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

目次

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 はどのように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。

これらの口グは、**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 に送信した攻撃者を示します。 IPS でキャプチャされたパケットは、ASA が NAT の実施後にパケットを 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。

```
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
```

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。

```
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
```

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。

```
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
```
復号化された ASA データ プレーン キャプチャ。

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