ASA/IPS FAQ:How IPS отображает непреобразованные реальные IP - адреса в журналах событий?

Содержание

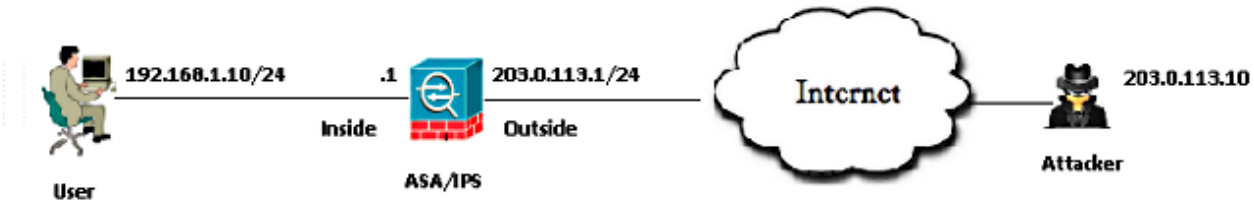
Введение

Этот документ объясняет, как система предотвращения вторжений Cisco (IPS) (IPS) отображается, непреобразованные реальные адреса IP в конечном счете регистрирует, невзирая на то, что Устройство адаптивной защиты (ASA) передает трафик к IPS после того, как это выполняет Технологию NAT.

Общие сведения

Топология

- Закрытый IP - адрес сервера: 192.168.1.10
- Открытый IP - адрес (преобразованного посредством NAT) сервера: 203.0.113.2
- IP-адрес атакующего: 203.0.113.10



Как IPS отображает непреобразованные реальные IP - адреса в журналах событий?

Пояснение

Когда ASA передает пакет к IPS, он инкапсулирует тот пакет в **Cisco ASA /** Заголовок протокола Объединительной платы **Модуля служб безопасности (SSM)**. Этот заголовок

содержит поле, которое представляет реальный IP - адрес внутреннего пользователя позади ASA.

Эти журналы показывают атакующему, который передает пакеты Протокола ICMP к открытому IP - адресу сервера, 203.0.113.2. Пакет, перехваченный на IPS, показывает, что ASA плывет на плоскодонке пакеты к IPS после выполнения 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
```

Вот журналы событий на IPS для пакетов запроса ICMP от атакующего.

```
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
```

Вот журналы событий на IPS для Ответа ICMP от внутреннего сервера.

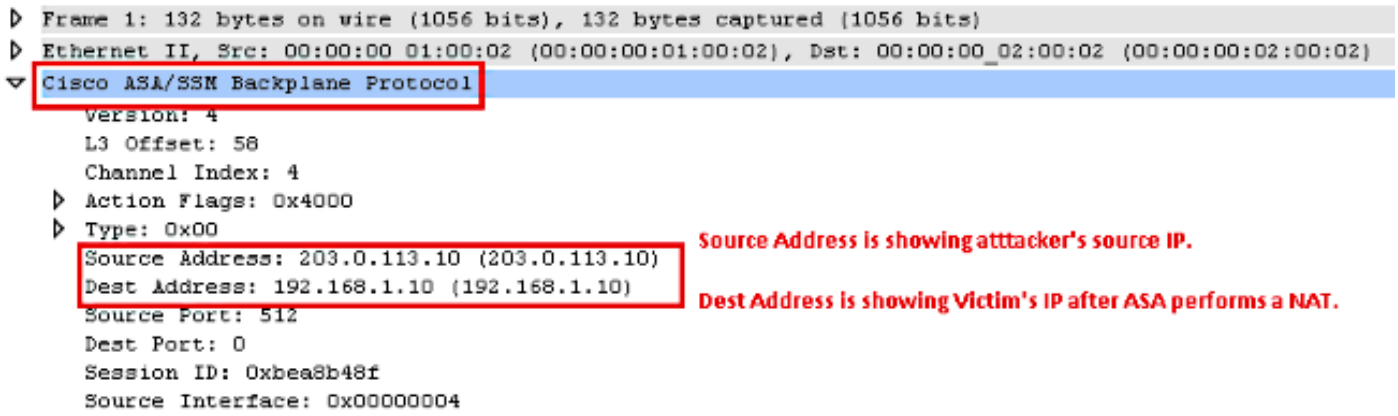
```
evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 1305
time: Dec 24, 2014 03:43:57 UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Reply id=2000 version=S666 type=other
created=20001127
subsigId: 0
sigDetails: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

Вот перехваты, собранные на **Плоскости Данных 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
```

Декодируемые перехваты **плоскости данных ASA**.



Дополнительные сведения

- [Руководство конфигурации интерфейса командой строки датчика системы предотвращения вторжений Cisco (IPS) для IPS 7.1]
- [Поток пакетов через межсетевой экран Cisco ASA]
- [Cisco Systems – техническая поддержка и документация]