

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Certificats de concentrateur VPN 3000 pour des clients vpn](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document comporte des instructions pas à pas sur la façon dont configurer les Concentrateurs de la gamme Cisco VPN 3000 avec des clients VPN avec l'utilisation des Certificats.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 4.0.4A de logiciel du concentrateur de Cisco VPN 3000.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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 des clients vpn

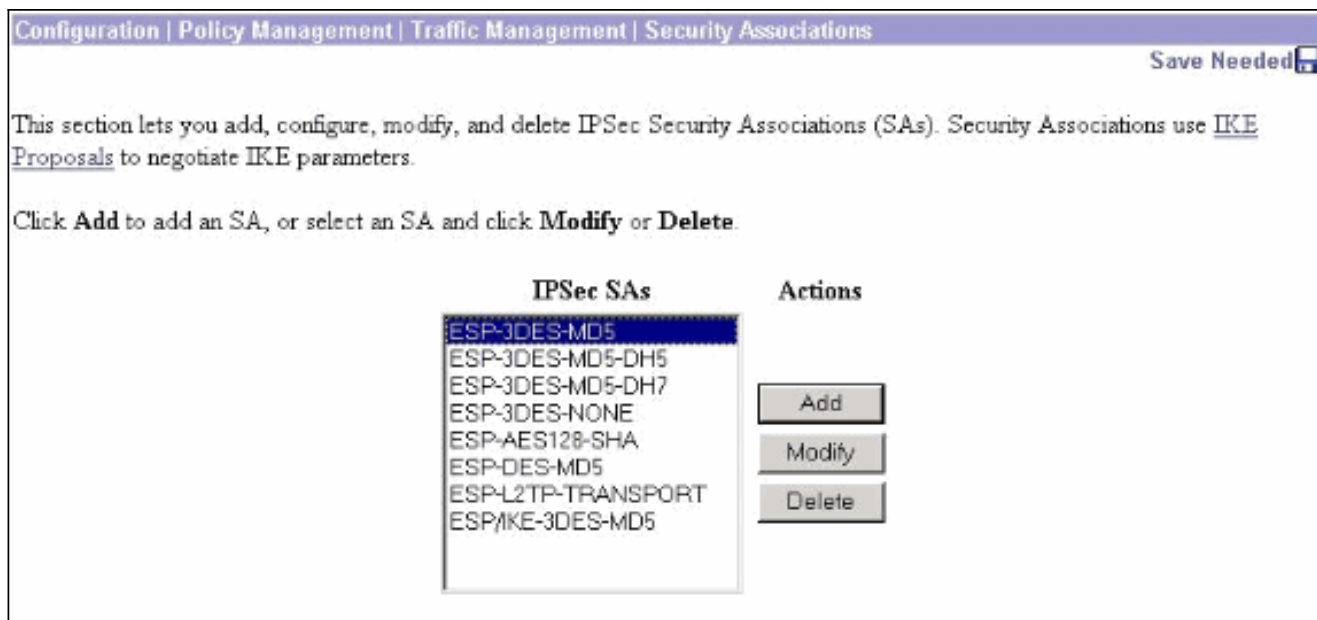
Terminez-vous ces étapes afin de configurer des Certificats de concentrateur VPN 3000 pour des clients vpn.

1. La stratégie IKE doit être configurée pour utiliser des Certificats sur le gestionnaire de gamme de concentrateur VPN 3000. Afin de configurer la stratégie IKE, **configuration > protocoles de système > de Tunnellisation > IPsec > propositions d'IKE**, et mouvement choisis **CiscoVPNClient-3DES-MD5-RSA** aux propositions actives.

