الأسئلة المتداولة حول ASA/IPS:كيف يعرض IPS عناوين IP الحقيقية غير المترجمة في سجلات الأحداث؟

المحتويات

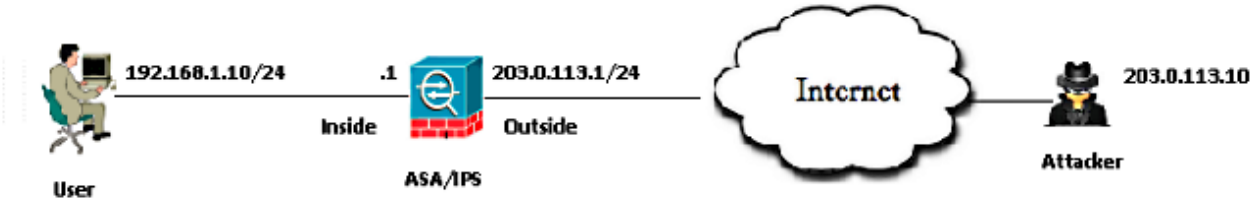
المقدمة

يشرح هذا المستند كيفية عرض نظام Cisco لمنع الاقتحام (IPS) لعناوين IP الحقيقية غير المترجمة في سجلات الأحداث، رغم أن جهاز الأمان القابل للتكيف (ASA) يرسل حركة مرور البيانات إلى IPS بعد أن يقوم بتنفيذ ترجمة عنوان الشبكة (NAT).

معلومات أساسية

طوبولوجيا

- عنوان IP الخاص للخادم: 192.168.1.10
- عنوان IP العام للخادم (تابع): 203.0.113.2
- عنوان IP للمهاجم: 203.0.113.10



كيف يعرض IPS عناوين IP الحقيقية غير المترجمة في سجلات الأحداث؟

الشرح

عندما يرسل ال ASA ربط إلى IPS، هو يغلف أن ربط في **ASA/Security Services Module (SSM)** cisco) خلف مستوى بروتوكول. يحتوي هذا الرأس على حقل يمثل عنوان IP الحقيقي للمستخدم الداخلي خلف ASA.

تظهر هذه السجلات المهاجم الذي يرسل حزم **بروتوكول رسائل التحكم في الإنترنت (ICMP)** إلى عنوان IP العام للخادم، 203.0.113.2. تظهر الحزمة الملتقطة على IPS أن ASA يلكم الحزم إلى IPS بعد تنفيذ 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
IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq 03:40:06.239024
                                                        length 40 ,31232
IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq 03:40:06.239117
                                                        length 40 ,31232
   IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq 03:40:06.239903
                                                        length 40 ,31232
   IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq 03:40:06.239946
                                                        length 40 ,31232
```

فيما يلي سجلات الأحداث على IPS لحزم طلب ICMP من المهاجم.

```
    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
```

فيما يلي سجلات الأحداث على IPS للرد على بروتوكول ICMP من الخادم الداخلي.

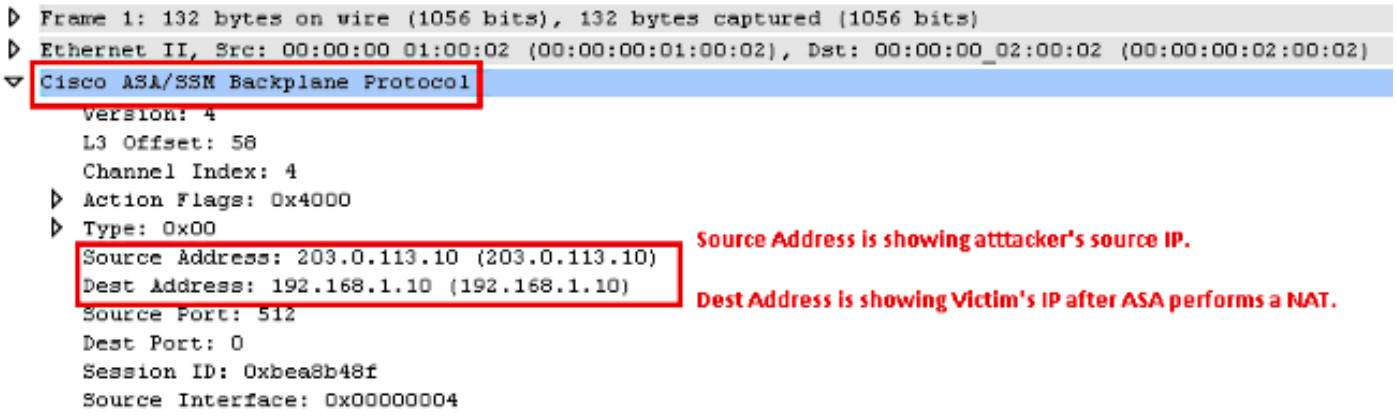
```
    evIdsAlert: eventId=6821490063344  vendor=Cisco  severity=informational
                                                              :originator
                                                              hostId: IPS
                                                        appName: sensorApp
                                                     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
```

فيما يلي عمليات الالتقاط التي تم تجميعها على **مستوى بيانات ASA**.

```
icmp: echo request :192.168.1.10 < 203.0.113.10       09:55:50.203267 :1
            icmp: echo reply :203.0.113.10 < 203.0.113.2 09:55:50.203877 :2
         icmp: echo request :192.168.1.10 < 203.0.113.10 09:55:51.203541 :3
            icmp: echo reply :203.0.113.10 < 203.0.113.2 09:55:51.204182 :4
```

التقاط **مستوى بيانات ASA** التي تم فك ترميزها.



معلومات ذات صلة

- دليل تكوين واجهة سطر الأوامر (CLI) لمستشعر نظام منع الاقتحام من Cisco ل IPS 7.1
- تدفق الحزمة عبر جدار حماية Cisco ASA
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).