مثال تكوين Catalyst 3750X Series Switch و ASA TrustSec دليل أستكشاف الأخطاء وإصلاحها

المحتويات

المقدمة

تصف هذه المقالة كيفية تكوين Cisco TrustSec (CTS) على جهاز الأمان القابل للتكيف (ASA) من Cisco ومحول Cisco Catalyst 3750X Series Switch (3750X).

لتعلم التخطيط بين علامات مجموعة الأمان (SGTs) وعناوين IP، يستخدم ASA بروتوكول تبادل الرقيب (SXP). ثم يتم إستخدام قوائم التحكم في الوصول (ACL) القائمة على الرقيب لتصفية حركة المرور. يقوم الطراز 3750X

بتنزيلات سياسات قائمة التحكم في الوصول (RBACL) المستندة إلى الأدوار من محرك خدمات الهوية (ISE) من Cisco وحركة مرور عوامل التصفية المستندة إلى هذه السياسات. تعرض هذه المقالة تفاصيل مستوى الحزمة لوصف كيفية عمل الاتصال وتصحيح الأخطاء المتوقعة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- مكونات CTS
- CLI تشكيل من ASA و cisco IOS®

المكونات المستخدمة

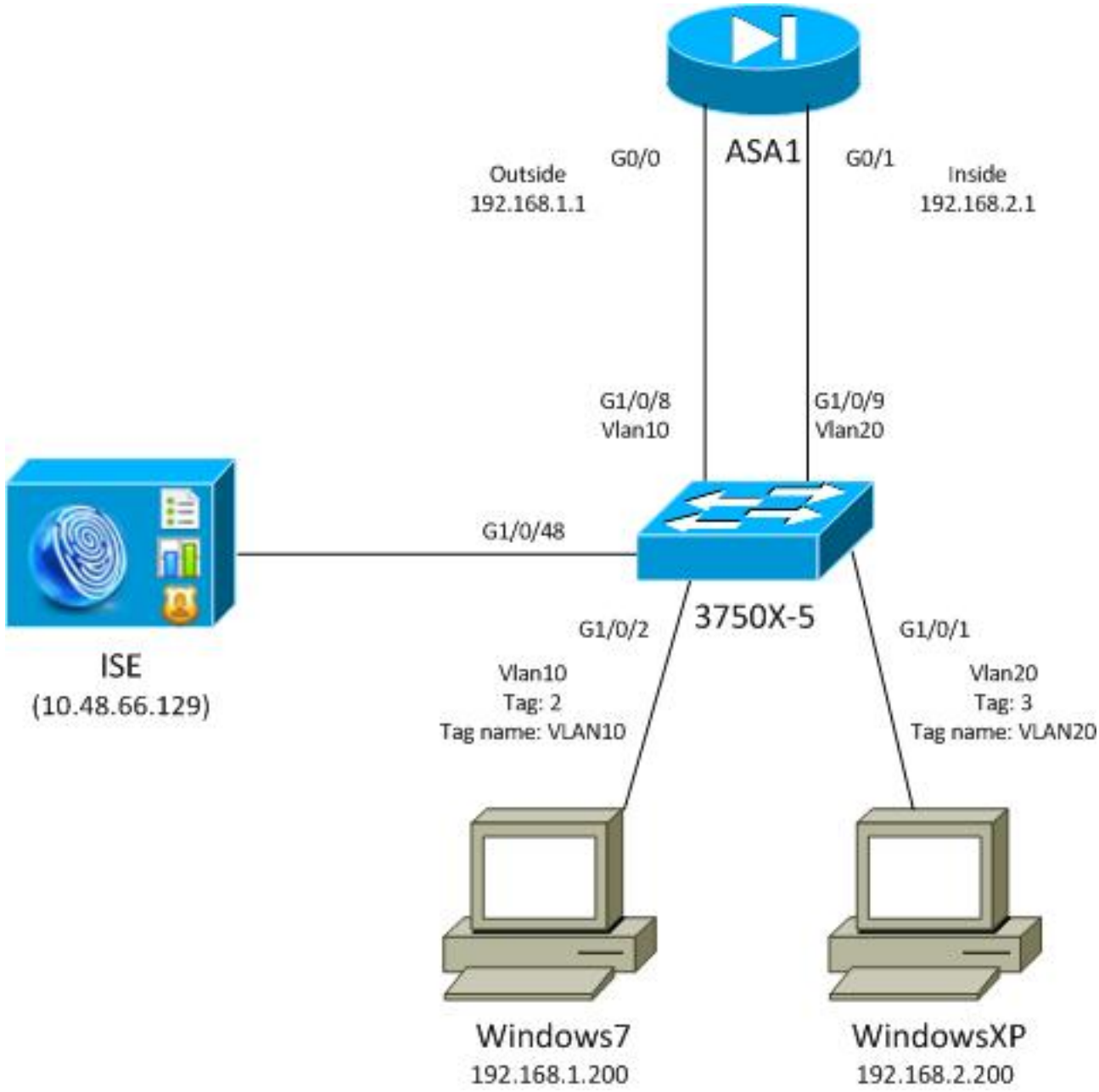
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج Cisco ASA، الإصدارات 9.1 والإصدارات الأحدث
- Microsoft (MS) Windows 7 و MS Windows XP
- برنامج Cisco 3750X، الإصدارات 15.0 والإصدارات الأحدث
- برنامج Cisco 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



تدفق حركة المرور

هنا تدفق حركة المرور:

- يتم تكوين المحول 3750X على **G1/0/1** و**G1/0/2** لمصادقة المنفذ.
- يتم إستخدام ISE كخادم المصادقة والتفويض والمحاسبة (AAA).
- يتم إستخدام تجاوز عنوان MAC (MAB) للمصادقة على نظام التشغيل MS Windows 7.
- يتم إستخدام IEEE 802.1x لنظام التشغيل MS Windows XP لتوضيح عدم أهمية طريقة المصادقة المستخدمة.

وبعد مصادقة ناجحة، يقوم ISE بإرجاع الرقيب ويربط 3750X هذه العلامة بجلسة المصادقة. كما يعلم المحول عناوين IP الخاصة بكلتا المحطات باستخدام الأمر **ip device tracking**. ثم يستخدم المحول SXP لإرسال جدول التعيين بين الرقيب وعنوان IP إلى ASA. يحتوي كلا جهازي MS Windows على توجيه افتراضي يشير إلى ASA.

بعد أن يتلقى ال ASA حركة مرور من عنوان IP الذي تم تعيينه إلى الرقيب، فإنه قادر على إستخدام قائمة التحكم بالوصول (ACL) استنادا إلى الرقيب. أيضا، عند إستخدام 3750X كموجه (البوابة الافتراضية لكل من محطتي MS Windows)، فإنه قادر على تصفية حركة المرور استنادا إلى السياسات التي تم تنزيلها من ISE.

فيما يلي خطوات التكوين والتحقق، والتي يتم توضيح كل منها في القسم الخاص بها لاحقا في المستند:

- مصادقة المنفذ باستخدام الأمر **ip device tracking** على الطراز 3750X
- تكوين ISE للمصادقة و SGT وسياسات قائمة التحكم في الوصول إلى مجموعة الأمان (SGACL)
- تكوين CTS على ASA و 3750X
- إمداد مسوغات الوصول المحمي (PAC) على 3750X (تلقائي) و ASA (يدوي)
- تحديث البيئة على محولات ASA و 3750X
- التحقق من مصادقة المنفذ وتطبيقها على الطراز 3750X
- تحديث النهج على الطراز 3750X
- تبادل SXP (تنسيق ASA كمستمع و 3750X كمكبر صوت)
- تصفية حركة المرور على ASA مع ACL للرقيب
- تصفية حركة المرور على الطراز 3750X مع السياسات التي تم تنزيلها من ISE

التكوينات

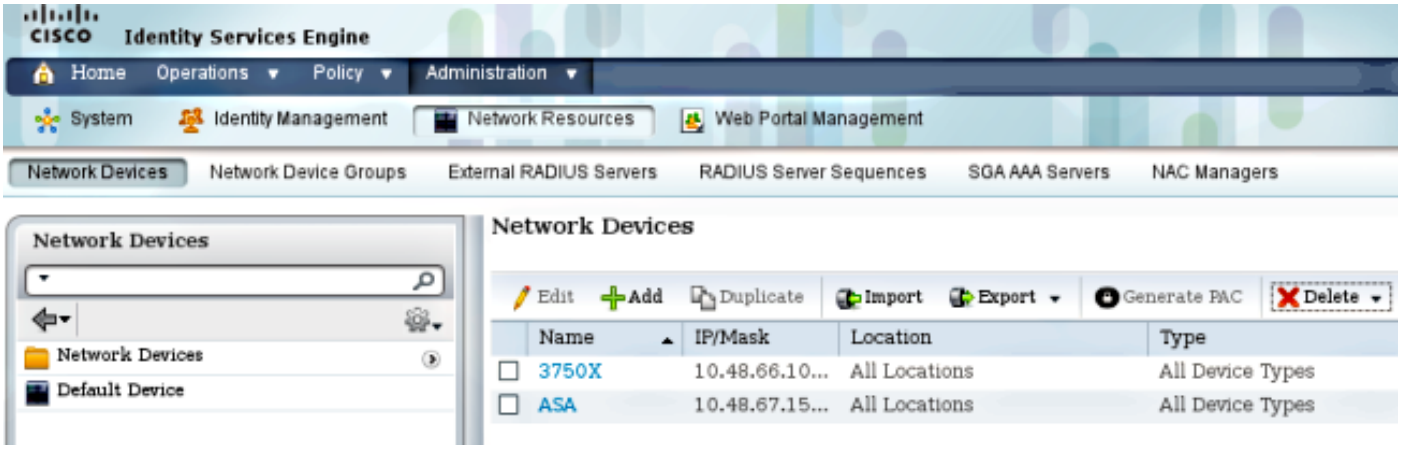
مصادقة المنفذ باستخدام الأمر *ip device tracking* على الطراز 3750X

هذا هو التكوين النموذجي ل 802.1x أو MAB. يلزم تغيير تفويض RADIUS (CoA) فقط عند إستخدام إعلام نشط من ISE.

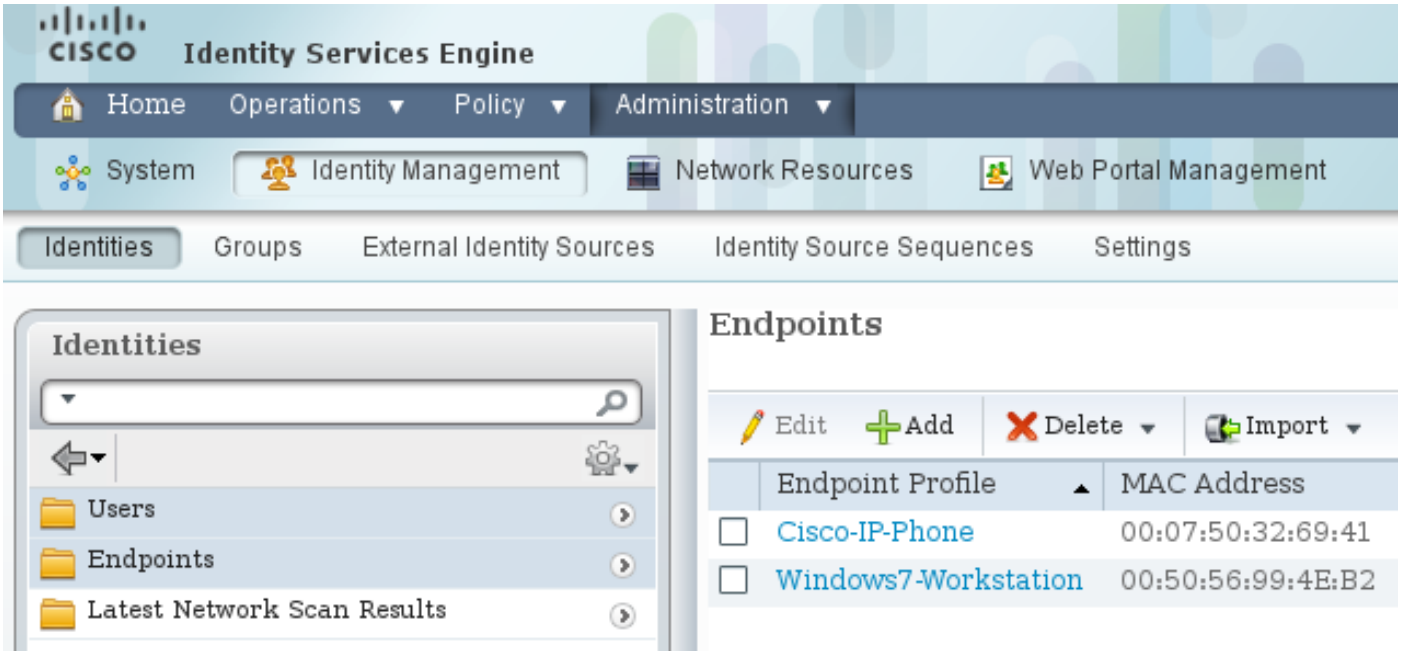
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

Radius COA!
aaa server radius dynamic-author
client 10.48.66.129 server-key cisco
server-key cisco

ip device tracking

interface GigabitEthernet1/0/1
description windowsxp
switchport mode access
authentication order mab dot1x
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast
!
interface GigabitEthernet1/0/2
description windows7
switchport mode access
authentication order mab dot1x
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast

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
```

تكوين ISE لسياسات المصادقة و SGT و SGACL

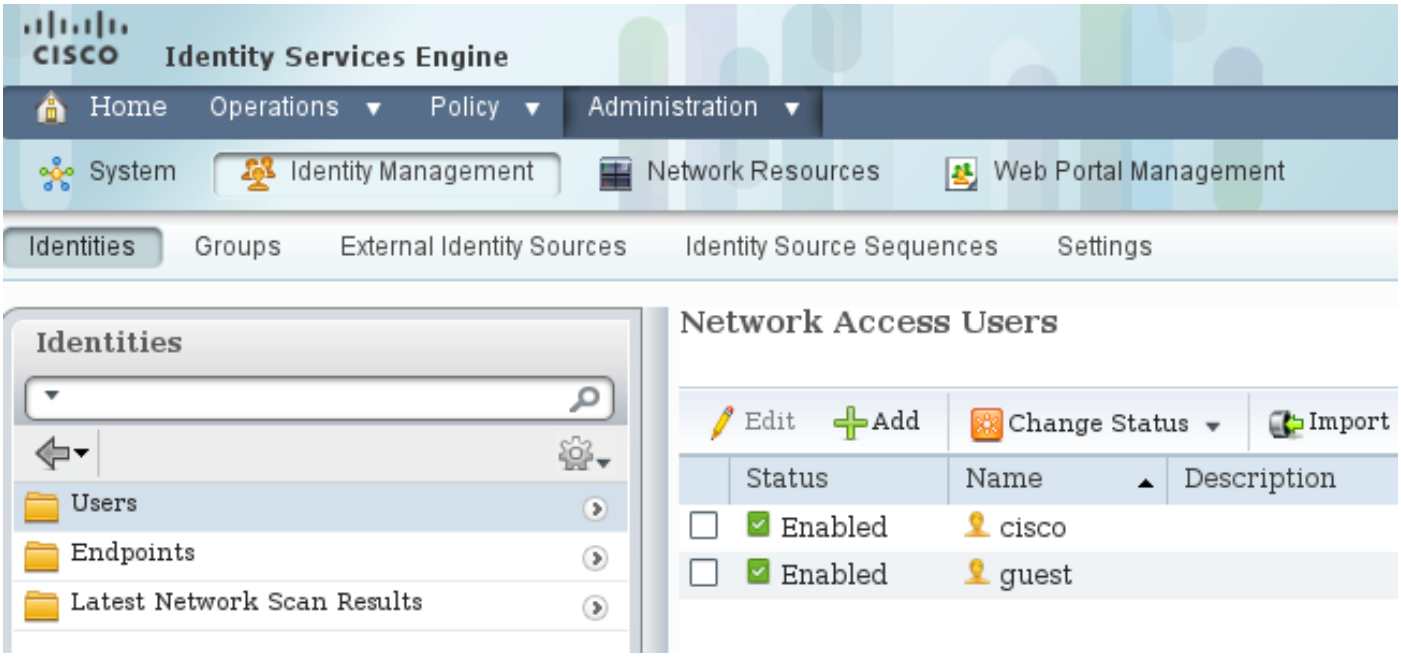
يجب أن يحتوي ISE على كلا جهازي الشبكة اللذين تم تكوينهما تحت **الإدارة > أجهزة الشبكة**:



بالنسبة لنظام MS Windows 7، والذي يستخدم مصادقة MAB، يجب إنشاء هوية نقطة النهاية (عنوان MAC) تحت **إدارة > إدارة الهوية > الهويات > نقاط النهاية**:

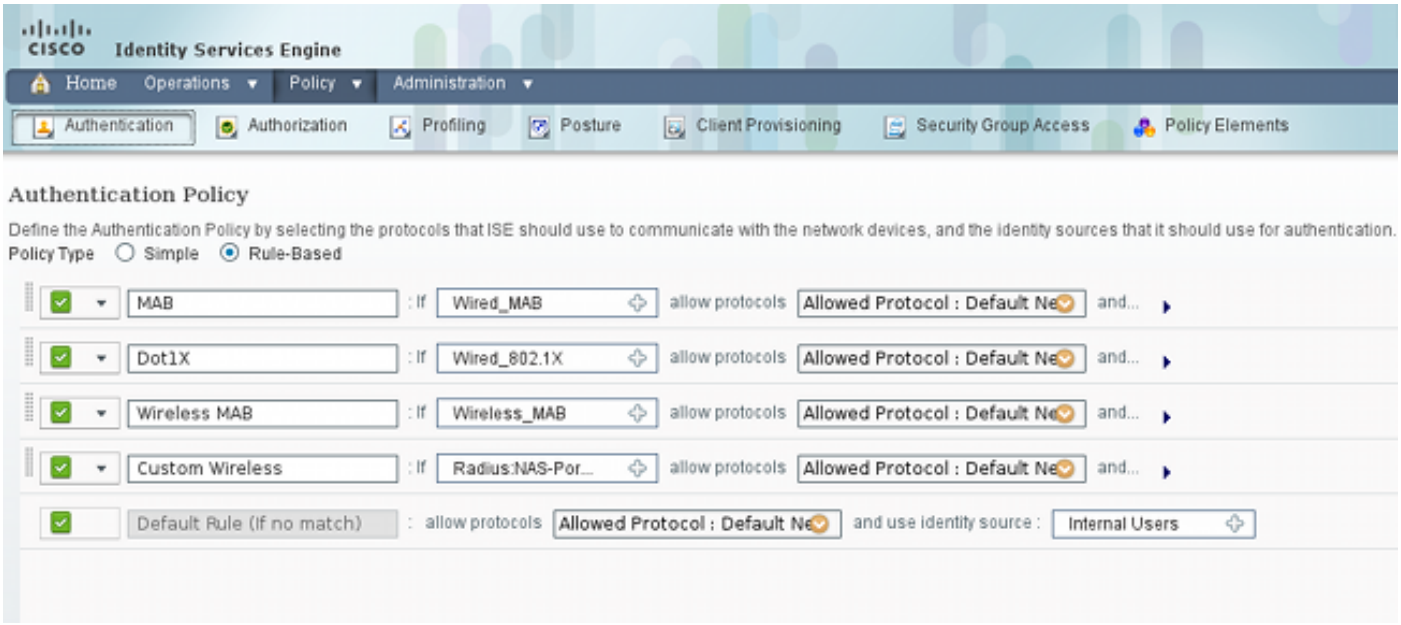


بالنسبة لنظام MS Windows XP، الذي يستخدم مصادقة 802. 1x، يجب عليك إنشاء هوية مستخدم (اسم مستخدم) تحت **إدارة > إدارة الهوية > الهويات > المستخدمون**:

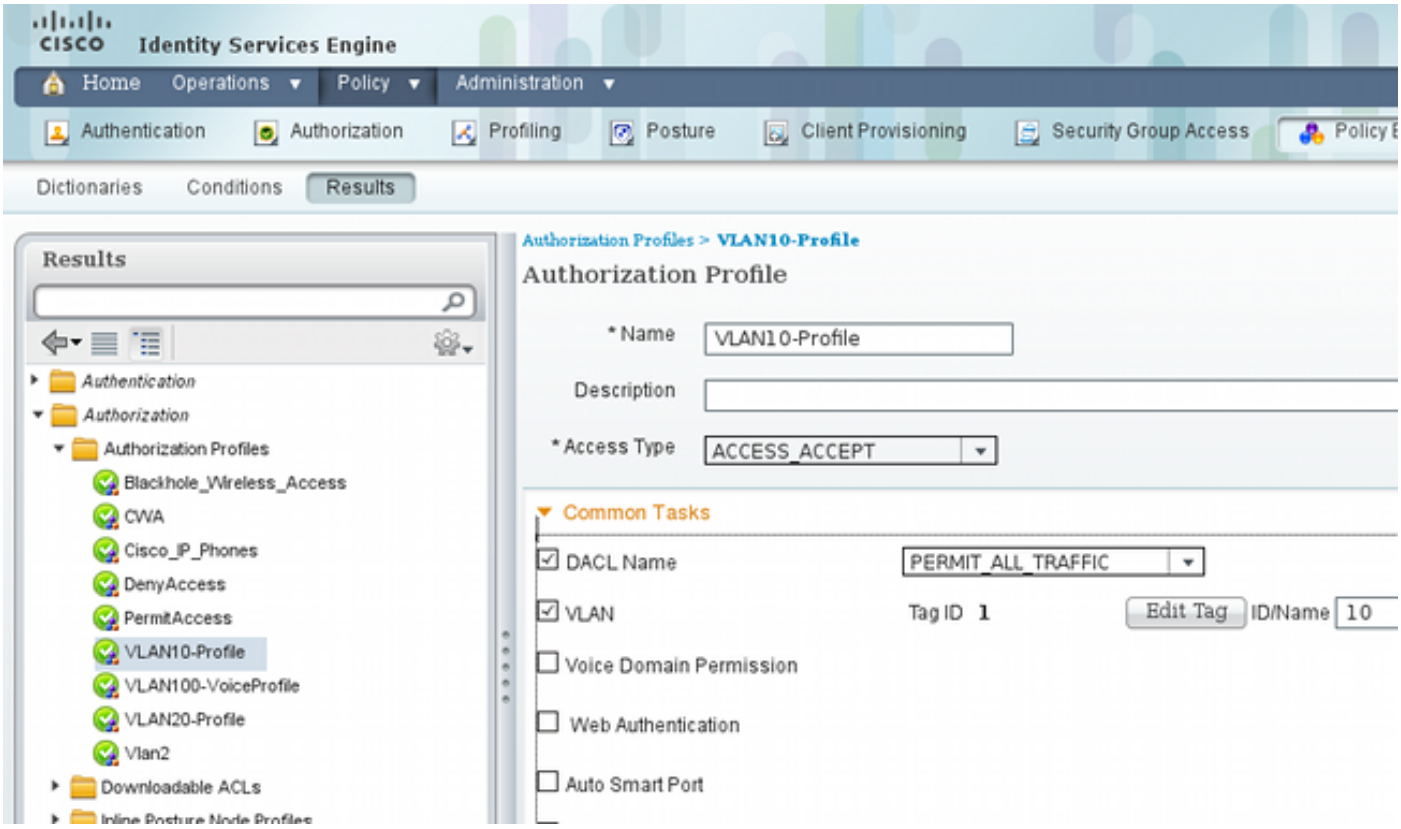


استعملت ال **username cisco** . قم بتكوين MS Windows XP ل EAP المحمي ببروتوكول المصادقة المتوسع (EAP-PEAP) باستخدام بيانات الاعتماد هذه.

في ISE، يتم إستخدام سياسات المصادقة الافتراضية (لا تغير هذا). الأولى هي سياسة مصادقة MAB، والثانية هي 802.1x:



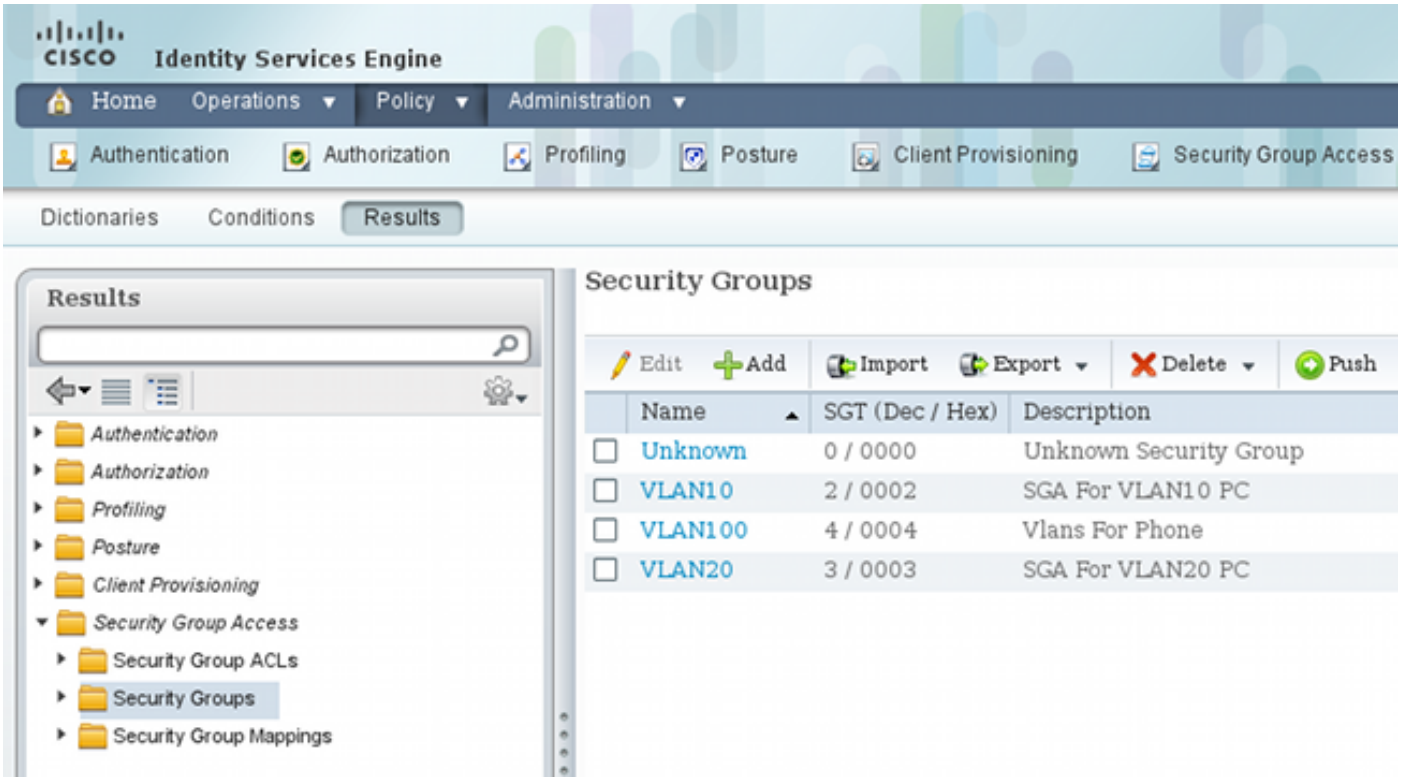
لتكوين سياسات التخويل، يجب عليك تحديد ملفات تعريف التخويل ضمن **نهج > نتائج > تخويل > ملفات تعريف التخويل**. يتم إستخدام ملف تعريف VLAN10 مع قائمة التحكم في الوصول (DACL) القابلة للتنزيل، والذي يسمح بجميع حركات المرور، لملف تعريف MS Windows 7:



