ASA 8.3及更高版本 — 使用ASDM配置檢測

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>預設全域性策略</u> <u>禁用應用程式的預設全域性檢查</u> <u>為非預設應用程式啟用檢測</u> <u>相關資訊</u>

<u>簡介</u>

本文檔為版本8.3(1)及更高版本的思科自適應安全裝置(ASA)提供配置示例,說明如何從應用程式的 全域性策略中刪除預設檢測,以及如何使用自適應安全裝置管理器(ASDM)為非預設應用程式啟用檢 測。

請參閱<u>PIX/ASA 7.X:在版本8.2及更低版本的</u>Cisco<u>ASA上,對相同</u>配置禁用預設全域性檢查並啟用 非預設應用檢查。

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本檔案中的資訊是根據搭載ASDM 6.3的Cisco ASA安全裝置軟體版本8.3(1)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

預設全域性策略

預設情況下,配置包含與所有預設應用檢測流量匹配並將某些檢測應用於所有介面上的流量的策略 (全域性策略)。 並非所有檢查都預設啟用。只能應用一個全域性策略。如果要修改全域性策略 ,必須編輯或禁用預設策略並應用新策略。(介面策略覆蓋全域性策略。)

在ASDM中,選擇**Configuration > Firewall > Service Policy Rules**以檢視具有預設應用程式檢查的 預設全域性策略,如下所示:



預設策略配置包括以下命令:

```
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
如果需要禁用全域性策略,請使用no service-policy global_policy global命令。若要使用ASDM删除
```

全域性策略,請選擇Configuration > Firewall > Service Policy Rules。然後,選擇全域性策略並按 一下Delete。

C	onfiguration > Firewall > Service	Policy	Rules						
	🗣 Add 👻 🗹 Edit 👔 Delete 🗇	4	X 🖻 🛍	< Q, Fir	id 🔤 Diagram 🕰 Pa	scket Trace			
	Traffic Classification								Dula Artices
	Name	#	Enabled	Match	Source	Destination	Service	Time	Rue Actors
	Global; Policy: global_policy								
	inspection_default			Match	≪) any	≪ls any	 default-inspect. 		Inspect DNS Map preset_dns_map Inspect ESMTP (13 more inspect actions)

注意:使用ASDM刪除服務策略時,將刪除關聯的策略和類對映。但是,如果使用CLI刪除服務策略 ,則只會從介面中刪除服務策略。類對映和策略對映保持不變。

<u>禁用應用程式的預設全域性檢查</u>

要禁用應用程式的全域性檢查,請使用inspect命令的no版本。

例如,要刪除對安全裝置偵聽的FTP應用程式的全域性檢查,請在類配置模式下使用no inspect ftp命令。

可從策略對映配置模式訪問類配置模式。若要移除組態,請使用命令的no形式。

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

要使用ASDM禁用FTP全域性檢查,請完成以下步驟:

注意:請參閱<u>允許ASDM的HTTPS訪問</u>以瞭解基本設定,以便通過ASDM訪問PIX/ASA。

選擇Configuration > Firewall > Service Policy Rules,然後選擇預設全域性策略。然後,按一下Edit編輯全域性檢測策略。

Configuration > Firewall > Ser	vice Policy	/ Rules						
🗣 Add 🕞 🗃 Edit 📋 Delete	÷ 4	🌡 👫 🏛 🕤	Q, Find 📴	🛿 Diagram 🥂 Pad	ket Trace			
Traffic Classification								Dulo Astions
Name	#	Enabled Ma	itch Sou	irce	Destination	Service	Time	Rule wetters
😑 Global; Policy: global_policy								
inspection_default		12	Match 🥌	any	≪) any	🔍 default-inspec		Inspect DNS Map preset_dhs_map Inspect ESMTP (12 preset ESMTP)

