التعامل مع مشكلة عدم انتظام الخادم وارتفاع استخدام وحدة المعالجة المركزية (CPU) الناتج عن الدودة "الحمراء المشفرة"

المحتويات

المقدمة

يصف هذا وثيقة ال "رمز أحمر" ومشكلة أن الكلمة يستطيع سببت في cisco يوجه بيئة. ويصف هذا المستند أيضا تقنيات منع إصابة الدودة ويقدم إرتباطات لنصائح ذات صلة تصف حلول المشكلات المتعلقة بالدودة.

تقوم الدودة "Code Red" باستغلال حالة الضعف في خدمة الفهرس الخاصة بالإصدار 5.0 من Microsoft Internet Information Server (IIS). عندما تصيب دودة "الرمز الأحمر" مضيفا، فإنها تتسبب في قيام المضيف باستطلاع ونقل سلسلة عشوائية من عناوين IP، مما يتسبب في زيادة حادة في حركة مرور الشبكة. وهذه مشكلة بشكل خاص إذا كانت هناك إرتباطات متكررة في الشبكة و/أو لم يتم إستخدام إعادة التوجيه السريع (CEF) لتحويل الحزم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

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.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

كيف تصيب دودة "الشفرة الحمراء" أنظمة أخرى

تحاول الدودة "Code Red" الاتصال بعناوين IP التي تم إنشاؤها بشكل عشوائي. يمكن لكل خادم IIS مصاب أن يحاول إصابة نفس مجموعة الأجهزة. أنت يستطيع تتبعت المصدر عنوان و TCP ميناء من الدودة لأن هو لا ينتحف. يتعذر على إعادة توجيه المسار العكسي للبث الأحادي (uRPF) منع هجوم الدودة لأن عنوان المصدر قانوني.

النصائح التي تناقش دودة "الشفرة الحمراء"

تصف هذه الإرشادات دودة "رمز أحمر"، وتشرح كيفية تصحيح البرامج التي تأثرت بالدودة:

- إستشارات الأمان من Cisco: دودة "رمز أحمر" - تأثير العميل
- تجاوز سعة التخزين المؤقت لامتداد ISAPI الخاص بخادم فهرس IIS البعيد
- IDA. "رمز أحمر"
- سيرت؟ الطراز الاستشاري CA-2001-19 "Code Red" WORM الذي يستغل تجاوز سعة التخزين المؤقت في مكتبة الارتباط الديناميكي (DLL) الخاصة بخدمة فهرسة نظام المعلومات الإدارية (IIS)

الأعراض

فيما يلي بعض الأعراض التي تشير إلى أن موجه Cisco يتأثر بدودة "الرمز الأحمر":

- عدد كبير من التدفقات في جداول NAT أو PAT (إذا كنت تستخدم NAT أو PAT).
- عدد كبير من طلبات ARP أو عواصف ARP في الشبكة (بسبب مسح عنوان IP).
- الاستخدام المفرط للذاكرة بواسطة إدخال IP وإدخال ARP وذاكرة التخزين المؤقت ل IP وعمليات CEF.
- إستخدام عال لوحدة المعالجة المركزية في ARP وإدخال IP و CEF و IPC.

- إستخدام عال لوحدة المعالجة المركزية (CPU) على مستوى المقاطعة بمعدلات حركة مرور منخفضة، أو إستخدام عال لوحدة المعالجة المركزية (CPU) على مستوى العملية في إدخال IP، إذا كنت تستخدم NAT.

يمكن أن تتسبب حالة انخفاض الذاكرة أو إستخدام وحدة المعالجة المركزية (CPU) بشكل كبير ومستدام (100 في المائة) على مستوى المقاطعة في إعادة تحميل موجه Cisco IOS®. ينتج إعادة التحميل عن عملية تسيء التصرف بسبب حالات الإجهاد.

إذا كنت لا تشك في أن الأجهزة الموجودة في الموقع الخاص بك مصابة بدودة "الرمز الأحمر" أو أنها الهدف منها، فراجع قسم المعلومات ذات الصلة للحصول على عناوين URLs إضافية حول كيفية أستكشاف أي مشاكل تواجهها وإصلاحها.

تعرف على الجهاز المصاب

أستخدم تحويل التدفق لتعريف عنوان IP المصدر للجهاز المتأثر. قم بتكوين ip route-cache flow على جميع الواجهات لتسجيل جميع التدفقات التي تم تحويلها بواسطة الموجه.

بعد بضع دقائق، قم بإصدار الأمر show ip cache flow لعرض الإدخالات المسجلة. خلال المرحلة الأولية من عدوى دودة "الشفرة الحمراء"، تحاول الدودة تكرار نفسها. يحدث النسخ المتماثل عندما ترسل الدودة طلبات HT إلى عناوين IP العشوائية. لذلك، أنت ينبغي بحث عن تدفق ذاكرة التخزين المؤقت مع غاية ميناء 80 (0050 ،HT في hex).

سير عمل show ip cache | يتضمن أمر 0050 يعرض كل إدخالات التخزين المؤقت مع منفذ 0050) 80 TCP في hex):

```
Router#show ip cache flow | include 0050
...

scram        scrappers    dative      DstIPaddress   Pr SrcP  DstP  Pkts
Vl1       193.23.45.35       Vl3        2.34.56.12    06 0F9F  0050     2
Vl1     211.101.189.208      Null     158.36.179.59    06 0457  0050     1
Vl1       193.23.45.35       Vl3      34.56.233.233    06 3000  0050     1
Vl1      61.146.138.212      Null     158.36.175.45    06 B301  0050     1
Vl1       193.23.45.35       Vl3      98.64.167.174    06 0EED  0050     1
Vl1      202.96.242.110      Null     158.36.171.82    06 0E71  0050     1
Vl1       193.23.45.35       Vl3      123.231.23.45    06 121F  0050     1
Vl1       193.23.45.35       Vl3       9.54.33.121    06 1000  0050     1
Vl1       193.23.45.35       Vl3       78.124.65.32    06 09B6  0050     1
Vl1      24.180.26.253       Null     158.36.179.166    06 1132  0050     1
```

إذا عثرت على عدد كبير بشكل غير طبيعي من الإدخالات مع نفس عنوان IP المصدر، وعنوان IP للوجهة العشوائية[1]، و (HTTP DSTp = 0050)، و (TCP PR = 06)، تكون قد حددت جهازا مصابا. في مثال الإخراج هذا، يكون عنوان IP للمصدر 193.23.45.35 ويأتي من VLAN1.

[1] لا يختار إصدار آخر من الدودة "Code Red"، يسمى "Code Red II"، عنوان IP للوجهة العشوائية تماما. بدلا من ذلك، يحتفظ "Code Red II" بجزء الشبكة من عنوان IP، ويختار جزء مضيف عشوائي من عنوان IP من أجل النشر. وهذا يسمح للدودة بنشر نفسها بشكل أسرع داخل الشبكة نفسها.

يستخدم "رمز أحمر II" هذه الشبكات والأقنعة:

```
Mask          Probability of Infection
      (random) 12.5%          0.0.0.0
(same class A) 50.0%        255.0.0.0
(same class B) 37.5%      255.255.0.0
```

عناوين IP الهدف التي يتم إستبعادها هي x.x.x.127 و x.x.x.224، ولا يسمح بأن يكون أي نظام ثماني 0 أو 255.

بالإضافة إلى ذلك، لا يحاول المضيف إعادة إصابة نفسه بالعدوى.

لمزيد من المعلومات، راجع الشفرة الحمراء (II) .

في بعض الأحيان، لا يمكنك تشغيل NetFlow لاكتشاف محاولة إصابة "Code Red". قد يحدث هذا لأنك تقوم بتشغيل إصدار من التعليمات البرمجية التي لا تدعم NetFlow، أو لأن الموجه لديه ذاكرة غير كافية أو مجزأة بشكل مفرط لتمكين NetFlow. cisco يوصي أن لا يمكن أنت NetFlow عندما هناك يتعدد مدخل قارن وفقط واحد مخرج قارن على المسحاج تخديد، لأن NetFlow حسبت على المدخل ممر. في هذه الحالة، من الأفضل أن يمكن محاسبة IP على واجهة مخرج وحيد.

ملاحظة: يقوم الأمر ip accounting بتعطيل DCEF. لا تقم بتمكين محاسبة IP على أي نظام أساسي حيث تريد إستخدام تحويل DCEF.

```
Router(config)#interface vlan 1000
Router(config-if)#ip accounting
```

```
Router#show ip accounting
Source          Destination      Packets               Bytes
  96                2          75.246.253.88    20.1.145.49
  48                1          17.152.178.57    20.1.145.43
  48                1            20.1.49.132    20.1.145.49
  96                2         169.187.190.170   20.1.104.194
 213                3              20.1.1.11   20.1.196.207
  48                1          43.129.220.118   20.1.145.43
  48                1          43.209.226.231    20.1.25.73
  96                2          169.45.103.230   20.1.104.194
  96                2           223.179.8.154    20.1.25.73
  96                2           169.85.92.164   20.1.104.194
 204                3              20.1.1.11    20.1.81.88
  96                2          169.252.106.60   20.1.104.194
  96                2           126.60.86.19   20.1.145.43
  96                2          43.134.116.199   20.1.145.49
  96                2          169.234.36.102   20.1.104.194
  96                2          15.159.146.29    20.1.145.49
```

في إخراج الأمر show ip accounting، ابحث عن عناوين المصدر التي تحاول إرسال الحزم إلى عناوين وجهة متعددة. إذا كان المضيف المصاب في مرحلة المسح الضوئي، فإنه يحاول إنشاء إتصالات HTTP بالموجهات الأخرى. لذلك ستشاهد محاولات للوصول إلى عناوين IP متعددة. تفشل معظم محاولات الاتصال هذه عادة. لذلك، ترى عدد قليل فقط من الحزم التي تم نقلها، كل منها بعدد بايت صغير. في هذا المثال، من المحتمل أن يكون 20.1.145.49 و 20.1.104.194 مصابين.

عندما تقوم بتشغيل التحويل متعدد الطبقات (MLS) على المادة حفازة sery 5000 ومادة حفازة sery 6000، أنت ينبغي أخذت خطوات مختلفة لتمكين حساب NetFlow وتتبع التواجد. في محول Cat6000 مزود ببطاقة ميزة Supervisor 1 Multilayer Switch Feature Card (MSFC1) أو SUP I/MSFC2، يتم تمكين MLS المستندة إلى NetFlow بشكل افتراضي، ولكن وضع التدفق هو الوجهة فقط. لذلك، لم يتم تخزين عنوان IP المصدر مؤقتا. يمكنك تمكين وضع "التدفق الكامل" لتعقب الأجهزة المضيفة المصابة باستخدام الأمر set mls flow full على المشرف.

للصيغة المختلطة، أستخدم الأمر **set mls flow full**:

```
6500-sup(enable)set mls flow full
.Configured IP flowmask is set to full flow
Warning: Configuring more specific flow mask may dramatically
.increase the number of MLS entries
```

بالنسبة لوضع IOS الأصلي، أستخدم الأمر mls flow ip full:

```
Router(config)#mls flow ip full
```

عندما تقوم بتمكين وضع "التدفق الكامل"، يتم عرض تحذير للإشارة إلى زيادة كبيرة في إدخالات MLS. يكون تأثير إدخالات MLS المتزايدة مبررا لمدة قصيرة إذا كانت شبكتك مليئة بالفعل بالدودة "Code Red". تتسبب الدودة في زيادة إدخالات MLS بشكل كبير وفي الارتفاع.

لعرض المعلومات المجمعة، أستخدم الأوامر التالية:

للصيغة المختلطة، أستخدم الأمر **set mls flow full**:

```
6500-sup(enable)set mls flow full
.Configured IP flowmask is set to full flow
Warning: Configuring more specific flow mask may dramatically
.increase the number of MLS entries
```

بالنسبة لوضع IOS الأصلي، أستخدم الأمر **mls flow ip full**:

```
Router(config)#mls flow ip full
```

عندما تقوم بتمكين وضع "التدفق الكامل"، يتم عرض تحذير للإشارة إلى زيادة كبيرة في إدخالات MLS. يكون تأثير إدخالات MLS المتزايدة مبررا لمدة قصيرة إذا كانت شبكتك مليئة بالفعل بالدودة "Code Red". تتسبب الدودة في زيادة إدخالات MLS بشكل كبير وفي الارتفاع.

لعرض المعلومات المجمعة، أستخدم الأوامر التالية:

بالنسبة للوضع المختلط، أستخدم الأمر show mls ent:

```
6500-sup(enable)show mls ent
 Destination-IP  Source-IP     Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst
                  ESrc DPort     SPort     Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ----------------- ------ ------ ----- --------------- --------------
                -------- -------- ----------- ---------- --------- --------- ----
```

ملاحظة: يتم ملء جميع هذه الحقول عندما تكون في وضع "التدفق الكامل".

بالنسبة لوضع IOS الأصلي، أستخدم الأمر **show mls ip**:

```
Router#show mls ip
DstIP           SrcIP           Prot:SrcPort:DstPort  Dst i/f:DstMAC
-------------------------------------------------------------------------
  Pkts         Bytes       SrcDstPorts    SrcDstEncap Age   LastSeen
-------------------------------------------------------------------------
```

عندما يحدد أنت المصدر عنوان وغاية ميناء متورط في الهجوم، أنت يستطيع ثبتت MLS إلى الخلف إلى "غاية فقط" أسلوب.

بالنسبة للوضع المختلط، أستخدم الأمر set mls flow destination:

```
6500-sup(enable) set mls flow destination
<Usage: set mls flow <destination|destination-source|full
```

بالنسبة لوضع IOS الأصلي، أستخدم الأمر mls flow ip destination:

```
Router(config)#mls flow ip destination
```

تتم حماية مجموعة Supervisor (SUP) II/MSFC2 من الهجوم لأنه يتم إجراء تحويل CEF في الأجهزة، ويتم الحفاظ على إحصائيات NetFlow. لذلك، حتى أثناء هجوم "رمز أحمر"، إذا قمت بتمكين وضع التدفق الكامل، فإن الموجه لا يتم إبطاله، بسبب آلية التحويل الأسرع. الأوامر لتمكين وضع التدفق الكامل وعرض الإحصائيات هي نفسها على كل من SUP I/MFSC1 و SUP II/MSFC2.

تقنيات الوقاية

أستخدم التقنيات المدرجة في هذا القسم لتقليل تأثير دودة "الرمز الأحمر" على الموجه إلى الحد الأدنى.

حظر حركة المرور إلى المنفذ 80

إذا كان من الممكن عمليا في شبكتك، فإن أسهل طريقة لمنع هجوم "الرمز الأحمر" هي منع جميع حركة المرور إلى المنفذ 80، وهو المنفذ المعروف جيدا ل WWW. قم بإنشاء قائمة وصول لرفض حزم IP الموجهة إلى المنفذ 80 وتطبيقها الواردة على الواجهة التي تواجه مصدر العدوى.

