

使用ISE和FirePower集成配置补救服务

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[FireSight管理中心 \(防御中心 \)](#)

[ISE补救模块](#)

[关联策略](#)

[ASA](#)

[ISE](#)

[配置网络接入设备\(NAD\)](#)

[启用自适应网络控制](#)

[隔离DAACL](#)

[隔离的授权配置文件](#)

[授权规则](#)

[验证](#)

[AnyConnect启动ASA VPN会话](#)

[FireSight关联策略命中](#)

[ISE执行隔离并发送CoA](#)

[VPN会话已断开](#)

[故障排除](#)

[FireSight \(防御中心 \)](#)

[ISE](#)

[错误](#)

[相关信息](#)

简介

本文档介绍如何在Cisco FireSight设备上使用补救模块来检测攻击，并使用思科身份服务引擎 (ISE)作为策略服务器自动补救攻击者。本文档中提供的示例介绍用于补救通过ISE进行身份验证的远程VPN用户的方法，但也可用于802.1x/MAB/WebAuth有线或无线用户。

注意：思科不正式支持本文档中引用的补救模块。它在社区门户上共享，任何人都可以使用。在版本5.4及更高版本中，还有一个基于pxGrid协议的更新补救模块。版本6.0不支持此模块，但计划在未来版本中支持此模块。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科自适应安全设备(ASA)VPN配置
- Cisco AnyConnect安全移动客户端配置
- Cisco FireSight基本配置
- Cisco FirePower基本配置
- 思科ISE配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco ASA 9.3版或更高版本
- 思科ISE软件版本1.3及更高版本
- Cisco AnyConnect安全移动客户端3.0版及更高版本
- 思科FireSight管理中心版本5.4
- 思科FirePower版本5.4(虚拟机(VM))

