Configurar serviços de correção com integração ISE e FirePower

Contents

Introduction

Este documento descreve como usar o módulo de correção em um dispositivo Cisco FireSight para detectar ataques e corrigir automaticamente o invasor com o uso do Cisco Identity Service Engine (ISE) como servidor de políticas. O exemplo fornecido neste documento descreve o método usado para remediar um usuário remoto de VPN que se autentica via ISE, mas também pode ser usado para um usuário 802.1x/MAB/WebAuth com ou sem fio.

Note: O módulo de correção mencionado neste documento não é oficialmente suportado pela Cisco. Ele é compartilhado em um portal da comunidade e pode ser usado por qualquer pessoa. Nas versões 5.4 e posteriores, também há um módulo de correção mais recente disponível, baseado no protocolo *pxGrid*. Este módulo não é suportado na versão 6.0, mas está planejado para ser suportado em versões futuras.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN do Cisco Adaptive Security Appliance (ASA)
- Configuração do Cisco AnyConnect Secure Mobility Client
- Configuração básica do Cisco FireSight
- Configuração básica do Cisco FirePower
- configuração do Cisco ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Cisco ASA versão 9.3 ou posterior
- Software Cisco ISE versões 1.3 e posteriores
- Cisco AnyConnect Secure Mobility Client versões 3.0 e posteriores
- Cisco FireSight Management Center versão 5.4
- Cisco FirePower versão 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.

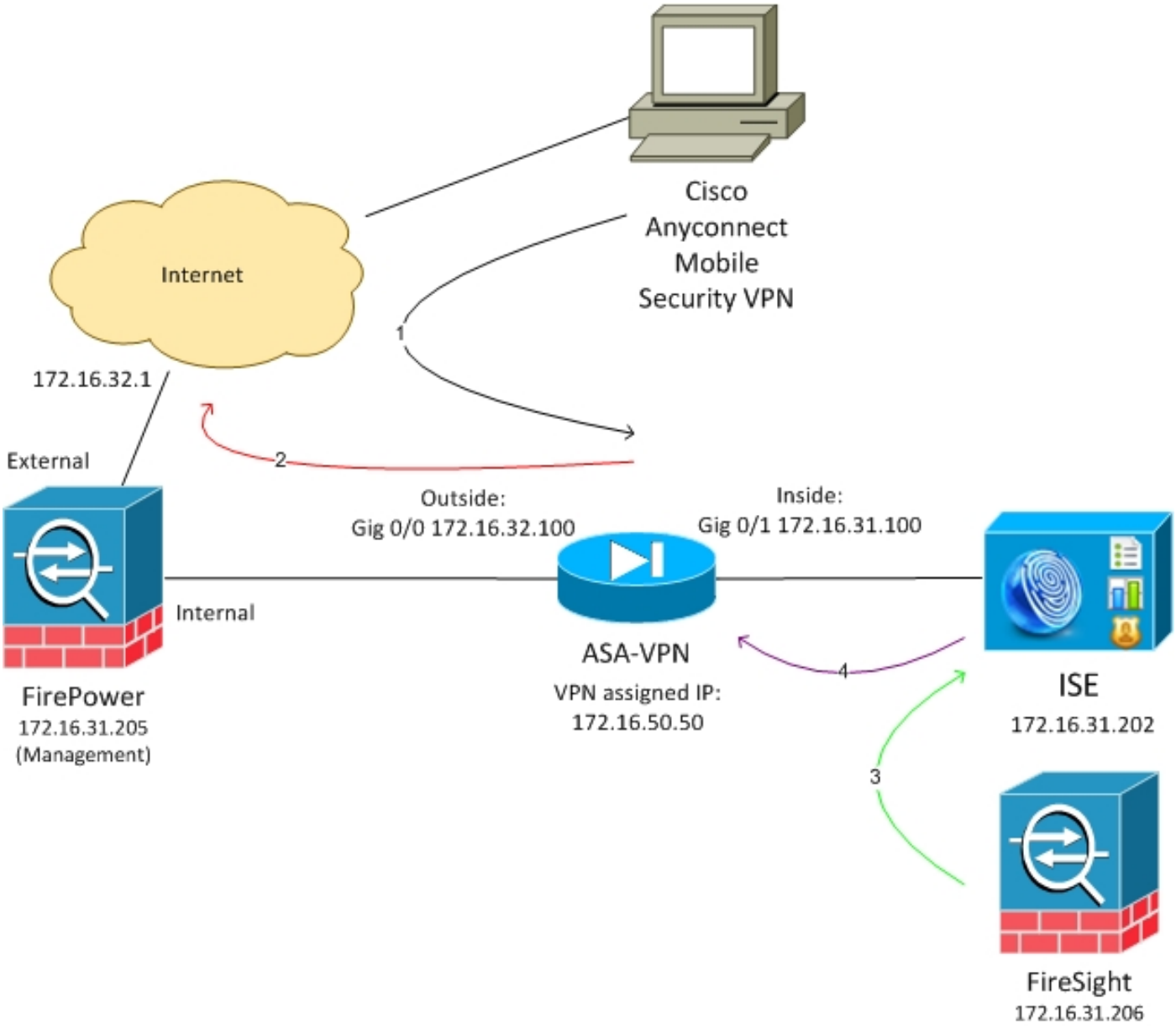
Configurar

Use as informações fornecidas nesta seção para configurar seu sistema.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

O exemplo descrito neste documento usa esta configuração de rede:



Este é o fluxo para esta configuração de rede:

1. O usuário inicia uma sessão VPN remota com o ASA (via Cisco AnyConnect Secure Mobility Versão 4.0).

2. O usuário tenta acessar *http://172.16.32.1*. (O tráfego é movido pelo FirePower, que é instalado na VM e gerenciado pelo FireSight.)

3. O FirePower é configurado para bloquear (em linha) o tráfego específico (políticas de acesso), mas também tem uma Política de correlação que é acionada. Como resultado, ele inicia a correção do ISE por meio da REST Application Programming Interface (API) (o

método *QuarantineByIP*).

4. Quando o ISE recebe a chamada da API REST, ele procura a sessão e envia uma Alteração de Autorização RADIUS (CoA - RADIUS Change of Authorization) para o ASA, que encerra essa sessão.

5. O ASA desconecta o usuário da VPN. Como o AnyConnect está configurado com acesso VPN *sempre conectado*, uma nova sessão é estabelecida; entretanto, desta vez, uma regra de autorização ISE diferente é combinada (para hosts em quarentena) e o acesso limitado à rede é fornecido. Neste estágio, não importa como o usuário se conecta e se autentica à rede; enquanto o ISE for usado para autenticação e autorização, o usuário terá acesso limitado à rede devido à quarentena.

Como mencionado anteriormente, esse cenário funciona para qualquer tipo de sessão autenticada (VPN, 802.1x/MAB/Webauth com fio, 802.1x/MAB/Webauth), desde que o ISE seja usado para autenticação e o dispositivo de acesso à rede ofereça suporte à CoA RADIUS (todos os dispositivos modernos da Cisco).

> **Tip**: Para mover o usuário para fora da quarentena, você pode usar a GUI do ISE. Versões futuras do módulo de correção também podem suportá-lo.

FirePower

> **Note**: Um dispositivo VM é usado para o exemplo descrito neste documento. Somente a configuração inicial é executada via CLI. Todas as políticas são configuradas no Cisco Defense Center. Para obter mais detalhes, consulte a seção Informações Relacionadas deste documento.

A VM tem três interfaces, uma para gerenciamento e duas para inspeção em linha (interna/externa).

Todo o tráfego dos usuários da VPN se move pelo FirePower.

FireSight Management Center (Defense Center)

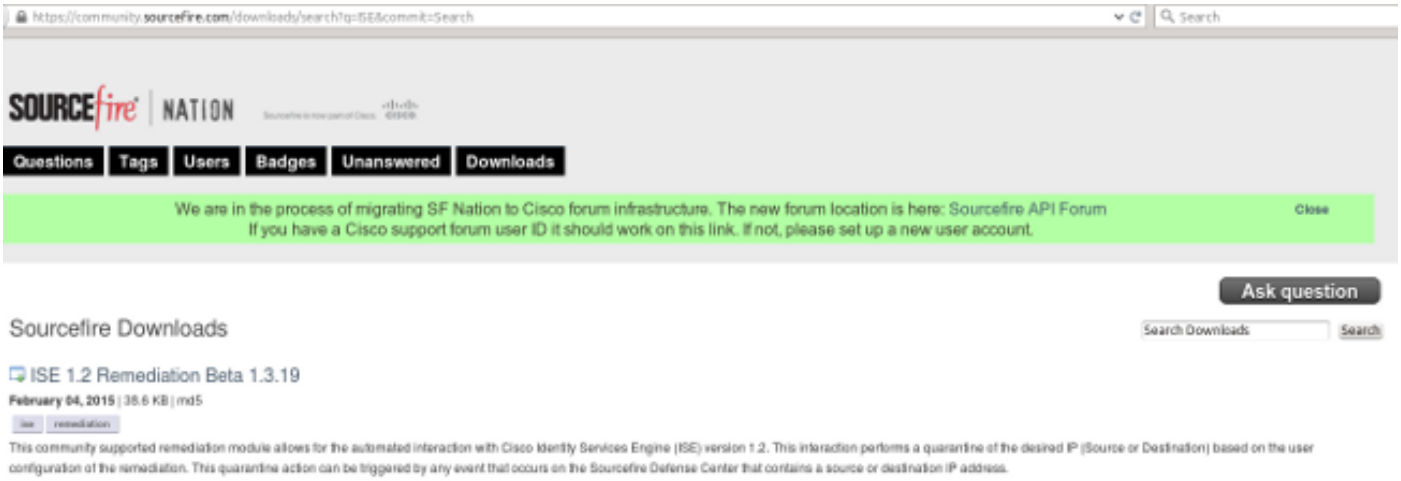
Política de controle de acesso

Depois de instalar as licenças corretas e adicionar o dispositivo FirePower, navegue até **Policies > Access Control** e crie a política de acesso usada para descartar o tráfego HTTP para 172.16.32.1:

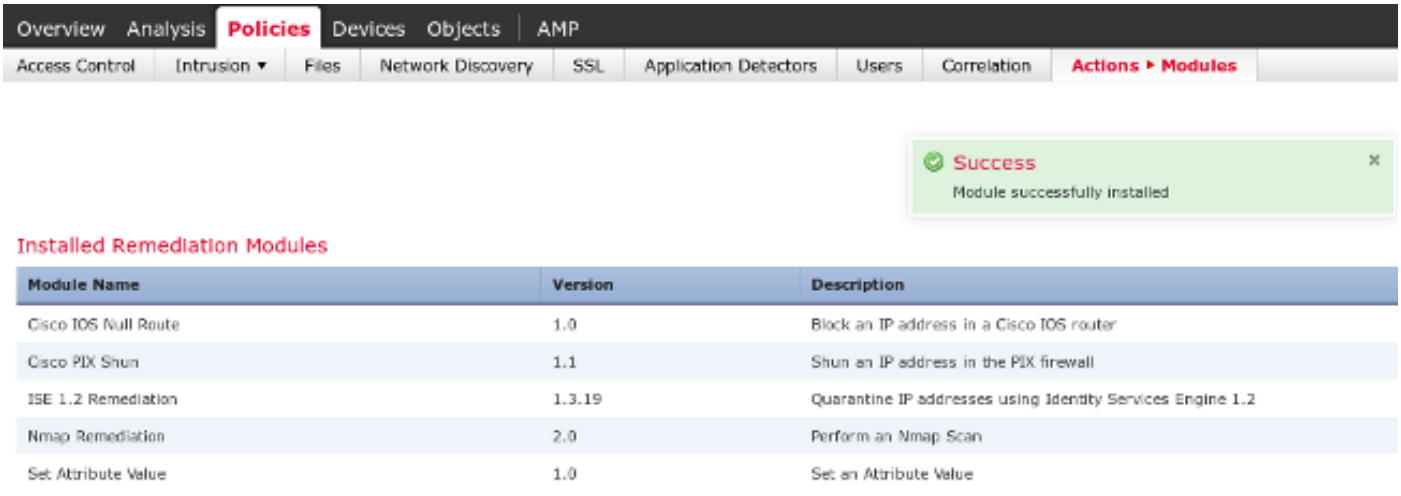
Todo o tráfego restante é aceito.

Módulo de correção do ISE

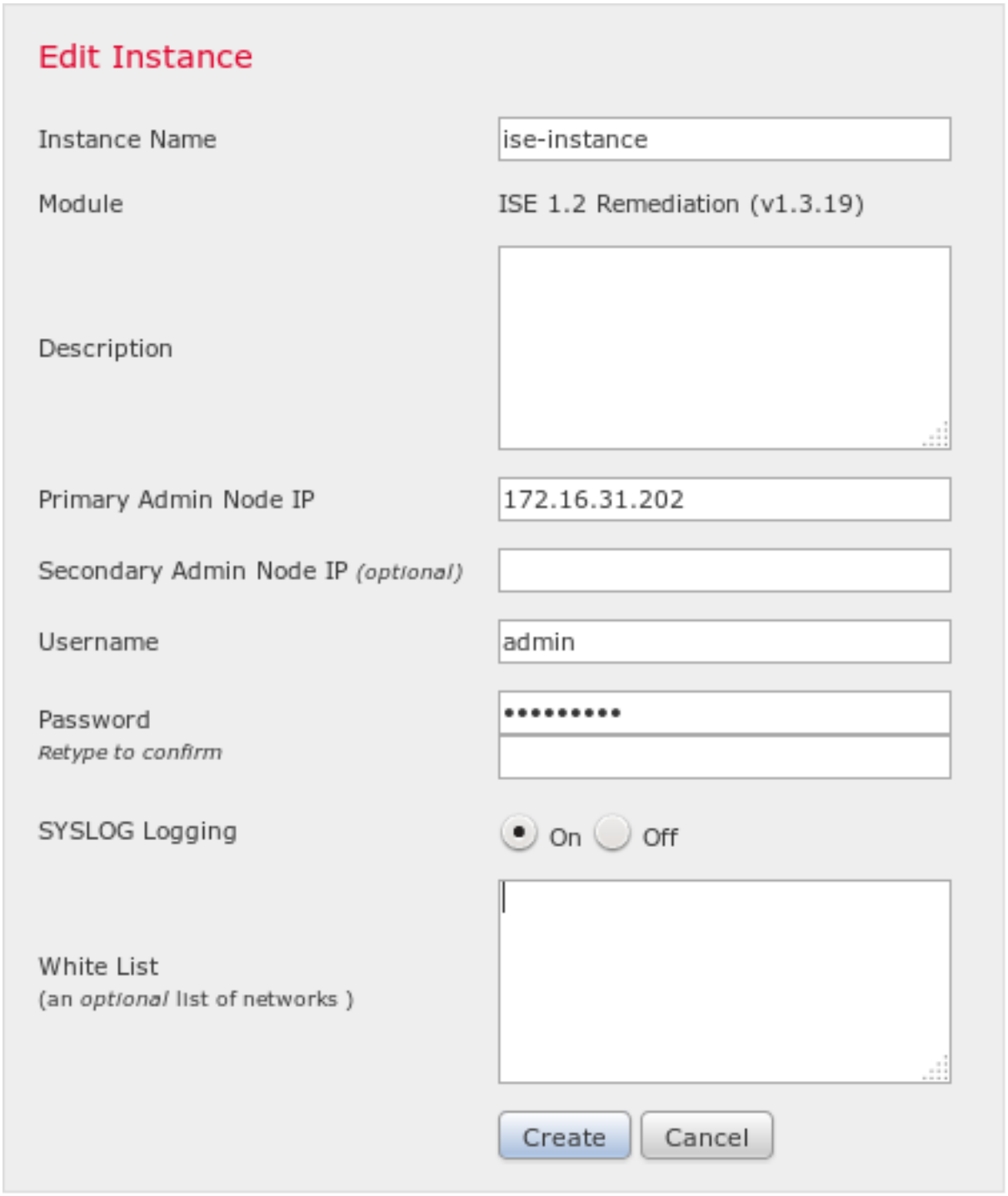
A versão atual do módulo ISE que é compartilhada no portal da comunidade é *ISE 1.2 Remediation Beta 1.3.19*:



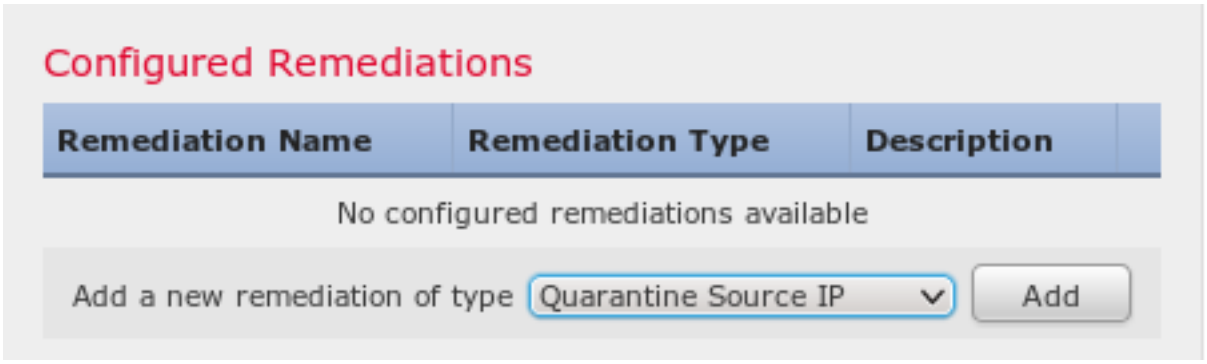
Navegue até **Policies > Actions > Remediations > Modules** e instale o arquivo:



A instância correta deve ser criada. Navegue até **Policies > Actions > Remediations > Instances** e forneça o endereço IP do Policy Administration Node (PAN), juntamente com as credenciais administrativas do ISE necessárias para a API REST (um usuário separado com a função *ERS Admin* é recomendado):

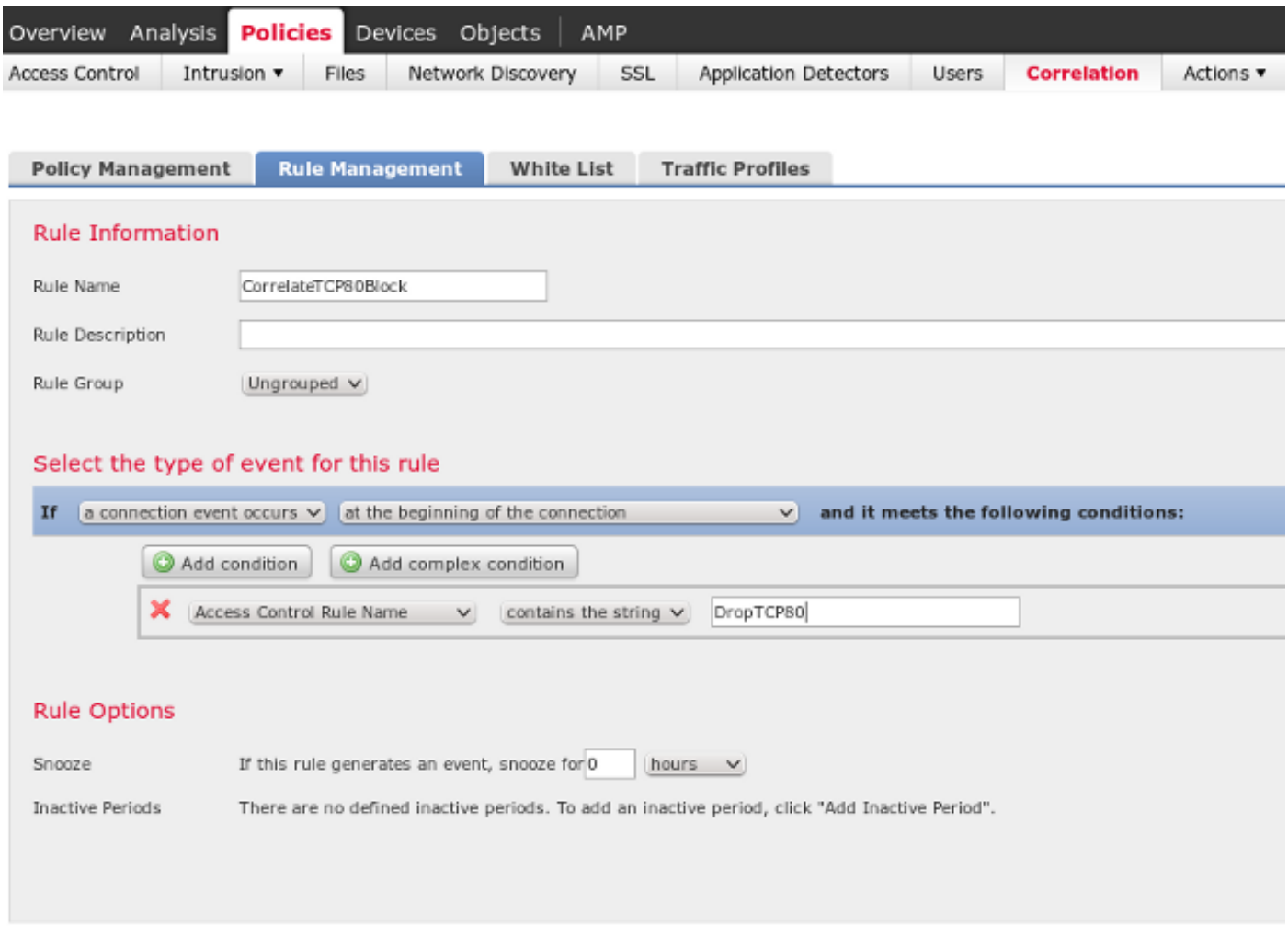


O endereço IP de origem (invasor) também deve ser usado para correção:

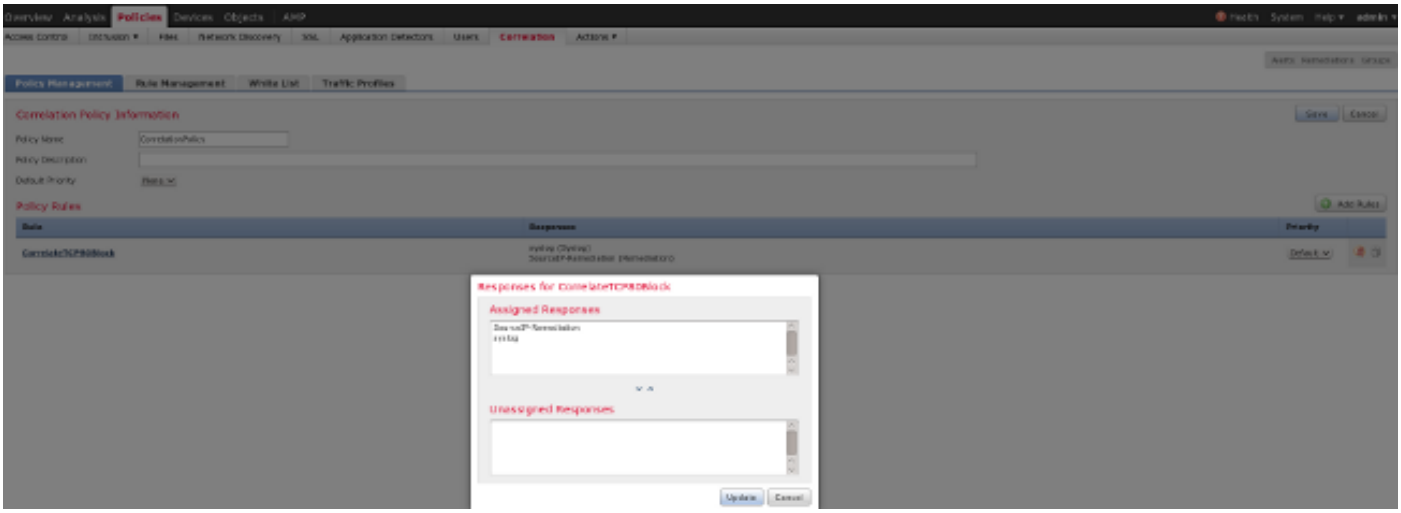


Política de correlação

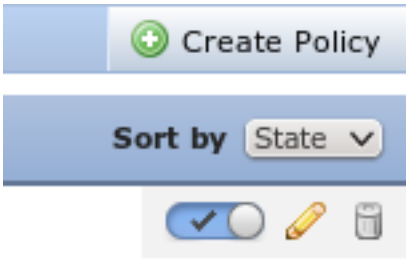
Agora você deve configurar uma regra de correlação específica. Esta regra é acionada no início da conexão que corresponde à regra de controle de acesso configurada anteriormente (*DropTCP80*). Para configurar a regra, navegue para **Políticas > Correlação > Gerenciamento de regras**:



Esta regra é usada na Política de correlação. Navegue até **Policies > Correlation > Policy Management** para criar uma nova política e adicione a regra configurada. Clique em **Corrigir** à direita e adicione duas ações: **correção para sourceIP** (configurado anteriormente) e **syslog**:



Assegure-se de habilitar a política de correlação:



ASA

Um ASA que atua como um gateway VPN é configurado para usar o ISE para autenticação. É também necessário habilitar a contabilidade e o 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
```

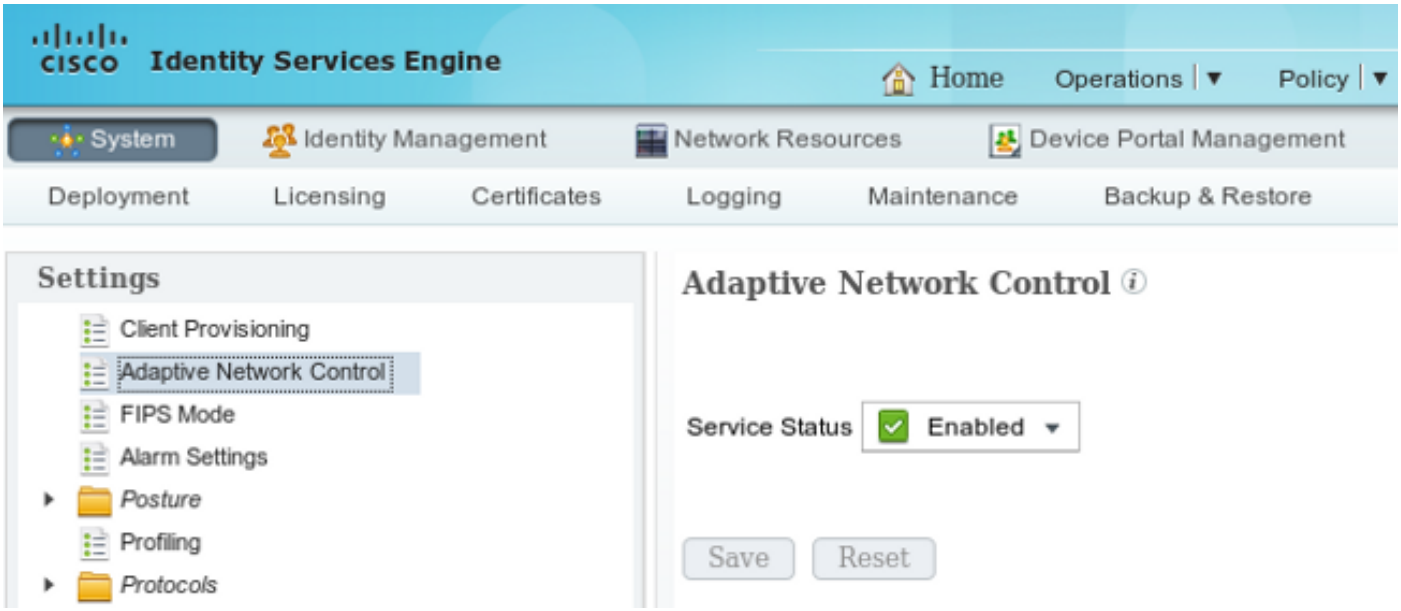
ISE

Configurar o NAD (Network Access Device, dispositivo de acesso à rede)

Navegue até **Administration > Network Devices** e adicione o ASA que atua como um cliente RADIUS.

Habilitar controle de rede adaptável

Navegue até **Administration > System > Settings > Adaptive Network Control** para ativar a API de quarentena e a funcionalidade:



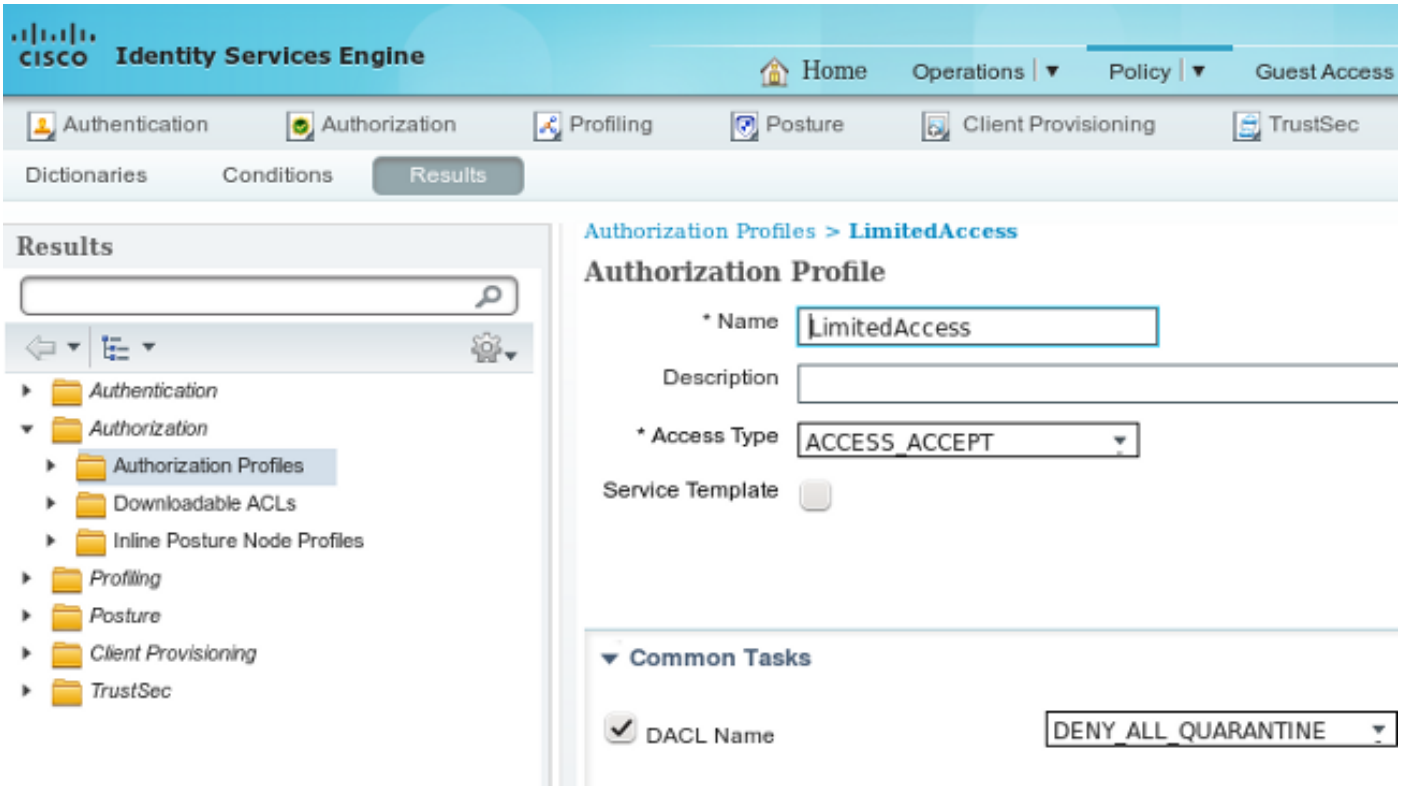
Note: Nas versões 1.3 e anteriores, esse recurso é chamado de *Serviço de proteção de endpoint*.

DACL de quarentena

Para criar uma Lista de Controle de Acesso (DACL - Access Control List) para download usada para os hosts em quarentena, navegue para **Política > Resultados > Autorização > ACL para download**.

Perfil de autorização para quarentena

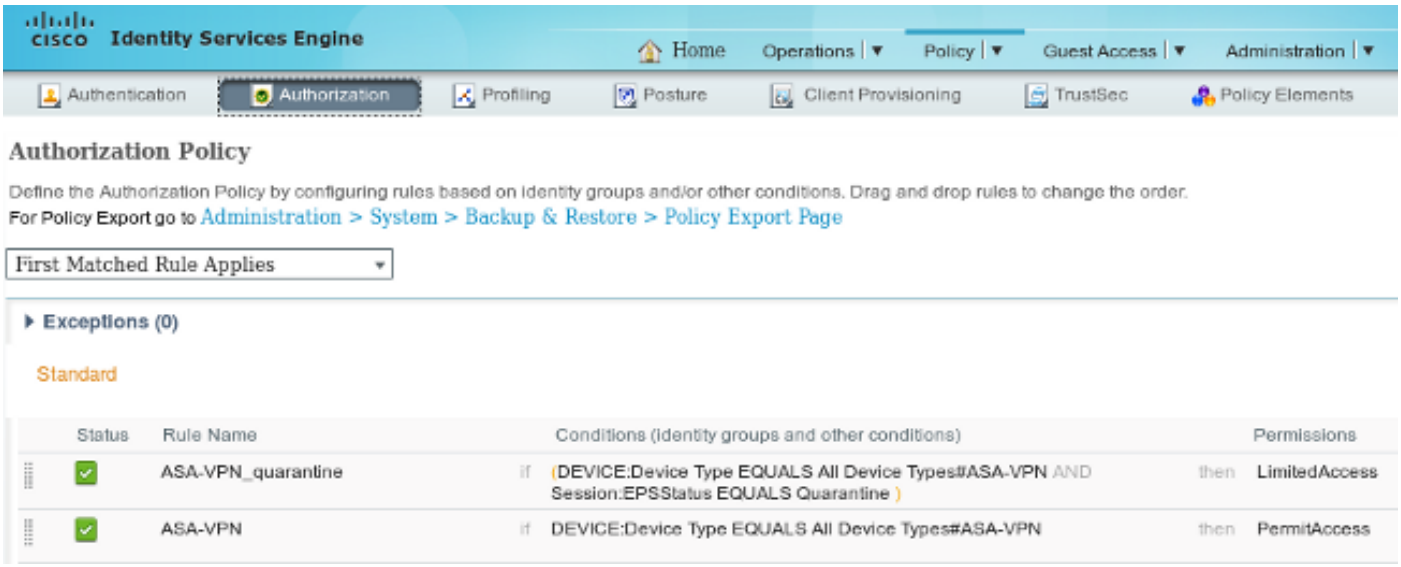
Navegue até **Policy > Results > Authorization > Authorization Profile** e crie um perfil de autorização com o novo DACL:



Regras de autorização

Você deve criar duas regras de autorização. A primeira regra (ASA-VPN) fornece acesso total para todas as sessões de VPN terminadas no ASA. A regra *ASA-VPN_quarantine* é acessada para a sessão VPN reautenticada quando o host já está em quarentena (o acesso limitado à rede é fornecido).

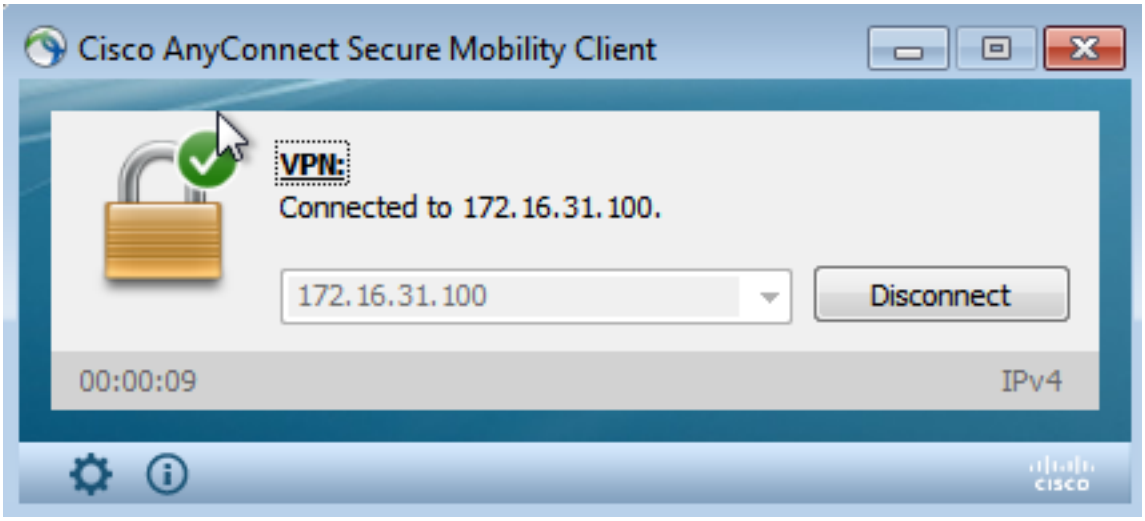
Para criar essas regras, navegue para **Política > Autorização**:



Verificar

Use as informações fornecidas nesta seção para verificar se a configuração funciona corretamente.

O AnyConnect inicia a sessão de VPN do ASA



O ASA cria a sessão sem qualquer DACL (acesso total à rede):

```
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>
```

O usuário tenta acessar

Quando o usuário tenta acessar http://172.16.32.1, a política de acesso é atingida, o tráfego correspondente é bloqueado inline e a mensagem de syslog é enviada do endereço IP de gerenciamento do 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,
```

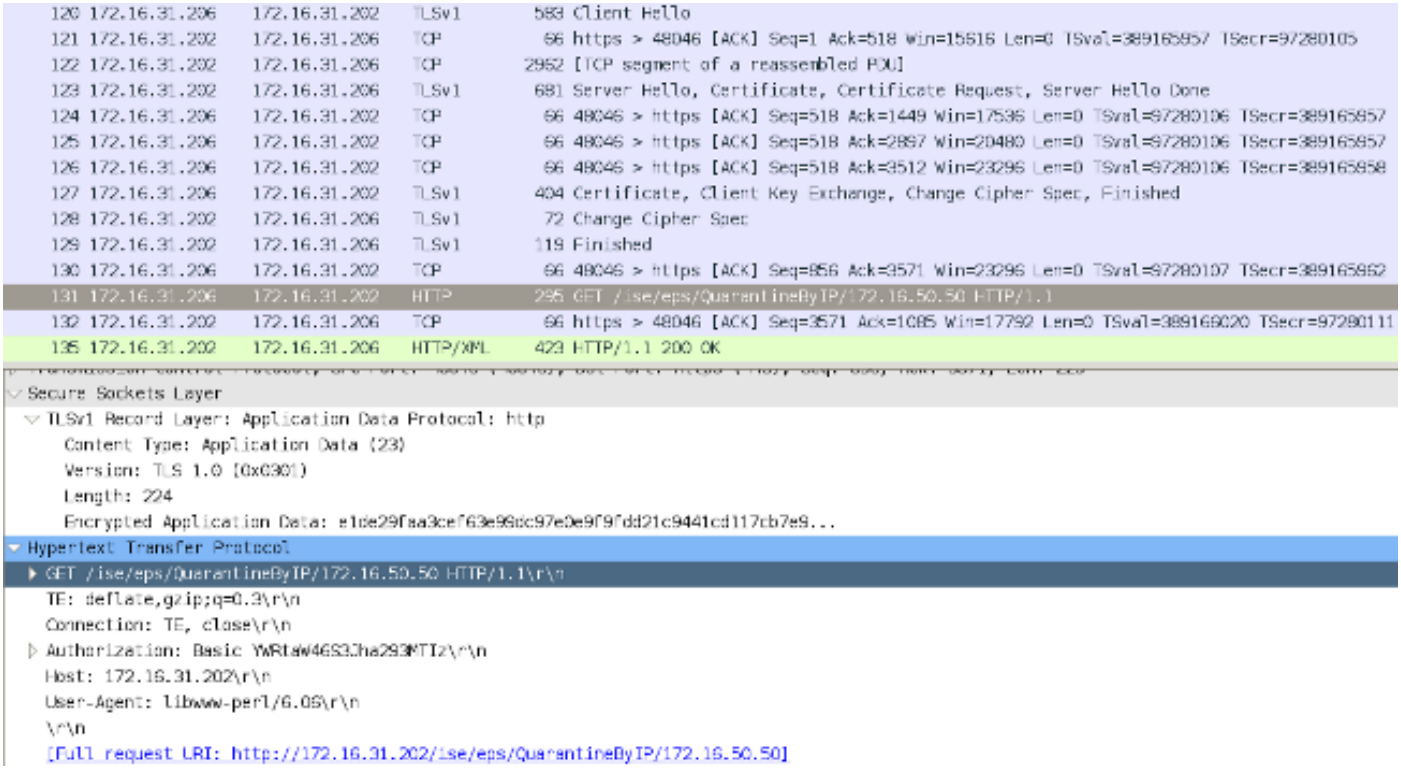
```
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 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
```

Acerto na política de correlação do FireSight

A Política de correlação do gerenciamento do FireSight (Defense Center) é atingida, o que é relatado pela mensagem de syslog enviada do Defense Center:

```
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)
```

Neste estágio, o Defense Center usa a chamada REST API (quarentena) para o ISE, que é uma sessão HTTPS e pode ser descriptografada no Wireshark (com o plug-in Secure Sockets Layer (SSL) e a chave privada do certificado administrativo PAN):



Na solicitação GET para o endereço IP do invasor, passa (172.16.50.50) e esse host é colocado em quarentena pelo ISE.

Navegue até **Análise > Correlação > Status** para confirmar a correção bem-sucedida:

O ISE realiza a quarentena e envia CoA

Neste estágio, o ISE *prrt-management.log* notifica que o CoA deve ser enviado:

```
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
```

O tempo de execução (prrt-server.log) envia a mensagem *de terminação* de CoA ao NAD, que encerra a sessão (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
```

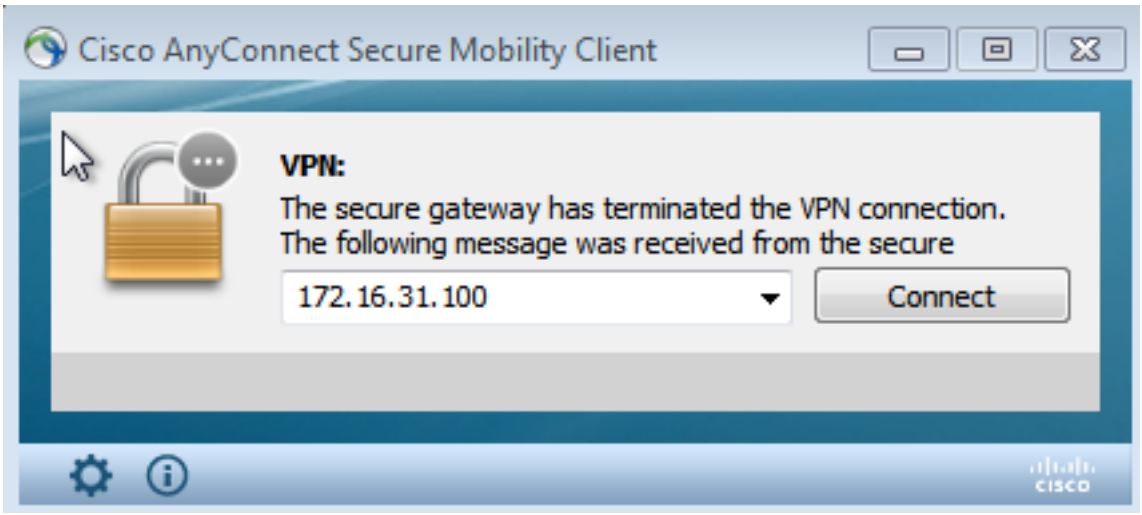
O *ise.psc* envia uma notificação semelhante a esta:

```
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
```

Quando você navega para **Operations > Authentication**, ele deve mostrar *Dynamic Authorization bem-sucedido*.

Sessão VPN desconectada

O usuário final envia uma notificação para indicar que a sessão está desconectada (para 802.1x/MAB/convidado com fio/sem fio, este processo é transparente):

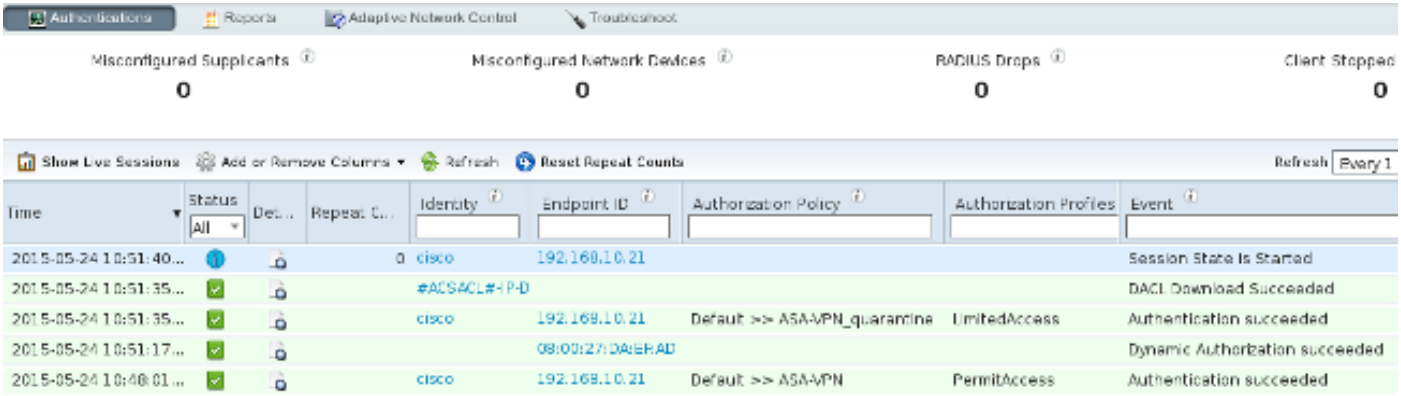


Os detalhes dos registros do Cisco AnyConnect mostram:

