# ASA 8.3 et versions ultérieures - Configuration de l'inspection à l'aide d'ASDM

### Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Stratégie globale par défaut Désactiver l'inspection globale par défaut pour une application Activer l'inspection pour une application non par défaut Informations connexes

### **Introduction**

Ce document fournit un exemple de configuration pour Cisco Adaptive Security Appliance (ASA) avec les versions 8.3(1) et ultérieures sur la façon de supprimer l'inspection par défaut de la stratégie globale pour une application et comment activer l'inspection pour une application autre que par défaut à l'aide d'Adaptive Security Device Manager (ASDM).

<u>Référez-vous à PIX/ASA 7.x : Désactivez l'inspection globale par défaut et activez l'inspection des</u> <u>applications non par défaut</u> pour la même configuration sur Cisco ASA avec les versions 8.2 et antérieures.

## **Conditions préalables**

### **Conditions requises**

Aucune spécification déterminée n'est requise pour ce document.

#### **Components Used**

Les informations de ce document sont basées sur le logiciel Cisco ASA Security Appliance version 8.3(1) avec 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**

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

### Stratégie globale par défaut

Par défaut, la configuration inclut une politique qui correspond à tout le trafic d'inspection d'application par défaut et applique certaines inspections au trafic sur toutes les interfaces (une politique globale). Toutes les inspections ne sont pas activées par défaut. Vous ne pouvez appliquer qu'une seule stratégie globale. Si vous souhaitez modifier la stratégie globale, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. (Une stratégie d'interface remplace la stratégie globale.)

Dans ASDM, choisissez **Configuration > Firewall > Service Policy Rules** pour afficher la stratégie globale par défaut qui a l'inspection d'application par défaut, comme indiqué ici :



La configuration de stratégie par défaut comprend les commandes suivantes :

```
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 vous devez désactiver la stratégie globale, utilisez la commande **no service-policy global\_policy global**. Afin de supprimer la stratégie globale à l'aide d'ASDM, choisissez **Configuration > Firewall > Service Policy Rules**. Ensuite, sélectionnez la stratégie globale et cliquez sur **Supprimer**.

C	onfiguration > Firewall > Service	Policy	Rules						
	🗣 Add 🕞 🗹 🗹 Edit 📋 Delete 🗇	÷	X 🖻 🛍	< 🛛 🔍 Fin	id 🖭 Diagram 🕰 Pa	cket Trace			
	Traffic Classification								Dulo Articos
	Name	#	Enabled	Match	Source	Destination	Service	Time	Kale ALCOTS
	Global; Policy: global_policy								
	inspection_default			Match	🤹 any	🧐 any	🔍 default-inspec		Inspect DN5 Map preset_dns_map.
									Inspect ESMTP
									(13 more inspect actions)

**Remarque :** lorsque vous supprimez la stratégie de service avec ASDM, la stratégie associée et les mappages de classes sont supprimés. Cependant, si la stratégie de service est supprimée à l'aide de l'interface de ligne de commande, seule la stratégie de service est supprimée de l'interface. La carte de classe et la carte de stratégie restent inchangées.

#### Désactiver l'inspection globale par défaut pour une application

Afin de désactiver l'inspection globale pour une application, utilisez la commande *no* version de la **commande inspect**.

Par exemple, afin de supprimer l'inspection globale pour l'application FTP à laquelle le dispositif de sécurité écoute, utilisez la commande **no inspect ftp** en mode de configuration de classe.

Le mode de configuration de classe est accessible à partir du mode de configuration de la carte de stratégie. Afin de supprimer la configuration, utilisez la forme *no* de la commande.

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

Afin de désactiver l'inspection globale pour FTP à l'aide d'ASDM, complétez ces étapes :

**Remarque :** Reportez-vous à <u>Autoriser l'accès HTTPS pour ASDM</u> pour les paramètres de base afin d'accéder au PIX/ASA par l'intermédiaire d'ASDM.

 Choisissez Configuration > Firewall > Service Policy Rules et sélectionnez la stratégie globale par défaut. Ensuite, cliquez sur Modifier pour modifier la stratégie d'inspection globale.

ŝ	giobaio.								
	Configuration > Firewall > Service	Policy	/ Rules						
	🗣 Add 🔹 🗹 Edit 📋 Delete 🏼 🗇	4	X 🐴 🛍	<ul> <li>Q, Fir</li> </ul>	nd 📴 Diagram 🕯	💐 Packet Trace			
	Traffic Classification								Dula Asting
I	Name	#	Enabled	Match	Source	Destination	Service	Time	Rue witters
	Global; Policy: global_policy								
	inspection_default			Match	≪ anγ	🖈 any	🔍 default (inspec		Inspect DNS Map preset_dhs_map     Inspect ESMTP     (13 more inspect actions)

 Dans la fenêtre Modifier une règle de stratégie de service, sélectionnez Inspection de protocole sous l'onglet Actions de règle. Assurez-vous que la case FTP est décochée. Ceci désactive l'inspection FTP comme indiqué dans l'image suivante. Cliquez ensuite sur OK,

#### puis sur

Appliquer.

otocol Inspection Intrusi	on Prevention Connection	n Settings QoS NetFlow	
Select all inspection rule	•5		
CTIQBE			
DCERPC	Configure		
🗹 DNS	Configure	DNS Inspect Map: preset_dns_map	
SMTP ESMTP	Configure		
ETP:	Configure		
V H.323 H.225	Configure		
🖌 H.323 RAS	Configure		
🔄 НТТР	Configure		
ICMP			
ICMP Error			
ILS I			
m IM	Configure		
IP-Options	Configure		
🔲 IPSec-Pass-Thru	Configure		
MMP	Configure		
MGCP	Configure		
NETBIOS	Configure		
PPTP			

**Remarque :** Pour plus d'informations sur l'inspection FTP, référez-vous à <u>PIX/ASA 7.x : Exemple</u> <u>de configuration de l'activation des services FTP/TFTP.</u>

#### Activer l'inspection pour une application non par défaut

L'inspection HTTP améliorée est désactivée par défaut. Afin d'activer l'inspection HTTP dans global\_policy, utilisez la commande **inspect http** sous class inspection\_default.

Dans cet exemple, toute connexion HTTP (trafic TCP sur le port 80) qui entre dans l'appliance de sécurité via n'importe quelle interface est classée pour inspection HTTP. *Comme la stratégie est une stratégie globale, l'inspection se produit uniquement lorsque le trafic entre dans chaque 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 ÷

Dans cet exemple, toute connexion HTTP (trafic TCP sur le port 80) qui entre ou sort du dispositif de sécurité via l'*interface externe est classée pour inspection 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 Pour configurer l'exemple ci-dessus à l'aide d'ASDM, procédez comme suit**:

1. Choisissez **Configuration > Firewall > Service Policy Rules** et cliquez sur **Add** afin d'ajouter une nouvelle stratégie de service

Configuration > Firewall > Ser	vice Policy	Rules						
🗣 Add 👻 🗭 Edit 🎁 Delete	<del>†</del>	🗶 📭 💼	- Q, n	d 🔁 Diagram	📿 Packet Trace			
Traffic Cessification								The fact times
Nere	0	Enabled	Natsh	Source	Destination	Service	Time	SU CADUTE
Elobal; Policy: global_policy								
inspection_default			Dig Huldi	णे अपू व	a) ay	🔍 defealt-mapee		Inspect DRS Happroset_dhs_map     Inspect ESHTP     UR note inspect estions)

2. Dans la fenêtre Ajouter une règle de stratégie de service - Stratégie de service, sélectionnez la case d'option en regard de Interface. Ceci applique la stratégie créée à une interface spécifique, qui est l'interface externe dans cet exemple. Indiquez un nom de stratégie, qui est outside-cisco-policy dans cet exemple. Cliquez sur Next (Suivant).

🖆 Add Service F	Policy Rule Wizard - Service Polic	у			
Adding a new service Step 1: Configure ( Step 2: Configure ) Step 3: Configure ( Create a Service Po	ce policy rule requires three steps: a service policy. the traffic classification criteria for the serv actions on the traffic classified by the serv plicy and Apply To:	vice policy ice policy (	rule. rule.		
Only one service rule into the exist	policy can be configured per interface or a ting service policy. Otherwise, you can cre outside - (create new service policy)	st global le ate a new	vel. If a service policy a service policy.	dready exists, then you	u can add a new
Policy Name:	outside-cisco-policy				
Description:					
🚫 Global - appli	es to all interfaces				
Policy Name:	global_policy				
Description:					
				< Back Next >	Cancel Help

 Dans la fenêtre Assistant Ajout de règle de stratégie de service - Critères de classification du trafic, indiquez le nouveau nom de classe de trafic. Le nom utilisé dans cet exemple est outside-class. Assurez-vous que la case à cocher en regard de TCP ou UDP Destination Port est cochée et cliquez sur Next (Suivant).

🖆 Add Service Policy Rule V	Wizard - Traffic Classification Criteria	×
• Create a new traffic class:	utside-class	
Description (optional):		
Traffic Match Criteria		_
Default Inspection Traff	ic	
Source and Destination 3	IP Address (uses ACL)	
Tunnel Group		
CP or UDP Destination	Port	
RTP Range		
IP DiffServ CodePoints (	(DSCP)	
IP Precedence		
Any traffic		
Use an existing traffic class:	inspection_default	
O Use class-default as the traffic	t dass.	
If traffic does not match a exis 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	

 Dans la fenêtre Assistant Ajout de règle de stratégie de service - Correspondance du trafic -Port de destination, sélectionnez la case d'option en regard de TCP sous la section
 Protocole. Ensuite, cliquez sur le bouton en regard de Service afin de choisir le service

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

5. Dans la fenêtre Browse Service, sélectionnez **HTTP** comme service. Cliquez ensuite sur **OK**.

Filter:		Protocol	Source Ports	Destination Ports	ICMP Type	Description	
į	··· TO> ctiqhe	tcp	default (1-65535)	2748	Term type	Description	~
	- 10 daytime	tcp	default (1-65535)	13			
	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			
	- 📧 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			
	😰 kerberos	tcp	default (1-65535)	750			
	- 👳 Klogin	tcp	default (1-65535)	543			
	😰 kshell	tcp	default (1-65535)	544			~

 Dans la fenêtre Assistant Ajout de règle de stratégie de service - Correspondance du trafic -Port de destination, vous pouvez voir que le service choisi est tcp/http. Cliquez sur Next (Suivant).

🖆 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. Dans la fenêtre Add Service Policy Rule Wizard - Rule Actions, cochez la case en regard de **HTTP**. Ensuite, cliquez sur **Configurer** en regard 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 RAS	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. Dans la fenêtre Select HTTP Inspect Map, cochez la case d'option **Use the Default HTTP inspection map**. L'inspection HTTP par défaut est utilisée dans cet exemple. Cliquez ensuite

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

9. Cliquez sur Finish.

Add Service Policy R	ule Wizard - Rule Act	ions		
rotocol Inspection Intrus	ion Prevention Connectio	n Settings QoS	NetFlow	
				 ~
	Configure			
DNS	Configure			
E FSMTP	Configure			
FTP	Configure			
H.323 H.225	Configure			
H.323 RA5	Configure			
	Configure			
ICMP				
ICMP Error				
11.5				
IM I	Configure			
IP-Options	Configure			
IPSec-Pass-Thru	Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				
				 ×

 Sous Configuration > Firewall > Service Policy Rules, vous verrez la nouvelle stratégie de service outside-cisco-policy (pour inspecter HTTP) ainsi que la stratégie de service par défaut déjà présente sur l'appliance. Cliquez sur Apply afin d'appliquer la configuration à 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								
<sup>1</sup> Inspection_default			L Match	🍩 any	iny 😳	Q, default-inspec		Q, Inspect DNS Map preset_dns_map Q, Inspect ESMTP (LS more inspect actions)
<								
					Apply Res	et		

# **Informations connexes**

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- <u>Cisco Adaptive Security Device Manager</u>
- Demandes de commentaires (RFC)
- Application de l'inspection du protocole de couche application
- Support et documentation techniques Cisco Systems