صحفلا نيوكت - ثدحألا تارادصإلاو ASA 8.3 مادختساب ASDM

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> <u>السياسة العمومية الافتراضية</u> <u>تعطيل الفحص العمومي الافتراضي لتطبيق ما</u> <u>تمكين الفحص للتطبيق غير الافتراضي</u> <u>معلومات ذات صلة</u>

<u>المقدمة</u>

يقدم هذا المستند نموذجا لتكوين جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدارات 8.3(1) والإصدارات الأحدث حول كيفية إزالة الفحص الافتراضي من السياسة العامة لتطبيق ما وكيفية تمكين الفحص لتطبيق غير افتراضي باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM).

ارجع إلى PIX/ASA 7.x: تعطيل الفحص العام الافتراضي وتمكين فحص التطبيق غير الافتراضي لنفس التكوين على Cisco ASA مع الإصدارات 8.2 والإصدارات الأقدم.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco ASA Security Appliance Software، الإصدار 8.3(1) مع ASDM 6.3.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

السياسة العمومية الافتراضية

بشكل افتراضي، يتضمن التكوين سياسة تطابق كل حركة مرور فحص التطبيق الافتراضية وتطبق بعض عمليات الفحص على حركة المرور على جميع الواجهات (سياسة عامة). ليست كل عمليات التفتيش ممكنة بشكل افتراضي. يمكنك تطبيق نهج عمومي واحد فقط. إذا كنت ترغب في تغيير النهج العام، يجب عليك إما تحرير النهج الافتراضي أو تعطيله وتطبيق نهج جديد. (يتجاوز نهج الواجهة السياسة العامة.)

في ASDM، أختر **تكوين > جدار حماية > قواعد سياسة الخدمة** لعرض السياسة العامة الافتراضية التي تحتوي على فحص التطبيق الافتراضي كما هو موضح هنا:

1	Home 🦓 Configuration 💽 Monitor in	4	🔚 Suve 🔇 Refresh 🔇 Back	0	terward 💡	2 Help					
	Preval 🚽 Q 🗵	E	ionfiguration > Firewall > Service	Policy	Robes						
ke la	Access Rules		🗣 Add 🔹 🗃 Eds: 📋 Delete 🛧	4	X 2n 🖄	- Q, n	nd 🔁 Dagnarr	🥂 Packet Trace			
8	- Q, Service Policy Rules		Traffic Classification		Easthad	and the second s	Forma	Deskinskins	Caulas I	Terra	Rule Actions
-	Filter Rules		Build Bolicy: global_policy		Enclosed	Matth	Source	DESCHARCH	Service	1010	
	- Liss Public Servers - Mail URL Filtering Servers		inspection_default			Ba Hatch	a a A	al A	 default-inspec 		Inspect DNS Map preset_dns_map Inspect PRITP
	Providence Detection										(L3 more hapect actions)
	- 📸 ketwork Objects/Groups - 🔛 Service Objects/Groups										
	⊟- 📴 Class Haps - 🖓 DN 5										
	HITP										
	RTSP										
	i 🖓 🖓 SIP E 🔀 Enspect Maps										
	DCERPC										
	ESVITP										
	3 Device Setup										
	Che Cerve Secur										
	C.B. main										
	Remote Access VPN										

يتضمن تكوين النهج الافتراضي الأوامر التالية:

```
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
إذا كنت بحاجة إلى تعطيل السياسة العامة، فاستخدم الأمر no service-policy global_policy global. لحذف
```

السياسة العامة باستخدام ASDM أختر **تكوين > جدار حماية > قواعد سياسة الخدمة**. ثم حدد النهج العام وانقر فوق

Configuration > Firewall > Servi	ce Policy	Rules						
🗣 Add 🕞 🎻 Edit 📋 Delete	1 4	X 🖻 🖷	• Q. Fit	nd 🔤 Diagram 🕰 Pa	acket Trace			
Traffic Classification								Rule Artices
Name	#	Enabled	Match	Source	Destination	Service	Time	Kale Actions
Global; Policy: global_policy								
inspection_default			🐚 Match	≪bany	🎨 any	 default-inspec 		Inspect DNS Map preset_dhs_map Inspect ESMTP (13 more inspect actions)

ملاحظة: عند حذف نهج الخدمة مع ASDM، يتم حذف مخططات الفئة والنهج المقترنة. ومع ذلك، في حالة حذف نهج الخدمة باستخدام CLI، تتم إزالة نهج الخدمة فقط من الواجهة. تبقى خريطة الفئة وخريطة السياسة بلا تغيير.

<u>تعطيل الفحص العمومي الافتراضي لتطبيق ما</u>

حذف.

لتعطيل الفحص العام لتطبيق ما، أستخدم الأمر no version من inspection.

على سبيل المثال، لإزالة الفحص العام لتطبيق FTP الذي يستمع إليه جهاز الأمان، أستخدم الأمر no inspection ftp في وضع تكوين الفئة.

يمكن الوصول إلى وضع تكوين الفئة من وضع تكوين خريطة السياسة. لإزالة التكوين، أستخدم نموذج no من الأمر.

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

لتعطيل الفحص العام ل FTP باستخدام ASDM، أكمل الخطوات التالية:

ملاحظة: راجع <u>السماح بوصول HTTPS ل ASDM</u> للإعدادات الأساسية للوصول إلى PIX/ASA من خلال ASDM.

1. أختر **تكوين > جدار الحماية > قواعد سياسة الخدمة** وحدد السياسة العامة الافتراضية. بعد ذلك، انقر فوق **تحرير** لتحرير سياسة التفتيش

									العام.
E	Configuration > Firewall > Service	Policy	Rules						
	🗣 Add 🔹 🗹 Edit 📋 Delete 🗇	$ \psi $	👗 🖻 🛍	V Q, Fit	nd 🔛 Diagra	m 🥂 Packet Trace			
	Traffic Classification								Pule Article
	Name	#	Enabled	Match	Source	Destination	Service	Time	NUIS ACCOLO
	😑 Global; Policy: global_policy								
	inspection_default			Match	≪ ary	🍫 any	default-inspec		Inspect DNS Map preset_dns_map Inspect ESMTP

2. من نافذة "تحرير قاعدة سياسة الخدمة"، أختر **فحص البروتوكول** ضمن علامة التبويب **إجراءات القاعدة**. تأكد من إلغاء تحديد خانة الاختيار FTP. يؤدي هذا إلى تعطيل فحص FTP كما هو موضح في الصورة التالية. ثم انقر فوق **موافق** ثم **تطبيق.**

🖆 Edit Service Policy Rule		
Traffic Classification Default In	repections Bule Actions	
	spectoris	
Protocol Inspection Intrusio	n Prevention Connection Settings QoS NetFlow	
Select all inspection rules	8	
DCERPC	Configure	
	Configure DNS Inspect Map: preset dns map	
ESMTP	Configure	
ETP.	Configure	
H.323 H.225	Configure	
H.323 RAS	Configure	
П НТТР	Configure	
ICMP		
ICMP Error		
E ILS		
IM	Configure	
IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
✓ NETBIOS	Configure	
PPTP		<u> </u>

ملاحظة: للحصول على مزيد من المعلومات حول فحص FTP، ارجع إلى <u>PIX/ASA 7.x: تمكين مثال تكوين خدمات</u>. <u>FTP/TFTP</u>.

<u>تمكين الفحص للتطبيق غير الافتراضي</u>

يتم تعطيل فحص HTTP المحسن بشكل افتراضي. لتمكين فحص HTTP في global_policy، أستخدم الأمر **فحص** http تحت http.

في هذا المثال، يتم تصنيف أي اتصال HTTP (حركة مرور TCP على المنفذ 80) يدخل جهاز الأمان من خلال أي واجهة لفحص HTTP. *لأن السياسة هي سياسة عامة، فإن التفتيش يحدث فقط عند دخول حركة المرور إلى كل واجهة*.

```
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
```

في هذا المثال، *يتم تصنيف* أي اتصال HTTP (حركة مرور TCP على المنفذ 80) يدخل جهاز الأمان أو يخرج منه من خلال *الواجهة الخارجية، لفحص 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** قم بإجراء هذه الخطوات لتكوين المثال أعلاه باستخدام ASDM

1. أخترت **تشكيل>جدار حماية>خدمة سياسة قاعدة** وطقطقة **يضيف** in order to أضفت جديد خدمة سياسة:

Fooliguration > Firewall > Ser	vice Polic	r Roles						
🗣 Add - 🕑 Edit 🏢 Delete	÷ +	3. Ra 🗈	l - Q, n	nd 🖭 Diagram	💐 Packet Trace			
Traffic Cossilication								The last deltament
Name	ø	Enabled	Match	Source	Destination	Service	Time	
Biobal; Policy: global_policy								
inspection_default			Ling March	र्छ बार्	th any	🔍 defealt-inspec		Inspect DVS Hap preset_drs_map Inspect ESHTP (19 more inspect actions)

2. من "معالج إضافة قاعدة سياسة الخدمة" - إطار "نهج الخدمة"، أختر زر الاختيار الموجود بجوار **الواجهة**. يطبق هذا النهج الذي تم إنشاؤه على واجهة معينة، والتي هي الواجهة **الخارجية** في هذا المثال. قم بتوفير اسم سياسة، وهو **خارجي-cisco-policy** في هذا المثال. انقر فوق Next (التالي).

r	Add Service P	Policy Rule Wizard - Service Polic	y		×
Ą	dding a new servio	ce policy rule requires three steps:			
S	ep 1: Configure a	a service policy.			
3	ep 2: Configure t	the traffic classification oriteria for the serv	vice policy	rule.	
50	ep 3: Conrigure a	actions on the tramic classified by the serv	ice policy r	ule.	
0	reate a Service Po	licy and Apply To:			-
	rule into the exist	policy can be configured per interface or a ting service policy. Otherwise, you can cre	ate a new	service policy.	
	 Interface: 	outside - (create new service policy) 👻			
	Policy Name:	outside-cisco-þolicy			
	Description:			-	
	🚫 Global - applie	es to all interfaces			
	Policy Name:	global_policy			
	Description:				
				Carrel Hal	
				< Back Next > Cancel Hel	P

3. من معالج "إضافة قاعدة سياسة الخدمة" - إطار معايير تصنيف حركة المرور، قم بتوفير اسم فئة حركة المرور الجديدة. الاسم المستخدم في هذا المثال هو **خارج الفئة**. ضمنت أن تدقيق صندوق بجوار **TCP أو UDP غاية ميناء** يكون فحصت وطقطقة **بعد** ذ**لك**.

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	×
Oreate a new traffic class:	outside-class	
Description (optional):		
Traffic Match Criteria		-
Default Inspection Trail	ffic	
Source and Destination	IP Address (uses ACL)	
Tunnel Group		
CP or UDP Destination	Port	
RTP Range		
IP DiffServ CodePoints	(DSCP)	
IP Precedence		
Any traffic		
Ouse an existing traffic class:	inspection_default	
OUse class-default as the traff	fic class.	
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 Help	

4. من معالج "إضافة قاعدة سياسة خدمة" - تطابق حركة المرور - نافذة المنفذ الوجهة، أختر زر الاختيار الموجود بجوار TCP ضمن قسم **البروتوكول**. ثم انقر فوق الزر الموجود بجوار **الخدمة** لاختيار الخدمة المطلوبة.

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

5. من نافذة "إستعراض الخدمة"، أختر HTTP كخدمة. ثم انقر فوق OK.

		1		1	1	
Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
- III ctiqbe	tcp	default (1-65535)	2748			^
- 12 daytim	e top	default (1-65535)	13			
- 😰 discard	tcp	default (1-65535)	9			
- 👓 domain	tcp	default (1-65535)	53			
- 😰 echo	tcp	default (1-65535)	7			
- 10 exec	tcp	default (1-65535)	512			
🗠 🔟 finger	tcp	default (1-65535)	79			
💷 ftp	tcp	default (1-65535)	21			
- 😰 ftp-dat	a top	default (1-65535)	20			
- 😰 gopher	tcp	default (1-65535)	70			
12> h323	tcp	default (1-65535)	1720			
- 😰 hostna	me top	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			
- IC inc	tcp	default (1-65535)	194			
- 😰 kerbera	os top	default (1-65535)	750			
- 👓 Klogin	tcp	default (1-65535)	543			
i 💼 takat	tcp	default (1-65535)	544			~
- IO KShell						

6. من معالج "إضافة قاعدة سياسة خدمة" - تطابق حركة المرور - نافذة المنفذ الوجهة، يمكنك أن ترى أن **الخدمة** المختارة هي tcp/http. انقر فوق Next (التالي).

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

7. من معالج "إضافة قاعدة سياسة الخدمة" - إطار "إجراءات القواعد"، حدد خانة الاختيار الموجودة بجوار HTTP. بعد ذلك، انقر فوق **تكوين** بجوار HTTP.

🖆 Add Service Policy Rub	e Wizard - Rule	Actions	
Protocol Inspection Intrusion	Prevention Conn	ection Settings OoS NetElow	
Ind date	Con		
CTIQBE			^
DCERPC	Configure		
DNS	Configure		
ESMTP	Configure		
FTP	Configure		
H.323 H.225	Configure		
H.323 RA5	Configure		
HTTB	Configure		
ICMP		•	
ICMP Error			
ILS			
MI 🔄	Configure		
IP-Options	Configure		
IPSec-Pass-Thru	Configure		
MMP	Configure		
MGCP	Configure		
NETBIOS	Configure		
PPTP			
RSH			~
		< Back Finish Cancel	Help

8. من نافذة خريطة فحص HTTP المحددة، تحقق من زر الخيار المجاور **لاستخدام خريطة فحص HTTP الافتراضية**. يتم إستخدام فحص HTTP الافتراضي في هذا المثال. ثم انقر فوق

Select HTTP Inspect Map	×
 Use the default HTTP inspection map 	
Select an HTTP inspect map for fine control over inspect	tion
Name	Ы
OK Capcel Help	
	_ فوق م

🖆 Add Service Policy Rule Wizard - Rule Actions 🛛 🛛 🔀								
Protocol Inspection Interview	n Prevention Conn	action Settings OoS NetElow						
Inclusion and a second se		locdon Jockings (203 Moti now						
CTIQBE		^						
DCERPC	Configure							
DN5	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-Thru	Configure							
MMP	Configure							
MGCP	Configure							
NETBIOS	Configure							
PPTP								
RSH								
		< Back Finish Cancel Hel	2					

10. تحت **تشكيل > جدار حماية > قواعد سياسة الخدمة**، سترى سياسة الخدمة التي تم تكوينها حديثا **خارج--cisco** in order (لفحص HTTP) مع سياسة الخدمة الافتراضية الموجودة بالفعل على الجهاز. طقطقة **يطبق** in order to طبقت التشكيل إلى ال cisco ASA.

Configuration > Firewall > Service Policy Rules									
💠 Add 🔸 🗃 Eelete 🎓 🌾 🐰 🐜 🏙 - 🗛 Find 🖽 Diagram 📖 Packet Trace									
Traffic Classification	Pule Artists								
Name	# Enabled	d Match Source	Destination	Service T	ime				
Interface: outside; Policy: outside-	cisco-policy								
outside-class		🖹 Match 🧠 any	🎱 any	😎 http	Q Inspect HTTP				
Global; Policy: global_policy									
¹ Inspection_default		lan Match 🥥 any	any	Q, default-inspec	Q_ Inspect DNS Map preset_dns_map Q_ Inspect ESMTP (13 more inspect actions)				
<									
Apply Reset									

<u>معلومات ذات صلة</u>

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
 - مدير أجهزة حلول الأمان المعدلة من <u>Cisco</u>
 - <u>طلبات التعليقات (RFCs)</u>
 - تطبيق فحص بروتوكول طبقة التطبيق
 - الدعم التقني والمَستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما