接数和TCP SYN攻击的曲线都有所下降。所以证明TCP intercept机制生效。但是总连接数还是处于一个不正常的状态。



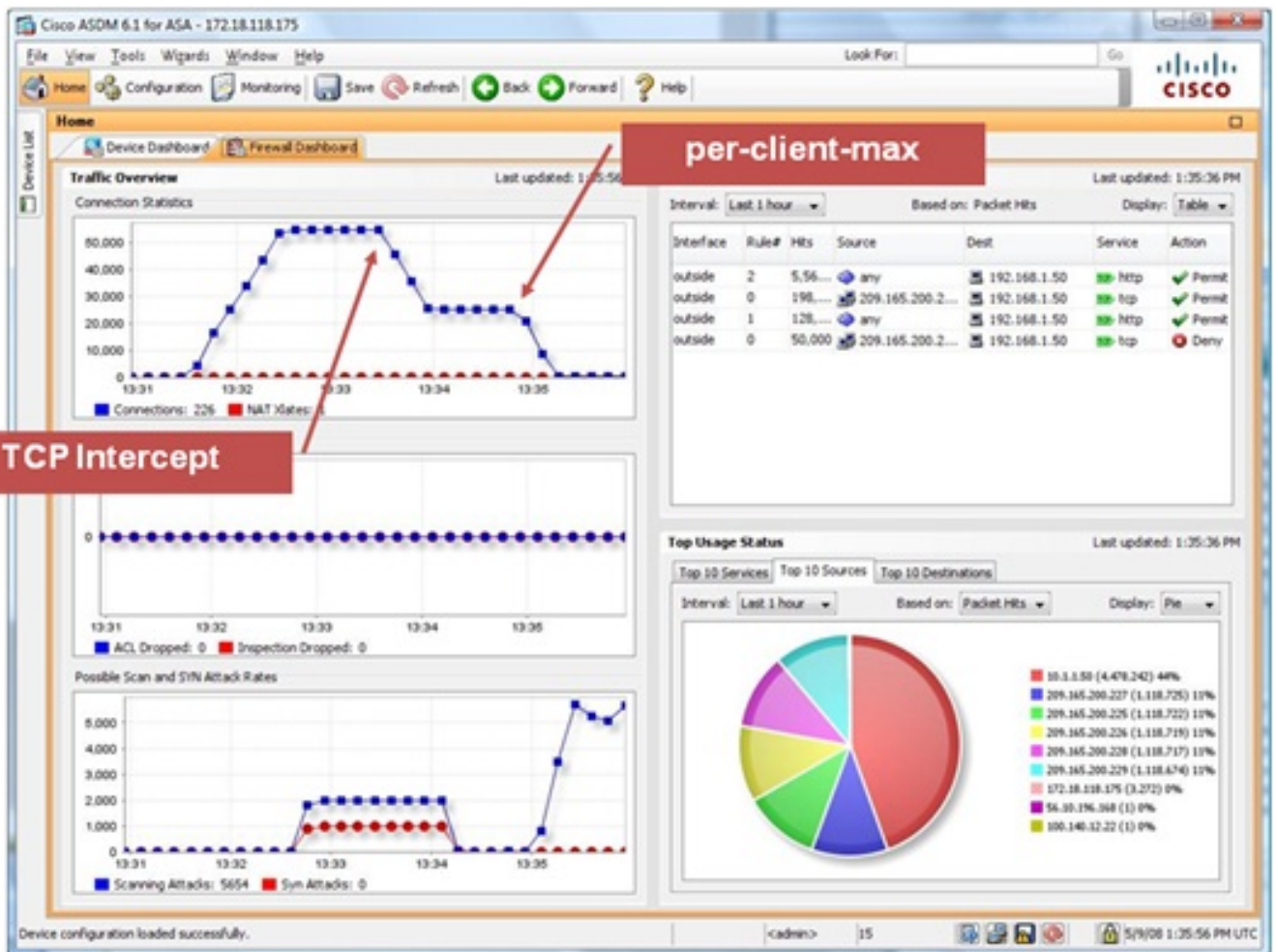
7) 限制每个客户端所能产生的最大连接数从而实现对垃圾连接的限制。

```

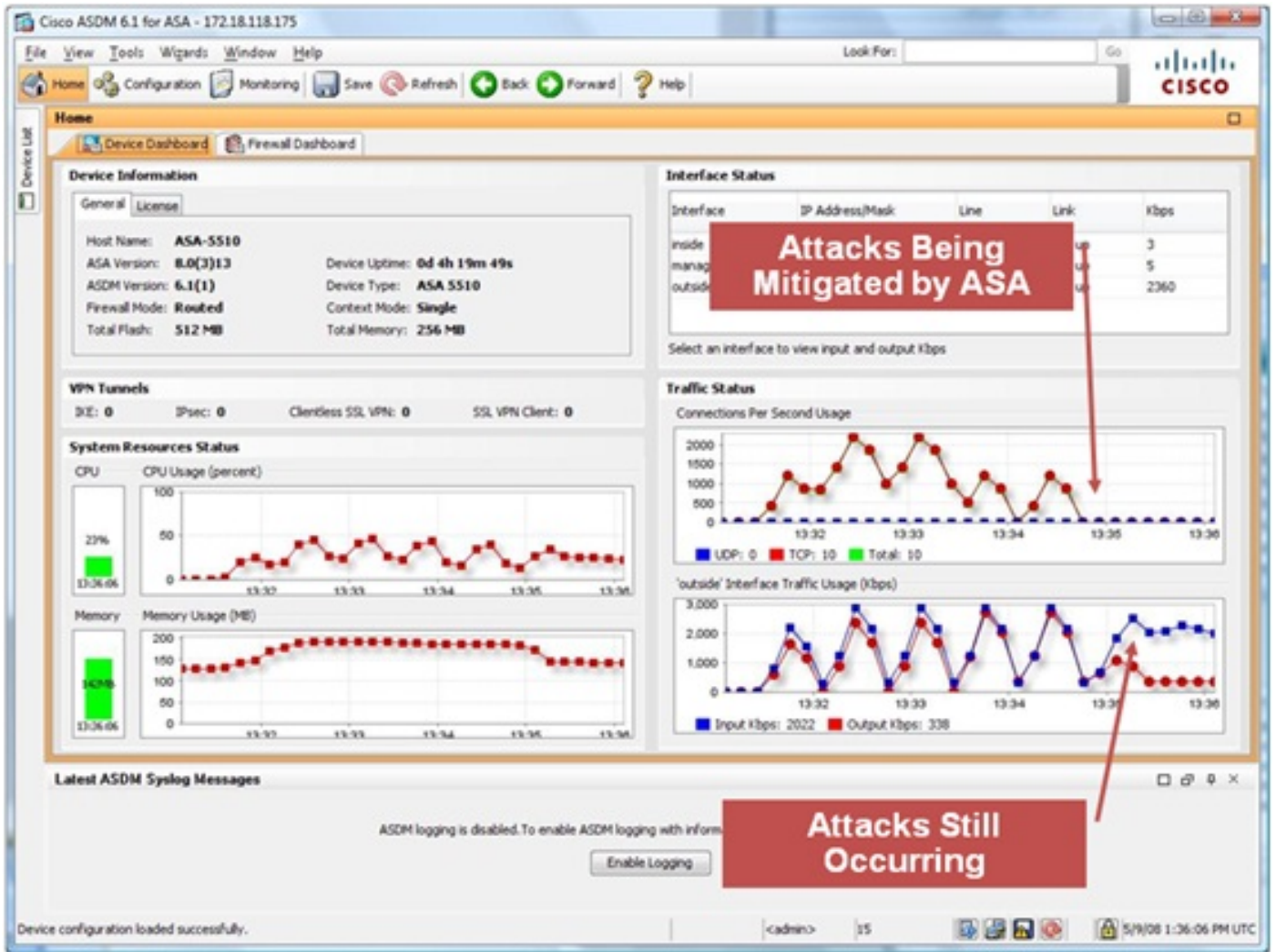
access-list 140 extended permit tcp any host 192.168.1.50 eq www
!
class-map protect
description Protect web server from attacks
match access-list 140
!
policy-map interface_policy
class protect
set connection embryonic-conn-max 100 per-client-max 25
!
service-policy interface_policy interface outside

```

8) 通过ASDM检查当前连接状态。发现连接数开始下降并恢复正常。



9) 利用ASDM跟踪攻击状态。此时攻击还是存在的但是ASA阻断了它们并保护了服务器的运行。



案例结果

经过在ASA上的调试，公司内部职员可以顺利的访问位于Web服务器群 Server_C。