

# و ISE لم اكن م اءءءء ساب ء ال ص إا ا تام ءء ن ءو كء FirePOWER

## المءءوءاء

[المءءوءة](#)

[المءءوءاء الأءاساءة](#)

[المءءوءاء](#)

[المءوءاء المءءءوءة](#)

[الءءوءءن](#)

[الرءم الءءءوءءء للءءءءة](#)

[FireSIGHT Management Center \(مركء ءءاع\)](#)

[وءءة معالءة ISE](#)

[ساءة الاربءاء](#)

[ASA](#)

[مءرك ءءماء كءء الهوءة \(ISE\)](#)

[ءءوءءن ءءاز الوءوء إلى الءءءة \(NAD\)](#)

[ءمءن الءءءم ءء الءءءة المءءءوءة](#)

[ءACL العزل](#)

[مءء ءءءءء الءءوءء للءءل](#)

[قواءء الءءوءءل](#)

[الءءءق من الصءءة](#)

[ءءء ءءسة عمل AnyConnect ASA VPN](#)

[إءاءة ساءة الاربءاء ءء FireSIGHT](#)

[ءقوء ISE باءراء عزل وارسال CoA](#)

[ءم قءع اءءال ءءسة عمل VPN](#)

[اسءكءاف الأءءاء وإءلاءءا](#)

[FireSIGHT \(مركء ءءاع\)](#)

[مءرك ءءماء كءء الهوءة \(ISE\)](#)

[ءءءاء](#)

[مءلوءاء ءاء صءة](#)

## المءءوءة

ءوءءء ءءا المءءءءء ءءءوءة إءءءءءء وءءة المءءءءة النمءوءة على ءءاز FireSIGHT من Cisco لاءءءءاف الءءءاء وإءلاءء المءاءءم ءلءاءبباً باءءءءءء مءرك ءءمة الهوءة (ISE) من Cisco كءاءم نءءء. ءءء المءال الواءء ءء ءءا المءءءءء الطرءءة الءءء ءءم إءءءءءءا لمءءءءة مءءءءءم صءءة VPN عن بعء الءءء ءقوءم بالمءاءءة عبر ISE، وءكن ءمءن إءءءءءءا أءبءا لمءءءءءم سلءءة أو لاسلكبء 802.1x/MAB/WebAuth.

مءلاءءة: لا ءءءم Cisco رسمبب وءءة المءءءءة النمءوءة المءءءر إءبب ءء ءءا المءءءءء. وءءم مءءءءءءا على ءوابة

مجتمع ويمكن إستخدامها من قبل أي شخص. في الإصدارات 5.4 والإصدارات الأحدث، هناك أيضا وحدة معالجة أحدث متوفرة استنادا 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 (VPN) (ASA 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 المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## التكوين

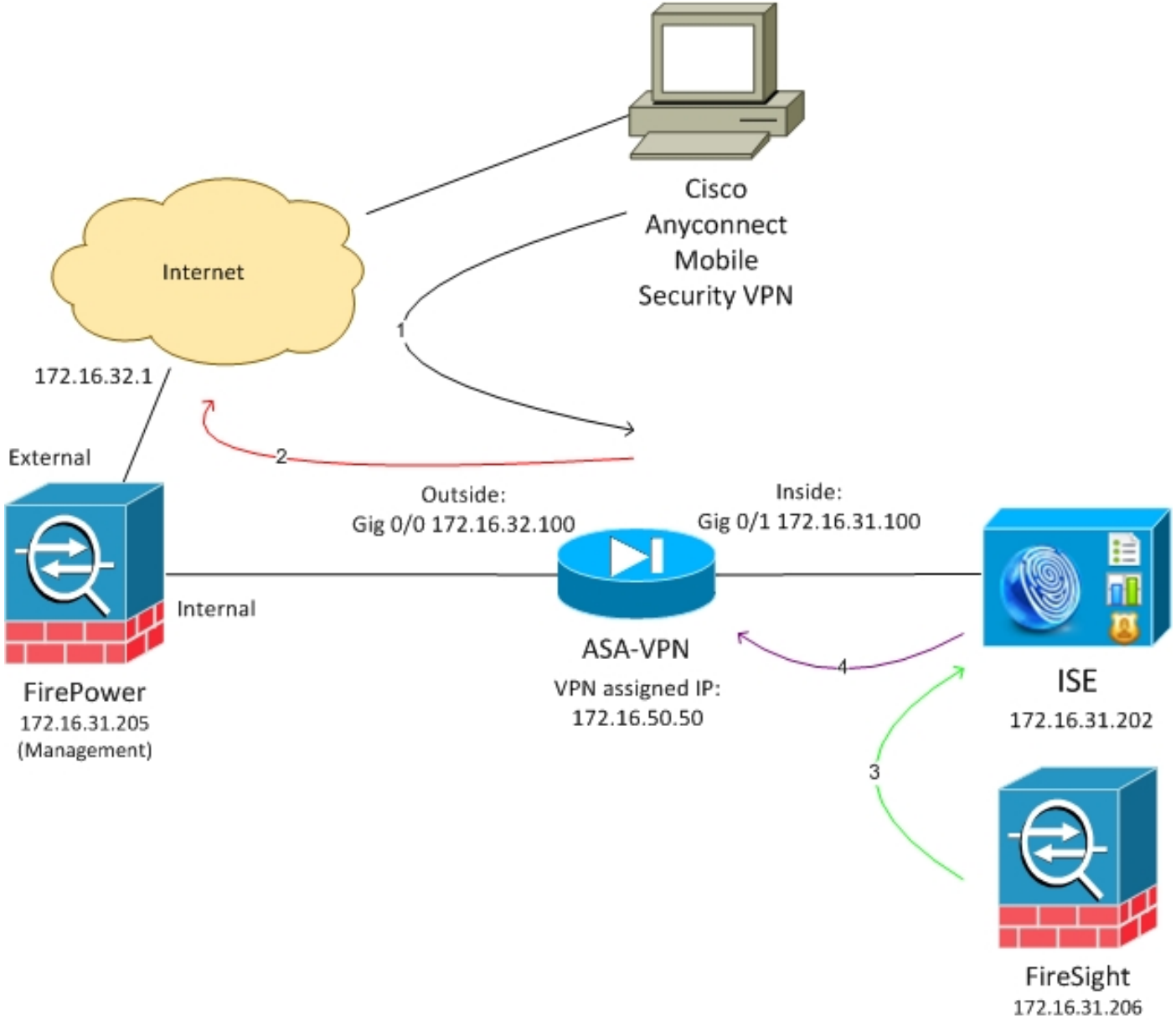
أستخدم المعلومات المقدمة في هذا القسم لتكوين النظام.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [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:

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

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

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

ما إن يستلم ISE ال REST API نداء، هو يبحث عن الجلسة وبرسل RADIUS تغير من تخويل (CoA) إلى ال ASA، أي ينهي أن جلسة.

5. يقطع ال ASA ال 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، لا يهم كيفية اتصال المستخدم بالشبكة ومصادقته لها؛ طالما يتم استخدام ISE للمصادقة والتفويض، فإن المستخدم لديه وصول محدود إلى الشبكة بسبب الحجر الصحي.

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

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

## FirePOWER

**ملاحظة:** يتم استخدام 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.

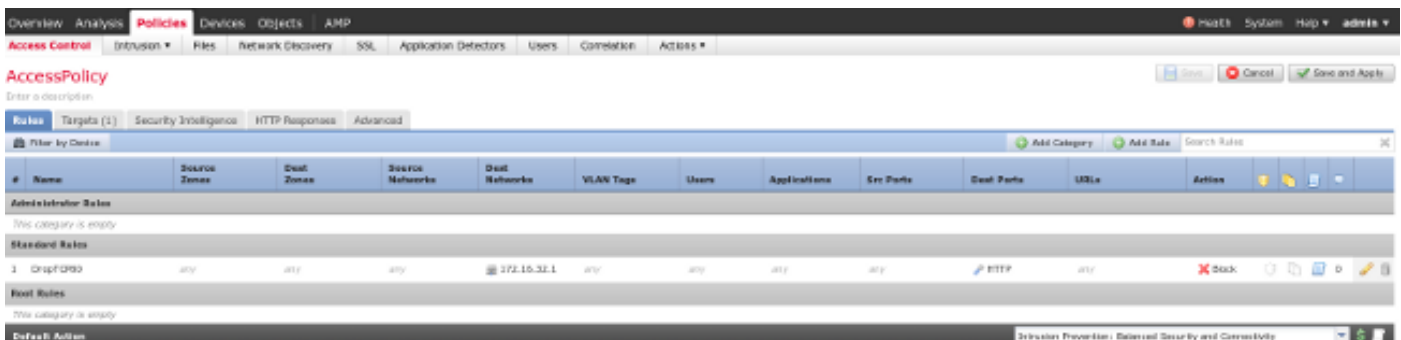
تشتمل الأجهزة الافتراضية على ثلاث واجهات، واحدة للإدارة واثنان للتفتيش الداخلي (داخلي/خارجي).

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

## FireSIGHT Management Center (مركز دفاع)

### سياسة التحكم في الوصول

بعد تثبيت التراخيص الصحيحة وإضافة جهاز FirePower، انتقل إلى السياسات < التحكم في الوصول وإنشاء سياسة الوصول التي يتم استخدامها 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



## Sourcefire Downloads

### ISE 1.2 Remediation Beta 1.3.19

February 04, 2015 | 38.6 KB | md5

[View](#) [Remediation](#)

This community supported remediation module allows for the automated interaction with Cisco Identity Services Engine (ISE) version 1.2. This interaction performs a quarantine of the desired IP (Source or Destination) based on the user configuration of the remediation. This quarantine action can be triggered by any event that occurs on the Sourcefire Defense Center that contains a source or destination IP address.

انتقل إلى السياسات < العمليات < التصحيحات < الوحدات النمطية وقم بتثبيت الملف:



**Success**  
Module successfully installed

### Installed Remediation Modules

Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall
ISE 1.2 Remediation	1.3.19	Quarantine IP addresses using Identity Services Engine 1.2
Nmap Remediation	2.0	Perform an Nmap Scan
Set Attribute Value	1.0	Set an Attribute Value

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

## Edit Instance

Instance Name	<input type="text" value="ise-instance"/>
Module	ISE 1.2 Remediation (v1.3.19)
Description	<div style="border: 1px solid #ccc; height: 100px;"></div>
Primary Admin Node IP	<input type="text" value="172.16.31.202"/>
Secondary Admin Node IP <i>(optional)</i>	<input type="text"/>
Username	<input type="text" value="admin"/>
Password <i>Retype to confirm</i>	<input type="password" value="....."/> <input type="password"/>
SYSLOG Logging	<input checked="" type="radio"/> On <input type="radio"/> Off
White List <i>(an optional list of networks )</i>	<div style="border: 1px solid #ccc; height: 100px;"></div>

كما يجب استخدام عنوان IP للمصدر (المهاجم) للإصلاح:

## Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		
Add a new remediation of type		<input type="button" value="Add"/>
	<input type="text" value="Quarantine Source IP"/>	

يجب تكوين قاعدة إرتباط 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:

The screenshot shows the 'Policy Management' section, specifically 'Rule Management'. The 'Rule Information' section includes:

- Rule Name: CorrelateTCP80Block
- Rule Description: (empty)
- Rule Group: Ungrouped

The 'Select the type of event for this rule' section shows the rule is triggered 'If a connection event occurs at the beginning of the connection and it meets the following conditions:'. A condition is added: 'Access Control Rule Name contains the string DropTCP80'.

The 'Rule Options' section shows 'Snooze' set to 0 hours and 'Inactive Periods' as 'There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".'

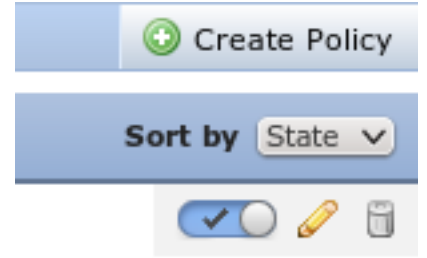
يتم استخدام هذه القاعدة في نهج الارتباط. انتقل إلى السياسات < الارتباط > إدارة السياسات لإنشاء سياسة جديدة، ثم أضف القاعدة التي تم تكوينها. انقر فوق إصلاح على اليمين وأضفت إجرائن: إصلاح ل sourceIP (تم تكوينه مسبقا) syslog:

The screenshot shows the 'Policy Management' section, specifically 'Rule Management'. The 'Correlation Policy Information' section includes:

- Policy Name: CorrelateTCP80Block
- Policy Description: (empty)
- Output Priority: (empty)

The 'Policy Rules' section shows a table with one rule: 'CorrelateTCP80Block' with a response of 'syslog (syslog)' and a priority of 'Default'. A modal window titled 'Responses for CorrelateTCP80Block' is open, showing 'Assigned Responses' with 'syslog (syslog)' and 'Unassigned Responses' (empty).

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.

## DAACL العزل

من أجل إنشاء قائمة تحكم في الوصول (DAACL) يمكن تنزيلها والتي يتم استخدامها للمضيفين المعزولين، انتقل إلى السياسة < النتائج < التفويض < قائمة التحكم في الوصول (ACL) القابلة للتنزيل.

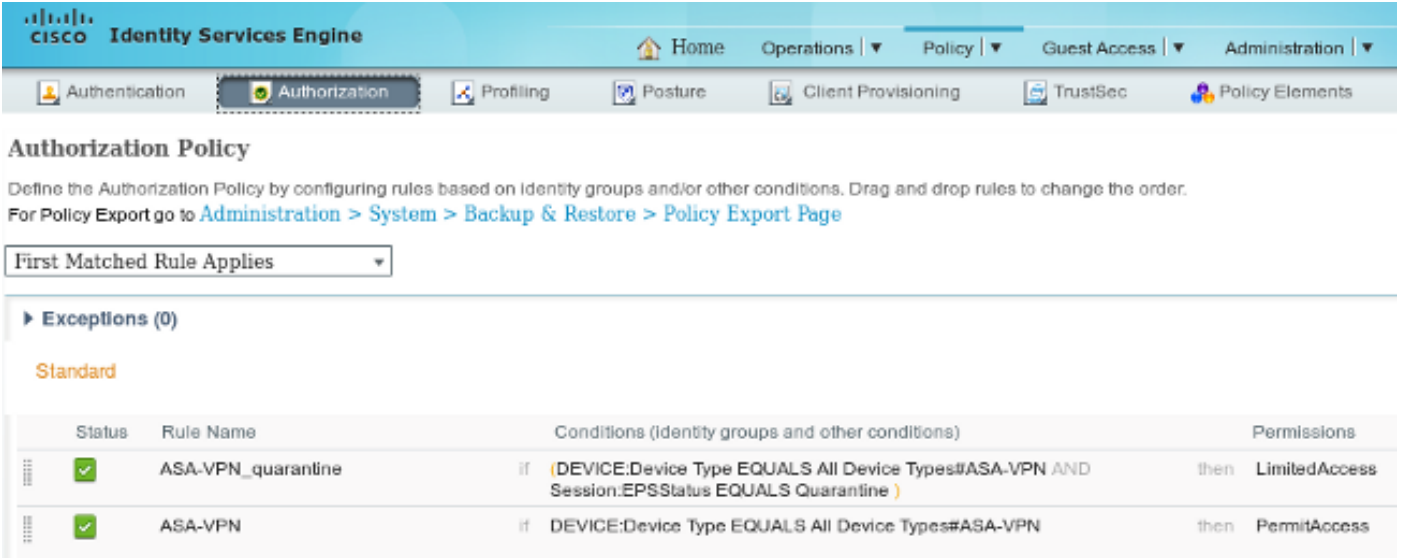
## ملف تعريف التحويل للعزل

انتقل إلى السياسة < النتائج < التحويل < ملف تعريف التحويل وقم بإنشاء ملف تعريف تحويل باستخدام قائمة التحكم في الوصول الخاصة بالمنفذ (DAACL) الجديدة:

## قواعد التحويل

يجب إنشاء قاعدتين للتحويل. 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:



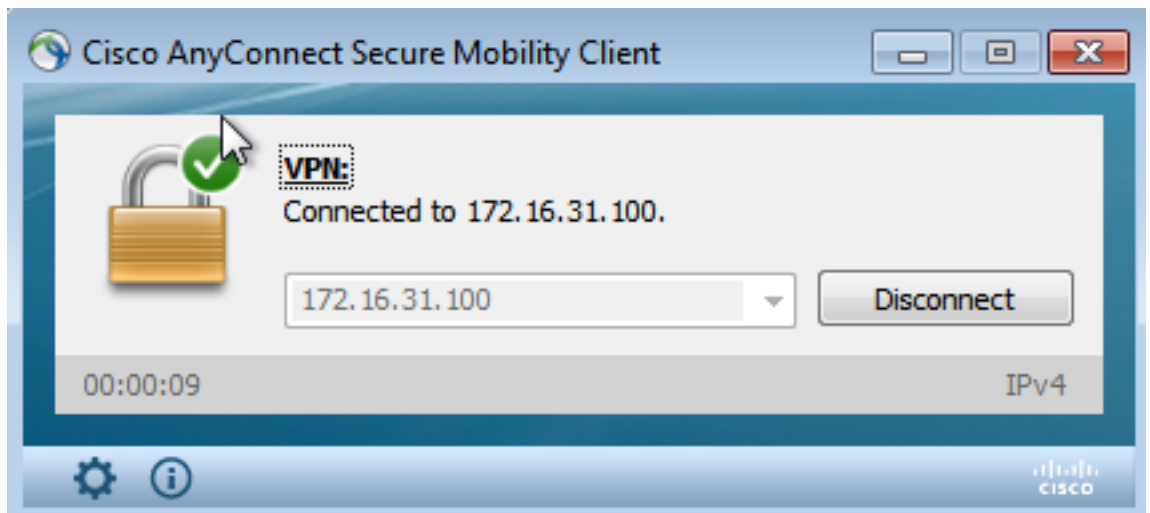
The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Policy. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. The main menu has tabs for Authentication, Authorization (selected), Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The page title is "Authorization Policy". Below the title, there is a description: "Define the Authorization Policy by configuring rules based on Identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page". A dropdown menu is set to "First Matched Rule Applies". Under "Exceptions (0)", there is a "Standard" section with a table of rules:

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	ASA-VPN_quarantine	if (DEVICE:Device Type EQUALS All Device Types#ASA-VPN AND Session:EPSStatus EQUALS Quarantine )	then LimitedAccess
✓	ASA-VPN	if DEVICE:Device Type EQUALS All Device Types#ASA-VPN	then PermitAccess

## 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>
```

## محاولة المستخدم الوصول

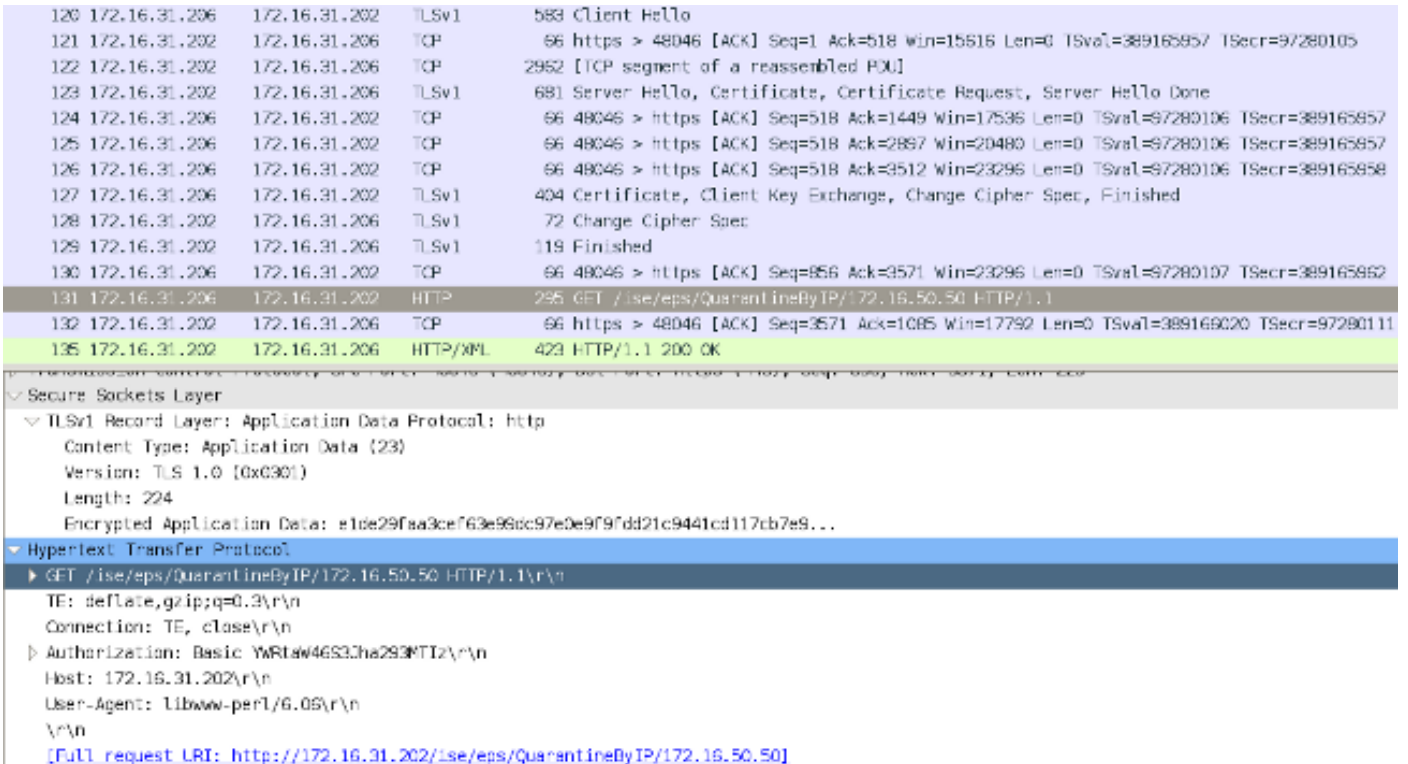
بمجرد أن يحاول المستخدم الوصول إلى <http://172.16.32.1>، يتم الوصول إلى سياسة الوصول، ويتم حظر حركة مرور البيانات المطابقة في السطر، ويتم إرسال رسالة syslog من عنوان IP الخاص بإدارة FirePower:

```
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
,Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A ,66
,SSL Cipher Suite: N/A, SSL Certificate: 0000000000000000000000000000000000000000000000000000000
: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
:SSL Ticket Id ,00000000000000000000000000000000000000000000000000000000000000000000000000000000
TCP} 172.16.50.50:49415 -> 172.16.32.1:80} ,00000000000000000000000000000000000000000000000000000000
```

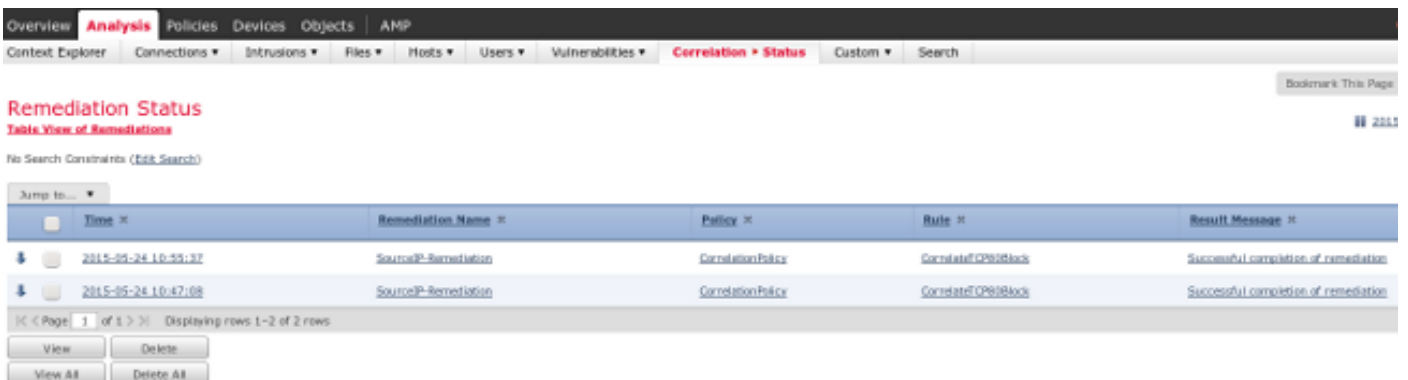
## إصابة سياسة الارتباط في FireSIGHT

يتم تنفيذ سياسة الارتباط لإدارة FireSight (مركز الدفاع)، والتي يتم الإبلاغ عنها بواسطة رسالة syslog التي يتم إرسالها من مركز الدفاع:

```
: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
في هذه المرحلة، يستخدم مركز الدفاع إستدعاء REST API (العزل) إلى ISE، وهي جلسة عمل HTTPS ويمكن فك تشفيرها في Wireshark (باستخدام المكون الإضافي لطبقة مآخذ التوصيل الآمنة (SSL) والمفتاح الخاص
```



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 *prrt-management.log* ISE 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 تنتهي الجلسة (ASA):

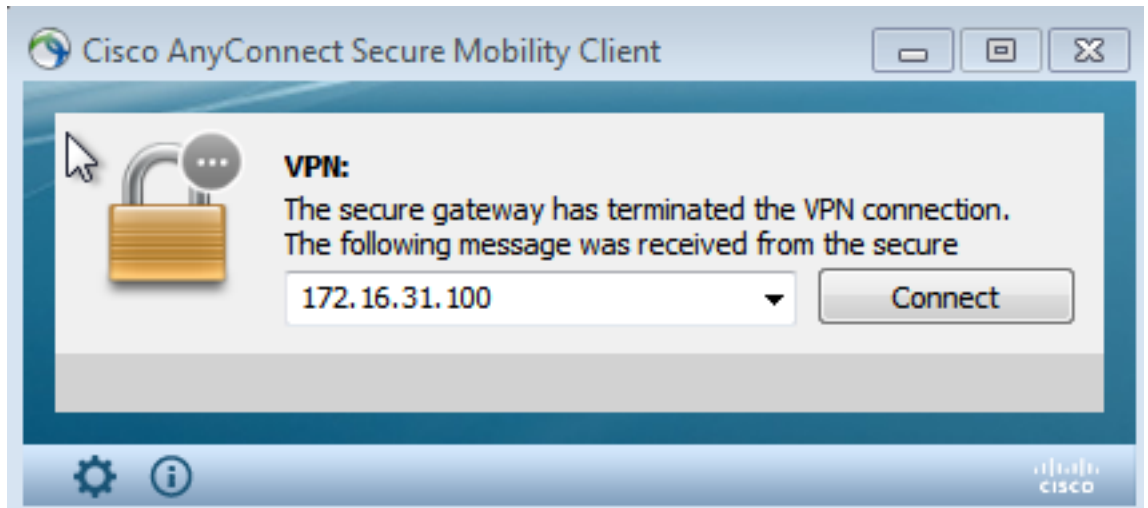
```
,DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893
) CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40
DisconnectRequest) Identifier=9 Length=124
[NAS-IP-Address - value: [172.16.31.100 [4]
[Calling-Station-ID - value: [08:00:27:DA:EF:AD [31]
[Acct-Terminate-Cause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

```
...AM Establishing VPN 10:48:05
.AM Connected to 172.16.31.100 10:48:05
...AM Disconnect in progress, please wait 10:48:20
.AM The secure gateway has terminated the VPN connection 10:51:20
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:

Misconfigured Supplicants		Misconfigured Network Devices		RADIUS Drops		Client Stopped	
0		0		0		0	

Time	Status	Def...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-05-24 10:51:40...			0	cisco	192.168.10.21			Session State Is Stated
2015-05-24 10:51:35...				#ACSACL#-IP-D				ACL Download Succeeded
2015-05-24 10:51:35...				cisco	192.168.10.21	Default >> ASA-VPN_quarantine	LimitedAccess	Authentication succeeded
2015-05-24 10:51:17...					08:00:27:DA5EFA0			Dynamic Authorization succeeded
2015-05-24 10:48:01...				cisco	192.168.10.21	Default >> ASA-VPN	PermitAccess	Authentication succeeded

**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    : ac10206400027000555c02e8
Security Grp    : none
.....
:DTLS-Tunnel
<some output omitted for clarity>
Filter Name     : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76

```

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها 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_
```

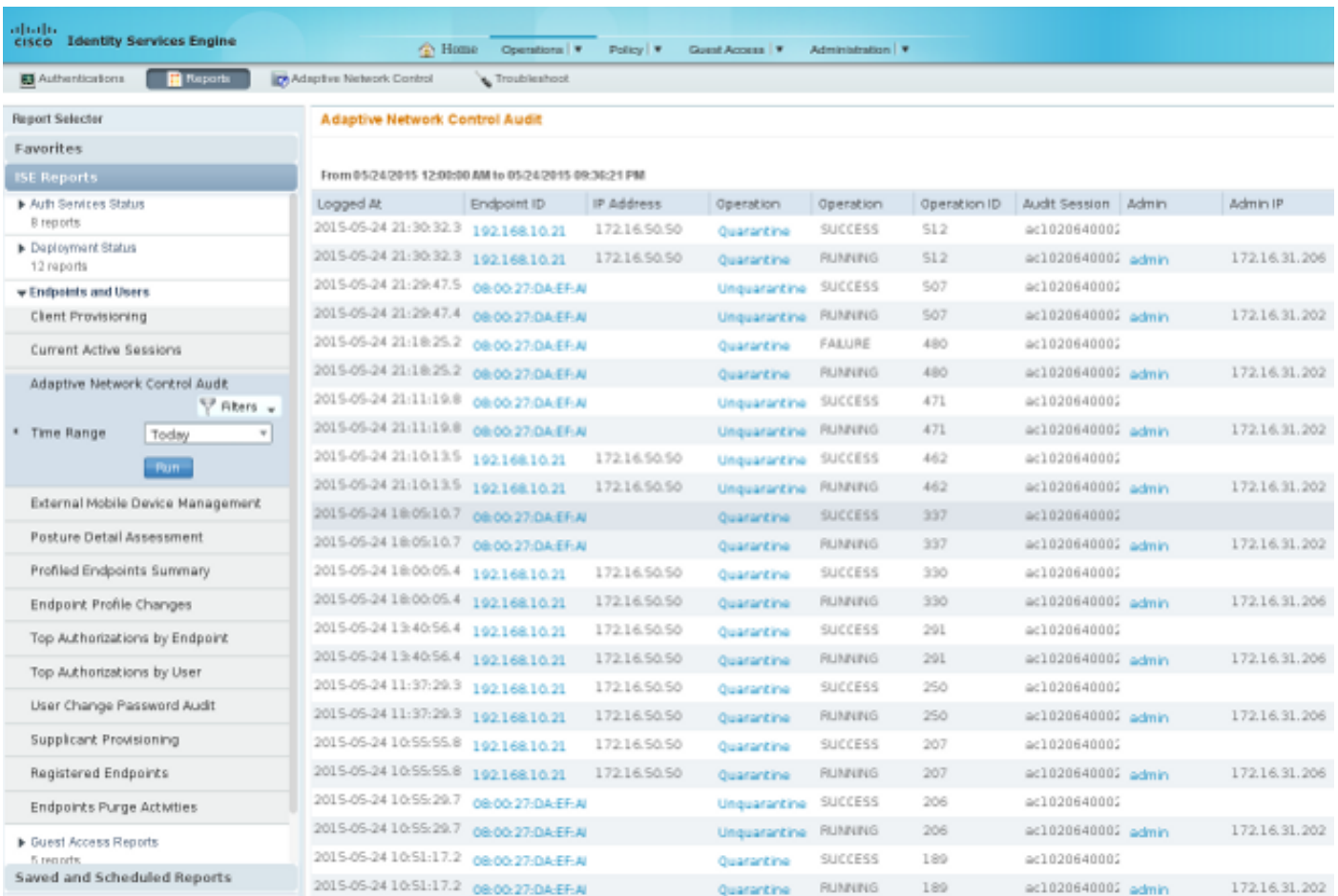
هذا نص برمجي بسيط يستخدم نظام تسجيل (SourceFire (SF) الفرعي القياسي. ما إن يتم الحل، أنت تستطيع أكدت النتيجة عن طريق ال `:var/log/messages/`

```
[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
as admin 172.16.50.50
```

## محرك خدمات كشف الهوية (ISE)

من المهم تمكين خدمة التحكم في الشبكة التكميلية على ISE. لعرض السجلات التفصيلية في عملية وقت التشغيل (`prrt-server.log` و `prrt-management.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:



Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session	Admin	Admin IP
2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	512	ac102064000;		
2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	512	ac102064000;	admin	172.16.31.206
2015-05-24 21:29:47.5	08:00:27:DA:EF:A		Unquarantine	SUCCESS	507	ac102064000;		
2015-05-24 21:29:47.4	08:00:27:DA:EF:A		Unquarantine	RUNNING	507	ac102064000;	admin	172.16.31.202
2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	FAILURE	480	ac102064000;		
2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	RUNNING	480	ac102064000;	admin	172.16.31.202
2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	SUCCESS	471	ac102064000;		
2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	RUNNING	471	ac102064000;	admin	172.16.31.202
2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	SUCCESS	462	ac102064000;		
2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	RUNNING	462	ac102064000;	admin	172.16.31.202
2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	SUCCESS	337	ac102064000;		
2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	RUNNING	337	ac102064000;	admin	172.16.31.202
2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	330	ac102064000;		
2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	330	ac102064000;	admin	172.16.31.206
2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	291	ac102064000;		
2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	291	ac102064000;	admin	172.16.31.206
2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	250	ac102064000;		
2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	250	ac102064000;	admin	172.16.31.206
2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	207	ac102064000;		
2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	RUNNING	207	ac102064000;	admin	172.16.31.206
2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	SUCCESS	206	ac102064000;		
2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	RUNNING	206	ac102064000;	admin	172.16.31.202
2015-05-24 10:51:17.2	08:00:27:DA:EF:A		Quarantine	SUCCESS	189	ac102064000;		
2015-05-24 10:51:17.2	08:00:27:DA:EF:A		Quarantine	RUNNING	189	ac102064000;	admin	172.16.31.202

## حشرات

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

## معلومات ذات صلة

- [تكوين تكامل WSA مع ISE لخدمات TrustSec المدركة](#)
- [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 ل Identity Services](#)
- [الدليل المرجعي لواجهة برمجة التطبيقات الخاصة بمحرك خدمات الهوية من Cisco، الإصدار 1.2 - مقدمة إلى مراقبة واجهات برمجة التطبيقات \(REST\)](#)
- [دليل مسؤول محرك خدمات الهوية من Cisco، الإصدار 1.3](#)
- [الدعم التقني والمستندات - سيسكو سيستمز](#)



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء دختسمل معد وء مء مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظءالم ءرء. ةصاءل مء ءل ب  
Cisco ءلءت. فرءم مچرت مءم دقء ءلءل ةء فارءءال ةمچرتل عم لءل او  
ءل ءمءءءء ءوچرلاب ءصوءء وء ءمچرتل هذه ةقء نء ءءل وءءس م  
Systems (رفوءم طبارل) ءل صأل ءرءل ءلءل دن تسمل