使用"1秒性能监控器"选项收集性能统计信息

目录

<u>简介</u> <u>1秒性能监控器</u> <u>在5.4版或更高版本上启用</u> <u>在5.4之前的版本上启用</u> <u>相关文档</u>

简介

在运行Sourcefire软件的设备上,您可以配置监控和报告自身性能的基本参数。性能统计信息对于排 除运行Snort的设备上的性能相关问题至关重要。本文档提供使用FireSIGHT管理中心启用此功能的 步骤。

警告:如果您的网络处于活动状态,并且您在生产系统上启用了1秒性能,则可能会影响网络 性能。仅当思科技术支持出于故障排除目的而请求时,才应启用此功能。

注意:本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采 用原始(默认)配置。

1秒性能监控器

1秒性能监控器功能允许您通过配置以下内容来指定系统更新设备性能统计信息的间隔:

• 秒数

• 分析的数据包数

自上次性能统计信息更新以来,指定的秒数已过时,系统会验证是否已分析指定数量的数据包。如 果是,系统会更新性能统计信息。否则,系统将等待指定数量的数据包进行分析。

在5.4版或更高版本上启用

步骤1:选择策略>访问控制。系统将显示Access Control Policy页面。

步骤 2: 单击要编辑的访问控制策略旁边的铅笔图标。

步骤 3:选择Advanced 选项卡。系统将显示访问控制策略高级设置页面。

Overview Ana	lysis	Policies	Devi	ces	Objects	AM	þ	
Access Control	Int	rusion v	Files	Ne	twork Discov	very	SSL	

Default Access Control

Enter a description

Rules	Targets	Security Intelligence	HTTP Responses	Advanced
-------	---------	-----------------------	----------------	----------

步骤 4:单击"Performance Settings(性能设置)"旁边的铅笔图标。

Performance Settings	Ø
Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

步骤 5: 在显示的弹出窗口中选择"性能统计"选项卡。修改上述数据包的采样时间或最小数量。

Performance Settings

Pattern Matching Limits	Performance S	tatistics	Regular Expression Limits	Intrusion Event	t Logging Limits	
Sample time (seconds)	30	0				
Minimum number of packets	10	000				
Troubleshooting Options						*
Revert to Defaults				OK	Cancel	

? ×

步骤 6:或者,展开"故障排除选项"部分,并仅在Cisco TAC要求修改这些选项时修改。

步骤7:Click OK.

步骤 8::必须保存并应用访问控制策略,更改才能生效。

在5.4之前的版本上启用

步骤 1:导航至Intrusion Policy页面。登录FireSIGHT管理中心。导航至**Policies > Intrusion >** Intrusion Policy。

步骤 2:编辑要应用的入侵策略。单击 铅笔图标编辑策略。



注意:由于此高级设置的设计,您只能在用作访问控制策略的默认操作的入侵策略中修改此配置。

步骤 3:添加策略层。单击Policy Layers(策略层),然后单击Add Layer。将层命名为"1秒Perfmon"。

	Add Shared Layer Add Layer
Add Layer	? × 🖉 🚑 🛅 🗒
Name 1 Second Perfm	ion 🥒 🚑 🛅 🖥
	OK Cancel

检查左面板中的Policy Layers,并确保新层"1 Second Perfmon"位于*所有其他*层之上。



步骤 4:启用性能统计信息配置。在"**性能设置**"下,选择"性能统计信息配置"旁**的"已启**用"单选**按钮** ,然后单击"编辑"。

Performance Settings		
Event Queue Configuration	 Enabled Disabled 	🥖 Edit
Latency-Based Packet Handling	Enabled Oisabled	🥜 Edit
Latency-Based Rule Handling	 Enabled Disabled 	🥜 Edit
Performance Statistics Configuration	Enabled Disabled	🥜 Edit
Performance Statistics Configuration Regular Expression Limits	 Enabled Disabled Enabled Disabled 	🥜 Edit
Performance Statistics Configuration Regular Expression Limits Rule Processing Configuration	 Enabled Disabled Enabled Disabled Disabled 	EditEditEditEdit

步骤 5: 将默认采样时间修改为1秒, 将最小数据包数修改为100个数据包。

Performance Statistics Configuration				
Settings				
Sample time	1	seconds		
Minimum number of packets	100			

步骤 6:单击左面板中的Policy Information,提交更改,并将更新的策略应用到要分析的设备。

Policy Information 🛕	
Variables	·
Rules	
FireSIGHT Recomm	nendations
Advanced Settings	;

步骤 7: 收集数据后恢复设置。要恢复,只需删除"1秒*性能监*控"策略层。

警告:不要忘记恢复配置。否则,可能会导致性能问题。

相关文档

- 查看入侵事件性能
- 生成入侵事件性能统计信息图