# مثال تكوين نفق ASA Client SSL VPN عبر IPsec LAN-to-LAN

## المحتويات


المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التحقق من الصحة
استكشاف الأخطاء وإصلاحها


## المقدمة

يوضح هذا المستند كيفية الاتصال بمدخل SSLVPN بدون عملاء لأجهزة الأمان المعدلة (ASA) من Cisco والوصول إلى خادم موجود في موقع بعيد متصل عبر نفق من شبكة LAN إلى شبكة LAN لبروتوكول IPsec.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين VPN SSL بدون عملاء.
- تكوين شبكة VPN من LAN إلى LAN

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى سلسلة ASA 5500-X التي تشغل الإصدار 9.2(1)، ولكنها تنطبق على جميع إصدارات ASA.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). تأكد من فهمك للتأثير المحتمل لأي أمر قبل إجراء التغييرات على شبكة مباشرة.

# معلومات أساسية

عندما تجتاز حركة مرور البيانات من جلسة SSLVPN بدون عميل نفق من شبكة LAN إلى شبكة LAN، لاحظ أن هناك إتصالين:

- من العميل إلى ASA
- من ال ASA إلى الغاية مضيف.

بالنسبة لاتصال مضيف ASA إلى الوجهة، يتم إستخدام عنوان IP الخاص بواجهة ASA "الأقرب" إلى مضيف الوجهة. لذلك، ال LAN-to-LAN مهمة حركة مرور ينبغي تضمنت proxy-identity من أن قارن عنوان إلى الشبكة بعيد.

**ملاحظة**: إذا تم إستخدام Smart-Tunnel للإشارة المرجعية، سيظل عنوان IP الخاص بواجهة ASA الأقرب إلى الوجهة قيد الاستخدام.

# التكوين

في هذا المخطط، هناك نفق من شبكة LAN إلى شبكة LAN بين جهازي ASA يسمح لحركة المرور من x.192.168.10 إلى x.192.168.20.

قائمة الوصول التي تحدد حركة المرور المثيرة للاهتمام لذلك النفق:

**ASA1**

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

**ASA2**

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

إذا حاول مستخدم SSLVPN عديم العملاء الاتصال بمضيف على شبكة x.192.168.20، فإن ASA1 يستخدم عنوان 209.165.200.225 كمصدر لحركة المرور تلك. نظرا لأن قائمة التحكم في الوصول إلى شبكة LAN إلى شبكة LAN ACL)) لا تحتوي على 209.168.200.225 كمعرف وكيل، فلا يتم إرسال حركة مرور البيانات عبر نفق من شبكة LAN إلى شبكة LAN.

لإرسال حركة مرور البيانات عبر نفق من شبكة LAN إلى شبكة LAN، يجب إضافة إدخال تحكم في الوصول (ACE) جديد إلى قائمة التحكم في الوصول (ACL) المثيرة للاهتمام.

**ASA1**

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

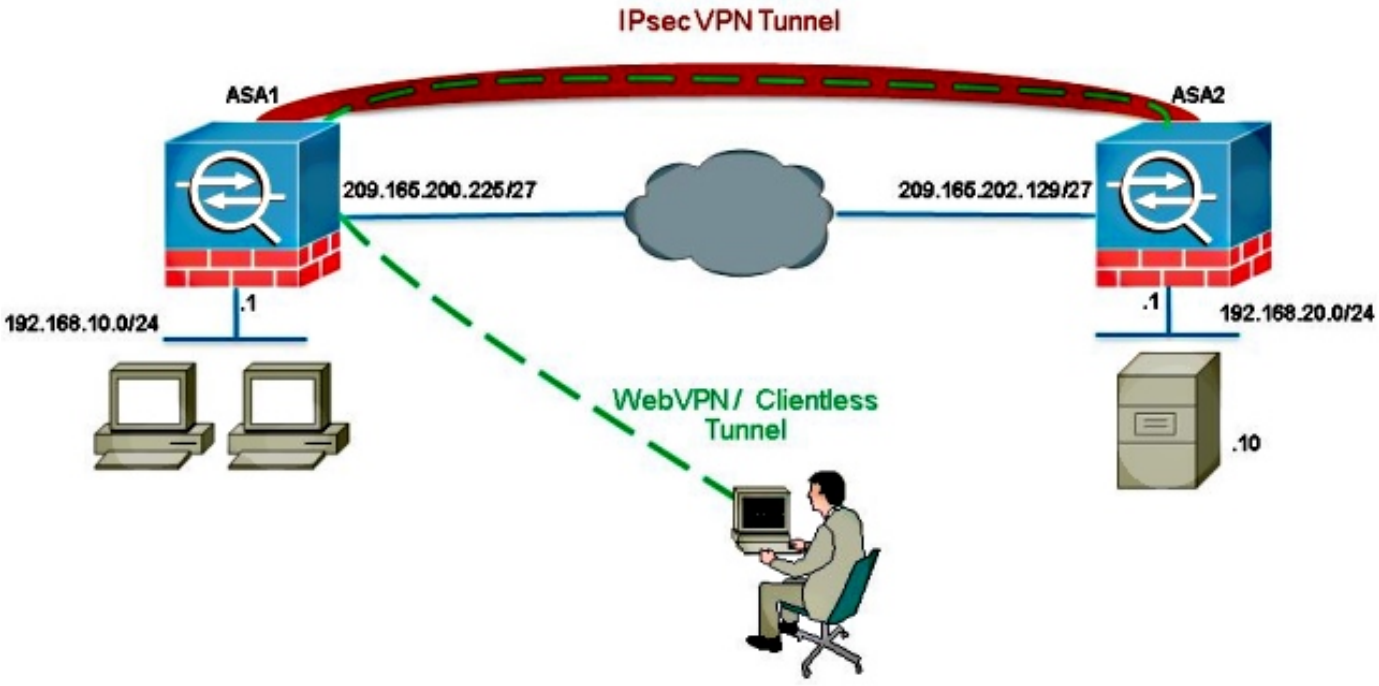
**ASA2**

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

ينطبق هذا المبدأ نفسه على التكوينات التي تحتاج فيها حركة مرور بيانات SSLVPN **دون عملاء إلى** تحويل نفس الواجهة التي تم إدخالها عليها، حتى إذا لم يكن من المفترض أن تمر عبر نفق من شبكة LAN إلى شبكة LAN.

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

### الرسم التخطيطي للشبكة




عادة، يقوم ASA2 بإجراء ترجمة عنوان المنفذ (PAT) ل 24/192.168.20.0 لتوفير الوصول إلى الإنترنت. وفي هذه الحالة، ينبغي إستبعاد حركة المرور من 24/192.168.20.0 على ASA 2 من عملية PAT عند انتقالها إلى 209.165.200.225. وإلا، فلن تتم الاستجابة عبر نفق الاتصال من شبكة LAN إلى شبكة LAN. على سبيل المثال:

#### ASA2

```
-nat (inside,outside) source static obj-192.168.20.0 obj
                                        destination 192.168.20.0
                                static obj-209.165.200.225 obj-209.165.200.225
                                                                !
                                        object network obj-192.168.20.0
                                nat (inside,outside) dynamic interface
```

## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

لمُخرَج الأمر **show**.

- **show crypto ipSec**-verify باستخدام هذا الأمر الذي تم إنشاء اقتران أمان (SA) بين عنوان IP لوكيل ASA1 والشبكة البعيدة. تحقق من زيادة العدادات المشفرة والتي تم فك تشفيرها عند وصول مستخدم SSLVPN عديم العملاء إلى هذا الخادم.

# استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

في حالة عدم إنشاء اقتران الأمان، يمكنك إستخدام تصحيح أخطاء IPsec لمعرفة سبب الفشل:

- **<debug crypto ipSec <level**

**ملاحظة**: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

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).