يتم إستخدام تكوين مماثل، VLAN20-Profile، ل MS Windows XP مع إستثناء رقم شبكة 20) VLAN).

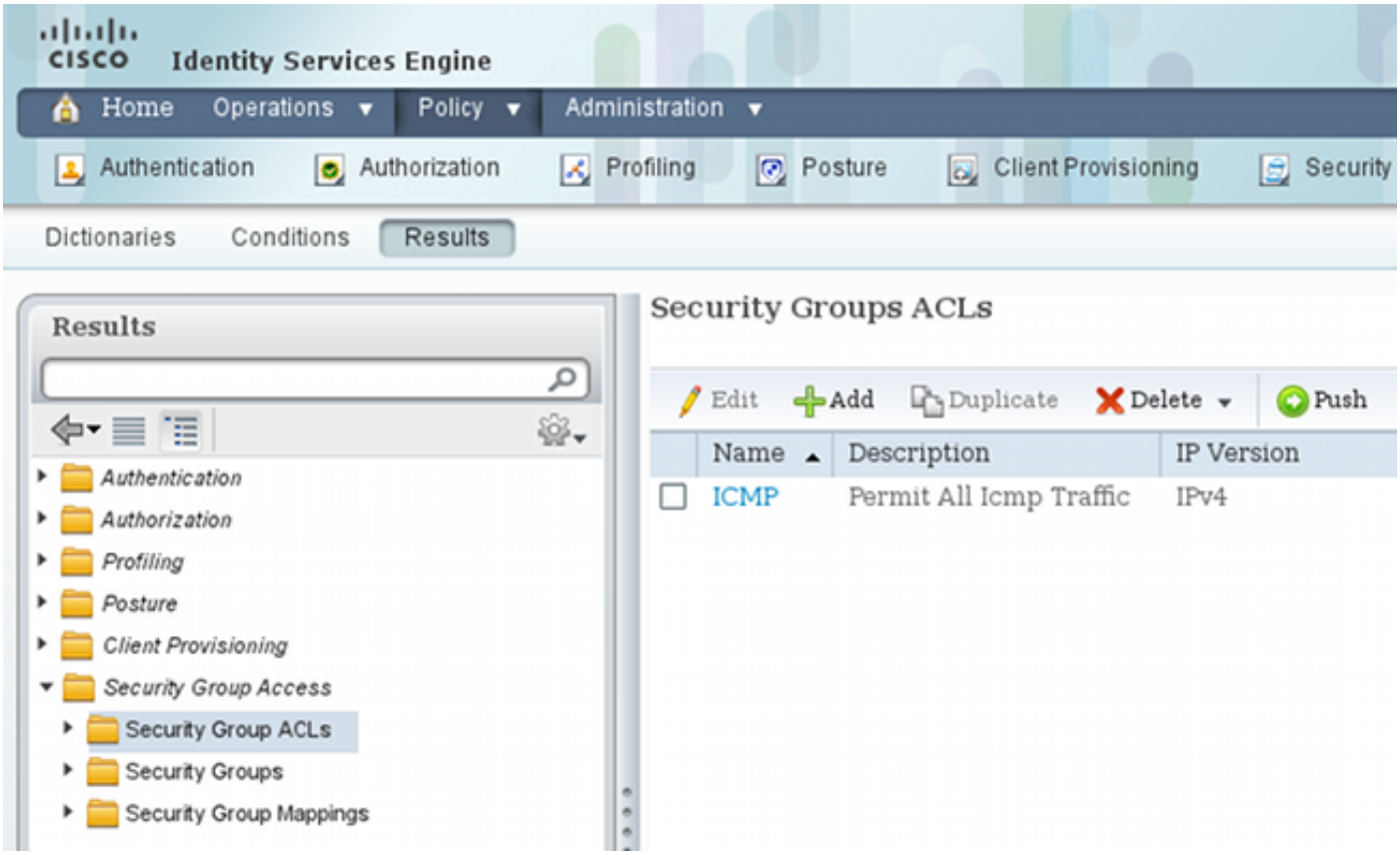
in order to شكلت ال SGT مجموعة (علامات) على ISE، انتقل إلى **سياسة > نتائج>تأمين وصول مجموعة>أمن مجموعات**.

ملاحظة: لا يمكن إختيار رقم علامة تمييز، بل يتم تحديده تلقائيا بواسطة أول رقم حر باستثناء 1. يمكنك تكوين اسم الرقيب فقط.

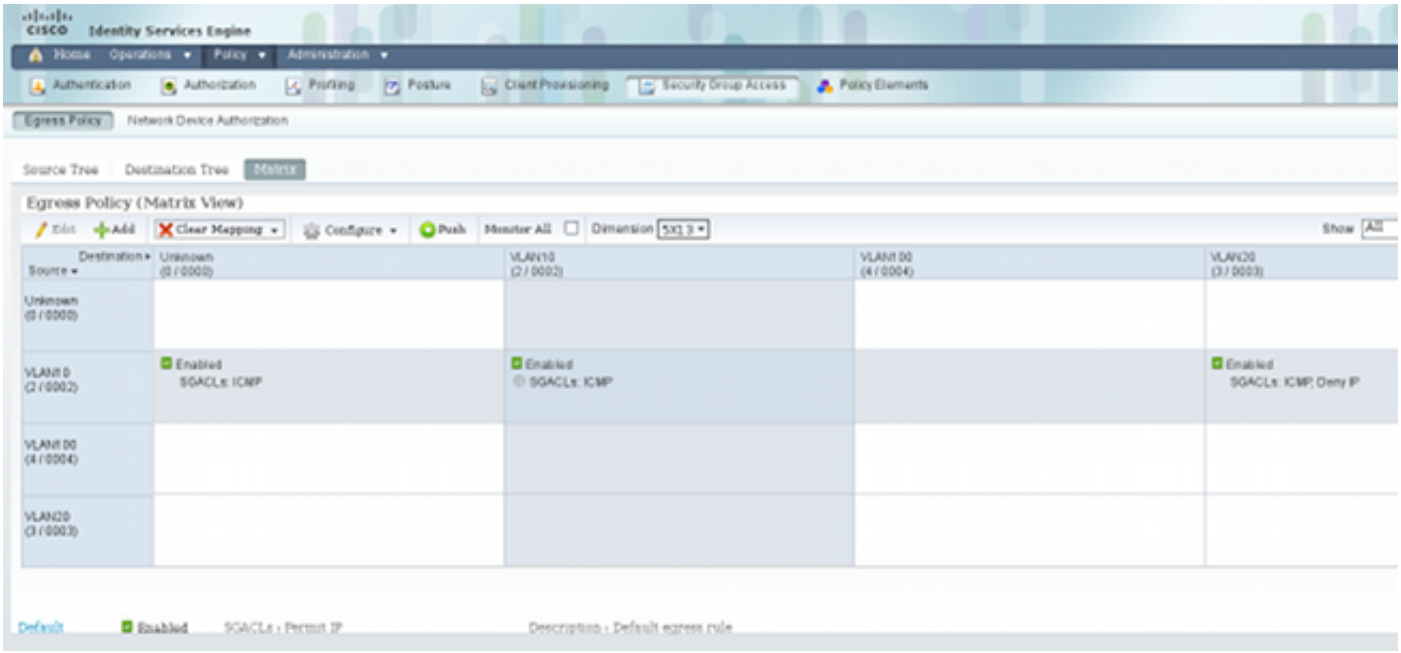


من أجل إنشاء SGACL للسماح بحركة مرور بروتوكول رسائل التحكم في الإنترنت (ICMP)، انتقل إلى **السياسة >**

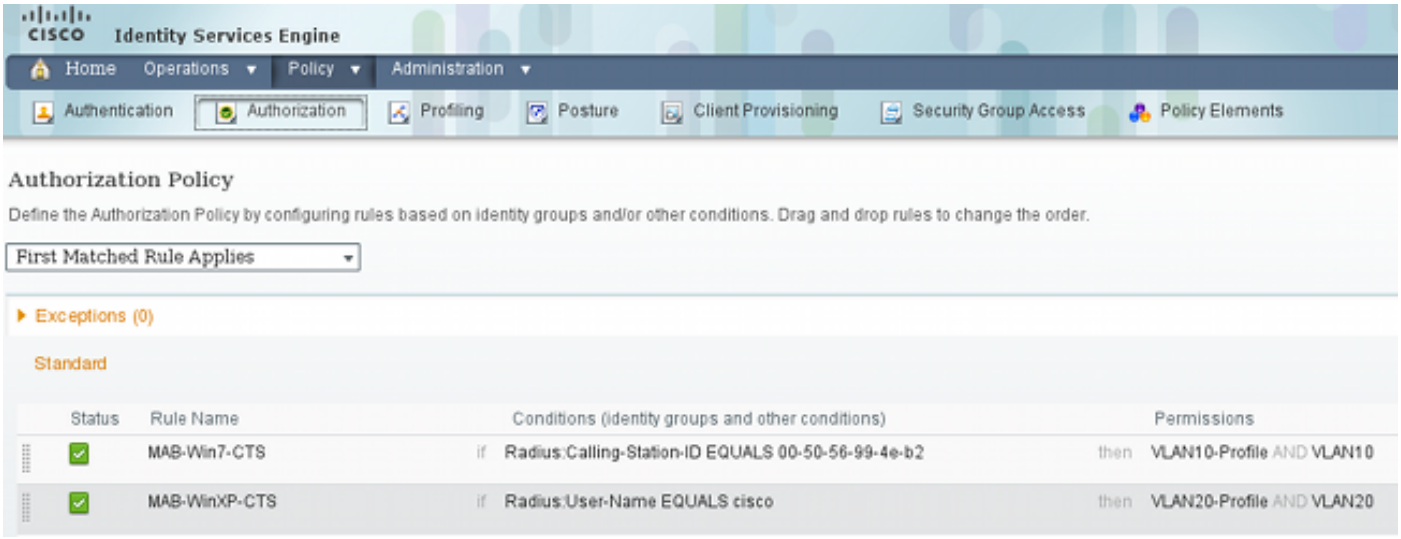
النتائج > وصول مجموعة الأمان > قوائم التحكم في الوصول لمجموعة الأمان:



لإنشاء سياسات، انتقل إلى **سياسة > وصول مجموعة الأمان > سياسة الخروج**. بالنسبة لحركة المرور بين شبكة VLAN10 وشبكة VLAN أو VLAN10 أو VLAN20 غير المعروفة، يتم إستخدام قائمة التحكم في الوصول (**السماح ب ICMP**):



لتعيين قواعد التخويل، انتقل إلى **نهج > تخويل**. بالنسبة لنظام التشغيل MS Windows 7 (عنوان MAC محدد)، يتم إستخدام **شبكة** VLAN10-profile، مع إرجاع شبكة VLAN10 وشبكة DACL، وشبكة VLAN10 الخاصة بملف تعريف الأمان مع الرقيب المسمى **VLAN10**. بالنسبة ل MS Windows XP (اسم مستخدم محدد)، يتم إستخدام **شبكة VLAN20-profile**، مع إرجاع شبكة VLAN رقم 20 وشبكة DACL، وشبكة VLAN20 الخاصة بملف تعريف الأمان مع الرقيب المسمى **VLAN20**.



قم بإنهاء تكوين المحول و ASA ليقبلوا سمات RADIUS الخاصة بالرقيب.

تكوين CTS على ASA و 3750X

يجب تكوين إعدادات CTS الأساسية. في الطراز 3750X، يجب عليك الإشارة إلى نهج الخادم التي يجب تنزيلها من خلالها:

