Autenticación externa AsyncOS con Cisco Identity Service Engine (Radius)

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Diagrama de la red Paso 1. Cree un grupo de identidad para la autenticación. Paso 2. Crear usuarios locales para autenticación. Paso 3. Crear perfiles de autorización. Paso 4. Cree una política de autorización. Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe la configuración requerida entre el dispositivo de seguridad Email Security Appliance (ESA) / Security Management Appliance (SMA) y Cisco Identity Services Engine (ISE) para una implementación exitosa de la autenticación externa con RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación, autorización y administración (AAA)
- Atributo RADIUS CLASS.
- Políticas de autorización y gestión de identidades de Cisco ISE.
- Funciones de usuario de Cisco ESA/SMA.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0

• Cisco SMA 13.6.2

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

No se probó la versión fuera de las enumeradas en la sección de componentes utilizados.

Antecedentes

Atributo Radius CLASS

Utilizado para la contabilidad, es un valor arbitrario que el servidor RADIUS incluye en todos los paquetes de contabilización.

El atributo class se configura en ISE (RADIUS) por grupo.

Cuando se considera que un usuario forma parte del grupo ISE/VPN que tiene el atributo 25 vinculado a él, el NAC aplica la política basándose en las reglas de asignación configuradas en el servidor de Identity Services Engine (ISE).

Configurar

Diagrama de la red



Identity Service Engine acepta las solicitudes de autenticación de ESA/SMA y las compara con una identidad de usuario y un grupo.

Paso 1. Cree un grupo de identidad para la autenticación.

Inicie sesión en el servidor ISE y Crear un grupo de identidades:

Vaya a Administration->Identity Management->Groups->User Identity Group. Como se muestra en la imagen.



Nota: Cisco recomienda un grupo de identidad en ISE para cada función ESA/SMA asignada.

Paso 2. Crear usuarios locales para autenticación.

En este paso, cree nuevos usuarios o asigne usuarios que ya existan al grupo de identidad que creamos en el paso 1. Inicie sesión en ISE y **navegue hasta Administration->Identity Management->Identities** y cree nuevos usuarios o asígneles a los usuarios de los grupos que ha creado. Como se muestra en la imagen.

Network Acce	ess Users	List > New Networ	k Access User				
 Networ 	rk Access	s User					
* Name	ESA_adm	in					
Status	🗹 Enab	oled 👻					
Email [admins@	mydomain.com					
▼ Passw	vords						
Passwor	rd Type:	Internal Users	•				
		Password		Re-Enter Password			
* Login F	Password	•••••				Generate Password) ()
Enable F	Password					Generate Password) ()
▼ User I	Informat	ion	User Groups	Q			
First Nar	me		<₽ • ■ •				
Last Nar	me		ALL_ACCOUNT	S (default)			
			Anyconnect				
 Accou 	int Optio	ns					
		Description	ESA_Admin				
			SA_DEMO				
Change	password	on next login		mins			
			SA_Monitor				
 Accou 	int Disab	le Policy	🕂 GROUP_ACCOU	JNTS (default)			
🗆 Dis	able accou	unt if date exceeds	GuestType_Cor	ntractor (default)	/y-mm-dd)		
			GuestType_Dai	ly (default)			
▼ User (Groups		GuestType_We	ekly (default)			
Select	an item	2					
Submit	Cancel]					

Paso 3. Crear perfiles de autorización.

La autenticación RADIUS se puede completar correctamente sin perfiles de autorización; sin embargo, no se asignaron roles. Para una configuración completa, **navegue hasta Política-**>**Elementos de política->Resultados->Autorización->Perfil de autorización.**

Nota: Cree un perfil de autorización por función que se va a asignar.

Authorization Profiles > Aav	ega_ESA_Admin
Authorization Profile	
* Name	ESA_Admin
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	delle Cisco 🗶 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
 Common Tasks 	
Web Authentication (Local Web Auth)
Airespace ACL Name	•
🗹 ASA VPN	Administrators 📀
AVC Profile Name	
 Advanced Attribute 	es Settings
Select an item	

Nota: Asegúrese de utilizar el atributo de clase radius 25 y proporcione un nombre. Este nombre debe coincidir con la configuración de AsyncOS (ESA/SMA). En la figura 3, Administradores es el nombre del atributo CLASS.

Paso 4. Cree una política de autorización.

Este último paso permite al servidor ISE identificar los intentos de inicio de sesión del usuario y asignar al perfil de autorización correcto.

En el caso de una autorización correcta, ISE devuelve un access-accept junto con el valor CLASS definido en el perfil de autorización.

Vaya a Política > Conjuntos de políticas > Agregar (+ símbolo)

ſ	+	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits	Actions	View
L	Search									
I	/	ø	New Policy Set 1			+	Select from list		٥	>

Asigne un nombre y seleccione el símbolo más para agregar las condiciones necesarias. Este entorno de laboratorio utiliza un Radius. NAS-IP-Address. Guarde la nueva política.

dentity S	Services Engine Home	Context Visibility		Work Centers	1	License Warning 🔺	Q,	0 (o c
Policy Sets F	Profiling Posture Client Provisionin	Policy Elements			Click here to do	visibility setup Do not	show this	s again.	×
Policy Sets					Reset Po	licyset Hitcounts	R	Reset	Save
+ Status	Policy Set Name	Description	Conditions	Allo	wed Protocols / Se	rver Sequence	Hits	Actions	View
Search									
0	ESA_Policy		Network Access-Device IF	P Address EQUALS 10.122.111.238	efault Network Access	× • +	16	٥	>

Para que las solicitudes de autorización coincidan correctamente, se deben agregar las

condiciones. Seleccionar

y agregar condiciones.

El entorno de laboratorio utiliza InternalUser-IdentityGroup y coincide con cada perfil de autorización.

➤ Auth	orization F	Policy (5)						
•					Results			
+	Status	Rule Name	Cond	litions	Profiles	Security Groups	Hits	Actions
Search	h							
	Ø	ESA Monitor	48-	InternalUser-IdentityGroup EQUALS User Identity Groups:ESA_Monitor	*ESA_Monitors +	Select from list 👻 🕇	0	٥
	Ø	ESA HelpDesk	48.	InternalUser-IdentityGroup EQUALS User Identity Groups:HelpDesk	×ESA_admin +	Select from list • +	0	٥

Paso 5. Habilite la autenticación externa en AsyncOS ESA/ SMA.

>

Inicie sesión en el dispositivo AsyncOS (ESA/SMA/WSA). Y **navegue hasta Administración del sistema > Usuarios > Autenticación externa > Habilitar autenticación externa** en ESA.

Edit External Authentication



Proporcione estos valores:

- Nombre de host del servidor RADIUS
- Puerto
- secreto compartido
- Valor de tiempo de espera (en segundos)
- Protocolo de autenticación

Seleccione Asignar usuarios autenticados externamente a varias funciones locales (recomendado). Como se muestra en la imagen.

Edit External Authentication

External Authentication Settings								
C Enable External Authentication								
Authentication Type:	RADIUS 😌							
RADIUS Server Information:	RADIUS Server Hostname	Port	Shar	ed Secret	Timeout Value (in seconds)	Authentic protocol	cation	Add Row
	x.x.x.x	1812	••••	••••	5	РАР	0	Ŵ
External Authentication Cache Timeout: ⑦	0 seconds							
Group Mapping:	Map externally authe	nticated u	sers to	multiple local roles	(recomme	ended)		
	RADIUS CLASS At	ribute		Role 🕐			A	dd Row
	Administrators			Administrator	0			Ŵ
	Monitors			Operator	0			۱.
	RADIUS CLASS attr	<i>ibutes are</i> enticated	case-s	sensitive. to the Administrator	role.		1	
Canad								Cubmit

Nota: El atributo de clase Radius DEBE coincidir con el nombre del atributo definido en el paso 3 (en tareas comunes asignadas como VPN ASA).

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Inicie sesión en su dispositivo AsyncOS y confirme que se ha concedido acceso y que la función asignada se ha asignado correctamente. Como se muestra en la imagen con la función de usuario invitado.

	2000V			Email Security Appliance is get
CISCO Email Secur	rity Virtual Appliance			
Monitor				
My Dashboard				
				🃜 Printable PDF 🗗
Attention — 🔺 You ca	an customize this "My Dashboard" p	bage by addi	ng report modules from different repor	ts.
> Ove	erview.		nview page can be accessed from Pion	
> Ove	rview.		aview page can be accessed non mon	•
System Overview Overview > Status	rview.		Overview > Quarantines - Top 3 by Disk I	Jsage (Policy and Virus)
System Overview Overview > Status	System Status:	Online	Overview > Quarantines - Top 3 by Disk (No quarantines are available	Jsage (Policy and Virus)
> Over System Overview Overview > Status	System Status: Incoming Messages per hour:	Online 0	Overview > Quarantines - Top 3 by Disk U No quarantines are available	Jsage (Policy and Virus)
> Ove	System Status: Incoming Messages per hour: Messages in Work Queue:	Online 0	Overview > Quarantines - Top 3 by Disk (No quarantines are available	Jsage (Policy and Virus)

Troubleshoot

Si el intento de inicio de sesión no funciona en el ESA con el mensaje "Nombre de usuario o contraseña no válidos". El problema podría estar en la Política de autorización.

Inicie sesión en ESA y, desde Autenticación externa, seleccione Asignar todos los usuarios autenticados externamente a la función de administrador.

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

Envíe y confirme los cambios. Realice un nuevo intento de inicio de sesión. En caso de que se inicie sesión correctamente, verifique dos veces el perfil de autorización de ISE Radius (atributo CLASS 25) y la configuración de la política de autorización.

Información Relacionada

- Guía de usuario de ISE 2.4
- Guía de usuario de AsyncOS