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

Contents

Introduction

Este documento inclui instruções passo a passo sobre como configurar os Cisco VPN 3000 Series Concentrators with VPN Clients com o uso de certificados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software Cisco VPN 3000 Concentrator versão 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.

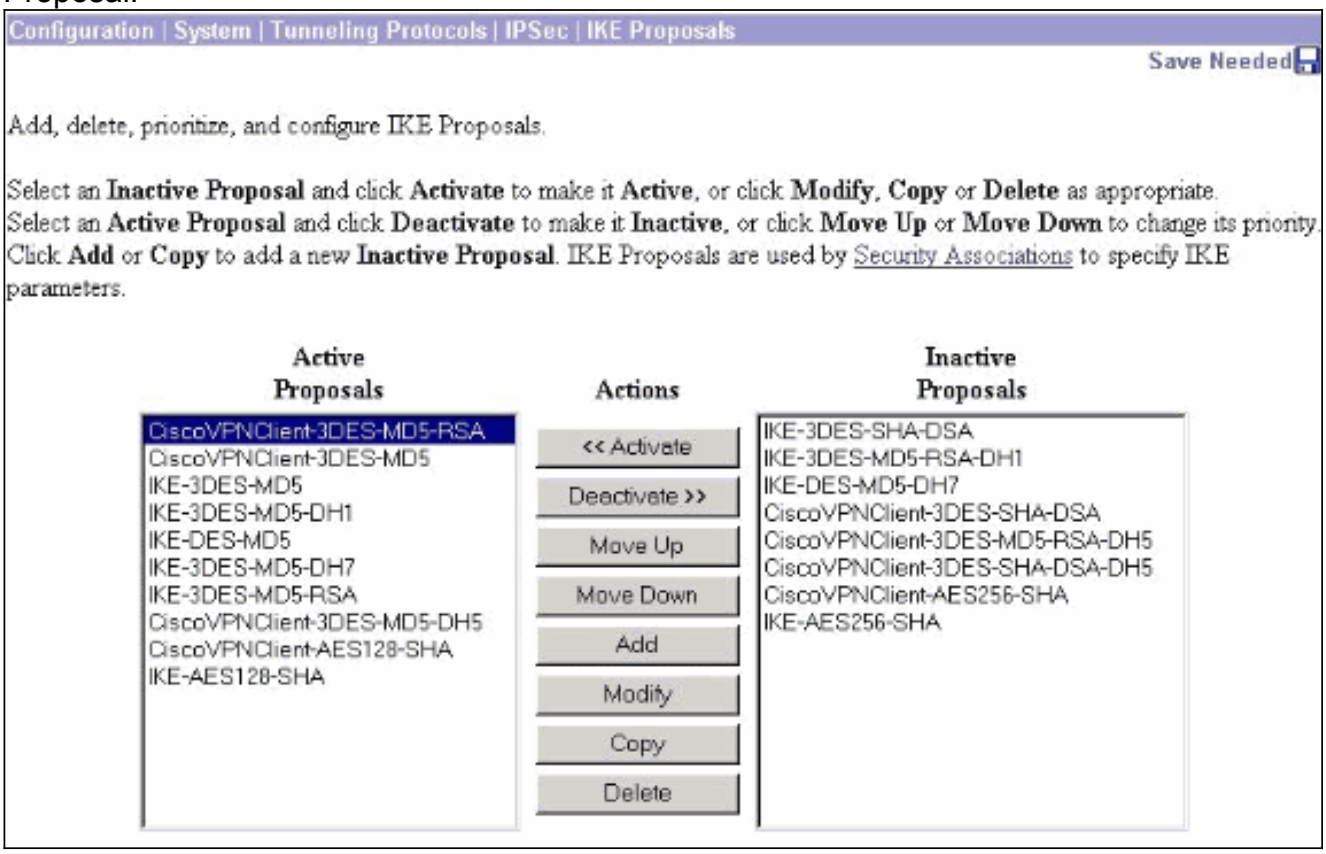
Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

