ASA/IPS FAQ: Como o IPS indica endereços IP real untranslated nos log de eventos?

Índice

Introdução

Este documento explica como o Sistema de prevenção de intrusões da Cisco (IPS) indica addressess reais untranslated IP nos log de eventos, embora a ferramenta de segurança adaptável (ASA) envie o tráfego ao IPS depois que executa o Network Address Translation (NAT).

Informações de Apoio

Topologia

- O endereço IP privado do server: 192.168.1.10
- O endereço IP público do server (Natted): 203.0.113.2
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante: 203.0.113.10

Como o IPS indica endereços IP real untranslated nos log de eventos?

Explicação

Quando o ASA envia um pacote ao IPS, encapsula esse pacote em um cabeçalho de protocolo do backplane do **Módulo de serviços de** Cisco **ASA/Security (SS)**. Este encabeçamento contém um campo que represente o endereço IP real do usuário interno atrás do ASA.

Estes logs mostram um atacante que envie pacotes do **Internet Control Message Protocol (ICMP) ao** endereço IP público do server, 203.0.113.2. O pacote capturado no IPS mostra que os pontapés ASA os pacotes ao IPS após o NAT de execução.

```
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
```

Está aqui o evento entra o IPS para pacotes de requisição ICMP do atacante.

```
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
```

Está aqui o evento entra o IPS para a resposta de ICMP do server interno.

```
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
```

Estão aqui as captações recolhidas no plano dos dados ASA.

```
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
```

Captações descodificadas do plano dos dados ASA.

Informações Relacionadas

- Guia de configuração de CLI do sensor de Sistema de prevenção de intrusões da Cisco para IPS 7.1
- O pacote corre através do Firewall de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems