ZBF موجه بتكوين مداخلا وأ DHCP لميمع

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات الميزة
تحليل البيانات
جدار الحماية المستند إلى المنطقة كعميل DHCP مع إجراء تمرير لحركة مرور UDP
التكوين
التحقق من الصحة
جدار حماية قائم على المنطقة مع إجراء تمرير لحركة مرور DHCP
التكوين
التحقق من الصحة
سيناريو التكوينات غير الصحيحة
الموجه كخادم DHCP
استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند كيفية تكوين موجه يعمل كخادم بروتوكول التحكم في المضيف الديناميكي (DHCP) أو عميل DHCP باستخدام ميزة جدار الحماية المستند إلى المنطقة (ZBF). لأنه من الشائع إلى حد ما أن يتم تمكين DHCP و ZBF في آن واحد، تساعد تلميحات التكوين هذه في ضمان التفاعل الصحيح لهذه الميزات.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من ال cisco ios ® برمجية منطقة baser جدار حماية. ارجع إلى دليل تصميم وتطبيق جدار الحماية المستند إلى المناطق للحصول على تفاصيل.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

أمر.

معلومات الميزة

عندما يتم تمكين ZBF على موجه IOS، يتم السماح بأي حركة مرور إلى المنطقة الذاتية (أي حركة المرور الموجهة إلى مستوى إدارة الموجه) بشكل افتراضي في قطار الرمز IOS 15.x.

إذا كنت قد قمت بإنشاء سياسة لأي منطقة (مثل "داخل" أو "خارج") للمنطقة الذاتية (السياسة الخارجية) أو العكس (سياسة عدم التدخل)، فيجب عليك تحديد حركة المرور المسموح بها بشكل صريح في السياسات المرفقة بهذه المناطق. أستخدم إجراء الفحص أو المرور لتحديد حركة المرور المسموح بها.

تحليل البيانات

يستخدم DHCP حزم بروتوكول مخطط بيانات المستخدم للبث (UDP) لاستكمال عملية DHCP. قد يتم إسقاط تكوينات جدار الحماية المستندة إلى المنطقة التي تحدد إجراء الفحص لحزم UDP للبث هذه بواسطة الموجه، وقد تفشل عملية DHCP. قد ترى أيضا رسالة السجل هذه:

```
FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair%
self-out class dhcp with ip ident 0
```

أحلت الإصدار يصف في cisco بق "ZBF، CSCso53376 id تفتيش لا يعمل ل بث حركة مرور."

لتجنب هذه المشكلة، قم بتعديل تكوين جدار الحماية المستند إلى المنطقة حتى يتم تطبيق إجراء المرور بدلا من إجراء الفحص على حركة مرور DHCP.

ملاحظة: لا يكون هذا مطلوبا إلا عند تطبيق سياسة على المنطقة الذاتية على الموجه.

جدار الحماية المستند إلى المنطقة كعميل DHCP مع إجراء تمرير لحركة مرور UDP

التكوين

يستخدم مثال التكوين هذا مجموعة إجراء المرور بدلا من إجراء الفحص في خريطة السياسة لجميع حركة مرور UDP إلى الموجه أو منه.

```
zone security outside
 zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp
```

```
policy-map type inspect out-to-self
            class type inspect dhcp
                                pass
                    class class-default
                                drop
policy-map type inspect self-to-out
            class type inspect dhcp
                                pass
                    class class-default
                                drop

zone-pair security out-to-self source outside destination self
                        service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
                        service-policy type inspect self-to-out
```

التحقق من الصحة

راجع syslogs للتحقق من حصول الموجه على عنوان DHCP بنجاح.

عندما يتم تكوين كل من سياسات الخروج إلى الذات والتخرج الذاتي لتمرير حركة مرور UDP، يمكن للموجه الحصول على عنوان IP من DHCP كما هو موضح في syslog هذا:

```
,DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.5%
mask 255.255.255.0
```

عندما يتم تكوين سياسة خارج المنطقة الذاتية لتمرير حركة مرور UDP، يمكن للموجه أيضا الحصول على عنوان IP من DHCP، ويتم إنشاء syslog هذا:

```
,DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.6%
mask 255.255.255.0
```

عندما يتم تكوين سياسة منطقة التخزين التلقائي لتمرير حركة مرور UDP، يمكن للموجه الحصول على عنوان IP من DHCP، ويتم إنشاء syslog هذا:

```
,DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.7%
mask 255.255.25
```

جدار حماية قائم على المنطقة مع إجراء تمرير لحركة مرور DHCP

التكوين

يوضح مثال التكوين التالي كيفية منع جميع حركة مرور UDP من منطقة داخل المنطقة الذاتية للموجه الخاص بك باستثناء حزم DHCP. أستخدم قائمة الوصول مع منافذ معينة للسماح بحركة مرور DHCP فقط؛ في هذا المثال، تم تحديد منفذ UDP 67 ومنفذ UDP 68 ليتم مطابقتهما. تحتوي خريطة الفئة التي تشير إلى قائمة الوصول على إجراء المرور المطبق.

```
    access-list extended 111
permit udp any any eq 67 10

    access-list extended 112
permit udp any any eq 68 10
```

```
class-map type inspect match-any self-to-out
                        match access-group 111
class-map type inspect match-any out-to-self
                        match access-group 112

                         zone security outside
                          zone security inside

                                interface Ethernet0/1
                      zone-member security outside
                               interface Ethernet0/2
                     zone-member security inside

                  policy-map type inspect out-to-self
                       class type inspect out-to-self
                                                pass
                            class class-default
                                                drop
                  policy-map type inspect self-to-out
                       class type inspect self-to-out
                                                pass
                            class class-default
                                                drop

zone-pair security out-to-self source outside destination self
                        service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
                        service-policy type inspect self-to-out
```

التحقق من الصحة

راجع الإخراج من الأمر **show policy-map inspection type zone-pair** لتأكيد أن الموجه يسمح لحركة مرور DHCP عبر جدار حماية المنطقة. في هذا المثال إخراج، تشير العدادات المميزة إلى أنه يتم تمرير الحزم من خلال جدار حماية المنطقة. إذا كانت هذه العدادات صفر، فهناك مشكلة في التكوين، أو أن الحزم لا تصل إلى الموجه لمعالجتها.

```
router#show policy-map type inspect zone-pair sessions

                     policy exists on zp out-to-self
                             Zone-pair: out-to-self
                Service-policy inspect : out-to-self
                  (Class-map: out-to-self (match-any
                            Match: access-group 112
                               packets, 924 bytes 3
                                second rate 0 bps 30
                                              Pass
                              packets, 1848 bytes 6

                (Class-map: class-default (match-any
                                        Match: any
                                              Drop
                                 packets, 0 bytes 0

                     policy exists on zp self-to-out
                             Zone-pair: self-to-out
                Service-policy inspect : self-to-out
                  (Class-map: self-to-out (match-any
                            Match: access-group 111
                              packets, 3504 bytes 6
                                second rate 0 bps 30
```

```
Pass
packets, 3504 bytes 6

(Class-map: class-default (match-any
Match: any
Drop
packets, 0 bytes 0
```

سيناريو التكوينات غير الصحيحة

يوضح سيناريو النموذج هذا ما يحدث عندما يتم تكوين الموجه بشكل غير صحيح لتحديد إجراء فحص حركة مرور DHCP. في هذا السيناريو، يتم تكوين الموجه كعميل DHCP. يرسل الموجه رسالة اكتشاف DHCP لمحاولة الحصول على عنوان IP. تم تكوين جدار الحماية المستند إلى المنطقة لفحص حركة مرور DHCP هذه. هذا مثال على تكوين ZBF:

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside

interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
inspect
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
inspect
class class-default
drop

zone-pair securiy out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

عندما يتم تكوين سياسة الاكتفاء الذاتي باستخدام إجراء الفحص لحركة مرور UDP، يتم إسقاط حزمة اكتشاف DHCP، ويتم إنشاء syslog هذا:

```
FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair%
self-out class dhcp with ip ident 0
```

عندما يتم تكوين كل من سياسة الذاتية للخرج والمخرج للذات باستخدام إجراء الفحص لحركة مرور UDP، يتم إسقاط حزمة اكتشاف DHCP، ويتم إنشاء syslog هذا:

```
FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair%
self-out class dhcp with ip ident 0
```

عندما يكون لسياسة الصادر الذاتي إجراء التفتيش الممكن، ويكون لسياسة الصادر الذاتي إجراء المرور الذي تم تمكينه لحركة مرور UDP، يتم إسقاط حزمة عرض DHCP بعد إرسال حزمة اكتشاف DHCP، ويتم إنشاء syslog هذا:

```
FW-6-DROP_PKT: Dropping udp session 192.168.1.1:67 255.255.255.255:68 on zone-pair%
out-self class dhcp with ip ident 0
```

الموجه كخادم DHCP

إذا كانت واجهة الموجهات الداخلية تعمل كخادم DHCP وإذا كان العملاء الذين يقومون بالاتصال بالواجهة الداخلية هم عملاء DHCP، يتم السماح بحركة مرور DHCP هذه بشكل افتراضي إذا لم يكن هناك سياسة منطقة داخلية إلى ذاتية أو ذاتية إلى الداخل.

ومع ذلك، إذا كان أحد هذين النهجين موجودا، فأنت بحاجة إلى تكوين إجراء تمرير لحركة مرور المصلحة (منفذ UDP 67 أو منفذ UDP 68) في سياسة خدمة زوج المنطقة.

استكشاف الأخطاء وإصلاحها

لا توجد حاليا أي معلومات خاصة حول أستكشاف الأخطاء وإصلاحها متوفرة لهذه التكوينات.

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).