

ASA-to-ASA Dynamic-to-Static IKEv1/IPsec نيوكت لاثم

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [تكوين ASDM](#)
- [ASA المركزي \(النظير الثابت\)](#)
- [ASA عن بعد \(النظير الديناميكي\)](#)
- [تكوين واجهة سطر الأوامر \(CLI\)](#)
- [تكوين ASA المركزي \(النظير الثابت\)](#)
- [ASA عن بعد \(النظير الديناميكي\)](#)
- [التحقق من الصحة](#)
- [أسيا الوسطى](#)
- [Remote-ASA](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [نظام ASA عن بعد \(البادئ\)](#)
- [Central-ASA \(مستجيب\)](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية تمكين جهاز الأمان القابل للتكيف (ASA) من قبول اتصالات VPN الديناميكية من موقع IPsec إلى موقع من أي نظير ديناميكي (ASA في هذه الحالة). كما يوضح الرسم التخطيطي للشبكة في هذا المستند، يتم إنشاء نفق IPsec عند بدء النفق من الطرف البعيد ASA فقط. لا يمكن ل Central-ASA بدء نفق VPN بسبب تكوين IPsec الديناميكي. عنوان IP الخاص ب Remote-ASA غير معروف.

قم بتكوين Central-ASA من أجل قبول الاتصالات بشكل ديناميكي من عنوان IP لبطاقة برة (0/0.0.0.0) ومفتاح مشترك مسبقا لبطاقة برة. بعد ذلك، يتم تكوين ASA عن بعد لتشغيل حركة مرور البيانات من الشبكات الفرعية المحلية إلى شبكات ASA المركزية كما هو محدد بواسطة قائمة وصول التشفير. يجري كلا الجانبين إستثناء ترجمة عنوان الشبكة (NAT) من أجل تجاوز NAT لحركة مرور IPsec.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج جدار الحماية (Cisco ASA 5510 و 5520)، الإصدار x.9 والإصدارات الأحدث.

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.

التكوين

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

الرسم التخطيطي للشبكة

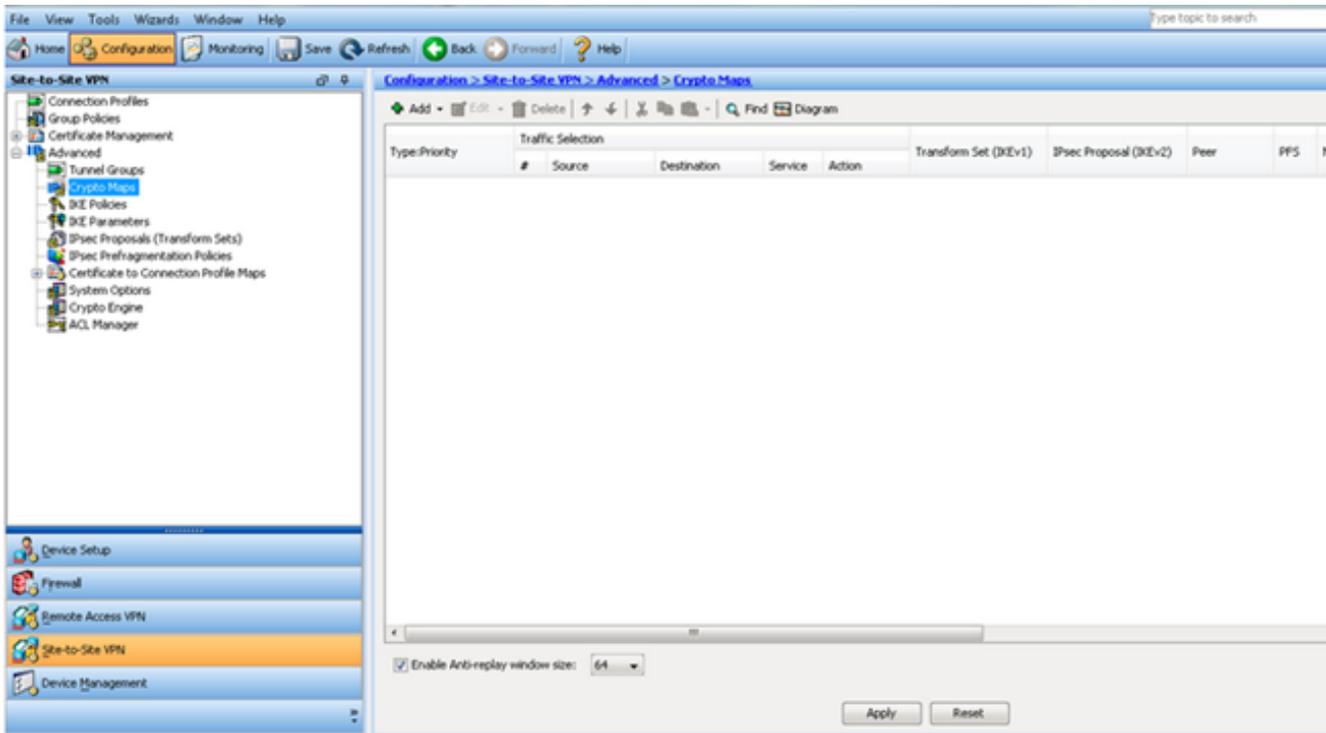


تكوين ASDM

ASA المركزي (النظير الثابت)

على ASA مع عنوان ساكن إستاتيكي، VPN setup بطريقتة أن هو يقبل توصيل حركي من نظير غير معروف بينما هو لا يزال يصادق النظير يستعمل IKEv1 مشترك مسبقا مفتاح:

1. أخترت تشكيل <موقع إلى موقع VPN> متقدم <تشفير خرائط. يعرض الإطار قائمة إدخال خريطة التشفير الموجودة بالفعل (إذا كان هناك أي). بما أن ASA لا يعرف ما هو عنوان IP للنظير، in order to ASA أن يقبل الاتصال يشكل خريطة ديناميكية مع مطابقة مجموعة التحويل (اقترح IPsec). انقر فوق إضافة (Add).



