

# Configure Remediation Services with ISE and FirePower Integration



Document ID: 119370

Contributed by Michal Garcarz, Cisco TAC Engineer.  
Nov 17, 2015

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used

#### Configure

- Network Diagram
- FireSight Management Center (Defence Center)
  - ISE Remediation Module
  - Correlation Policy
- ASA
- ISE
  - Configure Network Access Device (NAD)
  - Enable Adaptive Network Control
  - Quarantine DACL
  - Authorization Profile for Quarantine
  - Authorization Rules

#### Verify

- AnyConnect Initiates ASA VPN Session
- FireSight Correlation Policy Hit
- ISE Performs Quarantine and Sends CoA
- VPN Session is Disconnected

#### Troubleshoot

- FireSight (Defence Center)
- ISE
- Bugs

#### Related Information

## Introduction

This document describes how to use the remediation module on a Cisco FireSight appliance in order to detect attacks and automatically remediate the attacker with the use of the Cisco Identity Service Engine (ISE) as a policy server. The example that is provided in this document describes the method that is used for remediation of a remote VPN user who authenticates via the ISE, but it can also be used for an 802.1x/MAB/WebAuth wired or wireless user.

**Note:** The remediation module that is referenced in this document is not officially supported by Cisco. It is shared on a community portal and can be used by anyone. In Versions 5.4 and later, there is also a newer remediation module available that is based on the *pxGrid* protocol. This module is not supported in Version 6.0 but is planned to be supported in future versions.

# Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Adaptive Security Appliance (ASA) VPN configuration
- Cisco AnyConnect Secure Mobility Client configuration
- Cisco FireSight basic configuration
- Cisco FirePower basic configuration
- Cisco ISE configuration

## Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco ASA Version 9.3 or later
- Cisco ISE software Versions 1.3 and later
- Cisco AnyConnect Secure Mobility Client Versions 3.0 and later
- Cisco FireSight Management Center Version 5.4
- Cisco FirePower Version 5.4 (Virtual Machine (VM))

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.

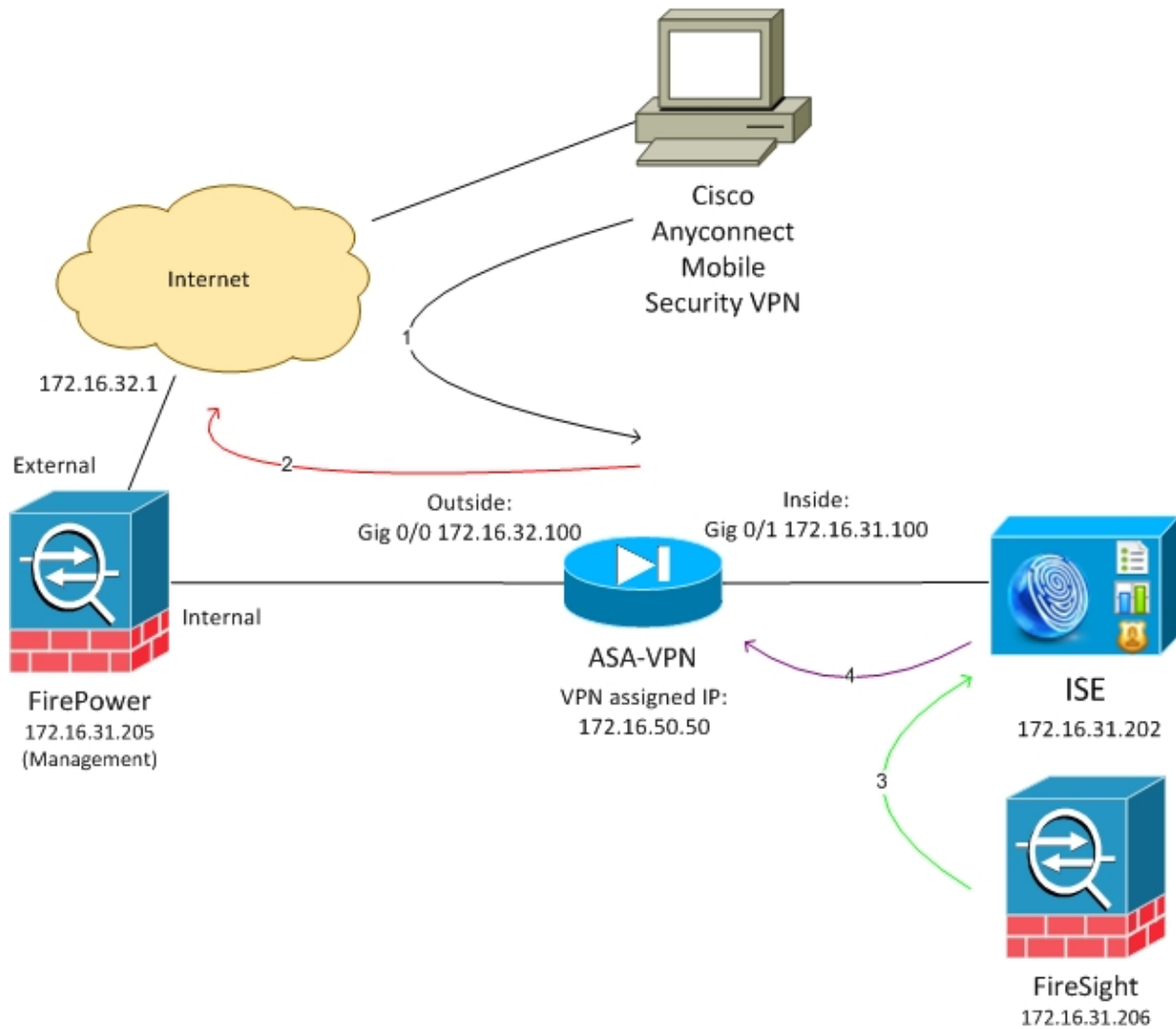
## Configure

Use the information that is provided in this section in order to configure your system.

**Note:** Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

## Network Diagram

The example that is described in this document uses this network setup:



Here is the flow for this network setup:

1. The user initiates a remote VPN session with the ASA (via Cisco AnyConnect Secure Mobility Version 4.0).
2. The user attempts to access `http://172.16.32.1`. (The traffic moves via FirePower, which is installed on the VM and is managed by FireSight.)
3. FirePower is configured so that it blocks (inline) that specific traffic (access policies), but it also has a Correlation Policy that is triggered. As a result, it initiates the ISE remediation via REST Application Programming Interface (API) (the *QuarantineByIP* method).
4. Once the ISE receives the REST API call, it looks up for the session and sends a RADIUS Change of Authorization (CoA) to the ASA, which terminates that session.
5. The ASA disconnects the VPN user. Since AnyConnect is configured with *Always-on* VPN access, a new session is established; however, this time a different ISE Authorization rule is matched (for quarantined hosts) and limited network access is provided. At this stage, it does not matter how the user connects and authenticates to the network; as long as the ISE is used for authentication and authorization, the user has limited network access due to quarantine.

As previously mentioned, this scenario works for any type of authenticated session (VPN, wired 802.1x/MAB/Webauth, wireless 802.1x/MAB/Webauth) as long as the ISE is used for authentication and the

network access device supports the RADIUS CoA (all modern Cisco devices).

**Tip:** In order to move the user out of quarantine, you can use the ISE GUI. Future versions of the remediation module might also support it.

## FirePower

**Note:** A VM appliance is used for the example that is described in this document. Only the initial configuration is performed via the CLI. All of the policies are configured from Cisco Defence Center. For more details, refer to the Related Information section of this document.

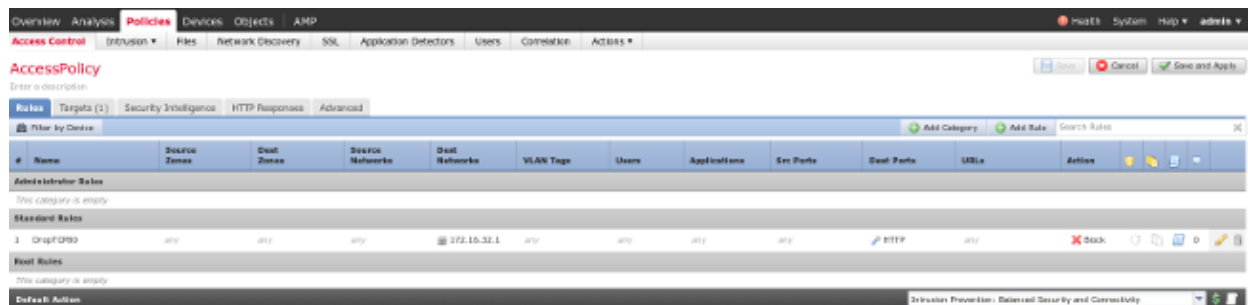
The VM has three interfaces, one for management and two for inline inspection (internal/external).

All of the traffic from the VPN users moves via FirePower.

## FireSight Management Center (Defence Center)

### Access Control Policy

After you install the correct licenses and add the FirePower device, navigate to **Policies > Access Control** and create the Access Policy that is used in order to drop the HTTP traffic to 172.16.32.1:



All other traffic is accepted.

### ISE Remediation Module

The current version of the ISE module that is shared on the community portal is *ISE 1.2 Remediation Beta 1.3.19*:



Navigate to **Policies > Actions > Remediations > Modules** and install the file:

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

The correct instance should then be created. Navigate to **Policies > Actions > Remediations > Instances** and provide the IP address of the Policy Administration Node (PAN), along with the ISE administrative credentials that are needed for the REST API (a separate user with the *ERS Admin* role is recommended):

**Edit Instance**

Instance Name: ise-instance

Module: ISE 1.2 Remediation (v1.3.19)

Description: [Empty text area]

Primary Admin Node IP: 172.16.31.202

Secondary Admin Node IP (optional): [Empty text field]

Username: admin

Password: [Masked password field]

Retype to confirm: [Empty text field]

SYSLOG Logging:  On  Off

White List (an optional list of networks): [Empty text area]

[Create] [Cancel]

The source IP address (attacker) should also be used for remediation:

### Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type

## Correlation Policy

You must now configure a specific correlation rule. This rule is triggered at the start of the connection that matches the previously configured access control rule (*DropTCP80*). In order to configure the rule, navigate to **Policies > Correlation > Rule Management**:

Overview Analysis **Policies** Devices Objects AMP

Access Control Intrusion Files Network Discovery SSL Application Detectors Users **Correlation** Actions

Policy Management **Rule Management** White List Traffic Profiles

### Rule Information

Rule Name:

Rule Description:

Rule Group:

### Select the type of event for this rule

If  at the beginning of the connection and it meets the following conditions:

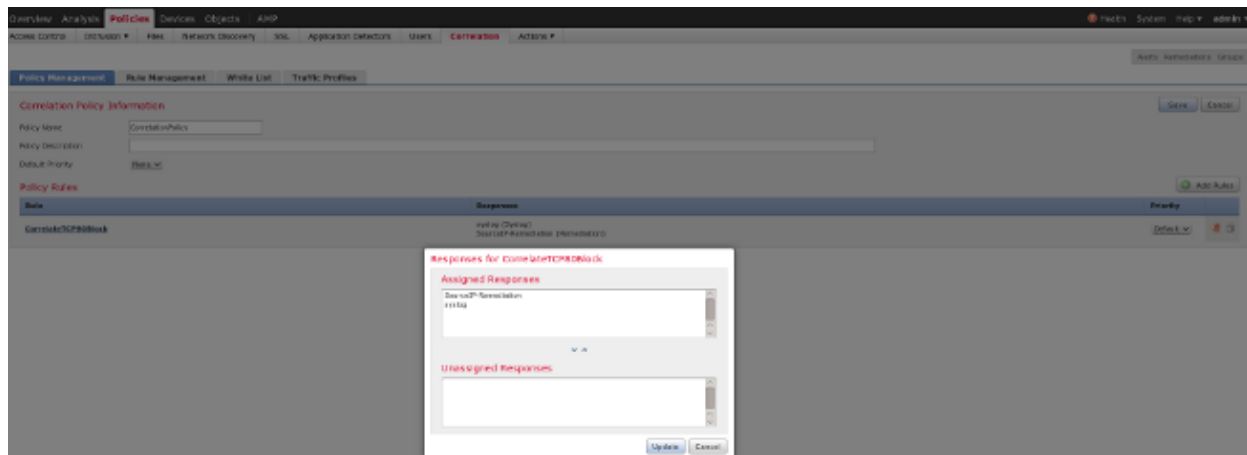
contains the string

### Rule Options

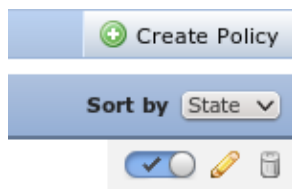
Snooze: If this rule generates an event, snooze for  hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

This rule is used in the Correlation Policy. Navigate to **Policies > Correlation > Policy Management** in order to create a new policy, and then add the configured rule. Click **Remediate** on the right and add two actions: **remediation for sourceIP** (configured earlier) and **syslog**:



Ensure that you enable the correlation policy:



## ASA

An ASA that acts as a VPN gateway is configured in order to use the ISE for authentication. It is also necessary to enable accounting and the RADIUS CoA:

```
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
```

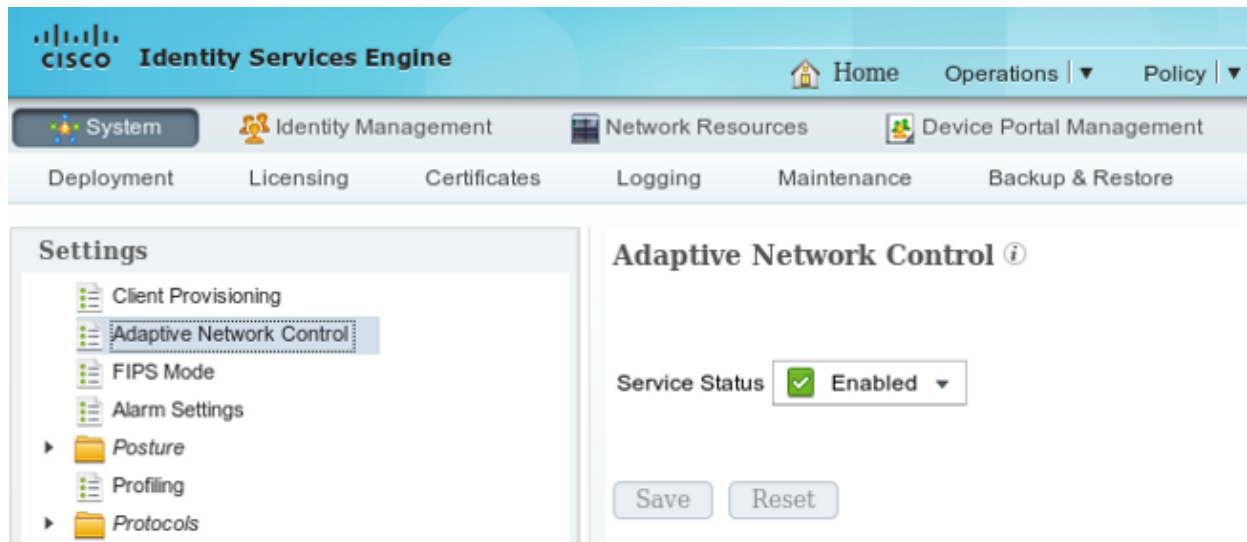
## ISE

### Configure Network Access Device (NAD)

Navigate to **Administration > Network Devices** and add the ASA that acts as a RADIUS client.

## Enable Adaptive Network Control

Navigate to **Administration > System > Settings > Adaptive Network Control** in order to enable quarantine API and functionality:



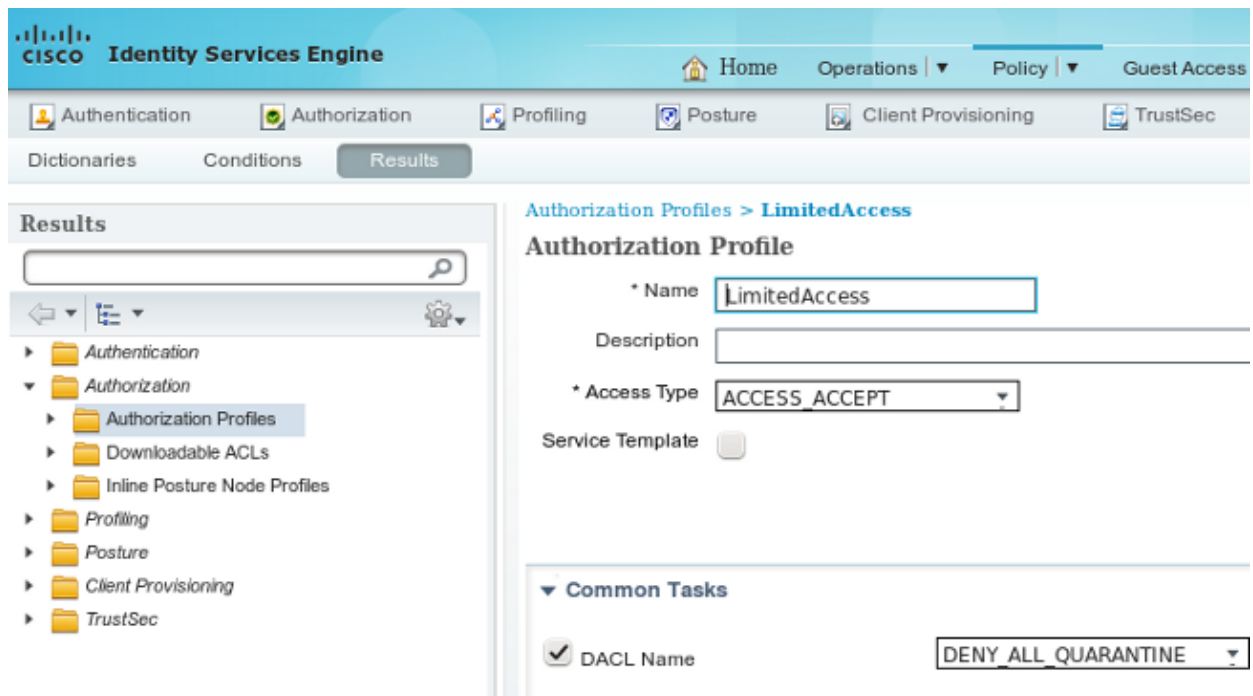
**Note:** In Versions 1.3 and earlier, this feature is called *Endpoint Protection Service*.

## Quarantine DACL

In order to create a Downloadable Access Control List (DACL) that is used for the quarantined hosts, navigate to **Policy > Results > Authorization > Downloadable ACL**.

## Authorization Profile for Quarantine

Navigate to **Policy > Results > Authorization > Authorization Profile** and create an authorization profile with the new DACL:

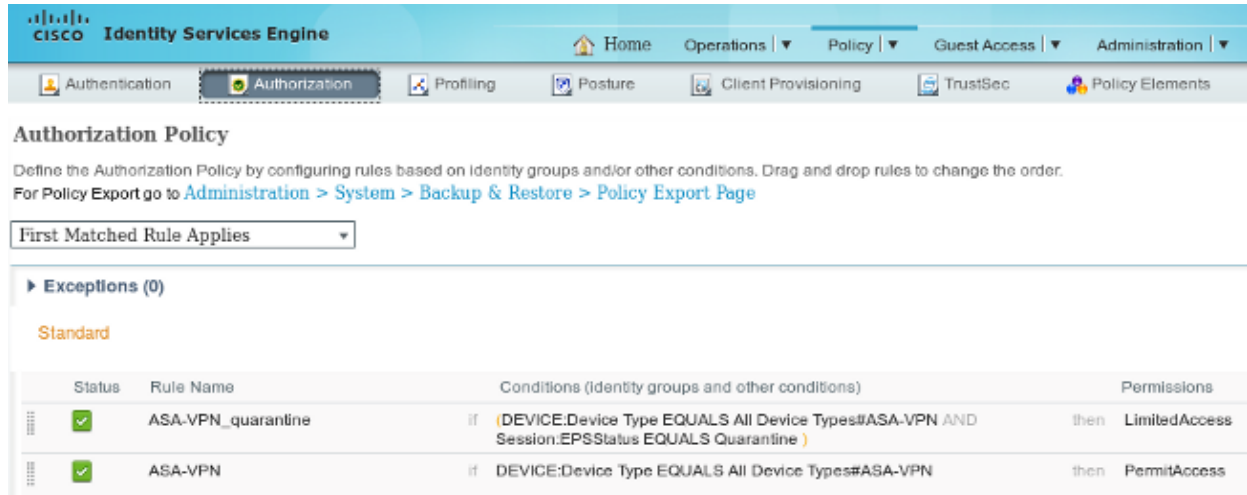




## Authorization Rules

You must create two authorization rules. The first rule (ASA-VPN) provides full access for all of the VPN sessions that are terminated on the ASA. The rule *ASA-VPN\_quarantine* is hit for the reauthenticated VPN session when the host is already in quarantine (limited network access is provided).

In order to create these rules, navigate to **Policy > Authorization**:



**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)

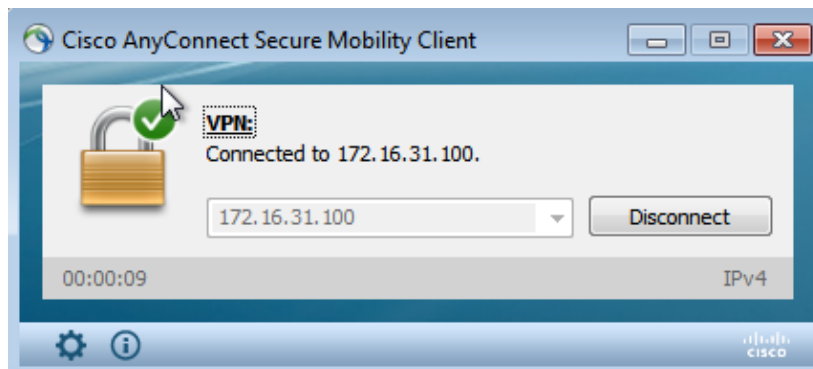
Standard

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

## Verify

Use the information that is provided in this section in order to verify that your configuration works properly.

### AnyConnect Initiates ASA VPN Session



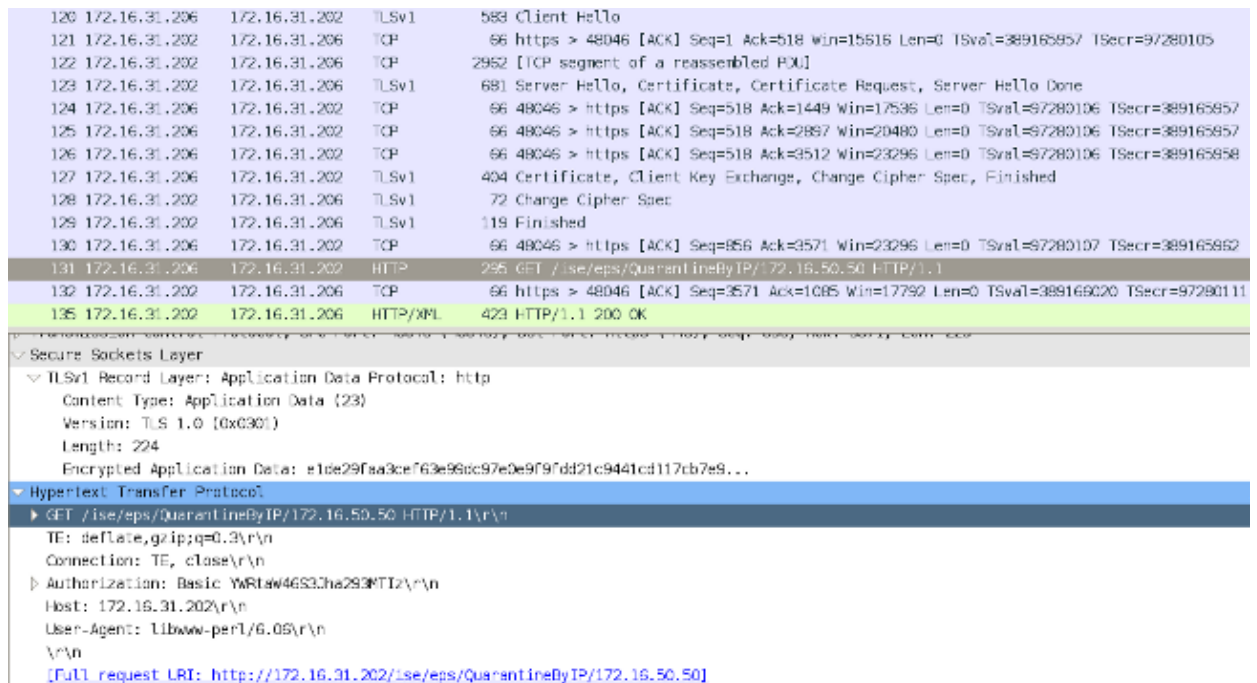
The ASA creates the session without any DACL (full network access):

```
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
```





In GET request for the IP address of the attacker is passed (172.16.50.50), and that host is quarantined by the ISE.

Navigate to **Analysis > Correlation > Status** in order to confirm the successful remediation:



## ISE Performs Quarantine and Sends CoA

At this stage, the ISE `prrt-management.log` notifies that the CoA should be sent:

```
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
```

The runtime (`prrt-server.log`) sends the CoA `terminate` message to the NAD, which terminates the 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

```

The *ise.psc* sends a notification similar to this:

```

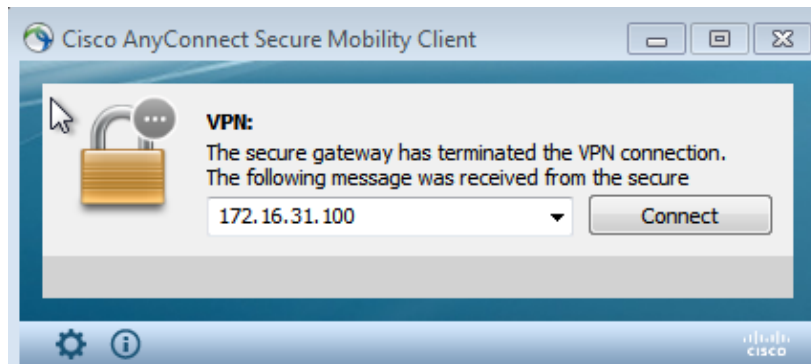
INFO [admin-http-pool51][] cisco.cpm.eps.prprt.PrprtManager -:::- PrprtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault

```

When you navigate to **Operations > Authentication**, it should show *Dynamic Authorization succeeded*.

## VPN Session is Disconnected

The end user sends a notification in order to indicate that the session is disconnected (for 802.1x/MAB/guest wired/wireless, this process is transparent):



Details from the Cisco AnyConnect logs show:

```

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 Session with Limited Access (Quarantine)

Because *always-on VPN* is configured, the new session is built immediately. This time, the ISE *ASA-VPN\_quarantine* rule is hit, which provides the limited network access:

Time	Status	Dec...	Repea: C...	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:DAE8:AD			Dynamic Authorbation succeeded
2015-05-24 10:48:01...				cisco	192.168.10.21	Default -> ASA-VPN	PermitAccess	Authentication succeeded

**Note:** The DACL is downloaded in a separate RADIUS request.

A session with limited access can be verified on the ASA with the **show vpn-sessiondb detail anyconnect** CLI command:

```
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
```

## Troubleshoot

This section provides information that you can use in order to troubleshoot your configuration.

### FireSight (Defence Center)

The ISE remediation script resides in this location:

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

This is a simple *perl* script that uses the standard SourceFire (SF) logging subsystem. Once remediation is executed, you can confirm the results via the */var/log/messages*:

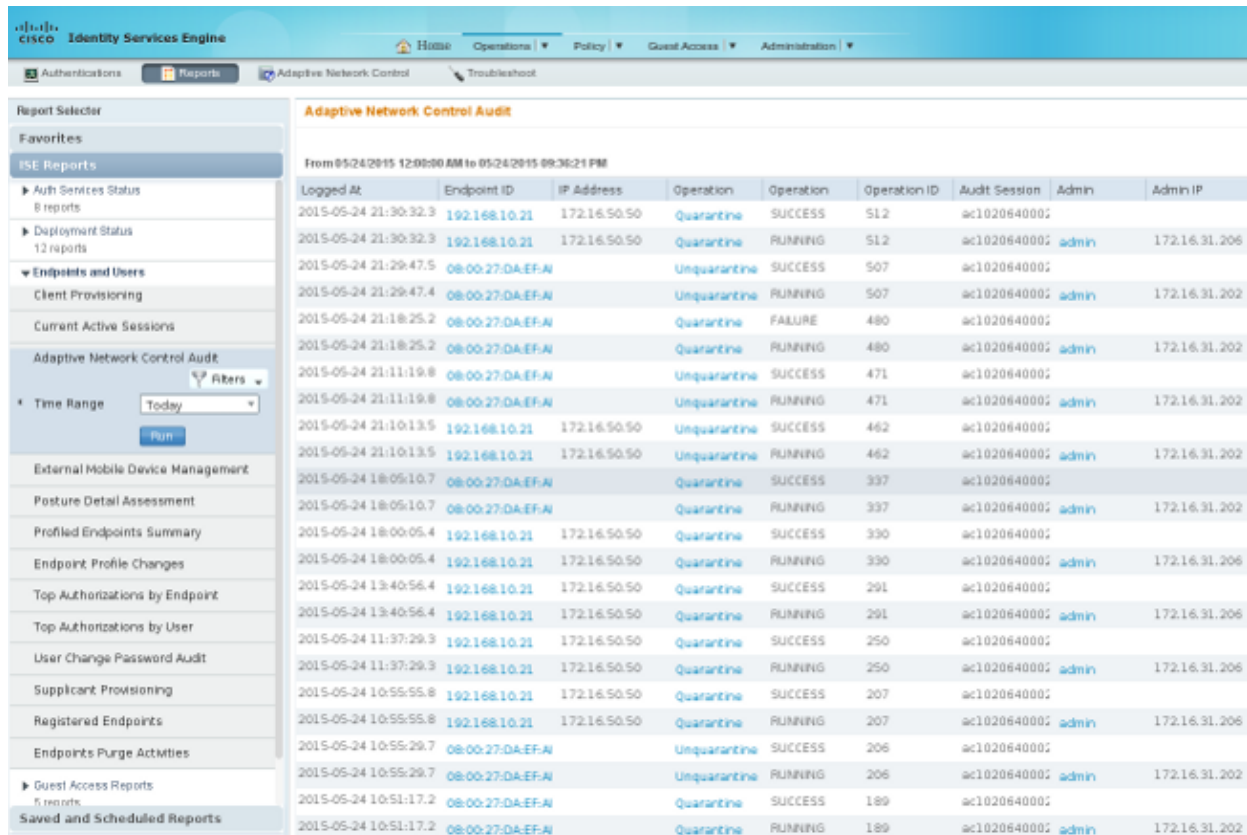
```
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
```

```
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

It is important that you enable the Adaptive Network Control service on the ISE. In order to view the detailed logs in a runtime process (*prrt-management.log* and *prrt-server.log*), you must enable the DEBUG level for Runtime-AAA. Navigate to **Administration > System > Logging > Debug Log Configuration** in order to enable the debugs.

You can also navigate to **Operations > Reports > Endpoint and Users > Adaptive Network Control Audit** in order to view the information for every attempt and result of a quarantine request:



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

## Bugs

Refer to Cisco bug ID CSCuu41058 (ISE 1.4 Endpoint Quarantine inconsistency and VPN failure) for information about an ISE bug that is related to VPN session failures (802.1x/MAB works fine).

## Related Information

- [Configure WSA Integration with ISE for TrustSec Aware Services](#)
- [ISE Version 1.3 pxGrid Integration with IPS pxLog Application](#)
- [Cisco Identity Services Engine Administrator Guide, Release 1.4 – Setup Adaptive Network Control](#)
- [Cisco Identity Services Engine API Reference Guide, Release 1.2 – Introduction to External RESTful Services API](#)

- **Cisco Identity Services Engine API Reference Guide, Release 1.2 – Introduction to the Monitoring REST APIs**
- **Cisco Identity Services Engine Administrator Guide, Release 1.3**
- **Technical Support & Documentation – Cisco Systems**

---

Updated: Nov 17, 2015

Document ID: 119370

---