ASA 8.3及更高版本 — 使用ASDM配置检测

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>规则</u> <u>默认全局策略</u> <u>禁用应用程序的默认全局检查</u> <u>启用非默认应用程序的检查</u> <u>相关信息</u>

<u>简介</u>

本文档为8.3(1)版及更高版本的思科自适应安全设备(ASA)提供配置示例,说明如何从应用的全局策 略中删除默认检测以及如何使用自适应安全设备管理器(ASDM)启用非默认应用的检测。

请参阅<u>PIX/ASA 7.X:对于8.2及更低版本的Cisco ASA上的相</u>同配置,禁用默认全局检测并启用非默 认应用检测。

<u>先决条件</u>

<u>要求</u>

本文档没有任何特定的要求。

<u>使用的组件</u>

本文档中的信息基于带ASDM 6.3的思科ASA安全设备软件版本8.3(1)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

<u>规则</u>

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

<u>默认全局策略</u>

默认情况下,配置包含的策略(全局策略)与所有默认应用程序检查数据流相匹配,并可对所有接

口上的数据流应用特定检查。 默认情况下,并非所有检查都会启用。只能应用一个全局策略。如果 希望修改全局策略,则必须编辑默认策略或禁用该策略并应用新的策略。(接口策略将覆盖全局策 略。)

在ASDM中,选择**Configuration > Firewall > Service Policy Rules**以查看具有默认应用检测的默认 全局策略,如下所示:



默认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
```

如果需要禁用全局策略,请使用no service-policy global_policy全局命令。要使用ASDM删除全局策略,请选择Configuration > Firewall > Service Policy Rules。然后,选择全局策略并单击**删除**。

C	Configuration > Firewall > Service Policy Rules									
	🗣 Add 👻 🗹 Edit 👔 Delete 🗇									
	Traffic Classification								Dide Astron	
	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删除服务策略时,关联的策略和类映射将被删除。但是,如果使用CLI删除服务策 略,则仅从接口删除服务策略。类映射和策略映射保持不变。

<u>禁用应用程序的默认全局检查</u>

要禁用应用程序的全局检查,请使用 inspect 命令的 no 版本。

例如,要删除对安全设备监听的 FTP 应用程序的全局检查,请在类配置模式下使用 no inspect ftp 命令。

可以从策略映射配置模式访问类配置模式。要删除该配置,请使用该命令的 no 形式。

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

要禁用使用ASDM的FTP全局检查,请完成以下步骤:

注意:要通过ASDM访<u>问PIX/ASA,请</u>参阅允许ASDM的HTTPS访问以获取基本设置。

 选择Configuration > Firewall > Service Policy Rules并选择默认全局策略。然后,单击Edit以 编辑全局检查策略。



2. 从Edit Service Policy Rule窗口,在Rule Actions选项卡**下选**择Protocol Inspection。确保未选 中FTP复选框。这会禁用FTP检测,如下一个映像所示。然后,单击OK(确定),然后单击 Apply。

rotacal Inspection Intrus	ion Prevention Connection Settings QoS NetFlow	
Select all inspection rul	es	
CTIQBE		
DCERPC	Configure	
DNS	Configure DNS Inspect Map: preset_dns_map	
SMTP ESMTP	Configure	
ETP:	Configure	
V H.323 H.225	Configure	
V H.323 RAS	Configure	
П НТТР	Configure	
ICMP		
ICMP Error		
ILS ILS		
IM 🔄	Configure	-
✓ IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
NETBIOS	Configure	
PPTP		

注:有关FTP检测的详细信息,请参阅PIX/ASA 7.x:启用 FTP/TFTP 服务配置示例。

<u>启用非默认应用程序的检查</u>

默认情况下,增强型 HTTP 检查处于禁用状态。要在global_policy中启用HTTP检测,请在class inspection_default下使**用inspect http**命令。

在本示例中,通过任何接口进入安全设备的所有 HTTP 连接(端口 80 上的 TCP 数据流)都将归类 为需要进行 HTTP 检查。由于该策略为全局策略,因此,只有当数据流进入每个接口时才会进行检 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

在本示例中,通过外部接口进入或流出安全设备的所有 HTTP 连接(端口 80 上的 TCP 数据流)都 将归类为需要进行 HTTP 检查。

```
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,请执行以下步骤:
```

1. 选择Configuration > Firewall > Service Policy Rules, 然后单击Add以添加新的服务策略

affic Cessification								
en 19		Enabled	alad Natsh	Source	Destination	Service	Time	Rule Actions
Slobal; Policy: global_policy								
inspection_default			Dig Hatch	() ay	10 ay	🔍 defealt-inspec		Inspect OVS Hap preset_drs_map Inspect ESMTP (10 more inspect actions)

2. 从Add Service Policy Rule Wizard - Service Policy窗口,选择Interface旁的单选按钮。这会将 创建的策略应用到特定接口,即本例中的**外部**接口。提供策略名称,在本**例中为外部**ciscopolicy。单击 **Next**。

🖆 Add Service P	Policy 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	te 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. actions on the traffic classified	
 Interface: 	outside - (create new service policy) 🛩	
Policy Name:	outside-cisco-bolicy	
Description:		
🔘 Global - applie	es to all interfaces	
Policy Name:	global_policy	
Description:		
	< Back Next > Cancel He	lp

3. 从Add Service Policy Rule Wizard - Traffic Classification Criteria窗口,提供新的流量类名。 本示例中使用的名称**为outside-class**。确保选中TCP或UDP Destination Port旁**的复选框,然** 后单击"下**一步"**。

Oreate a new traffic class:	outside-class
Description (optional):	
Traffic Match Criteria	
Default Inspection Tra	ffic
Source and Destination	n IP Address (uses ACL)
Tunnel Group	
CP or UDP Destinatio	n Port
RTP Range	
IP DiffServ CodePoints	s (DSCP)
IP Precedence	
Any traffic	
OUse an existing traffic class:	inspection_default
O Use class-default as the traf	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 a
	Canal Ha
	< back wext > Cancel He

选择TCP旁**边的**单选按钮。然后,单击"服务"旁**的按**钮以选择所需的服务。

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

5. 从"浏览服务"窗口中,选**择HTTP**作为服务。然后,单击OK。

Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description		
- tigbe	tcp	default (1-65535)	2748				
🛛 🚾 daytime	tcp	default (1-65535)	13				
- 100 discard	tcp	default (1-65535)	9				
- 😎 domain	tcp	default (1-65535)	53			1	
- 100 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				
- TO> http	tcp	default (1-65535)	80				
🚾 https	tcp	default (1-65535)	443				
- 😎 ident	tcp	default (1-65535)	113				
- 😰 imap4	tcp	default (1-65535)	143				
🚾 irc	tcp	default (1-65535)	194				
120> kerberos	tcp	default (1-65535)	750				
- 😎 klogin	tcp	default (1-65535)	543				
- 😰 kshell	tcp	default (1-65535)	544			~	

6. 从"添加服务策略规则向导 — 流量匹配 — 目标端口"窗口中,可以看到选**择的**服务是**tcp/http**。 单击 Next。

🖆 Add	Service Policy Rule Wizard - Traffic Match - Destination Port	X
Protocol		
Service:	tcp/http 🖃	
	To specify port range for the service, use nnn-nnn format	
	< Back	Next > Cancel Help

7. 在Add Service Policy Rule Wizard - Rule Actions窗口中,选中HTTP旁的复**选框**。然后,单击 HTTP旁边的Configure。

MOD DELVICE PUT	icy note wizaru -	MORE 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 RA5	Configure			
HTTP:	Configure			
ICMP				
ICMP Error				
ILS 🔁				
IM 🔄	Configure			
IP-Options	Configure			
IPSec-Pass-Th	ru Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				

8. 在Select HTTP Inspect Map窗口中,选中Use the Default HTTP inspection map旁**的单选按钮** 。本示例中使用默认HTTP检测。然后,单击**OK**。

🛋 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									

9. 单击 **完成**。

Add Service Poli	cy Rule Wizaru -	KUR ACTIONS			
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow		
CTIQ8E					^
DCERPC	Configure				
DN5	Configure				
ESMTP	Configure				
FTP	Configure				
🔄 H.323 H.225	Configure				
🔄 H. 323 RAS	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					~
				Contract Contract	

10. 在**Configuration > Firewall > Service Policy Rules**下,您将看到新配置的Service Policy outside-cisco-policy **(用于检查HTTP)以及设备上已存在的默认服务策略。**单击**Apply**以将 配置应用到Cisco ASA。

onfiguration > Firewall > Service Policy Rules									
💠 Add 🕞 💽 Edit 🏢 Delete 🛛 🖞	► 4	3 h 6	- Q, FI	nd 🖶 Diagram	Recket Trace				
Traffic Classification								Rule Artions	
Name	\$	Enabled	Match	Source	Destination	Service	Time	hav how o	
Interface: outside; Policy: outside control de class	-cisco-po	dicy	Do nast.	(D)	(a) and	and hits		O forest WTTP	
Ginhal: Policy: clobal policy			LE Macon	👽 any	any any	Mar Hoop		Q Dispect HTIP	
inspection_default			Din Match	🌗 any	i any	Q, default-inspec		Q, Inspect DNS Map preset_dns_map Q, Inspect ESMTP (13 more inspect actions)	
1									
					Apply Res	et			

相关信息

- <u>Cisco ASA 5500 系列自适应安全设备</u>
- Cisco 自适应安全设备管理器
- <u>请求注解 (RFC)</u>
- 应用应用层协议检查
- <u>技术支持和文档 Cisco Systems</u>