أمثلة IM لسيناريوهات VPN مختلفة على ASA

المحتويات

المقدمة

مدير الحدث المضمن لبرنامج Cisco IOS® هو نظام فرعي فعال ومرن يوفر اكتشاف أحداث الشبكة في الوقت الفعلي والأتمتة المدمجة. يمنحك هذا المستند أمثلة على الأماكن التي يمكن أن يساعد فيها IM في سيناريوهات VPN مختلفة

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من ال ASA IM سمة.

المكونات المستخدمة

يعتمد هذا المستند على جهاز الأمان القابل للتكيف (ASA) من Cisco الذي يشغل الإصدار 9.2(1) من البرنامج أو إصدار أحدث.

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

تم إستدعاء "إدارة الأحداث المضمنة" في الأصل "background-debug" على ASA، وكانت ميزة تستخدم لتصحيح

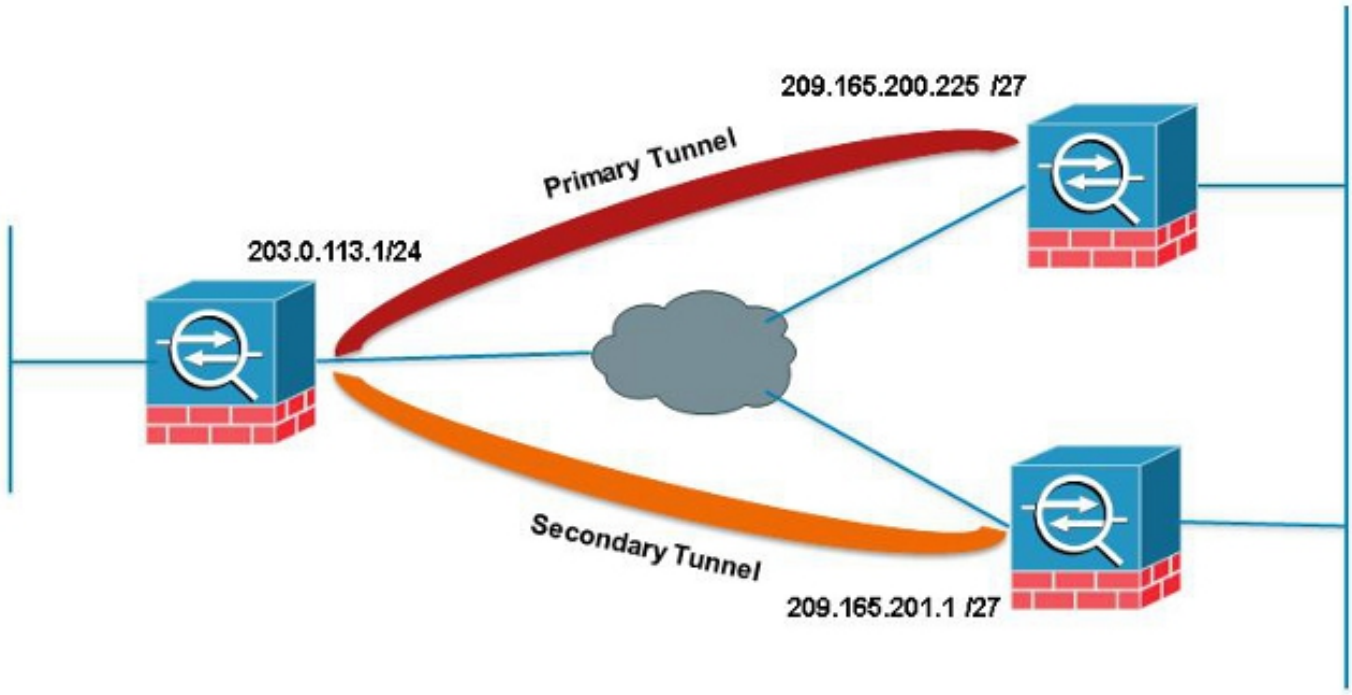
أخطاء مشكلة معينة. بعد المراجعة، تبين أنه مماثل بشكل كاف لبرنامج Cisco IOS Software IM، لذلك تم تحديثه لمطابقة واجهة سطر الأوامر (CLI) تلك.

تتيح لك ميزة EEM تصحيح المشاكل وتوفر تسجيل الأغراض العامة لاستكشاف الأخطاء وإصلاحها. فمعهد التدخل السريع يستجيب للاحداث في نظام التدخل السريع بالقيام بالاعمال. هناك نوعان من المكونات: الأحداث التي يتم تشغيلها من قبل مدير الحدث، والتطبيقات المتطورة لمدير الحدث التي تحدد الإجراءات. يمكنك إضافة أحداث متعددة إلى كل تطبيق لإدارة الأحداث يقوم بتشغيله لاستدعاء الإجراءات التي تم تكوينها عليه.

VPN PrePre

إذا قمت بتكوين شبكة VPN باستخدام عناوين IP نظيرة متعددة لإدخال تشفير، فسيتم إنشاء شبكة VPN باستخدام بروتوكول IP للنظير الاحتياطي بمجرد تعطل النظير الأساسي. ومع ذلك، بمجرد عودة النظير الأساسي، لا تستبق الشبكة الخاصة الظاهرية (VPN) عنوان IP الأساسي. أنت ينبغي يدويا محات ال SA موجود in order to restartup ال VPN مفاوضة أن يحول هو إلى العنوان أساسي.

```
ASA 1
crypto map outside_map 10 match address outside_cryptomap_20
crypto map outside_map 10 set peer 209.165.200.225 209.165.201.1
crypto map outside_map 10 set transform-set ESP-AES-256-SHA
crypto map outside_map interface outside
```



في هذا المثال، يتم إستخدام تجميع مستوى موقع IP (SLA) لمراقبة النفق الرئيسي. وفي حالة فشل هذا النظير، يتولى النظير الاحتياطي الأمر ولكن لا يزال إتفاقية مستوى الخدمة (SLA) تراقب الأساسي؛ وبمجرد ظهور الأساسي، سيقوم بروتوكول syslog الذي تم إنشاؤه بتشغيل IM لمسح النفق الثانوي مما يسمح ل ASA بإعادة التفاوض مع الأساسي مرة أخرى.

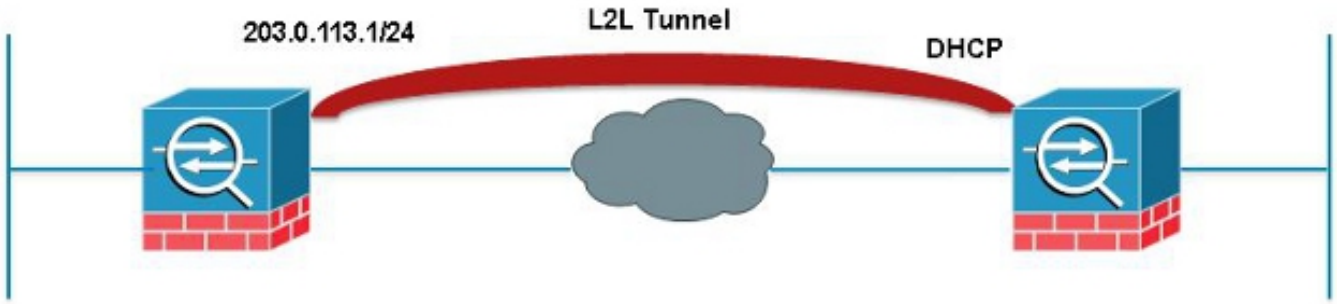
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
num-packets 3
frequency 10

sla monitor schedule 123 life forever start-time now
```

```
track 1 rtr 123 reachability

route outside 209.165.200.225 255.255.255.0 203.0.113.254 1 track 1

event manager applet PREEMPT
event syslog id 622001 occurs 2
"action 1 cli command "clear crypto ipsec sa peer 209.165.101.1
output none
```

L2L الديناميكية إلى الثابتة التي دائما ما تكون عالية

عند إنشاء نفق من شبكة LAN إلى شبكة LAN، يلزم معرفة عنوان IP لكل من نظاري IPSec. إذا لم يكن أحد عناوين IP معروفا لأنه ديناميكي، أي تم الحصول عليه عبر DHCP، فالبديل الوحيد هو إستخدام خريطة تشفير ديناميكية. يمكن بدء تشغيل النفق فقط من الجهاز باستخدام IP الديناميكي نظرا لأن النظير الآخر ليس لديه فكرة عن IP الجاري إستخدامه.

وهذه مشكلة في حال لم يكن هناك أحد خلف الجهاز الذي يحمل عنوان IP الديناميكي كي كي يصل إلى النفق عند نزوله، ومن ثم تكون هناك حاجة إلى وجود هذا النفق دائما في الأعلى. حتى إذا قمت بتعيين وضع الخمول-timeout إلى **لا شيء**، فإن هذا لن يعالج المشكلة لأن، على مفتاح، إذا لم يكن هناك حركة مرور يمر النفق سينخفض. وفي تلك اللحظة، فإن الطريقة الوحيدة لإظهار النفق مرة أخرى هي إرسال حركة مرور البيانات من الجهاز باستخدام IP الديناميكي. نفس الشيء ينطبق إذا كان النفق سينزل لسبب غير متوقع مثل DPDs، وهلم جرا.



سيقوم IM هذا بإرسال إختبار اتصال كل 60 ثانية عبر النفق مطابق ل SA المرغوب من أجل الحفاظ على الاتصال مرتفعا.

```
event manager applet VPN-Always-UP
event timer watchdog time 60
"action 1 cli command "ping inside 192.168.20.1
output none
```

قطع اتصال جميع إتصالات VPN الموجودة في وقت معين

لا يملك ال ASA طريقة أن يثبت قطع وقت صلب ل VPN جلسة. ولكن إذا فعلتم ذلك مع IM. يوضح هذا المثال كيفية الاتصال بكل من عملاء VPN وعملاء AnyConnect على الساعة 5:00 مساء

```
event manager applet VPN-Disconnect
event timer absolute time 17:00:00
"action 1 cli command "vpn-sessiondb logoff ra-ikev1-ipsec noconfirm
"action 2 cli command "vpn-sessiondb logoff anyconnect noconfirm
output none
```

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).