تكوين مركز VPN 3000 للاتصال بعميل VPN باستخدام الشهادات

المحتويات

المقدمة

يتضمن هذا المستند إرشادات خطوة بخطوة حول كيفية تكوين مركزات Cisco VPN 3000 Series مع عملاء VPN باستخدام الشهادات.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco VPN 3000 Concentrator نسخة 4.0.4a.

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.

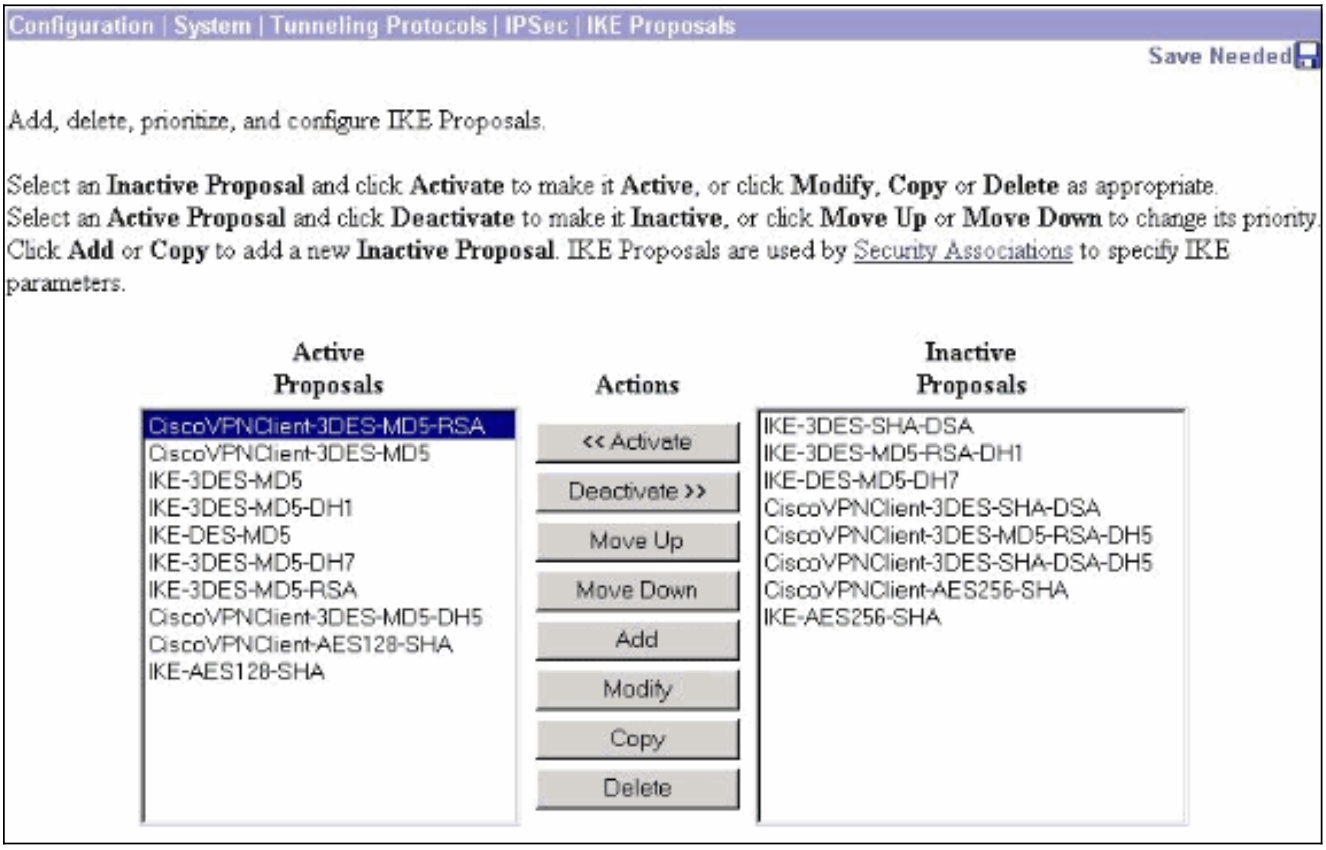
الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

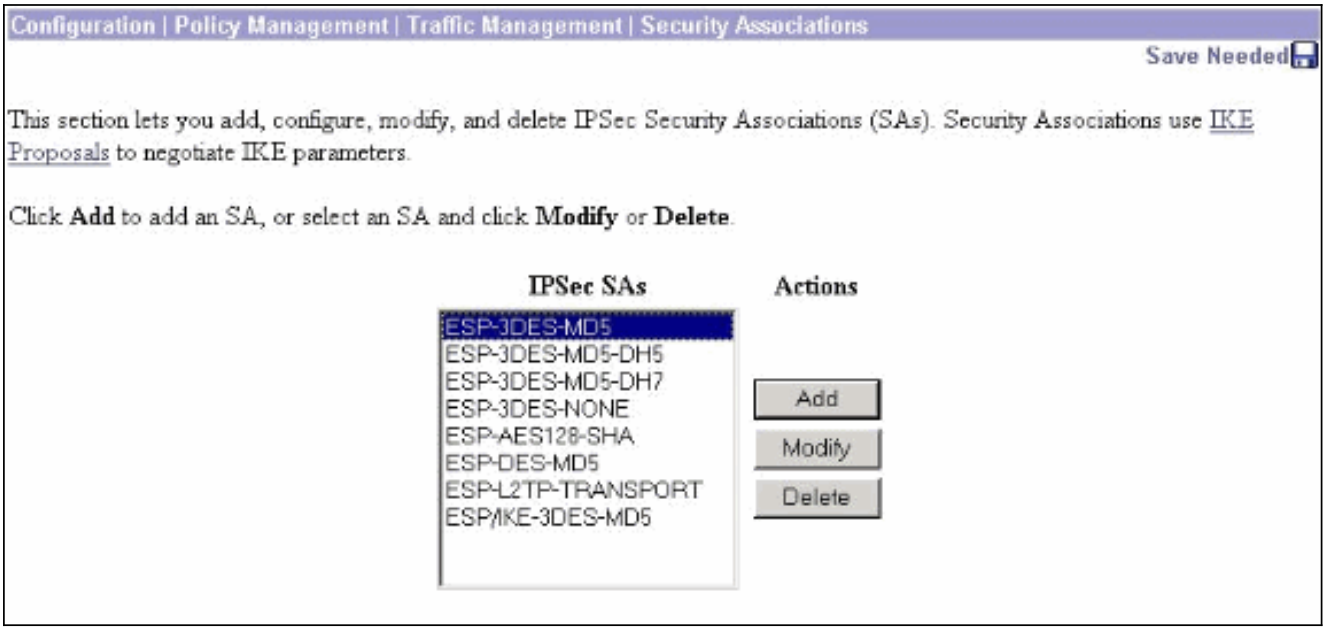
شهادات مركز VPN 3000 لعملاء VPN

أتمت هذا steps in order to شكلت VPN 3000 مركز شهادة ل VPN زبون.

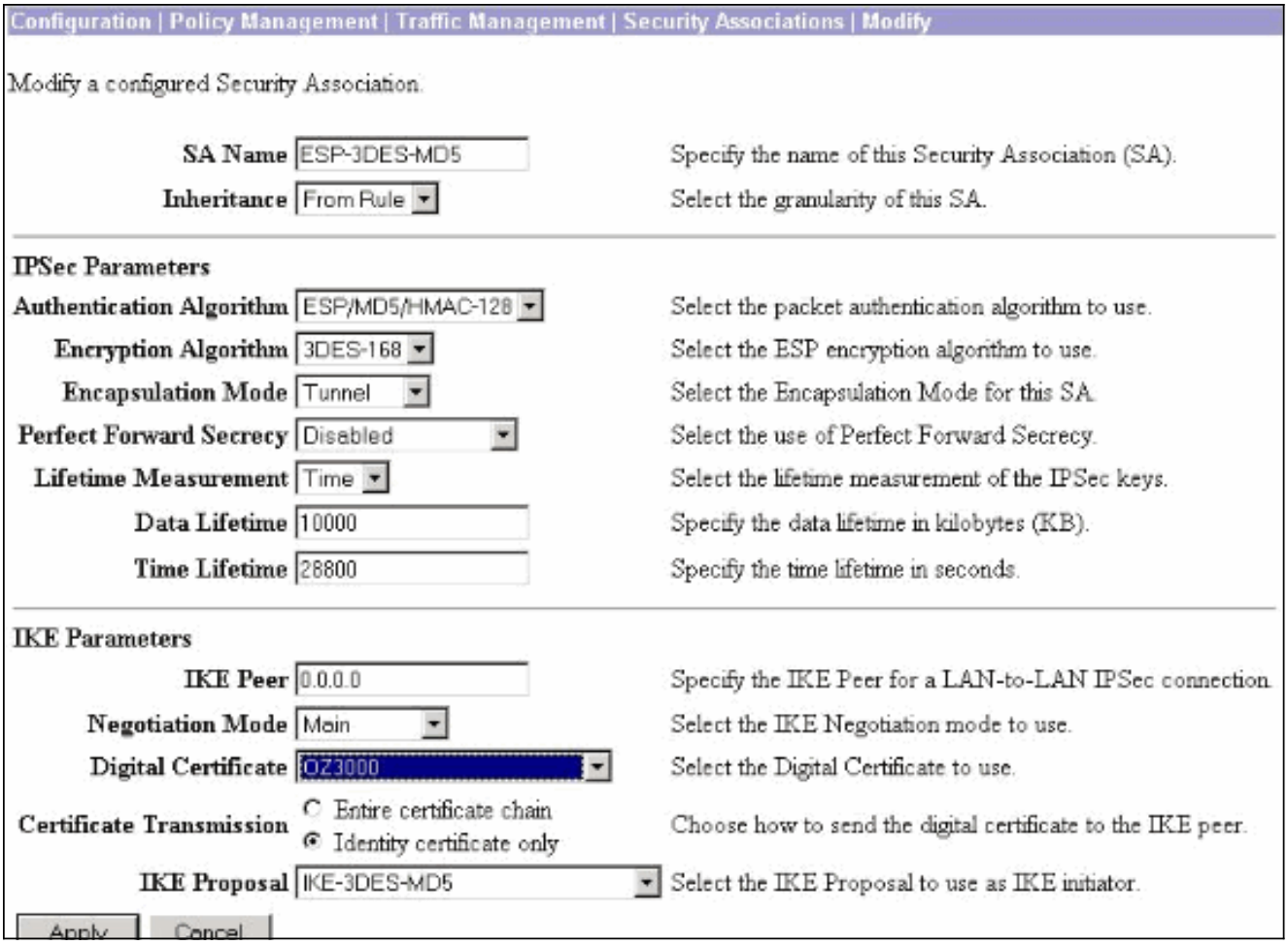
1. يجب تكوين سياسة IKE لاستخدام الشهادات الموجودة على "مدير سلسلة مركز VPN 3000". لتكوين سياسة IKE، حدد التكوين > النظام > بروتوكولات الاتصال النفقي>IPsec>**مقترحات IKE**، ونقل CiscoVPNClient-3DES-MD5-RSA إلى الاقتراحات النشطة.



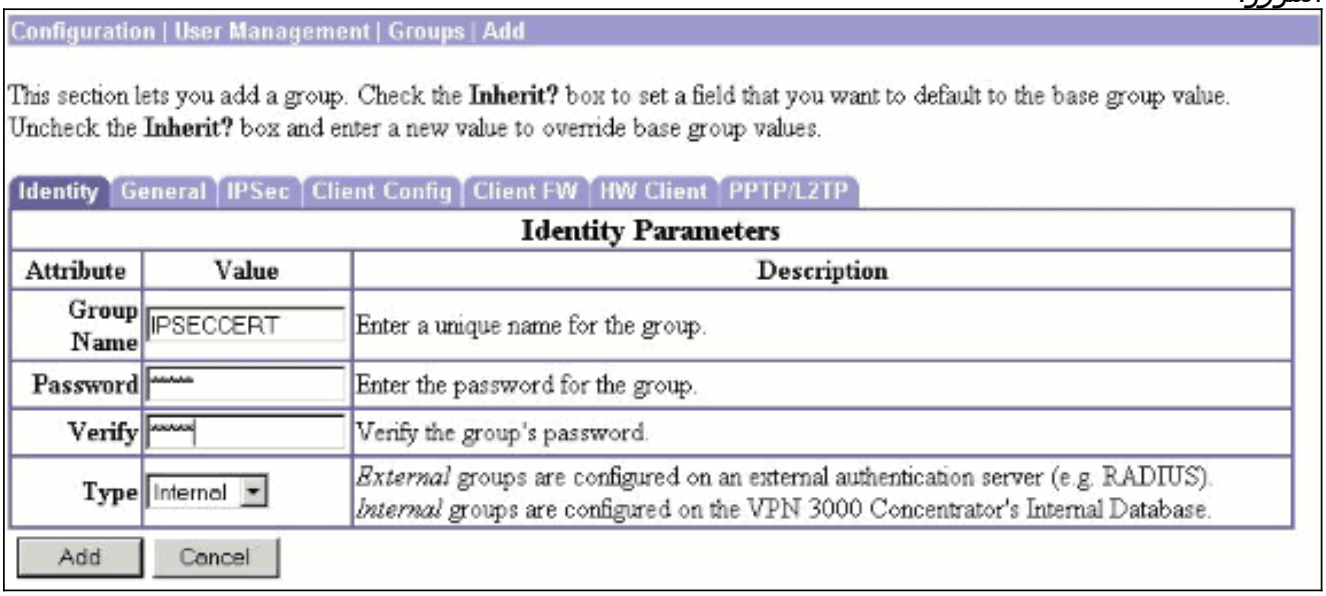
2. يجب أيضا تكوين نهج IPsec لاستخدام الشهادات. حدد تكوين > إدارة السياسة > إدارة حركة مرور البيانات>**اقترانات الأمان**، أبرز **ESP-3DES-MD5** ثم انقر فوق تعديل لتكوين سياسة IPsec لتكوين سياسة IPsec.



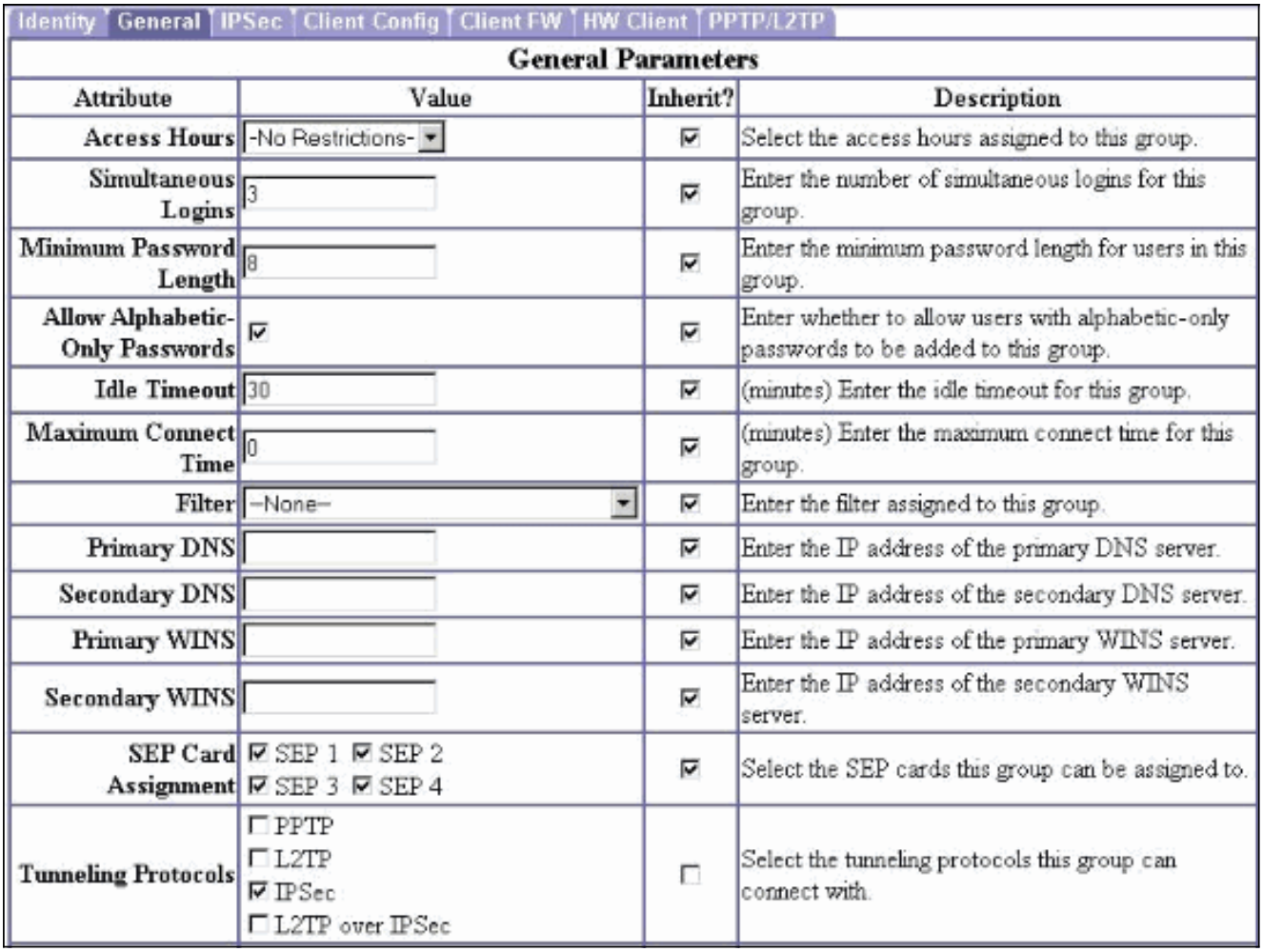
3. في نافذة "تعديل"، تحت "الشهادات الرقمية"، تأكد من تحديد شهادة هويتك المثبتة. تحت اقتراح IKE، حدد **CiscoVPNClient-3DES-MD5-RSA** وانقر فوق **تطبيق**.



4. من أجل تكوين مجموعة IPsec، حدد تكوين > **إدارة المستخدم** > **مجموعات** > **إضافة**، وقم بإضافة مجموعة تسمى IPSECCERT (يتطابق اسم مجموعة IPSECCERT مع الوحدة التنظيمية (OU) في شهادة الهوية)، وحدد كلمة مرور.لا تستخدم كلمة المرور هذه في أي مكان إذا كنت تستخدم شهادات. في هذا مثال، "cisco123" هي كلمة المرور.



5. في نفس الصفحة، انقر فوق علامة التبويب "عام" وتأكد من تحديد **IPsec** كبروتوكول الاتصال النفقي.



Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	-None-	☑	Enter the filter assigned to this group.
Primary DNS		☑	Enter the IP address of the primary DNS server.
Secondary DNS		☑	Enter the IP address of the secondary DNS server.
Primary WINS		☑	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☐	Select the tunneling protocols this group can connect with.

6. انقر فوق علامة التبويب IPsec وتأكد من تحديد اقتران أمان IPsec (SA) الذي تم تكوينه ضمن IPsec وانقر فوق
تطبيق.

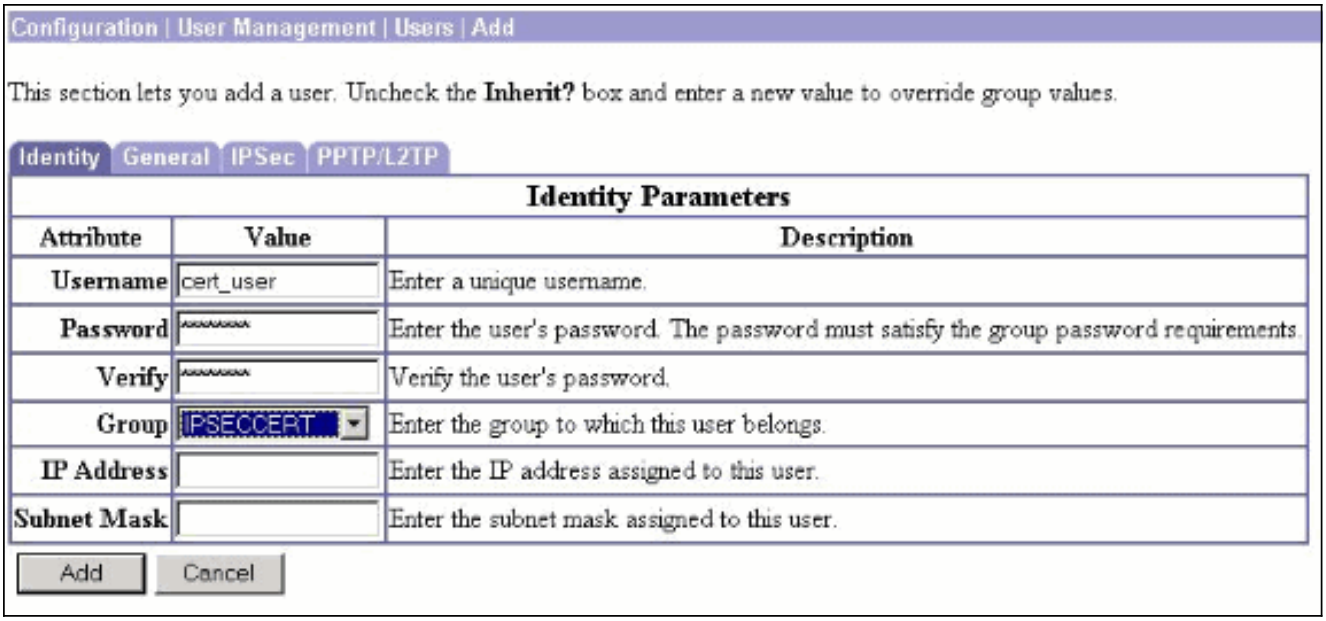
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

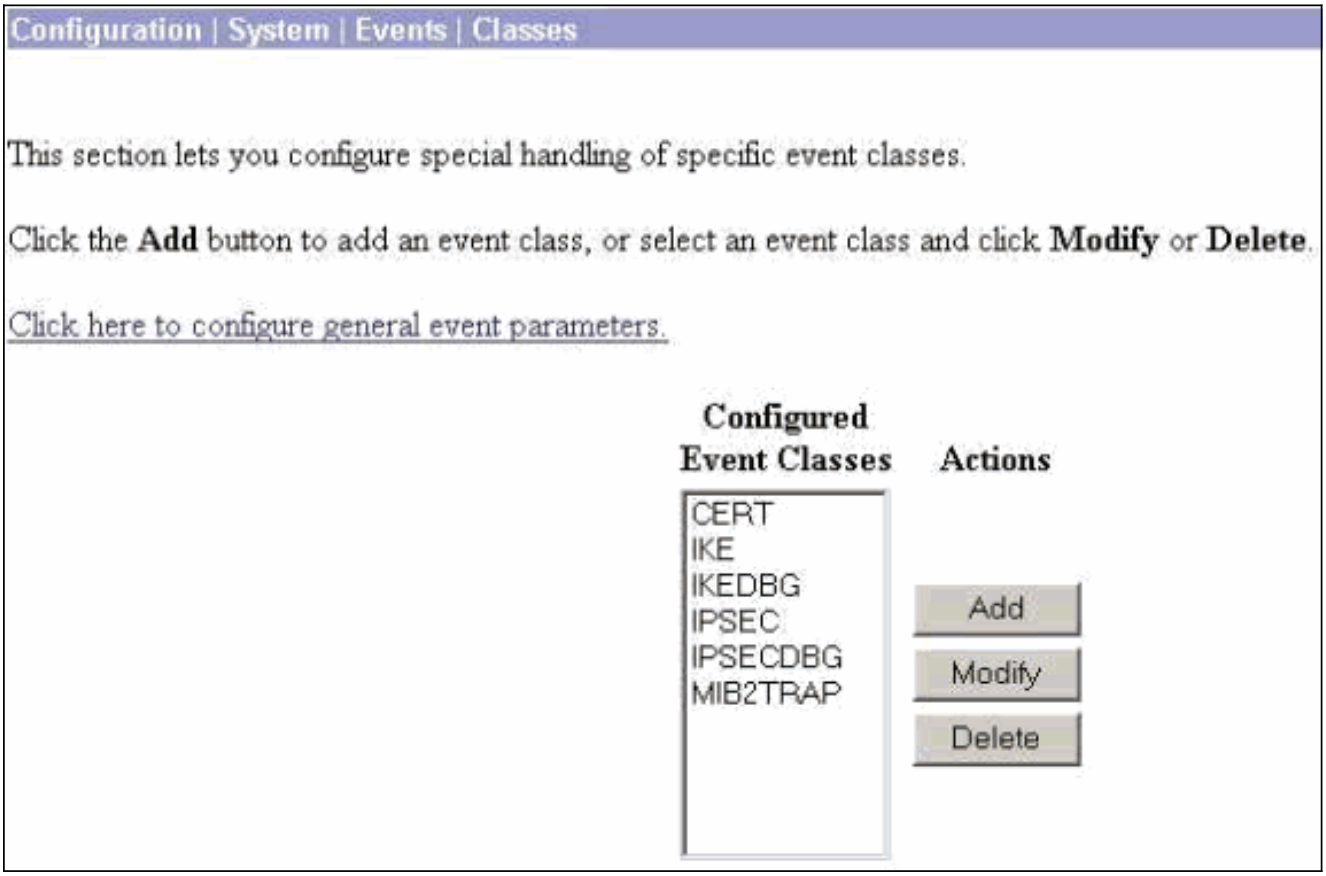
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	☑	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	Internal	☐	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None	☑	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	☐	☑	Check to require successful authorization.
DN Field	CN otherwise OU	☑	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
Authorization Required	☐	☑	Check to require successful authorization.
DN Field	CN otherwise OU	☑	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	☑	☑	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

Add | Cancel

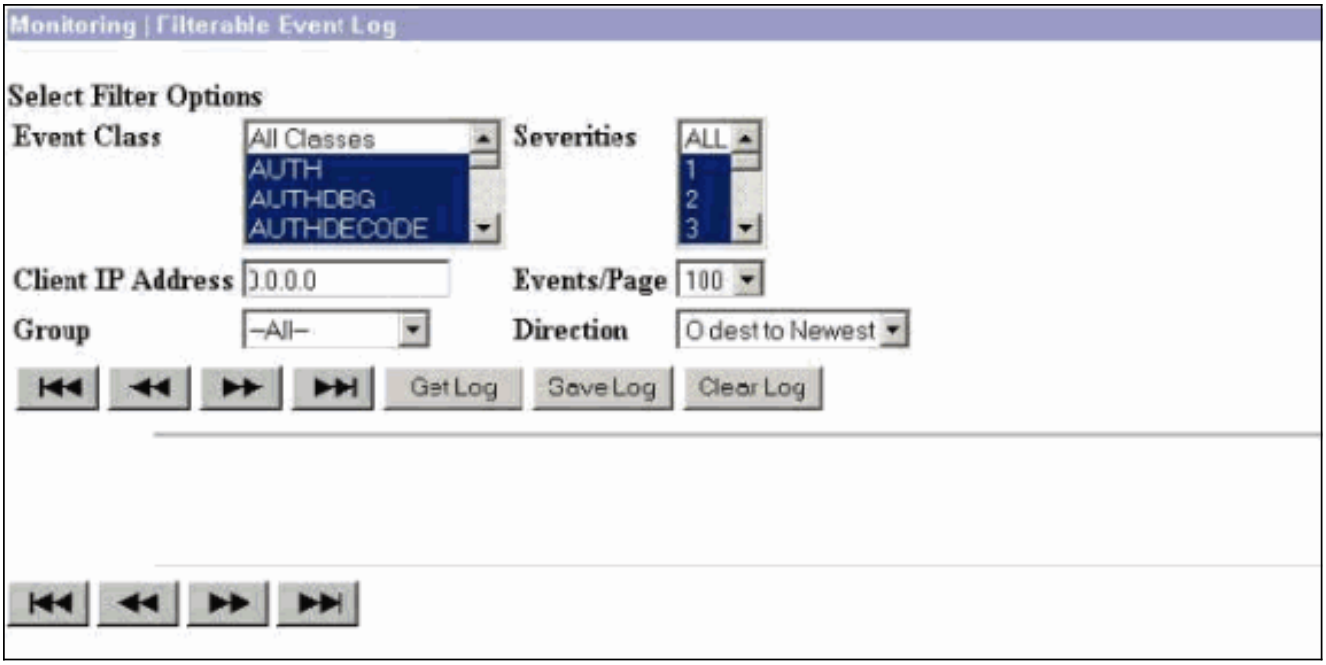
7. in order to شكلت IPsec مجموعة على ال VPN 3000 مركز، حددت تشكيل**<مستعمل إدارة>مستعمل<يضيف،يعين مستعمل إسم، كلمة، والمجموعة إسم، وبعد ذلك طقطقة يضيف**.في المثال، يتم إستخدام هذه الحقول:اسم المستخدم = cert_userكلمة المرور = Cisco123التحقق من الصحة = Cisco123المجموعة = IPSECCERT



8. لتمكين تصحيح الأخطاء على VPN 3000 Concentrator تحديد **تشكيل>نظام>أحداث>فئات** وأضفت هذه الفئات:فريق التحقيق 1-13آيك 1-10-1 6iKEDBG بروتوكول -1 IPSec 1-6IPSECDBG
10



9. حدد **مراقبة > سجل أحداث قابل للتصفية** لعرض تصحيح الأخطاء.



ملاحظة: إذا قررت تغيير عناوين IP، فيمكنك إجراء تسجيل لعناوين IP الجديدة وتثبيت الشهادة التي تم إصدارها لاحقا باستخدام هذه العناوين الجديدة.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

راجع أستكشاف أخطاء الاتصال وإصلاحها على مركز VPN 3000 للحصول على مزيد من المعلومات حول أستكشاف الأخطاء وإصلاحها.

معلومات ذات صلة

- مركزات Cisco VPN 3000 Series
- أجهزة Cisco VPN 3002 العميلة
- مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).