

# Gedifferentieerde verificatietypen op ASA-platforms voor beleidsbeslissingen op ISE

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[RADIUS VSA 3076/1500 clienttype, kenmerk](#)

[Configureren](#)

[Stap 1](#)

[Stap 2](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document beschrijft hoe u Cisco Identity Services Engine (ISE) moet configureren om het clienttype RADIUS-leverancierspecifieke kenmerk (VSA) te gebruiken om meerdere typen verificatie te differentiëren die worden gebruikt op de Cisco adaptieve security applicatie (ASA). Organisaties vereisen vaak beleidsbeslissingen die zijn gebaseerd op de authenticatie van de gebruiker aan de ASA. Dit stelt u ook in staat om beleid toe te passen op ontvangen beheerverbindingen op de ASA, die ons in staat stelt om RADIUS te gebruiken in plaats van TACACS+, wanneer verstandig.

## [Voorwaarden](#)

### [Vereisten](#)

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE-authenticatie en autorisatie.
- ASA-verificatiemethoden en RADIUS-configuratie.

### [Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security applicatie release 8.4.3
- Cisco Identity Services Engine release 1.1.

## Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## RADIUS VSA 3076/1500 clienttype, kenmerk

De eigenschap Client-Type werd toegevoegd in ASA release 8.4.3. Hiermee kan de ASA het type client naar de ISE sturen in pakketten met toegangsaanvraag (en accounting-aanvraag) en ISE in staat stellen beleidsbeslissingen te nemen op basis van die eigenschap. Deze eigenschap vereist geen configuratie op de ASA, en wordt automatisch verzonden.

De eigenschap Client-Type wordt momenteel gedefinieerd met deze integerwaarden:

1. Cisco VPN-client (Internet Key Exchange versie (IKEv1)
2. AnyConnect-client-SSL VPN
3. Clientloze SSL VPN
4. Cut-Through Proxy
5. L2TP/IPsec VPN
6. AnyConnect-client voor IPsec VPN (IKEv2)

## Configureren

In dit gedeelte wordt de informatie verstrekt die u nodig hebt om de ISE te configureren voor het gebruik van de eigenschap Client-Type die in dit document wordt beschreven.

### Stap 1

#### De aangepaste kenmerken maken




Als u de waarden van de eigenschap client-type aan ISE wilt toevoegen, maakt u de eigenschap en vult u de waarden in als een aangepast woordenboek.

1. Op ISE, navigeer naar **Policy > Policy Elementen > Woordenboeken > System**.
2. Binnen de **stysteemwoordenboeken**, navigeer naar **RADIUS > RADIUS-verkopers > Cisco-VPN3000**.
3. De verkoper-ID op het scherm moet 3076 zijn. Klik op het tabblad **Woordenboek-kenmerken**. Klik op **Add** (zie afbeelding 1). **Afbeelding 1: Woordenboek-kenmerken**

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

Bedek de velden in de vorm van de aangepaste RADIUS-leverancierkenmerken zoals in afbeelding 2. **Afbeelding 2: RADIUS-leverancierkenmerken**

## ▼ 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	⊗

Klik onder in het scherm op de knop **Opslaan**.

## Stap 2

### [Toevoegen clienttype-kenmerk](#)

Om de nieuwe eigenschap voor beleidsbeslissingen te gebruiken, de eigenschap aan een machtigingsregel toe te voegen in het vak voorwaarden.

1. In ISE, navigeer naar **Policy > Authorization**.
2. Maak een nieuwe regel of wijzig een bestaand beleid.
3. In het gedeelte onder voorwaarden van de regel vouwt u het deelvenster met voorwaarden uit en selecteert u **Een nieuwe conditionering maken** (voor een nieuwe regel) of **Eigenschappen/waarde toevoegen** (voor een bestaande regel).
4. In het veld **Selectietekens** navigeer naar **Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-client-type**.
5. Kies de juiste operator (**is gelijk aan** of **is niet gelijk aan**) voor uw omgeving.
6. Kies het **verificatietype** dat u wilt aanpassen.
7. Wijs een **vergunningresultaat toe** dat aan uw beleid aangepast is.
8. Klik op **Klaar**.
9. Klik op **Opslaan**.

Nadat de regel is gemaakt, zou de machtigingsvoorwaarde op het voorbeeld in afbeelding 3 moeten lijken.

### Afbeelding 3: Voorbeeld van machtigingsvoorwaarden

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

## Verifiëren

Om de eigenschap van het clienttype in gebruik te controleren, dient u de authenticaties van de ASA in ISE te onderzoeken.

1. Navigeren in naar **bewerkingen > Verificaties**
2. Klik op de knop **Details** voor de verificatie van de ASA.
3. Naar **andere kenmerken** bladeren en naar **CVPN300/ASA/PIX7x-Client-Type=** (zie afbeelding 4) bladeren

### **Afbeelding 4: Overige bijzonderheden**

```
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. Het veld **Overige Eigenschappen** dient de ontvangen waarde voor de echtheidscontrole aan te geven. De regel moet overeenkomen met het beleid dat in stap 2 van het configuratiegedeelte is gedefinieerd.

## Gerelateerde informatie

- [Cisco Identity Services Engine](#)
- [Cisco adaptieve security applicatie 5500 Series Next-generation firewalls](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)