

ISE- und FirePower-Integration - Beispiel für einen Problembhebungsservice

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Feuerkraft](#)

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

[Zugriffskontrollrichtlinie](#)

[ISE-Sanierungsmodul](#)

[Korrelationsrichtlinie](#)

[ASA](#)

[ISE](#)

[Netzwerkzugriffsgert \(Network Access Device, NAD\) konfigurieren](#)

[Adaptive Netzwerkkontrolle aktivieren](#)

[DACL-Quarantäne](#)

[Autorisierungsprofil für Quarantäne](#)

[Autorisierungsregeln](#)

[Überprüfen](#)

[AnyConnect initiiert ASA VPN-Sitzung](#)

[Zugriff auf Benutzerversuche](#)

[FireSight-Korrelationsrichtlinie Treffer](#)

[ISE führt Quarantäne aus und sendet CoA](#)

[VPN-Sitzung wird getrennt](#)

[VPN-Sitzung mit begrenztem Zugriff \(Quarantäne\)](#)

[Fehlerbehebung](#)

[FireSight \(Defense Center\)](#)

[ISE](#)

[Bug](#)

[Zugehörige Informationen](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

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.

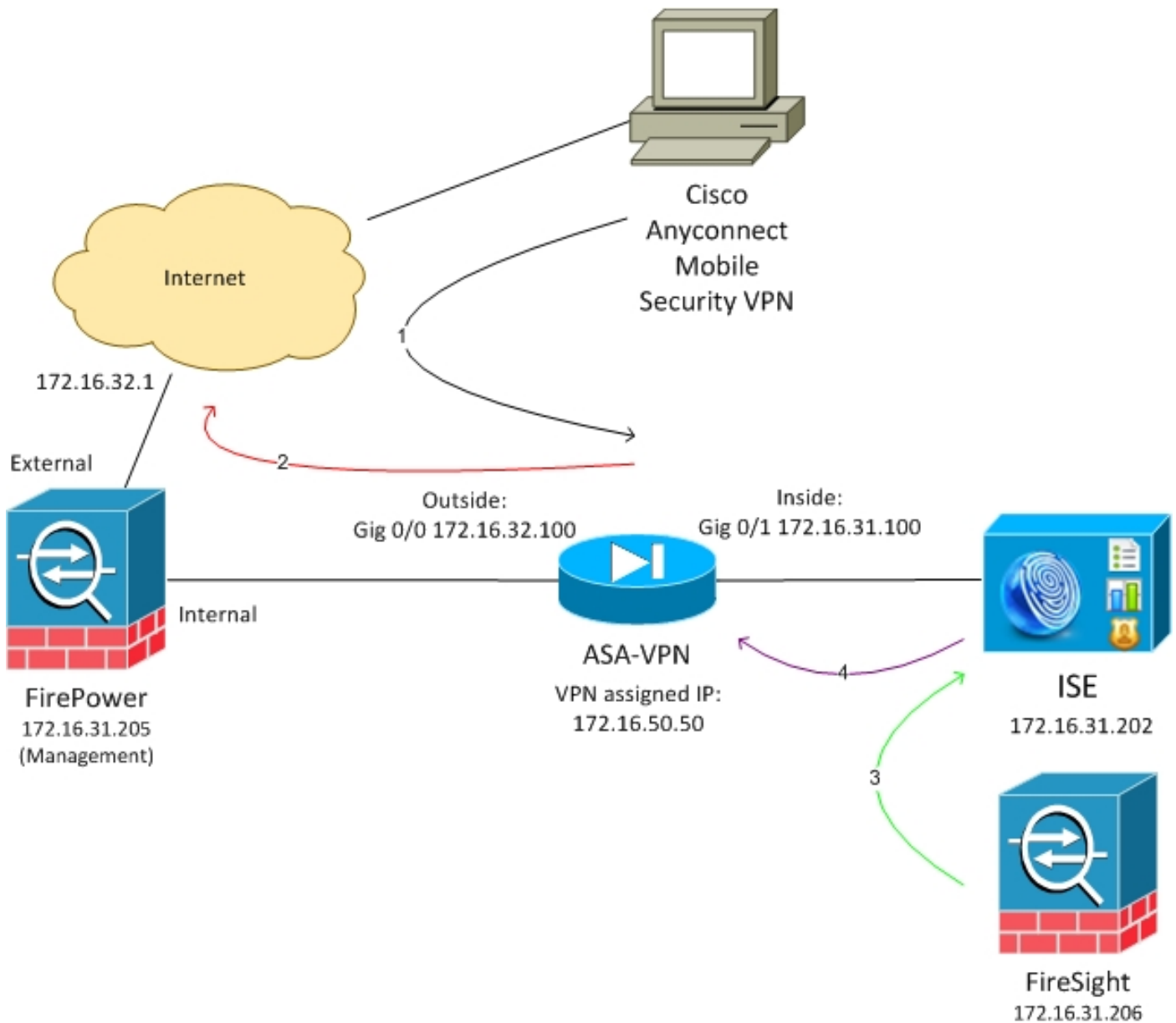
Konfigurieren

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-Problembeseitigung 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.

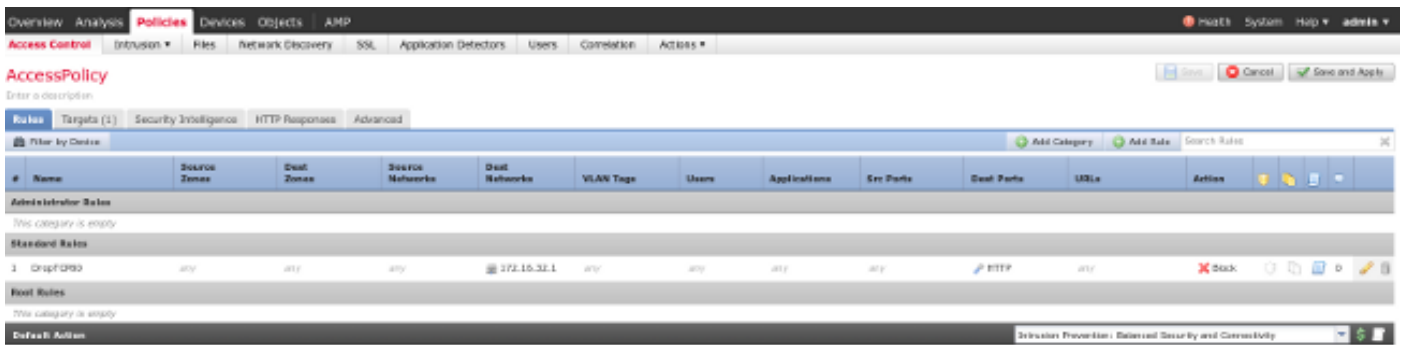
Das virtuelle System verfügt über drei Schnittstellen: eine für die Verwaltung und zwei für die Inline-Prüfung (intern/extern).

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

FireSight Management Center (Defense Center)

Zugriffskontrollrichtlinie

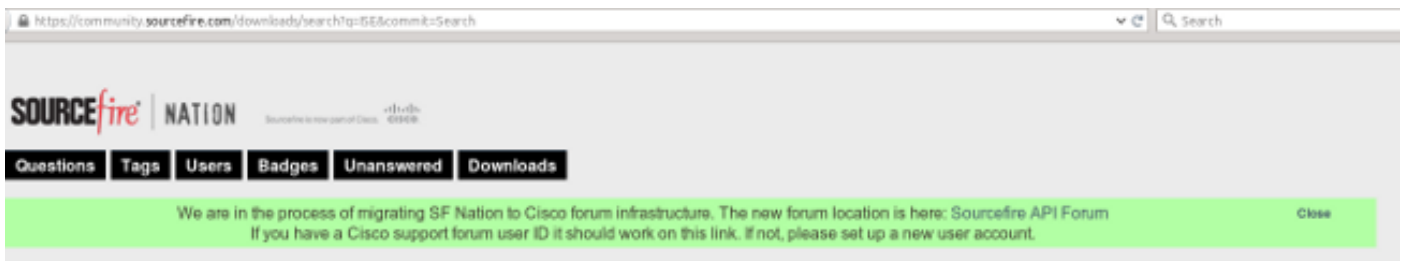
Nachdem Sie die richtigen Lizenzen installiert und das FirePower-Gerät hinzugefügt haben, navigieren Sie zu **Policies > Access Control (Richtlinien > Zugriffskontrolle)**, und erstellen Sie die Zugriffsrichtlinie, die verwendet wird, um den HTTP-Datenverkehr auf 172.16.32.1 zu verwerfen:



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*:



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.

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



Installed Remediation Modules

Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall
ISE 1.2 Remediation	1.3.19	Quarantine IP addresses using Identity Services Engine 1.2
Nmap Remediation	2.0	Perform an Nmap Scan
Set Attribute Value	1.0	Set an Attribute Value

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):

Edit Instance

Instance Name	<input type="text" value="ise-instance"/>
Module	ISE 1.2 Remediation (v1.3.19)
Description	<input type="text"/>
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>	<input type="text"/>

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

Configured Remediations

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

Korrelationsrichtlinie

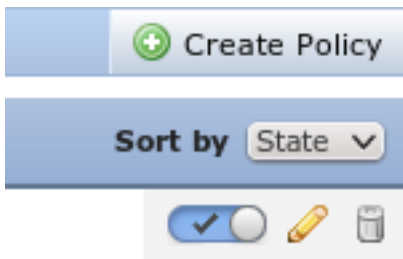
Sie müssen jetzt eine bestimmte Korrelationsregel konfigurieren. Diese Regel wird zu Beginn der Verbindung ausgelöst, die mit der zuvor konfigurierten Zugriffskontrollregel (*DropTCP80*) übereinstimmt. Um die Regel zu konfigurieren, navigieren Sie zu **Richtlinien > Korrelation > Regelverwaltung**:

The screenshot shows the configuration page for a rule named "CorrelateTCP80Block". The interface includes a top navigation bar with "Policies" selected, and a sub-navigation bar with "Rule Management" active. The "Rule Information" section shows the rule name, description, and group. The "Select the type of event for this rule" section is configured with the condition "a connection event occurs at the beginning of the connection and it meets the following conditions: Access Control Rule Name contains the string DropTCP80". The "Rule Options" section shows a snooze setting of 0 hours.

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: **Problembekämpfung für SourceIP** (früher konfiguriert) und **Syslog**:

The screenshot shows the "Correlation Policy Information" page. The policy name is "CorrelateTCP80Block". The "Policy Rules" section shows the rule "CorrelateTCP80Block" with a response of "SourceIP-Remediation". A modal window titled "Responses for CorrelateTCP80Block" is open, showing "Assigned Responses" with "SourceIP-Remediation" and "Unassigned Responses" which is currently empty.

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

Netzwerkzugriffsgert (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:

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 features a left-hand navigation pane with categories like 'Client Provisioning', 'Adaptive Network Control' (highlighted), 'FIPS Mode', 'Alarm Settings', 'Posture', 'Profiling', and 'Protocols'. The main pane displays the 'Adaptive Network Control' configuration, where the 'Service Status' is set to 'Enabled' (indicated by a green checkmark in a dropdown menu). Below this, there are 'Save' and 'Reset' buttons.

