Configurer les services de correction avec l'intégration ISE et FirePower

Contenu

Introduction

Ce document décrit comment utiliser le module de correction sur un appareil Cisco FireSight afin de détecter les attaques et de corriger automatiquement l'attaquant à l'aide de Cisco Identity Service Engine (ISE) en tant que serveur de stratégies. L'exemple fourni dans ce document décrit la méthode utilisée pour corriger un utilisateur VPN distant qui s'authentifie via ISE, mais il peut également être utilisé pour un utilisateur filaire ou sans fil 802.1x/MAB/WebAuth.

Note: Le module de correction référencé dans ce document n'est pas officiellement pris en charge par Cisco. Il est partagé sur un portail communautaire et peut être utilisé par n'importe qui. Dans les versions 5.4 et ultérieures, il existe également un nouveau module de correction basé sur le protocole *pxGrid*. Ce module n'est pas pris en charge dans la version 6.0, mais il est prévu de le faire dans les versions futures.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN de l'appareil de sécurité adaptatif Cisco (ASA)
- Configuration du client Cisco AnyConnect Secure Mobility
- Configuration de base de Cisco FireSight
- Configuration de base de Cisco FirePower
- Configuration de Cisco ISE

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Cisco ASA version 9.3 ou ultérieure
- Logiciel Cisco ISE versions 1.3 et ultérieures
- Cisco AnyConnect Secure Mobility Client versions 3.0 et ultérieures
- Cisco FireSight Management Center version 5.4
- Cisco FirePower version 5.4 (machine virtuelle)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

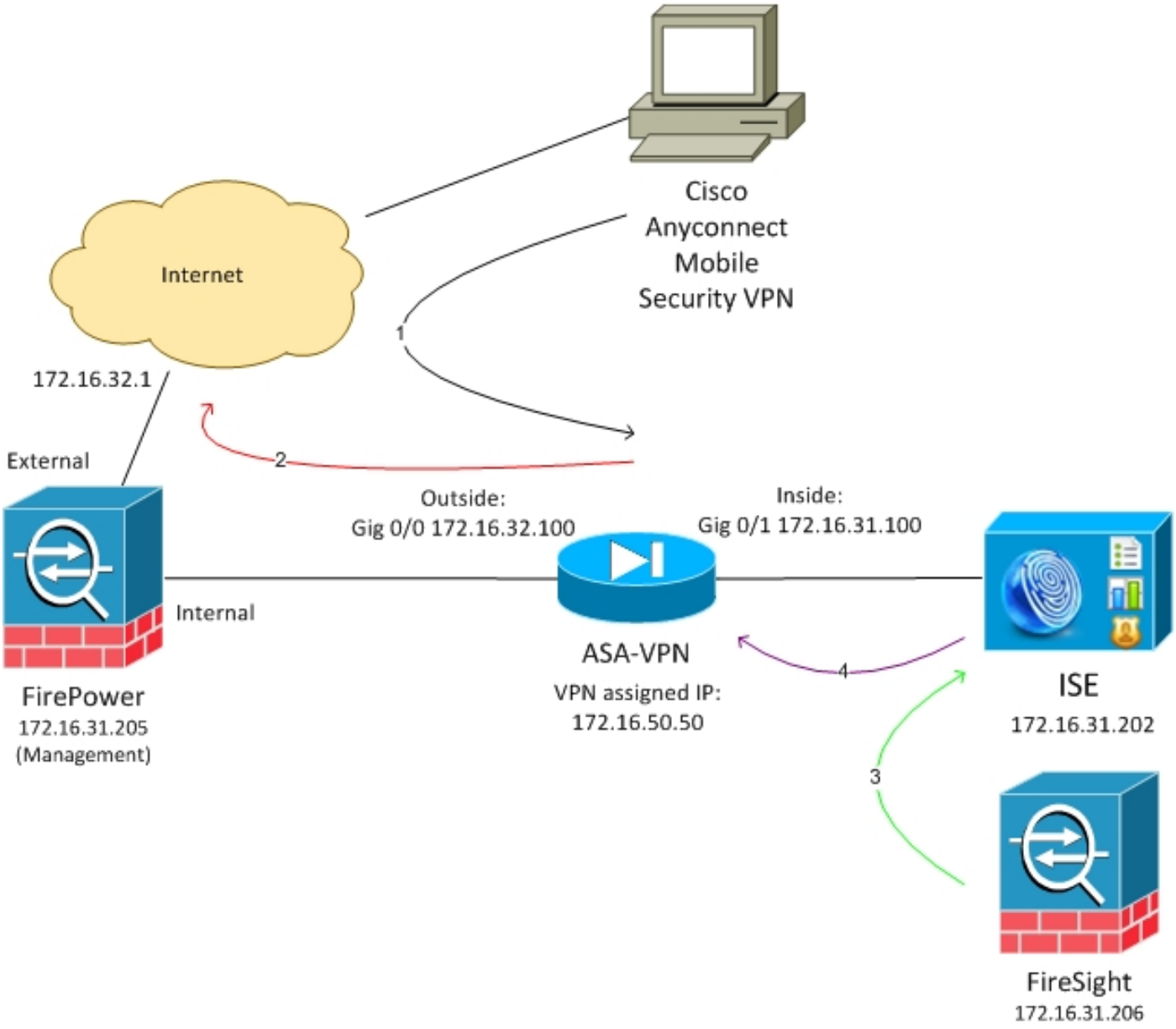
Configuration

Utilisez les informations fournies dans cette section afin de configurer votre système.

Note: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

L'exemple décrit dans ce document utilise cette configuration réseau :



Voici le flux de cette configuration réseau :

1. L'utilisateur lance une session VPN à distance avec l'ASA (via Cisco AnyConnect Secure Mobility Version 4.0).

2. L'utilisateur tente d'accéder à *http://172.16.32.1*. (Le trafic passe par FirePower, installé sur la machine virtuelle et géré par FireSight.)

3. FirePower est configuré de sorte qu'il bloque (en ligne) ce trafic spécifique (stratégies d'accès), mais il a également une stratégie de corrélation qui est déclenchée. Par

conséquent, il initie la correction ISE via l'API REST (Application Programming Interface) (la méthode *QuarantineByIP*).

4. Une fois que l'ISE a reçu l'appel de l'API REST, il recherche la session et envoie un changement d'autorisation RADIUS (CoA) à l'ASA, qui met fin à cette session.

5. L'ASA déconnecte l'utilisateur VPN. AnyConnect étant configuré avec un accès *permanent* VPN, une nouvelle session est établie ; cependant, cette fois, une règle d'autorisation ISE différente est mise en correspondance (pour les hôtes mis en quarantaine) et un accès réseau limité est fourni. À ce stade, peu importe la manière dont l'utilisateur se connecte et s'authentifie au réseau ; tant que l'ISE est utilisé pour l'authentification et l'autorisation, l'utilisateur a un accès réseau limité en raison de la quarantaine.

