Preguntas frecuentes sobre ASA/IPS: ¿Cómo muestra IPS direcciones IP reales no traducidas en los registros de eventos?

Contenido

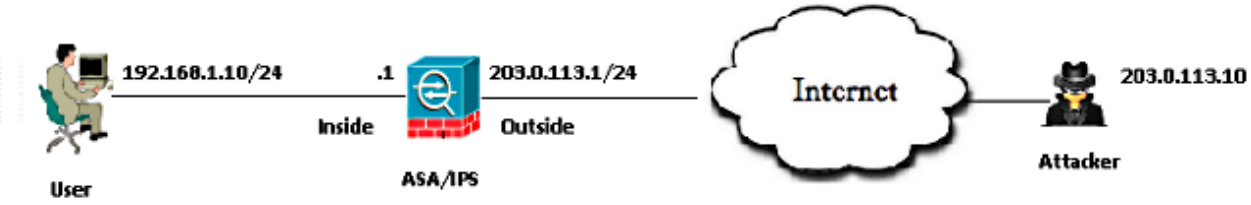
Introducción

Este documento explica cómo Cisco Intrusion Prevention System (IPS) muestra direcciones IP reales no traducidas en los registros de eventos, aunque Adaptive Security Appliance (ASA) envía tráfico al IPS después de realizar la traducción de direcciones de red (NAT).

Antecedentes

Topología

- La dirección IP privada del servidor: 192.168.1.10
- La dirección IP pública del servidor (Natted): 203.0.113.2
- Dirección IP del atacante: 203.0.113.10



¿Cómo muestra IPS direcciones IP reales no traducidas en los registros de eventos?

Explicación

Cuando el ASA envía un paquete al IPS, encapsula ese paquete en un encabezado de protocolo de placa base Cisco **ASA/Security Services Module (SSM)**. Este encabezado contiene un campo que representa la dirección IP real del usuario interno detrás del ASA.

Estos registros muestran un atacante que envía paquetes **ICMP (Internet Control Message Protocol) a la dirección IP pública del servidor, 203.0.113.2.** El paquete capturado en el IPS muestra que el ASA envía los paquetes al IPS después de realizar la 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
```

Estos son los registros de eventos en IPS para los paquetes de Solicitud ICMP del atacante.

```
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
```

Estos son los registros de eventos en IPS para la respuesta ICMP desde el servidor interno.

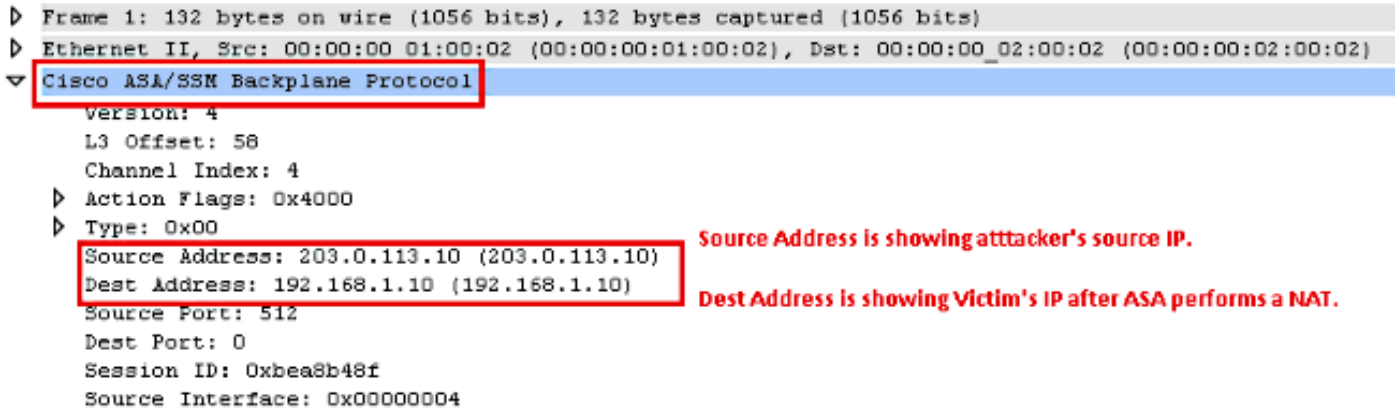
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

Estas son las capturas recopiladas en el **plano de datos 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
```

Capturas del **plano de datos ASA** descodificado.



Información Relacionada

- Guía de Configuración de CLI de Cisco Intrusion Prevention System Sensor para IPS 7.1
- Flujo de paquetes a través del firewall Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems