

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Certificados de concentrador VPN 3000 para clientes VPN](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento incluye instrucciones paso a paso sobre cómo configurar los Cisco VPN 3000 Series Concentrators con Clientes VPN con el uso de certificados.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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.

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 del concentrador VPN 3000 para los clientes VPN.

1. La política IKE debe configurarse para utilizar certificados en el VPN 3000 Concentrator Series Manager. Para configurar la política IKE, seleccione Configuration > System > Tunneling Protocols > IPsec > **IKE Proposals** y mueva CiscoVPNClient-3DES-MD5-RSA a las Propuestas Activas.

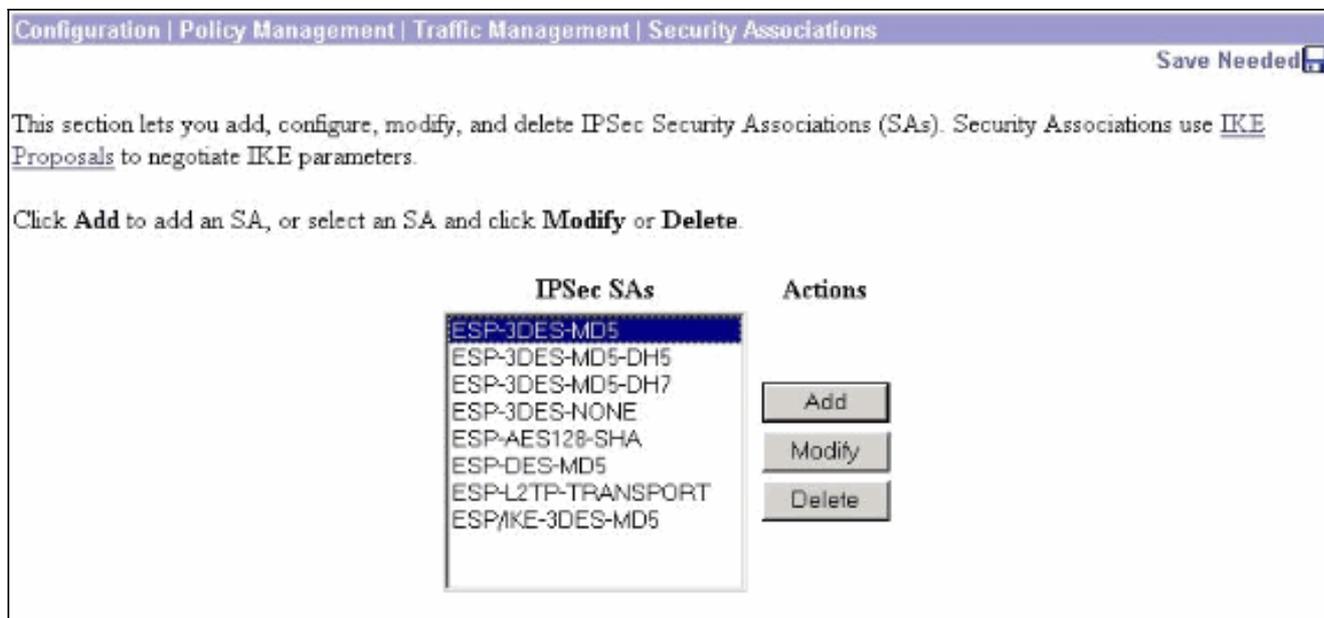
Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

