Configuration du concentrateur VPN 3000 pour communiquer avec le client VPN à l'aide de certificats

Contenu

Introduction

Ce document inclut des instructions détaillées sur la façon de configurer les concentrateurs de la gamme Cisco VPN 3000 avec des clients VPN avec l'utilisation de certificats.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le logiciel Cisco VPN 3000 Concentrator version 4.0.4A.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

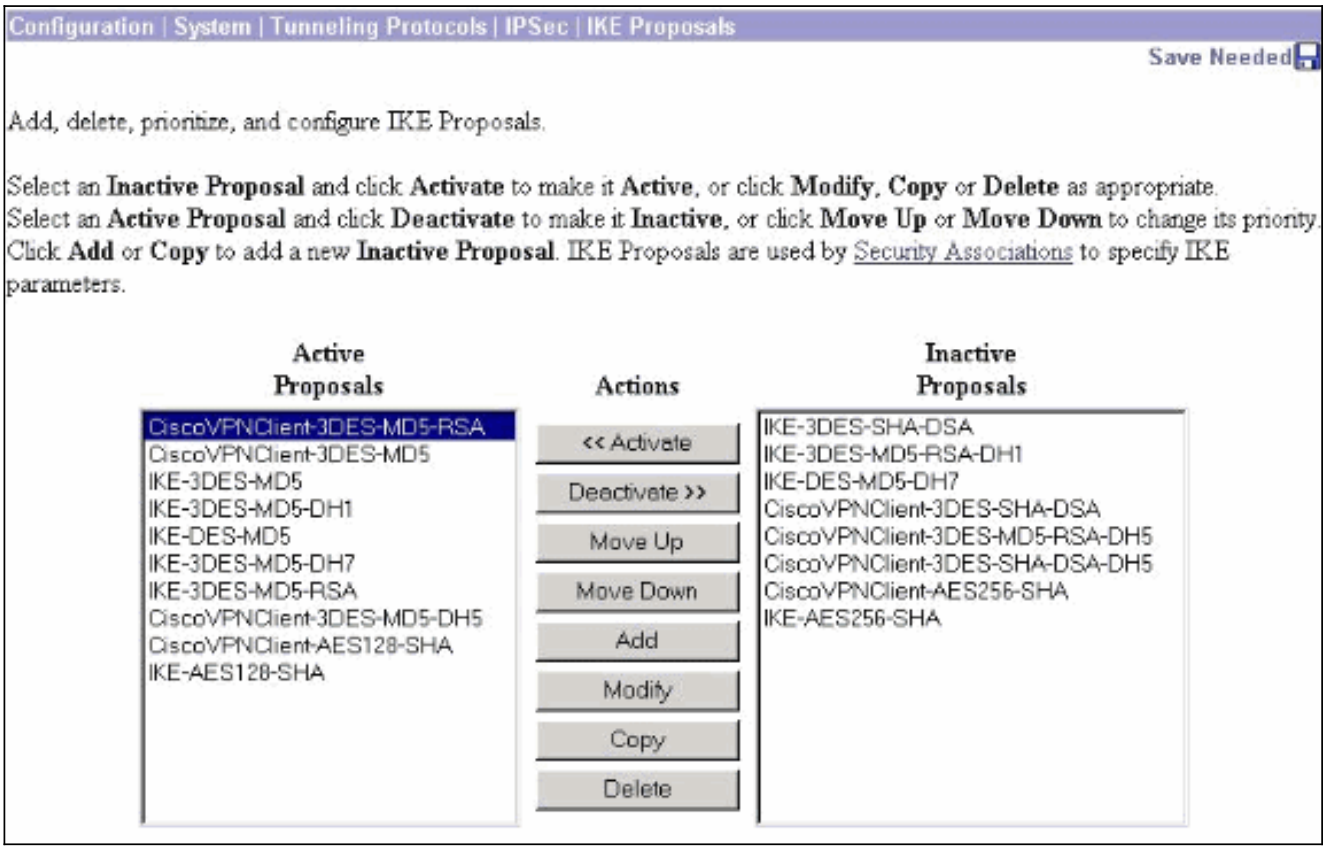
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

