Connecter l'appliance à un proxy Cisco Cloud Web Security

Cette rubrique contient les sections suivantes :

Comment configurer et utiliser les fonctionnalités en mode Cloud Connector

L'utilisation des fonctionnalités incluses dans le sous-ensemble Cloud Connector est la même qu'en mode standard, sauf indication contraire. Voir Comparaison des modes de fonctionnement pour de plus amples informations.

Cette rubrique contient des liens vers des emplacements de cette documentation qui fournissent des informations sur quelques-unes des principales fonctionnalités de Secure Web Appliance communes au mode standard et au mode Cloud Web Security Connector. À l'exception des paramètres de configuration de Cloud Connector et des informations sur l'envoi de groupes d'annuaires dans le nuage, les informations pertinentes se trouvent dans d'autres sections du document.

Cette rubrique contient des informations sur la configuration de Cloud Web Security Connector qui ne s'appliquent pas au mode standard.

Ce document ne contient pas d'informations sur le produit Cisco Cloud Web Security. La documentation relative à Cloud Connector est disponible à l'adresse suivante : http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

Déploiement en mode Cloud Connector

Lors de la configuration initiale de l'appliance, vous pouvez choisir de la déployer en mode Cloud Connector ou en mode standard. Vous pouvez également exécuter l'Assistant de configuration du système sur une appliance qui est actuellement déployée en mode standard pour la redéployer en mode Cloud Connector, si vous disposez des licences requises. L'exécution de l'Assistant de configuration du système remplace vos configurations existantes et supprime toutes les données existantes.

Le déploiement de l'appliance est identique en mode standard et en mode Cloud Security, sauf que les services de proxy Web et les services de supervision du trafic de la couche 4 ne sont pas disponibles en mode Cloud Web Security Connector.

Vous pouvez déployer Cloud Web Security Connector en mode de transfert explicite ou en mode transparent.

Pour modifier les paramètres de Cloud Connector après la configuration initiale, sélectionnez **Network** > **Cloud Connector** (Réseau > Cloud Connector).

Thèmes connexes

- Connexion, installation et configuration

Configuration de Cloud Connector

Before you begin

Voir Activation de l'accès à l'interface Web sur les appliances virtuelles.

Étape 1 Accédez à l'Interface Web de Secure Web Appliance :

Saisissez l'adresse IPv4 de Secure Web Appliance dans un navigateur Internet.

La première fois que vous exécutez l'Assistant de configuration du système, utilisez l'adresse IPv4 par défaut :

`https://192.168.42.42:8443`

-ou-

`http://192.168.42.42:8080`

`192.168.42.42` étant l'adresse IPv4 par défaut, `8080` le paramètre du port d'administration par défaut pour HTTP et `8443` le port d'administration par défaut pour HTTPS.

Étape 2 Sélectionnez **System Administration > System Setup Wizard** (Administration système >Assistant de configuration du système).

Étape 3 Acceptez les conditions du contrat de licence.

Étape 4 Cliquez sur **Start Setup** (Commencer la configuration).

Étape 5 Configurez les paramètres système :

Paramètres	Description
Default System Hostname (Nom d'hôte du système par défaut)	Nom d'hôte complet de Secure Web Appliance.

Paramètres	Description
DNS Server(s) [Serveur(s) DNS]	Serveurs DNS racine Internet pour les recherches de services de noms de domaine. Voir aussi DNS Settings (paramètres DNS).
NTP Server (Serveur NTP)	Serveur avec lequel synchroniser l'horloge système. La valeur par défaut est time.ironport.com.
Time Zone (Fuseau horaire)	Définit le fuseau horaire sur l'appliance de sorte que les horodatages dans les en-têtes des messages et les fichiers journaux soient corrects.

Étape 6 Sélectionnez **Cloud Web Security Connector** pour le mode de l'appliance.

