ASA 8.x: السماح بتشغيل تطبيق L2L VPN إنشاء نفق مع إعادة المستخدم

المحتويات

المقدمة

يقدم هذا المستند معلومات حول ميزة التدفقات النفقي المستمرة ل IPSec وكيفية الاحتفاظ بتدفق TCP عبر مقاطعة نفق VPN.

المتطلبات الأساسية

المتطلبات

يجب أن يكون لدى قراء هذا المستند فهم أساسي حول كيفية عمل الشبكة الخاصة الظاهرية (VPN). راجع هذه المستندات للحصول على مزيد من المعلومات:

- نموذج تكوين VPN L2L
- ASA مع L2L VPN

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco بالإصدار 8.2 والإصدارات الأحدث.

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

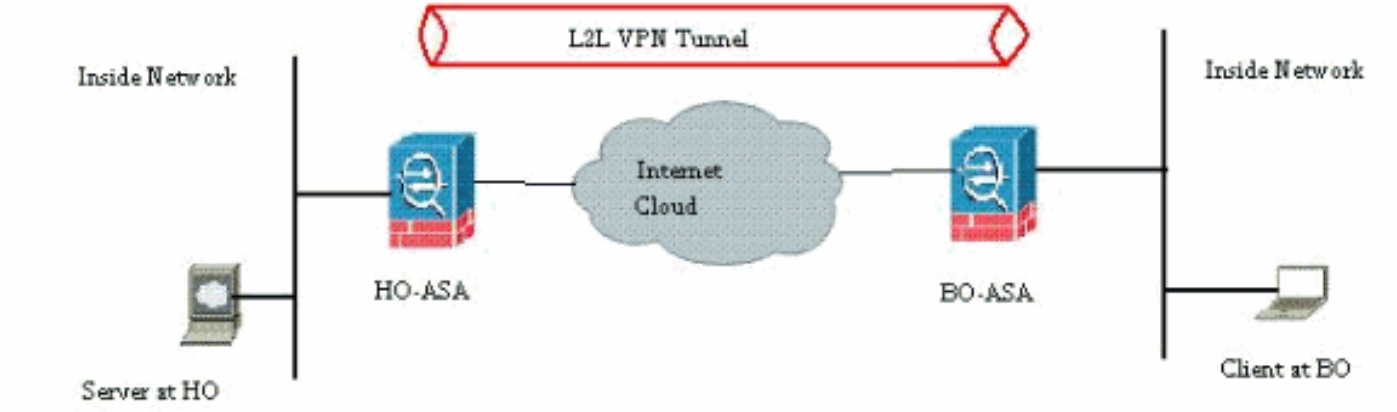
راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

كما هو موضح في الرسم التخطيطي للشبكة، يتم توصيل المكتب الفرعي (BO) بالمكتب الرئيسي (HO) من خلال شبكة VPN من موقع إلى موقع. ضع في الاعتبار أن أحد المستخدمين النهائيين في المكتب الفرعي يحاول تنزيل ملف كبير من الخادم الموجود في المكتب الرئيسي. تستغرق عملية التنزيل ساعات. يعمل نقل الملفات بشكل جيد حتى تعمل الشبكة الخاصة الظاهرية (VPN) بشكل صحيح. ومع ذلك، عند تعطيل شبكة VPN، يتم تعليق نقل الملفات ويتوجب على المستخدم إعادة بدء طلب نقل الملفات مرة أخرى من البداية بعد إنشاء النفق.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تنشأ هذه المشكلة بسبب الوظيفة المدمجة حول كيفية عمل ASA. يراقب ASA كل اتصال يمر عبره ويحافظ على إدخال في جدول حالته وفقا لميزة فحص التطبيق. يتم الاحتفاظ بتفاصيل حركة المرور المشفرة التي تمر عبر شبكة VPN في شكل قاعدة بيانات اقتران الأمان (SA). لسيناريو هذا المستند، يحتوي على تدفقين مختلفين لحركة مرور البيانات. الأولى هي حركة المرور المشفرة بين بوابات الشبكة الخاصة الظاهرية (VPN) والثانية هي تدفق حركة مرور البيانات بين الخادم في المكتب الرئيسي والمستخدم النهائي في المكتب الفرعي. عندما يتم إنهاء شبكة VPN، يتم حذف تفاصيل التدفق الخاصة ب SA هذا المعين. ومع ذلك، يصبح إدخال جدول الحالة الذي يتم الاحتفاظ به من قبل ASA لاتصال TCP هذا جامدا بسبب عدم وجود نشاط، مما يعيق التنزيل. وهذا يعني أن ASA سيظل يحتفظ باتصال TCP لذلك التدفق المعين أثناء إنهاء تطبيق المستخدم. ومع ذلك، ستصبح إتصالات TCP شاردة وفي نهاية المطاف المهلة بعد انتهاء صلاحية المؤقت الخامل ل TCP.

تم حل هذه المشكلة من خلال إدخال ميزة تسمى التدفقات النفقي المستمرة ل IPSec. تم دمج أمر جديد في Cisco ASA للاحتفاظ بمعلومات جدول الحالة في إعادة التفاوض على نفق VPN. الأمر موضح هنا:

```
sysopt connection preserve-vpn-flows
```

بشكل افتراضي، يتم تعطيل هذا الأمر. من خلال تمكين هذا، سيقوم Cisco ASA بالاحتفاظ بمعلومات جدول حالة

TCP عند إسترداد L2L VPN من التعطيل وإعادة إنشاء النفق.

في هذا السيناريو، يجب تمكين هذا الأمر على كلا طرفي النفق. إذا كان جهازا بخلاف Cisco في الطرف الآخر، فيجب أن يكون تمكين هذا الأمر على Cisco ASA كافيا. إذا تم تمكين الأمر عندما تكون الأنفاق نشطة بالفعل، فيجب مسح الأنفاق وإعادة إنشائها لكي يدخل هذا الأمر حيز التنفيذ. لمزيد من التفاصيل حول إزالة الأنفاق وإعادة إنشائها، ارجع إلى مسح الجهات الأمنية.

تفاصيل التوافق لهذه الميزة

تم إدخال هذه الميزة في برنامج Cisco ASA الإصدار 8.0.4 والإصدارات الأحدث. هذا مدعوم فقط ل هذا نوع ال VPN:

- أنفاق LAN إلى LAN
- أنفاق الوصول عن بعد في وضع امتداد الشبكة (NEM)

لا يساند هذا سمة ل هذا نوع من VPN:

- أنفاق الوصول عن بعد ل IPSec في وضع العميل
- أنفاق AnyConnect أو SSL VPN

هذه الميزة غير موجودة على الأنظمة الأساسية التالية:

- Cisco PIX مع برنامج الإصدار 6.0
- مركزات VPN من Cisco
- منصات IOS® من Cisco

لا يؤدي تمكين هذه الميزة إلى إنشاء أي حمل زائد إضافي على معالجة وحدة المعالجة المركزية الداخلية ل ASA لأنها ستحتفظ بنفس إتصالات TCP التي لدى الجهاز عند تشغيل النفق.

ملاحظة: ينطبق هذا الأمر على إتصالات TCP فقط. ليس له أي تأثير على حركة مرور UDP. سيتم تعطيل إتصالات UDP وفقا لفترة المهلة التي تم تكوينها.

التكوينات

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

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

يستعمل هذا وثيقة هذا تشكيل:

- Cisco ASA

هذا نموذج لمخرجات التكوين الجاري تشغيلها من جدار حماية Cisco ASA في أحد طرفي نفق VPN:

Cisco ASA

```
(ASA Version 8.2(1
!
hostname CiscoASA
domain-name example.com
<enable password <removed
<passwd <removed
names
!
```

```
                                        interface Ethernet0/0
                                                speed 100
                                              duplex full
                                            nameif outside
                                         security-level 0
                        ip address 209.165.201.2 255.255.255.248
                                                !
                                        interface Ethernet0/1
                                               nameif inside
                                          security-level 100
                             ip address 10.224.9.5 255.255.255.0
                                                !
                                        interface Ethernet0/2
                                                shutdown
                                              no nameif
                                        no security-level
                                            no ip address
                                                !
                                                !
                                    interface Management0/0
                                         nameif management
                                       security-level 100
                          ip address 10.224.14.10 255.255.255.0
                                                !
                                 boot system disk0:/asa822-k8.bin
                                              ftp mode passive
     Output Suppressed ! access-list test extended---!
  permit ip 10.224.228.0 255.255.255.128 any access-list
 test extended permit ip 10.224.52.0 255.255.255.128 any
         access-list 100 extended permit ip 10.224.228.0
  255.255.255.128 any access-list 100 extended permit ip
             10.224.52.0 255.255.255.128 any access-list
   inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
 10.224.10.0 255.255.255.0 ! !---Output Suppressed route
    inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
   0.0.0.0 255.255.255.255 209.165.201.1 1 timeout xlate
    3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
  h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
       0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
     uauth 0:05:00 absolute timeout tcp-proxy-reassembly
 0:01:00 dynamic-access-policy-record DfltAccessPolicy !
  !---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
   inside ! snmp-server enable traps snmp authentication
 linkup linkdown coldstart ! !--- To preserve and resume
 stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
 the timeout period after the tunnel drops and recovers.
                          sysopt connection preserve-vpn-flows
                                        service resetoutside
                                                !
  crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256
                                              esp-md5-hmac
crypto ipsec transform-set testSET esp-3des esp-md5-hmac
                             crypto map map1 5 match address 100
                       crypto map map1 5 set peer 209.165.200.10
                    crypto map map1 5 set transform-set testSET
                           crypto map map1 interface outside
                                crypto isakmp enable outside
                                       crypto isakmp policy 5
                                     authentication pre-share
```

```
                                                encryption 3des
                                                       hash sha
                                                      group 2
                                                    lifetime 86400
                                               crypto isakmp policy 10
                                              authentication pre-share
                                                    encryption des
                                                       hash sha
                                                      group 2
                                                    lifetime 86400
  Output Suppressed ! telnet timeout 5 ssh timeout 5---!
 console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! !---Output Suppressed
    ! tunnel-group 209.165.200.10 type ipsec-l2l tunnel-
  group 209.165.200.10 ipsec-attributes pre-shared-key *
!---Output Suppressed class-map inspection_default match
default-inspection-traffic ! policy-map type inspect dns
    preset_dns_map parameters message-length maximum 512
       policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
 inspect h323 ras inspect rsh inspect rtsp inspect esmtp
    inspect sqlnet inspect skinny inspect sunrpc inspect
        xdmcp inspect sip inspect netbios inspect tftp !
     service-policy global_policy global prompt hostname
 state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
                                                        end
```

تمكين هذه الميزة

افتراضيا، أعجزت هذا سمة. يمكن تمكين هذا الأمر باستخدام هذا الأمر في CLI من ASA:

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

ويمكن عرض ذلك باستخدام هذا الأمر:

```
CiscoASA(config)#show run all sysopt
       no sysopt connection timewait
       sysopt connection tcpmss 1380
  sysopt connection tcpmss minimum 0
       sysopt connection permit-vpn
    sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows
       no sysopt nodnsalias inbound
      no sysopt nodnsalias outbound
   no sysopt radius ignore-secret
      no sysopt noproxyarp outside
```

عند إستخدام ASDM، يمكن تمكين هذه الميزة من خلال اتباع هذا المسار:

التكوين > Remote Access VPN للوصول عن بعد > الوصول إلى الشبكة (العميل) > متقدم > IPsec > خيارات النظام.

بعد ذلك، تحقق من *خيار الاحتفاظ بتدفقات شبكة VPN ذات الحالة عند إسقاط النفق لوضع امتداد الشبكة (NEM).*

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show asp table vpn-context detail**— يعرض محتويات سياق VPN الخاصة بمسار الأمان السريع، والذي قد يساعدك على أستكشاف مشكلة وإصلاحها. فيما يلي عينة إخراج من الأمر **show asp table vpn-context** عند تمكين ميزة التدفقات النفقي الثابتة ل IPSec. لاحظ أنه يحتوي على علامة **KEEP** معينة.

```
CiscoASA(config)#show asp table vpn-context
,VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000
                                                                                gc=0
,VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000
                                                                                gc=0
```

استكشاف الأخطاء وإصلاحها

في هذا القسم، يتم تقديم حلول بديلة معينة لتجنب رفرفة الأنفاق. كما يتم توضيح ميزات وإيجابيات الحلول البديلة.

تعيين قيمة العمر الافتراضي ل IKE إلى صفر

يمكنك جعل نفق VPN يبقى حيا لوقت غير محدود، ولكن ليس لإعادة التفاوض، من خلال الحفاظ على قيمة فترة بقاء IKE كقيمة صفرية. يتم الاحتفاظ بالمعلومات المتعلقة ب SA بواسطة نظراء شبكة VPN حتى تنتهي صلاحية العمر. بتعيين قيمة كصفر، يمكنك جعل جلسة IKE هذه تدوم إلى الأبد. ومن خلال ذلك، يمكنك تجنب مشاكل فصل التدفق المتقطع أثناء إعادة تغطية النفق. يمكن القيام بذلك باستخدام هذا الأمر:

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

ومع ذلك، فإن هذا الأمر ينطوي على ميزة خاصة من حيث التضحية بمستوى الأمان الخاص بنفق الشبكة الخاصة الظاهرية (VPN). وتوفر إعادة صياغة جلسة عمل IKE في غضون فواصل زمنية محددة المزيد من الأمان لنفق VPN من حيث مفاتيح التشفير المعدلة في كل مرة، ويصبح من الصعب على أي متطفل فك ترميز المعلومات.

ملاحظة: لا يعني تعطيل عمر IKE أن النفق لا يعيد المفتاح على الإطلاق. ومع ذلك، سيقوم IPSec sa بإعادة المفتاح في الفترة الزمنية المحددة لأنه لا يمكن تعيين ذلك على صفر. الحد الأدنى لقيمة فترة البقاء المسموح بها ل IPSec SA هو 120 ثانية والحد الأقصى هو 214783647 ثانية. لمزيد من المعلومات حول هذا الأمر، ارجع إلى مدة بقاء IPSec SA.

رسالة خطأ عند إسقاط النفق

عندما لا يستعمل هذا سمة في التشكيل، ال cisco ASA يرجع هذا سجل رسالة عندما ال VPN أعجزت نفق:

```
53947  0:00:36  1135/10.0.0.100:  XX.XX.XX.XX/80: 57983     TCP     :ASA-6-302014
```

ويمكنكم ان تروا ان السبب هو ان **النفق قد دمر**.

ملاحظة: يجب تمكين تسجيل المستوى 6 للاطلاع على هذه الرسالة.

كيف تختلف هذه الميزة مع خيار إعادة تصنيف-VPN

يتم إستخدام خيار save-vpn-flow عند إرتداد نفق. وهذا يسمح بتدفق TCP السابق بالبقاء مفتوحا حتى عندما يعود النفق إلى الارتفاع، يمكن إستخدام التدفق نفسه.

عند إستخدام الأمر **sysopt connection reclassification-vpn**، فإنه يمسح أي تدفق سابق يتعلق بحركة المرور النفقي ويصنف التدفق الذي ينتقل عبر النفق. يتم إستخدام خيار إعادة تصنيف-VPN في حالة كان فيها تدفق TCP قد تم إنشاؤه بالفعل ولم يكن مرتبطا بشبكة VPN. هذا يخلق حالة حيث لا حركة مرور يتدفق عبر النفق بعد أن خلقت VPN. للحصول على مزيد من المعلومات حول هذا الأمر، ارجع إلى إعادة تصنيف-VPN ل sysopt.

معلومات ذات صلة

- موقع إلى موقع (L2L VPN) مع ASA
- صفحة وثائق Cisco ASA
- 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).