عميل الموجه والشبكة الخاصة الظاهرية (VPN) للإنترنت العام على مثال تكوين العصا

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد موجه موقع مركزي لتنفيذ حركة مرور IPsec على عصا. ينطبق هذا الإعداد على حالة خاصة حيث يمكن للموجه، دون تمكين الاتصال النفقي المنقسم، وللمستخدمين كثيري التنقل (عميل شبكة VPN من Cisco) الوصول إلى الإنترنت عبر موجه الموقع المركزي. لتحقيق ذلك، قم بتكوين خريطة السياسة في الموجه لتوجيه جميع حركة مرور بيانات VPN (عميل Cisco VPN) إلى واجهة إسترجاع. هذا يسمح الإنترنت حركة مرور أن يكون أيسر عنوان يترجم (PATed) إلى العالم الخارجي.

ارجع إلى PIX/ASA 7.x و VPN Client for Public Internet VPN على مثال تكوين Stick لإكمال تكوين مماثل على جدار حماية PIX المركزي للموقع.

ملاحظة: لتجنب تداخل عناوين IP في الشبكة، قم بتعيين تجمع عناوين IP مختلف تماما إلى عميل VPN (على سبيل المثال، 192.168.x.x.10، 172.16.x.x، x.x.x). يساعدك مخطط عنونة IP هذا على أستكشاف أخطاء الشبكة وإصلاحها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- cisco مسحاج تخديد 3640 مع cisco ios ® برمجية إطلاق 12.4
- Cisco VPN Client 4.8

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.

الاصطلاحات

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

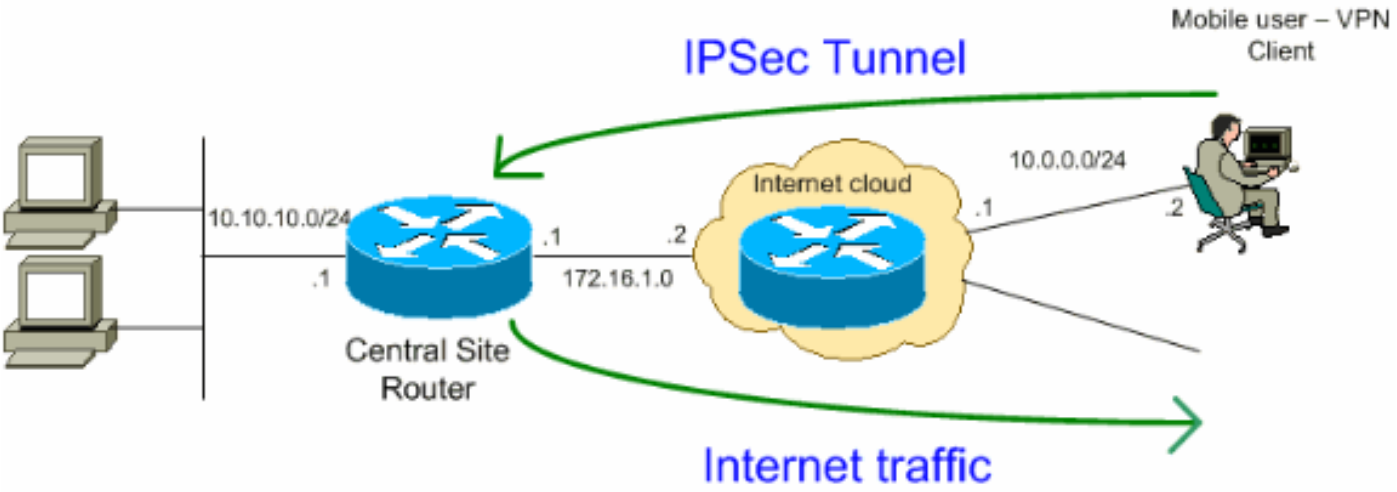
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- الموجّه
- عميل شبكة VPN من Cisco

