使用RADIUS伺服器將使用者鎖定到VPN 3000集中器組

目錄

簡介

Cisco VPN 3000集中器能夠將使用者鎖定到集中器組，該集中器組會覆蓋使用者在Cisco VPN 3000客戶端中配置的組。這樣，訪問限制可以應用於VPN集中器上配置的各種組，並確保使用者通過RADIUS伺服器鎖定到該組中。

本檔案將詳細介紹如何在Cisco Secure ACS for Windows和Cisco Secure for UNIX(CSUnix)上設定此功能。

VPN集中器上的配置類似於標準配置。通過在RADIUS使用者配置檔案中定義return屬性啟用將使用者鎖定到VPN集中器上定義的組的功能。此屬性包含管理員希望使用者鎖定到的VPN集中器組名稱。此屬性是Class屬性（IETF RADIUS屬性編號25），並且必須按以下格式返回到VPN集中器：

```
OU=groupname;
```

其中*groupname*是使用者鎖定的VPN集中器上組的名稱。*OU*必須以大寫字母表示，並且結尾必須有分號。

在本示例中，VPN客戶端軟體分發給具有現有連線配置檔案的所有使用者，使用*組名*為「Everyone」，密碼為「Anything」。 每個使用者都有一個單獨的使用者名稱/密碼（在本例中，使用者名稱/密碼為TEST/TEST）。 將使用者名稱傳送到RADIUS伺服器時，RADIUS伺服器會向下傳送使用者要加入的實際*群組*的相關資訊。在本例中，它是「filtergroup」。

如此一來，便可以完全控制對使用者透明的RADIUS伺服器上的群組指派。如果RADIUS伺服器沒有將群組指派給使用者，則使用者會保留在「Everyone」群組中。由於「Everyone」組具有非常嚴格的過濾器，因此使用者無法傳遞任何流量。如果RADIUS伺服器確實為使用者分配了組，則使用者

將繼承屬性，包括限制較少的篩選器，尤其是組屬性。在本示例中，您將過濾器應用於VPN集中器上的組「filtergroup」以允許所有流量。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

注意：這在ACS 3.3、VPN Concentrator 4.1.7和VPN Client 4.0.5上也已成功測試。

- Cisco VPN 3000 Concentrator系列版本4.0(1)Rel
- Cisco VPN使用者端版本4.0(1)Rel
- 適用於Windows的Cisco Secure ACS版本2.4至3.2
- Cisco Secure for UNIX 2.3、2.5和2.6版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

配置Cisco VPN 3000 Concentrator

注意：此配置假設VPN集中器已使用IP地址、預設網關、地址池等進行設定。使用者必須能夠在本地進行身份驗證，然後才能繼續。如果這不起作用，那麼這些更改將不會起作用。

1. 在**Configuration > System > Servers > Authentication**下，新增RADIUS伺服器的IP地址。
2. 新增伺服器後，使用**Test**按鈕驗證是否可以成功驗證使用者。如果此操作不起作用，則組鎖定不起作用。
3. 定義一個丟棄對內部網路中所有裝置的訪問的過濾器。這適用於組「Everyone」，因此即使使用者能夠驗證進入該組並保留在該組中，他們仍然無法訪問任何內容。
4. 在Configuration > **Policy Management > Traffic Management** > Rules下，新增名為Drop All的規則，並將所有內容保留為預設值。
5. 在Configuration > **Policy Management > Traffic Management > Filters**下，建立名為Drop All的過濾器，將所有內容保留為預設值，然後將Drop All規則新增到該過濾器。
6. 在**Configuration > User Management > Groups**下新增一個名為**Everyone**的組。這是所有使用者在VPN客戶端中預配置的組。它們最初通過身份驗證進入此組，然後在使用者身份驗證後被鎖定到其他組。正常定義組。確保在General頁籤下新增Drop All過濾器（剛剛建立）。若要對此組中的使用者使用RADIUS身份驗證，請將組的Type（在Identity頁籤下）設定為**Internal**，將Authentication（在IPSec頁籤下）設定為**RADIUS**。確保未檢查此組的組鎖定功能。**註：即**使您沒有定義「全部丟棄」篩選器，請確保此處至少定義了一個篩選器。
7. 應用過濾器，定義使用者的最終目標組（例如「filtergroup」）。**注意：**必須在此處定義篩選

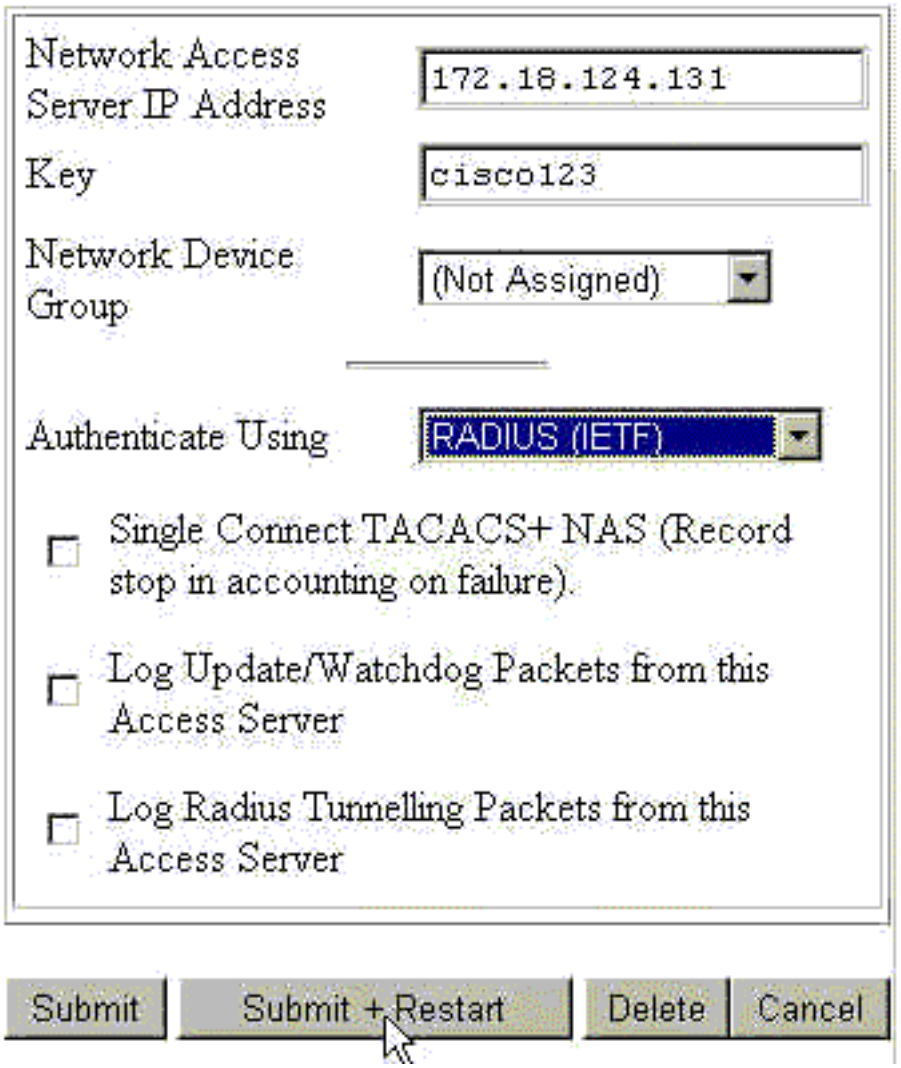
器。如果您不想阻止這些使用者的任何流量，請建立「Allow All」過濾器並應用「Any In」和「Any Out」規則。您必須定義某種型別的過濾器才能傳遞流量。若要對此組中的使用者使用RADIUS身份驗證，請將組的Type（在Identity頁籤下）設定為**Internal**，將Authentication（在IPSec頁籤下）設定為**RADIUS**。確保未檢查此組的組鎖定功能。

設定RADIUS伺服器

Cisco Secure ACS for Windows

這些步驟將您的Cisco Secure ACS for Windows RADIUS伺服器設定為將使用者鎖定到VPN集中器上配置的特定組中。請記住，在RADIUS伺服器上定義的組與VPN集中器上定義的組無關。您可以在RADIUS伺服器上使用群組，使使用者的管理更容易。這些名稱不必與VPN集中器上的配置匹配。

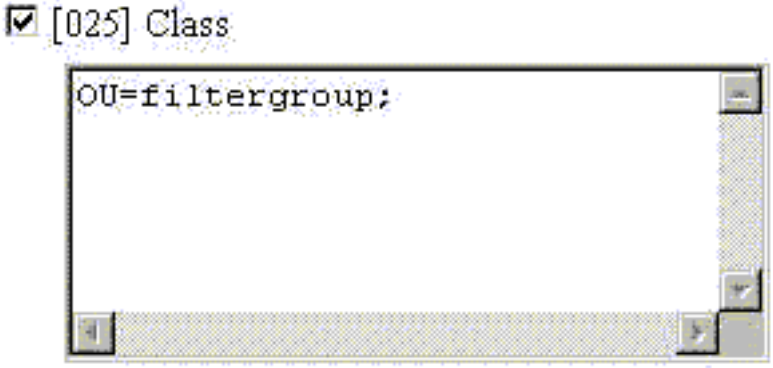
1. 在Network Configuration部分下將VPN Concentrator新增為RADIUS伺服器上的網路訪問伺服器(NAS)。在「NAS IP地址」框中新增VPN集中器的IP地址。在Key（金鑰）框中新增您之前在VPN集中器上定義的相同金鑰。從Authenticate Using下拉選單中，選擇**RADIUS(IETF)**。按一下「**Submit + Restart**」。



2. 在Interface Configuration下，選擇**RADIUS(IETF)**，並確保選中**屬性25(Class)**。這允許您在組/使用者配置中對其進行更改。
3. 新增使用者。在本示例中，使用者稱為「TEST」。 此使用者可位於任何Cisco Secure ACS for Windows組中。除了傳遞屬性25以告知VPN集中器使用者使用哪個組之外，適用於

