Configuración de servicios de remediación con ISE e integración de FirePower

Contenido

Introducción

Este documento describe cómo utilizar el módulo de remediación en un dispositivo Cisco FireSight para detectar ataques y remediar automáticamente al atacante con el uso de Cisco Identity Service Engine (ISE) como servidor de políticas. El ejemplo que se proporciona en este documento describe el método que se utiliza para la remediación de un usuario VPN remoto que se autentica a través de ISE, pero que también se puede utilizar para un usuario con cable o inalámbrico 802.1x/MAB/WebAuth.

Nota: Cisco no admite oficialmente el módulo de remediación al que se hace referencia en este documento. Se comparte en un portal comunitario y puede ser utilizado por cualquiera. En las versiones 5.4 y posteriores, también hay disponible un módulo de remediación más nuevo que se basa en el protocolo *pxGrid*. Este módulo no es compatible con la versión 6.0, pero está previsto que sea compatible con versiones futuras.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN de Cisco Adaptive Security Appliance (ASA)
- Configuración de Cisco AnyConnect Secure Mobility Client
- Configuración básica de Cisco FireSight
- Configuración básica de Cisco FirePower
- configuración de Cisco ISE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Cisco ASA versión 9.3 o posterior
- Software Cisco ISE versiones 1.3 y posteriores
- Cisco AnyConnect Secure Mobility Client versiones 3.0 y posteriores
- Cisco FireSight Management Center versión 5.4
- Cisco FirePower versión 5.4 (máquina virtual (VM))

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

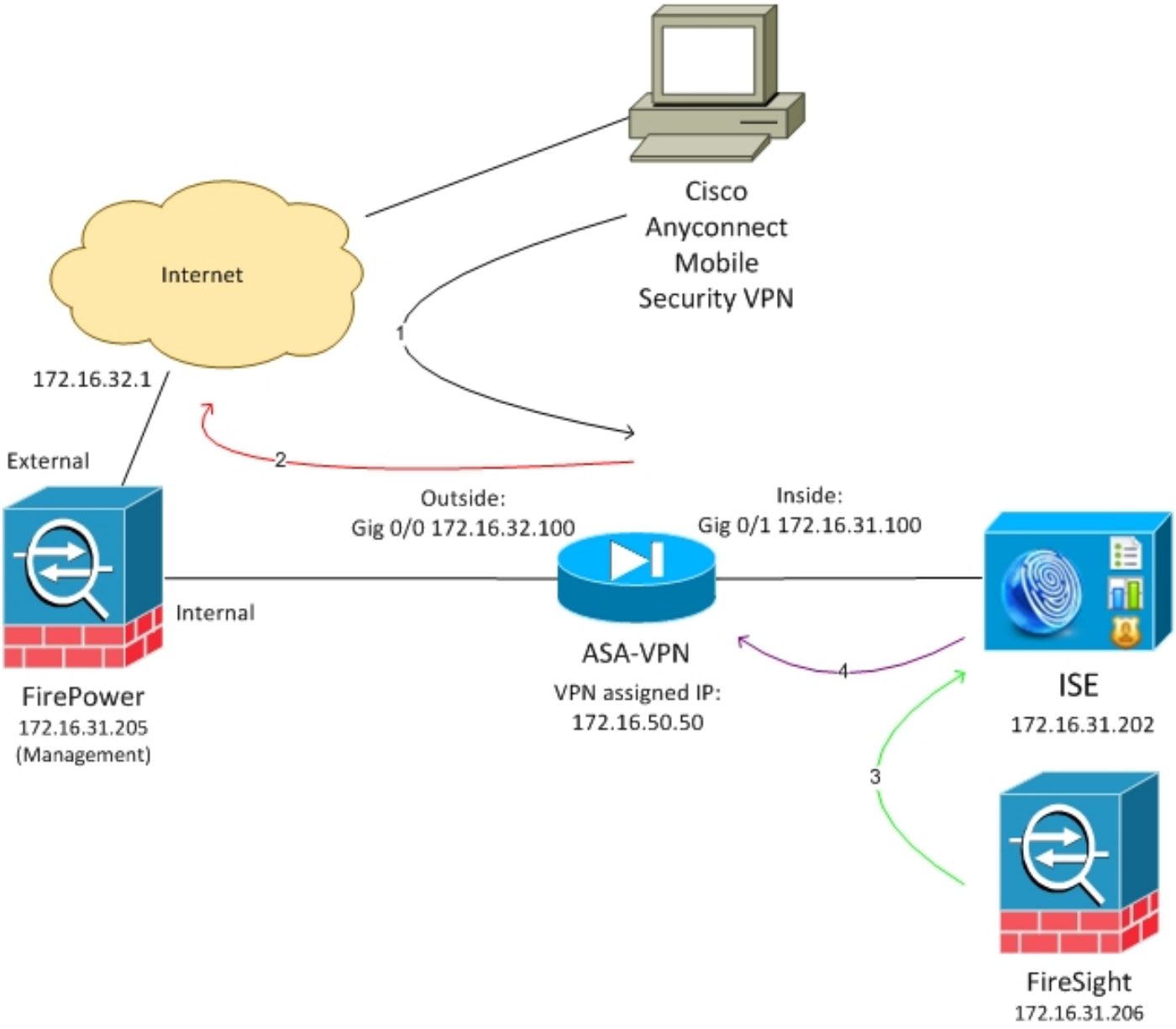
Configurar

Utilice la información proporcionada en esta sección para configurar el sistema.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

El ejemplo que se describe en este documento utiliza esta configuración de red:



Este es el flujo para esta configuración de red:

1. El usuario inicia una sesión VPN remota con el ASA (a través de Cisco AnyConnect Secure Mobility versión 4.0).

2. El usuario intenta acceder a *http://172.16.32.1*. (El tráfico se mueve a través de FirePower, que se instala en la máquina virtual y se gestiona mediante FireSight).

3. FirePower se configura de modo que bloquee (en línea) ese tráfico específico (políticas de acceso), pero también tiene una política de correlación que se activa. Como resultado, inicia

la remediación de ISE a través de la interfaz de programación de aplicaciones (API) REST (el método *QuarantineByIP*).

4. Una vez que el ISE recibe la llamada de la API REST, busca la sesión y envía un cambio de autorización de RADIUS (CoA) al ASA, que finaliza esa sesión.

5. El ASA desconecta al usuario de VPN. Dado que AnyConnect está configurado con acceso VPN *siempre activo*, se establece una nueva sesión; sin embargo, esta vez se establece una regla de autorización de ISE diferente (para hosts en cuarentena) y se proporciona acceso limitado a la red. En esta etapa, no importa cómo el usuario se conecte y autentique a la red; siempre y cuando el ISE se utilice para la autenticación y autorización, el usuario tiene acceso limitado a la red debido a la cuarentena.

Como se mencionó anteriormente, este escenario funciona para cualquier tipo de sesión autenticada (VPN, 802.1x/MAB/Webauth con cables, 802.1x/MAB/Webauth inalámbrico) siempre y cuando el ISE se utilice para la autenticación y el dispositivo de acceso a la red admita la RADIUS CoA (todos los dispositivos Cisco modernos).

> **Consejo:** Para sacar al usuario de la cuarentena, puede utilizar la GUI de ISE. Las versiones futuras del módulo de remediación también podrían ser compatibles con él.

FirePower

> **Nota:** Se utiliza un dispositivo VM para el ejemplo que se describe en este documento. Sólo la configuración inicial se realiza a través de la CLI. Todas las políticas se configuran desde Cisco Defense Center. Para obtener más detalles, consulte la sección Información Relacionada de este documento.

La VM tiene tres interfaces, una para la gestión y dos para la inspección en línea (interna/externa).

Todo el tráfico de los usuarios de VPN se mueve a través de FirePower.

FireSight Management Center (Defense Center)

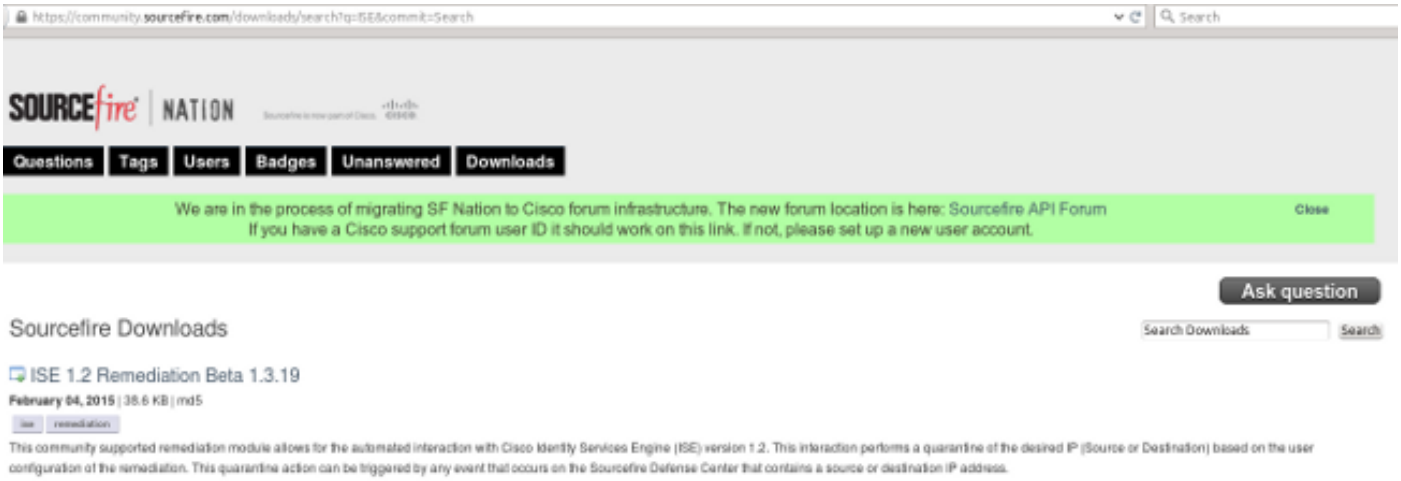
Política de control de acceso

Después de instalar las licencias correctas y agregar el dispositivo FirePower, navegue hasta **Políticas > Control de acceso** y cree la política de acceso que se utiliza para descartar el tráfico HTTP a 172.16.32.1:

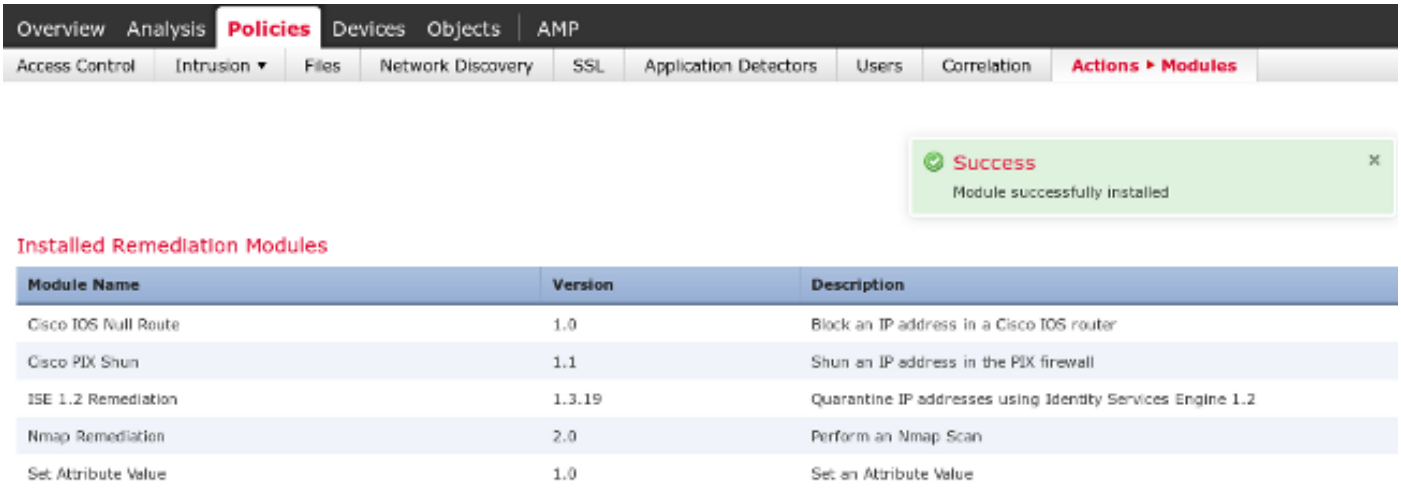
Se acepta el resto del tráfico.