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

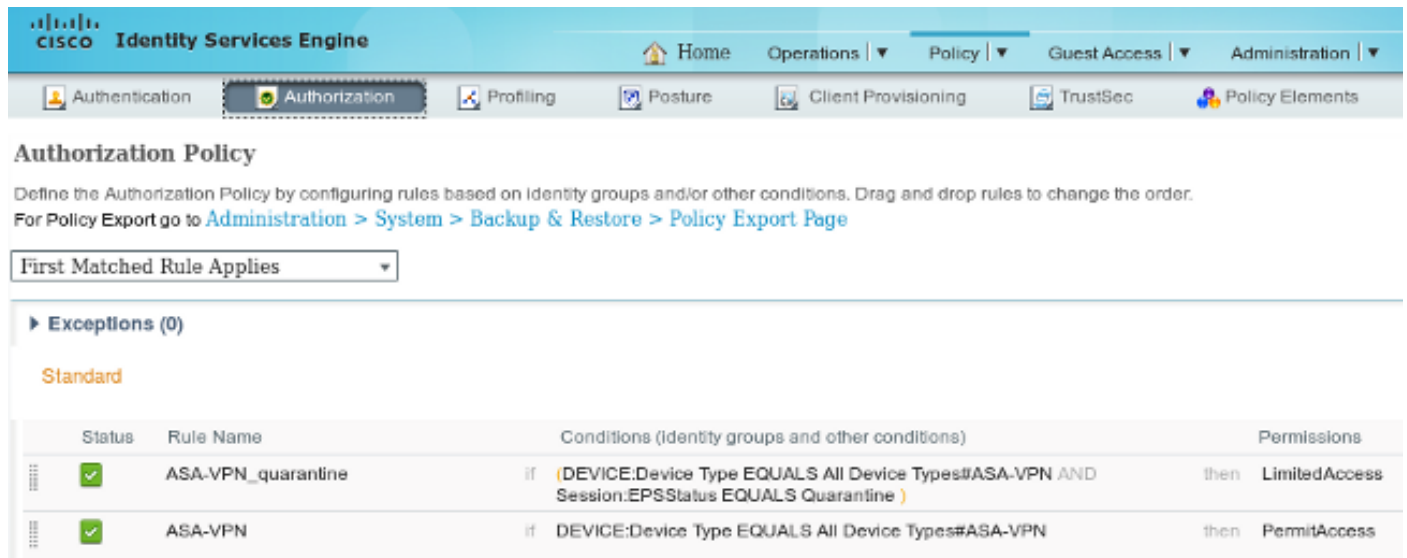
Navigieren Sie zu **Richtlinien > Ergebnisse > Autorisierung > Autorisierungsprofil**, und erstellen Sie ein Autorisierungsprofil mit der neuen DACL:

The screenshot shows 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 features a left-hand navigation pane with categories like 'Authentication', 'Authorization' (expanded to show 'Authorization Profiles', 'Downloadable ACLs', and 'Inline Posture Node Profiles'), 'Profiling', 'Posture', 'Client Provisioning', and 'TrustSec'. The main pane displays the 'Authorization Profile' configuration for 'LimitedAccess'. The 'Name' field is set to 'LimitedAccess'. The 'Access Type' dropdown is set to 'ACCESS_ACCEPT'. The 'Service Template' checkbox is unchecked. Below the main configuration, there is a 'Common Tasks' section with a 'DACL Name' dropdown set to 'DENY_ALL_QUARANTINE'.

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**:



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)

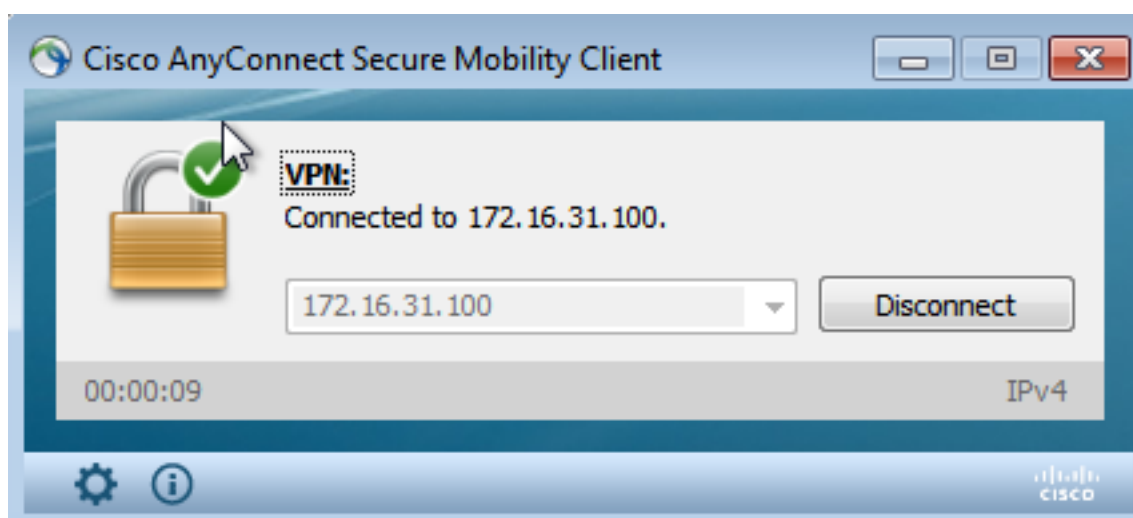
Standard

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

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
```


The image shows a Wireshark packet capture of an HTTPS connection. The key packets are:

- 120: Client Hello (TLSv1)
- 121: https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165957 TSecr=97280105
- 122: [TCP segment of a reassembled PDU]
- 123: Server Hello, Certificate, Certificate Request, Server Hello Done (TLSv1)
- 124: 48046 > https [ACK] Seq=518 Ack=1449 Win=17536 Len=0 TSval=97280106 TSecr=389165957
- 125: 48046 > https [ACK] Seq=518 Ack=2897 Win=20480 Len=0 TSval=97280106 TSecr=389165957
- 126: 48046 > https [ACK] Seq=518 Ack=3512 Win=23296 Len=0 TSval=97280106 TSecr=389165958
- 127: Certificate, Client Key Exchange, Change Cipher Spec, Finished (TLSv1)
- 128: Change Cipher Spec (TLSv1)
- 129: Finished (TLSv1)
- 130: 48046 > https [ACK] Seq=856 Ack=3571 Win=23296 Len=0 TSval=97280107 TSecr=389165962
- 131: 255 GET /ise/eps/QuarantineByIP/172.16.50.50 HTTP/1.1
- 132: 48046 > https [ACK] Seq=3571 Ack=1085 Win=17792 Len=0 TSval=389166020 TSecr=97280111
- 135: 429 HTTP/1.1 200 OK

The packet details for the GET request (131) show:

- 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 YWRtaW46S3Zha293MTIz\r\n
- Host: 172.16.31.202\r\n
- User-Agent: Libwww-perl/6.05\r\n
- \r\n

The full request URI is: <http://172.16.31.202/ise/eps/QuarantineByIP/172.16.50.50>

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 Problembhebung zu bestätigen:

The screenshot shows the 'Remediation Status' page in the Cisco ISE interface. The navigation path is 'Analysis > Policies > Devices > Objects > AMP'. The 'Correlation > Status' tab is active.

The table below shows the remediation status:

Time	Remediation Name	Policy	Rule	Result Message
2015-05-24 10:55:37	SourceIP-Remediation	CorrelationPolicy	CorrelateCPBlock	Successful completion of remediation
2015-05-24 10:47:08	SourceIP-Remediation	CorrelationPolicy	CorrelateCPBlock	Successful completion of remediation

Page 1 of 1, displaying rows 1-2 of 2 rows.

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=ac10206400021000555b9d36
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=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
```

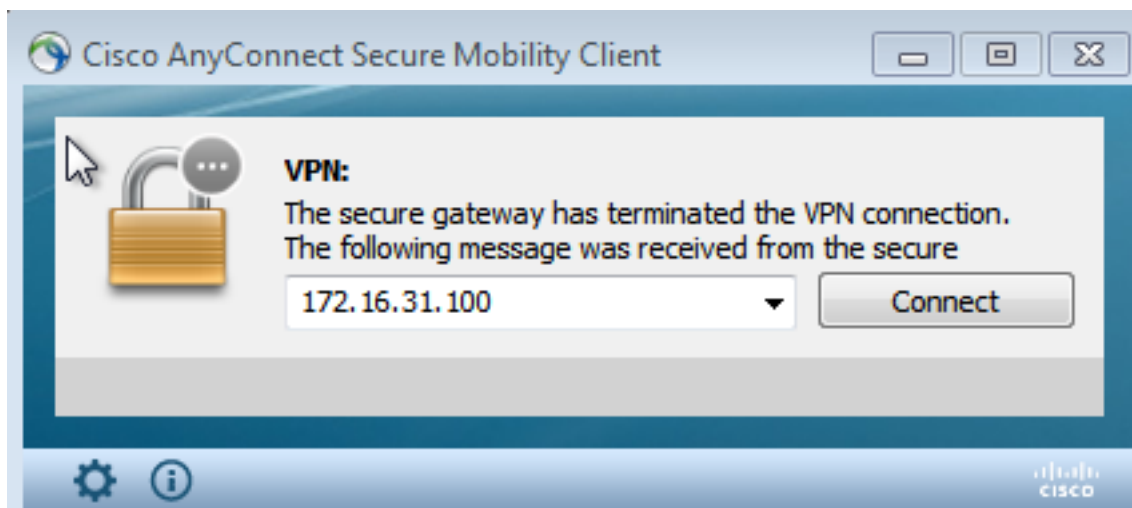
Die ise.psc sendet eine ähnliche Benachrichtigung:

```
INFO [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -:::- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAAddress=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:

The screenshot shows the Cisco ISE GUI with the following statistics at the top: Misconfigured Supplicants: 0, Misconfigured Network Devices: 0, RADIUS Drops: 0, and Client Stopped: 0. Below this is a table of live sessions with columns for Time, Status, Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event. The table contains five rows of session data.

Time	Status	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-05-24 10:51:40...	🟡	cisco	192.168.10.21			Session State Is Stated
2015-05-24 10:51:35...	🟢	#ACSACL#-P-D				ACL 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 10:48:01...	🟢	cisco	192.168.10.21	Default -> ASA-VPN	PermitAccess	Authentication succeeded

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  : ac10206400027000555c02e8
Security Grp  : none
```

```
.....
DTLS-Tunnel:
<some output omitted 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:

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	ac1020640000		
2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	512	ac1020640000	admin	172.16.31.206
2015-05-24 21:29:47.5	08:00:27:DA:EF:A		Unquarantine	SUCCESS	507	ac1020640000		
2015-05-24 21:29:47.4	08:00:27:DA:EF:A		Unquarantine	RUNNING	507	ac1020640000	admin	172.16.31.202
2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	FAILURE	480	ac1020640000		
2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	RUNNING	480	ac1020640000	admin	172.16.31.202
2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	SUCCESS	471	ac1020640000		
2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	RUNNING	471	ac1020640000	admin	172.16.31.202
2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	SUCCESS	462	ac1020640000		
2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	RUNNING	462	ac1020640000	admin	172.16.31.202
2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	SUCCESS	337	ac1020640000		
2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	RUNNING	337	ac1020640000	admin	172.16.31.202
2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	330	ac1020640000		
2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	330	ac1020640000	admin	172.16.31.206
2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	291	ac1020640000		
2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	291	ac1020640000	admin	172.16.31.206
2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	250	ac1020640000		
2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	250	ac1020640000	admin	172.16.31.206
2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	207	ac1020640000		
2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	RUNNING	207	ac1020640000	admin	172.16.31.206
2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	SUCCESS	206	ac1020640000		
2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	RUNNING	206	ac1020640000	admin	172.16.31.202
2015-05-24 10:51:17.2	08:00:27:DA:EF:A		Quarantine	SUCCESS	189	ac1020640000		
2015-05-24 10:51:17.2	08:00:27:DA:EF:A		Quarantine	RUNNING	189	ac1020640000	admin	172.16.31.202

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

-
- [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](#)