确定SWA中的解密速率

目录

简介

先决条件

- 要求
- 使用的组件

解密性能影响

计算解密百分比的步骤

- 来自CLI的整体流量统计信息

简介

本文档介绍用于计算安全网络设备(SWA)（以前称为WSA）中解密流量的百分比的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟安全网络设备(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的管理权限。

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。

解密性能影响

在SWA执行的所有服务中，从性能角度来看，对超文本传输协议安全(HTTPS)流量的评估最为重要。

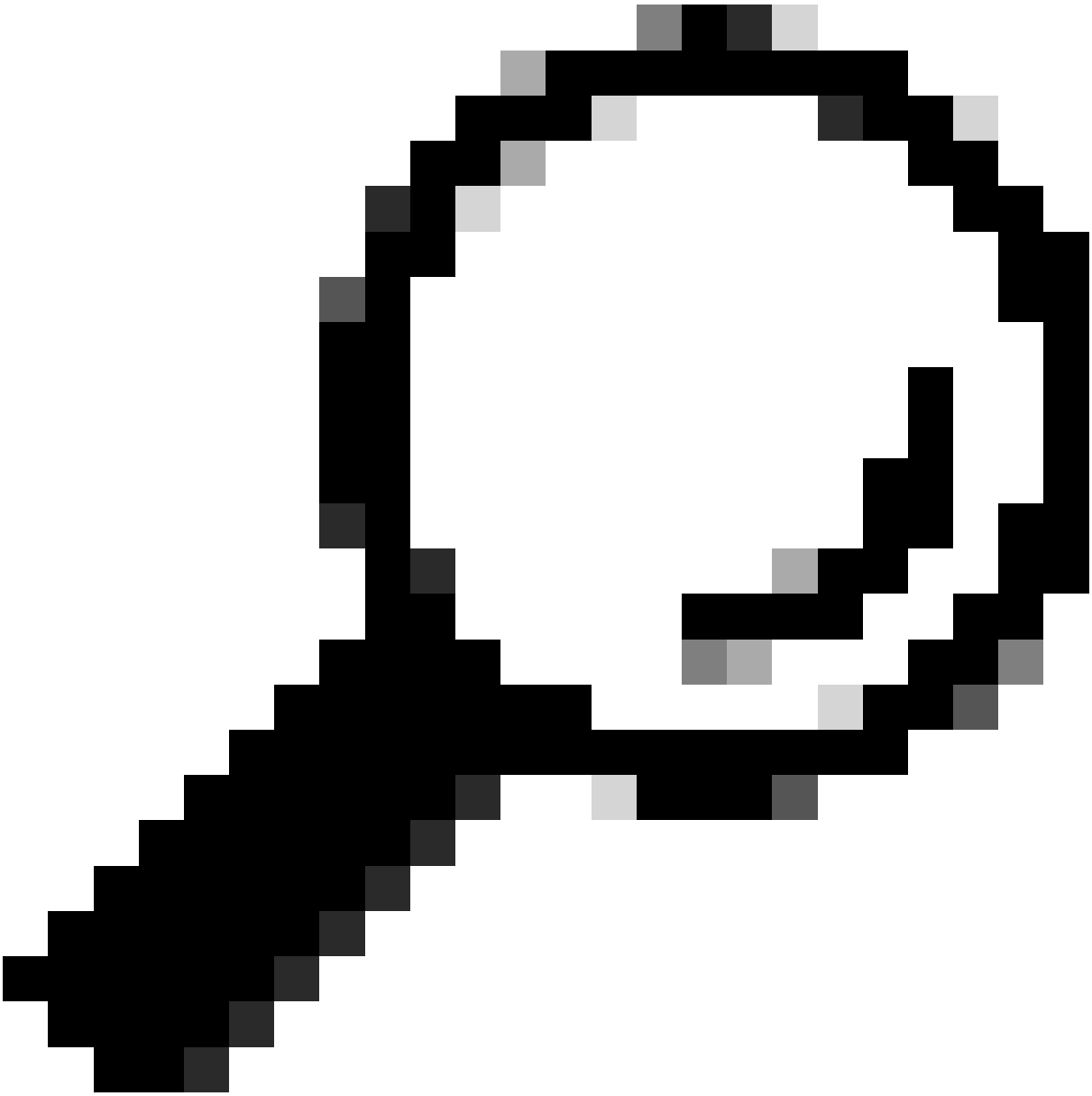
已解密流量的百分比对设备的大小有直接影响。管理员可以依靠至少75%的网络流量进行HTTPS。

初始安装后，必须确定解密流量的百分比，以确保准确设定对未来增长的预期。部署后，必须每季

度检查一次此编号。

如果解密率超过30%，并且SWA存在性能问题，建议执行以下操作之一：

- 删除解密策略中各种类别或受信任URL（例如Microsoft更新或防病毒更新）的解密
- 跨多个SWA进行负载均衡，以分配负载



提示：有关如何绕过SWA中解密的详细信息，请访问：https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

---

计算解密百分比的步骤

要查找与所有HTTPS流量相比已解密的HTTPS流量的百分比，请从SWA文件传输协议(FTP)复制

access_logs。

可以使用简单的Bash或PowerShell命令来获取此数字。下面是为每个环境描述的步骤：

1. 查找HTTPS连接总数（显式和透明）：

```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. 查找已解密HTTPS连接的数量：

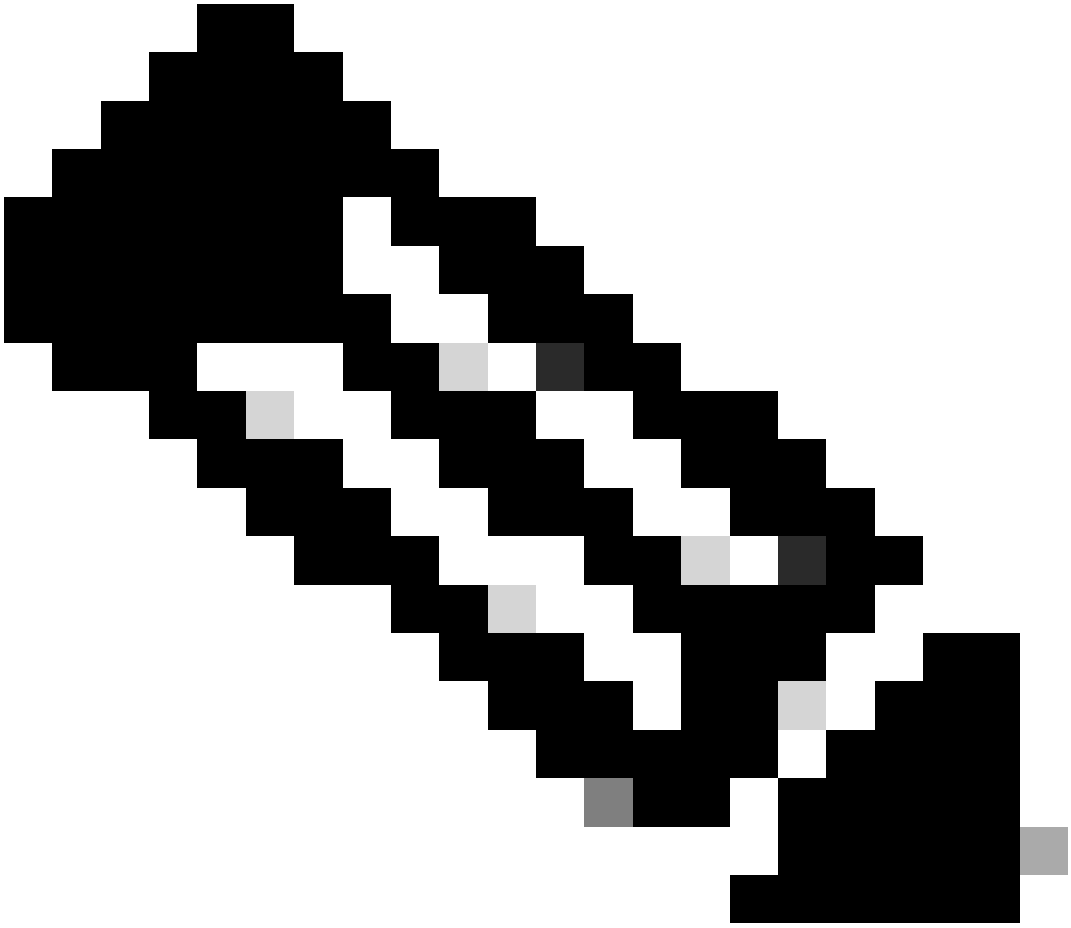
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT'| Select-String -Pattern 'DE
```

3. 将第二个值除以第一个值，然后乘以100。

来自CLI的整体流量统计信息

您可以使用accessloganalyzer命令在CLI中查看流量统计信息，该命令可以为您的报告选择时间范围或过去的N小时。



注意：命令的执行时间取决于所选的时间段。

```
SWA_CLI> accessloganalyzer

Choose the option to define the time range:
- HOURS - Last N hours.
- RANGE - Time range with start and end specified in  MM/DD/YYYY HH:MM:SS format.
[]> HOURS

Analyze logs upto N hours old (oldest on this WSA is N = 312 hours). Enter N:
[]> 10

The log processing might take more than 15 secs. Do you want to continue: (Yes/No)
[No]> yes



------------------------------------------------------------------------------------------------
                                        HTTP                HTTPS               Cumulative
---------------------------------------- ------------------- ------------------- --------------------
Num transactions                        1512509             4170261             5682770
```

Transaction/sec	42	115	157
Bandwidth (Mbps)	0.0001	0.0004	0.0003
Max Resp time (ms)	643269	285036670	285036670
Average Resp time(ms)	95663	141715	129458
Max Object size (KB)	92246	1215832	1215832
Avg Object size (Total Trans)(KB)	5	54	41
Avg Object size (Allowed Trans) (KB)	20	67	62
Methods			
GET	1295658	0	1295658
POST	34968	0	34968
CONNECT	0	4170261	4170261
Others	181883	0	181883
Status Codes			
1xx	0	0	0
2xx	319799	3351382	3671181
3xx	75011	0	75011
4xx	11697	115467	127164
5xx	1105999	703412	1809411

相关信息

AsyncOSAsyncOSor Cisco Cisco Web Appliance - LD (LimLDed Deployment) -思科

UCiscoure Web设备最佳实践-思科

HCisco使Office 365流量免于在Cisco WCiscocurity设备(WSA)上进行身份验证和解密- WSAco

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）。

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）。