외부 Syslog 서버에 경고를 전송하도록 FireSIGHT 시스템 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>침입 알림 전송</u> <u>상태 알림 전송</u> <u>1부: Syslog 경고 생성</u> <u>2부: 상태 모니터 알림 생성</u> 영향 플래그 전송, 이벤트 및 악성코드 알림 검색

소개

FireSIGHT System은 웹 인터페이스 내에서 다양한 이벤트 보기를 제공하지만, 중요한 시스템을 지 속적으로 모니터링할 수 있도록 외부 이벤트 알림을 구성할 수 있습니다. 다음 중 하나가 생성될 때 이메일, SNMP 트랩 또는 syslog를 통해 알림을 생성하도록 FireSIGHT 시스템을 구성할 수 있습니 다. 이 문서에서는 외부 Syslog 서버에서 알림을 전송하도록 FireSIGHT Management Center를 구 성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Syslog 및 FireSIGHT Management Center에 대한 지식이 있는 것이 좋습니다. 또한 방화벽에서 syslog 포트(기본값 514)를 허용해야 합니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 5.2 이상을 기반으로 합니다.

주의: 이 문서의 정보는 특정 랩 환경의 어플라이언스에서 작성되며, 지워진(기본) 컨피그레이 션으로 시작됩니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙 지하시기 바랍니다.

침입 알림 전송

- 1. FireSIGHT Management Center의 웹 사용자 인터페이스에 로그인합니다.
- 2. Policies > Intrusion > Intrusion Policy로 이동합니다.
- 3. 적용할 정책 옆에 있는 편집을 클릭합니다.

4. 고급 설정을 **클릭합니다**.

5. 목록에서 Syslog Alerting(Syslog 알림)을 찾아 Enabled(활성화됨)로 설정합니다.

Overview Analysis Policie	es Devices Objects FireAMP		Health	System Help 🔻	admin 🔻
Access Control Intrusion > In	ntrusion Policy Network Discovery	Application Detectors F	Files Users	Correlation A	ctions •
Edit Policy					
Policy Information	Advanced Settings				< Back
Variables	Verformance Settings				A
Rules	Event Over Configuration		0	A Edit	
FireSIGHT Recommendations	Event Queue Connguration	Enabled	O Disabled	Edic	
 Advanced Settings 	Latency-Based Packet Handling	Enabled	Disabled		
Policy Layers		0.0.0.0			
	Latency-Based Rule Handling	O Enabled	Disabled		
	Performance Statistics Configuration	Enabled	Disabled	🥜 Edit	
	Regular Expression Limits	Enabled	O Disabled	🥜 Edit	
	Rule Processing Configuration	Enabled	O Disabled	🥜 Edit	
	💯 External Responses				0
	SNMP Alerting	O Enabled	Disabled		
	Syslog Alerting	Enabled	O Disabled	🥜 Edit	

- 6. Syslog **알림**의 오른쪽 옆에 있는 **Edit를 클릭합니다**.
- 7. Logging Hosts 필드에 syslog 서버의 IP **주소를** 입력합니다.

8. 드롭다운 **메뉴**에서 적절한 기능 및 **심각도**를 선택합니다. 특정 기능 또는 심각도에 대한 알림을 허용하도록 syslog 서버를 구성하지 않는 한 이 값은 기본값으로 둘 수 있습니다.

Overview Analysis Policies	Devices Objects FireAMP		Health S	System Help	r admin v
Access Control Intrusion > Intr	rusion Policy Network Discovery	Application Detectors Files	Users C	Correlation	Actions 🔻
Edit Policy					
Policy Information	Syslog Alerting				< Back
Variables	Settings				
Rules		(Classic ID a delegar as		a the of Hank's	
FireSIGHT Recommendations	Logging Hosts	(single in address or	comma-separa	ated list)	
Advanced Settings	Facility AUTH V				
Back Orifice Detection	Priority EMERG V				
Checksum Verification					
DCE/RPC Configuration		Revert to Defaults			
DNS Configuration					
Event Queue Configuratio					
FTP and Telnet Configurat					
Global Rule Thresholding					
GTP Command Channel Co					

9. 이 화면의 왼쪽 상단 근처에 있는 정책 정보를 클릭합니다.

10. 변경사항 커밋 버튼을 클릭합니다.

11. 침입 정책을 다시 적용합니다.

참고: 경고를 생성하려면 액세스 제어 규칙에서 이 침입 정책을 사용합니다. 구성된 액세스 제어 규칙이 없는 경우 이 침입 정책을 액세스 제어 정책의 기본 작업으로 사용하도록 설정하 고 액세스 제어 정책을 다시 적용합니다.

이제 해당 정책에서 침입 이벤트가 트리거되면 침입 정책에 구성된 syslog 서버에도 알림이 전송됩니다.

상태 알림 전송

1부: Syslog 경고 생성

1. FireSIGHT Management Center의 웹 사용자 인터페이스에 로그인합니다.

2. 정책 > 조치 > 경고로 이동합니다.

Overview	Analysi	S Polici	es De	vices (Objects	F	ireAMP			Heal	th	System	Help 🔻	admin 🔻
Access Con	trol Int	rusion •	Files	Netwo	rk Discov	ery	Applica	tion Detectors	Us	ers (Corre	lation	Actions	Alerts
				Polici	es Rule E	ditor	White List	Traffic Profiles	Alerts	Remedia	tions	Groups	Health Mor	itor Alerts
Alerts Impact Flag Alerts Discover				overy Ev	ery Event Alerts Advanced Malware Protect			rotecti	ion Aler	ts				
												0	Create Aler	t •
Name									Тур	ю	In	Use	Enabled	

3. 웹 인터페이스의 오른쪽에 있는 경보 생성을 선택합니다.



4. Create Syslog Alert를 클릭합니다. 구성 팝업 창이 나타납니다.

5. 경고문의 이름을 입력합니다.

- 6. 호스트 필드에 syslog 서버의 IP 주소를 입력합니다.
- 7. syslog 서버에서 필요한 경우 포트를 변경합니다(기본 포트는 514).

8. 적절한 시설과 **심각도를 선택합니다**.

reate Sys	log Alert Configuration	?
Name		
Host		
Port	514	
Facility	ALERT	:
Severity	ALERT	;
Tag		
	Sav	Cancel

9. 저장 버튼을 클릭합니다. Policies > Actions > Alerts 페이지로 돌아갑니다.



10. Syslog 구성을 활성화합니다.

2부: 상태 모니터 알림 생성

다음 지침은 방금 생성한 syslog **알림**을 사용하는 Health Monitor Alerts를 구성하는 단계에 대해 설 명합니다(이전 섹션).

1. Policies > Actions > Alerts 페이지로 이동하여 페이지의 상단 근처에 있는 Health Monitor Alerts를 선택합니다.

Overview	Analysis	Policies	Devic	es Ob	jects	FireAMP			Health	S	ystem	Help 🔻	admin 🔻
Access Con	trol Intru	sion • I	Files 1	Network	Discovery	Applica	tion Detectors	Us	ers Co	rrela	ation	Action	s + Alerts
				Policies	Rule Editor	White List	Traffic Profiles	Alerts	Remediatio	ons (Groups	Health Mo	nitor Alerts
Alerts Impact Flag Alerts Discovery Event Alerts					Advance	ed Malware P	rotect	ion Alerts					
											٥	Create Ale	ert •
Name						Тур	e i	In Us	se	Enabled			

2. 상태 알림의 이름을 지정합니다.

3. 심각도를 **선택합니다**(Ctrl 키를 누른 채 클릭하면 둘 이상의 심각도 유형을 선택할 수 있음).

4. Module(모듈) 열에서 syslog 서버에 경고를 보낼 상태 모듈(예: Disk Usage)을 선택합니다.

5. 경고 열에서 이전에 생성한 syslog 경고를 선택합니다.

6. 저장 버튼을 클릭합니다.

영향 플래그 전송, 이벤트 및 악성코드 알림 검색

특정 영향 플래그, 특정 유형의 검색 이벤트 및 악성코드 이벤트가 포함된 이벤트에 대한 syslog 알 림을 전송하도록 FireSIGHT Management Center를 구성할 수도 있습니다. 그러기 위해서는 <u>1부</u>가 <u>필요합니다. Syslog 경고</u>를 생성한 다음 syslog 서버로 전송할 이벤트 유형을 구성합니다. Policies(정책) > Actions(작업) > Alerts(알림) 페이지로 이동한 다음 원하는 알림 유형에 대한 탭을 선택하면 됩니다.

Overview	Ana	lysis P	olicies	Devices	Objects	Fir	eAMP			Health	System	Help 🔻	admin 🔻
Access Co	ntrol	Intrusio	n.▼ Fi	les Net	work Disco	very	Applicat	tion Detectors	Us	ers Co	rrelation	Actions	Alerts
				Po	licies Rule	Editor V	White List	Traffic Profiles	Alerts	Remediatio	ons Groups	Health Mon	itor Alerts
Alerts	Alerts Impact Flag Alerts Disco			Discovery	overy Event Alerts Advanced Malware Pr			rotecti	ion Alerts				
											0	Create Aler	t •
Name									Тур	ю	In Use	Enabled	

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.