تكوين المصفوفات المتعددة ل TrustSec على ISE 2.2

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
مصفوفات متعددة
مصفوفات ديفكون
التكوين
الرسم التخطيطي للشبكة
التكوينات
1. تكوين المحول الأساسي ل RADIUS/CTS
2 - لجنة العمل الدائمة التابعة للجنة التقنية المعنية
3. تكوين CTS على محول.
4. تكوين CTS الأساسي على ISE.
5. المصفوفات المتعددة وتكوين DefCon على ISE.
6 - تصنيف الرقيب
7. تنزيل سياسة CTS
التحقق من الصحة
مصفوفات متعددة
نشر DefCon
استكشاف الأخطاء وإصلاحها
إعداد PAC
تنزيل بيانات البيئة
سياسات CTS

المقدمة

يصف هذا المستند إستخدام مصفوفات TrustSec المتعددة ومصفوفات DefCon في Cisco Identity Services Engine (ISE) 2.2. هذه ميزة TrustSec جديدة تم تقديمها في ISE 2.2 للحصول على مستويات أكثر دقة في الشبكة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بمكونات Cisco TrustSec (CTS)

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

المكونات المستخدمة

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

- Identity Services Engine، الإصدار 2.2
- المحول Cisco Catalyst Switch 3850 03.07.03.E
- المحول Cisco Catalyst Switch 3750X 15.2(4)E1
- أجهزة نظام التشغيل Windows 7

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

معلومات أساسية

في ISE 2.0، هناك إمكانية استخدام مصفوفة TrustSec إنتاج واحدة فقط لجميع أجهزة الشبكة. أضاف ISE 2.1 ميزة تسمى مصفوفة التشغيل المرحلي التي يمكن إستخدامها في مصفوفة الاختبار والتنفيذ. تم تطبيق السياسات التي تم إنشاؤها في مصفوفة الأغراض الاختبارات. أما باقي الأجهزة فهي التشغيل المرحلي فقط على أجهزة الشبكة المستخدمة للاختبارات. تعمل المصفوفة التشغيل المرحلي بمجرد التأكد من أن مصفوفة الإنتاج لا تزال تستخدم. يمكن نقل جميع الأجهزة الأخرى إليها وتصبح مصفوفة إنتاج جديدة بشكل جيد.

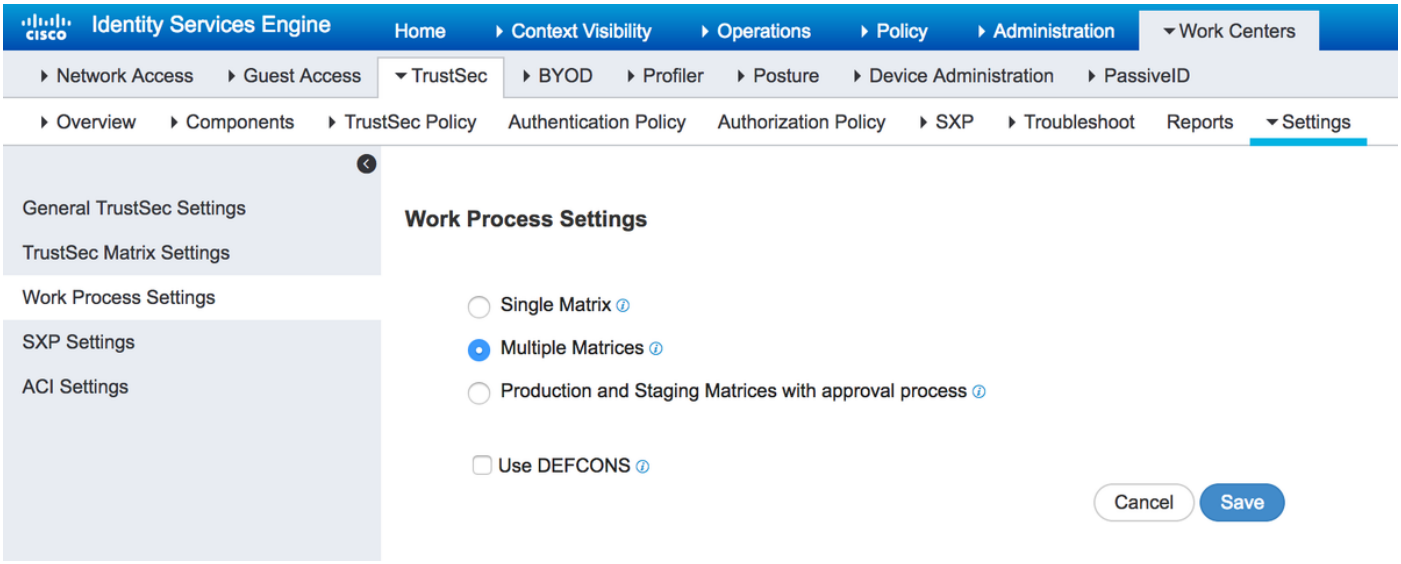
يأتي ISE 2.2 مزود بميزتين جديدتين من TrustSec:

1. مصفوفات متعددة - القدرة على تخصيص مصفوفات مختلفة لأجهزة الشبكة
2. DefCon Matrix - يتم دفع هذه المصفوفة إلى جميع أجهزة الشبكة في حالة معينة، والتي يتم تشغيلها بواسطة المسؤول

من الممكن إستخدام إما ميزة مصفوفة واحدة أو ميزة مصفوفة الإنتاج والتصنيف في ISE 2.2.

مصفوفات متعددة

لاستخدام مصفوفات متعددة، يجب عليك تمكين هذا الخيار تحت **مراكز العمل > TrustSec > الإعدادات > إعدادات عملية العمل**، كما هو موضح في الصورة:



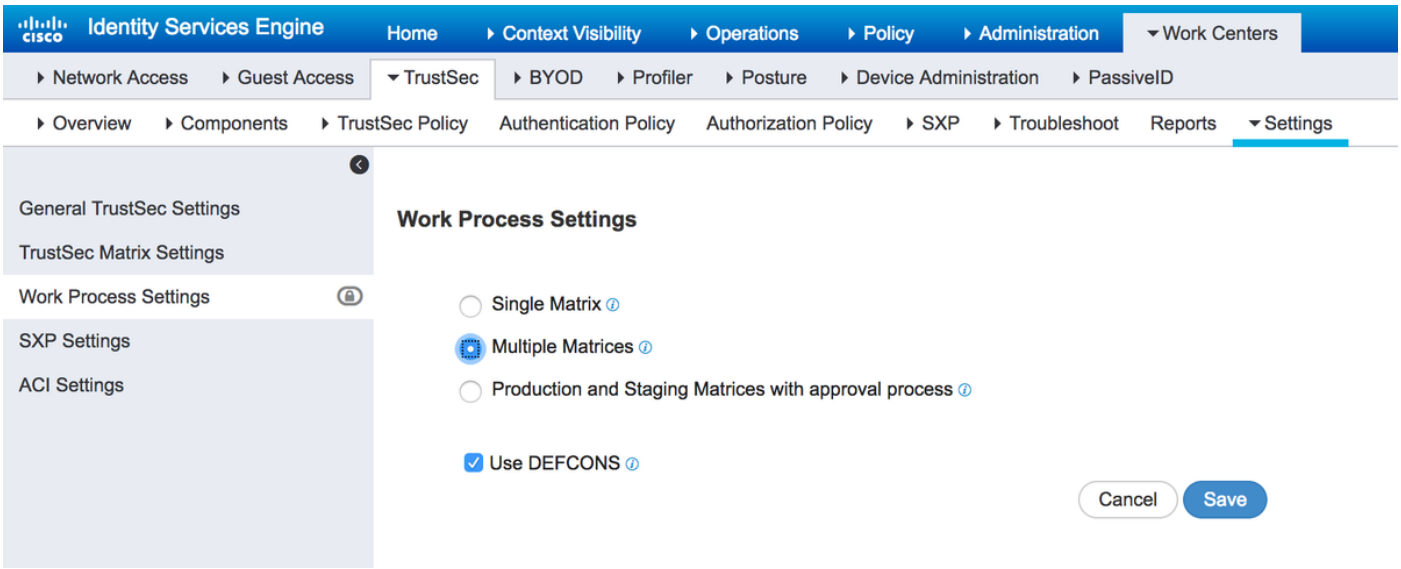
وبمجرد تمكين هذا، يمكنك إنشاء مصفوفات جديدة وفيما بعد على تعيين أجهزة الشبكة إلى المصفوفة المحددة.

مصفوفات ديفكون

مصفوفات DefCon هي مصفوفات خاصة جاهزة للنشر في أي وقت. عند النشر، يتم تعيين كافة أجهزة الشبكة تلقائيا إلى هذه المصفوفة. ما يزال ISE يتذكر مصفوفة الإنتاج الأخيرة لجميع أجهزة الشبكة، لذلك يمكن إرجاع هذا التغيير في أي نقطة عند إلغاء تنشيط DefCon. يمكنك تحديد حتى أربعة مصفوفات DefCon مختلفة:

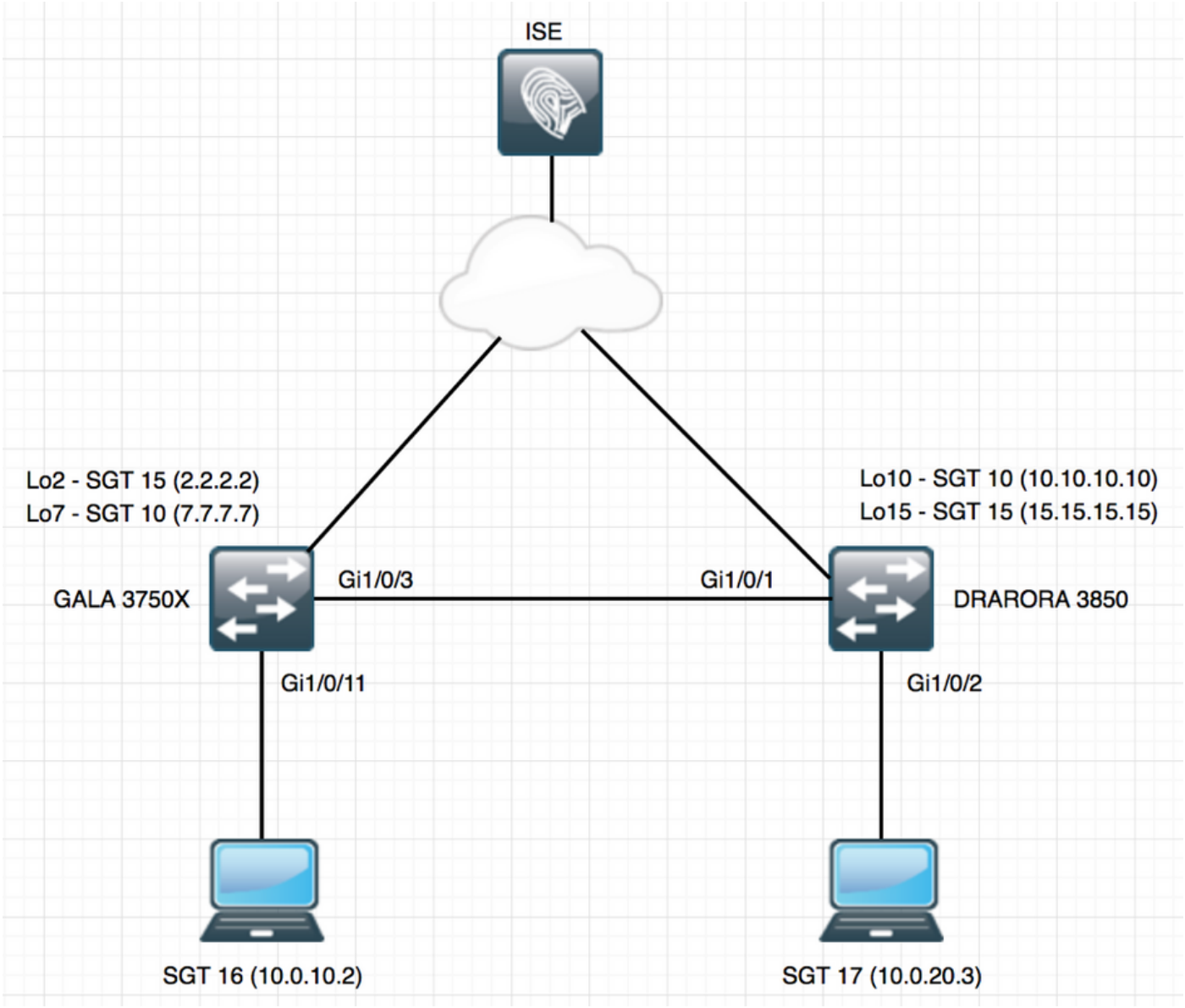
1. DefCon1 - هام
2. DefCon2 - شديد
3. DefCon3 - كبير
4. DefCon4 - متوسط

يمكن إستخدام مصفوفات DefCon مع جميع خيارات عملية العمل الثلاثة:



التكوين

الرسم التخطيطي للشبكة



التكوينات

لاستخدام مصفوفات متعددة، يجب تمكينها ضمن إعدادات عملية العمل. في هذا المثال، قم بتمكين مصفوفة DefCon أيضا.

1. تكوين المحول الأساسي ل RADIUS/CTS

```
radius server ISE
 address ipv4 10.48.17.161 auth-port 1812 acct-port 1813
 pac key cisco

aaa group server radius ISE
 server name ISE
 ip radius source-interface FastEthernet0

ip radius source-interface FastEthernet0

aaa server radius dynamic-author
 client 10.48.17.161 server-key cisco

aaa new-model aaa authentication dot1x default group ISE aaa accounting dot1x default start-stop
group ISE
```

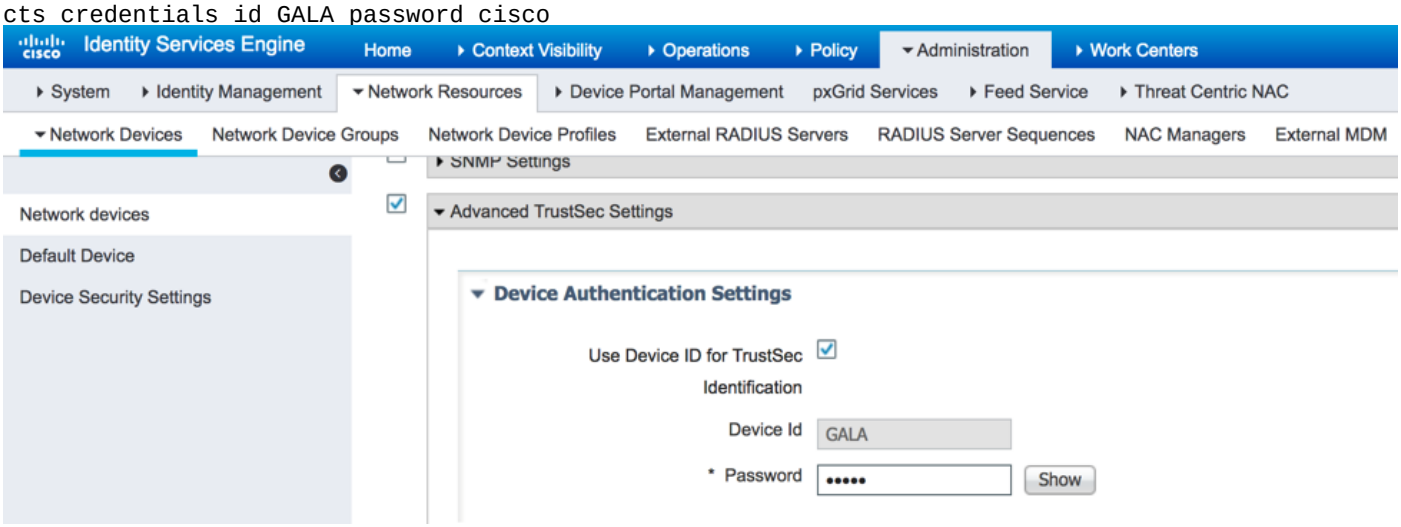
للحصول على معلومات CTS، يجب إنشاء قائمة تخويل CTS:

```
cts authorization list LIST
aaa authorization network LIST group ISE
```

2 - لجنة العمل الدائمة التابعة للجنة التقنية المعنية

لتلقي CTS PAC (بيانات اعتماد الوصول المحمي) من ISE، يجب تكوين نفس بيانات الاعتماد على المحول و ISE تحت تكوين TrustSec المتقدم لجهاز الشبكة:

```
cts credentials id GALA password cisco
```



وبمجرد تكوين هذا المحول، يمكن للمحول تنزيل مسوغ الوصول المحمي (PAC) ل CTS. يتم إرسال جزء واحد منه (PAC-Opaque) كزوج صوت/فيديو في كل طلب من RADIUS إلى ISE، لذلك يمكن ISE التحقق مما إذا كانت مسوغ الوصول المحمي لجهاز الشبكة هذا لا يزال صالحا:

```
GALA#show cts pacs
  AID: E6796CD7BBF2FA4111AD9FB4FEFB5A50
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: E6796CD7BBF2FA4111AD9FB4FEFB5A50
    I-ID: GALA
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:05:50 CEST Apr 5 2017
  PAC-Opaque:
000200B000030001000400010E6796CD7BBF2FA4111AD9FB4FEFB5A5000060094000300100012FABE10F3DCBCB152C54FA5
BFE124CB00000013586BB31500093A809E11A93189C7BE6EBDFB8FDD15B9B7252EB741ADCA3B2ACC5FD923AEB7BDFE48
A3A771338926A1F48141AF091469EE4AFC8C3E92A510BA214A407A33F469282A780E8F50F17A271E92D1FEE1A29ED427
B985F9A0E00D6CDC934087716F4DEAF84AC11AA05F7587E898CA908463BDA9EC7E65D827
  Refresh timer is set for 11y13w
```

3. تكوين CTS على محول ما.

بمجرد تنزيل مسوغ الوصول المحولات، يمكن للمحول طلب معلومات CTS إضافية (البيانات والسياسات البيئية):

```
GALA#cts refresh environment-data

GALA#show cts environment-data
CTS Environment Data
```

```
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-06:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.17.161, port 1812, A-ID E6796CD7BBF2FA4111AD9FB4FEFB5A50
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
    0-ce:Unknown
    2-ce:TrustSec_Devices
    3-ce:Network_Services
    4-ce:Employees
    5-ce:Contractors
    6-ce:Guests
    7-ce:Production_Users
    8-ce:Developers
    9-ce:Auditors
    10-ce:Point_of_Sale_Systems
    11-ce:Production_Servers
    12-ce:Development_Servers
    13-ce:Test_Servers
    14-ce:PCI_Servers
    15-ce:BYOD
    255-ce:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 07:48:41 CET Mon Jan 2 2006
Env-data expires in   0:23:56:02 (dd:hr:mm:sec)
Env-data refreshes in 0:23:56:02 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running

GALA#cts refresh policy

GALA#show cts role-based permissions
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

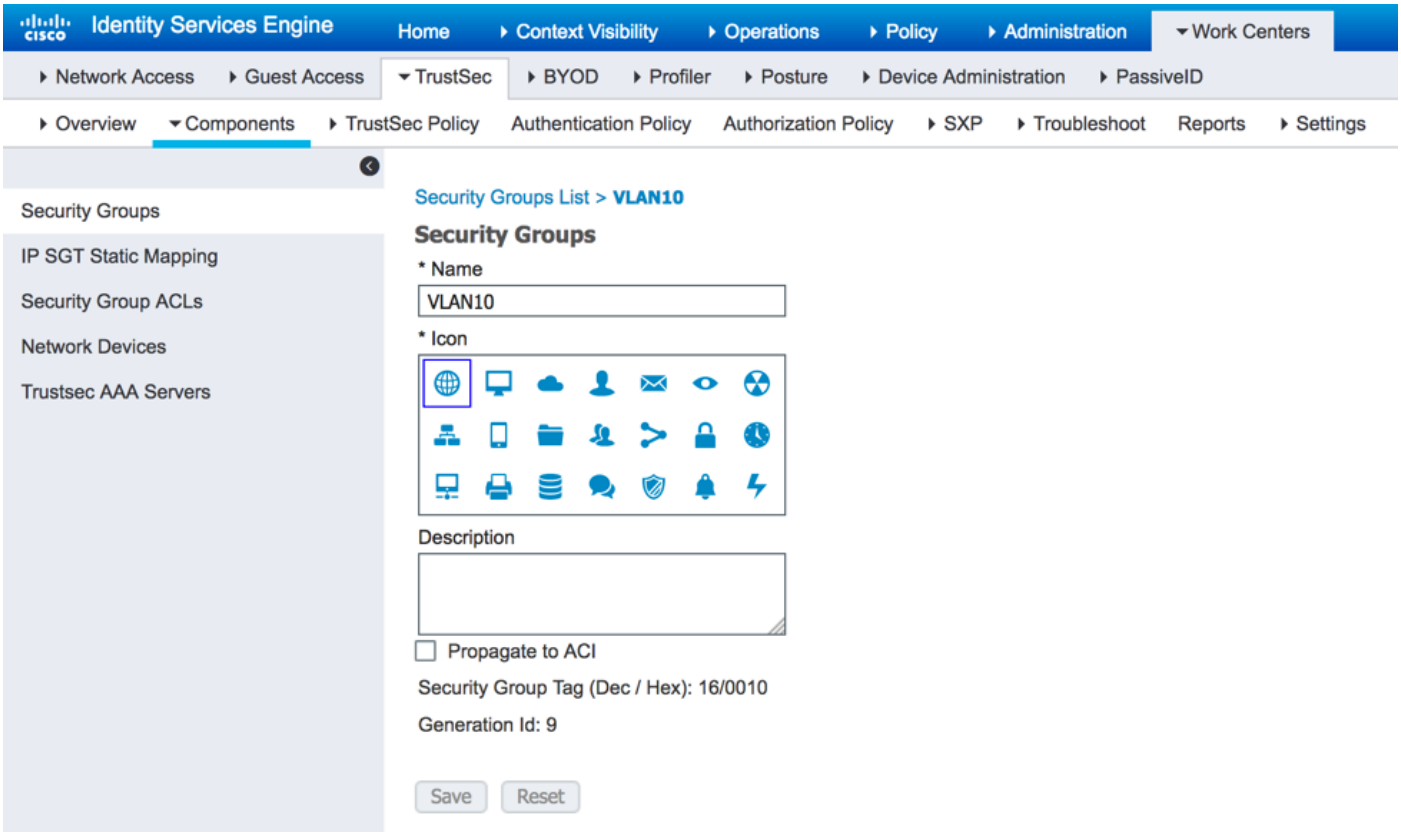
قد ترى أنه ال توجد سياسات قيد التنزيل من ISE، السبب هو أن تنفيذ CTS غير ممكن على المحول:

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-4094

GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

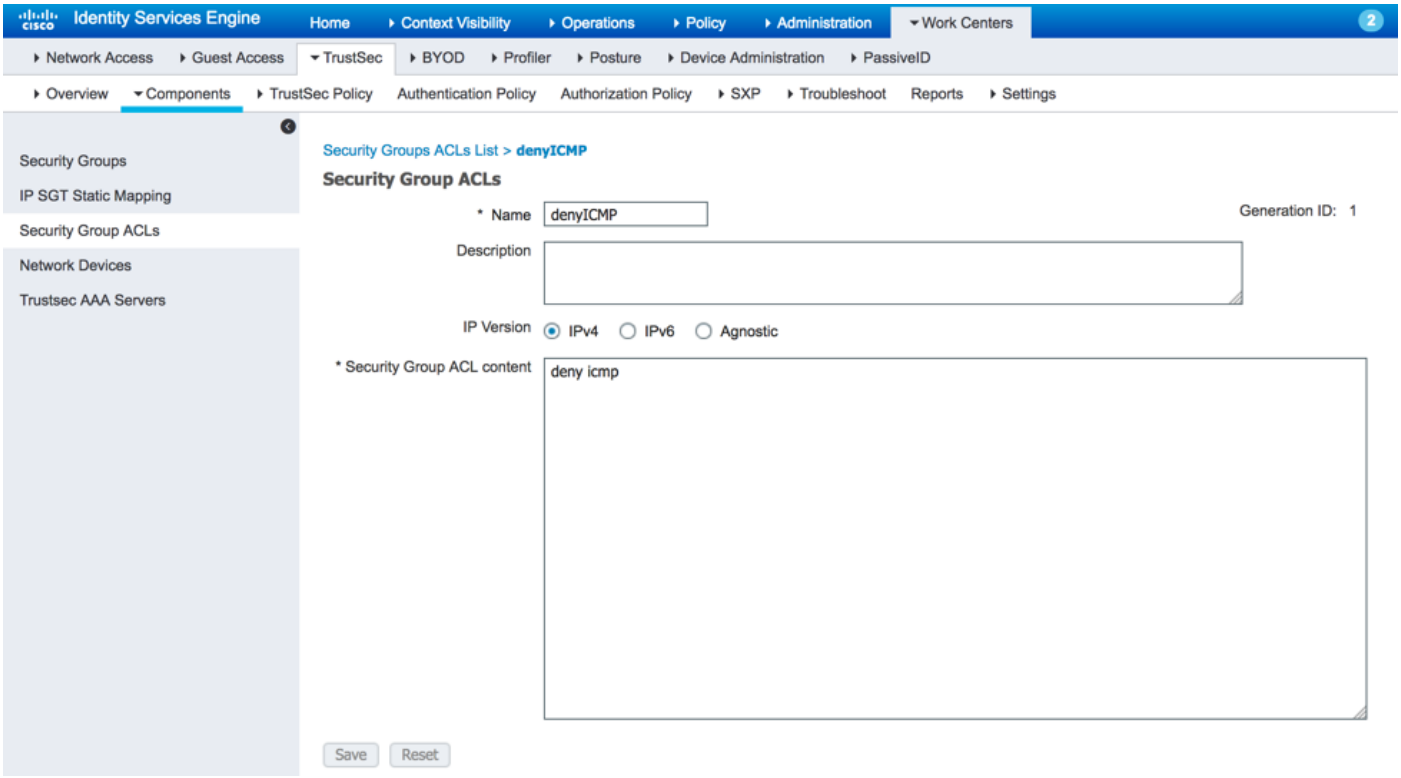
