Configuration des paramètres de transfert supplémentaires de l'appliance de sécurité Web pour l'application Webex

Introduction

Ce document décrit comment configurer les stratégies de contournement de l'appareil Web sécurisé (SWA/WSA) pour garantir la fonctionnalité appropriée de l'application Cisco Webex dans des conditions de déploiement spéciales.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Async OS pour Secure Web Appliance 14.x ou version ultérieure.
- Accès utilisateur de l'administrateur à l'interface utilisateur graphique (GUI) de l'appliance Web sécurisé.
- Administration de l'accès utilisateur à l'interface de ligne de commande (CLI) de l'appliance Web sécurisé.

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 l’incidence possible des commandes.

Problème

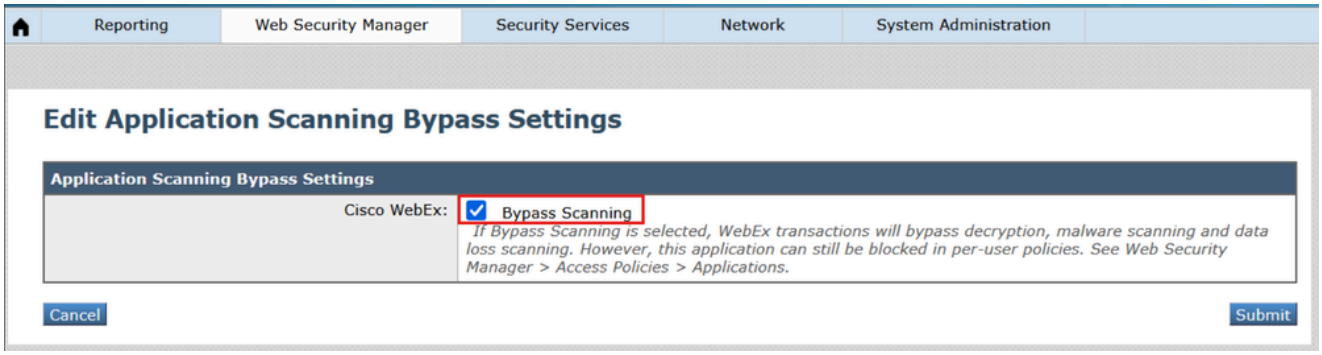
En fonction de la documentation publique Webex relative à la configuration requise du réseau pour les services Webex, le serveur proxy doit être configuré pour permettre au trafic de signalisation Webex d'accéder aux domaines/URL répertoriés dans le document. L'appliance Web sécurisée répond aux exigences de la plupart des environnements en activant la case à cocher Contournement de l'application Webex dans les paramètres de contournement. Toutefois, certaines configurations supplémentaires peuvent être requises sur l'appliance Web sécurisée pour éviter toute interruption de service dans l'application Webex. Les étapes suivantes sont recommandées pour de tels scénarios :

Contournement de l'analyse des applications Webex

La fonctionnalité Cisco Webex : Bypass Scanning est la première étape pour permettre au trafic de l'application Webex de passer sans filtre par l'appareil Web sécurisé. Elle doit être activée dans tous les environnements et scénarios de déploiement où les utilisateurs du poste de travail Webex ou des applications mobiles ont un trafic Web proxy via l'appliance Web sécurisé.

Étapes pour activer le contournement de l'analyse des applications Webex :

1. Dans l'interface utilisateur graphique de WSA, accédez à Web Security Manager > Bypass Settings > Edit Application Bypass Settings.
2. Cochez la case "Cisco WebEx".



1_wsa_bypass_scan_settings

3. Envoyer et valider les modifications

Lorsque ce paramètre est activé, il ne contourne pas le trafic transparent comme on pourrait s'y attendre une fois que les FQDN sont ajoutés à la liste de contournement sur l'appareil Web sécurisé. Au contraire, le trafic de l'application Webex est toujours transmis par proxy via l'appareil Web sécurisé, mais il sera transmis lors du déchiffrement avec l'étiquette de décision « PASSTHRU_AVC ». Vous trouverez ci-dessous un exemple de l'affichage dans les journaux d'accès :

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

Considérations relatives aux environnements uniques

Il existe quelques scénarios où des configurations supplémentaires sont requises pour que l'application Webex fonctionne lorsque le trafic est transféré par proxy via l'appliance Web sécurisé.

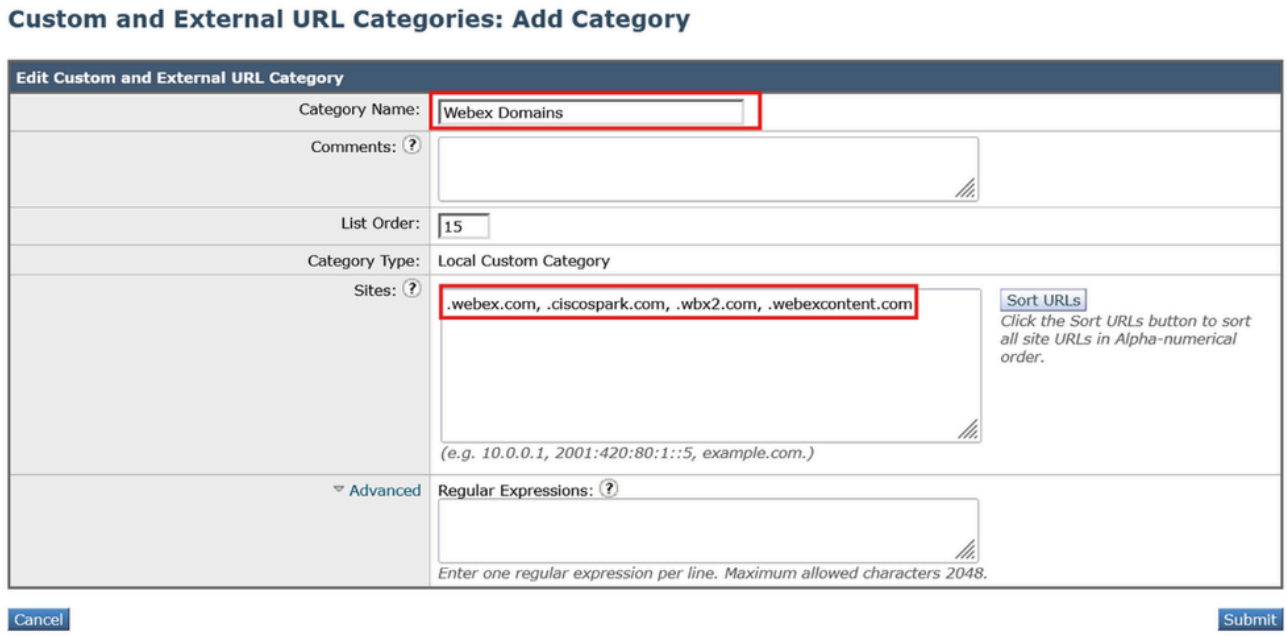
Scénario 1 : Les domaines Webex doivent être exemptés de l'authentification

Cela est particulièrement évident dans les environnements où les substituts IP ne sont pas activés dans le profil d'identification et où la redirection transparente est utilisée. D'après la documentation existante, l'application Webex est capable d'authentifier NTLMSSP sur les stations de travail

jointes au domaine où le proxy est explicitement défini. Sinon, il est recommandé de configurer une catégorie personnalisée pour les domaines Webex et de les exempter de l'authentification. Étapes pour exempter les domaines Webex de l'authentification :

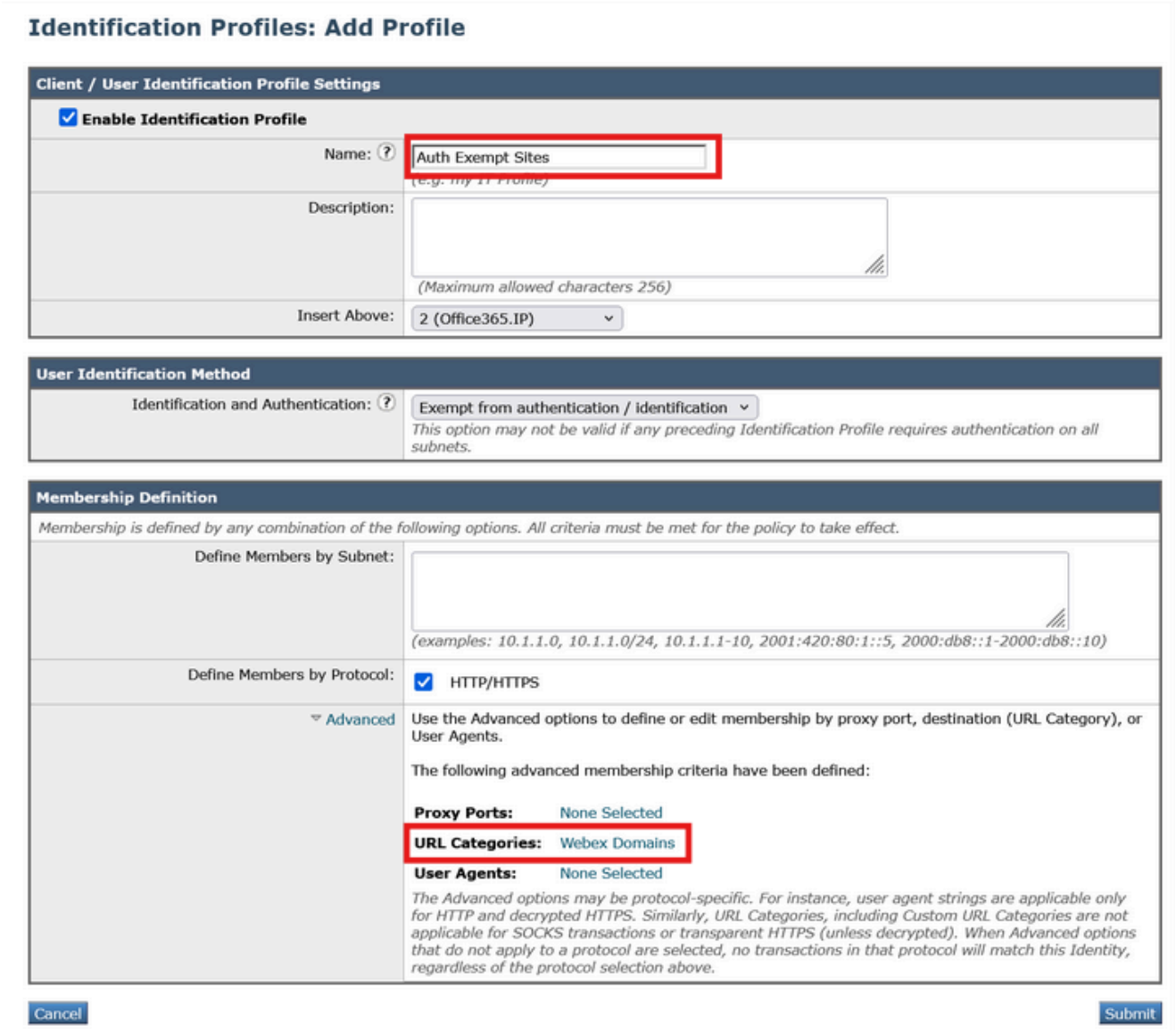
1. Dans l'interface utilisateur graphique de WSA, accédez à Web Security Manager > Custom and External URL Categories > Add Category.
2. Attribuez un nom à la nouvelle catégorie et placez les domaines suivants dans la section Sites :

```
.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
```



2_wsa_custom_url_category

3. Cliquez sur Submit. Accédez ensuite à Gestionnaire de sécurité Web > Profils d'identification > Ajouter un profil d'identification
4. Donnez un nom au nouveau profil, et dans la section Avancé pour Catégories d'URL, sélectionnez la nouvelle catégorie qui a été créée à l'étape #2



3_wsa_id_profile

5. Assurez-vous que l'option Identification et authentification du nouveau profil est définie sur Exempter de l'authentification/identification
6. Soumettre et valider les modifications.

Scénario 2 : Les domaines de contenu Webex ne sont pas entièrement respectés pour le contournement du décodage.

Il existe quelques sous-domaines liés à webexcontent.com qui ne passent pas automatiquement lors du déchiffrement lorsque le contournement de l'analyse d'application Webex est activé. Le contenu servi à partir de ces domaines est approuvé par l'application Webex lorsqu'il est déchiffré tant que le certificat de déchiffrement de l'appliance Web sécurisée est déjà ajouté au magasin de certificats racine approuvés de l'appareil, ou autrement signé par une autorité de certification interne qui est déjà approuvée par l'appareil exécutant l'application Webex. Toutefois, si le périphérique n'est pas géré et que le certificat de déchiffrement de l'appliance Web sécurisée n'est pas approuvé, ces domaines doivent être configurés pour être transmis lors du déchiffrement.

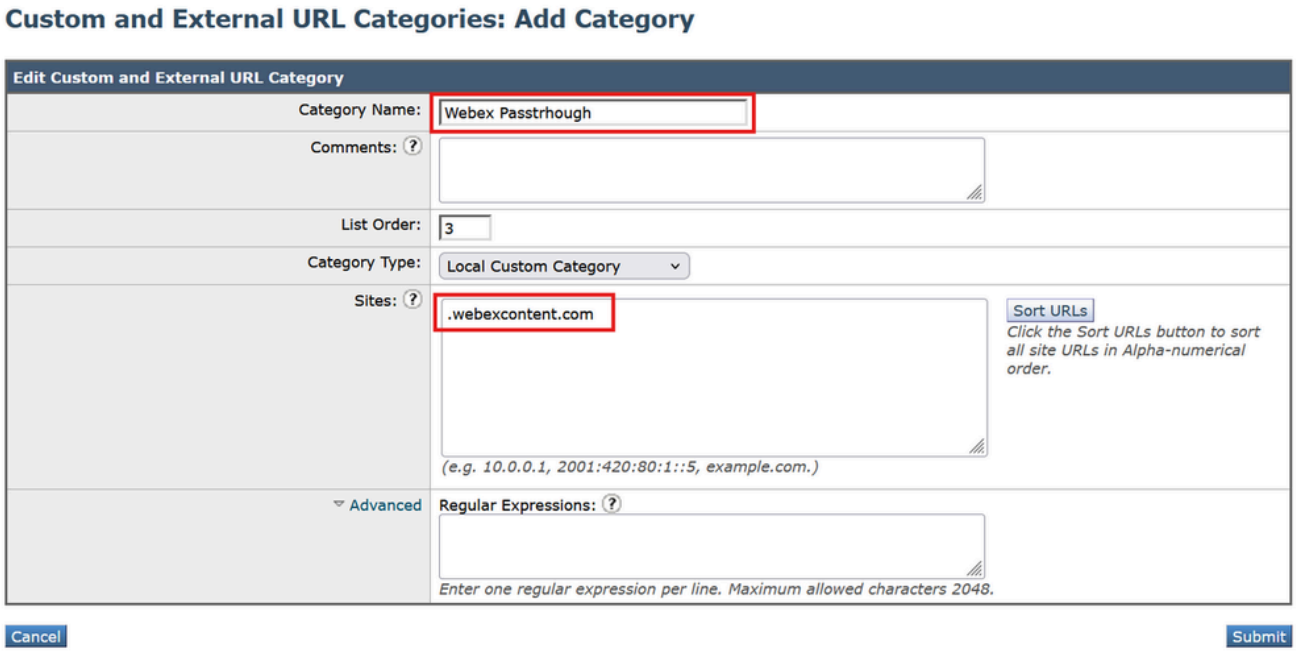
Lorsque le déploiement de redirection transparent est en place et qu'il y a plus d'un SWA le long

de l'usurpation d'adresse IP du client utilisé pour les groupes de redirection, le trafic peut être configuré pour rediriger vers l'appliance Web sécurisée en fonction de l'adresse IP de destination, et de même le trafic de retour des serveurs Web est configuré pour rediriger à travers l'appliance Web sécurisée en fonction de l'adresse source. Lorsque l'appliance Web sécurisée est configurée pour établir des connexions au serveur Web à l'aide de l'adresse IP qu'elle résout à l'aide de la recherche DNS, le trafic de retour peut être redirigé par inadvertance vers une autre appliance Web sécurisée et être ensuite abandonné. Ce problème affecte non seulement Webex, mais aussi d'autres applications de streaming vidéo, en raison de l'utilisation d'adresses IP tournantes sur les serveurs Web.

Étapes de configuration du passthrough lors du déchiffrement pour tous les domaines Webex :

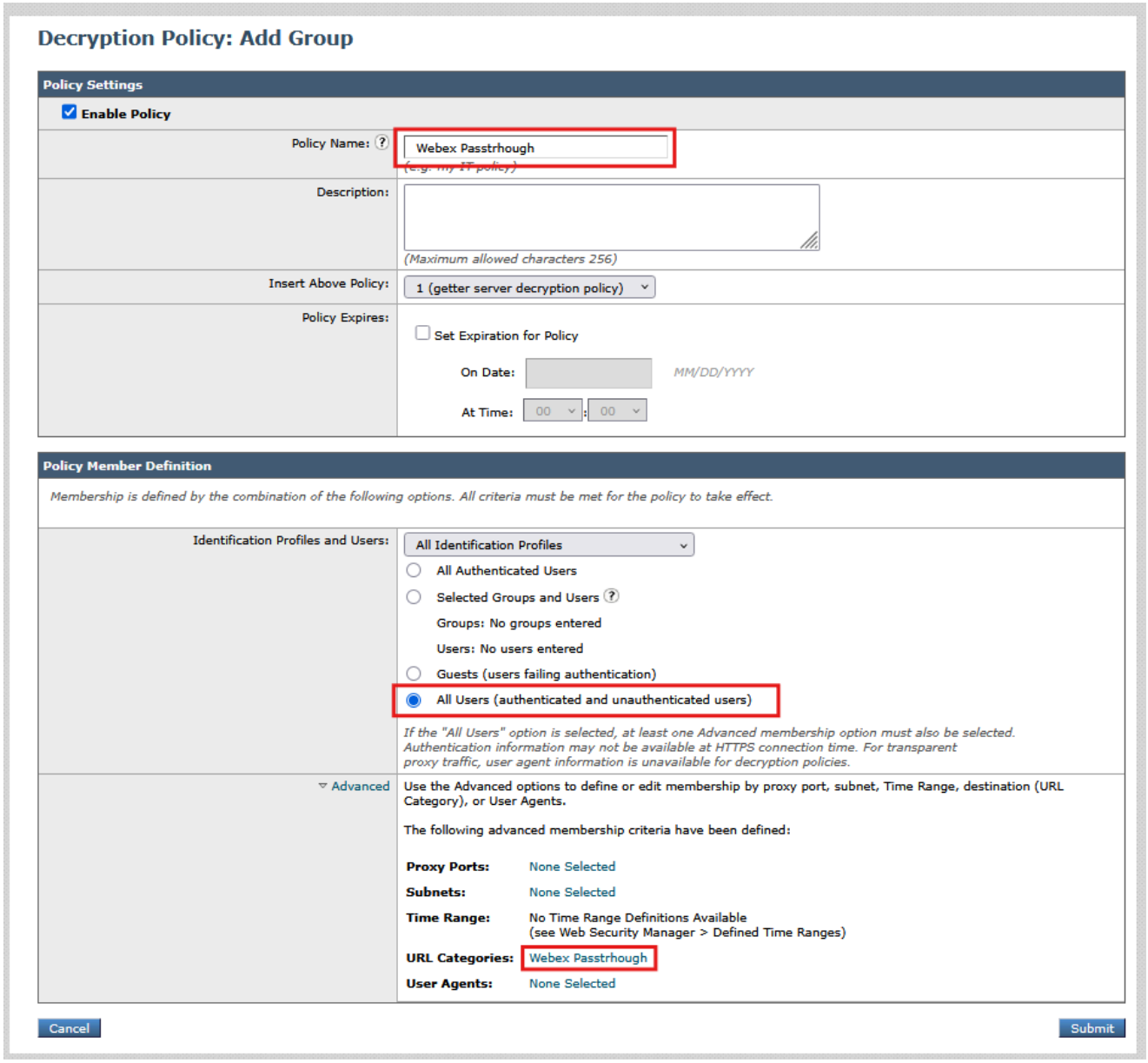
1. Assurez-vous que Webex Application Scanning Bypass est activé conformément aux instructions ci-dessus.
2. Dans l'interface utilisateur graphique de WSA, accédez à Web Security Manager > Custom and External URL Categories > Add Category.
3. Attribuez un nom à la nouvelle catégorie et placez le domaine suivant dans la section Sites :

```
.webexcontent.com
```



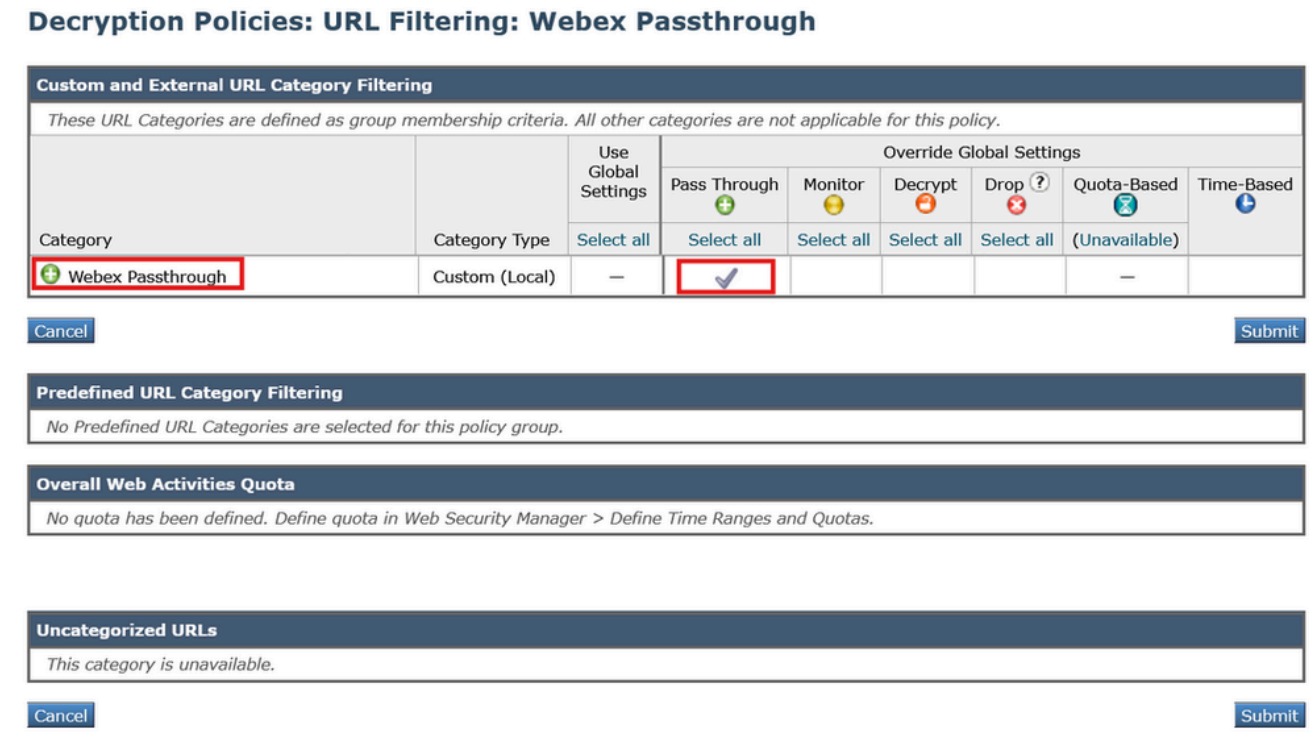
4_wsa_url_category

4. Cliquez sur Submit. Accédez à présent à Gestionnaire de sécurité Web > Stratégies de décodage > Ajouter une stratégie
5. Attribuez un nom à la nouvelle stratégie, définissez Profils d'identification et utilisateurs sur "Tous les utilisateurs" et, dans la section Avancé pour les catégories d'URL, sélectionnez la nouvelle catégorie créée à l'étape #3



5_wsa_decryption_policy

6. Cliquez sur Submit. Ensuite, cliquez sur la section Filtrage d'URL et définissez la catégorie personnalisée qui a été créée à l'étape #3 sur "Passthrough".



6_wsa_url_filtering

7. Envoyer et valider les modifications.

Si plusieurs appliances Web sécurisées sont déployées pour une redirection transparente et que l'usurpation d'adresse IP client est activée, deux solutions sont possibles :

1. Configurez les services WCCP sortants et de retour pour équilibrer la charge en fonction de l'adresse du client plutôt que de l'adresse du serveur.
2. Dans l'interface de ligne de commande WSA, définissez advanced proxyconfig > DNS > "Find web server by" pour toujours utiliser l'adresse IP fournie par le client sur les connexions au serveur Web (options 2 et 3). Pour plus d'informations sur ce paramètre, reportez-vous à la section DNS du guide Use Secure Web Appliance Best Practices.

Vérification

Une fois les paramètres d'intercommunication terminés, le trafic Webex sera traité dans les journaux d'accès en tant qu'intercommunication conformément aux politiques :

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

Examiner et surveiller l'application webex, si une lenteur ou une interruption de service est signalée, examiner les journaux d'accès une fois de plus et valider que tout le trafic côté webex est traité correctement.

Informations connexes

- Configuration réseau requise pour les services Webex
- Utilisation des meilleures pratiques de sécurisation des appliances Web

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.