Konfigurieren von Problembehebungsservices mit ISE- und FirePower-Integration

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie das Sanierungsmodul auf einer Cisco FireSight-Appliance verwenden, um Angriffe zu erkennen und den Angreifer mithilfe der Cisco Identity Service Engine (ISE) als Richtlinienserver automatisch zu beseitigen. Im vorliegenden Beispiel wird die Methode beschrieben, die zur Behebung von Remote-VPN-Benutzern verwendet wird, die sich über die ISE authentifizieren. Sie kann jedoch auch für 802.1x/MAB/WebAuth-Benutzer (kabelgebunden oder drahtlos) verwendet werden.

Hinweis: Das Sanierungsmodul, auf das in diesem Dokument verwiesen wird, wird von Cisco offiziell nicht unterstützt. Sie wird auf einem Community-Portal gemeinsam genutzt und kann von jedem Benutzer verwendet werden. In Version 5.4 und höher ist auch ein neues Sanierungsmodul verfügbar, das auf dem *pxGrid*-Protokoll basiert. Dieses Modul wird in Version 6.0 nicht unterstützt, soll aber in zukünftigen Versionen unterstützt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- VPN-Konfiguration der Cisco Adaptive Security Appliance (ASA)
- Konfiguration des Cisco AnyConnect Secure Mobility Client
- Grundkonfiguration von Cisco FireSight
- Grundkonfiguration von Cisco FirePower
- Cisco ISE-Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco ASA Version 9.3 oder höher
- Cisco ISE Software Version 1.3 und höher
- Cisco AnyConnect Secure Mobility Client Version 3.0 und höher
- Cisco FireSight Management Center Version 5.4
- Cisco FirePower Version 5.4 (virtuelles System (VM))

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

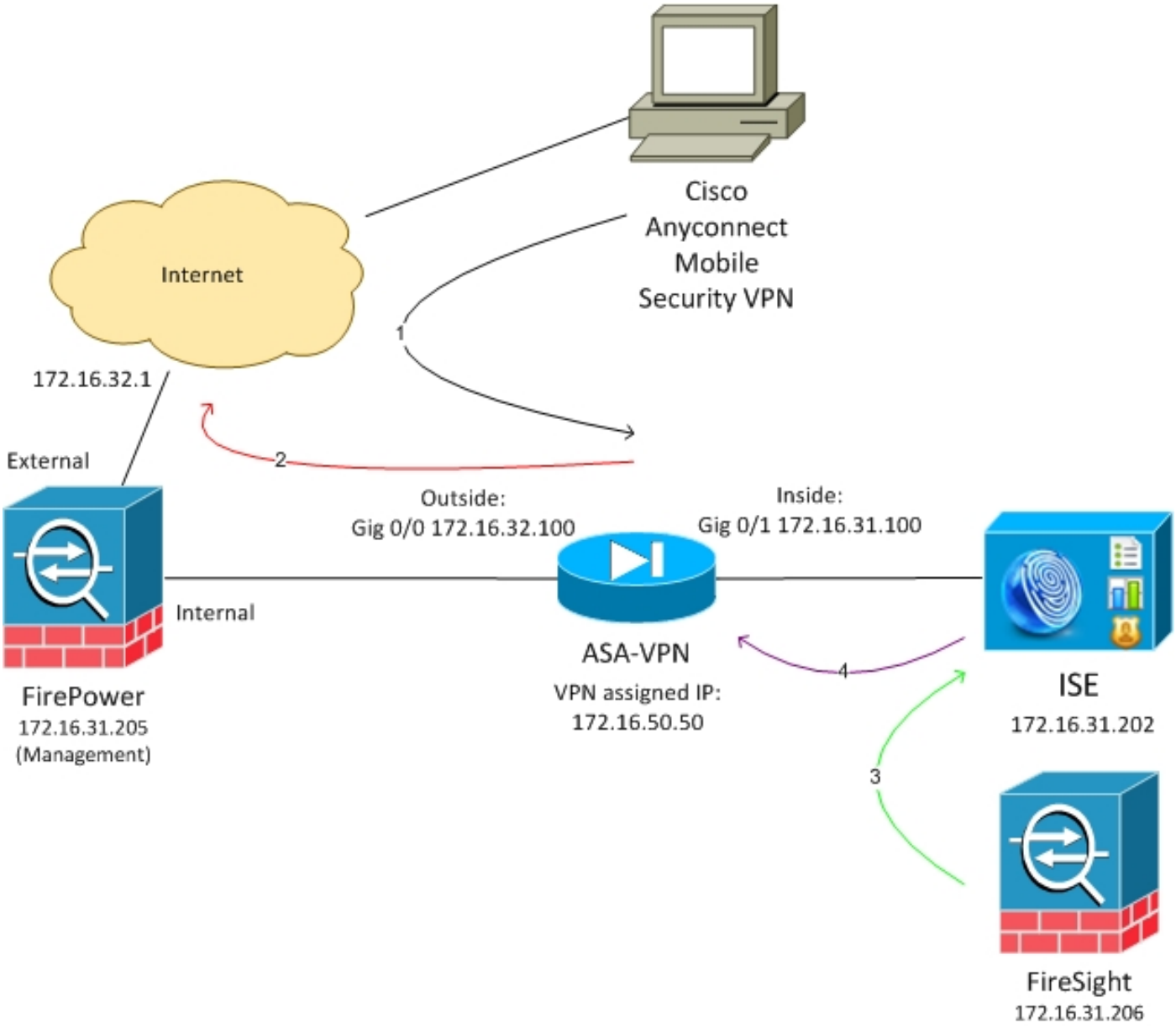
Konfigurieren

Verwenden Sie die Informationen in diesem Abschnitt, um Ihr System zu konfigurieren.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Das in diesem Dokument beschriebene Beispiel verwendet die folgende Netzwerkeinrichtung:



Der folgende Ablauf für diese Netzwerkeinrichtung:

1. Der Benutzer initiiert eine Remote-VPN-Sitzung mit der ASA (über Cisco AnyConnect Secure Mobility Version 4.0).

2. Der Benutzer versucht, auf *http://172.16.32.1* zuzugreifen. (Der Datenverkehr wird über FirePower übertragen, das auf dem virtuellen System installiert und von FireSight verwaltet wird.)

3. FirePower wird so konfiguriert, dass er (inline) den spezifischen Datenverkehr (Zugriffsrichtlinien) blockiert, aber auch eine Korrelationsrichtlinie, die ausgelöst wird. Infolgedessen initiiert es die ISE-Problembehebung über die REST Application Programming Interface (API) (die *QuarantineByIP*-Methode).

4. Sobald die ISE den REST-API-Anruf empfängt, sucht sie nach der Sitzung und sendet einen RADIUS Change of Authorization (CoA) an die ASA, die diese Sitzung beendet.

5. Die ASA trennt den VPN-Benutzer. Da AnyConnect mit *ständig verfügbarem* VPN-Zugriff konfiguriert ist, wird eine neue Sitzung eingerichtet. Diesmal wird jedoch eine andere ISE-Autorisierungsregel zugeordnet (für isolierte Hosts) und der Netzwerkzugriff beschränkt. Zum gegenwärtigen Zeitpunkt spielt es keine Rolle, wie der Benutzer eine Verbindung zum Netzwerk herstellt und sich authentifiziert. Solange die ISE für die Authentifizierung und Autorisierung verwendet wird, hat der Benutzer aufgrund der Quarantäne nur eingeschränkten Netzwerkzugriff.

Wie bereits erwähnt, funktioniert dieses Szenario für jede Art von authentifizierter Sitzung (VPN, kabelgebundenes 802.1x/MAB/Webauth, Wireless 802.1x/MAB/Webauth), solange die ISE für die Authentifizierung verwendet wird und das Netzwerkzugriffsgerät das RADIUS CoA (alle modernen Cisco Geräte) unterstützt.

> **Tipp**: Um den Benutzer aus der Quarantäne zu verschieben, können Sie die ISE-GUI verwenden. Künftige Versionen des Sanierungsmoduls können dieses ebenfalls unterstützen.

Feuerkraft

> **Hinweis**: Für das in diesem Dokument beschriebene Beispiel wird eine VM-Appliance verwendet. Nur die Erstkonfiguration wird über die CLI durchgeführt. Alle Richtlinien werden vom Cisco Defense Center konfiguriert. Weitere Informationen finden Sie im Abschnitt Zugehörige Informationen dieses Dokuments.

Das virtuelle System verfügt über drei Schnittstellen: eine für die Verwaltung und zwei für die Inline-Prüfung (intern/extern).

Der gesamte Datenverkehr der VPN-Benutzer wird über FirePower übertragen.

FireSight Management Center (Defense Center)

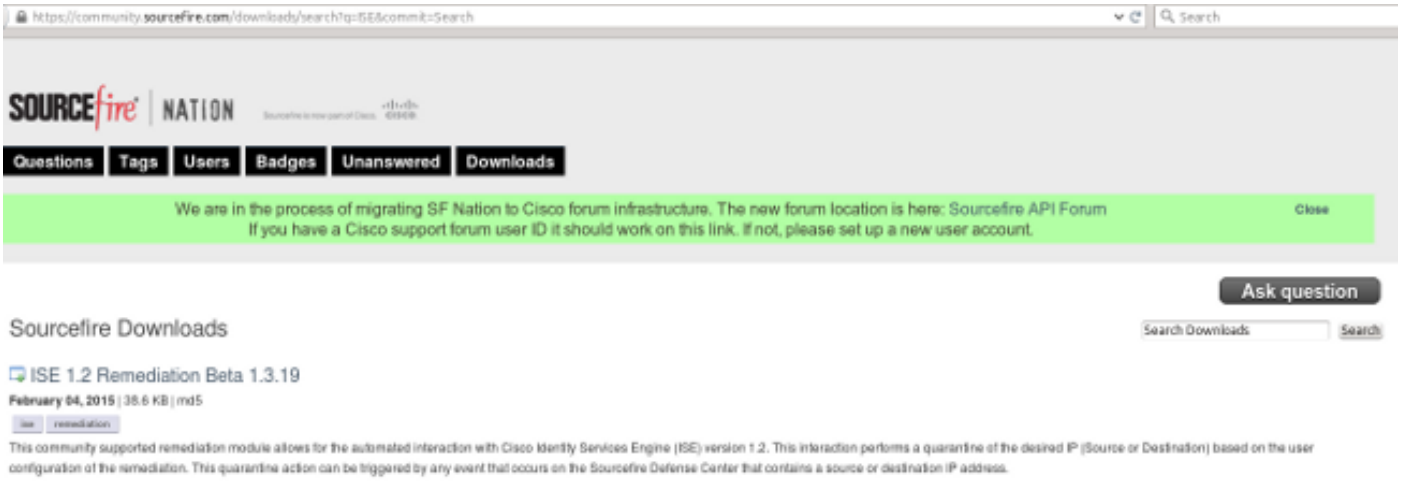
Zugriffskontrollrichtlinie

Nachdem Sie die richtigen Lizenzen installiert und das FirePower-Gerät hinzugefügt haben, navigieren Sie zu **Policies > Access Control (Richtlinien > Zugriffskontrolle),** und erstellen Sie die Zugriffsrichtlinie, die verwendet wird, um den HTTP-Datenverkehr auf 172.16.32.1 zu verwerfen:

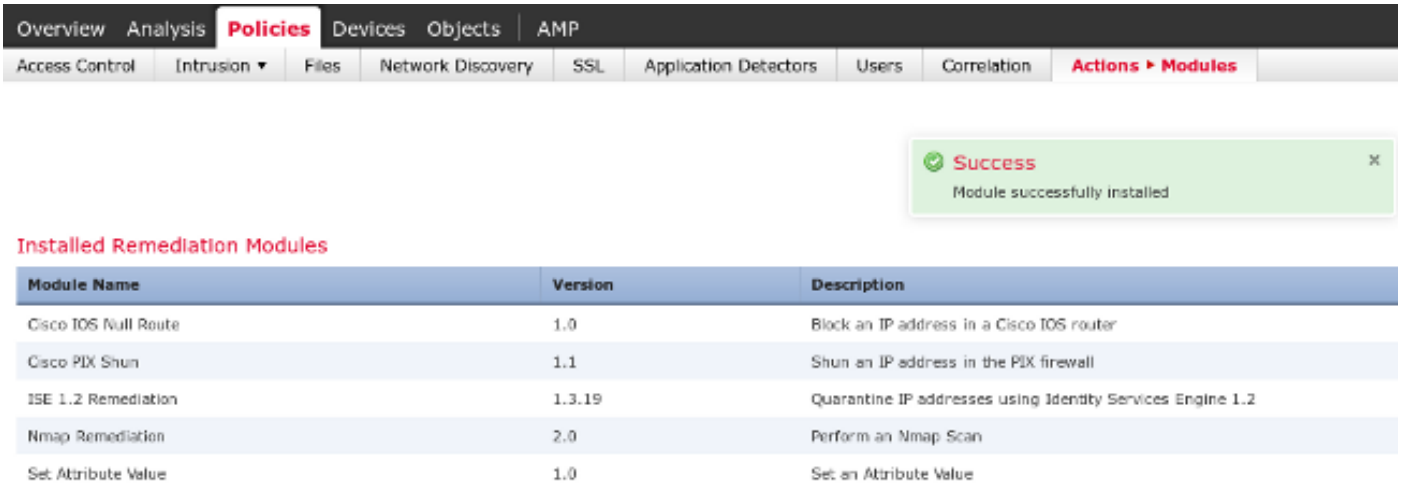
Alle anderen Zugriffe werden akzeptiert.

ISE-Sanierungsmodul

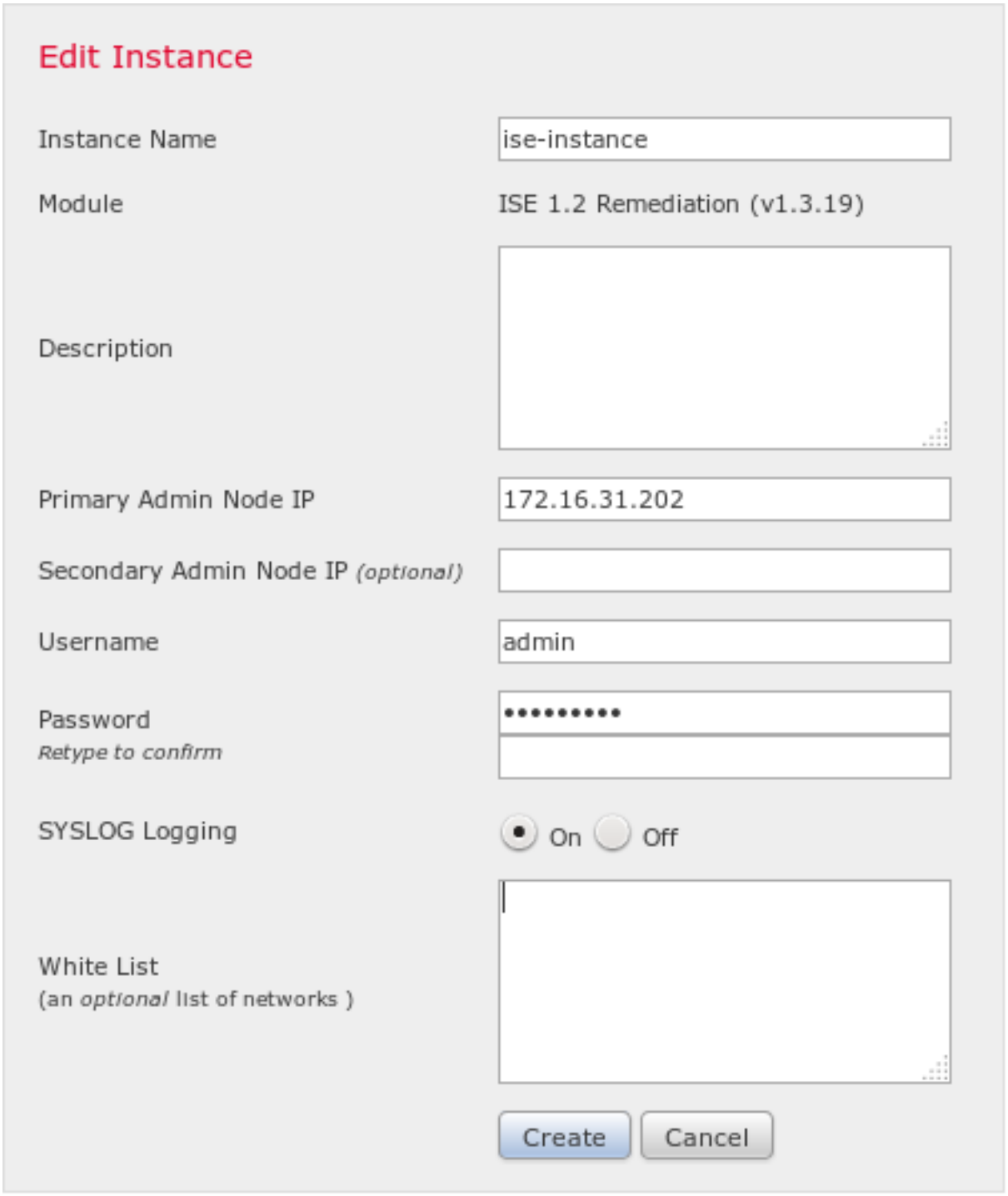
Die aktuelle Version des ISE-Moduls, das auf dem Community-Portal gemeinsam genutzt wird, ist *ISE 1.2 Remediation Beta 1.3.19*:



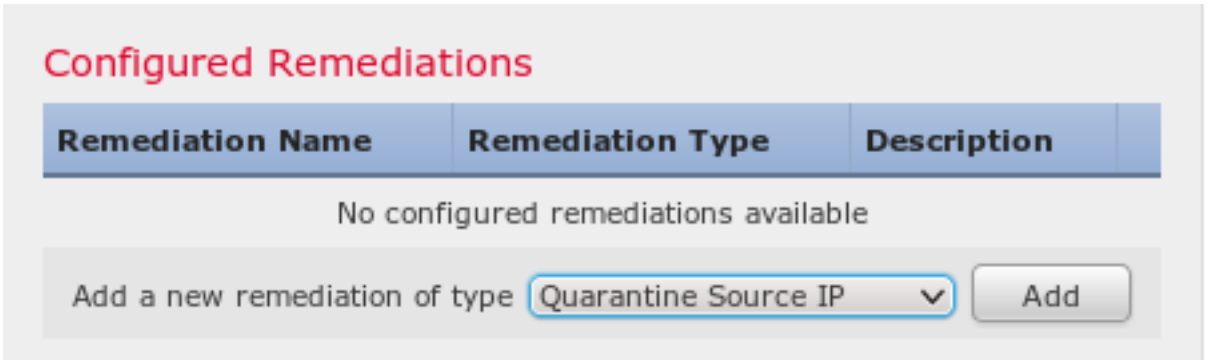
Navigieren Sie zu **Richtlinien > Aktionen > Korrekturen > Module,** und installieren Sie die Datei:



Dann sollte die richtige Instanz erstellt werden. Navigieren Sie zu **Policies > Actions > Remediations > Instances**, und geben Sie die IP-Adresse des Policy Administration Node (PAN) sowie die für die REST-API erforderlichen ISE-Administratoranmeldeinformationen an (ein separater Benutzer mit der *ERS Admin*-Rolle wird empfohlen):

