PIX/ASA 7.x و IOS: ةئزجت VPN

المحتويات

المقدمة

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

المتطلبات الأساسية

المتطلبات

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

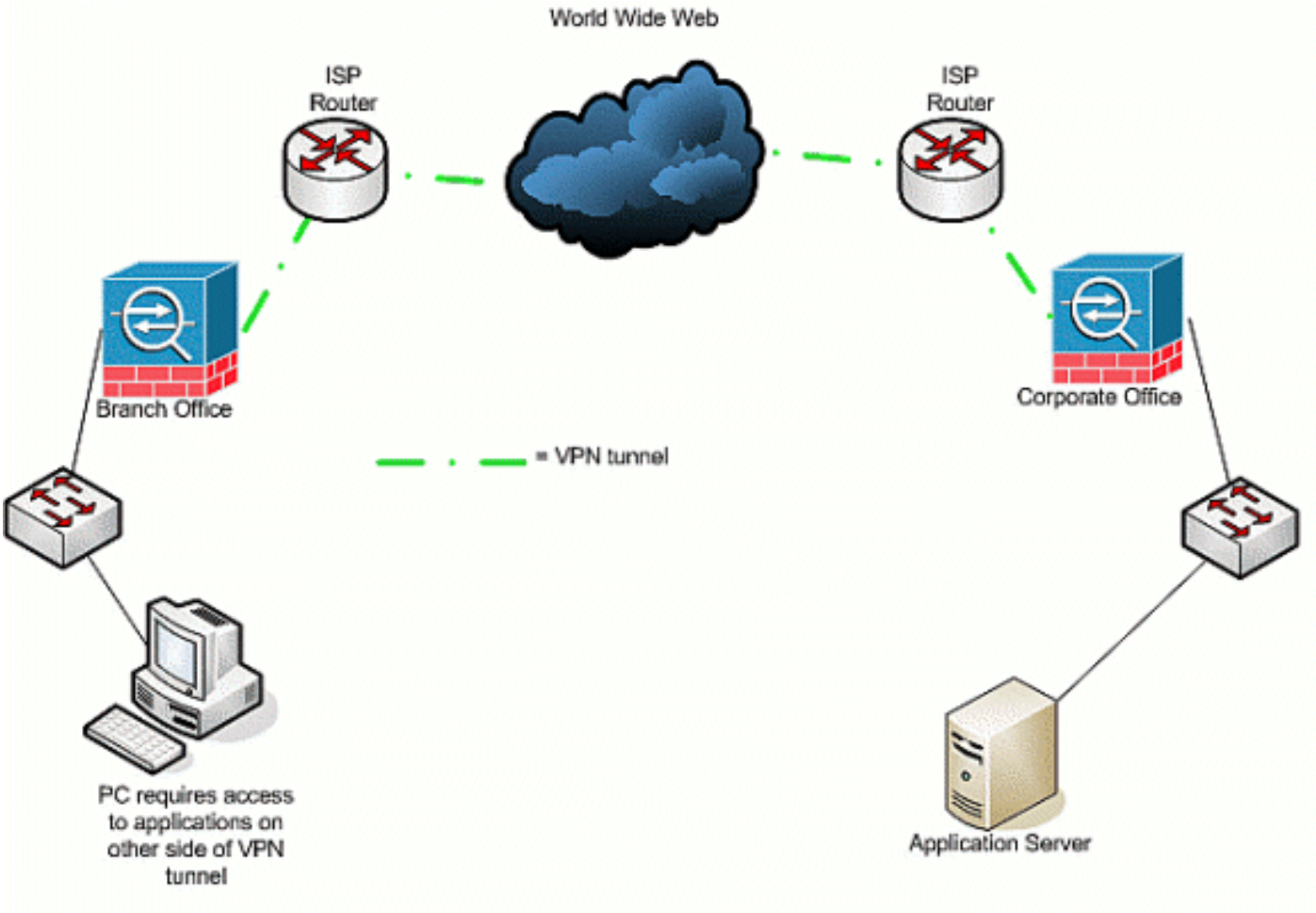
- الاتصال بين أقران شبكات VPN

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 اصطلاحات المستندات.