Módulo de solución de ISE

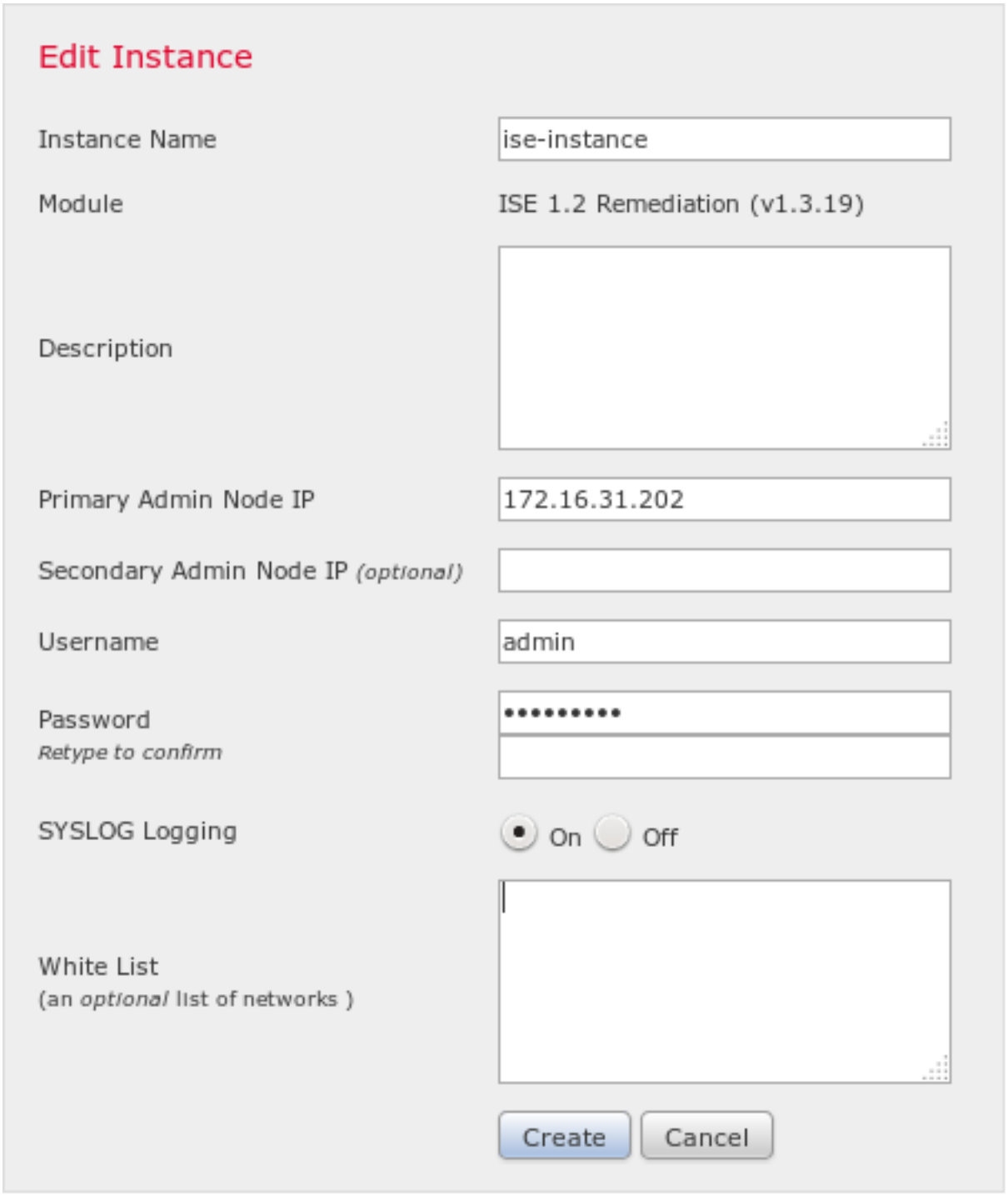
La versión actual del módulo ISE que se comparte en el portal de la comunidad es *ISE 1.2 Remediación Beta 1.3.19*:



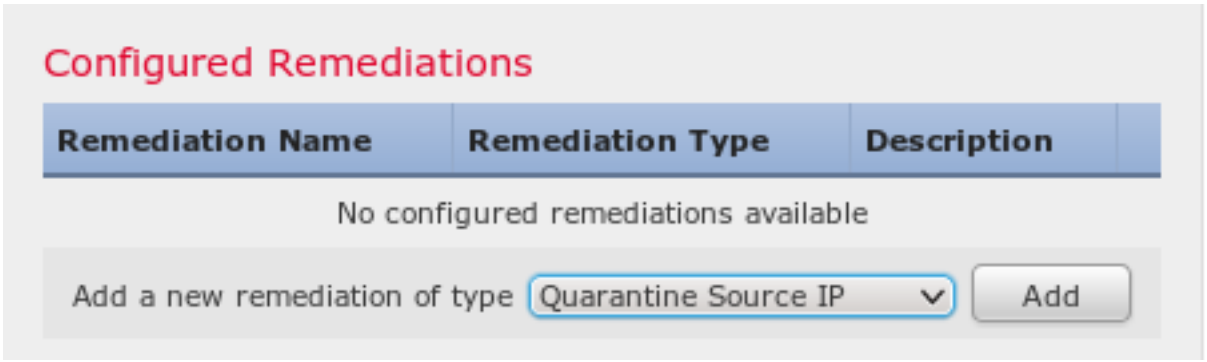
Navegue hasta **Políticas > Acciones > Remediaciones > Módulos** e instale el archivo:



Se debe crear la instancia correcta. Navegue hasta **Políticas > Acciones > Remediaciones > Instancias** y proporcione la dirección IP del nodo de administración de políticas (PAN), junto con las credenciales administrativas de ISE que se necesitan para la API REST (se recomienda un usuario independiente con el rol *Administrador de ERS*):

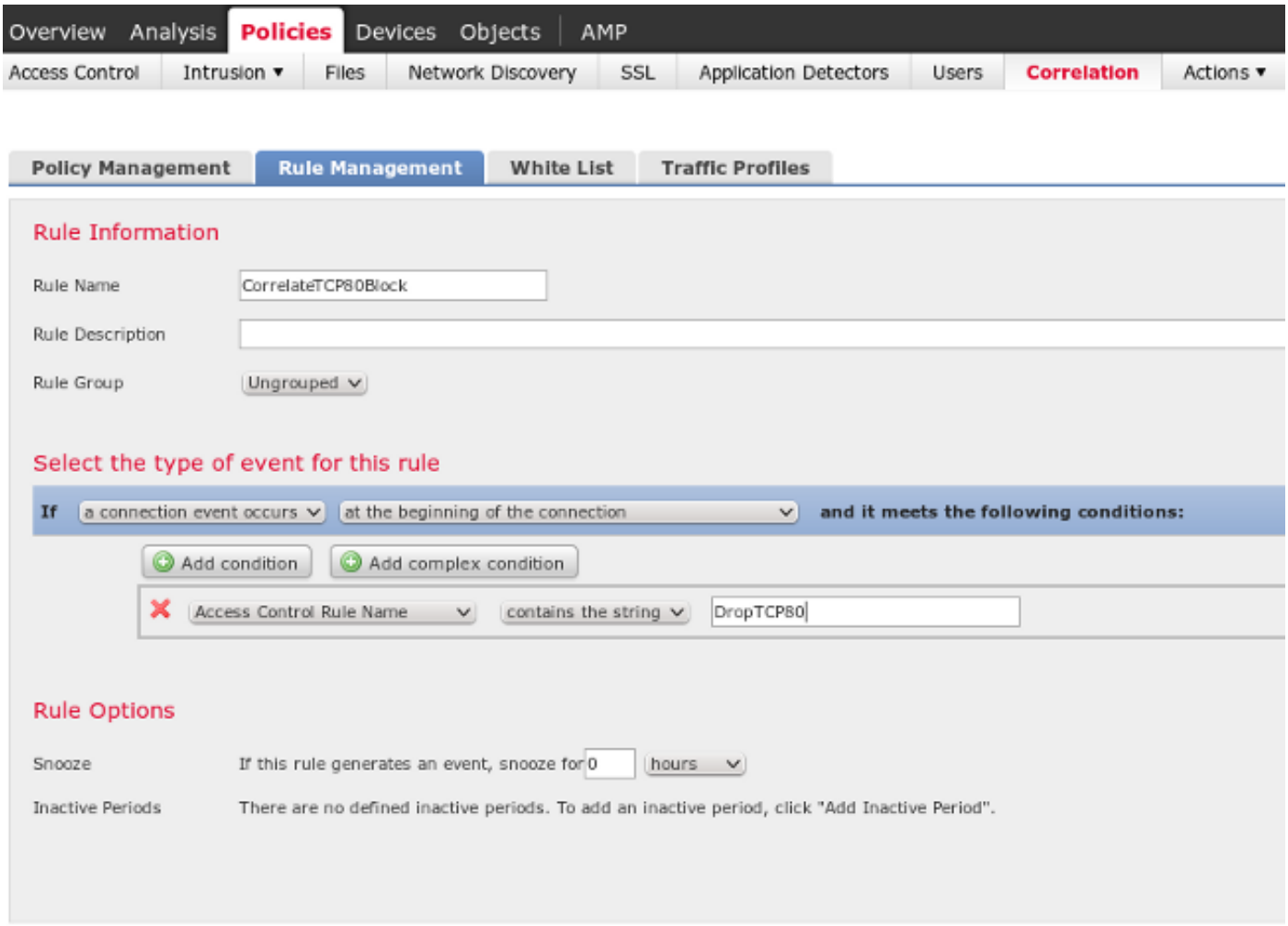


La dirección IP de origen (atacante) también debe utilizarse para la remediación:

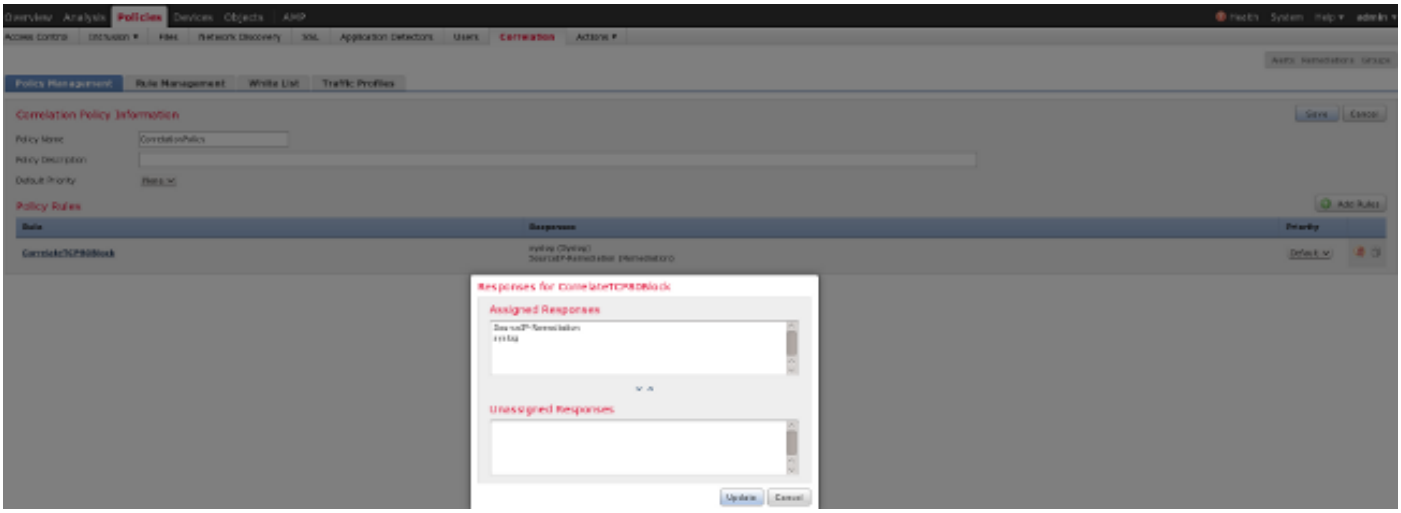


Política de correlación

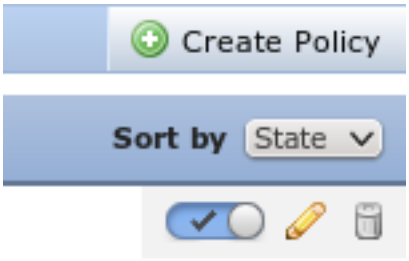
Ahora debe configurar una regla de correlación específica. Esta regla se activa al inicio de la conexión que coincide con la regla de control de acceso previamente configurada (*DropTCP80*). Para configurar la regla, navegue hasta **Políticas > Correlación > Administración de reglas**:



Esta regla se utiliza en la política de correlación. Navegue hasta **Políticas > Correlación > Administración de políticas** para crear una nueva política y luego agregue la regla configurada. Haga clic en **Remediar** a la derecha y agregue dos acciones: **remediación para sourceIP** (configurado anteriormente) y **syslog**:



Asegúrese de activar la política de correlación:



ASA

Se configura un ASA que actúa como gateway VPN para utilizar el ISE para la autenticación. También es necesario habilitar la contabilización y el 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
```

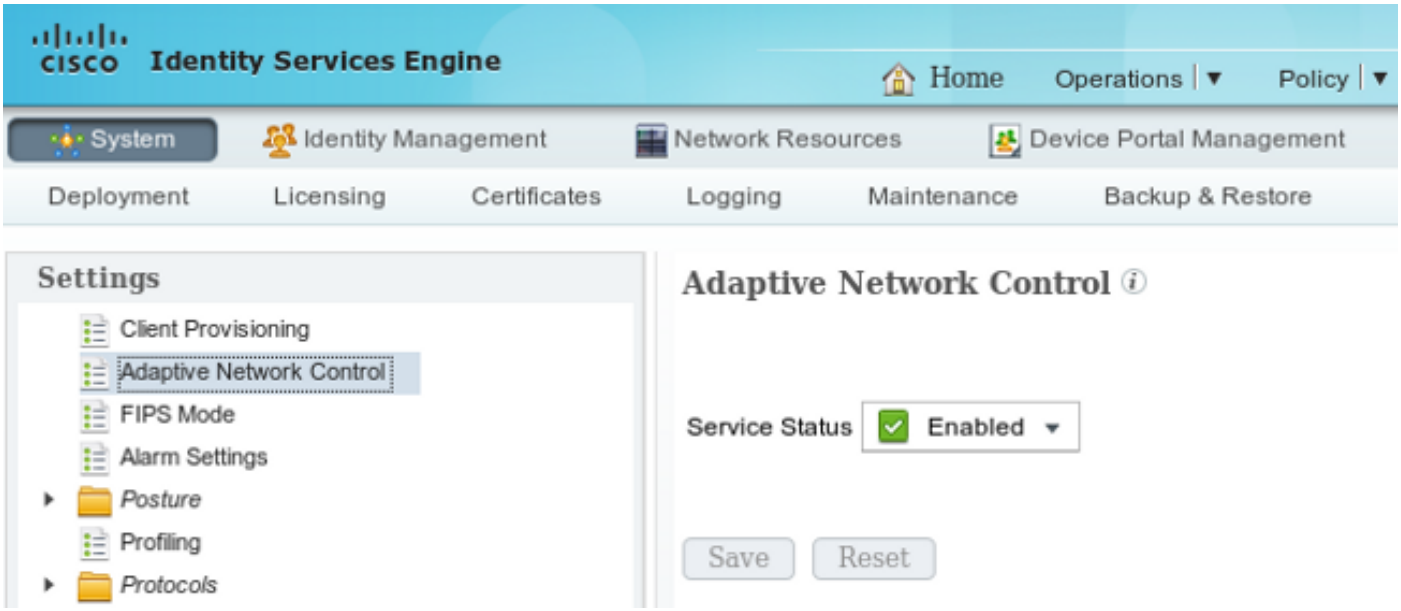
ISE

Configuración del dispositivo de acceso a la red (NAD)

Navegue hasta **Administration > Network Devices** y agregue el ASA que actúa como cliente RADIUS.

Habilitar el control de red adaptable

Navegue hasta **Administration > System > Settings > Adaptive Network Control** para habilitar la API y funcionalidad de cuarentena:



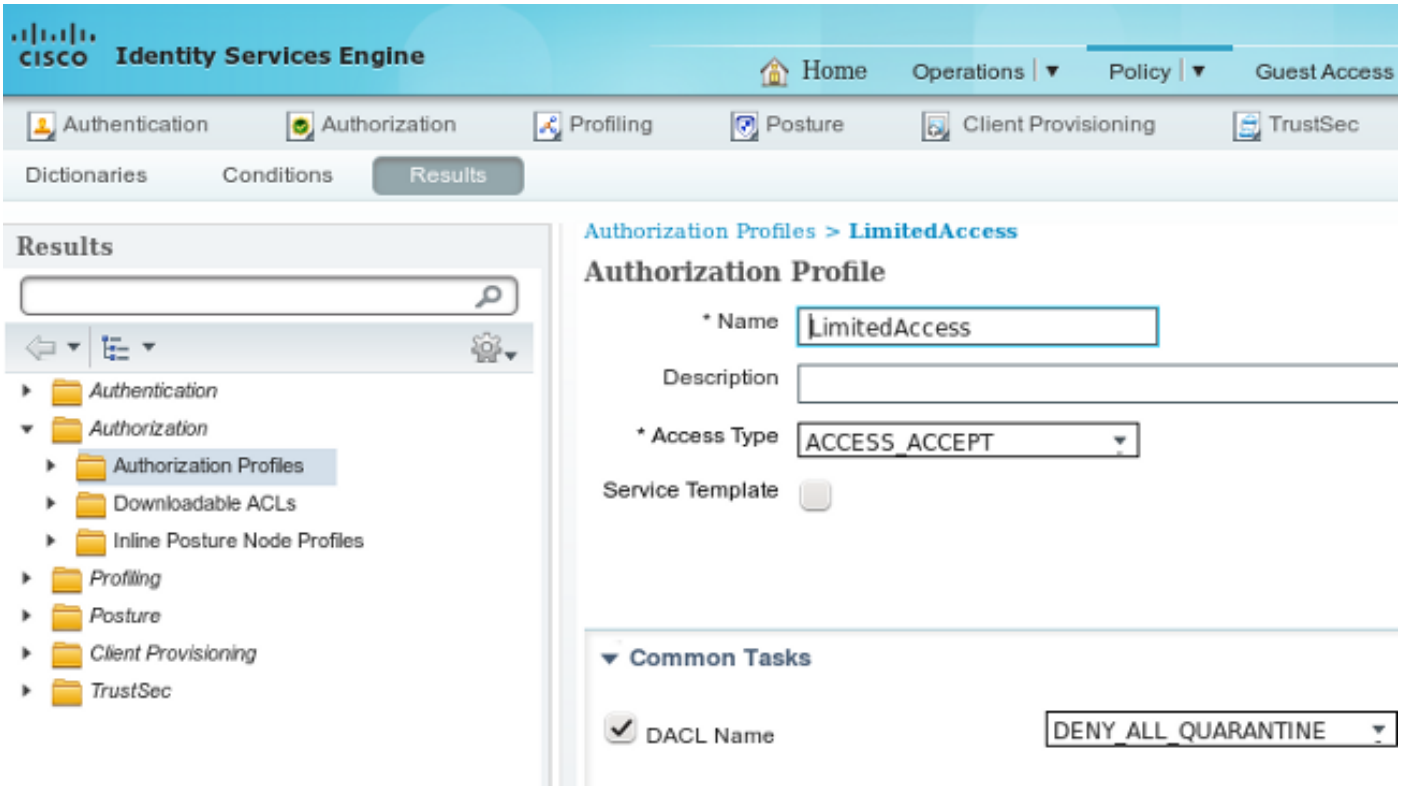
Nota: En las versiones 1.3 y anteriores, esta función se denomina *servicio de protección de terminales*.

DACL de cuarentena

Para crear una Lista de control de acceso (DACL) descargable que se utiliza para los hosts en cuarentena, navegue hasta **Política > Resultados > Autorización > ACL descargable**.

Perfil de autorización para cuarentena

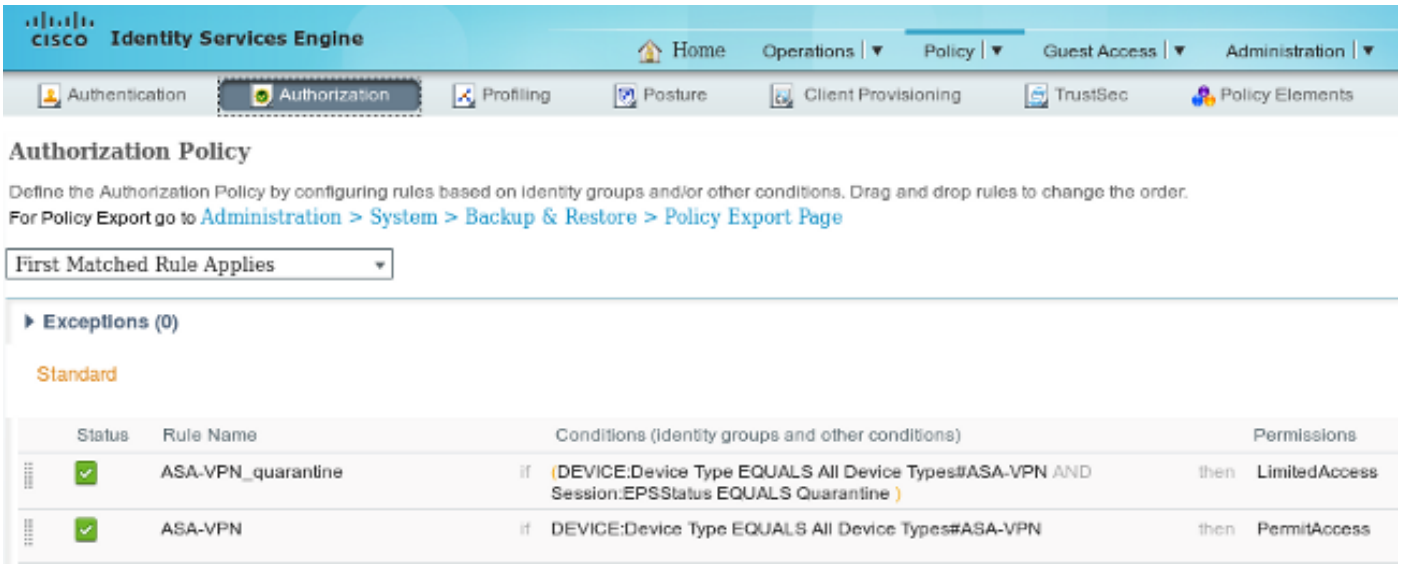
Navegue hasta **Policy > Results > Authorization > Authorization Profile** y cree un perfil de autorización con la nueva DACL:



Reglas de autorización

Debe crear dos reglas de autorización. La primera regla (ASA-VPN) proporciona acceso completo a todas las sesiones VPN que finalizan en el ASA. La regla *ASA-VPN_quarantine* se aplica a la sesión VPN reautenticada cuando el host ya está en cuarentena (se proporciona acceso limitado a la red).

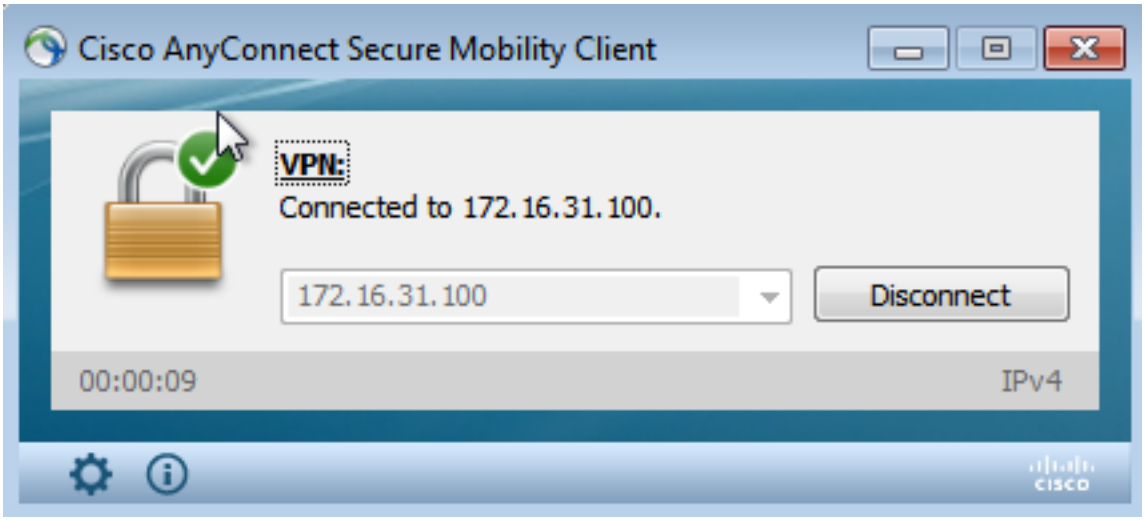
Para crear estas reglas, navegue hasta **Policy > Authorization**:



Verificación

Utilice la información proporcionada en esta sección para verificar que su configuración funcione correctamente.

AnyConnect inicia la sesión VPN de ASA



El ASA crea la sesión sin ningún DACL (acceso completo a la red):