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

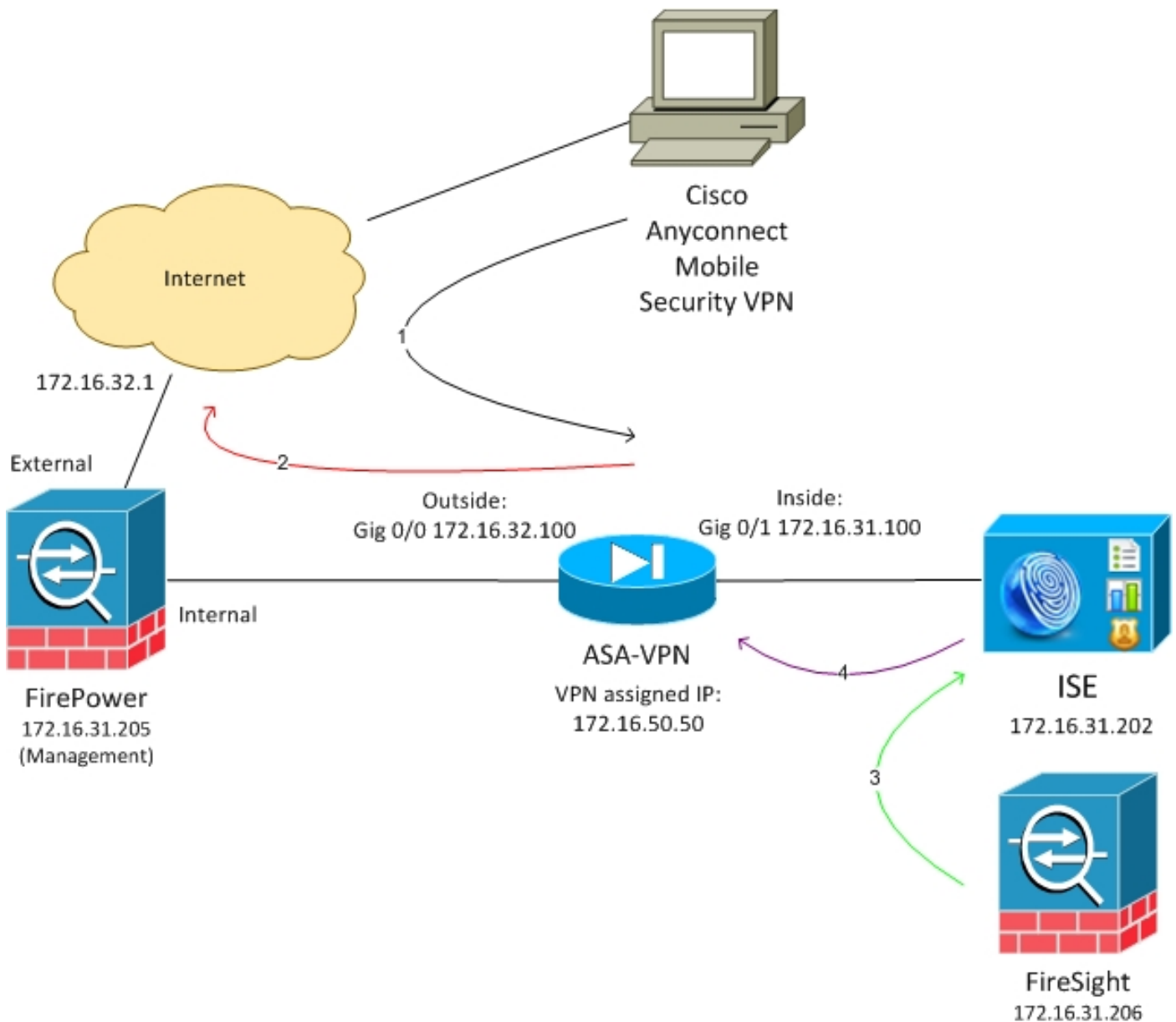
配置

使用本节中提供的信息配置系统。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档中介绍的示例使用此网络设置：



以下是此网络设置的流程：

1. 用户启动与ASA的远程VPN会话（通过Cisco AnyConnect安全移动版本4.0）。
2. 用户尝试访问 `http://172.16.32.1`。（流量通过FirePower移动，该FirePower安装在VM上，由FireSight管理。）
3. FirePower经过配置，可以阻止（内联）特定流量（访问策略），但它也具有触发的关联策略。因此，它通过REST应用程序接口(API)（QuarantineByIP方法）启动ISE补救。
4. 一旦ISE收到REST API调用，它会查找会话并向终止该会话的ASA发送RADIUS授权更改(CoA)。
5. ASA断开VPN用户的连接。由于AnyConnect配置了永远在线的VPN访问，因此会建立新会话；但是，这次会匹配不同的ISE授权规则（针对隔离主机），并提供有限的网络访问。在此阶段，用户如何连接和验证网络并不重要；只要ISE用于身份验证和授权，用户就因隔离而有限的网络访问。

如前所述，此方案适用于任何类型的经过身份验证的会话（VPN、有线802.1x/MAB/Webauth、无线802.1x/MAB/Webauth），只要ISE用于身份验证且网络访问设备支持RADIUS CoA（所有现代思

科设备)。

提示：要将用户移出隔离区，可以使用ISE GUI。未来版本的补救模块也可能支持它。

FirePower

注意：VM设备用于本文档中描述的示例。仅通过CLI执行初始配置。所有策略均从思科防御中心配置。有关详细信息，请参阅[本文档](#)的相关信息部分。

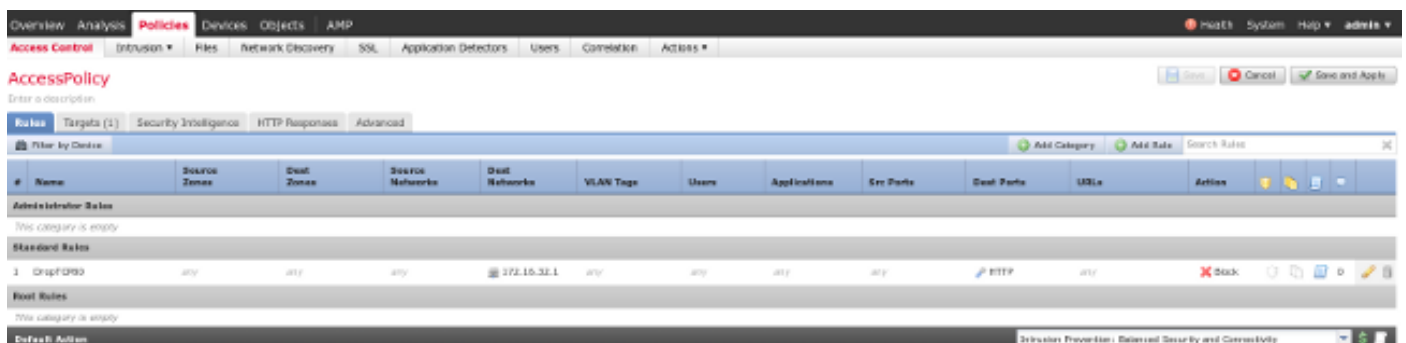
VM有三个接口，一个用于管理，两个用于内联检查（内部/外部）。

来自VPN用户的所有流量都通过FirePower进行传输。

FireSight管理中心（防御中心）

访问控制策略

安装正确的许可证并添加FirePower设备后，导航至**Policies > Access Control**并创建访问策略，以便将HTTP流量丢弃到172.16.32.1:



接受所有其他流量。

ISE补救模块

在社区门户上共享的ISE模块的当前版本是**ISE 1.2 Remediation Beta 1.3.19**:



Sourcefire Downloads

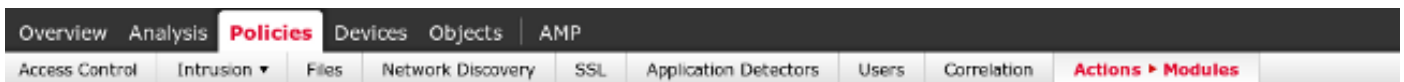
ISE 1.2 Remediation Beta 1.3.19

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.

导航至**策略>操作>补救>模块**并安装文件：



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

然后应创建正确的实例。导航至**Policies > Actions > Remediations > Instances**，并提供策略管理节点(PAN)的IP地址以及REST API所需的ISE管理凭据(建议使用具有ERS管理角色的单独用户)：

Edit Instance

Instance Name	<input type="text" value="ise-instance"/>
Module	ISE 1.2 Remediation (v1.3.19)
Description	<input type="text"/>
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>	<input type="text"/>

源IP地址 (攻击者) 也应用于补救 :

Configured Remediations

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

关联策略

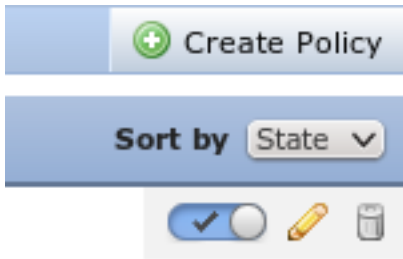
现在必须配置特定关联规则。此规则在连接开始时触发，该连接与先前配置的访问控制规则 (*DropTCP80*)匹配。要配置规则，请导航至**Policies > Correlation > Rule Management**:

The screenshot shows the 'Rule Management' configuration page for a rule named 'CorrelateTCP80Block'. The 'Rule Information' section includes fields for 'Rule Name' (CorrelateTCP80Block), 'Rule Description', and 'Rule Group' (Ungrouped). The 'Select the type of event for this rule' section is configured with 'If a connection event occurs at the beginning of the connection and it meets the following conditions:'. A single 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 none defined.

此规则用于关联策略。导航至**Policies > Correlation > Policy Management**以创建新策略，然后添加已配置的规则。单击右侧的**Remediate**并添加两个操作：**源IP(之前配置)**和**系统日志的补救**：

The screenshot shows the 'Policy Management' configuration page for a correlation policy named 'CorrelateTCP80Block'. The 'Policy Rules' section is expanded to show the rule 'CorrelateTCP80Block'. A modal window titled 'Responses for CorrelateTCP80Block' is open, displaying 'Assigned Responses' and 'Unassigned Responses' lists. The 'Assigned Responses' list contains 'SourceIP Remediation' and 'Syslog Remediation'. The 'Unassigned Responses' list is currently empty.

确保启用关联策略：



ASA

配置充当VPN网关的ASA以使用ISE进行身份验证。还必须启用记帐和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
```

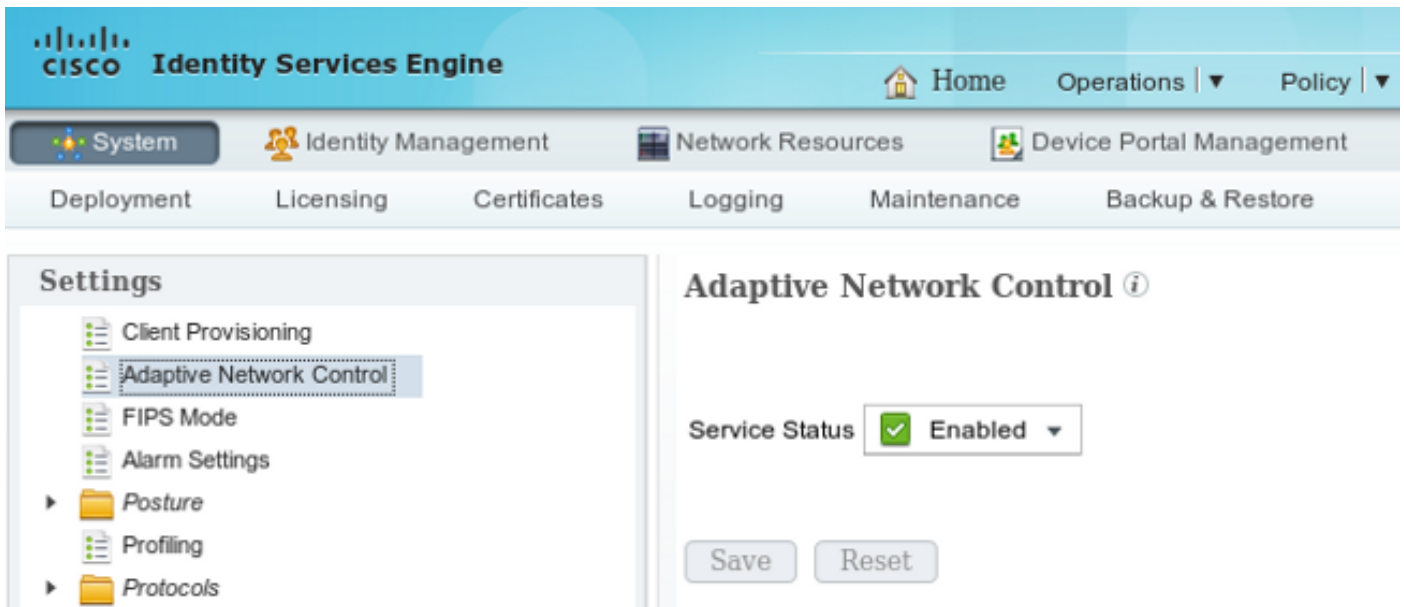
ISE

配置网络接入设备(NAD)

导航至Administration > Network Devices并添加充当RADIUS客户端的ASA。

启用自适应网络控制

导航到管理>System >设置>自适应网络控制以启用隔离API和功能：



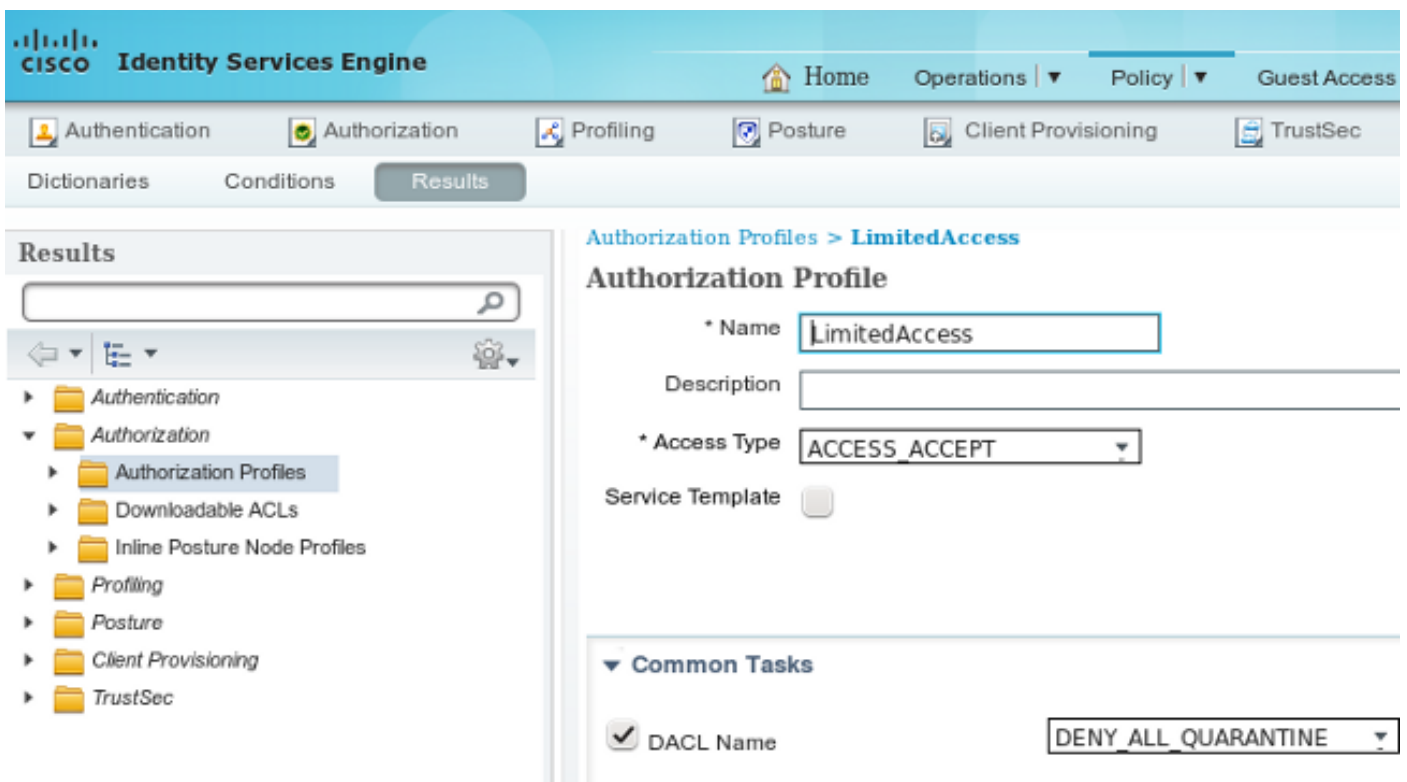
注意：在版本1.3及更低版本中，此功能称为终端保护服务。

隔离DAACL

要创建用于隔离主机的可下载访问控制列表(DACL)，请导航至Policy > Results > Authorization > Downloadable ACL。

隔离的授权配置文件

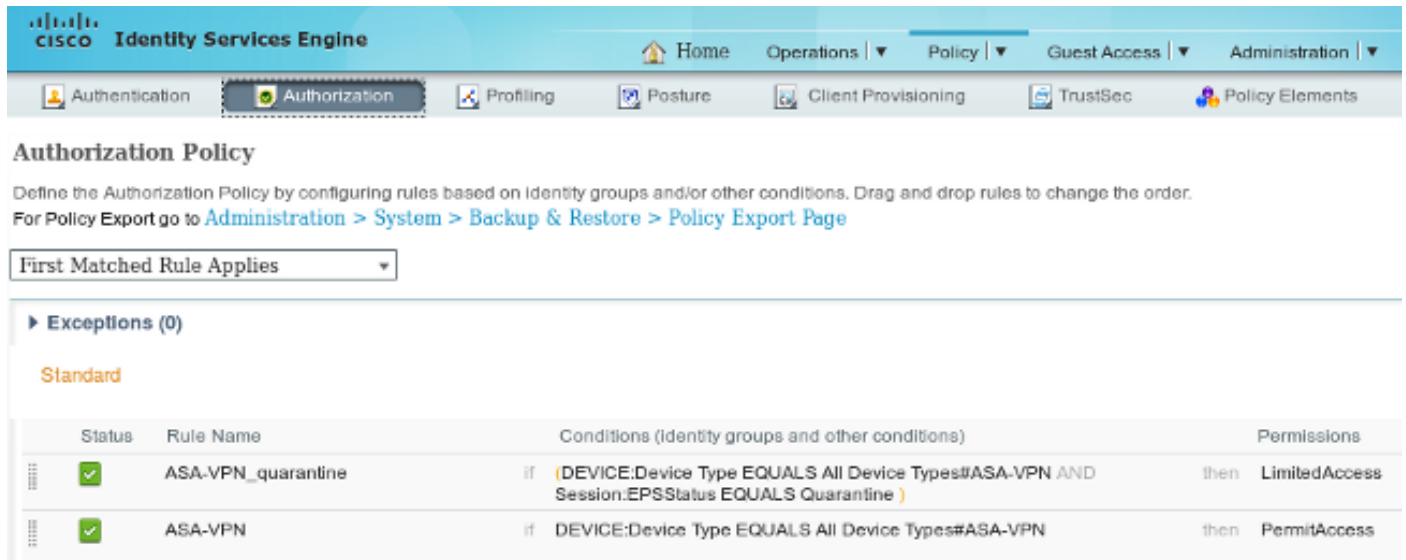
导航至Policy > Results > Authorization > Authorization Profile，然后使用新的DAACL创建授权配置文件：



授权规则

您必须创建两个授权规则。第一条规则(ASA-VPN)为在ASA上终止的所有VPN会话提供完全访问。当主机已在隔离区中时(提供有限的网络访问)，将为重新验证的VPN会话命中规则ASA-VPN_quarantine。

要创建这些规则，请导航至Policy > Authorization:



Authorization Policy

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](#)

First Matched Rule Applies

Exceptions (0)

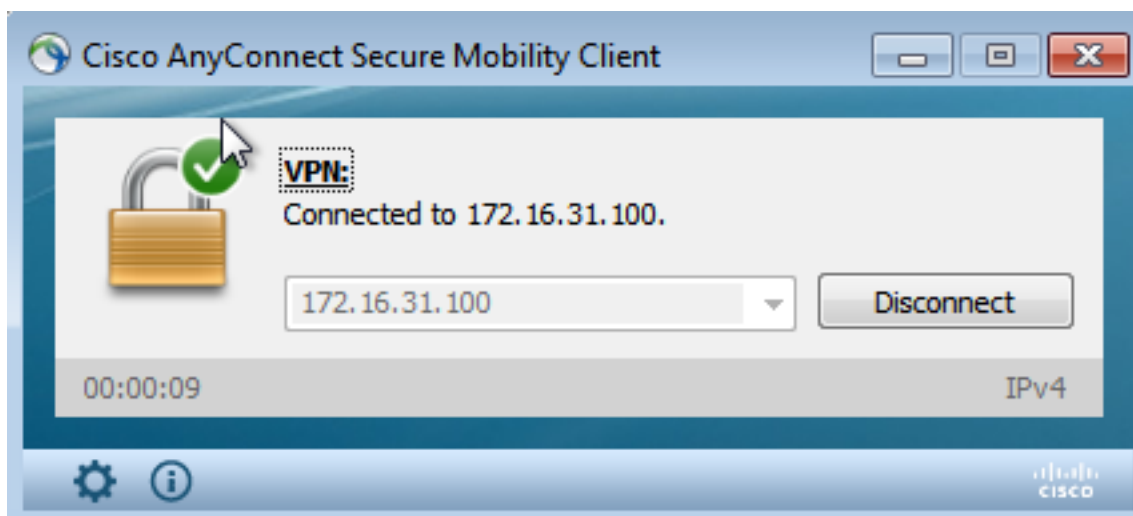
Standard

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

验证

使用本节中提供的信息验证配置是否正常工作。

AnyConnect启动ASA VPN会话



ASA创建会话时不使用任何DACL (完全网络访问) :

