Configuración del concentrador VPN 3000 para comunicarse con el cliente VPN por medio de los certificados

Contenido

Introducción

Este documento incluye las instrucciones paso a paso en cómo configurar el Concentradores Cisco VPN de la serie 3000 con los clientes VPN con el uso de los Certificados.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión de software 4.0.4A del Cisco VPN 3000 Concentrator.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

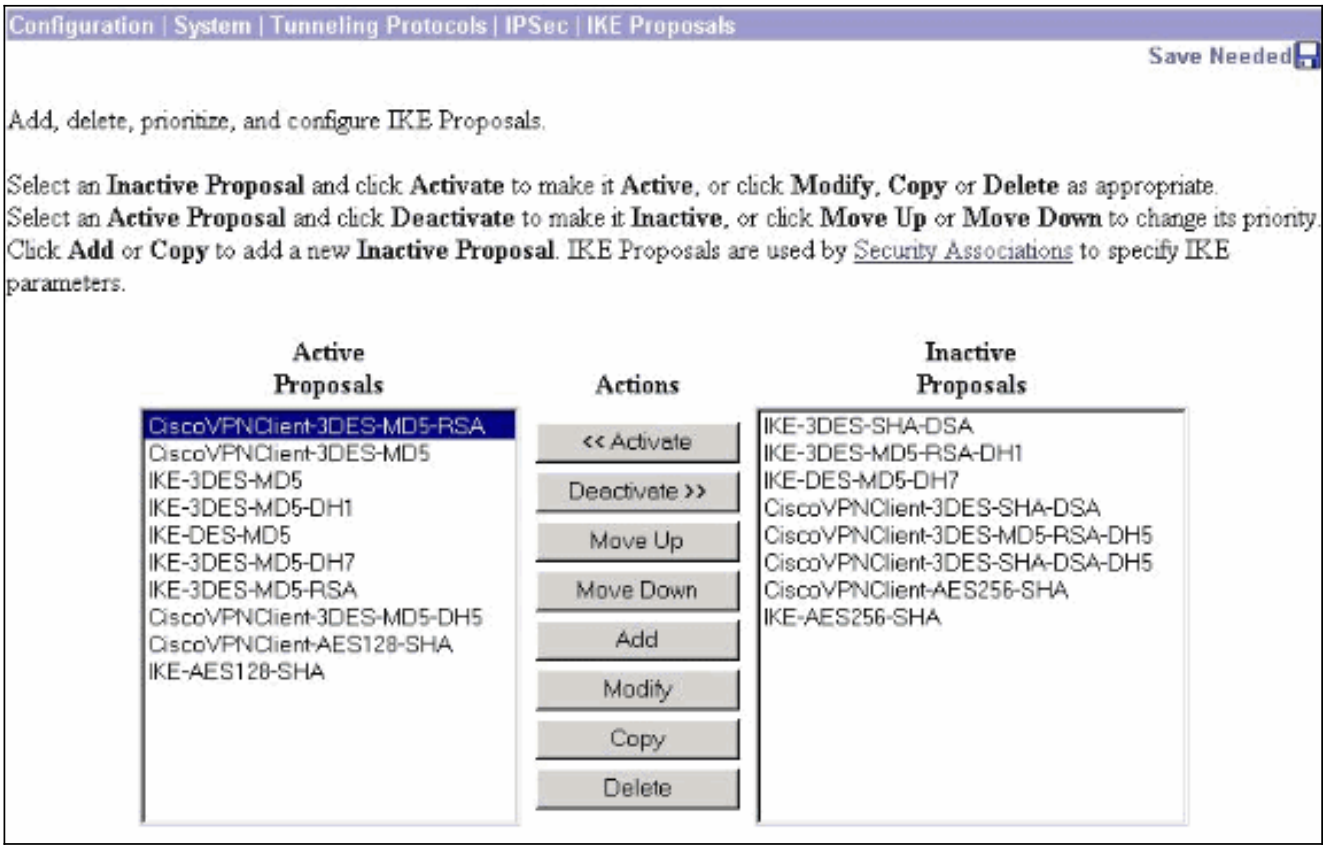
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

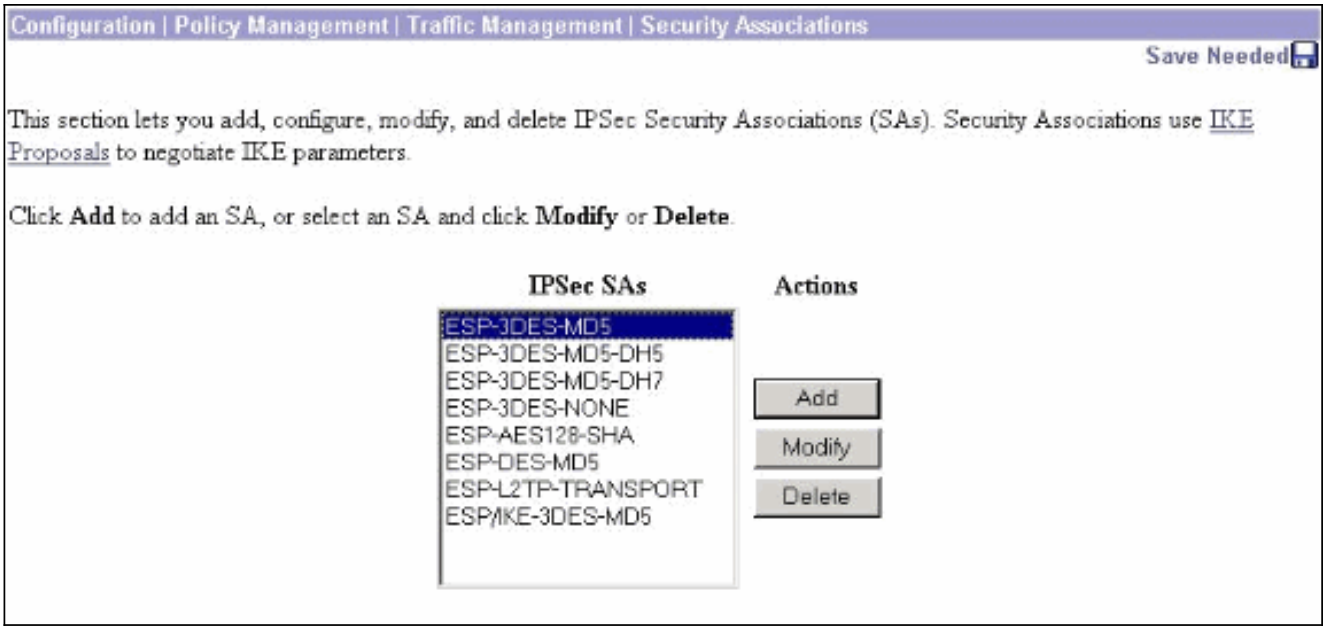
Certificados de concentrador VPN 3000 para clientes VPN

Complete estos pasos para configurar los Certificados concentradores VPN 3000 para los clientes VPN.

