ASA/PIX 7.X: Examen global predeterminado de la neutralización y Inspección de la aplicación no valor por defecto del permiso usando el ASDM

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Productos Relacionados Convenciones Política global predeterminada Inspección de la aplicación del no valor por defecto del permiso Verificación Información Relacionada

Introducción

Este documento describe cómo quitar la inspección predeterminada de la política global para una aplicación y cómo habilitar la inspección para una aplicación no predeterminada.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante de Cisco (ASA) esos funcionamientos la imagen del software 7.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con el dispositivo de seguridad PIX que funciona con

la imagen del software 7.x.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco</u> para obtener más información sobre las convenciones del documento.

Omita la política global

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique ciertos exámenes al tráfico en todas las interfaces (una política global). No todos los exámenes se habilitan por abandono. Usted puede aplicar solamente una política global. Si usted quiere alterar la política global, usted debe editar la política predeterminada o inhabilitarla y aplicar un nuevo. (Una directiva de la interfaz reemplaza la política global.)

La configuración de la política predeterminada incluye estos comandos:

```
class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
service-policy global_policy global
```

Inspección de la aplicación del no valor por defecto del permiso

Complete este procedimiento para habilitar la Inspección de la aplicación no valor por defecto en Cisco ASA:

1. Inicie sesión al ASDM. Vaya a las reglas de la configuración > del Firewall > de la política de servicio.

g	ionfiguration > Firew	vall > 9	Service Pol	icy Rules					
	🗣 Add 🔻 🗹 Edit 🎁 Delete 🆙 🌾 👗 🖳 📖 🗸 🔍 Find 🖽 Diagram 🔍 Packet Trace								
	Traffic Classification						P. J. 1. 1		
	Name	#	Enabled	Match	Source	Destination	Service	Time	RUB ACCOLS
	🖃 Global; Policy: global	policy	,						
	inspection_default			La Match	🆘 any	🌵 any	🔍 default-inspe		 Inspect DNS Map prese Inspect ESMTP (12 more inspect actions)

2. Si usted quiere guardar la configuración para la política global que incluye el Clase-mapa predeterminado y el Directiva-mapa del valor por defecto, pero quiere quitar la directiva global, vaya a las herramientas > a la interfaz de línea de comando y no utilice el ningún comando global de la política global de la servicio-directiva de quitar la directiva global. Entonces, el tecleo envía así que el comando se aplica al ASA.

🚰 Command Line Interface	×						
Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.							
Single Line Multiple Line Enable context sensitive help (?)							
no service-policy global_policy global							
Response:	2						
Result of the command: "no service-policy global_policy global"							
The command has been sent to the device							
Clear Response							
Send Close Help							

Nota: Con este paso la política global llega a ser invisible en el Administrador de dispositivos de seguridad adaptante (ASDM), pero se muestra en el CLI.

3. El tecleo **agrega** para agregar una nueva directiva como se muestra aquí:

aqui.	Jui.							
Configuration	n > Firewall > Service Policy Rules							
🗣 Add 👻 (📑 Edit 📋 Delete 🛧 🎸 🐰 ங 🛍 - 🔍 Find	d 🖭 Diagram 🐙 Packet Trace						
Traffic Classification								
Name	# Enabled Match Source	Destination Service	Time	KUB ACCUIS				

4. Aseegurese el botón de radio al lado de la **interfaz** se marca y eligen la interfaz que usted quiere aplicar la directiva del menú desplegable. Entonces, proporcione el **nombre de la**

directiva y la descripción. Haga clic en Next

/ O !	· · ·	`
(Sidu	Indinta	۱.
loigu		J.

🖆 Add Service P	Policy Rule Wizard - Service Policy		×						
Adding a new service Step 1: Configure & Step 2: Configure & Step 3: Configure &	Adding a new service policy rule requires three steps: Step 1: Configure a service policy. Step 2: Configure the traffic classification criteria for the service policy rule. Step 3: Configure actions on the traffic classified by the service policy rule. Create a Service Policy and Apply To:								
Create a Service Policy and Apply To: Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a nervice into the existing service policy. Otherwise, you can create a new service policy.									
 Interface: 	outside - (create new service policy) 🔽								
Policy Name:	outside-policy								
Description:	Policy on outside interface								
🔘 Global - appli	es to all interfaces	—							
Policy Name:	global-policy								
Description:			ן ן						
		< Back Next > Cancel He	P						

 Cree un nuevo clase-mapa para hacer juego tráfico TCP como el HTTP baja bajo el TCP. Haga clic en Next (Siguiente).

🖆 Add Service Policy Rule Wiza	rd - Traffic Classification Crit	leria	
• Create a new traffic class: outside	e-class]	
Description (optional):		•	
Traffic Match Criteria			
Default Inspection Traffic			
Source and Destination IP Ad	dress (uses ACL)		
Tunnel Group	_		
TCP or UDP Destination Port			
RTP Range	-		
IP DiffServ CodePoints (DSCP)		
IP Precedence	N		
Any traffic	13		
OUse an existing traffic class: insp	ection_default 📝		
OUse class-default as the traffic class			
If traffic does not match a existing t situation.	raffic class, then it will match the class	s-default traffic class. Class-default can be used in cat	ch all
		< Back Next > Cancel	Help

6. Elija el **TCP** como el protocolo.

🖆 Add Service Policy Rule Wizard - Traffic Match - Destination Port	
Protocol: UDP Service:	
To specify port range for the service, use nnn-nnn hormat.	
< Back Next > Cancel	Help

Elija el **puerto HTTP 80** como el servicio y haga clic la **AUTORIZACIÓN**.

C	Browse Service						
	🗣 Add 👻 📝 Edit	î Delete	0				
	iter:		~				Filter Clear
	ii.ci i	1					r inter [clear]
	Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
	= Prederined	ben.	default (1,65535)	5190			<u>^</u>
		ten	default (1-65535)	179			
	byp	ten	default (1-65535)	10			
	chargen	tro	default (1-65535)	3020			
	in citriv-ica	hen	default (1-65535)	1494			1
		ten	default (1-65535)	2748			
	- to daytime	tcp	default (1-65535)	13			
	discard	tcp	default (1-65535)	9			
		tcp	default (1-65535)	53			
	techo	tcp	default (1-65535)	7			
	TOP exec	tcp	default (1-65535)	512			
		tcp	default (1-65535)	79			
	TO ftp	tcp	default (1-65535)	21			
	🐨 🐨 ftp-data	tcp	default (1-65535)	20			
	gopher	tcp	default (1-65535)	70			
	10 h323	tcp	default (1-65535)	1720			
	nostname	tcp	default (1-65535)	101			
	- 🐨 http	tcp	default (1-65535)	80			
	- 100 https	tcp	default (1-65535)	443			
	ident	tcp	default (1-65535)	113			~
5	elected Service						
	Service >	n Astel					
	Service ->	.p/ncp					
						OK	Cancel
						- VA	Carlor

7. Elija el **HTTP** y el clic en Finalizar.

Add Service Pol	icy Rule Wizard - Ri	ule Actions
Protocol Inspection	Intrusion Prevention Co	onnection Settings QoS
CTIONS		
	Castinua	
	Configure	_
	Configure	_
E ETP	Configure	
	Configure	
- H.323 H.225	Configure	
H.JZJ KAS	Configure	
	Configure	
ICMP Error		
	Castlerus	
	Configure	
IPSec-Pass-T	nru Configure	
MGCP	Configure	
NETBIOS	Configure	
PPTP		
RSH		
RTSP	Configure	
SCCP (Skinny) Configure	×
		< Back Finish Cancel Help

8. El tecleo **se aplica** para enviar estos cambios de configuración al ASA del ASDM. Esto completa la

со	onfi	gura	aci	ción.		
-						

ç	ionfiguration > Fire	wall > 5	iervice Poli	cy Rules						
	🗣 Add 🝷 🗃 Edit 📋 Delete 🛧 🌾 👗 🦓 🎟 👘 🗸 🗛 Find 🖼 Diagram 💐 Packet Trace									
Traffic Classification Rule Actions										
	Name	#	Enabled	Match	Source	Destination	Service	Time	Rule Accors	
	□ Interface: outside;	Policy: o	outside-policy	,						
	outside-class			🕒 Match	🍫 any	🍫 any	😥 http		Inspect HTTP	
	<u>د</u>				10					X
						7				
					Apply	Reset				

Verificación

Utilice estos comandos show de verificar la configuración:

• Utilice el **comando class-map del funcionamiento de la demostración** de ver las correspondencias de la clase configuradas.

```
ciscoasa# sh run class-map
 Т
 class-map inspection_default
 match default-inspection-traffic
 class-map outside-class
 match port tcp eq www

    Utilice el comando policy-map del funcionamiento de la demostración de ver las

 correspondencias de políticas configuradas.
 ciscoasa# sh run policy-map
 policy-map type inspect dns preset_dns_map
  parameters
   message-length maximum 512
 policy-map global_policy
  class inspection_default
   inspect dns preset_dns_map
   inspect ftp
   inspect h323 h225
   inspect h323 ras
   inspect rsh
   inspect rtsp
   inspect esmtp
   inspect sqlnet
   inspect skinny
   inspect sunrpc
   inspect xdmcp
   inspect sip
   inspect netbios
   inspect tftp
 policy-map outside-policy
  description Policy on outside interface
  class outside-class
   inspect http
```

 Utilice el comando service-policy del funcionamiento de la demostración de ver las políticas de servicio configuradas.

```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- Referencias de comandos de las 5500 Series de Cisco ASA
- Página de soporte del Cisco Adaptive Security Device Manager (ASDM)
- <u>Cisco PIX Firewall Software</u>
- Solicitudes de Comentarios (RFC)
- Dispositivos de seguridad Cisco PIX de la serie 500
- Aplicación del examen del Application Layer Protocol
- <u>Referencias de Comandos de Cisco Secure PIX Firewall</u>
- Soporte Técnico y Documentación Cisco Systems