```
aaa authorization network ise group radius
cts authorization list ise
```

على ASA، يلزم فقط خادم AAA مع CTS الذي يشير إلى ذلك الخادم:

```
aaa-server ISE protocol radius
aaa-server ISE (mgmt) host 10.48.66.129
***** key
cts server-group ISE
```

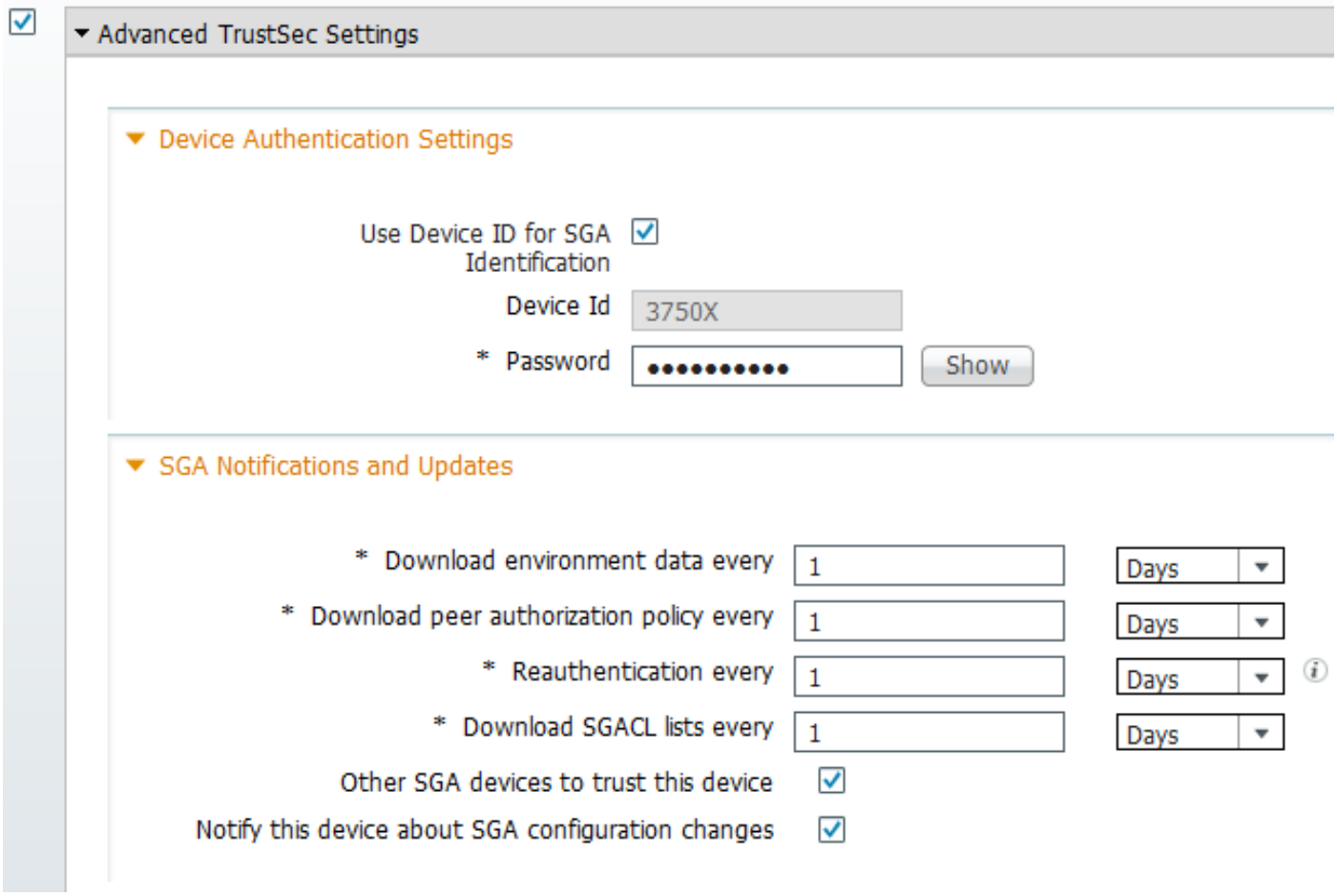
ملاحظة: في الطراز 3750X، يجب عليك الإشارة بشكل صريح إلى خادم ISE باستخدام الأمر **group radius**. وذلك لأن الطراز 3750X يستخدم توفير مسوغات الوصول المحمي (PAC) تلقائيا.

إمداد مسوغات الوصول المحمي (PAC) على 3750X (تلقائي) و ASA (يدوي)

يجب أن يصادق كل جهاز في سحابة CTS إلى خادم المصادقة (ISE) حتى يمكن الوثوق به بواسطة أجهزة أخرى. وهو يستخدم أسلوب المصادقة المتوسع-المرن لبروتوكول المصادقة من خلال البروتوكول الآمن ((EAP-FAST RFC 4851)) لهذا الغرض. تتطلب هذه الطريقة أن يتم تسليم مسوغ الوصول المحمي (PAC) خارج النطاق. يسمى هذا عملية أيضا **phase0**، ولا يعرف في أي RFC. PAC ل EAP-FAST له دور مماثل لشهادة تأمين طبقة النقل-بروتوكول المصادقة المتوسع (EAP-TLS). يتم إستخدام مسوغ الوصول المحمي (PAC) لإنشاء نفق آمن (المرحلة 1)، وهو مطلوب للمصادقة في المرحلة 2.

إعداد PAC على الطراز 3750X

يدعم الطراز 3750X توفير مسوغات الوصول المحمي (PAC) تلقائيا. يتم إستخدام كلمة مرور مشتركة على المحول و ISE لتنزيل PAC. أن كلمة السر ومعرف ينبغي كنت شكلت على ال ISE تحت **إدارة > شبكة مورد > شبكة أداة**. حدد المحول، ثم قم بتوسيع قسم **إعدادات TrustSec المتقدمة** من أجل التكوين:



دخلت in order to جعلت PAC يستعمل هذا ورقة اعتماد، هذا أمر:

```
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: 08:04:40 UTC Sep 25 2013
PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC59784000600940003
010094F559DAE0C837D7847F2454CAD7E80B0000001351C8235900093A803D7D427BFB5C6F0FBBDF
7EDF0818C58FECF97F8BDECF1B115FB0240260ADA8C96A46AA2A64C9EA2DB51E0E886768CA2D133D
2468D9D33339204BAA7E4CA2DE8E37FF1EB5BCB343408E9847998E301C26DDC6F91711F631A5B4C7
C2CB09EAB028630A3B22901FE3EF44F66FD019D09D2C46D92283
Refresh timer is set for 2y24w
```

إعداد PAC على ASA

لا يدعم ASA إلا توفير PAC اليدوي. هذا يعني أنه يجب عليك إنشاؤها يدويا على ISE (في أجهزة الشبكة/ASA):

بعد ذلك يجب تثبيت الملف (على سبيل المثال، مع FTP):

```
bsns-asa5510-17(config)# cts import-pac ftp://ftp:ftp@10.147.25.80/ASA.pac
password ciscocisco
PAC Imported Successfully!

bsns-asa5510-17(config)# show cts pac

PAC-Info:
  Valid until: Jul 04 2014 13:33:02
  AID:         c40a15a339286ceac28a50dbbac59784
  I-ID:        ASA
  A-ID-Info:   Identity Services Engine
  PAC-type:    Cisco Trustsec
PAC-Opaque:
  000200a80003000100040010c40a15a339286ceac28a50dbbac597840006008c000301
  0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
  e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
  c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
  7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

تحديث البيئة على ASA و 3750X

في هذه المرحلة، تم تثبيت مسوغ الوصول المحمي (PAC) على كلا الجهازين بشكل صحيح وبدء تنزيل بيانات بيئة ISE تلقائيا. هذه البيانات هي أساسا أرقام العلامات وأسمائها. دخلت in order to أطلقت بيئة تحديث على ال ASA، هذا أمر:

```
bsns-asa5510-17# cts refresh environment-data
```

للتحقق من ذلك على ASA (لسوء الحظ لا يمكنك رؤية علامات/أسماء SGT المحددة، ولكن يتم التحقق منها لاحقا)، أدخل هذا الأمر:

```
bsns-asa5510-17(config)# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          05:05:16 UTC Apr 14 2007
(Env-data expires in:      0:23:56:15 (dd:hr:mm:sec
(Env-data refreshes in:    0:23:46:15 (dd:hr:mm:sec
```

للتحقق من ذلك على 3750X، قم بتشغيل تحديث البيئة باستخدام هذا الأمر:

```
bsns-3750-5#cts refresh environment-data
```

دخلت in order to دققت النتيجة، هذا أمر:

```
bsns-3750-5#show cts environment-data
                                CTS Environment Data
                                ====================
                              Current state = COMPLETE
                              Last status = Successful
                                     :Local Device SGT
                               SGT tag = 0-01:Unknown
                                     :Server List Info
                          :(Installed list: CTSServerList1-0001, 1 server(s
Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784*
                                  (Status = ALIVE    flag(0x11
 ,auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins
                                                  deadtime = 20 secs
                                        :Security Group Name Table
                                                       : 0001-60
                                                  Unknown:0-47
                                                   VLAN10:2-47
                                                   VLAN20:3-47
                                                  VLAN100:4-47
                                    Transport type = CTS_TRANSPORT_IP_UDP
                                   Environment Data Lifetime = 86400 secs
                                 Last update time = 05:33:49 UTC Thu Apr 7 2011
                                (Env-data expires in   0:16:46:50 (dd:hr:mm:sec
                                (Env-data refreshes in 0:16:46:50 (dd:hr:mm:sec
                                    Cache data applied           = NONE
                                   State Machine is running
```

هذا يظهر أن كل علامات التمييز والأسماء المرادفة يتم تنزيلها بشكل صحيح.

التحقق من مصادقة المنفذ وتطبيقها على الطراز 3750X

بعد أن يحتوي الطراز 3750X على بيانات البيئة، يجب عليك التحقق من تطبيق الرقيبات على الجلسات المصدق عليها.

للتحقق من مصادقة MS Windows 7 بشكل صحيح، أدخل هذا الأمر:

```
bsns-3750-5#show authentication sessions interface g1/0/2
                    Interface:  GigabitEthernet1/0/2
                  MAC Address:  0050.5699.4eb2
                   IP Address:  192.168.1.200
                    User-Name:  00-50-56-99-4E-B2
                       Status:  Authz Success
                       Domain:  DATA
              Security Policy:  Should Secure
                Security Status:  Unsecure
              Oper host mode:  single-host
                  Oper control dir:  both
           Authorized By:  Authentication Server
                     Vlan Policy:  10
ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                         SGT:  0002-0
                    Session timeout:  N/A
                    Idle timeout:  N/A
        Common Session ID:  C0A800010000001002B67334C
                  Acct Session ID:  0x00000179
                  Handle:  0x94000101
```

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

يوضح الإخراج أنه يتم إستخدام **شبكة VLAN10** مع **الرقيب 0002** و DACL للسماح لجميع حركات المرور.

للتحقق من مصادقة MS Windows XP بشكل صحيح، أدخل هذا الأمر:

```
bsns-3750-5#sh authentication sessions interface 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:  C0A80001000000FE2B67334C
    Acct Session ID:  0x00000177
    Handle:  0x540000FF

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

يوضح الإخراج أنه يتم إستخدام **شبكة VLAN رقم 20** مع **الرقيب 0003** و DACL للسماح لجميع حركات المرور

يتم اكتشاف عناوين IP باستخدام وظيفة **تعقب جهاز IP**. يجب تكوين محول DHCP **للتطفل على بروتوكول DHCP**. بعد ذلك، بعد التطفل على إستجابة DHCP، يتعرف على عنوان IP الخاص بالعميل. بالنسبة لعنوان IP تم تكوينه بشكل ثابت (مثل هذا المثال)، يتم إستخدام وظيفة التطفل على **ARP** ، ويجب أن يرسل الكمبيوتر الشخصي أي حزمة ليتمكن المحول من اكتشاف عنوان IP الخاص به.

بالنسبة **لتعقب الجهاز**، قد يكون هناك حاجة إلى أمر مخفي لتنشيطه على المنافذ:

```
bsns-3750-5#ip device tracking interface g1/0/1
bsns-3750-5#ip device tracking interface g1/0/2
bsns-3750-5#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
-----------------------------------------------------------------------
     IP Address     MAC Address   Vlan  Interface                STATE
-----------------------------------------------------------------------
   0050.5699.4eb2  10   GigabitEthernet1/0/2     ACTIVE   192.168.1.200
   0050.5699.4ea1  20   GigabitEthernet1/0/1     ACTIVE   192.168.2.200

Total number interfaces enabled: 2
:Enabled interfaces
```

```
Gi1/0/1, Gi1/0/2
```

تحديث النهج على الطراز 3750X

ال 3750X (بخلاف ال ASA) يستطيع جلبت سياسة من ال ISE. قبل أن يقوم بتنزيل سياسة وتشغيلها، يجب تمكينه باستخدام الأوامر التالية:

```
bsns-3750-5(config)#cts role-based enforcement
bsns-3750-5(config)#cts role-based enforcement vlan-list 1-1005,1007-4094
```

في حالة عدم تمكينها، يتم تنزيل النهج ولكن لا يتم تثبيته ولا يتم إستخدامه للإنفاذ.

دخلت in order to أطلقت سياسة تحديث، هذا أمر:

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

دخلت in order to دققت أن السياسة يكون جلبت من ال ISE، هذا أمر:

```
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 2:VLAN10:
        ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
    Deny IP-00
```

يظهر الإخراج أن الجزء الضروري فقط من النهج يتم تنزيله.

في سحابة CTS، تحتوي الحزمة على رقيب المضيف المصدر، ويتم **التنفيذ في جهاز الوجهة**. هذا يعني أن الربط أرسلت من المصدر إلى آخر أداة، أي يكون ربطت مباشرة إلى الغاية مضيف. إن هذا الجهاز هو نقطة التنفيذ، حيث إنه يعرف رقيب الجنود الخاصين بالأجهزة المضيفة المتصلة مباشرة، ويعرف ما إذا كان يتعين السماح للحزمة الواردة مع رقيب مصدر أو رفضها بالنسبة للرقيب ذي الوجهة المحددة.

يستند هذا القرار إلى السياسات التي تم تنزيلها من ISE.

في هذا السيناريو، يتم تنزيل جميع السياسات. ومع ذلك، إذا قمت بمسح جلسة مصادقة MS Windows XP (SGT=VLAN20))، فلن تكون هناك حاجة إلى قيام المحول بتنزيل أي نهج (صف) يتوافق مع VLAN20، نظرا لعدم وجود مزيد من الأجهزة من ذلك الرقيب المتصل بالمحول.

يشرح قسم المتقدم (أستكشاف الأخطاء وإصلاحها) كيفية تحديد المحول 3750X للسياسات التي يجب تنزيلها مع فحص مستوى الحزمة.

تبادل SXP (تنسيق ASA كمستمع و 3750X كمكبر صوت)

إن مكتب الدعم المحلي لا يدعم الرقيب. كل الإطارات مع الرقيب يتم إسقاطها من قبل مكتب الدعم المحلي. لهذا السبب لا يمكن للطراز 3750X إرسال إطارات ذات علامات SGT إلى ASA. بدلا من ذلك، يتم إستخدام SXP. يسمح هذا البروتوكول ل ASA بتلقي معلومات من المحول حول التعيين بين عناوين IP والرقيب. ومع هذه المعلومات، يستطيع مكتب المساعدة على الوصول (ASA) تخطيط عناوين IP إلى الرقيب واتخاذ قرار استنادا إلى SGACL.

دخلت in order to شكلت ال 3750X كمكبر صوت، هذا أمر:

```
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.1 password default mode local
```

دخلت in order to شكلت ال ASA كمصغي، هذا أمر:

```
cts sxp enable
***** cts sxp default password
cts sxp default source-ip 192.168.1.1
cts sxp connection peer 192.168.1.10 password default mode local listener
```

دخلت in order to دققت أن ال ASA استلم ال يخطط، هذا أمر:

```
bsns-asa5510-17# show cts sxp sgt-map ipv4 detail
Total number of IP-SGT mappings : 2
Total number of IP-SGT mappings shown: 2

    SGT        : 2:VLAN10
IPv4       : 192.168.1.200
 Peer IP    : 192.168.1.10
           Ins Num    : 1
      Status     : Active
          Seq Num    : 49

    SGT        : 3:VLAN20
IPv4       : 192.168.2.200
 Peer IP    : 192.168.1.10
           Ins Num    : 1
      Status     : Active
          Seq Num    : 39
```

الآن، عندما يستلم ASA الربط قادم مع المصدر ip عنوان **192.168.1.200**، هو قادر على معاملته كما لو كان يأتي من **SGT=2**. بالنسبة لعنوان IP للمصدر **192.168.200.2**، فإنه قادر على معالجته كما لو كان قادما من **SGT=3**. يطبق ال نفسه للغاية عنوان.

ملاحظة: يجب أن يعرف الطراز 3750X عنوان IP الخاص بالمضيف المقترن. ويتم ذلك عن طريق تعقب جهاز IP. للحصول على عنوان IP مكون بشكل ثابت على المضيف الطرفي، يجب أن يتلقى المحول أي حزمة بعد المصادقة. يؤدي هذا إلى تشغيل تعقب جهاز IP للعثور على عنوان IP الخاص به، والذي يؤدي إلى تشغيل تحديث SXP. وعندما يكون الرقيب وحده معروفا، فإنه لا يتم إرساله عبر بروتوكول SXP.

تصفية حركة المرور على ASA مع ACL للرقيب

فيما يلي فحص لتكوين ASA:

```
interface Ethernet0/0
 nameif outside
 security-level 0
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
```

```
ip address 192.168.2.1 255.255.255.0
```

يتم إنشاء قائمة تحكم في الوصول (ACL) وتطبيقها على الواجهة الداخلية. وهو يسمح لجميع حركة مرور ICMP من **الرقيب=3** إلى **الرقيب=2** (يدعى **VLAN10**):

```
access-list inside extended permit icmp security-group tag 3 any security-group
                                                                  name VLAN10 any
                                    access-group inside in interface inside
```

ملاحظة: يمكنك إستخدام رقم علامة التمييز أو اسم علامة التمييز.

إذا قمت بإختبار الاتصال من MS Windows XP باستخدام عنوان IP للمصدر **192.168.2.200** (**SGT=3**) إلى MS Windows 7 بعنوان **SGT=2**) **192.168.1.200** IP)، فيقوم ASA بإنشاء اتصال:

```
ASA-6-302020: Built outbound ICMP connection for faddr 192.168.1.200/0%
(VLAN10) gaddr 192.168.2.200/512 laddr 192.168.2.200/512(3:VLAN20:2)
```

عندما تحاول إجراء نفس الإجراء مع Telnet، يتم حظر حركة المرور:

```
Deny tcp src inside:192.168.2.200/2478(3:VLAN20) dst outside:192.168.1.200/23
"VLAN10) by access-group "inside:2)
```

هناك كثير تشكيل خيار على ال ASA. من الممكن إستخدام كل من علامة الأمان وعنوان IP لكل من المصدر والوجهة. تسمح هذه القاعدة لحركة مرور ICMP ECHO من **علامة الرقيب = 3** وعنوان **192.168.2.200** IP إلى علامة الرقيب المسماة **VLAN10** وعنوان المضيف الوجهة **192.168.1.200**:

```
access-list inside extended permit icmp security-group tag 3 host 192.168.2.200
                    security-group name VLAN10 host 192.168.1.200 echo
```

ويمكن تحقيق ذلك أيضا مع مجموعات الكائنات:

```
object-group security SGT-VLAN-10
      security-group name VLAN10
object-group security SGT-VLAN-20
            security-group tag 3
       object-group network host1
network-object host 192.168.1.200
       object-group network host2
network-object host 192.168.2.200
object-group service my-icmp-echo
        service-object icmp echo

access-list inside extended permit object-group my-icmp-echo
object-group-security SGT-VLAN-20 object-group host2 object-group-security
SGT-VLAN-10 object-group host1
```

تصفية حركة المرور على الطراز 3750X مع تنزيل السياسات من ISE (RBACL)

من الممكن أيضا تحديد السياسات المحلية على المحول. ومع ذلك، يقدم هذا المثال السياسات التي تم تنزيلها من ISE. يسمح للنهج المحددة على ASA باستخدام كل من عناوين IP والرقباء (واسم المستخدم من Active Directory) في قاعدة واحدة. تسمح السياسات المعرفة على المحول (المحلي ومن ISE) فقط للرقيب. إذا كنت بحاجة إلى إستخدام عناوين IP في القواعد الخاصة بك، فيوصى بالتصفية على ASA.

يتم إختبار حركة مرور ICMP بين MS Windows XP و MS Windows 7. لهذا، يجب تغيير البوابة الافتراضية من ASA إلى 3750X على MS Windows. يحتوي المحول 3750X على واجهات توجيه ويمكن أن يوجه الحزم:

```
interface Vlan10
ip address 192.168.1.10 255.255.255.0
!
interface Vlan20
ip address 192.168.2.10 255.255.255.0
```

تم تنزيل السياسات من ISE بالفعل. دخلت in order to دقةت هم، هذا أمر:

```
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 2:VLAN10
ICMP-20
:IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20
ICMP-20
Deny IP-00
```

تخضع حركة المرور من **شبكة** VLAN10) MS Windows 7) إلى **شبكة** VLAN20) MS WindowsXP) إلى قائمة التحكم في الوصول (ICMP-20 ACL)، والتي يتم تنزيلها من ISE:

```
bsns-3750-5#show ip access-lists ICMP-20
(Role-based IP access list ICMP-20 (downloaded
permit icmp 10
```

دخلت in order to دقةت ال ACL، هذا أمر:

```
bsns-3750-5#show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
name   = Deny IP-00
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
:RBACL ACEs
deny ip

name   = ICMP-20
IP protocol version = IPV4
refcnt = 6
flag   = 0x41000000
stale  = FALSE
:RBACL ACEs
permit icmp

name   = Permit IP-00
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
:RBACL ACEs
permit ip
```

دخلت in order to دقةت ال رقيب يعين أن يتأكد أن حركة مرور من كلا مضيف يكون بشكل صحيح، هذا أمر:

```
bsns-3750-5#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================
LOCAL       2           192.168.1.200
LOCAL       3           192.168.2.200

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

يعمل بروتوكول ICMP من نظام التشغيل MS Windows 7 (**الرقيب=2**) إلى نظام التشغيل MS Windows XP (**الرقيب=3**) بشكل جيد مع قائمة التحكم في الوصول ICMP-20. يتم التحقق من هذا الإجراء من خلال عدادات التحقق من حركة المرور من **2** إلى **3** (15 حزمة مسموح بها):

```
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

          224            1695               0               0       0       2
            -               0               -               0       2       2

       132921          133258               0               0       *       *

           15               0               0               0       3       2
```

بعد محاولة إستخدام عداد Telnet، تزداد الحزم المرفوضة (غير مسموح به على قائمة التحكم في الوصول ICMP-20):

```
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

          224            1695               0               0       0       2
            -               0               -               0       2       2

       132969          133281               0               0       *       *

           15               0               2               0       3       2
```

ملاحظة: يرتبط حرف النجمة (*) الظاهر في المخرج بجميع حركات المرور غير المميزة (يسمى ذلك العمود والصف **غير معروفين** في Matrix على ISE، واستخدم رقم العلامة **0**).

عندما يكون لديك إدخال قائمة تحكم في الوصول (ACL) مع الكلمة الأساسية log (معرف على ISE)، يتم تسجيل تفاصيل الحزمة المقابلة والإجراءات المتخذة كما في أي قائمة تحكم في الوصول مع الكلمة الأساسية log.

التحقق من الصحة

ارجع إلى أقسام التكوين الفردية لإجراءات التحقق.

استكشاف الأخطاء وإصلاحها

إمداد PAC

قد تظهر المشاكل عند إستخدام توفير مسوغ الوصول المحمي (PAC) التلقائي. تذكر إستخدام الكلمة الأساسية **PAC** لخادم RADIUS. يستخدم إمداد PAC التلقائي على 3750X أسلوب EAP-FAST مع بروتوكول المصادقة المتوسع مع الأسلوب الداخلي باستخدام مصادقة بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (EAP-MSCHAPv2) من Microsoft. عندما تقوم بتصحيح الأخطاء، ترى رسائل RADIUS المتعددة التي هي جزء من تفاوض EAP-FAST المستخدم لبناء النفق الآمن، والذي يستخدم EAP-MSCHAPv2 مع المعرف وكلمة المرور اللذين تم تكوينهما للمصادقة.

يستخدم طلب RADIUS الأول **service-type=cts-pac-provisioning** AAA لإعلام ISE بأن هذا طلب PAC.

```
bsns-3750-5#debug cts provisioning events
bsns-3750-5#debug cts provisioning packets

=Mar  1 09:55:11.997: CTS-provisioning: New session socket: src*
                                    dst=10.48.66.129:1645 10.48.66.109:57516
      Mar  1 09:55:11.997: CTS-provisioning: Sending EAP Response/Identity to*
                                                                 10.48.66.129
  :Mar  1 09:55:11.997: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
:Mar  1 09:55:11.997: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
       Mar  1 09:55:11.997: CTS-provisioning: Received RADIUS challenge from*
                                                                 .10.48.66.129
      Mar  1 09:55:12.006: CTS-provisioning: Received TX_PKT from EAP method*
          Mar  1 09:55:12.006: CTS-provisioning: Sending EAPFAST response to*
                                                                 10.48.66.129
  :Mar  1 09:55:12.006: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
:Mar  1 09:55:12.106: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
       Mar  1 09:55:12.115: CTS-provisioning: Received RADIUS challenge from*
                                                                 .10.48.66.129
      Mar  1 09:55:12.744: CTS-provisioning: Received TX_PKT from EAP method*
          Mar  1 09:55:12.744: CTS-provisioning: Sending EAPFAST response to*
                                                                 10.48.66.129
  :Mar  1 09:55:12.744: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
:Mar  1 09:55:12.844: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
       Mar  1 09:55:12.844: CTS-provisioning: Received RADIUS challenge from*
                                                                 .10.48.66.129
      Mar  1 09:55:12.853: CTS-provisioning: Received TX_PKT from EAP method*
Mar  1 09:55:12.853: CTS-provisioning: Sending EAPFAST response to 10.48.66.129*
  :Mar  1 09:55:12.853: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
:Mar  1 09:55:12.853: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
       Mar  1 09:55:12.861: CTS-provisioning: Received RADIUS challenge from*
                                                                 .10.48.66.129
      Mar  1 09:55:12.861: CTS-provisioning: Received TX_PKT from EAP method*
Mar  1 09:55:12.861: CTS-provisioning: Sending EAPFAST response to 10.48.66.129*
  :Mar  1 09:55:12.861: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
:Mar  1 09:55:12.878: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
       Mar  1 09:55:12.878: CTS-provisioning: Received RADIUS challenge from*
                                                                 .10.48.66.129
      Mar  1 09:55:12.886: CTS-provisioning: Received TX_PKT from EAP method*
Mar  1 09:55:12.886: CTS-provisioning: Sending EAPFAST response to 10.48.66.129*
  :Mar  1 09:55:12.886: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
:Mar  1 09:55:12.895: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
```

```
Mar  1 09:55:12.895: CTS-provisioning: Received RADIUS challenge from*
                                                                .10.48.66.129
        Mar  1 09:55:12.895: CTS-provisioning: Received TX_PKT from EAP method*
Mar  1 09:55:12.895: CTS-provisioning: Sending EAPFAST response to 10.48.66.129*
    :Mar  1 09:55:12.903: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
  :Mar  1 09:55:12.912: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
         Mar  1 09:55:12.912: CTS-provisioning: Received RADIUS challenge from*
                                                                .10.48.66.129
        Mar  1 09:55:12.920: CTS-provisioning: Received TX_PKT from EAP method*
Mar  1 09:55:12.920: CTS-provisioning: Sending EAPFAST response to 10.48.66.129*
    :Mar  1 09:55:12.920: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
  :Mar  1 09:55:12.928: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
         Mar  1 09:55:12.928: CTS-provisioning: Received RADIUS challenge from*
                                                                .10.48.66.129
    Mar  1 09:55:12.970: CTS-pac-refresh: PAC C40A15A339286CEAC28A50DBBAC59784*
                                                refresh timer has been set for 20y30w
                            .Mar  1 09:55:12.970: CTS-provisioning: Ignoring key data*
        Mar  1 09:55:12.979: CTS-provisioning: Received TX_PKT from EAP method*
Mar  1 09:55:12.979: CTS-provisioning: Sending EAPFAST response to 10.48.66.129*
    :Mar  1 09:55:12.979: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129*
  :Mar  1 09:55:12.995: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129*
.Mar  1 09:55:12.995: CTS-provisioning: Received RADIUS reject from 10.48.66.129*
     Mar  1 09:55:12.995: CTS-provisioning: Successfully obtained PAC for A-ID*
                                                c40a15a339286ceac28a50dbbac59784
  Mar  1 09:55:12.995: CTS-provisioning: cts_provi_server_cleanup: 10.48.66.129*
    .Mar  1 09:55:12.995: CTS-provisioning: work complete, process terminating*
```

من المتوقع أن يرفض RADIUS في نهاية المخرج لأنك إستلمت PAC بالفعل، ولم يتبع مع عملية مصادقة إضافية.

تذكر ان مسوغات الوصول المحمي مطلوبة لكل الاتصالات الاخرى مع ISE. ولكن، إذا لم يكن لديك ذلك المحول، فإنه يستمر في محاولة تحديث البيئة أو النهج عند تكوينه. ثم، لا يربط هو PAC) **cts-opaqueue**) في طلبات RADIUS، مما يسبب الفشل.

إذا كان مفتاح PAC الخاص بك غير صحيح، تظهر رسالة الخطأ هذه على ISE:

```
The Message-Authenticator RADIUS attribute is invalid
```

أنت أيضا ترى هذا إنتاج من تصحيح الأخطاء (**debug cts provisioning + debug radius**) على المفتاح إن يكون مفتاح PAC خطأ:

```
Apr 20 10:07:11.768: CTS-provisioning: Sending EAP Response/Identity t
                            !Apr 20 10:07:15.325: RADIUS(0000024B): Request timed out
Apr 20 10:07:15.325: RADIUS: No response from (10.62.84.224:1645,1646) for
                                                                id 1645/37
```

إذا كنت تستخدم اصطلاح **خادم RADIUS** الحديث، فهذا يعرض:

```
radius server KRK-ISE
address ipv4 10.62.84.224 auth-port 1645 acct-port 1646
pac key CISCO
```

ملاحظة: يجب أن تستخدم نفس كلمة المرور على ISE التي أستخدمتها في **إعدادات مصادقة الجهاز**.

بعد توفير مسوغات الوصول المحمي (PAC) بنجاح، يتم عرض ذلك على ISE:

Authentication Summary	
Logged At:	June 26,2013 1:36:32.676 PM
RADIUS Status:	PAC provisioned
NAS Failure:	
Username:	3750
MAC/IP Address:	BC:16:65:25:A5:00
Network Device:	3750X : 10.48.66.109 :
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

تحديث البيئة

يتم إستخدام تحديث البيئة للحصول على البيانات الأساسية من ISE، والتي تتضمن رقم الرقيب والاسم. يظهر مستوى الحزمة أنه فقط ثلاثة طلبات واستجابات RADIUS ذات سمات.

بالنسبة للطلب الأول، يتلقى المحول اسم **CTSServerlist**. بالنسبة للقائمة الثانية، فإنه يتلقى تفاصيل تلك القائمة، وبالنسبة للقائمة الأخيرة، فإنه يتلقى كل الرقيب مع علامات وأسماء:

No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

```
Authenticator: b1672c429de0593417de4315ee0bd40c
[This is a response to a request in frame 5]
[Time from request: 0.008000000 seconds]
▾ Attribute Value Pairs
  ▾ AVP: l=14  t=User-Name(1): #CTSREQUEST#
      User-Name: #CTSREQUEST#
  ▸ AVP: l=40  t=State(24): 526561757468536573736696f6e3a30613330343238313030...
  ▸ AVP: l=50  t=Class(25): 434143533a30613330343238313030303031343033353143...
  ▸ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
  ▸ AVP: l=18  t=Message-Authenticator(80): ac8e7b6f0d59da776f0dbf1ffa04baf1
  ▾ AVP: l=39  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=33 t=Cisco-AVPair(1): cts:security-group-table=0001-5
  ▾ AVP: l=46  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=40 t=Cisco-AVPair(1): cts:security-group-info=0-0-00-Unknown
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=ffff-0-00-ANY
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=2-0-00-VLAN10
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=3-0-00-VLAN20
```

هنا يمكنك رؤية **الرقيب** 0،**ffff**، وأيضا إثنين معرفة بشكل مخصص: رقيب بطاقة 2 يعين **VLAN10** والرقيب بطاقة 3 يعين **VLAN20**.

ملاحظة: تتضمن جميع طلبات **CTS-PAC-Opaque** RADIUS كنتيجة لتوفير مسوغ الوصول المحمي (PAC).

