سحابة TrustSec مع 802.1x MACsec على مدة حفازة 3750X sery مفتاح تشكيل مثال

المحتويات

المقدمة

يصف هذا المقال الخطوات المطلوبة لتكوين سحابة Cisco TrustSec (CTS) باستخدام تشفير الارتباط بين محولين من السلسلة Catalyst 3750X Series (3750X).

يشرح هذا المقال عملية تشفير أمان التحكم في الوصول إلى الوسائط (MACsec) من المحول إلى المحول التي تستخدم بروتوكول إرتباط الأمان (SAP). تستخدم هذه العملية وضع IEEE 802.1x بدلا من الوضع اليدوي.

فيما يلي قائمة بالخطوات المعنية:

- توفير بيانات اعتماد الوصول المحمي (PAC) للأجهزة الأساسية وغير الأساسية
- مصادقة التحكم في الدخول إلى جهاز الشبكة (NDAC) تفاوض MACsec مع SAP لإدارة المفاتيح
- تحديث البيئة والسياسة
- مصادقة المنفذ للعملاء
- تعليم حركة المرور باستخدام رقم مجموعة الأمان (الرقيب)
- تنفيذ السياسة باستخدام قائمة التحكم في الوصول (ACL) الخاصة بمجموعة الأمان

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بمكونات CTS
- معرفة الأساسية ال CLI تشكيل من مادة حفازة مفاتح
- تجربة تكوين محرك خدمات الهوية (ISE)

المكونات المستخدمة

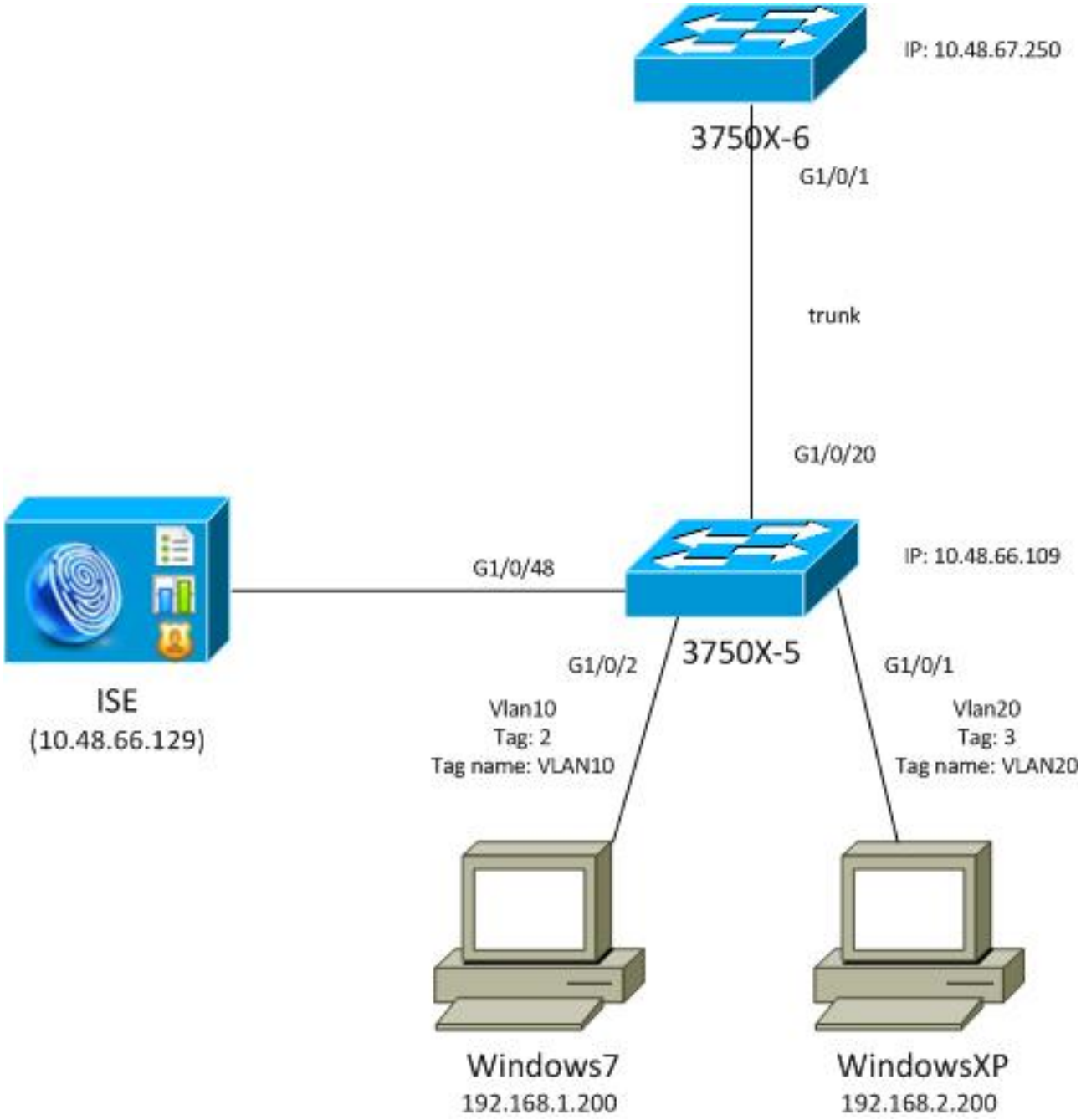
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Microsoft (MS) Windows 7 و MS Windows XP
- برنامج 3750X، الإصدارات 15.0 والإصدارات الأحدث
- برنامج ISE، الإصدارات 1.1.4 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة



في هذا الرسم التخطيطي لهيكل الشبكة، يكون المحول 3750X-5 هو الجهاز الأولي الذي يعرف عنوان IP الخاص ب ISE، وهو يقوم تلقائيا بتنزيل مسوغ الوصول المحمي (PAC) الذي يتم إستخدامه للمصادقة اللاحقة في سحابة CTS. يعمل جهاز البوذر كمصدق 802.1x للأجهزة غير الأولية. ال cisco مادة حفازة 3750X-6 sery مفتاح (3750X-6) ال ال بذرة أداة. يعمل كمسبب 802.1x لجهاز البوذر. بعد مصادقة الجهاز غير الأساسي على ISE من خلال الجهاز الأولي، يتم السماح بالوصول إلى سحابة CTS. بعد مصادقة ناجحة، يتم تغيير حالة المنفذ 802.1X على المحول 3750X-5 إلى **مصدق**، ويتم التفاوض على تشفير MACsec. ثم يتم وضع علامة على حركة مرور البيانات بين المحولات باستخدام أداة Sgt (الرقيب) والشفر.

تلخص هذه القائمة تدفق حركة المرور المتوقع:

- تتصل النسخة الأولية 3750X-5 ب ISE وتنزيلات مسوغات الوصول المحمي (PAC)، والتي يتم إستخدامها لاحقا لتحديث البيئة والسياسة.
- تقوم الاطابعة غير الأولية 3750X-6 بإجراء مصادقة 802.1X مع دور الاطالب للمصادقة/التخويل وتنزيل مسوغ الوصول المحمي (PAC) من ISE.
- يقوم 3750X-6 بتنفيذ مصادقة ثانية مرنة لبروتوكول 802.1X للمصادقة المتوسع من خلال جلسة عمل البروتوكول الآمن (EAP-FAST) للمصادقة مع النفق المحمي

استنادا إلى مسوغ الوصول المحمي.

- سياسات SGA الخاصة بالتنزيلات 3750X-5 لنفسها وبالنيابة عن 3750X-6.
- تحدث جلسة عمل SAP بين 3750X-5 و 3750X-6، ويتم التفاوض على شفرات MacSec، ويتم تبادل السياسة.
- تحدد حركة مرور بين المفتاحوتشفر.

تكوين المحولات الأولية وغير الأولية

تم تكوين الجهاز الأولي (3750X-5) من أجل إستخدام ISE كخادم RADIUS ل CTS:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

cts authorization list ise

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

يتم تمكين تنفيذ قائمة التحكم في الوصول (RBACL) المستندة إلى الأدوار وقائمة التحكم في الوصول المستندة إلى مجموعة الأمان (SGACL) (يتم إستخدامها لاحقا):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

يتم تكوين الجهاز غير الأساسي (3750X-6) فقط للمصادقة والتخويل والمحاسبة (AAA) دون الحاجة إلى تفويض RADIUS أو CTS:

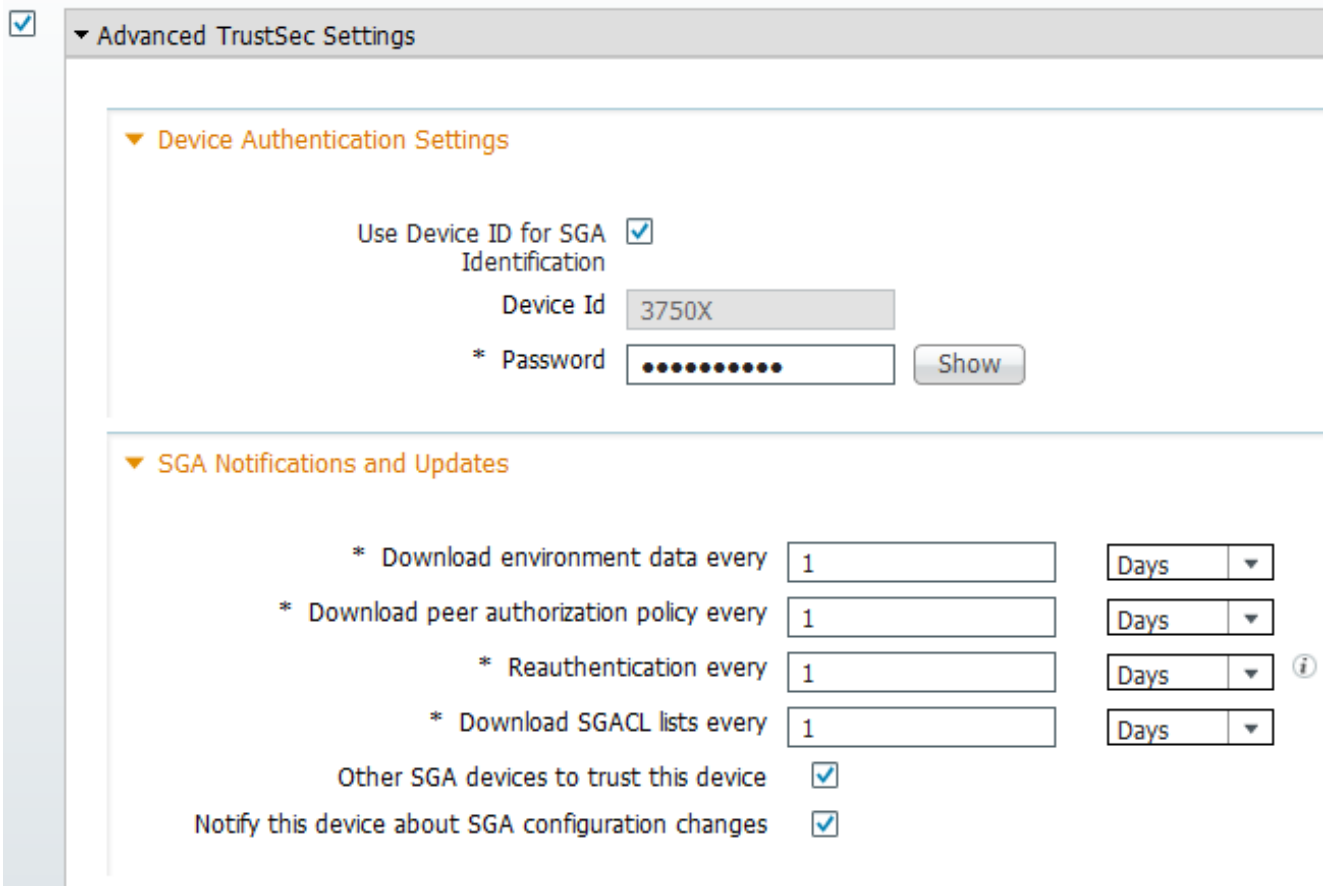
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

قبل أن يمكن أنت 802.1x على القارن، هو ضروري أن يشكل ال ISE.

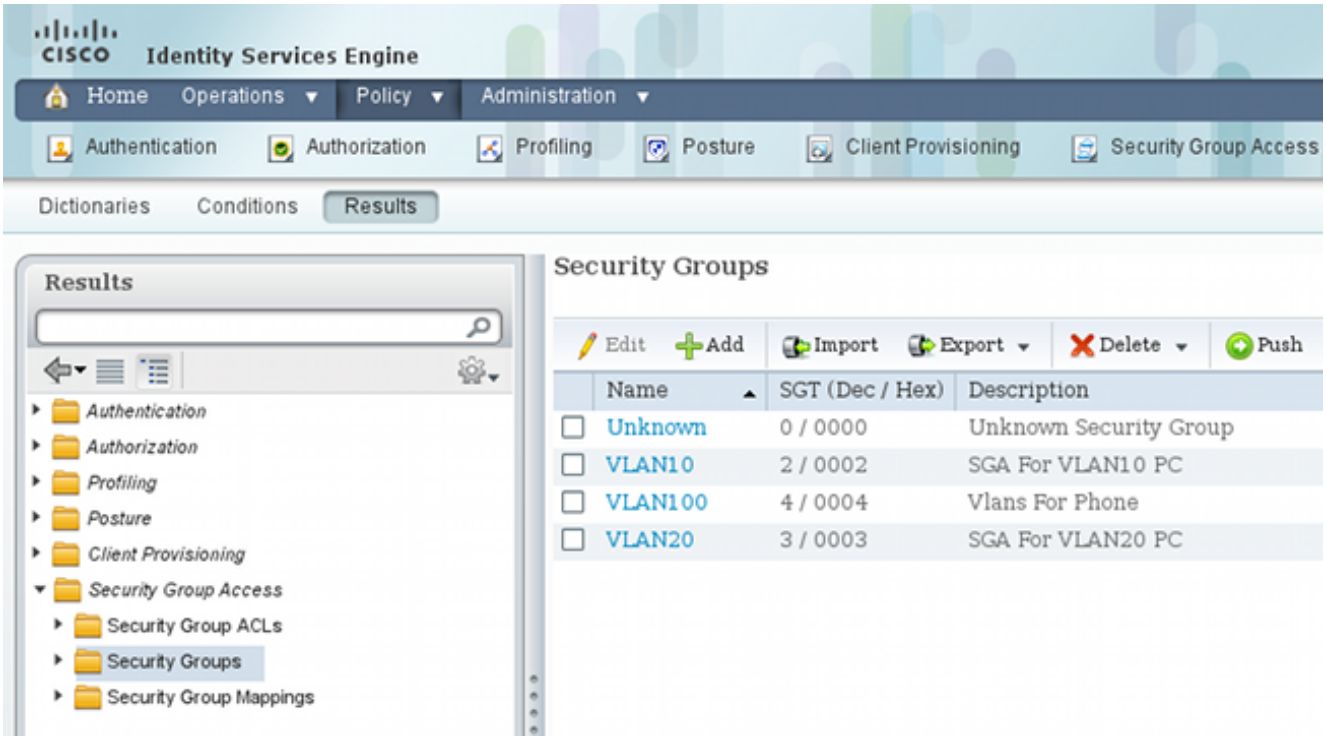
تكوين ISE

أتمت هذا steps in order to شكلت ال ISE:

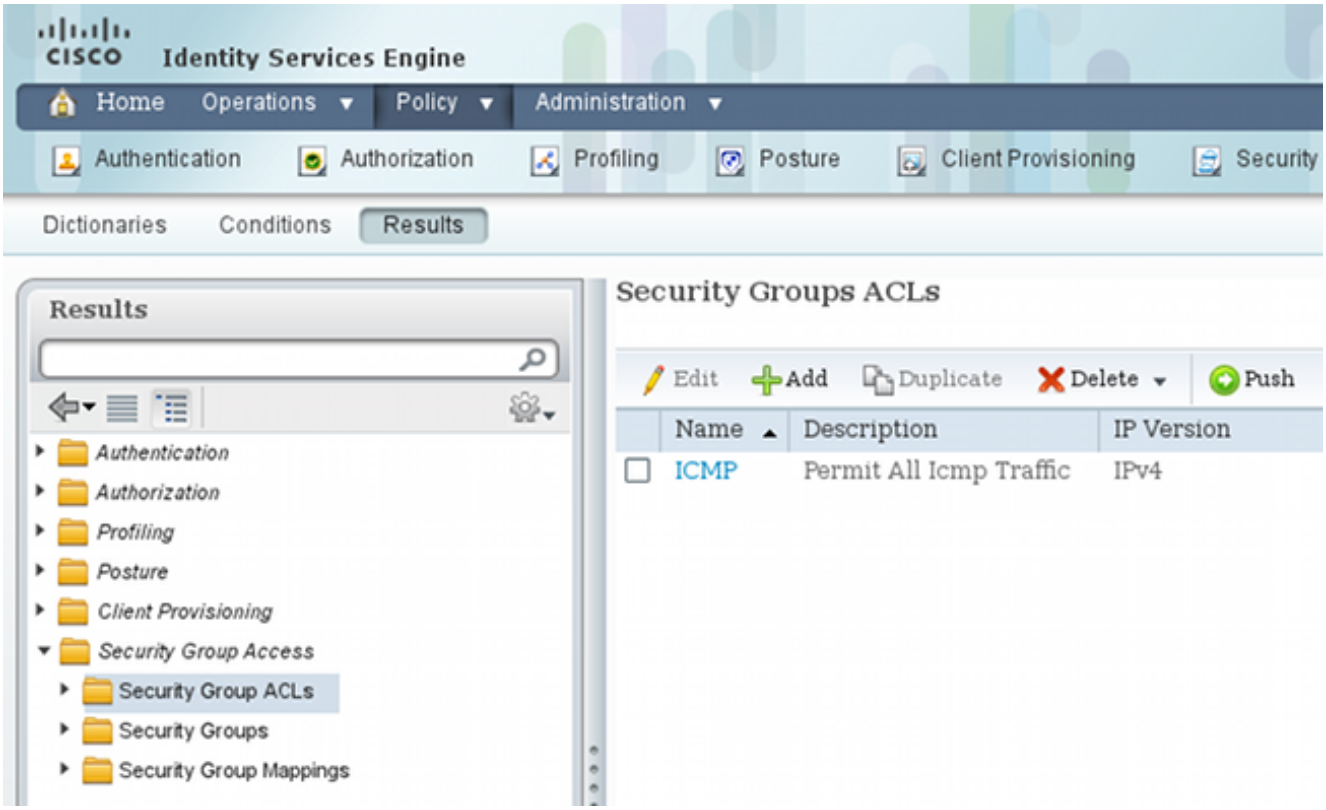
1. انتقل إلى **إدارة > موارد الشبكة > أجهزة الشبكة**، وأضف كلا المحولين كأجهزة وصول إلى الشبكة (NADs). تحت **إعدادات TrustSec المتقدمة**، قم بتكوين كلمة مرور CTS للاستخدام لاحقا على CLI (واجهة سطر الأوامر) للمحول.



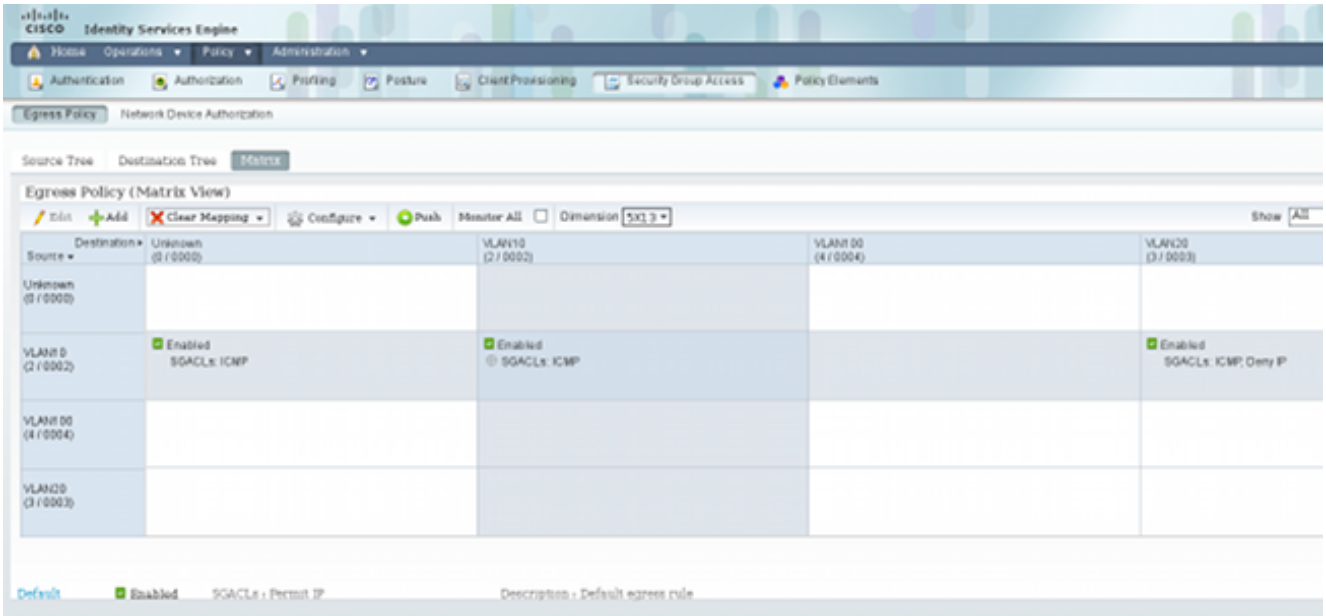
2. انتقل إلى **السياسة > عناصر السياسة > النتائج > الوصول إلى مجموعة الأمان > مجموعات الأمان**، وقم بإضافة الرقابات المناسبة. يتم تنزيل هذه العلامات عندما تطلب المحولات تحديث البيئة.



3. انتقل إلى **السياسة > عناصر السياسة > النتائج > وصول مجموعة الأمان > قوائم التحكم في الوصول لمجموعة الأمان**، وقم بتكوين SGACL.



4. انتقل إلى **السياسة > الوصول إلى مجموعة الأمان**، وحدد سياسة باستخدام المصفوفة.



ملاحظة: يجب تكوين نهج التخويل لمطلب MS Windows حتى يتمكن من تلقي العلامة الصحيحة. ارجع إلى [مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec دليل استكشاف الأخطاء وإصلاحها](#) للحصول على تكوين مفصل لهذا.

إمداد PAC لـ 3750X-5

هناك حاجة إلى مسوغات الوصول المحمي (PAC) للمصادقة في مجال CTS (مثل المرحلة 1 لـ EAP-FAST)، كما تستخدم من أجل الحصول على بيانات البيئة والسياسة من ISE. وبدون

مسوغ الوصول المحمي الصحيح، ال يمكن الحصول على تلك البيانات من مركز التقييم المستقل.

بعد تقديم بيانات الاعتماد الصحيحة على 3750X-5، يتم تنزيل مسوغات الوصول المحمي (PAC):

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

يتم تنزيل مسوغات الوصول المحمي (PAC) عبر EAP-FAST مع بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (MSCHAPv2) من Microsoft، مع بيانات الاعتماد المقدمة في CLI ونفس بيانات الاعتماد التي تم تكوينها على ISE.

يتم إستخدام مسوغ الوصول المحمي (PAC) لتحديث البيئة والنهج. لتلك الموحالات، أستخدم طلبات RADIUS مع **cisco av-pair cts-pac-opaque**، والتي يتم اشتقاقها من مفاتح PAC ويمكن فك تشفيرها على ISE.

إدمال PAC لمصادقة 3750X-6 و NDAC

in order for جديد أداة أن يكون قادر أن يرتبط إلى ال CTS لمجال، وهو ضروري أن يمكن 802.1x على ال عاثل ميناء.

يتم إستخدام بروتوكول SAP لإدارة المفاتيح ومفاوضات مجموعة التشفير. يستخدم رمز مصادقة رسائل Galois (GMAC) للمصادقة ووضع Galois/Counter (GCM) للتشفير.

في مفاتح البوذر:

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

في المحول غير الأساسي:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

هذا مدعوم فقط على منافذ خطوط الاتصال (مفاتيح-مفاتيح MACsec). بالنسبة ل MacSec لمضيف المحول، والذي يستخدم بروتوكول إتفاقية المفاتيح (MKA) بدلا من SAP، ارجع إلى تكوين تشفير MACsec.

مباشرة بعد تمكين 802.1x على المنافذ، يعمل المحول غير الأساسي كمكمل للمحول الأولي، وهو المصدق.

ويطلق على هذه العملية NDAC، وهدفها هو توصيل جهاز جديد بمجال CTS. المصادقة ثنائية الإتجاه، يحتوي الجهاز الجديد على بيانات اعتماد تم التحقق منها على ISE لخادم المصادقة. بعد توفير مسوغ الوصول المحمي (PAC)، يكون الجهاز أيضا متأكدا من إتصاله بمجال CTS.

> **ملاحظة**: يستخدم مسوغ الوصول المحمي (PAC) لإنشاء نفق تأمين طبقة النقل (TLS) ل EAP-FAST. يثق المحول 3750X-6 في مسوغات مسوغات الوصول المحمي (PAC) التي يوفرها الخادم بالطريقة التي يثق بها العميل في الشهادة المقدمة من الخادم بأسلوب EAP-TLS.

يتم تبادل رسائل RADIUS المتعددة:

07,13 10:18:14.848 AM	#CTSREQUEST#		3750X6				CTS Data Download Succeeded
07,13 10:18:14.838 AM	#CTSREQUEST#		3750X6				CTS Data Download Succeeded
07,13 10:18:14.829 AM	#CTSREQUEST#		3750X6				CTS Data Download Succeeded
07,13 10:18:05.029 AM	#CTSDEVICE#-3750X		3750X6				Peer Policy Download Succeeded
07,13 10:18:05.023 AM	#CTSDEVICE#-3750X6		3750X				Peer Policy Download Succeeded
07,13 10:18:05.009 AM	3750X6	10:F3:11:A7:E5:01	3750X	GigabitEthernet1/0/20	Permit Access	NotApplicable	Authentication succeeded
07,13 10:17:59.850 AM	3750X6	10:F3:11:A7:E5:01	3750X	GigabitEthernet1/0/20			PAC provisioned

يتم إستخدام الجلسة الأولى من ال 3750X (المحول الأولي) لتوفير مسوغ الوصول المحمي. يتم إستخدام EAP-FAST بدون PAC (يتم إنشاء نفق مجهول لمصادقة MSCHAPv2).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

يتم إستخدام اسم مستخدم وكلمة مرور MSCHAPv2 اللذين تم تكوينهما من خلال الأمر **CTS credentials**. كما يتم إرجاع رفض الوصول إلى RADIUS في النهاية، لأنه بعد توفير مسوغ الوصول المحمي (PAC) بالفعل، لا توجد حاجة إلى مزيد من المصادقة.

يشير الإدخال الثاني في السجل إلى مصادقة 802.1x. يستخدم EAP-FAST مع مسوغ الوصول المحمي (PAC) الذي تم توفيره سابقا.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

هذه المرة، النفق ليس مجهول الهوية، ولكنه محمي بواسطة مسوغات الوصول المحمي. مرة أخرى، يتم إستخدام نفس بيانات الاعتماد لجلسة عمل MSCHAPv2. ثم يتم التحقق منه مقابل قواعد المصادقة والتفويض على ISE، ويتم إرجاع قبول وصول RADIUS. بعد ذلك، يطبق المفتاح مصدق الشراع يرجع، وال 802.1x جلسة ل أن ميناء ينتقل إلى دولة مصرح.

ماذا تبدو عملية أول جلستين 802.1x من المحول الأولي؟

هنا أهم تصحيح الأخطاء من البذرة. تكشف البذور عن أن الميناء مرتفع، وتحاول تحديد أي دور

ينبغي أن يستعمل ل 802.1x - المقدم أو المصدق:

```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

أخيرا، استعملت المصدق دور، لأن المفتاح يتلقى منفذ إلى ال ISE. في 3750X-6، يتم إختيار دور الطالب.

تفاصيل حول تحديد دور 802.1x

ملاحظة: بعد أن يحصل المحول المتلقي على مسوغ الوصول المحولات (PAC) ويتم التصديق على 802.1X، يقوم بتنزيل بيانات البيئة (الموضحة الحقا)، ويتعلم عنوان IP الخاص بخادم AAA. في هذا المثال، يحتوي كال المحولين على اتصال (أساسي) مخصص ل ISE. وفيما بعد، يمكن أن تكون الأدوار مختلفة؛ فيصبح المحول الأول الذي يستقبل إستجابة من خادم AAA هو المصدق، ويصبح المحول الثاني هو المتلقي.

وهذا ممكن لأن كال المحولين اللذين يحملان خادم AAA الذي تم وضع عالمة AAA عليه على أنه من أول يصبح على قيد الحياة يرسل نالرعم طلب بروتوكول المصادقة المتوسع (EAP). ويستقبل EAP Identity Response هو المصدق، ويسقط طلبات الهوية الالحقة.

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

```
▸ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Cisco_a7:e5:01 (10:f3:11:a7:e5:01), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 15
  ▾ Extensible Authentication Protocol
      Code: Response (2)
      Id: 1
      Length: 15
      Type: Identity (1)
      Identity: CTS client
```

بعد تحديد دور 802.1X (في هذا السيناريو، يكون لـ 3750X-6 هو المطلوب، لأنه ليس له وصول إلى خادم AAA بعد)، تتضمن الحزم التالية تبادل EAP-FAST لتوفير PAC. يتم إستخدام **عميل CTS** لاسم مستخدم طلب RADIUS وكهوية EAP:

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

بعد بناء نفق EAP-FAST غير المعروف، تحدث جلسة MSCHAPv2 لاسم المستخدم **3750X6** (**مسوغات CTS**). من غير الممكن أن ترى ذلك على الموجه، لأنه نفق TLS (يشفر)، ولكن السجلات التفصيلية على ISE لتوفير PAC تثبت ذلك. يمكنك أن ترى **عميل CTS** لاسم مستخدم RADIUS وعلى هيئة إستجابة هوية EAP. ومع ذلك، بالنسبة للطريقة الداخلية (MSCHAP)، يتم إستخدام اسم المستخدم **3750X6**:

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

تجري مصادقة EAP-FAST الثانية. وفي هذه المرة، يستخدم مسوغ الوصول المحمي (PAC) الذي تم توفيره سابقا. مرة أخرى، يتم إستخدام **عميل CTS** كاسم مستخدم RADIUS والهوية الخارجية، ولكن يتم إستخدام **3750X6** للهوية الداخلية (MSCHAP). نجحت المصادقة:

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

ومع ذلك، ترجع ISE هذه المرة عدة سمات في حزمة قبول RADIUS:

Authentication Result

```
User-Name=3750X6
 State=ReauthSession:C0A800010000053A33FD79AF
 Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
 Session-Timeout=86400
 Termination-Action=RADIUS-Request
 EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
 cisco-av-pair=cts:security-group-tag=0000-01
 cisco-av-pair=cts:supplicant-cts-capabilities=sap
 MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
 MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

هنا، يغير المصدق مفتاح المينا إلى الدولة مصدق:

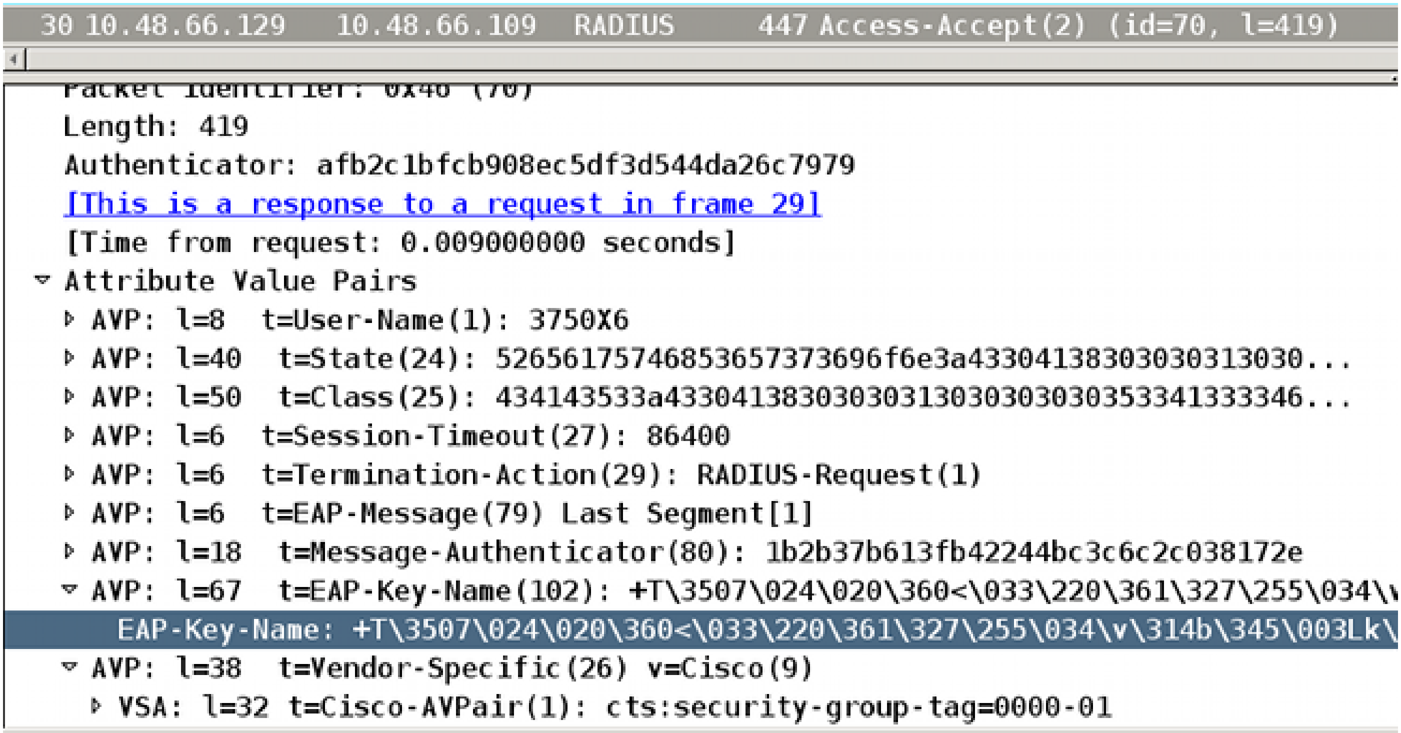
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

كيف يعلم محول المصدق أن اسم المستخدم هو **3750X6**؟ بالنسبة لاسم مستخدم RADIUS ووهوية EAP الخارجية، يتم إستخدام **عميل CTS**، ويتم تشفير الهوية الداخلية و الا تكون

مرئية للمصادقة. اسم المستخدم متعلم من قبل ISE. تحتوي حزمة RADIUS الأخيرة (قبول الوصول) على **اسم المستخدم=3750x6**، بينما تحتوي جميع الحزم الأخرى على **اسم المستخدم = عميل CTS**. هذا هو السبب الذي من أجله يتعرف المفتاح مطلب على اسم المستخدم الحقيقي. هذا السلوك متوافق مع RFC. من القسم [3. 0](#) الخاص[ب RFC3579](#):

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

في الحزمة الأخيرة من جلسة مصادقة 802.1x، يرجع ISE رسالة قبول RADIUS **جوز cisco-av** مع **EAP-Key-Name**:

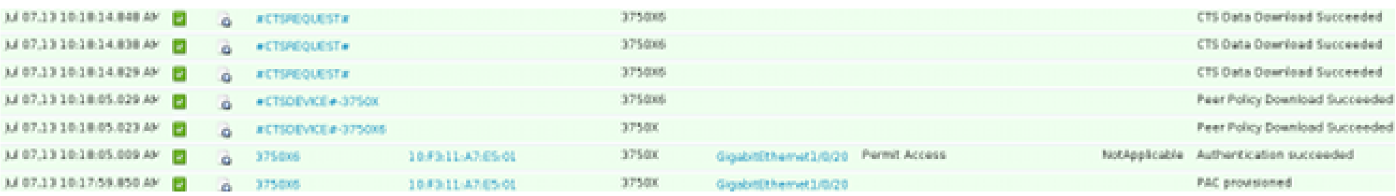


يتم إستخدام هذا كمادة أساسية للمفاوضات SAP.

مع سمتلم من رورم ةكرح تامالع يضع حاتفم قدصملا نأ ينعي اذه .بيقرلا زواجت مت امك **قيمة افتراضية = 0**. يمكنك تكوين قيمة محددة على ISE لإرجاع أي قيمة أخرى. يطبق هذا فقط لحركة مرور untagged، حركة مرور tagged ال تتم إعادة كتابتها لأن، افتراضيا، المصدق مفتاح يثق الحركة مرور من ال يصدق مطلب (غير أن هذا يستطيع أيضا كنت غيرت على ال ISE).

تنزيل سياسة SGA

هناك مبادالت إضافية عبر بروتوكول RADIUS (بدون EAP) بخالف الجلستين الأوليين ل 802.1x EAP-FAST (الأولى لتوفير مسوغ الوصول المحمي (PAC) والثانية للمصادقة). انه سجالت ISE مرة أخرى:



ويشير السجل الثالث (**تنزيل سياسة النظير**) إلى عملية تبادل بسيطة ل RADIUS: طلب

RADIUS وقبول RADIUS للمستخدم **3760x6**. هذا مطلوب لتنزيل سياسات حركة مرور البيانات من مقدم الطلب. أهم سمتين:

```
AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

بسبب هذا، المصدق مفتاح يثق حركة مرور أن يكون SGT-tagged بصاحب المطالبة (**cts:trusted-device=true**)، وأيضا يميز حركة مرور untagged مع **بطاقة=0**.

ويشير السجل الرابع إلى تبادل RADIUS نفسه. ومع ذلك، هذه المرة، فإنها خاصة بالمستخدم **3750X5** (المصدق). وذلك لأن كل النظيرين يجب ان يكون لديهما سياسة لبعضهما البعض. من المثير للاهتمام أن تلاحظ أن الطالب ال يزال ال يعرف عنوان IP الخاص بخادم AAA. هذا هو السبب في أن محول المصدق يقوم بتنزيل السياسة نيابة عن الطالب. يتم تمرير هذه المعلومات الحقا إلى الطالب (بالإضافة إلى عنوان ISE IP) في تفاوض SAP.

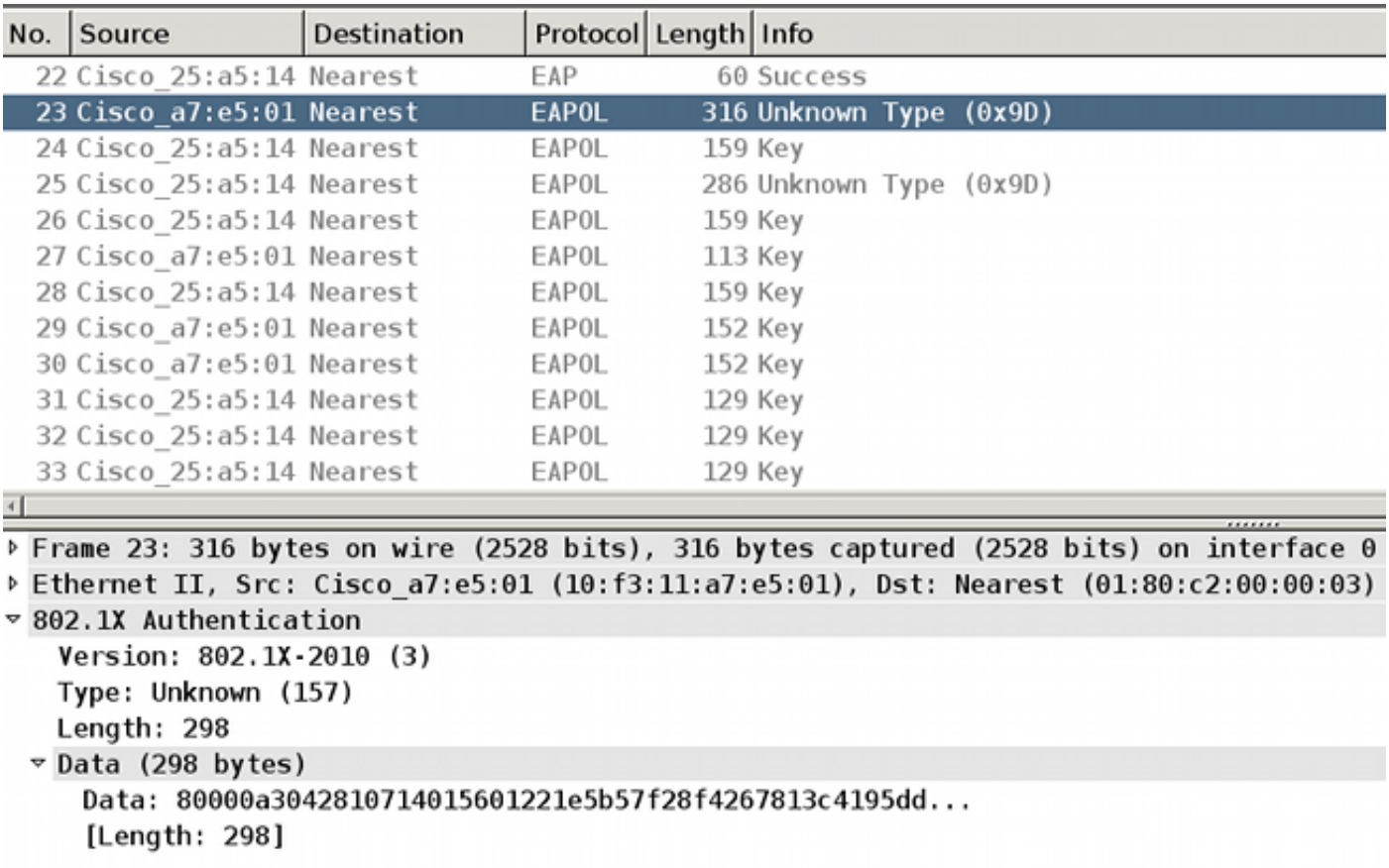
تفاوض SAP

بعد انتهاء جلسة مصادقة 802.1x مباشرة، يحدث تفاوض SAP. هذا التفاوض مطلوب من أجل:

- تفاوض مستويات التشفير (باستخدام الأمر **sap mode-list gcm-encrypt**) ومجموعات التشفير
- اشتقاق مفاتيح الجلسة لحركة مرور البيانات
- خضوع العملية إعادة التشكيل
- قم بإجراء فحوصات أمان إضافية وتأكد من تأمين الخطوات السابقة

تم تصميم بروتوكول SAP بواسطة Cisco Systems استنادا إلى مسودة إصدار 802.11i/D6.0. للحصول على تفاصيل، يمكنك طلب الوصول على [بروتوكول ارتباط أمان Cisco TrustSec - البروتوكول الذي يدعم الأمان الموثوق به من Cisco](#) لصفحة [Cisco Nexus 7000](#).

يتوافق تبادل SAP مع معيار 802.1AE. يتم تبادل مفاتيح بروتوكول المصادقة الموسع عبر شبكة LAN (EAPOL) بين الموجه والمصادق من أجل التفاوض على مجموعة تشفير، وتبادل معلمات الأمان، وإدارة المفاتيح. ولسوء الحظ، ليس لدى Wireshark جهاز فك الترميز لجميع أنواع EAP المطلوبة:



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

ويؤدي النجاح في إنجاز هذه المهام إلى إنشاء رابطة أمنية.

على المحول:

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
       authc success:              12
```

```
       authc reject:              1556
       authc failure:             0
       authc no response:         0
       authc logoff:              0
       sap success:               12
       sap fail:                  0
       authz success:             12
       authz fail:                0
       port auth fail:            0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

في المصدق:

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
       Peer ID               : unknown
```

```
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

هنا، يستعمل الميناء الأسلوب **gcm-encrypt**، لذلك هو يعني أن حركة مرور يكون كل من التصديق والتشفير، as well as true sgt-tagged. ال يستخدم أي من الجهازين سياسة تخويل جهاز الشبكة المحددة على ISE، وهو ما يعني أن جميع حركة المرور التي تم استهلالها من الجهاز تستخدم العلامة الافتراضية **0**. كما أن كل المحولين يثقان في الرقباء المتلقاة من النظير (بسبب سمات RADIUS من مرحلة تنزيل سياسة النظير).

تحديث البيئة والسياسة

بعد توصيل كل الجهازين بسحابة CTS، يتم بدء تحديث البيئة والسياسة. يلزم تحديث البيئة للحصول على الرقباء والأسماء، كما يلزم تحديث السياسة لتنزيل قائمة التحكم في الوصول الخاصة بالمنفذ (SGACL) المعرفة على ISE.

في هذه المرحلة، يكون مقدم الطلب يعرف بالفعل عنوان IP الخاص بخادم AAA، لذلك يمكنه القيام بذلك بنفسه.

ارجع إلى [مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أستكشاف الأخطاء وإصلاحها](#) للحصول على تفاصيل حول البيئة وتحديث السياسة.

يتذكر المفاتح المفاتح ال RADIUS ان دال عنوان، even when هناك ام من RADIUS ان دال يشكل وعندما ال CTS ينقطع خطوة (تجاه المصدق مفاتح). ومع ذلك، من الممكن إجبار المحول على نسيانه:

```
bsns-3750-6#show run | i radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
```

```
radius-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

دخلت in order to دقق البيئة وسياسة على المفتاح طالب، هذا أمر:

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running

bsns-3750-6#show cts role-based permissions
```

لماذا ال ظهر أي سياسات؟ ال ظهر أي نوع، لأنه يجب عليك تمكين **فرض CTS** لتطبيقهم:

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

لماذا يكون للمطالب سياسة واحدة فقط **لتجميع غير معروف** بينما للمصادقة المزيد؟

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

مصادقة المنفذ للعملاء

يتم توصيل عميل MS Windows بمصادقة على منفذ **g1/0/1** الخاص بالمحول 3750-5:

```
bsns-3750-5#show authentication sessions int g1/0/1
       Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                 SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

هنا، يعرف المفتاح 3750-5 أن حركة مرور من أن مضيف ينبغي كنت حددت مع **رقيب=3** عندما أرسلت إلى ال CTS سحابة.

تعليم حركة المرور مع الرقيب

كيف يمكنك شم حركة المرور والتحقق منها؟

اذه بعص نأل:

- متي دعم طاقتلا مزحلا نمضم طقف ةكرحل رورم IP (اذهو راطإ تنرثيإ دعم لدعم عم ةلومح SGT و MACsec).
- يحو للحم رسيأ (ةحسف نيب نيتماعد) ءانيم عم **لثامتملا خسنلا** ةلمكلا حاتفملا - اذه نكمأ لمعت، ريغ نأ ةلكشملا نأ يأ pc عم Wireshark طبري ىلإ ةياغلا ءانيم نم monitore ةسلج طقسي تاراطإلا ببسب قاقتفالا ىلإ دعم 802.1ae، يأ عيطتسي عقوت ىلع زاهجلا.
- ةحسف نيب نيتماعد ءانيم نود **لثامتملا خسنلا** ليزي ةلمكلا حاتفملا **cts** سأر لبق نأ عضي ىلع ةياغ ءانيم.

SGACL عم ةسايسلا ذيفنت

متي ذيفنت ةسايسلا يف ةباحس CTS امئاد يف ذفنم ةهجولا. كلذو نأل زاهجلا ريخألا طقف وه يذلا يعرف بيقر ةهجولا زاهجل ةطقن ةياهنلا لصتملا ةرشابم كلذب لوحملا. ةمزحلا لمحت طقف بيقرلا ردصملا. نيعتي ىلع بيقرلا لوؤسملا نع رادصإو ةهجولا ذاختإ رارقلا.

وه اذهو ببسلا يف نأ يأ ةزهجألا ال جاتحت ىلإ ليزنت عيمج تاسايسلا نم ISE. وبدلا نم كلذ، مهنإف نوجاتحي طقف ىلإ ءزج نم ةسايسلا قلعتملا بيقرلاب يذلاو يمتني كلذ زاهجلا نم لجأ ةزهجأ ةلصتم ةرشابم.

انه لا 3750-6، وهو حاتفملا كرتشملا:

```
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

كانه ناتسايس انه. لوألا وه صيقتلا ريصقت ةكرحل رورملا نودب تامالع زييمت (ىلإ/نم). يناثلا وه نم **2 بيقرلا** ىلإ بيقرلا يذلا ال لمحي ةمالع زييمت، وهو **0**. اذه جهنلا موجوم دوجو نأل زاهجلا هسفن مدختسي ةسايس SGA نم ISE، وهو يمتني ىلإ **SGT=0**. اضيأ، **0=بيقرلا** وه ةمالع ةيضارتفا. كلذل، بجي كيلع ليزنت عيمج تاسايسلا يتلا اهيدل دعاوق ةكرحل رورملا **نم/ىلإ SGT=0**. اذإ ترظن ىلإ ةفوفصملا، نورتس ةسايس ةدحاو طقف لثم: **نم 2 ىلإ 0**.

انه لا 3750-5، يأ نوكي قدصملا حاتفم:

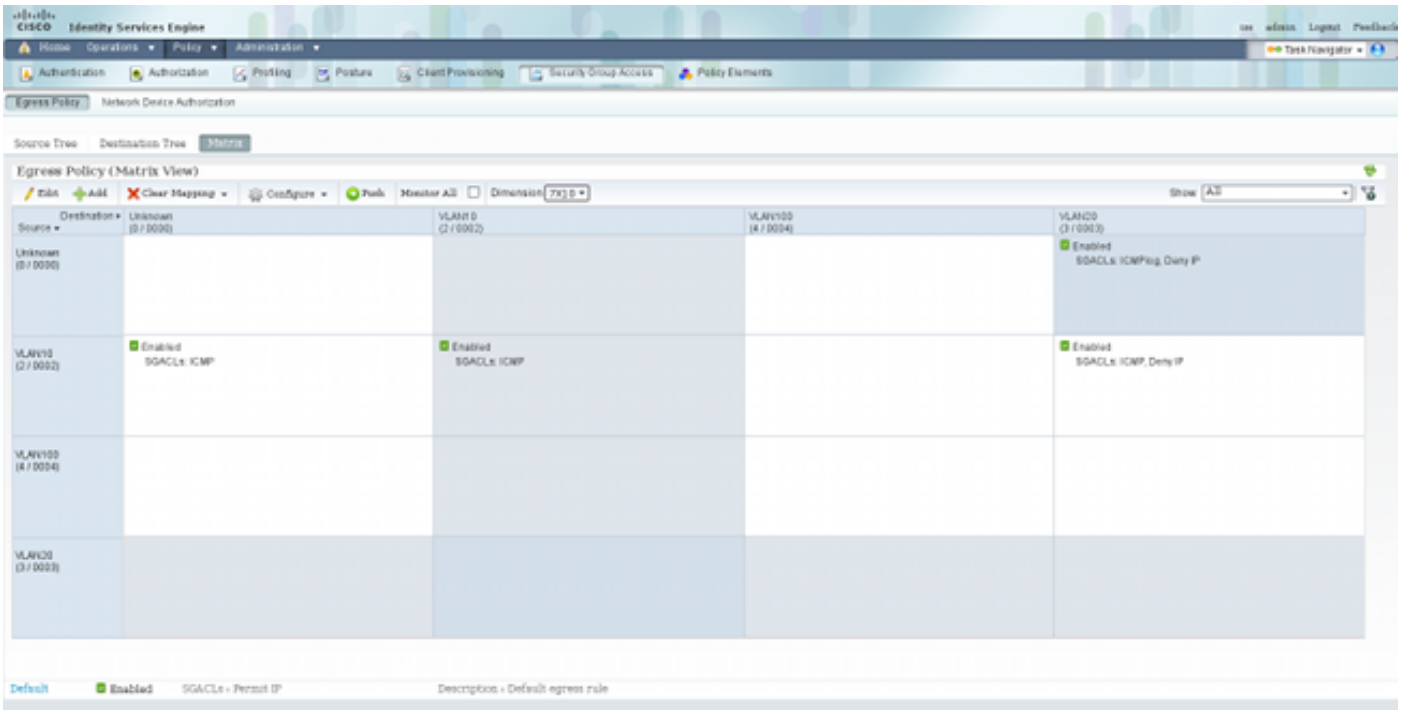
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

كانهو ةسايس ىرخأ انه: **نم 2 ىلإ 3**. كلذو نأل ليمع 802.1x (MS Windows) لصتم **ليجلاب 1/0/1** متو هزييمت **3=بيقرلاب**. اذهل ببسلا بجي كيلع ليزنت عيمج تاسايسلا **ىلإ SGT=3**.

لواح رابتخإ لاصتالا نم 3750x-6 (**0=بيقرلا**) ىلإ MS Windows XP (**3=بيقرلا**). لا 3750X-5 وه ةادأ نيتماعد نيب ةحسفلا.

لبق اذه، بجي كيلع نيوكت ةسايس ىلع رايعم ISE ةكرحل رورملا نم **0=بيقرلا ىلإ**

الرقيب=3. قام هذا المثال بإنشاء سجل SGACL لبروتوكول رسائل التحكم في الإنترنت (ICMP) باستخدام الخط فقط، **والسماح بسجل ICMP**، واستخدمه في المصفوفة لحركة المرور من **SGT=0 إلى SGT=3**:



فيما يلي تحديث للسياسة على المحول للإنفاذ، والتحقق من السياسة الجديدة:

```
bsns-3750-5#cts refresh policy
Policy refresh in progress

bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

للتحقق من تنزيل قائمة التحكم في الوصول (ACL) من ISE، أدخل هذا الأمر:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

للتحقق من تطبيق قائمة التحكم في الوصول (ACL) (دعم الأجهزة)، أدخل هذا الأمر:

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name    = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
 flag    = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale   = FALSE
```

```
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

فيما يلي العدادات قبل ICMP:

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

فيما يلي إختبار اتصال من **الرقيب=0** (موجه 3750-6) إلى نظام التشغيل MS Windows XP والعدادات (**الرقيب=3**):

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

فيما يلي عدادات قائمة التحكم في الوصول (ACL):

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
    10 permit icmp log (5 matches)
```

التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- دليل تكوين Cisco TrustSec لـ 3750
- دليل تكوين Cisco TrustSec لـ ASA 9.1
- نشر Cisco TrustSec وخريطة الطريق
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).