تصنيف مساعد الشبكة الخاصة الظاهرية (VPN) الإصدار 9.2 ASA ومثال تكوين التطبيق

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام ميزة جديدة في تصنيف مجموعة الأمان المعدلة (ASA) الخاص ب TrustSec (SGT) لمستخدمي الشبكة الخاصة الظاهرية (VPN)، الإصدار 9.2.1. يقدم هذا المثال إثنين من مستخدمي شبكة VPN الذين تم تعيين جدار حماية مختلف للرقيب ومجموعة الأمان (SGFW)، والذي يعمل على تصفية حركة مرور البيانات بين مستخدمي شبكة VPN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين ASA CLI وتكوين طبقة مأخذ التوصيل الآمنة (SSL) VPN
- معرفة أساسية بتكوين VPN للوصول عن بعد على ASA
- معرفة أساسية بمحرك خدمات الهوية (ISE) وخدمات TrustSec

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

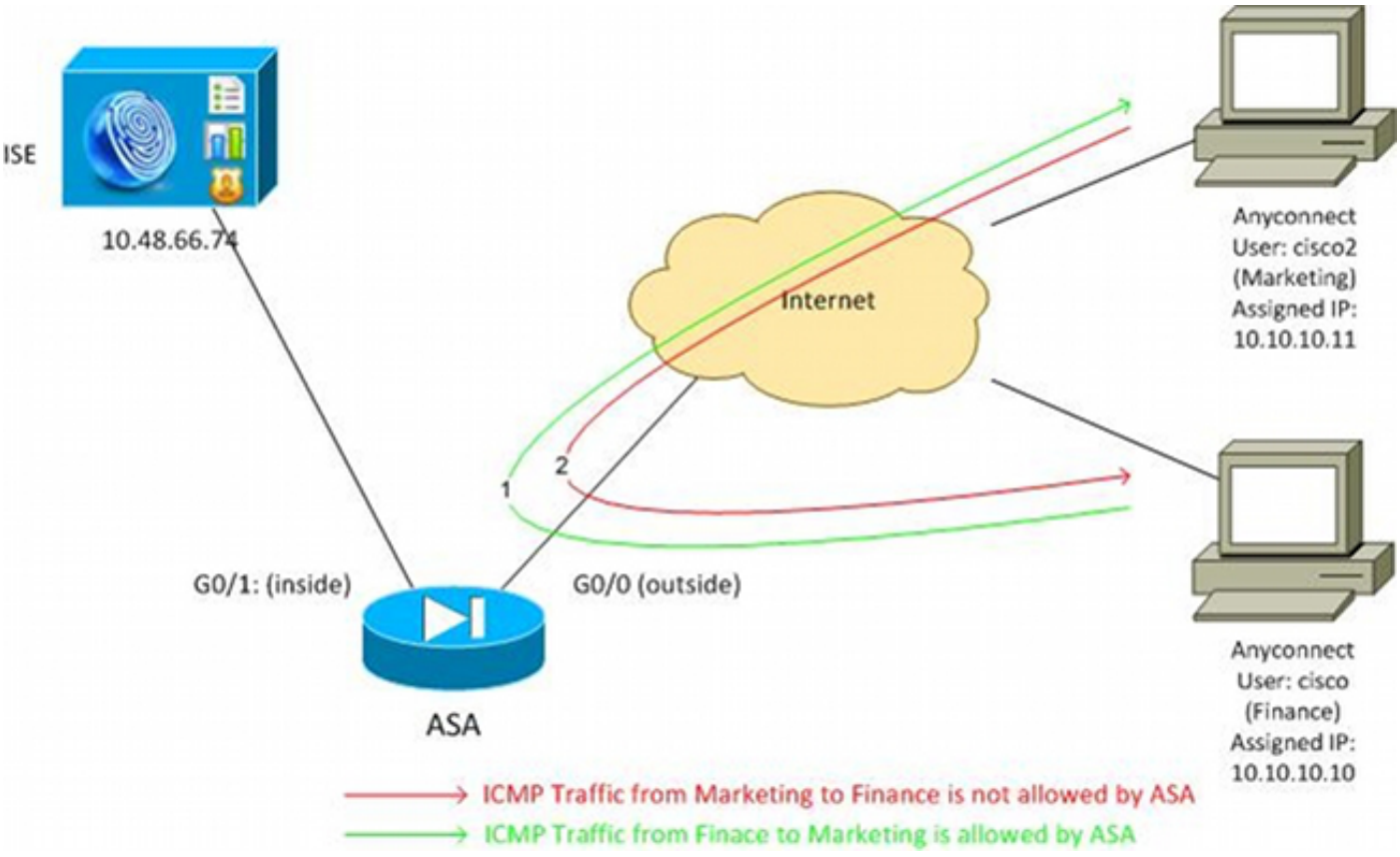
- برنامج Cisco ASA، الإصدار 9.2 والإصدارات الأحدث
- نظام التشغيل Windows 7 مع Cisco AnyConnect Secure Mobility Client، الإصدار 3.1
- Cisco ISE، الإصدار 1.2 والإصدارات الأحدث

التكوين

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

الرسم التخطيطي للشبكة

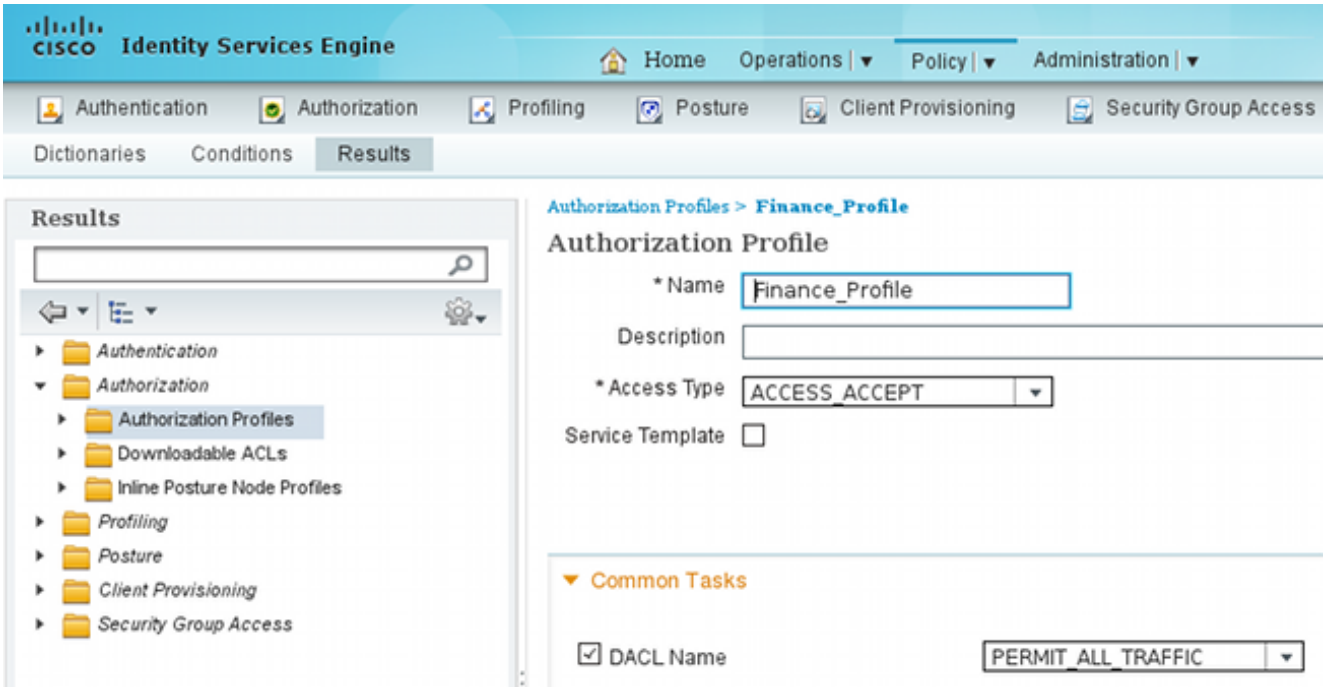
يتم تعيين مستخدم شبكة 'cisco' VPN لفريق التمويل، والذي يتم السماح له ببدء اتصال بروتوكول رسائل التحكم في الإنترنت (ICMP) بفريق التسويق. يتم تعيين مستخدم شبكة 'cisco2' VPN لفريق التسويق، غير مسموح له ببدء أي إتصالات.



