# ASA/PIX 7.X:기본 전역 검사 비활성화 및 ASDM을 사용하여 기본이 아닌 애플리케이션 검 사 활성화

## 목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>관련 제품</u> <u>표기 규칙</u> <u>기본 전역 정책</u> <u>기본 애플리케이션 검사 사용</u> <u>다음을 확인합니다.</u> <u>관련 정보</u>

# <u>소개</u>

이 문서에서는 응용 프로그램에 대한 전역 정책에서 기본 검사를 제거하는 방법 및 기본값이 아닌 응용 프로그램에 대해 검사를 활성화하는 방법에 대해 설명합니다.

# <u>사전 요구 사항</u>

#### <u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

#### <u>사용되는 구성 요소</u>

이 문서의 정보는 7.x 소프트웨어 이미지를 실행하는 Cisco ASA(Adaptive Security Appliance)를 기 반으로 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>관련 제품</u>

이 컨피그레이션은 7.x 소프트웨어 이미지를 실행하는 PIX Security Appliance와 함께 사용할 수도 있습니다.

### <u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# <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.)

기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.



# <u>기본 애플리케이션 검사 사용</u>

Cisco ASA에서 기본이 아닌 애플리케이션 검사를 활성화하려면 다음 절차를 완료합니다.

1. ASDM에 로그인합니다.Configuration(컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)로 이동합니다

Ī	Configuration > Firew	all > 9	iervice Poli	cy Rules					
	🗣 Add 🔻 🕼 Edit: 🏦 Delete   🎓 🌾   👗 🖳 📖 🚽 🔍 Find 🕾 Diagram 🔍 Packet Trace								
	Traffic Classification								
	Name	#	Enabled	Match	Source	Destination	Service	Time	RUIE ACCOTS
	🖃 Global; Policy: globa	_policy							
	inspection_default Match		Le Match	🖘 any 🔍 default-inspe				<ul> <li>Inspect DNS Map prese</li> <li>Inspect ESMTP (12 more inspect actions)</li> </ul>	

2. Default Class-map 및 Default Policy-map을 포함하는 전역 정책에 대한 컨피그레이션을 유지 하지만 정책을 전역적으로 제거하려면 Tools > Command Line Interface로 이동하여 no service-policy global-policy 전역 명령을 사용하여 정책을 전역적으로 제거합니다.그런 다음 Send를 클릭하여 명령이 ASA에 적용되도록 합니다

🚰 Command Line Interface		×					
Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.							
💿 Single Line i 🔘 Multiple Line	Enable context sensitive help (?)						
no service-policy global_policy global	×						
Response:							
Result of the command: "no se	rvice-policy global_policy global"						
The command has been sent to t	the device						
	Clear Response	7					
Send	Close Help						

**참고:** 이 단계에서는 ASDM(Adaptive Security Device Manager)에서 전역 정책이 표시되지 않 지만 CLI에 표시됩니다.

3. Add(**추가**)를 클릭하여 다음과 같이 새 정책을 추가합니다

Configuration > Firewall > Service Policy Rules								
💠 Add 🔸 🗃 Edit 🍿 Delete   🎓 🌾   🕉 ங 🏨 🛩   🔍 Find 🖼 Diagram 🐙 Packet Trace								
Traffic Classificat	Traffic Classification							
Name	# Enabled Match Source	Destination Service	Time	RUIB ACCONS				

 Interface 옆의 라디오 버튼이 선택되어 있는지 확인하고 드롭다운 메뉴에서 정책을 적용할 인 터페이스를 선택합니다.그런 다음 정책 이름과 설명을 입력합니다.Next(다음)를 클릭합니다

🖆 Add S	Service P	Policy Rule Wizard - Service Policy	ł		×				
Adding a new service policy rule requires three steps: Step 1: Configure a service policy. Step 2: Configure the traffic classification criteria for the service policy rule. Step 3: Configure actions on the traffic classified by the service policy rule. Create a Service Policy and Apply To: Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add rule into the existing service policy. Otherwise, you can create a new service policy.									
<ol> <li>Int</li> </ol>	erface:	outside - (create new service policy)							
Pol	icy Name:	outside-policy							
De	scription:	Policy on outside interface							
🔾 Gk	obal - appli	es to all interfaces							
Pol	icy Name:	global-policy							
De	scription:								
				< Back Next > Cancel He	P				

5. HTTP가 TCP에 속하는 TCP 트래픽과 매칭할 새 클래스 맵을 만듭니다.Next(다음)를 클릭합 니다

🖆 Add Service Policy Rule	Wizard - Traffic Classification Criteria	×
• Create a new traffic class:	outside-class	
Description (optional):		
Traffic Match Criteria		
Default Inspection Tra	ffic	
Source and Destination	n IP Address (uses ACL)	
Tunnel Group		
CP or UDP Destinatio	n Port	
RTP Range		
IP DiffServ CodePoints	s (DSCP)	
IP Precedence		
Any traffic	h?	
O Use an existing traffic class:	inspection_default	
🔘 Use class-default as the traf	fic dass.	
If traffic does not match a ex situation.	xisting traffic class, then it will match the class-default traffic class. Class-default can be used in catch a	ill
	< Back Next > Cancel He	łp.

### 6. TCP**를** 프로토콜로 선택합니다

🖆 Add Service Policy Rule Wizard - Traffic Match - Destination Port	
Protocol:  UDP Service: To specify port range for the service, use nnn-nnn hormat.	
< Back Next > Cance	Help

HTTP 포트 80을 서비스로 선택하고 OK를 클릭합니다

C	Browse Service						
	💠 Add 👻 📝 Edit		0.				
	Filter:		~				Filter Clear
	Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
							~
	👓 🚥 aol	tcp	default (1-65535)	5190			
	👓 🏧 bgp	tcp	default (1-65535)	179			
	- 🚾 chargen	tcp	default (1-65535)	19			
	😳 cifs	tcp	default (1-65535)	3020			_
	👓 💶 citrix-ica	tcp	default (1-65535)	1494			
	🚾 ctiqbe	tcp	default (1-65535)	2748			
	👓 🚾 daytime	tcp	default (1-65535)	13			
	😳 discard	tcp	default (1-65535)	9			
	tomain	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			
	- 10 gopher	tcp	default (1-65535)	70			
	100 h323	tcp	default (1-65535)	1720			
	- 100 hostname	tcp	default (1-65535)	101			
	- 😰 http	tcp	default (1-65535)	80			
	🗠 🚾 https	tcp	default (1-65535)	443			
	···· <b>10</b> > ident	tcp	default (1-65535)	113			~
1	Selected Service						
	Service -> to	:p/http					
						ОК	Cancel

7. **HTTP를 선택하고** Finish(**마침**)를 클릭합니다

rotocol Inspection	Intrusion Prevention	Connection Settings QoS	
CTIORE			
DCERPC	Configure		
DNS	Configure		
ESMTP	Configure		
FTP	Configure		
🔲 H.323 H.225	Configure		
🔄 H.323 RAS	Configure		
HTTP HTTP	Configure		
ICMP		42	
ICMP Error			
ILS 📃			
MI 🔄	Configure	<u></u>	
IPSec-Pass-T	hru Configure		
MGCP	Configure		
NETBIOS	Configure		
PPTP			
RSH			
RTSP	Configure		
SCCP (Skinny	() Configure		
		Seck	Einish Cancel Hr

8. Apply(**적용)**를 클릭하여 ASDM에서 ASA로 컨피그레이션 변경 사항을 전송합니다.이렇게 하 면 컨피그레이션이 완료됩니다

Configuration > Size	mall > Comico I	alieu Dulas						-			
coninquiration > Fire											
🌵 Add 🔻 🗹 Edit 📋 Delete   🛧 🔸   👗 🎼 🔳 🗸 Y 🔍 Find 🔄 Diagram 🔍 Packet Trace											
Traffic Classification	Traffic Classification										
Name	ame # Enabled Match Source Destination Service Time										
□ Interface: outside;	; Policy: outside-po	olicy									
outside-class		Match	🍫 any	🆘 any	10 http		Inspect HTTP				
6								X			
						_					
			Apply	Reset							
			Hppy	L Kesel							

<u>다음을 확인합니다.</u>

다음 show 명령을 사용하여 컨피그레이션을 확인합니다.

```
• 구성된 클래스 맵을 보려면 show run class-map 명령을 사용합니다.
 ciscoasa# sh run class-map
 1
 class-map inspection_default
 match default-inspection-traffic
 class-map outside-class
 match port tcp eq www
• 구성된 정책 맵을 보려면 show run policy-map 명령을 사용합니다.
 ciscoasa# sh run policy-map
 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
 policy-map outside-policy
  description Policy on outside interface
  class outside-class
   inspect http
 Т
• 구성된 서비스 정책을 보려면 show run service-policy 명령을 사용합니다.
 ciscoasa# sh run service-policy
 service-policy outside-policy interface outside
```

# <u>관련 정보</u>

- <u>Cisco ASA 5500 Series Adaptive Security Appliance</u>
- <u>Cisco ASA 5500 Series 명령 참조</u>
- <u>Cisco ASDM(Adaptive Security Device Manager) 지원 페이지</u>
- <u>Cisco PIX 방화벽 소프트웨어</u>
- <u>RFC(Request for Comments)</u>
- Cisco PIX 500 Series 보안 어플라이언스
- <u>애플리케이션 레이어 프로토콜 검사 적용</u>
- Cisco Secure PIX Firewall 명령 참조
- <u>기술 지원 및 문서 Cisco Systems</u>