Determine Decryption Rate in SWA

Contents

Introduction

This document describes steps to calculate the percentage of decrypted traffic in Secure Web Appliance(SWA) formerly known as WSA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Physical or Virtual Secure Web Appliance (SWA) Installed.
- License activated or installed.
- Secure Shell (SSH) Client.
- The setup wizard is completed.

- Administrative Access to the SWA.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Decryption Performance Impact

Of all the services performed by the SWA, evaluation of Hypertext Transfer Protocol Secure (HTTPS) traffic is the most significant from a performance standpoint.

The percentage of decrypted traffic has a direct impact on how the appliance must be sized. An administrator can count on at least 75% of web traffic to be HTTPS.

After initial installation, the percentage of decrypted traffic must be determined to ensure that the expectations for future growth are accurately set. After deployment, this number must be checked once per quarter.

If the decryption rate is more than 30% and SWA has performance issue, it is advised to either:

- Remove decryption on various categories or trusted URLs (such as Microsoft Update or Antivirus Updates) in the decryption policies
- Load balance across more SWAs to distribute the load

Tip: For more information about how to bypass decryption in SWA, please visit: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

Steps To Calculate Decryption Percentage

To find the percentage of HTTPS traffic that is decrypted in compare to all HTTPS traffic, copy the access_logs from SWA File Transfer Protocol (FTP).

Simple Bash or PowerShell commands can be used to obtain this number. Here are the steps that are described for each environment:

1. Find the number of total HTTPS connections (both explicit and transparent):

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

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

2. Find the number of decrypted HTTPS Connections:

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

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECTâ€™| Select-String -Pattern â€
```

3. Divide the second value by the first value and multiply by 100.

Overall Traffic Statistics From CLI

You can view the traffic stats in CLI, with **accessloganalyzer** command which you can choose time range or past **N** hours, for your report.

Note: The execution time of the command depends on the selected time period.

```
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

Related Information

User Guide for AsyncOSAsyncOSor Cisco SCisco Web Appliance - LD (LimLDed Deployment) - Cisco

UCiscocure Web Appliance Best Practices - Cisco

HCisco Exempt Office 365 Traffic From Authentication and Decryption on Cisco WCiscocurity Appliance (WSA) - WSAco