2. في نافذة "إنشاء قاعدة IPsec"، من "سياسة النفق" (خريطة التشفير) - علامة التبويب "أساسي"، أختار من الخارج من القائمة المنسدلة "الواجهة" والديناميكية من القائمة المنسدلة "نوع السياسة". في حقل الأولوية، قم بتعيين الأولوية لهذا الإدخال في حالة وجود إدخالات متعددة تحت الخريطة الديناميكية. بعد ذلك، انقر فوق تحديد بجوار حقل مقترح IPsec ل IKE v1 لتحديد مقترح IPsec.

Create IPsec Rule

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Interface: Policy Type: Priority:

IPsec Proposals (Transform Sets)

IKE v1 IPsec Proposal:

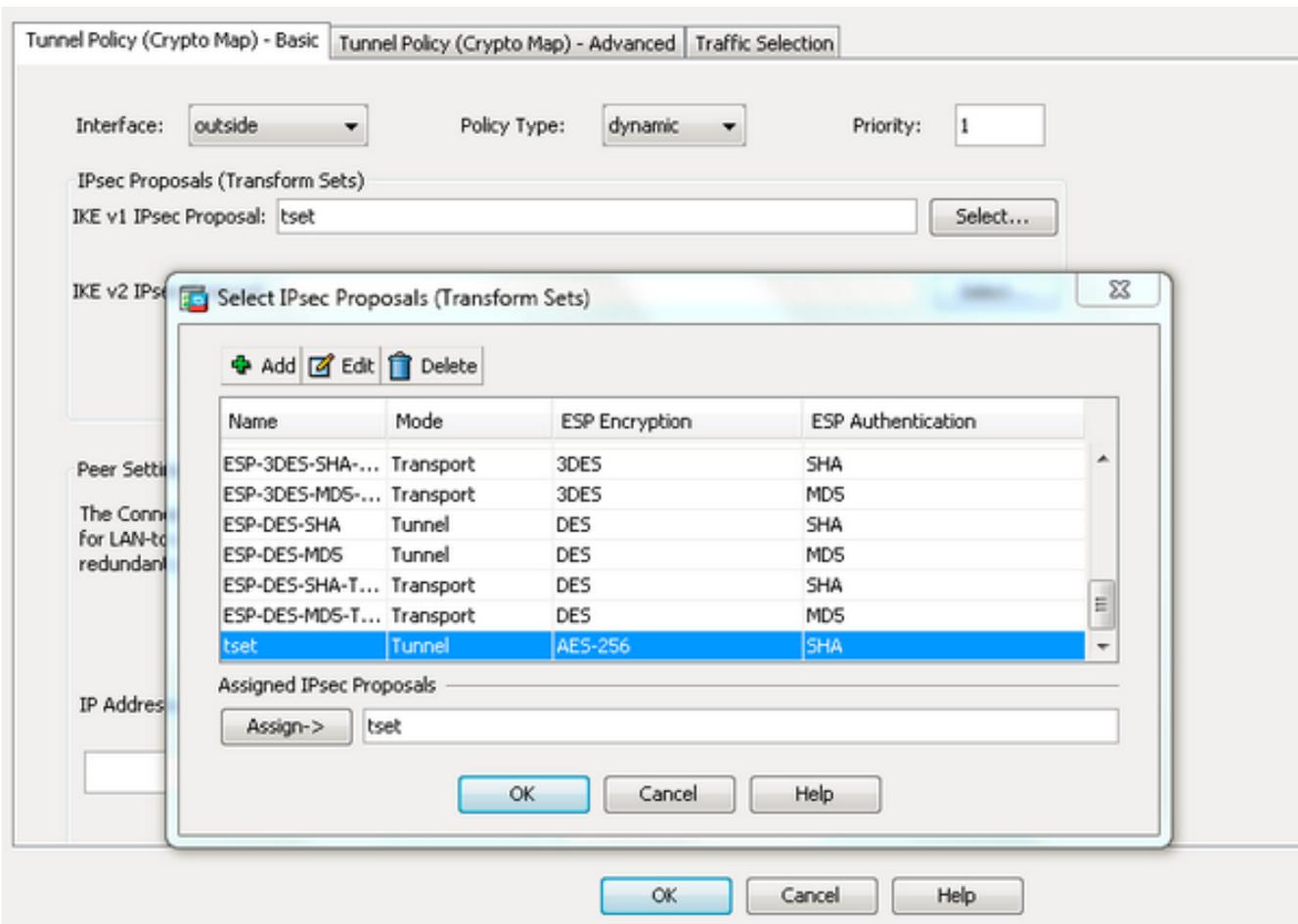
IKE v2 IPsec Proposal:

Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

IP Address of Peer to Be Added:

3. عند فتح شاشة تحديد مقترحات IPsec (مجموعات التحويل)، أختار من بين مقترحات IPsec الحالية أو انقر فوق إضافة لإنشاء اقتراح جديد واستخدام نفس الإجراء. انقر فوق موافق عند الانتهاء.



4. من علامة التبويب المتقدمة سياسة النفق (خريطة التشغيل)، حدد خانة الاختيار تمكين NAT-T (مطلوب إذا كان أي من النظراء خلف جهاز nat) وخانة الاختيار تمكين حقن المسار العكسي. عندما يأتي نفق VPN للنظير الديناميكي، يقوم ASA بتثبيت مسار ديناميكي لشبكة VPN البعيدة التي تم التفاوض عليها والتي تشير إلى واجهة .VPN

Create IPsec Rule

Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection

Enable NAT-T

Enable Reverse Route Injection

Security Association Lifetime Settings

Time: : : hh:mm:ss

Traffic Volume: unlimited KBytes

ESP v3

Validate incoming ICMP error messages

Enable Do Not Fragment (DF) policy

Enable Traffic Flow Confidentiality (TFC) packets. This is unavailable if IKEv1 is enabled.

OK Cancel Help

إختياريا، من علامة التبويب تحديد حركة مرور البيانات يمكنك أيضا تحديد حركة مرور VPN المثيرة للاهتمام للنظير الديناميكي وانقر فوق موافق.

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Action: Protect Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

Description:

More Options

Enable Rule

Source Service: (TCP or UDP service only) ⓘ

Time Range:

OK Cancel Help

Add Edit Delete | Up Down | Copy Paste | Find Diagram

Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
interface: outside						
dynamic: 65535.1	1	any4	any4	IP ip	Protect	tset

Enable Anti-replay window size:

وكما تمت الإشارة مسبقا، فنظرا لأن ASA لا يحتوي على أي معلومات حول عنوان IP الديناميكي البعيد للنظير، فإن طلب الاتصال غير المعروف يقع ضمن DefaultL2LGgroup الموجود على ASA بشكل افتراضي. لكي تتجح المصادقة في إنشاء المفتاح المشترك مسبقا (Cisco123 في هذا المثال) الذي تم تكوينه على النظير البعيد، يجب أن يتطابق مع مفتاح آخر ضمن DefaultL2LGgroup.

5. أخترت تشكيل <موقع إلى موقع VPN> متقدم <نفق مجموعة>، تقصير L2LGgroup، طقطقة يحرر وشكلت ال مرغوب مشترك مسبقا مفتاح. انقر فوق موافق عند الانتهاء.

Configure IPsec site-to-site tunnel groups.

Name	Group Policy	IKEv1 Enabled	IKEv2 Enabled
DefaultL2LGroup	DfltGrpPolicy	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Edit IPsec Site-to-site Tunnel Group: DefaultL2LGroup

Name:

IPsec Enabling

Group Policy Name:

(Following two fields are attributes of the group policy selected above.)

Enable IKE v1 Enable IKE v2

IPsec Settings

IKE v1 Settings

Authentication

Pre-shared Key:

Device Certificate:

IKE Peer ID Validation:

IKE Keepalive

Disable keepalives

Monitor keepalives

Confidence Interval: seconds

Retry Interval: seconds

ملاحظة: يؤدي هذا إلى إنشاء مفتاح حرف بدل مشترك مسبقا على النظير الثابت (Central-ASA). يمكن لأي جهاز/نظير يعرف هذا المفتاح المشترك مسبقا ومقترحاته المطابقة أن ينشئ بنجاح نفق VPN ويدخل الموارد عبر VPN. تأكد من عدم مشاركة هذا المفتاح الذي تم تزويده مسبقا مع كيانات غير معروفة وليس من السهل تخمينه.

6. أخترت تشكيل <موقع إلى موقع VPN> مجموعة سياسة وحدد المجموعة-سياسة من إختيارك (تقصير مجموعة سياسة في هذه الحالة). انقر فوق تحرير نهج المجموعة وتحريره في مربع الحوار "تحرير نهج المجموعة الداخلي". انقر فوق موافق عند الانتهاء.

Configuration > Site-to-Site VPN > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

[Add](#) [Edit](#) [Delete](#) [Assign](#)

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPNGroup;

Edit Internal Group Policy: DfltGrpPolicy

Name:

Tunneling Protocols: Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec

Filter: [Manage...](#)

Idle Timeout: Unlimited minutes

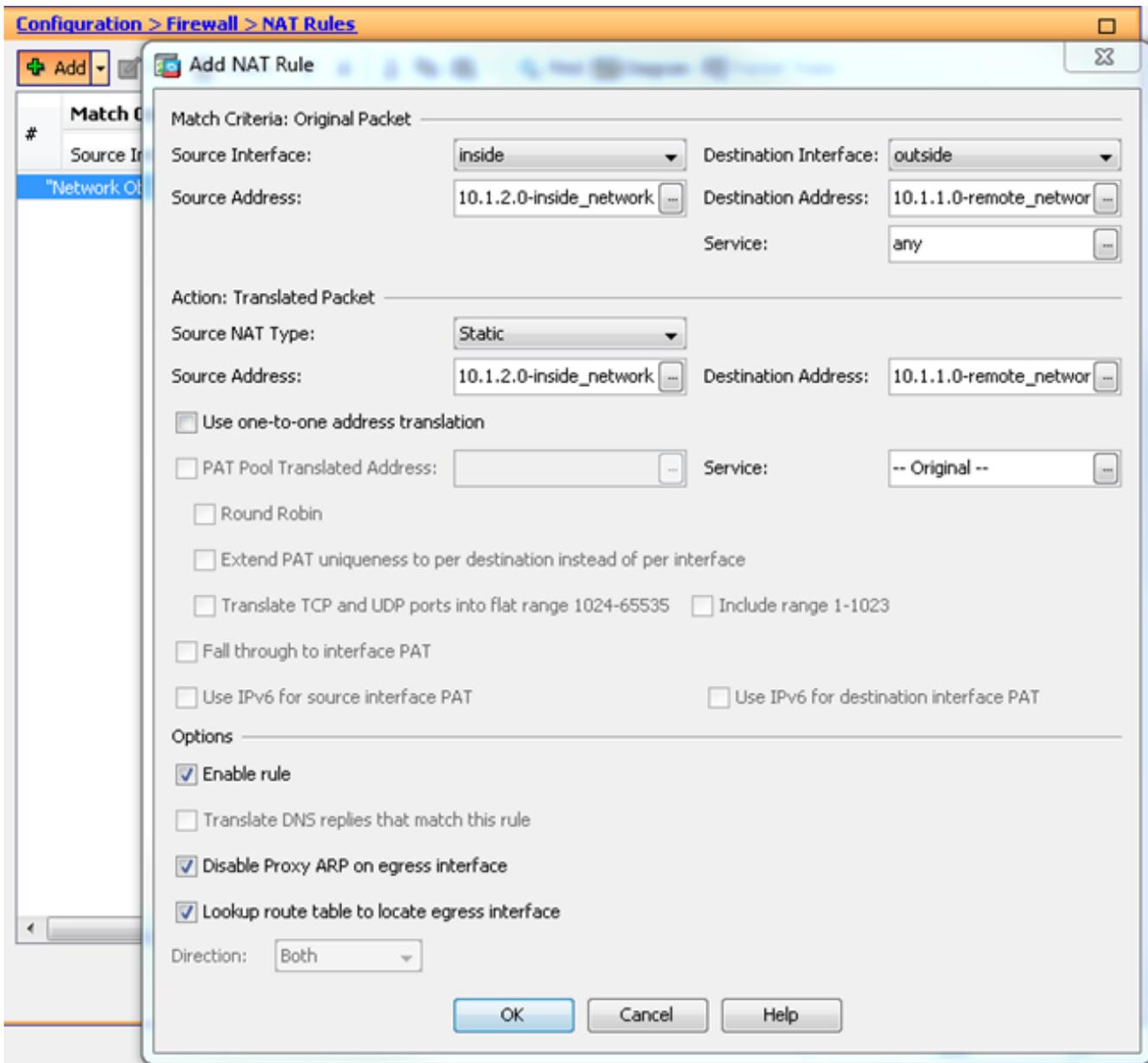
Maximum Connect Time: Unlimited minutes

[OK](#) [Cancel](#) [Help](#)

Find: Match Case

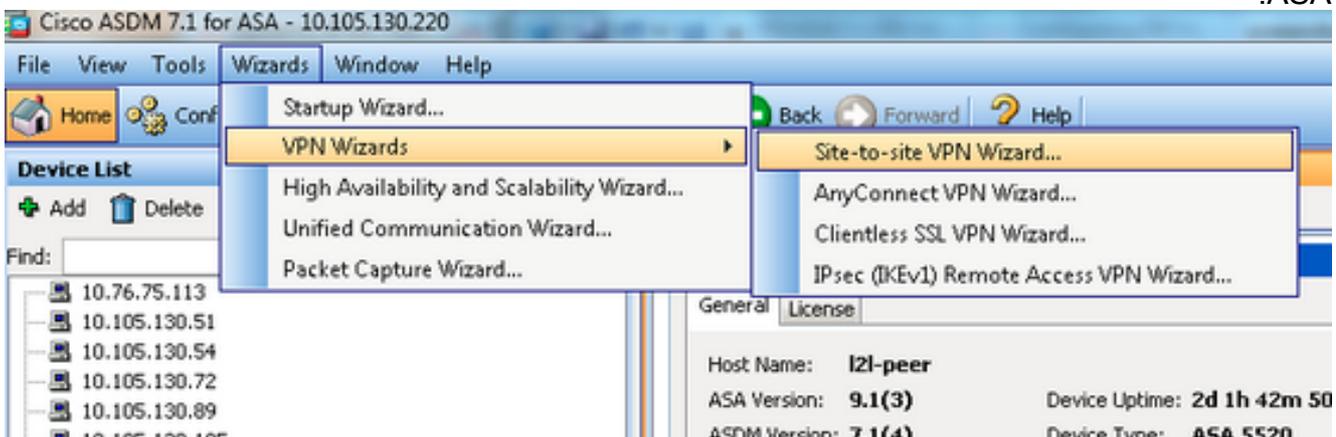
[Apply](#) [Reset](#)

7. أخترت تشكيل <جدار حماية> nat قاعدة ومن ال add nat قاعدة، شكلت ما من nat-exempt (nat قاعدة ل VPN حركة مرور. انقر فوق موافق عند الانتهاء.



ASA عن بعد (النظير الديناميكي)

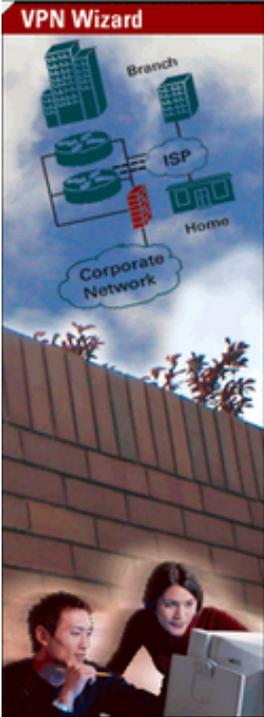
1. اختر المعالجات < معالجات VPN > معالج VPN من موقع إلى موقع بمجرد اتصال تطبيق ASDM بـ ASA.



2. انقر فوق Next (التالي).

Site-to-site VPN Connection Setup Wizard

VPN Wizard



Introduction

Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional protects the data using the IPsec protocol.



Here is a [video](#) on how to setup a site-to-site VPN connection.

< Back Next >

3. أخترت خارج من ال VPN منفذ قارن قائمة ميلان إلى جانب in order to عينت العنوان خارجي من النظر بعيد. حدد الواجهة (WAN) حيث يتم تطبيق خريطة التشفير. انقر فوق **Next** (التالي).

Site-to-site VPN Connection Setup Wizard

Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address:

VPN Access Interface:

< Back Next >

4. حدد البيئات المضيفة/الشبكات التي يجب السماح لها بالمرور من خلال نفق VPN. في هذه الخطوة، يلزمك توفير الشبكات المحلية والشبكات البعيدة لنفق الشبكة الخاصة الظاهرية (VPN). انقر فوق الأزرار المجاورة لحقول الشبكة المحلية والشبكة البعيدة واختر العنوان حسب المتطلبات. طقطقت بعد ذلك عندما أنت إنتهيت.

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
- 3. Traffic to protect**
4. Security
5. NAT Exempt
6. Summary

Traffic to protect

This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

IP Address Type: IPv4 IPv6

Local Network:

Remote Network:

< Back Next >

5. أدخل معلومات المصادقة التي سيتم استخدامها، والتي يتم مشاركتها مسبقاً في هذا المثال. المفتاح المشترك مسبقاً المستخدم في هذا المثال هو Cisco123. اسم مجموعة النفق هو عنوان IP النظير البعيد بشكل افتراضي إذا قمت بتكوين شبكة VPN من LAN إلى LAN ((L2L.

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
- 4. Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

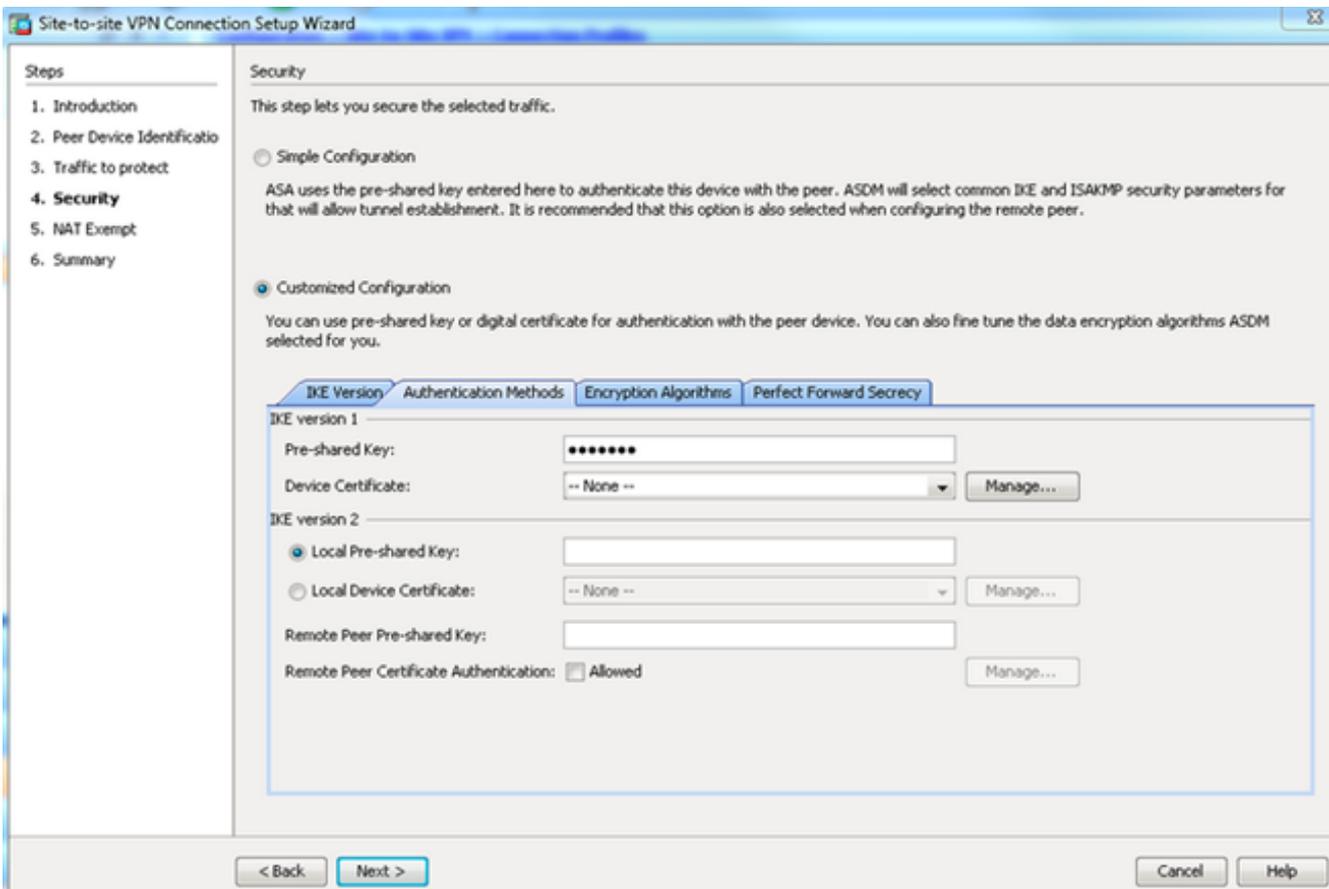
Pre-shared Key:

Customized Configuration

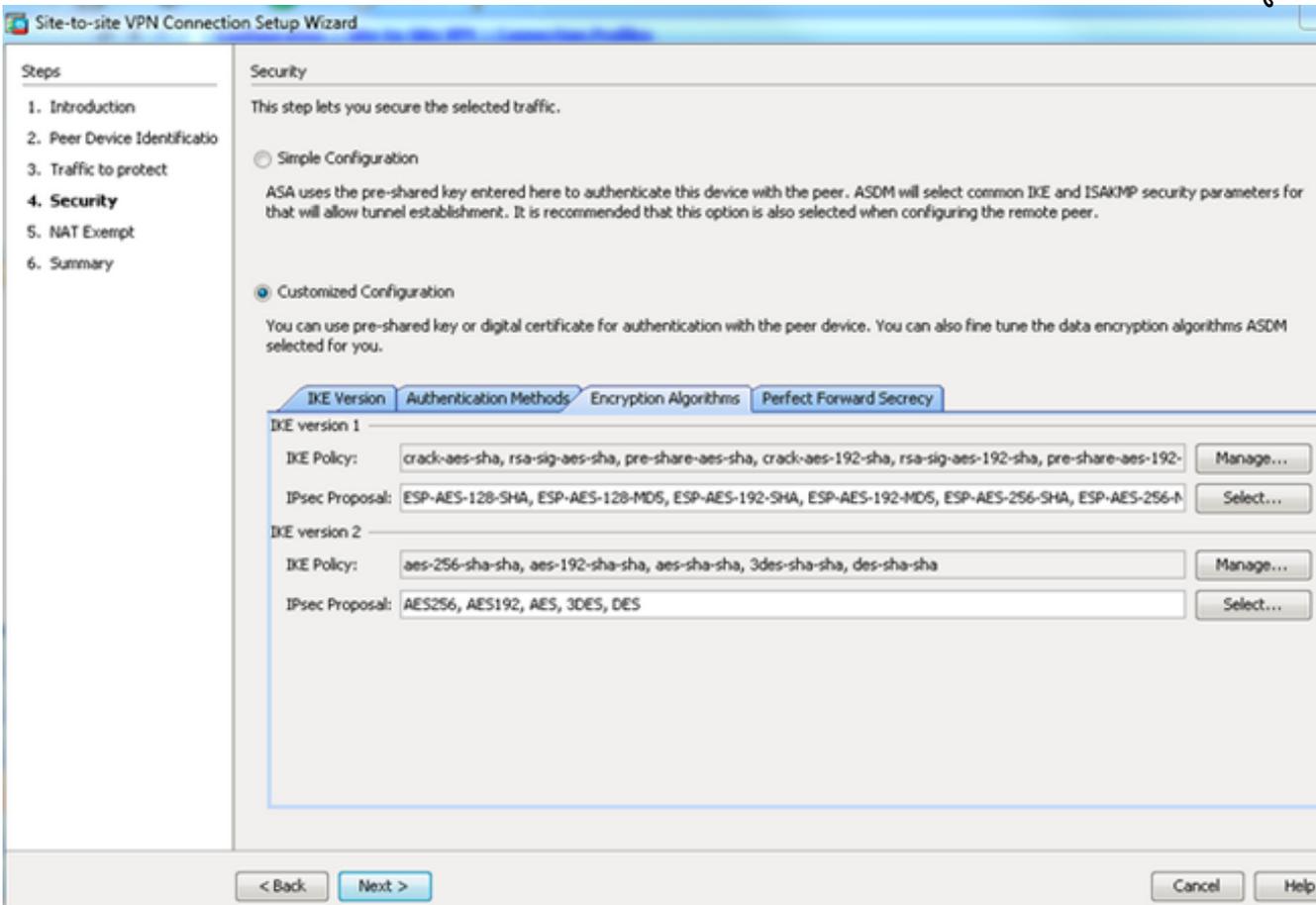
You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

< Back Next > Cancel Help

أو يمكنك تخصيص التكوين لتضمين سياسة IKE و IPsec التي تختارها. يجب أن يكون هناك سياسة مطابقة واحدة على الأقل بين الأقران: من علامة التبويب طرق المصادقة، أدخل مفتاح IKE الإصدار 1 المشترك مسبقاً في حقل المفتاح المشترك مسبقاً. في هذا مثال، هو Cisco123.



انقر فوق علامة التبويب خوارزميات التشفير.
 6. انقر فوق إدارة بجوار حقل نهج IKE، انقر فوق إضافة نهج IKE مخصص (phase-1) وتكوينه. انقر فوق موافق عند الانتهاء.



7. انقر فوق تحديد بجوار حقل مقترح IPsec وحدد عرض IPsec المطلوب. طقطقت بعد ذلك عندما أنت

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy

IKE version 1

IKE Policy: pre-share-aes-256-sha Manage...

IPsec Proposal: ESP-AES-256-SHA Select...

IKE version 2

IKE Policy: aes-256-sha-sha Manage...

IPsec Proposal: AES256, AES192, AES, 3DES, DES Select...

< Back Next > Cancel Help

إختباريا، يمكنك الانتقال إلى علامة التبويب "سرية إعادة التوجيه المثالية" وحدد خانة الاختيار تمكين سرية إعادة التوجيه الكاملة (PFS). طقطقت بعد ذلك عندما أنت

إنتهيت.

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy

Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future

Diffie-Hellman Group:

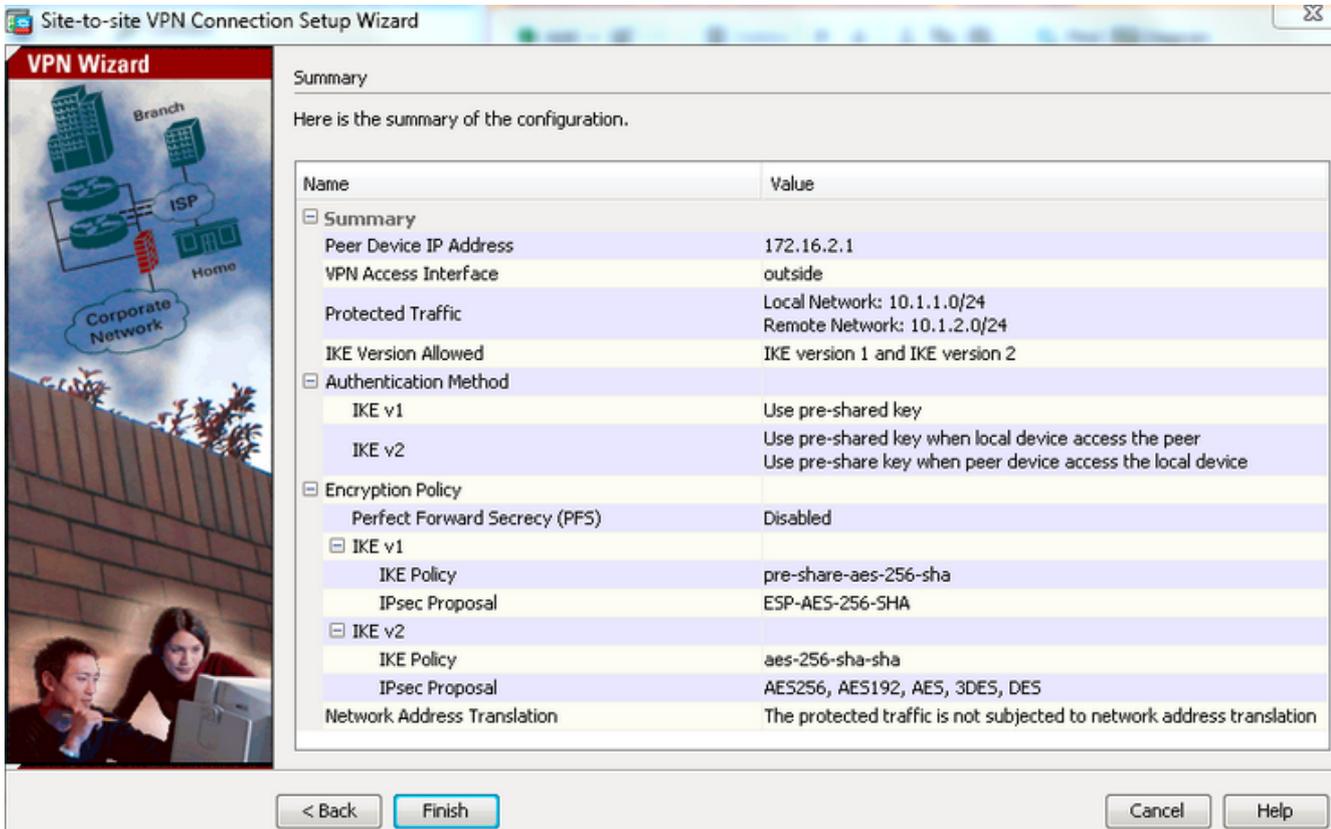
< Back Next > Cancel Help

8. حدد خانة الاختيار Except ASA side host/network من ترجمة العنوان لمنع حركة مرور النفق من بدء ترجمة عنوان الشبكة. أخترت إما محلي أو داخلي من القائمة المنسدلة in order to ثبتت القارن حيث شبكة

محلي يكون reachable. انقر فوق **Next**
(التالي).

The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window. The title bar reads 'Site-to-site VPN Connection Setup Wizard'. On the left, a 'Steps' pane lists the following steps: 1. Introduction, 2. Peer Device Identificatio, 3. Traffic to protect, 4. Security, 5. NAT Exempt (highlighted), and 6. Summary. The main area is titled 'NAT Exempt' and contains the text: 'This step allows you to exempt the local network addresses from network translation.' Below this text is a checked checkbox labeled 'Exempt ASA side host/network from address translation' and a dropdown menu currently set to 'inside'. At the bottom of the window, there are two buttons: '< Back' and 'Next >', with the 'Next >' button highlighted in blue.

9. يعرض ASDM ملخصا للشبكة الخاصة الظاهرية (VPN) التي تم تكوينها للتو. دققت وطققة إنجاز.



تكوين واجهة سطر الأوامر (CLI)

تكوين ASA المركزي (النظير الثابت)

1. قم بتكوين قاعدة no-nat/nat-exception لحركة مرور VPN كما يوضح هذا المثال:

```
object network 10.1.1.0-remote_network
  subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-inside_network
  subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
  destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
  no-proxy-arp route-lookup
```

2. قم بتكوين المفتاح المشترك مسبقا ضمن DefaultL2LGroup لمصادقة أي نظير ديناميكي L2L بعيد:

```
tunnel-group DefaultL2LGroup ipsec-attributes
  ikev1 pre-shared-key cisco123
```

3. تحديد سياسة المرحلة الثانية/ISAKMP:

```
crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

4. تعريف مجموعة تحويل المرحلة الثانية/سياسة IPsec:

```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```

5. قم بتكوين الخريطة الديناميكية باستخدام المعلمات التالية: مجموعة التحويل المطلوبة تمكين إدخال المسار

العكسي (RRI)، والذي يسمح لجهاز الأمان بمعرفة معلومات التوجيه للعملاء المتصلين (إختياري)

```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
  crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. ربط الخريطة الديناميكية بخريطة التشفير، وتطبيق خريطة التشفير وتمكين ISAKMP/IKEv1 على الواجهة

الخارجية:

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

ASA عن بعد (النظير الديناميكي)

1. تكوين قاعدة إستثناء NAT لحركة مرور VPN:

```
object network 10.1.1.0-inside_network
subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```

2. شكلت نفق-مجموعة لساكن إستاتيكي VPN نظير ومفتاح مشترك مسبقا.

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

3. تحديد سياسة المرحلة الأولى/ISAKMP:

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. تعريف مجموعة تحويل المرحلة الثانية/سياسة IPsec:

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

5. تكوين قائمة وصول تعرف حركة مرور/شبكة VPN المفيدة:

```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```

6. تكوين خريطة التشفير الثابتة باستخدام هذه المعلومات: قائمة وصول Crypto/VPN عنوان IPsec النظير

البعيد مجموعة التحويل المطلوبة

```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```

7. تطبيق خريطة التشفير وتمكين ISAKMP/IKEv1 على الواجهة الخارجية:

```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

التحقق من الصحة

أستخدم هذا القسم للتأكد من أن التكوين يعمل بشكل صحيح.

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

- `show crypto isakmp sa` - يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- `show crypto ipSec` - يعرض جميع رسائل IPsec الحالية.
- يوضح هذا القسم مثال مخرج التحقق لمكبيري الوصول (ASAs).

Central-ASA#show crypto isakmp sa

:IKEv1 SAs

Active SA: 1

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

Total IKE SA: 1

		IKE Peer: 172.16.1.1	1
Type	: L2L	Role	: responder
Rekey	: no	State	: MM_ACTIVE

Central-ASA# show crypto ipsec sa

interface: outside

Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

(local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0

(remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0

current_peer: 172.16.1.1

pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4#
 pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4#
 pkts compressed: 0, #pkts decompressed: 0#
 pkts not compressed: 4, #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#
 TFC rcvd: 0, #TFC sent: 0#
 Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0#
 send errors: 0, #recv errors: 0#

local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0

path mtu 1500, ipsec overhead 74(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: 30D071C0

current inbound spi : 38DA6E51

:inbound esp sas

(spi: 0x38DA6E51 (953839185

transform: esp-aes-256 esp-sha-hmac no compression

{ ,in use settings ={L2L, Tunnel, IKEv1

slot: 0, conn_id: 28672, crypto-map: outside_dyn_map

(sa timing: remaining key lifetime (kB/sec): (3914999/28588

IV size: 16 bytes

replay detection support: Y

:Anti replay bitmap

0x00000000 0x0000001F

:outbound esp sas

(spi: 0x30D071C0 (818966976

transform: esp-aes-256 esp-sha-hmac no compression

{ ,in use settings ={L2L, Tunnel, IKEv1

slot: 0, conn_id: 28672, crypto-map: outside_dyn_map

(sa timing: remaining key lifetime (kB/sec): (3914999/28588

IV size: 16 bytes

replay detection support: Y

:Anti replay bitmap

0x00000000 0x00000001

Remote-ASA#show crypto isakmp sa

:IKEv1 SAs

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

IKE Peer: 172.16.2.1 1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

Remote-ASA#show crypto ipsec sa

interface: outside

Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

access-list outside_cryptomap extended permit ip 10.1.1.0

255.255.255.0 10.1.2.0 255.255.255.0

(local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0

(remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0

current_peer: 172.16.2.1

pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4#

pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4#

pkts compressed: 0, #pkts decompressed: 0#

pkts not compressed: 4, #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#

TFC rcvd: 0, #TFC sent: 0#

Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0#

send errors: 0, #recv errors: 0#

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0

path mtu 1500, ipsec overhead 74(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: 38DA6E51

current inbound spi : 30D071C0

:inbound esp sas

(spi: 0x30D071C0 (818966976

transform: esp-aes-256 esp-sha-hmac no compression

{ ,in use settings ={L2L, Tunnel, IKEv1

slot: 0, conn_id: 8192, crypto-map: outside_map

(sa timing: remaining key lifetime (kB/sec): (4373999/28676

IV size: 16 bytes

replay detection support: Y

:Anti replay bitmap

0x00000000 0x0000001F

:outbound esp sas

(spi: 0x38DA6E51 (953839185

transform: esp-aes-256 esp-sha-hmac no compression

{ ,in use settings ={L2L, Tunnel, IKEv1

slot: 0, conn_id: 8192, crypto-map: outside_map

(sa timing: remaining key lifetime (kB/sec): (4373999/28676

IV size: 16 bytes

replay detection support: Y

:Anti replay bitmap

0x00000000 0x00000001

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمخرج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

أستخدم هذه الأوامر كما هو موضح:

```
<clear crypto ikev1 sa <peer IP address
.Clears the Phase 1 SA for a specific peer
```

تحذير: يعد الأمر **clear crypto isakmp sa** متطفلا لأنه يعمل على مسح جميع أنفاق شبكات VPN النشطة.

في الإصدار 8.0(3) من برنامج PIX/ASA والإصدارات الأحدث، يمكن مسح IKE SA فردي باستخدام الأمر **clear vpn-sessiondb <peer ip address <crypto isakmp sa <logoff tunnel-group <tunnel-group-name**. في إصدارات البرامج الأقدم من 8.0(3)، أستخدم الأمر **vpn-sessiondb** لمسح شبكات IKE و IPsec SAs لنفق واحد.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
[Do you want to logoff the VPN session(s)? [confirm
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

```
<clear crypto ipsec sa peer <peer IP address
.Clears the required Phase 2 SA for specific peer !!!
<debug crypto condition peer < Peer address
.Set IPsec/ISAKMP debug filters !!!
<debug crypto isakmp sa <debug level
.Provides debug details of ISAKMP SA negotiation !!!
<debug crypto ipsec sa <debug level
Provides debug details of IPsec SA negotiations !!!
undebg all
To stop the debugs !!!
```

تصحيح الأخطاء المستخدمة:

```
<debug cry condition peer <remote peer public IP
debug cry ikev1 127
debug cry ipsec 127
```

نظام ASA عن بعد (البادئ)

دخلت هذا ربط-tracer أمر in order to بدأت النفق:

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

.IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
:IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
.IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
(Crypto map (outside_map ,10.1.2.0
:
```

```
.
(Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0
+ (with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13)
VENDOR (13) + NONE (0) total length : 172
(Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0
(with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0
total length : 132
:
.
(Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0
+ (with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
(Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0
+ (with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
...<skipped>
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
+ (payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13)
NONE (0) total length : 96
,Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
VENDOR (13) + NONE (0) total length : 96 +
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
,Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
,Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED

Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
:Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy ID
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE)
ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 + (10)
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
+ (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10)
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
,Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
,Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
```

,Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1
(Security negotiation complete for LAN-to-LAN Group (172.16.2.1
Initiator, **Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51**

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76)

,Jan 19 22:00:06 [IKEv1]Group = **172.16.2.1, IP = 172.16.2.1**
(**PHASE 2 COMPLETED** (msgid=c45c7b30

(مستجيب) Central-ASA

(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0
+ (with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13)
VENDOR (13) + NONE (0) total length : 172

(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length :

(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0
(with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304 +

Jan 20 12:42:35 [IKEv1]IP = **172.16.1.1, Connection landed on tunnel_group**
DefaultL2LGroup

,Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1
...Generating keys for Responder

(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0
+ (with payloads : HDR + KE (4) + NONCE (10)
(VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20)
NONE (0) total length : 304

(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0
(with payloads : HDR + ID (5) + HASH (8)
IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 +

,Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1
ID_IPV4_ADDR ID received172.16.1.1

(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0
+ (with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
VENDOR (13) + NONE (0) total length : 96

Jan 20 12:42:35 [IKEv1]Group = **DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**

:Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM**
msg id = c45c7b30

Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
+ (RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1)
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200

Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote**
,IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0
:Protocol 0, Port 0

,Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup

```

IP = 172.16.1.1, Received local
,IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0
,Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
,Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
:Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0
.
(Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED (0)
:Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
,negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder
:Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0
.
,Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1
(PHASE 2 COMPLETED (msgid=c45c7b30
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0

```

معلومات ذات صلة

- [مراجع أوامر سلسلة ASA من Cisco](#)
- [صفحة دعم مفاوضات IPsec/بروتوكولات IKE](#)
- [طلبات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - نظام Cisco](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسملا اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچي ف ني م دختسم لل معد ي و تحم مي دقتل ل ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 ئ 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 أ ل ا ي ز ي ل ج ن إ ل ا دن ت س م ل ا