شبكة VPN للعميل عبر شبكة LAN مع مثال تكوين WLC اللاسلكية

المحتويات

المقدمة

يقدم هذا المستند مفهوم الشبكة الخاصة الظاهرية (VPN) في بيئة لاسلكية. يشرح المستند التكوينات المعنية بنشر نفق VPN بين عميل لاسلكي وخادم VPN من خلال وحدة تحكم في الشبكة المحلية اللاسلكية (WLC).

المتطلبات الأساسية

المتطلبات

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

- معرفة التحكم في الشبكة المحلية اللاسلكية (WLCs) وكيفية تكوين معلمات WLC الأساسية
- معرفة مفاهيم الوصول المحمي عبر شبكة WPA) Wi-Fi)
- معرفة أساسية بالشبكة الخاصة الظاهرية (VPN) وأنواعها
- معرفة IPsec
- معرفة أساسية بخوارزميات التشفير والمصادقة والتجزئة المتاحة

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 2006 WLC أن يركض صيغة 4.0.179.8
- نقطة الوصول في الوضع Lightweight (LAP) سلسلة Cisco 1000
- cisco 3640 أن يركض cisco ios ® برمجية إطلاق 12.4(8)
- عميل Cisco VPN، الإصدار 4.8

ملاحظة: يستخدم هذا المستند موجه من الطراز 3640 كخادم شبكة VPN. لدعم ميزات أمان أكثر تقدما، يمكنك أيضا إستخدام خادم شبكة خاصة ظاهرية (VPN) مخصص.

ملاحظة: لكي يعمل الموجه كخادم شبكة VPN، يحتاج إلى تشغيل مجموعة ميزات تدعم IPsec الأساسي.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

معلومات أساسية

الشبكة الخاصة الظاهرية (VPN) هي شبكة بيانات خاصة يتم إستخدامها لنقل البيانات بأمان داخل شبكة خاصة من خلال البنية الأساسية للاتصالات العامة مثل الإنترنت. تحافظ شبكة VPN هذه على خصوصية البيانات من خلال إستخدام بروتوكول نفق وإجراءات الأمان.

شبكة VPN للوصول عن بعد

يتم إستخدام تكوين شبكة VPN للوصول عن بعد للسماح لعملاء برامج VPN مثل مستخدمي الأجهزة المحمولة بالوصول الآمن إلى موارد الشبكة المركزية الموجودة خلف خادم VPN. في مصطلحات Cisco، تسمى خوادم VPN هذه والعملاء أيضا خادم Cisco Easy VPN والجهاز البعيد Cisco Easy VPN.

يمكن أن يكون الجهاز البعيد السهل VPN من Cisco موجهات Cisco IOS وأجهزة أمان PIX من Cisco وعملاء أجهزة Cisco VPN 3002 وعميل Cisco VPN. يتم إستخدامها لتلقي سياسات الأمان على اتصال نفق VPN من خادم Cisco Easy VPN. وهذا يؤدي إلى تقليل متطلبات التكوين إلى الحد الأدنى في الموقع البعيد. عميل شبكة VPN من Cisco هو عميل برنامج يمكن تثبيته على أجهزة الكمبيوتر الشخصية وأجهزة الكمبيوتر المحمولة وما إلى ذلك.

يمكن أن يكون خادم Cisco Easy VPN موجهات Cisco IOS وأجهزة الأمان PIX من Cisco ومحركات VPN 3000 من Cisco.

يستخدم هذا المستند برنامج عميل شبكة VPN من Cisco الذي يتم تشغيله على كمبيوتر محمول كعميل شبكة VPN وموجه Cisco 3640 IOS كخادم شبكة VPN. يستخدم المستند معيار IPsec لإنشاء نفق VPN بين عميل وخادم.

IPsec

IPsec هو إطار للمعايير المفتوحة تم تطويره بواسطة "فريق عمل هندسة الإنترنت" (IETF). يوفر IPsec الأمان لنقل المعلومات الحساسة عبر الشبكات غير المحمية مثل الإنترنت.

يوفر IPsec تشفيرا لبيانات الشبكة عند مستوى حزمة IP، والذي يوفر حلا أمنيا قويا يستند إلى المعايير. تتمثل المهمة الرئيسية ل IPsec في السماح بتبادل المعلومات الخاصة عبر اتصال غير آمن. يستخدم IPsec التشفير لحماية

المعلومات من الاعتراض أو التنصت. ومع ذلك، لاستخدام التشفير بكفاءة، ينبغي أن يتشارك كلا الطرفين سرا يستخدم لتشفير المعلومات وفك تشفيرها.

يعمل IPsec على مرحلتين للسماح بتبادل سري لسر مشترك:

- المرحلة 1—يعالج التفاوض حول معلمات الأمان المطلوبة لإنشاء قناة آمنة بين نظائر IPsec. يتم تنفيذ المرحلة الأولى بشكل عام من خلال بروتوكول تبادل مفتاح الإنترنت (IKE). إذا تعذر على نظير IPsec البعيد تنفيذ IKE، فيمكنك إستخدام التكوين اليدوي باستخدام مفاتيح تمت مشاركتها مسبقا لإكمال المرحلة 1.
- المرحلة 2—يستخدم النفق الآمن الذي تم إنشاؤه في المرحلة الأولى لتبادل معلمات الأمان المطلوبة لنقل بيانات المستخدم بالفعل. تستند الأنفاق الآمنة المستخدمة في كلا مرحلتي IPsec إلى اقترانات الأمان (SAs) المستخدمة في كل نقطة نهاية IPsec. تصف إجراءات الأمان معلمات الأمان، مثل نوع المصادقة والتشفير الذي توافق كلا النقطتين النهائيتين على إستخدامه.

يتم إستخدام معلمات الأمان المتبادلة في المرحلة 2 لإنشاء نفق IPsec الذي يتم إستخدامه بدوره لنقل البيانات بين عميل VPN والخادم.

راجع تكوين IPsec للحصول على مزيد من المعلومات حول IPsec وتكوينه.

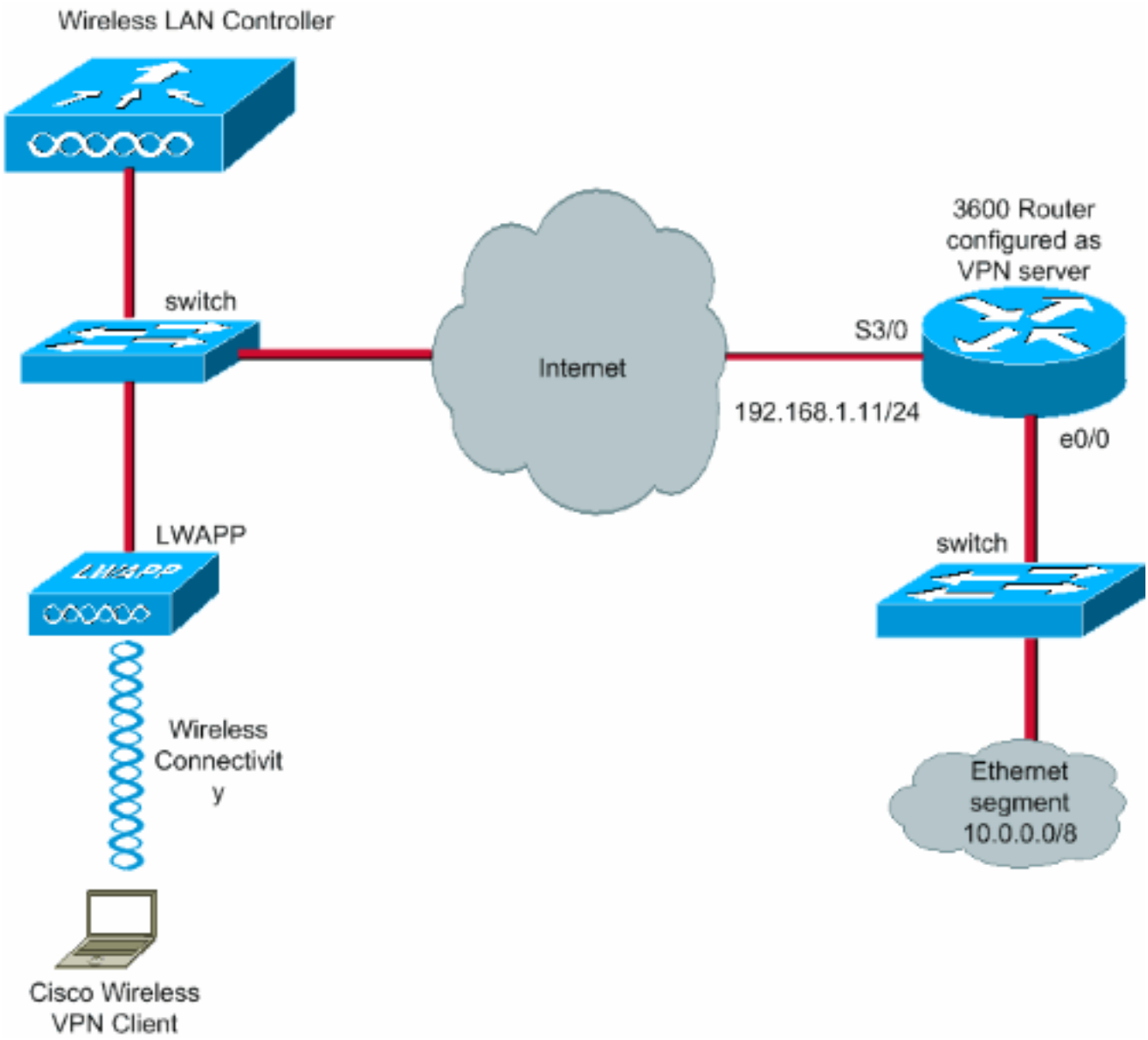
بمجرد إنشاء نفق VPN بين عميل VPN والخادم، *يتم إرسال سياسات الأمان المحددة في خادم VPN إلى العميل*. وهذا يؤدي إلى تقليل متطلبات التكوين إلى الحد الأدنى في جانب العميل.