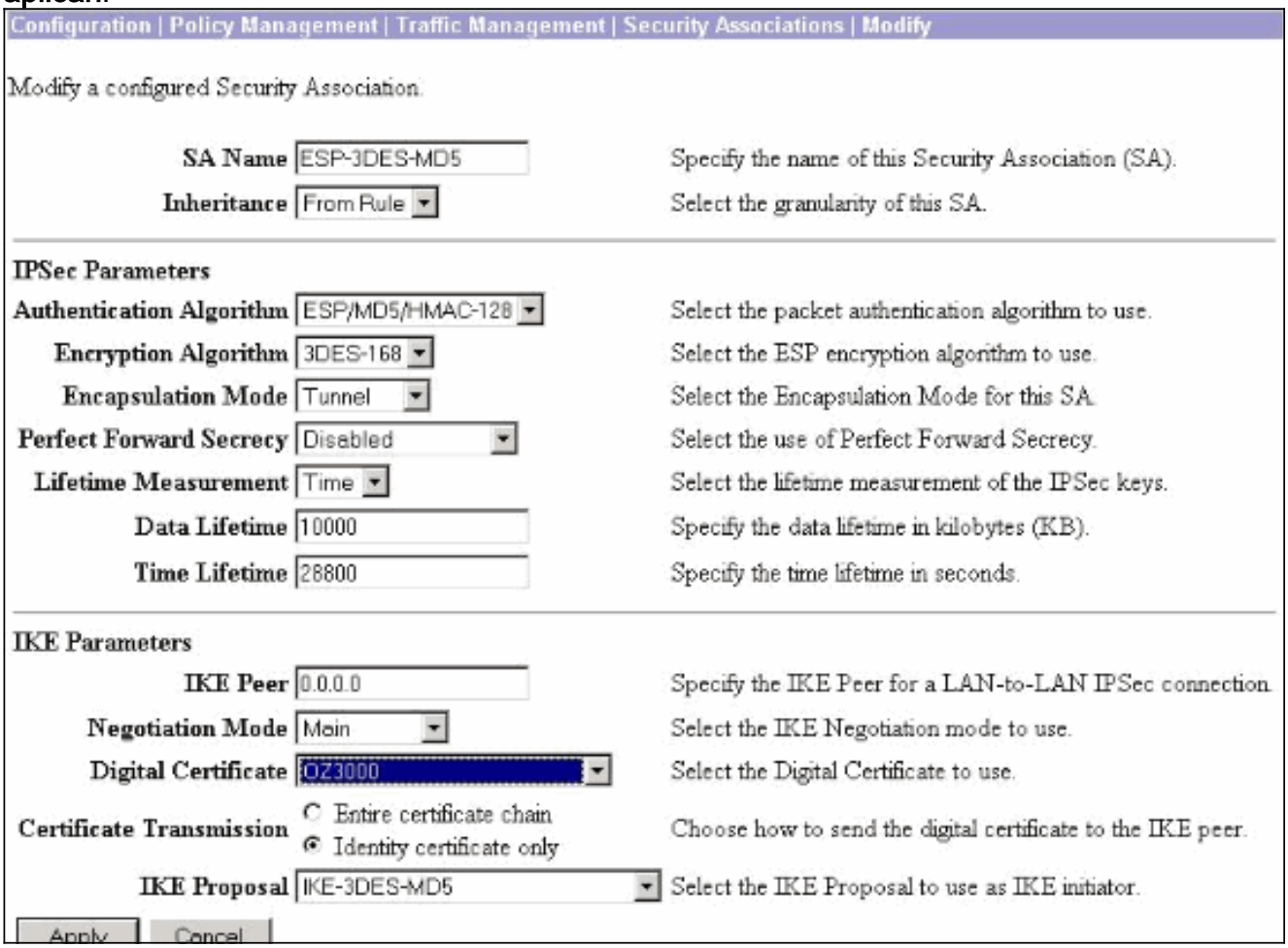
1. La política IKE se debe configurar para utilizar los Certificados en el administrador del VPN 3000 Concentrator Series. Para configurar la política IKE, el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE)** selecto, y el movimiento **CiscoVPNClient-3DES-MD5-RSA a las** propuestas
activas.



2. Usted debe también configurar la directiva del IPSec para utilizar los Certificados. **El Configuration (Configuración) > Policy Management (Administración de políticas) > Management Traffic (Administración de tráfico) > Security Associations (Asociaciones de seguridad)** selecto, el resaltado **ESP-3DES-MD5** y entonces hace clic **se modifica para configurar la directiva del IPSec** para configurar la directiva del
IPSec.