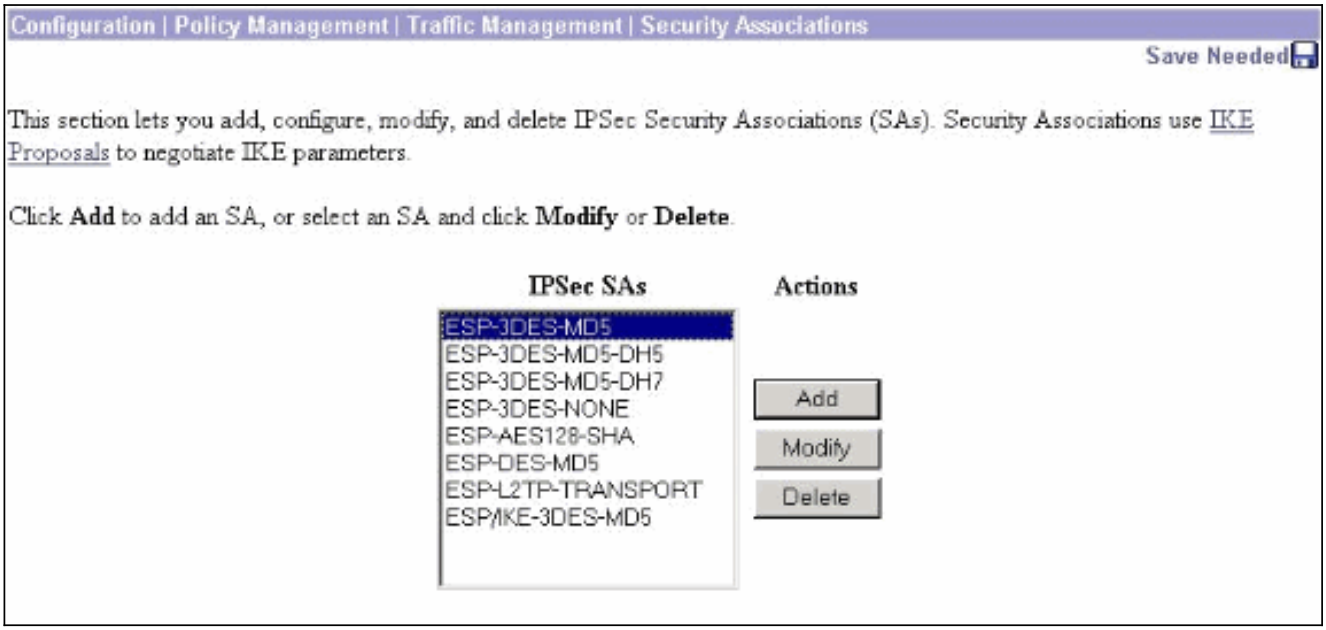
Certificados do VPN 3000 Concentrator para clientes VPN

Conclua estes passos para configurar certificados do VPN 3000 Concentrator para VPN Clients.