معلومات أساسية

يدعم IP طولا أقصى يبلغ 65536 بايت لحزمة IP، ولكن معظم بروتوكولات طبقة إرتباط البيانات تدعم طولا أصغر بكثير، ويطلق عليه وحدة الإرسال القصوى (MTU). استنادا إلى وحدة الحد الأقصى للنقل (MTU) المدعومة، قد يكون من الضروري تفكيك (تجزئة) حزمة IP لنقلها عبر نوع وسائط طبقة إرتباط بيانات معين. ويجب على الوجهة بعد ذلك إعادة تجميع الأجزاء مرة أخرى إلى حزمة IP الأصلية الكاملة.

Protocol	Additional Bytes
ESP (encryption and hash)	56
AH	24+
GRE	24
NAT-T/IPsec over UDP (UDP part)	8
IPsec over TCP (TCP part)	20
L2TP	12
PPTP	48
Outer IP header in IPsec tunnel mode or PPTP/L2TP	20
PPPoE	8

عندما تستخدم شبكة خاصة ظاهرية (VPN) لحماية البيانات بين نظائر شبكة خاصة 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 IPsec DMVPN L2L بين موجهات Cisco، حيث قمت بتنفيذ نفق GRE، فأنت بحاجة إلى هذه النفقات الإضافية: ESP و GRE و رأس IP الخارجي. إن يتلقى أنت IPSec برمجية زبون توصيل إلى VPN مدخل عندما حركة مرور يمر من خلال عنوان أداة، أنت تحتاج هذا إضافي مصاريف ل شبكة عنوان ترجمة- as well as ،Traversal (NAT-T) الخارجية ip رأس ل النفق أسلوب توصيل.

قضايا تتعلق بالتجزئة

عندما يرسل المصدر ربط إلى غاية، هو يضع قيمة في التحكم شعار مجال من ال ip عنوان أن يؤثر على تجزئة الربط بالأجهزة الوسيطة. طول علامة التحكم ثلاث 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 مجزأة. وتسمى 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:

- يلزم توفر مصروفات إضافية في دورات وحدة المعالجة المركزية (CPU) والذاكرة 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 إنتاجية 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 تجزئته*، وهو ما يعني أنه، إذا

كان الجهاز الوسيط يستلم الحزمة ويجب أن يتجزئها، 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 إستخدامها عادة لحزم IP. لمعرفة ما إذا كان التجزئة يحدث أو يحتاج إليه ولكن لا يمكن تنفيذه (تم تعيين بت DF)، قم أولا بإحضار جلسة عمل VPN الخاصة بك لأعلى. ثم يمكنك إستخدام أي من هذه الإجراءات الأربعة لاكتشاف التجزئة.

1. يوز 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 الاسم الصحيحة، هناك فرصة جيدة أن تكون التجزئة هي المشكلة.
2. من جهاز Windows أستخدم هذا: **ping -f -l packet_size_in_bytes destination_ip_address** <:\C.يتم إستخدام الخيار **-f** لتحديد عدم إمكانية تجزئة الحزمة. يتم إستخدام 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 هذه: *تحتاج الحزم إلى أن تكون مجزأة ولكن مجموعة DF.*
3. على موجهات Cisco، قم بتنفيذ الأمر **debug ip icmp** واستخدم الأمر **extended ping**. إذا رأيت *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، ولكن 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.
4. في أجهزة أمان Cisco، أستخدم عامل تصفية التقاط.`access-list outside_test` CiscoAsa(config)#`eq 80 172.22.1.1` **ملاحظة:** عندما تترك المصدر *بأي*، فإنه يسمح للمسؤول بمراقبة أي ترجمات لعنوان الشبكة (`access-list outside_test permit tcp` CiscoASA(config)#.NAT `eq 80 any 172.22.1.1` **ملاحظة:** عند عكس معلومات المصدر والوجهة، فإنها تسمح بالتقاط حركة المرور العائدة.`CiscoASA(config)# capture test interface_ outside_interface access-list` يحتاج المستخدم إلى بدء جلسة عمل جديدة باستخدام التطبيق X. بعد أن يقوم المستخدم ببدء جلسة عمل تطبيق X جديدة، يحتاج مسؤول ASA إلى إصدار الأمر **show capture outside_interface**.

