ISE和FirePower整合 — 補救服務示例

目錄

簡介

本文檔介紹如何使用Cisco FireSight裝置上的補救模組檢測攻擊，並使用Cisco身份服務引擎(ISE)作為策略伺服器自動補救攻擊者。本文檔中提供的示例描述了用於補救通過ISE進行身份驗證的遠端VPN使用者的方法，但它也可以用於802.1x/MAB/WebAuth有線或無線使用者。

附註：本文檔中引用的補救模組不是思科正式支援的。在社群門戶上共用，任何人都可以使用

。在5.4及更高版本中，還有一個基於*pxGrid*協定的更新補救模*塊可*用。6.0版不支援此模組，但計畫在未來版本中支援此模組。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Adaptive Security Appliance(ASA)VPN配置
- Cisco AnyConnect Security Mobility Solution — 遠端存取
- Cisco FireSight基本配置
- Cisco FirePower基本配置
- Cisco ISE配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7
- Cisco ASA 9.3版或更高版本
- Cisco ISE軟體版本1.3及更高版本
- Cisco AnyConnect安全行動化使用者端版本3.0及更新版本
- Cisco FireSight管理中心版本5.4
- Cisco FirePower 5.4版(虛擬機器(VM))

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

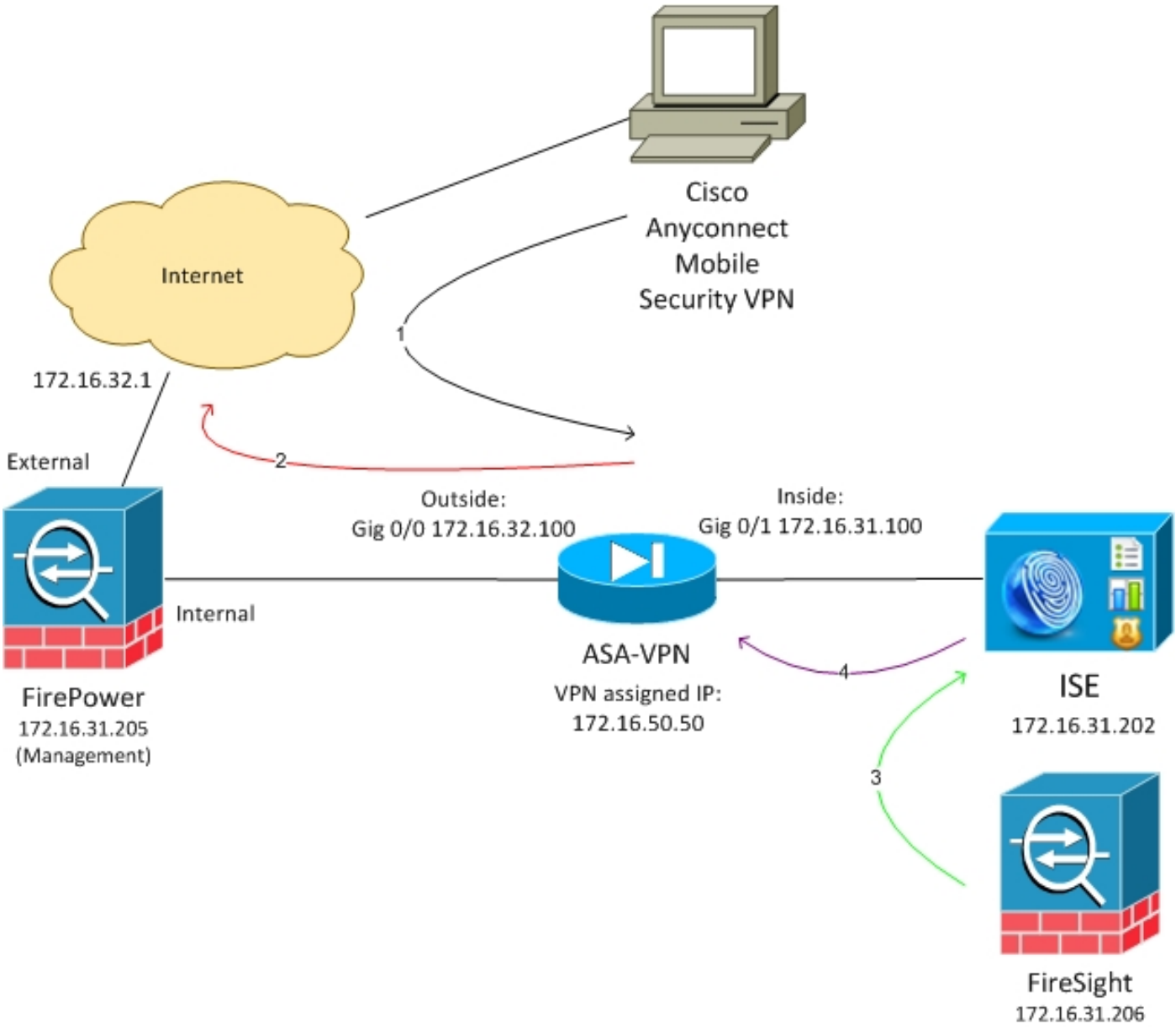
設定

使用本節提供的資訊來配置系統。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表

本文所述的範例使用以下網路設定：



以下是此網路設定的流程：

1. 使用者啟動與ASA的遠端VPN會話（通過Cisco AnyConnect安全移動版本4.0）。

2. 使用者嘗試訪問*http://172.16.32.1*。（流量通過FirePower移動，FirePower安裝在VM上並由FireSight管理。）

3. FirePower經過配置，能夠阻止（內嵌）特定流量（訪問策略），但它也具有已觸發的關聯策略。因此，它通過REST應用程式設計介面(API)(*QuarantineByIP方法)啟*動ISE補救。

4. ISE收到REST API呼叫後，會查詢會話並向ASA傳送RADIUS授權更改(CoA),ASA將終止該會話。

5. ASA斷開VPN使用者的連線。由於AnyConnect已配置*永遠線上*VPN訪問，因此會建立一個新會話；但是，這一次匹配了不同的ISE授權規則（對於隔離主機），並提供有限的網路訪問。在這個階段，使用者如何連線和驗證網路並不重要；只要ISE用於身份驗證和授權，使用者由於隔離而擁有有限的網路訪問許可權。

如前所述，只要使用ISE進行身份驗證，且網路接入裝置支援RADIUS CoA（所有現代Cisco裝置），此方案適用於任何型別的已驗證會話（VPN、有線802.1x/MAB/Webauth、無線

802.1x/MAB/Webauth）。

> **提示：**為了將使用者移出隔離區，您可以使用ISE GUI。補救模組的未來版本也可能支援該模組。

FirePower

> **附註**：VM裝置用於本文檔中描述的示例。僅通過CLI執行初始配置。所有策略都是從思科防禦中心配置的。如需更多詳細資訊，請參閱本檔案的相關資訊一節。

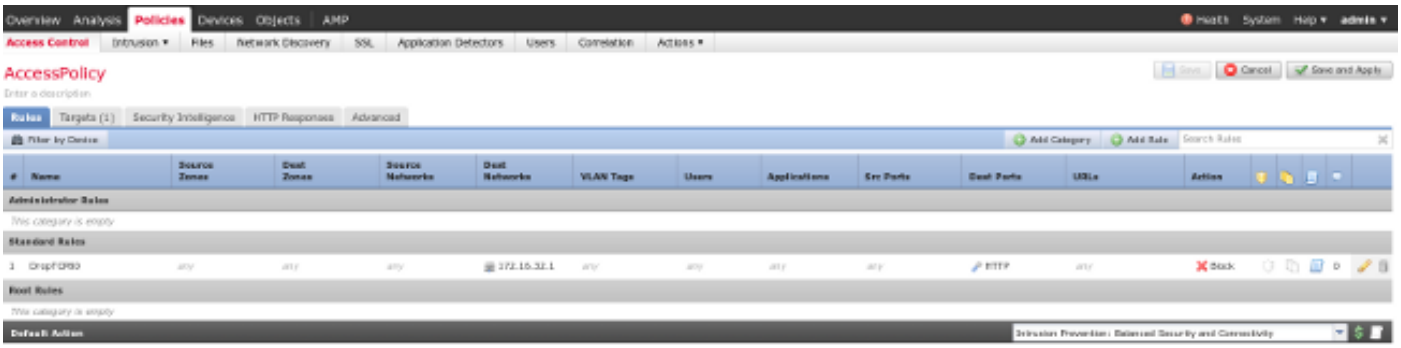
虛擬機器有三個介面，一個用於管理，兩個用於內聯檢查（內部/外部）。

來自VPN使用者的所有流量通過FirePower移動。

FireSight管理中心（防禦中心）

訪問控制策略

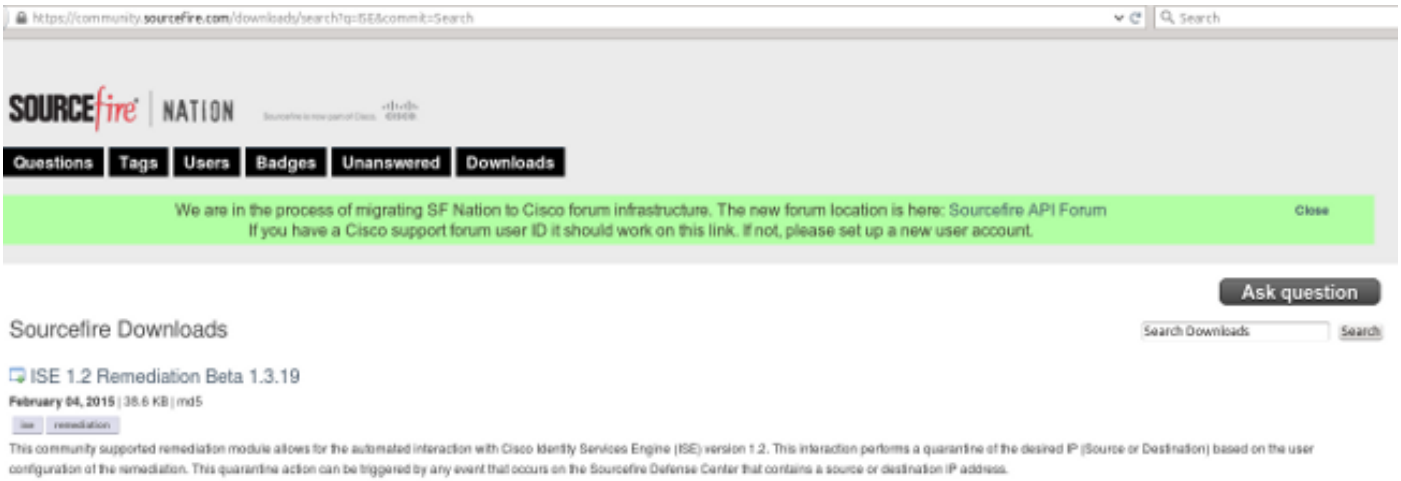
安裝正確的許可證並新增FirePower裝置後，導航到**Policies > Access Control**，然後建立用於將HTTP流量丟棄到172.16.32.1的訪問策略：



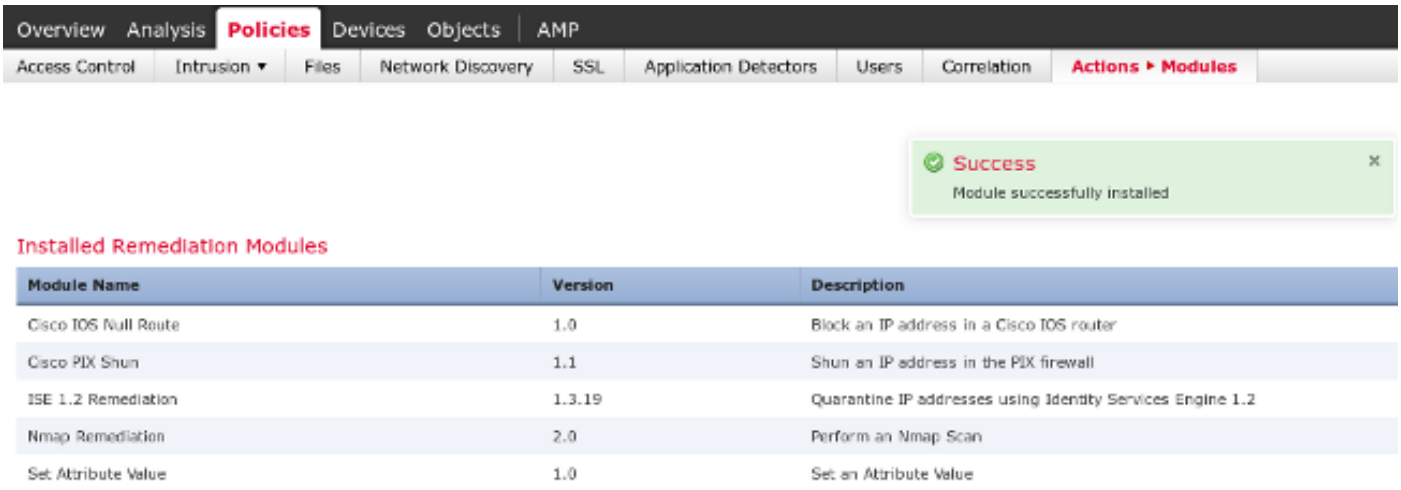
接受所有其他流量。

ISE補救模組

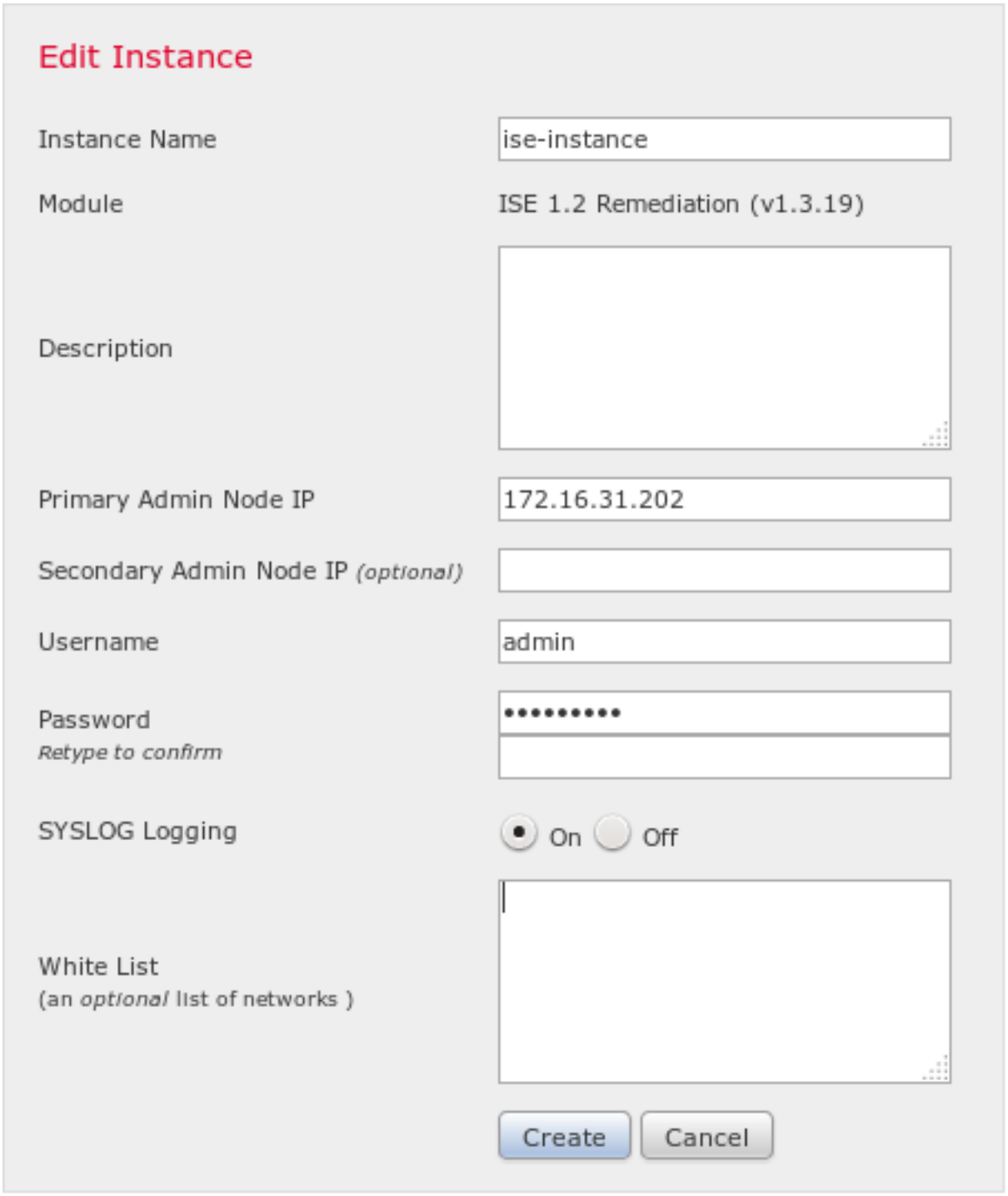
在社群門戶上共用的ISE模組的當前版本為*ISE 1.2 Remediation Beta 1.3.19*：



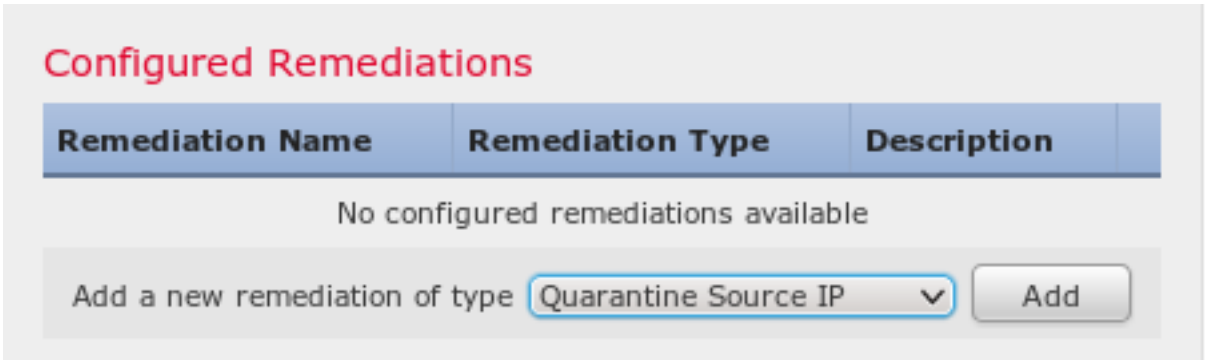
導航到**Policies > Actions > Remediations > Modules**並安裝檔案：



然後應建立正確的例項。導航到**Policies > Actions > Remediations > Instances**，並提供策略管理節點(PAN)的IP地址以及REST API所需的ISE管理憑據(建議使用具有*ERS Admin*角色的獨立使用者):

