FAQ ASA/IPS :Comment IPS affiche-t-il les adresses IP réelles non traduites dans les journaux d'événements ?

Contenu

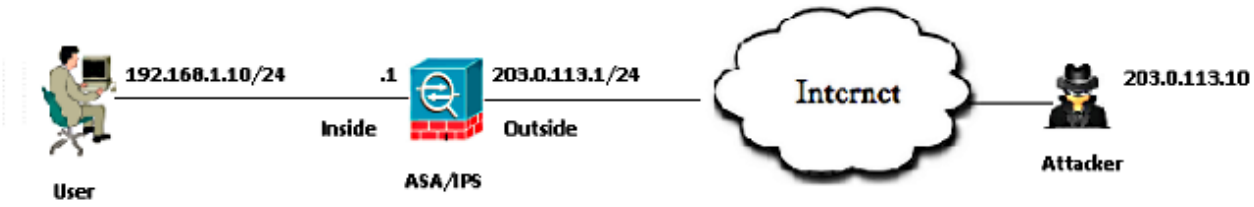
Introduction

Ce document explique comment le système de prévention des intrusions (IPS) de Cisco affiche les adresses IP réelles non traduites dans les journaux des événements, bien que l'appliance de sécurité adaptatif (ASA) envoie le trafic à l'IPS après avoir effectué la traduction d'adresses réseau (NAT).

Informations générales

Topologie

- Adresse IP privée du serveur : 192.168.1.10
- Adresse IP publique du serveur (Natted) : 203.0.113.2
- Adresse IP du pirate : 203.0.113.10



Comment IPS affiche-t-il les adresses IP réelles non traduites dans les journaux d'événements ?

Explication

Lorsque l'ASA envoie un paquet à IPS, il encapsule ce paquet dans un en-tête de protocole de fond de panier **ASA/SSM** de Cisco. Cet en-tête contient un champ qui représente l'adresse IP

réelle de l'utilisateur interne derrière l'ASA.

Ces journaux montrent un pirate qui envoie des paquets **ICMP (Internet Control Message Protocol)** à l'adresse IP publique du serveur, 203.0.113.2. Le paquet capturé sur l'IPS montre que l'ASA pond les paquets à l'IPS après avoir effectué 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
```

Voici les journaux des événements sur IPS pour les paquets de requête ICMP provenant de l'attaquant.

```
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
```

Voici les journaux des événements sur IPS pour la réponse ICMP à partir du serveur interne.

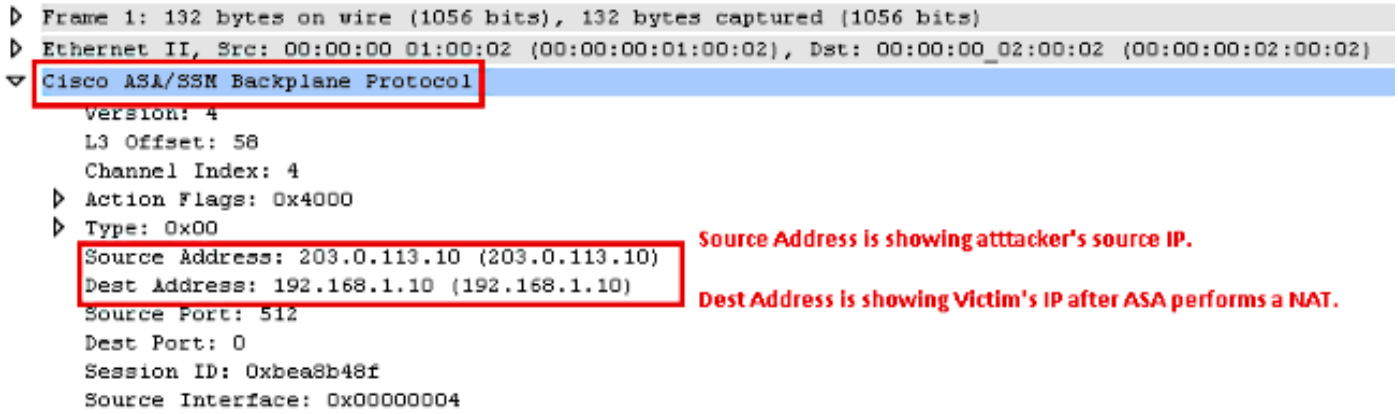
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
```

```
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
```

Voici les captures collectées sur le **plan de données 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
```

Captures **du plan de données ASA** décodées.



Informations connexes

- [Guide de configuration de l'interface en ligne de commande du capteur de système de prévention des intrusions Cisco pour IPS 7.1]
- [Flux de paquets via le pare-feu Cisco ASA]
- [Support et documentation techniques - Cisco Systems]