

Configurando o VPN 3000 concentrator PPTP com autenticação RADIUS do Cisco Secure ACS for Windows

Índice

[Introdução](#)

[Antes de Começar](#)

[Convenções](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configurando o VPN 3000 Concentrator](#)

[Adicionando e configurando o Cisco Secure ACS for Windows](#)

[Adicionando MPPE \(Criptografia\)](#)

[Relatório de adição](#)

[Verificar](#)

[Troubleshooting](#)

[Permitindo a eliminação de erros](#)

[Debuga - Boa autenticação](#)

[Possíveis erros](#)

[Informações Relacionadas](#)

[Introdução](#)

O Cisco VPN 3000 Concentrator apoia o método de tunelamento do protocolo de túnel Point-to-Point (PPTP) para clientes das janelas nativas. Os suportes de concentrador 40-bit e criptografia do 128-bit para uma conexão confiável fixada. Este documento descreve como configurar o PPTP em um VPN 3000 concentrator com o Cisco Secure ACS for Windows para a autenticação RADIUS.

Refira [configurar o firewall PIX segura Cisco para usar o PPTP](#) para configurar conexões PPTP ao PIX.

Refira [configurar a autenticação de PPTP do roteador do Cisco Secure ACS for Windows](#) para estabelecer uma conexão PC ao roteador; isto fornece a autenticação de usuário ao Cisco Secure Access Control System (ACS) 3.2 para o Windows Server antes que você permita o usuário na rede.

[Antes de Começar](#)

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Pré-requisitos

Este documento supõe que a autenticação de PPTP local está trabalhando antes de adicionar a autenticação RADIUS do Cisco Secure ACS for Windows. Veja por favor [como configurar o VPN 3000 concentrator PPTP com autenticação local](#) para obter mais informações sobre da autenticação de PPTP local. Para uma lista completa das exigências e das limitações, refira por favor [quando é a criptografia de PPTP apoiada em um Cisco VPN 3000 Concentrator?](#)

Componentes Utilizados

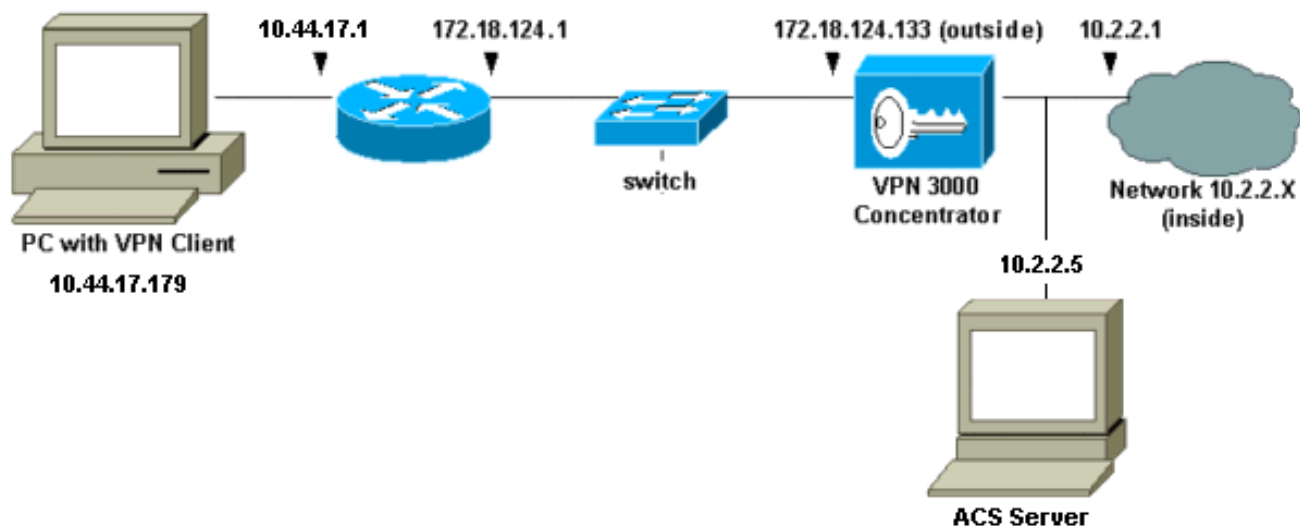
As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Versões 2.5 e mais recente do Cisco Secure ACS for Windows
- Versões 2.5.2.C e mais recente do VPN 3000 concentrator (esta configuração foi verificada com versão 4.0.x.)

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 você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



Configurando o VPN 3000 Concentrator

Adicionando e configurando o Cisco Secure ACS for Windows

Siga estas etapas para configurar o concentrador VPN para usar o Cisco Secure ACS for Windows.

1. No VPN 3000 concentrador, vá ao **Configuração > Sistema > Servidores > Servidores de Autenticação** e adicionar o server do Cisco Secure ACS for Windows e a chave ("cisco123" neste exemplo).

The screenshot shows a configuration window titled "Configuration | System | Servers | Authentication | Add". The main instruction is "Configure and add a user authentication server." Below this, there are several fields and a button:

- Server Type:** A dropdown menu is set to "RADIUS". A tooltip points to it, stating: "Selecting *Internal Server* will let you add users to the internal user database."
- Authentication Server:** A text box containing "10.2.2.5" with the instruction "Enter IP address or hostname."
- Server Port:** A text box containing "0" with the instruction "Enter 0 for default port (1645)."
- Timeout:** A text box containing "4" with the instruction "Enter the timeout for this server (seconds)."
- Retries:** A text box containing "2" with the instruction "Enter the number of retries for this server."
- Server Secret:** A text box with masked characters (asterisks) and the instruction "Enter the RADIUS server secret."
- Verify:** A text box with masked characters and the instruction "Re-enter the secret."

At the bottom left, there are two buttons: "Add" and "Cancel". A mouse cursor is pointing at the "Add" button.

2. No Cisco Secure ACS for Windows, adicionar o concentrador VPN à configuração de rede do servidor ACS, e identifique o tipo de

Access Server Setup For VPN3000

Network Access Server IP Address	<input type="text" value="10.2.2.1"/>
Key	<input type="text" value="cisco123"/>
Network Device Group	<input type="text" value="(Not Assigned)"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/>	Single Connect TACACS+ NAS (Record stop in accounting on failure).
<input type="checkbox"/>	Log Update/Watchdog Packets from this Access Server
<input type="checkbox"/>	Log Radius Tunneling Packets from this Access Server

dicionário.

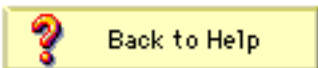
3. No Cisco Secure ACS for Windows, vá a **Interface Configuration > Radius (Microsoft)** e verifique os atributos da criptografia Point-to-Point microsoft (MPPE) de modo que os atributos apareçam na interface de

Edit

RADIUS (Microsoft)

User Group

- [026/311/007]
MS-MPPE-Encryption-Policy]
- [026/311/008]
MS-MPPE-Encryption-Types
- [026/311/012]
MS-CHAP-MPPE-Keys
- [026/311/016] MS-MPPE-Send-Key
- [026/311/017]
MS-MPPE-Recv-Key

 Back to Help

grupo.

4. No Cisco Secure ACS for Windows, adicionar um usuário. No grupo de usuário, adicionar os atributos MPPE (Microsoft RADIUS), caso que você exige a criptografia mais

Access Restrictions	Token Cards	Password Aging
IP Address Assignment	IETF Radius	Cisco VPN3000 Radius
MS MPPE Radius		

Microsoft RADIUS Attributes ?

[311\007] MS-MPPE-Encryption-Policy

Encryption Allowed ▾

[311\008] MS-MPPE-Encryption-Types

40-bit ▾

[311\012] MS-CHAP-MPPE-Keys

[311\016] MS-MPPE-Send-Key

[311\017] MS-MPPE-Recv-Key

tarde.

- No VPN 3000 concentrator, vá ao **Configuração > Sistema > Servidores > Servidores de Autenticação**. Selecione um Authentication Server da lista, e selecione então o teste. Autenticação de teste do concentrador VPN ao server do Cisco Secure ACS for Windows incorporando um nome de usuário e senha. Em uma boa autenticação, o concentrador VPN deve mostrar um mensagem " autenticação bem-sucedida ". As falhas no Cisco Secure ACS for Windows são **relatórios e atividade > falhas de tentativa** entrados. Em um padrão instale, estes relatórios são armazenados no disco em tentativas de C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed.

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name

Password


OK Cancel

- Desde que você tem verificado agora a autenticação do PC aos trabalhos do concentrador VPN e do concentrador ao server do Cisco Secure ACS for Windows, você pode reconfigurar o concentrador VPN para enviar usuários PPTP ao RAI0 do Cisco Secure ACS for Windows movendo o server do Cisco Secure ACS for Windows para a parte superior da lista de servidor. Para fazer isto no concentrador VPN, vá ao **Configuração > Sistema > Servidores > Servidores de Autenticação**.

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Authentication Servers	Actions
10.2.2.5 (Radius)  Internal (Internal)	<input type="button" value="Add"/>
	<input type="button" value="Modify"/>
	<input type="button" value="Delete"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>
	<input type="button" value="Test"/>

7. Vá ao **configuration > user management > ao grupo base** e selecione a aba **PPTP/L2TP**. No grupo base do concentrador VPN, assegure-se de que as opções para o PAP e o MSCHAPv1 estejam permitidas.

Configuration | User Management | Base Group

General IPsec **PPTP/L2TP**

PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input checked="" type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

8. Selecione o **tab geral** e assegure-se de que o PPTP esteja permitido na seção dos protocolos de tunelamento.

Idle Timeout	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect time	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
Filter	<input type="text" value="-None-"/>	Select the filter assigned to this group.
Primary DNS	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
Secondary DNS	<input type="text"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
Secondary WINS	<input type="text"/>	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	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.

9. Teste a autenticação de PPTP com o usuário no servidor Radius do Cisco Secure ACS for Windows. Se isto não trabalha, para satisfazer veja a [seção de debugging](#).

[Adicionando MPPE \(Criptografia\)](#)

Se a autenticação de PPTP do RAI0 do Cisco Secure ACS for Windows trabalha sem criptografia, você pode adicionar o MPPE ao VPN 3000 concentrator.

1. No concentrador VPN, vá ao **configuration > user management > ao grupo base**.
2. Sob a seção para a criptografia de PPTP, verifique as opções para ver se há **exigido, 40-bit, e 128-bit**. Desde que não todos os PC apoiam 40-bit e criptografia do 128-bit, verifique ambas as opções para permitir a negociação.
3. Sob a seção para protocolos de autenticação de PPTP, verifique a opção para ver se há o **MSCHAPv1**. (Você já configurou os atributos de usuário do Cisco Secure ACS for Windows 2.5 para a criptografia em uma etapa mais adiantada.)

PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking all options means that no authentication is required.
PPTP Encryption	<input checked="" type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

Nota: O cliente de PPTP deve ser reconhecido para ótimo ou criptografia de dados obrigatória e MSCHAPv1 (se uma opção).

[Relatório de adição](#)

Depois que você estabeleceu a autenticação, você pode adicionar a contabilidade ao concentrador VPN. Vá ao **Configuração > Sistema > Servidores > Servidores de Contabilidade** e adicionar o server do Cisco Secure ACS for Windows.

No Cisco Secure ACS for Windows, os registros de contabilidade aparecem como segue.

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id,
Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets,
Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

[Verificar](#)

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

[Troubleshooting](#)

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

[Permitindo a eliminação de erros](#)

Se as conexões não trabalham, você pode adicionar o PPTP e as classes de evento de autenticação ao concentrador VPN indo ao **Configuração > Sistema > Eventos > Classes > Modificar**. Você pode igualmente adicionar o PPTPDBG, o PPTPDECODE, o AUTHDBG, e as classes de evento authdecode, mas estas opções podem fornecer demasiada informação.

Configuration | System | Events | Classes | Modify

This screen lets you modify an event class configured for special handling.