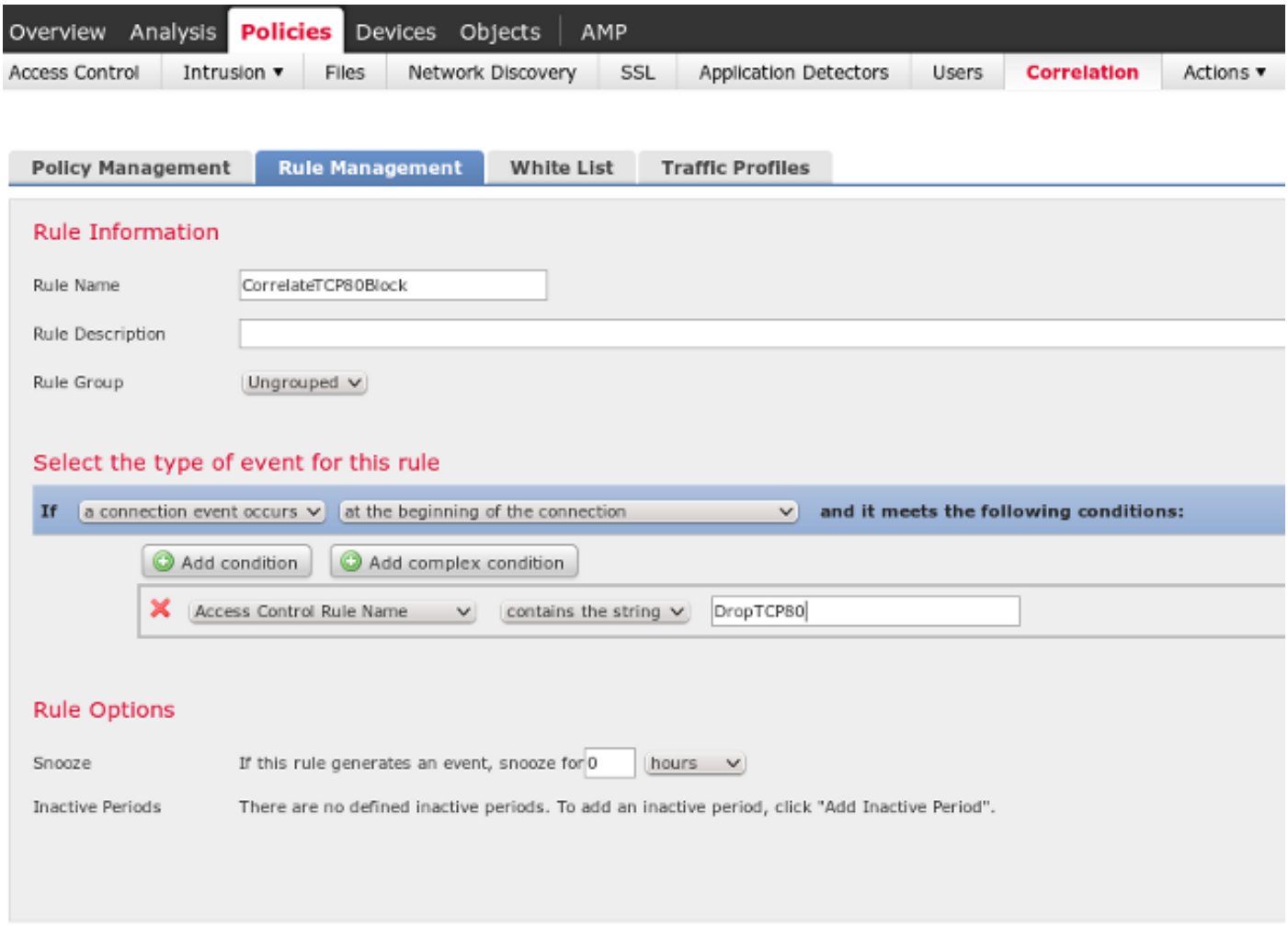


源IP地址（攻擊者）也應用於補救：

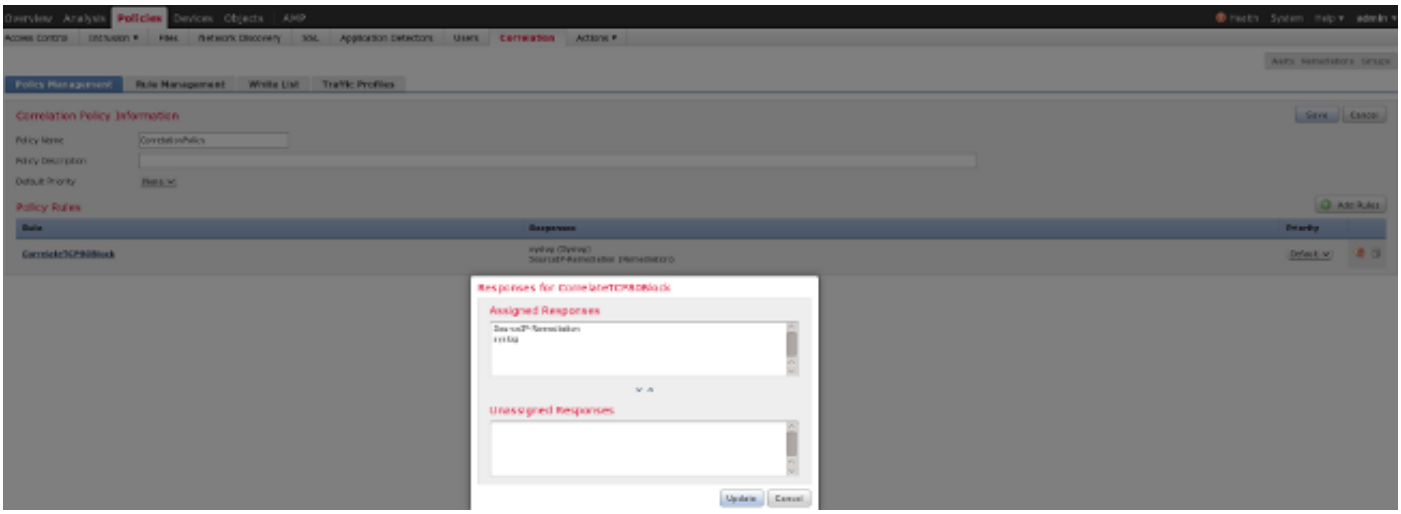


關聯策略

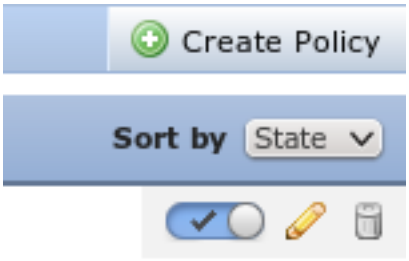
現在必須配置特定的關聯規則。此規則在連線開始時觸發，該連線與之前配置的訪問控制規則(*DropTCP80)相*匹配。 要配置規則，請導航到**Policies > Correlation > Rule Management**:



此規則用於關聯策略。導航到**Policies > Correlation > Policy Management**以建立新策略，然後新增配置的規則。按一下右側的**Remediate**並新增兩個操作：**針對源IP(**之前配置)和系統日誌**的補救**:



確保啟用關聯策略：



ASA

充當VPN網關的ASA配置為使用ISE進行身份驗證。還必須啟用記帳和RADIUS CoA:

```
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
```

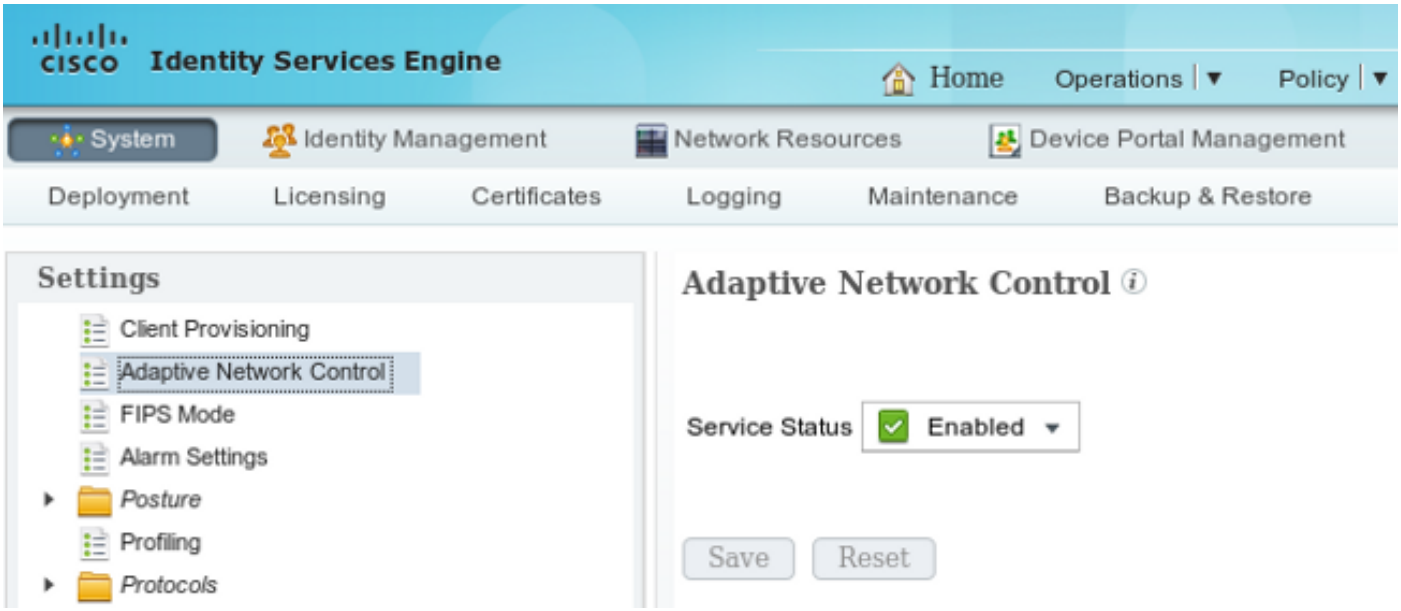
ISE

設定網路存取裝置(NAD)

導覽至**Administration > Network Devices**，然後新增充當RADIUS客戶端的ASA。

啟用自適應網路控制

導航到**Administration > System > Settings > Adaptive Network Control**以啟用隔離API和功能：



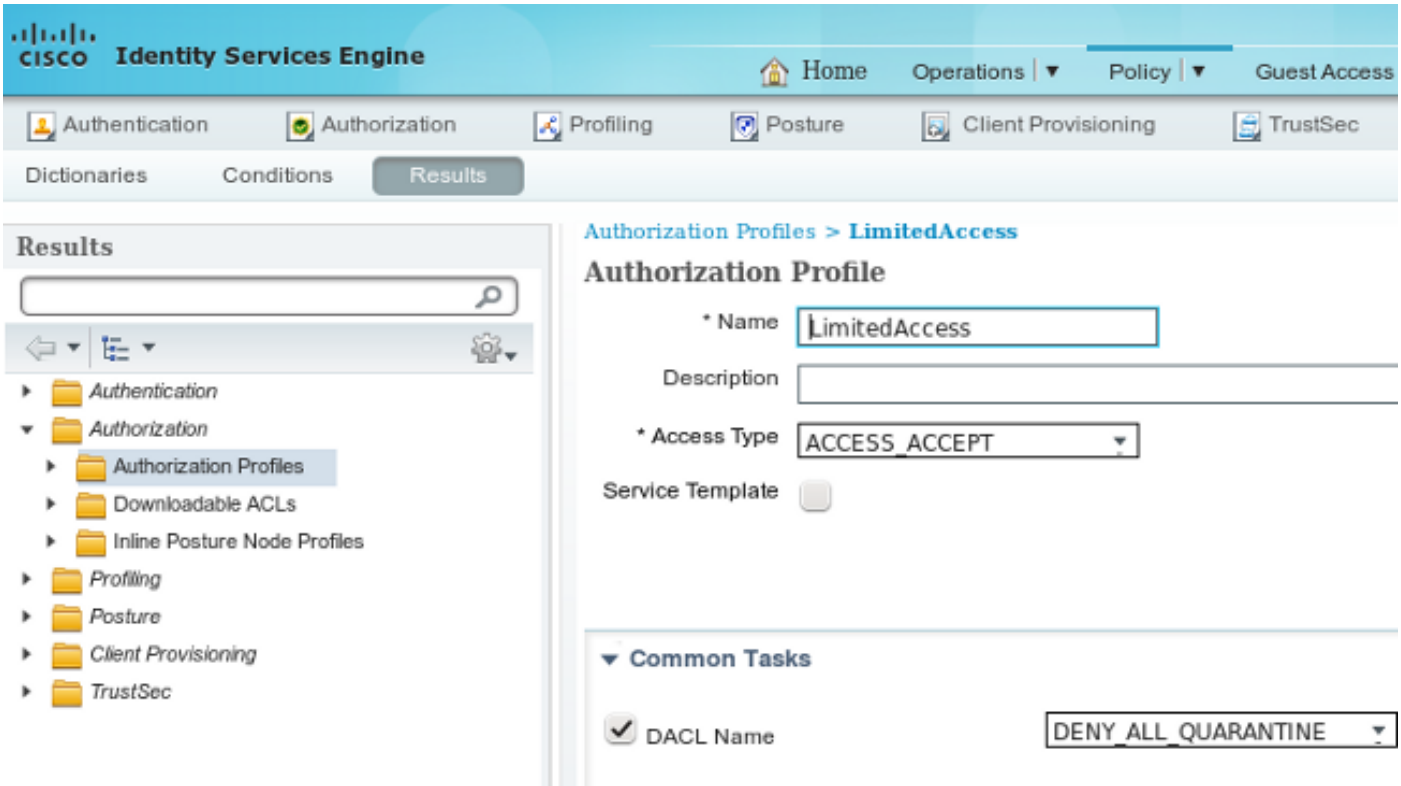
附註：在1.3及更低版本中，此功能稱為*Endpoint Protection Service*。

隔離DACL

要建立用於隔離主機的可下載訪問控制清單(DACL)，請導航至**Policy > Results > Authorization > Downloadable ACL**。

隔離區的授權配置檔案

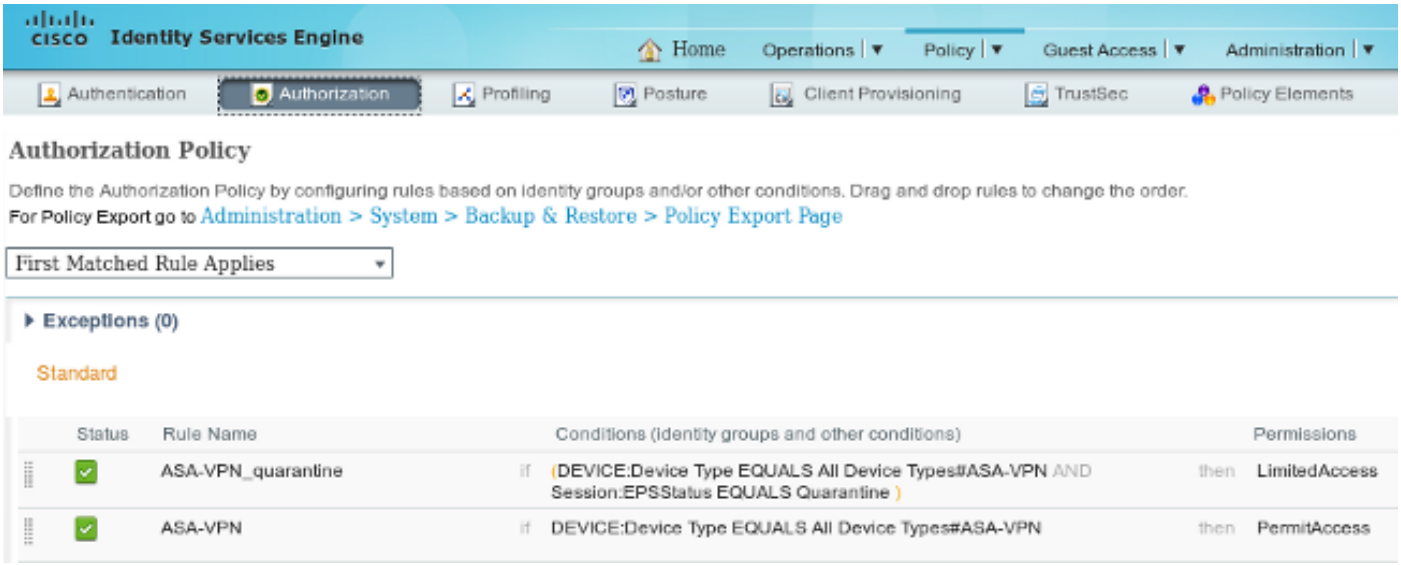
導覽至**Policy > Results > Authorization > Authorization Profile**，然後使用新的DACL建立授權配置檔案：



授權規則

您必須建立兩個授權規則。第一條 規則(ASA-VPN)為在ASA上終止的所有VPN會話提供完全訪問許可權。當主機已處於隔離狀態（提供有限的網路訪問）時，為重新身份驗證的VPN會話點選規則*ASA-VPN_quarantine*。

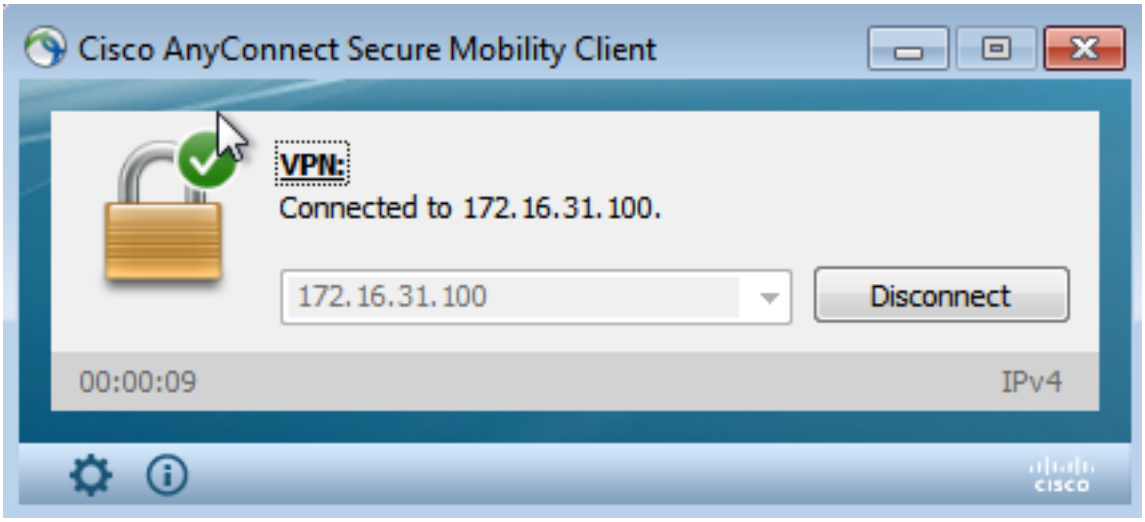
要建立這些規則，請導航到**Policy > Authorization**:



驗證

使用本節提供的資訊以驗證您的組態是否正常運作。

AnyConnect發起ASA VPN會話



ASA建立無任何DACL（完全網路訪問）的會話：

```
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>
```

使用者嘗試訪問

使用者嘗試訪問http://172.16.32.1後，訪問策略被命中，對應的流量被內聯阻止，系統日誌消息從FirePower管理IP地址傳送：

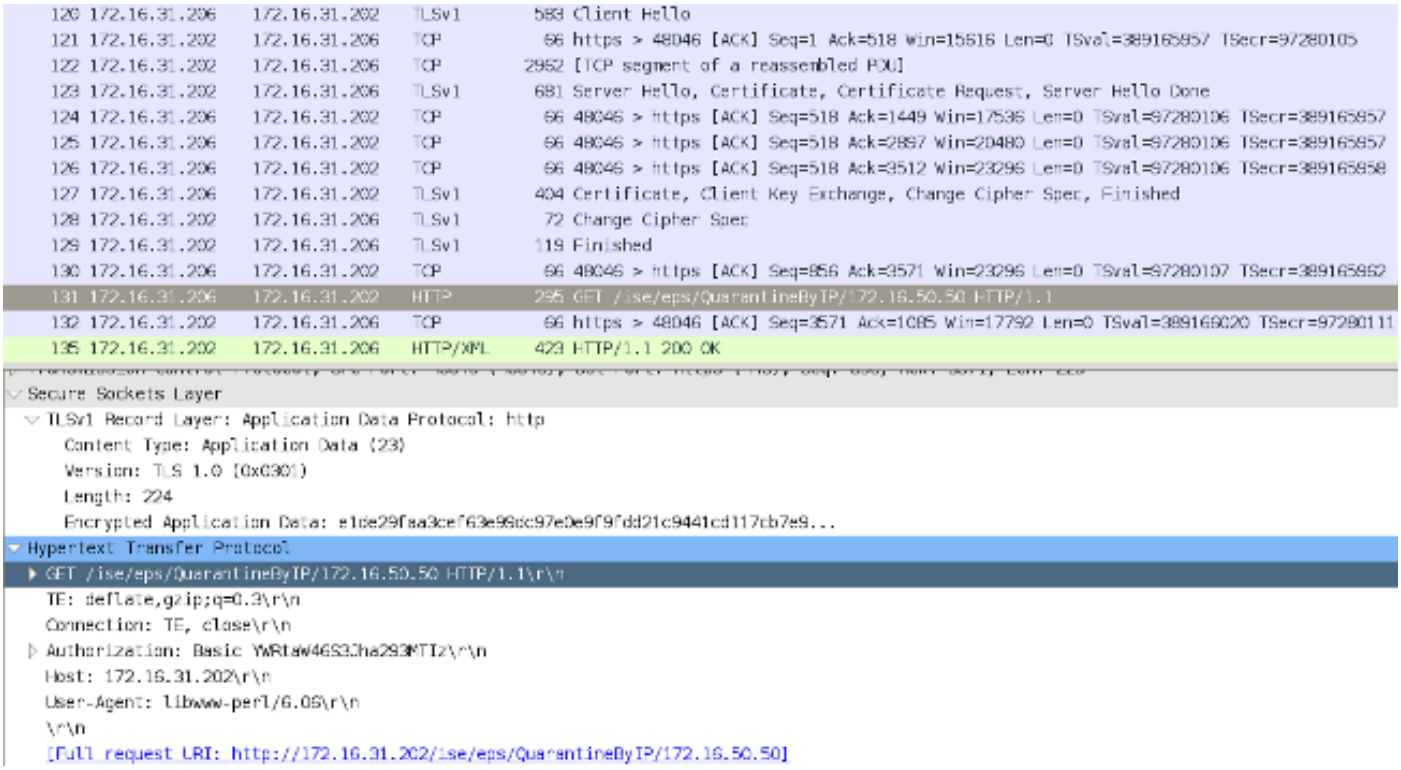
```
May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine
(cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User:
Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown,
 Access Control Rule Name: DropTCP80, Access Control Rule Action: Block,
Access 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:
00000000000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80
```

FireSight關聯策略命中

FireSight管理（防禦中心）關聯策略被命中，該策略由防禦中心傳送的系統日誌消息報告：

```
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)
```

在這個階段，防禦中心使用對ISE的REST API（隔離）呼叫，ISE是一個HTTPS會話，可以在Wireshark中解密(使用安全套接字層(SSL)外掛和PAN管理證書的私鑰):



在GET請求中，攻擊者的IP地址被通過(172.16.50.50)，該主機由ISE隔離。

導覽至**Analysis > Correlation > Status**，以確認成功的修正：

ISE執行隔離並傳送CoA

在此階段，ISE *prrt-management.log*通知應傳送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
```

運行時(prrt-server.log)將CoA *terminate*消息傳送到NAD，NAD將終止會話(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
```

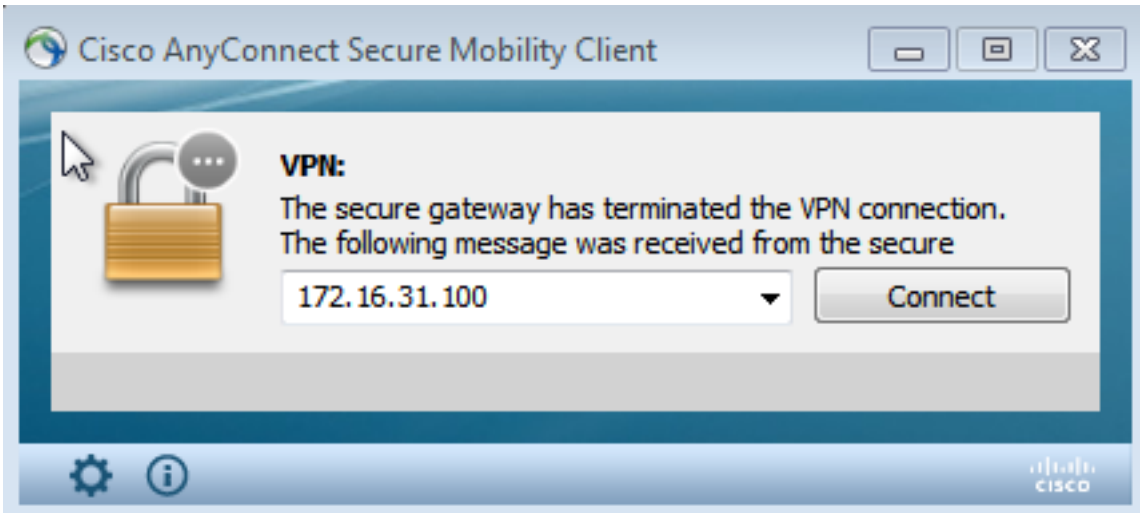
*ise.psc*會傳送類似以下內容的通知：

```
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
```

導航到**Operations > Authentication**時，它應顯示*Dynamic Authorization succeeded*。

VPN會話已斷開

終端使用者傳送通知以指示會話已斷開（對於802.1x/MAB/訪客有線/無線，此過程是透明的）：

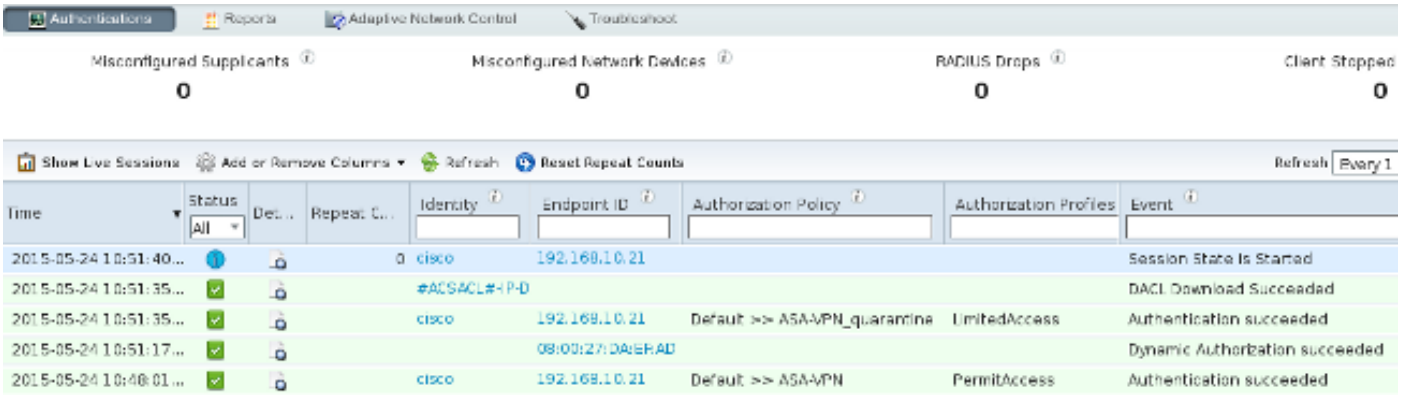


Cisco AnyConnect日誌中的詳細資訊顯示：

```
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
```

有限訪問的VPN會話（隔離）

由於*always-on VPN*已配置，因此會立即構建新會話。這一次，ISE *ASA-VPN_quarantine規則*被命中，該規則提供有限的網路訪問：



附註：DACL是在單獨的RADIUS請求中下載。

在ASA上，可以使用**show vpn-sessiondb detail anyconnect** CLI命令驗證具有受限訪問許可權的會話：

```
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 : ac1020640002700055 5c02e8
Security Grp : none

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

FireSight（防禦中心）

ISE補救指令碼位於以下位置：

```
root@Defence:/var/sf/remediations/ISE_1.3.19# ls
_lib_  ise-instance  ise-test.pl  ise.pl  module.template
```

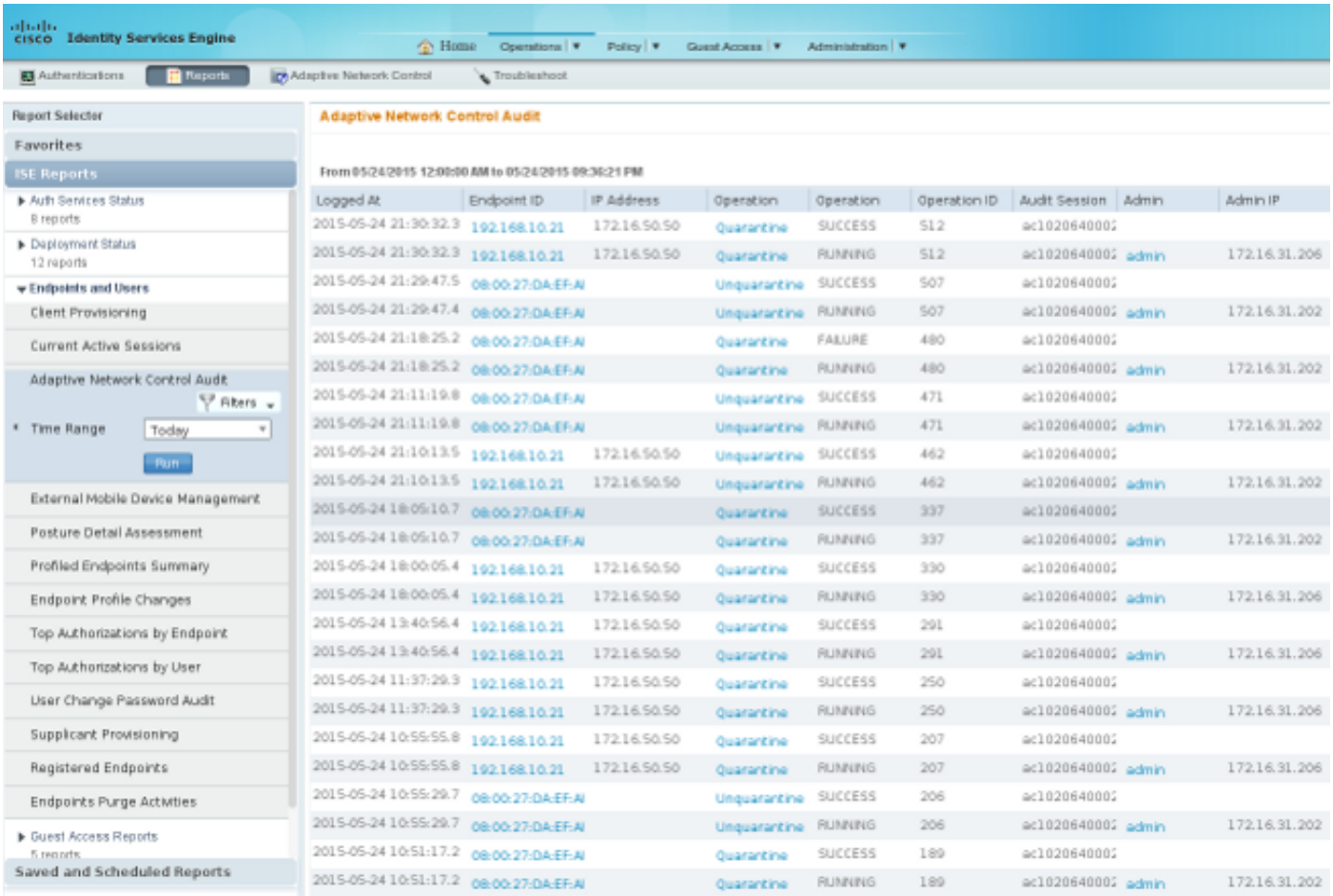
這是一個使用標準SourceFire(SF)日誌記錄子系統的簡單*perl*指令碼。執行補救後，可以通過*/var/log/messages*確認結果：

```
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
```

ISE

在ISE上啟用自適應網路控制服務非常重要。要檢視運行時進程(*prrt-management.log*和*prrt-server.log*)中的詳細日誌，必須為運行時AAA啟用DEBUG級別。導覽至**Administration > System > Logging > Debug Log Configuration**以啟用調試。

您還可以導航到**操作>報告>端點和使用者>自適應網路控制稽核**，以檢視隔離請求每次嘗試和結果的資訊：



錯誤

請參閱Cisco錯誤ID CSCuu41058（ISE 1.4終端隔離不一致和VPN故障）以瞭解與VPN會話故障（802.1x/MAB工作正常）相關的ISE錯誤資訊。

相關資訊

-
- ISE 1.3版pxGrid與IPS pxLog應用的整合

- 思科身份服務引擎管理員指南，版本1.4 — 設定自適應網路控制
- 思科身份服務引擎API參考指南，版本1.2 — 外部REST風格服務API簡介
- 思科身份服務引擎API參考指南，版本1.2 — 監控REST API簡介
- 思科身份服務引擎管理員指南，版本1.3
- 技術支援與檔案 — Cisco Systems