# ASA 8.3 e versioni successive - Configurazione dell'ispezione con ASDM

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Criterio globale predefinito Disabilita ispezione globale predefinita per un'applicazione Abilita ispezione per applicazione non predefinita Informazioni correlate

# **Introduzione**

In questo documento viene fornita una configurazione di esempio per Cisco Adaptive Security Appliance (ASA) con le versioni 8.3(1) e successive istruzioni su come rimuovere l'ispezione predefinita dai criteri globali di un'applicazione e su come abilitare l'ispezione per un'applicazione non predefinita utilizzando Adaptive Security Device Manager (ASDM).

Per ulteriori informazioni, fare riferimento al documento <u>PIX/ASA 7.X: Disabilitare l'ispezione</u> globale predefinita e abilitare l'ispezione delle applicazioni non predefinita per la stessa configurazione sull'appliance Cisco ASA con le versioni 8.2 e precedenti.

# **Prerequisiti**

## **Requisiti**

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco ASA Security Appliance versione 8.3(1) con ASDM 6.3.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## **Convenzioni**

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

# Criterio globale predefinito

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica determinate ispezioni al traffico su tutte le interfacce (un criterio globale). Non tutte le ispezioni sono abilitate per impostazione predefinita. È possibile applicare un solo criterio globale. Se si desidera modificare il criterio globale, è necessario modificare il criterio predefinito oppure disattivarlo e applicarne uno nuovo. Un criterio di interfaccia ha la precedenza sul criterio globale.

In ASDM, scegliere **Configurazione > Firewall > Regole criteri servizio** per visualizzare il criterio globale predefinito con l'ispezione dell'applicazione predefinita, come mostrato di seguito:



La configurazione predefinita dei criteri include i comandi seguenti:

```
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

Se è necessario disabilitare il criterio globale, utilizzare il comando **no service-policy global\_policy global\_policy**. Per eliminare il criterio globale utilizzando ASDM, scegliere **Configurazione > Firewall > Regole dei criteri di servizio**. Selezionare quindi il criterio globale e fare clic su **Elimina**.

1	Configuration > Firewall > Service Policy Rules											
	Traffic Classification		Dudo Antinos									
	Name	#	Enabled	Match	Source	Destination	Service	Time	KUB ALCOIN			
	Global; Policy: global_policy											
	inspection_default			🕒 Match	🍨 any	🎨 any	🔍 default-inspec		Inspect DNS Map preset_dns_map.			
									Inspect ESMTP			
									(13 more inspect actions)			

**Nota:** quando si elimina il criterio del servizio con ASDM, vengono eliminati anche i mapping dei criteri e delle classi associati. Tuttavia, se il criterio del servizio viene eliminato utilizzando CLI, solo il criterio del servizio viene rimosso dall'interfaccia. La mappa delle classi e la mappa dei criteri rimangono invariate.

#### Disabilita ispezione globale predefinita per un'applicazione

Per disabilitare l'ispezione globale per un'applicazione, utilizzare la versione *no* del comando **inspect**.

Ad esempio, per rimuovere l'ispezione globale dell'applicazione FTP su cui l'accessorio di sicurezza è in ascolto, usare il comando **no inspect ftp** in modalità di configurazione classe.

La modalità di configurazione delle classi è accessibile dalla modalità di configurazione della mappa dei criteri. Per rimuovere la configurazione, usare la forma *no* del comando.

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

Per disabilitare l'ispezione globale per FTP con ASDM, attenersi alla seguente procedura:

**Nota: per** accedere a <u>PIX/ASA</u> tramite ASDM, consultare le impostazioni di base di <u>Consenti</u> <u>accesso HTTPS</u> per <u>ASDM</u>.

 Scegliere Configurazione > Firewall > Regole criteri servizio e selezionare il criterio globale predefinito. Fare quindi clic su Modifica per modificare il criterio di ispezione globale.

giobalo.											
Configuration > Firewall > Service	Policy Ru	<u>iles</u>									
🗣 Add 🔹 💽 Edit 📋 Delete 🧳	÷   %	Ra (11	Q, Fir	id 🔛 Diagram 🕂 Pa	oket Trace						
Traffic Classification	Traffic Classification										
Name	# E	nabled N	Match	Source	Destination	Service	Time	Rule wotions			
Global; Policy: global_policy	Global; Policy: global_policy										
inspection_default			Match	≪trany	v() any	🔍 default-inspec		<ul> <li>Inspect DN5 Map preset_dns_map</li> <li>Inspect ESMTP</li> <li>(13 more basect actions)</li> </ul>			

2. Nella finestra Modifica regola dei criteri per i servizi scegliere Ispezione protocollo nella

scheda **Azioni regola**. Verificare che la casella di controllo **FTP** sia deselezionata. In questo modo l'ispezione FTP viene disattivata come mostrato nell'immagine seguente. Fare quindi clic su **OK** e su

#### Applica.

Protocol Inspection Televisi	on Provention	action Sattings Cost NatElaw	
Incrusi	on Prevendorn Com	ector seconds   Qos   Nethow	
Select all inspection rule	is .		
CTIQBE			^
DCERPC	Configure		
DNS	Configure	DNS Inspect Map: preset_dns_map	
ESMTP	Configure		
ETP:	Configure		
M.323 H.225	Configure		
M.323 RAS	Configure		2
HTTP	Configure		
ICMP			
ICMP Error			
ILS I			
MI 🔄	Configure		
IP-Options	Configure		
IPSec-Pass-Thru	Configure		
MMP	Configure		
MGCP	Configure		
✓ NETBIOS	Configure		
PPTP			~

**Nota:** per ulteriori informazioni sull'ispezione FTP, consultare il documento <u>PIX/ASA 7.x: Abilita</u> esempio di configurazione dei servizi <u>FTP/TFTP</u>.

#### Abilita ispezione per applicazione non predefinita

L'ispezione HTTP avanzata è disabilitata per impostazione predefinita. Per abilitare l'ispezione HTTP in global\_policy, utilizzare il comando **inspect http** in class\_inspection\_default.

Nell'esempio, qualsiasi connessione HTTP (traffico TCP sulla porta 80) che entra nell'appliance di sicurezza attraverso un'interfaccia qualsiasi viene classificata per l'ispezione HTTP. *Poiché il criterio è globale, l'ispezione viene eseguita solo quando il traffico entra in ciascuna interfaccia.* 

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** 

Nell'esempio, tutte le connessioni HTTP (traffico TCP sulla porta 80) che entrano o escono dall'appliance di sicurezza attraverso l'*interfaccia esterna vengono classificate per l'ispezione 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 Per configurare l'esempio precedente utilizzando ASDM, attenersi alla seguente procedura:** 

 Scegliere Configurazione > Firewall > Regole dei criteri di servizio e fare clic su Aggiungi per aggiungere un nuovo criterio di



 Nella finestra Aggiunta guidata regola dei criteri di servizio - Criteri di servizio scegliere il pulsante di opzione accanto a Interfaccia. In questo modo il criterio viene applicato a un'interfaccia specifica, ovvero l'interfaccia esterna di questo esempio. Specificare un nome di criterio esterno a cisco-policy in questo esempio. Fare clic su Next (Avanti).

🖆 Add Service 🛛	Policy Rule Wizard - Service Polic	cy	×
Adding a new servi Step 1: Configure 1 Step 2: Configure 1 Step 3: Configure 2 Create a Service Po Only one service rule into the exist	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 tion service policy. Otherwise, you can ce	vice policy rule. vice policy rule. at global level. If a service policy already exists, then you can add a new	
<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 Help	

 Nella finestra Criteri di classificazione traffico della procedura guidata Aggiungi regola dei criteri servizio specificare il nome della nuova classe di traffico. Il nome utilizzato in questo esempio è outside-class. Verificare che la casella di controllo accanto a Porta di destinazione TCP o UDP sia selezionata e fare clic su Avanti.

🖆 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	
Ouse an existing traffic class: inspection_default	
<ul> <li>Use class-default as the traffic class.</li> </ul>	
If traffic does not match a existing traffic class, then it will match the class-def situation.	ault traffic class. Class-default can be used in catch all
	Cancel Help

 Nella finestra Aggiunta guidata regola dei criteri del servizio - Corrispondenza traffico - Porta di destinazione, scegliere il pulsante di opzione accanto a TCP nella sezione Protocollo. Quindi, fare clic sul pulsante accanto a Servizio per scegliere il servizio richiesto.

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

5. Nella finestra Sfoglia servizio, scegliere **HTTP** come servizio. Quindi fare clic su **OK**.

Name Protoco			Source Ports Destination Ports ICMP Type Description					
	- TC> ctiabe	tcp	default (1-65535)	2748	10. 1 1/po		~	
	te daytime	tcp	default (1-65535)	13				
	10 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				
	ne> http	top	default (1-65535)	80	]			
	😰 https	tcp	default (1-65535)	443				
	👳 ident	tcp	default (1-65535)	113				
	😰 imap4	tcp	default (1-65535)	143				
	· 📭 inc	tcp	default (1-65535)	194				
	😰 kerberos	tcp	default (1-65535)	750				
	🚥 klogin	tcp	default (1-65535)	543				
		hen	default (1-65535)	544			~	

6. Dalla finestra Aggiunta guidata regola dei criteri del servizio - Corrispondenza traffico - Porta di destinazione è possibile verificare che il **servizio** scelto è **tcp/http**. Fare clic su **Next** (Avanti).

📬 Add S	ervice Policy Rule Wizard - Traffic Match - Destination P	ort 🔄 🔀
Protocol:		
Service:	tcp/http	
	To specify port range for the service, use nnn-nnn format	
		<back next=""> Cancel Help</back>

7. Nella finestra Aggiunta guidata regole dei criteri del servizio - Azioni regola selezionare la casella di controllo HTTP. Quindi, fare clic su **Configure** (Configura) accanto a 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 RA5	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. Nella finestra Seleziona mappa ispezione HTTP, selezionare il pulsante di opzione accanto a **Usa la mappa di ispezione HTTP predefinita**. In questo esempio viene utilizzata l'ispezione HTTP predefinita. Quindi fare clic su

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

9. Fare clic su **Finish** (Fine).

rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIQ8E				
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-Thr	ru Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				

 In Configurazione > Firewall > Regole dei criteri di servizio vengono visualizzati i criteri di servizio appena configurati esternamente a cisco-policy (per ispezionare il protocollo HTTP) insieme ai criteri di servizio predefiniti già presenti sull'accessorio. Per applicare la configurazione all'appliance Cisco ASA, fare clic su Apply.

onfiguration > Firewall > Service Policy Rules									
🗣 Add 🕞 🌌 Edit 🏢 Delete   🖞	- 4	3 🖬 📾	- Q Fi	nd 🎛 Diagram 🗐	Packet Trace				
Traffic Classification	affic Classification								
Name	# Enabled Match Source Destination Service Time					Time	Rule Actions		
E Interface: outside; Policy: outside	-cisco-po	alicy							
outside-class			🖹 Match	🧼 any	iany 🔿	😎 http		Q, Inspect HTTP	
Global; Policy: global_policy									
<sup>1</sup> inspection_default			la Match	🌗 any	🎱 any	Q, default-inspec		Q, Enspect DNS Map preset_dns_map Q, Enspect ESMTP (L3 more inspect actions)	
4									
				_					
					Apply Res	et			

## Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>RFC (Requests for Comments)</u>
- Applicazione dell'ispezione del protocollo a livello di applicazione
- Documentazione e supporto tecnico Cisco Systems