ASA/IPS常见问题：IPS如何在事件日志中显示未转换的实际IP地址？

目录

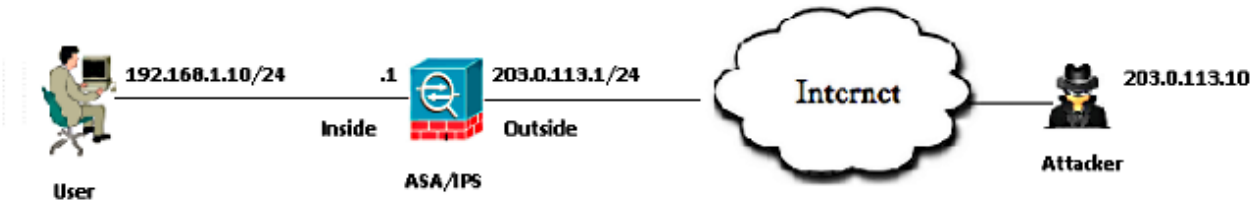
简介

本文档说明Cisco入侵防御系统(IPS)如何在事件日志中显示未转换的实际IP地址，尽管自适应安全设备(ASA)在执行网络地址转换(NAT)后会向IPS发送流量。

背景信息

拓扑

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



IPS如何在事件日志中显示未转换的实际IP地址？

解释

当ASA向IPS发送数据包时，它会将该数据包封装到Cisco **ASA/安全服务模块(SSM)背**板协议报头中。此报头包含一个字段，表示ASA后面内部用户的实际IP地址。

这些日志显示向服**务器公**有IP地址203.0.113.2发送Internet控制消息协议(ICMP)数据包的攻击者。IPS上捕获的数据包显示ASA在执行NAT后将数据包发送到IPS。

```
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
```

以下是来自攻击者的ICMP请求数据包的IPS事件日志。

```
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
```

以下是IPS上从内部服务器获取ICMP应答的事件日志。

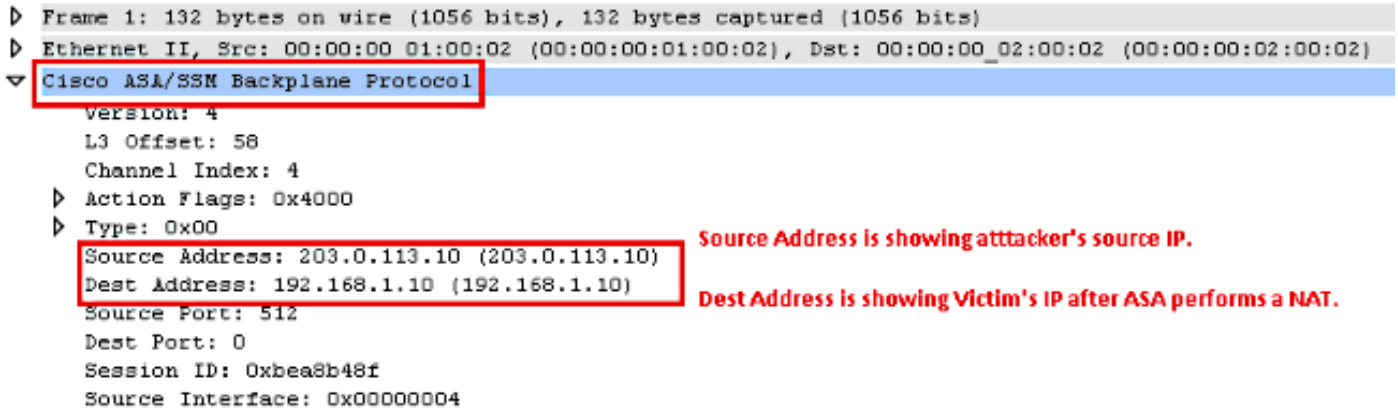
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: 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
```

以下是在ASA数据平面上**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数据平**面捕获。



相关信息

- [适用于IPS 7.1的思科入侵防御系统传感器CLI配置指南]
- [通过Cisco ASA防火墙的数据包流]
- [技术支持和文档 - Cisco Systems]