تكامل ISE و FirePower - مثال خدمة الإصلاح

المحتويات

[المقدمة](#)
[المتطلبات الأساسية](#)
[المتطلبات](#)
[المكونات المستخدمة](#)
[التكوين](#)
[الرسم التخطيطي للشبكة](#)
[FirePOWER](#)
[FireSIGHT Management Center (مركز دفاع)](#)
[سياسة التحكم في الوصول](#)
[وحدة معالجة ISE](#)
[سياسة الارتباط](#)
[ASA](#)
[محرك خدمات كشف الهوية (ISE)](#)
[تكوين جهاز الوصول إلى الشبكة (NAD)](#)
[تمكين التحكم في الشبكة المتكيفة](#)
[DACL العزل](#)
[ملف تعريف التخويل للعزل](#)
[قواعد التخويل](#)
[التحقق من الصحة](#)
[بدء جلسة عمل AnyConnect ASA VPN](#)
[محاولة المستخدم الوصول](#)
[إصابة سياسة الارتباط في FireSIGHT](#)
[موقع ISE بإجراء عزل وإرسال CoA](#)
[تم قطع اتصال جلسة عمل VPN](#)
[جلسة عمل VPN مع وصول محدود (عزل)](#)
[استكشاف الأخطاء وإصلاحها](#)
[FireSIGHT (مركز دفاع)](#)
[محرك خدمات كشف الهوية (ISE)](#)
[تحشرات](#)
[معلومات ذات صلة](#)
[مناقشات مجتمع دعم Cisco ذات الصلة](#)

المقدمة

يوضح هذا المستند كيفية إستخدام وحدة المعالجة النمطية على جهاز FireSIGHT من Cisco لاكتشاف الهجمات وإصلاح المهاجم تلقائيا باستخدام محرك خدمة الهوية (ISE) من Cisco كخادم نهج. يصف المثال الوارد في هذا المستند الطريقة التي يتم إستخدامها لمعالجة مستخدم شبكة VPN عن بعد الذي يقوم بالمصادقة عبر ISE، ولكن يمكن إستخدامها أيضا لمستخدم سلكية أو لاسلكي 802.1x/MAB/WebAuth.

ملاحظة: لا تدعم Cisco رسمياً وحدة المعالجة النمطية المشار إليها في هذا المستند. يتم مشاركتها على بوابة مجتمع ويمكن استخدامها من قبل أي شخص. في الإصدارات 5.4 والإصدارات الأحدث، هناك أيضاً وحدة معالجة أحدث متوفرة استناداً إلى بروتوكول *pxGrid*. هذه الوحدة النمطية غير مدعومة في الإصدار 6.0 ولكن من المخطط أن تكون مدعومة في الإصدارات المستقبلية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين جهاز الأمان القابل للتكيف (ASA) VPN من Cisco
- تكوين Cisco AnyConnect Secure Mobility Client
- تكوين Cisco FireSIGHT الأساسي
- التكوين الأساسي Cisco FirePOWER
- تكوين Cisco ISE

المكونات المستخدمة

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

- نظام التشغيل Microsoft Windows 7
- ASA الإصدار 9.3 أو إصدار أحدث من Cisco
- برنامج ISE الإصدارات 1.3 من Cisco والإصدارات الأحدث
- Cisco AnyConnect Secure Mobility Client، الإصدار 3.0 والإصدارات الأحدث
- Cisco FireSIGHT Management Center، الإصدار 5.4
- Cisco FirePOWER، الإصدار 5.4 (الجهاز الظاهري (VM)

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.

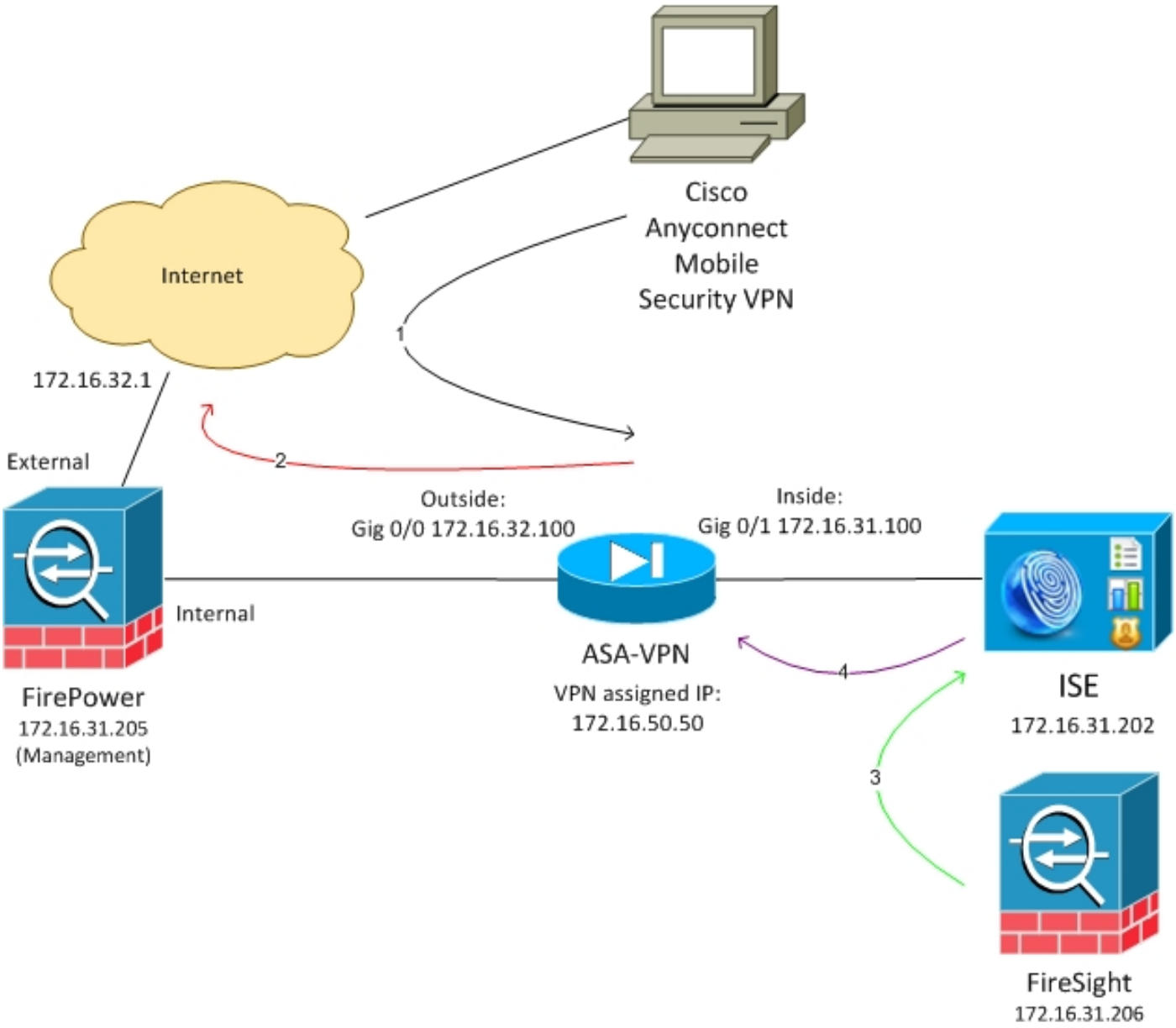
التكوين

أستخدم المعلومات المقدمة في هذا القسم لتكوين النظام.

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

الرسم التخطيطي للشبكة

يستخدم المثال الموضح في هذا المستند إعداد الشبكة التالي:



فيما يلي تدفق إعداد الشبكة هذا:

1. يقوم المستخدم ببدء جلسة عمل VPN عن بعد باستخدام ASA (عبر Cisco AnyConnect Secure Mobility الإصدار 4.0).

2. يحاول المستخدم الوصول إلى *http://172.16.32.1*. (تنتقل حركة المرور عبر FirePower، التي تم تثبيتها على الجهاز الظاهري (VM) وتتم إدارتها بواسطة FireSight.)

