ASA/IPS常見問題：IPS如何在事件日誌中顯示未轉換的實際IP地址？

目錄

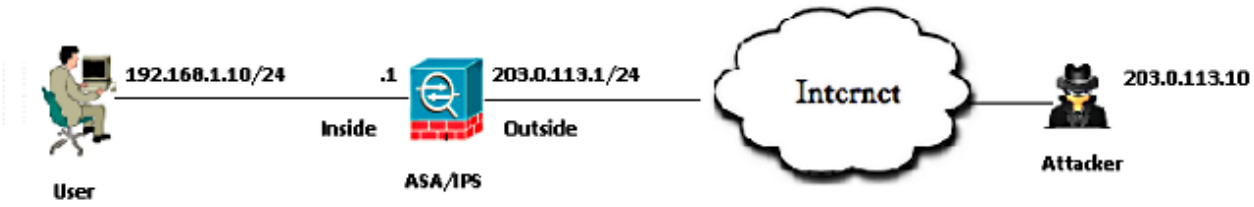
簡介

本文檔介紹思科入侵防禦系統(IPS)如何在事件日誌中顯示未轉換的實際IP地址，儘管自適應安全裝置(ASA)在執行網路地址轉換(NAT)之後會將流量傳送到IPS。

背景資訊

拓撲

- 伺服器的專用IP地址：192.168.1.10
- 伺服器的公用IP地址(Nat)： 203.0.113.2
- 攻擊者的IP地址：203.0.113.10



IPS如何在事件日誌中顯示未轉換的真實IP地址？

說明

當ASA將資料包傳送到IPS時，會將該資料包封裝到Cisco **ASA/安全服務模組(SSM)背板協**議報頭中。此報頭包含一個欄位，用於表示ASA後內部使用者的實際IP地址。

這些日誌顯示將網際網路控制消息協定(**Internet Control Message Protocol， ICMP)資料包傳送到伺服器的公共IP地址203.**0.113.2的攻擊者。在IPS上捕獲的資料包顯示，ASA在執行NAT後將這些資料包轉發到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
```

以下是攻擊者的IPS for ICMP請求資料包的事件日誌。

```
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
```

以下是來自內部伺服器的IPS for ICMP Reply事件記錄。

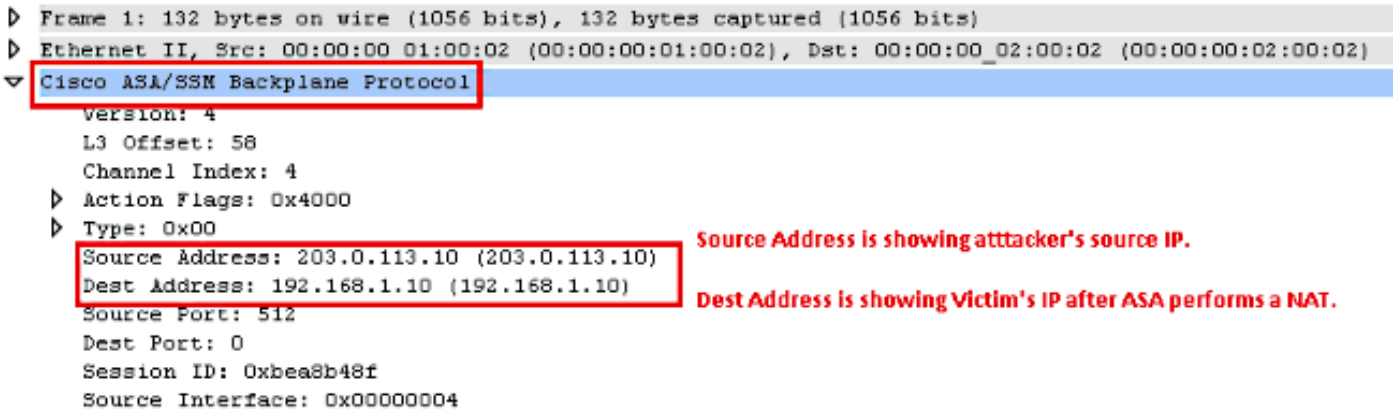
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

```
   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
```

解碼的ASA資料平面捕獲。



相關資訊

- [適用於IPS的Cisco入侵防禦系統感測器CLI配置指南7.1]
- [通過Cisco ASA防火牆的資料包流]
- [技術支援與文件 - Cisco Systems]