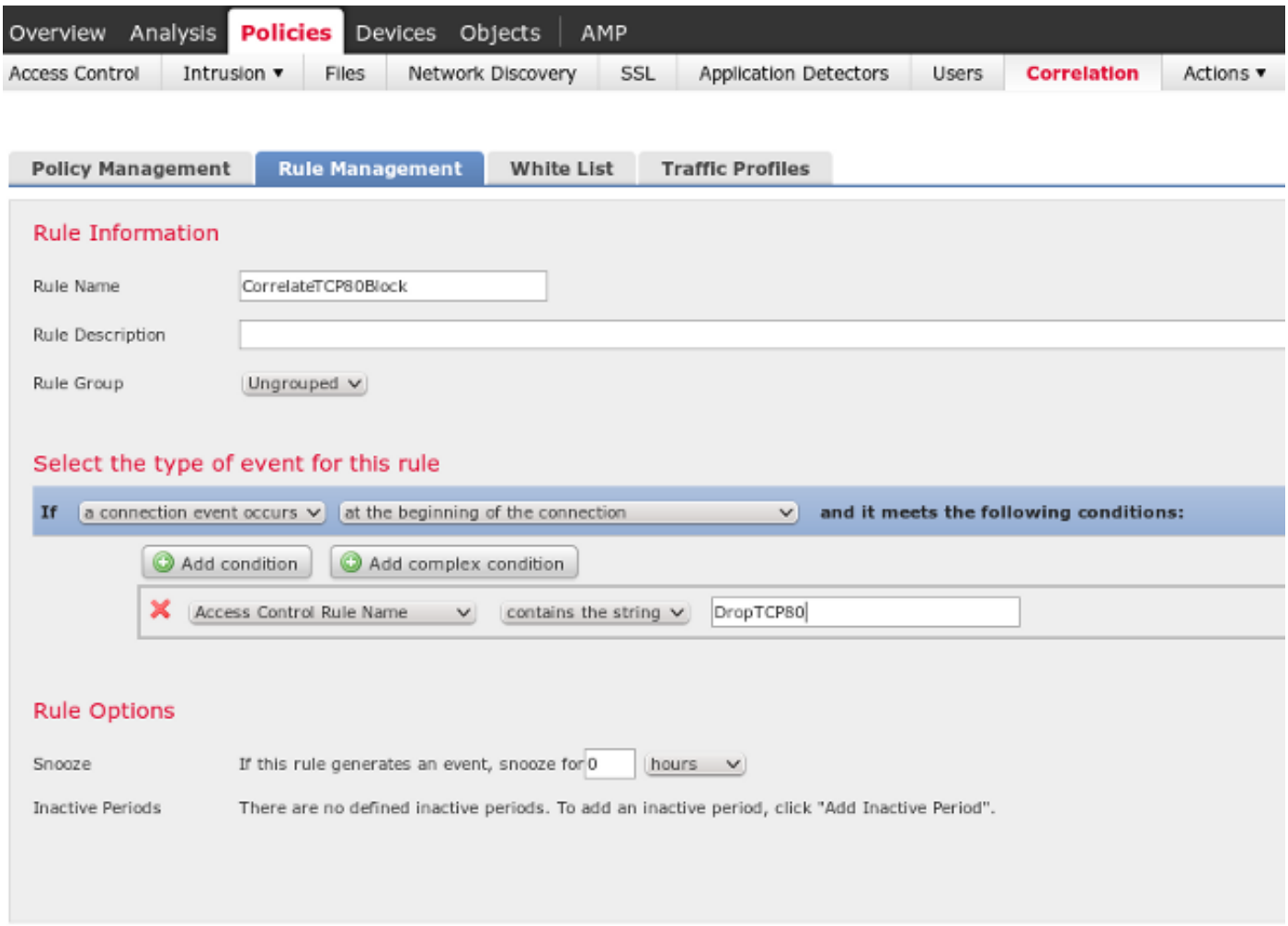


Die Quell-IP-Adresse (Angreifer) sollte auch zur Behebung verwendet werden:

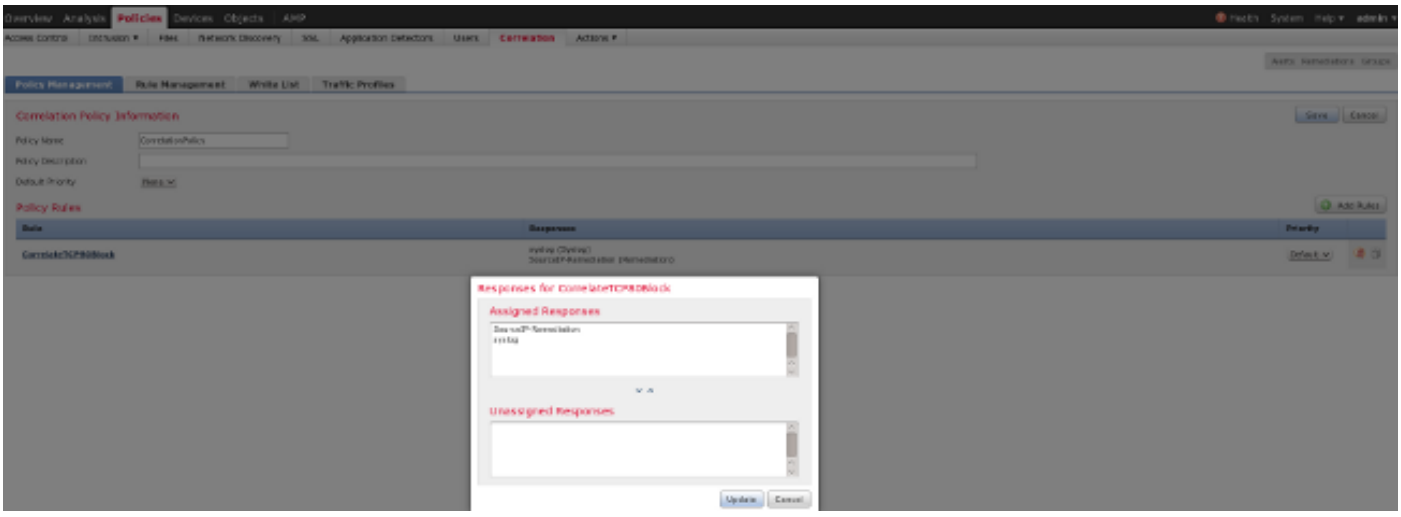


Korrelationsrichtlinie

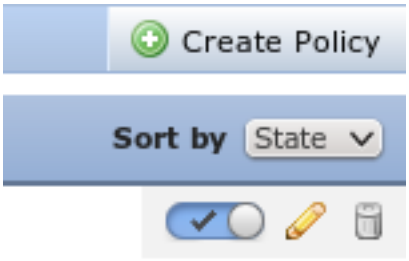
Sie müssen jetzt eine bestimmte Korrelationsregel konfigurieren. Diese Regel wird zu Beginn der Verbindung ausgelöst, die mit der zuvor konfigurierten Zugriffskontrollregel (*DropTCP80*) übereinstimmt. Um die Regel zu konfigurieren, navigieren Sie zu **Richtlinien > Korrelation > Regelverwaltung**:



Diese Regel wird in der Korrelationsrichtlinie verwendet. Navigieren Sie zu **Richtlinien > Korrelation > Richtlinienverwaltung**, um eine neue Richtlinie zu erstellen, und fügen Sie dann die konfigurierte Regel hinzu. Klicken Sie rechts **auf Beheben**, und fügen Sie zwei Aktionen hinzu: **Problembehebung für SourceIP** (früher konfiguriert) und **Syslog**:



Stellen Sie sicher, dass Sie die Korrelationsrichtlinie aktivieren:



ASA

Eine ASA, die als VPN-Gateway fungiert, wird konfiguriert, um die ISE für die Authentifizierung zu verwenden. Außerdem müssen Accounting und RADIUS CoA aktiviert werden:

```
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
```

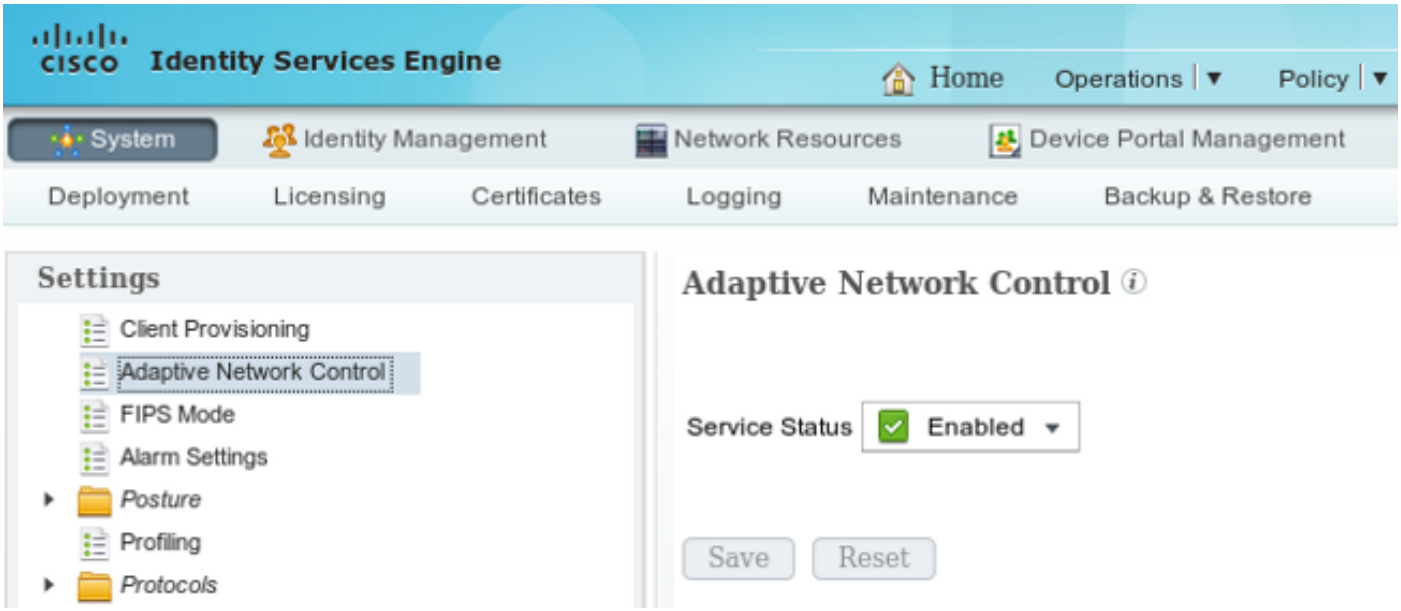
ISE

Netzwerkzugriffsgerät (Network Access Device, NAD) konfigurieren

Navigieren Sie zu **Administration > Network Devices**, und fügen Sie die ASA hinzu, die als RADIUS-Client fungiert.

Adaptive Netzwerkkontrolle aktivieren

Navigieren Sie zu **Administration > System > Settings > Adaptive Network Control**, um die Quarantäne-API und -Funktionalität zu aktivieren:



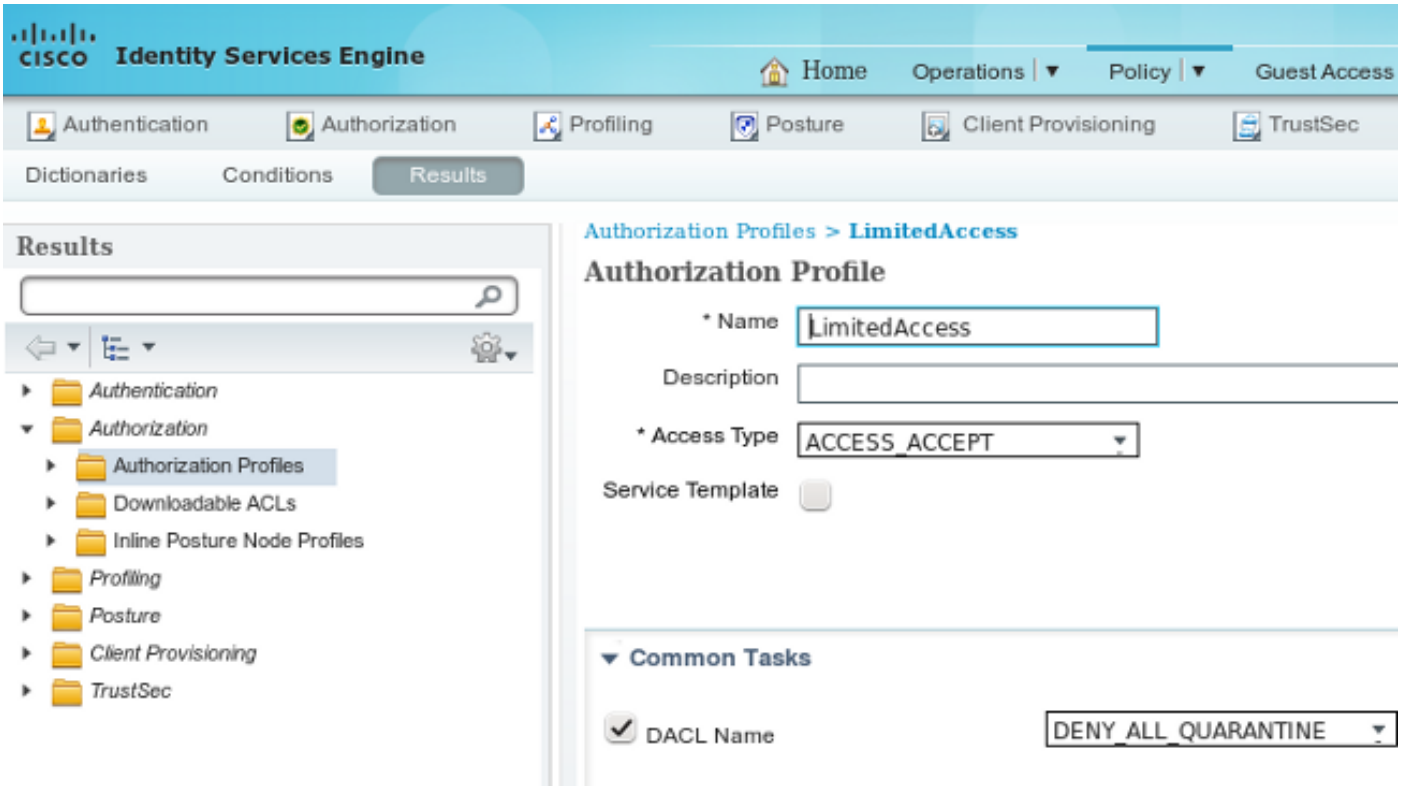
Hinweis: In Version 1.3 und früher wird diese Funktion als *Endpoint Protection Service* bezeichnet.

DACL-Quarantäne

Um eine herunterladbare Zugriffskontrollliste (DACL) für die isolierten Hosts zu erstellen, navigieren Sie zu **Richtlinien > Ergebnisse > Autorisierung > Herunterladbare ACL**.

Autorisierungsprofil für Quarantäne

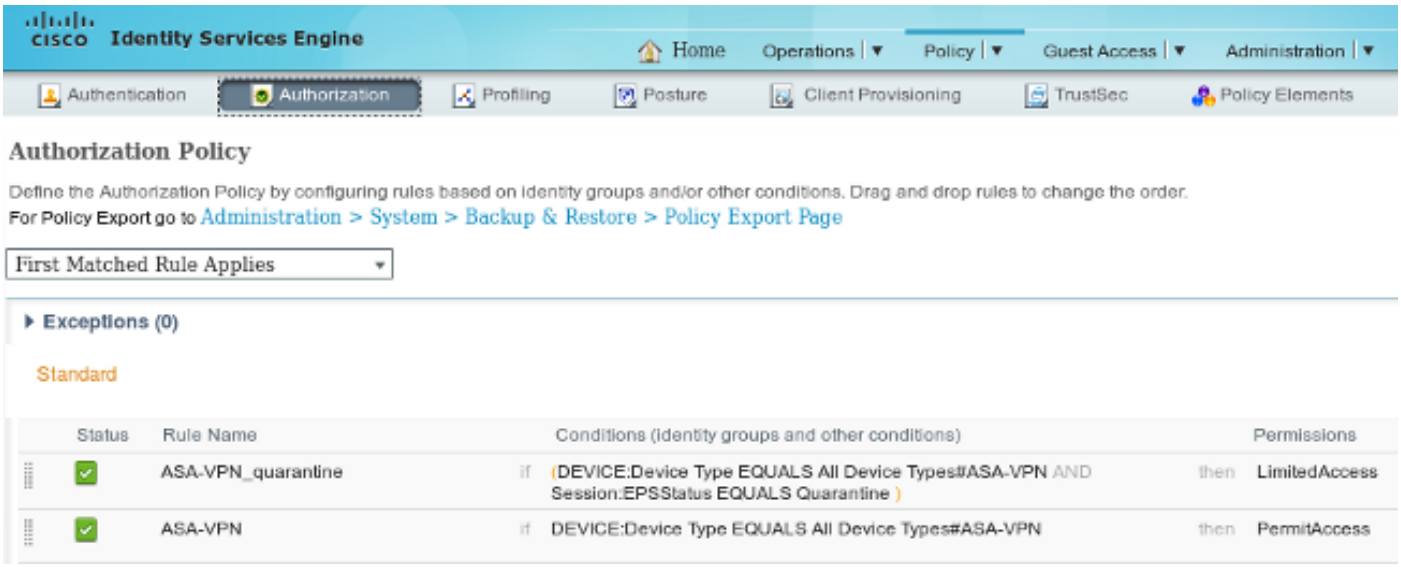
Navigieren Sie zu **Richtlinien > Ergebnisse > Autorisierung > Autorisierungsprofil**, und erstellen Sie ein Autorisierungsprofil mit der neuen DACL:



Autorisierungsregeln

Sie müssen zwei Autorisierungsregeln erstellen. Die erste Regel (ASA-VPN) bietet vollständigen Zugriff für alle auf der ASA terminierten VPN-Sitzungen. Die Regel *ASA-VPN_Quarantine* wird für die erneut authentifizierte VPN-Sitzung aufgerufen, wenn der Host bereits unter Quarantäne steht (der Netzwerkzugriff ist beschränkt).

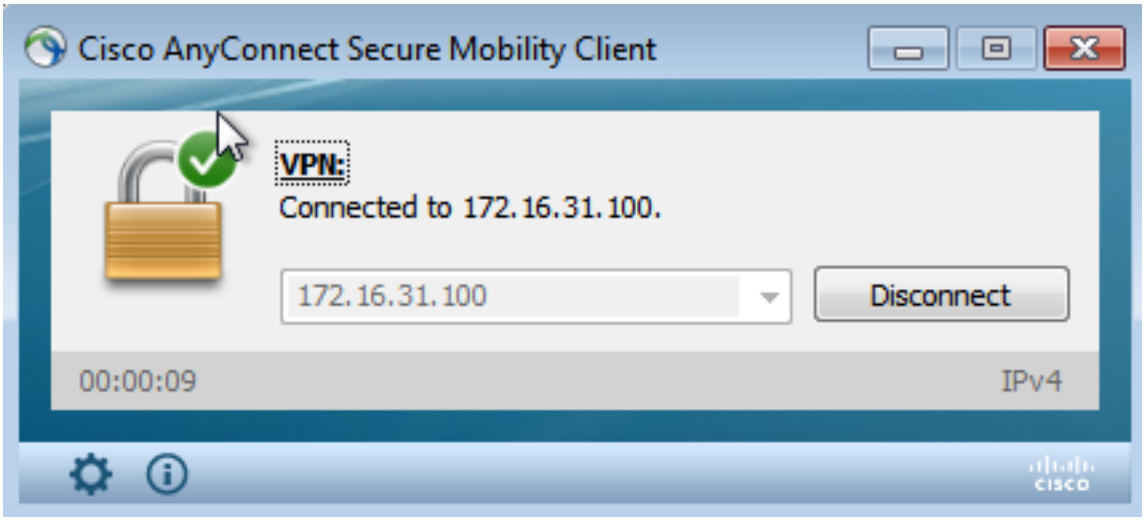
Navigieren Sie zum Erstellen dieser Regeln zu **Richtlinien > Autorisierung**:



Überprüfen

Verwenden Sie die Informationen in diesem Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

AnyConnect initiiert ASA VPN-Sitzung



Die ASA erstellt die Sitzung ohne DACL (vollständiger Netzwerkzugriff):

```
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>
```

Zugriff auf Benutzerversuche

Sobald der Benutzer versucht, auf http://172.16.32.1 zuzugreifen, wird die Zugriffsrichtlinie aufgerufen, der entsprechende Datenverkehr wird inline blockiert, und die Syslog-Meldung wird von der IP-Adresse der FirePower-Verwaltung gesendet:

```
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,
```

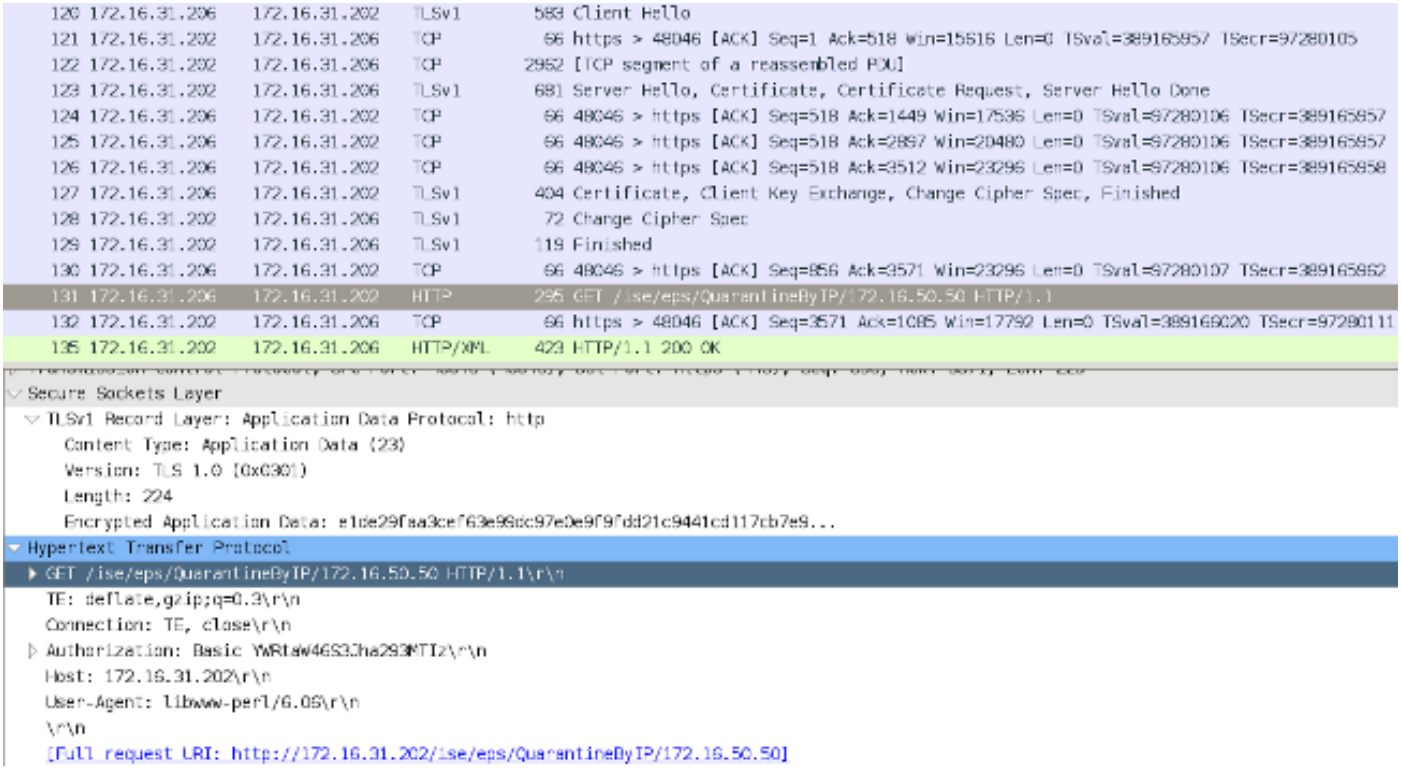
```
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: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

Die FireSight Management (Defense Center) Correlation-Richtlinie ist betroffen. Diese wird durch die Syslog-Meldung gemeldet, die vom Defense Center gesendet wird:

```
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 dieser Phase verwendet Defense Center den REST API-Aufruf (Quarantäne) für die ISE, eine HTTPS-Sitzung, die in Wireshark (mit dem SSL-Plug-in (Secure Sockets Layer) und dem privaten Schlüssel des PAN-Administrationszertifikats) entschlüsselt werden kann:



In GET-Anforderung für die IP-Adresse des Angreifers wird übergeben (172.16.50.50), und dieser Host wird von der ISE unter Quarantäne gestellt.

Navigieren Sie zu **Analyse > Korrelation > Status**, um die erfolgreiche Problembehebung zu bestätigen:

ISE führt Quarantäne aus und sendet CoA

In dieser Phase benachrichtigt die ISE *prrt-management.log*, dass der CoA gesendet werden soll:

```
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=ac1020640002100055 5b9d36
Calling-Station-ID=192.168.10.21
Acct-Terminate-Cause=Admin Reset
```

Die Common Language Runtime (prt-server.log) sendet die CoA-*Abschlussmeldung* an die NAD, die die Sitzung (ASA) beendet:

```
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=ac1020640002100055 5b9d36],
RadiusClientHandler.cpp:47
```

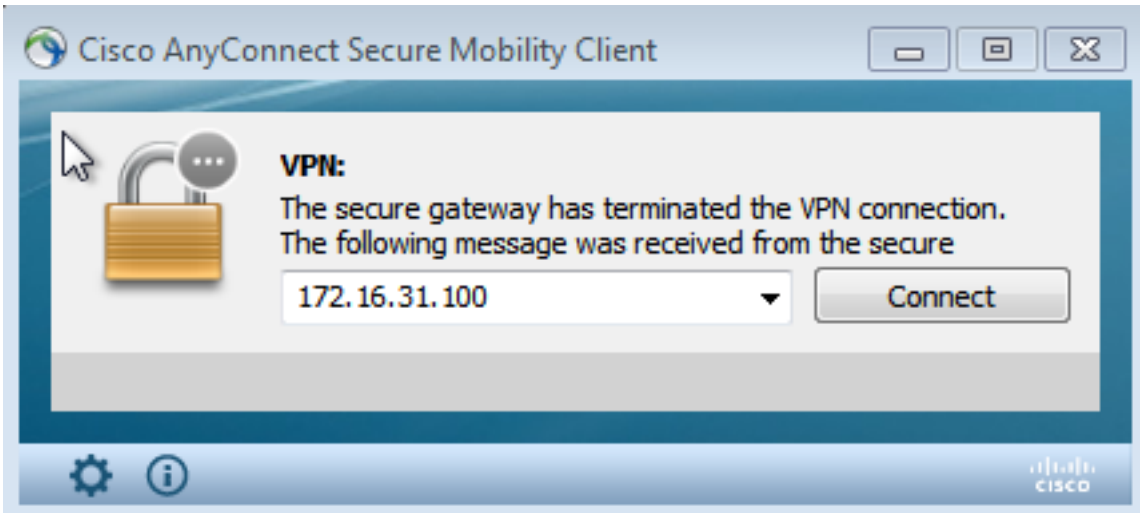
Die *ise.psc* sendet eine ähnliche Benachrichtigung:

```
INFO   [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -:::::- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac1020640002100055 5b9d36 UserName=cisco PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
```

Wenn Sie zu **Operations > Authentication (Vorgänge > Authentifizierung)** navigieren, sollte die *dynamische Autorisierung erfolgreich* angezeigt werden.

VPN-Sitzung wird getrennt

Der Endbenutzer sendet eine Benachrichtigung, um anzuzeigen, dass die Sitzung getrennt ist (bei 802.1x/MAB/kabelgebundenem/Wireless-Gastzugriff ist dieser Prozess transparent):

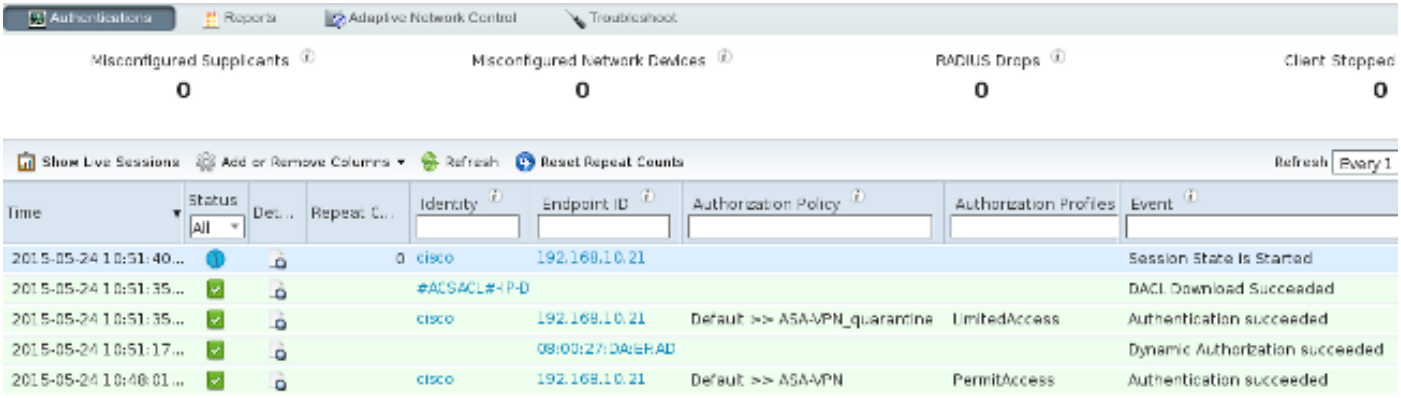


Details aus den Cisco AnyConnect-Protokollen werden angezeigt:

```
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-Sitzung mit begrenztem Zugriff (Quarantäne)

Da *stets verfügbares VPN* konfiguriert ist, wird die neue Sitzung sofort erstellt. Diesmal wird die ISE *ASA-VPN_Quarantine*-Regel getroffen, die den eingeschränkten Netzwerkzugriff bereitstellt:



Hinweis: Die DACL wird in einer separaten RADIUS-Anforderung heruntergeladen.

Eine Sitzung mit eingeschränktem Zugriff kann auf der ASA mit dem Befehl **show vpn-sessiondb detail anyconnect** CLI verifiziert werden:

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung in Ihrer Konfiguration verwenden können.

FireSight (Defense Center)

Das ISE-Sanierungsskript befindet sich an diesem Ort:

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

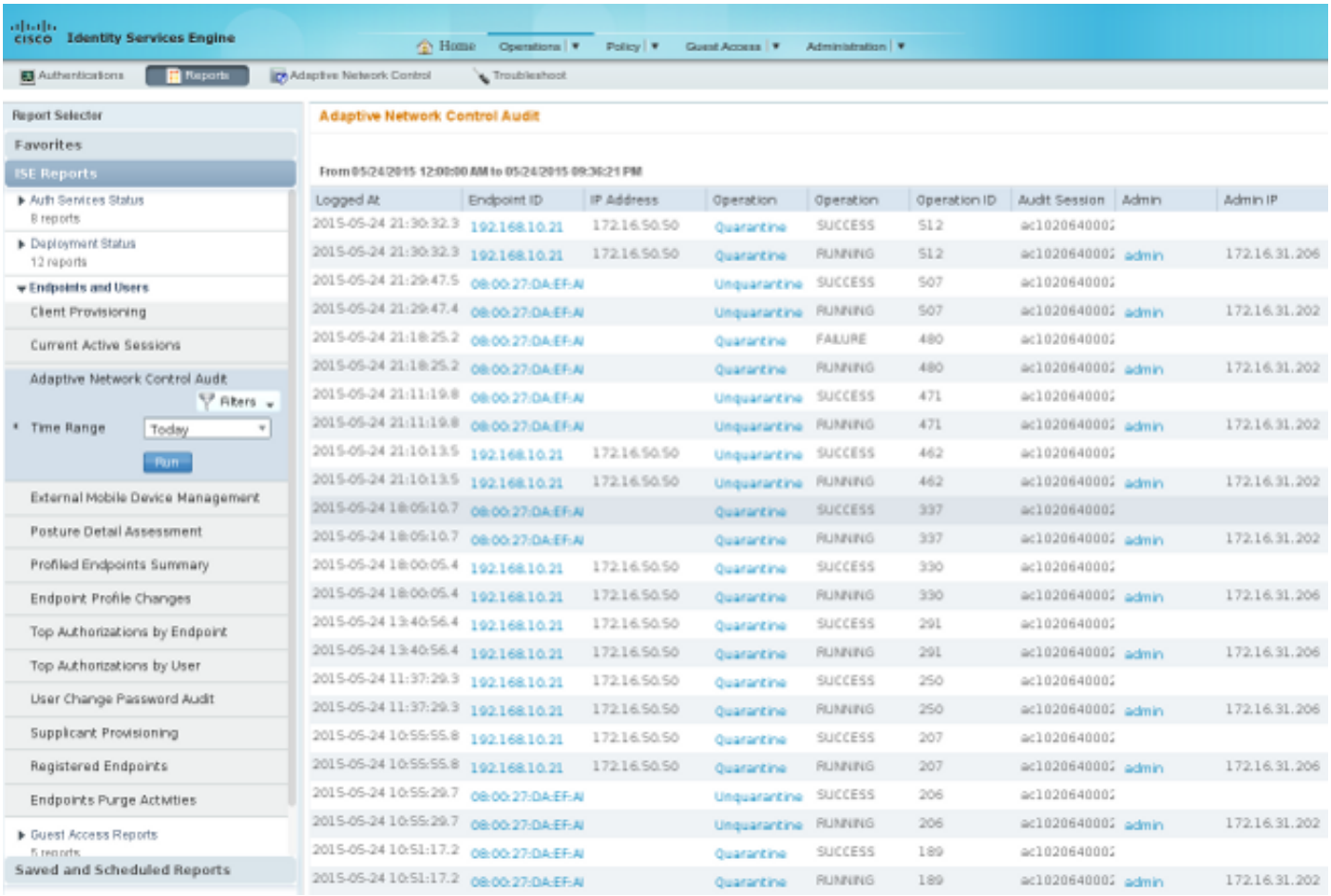
Dies ist ein einfaches *Perl*-Skript, das das Standard-SF-Protokollierungs-Subsystem verwendet. Sobald die Sanierung durchgeführt wurde, können Sie die Ergebnisse über die */var/log/messages* bestätigen:

```
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 ist wichtig, dass Sie den Adaptive Network Control Service auf der ISE aktivieren. Um die detaillierten Protokolle in einem Laufzeitprozess (*prt-management.log* und *port-server.log*) anzuzeigen, müssen Sie die DEBUG-Ebene für Runtime-AAA aktivieren. Navigieren Sie zu **Administration > System > Logging > Debug Log Configuration**, um das Debuggen zu aktivieren.

Sie können auch zu **Operations > Reports > Endpoint and Users > Adaptive Network Control Audit** (**Betrieb > Berichte > Endpunkt und Benutzer > Adaptive Network Control Audit**) navigieren, um die Informationen für jeden Versuch und das Ergebnis einer Quarantäneanforderung anzuzeigen:



Bug

Unter Cisco Bug ID CSCuu41058 (ISE 1.4 Endpoint Quarantine-Inkonsistenz und VPN-Ausfall) finden Sie Informationen zu einem ISE-Fehler, der mit VPN-Sitzungsfehlern zusammenhängt (802.1x/MAB funktioniert einwandfrei).

Zugehörige Informationen

- Konfigurieren der WSA-Integration mit der ISE für TrustSec-basierte Services
- ISE Version 1.3 pxGrid-Integration mit IPS pxLog-Anwendung
- Administratoranleitung für Cisco Identity Services Engine, Version 1.4 - Einrichten einer adaptiven Netzwerkkontrolle
- Cisco Identity Services Engine-API-Referenzhandbuch, Version 1.2 - Einführung in die externe RESTful Services-API
- Cisco Identity Services Engine API-Referenzhandbuch, Version 1.2 - Einführung in die Monitoring-REST-APIs
- Administratoranleitung für Cisco Identity Services Engine, Version 1.3

- Technischer Support und Dokumentation - Cisco Systems