ASA/PIX 7.X: Disabilita ispezione globale predefinita e Abilita ispezione applicazione non predefinita utilizzando ASDM

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Criterio globale predefinito Abilita ispezione applicazione non predefinita Verifica Informazioni correlate

Introduzione

In questo documento viene descritto come rimuovere il controllo predefinito dai criteri globali per un'applicazione e come abilitare il controllo per un'applicazione non predefinita.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata un'appliance Cisco Adaptive Security Appliance (ASA) con immagine software 7.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con l'appliance di sicurezza PIX con

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Criterio globale predefinito

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica determinate ispezioni al traffico su tutte le interfacce (un criterio globale). Non tutte le ispezioni sono abilitate per impostazione predefinita. È possibile applicare un solo criterio globale. Se si desidera modificare il criterio globale, è necessario modificare il criterio predefinito oppure disattivarlo e applicarne uno nuovo. Un criterio di interfaccia ha la precedenza sul criterio globale.

La configurazione predefinita dei criteri include i comandi seguenti:



Abilita ispezione applicazione non predefinita

Completare questa procedura per abilitare il controllo delle applicazioni non predefinite sull'appliance Cisco ASA:

1. Accedere ad ASDM. Selezionare Configurazione > Firewall > Regole dei criteri di servizio.

I	Configuration > Firew	all > 9	Service Pol	cy Rules					
	🕈 Add 🔹 🗹 Edit 👔								
	Traffic Classification	Dula Antinan							
	Name # Enabled Match		Source Destination Service		Service	Time	RUB ALUUTS		
	Global; Policy: global_policy								
	inspection_default			La Match	🖘 any	🍫 any	🔍 default-inspe		 Inspect DNS Map prese Inspect ESMTP (12 more inspect actions)

2. Se si desidera mantenere la configurazione per i criteri globali che include la mappa delle classi predefinita e la mappa dei criteri predefinita, ma si desidera rimuovere i criteri a livello globale, passare a Strumenti > Interfaccia da riga di comando e utilizzare il comando globale no service-policy per rimuovere i criteri a livello globale. Quindi, fare clic su Send per applicare il comando all'appliance ASA.

🖆 Command Line Interface	
Type a command to be sent directly to the device. For command help, type a command followed by a mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as para 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.	question ameter to g
Single Line	
no service-policy global_policy global	*
Response:	
Result of the command: "no service-policy global_policy global" The command has been sent to the device	
Clear Send Close Help	Response

Nota: con questo passaggio, la policy globale diventa invisibile in Adaptive Security Device Manager (ASDM), ma viene visualizzata nella CLI.

3. Per aggiungere un nuovo criterio, fare clic su **Add** (Aggiungi) come mostrato di seguito:

Configuration > Fi	irewall > Service Poli	icy Rules				
💠 Add 👻 🛒 Ea	iit 🃋 Delete 🛧 🦨	X 🖻 🛍 - Q I	Find 🖭 Diagram 🐙 Packet	Trace		
Traffic Classification						Dula Antiana
Name	# Enabled	Match Source	Destination	Service	Time	Rule Actions

4. Verificare che il pulsante di opzione accanto a **Interfaccia** sia selezionato e scegliere l'interfaccia a cui applicare il criterio dal menu a discesa. Fornire quindi il **Nome criterio** e la

Descrizione. Fare clic su Next

Add Service Policy Rule Wizard - Service Policy Image: Configure a service policy rule requires three steps: Step 1: Configure a service policy. Step 2: Configure the traffic classification onteria for the service policy rule. Step 3: Configure actions on the traffic classified by the service policy rule. Image: Configure actions on the traffic classified by the service policy rule. Create a Service Policy and Apply To: Image: Configure actions on the traffic classified by the service policy rule. Create a Service Policy and Apply To: Image: Configure actions on the traffic classified by the service policy rule. Create a Service Policy and Apply To: Image: Configure actions on the traffic classified by the service policy rule. Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy. Image: Image: Contract Con
Adding a new service policy rule requires three steps: Rep 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: Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy. Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy. Only one service policy on outside interface Description: Policy on outside interface Policy Name: outside-policy Description: Policy on outside interface Policy Name: olicbal-policy Description: olicbal-policy Description:
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: Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy. Immediate of the existing service policy. Otherwise, you can create a new service policy. Immediate of the existing 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: Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy. Image: Outside - (create new service policy) Image: Outside - (create new service policy) Image: Outside - (create new service policy) Image: Outside - outs
Step 3: Configure actions on the traffic classified by the service policy rule. 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 new rule 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 Policy Name: global-policy Description:
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 new rule 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 Policy Name: global-policy Description:
Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy. O Interface: O I
Interface: outside - (create new service policy) ♥ Policy Name: outside-policy Description: Policy on outside interface Policy Name: globel-policy Description:
Policy Name: outside-policy Description: Policy on outside interface Policy Name: global-policy Description:
Description: Policy on outside interface O Global - apples to all interfaces Policy Name: global-policy Description:
Global - applies to all interfaces Policy Name: global-policy Description:
Policy Name: global-policy Description:
Description:
< Back Next > Cancel Help

5. Creare una nuova mappa di classe per far corrispondere il traffico **TCP** mentre il traffico **HTTP** rientra in TCP. Fare clic su **Next** (Avanti).

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	×
Oreate a new traffic dass:	outside-class	
Description (optional):		
Traffic Match Criteria		
Default Inspection Trai	ffic	
Source and Destination	n IP Address (uses ACL)	
Tunnel Group		
CP or UDP Destination	n Port	
RTP Range		
IP DiffServ CodePoints	; (DSCP)	
IP Precedence		
Any traffic	4	
O Use an existing traffic class:	inspection_default	
O Use class-default as the traff	fic dass.	
If traffic does not match a ex situation.	xisting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all	I
	< Back Next > Cancel Hel	Þ

6. Selezionare **TCP** come protocollo.

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

Scegliere **Porta HTTP 80** come servizio e fare clic su **OK**.

C	Browse Service						
	🗣 Add 👻 🖼 Edit	î Delete	0				
	Elber:		~				Filter Clear
	News	Destand	Service Deute	Deskieskies Deska	LCMD Turns	Description	
	Name Dradafinad	Protocol	Source Ports	Destination Ports	тсмы туре	Description	
	- Predenned	tro	default (1-65535)	5190			-
	ban	trn	default (1-65535)	179			
	- to chargen	tcp	default (1-65535)	19			
	cifs	tcp	default (1-65535)	3020			
	citrix-ica	tcp	default (1-65535)	1494			=
	- re> ctiqbe	tcp	default (1-65535)	2748			
	- 10 daytime	tcp	default (1-65535)	13			
	to discard	tcp	default (1-65535)	9			
	- 100 domain	tcp	default (1-65535)	53			
	👓 🚥 echo	tcp	default (1-65535)	7			
	exec	tcp	default (1-65535)	512			
		tcp	default (1-65535)	79			
	👓 🏧 ftp	tcp	default (1-65535)	21			
	👓 🏧 ftp-data	tcp	default (1-65535)	20			
	- 100 gopher	tcp	default (1-65535)	70			
	100 h323	tcp	default (1-65535)	1720			
	- 100 hostname	tcp	default (1-65535)	101			
	- 😰 http	tcp	default (1-65535)	80			
	nttps	tcp	default (1-65535)	443			
		tcp	default (1-65535)	113			~
	Selected Service						
	Service -> to	:p/http					
						ОК	Cancel

7. Scegliere HTTP e fare clic su Fine.

Add Service Policy R	ule Wizard - Rule A	ctions	
rotocol Inspection Intrus	ion Prevention Connect	tion Settings QoS	
			^
	Configure		
DNS	Configure		
ESMTP	Configure		
FTP	Configure		
H.323 H.225	Configure		
H.323 RA5	Configure		
	Configure	N	
ICMP		43	
ICMP Error			
ILS I			
IM 🔄	Configure		
IPSec-Pass-Thru	Configure		
MGCP	Configure		-
NETBIOS	Configure		
PPTP			
RSH			
RTSP	Configure		
SCCP (Skinny)	Configure		~
		Sack Finish Cancel	Hel

8. Fare clic su **Apply** (Applica) per inviare le modifiche alla configurazione all'appliance ASA da ASDM. La configurazione è stata

completata. Configuration > Firewall > Service Policy Rules 💠 Add 👻 🚰 Edit 📋 Delete | 🛧 🎸 👗 🗞 🐘 🐘 🗸 🗛 Find 🖼 Diagram 💐 Packet Trace Traffic Classification Rule Actions # Enabled Match Source Name Destination Service Time □ Interface: outside; Policy: outside-policy 🕒 Match 🥠 any outside-class 😰 http 🔍 Inspect HTTP 🄄 any 4 X Apply Reset

Verifica

Utilizzare i seguenti comandi show per verificare la configurazione:

• Utilizzare il comando show run class-map per visualizzare le mappe classi configurate.

```
ciscoasa# sh run class-map
 1
 class-map inspection_default
 match default-inspection-traffic
 class-map outside-class
 match port tcp eq www
 Ţ
• Utilizzare il comando show run policy-map per visualizzare i mapping dei criteri configurati.
 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
 1
```

• Utilizzare il comando show run service-policy per visualizzare i criteri dei servizi configurati. ciscoasa# sh run service-policy service-policy outside-policy interface outside

Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- <u>Riferimenti per i comandi di Cisco ASA serie 5500</u>
- Pagina di supporto di Cisco Adaptive Security Device Manager (ASDM)
- <u>Software Cisco PIX Firewall</u>
- <u>RFC (Requests for Comments)</u>
- <u>Cisco PIX serie 500 Security Appliance</u>
- Applicazione dell'ispezione del protocollo a livello di applicazione
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Documentazione e supporto tecnico Cisco Systems