

Integrazione ISE e FirePower - esempio di servizio di ripristino

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[FirePower](#)

[Centro di gestione FireSight \(Defense Center\)](#)

[Policy di controllo dell'accesso](#)

[ISE Remediation Module](#)

[Criteri di correlazione](#)

[ASA](#)

[ISE](#)

[Configura dispositivo di accesso alla rete \(NAD\)](#)

[Abilita controllo adattivo della rete](#)

[DACL quarantena](#)

[Profilo di autorizzazione per quarantena](#)

[Regole di autorizzazione](#)

[Verifica](#)

[AnyConnect avvia una sessione VPN ASA](#)

[Tentativi di accesso utente](#)

[Riscontri criteri di correlazione FireSight](#)

[ISE mette in quarantena e invia il CoA](#)

[Sessione VPN disconnessa](#)

[Sessione VPN con accesso limitato \(quarantena\)](#)

[Risoluzione dei problemi](#)

[FireSight \(centro difesa\)](#)

[ISE](#)

[Bug](#)

[Informazioni correlate](#)

[Discussioni correlate nella Cisco Support Community](#)

Introduzione

In questo documento viene descritto come usare il modulo di monitoraggio e aggiornamento su un accessorio Cisco FireSight per rilevare gli attacchi e risolvere automaticamente il problema all'attacco usando Cisco Identity Service Engine (ISE) come policy server. L'esempio fornito in questo documento descrive il metodo usato per il monitoraggio e l'aggiornamento di un utente

VPN remoto che si autentica tramite ISE, ma può essere usato anche per un utente cablato o wireless 802.1x/MAB/WebAuth.

Nota: Il modulo di monitoraggio e aggiornamento a cui si fa riferimento in questo documento non è ufficialmente supportato da Cisco. È condiviso su un portale della community e può essere utilizzato da chiunque. Nelle versioni 5.4 e successive è disponibile anche un nuovo modulo di correzione basato sul protocollo *pxGrid*. Questo modulo non è supportato nella versione 6.0, ma è previsto che lo sia nelle versioni future.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Cisco ASA versione 9.3 o successive
- Software Cisco ISE versione 1.3 e successive
- Cisco AnyConnect Secure Mobility Client versione 3.0 e successive
- Cisco FireSight Management Center versione 5.4
- Cisco FirePower versione 5.4 (macchina virtuale (VM))

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

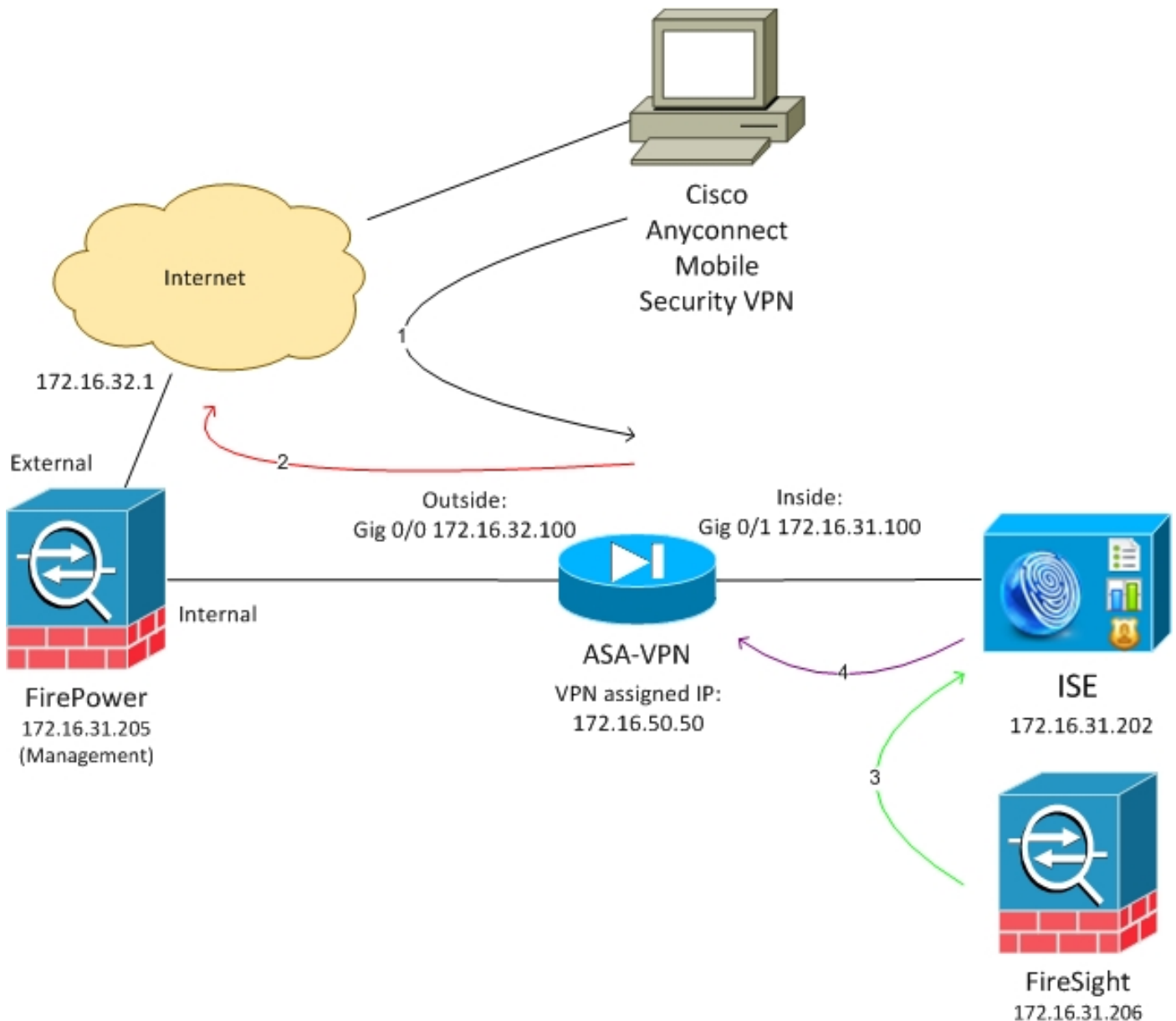
Configurazione

Utilizzare le informazioni fornite in questa sezione per configurare il sistema.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

L'esempio descritto in questo documento utilizza la seguente configurazione della rete:



Di seguito è riportato il flusso per questa configurazione della rete:

1. L'utente avvia una sessione VPN remota con l'ASA (tramite Cisco AnyConnect Secure Mobility versione 4.0).
2. L'utente tenta di accedere a <http://172.16.32.1>. (Il traffico si sposta tramite FirePower, che è installato sulla VM ed è gestito da FireSight.)
3. FirePower è configurato in modo da bloccare (inline) quel traffico specifico (criteri di

accesso), ma ha anche un criterio di correlazione che viene attivato. Di conseguenza, avvia il monitoraggio e l'aggiornamento di ISE tramite l'API REST (*QuarantineByIP* method).

- Una volta ricevuta la chiamata all'API REST, ISE cerca la sessione e invia una modifica di autorizzazione RADIUS (CoA) all'ASA, che termina la sessione.
- L'appliance ASA disconnette l'utente VPN. Poiché AnyConnect è configurato con l'accesso VPN *Always-on*, viene stabilita una nuova sessione; tuttavia, questa volta viene soddisfatta una regola di autorizzazione ISE diversa (per gli host in quarantena) e viene fornito un accesso alla rete limitato. In questa fase, non importa come l'utente si connette e si autentica alla rete; se l'ISE è usato per l'autenticazione e l'autorizzazione, l'utente ha un accesso limitato alla rete a causa della quarantena.

Come accennato in precedenza, questo scenario funziona per qualsiasi tipo di sessione autenticata (VPN, 802.1x cablata/MAB/Webauth, wireless 802.1x/MAB/Webauth) a condizione che l'ISE venga utilizzata per l'autenticazione e che il dispositivo di accesso alla rete supporti RADIUS CoA (tutti i moderni dispositivi Cisco).

Suggerimento: Per spostare l'utente dalla quarantena, è possibile usare l'interfaccia utente grafica di ISE. Anche le versioni future del modulo di correzione potrebbero supportarlo.

FirePower

Nota: Per l'esempio descritto in questo documento viene utilizzato un accessorio VM. Solo la configurazione iniziale viene eseguita dalla CLI. Tutti i criteri sono configurati da Cisco Defense Center. Per ulteriori informazioni, fare riferimento alla sezione [Informazioni correlate](#) di questo documento.

La VM dispone di tre interfacce, una per la gestione e due per l'ispezione in linea (interna/esterna).

Tutto il traffico proveniente dagli utenti VPN si sposta tramite FirePower.

Centro di gestione FireSight (Defense Center)

Policy di controllo dell'accesso

Dopo aver installato le licenze corrette e aver aggiunto il dispositivo FirePower, selezionare **Policies > Access Control** (Policy > Controllo di accesso) e creare i criteri di accesso utilizzati per indirizzare il traffico HTTP a 172.16.32.1:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action
1	HTTP	any	any		172.16.32.1	any	any	any				Block

Tutto il resto del traffico viene accettato.

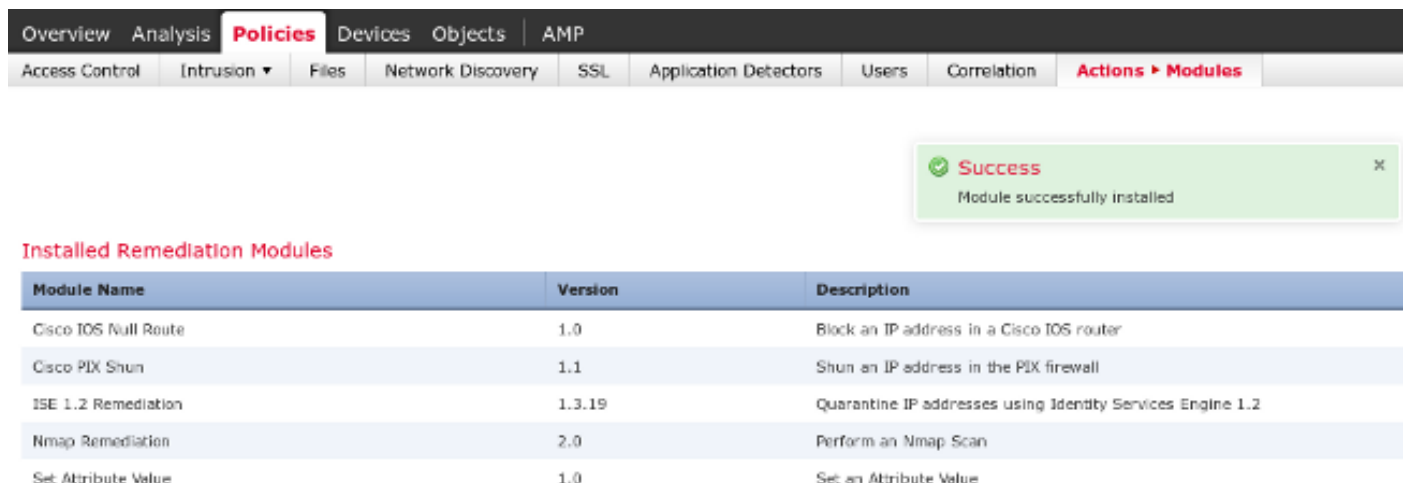
ISE Remediation Module

La versione corrente del modulo ISE condiviso sul portale della community è *ISE 1.2 Remediation Beta 1.3.19*:



The screenshot shows the Sourcefire Downloads page. At the top, there is a navigation bar with 'Questions', 'Tags', 'Users', 'Badges', 'Unanswered', and 'Downloads'. A green banner below the navigation bar states: 'We are in the process of migrating SF Nation to Cisco forum infrastructure. The new forum location is here: Sourcefire API Forum. If you have a Cisco support forum user ID it should work on this link. If not, please set up a new user account.' Below this, there is a search bar and an 'Ask question' button. The main content area is titled 'Sourcefire Downloads' and features a search bar. The first download item is 'ISE 1.2 Remediation Beta 1.3.19', dated February 04, 2015, with a size of 38.6 KB and a file type of md5. A description below the link states: '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.'

Passare a **Criteri > Azioni > Risoluzioni > Moduli** e installare il file:



The screenshot shows the Cisco ISE interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. Below this, there is a sub-navigation bar with 'Access Control', 'Intrusion', 'Files', 'Network Discovery', 'SSL', 'Application Detectors', 'Users', 'Correlation', and 'Actions > Modules'. A green success message box in the top right corner reads: 'Success: Module successfully installed'. Below the navigation bar, the 'Installed Remediation Modules' section is visible, containing a table with the following data:

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

Dovrebbe quindi essere creata l'istanza corretta. Passare a **Criteri > Azioni > Risoluzioni > Istanze** e fornire l'indirizzo IP del nodo di amministrazione delle policy (PAN), insieme alle credenziali amministrative ISE necessarie per l'API REST (si consiglia un utente separato con il ruolo *Amministratore ERS*):

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"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/>	

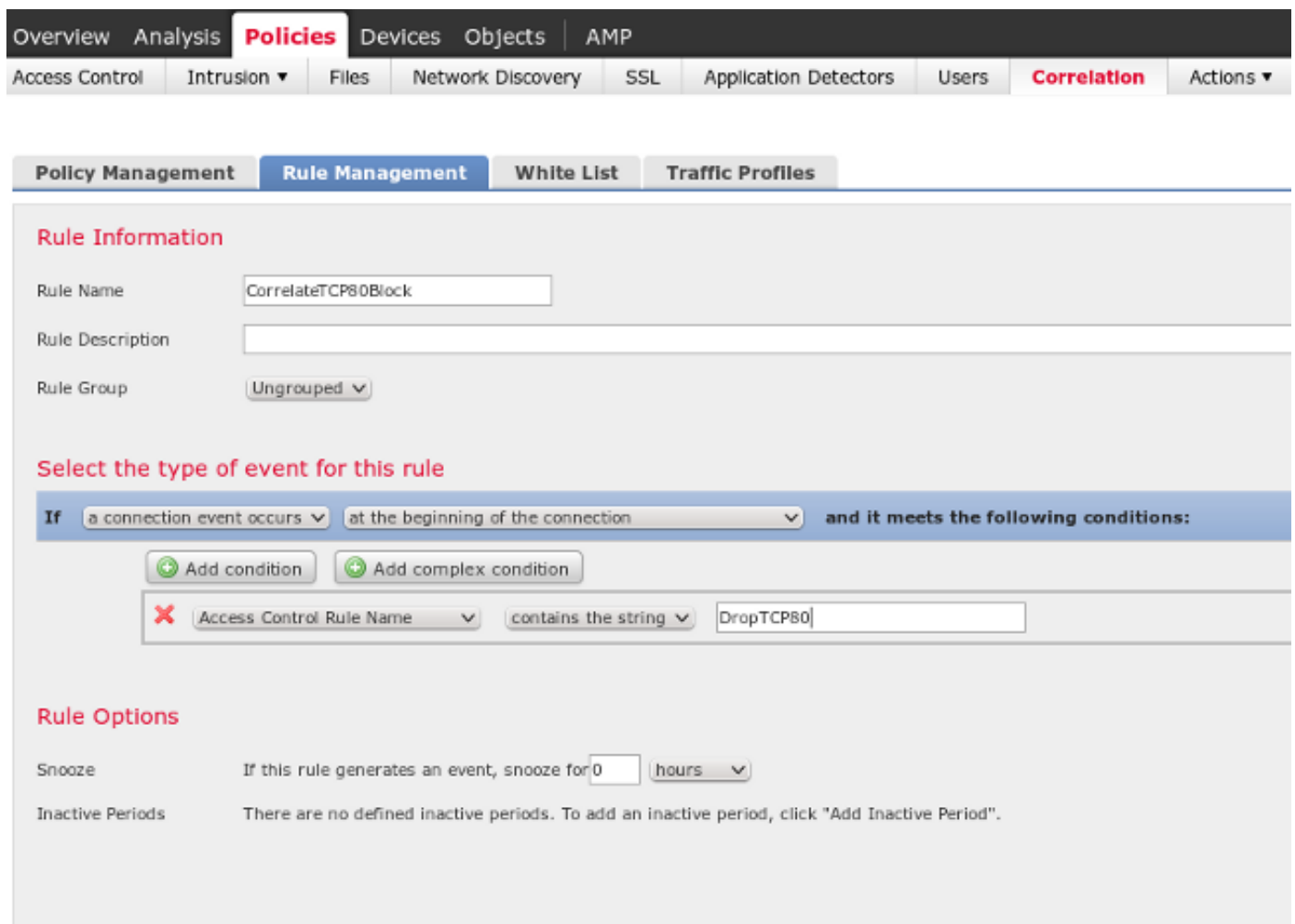
Anche l'indirizzo IP di origine (utente non autorizzato) deve essere utilizzato per il monitoraggio e l'aggiornamento:

Configured Remediations

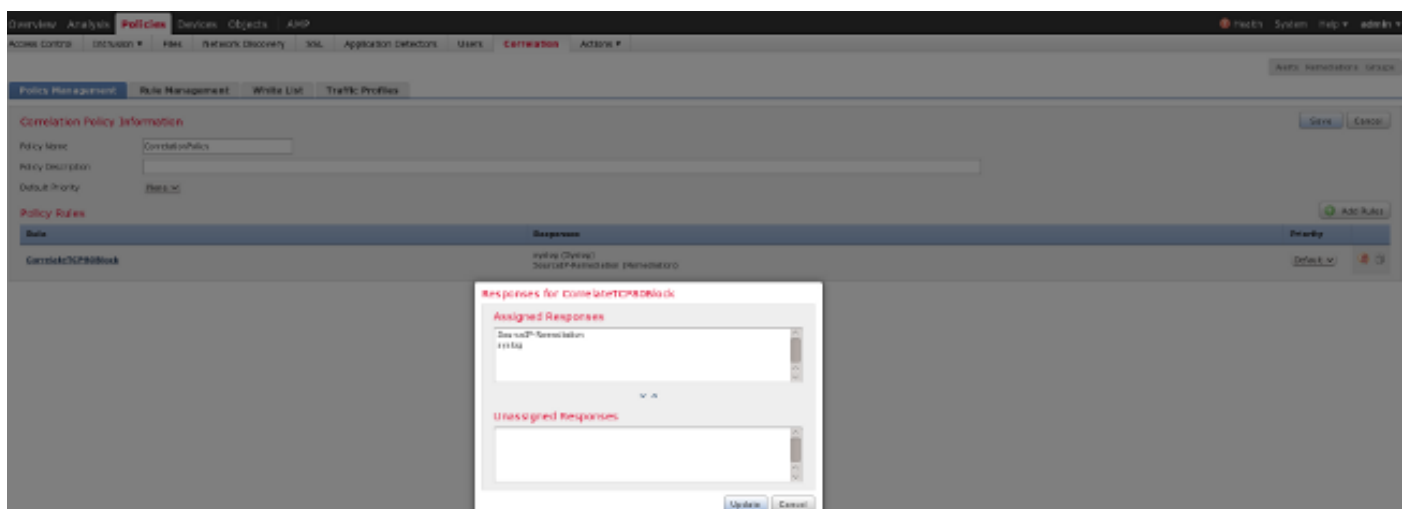
Remediation Name	Remediation Type	Description
No configured remediations available		
Add a new remediation of type		<input type="button" value="Add"/>
<input type="text" value="Quarantine Source IP"/>		

Criteri di correlazione

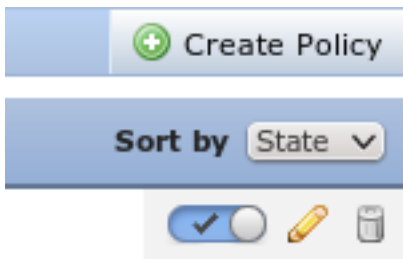
È necessario configurare una regola di correlazione specifica. Questa regola viene attivata all'inizio della connessione che corrisponde alla regola di controllo di accesso configurata in precedenza (*DropTCP80*). Per configurare la regola, passare a **Criteri > Correlazione > Gestione regole**:



Questa regola viene utilizzata nei criteri di correlazione. Passare a **Criteri > Correlazione > Gestione criteri** per creare un nuovo criterio, quindi aggiungere la regola configurata. Fare clic su **Risolvi** a destra e aggiungere due azioni: **monitoraggio e aggiornamento per sourceIP** (configurato in precedenza) e **syslog**:



Assicurarsi di abilitare il criterio di correlazione:



ASA

Un'ASA che funziona come gateway VPN è configurata in modo da usare ISE per l'autenticazione. È inoltre necessario abilitare la contabilità e il 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
```

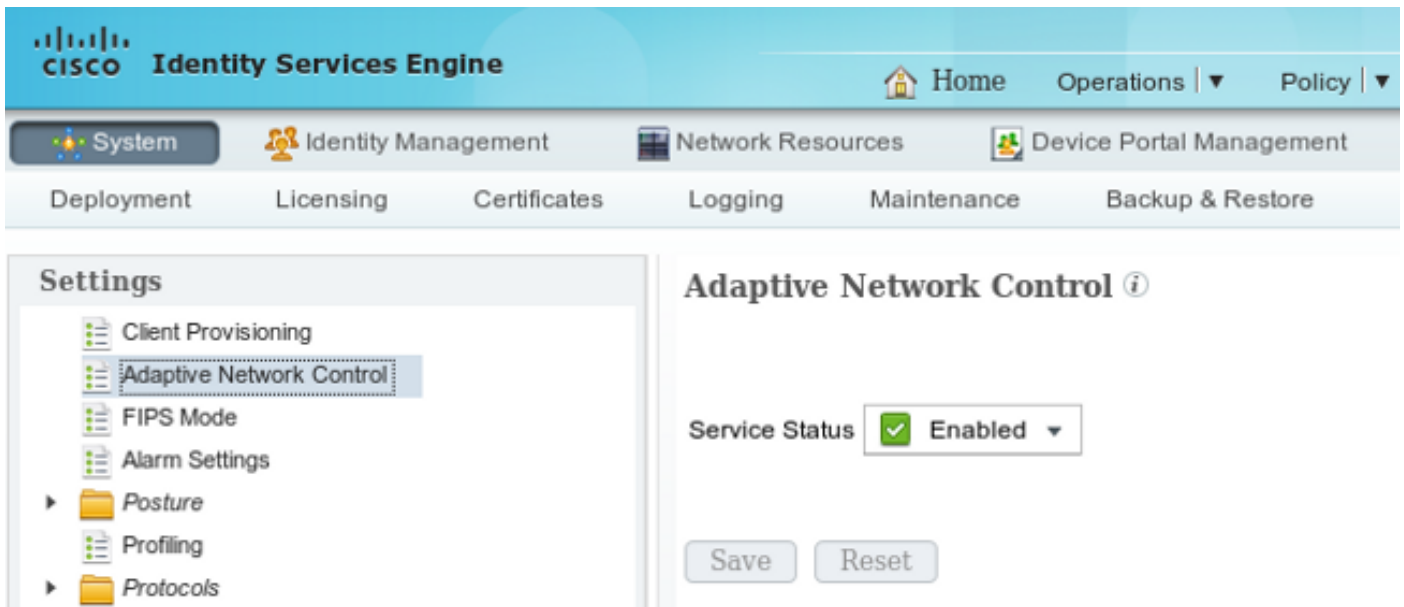
ISE

Configura dispositivo di accesso alla rete (NAD)

Selezionare **Amministrazione > Dispositivi di rete** e aggiungere l'appliance ASA che agirà come client RADIUS.

Abilita controllo adattivo della rete

Passare a **Amministrazione > Sistema > Impostazioni > Adaptive Network Control** per abilitare l'API e la funzionalità di quarantena:



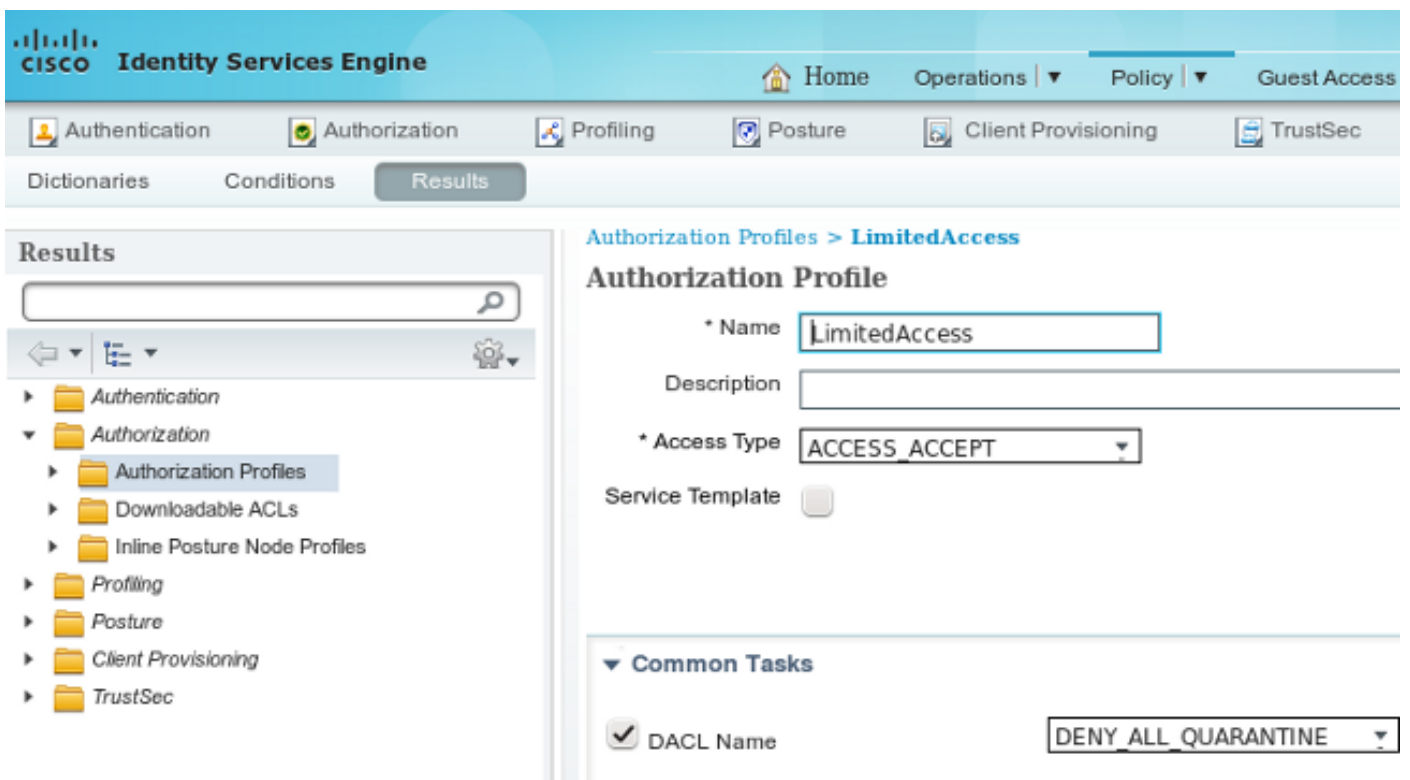
Nota: Nelle versioni 1.3 e precedenti questa funzionalità è denominata *Endpoint Protection Service*.

DACL quarantena

Per creare un elenco di controllo di accesso scaricabile (DACL, Downloadable Access Control List) da utilizzare per gli host in quarantena, selezionare **Policy > Results > Authorization > Downloadable ACL** (Policy > Risultati > Autorizzazione > ACL scaricabile).

Profilo di autorizzazione per quarantena

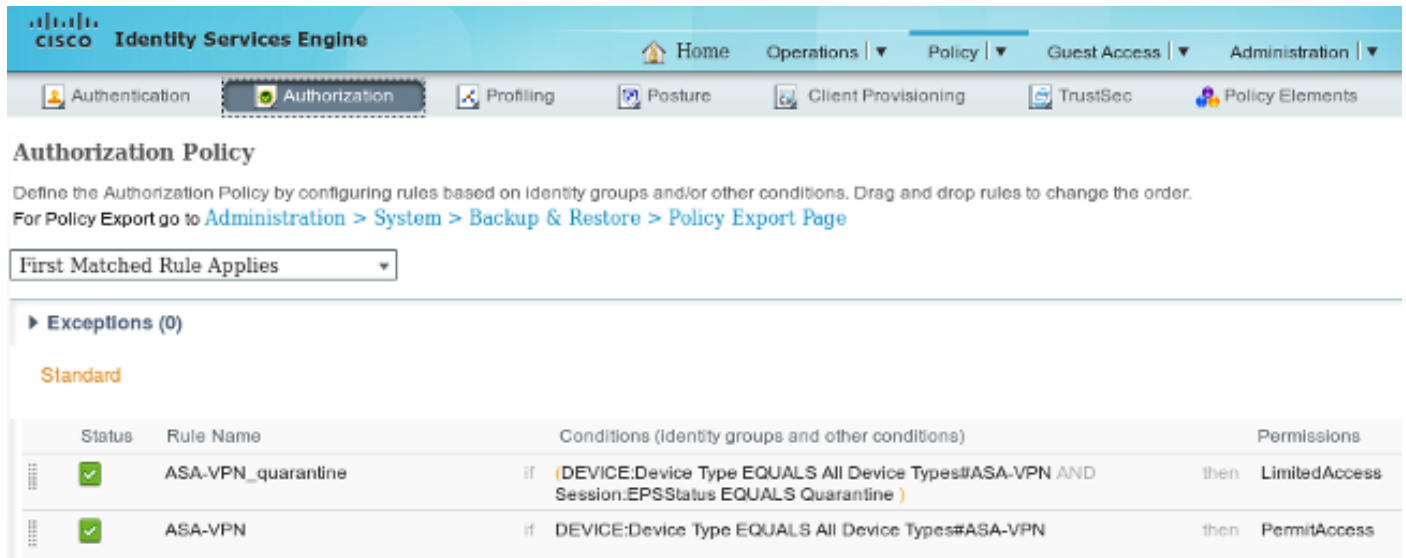
Passare a **Criterio > Risultati > Autorizzazione > Profilo autorizzazione** e creare un profilo di autorizzazione con il nuovo DACL:



Regole di autorizzazione

È necessario creare due regole di autorizzazione. La prima regola (ASA-VPN) fornisce l'accesso completo a tutte le sessioni VPN terminate sull'appliance ASA. La regola *ASA-VPN_quarantine* viene trovata per la sessione VPN riautenticata quando l'host è già in quarantena (è disponibile un accesso di rete limitato).

Per creare queste regole, passare a **Criterio > Autorizzazione**:



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)

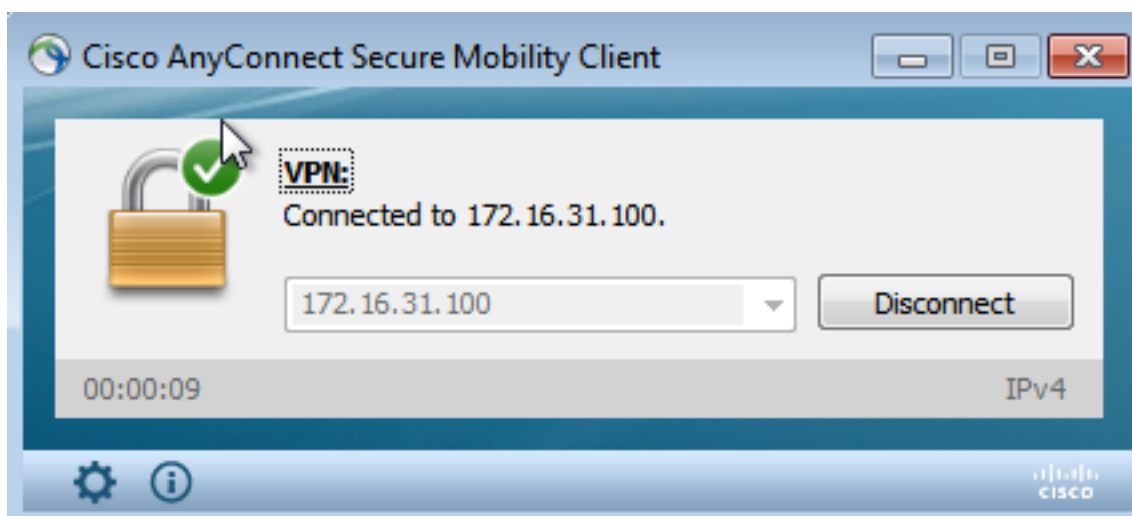
Standard

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

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni contenute in questa sezione.

AnyConnect avvia una sessione VPN ASA



L'ASA crea la sessione senza alcun DACL (accesso completo alla rete):

```
asav# show vpn-sessiondb details anyconnect
```

```
Session Type: AnyConnect
```



```

120 172.16.31.206 172.16.31.202 TLSv1 588 Client Hello
121 172.16.31.202 172.16.31.206 TCP 66 https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165957 TSecr=97280105
122 172.16.31.202 172.16.31.206 TCP 2952 [TCP segment of a reassembled PDU]
123 172.16.31.202 172.16.31.206 TLSv1 681 Server Hello, Certificate, Certificate Request, Server Hello Done
124 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=518 Ack=1449 Win=17536 Len=0 TSval=97280106 TSecr=389165957
125 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=518 Ack=2897 Win=20480 Len=0 TSval=97280106 TSecr=389165957
126 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=518 Ack=3512 Win=23296 Len=0 TSval=97280106 TSecr=389165958
127 172.16.31.206 172.16.31.202 TLSv1 404 Certificate, Client Key Exchange, Change Cipher Spec, Finished
128 172.16.31.202 172.16.31.206 TLSv1 72 Change Cipher Spec
129 172.16.31.202 172.16.31.206 TLSv1 119 Finished
130 172.16.31.206 172.16.31.202 TCP 66 48046 > https [ACK] Seq=856 Ack=3571 Win=23296 Len=0 TSval=97280107 TSecr=389165962
131 172.16.31.206 172.16.31.202 HTTP 255 GET /ise/eps/QuarantineByIP/172.16.50.50 HTTP/1.1
132 172.16.31.202 172.16.31.206 TCP 66 https > 48046 [ACK] Seq=3571 Ack=1085 Win=17792 Len=0 TSval=389166020 TSecr=97280111
135 172.16.31.202 172.16.31.206 HTTP/XML 423 HTTP/1.1 200 OK

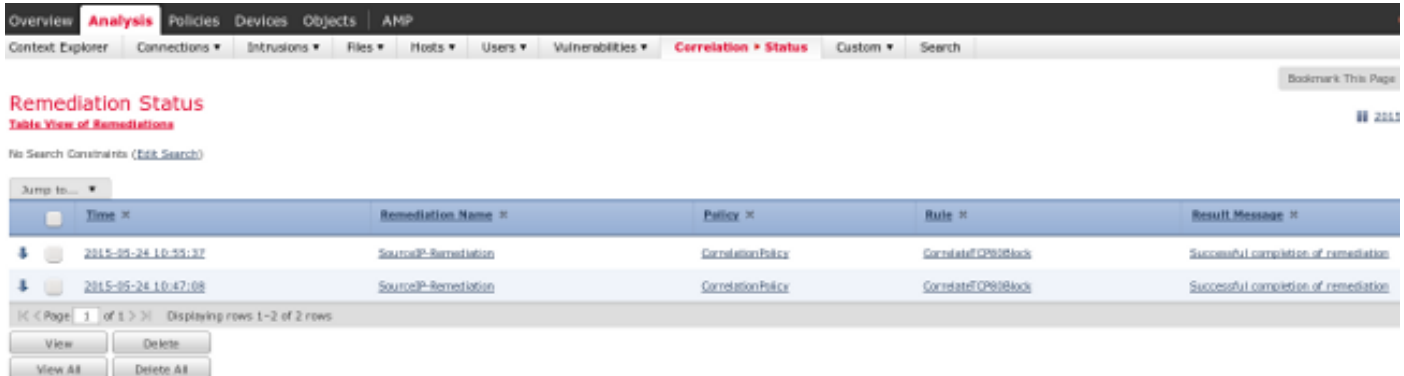
```

Secure Sockets Layer

- TLSv1 Record Layer: Application Data Protocol: http
 - Content Type: Application Data (23)
 - Version: TLS 1.0 [0x0301]
 - Length: 224
 - Encrypted Application Data: e1de29f5a3cef63e96cc97e0e9f9fdd21c9441cd117cb7e9...
- HyperText Transfer Protocol
 - 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 YWRtaW46S3Jha293MTIz\r\n
 - Host: 172.16.31.202\r\n
 - User-Agent: Libwww-perl/6.05\r\n
 - \r\n
 - [Full request LRI: http://172.16.31.202/ise/eps/QuarantineByIP/172.16.50.50]

In GET viene passata la richiesta dell'indirizzo IP dell'autore dell'attacco (172.16.50.50) e l'host viene messo in quarantena dall'ISE.

Per confermare l'esito positivo della risoluzione, selezionare **Analisi > Correlazione > Stato**:



ISE mette in quarantena e invia il CoA

In questa fase, ISE *port-management.log* notifica che il CoA deve essere inviato:

```

DEBUG [RMI TCP Connection(142)-127.0.0.1][] cisco.cpm.prvt.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

```

Il runtime (prrt-server.log) invia il messaggio di *terminazione* CoA al server AND, che termina la sessione (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:
[00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00]
  [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
```

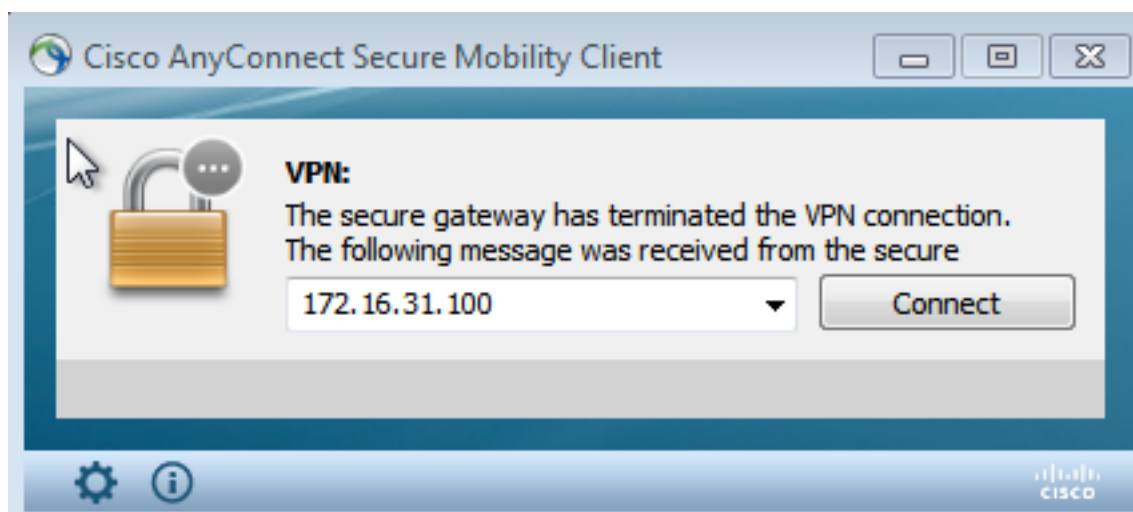
Il file *ise.psc* invia una notifica simile a questa:

```
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
```

Quando si passa a **Operazioni > Autenticazione**, dovrebbe essere visualizzato il messaggio Autorizzazione *dinamica riuscita*.

Sessione VPN disconnessa

L'utente finale invia una notifica per indicare che la sessione è disconnessa (per 802.1x/MAB/guest wired/wireless, questo processo è trasparente):



I dettagli dei log di Cisco AnyConnect mostrano:

```
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
```

Sessione VPN con accesso limitato (quarantena)

Poiché la *VPN sempre attiva* è configurata, la nuova sessione viene creata immediatamente.

Questa volta, viene trovata la regola ISE *ASA-VPN_quarantine*, che fornisce l'accesso alla rete limitato:

Time	Status	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-05-24 10:51:40...	🟡	cisco	192.168.10.21			Session State Is Started
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

Nota: DACL scaricato in una richiesta RADIUS separata.

Una sessione con accesso limitato può essere verificata sull'appliance ASA con il comando **show vpn-sessiondb detail anyconnect CLI**:

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

FireSight (centro difesa)

Lo script di monitoraggio e aggiornamento di ISE si trova nel seguente percorso:

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

Si tratta di un semplice script *perl* che utilizza il sottosistema di registrazione standard di SourceFire (SF). Una volta eseguito il monitoraggio e l'aggiornamento, è possibile confermare i risultati tramite */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

È importante abilitare il servizio Adaptive Network Control sull'ISE. Per visualizzare i log dettagliati in un processo di runtime (*prrt-management.log* e *prrt-server.log*), è necessario abilitare il livello DEBUG per Runtime-AAA. Per abilitare i debug, selezionare **Amministrazione > Sistema > Log > Debug Log Configuration** (Amministrazione > Sistema > Log > Configurazione log di debug).

È inoltre possibile passare a **Operazioni > Report > Endpoint e Utenti > Adaptive Network Control Audit** per visualizzare le informazioni per ogni tentativo e risultato di una richiesta di quarantena:

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	ac1020640005		
2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	512	ac1020640005	admin	172.16.31.206
2015-05-24 21:29:47.5	08:00:27:DA:EF:A		Unquarantine	SUCCESS	507	ac1020640005		
2015-05-24 21:29:47.4	08:00:27:DA:EF:A		Unquarantine	RUNNING	507	ac1020640005	admin	172.16.31.202
2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	FAILURE	480	ac1020640005		
2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	RUNNING	480	ac1020640005	admin	172.16.31.202
2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	SUCCESS	471	ac1020640005		
2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	RUNNING	471	ac1020640005	admin	172.16.31.202
2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	SUCCESS	462	ac1020640005		
2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	RUNNING	462	ac1020640005	admin	172.16.31.202
2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	SUCCESS	337	ac1020640005		
2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	RUNNING	337	ac1020640005	admin	172.16.31.202
2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	330	ac1020640005		
2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	330	ac1020640005	admin	172.16.31.206
2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	291	ac1020640005		
2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	291	ac1020640005	admin	172.16.31.206
2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	250	ac1020640005		
2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	250	ac1020640005	admin	172.16.31.206
2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	207	ac1020640005		
2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	RUNNING	207	ac1020640005	admin	172.16.31.206
2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	SUCCESS	206	ac1020640005		
2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	RUNNING	206	ac1020640005	admin	172.16.31.202
2015-05-24 10:51:17.2	08:00:27:DA:EF:A		Quarantine	SUCCESS	189	ac1020640005		
2015-05-24 10:51:17.2	08:00:27:DA:EF:A		Quarantine	RUNNING	189	ac1020640005	admin	172.16.31.202

Bug

Per informazioni su un bug ISE relativo a errori di sessione VPN (802.1x/MAB funziona correttamente), fare riferimento all'ID bug Cisco [CSCuu41058](https://tools.cisco.com/bugcenter/bug/?bugID=CSCuu41058) (ISE 1.4 Endpoint Quarantine Inconsistency and VPN Error).

Informazioni correlate

-
- [Integrazione di ISE versione 1.3 pxGrid con l'applicazione IPS pxLog](#)
- [Guida per l'amministratore di Cisco Identity Services Engine, versione 1.4 - Configurazione di Adaptive Network Control](#)
- [Guida di riferimento all'API Cisco Identity Services Engine, versione 1.2 - Introduzione all'API RESTful Services esterna](#)
- [Guida di riferimento alle API di Cisco Identity Services Engine, versione 1.2 - Introduzione alle API REST di monitoraggio](#)
- [Guida dell'amministratore di Cisco Identity Services Engine, versione 1.3](#)
- [Documentazione e supporto tecnico - Cisco Systems](#)