تقليل إستخدام ذاكرة إدخال ARP

يستخدم إدخال ARP كميات كبيرة من الذاكرة عندما يشير المسار الثابت إلى واجهة بث، مثل هذا:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

يتم إرسال كل حزمة للمسار الافتراضي إلى شبكة VLAN3. مهما، هناك ما من بعد جنجل عنوان يعين، لذلك، المسحاج تخديد يرسل طلب ARP للغاية عنوان. يرد موجه الخطوة التالية لتلك الوجهة بعنوان MAC الخاص به، ما لم يتم تعطيل ARP للوكيل. يخلق الرد من المسحاج تخديد مدخل إضافي في ال ARP طاولة حيث الغاية عنوان من الربط خططت إلى التالي جنجل عنوان MAC. ترسل الدودة "Code Red" الحزم إلى عناوين IP العشوائية، والتي تضيف إدخال ARP جديد لكل عنوان وجهة عشوائي. يستهلك كل إدخال ARP جديد المزيد من الذاكرة تحت عملية إدخال ARP.

لا تقم بإنشاء مسار افتراضي ثابت إلى واجهة، خاصة إذا كانت الواجهة تبث (Ethernet/Fast Ethernet/GE/SMDS أو متعددة النقاط (ترحيل الإطارات/ATM). يجب أن يشير أي مسار افتراضي ثابت إلى عنوان IP الخاص بموجه الخطوة التالية. بعد تغيير المسار الافتراضي إلى الإشارة إلى عنوان IP للجنجل التالي، أستخدم الأمر **clear arp-cache** لمسح جميع إدخالات ARP. يقوم هذا الأمر بإصلاح مشكلة إستخدام الذاكرة.

إستخدام تحويل إعادة التوجيه السريع (CEF) (Cisco Express Forwarding)

لتقليل إستخدام وحدة المعالجة المركزية (CPU) على موجه IOS، قم بالتغيير من التحويل السريع/الأمثل NetFlow/ إلى تحويل CEF. هناك بعض المحاذير لتمكين CEF. يناقش القسم التالي الفرق بين إعادة التوجيه السريع والتبديل السريع، ويشرح التأثيرات عند تمكين إعادة التوجيه السريع (CEF).

إعادة التوجيه السريع مقابل التحويل السريع من Cisco

تمكين ميزة إعادة التوجيه السريع (CEF) من تخفيف الحمل المتزايد لحركة المرور الناجم عن دودة "الرمز الأحمر". برنامج IOS® الإصدارات 11.1((12.0، CC، والدعم اللاحق CEF على الأنظمة الأساسية Cisco 7200/7500/GSR. يتوفر دعم CEF على الأنظمة الأساسية الأخرى في برنامج Cisco IOS الإصدار 12.0 أو إصدار أحدث. يمكنك إجراء المزيد من التحقيقات باستخدام أداة Software Advisor (مرشد البرامج).

في بعض الأحيان، لا يمكنك تمكين CEF على جميع الموجهات لأحد الأسباب التالية:

- الذاكرة غير كافية
- بنى منصات العمل غير المدعومة
- عمليات تضمين الواجهة غير المدعومة

سلوك التحويل السريع وتداعياته

فيما يلي المعاني الضمنية عند إستخدام التحويل السريع:

- ذاكرة التخزين المؤقت التي تستند إلى حركة مرور البيانات — تكون ذاكرة التخزين المؤقت فارغة حتى يقوم الموجه بتحويل الحزم وملء ذاكرة التخزين المؤقت.
- أول حزمة يتم تحويلها للعملية - أول حزمة يتم تحويلها للعملية، لأن ذاكرة التخزين المؤقت فارغة في البداية.
- ذاكرة التخزين المؤقت متعددة المستويات — يتم إنشاء ذاكرة التخزين المؤقت في جزء إدخال قاعدة معلومات التوجيه (RIB) الأكثر تحديدا في شبكة رئيسية. إذا كان RIB يحتوي على /24s للشبكة الرئيسية 131.108.0.0، فإن ذاكرة التخزين المؤقت يتم بناؤها مع /24s لهذه الشبكة الرئيسية.
- /32 يتم إستخدام ذاكرة التخزين المؤقت—/32 يتم إستخدام ذاكرة التخزين المؤقت لموازنة الحمل لكل وجهة. عندما تقوم ذاكرة التخزين المؤقت بموازنة التحميل، يتم بناء ذاكرة التخزين المؤقت ب /32s لتلك الشبكة الرئيسية.**ملاحظة:** من المحتمل أن يتسبب هذان العددان الأخيران في وجود ذاكرة تخزين مؤقت ضخمة تستهلك جميع الذاكرة.
- التخزين المؤقت في حدود الشبكة الرئيسية — باستخدام المسار الافتراضي، يتم إجراء التخزين المؤقت في حدود الشبكة الرئيسية.
- مدير ذاكرة التخزين المؤقت — يعمل مدير ذاكرة التخزين المؤقت كل دقيقة ويتحقق من 20/1 (5 في المائة) من ذاكرة التخزين المؤقت للإدخالات غير المستخدمة في حالات الذاكرة العادية، و 4/1 (25 في المائة) من ذاكرة التخزين المؤقت في حالة انخفاض الذاكرة (200 ك).