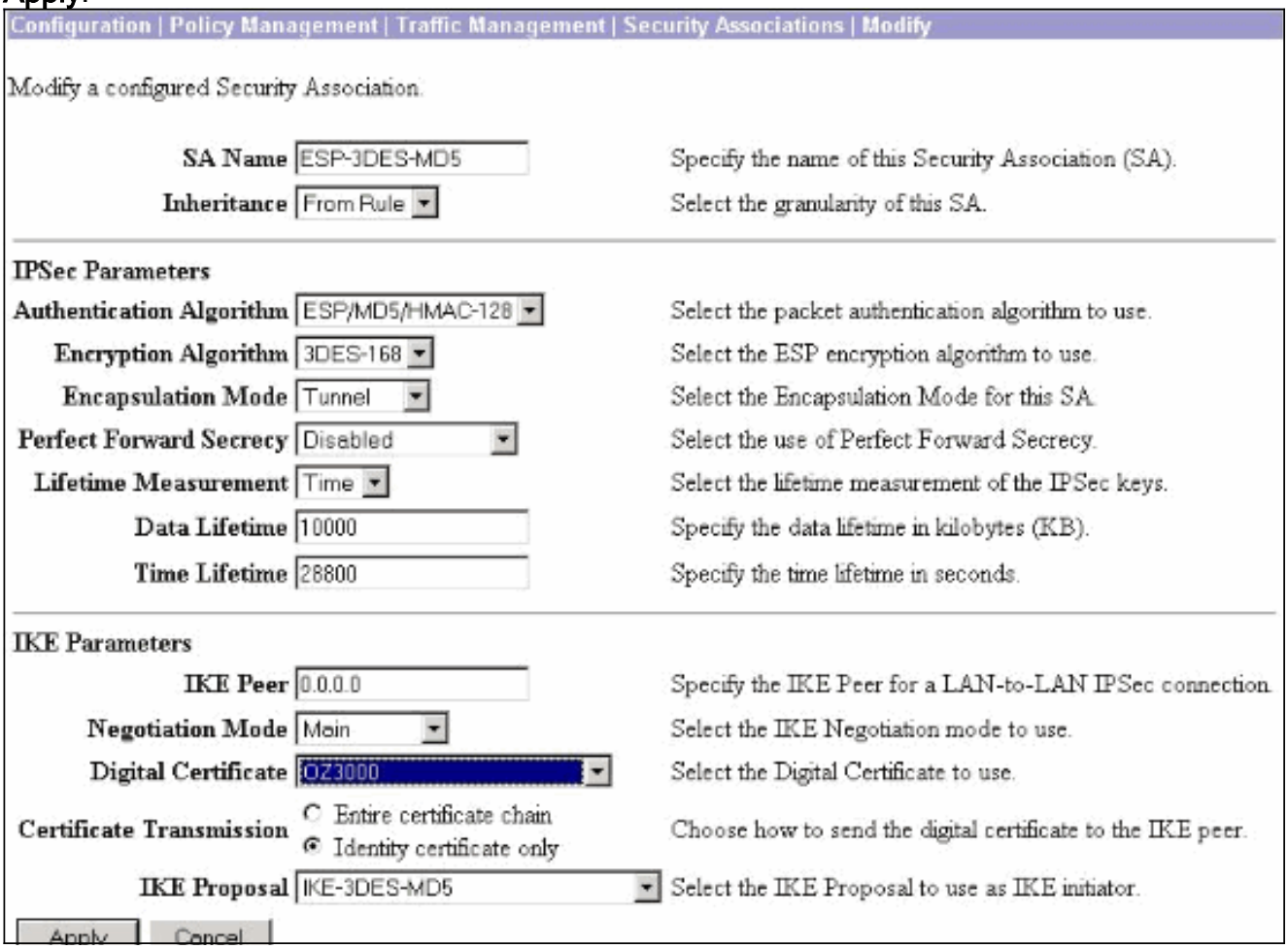
1. A política IKE deve ser configurada para usar certificados no VPN 3000 Concentrator Series Manager. Para configurar a política de IKE, selecione Configuration > System > Tunneling Protocols > **IPsec > IKE Proposal** e mova o **CiscoVPNClient-3DES-MD5-RSA** para as Ative Proposal.



