

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Fluxo de pacote](#)

[Configurar](#)

[Configurar o ISE](#)

1. [Crie o perfil do dispositivo de rede](#)

2. [Crie o dispositivo de rede](#)

3. [Configurar o servidor DHCP](#)

4. [Configurar o perfil da autorização](#)

[Configurar o NAD](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve os novos recursos no Identity Services Engine (ISE) que permite que a reorientação ocorra com os dispositivos da terceira do acesso de rede (NADs).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fluxo do convidado no ISE
- DNS e protocolos DHCP

[Componentes Utilizados](#)

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

- 2960 Series Switch de Cisco Catalys
- Cisco ISE, 2.1 da liberação

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

Os recursos avançados como o convidado, a postura e o Bring Your Own Device (BYOD) nas redes de modem, exigem uma comunicação direta entre o dispositivo do cliente e o servidor AAA. Em versões que precedentes ISE isto foi realizado enviando um dinâmico reorienta URL e Access Control List (ACL) ao NAD.

Há dois atributos imperativos que são enviados em um perfil da autorização para a reorientação no valor de atributo Paris (AV):

- Pares do AV Cisco? Reorienta a URL: O valor URL é dinâmico e é criado para cada sessão. As partes importantes de reorientam a URL são o nome de domínio qualificado de Fuly do nó do serviço da política (FQDN PSN) e o ID de sessão.
- Pares do AV Cisco? Reorienta o ACL: Este par AV contém um nome ACL que deva existir no NAD. Com a ajuda deste ACL, o NAD decide se os pacotes forem reorientados ou permitidos com o NAD.

A aproximação tradicional da reorientação pode somente ser executada com os dispositivos de Cisco NAD. Para o apoio NAD da terceira parte, a reorientação URL estática tinha sido adicionada em ISE 2.0. Quando esta aproximação for mais plataforma independente, ainda exige o apoio do Redireção do HTTP no NAD.

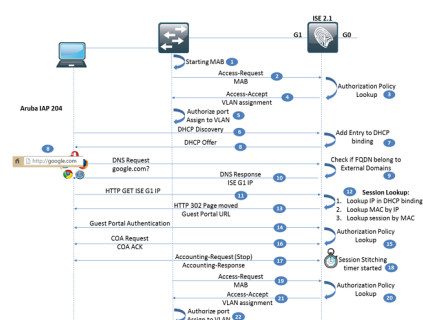
Começar com 2.1 ISE um estilo novo de reorienta foi adicionada. Esta aproximação não exige o apoio do Redireção do HTTP no NAD. A ideia principal atrás deste método é usar o ISE como um sinkhole DNS.

O DNS e a funcionalidade de servidor de DHCP foram adicionados à liberação do 2.1 ISE a fim usá-la como um sinkhole DNS. Agora o server ISE pode atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT aos usuários que precisam de ser reorientados e define-se como um servidor DNS. Isto permite que o ISE sereorienta- conexões do usuário sem nenhuma funcionalidade do servidor de Web no NAD. Contudo, o NAD deve ainda apoiar a mudança da atribuição da autorização (COA) e do VLAN dinâmico.

No ISE, esta aproximação pode ser usada para estes fluxos da reorientação:

- Fluxo do convidado: As respostas ISE a algum pedido DNS iniciado pelo usuário com seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT. Esta resposta faz com que o cliente estabeleça uma conexão de HTTP com ISE. Com respeito a isto, o ISE retorna a reorientação URL usando a página do código 302 do padrão HTTP movida.
- BYOD/Posture (Anyconnect somente)? em ambas as encenações, o aplicativo do abastecimento do suplicante (NSP) ou o módulo nativo da postura de Anyconnect iniciam uma conexão a enroll.cisco.com, que obtenha reorientada ao ISE usando as mesmas etapas que o fluxo do convidado.

Fluxo de pacote



1. O NAD começa o processo MAB para o dispositivo conectado. O processo MAB em switch Cisco começa de acordo com a prioridade do método de autenticação e não antes que o primeiro quadro esteja recebido do dispositivo final.
2. A solicitação de acesso MAB é enviada ao ISE.
3. O ISE avalia a política de autenticação e autorização para o pedido entrante do acesso. Durante a avaliação da política de autorização, o tipo de dispositivo de rede (ajuste do nível NAD) é comparado com o tipo de dispositivo de rede definido no perfil de autorização. Somente os perfis de autorização para o tipo de dispositivo de rede de harmonização podem ser selecionados.

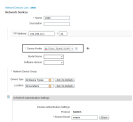
Nota: Para o convidado VLAN reorientado, o ISE precisa de selecionar um perfil de autorização que contém a reorientação da Web (CWA, MDM, NSP, CPP) e a atribuição de VLAN. A necessidade do cliente de ser atribuído a um segmento de rede que tenha o ISE como o único servidor DHCP.

1. O ISE retorna uma aceitação de acesso com informação de VLAN.
2. O interruptor autoriza a porta e aplica as configurações de vlan.
3. Os novatos DHCP do cliente descobrem. Se o PC é ficado situado no mesmo segmento que o ISE, o pacote alcança o ISE diretamente. Em caso de Conectividade L3 entre o cliente e o ISE, o IP ISE deve ser configurado como um endereço IP auxiliar no NAD para a transmissão de DHCP.
4. O ISE adiciona a informação cliente a sua tabela de ligação DHCP. O IP de cliente e o MAC são usados pelo ISE para a consulta da sessão.
5. A oferta de DHCP é enviada ao cliente. Nesta oferta, o endereço IP de Um ou Mais Servidores Cisco ICM NT ISE é especificado como o servidor DNS.
6. O usuário abre um navegador da Web e navega a google.com que provoque um pedido DNS ao ISE.
7. O ISE verifica se o FQDN do alvo pertence aos domínios externos. Se faz, a seguir o ISE envia este pedido a um servidor DNS definido nos ajustes do conjunto de DHCP. Se não o ISE retorna seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT na resposta.
8. O navegador da Web inicia uma conexão de TCP ao ISE e pedidos para google.com.
9. Nesta fase o ISE olha acima a sessão autenticada para o pedido entrante HTTP GET. Isto é importante para construir o correto reorienta a URL.

Nota: O ISE usa estas regras para a consulta da sessão:

1. IP da consulta no emperramento DHCP
2. Consulta MAC pelo IP
3. Sessão da consulta pelo MAC

1. O ISE responde com a página HTTP 302 movida para a reorientação URL.
2. O usuário é reorientado assim ao portal do convidado e o fluxo inteiro do convidado configurado no ISE ocorre aqui.
3. Após uma autenticação bem sucedida do convidado, o ISE é executado com as políticas de autorização uma vez mais para verificar se algum atributo novo esteve adicionado à sessão e se o valor-limite durante o fluxo do convidado exige a mudança da autorização (CoA). Uma vez que a política seguinte da autorização é identificada, o ISE prepara o pedido CoA.
4. A troca do pedido CoA/CoA ACK ocorre entre o ISE e o NAD. Um CoA da restauração do salto ou Admin da porta é uma obrigação porque este provoca a obtenção de um endereço IP de Um ou Mais Servidores Cisco ICM NT novo no VLAN final. O NAD precisa de apoiar o



- a. Note o ajuste para o perfil do dispositivo de rede.
- b. Todos ajustes restantes são padrão.

3. Configurar o servidor DHCP

O pool do servidor DHCP é limitado a um nó particular ISE e a sua relação. Navegue à administração > ao sistema > aos ajustes > aos serviços DHCP & DNS > Add

DHCP & DNS Services

a.

*Scope Name

Status Enabled

Node settings

b.

*ISE Node

*Network Interface

DHCP

c.

*Domain Name

*DHCP Address range to

*Subnet mask

*Network ID

Exclusion address range to

*Default gateway

*DHCP lease time seconds(5-300)

DNS

d.

External DNS servers

e.

External Domains

- a. O nome do escopo de DHCP precisa de ser configurado.

- b. Selecione o nó em que os serviços DNS e DHCP que devem ser executado e a relação nesse nó que deve ser usado.
- c. Defina o intervalo de endereço IP DHCP, o gateway padrão, os endereços excluídos do espaço e o tempo do aluguel de DHCP.
- d. Opcionalmente, defina endereços IP de Um ou Mais Servidores Cisco ICM NT externos do servidor DNS. Estes devem ser perguntados para domínios externos.
- e. Opcionalmente, defina nomes dos domínios externos. O ISE pergunta servidores DNS externos e retorna o endereço IP de Um ou Mais Servidores Cisco ICM NT real em vez do seus próprios.

4. Configurar o perfil da autorização

Navegue à política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização. Dois perfis da autorização são precisados para o fluxo completo do convidado:

- Reoriente o perfil da autorização (CWA1)
- Permita o perfil da autorização de acesso (PermitCWA2)

Authorization Profiles > CWA1

Authorization Profile

* Name

Description

* Access Type

Network Device Profile **a.**

Service Template

Track Movement

Passive Identity Tracking

▼ **Common Tasks**

DACL Name

ACL (Filter-ID)

VLAN Tag ID 1 ID/Name **b.**

▼ **Common Tasks**

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) **c.**

The network device profile selected above requires the following redirect URL to be configured manually on the network access device in order to enforce web redirection:
<https://iseHost:8443/portal/g?p=VldlxRKY7ab5RCDvoJZR7rQm5Q>

- a. Perfil do dispositivo de rede: Somente os pedidos de autenticação que vêm de NADs atribuíram a este perfil podem conduzir a este perfil da autorização,
- b. Configurações de vlan: Os VLAN definidos aqui devem existir no NAD. A relação ISE configurada para o DHCP deve ou pertencer a este VLAN ou deve ser configurada como o ajudante de IP no gateway que presta serviços de manutenção a este VLAN.
- c. Reoriente ajustes: Para o exemplo atual a autenticação da Web central foi definida como reorienta tipo, e portal patrocinado do convidado definido como um portal do convidado. O formulário ainda pede o nome da reorientação ACL. Desde que o perfil do dispositivo de rede foi reconfigurado para a URL estática reorienta, este nome ACL será enviado nunca ao NAD.

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile **a.**

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

ACL (Filter-ID)

VLAN Tag ID **1** ID/Name **b.**

- a. Perfil do dispositivo de rede: Somente os pedidos de autenticação que vêm de NADs atribuíram a este perfil podem conduzir a este perfil da autorização,
- b. Configurações de vlan: Após ter atribuído uma porta cliente a este VLAN, o usuário deve obter um endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP regular.

5. Configurar as políticas da autorização para o acesso do convidado

Navegue à política > à autorização. Configurar duas políticas: um para reorienta a ação e a outro para o acesso de usuário após a autenticação no portal do convidado.

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
b. <input checked="" type="checkbox"/>	CWA2	if GuestEndpoints AND Wired_MAB	then PermitCWA2
a. <input checked="" type="checkbox"/>	CWA1	if Wired_MAB	then CWA1

a. A primeira política da autorização combina o MAB prendido enquanto um método de autenticação e o perfil da autorização da reorientação são atribuídos em consequência.

b. A segunda política da autorização pode ser baseada em atributos de sessão (fluxo do caso = do convidado do uso/tipo grupo externo do convidado AD se os usuários convidado autenticados usando o AD) ou em atributos do valor-limite (grupo da identidade do valor-limite). O registo do dispositivo precisa de ser permitido no portal do convidado de usar o grupo da identidade do valor-limite.

Configurar o NAD

O switch Cisco foi configurado para o MAB na relação e tem o apoio COA.

Nota: O centro de assistência técnica da Cisco (TAC) não oferece nenhum apoio para a configuração de NADs da terceira.

Verificar

Um fluxo bem sucedido do convidado olha como este em operações ISE > em raio LiveLog:

Apr 03, 2016 01:09:24.457 PM	✓ d.	3C:97:0E:52:3F:D9	3C:97:0E:52:3F:D9	Windows7-W...	Default >> M...	Default >> CWA2	PermitCWA2	192.168.10.21	2960
Apr 03, 2016 01:09:12.606 PM	✓ c.		3C:97:0E:52:3F:D9						2960
Apr 03, 2016 01:08:48.200 PM	✓ b.	cisco	3C:97:0E:52:3F:D9					192.168.10.21	
Apr 03, 2016 01:08:01.987 PM	✓ a.		3C:97:0E:52:3F:D9		Default >> M...	Default >> CWA1	CWA1	192.168.30.3	2960

a. Esta é a primeira autenticação MAB. O perfil da autorização com reorienta é selecionado em consequência.

b. Esta é a autenticação do convidado. Depois que esta ação ISE faz uma re-avaliação da política para decidir se o CoA está precisado.

c. Um CoA foi terminado com sucesso.

d. Esta é a segunda autenticação MAB. O perfil da autorização para o acesso do convidado é selecionado em consequência.

Troubleshooting

Verifique se o endereço IP de Um ou Mais Servidores Cisco ICM NT é atribuído ao cliente corretamente. Isto pode ser feito recolhendo uma captura de pacote de informação no cliente ou no ISE.

Esta captação do cliente mostra a um aperto de mão bem sucedido DHCP com o IP DNS mesmos que o ISE.

```
149 12:45:36.38820  0.0.0.0      255.255.255.255  DHCP  142 DHCP Discover - Transaction ID 864822007
150 12:45:37.48120  192.168.10.38  255.255.255.255  DHCP  142 DHCP Offer - Transaction ID 864822007
151 12:45:37.48190  0.0.0.0      255.255.255.255  DHCP  142 DHCP Request - Transaction ID 864822007
152 12:45:37.49060  192.168.10.38  255.255.255.255  DHCP  142 DHCP ACK - Transaction ID 864822007

* Option (54) DHCP Server Identifier
  Length: 4
  DHCP Server Identifier: 192.168.10.38
* Option (52) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (DHCP) 5 minutes
* Option (53) Subnet Mask
  Length: 4
  Subnet Mask: 255.255.255.0
* Option (51) Domain Name
  Length: 22
  Domain Name: example.com
* Option (55) Router
  Length: 4
  Router: 192.168.10.1
* Option (63) Domain Name Server
  Length: 4
  Domain Name Server: 192.168.10.1
```


Verifique se o ISE está atuando corretamente como um sinkhole DNS. Uma captura de pacote de informação pode ajudar a confirmar se o pedido está indo ao ISE e se o ISE lhe responde com seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT:

```

539 12:45:58.142457 192.168.10.10 192.168.10.21 DNS 125 Standard query response 0xd5c0 A google.com A 192.168.10.10 NS sinkholens A 192.168.10.10
540 12:45:58.142552 192.168.10.10 192.168.10.21 DNS 125 Standard query response 0xa18e A google.com A 192.168.10.10 NS sinkholens A 192.168.10.10

```

```

> Frame 539: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0
> Ethernet II, Src: Vmware_be:1f:d7 (00:0c:29:be:1f:d7), Dst: WistronI_52:3f:d9 (3c:97:0e:52:3f:d9)
> Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 49823 (49823)
* Domain Name System (response)
  [Request In: 538]
  [Time: 0.000917000 seconds]
  Transaction ID: 0xd5c0
  > Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 1
  * Queries
    > google.com: type A, class IN
  * Answers
    > google.com: type A, class IN, addr 192.168.10.10
  * Authoritative nameservers
    > <Root>: type NS, class IN, ns sinkholens

```

Verifique se o HTTP reorienta trabalhos corretamente. Depois que obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT do recurso e estabelece uma conexão de TCP ao ISE, o cliente envia um pedido HTTP GET ao ISE. Isto pode ser confirmado em uma captura de pacote de informação do lado do cliente:

```

544 12:45:58.145234 192.168.10.21 192.168.10.10 HTTP 338 GET / HTTP/1.1
546 12:45:58.362935 192.168.10.10 192.168.10.21 HTTP 393 HTTP/1.1 302 Found
739 12:46:31.746585 192.168.10.21 239.255.255.250 SSDP 557 NOTIFY * HTTP/1.1

```

```

> Frame 544: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits) on interface 0
> Ethernet II, Src: WistronI_52:3f:d9 (3c:97:0e:52:3f:d9), Dst: Vmware_be:1f:d7 (00:0c:29:be:1f:d7)
> Internet Protocol Version 4, Src: 192.168.10.21, Dst: 192.168.10.10
> Transmission Control Protocol, Src Port: 49447 (49447), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 284
* Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
  Host: google.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-GB,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://google.com/]
  [HTTP request 1/1]
  [Response in frame: 546]

```

Ao mesmo tempo, o ISE determina se qualquer sessão existe para este cliente. Este processo de consulta da sessão no ISE pode ser log dentro verificado do prrt-Gerenciamento:

Após a consulta da sessão, o ISE retorna a reorientação URL ao cliente em uma resposta HTTP 302:

```

544 12:45:58.145234 192.168.10.21 192.168.10.10 HTTP 338 GET / HTTP/1.1
546 12:45:58.362935 192.168.10.10 192.168.10.21 HTTP 393 HTTP/1.1 302 Found
739 12:46:31.746585 192.168.10.21 239.255.255.250 SSDP 557 NOTIFY * HTTP/1.1

```

```

> Frame 546: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
> Ethernet II, Src: Vmware_be:1f:d7 (00:0c:29:be:1f:d7), Dst: WistronI_52:3f:d9 (3c:97:0e:52:3f:d9)
> Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.21
> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49447 (49447), Seq: 1, Ack: 285, Len: 339
* Hypertext Transfer Protocol
  > HTTP/1.1 302 Found\r\n
  Location: https://skuchere-ise21local.example.com:8443/portal/gateway?sessionId=C0A80A01000000291A109D9D&portal=6acc2e20
  Transfer-Encoding: chunked\r\n
  Date: Sun, 03 Apr 2016 10:45:40 GMT\r\n
  Server: \r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.217701000 seconds]
  [Request in frame: 544]
  > HTTP chunked response

```