2. 在Edit Service Policy Rule視窗中,選擇**Rule Actions**頁籤下的**Protocol Inspection**。確保未選中**FTP**覈取方塊。這將禁用FTP檢測,如下圖所示。然後,按一下「**OK**」,然後「**Apply**」。

rotacal Inspection Intrus	ion Prevention Connection Settings QoS NetFlow	
Select all increation rul	er	
	Configure	
	Configure	
ESMTP	Configure	
FTP	Configure	
H.323 H.225	Configure	
H.323 RAS	Configure	
HTTP	Configure	
ICMP		
ICMP Error		
ILS ILS		
IM 🔄	Configure	
✓ IP-Options	Configure	
🔲 IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
VETBIOS	Configure	
PPTP		

注意:有關FTP檢測的更多資訊,請參閱<u>PIX/ASA 7.x:啟用FTP/TFTP服務配置示例</u>。

<u>為非預設應用程式啟用檢測</u>

預設情況下,增強型HTTP檢測處於禁用狀態。要在global_policy中啟用HTTP檢查,請使用class inspection_default下的**inspect http**命令。

在本示例中,通過任何介面進入安全裝置的任何HTTP連線(埠80上的TCP流量)都屬於HTTP檢查 類別。由於策略是全域性策略,因此只有在流量進入每個介面時才進行檢查。

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

在本例中,通過外部介面進入或退出安全裝置的任何HTTP連線(埠80上的TCP流*量)都分類為* HTTP檢測。

```
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
要使用ASDM配置上述示例,請執行以下步驟:
```

1. 選擇Configuration > Firewall > Service Policy Rules, 然後按一下Add以新增新服務策略

infiguration > Firewall > Se	raire Polic	r Roles								
Promi + Larona III overse 7 + 8 + 1 III + 1 + 4 min 20104/pen 2017erse Trees										
Name Construction	٥	Enabled	Natsh	Source	Destination	Service	Time	Rule Actions		
Global; Policy: global_policy										
inspection_default			Ling Haat d a	ि बार	10 ary	🔍 defaalt inspect.		 Inspect DVS Hap preset_dris_map Inspect ESHTP (10 more inspect actions) 		

 在Add Service Policy Rule Wizard - Service Policy視窗中,選擇Interface旁邊的單選按鈕。這 會將建立的策略應用於特定介面,在本例中為Outside介面。提供一個策略名稱,在本例中為 outside-cisco-policy。按「Next」(下一步)。

🖆 Add Service P	olicy Rule Wizard - Service Policy	×
Adding a new service Step 1: Configure a Step 2: Configure t Step 3: Configure a Create a Service Po Only one service rule into the exist	e policy rule requires three steps: a service policy. he traffic classification criteria for the service policy rule. actions on the traffic classified by the service policy rule. licy and Apply To: policy can be configured per interface or at global level. If a service policy already exists, then you can add a new ing service policy. Otherwise, you can create a new service policy.	
 Interface: 	outside - (create new service policy) 💙	
Policy Name:	outside-cisco-þolicy	
Description:		
🔘 Global - applie	es to all interfaces	
Policy Name:	global_policy	
Description:		
	< Back Next > Cancel He	lp 🛛

3. 在「新增服務策略規則嚮導 — 流量分類標準」視窗中,提供新的流量類名稱。此示例中使用 的名稱為outside-class。確保選中TCP or UDP Destination Port旁邊的覈取方塊,然後按一下 Next。

Description (optional): Traffic Match Criteria Default Inspection Traffic	
Traffic Match Criteria	-
Default Inspection Traffic	
Source and Destination IP Address (uses ACL)	
Tunnel Group	
TCP or LDP Destination Port	
RTP Range	
ID DiffSeru CodeDointe (DSCD)	
IP Precedence	
Any traffic	
Use an existing traffic class: inspection_default	
Use class-default as the traffic class.	
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch situation.	h all
Carrel	Hel
	HIGI,

	🎼 Add Service Policy Rule Wizard - Traffic Match - Destination Port
	Service:
	To specify port range for the service, use nnn-nnn format.
1	

5. 在「瀏覽服務」視窗中,選擇HTTP作為服務。然後,按一下OK。

Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
- TO> ctiqbe	tcp	default (1-65535)	2748			-
😨 daytime	tcp	default (1-65535)	13			
- 10 discard	tcp	default (1-65535)	9			
- 👓 domain	tcp	default (1-65535)	53			1
😰 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			
- 😰 http	tcp	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	top	default (1-65535)	750			
- 🚥 klogin	tcp	default (1-65535)	543			
- 😰 kshell	tcp	default (1-65535)	544			~

6. 在Add Service Policy Rule Wizard - Traffic Match - Destination Port視窗中,您可以看到所選 的服務是tcp/http。按「Next」(下一步)。

🖆 Add S	Service Policy Rule Wizard - Traffic Match - Destination Port	×
Protocol:		
Service:	tcp/http	
	To specify port range for the service, use nnn-nnn format	
	< Back Next > Cancel Help	7
玍「新圴 ┨TTP旁	曾服務策略規則嚮導 — 規則操作」視窗中,選中HTTP旁邊的覈取方塊。然後,點過 5邊的Configure。	退

rotocol Inspection Intru	ision Prevention	Connection Settings	QoS NetFlow	
CTIQBE				
DCERPC	Configure			
DN5	Configure			
ESMTP	Configure			
FTP	Configure			
🔄 H.323 H.225	Configure			
🔄 H.323 RAS	Configure			
HTTE HTTE	Configure			
ICMP				
ICMP Error				
IL5				
🔄 IM	Configure			
IP-Options	Configure			
🔲 IPSec-Pass-Thru	Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				

8. 在「選擇HTTP檢查對映」視窗中,選中**使用預設HTTP檢查對映**旁邊的單選按鈕。本示例中使 用的是預設HTTP檢測。然後,按一下**OK**。

🖆 Select HTTP Inspect Map	
• Use the default HTTP inspection map	
Select an HTTP inspect map for fine control over	er inspection
Name	Add
OK Cancel Help	

9. 按一下「**Finish**」(結束)。

Add Service Poli	cy Rule Wizard -	Rule Actions		
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIQ8E				^
DCERPC	Configure			
DNS	Configure			
ESMTP	Configure			
FTP	Configure			
🔄 H.323 H.225	Configure			
🔄 H. 323 RAS	Configure			
HTTP:	Configure			
ICMP				
ICMP Error				
ILS I				
IMI 🔄	Configure			
IP-Options	Configure			
IPSec-Pass-Th	ru Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				~
				< Back Finish Cancel He

10. 在**Configuration > Firewall > Service Policy Rules**下,您將看到新配置的Service Policy **outside-cisco-policy**(檢查HTTP)以及裝置上已經存在的預設服務策略。按一下**Apply**以將 配置應用到Cisco ASA。

Configuration > Firewall > Service Policy Rules								
💠 Add 🔸 🗃 Edit 📋 Delete 🎓 🍝 🐰 🎭 🌉 - 🗛 Find 🖼 Diagram 🕮 Packet Trace								
Treffic Classification								Dula Artista
Name	\$	Enabled	Match	Source	Destination	Service	Time	RUPACIONS
Enterface: outside; Policy: outside-	cisco-po	dicy						
outside-class			😂 Match	🎱 any	i any	🚥 http		Q, Inspect HTTP
Global; Policy: global_policy			Description					
· Inspection_default			Lan Match	🍩 any	🎱 any	Q default-inspec		Q_ Inspect DNS Map preset_dns_map Q_ Inspect ESMTP (L3 more inspect actions)
<								
Apply Reset								

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 思科調適型資安裝置管理員
- <u>要求建議 (RFC)</u>
- 應用應用層協定檢查
- 技術支援與文件 Cisco Systems