配置FireSIGHT系统以将警报发送到外部系统日志 服务器

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>发送入侵警报</u> <u>发送运行状况警报</u> <u>第1部分: 创建系统日志警报</u> <u>第2部分: 创建运行状况监视器警报</u> 发送影响标志、发现事件和恶意软件警报

简介

虽然FireSIGHT系统在其网络界面内提供各种事件视图,但您可能要配置外部事件通知以促进对关 键系统的持续监控。您可以将FireSIGHT系统配置为生成警报,在生成以下内容之一时通过邮件、 SNMP陷阱或系统日志通知您。本文介绍如何配置FireSIGHT管理中心以在外部系统日志服务器上 发送警报。

先决条件

要求

Cisco建议您了解系统日志和FireSIGHT管理中心的相关知识。此外,防火墙中必须允许系统日志端 口(默认值为514)。

使用的组件

本文档中的信息基于软件版本5.2或更高版本。

警告:本文档中的信息是从特定实验环境中的设备创建的,并以清除(默认)配置开头。如果 您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

发送入侵警报

1.登录到FireSIGHT管理中心的Web用户界面。

2.导航到Policies > Intrusion > Intrusion Policy。

3.点击要应用的策略旁边的Edit。

4.单击Advanced Settings。

5.在列表中找到Syslog Alerting并将其设置为Enabled。

Overview Analysis Policie	es Devices Objects FireAMP	Healt	h System Help 🔻 admin 🔻
Access Control Intrusion > In	ntrusion Policy Network Discovery	Application Detectors Files Users	Correlation Actions •
Edit Policy			
Policy Information	Advanced Settings		< Back
Variables	Verformance Settings		•
Rules	Event Queue Configuration		A Edit
FireSIGHT Recommendations	Event Queue Contiguration	Enabled O Disabled	euic
 Advanced Settings 	Latency-Based Packet Handling	Enabled Disabled	
Policy Layers			
	Latency-Based Rule Handling	Enabled Disabled	
	Performance Statistics Configuration	Enabled Disabled	🥔 Edit
	Regular Expression Limits	Enabled Oisabled	🥔 Edit
	Rule Processing Configuration	Enabled Oisabled	🥜 Edit
	👺 External Responses		0
	SNMP Alerting	🗌 Enabled 🛛 🙆 Disabled	=
	Syslog Alerting	Enabled Oisabled	🥔 Edit 🗸

6.单击Syslog Alerting右侧的Edit。

7.在Logging Hosts字段中键入系统日志服务器的IP地址。

8.从下拉菜单中选择相应的Facility和Severity。 这些值可以保留为默认值,除非系统日志服务器配 置为接受特定设施或严重性的警报。

Overview Analysis Policies	Devices Objects FireAMP		Health	System Help	• ▼ admin ▼
Access Control Intrusion > Int	rusion Policy Network Discovery	Application Detectors Files	Users	Correlation	Actions •
Edit Policy					
Policy Information	Syslog Alerting				< Back
Variables	Settings				
Rules	Lessing Vecto	(Cingle ID address or		a rate d list)	
FireSIGHT Recommendations	Logging Hosts	(single iP address or	comma-sep	arated 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 Ce					

9.单击此屏幕左上角附近的Policy Information。

10.单击Commit Changes按钮。

11.重新应用入侵策略。

注意:为了生成警报,请在访问控制规则中使用此入侵策略。如果未配置访问控制规则,则将此入侵策略设置为用作访问控制策略的默认操作,并重新应用访问控制策略。

现在,如果在该策略上触发入侵事件,系统还会向在入侵策略上配置的系统日志服务器发送警报。

发送运行状况警报

第1部分: 创建系统日志警报

1.登录到FireSIGHT管理中心的Web用户界面。

2.定位至**策略>操作>预警**。

Overview	/ Ana	lysis	Policie	es De	vices (Objects	F	ireAMP			Hea	alth	System	Help 🔻	admin 🔻
Access Control Intrusion • F		Files	Files Network Discovery			Application Detectors			Users Cor		lation	Actions + Alert			
					Polici	es Rule I	Editor	White List	Traffic Profiles	Alerts	Remedi	iations	Groups	Health Mor	nitor Alerts
Alerts Impact Flag Alerts Discovery Event Alerts						Advanced Malware Protection Alerts									
													0	Create Ale	t •
Name										Тур	pe	In	Use	Enabled	

3.选择Web界面右侧的Create Alert。



4.单击Create Syslog Alert。系统将显示配置弹出窗口。

5.提供预警的名称。

6.在**主机**字段中填写系统日志服务器的IP地址。

7.如果需要,请更改系统日志服务器的端口(默认端口为514)。

8.选择适当的**设施**和严重性。

reate Sys	log Alert Configuration	?
Name		
Host		
Port	514	
Facility	ALERT	*
Severity	ALERT	\$
Tag		
	Sav	Cancel

9.单击**保存**按钮。您将返回Policies > Actions > Alerts页。

10.启用系统日志配置。



第2部分: 创建运行状况监视器警报

以下说明介绍了使用您刚刚创建的syslog警报(在上一节中)配置运行状况监控警报的步骤:

1.转到**策略>操作>警报**页,然后选择**运行状况监控器警报**,该页位于页面顶部。

Overview	rview Analysis Policies Devices Objects F						ireAMP Health S					admin 🔻
Access Control Intrusion • Fi		Files	les Network Discovery		Application Detectors		Use	ers Corr	elation	Actions	Alerts	
				Policies	Rule Editor	White List	Traffic Profiles	Alerts	Remediations	Groups	Health Mon	itor Alerts
Alerts	Impact Fl	ag Alerts	Disco	very Ever	nt Alerts	Advance	ed Malware P	rotectio	on Alerts			
										٢	Create Aler	t •
Name								Туре	e In	Use	Enabled	

2.为运行状况警报命名。

3.选择Severity(按住CTRL键的同时单击可用来选择多个严重性类型)。

4.从Module列中选择要向其发送警报的系统日志服务器的运行状况模块(例如,磁盘使用情况)。

5.从Alerts列中选择以前创建的syslog警报。

6.单击**保存**按钮。

发送影响标志、发现事件和恶意软件警报

您还可以配置FireSIGHT管理中心,以便针对具有特定影响标志、特定类型的发现事件和恶意软件 事件的事件发送系统日志警报。为此,您必须<u>第</u>1部分:<u>创建系统日志</u>警报,然后配置要发送到系统 日志服务器的事件类型。为此,您可以导航到**策略>操作>警报**页面,然后选择所需警报类型的选项 卡。

Overviev	v Analysis	Polici	es Dev	vices Ot	ojects	FireAMP			Hea	ilth :	System	Help 🔻	admin 🔻
Access Control Intrusion •		usion •	Files	Files Network Discovery		Applica	Application Detectors		ers	Correlation		Actions + Aler	
				Policies	Rule Editor	White List	Traffic Profiles	Alerts	Remedia	ations	Groups	Health Mon	itor Alerts
Alerts	erts Impact Flag Alerts Discovery Event Alerts						Advanced Malware Protection Alerts						
											٥	Create Aler	t •
Name								Тур	ю	Int	Use	Enabled	

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。