Remediatieservices met ISE en FirePower-integratie configureren

Inhoud

Inleiding

Dit document beschrijft hoe u de servicemodule op een Cisco FireSight-apparaat kunt gebruiken om aanvallen te detecteren en de aanvallen automatisch te herstellen met het gebruik van de Cisco Identity Services Engine (ISE) als beleidsserver. Het voorbeeld dat in dit document wordt gegeven, beschrijft de methode die wordt gebruikt voor het herstel van een externe VPN-gebruiker die via ISE authentiek verklaart, maar het kan ook worden gebruikt voor een bekabelde of draadloze gebruiker 802.1x/MAB/Webex.

Opmerking: De aanpassingsmodule waarnaar in dit document wordt verwezen wordt niet officieel ondersteund door Cisco. Het wordt gedeeld op een communautair portaal en kan door iedereen gebruikt worden. In versies 5.4 en hoger is er ook een nieuwere herstelmodule beschikbaar die is gebaseerd op het *pxGrid*-protocol. Deze module wordt niet ondersteund in versie 6.0, maar zal naar verwachting in toekomstige versies worden ondersteund.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco adaptieve security applicatie (ASA) VPN-configuratie
- Cisco AnyConnect Secure Mobility Client-configuratie
- Cisco FireSight-basisconfiguratie
- Cisco FirePower-basisconfiguratie
- Cisco ISE-configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco ASA versie 9.3 of hoger
- Cisco ISE-softwareversies 1.3 en hoger
- Cisco AnyConnect Secure Mobility Client versies 3.0 en hoger
- Cisco FireSIGHT Management Center versie 5.4
- Cisco FirePOWER versie 5.4 (virtuele machine)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

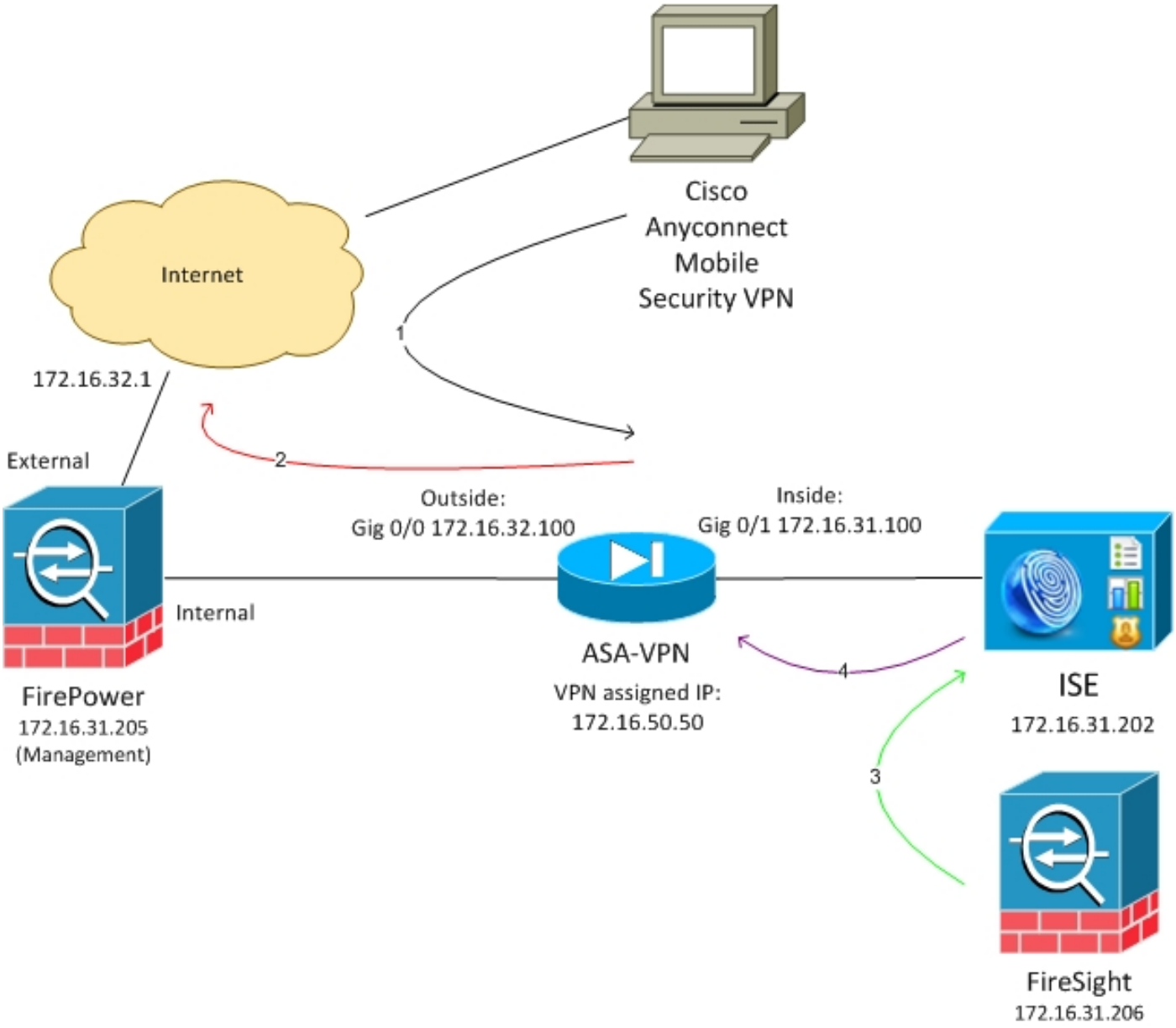
Configureren

Gebruik de informatie in dit gedeelte om het systeem te configureren.

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het in dit document beschreven voorbeeld gebruikt deze netwerkinstellingen:



Dit is de stroom voor deze netwerkinstellingen:

1. De gebruiker start een externe VPN-sessie met de ASA (via Cisco AnyConnect Secure Mobility versie 4.0).

2. De gebruiker probeert toegang te krijgen tot *http://172.16.32.1*. (Het verkeer verloopt via FirePower, dat op de VM is geïnstalleerd en wordt beheerd door FireSight.)

3. FirePower is zo geconfigureerd dat het dat specifieke verkeer blokkeert (inline) (toegangsbeleid), maar heeft ook een correlatiebeleid dat wordt geactiveerd. Als resultaat hiervan start het ISE-herstel via REST Application Programming Interface (API) (de *QuarantineByIP*-methode).

4. Zodra ISE de REST API-oproep ontvangt, zoekt zij naar de sessie en stuurt zij een RADIUS-wijziging van autorisatie (CoA) naar de ASA, die die sessie beëindigt.

5. De ASA ontkoppelt de VPN-gebruiker. Aangezien AnyConnect is ingesteld met een *altijd*-on VPN-toegang, wordt een nieuwe sessie ingesteld; deze keer wordt echter een andere ISE Authorization-regel (voor in quarantaine gehouden hosts) aangepast en wordt de beperkte toegang tot het netwerk geboden . In dit stadium is het niet van belang hoe de gebruiker zich aansluit op en authentiek verklaart op het netwerk; zolang de ISE wordt gebruikt voor verificatie en autorisatie, heeft de gebruiker beperkte toegang tot het netwerk als gevolg van quarantaine.

Zoals eerder vermeld, werkt dit scenario voor elk type geauthentiseerde sessie (VPN, bekabeld 802.1x/MAB/Webauth, draadloos 802.1x/MAB/Webauth) zolang ISE voor authenticatie wordt gebruikt en het apparaat voor netwerktoegang de RADIUS CoA (alle moderne Cisco-apparaten) ondersteunt.

> **Tip**: U kunt de gebruiker uit quarantaine plaatsen door de ISE GUI te gebruiken. Toekomstige versies van de saneringsmodule zouden dit ook kunnen ondersteunen.

FirePOWER

> **Opmerking:** Een VM-apparaat wordt gebruikt voor het voorbeeld dat in dit document wordt beschreven. Alleen de eerste configuratie wordt via de CLI uitgevoerd. Alle beleid wordt geconfigureerd vanuit Cisco Defense Center. Raadpleeg het gedeelte Verwante informatie van dit document voor meer informatie.

De VM heeft drie interfaces, één voor beheer en twee voor inline inspectie (intern/extern).

Al het verkeer van de VPN-gebruikers beweegt via FirePower.

FireSIGHT Management Center (Defense Center)

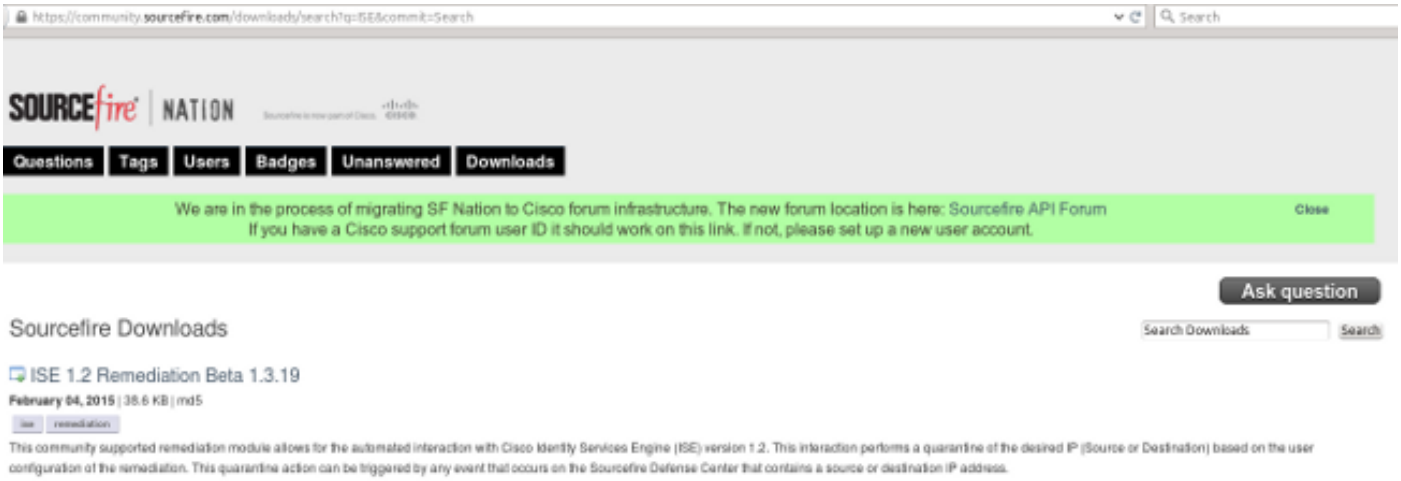
Toegangsbeheerbeleid

Nadat u de juiste licenties hebt geïnstalleerd en het FirePower-apparaat hebt toegevoegd, navigeer dan naar **Beleid > Toegangsbeheer** en maakte u het toegangsbeleid dat wordt gebruikt om het HTTP-verkeer te laten vallen naar 172.16.32.1:

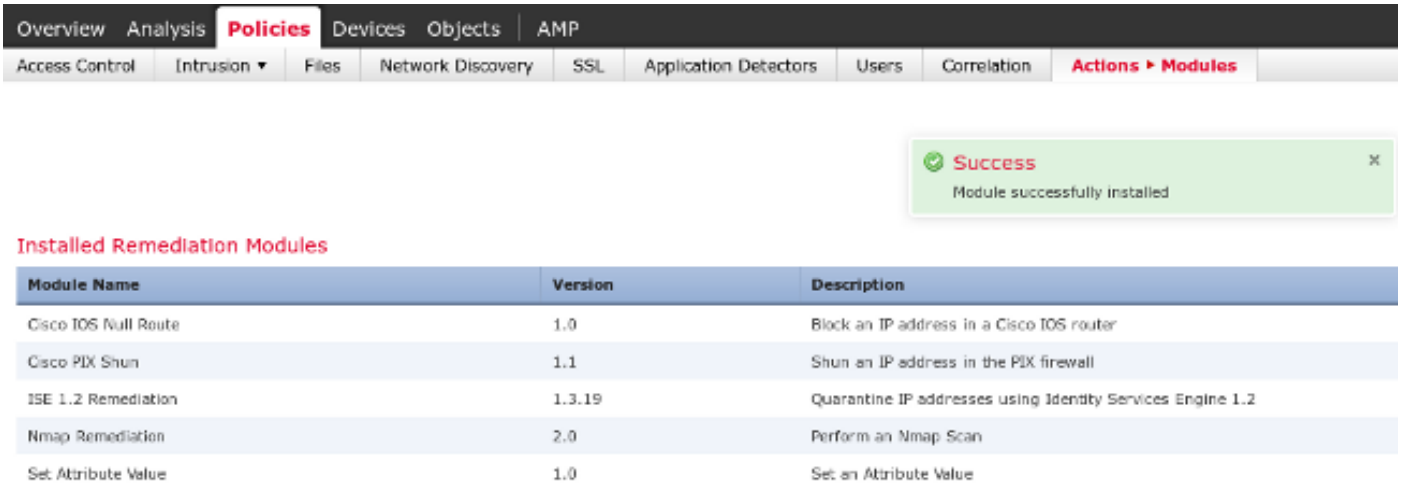
Al het andere verkeer is geaccepteerd.

ISE-servicemodule voor vernieuwing

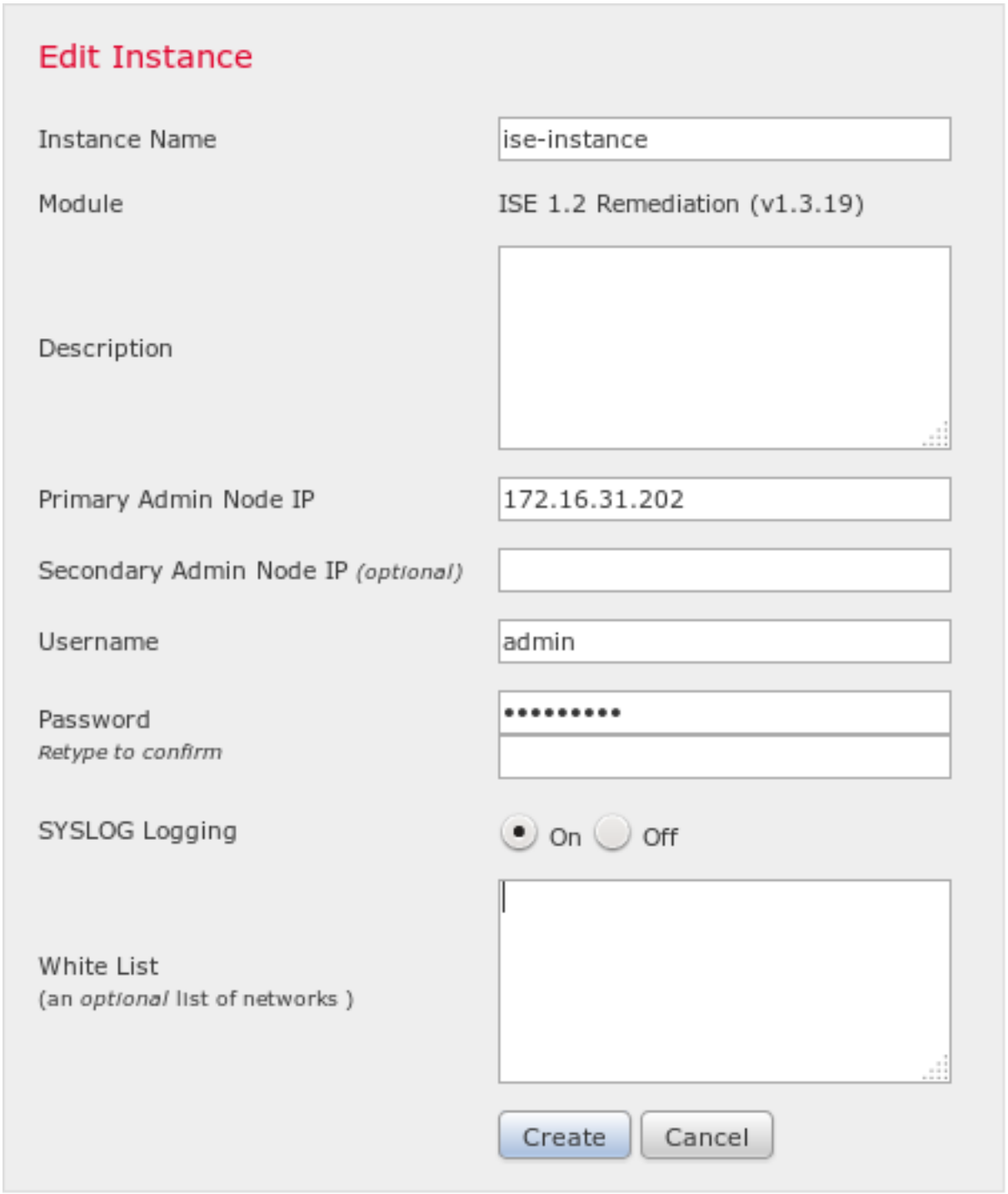
De huidige versie van de ISE-module die op het communautaire portaal wordt gedeeld, is *ISE 1.2 Remediation Bèta 1.3.19*:



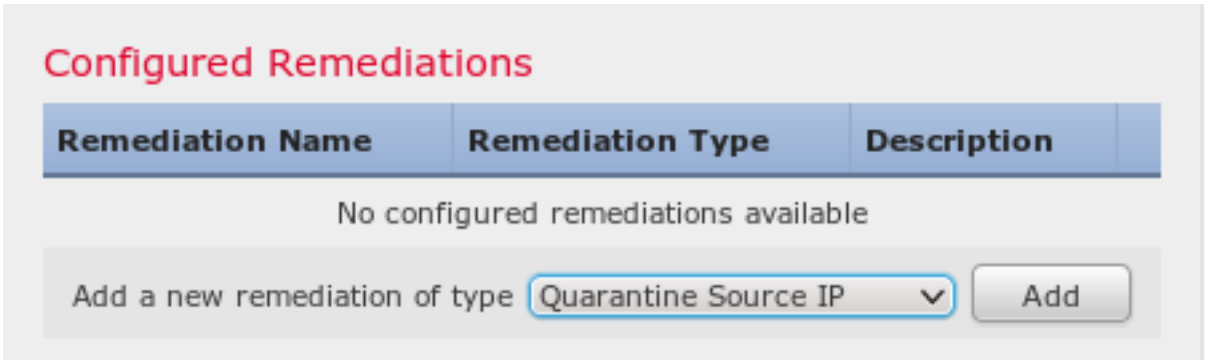
Navigeren in op **beleid > Handelingen > Verstellingen > Modules** en installeren het bestand:



Het juiste voorbeeld moet dan worden gecreëerd. Navigeer naar **beleid > Maatregelen > Remediations > Instanties** en verstrek het IP-adres van het beleidsbeheerknooppunt (PAN), samen met de ISE-administratieve aanmeldingsgegevens die nodig zijn voor REST API (een afzonderlijke gebruiker met de *ERS Admin*-rol wordt aanbevolen):

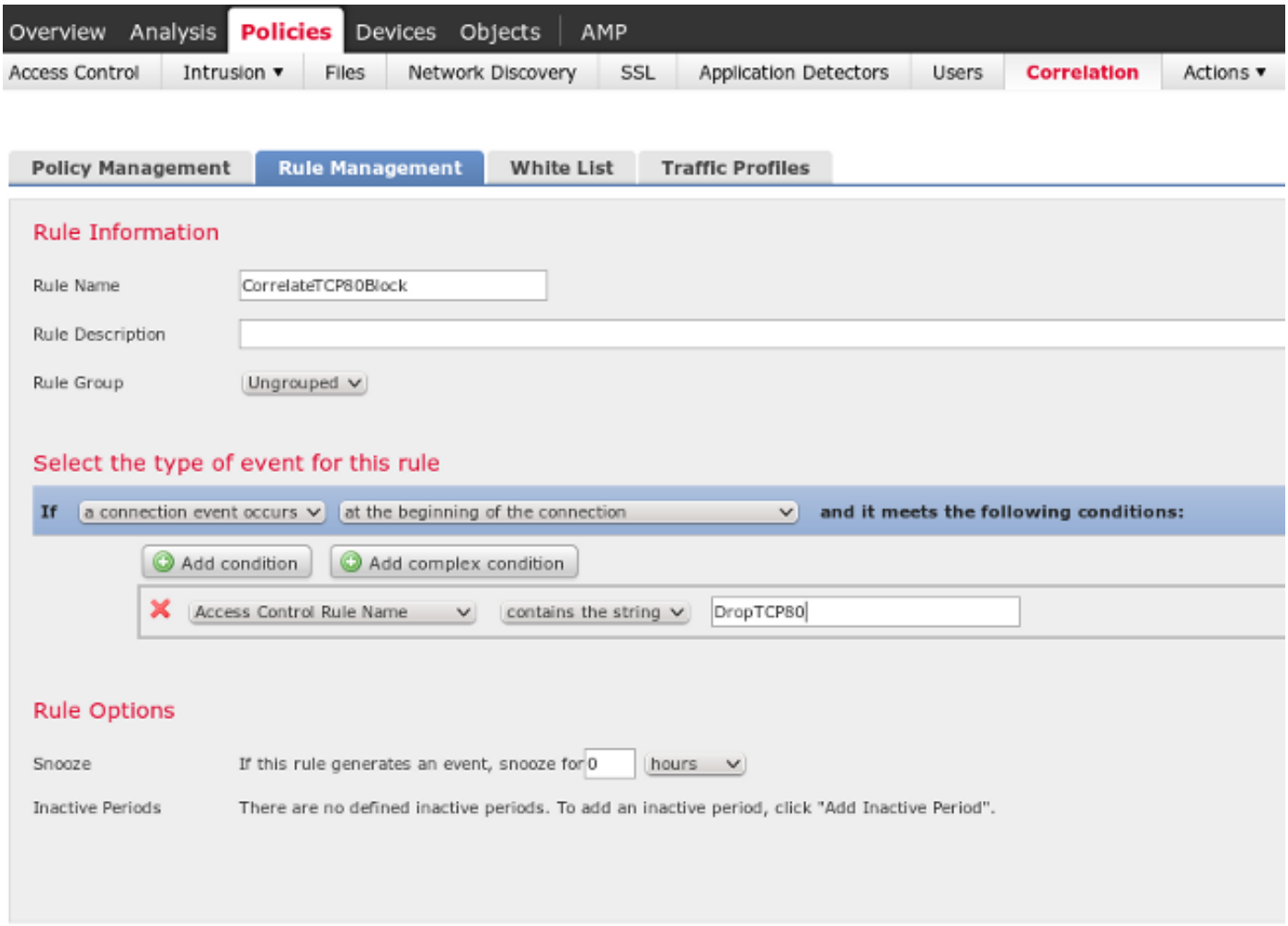


Het IP-adres van de bron (aanvaller) moet ook worden gebruikt voor herstel:

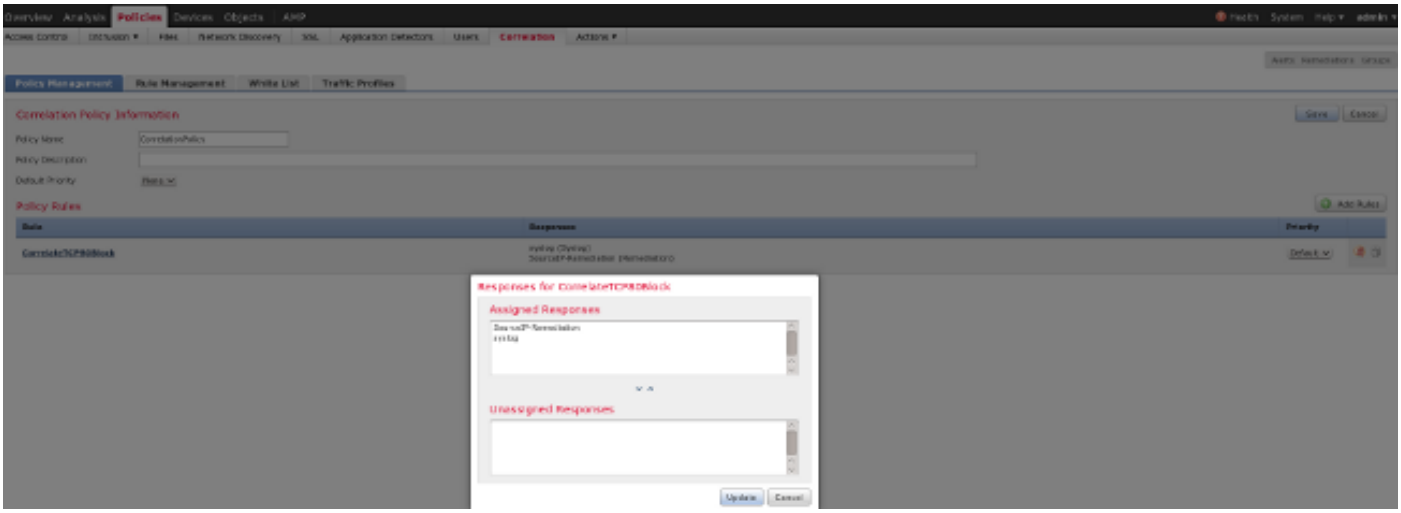


Correlatiebeleid

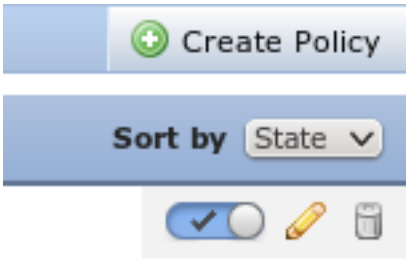
U moet nu een specifieke correlatieregel configureren. Deze regel wordt geactiveerd aan het begin van de verbinding die de eerder gevormde toegangscontroleregel (*DropTCP80*) aanpast. Om de regel te configureren volgt u **beleid > Correlatie > Regelbeheer**:



Deze regel wordt gebruikt in het Correlatiebeleid. Navigeer naar **beleid > Correlatie > Beleidsbeheer** om een nieuw beleid te creëren en voeg dan de geconfigureerde regel toe. Klik op **Opfrissen** aan de rechterkant en voeg twee handelingen toe: **sanering voor sourceIP** (eerder geconfigureerd) en **syslog**:



Zorg ervoor dat u het correlatiebeleid mogelijk maakt:



ASA

Een ASA die als VPN-gateway fungeert, wordt ingesteld om ISE voor verificatie te gebruiken. Het is ook noodzakelijk om de boekhouding en de RADIUS-CoA mogelijk te maken:

```
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
```

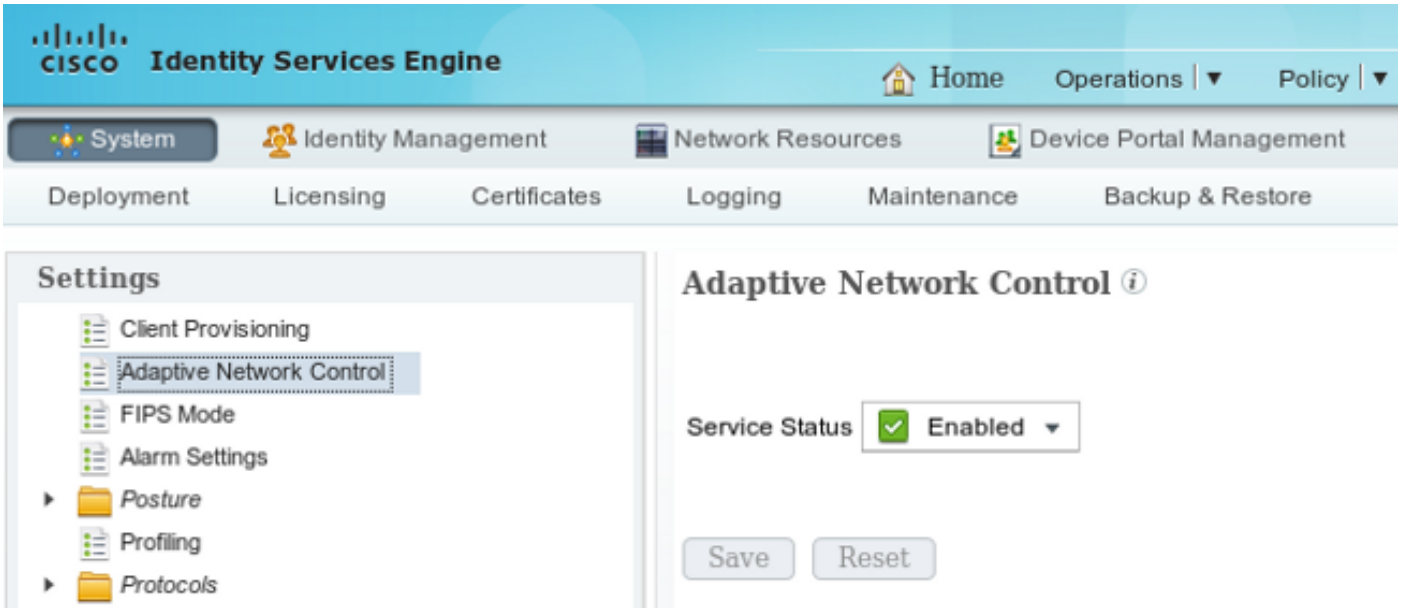
ISE

Netwerktoegangsapparaat (NAD) configureren

Navigeer naar **Beheer > Netwerkapparaten** en voeg de ASA toe die als een RADIUS-client werkt.

Adaptieve netwerkcontrole inschakelen

Navigeer naar **Beheer > Systeem > Instellingen > Adaptieve Netwerkcontrole** om quarantaine API en functionaliteit mogelijk te maken:



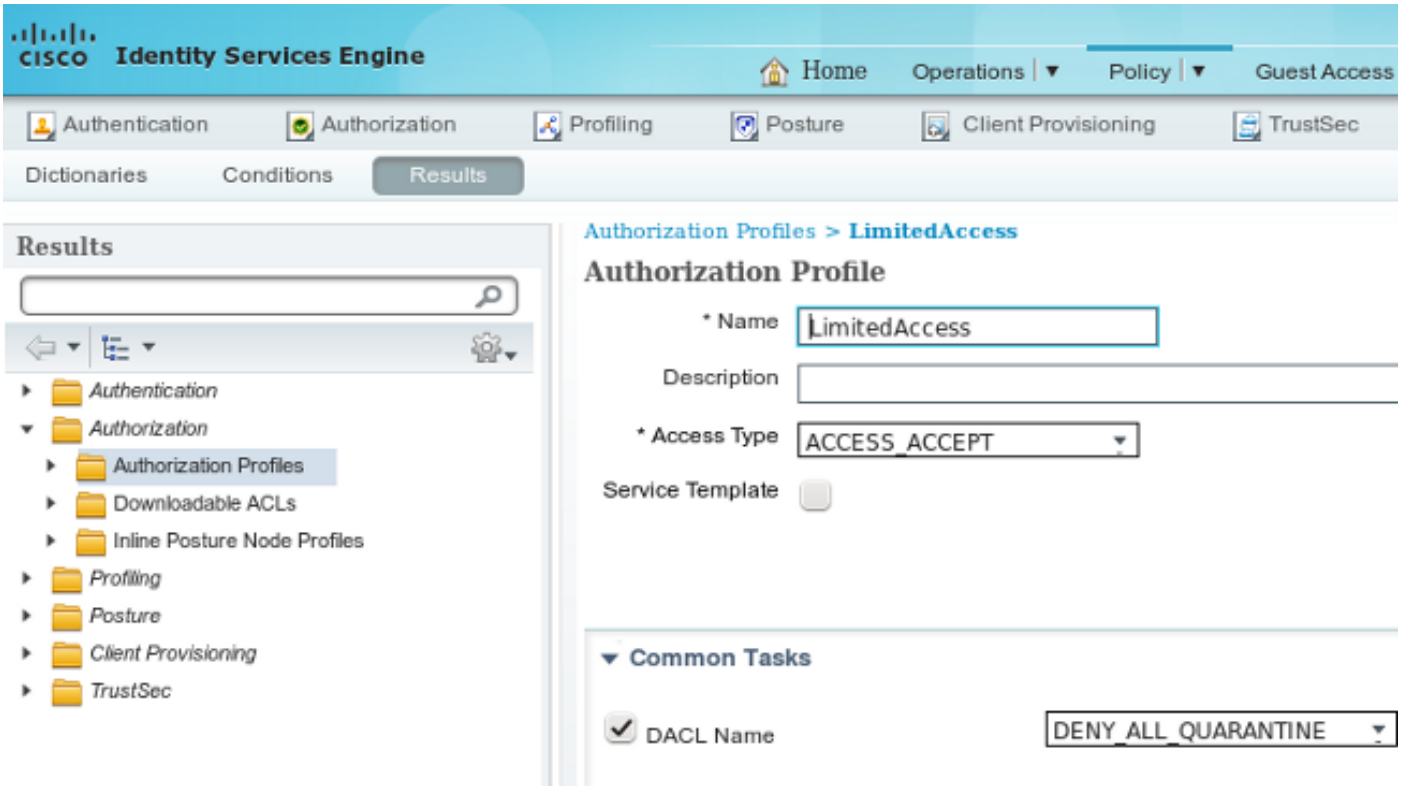
Opmerking: In versies 1.3 en eerder wordt deze optie *Endpoint Protection Service* genoemd.

Quarantine DACL

Als u een DACL-toegangscontrolelijst (Downloadable Access Control List) wilt maken die voor de in quarantaine geplaatste hosts wordt gebruikt, navigeer dan naar **Policy > Resultaten > Automation > Downloadbare ACL**.