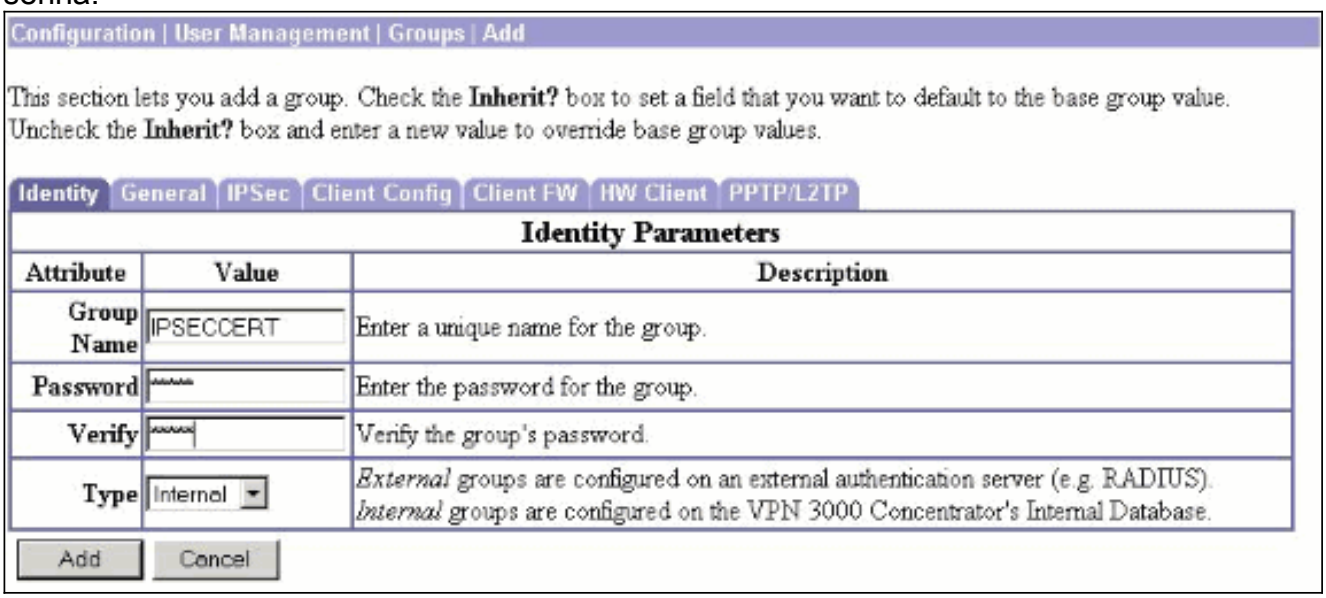
2. Você também deve configurar a política de IPsec para usar certificados. Selecione Configuration > Policy Management > Traffic Management > **Security Associations**, realce **ESP-3DES-MD5** e clique em **Modify para configurar a política de IPsec** para configurar a política de
IPsec.



3. Na janela Modificar, em Certificados Digitais, selecione o certificado de identidade instalado. Em IKE Proposal, selecione **CiscoVPNClient-3DES-MD5-RSA** e clique em **Apply**.

