

Cisco هجوم ىل Cisco VPN 3000 زكرم نيوكت

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوينات
تكوين مركز VPN
التحقق من الصحة
على الموجه
على مركز الشبكة الخاصة الظاهرية (VPN)
استكشاف الأخطاء وإصلاحها
على الموجه
مشكلة - تتعذر بدء النفق
PFS
معلومات ذات صلة

المقدمة

يوضح هذا التكوين النموذجي كيفية توصيل شبكة خاصة خلف موجه يعمل ببرنامج Cisco IOS® Software بشبكة خاصة خلف مركز Cisco VPN 3000. تعرف الأجهزة الموجودة على الشبكات بعضها البعض من خلال العناوين الخاصة بها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- Cisco 2611 مسحاج تخديد مع Cisco IOS برمجية إطلاق 12.3(1). ملاحظة: تأكد من تثبيت موجهات سلسلة 2600 من Cisco باستخدام صورة VPN IPsec التي تدعم ميزة VPN.
 - مركز Cisco VPN 3000 مع 4.0.1 b
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين مسموح (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.](#)

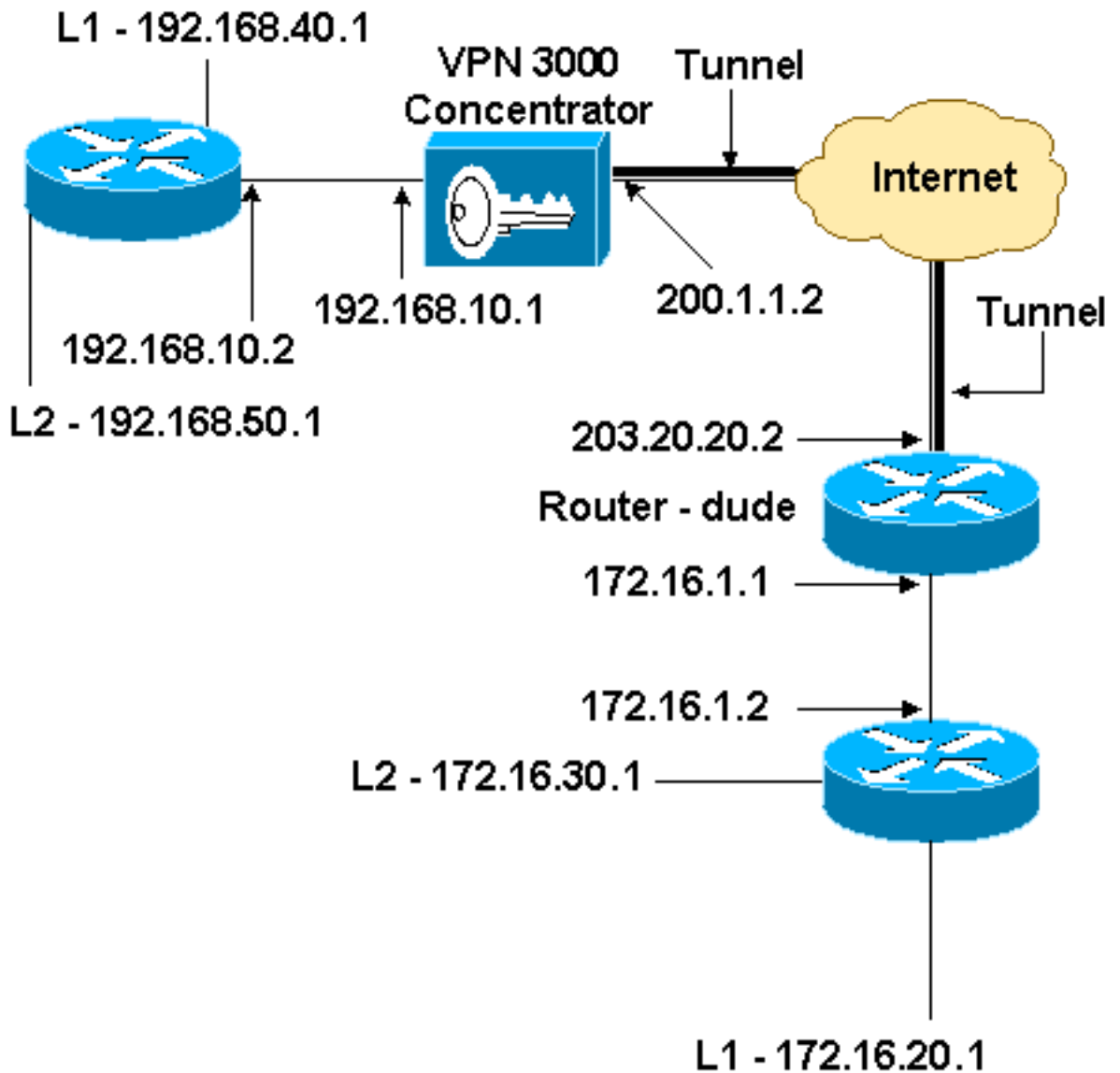
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي.



التكوينات

تكوين الموجه

```

                                version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
IKE policies. crypto isakmp policy 1 ---!!
    encr 3des
    hash md5
    authentication pre-share
    group 2
crypto isakmp key cisco123 address 200.1.1.2
IPsec policies. crypto ipsec transform-set to_vpn ---!!
    esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
    set peer 200.1.1.2
    set transform-set to_vpn
Traffic to encrypt. match address 101 ---!
!
interface Ethernet0/0
ip address 203.20.20.2 255.255.255.0
ip nat outside
half-duplex
crypto map to_vpn
!
interface Ethernet0/1
ip address 172.16.1.1 255.255.255.0
ip nat inside
half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
Traffic to encrypt. access-list 101 permit ip ---!!
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255

```

```

192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
Traffic to except from the NAT process. access-list ---!
110 deny ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end

```

تكوين مركز VPN

في هذا الإعداد المعملي، يتم الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) أولاً من خلال منفذ وحدة التحكم ويتم إضافة تكوين أدنى حتى يمكن إجراء التكوين الإضافي من خلال واجهة المستخدم الرسومية (GUI).

أخترت إدارة <reboot> نظام <reboot> جدول <reboot> يعيد مع مصنع/تقصير تشكيل أن يضمن أن هناك ما من تشكيل حالي في ال VPN مركز.

يظهر مركز VPN في التكوين السريع، ويتم تكوين هذه العناصر بعد إعادة التمهيد:

- الوقت/التاريخ
 - الواجهات/الأقنعة في التكوين <الواجهات (عام=200.1.1.2/24، خاص=192.168.10.1/24)>
 - البوابة الافتراضية في التكوين <النظام> (200.1.1.1) (ip routing > default_gateway)
- عند هذه النقطة، يمكن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال HTML من الشبكة الداخلية.

ملاحظة: نظراً لأن مركز الشبكة الخاصة الظاهرية (VPN) تتم إدارته من الخارج، فيجب عليك أيضاً تحديد:

- تكوين <واجهات <2-عام > تحديد عامل تصفية 1 > IP. خاص (افتراضي).
- إدارة <حقوق الوصول > قائمة التحكم في الوصول < إضافة مدير محطة عمل لإضافة عنوان IP الخاص ب المدير الخارجي.

لا يكون هذا ضروريا ما لم تقم بإدارة مركز VPN من الخارج.

1. أخترت تشكيل <قارن أن يعيد فحصت القارن بعد أن يشكل أنت ال

.gui

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• Power Supplies

2. أخترت تشكيل <نظام <ip routing <تقصير مدخل أن يشكل التقصير (إنترنت) مدخل والتقصير نفق (داخل) مدخل ل IPsec أن يبلغ الآخر شبكة فرعية في خاص.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

Apply Cancel

3. أخترت تشكيل <سياسة إدارة <شبكة قائمة أن يخلق الشبكة قائمة أن يعين الحركة مرور أن يكون يشفر. هذه هي الشبكات المحلية:

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
192.168.10.0/0.0.0.255
192.168.40.0/0.0.0.255
192.168.50.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Apply

Cancel

Generate Local List

هذه هي الشبكات
البعيدة:

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Apply

Cancel

Generate Local List

4. عند اكتمالها، هذان هما قائمتا الشبكة: **ملاحظة:** إذا لم يظهر نفق IPsec، فتتحقق لمعرفة ما إذا كانت حركة المرور المفيدة تتطابق على كلا الجانبين. يتم تحديد حركة المرور المثيرة للاهتمام بواسطة قائمة الوصول على مربعات Router و PIX. ويتم تعريفها بواسطة قوائم الشبكة في مركزات الشبكة الخاصة الظاهرية (VPN).

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

5. أخترت تشكيل نظام tunneling بروتوكول IPSec lan-to-LAN وعينت ال LAN-to-LAN نطق.

Add a new IPSec LAN-to-LAN connection.

Enable

Check to enable this LAN-to-LAN connection.

Name

Enter the name for this LAN-to-LAN connection.

Interface

Select the interface for this LAN-to-LAN connection.

Connection Type

Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.

Peers

203.20.20.2

Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.

Digital Certificate

Select the digital certificate to use.

Certificate Transmission Entire certificate chain

Choose how to send the digital certificate to the IKE peer.

Identity certificate only

Preshared Key

Enter the preshared key for this LAN-to-LAN connection.

Authentication

Specify the packet authentication mechanism to use.

Encryption

Specify the encryption mechanism to use.

IKE Proposal

Select the IKE Proposal to use for this LAN-to-LAN connection.

Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.	
Network List <input type="text" value="vpn_local_subnet"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.	
Network List <input type="text" value="router_subnet"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	
<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

6. بعد النقر فوق **تطبيق**، يتم عرض هذا الإطار مع التكوين الآخر الذي يتم إنشاؤه تلقائياً كنتيجة لتكوين نفق شبكة LAN إلى شبكة LAN.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

Authentication Server Internal
Group 203.20.20.2
Security Association L2L: to_router
Filter Rules L2L: to_router Out
L2L: to_router In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.

يمكن عرض معلمات IPsec من شبكة LAN إلى شبكة LAN التي تم إنشاؤها مسبقاً أو تعديلها في التكوين < النظام> إنشاء قنوات البروتوكولات< IPsec من شبكة LAN إلى شبكة LAN.

This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to [User Management](#) and configure a Group and User. To configure NAT over LAN-to-LAN, go to [LAN-to-LAN NAT Rules](#).

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary [Network Lists](#) prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

LAN-to-LAN Connection	Actions
to_router (203.20.20.2) on Ethernet 2 (Public)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

7. أخترت تشكيل <نظام tunneling> بروتوكول <IKE> IPSec مقترح أن يؤكد النشاط .IKE

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="<< Activate"/> <input type="button" value="Deactivate >>"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient3DES-MD5-RSA CiscoVPNClient3DES-SHA-DSA CiscoVPNClient3DES-MD5-RSA-DH5 CiscoVPNClient3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

8. أخترت تشكيل <سياسة إدارة> حركة مرور إدارة <أمن إتحاد> أن يشاهد القائمة ميلان إلى جانب من أمن اقترانات.

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs	Actions
ESP-3DES-MD5	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	
L2L: to_router	

9. انقر على اسم اقتران الأمان، ثم انقر على **تعديل** للتحقق من اقترانات الأمان.

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	203.20.20.2	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

[التحقق من الصحة](#)

يسرد هذا القسم أوامر **show** المستخدمة في هذا التكوين.

[على الموجه](#)

يوفر هذا القسم معلومات يمكنك إستخدامها 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 ipSec—يعرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية.
 - show crypto isakmp sa— يعرض جميع اقترانات أمان تبادل مفتاح الإنترنت الحالية في نظير.
 - show crypto engine connection active—يعرض إتصالات الجلسة المشفرة النشطة الحالية لجميع محركات التشفير.
- يمكنك إستخدام أداة بحث أوامر IOS (للعلماء المسجلين فقط) للاطلاع على مزيد من المعلومات حول أوامر معينة.