تكوين ISE

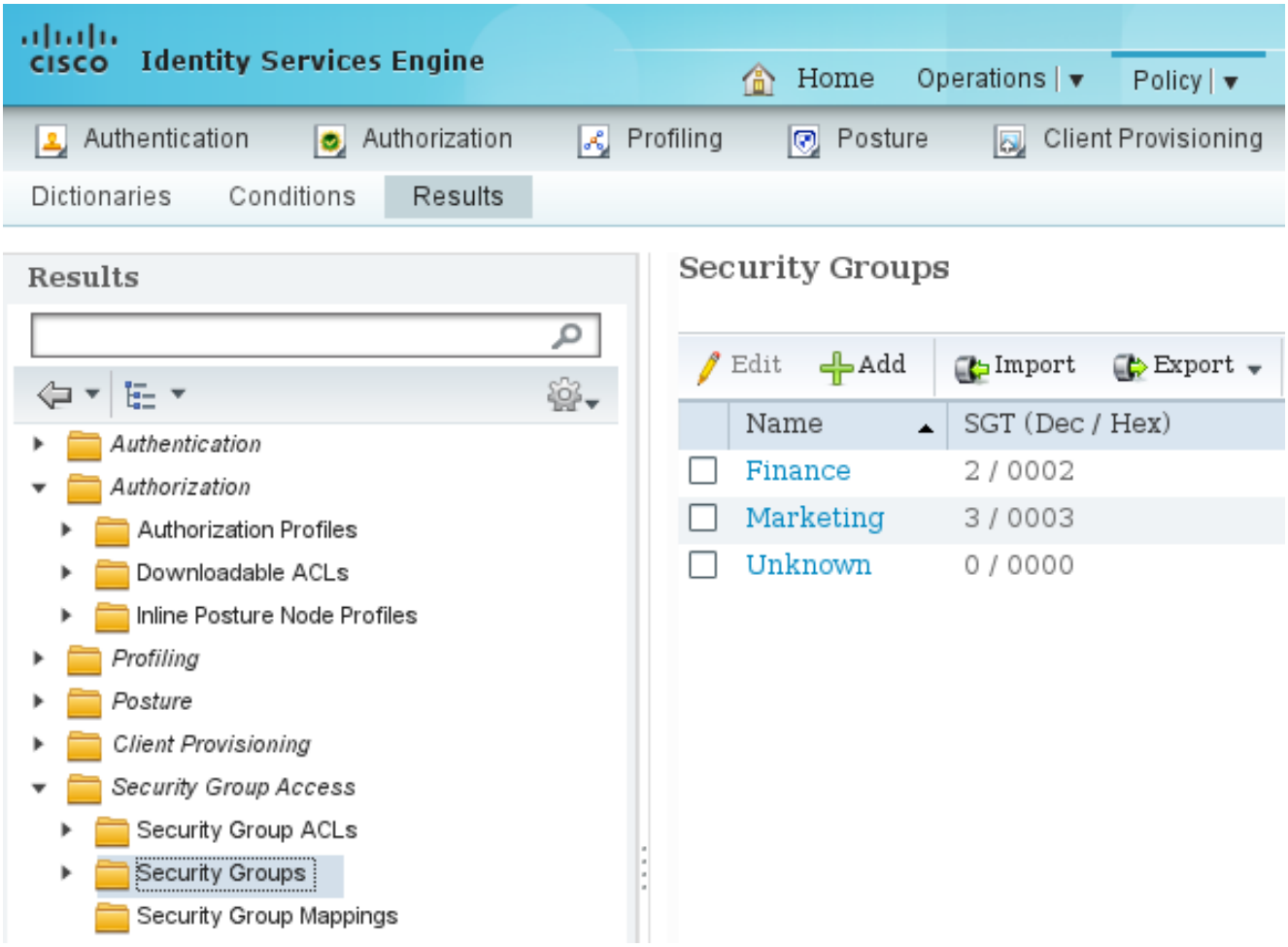
1. أخترت **إدارة>هوية إدارة>هوية** in order to أضفت وشكلت المستعمل 'cisco' (من مالي) و'cisco2' (من تسويق).
2. أخترت **إدارة>شبكة مورد>شبكة أداة** in order to أضفت وشكلت ال ASA كشبكة أداة.
3. أختر **سياسة > نتائج > تخويل > توصيفات تخويل** لإضافة ملفات تعريف تخويل التمويل والتسويق وتكوينها.يتضمن كلا التوصيفين سمة واحدة فقط، قائمة التحكم في الوصول القابلة للتنزيل (DACL)، التي

تسمح بجميع حركات المرور. فيما يلي مثال على
:Finance

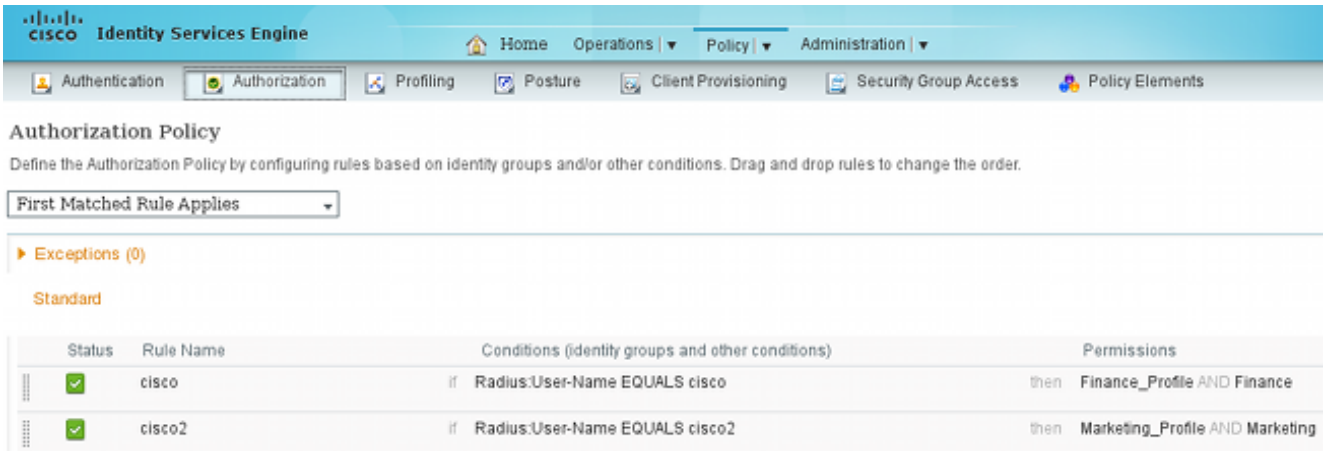


يمكن أن يكون لكل ملف تعريف قائمة تحكم في الوصول إلى النقل (DACL) محددة وتقييدية، ولكن لهذا السيناريو يتم السماح بجميع حركات المرور. يتم تنفيذ الأمر بواسطة SGFW، وليس قائمة التحكم في الوصول للوسائط (DACL) التي يتم تعيينها لكل جلسة من جلسات شبكات VPN. تسمح حركة المرور التي تتم تصفيتها باستخدام SGFW باستخدام معايير SGT فقط بدلا من عناوين IP التي تستخدمها قوائم التحكم في الوصول (DACL).

4. أختر **سياسة > نتائج > وصول مجموعة الأمان > مجموعات الأمان** لإضافة مجموعات "أداة التقييم الخاصة بالتسويق والمالية"
وتكوينها.



5. أخترت **سياسة>تخويل** in order to شكلت الإثنان تخويل قاعدة. تعين القاعدة الأولى Finance_profile (DACL الذي يسمح بحركة المرور الكاملة) بالإضافة إلى Sgt Group Finance لمستخدم "cisco". تعين القاعدة الثانية Marketing_profile (DACL التي تسمح لحركة المرور الكاملة) بالإضافة إلى ميزة التسويق من مجموعة SGT لمستخدم "Cisco2".



تكوين ASA

1. أتمت ال أساسي VPN تشكيل.

```
webvpn
 enable outside
 anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

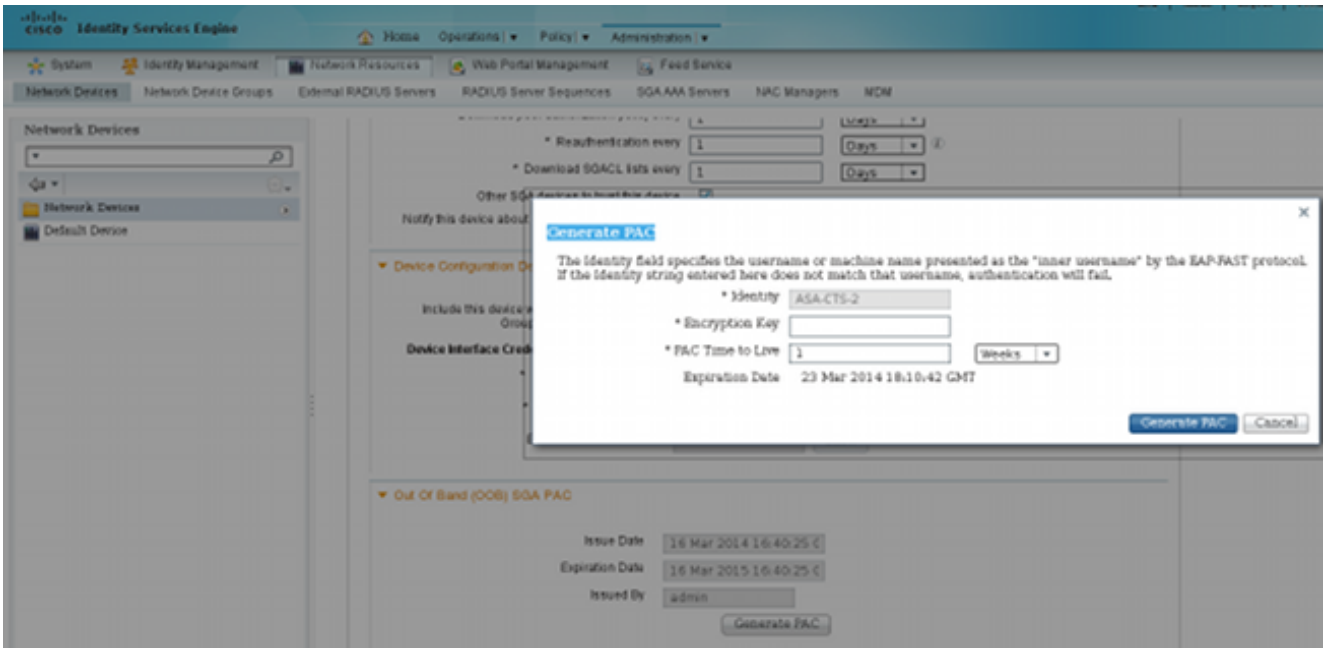
```
group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
accounting-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

2. أكمل تكوين AAA ASA و TrustSec.

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
***** key
cts server-group ISE
```

للانضمام إلى سحابة TrustSec، يحتاج ASA إلى المصادقة باستخدام بيانات اعتماد الوصول المحمي (PAC). لا يدعم ASA توفير PAC التلقائي، ولهذا السبب يجب إنشاء هذا الملف يدويا على ISE واستيراده إلى ASA.

3. أخترت **إدارة>شبكة مورد>شبكة أداة>ASA>متقدم TrustSec عملية إعداد** in order to خلقت PAC على ISE. أختر توفير **مسوغات الوصول المحمي (PAC) خارج النطاق** لإنشاء الملف.



4. إستيراد مسوغات الوصول المحمي إلى ASA.يمكن وضع الملف الذي تم إنشاؤه على خادم HTTP/FTP. يستخدم ASA ذلك لاستيراد الملف.

```
ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678
PAC Imported Successfully!
#ASA
ASA# show cts pac

:PAC-Info
Valid until: Mar 16 2015 17:40:25
AID: ea48096688d96ef7b94c679a17bdad6f
I-ID: ASA-CTS-2
A-ID-Info: Identity Services Engine
PAC-type: Cisco Trustsec
:PAC-Opaque
000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
```

```
2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
11d8378829cc007b91ced9117a
```

عندما يكون لديك مسوغ الوصول المحمي الصحيح، يقوم ASA تلقائيا بتحديث البيئة. تقوم هذه الوحدة بتنزيل المعلومات من فريق دعم المهندسين (ISE) حول مجموعات الرقيب الحالية.

```
ASA# show cts environment-data sg-table

:Security Group Table
Valid until: 17:48:12 CET Mar 17 2014
Showing 4 of 4 entries

SG Name                     SG Tag     Type
-------------     ------                -------
ANY                         65535     unicast
Unknown                         0     unicast
Finance                         2     unicast
Marketing                       3     unicast
```

5. قم بتكوين SGFW. تتمثل الخطوة الأخيرة في تكوين قائمة التحكم في الوصول (ACL) على الواجهة الخارجية التي تسمح لحركة مرور ICMP من "التمويل" إلى "التسويق".

```
access-list outside extended permit icmp security-group tag 2 any security-group
tag 3 any
access-group outside in interface outside
```

كما يمكن إستخدام اسم مجموعة الأمان بدلا من العلامة.

```
access-list outside extended permit icmp security-group name Finance any
security-group name Marketing any
```

لضمان أن القارن ACL يعالج VPN حركة مرور، هو ضروري أن يعجز الخيار أن افتراضيا يسمح VPN حركة مرور دون صحة عن طريق القارن ACL.

```
no sysopt connection permit-vpn
```

والآن ينبغي أن يكون مكتب المساعدة على الوصول (ASA) مستعدا لتصنيف مستخدمي الشبكة الخاصة الظاهرية (VPN) وتنفيذ الإنفاذ استنادا إلى الرقباء .

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يعرض الأمر أداة مترجم الإخراج (مسجل عملاء فقط) تدعم **عرض** أوامر. أستخدم "أداة مترجم الإخراج" لعرض تحليل **عرض** إخراج الأمر.

وبعد إنشاء الشبكة الخاصة الظاهرية (VPN)، يقدم مكتب الشؤون السياسية الرقيب الذي يتم تطبيقه على كل جلسة.

```
ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 10.10.10.10            Public IP    : 192.168.10.68
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 35934                  Bytes Rx     : 79714
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:49:15 CET Sun Mar 16 2014
Duration     : 0h:22m:57s
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A                    VLAN         : none
                                Audt Sess ID : c0a8700a000010005325d60b
                                Security Grp : 2:Finance

                                Username     : cisco2                 Index        : 2
                            Assigned IP  : 10.10.10.11           Public IP    : 192.168.10.80
                                Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
                                                    License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
                            Bytes Tx     : 86171                 Bytes Rx     : 122480
                                Group Policy : GP-SSL                Tunnel Group : RA
                                            Login Time   : 17:52:27 CET Sun Mar 16 2014
                                                    Duration     : 0h:19m:45s
                                                    Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
                                Audt Sess ID : c0a8700a000020005325d6cb
                                Security Grp : 3:Marketing
```

يسمح بروتوكول SGFW بحركة مرور بروتوكول ICMP من الشؤون المالية (SGT=2) إلى التسويق (SGT=3). لذلك يمكن للمستخدم 'cisco' إختبار اتصال المستخدم 'cisco2'.

```
C:\Users\admin>ping 10.10.10.11 -S 10.10.10.10

Pinging 10.10.10.11 from 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=3ms TTL=128
Reply from 10.10.10.11: bytes=32 time=4ms TTL=128
Reply from 10.10.10.11: bytes=32 time=6ms TTL=128
Reply from 10.10.10.11: bytes=32 time=5ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

العدادات تتزايد:

```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
("tag 2(name="Finance") any security-group tag 3(name="Marketing
any (hitcnt=4) 0x071f07fc
```

تم إنشاء الاتصال:

```
Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for
faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0
(laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco
```

يتم قبول حركة مرور الإرجاع تلقائيا، لأنه تم تمكين فحص ICMP.

عندما تحاول إختبار الاتصال من قسم التسويق (SGT=3) إلى قسم الشؤون المالية (SGT=2):

```
C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

تخبر ASA:

```
,Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2
    Marketing) dst outside:10.10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by:3
                                        [access-group "outside" [0x0, 0x0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

راجع هذه المستندات:

- سحابة TrustSec مع 802.1x MACsec على مادة حفازة 3750X sery مفتاح تشكيل مثال
- مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أستكشاف الأخطاء وإصلاحها

ملخص

تقدم هذه المقالة مثالا بسيطا حول كيفية تصنيف مستخدمي شبكات VPN وتنفيذ الإنفاذ الأساسي. كما يقوم SGFW بتصفية حركة مرور البيانات بين مستخدمي VPN وبقية الشبكة. يمكن إستخدام SXP (بروتوكول TrustSec Sgt Exchange Protocol) على ASA للحصول على معلومات التعيين بين IP و SGT. أن يسمح ASA أن ينفذ لكل نوع من جلسة أن يكون صنفت بشكل صحيح (VPN أو LAN).

في برنامج ASA، الإصدار 9.2 والإصدارات الأحدث، يدعم ASA أيضا تغيير تفويض (RFC 5176) (RADIUS (CoA). يمكن أن تتضمن حزمة RADIUS CoA التي يتم إرسالها من ISE بعد وضع الشبكة الخاصة الظاهرية (VPN) الناجح زوج Cisco-AV مع أداة رقيب تقوم بتعيين مستخدم متوافق إلى مجموعة مختلفة (أكثر أمانا). لمزيد من الأمثلة، راجع المقالات في قسم "المعلومات ذات الصلة".

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).