Determinación de la tasa de descifrado en SWA

Contenido

Introducción

Este documento describe los pasos para calcular el porcentaje de tráfico descifrado en Secure Web Appliance (SWA), anteriormente conocido como WSA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo web seguro (SWA) físico o virtual instalado.
- Licencia activada o instalada.
- Cliente Secure Shell (SSH).
- El asistente de configuración ha finalizado.
- Acceso administrativo al SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Impacto del rendimiento del descifrado

De todos los servicios que realiza el SWA, la evaluación del tráfico seguro del protocolo de transferencia de hipertexto (HTTPS) es la más significativa desde el punto de vista del

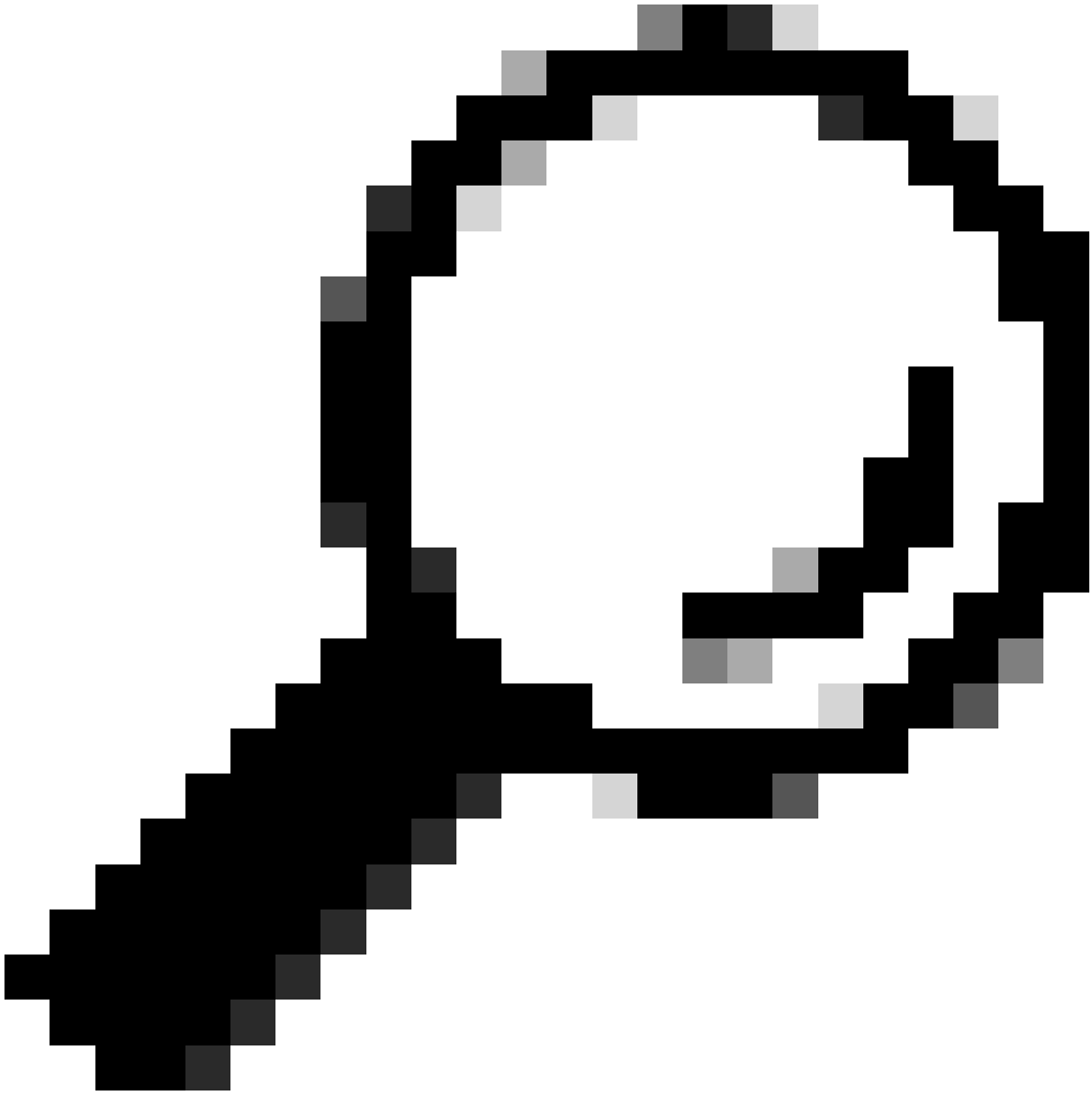
rendimiento.

El porcentaje de tráfico descifrado tiene un impacto directo en el tamaño del dispositivo. Un administrador puede contar con que al menos el 75% del tráfico web sea HTTPS.

Después de la instalación inicial, se debe determinar el porcentaje de tráfico descifrado para garantizar que las expectativas de crecimiento futuro se establezcan con precisión. Después de la implementación, este número debe comprobarse una vez al trimestre.

Si la tasa de descifrado es superior al 30% y SWA presenta problemas de rendimiento, se recomienda:

- Elimine el descifrado en varias categorías o URL de confianza (como Microsoft Update o Actualizaciones de antivirus) en las directivas de descifrado
- Equilibrio de carga entre más SWA para distribuir la carga



Sugerencia: para obtener más información sobre cómo omitir el descifrado en SWA, visite: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

Pasos Para Calcular El Porcentaje De Descifrado

Para encontrar el porcentaje de tráfico HTTPS que se descifra en comparación con todo el tráfico HTTPS, copie los access_logs del protocolo de transferencia de archivos (FTP) SWA.

Para obtener este número se pueden utilizar comandos de PowerShell o de Bash simple. Estos son los pasos que se describen para cada entorno:

1. Busque el número total de conexiones HTTPS (explícitas y transparentes):

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

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

2. Busque el número de conexiones HTTPS descifradas:

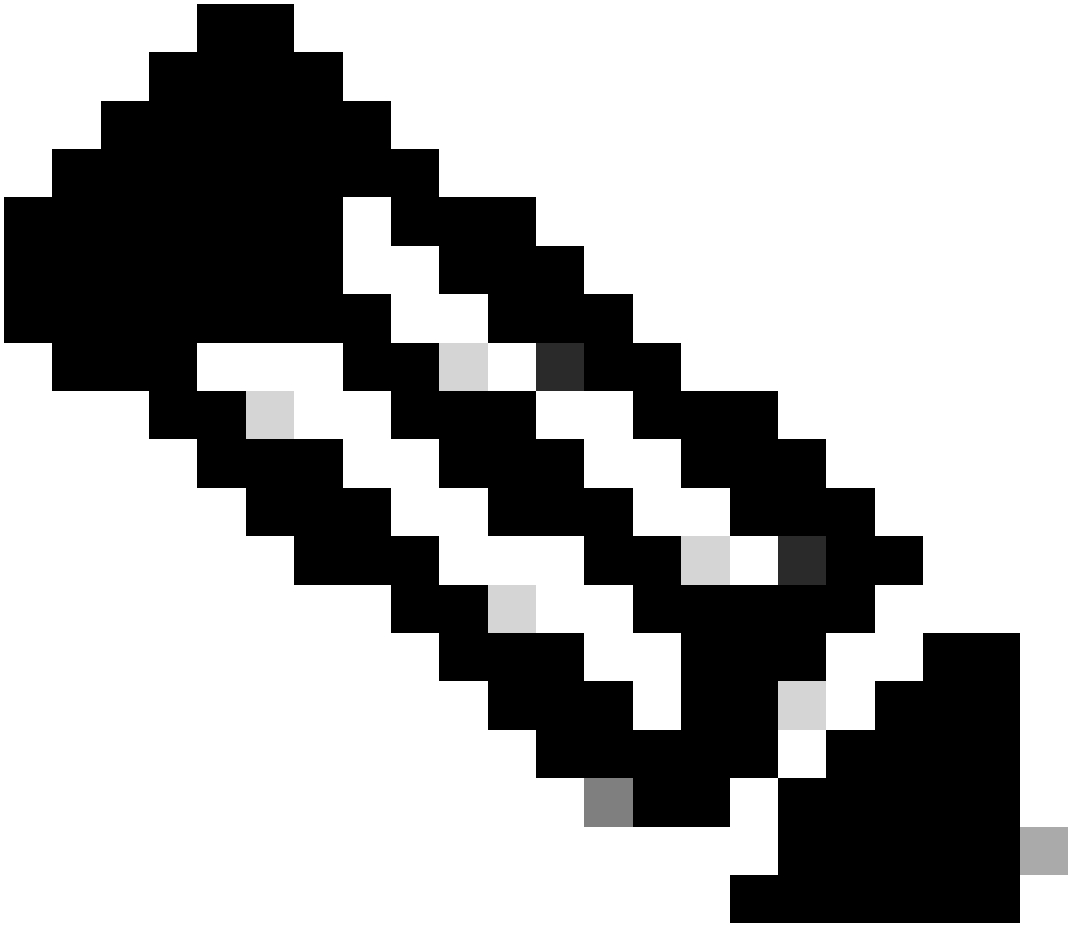
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

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

3. Divida el segundo valor por el primer valor y multiplique por 100.

Estadísticas de tráfico generales desde CLI

Puede ver las estadísticas del tráfico en CLI, con el comando accessloganalyzer, que puede elegir el rango de tiempo o las N horas pasadas, para su informe.



Nota: El tiempo de ejecución del comando depende del período de tiempo seleccionado.

```
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

Información Relacionada

Guía del usuario de AsyncOSAsyncOSo Cisco SCisco Web Appliance - LD (implementación de LimLDed) - Cisco

Prácticas recomendadas de dispositivos web de Cisco UCiscocure: Cisco

Tráfico de Cisco Office 365 exento de autenticación y descifrado en Cisco WCiscosecurity Appliance (WSA): WSAco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).