ASA 8.3 e posterior - Configurar inspeção usando o ASDM

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Política global padrão Desabilitar inspeção global padrão para um aplicativo Habilitar inspeção para aplicativo não padrão Informações Relacionadas

Introduction

Este documento fornece uma configuração de exemplo para o Cisco Adaptive Security Appliance (ASA) com versões 8.3(1) e posteriores sobre como remover a inspeção padrão da política global de um aplicativo e como habilitar a inspeção para um aplicativo não padrão usando o Adaptive Security Device Manager (ASDM).

Refira ao <u>PIX/ASA 7.x: Desative a inspeção global padrão e ative a inspeção de aplicativos não</u> <u>padrão</u> para a mesma configuração no Cisco ASA com versões 8.2 e anteriores.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software Cisco ASA Security Appliance versão 8.3(1) com 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.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Política global padrão

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica determinadas inspeções ao tráfego em todas as interfaces (uma política global). Nem todas as inspeções estão habilitadas por padrão. Você pode aplicar apenas uma política global. Para alterar a política global, você deve editar a política padrão ou desativá-la e aplicar uma nova. (Uma política de interface substitui a política global.)

No ASDM, escolha **Configuration > Firewall > Service Policy Rules** para exibir a política global padrão que tem a inspeção de aplicativo padrão como mostrado aqui:



A configuração de política padrão inclui estes 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

Se precisar desabilitar a política global, use o comando **global no service-policy global_policy**. Para excluir a política global usando o ASDM, escolha **Configuration > Firewall > Service Policy Rules**. Em seguida, selecione a diretiva global e clique em **Excluir**.

1	Ionfiguration > Firewall > Service	Policy	Rules						
	🗣 Add 🕞 🗹 Edit 📋 Delete 🗇	÷	X 🖻 🛍	< Q, Fir	id 📴 Diagram 🕰 Pa	cket Trace			
	Traffic Classification								Dulo Articos
	Nome	#	Enabled	Match	Source	Destination	Service	Time	KUB ALLOIS
	Global; Policy: global_policy								
	inspection_default			Match	≪) any	🎲 any	 default-inspec 		Inspect DNS Map preset_dns_map Inspect ESMTP (13 more inspect actions)

Observação: quando você exclui a política de serviço com o ASDM, a política associada e os mapas de classe são excluídos. No entanto, se a política de serviço for excluída usando CLI, somente a política de serviço será removida da interface. O mapa de classes e o mapa de políticas permanecem inalterados.

Desabilitar inspeção global padrão para um aplicativo

Para desabilitar a inspeção global de um aplicativo, use a versão no do comando inspect.

Por exemplo, para remover a inspeção global do aplicativo FTP ao qual o Security Appliance escuta, use o comando **no inspect ftp** no modo de configuração de classe.

O modo de configuração de classe é acessível a partir do modo de configuração do mapa de política. Para remover a configuração, use a forma *no* do comando.

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

Para desabilitar a inspeção global para FTP usando o ASDM, faça o seguinte:

Observação: consulte <u>Permitindo Acesso HTTPS para ASDM</u> para obter as configurações básicas para acessar o PIX/ASA por meio do ASDM.

 Escolha Configuration > Firewall > Service Policy Rules e selecione a política global padrão. Em seguida, clique em Editar para editar a política de inspeção

1	global.							
	Configuration > Firewall > Serv	ice Policy Rules						
	🗣 Add 🔹 🗹 Edit 📋 Delete	ታ 🐳 👗 🔖	🛍 - 🛛 Q Fi	nd 🔛 Diagram	advet Trace			
	Traffic Classification							Dida Artima
	Name	# Enabled	Match	Source	Destination	Service	Time	NUE ACCOLS
	😑 Global; Policy: global_policy							
	inspection_default		Match	≪ ary	v∯) any	 default-inspec 		Inspect DNS Map preset_dns_map Inspect ESMTP

 Na janela Editar regra de política de serviço, escolha Inspeção de protocolo na guia Ações da regra. Verifique se a caixa de seleção FTP está desmarcada. Isso desabilita a inspeção de FTP como mostrado na próxima imagem. Em seguida, clique em OK e em Aplicar.

rotacal Inspection Intrusi	on Prevention Connection Settings QoS NetFlow	
Select all inspection rule	aç	
DCERPC	Configure	
	Configure DNS Inspect Map: preset_dns_map	
SMTP	Configure	
ETR	Configure	
V H.323 H.225	Configure	
V H.323 RAS	Configure	
П НТТР	Configure	
ICMP		
ICMP Error		
ILS I		
MI 🔄	Configure	
✓ IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
VETBIOS	Configure	
PPTP		

Observação: para obter mais informações sobre a inspeção de FTP, consulte <u>PIX/ASA 7.x:</u> <u>Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP.</u>

Habilitar inspeção para aplicativo não padrão

A inspeção de HTTP aprimorada está desabilitada por padrão. Para habilitar a inspeção HTTP em global_policy, use o comando **inspect http** em class inspection_default.

Neste exemplo, qualquer conexão HTTP (tráfego TCP na porta 80) que entra no Security Appliance por meio de qualquer interface é classificada para inspeção HTTP. *Como a política é uma política global, a inspeção ocorre somente quando o tráfego entra em cada interface.*

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

Neste exemplo, qualquer conexão HTTP (tráfego TCP na porta 80) que entra ou sai do Security Appliance através da *interface externa é classificada para inspeção HTTP*.

```
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
```

Execute estas etapas para configurar o exemplo acima usando ASDM:

1. Escolha **Configuration > Firewall > Service Policy Rules** e clique em **Add** para adicionar uma nova política de

serviço:								
Configuration > Firewall > Serv	ire Policy	r Rules						
🗣 Add 🔹 💽 Edit 🏢 Delete	÷ +	3. 🖎 📾	- Q, n	nd 🔁 Diagram 🕰	Packet Trace			
Traffic Cassification								Dale Arthurs
Name	ø	Enabled	Match	Source	Destination	Service	Time	
Blobal; Policy: global_policy			Dis	1.0				
inspecton_denauc			na wata	o ay	047	a, de colorigios		Inspect DPS Map proset_driv_map Inspect ESMTP (10 more inspect actions)

2. Na janela Add Service Policy Rule Wizard - Service Policy, selecione o botão de opção ao lado de Interface. Isso aplica a política criada para uma interface específica, que é a interface externa neste exemplo. Forneça um nome de política, que é outside-cisco-policy neste exemplo. Clique em Next.

🖆 Add Service F	Policy Rule Wizard - Service Policy	×
Adding a new servic Step 1: Configure a Step 2: Configure a Step 3: Configure a Create a Service Po	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 exist	policy can be configured per incerrace or ac global level. If a service policy already exists, then you can add a new ting service policy. Otherwise, you can create a new service policy. outside - (create new service policy)	
Policy Name:	outside-cisco-þolicy	
Description:		
🔘 Global - appli	es to all interfaces	
Policy Name;	global_policy	
Description:		
		tala I
	< Back Next > Cancel F	leip

3. Na janela Add Service Policy Rule Wizard - Traffic Classification Criteria, forneça o novo nome da classe de tráfego. O nome usado neste exemplo é fora da classe. Verifique se a caixa de seleção ao lado de TCP ou UDP Destination Port (Porta de destino TCP ou UDP) está marcada e clique em Next (Avançar).

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	×
• Create a new traffic class:	outside-class	
Description (optional):		
Traffic Match Criteria		
Default Inspection Tra	ffic	
Source and Destination	1 IP Address (uses ACL)	
Tunnel Group		
CP or UDP Destination	a 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 traf	fic dass.	
If traffic does not match a ex situation.	dsting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all	
	< Back Next > Cancel Held	ิก

4. Na janela Add Service Policy Rule Wizard - Traffic Match - Destination Port (Assistente para adicionar regra de política de serviço - correspondência de tráfego - Porta de destino), escolha o botão de opção ao lado de TCP na seção Protocol (Protocolo). Em seguida, clique no botão ao lado de Serviço para escolher o serviço necessário.

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

5. Na janela Procurar serviço, escolha **HTTP** como o serviço. Em seguida, clique em **OK**.

Nam	ne	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
ļ	🚾 ctiqbe	tcp	default (1-65535)	2748			~
	daytime	tcp	default (1-65535)	13			
	😨 discard	tcp	default (1-65535)	9			
	- 😰 domain	tcp	default (1-65535)	53			. In 199
	😰 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	top	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			
	🚾 irc	tcp	default (1-65535)	194			
	12 kerberos	tcp	default (1-65535)	750			
	- 😰 klogin	tcp	default (1-65535)	543			
	😰 kshell	tcp	default (1-65535)	544			~

6. Na janela Add Service Policy Rule Wizard - Traffic Match - Destination Port (Assistente para adicionar regra de política de serviço - correspondência de tráfego - Porta de destino), você pode ver que o Serviço escolhido é tcp/http. Clique em Next.

🖆 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. Na janela Add Service Policy Rule Wizard - Rule Actions (Assistente para adicionar regra de política de serviço - Ações da regra), marque a caixa de seleção ao lado de HTTP. Em seguida, clique em Configurar ao lado de HTTP.

AUD SETVICE PUT	cy Kule Wizaru -	Rule Actions		
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIQBE				1
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			L
IPSec-Pass-Th	ru Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				~

8. Na janela Selecionar mapa de inspeção HTTP, marque o botão de opção ao lado de **Usar o** mapa de inspeção HTTP padrão. A inspeção HTTP padrão é usada neste exemplo. Em

	鱰 Select HTTP Inspect Map 🔄	
	 Use the default HTTP inspection map; Select an HTTP inspect map for fine control over 	inspection
	Name	Add
seguida, clique em OK .	OK Cancel Help	

9. Clique em Finish.

rotocol Inspection	trusion 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-Thro	Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				

 Em Configuration > Firewall > Service Policy Rules, você verá a Política de serviço recémconfigurada fora da cisco-policy (para inspecionar HTTP) junto com a política de serviço padrão já presente no dispositivo. Clique em Apply para aplicar a configuração ao Cisco ASA.

Configuration > Firewall > Service Policy Rules								
🗣 Add 🕞 🗃 Edit 🏦 Delete 🎓 🍝 🐰 🐜 🏨 - 🔍 Find 🖽 Diagram 👼 Packet Trace								
Treffic Classification								Data Antina
Name	\$	Enabled	Match	Source	Destination	Service	Time	Rule Actors
Interface: outside; Policy: outside	-cisco-p	alicy						
outside-class			👌 Match	🎱 any	🎱 any	😎 http		Q, Inspect HTTP
Global; Policy: global_policy								
* Inspection_default			L Match	🍩 any	iny 🧼 any	Q, default-inspec		Q, Inspect DNS Map preset_dns_map Q, Inspect ESMTP (LS more inspect actions)
<								
					Apply Res	et		

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- <u>Cisco Adaptive Security Device Manager</u>
- Solicitações de Comentários (RFCs)
- Aplicação da Inspeção do Protocolo da Camada de Aplicação
- <u>Suporte Técnico e Documentação Cisco Systems</u>