Exemplo de Configuração de Autenticação da Web Local do Portal de Convidado do Identity Services Engine

Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Informações de Apoio Configurar Processo LWA com o Portal de Convidado do ISE Diagrama de Rede Pré-requisitos de configuração Configurar o WLC Configure o ISE externo como a URL da Web globalmente Configurar as listas de controle de acesso (ACLs) Configurar o SSID (Service Set Identifier, Identificador do conjunto de servicos) para LWA **Configurar o ISE** Definir o dispositivo de rede Configurar a política de autenticação Configurar a política de autorização e o resultado Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar a autenticação da Web local (LWA) com o portal de convidado do Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Cisco Wireless LAN Controller (WLC)

Componentes Utilizados

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

- ISE versão 1.4
- WLC versão 7.4

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.

Informações de Apoio

Este documento descreve a configuração do LWA. No entanto, a Cisco recomenda que você use a CWA (Centralized Web Authentication) com o ISE sempre que possível. Há alguns cenários em que o LWA é preferencial ou a única opção, portanto, este é um exemplo de configuração para esses cenários.

Configurar

O LWA requer determinados pré-requisitos e uma configuração principal na WLC, bem como algumas alterações necessárias no ISE.

Antes de abordá-las, aqui está um esboço do processo LWA com o ISE.

Processo LWA com o Portal de Convidado do ISE

- 1. O navegador tenta buscar uma página da Web.
- 2. A WLC intercepta a solicitação HTTP(S) e a redireciona para o ISE.

Várias informações importantes são armazenadas nesse cabeçalho de redirecionamento HTTP. Aqui está um exemplo do URL de redirecionamento:

https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-

state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28 :cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/

No exemplo de URL, você pode ver que o usuário tentou acessar "yahoo.com". O URL também contém informações sobre o nome da Rede Local Sem Fio (WLAN - Wireless Local Area Network) (mlatosie_LWA) e os endereços MAC do ponto de acesso e do cliente (AP). No exemplo de URL, **1.1.1.1** é a WLC, e **mlatosieise.wlaaan.com** é o servidor ISE.

- 3. O usuário recebe a página de login de convidado do ISE e digita o nome de usuário e a senha.
- 4. O ISE executa a autenticação em relação à sua sequência de identidade configurada.
- 5. O navegador é redirecionado novamente. Desta vez, ele envia credenciais para a WLC. O navegador fornece o nome de usuário e a senha que o usuário inseriu no ISE sem nenhuma interação adicional do usuário. Aqui está um exemplo de solicitação GET para a WLC. GET

/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ity h&buttonClicked=4&err_flag=0

Novamente, o URL original (**yahoo.com**), o nome de usuário (**mlatosie@cisco.com**) e a senha (**ityh**) estão incluídos.

Note: Embora a URL esteja visível aqui, a solicitação real é enviada pela SSL (Secure Sockets Layer), indicada pelo HTTPS, e é difícil de interceptar.

- 6. A WLC usa RADIUS para autenticar esse nome de usuário e senha em relação ao ISE e permitir o acesso.
- 7. O usuário é redirecionado para o portal especificado. Consulte a seção "**Configurar o ISE** externo como o URL da Web" deste documento para obter mais informações.

Diagrama de Rede

Esta figura descreve a topologia lógica dos dispositivos usados neste exemplo.



Pré-requisitos de configuração

Para que o processo LWA funcione corretamente, um cliente precisa obter:

- Configuração de endereço IP e máscara de rede
- Rota padrão
- Servidor do Sistema de Nomes de Domínio (DNS)

Todos eles podem ser fornecidos com DHCP ou com a configuração local. A resolução DNS precisa funcionar corretamente para que o LWA funcione.

Configurar o WLC

Configure o ISE externo como a URL da Web globalmente

Em Security > Web Auth > Web Login Page, você pode acessar essas informações.

MONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			
Web Logi	n Page										
						_					
Web Auth	Web Authentication Type			ernal (Redirect	to external server)	0					
Redirect L	IRL after log	gin									
External Webauth URL				https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=2							
			Treep.			per unit en consecu		harden w			

Note: Este exemplo usa um URL de Webauth Externo e foi extraído do ISE Versão 1.4. Se você tiver uma versão diferente, consulte o guia de configuração para entender o que deve ser configurado.

Também é possível configurar essa configuração por WLAN. Ela está nas configurações de segurança específicas da WLAN. Eles substituem a configuração global.

Para descobrir a URL correta para o seu portal específico, escolha ISE > Guest Policy > Configure > your specific portal. Clique com o botão direito do mouse no link "URL de teste do portal" e escolha copiar local do link.

cisco Identity Services E	ngine		🟠 Home	Operations 🛛 🔻	Policy 🔻	Guest Access
Configure Manage	Accounts 🔜	Settings				
Portals Settings and Custon	nization					
Portal Name: *	Description:					
Sponsored Guest Portal (default)	Sponsors create g	guest accounts, and	guests access	the network using	their Portal t	test URL

Neste exemplo, o URL completo é:

https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9

Configurar as listas de controle de acesso (ACLs)

Para que a autenticação da Web funcione, o tráfego permitido deve ser definido. Determine se as ACLs FlexConnect ou ACLs normais devem ser usadas. Os APs FlexConnect usam ACLs FlexConnect, enquanto os APs que usam comutação centralizada usam ACLs normais.

Para entender em que modo um AP específico opera, escolha **Wireless > Access points** e escolha a caixa suspensa **AP name > AP Mode**. Uma implantação típica é **local** ou **FlexConnect**.

Em Segurança > Listas de Controle de Acesso, escolha ACLs FlexConnect ou ACLs. Neste exemplo, todo o tráfego UDP foi permitido para permitir especificamente o intercâmbio e o tráfego de DNS para o ISE (10.48.66.107).

0011												
Acces	s List Name	FLEX_0	GUE	ST								
Deny	Counters	63475	2									
Seq	Action	Source IP/Mas	k	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	Any	Any	Any	208398	
2	Permit	10.48.66.107 255.255.255.25	/ 5	0.0.0.0 0.0.0.0	/	TCP	Any	Any	Any	Any	32155	
3	Permit	0.0.0.0	/	10.48.66.107 255.255.255.25	/ 5	TCP	Any	Any	Any	Any	24532	

Este exemplo usa o FlexConnect, então **tanto** o FlexConnect quanto as ACLs padrão são definidas.

Esse comportamento é documentado no Cisco Bug ID <u>CSCue68065</u> em relação aos controladores WLC 7.4. Ele não é mais necessário no WLC 7.5, onde você só precisa de uma FlexACL e não precisa mais de uma ACL padrão

Configurar o SSID (Service Set Identifier, Identificador do conjunto de serviços) para LWA

Em WLANs, escolha a ID da WLAN para editar.

Configuração do Web Auth

General

Aplique as mesmas ACLs definidas na etapa anterior e habilite a autenticação da Web.

General Security	QoS Advanced				
Layer 2 Layer 3	AAA Servers				
Layer 3 Security None	\$				
Veb Policy					
Authentication					
O Passthrough					
O Conditional Web Redin	ect				
Splash Page Web Redi	rect				
On MAC Filter failure	2				
Preauthentication ACL	IPv4 FLEX_GUEST	IPv6 None	WebAuth FlexAcl	FLEX_GUEST	4
Over-ride Global Config	Enable				

Note: Se o recurso de comutação local do FlexConnect for usado, o mapeamento da ACL precisará ser adicionado no nível do AP. Isso pode ser encontrado em **Wireless > Access Points.** Escolha o **nome do AP** apropriado **> FlexConnect > External WebAuthentication ACLs**.

WLANs > Edit 'mlatosie_LWA'

All APs > APc89c.1d6e.a3cd > ACL Mappings

Sase Radio MAC	D8:De:DF:14:41:90	
VLAN ACL Mapp	bing	_
WLAN Id 0		
WebAuth ACL FI	LEX_GUEST ÷)
A	dd	
	au	
	AN Profile Name	WebAuth ACL
WLAN Id WLAN	AN Profile Name	WebAuth ACL
WLAN Id WLAN WebPolicies	AN Profile Name	WebAuth ACL
WLAN Id WLAN WebPolicies WebPolicy ACL	AN Profile Name	WebAuth ACL

Autenticação, autorização e configuração do servidor de contabilidade (AAA)

Neste exemplo, os servidores de autenticação e tarifação apontam para o servidor ISE definido anteriormente.

General	Security	QoS	Advanced						
Layer 2	Layer 3	AAA Se	ervers						
Select AAA	servers belo	w to over	ide use of defa	ault servers on	this WLAN				
Radius Servers									
Radius	Server Overwri	te interface	e Enabled						
			Authenticati	on Servers	Accounting Servers				
			🗹 Enabled		🗹 Enabled				
Server	1		IP:10.48.66	.107, Port:1812	‡] IP:10.48.66.107, Port:1813	\$			

Note: Os padrões na guia Avançado não precisam ser acrescentados.

Configurar o ISE

A configuração do ISE consiste em várias etapas.

Primeiro, defina o dispositivo como um dispositivo de rede.

Em seguida, assegure-se de que as regras de autenticação e autorização que acomodam essa troca existam.

Definir o dispositivo de rede

Em Administration > Network Resources > Network Devices, preencha estes campos:

- Nome de dispositivo
- Endereço IP do dispositivo
- Configurações de autenticação > Segredo compartilhado

III. I			10 M M	
10.1	0134	OPER .	Dovicor	
			LEVILES	
				-

	* Name Description	e WLC_7510-2			
	* IP Address:	10.48.39.88	32		
	Model Name Software Version	e 🛛 👻			
	* Network Devic	e Group			
	WLC Location	WLAAAN WLCs 📀	Set To Default Set To Default		
	Device Type	All Device Types 📀	Set To Default		
✓	✓ Authentication Set	ttings			
		Enable Au	thentication Settings Protocol	RADIUS	
			* Shared Secret	••••	Show

Configurar a política de autenticação

Em **Política > Autenticação**, adicione uma nova política de autenticação.

Este exemplo usa estes parâmetros:

- Nome: WLC_LWA_Guests
- Condição: Airespace:Airespace-Wlan-Id. Essa condição corresponde ao ID da WLAN 3, que é o ID do WLAN mlatosie_LWA que foi definido anteriormente na WLC.
- {opcional} Permite protocolos de autenticação que não exigem o certificado Non_Cert_Auth, mas os padrões podem ser usados.
- Guest_Portal_Sequence, que define que os usuários são usuários convidados definidos localmente.



Configurar a política de autorização e o resultado

Em Política > Autorização, defina uma nova política. Pode ser uma política muito básica, como:

		WLC_LWA_Guests	ActivatedGuest		PermitAccess
--	--	----------------	----------------	--	--------------

Essa configuração depende da configuração geral do ISE. Este exemplo é propositalmente simplificado.

Verificar

No ISE, os administradores podem monitorar e solucionar problemas de sessões ao vivo em **Operações > Autenticações**.

Duas autenticações devem ser vistas. A primeira autenticação é do portal do convidado no ISE. A segunda autenticação vem como uma solicitação de acesso da WLC ao ISE.

May 15,13 02:04:02.589 PM	2	9	mlatosie@cisco.com	WLC_7510-2	PermitAccess	ActivatedGuest	Authentication succeeded
May 15,13 02:03:59.819 PM	~	ò	mlatosie@cisco.com			ActivatedGuest	Guest Authentication Passed

Você pode clicar no ícone Authentication Detail Report para verificar quais políticas de autorização e de autenticação foram escolhidas.

Na WLC, um administrador pode monitorar clientes em Monitor > Client.

Aqui está um exemplo de um cliente que foi autenticado corretamente:

28:df:e9:13:47:db APc89c.1d6e.a3cd mlatosie_LWA mlatosie_LWA mlatosie@cisco.com 802.11bn Associated Yes 1 No

Troubleshoot

A Cisco recomenda que você execute depurações por meio do cliente sempre que possível.

Através da CLI, essas depurações fornecem informações úteis:

debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable

Informações Relacionadas

- Guia de configuração do Cisco ISE 1.x
- Guia de configuração do Cisco WLC 7.x
- Suporte Técnico e Documentação Cisco Systems