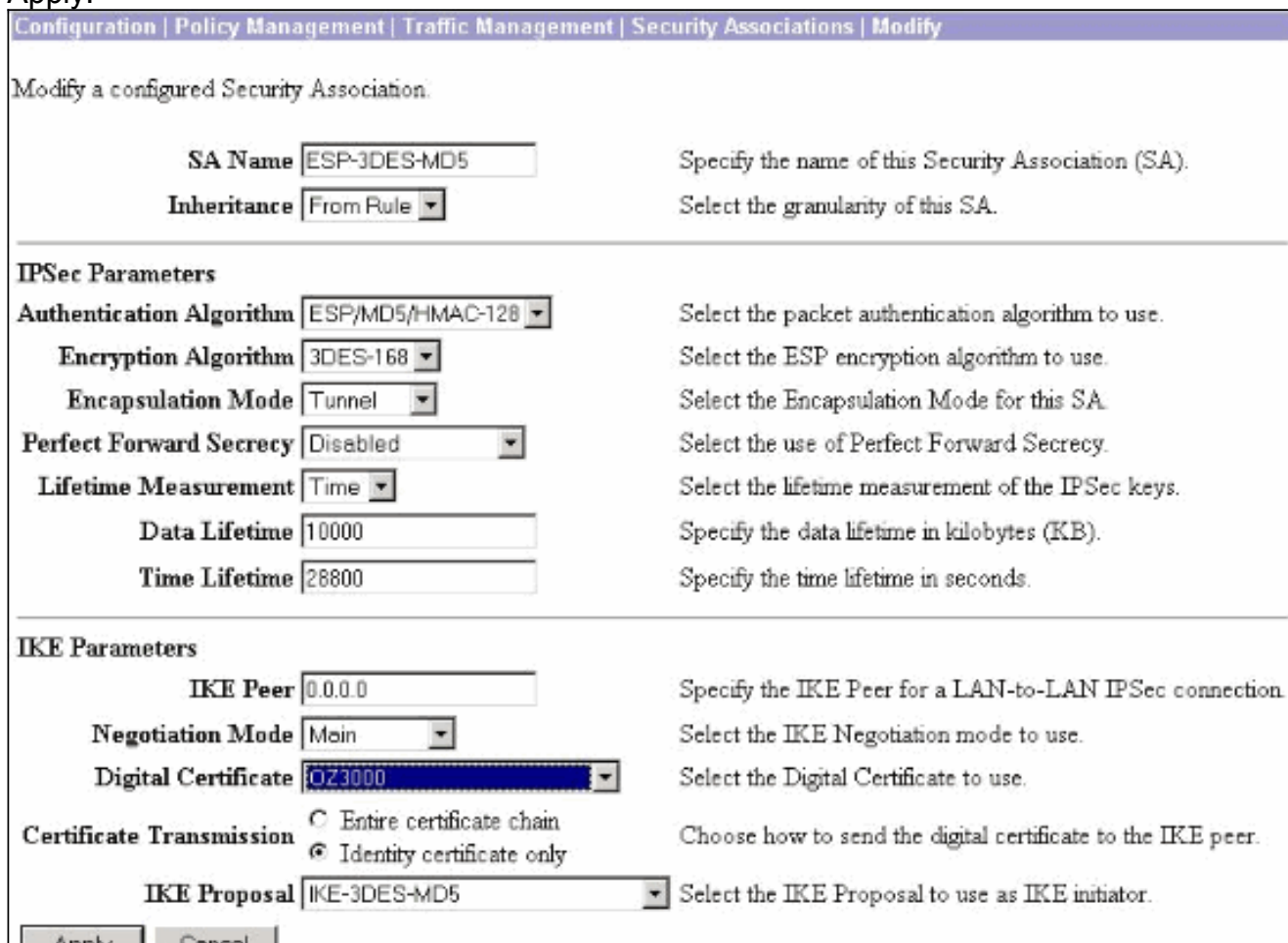
The screenshot shows the 'IKE Proposals' configuration page. At the top, there is a breadcrumb trail: 'Configuration | System | Tunneling Protocols | IPsec | IKE Proposals'. A 'Save Needed' button is in the top right. Below the breadcrumb, there is a description: 'Add, delete, prioritize, and configure IKE Proposals.' and instructions: '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-RSA	<< Activate	IKE-3DES-SHA-DSA
CiscoVPNClient-3DES-MD5	Deactivate >>	IKE-3DES-MD5-RSA-DH1
IKE-3DES-MD5	Move Up	IKE-DES-MD5-DH7
IKE-3DES-MD5-DH1	Move Down	CiscoVPNClient-3DES-SHA-DSA
IKE-DES-MD5	Add	CiscoVPNClient-3DES-MD5-RSA-DH5
IKE-3DES-MD5-DH7	Modify	CiscoVPNClient-3DES-SHA-DSA-DH5
IKE-3DES-MD5-RSA	Copy	CiscoVPNClient-AES256-SHA
CiscoVPNClient-3DES-MD5-DH5	Delete	IKE-AES256-SHA
CiscoVPNClient-AES128-SHA		
IKE-AES128-SHA		