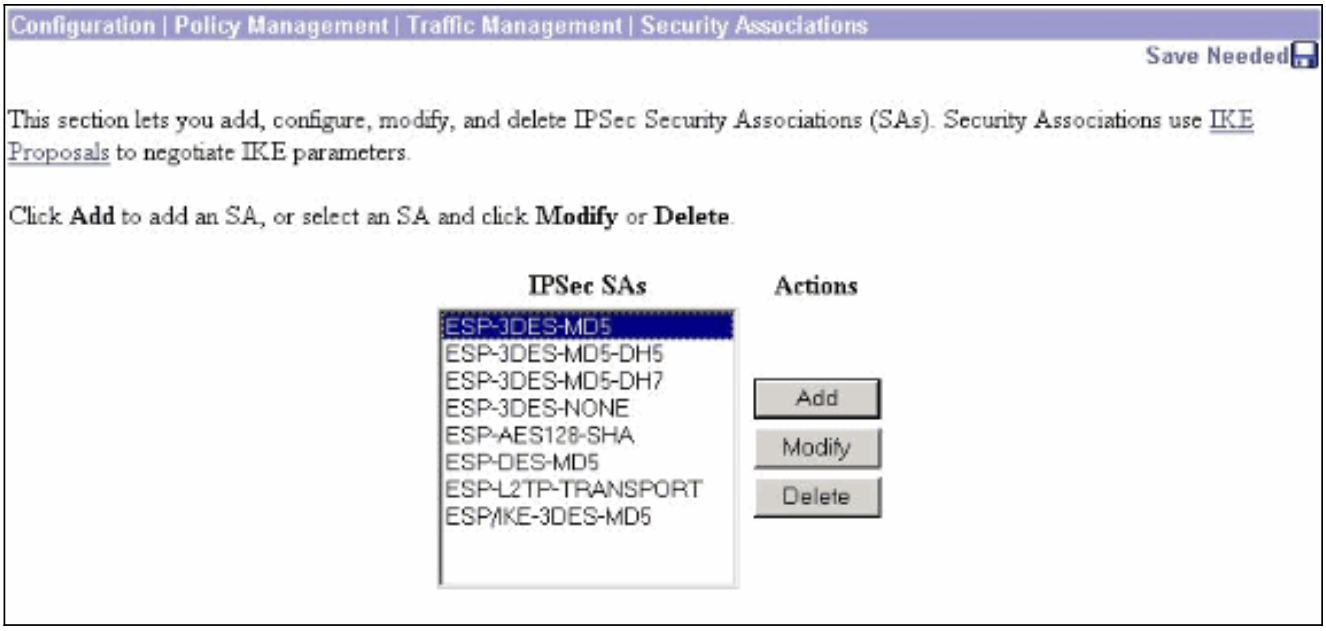
Certificats de concentrateur VPN 3000 pour clients VPN

Complétez ces étapes afin de configurer les certificats de concentrateur VPN 3000 pour les clients VPN.

