安全访问应用协议阻止阻止Internet连接

目录

- 问题
- 环境
- 分辨率
  - 步骤 1：确定阻止规则
  - 步骤 2：修改应用程序设置
  - 步骤 3：应用并验证更改
- 原因
- 相关内容

问题

迁移到Cisco Secure Access后，用户在尝试访问Web服务时遇到了互联网连接被阻止的情况。特定症状包括HTTP流量被安全策略阻止，阻止对合法网站和应用的访问。

阻止事件详细信息显示以下特征：

- 操作：已阻止
- 事件阻止原因：AC_RULE_MATCH_BLOCK
- 目的地：http://www.bing.com/api/shopping/v1/user/shoppingsettings
- 目的端口：443
- 类别：未分类

- 应用类别： 搜索
- 应用程序协议：超文本传输协议
- 协议：TCP

环境

- 思科安全访问部署
- 具有应用协议限制的活动安全策略

分辨率

解决方法涉及修改安全规则配置，以允许HTTP应用协议流量，同时维护真正不受信任的应用的安全状态。

步骤 1：确定阻止规则

在安全访问管理界面中查找导致阻止的特定规则：

- 规则名称:测试
- 当前配置使用应用程序设置块作为目标。

步骤 2：修改应用程序设置

访问规则配置并检查Destination:

- 导航到资源> Internet和SaaS资源>应用列表。然后，点击应用。
- 找到Application Protocol设置。

- 取消选中或从阻止的应用协议列表中删除HTTP。
- 确保为实际不受信任的应用保留其他安全控制。

步骤 3：应用并验证更改

保存规则修改并测试连接：

1. — 将配置更改应用于活动策略。

2. — 测试与之前被阻止的目的地的Internet连接。

3. — 监控安全日志，确保现在允许合法的HTTP流量。

4. — 验证其他安全保护是否仍然有效。

原因

根本原因是思科安全访问中的安全规则配置过于严格。规则配置为阻止所有HTTP应用协议流量，从而阻止合法的Web浏览和应用访问。HTTP协议阻止的广泛应用影响正常的Internet连接，用户访问合法的Web服务和使用HTTP/HTTPS协议的应用。

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）。