ASA 8.3 이상 - ASDM을 사용하여 검사 구성

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>기본 전역 정책</u> <u>응용 프로그램에 대한 기본 전역 검사 비활성화</u> <u>기본 응용 프로그램이 아닌 응용 프로그램에 대한 검사 사용</u> <u>관련 정보</u>

<u>소개</u>

이 문서에서는 애플리케이션에 대한 전역 정책에서 기본 검사를 제거하는 방법 및 ASDM(Adaptive Security Device Manager)을 사용하여 기본 이외의 애플리케이션에 대한 검사를 활성화하는 방법 에 대해 버전 8.3(1) 이상의 Cisco ASA(Adaptive Security Appliance)에 대한 샘플 컨피그레이션을 제공합니다.

PIX<u>/ASA 7.X 참조:</u> 버전 8.2 이하<u>의</u> Cisco ASA에서 동일한 컨피그레이션에 대해<u>Default Global</u> Inspection을 비활성화하고 Enable Non-Default Application Inspection을 활성화합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 ASDM 6.3이 포함된 Cisco ASA Security Appliance Software 버전 8.3(1)을 기반 으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

<u>기본 전역 정책</u>

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며 모든 인터페이스의 트래픽에 특정 검사를 적용합니다(글로벌 정책). 기본적으로 모든 검사 가 활성화되어 있는 것은 아닙니다. 하나의 전역 정책만 적용할 수 있습니다. 전역 정책을 변경하려 면 기본 정책을 수정하거나 비활성화하고 새 정책을 적용해야 합니다. (인터페이스 정책은 전역 정 책을 재정의합니다.)

ASDM에서 Configuration(컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규 칙)를 선택하여 기본 애플리케이션 검사가 있는 기본 전역 정책을 다음과 같이 확인합니다.



기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.

```
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
```

전역 정책을 비활성화해야 하는 경우 no service-policy global_policy 전역 명령을 사용합니다.

service-policy global_policy global

ASDM을 사용하여 전역 정책을 삭제하려면 Configuration(컨피그레이션) > **Firewall(방화벽)** > **Service Policy Rules(서비스 정책 규칙)를 선택합니다**. 그런 다음 전역 정책을 선택하고 Delete(**삭 제)**를 클릭합니다.

Configuration > Firewall > Servi	ice Policy	Rules						
🗣 Add 🔹 🌌 Edit 📋 Delete	1 4	X 🖻 🖷	• Q, Fit	nd 🔤 Diagram 🕰 Pa	acket Trace			
Traffic Classification								Dula Antina
Name	#	Enabled	Match	Source	Destination	Service	Time	Rule Actions
🖯 Global; Policy: global_policy								
inspection_default			Match	≪) any	≪) any	🔍 default-inspec		Inspect DNS Map preset_dhs_map Inspect ESMTP (13 more inspect actions)

참고: ASDM을 사용하여 서비스 정책을 삭제하면 관련 정책 및 클래스 맵이 삭제됩니다. 그러나 CLI를 사용하여 서비스 정책을 삭제하면 서비스 정책만 인터페이스에서 제거됩니다. 클래스 맵 및 정책 맵은 변경되지 않습니다.

응용 프로그램에 대한 기본 전역 검사 비활성화

응용 프로그램에 대한 전역 검사를 비활성화하려면 inspect 명령의 no 버전을 사용합니다.

예를 들어, 보안 어플라이언스가 수신 대기하는 FTP 애플리케이션에 대한 전역 검사를 제거하려면 클래스 컨피그레이션 모드에서 no inspect ftp 명령을 사용합니다.

클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션 을 제거하려면 이 명령의 *no* 형식을 사용합니다.

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

ASDM을 사용하여 FTP에 대한 전역 검사를 비활성화하려면 다음 단계를 완료하십시오.

참고: ASDM을 통해 PIX/ASA에 액세스하려면 <u>ASDM</u>에 대한 HTTPS 액세스 허용을 참조하십시오.

1. Configuration > Firewall > Service Policy Rules를 선택하고 기본 전역 정책을 선택합니다. 그 런 다음 Edit(편집)를 클릭하여 전역 검사 정책을 편집합니다

Configuration > Firewall > Service	Policy	Rules						-	
💠 Add 🕞 🗃 Edit 👔 Delete 🎓 🍜 👗 🎭 📖 🕤 🗛 Find 📴 Diagram 💐 Packet Trace									
Traffic Classification								Dula Artica	
Name	#	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)	

2. Edit Service Policy Rule(서비스 정책 규칙 수정) 창의 Rule Actions(규칙 작업) 탭 아래에 Protocol Inspection(프로토콜 검사)을 선택합니다. FTP 확인란이 선택되지 않았는지 확인합 니다. 그러면 다음 이미지에 표시된 대로 FTP 검사가 비활성화됩니다. 그런 다음 확인을 클릭 하고 적용 을 클릭합니다

rotocol Inspection Intrus	on Prevention Connection Settings QoS NetFlow	
Select all inspection rul	es	
CTIQBE		
DCERPC	Configure	
DNS	Configure DNS Inspect Map: preset_dns_map	
ESMTP	Configure	
ETP:	Configure	
M.323 H.225	Configure	
H.323 RAS	Configure	
	Configure	
ICMP		
ICMP Error		
ILS		
M []	Configure	
✓ IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	
VETBIOS	Configure	
PPTP		

참고: FTP 검사에 대한 자세한 내용은 <u>PIX/ASA 7.x: FTP/TFTP 서비스 컨피그레이션 예를 활성화</u> <u>합니다</u>.

<u>기본 응용 프로그램이 아닌 응용 프로그램에 대한 검사 사용</u>

고급 HTTP 검사는 기본적으로 비활성화되어 있습니다. global_policy에서 HTTP 검사를 활성화하 려면 class inspection_default 아래에서 inspect http 명령을 사용합니다.

이 예에서는 모든 인터페이스를 통해 보안 어플라이언스에 들어가는 모든 HTTP 연결(포트 80의 TCP 트래픽)이 HTTP 검사를 위해 분류됩니다. *정책은 전역 정책이므로 트래픽이 각 인터페이스에* 들어갈 때만 검사가 발생합니다.

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

이 예에서는 *외부 인터페이스*를 통해 보안 어플라이언스를 드나드는 HTTP 연결(포트 80의 TCP 트 래픽)이 *HTTP 검사를 위해 분류됩니다*.

```
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
ASDM을 사용하여 위의 예를 구성하려면 다음 단계를 수행합니다.
```

1. Configuration(**컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)를** 선택하고 Add(추가)를 클릭하여 새 서비스 정책을 추가합니다

magnification is threwall a service i	Policy	Roles						
🗣 Add 👻 💽 Edit 🏢 Delete 🗇	÷	3, 🗈 🛍	- Q.n	nd 🔁 Olagram 🕰 P	acket Trace			
Traffic Cessification								This fathers
Nerre	ø.	Enabled	Match	Source	Destination	Service	Time	
Elobal; Policy: global_policy								
inspection_default			Dig Huld i	() ay	(b) ay	🔍 defeult inspec		 Inspect ORS Hap prosit_drs_nap. Inspect CSHTP (10 more inspect actions)

2. Add Service Policy Rule Wizard - Service Policy(서비스 정책 추가 마법사 - 서비스 정책) 창에 서 Interface 옆의 라디오 버튼을 선택합니다. 이렇게 하면 특정 인터페이스에 생성된 정책이 적용됩니다. 이 인터페이스는 **외부** 인터페이스입니다. 이 예에서 outside-cisco-policy인 정책 이름을 입력합니다. Next(**다음)를 클릭합니다**

🖆 Add Service P	Policy Rule Wizard - Service Policy	×
Adding a new servic Step 1: Configure a 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. plicy 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.	
 Interface: 	outside - (create new service policy) 💙	
Policy Name:	outside-cisco-policy	
Description:		
🔘 Global - applie	es to all interfaces	
Policy Name:	global_policy	
Description:		
	< Back Next > Cancel He	-lb

3. Add Service Policy Rule Wizard - Traffic Classification Criteria 창에서 새 트래픽 클래스 이름 을 제공합니다. 이 예에서 사용되는 이름은 **outside-class입니다**. **TCP 또는 UDP Destination Port** 옆의 확인란이 선택되었는지 확인하고 **Next**(다음)를 클릭합니다

Create a new traffic class: outside-class Description (optional): Traffic Match Criteria Default Inspection Traffic Source and Destination IP Address (uses ACL) Tunnel Group FICP or LDP Destination Port RTP Range IP DiffServ CodePoints (DSCP) IP Precedence Any traffic Use an existing traffic class: Inspection_default 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 al situation.	🖥 Add Service Policy Rule	Wizard - Traffic Classification Criteria
Description (optional): Traffic Match Criteria Default Inspection Traffic Source and Destination IP Address (uses ACL) Tunnel Group Y FCP or UDP Destination Porti RTP Range IP DiffServ CodePoints (DSCP) IP Precedence Any traffic 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 al situation.	 Create a new traffic class: 	outside-class
Traffic Match Criteria Default Inspection Traffic Source and Destination IP Address (uses ACL) Tunnel Group VICP or UDP Destination Ports RTP Range IP DiffServ CodePoints (DSCP) IP Precedence Any traffic 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 al situation.	Description (optional):	
 □ Default Inspection Traffic □ Source and Destination IP Address (uses ACL) □ Tunnel Group ♥ SCP or UDP Destination Port □ RTP Range □ IP DiffServ CodePoints (DSCP) □ IP Precedence □ Any traffic ○ Use an existing traffic class: Inspection_default ▼ ○ 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 al situation. 	Traffic Match Criteria	
Source and Destination IP Address (uses ACL) Tunnel Group FCP or UDP Destination Parts RTP Range IP DiffServ CodePoints (DSCP) IP Precedence Any traffic Use an existing traffic class: If praffic 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 al situation. (Back Next > Cancel Hele)	Default Inspection Tra	ffic
☐ Tunnel Group Image Image IP DiffServ CodePoints (DSCP) IP Precedence Any traffic Use an existing traffic class: Inspection_default 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 al situation.	Source and Destinatio	n IP Address (uses ACL)
CCP or UDP Destination Port RTP Range IP DiffServ CodePoints (DSCP) IP Precedence Any traffic Use an existing traffic class: inspection_default v 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 al situation. Kext Next > Cancel Hell	Tunnel Group	
■ RTP Range IP DiffServ CodePoints (DSCP) IP Precedence Any traffic Use an existing traffic class: inspection_default 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 al situation. < Back Next > Cancel Hell	CP or UDP Destinatio	n Port
P DiffServ CodePoints (DSCP) P Precedence Any traffic Use an existing traffic class: Inspection_default 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 al situation. Sec. Next > Cancel Hele	RTP Range	
 □ IP Precedence □ Any traffic ○ Use an existing traffic class: inspection_default ○ 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 al situation. 	IP DiffServ CodePoints	; (DSCP)
Any traffic Use an existing traffic class: Inspection_default 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 al situation.	IP Precedence	
Use 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 al situation. Back Next > Cancel	Any traffic	
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 al situation. Back Next > Cancel Hel	Use an existing traffic class:	inspection_default
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 a situation.	🔿 Use class-default as the traf	fic dass.
< Back Next > Cancel Hel	If traffic does not match a ex situation.	risting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all
< Back Next > Cancel Hel		
< Back Next > Cancel Hel		
		< Back Next > Cancel Help

4. Add 8	Service Policy Rule Wizard - Traffic Match	- Destination Port(서비스 정책 규	'칙 추가 마법
사 - 트	트래픽 매치 - 대상 포트) 창에서 Protocol(프	프로토콜) 섹션에서 TCP 옆의 라디	오 버튼을 선
택합니	니다. 그런 다음 서비스 옆의 버튼을 클릭히	아이 필요한 서비스를 선택합니다	

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

5. Browse Service(서비스 찾아보기) 창에서 HTTP를 서비스로 선택합니다. 그런 다음 확인을 클 릭합니다

Name		Protocol	Source Ports	Destination Ports	ICMP Type	Description	1
	👁 ctiqbe	tcp	default (1-65535)	2748			~
1	👁 daytime	tcp	default (1-65535)	13			
	👁 discard	tcp	default (1-65535)	9			
1	👁 domain	tcp	default (1-65535)	53			1
1	👁 echo	tcp	default (1-65535)	7			
1	🕐 exec	tcp	default (1-65535)	512			
	👁 finger	tcp	default (1-65535)	79			
1	👁 ftp	tcp	default (1-65535)	21			
1	👁 ftp-data	tcp	default (1-65535)	20			
1	😟 gopher	tcp	default (1-65535)	70			
1	👁 h323	tcp	default (1-65535)	1720			
1	👁 hostname	tcp	default (1-65535)	101			
1	👁 http	tcp	default (1-65535)	80			
	👁 https	tcp	default (1-65535)	443			
1	👁 ident	tcp	default (1-65535)	113			
1	👁 imap4	tcp	default (1-65535)	143			
1	👁 irc	tcp	default (1-65535)	194			
	👁 kerberos	tcp	default (1-65535)	750			
1	👁 klogin	tcp	default (1-65535)	543			
	👁 kshell	tcp	default (1-65535)	544			~

6. Add Service Policy Rule Wizard - Traffic Match - Destination Port(서비스 정책 규칙 추가 마법 사 - 트래픽 일치 - 대상 포트) 창에서 선택한 **서비스**가 **tcp/http**임을 확인할 수 있습니다. Next(**다음)를 클릭합니다**

🖆 Add S	Service Policy Rule Wizard - Traffic Match - D	estination Port 📃 🔀
Protocol:]
Service:	tcp/http	
	To specify port range for the service, use nnn-nnn forma	
		<back next=""> Cancel Help</back>
		/ 니니 / 귀켓 그런 국가 되었다. 그런 자아 카

7. Add Service Policy Rule Wizard - Rule Actions(서비스 정책 규칙 추가 마법사 - 규칙 작업) 창 에서 HTTP 옆의 확인란을 선택합니다. 그런 다음 HTTP 옆에 있는 Configure를 클릭합니다

ALLE SELVICE PUT	cynde wizdru -	More ACTIONS		
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIQBE				
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				
				Capcel Hinich Capcel Hi

8. Select HTTP Inspect Map(HTTP 검사 맵 선택) 창에서 Use the Default **HTTP inspection** map(기본 HTTP 검사 맵 사용) 옆의 라디오 버튼을 선택합니다. 이 예에서는 기본 HTTP 검사 가 사용됩니다. 그런 다음 확인을 클릭합니다

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

9. 마침을 클릭합니다

ABB BBF MBB PUI	ey Kule A Mail u -	MENS ACTIONS		
rotocol Inspection	Intrusion Prevention	Connection Settings	QoS NetFlow	
CTIOBE				
DCERPC	Configure			
DNS	Configure			
ESMTP	Configure			
FTP	Configure			
H.323 H.225	Configure			
H.323 RA5	Configure			
HTTP:	Configure			
ICMP				
ICMP Error				
🛄 1LS				
IM 🔄	Configure			
IP-Options	Configure			_
IPSec-Pass-Th	ru Configure			
MMP	Configure			
MGCP	Configure			
NETBIOS	Configure			
PPTP				
RSH				N
			C	Back Finish Consel his

10. Configuration(**컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙**)에 서 새로 구성된 서비스 정책 **outside-cisco-policy**(HTTP 검사를 위해)가 어플라이언스에 이미 있는 기본 서비스 정책과 함께 표시됩니다. Cisco ASA에 컨피그레이션을 적용하려면 Apply를 클릭합니다

onfiguration > Firewall > Service Policy Rules										
🗣 Add 🕞 🗃 Edit 👕 Delete 🎓 🍝 👗 🎭 🌉 - 🗛 Find 💬 Diagram 🛲 Packet Trace										
Traffic Classification	Dula Astima									
Name	\$	Enabled	Match	Source	Destination	Service	Time	Rule Accions		
Interface: outside; Policy: outside	-cisco-po	alicy					_			
outside-class			👌 Match	🎱 any	iany 💿	😎 http		Q, Inspect HTTP		
Global; Policy: global_policy										
inspection_default			La Match	🌗 any	iny 🔇	Q, default-inspec		Q, Enspect DNS Map preset_dns_map Q, Enspect ESMTP (LS more inspect actions)		
<					Ш					
Apply Reset										

<u>관련 정보</u>

- <u>Cisco ASA 5500 Series Adaptive Security Appliance</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>RFC(Request for Comments)</u>
- 애플리케이션 레이어 프로토콜 검사 적용
- <u>기술 지원 및 문서 Cisco Systems</u>