

Configuração do VPN 3000 Concentrator para se comunicar com o VPN Client usando certificados

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Certificados do VPN 3000 Concentrator para clientes VPN](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento inclui instruções passo a passo em como configurar o Concentradores Cisco VPN série 3000 com os clientes VPN com o uso dos Certificados.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

A informação neste documento é baseada na versão de software 4.0.4A do Cisco VPN 3000 Concentrator.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Certificados do VPN 3000 Concentrador para clientes VPN

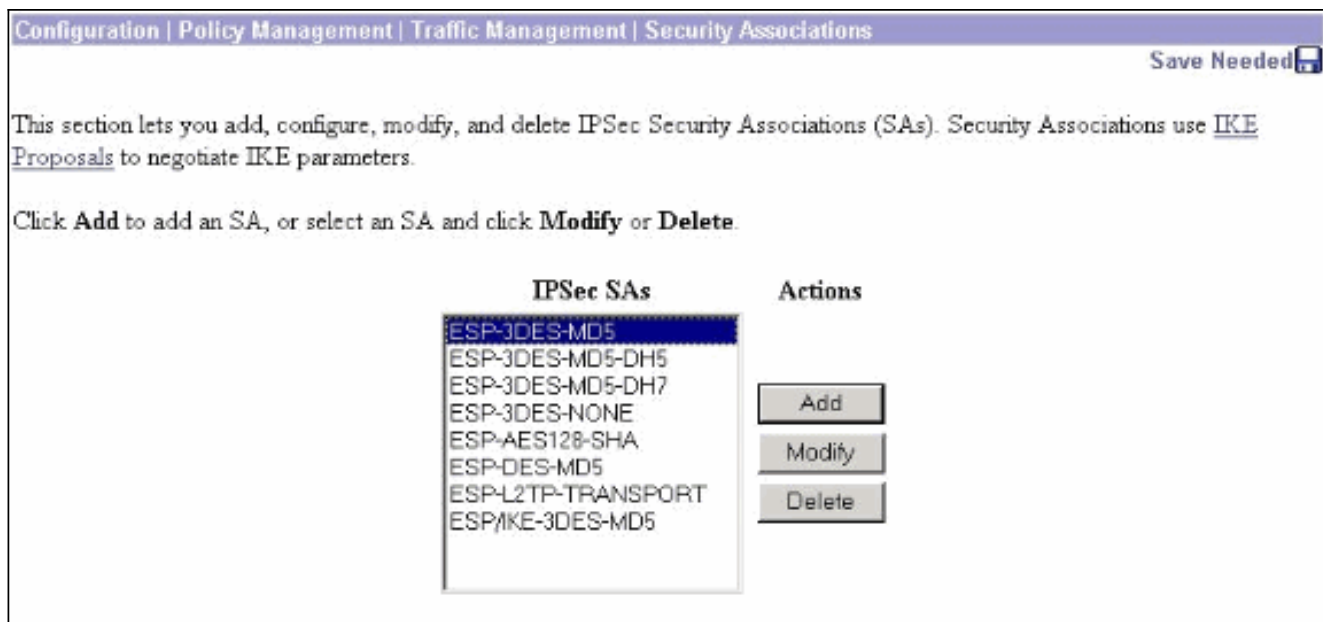
Termine estas etapas a fim configurar Certificados do VPN 3000 concentrador para clientes VPN.

1. A política de IKE deve ser configurada para usar Certificados no gerente da VPN 3000 Concentrador Series. A fim configurar a política de IKE, o **configuração > sistema > protocolos de tunelamento > IPSEC > propostas de IKE** seletor, e o movimento **CiscoVPNClient-3DES-MD5-RSA** aos propósitos ativo.