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند التكوينات التالية:

- عنوان IP لواجهة الإدارة الخاص ب WLC-172.16.1.10/16
- عنوان IP لواجهة AP-Manager الخاصة بواجهة WLC-172.16.1.11/16
- العبارة الافتراضية—16/172.16.1.20**ملاحظة:** في شبكة مباشرة، يجب أن تشير هذه العبارة الافتراضية إلى الواجهة الواردة للموجه المباشر الذي يربط عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بباقي الشبكة و/أو بالإنترنت.
- عنوان IP الخاص بخادم VPN S3/0-192.168.1.11/24**ملاحظة:** يجب أن يشير عنوان IP هذا إلى الواجهة التي تنهي نفق VPN في جانب خادم VPN. في هذا المثال، S3/0 هو الواجهة التي تنهي نفق VPN في خادم VPN.
- يستخدم مقطع الشبكة المحلية (LAN) في خادم VPN نطاق عنوان IP الخاص ب 8/10.0.0.0.



التكوين

في البنية المركزية لشبكة WLAN، من أجل السماح لعميل شبكة VPN لاسلكية مثل كمبيوتر محمول لإنشاء نفق VPN مع خادم شبكة VPN، من الضروري أن يترافق العميل مع نقطة وصول (LAP) في الوضع Lightweight (LAP)) تحتاج بدورها إلى التسجيل مع وحدة تحكم في الشبكة المحلية اللاسلكية (WLC). يتلقى هذه وثيقة ال{lap}upper بما أن يكون سجلت مع ال WLC يستعمل ال subnet محلي بث إكتشاف عملية شرح في خفيف وزن ap (ثنى) تسجيل إلى لاسلكي lan جهاز تحكم (WLC).

الخطوة التالية هي تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لشبكة VPN.

إنهاء الشبكة الخاصة الظاهرية (VPN) والتمرير

مع وجود وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs) الأولى من الإصدار 4 من Cisco، يتم دعم ميزة تسمى إنهاء VPN لبروتوكول IPsec (دعم IPsec). تمكن هذه الميزة وحدات التحكم هذه من إنهاء جلسات عمل عميل شبكة VPN مباشرة على وحدة التحكم. وباختصار، تمكن هذه الميزة وحدة التحكم نفسها من العمل كخادم شبكة VPN. غير أن هذا يتطلب تثبيت وحدة جهاز إنهاء شبكة VPN منفصلة في وحدة التحكم.

دعم IPsec VPN هذا غير متوفر في:

- Cisco 2000 Series WLC
- أي WLCs تشغل الإصدار 4.0 أو الأحدث

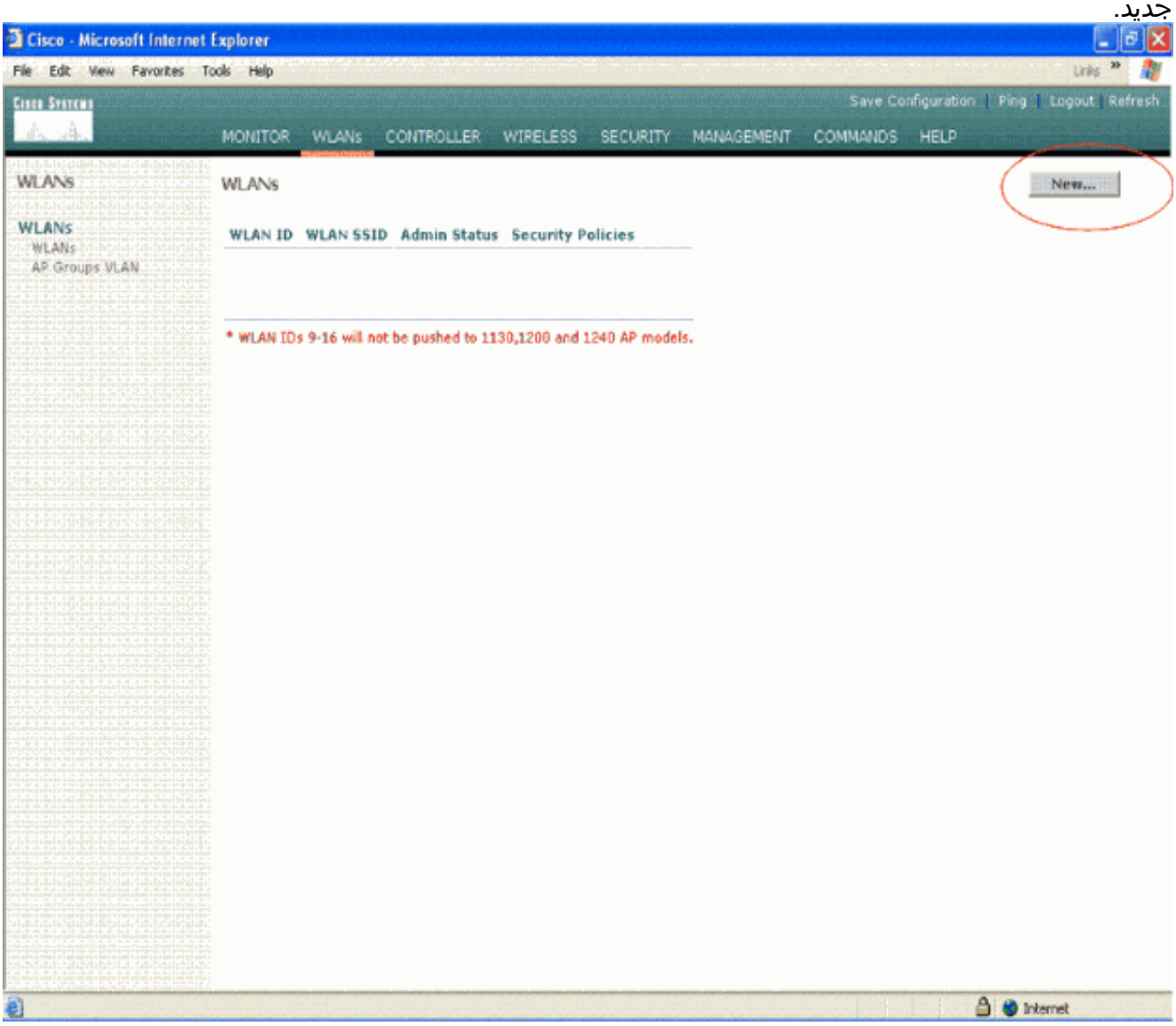
لذلك، ال VPN وحيد يساند سمة في صيغة متأخر من VPN Pass-Through 4،0. هذا سمة أيضا ساندت في ال cisco 2000 sery WLC.

VPN Pass-Through هي ميزة تسمح للعميل بإنشاء نفق فقط مع خادم VPN محدد. لذلك، إذا كنت بحاجة إلى الوصول بأمان إلى خادم VPN الذي تم تكوينه وكذلك خادم VPN آخر أو الإنترنت، فهذا لا يمكن مع تمكين تمرير VPN على وحدة التحكم. تحت هذا متطلب، أنت تحتاج أن يعجز VPN Pass-Through. ومع ذلك، يمكن تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعمل ككلمة مرور للوصول إلى عبارات VPN متعددة عند إنشاء قائمة تحكم في الوصول (ACL) مناسبة وتطبيقها على شبكة WLAN المقابلة. لذلك، في ظل هذه السيناريوهات التي تريد فيها الوصول إلى عبارات VPN متعددة للتكرار، قم بتعطيل مرور الشبكة الخاصة الظاهرية (VPN) وإنشاء قائمة تحكم في الوصول (ACL) تتيح الوصول إلى بوابات الشبكة الخاصة الظاهرية (VPN) وتطبيق قائمة التحكم في الوصول إلى الشبكة المحلية اللاسلكية (WLAN).

