VPN 3000集中器上的Cisco VPN客戶端使用者和組屬性處理

目錄

簡介

本文檔介紹如何在VPN集中器上對Cisco VPN客戶端進行身份驗證，以及Cisco VPN 3000集中器如何使用使用者和組屬性。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於Cisco VPN 3000集中器。

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。

VPN客戶端連線到VPN 3000集中器

當VPN客戶端連線到VPN 3000集中器時，最多可以進行四個身份驗證。

1. 組經過身份驗證。（這通常稱為「隧道組」。）
2. 使用者通過驗證。
3. （可選）如果使用者是另一個組的一部分，則此組隨後進行身份驗證。如果使用者不屬於另一個組或隧道組，則使用者預設為基本組，不會執行此步驟。
4. 步驟1中的「通道群組」將再次進行驗證。(這會在使用「群組鎖定」功能的情況下完成。2.1版或更高版本提供此功能。)

這是您在通過內部資料庫進行身份驗證的VPN客戶端的事件日誌中看到的事件示例（「testuser」是組「Engineering」的一部分）。

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

注意：要檢視這些事件，必須在Configuration > System > Events > Classes中將Auth事件類配置為嚴重性為1-6。

組鎖定功能 — 如果在Group - Tunnel_Group上啟用組鎖定功能，則使用者必須是Tunnel_Group的一部分才能連線。在上一個示例中，您將看到所有相同的事件，但「testuser」沒有連線，因為它們是Group - Engineering的一部分，而不是Group - Tunnel_Group的一部分。您還會看到以下事件：

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

有關組鎖定功能和示例配置的其他資訊，請參閱使用RADIUS伺服器將使用者鎖定到VPN 3000集中器組。

通過RADIUS在外部驗證組和使用者

VPN 3000集中器還可以配置為通過RADIUS伺服器對外部使用者和組進行身份驗證。這仍需要在VPN集中器上配置組的名稱，但組型別配置為「外部」。

- 如果RADIUS伺服器支援供應商特定屬性(VSA)，則外部組可以返回Cisco/Altiga屬性。
- RADIUS未返回的任何Cisco/Altiga屬性都預設為基本組中的值。
- 如果RADIUS伺服器不支援VSA，則ALL屬性預設為基本組屬性。

注意：RADIUS伺服器處理組名稱與使用者名稱沒有區別。RADIUS伺服器上的群組設定方式與標準使用者相同。

以下步驟概述了IPSec客戶端連線到VPN 3000集中器時，如果使用者和組都進行了外部身份驗證，會發生什麼情況。與內部情況類似，最多可以進行四個身份驗證。

1. 群組是透過RADIUS進行驗證。RADIUS伺服器可為群組傳回多個屬性，甚至根本不會傳回任何屬性。RADIUS伺服器至少需要傳回Cisco/Altiga屬性「IPSec Authentication = RADIUS」，以告訴VPN集中器如何驗證使用者。如果不是，則基本組的IPSec身份驗證方法需要設定為「RADIUS」。
2. 使用者透過RADIUS進行驗證。RADIUS伺服器可為使用者傳回多個屬性，甚至根本不會傳回任何屬性。如果RADIUS伺服器返回屬性CLASS(標準RADIUS屬性#25)，則VPN 3000集中器

會使用該屬性作為組名稱並移至步驟3，否則，它將轉至步驟4。
3. 接下來透過RADIUS驗證使用者群組。RADIUS伺服器可為群組傳回多個屬性，甚至根本不會傳回任何屬性。
4. 步驟1中的「通道群組」會透過RADIUS再次進行驗證。身份驗證子系統必須再次對隧道組進行身份驗證，因為它尚未儲存步驟1中身份驗證的屬性（如果有）。如果使用「組鎖定」功能，則會執行此操作。

VPN 3000集中器如何使用使用者和組屬性

在VPN 3000集中器對使用者和組進行身份驗證後，它必須組織所接收的屬性。VPN集中器按此優先順序使用屬性。無論身份驗證是在內部還是外部完成：

1. **使用者屬**性 — 這些屬性優先於所有其他屬性。
2. **組屬性** — 使用者屬性中缺少的任何屬性均由組屬性填充。任何相同內容都將被使用者屬性覆蓋。
3. **隧道組屬**性 — 使用者或組屬性中缺少的任何屬性均由隧道組屬性填充。任何相同內容都將被使用者屬性覆蓋。
4. **基本組屬**性 — 使用者、組或隧道組屬性中缺少的任何屬性均由基本組屬性填充。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- Cisco VPN使用者端支援頁面
- IPSec支援頁面
- RADIUS 支援頁面
- 要求建議 (RFC)
- 技術支援 - Cisco Systems