

# ASA/IPS FAQ : IPS如何显示在事件日志的未翻译的实际IP地址？

## 目录

[简介](#)

[背景信息](#)

[IPS如何显示在事件日志的未翻译的实际IP地址？](#)

[相关信息](#)

## 简介

本文解释思科入侵防御系统(IPS)如何显示在事件日志的未翻译的实时IP addresses，虽然可适应安全工具(ASA)发送流量对IPS，在执行网络地址转换(NAT)后。

## 背景信息

### 拓扑

- 服务器的专用IP地址：192.168.1.10
- 服务器(Natted)的公网IP地址：203.0.113.2
- 攻击者的IP地址：203.0.113.10

## IPS如何显示在事件日志的未翻译的实际IP地址？

### 说明

当ASA发送数据包对IPS时，封装该数据包到思科ASA/Security服务模块(SSM)背板协议报头。此报头包含代表内部的用户实际IP地址在ASA后的字段。

这些日志显示发送互联网控制消息协议(ICMP)数据包对服务器的公网IP地址的攻击者，203.0.113.2。在IPS捕获的数据包显示ASA踢数据包对IPS在执行的NAT以后。

```
IPS# packet display PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: po0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on po0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
03:40:06.239024 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239117 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239903 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
```

31232, length 40

03:40:06.239946 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq

31232, length 40

**这是事件注册ICMP请求包的IPS从攻击者。**

```
evIdsAlert: eventId=6821490063343 vendor=Cisco severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Request id=2004 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: ICMP Echo Request
interfaceGroup: vs0
vlan: 0
participants:
attacker:
addr: 203.0.113.10 locality=OUT
target:
addr: 192.168.1.10 locality=OUT
os: idSource=unknown type=unknown relevance=relevant
alertDetails: InterfaceAttributes: context="single_vf" physical="Unknown"
backplane="PortChannel0/0" ;
riskRatingValue: 35 targetValueRating=medium attackRelevanceRating=relevant
threatRatingValue: 35
interface: PortChannel0/0 context=single_vf physical=Unknown backplane=
PortChannel0/0
protocol: icmp
```

**这是事件注册ICMP回复的IPS从内部的服务器。**

```
evIdsAlert: eventId=6821490063344 vendor=Cisco severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: ICMP Echo Reply
interfaceGroup: vs0
vlan: 0
participants:
attacker:
addr: 192.168.1.10 locality=OUT
target:
addr: 203.0.113.10 locality=OUT
os: idSource=unknown type=unknown relevance=relevant
alertDetails: InterfaceAttributes: context="single_vf" physical="Unknown"
backplane="PortChannel0/0" ;
riskRatingValue: 35 targetValueRating=medium attackRelevanceRating=relevant
threatRatingValue: 35
interface: PortChannel0/0 context=single_vf physical=Unknown backplane=
PortChannel0/0
protocol: icmp
```

**这是在ASA数据层面收集的捕获。**

```
1: 09:55:50.203267 203.0.113.10 > 192.168.1.10: icmp: echo request
2: 09:55:50.203877 203.0.113.2 > 203.0.113.10: icmp: echo reply
```

```
3: 09:55:51.203541 203.0.113.10 > 192.168.1.10: icmp: echo request  
4: 09:55:51.204182 203.0.113.2 > 203.0.113.10: icmp: echo reply
```

解码的ASA数据层面捕获。

## 相关信息

- [思科入侵防御系统传感器IPS的7.1 CLI配置指南](#)
- [数据包流经思科ASA防火墙](#)
- [技术支持和文档 - Cisco Systems](#)