في الكل الإصدارين، يمكنك الاطلاع على القيم الافتراضية - تم إنشاء SGTs بشكل افتراضي (0، 2-15، 255) وتم توجيه IP للتصريح الافتراضي.

4. تكوين CTS الأساسي على ISE.

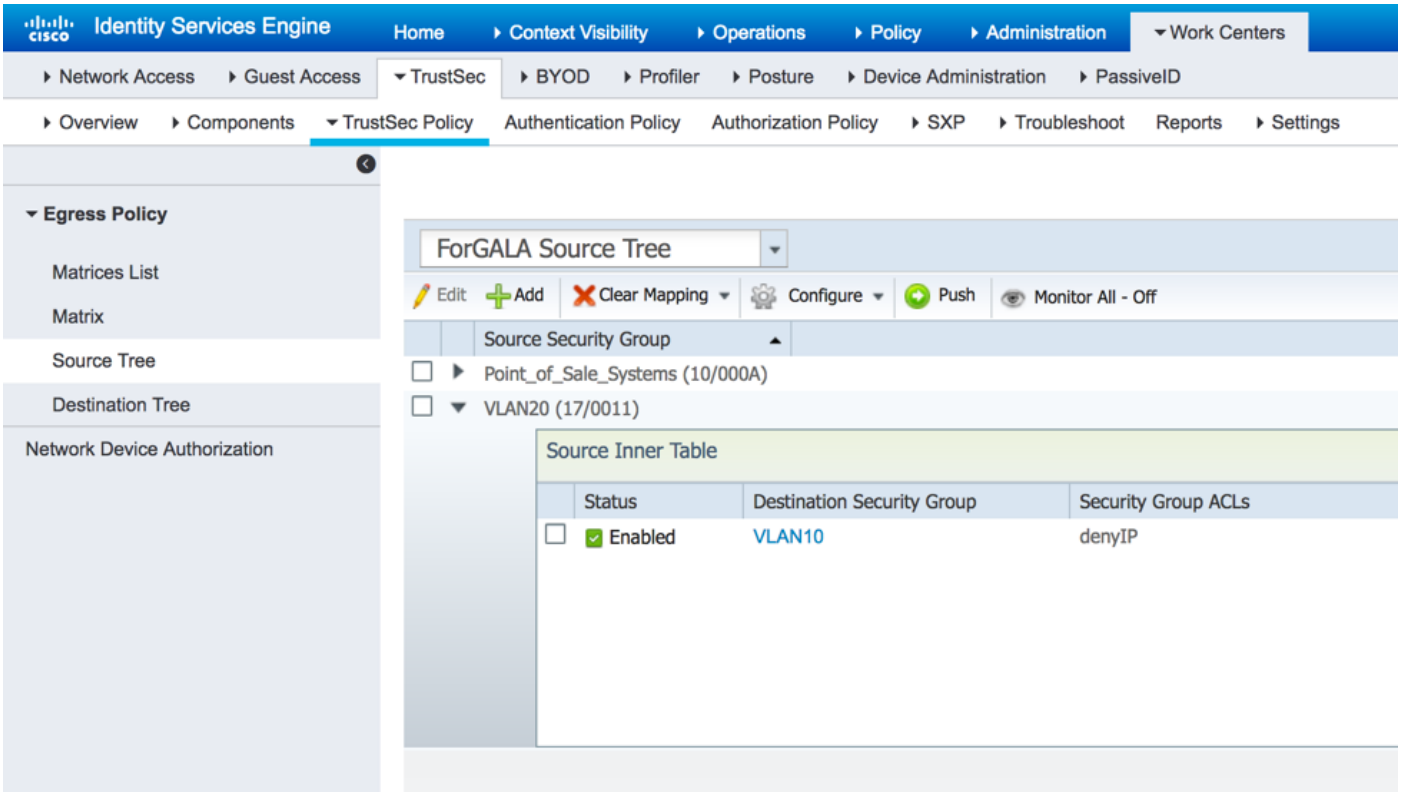
قم بإنشاء العلامات مجموعة أمان جديدة (SGTs) وقليل من السياسات على ISE لكي تستخدمها الحق. انتقل إلى **مراكز العمل > TrustSec > المكونات > مجموعات الأمان**، انقر فوق **إضافة** لإنشاء مساعد رقيب جديد:



لإنشاء قائمة التحكم في الوصول إلى مجموعة الأمان (SGACL) لتصفية حركة المرور، أخترقوائم التحكم في الوصول لمجموعة الأمان، كما هو موضح في الصورة:

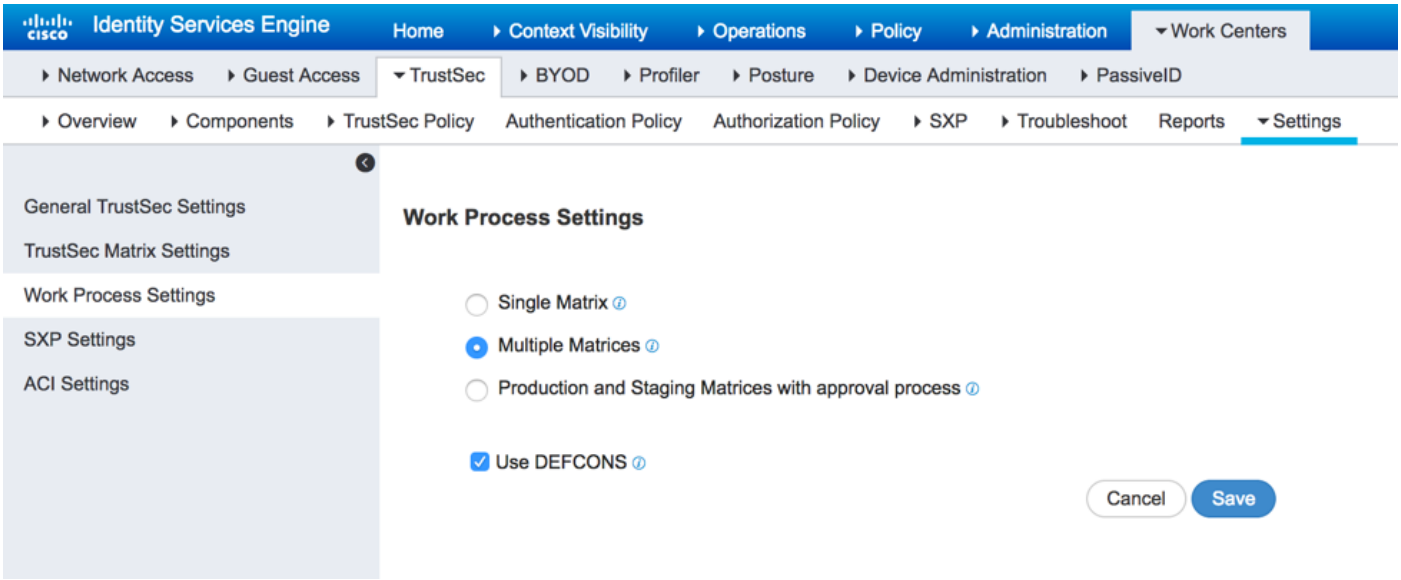


وبالمثل، يمكنك إنشاء مجموعات أخرى من الرقاب والقوائم الصغيرة الحجم القابلة للتجميع (SGACLs). بمجرد إنشاء SGTs و SGACLs، يمكنك ربطهم معا في سياسات CTS، للقيام بذلك، انتقل إلى مراكز العمل > TrustSec > سياسة TustSec > سياسة الخروج > شجرة المصدر، كما هو موضح في الصورة:



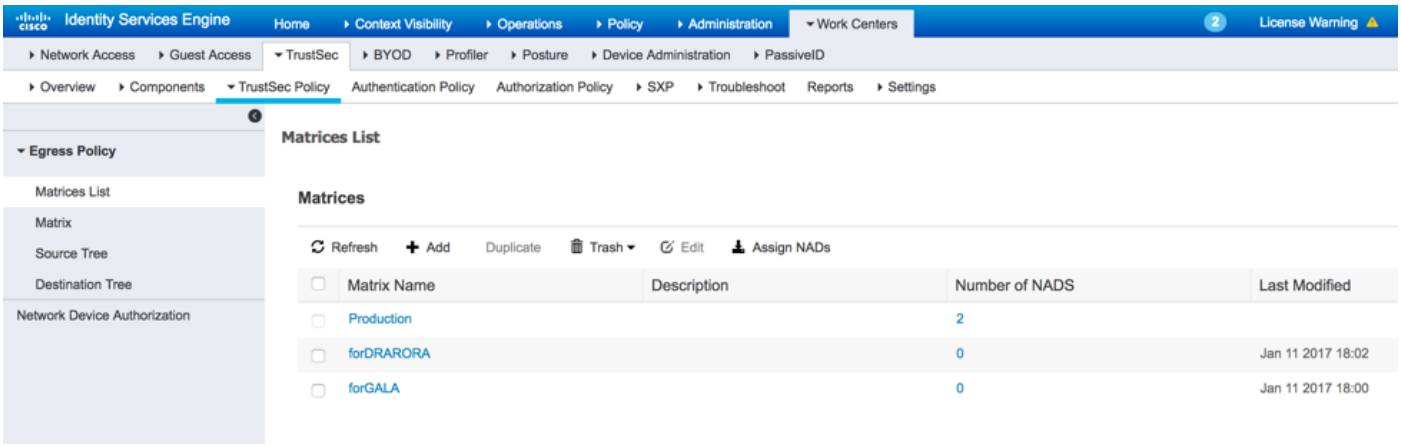
5. المصفوفات المتعددة وتكوين DefCon على ISE.

في هذا المثال، لقد قمت بتكوين سياسات ل **مصفوفة ل GALA**. للتبديل بين المصفوفات، يمكنك إستخدام القائمة المنسدلة. لتمكين مصفوفات متعددة، انتقل إلى **مراكز العمل > TrustSec > إعدادات > إعدادات عملية العمل** وتمكين مصفوفات متعددة ومصفوفات DefCon، كما هو موضح في الصورة:

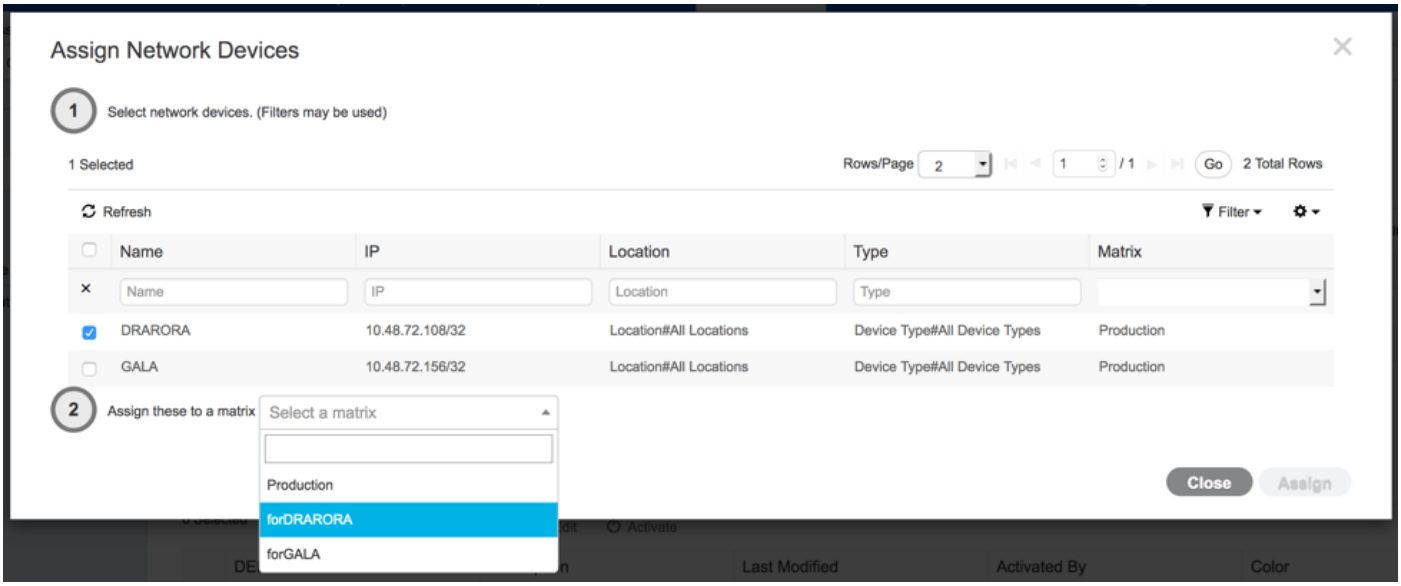


عند تمكين هذا الخيار، هناك مصفوفة إنتاج افتراضية متاحة، بالرغم من أنك قد تقوم بإنشاء مصفوفات أخرى. انتقل إلى **مراكز العمل > TrustSec > TrustSec Policy > Egress Policy > قائمة المصفوفات** وانقر **إضافة**:

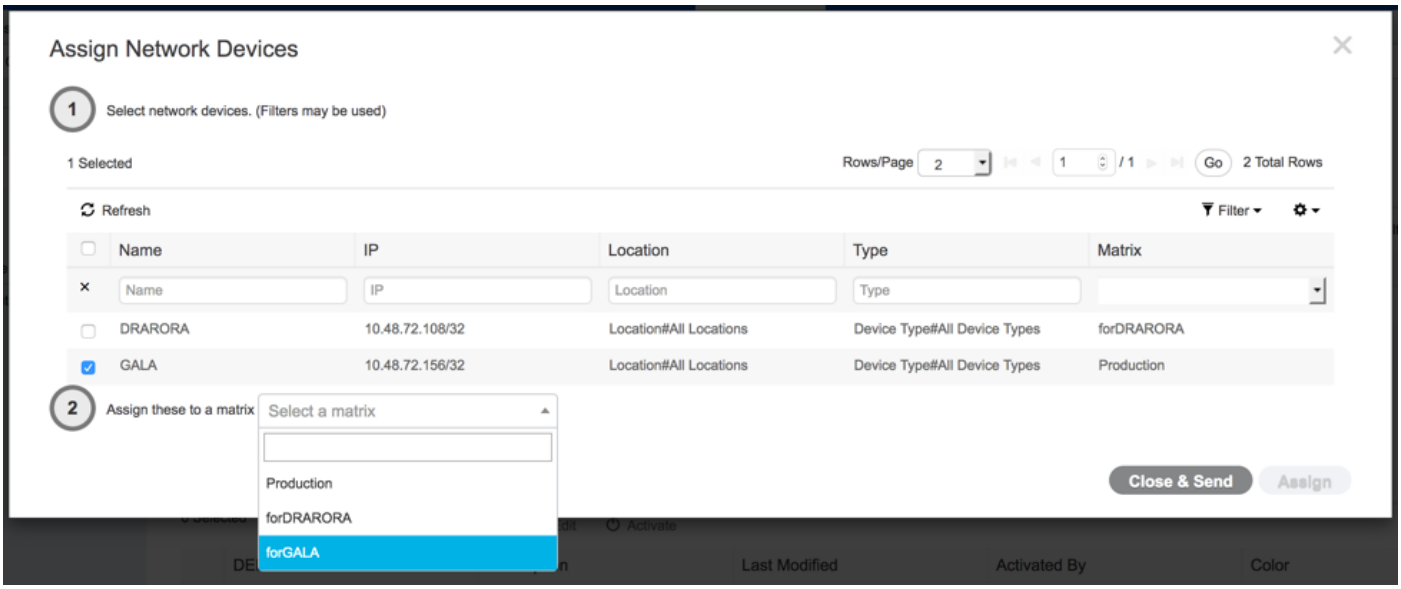
وهناك خيار لنسخ السياسات التي ينبغي أن تصبح جزءا من السياسات الجديدة من المصفوفة القائمة بالفعل. قم بإنشاء مصفوفتين - واحدة للموجل 3750X، والأخرى للموجل 3850. بمجرد إنشاء المصفوفات، يجب تعيين أجهزة الشبكة إلى هذه المصفوفات، لأنه بشكل افتراضي يتم تعيين جميع أجهزة الوصول إلى الشبكة التي تم تمكين TrustSec لها إلى مصفوفة الإنتاج.



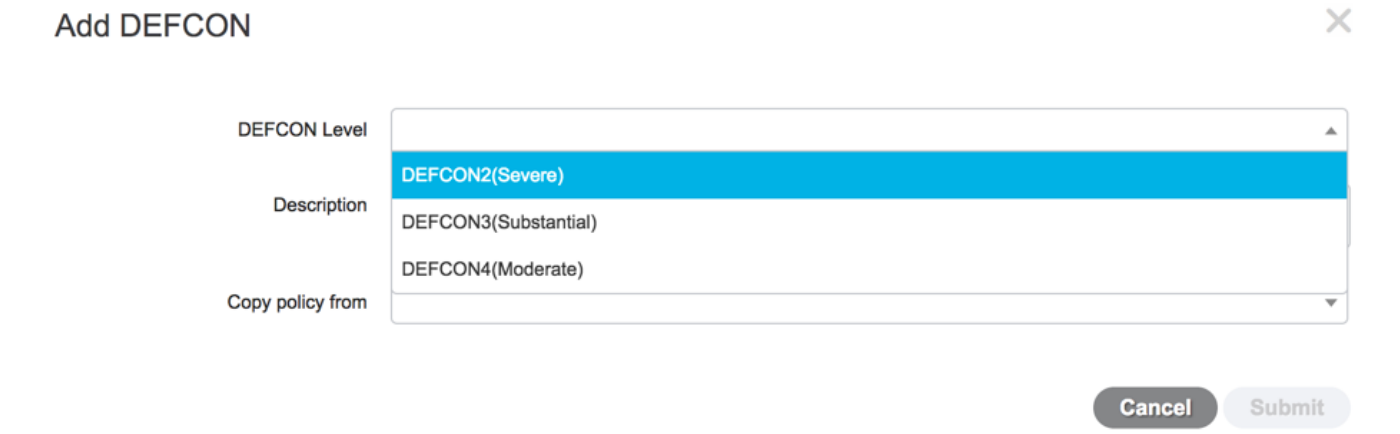
لتعيين NADs، انقر فوق **تعيين NAD** خيار ضمن قائمة المصفوفات، حدد الجهاز الذي تريد تعيين المصفوفة له واختر المصفوفة التي تم إنشاؤها من القائمة المنسدلة وانقر فوق **تعيين**، كما هو موضح في الصورة:



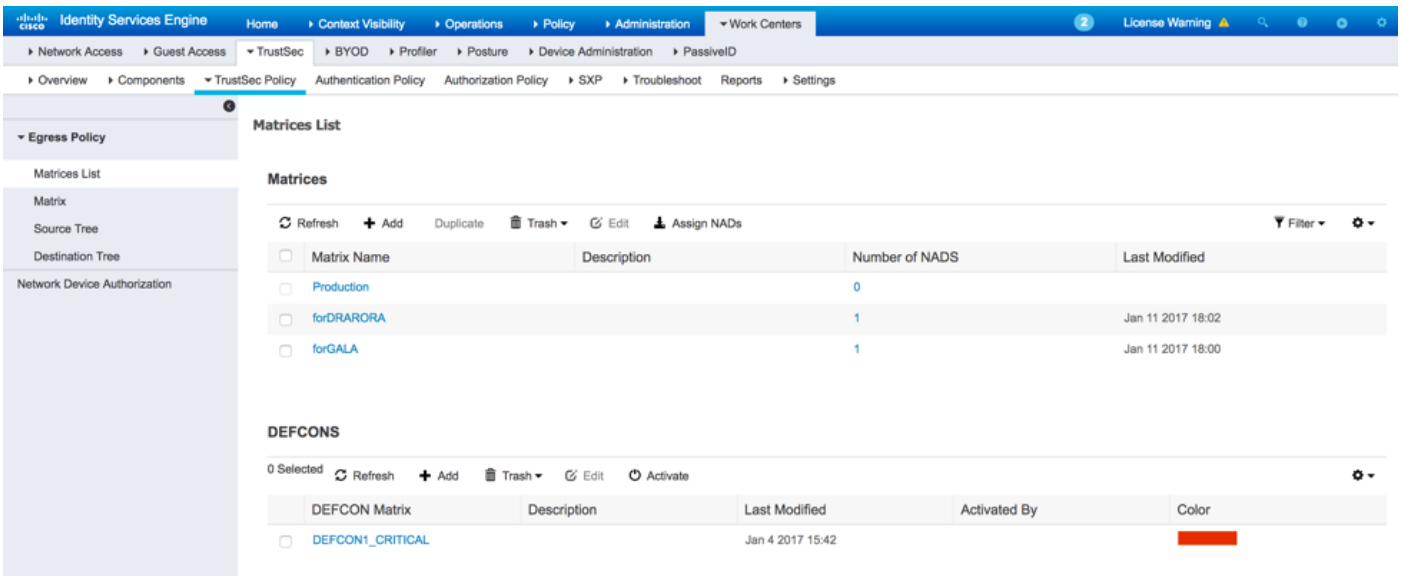
يمكنك تنفيذ نفس الإجراء للأجهزة الأخرى، متبوعا بالزر نقر على **تعيين**:



بمجرد تنفيذ جميع التغييرات، انقر فوق **إغلاق وإرسال**، الذي يرسل جميع التحديثات إلى الأجهزة لإجراء تحديث لنهج CTS لتنزيل أخرى جديدة. وبالمثل، قم بإنشاء مصفوفة DefCon، والتي يمكنك نسخها من المصفوفات الموجودة:



تبدو السياسات النهائية كما يلي:

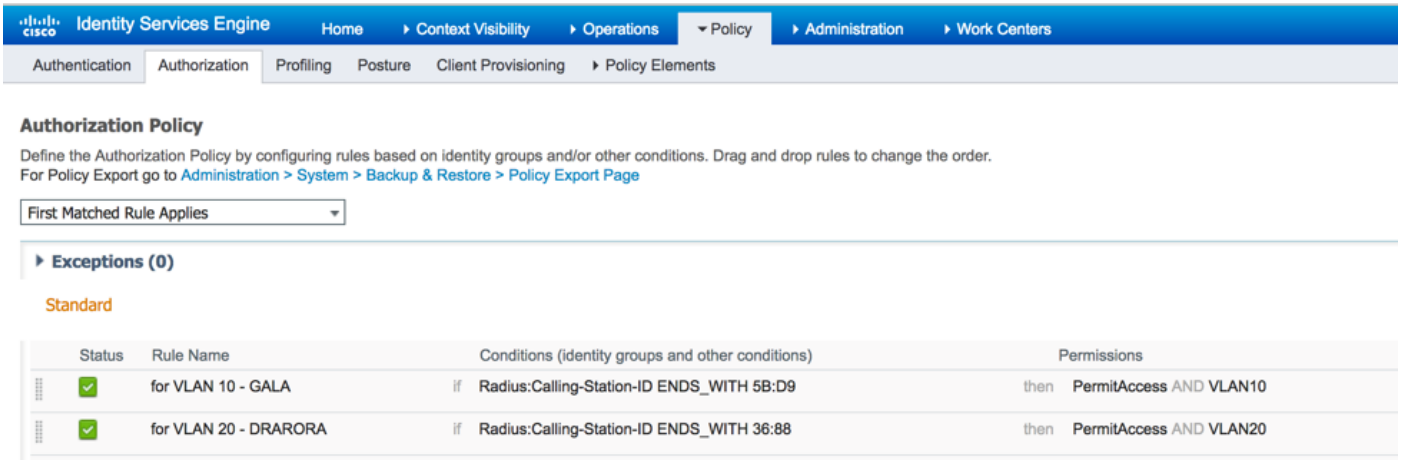


6 - تصنيف الرقيب

هناك خياران لعلامات التمييز لتعيينات العملاء (إنشاء تعيينات IP-SGT):

- *ساكن إستاتيكي* - مع ***بطاقة الرقيب IP_Address القائمة على الأدوار من CTS***
- *ديناميكية* - عبر مصادقة dot1x (يتم تعيين العلامة كنتيجة للمصادقة الناجحة)

أستخدم كلا الخيارين هنا، يحصل جهازان من Windows على علامة SGT عبر واجهات مصادقة dot1x و loopback مع علامة SGT ثابتة. لنشر التخطيط الديناميكي، قم بإنشاء سياسات تخويل للعملاء النهائيين:



لإنشاء تخطيط ساكن إستاتيكي ل IP-SGT، أستخدم الأوامر (مثال لمحول GALA):