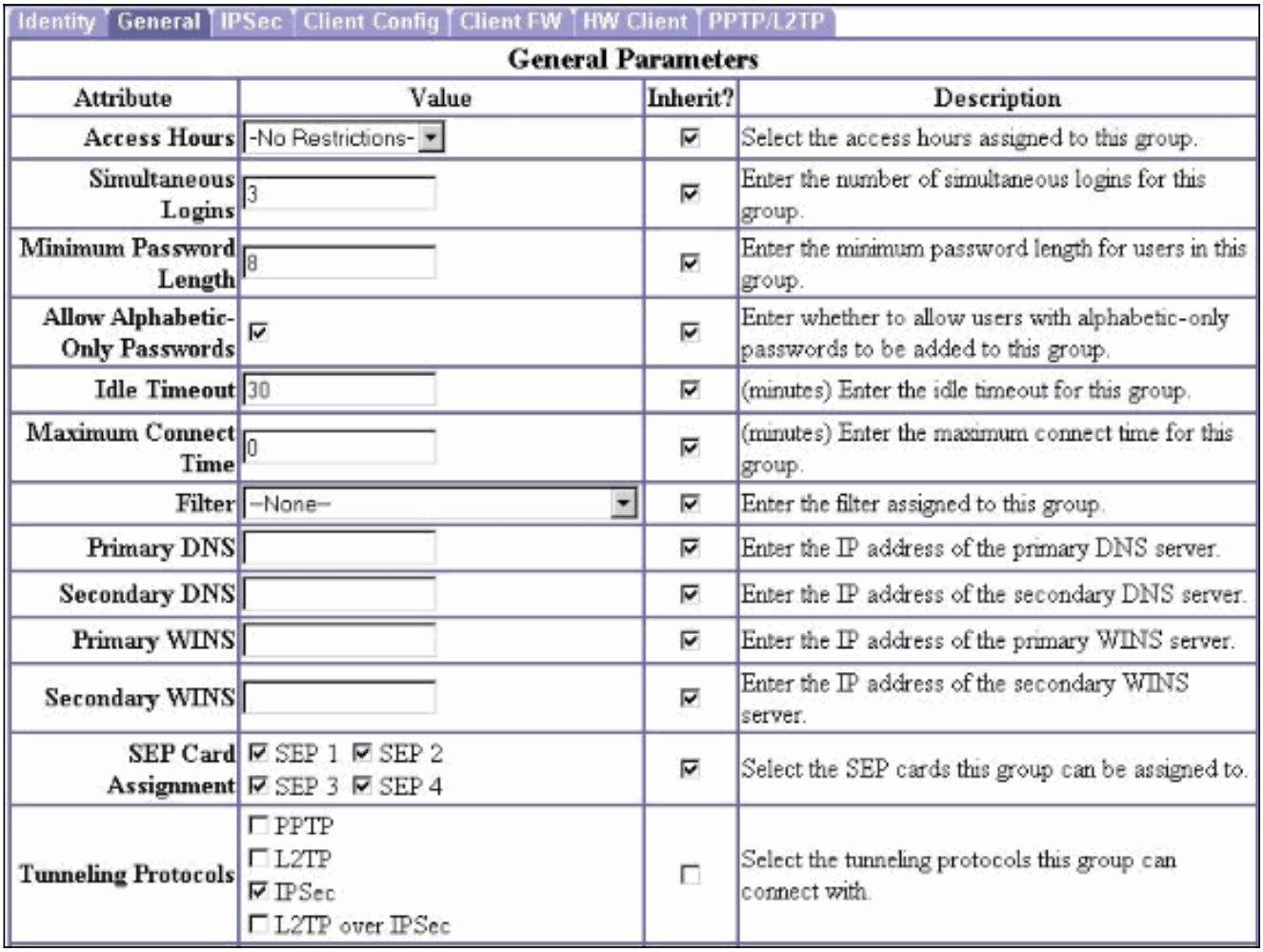


4. Para configurar um grupo IPsec, selecione Configuration > **User Management > Groups > Add**, adicione um grupo chamado **IPSECCERT** (o nome do grupo IPSECCERT corresponde à OU (Organizational Unit, unidade organizacional) no certificado de identidade) e selecione uma senha.Esta senha não será usada em nenhum lugar se você usar certificados. Neste exemplo, "cisco123" é a
senha.



5. Na mesma página, clique na guia Geral e certifique-se de selecionar **IPsec** como o Tunneling

Protocol.

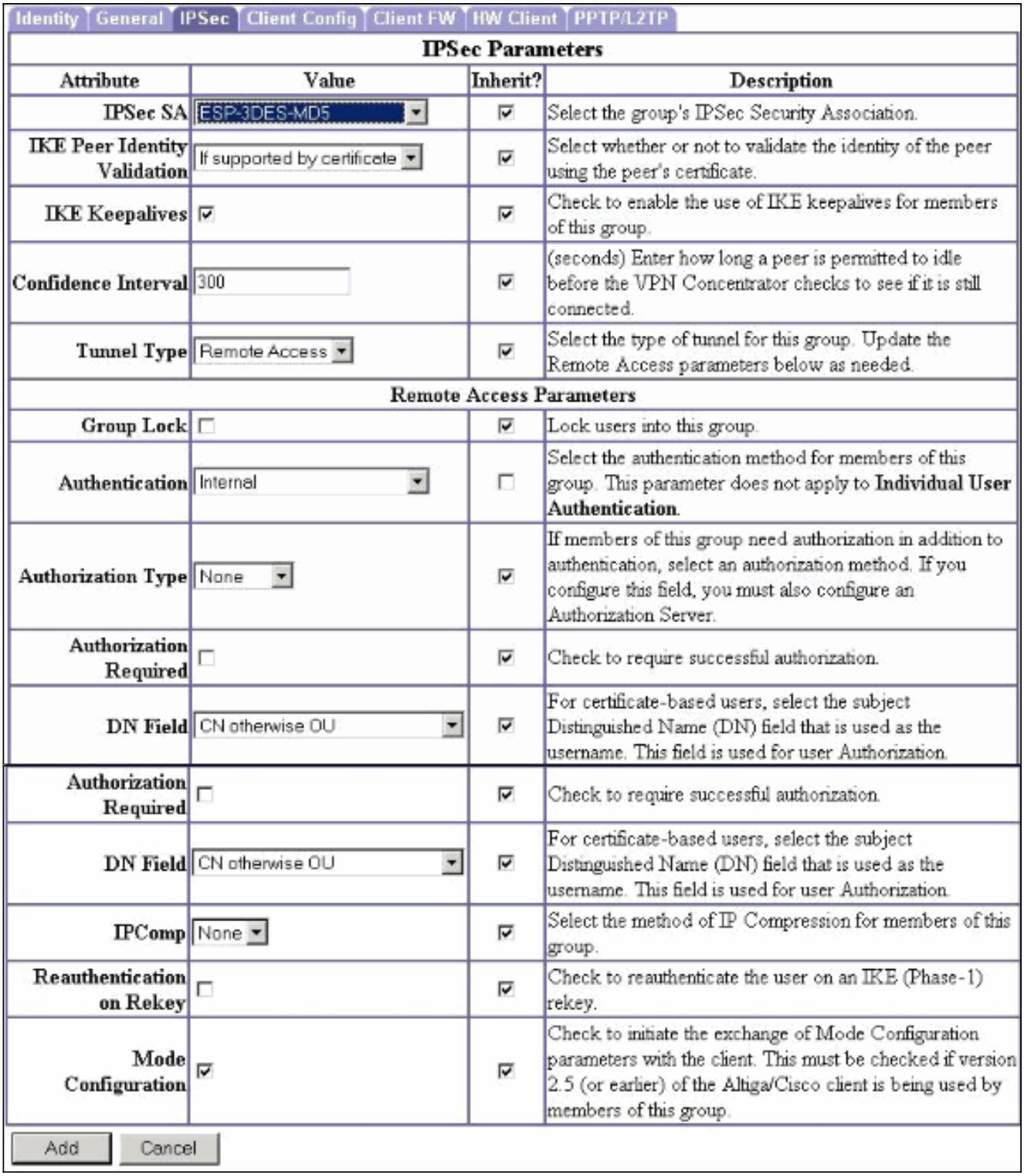


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Clique na guia IPsec (IPsec) e certifique-se de que a associação de segurança (SA) IPsec configurada esteja selecionada em IPsec SA e clique em **Apply**.



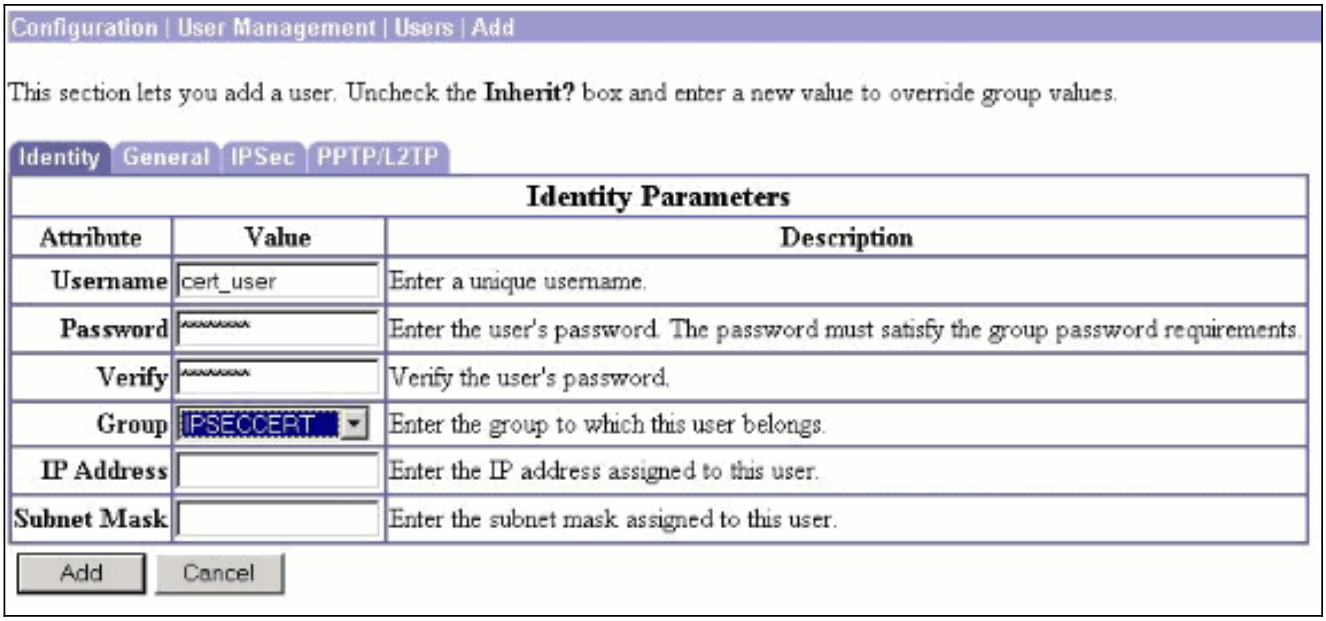
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

