ASA 8.2: تدفق الحزمة من خلال جدار حماية ASA

المحتويات

المقدمة

يصف هذا المستند تدفق الحزمة من خلال جدار حماية لأجهزة الأمان المعدلة (ASA) من Cisco. وهو يعرض إجراء Cisco ASA لمعالجة الحزم الداخلية. وهو يناقش أيضا الاحتمالات المختلفة حيث يمكن إسقاط الحزمة وحالات مختلفة حيث تتقدم الحزمة للأمام.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من cisco 5500 sery ASAs.

المكونات المستخدمة

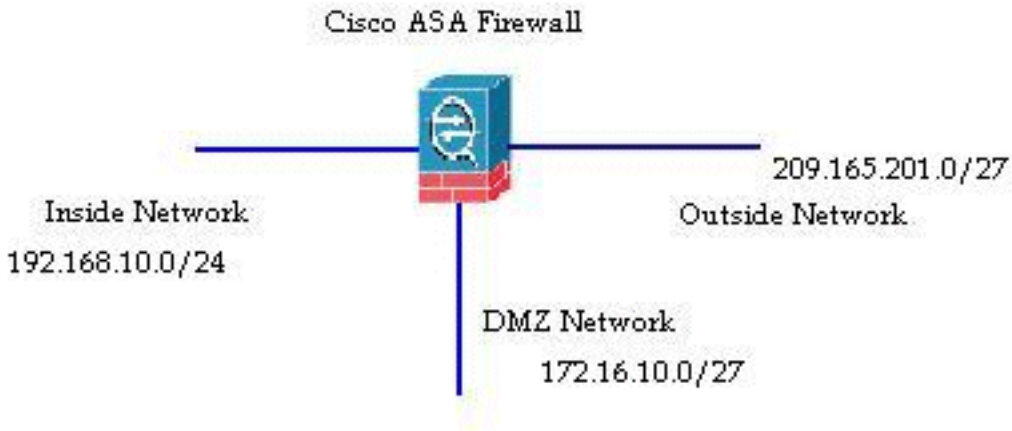
أسست المعلومة في هذا وثيقة على cisco ASA 5500 sery ASAs أن يركض برمجية صيغة 8.2.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

دعات القارن أن يستلم الربط **المدخل** قارن والقارن من خلال أي الربط يخرج دعات **المخرج** قارن. عندما تشير إلى

تدفق الحزمة من خلال أي جهاز، فإن المهمة يمكن تبسيطها بسهولة إذا نظرت إليها من حيث هاتين الواجهات. وفيما يلي نموذج لسيناريو:



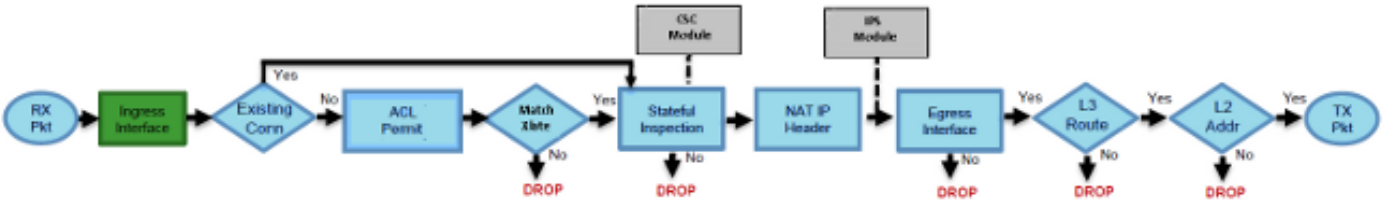
عندما يحاول مستخدم داخلي (192.168.10.5) الوصول إلى خادم ويب في شبكة المنطقة المجردة من السلاح (172.16.10.5)، يبدو تدفق الحزمة كما يلي:

- عنوان المصدر - 192.168.10.5
- منفذ المصدر - 22966
- عنوان الوجهة - 172.16.10.5
- غاية ميناء - 8080
- واجهة الدخول - في الداخل
- واجهة الخروج - DMZ
- البروتوكول المستخدم - TCP (بروتوكول التحكم في الإرسال)

بعد أن تحدد تفاصيل تدفق الحزمة كما هو موضح هنا، من السهل عزل الإصدار إلى إدخال التوصيل المحدد هذا.

خوارزمية عملية حزمة ASA من Cisco

هنا رسم بياني من كيف ال cisco ASA يعالج الربط أن هو يستلم:



هنا الخطوات الفردية بالتفصيل:

1. وصلت الربط في المدخل قارن.
2. ما إن تصل الربط إلى المصد داخلي من القارن، المدخل قارن زادت بواحد.
3. يبحث Cisco ASA أولا في تفاصيل جدول الاتصال الداخلي الخاص به للتحقق من ما إذا كان هذا اتصال حالي. إذا تطابق تدفق الحزمة مع اتصال حالي، يتم تجاوز التحقق من قائمة التحكم في الوصول (ACL) ويتم نقل الحزمة إلى الأمام.إذا لم يتطابق تدفق الحزمة مع اتصال حالي، فسيتم التحقق من حالة TCP. إذا كانت حزمة SYN أو UDP (بروتوكول مخطط بيانات المستخدم)، حينئذ تتم زيادة عداد الاتصال بمقدار واحد ويتم إرسال الحزمة للتحقق من قائمة التحكم في الوصول. إذا لم تكن حزمة SYN، يتم إسقاط الحزمة ويتم تسجيل الحدث.
4. تتم معالجة الحزمة وفقا لقوائم التحكم في الوصول (ACL) للواجهة. يتم التحقق منه بالترتيب التسلسلي