No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

```
▸ Raw packet data
▸ Internet Protocol Version 4, Src: 10.48.66.109 (10.48.66.109), Dst: 10.48.66.129
▸ User Datagram Protocol, Src Port: sightline (1645), Dst Port: sightline (1645)
▾ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xa6 (166)
    Length: 319
    Authenticator: 60a2c0dbab563d6a0f4b44910f646d9e
    [The response to this request is in frame 2]
  ▾ Attribute Value Pairs
    ▾ AVP: l=203  t=Vendor-Specific(26) v=Cisco(9)
      ▸ VSA: l=197 t=Cisco-AVPair(1): cts-pac-opaque=\000\002\000\260\000\003\000\0
    ▾ AVP: l=14  t=User-Name(1): #CTSREQUEST#
        User-Name: #CTSREQUEST#
    ▾ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
      ▸ VSA: l=28 t=Cisco-AVPair(1): cts-environment-data=3750X
    ▸ AVP: l=18  t=User-Password(2): Encrypted
    ▸ AVP: l=6  t=Service-Type(6): Dialout-Framed-User(5)
    ▸ AVP: l=6  t=NAS-IP-Address(4): 10.48.66.109
    ▸ AVP: l=18  t=Message-Authenticator(80): a16f5aea9af1cb47abb0d06d229eeec7
```

في 3750X، يجب أن ترى تصحيح الأخطاء لجميع استجابات RADIUS الثلاث والقوائم المقابلة وتفاصيل القائمة وقائمة الرقيب-الداخل المحددة:

```
bsns-3750-5#debug cts environment-data all

        Mar  1 10:05:07.454: CTS env-data&colon; cleanup mcast SGT table*
    Mar  1 10:05:18.057: CTS env-data&colon; Force environment-data refresh*
        = Mar  1 10:05:18.057: CTS env-data&colon; download transport-type*
                                                    CTS_TRANSPORT_IP_UDP
 ,Mar  1 10:05:18.057:     cts_env_data START: during state env_data_complete*
                                                    (got event 0(env_data_request
      <- Mar  1 10:05:18.057: @@@ cts_env_data START: env_data_complete*
                                                    env_data_waiting_rsp
   Mar  1 10:05:18.057: env_data_waiting_rsp_enter: state = WAITING_RESPONSE*
      Mar  1 10:05:18.057: env_data_request_action: state = WAITING_RESPONSE*
     ,(Mar  1 10:05:18.057: cts_env_data_is_complete: FALSE, req(x0), rec(x0*
            (expect(x81), complete1(x85), complete2(xB5), complete3(x28B5
 ,Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD*
                                                    attempt public group
  Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP*
     (Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)AAA req(x7C3DF10*
                (Mar  1 10:05:18.057: cts_aaa_attr_add: AAA req(0x7C3DF10*
                    #Mar  1 10:05:18.057:   username = #CTSREQUEST*
                Mar  1 10:05:18.057:   cts-environment-data = 3750X*
.Mar  1 10:05:18.057: cts_aaa_req_send: AAA req(0x7C3DF10) successfully sent to AAA*
     (Mar  1 10:05:18.083: cts_aaa_callback: (CTS env-data)AAA req(0x7C3DF10*
                                                    response success
```

```
                                .(Mar  1 10:05:18.083:   AAA attr: Unknown type (447*
                                .(Mar  1 10:05:18.083:   AAA attr: Unknown type (220*
                                .(Mar  1 10:05:18.083:   AAA attr: Unknown type (275*
                    .Mar  1 10:05:18.083:   AAA attr: server-list = CTSServerList1-0001*
                         .Mar  1 10:05:18.083:   AAA attr: security-group-tag = 0000-00*
                       .Mar  1 10:05:18.083:   AAA attr: environment-data-expiry = 86400*
                         .Mar  1 10:05:18.083:   AAA attr: security-group-table = 0001-5*
                       Mar  1 10:05:18.083: CTS env-data&colon; Receiving AAA attributes*
                                                                      CTS_AAA_SLIST
                            slist name(CTSServerList1) received in 1st Access-Accept
                                                 slist name(CTSServerList1) created
                                      CTS_AAA_SECURITY_GROUP_TAG - SGT = unicast-unknown-00
                                                  .CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400
                                                                 CTS_AAA_SGT_NAME_LIST
                                               table(0001) received in 1st Access-Accept
                                                                   ()old name(), gen
                                                              (new name(0001), gen(50
                                                                    CTS_AAA_DATA_END
                                Mar  1 10:05:18.083:     cts_env_data WAITING_RESPONSE: during state*
                                                 (env_data_waiting_rsp, got event 1(env_data_received
                     <- Mar  1 10:05:18.083: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp*
                                                                    env_data_assessing
                                 Mar  1 10:05:18.083: env_data_assessing_enter: state = ASSESSING*
                                Mar  1 10:05:18.083: env_data_assessing_action: state = ASSESSING*
                        ,(Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83*
                                   (expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5
                    ,Mar  1 10:05:18.083:     cts_env_data ASSESSING: during state env_data_assessing*
                                                           (got event 3(env_data_incomplete
                              <- Mar  1 10:05:18.083: @@@ cts_env_data ASSESSING: env_data_assessing*
                                                                    env_data_waiting_rsp
                           Mar  1 10:05:18.083: env_data_waiting_rsp_enter: state = WAITING_RESPONSE*
                              Mar  1 10:05:18.083: env_data_request_action: state = WAITING_RESPONSE*
                        ,(Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83*
                                   (expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5
                    ,Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD*
                                                                    attempt public group
                           Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP*
                              (Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)AAA req(x792FFD0*
                                            (Mar  1 10:05:18.083: cts_aaa_attr_add: AAA req(0x792FFD0*
                                                  #Mar  1 10:05:18.091:   username = #CTSREQUEST*
                                        Mar  1 10:05:18.091:   cts-server-list = CTSServerList1*
.Mar  1 10:05:18.091: cts_aaa_req_send: AAA req(0x792FFD0) successfully sent to AAA*
                              (Mar  1 10:05:18.099: cts_aaa_callback: (CTS env-data)AAA req(0x792FFD0*
                                                                      response success
                                .(Mar  1 10:05:18.099:   AAA attr: Unknown type (447*
                                .(Mar  1 10:05:18.099:   AAA attr: Unknown type (220*
                                .(Mar  1 10:05:18.099:   AAA attr: Unknown type (275*
                    .Mar  1 10:05:18.099:   AAA attr: server-list = CTSServerList1-0001*
                   :Mar  1 10:05:18.099:   AAA attr: server = c40a15a339286ceac28a50dbbac59784*
                                                                    .10.48.66.129:1812
                       Mar  1 10:05:18.099: CTS env-data&colon; Receiving AAA attributes*
                                                                      CTS_AAA_SLIST
                                 (2nd Access-Accept slist name(CTSServerList1), gen(0001
                                                                      CTS_AAA_SERVERS
                     server (c40a15a339286ceac28a50dbbac59784:10.48.66.129:1812) added
                                                                    CTS_AAA_DATA_END
                                Mar  1 10:05:18.099:     cts_env_data WAITING_RESPONSE: during state*
                                                 (env_data_waiting_rsp, got event 1(env_data_received
                     <- Mar  1 10:05:18.099: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp*
                                                                    env_data_assessing
                                 Mar  1 10:05:18.099: env_data_assessing_enter: state = ASSESSING*
                                Mar  1 10:05:18.099: env_data_assessing_action: state = ASSESSING*
                        ,(Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87*
                                   (expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5
```

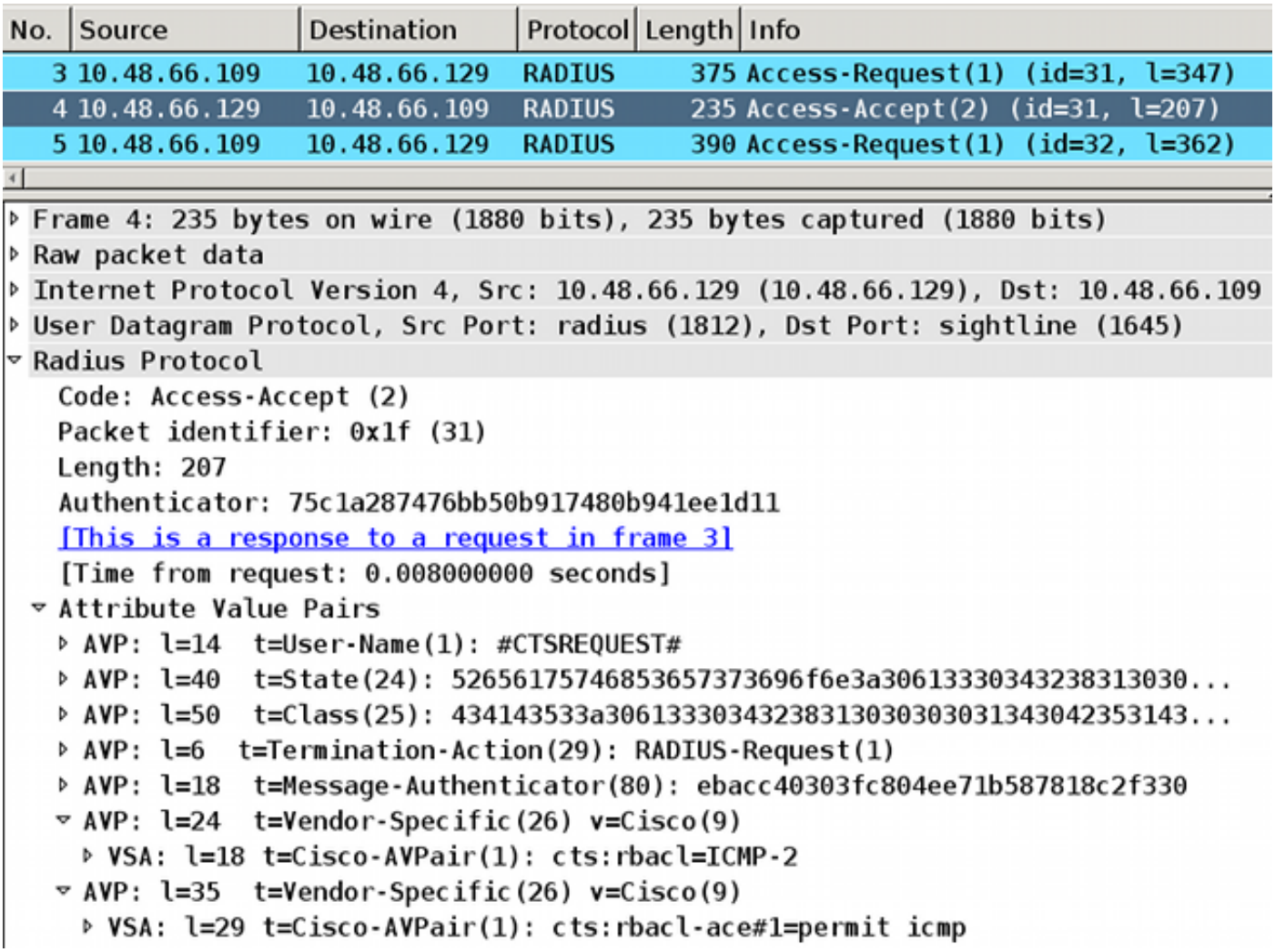
```
,Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing*
                                                    (got event 3(env_data_incomplete
            <- Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing*
                                                      env_data_waiting_rsp
          Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE*
             Mar  1 10:05:18.099: env_data_request_action: state = WAITING_RESPONSE*
      ,(Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87*
                    (expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5
   Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)Using private server group*
         Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP*
            (Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)AAA req(x7A6C4AC*
                         (Mar  1 10:05:18.099: cts_aaa_attr_add: AAA req(0x7A6C4AC*
                                  #Mar  1 10:05:18.099:   username = #CTSREQUEST*
                               Mar  1 10:05:18.099:   cts-security-group-table = 0001*
.Mar  1 10:05:18.099: cts_aaa_req_send: AAA req(0x7A6C4AC) successfully sent to AAA*
            (Mar  1 10:05:18.108: cts_aaa_callback: (CTS env-data)AAA req(0x7A6C4AC*
                                                      response success
                                  .(Mar  1 10:05:18.108:   AAA attr: Unknown type (447*
                                  .(Mar  1 10:05:18.108:   AAA attr: Unknown type (220*
                                  .(Mar  1 10:05:18.108:   AAA attr: Unknown type (275*
                        .Mar  1 10:05:18.108:   AAA attr: security-group-table = 0001-5*
                 .Mar  1 10:05:18.108:   AAA attr: security-group-info = 0-0-00-Unknown*
                  .Mar  1 10:05:18.108:   AAA attr: security-group-info = ffff-0-00-ANY*
                  .Mar  1 10:05:18.108:   AAA attr: security-group-info = 2-0-00-VLAN10*
                  .Mar  1 10:05:18.108:   AAA attr: security-group-info = 3-0-00-VLAN20*
                     Mar  1 10:05:18.108:  CTS env-data&colon; Receiving AAA attributes*
                                                          CTS_AAA_SGT_NAME_LIST
                                           table(0001) received in 2nd Access-Accept
                                                        (old name(0001), gen(50
                                                        (new name(0001), gen(50
                                    CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-unknown-00
                                          flag (128) server name (Unknown) added
                                            (name (0001), request (1), receive (1
                              Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
                                    CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-default-00
                                             flag (128) server name (ANY) added
                                            (name (0001), request (1), receive (1
                              Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
                                             CTS_AAA_SGT_NAME_INBOUND - SGT = 2-00
                                           flag (128) server name (VLAN10) added
                                            (name (0001), request (1), receive (1
                              Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
                                             CTS_AAA_SGT_NAME_INBOUND - SGT = 3-00
                                           flag (128) server name (VLAN20) added
                                            (name (0001), request (1), receive (1
                              Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
                                                          CTS_AAA_DATA_END
                        Mar  1 10:05:18.108:     cts_env_data WAITING_RESPONSE: during state*
                                        (env_data_waiting_rsp, got event 1(env_data_received
          <- Mar  1 10:05:18.108: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp*
                                                        env_data_assessing
                           Mar  1 10:05:18.108: env_data_assessing_enter: state = ASSESSING*
                          Mar  1 10:05:18.108: env_data_assessing_action: state = ASSESSING*
      ,(Mar  1 10:05:18.116: cts_env_data_is_complete: TRUE, req(x2085), rec(x2C87*
                    (expect(x81), complete1(x85), complete2(xB5), complete3(x28B5
   ,Mar  1 10:05:18.116:     cts_env_data ASSESSING: during state env_data_assessing*
                                                    (got event 4(env_data_complete
            <- Mar  1 10:05:18.116: @@@ cts_env_data ASSESSING: env_data_assessing*
                                                      env_data_complete
                          Mar  1 10:05:18.116: env_data_complete_enter: state = COMPLETE*
                          Mar  1 10:05:18.116: env_data_install_action: state = COMPLETE*
```

تحديث النهج

تحديث النهج معتمد فقط على المحول. يشبه التحديث البيئي. هذه ببساطة طلبات RADIUS وقبولها.