3. تم تكوين FirePower بحيث يقوم بحظر (في السطر) حركة المرور المحددة (سياسات الوصول)، ولكن لديه أيضا سياسة ارتباط يتم تشغيلها. ونتيجة لذلك، فإنه يبدأ عملية إصلاح ISE عبر واجهة برمجة تطبيقات REST (API) (أسلوب *QuarantineByIP*).

4. ما إن يستلم ISE الـ REST API نداء، وه يبحث عن الجلسة ويرسل RADIUS تغيير من تخويل (CoA) إلى الـ ASA، أي ينهي أن جلسة.

5. يقطع الـ ASA الـ VPN مستعمل. بما أن AnyConnect يتم تكوينه باستخدام وصول VPN *الدائم*، يتم إنشاء جلسة عمل جديدة، ومع ذلك، هذه المرة يتم مطابقة قاعدة تفويض ISE مختلفة (للمضيفين المحاصرين) ويتم توفير وصول محدود إلى الشبكة. في هذه المرحلة، الـ ISE يعرف كيفية اتصال المستخدم بالشبكة ومصادقته لما؛ طالما يتم إستخدام ISE للمصادقة والتفويض، فإن المستخدم لديه وصول محدود إلى الشبكة بسبب الحجر الصحي.

وكما ذكر سابقا، يعمل هذا السيناريو لأي نوع من جلسات العمل التي تمت مصادقتها (VPN، wireless 802.1x/MAB/WebAuth، wireless 802.1x/MAB/WebAuth) طالما يتم إستخدام ISE للمصادقة ويدعم جهاز الوصول إلى الشبكة RADIUS CoA (جميع أجهزة Cisco الحديثة).

> **تلميح**: من أجل نقل المستخدم خارج الحجر الصحي، يمكنك إستخدام واجهة المستخدم الرسومية (GUI) لـ ISE. قد تدعم الإصدارات المستقبلية من وحدة المعالجة أيضا.

FirePOWER

> **ملاحظة**: يتم إستخدام جهاز VM للمثال الموضح في هذا المستند. يتم إجراء التكوين الأولي فقط عبر واجهة سطر الأوامر. يتم تكوين جميع السياسات من Cisco Defense Center. لمزيد من التفاصيل، ارجع إلى قسم المعلومات ذات الصلة في هذا المستند.

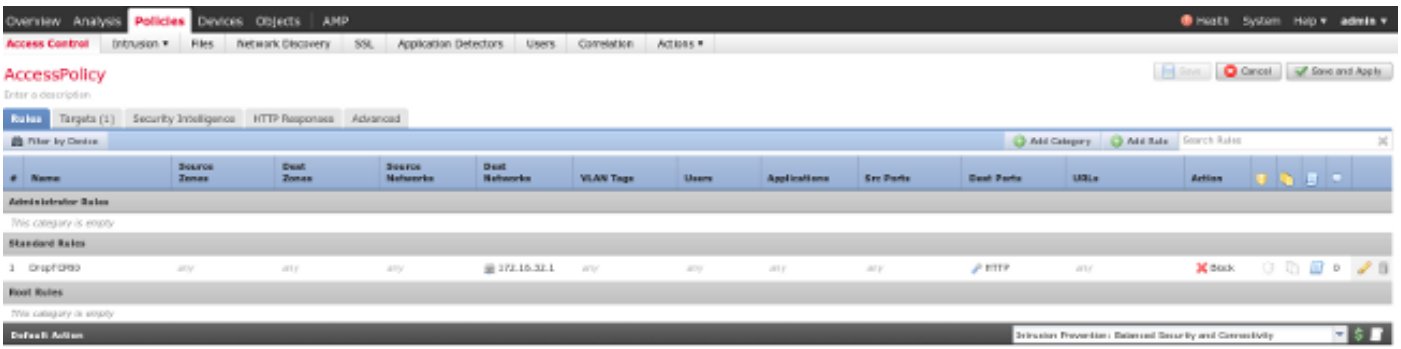
تشتمل الأجهزة الافتراضية على ثلاث واجهات، واحدة للإدارة واثنتان للتفتيش الداخلي (داخلي/خارجي).

تنتقل جميع حركات المرور من مستخدمي الشبكة الخاصة الظاهرية (VPN) عبر FirePOWER.

FireSIGHT Management Center (مركز دفاع)

سياسة التحكم في الوصول

بعد تثبيت الترخيص الصحيحة وإضافة جهاز FirePower، انتقل إلى **السياسات > التحكم في الوصول** وإنشاء سياسة الوصول التي يتم إستخدامها لإسقاط حركة مرور HTTP إلى 172.16.32.1:

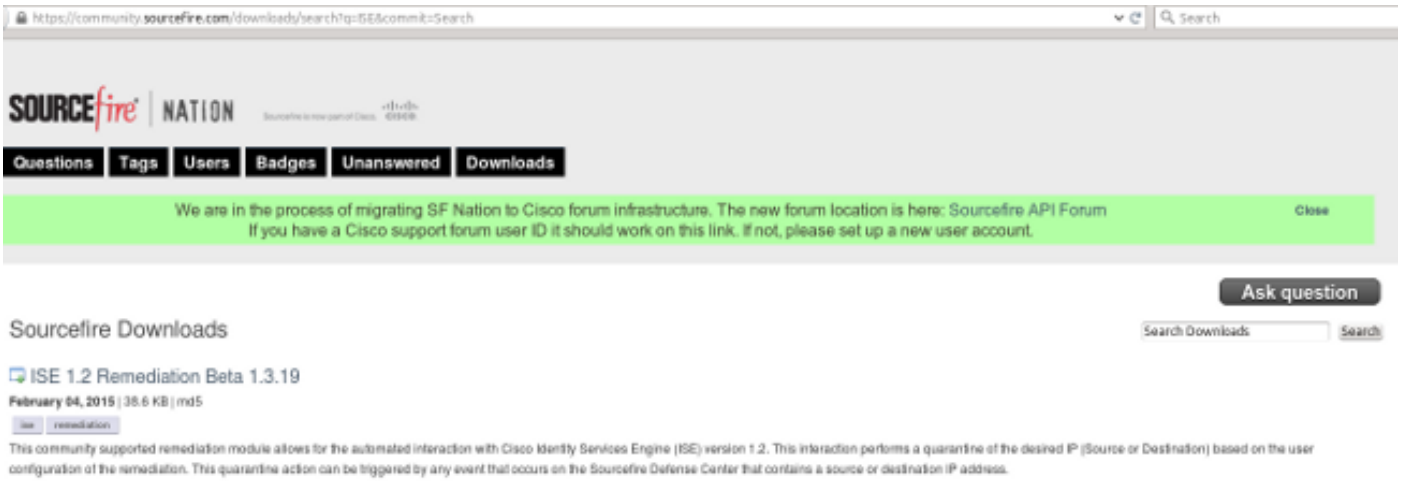


تم قبول جميع حركات المرور الأخرى.

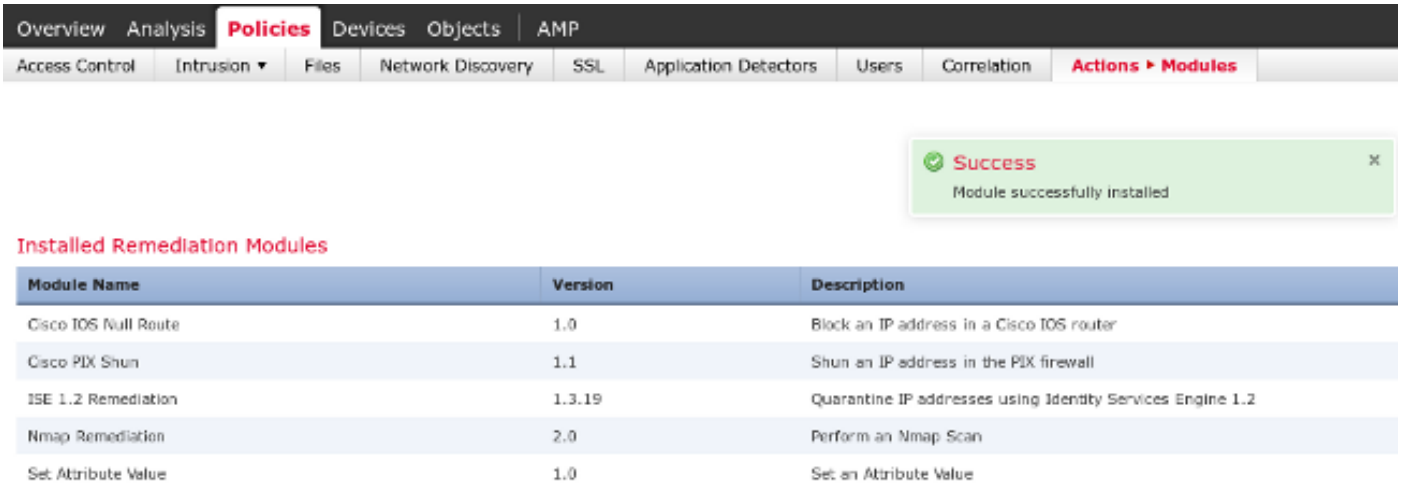
وحدة معالجة ISE

الإصدار الحالي من وحدة ISE النمطية التي تتم مشاركتها على بوابة المجتمع هو *ISE 1.2*

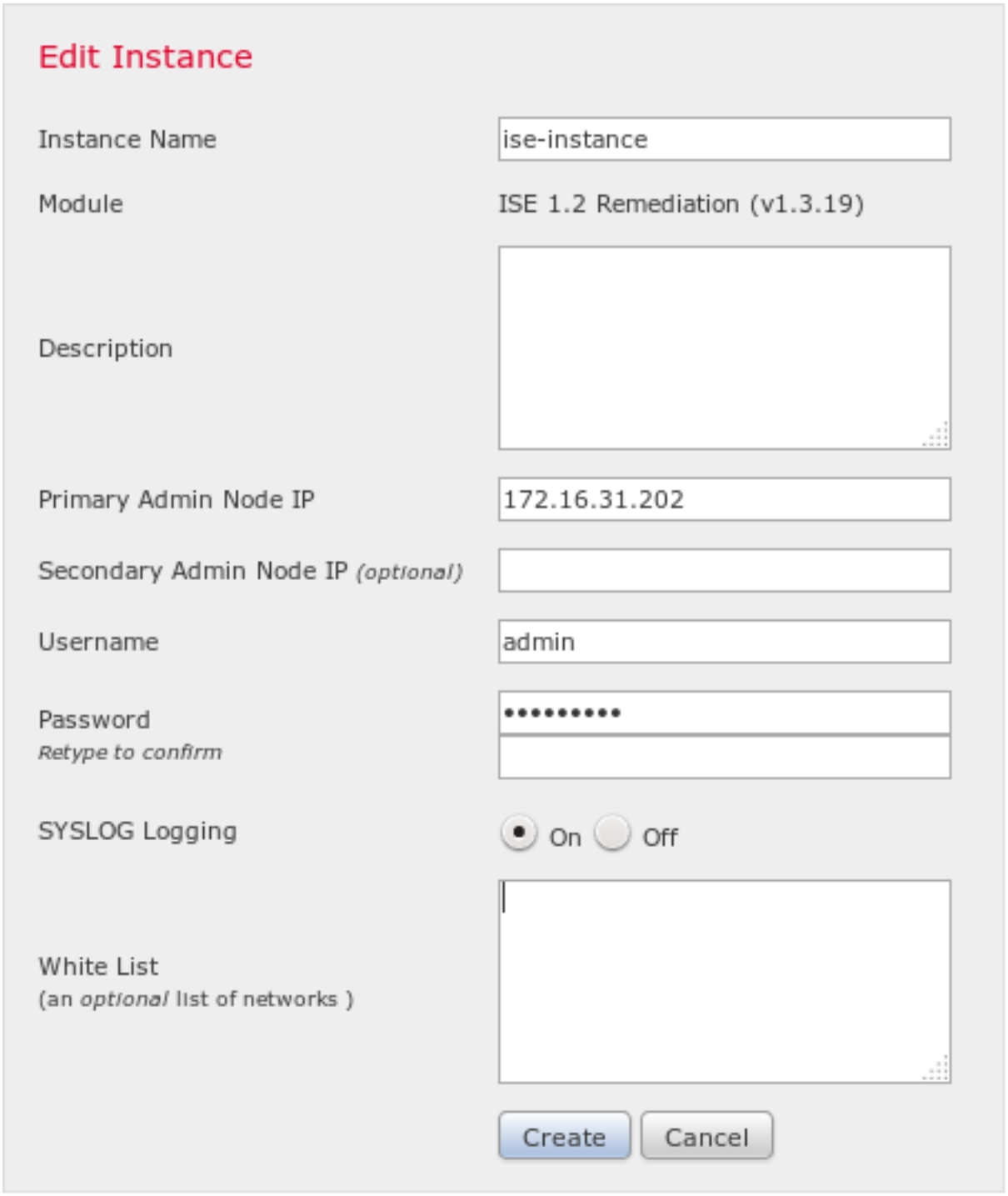
Remediation Beta 1.3.19:



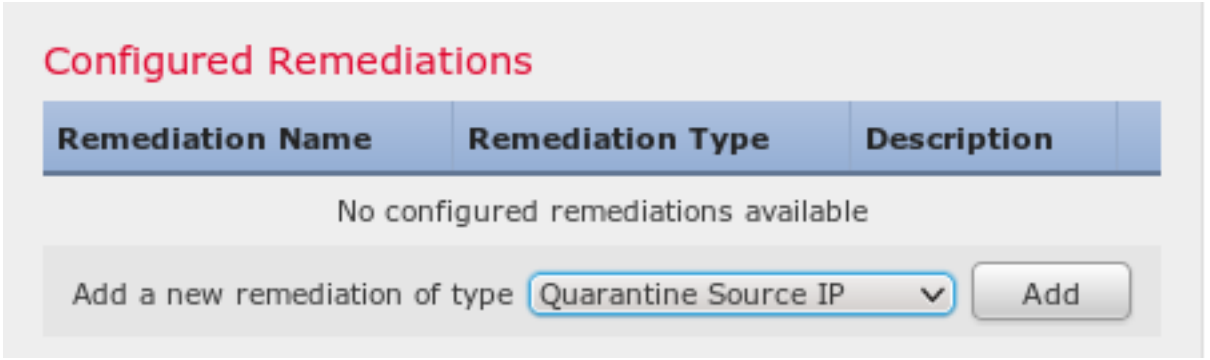
انتقل إلى **السياسات > العمليات > التصحيحات > الوحدات النمطية** وقم بتثبيت الملف:



يجب إنشاء المثيل الصحيح بعد ذلك. انتقل إلى **السياسات > الإجراءات > التصحيحات > المثيلات** ووفر عنوان IP لعقدة إدارة السياسة (PAN)، بالإضافة إلى بيانات الاعتماد الإدارية ل ISE اللازمة لواجهة برمجة تطبيقات REST (يوصى باستخدام مستخدم منفصل مع دور *مسؤول ERS*):

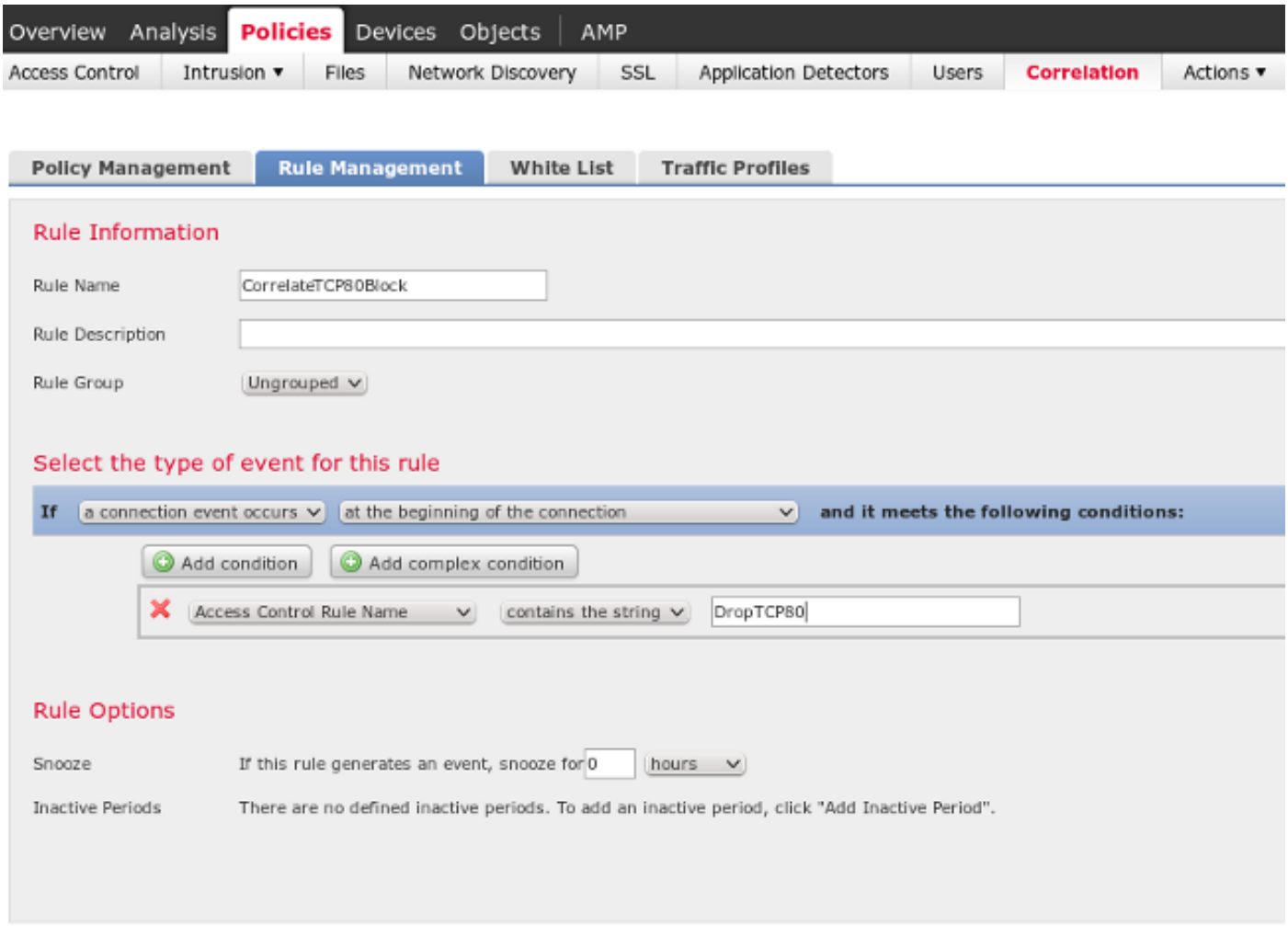


كما يجب إستخدام عنوان IP للمصدر (المهاجم) للإصلاح:

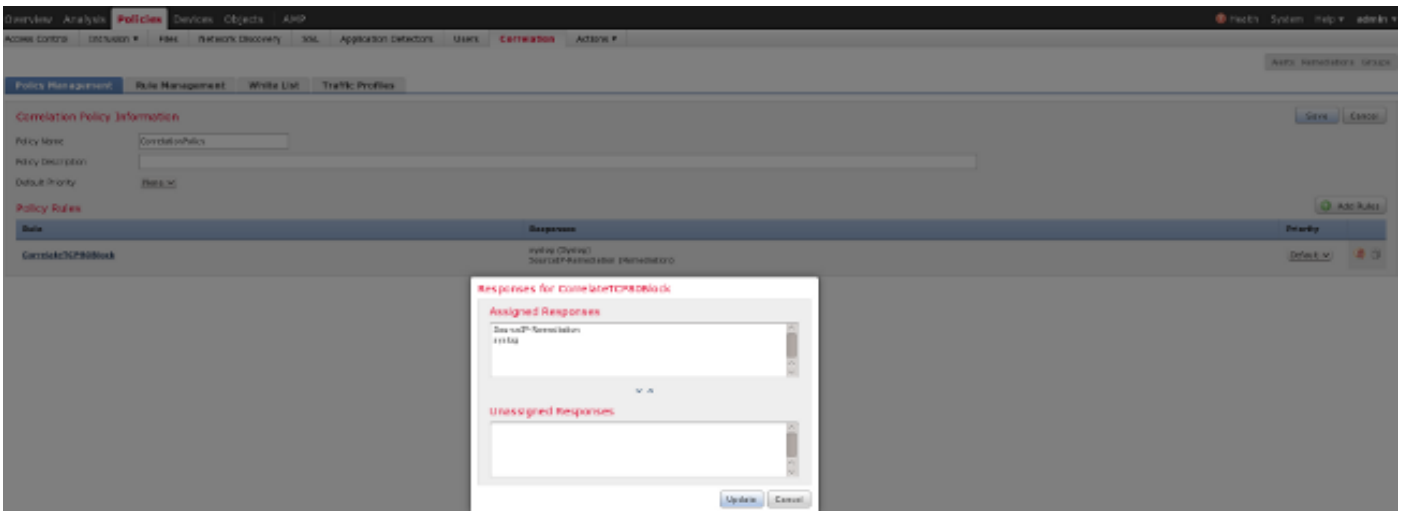


سياسة الارتباط

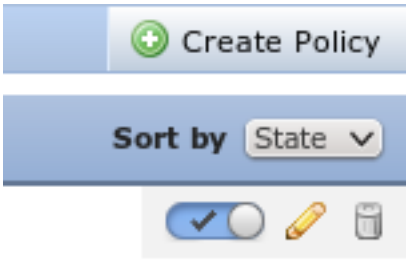
يجب تكوين قاعدة ارتباط محددة الآن. يتم تشغيل هذه القاعدة في بداية الاتصال الذي يطابق قاعدة التحكم في الوصول التي تم تكوينها مسبقا (*DropTCP80*). لتكوين القاعدة، انتقل إلى **السياسات > الارتباط > إدارة القاعدة**:



يتم إستخدام هذه القاعدة في نهج الارتباط. انتقل إلى **السياسات > الارتباط > إدارة السياسات** لإنشاء سياسة جديدة، ثم أضف القاعدة التي تم تكوينها. انقر فوق **إضافة** على اليمين وأضفت إجراءين: **إضافة ل sourceIP** (تم تكوينه مسبقا) و**syslog**:



تأكد من تمكين نهج الارتباط:



ASA

يتم تكوين ASA الذي يعمل كبوابة VPN لاستخدام ISE للمصادقة. ومن الضروري أيضا تمكين المحاسبة وعامل RADIUS:

```
tunnel-group SSLVPN-FIRESIGHT general-attributes
 address-pool POOL-VPN
authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy POLICY

aaa-server ISE protocol radius
 interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
 key *****

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

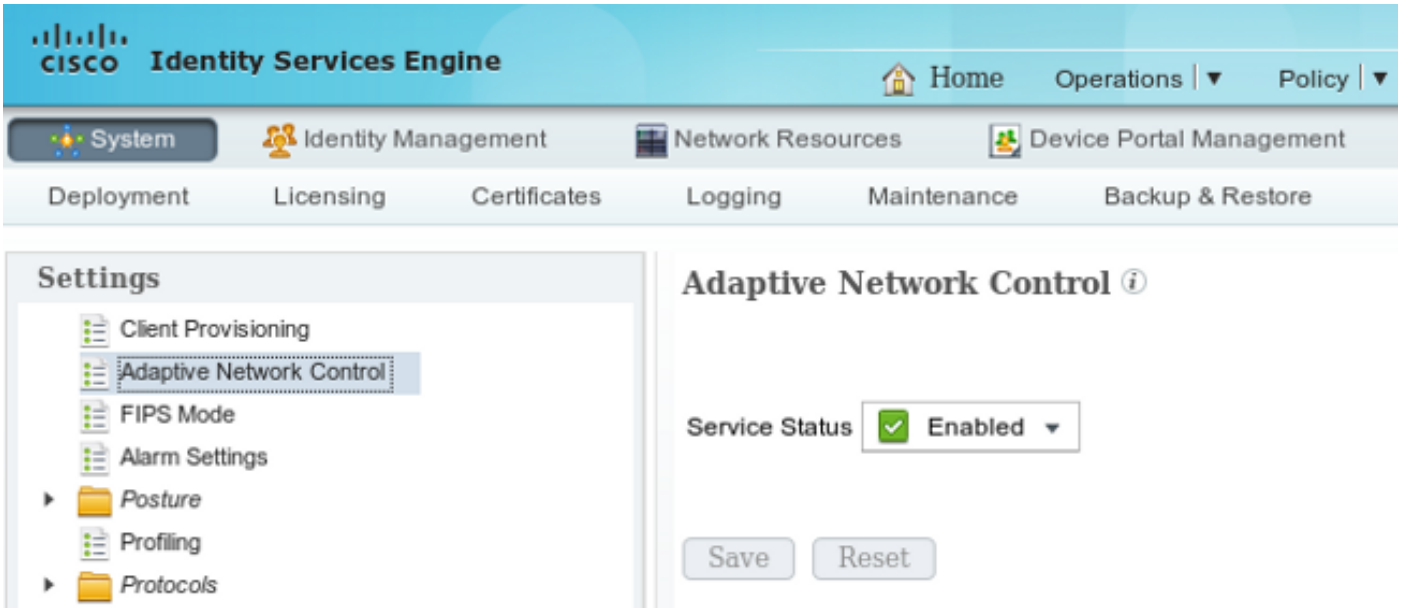
محرك خدمات كشف الهوية (ISE)

تكوين جهاز الوصول إلى الشبكة (NAD)

انتقل إلى **إدارة > أجهزة الشبكة** وأضف ASA الذي يعمل كعميل RADIUS.

تمكين التحكم في الشبكة المتكيفة

انتقل إلى **إدارة > نظام > إعدادات > تحكم شبكة تكيفي** لتمكين واجهة برمجة تطبيقات الحجر الصحي والوظائف:



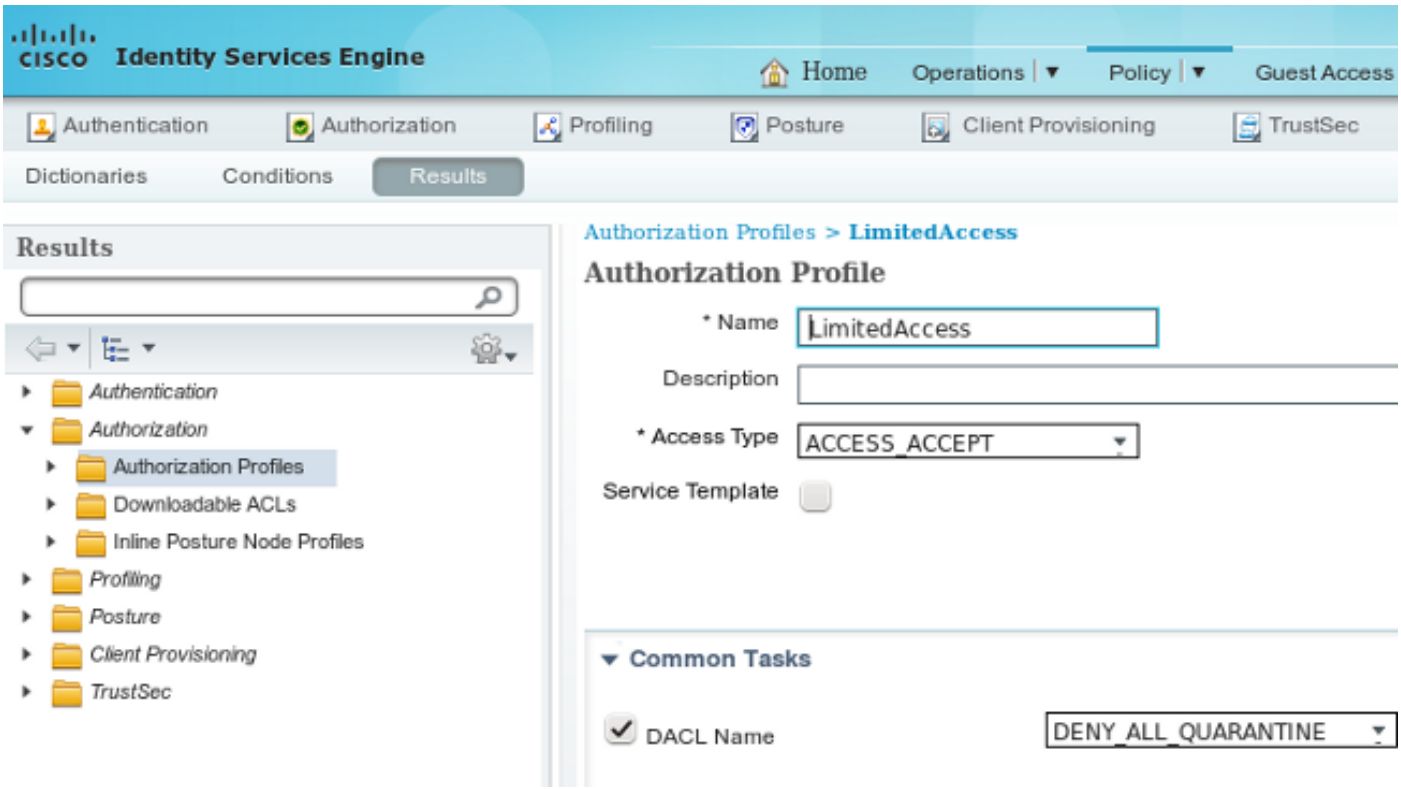
ملاحظة: في الإصدارات 1.3 والإصدارات السابقة، تسمى هذه الميزة *خدمة حماية نقطة النهاية*.

DACL العزل

من أجل إنشاء قائمة تحكم في الوصول (DACL) يمكن تنزيلها والتي يتم إستخدامها للمضيفين المعزولين، انتقل إلى **السياسة > النتائج > التفويض > قائمة التحكم في الوصول (ACL) القابلة للتنزيل**.

ملف تعريف التخويل للعزل

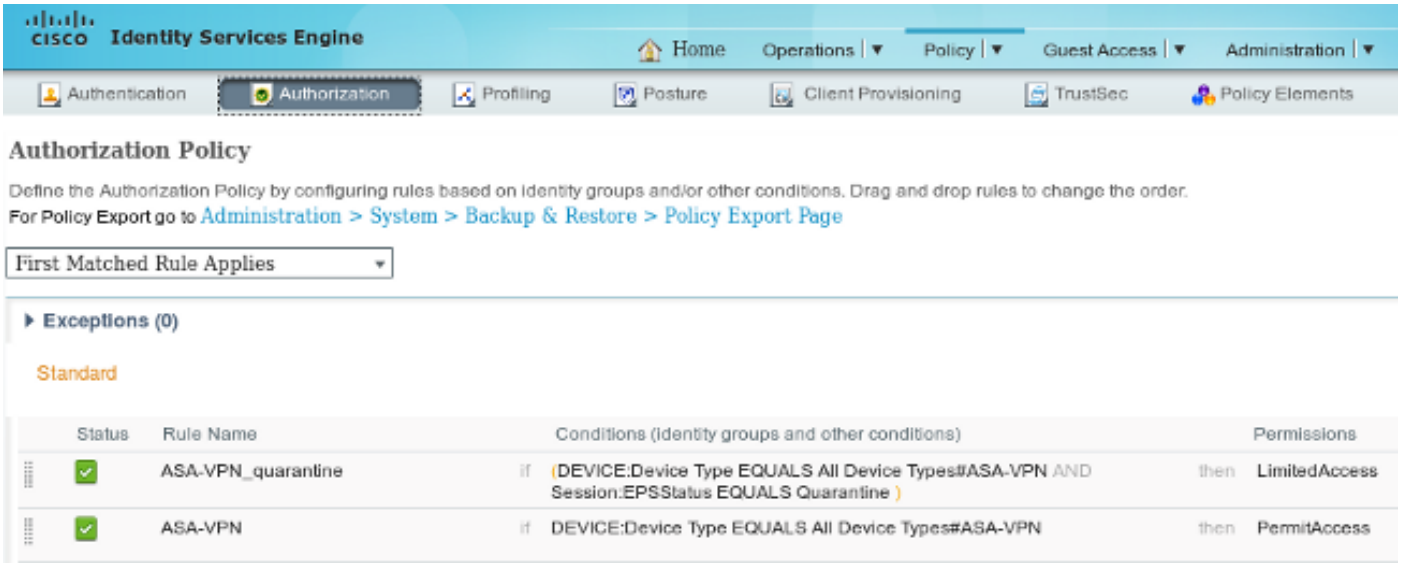
انتقل إلى **السياسة > النتائج > التخويل > ملف تعريف التخويل** وقم بإنشاء ملف تعريف تخويل باستخدام قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) الجديدة:



قواعد التخويل

يجب إنشاء قاعدتين للتخويل. توفر القاعدة الأولى (ASA-VPN) الوصول الكامل لجميع جلسات VPN التي يتم إنهاؤها على ASA. يتم الوصول إلى القاعدة *ASA-VPN_QUARANTINE* لجلسة عمل الشبكة الخاصة الظاهرية (VPN) التي تمت إعادة مصادقتها عندما يكون المضيف بالفعل في وضع العزل (يتم توفير الوصول المحدود إلى الشبكة).

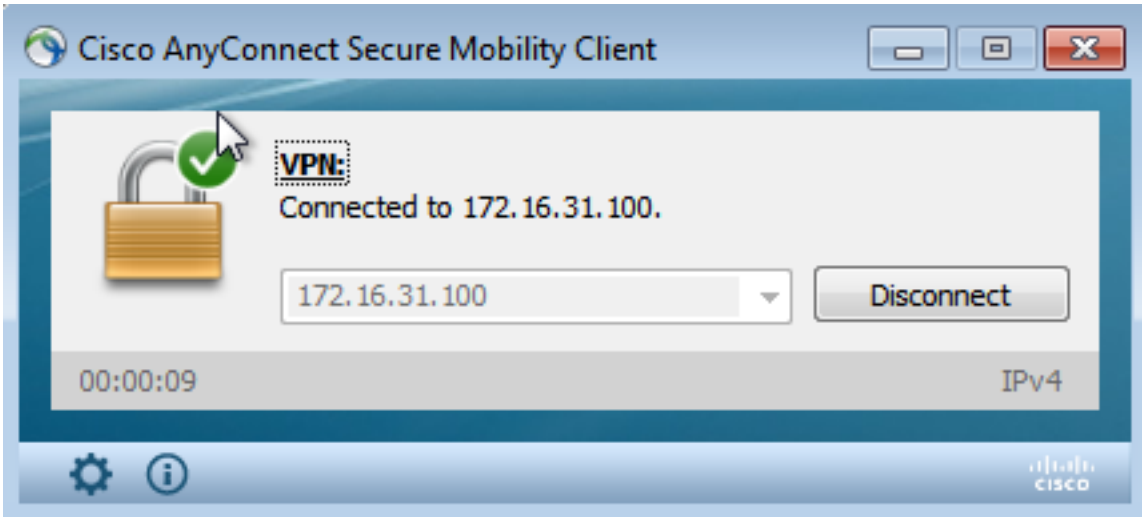
لإنشاء هذه القواعد، انتقل إلى **السياسة > التفويض**:



التحقق من الصحة

أستخدم المعلومات المقدمة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

بدء جلسة عمل AnyConnect ASA VPN



يقوم ASA بإنشاء الجلسة بدون أي DACL (وصول كامل إلى الشبكة):

```
asav# show vpn-sessiondb details anyconnect

Session Type: AnyConnect
```

```
Username     : cisco                  Index        : 37
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.21
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     : 18706                  Bytes Rx     : 14619
Group Policy : POLICY                 Tunnel Group : SSLVPN-FIRESIGHT
Login Time   : 03:03:17 UTC Wed May 20 2015
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : ac10206400025000555bf975
Security Grp : none

......
DTLS-Tunnel:
 <some output omitted for clarity>
```

لوصولا مدختسملا ةلواحم

لوصولا ةسايس ىلإ لوصولا متي ،http://172.16.32.1 ىلإ لوصولا مدختسملا لواحي نأ درجمب، IP ناونع نم syslog ةلاسر لاسرإ متيو ،رطسلا يف ةقباطملا تانايبلا رورم ةكرح رظح متيو FirePower: ةرادإب صاخلا

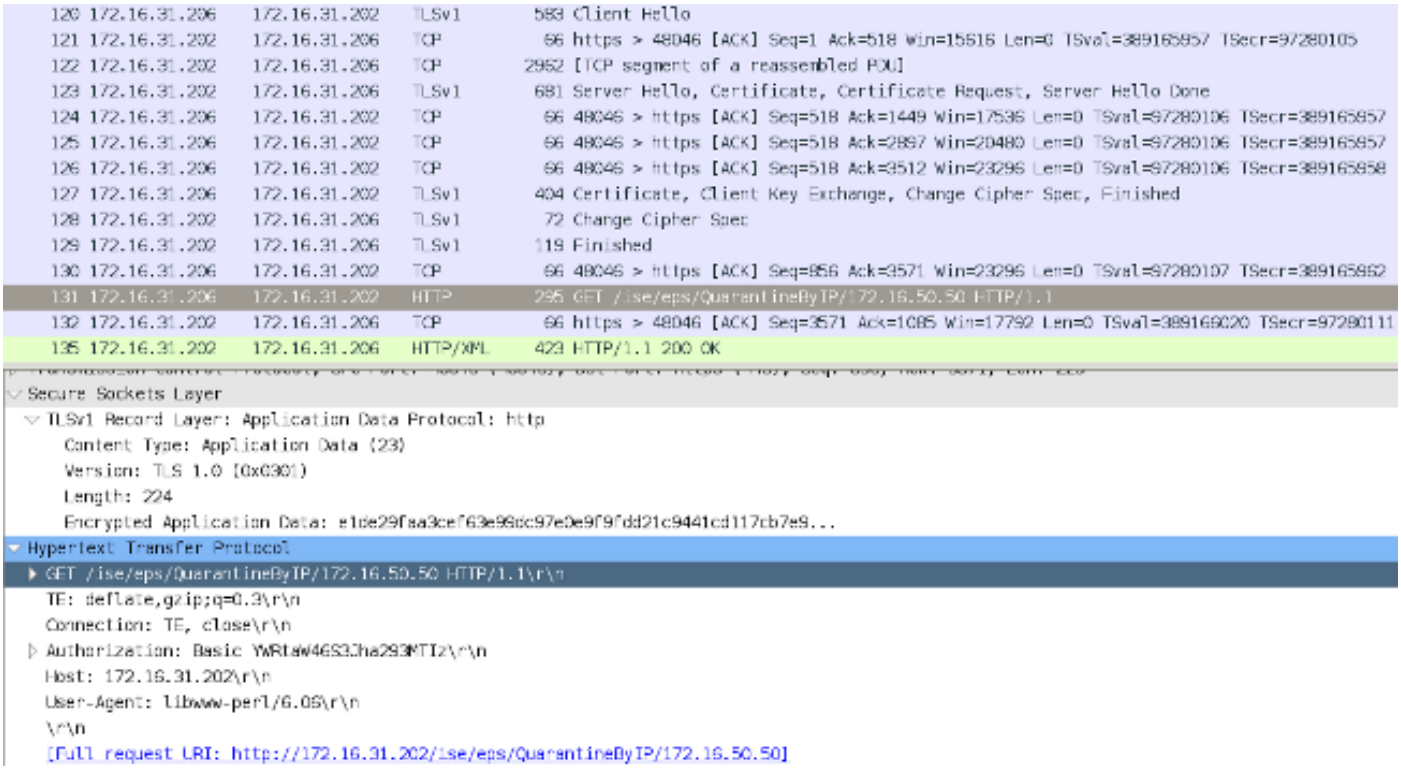
```
May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine
(cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User:
Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown,
 Access Control Rule Name: DropTCP80, Access Control Rule Action: Block,
Access Control Rule Reasons: Unknown, URL Category: Unknown, URL Reputation:
Risk unknown, URL: Unknown, Interface Ingress: eth1, Interface Egress: eth2,
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes:
66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A,
SSL Cipher Suite: N/A, SSL Certificate: 0000000000000000000000000000000000000000,
SSL Subject CN: N/A, SSL Subject Country: N/A, SSL Subject OU: N/A, SSL Subject Org:
N/A, SSL Issuer CN: N/A, SSL Issuer Country: N/A, SSL Issuer OU: N/A, SSL Issuer Org:
N/A, SSL Valid Start Date: N/A, SSL Valid End Date: N/A, SSL Version: N/A, SSL Server
Certificate Status: N/A, SSL Actual Action: N/A, SSL Expected Action: N/A, SSL Server
Name: (null), SSL URL Category: N/A, SSL Session ID:
0000000000000000000000000000000000000000000000000000000000000000, SSL Ticket Id:
0000000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80
```

FireSIGHT يف طابترالا ةسايس ةباصإ

متي تنفيذ ةسايس طابترالا ةرادإل FireSight (زكرم عافدلا)، يتلاو متي غالبإلا اهنع ةطساوب ةلاسر syslog يتلا متي اهلاسرإ نم زكرم عافدلا:

```
May 24 09:37:10 172.16.31.206 SFIMS: Correlation Event:
CorrelateTCP80Block/CorrelationPolicy at Sun May 24 09:37:10 2015 UTCConnection Type:
FireSIGHT 172.16.50.50:49415 (unknown) -> 172.16.32.1:80 (unknown) (tcp)
```

يف هذه ةلحرملا، يستخدم زكرم عافدلا ءاعدتسا REST API (لزعلا) ىلإ ISE، وهي ةسلج لمع HTTPS نكميو كف اهريفشت يف Wireshark (مادختساب نوكملا يفاضإلا طبقلل ةقبطم ذخآم ةنمآلا ليصوتلا (SSL) حاتفملاو صاخلا ةداهشلل ةيرادإلا PAN):



في طلب GET لعنوان IP الخاص بالمهاجم يتم تمريره (172.16.50.50)، وهذا المضيف يتم حظره بواسطة ISE.

انتقل إلى **تحليل > إرتباط > حالة** لتأكيد المعالجة الناجحة:

يقوم ISE بإجراء عزل وإرسال CoA

في هذه المرحلة، يخطر ISE *prrt-management.log* بأنه يجب إرسال CoA:

```
DEBUG  [RMI TCP Connection(142)-127.0.0.1][] cisco.cpm.prrt.impl.PrRTLoggerImpl
-:::- send() - request instanceof DisconnectRequest
        clientInstanceIP = 172.16.31.202
        clientInterfaceIP = 172.16.50.50
       portOption = 0
       serverIP = 172.16.31.100
       port = 1700
       timeout = 5
       retries = 3
       attributes = cisco-av-pair=audit-session-id=ac10206400021000555b9d36
Calling-Station-ID=192.168.10.21
Acct-Terminate-Cause=Admin Reset
```

وقت التشغيل (prrt-server.log) يرسل رسالة *إنهاء* CoA إلى NAD، والتي تنهي الجلسة (ASA):

```
DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893,
CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40 (
DisconnectRequest) Identifier=9 Length=124
    [4] NAS-IP-Address - value: [172.16.31.100]
     [31] Calling-Station-ID - value: [08:00:27:DA:EF:AD]
    [49] Acct-Terminate-Cause - value: [Admin Reset]
    [55] Event-Timestamp - value: [1432457729]
    [80] Message-Authenticator - value:
[00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00]
    [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
```

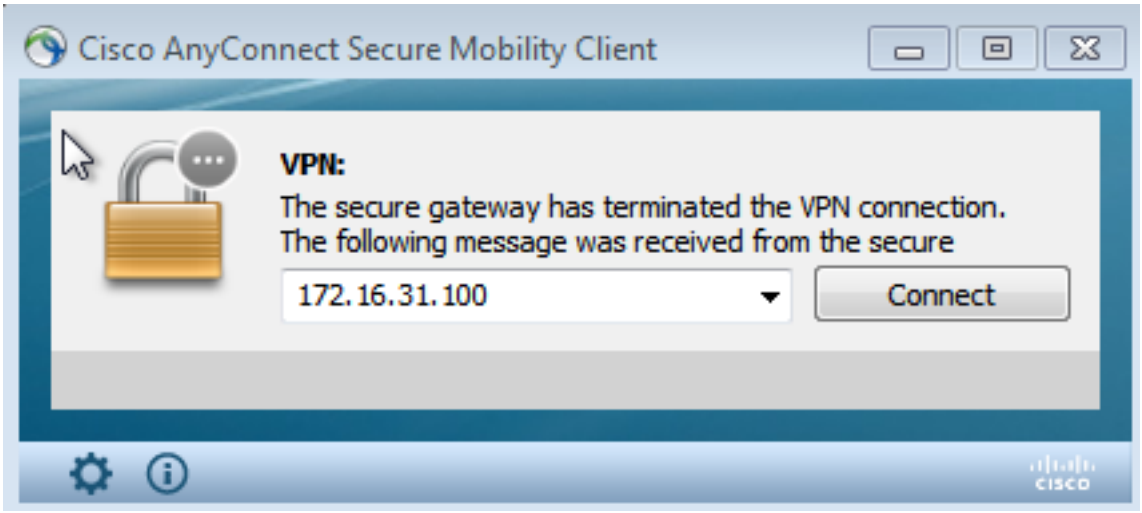
ترسل ISE.psc إخطارا مماثلا لهذا:

```
INFO   [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -::::::- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
```

عند الانتقال إلى **العمليات > المصادقة**، يجب أن يعرض *التفويض الديناميكي بنجاح*.

تم قطع اتصال جلسة عمل VPN

يرسل المستخدم النهائي إشعارا للإشارة إلى قطع اتصال جلسة العمل (تكون هذه العملية شفافة بالنسبة إلى 802.1x/MAB/guest wired/wireless):



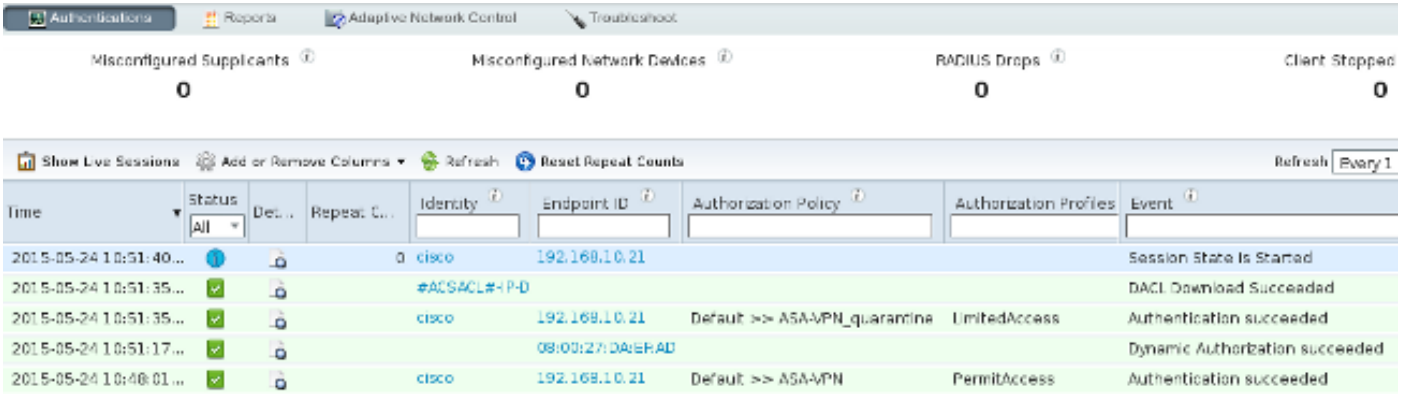
التفاصيل من عرض سجلات Cisco AnyConnect:

```
10:48:05 AM Establishing VPN...
10:48:05 AM Connected to 172.16.31.100.
10:48:20 AM Disconnect in progress, please wait...
10:51:20 AM The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: COA initiated
```

جلسة عمل VPN مع وصول محدود (عزل)

بسبب تكوين *شبكة VPN* المتصلة دائما، يتم إنشاء الجلسة الجديدة على الفور. وفي هذه المرة، يتم الوصول إلى قاعدة ISE *ASA-VPN_QUARANTINE*، التي توفر الوصول المحدود

إلى الشبكة:



ملاحظة: يتم تنزيل قائمة التحكم في الوصول إلى البنية الأساسية (DACL) في طلب منفصل للحصول على RADIUS.

يمكن التحقق من جلسة عمل ذات وصول محدود على ASA باستخدام أمر واجهة سطر الأوامر **show vpn-sessionDB detail anyConnect**:

```
asav# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 39
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.21
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     : 11436                  Bytes Rx     : 4084
Pkts Tx      : 8                      Pkts Rx      : 36
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : POLICY                 Tunnel Group : SSLVPN-FIRESIGHT
Login Time   : 03:43:36 UTC Wed May 20 2015
Duration     : 0h:00m:10s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : ac1020640002700055c02e8
Security Grp : none

.......
DTLS-Tunnel:
 <some output ommited for clarity>
 Filter Name  : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

FireSIGHT (مركز دفاع)

يوجد البرنامج النصي لإصلاح ISE في هذا الموقع:

```
root@Defence:/var/sf/remediations/ISE_1.3.19# ls
```

```
_lib_  ise-instance  ise-test.pl  ise.pl  module.template
```

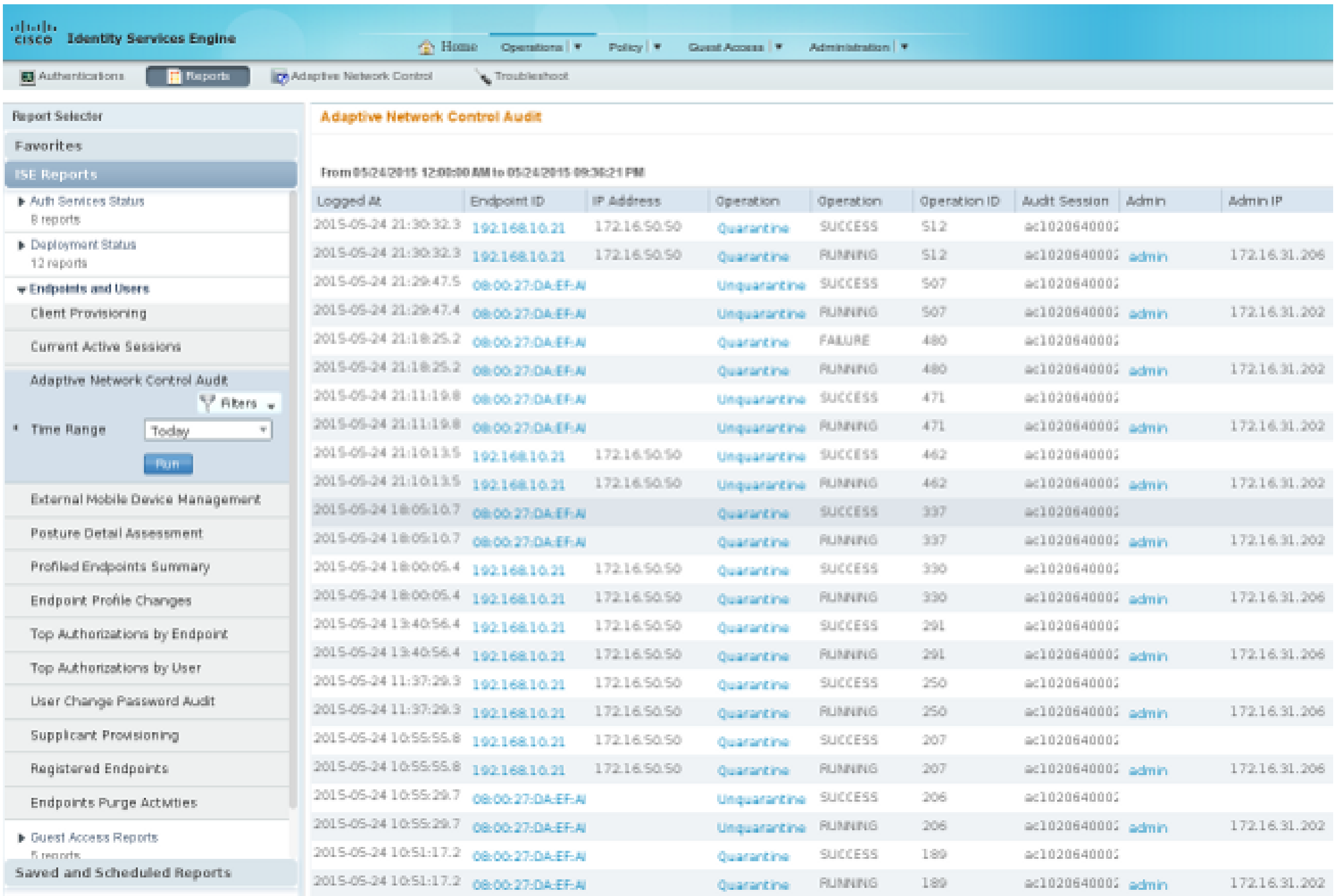
هذا نص برمجي بسيط يستخدم نظام تسجيل SourceFire (SF) الفرعي القياسي. ما إن يتم الحل، أنت يستطيع أكدت النتيجة عن طريق ال */var/log/messages*:

```
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) 172.16.31.202 - Success 200 OK - Quarantined
172.16.50.50 as admin
```

محرك خدمات كشف الهوية (ISE)

من المهم تمكين خدمة التحكم في الشبكة التكييفية على ISE. لعرض السجلات التفصيلية في عملية وقت التشغيل (*prrt-management.log* و*prrt-server.log*)، يجب تمكين مستوى تصحيح الأخطاء ل Runtime-AAA. انتقل إلى **إدارة > نظام > تسجيل > تكوين سجل تصحيح الأخطاء** لتمكين تصحيح الأخطاء.

يمكنك أيضا الانتقال إلى **العمليات > التقارير > نقاط النهاية والمستخدمين > تدقيق عنصر التحكم في الشبكة القابل للتكيف** لعرض المعلومات الخاصة بكل محاولة وكل نتيجة لأي طلب عزل:



حشرات

أحلت cisco بق id CSCuu41058 (ISE 1.4 نهاية تحصين عدم تساوق و VPN إخفاق) لمعلومة حول ISE خطأ أن يكون متعلق VPN جلسة إخفاق (802.1x/MAB يعمل غرامة).

معلومات ذات صلة

-
- تكامل ISE الإصدار 1.3 PXgrid مع تطبيق IPS PXlog
- دليل مسؤول محرك خدمات الهوية من Cisco، الإصدار 1.4 - إعداد التحكم في الشبكة القابل للتكيف
- الدليل المرجعي لواجهة برمجة التطبيقات (API) لمحرك خدمات الهوية من Cisco، الإصدار 1.2 - مقدمة إلى واجهة برمجة التطبيقات (API) الخارجية لـ Identity Services
- الدليل المرجعي لواجهة برمجة التطبيقات الخاصة بمحرك خدمات الهوية من Cisco، الإصدار 1.2 - مقدمة إلى واجهات برمجة التطبيقات (REST)
- دليل مسؤول محرك خدمات الهوية من Cisco، الإصدار 1.3
- دعم & توثيق - سيسكو سيستمز

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).