Créer des politiques de déchiffrement pour contrôler le trafic HTTPS

Cette rubrique contient les sections suivantes :

Survol de la création de politiques de déchiffrement pour contrôler le trafic HTTPS

Les politiques de déchiffrement définissent le traitement du trafic HTTPS au sein du proxy Web :

- Quand déchiffrer le trafic HTTPS.
- Comment gérer les demandes qui utilisent des certificats de sécurité non valides ou révoqués

Vous pouvez créer des politiques de déchiffrement pour gérer le trafic HTTPS des manières suivantes :

- Transmettez le trafic chiffré
- Déchiffrez le trafic et appliquer les politiques d'accès basées sur le contenu définies pour le trafic HTTP. Cela rend également l'analyse des programmes malveillants possible

  .
- Abandonnez la connexion HTTPS
- Supervisez la demande (n'effectuez aucune action finale) pendant que le proxy Web continue d'évaluer la demande par rapport aux politiques qui peuvent mener à une action finale d'abandon, de transmission ou de déchiffrement.

Caution **Manipulez les informations nominatives avec prudence :** si vous choisissez de déchiffrer la session HTTPS d'un utilisateur final, les journaux d'accès et les rapports Secure Web Appliance peuvent contenir des renseignements nominatifs. L'administrateur peut configurer la quantité de texte d'URI stockée dans les journaux à l'aide de la commande de l'interface de ligne de commande `advancedproxyconfig` et de la sous-commande `HTTPS`. Vous pouvez consigner l'URI entier ou une forme partielle de l'URI en supprimant la partie requête. Cependant, même lorsque vous choisissez de supprimer la requête de l'URI, des renseignements nominatifs peuvent toujours être conservés.

Gestion du trafic HTTPS à l'aide de politiques de déchiffrement – Présentation des tâches

Étape	Liste des tâches pour la gestion du trafic HTTPS par le biais de politiques de déchiffrement	Liens vers des rubriques et des procédures connexes
1	Activation du proxy HTTPS	Activation du proxy HTTPS, on page 5
2	Charger ou générer un certificat et une clé	• Chargement d'un certificat racine et d'une clé, on page 11 • Génération d'un certificat et d'une clé pour le proxy HTTPS, on page 12
3	Configuration des options de déchiffrement	Configuration des options de déchiffrement, on page 8
5	(Facultatif) Configurer la gestion des certificats non valides	Configuration du traitement des certificats non valides, on page 13
6	(Facultatif) Activation de la vérification de l'état de révocation en temps réel	Activation de la vérification de l'état de révocation en temps réel, on page 14
7	(Facultatif) Gérer les certificats approuvés et les certificats bloqués	Certificats racine approuvés, on page 15

Gestion du trafic HTTPS à l'aide de politiques de déchiffrement – Bonnes pratiques

Créez moins de groupes de politiques de déchiffrement plus généraux qui s'appliquent à tous les utilisateurs ou des groupes d'utilisateurs moins nombreux et plus importants sur le réseau. Ensuite, si vous devez appliquer un contrôle plus granulaire au trafic HTTPS déchiffré, utilisez des groupes de politiques d'accès plus spécifiques.

Politiques de déchiffrement

L'appliance peut effectuer l'une des actions suivantes sur une demande de connexion HTTPS :

Option	Description
Monitor (Superviser)	La supervision est une action intermédiaire qui indique que le proxy Web doit continuer à évaluer la transaction par rapport aux autres paramètres de contrôle pour déterminer l'action finale à appliquer.
Drop (abandonner)	L'appliance abandonne la connexion et ne transmet pas la demande de connexion au serveur. L'appliance n'informe pas l'utilisateur qu'il a abandonné la connexion.
Pass through (Intercommunication)	L'appliance traverse la connexion entre le client et le serveur sans inspecter le contenu du trafic. Cependant, avec une politique de transmission standard, Secure Web Appliance vérifie la validité du serveur demandé en déclenchant une liaison HTTPS avec le serveur. Cette vérification de validité inclut la validation du certificat du serveur. En cas d'échec de la vérification du serveur, la transaction est bloquée. Vous pouvez ignorer les contrôles de validation pour des sites spécifiques en configurant des politiques qui intègrent des catégories personnalisées incluant ces sites, indiquant ainsi que ces sites sont fiables : ces sites sont transmis sans contrôles de validité. Faites attention lors de la configuration de politiques qui permettent d'ignorer les contrôles de validité.
Decrypt Déchiffrer	L'appliance autorise la connexion, mais inspecte le contenu du trafic. Il déchiffre le trafic et applique des politiques d'accès au trafic déchiffré comme s'il s'agissait d'une connexion HTTP en texte brut. En déchiffrant la connexion et en appliquant des politiques d'accès, vous pouvez analyser le trafic à la recherche de programmes malveillants.

Toutes les actions, à l'exception de la fonction Superviser, sont des « actions finales » que le proxy Web applique à une transaction. Une action finale est une action qui amène le proxy Web à interrompre l'évaluation de la transaction par rapport à d'autres paramètres de contrôle. Par exemple, si une politique de déchiffrement est configurée pour surveiller les certificats de serveur non valides, le proxy Web ne prend pas de décision finale sur la façon de gérer la transaction HTTPS si le serveur contient un certificat non valide. Si une politique de déchiffrement est configurée pour bloquer les serveurs présentant un score de réputation Web faible, toute demande adressée à un serveur possédant un score de réputation faible est abandonnée sans que les actions de la catégorie d'URL soient prises en compte.

Le diagramme suivant montre comment le proxy Web évalue une demande d'un client par rapport aux groupes de la politique de déchiffrement. Contrôle du trafic HTTPS affiche l'ordre utilisé par le proxy Web lors de l'évaluation des paramètres de contrôle pour les politiques de déchiffrement. Application des actions de politique d'accès indique l'ordre utilisé par le proxy Web lors de l'évaluation des paramètres de contrôle pour les politiques d'accès.

Figure 1: Application des actions de la politique de déchiffrement

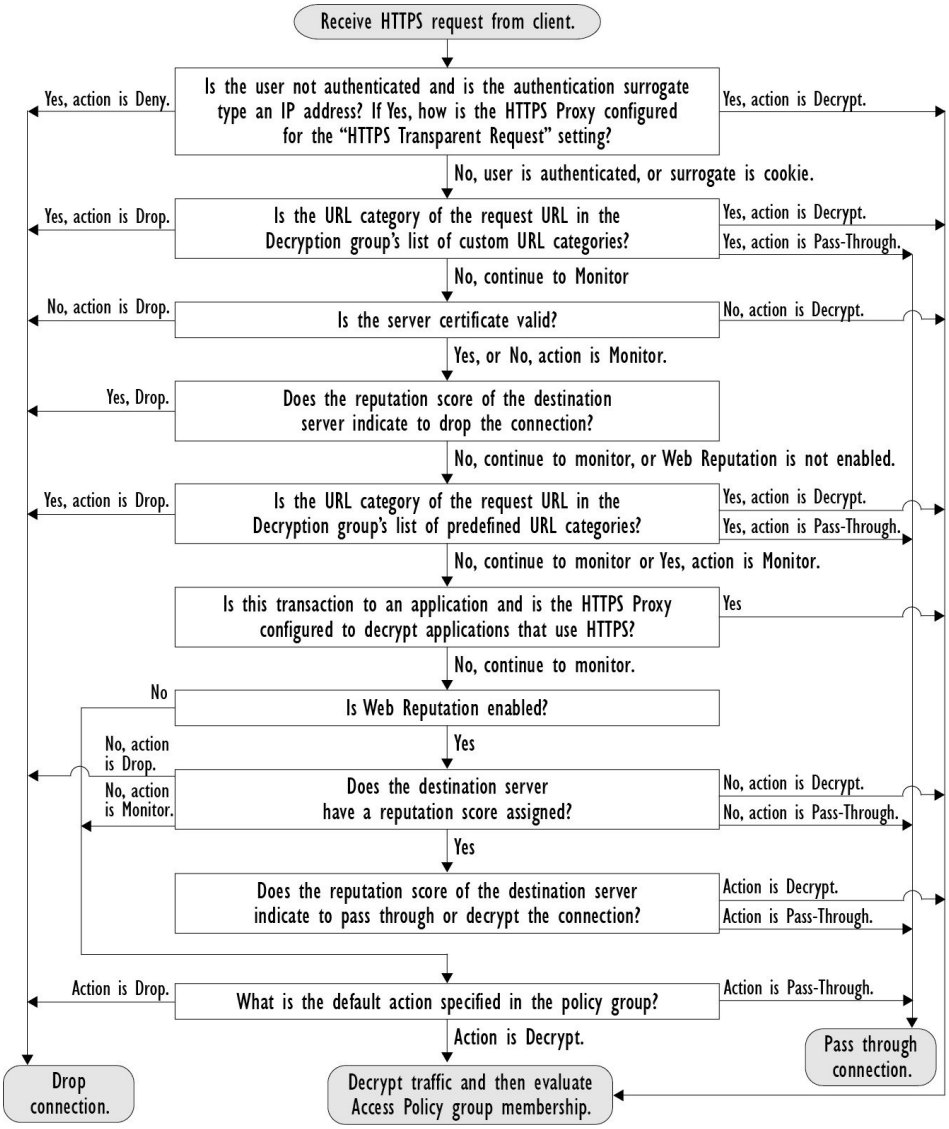
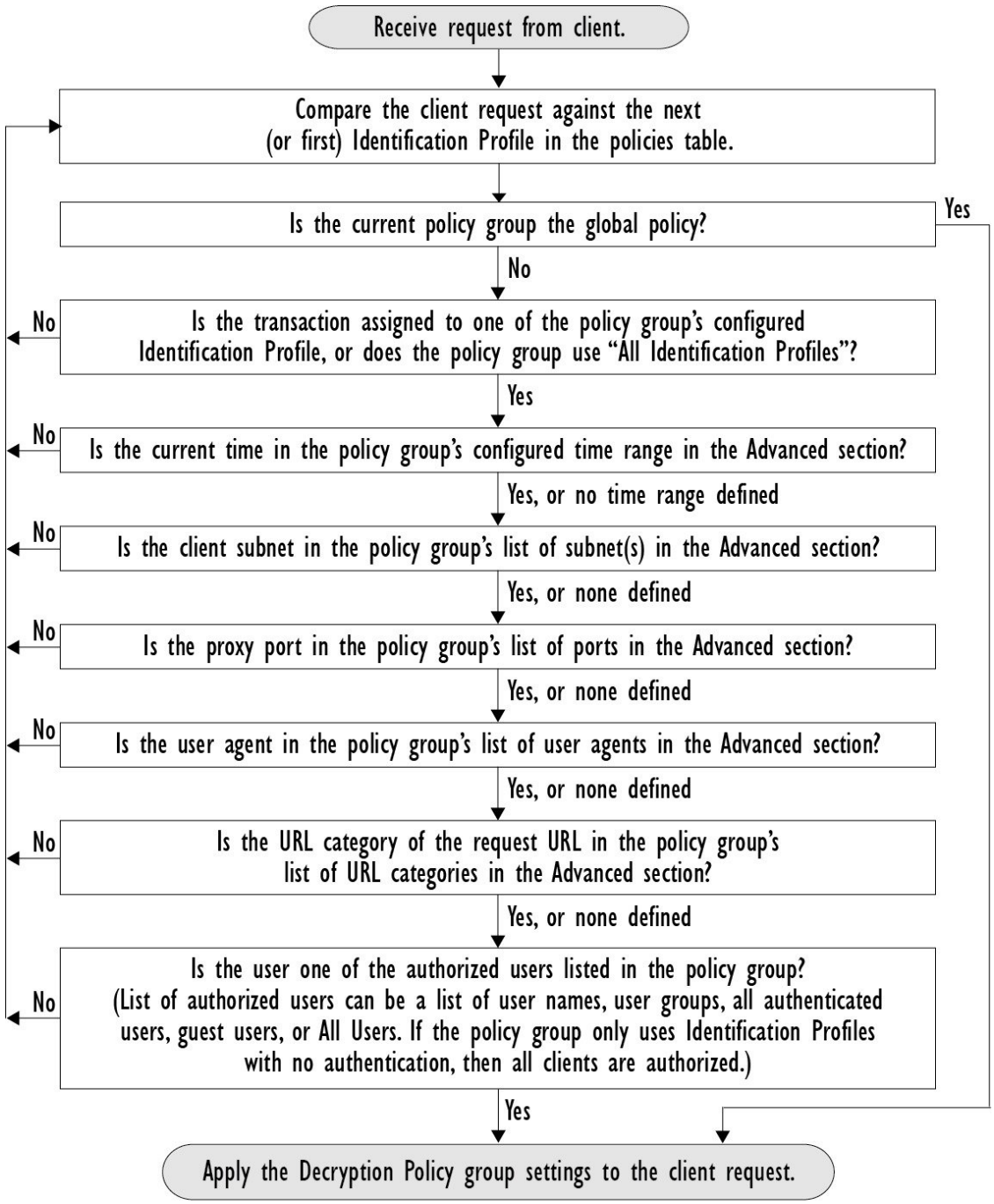


Figure 2: Flux de transaction des groupes de politiques pour les politiques de déchiffrement



Activation du proxy HTTPS

Pour surveiller et déchiffrer le trafic HTTPS, vous devez activer le proxy HTTPS. Lorsque vous activez le proxy HTTPS, vous devez configurer ce que l'appliance utilise comme certificat racine lorsqu'elle envoie des certificats de serveur autosignés aux applications clientes sur le réseau. Vous pouvez télécharger un

certificat racine et une clé dont votre organisation dispose déjà, ou vous pouvez configurer l'appliance de sorte qu'elle génère un certificat et une clé avec les informations que vous saisissez.

Une fois le proxy HTTPS activé, toutes les décisions de politique HTTPS sont prises en charge par les politiques de déchiffrement. Vous pouvez aussi configurer dans cette page ce que l'appliance fait du trafic HTTPS lorsque le certificat du serveur n'est pas valide.

Before you begin

Lorsque le proxy HTTPS est activé, les règles spécifiques à HTTPS dans les politiques d'accès sont désactivées et le proxy Web traite le trafic HTTPS déchiffré à l'aide des règles pour HTTP.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS), cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Le contrat de licence du proxy HTTPS s'affiche.

Étape 2 Lisez les conditions du contrat de licence du proxy HTTPS et cliquez sur **Accept** (Accepter).

Étape 3 Vérifiez que le champ Enable HTTPS Proxy (Activer le proxy HTTPS) est activé.

Étape 4 Dans le champ **HTTPS Ports to Proxy** (Ports HTTPS vers le proxy), saisissez les ports que l'appliance doit vérifier pour le trafic HTTPS. Le port par défaut est 443.

Note Secure Web Appliance peut utiliser un maximum de 30 ports comme proxy : 3 ports sont toujours réservés pour le proxy FTP et 27 ports peuvent être configurés comme proxy HTTP et HTTPS.

Étape 5 Chargez ou générez un certificat racine/de signature à utiliser pour le déchiffrement.

Note Si l'appliance a à la fois un certificat et une paire de clés téléchargés et un certificat et une paire de clés générés, elle utilise uniquement le certificat et la paire de clés actuellement sélectionnés dans la section Root Certificate for Signing (Certificat racine pour signature).

Étape 6 Dans la section HTTPS transparent Request (Demande HTTPS transparente), sélectionnez l'une des options suivantes :

- Decrypt the HTTPS request and redirect for authentication (Déchiffrer la demande HTTPS et rediriger pour authentification)
- Deny the HTTPS request (Refuser la demande HTTPS)

Ce paramètre s'applique uniquement aux transactions qui utilisent l'adresse IP comme substitution d'authentification et lorsque l'utilisateur n'a pas encore été authentifié.

Note Ce champ ne s'affiche que lorsque l'appliance est déployée en mode transparent.

Étape 7 **Note** Le déchiffrement peut faire échouer certaines applications, sauf si le certificat racine de signature est installé sur le client. Pour en savoir plus sur le certificat racine de l'appliance, consultez Gestion de la validation et du déchiffrement des certificats pour HTTPS, on page 10.

Étape 8 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

• Gestion de la validation et du déchiffrement des certificats pour HTTPS, on page 10

Contrôle du trafic HTTPS

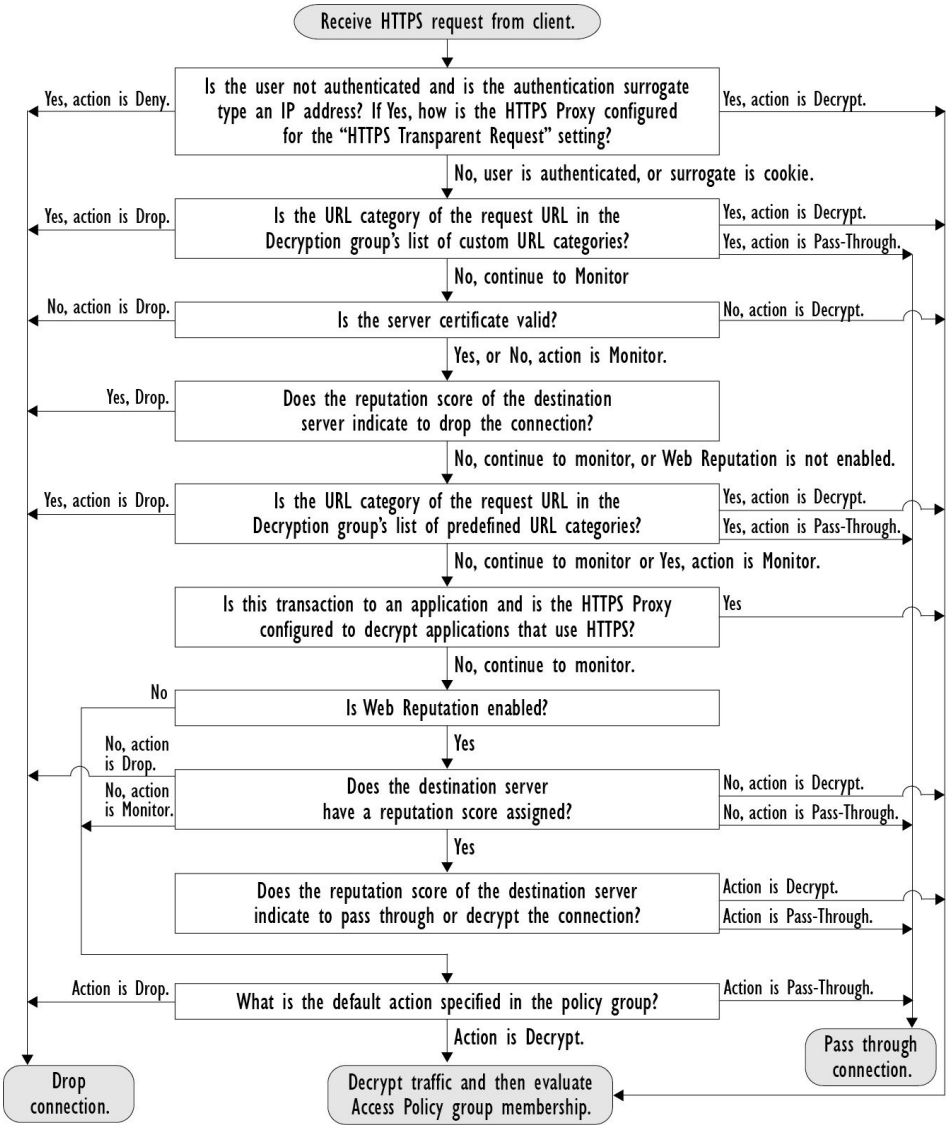
Après que Secure Web Appliance a affecté une demande de connexion HTTPS à un groupe de politiques de déchiffrement, la demande de connexion hérite des paramètres de contrôle de ce groupe de politiques. Les paramètres de contrôle du groupe de politiques de déchiffrement déterminent si l'appliance déchiffre, abandonne ou transmet la connexion :

Option	Description
URL Categories (Catégories d'URL)	Vous pouvez configurer l'action à entreprendre sur les demandes HTTPS pour chaque catégorie d'URL prédéfinie et personnalisée. Cliquez sur le lien sous la colonne URL Filtering (Filtrage d'URL) pour le groupe de politiques que vous souhaitez configurer. **Note** Si vous souhaitez *bloquer* (avec notification de l'utilisateur final) une catégorie d'URL particulière pour les demandes HTTPS au lieu de l'abandonner (sans notification de l'utilisateur final), choisissez de déchiffrer cette catégorie d'URL dans le groupe de politiques de déchiffrement, puis choisissez de bloquer la même URL dans le groupe de politiques d'accès.
Web Reputation (Réputation Web)	Vous pouvez configurer l'action à entreprendre sur les demandes HTTPS en fonction du score de réputation Web du serveur demandé. Cliquez sur le lien sous la colonne Web Reputation (Réputation Web) pour le groupe de politiques que vous souhaitez configurer.
Default Action (Action par défaut)	Vous pouvez configurer l'action que l'appliance doit effectuer quand aucun des autres paramètres ne s'applique. Cliquez sur le lien sous la colonne Default Action (Action par défaut) pour le groupe de politiques que vous souhaitez configurer. **Note** L'action configurée par défaut n'affecte la transaction que si aucune décision n'est prise en fonction de la catégorie d'URL ou du score de réputation Web. Si le filtrage de réputation Web est désactivé, l'action par défaut s'applique à toutes les transactions qui correspondent à une action Monitor (Superviser) dans une catégorie d'URL. Si le filtrage de réputation Web est activé, l'action par défaut est utilisée uniquement si l'action Monitor (Superviser) est sélectionnée pour les sites sans score de réputation.

Pour contourner le trafic chiffré ayant un bon score de réputation Web, assurez-vous de désactiver l'option **Decrypt for Application Detection** (Déchiffrer pour la détection des applications) dans la section **Decryption Options** (Options de déchiffrement) de la page HTTPS Proxy Settings (Paramètres du proxy HTTPS).

Le diagramme suivant montre comment l'appliance détermine l'action à exécuter sur une demande HTTPS après avoir affecté une politique de déchiffrement particulière à la demande. Le score de réputation Web du serveur de destination est évalué une seule fois, mais le résultat est appliqué à deux étapes différentes dans le flux de décision. Par exemple, l'action Drop (Abandonner) du score de réputation Web remplace toute action spécifiée pour les catégories d'URL prédéfinies.

Figure 3: Application des actions de la politique de déchiffrement



Configuration des options de déchiffrement

Before you begin

Vérifiez que le proxy HTTPS est activé, comme décrit dans Activation du proxy HTTPS, on page 5.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Activez les options de déchiffrement.

Option de déchiffrement	Description
Decrypt for Authentication (Déchiffrer pour authentification)	Pour les utilisateurs qui n'ont pas été authentifiés avant cette transaction HTTPS, autorisez le déchiffrement pour l'authentification.
Decrypt for End-User Notification (Déchiffrer pour notification à l'utilisateur final)	Autorisez le déchiffrement pour qu'AsyncOS puisse afficher la notification de l'utilisateur final. **Note** Si le certificat est non valide et que les certificats non valides sont définis pour être abandonnés, lors de l'exécution d'une trace de politique, la première action enregistrée pour la transaction est « decrypt » (déchiffrer).
Decrypt for End-User Acknowledgment (Déchiffrer pour l'accusé de réception de l'utilisateur final)	Pour les utilisateurs qui n'ont pas accusé réception du proxy Web avant cette transaction HTTPS, autorisez le déchiffrement pour qu'AsyncOS puisse afficher l'accusé de réception de l'utilisateur final.
Decrypt for Application Detection (Déchiffrer pour la détection d'applications)	Améliore la capacité d'AsyncOS à détecter les applications HTTPS.

Authentification et connexions HTTPS

L'authentification au niveau de la couche de connexion HTTPS est disponible pour les types de demandes suivants :

Option	Description
Explicit requests (Demandes explicites)	• authentification sécurisée du client désactivée ou • authentification sécurisée du client activée et substitution basée sur IP
Transparent requests (Demandes transparentes)	• Substitution basée sur IP, déchiffrement pour l'authentification activé ou • substitution basée sur IP, client authentifié précédemment à l'aide d'une demande HTTP

Certificats racines

Le proxy HTTPS utilise les certificats racine et les fichiers de clé privée que vous chargez sur l'appliance pour déchiffrer le trafic. Le certificat racine et les fichiers de clé privée que vous chargez sur l'appliance doivent être au format PEM; le format DER n'est pas pris en charge.

Vous pouvez saisir les informations de certificat racine comme suit :

- **Generate (Générer).** Vous pouvez saisir des informations de base sur l'organisation, puis cliquer sur un bouton pour que l'appliance génère le reste du certificat et une clé privée.

- **Upload (Charger).** Vous pouvez charger un fichier de certificat et le fichier de clé privée correspondant créé hors de l'appliance.

Note Vous pouvez également charger un certificat intermédiaire signé par une autorité de certification racine. Lorsque le proxy Web imite le certificat du serveur, il envoie le certificat chargé avec le certificat imité à l'application client. De cette façon, tant que le certificat intermédiaire est signé par une autorité de certification racine approuvée par l'application cliente, l'application fera également confiance au certificat de serveur imité. Consultez À propos des certificats et des clés pour obtenir de plus amples renseignements.

Vous pouvez choisir comment gérer les certificats racine émis par Secure Web Appliance :

- **Inform users to accept the root certificate (Informer les utilisateurs d'accepter le certificat racine).** Vous pouvez informer les utilisateurs de votre organisation des nouvelles politiques de l'entreprise et leur dire d'accepter le certificat racine fourni par l'entreprise en tant que source de confiance.
- **Add the root certificate to client machines (Ajouter le certificat racine sur les machines clientes).** Vous pouvez ajouter le certificat racine sur toutes les machines clientes du réseau en tant qu'autorité de certification racine approuvée. De cette façon, les applications client acceptent automatiquement les transactions avec le certificat racine.

Étape 1 Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cliquez sur le lien Download Certificate (Télécharger le certificat) correspondant au certificat généré ou chargé.

Note Pour réduire la possibilité que les machines clientes obtiennent une erreur de certificat, envoyez les modifications après avoir généré ou chargé le certificat racine dans Secure Web Appliance, puis distribuez le certificat aux machines clientes et validez les modifications sur l'appliance.

Gestion de la validation et du déchiffrement des certificats pour HTTPS

Secure Web Appliance valide les certificats avant d'inspecter et de déchiffrer le contenu.

Certificats valides

Qualités d'un certificat valide :

- **Non expiré.** La période de validité du certificat inclut la date du jour courant.
- **Autorité de certification reconnue.** L'autorité de certification émettrice est incluse dans la liste des autorités de certification approuvées stockée sur Secure Web Appliance.
- **Signature valide.** La signature numérique a été correctement mise en œuvre selon des normes cryptographiques.
- **Des noms uniformes.** Le nom commun correspond au nom d'hôte spécifié dans l'en-tête HTTP.
- **Non révoqué.** L'autorité de certification émettrice n'a pas révoqué le certificat.

Thèmes connexes

- Activation de la vérification de l'état de révocation en temps réel, on page 14
- Configuration du traitement des certificats non valides, on page 13
- Options de vérification de l'état de révocation des certificats, on page 13

Traitement des certificats non valides

L'appliance peut effectuer l'une des actions suivantes pour les certificats de serveur non valides :

- **Drop.**
- **Decrypt.**
- **Supervision.**

Certificats non valides pour plusieurs raisons

Pour les certificats de serveur qui ne sont pas valides en raison d'une autorité racine non reconnue et d'un certificat expiré, le proxy HTTPS effectue l'action qui s'applique aux autorités racine non reconnues.

Dans tous les autres cas, pour les certificats de serveur qui ne sont pas valides pour plusieurs raisons à la fois, le proxy HTTPS effectue les actions dans l'ordre, de la plus restrictive à la moins restrictive.

Avertissements de certificat non fiable pour les connexions déchiffrées

Lorsque Secure Web Appliance rencontre un certificat non valide et est configuré pour déchiffrer la connexion, AsyncOS crée un certificat non fiable qui exige que l'utilisateur final accepte ou rejette la connexion. Le nom commun du certificat est « Untrusted Certificate Warning » (Avertissement de certificat non fiable).

L'ajout de ce certificat non approuvé à la liste des certificats approuvés supprimera la possibilité pour l'utilisateur final d'accepter ou de rejeter la connexion.

Quand AsyncOS génère l'un de ces certificats, il crée une entrée de journal de proxy avec le texte « Signing untrusted key » ou « Signing untrusted cert » (Signature d'une clé non approuvée) ou « Signing untrusted cert » (Signature de certificat non approuvé).

Chargement d'un certificat racine et d'une clé

Before you begin

Activez le proxy HTTPS. Activation du proxy HTTPS, on page 5.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Use Uploaded Certificate and Key** (Utiliser le certificat et la clé téléchargés).

Étape 4 Cliquez sur **Browse** (Parcourir) dans le champ Certificate (Certificat) pour naviguer jusqu'au fichier de certificat stocké sur l'ordinateur local.

Si le fichier que vous téléchargez contient plusieurs certificats ou clés, le proxy Web utilise le premier certificat ou la première clé du fichier.

Étape 5 Cliquez sur **Browse** (Parcourir) dans le champ Key (Clé) pour accéder au fichier de clé privée.

Note La longueur de la clé doit être de 512, 1024 ou 2048 bits.

Étape 6 Sélectionnez **Key is Encrypted** (La clé est chiffrée) si la clé est chiffrée.

Étape 7 Cliquez sur **Upload Files** (Charger les fichiers) pour transférer le certificat et les fichiers de clé vers Secure Web Appliance.

Les informations sur le certificat chargé sont affichées sur la page Edit HTTPS Proxy Settings (Modifier les paramètres de proxy HTTPS).

Étape 8 (Facultatif) Cliquez sur **Download Certificate** (Télécharger le certificat) afin de pouvoir le transférer vers les applications clientes sur le réseau.

Étape 9 Envoyez et validez vos modifications.

Génération d'un certificat et d'une clé pour le proxy HTTPS

Before you begin

Activez le proxy HTTPS. Activation du proxy HTTPS, on page 5.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Use Generate Certificate and Key** (Utiliser le certificat et la clé générés).

Étape 4 Cliquez sur **Generate New Certificate and Key** (Générer un nouveau certificat et une nouvelle clé).

Étape 5 Dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé), saisissez les informations à afficher dans le certificat racine.

Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ **Common Name** (Nom commun).

Étape 6 Cliquez sur **Generate** (Générer).

Étape 7 Les informations sur le certificat généré sont affichées sur la page Edit HTTPS Proxy Settings (Modifier les paramètres de proxy HTTPS).

Étape 8 (Facultatif) Cliquez sur **Download Certificate** (Télécharger le certificat) afin de pouvoir le transférer vers les applications clientes sur le réseau.

Étape 9 (Facultatif) Cliquez sur le lien **Download Certificate Signing Request** (Télécharger la requête de signature de certificat) afin de pouvoir envoyer la requête de signature de certificat (CSR) à une autorité de certification (CA).

Étape 10 (Facultatif) Après avoir reçu le certificat signé de l'autorité de certification, chargez-le dans Secure Web Appliance. Vous pouvez le faire à tout moment après avoir généré le certificat sur l'appliance.

Étape 11 Envoyez et validez les modifications.

Configuration du traitement des certificats non valides

Before you begin

Vérifiez que le proxy HTTPS est activé, comme décrit dans Activation du proxy HTTPS, on page 5.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Pour chaque type d'erreur de certificat, définissez la réponse du proxy : **Drop**, **Decrypt**, or **Monitor**.

Type d'erreur de certificat	Description
Expiré	La date actuelle se trouve en dehors de la plage de validité du certificat.
Nom d'hôte non concordant	Le nom d'hôte dans le certificat ne correspond pas au nom d'hôte auquel le client tentait d'accéder. **Note** Le proxy Web ne peut effectuer une correspondance de nom d'hôte que s'il est déployé en mode de transfert explicite. Lorsqu'il est déployé en mode transparent, il ne connaît pas le nom d'hôte du serveur de destination (il ne connaît que l'adresse IP). Il ne peut donc pas le comparer au nom d'hôte indiqué dans le certificat du serveur.
Autorité racine/émetteur non reconnu	L'autorité racine ou une autorité de certification intermédiaire n'est pas reconnue.
Certificat de signature non valide	Il y a eu un problème avec le certificat de signature.
Certificat feuille non valide	Un problème est survenu avec le certificat feuille, notamment un problème de rejet, de décodage ou de non-concordance.
Tous les autres types d'erreurs	La plupart des autres types d'erreurs sont dues au fait que l'appliance n'est pas en mesure d'établir la liaison SSL avec le serveur HTTPS. Pour de plus amples renseignements sur d'autres scénarios d'erreur liés aux certificats de serveur, consultez l'adresse http://www.openssl.org/docs/apps/verify.html.

Étape 4 Envoyez et validez les modifications.

Options de vérification de l'état de révocation des certificats

Pour déterminer si l'autorité de certification émettrice a révoqué un certificat, Secure Web Appliance peut effectuer une vérification auprès de l'autorité de certification émettrice des manières suivantes :

- **Liste de révocation de certificat (certificats Comodo uniquement)** Secure Web Appliance vérifie la liste de révocation des certificats de Comodo. Comodo gère cette liste et la met à jour en fonction de ses propres politiques. Selon la date de la dernière mise à jour, la liste de révocation des certificats peut être obsolète au moment de la vérification par Secure Web Appliance.
- **Protocole d'état du certificat en ligne (OCSP).** Secure Web Appliance vérifie l'état de révocation auprès de l'autorité de certification émettrice en temps réel. Si l'autorité de certification émettrice prend

en charge OCSP, le certificat contient une URL pour la vérification de l'état en temps réel. Cette fonctionnalité est activée par défaut pour les nouvelles installations et désactivée par défaut pour les mises à jour.

Note Secure Web Appliance effectue l'interrogation OCSP uniquement pour les certificats qu'il juge valides à tous les autres égards et qui comprennent l'URL OCSP.

Thèmes connexes

- Activation de la vérification de l'état de révocation en temps réel, on page 14
- Configuration du traitement des certificats non valides, on page 13

Activation de la vérification de l'état de révocation en temps réel

Before you begin

Assurez-vous que le proxy HTTPS est activé. Consultez Activation du proxy HTTPS, on page 5.

Étape 1 **Security Services > HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Enable Online Certificate Status Protocol (OCSP)** [Activer le protocole d'état du certificat en ligne (OCSP)].

Étape 4 Configurez les propriétés de **OCSP Result Handling** (Gestion des résultats OCSP).

Cisco recommande de configurer les options de gestion des résultats OCSP sur les mêmes actions que les options de gestion des certificats non valides. Par exemple, si vous renseignez Expired Certificate (Certificat expiré) par Monitor (Superviser), définissez le certificat révoqué sur Monitor (Superviser).

Étape 5 (Facultatif) Développez la section Advanced configuration (Configuration avancée) et configurez les paramètres décrits ci-dessous.

Nom du champ	Description
OCSP Valid Response Cache Timeout (Délai d'expiration du cache de réponse valide OCSP)	Temps d'attente avant de revérifier une réponse OCSP valide en secondes (s), minutes (m), heures (h) ou jours (d). L'unité par défaut est seconde. La plage valide est comprise entre 1 seconde et 7 jours.
OCSP Invalid Response Cache Timeout (Délai d'expiration du cache de réponse OCSP non valide)	Temps d'attente avant de revérifier une réponse OCSP non valide en secondes (s), minutes (m), heures (h) ou jours (d). L'unité par défaut est seconde. La plage valide est comprise entre 1 seconde et 7 jours.

Nom du champ	Description
OCSP Network Error Cache Timeout (Délai d'expiration du cache d'erreur de réseau OCSP)	Temps d'attente avant de tenter de contacter à nouveau le répondeur OCSP après avoir échoué à obtenir une réponse, en secondes (s), minutes (m), heures (h) ou jours (d). Plage valide comprise entre 1 seconde et 24 heures.
Allowed Clock Skew (Décalage d'horloge autorisé)	Différence maximale autorisée dans les paramètres de temps entre le Secure Web Appliance et le répondeur OCSP, en secondes (s) ou en minutes (m). Plage valide comprise entre 1 seconde et 60 minutes.
Maximum Time to Wait for OCSP Response (Temps d'attente maximal d'une réponse OCSP)	Temps maximal d'attente d'une réponse du répondeur OCSP. La plage valide est comprise entre 1 seconde et 10 minutes. Indiquez une durée plus courte pour réduire les délais d'accès de l'utilisateur final aux requêtes HTTPS au cas où le répondeur OCSP ne serait pas disponible.
Use upstream proxy for OCSP checking (Utiliser un proxy en amont pour la vérification OCSP)	Nom de groupe des proxys en amont.
Servers exempt from upstream proxy (Serveurs dispensés du proxy en amont)	Adresses IP ou noms d'hôte des serveurs à exclure. Peut être laissé vide.

Étape 6 Envoyez et validez les modifications.

Certificats racine approuvés

Le Secure Web Appliance est livré avec et gère une liste de certificats racine approuvés. Les sites Web dotés de certificats approuvés n'ont pas besoin de déchiffrement.

Vous pouvez gérer la liste des certificats approuvés, en y ajoutant et en en supprimant fonctionnellement des certificats. Bien que Secure Web Appliance ne supprime pas les certificats de la liste principale, il vous permet de remplacer la confiance dans un certificat, ce qui supprime fonctionnellement le certificat de la liste approuvée.

Ajout de certificats à la liste approuvée

Before you begin

Vérifiez que le proxy HTTPS est activé. Consultez Activation du proxy HTTPS, on page 5.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Manage Trusted Root Certificates** (Gérer les certificats racine approuvés).

Étape 3 Cliquez sur **Import** (Importer).

Étape 4 Cliquez sur **Browse** (Parcourir) et accédez au fichier de certificat.

Étape 5 **Envoyez** et **validez** les modifications.

Recherchez le certificat que vous avez téléchargé dans la liste **Custom Trusted Root Certificates** (Certificats racine approuvés personnalisés).

Suppression de certificats de la liste approuvée

Étape 1 Sélectionnez **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Manage Trusted Root Certificates** (Gérer les certificats racine approuvés).

Étape 3 Cochez la case **Override Trust** (Remplacer la confiance) correspondant au certificat que vous souhaitez supprimer de la liste.

Étape 4 **Envoyez** et **validez** les modifications.

Routage du trafic HTTPS

La capacité d'AsyncOS à acheminer les transactions HTTPS en fonction des informations stockées dans les en-têtes des clients est limitée et différente pour le HTTPS transparent et explicite.

Option	Description
Transparent HTTPS (HTTPS transparent)	Dans le cas d'un HTTPS transparent, AsyncOS n'a pas accès aux informations dans les en-têtes du client. Par conséquent, AsyncOS ne peut pas appliquer les politiques de routage si une politique de routage ou un profil d'identification repose sur les informations contenues dans les en-têtes de client.
Explicit HTTPS (HTTPS explicite)	Dans le cas d'un protocole HTTPS explicite, AsyncOS a accès aux informations suivantes dans les en-têtes des clients : • URL • Numéro du port de destination Par conséquent, 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.

Résolution de problèmes relatifs aux déchiffrement/HTTPS/certificats

- Accès aux sites HTTPS à l'aide de politiques de routage avec critères de catégorie d'URL
- HTTPS avec substituts basés sur IP et demandes transparentes
- Contournement du déchiffrement pour des sites Web particuliers
- Alerte : Problème lié au certificat de sécurité

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.