ASA/IPS FAQ: Hoe toont IPS onvertaalde echte IP-adressen in gebeurtenissen?

Inhoud

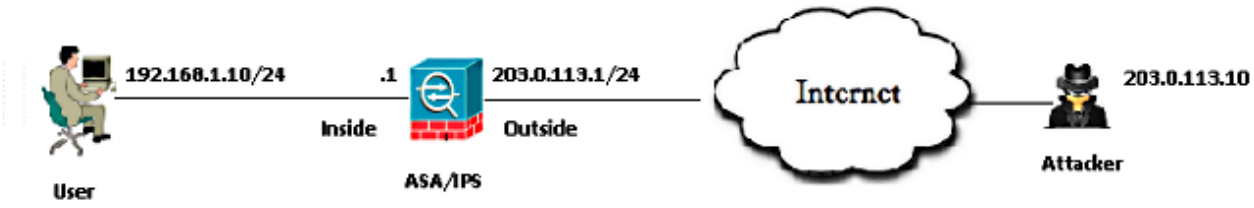
Inleiding

Dit document legt uit hoe het Cisco Inbraakpreventiesysteem (IPS) niet-vertaalde echte IP-adressen in de gebeurtenis-documenten weergeeft, hoewel de Adaptieve security applicatie (ASA) verkeer naar IPS stuurt nadat deze IP-adresomzetting (NAT) heeft uitgevoerd.

Achtergrondinformatie

Topologie

- Het Private IP-adres van de server: 192.168.1.10
- Het openbare IP-adres van de server (natted): 203.0.113.2
- IP-adres van de aanvaller: 203.0.113.10



Hoe toont IPS onvertaalde echte IP-adressen in gebeurtenis-logs?

verklaring

Wanneer de ASA een pakje naar IPS verstuurt, kapselt het dat pakje in een Cisco **ASA/Security Services Module (SSM)** backplane Protocol. Deze header bevat een veld dat het echte IP-adres weergeeft van de interne gebruiker achter de ASA.

Deze logs tonen een aanvaller die **ICMP-**pakketten (**Internet Control Message Protocol)** naar het

openbare IP-adres van de server, 203.0.113.2 stuurt. Het pakket dat op IPS is opgenomen, toont dat de ASA-pakketten na het uitvoeren van NAT naar IPS-pakketten worden geprikt.

```
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
```

Hier zijn de eventlogbestanden op IPS voor pakketten ICMP-aanvraag van de aanvaller.

```
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
```

Hier zijn de eventlogbestanden op IPS voor ICMP antwoord van de binnenserver.

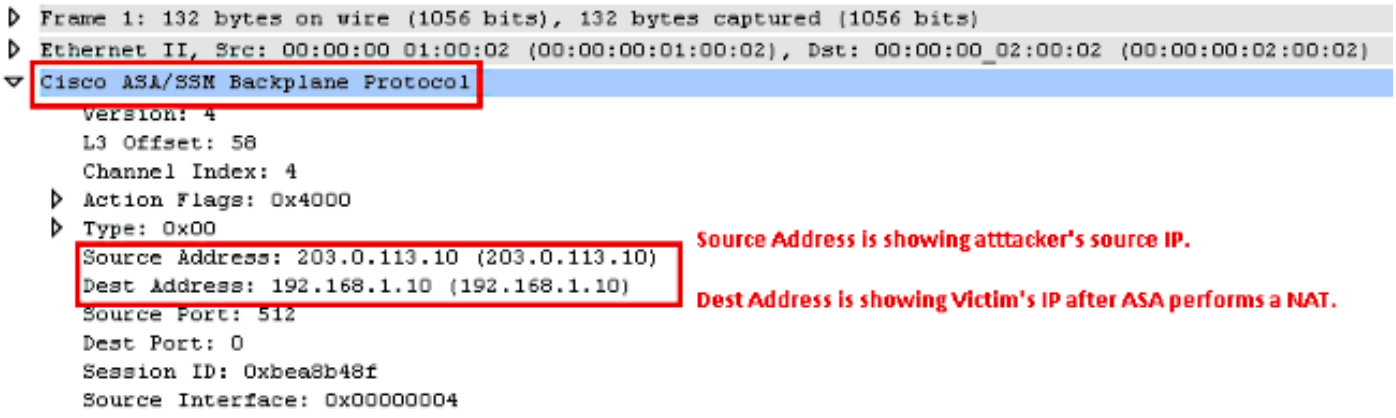
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

Hier zijn opgenomen op het **ASA Data Plane.**

```
   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
```

Gedecodeerde **ASA**-datacommunicatie-opnamen.



Gerelateerde informatie

- [Cisco-configuratiegids voor inbraakpreventiesysteem Sensor CLI voor IPS 7.1]
- [PacketFlow via Cisco ASA-firewall]
- [Technische ondersteuning en documentatie – Cisco Systems]