Licentieprofiel voor Quarantine

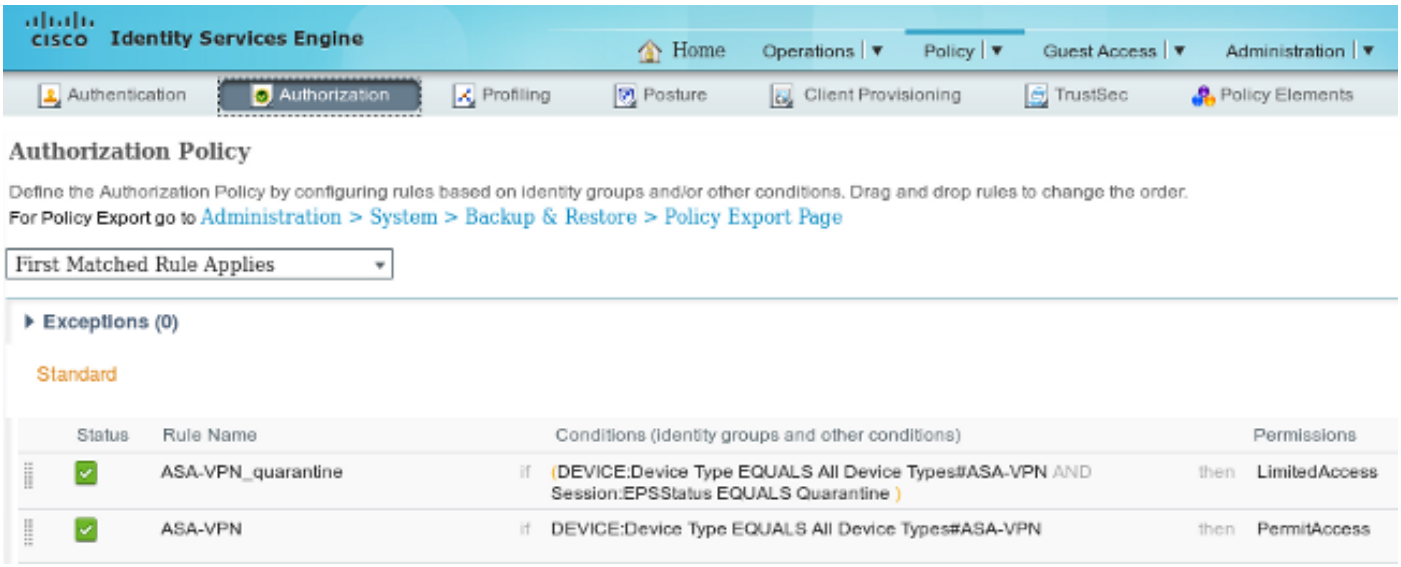
Navigeren in naar **beleid > Resultaten > Vergunning > Vergunningsprofiel** en maken een autorisatieprofiel met de nieuwe DACL:



machtigingsregels

U moet twee vergunningsregels opstellen. De eerste regel (ASA-VPN) verleent volledige toegang voor alle VPN sessies die op de ASA worden beëindigd. De regel *ASA-VPN_quarantaine* wordt ingedrukt voor de opnieuw geauthentiseerde VPN sessie wanneer de host al in quarantaine is geplaatst (de beperkte toegang tot het netwerk wordt verleend).

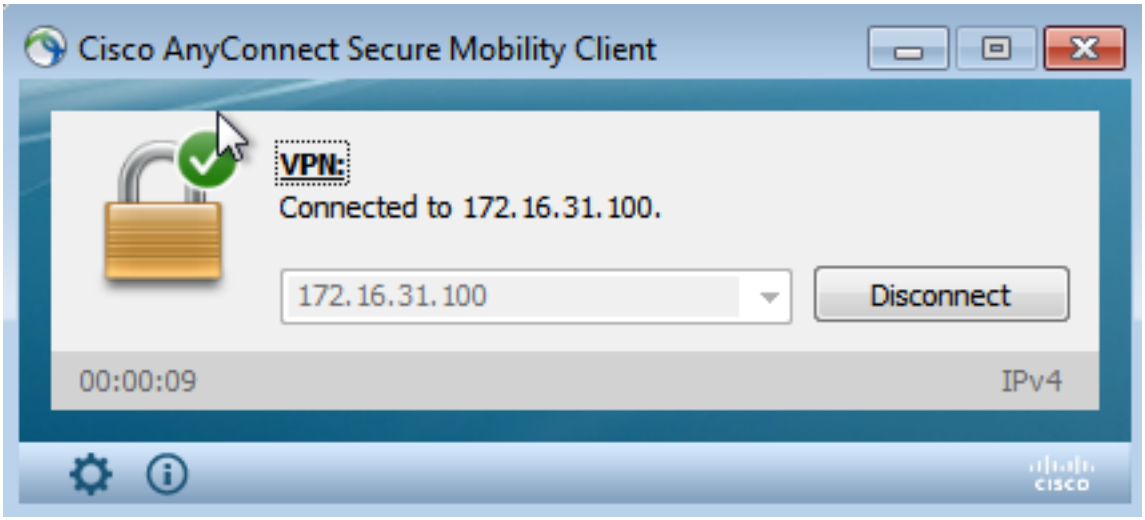
Om deze regels te maken, navigeer dan naar **Beleids > Vergunning**:



Verifiëren

Gebruik de informatie in deze sectie om te controleren of uw configuratie correct werkt.

AnyConnect start ASA VPN-sessie



ASA creëert de sessie zonder DACL (volledige netwerktoegang):

```
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>
```

Toegang tot gebruikerspogingen

Zodra de gebruiker probeert om toegang tot http://172.16.32.1 te krijgen, wordt het toegangsbeleid gevolgd, wordt het verkeer dat correspondeert online geblokkeerd en wordt het syslogbericht verzonden vanaf het FirePower Management IP-adres:

```
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:
```

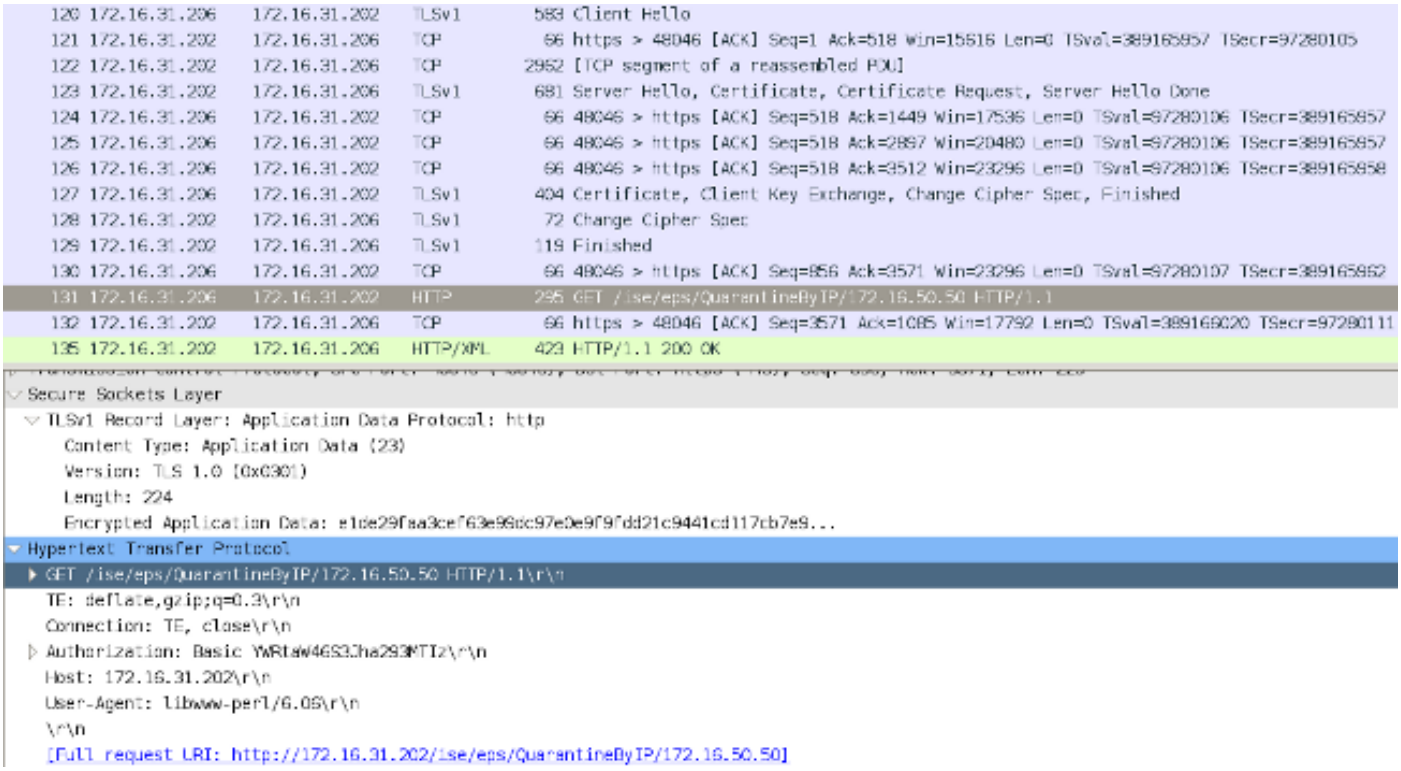
```
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes:
66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A,
SSL Cipher Suite: N/A, SSL Certificate: 0000000000000000000000000000000000000000,
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
```

FireSight Correlatie Policy Sit

Het FireSight Management (Defense Center) Correlatiebeleid is aangetast, wat wordt gemeld door het syslog-bericht dat vanuit Defense Center wordt verstuurd:

```
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)
```

In dit stadium gebruikt het Defense Center de REST API (quarantaine)-oproep naar ISE, een HTTPS-sessie, die kan worden gedecrypteerd in Wireshark (met de Secure Socket Layer (SSL) plug-in en de privé-sleutel van het PAN-bestuurlijke certificaat):



In GET is het verzoek om het IP-adres van de aanvaller doorgegeven (172.16.50.50) en die host wordt in quarantaine geplaatst door de ISE.

Navigeer naar **Analyse > Correlatie > Status** om het succesvolle herstel te bevestigen:

ISE voert quarantaine uit en zendt CoA toe

In dit stadium deelt ISE *prrt-management.log* mee dat de CoA moet worden verstuurd:

```
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
```

Met behulp van een opdrachtregel (prt-server.log) wordt het bericht van CoA naar de NAD verstuurd, dat de sessie (ASA) beëindigt:

```
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
```

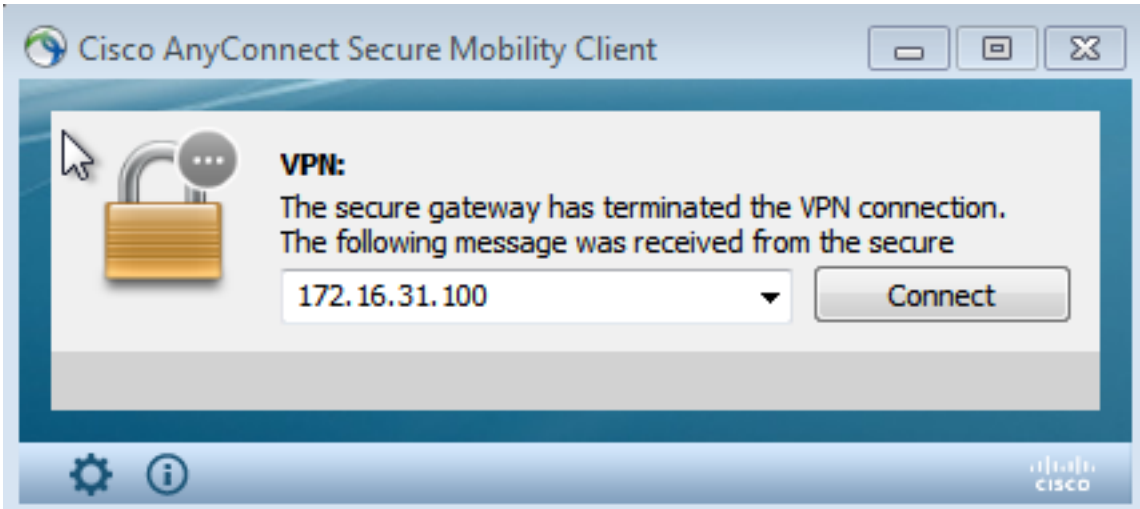
De *ise.psc* stuurt een soortgelijke kennisgeving:

```
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
```

Wanneer u navigeert naar **Operations > Verificatie**, dient u te tonen dat *Dynamische autorisatie is gelukt*.

VPN-sessie is losgekoppeld

De eindgebruiker stuurt een kennisgeving om aan te geven dat de sessie losgekoppeld is (dit proces is transparant voor 802.1x/MAB/gast bedraad/wireless):

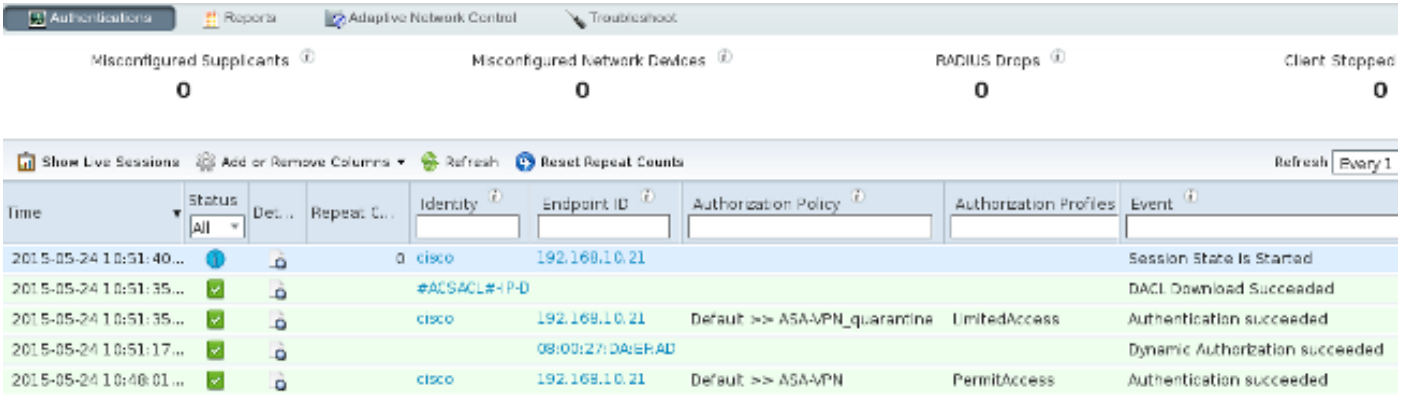


Details uit de Cisco AnyConnect-logbestanden tonen:

```
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
```

VPN-sessie met beperkte toegang (quarantaine)

Omdat *altijd-on VPN* is geconfigureerd wordt de nieuwe sessie onmiddellijk gebouwd. Dit keer wordt de ISE *ASA-VPN_quarantaineregel* geraakt, die de beperkte netwerktoegang verleent:



Opmerking: De DACL wordt gedownload in een afzonderlijk RADIUS-verzoek.

Een sessie met beperkte toegang kan op de ASA met de **show vpn-sessiondb detail** worden geverifieerd **in elke connect** CLI-opdracht:

```
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
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

FireSight (defensiecentrum)

Het ISE-herstelscript bevindt zich op deze locatie:

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

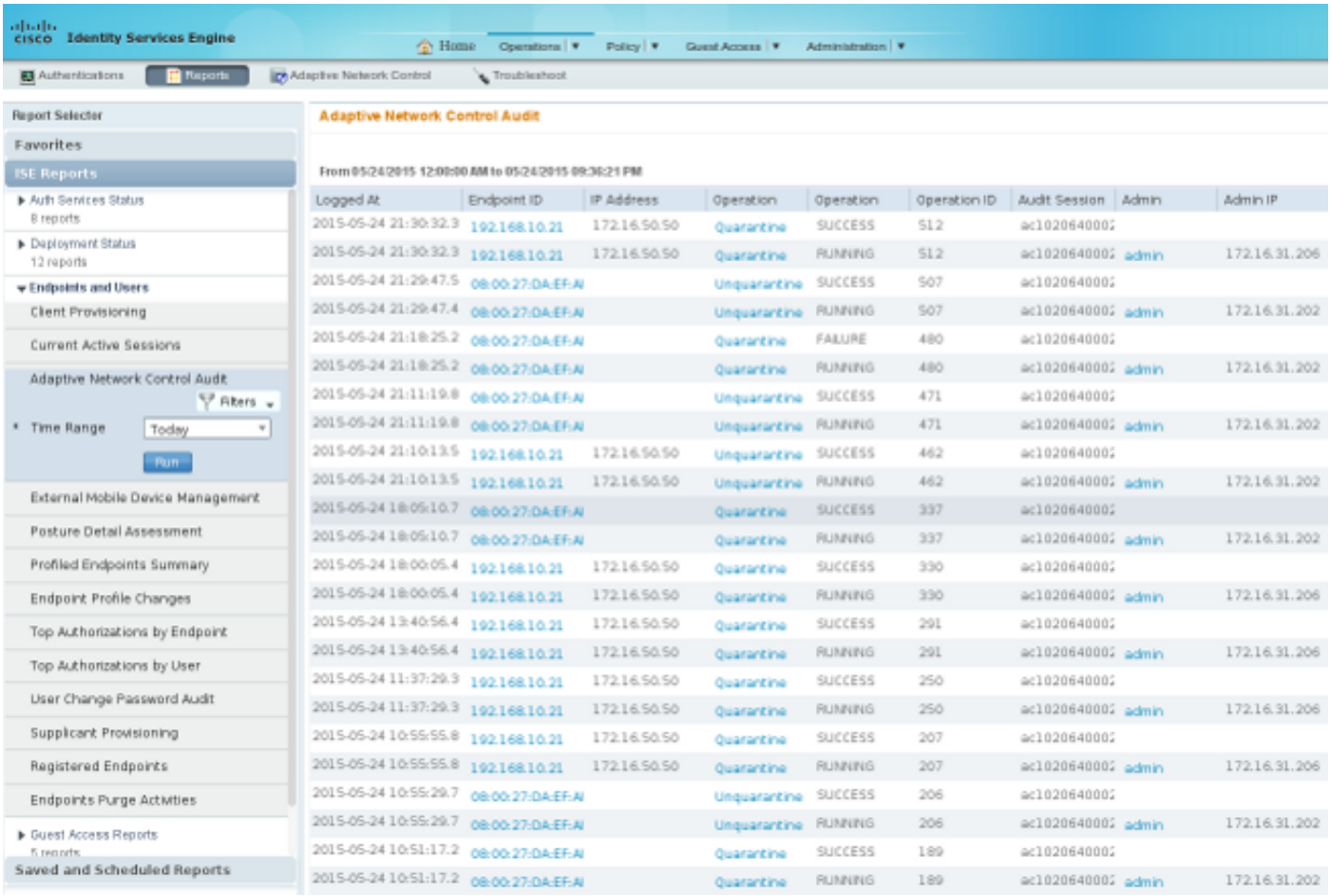
Dit is een eenvoudig *perl* script dat het standaard SourceFire (SF) logging subsysteem gebruikt. Nadat het herstel is uitgevoerd, kunt u de resultaten bevestigen via de */var/log/berichten*:

```
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

Het is belangrijk dat u de Adaptieve Network Control Service op ISE instelt. Om de gedetailleerde logbestanden in een run-proces te bekijken (*prt-management.log* en *prt-server.log*) moet u het DEBUG-niveau inschakelen voor de Runtime-AAA. Navigeer naar **Administratie > Systeem > Vastlegging > Logconfiguratie > Debug Log configuratie** om de knoppen in te schakelen.

U kunt ook navigeren naar **Operations > Rapporten > Endpoint en gebruikers > Adaptieve audit van netwerkcontrole** om informatie te bekijken voor elke poging en resultaat van een quarantaineverzoek:



Bugs

Raadpleeg Cisco bug-ID CSCu41058 (ISE 1.4 Endpoint Quarantine inconsistentie en VPN-storing) voor informatie over een ISE-bug die is gerelateerd aan VPN-sessies (prima werkt 802.1x/MAB).

Gerelateerde informatie

- WSA-integratie met ISE configureren voor TrustSec Aware Services
- ISE versie 1.3 pxGrid-integratie met IPS PxLog toepassing
- Administrator Guide van Cisco Identity Services Engine, release 1.4 - adaptieve netwerkcontrole instellen
- Referentiegids voor Cisco Identity Services Engine API, release 1.2 - Inleiding naar API voor boekingen met externe REST-services
- Cisco Identity Services Engine API Referentiegids, release 1.2 - Inleiding naar de BEWAKING REST API's
- Administrator-gids voor Cisco Identity Services Engine, release 1.3

- Technische ondersteuning en documentatie - Cisco-systemen