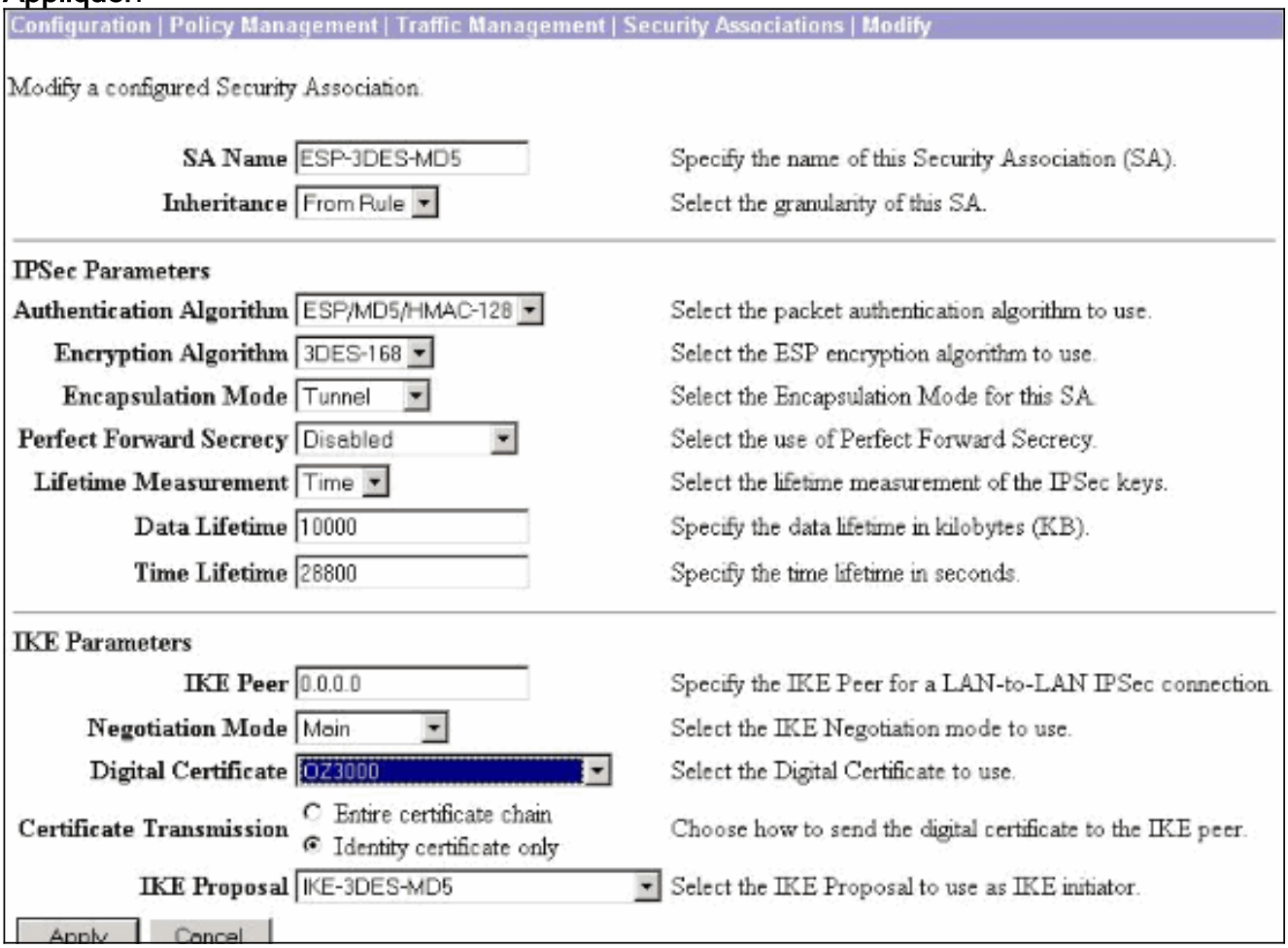
1. La stratégie IKE doit être configurée pour utiliser des certificats sur le gestionnaire de la gamme de concentrateurs VPN 3000. Afin de configurer la stratégie IKE, sélectionnez Configuration > System > Tunneling Protocols > **IPsec > IKE Propositions**, et déplacez **CiscoVPNlient-3DES-MD5-RSA** vers les propositions actives.



