

إلى دن تسمل هيجوت لانيوكت يني نكمي فيك ددعتم هجوم وألوحم يلع (PBR) ةسايس لاني رورم ةكرح هيجوت ةداعإل Cisco نم تاقب طلا WSA؟ إلى تانايب لاني

المحتويات

[سؤال:](#)

سؤال:

كيف يمكنني تكوين التوجيه المستند إلى السياسة (PBR) على محول أو موجه متعدد الطبقات من Cisco لإعادة توجيه حركة مرور البيانات إلى WSA؟

البيئة: جهاز أمان الويب (WSA) من Cisco، الوضع الشفاف - محول L4

عندما يتم تكوين WSA في الوضع الشفاف باستخدام محول L4، فلا حاجة إلى تكوين على WSA. يتم التحكم في إعادة التوجيه بواسطة المحول L4 switch (أو الموجه).

من الممكن استخدام التوجيه المستند إلى السياسة (PBR) لإعادة توجيه حركة مرور الويب إلى WSA. ويتم تحقيق ذلك من خلال مطابقة حركة المرور الصحيحة (استنادا إلى منافذ TCP) وتوجيه الموجه/المحول لإعادة توجيه حركة المرور هذه إلى WSA.

في المثال التالي، توجد واجهة البيانات/الوكيل الخاصة ب WSA (إما M1 أو P1 حسب التكوين) على واجهة شبكة VLAN مخصصة للمحول/الموجه متعدد الطبقات (VLAN 3) وموجه الإنترنت على واجهة شبكة VLAN مخصصة أيضا (VLAN4). زبون على VLAN1 و VLAN2.

التهيئة الأولية (يتم عرض الأجزاء ذات الصلة فقط)

```
interface VLAN1
  VLAN 1 DESC مستخدم
  عنوان IP 10.1.1.1 255.255.255.0
!
interface VLAN2
  VLAN 2 DESC مستخدم
  عنوان IP 10.1.2.1 255.255.255.0
!
interface VLAN3
  برنامج Cisco WSA المخصص لشبكة VLAN
  عنوان IP 192.168.1.1 255.255.255.252
!
VLAN4 قارن
```

موجه الإنترنت DESC لشبكة VLAN المخصصة
عنوان IP 192.168.2.1 255.255.255.252
!
ip route 0.0.0.0.0.0.0 192.168.2.2

بافتراض المثال المذكور أعلاه، و Cisco WSA الذي يحتوي على عنوان IP رقم 192.168.1.2، يمكنك إضافة الأوامر التالية لإعداد التوجيه المستند إلى السياسة (PBR):

الخطوة 1: تحديد حركة مرور الويب

! مطابقة حركة مرور HTTP
يسمح ب access-list 100 ب TCP 10.1.1.0.0.255 أي 80 eq
السماح ل access-list 100 ب TCP 10.1.2.0 0.0.255 أي 80 eq
! مطابقة حركة مرور HTTPS
يسمح ب access-list 100 ب TCP 10.1.1.0.0.255 any eq 443
يسمح ب access-list 100 ب TCP 10.1.2.0 0.0.0.255 any eq 443

الخطوة 2: حدد خريطة مسار للتحكم في مكان إخراج الحزم.

تصريح الويب المتقدم لخريطة الطريق 10
مطابقة عنوان IP 100
set ip next-hop 192.168.1.2

الخطوة 3: تطبيق خريطة المسار على الواجهة الصحيحة.

! لاحظ أنه يجب تطبيق هذا على واجهة المصدر (جانب العميل)
interface VLAN1
ip policy route-map ForwardWeb
!
interface VLAN2
ip policy route-map ForwardWeb

ملاحظة: تحتوي هذه الطريقة لإعادة توجيه حركة المرور (PBR) على بعض القيود. المشكلة الرئيسية مع هذا الأسلوب أن حركة المرور ستم دائما إعادة توجيهها إلى WSA حتى إذا لم يكن الجهاز يمكن الوصول إليه (بسبب مشاكل الشبكة على سبيل المثال). لذا، فليس هناك فشل بشأن الخيار.

لحل هذا النقص، يمكنك تكوين أي مما يلي:

1. PBR مع خيارات التبع عند استخدام موجهات Cisco. استعملت هذا سمة أن يدقق التوفر من التالي جنجل قبل أن يعيد حركة مرور.

المزيد من التفاصيل حول المقالة التالية:

[التوجيه المستند إلى السياسة مع مثال تكوين ميزة خيارات التعقب المتعددة](#)

2. خيارات التبع غير متوفرة لمحولات Cisco Catalyst Switches. ومع ذلك، هناك حل بديل متقدم متاح لتحقيق نفس السلوك.

يمكن العثور على التفاصيل على موقع Cisco Wiki التالي:

[التوجيه القائم على السياسة \(PBR\) مع تعقب محولات Catalyst 3xxx - حل بديل باستخدام IM](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا