访问安全Web设备日志

目录

简介

先决条件

- 要求
- 使用的组件

SWA日志类型

查看日志

- 通过GUI下载日志文件
- 从CLI查看日志

在安全Web设备上启用FTP

相关内容

简介

本文档介绍查看安全Web设备(SWA)日志的方法。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟SWA。
- 许可证已激活或已安装。
- 安全外壳(SSH)客户端。
- 安装向导已完成。

- 对SWA的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

SWA日志类型

安全Web设备通过将自己的系统和流量管理活动写入日志文件来记录这些活动。管理员可以查阅这些日志文件来监控和排除设备故障。

此表描述安全Web设备日志文件类型。

日志文件类型	描述	是否支持Syslog Push?	默认情况下启用？
访问控制引擎日志	记录与Web代理ACL（访问控制列表）评估引擎相关的消息。	无	无
安全终端引擎日志	记录有关文件信誉扫描和文件分析的信息（安全终端。）	Yes	Yes
审核日志	记录AAA（身份验证、授权和记帐）事件。记录与应用程序和命令行界面的所有用户交互，并捕获已提交的更改。 以下是一些审核日志详细信息： • 用户 — 登录 • 用户 — 登录失败密码不正确 • 用户 — 登录失败未知用户名 • 用户 — 登录失败帐户已过期 • 用户 — 注销 • 用户 — 锁定 • 用户 — 已激活 • 用户 — 密码更改 • 用户 — 密码重置	Yes	Yes

日志文件类型	描述	是否支持Syslog Push?	默认情况下启用？
	• 用户 — 安全设置/配置文件更改 • 用户 — 已创建 • 用户 — 已删除/已修改 • 组/角色 — 删除/修改 • 组/角色 — 权限更改		
访问日志	记录Web代理客户端历史记录。	Yes	Yes
ADC引擎框架日志	记录与Web代理和ADC引擎之间的通信相关的消息。	无	无
ADC引擎日志	记录来自ADC引擎的调试消息。	Yes	Yes
身份验证框架日志	记录身份验证历史记录和消息。	无	Yes
AVC引擎框架日志	记录与Web代理和AVC引擎之间的通信相关的消息。	无	无
AVC引擎日志	记录来自AVC引擎的调试消息。	Yes	Yes
CLI审核日志	记录命令行界面活动的历史审核。	Yes	Yes
配置日志	记录与Web代理配置管理系统相关的消息。	无	无
连接管理日志	记录与Web代理连接管理系统相关的消息。	无	无
数据安全日志	记录由思科数据安全过滤器评估的上传请求的客户端历史记录。	Yes	Yes
数据安全模块日志	记录与思科数据安全过滤器相关的消息。	无	无
DCA引擎框架日志	记录与Web代理和Cisco Web Usage Controls Dynamic Content Analysis引擎之间的通信相关的消息。	无	无

日志文件类型	描述	是否支持Syslog Push?	默认情况下启用？
（动态内容分析）			
DCA引擎日志 （动态内容分析）	记录与思科网络使用控制动态内容分析引擎相关的消息。	Yes	Yes
默认代理日志	记录与Web代理相关的错误。 这是所有与Web代理相关的日志中最基本的。要排除与Web代理相关的更具体问题，请为适用的Web代理模块创建日志订阅。	Yes	Yes
磁盘管理器日志	记录与写入到磁盘上的缓存相关的Web代理消息。	无	无
外部身份验证日志	记录与使用外部身份验证功能相关的消息，例如与外部身份验证服务器的通信成功或失败。 即使禁用了外部身份验证，此日志也包含有关本地用户成功登录或登录失败的消息。	无	Yes
反馈日志	记录报告错误分类页面的Web用户。	Yes	Yes
FTP代理日志	记录与FTP代理相关的错误和警告消息。	无	无
FTP服务器日志	记录使用FTP上传到安全网络设备以及从安全网络设备下载的所有文件。	Yes	Yes
GUI日志 (图形用户界面)	在Web界面中记录页面刷新的历史记录。GUI日志还包含有关SMTP事务的信息，例如有关从设备以电子邮件发送的计划报告的信息。	Yes	Yes
Haystack日志	Haystack日志记录Web事务跟踪数据处理。	Yes	Yes
HTTPS日志	记录特定于HTTPS代理的Web代理消息（启用HTTPS代理时）。	无	无

日志文件类型	描述	是否支持Syslog Push?	默认情况下启用？
ISE服务器日志	记录ISE服务器连接和运行信息。	Yes	Yes
许可证模块日志	记录与Web代理的许可证和功能密钥处理系统相关的消息。	无	无
日志记录框架日志	记录与Web代理的日志记录系统相关的消息。	无	无
日志日志	记录与日志管理相关的错误。	Yes	Yes
McAfee集成框架日志	记录与Web代理和McAfee扫描引擎之间的通信相关的消息。	无	无
McAfee日志	记录来自McAfee扫描引擎的防恶意软件扫描活动的状态。	Yes	Yes
内存管理器日志	记录与管理所有内存（包括Web代理进程的内存缓存）相关的Web代理消息。	无	无
其他代理模块日志	记录开发人员或客户支持最常使用的Web代理消息。	无	无
AnyConnect安全移动后台守护程序日志	记录安全Web设备和AnyConnect客户端之间的交互，包括状态检查。	Yes	Yes
NTP 日志 （网络时间协议）	记录网络时间协议对系统时间所做的更改。	Yes	Yes
PAC文件托管守护程序日志	记录客户端的代理自动配置(PAC)文件使用情况。	Yes	Yes
代理旁路日志	记录绕过Web代理的事务。	无	Yes
报告日志	记录报告生成的历史记录。	Yes	Yes

日志文件类型	描述	是否支持Syslog Push?	默认情况下启用？
报告查询日志	记录与报告生成相关的错误。	Yes	Yes
请求调试日志	从所有Web代理模块日志类型中记录有关特定HTTP事务的非常详细的调试信息。建议创建此日志订阅，以便在不创建所有其他代理日志订阅的情况下，对特定事务的代理问题进行故障排除。 注意：您只能在CLI中创建此日志订阅。	无	无
身份验证日志	记录与访问控制功能相关的消息。	Yes	Yes
SHD日志 （系统运行状况守护程序）	记录系统服务的运行状况历史以及意外守护程序重新启动的历史记录。	Yes	Yes
SNMP日志	记录与SNMP网络管理引擎相关的调试消息。	Yes	Yes
SNMP模块日志	记录与与SNMP监控系统交互相关的Web代理消息。	无	无
Sophos集成框架日志	记录与Web代理和Sophos扫描引擎之间的通信相关的消息。	无	无
Sophos日志	记录来自Sophos扫描引擎的防恶意软件扫描活动的状态。	Yes	Yes
状态日志	记录与系统相关的信息，例如功能密钥下载。	Yes	Yes
系统日志	记录DNS、错误和提交活动。	Yes	Yes
流量监控器错误日志	记录L4TM接口并捕获错误。	Yes	Yes
流量监控器日志	记录添加到L4TM块的站点并允许列表。	无	Yes

日志文件类型	描述	是否支持Syslog Push?	默认情况下启用？
UDS日志 （用户发现服务）	记录有关Web代理如何发现用户名而不执行实际身份验证的数据。它包括有关与安全移动性的思科自适应安全设备交互以及与Novell eDirectory服务器集成以实现透明用户识别的信息。	Yes	Yes
更新程序日志	记录WBRS和其他更新的历史记录。	Yes	Yes
W3C日志	以符合W3C的格式记录Web代理客户端历史记录。 有关详细信息.	Yes	无
WBNP日志 （SensorBase网络参与）	记录Cisco SensorBase网络参与上传到SensorBase网络的历史记录。	无	Yes
WBRS框架日志 （Web声誉得分）	记录与Web代理和Web信誉过滤器之间的通信相关的消息。	无	无
WCCP模块日志	记录与实施WCCP相关的Web代理消息。	无	无
Webcat集成框架日志	记录与Web代理和与Cisco Web使用控制关联的URL过滤引擎之间的通信相关的消息。	无	无
Webroot集成框架日志	记录与Web代理和Webroot扫描引擎之间的通信相关的消息。	无	无
Webroot日志	记录来自Webroot扫描引擎的防恶意软件扫描活动的状态。	Yes	Yes
欢迎页面确认日志	记录点击最终用户确认页面上的Accept（接受）按钮的Web客户端的历史记录。	Yes	Yes

查看日志

默认情况下，日志存储在SWA本地。您可以通过GUI下载本地存储的日志文件，也可以从CLI查看日志。

通过GUI下载日志文件



注意：必须在设备上启用FTP。要启用FTP，请参阅本文中的在安全Web设备上启用FTP。

您可以从GUI下载日志文件：

步骤1.登录GUI。

步骤2.导航到系统管理。

步骤3.选择Log Subscriptions。

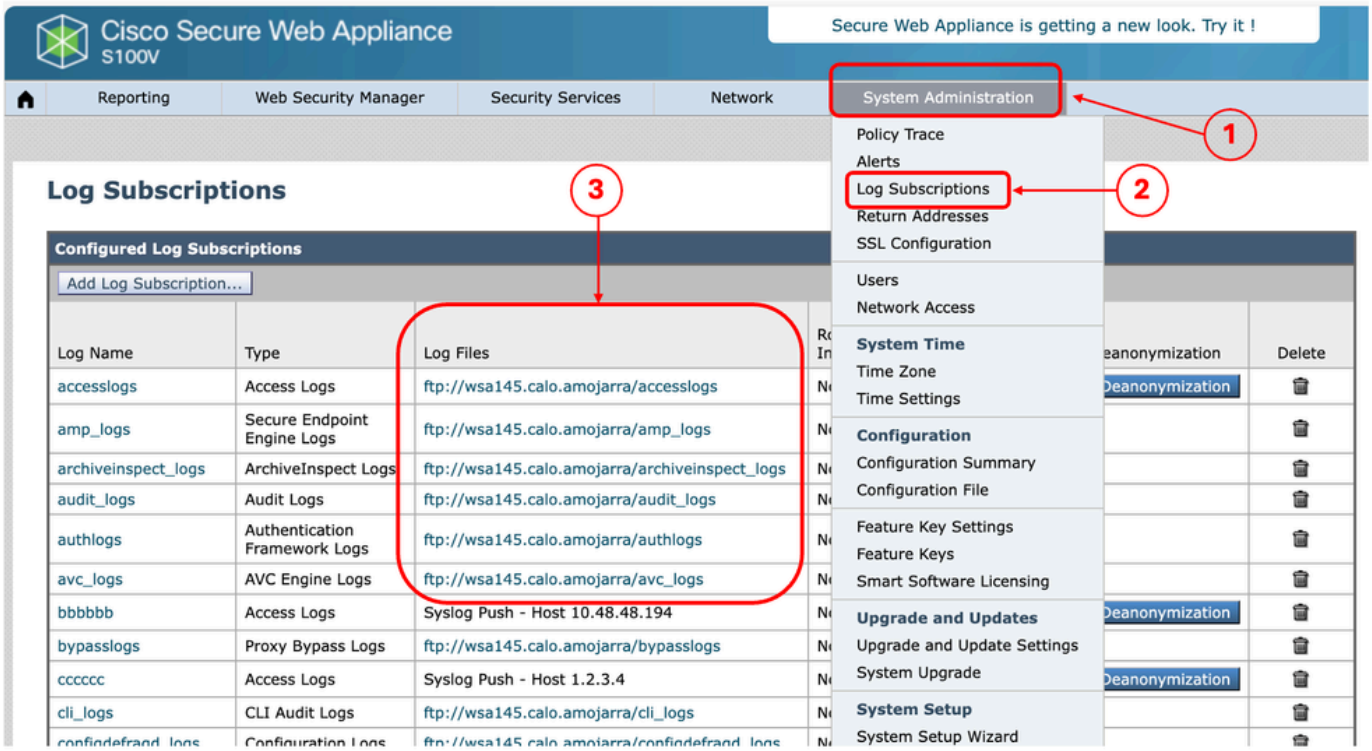
步骤4.在日志订阅列表的Log Files列中单击日志订阅的名称。

步骤5.出现提示时，输入administrators 用户名和密码以访问设备。

步骤6.登录后，单击其中一个日志文件，在浏览器中查看该文件或将其保存到磁盘。



提示：刷新浏览器以获取更新的结果。



映像 — 下载日志文件

注意：如果日志订阅已压缩，请下载、解压缩，然后打开它。

从CLI查看日志

您可以从CLI查看日志。在这种情况下，您可以访问实时日志或过滤日志中的关键字。

步骤1.连接到CLI。

步骤2.键入grep并按Enter。

步骤3.输入要查看的日志编号。

步骤4.（可选）可以通过定义正则表达式或单词来过滤输出，否则，请按Enter。

第 5 步： 如果您需要搜索在步骤4中输入的关键字，则要不区分大小写，请在是否希望此搜索不区分大小写？[Y]>否则键入N并按Enter。

步骤6.如果需要从搜索中排除关键字，请在是否要搜索不匹配的行中键入Y。[N]>否则，按Enter键。

步骤7.如果需要查看实时日志，请在是否要跟踪日志？[N]>否则，请按Enter键。

步骤8.如果要对日志进行分页以按页查看它们，请在是否要对输出进行分页？[N]>，否则按Enter。

 提示：如果选择分页，可以按q.退出日志。

以下输出示例显示了其中包含“警告”的所有行：

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

在安全Web设备上启用FTP

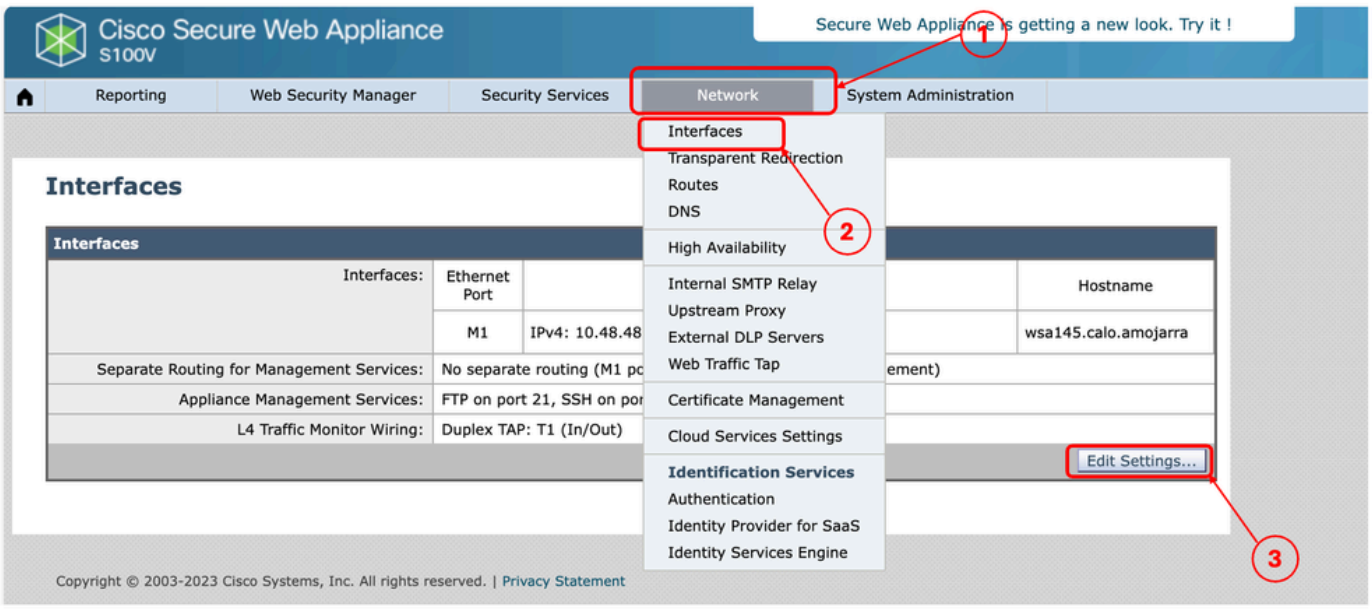
默认情况下，SWA上未启用FTP。要启用FTP:

步骤1.登录GUI。

步骤2.导航到网络。

步骤3.选择接口。

步骤4.单击Edit Settings。

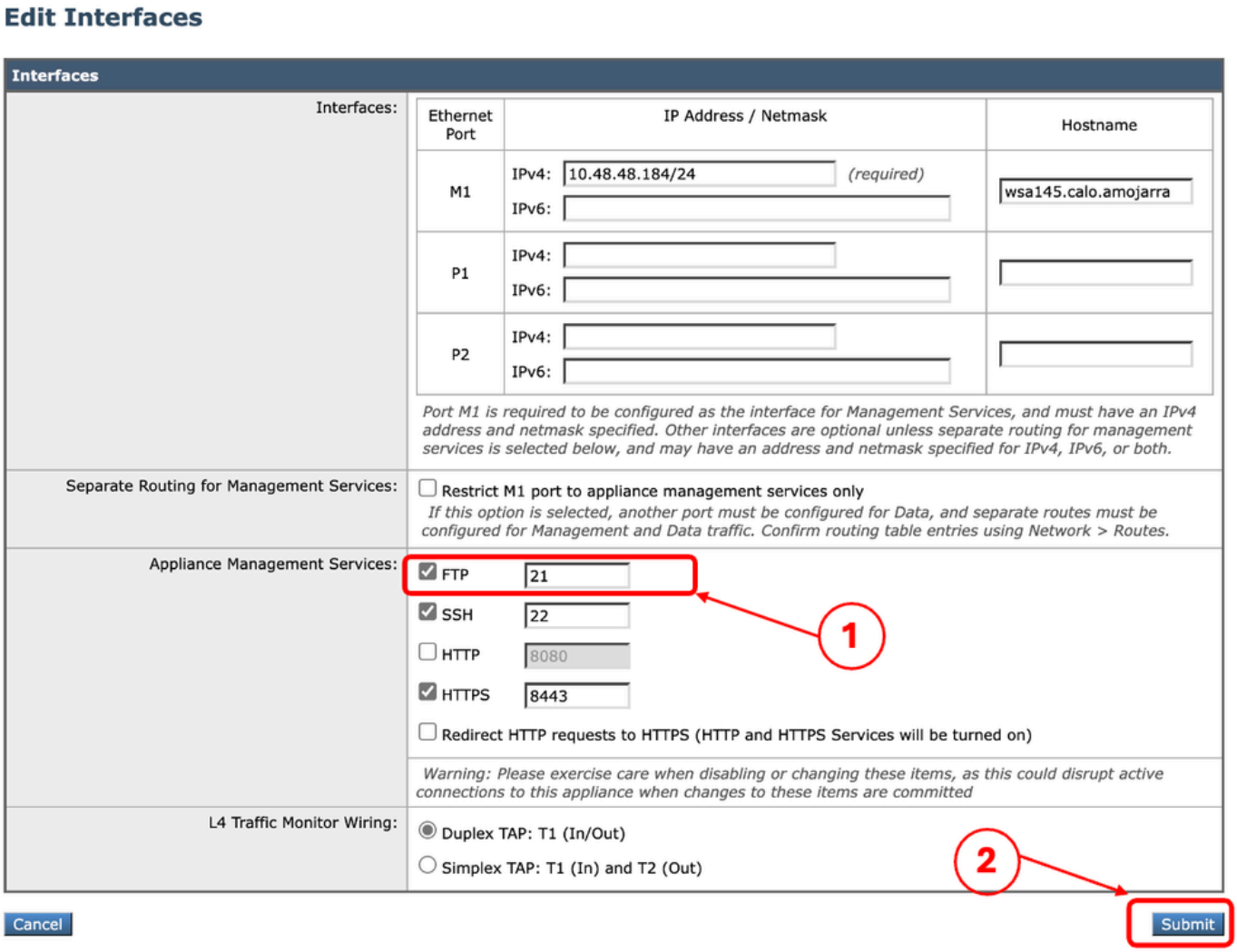


映像 — 在SWA上启用FTP

步骤5.选中FTP复选框。

步骤6.提供FTP的TCP端口号（默认FTP端口为21）。

步骤7.提交并提交更改。



映像 — 在SWA中配置FTP参数

相关内容

- 思科安全网络设备AsyncOS 15.0用户指南 — LD（有限部署） — 故障排除……
- 使用Microsoft Server - Cisco在安全Web设备中配置SCP推送日志

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）。