# ASA 8.3以降:ASDMを使用したインスペクショ ンの設定

### 内容

<u>概要 前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>デフォルトのグローバル ポリシー</u> <u>アプリケーションのデフォルト グローバル インスペクションを無効にする</u> <u>デフォルト以外のアプリケーションのインスペクションを有効にする</u> 関連情報

### 概要

このドキュメントでは、アプリケーションのグローバル ポリシーからデフォルトの検査を削除す る方法と、Adaptive Security Device Manager (ASDM)を使用してデフォルト以外のアプリケー ションの検査を有効にする方法に関する、バージョン 8.3(1) 以降の Cisco 適応型セキュリティ ア プライアンス (ASA)の設定例を示します。

詳細は、『<u>PIX/ASA 7.X:デフォルトのデフォルト グローバル インスペクションを無効にして、</u> デフォルト以外のアプリケーションのインスペクションを有効にする』(Cisco ASA バージョン <u>8.2 以前の同じ構成が対象)を参照してください。</u>

## <u>前提条件</u>

#### <u>要件</u>

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco ASA セキュリティ アプライアンス ソフトウェア バージョン 8.3(1) と ASDM 6.3 が稼働する環境に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。 ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

# <u>デフォルトのグローバル ポリシー</u>

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致 するポリシーが設定に含まれ、特定のインスペクションがすべてのインターフェイスのトラフィ ックに適用されます(グローバル ポリシー)。 すべてのインスペクションがデフォルトでイネー ブルになっているわけではありません。適用できるグローバル ポリシーは 1 つだけです。グロー バル ポリシーを変更する場合は、デフォルト ポリシーを編集するか無効にし、新しいポリシーを 適用する必要があります。(インターフェイス ポリシーはグローバル ポリシーに優先します)。

ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] を選択して、以下に示すデフォルトのアプリケーション インスペクションを持つデフォルトのグローバル ポリシーを表示します。



デフォルト ポリシー設定には、次のコマンドが含まれています。

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

グローバル ポリシーを無効にする必要がある場合は、**no service-policy global\_policy グローバル** コマンドを使用します。ASDM を使用してグローバル ポリシーを削除するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択します。次に、グローバル ポリシーを選択し、 [Delete] をクリックします。

1	Configuration > Firewall > Service Policy Rules										
	💠 Add 🕞 🗃 Edit 📋 Delete 🖙 🌾 🐇 🏝 💼 🕤 🔍 Find 🖼 Diagram 🕰 Packet Trace										
	Traffic Classification	Iraffic Classification									
	Nome	#	Enabled	Match	Source	Destination	Service	Time	Rule Actions		
	Global; Policy: global_policy										
	inspection_default			🕒 Match	🤹 any	🎨 any	🔍 default-inspec		Inspect DNS Map preset_dns_map.		
									Inspect ESMTP		
									(13 more inspect actions)		

注:ASDMを使用してサービスポリシーを削除すると、関連付けられたポリシーとクラスマップ が削除されます。ただし、CLIを使用してサービス ポリシーが 削除された場合は、サービス ポ リシーのみがインターフェイスから削除されます。クラス マップおよびポリシー マップは変更さ れずそのまま残ります。

### <u>アプリケーションのデフォルト グローバル インスペクションを無効にする</u>

アプリケーションのグローバル インスペクションを無効にするには、*inspect* コマンドの no バー ジョンを使用します。

たとえば、セキュリティ アプライアンスでリッスンする FTP アプリケーションのグローバル インスペクションを削除するには、クラス コンフィギュレーション モードで no inspect ftp コマンドを使用します。

クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードか らアクセスできます。設定を削除するには、このコマンドの no 形式を使用します。

ASA(config)#policy-map global\_policy ASA(config-pmap)#class inspection\_default ASA(config-pmap-c)#**no inspect ftp** 

ASDM を使用して FTP のグローバル インスペクションを無効にするには、次の手順を実行して ください。

**注:ASDMを介**してPIX/ASAにアクセスす<u>る基本的な設定</u>については、『ASDM用のHTTPSアク セスの許可』を参照してください。

1. [Configuration] > [Firewall] > [Service Policy Rules] を選択して、デフォルトのグローバル ポリシーを選択します。次に、グローバル インスペクション ポリシーを編集するには、[Edit]をクリックします。

	Configuration > Firewall > Service	Policy	Rules								
	🗣 Add 🔹 🧭 Edit 📋 Delete 🌖	4	አ 🖻 🛍	< Q Fir	nd 🔛 Diagram 🏹 Pa	cket Trace					
L	Traffic Classification	Treffic Classification									
L	Name	# Enabled Match		Match	Source Destination		Service Time		Rule woolons		
L	😑 Global; Policy: global_policy										
	inspection_default			📭 Match	🔹 any	🊸 any	🔍 default-inspec		Inspect DNS Map preset_dns_map		
									Q Inspect ESMTP		
									(13 more banect actions)		

2. [Edit Service Policy Rule] ウィンドウで、[Rule Actions] タブの [Protocol Inspection] を選択 します。[FTP] チェック ボックスがオフになっていることを確認します。これにより、次の 画像に示すように、FTP インスペクションが無効になります。次に、[OK] をクリックして から [Apply] をクリックします。

otocol Inspection Intrusi	n Prevention Connection Settings QoS NetFlo	wo
Select all inspection rule	s	
CTIQBE		
DCERPC	Configure	
🗹 DNS	Configure DNS Inspect Map: preset	_dns_map
ESMTP	Configure	
ETP:	Configure	
🗹 H.323 H.225	Configure	
🖌 H.323 RAS	Configure	
MTTP	Configure	
ICMP		
ICMP Error		
🔲 ILS		
MI 🔝	Configure	
🗹 IP-Options	Configure	
🔝 IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
VETBIOS	Configure	
PPTP		

**注:FTP**インスペクションの詳細については、『<u>PIX/ASA 7.x:FTP/TFTP サービスをイネーブル</u> <u>にする設定例</u>』を参照してください。

### <u>デフォルト以外のアプリケーションのインスペクションを有効にする</u>

拡張 HTTP インスペクションは、デフォルトではディセーブルになっています。global\_policy の HTTP インスペクションを有効にするには、クラスの inspection\_default 下で **inspect http コマン ドを使用します。** 

この例では、任意のインターフェイスを通過してセキュリティ アプライアンスに入るすべての

HTTP 接続(ポート 80 の TCP トラフィック)が HTTP インスペクション対象として分類されま す。*このポリシーはグローバル ポリシーであるため、インスペクションが発生するのは各インタ ーフェイスにトラフィックが入ったときだけです*。

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

#### この例では、セキュリティ アプライアンスを出入りする HTTP 接続(ポート 80 の TCP トラフ ィック)で外*部インターフェイスを通過するすべての接続が HTTP インスペクション対象として 分類されます*。

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** ASDM を使用して上記の例を設定するには、次の手順を実行します。

1. 新しいサービス ポリシーを追加するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] をクリックします。

at s	a Enda	al Natch Source	Destination	Server Ter	Rule Actions
Riphal: Policy: clobal_policy					-
inspection_default		ing Hatch 🔿 any	(b ary	🔍 defealt inspect	<ul> <li>Inspect DRS Hap preset_drs_map</li> <li>Inspect ESHTP (10 more inspect actions)</li> </ul>

 [Add Service Policy Rule Wizard - Service Policy] ウィンドウから、[Interface] の横にあるオ プション ボタンを選択します。これにより、作成したポリシーが特定のインターフェイス (この例では Outside interface)に適用されます。ポリシー名(この例では outside-ciscopolicy)を付けます。[next] をクリックします。

🖆 Add Service P	Policy Rule Wizard - Service Policy	×
Adding a new servic Step 1: Configure t Step 2: Configure t Step 3: Configure a 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 service policy rule. actions on the traffic classified by the service policy rule. policy and Apply To: policy can be configured per interface or at global level. If a service policy already exists, then you can add a new ting service policy. Otherwise, you can create a new service policy.	
<ul> <li>Interface:</li> </ul>	outside - (create new service policy) 👻	
Policy Name:	outside-cisco-policy	
Description:		
🔘 Global - applie	es to al interfaces	
Policy Name:	global_policy	
Description:		
	< Back Next > Cancel H	qle

3. [Add Service Policy Rule Wizard - Traffic Classification Criteria] ウィンドウから、新しいトラ フィック クラスの名前を指定します。この例で使用する名前は、outside-classです。[TCP or UDP Destination Port] の隣のチェック ボックスがオンになっていることを確認して、 [Next] をクリックします。

🖆 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 DIFServ CodePoints (DSCP)
IP Precedence
Any traffic
Ouse 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
siddoon
< Back Next > Cancel Help
Add Service Policy Rule Wizard - Traffic Match - Destination Port] ウィンドウから、 Protocol] セクションの [TCP] の横にあるオプション ボタンを選択します。次に、必要な -ビスを選択するには、[Service] の横にあるボタンをクリックします。
🖀 Add Service Policy Rule Wizard - Traffic Match - Destination Port

5. [Browse Service] ウィンドウで、サービスとして [HTTP] を選択します。次に、[OK] をクリ ックします。

To specify port range for the service, use nnn-nnn format.

Protocol: 💿 TCP 🔵 UDP

Service:

Name Protocol			Source Ports	Destination Ports	ICMP Type	Description		
i.	• rotiche	tcp	default (1-65535)	2748	Tenir Type	Description	~	
_	· 102 daytime	tcp	default (1-65535)	13				
-	tiscard	tcp	default (1-65535)	9				
_	😰 domain	tcp	default (1-65535)	53			1	
-	😳 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-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	tcp	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			~	

6. [Add Service Policy Rule Wizard - Traffic Match - Destination Port] ウィンドウで、選択され た [Service] が **tcp/http であることを確認できます。**[next] をクリックします。

🖆 Add	Service Policy Rule Wizard - Traffic Match - Desti	nation Port 📃 🔀
Protocol: Service:	CP UDP      tcp/http     To specify port range for the service, use nnn-nnn format	
L	to speak y partitinge for the second place internation	
		< Back Next > Cancel Help

7. [Add Service Policy Rule Wizard - Rule Actions] ウィンドウから、[HTTP] の隣にあるチェッ クボックスをオンにします。次に、[HTTP]の横にある [Configure] をクリックします。

Add Service Poli	cy Rule Wizard - F	Rule Actions			
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	1	
CTIOBE					~
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				
IPSec-Pass-Th	ru Configure				
MMP	Configure				
MGCP	Configure				
NETBIOS	Configure				
PPTP					
RSH					~
				< Back	Finish Cancel He

8. [Select HTTP Inspect Map] ウィンドウから、[Use the Default HTTP inspection map] の横に あるラジオ ボタンをオンにします。この例では、デフォルトの HTTP インスペクションを 使用します。次に、[OK] をクリックします。

<b>1</b>	Select HTTP Inspect Map 🔡
0	Use the default HTTP inspection map
0	Select an HTTP inspect map for fine control over inspection
	Name Add
	OK Cancel Help

9. [Finish] をクリックします。

rotocol Inspection Int	trusion Prevention	Connection Settings	QoS NetFlow	
CTIQ8E				
DCERPC	Configure			
DNS	Configure			
ESMTP	Configure			
FTP	Configure			
N.323 H.225	Configure			
H.323 RA5	Configure			
HTTP:	Configure			
ICMP				
ICMP Error				
🗌 1LS				
🛄 IM	Configure			
IP-Options	Configure			
IPSec-Pass-Thru	Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				

10. [Configuration] > [Firewall] > [Service Policy Rules] で、新しく設定したサービス ポリシー である outside-cisco-policy (HTTP インスペクション用)が、アプライアンスに既に存在 するデフォルトのサービス ポリシーとともに表示されます。[Apply] をクリックして Cisco ASA に設定に適用します。

onfiguration > Firewall > Service Policy Rules								
🗣 Add 🔸 🏹 Edit 🏢 Delete 👌	14	3 🖬 📾	- Q Pi	nd 🕎 Diagram I	Racket Trace			
Traffic Classification								Dula Astiona
Name	\$	Enabled	Match	Source	Destination	Service	Time	KUE ACCORS
Enterface: outside; Policy: outside	-cisco-po	alicy						
outside-class			🕒 Match	🎱 any	iany iang	😎 http		Q, Inspect HTTP
Global; Policy: global_policy								
* Inspection_default			La Match	🌗 any	any	Q, default-inspec		Q_ Inspect DNS Map preset_dns_map Q_ Inspect ESMTP (13 more inspect actions)
<								
					Apply Res	et		

# <u>関連情報</u>

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Adaptive Security Device Manager
- Requests for Comments (RFCs)
- アプリケーション層プロトコル検査の適用
- ・ テクニカル サポートとドキュメント – Cisco Systems