

# LAN ءكباش لى لـ LAN ءكباش نم IPsec ق فن لاثم عم هجوم و Cisco VPN 3000 زكرم نىب AES نىوكت

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [الرسم التخطيطى للشبكة](#)
- [التكوينات](#)
- [تكوين مركز VPN](#)
- [التحقق من الصحة](#)
- [التحقق من تكوين الموجه](#)
- [التحقق من تكوين مركز VPN](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [استكشاف أخطاء الموجه وإصلاحها](#)
- [استكشاف أخطاء مركز الشبكة الخاصة الظاهرية \(VPN\) وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بين مركز Cisco VPN 3000 وموجه Cisco مع معيار التشفير المتقدم (AES) كخوارزمية التشفير.

AES هو منشور جديد عن "معيار معالجة المعلومات الاتحادي" (FIPS) تم إنشاؤه بواسطة المعهد الوطني للمعايير والتكنولوجيا (NIST) لاستخدامه كطريقة تشفير. يحدد هذا المعيار خوارزمية تشفير AES المتماثل التي تستبدل معيار تشفير البيانات (DES) كتحويل للخصوصية لكل من IPsec و Internet Key Exchange (IKE). يحتوي AES على ثلاثة أطوال مفاتيح مختلفة، ومفتاح 128-بت (الافتراضي)، ومفتاح 192-بت، ومفتاح 256-بت. تضيف ميزة AES في Cisco IOS دعم لمعيار التشفير الجديد AES، مع وضع توصيل كتل التشفير (CBC)، إلى IPsec.

ارجع إلى [موقع مركز موارد أمان الكمبيوتر لـ NIST](#) للحصول على مزيد من المعلومات حول AES.

ارجع إلى [نفق IPsec من شبكة LAN إلى شبكة LAN بين مركز VPN 3000 ومثال تكوين جدار حماية PIX](#) للحصول على مزيد من المعلومات حول تكوين نفق من شبكة LAN إلى شبكة LAN بين مركز VPN 3000 وجدار حماية PIX.

ارجع إلى [مثال تكوين مركز VPN 3000 لـ IPsec Tunnel بين PIX 7.x و VPN 3000](#) للحصول على مزيد من المعلومات عندما يحتوي PIX على إصدار برنامج 7.1.

# المتطلبات الأساسية

## المتطلبات

يتطلب هذا المستند فهما أساسيا لبروتوكول IPsec. ارجع إلى [مقدمة عن تشفير IPsec](#) لمعرفة المزيد حول IPsec. تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- **متطلبات الموجه** - تم إدخال ميزة AES في البرنامج Cisco IOS Software، الإصدار 12.2(13)T. لتمكين AES، يجب أن يدعم الموجه لديك IPsec ويشغل صورة IOS باستخدام المفاتيح الطويلة "k9" (النظام الفرعي "k9"). **ملاحظة:** يتوفر أيضا دعم الأجهزة ل AES على الوحدات النمطية VPN للتعجيل Cisco 2600XM و Cisco 2691 و 3725 و 3745 AES. لا تتضمن هذه الميزة أي تأثيرات في التكوين ويتم تحديد وحدة الجهاز النمطية تلقائيا إذا كان كلاهما متوفرا.
- **متطلبات مركز الشبكة الخاصة الظاهرية (VPN)** - تم تقديم دعم البرنامج لميزة AES في الإصدار 3.6. يتم توفير دعم الأجهزة من خلال معالج التشفير الجديد المحسن والقابل للتطوير (SEP-E). لا تتضمن هذه الميزة أي تأثيرات تكوين. **ملاحظة:** في الإصدار 3.6.3 من مركز Cisco VPN 3000، لا تتفاوض الأنفاق إلى AES بسبب معرف تصحيح الأخطاء من [CSCdy88797](#) Cisco ([للعلماء المسجلين فقط](#)). تم حل هذا من الإصدار 3.6.4. **ملاحظة:** يستخدم مركز Cisco VPN 3000 إما وحدات SEP أو SEP-E، وليس كلاهما. لا تقم بتهيئة كليهما على نفس الجهاز. إذا قمت بتهيئة وحدة SEP-E على مركز VPN يحتوي بالفعل على وحدة SEP، فإن مركز VPN يعجز وحدة SEP ويستخدم وحدة SEP فقط.

## المكونات المستخدمة

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

- Cisco 3600 sery مسحاج تخديد مع cisco ios برمجية إطلاق 12.3(5)
  - مركز Cisco VPN 3060 مع برنامج الإصدار 4.0.3
- 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.](#)

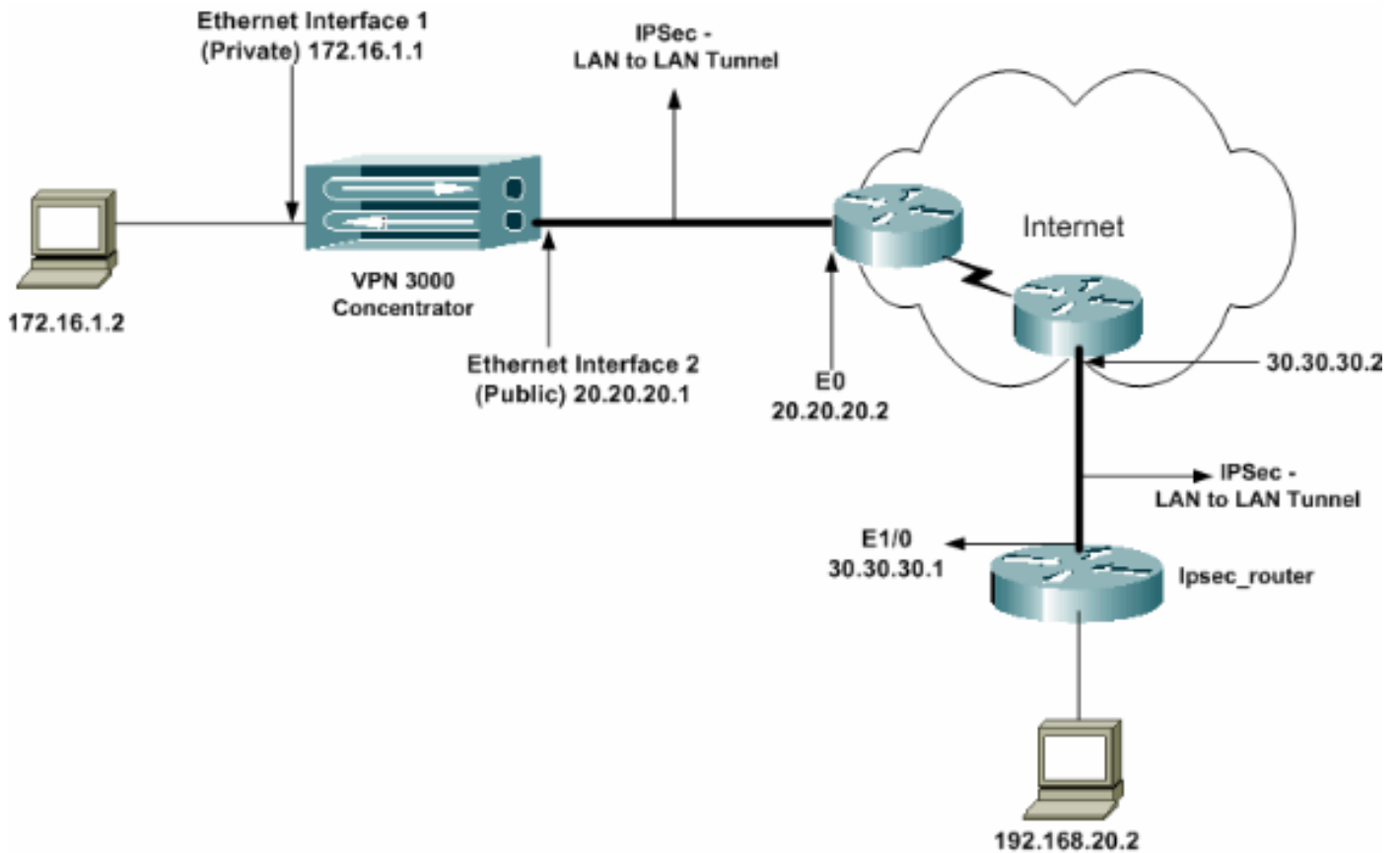
## التكوين

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

**ملاحظة:** استخدم [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:



## التكوينات

يستخدم هذا المستند التكوينات التالية:

- [موجه IPsec](#)
- [مركز VPN](#)

### تكوين IPsec\_Router

```

version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
Configuration for IKE policies. crypto isakmp ---!
policy 1
Enables the IKE policy configuration (config- ---!
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
Specifies the encryption algorithm as AES with a ---!
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
Specifies the preshared key "cisco123" which !--- ---!

```

```

! .should be identical at both peers
Configuration for IPsec policies. crypto ipsec ---!
    security-association lifetime seconds 28800
    Specifies the lifetime of the IPsec security ---!
association (SA). ! crypto ipsec transform-set vpn esp-
    aes 256 esp-md5-hmac
    Enables the crypto transform configuration mode, ---!
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
    isakmp
    Indicates that IKE is used to establish the IPsec ---!
    SA for protecting !--- the traffic specified by this
    crypto map entry. set peer 20.20.20.1
    Sets the IP address of the remote end (VPN ---!
    Concentrator). set transform-set vpn
    Configures IPsec to use the transform-set "vpn" ---!
    defined earlier. ! !--- Specifies the traffic to be
    encrypted. match address 110
!
    interface Ethernet1/0
    ip address 30.30.30.1 255.255.255.0
    ip nat outside
    half-duplex
    crypto map vpn
    Configures the interface to use the crypto map ---!
    ! ."vpn" for IPsec
    interface FastEthernet2/0
    ip address 192.168.20.1 255.255.255.0
    ip nat inside
    duplex auto
    speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 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 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
    172.16.0.0 0.0.255.255
    This crypto ACL-permit identifies the matching ---!
    traffic !--- flows to be protected via encryption. !---
    Specifies the traffic not to be encrypted. access-list
    120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
    0.0.255.255
    This crypto ACL-deny identifies the matching ---!
    ! .traffic flows not to be encrypted
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
    The access control list (ACL) used in the NAT ---!
    configuration exempts !--- the LAN-to-LAN traffic from
    the NAT process, !--- but allows all traffic going to
    ! .the Internet to be translated
    route-map nonat permit 10
    The traffic flows not encrypted from the !--- peer ---!
    network are allowed. match ip address 120
!
    line con 0
    line aux 0
    line vty 0 4
    login
!

```

ملاحظة: على الرغم من أن صياغة قائمة التحكم في الوصول (ACL) لم تتغير، إلا أن المعاني مختلفة قليلا لقوائم التحكم في الوصول (ACL) المشفرة. في قوائم التحكم في الوصول (ACL) المشفرة، يحدد السماح أنه يجب تشفير الحزم المطابقة، بينما يحدد الرفض أن الحزم المطابقة لا تحتاج إلى التشفير.

## تكوين مركز VPN

لا يتم برمجة مراكز VPN مسبقا باستخدام عناوين IP في إعدادات المصنع الخاصة بها. أنت يضطر استعملت الوحدة طرفية للتحكم مينا أن بشكل التشكيل أولي أي يكون baser أمر خط قارن (CLI). ارجع إلى [تكوين مراكز VPN من خلال وحدة التحكم](#) للحصول على معلومات حول كيفية التكوين من خلال وحدة التحكم.

بعد تكوين عنوان IP على واجهة إيثرنت 1 (الخاصة)، يمكن تكوين الباقي إما باستخدام CLI أو من خلال واجهة المستعرض. تدعم واجهة المستعرض كلا من HTTP و HTTP عبر طبقة مأخذ التوصيل الآمنة (SSL).

يتم تكوين هذه المعلمات من خلال وحدة التحكم:

- **الوقت/التاريخ - الوقت والتاريخ الصحيحان مهمان للغاية.** فهي تساعد على ضمان دقة إدخالات التسجيل والمحاسبة، وأن النظام يمكنه إنشاء شهادة أمان صالحة.
  - **واجهة Ethernet 1 (الخاصة) - عنوان IP وقناع (من مخطط الشبكة 24/172.16.1.1).**
- عند هذه النقطة، يمكن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال متصفح HTML من الشبكة الداخلية. أحلت لمعلومة على بشكل ال VPN مركز في CLI أسلوب، [تشكيل سريع يستعمل CLI](#).

1. اكتب عنوان IP الخاص بالواجهة الخاصة من مستعرض الويب لتمكين واجهة واجهة المستخدم الرسومية (GUI). انقر على أيقونة **حفظ ما يلزم** لحفظ التغييرات في الذاكرة. اسم المستخدم وكلمة المرور الافتراضيان في المصنع هما "admin" وهو أمر حساس لحالة الأحرف.

The screenshot shows the web interface for the VPN 3000 Concentrator Series Manager. The page has a header with 'VPN 3000 Concentrator Series Manager' and navigation links for 'Main | Help | Support | Logout'. Below the header, it indicates 'Logged in: admin' and 'Configuration | Administration | Monitoring'. The main content area is titled 'Main' and contains a welcome message: 'Welcome to the VPN 3000 Concentrator Manager.' It then provides instructions on how to use the interface, including a list of main functions: Configuration, Administration, and Monitoring. It also lists navigation options: Main, Help, Support, and Logout. At the bottom, it lists icons for Save, Save Needed, Reset, Restore, and Refresh.

2. بعد إضافة واجهة المستخدم الرسومية، حدد التكوين <الواجهات > إيثرنت 2 (عام) لتكوين واجهة إيثرنت 2.

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

General RIP OSPF Bandwidth

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	20.20.20.1	
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00:90:A4:00:41:F9	The MAC address for this interface.
	Filter	2: Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPsec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPsec encapsulation, fragment prior to interface transmission	
		<input type="radio"/> Fragment prior to IPsec encapsulation, with Path MTU Discovery (ICMP)	
		<input type="radio"/> Fragment prior to IPsec encapsulation, without Path MTU Discovery (Clear DF bit)	

Apply Cancel

3. حدد تكوين نظام توجيه IP البوابات الافتراضية تكوين البوابة الافتراضية (الإنترنت) وبوابة النفق الافتراضية (الداخلية) ل IPsec للوصول إلى الشبكات الفرعية الأخرى في الشبكة الخاصة. في هذا السيناريو، هناك شبكة فرعية واحدة فقط متوفرة على الشبكة الداخلية.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway 20.20.20.2 Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

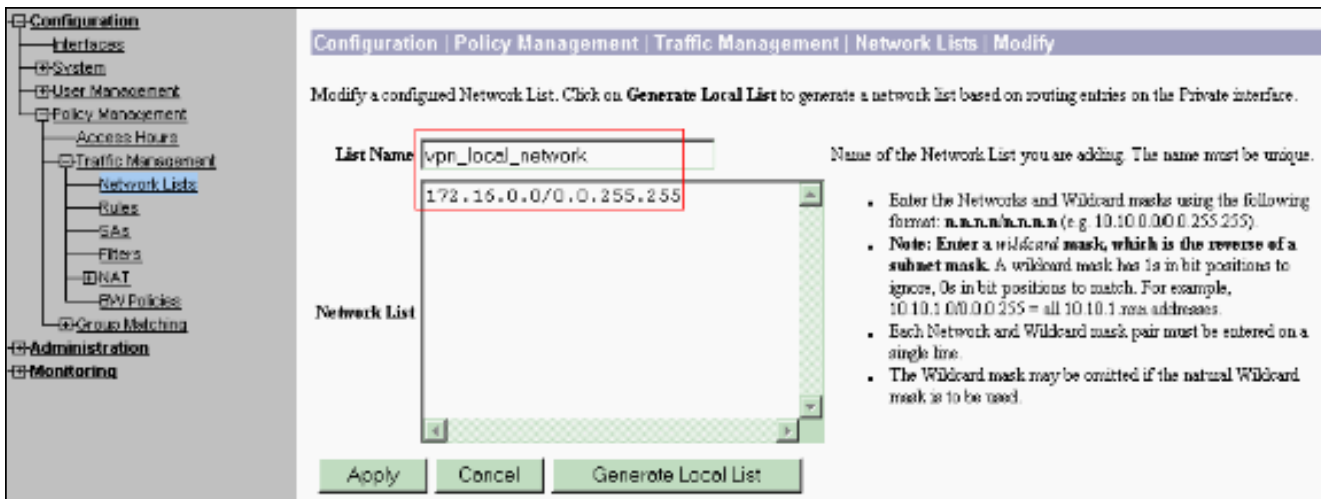
Metric 1 Enter the metric, from 1 to 16.

Tunnel Default Gateway 172.16.1.2 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

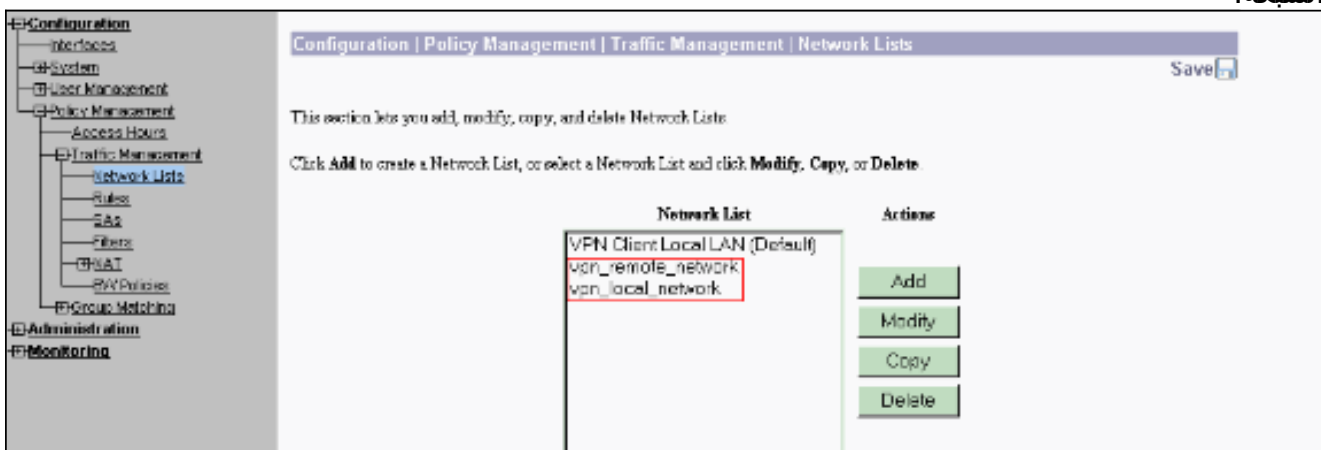
4. حدد تكوين إدارة السياسة إدارة حركة مرور البيانات <قوائم الشبكة> إضافة لإنشاء قوائم الشبكة التي تحدد حركة المرور التي سيتم تشفيرها. يمكن الوصول إلى الشبكات المذكورة في القائمة إلى الشبكة البعيدة. الشبكات الموضحة في القائمة أدناه هي شبكات محلية. يمكنك أيضا إنشاء قائمة الشبكة المحلية تلقائيا من خلال RIP عند النقر فوق إنشاء قائمة محلية.



5. الشبكات الموجودة في هذه القائمة هي شبكات بعيدة وتحتاج إلى تكوينها يدويا. للقيام بهذا الإجراء، أدخل الشبكة/حرف البدل لكل شبكة فرعية يمكن الوصول إليها.



عند اكتمالها، هذان هما قائمتا الشبكة:



6. حدد تكوين < نظام > بروتوكولات إنشاء قنوات < IPsec LAN إلى شبكة LAN > إضافة وتعريف نفق شبكة LAN إلى شبكة LAN. هذه النافذة لها ثلاثة أقسام. القسم العلوي خاص بمعلومات الشبكة والقسمين الأسفل مخصص لقوائم الشبكة المحلية والبعيدة. في قسم معلومات الشبكة، حدد تشفير AES ونوع المصادقة ومفتاح IKE واكتب المفتاح المشترك مسبقا. في الأقسام السفلى، أشر إلى قوائم الشبكة التي قمت بإنشائها بالفعل، على كل من القوائم المحلية والقوائم البعيدة على التوالي.



Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN | Add

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 *Originator-Only* connection may have multiple peers specified below.

Peers  Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originator-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  
 Identity certificate only Choose how to send the digital certificate to the IKE peer.

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.

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN | Add

Filter  Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.

IPsec NAT-T  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  Choose the bandwidth policy to apply to this LAN-to-LAN connection.

Routing  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  Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

Wildcard Mask  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 xxx addresses.

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

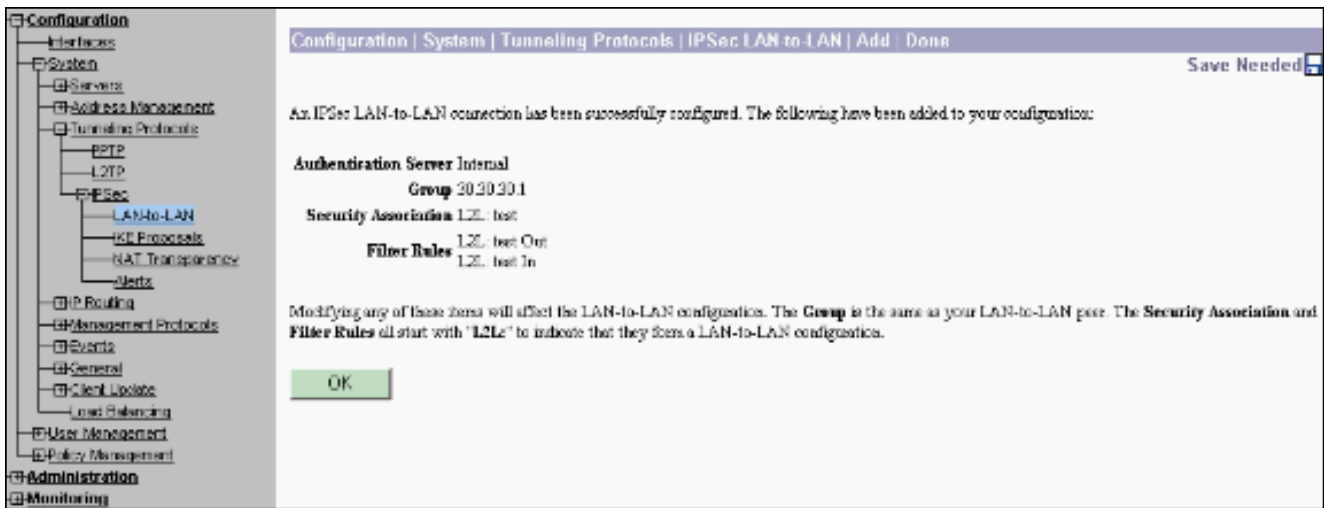
Network List  Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

Wildcard Mask  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 xxx addresses.

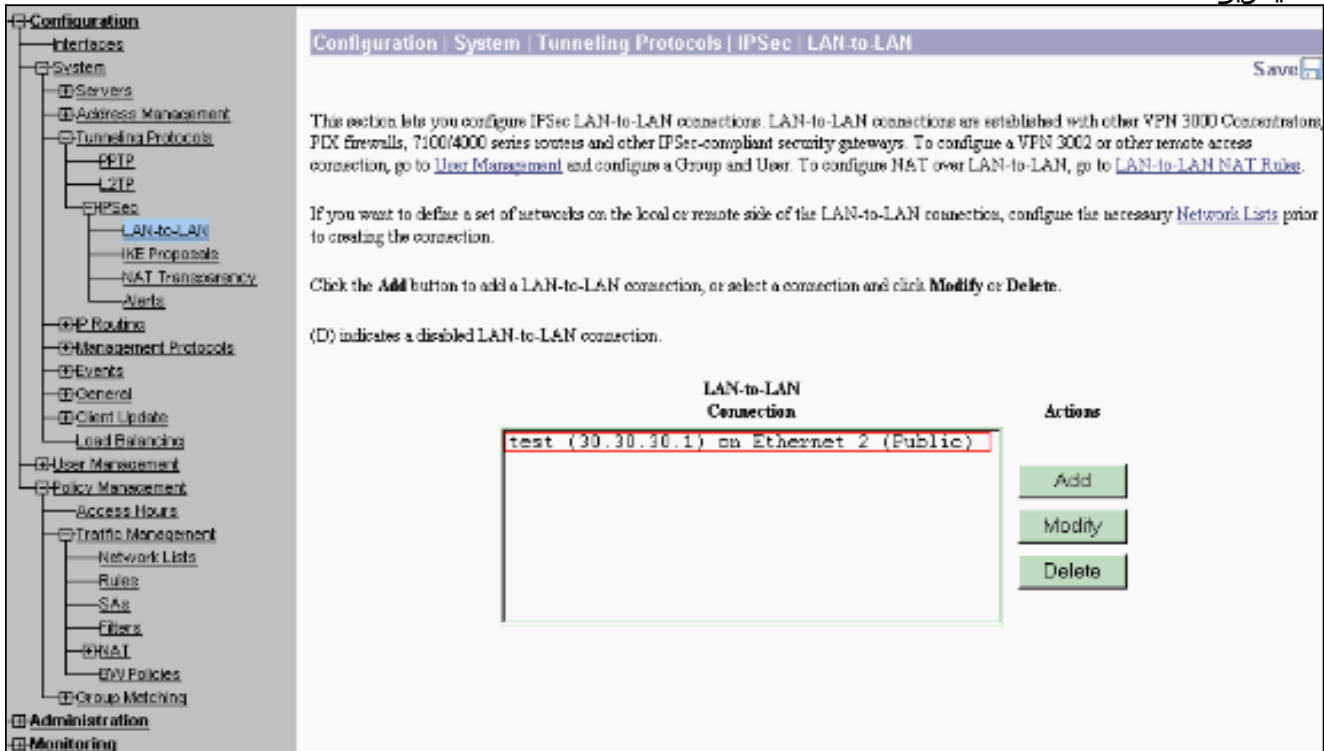
7. بعد النقر فوق **إضافة**، إذا كان إتصالك صحيحا، يتم تقديمك مع نافذة **IPsec LAN-to-LAN-Add-Done**. يقدم هذا نافذة خلاصة من النفق تشكيل معلومة. كما أنه يقوم بتكوين اسم المجموعة واسم SA واسم عامل التصفية تلقائيا. يمكنك تحرير أية معلمات في هذا الجدول.





عند هذه النقطة، تم إعداد نفق IPsec LAN إلى LAN ويمكنك بدء العمل. إذا، لسبب ما، لم يعمل النفق، يمكنك التحقق من المكونات الخاطئة.

8. يمكنك عرض معلمات IPsec التي تم إنشاؤها مسبقاً من شبكة LAN إلى شبكة LAN أو تعديلها عند تحديد التكوين < النظام > بروتوكولات الاتصال النفقي < IPsec من شبكة LAN إلى شبكة LAN. يوضح هذا الرسم "test" كاسم النفق والواجهة العامة للطرف البعيد هو 30.30.30.1 وفقاً للسيناريو.



9. وفي بعض الأحيان، قد لا يظهر النفق الخاص بك إذا كان اقتراح IKE الخاص بك مدرجاً في قائمة الاقتراحات غير النشطة. حدد تكوين < نظام > بروتوكولات إنشاء قنوات الاتصال النفقي < IPsec > مقترحات IKE لتكوين مقترح IKE النشط. إذا كان عرض IKE الخاص بك مدرجاً في قائمة "الاقتراحات غير النشطة"، يمكنك تمكينه عند تحديد عرض IKE والنقر فوق الزر **تنشيط**. في هذا الرسم، يوجد الاقتراح المحدد "IKE-AES256-SHA" في قائمة الاقتراحات النشطة.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

Save

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
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA IKE-3DES-MD5-RSA <b>IKE-AES256-SHA</b>	<< Activate Deactivate >> Move Up Move Down Add Modify Copy Delete	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA

10. حدد تكوين <إدارة السياسة> إدارة حركة مرور البيانات <اقترانات الأمان للتحقق من صحة معلمات SA.

Configuration | Policy Management | Traffic Management | Security Associations

Save

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 ESP-3DES-MD5-DH5 ESP-3DES-MD5-DH7 ESP-3DES-NONE ESP-AES128-SHA ESP-DES-MD5 ESP-L2TP-TRANSPORT ESP/IKE-3DES-MD5 <b>L2L test</b>	Add Modify Delete

11. طقطقت ال sa إسم (في هذه الحالة، L2L: إختيار)، وبعد ذلك طقطقت يعدل أن يدقق ال SAs. إذا لم تتطابق أي من المعلمات مع تكوين النظير البعيد، يمكن تغييرها هنا.

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name: L2L\_test Specify the name of this Security Association (SA).

Inheritance: From Rule Select the granularity of this SA.

---

**IPSec Parameters**

Authentication Algorithm: ESP/MD5/HMAC-128 Select the packet authentication algorithm to use.

Encryption Algorithm: AES-256 Select the ESP encryption algorithm to use.

Encapsulation Mode: Tunnel Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy: Disabled Select the use of Perfect Forward Secrecy.

Lifetime Measurement: True Select the lifetime measurement of the IPSec keys.

Data Lifetime: 10000 Specify the data lifetime in kilobytes (KB).

Time Lifetime: 28800 Specify the time lifetime in seconds.

---

**IKE Parameters**

Connection Type: Bidirectional The Connection Type and IKE Peer cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.

IKE Peers: 30 30 30 1

Negotiation Mode: Main Select the IKE Negotiation mode to use.

Digital Certificate: None (Use Pre-shared Keys) Select the Digital Certificate to use.

Certificate Transmission:
 Entire certificate chain. Choose how to send the digital certificates to the IKE peer.
 Identity certificate only

IKE Proposal: IKE:AES256-SHA Select the IKE Proposal to use as IKE initiator.

Apply Cancel

## التحقق من الصحة

## التحقق من تكوين الموجه

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

يتم دعم بعض أوامر العرض بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر العرض.

- **show crypto isakmp sa** — يعرض جميع شبكات IKE الحالية في نظير. تشير QM\_IDLE إلى أن SA لا يزال مصدقا عليه مع نظيره ويمكن استخدامه لمبادلات الوضع السريع اللاحقة. وهي في حالة من الهدوء والسكون.

```
ipsec_router#show crypto isakmp sa
```

```
dst          src          state  conn-id  slot
QM_IDLE     1           0      30.30.30.1  20.20.20.1
```

- **show crypto ipSec** — يعرض الإعدادات المستخدمة من قبل موجهات الخدمات (SAs) الحالية. تحقق من عناوين IP النظيرة والشبكات التي يمكن الوصول إليها عند كل من النهايات المحلية والبعيدة ومجموعة التحويل التي يتم استخدامها. يوجد إثنان من ESP SAs، واحد في كل اتجاه. بما أن مجموعات تحويل AH يتم استخدامها، فهي فارغة.

```
ipsec_router#show crypto ipsec sa
```

```
interface: Ethernet1/0
```

```
Crypto map tag: vpn, local addr. 30.30.30.1
```

```
:protected vrf
```

```
(local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0
```

```
(remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0
```

```

current_peer: 20.20.20.1:500
    {,PERMIT, flags={origin_is_acl
pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145#
    pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51#
        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.: 30.30.30.1, remote crypto endpt.: 20.20.20.1
    path mtu 1500, media mtu 1500
    current outbound spi: 54FA9805
        :inbound esp sas
            (spi: 0x4091292(67703442
                , transform: esp-256-aes esp-md5-hmac
                    { ,in use settings ={Tunnel
                        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
(sa timing: remaining key lifetime (k/sec): (4471883/28110
                    IV size: 16 bytes
                        replay detection support: Y
                            :inbound ah sas
                                :inbound pcp sas
                                    :outbound esp sas
                                        (spi: 0x54FA9805(1425709061
                                            , transform: esp-256-aes esp-md5-hmac
                                                { ,in use settings ={Tunnel
                                                    slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
(sa timing: remaining key lifetime (k/sec): (4471883/28110
                                                        IV size: 16 bytes
                                                            replay detection support: Y
                                                                :outbound ah sas
                                                                    :outbound pcp sas

```

• **show crypto engine connections active**—يعرض إتصالات الجلسة المشفرة النشطة الحالية لجميع محركات التشفير. كل معرف اتصال فريد. يتم عرض عدد الحزم التي يتم تشفيرها وفك تشفيرها في العمودين

الأخيرين.

```
ipsec_router#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt	
Ethernet1/0	30.30.30.1	set		HMAC_SHA+AES_256_C	0	0	1
Ethernet1/0	30.30.30.1	set		HMAC_MD5+AES_256_C	0	19	2000
Ethernet1/0	30.30.30.1	set		HMAC_MD5+AES_256_C	19	0	2001

## التحقق من تكوين مركز VPN

أكمل هذه الخطوات للتحقق من تكوين مركز VPN.

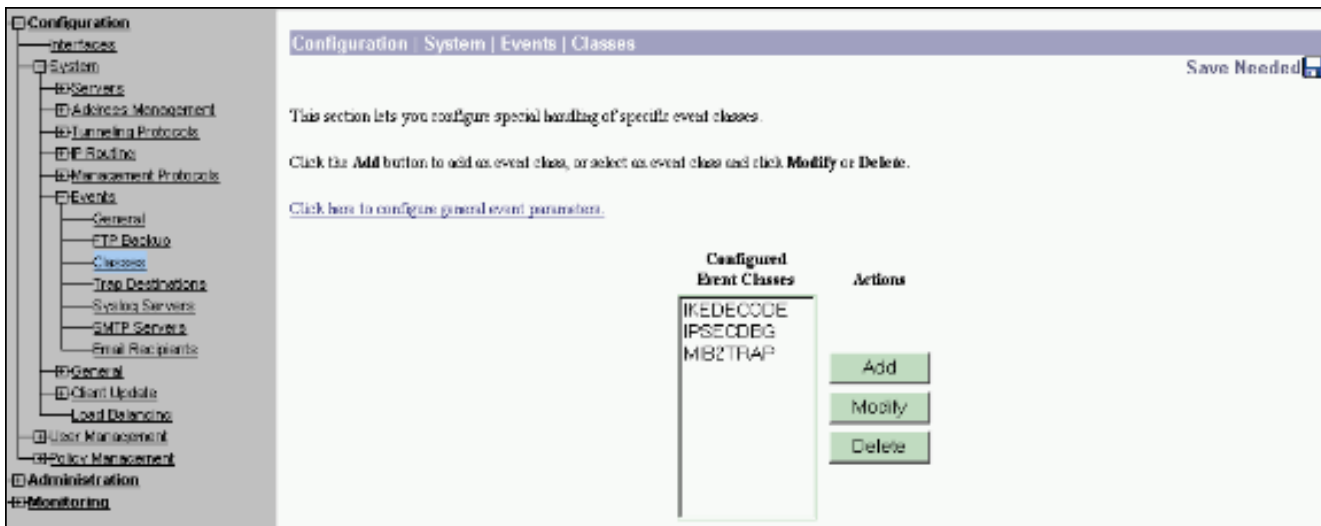
1. كما هو الحال لإظهار أوامر `show crypto isakmp sa` و `crypto ips sa` على الموجهات، يمكنك عرض إحصائيات IPsec و IKE عند تحديد المراقبة < الإحصائيات > IPsec على مركزات VPN.

Monitoring | Statistics | IPsec Thursday, 01 January 2004 19:32:36

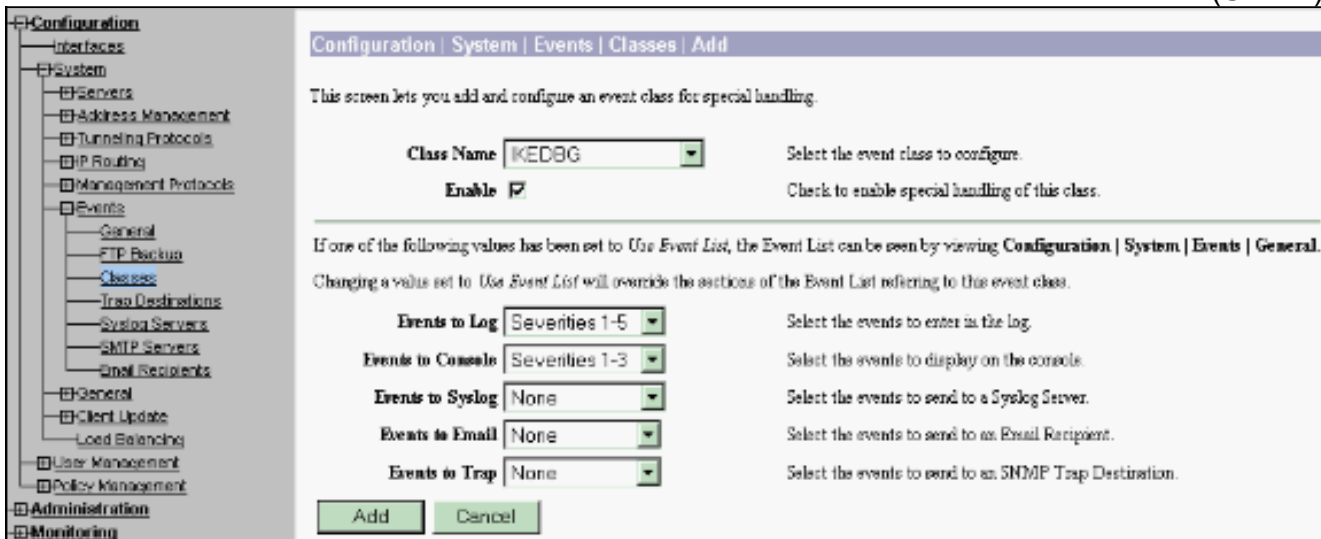
IKE (Phase 1) Statistics		IPsec (Phase 2) Statistics	
Action Tunnels	1	Action Tunnels	1
Total Tunnels	2	Total Tunnels	2
Received Bytes	5545268	Received Bytes	3608
Sent Bytes	5553204	Sent Bytes	5376
Received Packets	60187	Received Packets	145
Sent Packets	60299	Sent Packets	51
Received Packets Dropped	0	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	60084	Sent Packets Dropped	0
Sent Notifies	120172	Inbound Authentications	145
Received Phase-2 Exchanges	2	Failed Inbound Authentications	0
Sent Phase-2 Exchanges	49	Outbound Authentications	51
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	145
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	51
Phase-2 SA Delete Requests Received	0	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	30	System Capability Failures	0
Initiated Tunnels	0	No SA Failures	0
Failed Initiated Tunnels	0	Protocol Use Failures	0
Failed Remote Tunnels	0		
Authentication Failures	0		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
No-SA Failures	0		

2. وكما هو الحال مع الأمر `show crypto engine connections active` على الموجهات، يمكنك استخدام نافذة Administration-Sessions على مركز VPN لعرض المعلومات والإحصائيات لجميع اتصالات LAN إلى شبكة LAN النشطة عبر بروتوكول IPsec أو الأنفاق.





2. أثناء الإضافة، يمكنك أيضا تحديد مستوى الخطورة لكل فئة، استنادا إلى مستوى الخطورة الذي يتم إرسال التنبيه إليه. يمكن التعامل مع الإنذارات باستخدام إحدى هذه الأساليب: حسب السجل معروض على وحدة التحكمم الإرسال إلى خادم UNIX Syslog تم الإرسال كبريد إلكترونيتم إرسالها كفخ إلى خادم بروتوكول إدارة الشبكة البسيط (SNMP)



3. حدد مراقبة < سجل أحداث قابل للتصفية لمراقبة الإنذارات التي تم تمكينها.



Configuration

- Interfaces
- System
  - Services
  - Address Management
  - Tunneling Protocols
  - IP Routing
  - Management Protocols
  - Events
    - General
    - FTP Backlog
    - Classes
    - Trap Destinations
    - Syslog Servers
    - SMTP Servers
    - Email Recipients
  - General
  - Client Update
  - Load Balancing
- User Management
- Policy Management
- Administration
  - Monitoring
    - Routing Table
    - Dynamic Filters
    - Filterable Event Log
    - Live Event Log
  - System Status
  - Sessions
  - Statistics

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes  
 AUTH  
 AUTHDBG  
 AUTHDECODE

Severities: ALL  
 1  
 2  
 3

Client IP Address: 0.0.0.0

Event/Page: 100

Group: -All-

Direction: Oldest to Newest

Get Log Save Log Clear Log

```

37992 01/02/2004 11:58:29.540 SRV-F IKEDEBUG/0 RPT-61097 30.30.30.1
ISAKMP HEADER : | Version 1.0 |
Initiator Cookie(S):  A8 A8 8C 63 09 CA 58 25
Responder Cookie(S):  6D B2 66 02 86 CD 12 6C
Next Payload :  HASH (8)
Exchange Type :  Oakley Informational
Flags : 1 (ENCRYPT)
Message ID : a3905cad
Length : 92

37999 01/02/2004 11:58:29.540 SRV-F IKEDEBUG/0 RPT-61098 30.30.30.1
Notify Payload Decode :
DOT : IPSEC (1)
Protocol : ISAKMP (1)
Message : DPD 1-0-THREE-ACT (96137)
Spi : A8 A8 8C 63 09 CA 58 25 6D B2 66 02 86 CD 12 6C
Length : 32

38005 01/02/2004 11:58:49.540 SRV-F IKEDEBUG/0 RPT-61099 30.30.30.1
ISAKMP HEADER : | Version 1.0 |
Initiator Cookie(S):  A8 A8 8C 63 09 CA 58 25
Responder Cookie(S):  6B B2 66 02 86 CD 12 6C
Next Payload :  HASH (8)
Exchange Type :  Oakley Informational

```

CISCO SYSTEMS

## معلومات ذات صلة

- [معيار التشفير المتقدم \(AES\)](#)
- [وحدة تشفير VPN DES/3DES/AES](#)
- [عمليات تكوين نموذج IPsec](#)
- [صفحة دعم عميل Cisco VPN 3000 Series](#)
- [صفحة دعم مفاوضة IPsec/بروتوكولات IKE](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ 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 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 (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا