ASA/IPS FAQ:IPS는 이벤트 로그에 변환되지 않은 실제 IP 주소를 어떻게 표시합니까?

목차

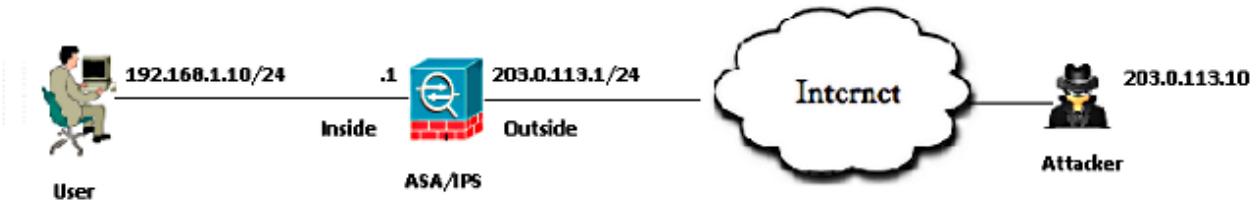
소개

이 문서에서는 ASA(Adaptive Security Appliance)가 NAT(Network Address Translation)를 수행한 후 IPS로 트래픽을 전송하지만 Cisco IPS(Intrusion Prevention System)가 이벤트 로그에 변환되지 않은 실제 IP 주소를 표시하는 방법에 대해 설명합니다.

배경 정보

토폴로지

- 서버의 개인 IP 주소:192.168.1.10
- 서버의 공용 IP 주소(네이티브): 203.0.113.2
- 공격자의 IP 주소:203.0.113.10



IPS는 이벤트 로그에 변환되지 않은 실제 IP 주소를 어떻게 표시합니까?

설명

ASA가 IPS에 패킷을 전송하면 해당 패킷을 Cisco **ASA/SSM(Security Services Module)** Backplane Protocol 헤더**로 캡슐화합니다**.이 헤더에는 ASA 뒤에 있는 내부 사용자의 실제 IP 주소를 나타내는 필드가 포함되어 있습니다.

이러한 로그는 서버의 공용 IP 주소 203.0.113.2으로 **ICMP(Internet Control Message Protocol)** 패

킷을 전송하는 공격자를 보여줍니다. IPS에서 캡처된 패킷은 NAT를 수행한 후 IPS로 패킷을 푸시합니다.

```
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
```

다음은 공격자의 ICMP 요청 패킷에 대한 IPS의 이벤트 로그입니다.

```
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
```

내부 서버에서 ICMP 회신을 위한 IPS의 이벤트 로그는 다음과 같습니다.

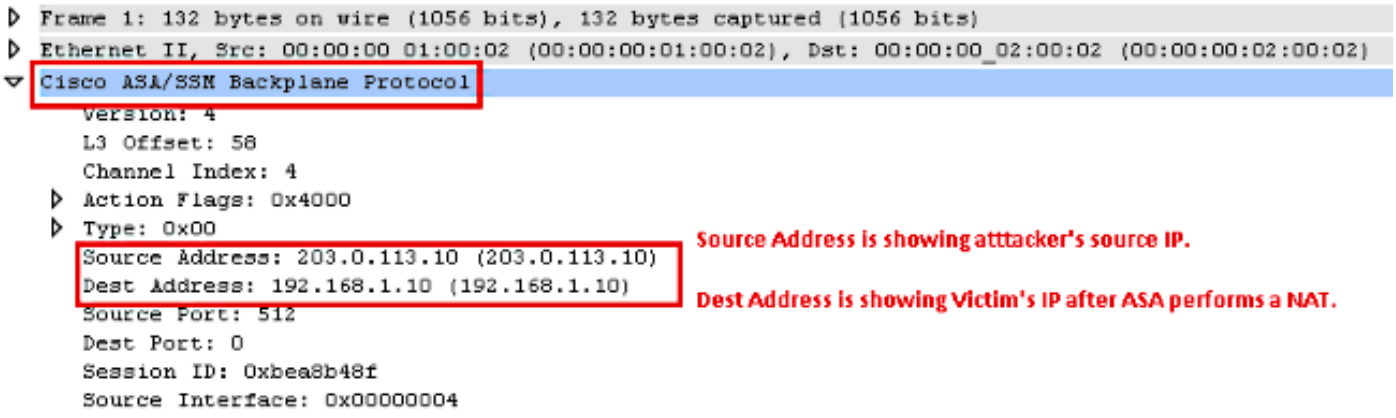
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

다음은 **ASA 데이터 플레인**에서 수집된 **캡처입니다.**

```
   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
```

디코딩된 **ASA 데이터 플레인** 캡처



관련 정보

- IPS 7.1용 Cisco Intrusion Prevention System Sensor CLI 컨피그레이션 가이드
- Cisco ASA 방화벽을 통한 패킷 흐름
- 기술 지원 및 문서 – Cisco Systems