Determinar a taxa de descriptografia em SWA

Contents

Introdução

Este documento descreve as etapas para calcular a porcentagem de tráfego descriptografado no Secure Web Appliance(SWA), anteriormente conhecido como WSA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo da Web seguro (SWA) físico ou virtual instalado.
- Licença ativada ou instalada.
- Cliente Secure Shell (SSH).
- O assistente de instalação foi concluído.

- Acesso administrativo ao SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Impacto no desempenho da descriptografia

De todos os serviços executados pelo SWA, a avaliação do tráfego do protocolo HTTPS é a mais significativa do ponto de vista do desempenho.

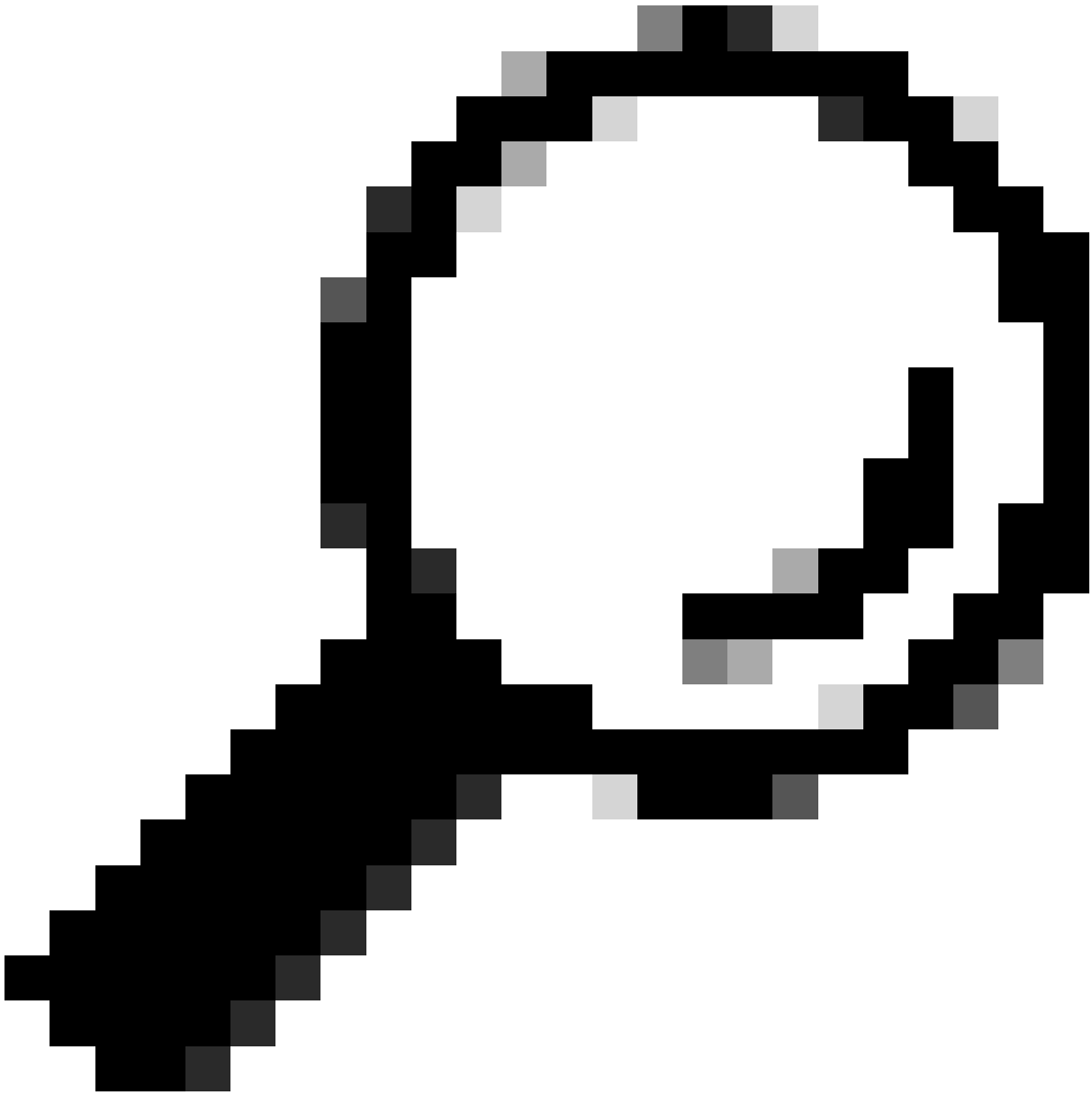
A porcentagem de tráfego descriptografado tem um impacto direto sobre como o dispositivo deve ser dimensionado. Um administrador pode contar com pelo menos 75% do tráfego da Web para ser HTTPS.

Após a instalação inicial, a porcentagem de tráfego descriptografado deve ser determinada para garantir que as expectativas de crescimento futuro sejam definidas com precisão. Após a implantação, esse número deve ser verificado uma vez por trimestre.

