

# Solución de problemas de latencia de dispositivo web seguro

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Causas frecuentes de la alta latencia en SWA](#)

[Herramientas de solución de problemas de latencia SWA](#)

[Estado del sistema](#)

[Capacidad del sistema](#)

[Analizar destinos principales](#)

[Analizar usuarios principales](#)

[Registros SHD](#)

[Utilización de registros de acceso para solucionar problemas de latencia](#)

[Tiempo de autenticación alto](#)

[Tiempo DNS alto](#)

[Tiempo de motor de escaneo alto](#)

[Práctica recomendada al conectar la captura de paquetes](#)

[Complejidad de configuración](#)

[Comandos CLI](#)

[Versión](#)

[mostraralertas](#)

[process status](#)

[detalle de estado](#)

[lpcheck](#)

[velocidad](#)

[Recopilación de registros para una latencia alta](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe los pasos de troubleshooting para hacer frente a la alta latencia, el alto disco y la alta CPU en Cisco Secure Web Appliance (SWA).

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Cisco SWA
- Métodos de implementación de proxy (explícito y transparente)
- Comandos de la interfaz de línea de comandos (CLI) 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.

## Antecedentes

Al ponerse en contacto con el soporte técnico de Cisco, se le solicitará que proporcione detalles sobre la actividad de la red SWA entrante y saliente, que se puede supervisar mediante la ejecución de una captura de paquetes para recopilar el tráfico con fines de depuración o verificación.

## Causas frecuentes de la alta latencia en SWA

En general, hay tres categorías principales para la alta latencia en SWA:

1. Dimensionamiento inadecuado de los SWA o recursos sobrecargados
2. Configuraciones complejas
3. Problemas de latencia relacionados con la red

Una de las causas más comunes de la alta latencia en SWA es el tamaño inadecuado de la solución. El dimensionamiento adecuado es fundamental para garantizar que el sistema SWA dispone de recursos suficientes para gestionar las cargas de trabajo actuales y futuras. Si el sistema no tiene el tamaño adecuado, puede tener dificultades para procesar las solicitudes de forma eficaz, lo que provoca retrasos en las operaciones y reduce el rendimiento. Factores como el número de usuarios, el volumen de descifrado y las demandas de análisis específicas deben evaluarse cuidadosamente durante la implementación para evitar las limitaciones de recursos. Si no se ajusta la capacidad de SWA a las necesidades de la organización, puede producirse una latencia persistente y una experiencia del usuario degradada.

Las configuraciones complejas pueden degradar el rendimiento y causar latencia en el SWA,

especialmente bajo una carga alta, ya que cada solicitud debe procesarse a través de numerosas condiciones.

La latencia relacionada con la red puede provenir del propio SWA, de servicios de terceros como Active Directory, DLP, DNS o de retrasos en la red entre el cliente, SWA y servidores ascendentes.

El análisis de las solicitudes enviadas al SWA, incluida la identificación de los principales usuarios y las URL a las que se accede con más frecuencia, puede ayudar a descubrir posibles comportamientos incorrectos y a identificar las causas principales de la latencia. Esta información es muy valiosa para diagnosticar problemas de rendimiento, gestionar el consumo de ancho de banda y garantizar el uso adecuado del sistema.

## Herramientas de solución de problemas de latencia SWA

### Estado del sistema

Siga estos pasos para comprobar el consumo de recursos actual en SWA:

Paso 1. Acceder a la interfaz gráfica de usuario (GUI) de SWA.

Paso 2. Vaya a Informes > Información del sistema > Estado del sistema.

Paso 3. Compruebe estas métricas críticas para evaluar el rendimiento del sistema:

- Uso de la CPU (%): Indica la carga actual de la CPU
- Uso de RAM (%): Refleja la utilización de la memoria
- Uso de informes/registros (%): Muestra el porcentaje de espacio en disco que se utiliza para informes y registros
- Tiempo de Actividad del Sistema: Muestra el tiempo total que el sistema ha estado ejecutándose sin reiniciar