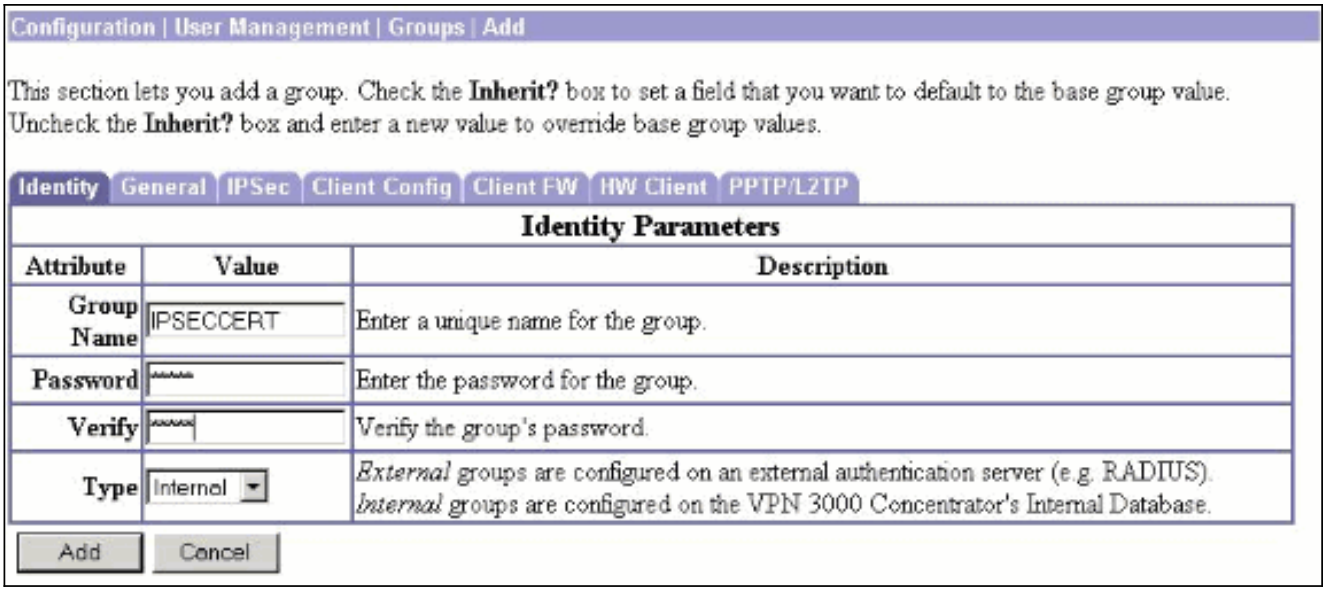
2. Vous devez également configurer la stratégie IPsec pour utiliser des certificats. Sélectionnez Configuration > Policy Management > Traffic Management > **Security Associations**, mettez en surbrillance **ESP-3DES-MD5**, puis cliquez sur **Modify pour configurer la stratégie IPsec** pour configurer la stratégie IPsec.



3. Dans la fenêtre Modifier, sous Certificats numériques, assurez-vous de sélectionner votre certificat d'identité installé. Sous Proposition IKE, sélectionnez **CiscoVPNlient-3DES-MD5-RSA** et cliquez sur **Appliquer**.



4. Afin de configurer un groupe IPsec, sélectionnez Configuration > **User Management > Groups > Add**, ajoutez un groupe appelé **IPSECCERT** (le nom du groupe IPSECCERT correspond à l'unité d'organisation (OU) du certificat d'identité) et sélectionnez un mot de passe.Ce mot de passe n'est utilisé nulle part si vous utilisez des certificats. Dans cet exemple, « cisco123 » est le mot de passe.



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.