يطلب المحول جميع قوائم التحكم في الوصول (ACL) ضمن القائمة الافتراضية. ثم، بالنسبة لكل قائمة تحكم في الوصول (ACL) غير محدثة (أو غير موجودة)، فإنها ترسل طلبا آخر للحصول على التفاصيل.

فيما يلي مثال على الاستجابة عند طلب قائمة التحكم في الوصول إلى ICMP-20:



تذكر أنه يجب أن يكون لديك **تطبيق قائم على الأدوار** تم تكوينه من أجل فرض قائمة التحكم في الوصول (ACL) هذه.

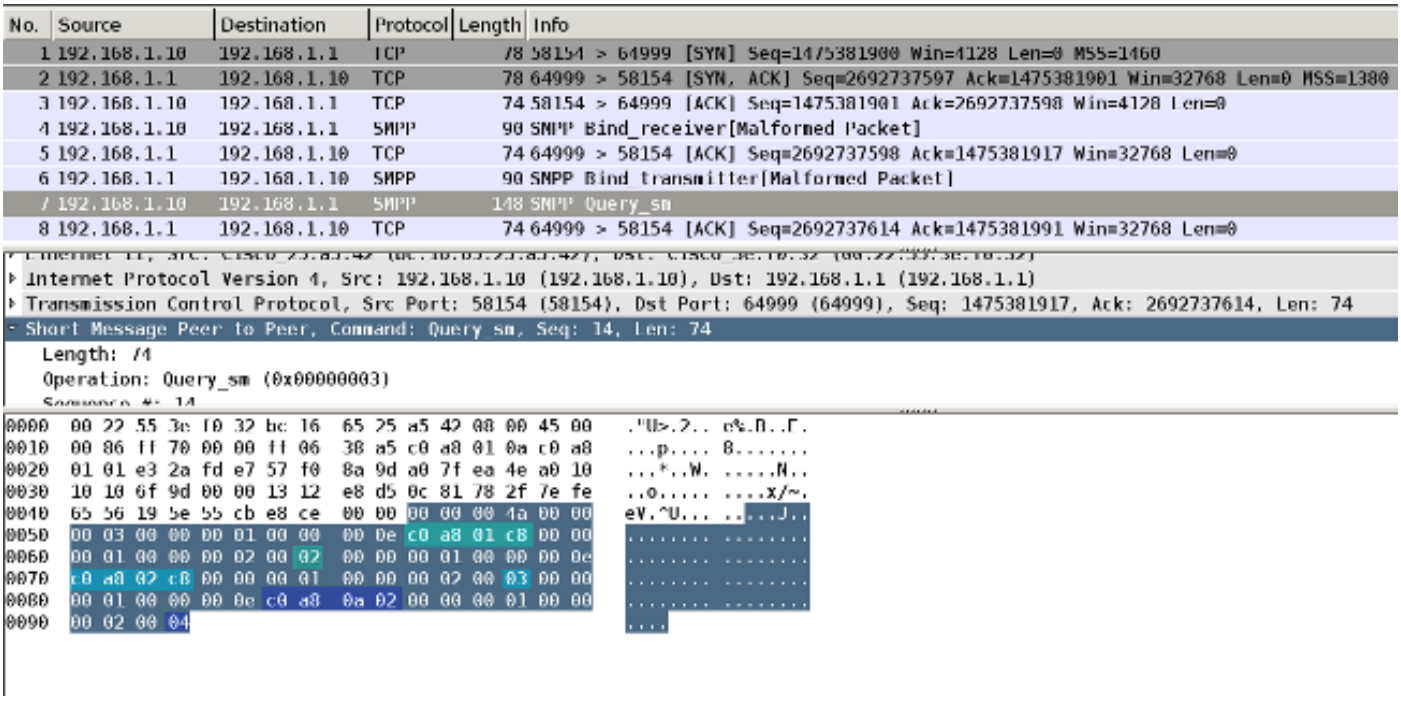
يشير تصحيح الأخطاء إلى ما إذا كانت هناك تغييرات (استنادا إلى معرف الجيل). إذا كان الأمر كذلك، يمكنك إزالة تثبيت النهج القديم إذا لزم الأمر، وتثبيت نهج جديد. ويتضمن ذلك برمجة ASIC (دعم الأجهزة).

```
bsns-3750-5#debug cts all

Mar 30 02:39:37.151:  CTS authz entry: peer(Unknown-2) Receiving AAA attributes
                (rcv rbacl list: flags: req(81)rcv(0)wait(80)prev(0)install(880
                                                        SGT = 2-01:VLAN10 -
                                                        SGT = 2-01:VLAN10 -
                                        current arg_cnt=8, expected_num_args=11
                        (3rd Access-Accept rbacl received name(ICMP), gen(20
                                        (received_policyp->sgt(2-01:VLAN10
                                (existing sgt_policy(73FFDB4) sgt(2-01:VLAN10
                        RBACL name(ICMP-20)flag(40000000) already exists
                (acl_listp(740266C) old_acl_infop(0),exist_rbacl_type(0
                                        .CTS_AAA_AUTHORIZATION_EXPIRY = 86400
```

```
CTS_AAA_DATA_END

- Mar 30 02:39:37.176: cts_authz_entry_complete_action: Policy download complete
                    (peer(Unknown-2) SGT(2-01:VLAN10) status(RBACL-POLICY SUCCEEDED
                                :Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb
                                        :Mar 30 02:39:37.176: uninstall cb_ctx
                                    Mar 30 02:39:37.176:   session_hdl = F1000003
(Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB
                                        Mar 30 02:39:37.176:   ip_version  = IPV6
                                        Mar 30 02:39:37.176:   src-or-dst  = BOTH
                                 (Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0
                            (Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(C0000000
                                :Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb
                                        :Mar 30 02:39:37.176: uninstall cb_ctx
                                    Mar 30 02:39:37.176:   session_hdl = F1000003
(Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB
                                        Mar 30 02:39:37.176:   ip_version  = IPV4
                                        Mar 30 02:39:37.176:   src-or-dst  = BOTH
                                 (Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0
                            (Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(40000000

                                        :Mar 30 02:39:37.210: install cb_ctx
                                    Mar 30 02:39:37.210:   session_hdl = F1000003
(Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB
                                        Mar 30 02:39:37.210:   ip_version  = IPV6
                                         Mar 30 02:39:37.210:   src-or-dst  = SRC
                                (Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(C0000000
                                     (Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0
  Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Waiting for more RBM callback
    (for remaining IP version(40000000) RBACL policy(73FFDB4) for SGT(2-01:VLAN10
                                                                (flag(41400001
                                    :Mar 30 02:39:37.210: cts_authz_rbacl_install_cb
                                        :Mar 30 02:39:37.210: install cb_ctx
                                    Mar 30 02:39:37.210:   session_hdl = F1000003
(Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB
                                        Mar 30 02:39:37.210:   ip_version  = IPV4
                                         Mar 30 02:39:37.210:   src-or-dst  = SRC
                                (Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(40000000
                                     (Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0
(Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Program RBACL policy(73FFDB4
                                                for SGT(2-01:VLAN10) flag(41400001) success
```

تبادل SXP

يتم تشغيل تحديث SXP بواسطة رمز تعقب جهاز IP الذي يعثر على عنوان IP الخاص بالجهاز. بعد ذلك، يتم إستخدام بروتوكول الرسائل القصيرة Peer-to-Peer (SMPP) لإرسال التحديثات. إنه يستعمل **TCP خيار 19** للمصادقة، أي يكون ال نفسه مثل حد مدخل بروتوكول (BGP). حمولة SMPP غير مشفرة. لا يتوفر لدى Wireshark جهاز فك التشفير المناسب لحمولة SMPP، ولكن من السهل العثور على البيانات بداخلها:



- أول واحد، **c8 01 a8 c0**، هو **192.168.1.200** وله **بطاقة 2**.
- الثاني، **c8 02 a8 c0**، هو **192.168.2.200** وبه **علامة 3**.
- الثالثة **02 0a a8 c0**، هي **192.168.10.2** وبها **العلامة 4** (هذه استعملت لاختبار هاتف **الرقيب=4**)

فيما يلي بعض عمليات تصحيح الأخطاء على المحول 3750X بعد اكتشاف تعقب جهاز IP لعنوان IP الخاص بنظام التشغيل MS Windows 7:

```
bsns-3750-5#debug cts sxp message
bsns-3750-5#debug cts sxp internal
bsns-3750-5#debug cts sxp conn
bsns-3750-5#debug cts sxp mdb
bsns-3750-5#debug cts sxp error

Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_message_event = CTS_SXPMSG_REQUEST
Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_request  CTS_SXPMSG_REQ_CONN_NVGEN
                     Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
                     Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
                Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_process_request boolean set
           Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_send_request set boolean after
                          Apr  7 00:40:05.418: CTS-SXP-CONN:is_cts_sxp_rf_active
 Apr  7 00:40:05.418: CTS-SXP-MDB:sxp_export_ipsgt_change 192.168.1.200/32 add 1
```

هنا ال يماثل تصحيح على ال ASA:

```
bsns-asa5510-17# debug cts sxp all

ASA-7-776018: CTS SXP: Binding 192.168.1.200->2:VLAN10 from peer 192.168.1.10%
                                                .instance 1) added in SXP database)
 ASA-7-776019: CTS SXP: Binding 192.168.1.200->2:VLAN10 added. Update binding%
                                                                  .manager
 ASA-6-776251: CTS SGT-MAP: Binding 192.168.1.200->2:VLAN10 from SXP added to%
                                                               .binding manager
 ASA-7-776014: CTS SXP: SXP received binding forwarding request (add) binding%
                                                              .VLAN10:2<192.168.1.200-
```

in order to رأيت كثير تصحيح على ال ASA، أنت يستطيع مكنت ال debudebuing مستوى إسهاب:

```
bsns-asa5510-17# debug cts condition level detail
```

```
debug cts condition level detail is enable
```

SGACL على ASA

بعد أن يقوم ASA بتثبيت تعيينات SGT التي يتلقاها SXP بشكل صحيح، يجب أن تعمل قائمة التحكم في الوصول لمجموعات الأمان بشكل صحيح. عندما تواجه مشاكل مع التعيين، أدخل:

```
bsns-asa5510-17# debug cts sgt-map
```

تعمل قائمة التحكم في الوصول (ACL) مع مجموعة الأمان بنفس الطريقة التي تعمل بها لعنوان IP أو هوية المستخدم. تكشف السجلات عن مشاكل، والدخل الدقيق لقائمة التحكم في الوصول (ACL) التي تم الوصول إليها.

فيما يلي إختبار اتصال من نظام التشغيل MS Windows XP إلى نظام التشغيل MS Windows 7 يوضح أن أداة تعقب الحزم تعمل بشكل صحيح:

```
bsns-asa5510-17# packet-tracer input inside icmp 192.168.2.200 8 0 192.168.1.200
                                                                          detailed
                                                        <output ommitted>

                                                                  Phase: 2
                                                          Type: ACCESS-LIST
                                                               Subtype: log
                                                           Result: ALLOW
                                                                  :Config
                                                 access-group inside in interface inside
          access-list inside extended permit icmp security-group tag 3 any security-group
                                                                name VLAN10 any
                                                    :Additional Information
                                                 :Forward Flow based lookup yields rule
                                 in  id=0xaaf2ae80, priority=13, domain=permit, deny=false
                ,hits=185, user_data=0xaa2f5040, cs_id=0x0, use_real_addr, flags=0x0
                                                                     protocol=1
                          src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=3:VLAN20
                dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=2:VLAN10, dscp=0x0
                                                 input_ifc=inside, output_ifc=any

                                                        <output ommitted>
```

معلومات ذات صلة

- دليل تكوين Cisco TrustSec ل 3750
- دليل تكوين Cisco TrustSec ل 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).