ISE と Firepower の統合での修復サービスの設定

内容

概要

このドキュメントでは、Cisco Identity Services Engine（ISE）をポリシー サーバとして使用して攻撃を検出し自動的に是正するために、Cisco FireSight アプライアンスの修復モジュールを使用する方法について説明します。このドキュメントで紹介されている例では ISE 経由で認証するリモート VPN ユーザの修復方法を説明していますが、802.1x/MAB/WebAuth の有線または無線ユーザにも適用できます。

注：このドキュメントで参照される修復モジュールは、正式にはシスコでサポートされていません。このモジュールは、コミュニティ ポータルサイトで共有されているもので、どなたでも使用できます。バージョン 5.4 以降では、*pxGrid プロトコルに基づく新しい修復モジュールが利用可能です*。このモジュールは、バージョン 6.0 ではサポートされていませんが、将来のリリースでサポートされる予定です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco 適応型セキュリティ アプライアンス（ASA）VPN の設定
- Cisco AnyConnect セキュア モビリティ クライアントの設定
- Cisco FireSight の基本設定
- Cisco FirePower の基本設定
- Cisco ISE の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft Windows 7
- Cisco ASA バージョン 9.3 以降
- Cisco ISE ソフトウェア バージョン 1.3 以降
- Cisco AnyConnect Secure Mobility Client バージョン 3.0 以降
- Cisco FireSight Management Center バージョン 5.4
- Cisco FirePOWER バージョン 5.4（仮想マシン（VM））

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

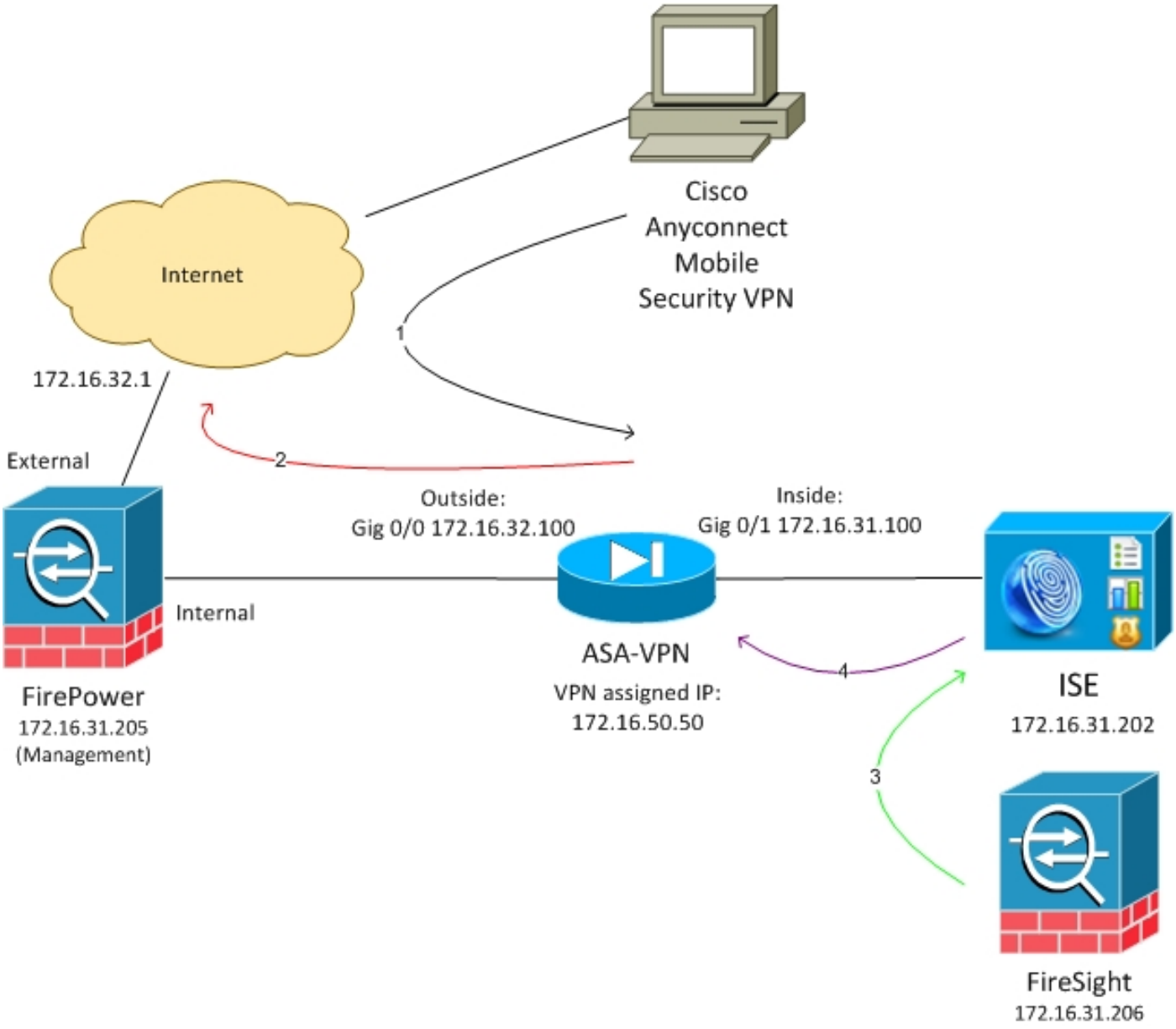
設定

この項で説明する情報を使用して、システムを設定します。

注：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントで説明されている例では、次のネットワーク設定が使用されています。



このネットワーク設定のフローを次に示します。

1. ユーザが ASA を使用してリモート VPN セッションを開始する（Cisco AnyConnect セキュア モビリティ バージョン 4.0 経由）。

2. ユーザは*http://172.16.32.1*にアクセスしようとします（トラフィックはVMにインストールされ、FireSightによって管理されるFirePower経由で移動します）。

3. FirePower は、その特定のトラフィックを（インラインで）ブロックするように設定されていますが（アクセス ポリシー）、トリガーされる相関ポリシーもあります。その結果、

REST アプリケーション プログラミング インターフェイス（API）経由で ISE の修復が開始される（*QuarantineByIP メソッド*）。

4. ISE が REST API コールを受信すると、セッションを検索し、ASA に RADIUS Change of Authorization（CoA）を送信します。それにより、セッションは終了します。

5. ASA が VPN ユーザを切断する。AnyConnect には *Always-on VPN アクセスが設定されているため、新しいセッションが確立される*。ただし、今回は別の ISE 認可ルールが（検疫されたホストに対して）一致し、制限されたネットワーク アクセスが提供される。この段階では、ユーザがどのようにネットワークに接続し、認証するとしても、認証および認可に ISE が使用されている限り、検疫の結果としてユーザのネットワーク アクセスは制限されます。

前に説明したように、このシナリオは、ISE が認証に使用され、ネットワーク アクセス デバイスが RADIUS CoA（シスコのすべての最新のデバイス）をサポートする限り、認証済みセッション（VPN、有線、ワイヤレス 802.1x/MAB/Webauth 802.1x/MAB/Webauth）の任意のタイプで動作します。

ヒント：ユーザの隔離を解除するには、ISE GUI を使用できます。今後のバージョンの修復モジュールでも、サポートされる可能性があります。

Firepower

注：このドキュメントで説明されている例では、VM アプライアンスが使用されています。初期設定のみ、CLI から行います。ポリシーはすべて Cisco Defence Center から設定されます。詳細については、このドキュメントの「関連情報」のセクションを参照してください。

VM には 3 つのインターフェイスがあり、1 つは管理用、あとの 2 つはインライン検査（内部/外部）用です。

VPN ユーザからのすべてのトラフィックは、FirePOWER を経由します。

FireSight Management Center（Defence Center）

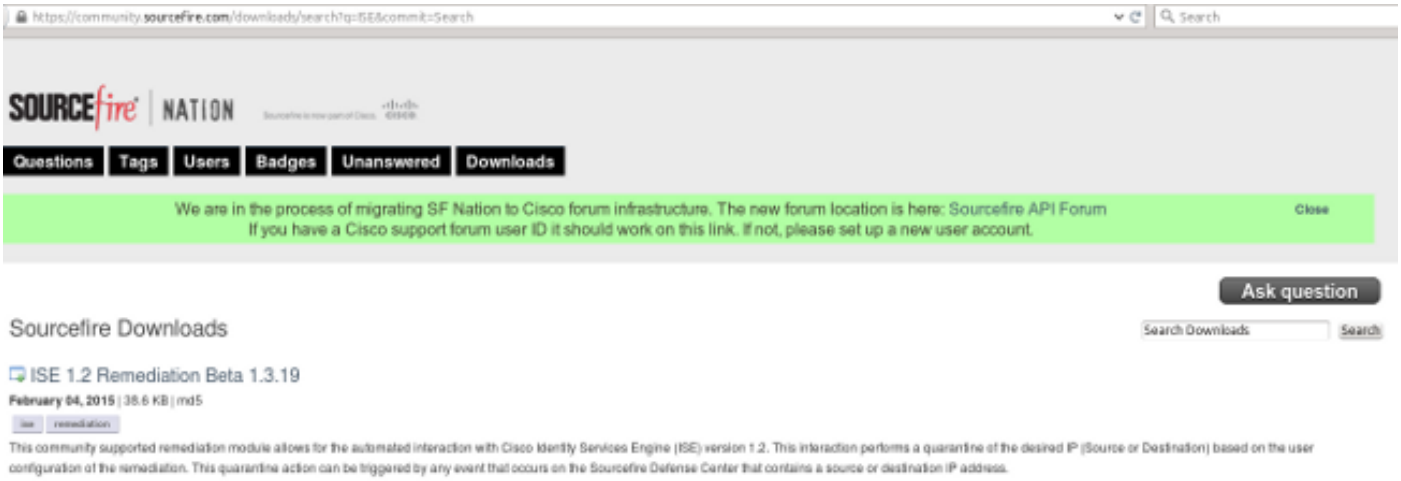
アクセス コントロール ポリシー

正しいライセンスをインストールして FirePower デバイスを追加してから、[Policies] > [Access Control] の順に移動し、HTTP トラフィックを 172.16.32.1 にドロップするのに使用するアクセス ポリシーを作成します。

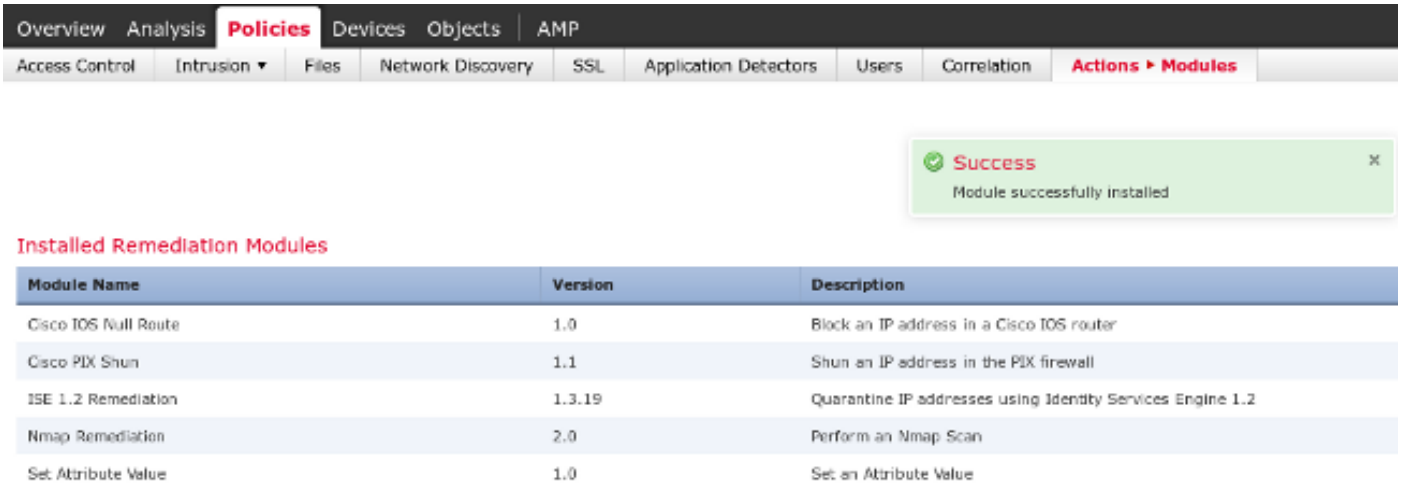
他のトラフィックはすべて受け入れられます。

ISE 修復モジュール

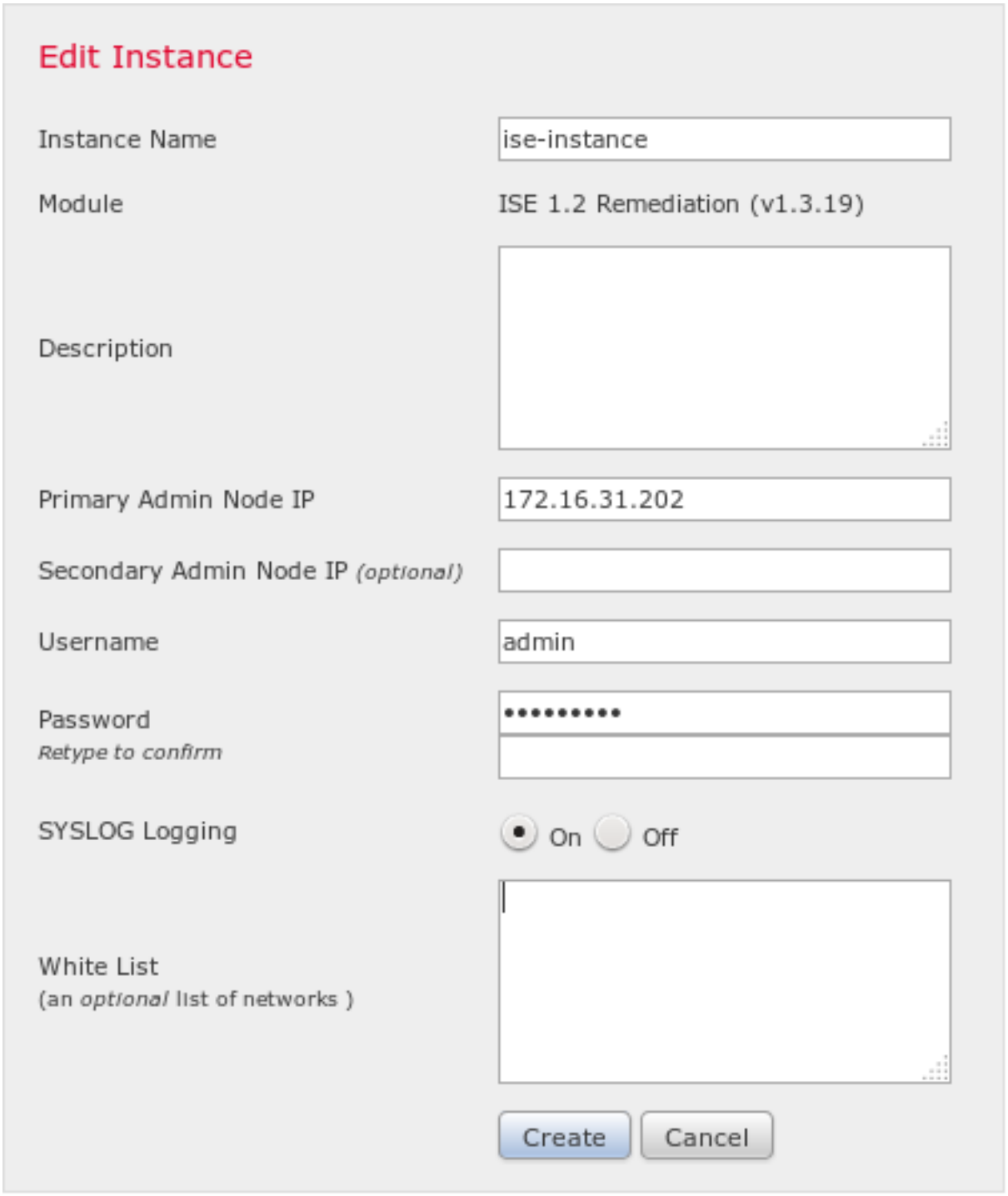
コミュニティ ポータルで共有されている ISE モジュールの現在のバージョンは、*ISE 1.2 Remediation Beta 1.3.19* です。



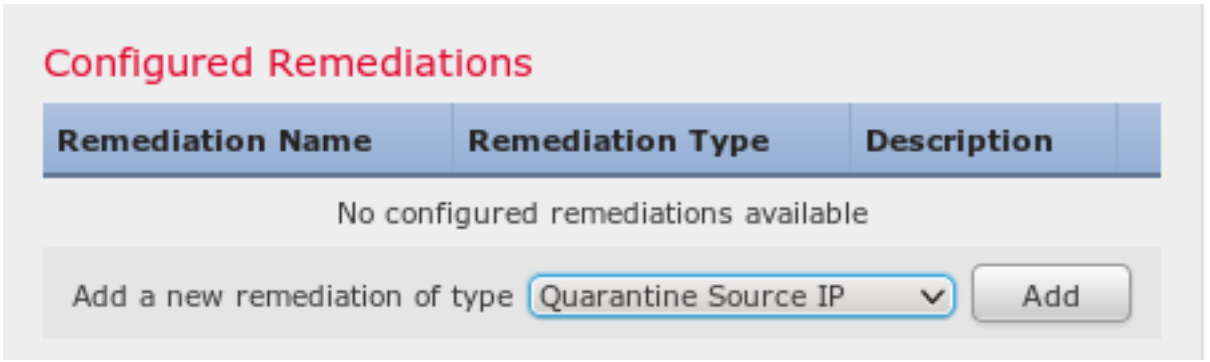
[Policies] > [Actions] > [Remediations] > [Modules] に移動し、ファイルをインストールします。



すると、正しいインスタンスが作成されます。[Policies] > [Actions] > [Remediations] > [Instances] に移動し、ポリシー管理ノード（PAN）の IP アドレス、および REST API に必要な ISE 管理クレデンシャル（*ERS Admin の役割を付与された別個のユーザを推奨*）を指定します。

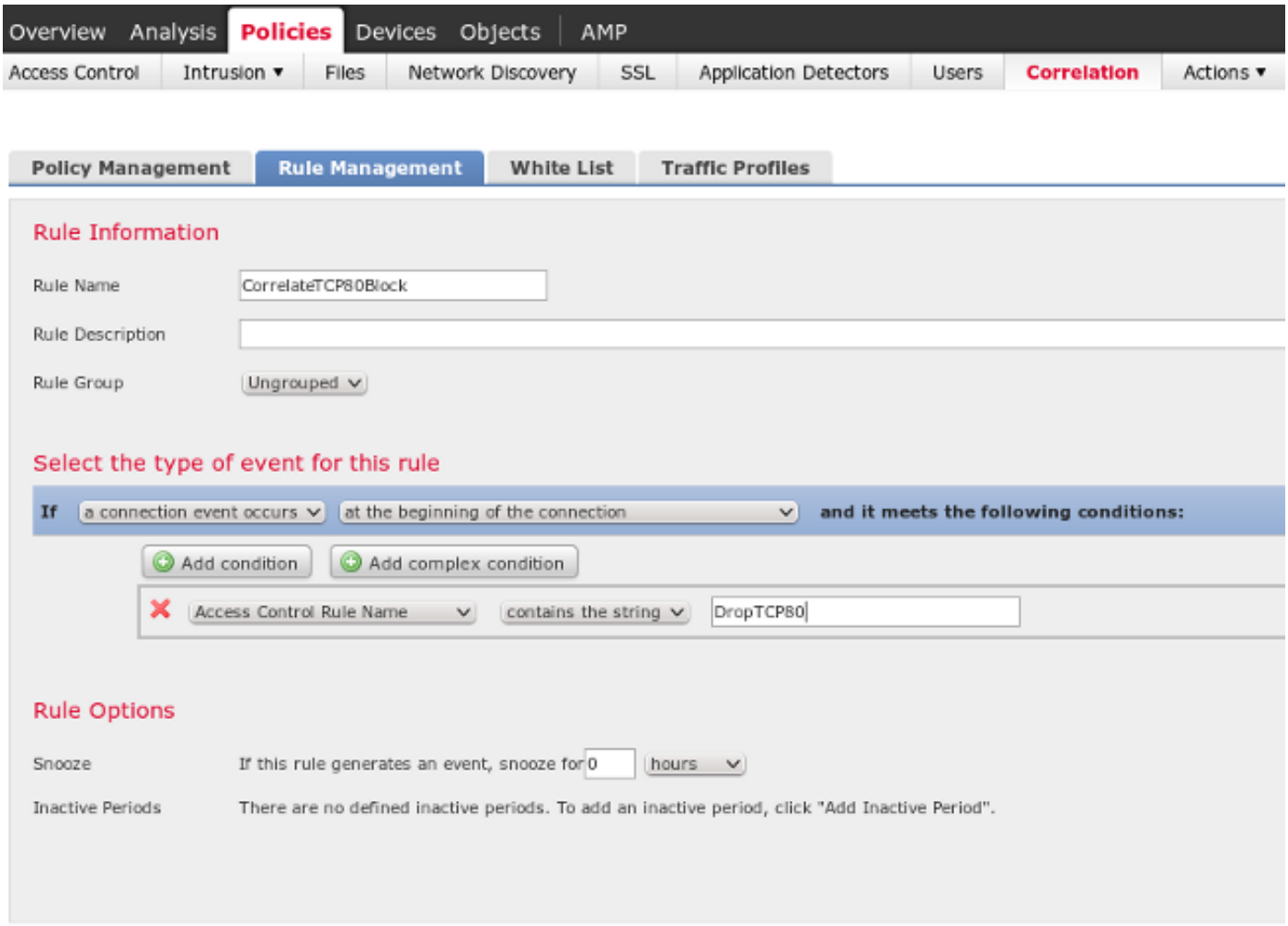


修復には、送信元 IP アドレス (攻撃者の) も使用する必要があります。

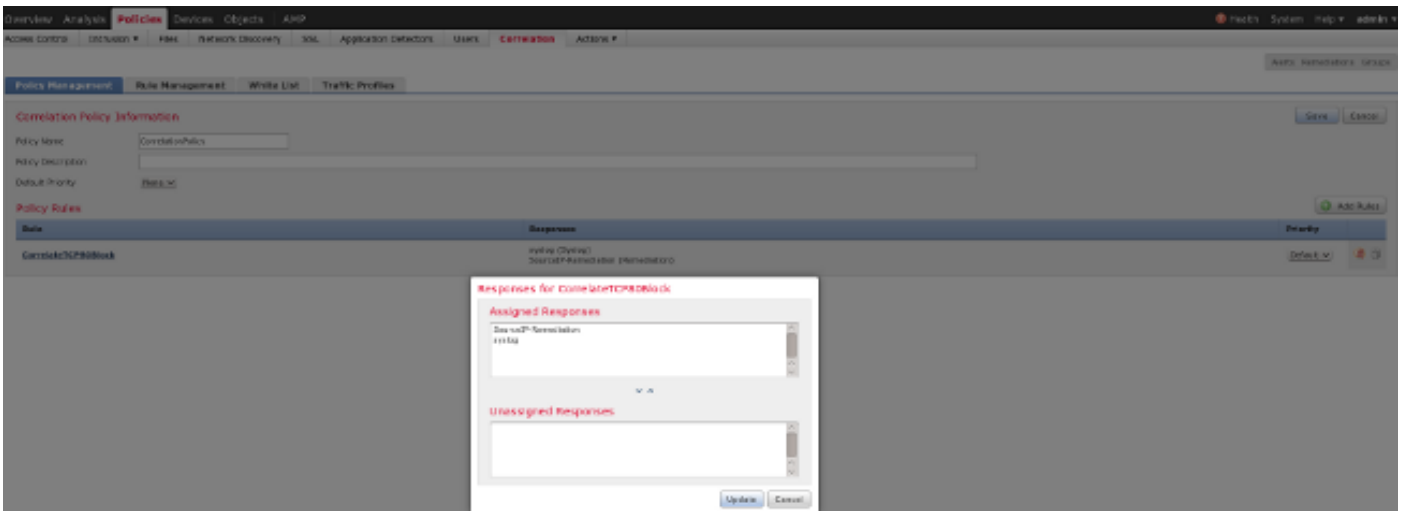


相関ポリシー

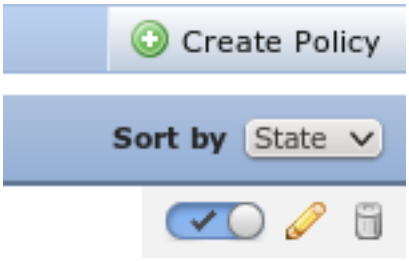
ここで、特定の相関ルールを設定する必要があります。このルールは、あらかじめ設定されたアクセス制御ルール（*DropTCP80*）に一致する接続の開始時にトリガーされます。 ルールを設定するには、[Policies] > [Correlation] > [Rule Management] に移動します。



このルールは、相関ポリシーで使用されます。[Policies] > [Correlation] > [Policy Management] に移動して新しいポリシーを作成し、設定したルールを追加します。右側の [Remediate] をクリックし、**remediation for sourceIP（以前に設定）および syslog**：



相関ポリシーがイネーブルであることを確認します。



ASA

認証に ISE を使用するため、VPN ゲートウェイとして動作する ASA を設定します。また、アカウンティングおよび RADIUS CoA を有効にすることも必要です。

```
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
```

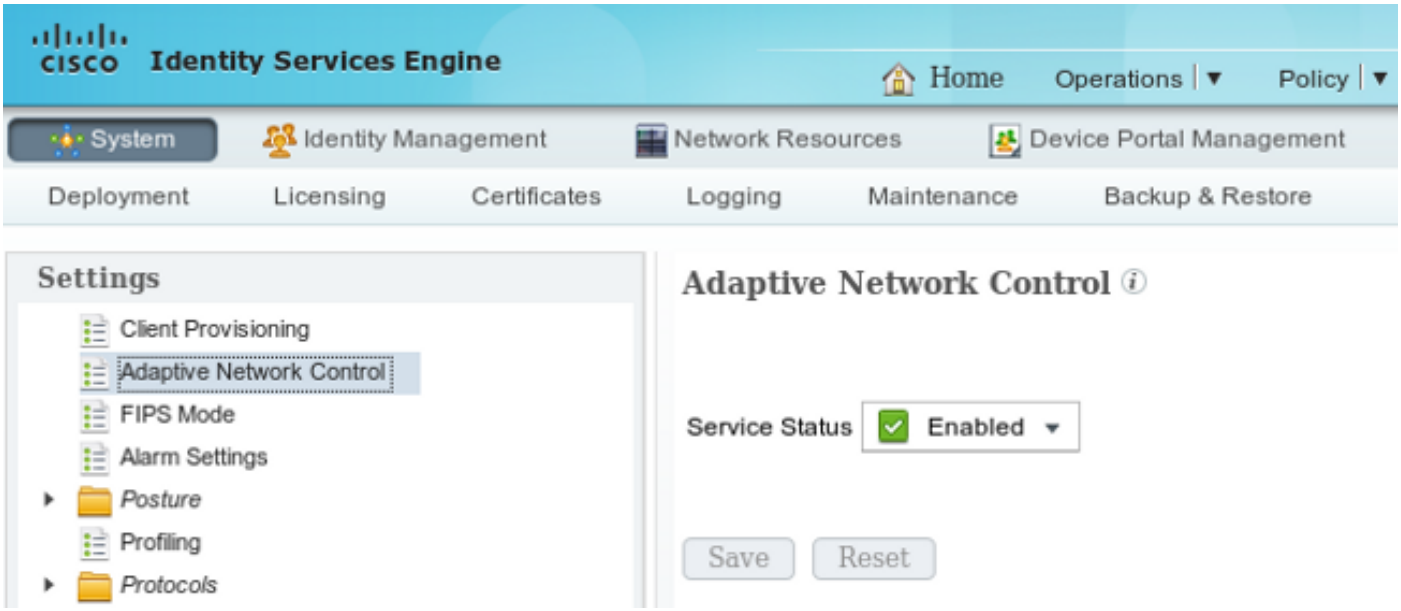
ISE

ネットワーク アクセス デバイス（NAD）の設定

[Administration] > [Network Devices] に移動し、RADIUS クライアントとして動作する ASA を追加します。

適応型のネットワーク制御の有効化

検疫の API と機能を有効にするため、[Administration] > [System] > [Settings] > [Adaptive Network Control] に移動します。



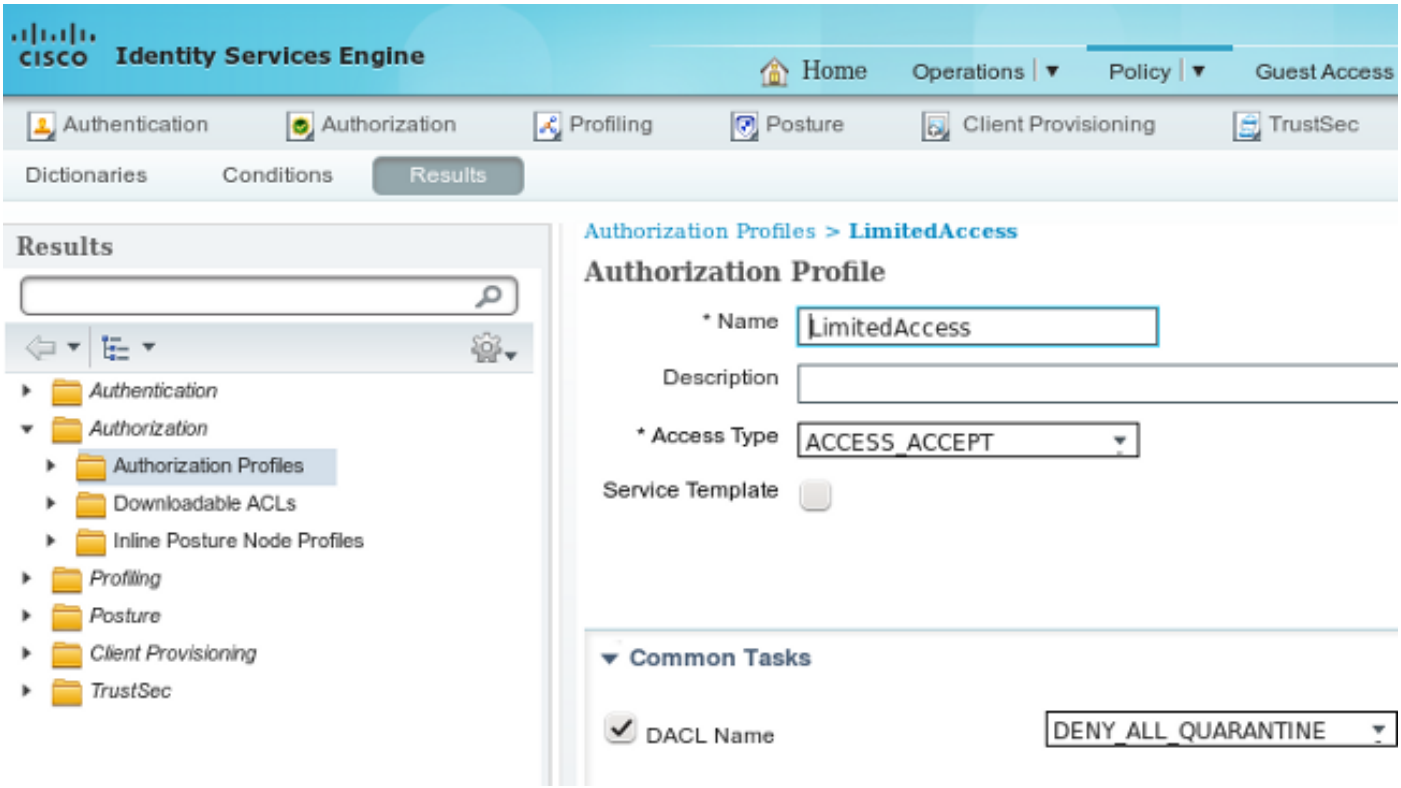
注：バージョン 1.3 以前では、この機能は*エンドポイント保護サービス*という名称になっています。

検疫 DACL

検疫されたホストで使用されるダウンロード可能アクセス制御リスト（DACL）を作成するには、[Policy] > [Results] > [Authorization] > [Downloadable ACL] の順に移動します。

検疫用認可プロファイル

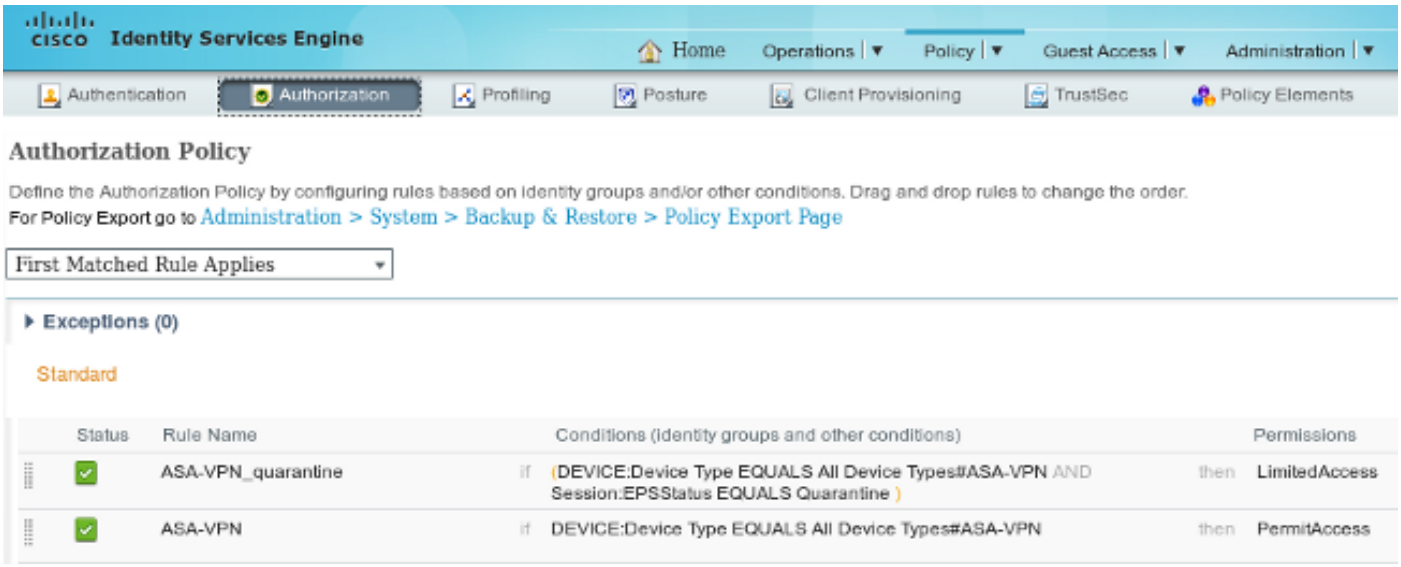
[Policy] > [Results] > [Authorization] > [Authorization Profile] に移動し、新しい DACL により認可プロファイルを作成します。



認可ルール

2 つの認可ルールを作成する必要があります。最初のルール（ASA-VPN）は ASA で終端する VPN セッションすべてへのフル アクセスを提供します。*ASA-VPN_quarantine 規則は、ホストが検疫済みである（制限付きネットワーク アクセスが提供されている）場合に、再認証された VPN セッションにヒットします。*

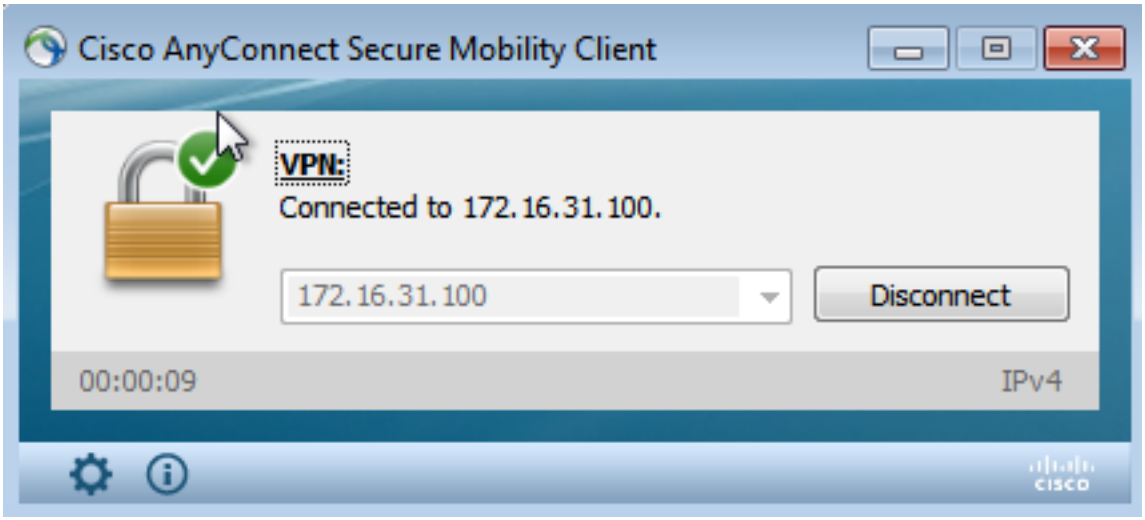
これらのルールを作成するため、[Policy] > [Authorization] に移動します。



確認

このセクションに記載されている情報を使用して、設定が適切に機能するか確認します。

AnyConnect が ASA VPN セッションを開始する



ASA は DACL なしでセッションを作成します (フル ネットワーク アクセス) 。

```
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>
```

ユーザによるアクセス試行

ユーザが http://172.16.32.1 にアクセスしようとすると、アクセス ポリシーがヒットし、対応するトラフィックがインラインでブロックされて、FirePower の管理 IP アドレスから syslog メッセージが送信されます。

```
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:
```

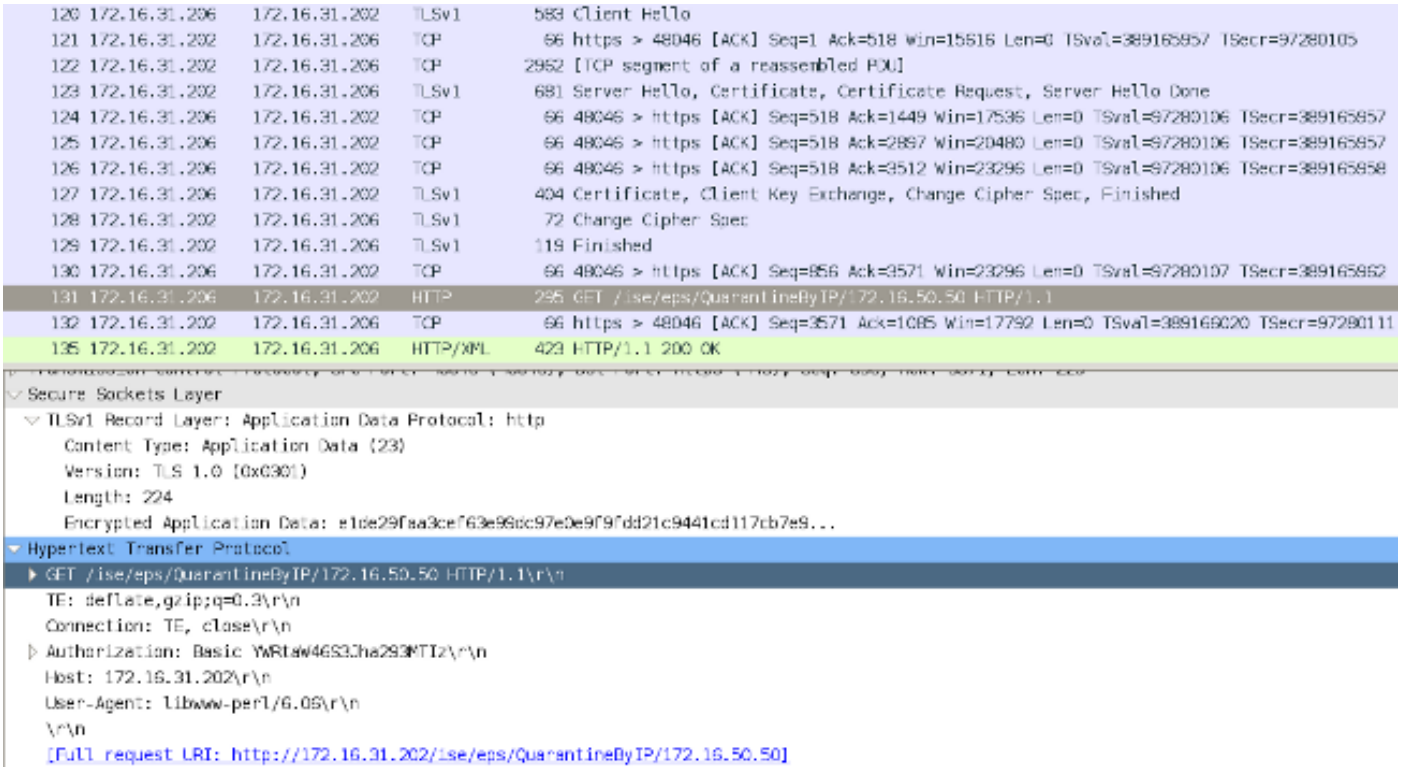
```
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes:
66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A,
SSL Cipher Suite: N/A, SSL Certificate: 0000000000000000000000000000000000000000,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

FireSight Management (Defense Center) 相関ポリシーがヒットします。これは、Defense Center から送信される syslog メッセージで報告されます。

```
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)
```

この段階で Defense Center は、ISE に対する REST API (隔離) 呼び出しを使用します。これは HTTPS セッションであり、(Secure Sockets Layer (SSL) プラグインおよび PAN 管理証明書の秘密鍵を使用して) Wireshark で復号化できます。



GET 要求では、攻撃者の IP アドレス (172.16.50.50) が渡され、そのホストが ISE により隔離されます。

修復が正常に実行されたことを確認するため、[Analysis] > [Correlation] > [Status] に移動します。

ISE が隔離を実行し、CoA を送信する

この段階で、ISE prrt-management.log により、CoA の送信が必要であることが通知されます。

```
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
```

ランタイム(prrt-server.log)はCoA終了メッセージをNADに*送信*し、セッション(ASA)を終了します。

```
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
```

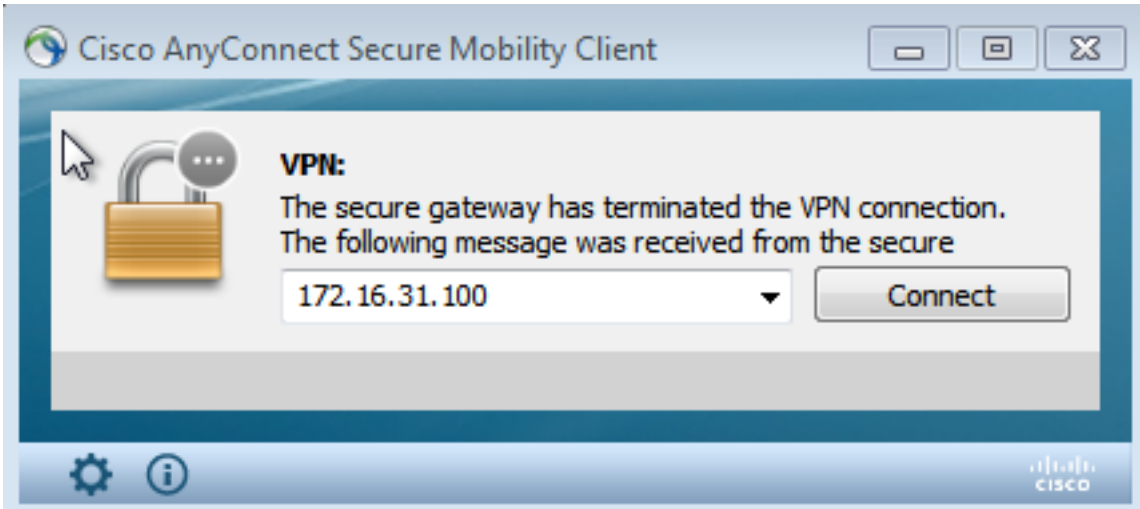
ise.psc が、次のような通知を送信します。

```
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
```

[Operations] > [Authentication] に移動すると、[Dynamic Authorization succeeded] が表示されるはずです。

VPN セッションが切断される

エンドユーザは、セッションが切断されていることを示すために通知を送信します（有線またはワイヤレスの 802.1x/MAB/ゲストの場合、このプロセスは透過的に実行されます）。

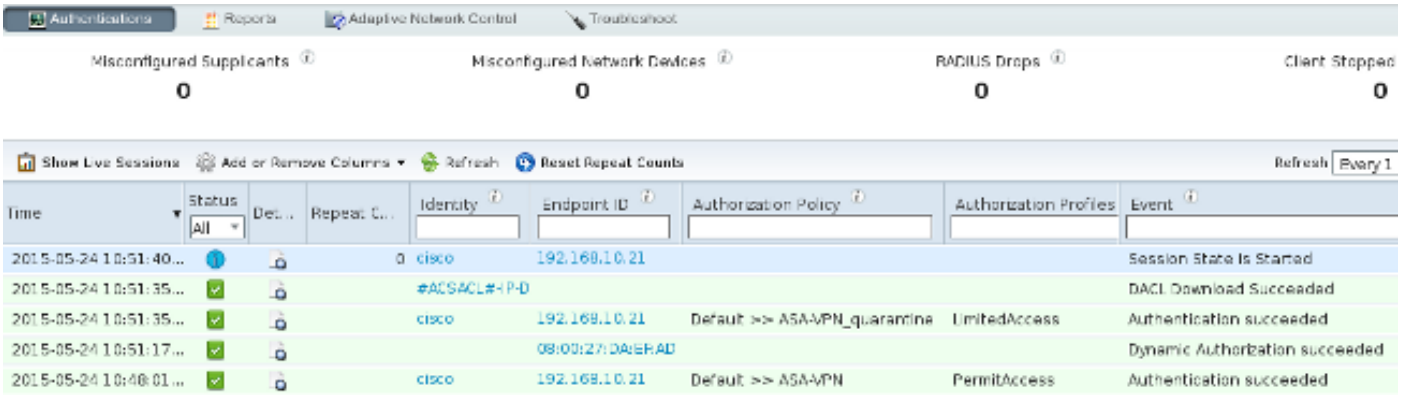


Cisco AnyConnect ログに次のような詳細が記録されます。

```
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
```

制限付きアクセスの VPN セッション（検疫）

*always-on VPN が設定されているため、すぐに新しいセッションが確立されます。*今回は、ISE *ASA-VPN_quarantine ルールがヒットするため、制限されたネットワーク アクセスが提供されます。*



注：DACL が別の RADIUS 要求でダウンロードされます。

アクセスが限られているセッションについては、**show vpn-sessiondb detail anyconnect の CLI コマンドを使用して、ASA で確認できます。**

```
asav# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

```
Username     : cisco                  Index        : 39
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.21
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 11436                  Bytes Rx     : 4084
Pkts Tx      : 8                      Pkts Rx      : 36
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : POLICY                 Tunnel Group : SSLVPN-FIRESIGHT
Login Time   : 03:43:36 UTC Wed May 20 2015
Duration     : 0h:00m:10s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : ac10206400027000555c02e8
Security Grp : none

.......
DTLS-Tunnel:
 <some output ommited for clarity>
  Filter Name  : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

FireSight (Defence Center)

ISE 修復スクリプトは次の場所にあります。

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

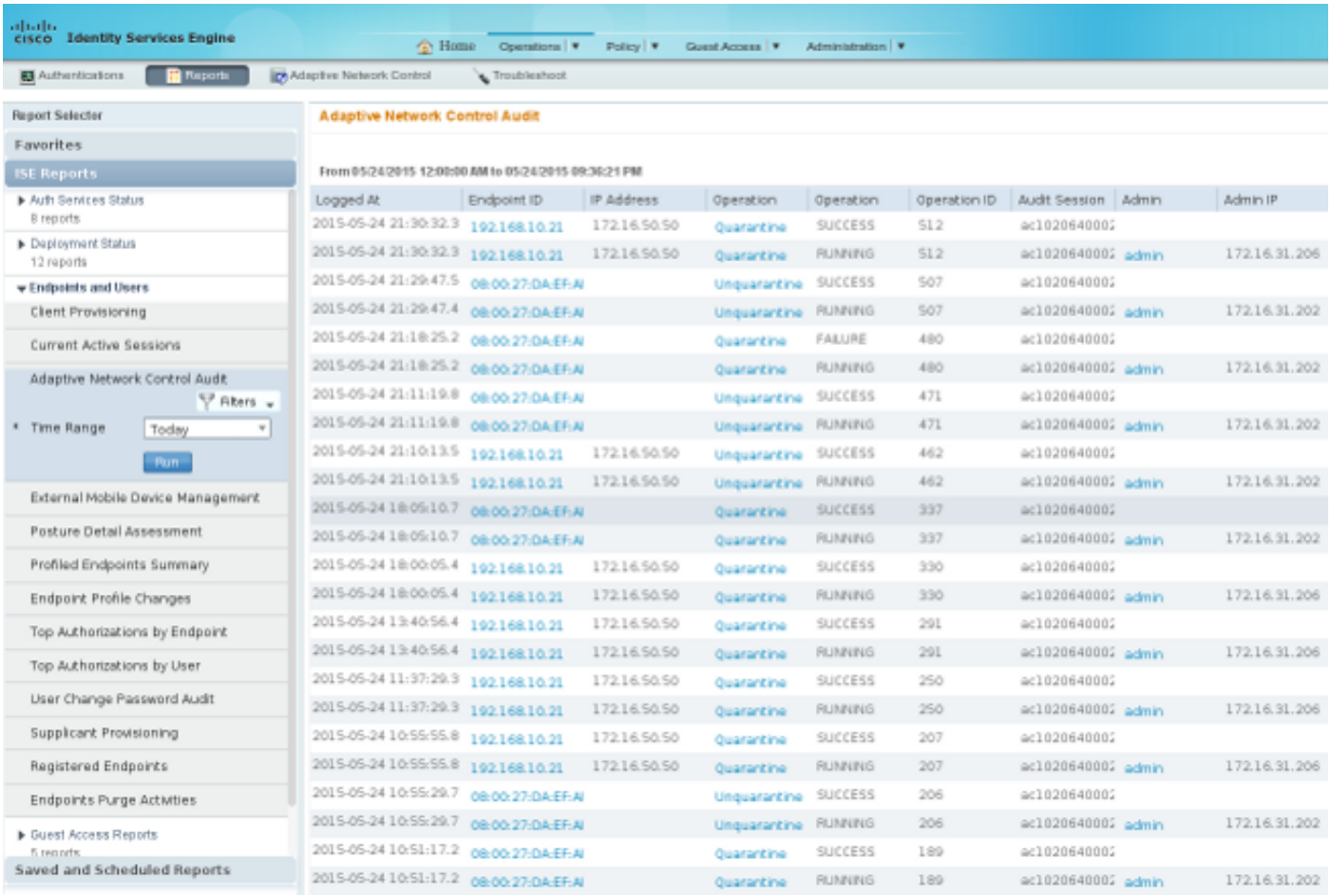
これは、標準的な SourceFire (SF) ロギング サブシステムを使用した単純な *Perl スクリプト*です。修復が実行されると、*/var/log/messages* で結果を確認できます。

```
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

ISE で適応型ネットワーク制御サービスを有効化することが重要です。ランタイム プロセスで詳細なログ (*prrt-management.log* と *prrt-server.log*) を表示するには、Runtime-AAA の DEBUG レベルを有効にする必要があります。[Administration] > [System] > [Logging] > [Debug Log Configuration] の順に移動し、デバッグを有効にします。

また、[Operations] > [Reports] > [Endpoint and Users] > [Adaptive Network Control Audit] に移動すると、隔離要求のすべての試行と結果の情報を表示することができます。



バグ

VPN セッション障害関連の ISE バグ（802.1x/MAB は正常に動作します）についての詳細は、Cisco Bug IDCSCuu41058（「ISE 1.4 エンドポイント検疫の不一致および VPN 障害」）を参照してください。

関連情報

- TrustSec 認識サービス用の ISE と WSA との統合設定
- IPS pxLog アプリケーションとの ISE バージョン 1.3pxGrid 統合
- Cisco Identity Services Engine 管理者ガイド、リリース 1.4 – 適応型ネットワーク制御サービスの設定
- Cisco Identity Services Engine API リファレンス ガイド、リリース 1.2：外部 RESTful サービス API の概要
- Cisco Identity Services Engine API リファレンス ガイド、リリース 1.2：モニタリング REST の概要
- Cisco Identity Services Engine 管理ガイド リリース 1.3

- テクニカル サポートとドキュメント - Cisco Systems