تكوين عمليات ASA 9.3.1 TrustSec المضمنة

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام الميزة التي تم تنفيذها في وضع علامة داخل جهاز الأمان القابل للتكيف (ASA) الإصدار 9.3.1 - TrustSec. وتتيح هذه الميزة ل ASA إمكانية تلقي إطارات TrustSec وكذلك إرسالها. بهذه الطريقة يمكن دمج ASA بسهولة داخل مجال TrustSec دون الحاجة إلى إستخدام بروتوكول TrustSec Sgt Exchange (SXP).

يقدم هذا المثال مستخدم شبكة VPN عن بعد تم تعيين علامة مجموعة الأمان (SGT) له = 3 (التسويق) و 802.1x للمستخدم الذي تم تعيين العلامة الرقيب لها = 2 (الشؤون المالية). يتم تنفيذ حركة المرور بواسطة كل من ASA باستخدام قائمة التحكم في الوصول إلى مجموعة الأمان (SGACL) المحددة محليا ومحول Cisco IOS® باستخدام قائمة التحكم في الوصول المستندة إلى الأدوار (RBACL) التي تم تنزيلها من محرك خدمات الهوية (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين ASA CLI وتكوين طبقة مأخذ التوصيل الآمنة (SSL) VPN
- تكوين VPN للوصول عن بعد على ASA
- خدمات ISE و TrustSec

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- برنامج Cisco ASA، الإصدار 9.3.1 والإصدارات الأحدث
- أجهزة Cisco ASA 55x5 أو ASAv
- نظام التشغيل Windows 7 مع Cisco AnyConnect Secure Mobility Client، الإصدار 3.1
- المحول Cisco Catalyst 3750X switch ببرنامج 15.0.2 والإصدارات الأحدث
- Cisco ISE، الإصدار 1.2 والإصدارات الأحدث

التكوين

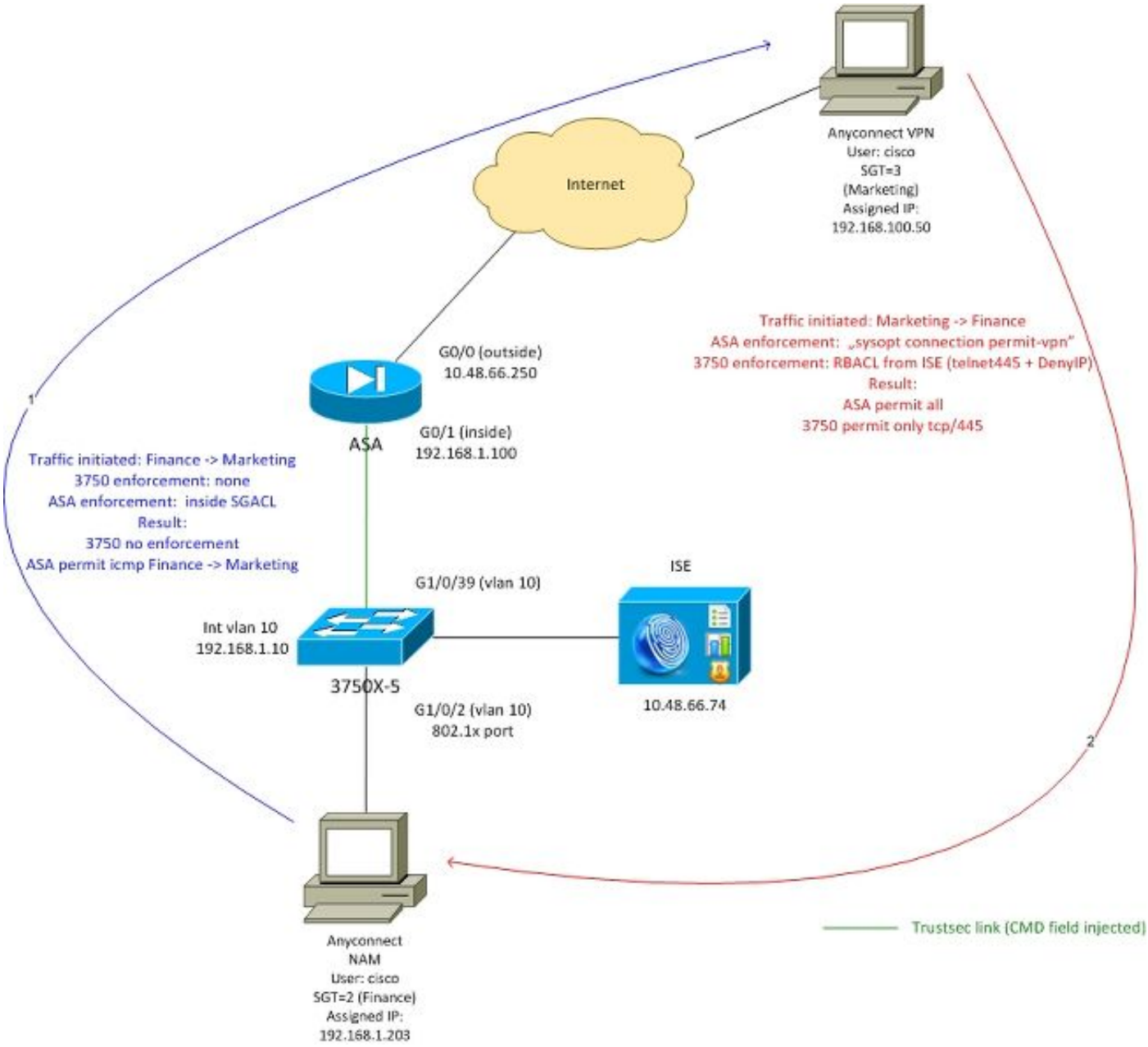
ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يتم تكوين الاتصال بين ASA و 3750X ل CTS اليدوي. وهذا يعني أن كلا الجهازين يمكن أن يرسل ويستلم إطارات إيثرنت معدلة باستخدام حقل بيانات تعريف Cisco (CMD). يشمل ذلك الحقل علامة مجموعة الأمان (SGT) التي تصف مصدر الحزمة.

ينهي مستخدم شبكة VPN البعيدة جلسة SSL على ASA ويعين له رقيب رقم 3 (التسويق).

تم تعيين رمز SGT رقم 2 لمستخدم الشركات المحلية بدقة 802.1x بعد إجراء المصادقة الناجحة (الشؤون المالية).



تم تكوين ASA SGACL على الواجهة الداخلية التي تسمح بحركة مرور ICMP التي يتم استهلالها من Finance إلى Marketing.

يسمح ASA بجميع حركة المرور التي تم بدؤها من إزالة مستخدم شبكة VPN (بسبب تكوين "sysopt connection allowed-vpn").

SGACL على ASA هي حالة تعني أنه بمجرد إنشاء التدفق، يتم قبول الحزمة العائدة تلقائيا (استنادا إلى الفحص).

يستخدم المحول 3750 switch RBACL للتحكم في حركة المرور المستلمة من Marketing to Finance.

RBACL عديم الحالة مما يعني أنه يتم التحقق من كل حزمة ولكن يتم تنفيذ TrustSec على نظام 3750X الأساسي في الوجهة. محول هذه الطريقة مسؤول عن فرض حركة المرور من التسويق إلى التمويل.

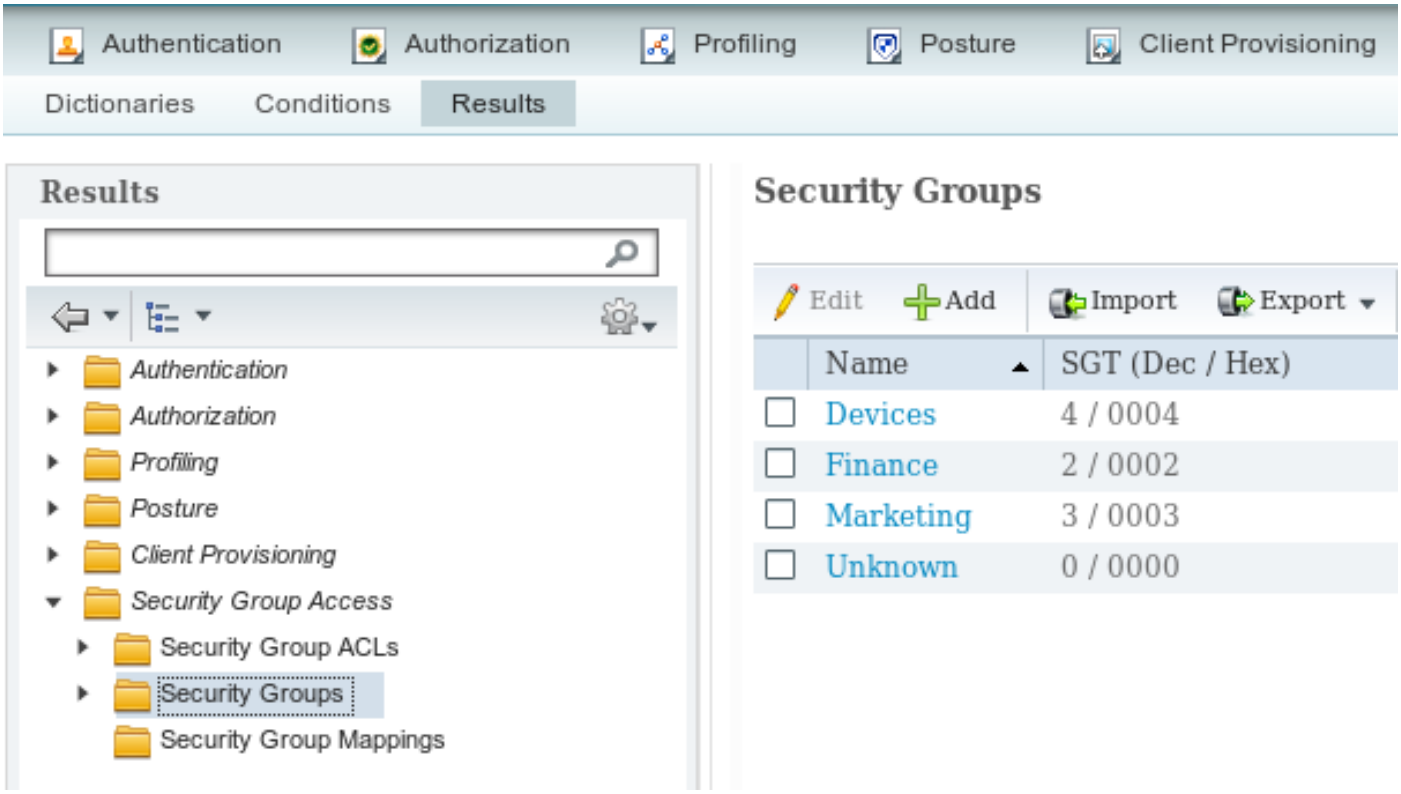
ملاحظة: يمكن إستخدام جدار الحماية المستند إلى منطقة Cisco IOS® Zone على سبيل المثال، ارجع إلى:

ملاحظة: يمكن أن يحتوي ASA على SGACL الذي يتحكم في حركة المرور التي تأتي من مستخدم شبكة VPN البعيدة. ولتبسيط السيناريو، لم يقدم في هذه المقالة. على سبيل المثال، ارجع إلى: ASA الإصدار 9.2 VPN Sgt Classification and Enforcement Configuration Example

ISE - خطوات التكوين

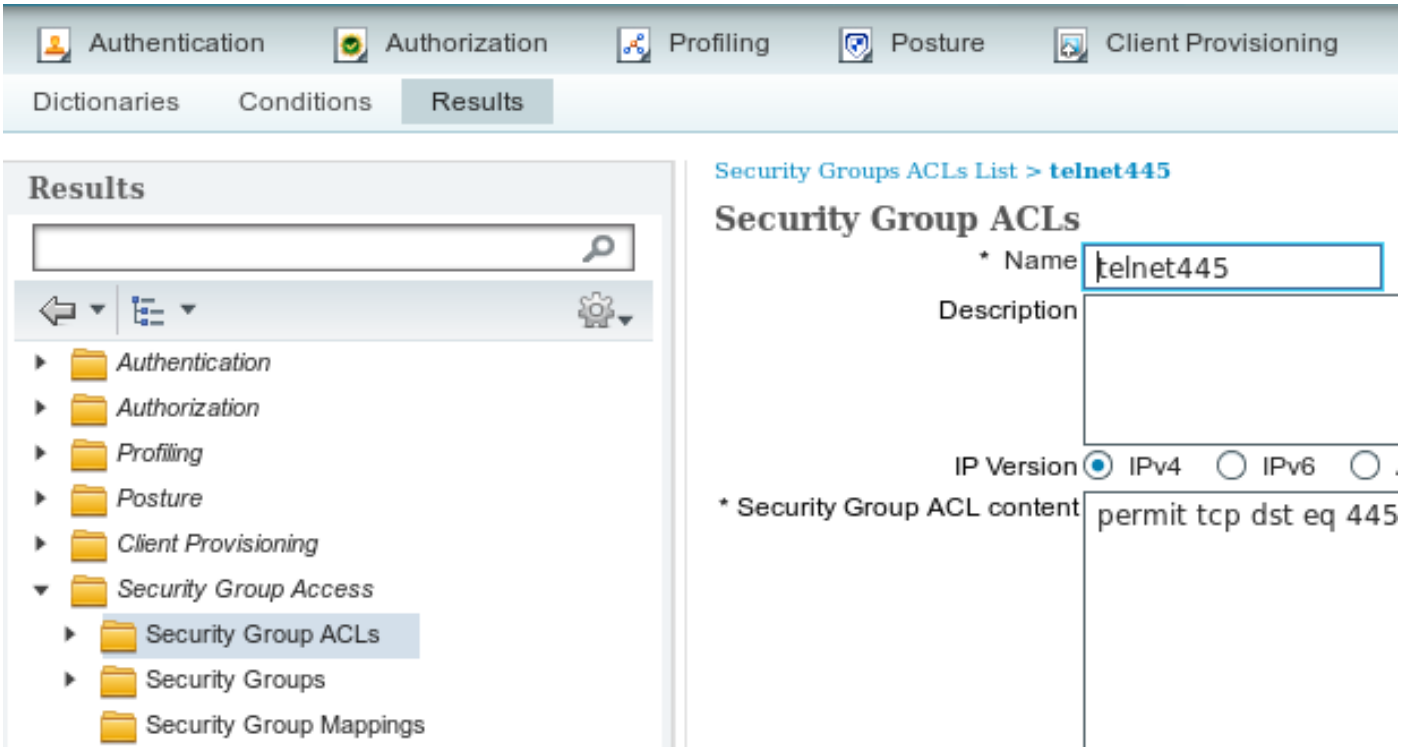
1 - رقيب للشؤون المالية والتسويقية

انتقل إلى **Policy > Results > Security Group Access (السياسة) > مجموعات الأمان** Security Groups (مجموعات الأمان) **Security Groups (مجموعات** الأمان) **Security** Groups (أداة SGT for Finance and Marketing) كما هو موضح في هذه الصورة.



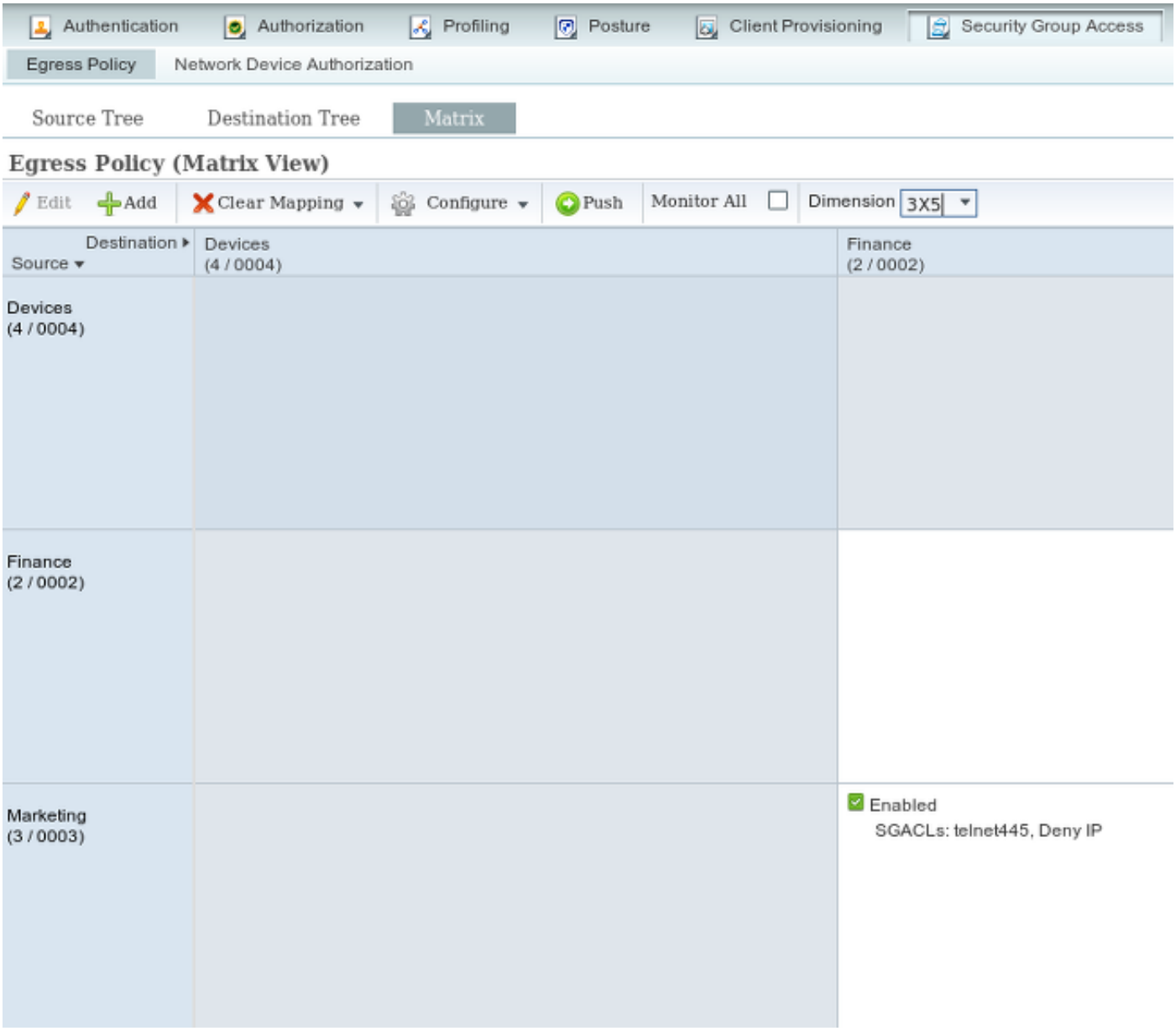
2. قائمة التحكم في الوصول (ACL) الخاصة بمجموعة الأمان لتسويق حركة المرور > التمويل

انتقل إلى **السياسة > النتائج > وصول مجموعة الأمان > قائمة التحكم في الوصول لمجموعة الأمان** وإنشاء قائمة التحكم في الوصول (ACL) التي يتم إستخدامها للتحكم في حركة المرور من التسويق إلى التمويل. يسمح فقط ب TCP/445 كما هو موضح في هذه الصورة.



3. ربط قائمة التحكم في الوصول (ACL) في المصفوفة

انتقل إلى **سياسة > سياسة الخروج > قائمة التحكم في الوصول** إلى **مصفوفة** الربط التي تم تكوينها للمصدر: **التسويق** والوجهة: **التمويل**. قم أيضا بإرفاق **رفض IP** كآخر قائمة تحكم في الوصول (ACL) لإسقاط جميع حركة المرور الأخرى كما هو موضح في الصورة. (بدون إرفاق النهج الافتراضي، يتم السماح بأي)



4. قاعدة التفويض لتعيين الوصول إلى الشبكة الخاصة الظاهرية (VPN) للرقيب = 3 (التسويق)

انتقل إلى **نهج > تفويض** وإنشاء قاعدة للوصول إلى الشبكة الخاصة الظاهرية (VPN) البعيدة. ستحصل جميع إتصالات الشبكة الخاصة الظاهرية (VPN) التي يتم تأسيسها عبر عميل AnyConnect 4.x على الوصول الكامل (PermitAccess) وسيتم تعيين العلامة 3 (التسويق) لها من قبل الرقيب. الشرط هو إستخدام امتدادات هوية AnyConnect (ACIDEX):

```
Rule name: VPN
Condition: Cisco:cisco-av-pair CONTAINS mdm-tlv=ac-user-agent=AnyConnect Windows 4
Permissions: PermitAccess AND Marketing
```

5. قاعدة التفويض الخاصة بتعيين الوصول لمعيار 802. 1x الرقيب = 2 (الشؤون المالية)

انتقل إلى **نهج > تفويض** وإنشاء قاعدة للوصول إلى 802.1x. طالب ينهي جلسة 802.1x على 3750 مفتاح مع username **cisco** سيحصل على الوصول الكامل (PermitAccess) وسيعين الرقيب بطاقة 2 (الشؤون المالية).

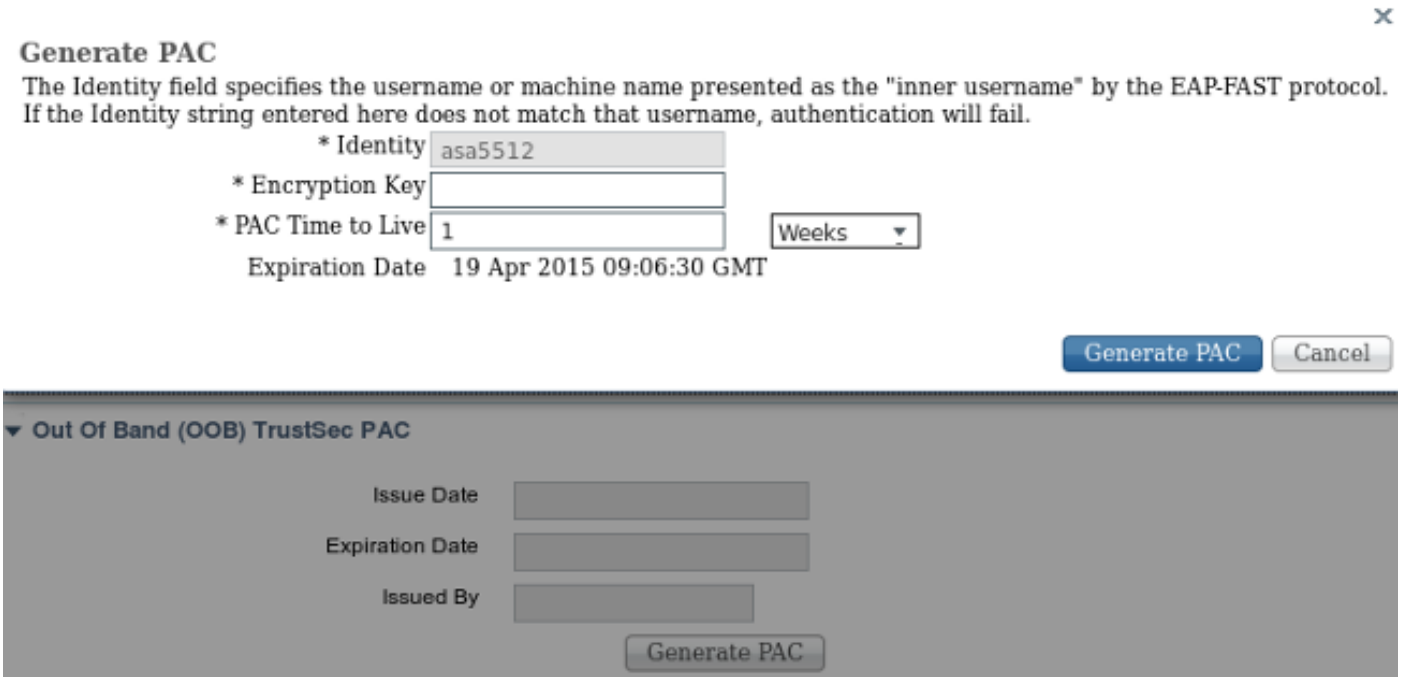
```
Rule name: 802.1x
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
```

```
Permissions: PermitAccess AND Finance
```

6. إضافة جهاز شبكة، إنشاء PAC ل ASA

لإضافة ASA إلى مجال TrustSec، من الضروري إنشاء ملف PAC يدويا. يتم إستيراد هذا الملف على ASA.

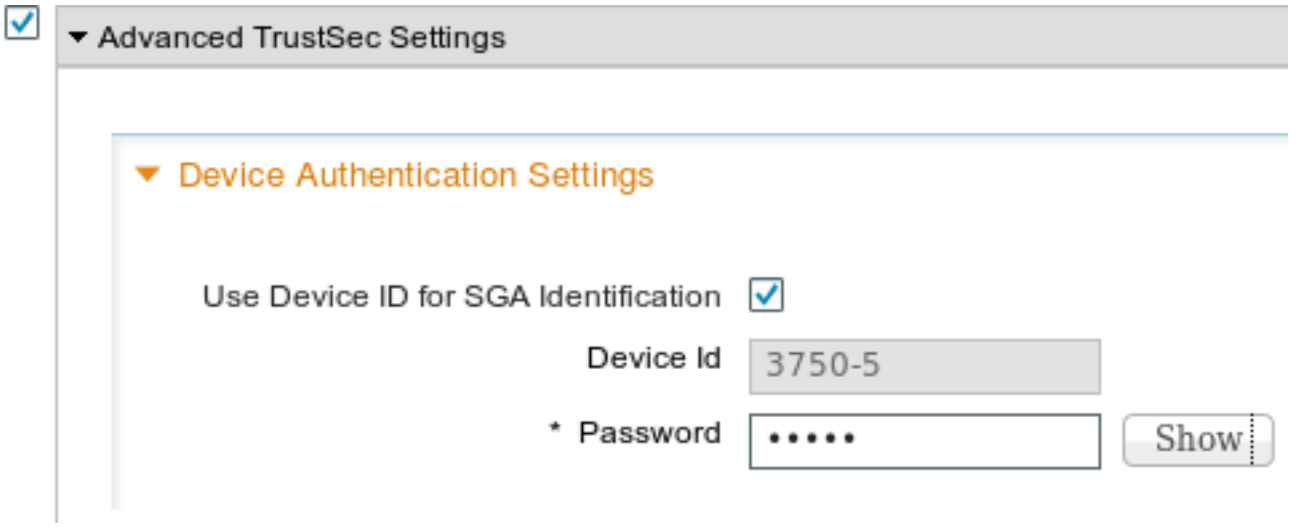
التي يمكن تكوينها من **الإدارة > أجهزة الشبكة**. بعد إضافة ASA، قم بالتمرير لأسفل إلى **إعدادات TrustSec** وإنشاء **مسوغات الوصول المحمي (PAC)** كما هو موضح في هذه الصورة.



تدعم المحولات (3750X) إمداد مسوغ الوصول المحولات (PAC) التلقائي، لذلك يلزم تنفيذ الخطوات فقط ل ASA التي تدعم إمداد مسوغ الوصول المحولات يدويا فقط.

7. إضافة جهاز شبكة، تكوين سر لتوفير PAC التلقائي للمحول

بالنسبة للمحول الذي يستخدم توفير مسوغ الوصول المحمي (PAC) التلقائي، يجب تعيين سر صحيح، كما هو موضح في هذه الصورة.



ملاحظة: تستخدم مسوغات الوصول المحمي (PAC) لمصادقة بيانات بيئة ISE وتنزيلها (مثل SGT) بالإضافة إلى السياسة (ACL). يدعم ASA بيانات البيئة فقط، ويجب تكوين السياسات يدويا على ASA. يدعم Cisco IOS® كليهما، لذلك يمكن تنزيل السياسات من ISE.

ASA - خطوات التكوين

1. الوصول الأساسي إلى الشبكة الخاصة الظاهرية (VPN)

تكوين الوصول الأساسي إلى SSL VPN ل AnyConnect باستخدام ISE للمصادقة.

```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.62.145.41
key cisco

webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
address-pool (outside) POOL
authentication-server-group ISE
default-group-policy TAC
tunnel-group TAC webvpn-attributes
group-alias TAC enable

ip local pool POOL 192.168.100.50-192.168.100.60 mask 255.255.255.0
```

2. إستيراد مسوغات الوصول المحمي وتمكين cts

إستيراد PAC الذي تم إنشاؤه ل ASA (من الخطوة 6 من تكوين ISE). أستخدم مفتاح التشفير نفسه:

```
BSNS-ASA5512-4# cts import-pac http://10.229.20.86/asa5512.pac password ciscocisco
PAC Imported Successfully
```

للتحقق من:

```
BSNS-ASA5512-4# show cts pac

PAC-Info:
Valid until: Apr 11 2016 10:16:41
AID: c2dcb10f6e5474529815aed11ed981bc
I-ID: asa5512
A-ID-Info: Identity Services Engine
PAC-type: Cisco Trustsec
PAC-Opaque:
000200b000030001000400010c2dcb10f6e5474529815aed11ed981bc00060094000301
007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

تمكين cts:

```
cts server-group ISE
```

بعد تمكين CTS، يجب أن يقوم ASA بتنزيل بيانات البيئة من ISE:

```
BSNS-ASA5512-4# show cts environment-data
                        CTS Environment Data
                        ====================
                            Status:                    Active
                       Last download attempt:     Successful
                       Environment Data Lifetime: 86400 secs
                Last update time:          10:21:41 UTC Apr 11 2015
               (Env-data expires in:       0:00:37:31 (dd:hr:mm:sec
               (Env-data refreshes in:     0:00:27:31 (dd:hr:mm:sec
```

3. SGACL لتمويل حركة المرور > التسويق

قم بتكوين SGACL على الواجهة الداخلية. تسمح قائمة التحكم في الوصول (ACL) ببدء حركة مرور ICMP فقط من الشؤون المالية إلى التسويق.

```
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
access-group inside in interface inside
```

يجب أن يوسع ASA اسم علامة التمييز للرقم:

```
BSNS-ASA5512-4(config)# show access-list inside
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=47) 0x5633b153
```

4. تمكين CTS على الواجهة الداخلية

بعد أن يمكن أنت cts على القارن داخلي من ASA:

```
interface GigabitEthernet0/1
 nameif inside
 cts manual
  policy static sgt 100 trusted
 security-level 100
 ip address 192.168.1.100 255.255.255.0
```

يمكن أن يرسل ASA إطارات TrustSec ويستقبلها (إطارات إيثرنت مع حقل CMD). يفترض ASA أن كل إطارات الدخول بدون علامة يجب أن يتم التعامل معها كما مع العلامة 100. كل إطارات المدخل التي تتضمن علامة التمييز بالفعل سيتم الوثوق بها.

المحول - خطوات التكوين

1 - قاعدة 802.1x

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
```

```
switchport access vlan 10
switchport mode access
authentication host-mode multi-domain
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

مع هذا التكوين، بعد تفويض 802.1x الناجح، يجب تعيين العلامة 2 (الشؤون المالية) للمستخدم (المعتمد عبر ISE).

2. تكوين CTS وتقديمه

وبالمثل، بالنسبة ل ASA، يتم تكوين CTS ويشير إلى ISE:

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

أيضا، مكنت فرض على حد سواء للطبقة 3 والطبقة 2 (كل VLANs):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1008-4094
```

لتوفير مسوغات الوصول المحمي (PAC) تلقائيا:

```
bsns-3750-5#cts credentials id 3750-5 password ciscocisco
```

ثانية، كلمة ينبغي طابقت مع ال يماثل تشكيل على ISE (**شبكة أداة>مفتاح > TrustSec**). يقوم Cisco IOS®بتهيئة جلسة EAP-FAST باستخدام ISE الآن للحصول على مسوغ الوصول المحمي PAC. يمكن العثور على مزيد من التفاصيل حول هذه العملية هنا:

[مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أستكشاف الأخطاء وإصلاحها](#)

للتحقق من تثبيت مسوغ الوصول المحمي (PAC):

```
bsns-3750-5#show cts pacs
AID: EA48096688D96EF7B94C679A17BDAD6F
:PAC-Info
PAC-type = Cisco Trustsec
AID: EA48096688D96EF7B94C679A17BDAD6F
I-ID: 3750-5
A-ID-Info: Identity Services Engine
Credential Lifetime: 14:41:24 CEST Jul 10 2015
PAC-Opaque:
000200B000030001000400010EA48096688D96EF7B94C679A17BDAD6F000600940003010036 5AB3133998C86C1BA1B418
968C60690000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
Refresh timer is set for 4y14w
```

3. تمكين CTS على الواجهة إلى ASA

```
interface GigabitEthernet1/0/39
switchport access vlan 10
switchport mode access
cts manual
policy static sgt 101 trusted
```

من الآن فصاعدا، يجب أن يكون المحول جاهزا لمعالجة إطارات TrustSec وإرسالها وفرض السياسات التي تم تنزيلها من ISE.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تمت تغطية التحقق في أقسام منفردة من هذا المستند.

استكشاف الأخطاء وإصلاحها

مهمة الرقيب

بعد تأسيس جلسة الشبكة الخاصة الظاهرية (VPN) إلى ASA، يجب تأكيد تعيين الرقيب الصحيح:

```
BSNS-ASA5512-4# show vpn-sessiondb anyconnect

                                    Session Type: AnyConnect

                        Username     : cisco                  Index        : 13
                    Assigned IP  : 192.168.100.50         Public IP    : 10.229.20.86
                        Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
                                          License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
  Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA1
                       Bytes Tx     : 10308                  Bytes Rx     : 10772
                     Group Policy : TAC                      Tunnel Group : TAC
                                   Login Time   : 15:00:13 UTC Mon Apr 13 2015
                                                  Duration     : 0h:00m:25s
                                                  Inactivity   : 0h:00m:00s
                    VLAN Mapping : N/A                       VLAN         : none
                                      Audt Sess ID : c0a801640000d000552bd9fd
                                                  Security Grp : 3:Marketing
```

وفقا لقواعد التخويل في ISE، تم تعيين جميع مستخدمي AnyConnect4 لعلامة التسويق.

نفس مع 802.1x جلسة على المفتاح. بعد انتهاء وحدة تحليل شبكة NAM) AnyConnect)، سيقوم محول المصادقة بتطبيق العلامة الصحيحة التي تم إرجاعها من ISE:

```
bsns-3750-5#show authentication sessions interface g1/0/2 details
                                  Interface:  GigabitEthernet1/0/2
                                        MAC Address:  0050.5699.36ce
                                             IPv6 Address:  Unknown
                                          IPv4 Address:  192.168.1.203
                                               User-Name:  cisco
                                           Status:  Authorized
                                                 Domain:  DATA
                                          Oper host mode:  multi-domain
                                                 Oper control dir:  both
                                                  Session timeout:  N/A
                                Common Session ID:  0A30426D000000130001B278
                                             Acct Session ID:  Unknown
                                           Handle:  0x53000002
                                        Current Policy:  POLICY_Gi1/0/2
```

```
                                                                :Local Policies
                                (Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150
                                                        Security Policy:  Should Secure
                                                        Security Status:  Link Unsecure

                                                                :Server Policies
                                                            SGT Value:  2

                                                                :Method status list
                                                    Method           State
                                                dot1x            Authc Success
                                                    mab              Stopped
```

وفقا لقواعد التخويل في ISE، يجب تعيين جميع المستخدمين المتصلين بذلك المحول إلى SGT = 2 (الشؤون المالية).

تنفيذ على ASA

عندما تحاول إرسال حركة مرور من Finance (192.168.1.203) إلى Marketing (192.168.100.50)، فإنها تصل إلى واجهة ASA الداخلية. بالنسبة لطلب صدى ICMP، فإنه يقوم بإنشاء الجلسة:

```
Built outbound ICMP connection for faddr 192.168.100.50/0(LOCAL\cisco, 3:Marketing) gaddr
(192.168.1.203/1 laddr 192.168.1.203/1(2
```

وزيادة عدادات قائمة التحكم في الوصول (ACL):

```
BSNS-ASA5512-4(config)# sh access-list

access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
(group name Marketing(tag=3) any (hitcnt=138
```

ويمكن تأكيد ذلك أيضا عند النظر في عمليات التقاط الحزم. لاحظ أن علامات التمييز الصحيحة معروضة:

```
BSNS-ASA5512-4(config)# capture CAP interface inside
BSNS-ASA5512-4(config)# show capture CAP

  1: 15:13:05.736793       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  2: 15:13:05.772237         INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
  3: 15:13:10.737236       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  4: 15:13:10.772726         INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
```

يوجد طلب صدى ICMP قادم تم تمييزه بالرقيب = 2 (الشؤون المالية) ثم إستجابة من مستخدم VPN تم تمييزه بواسطة ASA مع الرقيب = 3 (التسويق). أداة أخرى لاستكشاف الأخطاء وإصلاحها، يتم أيضا إعداد أداة تعقب الحزم TrustSec.

لسوء الحظ، لا يرى 802.1x من الكمبيوتر هذا الجواب لأنه محظور بواسطة RBACL عديم الحالة على المحول (شرح في القسم التالي).

أداة أخرى لاستكشاف الأخطاء وإصلاحها، يتم أيضا إعداد أداة تعقب الحزم TrustSec. دعنا نؤكد ما إذا كان سيتم قبول حزمة ICMP الواردة من Finance:

```
BSNS-ASA5512-4# packet-tracer input inside icmp inline-tag 2 192.168.1.203 8 0 192.168.100.50
Mapping security-group 3:Marketing to IP address 192.168.100.50

                                                                Phase: 1
                                                            Type: CAPTURE
                                                                :Subtype
```

```
                                                    Result: ALLOW
                                                          :Config
                                                :Additional Information
                                                        MAC Access list

                                                             Phase: 2
                                                   Type: ACCESS-LIST
                                                             :Subtype
                                                    Result: ALLOW
                                                          :Config
                                                    Implicit Rule
                                                :Additional Information
                                                        MAC Access list

                                                             Phase: 3
                                                   Type: ROUTE-LOOKUP
                                          Subtype: Resolve Egress Interface
                                                    Result: ALLOW
                                                          :Config
                                                :Additional Information
                                  found next-hop 10.48.66.1 using egress ifc  outside

                                                             Phase: 4
                                                   Type: ACCESS-LIST
                                                        Subtype: log
                                                    Result: ALLOW
                                                          :Config
                                        access-group inside in interface inside
access-list inside extended permit icmp security-group name Finance any security-group name
                                                                Marketing any
                                                :Additional Information

                                                <some output omitted for clarity>

                                                            Phase: 13
                                                   Type: FLOW-CREATION
                                                             :Subtype
                                                    Result: ALLOW
                                                          :Config
                                                :Additional Information
                                  New flow created with id 4830, packet dispatched to next module

                                                             :Result
                                                input-interface: inside
                                                       input-status: up
                                                  input-line-status: up
                                          output-interface: NP Identity Ifc
                                                      output-status: up
                                                 output-line-status: up
                                                          Action: allow
```

دعنا نحاول أيضا بدء أي اتصال TCP من Finance to Marketing، والذي يجب حظره بواسطة ASA:

```
Deny tcp src inside:192.168.1.203/49236 dst outside:192.168.100.50/445(LOCAL\cisco, 3:Marketing)
[by access-group "inside" [0x0, 0x0
```

تنفيذ المحول

دعنا التحقق مما إذا كان المحول قد قام بتنزيل السياسات من ISE بشكل صحيح:

```
bsns-3750-5#show cts role-based permissions
```

```
:IPv4 Role-based permissions default
                                                    Permit IP-00
:IPv4 Role-based permissions from group 2:Finance to group Unknown
                                                    test_deny-30
:IPv4 Role-based permissions from group 8 to group Unknown
                                                  permit_icmp-10
:IPv4 Role-based permissions from group Unknown to group 2:Finance
                                                    test_deny-30
                                                    Permit IP-00
:IPv4 Role-based permissions from group 3:Marketing to group 2:Finance
                                                    telnet445-60
                                                     Deny IP-00
                                RBACL Monitor All for Dynamic Policies : FALSE
                                RBACL Monitor All for Configured Policies : FALSE
```

تم تثبيت النهج الذي يتحكم في حركة مرور البيانات من "التسويق إلى "التمويل" بشكل صحيح. يتم السماح فقط ب TCP/445 وفقا ل RBACL:

```
bsns-3750-5#show cts rbacl telnet445
                                                    CTS RBACL Policy
                                                    ================
                                        RBACL IP Version Supported: IPv4
                                                  name   = telnet445-60
                                             IP protocol version = IPV4
                                                      refcnt = 2
                                                  flag   = 0x41000000
                                                  stale  = FALSE
                                                     :RBACL ACEs
                                                permit tcp dst eq 445
```

وهذا هو السبب وراء إسقاط إستجابة ICMP Echo التي تأتي من Marketing to Finance. ويمكن التأكد من ذلك بالتحقق من العدادات لحركة المرور من الرقيب 3 إلى الرقيب 2:

```
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

                  3645233         223613              0               0       *       *

                      122              0              0               0       2       0

                        0              0             65               0       2       3

                        0            179              0               0       0       2

                        0              0              0               0       0       8
```

تم إسقاط الحزم بواسطة الأجهزة (العداد الحالي هو 65 ويتم زيادته كل ثانية).

ماذا لو تم بدء اتصال TCP/445 من التسويق؟

يسمح ASA بذلك (يقبل جميع حركة مرور VPN بسبب "sysopt connection allowed-vpn"):

```
Built inbound TCP connection 4773 for outside:192.168.100.50/49181
(192.168.100.50/49181)(LOCAL\cisco, 3:Marketing) to inside:192.168.1.203/445 (192.168.1.203/445)
((cisco
```

خلقت الجلسة صحيح:

```
BSNS-ASA5512-4(config)#  show conn all | i 192.168.100.50
TCP outside  192.168.100.50:49181 inside  192.168.1.203:445, idle 0:00:51, bytes 0, flags UB
```

و، Cisco IOS® يقبلها بما أنها تطابق Telnet445 RBACL. تزداد العدادات الصحيحة:

```
bsns-3750-5#show cts role-based counters from 3 to 2
3               0               65              0       2       3
```

(العمود الأخير هو حركة مرور مسموح بها من قبل الجهاز). مسموح بجلسة العمل.

يتم تقديم هذا المثال الغرض لإظهار الفرق في تكوين سياسات TrustSec وتنفيذها على ASA و Cisco IOS®. كن على دراية بإختلافات سياسات Cisco IOS® التي تم تنزيلها من جدار الحماية RBACL) ISE عديم الحالة) وجدار الحماية المستند إلى المنطقة الموعية ل TrustSec.

معلومات ذات صلة

- ASA الإصدار 9.2.1 VPN Posture مع مثال تكوين ISE
- مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أستكشاف الأخطاء وإصلاحها
- دليل تكوين محول Cisco TrustSec: فهم Cisco TrustSec
- تكوين خادم خارجي لتفويض مستخدم جهاز الأمان
- دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN، الإصدار 9.1
- دليل مستخدم محرك خدمات الهوية من Cisco، إصدار 1.2
- 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).