Uso de las prácticas recomendadas de Secure Web Appliance

Contenido

Introducción

En este documento se describen las prácticas recomendadas para configurar Cisco Secure Web Appliance (SWA).

Antecedentes

Esta guía está pensada como referencia para la configuración de prácticas recomendadas y aborda muchos aspectos de una implementación de SWA, incluidos el entorno de red compatible, la configuración de políticas, la supervisión y la resolución de problemas. Aunque las prácticas recomendadas que se describen

aquí son importantes para que las entiendan todos los administradores, arquitectos y operadores, solo son directrices y deben tratarse como tales. Cada red tiene sus propios requisitos y retos específicos.

Como dispositivo de seguridad, el SWA interactúa con la red de varias formas exclusivas. Es tanto un origen como un destino del tráfico web; actúa al mismo tiempo como un servidor web y un cliente web. Como mínimo, emplea técnicas de simulación de direcciones IP en el servidor y técnicas de "man-in-the-middle" para inspeccionar transacciones HTTPS. También puede falsificar direcciones IP de cliente, lo que añade otra capa de complejidad a la implementación e impone requisitos adicionales a la configuración de red auxiliar. Esta guía aborda los problemas más comunes relacionados con la configuración del dispositivo de red relacionado.

La configuración de la política SWA tiene implicaciones no solo para la eficacia y la aplicación de la seguridad, sino también para el rendimiento del dispositivo. Esta guía explica cómo la complejidad de una configuración afecta a los recursos del sistema. Define la complejidad en este contexto y describe cómo minimizarla en el diseño de políticas. También se presta atención a las funciones específicas y a cómo deben configurarse para aumentar la seguridad, la escalabilidad y la eficacia.

En la sección Supervisión y alertas de este documento se explican las formas más eficaces de supervisar el dispositivo. También se describe la supervisión del rendimiento y la disponibilidad, así como el uso de los recursos del sistema. También proporciona información útil para la resolución de problemas básicos.

Entorno de red

ICMP

Path MTU Discovery, como se define en RFC 1191, El mecanismo determina el tamaño máximo de un paquete a lo largo de las trayectorias arbitrarias. En el caso de IPv4, un dispositivo puede determinar la unidad de transmisión máxima (MTU) de cualquier paquete a lo largo de una ruta mediante la configuración del bit Donâ€™t Fragment (DF) en el encabezado IP del paquete. Si, en algún link a lo largo de la trayectoria, un dispositivo no puede reenviar el paquete sin fragmentarlo, un mensaje de **Fragmentación necesaria del Protocolo de mensajes de control de Internet (ICMP) (tipo 3, código 4)** se devuelve al origen. El cliente entonces reenvía un paquete más pequeño. Esto continúa hasta que se descubre la MTU para la trayectoria completa. IPv6 no admite la fragmentación y utiliza un mensaje ICMPv6 de paquete demasiado grande (tipo 2) para indicar la incapacidad de encajar un paquete a través de un vínculo determinado.

Debido a que el proceso de fragmentación de paquetes puede tener un impacto severo en el rendimiento de un flujo TCP, el SWA utiliza Path MTU Discovery. Los mensajes ICMP mencionados deben estar habilitados en los dispositivos de red relevantes para permitir que el SWA determine la MTU para su trayectoria a través de la red. Este comportamiento se puede inhabilitar en el SWA que utiliza el comando pathmtudiscovery **command-line interface (CLI)**. Esto hace que la MTU predeterminada descienda a 576 bytes (según RFC 879), lo que afecta seriamente al rendimiento. El administrador debe realizar el paso adicional de configurar manualmente la MTU en el SWA de etherconfig CLI.

En el caso del **protocolo de comunicación de caché web (WCCP)**, el tráfico web se redirige al SWA desde otro dispositivo de red a lo largo de la ruta del cliente a Internet. En este caso, otros protocolos, como ICMP, no se redirigen al SWA. Existe la posibilidad de que el SWA pueda activar un mensaje ICMP Fragmentation Needed de un router de la red, pero el mensaje no se entregará al SWA. Si esto es una posibilidad en la red,

la Detección de MTU de Trayectoria debe estar inhabilitada. Como se mencionó, con esta configuración, el paso adicional de configurar manualmente la MTU en el SWA de etherconfig El comando CLI es obligatorio.

Firewalls

En una configuración predeterminada, el SWA no falsifica la dirección IP del cliente al realizar el proxy de una conexión. Esto significa que todo el tráfico web saliente se origina en la dirección IP SWA. Es necesario asegurarse de que los dispositivos de **traducción de direcciones de red (NAT)** tengan un grupo de direcciones y puertos externos lo suficientemente grande como para admitir esto. Es una buena idea dedicar una dirección específica para este propósito.

Algunos firewalls emplean protecciones **de denegación de servicio (DoS)** u otras funciones de seguridad que se activan cuando un gran número de conexiones simultáneas se originan en una única dirección IP de cliente. Cuando la suplantación de IP de cliente no está habilitada, la dirección IP SWA debe excluirse de estas protecciones.

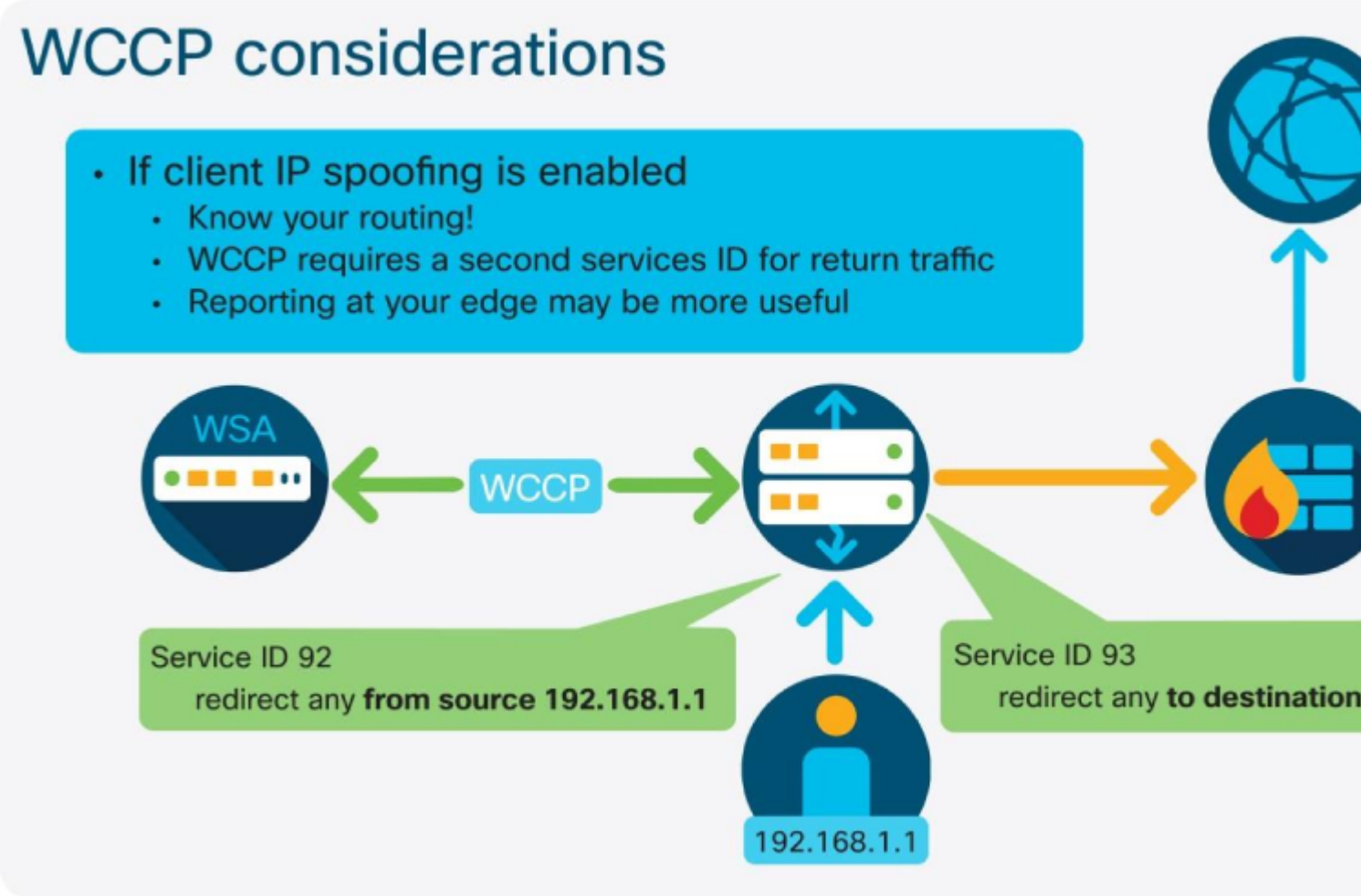
Unicast Reverse Path Forwarding

El SWA falsifica la dirección IP del servidor cuando se comunica con un cliente, y opcionalmente se puede configurar para falsificar la dirección IP del cliente cuando se comunica con un servidor ascendente. Las protecciones como **Unicast Reverse Path Forwarding (uRPF)** se pueden habilitar en los switches para garantizar que un paquete entrante coincida con el puerto de ingreso esperado. Estas protecciones verifican la interfaz de origen de un paquete contra la tabla de ruteo para asegurarse de que llegó al puerto esperado. El SWA debe quedar exento de estas protecciones cuando proceda.

Suplantación de IP con WCCP

Cuando la función de suplantación de IP está activada en el SWA, las solicitudes salientes dejan que el dispositivo utilice la dirección de origen de la solicitud de cliente original. Esto requiere una configuración adicional de la infraestructura de red relacionada para garantizar que los paquetes de retorno se enruten a la interfaz de salida SWA, en lugar del cliente que originó la solicitud.

Cuando se implementa WCCP en un dispositivo de red (router, switch o firewall), se define un ID de servicio que coincide con el tráfico según una **lista de control de acceso (ACL)**. A continuación, el ID de servicio se aplica a una interfaz y se utiliza para hacer coincidir el tráfico para su redirección. Si se habilita la suplantación de IP, se debe crear un segundo ID de servicio para garantizar que el tráfico de retorno también se redirija al SWA.



Configuración de red SWA

Interfaces

El SWA tiene cinco interfaces de red utilizables: M1, P1, P2, T1 y T2. Cada uno de ellos debe ser aprovechado para su propósito específico siempre que sea posible. Es conveniente utilizar cada puerto por sus propios motivos. La interfaz M1 debe estar conectada a una red de administración dedicada y se debe habilitar el ruteo dividido para limitar la exposición de los servicios administrativos. El P1 se puede limitar al tráfico de solicitudes de clientes. Por el contrario, el P2 no puede aceptar solicitudes de proxy explícitas. Esto reduce la cantidad de tráfico en cada interfaz y permite una mejor segmentación en el diseño de la red.

Los puertos T1 y T2 están disponibles para la función **Monitor de tráfico de capa 4 (L4TM)**. Esta función supervisa un puerto de capa 2 duplicado y añade la capacidad de bloquear el tráfico basándose en una lista bloqueada de direcciones IP y nombres de dominio malintencionados conocidos. Para ello, observa las direcciones IP de origen y de destino del tráfico y envía un paquete de restablecimiento de TCP o un mensaje de puerto inalcanzable si la lista de bloqueados coincide. El tráfico enviado con cualquier protocolo se puede bloquear con esta función.

Incluso si la función L4TM no está habilitada, la derivación transparente se puede mejorar cuando los puertos T1 y T2 están conectados a un puerto reflejado. En el caso de WCCP, el SWA solo conoce la dirección IP de origen y destino de un paquete entrante y debe tomar la decisión de proxy o de omitirlo en función de esa información. El SWA resuelve todas las entradas de la lista de configuración de desvío cada 30 minutos, independientemente del **tiempo de vida (TTL) del** registro. Sin embargo, si la función L4TM

está activada, el SWA puede utilizar consultas DNS snooped para actualizar estos registros con mayor frecuencia. Esto reduce el riesgo de un falso negativo en un escenario donde el cliente ha resuelto una dirección diferente del SWA.

Routing de red de administración

Si la red de administración dedicada no tiene acceso a Internet, cada servicio se puede configurar para utilizar la tabla de ruteo de datos. Esto se puede adaptar para adaptarse a la topología de la red, pero en general, se recomienda utilizar la red de gestión para todos los servicios del sistema y la red de datos para el tráfico del cliente. A partir de la versión 11.0 de AsyncOS, los servicios para los cuales se puede establecer el ruteo son:

- Fuentes de URL externas
- Reputación y análisis de archivos de **protección frente a malware avanzado (AMP)**
- Actualizaciones y mejoras
- DNS
- Directorio activo

Para el filtrado de salida adicional del tráfico de gestión, se pueden configurar direcciones estáticas para su uso en estos servicios:

- Fuentes de URL externas:
  1. La personalización depende de dónde se alojan
  2. Reputación y análisis de archivos de AMP
  3. cloud-sa.amp.cisco.com (América del Norte)
  4. cloud-sa.eu.amp.cisco.com (Europa)
  5. cloud-sa.apjc.amp.cisco.com (Asia Pacífico)

- Actualizaciones y mejoras:
  1. downloads-static.ironport.com
  2. updates-static.ironport.com

Telemetría TALOS

El grupo Cisco Talos es conocido por identificar amenazas nuevas y emergentes. Todos los datos enviados a Talos son anónimos y almacenados en los Data Centers de EE. UU. La participación en SensorBase mejora la categorización y la identificación de amenazas web y conduce a una mejor protección frente a SWA, así como a otras soluciones de seguridad de Cisco.

DNS

Las prácticas recomendadas de seguridad del Servidor de nombres de dominio (DNS) sugieren que cada red debe alojar dos solucionadores DNS: uno para los registros autoritativos de un dominio local y otro para la resolución recursiva de dominios de Internet. Para ello, el SWA permite configurar servidores DNS para dominios específicos. Si sólo hay un servidor DNS disponible para las consultas locales y recursivas, tenga en cuenta la carga adicional que agrega cuando se utiliza para todas las consultas SWA. La mejor opción puede ser utilizar la resolución interna para dominios locales y la resolución raíz de Internet para dominios externos. Esto depende del perfil de riesgo y la tolerancia del administrador.

De forma predeterminada, el SWA almacena en caché un registro DNS durante un mínimo de 30 minutos, independientemente del TTL del registro. Los sitios web modernos que hacen un uso intensivo de las **redes de distribución de contenido (CDN)** tienen registros TTL bajos, ya que sus direcciones IP cambian con frecuencia. Esto podría dar lugar a que un cliente almacene en caché una dirección IP para un servidor determinado y que el SWA almacene en caché una dirección diferente para el mismo servidor. Para

contrarrestar esto, el TTL predeterminado SWA se puede reducir a cinco minutos desde estos comandos CLI:

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

Los servidores DNS secundarios deben configurarse en caso de que el principal no esté disponible. Si todos los servidores están configurados con la misma prioridad, la IP del servidor se elige aleatoriamente. Dependiendo del número de servidores configurados, el tiempo de espera para un servidor determinado varía. La tabla es el tiempo de espera para una consulta de hasta seis servidores DNS:

Número de servidores DNS	**Tiempo de espera de consulta (en secuencia)**
1	60
2	5, 45
3	5, 10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

También hay opciones de DNS avanzadas disponibles sólo a través de la CLI. Estas opciones están disponibles en CLI:

advancedproxyconfig > DNS comando. Seleccione una de estas opciones:

- 0: utilice siempre las respuestas DNS en orden
- 1: utilice la dirección suministrada por el cliente y luego DNS
- 2: uso limitado de DNS
- 3: uso muy limitado de DNS

Para las opciones 1 y 2, se utiliza DNS si Web Reputation está activado.

Para las opciones 2 y 3, DNS se utiliza para las solicitudes de proxy explícitas, si no hay un proxy upstream o en el caso de que falle el proxy upstream configurado.

Para todas las opciones, DNS se utiliza cuando las direcciones IP de destino se utilizan en la pertenencia a políticas.

Estas opciones controlan cómo el SWA decide la dirección IP a la que conectarse al evaluar una solicitud de cliente. Cuando se recibe una solicitud, el SWA ve una dirección IP de destino y un nombre de host. El SWA debe decidir si confía en la dirección IP de destino original para la conexión TCP o si realiza su propia resolución DNS y utiliza la dirección resuelta. El valor predeterminado es "0 = Utilizar siempre las respuestas DNS en orden", lo que significa que el SWA no confía en que el cliente proporcione la dirección IP.

- Opción 1: el SWA prueba la dirección IP proporcionada por el cliente para la conexión, pero vuelve a la dirección resuelta si falla. La dirección resuelta se utiliza para la evaluación de políticas (categoría web, reputación web y demás).
- Opción 2: el SWA solo utiliza la dirección proporcionada por el cliente para la conexión y no retrocede. La dirección resuelta se utiliza para la evaluación de políticas (categoría web, reputación web, etc.).
- Opción 3: el SWA solo utiliza la dirección proporcionada por el cliente para la conexión y no retrocede. La dirección IP proporcionada por el cliente se utiliza para la evaluación de políticas (categoría web, reputación web, etc.).

La opción elegida depende de cuánta confianza debe depositar el administrador en el cliente al determinar la dirección resuelta para un nombre de host determinado. Si el cliente es un proxy de flujo descendente, elija la opción 3 para evitar la latencia añadida de búsquedas de DNS innecesarias.

Equilibrio de carga

WCCP permite un equilibrio de carga de tráfico transparente cuando se utilizan hasta ocho dispositivos. Permite equilibrar los flujos de tráfico basados en hash o máscara, se puede ponderar en caso de que haya una mezcla de modelos de dispositivos en la red y se pueden agregar y eliminar dispositivos del grupo de servicios sin tiempo de inactividad. Una vez que la necesidad excede lo que se puede manejar con ocho SWA, se recomienda utilizar un balanceador de carga dedicado.

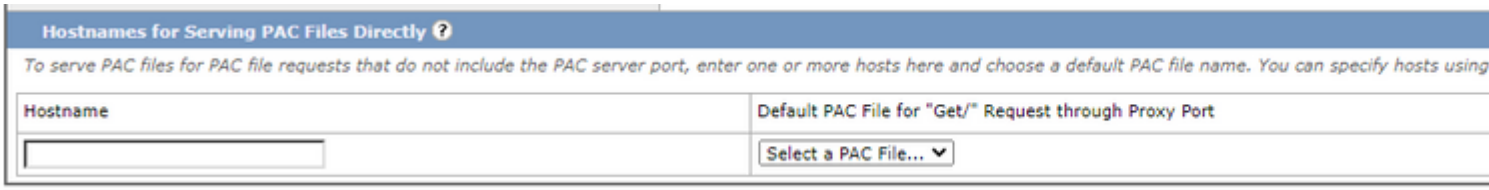
Las prácticas recomendadas específicas para la configuración de WCCP varían en función de la plataforma utilizada. Para los switches Cisco Catalyst®, las prácticas recomendadas se documentan en el informe técnico de la solución Cisco Catalyst Instant Access.

WCCP tiene limitaciones cuando se utiliza con un dispositivo de seguridad adaptable de Cisco (ASA). Es decir, no se admite la suplantación de IP de cliente, y los clientes y SWA deben estar detrás de la misma interfaz. Por esta razón, es más flexible utilizar un switch o router de capa 4 para redirigir el tráfico. La configuración de WCCP en la plataforma ASA se describe en WCCP en ASA: Conceptos, Limitaciones y Configuración.

Para implementaciones explícitas, el método más implementado es un archivo de configuración automática de proxy (PAC), pero tiene muchos inconvenientes y consecuencias de seguridad que están fuera del alcance de este documento. Si se implementa un archivo PAC, se recomienda utilizar objetos de directiva de grupo (GPO) para configurar la ubicación en lugar de confiar en el Protocolo de detección automática de proxy web (WPAD), que es un destino común de los atacantes y que se puede explotar fácilmente si se configura incorrectamente. El SWA puede alojar varios archivos PAC y controlar su caducidad en la caché del navegador.

Se puede solicitar un archivo PAC directamente desde el SWA desde un número de puerto TCP

configurable (9001 de forma predeterminada). Si no se especifica un puerto, la solicitud se puede enviar al propio proceso proxy como si fuera una solicitud web saliente. En este caso, es posible suministrar un archivo PAC específico basado en el encabezado de host HTTP presente en la solicitud.



Kerberos se debe configurar de manera diferente cuando se utiliza en un entorno de alta disponibilidad. El SWA proporciona soporte para archivos keytab, que permite que varios nombres de host se asocien con un **nombre de principio de servicio (SPN)**. Para obtener más información, vea Crear una cuenta de servicio en Windows Active Directory para la autenticación Kerberos en implementaciones de alta disponibilidad .

Autenticación activa

Kerberos es un protocolo de autenticación más seguro y ampliamente admitido que el **proveedor de soporte de seguridad de NT LAN Manager (NTLMSSP)**. El sistema operativo Apple OS X no admite NTLMSSP, pero puede usar Kerberos para autenticarse si el dominio se ha unido. No se debe utilizar la autenticación básica, ya que envía credenciales sin cifrar en el encabezado HTTP y un atacante de la red puede rastrearlas fácilmente. Si se debe utilizar la autenticación básica, se debe habilitar el cifrado de credenciales para garantizar que las credenciales se envían a través de un túnel cifrado.

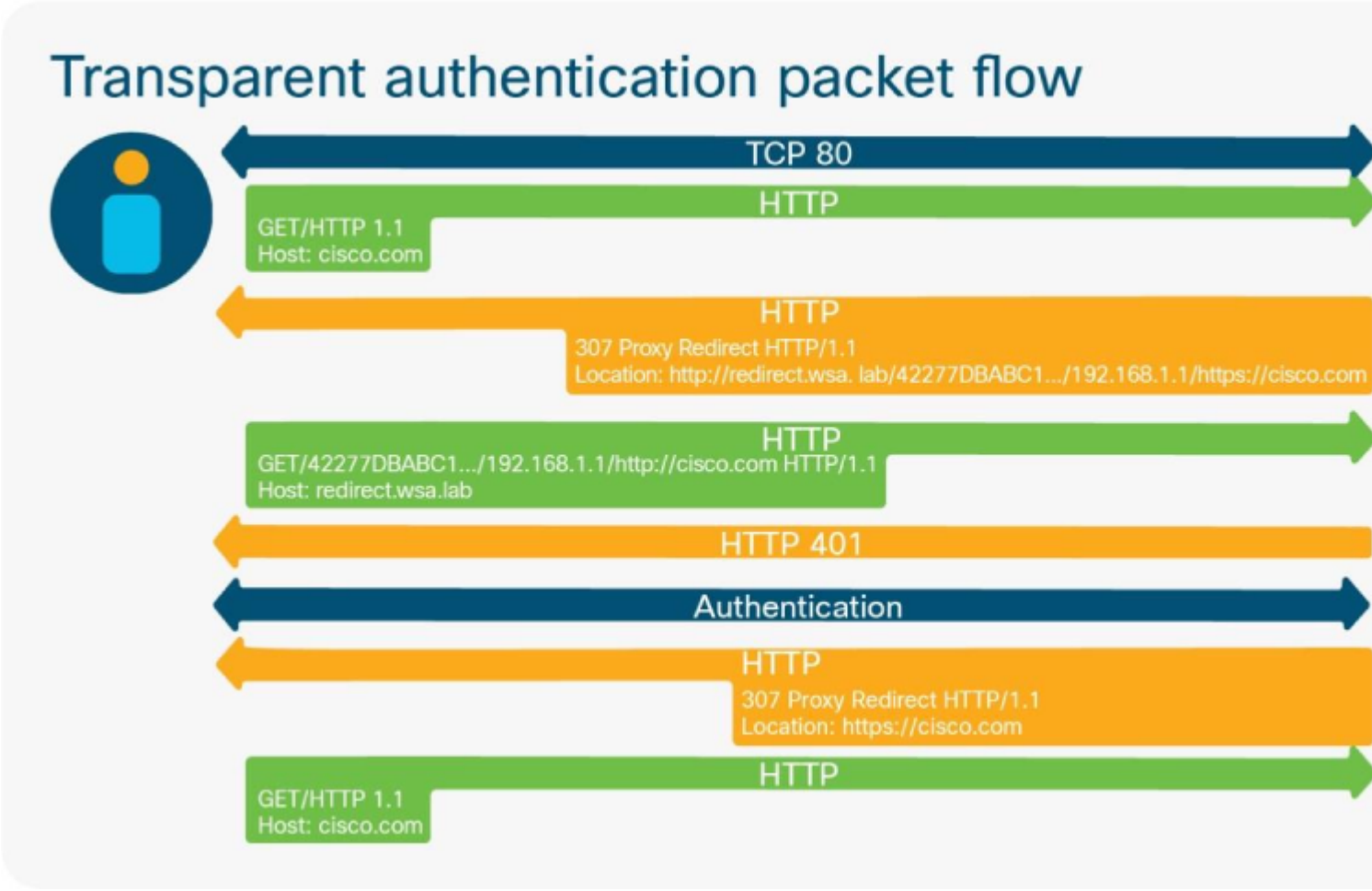
Se debe agregar más de un controlador de dominio a la configuración para garantizar la disponibilidad, pero no existe un equilibrio de carga inherente para este tráfico. El SWA envía un paquete SYN TCP a todos los controladores de dominio configurados y el primero en responder se utiliza para la autenticación.

El "nombre de host de redirección" que se configura en la página de configuración de autenticación determina dónde se envía un cliente transparente para completar la autenticación. Para que un cliente de Windows complete la autenticación integrada y logre el **inicio de sesión único (SSO)**, el nombre de host de redirección debe estar en la zona "Sitios de confianza" del panel de control "Opciones de Internet". El protocolo Kerberos requiere que el **nombre de dominio completo (FQDN)** se utilice para especificar un recurso, lo que significa que el nombre "shortname" (o "NETBIOS") no se puede utilizar si Kerberos es el mecanismo de autenticación previsto. El FQDN debe agregarse manualmente a los "Sitios de confianza" (por ejemplo, mediante la directiva de grupo). Además, el inicio de sesión automático con nombre de usuario y contraseña debe configurarse en el panel de control "Opciones de Internet".

Firefox también requiere una configuración adicional para que el explorador complete la autenticación con proxies de red. Estos parámetros se pueden configurar en la página **about:config**. Para que Kerberos se complete correctamente, el nombre de host de redirección debe agregarse a la opción **network.negotiate-auth.trusted-uris**. Para NTLMSSP, se debe agregar a la opción **network.automatic-ntlm-auth.trusted-uris**.

Los sustitutos de autenticación se utilizan para recordar a un usuario autenticado durante un período establecido después de que se haya completado la autenticación. Siempre que sea posible, se deben utilizar sustitutos IP para limitar el número de eventos de autenticación activos que se producen. La autenticación activa de un cliente es una tarea que consume muchos recursos, especialmente cuando se utiliza Kerberos. El tiempo de espera sustituto es de 3600 segundos (una hora) de forma predeterminada y se puede reducir, pero el valor mínimo recomendado es de 900 segundos (15 minutos).

Esta imagen muestra cómo se utiliza "redirect.WSA.lab" como nombre de host de redirección.



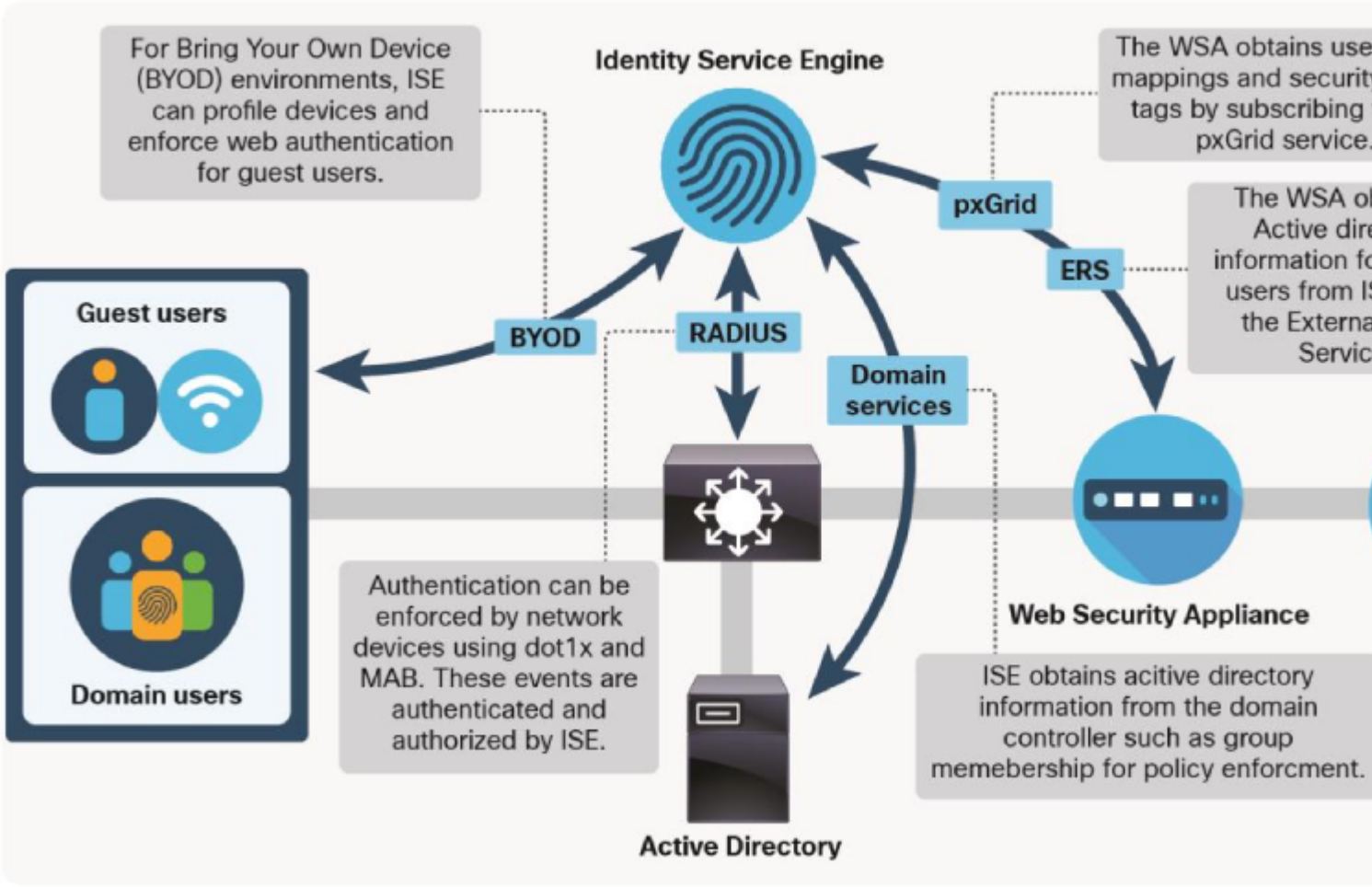
Autenticación pasiva

El SWA puede aprovechar otras plataformas de seguridad de Cisco para identificar de forma pasiva a los usuarios de proxy. La identificación pasiva de los usuarios elimina la necesidad de un desafío de autenticación directo y cualquier comunicación de Active Directory desde el SWA, lo que a su vez reduce la latencia y el uso de recursos en el dispositivo. Los mecanismos disponibles actualmente para la autenticación pasiva son el **agente de directorio de contexto (CDA)**, **Identity Services Engine (ISE)** y el conector de identidad pasiva de **Identity Services Connector (ISE-PIC)**.

ISE es un producto con numerosas funciones que ayuda a los administradores a centralizar sus servicios de autenticación y a aprovechar un amplio conjunto de controles de acceso a la red. Cuando ISE obtiene información sobre un evento de autenticación de usuario (ya sea a través de la autenticación Dot1x o de la redirección de autenticación web), rellena una base de datos de sesión que contiene información sobre el usuario y el dispositivo implicados en la autenticación. El SWA se conecta a ISE a través de **Platform Exchange Grid (pxGrid)** y obtiene el nombre de usuario, la dirección IP y la etiqueta de grupo de seguridad (SGT) asociados a una conexión proxy. Desde la versión 11.7 de AsyncOS, el SWA también puede consultar el **servicio de restauración externa (ERS)** en ISE para obtener información de grupo.

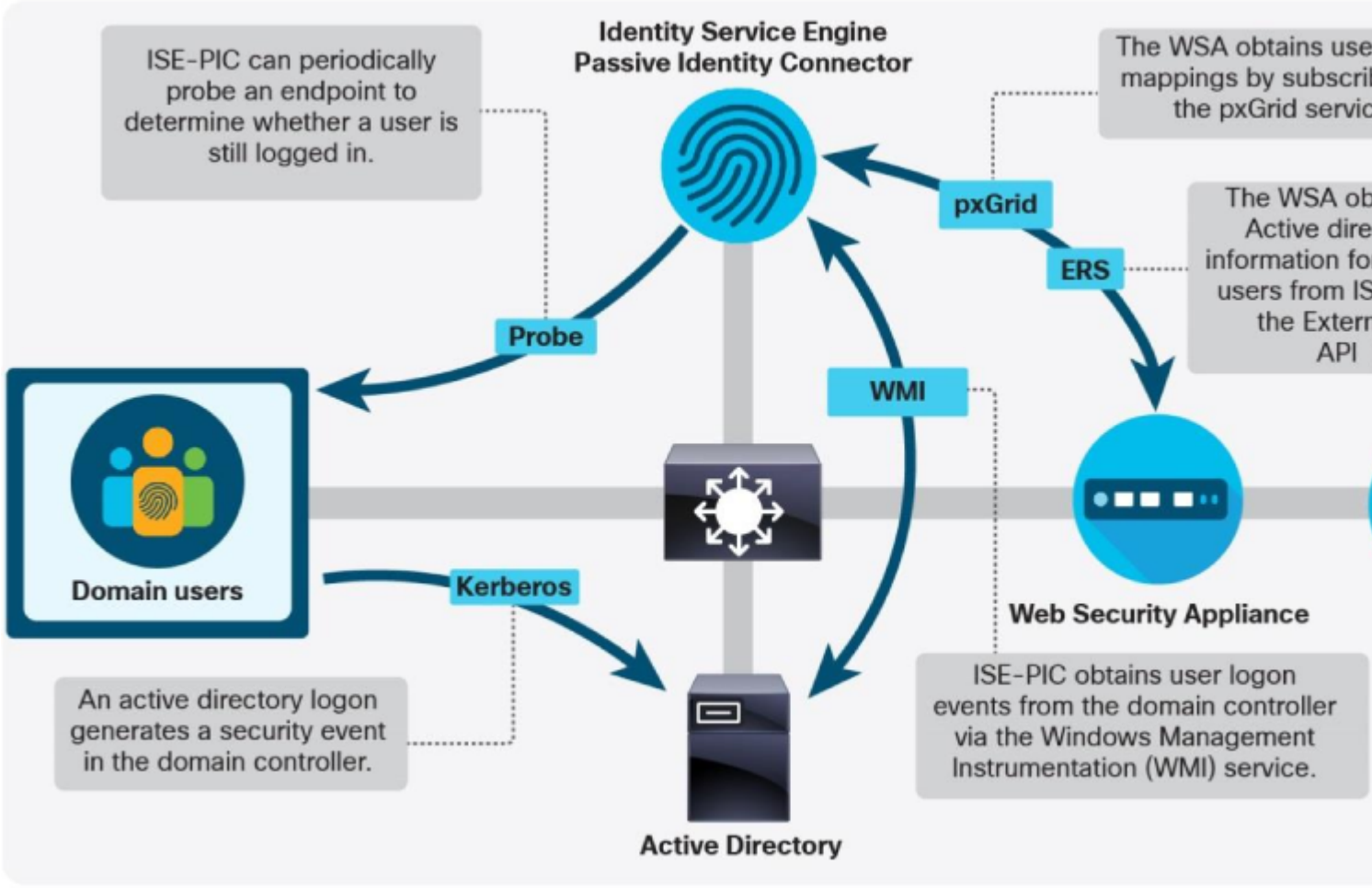
Las versiones sugeridas son ISE 3.1 y SWA 14.0.2-X y posteriores. Para obtener más información sobre la matriz de compatibilidad de ISE para SWA, consulte Matriz de compatibilidad de ISE para Secure Web Appliance .

Para obtener más información sobre los pasos completos de la integración, consulte la Guía del usuario final del dispositivo de seguridad web.



Cisco anuncia el fin del ciclo de vida del software Cisco Context Directory Agent (CDA). Consulte Cisco Context Directory Agent (CDA).

A partir del parche 6 de CDA, es compatible con Microsoft Server 2016. Sin embargo, se recomienda activamente a los administradores que migren sus implementaciones de CDA a ISE-PIC. Ambas soluciones utilizan WMI para suscribirse al Registro de eventos de seguridad de Windows con el fin de generar asignaciones de usuario a IP (conocidas como "sesiones"). En el caso de CDA, el SWA consulta estas asignaciones con RADIUS. En el caso de ISE-PIC, se utilizan las mismas conexiones PxGrid y ERS que en la implementación completa de ISE. La funcionalidad de ISE-PIC está disponible en una instalación completa de ISE, así como en un appliance virtual independiente.

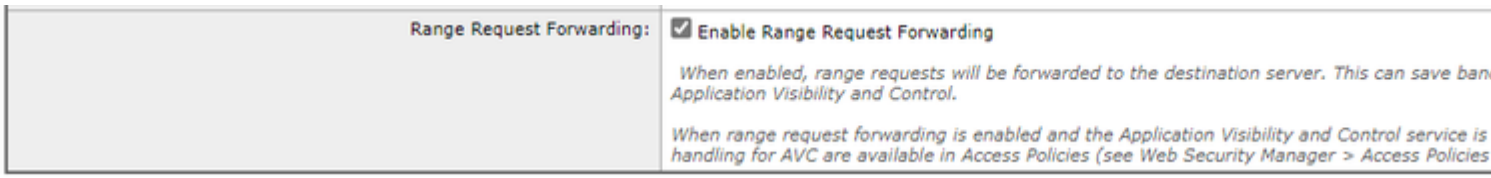


Configuración de servicios

Proxy web

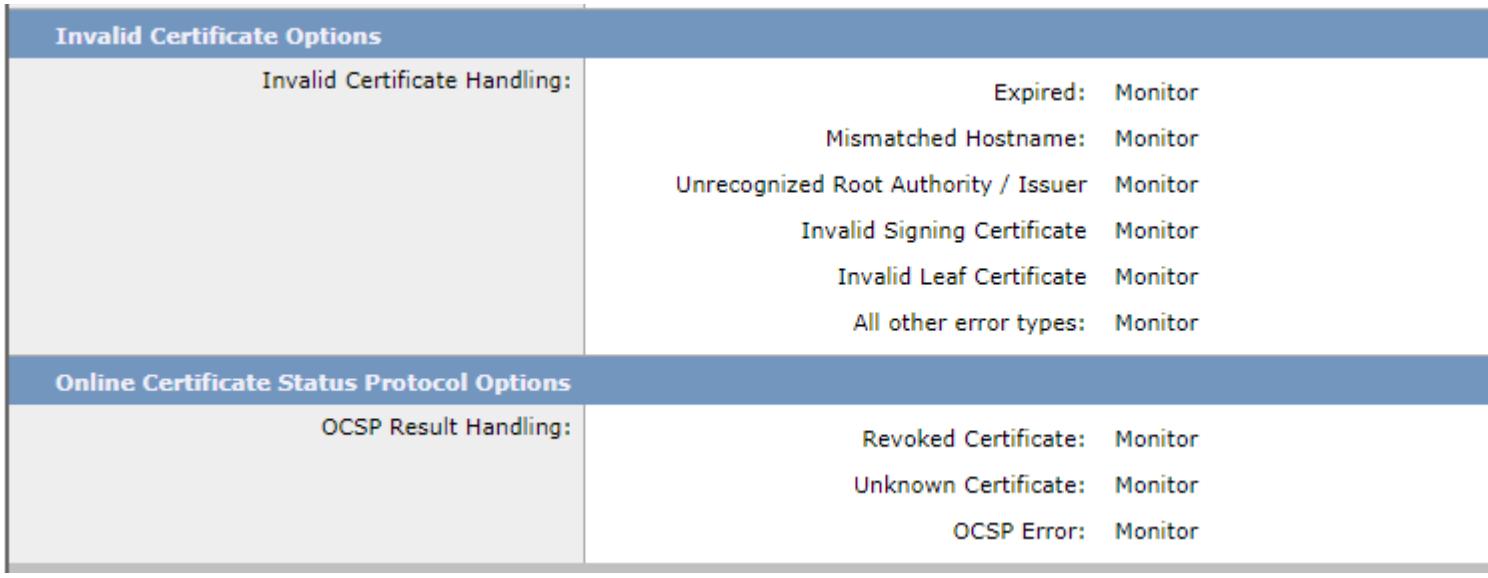
El almacenamiento en caché debe estar habilitado en la configuración del proxy web para ahorrar ancho de banda y aumentar el rendimiento. Esto es cada vez menos importante a medida que aumenta el porcentaje de tráfico HTTPS porque el SWA no almacena en caché de forma predeterminada las transacciones HTTPS. Si el proxy se implementa para servir sólo a clientes explícitos, se debe especificar el modo de reenvío para rechazar cualquier tráfico que no esté específicamente destinado al servicio de proxy. De este modo, se reduce la superficie de ataque del dispositivo y se practica un buen principio de seguridad: apáguelo si no es necesario.

Los encabezados de solicitud de rango se utilizan en las solicitudes HTTP para especificar el rango de bytes de un archivo que se va a descargar. Es comúnmente utilizado por el sistema operativo y los demonios de actualización de la aplicación para transferir pequeñas porciones de un archivo a la vez. De forma predeterminada, el SWA elimina estos encabezados para que pueda obtener el archivo completo con fines de análisis antivirus (antivirus), reputación y análisis de archivos, y **control de visibilidad de la aplicación (AVC)**. Si se habilita el reenvío de encabezados de solicitud de intervalo globalmente en la configuración de proxy, los administradores pueden crear políticas de acceso individuales que reenvíen o eliminen dichos encabezados. Para obtener más información sobre esta configuración, consulte la sección **Políticas de acceso**.



Proxy HTTPS

Las prácticas recomendadas de seguridad sugieren que las claves privadas deben generarse en el dispositivo en el que se utilizan y nunca deben transportarse a otro lugar. El asistente para proxy HTTPS permite la creación del par de claves y el certificado utilizados para el descifrado de las conexiones de **seguridad de la capa de transporte (TLS)**. La **Solicitud de firma de certificado (CSR)** se puede descargar y firmar por una **Autoridad de certificación (CA)** interna. En un entorno de **Active Directory (AD)**, este es el mejor método, ya que todos los miembros del dominio confían automáticamente en una CA integrada en AD y no se requieren pasos adicionales para implementar el certificado.
Una función de seguridad del proxy HTTPS es validar los certificados del servidor. Las prácticas recomendadas sugieren que los certificados no válidos requieren que se descarte la conexión. La habilitación del descifrado para EUN permite que SWA presente una página de bloqueo explicando la razón del bloqueo. Si no se activa esta opción, los sitios HTTPS bloqueados provocarán un error en el navegador. Esto conlleva un aumento de los tickets del soporte técnico y la suposición por parte del usuario de que hay algo averiado, en lugar de tener la certeza de que el SWA ha bloqueado la conexión. Todas las opciones de certificado no válidas deben configurarse como mínimo en Descifrar. Dejar cualquiera de estas opciones como Monitor no puede registrar mensajes de error útiles en caso de que los problemas de certificado impidan que se cargue un sitio.



Del mismo modo, las comprobaciones del **Protocolo de Servicios de Certificate Server en línea (OCSP)** deben dejarse habilitadas y el Monitor no debe utilizarse para ninguna opción. Los certificados revocados deben ser descartados y todos los demás deben ser al menos configurados en Descifrar para permitir el registro de mensajes de error relevantes. **El seguimiento del acceso a la información de autoridad (AIA chasing)** es un medio por el cual un cliente puede recopilar al firmante del certificado y una dirección URL desde la que se pueden obtener certificados adicionales. Por ejemplo, si una cadena de certificados recibida de un servidor está incompleta (le falta un certificado intermedio o raíz), el SWA puede comprobar el campo AIA y utilizarlo para obtener los certificados que faltan y verificar la autenticidad. Esta configuración sólo está disponible en la CLI a partir de estos comandos:

```
SWA_CLI> advancedproxyconfig
```

```
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> HTTPS
...
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
[Y]>
...
```

> **Nota**: esta configuración está habilitada de forma predeterminada y no debe deshabilitarse, ya que muchos servidores modernos dependen de este mecanismo para proporcionar una cadena de confianza completa a los clientes.

Monitor de tráfico de capa 4 (L4TM)

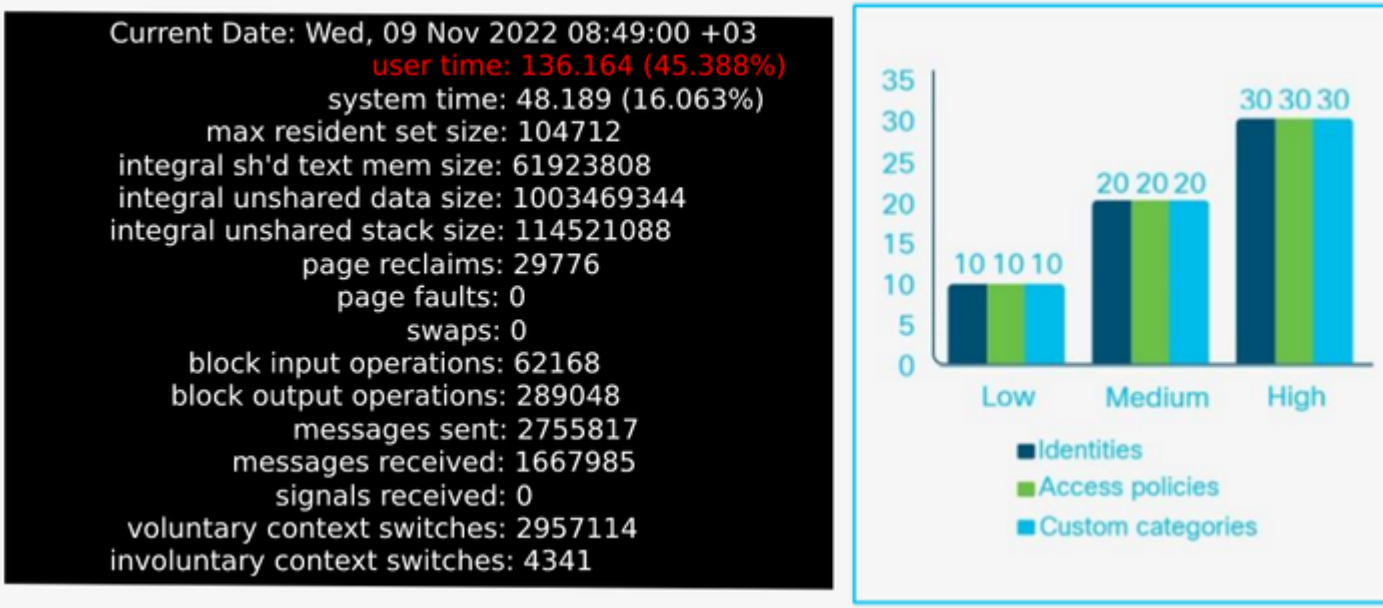
El L4TM es una forma muy eficaz de ampliar el alcance del SWA para incluir el tráfico malintencionado que no atraviesa el proxy, incluido el tráfico en todos los puertos TCP y UDP. Los puertos T1 y T2 están diseñados para conectarse a una sesión de supervisión de switch o a una toma de red, lo que permite a SWA supervisar pasivamente todo el tráfico de los clientes. Si se ve tráfico destinado a una dirección IP maliciosa, el SWA puede terminar las sesiones TCP enviando un RST mientras falsifica la dirección IP del servidor. Para el tráfico UDP, puede enviar un mensaje de Puerto inalcanzable. Al configurar la sesión de supervisión, se recomienda excluir todo el tráfico destinado a la interfaz de administración del SWA para evitar que la función pueda interferir con el acceso al dispositivo.
Además de monitorear el tráfico malicioso, el L4TM también indaga en las consultas DNS para actualizar la lista de configuración de desvío. Esta lista se utiliza en implementaciones WCCP para devolver ciertas solicitudes al router WCCP para el enrutamiento directo al servidor web. Los paquetes que coinciden con la lista de configuración de omisión no son procesados por el proxy. La lista puede contener direcciones IP o nombres de servidor. El SWA resuelve cualquier entrada de la lista de configuración de desvío cada 30 minutos, independientemente del TTL del registro. Sin embargo, si la función L4TM está activada, el SWA puede utilizar consultas DNS snooped para actualizar estos registros con mayor frecuencia. Esto reduce el riesgo de un falso negativo en un escenario donde el cliente ha resuelto una dirección diferente del SWA.

Configuración de políticas

Una configuración de políticas correcta es fundamental para el rendimiento y la escalabilidad del SWA. Esto es así no solo por la eficacia de las propias políticas a la hora de proteger a los clientes y hacer cumplir los requisitos de la empresa. La forma en que se configuran las políticas tiene un impacto directo en el uso de los recursos y en el estado y el rendimiento general del análisis de rendimiento. Un conjunto de políticas demasiado complejo o mal diseñado puede causar inestabilidad y una respuesta lenta del dispositivo.

Complejidad

En la elaboración de las políticas de los enfoques sectoriales se utilizan diversos elementos normativos. El archivo XML que se genera a partir de la configuración se utiliza para crear varios archivos de configuración back-end y reglas de acceso. Cuanto más compleja sea la configuración, más tiempo tendrá el proceso proxy para evaluar los diversos conjuntos de reglas de cada transacción. En la evaluación comparativa y el dimensionamiento del SWA, se crea un conjunto básico de elementos de políticas que representan tres niveles de complejidad de la configuración. Diez perfiles de identidad, políticas de descifrado y políticas de acceso, junto con diez categorías personalizadas que contienen diez entradas de expresiones regulares, cincuenta direcciones IP de servidor y 420 nombres de host de servidor, se considera una configuración de baja complejidad. Al multiplicar cada una de estas cifras por dos y tres, se obtiene una configuración de complejidad media y alta, respectivamente.
Cuando una configuración se vuelve demasiado compleja, los primeros síntomas suelen incluir una respuesta lenta en la interfaz web y la CLI. No puede haber un impacto significativo en los usuarios al principio. Pero cuanto más compleja es la configuración, más tiempo debe pasar el proceso proxy en modo usuario. Debido a esto, verificar el porcentaje de tiempo empleado en este modo puede ser una manera útil de diagnosticar una configuración excesivamente compleja como la causa de un SWA lento.
El tiempo de CPU, en segundos, se registra en el registro track_stats cada cinco minutos. Esto significa que el porcentaje de tiempo del usuario se puede calcular como (tiempo del usuario + tiempo del sistema)/300. A medida que el tiempo del usuario se acerca a 270, el proceso está gastando demasiados ciclos de CPU en modo de usuario, y esto se debe casi siempre a que la configuración es demasiado compleja para analizarla de manera eficiente.



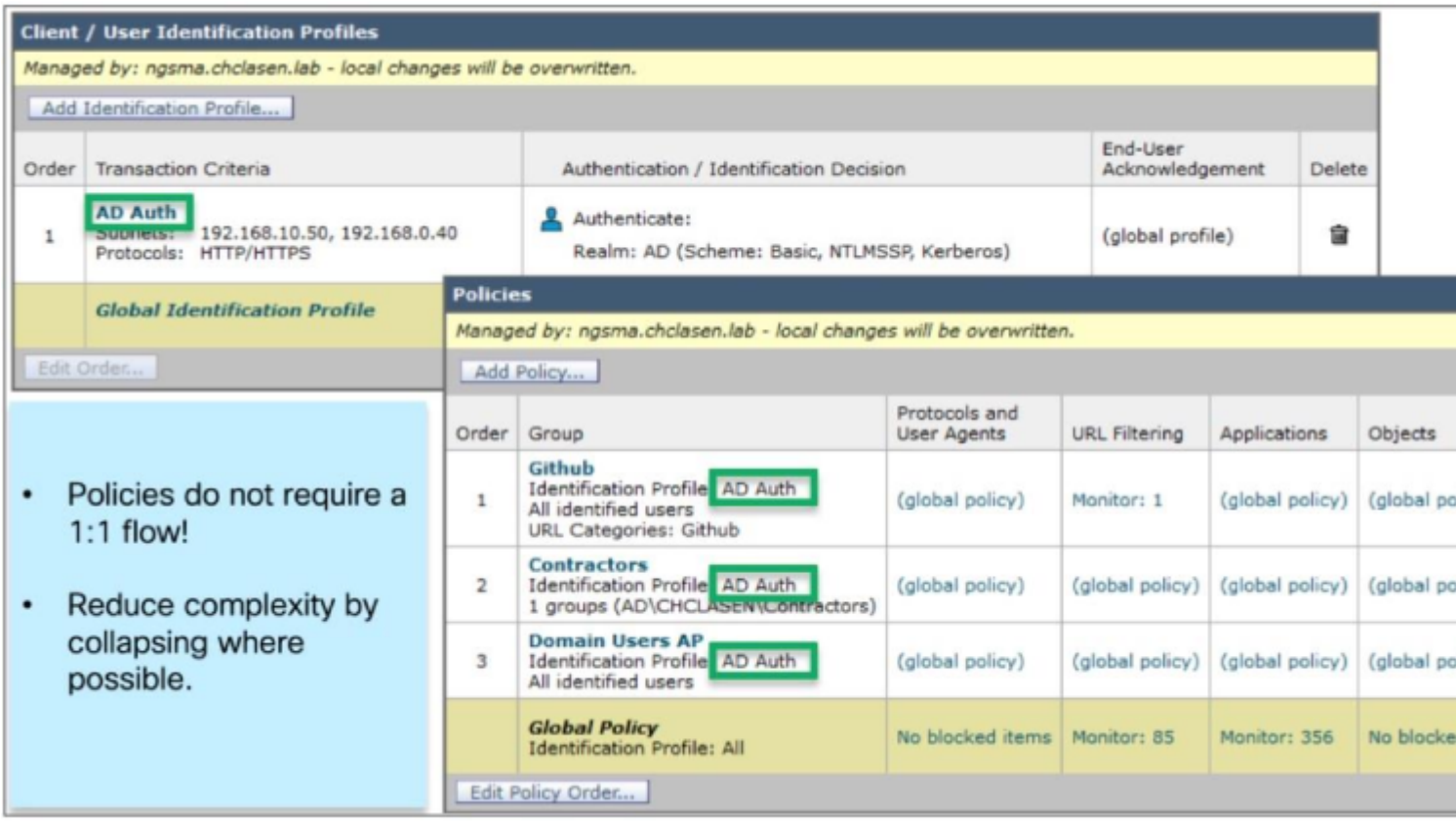
Perfiles de identificación

Los perfiles de identificación (ID) son los primeros elementos de política que se evalúan cuando se recibe una nueva solicitud. Toda la información configurada en la primera sección del perfil de ID se evalúa con un AND lógico. Esto significa que todos los criterios deben coincidir para que la solicitud coincida con el perfil. Al crear una política, solo debe ser tan específica como sea absolutamente necesario. Los perfiles que incluyen direcciones de host individuales casi nunca son necesarios y pueden dar lugar a configuraciones dispersas. Aprovechar la cadena de usuario-agente que se encuentra en los encabezados HTTP, la lista de categorías personalizadas o la subred suele ser una mejor estrategia para limitar el alcance de un perfil.

En general, las políticas que requieren autenticación se configuran en la parte inferior y las excepciones se agregan en la parte superior. Al solicitar directivas que no requieren autenticación, las directivas más

utilizadas deben estar lo más cerca posible de la parte superior. No confíe en la autenticación fallida para restringir el acceso. Si se sabe que un cliente de la red no puede autenticarse en un proxy, debe estar exento de autenticación y bloqueado en las directivas de acceso. Los clientes que no pueden autenticarse de forma repetida envían solicitudes no autenticadas al SWA, que utilizan recursos y pueden provocar una utilización excesiva de la CPU y la memoria.

Un error habitual de los administradores es que debe haber un perfil de ID único y la correspondiente política de descifrado y política de acceso. Esta es una estrategia ineficiente para la configuración de políticas. Siempre que sea posible, las políticas deben estar "contraídas" para que un único perfil de ID se pueda asociar con varias políticas de acceso y descifrado. Esto es posible porque todos los criterios en una política dada deben coincidir para que el tráfico coincida con la política. Ser más general en la política de autenticación y más específico en las políticas resultantes permite menos políticas en su conjunto.



Políticas de descifrado

Al igual que con el perfil de ID, los criterios establecidos en la política de descifrado también se evalúan como AND lógico, con una excepción importante cuando se utiliza información de ISE. El funcionamiento de la coincidencia de políticas depende de los elementos configurados (grupo AD, usuario o SGT):

- Grupos y usuarios de AD: sin cambios en el comportamiento anterior; la directiva coincide si el usuario es miembro del grupo, O bien el usuario está especificado en la directiva.
- Grupos y usuarios de SGT y AD: la política coincide si el usuario está asociado a SGT AND es miembro del grupo AD, O bien el usuario está especificado en la política.
- SGT y usuarios: la política coincide si el usuario está asociado con la SGT o si el usuario está especificado en la política.