## System Status

Printable PDF

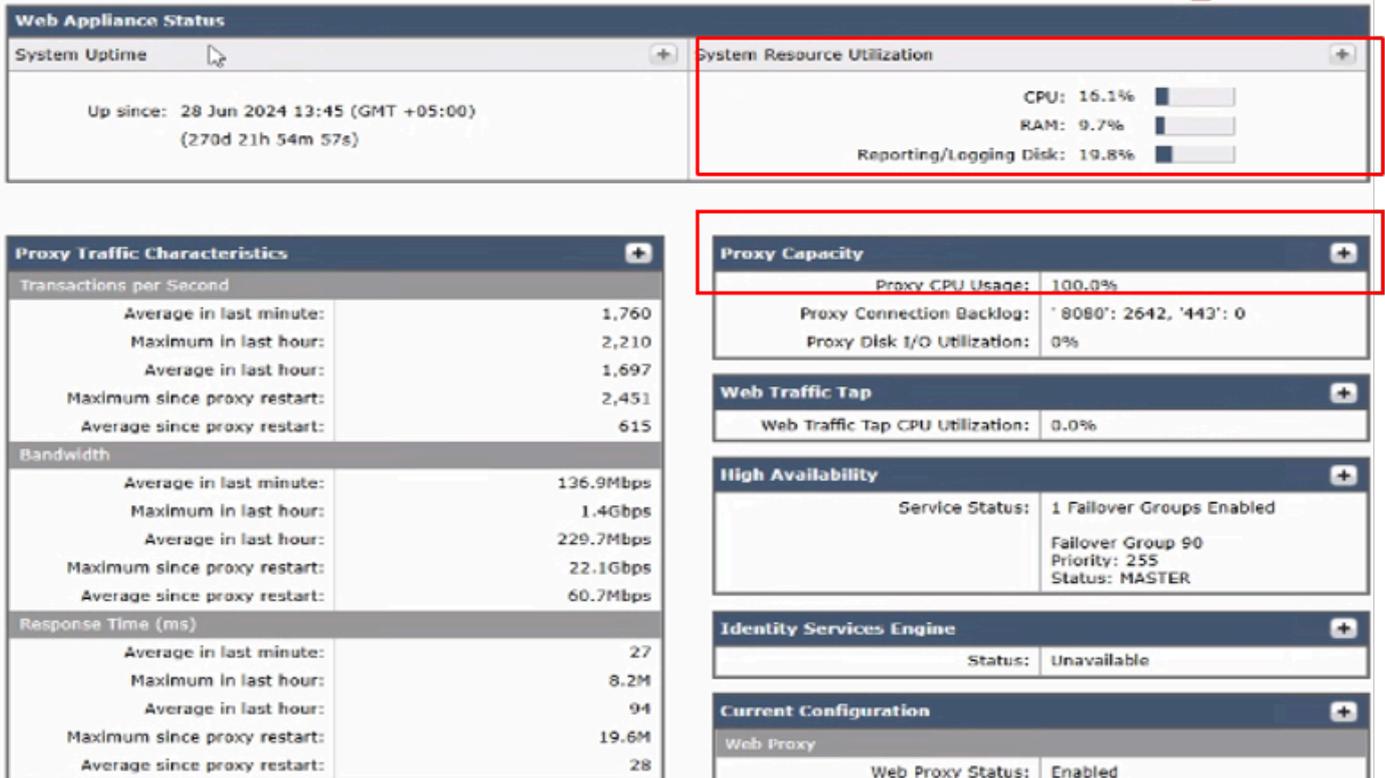


Imagen- Estado del sistema

Esta página proporciona una descripción general del estado actual de la RAM, la CPU y el uso del disco. Para ver el uso de recursos a lo largo del tiempo, en la GUI de SWA, vaya a Informes y seleccione Capacidad del sistema.

## Capacidad del sistema

La página Capacidad del Sistema del análisis de rendimiento proporciona una vista completa de las métricas de rendimiento y utilización de recursos en un rango de tiempo específico. Esta página ofrece gráficos detallados para ayudar a supervisar y analizar el comportamiento del sistema, garantizando un rendimiento óptimo e identificando posibles cuellos de botella.

Los gráficos y las métricas disponibles en la página Capacidad del Sistema son:

1. Uso general de la CPU: Muestra el uso total de la CPU y ofrece una descripción general de alto nivel del rendimiento del sistema.
2. Uso de la CPU por función: desglosa el uso de la CPU en función de funciones específicas, incluidas:
  - Proxy web
  - Registro
  - Informes
  - McAfee
  - Sophos
  - Webroot
  - Uso aceptable y reputación

3. Tiempo/latencia de respuesta (milisegundos): realiza un seguimiento de los tiempos de respuesta para identificar cualquier retraso en el procesamiento de las solicitudes.
4. Transacciones por segundo: Muestra el número de transacciones gestionadas por el SWA por segundo.
5. Conexiones fuera: Supervisa el número de conexiones salientes que se están estableciendo.
6. Ancho de banda de salida (bytes): Mide la cantidad de ancho de banda saliente que se está utilizando.
7. Memoria del búfer del proxy (%): Muestra el porcentaje de memoria utilizado por el proceso proxy.

Compruebe las métricas para detectar cualquier indicio de uso elevado de recursos en este panel.