Class Name	<input type="text" value="PPTP"/>	
Enable	<input checked="" type="checkbox"/>	Check to enable special handling of this class.
Severity to Log	<input type="text" value="1-9"/>	Select the range of severity values to enter in the log.
Severity to Console	<input type="text" value="1-3"/>	Select the range of severity values to display on the console.
Severity to Syslog	<input type="text" value="None"/>	Select the range of severity values to send to a Syslog server.
Severity to Email	<input type="text" value="None"/>	Select the range of severity values to send via email to the recipient list.
Severity to Trap	<input type="text" value="None"/>	Select the range of severity values to send to an SNMP system.

Você pode recuperar o log de eventos indo à **monitoração > log de eventos**.

Monitoring | Event Log

Select Filter Options

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

Severities: ALL (dropdown menu showing 1, 2, 3)

Client IP Address: 0.0.0.0 (text input)

Events/Page: 100 (dropdown menu)

Direction: Oldest to Newest (dropdown menu)

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

```

1 12/04/2000 14:51:32.600 SEV=4 AUTH/22 RPT=21
User pptpuser disconnected

2 12/04/2000 14:51:32.600 SEV=4 PPTP/35 RPT=14 10.44.17.179
Session closed on tunnel 10.44.17.179 (peer 0, local 45636, serial 0), re
Administrative shutdown (No additional info)

4 12/04/2000 14:51:32.640 SEV=4 PPTP/34 RPT=14 10.44.17.179
Tunnel to peer 10.44.17.179 closed, reason: Stop-Local-Shutdown (No addit
info)

6 12/04/2000 14:51:49.150 SEV=4 PPTP/47 RPT=15 10.44.17.179
Tunnel to peer 10.44.17.179 established

```

[Debuga - Boa autenticação](#)

Os debug correto no concentrador VPN olharão similares ao seguinte.

```

1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected

```

[Possíveis erros](#)

Você pode encontrar possíveis erros como mostrado abaixo.

[Nome de usuário incorreto ou senha no servidor Radius do Cisco Secure ACS for Windows](#)

- **Resultado do debug do VPN 3000 concentrator**6 12/06/2000 09:33:03.910 SEV=4 PPTP/47
RPT=21 10.44.17.179
Tunnel to peer 10.44.17.179 established
- 7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179
- 8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23
- 9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser
- 11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [baduser]
disconnected.. failed authentication (MSCHAP-V1)
- 12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
- **Registro de saída do Cisco Secure ACS for Windows**03/18/2000,08:02:47,Authen failed,
baduser,,,CS user
unknown,,,1155,10.2.2.1
- **A mensagem que o usuário vê (de Windows 98)**Error 691: The computer you have dialed in to
has denied access because
the username and/or password is invalid on the domain.

A “criptografia de MPPE exigida” é selecionada no concentrador, mas o server do Cisco Secure ACS for Windows não é configurado para MS-RACHADURA-MPPE-chaves e MS-RACHADURA-MPPE-tipos

- **Resultado do debug do VPN 3000 concentrator**Se o AUTHDECODE (severidade 1-13) e o PPTP debugam (severidade 1-9) estão ligada, o log mostram que o server do Cisco Secure ACS for Windows não está enviando o atributo específico de fornecedor 26 (0x1A) na aceitação de acesso do server (log parcial).2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0
RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE .N.,..u.16Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF ..//.....
- 2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [CSNTUSER] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
- **O registro de saída do Cisco Secure ACS for Windows não mostra nenhuma falha.**
- **A mensagem que o usuário vê**Error 691: The computer you have dialed in to has denied
access because
the username and/or password is invalid on the domain.

[Informações Relacionadas](#)

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de suporte ao cliente do Cisco VPN 3000 Series](#)
- [Página de suporte do IPSec](#)
- [Cisco Secure ACS para página de suporte do Windows](#)
- [Página de suporte RADIUS](#)
- [Página de suporte do PPTP](#)
- [RFC 2637: Protocolo de túnel ponto-a-ponto \(PPTP\)](#)

- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)