الموجّه

```
VPN#show run
...Building configuration

Current configuration : 2170 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
!
boot-start-marker
boot-end-marker
!
!
Enable authentication, authorization and accounting ---!
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
In order to enable Xauth for user authentication, ---!
.!--- enable the aaa authentication commands


aaa authentication login userauthen local

In order to enable group authorization, enable !--- ---!
.the aaa authorization commands

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
For local authentication of the IPsec user, !--- ---!
create the user with a password. username user password
0 cisco
!
!
!
Create an Internet Security Association and !--- ---!
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2

Create a group that is used to specify the !--- ---!
WINS and DNS server addresses to the VPN Client, !---
along with the pre-shared key for authentication. crypto
isakmp client configuration group vpnclient
key cisco123
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
!
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 earlier. crypto dynamic-map dynmap
                                                            10
                                          set transform-set myset
                                                   reverse-route
                                                               !

  Create the actual crypto map, !--- and apply the ---!
       AAA lists that were created earlier. crypto map
       clientmap client authentication list userauthen
        crypto map clientmap isakmp authorization list
                                                    groupauthor
     crypto map clientmap client configuration address
                                                         respond
   crypto map clientmap 10 ipsec-isakmp dynamic dynmap
                                                               !
                                                               !
                                                               !
                                                               !
    Create the loopback interface for the VPN user ---!
                                traffic . interface Loopback0
                        ip address 10.11.0.1 255.255.255.0
                                                 ip nat inside
                                       ip virtual-reassembly
                                                               !
                                                interface Ethernet0/0
                                    ip address 10.10.10.1 255.255.255.0
                                                      half-duplex
                                                   ip nat inside

  Apply the crypto map on the interface. interface ---!
                                                  FastEthernet1/0
                        ip address 172.16.1.1 255.255.255.0
                                                 ip nat outside
                                       ip virtual-reassembly
                            ip policy route-map VPN-Client
                                                    duplex auto
                                                     speed auto
                                          crypto map clientmap
                                                               !
                                                  interface Serial2/0
                                                       no ip address
                                                               !
                                                  interface Serial2/1
                                                       no ip address
                                                            shutdown
                                                               !
                                                  interface Serial2/2
                                                       no ip address
                                                            shutdown
                                                               !
                                                  interface Serial2/3
                                                       no ip address
                                                            shutdown
 Create a pool of addresses to be !--- assigned to ---!
    the VPN Clients. ! ip local pool ippool 192.168.1.1
                                                      192.168.1.2
                                                   ip http server
                                          no ip http secure-server
                                                               !
                                ip route 10.0.0.0 255.255.255.0 172.16.1.2
```

