Cambios en la versión de Secure Web Appliance

Contenido

Introducción

Este documento describe los cambios principales y las funciones añadidas en las diferentes versiones de Secure Web Appliance (SWA).

Prerequisites

Requirements

No hay requisitos especiales para este artículo.

Las abreviaturas utilizadas en este artículo son:

LD: Implementación limitada.

GD: Implementación general.

MD: implementación de mantenimiento

ED: Implementación temprana.

HP: parche de conexión.

CLI: Interfaz de línea de comandos.

GUI: interfaz gráfica de usuario

HTTP: protocolo de transferencia de hipertexto.

HTTPS: protocolo de transferencia de hipertexto seguro.

ECDSA: algoritmo de firma digital de curva elíptica.

PID: identificador de proceso.

CTR: Cisco Threat Response.

AMP: protección frente a malware avanzado.

URL: Localizador uniforme de recursos.

CDA: agente de directorio de contexto.

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.

Historial de cambios por versión

Versión	Tipo	Cambios de comportamiento	Mejoras/funciones añadidas
12.0.1-268	LD	- Los requisitos de memoria y CPU del sistema cambian de la versión 12.0 en adelante. - De forma predeterminada, TLSv1.3 está habilitado en el dispositivo. - El cifrado 'TLS_AES_256_GCM_SHA384' se agrega a la lista de cifrado predeterminada.	- La versión Cisco AsyncOS 12.0 proporciona un dispositivo de seguridad web de alto rendimiento (HP) para las plataformas S680, S690 y S695. - Se agrega un nuevo subcomando high performance bajo el comando main advanced proxyconfig para habilitar y deshabilitar el modo de alto rendimiento. - Integración del SWA con el portal Cisco Threat Response (CTR). - El dispositivo admite la versión TLSv1.3. - La función de copia de seguridad del archivo de configuración se mueve del submenú "Registrar suscripciones" al "Archivo de configuración" en Administración del sistema. - El dispositivo ahora soporta la carga del certificado ECDSA para el proxy HTTPS.

			- Se agrega un nuevo subcomando CLI proxyscannermap de diagnóstico en diagnostic > proxy. Tto muestra la asignación de PID entre cada proxy y el proceso del analizador correspondiente. - La nueva opción searchdetails se agrega bajo el comando CLI authcache. - El nuevo subcomando CTROBSERVABLE se agrega bajo el comando CLI reportingconfig para habilitar o inhabilitar la indexación basada en CTR.
12.0.1-334	GD		- Se agrega un nuevo analizador de subcomandos bajo el comando principal advanced proxyconfig para excluir los tipos MIME que analizará el motor AMP.
12.0.2-004	MD	- Utilice TLS 1.2 o versiones posteriores para conectar el dispositivo al servidor de Reputación de archivos de AMP. - AMÉRICA (antigua) cloud-sa.amp.sourcefire.com no se puede configurar en el dispositivo.	- Una nueva opción "Ingrese el número de exploraciones simultáneas que admitirá AMP" se agrega en el comando principal CLI advanced proxyconfig > scanners > AMP. puede cambiar el veredicto predeterminado Unscannable de long running scan eviction a Timeout y viceversa del nuevo subcomando eviction de CLI en el comando principal CLI advanced proxyconfig > scanners.
12.02-012	MD		- Los mensajes de alerta se activan en la interfaz de usuario web del dispositivo cuando el proxy Malloc Memory supera el 90% del límite de Malloc Memory proxy y se envía una notificación por correo electrónico a todos los 'destinatarios de alerta' configurados para recibir alertas críticas de 'Web Proxy'. - La nueva interfaz web proporciona un nuevo aspecto para supervisar los

			informes y realizar un seguimiento de los servicios web.
12.0.3-005	MD		
12.0.3-007	MD		- Nueva notificación de actualización de categorías de URL
12.0.4-002	MD		
12.0.5-011	MD	- TLSv1.2 está habilitado de forma predeterminada para la interfaz de usuario web de administración de dispositivos - La reanudación de la sesión está desactivada de forma predeterminada.	- Se agrega un mensaje para indicar el fin del soporte para CDA en la sección de configuración de CDA.
12.5.1-011	LD	- De forma predeterminada, la función Cisco Success Network está activada en el dispositivo. - Estos registros se modifican para incluir más detalles: Los registros de acceso ahora muestran el nombre de usuario cuando falla la autenticación. Los registros del marco de autenticación ahora muestran la dirección IP del cliente para estos protocolos de autenticación fallidos: NTLM, BASIC, SSO (Transparente)	- La versión 12.5 de Cisco AsyncOS proporciona un dispositivo de seguridad web de alto rendimiento (HP) para las plataformas S680, S690 y S695. Esto aumenta el rendimiento del tráfico de los dispositivos actuales de gama alta. - Ahora puede actualizar a la versión 12.5 y utilizar el modo de alto rendimiento en los modelos (S680, S690, S695, S680F, S690F y S695F), incluso si ha activado estas funciones en su dispositivo: • Toque Tráfico web • Cuotas de tiempo y volumen • Límites generales de ancho de banda - Ahora puede configurar la suplantación de IP de proxy web creando un perfil de suplantación de IP y agregándolo a las políticas de ruteo. - Ahora puede crear una categoría de URL

			personalizada para YouTube y establecer políticas en la categoría personalizada de YouTube para un control de acceso seguro. - En la nueva interfaz web, el dispositivo tiene una nueva página (Supervisión > Estado del sistema) para mostrar el estado y la configuración actuales del dispositivo. - La función Cisco Success Network (CSN) permite a Cisco recopilar información de telemetría sobre el uso de funciones del dispositivo. - API REST para red, suscripción a registro y otras configuraciones.
12.5.1-035	GD	- Desaprobación de TLS 1.0/1.1: Utilice TLS 1.2 o versiones posteriores para conectar el dispositivo al servidor de reputación de archivos de AMP. AMÉRICA (antigua) cloud-sa.amp.sourcefire.com se elimina de la lista de servidores de Reputación de archivos de AMP, por lo que AMÉRICA (antigua) cloud-sa.amp.sourcefire.com no se puede configurar en el dispositivo.	- La configuración del tamaño de la memoria caché para la autenticación (Red > Autenticación > Configuración de autenticación > Opciones de caché de credenciales) no es compatible con AsyncOS 12.5.1-035 y versiones posteriores.
12.5.1-043	GD		- Los mensajes de alerta se muestran en la interfaz de usuario web del dispositivo (Administración del sistema > Alertas > Ver alertas principales): • cuando la memoria malloc de proxy supera el 90% del límite de memoria malloc de proxy • cuando el proxy se reinicia en el 100% de la memoria malloc

			En ambos casos, se envía una notificación por correo electrónico a todos los "destinatarios de alerta" configurados para recibir alertas críticas de "proxy web".
12.5.2-007	MD		- Se introduce una nueva notificación de actualización de categorías de URL en el banner. También se envía a los usuarios una notificación por correo electrónico sobre las próximas actualizaciones de categorías de URL.
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	- Desde la versión 12.5.4 de Cisco AsyncOS, TLSv1.2 está habilitado de forma predeterminada para la interfaz de usuario web de administración de dispositivos. - Después de una actualización a la versión 12.5.4 de Cisco AsyncOS, la reanudación de la sesión está deshabilitada de forma predeterminada. - El mensaje se agrega para indicar el fin del soporte para CDA en la sección de configuración de CDA	
12.5.4-011	MD-Refresh		
12.5.5-004	MD		- Después de una actualización a Cisco AsyncOS 12.5, recibirá un mensaje para reiniciar el proceso proxy cuando ejecute el comando networktuning por primera vez.

12.5.5-008	MD-Refresh		
12.5.6-008	MD		
14.0.1-014	LD	- De forma predeterminada, la función HTTP 2.0 está desactivada. Para habilitar esta característica, utilice el comando <HTTP2>. - AsyncOS 14.0 para Cisco Web Security Appliance admite la reanudación de la sesión de TLSv1.3 en el cliente y el servidor. - Se modifican los períodos de validez de estos certificados: • HTTPS • ISE • SAAS • Certificados de dispositivo • Certificado de administración/demostración - La CLI y la GUI del dispositivo ahora muestran un mensaje cuando falla una actualización debido a un nombre de registro y un nombre de archivo no válidos en las suscripciones de registro. - De forma predeterminada, el intervalo de sondeo se establece en 24 horas. - Después de actualizar a esta versión, no puede realizar la prueba de inicio para la autenticación LDAP si el campo DN base (nombre distintivo base) (Red > Autenticación > Agregar rango) está vacío.	- El dispositivo de seguridad Cisco Web Security Appliance ahora admite la integración con Cisco SecureX. - Puede configurar perfiles de encabezado personalizados para solicitudes HTTP y puede crear varios encabezados bajo un perfil de reescritura de encabezado. - Ahora puede configurar el esquema de autenticación basada en encabezado para un directorio activo. El cliente y el dispositivo de seguridad web consideran que el usuario está autenticado y no vuelven a solicitar la autenticación ni las credenciales de usuario. La función X-Authenticated funciona cuando el dispositivo de seguridad web actúa como un dispositivo ascendente. - Se ha mejorado el panel de estado del sistema del dispositivo: • Ficha Capacidad: una ficha que proporciona detalles sobre el rango de tiempo, el uso de memoria y CPU del sistema, el ancho de banda y RPS, el uso de CPU por función y las conexiones de cliente o servidor. • Las Características de tráfico de proxy de la ficha Estado proporcionan detalles de las conexiones de cliente y servidor. • El tiempo de respuesta del servicio ahora incluye más detalles sobre los gráficos de barras y también datos de leyenda de fechas anteriores.

			- Ahora puede recuperar la información de configuración y realizar cambios (como modificar la información actual, agregar una nueva información o eliminar una entrada) en los datos de configuración del dispositivo mediante API REST para políticas de gestión, políticas de acceso y políticas de omisión - La versión 14.0 de Cisco AsyncOS admite HTTP 2.0 para solicitudes y respuestas web sobre TLS. La compatibilidad con HTTP 2.0 requiere la negociación basada en TLS ALPN, que solo está disponible a partir de la versión TLS 1.2. En esta versión, HTTPS 2.0 no es compatible con estas funciones: • Toque Tráfico web • DLP externa • Ancho de banda total y ancho de banda de aplicaciones - Se introduce un nuevo comando CLI <HTTP2> para habilitar o deshabilitar las configuraciones HTTP 2.0. No puede activar ni desactivar HTTP 2.0 ni restringir el dominio para HTTP 2.0 a través de la interfaz de usuario web del dispositivo. - La configuración de HTTP 2.0 no es compatible con Cisco Secure Email and Web Manager - La CLI muestra el nuevo mensaje de advertencia cuando intenta utilizar el certificado predeterminado de cualquiera de estas funciones: • Certificado del dispositivo (en la interfaz de usuario web, vaya a Red > Administración de certificados > Certificado del dispositivo) • Certificado de cifrado de credenciales (en la interfaz de

			usuario web, vaya a Red > Autenticación > Editar configuración > Sección Avanzadas) • Certificado de IU de gestión de HTTPS (en la interfaz de línea de comandos, utilice certconfig > SETUP) - Se agrega un nuevo subcomando OCSPVALIDATION_FOR_SERVER_CERT bajo el comando certconfig. Con este nuevo subcomando puede habilitar la validación de OCSP para los certificados de servidor LDAP y Updater. Si la validación de certificados está habilitada, puede recibir una alerta si se revocan los certificados implicados en la comunicación. - Se agrega un nuevo comando CLI recopilerdconfig para configurar la funcionalidad de sondeo entre el dispositivo y el servidor de autenticación. - Ahora puede elegir entre la interfaz de administración y de datos, mientras configura la función de licencia inteligente en el dispositivo.
14.0.1-040	LD	- Cuando habilita las licencias de software inteligentes y registra su dispositivo de seguridad web con Cisco Smart Software Manager, los servicios en la nube de Cisco (Red > Configuración de servicios en la nube) habilita y registra automáticamente su dispositivo web seguro a través del portal de servicios en la nube de Cisco. - No puede desactivar ni anular el registro del servicio en la nube de Cisco si se ha registrado la licencia inteligente en su dispositivo.	- Puede ver los detalles de la cuenta inteligente creada en el portal de Cisco Smart Software Manager desde el comando smartaccount info en la CLI. - Si el certificado de los servicios en la nube de Cisco ha caducado o está a punto de hacerlo, el servicio en la nube de Cisco renueva automáticamente el certificado después de la actualización a AsyncOS 14.0.1-040. - Si el certificado de Cisco Cloud Services ha caducado, ahora puede descargar un nuevo certificado del portal de Cisco Talos Intelligence Services del subcomando cloudserviceconfig > fetchcertificate en la CLI.

		- Si ya ha registrado sus dispositivos en Cisco Smart Software Manager y no ha configurado los servicios en la nube de Cisco, los servicios en la nube de Cisco se habilitan automáticamente después de actualizar a AsyncOS 14.0.1-040. De forma predeterminada, la región se registra como América y puede modificarla (Europa y APJC) según sea necesario. - No puede desactivar ni anular el registro del servicio en la nube de Cisco si la licencia inteligente está registrada en su dispositivo.	- Puede registrar automáticamente el dispositivo de seguridad web con el portal de servicios en la nube de Cisco (subcomando cloudserviceconfig > autoregister en la CLI) - Puede cargar el certificado para el dispositivo virtual y los dispositivos de hardware desde el subcomando updateconfig > clientcertificate en la CLI. - Se introduce una nueva notificación de actualización de categorías de URL en el banner. También se envía una notificación por correo electrónico a los usuarios sobre las próximas actualizaciones de categorías de URL.
14.0.1-053	GD		
14.0.1-503	HP		
14.0.2-012	MD	- En la versión 14.0.2 de Cisco AsyncOS, TLSv1.2 está habilitado de forma predeterminada para la Interfaz de usuario web de administración de dispositivos en Administrador del sistema > Configuración SSL. - La reanudación de la sesión está desactivada de forma predeterminada.	- Se agrega un mensaje para indicar el fin del soporte para CDA en la sección de configuración de CDA. - Ahora puede elegir entre la interfaz de datos o de administración para Smart License Registration en la lista desplegable Test Interface .
14.0.3-014	MD	- Después de una actualización a Cisco AsyncOS 14.0, recibirá un mensaje para reiniciar el proceso proxy cuando ejecute el comando networktuning por primera vez.	
14.0.3-502	HP	- Cuando Secure Web Appliance	

		funciona en modo de alto rendimiento, el agotamiento del límite de montón desactiva la alta latencia y acepta controladores. Esto reduce el número de conexiones.	
14.0.4-005	MD		
14.5.0-498	LD	- Cambio de marca del producto: • AMP para terminales, protección frente a malware avanzado y AMP se han cambiado a Terminal seguro • Thread Grid (Análisis de archivos) cambiado a Malware Analytics - La solicitud de clasificación errónea se envía a través de HTTPS y, por lo tanto, no recibe notificaciones de alertas de seguridad. - La versión de Samba se ha actualizado a la versión 4.11.15. - TLSv1.2 está habilitado de forma predeterminada para la interfaz de usuario web de administración de dispositivos en Administrador del sistema > Configuración SSL . - En una instalación nueva de AsyncOS 14.5, el valor de las configuraciones de certificado de Hostname caducado y no coincidente en la página HTTPS Proxy está seleccionado de forma predeterminada como Drop en lugar de Monitor.	- El dispositivo web seguro ahora puede validar la respuesta DNS recibida del servidor DNS que admite firmas criptográficas. - El dispositivo web seguro restringe el número de conexiones simultáneas iniciadas por el cliente a un valor configurado. - Con la versión 14.5 de AsyncOS, Cisco Web Security Appliance se ha cambiado a Cisco Secure Web Appliance - La etiqueta de decisión de registro de acceso del grupo de políticas de descifrado se agrega con EUN (notificación de usuario final) cuando aparece la página EUN en el navegador web del cliente. - La función de clonación de directivas permite copiar o clonar las configuraciones de una directiva y crear una nueva directiva. - Puede administrar el ancho de banda del tráfico configurando el valor del ancho de banda en el perfil de cuota y asignando el perfil de cuota en la categoría de URL de la política de acceso o la cuota de actividad web general. - API REST para configurar políticas de gestión, políticas de descifrado, políticas de routing, políticas de suplantación de IP,

			Anti-Malware y reputación, rangos de autenticación, Cisco Smart Software License, Cisco Umbrella Seamless ID, servicios de identidad y configuración del sistema. - Puede integrar la implementación de ISE-SXP con Cisco Secure Web Appliance para la autenticación pasiva. Esto le permite obtener todas las asignaciones definidas, incluidas las asignaciones de dirección SGT a IP que se publican a través de SXP. - La función Cisco Umbrella Seamless ID permite que el dispositivo transfiera la información de identificación del usuario a Cisco Umbrella Secure Web Gateway (SWG) después de una autenticación correcta. - Se agrega un mensaje para indicar el fin del soporte para CDA en la sección de configuración de CDA. - Ahora puede elegir entre la interfaz de datos o de administración para Smart License Registration en la lista desplegable Test Interface . - Después de una actualización a Cisco AsyncOS 14.5, recibirá un mensaje para reiniciar el proceso proxy cuando ejecute el comando networktuning por primera vez.
14.5.0-537	GD		- Cisco Secure Email and Web Manager (SMA) también puede gestionar estas políticas con la opción de clonación en Secure Web Appliance: • Política de acceso • Perfil de identificación • Política de descifrado • Política de enrutamiento

14.5.1-008	MD		
14.5.1-016	MD		
14.6.0-108	LD		- AsyncOS 14.6 proporciona compatibilidad con Cisco Umbrella con Cisco Secure Web Appliance (SWA). La integración de Umbrella y Secure Web Appliance facilita la implementación de políticas web comunes de Umbrella a Secure Web Appliance.
15.0.0-322	LD	- La versión de FreeBSD ha sido actualizada a FreeBSD 13.0. - Cisco SSL versión 1.0.2 a Cisco SSL versión 1.1.1. - Se han actualizado los motores Talos como AVC, WBRSD, DCA y Beaker. - Se han actualizado los motores de análisis como Webroot y McAfee.	- Estas mejoras realizadas en la función de licencias de software inteligente: • Reserva de licencia • Conversión basada en dispositivo: después de registrar un dispositivo web seguro con una licencia inteligente, todas las licencias clásicas válidas actuales se convierten automáticamente en licencias inteligentes con el proceso Conversión basada en dispositivo (DLC). Estas licencias convertidas se actualizan en la cuenta virtual del portal CSSM. - Puede administrar el ancho de banda del tráfico configurando el valor del ancho de banda en el perfil de cuota y asignando el perfil de cuota en la política de descifrado y la política de acceso, la categoría de URL o la cuota de actividad web general. - La función de clonación de directivas permite copiar o clonar las configuraciones de una directiva y crear una nueva directiva. - Motor de descubrimiento y control de aplicaciones (ADC): un componente de política de uso

			aceptable que inspecciona el tráfico web para obtener un mayor conocimiento y control del tráfico web utilizado para las aplicaciones. Con AsyncOS 15.0, puede utilizar AVC o el motor ADC para supervisar el tráfico web. AVC está activado de forma predeterminada. El motor ADC admite el modo de alto rendimiento. - API REST para configuración de ADC - El administrador puede optar por configurar un nombre de usuario SNMPv3 personalizado que no sea el nombre de usuario predeterminado v3get. - La longitud máxima del encabezado personalizado es 16k. - Opción para elegir la interfaz de túnel seguro y la conexión de acceso remoto.
15.0.0-335	GD	- Conversión basada en dispositivo: después de registrar un dispositivo web seguro con licencias inteligentes, todas las licencias clásicas válidas actuales se convierten automáticamente en licencias inteligentes con el proceso Conversión basada en dispositivo (DLC). Estas licencias convertidas se actualizan en la cuenta virtual del portal CSSM. - AVC está activado de forma predeterminada. - Cisco SSL versión 1.0.2 a Cisco SSL versión 1.1.1 - Se han actualizado los motores Talos como AVC, WBRSD, DCA y Beaker. - Se han actualizado los motores	- Reserva de licencias: puede reservar licencias para funciones habilitadas en Secure Web Appliance sin conectarse al portal Cisco Smart Software Manager (CSSM). Esto resulta principalmente beneficioso para los usuarios que implementan Secure Web Appliance en un entorno de red altamente seguro sin comunicación a Internet ni a dispositivos externos. - Puede administrar el ancho de banda del tráfico configurando el valor del ancho de banda en el perfil de cuota y asignando el perfil de cuota en la categoría de URL de política de descifrado y política de acceso o la cuota de actividad web general. - La función de clonación de directivas permite copiar o clonar las configuraciones de una directiva y crear una nueva directiva.

		de análisis como Webroot y McAfee. - FreeBSD 13.0 es compatible solamente con la versión 1.1.1 de Cisco SSL. Solo los algoritmos de cifrado, mac y kex compatibles con Cisco SSH pueden ser soportados para la conectividad SSH a FreeBSD 13.0. - La función DCA de Secure Web Appliance está desactivada como parte de la versión AsyncOS15.0 GD.Puede activarla después de actualizar a esta versión accediendo a Servicios de seguridad>Controles de uso aceptable y marcando la casilla de verificación DCA. - Las operaciones SNMPWALK/SNMPGET para los OID SNMP para la memoria Malloc de proxy no se soportan en los SWA multiproxy (S690, S695, S1000V).	- Admite el motor Application Discovery and Control (ADC), un componente de política de uso aceptable que inspecciona el tráfico web para obtener una comprensión y un control más profundos del tráfico web utilizado para las aplicaciones. ahora puede utilizar el motor AVC o ADC para supervisar el tráfico web. - El motor ADC admite el modo de alto rendimiento. - Ahora puede recuperar la información de configuración y realizar cualquier cambio (como modificar la información actual, agregar una nueva información o eliminar una entrada) en los datos de configuración de la directiva de acceso del dispositivo con las API REST. -Ael administrador puede optar por configurar un nombre de usuario SNMPv3 personalizado que no sea el nombre de usuario predeterminado v3get. - La longitud máxima de los encabezados personalizados para las solicitudes web es 16k. - Opción para elegir la interfaz de túnel seguro y la conexión de acceso remoto

Componentes de código abierto

A continuación se muestra la lista de cambios en el componente de código abierto utilizado en SWA:

Versión	11.8.X	12.0.X	12.5.X	14.0.X	14.5.X	14.6.X	15.0.X
freebsd	10.4	10.4	10.4	11.2	11.2	11.2	13.0

Información Relacionada

- Notas de la versión de AsyncOS 12.0 para Cisco Web Security Appliances: Cisco
- Notas de la versión de AsyncOS 12.5 para Cisco Web Security Appliances: Cisco
- Notas de la versión de AsyncOS 14.0 para Cisco Web Security Appliances: Cisco
- Notas de la versión de AsyncOS 14.5 para Cisco Secure Web Appliance: Cisco
- ¿Cuál es la terminología de la versión para la seguridad de contenido? (cisco.com)
- Guía de instalación de Cisco Secure Email and Web Virtual Appliance
- Soporte Técnico y Documentación - Cisco Systems

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).