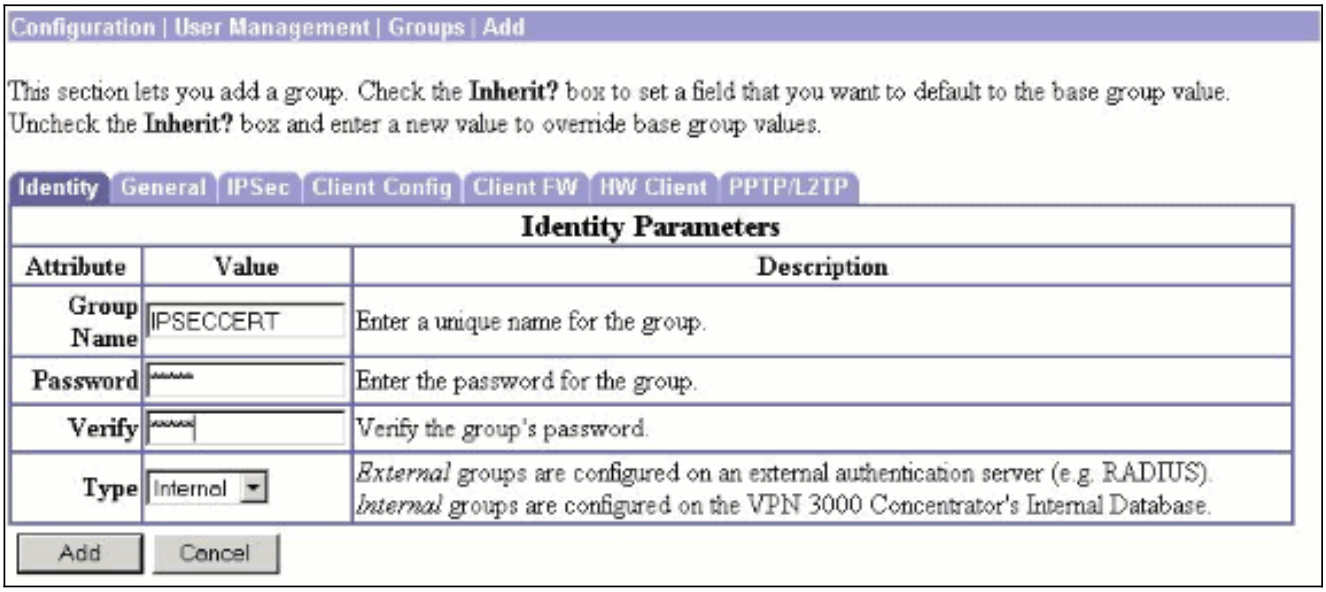


3. En la ventana de la modificación, bajo los Certificados digitales, aseegurese seleccionar su certificado de identidad instalado. Bajo la propuesta IKE, **CiscoVPNClient-3DES-MD5-RSA** selectos y el tecleo **se aplican**.



4. Para configurar a un grupo IPSec, seleccione el **Configuration (Configuración) > User Management (Administración del usuario) >Groups (Grupos) > Add (Agregar)**, agregan a un grupo llamado **IPSECCERT** (el nombre del grupo IPSECCERT hace juego la unidad organizativa (OU) en el certificado de identidad), y seleccionan una contraseña.Esta contraseña no se utiliza dondequiera si usted utiliza los Certificados. En este ejemplo, el "cisco123" es la

contraseña.



Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

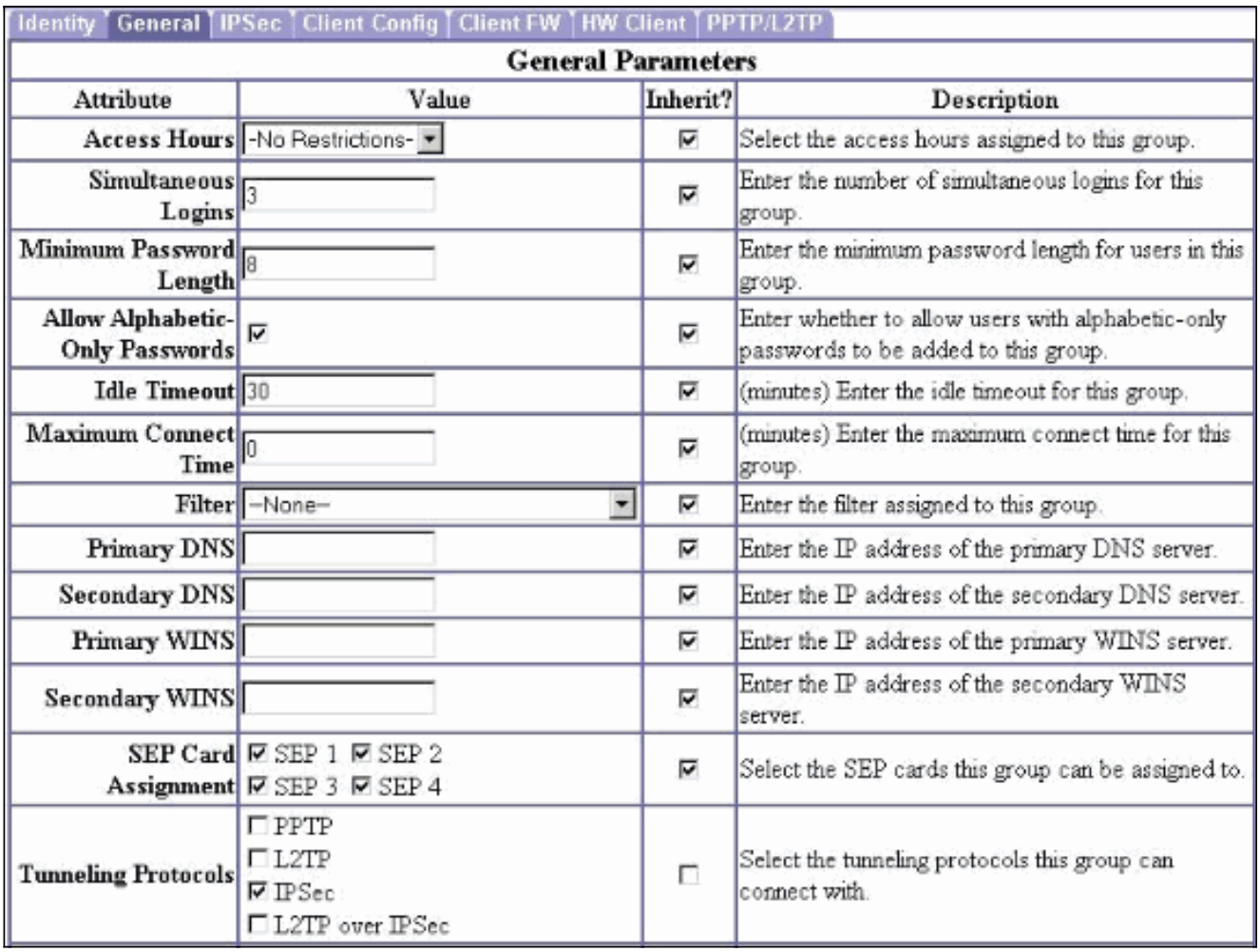
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Group Name	IPSECCERT	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

Add | Cancel

5. En la misma página, haga clic la ficha general y aseegurese que usted selecciona el **IPSec** como el Tunneling
Protocol.