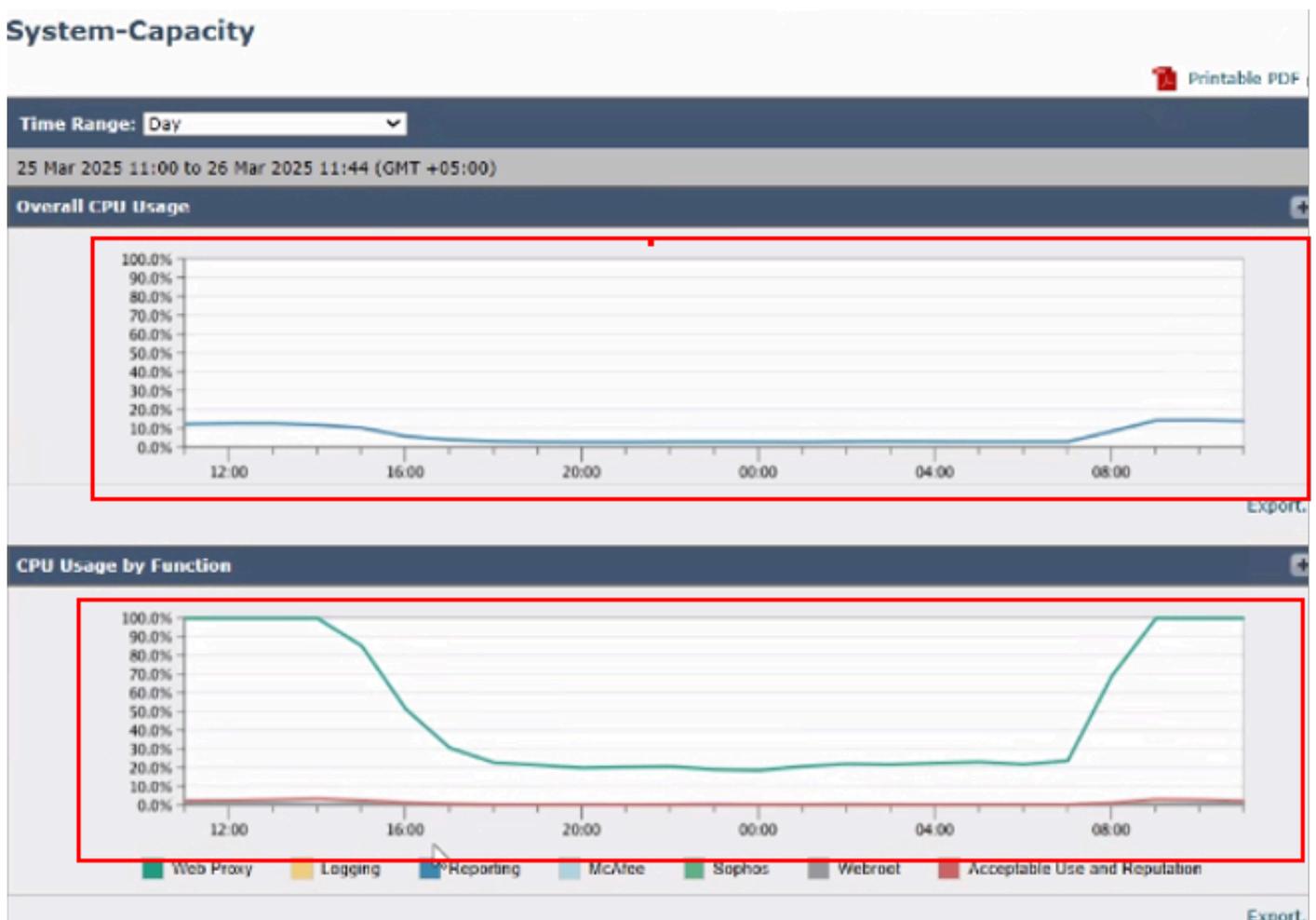
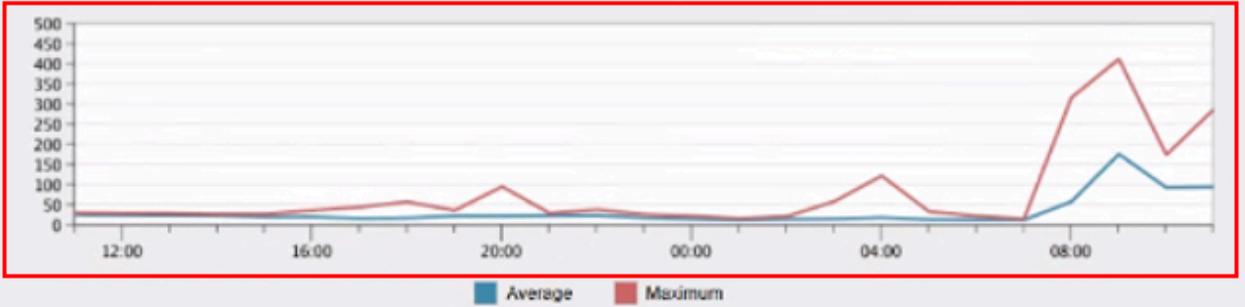


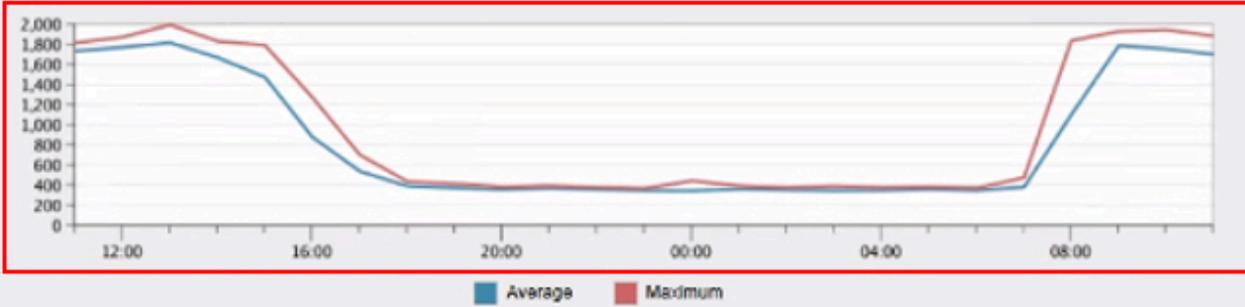
Imagen - Capacidad del sistema

Response Time/Latency (milliseconds) +



Export..

Transactions Per Second +



Export..

Connections Out +

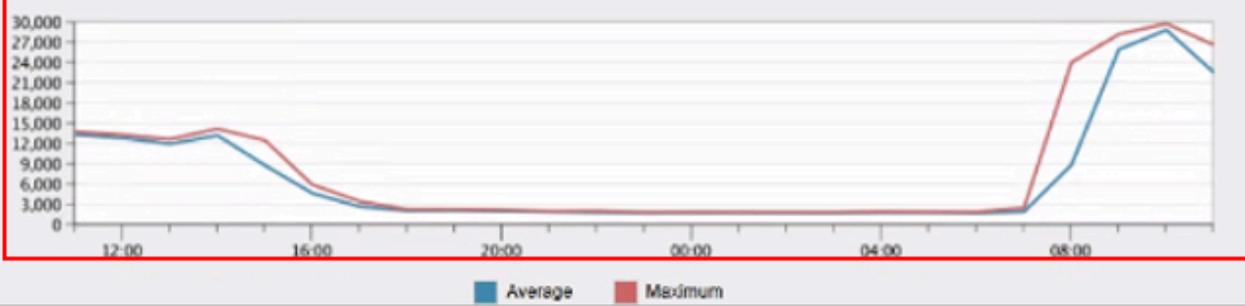


Imagen: transacciones SWA por segundo y conexiones salientes



Imagen - Uso de memoria SWA

## Analizar destinos principales

Para analizar los principales destinos, navegue hasta la GUI de SWA, navegue hasta Reporting y seleccione Websites. Revise la lista de los principales sitios web HTTP/HTTPS e identifique los dominios con mayor tráfico o a los que se accede con más frecuencia.

De acuerdo con sus conclusiones, considere la posibilidad de omitir o eximir las URL genéricas, como Microsoft Updates, Adobe, Office365 y las plataformas de reuniones en línea. Este enfoque ayuda a reducir el tráfico en el SWA, lo que se traduce en una menor latencia y una menor carga de procesamiento de proxy.

## Web Sites

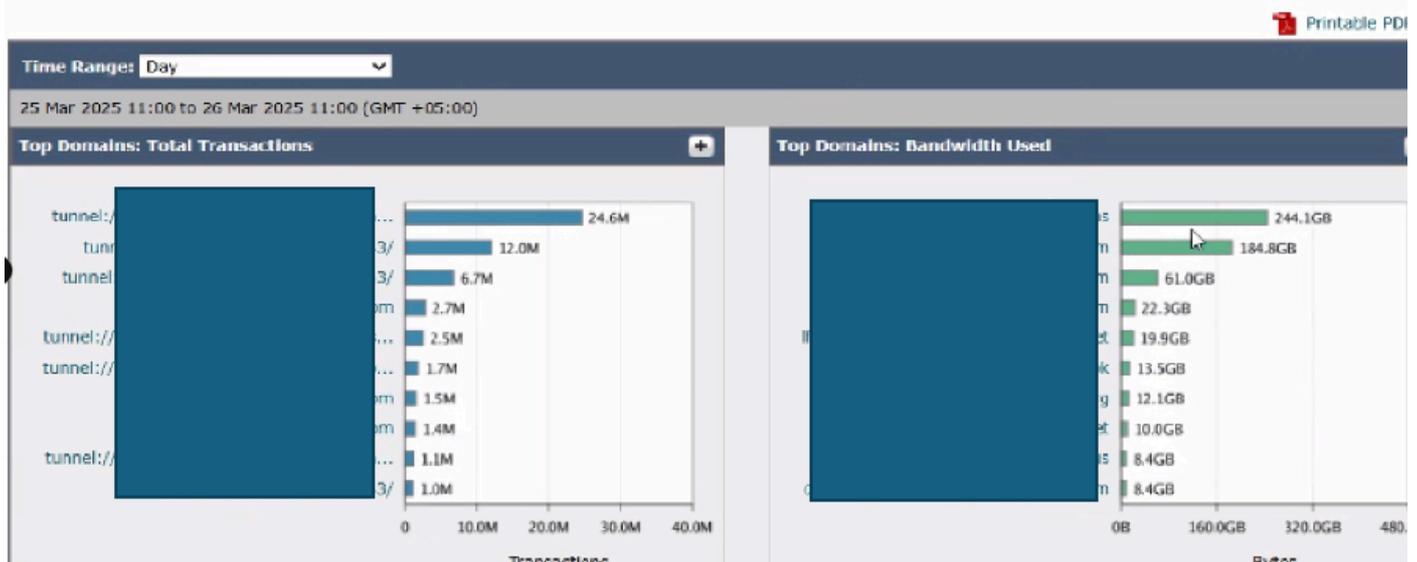


Imagen- Panel de sitios web principales de SWA

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
	0B	23514:57	0	24.6M	24.6M
	0B	1909:50	0	12.0M	12.0M
	0B	26710:03	0	6.7M	6.7M
	3.0MB	4941:17	2,798	2.7M	2.7M
	0B	10029:17	0	2.5M	2.5M
	0B	2579:58	0	1.7M	1.7M
	4.2GB	5981:18	1.5M	0	1.5M
	184.8GB	2125:54	1.4M	1,806	1.4M
	0B	2062:27	0	1.1M	1.1M
	0B	1354:09	0	1.0M	1.0M
Totals (all available data):	741.1GB	111839:46	6.7M	64.8M	71.5M

Imagen- Panel de dominios principales SWA

## Analizar usuarios principales

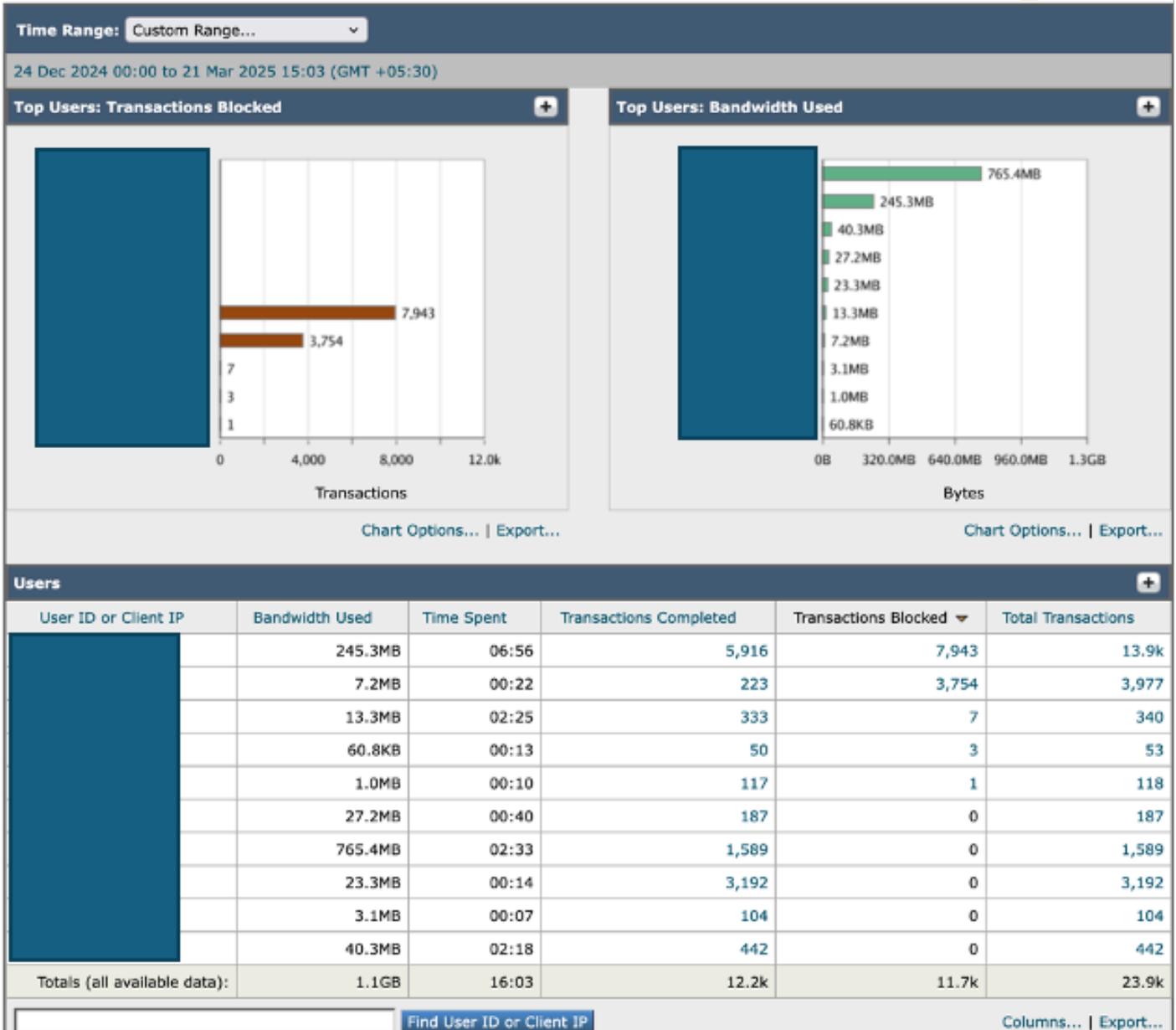
Para identificar fuentes potenciales de tráfico excesivo, navegue hasta la GUI de SWA desde Reporting y elija Users.

Revise la lista para determinar qué usuarios generan el mayor número de transacciones para el SWA. Además, verifique si hay máquinas de usuario que estén generando el mayor número de transacciones para el SWA y que consuman el ancho de banda máximo.

Este análisis puede ayudar a identificar a los usuarios o dispositivos responsables de las cargas de tráfico significativas, lo que permite llevar a cabo acciones específicas para reducir la sobrecarga general del sistema.

# Users

Printable PDF



Panel de usuarios principales de Image-SWA

## Registros SHD

Al revisar SHD\_log, puede analizar algunas de las métricas de rendimiento, como el número de sesiones de los usuarios a SWA (CliConn), el número de sesiones de SWA a Internet (SrvConn), el promedio de solicitudes por segundo (Reqs), etc.

Para obtener más información sobre el registro de SHD, consulte el enlace [Resolución de problemas de rendimiento de dispositivos web seguros con registros de SHD](#),

Algunos parámetros clave para revisar en los registros SHD son:

- ClientConns: Número de conexiones de cliente activas

- ServerConns: Número de conexiones de servidor activas
- ProxLd: Carga media del proceso de proxy
- CPULD: Carga media total de CPU
- RAMUTIL: utilización de RAM
- Latencia: tiempo medio de servicio en un minuto
- DiskUtil: uso del disco y rendimiento de E/S

Como en este ejemplo, tener alrededor de 1,600 Solicitudes por Segundo, conduce a una alta carga de proceso de proxy.

```
Wed Mar 26 11:09:30 2025 Info: Status: CPULd 16.3 DskUtil 19.9 RAMUtil 9.3 Reqs 1661 Band 152966 Latency
Wed Mar 26 11:10:31 2025 Info: Status: CPULd 13.6 DskUtil 19.9 RAMUtil 9.5 Reqs 1699 Band 107048 Latency
Wed Mar 26 11:11:31 2025 Info: Status: CPULd 15.0 DskUtil 19.9 RAMUtil 9.5 Reqs 1669 Band 178803 Latency
Wed Mar 26 11:12:31 2025 Info: Status: CPULd 17.6 DskUtil 19.9 RAMUtil 9.2 Reqs 1785 Band 143721 Latency
```

