

# ISE en FirePower-integratie - voorbeeld van servicsherstel

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[FirePOWER](#)

[FireSIGHT Management Center \(Defense Center\)](#)

[Toegangsbeheerbeleid](#)

[ISE-servicemodule voor vernieuwing](#)

[Correlatiebeleid](#)

[ASA](#)

[ISE](#)

[Netwerktoegangsapparaat \(NAD\) configureren](#)

[Adaptieve netwerkcontrole inschakelen](#)

[Quarantine DACL](#)

[Licentieprofiel voor Quarantine](#)

[machtigingsregels](#)

[Verifiëren](#)

[AnyConnect start ASA VPN-sessie](#)

[Toegang tot gebruikerspogingen](#)

[FireSight Correlatie Policy Sit](#)

[ISE voert quarantaine uit en zendt CoA toe](#)

[VPN-sessie is losgekoppeld](#)

[VPN-sessie met beperkte toegang \(quarantaine\)](#)

[Problemen oplossen](#)

[FireSight \(defensiecentrum\)](#)

[ISE](#)

[Bugs](#)

[Gerelateerde informatie](#)

[Gerelateerde Cisco Support Community-discussies](#)

## 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 beleidserver. 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.

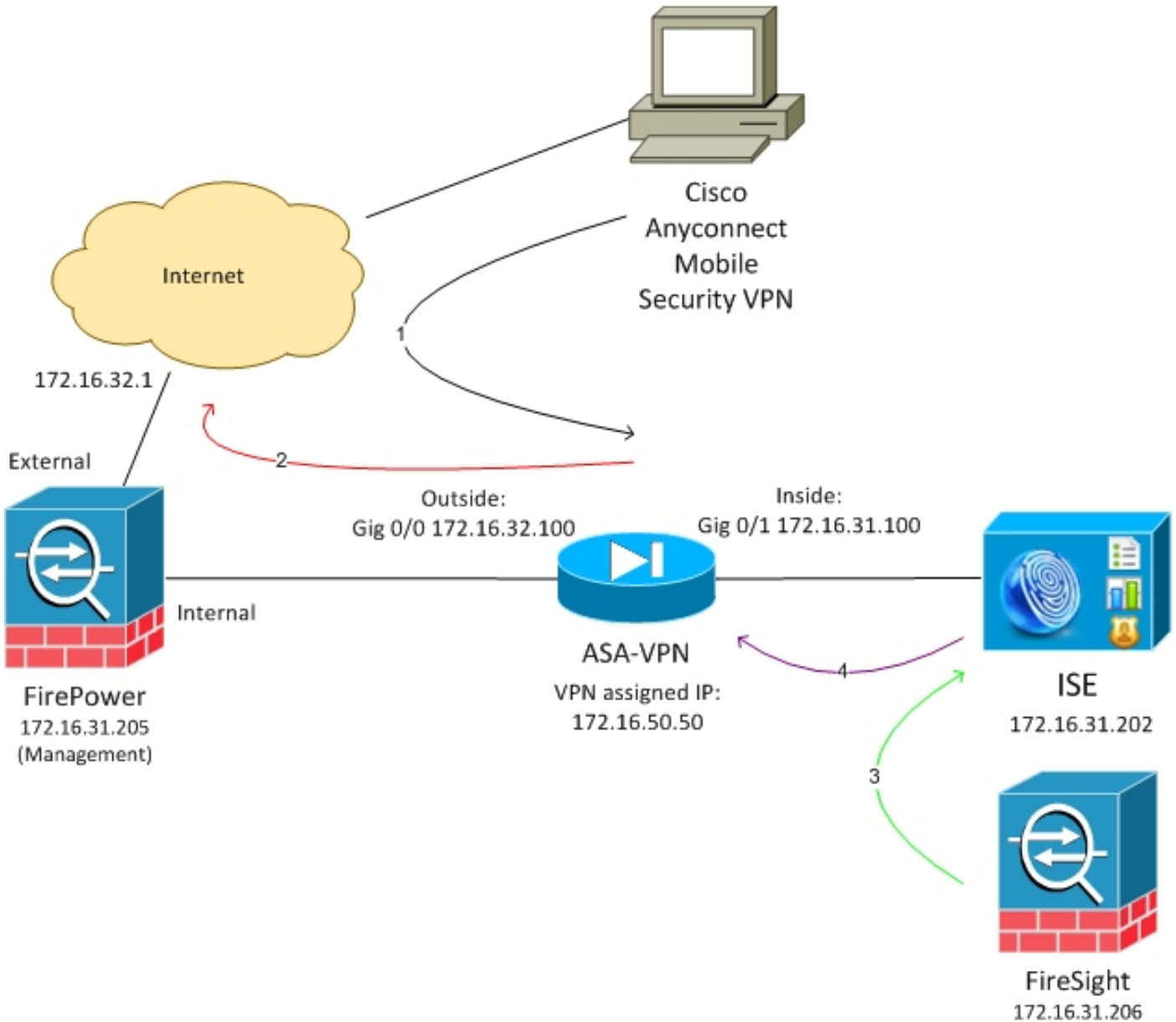
## Configureren

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.

## Netwerkdigram

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.

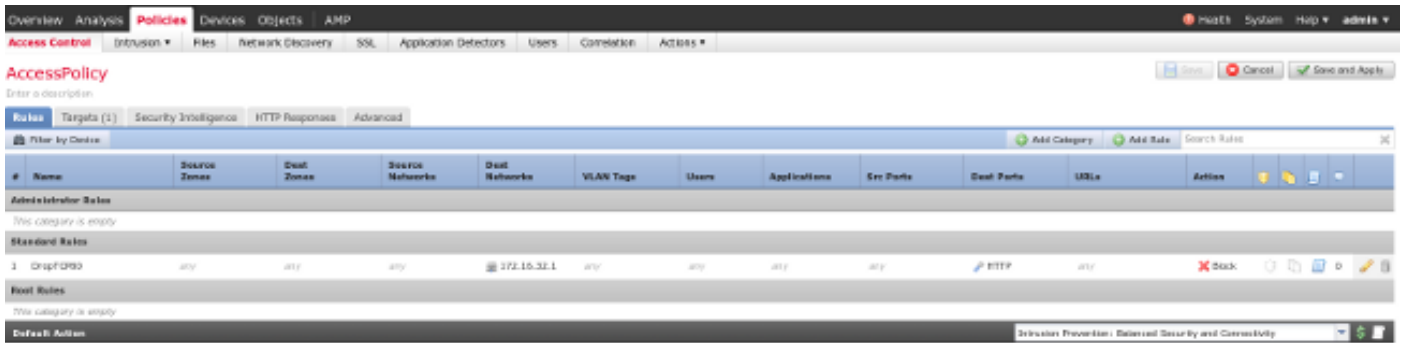
De VM heeft drie interfaces, één voor beheer en twee voor inline inspectie (intern/extern).

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

## FireSIGHT Management Center (Defense Center)

### Toegangsbeheerbeleid

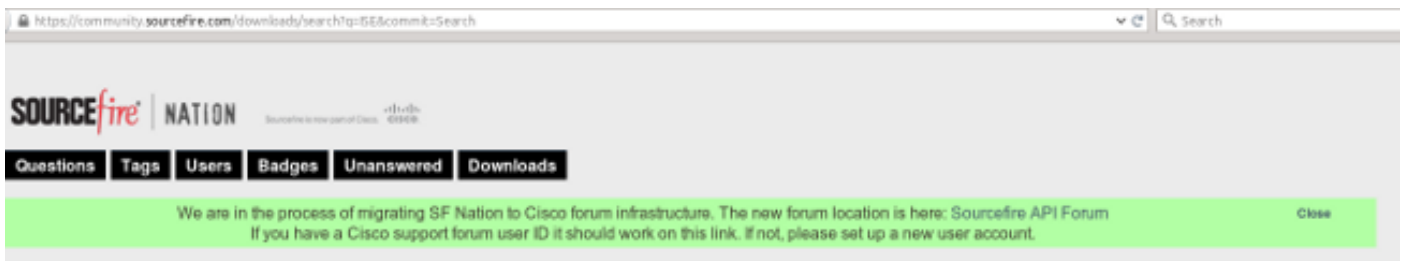
Nadat u de juiste licenties hebt geïnstalleerd en het FirePower-apparaat hebt toegevoegd, navigeer dan naar **Beleid > Toegangsbeheer** en maak u het toegangsbeleid dat wordt gebruikt om het HTTP-verkeer naar 172.16.32.1 te laten vallen:



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 Beta 1.3.19*:



### Sourcefire Downloads

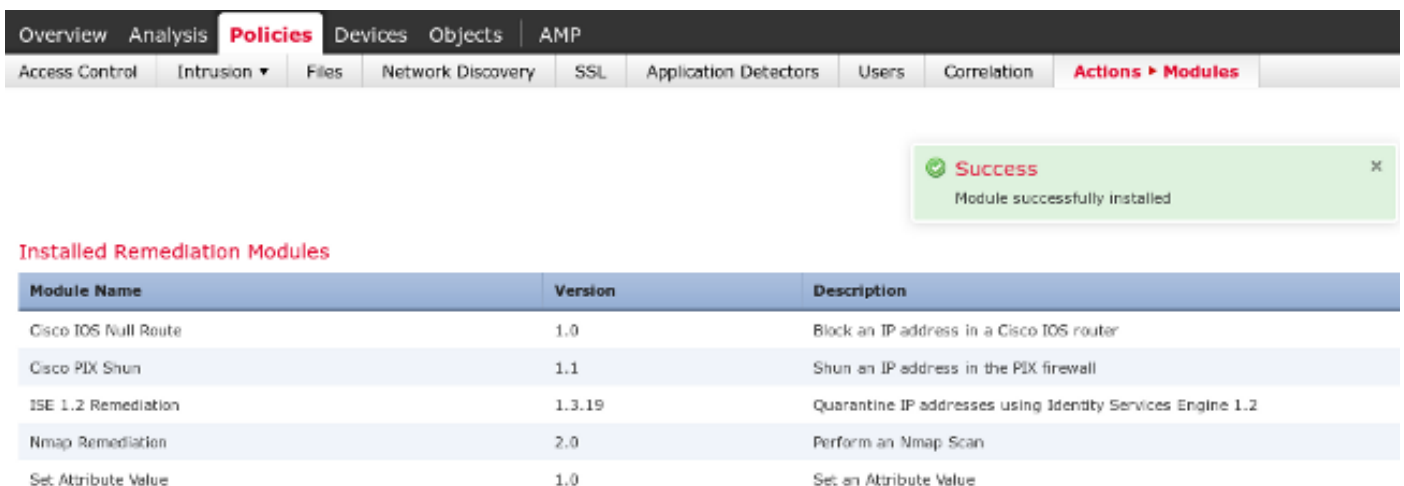
#### ISE 1.2 Remediation Beta 1.3.19

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.

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):

## Edit Instance

Instance Name	<input type="text" value="ise-instance"/>
Module	ISE 1.2 Remediation (v1.3.19)
Description	<div style="border: 1px solid #ccc; height: 100px;"></div>
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>	<div style="border: 1px solid #ccc; height: 100px;"></div>

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

## Configured Remediations

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

Correlatiebeleid

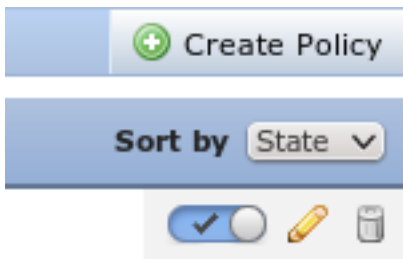
U moet nu een specifieke correlatieregel configureren. Deze regel wordt geactiveerd aan het begin van de verbinding die de eerder gevormde toegangscontroleregel (*DropTCP80*) aanpast. Om de regel te configureren volgt u **beleid > Correlatie > Regelbeheer**:

The screenshot shows the 'Rule Management' section of the Palo Alto Networks Policy Manager. The 'Rule Information' section is active, showing the rule name 'CorrelateTCP80Block', an empty description, and the 'Ungrouped' group. Below this, the 'Select the type of event for this rule' section is configured with the condition: '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.

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 **Oprissen** aan de rechterkant en voeg twee handelingen toe: **sanering voor sourceIP** (eerder geconfigureerd) en **syslog**:

The screenshot shows the 'Correlation Policy Information' section of the Palo Alto Networks Policy Manager. The policy name is 'CorrelateTCP80Block'. Below this, the 'Policy Rules' section is visible, showing a table with columns for Rule, Response, and Priority. A modal window titled 'Responses for CorrelateTCP80Block' is open, showing 'Assigned Responses' with 'San sourceIP' and 'Unassigned Responses'.

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:



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Device Portal Management'. A secondary navigation bar contains 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', and 'Backup & Restore'. The main content area is titled 'Settings' and lists various configuration options: Client Provisioning, Adaptive Network Control (highlighted), FIPS Mode, Alarm Settings, Posture, Profiling, and Protocols. To the right, the 'Adaptive Network Control' configuration page is shown, featuring a 'Service Status' dropdown menu set to 'Enabled' with a green checkmark, and 'Save' and 'Reset' buttons.

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

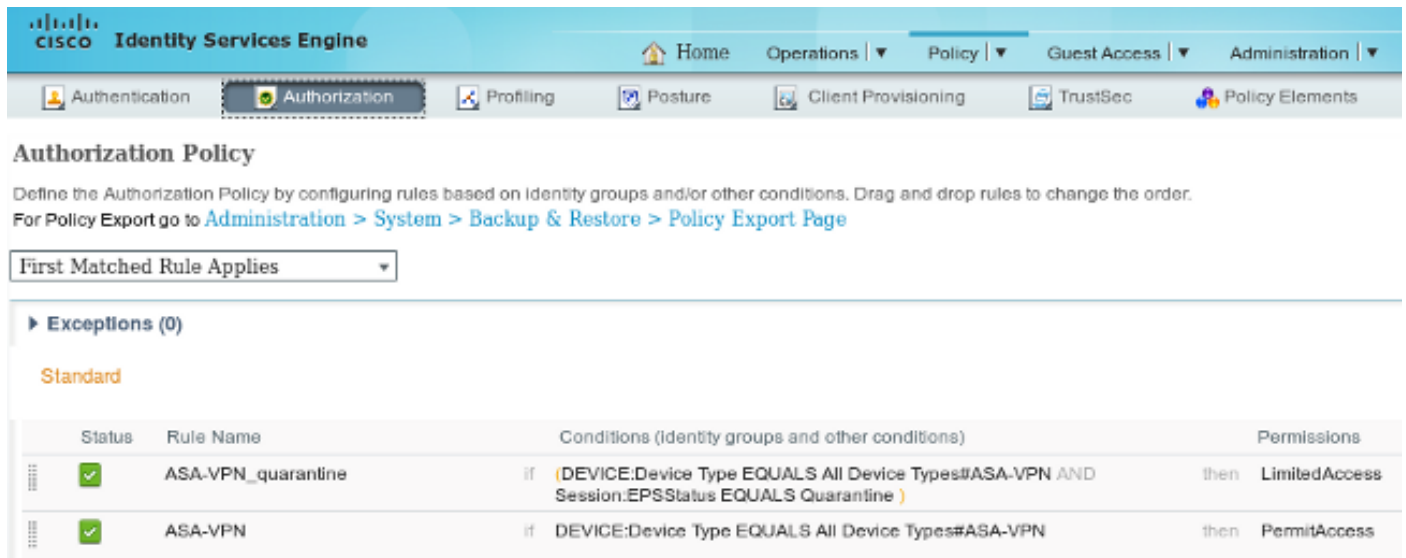
Navigeren in naar **beleid > Resultaten > Vergunning > Vergunningsprofiel** en maken een autorisatieprofiel met de nieuwe DACL:

The screenshot displays the Cisco Identity Services Engine (ISE) web interface for configuring an authorization profile. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Guest Access'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'TrustSec'. A secondary navigation bar contains 'Dictionaries', 'Conditions', and 'Results' (highlighted). The main content area is titled 'Results' and shows a search bar and a navigation tree on the left. The tree includes 'Authentication', 'Authorization' (expanded), 'Authorization Profiles', 'Downloadable ACLs', 'Inline Posture Node Profiles', 'Profiling', 'Posture', 'Client Provisioning', and 'TrustSec'. The 'Authorization Profiles > LimitedAccess' configuration page is shown, featuring an 'Authorization Profile' section with the following fields: '\* Name' (LimitedAccess), 'Description', '\* Access Type' (ACCESS\_ACCEPT), and 'Service Template' (unchecked). Below this, the 'Common Tasks' section includes a checked 'DACL Name' field with a dropdown menu set to 'DENY\_ALL\_QUARANTINE'.

## 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**:



**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)

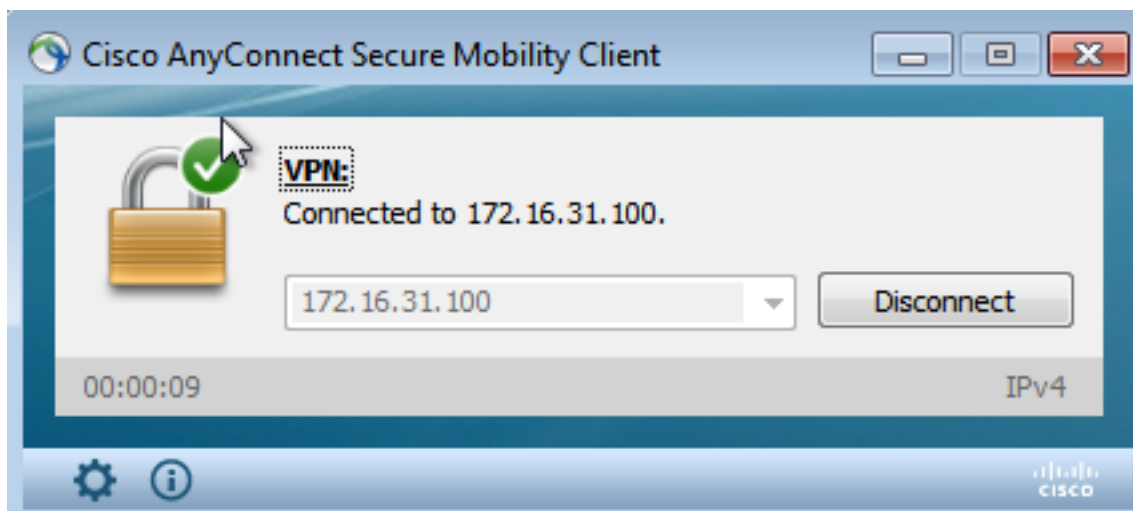
Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	ASA-VPN_quarantaine	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

## 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
```



```

120 172.16.31.206 172.16.31.202 TLSv1 588 Client Hello
121 172.16.31.202 172.16.31.206 TCP 66 https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165957 TSecr=97280105
122 172.16.31.202 172.16.31.206 TCP 2952 [TCP segment of a reassembled PDU]
123 172.16.31.202 172.16.31.206 TLSv1 681 Server Hello, Certificate, Certificate Request, Server Hello Done
124 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=518 Ack=1449 Win=17536 Len=0 TSval=97280106 TSecr=389165957
125 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=518 Ack=2897 Win=20480 Len=0 TSval=97280106 TSecr=389165957
126 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=518 Ack=3512 Win=23296 Len=0 TSval=97280106 TSecr=389165958
127 172.16.31.206 172.16.31.202 TLSv1 404 Certificate, Client Key Exchange, Change Cipher Spec, Finished
128 172.16.31.202 172.16.31.206 TLSv1 72 Change Cipher Spec
129 172.16.31.202 172.16.31.206 TLSv1 119 Finished
130 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=856 Ack=3571 Win=23296 Len=0 TSval=97280107 TSecr=389165962
131 172.16.31.206 172.16.31.202 HTTP 255 GET /ise/eps/QuarantineByIP/172.16.50.50 HTTP/1.1
132 172.16.31.202 172.16.31.206 TCP 66 https > 48046 [ACK] Seq=3571 Ack=1085 Win=17792 Len=0 TSval=389166020 TSecr=97280111
135 172.16.31.202 172.16.31.206 HTTP/XML 423 HTTP/1.1 200 OK

```

Secure Sockets Layer

- TLSv1 Record Layer: Application Data Protocol: http
  - Content Type: Application Data (23)
  - Version: TLS 1.0 [0x0301]
  - Length: 224
  - Encrypted Application Data: e1de29faa3cef63e96cc97e0e9f9fdd21c9441cd117cb7e9...
- HyperText Transfer Protocol
  - GET /ise/eps/QuarantineByIP/172.16.50.50 HTTP/1.1\r\n
  - TE: deflate,gzip;q=0.3\r\n
  - Connection: TE, close\r\n
  - Authorization: Basic YWRtaW46S3Jha293MTIz\r\n
  - Host: 172.16.31.202\r\n
  - User-Agent: Libwww-perl/6.05\r\n
  - \r\n
  - [Full request LRI: http://172.16.31.202/ise/eps/QuarantineByIP/172.16.50.50]

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 *prtt-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

```



wordt de ISE *ASA-VPN\_quarantaineregel* geraakt, die de beperkte netwerktoegang verleent:

Time	Status	Device	Repeat Count	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-05-24 10:51:40...	🟡		0	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:DA:EF:AD			Dynamic Authorization succeeded
2015-05-24 10:40:01...	🟢			cisco	192.168.10.21	Default -> ASA-VPN	PermitAccess	Authentication succeeded

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  : ac10206400027000555c02e8
Security Grp  : none
```

```
.....
DTLS-Tunnel:
<some output omitted 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 (*pvt-management.log* en *pvt-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 quarantainezoek:

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

## 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

- 
- [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](#)