

نيوكت لاثم عم IOS تاهجوم ني ب IPsec ةلخادتم لة صاخلا تاكبش ل

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تكوين موجه Cisco IOS في شبكة VPN من موقع إلى موقع IPsec مع عناوين الشبكة الخاصة المتداخلة خلف عبارات VPN.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى موجهات Cisco IOS 3640 التي تشغل الإصدار 12.4 من البرنامج.

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 تلميح Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

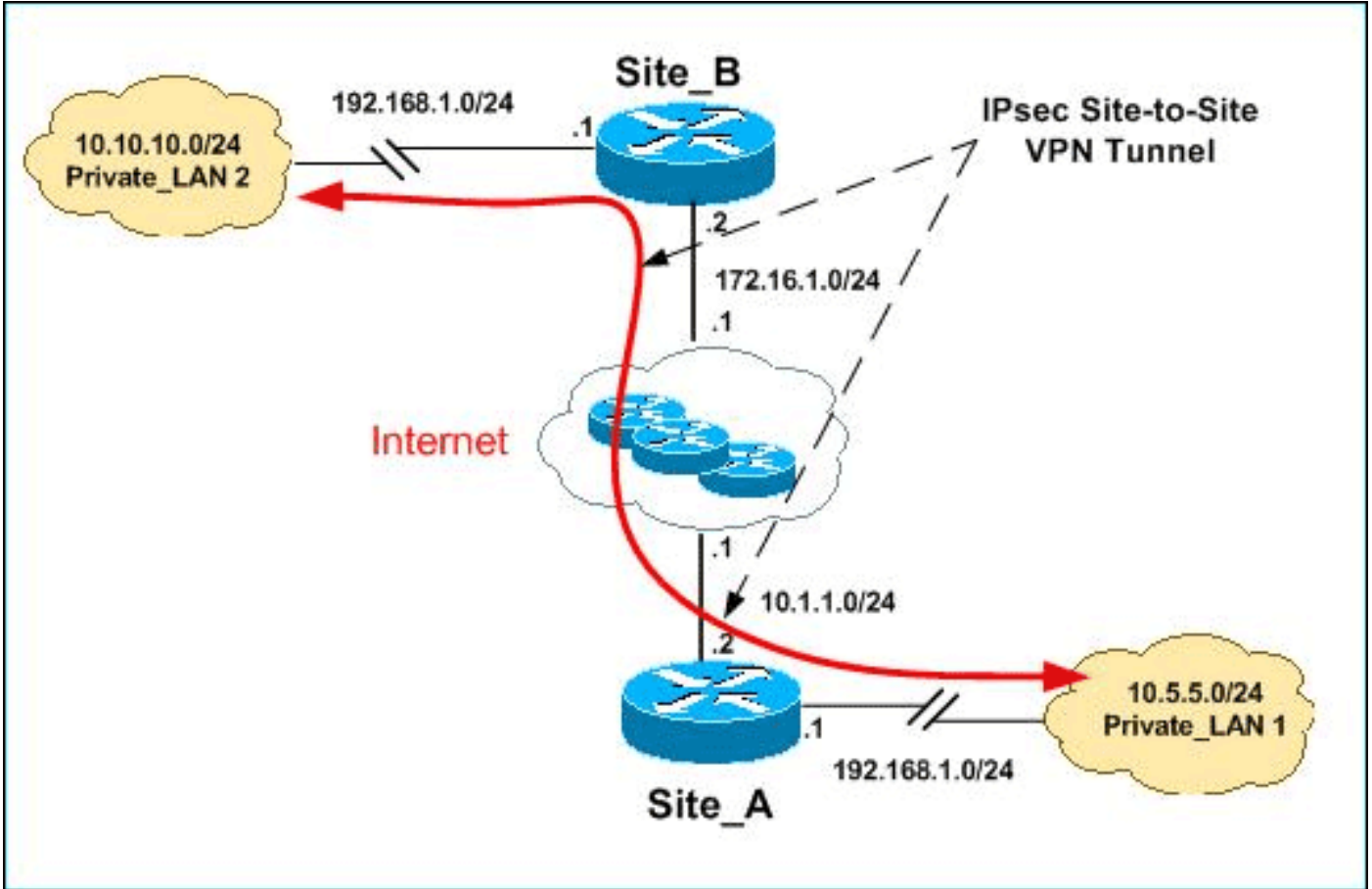
التكوين

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

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [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 عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

يحتوي كل من Private_LAN1 و Private_LAN2 على شبكة IP فرعية من 192.168.1.0/24. يقوم هذا بمحاكاة مساحة العنوان المتداخلة خلف كل جانب من نفق IPsec.

في هذا المثال، يقوم الموجه Site_A بتنفيذ ترجمة ثنائية الإتجاه حتى يمكن للشبكات المحلية الخاصة الإثنان الاتصال عبر نفق IPsec. تعني الترجمة أن Private_LAN1 "يرى" Private_LAN2 على أنه 24/10.10.10.0 من خلال نفق IPsec، و Private_LAN2 "يرى" Private_LAN1 على أنه 24/10.5.5.0 من خلال نفق IPsec.

[التكوينات](#)

يستخدم هذا المستند التكوينات التالية:

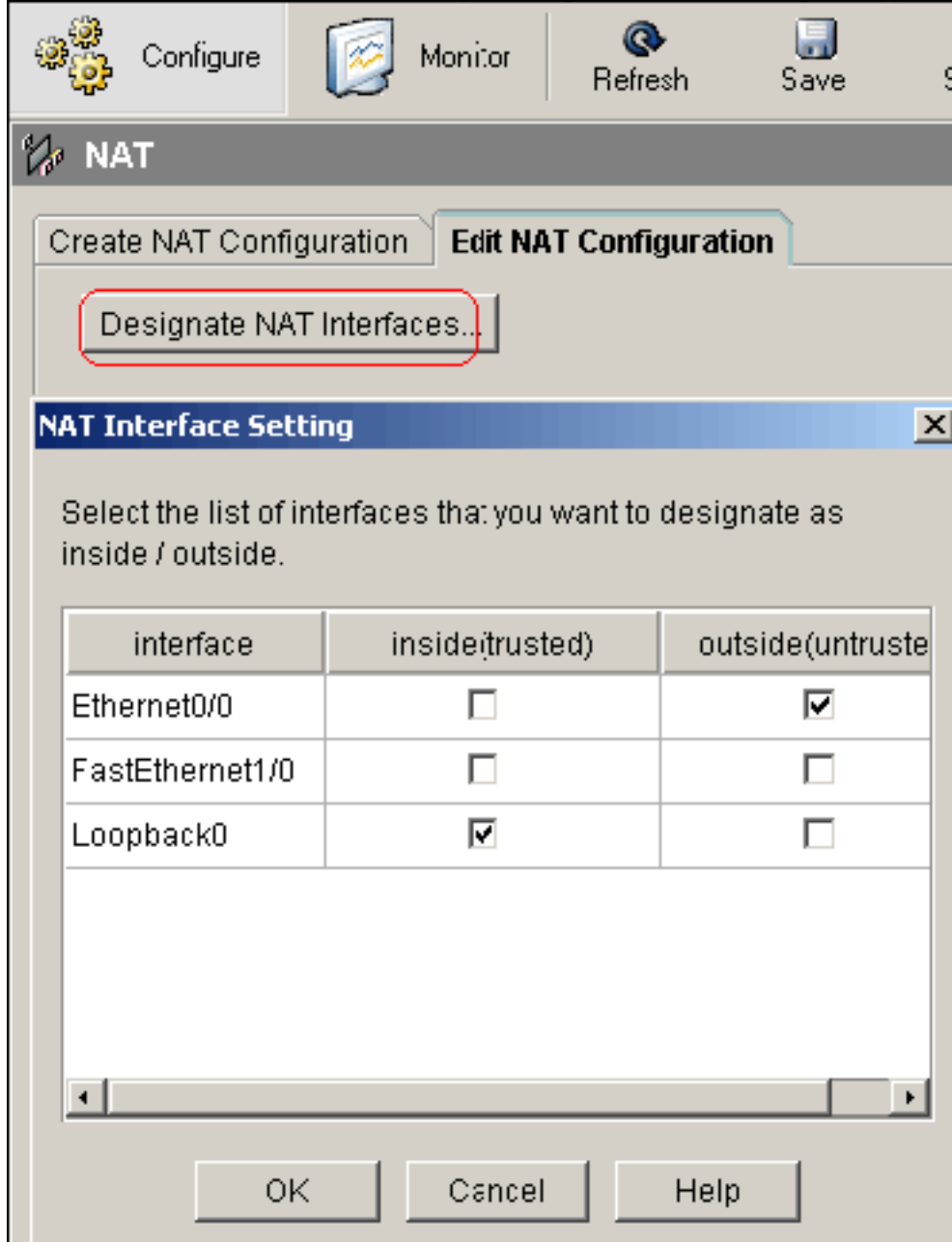
- [تكوين SDM للموجه SITE_A](#)
- [تكوين واجهة سطر الأوامر للموجه SITE_A](#)
- [تكوين موجه SITE_B](#)

ملاحظة: يفترض هذا المستند تكوين الموجه باستخدام الإعدادات الأساسية مثل تكوين الواجهة، وما إلى ذلك. راجع [تكوين الموجه الأساسي باستخدام SDM](#) للحصول على مزيد من المعلومات.

تكوين NAT

أكمل هذه الخطوات لاستخدام NAT لتكوين إدارة قاعدة بيانات المحول (SDM) على الموجه site_a:

1. اخترت بشكل nat <بحرر تشكيل nat>، وطققة يعين nat قارن in order to عينت قارن موثوق به وغير موثوق



به كما هو موضح.

2. وانقر فوق OK.

3. ططققة يضيف in order to شكلت ال nat ترجمة من الداخل إلى الخارج إتجاه كما هو

Add Address Translation Rule

Static Dynamic

Direction: From inside to outside

Translate from interface

Inside Interface(s): Loopback0

IP address: 192.168.1.0

Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Outside Interface(s): Ethernet0/0

Type: IP address

Interface: Ethernet0/0

IP address: 10.5.5.0

Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

موضح.
4. وانقر فوق
.OK

Network Address Translation Rules			
Inside Interface(s):		Loopback0	
Outside Interface(s):		Ethernet0/0	
Original address	Translated address	Rule Type	Add...
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static	

5. مرة أخرى، طقطقت يضيف in order to شكلت ال nat ترجمة من الخارج إلى الداخل إتجاه كما هو

Add Address Translation Rule

Static Dynamic

Direction: From outside to inside

Translate from interface

Outside Interface(s): Ethernet0/0

IP address: 10.10.10.0

Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Inside Interface(s): Loopback0

IP address: 192.168.1.0

Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

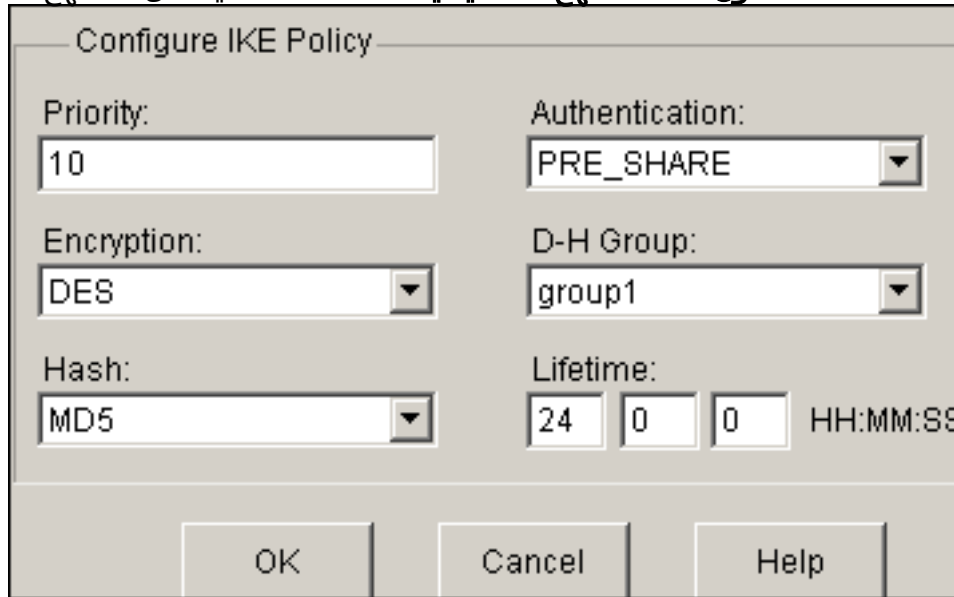
موضح
6. وانقر فوق
.OK

Network Address Translation Rules		
Inside Interface(s):	Loopback0	
Outside Interface(s):	Ethernet0/0	
Original address	Translated address	Rule Type
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static
192.168.1.0-192.168.1.255	10.10.10.0-10.10.10.255	Static

ملاحظة: فيما يلي تكوين CLI المكافئ:
تكوين VPN

أتمت هذا steps in order to استعملت VPN أن يشكل SDM على ال site_a مسح تحديد:

1. أخترت بشكل <VPN>VPN مكون <IKE> IKE < نهج <IKE> يضيف in order to عينت ال ike نهج كما هو موضح في



Configure IKE Policy

Priority: 10

Authentication: PRE_SHARE

Encryption: DES

D-H Group: group1

Hash: MD5

Lifetime: 24 0 0 HH:MM:SS

OK Cancel Help

هذه الصورة.

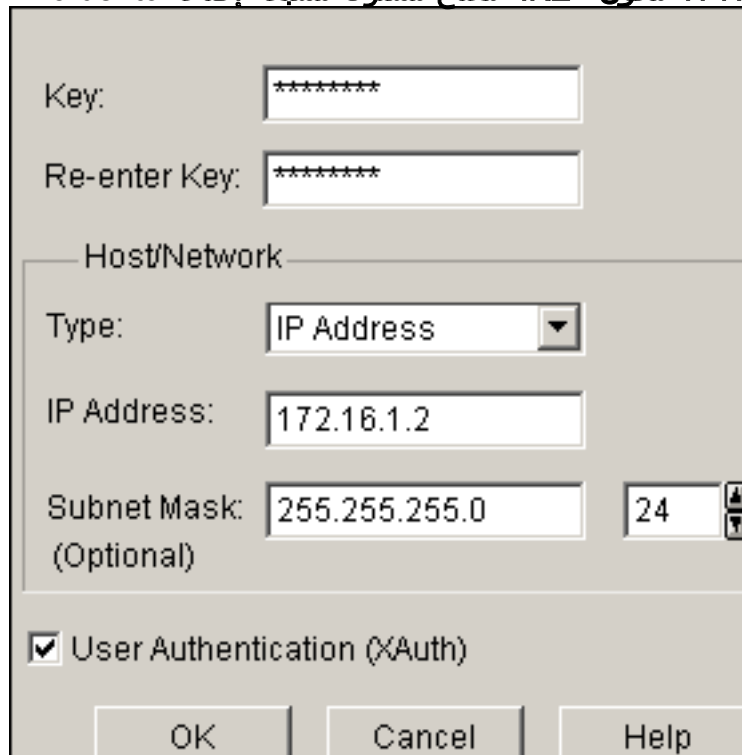
2. وانقر فوق

.OK

IKE Policies						
Priority	Encryption	Hash	D-H Group	Authentication	Type	
10	DES	MD5	group1	PRE SHARE	User Defined	

ملاحظة: فيما يلي تكوين CLI المكافئ:

3. أخترت بشكل <VPN>VPN مكون <IKE>IKE <مفتاح مشترك مسبقا>إضافة in order to ثبت ال pre-shared مفتاح



Key: *****

Re-enter Key: *****

Host/Network

Type: IP Address

IP Address: 172.16.1.2

Subnet Mask: 255.255.255.0 24

User Authentication (XAuth)

OK Cancel Help

قيمة مع نظير عنوان.

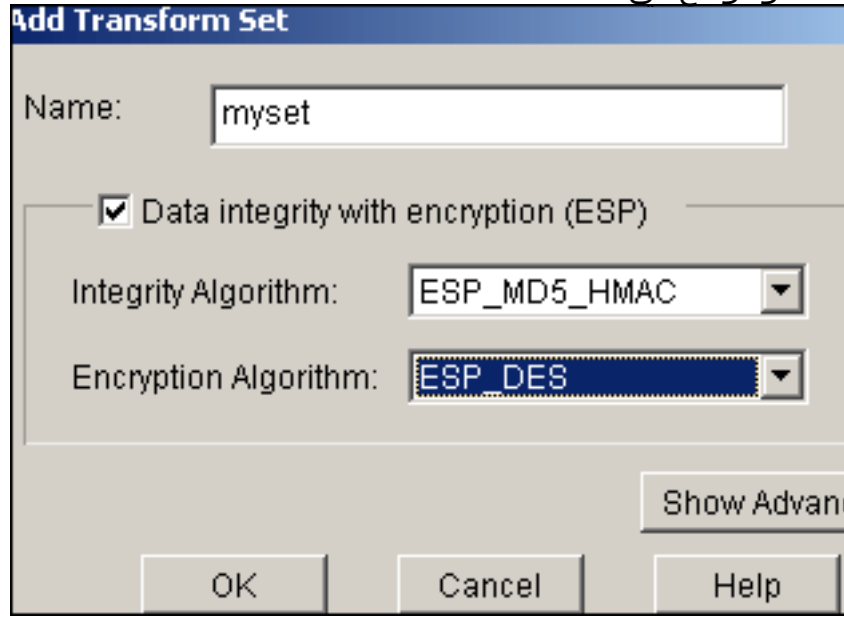
4. وانقر فوق

.OK

Pre-shared Keys		
Peer IP/Name	Subnet Mask	pre-shared key
172.16.1.2	255.255.255.0	*****

ملاحظة: فيما يلي تكوين CLI المكافئ:

5. أخترت بشكل <VPN>VPN مكون <IPSec>IPSec تحويل مجموعة < إضافة > in order to خلقت تحويل مجموعة myset كما هو موضح في هذه



الصورة.

6. وانقر فوق

.OK



Name	ESP Encryption	ESP Integrity	AH Integrity
myset	ESP_DES	ESP_MD5_HMAC	

ملاحظة: فيما يلي تكوين CLI المكافئ:

7. أخترت بشكل <VPN>VPN مكون <IPSec>IPSec قاعدة (ACLs) < إضافة > in order to خلقت تشفير إلى التحكم في الوصول قائمة (ACL)

Add a Rule

Name/Number: Type:

Description:

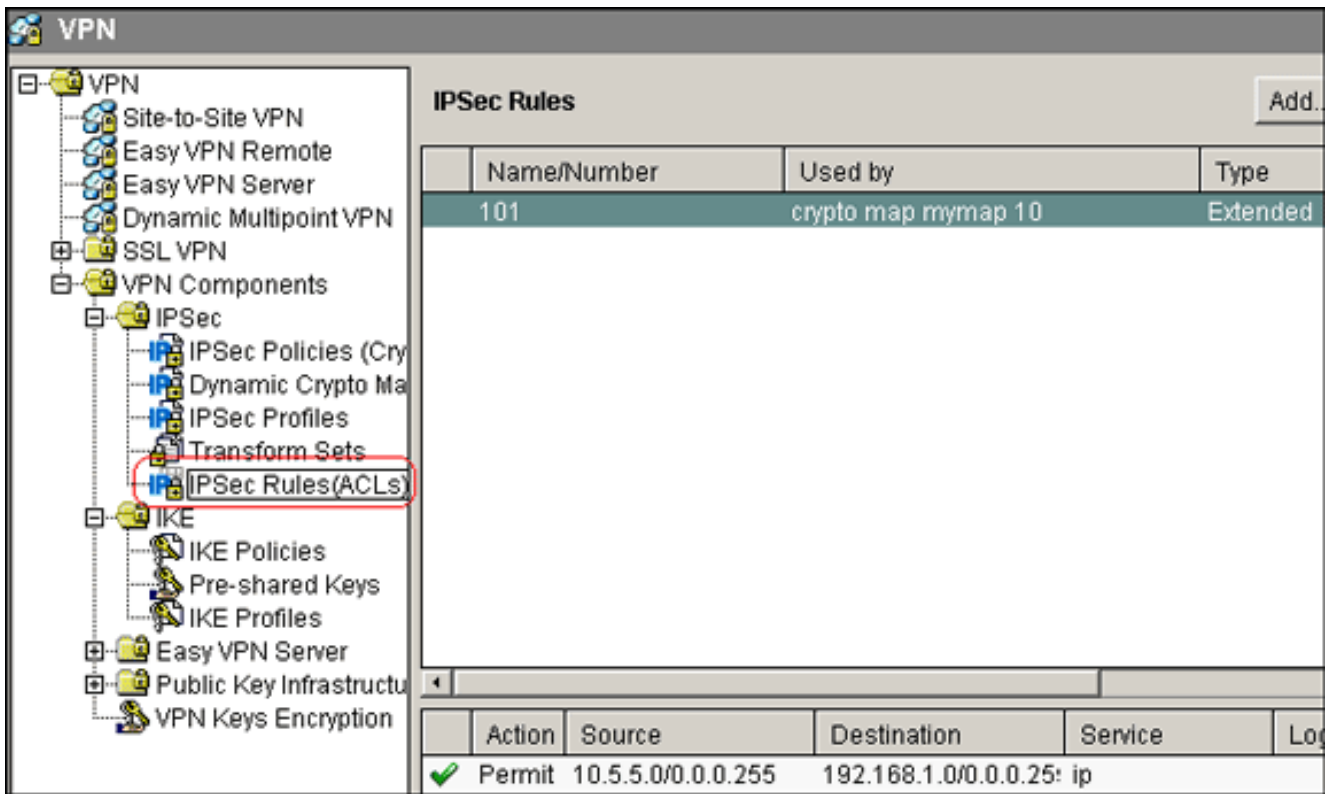
Rule Entry

```
permit ip 10.5.5.0 0.255.255.255 192.168.1.0 0.255.
```

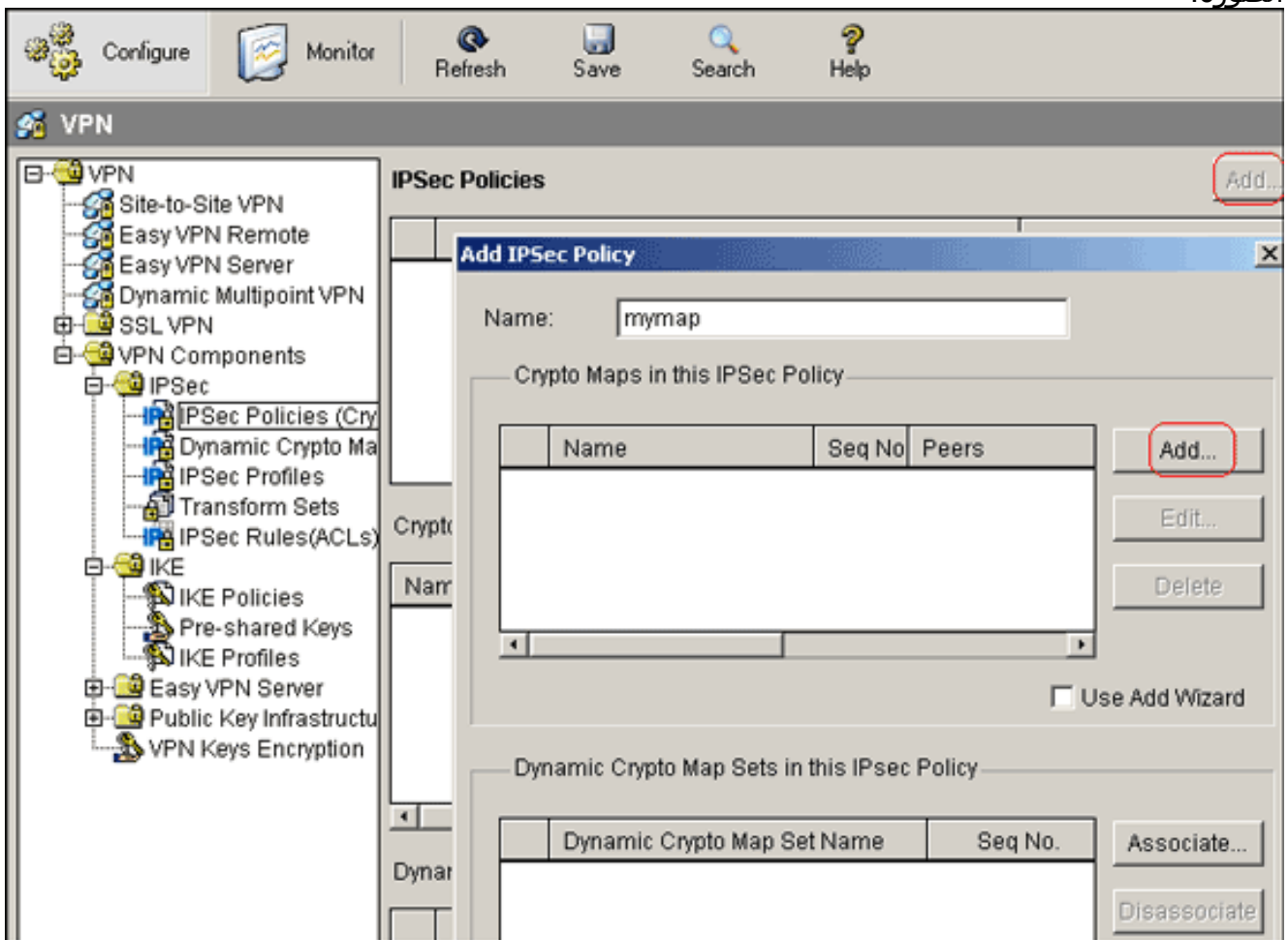
Interface Association
None.

101

8. وانقر فوق
.OK



ملاحظة: فيما يلي تكوين CLI المكافئ:
 9. أختار تكوين < VPN > مكونات IPsec < سياسات IPsec > إضافة in order to خلقت بلوري خريطة mymap كما هو موضح في هذه الصورة.



10. انقر فوق إضافة (Add). انقر على علامة التبويب عام واستبقي الإعدادات

Add Crypto Map

General Peer Information Transform Sets IPsec Rule

Name of IPsec Policy: mymap

Description:

Sequence Number: 1

Security Association Lifetime:
1 0 0 HH:MM:SS 4608000 Kilobytes

Idle Time:
HH:MM:SS

Perfect Forward Secrecy group1

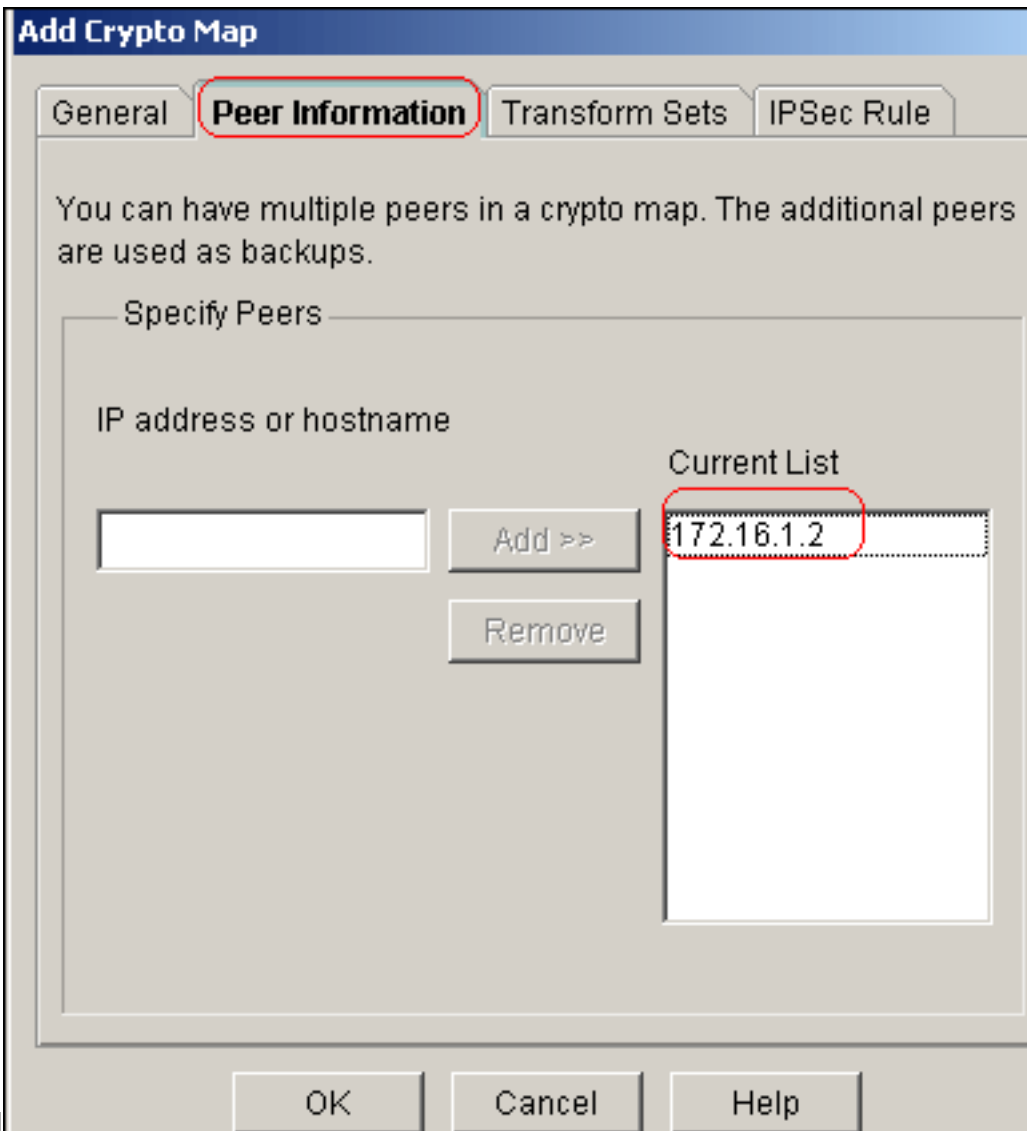
Reverse Route Injection

OK Cancel Help

انقر فوق علامة

الافتراضية.

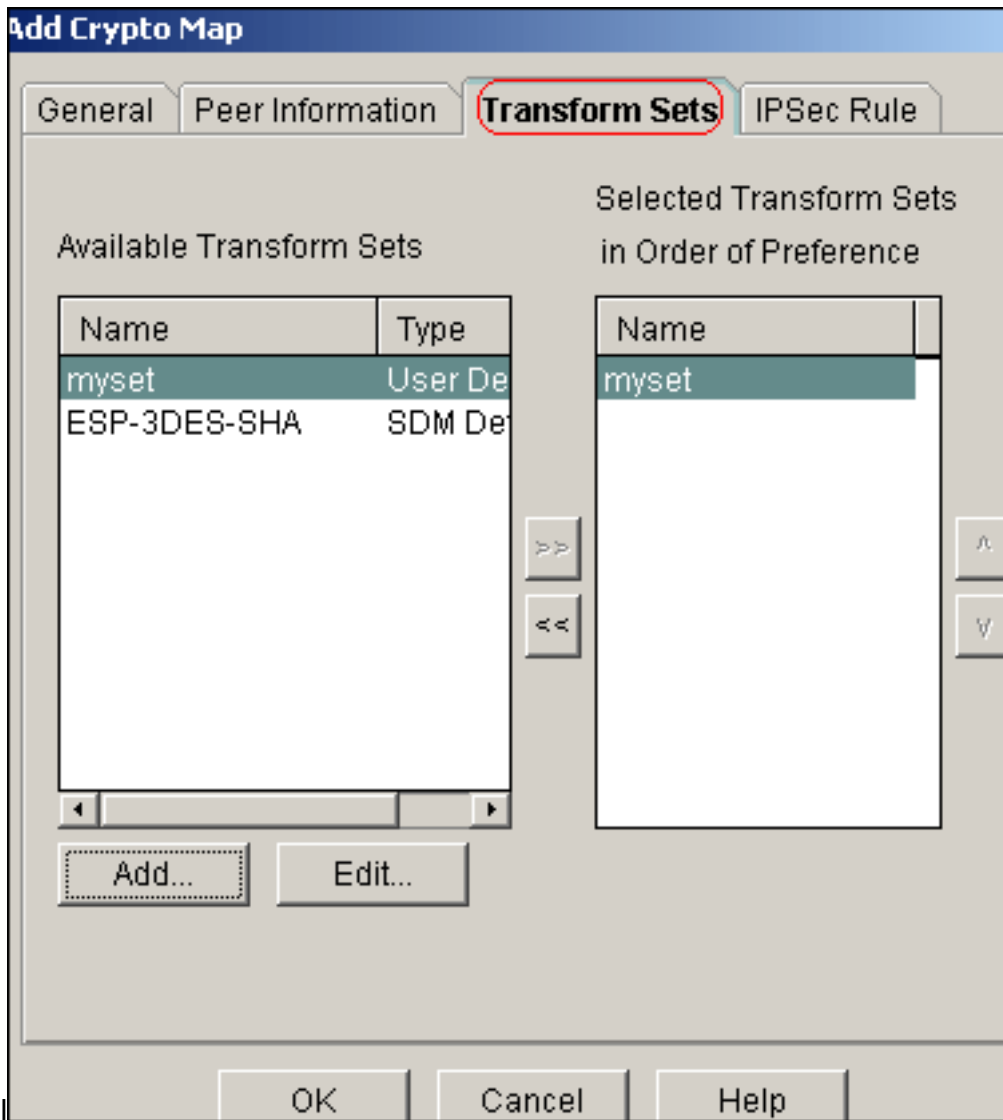
التبويب معلومات النظير لإضافة عنوان IP للنظير



انقر

.172.16.1.2

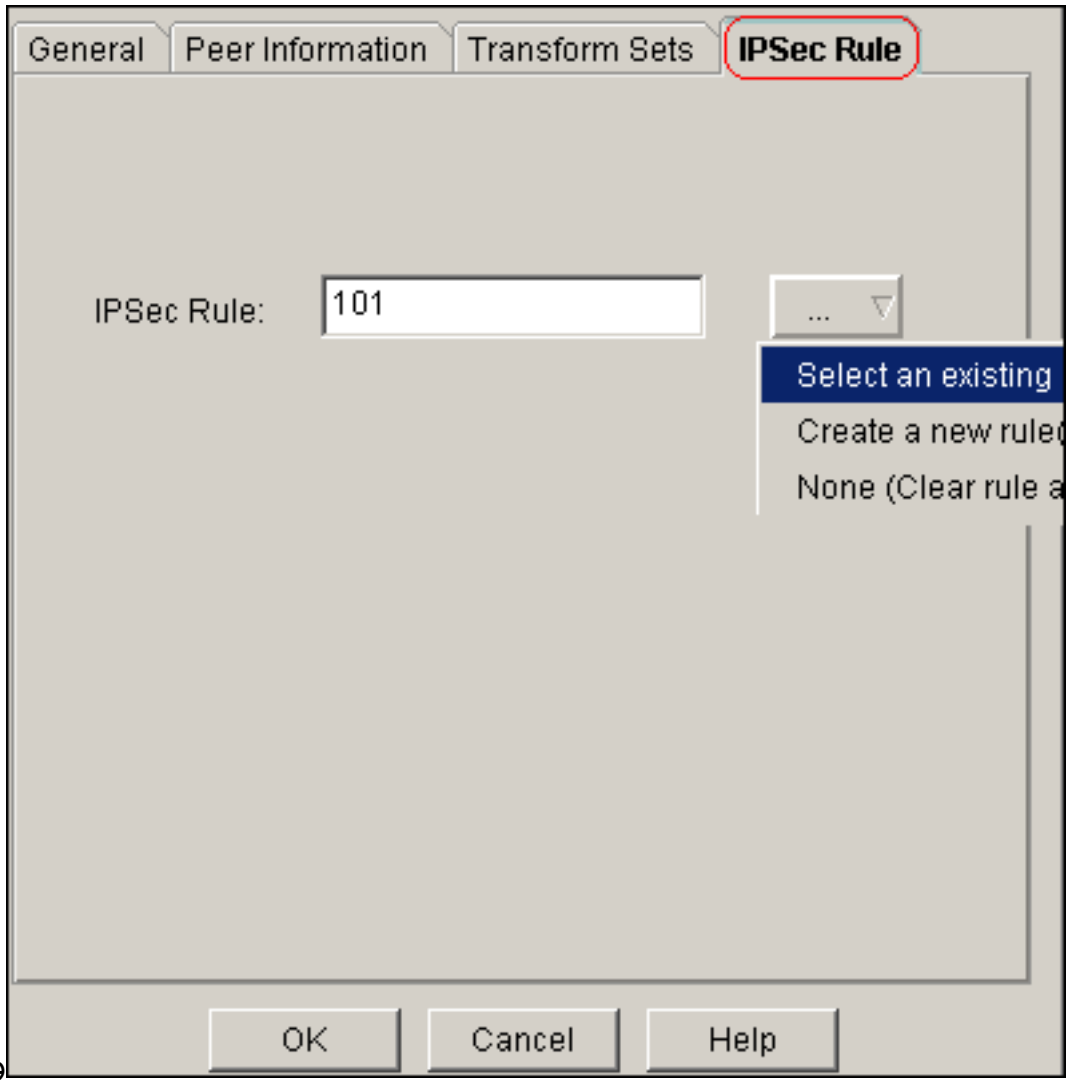
صفحة مجموعات التحويل لتحديد مجموعة ملفات التحويل



انقر فوق

المطلوبة.

علامة التبويب قاعدة IPsec لتحديد قائمة التحكم في الوصول (ACL) المشفرة الحالية

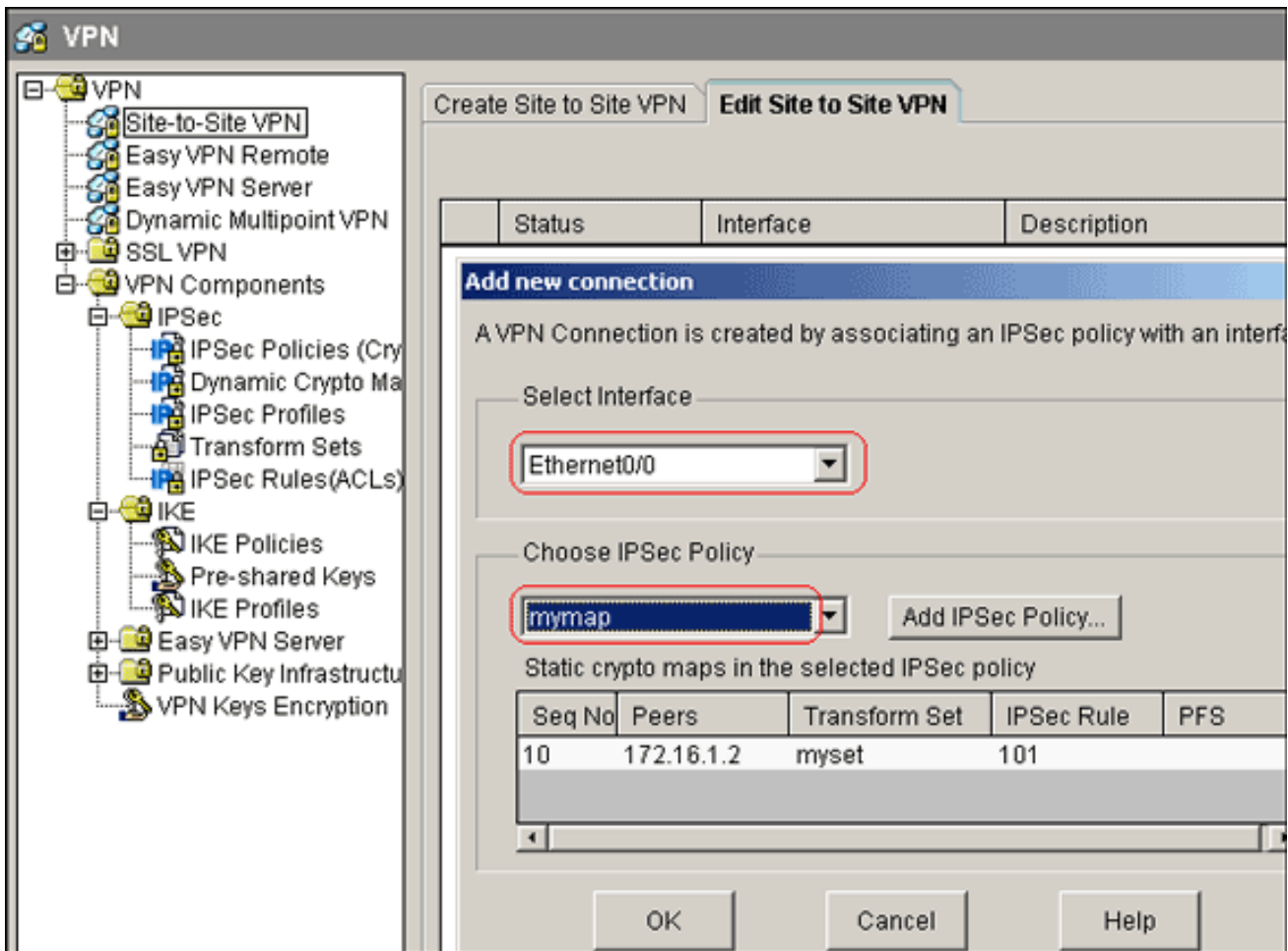


وانقر فوق

.101

OK. ملاحظة: فيما يلي تكوين CLI المكافئ:

11. أخترت بشكل <VPN>VPN من موقع إلى موقع <يحرر VPN من موقع إلى موقع> إضافة in order to طبقت تشفير خريطة mymap إلى القارن إترنت 0/0.



12. وانقر فوق OK. ملاحظة: فيما يلي تكوين CLI المكافئ:

تكوين واجهة سطر الأوامر للموجه SITE A

```

SITE_A موجه
Site_A#show running-config
Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from*
console by console
...Building configuration

Current configuration : 1545 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
!
ip cef

```

```

!
!
crypto isakmp policy 10
    hash md5
    authentication pre-share
Defines ISAKMP policy. crypto isakmp key 6 L2L12345 ---!
    address 172.16.1.2 255.255.255.0

    Defines pre-shared secret used for IKE ---!
authentication !! crypto ipsec transform-set myset esp-
    des esp-md5-hmac
Defines IPSec encryption and authentication ---!
algorithms. ! crypto map mymap 10 ipsec-isakmp
    set peer 172.16.1.2
    set transform-set myset
    match address 101
Defines crypto map. !!! interface Loopback0 ip ---!
    address 192.168.1.1 255.255.255.0 ip nat inside
    ip virtual-reassembly
!
    interface Ethernet0/0
    ip address 10.1.1.2 255.255.255.0
    ip nat outside
    ip virtual-reassembly
    half-duplex
    crypto map mymap
Apply crypto map on the outside interface. !!! --- ---!
    Output Suppressed ! ip http server no ip http secure-
    server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0
/24

    Static translation defined to translate ---!
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
    source static network 192.168.1.0 10.10.10.0 /24

    Static translation defined to translate ---!
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
    ! access-list 101 permit ip 10.5.5.0 0.0.0.255
    192.168.1.0 0.0.0.255

    Defines IPSec interesting traffic. !--- Note that ---!
    the host behind Site_A router communicates !--- to
    Private_LAN2 using 10.10.10.0/24. !--- When the packets
    arrive at the Site_A router, they are first !---
    translated to 192.168.1.0/24 and then encrypted by
    IPSec. !! control-plane !! line con 0 line aux 0 line
    #vty 0 4 !! end Site_A

```

تكوين واجهة سطر الأوامر لموجه SITE B

SITE_B موجه

```

Site_B#show running-config
...Building configuration

```

```

Current configuration : 939 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
set peer 10.1.1.2
set transform-set myset
match address 101
!
!
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
ip address 172.16.1.2 255.255.255.0
crypto map mymap
!
Output Suppressed ! ip classless ip route 0.0.0.0 ---!
0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end
#Site_B

```

[التحقق من الصحة](#)

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

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر `show`.

• **show crypto isakmp sa** — يعرض جميع اقترانات أمان تبادل مفتاح الإنترنت (IKE) الحالية (SAs) في نظير.

```
Site_A#show crypto isakmp sa
dst          src          state          conn-id slot status
QM_IDLE          1          0 ACTIVE          10.1.1.2      172.16.1.2
```

• **show crypto isakmp sa detail** — يعرض تفاصيل جميع شبكات IKE الحالية في نظير.

```
Site_A#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
```

```
C-id Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime
                                           .Cap
ACTIVE des md5 psk 1 23:59:42          172.16.1.2      10.1.1.2      1
```

(Connection-id:Engine-id = 1:1(software

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

```
Site_A#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: mymap, local addr 10.1.1.2

(protected vrf: (none
(local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0
current_peer 172.16.1.2 port 500
{,PERMIT, flags={origin_is_acl
pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2#
pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0#
pkts not decompressed: 0, #pkts decompress failed: 0#
send errors 3, #recv errors 0#

local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
(current outbound spi: 0x1A9CDC0A(446487562

:inbound esp sas
(spi: 0x99C7BA58(2580003416
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
conn id: 2002, flow_id: SW:2, crypto map: mymap
(sa timing: remaining key lifetime (k/sec): (4478520/3336
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

:inbound ah sas

:inbound pcg sas

:outbound esp sas
(spi: 0x1A9CDC0A(446487562
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
conn id: 2001, flow_id: SW:1, crypto map: mymap
(sa timing: remaining key lifetime (k/sec): (4478520/3335
IV size: 8 bytes
replay detection support: Y
```

Status: ACTIVE

:outbound ah sas

:outbound pcp sas

#Site_A

• عرض ترجمات ip nat—يعرض معلومات فتحة الترجمة.

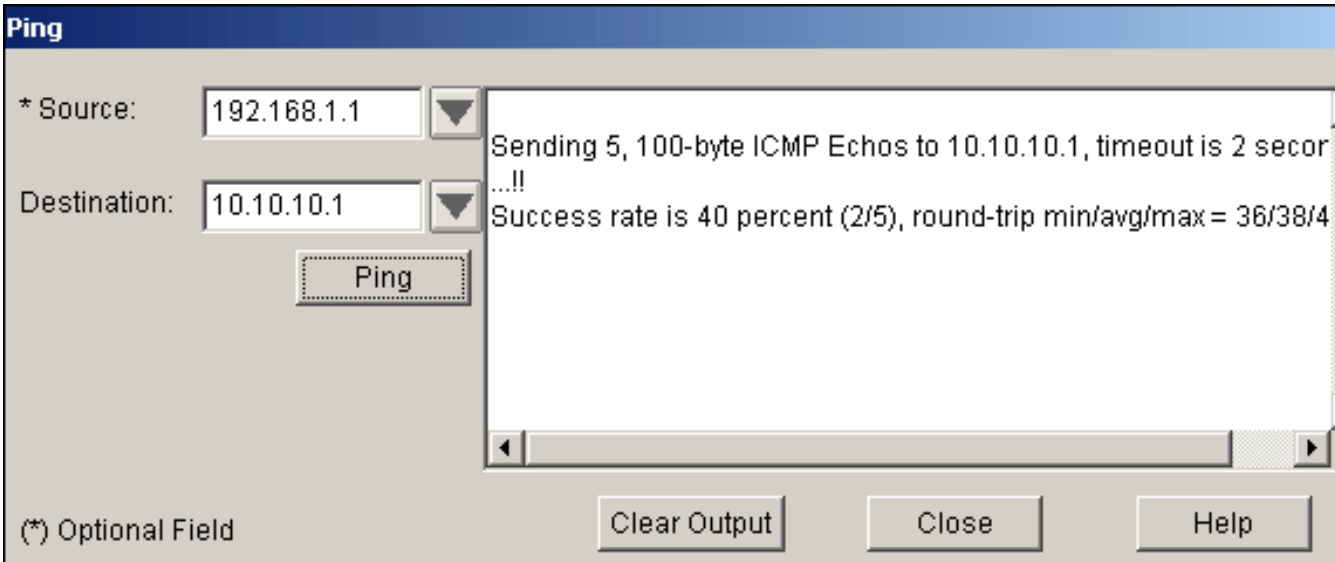
```
Site_A#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
-----
192.168.1.1           10.10.10.1        ---                ---
192.168.1.0           10.10.10.0        ---                ---
---                   ---                192.168.1.1       10.5.5.1
---                   ---                192.168.1.0       10.5.5.0
```

• show ip nat statistics—يعرض معلومات ثابتة حول الترجمة.

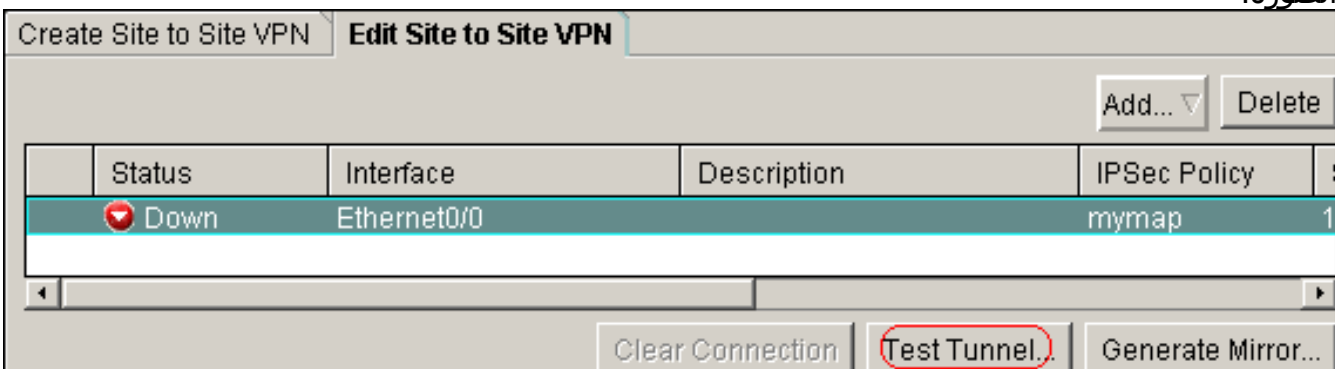
```
Site_A#show ip nat statistics
(Total active translations: 4 (2 static, 2 dynamic; 0 extended)
:Outside interfaces
  Ethernet0/0
:Inside interfaces
  Loopback0
  Hits: 42 Misses: 2
  CEF Translated packets: 13, CEF Punted packets: 0
  Expired translations: 7
:Dynamic mappings
  Queued Packets: 0
#Site_A
```

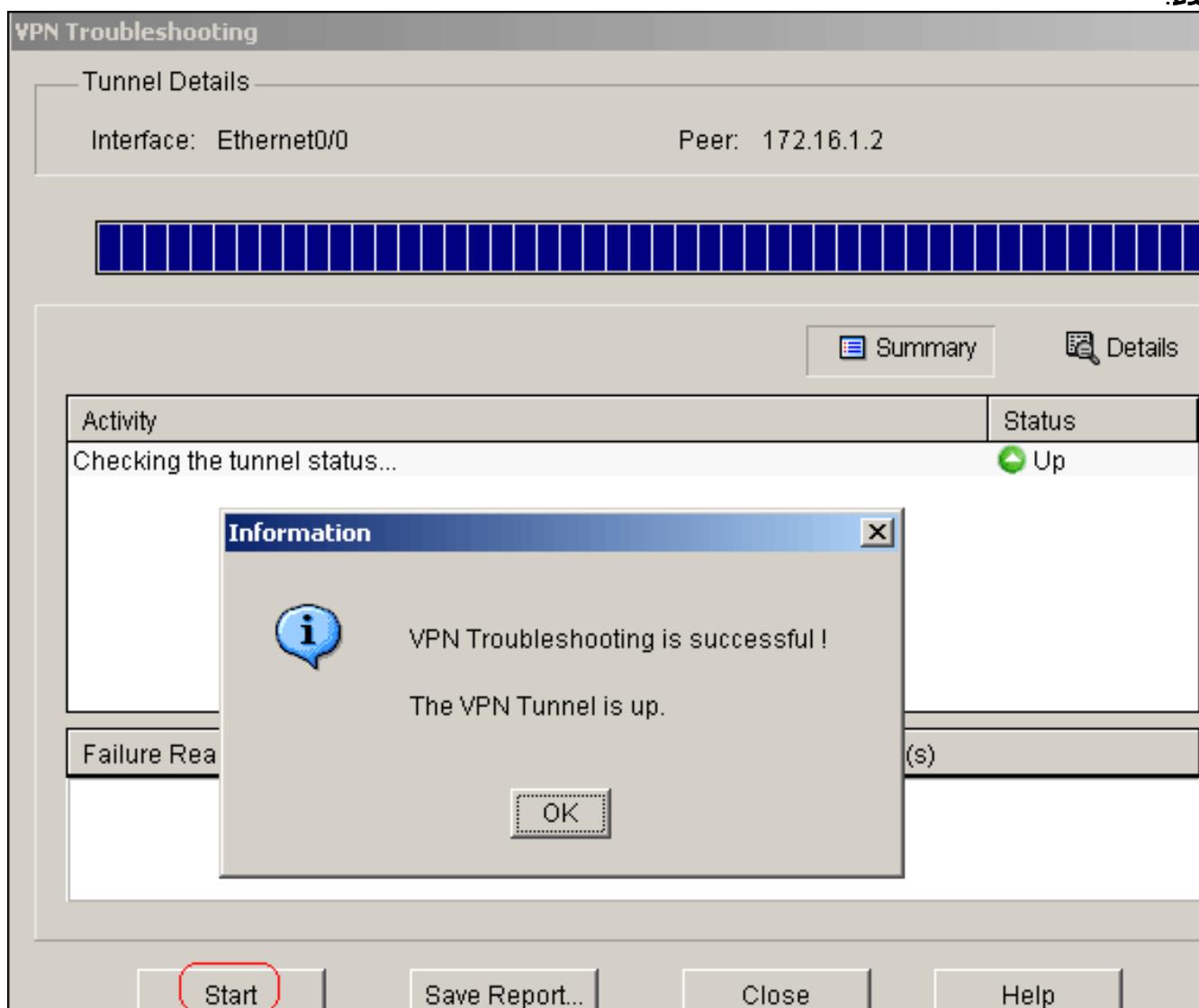
- أتمت هذا steps in order to دقت التوصيل: في إدارة قاعدة بيانات المحول (SDM)، أختار الأدوات < اختبار الاتصال لإنشاء نفق VPN ل IPsec باستخدام عنوان IP المصدر كعنوان 192.168.1.1 وعنوان IP للوجهة كعنوان

10.10.10.1



انقر فوق اختبار النفق للتحقق من إنشاء نفق VPN ل IPsec كما هو موضح في هذه الصورة.





استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

```

Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
:[Protocol [ip
Target IP address: 10.10.10.1
:[Repeat count [5
:[Datagram size [100
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 192.168.1.1
:[Type of service [0
:[Set DF bit in IP header? [no
:[Validate reply data? [no
:[Data pattern [0xABCD
:[Loose, Strict, Record, Timestamp, Verbose[none
:[Sweep range of sizes [n
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds

```

```
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
#Site_A
Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet*
et0/0), routed via FIB
Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len*
sending ,100
) Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1*
Loopback0), routed via RIB
Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc*
vd 4
Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet*
et0/0), routed via FIB
Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len*
sending ,100
) Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1*
Loopback0), routed via RIB
Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc*
vd 4
Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet*
et0/0), routed via FIB
Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len*
sending ,100
) Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1*
Loopback0), routed via RIB
Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc*
vd 4
Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet*
et0/0), routed via FIB
Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len*
sending ,100
) Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1*
Loopback0), routed via RIB
Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc*
vd 4
Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet*
et0/0), routed via FIB
Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len*
sending ,100
) Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1*
Loopback0), routed via RIB
Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc*
vd 4
```

معلومات ذات صلة

- [حلول أكتشاف أخطاء الشبكة الخاصة الظاهرية \(VPN\) عبر بروتوكول IPsec للوصول عن بعد و L2L الأكثر شيوعا](#)
- [IPsec بين ASA/PIX و Cisco VPN 3000 Concentrator مع مثال تكوين الشبكات الخاصة المتداخلة](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م 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