Häufig gestellte Fragen zu ASA/IPS: Wie zeigt IPS in Ereignisprotokollen unübersetzte echte IP-Adressen an?

Inhalt

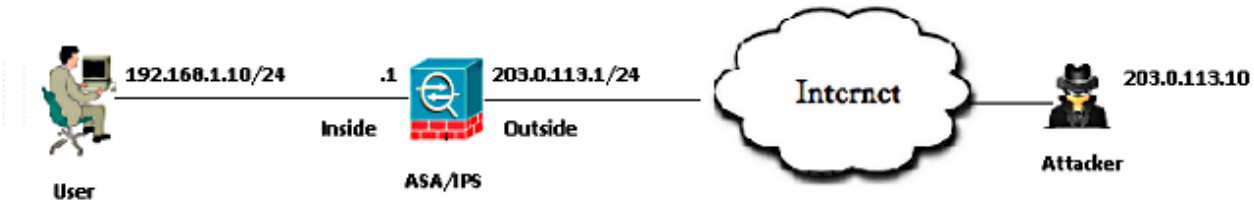
Einführung

In diesem Dokument wird erläutert, wie das Cisco Intrusion Prevention System (IPS) in den Ereignisprotokollen unübersetzte tatsächliche IP-Adressen anzeigt, obwohl die Adaptive Security Appliance (ASA) Datenverkehr an das IPS sendet, nachdem sie Network Address Translation (NAT) ausgeführt hat.

Hintergrundinformationen

Topologie

- Die private IP-Adresse des Servers: 192.168.1.10
- Die öffentliche IP-Adresse des Servers (Natted): 203.0.113.2
- Die IP-Adresse des Angreifers: 203,0,113,10



Wie zeigt IPS in Ereignisprotokollen unübersetzte reale IP-Adressen an?

Erläuterung

Wenn die ASA ein Paket an IPS sendet, kapselt sie dieses Paket in einen Cisco **ASA/Security Services Module (SSM)** Backplane Protocol-Header. Dieser Header enthält ein Feld, das die

tatsächliche IP-Adresse des internen Benutzers hinter der ASA darstellt.

Diese Protokolle zeigen einem Angreifer, der **ICMP-**Pakete **(Internet Control Message Protocol)** an die öffentliche IP-Adresse des Servers 203.0.113.2 sendet. Das auf dem IPS erfasste Paket zeigt, dass die ASA die Pakete nach der NAT an IPS ausführt.

```
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 sind die Ereignisprotokolle für IPS für ICMP Request-Pakete vom Angreifer.

```
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 sind die Ereignisprotokolle für IPS für ICMP Reply vom internen Server.

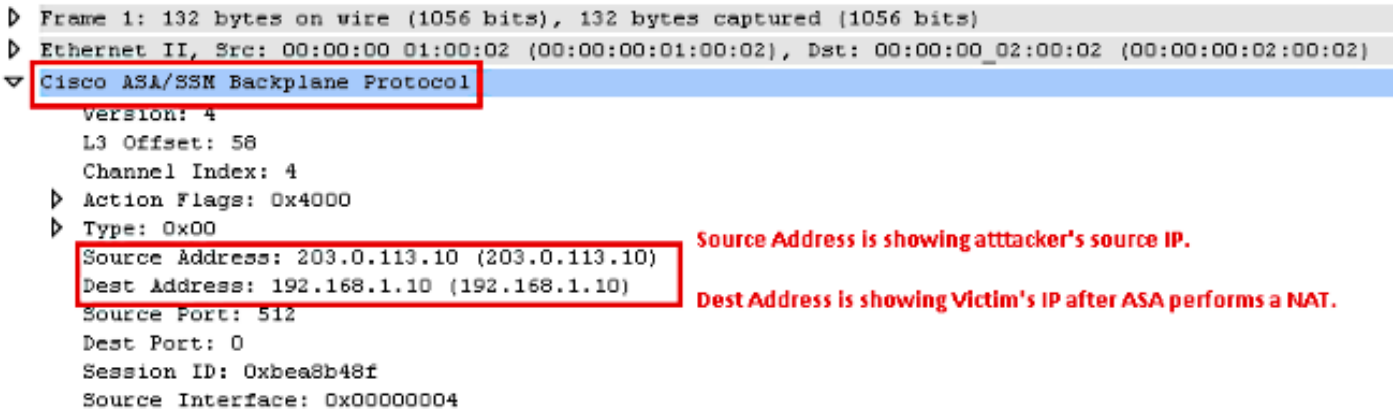
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
```

```
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 finden Sie die auf der **ASA-Datenebene** gesammelten **Aufzeichnungen.**

```
   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
```

Dekodierte Erfassung von **ASA-Datenebene**.



Zugehörige Informationen

- Cisco Intrusion Prevention System Sensor CLI-Konfigurationsleitfaden für IPS 7.1
- Paketfluss durch die Cisco ASA Firewall
- Technischer Support und Dokumentation - Cisco Systems