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:

Overview Analysis	Policies Devi	ces Objects AM	P								🛛 Heath 🛛 S	ystem Ha	p∓ ad	inin v
Access Control Unit	rusion * Files	Network Discovery	SSL Application D	etectors Users	Correlation	Actions =								
AccessPolicy											inve 🛛 🔘 O	most 🖌	Save and	Apply
Enter o description														
Rules Targets (1)	Rules Targets (1) Security Intelligence HTTP Responses Advanced													
🏥 Filter by Desice									Q AN C	legery 😳 Add Bala	Search Rales			×
* Name	Source James	Dust Zonas	Searce Natureris	Deat Naturorius	VLAN Tage	Users	Applications	Sec Parts	Deat Parts	URLa	Action			
Asteri a intractor: Ballon														
This category is empty														
Standard Rales														
1 Drup10989	any	any .	any	# 172.15.32.1	WV.	101	any	any.	₽ HITP	any .	X Black		0	/ 8
Root Roles														
This category is emply														
Defeall Address									Stirunian I	Noverlage: Deletion Deca	By and Gene	ilvity.	*	\$ 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:

Overview Analysis Policies Devices Objects	AMP			
Access Control Intrusion • Files Network Discovery	SSL Application Detecto	rs Users	Correlation	Actions + Modules
			Success Module succe	× ssfully installed
Installed Remediation Modules				
Module Name	Version	Description		
Cisco IOS Null Route	1.0	Block an IP ad	ldress in a Cisco IX	05 router
Cisco PIX Shun	1.1	Shun an IP ad	Idress in the PIX fi	rewall
ISE 1.2 Remediation	1.3.19	Quarantine IP	addresses using 1	dentity Services Engine 1.2
Nmap Remediation	2.0	Perform an N	map Scan	
Set Attribute Value	1.0	Set an Attribu	te 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	
Primary Admin Node IP	172.16.31.202
Secondary Admin Node IP (optional)	
Username	admin
Password Retype to confirm	•••••
SYSLOG Logging	• On Off
White List (an <i>optional</i> list of networks)	Create Cancel

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

Configured Remediations							
Remediation Name	Remediation Type	Description					
No confi	igured remediations availabl	e					
Add a new remediation of	type Quarantine Source IP	✓ Add					

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 CorrelateTCP80Block
Rule Description
Rule Group
Select the type of event for this rule
If a connection event occurs V (at the beginning of the connection V) and it meets the following conditions:
Add condition Add complex condition
X Access Control Rule Name V Contains the string V DropTCP80
Rule Options
Snooze If this rule generates an event, snooze for 0 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**:

Overview Analysis 💌	cles Devices Objects AHP	🚳 Headin - System - Heip 🕶 - edenler n
ACCHINE CONTROL DISC TAKEN	Here Instructure Description and Application Detectors Users Centreation Actions	
		Airs senectors brack
Policy Henapervent	isle Hanagement Write List Traffic Profiles	
Correlation Policy 3st	mation	Serve Corcor
Policy Mane	ConstationMaile	
Parcy Description		
Output: Priority	Per Million Control Co	
Policy Rules		Q Add Rukes
Bala	Barperson .	Driwky
Garrelete 767908lock	ingel na (Diversia) Sourceatt Mannach adma (Mannachattaro)	Drint v 4 3
	Rus paraes for Example Levert294094304	

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:

cisco Identi	ty Services Er	ngine		🟠 Home	Operations 🔻	Policy 🔻
🙀 System	聲 Identity Ma	nagement	Network Reso	ources 🛛 🛃 D	evice Portal Mana	igement
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Re	store
Settings Client Provi Adaptive Ne FIPS Mode Alarm Settin	sioning etwork Control		Adaptive Service State	Network Con	ntrol € ▼	
 Profiling Protocols 			Save	Reset		

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:

cisco Identity Services Engine	1	Home	Operations	Policy	▼ Guest	Access
Authentication 💿 Authorization	🕻 Profiling 🛛 💽 F	osture	딣 Client Pro	ovisioning	🚊 Trus	tSec
Dictionaries Conditions Results						
Results	Authorization Prof Authorization * Name Description * Access Type Service Template	iles > Limi Profile	Access ACCEPT	Ţ		
Client Provisioning TrustSec	▼ Common Ta	sks			0.145.447.11	1
	DACL Name		Ľ	DENY_ALL_	QUARANTIN	E .

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**:

ciso	ili. co Ide	ntity Services Engine		☆ Home	Operations 🔻	Policy V	Guest Access	Ac	tministration 🔻
1	Authentic	ation 🥑 Authorization	Rev Profiling	💽 Posture	👸 Client Provi	sioning	🔄 TrustSec	🐥 Po	licy Elements
Auth Define For Pol	orizatio the Autho licy Export Matched	n Policy nization Policy by configuring rules is go to Administration > System Rule Applies *	based on identity g > Backup & Res	roups and/or other store > Policy Ex	conditions. Drag a port Page	and drop rules	to change the order		
> Ex	ceptions Indard	(0)							
	Status	Rule Name	Cond	ditions (identity gro	ups and other cond	ditions)			Permissions
1		ASA-VPN_quarantine	if (DEV Sessi	ICE:Device Type E ion:EPSStatus EQ	QUALS All Device JALS Quarantine)	Types#ASA-\	PN AND	then	LimitedAccess
1	2	ASA-VPN	if DEV	CE:Device Type E	QUALS All Device	Types#ASA-V	PN	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
                                     Public IP
Assigned IP : 172.16.50.50
                                                  : 192.168.10.21
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
            : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
          : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
: 18706 Bytes Rx : 14619
Hashing
Bytes Tx
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>
```

User Attempts Access

Once the user attempts to access http://172.16.32.1, the access policy is hit, the traffic that corresponds is blocked inline, and the syslog message is sent from the FirePower management IP address:

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 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:

FireSight Correlation Policy Hit

The FireSight management (Defence Center) Correlation Policy is hit, which is reported by the syslog message that is sent from Defence 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)
```

At this stage, Defence Center uses the REST API (quarantine) call to the ISE, which is an HTTPS session and can be decrypted in Wireshark (with the Secure Sockets Layer (SSL) plugin and the private key of the PAN administrative certificate):

120	172.16.31.206	172,16,31,202	TLSv1	583 Client Hello						
121	172,16.31,202	172.16.31.206	TOP	66 https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165857 TSecr=97280105						
122	172.16.31.202	172,16,31,206	TCP	2962 [TCP segment of a reassembled PDU]						
123	172.16.31.202	172.16.31.206	T_Sv1	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=389165857						
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=389165858						
127	172.16.31.206	172.16.31.202	T_Sv1	404 Certificate, Client Key Exchange, Change Cipher Spec, Finished						
128	172.16.31.202	172.16.31.206	T_Sv1	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	HITP	295 GET /ise/eps/QuarantineByTP/172.16.50.50 HTTP/1.1						
132	172.16.31.202	172.16.31.206	TOP	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						
p tranos	CODINI CONCLUCT	Inconstruction	CT 10010 T	001077 001 10111 11100 1 11077 0007 000						
✓ Secure	Sockets Layer									
⇒ ILSi	1 Record Layer:	Application Data	Protocol:	http						
Co	ntent Type: Appl.	ication Data (23	2							
Ve	rsion: TLS 1.0 (6x6301)								
Le	ngth: 224									
En	crypted Applicat	ion Data: elde29	fsa3cef63e9	Sdc97e9e9F9Fdd21c9441cd117cb7e9						
V Hypent	ext Transfer Pro	tocol								
_ ▶ GET	/ise/eps/Quarant	ineByIP/172.16.5	0.50 HTTP/1	. 1\r\n						
TE:	deflate,gzip;q=0	.3\r\n								
Conn	ection: TE, clos	e\r\n								
▷ Auth	orization: Basic	WRtaW46S30ha29	3MTI2\r\n							
Host	: 172.16.31.202\	r\n								
User	User-Agent: libwww-perl/6.05\r\n									
\r\n	\r\n									
[Eut	[Full request URI: http://172.16.31.202/ise/eps/QuarantineByIP/172.16.50.50]									

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:

Analysis Policies Devices Objects AMP								
Context Explorer Connections Intrusions Files	 Hosts	errelation + Status Custom +	Search					
				Boskmark This Page				
Remediation Status								
No Search Constraints (<u>Edit Search</u>)								
Jump to								
_ Time ×	Remediation Name #	Pattery ×	Rule ×	Result Message ×				
\$ <u>2115-01-24 10-55:57</u>	SourceiP-Remediation	CorrelationPolicy	Constatut (290)Block	Successful completion of remediation				
3 2015-05-24.10:47:08	SourcelP-Remediation	Correlation Policy	CorrelateT0990Block	Successful completion of remediation				
$ < < Page_1_of\ t > > $. Displaying rows 1–2 of 2 rows								
View Delete								

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:
```

- [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.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
```

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):

🕥 Cisco AnyCo	nnect Secure Mobility Client		8
	VPN: The secure gateway has terminated the VP The following message was received from to 172.16.31.100	N connection. he secure Connect	
‡ (i)			cisco

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:

Authentical	iona	# Report	19	Adaptive	Network Centre	I Troubleshoot				
Misconfigured Supplicants 🛞					Misco	nfigured Network Devic	es @	RADIUS Drops @	Client Stopped	
0					0		0	0		
🚮 Show Live S	essions	😂 Add or	Remo	ve Columns 🔻	🔗 Refresh	🕐 Reset Repeat Counts			Refresh Every 1	
Time	•	itatus All 👻 De	et	Repeat C	Identity ®	Endpoint ID	Authorization Policy	Authorization Profiles	Event ①	
2015-05-2410:	51:40	0	ò	0	cisco	192,169,10,21			Session State is Started	
2015-05-2410:	S1:35	V	ò		#ACSACL#HP	9 0			DACL Download Succeeded	
2015-05-2410:	51:35	×	ò		cisco	192,169,10,21	${\tt Default} >> {\tt ASA-VPN}_quarantine$	UmitedAccess	Authentication succeeded	
2015-05-2410;	51:17	X	ò			08:00:27:DA:ER.AD			Dynamic Authorization succeeded	
2015-05-2410;	48:01	Z	ò		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
                                   Index : 39
Public IP : 192.168.10.21
Username
           : cisco
Assigned IP : 172.16.50.50
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
            : AnyConnect Essentials
License
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
Pkts Tx : 8
                                  Bytes Rx : 4084
                                   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:

cisco Identity Services Engine	A Har	10 Operations	Policy V De	ent Access V	Administration								
Authentications 📑 Reports 🔯 A	dapitve Network Conitol	Troubleshoot											
Report Selector Adjustice Nativork Control Audit													
Favorites													
ISE Reports	From 05/24/2015 12:00:00	AM to 05/24/2015 09	:36:21 PM										
Aufn Services Status	Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session Admin	Admin IP					
B reports	2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	512	ec1020640005						
Deployment Status 12 reports	2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	512	ac1020640005 admin	172.16.31.206					
* Endpoints and Users	2015-05-24 21:29:47.5	08:00:27:DA-EF-M		Unquarantine	SUCCESS	507	ac1020640005						
Client Provisioning	2015-05-24 21:29:47.4	08:00:27:DA-EF-M		Unquarantine	RUNNING	507	ac1020640005 admin	172.16.31.202					
Current Active Sessions	2015-05-24 21:18:25.2	08-00-27-DA-EF-M		Quarantine	FALURE	480	ac1020640005						
Adaption Matanack Control Audit	2015-05-24 21:18:25.2	08-00-27-DA-EF-M		Quarantine	RUNNING	480	ac1020640005 admin	172.16.31.202					
Adaptive Network Control Audit	2015-05-24 21:11:19.8	08-00-27-DA-EF-M		Unquarantine	SUCCESS	471	ac1020640005						
* Time Range Today *	2015-05-24 21:11:19.8	08:00.27:DA-EF-M		Unquarantine	RUNNING	471	ac1020640005 admin	172.16.31.202					
Date	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					
External Mobile Device Management	2015-05-24 18:05:10.7	08:00:27:DA-EF-M		Quarantine	SUCCESS	337	ac1020640005						
Posture Detail Assessment	2015-05-24 18:05:10.7	08-00-27-DA-EF-A		Quarantine	RUNNING	337	ac1020640005 admin	172.16.31.202					
Profiled Endpoints Summary	2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	330	ac1020640005						
Endpoint Profile Changes	2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	330	ac1020640005 admin	172.16.31.206					
Top Authorizations by Endpoint	2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	291	ac1020640005						
Ten behavioring bullers	2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	291	ac1020640005 admin	172.16.31.206					
Top Authorizations by User	2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	250	ac1020640005						
User Change Password Audit	2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	250	ac1020640005 admin	172.16.31.206					
Supplicant Provisioning	2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	207	ac1020640005						
Registered Endpoints	2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	RUNNING	207	ac1020640005 admin	172.16.31.206					
Endpoints Purge Activities	2015-05-24 10:55:29.7	08:00:27:DA-EF-A		Unquarantine	SUCCESS	206	ac1020640005						
 Buart Access Reports 	2015-05-24 10:55:29.7	08:00:27:DA-EF-A		Unquarantine	RUNNING	206	ac1020640005 admin	172.16.31.202					
5 reads	2015-05-24 10:51:17.2	08:00:27:DA-EF-A		Quarantine	SUCCESS	189	ac1020640005						
Saved and Scheduled Reports	2015-05-24 10:51:17.2	08:00:27:0A-EF-A		Quarantine	RUNNING	189	ac1020640005 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