```
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
```

Sessão VPN com acesso limitado (quarentena)

Como a *VPN sempre ativa* está configurada, a nova sessão é criada imediatamente. Desta vez, a regra *ASA-VPN_quarantine* do ISE é atingida, o que fornece o acesso limitado à rede:



Note: O DACL é baixado em uma solicitação RADIUS separada.

Uma sessão com acesso limitado pode ser verificada no ASA com o comando CLI **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 ommited for clarity>
  Filter Name  : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

Troubleshoot

Esta seção fornece informações que você pode usar para solucionar problemas de sua configuração.

FireSight (Centro de defesa)

O script de correção do ISE reside neste local:

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

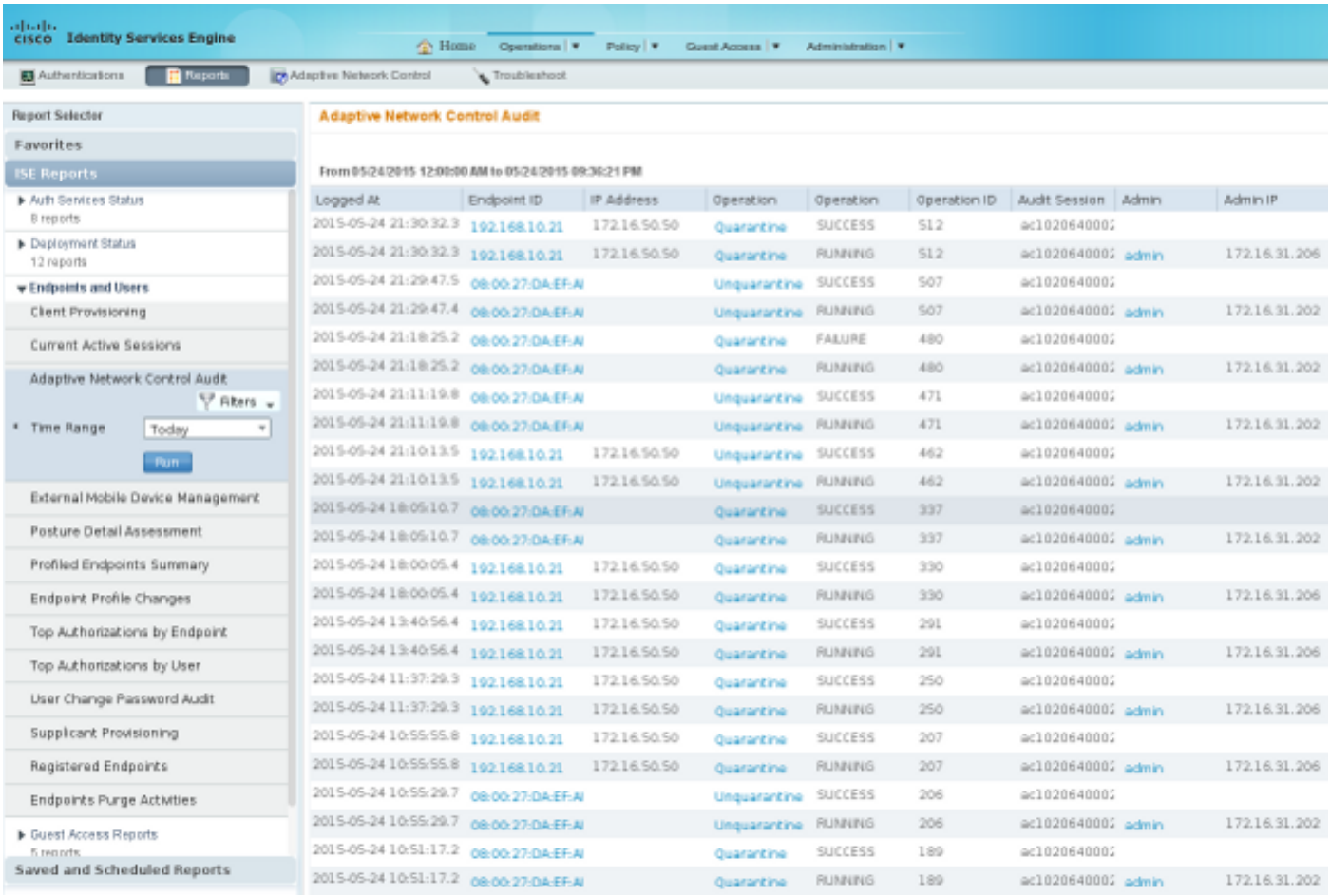
Este é um script de *perl* que usa o subsistema de registro padrão SourceFire (SF). Depois que a correção for executada, você poderá confirmar os resultados por meio do */var/log/messages*:

```
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

Éimportante que você habilite o serviço de controle de rede adaptável no ISE. Para visualizar os registros detalhados em um processo de tempo de execução (*prrt-management.log* e *prrt-server.log*), você deve habilitar o nível DEBUG para Runtime-AAA. Navegue até **Administration > System > Logging > Debug Log Configuration** para habilitar as depurações.

Você também pode navegar para **Operations > Reports > Endpoint and Users > Adaptive Network Control Audit** para exibir as informações de todas as tentativas e resultados de uma solicitação de quarentena:



Bugs

Consulte o bug da Cisco ID CSCuu41058 (inconsistência de quarentena de endpoint ISE 1.4 e falha de VPN) para obter informações sobre um bug do ISE relacionado a falhas de sessão VPN (802.1x/MAB funciona bem).

Informações Relacionadas

- Configurar a integração do WSA com o ISE para serviços cientes do TrustSec
- Integração do ISE versão 1.3 pxGrid com aplicativo IPS pxLog
- Cisco Identity Services Engine Administrator Guide, versão 1.4 - Setup Adaptive Network Control
- Guia de referência de API do Cisco Identity Services Engine, versão 1.2 - Introdução à API de Serviços RESTful Externos
- Guia de referência da API do Cisco Identity Services Engine, versão 1.2 - Introdução às APIs REST de monitoramento
- Guia do administrador do Cisco Identity Services Engine, versão 1.3

- Suporte técnico e documentação - Cisco Systems