ASA 8.3 y posterior - Configuración de la inspección mediante ASDM

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Política global predeterminada Inhabilitar la inspección global predeterminada para una aplicación Habilitar inspección para aplicación no predeterminada Información Relacionada

Introducción

Este documento proporciona una configuración de ejemplo para Cisco Adaptive Security Appliance (ASA) con las versiones 8.3(1) y posteriores sobre cómo eliminar la inspección predeterminada de la política global para una aplicación y cómo habilitar la inspección para una aplicación no predeterminada mediante Adaptive Security Device Manager (ASDM).

Consulte <u>PIX/ASA 7.x: Inhabilite la Inspección Global Predeterminada y Enable Non-Default</u> <u>Application Inspection</u> para la misma configuración en Cisco ASA con las versiones 8.2 y anteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la versión 8.3(1) del Cisco ASA Security Appliance Software con ASDM 6.3.

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Política global predeterminada

De forma predeterminada, la configuración incluye una política que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica ciertas inspecciones al tráfico en todas las interfaces (una política global). No todas las inspecciones están habilitadas de forma predeterminada. Sólo puede aplicar una política global. Si desea modificar la directiva global, debe editar la directiva predeterminada o desactivarla y aplicar una nueva. (Una política de interfaz invalida la política global.)

En ASDM, elija **Configuration > Firewall > Service Policy Rules** para ver la política global predeterminada que tiene la inspección de aplicación predeterminada como se muestra aquí:



La configuración de 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

Si necesita inhabilitar la política global, utilice el comando **no service-policy global_policy**. Para eliminar la política global usando ASDM elija **Configuration > Firewall > Service Policy Rules**. A continuación, seleccione la política global y haga clic en **Eliminar**.

Configuration > Fire	wall > Service Pol	licy Rules						
🖶 Add 🕞 🎯 Edit 🕯	📋 Delete 🔶 🗲	🕹 🖕 🛍	Q Fit	nd 📴 Diagram	😋 Packet Trace			
Traffic Classification								Bula Artisoc
Name	*	Enabled	Match	Source	Destination	Service	Time	KUB ALLOIS
🗄 Global; Policy: globa	_policy							
inspection_default			Match	st any	🍨 any	default-inspec		Inspect DNS Map preset_dns_map Inspect ESMTP
								(13 more inspect actions)

Nota: Cuando elimina la política de servicio con ASDM, se eliminan la política asociada y los mapas de clase. Sin embargo, si se elimina la política de servicio mediante CLI, sólo se quita la política de servicio de la interfaz. El mapa de clase y el mapa de política permanecen inalterados.

Inhabilitar la inspección global predeterminada para una aplicación

Para inhabilitar la inspección global para una aplicación, utilice la versión no del comando inspect.

Por ejemplo, para quitar la inspección global de la aplicación FTP a la que escucha el dispositivo de seguridad, utilice el comando **no inspect ftp** en el modo de configuración de clase.

Se puede acceder al modo de configuración de clase desde el modo de configuración de policy map. Para quitar la configuración, utilice la forma *no* del comando.

```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#no inspect ftp
```

Para inhabilitar la inspección global para FTP mediante ASDM, complete estos pasos:

Nota: Refiérase a <u>Permiso de Acceso HTTPS para ASDM</u> para la configuración básica para acceder al PIX/ASA a través de ASDM.

 Elija Configuration > Firewall > Service Policy Rules y seleccione la política global predeterminada. A continuación, haga clic en Editar para editar la directiva de inspección global.

3	giobai.								
	Configuration > Firewall > Servic	e Polic	y Rules						
	🗣 Add 🔹 🗹 Edit 📋 Delete 📑	14	አ 🖻 🛍	 Q Fit 	nd 📴 Diagram	🥂 Packet Trace			
I	Traffic Classification								Dula Antiona
I	Name	#	Enabled	Match	Source	Destination	Service	Time	Rule actions
I	🗄 Global; Policy: global_policy								
	inspection_default			Match	🔨 any	🧐 any	• default-inspec		🔍 Inspect DNS Map preset_dns_map
									Inspect ESMTP (13 more losned; actions)

 En la ventana Edit Service Policy Rule, elija Protocol Inspection en la ficha Rule Actions. Asegúrese de que la casilla de verificación FTP esté desactivada. Esto inhabilita la inspección FTP como se muestra en la siguiente imagen. A continuación, haga clic en Aceptar y, a continuación, Aplicar.

Protocol Inspection Intrus	on Prevention Connection Settings QoS NetFlow	
Select all inspection rul	35	
CTIQBE		
DCERPC	Configure	
INS DNS	Configure DNS Inspect Map: preset_dns_map	
C ESMTP	Configure	
ETR	Configure	
V H.323 H.225	Configure	
🗹 H.323 RAS	Configure	
HTTP	Configure	
ICMP		
ICMP Error		
ILS I		
IM 🔄	Configure	
IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
✓ NETBIOS	Configure	
PPTP		

Nota: Para obtener más información sobre la inspección de FTP, consulte <u>PIX/ASA 7.x: Ejemplo</u> <u>de Configuración de Enable FTP/TFTP Services</u>.

Habilitar inspección para aplicación no predeterminada

La inspección HTTP mejorada está desactivada de forma predeterminada. Para habilitar la inspección HTTP en global_policy, utilice el **comando inspect http** bajo class inspection_default.

En este ejemplo, cualquier conexión HTTP (tráfico TCP en el puerto 80) que entre en el dispositivo de seguridad a través de cualquier interfaz se clasifica para la inspección HTTP. *Debido a que la política es una política global, la inspección ocurre sólo cuando el tráfico entra en cada interfaz*.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

En este ejemplo, cualquier conexión HTTP (tráfico TCP en el puerto 80) que entre o salga del

ASA(config)#class-map outside-class ASA(config-cmap)#match port tcp eq www ASA(config)#policy-map outside-cisco-policy ASA(config-pmap)#class outside-class ASA(config-pmap-c)#inspect http ASA(config)#service-policy outside-cisco-policy interface **outside Realice estos pasos para configurar el ejemplo anterior usando ASDM:**

1. Elija **Configuration > Firewall > Service Policy Rules** y haga clic en **Add** para agregar una nueva política de

figuration > Firewall > Se	rvice Polic	y Rules						
Add - 🗹 Odt 🎁 Delete	++	👗 🗈 📾	- Q, n	nd 💽 Diagram	🔍 Packet Trace			
raffic Cassification								and a definition of
arre		Enabled	Natsh	Source	Destination	Service	Time	su e Actions
Slobal; Policy: global_policy								
inspection_default			Den Ha tch	() ay	10 ay	🔍 defaalt inspesii.		 Inspect DNS Hap preset_drs_map Inspect ESMTP If increaring pect actions)
								(18 more inspect actions)

2. En la ventana Asistente para agregar reglas de política de servicio - Política de servicio, elija el botón de opción junto a Interfaz. Esto aplica la política creada a una interfaz específica, que es la interfaz externa en este ejemplo. Proporcione un nombre de política, que es outside-cisco-policy en este ejemplo. Haga clic en Next (Siguiente).

🖆 Add Service I	Policy Rule Wizard - Service Policy	×
Adding a new servi Step 1: Configure Step 2: Configure Step 3: Configure Create a Service Pr	ice policy rule requires three steps: a service policy. the traffic classification criteria for the service policy rule. actions on the traffic classified by the service policy rule.	
rule into the exis	sting service policy. Otherwise, you can create a new service policy. outside - (create new service policy) • outside-cisco-bolicy	
Description:		
🔘 Global - appli	lies to all interfaces	
Policy Name:	global_policy	
Description:		
	< Back Next > Cancel He	:lp

3. En la ventana Asistente para agregar reglas de política de servicio - Criterios de clasificación de tráfico, proporcione el nuevo nombre de clase de tráfico. El nombre utilizado en este ejemplo es outside-class. Asegúrese de que la casilla de verificación junto a TCP o UDP Destination Port esté marcada y haga clic en Next.

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	×
Create a new traffic class:	outside-class	
Description (optional):		
Traffic Match Criteria		
Default Inspection Traff	ic	
Source and Destination	IP Address (uses ACL)	
Tunnel Group		
CP or UDP Destination	Port	
RTP Range		
IP DiffServ CodePoints	(DSCP)	
IP Precedence		
Any traffic		
O Use an existing traffic class:	inspection_default	
O Use class-default as the traffic	c dass.	
If traffic does not match a exi situation.	sting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all	
	< Back Next > Cancel Help	

4. En la ventana Add Service Policy Rule Wizard - Traffic Match - Destination Port, elija el botón de opción situado junto a TCP en la sección Protocol. A continuación, haga clic en el botón situado junto a Servicio para elegir el servicio requerido.

🕵 Add Service Policy Rule Wizard - Traffic Match - Destination Port
Protocol: TCP UDP
Service:
To specify port range for the service, use nnn-nnn format.

5. En la ventana Browse Service, elija **HTTP** como servicio. A continuación, haga clic en **Aceptar**.

Name	e	Protocol	Source Ports	Destination Ports	ICMP Type	Description	·
	- TC> ctiabe	tcp	default (1-65535)	2748	10. 1 1/po		~
	te daytime	tcp	default (1-65535)	13			
	10 discard	tcp	default (1-65535)	9			
	😰 domain	tcp	default (1-65535)	53			
	😰 echo	tcp	default (1-65535)	7			
	😰 exec	tcp	default (1-65535)	512			
	😰 finger	tcp	default (1-65535)	79			
	🐨 ftp	tcp	default (1-65535)	21			
	😰 ftp-data	tcp	default (1-65535)	20			
	😰 gopher	tcp	default (1-65535)	70			
	👳 h323	tcp	default (1-65535)	1720			
	😰 hostname	tcp	default (1-65535)	101			
	ne> http	top	default (1-65535)	80]		
	😰 https	tcp	default (1-65535)	443			
	👳 ident	tcp	default (1-65535)	113			
	😰 imap4	tcp	default (1-65535)	143			
	· 📭 inc	tcp	default (1-65535)	194			
	😰 kerberos	tcp	default (1-65535)	750			
	🚥 klogin	tcp	default (1-65535)	543			
		hen	default (1-65535)	544			~

 En la ventana Asistente para agregar reglas de política de servicio - Coincidencia de tráfico -Puerto de destino, puede ver que el servicio elegido es tcp/http. Haga clic en Next (Siguiente).

🖆 Add S	ervice Policy Rule Wizard - Traffic Match - De	stination Port 📃 🔀
Protocol:		
Service:	tcp/http	
	To specify port range for the service, use nnn-nnn format	
		< Back Next > Cancel Help

7. En la ventana Asistente para agregar reglas de política de servicio - Acciones de regla, active la casilla de verificación situada junto a HTTP. A continuación, haga clic en Configurar junto a HTTP.

Protocol Inspection Intrusion Prevention Connection Settings QoS NetFlow CTTQBE CTTQBE DCERPC Configure ESMTP Configure FTP Configure H.323 RAS Configure H.323 RAS Configure ICMP Configure ICMP Configure IS M Configure PP-Options Configure PSec-Pass-Thru Configure MMP Configure Configure MMP Configure Configure MMP Configure Conf		
CTIQEE DCERPC Configure DNS Configure ESMTP Configure FTP Configure H.323 RAS Configure H.323 RAS Configure VITTP Configure ICMP Configure ICMP Error IS IS Configure IP-Options Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MSCP Configure NETBIOS Configure PPTP Configure RSH	ings QoS NetFlow	
CTIQBE DCERPC Configure DNS Configure ESMTP Configure FTP Configure H.323 H.225 Configure H.323 RAS Configure VITTE Configure ICMP Configure ICMP Error ILS IM Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MSCP Configure NETBIOS Configure PPTP ENH		
DCERPCConfigureDNSConfigureESMTPConfigureFTPConfigureH.323 H.225ConfigureH.323 RASConfigureV HTTRConfigureICMPConfigureICMPICMPICMPConfigureJP-OptionsConfigureIP-OptionsConfigureIP-Sec-Pass-ThruConfigureMMPConfigureMMPConfigureSHI		î
DNS Configure ESMTP Configure FTP Configure H.323 H.225 Configure H.323 RAS Configure H.323 RAS Configure I.H.323 RAS Configure I.H.323 RAS Configure I.M Configure I.CMP Error II.S I.I.S Configure I.P-Options Configure I.PSec-Pass-Thru Configure I.PSec-Pass-Thru Configure MMP Configure MSCP Configure MSCP Configure NETBIOS Configure PPTP Configure		
ESMTP Configure FTP Configure H.323 H.225 Configure H.323 RA5 Configure H.323 RA5 Configure V HTTR Configure ICMP ICMP ICMP Configure IS Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MSCP Configure NETBIOS Configure PPTP SH		
FTP Configure H.323 H.225 Configure H.323 RA5 Configure H.323 RA5 Configure Configure Configure ICMP ICMP ICMP Configure ILS Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MMP Configure MMP Configure MMP Configure MMP Configure MSCP Configure NETBIOS Configure PPTP Configure RSH		
H.323 H.225 Configure H.323 RAS Configure ITHE Configure ICMP ICMP ICMP Error I ILS Interform IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP Configure RSH		
H.323 RA5 Configure ICMP Configure ICMP Error ILS ILS Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure MGCP Configure NETBIOS Configure PPTP RSH		
HITTE Configure ICMP ICMP Error ILS IM Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MMP Configure MSCP Configure NETBIOS Configure PPTP RSH		
ICMP ICMP Error ILS IM Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP Endigure		
ICMP Error ILS IM Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP Configure RSH		
ILS IM Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP Ensity		
IM Configure IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP Configure RSH		
IP-Options Configure IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP E RSH E		
IPSec-Pass-Thru Configure MMP Configure MGCP Configure NETBIOS Configure PPTP RSH		
MMP Configure MGCP Configure NETBIOS Configure PPTP Ensh		
MGCP Configure NETBLOS Configure PPTP RSH		
NETBIOS Configure PPTP RSH		
PPTP RSH		
RSH		

8. En la ventana Select HTTP Inspect Map, verifique el botón de opción situado junto a **Use the Default HTTP Inspection Map**. En este ejemplo se utiliza la inspección HTTP predeterminada. A continuación, haga clic en

	🕵 S	elect HTTP Inspect Map 🔛
	0	Use the default HTTP inspection map
	0	Select an HTTP inspect map for fine control over inspection
		Name Add
		OK Cancel Help
Aceptar.		

9. Haga clic en Finish (Finalizar).

rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIQBE				-
DCERPC	Configure			
DNS	Configure			
ESMTP	Configure			
FTP	Configure			
🔄 H.323 H.225	Configure			
H.323 RA5	Configure			
HTTP:	Configure			
ICMP				
ICMP Error				
ILS I				
IM 🔄	Configure			
IP-Options	Configure			
IPSec-Pass-Th	ru Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				

 En Configuration > Firewall > Service Policy Rules, verá la política de servicio recientemente configurada outside-cisco-policy (para inspeccionar HTTP) junto con la política de servicio predeterminada que ya está presente en el dispositivo. Haga clic en Aplicar para aplicar la configuración a Cisco ASA.

Configuration > Firewall > Service Policy Rules								
💠 Add 🕞 🗃 Edit 🏦 Delete 🎓 🍝 🐰 🐜 🏨 - 🔍 Find 🖽 Diagram 🕮 Packet Trace								
Treffic Classification								
Name	\$	Enabled	Match	Source	Destination	Service	Time	Rule Actions
E Interface: outside; Policy: outside-	cisco-po	dicy						
outside-class			🕒 Match	🎱 any	iany any	🚥 http		Q, Inspect HTTP
Global; Policy: global_policy								
¹ Inspection_default			L Match	🎱 any	🎱 any	Q, default-inspec		Q, Enspect DNS Map preset_dns_map Q, Enspect ESMTP (L3 more inspect actions)
<								
					Apply Rese	t		

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Solicitudes de Comentarios (RFC)
- Aplicación de la Inspección del Protocolo de Capa de Aplicación
- Soporte Técnico y Documentación Cisco Systems