```
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>

用户尝试访问

一旦用户尝试访问http://172.16.32.1，访问策略就会命中，对应的流量会内联被阻止，系统日志消息会从FirePower管理IP地址发送：

```

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: 000000000000000000000000000000000000000000000000000000000000000000000000,
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:
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000, SSL Ticket Id:
000000000000000000000000000000000000000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80

```

FireSight关联策略命中

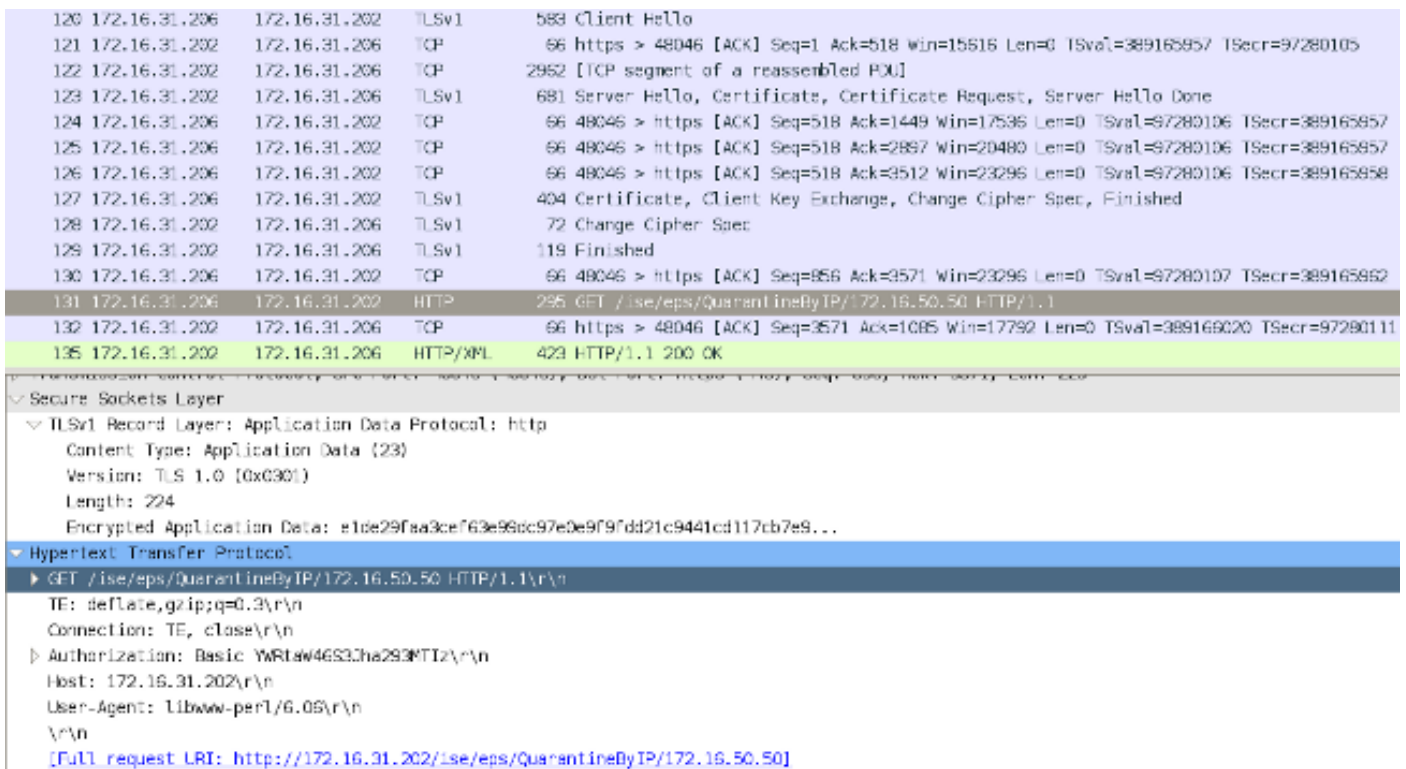
FireSight管理 (防御中心) 关联策略命中，由从防御中心发送的系统日志消息报告：

```

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)

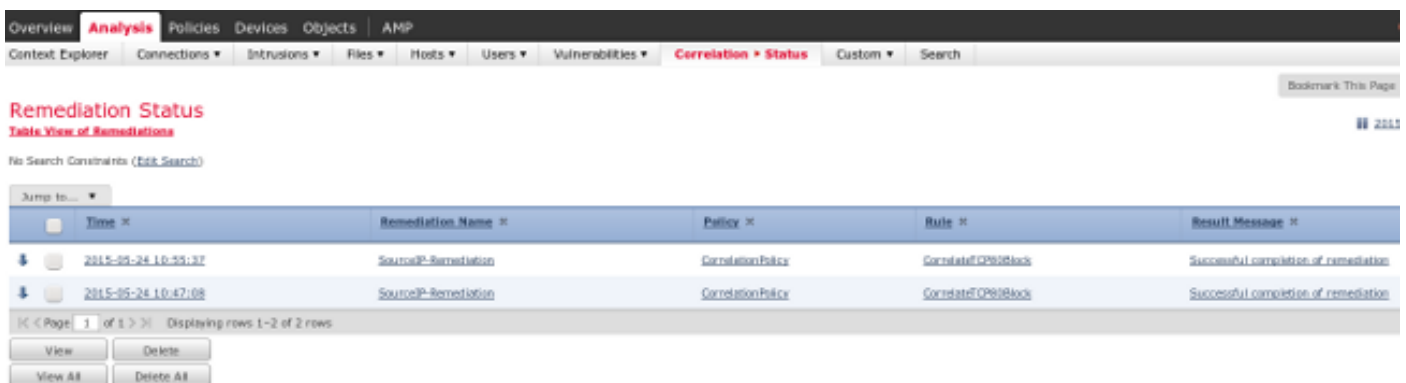
```

在此阶段，防御中心对ISE使用REST API (隔离) 调用，ISE是HTTPS会话，可在Wireshark中解密 (使用安全套接字层(SSL)插件和PAN管理证书的私钥):



在GET请求中，攻击者的IP地址被传递(172.16.50.50)，并且该主机被ISE隔离。

导航至Analysis > Correlation > Status，以确认成功的补救：



ISE执行隔离并发送CoA

在此阶段，ISE *prrt-management.log*通知应发送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
```

运行时(prrt-server.log)将CoA终止消息发送到NAD，NAD终止会话(ASA):

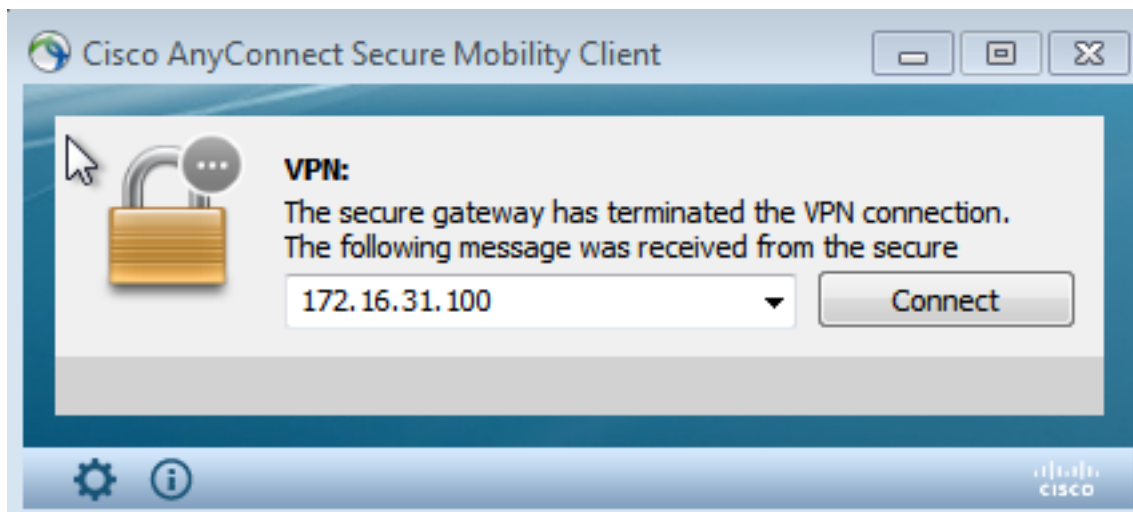
```
DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893,
CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40 (
DisconnectRequest) Identifier=9 Length=124
  [4] NAS-IP-Address - value: [172.16.31.100]
  [31] Calling-Station-ID - value: [08:00:27:DA:EF:AD]
  [49] 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发送类似于以下内容的通知：

```
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 PDPIAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
导航至“操作”>“身份验证”时，应显示“动态授权成功”。
```

VPN会话已断开

最终用户发送通知以指示会话已断开（对于802.1x/MAB/访客有线/无线，此过程是透明的）：



Cisco AnyConnect日志的详细信息显示：

```
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
```

访问受限的VPN会话（隔离）

由于配置了永远在线VPN，因此会立即建立新会话。此时，ISE ASA-VPN_quarantine规则被命中，提供有限的网络访问：

Time	Status	Dev...	Repeats C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-05-24 10:51:40...				cisco	192.168.10.21			Session State Is Started
2015-05-24 10:51:35...				#ACSACL#-IP-D				DACL 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:DAI-E-A-D			Dynamic Authorization succeeded
2015-05-24 10:40:01...				cisco	192.168.10.21	Default => ASA-VPN	PermitAccess	Authentication succeeded

注意：DACL在单独的RADIUS请求中下载。

在ASA上，可以使用show vpn-sessiondb detail anyconnect CLI命令验证访问受限的会话：

```
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
```

故障排除

本节提供可用于排除配置故障的信息。

FireSight (防御中心)

ISE补救脚本驻留在以下位置：

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

这是一个使用标准SourceFire(SF)日志记录子系统的简单Perl脚本。执行补救后，可以通过

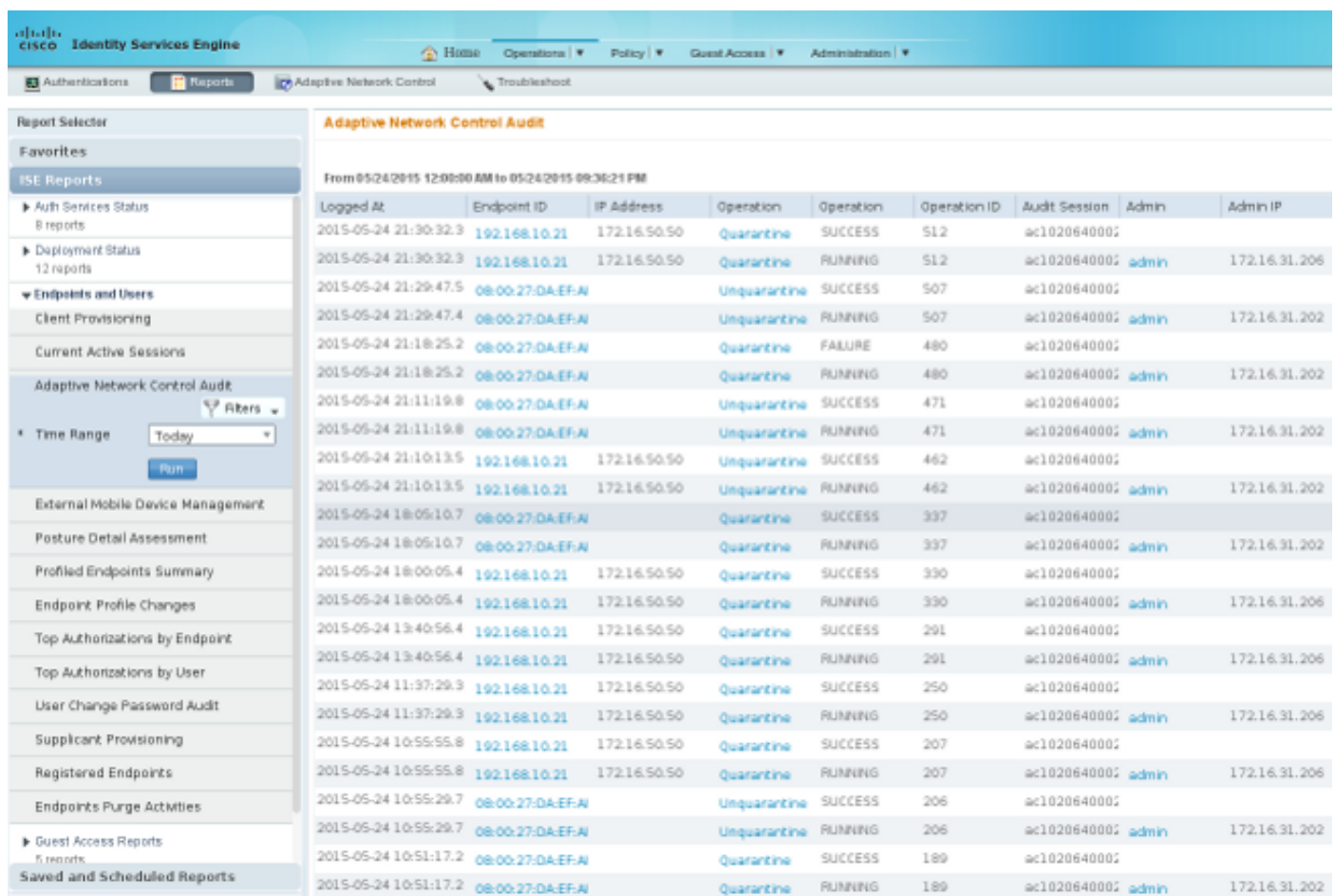
/var/log/messages确认结果:

```
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上启用自适应网络控制服务非常重要。要查看运行时进程(*prrt-management.log*和*prrt-server.log*)中的详细日志，必须为Runtime-AAA启用DEBUG级别。导航至Administration > System > Logging > Debug Log Configuration以启用调试。

您还可以导航至操作>报告>终端和用户>自适应网络控制审核，以查看隔离请求每次尝试和结果的信息：



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

错误

有关与VPN会话故障（802.1x/MAB工作正常）相关的ISE Bug的信息，请参阅Cisco Bug ID [CSCuu41058](#)（ISE 1.4终端隔离不一致和VPN故障）。

相关信息

- [为 TrustSec 感知服务配置 WSA 与 ISE 的集成](#)
- [ISE版本1.3 pxGrid与IPS pxLog应用集成](#)
- [思科身份服务引擎管理员指南，版本1.4 — 设置自适应网络控制](#)
- [思科身份服务引擎API参考指南，版本1.2 — 外部RESTful服务API简介](#)
- [思科身份服务引擎API参考指南，版本1.2 — 监控REST API简介](#)
- [思科身份服务引擎管理员指南，版本1.3](#)
- [技术支持和文档 - Cisco Systems](#)