لتغيير القيم الواردة أعلاه، أستخدم الأمر **ip cache-ager-interval X Y Z**، حيث:

- X هو <0-2147483> عدد الثواني بين عمليات التشغيل غير النشطة. الافتراضي = 60 ثانية.
- Y هي <2-50> 1/(Y+1) من ذاكرة التخزين المؤقت إلى العمر لكل تشغيل (ذاكرة منخفضة). الافتراضي = 4.
- Z هو <3-100> 1/(Z+1) من ذاكرة التخزين المؤقت إلى العمر لكل تشغيل (عادي). الافتراضي = 20.

هنا عينة تشكيل أن يستعمل **ip cache-ager 60 5 25**.

```
Router#show ip cache
IP routing cache 2 entries, 332 bytes
adds, 25 invalidates, 0 refcounts 27
.(Cache aged by 1/25 every 60 seconds (1/5 when memory is low
,Minimum invalidation interval 2 seconds, maximum interval 5 seconds
quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 03:55:12 ago

Prefix/Length          Age    Interface     Next Hop
Serial1       4.4.4.1    03:44:53        4.4.4.1/32
Ethernet1    20.4.4.1    00:03:15    192.168.9.0/24

Router#show ip cache verbose
IP routing cache 2 entries, 332 bytes
adds, 25 invalidates, 0 refcounts 27
.(Cache aged by 1/25 every 60 seconds (1/5 when memory is low
,Minimum invalidation interval 2 seconds, maximum interval 5 seconds
quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 03:57:31 ago
Prefix/Length       Age       Interface       Next Hop
Serial1         4.4.4.1  03:47:13          4.4.4.1/32-24
```

```
                                        0F000800   4
Ethernet1       20.4.4.1  00:05:35        192.168.9.0/24-0
                00000C34A7FC00000C13DBA90800  14
```

بناء على إعداد نص ذاكرة التخزين المؤقت، تخرج بعض النسبة المئوية لإدخالات ذاكرة التخزين المؤقت الخاصة بك من جدول ذاكرة التخزين المؤقت السريعة. عندما يتم تدفق الإدخالات بسرعة، تصبح نسبة أكبر من قيم جدول ذاكرة التخزين المؤقت السريعة، ويصبح جدول ذاكرة التخزين المؤقت أصغر. ونتيجة لذلك، يقل إستهلاك الذاكرة على الموجه. العيب هو أن حركة المرور تستمر في التدفق للإدخالات التي تم تقادمها من جدول ذاكرة التخزين المؤقت. يتم تحويل الحزم الأولية للعملية، مما يتسبب في حدوث إرتفاع قصير في إستهلاك وحدة المعالجة المركزية في **إدخال IP** حتى يتم إنشاء إدخال ذاكرة تخزين مؤقت جديد للتدفق.

من برنامج Cisco IOS الإصدار 10.3(8) و 11.0(3) والإصدارات الأحدث، يتم معالجة عميل ذاكرة التخزين المؤقت ل IP بشكل مختلف، كما هو موضح هنا:

- لا يتوفر الأمر **ip cache-ager-interval** و**ip cache-invalidate-delay** إلا إذا تم تعريف الأمر **service internal** في التكوين.
- إذا تم تعيين الفترة بين الإبطال غير الهام إلى 0، يتم تعطيل العملية غير النشطة بالكامل.
- يتم التعبير عن الوقت بالثواني.

ملاحظة: عند تنفيذ هذه الأوامر، يزداد إستخدام وحدة المعالجة المركزية (CPU) للموجه. أستخدم هذه الأوامر فقط عند الضرورة المطلقة.

```
? Router#clear ip cache
A.B.C.D Address prefix
!CR>--> will clear the entire cache and free the memory used by it>

Router#debug ip cache
IP cache debugging is on
```

فوائد إعادة التوجيه السريع

- يتم إنشاء جدول قاعدة معلومات إعادة التوجيه (FIB) استنادا إلى جدول التوجيه. لذلك، توجد معلومات إعادة التوجيه قبل إعادة توجيه الحزمة الأولى. كما يحتوي FIB على /32 إدخالا لمضيفي الشبكة المحلية (LAN) المتصلة مباشرة.
- يحتوي جدول التجاور (ADJ) على معلومات إعادة كتابة الطبقة 2 للنقلات التالية والمضيفين المتصلين مباشرة (يقوم إدخال ARP بإنشاء تجاور CEF).
- لا يوجد مفهوم رهان ذاكرة التخزين المؤقت مع CEF لزيادة إستخدام وحدة المعالجة المركزية. يتم حذف إدخال FIB في حالة حذف إدخال جدول توجيه.

تحذير: مرة أخرى، يعني المسار الافتراضي الذي يشير إلى واجهة بث أو متعدد النقاط أن الموجه يرسل طلبات ARP لكل وجهة جديدة. من المحتمل أن تقوم طلبات ARP من الموجه بإنشاء جدول تجاور ضخم حتى تنفذ ذاكرة الموجه. إذا فشل CEF في تخصيص CEF/DCEF للذاكرة، فإنه يعطل نفسه. ستحتاج إلى تمكين CEF/DCEF يدويا مرة أخرى.

نموذج الإخراج: CEF

وفيما يلي بعض مخرجات عينة من الأمر show ip cef summary ، الذي يعرض إستخدام الذاكرة. هذا الإخراج هو لقطة من خادم المسار Cisco 7200 باستخدام برنامج Cisco IOS الإصدار 12.0.

```
Router>show ip cef summary
(IP CEF with switching (Table Version 2620746
routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 84625 109212
leaves, 8000 nodes, 22299136 bytes, 2620745 inserts, 2511533 109212
                                                        invalidations
load sharing elements, 5712 bytes, 109202 references 17
```

```
                universal per-destination load sharing algorithm, id 6886D006
                                CEF resets, 1 revisions of existing leaves 1
                                        in-place/0 aborted modifications 1
                       (Resolution Timer: Exponential (currently 1s, peak 16s
                                    refcounts:  2258679 leaf, 2048256 node

                                          Adjacency Table has 16 adjacencies


                                    Router>show processes memory | include CEF
    PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
CEF process 0          0          146708     1700       147300     0   73
CEF Scanner 0          0          7404       0          608        0   84


                                    Router>show processes memory | include BGP

   BGP Open 0          0          6864       6891444    6891444    0   2
   BGP Open 0          0          8028       2296       3444       0   80
   BGP Open 0          0          7944       476420     477568     0   86
 BGP Router 0          0          338145696  102734200  2969013892 0   87
    BGP I/O 4954624    131160     7440       2517286276 56693560   0   88
BGP Scanner 0          0          75308      68633812   69280      0   89
   BGP Open 0          0          6876       6564264    6564264    0   91
   BGP Open 0          780        6796       7633052    7635944    0   101
   BGP Open 0          0          6796       7591724    7591724    0   104
   BGP Open 0          780        6796       7266840    7269732    0   105
   BGP Open 0          0          6796       7600908    7600908    0   109
   BGP Open 0          780        6796       7265692    7268584    0   110


                                  Router>show memory summary | include FIB

                         Alloc PC        Size     Blocks      Bytes    What
                  0x60B8821C        448          7       3136    FIB: FIBIDB
          0x60B88610      12000          1      12000    FIB: HWIDB MAP TABLE
                 0x60B88780        472          6       2832    FIB: FIBHWIDB
                 0x60B88780        508          1        508    FIB: FIBHWIDB
           0x60B8CF9C       1904          1       1904    FIB 1 path chunk pool
           0x60B8CF9C      65540          1      65540    FIB 1 path chunk pool
                0x60BAC004       1904        252     479808    FIB 1 path chun
                0x60BAC004      65540        252   16516080    FIB 1 path chun


                                  Router>show memory summary | include CEF

              0x60B8CD84       4884          1       4884    CEF traffic info
                   0x60B8CF7C         44          1         44    CEF process
            0x60B9D12C      14084          1      14084    CEF arp throttle chunk
               0x60B9D158        828          1        828    CEF loadinfo chunk
               0x60B9D158      65540          1      65540    CEF loadinfo chunk
                 0x60B9D180        128          1        128    CEF walker chunk
                 0x60B9D180        368          1        368    CEF walker chunk
                   0x60BA139C         24          5        120    CEF process
                   0x60BA139C         40          1         40    CEF process
                   0x60BA13A8         24          4         96    CEF process
                   0x60BA13A8         40          1         40    CEF process
                   0x60BA13A8         72          1         72    CEF process
                   0x60BA245C         80          1         80    CEF process
                   0x60BA2468         60          1         60    CEF process
               0x60BA65A8      65488          1      65488    CEF up event chunk


                                  Router>show memory summary | include adj
```

```
0x60B9F6C0        280          1        280    NULL adjacency
0x60B9F734        280          1        280    PUNT adjacency
0x60B9F7A4        280          1        280    DROP adjacency
0x60B9F814        280          1        280    Glean adjacency
0x60B9F884        280          1        280    Discard adjacency
0x60B9F9F8      65488          1      65488    Protocol adjacency chunk
```

امور يجب التأمل فيها

عندما يكون عدد التدفقات كبيرا، تستهلك إعادة التوجيه السريع (CEF) بشكل نموذجي ذاكرة أقل من التحويل السريع. إذا كانت الذاكرة مستهلكة بالفعل من قبل ذاكرة تخزين مؤقت للتحويل السريع، فيجب عليك مسح ذاكرة تخزين ARP المؤقت (من خلال الأمر **clear ip arp**) قبل تمكين ميزة إعادة التوجيه السريع (CEF).

ملاحظة: عند مسح ذاكرة التخزين المؤقت، يحدث إرتفاع في إستخدام وحدة المعالجة المركزية للموجه.

"الشفرة الحمراء" غالبا أسئلة و إجاباتها

س. أستخدم NAT، وأتمتع باستخدام 100 بالمائة من وحدة المعالجة المركزية (CPU) في إدخال IP. عندما أقوم بتنفيذ عرض وحدة المعالجة المركزية (CPU)، يكون إستخدام وحدة المعالجة المركزية (CPU) الخاصة بي مرتفعا في مستوى المقاطعة - 99/100 أو 98/99. هل يمكن ربط ذلك ب "رمز أحمر"؟

a. هناك مؤخرا يثبت nat cisco بق (CSCdu63623 (يسجل زبون فقط) أن يتضمن قابلية توسع. عند وجود عشرات الآلاف من تدفقات NAT (استنادا إلى نوع النظام الأساسي)، يتسبب الخطأ في إستخدام 100 بالمائة من وحدة المعالجة المركزية (CPU) على مستوى المعالجة أو المقاطعة.

لتحديد ما إذا كان هذا الخطأ هو السبب، قم بإصدار الأمر **show align**، وتحقق ما إذا كان الموجه يواجه أخطاء المحاذاة. إذا رأيت أخطاء المحاذاة أو الوصول الزائف للذاكرة، قم بإصدار الأمر **show align** عدة مرات وانظر إذا كانت الأخطاء في إرتفاع. إذا كان عدد الأخطاء في أزدياد، يمكن أن تكون أخطاء المحاذاة سبب إستخدام وحدة المعالجة المركزية المرتفع على مستوى المقاطعة، وليس أخطاء CSCdu63623 Cisco (العملاء المسجلون فقط). لمزيد من المعلومات، ارجع إلى أستكشاف الأخطاء الزائفة للوصول والمحاذاة وإصلاحها.

يعرض الأمر **show ip nat translation** عدد الترجمات النشطة. نقطة الانهيار لمعالج فئة NPE-300 هي حوالي 20،000 إلى 40،000 ترجمة. يختلف هذا الرقم بناء على النظام الأساسي.

وقد لاحظ بعض الزبائن سابقا مشكلة الانهيار هذه، ولكن بعد عرض "الشفرة الحمراء"، واجه المزيد من العملاء هذه المشكلة. الوحيد workaround أن يركض nat (بدلا من ضرب)، لذلك هناك أقل ترجمة نشط. إذا كان لديك 7200، فاستخدم NSE-1، وقم بخفض قيم مهلة NAT.

س. أنا أدير IRB، وأواجه إستخدام عال لوحدة المعالجة المركزية في عملية إدخال HyBridge. لماذا يحدث هذا؟ هل له علاقة ب "الشفرة الحمراء"؟

أ. تتعامل عملية إدخال HyBridge مع أي حزم لا يمكن تحويلها بسرعة بواسطة عملية IRB. يمكن أن يكون عدم قدرة عملية IRB على تبديل الحزمة بسرعة بسبب:

- الحزمة هي حزمة بث.
- الحزمة هي حزمة بث متعدد.
- الوجهة غير معروفة، ويلزم تشغيل ARP.
- هناك وحدات بيانات بروتوكول الجسر (BPDUs) للشجرة المتفرعة.

يواجه إدخال HyBridge مشاكل إذا كان هناك آلاف من واجهات الاتصال من نقطة إلى نقطة في نفس مجموعة الجسر. يواجه HyBridge Input أيضا بعض المشاكل (ولكن بدرجة أقل) إذا كان هناك الآلاف من نقاط الدخول الثابتة في نفس الواجهة البينية متعددة النقاط.

ما هي الاسباب المحتملة للمشاكل مع ال IRB؟ افترض أن جهاز مصاب ب "رمز أحمر" يقوم بفحص عناوين IP.

- يحتاج المسحاج تخديد أن يرسل طلب ARP لكل غاية عنوان. ينتج فيض من طلبات ARP على كل VC في مجموعة الجسر لكل عنوان تم مسحه ضوئيا. لا تتسبب عملية ARP العادية في حدوث مشكلة في وحدة المعالجة المركزية. ومع ذلك، إذا كان هناك إدخال ARP بدون إدخال جسر، فإن الموجه يفيض الحزم الموجهة للعناوين التي توجد لها إدخالات ARP بالفعل. يمكن أن يتسبب ذلك في إستخدام عال لوحدة المعالجة المركزية (CPU) لأن حركة مرور البيانات تم تحويلها للعملية. لتجنب المشكلة، قم بزيادة وقت تقادم الجسر (الافتراضي 300 ثانية أو 5 دقائق) لمطابقة أو تجاوز مهلة ARP (الافتراضي 4 ساعات) حتى تتم مزامنة المؤقتين.
- العنوان الذي يحاول المضيف النهائي إصابته هو عنوان بث. يفعل الموجه ما يعادل بث شبكة فرعية يلزم نسخه بواسطة عملية إدخال HyBridge. ولا يحدث هذا إذا تم تكوين الأمر **no ip directed-broadcast**. من برنامج Cisco IOS الإصدار 12.0، يتم تعطيل الأمر **ip directed-broadcast** بشكل افتراضي، وهو ما يتسبب في إسقاط جميع عمليات البث الموجهة إلى IP.
- فيما يلي ملاحظة جانبية لا ترتبط ب "رمز أحمر" وتتعلق ببنى IRB:يلزم نسخ حزم البث المتعدد والبث من الطبقة 2. لذلك، يمكن أن تؤدي مشكلة في خوادم IPX التي يتم تشغيلها على مقطع بث إلى قطع الارتباط. يمكنك إستخدام سياسات المشترك لتجنب المشكلة. لمزيد من المعلومات، ارجع إلى دعم جسر خط المشترك الرقمي X (xDSL). يجب أيضا مراعاة قوائم الوصول إلى الجسر، التي تحد من نوع حركة المرور المسموح بها للمرور عبر الموجه.
- من أجل تخفيف مشكلة IRB هذه، يمكنك إستخدام مجموعات جسر متعددة، وضمان وجود تخطيط واحد إلى واحد ل BVIs، الواجهات الفرعية و VCs.
- يعتبر RBE أعلى من IRB لأنه يجنب مكدس التوصيل بالكامل. يمكنك الترحيل إلى RBE من IRB. وهذه الأخطاء من Cisco تلهم مثل هذا الترحيل:CSCdr1146 (العملاء المسجلون فقط)CSCdp18572 (العملاء المسجلون فقط)CSCds40806 (العملاء المسجلون فقط)

نسبة إستخدام وحدة المعالجة المركزية (CPU) عالية عند مستوى المقاطعة، كما أنني أستلم بعض الحركات في حالة محاولة إستخدام سجل العرض. كما أن معدل حركة المرور أعلى قليلا من المعدل الطبيعي. فما هو سبب ذلك؟

a. هنا مثال على إخراج الأمر **show logging**:

```
Router#show logging
(Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns
                          ^
  this value is non-zero
          Console logging: level debugging, 9 messages logged
```

تحقق ما إذا كنت قد قمت بتسجيل الدخول إلى وحدة التحكم أم لا. إذا كان الأمر كذلك، فتحقق مما إذا كانت هناك طلبات HTTP لحركة مرور البيانات. بعد ذلك، تحقق مما إذا كانت هناك أي قوائم وصول تحتوي على كلمات أساسية للسجل أو تصحيح الأخطاء التي تراقب تدفقات IP معينة. إذا كانت التوهجات في إرتفاع، فقد يكون ذلك بسبب عدم قدرة وحدة التحكم، التي عادة ما تكون جهاز بود 9600، على معالجة كمية المعلومات المستلمة. في هذا السيناريو، يقوم الموجه بتعطيل المقاطعات ولا يفعل شيئا سوى معالجة رسائل وحدة التحكم. يتمثل الحل في تعطيل تسجيل وحدة التحكم أو إزالة أي نوع من التسجيل تقوم به.

Q. يمكنني رؤية العديد من محاولات اتصال HTTP على موجه IOS الخاص بي الذي يشغل ip http-server. هل هذا يسبب فحص الدودة "الأحمر الشفرة"؟

أ. يمكن أن يكون "رمز أحمر" السبب هنا. توصي Cisco بتعطيل الأمر **ip http server** على موجه IOS حتى لا يحتاج إلى التعامل مع العديد من محاولات الاتصال من الأجهزة المضيفة المصابة.

الحلول

هناك حلول بديلة مختلفة تناقش في النصائح التي تناقش قسم دودة "الشفرة الحمراء". ارجع إلى إستشارات الحلول البديلة.

وهناك طريقة أخرى لحظر "رمز أحمر" في نقاط الدخول إلى الشبكة تستخدم قوائم التحكم في الوصول (ACL) والتعرف على التطبيق المستند إلى الشبكة (NBAR) داخل برنامج IOS على موجهات Cisco. أستخدم هذه الطريقة بالاقتران مع برامج التصحيح الموصى بها لخوادم IIS من Microsoft. لمزيد من المعلومات حول هذه الطريقة، ارجع إلى إستخدام قوائم التحكم في الوصول (ACLs) وقوائم التحكم في الوصول (NBAR) لحظر الكلمة "رمز أحمر" في نقاط الدخول إلى الشبكة.

معلومات ذات صلة

- أستكشاف مشكلات الذاكرة وإصلاحها
- أستكشاف أخطاء تسريبات المخزن المؤقت وإصلاحها
- استكشاف أخطاء الاستخدام العالي لوحدة المعالجة المركزية على موجّهات Cisco وإصلاحها
- أستكشاف أخطاء الموجه وإصلاحها
- أستكشاف الأخطاء وإصلاحها بالملاحظات الفنية - الموجهات
- أستكشاف أخطاء الموجه وإصلاحها
- 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).