使用Microsoft RADIUS配置Cisco VPN 3000集中器

目錄

簡介
必要條件
需求
採用元件
慣例
在Windows 2000和Windows 2003上安裝並配置RADIUS伺服器
安裝RADIUS伺服器
使用IAS配置Microsoft Windows 2000 Server
使用IAS配置Microsoft Windows 2003 Server
配置用於RADIUS身份驗證的Cisco VPN 3000集中器
驗證
疑難排解
WebVPN身份驗證失敗
針對Active Directory的使用者身份驗證失敗
相關資訊

<u>簡介</u>

Microsoft Internet Authentication Server(IAS)和Microsoft Commercial Internet System(MCIS 2.0)目前可用。Microsoft RADIUS伺服器很方便,因為它使用主域控制器上的Active Directory作為 其使用者資料庫。不再需要維護單獨的資料庫。它還支援點對點隧道協定(PPTP)VPN連線的40位和 128位加密。請參閱<u>Microsoft清單:配置撥號的IAS和VPN訪問文檔</u>,瞭解更多資訊。

必要條件

<u>需求</u>

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

<u>慣例</u>

<mark>請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u></mark>

在Windows 2000和Windows 2003上安裝並配置RADIUS伺服器

安裝RADIUS伺服器

如果尚未安裝RADIUS伺服器(IAS),請執行以下步驟,以進行安裝。如果您已安裝RADIUS伺服器 ,請繼續執行<u>組態步驟</u>。

- 1. 插入Windows Server光碟並啟動安裝程式。
- 2. 按一下Install Add-On Components,然後按一下Add/Remove Windows Components。
- 3. 在元件中,按一下Networking Services(但不選中或清除覈取方塊),然後按一下Details。
- 4. 選中Internet Authentication Service, 然後按一下OK。
- 5. 按「Next」(下一步)。

使用IAS配置Microsoft Windows 2000 Server

完成以下步驟即可設定RADIUS伺服器(IAS)和啟動服務,以便在VPN集中器上驗證使用者身分。

- 1. 選擇開始>程式>管理工具> Internet身份驗證服務。
- 2. 按一下右鍵Internet Authentication Service,然後從出現的子選單中按一下Properties。
- 3. 前往RADIUS索引標籤檢查連線埠的設定。如果您的RADIUS驗證和RADIUS記帳使用者資料 包協定(UDP)埠與驗證和記帳中提供的預設值(1812和1645,1813和1646)不同,請鍵入您的 埠設定。完成後按一下OK。注意:請勿更改預設埠。使用逗號將多個埠設定用於身份驗證或 記帳請求,從而分隔埠。
- 4. 按一下右鍵Clients並選擇New Client,以將VPN集中器作為身份驗證、授權和記帳(AAA)客戶 端新增到RADIUS伺服器(IAS)。注意:如果在兩個Cisco VPN 3000集中器之間配置了冗餘 ,則還必須將備份的Cisco VPN 3000集中器作為RADIUS客戶端新增到RADIUS伺服器。
- 5. 輸入友好名稱並選擇為Protocol Radius。
- 6. 在下一個視窗中使用IP地址或DNS名稱定義VPN集中器。
- 7. 從客戶端 供應商捲軸中選擇Cisco。
- 8. 輸入共用金鑰。注意:您必須記住您使用的確切密碼。您需要此資訊才能配置VPN集中器。
- 9. 按一下「Finish」(結束)。
- 10. 按兩下Remote Access Policies,然後按兩下顯示在視窗右側的策略。注意:安裝IAS後,遠端訪問策略應該已經存在。在Windows 2000中,根據使用者帳戶的撥入屬性和遠端訪問策略 授予授權。遠端訪問策略是一組條件和連線設定,使網路管理員在授權連線嘗試時更具靈活 性。Windows 2000路由和遠端訪問服務和Windows 2000 IAS都使用遠端訪問策略來確定是 接受還是拒絕連線嘗試。在這兩種情況下,遠端訪問策略都儲存在本地。有關如何處理連線 嘗試的詳細資訊,請參閱Windows 2000 IAS文檔。

Allow access if dial-in permission is enabled Properties				
Settings				
Policy name: Allow access if dial-in permission is enabled				
Specify the conditions to match:				
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00; ¹				
Add Remove Edit				
If a user matches the conditions				
Grant remote access permission				
C Deny remote access permission				
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.				
Edit Profile				
OK Cancel Apply				

- 11. 選擇**授予遠端訪問許可權**,然後按一下**編輯配置檔案**以配置撥入屬性。
- 12. 在Authentication頁籤上選擇要用於身份驗證的協定。選中Microsoft Encrypted Authentication version 2並取消選中所有其他身份驗證協定。注意:此撥入配置檔案中的設定 必須與VPN 3000集中器配置和撥入客戶端中的設定匹配。在此示例中,使用不採用PPTP加 密的MS-CHAPv2身份驗證。
- 13. 在Encryption頁籤上選中No Encryption。
- 14. 按一下「OK」以關閉「撥入」設定檔,然後按一下「OK」以關閉遠端存取原則視窗。
- 15. 按一下右鍵Internet身份驗證服務,然後按一下控制檯樹中的啟動服務。注意:您也可以使用 此功能停止服務。
- 16. 完成這些步驟,修改使用者以允許連線。選擇Console > Add/Remove Snap-in。按一下 Add並選擇Local Users and Groups管理單元。按一下「Add」。確保選擇Local Computer按 一下「Finish」,然後「OK」。
- 17. 展開Local User and Groups,然後按一下左窗格中的Users資料夾。在右窗格中,按兩下要 允許訪問的使用者(VPN使用者)。
- 18. 轉到「撥入」頁籤,然後在「遠端訪問許可權(撥入或VPN)」下選擇Allow Access。

test Properties	<u>?</u> ×
General Member Of Profile Dial-in	
Remote Access Permission (Dial-in or VPN)	
Allow access	
C Deny access	
Control access through Remote Access Policy	
Verify Caller-ID:	
Callback Options	
No Callback	
C Set by Caller (Routing and Remote Access Service only)	
C Always Callback to:	
Assign a Static IP Address	
Apply Static Routes	
Define routes to enable for this Dial-in	
OK Cancel	Apply

19. 按一下「Apply」和「OK」以完成操作。如果需要,可以關閉Console Management視窗並 儲存會話。您修改的使用者現在可以通過VPN客戶端訪問VPN集中器。請記住,IAS伺服器 僅對使用者資訊進行身份驗證。VPN集中器仍然執行組身份驗證。

使用IAS配置Microsoft Windows 2003 Server

完成以下步驟,以便使用IAS配置Microsoft Windows 2003伺服器。

注意:這些步驟假設IAS已安裝在本地電腦上。如果不是,請通過**控制面板>新增/刪除程式**新增此項 。

- 選擇Administrative Tools > Internet Authentication Service,然後按一下右鍵RADIUS Client以新增新的RADIUS客戶端。鍵入客戶端資訊後,按一下OK。
- 2. 輸入友好名稱。
- 3. 在下一個視窗中使用IP地址或DNS名稱定義VPN集中器。
- 4. 從客戶端 供應商捲軸中選擇Cisco。
- 5. 輸入共用金鑰。注意:您必須記住您使用的確切密碼。您需要此資訊才能配置VPN集中器。
- 6. 按一下「**OK**」以完成。
- 7. 轉到**遠端訪問策略**,按一下右鍵**連線到其他訪問伺服器**,然後選擇**屬性**。
- 8. 選擇**授予遠端訪問許可權**,然後按一下**編輯配置檔案**以配置撥入屬性。

- 9. 在Authentication頁籤上選擇要用於身份驗證的協定。選中Microsoft Encrypted Authentication version 2並取消選中所有其他身份驗證協定。注意:此撥入配置檔案中的設定必須與VPN 3000集中器配置和撥入客戶端中的設定匹配。在此示例中,使用不採用PPTP加密的MS-CHAPv2身份驗證。
- 10. 在Encryption頁籤上選中No Encryption。



- 12. 按一下右鍵Internet身份驗證服務,然後按一下控制檯樹中的啟動服務。注意:您也可以使用 此功能來停止服務。
- 13. 選擇Administrative Tools > Computer Management > System Tools > Local Users and Groups,按一下右鍵Users,然後選擇New Users,以便將使用者新增到本地電腦帳戶中。
- 14. 使用思科密碼「vpnpassword」新增使用者並檢查此配置檔案資訊。在「General(常規)」 頁籤上,確保選中Password Never Expired選項,而不是「User Must Change Password(使用者必須更改密碼)」選項。在「撥入」頁籤上,為**允許訪問**(或保留「通過 遠端訪問策略控制訪問」的預設設定)選擇選項。完成後按一下OK。

desktop [hanky] - Microsoft In	ternet Explorer provided by Cisco Systems, Inc.	_10
Edit Yew Fgvorites Loois (yap	1
× - → - ◎ ② ③ ③ ◎ ∞	ech @Favortes @Meda 🔇 🔂 🕁 🖾 🔄	
http://10.66.79.229:5800		🛫 🗟 Go Link
area opon opcost oex		
Computer	Sca Properties 21× General Member Of Positie Environment Sections Remote Access Permission (Dialer or VPN) Dialer Image: Control Dialer Image: Control Dialer Catheor Access Permission (Dialer or VPN) Along access Image: Control Dialer Image: Control Dialer Catheor Access Permission (Dialer or VPN) Image: Control Dialer Image: Control Dialer Image: Control Dialer Catheor Dialer Dialer (Dialer Access Policy) Image: Control Dialer Image: Control Dialer Image: Control Dialer Marge Catheor Dialer Catheor Dialer (Pouting and Benote Access Service orbit) Image: Control Dialer Image: Control Dialer Arrige a Static IP Address Image: Control Dialer Image: Control Dialer Image: Control Dialer OK Cancel Dialer Image: Control Dialer Image: Control Dialer	
0		g Internet
		AND R COMM HAND

配置用於RADIUS身份驗證的Cisco VPN 3000集中器

完成以下步驟,配置用於RADIUS身份驗證的Cisco VPN 3000集中器。

使用Web瀏覽器連線到VPN集中器,然後從左側框架選單中選擇Configuration > System > Servers > Authentication。

Configuration System Servers Authentication	
	Save Needed
This section lets you configure parameters for servers that au You should have a properly configured RADIUS, NT Doma can configure the internal server and <u>add users to the internal</u>	thenticate users. in, SDI or Kerberos/Active Directory server to access, or you <u>database</u> .
Click the Add button to add a server, or select a server and	click Modify, Delete, Move, or Test.
Authentication Servers	Actions Add Modify Delete Move Up Move Down Test

2. 按一下Add並配置這些設定。伺服器型別= RADIUS身份驗證伺服器= RADIUS伺服器(IAS)的 IP地址或主機名伺服器埠= 0(0=預設=1645)伺服器密碼=與配置RADIUS伺服器一節中的步 驟8相同

Configuration System Servers Authentication	Add
Configure and add a user authentication server.	
Server Type RADIUS	Selecting <i>Internal Server</i> will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.
Authentication Server	Enter IP address or hostname.
Used For User Authentication 💌	Select the operation(s) for which this RADIUS server will be used.
Server Port 0	Enter 0 for default port (1645).
Timeout 4	Enter the timeout for this server (seconds).
Retries 2	Enter the number of retries for this server.
Server Secret	Enter the RADIUS server secret.
Verify ••••••	Re-enter the secret.
Add Cancel	

- 3. 按一下「Add」將變更新增到執行組態中。
- 4. 按一下Add,選擇Internal Server作為Server Type,然後按一下Apply。稍後需要此命令以配置IPsec組(您只需要伺服器型別=內部伺服器)。

Configuration System Servers Authentication Add
Configure and add a user authentication server.
Server Type Internal Server Selecting Internal Server will let you add users to the internal user database.
Apply Cancel

5. 為PPTP使用者或VPN客戶端使用者配置VPN集中器。PPTP完成這些步驟,以便為PPTP使用 者配置。選擇Configuration > User Management > Base Group,然後按一下PPTP/L2TP頁籤 。選擇MSCHAPv2,然後在PPTP Authentication Protocols部分取消選中其他身份驗證協定。

Configuration User Management Base Group					
General IPSec Client Config Client FM HW Client PPTP/L2TP WebVPN NAC					
	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 Prozy	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.			
L2TP 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.			
L2TP Encryption	□ Required □ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for L2TP connections for this group.			
L2TP Compression		Check to enable MPPC compression for L2TP connections for this group.			
Apply Cancel					

按一下頁面底部的**Apply**,將更改新增到運行配置中。現在,PPTP使用者連線時,會透過 RADIUS伺服器(IAS)進行驗證。VPN使用者端完成以下步驟,以便為VPN客戶端使用者進行配 <u>置。選擇Configuration > User Management > Groups</u>,然後按一下Add以新增新組。

Configuration User Management Groups				
			Save Needed 🔒	
This section lets you configure groups. A group is a collection of users treated as a single entity. Click the Add Group button to add a group, or select a group and click Delete Group or Modify Group . To modify other group parameters, select a group and click the appropriate button.				
Actions	Current Groups	Modify		
	—Empty—	Authentication Servers		
Add Group		Authorization Servers		
		Accounting Servers		
Modify Group		Address Pools		
Delate Querre		Client Update		
Delete Group		Bandwidth Assignment		
		WebVPN Servers and URLs		
		WebVPN Port Forwarding		
	-			

鍵入組名(例如IPsecUsers)和密碼。

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 WebVPN NAC

Identity Parameters			
Attribute	Attribute Value Description		
Group Name	IPSecUsers	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 Databas			
Add	Cancel		

此密碼用作通道交涉的預共用金鑰。轉到IPSec頁籤並將Authentication設定為RADIUS。

Configuration Administration Monitoria			itoring	
			below as needed.	-
Remote Access Parameters		'S		
Group Lock		V	Lock users into this group.	
Authentication	RADIUS		Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .	
Authorization Type	None 💌	ব	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		V	Check to require successful authorization.	
DN Field	CN otherwise OU	শ	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 💌	2	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.	
			Dennit or dent MDN Clients according to	-

這允許透過RADIUS驗證伺服器驗證IPsec使用者端。按一下頁面底部的Add,將更改新增到運 行配置中。現在,當IPsec客戶端連線並使用您配置的組時,它們將由RADIUS伺服器進行身 份驗證。



目前沒有適用於此組態的驗證程序。

<u>疑難排解</u>

WebVPN身份驗證失敗

以下各節提供了可用於對配置進行故障排除的資訊。

•問題:WebVPN使用者無法對RADIUS伺服器進行身份驗證,但可以通過VPN集中器的本地資料 庫成功進行身份驗證。它們會收到錯誤,例如「登入失敗」和此消息。

Cisco Systems	SECURE DESKTOP for WEBVPN		
This comp	iter does not match any location.		
	OK		
	······································		

原因:當使用除集中器內部資料庫

之外的任何資料庫時,通常會發生此類問題。WebVPN使用者首次連線到集中器時必須使用預 設身份驗證方法時點選基本組。此方法通常設定為集中器的內部資料庫,而不是已配置的 RADIUS或其他伺服器。**解決方案**:WebVPN使用者進行身份驗證時,集中器會檢查在 **Configuration > System > Servers > Authentication**中定義的伺服器清單,並使用頂部的清單。 確保將您希望WebVPN使用者進行身份驗證的伺服器移至此清單頂部。例如,如果RADIUS應 是驗證方法,則需要將RADIUS伺服器移動到清單頂端,以將驗證推送到它。**注意:**僅因為 WebVPN使用者最初點選了基本組,並不意味著他們只限於基本組。可以在集中器上配置其他 WebVPN組,並且使用者可以由填充屬性25(**OU=groupname)的RADIUS伺服器分配給**。如需 詳細說明,請參閱使用RADIUS伺服器將使用者鎖定到VPN 3000集中器群組。

<u>針對Active Directory的使用者身份驗證失敗</u>

在Active Directory伺服器中,在失敗使用者的使用者屬性的「帳戶」頁籤上,可以看到以下覈取方 塊:

[x]不需要預先驗證

如果取消選中此覈取方塊,請選中,並嘗試再次與此使用者進行身份驗證。

<u>相關資訊</u>

- <u>Cisco VPN 3000系列集中器</u>
- Cisco VPN 3002硬體使用者端
- IPSec 協商/IKE 通訊協定
- RADIUS (遠端驗證撥入使用者服務) 支援頁面
- 遠端驗證撥入使用者服務(RADIUS)
- 技術支援與文件 Cisco Systems