

ASA CSC安全服务模块如何作为HTTP数据流的一个代理？

Contents

[Introduction](#)

[ASA CSC安全服务模块如何作为HTTP数据流的一个代理？](#)

[Related Information](#)

Introduction

本文描述Cisco ASA内容安全和控制(CSC)安全服务模块如何能作为HTTP数据流的一个代理服务器。

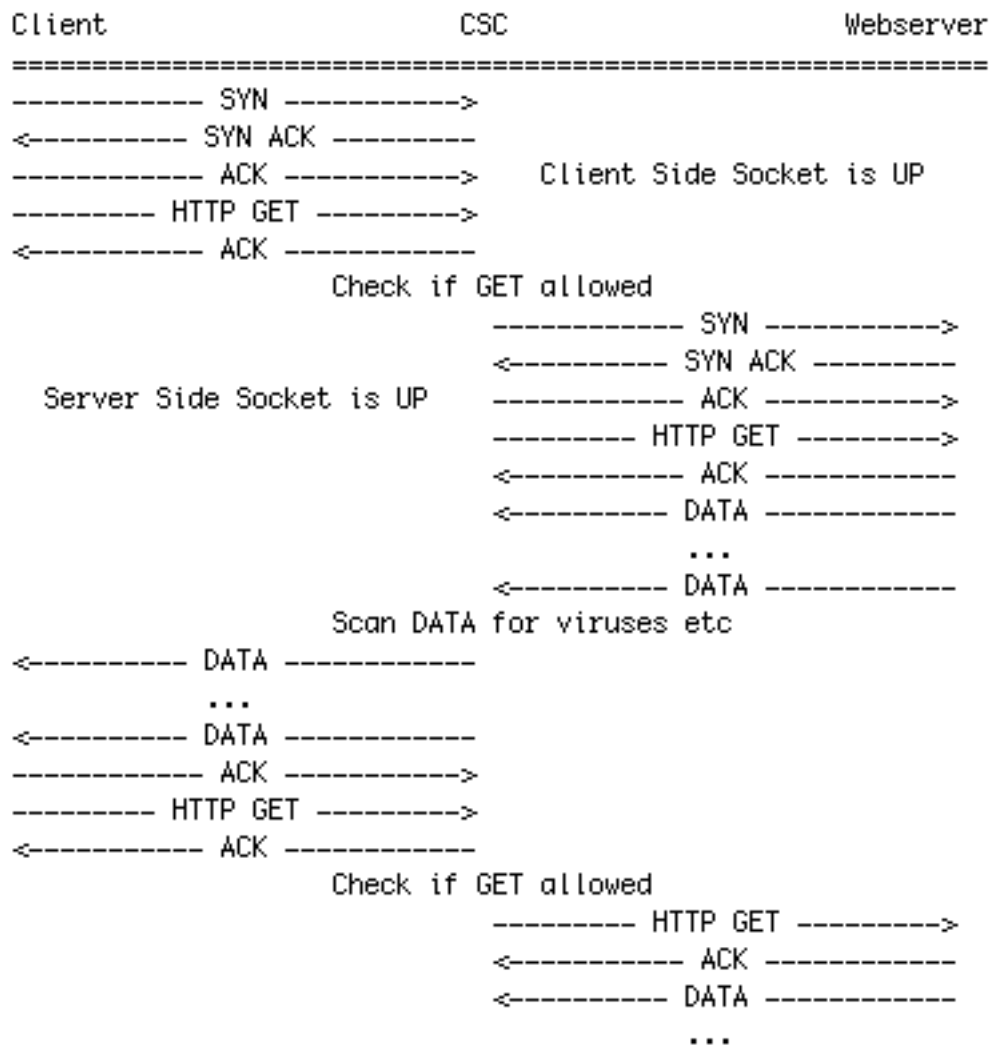
有关文档规则的信息，请参阅 [Cisco 技术提示规则](#)。

Q. ASA CSC安全服务模块如何作为HTTP数据流的代理？

A. 了解在建立HTTP连接涉及的步骤通过CSC模块将帮助您了解其他问题(例如页错误和性能问题)：

1. 当用户设法连接到站点时，他们的浏览器发送一个同步信息包到该站点的IP地址。
2. CSC模块，作为代理，截断同步信息包并且回复以SYN-ACK代表站点。
3. Web浏览器，没有察觉到，CSC模块作为代理，回复以ACK和连接形成在客户端机器和CSC模块HTTP代理引擎之间。**Note:** 前半此连接指客户端插槽(CSS)。
4. 这时，浏览器认为与站点的连接启用和工作，并且发送HTTP GET请求。
5. HTTP GET请求由CSC模块处理;即根据URL阻塞/filtering/WRS设置核对。如果请求允许，CSC模块开始建立与Web服务器的连接在站点。
6. HTTP代理引擎发送一个TCP Syn信息包用IP原地址，并且匹配原始TCP SYN客户端的源端口认为发送了到Web服务器(如被接受在CSS)。Web服务器回复以SYN ACK，并且HTTP代理引擎回应ACK。这时，服务器端的插槽(SSS)是UP。
7. HTTP代理引擎发送客户端的HTTP GET到Web服务器，并且Web服务器回复以内容。
8. 此内容被扫描/被检查。如果它是干净的，内容转发回到客户端。
9. 这些同样步骤为自客户端的其他Web请求被重复所有Web服务器的。

注意客户端浏览器从未确实连接到站点;它连接到CSC假装是站点如此镜像所示的模块：



Related Information

- [Technical Support & Documentation - Cisco Systems](#)