Se a taxa de descriptografia for superior a 30% e o SWA tiver problemas de desempenho, é aconselhável:

- Remova a descriptografia em várias categorias ou URLs confiáveis (como o Microsoft Update ou as atualizações antivírus) nas políticas de descriptografia
- Balanceamento de carga em mais SWAs para distribuir a carga

---



Dica: para obter mais informações sobre como ignorar a descriptografia em 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

Etapas para Calcular o Percentual de Descriptografia

Para localizar a porcentagem de tráfego HTTPS descriptografado em comparação a todo o tráfego HTTPS, copie os access_logs do FTP (File Transfer Protocol) do SWA.

Os comandos Simple Bash ou PowerShell podem ser usados para obter esse número. Estas são as etapas descritas para cada ambiente:

1. Localize o número total de conexões HTTPS (explícitas e transparentes):

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

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

2. Localize o número de Conexões HTTPS descriptografadas:

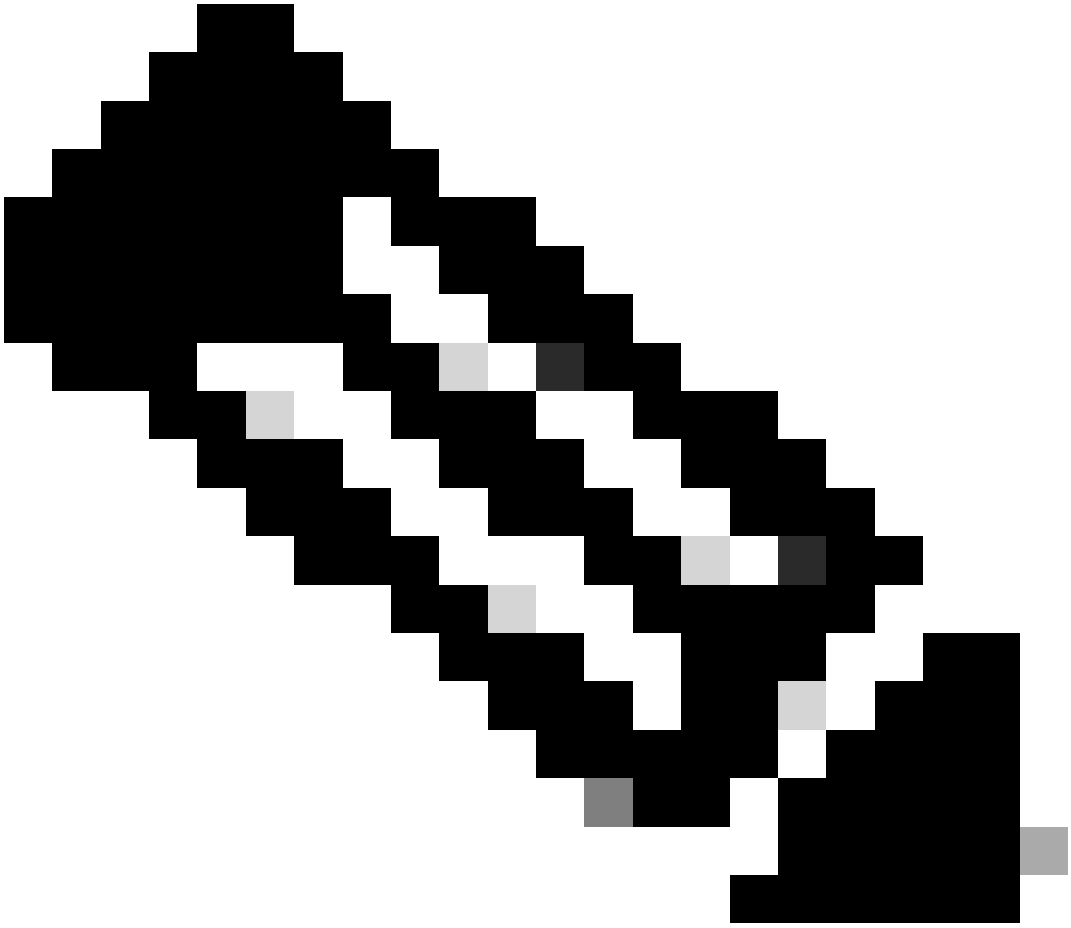
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

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

3. Divida o segundo valor pelo primeiro e multiplique por 100.

Estatísticas gerais de tráfego da CLI

Você pode exibir as estatísticas de tráfego na CLI, com o comando accessloganalyzer, que permite escolher o intervalo de tempo ou as N últimas horas, para o relatório.



Observação: o tempo de execução do comando depende do período selecionado.

```
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

Informações Relacionadas

Manual do usuário para AsyncOSAsyncOSou Cisco SCisco Web Appliance - LD (implantação LimLD) - Cisco

Práticas recomendadas para dispositivos da Web UCiscocure - Cisco

Tráfego do Office 365 isento da Cisco de autenticação e descriptografia no Cisco WSA (WCiscocurity Appliance) - WSAco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.