

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

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

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[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 Concentrador para clientes VPN

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

1. A política IKE deve ser configurada para usar certificados no VPN 3000 Concentrador 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 Active Proposal.

The screenshot shows the 'IKE Proposals' configuration page. The breadcrumb trail is 'Configuration | System | Tunneling Protocols | IPsec | IKE Proposals'. A 'Save Needed' icon 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 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.

The screenshot shows the 'Security Associations' configuration page. The breadcrumb trail is 'Configuration | Policy Management | Traffic Management | Security Associations'. A 'Save Needed' icon is in the top right. Below the breadcrumb, there is a description: 'This section lets you add, configure, modify, and delete IPsec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.' and instructions: 'Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.'

| IPsec SAs | Actions |
|--------------------|---------|
| ESP-3DES-MD5 | Add |
| ESP-3DES-MD5-DH5 | Modify |
| ESP-3DES-MD5-DH7 | Delete |
| ESP-3DES-NONE | |
| ESP-AES128-SHA | |
| ESP-DES-MD5 | |
| ESP-L2TP-TRANSPORT | |
| ESP/IKE-3DES-MD5 | |

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**.

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

Certificate Transmission Entire certificate chain Choose how to send the digital certificate to the IKE peer.
 Identity certificate only

IKE Proposal Select the IKE Proposal to use as IKE initiator.

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.

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 | <input type="text" value="IPSECCERT"/> | Enter a unique name for the group. |
| Password | <input type="text" value="cisco123"/> | Enter the password for the group. |
| Verify | <input type="text" value="cisco123"/> | Verify the group's password. |
| Type | <input type="text" value="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> |

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- | <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 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 | <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 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

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 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

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

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE

Severities: ALL, 1, 2, 3

Client IP Address: J.0.0.0

Events/Page: 100

Group: -All-

Direction: O dest to Newest

Get Log, Save Log, Clear Log

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](#)