نفق IPsec الديناميكي بين ASA الذي تم توجيهه بشكل ثابت وموجه Cisco IOS الذي تم توجيهه ديناميكيا والذي يستخدم مثال تكوين CCP

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين كيفية تمكين جهاز أمان PIX/ASA لقبول إتصالات IPsec الديناميكية من موجه Cisco IOS®. في هذا السيناريو، يحدد نفق IPsec متى يتم بدء النفق من نهاية الموجه فقط. تعذر على ASA بدء نفق VPN بسبب تكوين IPsec الديناميكي.

يتيح هذا التكوين جهاز أمان PIX إنشاء نفق ديناميكي من شبكة LAN إلى شبكة LAN (L2L) باستخدام موجه VPN عن بعد. يستقبل هذا الموجه بشكل ديناميكي عنوان IP العام الخارجي من موفر خدمة الإنترنت الخاص به. يوفر بروتوكول تكوين المضيف الديناميكي (DHCP) هذه الآلية من أجل تخصيص عناوين IP بشكل ديناميكي من الموفر. وهذا يسمح بإعادة إستخدام عناوين IP عندما لا تعود البيئات المضيفة بحاجة إليها.

يتم إجراء التكوين على الموجه باستخدام محترف تكوين Cisco (CCP). CCP هو أداة إدارة أجهزة تستند إلى واجهة المستخدم الرسومية (GUI) تتيح لك تكوين الموجهات المستندة إلى Cisco IOS. أحلت أساسي مسحاج تخديد تشكيل يستعمل cisco تشكيل محترف ل كثير معلومة على كيف أن يشكل مسحاج تخديد مع CCP.

ارجع إلى الموقع إلى موقع (L2L VPN) مع ASA للحصول على مزيد من أمثلة المعلومات والتكوين على إنشاء نفق IPsec الذي يستخدم موجهات ASA و Cisco IOS.

ارجع إلى الموقع إلى موقع VPN (L2L) مع IOS للحصول على مزيد من المعلومات ومثال التكوين على إنشاء نفق IPSec الديناميكي باستخدام PIX وموجه Cisco IOS.

المتطلبات الأساسية

المتطلبات

قبل أن تحاول إجراء هذا التكوين، تأكد من أن كل من ASA والموجه لديه اتصال بالإنترنت لإنشاء نفق IPSec.

المكونات المستخدمة

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

- cisco ios مسحاج تخديد 1812 أن يركض cisco ios برمجية إطلاق 12.4
- برنامج Cisco ASA 5510 الإصدار 8.0.3

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.

معلومات أساسية

في هذا السيناريو، تقع شبكة 192.168.100.0 خلف موجه ASA وشبكة 192.168.200.0 خلف موجه Cisco IOS. يفترض أن الموجه يحصل على عنوانه العام من خلال DHCP من ISP الخاص به. بما أن هذا يشكل مشكلة في تكوين نظير ساكن إستاتيكي على نهاية ASA، فأنت بحاجة إلى الوصول إلى طريقة تكوين التشفير الديناميكي لإنشاء نفق من موقع إلى موقع بين ASA وموجه Cisco IOS.

ترجمة مستخدمي الإنترنت في نهاية ASA إلى عنوان IP الخاص بواجهة خارجية. يفترض أنه لم يتم تكوين NAT على نهاية موجه Cisco IOS.

والآن هذه هي الخطوات الأساسية التي سيتم تكوينها على نهاية ASA لإنشاء نفق ديناميكي:

1. التكوين المرتبط ب ISAKMP المرحلة 1
2. تكوين إعفاء nat
3. تكوين خريطة التشفير الديناميكية

يحتوي موجه Cisco IOS على خريطة تشفير ثابتة تم تكوينها لأنه يفترض أن يكون لموجه ASA عنوان IP عام ثابت. الآن، هذه هي قائمة الخطوات الرئيسية التي سيتم تكوينها على نهاية موجه Cisco IOS لإنشاء نفق IPsec الديناميكي.

1. التكوين المرتبط ب ISAKMP المرحلة 1
2. التكوين المرتبط بخريطة التشفير الثابتة

ويتم وصف هذه الخطوات بالتفصيل في هذه التكوينات.

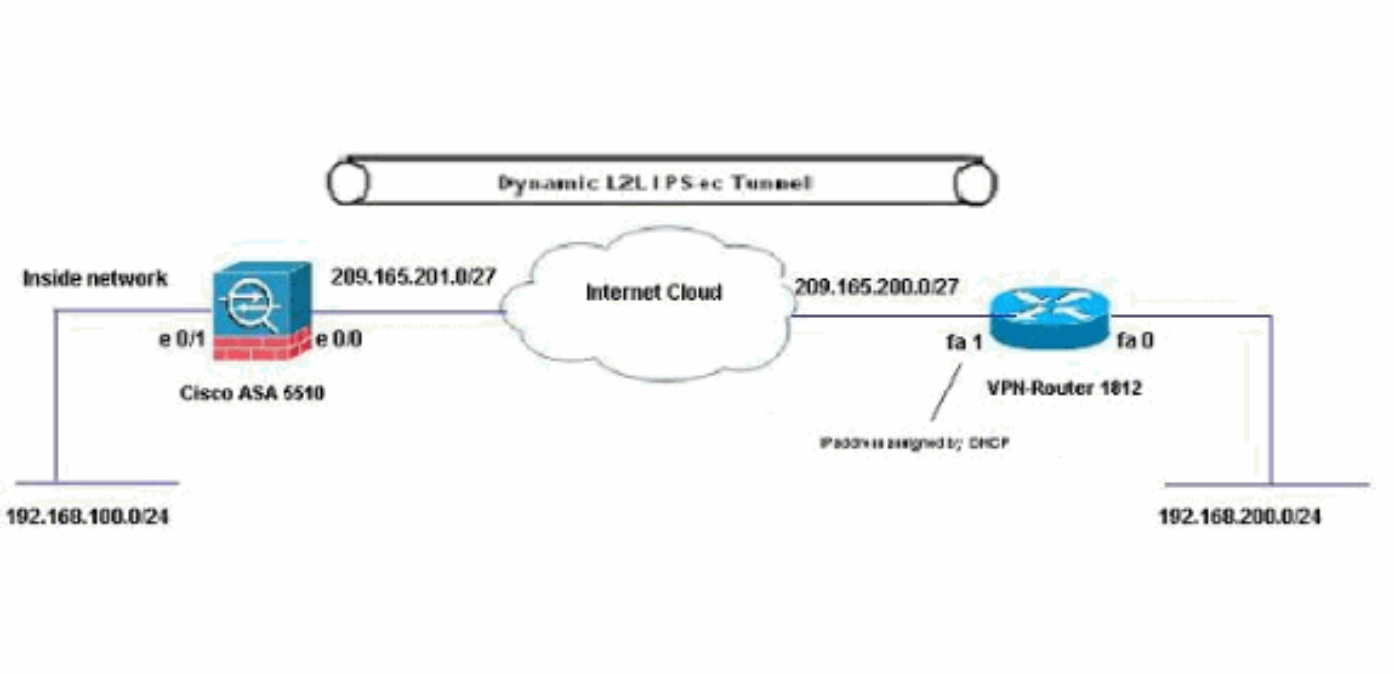
التكوين

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

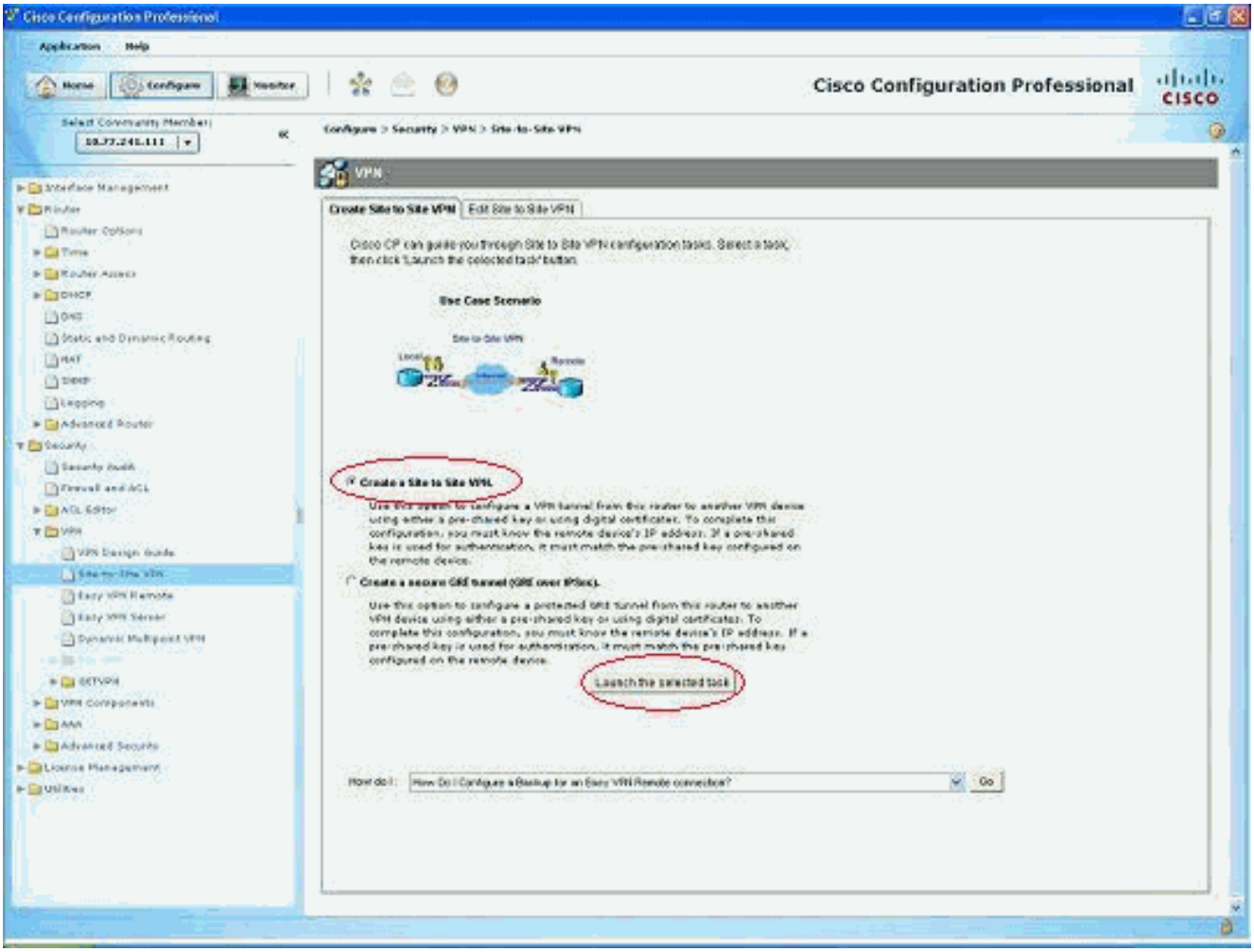
يستخدم هذا المستند إعداد الشبكة التالي:



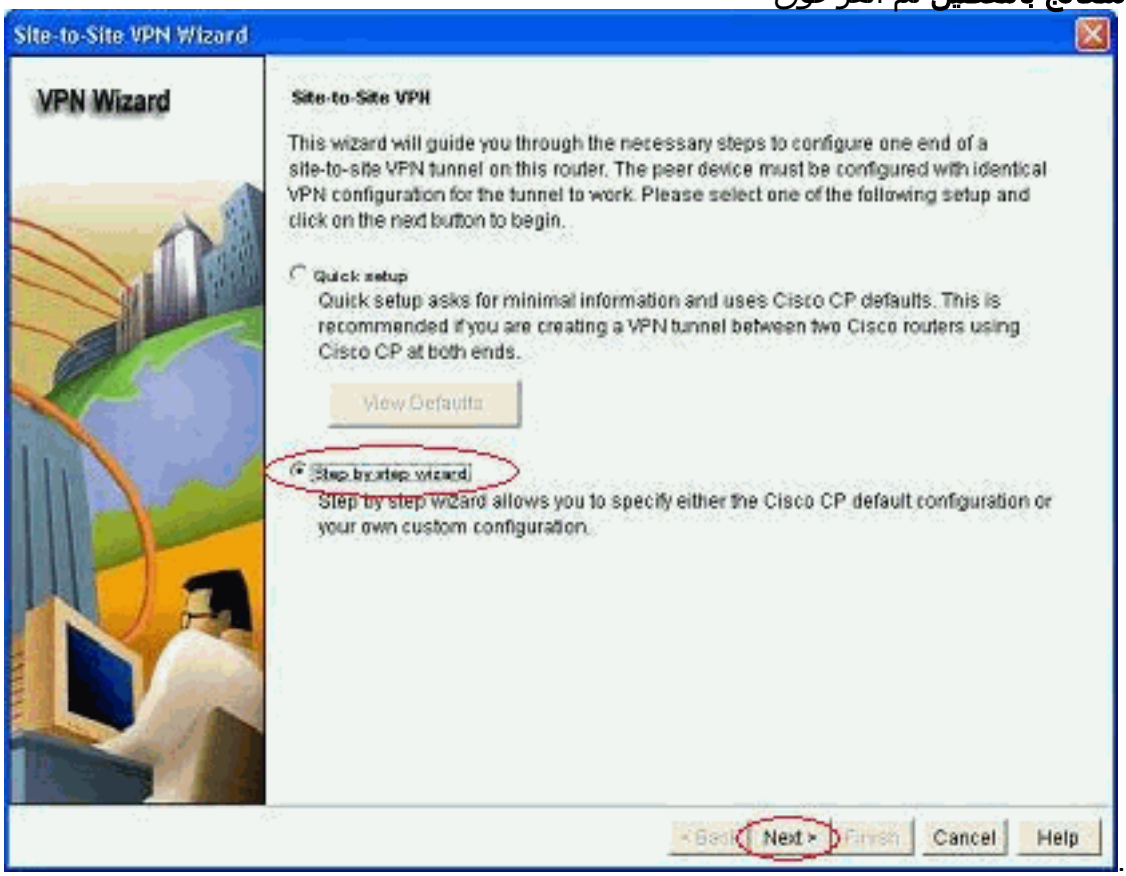
التكوينات

هذا هو تكوين VPN ل IPsec على موجه VPN مع CCP. أكمل الخطوات التالية:

1. افتح تطبيق CCP واخترت **يشكل>أمن>VPN>موقع إلى موقع VPN**. انقر فوق **تشغيل علامة التبويب المحددة**.

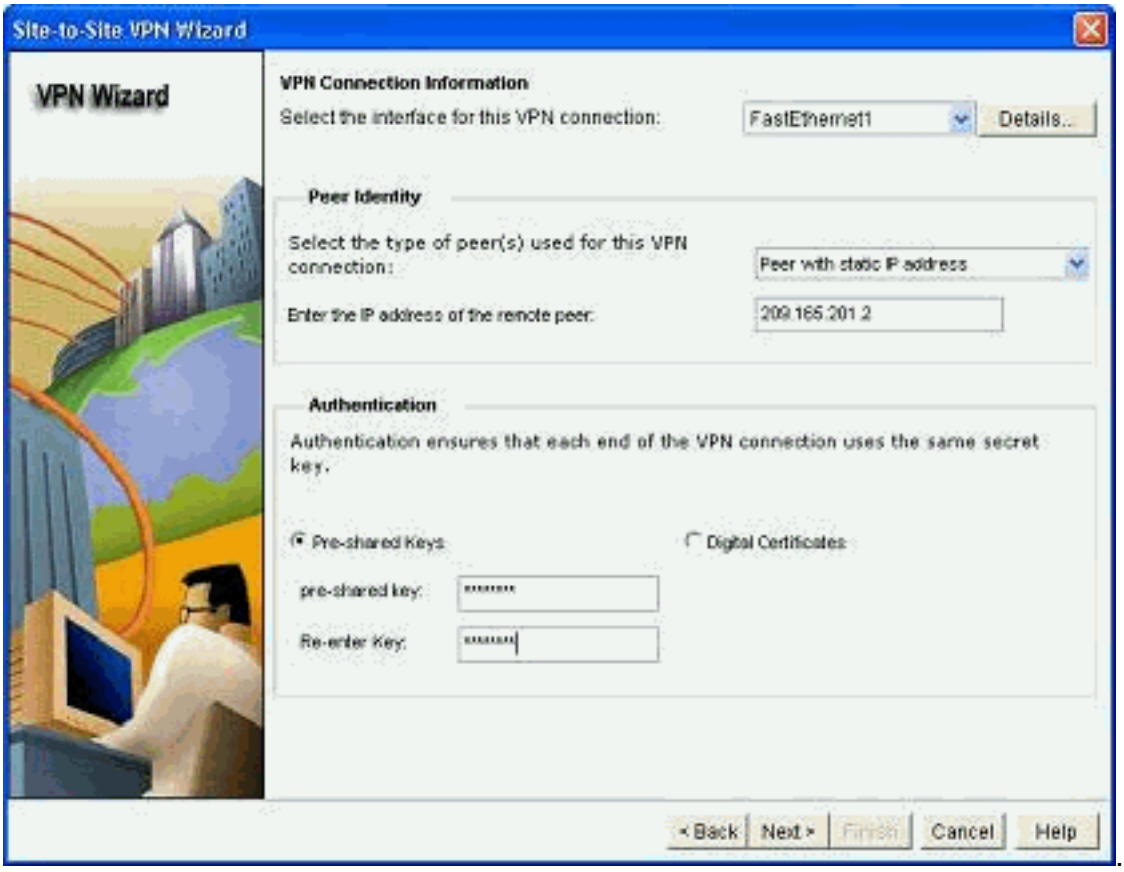


2. أختر **المعالج بالتفصيل** ثم انقر فوق



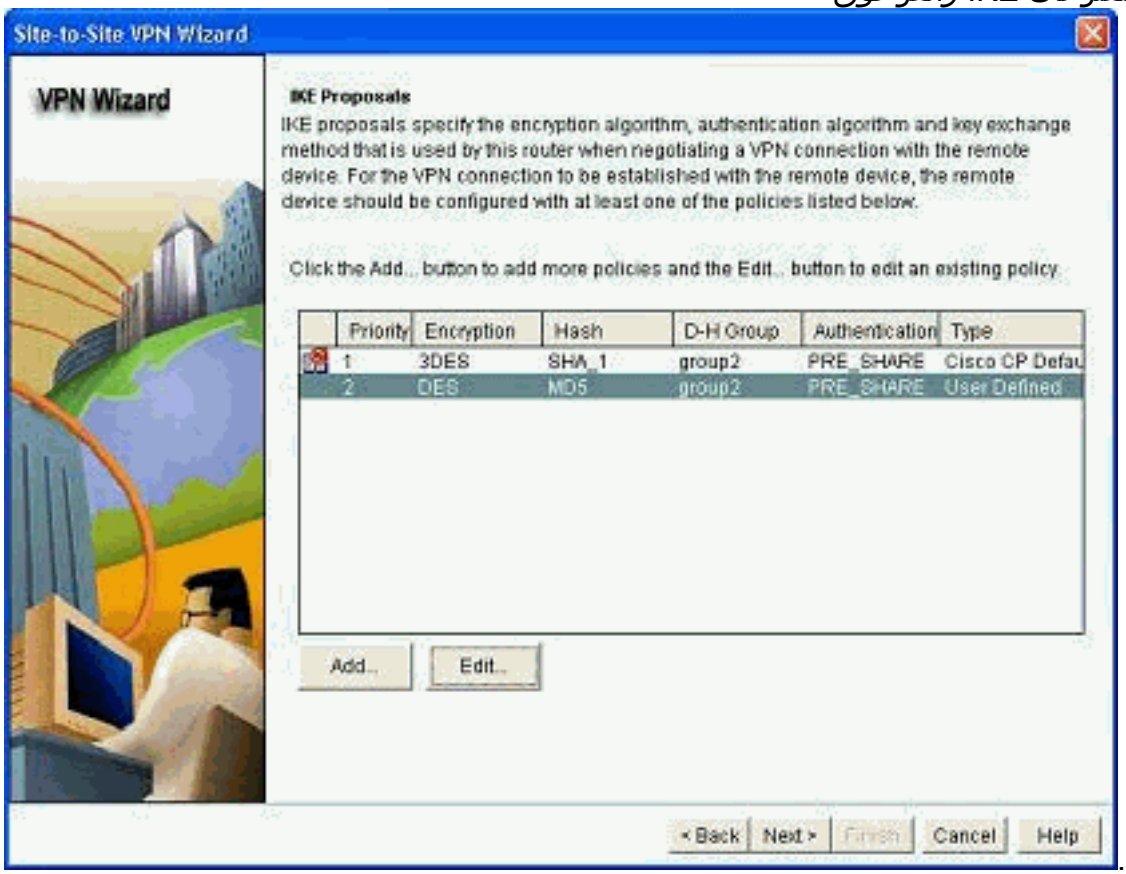
التالي.

3. املأ عنوان IP للنظير البعيد مع تفاصيل



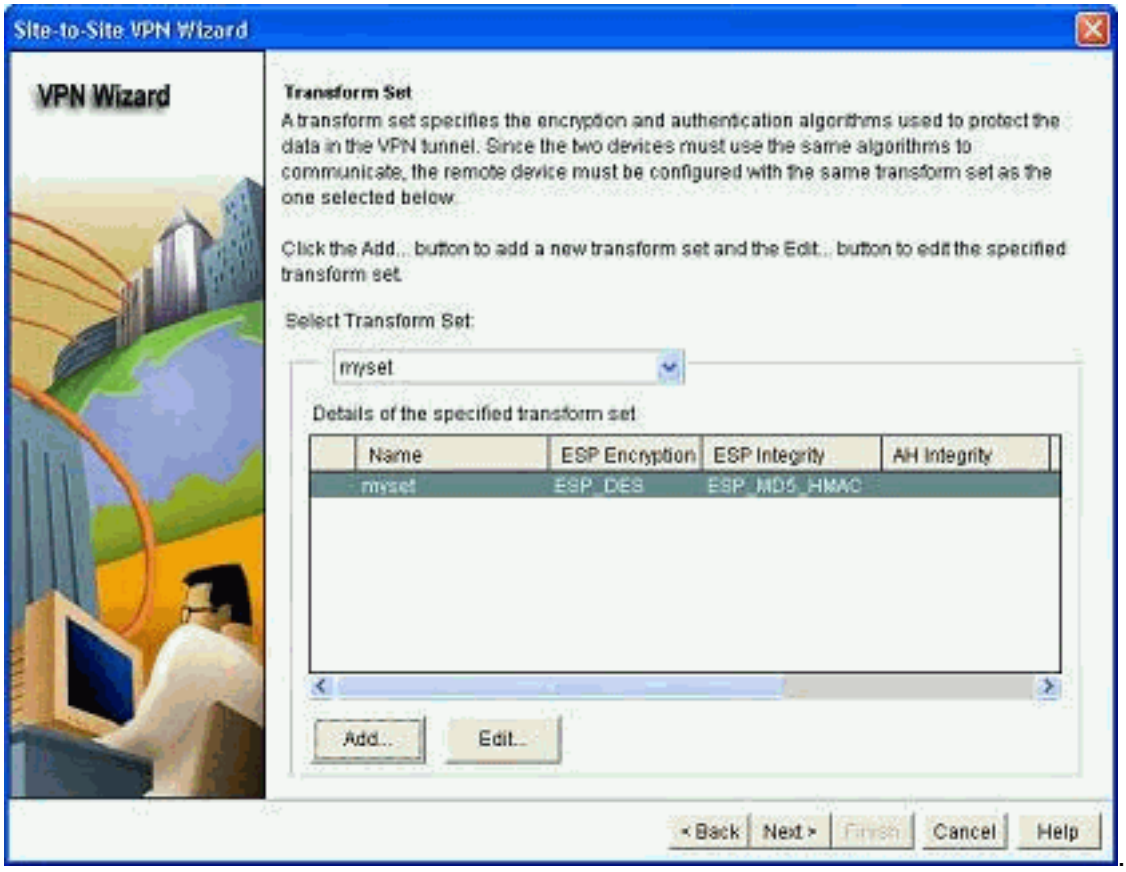
المصادقة.

4. أختر مقترحات IKE وانقر فوق



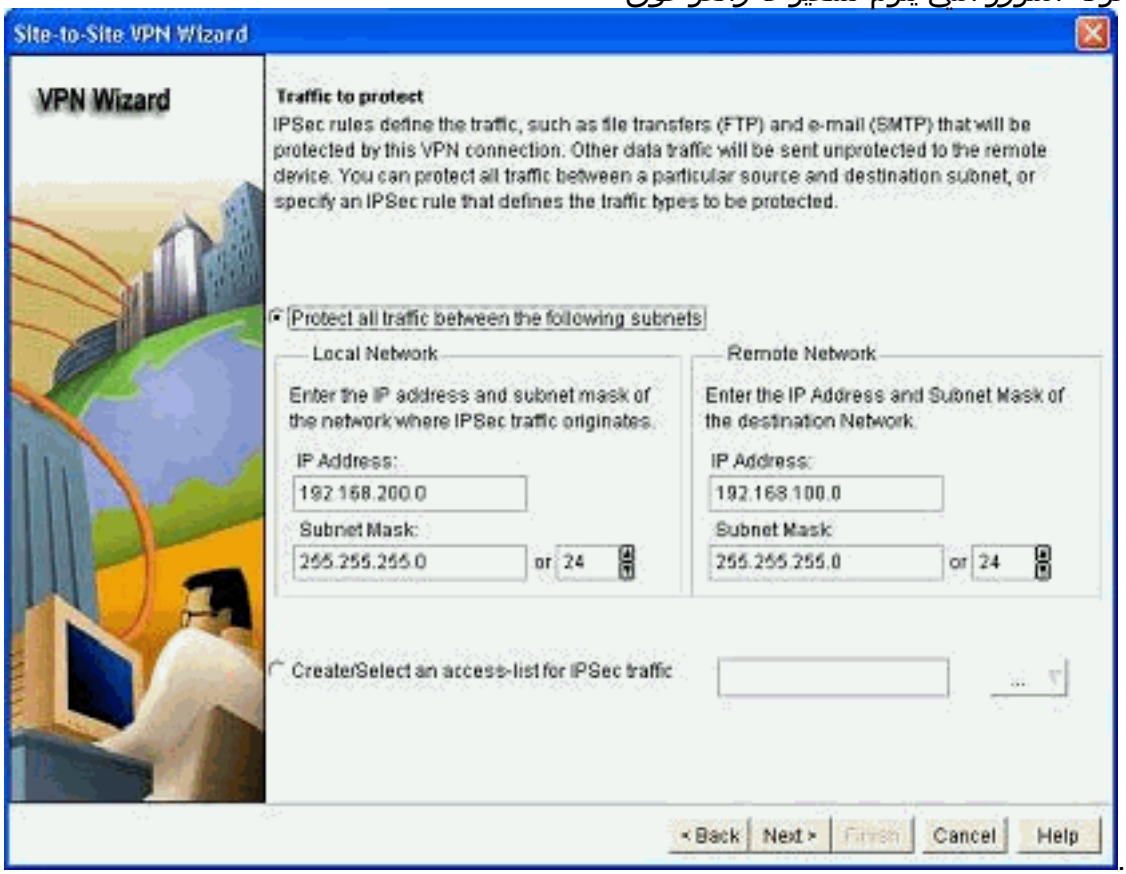
التالي.

5. حدد تفاصيل مجموعة التحويل وانقر



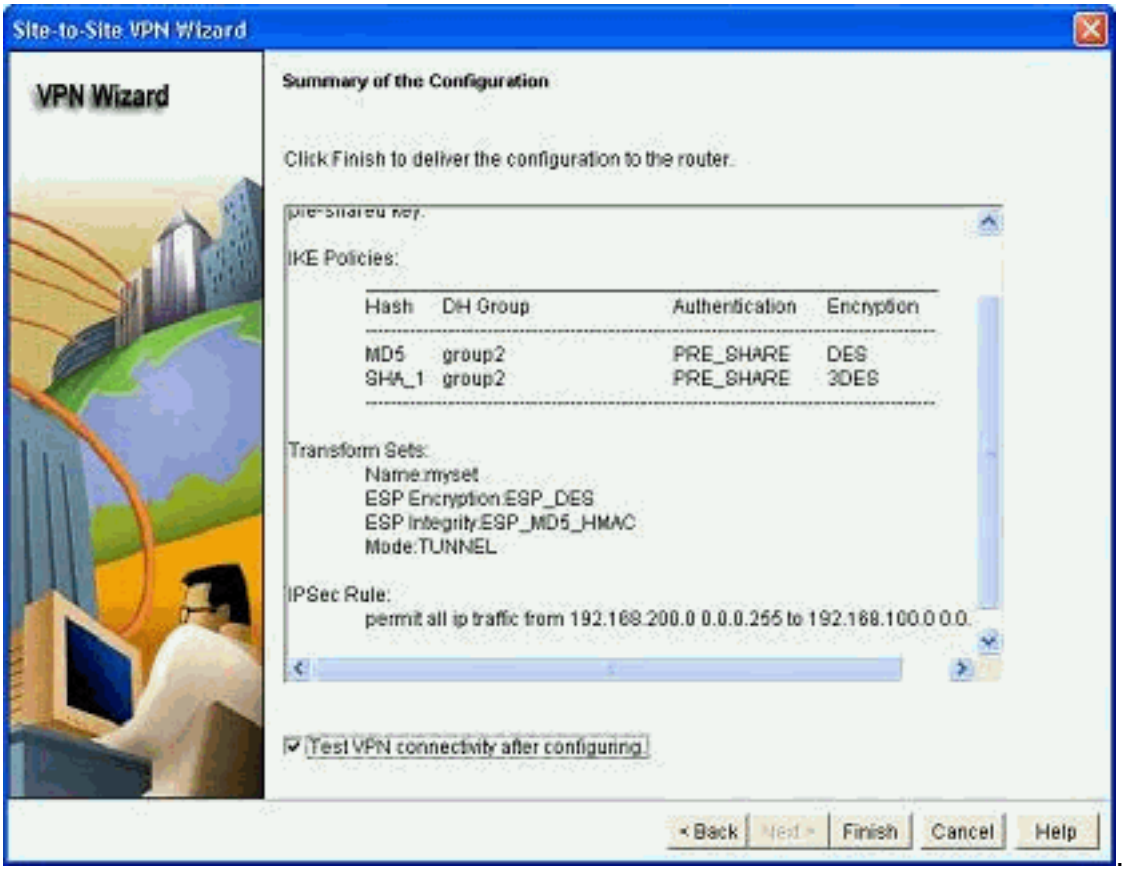
التالي.

6. حدد حركة المرور التي يلزم تشفيرها وانقر فوق



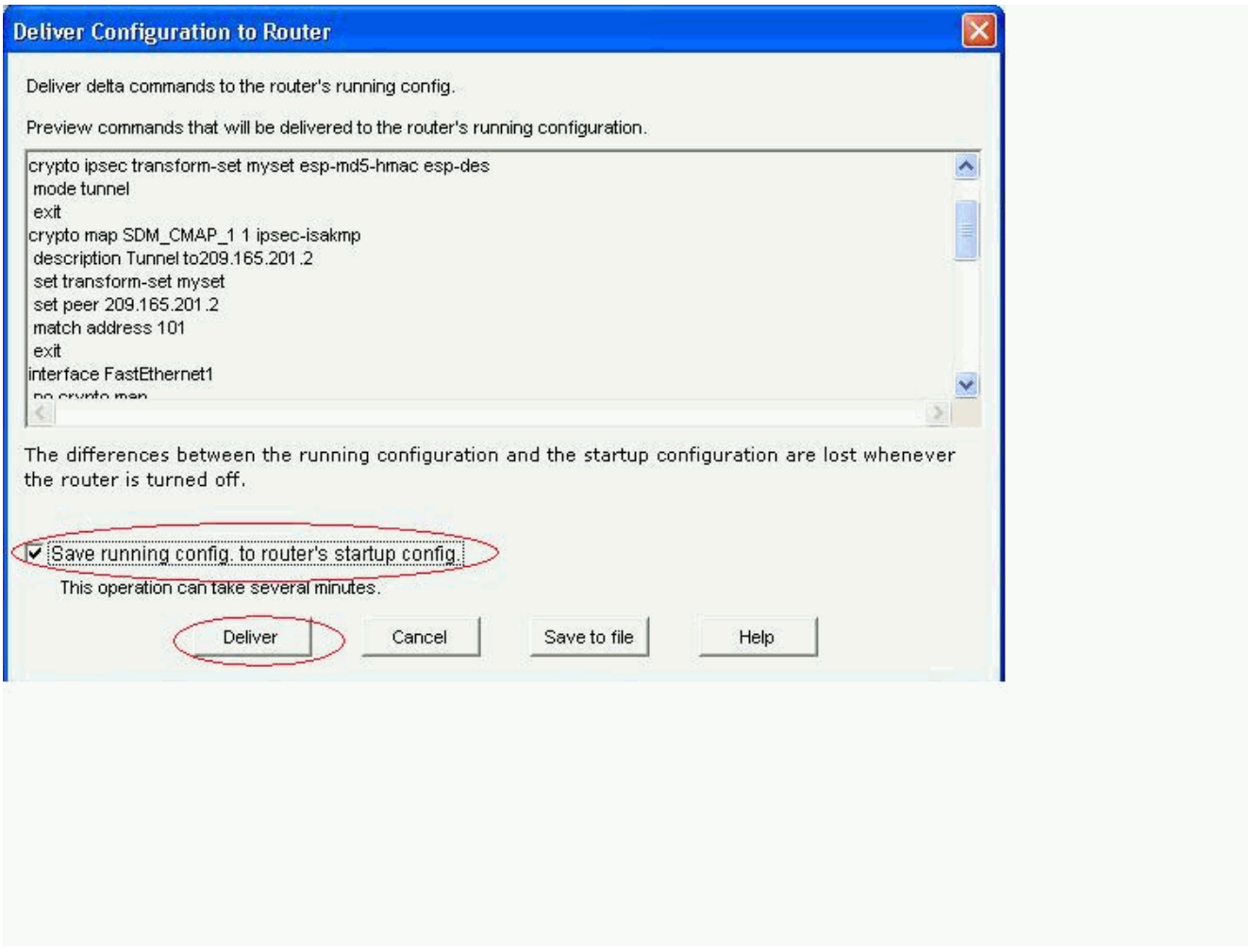
التالي.

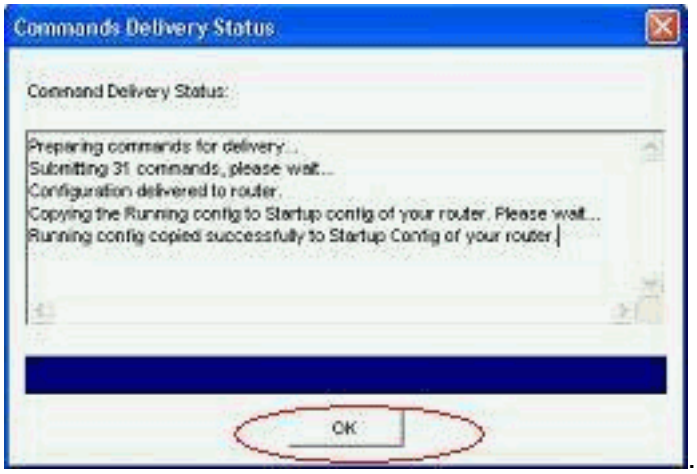
7. تحقق من ملخص تكوين IPsec للتشفير وانقر فوق



إنهاء.

8. طقطقة **يسلم** in order to أرسلت التشكيل إلى ال -VPN router.





9. وانقر فوق **OK**.

تكوين واجهة سطر الأوامر (CLI)

- سيسكوسا
- موجه VPN

سيسكوسا

```
ciscoasa(config)#show run
Saved :
:
(ASA Version 8.0(3
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
Output suppressed access-list nonat extended permit ---!
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0

no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
Define the nat-translation for Internet users ---!!
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!
Define the nat-exemption policy for VPN traffic ---!!
nat (inside) 0 access-list nonat
!
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
Configure the IPsec transform-set crypto ipsec ---!!
transform-set myset esp-des esp-md5-hmac
!
Configure the dynamic crypto map crypto dynamic- ---!!
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
Configure the phase I ISAKMP policy crypto isakmp ---!!
policy 10
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
!
Configure the default L2L tunnel group parameters ---!!
tunnel-group DefaultL2LGroup IPSec-attributes
* pre-shared-key
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
```

```
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
 !
service-policy global_policy global
 prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
 end :
#(ciscoasa(config
```

يخلق CCP هذا تشكيل على ال VPN-router.

موجه VPN

```
VPN-Router#show run
...Building configuration
!
 version 12.4
service timestamps debug datetime msec
 service timestamps log datetime msec
 no service password-encryption
!
hostname VPN-Router
!
!
 username cisco privilege 15 secret 5
 /$1$UQxM$WvwDZbfDhK3wS26C9xYns
 username test12 privilege 15 secret 5
 $1$LC0U$ex3tp4hM8CYD.HJSRDfQO1
!
Output suppressed no aaa new-model ip subnet-zero ---!!
 ! ip cef ! crypto isakmp enable outside
!
 crypto isakmp policy 1
 encrypt 3des
 authentication pre-share
 group 2
 !
 crypto isakmp policy 2
 hash md5
 authentication pre-share
 group 2
 !
!
crypto isakmp key cisco123 address 209.165.201.2
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
!
crypto map SDM_CMAP_1 1 IPSec-isakmp
 description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
                                        match address 101
                                                        !
                                                        !
                                                        !
                                                interface BRI0
                                                no ip address
                                                     shutdown
                                                        !
                                              interface Dot11Radio0
                                                      no ip address
                                                           shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
                                  12.0 18.0 24.0 36.0 48.0 54.0
                                             station-role root
                                                        !
                                              interface Dot11Radio1
                                                      no ip address
                                                           shutdown
    speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
                                                           48.0 54.0
                                             station-role root
                                                        !
                                           interface FastEthernet0
                    ip address 192.168.200.1 255.255.255.0
                                                 duplex auto
                                                  speed auto
                                                        !
                                           interface FastEthernet1
                                                  ip address dhcp
                                                 duplex auto
                                                  speed auto
                                           crypto map SDM_CMAP_1
                                                        !
                                           interface FastEthernet2
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet3
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet4
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet5
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet6
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet7
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet8
                                                    no ip address
                                                         shutdown
                                                        !
                                           interface FastEthernet9
                                                    no ip address
                                                         shutdown
```

```
!
interface Vlan1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!
Output suppressed ! ip http server ip http ---!!
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 login local
transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
transport input telnet ssh
!
no scheduler allocate
end
```

التحقق من الصحة

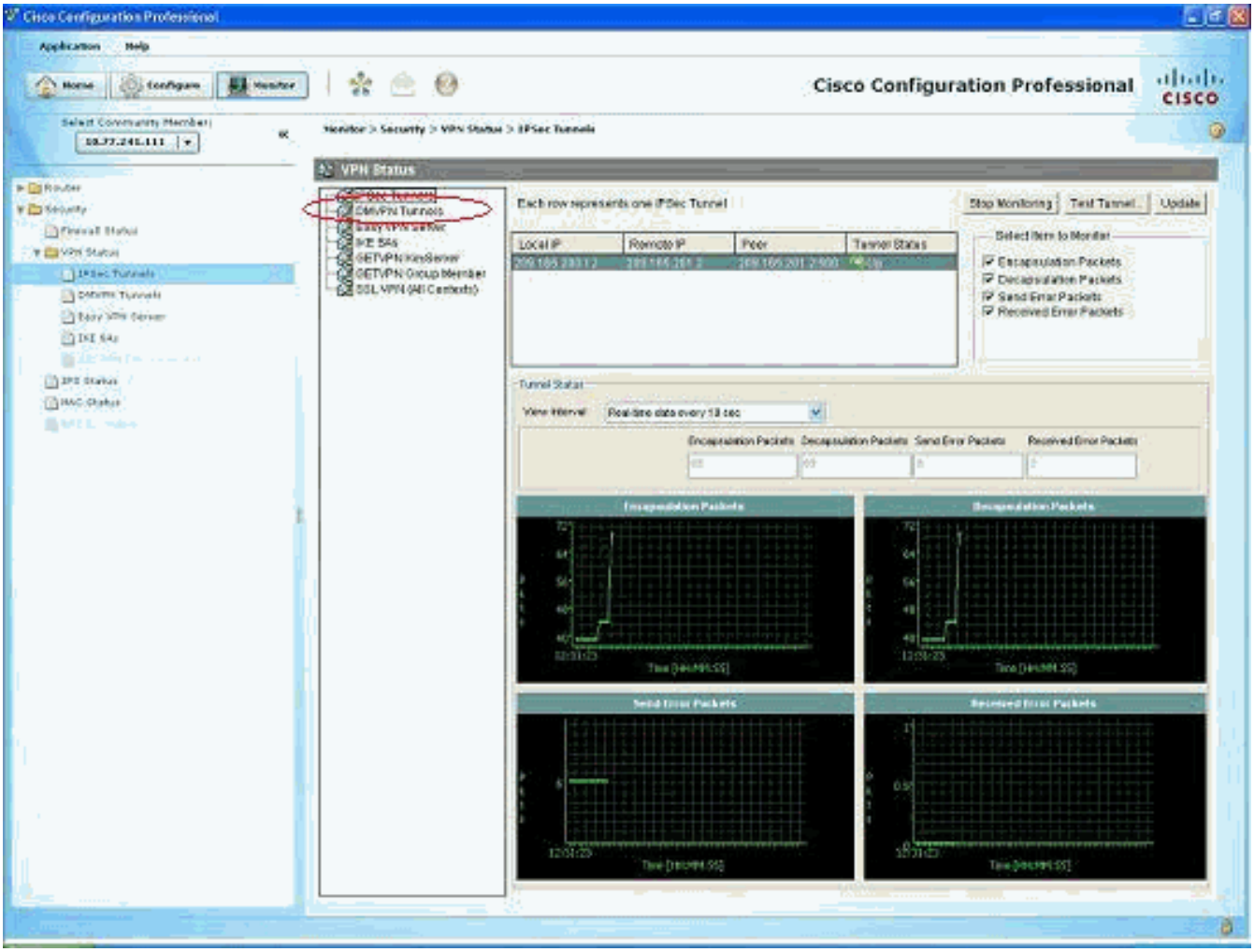
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

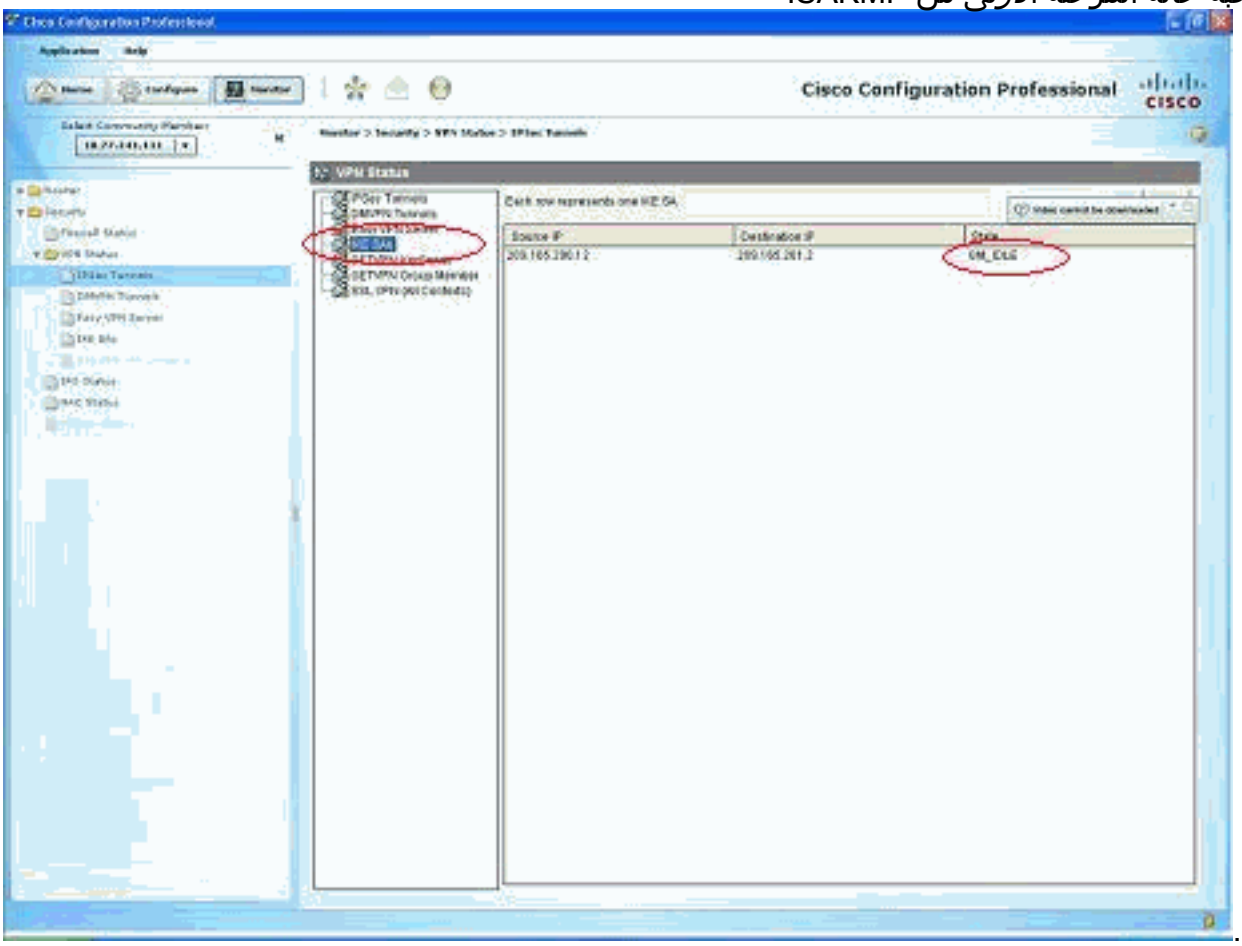
- التحقق من معلمات النفق من خلال CCP
- التحقق من حالة النفق من خلال ASA CLI
- التحقق من معلمات النفق من خلال CLI للموجه

التحقق من معلمات النفق من خلال CCP

- قم بمراقبة حركة مرور البيانات عبر نفق IPsec.



- مراقبة حالة المرحلة الأولى من ISAKMP



.SA

التحقق من حالة النفق من خلال ASA CLI

- تحقق من حالة المرحلة الأولى من ISAKMP SA.

```
ciscoasa#show crypto isakmp sa

                                                    Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
                                                    Total IKE SA: 1

                                          IKE Peer: 209.165.200.12   1
                Type    : L2L                Role    : responder
                Rekey   : no                 State   : MM_ACTIVE
                                                          #ciscoasa
```

ملاحظة: لاحظ دور "المستجيب"، والذي يشير إلى أن بادئ هذا النفق يقع على الطرف الآخر، على سبيل المثال، موجه VPN.

- تحقق من معلمات IPsec SA للمرحلة الثانية.

```
ciscoasa#show crypto ipsec sa
                                                    interface: outside
                Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2

      (local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0
      (remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0
                                          current_peer: 209.165.200.12

                                    pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29#
                                    pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29#
                                  pkts compressed: 0, #pkts decompressed: 0#
          pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0#
             pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
        PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                      send errors: 0, #recv errors: 0#

        local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12

                               path mtu 1500, IPSec overhead 58, media mtu 1500
                                    current outbound spi: E7B37960

                                                    :inbound esp sas
                                      (spi: 0xABB49C64 (2880740452
                            transform: esp-des esp-md5-hmac none
                                { ,in use settings ={L2L, Tunnel
                        slot: 0, conn_id: 4096, crypto-map: mymap
        (sa timing: remaining key lifetime (kB/sec): (4274997/3498
                                                  IV size: 8 bytes
                                    replay detection support: Y
                                                   :outbound esp sas
                                      (spi: 0xE7B37960 (3887298912
                            transform: esp-des esp-md5-hmac none
                                { ,in use settings ={L2L, Tunnel
                        slot: 0, conn_id: 4096, crypto-map: mymap
        (sa timing: remaining key lifetime (kB/sec): (4274997/3498
                                                  IV size: 8 bytes
                                    replay detection support: Y
```

التحقق من معلمات النفق من خلال CLI للموجه

- تحقق من حالة المرحلة الأولى من ISAKMP SA.

```
                                                VPN-Router#show crypto isakmp sa
 dst             src             state          conn-id slot status
 QM_IDLE              1    0 ACTIVE  209.165.200.12   209.165.201.2
```

- تحقق من معلمات IPsec SA للمرحلة الثانية.

```
VPN-Router#show crypto ipsec sa

                                        interface: FastEthernet1
                    Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12

                                        (protected vrf: (none
      (local  ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0
      (remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0
                                    current_peer 209.165.201.2 port 500
                                       {,PERMIT, flags={origin_is_acl
                    pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39#
                    pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39#
                              pkts compressed: 0, #pkts decompressed: 0#
                          pkts not compressed: 0, #pkts compr. failed: 0#
                    pkts not decompressed: 0, #pkts decompress failed: 0#
                                    send errors 6, #recv errors 0#

  local crypto endpt.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
                                        path mtu 1500, ip mtu 1500
                             (current outbound spi: 0xABB49C64(2880740452

                                                 :inbound esp sas
                                       (spi: 0xE7B37960(3887298912
                                  , transform: esp-des esp-md5-hmac
                                       { ,in use settings ={Tunnel
       conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
          (sa timing: remaining key lifetime (k/sec): (4481818/3375
                                                IV size: 8 bytes
                                       replay detection support: Y
                                                 Status: ACTIVE

                                                  :inbound ah sas

                                                 :inbound pcp sas

                                                 :outbound esp sas
                                       (spi: 0xABB49C64(2880740452
                                  , transform: esp-des esp-md5-hmac
                                       { ,in use settings ={Tunnel
       conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
          (sa timing: remaining key lifetime (k/sec): (4481818/3371
                                                IV size: 8 bytes
                                       replay detection support: Y
                                                 Status: ACTIVE

                                                  :outbound ah sas

                                                 :outbound pcp sas
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- تمزيق إتصالات التشفير الموجودة.

```
ciscoasa#clear crypto ipsec sa
ciscoasa#clear crypto isakmp sa

VPN-Router#clear crypto isakmp
```

- أستخدم أوامر **تصحيح الأخطاء** لاستكشاف أخطاء نفق VPN وإصلاحها.**ملاحظة:** إذا قمت بتمكين تصحيح الأخطاء، فقد يؤدي ذلك إلى تعطيل تشغيل الموجه عندما تواجه الشبكات البينية حالات تحميل مرتفع.**أستخدم أوامر تصحيح الأخطاء بحذر. بشكل عام، يوصى باستخدام هذه الأوامر فقط تحت توجيه ممثل الدعم الفني للموجه لديك عند أستكشاف أخطاء معينة وإصلاحها.**

```
ciscoasa#debug crypto engine
ciscoasa#debug crypto isakmp
ciscoasa#debug crypto IPSec
#ciscoasa

VPN-Router#debug crypto engine
Crypto Engine debugging is on
VPN-Router#debug crypto isakmp
Crypto ISAKMP debugging is on
VPN-Router#debug crypto ipsec
Crypto IPSEC debugging is on
#VPN-Router
```

راجع debug crypto isakmp في فهم أوامر تصحيح الأخطاء واستخدامها للحصول على مزيد من المعلومات حول أوامر تصحيح الأخطاء.

معلومات ذات صلة

- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- وثائق برنامج نظام تشغيل جهاز أمان Cisco ASA
- حلول أستكشاف أخطاء IPSec VPN وإصلاحها الأكثر شيوعا
- طلبات التعليقات (RFCs)

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).