Domande frequenti su ASA/IPS: in che modo IPS visualizza gli indirizzi IP reali non tradotti nei registri eventi?

Sommario

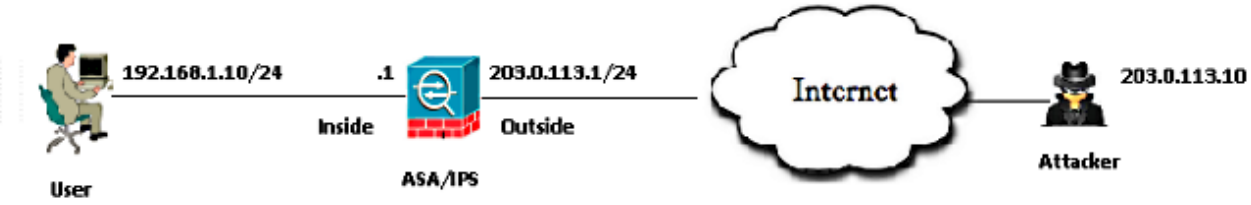
Introduzione

Questo documento spiega come Cisco Intrusion Prevention System (IPS) visualizzi nei log eventi gli indirizzi IP reali non tradotti, anche se Adaptive Security Appliance (ASA) invia traffico all'IPS dopo aver eseguito Network Address Translation (NAT).

Premesse

Topologia

- Indirizzo IP privato del server: 192.168.1.10
- Indirizzo IP pubblico del server (Natted): 203.0.113.2
- Indirizzo IP dell'autore dell'attacco: 203.0.113.10



In che modo IPS visualizza gli indirizzi IP reali non tradotti nei registri eventi?

Spiegazione

Quando l'ASA invia un pacchetto all'IPS, il pacchetto viene incapsulato in un'intestazione del protocollo backplane Cisco **ASA/Security Services Module (SSM)**. L'intestazione contiene un campo che rappresenta l'indirizzo IP reale dell'utente interno dietro l'appliance ASA.

Questi log mostrano un utente malintenzionato che invia pacchetti **ICMP (Internet Control Message Protocol)** all'indirizzo IP pubblico del server, 203.0.113.2. Il pacchetto acquisito sull'IPS mostra che l'ASA invia i pacchetti all'IPS dopo aver eseguito il protocollo 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
```

Di seguito sono riportati i registri eventi su IPS per i pacchetti di richiesta ICMP inviati dall'autore dell'attacco.

```
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
```

Di seguito sono riportati i registri eventi su IPS per la risposta ICMP dal server interno.

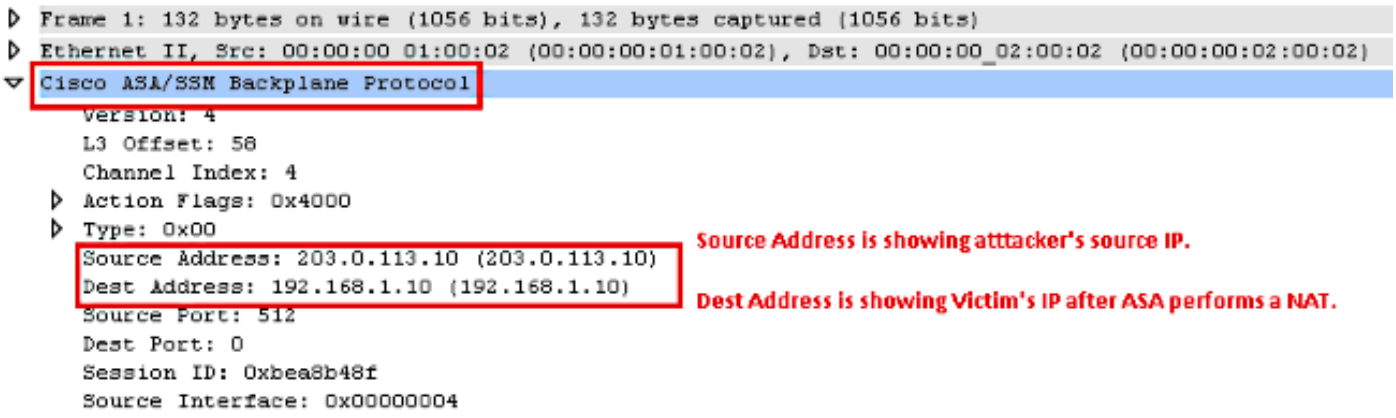
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

Di seguito sono riportate le clip raccolte sul **Data Plane 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
```

Acquisizioni decodificate **ASA Data Plane**.



Informazioni correlate

- Guida alla configurazione di Cisco Intrusion Prevention System Sensor CLI per IPS 7.1
- Flusso di pacchetti attraverso Cisco ASA Firewall
- Documentazione e supporto tecnico – Cisco Systems