حظر حزم ARP باستخدام قوائم الوصول إلى VLAN على شبكة الوصول إلى خارج MAC و 3750 و 3560 و 3550 و 2970 Catalyst محولات Series Switches

المحتويات

المقدمة

يناقش هذا وثيقة التشكيل ل cisco مادة حفازة 3550 sery مفتاح. أنت يستطيع استعملت أي مادة حفازة 2970، 3560، أو 3750 sery مفتاح في هذا سيناريو in order to نلت ال نفسه نتيجة. يوضح المستند كيفية تكوين قائمة التحكم في الوصول إلى MAC (ACL) لحظر الاتصال بين الأجهزة داخل شبكة VLAN. يمكنك حظر مضيف واحد أو مجموعة من البيئات المضيفة، بناء على صانع بطاقة واجهة الشبكة المضيفة (NIC) المهايئ. يمكنك حظر مجموعة من الأجهزة المضيفة إذا قمت بعدم السماح لحزم بروتوكول تحليل العنوان (ARP) التي تنشأ من هذه الأجهزة استنادا إلى تعيينات UI (IEEE Organization Unique Identifier) و company_id.

في شبكة ما، يمكنك حظر حزم طلب ARP لتقييد وصول المستخدم. في بعض سيناريوهات الشبكة، تريد حظر حزم ARP استنادا إلى عناوين MAC للطبقة 2، وليس إلى عنوان IP. أنت يستطيع أنجزت هذا نوع القيد إن يخلق أنت ماك عنوان ACLs و VLAN منفذ خريطة وطبقهم إلى VLAN قارن.

المتطلبات الأساسية

المتطلبات

ارجع إلى تعينات IEEE WI و Company_ID لتحديد تعيينات IEEE WI و Company_ID.

المكونات المستخدمة

المعلومات الواردة في هذا المستند قائمة على المحول Cisco Catalyst 3550 Switch.

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.

المنتجات ذات الصلة

آخر مفتاح أن يساند الأمر في هذا تشكيل يتضمن مادة حفازة 2970، 3560، أو 3750 sery مفتاح.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

in order to شكلت {upper{mac address يصفي وطبقت هو إلى ال VLAN قارن، أنت ينبغي أتمت عدة steps. أولا، أنت تقوم بإنشاء خرائط الوصول إلى شبكة VLAN لكل نوع من حركة المرور التي يجب تصفيتها. أنت تحدد عنوان MAC أو نطاق من عناوين MAC للحجب. أنت تحتاج أيضا إلى تحديد حركة مرور ARP في قائمة الوصول. وفقا RFC 826 ، يستخدم إطار ARP نوع بروتوكول الإيثرنت بالقيمة 0x806. يمكنك التصفية على هذا النوع من البروتوكولات كحركة مرور مثيرة للاهتمام لقائمة الوصول.

1. في وضع التكوين العام، قم بإنشاء قائمة وصول موسعة باسم MAC باسم ARP_Packet.أدخل الأمر **mac access-list extended** *acl_name* وأضف عنوان MAC المضيف أو العناوين التي تريد حظرها.

```
Switch(config)#mac access-list extended ARP_Packet
Switch(config-ext-nacl)#permit host 0000.861f.3745 host 0006.5bd8.8c2f 0x806 0x0
Switch(config-ext-nacl)#end
#(Switch(config
```

2. أدخل الأمر **vlan access-map** *map_ name* والأمر **action drop**، وهو الإجراء الذي يجب تنفيذه.يستخدم الأمر **vlan access-map** *map_ name* قائمة وصول MAC التي قمت بإنشائها لحظر حركة مرور ARP من الأجهزة المضيفة.

```
Switch(config)#vlan access-map block_arp 10

Switch (config-access-map)#action drop
Switch (config-access-map)#match mac address ARP_Packet
```

3. أضفت خط إضافي إلى ال نفسه VLAN منفذ خريطة in order to أرسلت الإستراحة من الحركة مرور.

```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```

4. أختر خريطة وصول إلى شبكة VLAN وتطبيقها على واجهة شبكة VLAN.دخلت **ال VLAN مرشح** vlan_number **vlan-list** *vlan_access_map_name* أمر.

```
Switch(config)#vlan filter block_arp vlan-list 2
```

عينة من التكوين

يقوم هذا التكوين العينة بإنشاء ثلاث قوائم وصول MAC وثلاث خرائط وصول VLAN. يطبق التكوين خريطة الوصول الثالثة لشبكة VLAN على واجهة شبكة VLAN رقم 2.

المحول Switch 3550

```
mac access-list extended ARP_Packet
permit host 0000.861f.3745 host 0006.5bd8.8c2f 0x806 0x0
is blocks communication between hosts with this MAC. ! mac access-list extended ARP_ONE_OUI permit ---!
8600.0000 0000.00ff.ffff any 0x806 0x0 !--- This blocks any ARP packet that originates from this vendor
  OUI. ! mac access-list extended ARP_TWO_OUI permit 0000.8600.0000 0000.00ff.ffff any 0x806 0x0 permit
6.5b00.0000 0000.00ff.ffff any 0x806 0x0 !--- This blocks any ARP packet that originates from these two
   vendor OUIs. ! vlan access-map block_arp 10 action drop match mac address ARP_Packet vlan access-map
k_arp 20 action forward vlan access-map block_one_oui 10 action drop match mac address ARP_ONE_OUI vlan
cess-map block_one_oui 20 action forward vlan access-map block_two_oui 10 action drop match mac address
O_OUI vlan access-map block_two_oui 20 action forward ! vlan filter block_two_oui vlan-list 2 !--- This
```

.applies the MAC ACL name "block_two_oui" to VLAN 2

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يمكنك التحقق مما إذا كان المحول قد تعلم عنوان MAC أو إدخال ARP قبل تطبيق قائمة التحكم في الوصول (ACL) إلى MAC. أدخل الأمر **show mac-address-table**، كما يوضح هذا المثال.

يدعم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) (للعملاء المسجلين فقط) أوامر **show** معينة. أستخدم CLI Analyzer (محلل واجهة سطر الأوامر) لعرض تحليل مخرج الأمر **show**.

```
switch#show mac-address-table dynamic vlan 2
                Mac Address Table
-------------------------------------------

 Vlan    Mac Address   Type        Ports
 -----   --------   -----------   ----
0000.861f.3745 DYNAMIC    Fa0/21  2
0006.5bd8.8c2f DYNAMIC    Fa0/22  2
Total Mac Addresses for this criterion: 2

                                        switch#show ip arp
Protocol  Address   Age (min)  Hardware Addr   Type  Interface
Internet  10.1.1.2         26  0000.861f.3745  ARPA  Vlan2
Internet  10.1.1.3         21  0006.5bd8.8c2f  ARPA  Vlan2
Internet  10.1.1.1          -  000d.65b6.9700  ARPA  Vlan2
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- دعم منتجات المحولات
- دعم تقنية تحويل شبكات LAN
- 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).