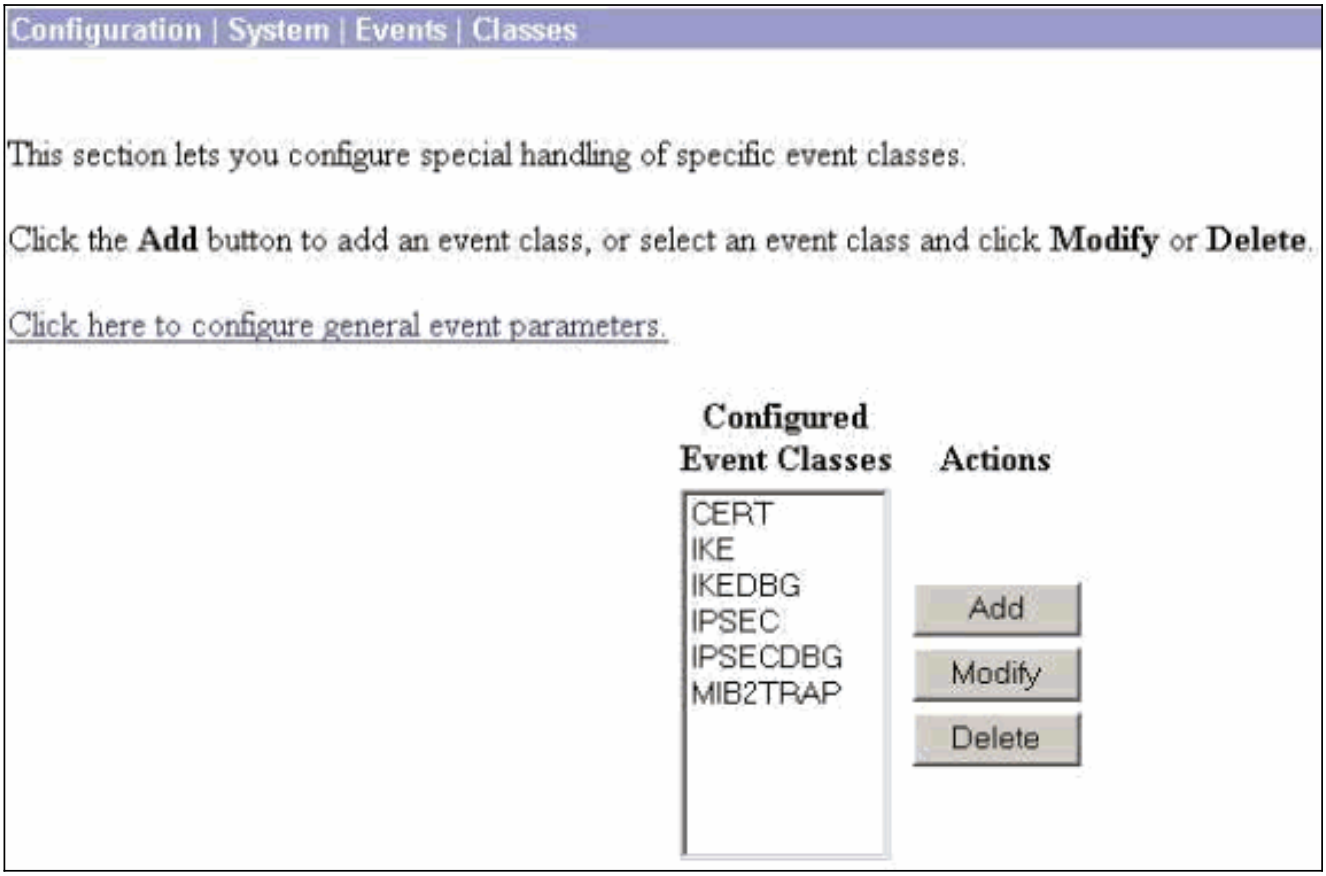
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of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

