Notes de version pour AsyncOS 14.5 pour Cisco Secure Web Appliance

Première publication : 2022-04-11

Dernière modification : 2024-01-31

À propos de Secure Web Appliance

Cisco Secure Web Appliance intercepte et surveille le trafic Internet et applique des politiques pour protéger votre réseau interne contre les programmes malveillants, les pertes de données sensibles, la perte de productivité et d'autres menaces Internet.

Nouveautés

Nouveautés d'AsyncOS 14.5.2-011 MD (déploiement de maintenance)

Cette version contient un certain nombre de corrections de bogues; consultez la section Problèmes connus et résolus dans la version 14.5.2-011, à la page 19 pour en savoir plus.

Nouveautés d'AsyncOS 14.5.1-016 MD (déploiement de maintenance) : actualisation

Cette version contient un certain nombre de corrections de bogues; consultez la section Problèmes connus et résolus dans la version 14.5.1-016, à la page 19 pour en savoir plus.

Nouveautés d'AsyncOS 14.5.1-008 MD (déploiement de maintenance)

Cette version contient un certain nombre de corrections de bogues; consultez la section Problèmes connus et résolus dans la version 14.5.1-008, à la page 19 pour en savoir plus.

Nouveautés d'AsyncOS 14.5.0-537 GD (déploiement général)

Cette version contient un certain nombre de corrections de bogues; consultez la section Problèmes connus et résolus dans la version 14.5.0-537, à la page 19 pour en savoir plus.

Nouveautés d'AsyncOS 14.5.0-498 LD (déploiement limité)

Les fonctionnalités suivantes sont intégrées à cette version :

<table>
<tr><th>Fonctionnalités</th><th colspan="2">Description</th></tr>
<tr><td>DNS sécurisé</td><td colspan="2">Secure Web Appliance peut désormais valider la réponse DNS reçue du serveur DNS à l'aide de signatures cryptographiques.

Consultez la section « Editing DNS Settings » (Modification des paramètres DNS) du guide d'utilisation.</td></tr>
<tr><td>Nombre maximal de connexions par client</td><td colspan="2">Secure Web Appliance limite le nombre de connexions simultanées initiées par le client à une valeur configurée.

Consultez la section « Configuring Web Proxy Settings » (Configuration des paramètres du proxy Web) du guide d'utilisation.</td></tr>
<tr><td rowspan="3">Changement de marque de Cisco Web Security Appliance pour Cisco Secure Web Appliance</td><td colspan="2">À partir de la version 14.5 d'AsyncOS, Cisco Web Security Appliance a été renommé Cisco Secure Web Appliance dans l'interface Web et dans toute la documentation destinée à l'utilisateur.</td></tr>
<tr><td>Ancienne terminologie</td><td>Nouvelle terminologie</td></tr>
<tr><td>Dispositif de sécurité Web</td><td>Secure Web Appliance</td></tr>
<tr><td rowspan="6">Changement de marque du produit</td><td>Ancienne terminologie</td><td>Nouvelle terminologie</td></tr>
<tr><td>AMP pour les points terminaux</td><td>Cisco Secure Endpoint</td></tr>
<tr><td>Protection améliorée contre les programmes malveillants</td><td>Cisco Secure Endpoint</td></tr>
<tr><td>AMP</td><td>Cisco Secure Endpoint</td></tr>
<tr><td>Thread Grid</td><td>Analyse des programmes malveillants</td></tr>
<tr><td colspan="2">Remarque Les occurrences des termes renommés présents dans ce document ne correspondent pas à l'interface Web. Dans l'interface Web, les appellations « AMP pour les points terminaux », « Protection améliorée contre les programmes malveillants » et « AMP » sont appelés « Analyse des programmes malveillants ». L'interface Web sera mise à jour dans la prochaine version.</td></tr>
<tr><td>Demandes de classification erronée</td><td colspan="2">La demande de classification erronée est envoyée par HTTPS et, par conséquent, vous ne recevez pas de notifications d'alertes de sécurité.

Consultez la section « Configuring On-Box End-User Notification Pages » (Configuration des pages de notification à l'utilisateur final sur le boîtier) du guide d'utilisation.</td></tr>
<tr><td>Nouvelles balises de décision accesslog</td><td colspan="2">EUN (Notification à l'utilisateur final) s'ajoute à la balise de décision accesslog du groupe de politiques de déchiffrement lorsque la page EUN s'affiche sur le navigateur Web du client.

Consultez la section « ACL Decision Tags » (Balises de décision ACL) du guide d'utilisation.</td></tr>
</table>

Fonctionnalités	Description
Politique de clonage	La fonction « politique de clonage » vous permet de copier ou de cloner les configurations existantes d'une politique et de créer une nouvelle politique. Consultez la section « Policy Configuration » (Configuration des politiques) du guide d'utilisation.
Contrôle accru de la bande passante	Vous pouvez gérer la bande passante du trafic en configurant la valeur de la bande passante dans le profil de quota et en mappant le profil de quota dans la catégorie d'URL de la politique d'accès ou le quota global d'activités Web. Consultez la section « Defining Time, Volume, and Bandwidth Quotas » (Définir les quotas de temps, de volume et de bande passante) du guide d'utilisation.
API REST pour la configuration des politiques de gestion, des politiques de déchiffrement, des politiques de routage, des politiques d'usurpation d'adresse IP, des anti-programmes malveillants et de la réputation, des domaines d'authentification, de la licence logicielle Smart de Cisco, de Cisco Umbrella Seamless ID, des services d'identité et de la configuration du système	Vous pouvez désormais récupérer des informations de configuration et apporter des modifications (par exemple, modifier des informations existantes, ajouter de nouvelles informations ou supprimer une entrée) aux données de configuration de l'appliance à l'aide de REST API. Consultez la section « AsyncOS API 14.5 for Cisco Secure Web Appliance - Getting Started Guide » (API AsyncOS 14.5 pour Cisco Secure Web Appliance – Guide de démarrage).
Intégration d'ISE-SXP	Vous pouvez intégrer le déploiement d'ISE-SXP à Cisco Secure Web Appliance pour une authentification passive. Cela vous permet d'obtenir tous les mappages définis, y compris les mappages SGT-IP qui sont publiés par SXP. Consultez la section « Configure ISE-SXP Integration » (Configuration de l'intégration ISE-SXP) du guide d'utilisation.

Fonctionnalités	Description
Cisco Umbrella Seamless ID	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. Le Cisco Umbrella SWG vérifie les informations de l'utilisateur dans Active Directory en fonction des informations d'identification authentifiées et reçues de Secure Web Appliance. Le Cisco Umbrella SWG considère l'utilisateur comme authentifié et lui fournit un accès en fonction des politiques de sécurité définies. Secure Web Appliance transmet les informations d'identification de l'utilisateur à Cisco Umbrella SWG à l'aide des en-têtes HTTP : X-USWG-PKH, X-USWG-SK et X-USWG-Data. **Remarque** Les en-têtes de Cisco Umbrella Seamless ID remplacent les en-têtes du même nom sur Secure Web Appliance, le cas échéant. La fonctionnalité Cisco Umbrella Seamless ID prend en charge le schéma d'authentification avec Active Directory uniquement. Cette fonctionnalité ne prend pas en charge LDAP, Cisco Identity Services Engine (ISE) et Cisco Context Directory Agent (CDA). Cisco Umbrella SWG ne prend pas en charge le trafic FTP et SOCKS. Consultez la section « Cisco Umbrella Seamless ID » du guide d'utilisation.
Améliorations	
Mise à niveau Samba	La version Samba a été mise à niveau vers la version 4.11.15. Vous pouvez activer ou désactiver la prise en charge du protocole SMB1 pour la version Samba 4.11.15 à l'aide de la commande *smbprotoconfig*. Par défaut, cette prise en charge est désactivée et peut être activée en fonction de la configuration du domaine d'authentification. Consultez la section « Secure Web Appliance CLI Commands » (Commandes de la CLI de Secure Web Appliance) du guide d'utilisation.

Remarque (Pour TAC seulement)

En raison du rétablissement mineur de la CLI, les ports de proxy HTTPS sont désactivés sur les appliances virtuelles pour la sécurité du Web. Activez HTTPS sur l'interface à l'aide de la commande *interfaceconfig*.

Changements de comportement

Changements de comportement dans AsyncOS 14.5.0-537 GD (déploiement général)

Politique de clonage	Les politiques suivantes avec l'option de clonage dans Secure Web Appliance peuvent également être gérées par Cisco Secure Email and Web Manager (SMA). • Accès • Profil d'identification • Déchiffrement • Routage

Changements de comportement dans AsyncOS 14.5.0-498 LD (déploiement limité)

Configuration SSL	TLSv1.2 est activé par défaut pour l'interface utilisateur Web de gestion de l'appliance sous **System Administrator** > **(Administrateur système) SSL Configuration** (Configuration SSL) afin de prendre en charge le navigateur Chrome, version 98.0.4758.80 ou ultérieure.
Reprise de session	Après une mise à niveau, la reprise de session est désactivée par défaut.
Context Directory Agent (CDA)	Context Directory Agent (CDA) n'est plus pris en charge. Il est recommandé de configurer ISE/ISE-PIC pour une identification transparente de l'utilisateur afin d'obtenir la même fonctionnalité. Les options de configuration du CDA ne seront plus disponibles dans les versions ultérieures. Pour en savoir plus, consultez la End-of-Sale and End-of-Life Announcement for the Cisco Context Directory Agent (l'annonce de fin de vente et de fin de vie du Context Directory Agent [CDA] de Cisco).
Sélection de l'interface pour l'enregistrement de la licence Smart	Vous pouvez maintenant choisir entre l'interface de données ou l'interface de gestion dans la liste déroulante **Test Interface** (Interface de test). **Remarque** Assurez-vous que l'interface de données et l'interface de gestion sont configurées. Après une mise à niveau, lorsque le routage fractionné est activé, la **Test Interface** (Interface de test) pour la licence Smart dans l'interface Web affiche **Data Interface** (interface de données). Si le routage fractionné est désactivé, la **Management Interface** (Interface de gestion) s'affiche.
Proxy HTTPS – gestion des certificats non valides	Sur une nouvelle installation d'AsyncOS 14.5, la valeur des configurations de certificats de **nom d'hôte** expiré **et non concordant** sur la page du proxy HTTPS sera sélectionnée par défaut comme **Drop** (Abandonner) au lieu de **Monitor** (Surveiller). **Remarque** Ceci s'applique uniquement à une nouvelle installation et non à une mise à niveau. La mise à niveau de l'appliance conservera la même configuration de la version précédente.

Réglage du réseau	Après une mise à niveau vers Cisco AsyncOS 14.5, vous recevrez une invite pour redémarrer le processus de proxy lorsque vous exécuterez la commande *networktuning* pour la première fois. **Remarque** Pour les versions d'AsyncOS antérieures à 14.5, cette invite de redémarrage du processus de proxy n'est pas disponible. Si la commande a été exécutée dans l'une des versions précédentes avant une mise à niveau, l'invite ne sera pas déclenchée.

Accès à la nouvelle interface Web

La nouvelle interface Web offre une nouvelle présentation pour les rapports de surveillance et les services Web de suivi. Vous pouvez accéder à la nouvelle interface Web de la manière suivante :

- Connectez-vous à l'ancienne interface Web et cliquez sur le lien **Secure Web Appliance is getting a new look. Try it!!** (Secure Web Appliance fait peau neuve. Faites-en l'essai!!). Lorsque vous cliquez sur ce lien, un nouvel onglet s'ouvre dans votre navigateur Web et vous dirige à `https://wsa01-enterprise.com:<trailblazer-https-port>/ng-login`, où `wsa01-enterprise.com` est le nom d'hôte de l'appliance et `<trailblazer-https-port>` est le port HTTPS novateur configuré sur l'appliance pour accéder à la nouvelle interface Web.

Important!

- Vous devez vous connecter à l'ancienne interface Web de l'appliance.
- Assurez-vous que votre serveur DNS peut résoudre le nom d'hôte de l'appliance que vous avez spécifié.
- Par défaut, la nouvelle interface Web a besoin des ports TCP 6080, 6443 et 4431 pour être opérationnelle. Assurez-vous que ces ports ne sont pas bloqués par le pare-feu de l'entreprise.
- Le port par défaut pour accéder à la nouvelle interface Web est 4431. Cet élément peut être personnalisé à l'aide de la commande CLI **trailblazerconfig**. Pour en savoir plus sur la commande **trailblazerconfig** de la CLI, consultez le chapitre « Command Line Interface » (interface de commande en ligne) du guide d'utilisation.
- La nouvelle interface Web a également besoin de ports d'API AsyncOS (surveillance) pour HTTP et HTTPS. Par défaut, ces ports sont 6080 et 6443. Les ports de l'API AsyncOS (surveillance) peuvent également être personnalisés à l'aide de la commande de la CLI **interfaceconfig**. Pour plus d'informations sur la commande de la CLI **interfaceconfig**, consultez le chapitre « Command Line Interface » (Interface de commande en ligne) du guide d'utilisation.

Si vous modifiez ces ports par défaut, vérifiez que les ports personnalisés pour la nouvelle interface Web ne sont pas bloqués dans le pare-feu de l'entreprise.

La nouvelle interface Web s'ouvre dans une nouvelle fenêtre de navigateur et vous devez vous reconnecter pour y accéder. Si vous souhaitez vous déconnecter complètement de l'appliance, vous devez vous déconnecter de la nouvelle et de l'ancienne interface Web de votre appliance.

Pour une navigation et un affichage sans problème des pages HTML, Cisco recommande d'utiliser les navigateurs suivants pour accéder à la nouvelle interface Web de l'appliance (AsyncOS 11.8 et les versions ultérieures) :

- Google Chrome
- Mozilla Firefox

Vous pouvez accéder à l'ancienne interface Web de l'appliance sur n'importe lequel des navigateurs pris en charge.

La résolution prise en charge pour la nouvelle interface Web de l'appliance (AsyncOS 11.8 et les versions ultérieures) est comprise entre 1280 x 800 et 1680 x 1050. La meilleure résolution d'affichage est de 1440 x 900, pour tous les navigateurs.

Remarque Cisco ne recommande pas d'afficher la nouvelle interface Web de l'appliance sur des résolutions plus élevées.

Classification des versions

Chaque version est identifiée par le type de version (ED – Déploiement précoce, GD – Déploiement général, etc.). Pour une explication de ces termes, consultez la section http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf.

Matériel pris en charge pour cette version

La version de base peut être mise à niveau sur toutes les plateformes existantes prises en charge, tandis que la prise en charge des performances améliorées est disponible uniquement pour les modèles de matériel suivants :

- Sx90/F
- Sx95/F

Remarque AsyncOS version 14.5 sera la dernière version prise en charge sur les modèles Sx90/F.

Modèles virtuels :

- S100v
- S300v

  Les configurations requises du CPU et de la mémoire du système ont été modifiées à partir de la version 12.5. Pour en savoir plus, consultez le Cisco Content Security Virtual Appliance Installation Guide (Guide d'installation de l'appliance virtuelle Cisco pour la sécurité du contenu).
- S600v
- S1000v

Remarque Utilisez les SFP de Cisco livrés avec l'appliance.

Chemins de mise à niveau

Mise à niveau vers AsyncOS 14.5.2-011

Remarque Avant de procéder à la mise à niveau vers cette version, enregistrez une copie du fichier de configuration de l'appliance dans un emplacement autre que l'appliance.

Vous pouvez effectuer la mise à niveau vers la version 14.5.2-011 d'AsyncOS pour Cisco Secure Web Appliance à partir des versions suivantes :

- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-511
- 11.8.1-604
- 11.8.1-702
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.3-503
- 12.0.4-002
- 12.0.5-011
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-011
- 12.5.3-002
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-005
- 12.5.5-008
- 12.5.5-501
- 12.5.6-008
- 12.7.0-033
- 14.0.0-467
- 14.0.1-014
- 14.0.1-040
- 14.0.1-053
- 14.0.2-012
- 14.0.3-007
- 14.0.3-014
- 14.0.4-005
- 14.1.0-032
- 14.1.0-041
- 14.1.0-047
- 14.5.0-388
- 14.5.0-455
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-008
- 14.5.1-016

Mise à niveau vers AsyncOS 14.5.1-016

Remarque Lors de la mise à niveau, ne connectez aucun périphérique (clavier, souris, périphériques de gestion (Raritan), etc.) aux ports USB de l'appliance.

Vous pouvez effectuer la mise à niveau vers la version 14.5.1-016 d'AsyncOS pour Cisco Secure Web Appliance depuis les versions suivantes :

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14.0.1-014
11.8.1-028	12.0.2-012	14.0.1-040

11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014
11.8.3-021	12.5.1-011	14.0.4-005
11.8.3-501	12.5.1-035	14.1.0-032
11.8.4-004	12.5.1-043	14.1.0-041
	12.5.2-011	14.1.0-047
	12.5.3-002	14.5.0-388
	12.5.3-006	14.5.0-455
	12.5.4-005	14.5.0-498
	12.5.4-011	14.5.0-537
	12.5.5-004	14.5.0-673
	12.5.5-005	14.5.1-008
	12.5.5-008	
	12.7.0-033	

Mise à niveau vers AsyncOS 14.5.1-008

Remarque Lors de la mise à niveau, ne connectez aucun périphérique (clavier, souris, périphériques de gestion (Raritan), etc.) aux ports USB de l'appliance.

Vous pouvez effectuer la mise à niveau vers la version 14.5.1-008 d'AsyncOS pour Cisco Secure Web Appliance depuis les versions suivantes :

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14.0.1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014

11.8.3-021	12.5.1-011	14.1.0-032
11.8.3-501	12.5.1-035	14.1.0-041
11.8.4-004	12.5.1-043	14.1.0-047
	12.5.2-011	14.5.0-388
	12.5.3-002	14.5.0-455
	12.5.3-006	14.5.0-498
	12.5.4-005	14.5.0-537
	12.5.4-011	14.5.0-673
	12.5.5-004	
	12.5.5-005	
	12.5.5-008	
	12.7.0-033	

Mise à niveau vers AsyncOS 14.5.0-537

Remarque Lors de la mise à niveau, ne connectez aucun périphérique (clavier, souris, périphériques de gestion (Raritan), etc.) aux ports USB de l'appliance.

Vous pouvez effectuer la mise à niveau vers la version 14.5.0-537 d'AsyncOS pour Cisco Secure Web Appliance depuis les versions suivantes :

11.8.0-453	12.0.1-268	14.0.0-467
11.8.1-023	12.0.1-334	14.0.1-014
11.8.1-028	12.0.2-004	14.0.1-040
11.8.1-511	12.0.2-012	14.0.1-053
11.8.1-604	12.0.3-005	14.0.1-503
11.8.1-702	12.0.3-007	14.0.2-012
11.8.2-009	12.0.4-002	14.1.0-032
11.8.2-702	12.5.1-011	14.1.0-041
11.8.3-021	12.5.1-035	14.1.0-047
11.8.3-501	12.5.1-043	14.5.0-388
11.8.4-004	12.5.2-007	14.5.0-455
	12.5.2-011	14.5.0-498

12.5.3-002

12.5.4-005

12.5.4-011

12.7.0-033

Mise à niveau vers AsyncOS 14.5.0-498

Remarque Lors de la mise à niveau, ne connectez aucun périphérique (clavier, souris, périphériques de gestion (Raritan), etc.) aux ports USB de l'appliance.

Vous pouvez effectuer la mise à niveau vers la version 14.5.0-498 d'AsyncOS pour Cisco Secure Web Appliance depuis les versions suivantes :

11.8.0-453	12.0.1-268	14.0.0-467
11.8.1-023	12.0.1-334	14.0.1-014
11.8.1-028	12.0.2-004	14.0.1-040
11.8.1-511	12.0.2-012	14.0.1-053
11.8.1-604	12.0.3-005	14.0.2-012
11.8.1-702	12.0.3-007	14.1.0-032
11.8.2-009	12.0.4-002	14.1.0-041
11.8.2-702	12.5.1-011	14.1.0-047
11.8.3-021	12.5.1-035	14.5.0-388
11.8.3-501	12.5.1-043	14.5.0-455
11.8.4-004	12.5.2-007	
	12.5.2-011	
	12.5.3-002	
	12.7.0-033	

Configuration requise après la mise à niveau

Après avoir effectué la mise à niveau vers la version 14.5.1-016, vous devez effectuer les étapes suivantes si vous n'avez pas enregistré votre appliance auprès de Cisco Threat Response :

Procédure

Étape 1 Créez un compte d'utilisateur dans le portail Cisco Threat Response avec des droits d'accès d'administrateur.

Pour créer un nouveau compte d'utilisateur, accédez à la page de connexion du portail Cisco Threat Response à l'aide de l'URL suivante : https://visibility.amp.cisco.com et cliquez sur « Create a Cisco Security Account » (Créer un compte de sécurité Cisco). Si vous ne parvenez pas à créer un nouveau compte d'utilisateur, communiquez avec Cisco TAC pour obtenir de l'aide.

Étape 2 Pour enregistrer votre appliance auprès du portail en nuage Security Services Exchange (SSE), générez un jeton à partir du portail SSE qui correspond à votre région.

Lors de l'enregistrement sur le portail en nuage SSE, sélectionnez le nom de domaine complet (FQDN) suivant en fonction de votre région dans l'interface utilisateur Web de votre appliance :

- AMÉRIQUES (*api-sse.cisco.com*)
- EUROPE (*api.eu.sse.itd.cisco.com*)
- ASIE-PACIFIQUE, JAPON ET CHINE (*api.apj.sse.itd.cisco.com*)

Étape 3 Assurez-vous d'activer Cisco Threat Response sous Cloud Services (Services en nuage) sur le portail Security Services Exchange. Assurez-vous d'ouvrir le port HTTPS (entrée et sortie) 443 sur le pare-feu pour le FQDN *api-sse.cisco.com* (Amérique) afin d'enregistrer votre appliance auprès du portail Security Services Exchange.

Pour déployer une appliance virtuelle, consultez le *Cisco Content Security Virtual Appliance Installation Guide* (Guide d'installation de l'appliance virtuelle Cisco pour la sécurité du contenu), disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Détails sur la compatibilité

Compatibilité avec Cisco AsyncOS pour la gestion de la sécurité

Pour la compatibilité entre cette version et les versions d'AsyncOS pour la gestion de la sécurité du contenu de Cisco, consultez la matrice de compatibilité à l'adresse : https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html.

IPv6 et Kerberos non disponibles en mode Cloud Connector

Lorsque l'appliance est configurée en mode Cloud Connector, des options non disponibles pour les adresses IPv6 et l'authentification Kerberos s'affichent sur les pages de l'interface Web. Bien que les options semblent disponibles, elles ne sont pas prises en charge dans le mode Cloud Connector. Ne tentez pas de configurer l'appliance pour utiliser les adresses IPv6 ou l'authentification Kerberos en mode Cloud Connector.

Prise en charge fonctionnelle des adresses IPv6

Caractéristiques et fonctionnalités qui prennent en charge les adresses IPv6 :

- Interfaces de ligne de commande et interfaces Web. Vous pouvez accéder à l'appliance via http://[2001:2:2::8]:8080 ou https://[2001:2:2::8]:8443
- Exécution d'actions de proxy sur le trafic de données IPv6 (HTTP/HTTPS/SOCKS/FTP)
- Serveurs DNS IPv6
- Redirection transparente avec le WCCP 2.01 (commutateur Cat6K) et la couche 4
- Proxys en amont
- Services d'authentification
  - Active Directory (NTLMSSP, Basic et Kerberos)
  - LDAP
  - SSO pour le logiciel-service
  - Identification transparente de l'utilisateur par le biais de CDA (la communication avec CDA se fait par IPv4 seulement)
  - Chiffrement des informations d'authentification
- Rapports Web et suivi Web
- Serveurs DLP externes (la communication entre l'appliance et le serveur DLP se fait par IPv4 seulement)
- Hébergement de fichiers PAC
- Protocoles : NTP, RADIUS, SNMP et syslog sur le serveur de gestion

Caractéristiques et fonctionnalités qui nécessitent des adresses IPv4 :

- Relais SMTP interne
- Authentification extérieure
- Méthode push pour les abonnements aux journaux : FTP, SCP et syslog
- Serveurs NTP
- Serveurs de mise à jour locaux, y compris les serveurs proxys pour les mises à jour
- Services d'authentification
- AnyConnect Security Mobility
- Serveurs d'authentification Novell eDirectory
- Logo personnalisé pour les pages de notification à l'utilisateur final
- Communication entre Secure Web Appliance et l'appliance de gestion de la sécurité
- Versions de WCCP antérieures à 2.01
- SNMP

Disponibilité de l'authentification Kerberos pour les systèmes d'exploitation et les navigateurs

Vous pouvez utiliser l'authentification Kerberos avec les systèmes d'exploitation et les navigateurs suivants :

- Windows Server 2003, 2008, 2008R2 et 2012.
- Dernières versions des navigateurs Safari et Firefox sur Mac (version OSX 10.5 et ultérieure)
- IE (version 7 ou ultérieure) et dernières versions des navigateurs Firefox et Chrome sur Windows 7 ou version ultérieure.

L'authentification Kerberos n'est pas disponible avec les systèmes d'exploitation et les navigateurs suivants :

- Systèmes d'exploitation Windows non mentionnés ci-dessus
- Navigateurs non mentionnés ci-dessus
- iOS et Android

Déploiement d'une appliance virtuelle

Pour déployer une appliance virtuelle, consultez le *Cisco Content Security Virtual Appliance Installation Guide* (Guide d'utilisation de l'appliance virtuelle Cisco pour la sécurité du contenu, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Migration d'une appliance matérielle vers une appliance virtuelle

Procédure

Étape 1 Configurez votre appliance virtuelle avec cette version d'AsyncOS en utilisant la documentation décrite dans la section Configuration requise après la mise à niveau, à la page 12.

Remarque Assurez-vous que les mises à jour des services de sécurité sont installées avec succès.

Étape 2 Mettez à niveau votre appliance matérielle vers cette version d'AsyncOS.

Étape 3 Enregistrez le fichier de configuration de votre appliance matérielle mise à niveau.

Étape 4 Chargez le fichier de configuration de l'appliance matérielle sur l'appliance virtuelle.

Si vos appliances matérielle et virtuelle ont des adresses IP différentes, désélectionnez Load Network Settings (Charger les paramètres réseau) avant de charger le fichier de configuration.

Étape 5 Validez vos modifications.

Étape 6 Accédez à **Authentification** > **Network**(Réseau) et joignez à nouveau le domaine. Sinon, les identités ne fonctionneront pas.

Mise à niveau d'AsyncOS pour le Web

Avant de commencer

- Conformez-vous aux exigences préalables à la mise à niveau, y compris la mise à jour du micrologiciel du contrôleur RAID.

- Connectez-vous en tant qu'administrateur.

Procédure

Étape 1 Sur la page **System Administration (Administration du système)** > **Configuration File**(Fichier de configuration), enregistrez le fichier de configuration XML depuis Secure Web Appliance.

Étape 2 Sur la page**System Administration (Administration du système)** > **System Upgrade (Mise à niveau du système)**, cliquez sur **Upgrade Options** (Options de mise à niveau).

Étape 3 Vous pouvez sélectionner **Download and install** (Télécharger et installer) ou **Download only** (Télécharger seulement).

Faites votre choix parmi la liste des mises à niveau disponibles.

Étape 4 Cliquez sur **Proceed** (Procéder).

Si vous avez choisi **Download only** (Télécharger seulement), la mise à niveau sera téléchargée sur l'appliance.

Étape 5 Si vous avez choisi **Download and install** (Télécharger et installer), une fois la mise à niveau terminée, cliquez sur **Reboot Now** (Redémarrer maintenant) pour redémarrer Secure Web Appliance.

Remarque Pour vérifier que le navigateur charge le nouveau contenu de l'aide en ligne dans la version mise à niveau d'AsyncOS, vous devez quitter le navigateur, puis l'ouvrir à nouveau avant de consulter l'aide en ligne. Cette opération permet d'effacer le cache du navigateur de tout contenu obsolète.

Important! Actions requises après la mise à niveau

Afin de vous assurer que votre appliance continue de fonctionner correctement après la mise à niveau, vous devez tenir compte des éléments suivants :

- Remplacement des suites cryptographiques par défaut des services de proxy par les suites cryptographiques recommandées par Cisco
- Appliances virtuelles : modifications requises pour la correction de la faille de sécurité SSH
- Analyse de fichier : modifications requises pour afficher les détails des résultats d'analyse dans le nuage
- Analyse de fichier : vérifier les types de fichiers à analyser
- Points non échappés dans les expressions régulières

Remplacement des suites cryptographiques par défaut des services de proxy par les suites cryptographiques recommandées par Cisco

À partir d'AsyncOS 9.1.1 et les versions ultérieures, les suites de chiffrement par défaut disponibles pour les services de proxy sont modifiées afin d'inclure uniquement les suites de chiffrement sécurisées.

Cependant, si vous effectuez une mise à niveau depuis AsyncOS 9.xx et des versions ultérieures, les suites de chiffrement par défaut des services de proxy ne sont pas modifiées. Pour une sécurité accrue, Cisco vous recommande de remplacer les suites de chiffrement par défaut des services de proxy par les suites de chiffrement recommandées par Cisco après la mise à niveau. Procédez comme suit :

Procédure

Étape 1 Connectez-vous à votre appliance en utilisant l'interface Web.

Étape 2 Cliquez sur**System Administration (Administration du système)** > **SSL Configuration**(Configuration SSL).

Étape 3 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 4 Sous **Proxy Services** (Services de proxy), définissez le champ **Cipher(s) to Use** (Chiffrements à utiliser) comme suit :

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DHE-
DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:TLS_AES_256_GCM_SHA384
```

Mise en garde Assurez-vous de coller la chaîne ci-dessus en tant que chaîne unique sans retour de chariot ni espace.

Étape 5 Soumettez et validez les modifications.

Vous pouvez également utiliser la commande **sslconfig** dans l'interface de commande en ligne (CLI) pour effectuer les étapes ci-dessus.

Appliances virtuelles : modifications requises pour la correction de la faille de sécurité SSH

Les configuration requises de cette section ont été introduites dans AsyncOS 8.8.

La faille de sécurité suivante sera corrigée lors de la mise à niveau si elle existe sur votre appliance :

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport.

Remarque Ce correctif est requis uniquement pour les versions d'appliances virtuelles qui ont été téléchargées ou mises à niveau avant le 25 juin 2015.

Si vous n'avez pas corrigé ce problème avant la mise à niveau, un message s'affichera pendant la mise à niveau pour indiquer que le problème a été résolu. Si ce message s'affiche, les actions suivantes sont nécessaires pour rétablir le bon fonctionnement de votre appliance après la mise à niveau :

- Supprimez l'entrée existante pour votre appliance de la liste des hôtes connus dans votre utilitaire ssh. Une fois la nouvelle clé créée, connectez-vous à l'appliance par SSH et acceptez la connexion.
- Effacez l'ancienne clé d'hôte SSH de l'appliance sur le serveur distant si vous utilisez la transmission SCP pour transférer les journaux vers un serveur distant (y compris Splunk).
- Si votre déploiement comprend une appliance de gestion Cisco pour la sécurité du contenu, consultez les instructions importantes dans les notes de version de cette appliance.

Analyse de fichier : modifications requises pour afficher les détails des résultats d'analyse dans le nuage

Si vous avez déployé plusieurs appliances pour la sécurité du contenu (Web, de messagerie et/ou de gestion) et que vous souhaitez afficher les résultats détaillés de l'analyse de fichiers dans le nuage pour tous les fichiers téléversés depuis toutes les appliances de votre organisation, vous devez configurer un groupe d'appliances

sur chacune des appliances après la mise à niveau. Pour configurer des groupes d'appliances, consultez la section File Reputation Filtering and File Analysis (Filtrage de la réputation des fichiers et analyse des fichiers).

Analyse de fichier : vérifier les types de fichiers à analyser

L'URL du serveur en nuage d'analyse des fichiers a été modifiée dans AsyncOS 8.8 et, par conséquent, les types de fichiers qui peuvent être analysés pourraient avoir changé après la mise à niveau. Vous devriez recevoir une alerte en cas de changements. Pour vérifier les types de fichiers sélectionnés pour l'analyse, sélectionnez **Security Services (Services de sécurité)** > **Anti-Malware and Reputation**(Anti-programme malveillant et réputation) et examinez les paramètres de la protection avancée contre les programmes malveillants.

Points non échappés dans les expressions régulières

À la suite des mises à niveau du moteur d'expressions régulières, vous pouvez recevoir une alerte concernant des points non échappés dans les définitions de schéma existantes après la mise à jour de votre système. Tout point non échappé dans un schéma qui renverra plus de 63 caractères après le point sera désactivé par le moteur de correspondance de schémas Velocity, et une alerte à cet effet vous sera envoyée. Vous continuerez de recevoir une alerte après chaque mise à jour jusqu'à ce que vous corrigiez ou remplaciez le schéma. En général, les points non échappés dans une expression régulière plus grande peuvent être problématiques et doivent être évités.

Mises à jour de la documentation

Le guide d'utilisation disponible sur le site Web (www.cisco.com) pourrait être plus à jour que l'aide en ligne. Pour obtenir le guide d'utilisation et d'autres documents sur ce produit, cliquez sur le bouton **View PDF** (Afficher le PDF) dans l'aide en ligne ou visitez l'URL indiquée à la section Documentation associée, à la page 20.

Problèmes connus et résolus

- Configurations requises de l'outil de recherche de bogues
- Listes des problèmes connus et résolus
- Recherche d'informations sur les problèmes connus et résolus

Configurations requises de l'outil de recherche de bogues

Créez un compte Cisco si vous n'en avez pas déjà un. Allez sur https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Listes des problèmes connus et résolus

Problèmes connus et résolus dans la version 14.5.2-011

Connectez-vous à l'outil de recherche de bogues de Cisco en utilisant les informations d'authentification de votre compte Cisco pour afficher la liste des bogues corrigés.

- Problèmes résolus
- Problèmes connus

Problèmes connus et résolus dans la version 14.5.1-016

- Problèmes résolus
- Problèmes connus

Problèmes connus et résolus dans la version 14.5.1-008

- Problèmes résolus
- Problèmes connus

Problèmes connus et résolus dans la version 14.5.0-537

- Problèmes résolus
- Problèmes connus

Problèmes connus et résolus dans la version 14.5.0-498

- Problèmes résolus
- Problèmes connus

Recherche d'informations sur les problèmes connus et résolus

Utilisez l'outil de recherche de bogues de Cisco pour trouver les informations à jour sur les problèmes connus et résolus.

Avant de commencer

Créez un compte Cisco si vous n'en avez pas déjà un. Allez sur https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Procédure

Étape 1 Allez sur https://tools.cisco.com/bugsearch/.

Étape 2 Connectez-vous avec les informations d'authentification de votre compte Cisco.

Étape 3 Cliquez sur **Select from list (Sélectionner à partir de la liste)** > **Security (Sécurité)** > **Web Security (Sécurité Web)** > **Cisco Secure Web Appliance**, puis cliquez sur **OK**.

Étape 4 Dans le champ **Releases** (versions), entrez la version, par exemple, x.x.x.

Étape 5 Selon vos besoins, effectuez l'une des opérations suivantes :

- Pour afficher la liste des problèmes résolus, sélectionnez **Fixed in these Releases** (Résolus dans ces versions) dans la liste déroulante **Releases** (Versions).
- Pour afficher la liste des problèmes connus, dans le menu déroulant **Releases** (Versions), sélectionnez **Affecting these Releases** (Touchant ces versions), puis dans la liste déroulante **Status** (État), sélectionnez **Open** (Ouvrir).

Remarque Si vous avez des questions ou des problèmes, cliquez sur les liens **Help** (Aide) ou **Feedback** (Commentaire) dans le coin supérieur droit de l'outil. Une visite interactive est également possible; pour l'afficher, cliquez sur le lien situé dans la barre orangée au-dessus des champs de recherche.

Documentation associée

Documentation	Emplacement
Guide d'utilisation de Cisco Secure Web Appliance	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Guide d'utilisation de l'appliance de gestion Cisco pour la sécurité du contenu	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Guide d'installation de l'appliance virtuelle	https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html

Soutien

Communauté de soutien Cisco

La communauté de soutien Cisco est un forum en ligne destiné aux clients, aux partenaires et aux employés de Cisco. Il fournit un endroit pour discuter des questions générales de sécurité Web ainsi que des informations techniques sur des produits Cisco spécifiques. Vous pouvez publier des sujets sur le forum pour poser des questions et partager des informations avec d'autres utilisateurs de Cisco.

Pour accéder à la communauté de soutien Cisco sur la sécurité Web et la gestion associée :

https://supportforums.cisco.com/community/5786/web-security

Service à la clientèle

Remarque Pour obtenir de l'aide sur les appliances virtuelles, communiquez avec Cisco TAC. Ayez votre numéro de licence virtuelle (VLN) à portée de la main avant de communiquer avec Cisco TAC.

Cisco TAC :

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.

Site d’assistance pour l’ancien IronPort :

http://www.cisco.com/web/services/acquisitions/ironport.html.

Pour les problèmes non critiques, vous pouvez également accéder au service à la clientèle à partir de l’appliance. Pour obtenir des instructions, consultez la section Troubleshooting (Dépannage) du Secure Web Appliance User Guide (Guide d’utilisation de Secure Web Appliance).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Les adresses IP (Internet Protocol) et les numéros de téléphone utilisés dans ce document ne sont pas censés correspondre à des adresses ni à des numéros de téléphone réels. Tous les exemples, résultats d'affichage de commandes, schémas de topologie de réseau et autres illustrations inclus dans ce document sont donnés à titre indicatif uniquement. L'utilisation d'adresses IP ou de numéros de téléphone réels à titre d'exemple est non intentionnelle et fortuite.

© 2023 Cisco Systems, Inc. Tous droits réservés.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.