Windows組的Cisco Secure ACS與VPN集中器組之間沒有關聯。此使用者被置於「Group_1」中。

4. 在「組設定」下，編輯組的設定（在我們的示例中，這是「Group_1」）。
5. 按一下綠色**IETF RADIUS**按鈕可轉至相應的屬性。
6. 向下滾動並修改屬性25。
7. 新增屬性，如下所示。替換要將使用者鎖定到的組名以替換filtergroup。確保OU以大寫字母表示，並且組名後有分號。

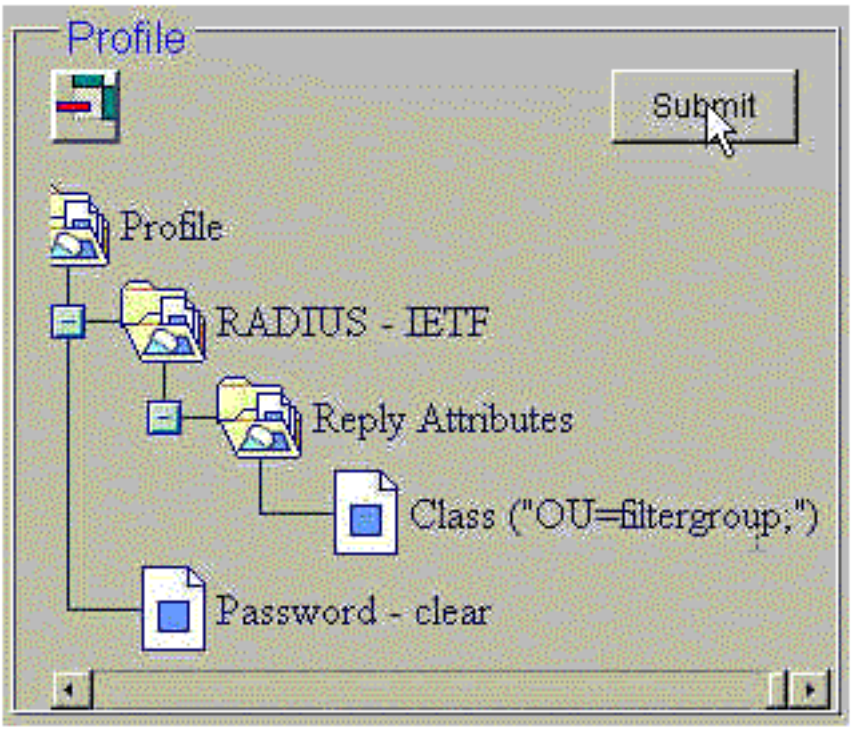


8. 按一下「**Submit + Restart**」。

Cisco Secure for UNIX

這些步驟將您的Cisco Secure UNIX RADIUS伺服器設定為將使用者鎖定到VPN集中器上配置的特定組中。請記住，在RADIUS伺服器上定義的組與VPN集中器上定義的組無關。您可以在RADIUS伺服器上使用群組，使使用者的管理更容易。這些名稱不必與VPN集中器上的配置匹配。

1. 在「高級」部分下將VPN集中器作為NAS新增到RADIUS伺服器。選擇允許將屬性25作為回覆屬性傳送的字典。例如IETF或Ascend。
2. 新增使用者。在本示例中，使用者為「TEST」。 此使用者可位於任何Cisco Secure UNIX組中或不位於任何組中。除了傳遞屬性25以告知VPN集中器使用者使用哪個組之外，Cisco Secure UNIX組和VPN集中器組之間沒有關聯。
3. 在使用者/組配置檔案下，定義RADIUS(IETF)返回屬性。
4. 新增Class屬性，屬性編號**25**，並將其**值OU=filtergroup;**。將VPN集中器上定義的組替換為filtergroup。**注意：**在Cisco Secure UNIX中，定義由引號包圍的屬性。屬性傳送到VPN集中器時，這些屬性被刪除。使用者/組配置檔案應如下所示。



5. 按一下**Submit**儲存每個條目。完成的Cisco Secure UNIX條目類似於以下輸出：

```
# ./ViewProfile -p 9900 -u NAS.172.18.124.132
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
Dictionary="DICTIONARY.IETF"

}

# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"
 !--- The semi-colon does NOT appear !--- after the group name, even though it has to be
included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
check_items= { 2="Anything" } } }
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- VPN 3000集中器上的Cisco VPN 3000客戶端使用者和組屬性處理
- RADIUS（遠端驗證撥入使用者服務）技術支援頁面
- Cisco VPN 3000系列集中器支援頁
- Cisco VPN 3000客戶端支援頁
- IP安全通訊協定(IPSec)產品支援頁面
- 要求建議 (RFC)
- Cisco Secure ACS for Windows產品支援頁面
- 安全產品現場通知
- Cisco Secure ACS for UNIX產品支援頁
- 技術支援 - Cisco Systems