لإدخالات قائمة التحكم بالوصول (ACL) وإذا طابق أي من إدخالات قائمة التحكم بالوصول (ACL)، فإنه يتحرك إلى الأمام. وإلا، يتم إسقاط الحزمة وتسجيل المعلومات. تتم زيادة عدد مرات الوصول إلى قائمة التحكم في الوصول (ACL) بمقدار واحد عندما تتطابق الحزمة مع إدخال قائمة التحكم في الوصول (ACL).

5. يتم التحقق من الحزمة لقواعد الترجمة. إذا مرت حزمة من خلال هذا التحقق، يتم إنشاء إدخال اتصال لهذا التدفق وتنتقل الحزمة إلى الأمام. وإلا، يتم إسقاط الحزمة وتسجيل المعلومات.
6. تخضع الحزمة لفحص فحص. يتحقق هذا الفحص مما إذا كان تدفق الحزمة المحدد هذا متوافقا مع البروتوكول أم لا. يحتوي ASA من Cisco على محرك فحص مدمج يقوم بفحص كل اتصال وفقا لمجموعة الوظائف المحددة مسبقا على مستوى التطبيق. إذا اجتاز التفتيش، يتحرك إلى الامام. وإلا، يتم إسقاط الحزمة وتسجيل المعلومات.سيتم تنفيذ فحوصات أمان إضافية إذا كانت هناك وحدة أمان محتوى (CSC) مشمولة.
7. تتم ترجمة معلومات رأس IP طبقا لقاعدة ترجمة عنوان الشبكة/ترجمة عنوان المنفذ (NAT/PAT) ويتم تحديث المبالغ المرجعية وفقا لذلك. تتم إعادة توجيه الحزمة إلى الوحدة النمطية لخدمات الأمان والفحص والمنع المتقدم (AIP-SSM) لفحوصات الأمان المتعلقة ب IPS عندما تكون وحدة AIP النمطية المعنية.
8. أرسلت الربط إلى المخرج قارن يؤسس على الترجمة قاعدة. إن ما من مخرج عينت قارن في الترجمة قاعدة، بعد ذلك الغاية قارن قررت يؤسس على الشامل ممر بحث.
9. على واجهة الخروج، يتم إجراء بحث مسار الواجهة. تذكر، يتم تحديد واجهة المخرج بواسطة قاعدة الترجمة التي تأخذ الأولوية.
10. بمجرد العثور على مسار للطبقة 3 والتعرف على الخطوة التالية، يتم تنفيذ دقة الطبقة 2. تحدث إعادة كتابة الطبقة 2 من رأس MAC في هذه المرحلة.
11. بثت الربط على السلك، وزيادة قارن على المخرج قارن.

شرح NAT

ارجع إلى هذه المستندات للحصول على مزيد من التفاصيل حول ترتيب عملية NAT:

- برنامج ASA الإصدار 8.2 من Cisco وما قبله
- برنامج ASA الإصدار 8.3 من Cisco والإصدارات الأحدث

إظهار الأوامر

هنا بعض الأوامر المفيدة التي تساعد على تعقب تفاصيل تدفق الحزمة في مراحل مختلفة من العملية:

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

رسائل Syslog

توفر رسائل syslog معلومات مفيدة حول معالجة الحزمة. فيما يلي بعض الأمثلة على رسائل syslog لمرجعك:

- رسالة syslog عند عدم وجود إدخال اتصال:

```
ASA-6-106015: Deny TCP (no connection) from IP_address/port to%
IP_address/port flags tcp_flags on interface interface_name
```

- رسالة Syslog عندما يتم رفض الحزمة بواسطة قائمة التحكم في الوصول (ACL):
```
[ASA-4-106023: Deny protocol src [interface_name:source_address/source_port%
dst interface_name:dest_address/dest_port by access_group acl_ID
```
- رسالة syslog عند عدم العثور على قاعدة ترجمة:
```
:ASA-3-305005: No translation group found for protocol src interface_name%
source_address/source_port dst interface_name:dest_address/dest_port
```
- رسالة syslog عندما يتم رفض الحزمة بواسطة فحص الأمان:
```
ASA-4-405104: H225 message received from outside_address/outside_port to%
inside_address/inside_port before SETUP
```
- رسالة syslog عند عدم وجود معلومات المسار:
```
ASA-6-110003: Routing failed to locate next-hop for protocol from src%
interface:src IP/src port to dest interface:dest IP/dest port
```

للحصول على قائمة كاملة بجميع رسائل syslog التي تم إنشاؤها بواسطة Cisco ASA مع شرح موجز، ارجع إلى رسائل Cisco ASA Series Syslog.

معلومات ذات صلة

- صفحة دعم Cisco من ASA
- cisco ASA 5500 sery أمر مرجع، 8.2
- دليل تكوين سلسلة Cisco ASA 5500، 8.3
- 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).