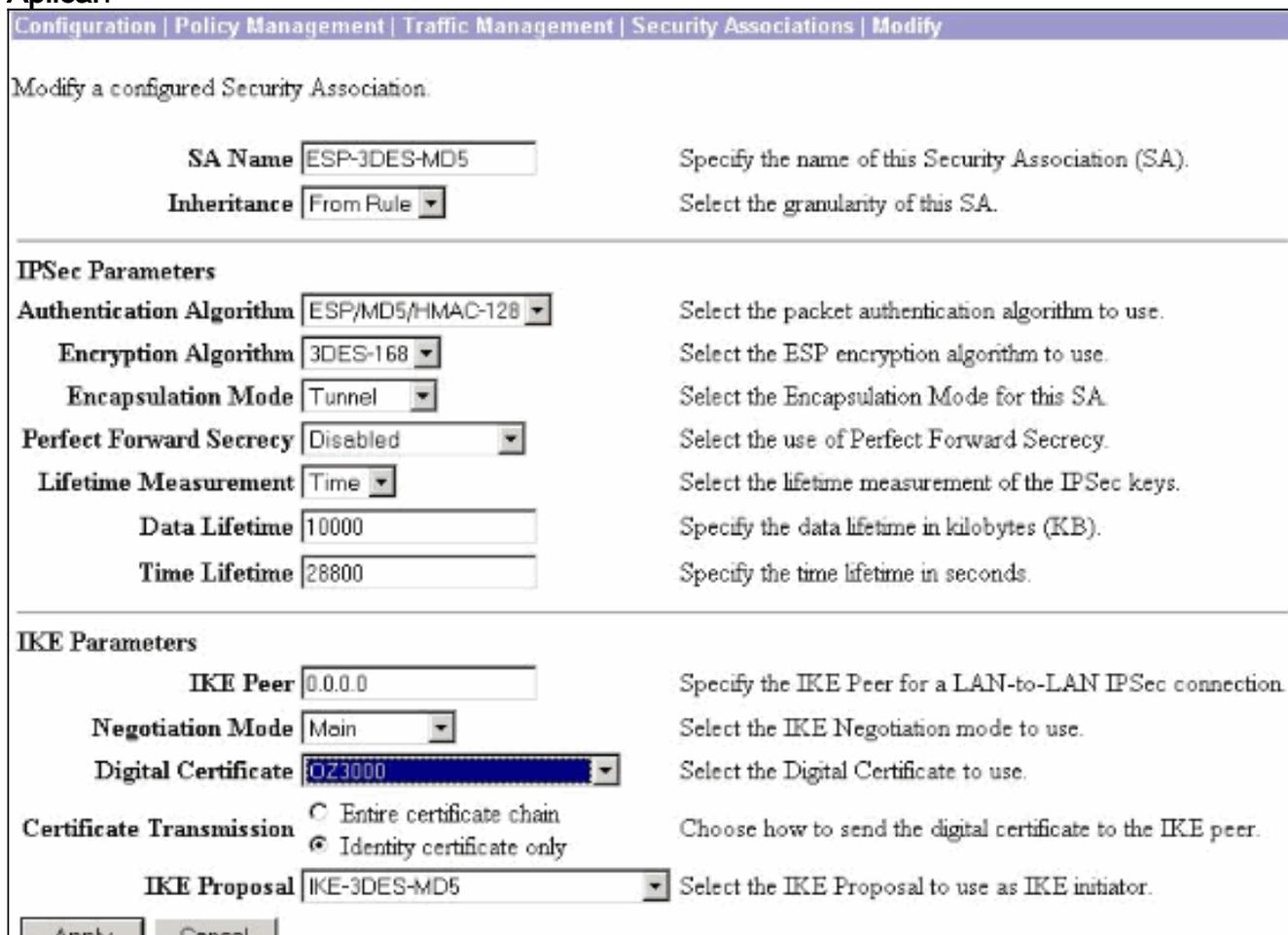
Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority. Click **Add** or **Copy** 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-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. También debe configurar la política IPsec para utilizar los certificados. Seleccione Configuration > Policy Management > Traffic Management > **Security Associations**, resalte ESP-3DES-MD5 y luego haga clic en Modify para configurar la política IPsec para configurar la política IPsec.



3. En la ventana Modificar, en Certificados digitales, asegúrese de seleccionar el certificado de identidad instalado. En Propuesta IKE, seleccione CiscoVPNClient-3DES-MD5-RSA y haga clic en **Aplicar**.



4. Para configurar un grupo IPsec, seleccione Configuration > User Management > Groups > Add, agregue un grupo llamado IPSECCERT (el nombre del grupo IPSECCERT coincide con la unidad organizativa (OU) en el certificado de identidad) y seleccione una contraseña. Esta contraseña no se utiliza en ningún lugar si utiliza certificados. En este ejemplo, "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	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Add Cancel

5. En la misma página, haga clic en la ficha General y asegúrese de seleccionar IPsec como Tunneling 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. Haga clic en la ficha IPsec y asegúrese de que la Asociación de seguridad IPsec (SA) configurada esté seleccionada en SA IPsec y haga clic en Aplicar.

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. Para configurar un grupo IPsec en el VPN 3000 Concentrator, seleccione Configuration > User Management > Users > Add, especifique un Nombre de Usuario, una Contraseña y el Nombre de Grupo, y luego haga clic en Add. En el ejemplo, se utilizan estos campos: Nombre de usuario = cert_user Contraseña = cisco123 Verificar = cisco123 Grupo = 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. Para habilitar la depuración en el VPN 3000 Concentrator, seleccione **Configuration > System > Events > Classes** y agregue estas clases: 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. Seleccione **Monitoring > Filterable Event Log** para ver las depuraciones.

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: <<<, <<, >>, >>>

Nota: Si decide cambiar las direcciones IP, puede inscribirse en las nuevas direcciones IP e instalar el certificado emitido más tarde con esas nuevas direcciones.

[Verificación](#)

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

[Troubleshoot](#)

Consulte [Resolución de Problemas de Conexión en el VPN 3000 Concentrator](#) para obtener más información sobre la solución de problemas.

[Información Relacionada](#)

- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Negociación IPSec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)