2. Vous devez également configurer la stratégie d'IPsec pour utiliser des Certificats. La **configuration > la Gestion des stratégies > la gestion de trafic > les associations de sécurité** choisies, le point culminant **ESP-3DES-MD5** et cliquent sur alors **modifier pour configurer la stratégie d'IPsec** pour configurer la stratégie d'IPsec.



3. Sur la fenêtre de modifier, sous des Certificats numériques, veillez à sélectionner votre certificat d'identité installé. Sous la proposition d'IKE, CiscoVPNClient-3DES-MD5-RSA choisis et cliquent sur Apply.



4. Afin de configurer un groupe d'IPsec, le **Configuration > User Management > Groups** choisi > **ajoutent**, ajoutent un groupe appelé l'**IPSECCERT** (le nom de groupe IPSECCERT apparie l'unité organisationnelle (OU) dans le certificat d'identité), et sélectionnent un mot de passe. Ce mot de passe n'est pas utilisé n'importe où 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. À la même page, cliquez sur l'onglet Général et assurez-vous que vous sélectionnez IPsec en tant que perçage d'un tunnel Protocol.

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

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

6. Cliquez sur l'onglet d'IPsec et assurez-vous que votre association configurée de sécurité IPsec (SA) est sélectionnée sous IPsec SA 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	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	<input checked="" type="checkbox"/>	(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	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>			

7. Afin de configurer un groupe d'IPsec sur le concentrateur VPN 3000, le **Configuration > User Management** choisi > les **utilisateurs > ajoutent**, spécifient un nom d'utilisateur, le mot de passe, et le nom de groupe, et puis cliquent sur Add. Dans l'exemple, ces champs sont utilisés : Nom d'utilisateur = cert_user Mot de passe = cisco123 Vérifiez = cisco123 Groupe = IPSECCERT

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPsec | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	cert_user	Enter a unique username.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

8. Afin d'activer l'élimination des imperfections sur la **configuration** > le **système** > les **événements** > les **classes** choisis de concentrateur VPN 3000 et ajouter ces classes :CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-10

Configuration | System | Events | Classes

This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

[Click here to configure general event parameters.](#)

Configured Event Classes	Actions
CERT IKE IKEDBG IPSEC IPSECDBG MIB2TRAP	Add Modify Delete

9. La **surveillance** choisie > commande **filtrable de procédure de connexion d'événement** pour visualiser met au point.

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

Events/Page: 100

Group: -All-

Direction: 0 dest to Newest

Get Log, Save Log, Clear Log

Navigation arrows: <<<, <<, >>, >>>

Note: Si vous décidez de changer les adresses IP, vous pouvez faire une inscription des nouvelles adresses IP et installer le certificat délivré plus tard avec ces nouvelles adresses.

Vérifiez

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

Dépannez

Référez-vous aux [problèmes de connexion de dépannage sur le concentrateur VPN 3000](#) pour davantage d'information 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](#)