通过与Meraki集成的安全访问解决Azure托管的FQDN连接问题

目录

问题

当用户流量通过Meraki路由到思科安全访问时，尽管安全访问日志显示流量为“允许”，但是特定Azure托管的FQDN将无法访问。 此问题主要影响使用非标准端口连接到这些FQDN的RDP连接。

在安全访问门户中按FQDN搜索日志时，仅显示“允许”状态的DNS安全日志。但是，RDP与非标准端口上相同目标的RDP连接失败。当FQDN解析为IP地址且活动搜索使用目标IP时，会泄漏已阻止流量的云防火墙日志。

环境

- 集成Meraki的思科安全访问(SSE)
- 具有本地分流功能的Meraki控制面板
- Azure托管的开发资源需要在非标准端口上进行RDP访问
- 通过Meraki隧道路由流量以实现安全访问

分辨率

即时解决方法

将受影响的FQDN添加到Meraki本地分流规则，以绕过特定目标的安全访问，详情见以下各节。

步骤 1：访问Meraki控制面板

导航到Meraki控制面板并找到本地分流配置部分。

步骤 2：配置本地分流规则

将有问题的FQDN添加到本地分流规则，以绕过安全访问路由。此配置更改会绕过安全访问隧道，将流量直接从Meraki路由到互联网，从而立即恢复受影响用户的访问。

故障排除和分析

步骤 1：按FQDN进行日志分析

使用FQDN搜索安全访问活动日志。这主要显示DNS安全日志，并可显示端口443上Web流量的“允许”状态。

步骤 2：按目标IP进行的日志分析

将FQDN解析为其IP地址，并使用目标IP而不是FQDN搜索活动日志。这将显示显示阻止流量的云防火墙日志，提供实际的流量处置情况。

步骤 3：检验流量

确认仅当流量遵循路径时才出现此问题：用户→用Meraki →隧道→安全访→互联网。测试通过本地分支的旁路解决连接问题。

长期解决方案

观察到的行为被确定为当前安全访问实施中的预期功能。已打开功能请求(FR CSE-I-5543)，以解决与以下内容相关的可视性和功能问题：

- 基于FQDN的日志搜索与基于IP的日志搜索之间的差异
- DNS安全和云防火墙日志之间不一致的流量处置报告
- 提高非标准端口上RDP流量的可见性

原因

此问题源于安全访问在非标准端口上通过RDP访问时，处理和报告Azure托管的FQDN流量的方式存在差异。按FQDN搜索日志时，系统主要显示DNS安全日志，显示Web流量的“允许”状态（通常为端口443）。 但是，非标准端口上的实际RDP流量正在由云防火墙规则处理，这些规则仅在按解析的目标IP地址而不是FQDN搜索时可见。

这会造成可视性差距，管理员在基于FQDN的搜索中看到“允许”流量，而实际RDP连接被防火墙策略阻止，而这些策略仅在基于IP的日志搜索中很明显。该行为当前被视为预期功能，但已提交功能请求以提高不同搜索方法中流量报告的可见性和一致性。

相关内容

- 思科技术支持和下载

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）。