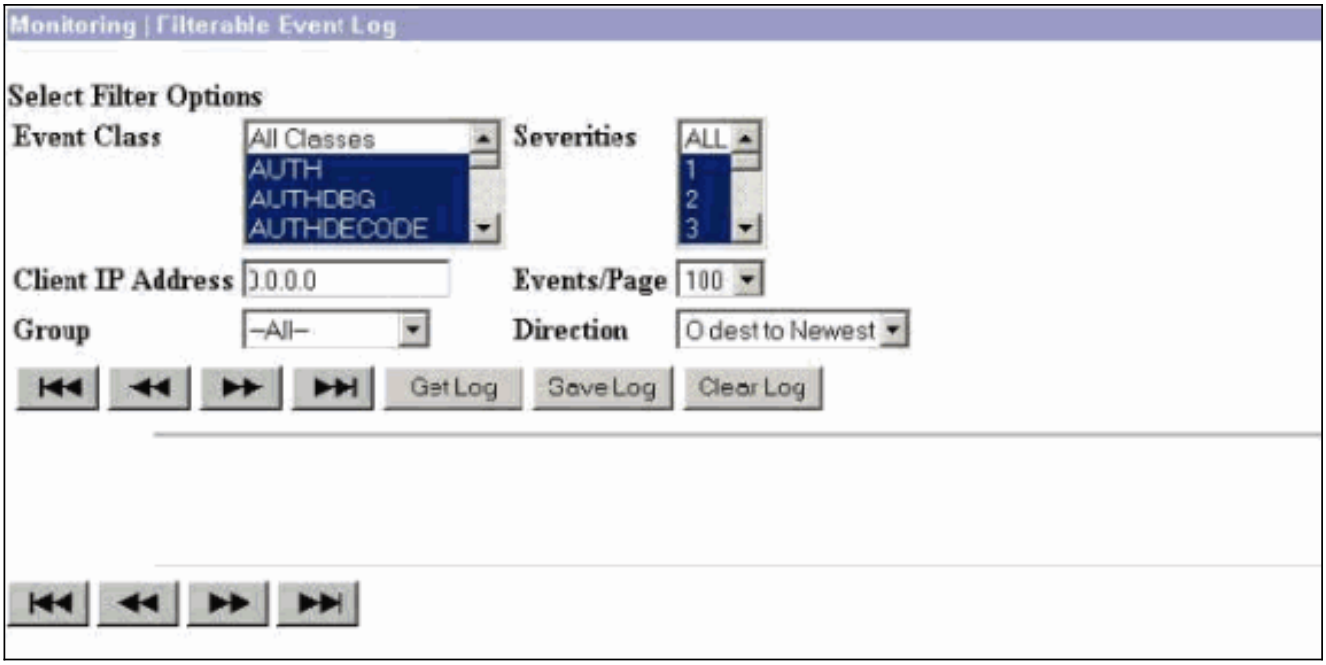
7. Para configurar um grupo IPsec no VPN 3000 Concentrator, selecione Configuration **> User Management > Users > Add**, especifique um User Name, Password e o nome do grupo e clique em **Add**.No exemplo, esses campos são usados:Nome de usuário = cert_userSenha = cisco123Verificar = cisco123Grupo = IPSECCERT



8. Para habilitar a depuração no VPN 3000 Concentrator, selecione **Configuration > System > Events > Classes** e adicione estas classes:CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. Selecione **Monitoring > Filterable Event Log** para exibir as depurações.



Observação: se você decidir alterar os endereços IP, poderá fazer uma inscrição dos novos endereços IP e instalar o certificado emitido posteriormente com esses novos endereços.

Verificar

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

Troubleshoot

Consulte Troubleshooting de Problemas de Conexão no VPN 3000 Concentrator para obter mais informações sobre troubleshooting.

Informações Relacionadas

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems