ASA 8.3 und höher - Konfigurieren der Inspektion mithilfe von ASDM

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Globale Standardrichtlinie Deaktivieren der globalen Standardüberprüfung für eine Anwendung Überprüfung für nicht standardmäßige Anwendung aktivieren Zugehörige Informationen

Einleitung

Dieses Dokument enthält eine Beispielkonfiguration für die Cisco Adaptive Security Appliance (ASA) mit Version 8.3(1) und höher, in der erläutert wird, wie die Standardprüfung für eine Anwendung aus der globalen Richtlinie entfernt wird und wie die Überprüfung für eine nicht standardmäßige Anwendung mithilfe des Adaptive Security Device Manager (ASDM) aktiviert wird.

Weitere Informationen finden Sie unter <u>PIX/ASA 7.X: Deaktivieren Sie die globale</u> <u>Standardinspektion, und aktivieren Sie</u> für dieselbe Konfiguration auf der Cisco ASA mit Version 8.2 oder früher<u>die Nicht-Standard-Anwendungsinspektion</u>.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA Security Appliance Software Version 8.3(1) mit ASDM 6.3.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Globale Standardrichtlinie

Standardmäßig enthält die Konfiguration eine Richtlinie, die dem gesamten standardmäßigen Anwendungsinspektionsverkehr entspricht und bestimmte Überprüfungen auf den Datenverkehr an allen Schnittstellen anwendet (eine globale Richtlinie). Nicht alle Überprüfungen sind standardmäßig aktiviert. Sie können nur eine globale Richtlinie anwenden. Wenn Sie die globale Richtlinie ändern möchten, müssen Sie entweder die Standardrichtlinie bearbeiten oder deaktivieren und eine neue Richtlinie anwenden. (Eine Schnittstellenrichtlinie überschreibt die globale Richtlinie.)

Wählen Sie im ASDM **Configuration > Firewall > Service Policy Rules** (Konfiguration > Firewall > Service-Richtlinienregeln) aus, um die globale Standardrichtlinie anzuzeigen, deren Standardanwendungsinspektion wie folgt lautet:



Die Standardrichtlinienkonfiguration umfasst die folgenden Befehle:

```
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-po	olicy global_policy global

Wenn Sie die globale Richtlinie deaktivieren müssen, verwenden Sie den globalen Befehl **no** service-policy global_policy. Um die globale Richtlinie mithilfe von ASDM zu löschen, wählen Sie Configuration > Firewall > Service Policy Rules aus. Wählen Sie anschließend die globale Richtlinie aus, und klicken Sie auf Löschen.

[Configuration > Firewall > Service Policy Rules										
	🗣 Add 👻 🗹 Edit 📋 Delete 🗇 🐳 👗 🖳 💼 🚽 🔍 Find 🖼 Diagram 🗠 Packet Trace										
	Traffic Classification	Traffic Classification									
	Name	lame # Enabled Match Source Destination Service Time							Rule Actions		
	Global; Policy: global_policy										
	inspection_default	inspection_default 🔍 👘 Match 🚸 any 👘 any 🔍 default-inspect 🔍 Inspect DNS Map preset_dns_map									
									Inspect ESMTP (13 more lospect actions)		

Hinweis: Wenn Sie die Service-Richtlinie mit ASDM löschen, werden die zugehörigen Richtlinienund Klassenzuordnungen gelöscht. Wenn die Dienstrichtlinie jedoch mithilfe der CLI gelöscht wird, wird nur die Dienstrichtlinie von der Schnittstelle entfernt. Die Klassenzuordnung und Richtlinienzuordnung bleiben unverändert.

Deaktivieren der globalen Standardüberprüfung für eine Anwendung

Um die globale Überprüfung für eine Anwendung zu deaktivieren, verwenden Sie die *no*-Version des Befehls **inspect**.

Um z. B. die globale Überprüfung für die FTP-Anwendung zu entfernen, an die die Sicherheits-Appliance überwacht, verwenden Sie den Befehl **no inspect ftp** im Klassenkonfigurationsmodus.

Der Klassenkonfigurationsmodus kann über den Konfigurationsmodus für die Richtlinienzuordnung aufgerufen werden. Um die Konfiguration zu entfernen, verwenden Sie die *no*-Form des Befehls.

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

Gehen Sie wie folgt vor, um die globale Überprüfung für FTP mithilfe von ASDM zu deaktivieren:

Hinweis: Unter Zulassen von HTTPS-Zugriff für ASDM finden Sie grundlegende Einstellungen, um über ASDM auf PIX/ASA zuzugreifen.

 Wählen Sie Konfiguration > Firewall > Service Policy Rules (Regeln f
ür Service-Richtlinien) aus, und wählen Sie die globale Standardrichtlinie aus. Klicken Sie dann auf Bearbeiten, um die globale Überpr
üfungsrichtlinie zu bearbeiten.

2. Wählen Sie im Fenster "Edit Service Policy Rule" (Servicerichtlinienregel bearbeiten) auf der Registerkarte Rule Actions (Regelaktionen) die Option Protocol Inspection

(Protokollüberprüfung) aus. Stellen Sie sicher, dass das Kontrollkästchen FTP deaktiviert ist. Dadurch wird die FTP-Prüfung wie im nächsten Bild gezeigt deaktiviert. Klicken Sie dann auf OK und dann auf

Übernehmen.

dit Service Policy Rule)	
affic Classification Default	Inspections Rule Actions	
Protocol Inspection Intrus	ion Prevention Connection Settings QoS NetFlow	
Select all inspection rul	ec.	
	Configure	
	Configure DNS Inspect Map: preset dns map	
SMTP	Configure	
ETR	Configure	
H.323 H.225	Configure	
H.323 RAS	Configure	=
НТТР	Configure	
ICMP		
ICMP Error		
ILS ILS		
<u>—</u> IМ	Configure	-
✓ IP-Options	Configure	
🔲 IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
✓ NETBIOS	Configure	
PPTP		<u>~</u>
	OK Cancel Help	

Hinweis: Weitere Informationen zur FTP-Prüfung finden Sie unter <u>PIX/ASA 7.x: Aktivieren des</u> Konfigurationsbeispiels für FTP-/TFTP-Dienste.

Überprüfung für nicht standardmäßige Anwendung aktivieren

Die erweiterte HTTP-Überprüfung ist standardmäßig deaktiviert. Um die HTTP-Überprüfung in global_policy zu aktivieren, verwenden Sie den Befehl **inspect http** unter class inspect_default.

In diesem Beispiel wird jede HTTP-Verbindung (TCP-Datenverkehr an Port 80), die über eine beliebige Schnittstelle in die Sicherheits-Appliance gelangt, für die HTTP-Prüfung klassifiziert. *Da es sich bei der Richtlinie um eine globale Richtlinie handelt, erfolgt die Überprüfung nur, wenn der Datenverkehr in die einzelnen Schnittstellen eingeht.*

```
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 diesem Beispiel *wird* jede HTTP-Verbindung (TCP-Datenverkehr an Port 80), die über die *externe Schnittstelle* in die Sicherheits-Appliance eingeht oder diese verlässt, *für die HTTP-Überprüfung klassifiziert*.

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**

Führen Sie die folgenden Schritte aus, um das obige Beispiel mithilfe von ASDM zu konfigurieren:

 Wählen Sie Konfiguration > Firewall > Service Policy Rules und klicken Sie auf Add, um eine neue Service-Richtlinie

add - 🐨 site 🕮 salara		V Do atta	- 0.0	a del como d	Carlet Trans				
🖌 500 - 🛐 500 🗍 56658 3. 4. 👻 👘 💷 - of 100 🐻 565500 rdS									
raffic Cassification	essification							Rule Actions	
are sided rates added as been	,	Enabled	Match	Source	Destination	Service	TIPN		
is coar; Policy: global_policy			Do wash	all some	10.000	 Address in some 		 Increase COIN Management where more 	
a sherri n Cherger								Inspect CSHTP (16 more inspect actions)	

 Wählen Sie im Fenster Assistent für die Hinzufügen von Service-Richtlinienregeln -Servicerichtlinie das Optionsfeld neben Schnittstelle aus. Damit wird die Richtlinie auf eine bestimmte Schnittstelle angewendet, die in diesem Beispiel die externe Schnittstelle ist. Geben Sie einen Richtliniennamen ein, der in diesem Beispiel außerhalb von cisco-policy liegt. Klicken Sie auf Weiter.

🖆 Add Service I	Policy Rule Wizard - Service Polic	у			×
Adding a new servi 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 policy and Apply To: policy can be configured per interface or a	vice policy ice policy :	rule. rule.	already evists then you	I can add a new
rule into the exis	outside - (create new service policy)	ate a new	service policy.		
Description:					
🔘 Global - appli	es to all interfaces				
Policy Name:	global_policy				
Description:					
				< Back Next >	Cancel Help

 Geben Sie im Fenster Add Service Policy Rule Wizard - Traffic Classification Criteria (Hinzufügen von Service-Richtlinienregeln - Klassifizierungskriterien) den neuen Namen der Verkehrsklasse an. Der in diesem Beispiel verwendete Name ist Fremdklasse. Stellen Sie sicher, dass das Kontrollkästchen neben TCP- oder UDP-Zielport aktiviert ist, und klicken Sie auf

Weiter.

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	×
• Create a new traffic class:	outside-class	
Description (optional):		
Traffic Match Criteria		_
Default Inspection Traf	fic	
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	
Ouse class-default as the traffic	ic class.	
If traffic does not match a exi situation.	isting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all	
	< Back Next > Cancel Help	

4. Wählen Sie im Abschnitt "**Protokoll"** im Fenster "Assistent für die Richtlinie zum Hinzufügen von Services - Datenverkehrszuordnung - Ziel-Port" das Optionsfeld neben **TCP** aus. Klicken Sie dann auf die Schaltfläche neben **Service**, um den gewünschten Service auszuwählen.

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

 Wählen Sie im Fenster Service durchsuchen die Option HTTP als Service aus. Klicken Sie anschließend auf OK.

Nam	ie.	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
-		tcp	default (1-65535)	2748	10/11 //po	Costapolit	~
-	daytime	tcp	default (1-65535)	13			
-	teo discard	tcp	default (1-65535)	9			
_	😟 domain	tcp	default (1-65535)	53			1
-	👓 🚾 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			
-	👓 💶 🚾 🚥	tcp	default (1-65535)	543			
-	🗠 💶 kshell	tcp	default (1-65535)	544			~

6. Im Fenster Assistent für die Richtlinie für das Hinzufügen von Services -

Datenverkehrszuordnung - Zielport können Sie sehen, dass der ausgewählte Service tcp/http lautet. Klicken Sie auf

Weiter.

🖆 Add	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 > Cance	s Help

7. Aktivieren Sie im Fenster Assistent für das Hinzufügen von Service-Richtlinien -Regelaktionen das Kontrollkästchen neben HTTP. Klicken Sie dann neben HTTP auf Konfigurieren.

Add Service Policy	Rule Wizard - Rule Actions	
Protocol Inspection Int	usion Prevention Connection Settings QoS NetFlow	
		~
	Configure	
DNS	Configure	
ESMTP	Configure	
FTP	Configure	
	Configure	
H.323 RA5	Configure	
HTTP	Configure	
ICMP		
ICMP Error		
ILS I		
IM 🔄	Configure	
IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
NETBIOS	Configure	
PPTP		
RSH		~
		Back Finish Cancel Hel

8. Aktivieren Sie im Fenster Select HTTP Inspect Map (HTTP-Inspektionszuordnung auswählen) das Optionsfeld neben **Use the Default HTTP Inspection Map (Standard-HTTP-Inspektionszuordnung verwenden)**. In diesem Beispiel wird die HTTP-Standardprüfung verwendet. Klicken Sie anschließend auf

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

9. Klicken Sie auf **Fertig** stellen.

otocol Inspection Intrusi	an Prevention Connectio	n Settings QoS	NetFlow	
CTIQBE				
DCERPC	Configure			
DN5	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			
IPSec-Pass-Thru	Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				
-				

10. Unter **Configuration > Firewall > Service Policy Rules** (Konfiguration > Firewall > Service-Richtlinienregeln) sehen Sie die neu konfigurierte Service-Richtlinie **außerhalb von Cisco** (zum Überprüfen von HTTP) zusammen mit der auf der Appliance bereits vorhandenen Standard-Service-Richtlinie. Klicken Sie auf **Apply**, um die Konfiguration auf die Cisco ASA anzuwenden.

Configuration > Firewall > Service	Policy	Rules								
💠 Add 🔸 🗃 Edit 👕 Delete 🎓 🎸 🐰 🐜 🏛 🤚 🔍 Find 💬 Diagram 👼 Packet Trace										
Traffic Classification	Dula Astions									
Name	\$	Enabled	Match	Source	Destination	Service	Time	NUE ACCOLS		
Enterface: outside; Policy: outside-	isco-po	dicy								
outside-class			🖹 Match	🎱 any	🍥 any	😎 http		Q, Inspect HTTP		
Global; Policy: global_policy			Description							
· inspection_default			LE) Match	🎱 any	🥥 any	Q, default-inspec		Q Inspect DNS Map preset_dns_map Q Inspect ESMTP (L3 more inspect actions)		
<										
					Apply Reset					

Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Anforderungen für Kommentare (RFCs)
- Anwenden der Protokollüberprüfung auf Anwendungsebene
- Technischer Support und Dokumentation für Cisco Systeme