目录

简介

本文描述如何配置Web安全工具(WSA) /Cisco路由器为了支持HTTP、HTTPS和本地FTP流量透明重定向与WEB缓存通信协议(WCCP)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Web运行AsyncOS版本6.0或以上的安全工具
- 在WSA启用的本地FTP代理
- WCCPv2兼容的Cisco路由器/交换机或者ASA防火墙

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

当本地FTP流量重定向透明地对WSA时， WSA典型地收到在标准的FTP端口21的流量。因此，WSA的本地FTP代理在端口21应该侦听(默认情况下本地FTP代理是8021)。在GUI中，请选择**安全服务**>验证的**FTP代理**。

WSA配置

1. 创建FTP流量的一标识。在GUI中，请选择**Web安全经理>标识**并且保证验证为此ID禁用。
2. 创建访问策略。在GUI中，请选择**Web安全经理**>Access**策略，**参考标识step1。

3. 在FTP代理设置下，请修改FTP被动端口是11000-11006为了保证所有端口适合到一单路供电的组。
4. 创建这些WCCP服务ID ：

   名称服务端口
   web-cache 0 80 *(二者择一，您能使用98自定义Web缓存，如果使用多个WSAs)*
   ftp本地60 21,11000,11001,11002,11003,11004,11005,11006
   https缓存70 443

这些示例重定向三内部子网，当他们绕过所有私下寻址的目的地以及单个内部主机的时WCCP重定向。

示例ASA配置

示例交换机配置(c3560)

这在多数路由器应该也是运作。

注意：由于WCCP技术限制，最多八个端口可以每个WCCP服务ID分配。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。