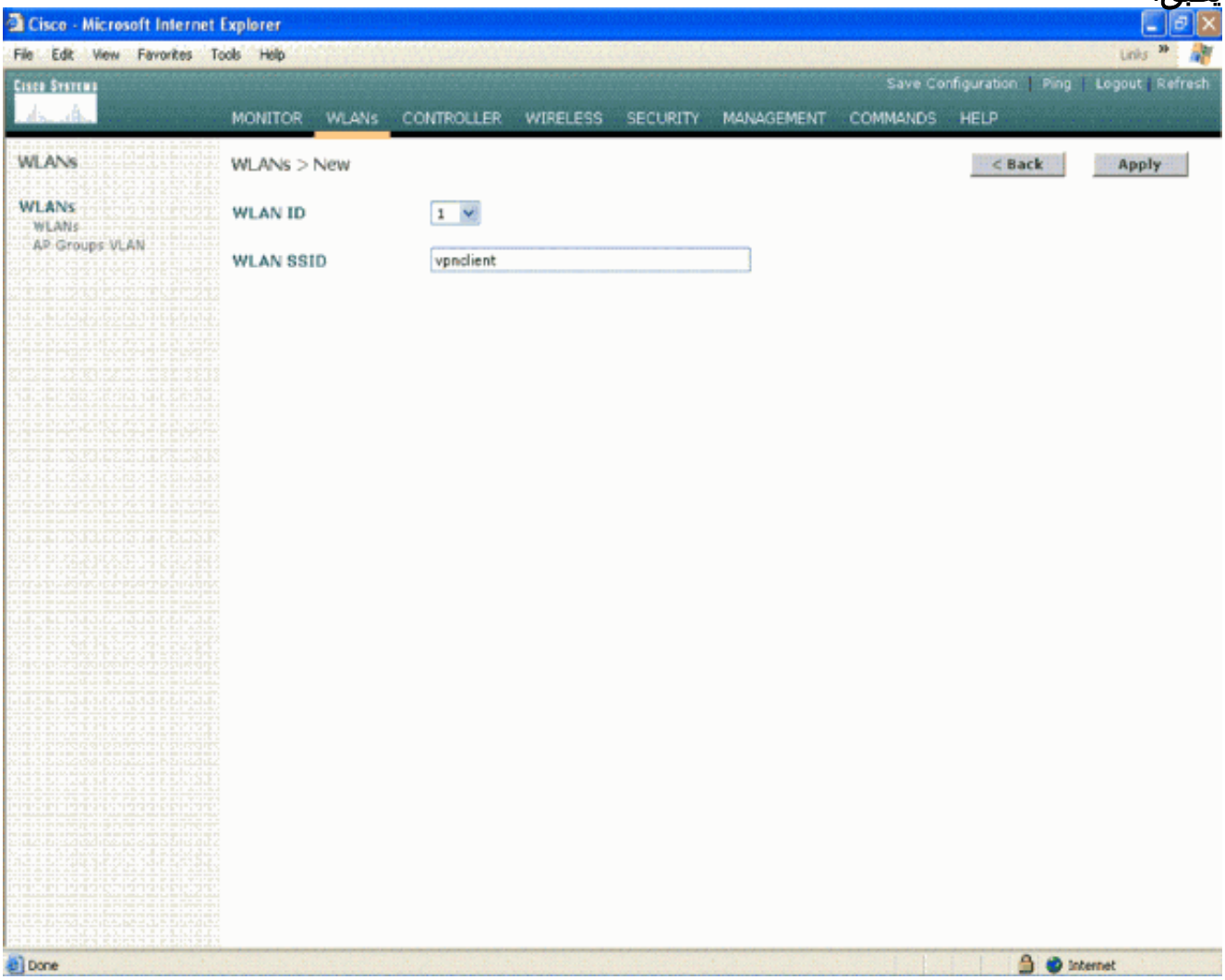
تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمرور VPN

أتمت هذا steps in order to شكلت VPN Pass-through.

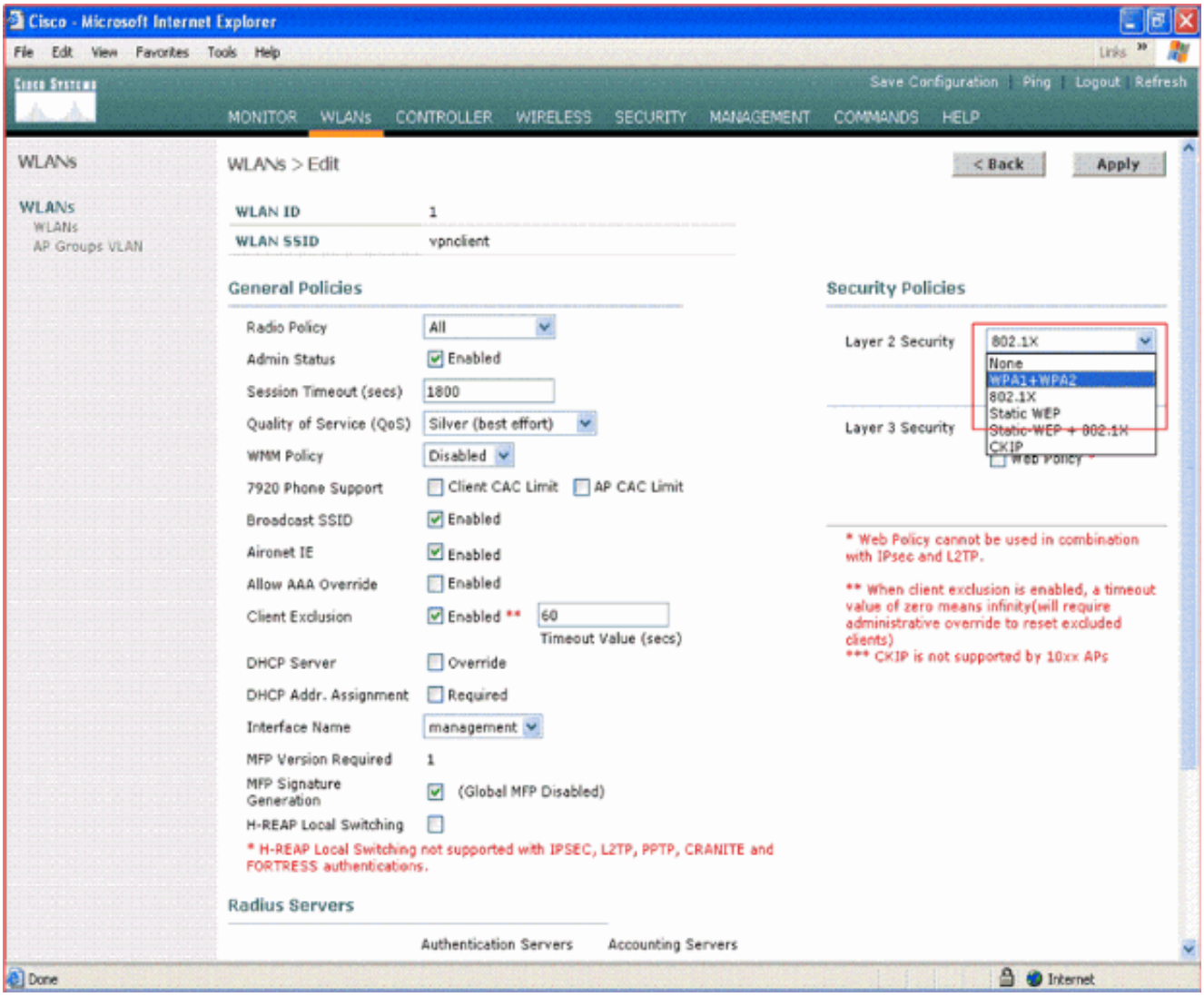
1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **شبكة WLAN** للانتقال إلى صفحة شبكات WLAN.
2. طقطقت **جديد** in order to خلقت WLAN جديد.



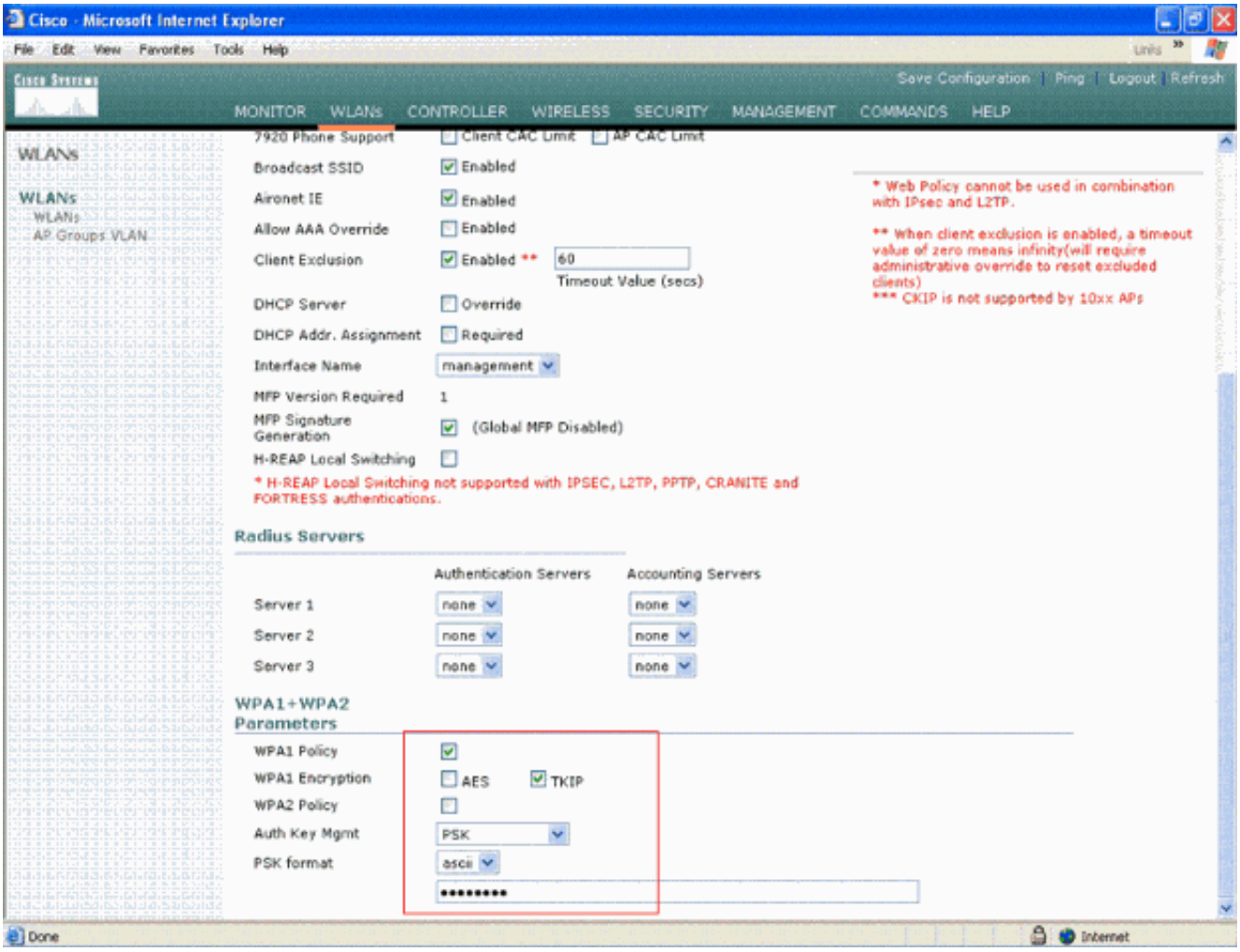
3. يتم تسمية WLAN SSID باسم **vpnClient** في هذا المثال. طقطقة **يطبق**.



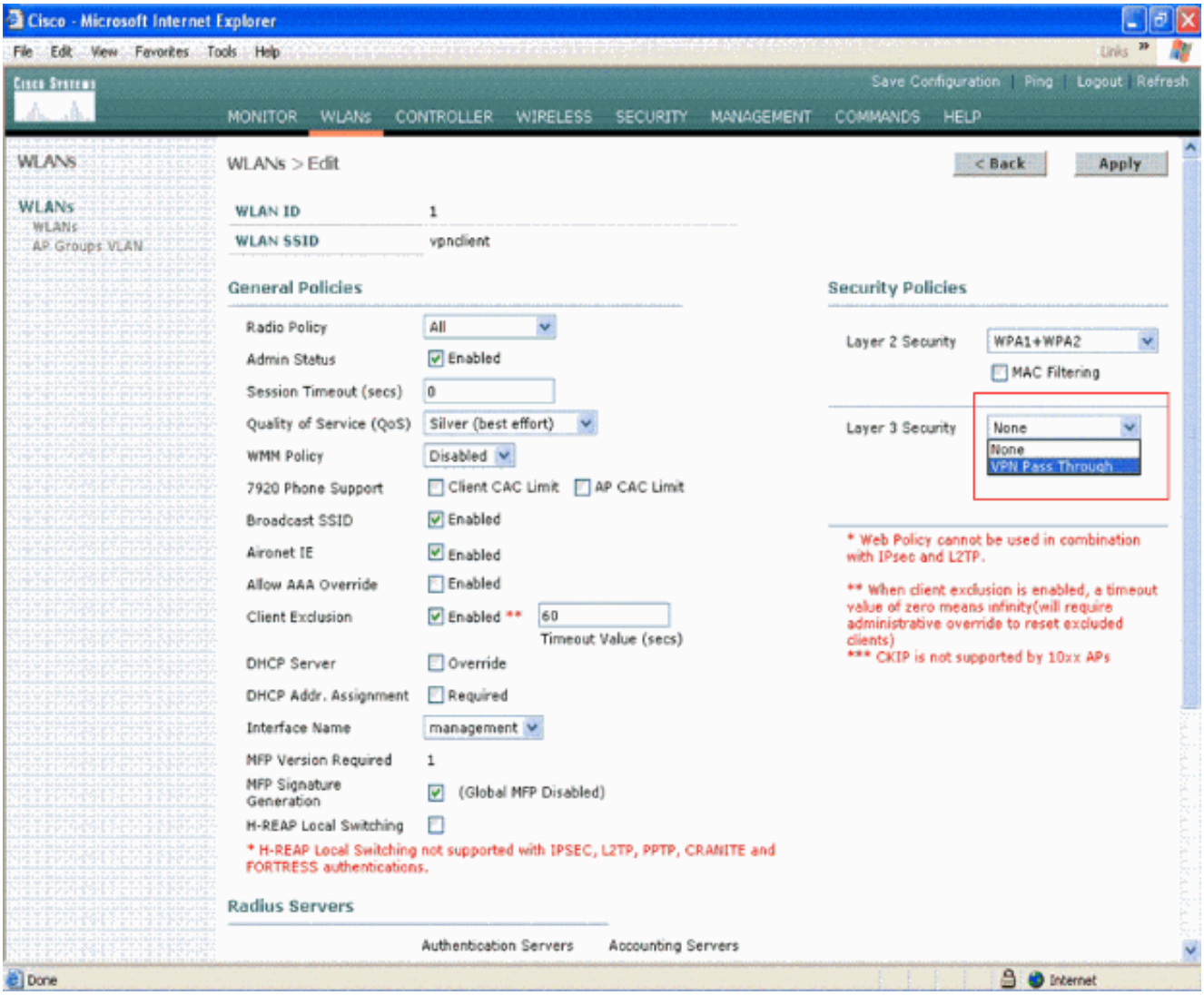
4. تكوين SSID الخاص ب VPNclient مع أمان الطبقة 2. *هذا إختياري*.يستخدم هذا المثال **WPA1+WPA2** كنوع
تأمين.



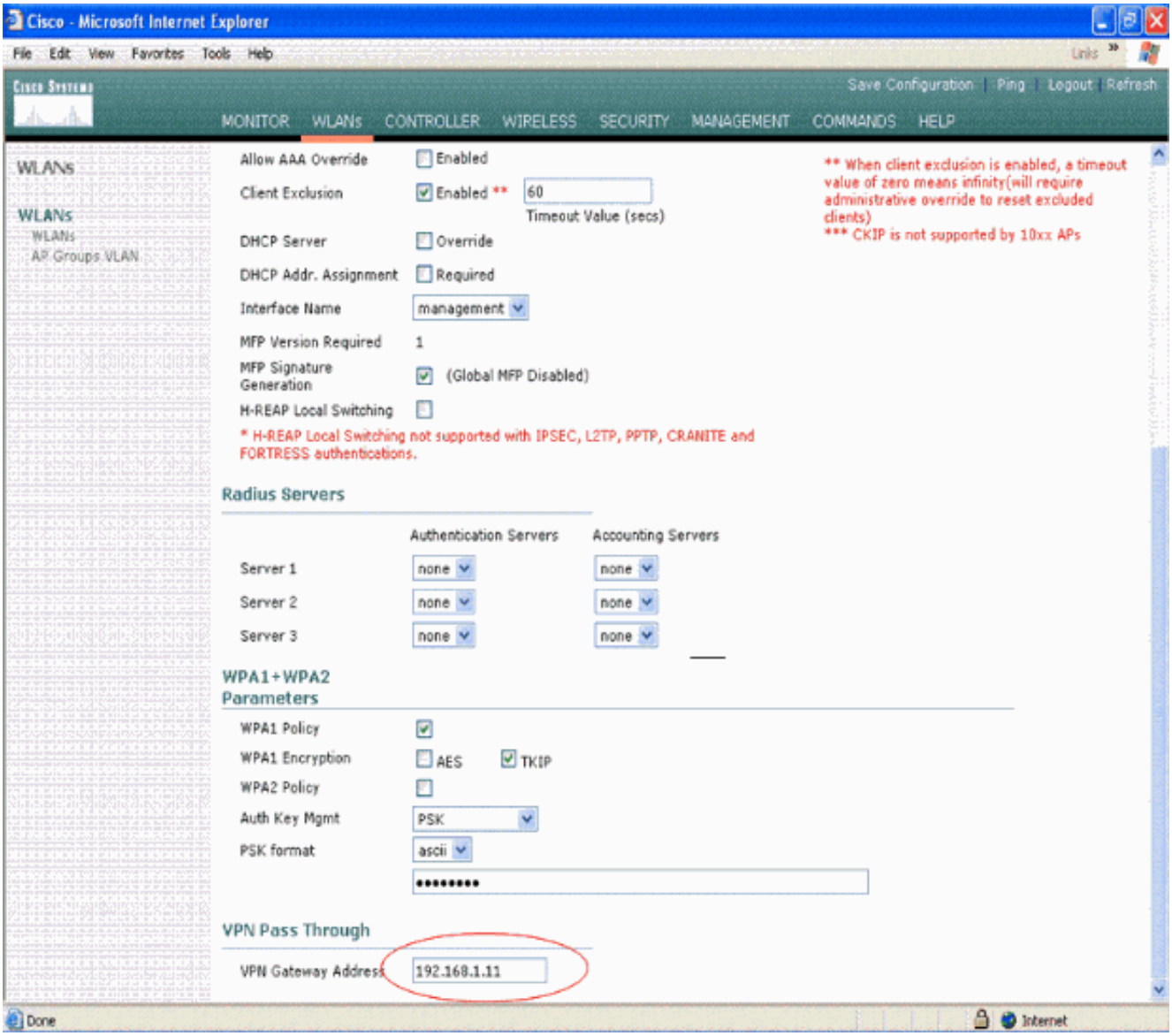
5. قم بتكوين نهج WPA ونوع إدارة مفتاح المصادقة المراد إستخدامهما.يستخدم هذا المثال **مفتاح مشترك مسبقا (PSK)** لإدارة مفاتيح المصادقة. بمجرد تحديد PSK، حدد **ASCII** كتنسيق PSK واكتب قيمة PSK. يجب أن تكون هذه القيمة هي نفسها في تكوين SSID للعميل اللاسلكي حتى يتمكن العملاء الذين ينتمون إلى SSID هذا من الاقتران بشبكة WLAN هذه.



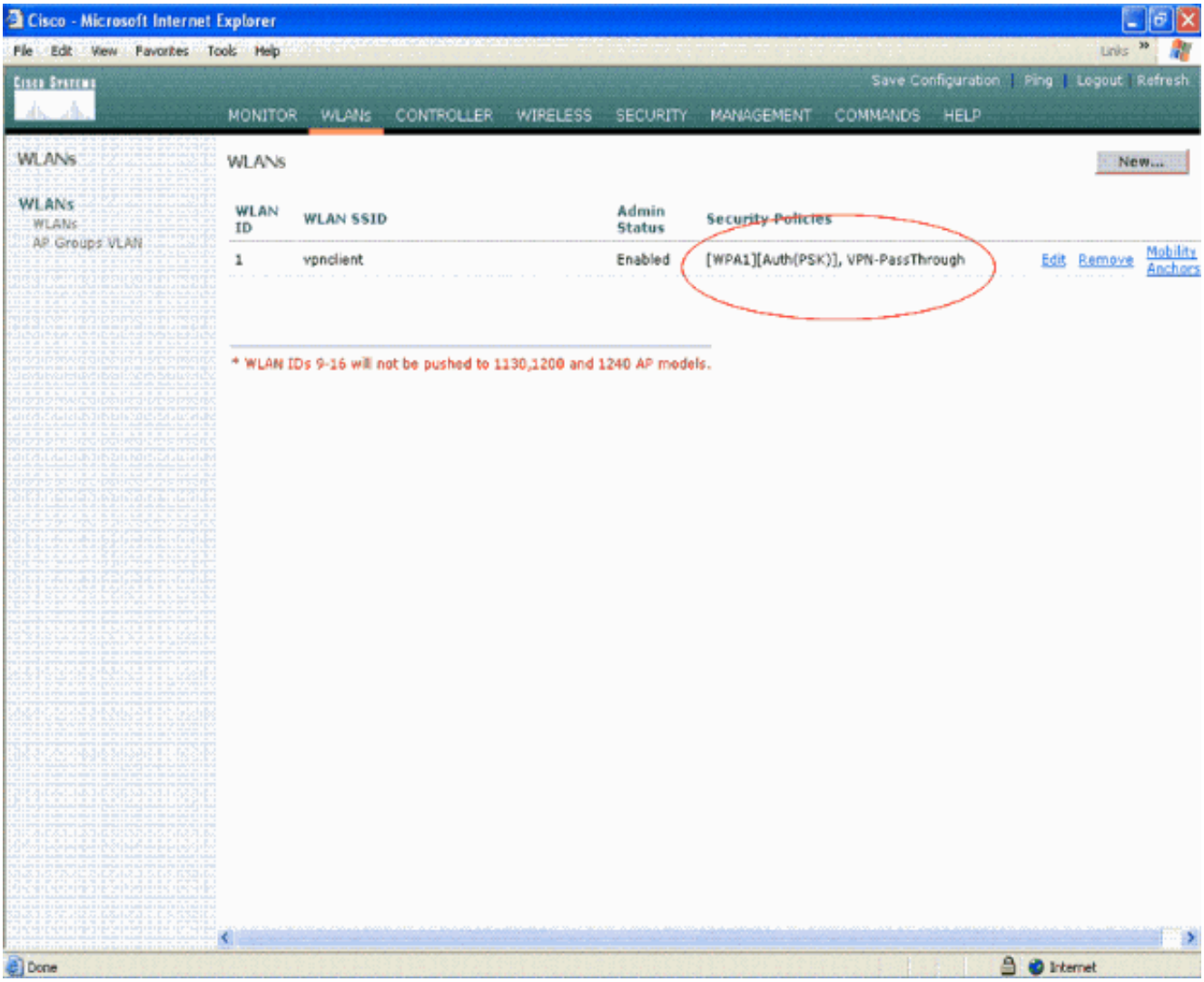
6. حدد **مرور VPN** كتأمين الطبقة 3. هنا مثال.



7. بمجرد تحديد مرور VPN كأمان الطبقة 3، أضف عنوان بوابة شبكة VPN كما يوضح هذا المثال.يجب أن يكون عنوان العبارة هذا هو عنوان IP الخاص بالقارن الذي ينهي نفق VPN في جانب الخادم. في هذا المثال، عنوان IP الخاص بواجهة (S3/0 (192.168.1.11/24 في خادم VPN هو عنوان البوابة الذي سيتم تكوينه.



8. طقطقة **يطبق**. تم الآن تكوين الشبكة المحلية اللاسلكية (WLAN) المسماة *vpnClient* لتمرير شبكة VPN.



تكوين خادم VPN

يعرض هذا التكوين الموجه 3640 من Cisco كخادم VPN.

ملاحظة: لضمان البساطة، يستخدم هذا التكوين التوجيه الثابت للحفاظ على إمكانية الوصول إلى IP بين نقاط النهاية. يمكنك إستخدام أي بروتوكول توجيه ديناميكي مثل بروتوكول معلومات التوجيه (RIP) وفتح أقصر مسار أولا (OSPF) وما إلى ذلك للحفاظ على إمكانية الوصول.

ملاحظة: لا يتم إنشاء النفق إذا لم يكن هناك إمكانية وصول IP بين العميل والخادم.

ملاحظة: يفترض هذا المستند أن المستخدم على دراية بكيفية تمكين التوجيه الديناميكي في الشبكة.

موجّه Cisco 3640

```
vpnrouter#show running-config

...Building configuration

Current configuration : 1623 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
 Create an Internet Security Association and Key ---!
 Management !--- Protocol (ISAKMP) policy for Phase 1
 negotiation. hash md5
Choose the hash algorithm to be md5. authentication ---!
 pre-share
 The authentication method selected is pre-shared. ---!
 group 2
 With the group command, you can declare what size ---!
    modulus to !--- use for Diffie-Hellman calculation.
 Group 1 is 768 bits long, !--- and group 2 is 1024 bits
 .long


 crypto isakmp client configuration group employee key
 cisco123 pool mypool
 !
        Create the Phase 2 policy for actual data ---!
 encryption. crypto ipsec transform-set myset esp-3des
 esp-md5-hmac
 Create a dynamic map and apply the transform set ---!
  that was created. !--- Set reverse-route for the VPN
 server. crypto dynamic-map mymap 10 set transform-set
 myset reverse-route
 !
crypto map clientmap isakmp authorization list employee
```

```
                                        .Create the crypto map ---!
crypto map clientmap client configuration address crypto
                                  map clientmap 10 ipsec-isakmp dynamic mymap
                                                                          !
                                Apply the employee group list that was created ---!
                                                                    .earlier
                                                                          !
                                                                          !
                                                                          !
                                                                          !
                                                        interface Ethernet0/0
                                                 ip address 10.0.0.20 255.0.0.0
                                                                half-duplex
                                                                          !
                                                       interface Serial3/0
                                             ip address 192.168.1.11 255.255.255.0
                                                          clock rate 64000
                                                            no fair-queue
                                                       crypto map clientmap
Apply the crypto map to the interface. ! interface ---!
 Serial3/1 no ip address shutdown ! interface Serial3/2
     no ip address shutdown ! interface Serial3/3 no ip
   address shutdown ! interface Serial3/4 no ip address
shutdown ! interface Serial3/5 no ip address shutdown !
 interface Serial3/6 no ip address shutdown ! interface
  Serial3/7 no ip address shutdown ip local pool mypool
                                                  10.0.0.50 10.0.0.60
 Configure the Dynamic Host Configuration Protocol ---!
      !--- (DHCP) pool which assigns the tunnel !--- IP
    address to the wireless client. !--- This tunnel IP
 address is different from the IP address !--- assigned
   locally at the wireless client (either statically or
dynamically). ip http server no ip http secure-server !
   ip route 172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! !
control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0
        line vty 0 4 ! ! end ip subnet-zero . . . ! end
```

ملاحظة: يستخدم هذا المثال مصادقة المجموعة فقط. وهو لا يستخدم مصادقة المستخدم الفردية.

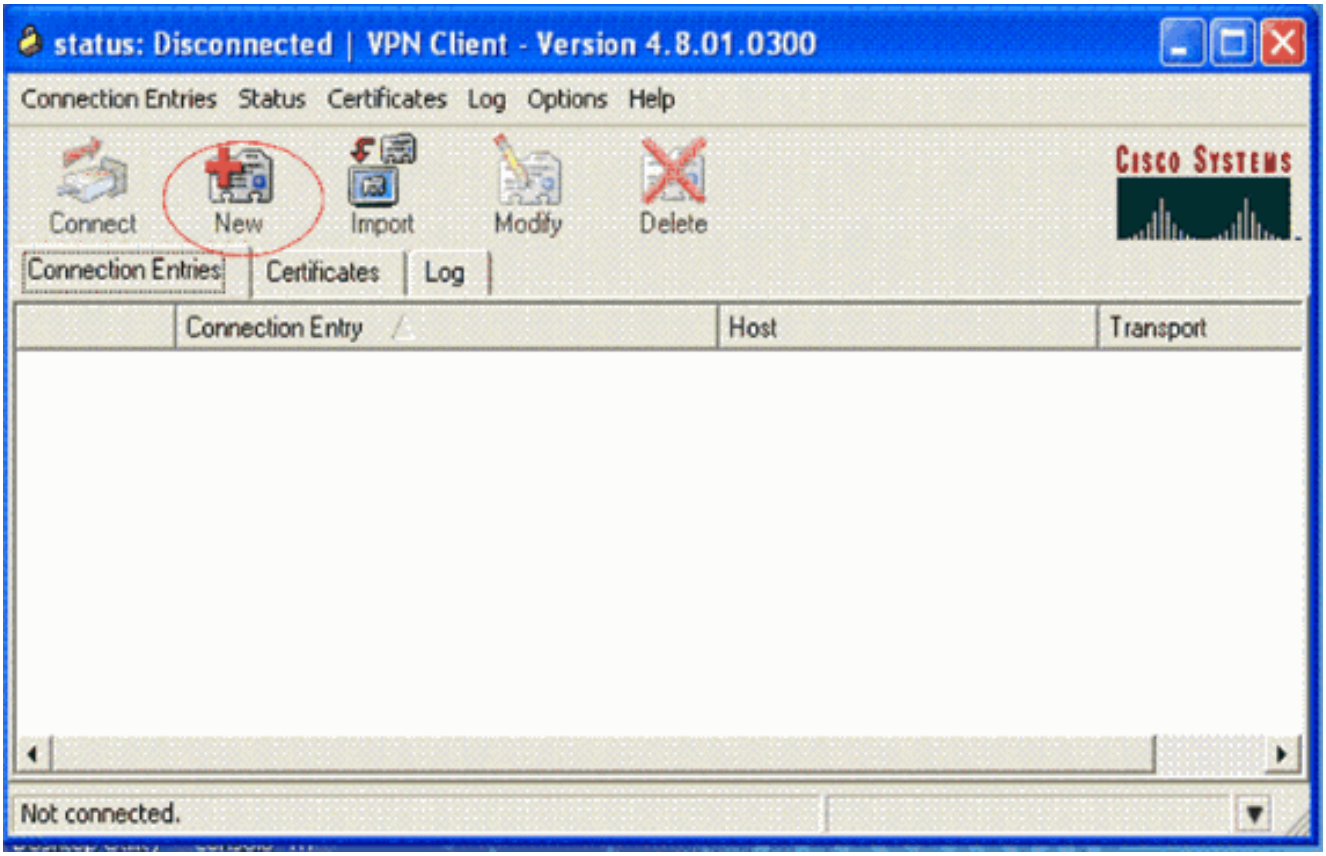
تكوين عميل شبكة VPN

يمكن تنزيل عميل شبكة VPN البرمجية من مركز البرامج Cisco.com.

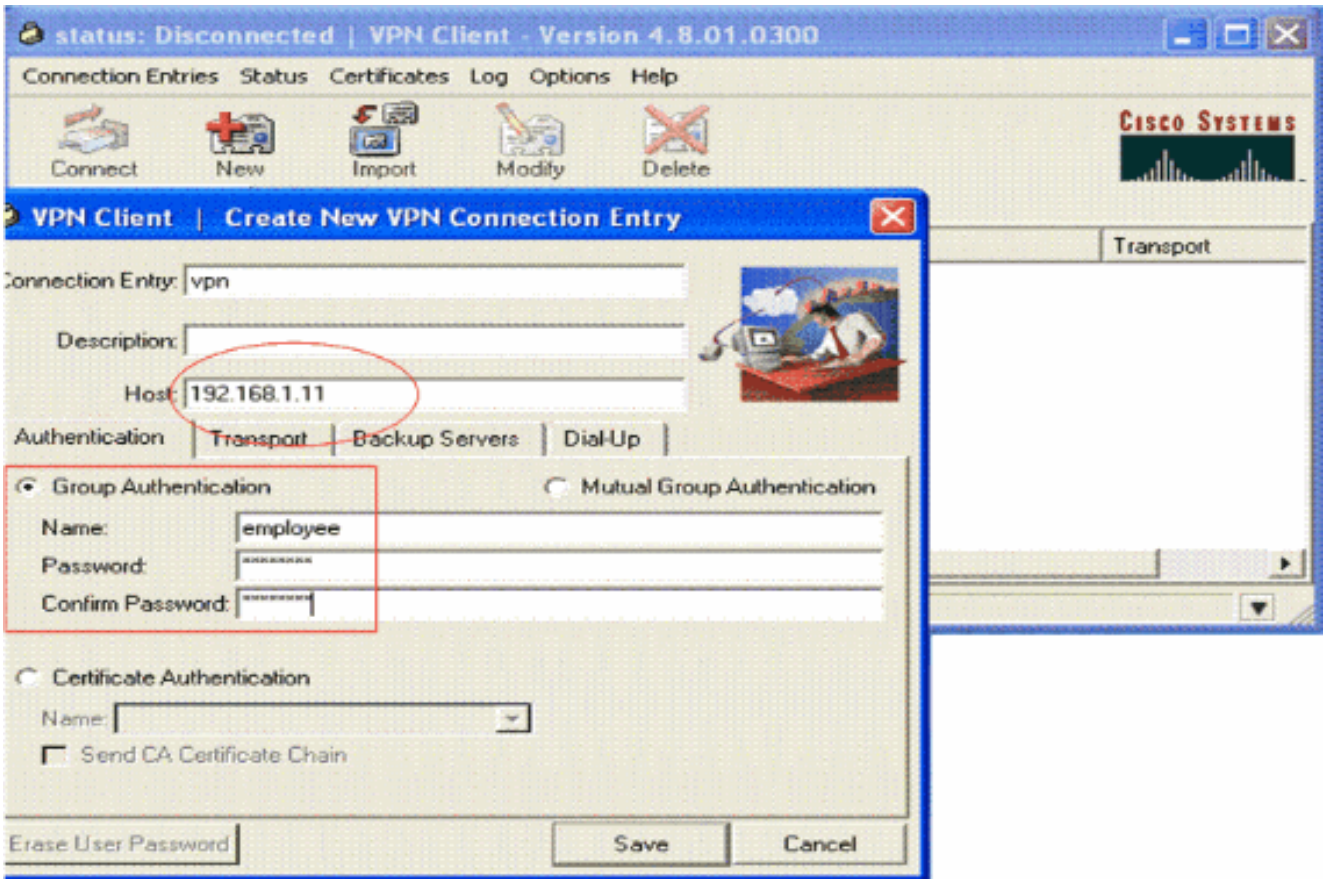
ملاحظة: تتطلب بعض برامج Cisco تسجيل الدخول باستخدام اسم مستخدم وكلمة مرور CCO.

أتمت هذا steps in order to شكلت ال VPN زبون.

1. شكل العميل اللاسلكي (الكمبيوتر المحمول)، أختر **Start (البدء) > Programs (البرامج) > Cisco Systems VPN Client (عميل الشبكة الخاصة الظاهرية (VPN))** للوصول إلى عميل الشبكة الخاصة الظاهرية (VPN). هذا هو الموقع الافتراضي الذي يتم فيه تثبيت عميل VPN.
2. طقطقت **جديد** in order to أطلقت ال create جديد VPN توصيل مدخل نافذة.



3. أدخل اسم "إدخال الاتصال" مع وصف. هذا المثال *usesvpn*.حقل الوصف إختياري. دخلت العنوان من ال VPN نادل في المضيف صندوق. ثم أدخل اسم مجموعة VPN وكلمة المرور وانقر على **حفظ**.