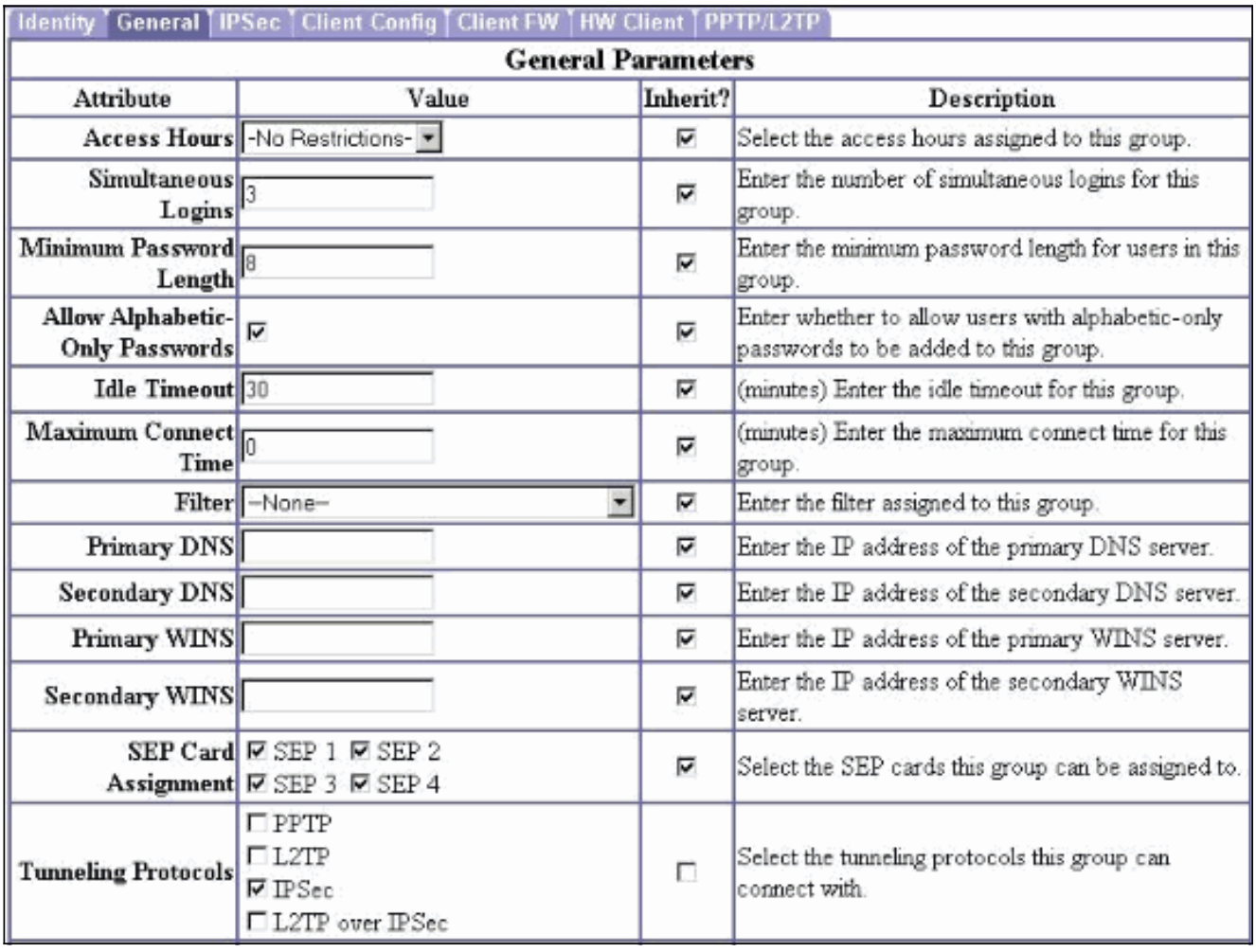
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Sur la même page, cliquez sur l'onglet Général et assurez-vous de sélectionner **IPsec** comme protocole de tunnellisation.

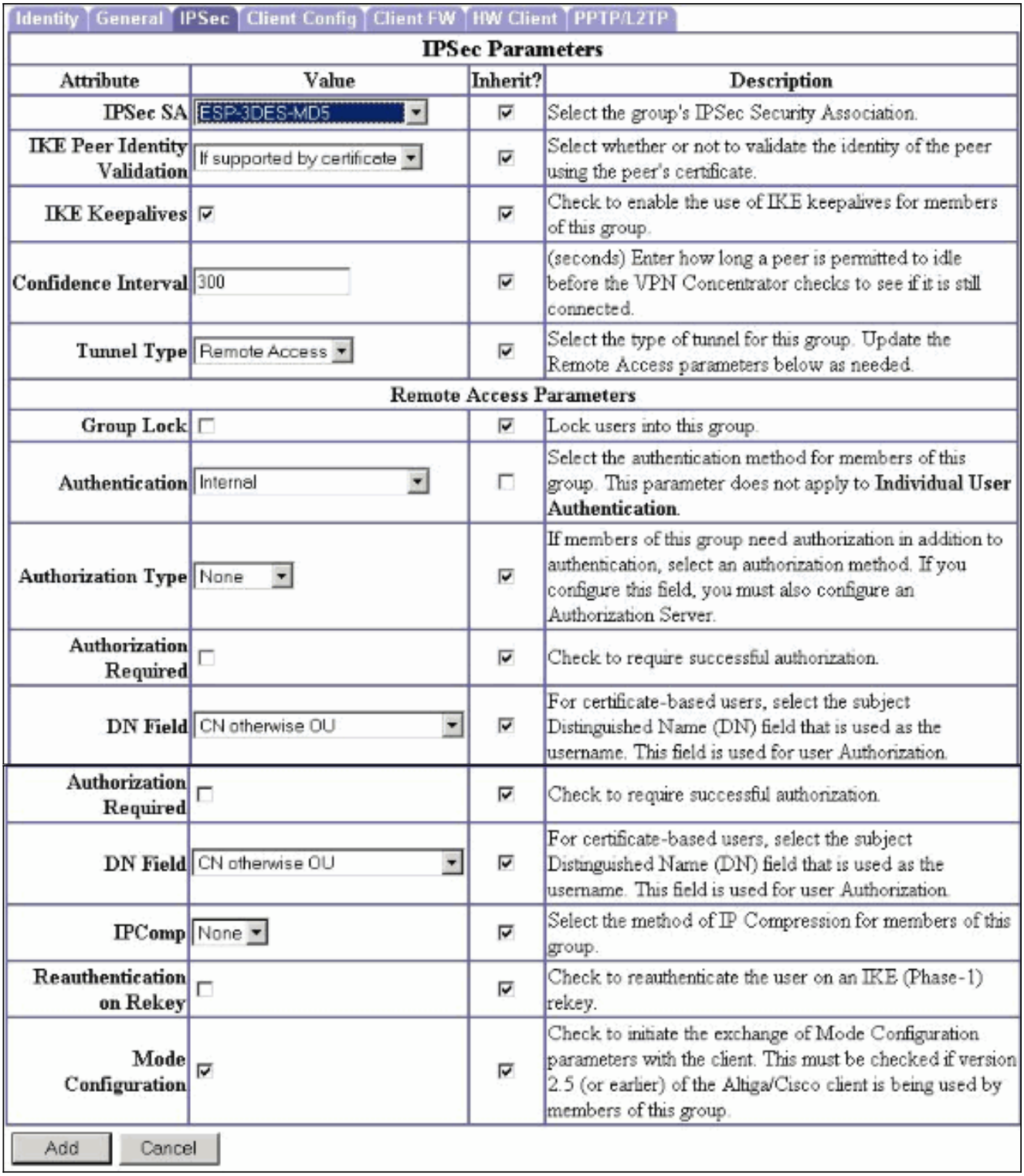


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Cliquez sur l'onglet IPsec et assurez-vous que votre association de sécurité IPsec (SA) configurée est sélectionnée sous SA IPsec et cliquez sur **Apply**.



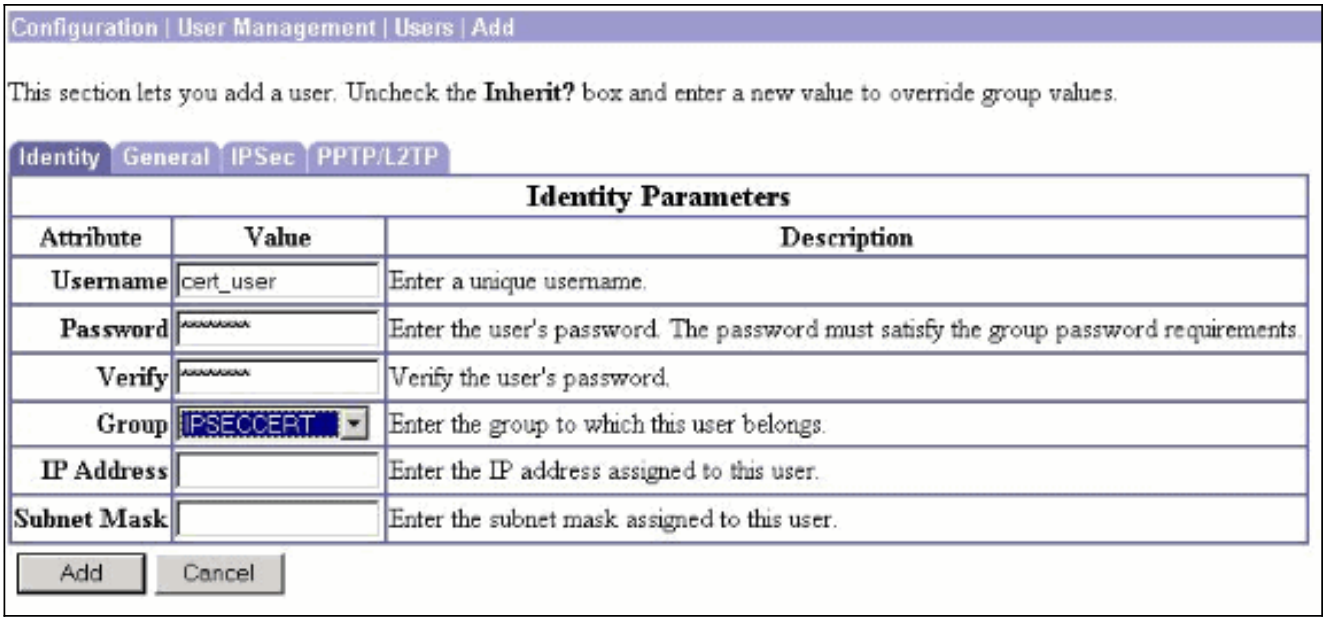
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

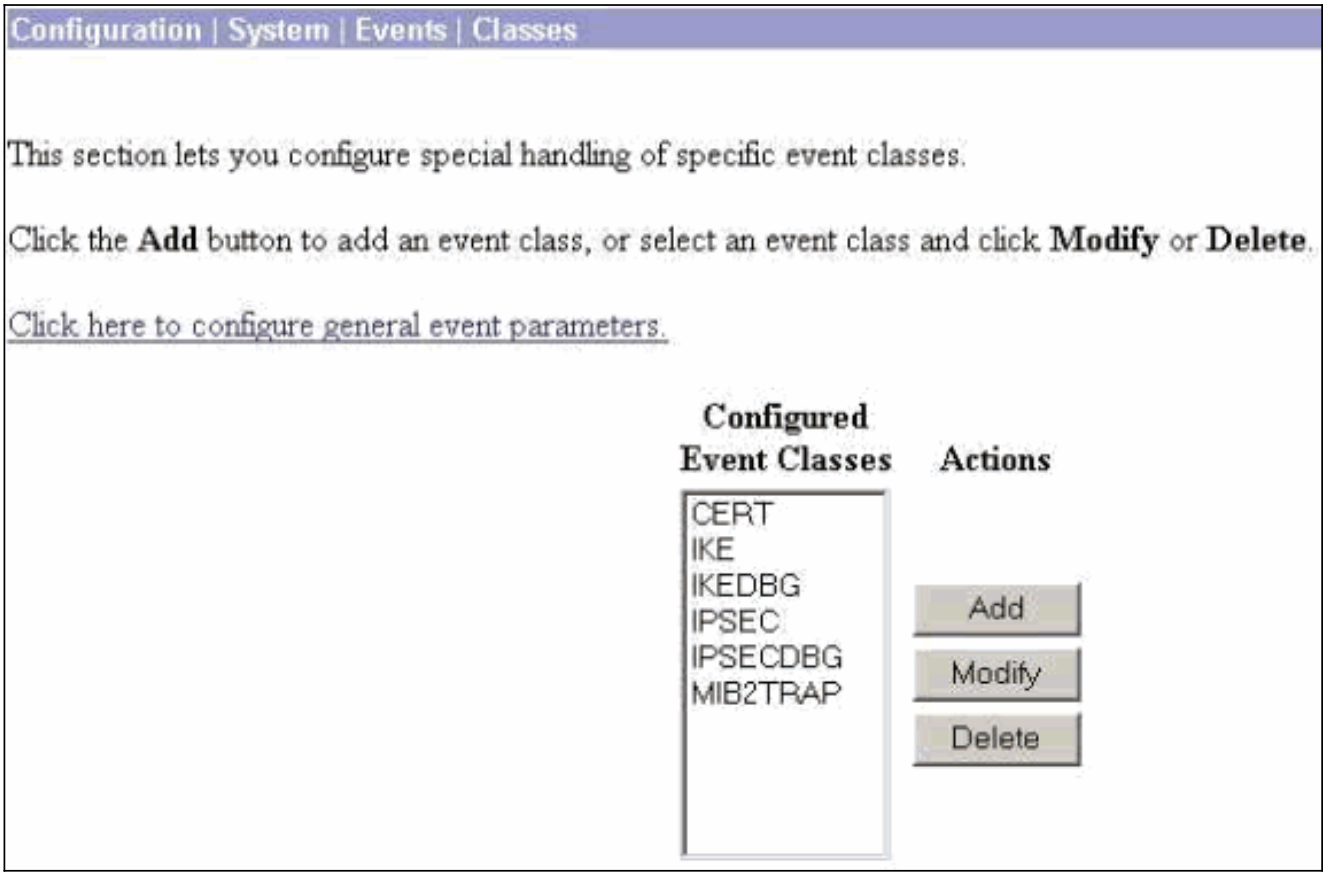
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of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

