

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

Contenido

[Introducción](#)

[Antecedentes](#)

[¿Cómo el IPS visualiza los IP Address reales sin traducir en los registros de acontecimientos?](#)

[Información Relacionada](#)

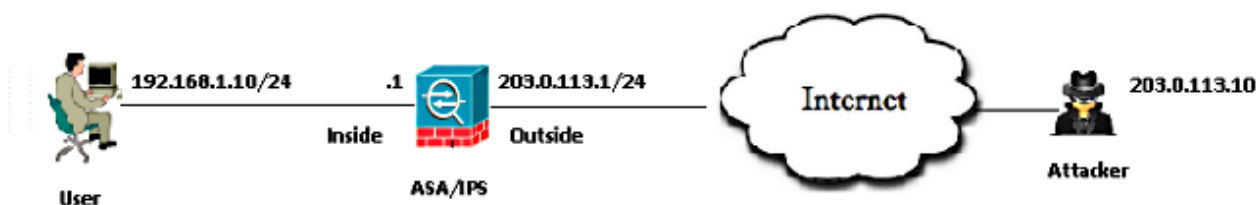
Introducción

Este documento explica cómo el (IPS) del Cisco Intrusion Prevention System visualiza los addressses 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.

```
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 la respuesta de ICMP del servidor interior.

```
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 están las capturas recogidas en el avión de los datos ASA.

```
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
```

Capturas decodificadas del avión de los datos ASA.

```
▶ Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
▶ Ethernet II, Src: 00:00:00 01:00:02 (00:00:00:01:00:02), Dst: 00:00:00_02:00:02 (00:00:00:02:00:02)
▼ Cisco ASA/SSM Backplane Protocol
  Version: 4
  L3 Offset: 58
  Channel Index: 4
  ▶ Action Flags: 0x4000
  ▶ Type: 0x00
  Source Address: 203.0.113.10 (203.0.113.10)
  Dest Address: 192.168.1.10 (192.168.1.10)
  Source Port: 512
  Dest Port: 0
  Session ID: 0xbea8b48f
  Source Interface: 0x00000004
```

Source Address is showing attacker's source IP.

Dest Address is showing Victim's IP after ASA performs a NAT.

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](#)