Como configurar o PPTP do concentrador VPN 3000 com autenticação local

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Diagrama de Rede Conventions Configurar o VPN 3000 Concentrator com autenticação local Configuração do Microsoft PPTP Client Windows 98 - Instalar e configurar o recurso PPTP Windows 2000 - Configurando o recurso PPTP Windows NT Windows Vista Adicionar MPPE (criptografia) Verificar Verificar o VPN Concentrator Verificar o PC Debug Depuração do VPN 3000 - Boa autenticação Troubleshoot Possíveis problemas da Microsoft a serem solucionados Informações Relacionadas

Introduction

O Cisco VPN 3000 Concentrator suporta o método de tunelamento PPTP (Point-to-Point Tunnel Protocol) para clientes nativos do Windows. Há suporte para criptografia de 40 e 128 bits disponível nesses VPN Concentrators para uma conexão segura e confiável.

Consulte <u>Configurando o VPN 3000 Concentrator PPTP com autenticação RADIUS do Cisco</u> <u>Secure ACS para Windows</u> para configurar o VPN Concentrator para usuários PPTP com autenticação estendida usando o Cisco Secure Access Control Server (ACS).

Prerequisites

Requirements

Certifique-se de atender aos pré-requisitos mencionados em <u>When is PPTP Encryption Supported</u> on a Cisco VPN 3000 Concentrator? (Quando a criptografia PPTP é suportada em um Cisco VPN <u>3000 Concentrator?</u>) antes de tentar esta configuração.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- VPN 3015 Concentrator com versão 4.0.4.A
- PC Windows com cliente PPTP

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

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

Configurar o VPN 3000 Concentrator com autenticação local

Conclua estes passos para configurar o VPN 3000 Concentrator com autenticação local.

- 1. Configure os respectivos endereços IP no VPN Concentrator e verifique se você tem conectividade.
- Verifique se a autenticação PAP está selecionada na guia Configuration > User Management > Base Group PPTP/L2TP.

Configuration User Management Base Group					
General IPSec Client Config Client FW HW Client PPTP/L2TP					
	PPTP/L2TP Parameters				
Attribute Value Description					
Use Client Address		Check to accept and use an IP address received from the client.			
PPTP Authentication Protocols	 ☑ PAP ☑ CHAP ☑ MSCHAPv1 ☑ MSCHAPv2 ☑ EAP Proxy 	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking <i>all</i> options means that <i>no</i> authentication is required.			
PPTP Encryption	□ Required □ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for PPTP connections for this group.			
PPTP Compression		Check to enable MPPC compression for PPTP connections for this group.			

3. Selecione **Configuration > System > Tunneling Protocols > PPTP** e verifique se **Enabled** está marcado.

Configuration System Tunneling Protocols PPTP					
This section lets you configure system-wide	This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.				
Disabling PPTP will terminate any active PPTP sessions.					
Enabled 🔽					
Maximum Tunnel Idle Time	seconds				
Packet Window Size 16	packets				
Limit Transmit to Window	Check to limit the transmitted packets based on the peer's receive window.				
Max. Tunnels 0	Enter 0 for unlimited tunnels.				
Max. Sessions/Tunnel 0	Enter 0 for unlimited sessions.				
Packet Processing Delay 1	10 ^{ths} of seconds				
Acknowledgement Delay 500	milliseconds				
Acknowledgement 3	seconds				
Apply Cancel					

 Selecione Configuration > User Management > Groups > Add e configure um grupo PPTP. Neste exemplo, o nome do grupo é "pptpgroup" e a senha (e verifique a senha) é "cisco123".

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 Mode Config Client FW HW Client PPTP/LZTP					
Identity Parameters					
Attribute	Attribute Value Description				
Group Name	pptpgroup	Enter a unique name for the group.			
Password	Robiologiak	Enter the password for the group.			
Verify	Rokolokokok	Verify the group's password.			
Туре	Internal 💌	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.			
Add	Cancel				

5. Na guia Geral do grupo, certifique-se de que a opção **PPTP** esteja habilitada em protocolos de

autenticação.

Configuration | User Management | Base Group

General IPSec Client Config Client FW HW Client PPTP/L2TP

General Parameters					
Attribute	Value	Description			
Access Hours	-No Restrictions-	Select the access hours for this group.			
Simultaneous Logins	3	Enter the number of simultaneous logins for users in 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 time out for this group.			
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.			
Filter	-None-	Select the filter assigned to this group.			
Primary DNS		Enter the IP address of the primary DNS server for this group.			
Secondary DNS		Enter the IP address of the secondary DNS server.			
Primary WINS		Enter the IP address of the primary WINS server for this group.			
Secondary WINS		Enter the IP address of the secondary WINS server.			

SEP Card Assignment	V SEP 1 V SEP 2 V SEP 3 V SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	☞ PPTP ☞ L2TP ☞ IPSec □ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm		Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.
Apply Cancel		

 Na guia PPTP/L2TP, habilite a autenticação PAP e desabilite a criptografia (a criptografia pode ser habilitada a qualquer momento no futuro).

Configuration | User Management | Groups | Modify pptpgroup 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 **PPTP/L2TP** Parameters Inherit? Attribute Value Description Use Client Check to accept and use an IP address received 2 Address from the client. Check the authentication protocols allowed by this 🗹 PAP group. The choices available are determined by PPTP CHAP base group settings. Refer to the online help for 2 Authentication MSCHAPv1 authentication protocol dependencies. Protocols MSCHAPv2 Unchecking all options means that no EAP Proxy authentication is required. Required Select the allowed encryption methods for PPTP PPTP Encryption
Require Stateless connections for this group. 🗆 40-bit 🗖 128-bit PPTP Check to enable compression for PPTP 2 Compression connections for this group.

7. Selecione Configuration > User Management > Users > Add, e configure um usuário local (chamado de "pptpuser") com a senha cisco123 para autenticação PPTP. Coloque o usuário no "pptpgroup" previamente definido:

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		
User Name	pptpuser	Enter a unique user name.		
Password	skokokokokokokok	Enter the user's password. The password must satisfy the group password requirements.		
Verify	kekekekekekekek	Verify the user's password.		
Group	pptpgroup 💌	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. Na guia Geral do usuário, verifique se a opção **PPTP** está habilitada nos protocolos de tunelamento.

Configuration | User Management | Users | Modify pptpuser

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPSec PPTP/L2TP

General Parameters				
Attribute	Value	Inherit?	Description	
Access Hours	-No Restrictions-	2	Select the access hours assigned to this user.	
Simultaneous Logins	3	ব	Enter the number of simultaneous logins for this user.	
Idle Timeout	30	V	(minutes) Enter the idle timeout for this user.	
Maximum Connect Time	0	V	(minutes) Enter the maximum connect time for this user.	
Filter	-None-	2	Enter the filter assigned to this user.	
Tunneling Protocols	 ✓ PPTP ✓ L2TP ✓ IPSec □ L2TP over IPSec 	ব	Select the tunneling protocols this user can connect with.	
Apply Can	cel			

9. Selecione Configuration > System > Address Management > Pools para definir um pool de

endereços para o gerenciamento de endereços.

Configuration | System | Address Management | Pools

This section lets you configure IP Address Pools.

Click the Add button to add a pool entry, or select a pool and click Modify, Delete or Move.

IP Pool Entry	Actions
172.16.1.10 - 172.16.1.20	Add
	Modify
	Delete
	Move Up
	Move Dowr

 Selectione Configuration > System > Address Management > Assignment e directione o VPN Concentrator para usar o pool de enderecos.

Configuration System Address Management Assignment				
This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.				
Use Client Address 🗖	Check to use the IP address supplied by the client. This can be overridden by user/group configuration.			
Use Address from Authentication Server	Check to use an IP address retrieved from an authentication server for the client.			
Use DHCP 🗆	Check to use DHCP to obtain an IP address for the client.			
Use Address Pools 🗹	Check to use internal address pool configuration to obtain an IP address for the client.			
Apply Cancel				

Configuração do Microsoft PPTP Client

Observação: nenhuma das informações disponíveis aqui sobre a configuração do software Microsoft vem com garantia ou suporte para o software Microsoft. O suporte ao software Microsoft está disponível na <u>Microsoft</u>.

Windows 98 - Instalar e configurar o recurso PPTP

Instalação

Conclua estes passos para instalar o recurso PPTP.

