如何建立與Active Directory組匹配的訪問策略組？

目錄

問題

如何建立與Active Directory(AD)組匹配的訪問策略組？

第一步是配置身份驗證領域(NT LAN Manager(NTLM)領域)和使用身份驗證領域的身份。

---

1. 在網路安全裝置(WSA)的**網路>身份驗證**下建立NTLM領域。
2. 配置NTLM領域後，請選擇**Web Security Manager > Identities**，然後按一下**Add Identity**。
3. 按照以下步驟建立身份： 名稱:Auth.Id在上方插入：1通過身份驗證定義成員：*<NTLM領域名稱>*方案：**使用基本或NTLMSSP**或**使用NTLMSSP**將所有其他設定保留為預設值。
   如果要針對選定的客戶端測試身份驗證，請使用**Define Members By Subnet**並指定請求客戶端的IP。這允許WSA僅為這些選定的客戶端請求身份驗證。按一下「**Submit**」。

此時，您應該只具有兩個身份：**Auth.Id**和**Global Identity Policy**，並在**Auth.Id**身份上啟用身份驗證。

下一步是使用**Auth.Id**身份並基於此身份建立訪問策略。您可以在訪問策略中指定所需的AD組或使用者。

---

1. 選擇**GUI > Web Security Manager > Access Policies**。
2. 按一下**Add Policy**。
3. 按照以下步驟建立訪問策略： 策略名稱：Sales.Policy在策略上插入：1身份策略：Auth.Id — 指定**授權組和使用者**手動輸入組名，或按一下**刷新目錄**以獲取AD上存在的使用者清單。選擇使用者後，按一下**Add**。完成後按一下**Submit**。

如果需要建立其他訪問策略，請按一下**Add Policy**，然後為新的AD組建立其他訪問策略。

您不應為同一身份驗證領域建立新身份。只要身份未繫結到**Proxy Ports**、**URL Categories**、**User Agents**或**Define Members by Subnet**，即可重複使用現有身份(Auth.Id)並為不同的AD組建立新的訪問策略。

對於使用不同AD組的多個訪問策略，設定應如下所示：

身份

"Auth.Id"
"全域性身份策略"

訪問策略

使用「Auth.Id」的「Sales.Policy」
使用「Auth.Id」的「Support.Policy」
使用「Auth.Id」的「Manager.Policy」
使用「Auth.Id」的「Admin.Policy」
使用「All」的「Global Policy」