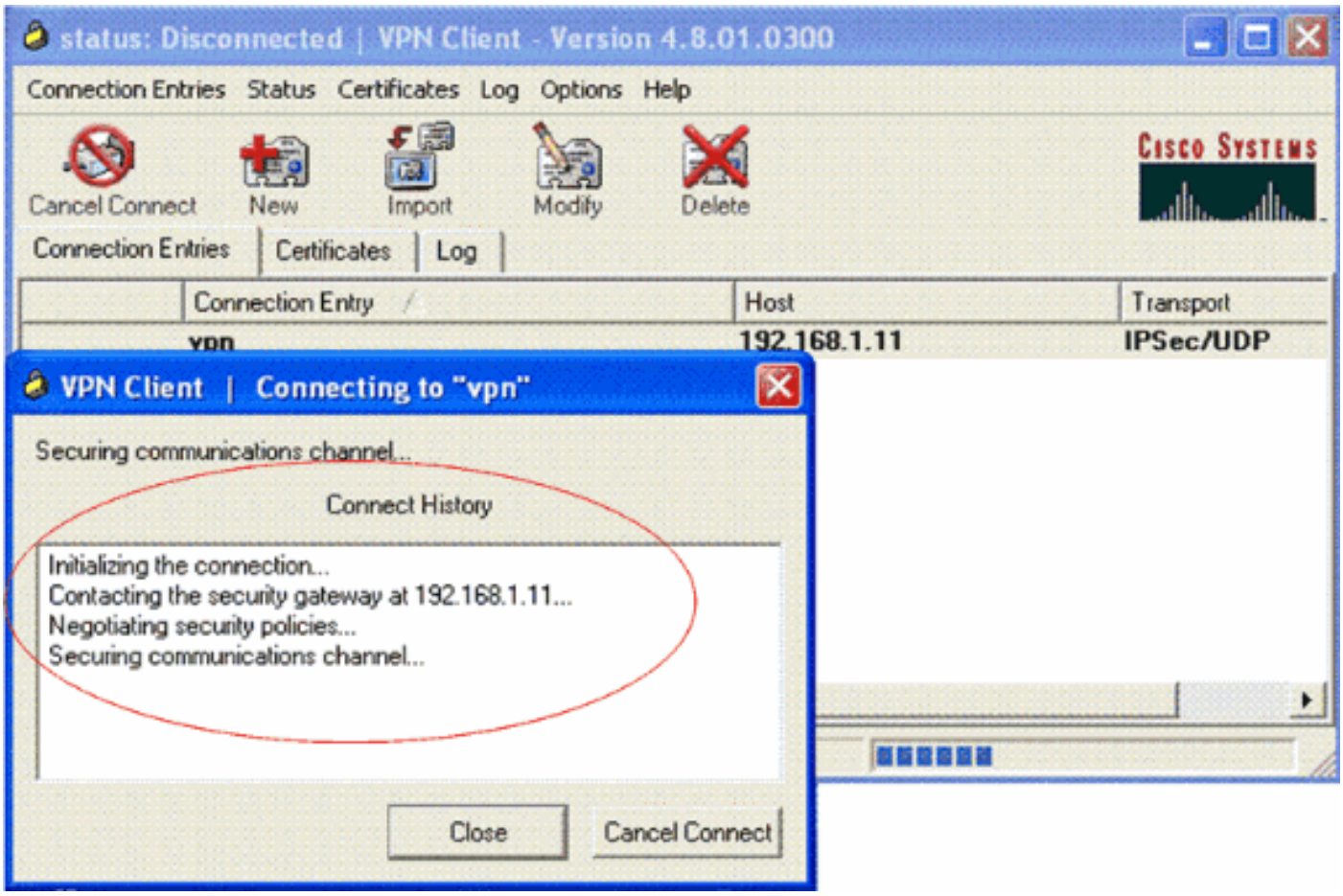
ملاحظة: يجب أن يكون اسم المجموعة وكلمة المرور اللذان تم تكوينهما هنا متماثلين مع اسم المجموعة الذي تم تكوينه في خادم VPN. يستخدم هذا المثال اسم *الموظف* وكلمة المرور *Cisco123*.

التحقق من الصحة

للتحقق من هذا التكوين، قم بتكوين **SSID vpnClient** في العميل اللاسلكي باستخدام نفس معلمات الأمان التي تم تكوينها في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) واقران العميل بشبكة WLAN هذه. هناك عدة مستندات توضح كيفية تكوين عميل لاسلكي بتوصيف جديد.

بمجرد اقتران العميل اللاسلكي، انتقل إلى عميل VPN وانقر على الاتصال الذي قمت بتكوينه. ثم انقر فوق **اتصال** من الإطار الرئيسي لعميل شبكة VPN.

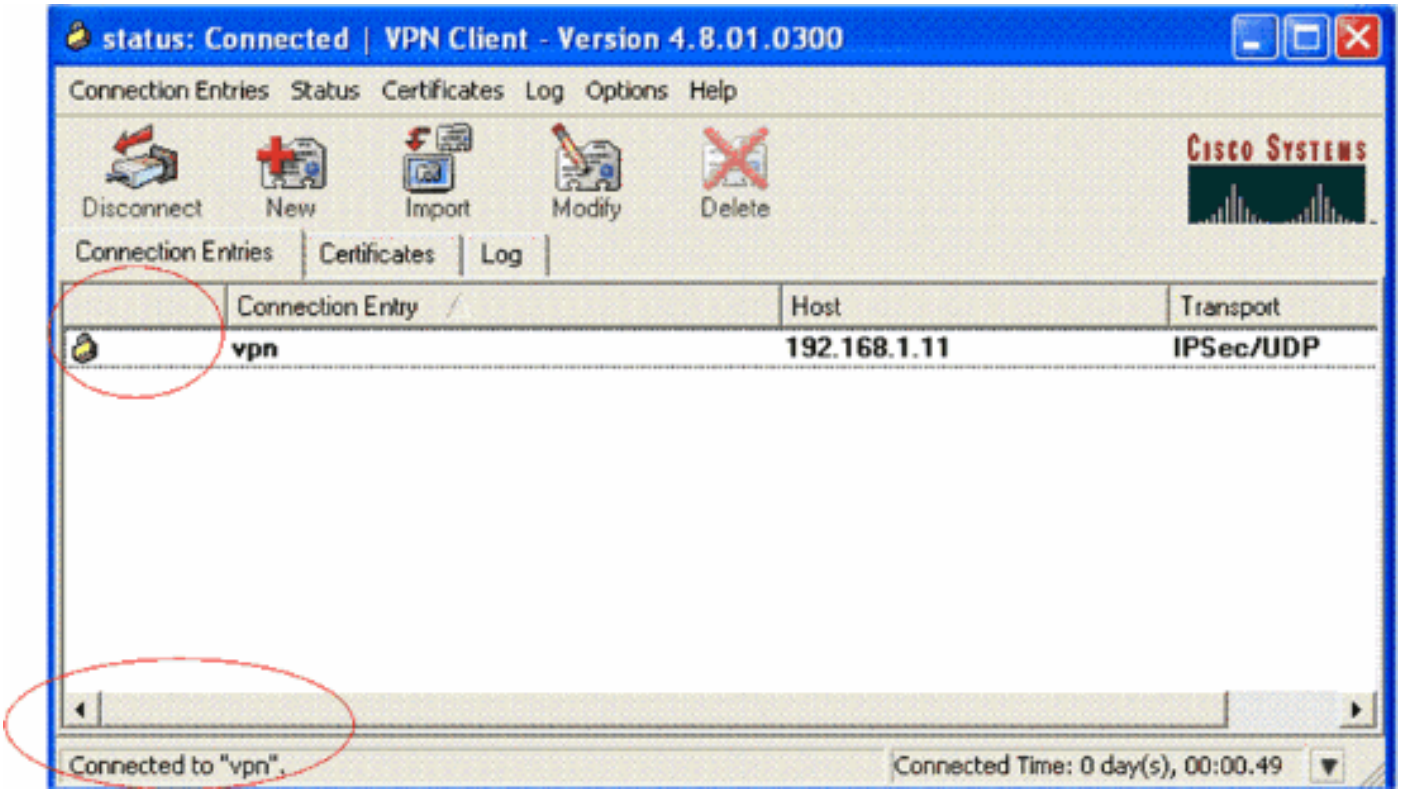
يمكنك مشاهدة معلمات أمان المرحلة الأولى والمرحلة الثانية التي تم التفاوض بشأنها بين العميل والخادم.



