# ASA 8.3 en hoger - Inspectie configureren met ASDM

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Standaard mondiaal beleid Standaard wereldwijde inspectie voor een toepassing uitschakelen Inspectie inschakelen voor niet-standaard toepassing Gerelateerde informatie

# Inleiding

Dit document biedt een voorbeeldconfiguratie voor Cisco adaptieve security applicatie (ASA) met versies 8.3(1) en hoger hoe de standaardinspectie van mondiaal beleid voor een toepassing kan worden verwijderd en hoe de inspectie voor een niet-standaard toepassing kan worden uitgevoerd met behulp van Adaptieve Security Devices Manager (ASDM).

Raadpleeg <u>PIX/ASA 7.X: Standaard wereldwijde inspectie uitschakelen en niet-standaard</u> <u>toepassingsinspectie inschakelen</u> voor dezelfde configuratie op Cisco ASA met versies 8.2 en eerder.

## **Voorwaarden**

### **Vereisten**

Er zijn geen specifieke vereisten van toepassing op dit document.

#### Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA security applicatie versie 8.3(1) met ASDM 6.3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### **Conventies**

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

## Standaard mondiaal beleid

Standaard omvat de configuratie een beleid dat overeenkomt met al het standaard toepassingsinspectieverkeer en past de configuratie bepaalde inspecties op alle interfaces toe (een mondiaal beleid). Niet alle inspecties zijn standaard ingeschakeld. Je kunt maar één mondiaal beleid toepassen. Als u het algemene beleid wilt wijzigen, moet u het standaardbeleid bewerken of uitschakelen en een nieuw beleid toepassen. (Een interfacebeleid heeft voorrang op het mondiaal beleid.)

In ASDM, kies **Configuration > Firewall > Service Policy Regels** om het standaard wereldwijde beleid te bekijken dat de standaard toepassingsinspectie heeft zoals hieronder wordt getoond:



De standaard beleidsconfiguratie bevat deze opdrachten:

```
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
```

Als je het globale beleid moet uitschakelen gebruik de **geen service-beleid global\_policy** opdracht. Als u het wereldwijde beleid wilt verwijderen met ASDM, kiest u **Configuration > Firewall > Service Policy Regels**. Selecteer vervolgens het algemene beleid en klik op **Verwijderen**.

¢	onfiguration > Firewall > Service	Policy	Rules						
	💠 Add 🕞 🗹 Edit 📋 Delete 🗇	÷	X 🖻 🛍	< Q, Fir	id 📴 Diagram 🕰 Pa	cket Trace			
	Traffic Classification								Rula Articos
	Name	#	Enabled	Match	Source	Destination	Service	Time	KUB HLUDIS
	Global; Policy: global_policy								
	inspection_default			Match	≪) any	4 any	<ul> <li>default-inspec</li> </ul>		Inspect DNS Map preset_dns_map     Inspect ESMTP     (13 more inspect actions)

**Opmerking:** wanneer u het servicepakket met ASDM verwijdert, worden de bijbehorende beleidslijnen en klassenkaarten verwijderd. Als echter het servicebeleid met CLI is verwijderd, wordt alleen het servicebeleid uit de interface verwijderd. De klassenkaart en de beleidskaart blijven ongewijzigd.

#### Standaard wereldwijde inspectie voor een toepassing uitschakelen

Om mondiale inspectie voor een toepassing uit te schakelen, gebruikt u de *geen* versie van de **inspectie-**opdracht.

Om bijvoorbeeld de algemene inspectie voor de FTP-toepassing te verwijderen waarnaar het security apparaat luistert, gebruikt u de opdracht **no-inspect ftp** in klasse-configuratiemodus.

De configuratiemodus van de klasse is toegankelijk vanuit de configuratie van de beleidskaart. Gebruik de opdracht om de configuratie te verwijderen.

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

Voltooi de volgende stappen om wereldwijde inspectie voor FTP uit te schakelen met ASDM:

**Opmerking:** Raadpleeg <u>HTTPS-toegang voor ASDM</u> voor basisinstellingen om toegang te krijgen tot de PIX/ASA via ASDM.

1. Kies **Configuration > Firewall > Service Policy Regels** en selecteer de optie mondiaal standaardbeleid. Klik vervolgens op **Bewerken** om het algemene inspectiebeleid te bewerken

pewerken.								
Configuration > Firewall > Servi	ce Polic	y Rules						
🗣 Add 🔹 🗹 Edit 👔 Delete	¢ 4	አ 🖻 🛍	<ul> <li>Q Fir</li> </ul>	nd 🔛 Diagram	🟹 Packet Trace			
Traffic Classification								Dula Artices
Name	#	Enabled	Match	Source	Destination	Service	Time	NUE ACCOLS
Global; Policy: global_policy								
inspection_default			Match	🔹 any	🧐 any	🔍 default-inspec		Inspect DNS Map preset_dns_map
								Inspect ESMTP
								(13 more inspect actions)

2. Selecteer in het venster Service Policy Rule de optie **Protocol Inspectie** onder het tabblad **Regel**. Controleer of het vakje **FTP** is ingeschakeld. Hiermee wordt de FTP-inspectie

uitgeschakeld zoals in de volgende afbeelding wordt weergegeven. Klik vervolgens op **OK** en **Toepassen**.

otocol Inspection Intrus	n Prevention Connection Settings QoS NetFlow	w
Select all inspection rul	\$	
	-	
DCERPC	Configure	
DNS	Configure DNS Inspect Map: preset_	dns_map
ESMTP	Configure	
ETE	Configure	
V H.323 H.225	Configure	
🗹 H.323 RAS	Configure	
НТТР	Configure	
ICMP		
ICMP Error		
ILS		
IM 📃	Configure	-
✓ IP-Options	Configure	
🔲 IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
NETBIOS	Configure	
PPTP		

**Opmerking:** Raadpleeg voor meer informatie over FTP-inspectie <u>PIX/ASA 7.x:</u> <u>Configuratievoorbeeld FTP/TFTP-services inschakelen</u>.

#### Inspectie inschakelen voor niet-standaard toepassing

Uitgebreide HTTP-inspectie is standaard uitgeschakeld. Om HTTP inspectie in global\_policy mogelijk te maken, gebruik de opdracht **http** onder class inspection\_default.

In dit voorbeeld wordt elke HTTP-verbinding (TCP-verkeer op poort 80) die het security apparaat via een interface ingaat, geclassificeerd voor HTTP-inspectie. *Omdat het beleid een mondiaal beleid is, komt de inspectie slechts voor als het verkeer elke interface ingaat.* 

```
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
```

In dit voorbeeld *wordt* elke HTTP-verbinding (TCP-verkeer op poort 80) die het security apparaat binnenkomt of verlaat via de *externe interface geclassificeerd voor HTTP-inspectie*.

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 Voer deze stappen uit om het bovenstaande voorbeeld te configureren via ASDM:** 

1. Kies Configuration > Firewall > Service Policy Regels en klik op Add om een nieuw servicebeleid toe te

voegen:								
Configuration > Firewall > Se	rvice Polic	y Roles						
🗣 Add 🔹 💽 Edit 🎁 Delete	++	👗 🗈 📾	- <b>0</b> , n	nd 🖭 Diagram	🔍 Packet Trace			
Traffic Cassification								This Arthur
Name		Enabled	Match	Source	Destination	Service	Time	Page Actions
∃ Gobal; Policy: global_policy								
inspection_default			<b>Den March</b>	th any	(b ay	🔍 defealt-inspec		<ul> <li>Inspect ONS Map preset_drs_nap</li> <li>Inspect ESMTP</li> <li>(10 more inspect actions)</li> </ul>

 Kies in het venster Service Policy Wizard - Service Policy de radioknop naast interface. Dit past het beleid toe dat op een specifieke interface is gecreëerd, de interface buiten in dit voorbeeld. Geef een beleidsnaam op, die buiten-cisco-beleid in dit voorbeeld is. Klik op Volgende.

🖆 Add Service F	Policy Rule Wizard - Service Polic	y		×
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 ser- actions on the traffic classified by the serv vilcy 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	st global le ate a new	ivel. If a service policy already exists, then you can add a new service policy.	
<ul> <li>Interface:</li> </ul>	outside - (create new service policy) 🌱			
Policy Name:	outside-cisco-policy			
Description:				
🔘 Global - appli	es to all interfaces			
Policy Name:	global_policy			
Description:				
				_
			< Back Next > Cancel H	#p

 Van de wizard Servicebeleid toevoegen - Verkeersclassificatiecriteria - geeft u de naam van de nieuwe verkeersklasse op. De naam die in dit voorbeeld wordt gebruikt is van buiten klasse. Zorg ervoor dat het aankruisvakje naast TCP- of UDP-doelpoort is ingeschakeld en klik op Volgende.

🖆 Add Service Policy Rule Wizard - Traffic Classification Criteria 🛛 🛛 🔀
Create a new traffic class: outside-class
Description (optional):
Traffic Match Criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
Tunnel Group
CP or UDP Destination 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 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 all situation.
< Back Next > Cancel Help

4. Kies in het venster Add Service Policy Rule - Traffic Match - Destination Port de radioknop naast **TCP** onder de sectie **Protocol**. Klik vervolgens op de knop naast **Service** om de gewenste service te

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

5. Kies HTTP als service in het venster Bladeren service. Klik vervolgens op OK.

Name		Protocol	Source Ports Destination Ports ICMP Type Description						
	😰 ctiqbe	tcp	default (1-65535)	2748			~		
	10 daytime	tcp	default (1-65535)	13					
	😰 discard	tcp	default (1-65535)	9					
	😰 domain	tcp	default (1-65535)	53			in in		
	😰 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	top	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			~		

 Van de Wizard Toevoegen Service Policy - Traffic Match - Destination Port venster kunt u zien dat de gekozen service tcp/http is. Klik op Volgende.

🖆 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 H	ielp

7. Van de Wizard Toevoegen Service Policy - Regel Handelingen, controleer het aankruisvakje naast HTTP. Klik vervolgens op **Configureren** naast HTTP.

AUD SELVICE PUU	cy Kule Wizaru -	KUR ACTIONS		
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIQBE				
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				
				Sark Finish Cancel He

8. Controleer in het venster Select HTTP Inspect Map de radioknop naast **Gebruik de standaard HTTP-inspectiekaart**. De standaard HTTP inspectie wordt in dit voorbeeld gebruikt. Klik vervolgens op

🖆 Select HTTP Inspect Map	×
<ul> <li>Use the default HTTP inspection map</li> </ul>	
Select an HTTP inspect map for fine control over in	nspection
Name	Add
	_
OK Cancel Help	
	Select HTTP Inspect Map   Use the default HTTP inspection map     Select an HTTP inspect map for fine control over in     Name     OK     Cancel   Help

9. Klik op Voltooien.

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				
				 ×

10. Onder Configuration > Firewall > Service Policy Regels, ziet u het nieuwe geconfigureerde servicebeleid buiten-cisco-beleid (om HTTP te inspecteren). Dit geldt ook voor het standaard servicepakket dat al op het apparaat aanwezig is. Klik op Toepassen om de configuratie op Cisco ASA toe te passen.

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 😳	Q, default-inspec		Q, Inspect DNS Map preset_dns_map Q, Inspect ESMTP (LS more inspect actions)
<								
					Apply Res	et		

### **Gerelateerde informatie**

- Adaptieve security applicaties van Cisco ASA 5500 Series
- <u>Cisco adaptieve security apparaatbeheer</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Toepassend Application Layer Protocol-inspectie</u>
- Technische ondersteuning en documentatie Cisco Systems