- 1. Selecione Iniciar > Configurações > Painel de controle > Adicionar novo hardware (Avançar) > Selecionar na lista > Adaptador de rede (Avançar).
- 2. Selecione Microsoft no painel esquerdo e Microsoft VPN Adapter no painel direito.

Configurar

Conclua estes passos para configurar o recurso PPTP.

- 1. Selecione Iniciar > Programas > Acessórios > Comunicações > Rede dial-up > Fazer nova conexão.
- 2. Conecte-se usando o Adaptador VPN Microsoft no prompt Select a device (Selecionar um dispositivo). O IP do Servidor VPN é o ponto de extremidade do túnel 3000.

A autenticação padrão do Windows 98 usa criptografia de senha (por exemplo, CHAP ou MSCHAP). Para desativar inicialmente essa criptografia, selecione **Propriedades > Tipos de servidor** e desmarque as caixas **Senha criptografada** e **Exigir criptografia de dados**.

Windows 2000 - Configurando o recurso PPTP

Conclua estes passos para configurar o recurso PPTP.

- 1. Selecione Iniciar > Programas > Acessórios > Comunicações > Conexões de Rede e Discagem > Fazer nova conexão.
- 2. Clique em Avançar e selecione Conectar-se a uma rede privada através da Internet > Discar uma conexão antes (não selecione esta opção se usar uma LAN).
- 3. Clique em **Next** novamente e insira o nome de host ou IP do ponto final do túnel, que é a interface externa do VPN 3000 Concentrator. Neste exemplo, o endereço IP é 161.44.17.1.

Selecione **Propriedades > Segurança para a conexão > Avançado** para adicionar um tipo de senha como PAP. O padrão é MSCHAP e MSCHAPv2, não CHAP ou PAP.

A encriptação de dados é configurável nesta área. Você pode desativá-lo inicialmente.

Windows NT

Você pode acessar informações sobre como configurar clientes Windows NT para PPTP no <u>site</u> <u>da Microsoft</u>.

Windows Vista

Conclua estes passos para configurar o recurso PPTP.

- 1. No botão Iniciar, escolha Conectar a.
- 2. Escolha Configurar uma conexão ou uma rede.
- 3. Escolha Conectar-se a um local de trabalho e clique em Avançar.
- 4. Escolha Usar minha conexão com a Internet (VPN). Observação: se for solicitado "Deseja usar uma conexão que já tenha", escolha Não, crie uma nova conexão e clique em Avançar.
- 5. No campo Endereço de Internet, digite pptp.vpn.univ.edu, por exemplo.

- 6. No campo Nome de destino, digite UNIVVPN, por exemplo.
- 7. No campo **Nome de usuário**, digite sua ID de logon UNIV. Sua ID de login UNIV é a parte do seu endereço de e-mail antes de **@univ.edu**.
- 8. No campo Senha, digite sua senha de ID de logon UNIV.
- 9. Clique no botão Create (Criar) e clique no botão Close (Fechar).
- 10. Para se conectar ao servidor VPN depois de criar a conexão VPN, clique em Iniciar e em **Conectar a**.
- 11. Escolha a conexão VPN na janela e clique em Connect.

Adicionar MPPE (criptografia)

Certifique-se de que a conexão PPTP funcione sem criptografia antes de adicionar criptografia. Por exemplo, clique no botão **Connect** no cliente PPTP para verificar se a conexão foi concluída. Se você decidir exigir criptografia, a autenticação MSCHAP deve ser usada. No VPN 3000, selecione **Configuration > User Management > Groups**. Em seguida, na guia PPTP/L2TP do grupo, desmarque **PAP**, marque **MSCHAPv1** e marque **Obrigatório para criptografia PPTP**.

Configuration | User Management | Groups | Modify pptpgroup 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 Con	ng Clien	TEW HWULIENT PPTP/LZTP	
PPTP/L2TP Parameters				
Attribute	Value	Inherit?	Description	
Use Client Address		N	Check to accept and use an IP address received from the client.	
PPTP Authentication Protocols	□ PAP □ CHAP ☑ MSCHAPv1 □ MSCHAPv2 □ EAP Proxy		Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking all options means that <i>no</i> authentication is required.	
PPTP Encryption	 ☑ Required □ Require Stateless ☑ 40-bit ☑ 128-bit 		Select the allowed encryption methods for PPTP connections for this group.	
PPTP Compression		N	Check to enable compression for PPTP connections for this group.	