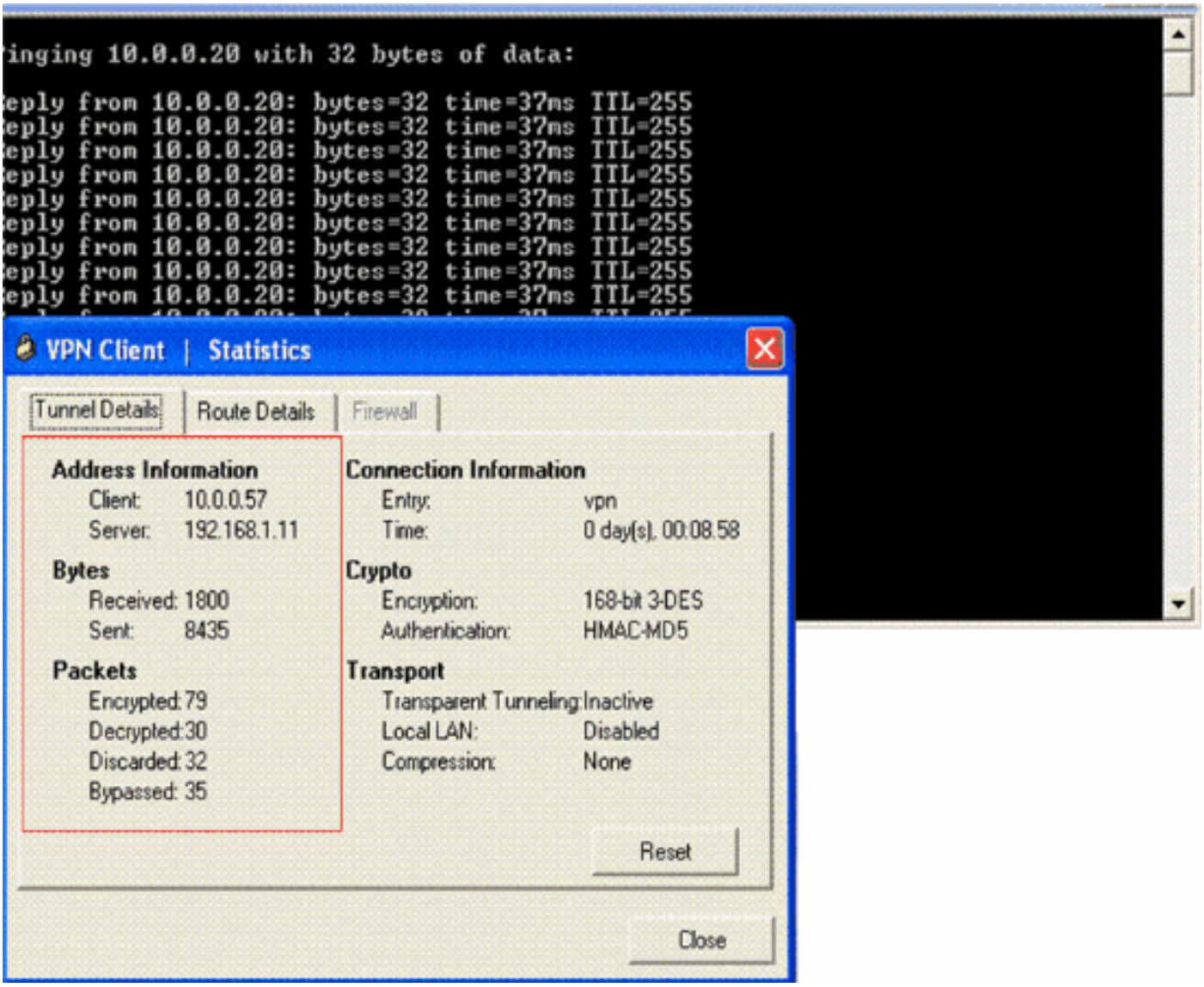
ملاحظة: لإنشاء نفق VPN هذا، يجب أن يكون لعميل شبكة VPN والخادم إمكانية الوصول إلى IP بينهما. إذا لم يتمكن عميل شبكة VPN من الاتصال ببوابة الأمان (خادم VPN)، فلن يتم إنشاء النفق ويتم عرض مربع تنبيه على جانب العميل مع هذه الرسالة:

```
Reason 412: The remote peer is no longer responding
```

لضمان إنشاء نفق VPN بشكل صحيح بين العميل والخادم، يمكنك العثور على أيقونة قفل يتم إنشاؤها بجوار عميل شبكة VPN الذي تم إنشاؤه. يشير شريط الحالة أيضا **إلى أنه متصل ب "VPN"**. فيما يلي مثال.



أيضا، ضمنت أن أنت يستطيع أن يبث بنجاح معطيات إلى ال LAN قطعة في النادل جانب من ال VPN زبون والعكس صحيح. من القائمة الرئيسية لعميل شبكة VPN، أختر **الحالة > الإحصائيات**. هناك يمكنك العثور على إحصائيات الحزم المشفرة وغير المشفرة التي يتم تمريرها عبر النفق.



في لقطة الشاشة هذه، يمكنك رؤية عنوان العميل على أنه 10.0.0.57. هذا هو العنوان الذي يقوم خادم شبكة VPN بتعيينه للعميل من التجمع الذي تم تكوينه محليا بعد تفاوض المرحلة 1 الناجح. وبمجرد إنشاء النفق، يقوم خادم VPN تلقائيا بإضافة مسار إلى عنوان IP المعين ل DHCP هذا في جدول التوجيه الخاص به.

كما يمكنك رؤية عدد الحزم المشفرة تتزايد أثناء نقل البيانات من العميل إلى الخادم وعدد الحزم التي تم فك تشفيرها يتزايد أثناء نقل بيانات عكسي.

ملاحظة: نظرا لتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتمرير الشبكة الخاصة الظاهرية (VPN)، فإنه يسمح للعميل بالوصول فقط إلى المقطع المتصل ببوابة الشبكة الخاصة الظاهرية (هنا، يتم تكوين خادم VPN 192.168.1.11) للتمرير. يقوم هذا بتصفية كل حركة المرور الأخرى.

يمكنك التحقق من هذا الإجراء من خلال تكوين خادم VPN آخر بنفس التكوين وتكوين إدخال اتصال جديد لخادم VPN هذا في عميل VPN. الآن، عندما تحاول إنشاء نفق مع خادم VPN هذا، فهذا الخادم غير ناجح. وذلك لأن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يقوم بتصفية حركة المرور هذه ويسمح بنفق فقط لعنوان عبارة شبكة VPN الذي تم تكوينه للتمرير من خلال شبكة VPN.

أنت يستطيع أيضا دققت التشكيل من ال CLI من ال VPN نادل.

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

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

هذا عرض أمر يستعمل في ال VPN نادل قد يكون أيضا مفيد أن يساعد أنت دققت النفق وضع.

- يتم إستخدام الأمر **show crypto session** للتحقق من حالة النفق. هنا مثال إنتاج من هذا أمر.

```
Crypto session current status

Interface: Serial3/0
Session status: UP-ACTIVE
Peer: 172.16.1.20 port 500
IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58
Active SAs: 2, origin: dynamic crypto map
```

- يتم إستخدام **نهج show crypto isakmp** لعرض معلمات المرحلة 1 التي تم تكوينها.

استكشاف الأخطاء وإصلاحها

كما يمكن إستخدام أوامر **debug** و**show** الموضحة في قسم التحقق من الصحة لاستكشاف الأخطاء وإصلاحها.

- **debug crypto isakmp**
- **debug crypto ipSec**
- **عرض جلسة التشفير**

- يعرض الأمر **debug crypto isakmp** في خادم VPN عملية التفاوض للمرحلة الأولى بالكامل بين العميل والخادم. فيما يلي مثال على مفاوضات المرحلة الأولى الناجحة.

```
-------------------------------------------------------------------
        -------------------------------------------------------------
                -------------------------------------------------------------
Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14*
                                                  against priority 1 policy
                                Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC*
                                        Aug 28 10:37:29.515: ISAKMP:      hash MD5*
                                    Aug 28 10:37:29.515: ISAKMP:      default group 2*
                                     Aug 28 10:37:29.515: ISAKMP:      auth pre-share*
                                  Aug 28 10:37:29.515: ISAKMP:      life type in seconds*
    Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B*
Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0*
                                                                      Aug 28*
                    :Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA authentication status*
                                                                  authenticated
                ,Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact*
                  bring down existing phase 1 and 2 SA's with local 192.168.1.11
                                                  remote 172.16.1.20 remote port 500
                    Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to*
                                                    the address pool: 10.0.0.57
Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool*
 Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA*
                  Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade*
                                                          to QM_IDLE 1583442981
                                Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY*
                                                      RESPONDER_LIFETIME protocol 1
                                              spi 1689265296, message ID = 1583442981
                                Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to*
                                      my_port 500 peer_port 500 (R) QM_IDLE 172.16.1.20
                                Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981*
                              Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400*
```

```
Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH*
Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2*
                     New State = IKE_P1_COMPLETE
```

- يعرض الأمر debug crypto ipSec الموجود على خادم VPN تفاوض IPsec للمرحلة 1 بنجاح وإنشاء نفق VPN. فيما يلي مثال:

```
------------------------------------------------------------------------
  ------------------------------------------------------------------
------------------------------------------------------------------------
Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages*
Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA*
                                from 192.168.1.11 to 172.16.1.20 for prot 3
Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages*
                                , :(Aug 28 10:40:04.279: IPSEC(initialize_sas*
          ,key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20)
                                ,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                             ,(remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1
                  ,(protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel
                                             ,lifedur= 2147483s and 0kb
               spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
                                , :(Aug 28 10:40:04.279: IPSEC(initialize_sas*
         ,key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20)
                                ,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                             ,(remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1
                  ,(protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel
                                             ,lifedur= 2147483s and 0kb
               spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for*
                                     peer or rekeying for peer 172.16.1.20
Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0*
Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added*
via 172.16.1.20 in IP DEFAULT TABLE with tag 0 255.255.255.255 10.0.0.58
Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F*
,Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58*
                                                  dest_port 0

                                ,Aug 28 10:40:04.287: IPSEC(create_sa): sa created*
                                        ,sa) sa_dest= 192.168.1.11, sa_proto= 50)
                                             ,(sa_spi= 0x8538A817(2235082775
                           sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
Aug 28 10:40:04.287: IPSEC(create_sa): sa created*,
                                     ,sa) sa_dest= 172.16.1.20, sa_proto= 50)
                                             ,(sa_spi= 0xFFC80936(4291299638
                           sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

معلومات ذات صلة

- مقدمة لتشفير أمان IP (IPsec)
- مفاوضة IPsec/صفحة دعم بروتوكول IKE
- تكوين أمان شبكة IPsec
- Cisco Easy VPN Q&A
- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 4.0 من Cisco
- مثال على تكوين ACL على وحدة تحكّم الشبكة المحلية اللاسلكية
- الأسئلة المتداولة حول وحدة التحكّم في الشبكة المحلية اللاسلكية (WLC)
- صفحة الدعم اللاسلكي
- 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).