De todos los servicios que realiza el SWA, la evaluación del tráfico 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 se debe comprobar una vez al trimestre. Encontrar el porcentaje de tráfico HTTPS que es descifrado por el SWA es fácil de hacer con una copia de access_logs, incluso sin software de administración de registros adicional. 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):

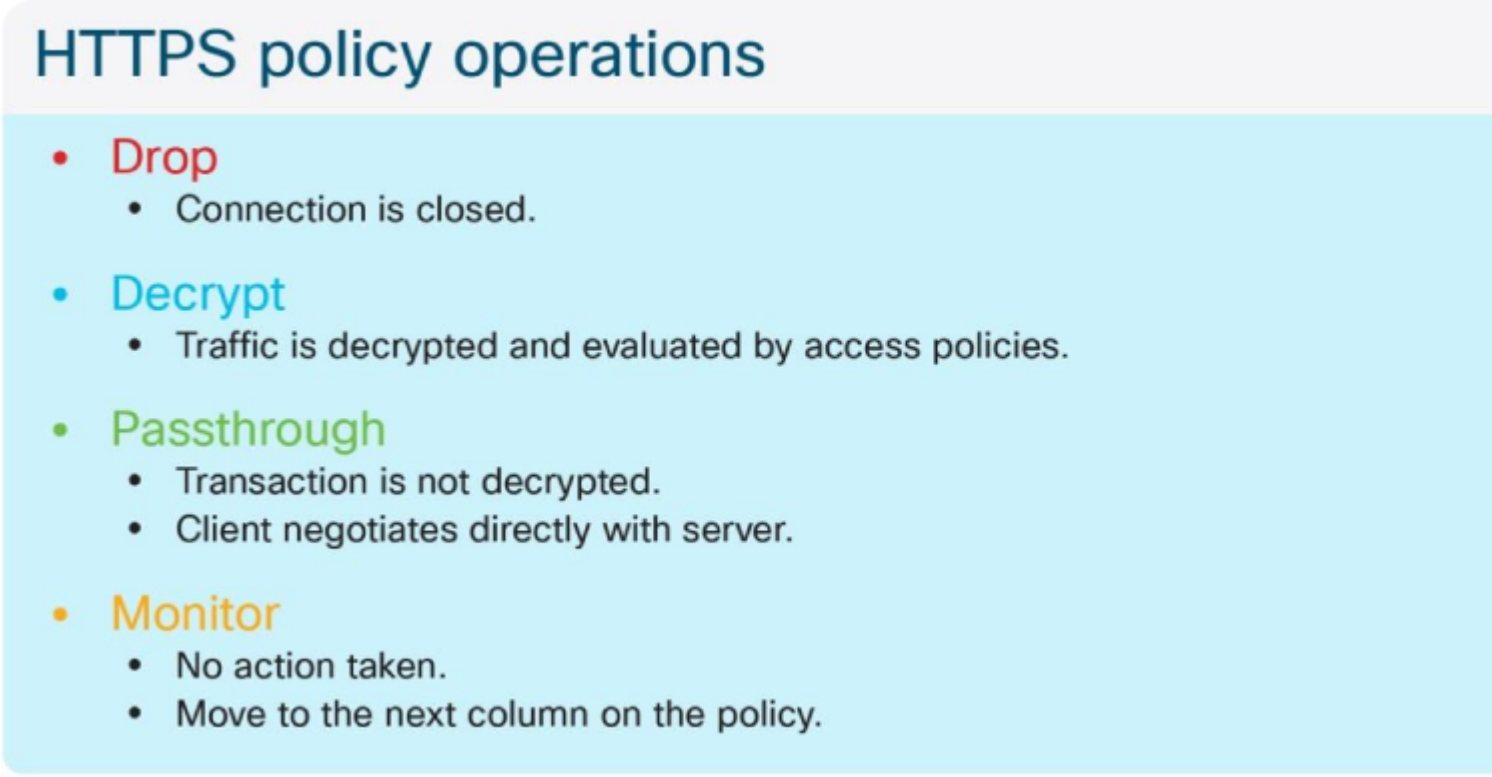
```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

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

2. Busque el número de conexiones HTTPS descifradas:

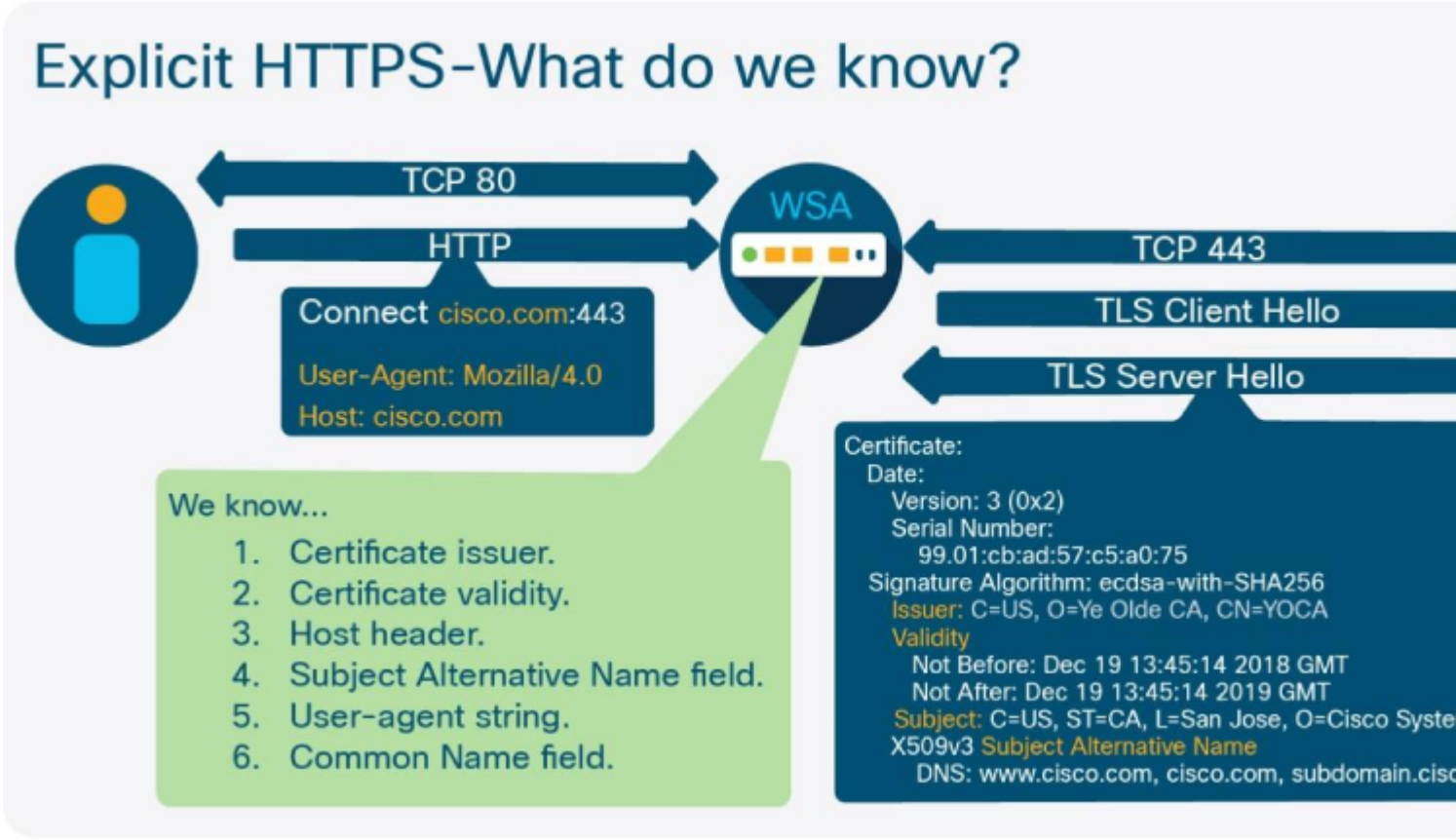
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

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

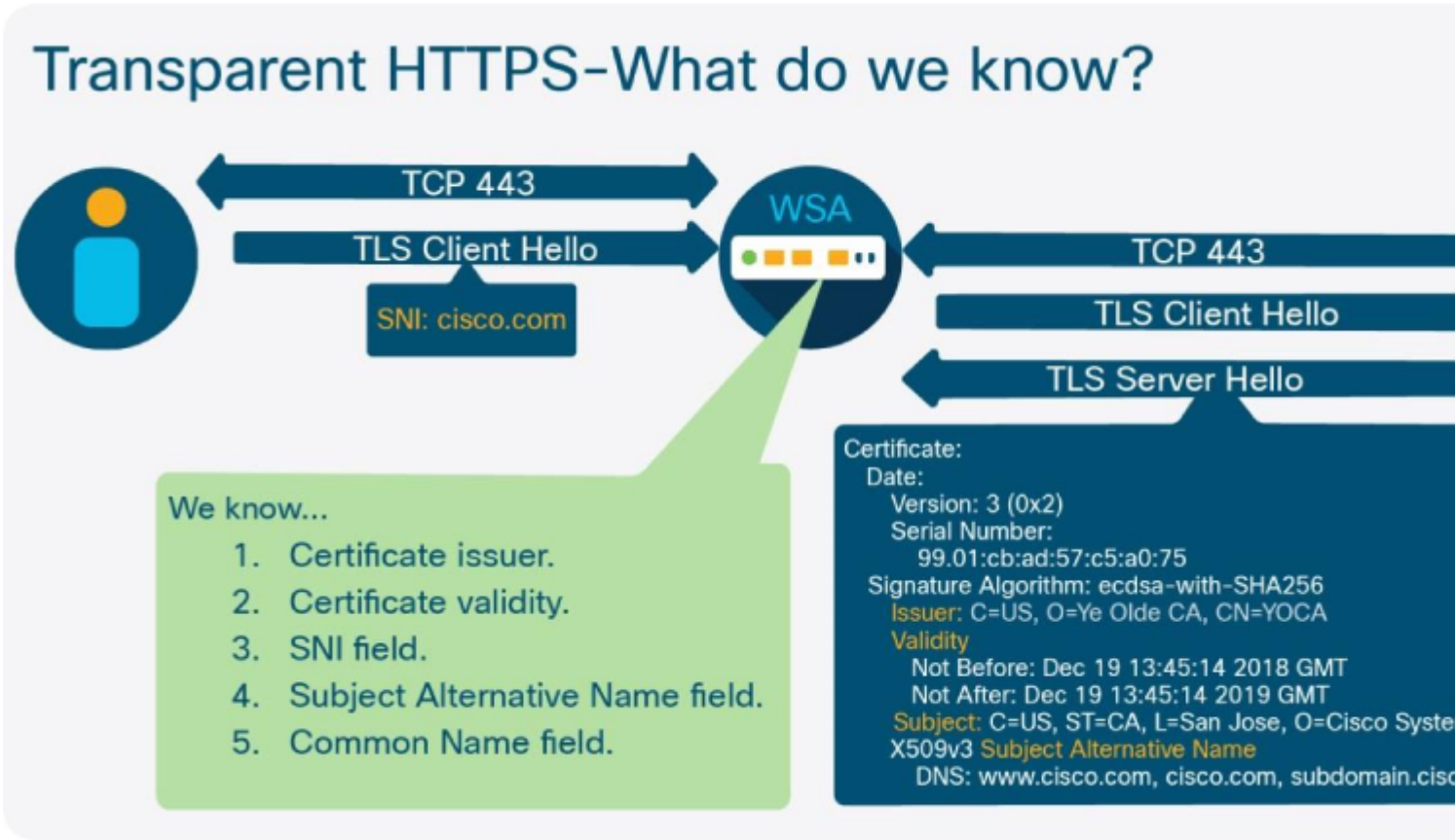
3. Divida el segundo valor por el primer valor y multiplique por 100.

Al diseñar políticas de descifrado, es importante comprender cómo las diversas acciones enumeradas en la política hacen que el dispositivo evalúe las conexiones HTTPS. La acción de paso a través se utiliza cuando se debe permitir que el cliente y el servidor finalicen cada extremo de su sesión TLS sin que el SWA descifre cada paquete. Incluso si un sitio está configurado para pasar a través de, el SWA debe seguir siendo necesario para completar un intercambio de señales TLS con el servidor. Esto se debe a que el SWA debe elegir bloquear una conexión basada en la validez del certificado y debe iniciar una conexión TLS con el servidor para obtener el certificado. Si el certificado es válido, el SWA cierra la conexión y permite al cliente continuar configurando la sesión directamente con el servidor.



El único caso en el que el SWA no realiza ningún intercambio de señales TLS es cuando el nombre del servidor o la dirección IP está presente en una categoría personalizada, que está configurada como passthrough, y el nombre del servidor está disponible en HTTP CONNECT o TLS Client Hello. En un escenario explícito, el cliente proporciona el nombre de host del servidor al proxy antes de la iniciación de la sesión TLS (en el encabezado de host), por lo que este campo se compara con la categoría personalizada. En una implementación transparente, el SWA comprueba el campo **Indicación de nombre de servidor (SNI)** en el mensaje de saludo del cliente TLS y lo evalúa en función de la categoría personalizada. Si el encabezado de host o SNI no está presente, el SWA debe continuar el protocolo de enlace con el servidor para verificar los campos **Nombre alternativo del sujeto (SAN)** y **Nombre común (CN)** en el certificado, en ese orden.
Lo que este comportamiento significa para el diseño de políticas es que el número de protocolos de enlace TLS se puede reducir determinando servidores conocidos e internamente fiables y configurándolos para que pasen de la lista de categorías personalizada, en lugar de depender de la categoría web y la puntuación de reputación, que aún requieren que el SWA complete un protocolo de enlace TLS con el servidor. Sin embargo, es importante tener en cuenta que esto también impide las comprobaciones de validez de certificados.





La velocidad a la que aparecen los nuevos sitios en la Web, es probable que sea un número de sitios no clasificados por la reputación de la Web y las bases de datos de categorizaciones utilizadas por el SWA. Esto no indica que el sitio sea necesariamente más propenso a ser malintencionado y, además, todos estos sitios seguirán sujetos a análisis antivirus, a análisis y reputación de archivos de AMP y a cualquier bloqueo o análisis de objetos que se configure. Por estas razones, en la mayoría de las circunstancias no se

recomienda descartar sitios no clasificados. Es mejor configurarlos para que sean descifrados y analizados por los motores antivirus y evaluados por AVC, AMP, políticas de acceso, etc. Hay más información sobre los sitios sin categorizar en la sección **Políticas de acceso**.

Políticas de acceso

Al igual que con el perfil de ID, los criterios establecidos en la política de descifrado también se evalúan como AND lógico con una excepción importante cuando se utiliza información de ISE. A continuación se explica el comportamiento de coincidencia de políticas, en función de los elementos configurados (grupo AD, usuario o SGT):

- Grupos y usuarios de AD: sin cambios en el comportamiento anterior; la directiva coincide si el usuario es miembro de un grupo, O el usuario está especificado en la directiva.
- Grupos y usuarios de SGT y AD: la política coincide si el usuario está asociado con SGT AND es miembro del grupo AD, O bien el usuario está especificado en la política.
- SGT y usuarios: la política coincide si el usuario está asociado con SGT O si el usuario está especificado en la política.

El tráfico HTTP se evalúa frente a las políticas de acceso inmediatamente después de ser autenticado. El tráfico HTTPS se evalúa después de ser autenticado y si la acción de descifrado se aplica según la política de descifrado correspondiente. Para las solicitudes descifradas, hay dos entradas access_log. La primera entrada del registro muestra la acción aplicada a la conexión TLS inicial (descifrar) y una segunda entrada del registro muestra la acción aplicada por la política de acceso a la solicitud HTTP descifrada.
Como se explica en la sección **Proxy Web**, los encabezados de solicitud de rango se utilizan para solicitar un rango de bytes específico de un archivo y son utilizados comúnmente por el SO y los servicios de actualización de aplicaciones. El SWA, de forma predeterminada, elimina estos encabezados de las solicitudes salientes, porque sin el archivo completo, es imposible realizar un escaneo de malware o utilizar las funciones de AVC. Si muchos hosts de la red solicitan con frecuencia intervalos de bytes pequeños para recuperar las actualizaciones, esto puede hacer que el SWA descargue el archivo completo varias veces simultáneamente. Esto puede agotar rápidamente el ancho de banda de Internet disponible y provocar interrupciones del servicio. Las causas más comunes de este escenario de falla son los demonios de actualización de software de Microsoft Windows y Adobe.
Para mitigar esto, la mejor solución es dirigir este tráfico alrededor del SWA por completo. Esto no siempre es factible para entornos implementados de forma transparente y, en estos casos, la siguiente mejor opción es crear políticas de acceso dedicadas para el tráfico y habilitar el reenvío de encabezado de solicitud de rango en esas políticas. Se debe tener en cuenta que el análisis AV y AVC no son posibles para estas solicitudes, por lo que las políticas deben diseñarse cuidadosamente para que solo se dirijan al tráfico deseado. A menudo, la mejor manera de lograrlo es hacer coincidir la cadena de usuario-agente que se encuentra en el encabezado de la solicitud. La cadena de agente de usuario para los demonios de actualización comunes se puede encontrar en línea, o las solicitudes pueden ser capturadas por un administrador y examinadas. La mayoría de los servicios de actualización, incluidas las actualizaciones de software de Microsoft Windows y Adobe, no utilizan HTTPS.
Como se describe en la sección **Políticas de descifrado**, no se recomienda descartar los sitios sin categorizar en las políticas de descifrado. Por los mismos motivos, no se recomienda bloquearlos en las políticas de acceso. El motor de análisis de contenido dinámico (DCA) puede utilizar el contenido de un sitio determinado, junto con otros datos heurísticos, para clasificar sitios que, de lo contrario, se marcarían como no categorizados mediante búsquedas de bases de datos de URL. Al habilitar esta característica, se reduce el número de veredictos no categorizados en el SWA.
En la configuración de Exploración de objetos de una directiva de acceso, existe la posibilidad de inspeccionar varios tipos de archivos de almacenamiento. Si la red descarga regularmente archivos de almacenamiento como parte de las actualizaciones de la aplicación, su activación puede aumentar considerablemente el uso de la CPU. Este tráfico debe identificarse con antelación y quedar exento si se pretende inspeccionar todos los archivos de almacenamiento. El primer lugar para investigar los posibles métodos para identificar este tráfico es la cadena de agente de usuario, ya que esto puede ayudar a evitar las

listas de IP permitidas que pueden volverse engorrosas de mantener.

Categorías de URL externas y personalizadas

Las listas de categorías personalizadas se utilizan para identificar un servidor por dirección IP o nombre de host. Es posible utilizar expresiones regulares (regex) para especificar patrones con los que se pueden hacer coincidir los nombres de servidor. Utilizar un patrón de expresiones regulares para hacer coincidir un nombre de servidor requiere muchos más recursos que utilizar una coincidencia de subcadenas, por lo que sólo se deben utilizar cuando sea absolutamente necesario. Se puede agregar un "." al principio de un nombre de dominio para que coincida con un subdominio sin necesidad de regex. Por ejemplo, ".cisco.com" también coincide con "www.cisco.com."
Como se explica en la sección **Complejidad**, la complejidad baja se define como diez listas de categorías personalizadas, la complejidad media como veinte y la complejidad alta como treinta. Se recomienda mantener este número por debajo de veinte, especialmente si las listas utilizan patrones de expresiones regulares o contienen un gran número de entradas. Consulte la sección **Políticas de acceso** para obtener detalles adicionales sobre el número de entradas para cada tipo.
Las fuentes de URL externas son mucho más flexibles que las listas de categorías personalizadas estáticas, y aprovecharlas puede tener un impacto directo en la seguridad, ya que eliminan la necesidad de que un administrador las mantenga manualmente. Debido a que esta función se puede utilizar para recuperar listas que no son mantenidas o controladas por el administrador SWA, la capacidad de agregar excepciones individuales a las direcciones descargadas se agregó en la versión 11.8 de AsyncOS.
La API de Office365 es especialmente útil para tomar decisiones de políticas en este servicio implementado con frecuencia y se puede aprovechar para aplicaciones individuales (PowerPoint, Skype, Word, etc.).
Microsoft recomienda omitir los proxies para todo el tráfico de Office 365 para optimizar el rendimiento. La documentación de Microsoft indica:
"Mientras que la inspección y la interrupción de SSL crean la mayor latencia, otros servicios como la autenticación de proxy y la búsqueda de reputación pueden provocar un rendimiento deficiente y una mala experiencia del usuario. Además, estos dispositivos de red perimetral necesitan suficiente capacidad para procesar todas las solicitudes de conexión a la red. Se recomienda omitir el proxy o los dispositivos de inspección para las solicitudes directas de red de Office 365."https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide .

Puede resultar difícil utilizar esta guía en un entorno de proxy transparente. A partir de la versión 11.8 de AsyncOS, es posible utilizar la lista de categorías dinámica recuperada de la API de Office365 para rellenar la lista de configuración de omisión. Esta lista se utiliza para enviar tráfico redirigido de forma transparente de vuelta al dispositivo WCCP para el ruteo directo.
Al omitir todo el tráfico de Office 365, se crea un punto ciego para los administradores que requieren algunos controles de seguridad básicos y la generación de informes para este tráfico. Si el SWA no omite el tráfico de Office 365, es importante comprender los retos técnicos específicos que pueden surgir. Una de ellas es el número de conexiones que requieren las aplicaciones. El tamaño debe ajustarse adecuadamente para admitir las conexiones TCP persistentes adicionales que requieren las aplicaciones de Office365. Esto puede aumentar el recuento total de conexiones entre diez y quince sesiones TCP persistentes por usuario.
Las acciones de descifrado y recifrado realizadas por el proxy HTTPS introducen una pequeña cantidad de latencia en las conexiones. Las aplicaciones de Office 365 pueden ser muy sensibles a la latencia y, si otros factores, como la lentitud de la conexión WAN y la disparidad de la ubicación geográfica, lo agravan, la experiencia del usuario puede verse afectada.
Algunas aplicaciones de Office 365 emplean parámetros TLS propios que evitan que el proxy HTTPS complete un protocolo de enlace con el servidor de aplicaciones. Esto es necesario para validar el certificado o recuperar el nombre de host. Cuando se combina con una aplicación como Skype Empresarial que no envía un campo de **indicación de nombre de servidor (SNI)** en su mensaje de saludo de cliente TLS, se hace necesario omitir este tráfico por completo. AsyncOS 11.8 ha introducido la capacidad de eludir el tráfico basado únicamente en la dirección IP de destino, sin comprobaciones de certificados para abordar este escenario.

Monitores y alertas

Monitores CLI

La CLI de SWA proporciona comandos para la supervisión en tiempo real de procesos importantes. Los comandos más útiles son los que muestran estadísticas relacionadas con el proceso prox. El comando **status detail** es una buena fuente para un resumen de las métricas de uso y rendimiento de recursos, incluidos el tiempo de actividad, el ancho de banda utilizado, la latencia de respuesta, el número de conexiones, etc. A continuación se muestra un ejemplo de salida de este comando:

```
SWA_CLI>  status detail

Status as of:                  Fri Nov 11 14:06:52 2022 +03
Up since:                      Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                                3.3%
  RAM                                6.2%
  Reporting/Logging Disk            45.6%
Transactions per Second:
  Average in last minute               55
  Maximum in last hour                201
  Average in last hour                 65
  Maximum since proxy restart        1031
  Average since proxy restart          51
Bandwidth (Mbps):
  Average in last minute            4.676
  Maximum in last hour            327.258
  Average in last hour             10.845
  Maximum since proxy restart     1581.297
  Average since proxy restart       11.167
Response Time (ms):
  Average in last minute               635
  Maximum in last hour              376209
  Average in last hour                 605
  Maximum since proxy restart      2602943
  Average since proxy restart          701
Cache Hit Rate:
  Average in last minute                 0
  Maximum in last hour                   2
  Average in last hour                   0
  Maximum since proxy restart           15
  Average since proxy restart            0
Connections:
  Idle client connections              186
  Idle server connections              184
  Total client connections            3499
  Total server connections            3632
SSLJobs:
  In queue Avg in last minute            4
  Average in last minute             45214
  SSLInfo Average in last min           94
Network Events:
  Average in last minute               0.0
  Maximum in last minute                35
  Network events in last min        124502
```

El comando **rate** muestra información en tiempo real sobre el porcentaje de CPU utilizado por el proceso prox, así como el número de solicitudes por segundo (RPS) y estadísticas de caché. Este comando continúa sondeando y mostrando el nuevo resultado hasta que se interrumpe. Este es un ejemplo del resultado de este comando:

```
SWA_CLI>  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
  5.00    51      1    147    370      2283      2268    0.6    48    37
  4.00    36      0    128    237     21695     21687    0.0    47    38
  4.00    48      2    179    307      8168      8154    0.2    65    33
  5.00    53      0    161    372      2894      2880    0.5    48    32
  6.00    52      0    198    328     15110     15100    0.1    63    33
  6.00    77      0    415    363      4695      4684    0.2    48    34
  7.00    85      1    417    433      5270      5251    0.4    49    35
  7.00    67      1    443    228      2242      2232    0.5    85    44
```

El comando **tcpservices** muestra información sobre los puertos de escucha de procesos seleccionados. También se muestra una explicación de cada proceso y la combinación de dirección y puerto:

```
SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  coeuslogd    - Main WSA controller
  gui          - GUI process
  hermes       - Mail server for sending alerts, etc.
  java         - Processes for storing and querying Web Tracking data
  musd         - AnyConnect Secure Mobility server
  pacd         - PAC file hosting daemon
  prox         - WSA proxy
  trafmon      - L4 Traffic Monitor
  uds          - User Discovery System (Transparent Auth)
  wccpd        - WCCP daemon

COMMAND      USER         TYPE NODE   NAME
connector    root         IPv4 TCP    127.0.0.1:8823
java         root         IPv6 TCP    [::127.0.0.1]:18081
hybridd      root         IPv4 TCP    127.0.0.1:8833
gui          root         IPv4 TCP    172.16.40.80:8443
ginetd       root         IPv4 TCP    172.16.40.80:ssh
nginx        root         IPv6 TCP    *:4431
nginx        root         IPv4 TCP    127.0.0.1:8843
```

```
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
api_serve    root         IPv4 TCP    172.16.40.80:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    172.16.40.80:6443
chimera      root         IPv4 TCP    127.0.0.1:6380
nectar       root         IPv4 TCP    127.0.0.1:6382
redis-ser    root         IPv4 TCP    127.0.0.1:6383
redis-ser    root         IPv4 TCP    127.0.0.1:6379
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25255
prox         root         IPv4 TCP    127.0.0.1:socks
prox         root         IPv6 TCP    [::1]:socks
prox         root         IPv4 TCP    172.16.11.69:socks
prox         root         IPv4 TCP    172.16.11.68:socks
prox         root         IPv4 TCP    172.16.11.252:socks
prox         root         IPv4 TCP    127.0.0.1:ftp-proxy
prox         root         IPv6 TCP    [::1]:ftp-proxy
prox         root         IPv4 TCP    172.16.11.69:ftp-proxy
prox         root         IPv4 TCP    172.16.11.68:ftp-proxy
prox         root         IPv4 TCP    172.16.11.252:ftp-proxy
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
```

```
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25256
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.21.11.69:https
prox         root         IPv4 TCP    172.21.11.68:https
prox         root         IPv4 TCP    172.21.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25257
smart_age    root         IPv6 TCP    [::127.0.0.1]:65501
smart_age    root         IPv6 TCP    [::127.0.0.1]:28073
interface    root         IPv4 TCP    127.0.0.1:domain
stunnel      root         IPv4 TCP    127.0.0.1:32137
```

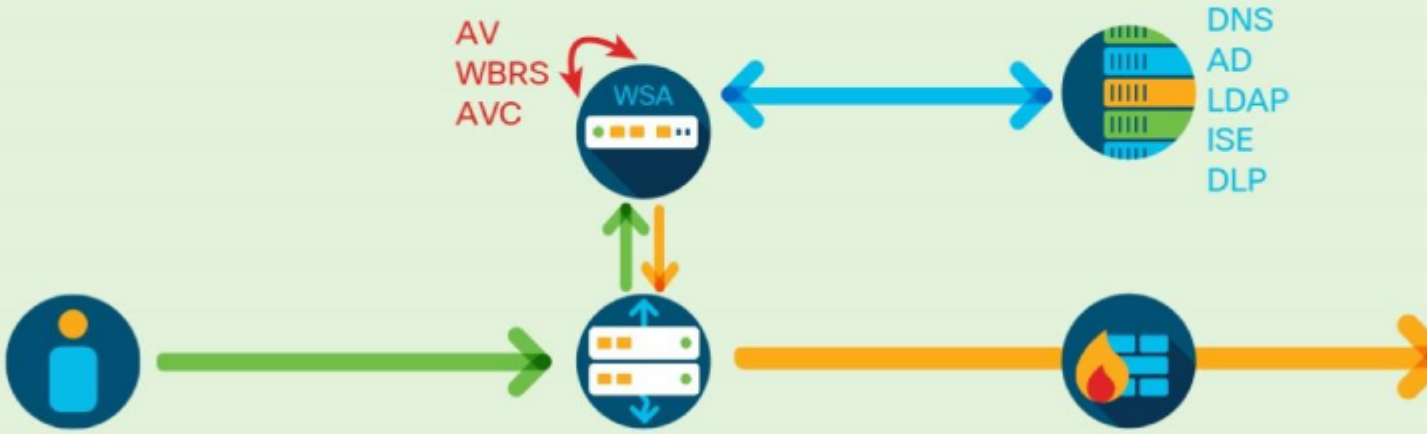
Registro

El tráfico web es muy dinámico y variado. Una vez finalizada la implementación de un proxy, es importante volver a evaluar periódicamente la cantidad y composición del tráfico que pasa a través del dispositivo. Debe comprobar el porcentaje de tráfico descifrado de forma regular (una vez al trimestre) para asegurarse de que el tamaño es coherente con las expectativas y especificaciones de la instalación inicial. Esto se puede hacer con un producto de administración de registros como **Advanced Web Security Reporting (AWSR)** o con comandos simples de Bash o PowerShell con los registros de acceso. El número de RPS también se debe reevaluar periódicamente para garantizar que el dispositivo tenga suficiente sobrecarga para tener en cuenta los picos de tráfico y la posible conmutación por fallo en una configuración de alta disponibilidad y equilibrio de carga.

El registro track_stats se anexa cada cinco minutos e incluye varias secciones de salida directamente relacionadas con el proceso prox y sus objetos en la memoria. Las secciones que muestran la latencia media de varios procesos de solicitud, incluidos el tiempo de búsqueda de DNS, el tiempo de análisis del motor antivirus y muchos otros campos útiles, son las más útiles para supervisar el rendimiento. Este registro no se puede configurar desde la GUI ni desde la CLI y solo se puede acceder a él a través del protocolo de copia segura (SCP) o del protocolo de transferencia de archivos (FTP). Este es el registro más importante que se debe tener al solucionar problemas de rendimiento, por lo que se debe sondear con frecuencia.

Where can latency be introduced?

- Client Side
- External Services
- Internal Services
- Server Side

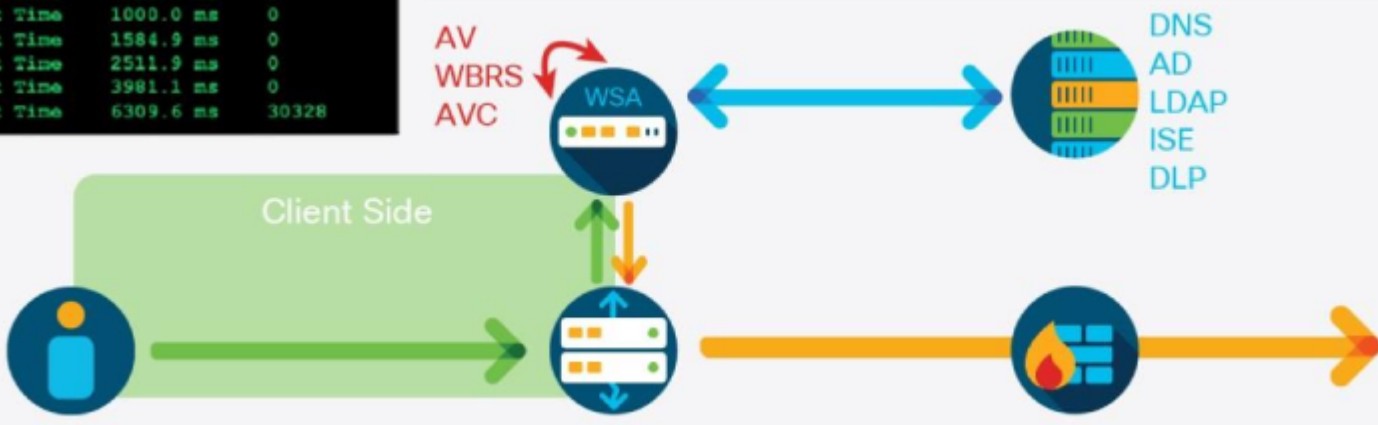


Client side latency

```
Client Time       1.0 ms    15575
Client Time       1.6 ms    185
Client Time       2.5 ms    855
Client Time       4.0 ms    573
Client Time       6.3 ms    180
Client Time      10.0 ms    264
Client Time      15.8 ms    580
Client Time      25.1 ms    924
Client Time      39.8 ms    1330
Client Time      63.1 ms    4936
Client Time     100.0 ms    5278
Client Time     158.5 ms    10
Client Time     251.2 ms    13
Client Time     398.1 ms    0
Client Time     631.0 ms    0
Client Time    1000.0 ms    0
Client Time    1584.9 ms    0
Client Time    2511.9 ms    0
Client Time    3981.1 ms    0
Client Time    6309.6 ms    30328
```

- **“Client Time”** in **track_stats** log.
- The amount of time in milliseconds that the client was wa response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field **% : 1>**

%:1>	x-p2c-first-byte-time	Wait-time for first byte written

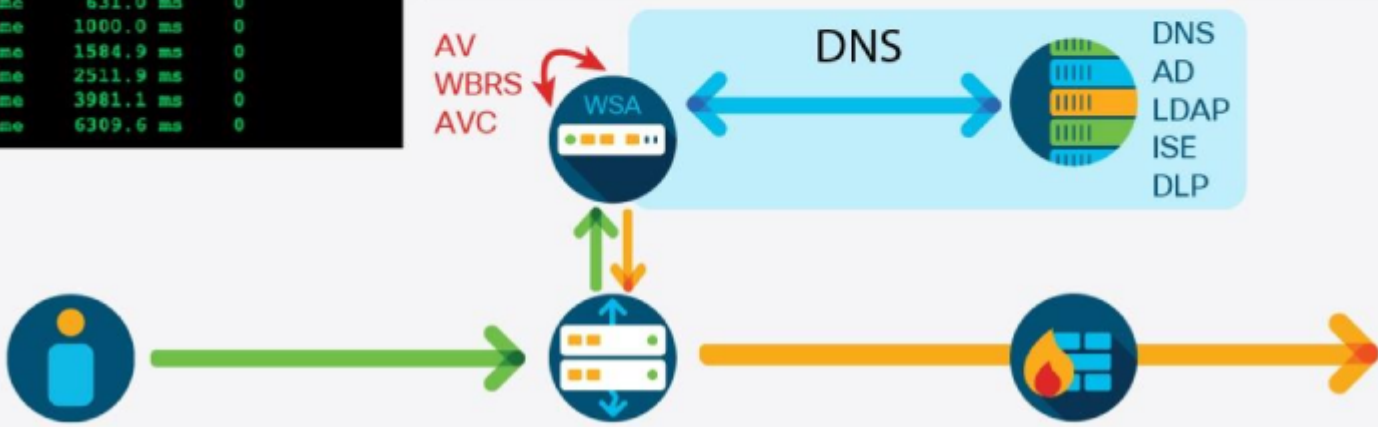


DNS latency

```
DNS Time       1.0 ms    51
DNS Time       1.6 ms    347
DNS Time       2.5 ms    152
DNS Time       4.0 ms    71
DNS Time       6.3 ms    98
DNS Time      10.0 ms    7
DNS Time      15.8 ms    11
DNS Time      25.1 ms    13
DNS Time      39.8 ms    2
DNS Time      63.1 ms    3
DNS Time     100.0 ms    7
DNS Time     158.5 ms    16
DNS Time     251.2 ms    4
DNS Time     398.1 ms    1
DNS Time     631.0 ms    0
DNS Time    1000.0 ms    0
DNS Time    1584.9 ms    0
DNS Time    2511.9 ms    0
DNS Time    3981.1 ms    0
DNS Time    6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited response.
- Calls for investigation for your DNS resolvers (or path to
- **access logs** can show this in custom field **% : >d**

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy send a DNS result to ehe Web

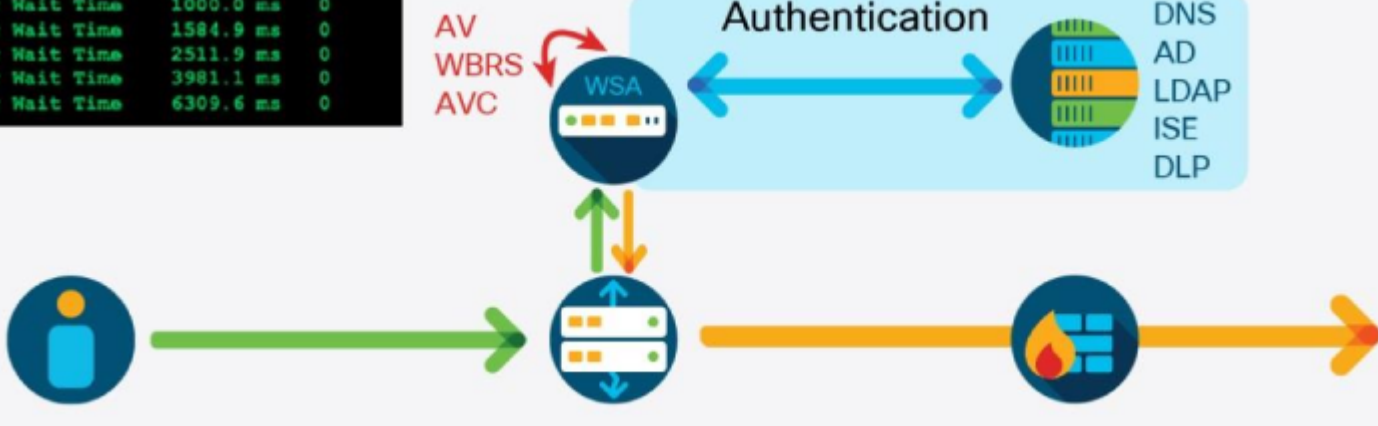


Authentication latency

```
Server Wait Time       1.0 ms    0
Server Wait Time       1.6 ms    0
Server Wait Time       2.5 ms    0
Server Wait Time       4.0 ms    0
Server Wait Time       6.3 ms    0
Server Wait Time      10.0 ms    0
Server Wait Time      15.8 ms    0
Server Wait Time      25.1 ms    0
Server Wait Time      39.8 ms    0
Server Wait Time      63.1 ms    0
Server Wait Time     100.0 ms    0
Server Wait Time     158.5 ms    1
Server Wait Time     251.2 ms    1
Server Wait Time     398.1 ms    0
Server Wait Time     631.0 ms    0
Server Wait Time    1000.0 ms    0
Server Wait Time    1584.9 ms    0
Server Wait Time    2511.9 ms    0
Server Wait Time    3981.1 ms    0
Server Wait Time    6309.6 ms    0
```

- There are two metrics: **“Auth Helper Wait Time”** and **“A Service Wait Time.”**
- Use the first to get pure auth time without the request tim
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the respo Web Proxy authentication proc Web Proxy sent the request.

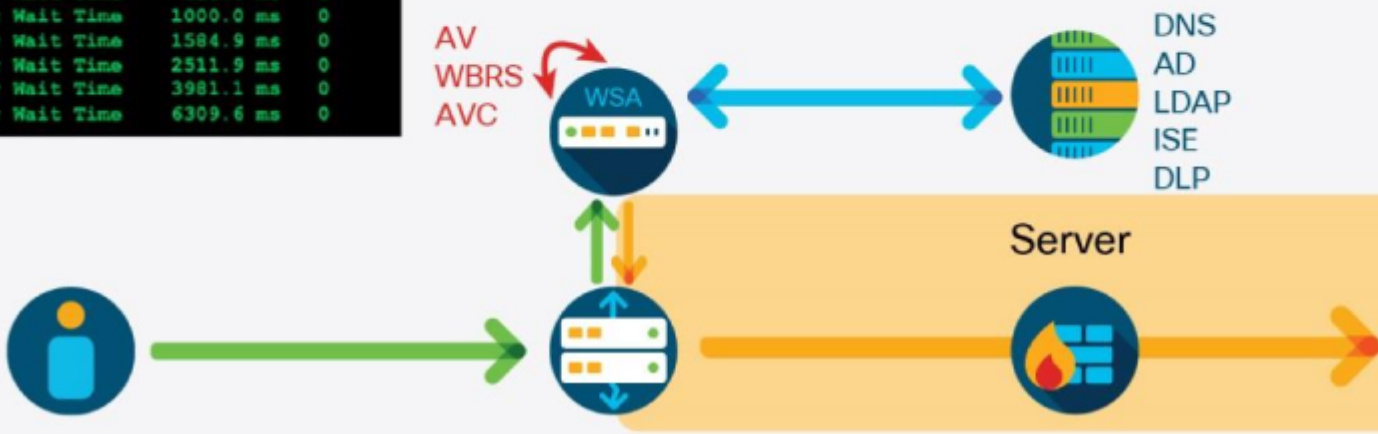


Server latency-wait time

Server Wait Time	1.0 ms	0
Server Wait Time	1.6 ms	0
Server Wait Time	2.5 ms	0
Server Wait Time	4.0 ms	0
Server Wait Time	6.3 ms	0
Server Wait Time	10.0 ms	0
Server Wait Time	15.8 ms	0
Server Wait Time	25.1 ms	0
Server Wait Time	39.8 ms	0
Server Wait Time	63.1 ms	0
Server Wait Time	100.0 ms	0
Server Wait Time	158.5 ms	1
Server Wait Time	251.2 ms	1
Server Wait Time	398.1 ms	0
Server Wait Time	631.0 ms	0
Server Wait Time	1000.0 ms	0
Server Wait Time	1584.9 ms	0
Server Wait Time	2511.9 ms	0
Server Wait Time	3981.1 ms	0
Server Wait Time	6309.6 ms	0

- The amount of time in milliseconds that the WSA waited byte of the server response.
- Calls for investigation of your upstream devices and WAN
- **access logs** can show this in custom field **% : >1**

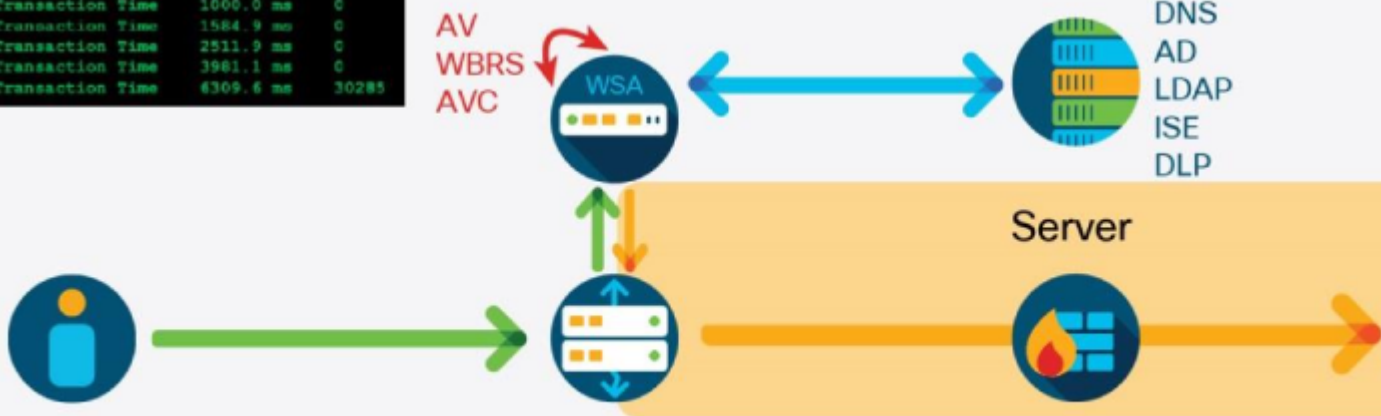
%:>1	x-s2p-first-byte-time	Wait-time for first response by

