网络中断后的WSA上游代理运行状况检查问题

目录

问题

在长时间的网络中断后，配置为使用FQDN指定的上游代理的思科网络安全设备(WSA)可能无法恢复将流量转发到上游代理并直接发送流量。此问题在WSA在网络中断期间将上游代理标记为“停机”时显现出来，但无法识别上游代理何时再次变为可用，即使网络连接已恢复也是如此。

观察到的具体症状包括：

- 通过FQDN和“故障处理=直接执行”使用上游代理配置WSA
- 影响上游代理和DNS服务器连接的长期网络中断
- 网络恢复后，访问日志不显示DEFAULT_PARENT标记，表示流量继续绕过上游代理
- 一个WSA设备上出现问题，而同一环境中的另一个设备正常运行

环境

- 思科网络安全设备(WSA)S系列
- AsyncOS 14.5.2-011（受影响版本）
- Hardware:S695
- 使用FQDN规范配置的上游代理
- 配置为“直接前往”的故障处理
- 具有L2交换机基础设施的网络环境

分辨率

通过将AsyncOS升级到包含CSCwi13124修复程序的版本，可以解决此问题。已在以下AsyncOS版本中修复了此Bug:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

当前版本的临时解决方法

对于无法立即升级的环境，可通过调整用于检查无响应的上游代理的最大空闲超时来临时缓解问题：

步骤 1：访问CLI并导航至高级代理配置：

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

步骤 2：修改最大空闲超时设置：

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

步骤 3：将默认最大值（86400秒/24小时）减小为较小的值，以缩短运行状况检查之间的时间。

立即恢复方法

如果问题当前影响流量，则下一个命令可以立即恢复上游代理功能：

步骤 1：访问诊断菜单：

```
CLI > diagnostic > PROXY > kick
```

这将重新启动代理进程并恢复正常的上游代理操作。

验证和测试程序

要测试问题是存在还是在升级后已解决，请查看以下步骤：

步骤 1：建立基线监视

监控访问日志和代理日志以确认WSA正在向上游代理发送流量。检验流量是否到达上游代理端。

步骤 2：模拟网络中断

确认到上游代理的正常流量后，断开以下连接：

- WSA到上游代理连接
- WSA到DNS服务器连接

步骤 3：监控器故障检测

检查代理日志和系统日志以了解以下指标：

- 代理日志可以将上游代理显示为“……声明的dead”
- 系统日志可以显示“严重：查询DNS服务器时已达到最大失败次数……"

步骤 4：保持中断状态

如果不重新启动代理进程，请保持步骤2的disconnected状态并继续生成请求约10小时。

步骤 5：恢复连接

约10小时后，恢复步骤2中断开的连接。

步骤 6：监控恢复行为

完成第5步后，无需重新启动代理进程即可监控访问日志和代理日志：

- 在固定系统中：流量恢复流经上游代理，代理日志显示正常运行状态转换

- 在受影响的系统中：访问日志显示流量继续绕过上游代理，并且代理日志不会显示“…… ...已生病，现在正常”或“…… ...已健康，现在已生病”消息

原因

此问题的根本原因是上游代理运行状况检查机制中存在逻辑缺陷。当WSA确定已配置的上游代理为“死机”（无响应）时，它实施指数回退算法，使每次失败后的运行状况检查间隔加倍。此时间间隔最多可以达到24小时（86400秒）。

当上游代理在这些扩展间隔之一期间再次变得可用时，会发生此问题。即使代理已恢复并且正常响应，WSA也不会执行运行状况检查，直到完整配置的时间间隔已过。这可能会导致长达24小时的持续直接流量路由，而不是继续使用上游代理。

此行为会影响WSA配置，其中：

- 上游代理由DNS主机名/FQDN（不是IP地址）指定
- “故障处理”设置为“直接处理”
- 扩展的网络中断会影响上游代理和DNS服务器连接

Cisco Bug ID:CSCwi13124

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）。