ASA/IPS FAQ: ¿Cómo el IPS visualiza los IP Address reales sin traducir en los registros de acontecimientos?

Contenido

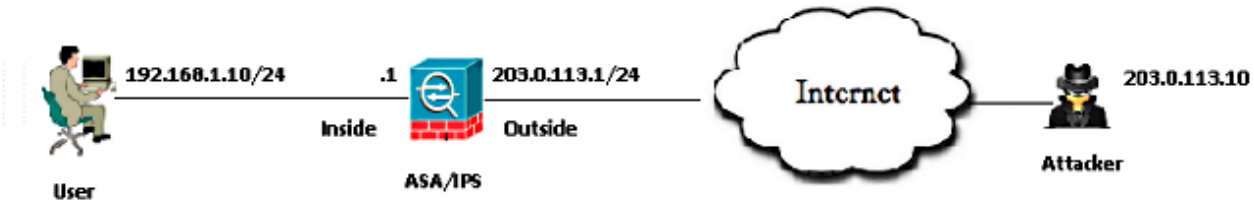
Introducción

Este documento explica cómo el (IPS) del Cisco Intrusion Prevention System visualiza los addressess reales sin traducir IP en los registros de acontecimientos, aunque el dispositivo de seguridad adaptante (ASA) envíe el tráfico al IPS después de que realice el Network Address Translation (NAT).

Antecedentes

Topología

- El IP Address privado del servidor: 192.168.1.10
- El IP Address público del servidor (Natted): 203.0.113.2
- La dirección IP del atacante: 203.0.113.10



¿Cómo el IPS visualiza los IP Address reales sin traducir en los registros de acontecimientos?

Explicación

Cuando el ASA envía un paquete al IPS, encapsula ese paquete en un encabezamiento del protocolo del backplane del **Módulo de servicios de** Cisco **ASA/Security (SS)**. Esta encabezado

contiene un campo que represente el IP Address real del usuario interior detrás del ASA.

Estos registros muestran un atacante que envíe los paquetes del **Internet Control Message Protocol (ICMP) al** IP Address público del servidor, 203.0.113.2. El paquete capturado en el IPS muestra que el ASA lleva en batea los paquetes al IPS después del NAT de ejecución.

```
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
```

Aquí está el evento abre una sesión el IPS para los paquetes de pedidos 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
```

Aquí está el evento abre una sesión el IPS para la respuesta de ICMP del servidor interior.

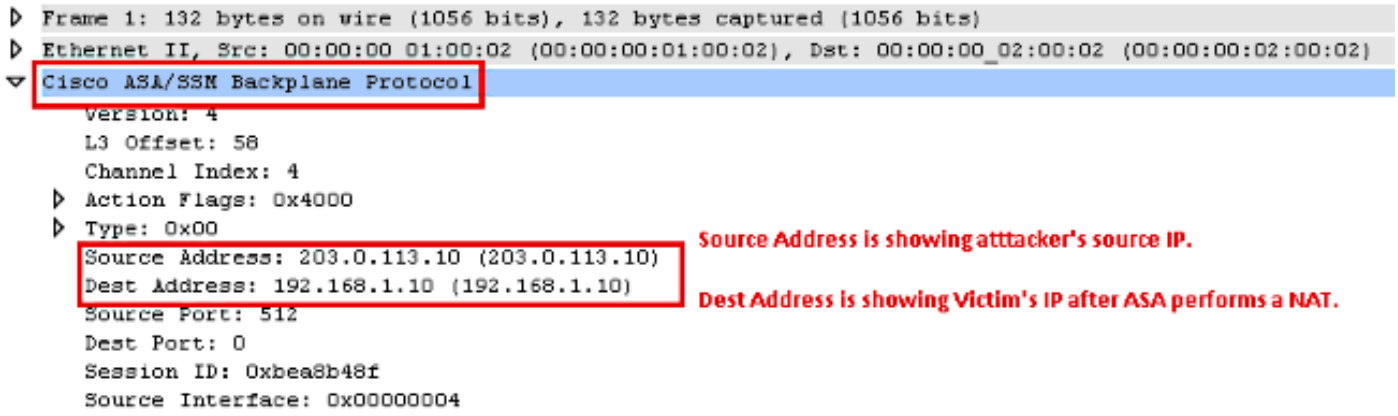
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

Aquí están las capturas recogidas en el **avión de los 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 decodificadas del **avión de los datos ASA**.



Información Relacionada

- [Guía de configuración CLI del sensor de Cisco Intrusion Prevention System para IPS 7.1]
- [El paquete atraviesa el Firewall de Cisco ASA]
- [Soporte Técnico y Documentación - Cisco Systems]