Comme mentionné précédemment, ce scénario fonctionne pour tout type de session authentifiée (VPN, câblé 802.1x/MAB/Webauth, sans fil 802.1x/MAB/Webauth) tant que l'ISE est utilisé pour l'authentification et que le périphérique d'accès réseau prend en charge la CoA RADIUS (tous les périphériques Cisco modernes).

> **Astuce** : Afin de déplacer l'utilisateur hors de quarantaine, vous pouvez utiliser l'interface utilisateur graphique ISE. Les versions futures du module de correction pourraient également le prendre en charge.

FirePower

> **Note**: Une appliance VM est utilisée pour l'exemple décrit dans ce document. Seule la configuration initiale est effectuée via l'interface de ligne de commande. Toutes les stratégies sont configurées à partir de Cisco Defense Center. Pour plus de détails, consultez la section Informations connexes de ce document.

La machine virtuelle dispose de trois interfaces, une pour la gestion et deux pour l'inspection en ligne (interne/externe).

Tout le trafic des utilisateurs VPN passe par FirePower.

FireSight Management Center (Centre de défense)

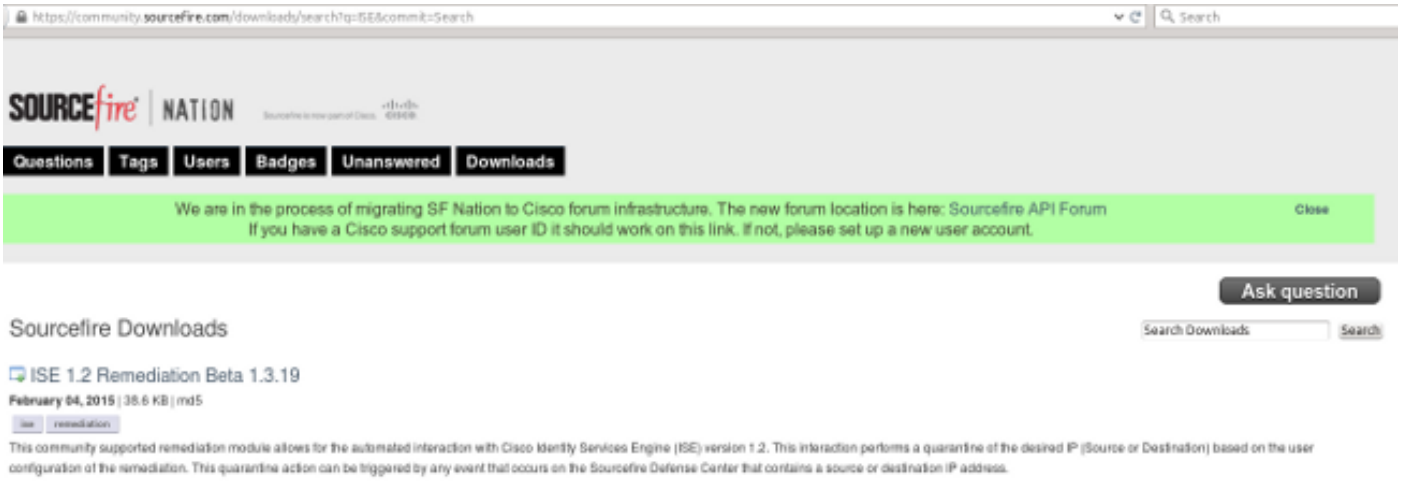
Stratégie de contrôle d'accès

Après avoir installé les licences appropriées et ajouté le périphérique FirePower, accédez à **Policies > Access Control** et créez la stratégie d'accès utilisée afin de supprimer le trafic HTTP vers 172.16.32.1 :

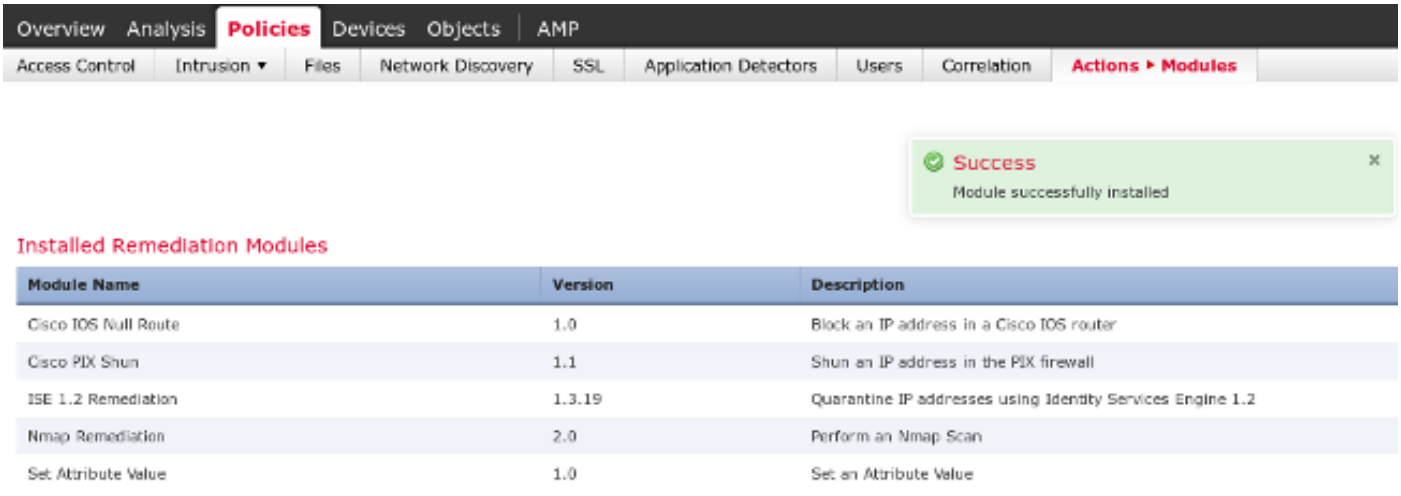
Tout autre trafic est accepté.

Module de correction ISE

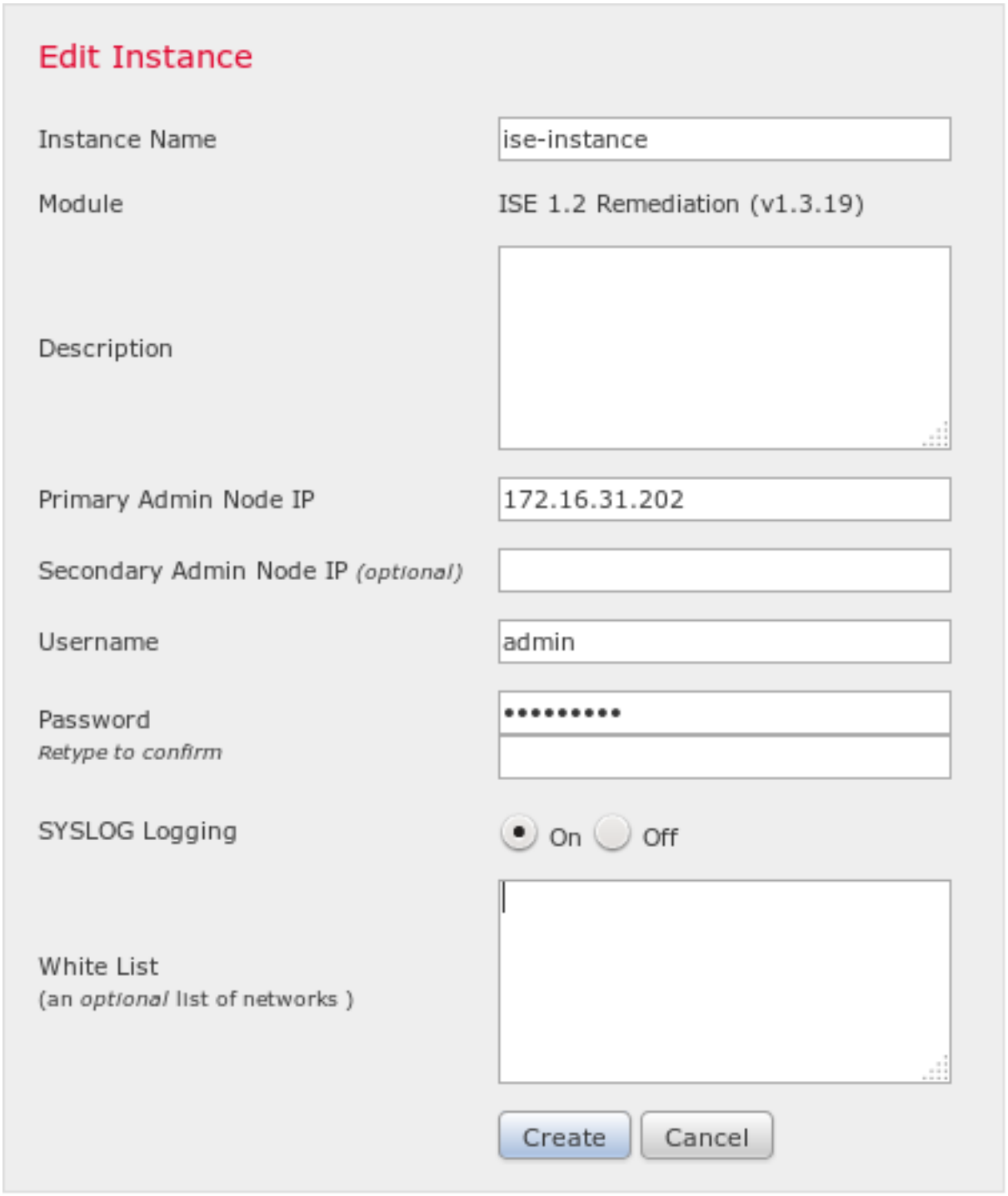
La version actuelle du module ISE qui est partagée sur le portail communautaire est *ISE 1.2 Remediation Beta 1.3.19* :



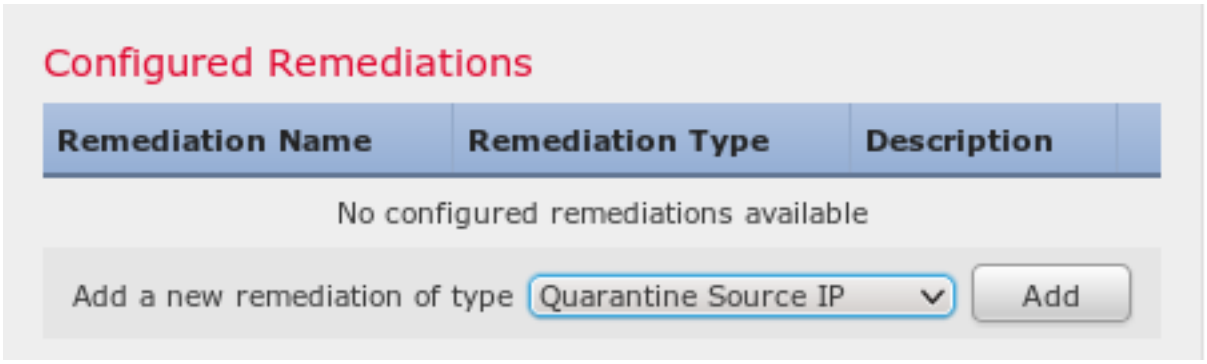
Accédez à **Politiques > Actions > Corrections > Modules** et installez le fichier :



L'instance correcte doit ensuite être créée. Accédez à **Stratégies > Actions > Corrections > Instances** et indiquez l'adresse IP du noeud Administration des stratégies (PAN), ainsi que les informations d'identification d'administration ISE nécessaires pour l'API REST (un utilisateur distinct avec le rôle *Administrateur ERS* est recommandé) :

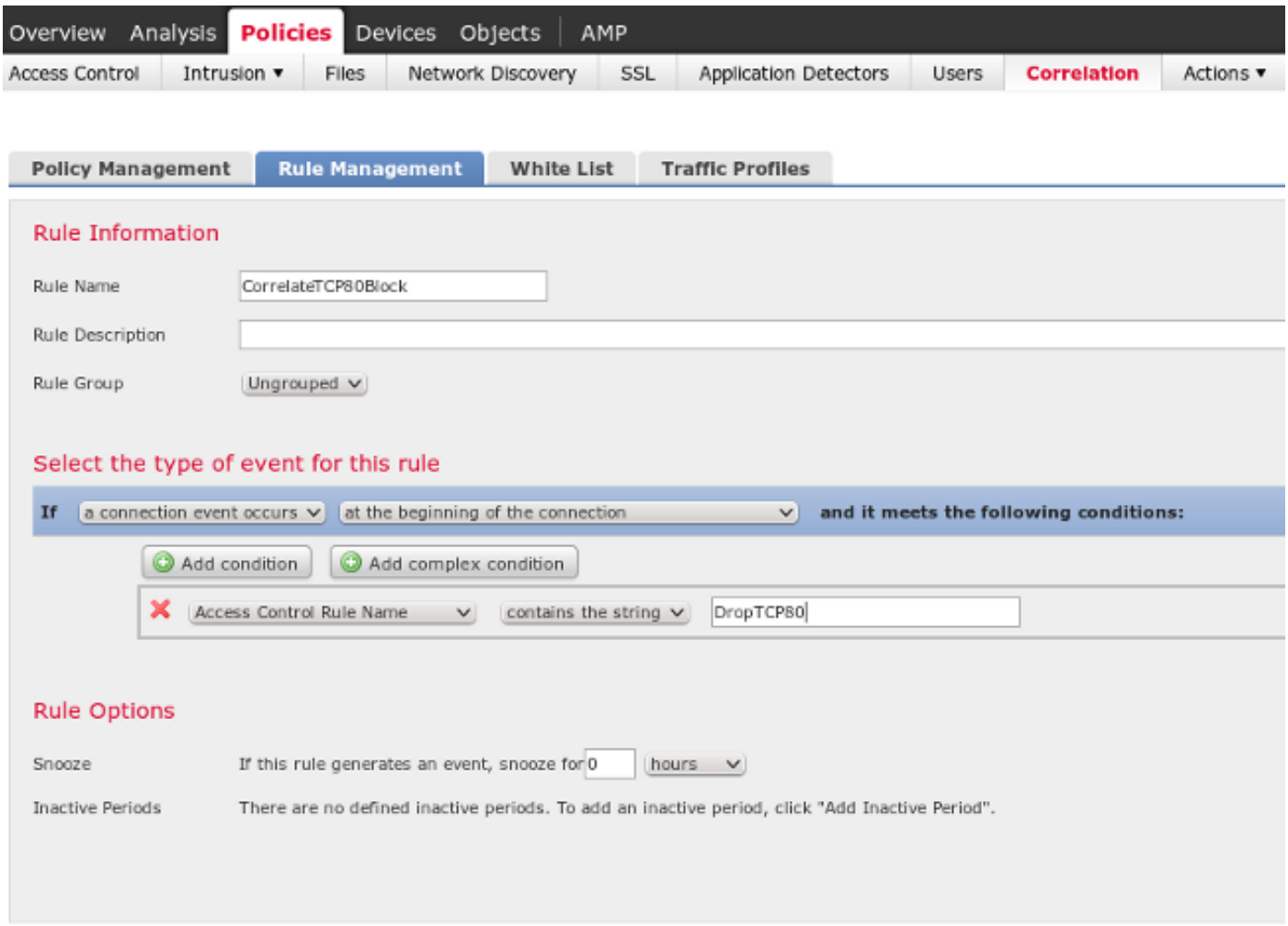


L'adresse IP source (pirate) doit également être utilisée pour la correction :

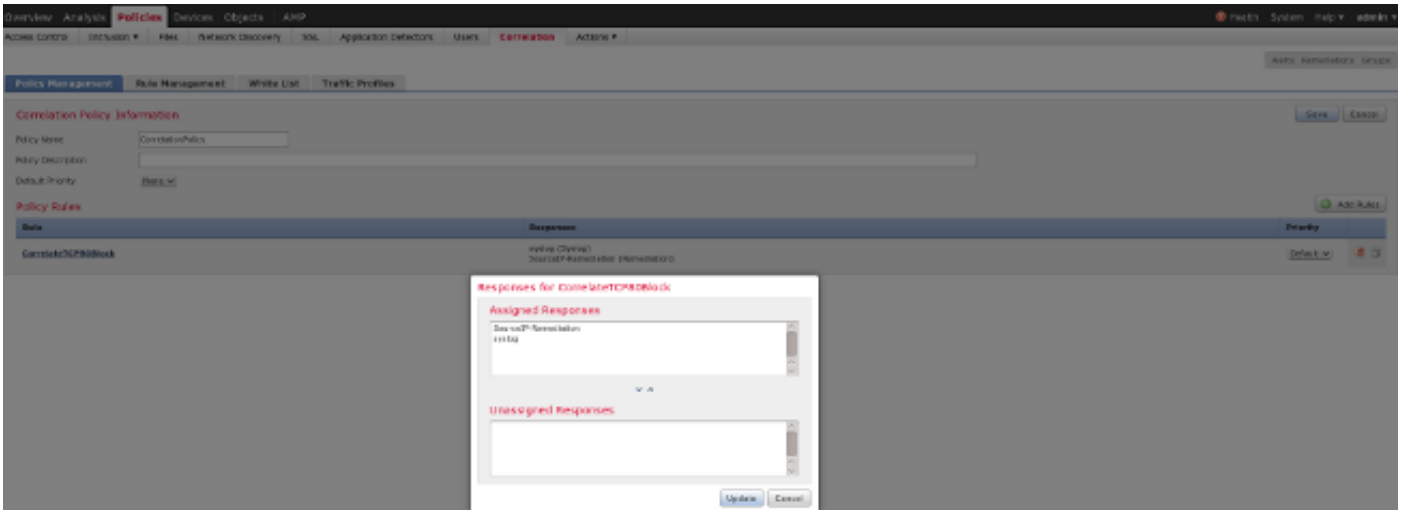


Stratégie de corrélation

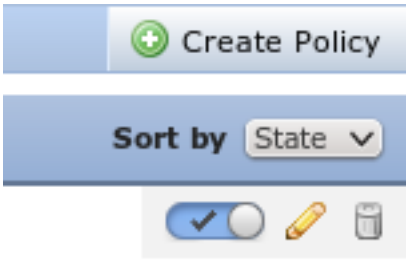
Vous devez maintenant configurer une règle de corrélation spécifique. Cette règle est déclenchée au début de la connexion qui correspond à la règle de contrôle d'accès précédemment configurée (*DropTCP80*). Afin de configurer la règle, accédez à **Politiques > Corrélation > Gestion des règles** :



Cette règle est utilisée dans la stratégie de corrélation. Accédez à **Stratégies > Corrélation > Gestion des stratégies** afin de créer une nouvelle stratégie, puis ajoutez la règle configurée. Cliquez sur **Remediate** à droite et ajoutez deux actions : **correction pour sourceIP** (configuré précédemment) et **syslog** :



Assurez-vous d'activer la stratégie de corrélation :



ASA

Un ASA qui agit comme une passerelle VPN est configuré afin d'utiliser l'ISE pour l'authentification. Il est également nécessaire d'activer la comptabilité et la CoA RADIUS :

```
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
```

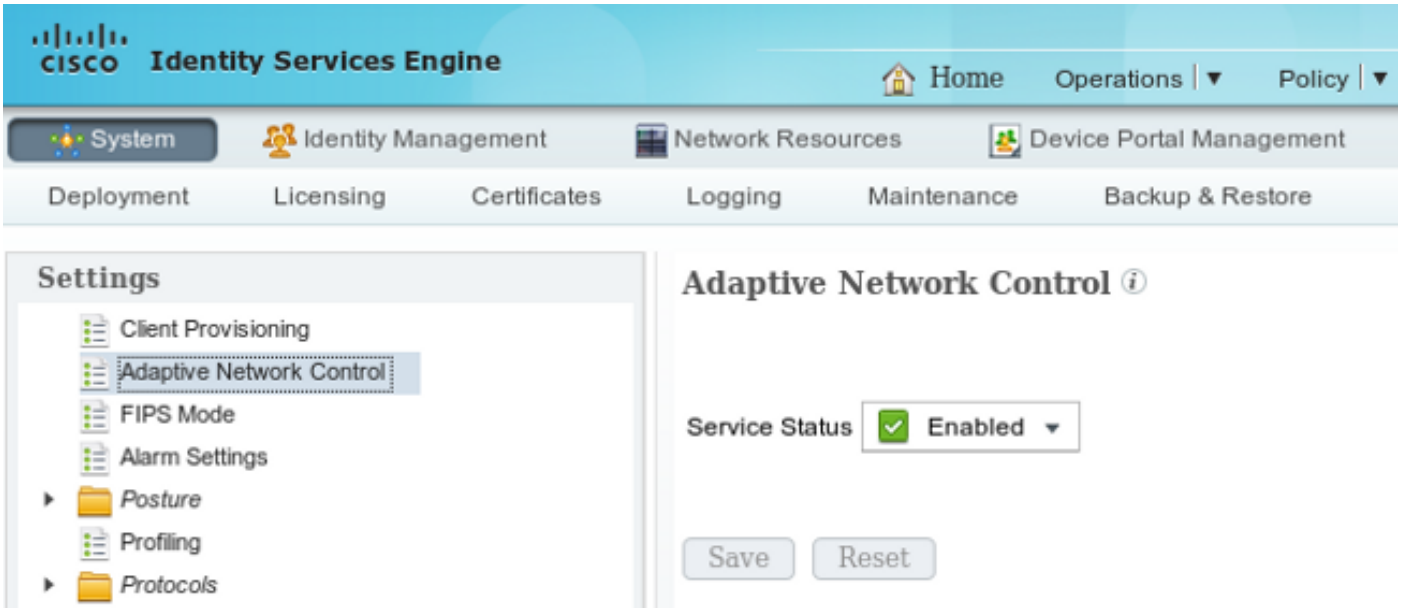
ISE

Configurer le périphérique d'accès au réseau (NAD)

Accédez à **Administration > Network Devices** et ajoutez l'ASA qui agit en tant que client RADIUS.

Activer le contrôle réseau adaptatif

Accédez à **Administration > System > Settings > Adaptive Network Control** afin d'activer l'API et la fonctionnalité de quarantaine :



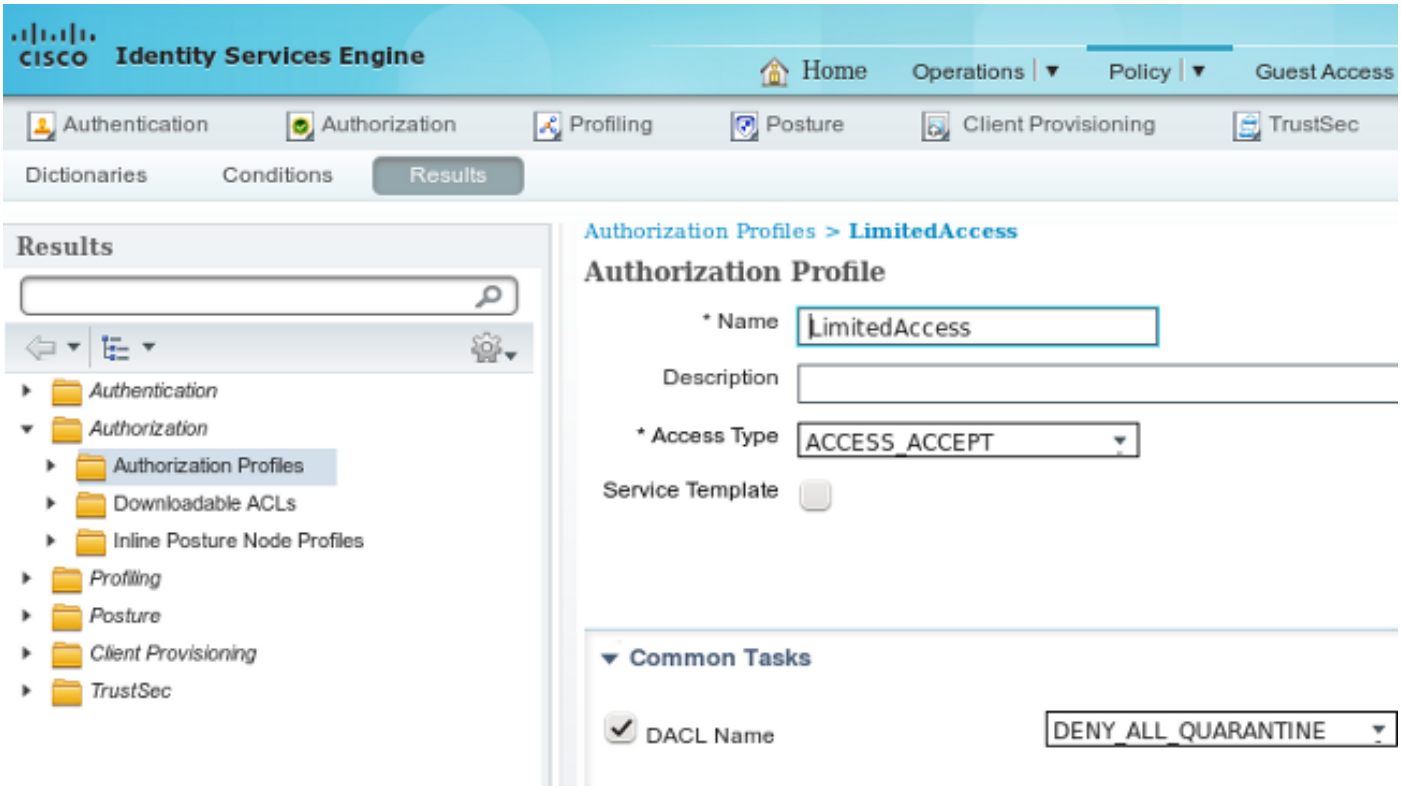
Note: Dans les versions 1.3 et antérieures, cette fonctionnalité est appelée *Service de protection des points de terminaison*.

DACL de quarantaine

Afin de créer une liste de contrôle d'accès téléchargeable (DACL) utilisée pour les hôtes mis en quarantaine, accédez à **Stratégie > Résultats > Autorisation > Liste de contrôle d'accès téléchargeable**.

Profil d'autorisation pour la quarantaine

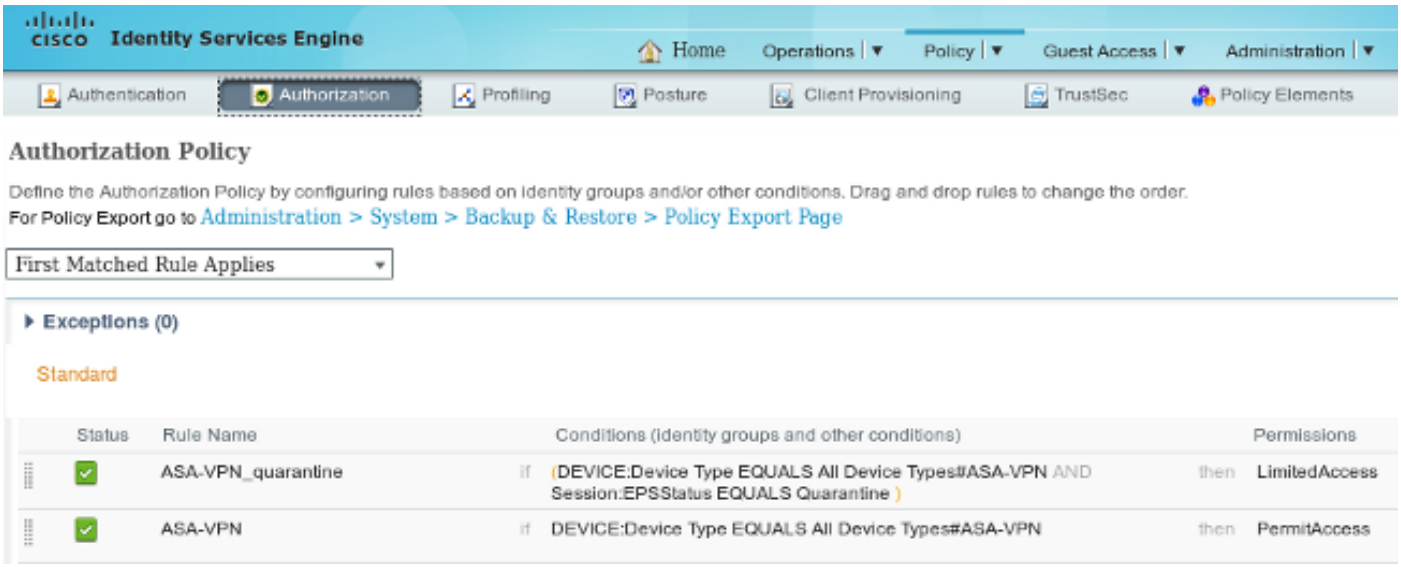
Accédez à **Stratégie > Résultats > Autorisation > Profil d'autorisation** et créez un profil d'autorisation avec la nouvelle DACL :



Règles d'autorisation

Vous devez créer deux règles d'autorisation. La première règle (ASA-VPN) fournit un accès complet à toutes les sessions VPN terminées sur l'ASA. La règle *ASA-VPN_quarantine* est utilisée pour la session VPN réauthentifiée lorsque l'hôte est déjà en quarantaine (accès réseau limité fourni).

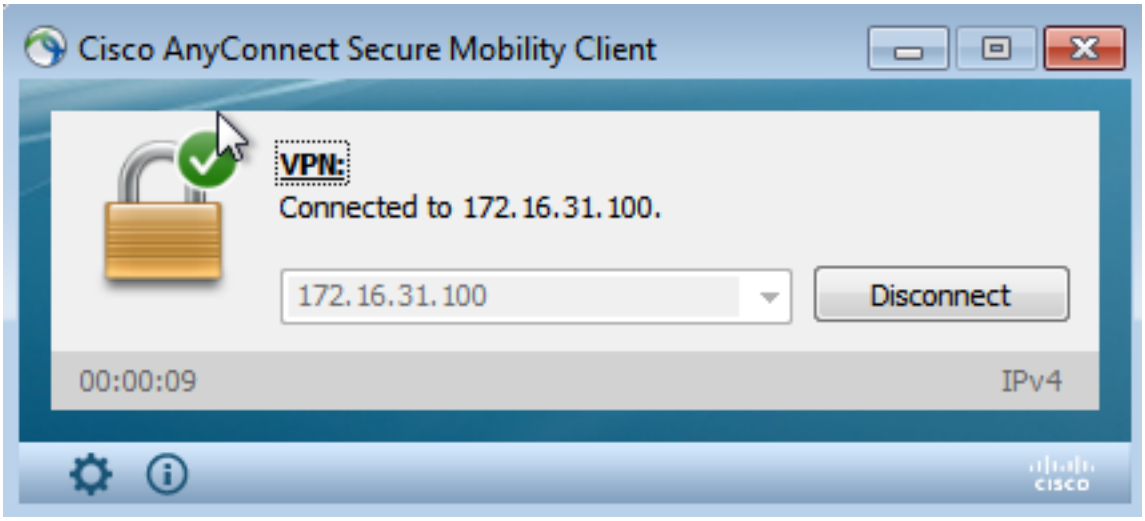
Pour créer ces règles, accédez à **Policy > Authorization** :



Vérification

Utilisez les informations fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

AnyConnect lance une session VPN ASA



L'ASA crée la session sans DACL (accès réseau complet) :

```
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>
```

Tentatives d'accès utilisateur

Une fois que l'utilisateur tente d'accéder à http://172.16.32.1, la stratégie d'accès est atteinte, le trafic correspondant est bloqué en ligne et le message syslog est envoyé à partir de l'adresse IP de gestion FirePower :

```
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,
```

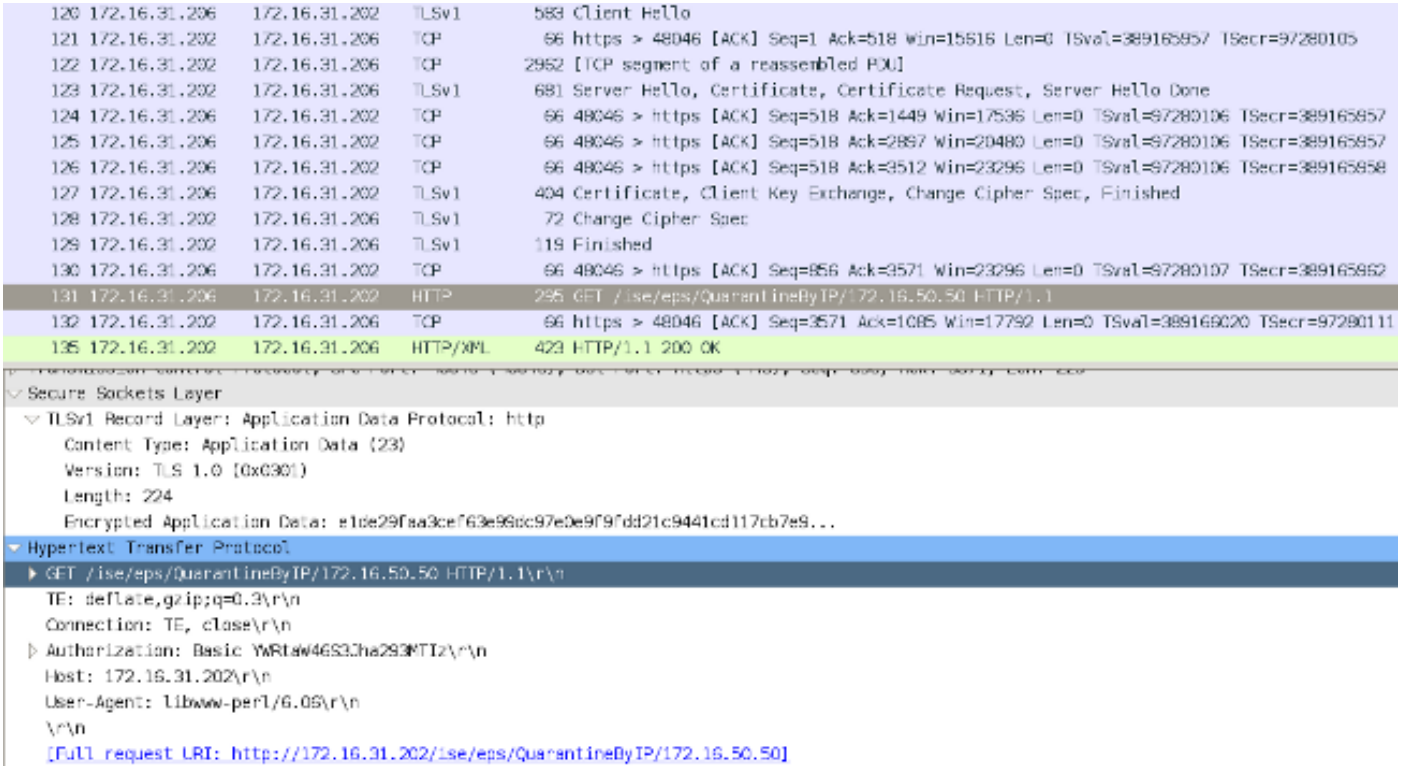
```
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: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

Atteinte à la stratégie de corrélation FireSight

La stratégie de corrélation FireSight Management (Defense Center) est activée, ce qui est signalé par le message syslog envoyé par Defense Center :

```
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)
```

Àce stade, Defense Center utilise l'appel d'API REST (quarantaine) à l'ISE, qui est une session HTTPS et peut être déchiffré dans Wireshark (avec le plug-in SSL (Secure Sockets Layer) et la clé privée du certificat administratif PAN) :



Dans la requête GET, l'adresse IP du pirate est transmise (172.16.50.50) et cet hôte est mis en quarantaine par l'ISE.

Accédez à **Analysis > Correlation > Status** afin de confirmer la correction réussie :

ISE effectue la quarantaine et envoie la CoA

Àce stade, ISE *prrt-management.log* indique que la CoA doit être envoyée :

```
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
```

Le runtime (prrt-server.log) envoie le message de *fin* CoA au NAD, qui met fin à la session (ASA) :

```
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
```

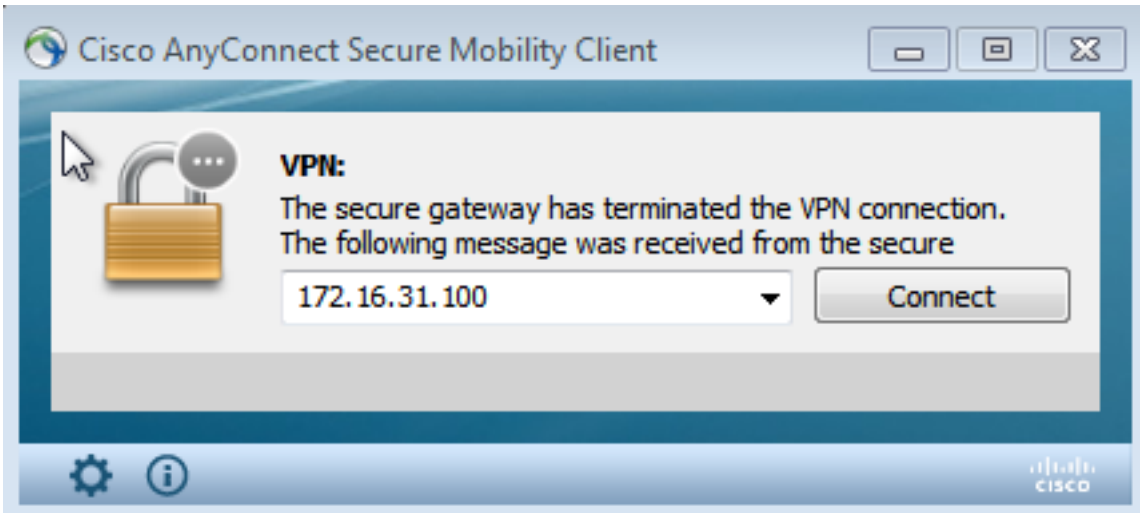
Le *ise.psc* envoie une notification similaire à ceci :

```
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
```

Lorsque vous naviguez jusqu'à **Operations > Authentication**, il doit afficher *Dynamic Authorization réussi*.

La session VPN est déconnectée

L'utilisateur final envoie une notification afin d'indiquer que la session est déconnectée (pour 802.1x/MAB/invité filaire/sans fil, ce processus est transparent) :

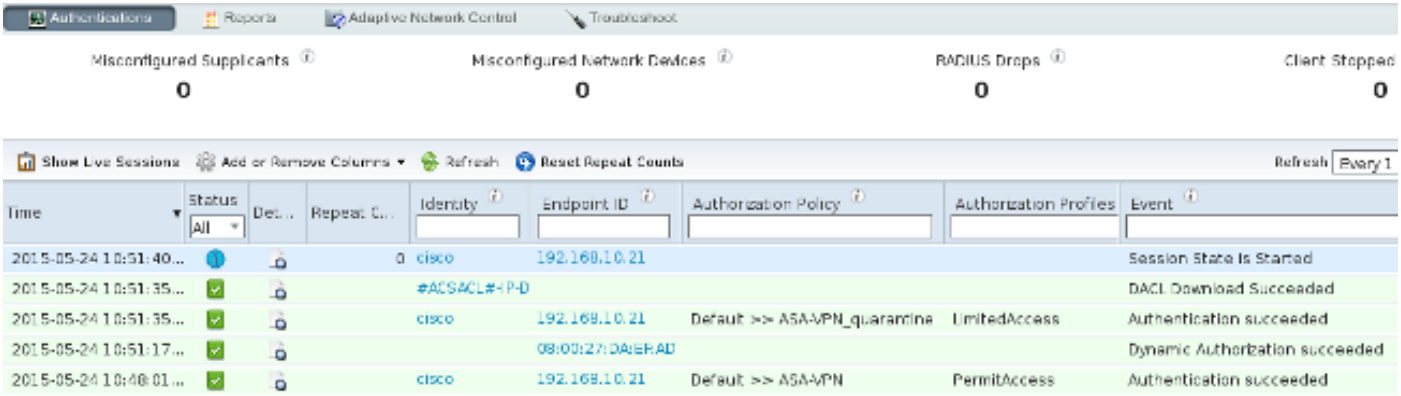


Les détails des journaux Cisco AnyConnect indiquent :

```
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
```

Session VPN avec accès limité (quarantaine)

Comme *le VPN toujours actif* est configuré, la nouvelle session est immédiatement créée. Cette fois, la règle ISE *ASA-VPN_quarantine* est activée, ce qui fournit l'accès réseau limité :



Note: La DACL est téléchargée dans une requête RADIUS distincte.

Une session avec un accès limité peut être vérifiée sur l'ASA avec la commande CLI **show vpn-sessiondb detail anyconnect** :

```
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
```

Dépannage

Cette section fournit des renseignements qui vous permettront de régler les problèmes de configuration.

FireSight (Centre de défense)

Le script de conversion ISE se trouve à cet emplacement :

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

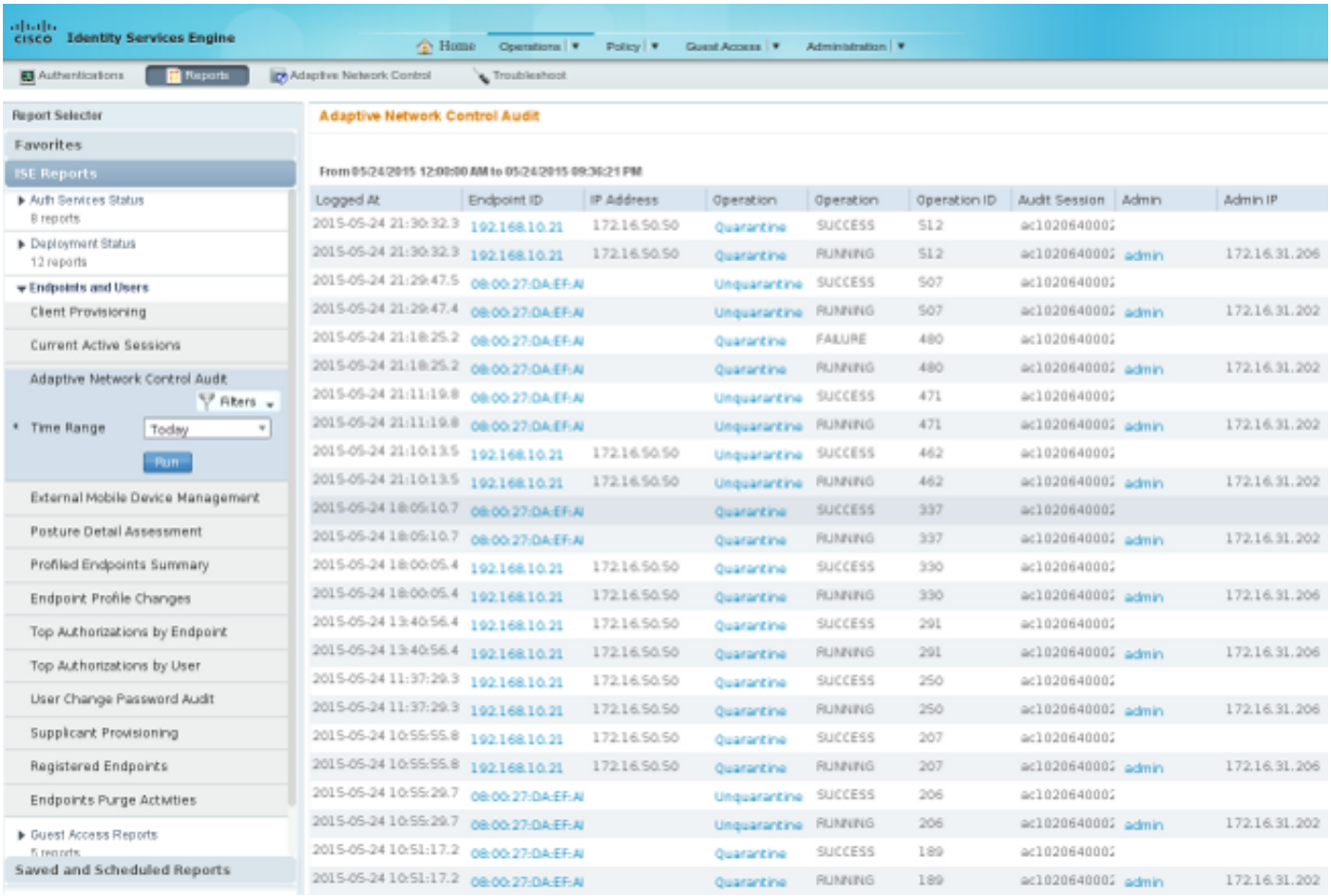
Il s'agit d'un script *perl* simple qui utilise le sous-système de journalisation SourceFire (SF) standard. Une fois la correction exécutée, vous pouvez confirmer les résultats via le */var/log/messages* :

```
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

Il est important d'activer le service Adaptive Network Control sur ISE. Pour afficher les journaux détaillés dans un processus d'exécution (*prrt-management.log* et *prrt-server.log*), vous devez activer le niveau DEBUG pour Runtime-AAA. Accédez à **Administration > System > Logging > Debug Log Configuration** afin d'activer les débogages.

Vous pouvez également accéder à **Operations > Reports > Endpoint and Users > Adaptive Network Control Audit** afin d'afficher les informations pour chaque tentative et résultat d'une demande de quarantaine :



Bugs

Référez-vous à l'ID de bogue Cisco CSCuu41058 (incohérence de la quarantaine des terminaux ISE 1.4 et échec VPN) pour des informations sur un bogue ISE lié aux échecs de session VPN (802.1x/MAB fonctionne correctement).

Informations connexes

- Configurez l'intégration du WSA au moyen des services ISE TrustSec
- Intégration ISE version 1.3 pxGrid avec l'application IPS pxLog
- Guide de l'administrateur de Cisco Identity Services Engine, version 1.4 - Configuration du contrôle réseau adaptatif
- Guide de référence de l'API de Cisco Identity Services Engine, version 1.2 - Présentation de l'API de services REST externes
- Guide de référence de l'API Cisco Identity Services Engine, version 1.2 - Présentation des API REST de surveillance
- Guide de l'administrateur de Cisco Identity Services Engine, version 1.3

- Documentation et assistance techniques - Cisco Systems