

ASA/IPSに関するFAQ:IPSは変換されていない 実際のIPアドレスをイベントログでどのように 表示しますか。

内容

[概要](#)

[背景説明](#)

[IPS は未変換の実際の IP アドレスをイベント ログでどのように表示しますか。](#)

[関連情報](#)

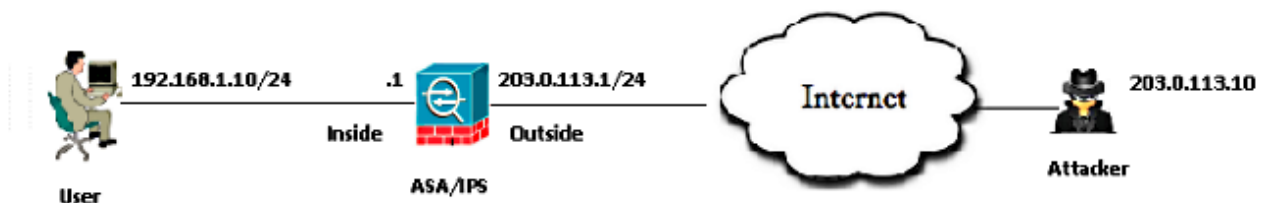
概要

このドキュメントでは、適応型セキュリティ アプライアンス (ASA) がネットワーク アドレス変換 (NAT) を実行した後でトラフィックを IPS に送信する場合でも、Cisco Intrusion Prevention System (IPS) が変換されていない実際の IP アドレスをイベント ログに表示する方法を説明します。

背景説明

トポロジ

- サーバのプライベート IP アドレス。192.168.1.10
- サーバのパブリック IP アドレス (NAT 済み)。 203.0.113.2
- 攻撃者の IP アドレス。203.0.113.10



IPS は未変換の実際の IP アドレスをイベント ログでどのように 表示しますか。

説明

ASA は IPS にパケットを送信する場合、そのパケットを Cisco ASA/セキュリティ モジュール (SSM) バックプレーン プロトコル ヘッダーにカプセル化します。このヘッダーには、ASA の

背後にいる内部ユーザの実際の IP アドレスを表すフィールドが含まれています。

これらのログは、Internet Control Message Protocol(ICMP)パケットをサーバのパブリックIPアドレス203.0.113.2に送信する攻撃者を示しています。IPSでキャプチャされたパケットは、ASAがNATの実行後にパケットをIPSにパントすることを示します。

```
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
```

攻撃者からの ICMP リクエスト パケットに関する IPS のイベント ログを次に示します。

```
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
```

内部サーバからの ICMP 応答に関する IPS のイベント ログを次に示します。

```
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
```

ASA データ プレーンで収集されたキャプチャを次に示します。

```
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
```

復号化された ASA データ プレーン キャプチャ。

```
▷ Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
▷ Ethernet II, Src: 00:00:00 01:00:02 (00:00:00:01:00:02), Dst: 00:00:00 02:00:02 (00:00:00:02:00:02)
▼ Cisco ASA/SSM Backplane Protocol
  version: 4
  L3 Offset: 58
  Channel Index: 4
  ▷ Action Flags: 0x4000
  ▷ Type: 0x00
  Source Address: 203.0.113.10 (203.0.113.10)
  Dest Address: 192.168.1.10 (192.168.1.10)
  Source Port: 512
  Dest Port: 0
  Session ID: 0xbea8b48f
  Source Interface: 0x00000004
```

Source Address is showing attacker's source IP.

Dest Address is showing Victim's IP after ASA performs a NAT.

関連情報

- [Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.1](#)
- [Cisco ASA ファイアウォールを介するパケット フロー](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)