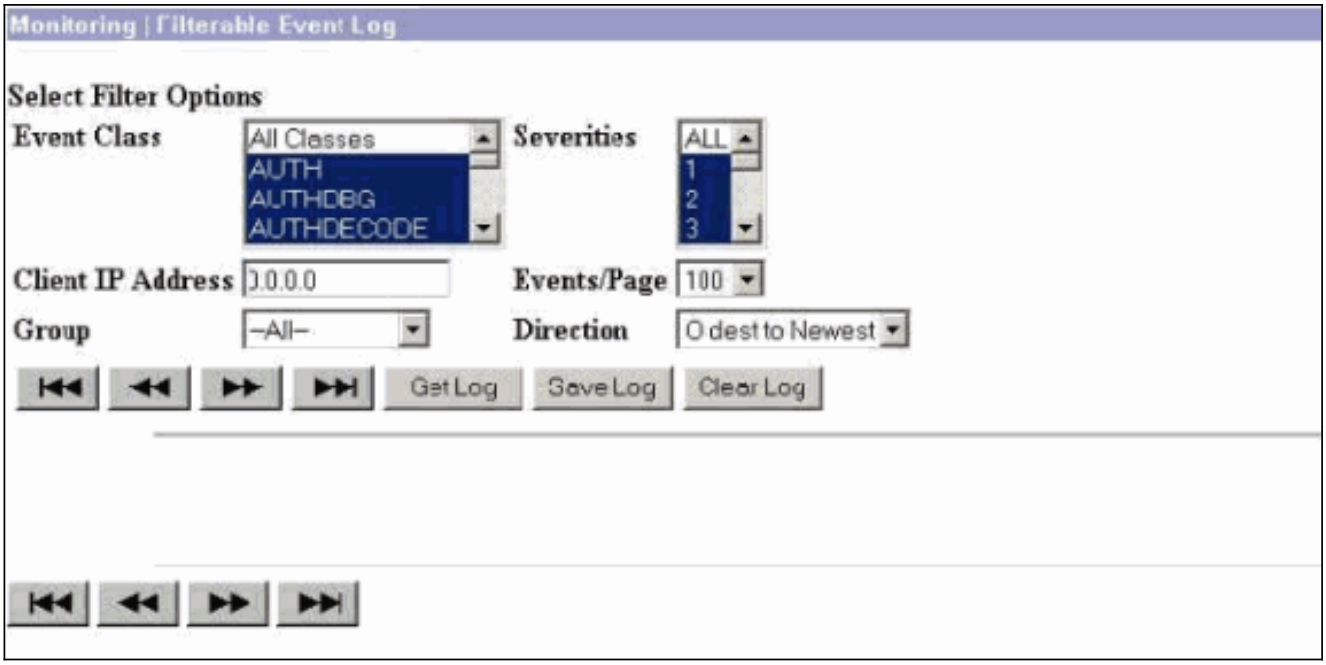
7. Afin de configurer un groupe IPsec sur le concentrateur VPN 3000, sélectionnez Configuration > **User Management > Users > Add**, spécifiez un nom d'utilisateur, un mot de passe et le nom du groupe, puis cliquez sur **Add**.Dans l'exemple, ces champs sont utilisés :Nom d'utilisateur = cert_userMot de passe = cisco123Vérifier = cisco123Groupe = IPSECCERT



8. Afin d'activer le débogage sur le concentrateur VPN 3000, sélectionnez **Configuration > System > Events > Classes** et ajoutez ces classes :CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. Sélectionnez **Monitoring > Filterable Event Log** afin d'afficher les débogages.



Remarque : si vous décidez de modifier les adresses IP, vous pouvez inscrire les nouvelles adresses IP et installer le certificat émis ultérieurement avec ces nouvelles adresses.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Référez-vous à Dépannage des problèmes de connexion sur le concentrateur VPN 3000 pour plus d'informations de dépannage.

Informations connexes

- Concentrateurs VPN de la gamme Cisco 3000
- Cisco VPN 3002 Hardware Clients
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems