الأسئلة المتداولة حول ASA: كيف يمكنك تفسير syslog التي تم إنشاؤها بواسطة ASA عندما يقوم ببناء الاتصالات أو تمزيقها؟

المحتويات

المقدمة
كيف يمكنك تفسير syslog التي تم إنشاؤها بواسطة ASA عندما يقوم ببناء الاتصالات أو تمزيقها؟
مخطط الشبكة
مخطط الشبكة (واجهات الأمان نفسها)
معلومات ذات صلة

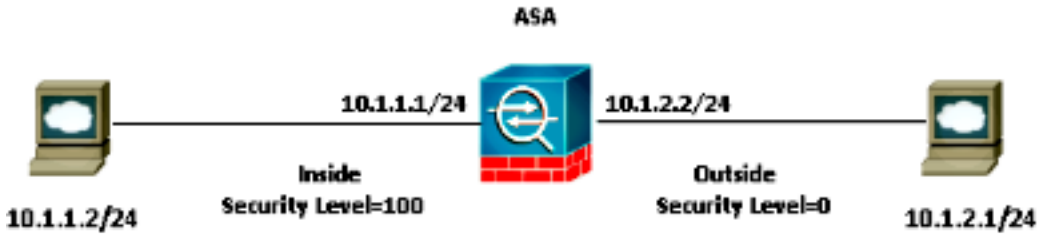
المقدمة

يوضح هذا المستند كيفية تفسير الإنشاء الخاص ببروتوكول التحكم في الإرسال (TCP)/بروتوكول مخطط بيانات المستخدم (UDP) على جهاز جهاز جهاز الأمان القابل للتكيف (ASA) عند إنشاء الاتصالات وتنزيلها.

كيف يمكنك تفسير syslog التي تم إنشاؤها بواسطة ASA عندما يقوم ببناء الاتصالات أو تمزيقها؟

تستند جميع syslog التي تمت مناقشتها في هذا المستند إلى مخططات الشبكة الموضحة هنا.

مخطط الشبكة



السيناريو 1: يتم الحصول على حركة مرور الإدارة إلى واجهة ASA الداخلية (الهوية) من المضيف الداخلي

```
ASA-6-302013: Built inbound TCP connection 8 for%
inside:10.1.1.2/12523 (10.1.1.2/12523) to NP Identity
(Ifc:10.1.1.1/22 (10.1.1.1/22

:ASA-6-302014: Teardown TCP connection 8 for inside%
to NP Identity Ifc:10.1.1.1/22 duration 10.1.1.2/12523
bytes 2436 TCP FINs 0:00:53
```

السيناريو 2: يتم الحصول على حركة مرور البيانات من خلال ASA من المضيف الداخلي ويتم توجيهها إلى المضيف الخارجي

```
(ASA-6-302013: Built outbound TCP connection 9 for outside:10.1.2.1/22 (10.1.2.1/22%
(to inside:10.1.1.2/53496 (10.1.1.2/53496

:ASA-6-302014: Teardown TCP connection 9 for outside:10.1.2.1/22 to inside%
duration 0:00:30 bytes 0 SYN Timeout 10.1.1.2/53496
```

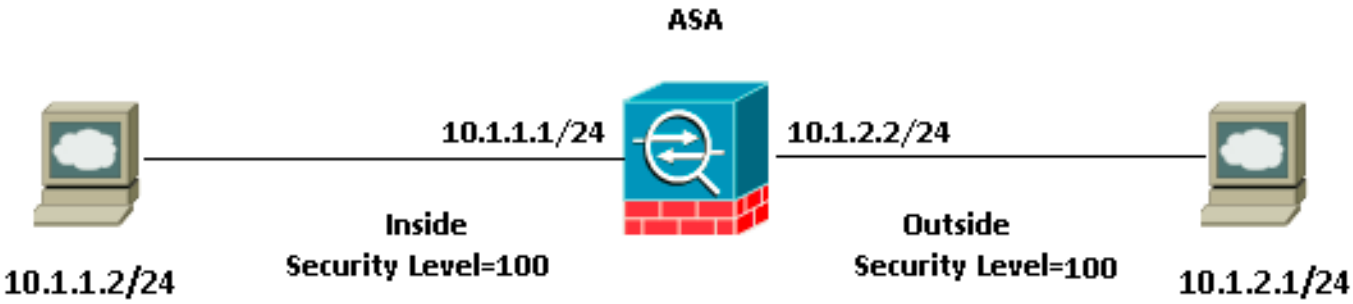
السيناريو 3: يتم الحصول على حركة مرور الإدارة إلى واجهة ASA الخارجية (الهوية) من المضيف الخارجي

```
ASA-6-302013: Built inbound TCP connection 10 for outside:10.1.2.1/28218%
(to NP Identity Ifc:10.1.2.2/22 (10.1.2.2/22 (10.1.2.1/28218)

ASA-6-302014: Teardown TCP connection 10 for outside:10.1.2.1/28218 to NP%
Identity Ifc:10.1.2.2/22 duration 0:00:33 bytes 968 TCP Reset-O
```

السيناريو 4: يتم الحصول على حركة مرور البيانات من خلال ASA من المضيف الخارجي ويتم توجيهها إلى المضيف الداخلي

```
ASA-6-302013: Built inbound TCP connection 11 for outside:10.1.2.1/21647%
(to inside:10.1.1.2/22 (10.1.1.2/22 (10.1.2.1/21647)

ASA-6-302014: Teardown TCP connection 11 for outside:10.1.2.1/21647 to%
inside:10.1.1.2/22 duration 0:00:00 bytes 0 TCP Reset
```

مخطط الشبكة (واجهات الأمان نفسها)



السيناريو 1: يتم الحصول على حركة مرور البيانات من خلال ASA من المضيف الداخلي ويتم توجيهها إلى المضيف الخارجي

```
(ASA-6-302013: Built inbound TCP connection 0 for inside:10.1.1.2/28075 (10.1.1.2/28075%
(to outside:10.1.2.1/23 (10.1.2.1/23

ASA-6-302014: Teardown TCP connection 0 for inside:10.1.1.2/28075 to outside:10.1.2.1/23%
duration 0:00:46 bytes 144 TCP FINs
```

السيناريو 2: يتم الحصول على حركة مرور البيانات من خلال ASA من المضيف الخارجي إلى المضيف الداخلي

```
(ASA-6-302013: Built inbound TCP connection 1 for outside:10.1.2.1/17891 (10.1.2.1/17891%
(to inside:10.1.1.2/23 (10.1.2.5/23

ASA-6-302014: Teardown TCP connection 1 for outside:10.1.2.1/17891 to inside:10.1.1.2/23%
duration 0:00:08 bytes 165 TCP FIN
```

*حيث 10.1.2.5 هو عنوان NAT IP الثابت لـ 10.1.1.2

معلومات ذات صلة

- أدلة مرجع جدران الحماية من الجيل التالي Cisco ASA 5500 Series
- أدلة تكوين جدران الحماية من الجيل التالي Cisco ASA 5500 Series
- 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).