```
interface Loopback7
 ip address 7.7.7.7 255.255.255.0

interface Loopback2
 ip address 2.2.2.2 255.255.255.0

cts role-based sgt-map 2.2.2.2 sgt 15
cts role-based sgt-map 7.7.7.7 sgt 10
```

بعد نجاح المصادقة، يقوم العميل بتنفيذ نهج التخويل برقم محدد للرقيب في إحدى النتائج:

```
GALA#show authentication sessions interface Gi1/0/11 details
            Interface:  GigabitEthernet1/0/11
          MAC Address:  0050.5699.5bd9
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.10.2
            User-Name:  00-50-56-99-5B-D9
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
   Common Session ID:  0A30489C000000120002330D
     Acct Session ID:  0x00000008
              Handle:  0xCE000001
      Current Policy:  POLICY_Gi1/0/11

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
```

```
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
            SGT Value:  16

Method status list:
       Method           State

       mab              Authc Success
```

يمكنك التحقق من جميع تعييناتIP-SGT باستخدام الأمر **show cts - تعيين قائم على الأدوار -** الكل، حيث ترى مصدر كل خطيط (محلي - عبر مصادقة dot1x، CLI - تعيين ثابت):

```
GALA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
2.2.2.2                 15      CLI
7.7.7.7                 10      CLI
10.0.10.2               16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of LOCAL    bindings = 1
Total number of active   bindings = 3
```

7. تنزيل سياسة CTS

بمجرد أن يحتوي المحول على مسوغات وصول محمي (CTS) وبيانات البيئة يتم تنزيلها، يمكن أن يطلب سياسات CTS. القوة المحول بتنزيل جميع السياسات، لكن فقط السياسات المطلوبة - سياسات حركة المرور الموجهة إلى عالمات SGT المعروفة - في حالة المحول GALA، فإنه يطلب من ISE تلك السياسات:

- سياسة المرور للرقيب 15
- سياسة المرور للرقيب العاشر
- سياسة المرور للرقيب 16

مخرجات كل السياسات لمحول GALA:

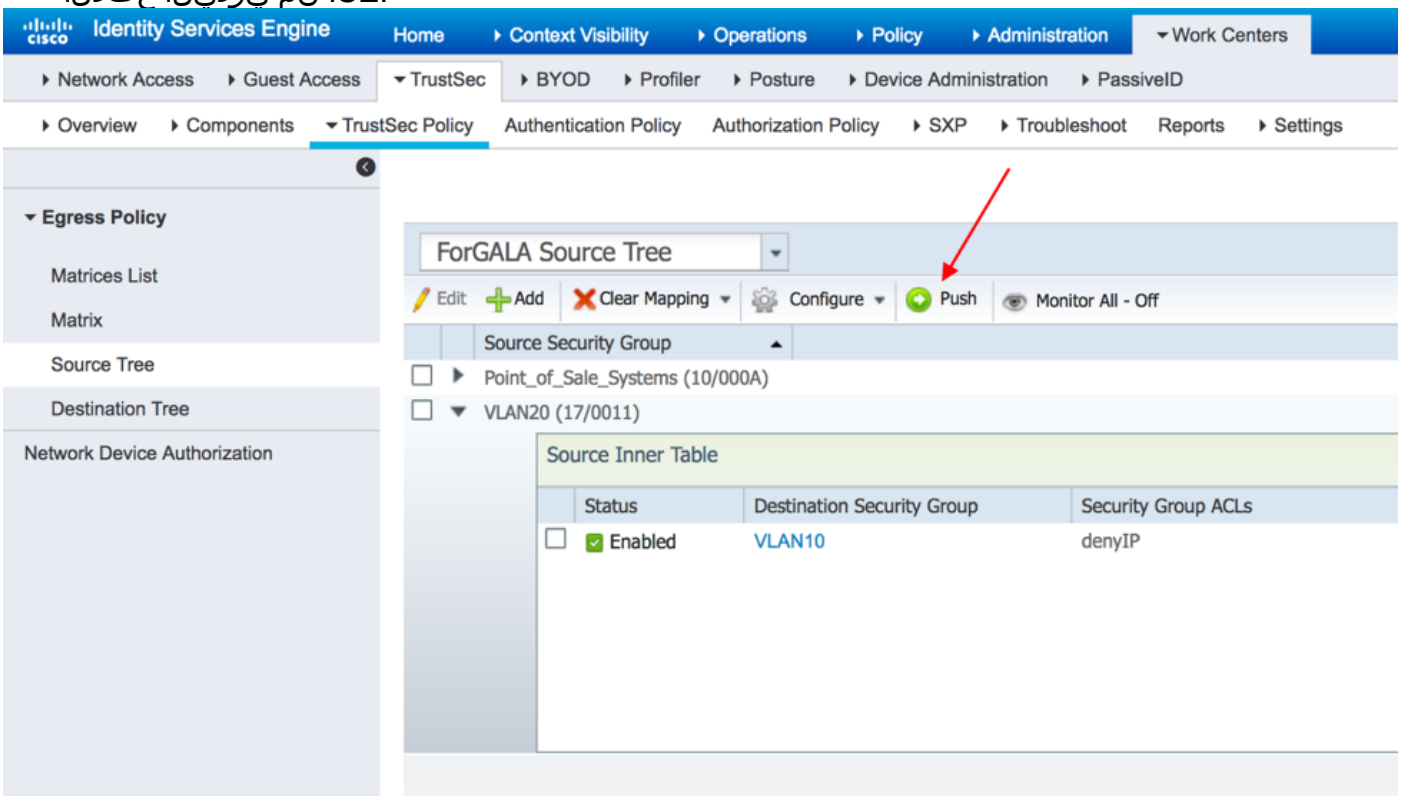
```
GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
denyIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

يحصل المحول على السياسات بطريقتين:

- تحديث CTS من المحول نفسه:

```
GALA#cts refresh policy
```

- الدفع اليدوي من ISE:



التحقق من الصحة

مصفوفات متعددة

التعيينات النهائية للربيب-IP وسياسات CTS على كل المحولين في هذا المثال:

المحول GALA:

```
GALA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
2.2.2.2                 15      CLI
7.7.7.7                 10      CLI
10.0.10.2               16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of LOCAL    bindings = 1
Total number of active   bindings = 3

GALA#show cts role-based permissions
IPv4 Role-based permissions default:
   Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
   denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
   permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
   permitIP-20
```

```
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

GALA#show cts rbacl | s permitIP
 name   = permitIP-20
   permit ip

GALA#show cts rbacl | s deny
 name   = denyIP-20
   deny ip
```

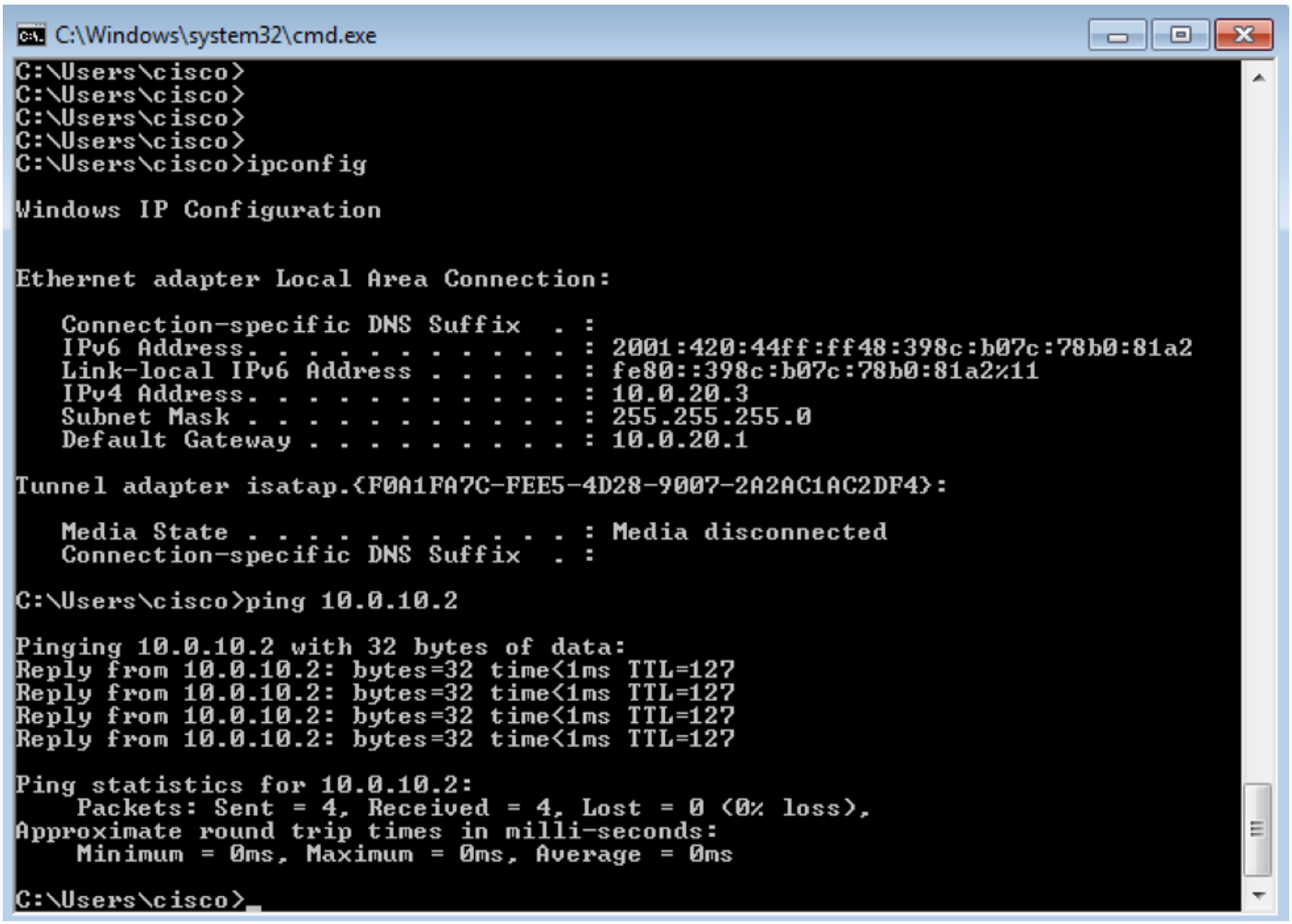
لوحم Drarora:

```
DRARORA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.0.20.3               17      LOCAL
10.10.10.10             10      CLI
15.15.15.15             15      CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of LOCAL    bindings = 1
Total number of active   bindings = 3

DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
   Permit IP-00
IPv4 Role-based permissions from group 17:VLAN20 to group 10:Point_of_Sale_Systems:
   permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
   permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
   permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
   denyIP-20
IPv4 Role-based permissions from group 16:VLAN10 to group 17:VLAN20:
   permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

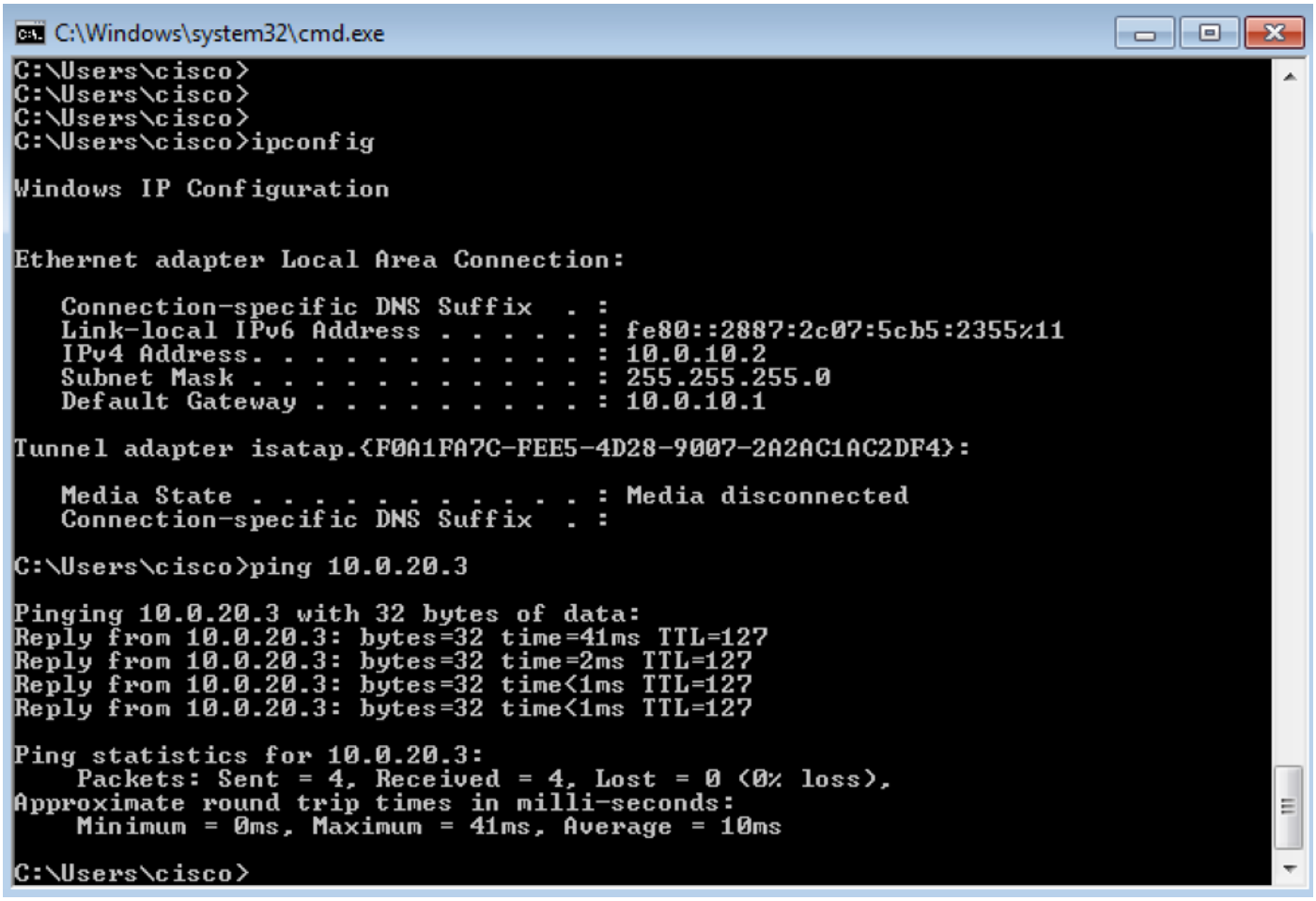
لاحظ أن السياسات الخاصة بكل المحولين مختلفة (حتى أن السياسة نفسها من 10 إلى 15 مختلفة بالنسبة لمحول GALA و DRARORA). وهذا يعني أن المرور من الرقيب 10 إلى 15 مسموح به على درارورا ولكنه ممنوع على التجول:

```
DRARORA#ping 15.15.15.15 source Loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.15.15.15, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

GALA#ping 2.2.2.2 source Loopback 7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
U.U.U
Success rate is 0 percent (0/5)
```

وبالمثل، من نافذة واحدة، يمكنك الوصول إلى نافذة أخرى (الرقيب 17 -> الرقيب 16):



وطريقة أخرى (الرقيب 16 -> الرقيب 17):



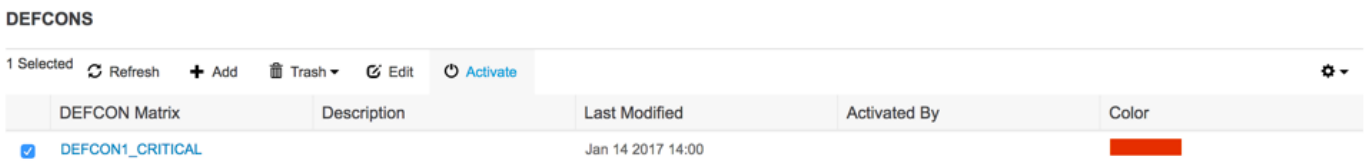
لتأكيد تطبيق نهج CTS الصحيح، تحقق من إخراج العدادات **المستندة إلى الأدوار** show cts:

```
GALA#sh 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

17      16      0               0               0               8
17      15      0               -               0               -

10      15      4               0               0               0

*       *       0               0               127             26
```

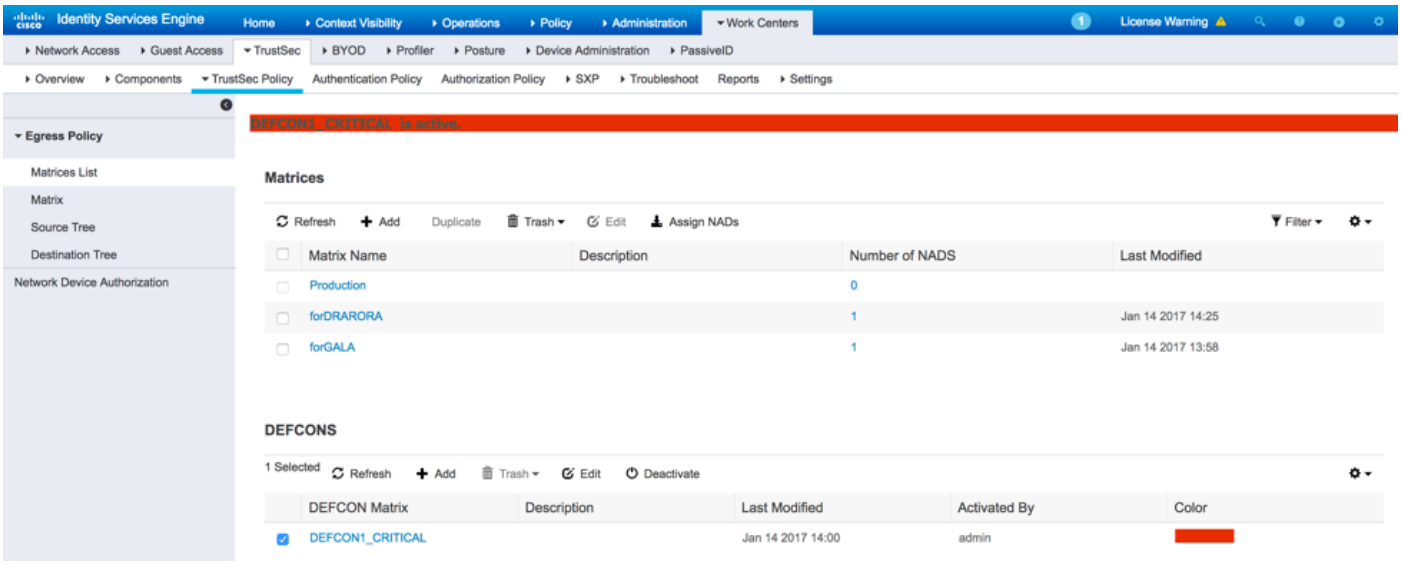
تحتوي GALA على 8 حزم مسموح بها (4 من ping 16->17 و 4 من ping 17->16).

نشر DefCon

عند الحاجة، قم بنشر مصفوفة DefCon تحت **مراكز العمل > TrustSec > TrustSec Policy > Egress Policy > قائمة المصفوفات**، تحقق من مصفوفة DefCon التي تريد تنشيطها وانقر فوق **تنشيط**:



بمجرد تنشيط DefCon، تبدو القائمة في ISE كما يلي:



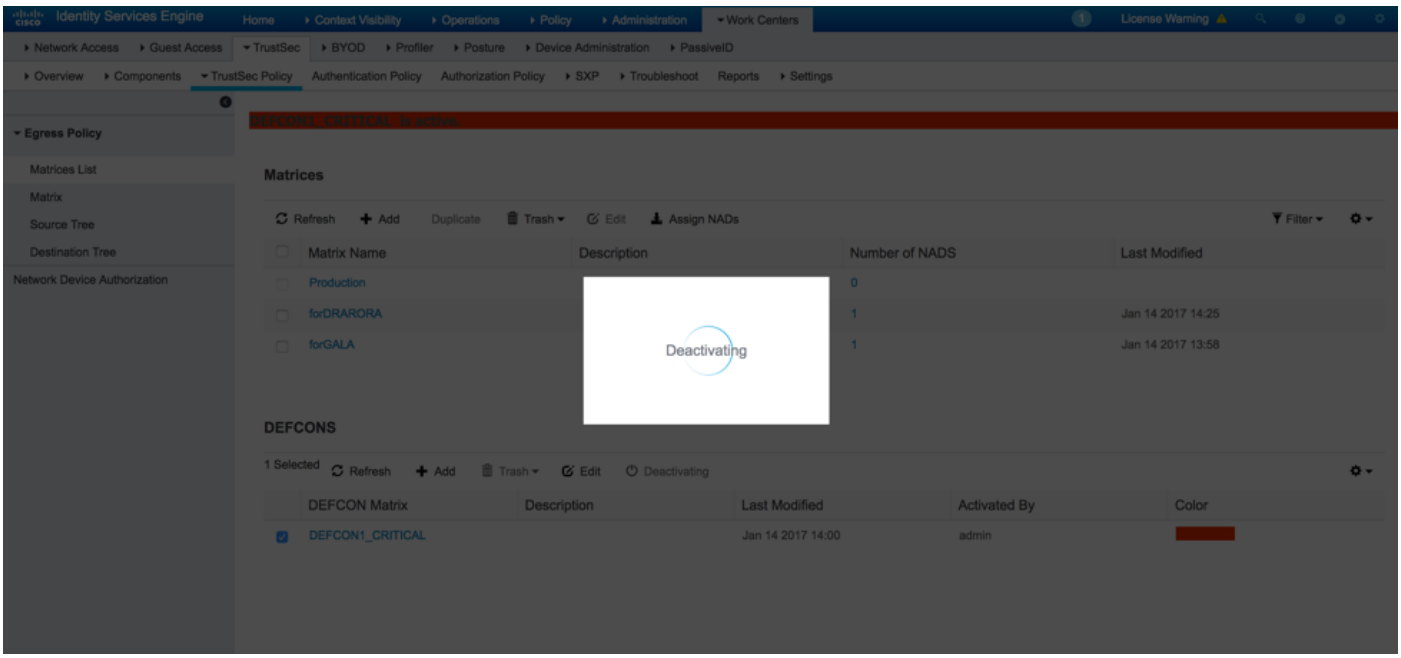
وسياسات حول المحولات:

```
GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems:
denyIP-20
IPv4 Role-based permissions from group 15:BYOD to group 16:VLAN10:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
denyIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems:
denyIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

غير مسموح بحركة المرور من الرقيب 15 إلى الرقيب 10 على كل المحولين:

```
DRARORA#ping 10.10.10.10 source Loopback 15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
Packet sent with a source address of 15.15.15.15
U.U.U
Success rate is 0 percent (0/5)

GALA#ping 7.7.7.7 source Loopback 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
U.U.U
Success rate is 0 percent (0/5)
```

بمجرد إستقرار النشر مرة أخرى، يمكنك إلغاء تنشيط DefCon وطلب المحولات النهج القديمة. لإلغاء تنشيط DefCon، انتقل إلى **مراكز العمل > TrustSec > TrustSec Policy > Egress Policy > قائمة المصفوفات**، تحقق من مصفوفة DefCon النشطة وانقر فوق **إلغاء التنشيط**:



يقوم كل المحولين بطلب السياسات القديمة على الفور:

```
DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 17:VLAN20 to group 10:Point_of_Sale_Systems:
permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
denyIP-20
IPv4 Role-based permissions from group 16:VLAN10 to group 17:VLAN20:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

استكشاف الأخطاء وإصلاحها

إمداد PAC

يعد هذا جزءا من إعداد مسوغ الوصول المحمي (PAC) الناجح:

```
GALA#debug cts provisioning packets
GALA#debug cts provisioning events

*Jan  2 04:39:05.707: %SYS-5-CONFIG_I: Configured from console by console
*Jan  2 04:39:05.707: CTS-provisioning: Starting new control block for server 10.48.17.161:
*Jan  2 04:39:05.707: CTS-provisioning: cts_provi_init_socket: Checking for any vrf associated
with 10.48.17.161
*Jan  2 04:39:05.707: CTS-provisioning: New session socket: src=10.48.72.156:65242
dst=10.48.17.161:1812
*Jan  2 04:39:05.716: CTS-provisioning: cts_provi_init_socket: Checking for any vrf associated
with 10.48.17.161
*Jan  2 04:39:05.716: CTS-provisioning: cts_provi_init_socket: Adding vrf-tableid: 0 to socket
*Jan  2 04:39:05.716: CTS-provisioning: New session socket: src=10.48.72.156:65242
dst=10.48.17.161:1812
*Jan  2 04:39:05.716: CTS-provisioning: Sending EAP Response/Identity to 10.48.17.161
*Jan  2 04:39:05.716: CTS-provisioning: OUTGOING RADIUS msg to 10.48.17.161:
1E010EE0:          01010090 64BCBC01 7BEF347B
1E010EF0: 1E32C02E 8402A83D 010C4354 5320636C
1E010F00: 69656E74 04060A30 489C3D06 00000000
1E010F10: 06060000 00021F0E 30303037 37643862
1E010F20: 64663830 1A2D0000 00090127 4141413A
1E010F30: 73657276 6963652D 74797065 3D637473
1E010F40: 2D706163 2D70726F 76697369 6F6E696E
1E010F50: 674F1102 00000F01 43545320 636C6965
1E010F60: 6E745012 73EBE7F5 CDA0CF73 BFE4AFB6
1E010F70: 40D723B6 00
*Jan  2 04:39:06.035: CTS-provisioning: INCOMING RADIUS msg from 10.48.17.161:
1EC68460:          0B0100B5 E4C3C3C1 ED472766
1EC68470: 183F41A9 026453ED 18733634 43504D53
1EC68480: 65737369 6F6E4944 3D306133 30313161
1EC68490: 314C3767 78484956 62414976 37316D59
1EC684A0: 525F4D56 34517741 4C362F69 73517A72
1EC684B0: 7A586132 51566852 79635638 3B343353
1EC684C0: 65737369 6F6E4944 3D766368 72656E65
1EC684D0: 6B2D6973 6532322D 3432332F 32373238
1EC684E0: 32373637 362F3137 37343B4F 1C017400
1EC684F0: 1A2B2100 040010E6 796CD7BB F2FA4111
1EC68500: AD9FB4FE FB5A5050 124B76A2 E7D34684
1EC68510: DD8A1583 175C2627 9F00
*Jan  2 04:39:06.035: CTS-provisioning: Received RADIUS challenge from 10.48.17.161.
*Jan  2 04:39:06.035: CTS-provisioning: A-ID for server 10.48.17.161 is
"e6796cd7bbf2fa4111ad9fb4fefb5a50"
*Jan  2 04:39:06.043: CTS-provisioning: Received TX_PKT from EAP method
*Jan  2 04:39:06.043: CTS-provisioning: Sending EAPFAST response to 10.48.17.161
*Jan  2 04:39:06.043: CTS-provisioning: OUTGOING RADIUS msg to 10.48.17.161:
<...>
*Jan  2 04:39:09.549: CTS-provisioning: INCOMING RADIUS msg from 10.48.17.161:
1EC66C50:          0309002C 1A370BBB 58B828C3
1EC66C60: 3F0D490A 4469E8BB 4F06047B 00045012
1EC66C70: 7ECF8177 E3F4B9CB 8B0280BD 78A14CAA
1EC66C80: 4D
*Jan  2 04:39:09.549: CTS-provisioning: Received RADIUS reject from 10.48.17.161.
*Jan  2 04:39:09.549: CTS-provisioning: Successfully obtained PAC for A-ID
e6796cd7bbf2fa4111ad9fb4fefb5a50
```

من المتوقع رفض RADIUS نظرا لانتهاء إعداد مسوغ الوصول المحمي (PAC) بنجاح.

تنزيل بيانات البيئة

هذا يبدي ال ناجح بيئة تنزيل معطيات من المفتاح:

```
GALA#debug cts environment-data

GALA#
*Jan  2 04:33:24.702: CTS env-data: Force environment-data refresh
*Jan  2 04:33:24.702: CTS env-data: download transport-type = CTS_TRANSPORT_IP_UDP
*Jan  2 04:33:24.702:     cts_env_data START: during state env_data_complete, got event
0(env_data_request)

*Jan  2 04:33:24.702: cts_aaa_attr_add: AAA req(0x5F417F8)
*Jan  2 04:33:24.702:   username = #CTSREQUEST#
*Jan  2 04:33:24.702: cts_aaa_context_add_attr: (CTS env-data SM)attr(GALA)
*Jan  2 04:33:24.702:   cts-environment-data = GALA
*Jan  2 04:33:24.702: cts_aaa_attr_add: AAA req(0x5F417F8)
*Jan  2 04:33:24.702: cts_aaa_context_add_attr: (CTS env-data SM)attr(env-data-fragment)
*Jan  2 04:33:24.702:   cts-device-capability = env-data-fragment
*Jan  2 04:33:24.702: cts_aaa_req_send: AAA req(0x5F417F8) successfully sent to AAA.
*Jan  2 04:33:25.474: cts_aaa_callback: (CTS env-data SM)AAA req(0x5F417F8) response success
*Jan  2 04:33:25.474: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(GALA)
*Jan  2 04:33:25.474: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(env-data-fragment)

*Jan  2 04:33:25.474:   AAA attr: Unknown type (450).
*Jan  2 04:33:25.474:   AAA attr: Unknown type (274).
*Jan  2 04:33:25.474:   AAA attr: server-list = CTSServerList1-0001.
*Jan  2 04:33:25.482:   AAA attr: security-group-tag = 0000-10.
*Jan  2 04:33:25.482:   AAA attr: environment-data-expiry = 86400.
*Jan  2 04:33:25.482:   AAA attr: security-group-table = 0001-19.
*Jan  2 04:33:25.482: CTS env-data: Receiving AAA attributes
  CTS_AAA_SLIST
    slist name(CTSServerList1) received in 1st Access-Accept
    slist name(CTSServerList1) created
  CTS_AAA_SECURITY_GROUP_TAG - SGT = 0-10:unicast-unknown
  CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
  CTS_AAA_SGT_NAME_LIST
    table(0001) received in 1st Access-Accept
    need a 2nd request for the SGT to SG NAME entries
    new name(0001), gen(19)
  CTS_AAA_DATA_END

*Jan  2 04:33:25.784: cts_aaa_callback: (CTS env-data SM)AAA req(0x8853E60) response success
*Jan  2 04:33:25.784: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(0001)
*Jan  2 04:33:25.784:   AAA attr: Unknown type (450).
*Jan  2 04:33:25.784:   AAA attr: Unknown type (274).
*Jan  2 04:33:25.784:   AAA attr: security-group-table = 0001-19.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 0-10-00-Unknown.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = ffff-13-00-ANY.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 9-10-00-Auditors.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = f-32-00-BYOD.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 5-10-00-Contractors.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 8-10-00-Developers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = c-10-00-Development_Servers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 4-10-00-Employees.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 6-10-00-Guests.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 3-10-00-Network_Services.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = e-10-00-PCI_Servers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = a-23-00-Point_of_Sale_Systems.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = b-10-00-Production_Servers.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 7-10-00-Production_Users.
```

```
*Jan  2 04:33:25.793:   AAA attr: security-group-info = ff-10-00-Quarantined_Systems.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = d-10-00-Test_Servers.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 2-10-00-TrustSec_Devices.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 10-24-00-VLAN10.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 11-22-00-VLAN20.
*Jan  2 04:33:25.793:  CTS env-data: Receiving AAA attributes
  CTS_AAA_SGT_NAME_LIST
    table(0001) received in 2nd Access-Accept
    old name(0001), gen(19)
    new name(0001), gen(19)
  CTS_AAA_SGT_NAME_INBOUND - SGT = 0-68:unicast-unknown
   flag (128) sgname (Unknown) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 65535-68:unicast-default
   flag (128) sgname (ANY) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 9-68
   flag (128) sgname (Auditors) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 15-68
   flag (128) sgname (BYOD) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 5-68
   flag (128) sgname (Contractors) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 8-68
   flag (128) sgname (Developers) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 12-68
   flag (128) sgname (Development_Servers) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 4-68
   flag (128) sgname (Employees) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, na
*Jan  2 04:33:25.793:     cts_env_data WAITING_RESPONSE: during state env_data_waiting_rsp, got
event 1(env_data_received)
*Jan  2 04:33:25.793: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Jan  2 04:33:25.793: env_data_assessing_enter: state = ASSESSING
*Jan  2 04:33:25.793: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)
*Jan  2 04:33:25.793: env_data_assessing_action: state = ASSESSING
*Jan  2 04:33:25.793: cts_env_data_is_complete: FALSE, req(x1085), rec(x1487)
*Jan  2 04:33:25.793: cts_env_data_is_complete: TRUE, req(x1085), rec(x1487), expect(x81),
complete1(x85), complete2(xB5), complete3(x1485)
*Jan  2 04:33:25.793:     cts_env_data ASSESSING: during state env_data_assessing, got event
4(env_data_complete)
*Jan  2 04:33:25.793: @@@ cts_env_data ASSESSING: env_data_assessing -> env_data_complete
*Jan  2 04:33:25.793: env_data_complete_enter: state = COMPLETE
*Jan  2 04:33:25.793: env_data_install_action: state = COMPLETE
```

سياسات CTS

يتم دفع سياسات CTS كجزء من رسائل RADIUS، لذلك يجب أن يكون مكون تسجيل **وقت التشغيل AAA** الذي تم تعيينه لتصحيح أخطاء ISE (**الإدارة > التسجيل > تكوين سجل الأخطاء**) والتصحيح أدناه على المحول كافيا لاستكشاف أخطاء أي مشاكل متعلقة ب CTS وإصلاحها:

```
debug cts coa
debug radius
```

بالإضافة إلى ذلك، تحقق من السياسات المطابقة على المحول - على 3750X:

```
GALA#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

10      15      5               0               0               0

*       *       0               0               815             31

17      15      0               0               0               0
17      16      0               -               0               -
```

أنت لا يستطيع أن يستعمل نفسه أمر على 3850، بسبب CiscoBUGid CSCuu32958.

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).