على مركز الشبكة الخاصة الظاهرية (VPN)

أخترت تشكيل <نظام> <حدث> <صنف> يعدلأن يركض تسجيل. تتوفر هذه الخيارات:

- آيك
 - lkedbg
 - إيكيديكود
 - IPSEC
 - IPSECDBG
 - إيسيديكوده
- الخطورة إلى السجل = 13-1

الخطورة بالنسبة لوحدة التحكم = 3-1

حدد مراقبة < سجل الأحداث لاسترداد سجل الأحداث.

استكشاف الأخطاء وإصلاحها

على الموجه

أحلت معلومة مهم على Debug أمر قبل أن يحاول أنت أي يضبط أمر.

- debug crypto engine—يعرض حركة مرور البيانات التي يتم تشفيرها.
- debug crypto ipSec—يعرض مفاوضات IPsec للمرحلة 2.
- debug crypto isakmp—يعرض مفاوضات ISAKMP للمرحلة 1.

مشكلة - بتعذر بدء النفق

رسالة خطأ

```
SEV=3 AUTH/5 RPT=1863 10.19.187.229 14:37:45.430 10/26/2007 20932
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified
```

الحل

أتمت هذا الإجراء in order to شكلت العدد المرغوب من عمليات تسجيل الدخول المتزامنة أو ثبتت ال login متزامن

إلى 5 ل هذا SA:

انتقل إلى التكوين < إدارة المستخدم < مجموعات < تعديل 10.19.187.229 < عام < عمليات تسجيل الدخول المتزامنة وتغيير عدد عمليات تسجيل الدخول إلى 5.

PFS

في مفاوضات IPsec، تضمن سرية إعادة التوجيه الكاملة (PFS) عدم إرتباط كل مفتاح تشفير جديد بأي مفتاح سابق. إما أن تقوم بتمكين أو تعطيل PFS على كل من نظائر النفق. وإلا، لا يتم إنشاء نفق IPsec الخاص بشبكة LAN إلى شبكة (LAN (L2L في الموجهات.

لتحديد أنه يجب على IPsec طلب PFS عند طلب اقترانات أمان جديدة لإدخال خريطة التشفير هذا، أو أن IPsec يتطلب PFS عندما يستلم طلبات اقترانات أمان جديدة، أستخدم الأمر `set pfs` في وضع تكوين خريطة التشفير. لتحديد أنه لا يجب على IPsec طلب PFS، أستخدم الصيغة `no` من هذا الأمر.

```
[set pfs [group1 | group2  
no set pfs
```

بالنسبة لأمر مجموعة ملفات PFS:

- المجموعة 1 — يحدد أن IPsec يجب أن يستخدم مجموعة وحدات Diffie-Hellman الرئيسية ذات 768 بت عند إجراء تبادل Diffie-Hellman جديد.
 - المجموعة 2 — يحدد أن IPsec يجب أن يستخدم مجموعة وحدات Diffie-Hellman الرئيسية ذات 1024 بت عند إجراء تبادل Diffie-Hellman جديد.
- بشكل افتراضي، لا يتم طلب ملفات PFS. إذا لم يتم تحديد مجموعة باستخدام هذا الأمر، فسيتم استخدام المجموعة 1 كافتراضي.

مثال:

```
Router(config)#crypto map map 10 ipsec-isakmp  
Router(config-crypto-map)#set pfs group2
```

راجع [مرجع أمر أمان Cisco IOS](#) للحصول على مزيد من المعلومات حول الأمر `set pfs`.

معلومات ذات صلة

- [حلول استكشاف أخطاء الشبكة الخاصة الظاهرية \(VPN\) عبر بروتوكول IPsec للوصول عن بعد و L2L الأكثر شيوعاً](#)
- [مركزات Cisco VPN 3000 Series](#)
- [أجهزة Cisco VPN 3002 العملية](#)
- [مفاوضة IPsec/بروتوكولات IKE](#)
- [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