

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

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

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

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

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

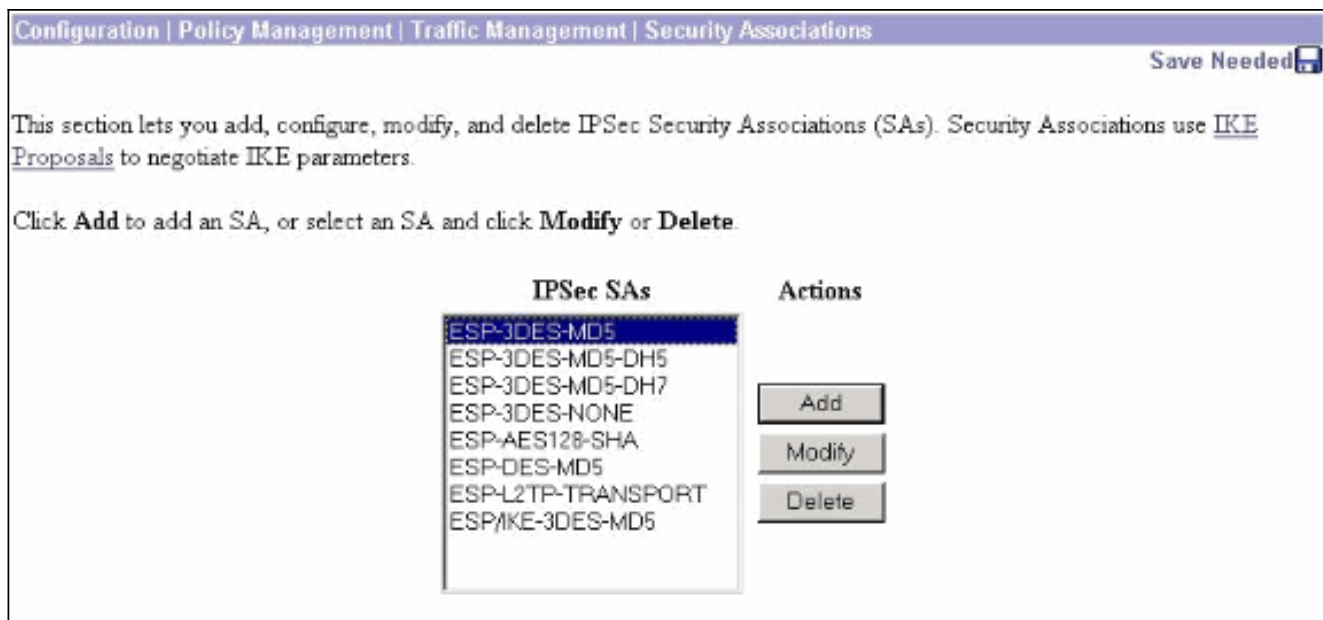
Complete estos pasos para configurar los Certificados concentradores VPN 3000 para los clientes VPN.

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.