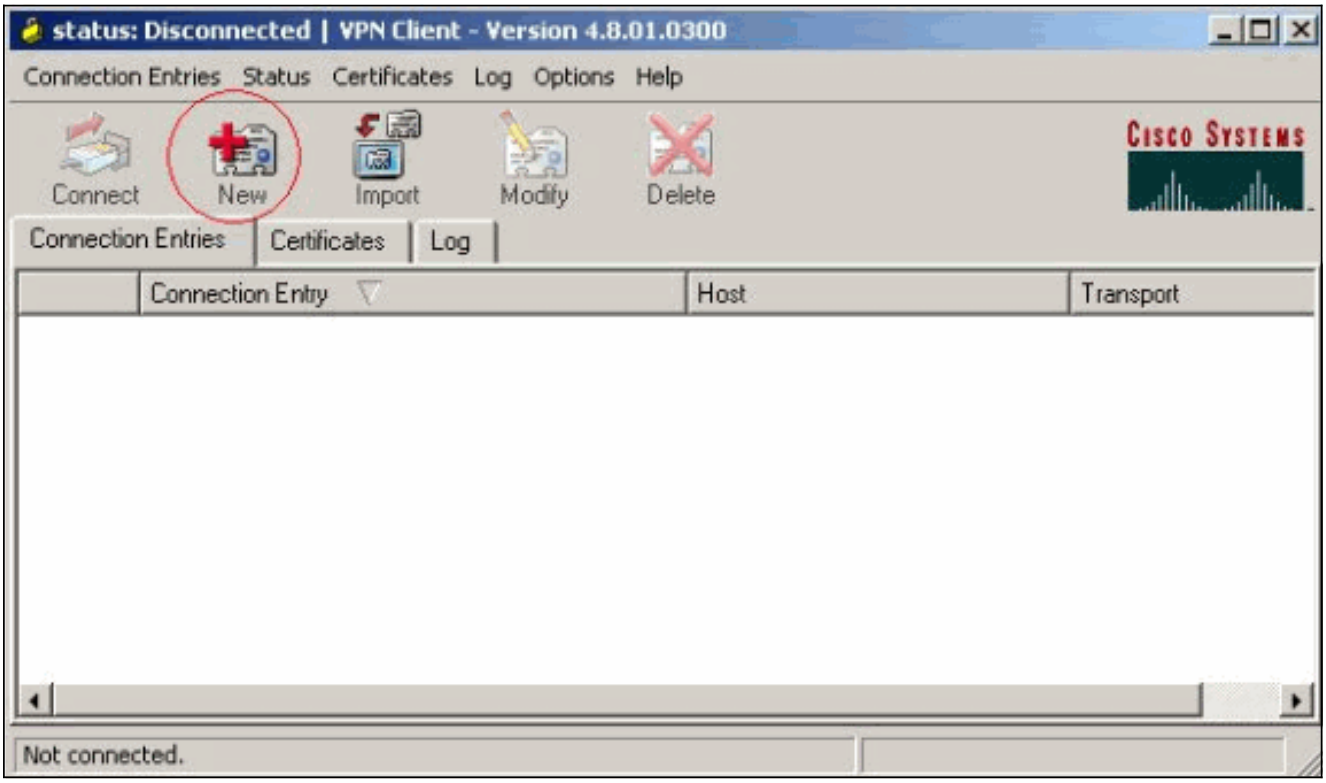
```
 Enables Network Address Translation (NAT) !--- of ---!
  the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address. ip
    nat inside source list 101 interface FastEthernet1/0
                                                  overload
                                                         !
The access list is used to specify which traffic is ---!
 to be translated for the !--- outside Internet. access-
                                  list 101 permit ip any any

 Interesting traffic used for policy route. access- ---!
            list 144 permit ip 192.168.1.0 0.0.0.255 any
  Configures the route map to match the interesting ---!
traffic (access list 144) !--- and routes the traffic to
      next hop address 10.11.0.2. ! route-map VPN-Client
                                                permit 10
                                     match ip address 144
                                  set ip next-hop 10.11.0.2
                                                         !
                                                         !
                                               control-plane
                                                         !
                                                 line con 0
                                                 line aux 0
                                                line vty 0 4
                                                         !
                                                       end
```

تكوين VPN Client 4.8

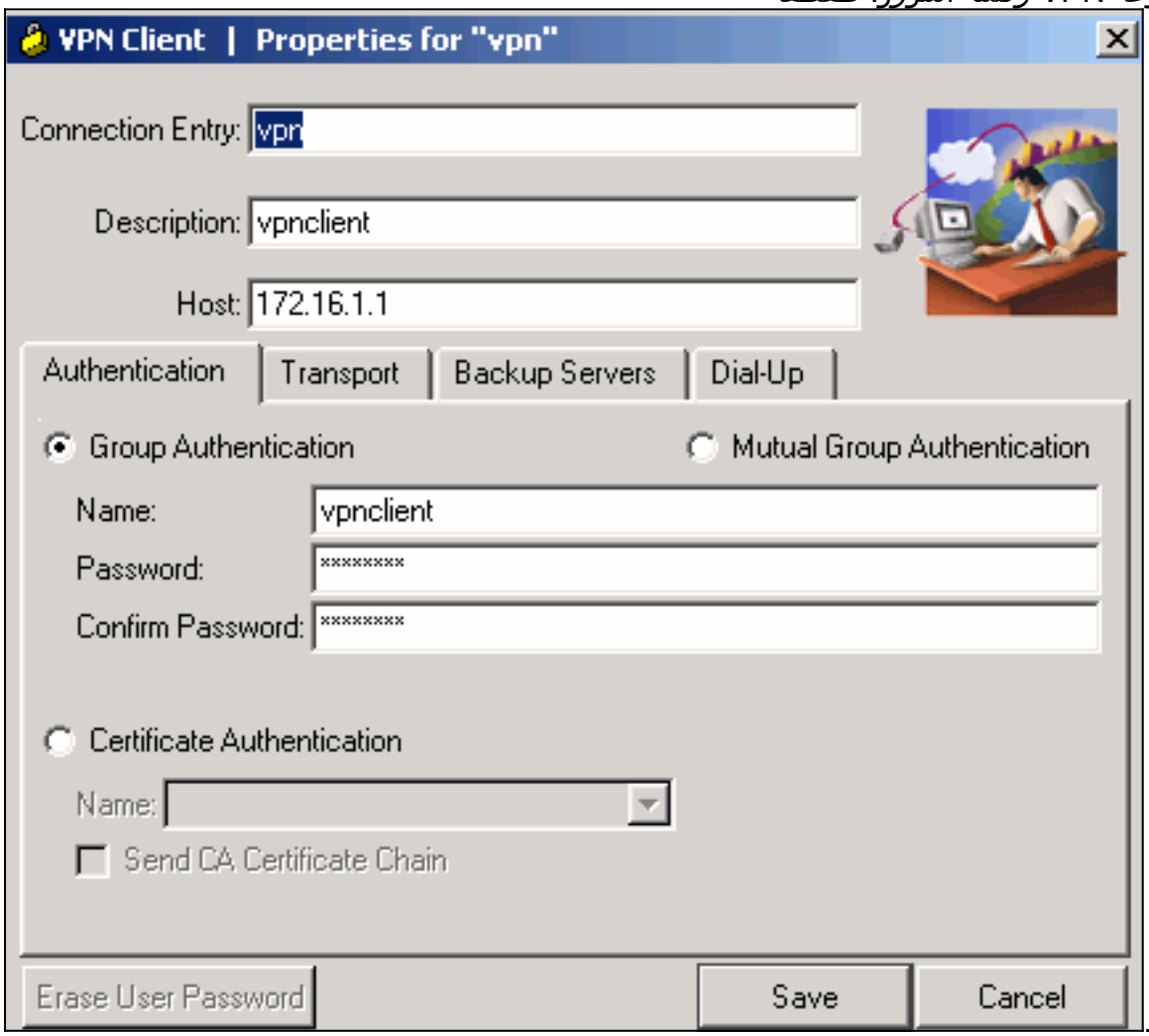
أتمت هذا steps in order to شكلت ال VPN زبون 4.8.

1. أخترت **بداية>برنامج>VPN Cisco Systems زبون>VPN زبون**.
2. طقطقت **جديد** in order to أطلقت ال create جديد VPN توصيل مدخل نافذة.



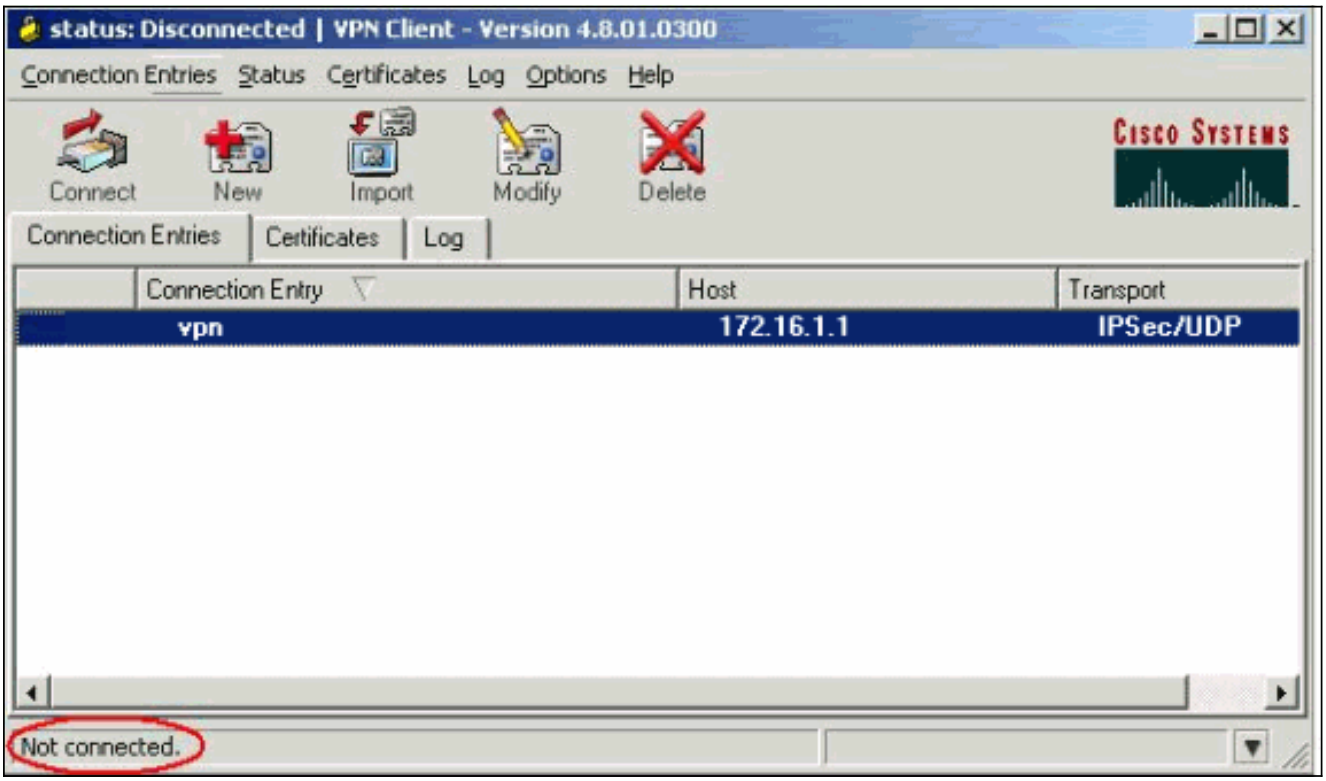
3. أدخل اسم إدخال الاتصال مع وصف ما، وأدخل عنوان IP الخارجي للموجه في المربع المضيف، وأدخل اسم

مجموعة VPN وكلمة المرور. طقطقة



حفظ.

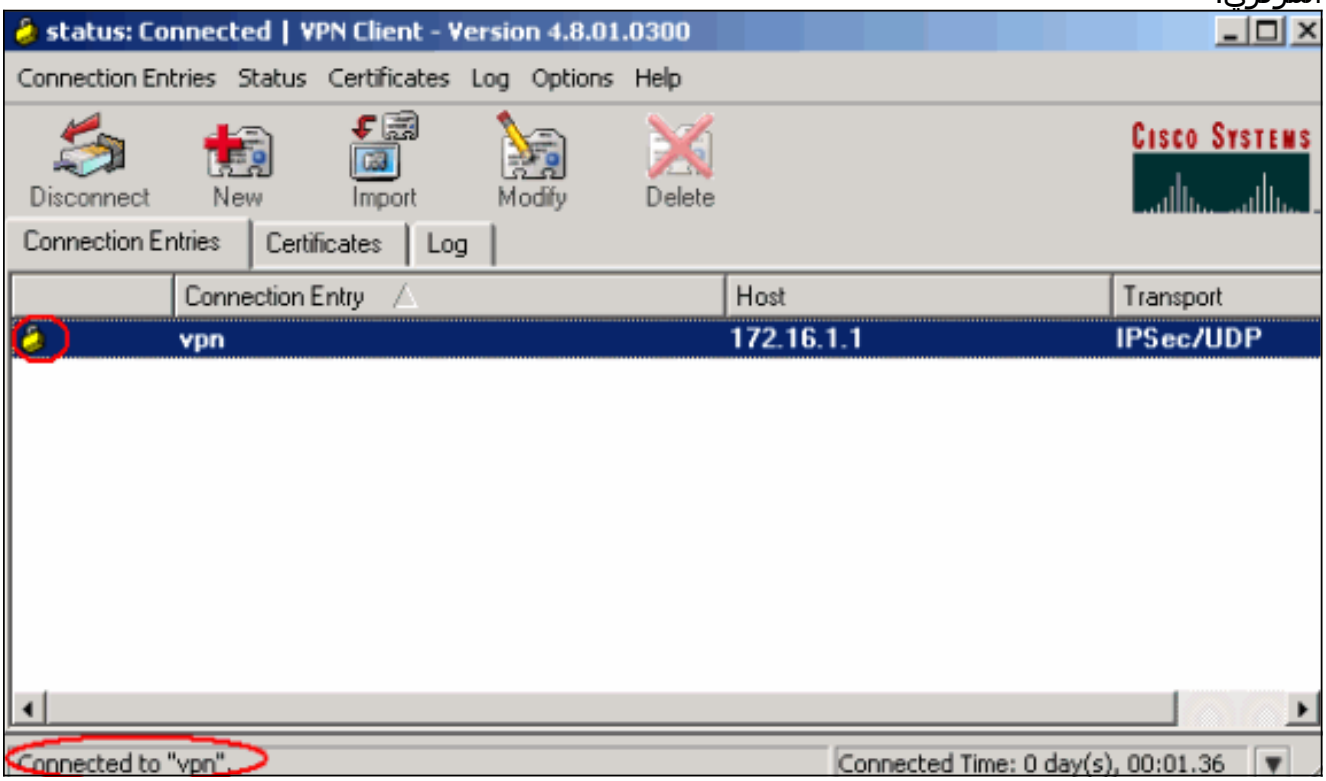
4. انقر على الاتصال الذي تريد إستخدامه وانقر فوق **الاتصال** من الإطار الرئيسي لعميل شبكة VPN.



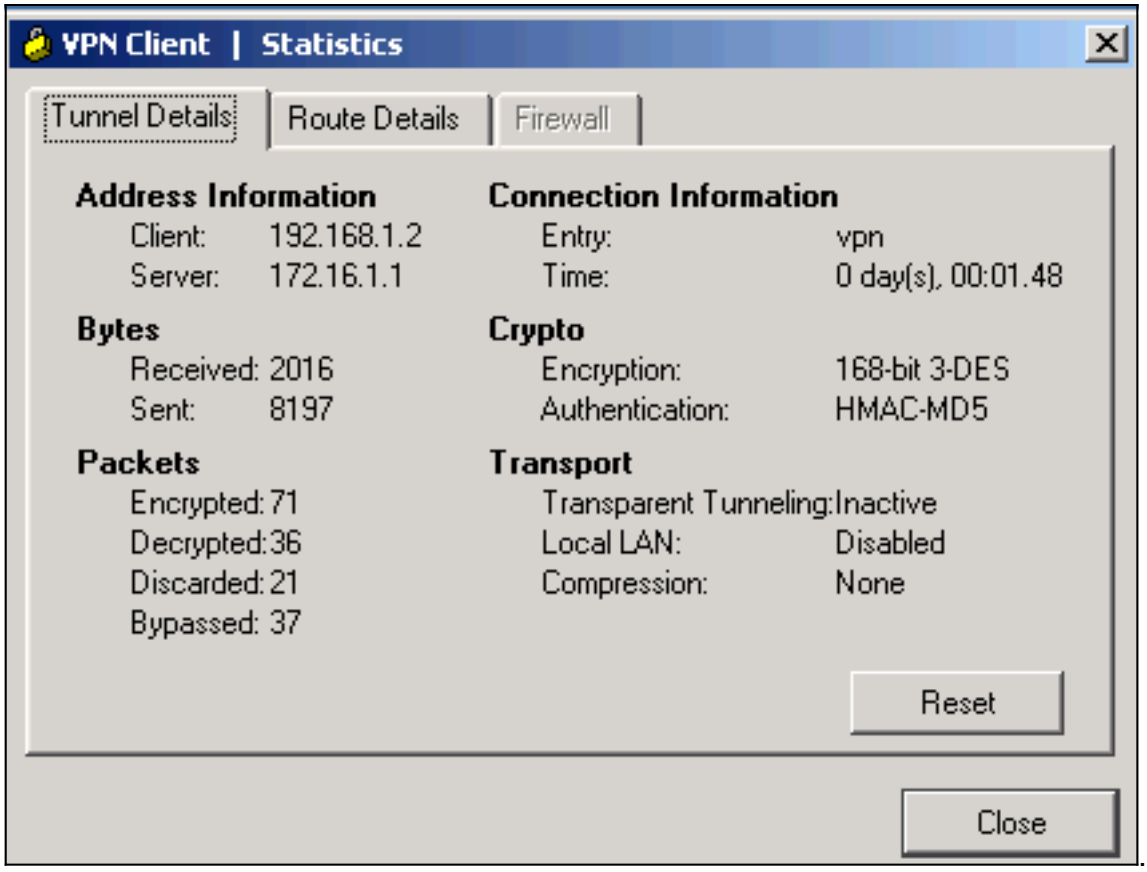
5. دخلت عندما طلب، ال username وكلمة معلومة ل Xauth وطقطقة to order in **ok** ربطت إلى الشبكة

بعيد.

6. يتم اتصال عميل شبكة VPN بالموجه في الموقع المركزي.



7. أخترت **وضع>إحصاء** in order to فحصت النفق إحصائيات من ال VPN



زبون.

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

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

- **show crypto isakmp sa**— يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.

```
VPN#show crypto ipsec sa

                                 interface: FastEthernet1/0
                       Crypto map tag: clientmap, local addr 172.16.1.1

                                   (protected vrf: (none
                  (local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
    (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0
                                 current_peer 10.0.0.2 port 500
                                       {}=PERMIT, flags
                  pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270#
                  pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270#
                               pkts compressed: 0, #pkts decompressed: 0#
                          pkts not compressed: 0, #pkts compr. failed: 0#
                    pkts not decompressed: 0, #pkts decompress failed: 0#
                                    send errors 0, #recv errors 0#

              local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
                        path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
                           (current outbound spi: 0xEF7C20EA(4017889514

                                                 :inbound esp sas
                                        (spi: 0x17E0CBEC(400608236
                                , transform: esp-3des esp-md5-hmac
                                       { ,in use settings ={Tunnel
```

```
     conn id: 2001, flow_id: SW:1, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4530341/3288
                                          IV size: 8 bytes
                                 replay detection support: Y
                                             Status: ACTIVE

                                               :inbound ah sas

                                              :inbound pcp sas

                                             :outbound esp sas
                                   (spi: 0xEF7C20EA(4017889514
                          , transform: esp-3des esp-md5-hmac
                                  { ,in use settings ={Tunnel
     conn id: 2002, flow_id: SW:2, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4530354/3287
                                          IV size: 8 bytes
                                 replay detection support: Y
                                             Status: ACTIVE

                                              :outbound ah sas

                                             :outbound pcp sas
```

- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل SAs الحالية.

```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
QM_IDLE              15    0 ACTIVE       10.0.0.2      172.16.1.1
```

استكشاف الأخطاء وإصلاحها

أوامر استكشاف الأخطاء وإصلاحها

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**.

- **debug crypto ipSec**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- عميل شبكة VPN من Cisco - دعم المنتج
- الموجه من Cisco - دعم المنتج
- 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).