حلول لمشكلات التأطير

هناك طرق مختلفة يمكنك من خلالها حل المشاكل المتعلقة بالتجزئة. وتناقش هذه المسائل في هذا الفرع.

الطريقة 1: إعداد MTU الثابت

يمكن أن يقوم إعداد MTU الثابت بحل مشكلات التجزئة.

1. **تغيير MTU على الموجه:**لاحظ أنه إذا قمت بضبط وحدة الحد الأقصى للنقل (MTU) يدويا على الجهاز، فإنها تعلم الجهاز، الذي يعمل كبوابة شبكة VPN، بتجزئة الحزم المستلمة قبل أن تقوم بحماية الحزم وإرسالها عبر النفق. يفضل أن يكون الموجه يحمي حركة المرور ثم يقوم بتجزئتها، ولكن الجهاز يقطعها.**تحذير:** إذا قمت بتغيير حجم وحدة الحد الأقصى للنقل (MTU) على أي واجهة جهاز، فإنه يتسبب في تدمير جميع الأنفاق التي تم إنهاؤها على تلك الواجهة وإعادة بنائها.على موجهات Cisco، أستخدم الأمر **ip** لضبط حجم MTU على الواجهة التي يتم فيها إنهاء شبكة VPN:

```
#_router (config)# interface type [slot_#/] port
router (config-if)# ip mtu MTU_size_in_bytes
```

تغيير MTU على ASA/PIX:على أجهزة ASA/PIX، أستخدم الأمر لضبط حجم MTU في وضع التكوين العام2. 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:

```
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:**يحدث 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.

```
#_router (config)# interface type [slot_#/] port
router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes
```

2. **تغيير MSS على ASA/PIX:**لضمان أن الحد الأقصى لحجم مقطع TCP لا يتجاوز القيمة التي قمت بتعيينها وأن الحد الأقصى ليس أقل من حجم محدد، أستخدم الأمر **sysopt connection** في وضع التكوين العام. لاسترجاع الإعداد الافتراضي، أستخدم نموذج **ثلاثي** الشكل من هذا الأمر. القيمة القصوى الافتراضية هي 1380 بايت. يتم تعطيل الميزة الدنيا بشكل افتراضي (يتم تعيينها على 0).لتغيير الحد الأقصى الافتراضي ل MSS، قم بما يلي:

```
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 جهاز 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 ل MSS، قم بما يلي:

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

جهاز الأمان (config)# `sysopt tcp-mss minimum MSS_size_in_bytes` **ملاحظة:** ارجع إلى تكوين MPF للسماح بالحزم التي تتجاوز MSS قسم من المستند PIX/ASA 7.x إصدار: 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 (PMTUD) (MTU)

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 هذا مشكلة إذا كان هناك أكثر من مسار واحد بينك وبين 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 مجموعة بت DF. أستخدم الأمر **set ip df** لمسح بت DF والسماح بتجزئة الحزمة وإرسالها. يمكن أن يبطئ التجزئة سرعة إعادة توجيه الحزمة على الشبكة، لكن يمكن إستخدام قوائم الوصول للحد من عدد الحزم التي يتم مسح بت DF عليها.