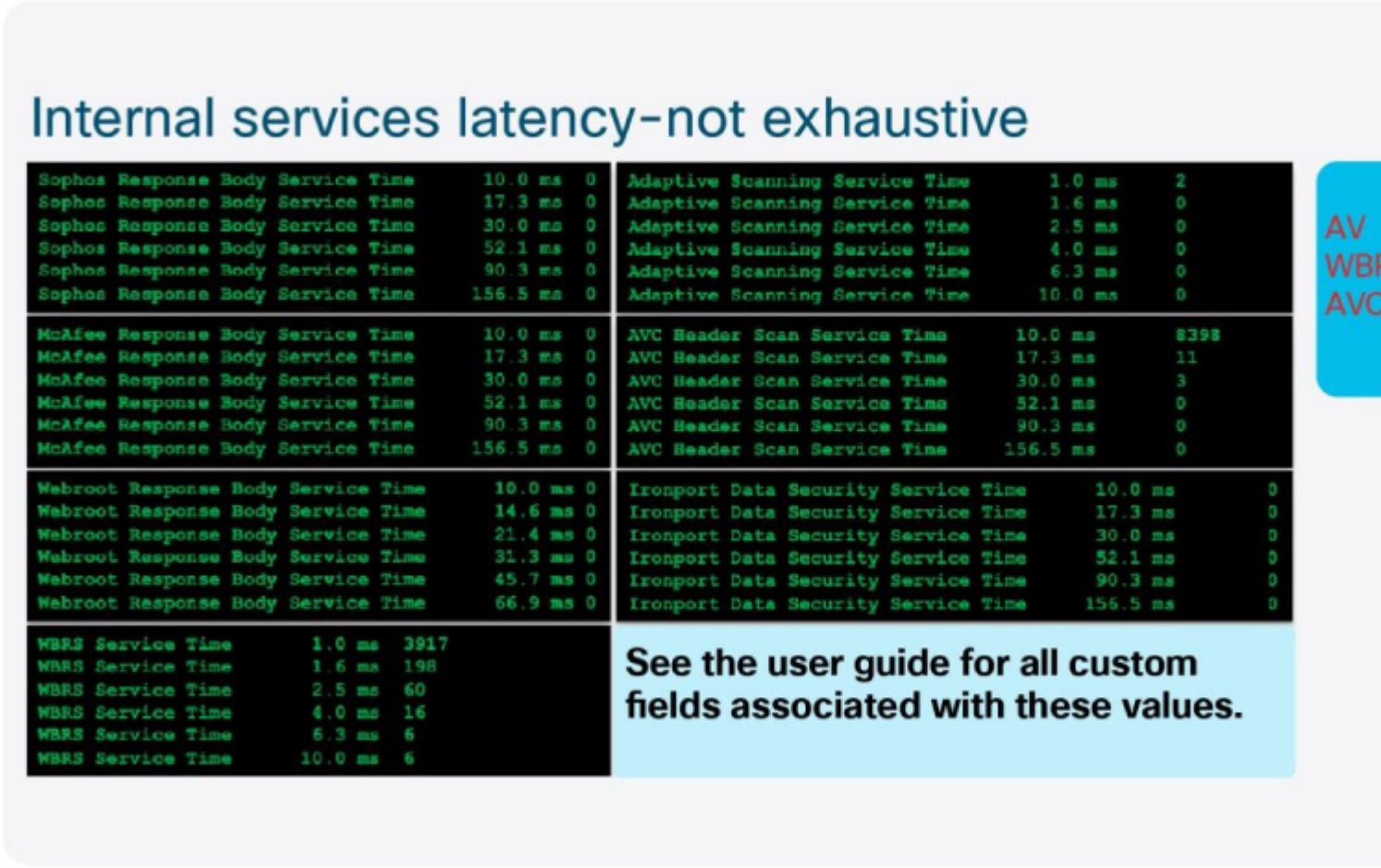


Server latency-transaction time

Server Transaction Time	1.0 ms	1422
Server Transaction Time	1.6 ms	858
Server Transaction Time	2.5 ms	1035
Server Transaction Time	4.0 ms	1106
Server Transaction Time	6.3 ms	758
Server Transaction Time	10.0 ms	810
Server Transaction Time	15.8 ms	288
Server Transaction Time	25.1 ms	45
Server Transaction Time	39.8 ms	73
Server Transaction Time	63.1 ms	4221
Server Transaction Time	100.0 ms	8097
Server Transaction Time	158.5 ms	5
Server Transaction Time	251.2 ms	0
Server Transaction Time	398.1 ms	2
Server Transaction Time	631.0 ms	0
Server Transaction Time	1000.0 ms	0
Server Transaction Time	1584.9 ms	0
Server Transaction Time	2511.9 ms	0
Server Transaction Time	3981.1 ms	0
Server Transaction Time	6309.6 ms	30285

- The amount of time in milliseconds for the entire server-s transaction to complete.
- Calls for investigation of your upstream devices and WAN
- No **access logs** custom field, but can be determined by a combinationof them.





Una línea de registro SHD individual se escribe cada 60 segundos y contiene muchos campos que son importantes para la supervisión del rendimiento, como la latencia, RPS y conexiones totales en el lado del cliente y en el lado del servidor. Este es un ejemplo de una línea de registro SHD:

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 619
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 774
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 791
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 1403
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

Se pueden agregar campos personalizados adicionales a los access_logs que denotan la información de latencia para solicitudes individuales. Estos campos incluyen la respuesta del servidor, la resolución de DNS y la latencia del analizador antivirus. Los campos deben agregarse al registro para obtener información valiosa que se utilizará para la solución de problemas. Esta es la cadena de campo personalizada recomendada para su uso:

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms):
```

```
, Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<, R

a; DNS response = %:

d, WBRS response = %:

r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respons

s, AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ][Client Port = %F, Server IP = %k,
```

La información de rendimiento derivada de estos valores es la siguiente:

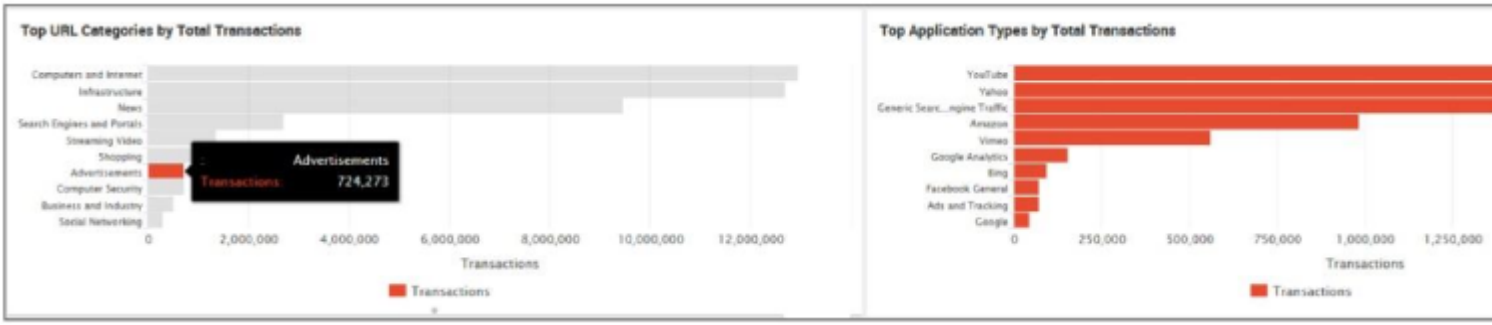
Campo personalizado	**Descripción**
%:<a	Tiempo de espera para recibir la respuesta del proceso de autenticación de proxy web, después de que el proxy web envió la solicitud.
%:<b	Tiempo de espera para escribir el cuerpo de la solicitud en el servidor después del encabezado.
%:<d	Tiempo de espera para recibir la respuesta del proceso DNS del proxy web, después de que el proxy web envió la solicitud.
%:<h	Tiempo de espera para escribir el encabezado de solicitud en el servidor después del

	primer byte.
%:<r	Tiempo de espera para recibir la respuesta de los filtros de reputación web, después de que el proxy web haya enviado la solicitud.
%:<s	Tiempo de espera para recibir el veredicto del proceso anti spyware de proxy web, después de que el proxy web envió la solicitud.
%:>	Tiempo de espera para el primer byte de respuesta del servidor.
%:>a	Tiempo de espera para recibir la respuesta del proceso de autenticación de proxy web, que incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:>b	Tiempo de espera para el cuerpo de la respuesta completa después de recibir el encabezado.
%:>c	Tiempo necesario para que el proxy web lea una respuesta de la caché de disco.
%:>d	Tiempo de espera para recibir la respuesta del proceso DNS del proxy web, incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:>h	Tiempo de espera para el encabezado del servidor después del primer byte de respuesta.
%:>r	Tiempo de espera para recibir el veredicto de los filtros de reputación web, que incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:>s	Tiempo de espera para recibir el veredicto del proceso antispyware de proxy web, que incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:1<	Tiempo de espera para el primer byte de solicitud de la nueva conexión de cliente.
%:1>	Tiempo de espera para el primer byte escrito en el cliente.
%:b<	Tiempo de espera para el cuerpo completo del cliente.
%:b>	Tiempo de espera para el cuerpo completo escrito al cliente.
%:e>	Tiempo de espera para recibir la respuesta del motor de análisis de AMP, después de que el proxy web haya enviado la solicitud.
%:e<	El tiempo de espera para recibir el veredicto del motor de análisis de AMP incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:h<	Tiempo de espera para el encabezado de cliente completo después del primer byte.
%:h>	Tiempo de espera para el encabezado completo escrito en el cliente.
%:m<	Tiempo de espera para recibir el veredicto del motor de exploración de McAfee, que incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:m>	Tiempo de espera para recibir la respuesta del motor de exploración de McAfee, después de que el proxy web haya enviado la solicitud.
%F	Puerto de origen del cliente.
%p	Puerto del servidor Web.
%k	Dirección IP del origen de datos (dirección IP del servidor Web).
%:w<	Tiempo de espera para recibir el veredicto del motor de análisis de Webroot, que incluye el tiempo necesario para que el proxy web envíe la solicitud.
%:w>	Espere a recibir la respuesta del motor de análisis de Webroot, después de que el proxy web haya enviado la solicitud.

El modelo de licencias SWA permite la reutilización de licencias de dispositivos físicos para dispositivos virtuales. Puede aprovechar esta oportunidad e implementar dispositivos SWAv de prueba para su uso en entornos de laboratorio. Las nuevas funciones y configuraciones se pueden probar de esta manera para garantizar la estabilidad y la fiabilidad sin infringir los términos de licencia y, al mismo tiempo, sin infringirlos.

Informes avanzados de seguridad web (AWSR)

Se debe aprovechar AWSR para aprovechar al máximo los datos de informes del SWA. Especialmente, en entornos en los que se implementan muchos SWA, esta solución es muchas veces más escalable que la utilización de informes centralizados en un **appliance de gestión de seguridad (SMA)**, y proporciona atributos de informes personalizados que añaden una inmensa cantidad de profundidad y personalización a los datos. Los informes se pueden agrupar y personalizar para satisfacer las necesidades de cualquier organización. El grupo de servicios avanzados de Cisco debe aprovechar el tamaño de AWSR.



Alertas por correo electrónico

El sistema de alerta de correo electrónico integrado en el SWA se aprovecha mejor como sistema de alerta de línea de base. Debe ajustarse adecuadamente para satisfacer las necesidades del administrador, ya que puede ser muy ruidoso si se habilitan todos los eventos informativos. Es más importante limitar las alertas y supervisarlas de forma activa que alertar de todo e ignorarlas como spam.

Configuración de alertas	**Configuración**
Dirección de origen que se utilizará al enviar alertas	Generado automáticamente
Número inicial de segundos de espera antes de enviar una alerta duplicada	300 Segundos
Número máximo de segundos de espera antes de enviar una alerta duplicada	3600 Segundos

Supervisión de disponibilidad

Hay dos métodos que se pueden utilizar para supervisar la disponibilidad de un proxy web. La primera es la supervisión de **capa 3 (L3)**, que comprueba si la dirección IP del dispositivo es accesible en la red. La manera más simple de probar esto es enviar una solicitud de **eco ICMP (ping)** a la dirección a intervalos regulares y verificar si hay un paquete de respuesta. Los atributos de la respuesta, como TTL, y la latencia se pueden analizar para determinar el estado de la capa de red.

Es posible que un dispositivo pueda responder a los pings pero que los procesos proxy no respondan o sean intermitentes. Por ello, es recomendable emplear un monitor de **capa 7 (L7)**, que envíe una solicitud de proxy explícita al dispositivo y espere un código de respuesta HTTP **200 OK**. Esto prueba no solo la disponibilidad de la interfaz de red, sino también la capacidad de respuesta de los servicios proxy y la

viabilidad de los servicios ascendentes si se solicita un recurso externo. Este tipo de monitoreo normalmente toma la forma de una solicitud HTTP **HEAD** explícita que solicita al proxy que se conecte a un recurso. El método **HEAD** solicita que los encabezados que se devolverían deben ser enviados por el cliente a una solicitud **GET**, pero incluye sólo los encabezados de respuesta y ningún dato.

Si utiliza un script o una herramienta de supervisión **L7**, es importante asegurarse de que el tráfico esté exento de autenticación. De lo contrario, esto da lugar a errores de autenticación regulares y al consumo de recursos. Cuando se utiliza una cadena personalizada de usuario-agente en la herramienta de supervisión, se debe emplear para identificar el tráfico. Aunque el tráfico está exento de autenticación, se puede restringir el acceso innecesario a Internet a través de las políticas de acceso.

Cuando utiliza uno o más de estos métodos, un administrador debe establecer una línea base de métricas aceptables en torno a la respuesta de proxy y utilizarla para crear umbrales de alerta. Debe dedicar tiempo a recopilar las respuestas de dichas comprobaciones y antes de decidir cómo desea configurar los umbrales y la alerta.

Supervisión SNMP

El **protocolo simple de administración de red (SNMP)** es el método principal para supervisar el estado del dispositivo. Se puede utilizar para recibir alertas del dispositivo (capturas) o para sondear varios **identificadores de objeto (OID)** para recopilar información. Hay muchos OID disponibles en el SWA que cubren todos los aspectos, desde el uso de hardware hasta el uso de recursos, pasando por la información de procesos individuales y las estadísticas de solicitudes.

Hay una serie de **MIB** específicas **que** se deben supervisar por motivos relacionados con el hardware y el rendimiento. La lista completa de MIB se puede encontrar aquí: https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt.

Esta es una lista de las MIB recomendadas para monitorear y no una lista exhaustiva:

OID de hardware	Nombre
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raidStatus
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	gradosCelsius

Este es un mapa de OID directamente a la salida del comando CLI **status detail**:

OID (ID del objeto)	Nombre	Campo de detalle de estado
Recursos del sistema		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUtilization	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	porCientoUtilizaciónMemoria	RAM

Transacciones por segundo		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Transacciones promedio por segundo en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	Número máximo de transacciones por segundo en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	Transacciones promedio por segundo en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Número máximo de transacciones por segundo desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	Transacciones medias por segundo desde el reinicio del proxy.
Ancho de banda		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	Ancho de banda medio en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Ancho de banda máximo en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	Ancho de banda medio en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Ancho de banda máximo desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Ancho de banda medio desde reinicio del proxy.
Tiempo de respuesta		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Tasa promedio de aciertos de caché en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Tasa máxima de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Tasa promedio de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Tasa de aciertos de caché máxima desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Tasa media de aciertos de caché desde el reinicio del proxy.
Tasa de aciertos de caché		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Tasa promedio de aciertos de caché en el último minuto.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Tasa máxima de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Tasa promedio de aciertos de caché en la última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Tasa de aciertos de caché máxima desde el reinicio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Tasa media de aciertos de caché desde el reinicio del proxy.
Conexiones		

1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Conexiones de cliente inactivas.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	Conexiones de servidor inactivas.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	Conexiones de cliente totales.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	Conexiones de servidor totales.

Conclusión

Esta guía pretende describir los aspectos más importantes de la configuración, implementación y supervisión de SWA. Como guía de referencia, su objetivo es proporcionar información valiosa para aquellos que querían garantizar el uso más eficaz del SWA. Las prácticas recomendadas descritas aquí son importantes para la estabilidad, escalabilidad y eficacia del dispositivo como herramienta de seguridad. También pretende seguir siendo un recurso relevante a medida que avanza y, por lo tanto, debe actualizarse con frecuencia para reflejar los cambios en los entornos de red y los conjuntos de funciones de productos.

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).