```
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>
```

El usuario intenta acceder

Una vez que el usuario intenta acceder a http://172.16.32.1, la política de acceso se activa, el tráfico correspondiente se bloquea en línea y el mensaje syslog se envía desde la dirección IP de administración de 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,
```

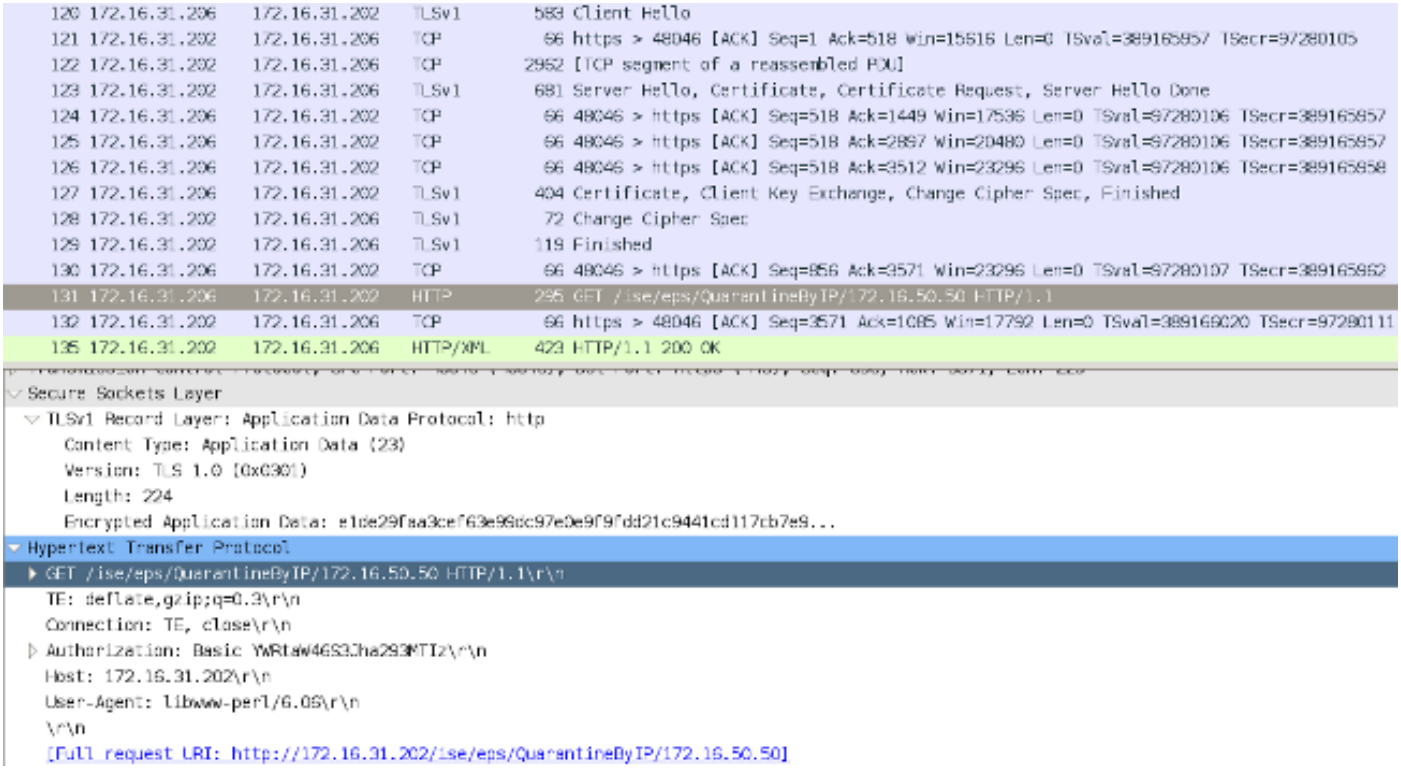
Security Zone Ingress: Internal, Security Zone Egress: External, Security Intelligence Matching IP: None, Security Intelligence Category: None, Client Version: (null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0, NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes: 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: 00000000000000000000000000000000000000, {TCP} **172.16.50.50:49415 -> 172.16.32.1:80**

Golpe en la política de correlación de FireSight

Se activa la política de correlación de administración de FireSight (Centro de defensa), que se informa mediante el mensaje syslog que se envía desde el Centro de defensa:

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)

En esta etapa, Defense Center utiliza la llamada de la API REST (cuarentena) al ISE, que es una sesión HTTPS y se puede descifrar en Wireshark (con el complemento Secure Sockets Layer (SSL) y la clave privada del certificado administrativo PAN):



En la solicitud GET para la dirección IP del atacante se pasa (172.16.50.50) y ese host está en cuarentena por el ISE.

Navegue hasta **Análisis > Correlación > Estado** para confirmar la corrección exitosa:

ISE realiza la cuarentena y envía la CoA

En esta etapa, ISE *prrt-management.log* notifica que se debe enviar la 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
```

El motor en tiempo de ejecución (prrt-server.log) envía el *mensaje* de finalización de CoA al NAD, que finaliza la sesión (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
```

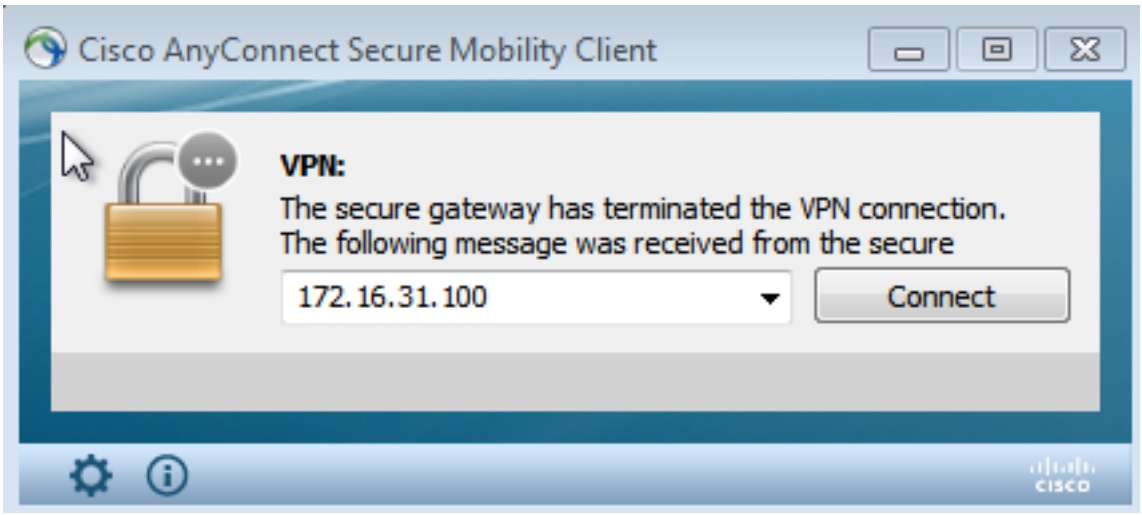
El *ise.psc* envía una notificación similar a esta:

```
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
```

Cuando navega a **Operaciones > Autenticación**, debe mostrar *Autorización Dinámica exitosa*.

La sesión VPN está desconectada

El usuario final envía una notificación para indicar que la sesión está desconectada (para 802.1x/MAB/invitado por cable/inalámbrico, este proceso es transparente):

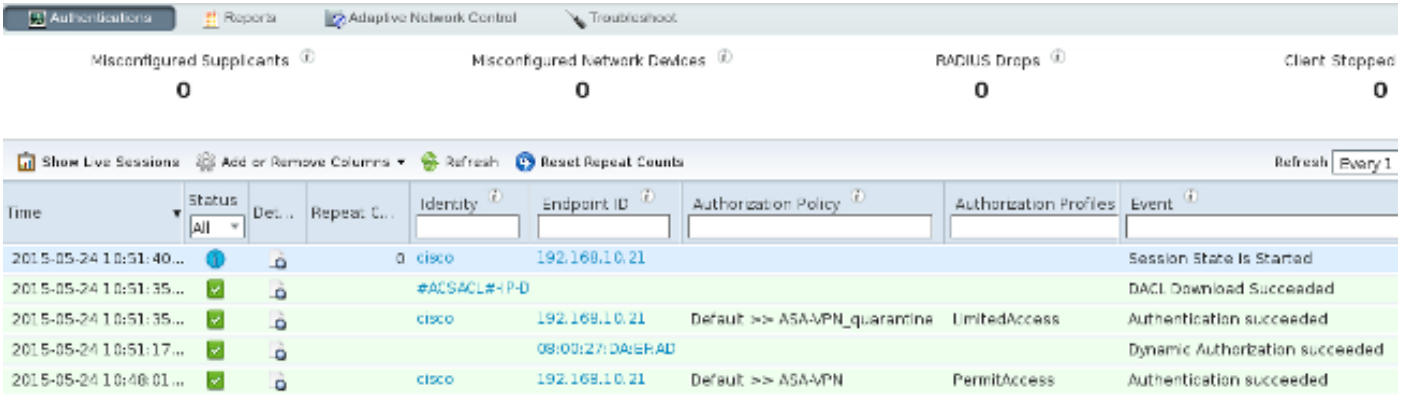


Los detalles de los registros de Cisco AnyConnect muestran:

```
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
```

Sesión VPN con acceso limitado (cuarentena)

Debido a que *siempre activa VPN* está configurada, la nueva sesión se genera inmediatamente. Esta vez, se aplica la regla ISE *ASA-VPN_quarantine*, que proporciona el acceso limitado a la red:



Nota: La DACL se descarga en una solicitud RADIUS independiente.

Una sesión con acceso limitado se puede verificar en el ASA con el comando **show vpn-sessiondb detail anyconnect** CLI:

```
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 ommited for clarity>
  Filter Name  : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

Troubleshoot

Esta sección proporciona información que puede utilizar para resolver problemas de su configuración.

FireSight (centro de defensa)

El script de remediación de ISE reside en esta ubicación:

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

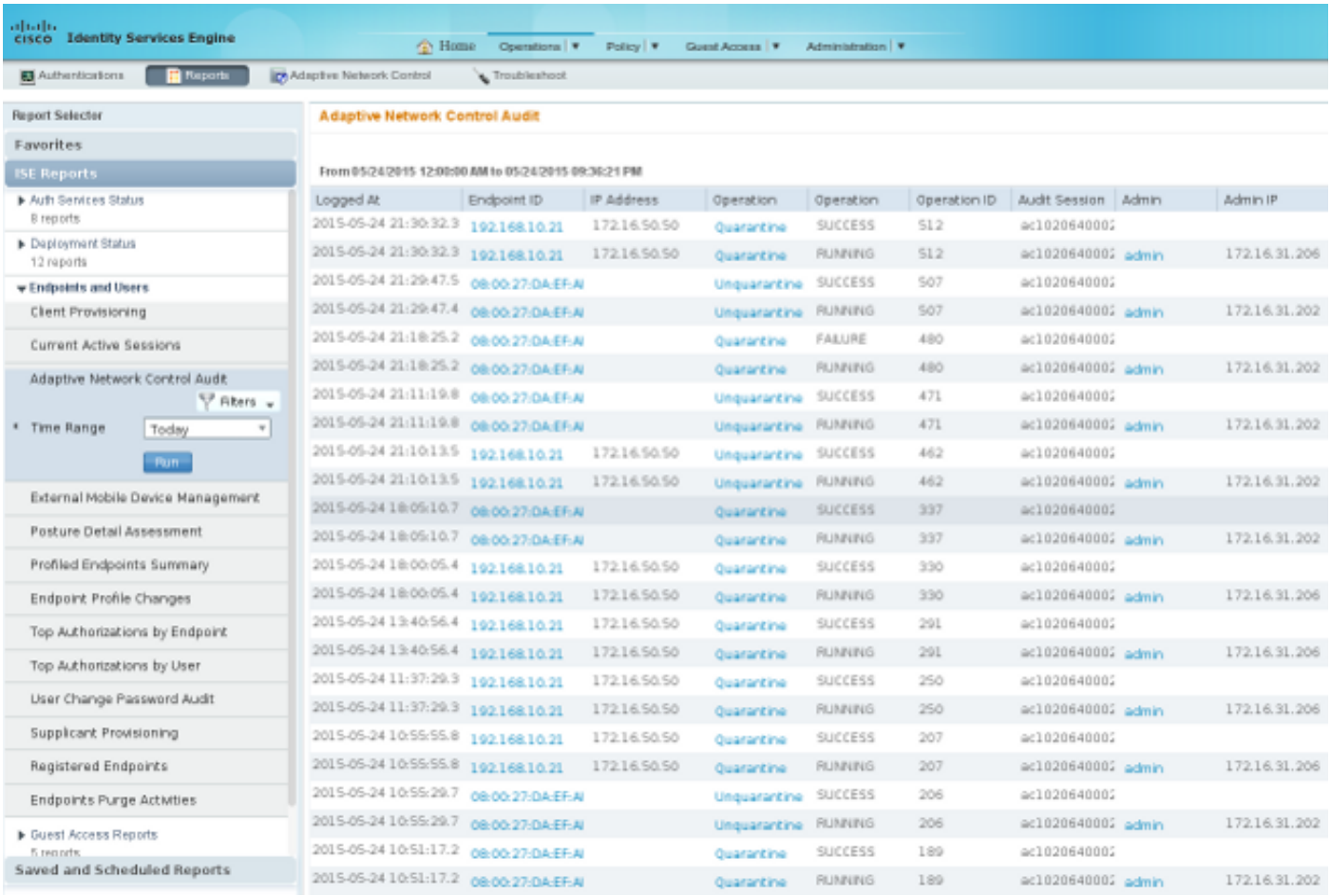
Se trata de un script *perl* simple que utiliza el subsistema de registro estándar SourceFire (SF). Una vez que se ejecuta la remediación, puede confirmar los resultados a través de */var/log/messages*:

```
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
```

ISE

Es importante que habilite el servicio Adaptive Network Control en ISE. Para ver los registros detallados en un proceso en tiempo de ejecución (*prrt-management.log* y *prrt-server.log*), debe habilitar el nivel DEBUG para Runtime-AAA. Navegue hasta **Administración > Sistema > Registro > Configuración de registro de depuración** para habilitar las depuraciones.

También puede navegar a **Operaciones > Informes > Terminal y Usuarios > Auditoría de Control de Red Adaptativa** para ver la información de cada intento y resultado de una solicitud de cuarentena:



Errores

Consulte Cisco bug ID CSCuu41058 (Inconsistencia de ISE 1.4 Endpoint Quarantine y falla de VPN) para obtener información sobre un error de ISE relacionado con fallas de sesión de VPN (802.1x/MAB funciona correctamente).

Información Relacionada

- Configuran la integración de WSA con ISE para TrustSec Aware Services
- ISE versión 1.3 pxGrid Integration con la aplicación IPS pxLog
- Guía del administrador de Cisco Identity Services Engine, versión 1.4 - Configuración del control de red adaptable
- Guía de referencia de la API de Cisco Identity Services Engine, versión 1.2 - Introducción a la API de servicios RESTful externos
- Guía de referencia de la API de Cisco Identity Services Engine, versión 1.2 - Introducción a las API REST de supervisión
- Guía del administrador de Cisco Identity Services Engine, versión 1.3

- Asistencia técnica y documentación - Cisco Systems