

Configurar a detecção e a aplicação anômalas do valor-limite em ISE 2.2

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Etapa 1. Permita a detecção anômala.](#)

[Etapa 2. Configurar a política da autorização.](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a detecção e a aplicação anômalas do valor-limite. Esta é uma característica de perfilamento nova introduzida no Cisco Identity Services Engine (ISE) para a visibilidade aumentada da rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração prendida do desvio da autenticação de MAC (MAB) no interruptor
- Configuração wireless MAB no controlador do Wireless LAN (WLC)
- Mudança da configuração da autorização (CoA) em ambos os dispositivos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

1. Identity Services Engine 2.2
2. Controlador 8.0.100.0 do Wireless LAN
3. Interruptor 3750 15.2(3)E2 do Cisco catalyst

4. Windows 10 com prendido e adaptadores Wireless

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O ISE pode detectar os valores-limite que são envolvidos na falsificação do MAC address. Uma vez que é detectado, o ISE pode tomar a ação (com CoA) e reforçar determinadas políticas para restringir o acesso do valor-limite suspeito.

Uma vez que a detecção é permitida, o ISE monitora toda a informação nova recebida para valores-limite existentes e verifica se estes atributos mudaram:

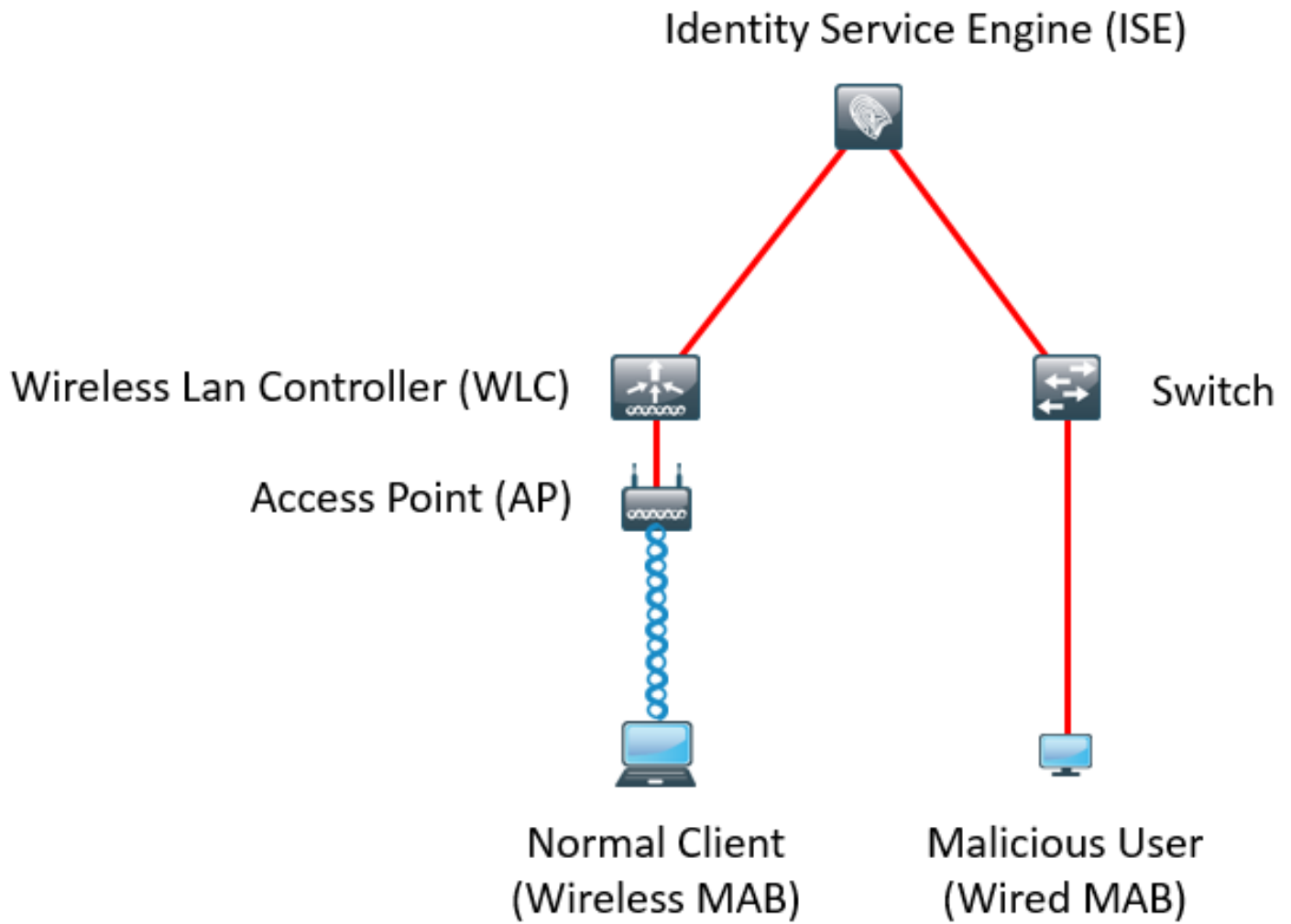
1. **NAS-Porta-tipo** - Determina se o método de acesso deste valor-limite mudou. Por exemplo, se o mesmo MAC address que conectou através do dot1x prendido é usado para o dot1x wireless e o visto-versa.
2. **Classe ID DHCP** - Determina se o tipo de cliente/vendedor do valor-limite mudou. Isto aplica-se somente quando o atributo da classe ID DHCP é povoado com algum valor e mudado então a um outro valor. Se um valor-limite é configurado com um IP Estático, o atributo da classe ID DHCP não estará povoado no ISE. Mais tarde, se umas outras paródias do dispositivo o MAC address e os usos DHCP, a classe ID mudarão de um valor vazio a uma corda específica. Isto não provocará a detecção do comportamento de Anomouls.
3. **Política do valor-limite** - Uma mudança no perfil do valor-limite da **impressora** ou do **telefone IP à estação de trabalho**.

Uma vez que o ISE detecta uma das mudanças mencionadas acima, o atributo de AnomalousBehaviour está adicionado ao valor-limite e ao grupo para retificar. Isto pode ser usado mais tarde como uma circunstância em políticas da autorização para restringir o acesso para o valor-limite nas autenticações futuras.

Se a aplicação é configurada, o ISE pode enviar um CoA uma vez que a mudança é detectada para autenticar novamente ou executar um salto da porta para o valor-limite. Se de fato, pode quarantine o valor-limite anômalo segundo as políticas da autorização que estiveram configuradas.

Configurar

Diagrama de Rede



Configurações

Os MAB simples e as configurações de AAA são executados no interruptor e no WLC. Para utilizar esta característica, siga estas etapas:

Etapa 1. Permita a detecção anômala.

Navegue à **administração > ao sistema > aos ajustes > perfilando**.

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

A primeira opção permite que o ISE detecte todo o comportamento anômalo mas nenhum CoA é enviado (modo da visibilidade-Somente). A segunda opção permite que o ISE envie o CoA uma vez que o comportamento anômalo é detectado (modo da aplicação).

Etapa 2. Configurar a política da autorização.

Configurar o atributo de Anomalousbehaviour como uma condição na política da autorização, segundo as indicações da imagem:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	Normal Client	if DEVICE:Location EQUALS All Locations	then PermitAccess

Verificar

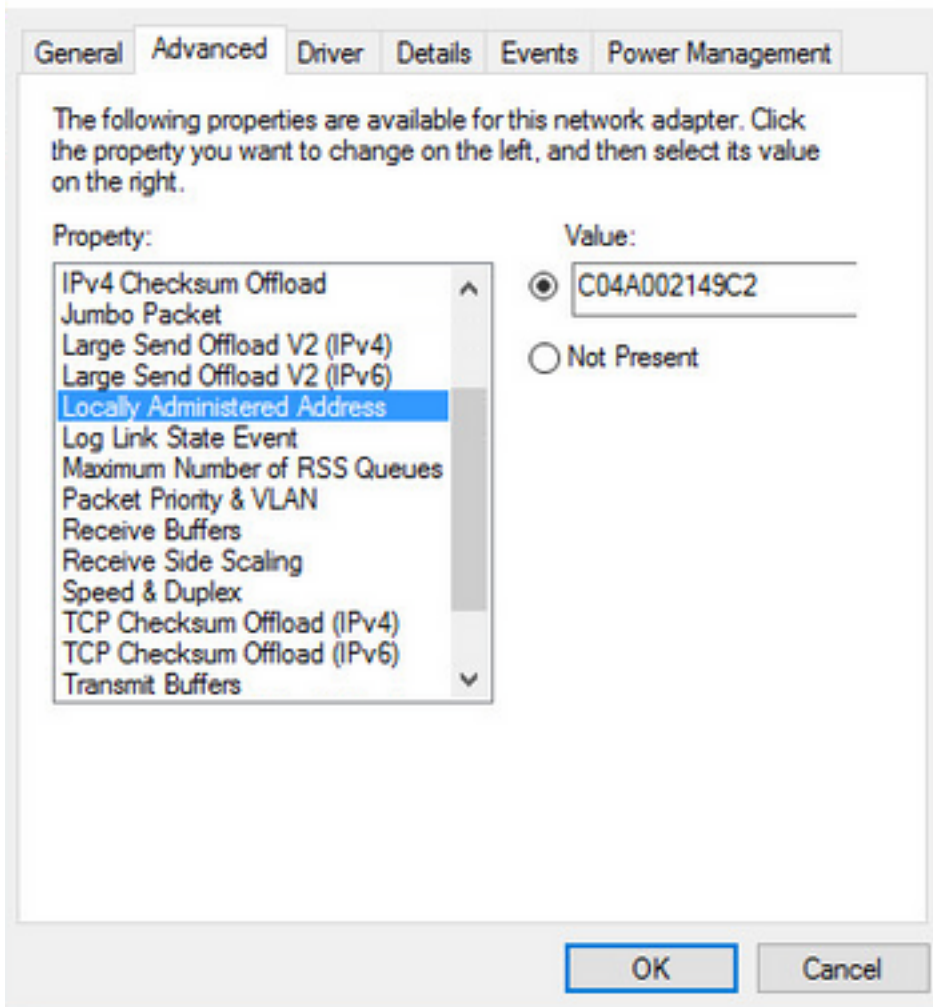
Conecte com um adaptador Wireless. Use o comando `ipconfig /all` encontrar o MAC address do adaptador Wireless, segundo as indicações da imagem:

```
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
```

Para simular um usuário malicioso, você pode spoof o MAC address do adaptador do Ethernet combinar o MAC address do usuário normal.

Intel(R) 82574L Gigabit Network Connection Properties



Uma vez que o usuário normal conecta, você pode ver uma entrada do valor-limite no base de dados. Mais tarde, o usuário malicioso conecta usando um MAC address falsificado.

Dos relatórios você pode ver a conexão inicial do WLC. Mais tarde, o usuário malicioso conecta e o 10 segundos depois, um CoA é provocado devido à detecção do cliente anômalo. Desde que o tipo global CoA é ajustado a **Reauth**, o valor-limite tenta conectar outra vez. O ISE já ajustou o atributo de AnomalousBehaviour para retificar assim que o ISE combina a primeira regra e nega o usuário.

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
2016-12-30 20:37:59.728	✘	of the following rules.	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
2016-12-30 20:37:59.704	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:37:49.614	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:22:00.193	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

Segundo as indicações da imagem, você pode ver os detalhes sob o valor-limite na aba da visibilidade do contexto:

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










Como você pode ver, o valor-limite pode ser suprimido do base de dados para cancelar este atributo.

Segundo as indicações da imagem, o painel inclui uma aba nova para mostrar o número de clientes que exibem este comportamento:

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

Summary Endpoints Guests Vulnerability Threat +

METRICS

Total Endpoints 	Active Endpoints 	Rejected Endpoints 	Anomalous Behavior 	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...	

Troubleshooting

A fim pesquisar defeitos, permita o perfilador debugam, como você navega à administração > ao sistema > registrando > debuga a configuração do log.

Component Name	Log Level	Description
<input type="radio"/> portal-web-action	INFO	Base Portal debug messages
<input type="radio"/> posture	INFO	Posture debug messages
<input type="radio"/> previewportal	INFO	Preview Portal debug messages
<input checked="" type="radio"/> profiler	DEBUG	profiler debug messages
<input type="radio"/> provisioning	INFO	Client Provisioning client debug messages

A fim encontrar o arquivo ISE Profiler.log, navegue às operações > aos logs da transferência > debugam logs, segundo as indicações da imagem:

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

Estes logs mostram alguns snippet do arquivo de Profiling.log. Como você pode ver, o ISE podia detectar que o valor-limite com MAC address de C0:4A:00:21:49:C2 mudou o método de acesso

comparando os valores velhos e novos do NAS-Porta-tipo atributos. É wireless mas é mudado aos Ethernet.

```
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 [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpooferingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 DEBUG [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpooferingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 INFO [MACSpooferingEventHandler-52-thread-1][[]
com.cisco.profiler.api.MACSpooferingManager -: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 [MACSpooferingEventHandler-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 [MACSpooferingEventHandler-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 [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

Consequentemente, o ISE toma a ação desde que a aplicação é permitida. A ação aqui é enviar um CoA segundo a configuração global nos ajustes de perfilamento mencionados acima. Em nosso exemplo, o tipo CoA é ajustado a Reauth que permite que o ISE autenticar novamente o valor-limite e verifique novamente as regras que foram configuradas. Esta vez, combina a regra anômala do cliente e consequentemente nega-se.

```
2016-12-30 20:37:49,625 INFO [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Taking mac
spoofering enforcement action for mac: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 INFO [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -: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

Informações Relacionadas

- [Guia de Administração ISE 2.2](#)