1. قد تتسبب ثلاث مشكلات في عدم عمل PMTUD:يمكن أن يقوم الموجه الوسيط بإسقاط الحزمة وعدم الاستجابة باستخدام رسالة ICMP. وهذا غير شائع جدا على الإنترنت، ولكنه يمكن أن يكون شائعا داخل شبكة حيث تم تكوين الموجهات لعدم الاستجابة باستخدام رسائل ICMP الذي يتعذر الوصول إليه.يمكن أن يستجيب الموجه الوسيط برسالة ICMP الذي يتعذر الوصول إليه، ولكن، في تدفق الإرجاع، يقوم جدار حماية بحظر هذه الرسالة. وهذا حدوث أكثر شيوعا.تشق رسالة ICMP الذي يتعذر الوصول إليه طريقها مرة أخرى إلى المصدر، ولكن المصدر يتجاهل رسالة التجزئة. وهذه هي أكثر القضايا الثلاث شيوعا.إذا واجهت الإصدار الأول، يمكنك إما مسح بت DF في رأس IP الذي وضعه المصدر هناك أو ضبط حجم TCP MSS يدويا. لمسح بت DF، يجب أن يغير الموجه الوسيط القيمة من 1 إلى 0. عادة ما يتم القيام بذلك بواسطة موجه في شبكتك قبل أن تغادر الحزمة الشبكة. هذا تكوين رمز بسيط يقوم بذلك على موجه يستند إلى IOS:

```
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
```

2. **أنفاق PMTUD و GRE**وبشكل افتراضي، لا يقوم الموجه بتنفيذ PMTUD على حزم نفق GRE التي يقوم بتوليد نفسه. لتمكين PMTUD على واجهات نفق GRE ومشاركة الموجه في عملية ضبط MTU لأجهزة المصدر/الوجهة لحركة المرور التي تجتاز النفق، أستخدم هذا التكوين:الموجه (config) # `interface` `tunnel_#`الموجه (config-if) # `tunnel path-mtu-discovery`يتيح الأمر **tunnel path-mtu-discovery** PMTUD لواجهة نفق GRE الخاصة بالموجه. تحدد المعلمة Age-Timer الاختيارية عدد الدقائق التي تقوم بعدها واجهة النفق بإعادة تعيين الحد الأقصى لحجم MTU الذي تم اكتشافه، ناقص 24 بايت لرأس GRE. إذا قمت بتحديد *لا نهائي* للمؤقت، فلن يتم إستخدام المؤقت. تحدد المعلمة min-mtu الحد الأدنى لعدد وحدات البايت التي تحتوي على قيمة MTU.
3. **PIX/ASA 7.x - مسح أمر عدم التجزئة (DF)** أو معالجة الملفات أو الحزم الكبيرة.ما زلت غير قادر على الوصول بشكل صحيح إلى الإنترنت أو الملفات الكبيرة أو التطبيقات عبر النفق لأنه يعطي رسالة الخطأ بحجم MTU هذه:

```
,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 الواجهة الخارجية للجهاز. قم بتكوين سياسة بت DF لحزم IPSec باستخدام الأمر **crypto ipSec df-bit** في وضع التكوين العام.

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

تتيح لك ميزة بت DF باستخدام أنفاق IPSec تحديد ما إذا كان جهاز الأمان يمكنه مسح بت (DF) من الرأس المغلف أو ضبطه أو نسخه. يحدد بت DF الموجود داخل رأس IP ما إذا كان يسمح للجهاز بتجزئة حزمة أم لا.أستخدم الأمر **crypto ipSec df-bit** في وضع التكوين العام لتكوين جهاز الأمان لتحديد بت DF في رأس مغلف.عندما تقوم بتضمين حركة مرور صيغة النفق IPSec، أستخدم إعداد `clear-df` لبت DF. يتيح هذا الإعداد للجهاز إرسال حزم أكبر من حجم MTU المتاح. ويكون هذا الإعداد مناسبا أيضا إذا كنت لا تعرف حجم وحدة الحد الأقصى للنقل (MTU) المتوفر.

ملاحظة: إذا كنت لا تزال تواجه مشاكل التجزئة والحزم المسقطة، بشكل إختياري، 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 (للعملاءالمسجلين 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:

```
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 رد.**ملاحظة** 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:

```
sysopt connection tcpmss 1300
```

على الموجه:

```
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 وحاول إنشاء 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 للوصول 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).