Perguntas frequentes sobre ASA/IPS: como o IPS exibe endereços IP reais não traduzidos em logs de eventos?

Contents

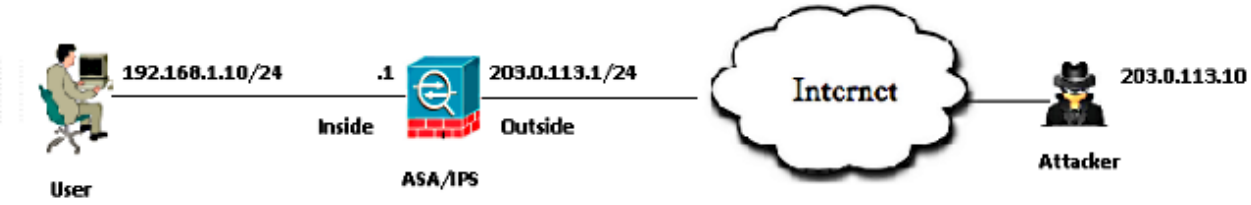
Introduction

Este documento explica como o Cisco Intrusion Prevention System (IPS) exibe endereços IP reais não traduzidos nos registros de eventos, embora o Adaptive Security Appliance (ASA) envie tráfego para o IPS depois de executar a Network Address Translation (NAT).

Informações de Apoio

Topologia

- O endereço IP privado do servidor: 192.168.1.10
- O endereço IP público do servidor (Natted): 203.0.113.2
- O endereço IP do invasor: 203.0.113.10



Como o IPS exibe endereços IP reais não traduzidos em registros de eventos?

Explicação

Quando o ASA envia um pacote para o IPS, ele encapsula esse pacote em um cabeçalho do Backplane Protocol do Cisco **ASA/Security Services Module (SSM)**. Este cabeçalho contém um campo que representa o endereço IP real do usuário interno por trás do ASA.

Esses registros mostram um invasor que envia pacotes ICMP (Internet Control Message Protocol) para o endereço IP público do servidor, 203.0.113.2. O pacote capturado no IPS mostra que o ASA crava os pacotes no IPS após executar o NAT.

```
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
```

Aqui estão os registros de eventos no IPS para pacotes de Solicitação ICMP do invasor.

```
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
```

Aqui estão os registros de eventos no IPS para resposta ICMP do servidor interno.

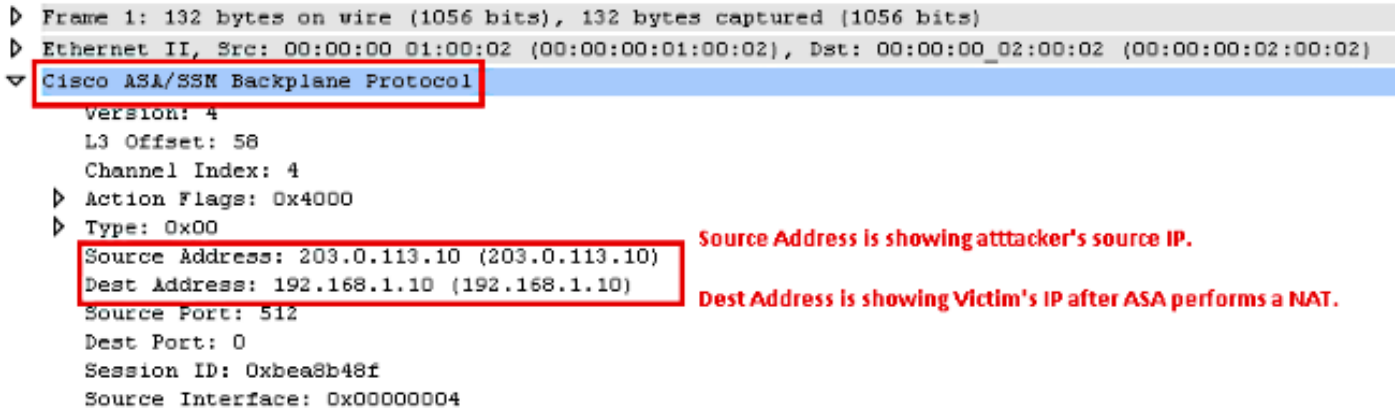
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

Aqui estão as capturas coletadas no **plano de dados ASA.**

```
   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
```

Plano de **dados ASA** decodificado captura.



Informações Relacionadas

- Guia de configuração do Cisco Intrusion Prevention System Sensor CLI para IPS 7.1
- Fluxo de pacotes pelo firewall Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems