配置Cisco ASA Shun功能以免除虚拟设备

目录

简介

本文档介绍如何配置Cisco ASA以从威胁检测组件中免除虚拟设备。Cisco ASA威胁检测组件对DNS和其他协议执行数据包检测。Umbrella支持建议对以下ASA配置进行更改，以防止此功能与我们的虚拟设备发生冲突：

- 如本文所述，使虚拟设备免于遭受威胁检测“shun”功能。
- 使虚拟设备免受DNS数据包检测，以允许本文所介绍的DNS加密(DNScrypt):Cisco ASA防火墙阻止DNScrypt。

威胁检测“Shun”功能

启用“Shun”功能后，ASA可以完全阻止触发威胁检测规则的源IP地址。有关更多详情，请参阅思科文章：[ASA威胁检测功能和配置](#)。

虚拟设备通常会向Umbrella DNS解析器发送大量的DNS查询。在连接到解析器时出现本地问题（例如临时网络中断/延迟）时，这些查询可能会失败。由于发送的查询数量庞大，即使只有一小部分发生故障，ASA也会避开虚拟设备；这会导致DNS在一段时间内完全中断。

免除虚拟设备

注意：本文中的命令仅作为指导说明，建议您在更改生产环境之前咨询思科专家。

通过CLI:

- 要免除避开设备IP，请运行以下命令： **no shun**

通过ASDM接口：

- 选择Configuration > Firewall > Threat Detection窗格。
- 要免除避开设备IP地址，请在“从规避中排除的网络”字段中输入一个地址。可以输入多个地址或子网，用逗号分隔。

确定设备是否被“避开了”

如果没有执行这些步骤，设备可能会在某些情况下变得“避开”，从而导致DNS中断。

当虚拟设备没有外部连接时，Cisco ASA控制台按以下方式记录事件：

4|2014年6月06日14:00:42|401004:避开的数据包：内部接口上的192.168.1.3 ==> 208.67.222.222
4|2014年6月06日14:00:42|401004:避开的数据包：内部接口上的192.168.1.3 ==> 208.67.222.222

要查看当前规避的IP地址的列表，请在ASA上运行以下命令： **show shun**

要立即清除当前规避的IP地址，请在ASA上运行以下命令： **clear shun**

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）。