

# نيوكت لاثم لالڤ نم ASA VPN ليمع لاصتا L2L قفن

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [إضافة إدخال ديناميكي جديد](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)

## المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco للسماح باتصال عميل VPN عن بعد من عنوان نظير من شبكة LAN إلى شبكة (L2L) LAN.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco من ASA
- [شبكات VPN للوصول عن بعد](#)
- [شبكات VPN من شبكة LAN إلى شبكة LAN](#)

### المكونات المستخدمة

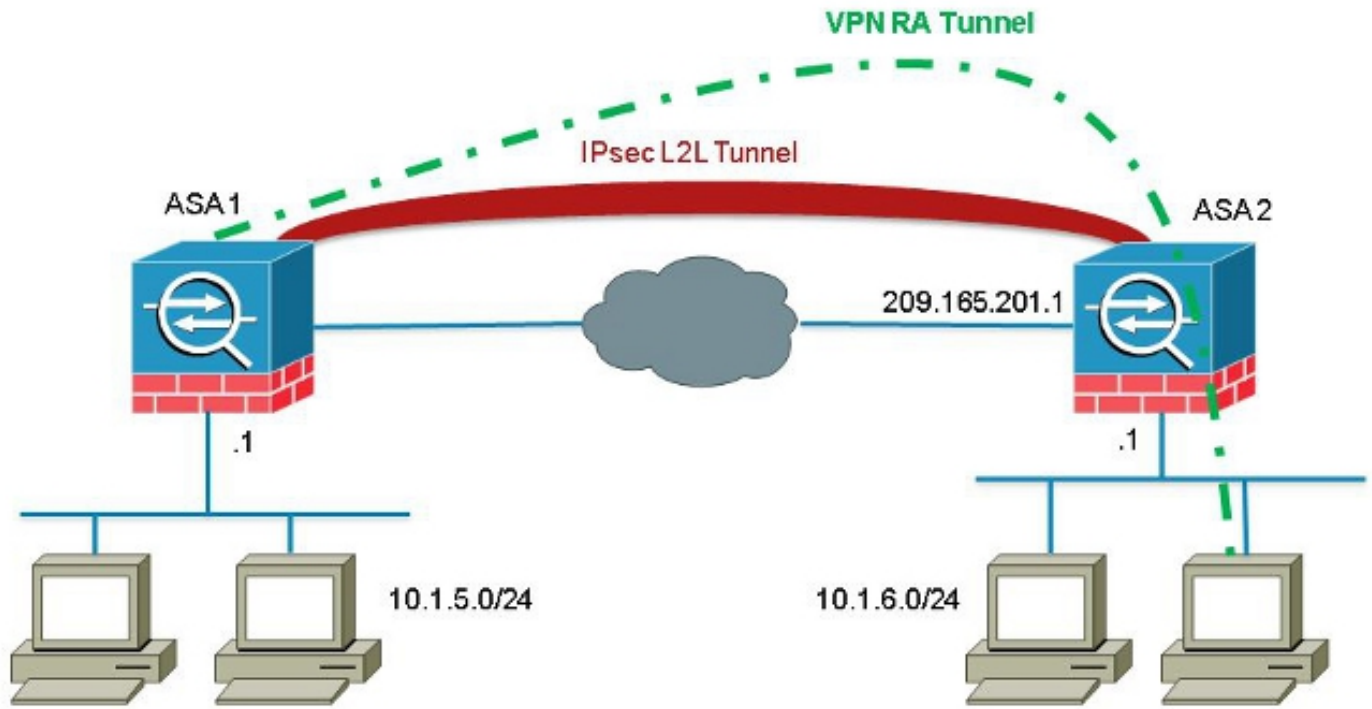
أسست المعلومة في هذا وثيقة على ال Cisco 5520 sery ASA أن يركض برمجية صيغة 8.4(7).

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.

## معلومات أساسية

على الرغم من أنه ليس من الشائع مواجهة سيناريو حيث يحاول عميل شبكة VPN إنشاء اتصال من خلال نفق L2L، فقد يحتاج المسؤولون إلى تخصيص امتيازات معينة أو قيود وصول إلى مستخدمين بعينين وتوجيههم إلى استخدام عميل البرنامج عندما يكون الوصول إلى هذه الموارد مطلوباً.

ملاحظة: نجح هذا السيناريو في الماضي، ولكن بعد ترقية وحدة الاستقبال والبث ASA إلى الإصدار 8.4(6) أو إصدار أحدث، لم يعد عميل شبكة VPN قادراً على إنشاء الاتصال.



قدم معرف تصحيح الأخطاء من [Cisco CSCuc75090](#) تغيير السلوك. سابقاً، باستخدام Private Internet Exchange (PIX)، عندما لم يكن وكيل أمان بروتوكول الإنترنت (IPSec) يطابق قائمة التحكم في الوصول إلى خريطة التشفير (ACL)، استمر في التحقق من الإدخالات التي تقع أسفل القائمة بشكل أكبر. يتضمن ذلك تطابقات مع خريطة تشفير ديناميكية دون تحديد نظير.

اعتبر هذا الأمر نقطة ضعف، حيث يمكن للمسؤولين عن بعد الوصول إلى الموارد التي لم يقصدها مسؤول وحدة الاستقبال والبث عند تكوين L2L الثابت.

تم إنشاء إصلاح يضيف شيكا لمنع التطابقات مع إدخال خريطة تشفير بدون نظير عندما قام بالفعل بالتحقق من إدخال خريطة يطابق النظير. ومع ذلك، فقد أثر ذلك على السيناريو الذي تتم مناقشته في هذه الوثيقة. وعلى وجه الخصوص، لا يمكن لعميل VPN بعيد يحاول الاتصال من عنوان نظير L2L الاتصال بنقطة الاستقبال والبث.

## التكوين

استعملت هذا قسم in order to شكلت ال ASA in order to سمحت بعيد VPN زبون توصيل من L2L نظير عنوان.

إضافة إدخال ديناميكي جديد

in order to VPN بعيد توصيل من L2L نظير عنوان، أنت ينبغي أضفت جديد حركي مدخل أن يحتوي ال نفسه نظير عنوان.

**ملاحظة:** يجب أيضا ترك إدخال ديناميكي آخر بدون نظير حتى يمكن لأي عميل من الإنترنت الاتصال أيضا.

وفيما يلي مثال على تكوين عمل خريطة التشفير الديناميكية السابق:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
```

```
crypto map outside_map 1 match address outside_cryptomap_1
```

```
crypto map outside_map 1 set peer 209.165.201.1
```

```
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
```

```
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

فيما يلي تكوين خريطة التشفير الديناميكي باستخدام الإدخال الديناميكي الجديد الذي تم تكوينه:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
```

```
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
```

```
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA
```

```
crypto map outside_map 1 match address outside_cryptomap_1
```

```
crypto map outside_map 1 set peer 209.165.201.1
```

```
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
```

```
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

## التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچ م ادخت ساب دن تسم ل اذ ه Cisco ت مچرت  
م ل اء ان ا مچ ي ف ن م دخت س م ل م عد و ت م م م دقت ل ة يرش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا