VPN ةئزجت :IOS و PIX/ASA 7.x

المحتويات

المقدمة

يأخذك هذا المستند خلال الخطوات المطلوبة لتخفيف المشاكل التي يمكن أن تحدث مع تجزئة حزمة. مثال على مشكل التجزئة هو القدرة على إختبار اتصال مرور شبكة ولكن عدم القدرة على الاتصال بذلك المرور نفسه باستخدام تطبيق معين، مثل البريد الإلكتروني أو قواعد البيانات.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- اتصال بين أقران شبكات VPN

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع إصدارات الأجهزة والبرامج التالية:

- موجهات IOS
- أجهزة أمان PIX/ASA

الاصطلاحات

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

معلومات أساسية

يعدم IP الوط أقصى يبلغ 65536 بايت لحزمة IP، ولكن معظم بروتوكولات طبقة إرتباط البيانات تدعم الوط أصغر بكثير، يطلق عليه وحدة الإرسال القصوى (MTU). استنادا إلى وحدة الحد الأقصى للنقل (MTU) المدعومة، قد يكون من الضروري تفكيك (تجزئة) حزم IP يجب على الوجهة بعد ذلك إعادة تجميع ومع بعض تطبيقات نوع طبقة إرتباط البيانات. لنقلها عبر نوع معين. الأجزاء مرة أخرى إلى حزمة IP الأصلية الكاملة.

عندما تستخدم شبكة خاصة ظاهرية (VPN) لحماية البيانات بين شبكتين خاصة نظائر ظاهرية (VPN)، يتم إضافة مصروفات إضافية إلى البيانات الأصلية، والتي يمكن أن تتطلب حدوث التجزئة. يسرد هذا الجدول الحقول التي من المحتمل أن تتم إضافتها إلى البيانات المحمية لدعم اتصال VPN. لاحظ أنه يمكن أن تكون هناك بروتوكولات متعددة ضرورية، مما يزيد من حجم الحزمة الأصلية. على سبيل المثال، إذا كنت تستخدم اتصال L2L DMVPN IPsec بين موجهات Cisco، حيث تقوم بتنفيذ نفق GRE، فأنت بحاجة إلى هذه النفقات الإضافية: ESP و GRE و رأس IP الخارجي. إن كنت تتلقى IPSec برمجية زبون إضافي إلى VPN لخدم عندما حركة مرور يمر من خلال عنوان أداة، أنت تحتاج هذا إضافي فيصول ل شبكة عنوان ترجمة- Traversal (NAT-T)، as well as الخارجية ip رأس ل النفق أسلوب وصيل.

قضايا تتعلق بالتجزئة

عندما يرسل المصدر ربط إلى غاية، هو يضع قيمة في التحكم راية مجال من ال ip عنوان أن يؤثر على تجزئة الربط بالأجهزة الوسيطة. طول العلامة التحكم ثالث وحدات بت، ولكن يتم إستخدام الاثنتين الأوليين فقط في التجزئة. إذا تم تعيين بت الثاني على 0، يتم السماح للحزمة بأن تكون مجزأة؛ إذا تم تعيينها على 1، لا يتم السماح للحزمة بأن تكون أجزاء. وتستخدم وحدة بت الثانية عادة بتجزئة عدم التجزئة (DF). تحدد وحدة بت ثالثة وقت حدوث التجزئة، وما إذا كانت هذه الحزمة المجزأة هي الجزء الأخير (تم تعيينها على 0) أو إذا كان هناك المزيد من الأجزاء (تم تعيينها على 1) التي تشكل الحزمة.

هناك أربعة مناطق يمكن أن تخلق مشاكل عندما يكون التجزئة مطلوبا:

- الذاكرة ووحدة المعالجة المركزية (CPU) دورات في إضافية مصروفات رفوت مزلي

بواسطة الجهازين اللذين يجريان التجزئة وإعادة التجميع.

- إذا تم إسقاط جزء واحد في الطريق إلى الوجهة، لا يمكن إعادة تجميع الحزمة ويجب تجزئة الحزمة بالكامل وإرسالها مرة أخرى. وهذا يخلق مشاكل لإنتاجية إضافية، خاصة في الحالات التي تكون فيها حركة المرور المعنية محدودة المعدل، ويرسل المصدر حركة مرور البيانات أعلى من الحد المسموح به.

- قد تواجه تصفية الحزم وجدران الحماية المعبرة عن الحالة صعوبة في معالجة الأجزاء. عند حدوث التجزئة، يحتوي الجزء الأول على رأس IP خارجي والرأس الداخلي، مثل TCP و UDP و ESP وغيرها، وجزء من الحمولة. الأجزاء التالية من عقد الحزمة الأصلي ورأس IP الخارجي ومتابعة الحمولة. المشكلة مع هذه العملية هي أن بعض جدران الحماية تحتاج إلى رؤية معلومات الرأس الداخلية في كل حزمة لاتخاذ قرارات تصفية ذكية؛ إذا كانت هذه المعلومات مفقودة، فيمكنها دون قصد إسقاط جميع الأجزاء، باستثناء الجزء الأول.

- يمكن أن يثبت المصدر في رأس IP الخاص بالحزمة بت التحكم الثالث على عدم تجزئة، وهو ما يعني أنه، إذا كان الجهاز الوسيط يستلم الحزمة ويجب أن يجزئها، فإن الجهاز الوسيط لا يمكنه تجزئتها. بدلا من ذلك، يسقط الجهاز الوسيط الحزمة.

المهمة الرئيسية

اكتشاف التجزئة

تستخدم معظم الشبكات شبكة الإيثرنت، ذات قيمة MTU افتراضية تبلغ 1500 بايت، والتي يتم استخدامها عادة لحزم IP. معرفة ما إذا كان التجزئة يحدث أو يحتاج إليه ولكن لا يمكن تنفيذه (تم تعيين بت DF)، قم أولا بإحضار سلسلة عمل VPN الخاصة بكل أعلى. ثم يمكنك استخدام أي من هذه الإجراءات الأربعة لاكتشاف التجزئة.

1. يؤز جهاز موجود في الطرف الآخر. هذا تحت افتراض أن الرنين مسموح به عبر النفق. في حالة نجاح هذا الإجراء، حاول الوصول إلى تطبيق عبر نفس الجهاز؛ على سبيل المثال، إذا كان أحد خوادم Microsoft للبريد الإلكتروني أو سطح المكتب البعيد عبر النفق، فافتح Outlook وحاول تنزيل البريد الإلكتروني الخاص بك، أو حاول تنزيل "سطح المكتب البعيد" إلى الخادم. إذا لم ينجح ذلك، ولديك دقة المسار الصحيحة، فهناك فرصة جيدة أن تكون التجزئة هي المشكلة.

2. من جهاز Windows استخدم هذا: C:\> ping -f -l packet_size_in_bytes destination_ip_address.

   يتم استخدام الخيار -f لتحديد عدم إمكانية تجزئة الحزمة. يتم استخدام الخيار -l لتحديد طول الحزمة. حاول أولا مع حجم حزمة 1،500. على سبيل المثال، ping -f -l 1500 192.168.100. إذا كان التجزئة مطلوبا ولكن لا يمكن تنفيذه، فأنت تتلقى رسالة مثل هذا: تحتاج الحزم إلى أن تكون مجزأة ولكن مجموعة DF.

3. إذا رأيت على موجهات Cisco، قم بتنفيذ الأمر debug ip icmp واستخدم الأمر extended ping. تجزئة ICMP:dst (x.x.x.x) مطلوبة ومجموعة DF، يتعذر الوصول إليها مرسلة إلى y.y.y، حيث x.x.x.x هو جهاز وجهة، و y.y.y هو الموجه الخاص بك، يخبرك جهاز وسيط أن التجزئة مطلوبة، ولكنك لأنك قمت بتعيين بت DF في طلب الصدى، فإن الجهاز الوسيط لا يمكنه تجزئته لإعادة توجيهه إلى الخطوة التالية. في هذه الحالة، قم بتخفيض حجم وحدة الحد الأقصى للنقل (MTU) تدريجيا من إختبارات الاتصال حتى تجد واحدة تعمل.

في أجهزة أمان Cisco، أستخدم عامل تصفية الالتقاط.4.