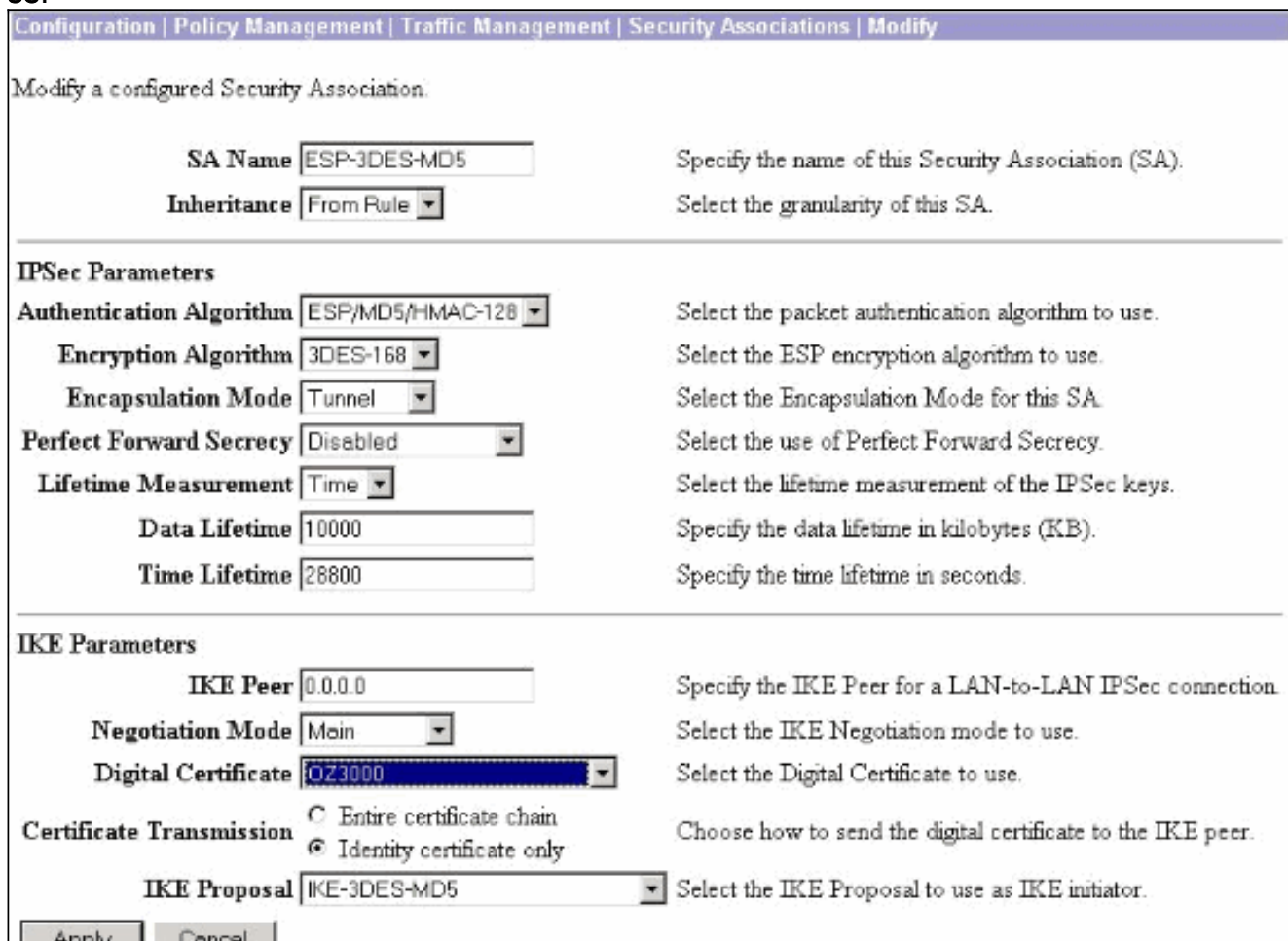
The screenshot shows the 'IKE Proposals' configuration page. The breadcrumb trail is 'Configuration | System | Tunneling Protocols | IPsec | IKE Proposals'. A 'Save Needed' button is in the top right. Below the breadcrumb, there is a description: 'Add, delete, prioritize, and configure IKE Proposals.' 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. Você deve igualmente configurar a política de IPsec para usar Certificados. O **Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança** seletor, o destaque **ESP-3DES-MD5** e clica então **altera** para configurar a política de IPsec para configurar a política de IPsec.



3. No indicador da alteração, sob Certificados digitais, certifique-se selecionar seu certificado de identidade instalado. Sob a proposta IKE, CiscoVPNClient-3DES-MD5-RSA seletos e o clique **aplicam-se**.



4. A fim configurar um grupo IPSec, selecione o **configuração > gerenciamento de usuário > grupos > adicionar**, adicionam um grupo chamado IPSECCERT (o nome do grupo IPSECCERT combina a unidade organizacional (OU) no certificado de identidade), e selecionam uma senha. Esta senha não é usada em qualquer lugar se você usa Certificados. Neste exemplo, "cisco123" é a senha.

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. Na mesma página, clique o tab geral e certifique-se de que você seleciona o IPsec como o protocolo de tunelamento.

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. Clique a aba do IPsec e certifique-se de que sua associação de segurança IPsec configurada (SA) está selecionada sob IPsec SA e clique **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. A fim configurar um grupo IPSec no VPN 3000 concentrator, selecione o **configuração > gerenciamento de usuário > usuários > adicionar**, especifique um nome de usuário, a senha, e o nome do grupo, e clique-os então **adicionam**. No exemplo, estes campos são usados: Nome de usuário = cert_user Senha = 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. A fim permitir a eliminação de erros no **configuração > sistema > eventos > classes** seletor do VPN 3000 concentrator e adicionar estas 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	Add Modify Delete
IKE	
IKEDBG	
IPSEC	
IPSECDBG	
MIB2TRAP	

9. A **monitoração** seletor > ordem filtrável do início de uma sessão do evento para ver debuga.

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

Note: Se você decide mudar os endereços IP de Um ou Mais Servidores Cisco ICM NT, você pode fazer um registro dos endereços IP de Um ou Mais Servidores Cisco ICM NT novos e instalar o certificado emitido mais atrasado com aqueles endereços novos.

[Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

[Troubleshooting](#)

Refira [pesquisando defeitos problemas de conexão no VPN 3000 concentrator](#) para a informação adicional de Troubleshooting.

[Informações Relacionadas](#)

- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)