## Utilización de registros de acceso para solucionar problemas de latencia

Cuando se producen problemas de latencia con el proxy del tráfico a través de un SWA, los registros de acceso pueden servir como una herramienta valiosa para identificar la causa raíz probable. Para mejorar los esfuerzos de solución de problemas, puede modificar la configuración existente del registro de acceso o crear un nuevo registro de acceso. Al incluir parámetros de rendimiento en el campo personalizado, puede obtener información más detallada sobre los factores que contribuyen a la latencia, lo que permite un análisis y una resolución más eficaces.

Para obtener más información sobre los parámetros de rendimiento y los pasos de configuración, consulte el enlace: [Configure Performance Parameter in Access Logs](#)

Esta es la guía detallada para recopilar registros en el SWA: [Acceder a registros de appliances web seguros](#)

Los orígenes de latencia se pueden analizar examinando los parámetros clave que ayudan a determinar si se producen retrasos entre el cliente y el SWA, dentro de los procesos internos del SWA o entre el SWA y el servidor web. Entre los indicadores importantes que se deben tener en cuenta se incluyen los servicios basados en la red, como la resolución de DNS, el tiempo de autenticación y los tiempos de respuesta del servidor o el cliente. Además, se deben evaluar los retrasos causados por motores de análisis como AMP, Sophos y AVC para identificar su impacto en la latencia general.



```
1750344193.093 5272 10.10.20.30 TCP_MISS_SSL/200 39 CONNECT tunnel://cisco.com:443/
" cisco\user@cisco.com" DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-
Authentication_Profile-DefaultGroup-NONE-NONE-DefaultGroup-NONE <" C_Cis",6.3,1,"-","-","-","-","-","-
","-","-","-","-","-","-","IW_Com","-","-","Computer","-","Unknown","Unknown","-","-","0.06,0,-","-","-
","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-
" [ Request Details: ID = 169121930, User Agent = "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36", AD
Group Memberships = ( NTLMSSP ) " Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request
Header = 0, Request to Server = 0, 1st byte to client = 3, Response Header = 0, Client Body = 9 ] [ Rx Wait
Times (in ms): 1st request byte = 0, Request Header = 0, Client Body = 0, 1st response byte = 0, Response
header = 0, Server response = 13, Disk Cache = 0; Auth response = 5210, Auth total = 33; DNS response =
0, DNS total = 0, WBRs response = 0, WBRs total = 0, AVC response = 0, AVC total = 0, DCA response = 0,
DCA total = 0, McAfee response = 0, McAfee total = 0, Sophos response = 0, Sophos total = 0, Webroot
response = 0, Webroot total = 0, Anti-Spyware response = 0, Anti-Spyware total = 0; AMP response = 0,
AMP total = 0; Latency = 5243; " 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP =
10.20.30.40, Server Port = 443]
```

Imagen - Muestra de latencia de autenticación alta

## Tiempo DNS alto

Si el tiempo de respuesta de DNS es alto, esta información es necesaria para que el TAC resuelva los problemas de latencia de DNS:

- Configuración SWA actual
- Registros del sistema en modo de seguimiento
- Dirección IP de servidores DNS
- Capturas de paquetes de
  - Equipo cliente
  - SWA (Filtrado con dirección IP de servidores DNS)
- Asegúrese de que los registros de accesos tienen %:<d y %:>d en el campo personalizado
- archivo HAR del cliente mientras se reproduce el problema

Para obtener más información sobre la configuración y la resolución de problemas de DNS, consulte el enlace [Resolución de problemas del servicio DNS del dispositivo web seguro](#)

Este ejemplo muestra el tiempo de latencia alta relacionado con la resolución de nombres DNS:



Si los motores de escaneo muestran una respuesta alta, para una recuperación inmediata, puede reiniciar el servicio de escaneo desde CLI mediante estos pasos:

Paso 1. Escriba `diagnostic` y presione Enter (Este es un comando oculto y necesita escribir el comando exacto).

Paso 2. Seleccione `SERVICIOS`.

Paso 3. Para reiniciar el servicio `WBRS`, elija `WBRS`; de lo contrario, vaya al paso 6.

Paso 4. Elija `RESTART`.

Paso 5. Siga presionando Intro para salir del asistente.

Paso 6. En caso de que esté planeando reiniciar cualquier motor de escaneo de Malware, elija `ANTIVIRUS`.

Paso 7. Seleccione sus escáneres.

Paso 8. Elija `RESTART`.

Paso 9. Siga presionando Intro para salir del asistente.



Advertencia: El reinicio de los servicios internos provoca la interrupción del servicio. Recomiende realizar esto en horas fuera de producción o por precaución.

---

## Práctica Recomendada Al Conectar La Captura De Paquetes

Al realizar cualquier captura de paquetes, recopile y comparta esta información con el TAC de Cisco.

- Dirección IP del cliente.
- La URL a la que estaba intentando acceder.
- La dirección IP resuelta para esa URL desde el PC cliente y desde el SWA.
- Experiencia del usuario (por ejemplo, la página no se ha cargado o tiene una carga parcial, y si hay algún mensaje de error, realice una captura de pantalla).
- Marca de tiempo de la prueba.
- Cierre todos los demás navegadores y aplicaciones del equipo cliente. Acceda al sitio web, capture los registros en el Bloc de notas para un intento de éxito o error y compártalos con

el Soporte técnico de Cisco.

Para obtener información detallada sobre cómo realizar la captura de paquetes en SWA, refiérase al link [Configure Packet Capture on Content Security Appliance](#)

## Complejidad de configuración

Otra causa común de latencia alta y bajo rendimiento es la complejidad de la configuración. Esto ocurre cuando el SWA se configura con un número excesivo de condiciones, perfiles y políticas. Esta complejidad puede aumentar considerablemente los tiempos de respuesta y suponer una carga pesada para el proceso proxy. Este problema tiende a ser más pronunciado durante las horas punta, cuando el tráfico es más alto.

A continuación, se ofrecen algunas sugerencias para optimizar la configuración:

1. Limitar descifrado HTTPS: Solo descifre el tráfico esencial para sus políticas de seguridad. Siempre que sea posible, reduzca la sobrecarga de procesamiento mientras mantiene la seguridad.
2. Dé prioridad a las políticas de eficiencia: Organice las políticas que se utilizan con más frecuencia en la parte superior de la lista de políticas. Esto garantiza un procesamiento más rápido al abordar primero el tráfico más exigente.
3. Simplificar el diseño de políticas: Simplifique las políticas minimizando su número tanto como sea posible. Esto reduce el procesamiento innecesario y mejora el rendimiento general del sistema.
4. Optimizar el análisis de antimalware y antivirus: revise las configuraciones de análisis para los procesos de antimalware y antivirus. Estos pueden requerir un uso intensivo de la CPU, por lo que ajustarlos puede reducir considerablemente el consumo de recursos sin poner en peligro la seguridad.
5. Utilizar expresiones regulares ligeras: Evite las expresiones regulares complejas o que consumen muchos recursos. Asegúrese de que caracteres como puntos (.) y estrellas (\*) se hayan escapado correctamente para reducir la tensión de procesamiento y evitar ineficiencias.

Para obtener información detallada sobre las prácticas recomendadas de SWA, visite [Usar prácticas recomendadas de dispositivos web seguros](#)

## Comandos CLI

### Versión

Utilice el comando `version` para verificar la asignación de hardware (para el SWA virtual) y el estado de RAID (para el SWA físico). Compruebe la configuración de hardware: Asegúrese de que el número de núcleos de CPU, la memoria y los discos duros estén asignados según lo esperado. En los modelos virtuales, el estado de RAID se muestra como Desconocido; si el estado de RAID es Degradado o Error en el dispositivo físico, póngase en contacto con Cisco TAC para revisar el estado del disco desde el back end.

A continuación se muestra un ejemplo de asignación de más CPU al SWA que puede dar lugar a un comportamiento incorrecto:

```
SWA Lab> version
Current Version
=====
Product: Cisco S100V Secure Web Appliance
Model: S100V
BIOS: 6.00
CPUs: 3 expected, 4 allocated
Memory: 8192 MB expected, 8192 MB allocated
Hard disk: 200 GB, or 250 GB expected; 200 GB allocated
RAID: NA
RAID Status: Optimal
```

## mostraralertas

Utilice el comando `displayalerts` para verificar los mensajes de alerta relacionados con la red SWA que pueden indicar la causa raíz.

En este ejemplo, el servidor DNS en la dirección IP 10.10.10.10 no respondía y el mensaje "El servicio de Reputación de archivos no es accesible" puede indicar un problema de conectividad de red.

```
SWA LAB> displayalerts
Date and Time Stamp          Description
-----
26 Mar 2025 11:20:07 +0500 The File Reputation service is not reachable.
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 10:16:18 +0500 Warning: Communication with the File Reputation service has been established
```

## process\_status

Utilice el comando `process_status` para ver el uso del proceso y la memoria de los servicios internos SWA.

Si el proceso Prox, que es el proceso principal que maneja el proxy de tráfico, excede consistentemente el 100% de uso durante varios minutos, indica una carga alta sostenida en el proceso. Sin embargo, los picos cortos ocasionales en el uso de la CPU en el proxy u otros procesos son normales y esperados.

<#root>

```
SWA LAB> process_status
USER      PID
```

%CPU

%MEM

	VSZ	RSS	TT	STAT	STARTED		TIME			
<b>COMMAND</b>										
root	11	2805.4	0.0		0	512	- RNL	28Jun24	11863204:12.63	idle
root	71189									
102.0										
19.5										
6670700	6478032	-	R		23Feb25	18076	:32.80			
<b>prox</b>										
root	91880	99.0	0.6	369564	214832	-	R	28Jun24	58854:51.78	counterd
root	91267	76.0	0.9	379804	292324	-	R	28Jun24	59371:01.26	counterd
root	12	25.9	0.0	0	1600	-	WL	28Jun24	30899:57.88	intr
root	46955	25.0	0.2	91260	59336	-	S	23Jan25	7547:02.96	wbnpd
root	95056	23.0	11.2	5369332	3710348	-	I	28Jun24	31719:23.99	java
root	93190	12.0	1.4	3118384	456088	-	S	01:15	29:57.05	beakerd
root	64579	11.0	0.2	101336	71204	-	S	6Aug24	12074:55.55	coeuslogd

## detalle de estado

El comando status detail proporciona un resumen en tiempo real del uso de los recursos del sistema, las métricas del tráfico de red y las estadísticas de conexión, reflejando el estado y el rendimiento general del SWA. Refleja la vista Estado del sistema en la GUI para una supervisión y resolución de problemas rápidas.

<#root>

SWA LAB> Status detail

Status as of: Wed Mar 26 11:51:27 2025 PKT

Up since: Fri Jun 28 13:45:43 2024 PKT (270d 22h 5m 43s)

System Resource Utilization:

CPU 16.0%

RAM 10.3%

<b>Reporting/Logging Disk</b>	<b>19.8%</b>
<b>Transactions per Second:</b>	
Average in last minute	1745
Maximum in last hour	2210
Average in last hour	1708
Maximum since proxy restart	2451
Average since proxy restart	615
<b>Bandwidth (Mbps):</b>	
Average in last minute	149.699
Maximum in last hour	1356.387
Average in last hour	229.634
Maximum since proxy restart	22075.244
Average since proxy restart	60.689
<b>Response Time (ms):</b>	
Average in last minute	99
Maximum in last hour	8194128
Average in last hour	87
Maximum since proxy restart	19608632
Average since proxy restart	28
<b>Cache Hit Rate:</b>	
Average in last minute	3
Maximum in last hour	6
Average in last hour	2
Maximum since proxy restart	89
Average since proxy restart	2
<b>Connections:</b>	
Idle client connections	3481
Idle server connections	754
<b>Total client connections</b>	<b>21866</b>
<b>Total server connections</b>	<b>19049</b>
<b>SSLJobs:</b>	
In queue Avg in last minute	0
Average in last minute	12050
SSLInfo Average in last min	0
<b>Network Events:</b>	
Average in last minute	16.0
Maximum in last minute	171
Network events in last min	151918

## Ipcheck

El comando ipcheck muestra información detallada del sistema para Secure Web Appliance, incluidas las especificaciones de hardware, el uso del disco, las interfaces de red, las claves de software instaladas y los detalles de la versión, lo que proporciona una instantánea completa del estado actual del dispositivo.

```
<#root>
```

```
SWA LAB > ipcheck
```

```

Ipcheck Rev          1
Date                 Fri Mar 21 16:34:56 2025
Model                S100V
Platform             vmware (VMware Virtual Platform)
Secure Web Appliance Version  Version: 15.2.1-011
Build Date           2024-10-03
Install Date         2025-02-13 17:49:24
Burn-in Date         Unknown
BIOS Version         6.00
RAID Version         NA
RAID Status          Unknown
RAID Type            NA
RAID Chunk           Unknown
BMC Version          NA
Disk 0               200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
Disk Total           200GB

Root                 4GB 64%

Nextroot             4GB 65%

Var                  400MB 38%

Log                  130GB 24%

DB                   2GB 0%

Swap                 8GB
Proxy Cache          50GB
RAM Total            8192M

```

## velocidad

El comando rate imprime las velocidades de conexión y el número de solicitudes por segundo para cada 10 segundos .

<#root>

```

SWA LAB> rate
Press Ctrl-C to stop.

```

%proxy	reqs		client	server	%bw	disk	disk		
CPU	/sec	hits	blocks	misses	kb/sec	kb/sec	saved	wrs	rds
100.00	1800	17	16352	1626	178551	178551	0.0	2366	0

100.00	1813	18	16453	1659	226301	224952	0.6	3008	0
99.00	1799	10	16338	1645	206234	206234	0.0	3430	1

## Recopilación de registros para una latencia alta

Depende de la sección en la que esté viendo un tiempo de respuesta alto de los registros de acceso o una carga de proceso alta de los registros SHD. Para obtener más información sobre la solución de problemas, es mejor cambiar la suscripción de registro correspondiente a Debug.

---



Advertencia: Establecer el nivel de registro para depurar o rastrear puede aumentar el uso de los recursos y hacer que los archivos de registro giren o se sobrescriban rápidamente.

---

Campo de registro de acceso	Campo de registro SHD	Suscripción a registro correspondiente
Respuesta de autenticación , total de autenticación	—	authlogs
Respuesta DNS, total DNS	—	system_logs
Respuesta WBRS, total WBRS	Wbrs_WucLd	póngase en contacto con el TAC de Cisco
Respuesta AVC, total AVC	—	avc_logs
Respuesta de McAfee, total de McAfee	McafeeLd	mcafee_logs
Respuesta de Sophos, total de Sophos	SophosLd	sophos_logs
Respuesta de Webroot, total de Webroot	WebrootLd	webrootlogs
Respuesta de AMP, total de AMP	AMPLd	amp_logs

## Información Relacionada

[Solución de problemas de rendimiento de appliances web seguros con registros SHD](#)

[Acceder a registros de appliances web seguros](#)

[Configuración de la captura de paquetes en el dispositivo de seguridad de contenido](#)

[Uso de las prácticas recomendadas de Secure Web Appliance](#)

[Configurar el parámetro de rendimiento en registros de acceso](#)

[Solución de problemas de estados de proceso inusuales en SWA](#)

[Determinación de la tasa de descifrado en SWA](#)

[Solucionar problemas del servicio DNS de dispositivo web seguro](#)

[Acceder a registros de appliances web seguros](#)

## 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).