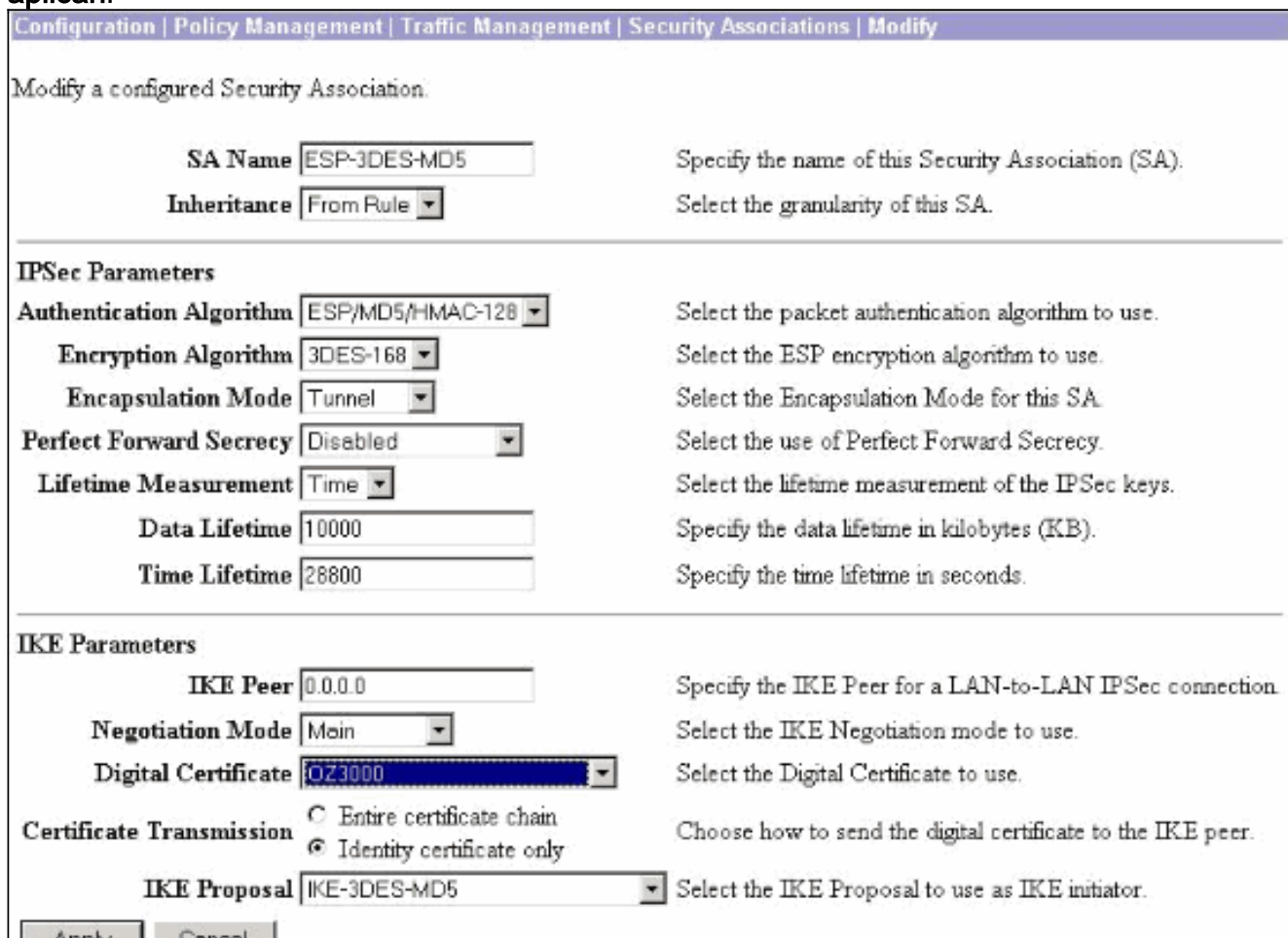
The screenshot shows the 'IKE Proposals' configuration page. At the top, there is a breadcrumb trail: 'Configuration | System | Tunneling Protocols | IPSec | IKE Proposals'. A 'Save Needed' icon is in the top right corner. Below the breadcrumb, there is a description: 'Add, delete, prioritize, and configure IKE Proposals.' followed by 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. 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, asegúrese de seleccionar su certificado de identidad instalado. Bajo la propuesta IKE, CiscoVPNClient-3DES-MD5-RSA seleccione y el teclado 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

- En la misma página, haga clic la ficha general y asegúrese 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-	<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.

- Haga clic la lengüeta del IPsec y asegúrese 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	<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 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 Add. En el ejemplo, se utilizan estos campos: Nombre de usuario = cert_user Contraseña = cisco123 Verifique = 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 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

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

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes (dropdown menu with options: AUTH, AUTHDBG, AUTHDECODE)

Severities: ALL (dropdown menu with options: 1, 2, 3)

Client IP Address: 0.0.0.0 (text input)

Events/Page: 100 (dropdown menu)

Group: -All- (dropdown menu)

Direction: 0 dest to Newest (dropdown menu)

Buttons: <<< << >> >>> Get Log Save Log Clear Log

Buttons: <<< << >> >>>

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](#)