

# 區分ASA平台上的身份驗證型別，以便在ISE上做出策略決策

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[RADIUS VSA 3076/150使用者端型別屬性](#)

[設定](#)

[步驟1](#)

[步驟2](#)

[驗證](#)

[相關資訊](#)

## 簡介

本文檔介紹如何配置思科身份服務引擎(ISE)以利用客戶端型別RADIUS供應商特定屬性(VSA)來區分思科自適應安全裝置(ASA)上使用的多種身份驗證型別。組織通常需要根據使用者向ASA進行身份驗證的方式做出策略決策。此功能也允許您對ASA上的已接收管理連線應用策略，這樣我們可以謹慎使用RADIUS代替TACACS+。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ISE身份驗證和授權。
- ASA身份驗證方法和RADIUS配置。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科調適型安全裝置版本8.4.3。
- 思科身分識別服務引擎版本1.1。

### 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## [RADIUS VSA 3076/150使用者端型別屬性](#)

Client-Type屬性新增在ASA 8.4.3版中，允許ASA向ISE傳送在Access-Request ( 和Accounting-Request ) 資料包中進行身份驗證的客戶端型別，並允許ISE根據該屬性做出策略決策。此屬性不需要在ASA上進行配置，並且會自動傳送。

Client-Type屬性當前使用以下整數值定義：

1. Cisco VPN使用者端(Internet金鑰交換版本(IKEv1))
2. AnyConnect客戶端SSL VPN
3. 無客戶端SSL VPN
4. 直通代理
5. L2TP/IPsec SSL VPN
6. AnyConnect客戶端IPsec VPN(IKEv2)

## [設定](#)

本節提供配置ISE以使用本文檔所述客戶端型別屬性所需的資訊。

### [步驟1](#)

#### [建立自定義屬性](#)



要將客戶端型別屬性值新增到ISE，請建立屬性並將其值填充為自定義詞典。

1. 在ISE上，導航到**Policy > Policy Elements > Dictionaries > System**。
2. 在**System**詞典中，導覽至**RADIUS > RADIUS Vendors > Cisco-VPN3000**。
3. 螢幕上的供應商ID應為3076。按一下**Dictionary Attributes**選項卡。按一下「Add」（請參見圖1）。**圖1:字典屬性**

Dictionary

Dictionary Attributes

## Dictionary Attributes

 Add Edit Delete

<input type="checkbox"/>	Name	Attribute Numb... ▲	Type	Direction
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	1	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	10	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	11	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	12	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	128	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	129	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	13	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	131	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	132	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	133	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	134	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	135	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	136	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	137	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	15	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7x-...	150	UINT32	BOTH

填充自定義RADIUS供應商屬性表單中的欄位，如圖2所示。圖2:RADIUS供應商屬性

## ▼ RADIUS Vendor Attribute

\* Attribute Name

Description

\* Internal Name

\* Data Type

\* Direction

\* ID  (0-255)

Does this attribute support Tagging Is this a attribute allowed multiple times in Authz Profile 

## Allowed Values

+ Add - Delete

<input type="checkbox"/>	Name	Value	isDefault
<input type="checkbox"/>	Cisco VPN Client (IKEv1)	1	⊗
<input type="checkbox"/>	AnyConnect Client SSL...	2	⊗
<input type="checkbox"/>	Clientless SSL VPN	3	⊗
<input type="checkbox"/>	Cut-Through-Proxy	4	⊗
<input type="checkbox"/>	L2TP/IPsec SSL VPN	5	⊗
<input type="checkbox"/>	AnyConnect Client IPse...	6	⊗

按一下螢幕底部的**Save**按鈕。

## 步驟2

### 新增客戶端型別屬性

為了將新屬性用於策略決策，請在條件部分將該屬性新增到授權規則。

1. 在ISE中，導航到**Policy > Authorization**。
2. 建立新規則或修改現有策略。
3. 在規則的條件部分，展開條件窗格，然後選擇**建立新條件**（對於新規則）或**新增屬性/值**（對於預先存在的規則）。
4. 在**Select Attribute**欄位中，導航至**Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type**。
5. 為您的環境選擇適當的運算子（等於或不等於）。
6. 選擇要匹配的**Authentication**型別。
7. 分配適合您的策略的授權結果。
8. 按一下「**完成**」。
9. 按一下「**Save**」。

建立規則後，授權條件應類似於圖3中的示例。

### 圖3:授權條件示例

```
if Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type EQUALS Cut-Through-Proxy
```

## 驗證

要驗證客戶端型別屬性是否正在使用，請檢查ISE中來自ASA的身份驗證。

1. 導航到**操作 > 身份驗證**
2. 按一下**Details**按鈕從ASA進行身份驗證。
3. 向下滾動到**Other Attributes**，並查詢**CVPN3000/ASA/PIX7x-Client-Type=**（請參見圖4）

#### 4:其他屬性詳細資訊

```
ConfigVersionId=4, DestinationPort=1812, Protocol=Radius, CVPN3000/ASA/PIX7x-Client-Type=4, CPMSessionID=0e24970b0000000051000B89, EndPointMACAddress=00-55-44-33-22-11, Device Type=Device Type#All Device Types, Location=Location#All Locations, Device IP Address=172.18.254.150
```

4. **Other Attributes**欄位應指明收到的身份驗證值。規則應與配置部分步驟2中定義的策略相匹配。

## 相關資訊

- [思科身分識別服務引擎](#)
- [思科調適型安全裝置5500系列下一代防火牆](#)
- [技術支援與文件 - Cisco Systems](#)