ASA/PIX 7.X: Standaard wereldwijde inspectie uitschakelen en geen standaardinspectie voor toepassingen inschakelen met ASDM

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Standaard mondiaal beleid Toepassingsinspectie zonder standaardinstelling inschakelen Verifiëren Gerelateerde informatie

Inleiding

Dit document beschrijft hoe de standaardinspectie voor een toepassing uit het algemene beleid kan worden verwijderd en hoe de inspectie voor een niet-standaardtoepassing mogelijk kan worden gemaakt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco adaptieve security applicatie (ASA) die de 7.x software-afbeelding draait.

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.

Verwante producten

Deze configuratie kan ook worden gebruikt met de PIX security applicatie die het 7.xsoftwarebeeld draait.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> 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.)

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
```

Toepassingsinspectie zonder standaardinstelling inschakelen

Voltooi deze procedure om een niet-standaardinspectie van toepassingen op Cisco ASA mogelijk te maken:

 Aanmelden bij ASDM. Ga naar Configuration > Firewall > Service Policy rules.

onfiguration > Firew	all > 9	iervice Poli	cy Rules					0	
💠 Add 🔽 🖉 Edit: 🍿 Delete 🖙 🌾 🐇 🛍 📖 🐇 🔍 🗛 Find 🕾 Diagram 🗠 Packet Trace									
Traffic Classification								Dulo Actions	
Name # Enabled Match Source Destination Service Time								Rule Actions	
Global; Policy: global	_policy								
inspection_default			Le Match	🆘 any	🎨 any	🔍 default-inspe		 Inspect DNS Map prese Inspect ESMTP (12 more inspect actions) 	
	Add ▼ Z Edit Traffic Classification Name Global; Policy: global inspection_default	Add Add Cassification Firewall > S Cassification Name Global; Policy: global_policy inspection_default	Image: Add Image: Policy Classification Traffic Classification Name # Enabled Image: Global; Policy: global_policy Inspection_default	Image: Add Image: Price Policy Rules Image: Policy Rules <td< th=""><th>Image: Add Image: Price Policy Rules Image: Policy Bulk Image: Policy Bulk</th><th>Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Add → C Edit</th><th>Add → Etit</th></tr<></th></td<>	Image: Add Image: Price Policy Rules Image: Policy Bulk Image: Policy Bulk	Image: Add Image: Price Policy Rules Image: Add Image: Policy Rules Image: Policy Rules <tr< th=""><th>Add → C Edit</th><th>Add → Etit</th></tr<>	Add → C Edit	Add → Etit	

2. Als u de Configuration for Global Policy wilt behouden, die Default Class-map en Default Policy-map bevat, maar het beleid mondiaal wil verwijderen, gaat u naar Gereedschappen > Opdrachtlijn-interface en gebruikt u de mondiale opdracht van mondiaal beleid zonder service-beleid om het beleid wereldwijd te verwijderen. Klik vervolgens op Verzend zodat de opdracht van toepassing is op de ASA.

🖆 Command Line Interface	
Type a command to be sent directly to the o mark. For commands that would prompt for the command and send it to the device. To Configuration to Flash menu option to save	device. For command help, type a command followed by a question confirmation, add an appropriate noconfirm option as parameter to make the changes permanent, use the File > Save Running the configuration to flash.
💿 Single Line i 🔘 Multiple Line	Enable context sensitive help (?)
no service-policy global_policy global	
Response:	
Result of the command: "no se: The command has been sent to t	rvice-policy global_policy global"
Send	Clear Response Close Help

Opmerking: bij deze stap wordt het Global Policy onzichtbaar in de Adaptieve Security ApparaatManager (ASDM), maar wordt weergegeven in de CLI.

3. Klik op **Toevoegen** om een nieuw beleid toe te voegen zoals hieronder wordt weergegeven:

Configuration > Firewall > Service Policy Rules								
🗣 Add 🗸 📷 Edit 🍵 Delete 🛧 🍝 👗 🐜 💼 🤟 🗛 Find 🖼 Diagram 💐 Packet Trace								
Traffic Classification								
Name	# Enabled	Match Source	Destination	Service	Time	Rule Actions		

4. Zorg ervoor dat de radioknop naast **Interface** is ingeschakeld en kies de interface die u het beleid wilt toepassen in het vervolgkeuzemenu. Typ vervolgens de **beleidsnaam** en de

beschrijving. Klik op Volgende

🖆 Add Service Policy Rule Wizard - Service Policy	×									
Adding a new service policy rule requires three steps:										
Step 1: Configure a service policy.										
Step 2: Configure the traffic classification criteria for the service policy rule.										
Step 3: Configure actions on the traffic classified by the service policy rule.										
Create a Service Policy and Apply To:										
Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can a rule into the existing service policy. Otherwise, you can create a new service policy.	add a new									
⊙ Interface: outside - (create new service policy) ▼										
Policy Name: outside-policy										
Description: Policy on outside interface										
Global - applies to all interfaces										
Policy Name: global-policy										
Description										
< Back Next > Car	ncel Help									

- 5. Maak een nieuwe class-map om het **TCP-**verkeer aan te passen als **HTTP** onder TCP valt. Klik op
 - Volgende.

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	X
• Create a new traffic class:	outside-class	
Description (optional):		
Traffic Match Criteria		
Default Inspection Tra	iffic	
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	N	
Any traffic	ki da kara kara kara kara kara kara kara k	
Ouse an existing traffic class:	inspection_default	
O Use class-default as the traf	ífic class.	
If traffic does not match a e situation.	xisting traffic class, then it will match the class-default traffic class. Class-default can be used in catch a	lle
	< Back Next > Cancel He	slp
		_

6. Kies **TCP** als het protocol.

🖆 Add Service Policy Rule Wizard - Traffic Match - Destination Port	
Service:	
< Back	Next > Cancel Help

Kies HTTP poort 80 als de service en klik op OK.

C	Browse Service						×
	🗣 Add 👻 🖼 Edit	î Delete	0				
	Filter		~				Filter Clear
	hame.	Drohosol	Secure Darks	Destination Ports	ICMD Turne	Description	
	Name Dradafinad	Protocol	Source Ports	Deschadon Ports	теме туре	Description	
	in top and	tcp	default (1-65535)	5190			-
	ban	tcp	default (1-65535)	179			
	- to chargen	tcp	default (1-65535)	19			
	cifs	tcp	default (1-65535)	3020			
	citrix-ica	tcp	default (1-65535)	1494			=
		tcp	default (1-65535)	2748			
	😳 daytime	tcp	default (1-65535)	13			
	. too discard	tcp	default (1-65535)	9			
	too domain	tcp	default (1-65535)	53			
	👓 🚥 echo	tcp	default (1-65535)	7			
	exec	tcp	default (1-65535)	512			
	TOP 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			
	100 h323	tcp	default (1-65535)	1720			
	🗠 🚾 hostname	tcp	default (1-65535)	101			
	- 😰 http	tcp	default (1-65535)	60			
	👓 🚾 https	tcp	default (1-65535)	443			
	···· 10 > ident	tcp	default (1-65535)	113			~
-	Selected Service						
	Service -> to	:p/http					
						ОК	Cancel

7. Kies HTTP en klik op Voltooien.

Add Service Pol	icy Rule Wizard - I	Rule Actions
Protocol Inspection	Intrusion Prevention	Connection Settings QoS
CTIONS		
	Configure	
	Configure	·····
	Configure.	
E SMIP	Configure.	
	Configure.	····
H.323 H.225	Conngure.	
H.323 RAS	Configure.	····
HTTB	Configure.	
		, i i i i i i i i i i i i i i i i i i i
ICMP Error		
ILS I		
IM 🔄	Configure.	···
IPSec-Pass-T	hru Configure.	···
MGCP	Configure.	
NETBIOS	Configure.	
PPTP		
RSH		
RTSP	Configure.	
SCCP (Skinny) Configure.	
		Canada Hak

8. Klik op **Toepassen** om deze configuratieveranderingen in de ASA in de ASDM te verzenden. Dit voltooit de

со	nfig	ura	tie.

Cor	figuration > Firev	vall > 5	iervice Poli	cy Rules						
4	🗣 Add 🔻 🇃 Edit 📋 Delete 🛧 🔸 👗 🖳 💼 👻 🔍 G. Find 🔤 Diagram 💐 Packet Trace									
Т	raffic Classification								- Pula Actions	
N	Name # Enabled Match Source Destination Service Time								Rue Accors	
	Interface: outside;	Policy: c	utside-policy	-						
	outside-class			🕒 Match	🍫 any	🥎 any	100 http		Inspect HTTP	
4					10					2
						-				
					Apply	Reset				

Verifiëren

Gebruik deze knoppen om de configuratie te controleren:

• Gebruik de opdracht show run class-map om de geconfigureerde class-maps te bekijken.

```
ciscoasa# sh run class-map
 1
 class-map inspection_default
 match default-inspection-traffic
 class-map outside-class
 match port tcp eq www

    Gebruik de opdracht Show run beleid-map om de geconfigureerde beleidskaarten te bekijken.

 ciscoasa# sh run policy-map
 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
 policy-map outside-policy
  description Policy on outside interface
  class outside-class
   inspect http
 1

    Gebruik de opdracht showrun service-beleid om het geconfigureerde servicebeleid te
```

```
bekijken.
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Gerelateerde informatie

- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- <u>Cisco ASA 5500 Series Opdrachtreferenties</u>
- Ondersteuning van Cisco Adapter Security Apparaat Manager (ASDM) pagina
- <u>Cisco PIX-firewallsoftware</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Cisco PIX 500 Series security applicaties</u>
- Toepassend Application Layer Protocol-inspectie
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Technische ondersteuning en documentatie Cisco Systems