Modifications de version de Secure Web Appliance

Table des matières

Introduction

Ce document décrit les principales modifications et les fonctionnalités ajoutées dans différentes versions de Secure Web Appliance (SWA).

Conditions préalables

Exigences

Il n'y a pas d'exigences particulières pour cet article.

Les abréviations utilisées dans ces articles sont les suivantes :

LD : déploiement limité.

GD : Déploiement général.

MD : déploiement de maintenance

ED : Déploiement précoce.

HP : correctif à chaud.

CLI : interface de ligne de commande.

GUI : interface utilisateur graphique

HTTP : Hypertext Transfer Protocol.

HTTPS : Protocole de transfert hypertexte sécurisé.

ECDSA : Algorithme de signature numérique à courbe elliptique.

PID : identificateur de processus.

CTR : Cisco Threat Response.

AMP : Advanced Malware Protection.

URL : Uniform Resource Locator.

ADC : Agent de répertoire de contexte.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Historique des modifications par version

Version	Type	Changements de comportement	Améliorations / Fonctionnalités ajoutées
12.0.1-268	LD	- Les exigences en matière de CPU et de mémoire du système sont modifiées à partir de la version 12.0. - Par défaut, TLSv1.3 est activé sur l'appliance. - Le chiffre « TLS_AES_256_GCM_SHA384 » est ajouté à la liste de chiffrement par défaut.	- La version 12.0 de Cisco AsyncOS fournit un dispositif de sécurité Web avec hautes performances (HP) pour les plates-formes S680, S690 et S695. - Une nouvelle sous-commande **high performance** est ajoutée sous la commande **advanced proxyconfig** principale pour activer et désactiver le mode haute performance. - Intégration du SWA au portail Cisco Threat Response (CTR). - L'appliance prend en charge la version TLSv1.3. - La fonction de sauvegarde du fichier de configuration est déplacée du sous-menu « **Log Subscriptions** » vers « **Configuration File** » sous **System Administration**. - L'appliance prend désormais en charge le téléchargement du certificat **ECDSA** pour le proxy **HTTPS**. - Une nouvelle sous-commande diagnostic **CLI proxyscannermap** est ajoutée sous **diagnostic** > **proxy**. Tto affiche le mappage **PID** entre chaque proxy et le processus d'analyseur correspondant. - La nouvelle option **searchdetails** est ajoutée sous la commande **CLI authcache**. - La nouvelle sous-commande **CTROBSERVABLE** est ajoutée sous la

			commande **CLI reportingconfig** pour activer ou désactiver l'indexation basée sur l'observation de **CTR**.
12.0.1-334	DIEU		- Une nouvelle sous-commande scanners est ajoutée sous la commande **advanced proxyconfig** principale pour exclure les types MIME à analyser par le moteur **AMP**.
12.0.2-004	MD	- Utilisez TLS 1.2 ou les versions ultérieures pour connecter l'appliance au serveur AMP File Reputation. - AMERICAS (Legacy) cloud-sa.amp.sourcefire.com ne peut pas être configuré sur l'appliance.	- Une nouvelle option « Entrez le nombre d'analyses simultanées à prendre en charge par AMP » est ajoutée dans la commande **CLI** principale **advanced proxyconfig** > **scanners** > **AMP**. vous pouvez modifier le verdict Unscannable par défaut de l'éviction de l'analyse en cours d'exécution en Timeout et vice-versa à partir de la nouvelle **éviction de** sous-commande de l'interface de ligne de commande dans la commande principale de l'**interface de ligne de commande advanced proxyconfig** > **scanners**.
12.02-012	MD		- Des messages d'alerte sont déclenchés sur l'interface utilisateur Web de l'appliance Lorsque la **mémoire Malloc** proxy dépasse 90 % de la limite de mémoire Malloc proxy et qu'une notification par e-mail est envoyée à tous les « destinataires d'alertes » configurés pour recevoir des alertes critiques de « Proxy Web ». - La nouvelle interface Web offre une nouvelle apparence pour la **surveillance** des rapports et le **suivi des** services Web.
12.0.3-005	MD		
12.0.3-007	MD		- Notification de mise à jour des nouvelles catégories d'**URL**
12.0.4-002	MD		
12.0.5-011	MD	- TLSv1.2 est activé par défaut pour	- Un message est ajouté pour indiquer la fin

		l'interface utilisateur Web de gestion du matériel - La **reprise de session** est désactivée par défaut.	de la prise en charge de CDA dans la section de configuration CDA.
12.5.1-011	LD	- Par défaut, la fonctionnalité Cisco Success Network est activée sur l'appliance. - Ces journaux sont modifiés pour inclure plus de détails : Les journaux d'accès affichent désormais le nom d'utilisateur lorsque l'authentification échoue. Les journaux du cadre d'authentification affichent maintenant l'adresse IP du client pour ces protocoles d'authentification ayant échoué : NTLM, BASIC, SSO (transparent)	- La version 12.5 de Cisco AsyncOS fournit un dispositif de sécurité Web avec hautes performances (HP) pour les plates-formes S680, S690 et S695. Ceci augmente les performances de trafic des appliances haut de gamme actuelles. - Vous pouvez désormais passer à la version 12.5 et utiliser le mode hautes performances sur les modèles (S680, S690, S695, S680F, S690F et S695F), même si vous avez activé les fonctionnalités suivantes sur votre appliance : • Robinet Trafic Web • Quotas de volume et de temps • Limites de bande passante globales - Vous pouvez maintenant configurer l'usurpation IP du proxy Web en créant un profil d'usurpation IP et en l'ajoutant aux stratégies de routage. - Vous pouvez maintenant créer une catégorie d'URL personnalisée pour YouTube et définir des stratégies sur la catégorie personnalisée YouTube pour un contrôle d'accès sécurisé. - Dans la nouvelle interface Web, l'appliance dispose d'une nouvelle page (Surveillance > État du système) pour afficher l'état actuel et la configuration de l'appliance. - La fonctionnalité Cisco Success Network (CSN) permet à Cisco de collecter des données télémétriques sur l'utilisation des fonctionnalités de l'appliance. - API REST pour le réseau, l'abonnement au journal et d'autres configurations.
12.5.1-035	DIEU	- Dépréciation de TLS 1.0/1.1 : Utilisez TLS 1.2 ou les versions ultérieures pour connecter l'appliance au serveur AMP File	- La configuration de la taille du cache pour l'authentification (Réseau > Authentification > Paramètres d'authentification > Options du cache des informations d'identification) n'est pas prise en charge par AsyncOS 12.5.1-035

		Reputation. AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com** est supprimé de la liste des serveurs de réputation de fichiers AMP. AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com** ne peut donc pas être configuré sur l'appliance.	et les versions ultérieures.
12.5.1-043	DIEU		- Les messages d'alerte s'affichent dans l'interface utilisateur Web de l'appliance (Administration système > Alertes > Afficher les alertes principales) : • lorsque la mémoire malloc proxy dépasse 90 % de la limite de mémoire malloc proxy • lorsque le proxy est redémarré sur 100 % de la mémoire malloc Dans les deux cas, une notification par e-mail est envoyée à tous les « destinataires d'alertes » configurés pour recevoir des alertes critiques de « Proxy Web ».
12.5.2-007	MD		- Une nouvelle notification de mise à jour des catégories d'URL est introduite dans la bannière. Une notification par e-mail sur les prochaines mises à jour de catégorie d'URL est également envoyée aux utilisateurs.
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	- À partir de la version 12.5.4 de Cisco AsyncOS, TLSv1.2 est activé par défaut pour l'interface utilisateur Web de gestion du matériel. - Après une mise à niveau vers Cisco AsyncOS 12.5.4, la reprise de session est désactivée par défaut. - Le message est ajouté pour indiquer la fin de la prise en charge de CDA dans la section de configuration CDA	

12.5.4-011	MD-Refresh		
12.5.5-004	MD		- Après une mise à niveau vers Cisco AsyncOS 12.5, un message vous invite à redémarrer le processus proxy lorsque vous exécutez la commande **networktuning** pour la première fois.
12.5.5-008	MD-Refresh		
14.0.1-014	LD	- Par défaut, la fonctionnalité HTTP 2.0 est désactivée. Pour activer cette fonctionnalité, utilisez la commande <HTTP2>. - AsyncOS 14.0 for Cisco Web Security Appliance prend en charge la reprise de session TLSv1.3 sur le client et le serveur. - Les périodes de validité de ces certificats sont modifiées : • HTTPS • ISE • SAAS • Certificats d'appareil • Certificat de démonstration/gestion - L'interface de ligne de commande et l'interface utilisateur graphique de l'appliance affichent désormais un message lorsqu'une mise à niveau échoue en raison d'un nom de journal et d'un nom de fichier non valides dans les abonnements au journal. - Par défaut, l'intervalle d'interrogation est défini sur 24 heures. - Après la mise à niveau vers cette version, vous ne pouvez pas effectuer le test de démarrage pour l'authentification LDAP si le champ Base DN (Base Distinguished Name) (Réseau > Authentification > Ajouter un domaine) est vide.	- L'appliance de sécurité Web Cisco prend désormais en charge l'intégration avec Cisco SecureX. - Vous pouvez configurer des profils d'en-tête personnalisés pour les requêtes HTTP et créer plusieurs en-têtes sous un profil de réécriture d'en-tête. - Vous pouvez maintenant configurer le schéma d'authentification basé sur l'en-tête pour un Active Directory. Le client et l'appareil de sécurité Web considèrent l'utilisateur comme authentifié et ne demandent pas à nouveau l'authentification ou les informations d'identification de l'utilisateur. La fonctionnalité X-Authenticated fonctionne lorsque l'appareil de sécurité Web agit comme un périphérique en amont. - Le tableau de bord d'état du système de l'appliance a été amélioré : • Onglet Capacity : onglet fournissant des détails sur la plage de temps, l'utilisation de l'UC et de la mémoire du système, la bande passante et le RPS, l'utilisation de l'UC par fonction et les connexions client ou serveur. • Les caractéristiques du trafic proxy sous l'onglet État fournissent des détails sur les connexions client et serveur. • Le temps de réponse du service inclut désormais plus de détails sur les

			graphiques à barres et également des données de légende pour les dates précédentes. - Vous pouvez désormais récupérer des informations de configuration et effectuer des modifications (telles que la modification des informations actuelles, l'ajout d'une nouvelle information ou la suppression d'une entrée) dans les données de configuration de l'appliance. Utilisez les API REST pour les stratégies de gestion, les stratégies d'accès et les stratégies de contournement - La version 14.0 de Cisco AsyncOS prend en charge HTTP 2.0 pour les requêtes et les réponses Web sur TLS. La prise en charge de HTTP 2.0 nécessite une négociation basée sur ALPN TLS, qui n'est disponible qu'à partir de la version TLS 1.2. Dans cette version, HTTPS 2.0 n'est pas pris en charge pour les fonctionnalités suivantes : • Robinet Trafic Web • DLP externe • Bande passante globale et bande passante des applications - Une nouvelle commande CLI <HTTP2> est introduite pour activer ou désactiver les configurations HTTP 2.0. Vous ne pouvez pas activer ou désactiver HTTP 2.0 et restreindre le domaine pour HTTP 2.0 via l'interface utilisateur Web de l'appliance. - La configuration de HTTP 2.0 n'est pas prise en charge par Cisco Secure Email and Web Manager - L'interface de ligne de commande affiche le nouveau message d'avertissement lorsque vous essayez d'utiliser le certificat par défaut de l'une de ces fonctions : • Certificat d'appareil (dans l'interface utilisateur Web, accédez à Réseau > Gestion des certificats > Certificat d'appareil) • Certificat de chiffrement des informations d'identification (dans l'interface utilisateur Web, accédez à Réseau > Authentification > Modifier les paramètres > Section Avancé)

			• Certificat de l'interface utilisateur de gestion HTTPS (dans l'interface de ligne de commande, utilisez certconfig > SETUP) - Une nouvelle sous-commande OCSPVALIDATION_FOR_SERVER_CERT est ajoutée sous **certconfig**. Avec cette nouvelle sous-commande, vous pouvez activer la validation OCSP pour les certificats de serveur LDAP et Updater. Si la validation du certificat est activée, vous pouvez recevoir une alerte si les certificats impliqués dans la communication sont révoqués. - Une nouvelle commande CLI **rassemberdconfig** est ajoutée pour configurer la fonctionnalité d'interrogation entre l'appliance et le serveur d'authentification. - Vous pouvez désormais choisir entre l'interface de gestion et l'interface de données, tout en configurant la fonction de licence Smart sur l'appliance.
14.0.1-040	LD	- Lorsque vous activez les licences logicielles intelligentes et que vous enregistrez votre appareil de sécurité Web avec Cisco Smart Software Manager, les services cloud Cisco (Network > Cloud Service Settings) active et enregistre automatiquement votre appliance Web sécurisée via le portail Cisco Cloud Services. - Vous ne pouvez pas désactiver ou annuler l'enregistrement de Cisco Cloud Service si la licence Smart est enregistrée sur votre appliance. - Si vous avez déjà enregistré vos appareils auprès de Cisco Smart Software Manager et que vous n'avez pas configuré les services cloud Cisco, les services cloud Cisco sont automatiquement activés après la mise à niveau vers AsyncOS 14.0.1-040. Par défaut, la région est enregistrée en tant qu'Amérique et vous pouvez la modifier (Europe et APJC) si nécessaire.	- Vous pouvez afficher les détails du compte Smart créé dans le portail Cisco Smart Software Manager à l'aide de la commande **smartaccount tinfo** dans l'interface de ligne de commande. - Si le certificat des services cloud Cisco a expiré ou est sur le point d'expirer, le service cloud Cisco renouvelle automatiquement le certificat après la mise à niveau vers AsyncOS 14.0.1-040. - Si le certificat Cisco Cloud Services a expiré, vous pouvez maintenant télécharger un nouveau certificat à partir du portail Cisco Talos Intelligence Services à partir de la sous-commande **cloudserviceconfig** > **fetchcertificate** dans l'interface de ligne de commande. - Vous pouvez enregistrer automatiquement l'appliance de sécurité Web avec le portail de service cloud Cisco (**cloudserviceconfig** > sous-commande **autoregister** dans la CLI) - Vous pouvez charger le certificat pour l'appliance virtuelle et les appliances

		- Vous ne pouvez pas désactiver ou annuler l'enregistrement de Cisco Cloud Service si la licence Smart est enregistrée sur votre appliance.	matérielles à partir de la sous-commande **updateconfig** > **clientcertificate** dans l'interface de ligne de commande. - Une nouvelle notification de mise à jour des catégories d'URL est introduite dans la bannière. Une notification par e-mail est également envoyée aux utilisateurs concernant les prochaines mises à jour de catégorie d'URL.
14.0.1-053	DIEU		
14.0.1-503	HP		
14.0.2-012	MD	- Dans la version 14.0.2 de Cisco AsyncOS, TLSv1.2 est activé par défaut pour l'interface utilisateur Web de gestion du matériel sous Administrateur système > Configuration SSL. - La reprise de session est désactivée par défaut.	- Un message est ajouté pour indiquer la fin de la prise en charge de CDA dans la section de configuration CDA. - Vous pouvez maintenant choisir entre l'interface de données ou l'interface de gestion pour l'enregistrement de licence Smart dans la liste déroulante Interface de test.
14.0.3-014	MD	- Après une mise à niveau vers Cisco AsyncOS 14.0, un message vous invite à redémarrer le processus proxy lorsque vous exécutez la commande **networktuning** pour la première fois.	
14.0.3-502	HP	- Lorsque Secure Web Appliance fonctionne en mode hautes performances, l'épuisement de la limite de tas désactive la latence élevée et accepte les gestionnaires. Il en résulte un nombre moins élevé de connexions.	
14.0.4-005	MD		
14.5.0-498	LD	- Rebranding du produit : • AMP for Endpoints, Advanced Malware Protection et AMP ont été	- L'appliance Web sécurisée peut désormais valider la réponse DNS reçue du serveur DNS qui prend en charge les signatures cryptographiques.

		remplacés par **Terminaux sécurisés** • Thread Grid (Analyse de fichiers) est passé à **Malware Analytics** - La demande d'erreur de classification est envoyée via HTTPS et par conséquent vous ne recevez pas de notifications d'alerte de sécurité. - La version Samba a été mise à niveau vers la version 4.11.15. - TLSv1.2 est activé par défaut pour l'interface utilisateur Web Appliance Management sous System Administrator > SSL Configuration . - Lors d'une nouvelle installation d'AsyncOS 14.5, la valeur des configurations de certificats de nom d'hôte expiré et non concordant dans la page Proxy HTTPS est sélectionnée par défaut comme **Abandon** au lieu de **Surveillance**.	- L'appliance Web sécurisée limite le nombre de connexions simultanées initiées par le client à une valeur configurée. - Avec AsyncOS version 14.5, Cisco Web Security Appliance a été renommé Cisco Secure Web Appliance - La balise de décision accesslog dans le groupe Decrypt Policy est ajoutée à EUN (End user Notification) lorsque la page EUN apparaît dans le navigateur Web du client. - La fonction de stratégie de clonage vous permet de copier ou de cloner les configurations d'une stratégie et de créer une nouvelle stratégie. - Vous pouvez gérer la bande passante du trafic en configurant la valeur de bande passante dans le profil de quota et en mappant le profil de quota dans la catégorie d'URL de stratégie d'accès ou le quota d'activité Web global. - API REST pour configurer les politiques de gestion, les politiques de décryptage, les politiques de routage, les politiques d'usurpation d'adresse IP, la protection contre les programmes malveillants et la réputation, les domaines d'authentification, la licence logicielle Cisco Smart, l'ID transparent Cisco Umbrella, les services d'identité et la configuration du système. - Vous pouvez intégrer le déploiement ISE-SXP avec l'appliance Web sécurisé Cisco pour une authentification passive. Cela vous permet d'obtenir tous les mappages définis, y compris les mappages d'adresses SGT à IP qui sont publiés via SXP. - La fonctionnalité Cisco Umbrella Seamless ID permet à l'appliance de transmettre les informations d'identification de l'utilisateur à Cisco Umbrella Secure Web Gateway (SWG) après une authentification réussie. - Un message est ajouté pour indiquer la fin de la prise en charge de CDA dans la section de configuration CDA. - Vous pouvez maintenant choisir entre l'interface de données ou l'interface de gestion

			pour l'enregistrement de licence Smart dans la liste déroulante Interface de test. - Après une mise à niveau vers Cisco AsyncOS 14.5, un message vous invite à redémarrer le processus proxy lorsque vous exécutez la commande **networktuning** pour la première fois.
14.5.0-537	DIEU		- Ces politiques avec l'option clone dans Secure Web Appliance peuvent également être gérées par Cisco Secure Email and Web Manager (SMA) : • Politique d'accès • Profil d'identification • Politique de déchiffrement • Politique de routage
14.5.1-008	MD		
14.5.1-016	MD		
14.6.0-108	LD		- AsyncOS 14.6 prend en charge Cisco Umbrella avec Cisco Secure Web Appliance (SWA). L'intégration d'Umbrella et de Secure Web Appliance facilite le déploiement de politiques Web communes d'Umbrella à Secure Web Appliance.
15.0.0-322	LD	- La version FreeBSD a été mise à jour vers FreeBSD 13.0. - Cisco SSL version 1.0.2 à Cisco SSL version 1.1.1. - Les moteurs Talos tels que AVC, WBRSD, DCA et Beaker ont été mis à niveau. - Les moteurs d'analyse tels que Webroot et McAfee ont été mis à niveau.	- Les améliorations suivantes ont été apportées à la fonction Smart Software Licensing : • Réservation de licence • Conversion avec dispositif : une fois que vous avez enregistré l'appareil Web sécurisé avec une licence Smart, toutes les licences classiques valides sont automatiquement converties en licences Smart à l'aide du processus de conversion avec dispositif (DLC). Ces licences converties sont mises à jour dans le compte virtuel du portail CSSM. - Vous pouvez gérer la bande passante du trafic en configurant la valeur de bande

			passante dans le profil de quota et en mappant le profil de quota dans la stratégie de déchiffrement et la stratégie d'accès, la catégorie d'URL ou le quota d'activité Web global. - La fonction de stratégie de clonage vous permet de copier ou de cloner les configurations d'une stratégie et de créer une nouvelle stratégie. - Moteur ADC (Application Discovery and Control) : un composant de politique d'utilisation acceptable qui inspecte le trafic web afin de mieux comprendre et contrôler le trafic web utilisé pour les applications. Avec AsyncOS 15.0, vous pouvez utiliser le moteur AVC ou ADC pour surveiller le trafic Web. Par défaut, AVC est activé. Le moteur ADC prend en charge le mode hautes performances. - API REST pour la configuration ADC - L'administrateur peut choisir de configurer un nom d'utilisateur SNMPv3 personnalisé autre que le nom d'utilisateur par défaut v3get. - La longueur maximale de l'en-tête personnalisé est de 16 Ko. - Option permettant de choisir l'interface de tunnel sécurisée et la connexion d'accès à distance.

Composants Open Source

Voici la liste des modifications apportées au composant open source utilisé dans SWA :

Version	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

Informations connexes

- Notes de version d'AsyncOS 12.0 pour les appareils de sécurité Web Cisco - Cisco
- Notes de version d'AsyncOS 12.5 pour les appareils de sécurité Web Cisco - Cisco
- Notes de version d'AsyncOS 14.0 pour les appareils de sécurité Web Cisco - Cisco
- Notes de version d'AsyncOS 14.5 pour Cisco Secure Web Appliance - Cisco
- Quelle est la terminologie de la version relative à la sécurité du contenu ? (cisco.com)
- Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web
- **Assistance et documentation techniques - Cisco Systems**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.