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

O cliente PPTP deve ser reconfigurado para criptografia de dados opcional ou obrigatória e MSCHAPv1 (se for uma opção).

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

Verificar o VPN Concentrator

Você pode iniciar a sessão PPTP discando do cliente PPTP criado anteriormente na seção <u>Configuração do cliente PPTP da Microsoft</u>.

Use a janela Administration >Administer Sessions no VPN Concentrator para exibir os parâmetros e as estatísticas de todas as sessões de PPTP ativas.

Verificar o PC

Emita o comando **ipconfig** no modo de comando do PC para ver se o PC tem dois endereços IP. Um é seu próprio endereço IP e o outro é atribuído pelo VPN Concentrator do pool de endereços IP. Neste exemplo, o endereço IP 172.16.1.10 é o endereço IP atribuído pelo VPN Concentrator.



Debug

Se a conexão não funcionar, a depuração de classe de evento PPTP pode ser adicionada ao VPN Concentrator. Selecione **Configuração > Sistema > Eventos > Classes > Modificar** ou **Adicionar** (mostrado aqui). As classes de eventos PPTPDBG e PPTPDECODE também estão disponíveis, mas podem fornecer muitas informações.

Configuration System Events Classes Add				
This screen lets you add and configure an event class for special handling.				
Class Name PPTP	Select the event class to configure.			
Enable 🖂	Check to enable special handling of this class.			
Severity to Log 1-13	Select the range of severity values to enter in the log.			
Console	Select the range of severity values to display on the console.			
Syslog	Select the range of severity values to send to a Syslog server.			
Severity to Email None 💌	Select the range of severity values to send via email to the recipient list.			
Severity to Trap None 💌	Select the range of severity values to send to an SNMP system.			
Add Cancel				

O registro de eventos pode ser recuperado de **Monitoring > Filterable Event Log**.

Monitoring Filteral	ble Event Log			
<u> </u>	, i i i i i i i i i i i i i i i i i i i			
Select Filter Option	ns			
Event Class	All Classes AUTH AUTHDBG AUTHDECODE	Severities	ALL 1 2 3 V	
Client IP Address	0.0.0.0	Events/Page	100 💌	
Group	-All-	Direction	Oldest to Newest 💌	
H4 +4 >	Get Log	Save Log	Clear Log	
1 09/30/2004 09:	:34:05.550 SEV=4 P	PTP/47 RPT=	10 171.69.89.129	
Tunnel to peer :	171.69.89.129 esta	blished		
2 09/30/2004 09:34:05.550 SEV=4 PPTP/42 RPT=10 171.69.89.129 Session started on tunnel 171.69.89.129				
3 09/30/2004 09:34:08.750 SEV=5 PPP/8 RPT=8 171.69.89.129				
User [pptpuser]				
Authenticated successfully with PAP				
4 09/30/2004 09:34:12.590 SEV-4 AUTH/22 RPT-6				
User [pptpuser]	Group [pptpgroup]	connected,	Session Type: PPTP	

Depuração do VPN 3000 - Boa autenticação

Tunnel to peer 171.69.89.129 established

- 2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129 Session started on tunnel 171.69.89.129
- 3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129 User [pptpuser] Authenticated successfully with MSCHAP-V1
- 4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22

User [pptpuser] Group [Base Group] connected, Session Type: PPTP

Clique na janela **Detalhes** do status do usuário PPTP para verificar os parâmetros no PC Windows.

pptpuser Status			<u>?</u> ×
General Details			
General Details Property Authentication Encryption Compression PPP multilink framing Server IP address Client IP address	Value MS CHAP MPPE 128 (none) Off 161.44.17.1 172.16.1.10		
		Clo	se

Troubleshoot

Estes são possíveis erros que você pode encontrar:

- Nome de usuário ou senha incorretaSaída de depuração do VPN 3000 Concentrator:
 - 1 09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129 Tunnel to peer 171.69.89.129 established
 - 2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129 Session started on tunnel 171.69.89.129
 - 3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129 Authentication rejected: Reason = User was not found handle = 44, server = (none), user = pptpusers, domain = <not specified>
 - 5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129 User [pptpusers]

disconnected.. failed authentication ($\ensuremath{\mathsf{MSCHAP-V1}}$)

- 6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129 Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761), reason: Error (No additional info)
- 8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129 Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)

A mensagem que o usuário vê (do 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 mensagem que o usuário vê (do Windows 2000):

Error 691: Access was denied because the username and/or password was invalid on the domain.

 A opção "Criptografia necessária" está selecionada no PC, mas não no VPN ConcentratorA mensagem que o usuário vê (do Windows 98):

Error 742: The computer you're dialing in to does not support the data encryption requirements specified. Please check your encryption settings in the properties of the connection. If the problem persists, contact your network administrator.

A mensagem que o usuário vê (do Windows 2000): Error 742: The remote computer does not support

the required data encryption type

 "Encryption Required" (Criptografia necessária) (128 bits) é selecionado no VPN Concentrator com um PC que oferece suporte apenas à criptografia de 40 bitsSaída de depuração do VPN 3000 Concentrator:

4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [pptpuser] disconnected. PPTP Encryption configured as REQUIRED.. remote client not supporting it.

A mensagem que o usuário vê (do Windows 98): Error 742: The remote computer does not support the required data encryption type.

A mensagem que o usuário vê (do Windows 2000):

Error 645 Dial-Up Networking could not complete the connection to the server. Check your configuration and try the connection again.

 O VPN 3000 Concentrator está configurado para MSCHAPv1 e o PC está configurado para PAP, mas não podem concordar com um método de autenticaçãoSaída de depuração do VPN 3000 Concentrator:

8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129

User [pptpuser] disconnected. Authentication protocol not allowed. A mensagem que o usuário vê (do Windows 2000): Error 691: Access was denied because the username and/or password was invalid on the domain.

Possíveis problemas da Microsoft a serem solucionados

- Como Manter conexões de RAS Ativas Após o Fim da SessãoQuando você faz logoff de um cliente do Serviço de Acesso Remoto (RAS - Remote Access Service) do Windows, todas as conexões RAS são automaticamente desconectadas. Ative a chave KeepRasConnections no registro do cliente RAS para permanecer conectado após o logoff. Consulte o <u>artigo da Base</u> <u>de conhecimento Microsoft - 158909</u> para obter mais informações.
- O Usuário Não é Alertado ao Conectar com Credenciais no CacheOs sintomas desse problema são quando você tenta fazer logon em um domínio a partir de uma estação de trabalho baseada no Windows ou de um servidor membro e um controlador de domínio não pode ser localizado e nenhuma mensagem de erro é exibida. Em vez disso, você será

conectado ao computador local usando as credenciais em cache. Consulte o <u>artigo da Base</u> <u>de conhecimento Microsoft - 242536</u> para obter mais informações.

 Como Escrever um Arquivo LMHOSTS para a Validação de Domínio e Outros Problemas de Resolução de NomesPode haver casos em que você enfrenta problemas de resolução de nomes em sua rede TCP/IP e precisa usar arquivos LMHOSTS para resolver nomes NetBIOS. Este artigo discute o método apropriado usado para criar um arquivo LMHOSTS para ajudar na resolução de nome e validação de domínio. Consulte o <u>artigo da Base de</u> <u>conhecimento Microsoft - 180094</u> para obter mais informações.

Informações Relacionadas

- <u>RFC 2637: Point-to-Point Tunneling Protocol (PPTP)</u>
- Páginas de suporte do Cisco Secure ACS para Windows
- Quando a criptografia PPTP é suportada em um Cisco VPN 3000 Concentrator?
- <u>Configurando o VPN 3000 Concentrator e o PPTP com a autenticação RADIUS do Cisco</u> <u>Secure ACS para Windows</u>
- Página de suporte do Cisco VPN 3000 Concentrator
- Páginas de suporte ao Cisco VPN 3000 Client
- Páginas de Suporte do Produto IPSec (Protocolo de Segurança IP)
- Páginas de suporte do produto PPTP
- <u>Suporte Técnico e Documentação Cisco Systems</u>