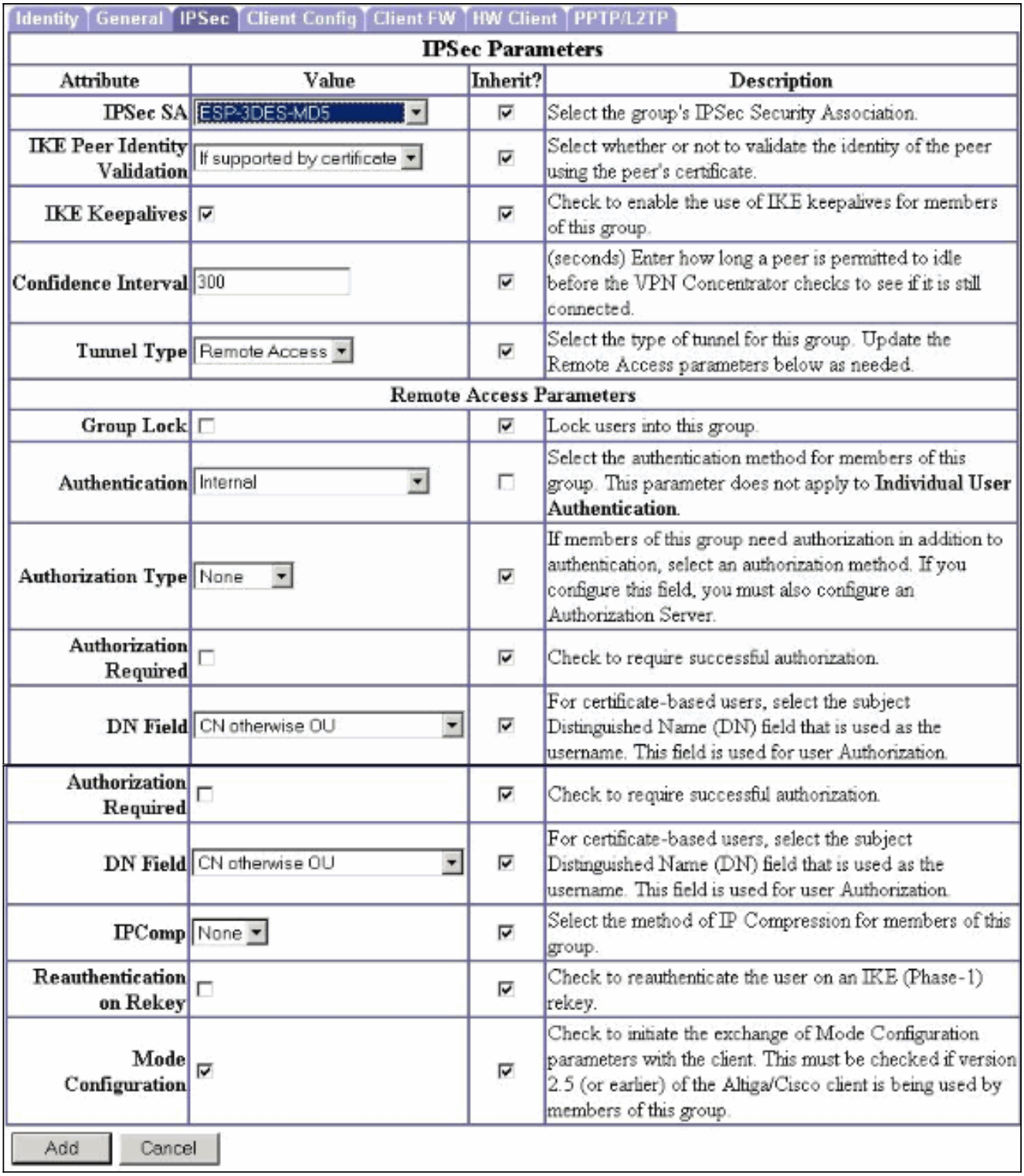


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Haga clic la lengueta del IPSec y aseegurese que seleccionan a su asociación de seguridad IPSec configurada (SA) bajo IPSec SA y tecleo **se aplica**.



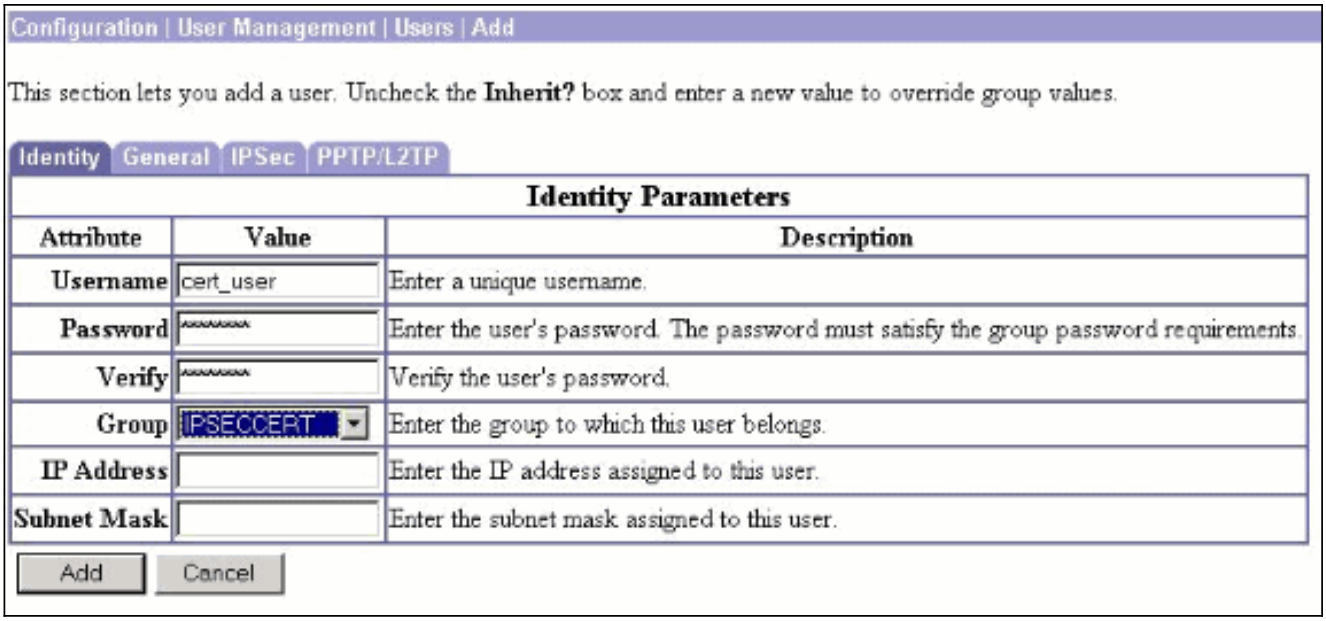
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