- CiscoAsa(config)#`access-list outside_test يسمح أي مضيف 172.22.1.1 eq 80`

  ملاحظة: عندما تترك المصدر بأي، فإنه يسمح للمستخدمين بمراقبة أي ترجمات عنوان الشبكة (NAT).

- CiscoASA(config)#`access-list outside_test permit tcp مضيف 172.22.1.1 eq 80 any`

  ملاحظة: عند عكس معلومات المصدر والوجهة، فإنها تسمح بالتقاط حركة المرور العائدة.

- `CiscoASA(config)# capture outside_interface access-list خارج_test interface خارج`

  أدبي أن دعب .X قيبطتلا عم ةديدج لمع ةسلج ءدب ىلإ مدختسملا جاتحي المستخدم جلسة عمل تطبيق X جديدة، يحتاج مؤشر ASA إلى إصدار الأمر show capture outside_interface.

حلول المشكلات التأطير

هذه شقانتو .ةئزجتلاب ةقلعتملا لكاشملا لح اهلالخ نم كنكمي ةفلتخم قرط كانه عرفلا اذه يف لئاسملا.

الطريقة 1: إعداد MTU الثابت

يمكن أن يوقع إعداد MTU الثابت بحل مشكلات التجزئة.

تغيير MTU على الموجه:1.

لاحظ أنه إذا قمت بضبط وحدة الحد الأقصى للنقل (MTU) يدويا على الجهاز، فإنها توقت أن قبل ةملتسملا مزحلا ةئزجتب ،VPN ةكبش ةباوبك لمعي يذلا الجهاز، تعمل موقع مث رورملا ةكرح يمحي هجوملا نوكي نأ لضفي .قفنلا ربع اهلاسرإو مزحلا ةيامحب الجهاز يقطعها، ولكن تتجزئها.

تحذير: إذا قمت بتغيير حجم وحدة الحد الأقصى للنقل (MTU) على أي جهاز واجهة، فإنه يتسبب في تدمير جميع الأنفاق التي تم إنشاؤها على تلك الواجهة وإعادة بنائها.

على موجهات Cisco، أستخدم الأمر ip لضبط حجم MTU على الواجهة التي يتم فيها إنهاء شبكة VPN:

<#root>

```
router (config)#
interface type [slot_#/] port_#

router (config-if)#
ip mtu MTU_size_in_bytes
```

2:تغيير MTU على ASA/PIX.

على أجهزة ASA/PIX، أستخدم الأمر مجم طبض MTU في وضع التكوين العام. وبشكل افتراضي، يتم تعيين وحدة الحد الأقصى للنقل (MTU) على 1500. على سبيل المثال، إذا كان لديك واجهة على جهاز الأمان الخاص بك تم تسميتها خارجي (حيث يتم إنهاء شبكة VPN)، وقد قمت بتحديد (من خلال المقاييس المدرجة في قسم اكتشاف التجزئة) أنك تريد إستخدام 1380 كحجم الجزء، فاستخدم هذا الأمر:

```
<#root>
security appliance (config)#
mtu Outside 1380
```

الطريقة 2: الحد الأقصى لحجم مقطع TCP

يمكن أن يقوم الحد الأقصى لحجم مقطع TCP بحل المشاكل المتعلقة بالتجزئة.

ملاحظة: تعمل هذه الميزة فقط مع بروتوكول TCP، ويتعين على بروتوكولات IP الأخرى إستخدام حل آخر لحل مشاكل تجزئة IP. حتى إذا قمت بضبط وحدة الحد الأقصى للنقل (MTU) الخاصة ببروتوكول IP على الموجه، فإنه لا يؤثر على ما يفاوض به المضيفان النهائيان داخل مصافحة TCP الثلاثية مع TCP MSS.

1:تغيير MSS على الموجه.

تحدث التجزئة مع حركة مرور TCP لأن حركة مرور TCP يتم إستخدامها عادة لنقل كميات كبيرة من البيانات. يدعم TCP ميزة تسمى TCP الحد الأقصى لحجم المقطع (MSS) التي تسمح لكلا الجهازين بالتفاوض حول حجم مناسب لحركة مرور TCP. يتم تكوين قيمة MSS بشكل ثابت على كل جهاز وتمثل حجم المخزن المؤقت لاستخدامه للحزمة المتوقعة. عندما يقوم جهازان بإنشاء إتصالات TCP، فإنهما يقارنان قيمة MSS المحلية مع قيمة MTU المحلية ضمن المصافحة ثلاثية الإتجاه، وأيا كان الأقل يتم إرساله إلى النظير البعيد. ثم يستعمل الرفيقان أدنى القيمتين المتبادلتين. لتكوين هذه الميزة، قم بما يلي:

على موجهات Cisco، أستخدم الأمر tcp adjust-mss على الواجهة التي يتم إنهاء VPN عليها.

```
<#root>
router (config)#
interface type [slot_#/] port_#
router (config-if)#
ip tcp adjust-mss MSS_Size_in_bytes
```

تغيير MSS على ASA/PIX:2.

لضمان أن الحد الأقصى لحجم مقطع TCP الذي تتجاوز القيمة التي قمت بتعيينها أو تأكيد الحد الأقصى ليس أقل من حجم محدد، أستخدم الأمر sysopt connection في وضع التكوين العام. استرجاع الإعداد الافتراضي، أستخدم نموذج ثالث الشكل من هذا الأمر. القيمة القصوى الافتراضية هي 1380 بايت. يتم تعطيل الميزة الدنيا بشكل افتراضي (يتم تعيينها على 0).

لتغيير الحد الأقصى الافتراضي لـ MSS، قم بما يلي:

```
<#root>

security appliance (config)#

sysopt connection tcp-mss MSS_size_in_bytes
```

ملاحظة: إذا قمت بضبط الحجم الأقصى ليكون أكبر من 1380، يمكن أن تصبح الحزم مجزأة، تعتمد على حجم MTU (والذي هو 1500 بشكل افتراضي). يمكن أن تؤثر أعداد كبيرة من الأجزاء على أداء جدار الأمان عند إستخدامه لميزة "حماية الإطارات". إذا قمت بضبط الحد الأدنى للحجم، فإنه يمنع خادم TCP من إرسال العديد من حزم بيانات TCP الصغيرة إلى العميل ويؤثر على أداء الخادم والشبكة.

لتغيير الحد الأدنى لـ MSS، قم بما يلي:

```
security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes
```

جدار الأمان (config)# sysopt tcp-mss minimum MSS_size_in_bytes

ملاحظة: ارجع إلى تكوين MPF للسماح بالحزم التي تتجاوز MSS قسم من المستند إلى إصدار PIX/ASA 7.x: MSS التي تم تجاوزها - يتعذر على عملاء HTTP الاستعراض إلى بعض مواقع الويب للحصول على مزيد من المعلومات للسماح لحزم MSS التي تم تجاوزها بطريقة أخرى.

الطريقة 3: اكتشاف مسار وحدة الحد الأقصى للنقل (MTU) (PMTUD)

يمكن أن يقوم PMTUD بحل مشكلات التجزئة.

المشكلة الرئيسية مع TCP MSS هي أن المسؤول يجب أن يعرف القيمة التي سيتم تكوينها على الموجه لمنع حدوث التجزئة. قد يمثل هذه المشكلة إذا كان هناك أكثر من مسار واحد بين موقع شبكة VPN البعيدة، أو عندما تقوم بتنفيذ الاستعلام الأولي الخاص بك، فستجد أن وحدة الحد الأقصى للنقل (MTU) الأصغر من الثانية أو الثالثة، بدلا من الأصغر، تعتمد على قرار التوجيه المستخدم في الاستعلام الأولي. باستخدام PMTUD، يمكنك تحديد قيمة MTU لحزم IP التي تتجنب التجزئة. إذا تم حظر رسائل ICMP بواسطة موجه، فإن وحدة الحد الأقصى للنقل (MTU) للمسار تكون مكسورة، ويتم تجاهل الحزم ذات

نكمي .اهلاسرإو ةمزحلا ةئزجتب حامسلاو DF تب حسمل set ip df رمألا مدختسأ .DF تب ةعومجم مئاوق مادختسإ نكمي نكل ،ةكبشلا ىلع ةمزحلا هيجوت ةداعإ ةعرس ةئزجتلا ئطبي نأ .هيلع DF تب حسم متي يتلا مزحلا ددع نم دحلل لوصولا

.1:PMTUD لمع مدع يف تالكشم ثالث ببستت دق

- ةلاسر مادختساب ةباجتسالا مدعو ةمزحلا طاقسإب طيسولا هجوملا موقي نأ نكمي ةكبش لخاد اعئاش نوكي نأ نكمي هنكلو ،تنرتنإلا ىلع ادج عئاش ريغ اذهو .ICMP رذعتي يذلا ICMP لئاسر مادختساب ةباجتسالا مدعل تاهجوملا نيوكت مت ثيح .هيلإ لوصولا
- ،هيلإ لوصولا رذعتي يذلا ICMP ةلاسرب طيسولا هجوملا بيجتسي نأ نكمي نكلو ،ةلاسرلا هذه رظحب ةيامحلا رادج موقي ،عاجرإلا قفدت يف .رثكأ ثودح اذهو .اعويش
- تشق ةلاسر ICMP يذلا رذعتي لوصولا هيلإ طيرقاه ةرم ىرخأ ىلإ ،ردصملا نكلو ردصملا يتجاهل ةلاسر ةئزجتلا .ةذهو يه رثكأ اياضقلا ثالثلا .اعويش

اذإ اهتجاو رادصإلا ،لوألا يمكنك امإ حسم تب DF يف سأر IP يذلاو هعضو ردصملا ناكوأ طبض مجح TCP MSS .اديودي حسمل تب DF، بجي نأ ريغي هجوملا طيسولا ةميقلا نم 1 ىلإ .0 ةداع ام متي ةميقلا مايقلا كلذب ةطساوب هجوم يف كتكبش لبق نأ رداغت ةمزحلا :IOS ىلإ دنتسي هجوم ىلع كلذب موقي طيسب زمر نيوكت اذه .ةكبشلا

<#root>

```
Router (config) #

access-list ACL_# permit tcp any any

Router (config) #

route-map route_map_name permit seq#

Router (config-route-map) #

match ip address ACL_#

Router (config-route-map) #

set ip df 0

Router (config-route-map) #

exit

Router (config) #

interface type [slot#/]port #

Router (config-if) #

ip policy router-map route_map_name
```

.2GRE و PMTUD قافنأ

- ويتم تنفيذ PMTUD على حزم GRE التي تمر عبر الموجه، ولكنها غير مفعلة بشكل افتراضي. لتمكين PMTUD على حزم GRE، استخدم الأمر tunnel path-mtu-discovery على الموجهات التي تعمل كنقاط نهاية لنفق GRE. بما أن المضيف ينتج حزمة بحجم كبير جدًا ولم يتم تعيين بت DF، فإن تجزئة الحزمة ستتم، ومن ثم، الموجه لا يمكنه أن يتم إرسالها عبر النفق بسبب وجود بت DF:
  - الموجه (config) # `interface tunnel_#`
  - الموجه (config-if) # `tunnel path-mtu-discovery`

  الخاصة GRE نفق PMTUD tunnel path-mtu-discovery الأمر حيث يتيح الموجه يتم تحديد الحد الأقصى لحجم MTU الذي تم اكتشافه، وعدد الدقائق التي يستمر فيها وقت Age-Timer الاختيارية المعلمة بعدها إعادة تعيين الحد الأقصى لحجم MTU وإعادة تحديدها. إذا لم تقم بتحديد المعلمة، فلن يتم تعيين القيمة. تتم إضافة 24 بايت إضافية للحزمة GRE. يتم تحديد الحد الأدنى لعدد وحدات البايت التي يحتوي عليها قيمة MTU. تحدد المعلمة min-mtu الحد الأدنى لعدد وحدات البايت التي يحتوي عليها قيمة MTU.

3.مشكلة الحزم الكبيرة أو المعالجة الخاطئة للتجزئة أو الجسر (DF) عدم تجزئة - PIX/ASA 7.x

أو الكبيرة الحزم أو المعالجة قادر على الوصول إلى الإنترنت بشكل صحيح، ما لم تكن غير قادرة على الوصول بشكل صحيح إلى الإنترنت أو المعالجة الكبيرة حجم MTU الخاص بالنفق لأن هذه الرسالة تعطي مؤشرًا حول حجم الخطأ:

<#root>

```
PMTU-D packet 1440 bytes greater than effective mtu 1434,
dest_addr=10.70.25.1, src_addr=10.10.97.55, prot=TCP
```

لحل هذه المشكلة، تأكد من مسح بت DF من الحزمة الخارجية للجهاز. قم بتكوين سياسة بت DF لحزم IPSec باستخدام الأمر crypto ipSec df-bit في وضع التكوين العام.

<#root>

```
pix(config)# crypto ipsec df-bit clear-df outside
```

تتيح كل ميزة بت DF باستخدام أنفاق IPSec تحديد ما إذا كان الجهاز الأمني يمكنه مسح أو ضبط أو نسخ بت DF من رأس IP المغلف. يحدد بت DF الموجود داخل رأس IP ما إذا كان يسمح للجهاز بتجزئة حزمة أو لا.

استخدم الأمر crypto ipSec df-bit في وضع التكوين العام لتكوين الجهاز الأمني لتحديد بت DF في رأس مغلف.

عند تضمين حركة مرور صيغة النفق IPSec، استخدم إعداد clear-df لبت DF. يتيح هذا الإعداد للجهاز إرسال حزم أكبر من حجم MTU المتاح. ويكون هذا الإعداد مناسبًا أيضًا إذا كنت لا تعرف حجم وحدة الحد الأقصى للنقل (MTU) المتوفر.

ملاحظة: إذا كنت لا تزال تواجه مشاكل التجزئة والحزم المسقطة، بشكل اختياري، يمكنك

ضبط حجم MTU يدويا باستخدام أمر واجهة ip mtu. في هذه الحالة، يقوم الموجه بتقسيم الحزمة إلى أجزاء قبل حمايتها. يمكن إستخدام هذا الأمر بالاشتراك مع PMTUD و/أو TCP MSS.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

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

استكشاف الأخطاء وإصلاحها

خطأ تشفير VPN

بافتراض أن نفق IPSec قد تم إنشاؤه بين الموجه و PIX. إذا رأيت رسائل خطأ التشفير التي يتم إسقاط الحزم، أكمل الخطوات التالية لحل المشكلة:

1. قم بإجراء تتبع sniffer من العميل إلى جانب الخادم لمعرفة أي من MTU الأفضل للاستخدام.

   يمكنك أيضا إستخدام إختبار الاتصال:

```
<#root>

ping  -l   1400  192.168.1.1 -f
```

   192.168.1.1 هو عنوان IP الخاص بالجهاز البعيد.

2. استمر في تقليل قيمة 1400 بمقدار 20 حتى يكون هناك در.

   لاحظ القيمة السحرية، والتي تعمل في معظم الحالات، هي 1300.

3. بعد تحقيق الحد الأقصى المناسب لحجم المقطع، قم بتعديله بشكل مناسب للأجهزة المستخدمة:

   على جدار حماية PIX:

```
<#root>

sysopt connection tcpmss 1300
```

   على الموجه:

<#root>

```
ip tcp adjust-mss 1300
```

مشكلات RDP و Citrix

المشكلة:

يمكنك إختبار الاتصال بين شبكات VPN، ولكن لا يمكن إنشاء بروتوكول سطح المكتب البعيد (RDP) واتصالات Citrix عبر النفق.

الحل:

يمكن أن تكون المشكلة هي حجم وحدة الحد الأقصى للنقل (MTU) على الكمبيوتر خلف PIX/ASA. قم بتعيين حجم وحدة الحد الأقصى للنقل (MTU) على 1300 لجهاز العميل لإنشاء اتصال Citrix عبر نفق VPN.

معلومات ذات صلة

- حل مشاكل تجزئة IP و MTU و MSS و PMTUD مع GRE و IPSec
- إصدار PIX/ASA 7.0: تجاوز MSS - يتعذر على عملاء HTTP الاستعراض إلى بعض مواقع الويب
- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPSec لوصول عن بعد و L2L الأكثر شيوعا
- لماذا لا أستطيع تصفح الإنترنت عند إستخدام نفق GRE
- 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).