Étape 7 Configurez les paramètres du Cloud Connector :

Paramètres	Description
Cloud Web Security Proxy Servers (Serveurs proxy Cloud Web Security)	Adresse du serveur proxy dans le nuage (CPS), par exemple, proxy1743.scansafe.net.
Failure Handling (Gestion des échecs)	Si AsyncOS ne parvient pas à se connecter à un proxy Cloud Web Security, sélectionnez **Connect directly** (Se connecter directement) pour vous connecter directement à Internet ou sélectionnez **Drop requests** (Abandonner les demandes).
Cloud Web Security Authorization Scheme (Schéma d'autorisation Cloud Web Security)	Méthode d'autorisation des transactions : • Adresse IPv4 publique de Secure Web Appliance • Clé d'autorisation incluse avec chaque transaction. Vous pouvez générer une clé d'autorisation dans le portail Cisco Cloud Web Security.

Étape 8 Configurez le câblage et les interfaces réseau :

Paramètres	Description
Ethernet Port (Port Ethernet)	Si vous configurez l'interface M1 pour le trafic de gestion uniquement, vous devez configurer l'interface P1 pour le trafic de données. Cependant, vous pouvez configurer l'interface P1 même lorsque l'interface M1 est utilisée à la fois pour la gestion et le trafic de données.
IP Address (Adresse IP)	Adresse IPv4 à utiliser pour gérer Secure Web Appliance.
Network Mask (Masque réseau)	Masque réseau à utiliser lors de la gestion de Secure Web Appliance sur cette interface réseau.
Hostname (Nom d'hôte)	Nom d'hôte à utiliser lors de la gestion de Secure Web Appliance sur cette interface réseau.

Étape 9 Configurez les voies de routage pour le trafic de gestion et de données :

Paramètres	Description
Default Gateway (Passerelle par défaut)	Adresse IPv4 par défaut de la passerelle à utiliser pour le trafic via l'interface de gestion et/ou de données.
Name (Nom)	Nom utilisé pour identifier la voie de routage statique.
Internal Network (Réseau interne)	Adresse IPv4 pour la destination de cette voie de routage sur le réseau.
Internal Gateway (Passerelle interne)	Adresse IPv4 de la passerelle pour cette voie de routage. Une passerelle de routage doit résider sur le même sous-réseau que l'interface de gestion ou de données sur laquelle elle est configurée.

Étape 10 Configurez les paramètres de connexion transparents :

Note Par défaut, le Cloud Connector est déployé en mode transparent, ce qui nécessite une connexion à un commutateur de couche 4 ou à un routeur WCCP version 2.

Paramètres	Description
Layer-4 Switch (Commutateur de couche 4) ou No Device (Aucun périphérique)	• Le Secure Web Appliance est connecté à un commutateur de couche 4. ou • Vous déploierez le Cloud Connector en mode de transfert explicite.
WCCP v2 Router (Routeur WCCP v2)	Le Secure Web Appliance est connecté à un routeur compatible avec WCCP version 2. Remarque : Une phrase secrète peut contenir jusqu'à sept caractères et est facultative.

Étape 11 Configurez les paramètres d'administration :

Paramètres	Description
Administrator Passphrase (Phrase secrète de l'administrateur)	Phrase secrète pour l'accès à Secure Web Appliance. La phrase secrète doit comporter au moins six caractères.
Email system alerts to (Alertes du système par e-mail à)	Adresse de messagerie à laquelle l'appliance envoie des alertes.
Send Email via SMTP Relay Host (Envoyer un e-mail par l'intermédiaire de l'hôte de relais SMTP)	(Facultatif) Nom d'hôte ou adresse d'un hôte de relais SMTP qu'utilise AsyncOS pour envoyer les messages par e-mail générés par le système. L'hôte de relais SMTP par défaut comprend les serveurs de messagerie répertoriés dans l'enregistrement MX. Le numéro de port par défaut est 25.
AutoSupport (AutoAssistance)	L'appliance peut envoyer des alertes système et un rapport d'état hebdomadaire à l'assistance client de Cisco.

Étape 12 Passez en revue et installez :

a) Passez en revue l'installation.
b) Cliquez sur **Previous** (Précédent) pour revenir en arrière et apporter des modifications.
c) Cliquez sur **Install This Configuration** (Installer cette configuration) pour continuer avec les informations que vous avez fournies.

What to do next

Thèmes connexes

- Prévention de la perte de données sécurisées, on page 7
- Interfaces réseau
- Configuration des routages de trafic TCP/IP
- Configuration de la redirection transparente
- Gestion des alertes
- Configuration d'un hôte de relais SMTP

Contrôle de l'accès au Web à l'aide des groupes de répertoires dans le nuage

Vous pouvez utiliser Cisco Cloud Web Security pour contrôler l'accès Web en fonction des groupes de répertoires. Lorsque le trafic vers Cisco Cloud Web Security est acheminé par l'intermédiaire d'un Secure Web Appliance en mode Cloud Connector, Cisco Cloud Web Security doit recevoir les informations de groupe de répertoires avec les transactions de Cloud Connector pour pouvoir appliquer les politiques de nuage basées sur les groupes.

Before you begin

Ajoutez un domaine d'authentification à la configuration Secure Web Appliance.

Étape 1 Accédez à **Network** > **Cloud Connector** (Réseau > Cloud Connector).

Étape 2 Dans la zone **Cloud Policy Directory Groups** (Groupes d'annuaires de politiques de nuage), cliquez sur **Edit Groups** (Modifier les groupes).

Étape 3 Sélectionner les groupes d'utilisateurs et les groupes d'ordinateurs pour lesquels vous avez créé des politiques de nuage dans Cisco Cloud Web Security.

Étape 4 Cliquez sur **Add** (Ajouter).

Étape 5 Cliquez sur **Done** (Terminé) et validez vos modifications.

What to do next

Informations connexes

- Domaines d'authentification

Contournement du serveur proxy dans le nuage

Les politiques de routage dans le nuage vous permettent d'acheminer le trafic Web vers les proxys Cisco Cloud Web Security ou directement vers Internet sur la base des caractéristiques suivantes :

- **Identification Profile** (Profil d'identification)
- Proxy Port (Port du serveur proxy)
- Subnet (Sous-réseau)
- URL Category (Catégorie URL)
- User Agent (Agent d'utilisateur)

Le processus de création de politiques de routage du nuage en mode Cloud Connector est identique au processus de création de politiques de routage en mode standard.

Thèmes connexes

- Création d'une politique

Prise en charge partielle de FTP et HTTPS en mode Cloud Connector

Secure Web Appliance en mode Cloud Connector ne prend pas entièrement en charge FTP ou HTTPS.

FTP

FTP n'est pas pris en charge par Cloud Connector. AsyncOS abandonne le trafic FTP natif lorsque l'appliance est configurée pour Cloud Connector.

FTP sur HTTP est pris en charge en mode Cloud Connector.

HTTPS

Cloud Connector ne prend pas en charge le déchiffrement. Il transmet le trafic HTTPS sans déchiffrer.

Comme Cloud Connector ne prend pas en charge le déchiffrement, AsyncOS n'a généralement pas accès aux informations dans les en-têtes clients du trafic HTTPS. Par conséquent, AsyncOS ne peut généralement pas appliquer les politiques de routage qui reposent sur les informations contenues dans les en-têtes chiffrés. C'est toujours le cas pour les transactions HTTPS transparentes. Par exemple, pour les transactions HTTPS transparentes, AsyncOS n'a pas accès au numéro de port dans l'en-tête du client HTTPS et, par conséquent, il ne peut pas correspondre à une politique de routage basée sur le numéro de port. Dans ce cas, AsyncOS utilise la politique de routage par défaut.

Il y a deux exceptions pour les transactions HTTPS explicites. AsyncOS a accès aux informations suivantes pour les transactions HTTPS explicites :

- URL
- Numéro du port de destination

Pour les transactions HTTPS explicites, il est possible de mettre en correspondance une politique de routage basée sur l'URL ou le numéro de port.

Prévention de la perte de données sécurisées

Vous pouvez intégrer Cloud Connector à des serveurs externes de protection contre la perte de données en sélectionnant **Network** > **External DLP Servers** (Réseau > Serveur DLP externes).

Thèmes connexes

- Prévenir la perte de données sensibles

Affichage des noms d'utilisateurs et de groupes et des adresses IP

Pour afficher les noms de groupes, les noms d'utilisateur et les adresses IP configurés, accédez à la page whoami.scansafe.net.

Abonnement aux journaux Cloud Connector

Les journaux Cloud Connector fournissent des informations utiles pour résoudre les problèmes rencontrés par Cloud Connector, par exemple, les utilisateurs et les groupes authentifiés, l'en-tête en nuage et la clé d'autorisation.

Étape 1 Accédez à **System Administration** > **Log Subscriptions** (Administration système > Abonnement aux journaux).
Étape 2 Sélectionnez **Cloud Connector Logs** (Journaux Cloud Connector) dans le menu **Log Type** (Type de journal).
Étape 3 Tapez un nom dans le champ **Log Name** (Nom du journal).
Étape 4 Définissez le niveau de journalisation.
Étape 5 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Superviser l'activité du système au moyen de journaux

Profils d'identification et authentification avec Cloud Web Security Connector

Cloud Web Security Connector prend en charge l'authentification de base et NTLM. Vous pouvez également contourner l'authentification pour certaines destinations.

En mode Cloud Connector, à l'aide d'un domaine Active Directory, vous pouvez identifier les demandes de transaction comme provenant d'ordinateurs spécifiques. Le service d'ID d'ordinateur n'est pas disponible en mode standard.

À deux exceptions près, l'authentification fonctionne de la même manière dans Secure Web Appliance, que ce soit dans la configuration standard ou dans la configuration Cloud Connector. Exceptions :

- Le service d'ID d'ordinateur n'est pas disponible en mode standard.
- AsyncOS ne prend pas en charge Kerberos lorsque l'appliance est configurée en mode Cloud Connector.

Note Les profils d'identification basés sur l'agent utilisateur ou l'URL de destination ne sont pas pris en charge pour le trafic HTTPS.

Thèmes connexes

- Identification des ordinateurs pour l'application des politiques, on page 8
- Accès invité pour les utilisateurs non authentifiés, on page 9
- Classifier les utilisateurs finaux pour l'application des politiques
- Survol de l'acquisition des informations d'authentification de l'utilisateur final

Identification des ordinateurs pour l'application des politiques

En activant le service d'ID d'ordinateur, AsyncOS peut appliquer des politiques basées sur l'ordinateur qui a effectué la demande de transaction plutôt que sur l'utilisateur authentifié, l'adresse IP ou un autre identifiant. AsyncOS utilise NetBIOS pour acquérir l'ID de l'ordinateur.

Note Sachez que le service d'identité de l'ordinateur n'est disponible que par le biais des domaines Active Directory. Si aucun domaine Active Directory n'est configuré, ce service est désactivé.

Étape 1 Sélectionnez **Network > Machine ID Service** (Réseau > Service d'ID d'ordinateur).

Étape 2 Cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Étape 3 Configurez les paramètres d'identification de l'ordinateur :

Paramètres	Description
Enable NetBIOS for Machine Identification (Activer NetBIOS pour l'identification de l'ordinateur)	Sélectionnez cette option pour activer le service d'identification de l'ordinateur.
Realm (Domaine)	Le domaine Active Directory à utiliser pour identifier l'ordinateur qui lance la demande de transaction.
Failure Handling (Gestion des échecs)	Si AsyncOS ne peut pas identifier l'ordinateur, doit-il abandonner la transaction ou continuer la mise en correspondance de politiques?

Étape 4 Envoyez et validez vos modifications.

Accès invité pour les utilisateurs non authentifiés

Si Secure Web Appliance est configuré pour fournir un accès invité aux utilisateurs non authentifiés, en mode Cloud Connector, AsyncOS affecte les utilisateurs invités au groupe __GUEST_GROUP__ et envoie ces informations à Cisco Cloud Web Security. Utilisez des identités pour fournir un accès invité aux utilisateurs non authentifiés. Utilisez les politiques Cisco Cloud Web Security pour contrôler ces utilisateurs invités.

Thèmes connexes

- Octroi d'un accès invité après échec de l'authentification

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.