

مظنأ ىل ع قداصم لآ عاونأ نىب زىم لآ ىل ع ةساي س لآ تارارق ذاخ تال ةي س اس لآ ASA ISE

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[سمة نوع العميل ل RADIUS VSA 3076/150](#)

[التكوين](#)

[الخطوة 1](#)

[الخطوة 2](#)

[التحقق من الصحة](#)

[معلومات ذات صلة](#)

[المقدمة](#)

يصف هذا المستند كيفية تكوين محرك خدمات الهوية من ISE (Cisco) لاستخدام سمة VSA الخاصة ببيع RADIUS من نوع العميل (VSA) للتمييز بين أنواع متعددة من المصادقة المستخدمة على جهاز الأمان القابل للتكيف (ASA) من Cisco. غالبا ما تتطلب المؤسسات قرارات تتعلق بالسياسات استنادا إلى الطريقة التي تتم بها مصادقة المستخدم على ASA. وهذا يتيح لك أيضا تطبيق السياسة على إتصالات الإدارة المستلمة على ASA، والتي تتيح لنا استخدام RADIUS بدلا من TACACS+، عندما يكون ذلك حكيمًا.

[المتطلبات الأساسية](#)

[المتطلبات](#)

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مصادقة ISE والتحويل.
- طرق مصادقة ASA وتكوين RADIUS.

[المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز Cisco Adaptive Security Appliance، الإصدار 8.4.3.
- محرك خدمات تعريف Cisco الإصدار 1.1.

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

RADIUS VSA 3076/150 ل نوع العميل

تمت إضافة السمة نوع العميل في الإصدار 8.4.3 من ASA، والذي يسمح ل ASA بإرسال نوع العميل الذي يصدق على ISE في حزم طلب الوصول (و accounting-request)، ويسمح ل ISE باتخاذ قرارات السياسة استنادا إلى هذه السمة. لا تتطلب هذه السمة أي تكوين على ASA، ويتم إرسالها تلقائيا.

تم تعريف السمة Client-Type حاليا مع قيم العدد الصحيح التالية:

1. عميل Cisco VPN (إصدار تبادل مفتاح الإنترنت (IKEv1)
2. AnyConnect Client SSL VPN
3. ClientWithout SSL VPN
4. بروكسي قطع
5. L2TP/IPsec SSL VPN
6. (AnyConnect Client IPsec VPN (IKEv2

التكوين

في هذا القسم، يتم توفير المعلومات التي تحتاج إليها لتكوين ISE لاستخدام سمة نوع العميل الموضحة في هذا المستند.

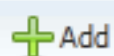
الخطوة 1

إنشاء السمة المخصصة

لإضافة قيم سمة نوع العميل إلى ISE، قم بإنشاء السمة وتعميم قيمها كقاموس مخصص.

1. على ISE، انتقل إلى السياسة < عناصر السياسة < القواميس < النظام.
2. ضمن قواميس النظام، انتقل إلى RADIUS < بائعي Cisco-VPN3000 > RADIUS.
3. يجب أن يكون معرف المورد على الشاشة هو 3076. انقر على صفحة خصائص القاموس. انقر فوق إضافة (راجع الشكل 1). شكل 1: خصائص القاموس

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

ملء الحقول الموجودة في نموذج سمة مورد RADIUS المخصص كما هو موضح في الشكل 2. شكل 2: سمة مورد RADIUS

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 checked="" type="checkbox"/>
<input type="checkbox"/>	AnyConnect Client SSL...	2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Clientless SSL VPN	3	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Cut-Through-Proxy	4	<input checked="" type="checkbox"/>
<input type="checkbox"/>	L2TP/IPsec SSL VPN	5	<input checked="" type="checkbox"/>
<input type="checkbox"/>	AnyConnect Client IPse...	6	<input checked="" type="checkbox"/>

انقر فوق زر حفظ في أسفل الشاشة.

الخطوة 2

إضافة سمة نوع العميل

لاستخدام السمة الجديدة لقرارات النهج، قم بإضافة السمة إلى قاعدة تحويل في قسم الشروط.

1. في ISE، انتقل إلى السياسة < التفويض.
 2. إنشاء قاعدة جديدة أو تعديل سياسة موجودة.
 3. في قسم الشروط من القاعدة، قم بتوسيع جزء الشروط وحدد إما إنشاء شرط جديد (لقاعدة جديدة) أو إضافة سمة/قيمة (لقاعدة موجودة مسبقاً).
 4. في حقل تحديد سمة، انتقل إلى Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-client-type.
 5. اختر المشغل المناسب (يساوي أو لا يساوي) لبيئتك.
 6. اختر نوع المصادقة الذي تريد مطابقته.
 7. قم بتعيين نتيجة تحويل مناسبة للنهج الخاص بك.
 8. طقطقة تم.
 9. طقطقة حفظ.
- بعد إنشاء القاعدة، يجب أن يبدو شرط التحويل مماثلاً للمثال الموجود في الشكل 3.

الشكل 3: مثال حالة التحويل

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

التحقق من الصحة

للتحقق من أن السمة Client-Type قيد الاستخدام، قم بفحص المصادقة من ASA في ISE.

1. انتقل إلى العمليات < المصادقة

2. طقطقت التفاصيل زر للمصادقة من ال ASA.

3. قم بالتمرير إلى سمات أخرى وابحث عن **CVPN3000/ASA/PIX7x-client-type** (راجع الشكل 4) الشكل 4:
تفاصيل السمات الأخرى

```
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. يجب أن يشير حقل السمات الأخرى إلى القيمة المستلمة للمصادقة. يجب أن تتطابق القاعدة مع السياسة المحددة في الخطوة 2 من قسم التكوين.

معلومات ذات صلة

- [محرك خدمات الهوية من Cisco](#)
- [أجهزة الأمان المعدلة Cisco 5500 Series جدران الحماية من الجيل التالي](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل