**ASWG上网安全预检查脚本指导说明**

该脚本使用python编写, 主要目的用户快速检查客户环境是否达到上网安全和数据防泄漏的基本要求。脚本使用包括三部分：配置ASWG及DLP策略、安装wkhtmltopdf工具、运行脚本获取测试结果。测试脚本位于：

[\\file4.skyguardmis.com\GuestUpload\ts-team\zhangguoxin\ASWG\测试工具\aswg.rar](file:///\\\\file4.skyguardmis.com\\GuestUpload\\ts-team\\zhangguoxin\\ASWG\\测试工具\\aswg.rar)

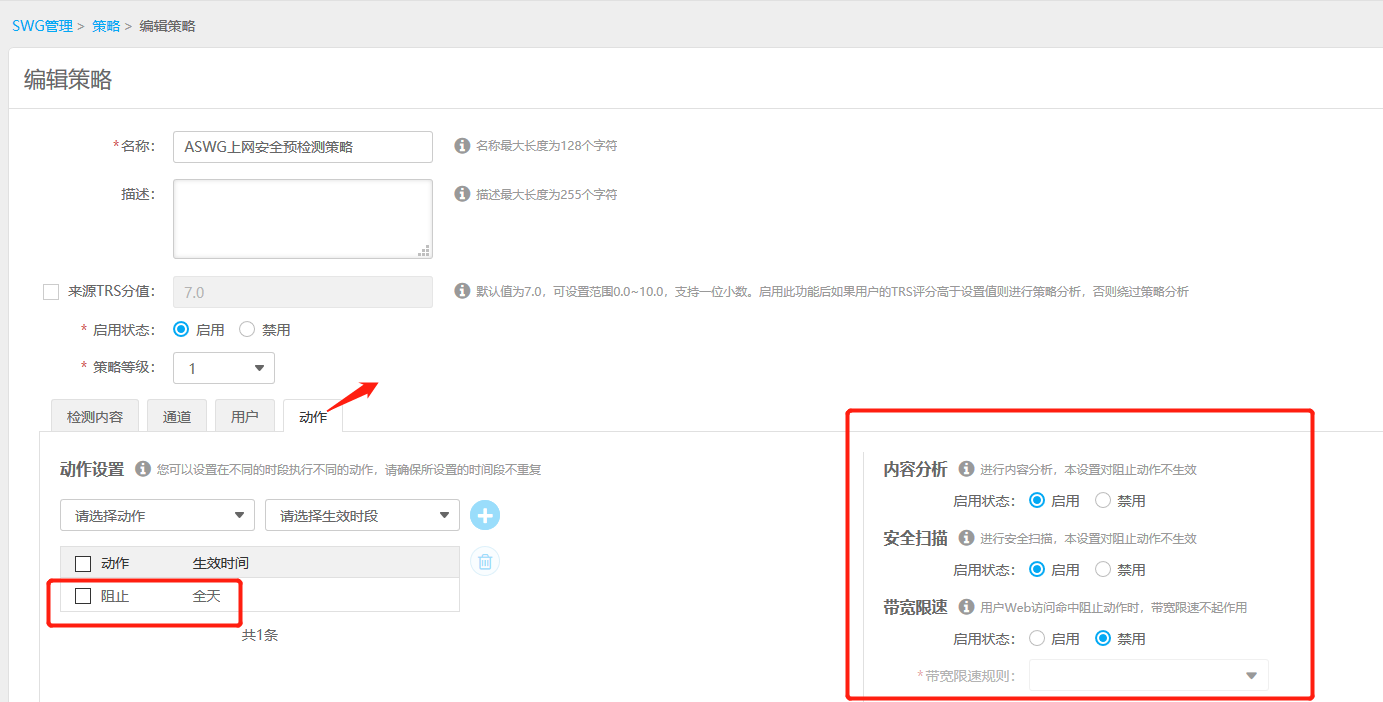
1. **配置ASWG及DLP策略。**
2. 将测试客户端加入ASWG代理免认证。如果客户端集成代理认证，可以忽略此步骤。



1. 添加SWG策略。

配置ASWG URL分类阻断策略，识别不安全的URL：包括恶链、暴力、色情、武器售卖等URL。





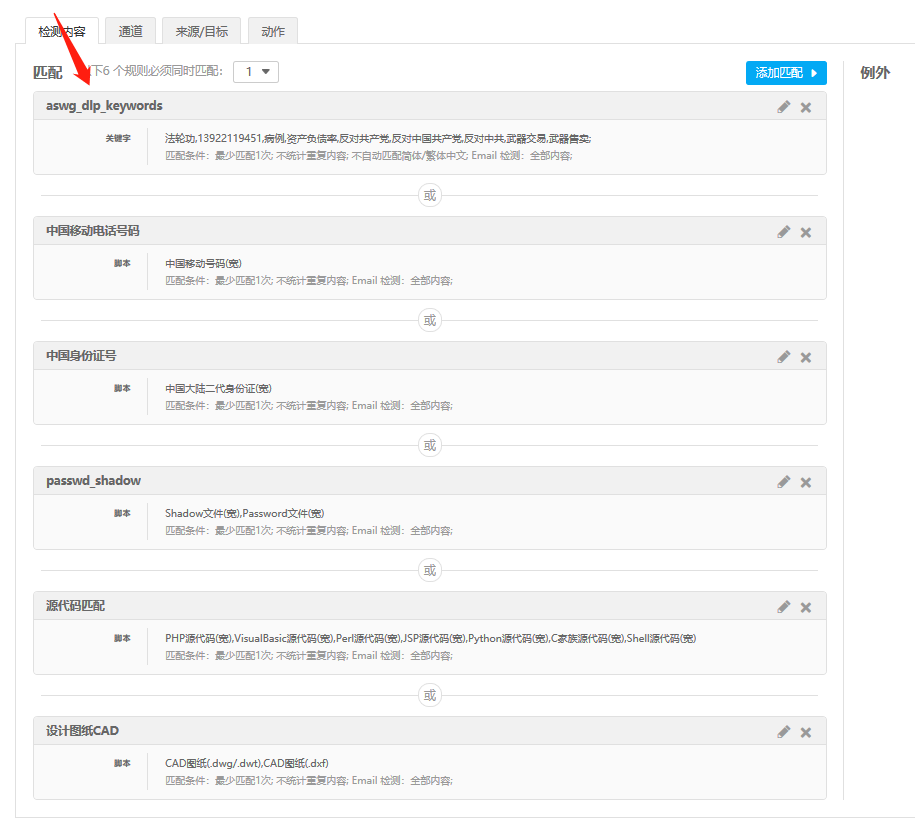
配置ASWG默认策略：全匹配，所有通道，所有用户，动作放行同时勾选“内容分析”（数据防泄漏）和“安全分析”（防病毒/木马等）。



1. 配置DLP检查策略，动作“保护”。



当前测试策略的“检测内容”设置如下：（TODO：后续完善样本文件和测试功能项后再更新DLP策略设置）



1. **在上网测试客户端安装HTML转换为PDF工具： wkhtmltopdf。**

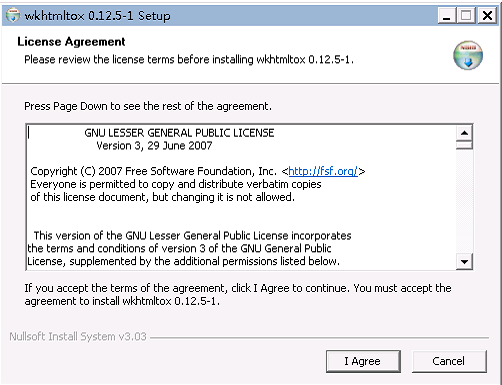
使用默认安装并设置（bin目录）用户环境变量即可。具体步骤如下：（如无需PDF格式报告，可忽略步骤）

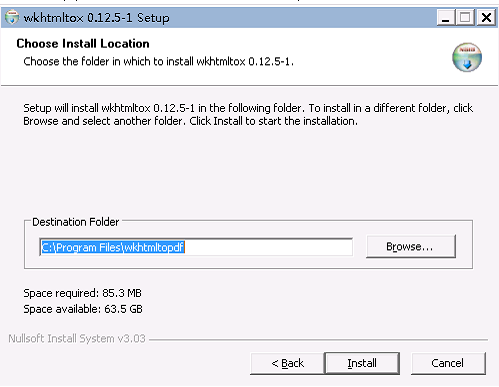
1. 下载wkhtmltopdf: 从压缩包目录直接安装：aswg/static/wkhtmltopdf

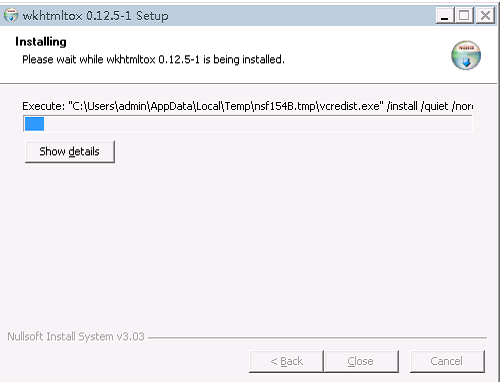
或者登录官网地址下载：

<https://wkhtmltopdf.org/downloads.html>

1. 默认方式安装wkhtmltopdf





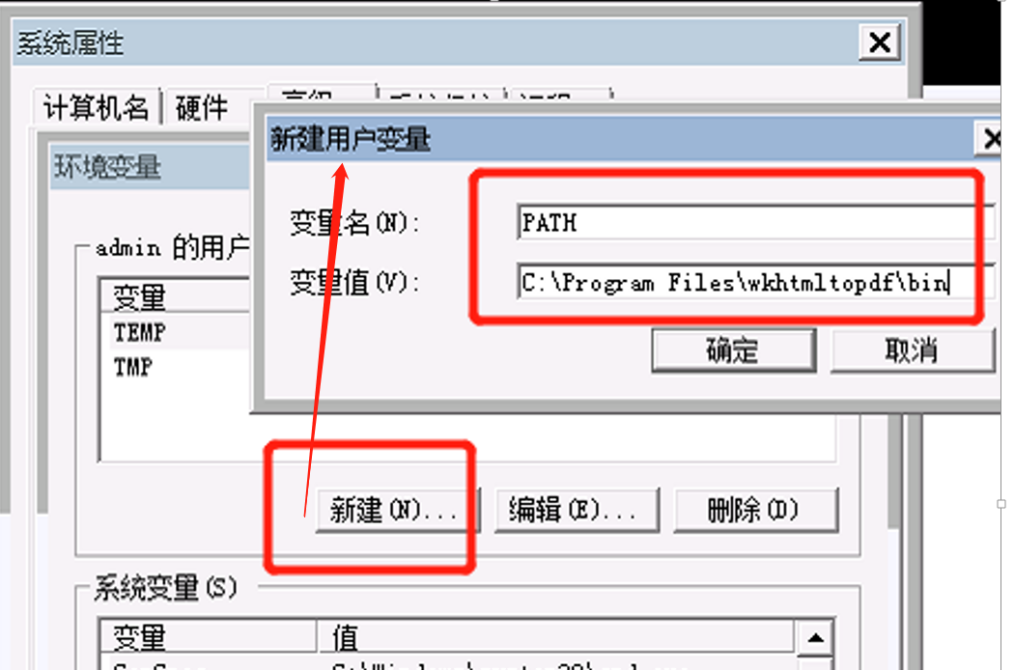


1. 设置bin目录环境变量：

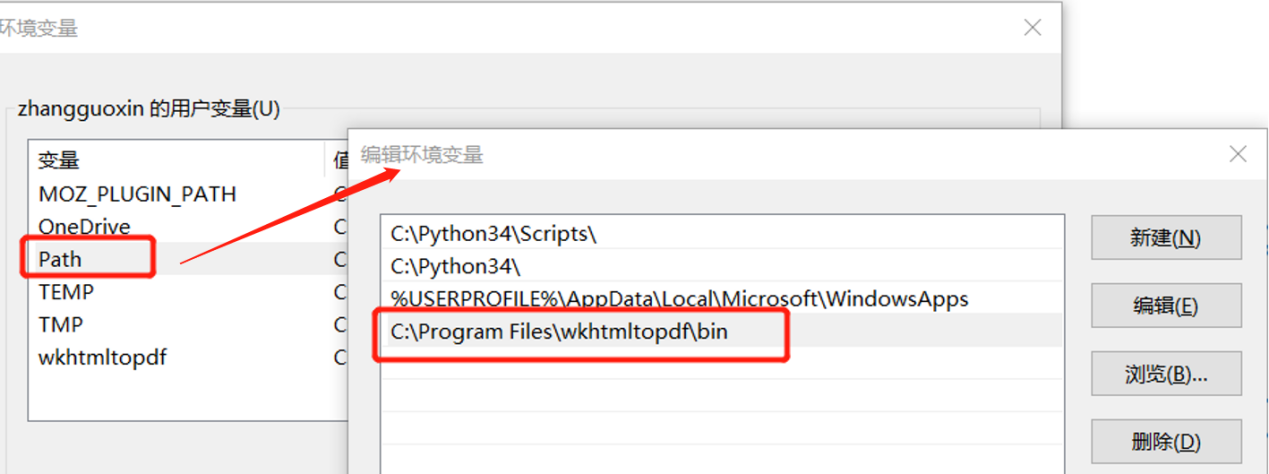
举例说明，如果wkhtmltopdf默认安装路径为：C:\Program Files\wkhtmltopdf

设置环境变量如下：

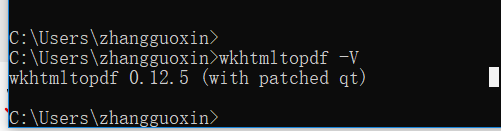
Win7系统 – 我的电脑-属性-高级系统设置-环境变量：



Win10系统设置 - 搜索环境变量 -- 设置用户环境变量- 在PATH变量-添加bin目录： C:\Program Files\wkhtmltopdf\bin



1. 在cmd 下测试： wkhtmltopdf -V， 有输出正确的版本 表明 wkhtmltopdf 安装和设置完成。



1. **脚本运行**
2. 脚本文件和目录说明：



1. doc目录：放置详细说明文档。
2. static目录：包含html模板文件、bootstrap/css文件、图标、swg/dlp样本文件等。
3. result目录：保存脚本运行的结果生成报告，包括html文件和pdf文件。
4. aswg.exe：主程序，用于模拟用户上网行为，触发策略、分析返回结果、生成HTML格式的报告；该程序运行的结果（.html）会保存在result目录。aswg.exe有三种使用方法：

第一种方式-不设置ASWG代理，直接上网：直接双击运行或者在cmd命令下无参数运行。

第二种方式-指定ASWG代理上网（加 <IP:Port> 参数）：aswg.exe 172.18.230.23:8080。

第三种方式-使用默认ASWG代理(使用1作为参数)，默认代理指向华为云的ASWG代理（当前云端服务器是关闭的状态）： aswg.exe 1

1. html2pdf.exe

功能：把result目录下的所有未生成为PDF报告的HTML文件。

使用方法：直接双击或者cmd下无参数运行即可。

注：如有已经同名相同名称的pdf文件时，不会转换该同名的html文件。

1. readme.txt 简单使用说明文件。
2. 其他
3. 把脚本主目录aswg拷贝到Windows上网客户端的某个目录（最好是WIN10系统，win7未测试）；并使用cmd命令进入该目录。
4. 客户端模拟无ASWG代理的情况：直接运行aswg.exe

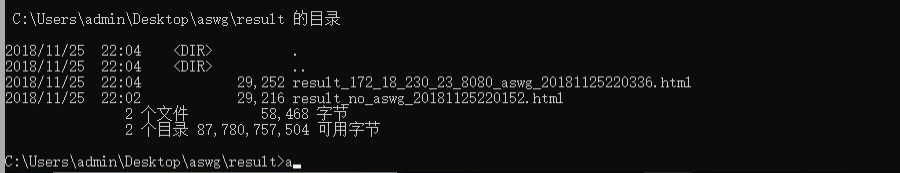


1. 客户端模拟设置ASWG代理上网的情况：

aswg.exe <aswg\_ip:port> (比如：aswg.exe 172.18.230.23:8080)



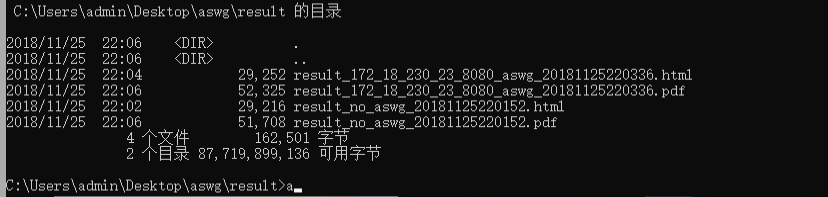
1. 在result目录即可通过浏览器查看上网安全检查结果：html格式。



1. 运行html2pdf.exe，生成pdf格式报告。



查看生成的同名PDF报告：



1. 可登录UCSS查看事件和策略，并进行详细分析。
2. **测试报告示例：（**样本PDF报告见于：aswg/static/report**）**
3. 无ASWG代理，直接上网报告。



1. ASWG代理上网报告。



1. **Todo**