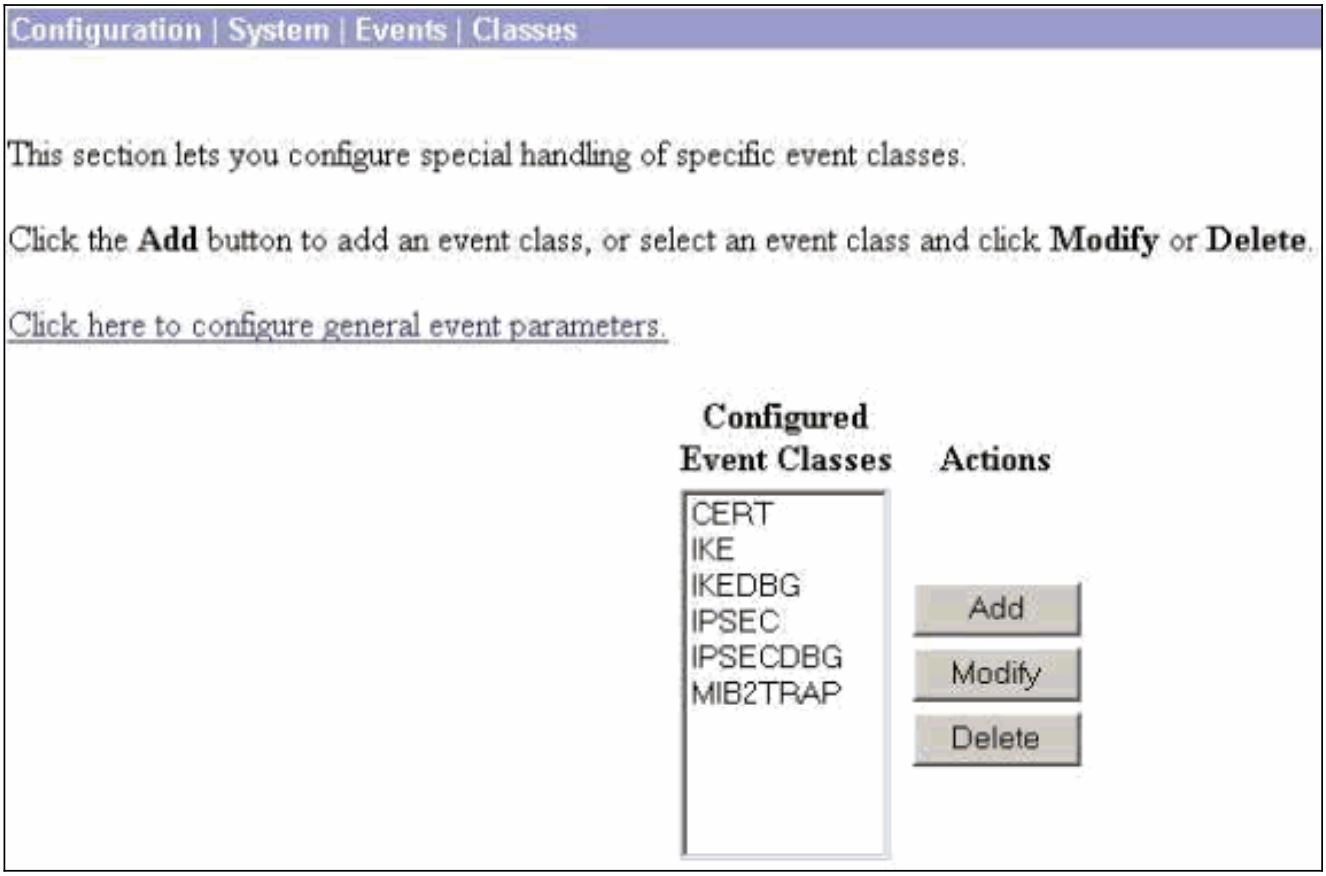
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of 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

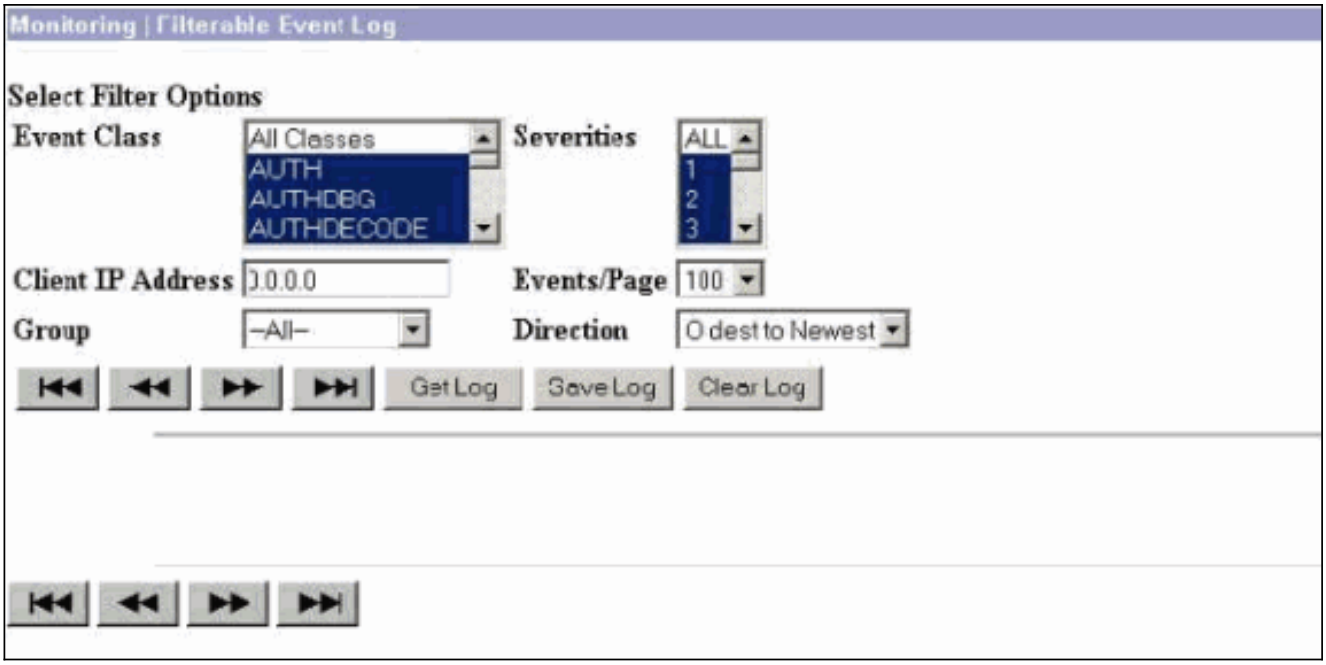
7. Para configurar a un grupo IPSec en el concentrador VPN 3000, seleccione el **Configuration (Configuración) > User Management (Administración del usuario) > Users (Usuarios) > Add (Agregar)**, especifique un Nombre de usuario, contraseña, y el nombre del grupo, y entonces haga click en AddEn el ejemplo, se utilizan estos campos:Nombre de usuario = cert_userContraseña = cisco123Verifique = cisco123Grupo = IPSECCERT



8. Para habilitar el debugging en el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases)** selecto concentrador VPN 3000 y agregar estas clases:CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-10



9. Orden selecta del **login de la supervisión** > del **Filterable Event (Evento filtrable)** para ver los debugs.



Nota: Si usted decide cambiar los IP Addresses, usted puede hacer una inscripción de los nuevos IP Addresses y instalar el certificado publicado más adelante con esos nuevos direccionamientos.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Refiera a los Problemas de conexión del troubleshooting en el concentrador VPN 3000 para la más información sobre Troubleshooting.

Información Relacionada

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems