

配置异常终端检测和执行在ISE 2.2

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[步骤1. Enable \(event\)异常检测。](#)

[步骤2.配置授权策略。](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述异常终端检测和执行。这是在思科身份服务引擎介绍的一个新的描出的功能(ISE)方面增强版网络可见度的。

先决条件

要求

Cisco 建议您了解以下主题：

- 在交换机的有线的MAC验证旁路(MAB)配置
- 在无线局域网控制器(WLC)的无线MAB配置
- 授权(CoA)配置的崔凡吉莱在两个设备的

使用的组件

本文档中的信息基于以下软件和硬件版本：

1. 身份服务引擎2.2
2. 无线局域网控制器8.0.100.0
3. Cisco Catalyst交换机3750 15.2(3)E2
4. Windows 10用有线的和无线适配器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

ISE能检测在MAC地址伪装涉及的终端。一旦它检测，ISE能采取行动(与CoA)和强制执行某些策略限制可疑终端的访问。

一旦检测启用，ISE监控为现有终端接收的所有最新信息和检查这些属性是否更改：

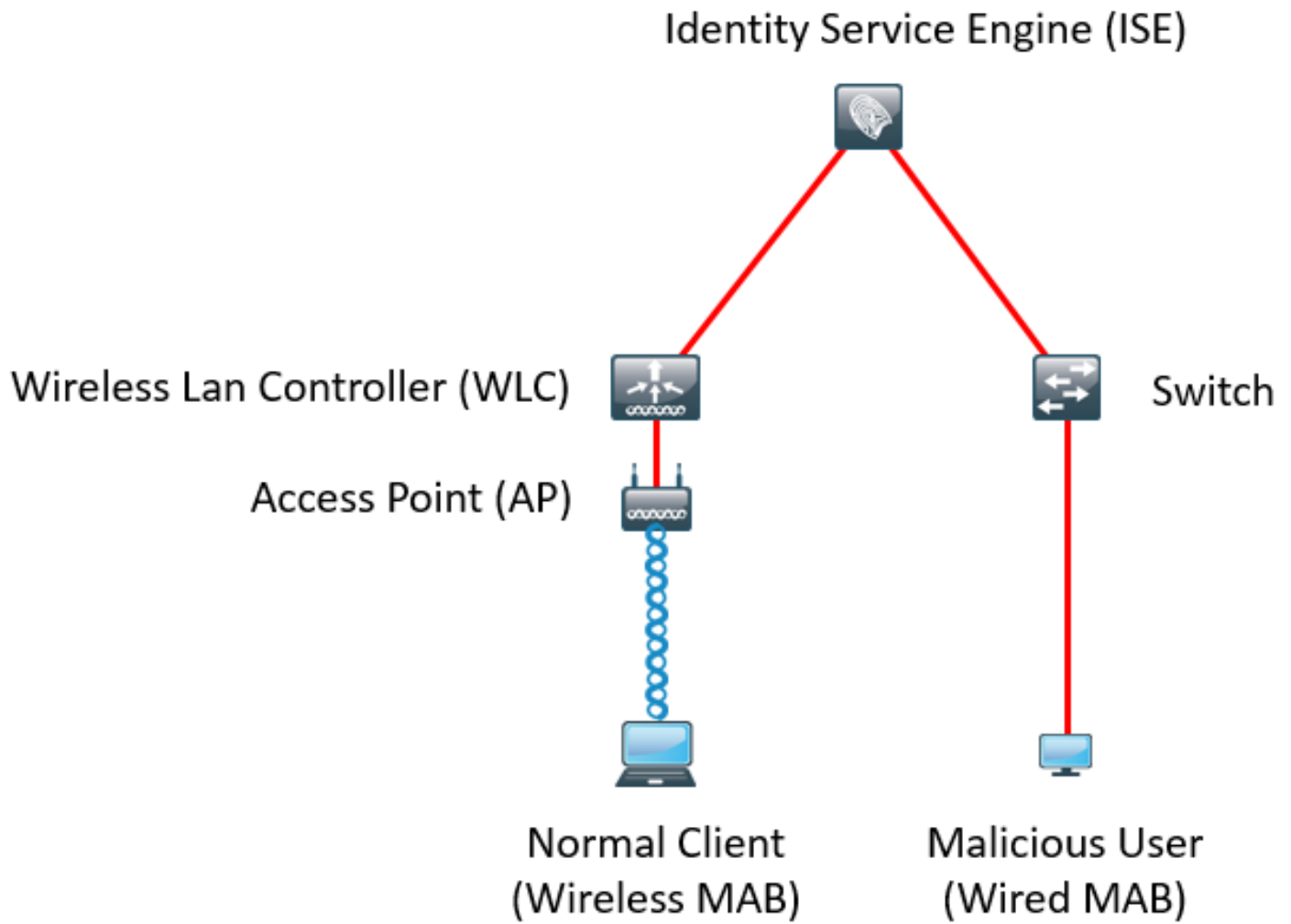
1. **NAS端口类型**-确定此终端访问方法是否更改。例如，如果通过有线的Dot1x连接的同一MAC地址使用无线Dot1x和签证versa。
2. **DHCP中集集团ID** -确定终端的客户端/供应商种类是否更改。当DHCP类ID属性带有有些值和然后更改对另一个值时，这只应用。如果终端配置与静态IP，DHCP类ID属性在ISE不会填充。稍后，如果另一个设备伪装MAC地址并且使用DHCP，中集集团ID从一个空值将变成一个特定字符串。这不会触发Anomouls行为检测。
3. **终端策略**-在终端配置文件上的一个变化从打印机或IP电话到工作站。

一旦ISE检测以上提到的其中一更改，AnomalousBehaviour属性被添加到终端和集对真。这在授权策略可以稍后用于，情况限制终端的访问在将来认证。

如果执行配置，ISE能发送CoA，一旦更改检测重新鉴别或执行终端的端口跳动。如果实际上，它可以根据配置的授权策略检疫异常终端。

配置

网络图



配置

简单MAB和AAA配置在交换机和WLC被执行。要使用此功能，请遵从这些步骤：

步骤1. Enable (event)异常检测。

导航对**管理>System >设置>描出**。

Profiler Configuration

* CoA Type:

Current custom SNMP community strings:

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter: Enabled [?](#)

Enable Anomalous Behaviour Detection: Enabled [?](#)

Enable Anomalous Behaviour Enforcement: Enabled

第一个选项允许ISE检测所有异常行为，但是CoA没有发送(可见性模式)。第二个选项允许ISE发送CoA，一旦异常行为检测(执行模式)。

步骤2.配置授权策略。

如镜像所显示，配置Anomalousbehaviour属性作为在授权策略的一个条件，：

▼ Exceptions (1)			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	Anomalous Client	if (EndPoints:AnomalousBehaviour EQUALS true AND DEVICE:Location EQUALS All Locations)	then DenyAccess
Standard			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	Normal Client	if DEVICE:Location EQUALS All Locations	then PermitAccess

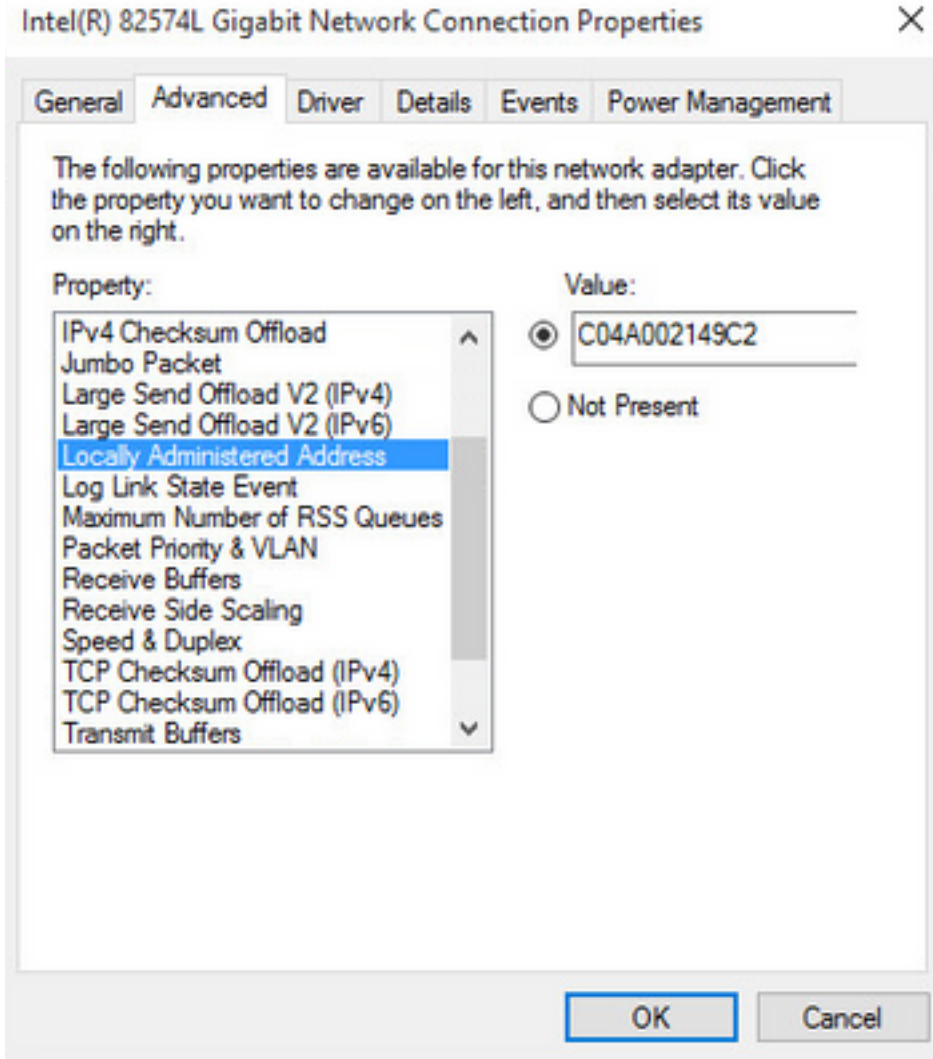
验证

连接无线适配器。请使用ipconfig命令/all查找无线适配器MAC地址，如镜像所显示：

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . : 
Description . . . . . : 802.11n USB Wireless LAN Card
Physical Address. . . . . : C0-4A-00-21-49-C2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1c54:884a:33c0:bcf1%4(Preferred)
IPv4 Address. . . . . : 192.168.1.38(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, December 30, 2016 5:17:12 AM
Lease Expires . . . . . : Friday, December 30, 2016 6:17:12 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 46156288
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-F3-74-5F-C0-4A-00-21-49-C2
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpi . . . . . : Enabled
```

要模拟恶意用户，您可以伪装以太网适配器的MAC地址匹配普通用户的MAC地址。



一旦普通用户连接，您能看到在数据库的一个终端条目。之后，使用用欺骗性MAC地址，恶意用户连接。

从报告您能看到从WLC的初始连接。之后，恶意用户连接，并且10几秒后，CoA被触发的归结于异常客户端的检测。因为全局CoA类型设置为**Reauth**，终端设法再连接。ISE已经设置AnomalousBehaviour属性对真，因此ISE匹配第一个规则并且拒绝用户。

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
Match Logged At of the following rules. <input type="text" value="Enter Advanced Filter Nam"/> <input type="button" value="Save"/>						
Loaded At	Within	Custom	From	12/30/2016 8:00	To	12/30/2016 8:38 <input type="button" value="Filter"/>
2016-12-30 20:37:59.728	<input checked="" type="checkbox"/>		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
2016-12-30 20:37:59.704	<input checked="" type="checkbox"/>		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:37:49.614	<input checked="" type="checkbox"/>		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:22:00.193	<input checked="" type="checkbox"/>		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

如镜像所显示，您能看到详细信息在上下文可见性选项卡的终端下：

C0:4A:00:21:49:C2   

 MAC Address: C0:4A:00:21:49:C2
Username: c04a002149c2
Endpoint Profile: TP-LINK-Device
Current IP Address: 192.168.1.38
Location: Location → All Locations


Applications **Attributes** Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	TP-LINK-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
----------------	-----------------

No data found. [Add custom attributes here.](#)

Other Attributes

AAA-Server	sth-nice
AD-Last-Fetch-Time	1483130280592
Acct-Input-Gigawords	0
Acct-Output-Gigawords	0
Airespace-Wlan-Id	3
AllowedProtocolMatchedRule	MAB
AnomalousBehaviour	true






正如你看到的终端可以从数据库删除清除此属性。

如镜像所显示，控制面板包括一新的选项卡显示显示此行为的客户端数量：

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Summary Endpoints Guests Vulnerability Threat +

METRICS

Total Endpoints ①	Active Endpoints ①	Rejected Endpoints ①	Anomalous Behavior ①	Authenti
 1	 0	 0	 1	

Filters: Anomalous Endpoints

MAC Address	Anomalous Behavior	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS
C0:4A:00:21:49:C2	true	192.168.1.38	c04a002149c2		Location → All...	TP-LINK-Device		TP-LINK TECHNOLOGI...	

故障排除

为了排除故障，启用仿形铣床调试，您导航对**管理>System >记录日志>调试日志配置**。

Component Name	Log Level	Description
portal-web-action	INFO	Base Portal debug messages
posture	INFO	Posture debug messages
previewportal	INFO	Preview Portal debug messages
profiler	DEBUG	profiler debug messages
provisioning	INFO	Client Provisioning client debug messages

如镜像所显示，为了查找ISE **Profiler.log**文件，请导航对**操作>下载日志>调试日志**，：

Debug Log Type	Log File	Description
	prrt-server.log.7	
	prrt-server.log.8	
	prrt-server.log.9	
profiler	profiler.log	Profiler debug messages

这些日志显示一些片断从**Profiling.log**文件。正如你看到的ISE能检测与C0:4A:00:21:49:C2 MAC地址的终端通过比较类型属性的旧有和新的值更改访问方法。它是无线，但是更改对以太网。


```
2016-12-30 20:37:43,874 DEBUG [EndpointHandlerWorker-2-34-thread-1][[]
cisco.profiler.infrastructure.profiling.ProfilerManager -:Profiling:- Classify hierarchy
C0:4A:00:21:49:C2
2016-12-30 20:37:43,874 DEBUG [MACSpoofingEventHandler-52-thread-1][[]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 DEBUG [MACSpoofingEventHandler-52-thread-1][[]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 INFO [MACSpoofingEventHandler-52-thread-1][[]
com.cisco.profiler.api.MACSpoofingManager -:ProfilerCollection:- Anomalous Behaviour Detected:
C0:4A:00:21:49:C2 AttrName: NAS-Port-Type Old Value: Wireless - IEEE 802.11 New Value: Ethernet
2016-12-30 20:37:49,620 DEBUG [MACSpoofingEventHandler-52-thread-1][[]
cisco.profiler.infrastructure.cache.EndPointCache -:ProfilerCollection:- Updating end point: mac
- C0:4A:00:21:49:C2
2016-12-30 20:37:49,621 DEBUG [MACSpoofingEventHandler-52-thread-1][[]
cisco.profiler.infrastructure.cache.EndPointCache -:ProfilerCollection:- Reading significant
attribute from DB for end point with mac C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 DEBUG [MACSpoofingEventHandler-52-thread-1][[]
profiler.infrastructure.probemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

所以，因为实施启用，ISE采取行动。此处操作是发送CoA根据在以上提到的描出的设置的全局配置。在我们的示例中，CoA类型设置为允许ISE重新鉴别终端和复校规则配置的Reauth。这时，它匹配异常客户端规则并且拒绝。

```
2016-12-30 20:37:49,625 INFO [MACSpoofingEventHandler-52-thread-1][[]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Taking mac
spoofing enforcement action for mac: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 INFO [MACSpoofingEventHandler-52-thread-1][[]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Triggering
Delayed COA event. Should be triggered in 10 seconds
2016-12-30 20:37:49,625 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received CoAEvent
notification for endpoint: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Configured Global CoA command
type = Reauth
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received
FirstTimeProfileCoAEvent for endpoint: C0:4A:00:21:49:C2
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Wait for endpoint:
C0:4A:00:21:49:C2 to update - TTL: 1
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Setting timer for endpoint:
C0:4A:00:21:49:C2 to: 10 [sec]
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Rescheduled event for
endpoint: C0:4A:00:21:49:C2 to retry - next TTL: 0
2016-12-30 20:37:59,644 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- About to call CoA for nad IP:
10.62.148.106 for endpoint: C0:4A:00:21:49:C2 CoA Command: Reauth
2016-12-30 20:37:59,645 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Applying CoA-REAUTH by AAA
Server: 10.48.26.89 via Interface: 10.48.26.89 to NAD: 10.62.148.106
```

相关信息

- [ISE 2.2管理指南](#)