Contourner le trafic dans l'appliance Web sécurisée

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Différents types de contournement
- Procédures de contournement SWA par type de déploiement
  - Contourner le trafic dans un déploiement explicite
    - Configuration du fichier PAC
    - Configuration du navigateur (Microsoft Edge, Internet Explorer, Google Chrome)
    - Configuration du navigateur (Mozilla Firefox)
    - Configuration du navigateur (Apple Safari)
    - Configuration de la stratégie de groupe
  - Contourner le trafic dans un déploiement transparent
    - Paramètre de contournement SWA
    - Redirection du trafic à partir du protocole WCCP (Web Cache Communication Protocol)/PBR (Policy Based Router)
- Configuration de l'intercommunication et autorisation du trafic dans SWA
- Autres informations utiles

Introduction

Ce document décrit les étapes pour contourner le trafic dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.
- Protocoles réseau et proxy de base

Cisco recommande d'installer les outils suivants :

- SWA physique ou virtuel
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA

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.

Différents types de contournement

Dans SWA, il existe trois manières différentes de contourner le trafic pour l'empêcher d'atteindre le SWA, selon votre déploiement de proxy (déploiement explicite ou transparent), ou d'être analysé et analysé par le SWA. Voici un bref aperçu de ces trois concepts :

- Contourner : Paramètre qui empêche le trafic d'atteindre le SWA, ce qui réduit l'utilisation de la carte réseau et élimine le besoin d'une session entre l'utilisateur et l'appliance.
- Passthrough : Cette configuration empêche le SWA de déchiffrer le trafic HTTPS. Malgré cela, le SWA continue de faciliter deux sessions distinctes : un entre le client et le SWA, et un second entre le SWA et le serveur Web.
- Allow: Paramètre de la stratégie d'accès où le trafic HTTP ou décrypté ignore l'inspection par les moteurs SWA internes, tels qu'AMP, Sophos, WebRoot et le filtre d'application. Dans ce cas, deux sessions sont toujours utilisées dans le SWA.

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP	✓	✗	GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP	✓	✗	WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP	✗	✓	From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP	✗	✓	From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP	✓	✓	GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP	✓	✓	GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

Image - Tableau comparatif

Procédures de contournement SWA par type de déploiement

Les procédures de contournement varient en fonction de votre modèle de déploiement de proxy. Voici un bref aperçu de chaque type :

- Déploiement explicite : Les clients sont configurés manuellement pour diriger le trafic vers le proxy.
- Déploiement transparent : L'infrastructure réseau redirige automatiquement le trafic vers le proxy, sans nécessiter de configuration côté client.

Contourner le trafic dans un déploiement explicite

Pour contourner le trafic dans le déploiement explicite, vous devez configurer le client pour qu'il ne transfère pas la requête Web pour les URL souhaitées vers le SWA. Comme l'illustre ce schéma de réseau, une partie du trafic est acheminée directement vers le pare-feu ou la passerelle par défaut pour contourner le SWA (chemin numéro 2).

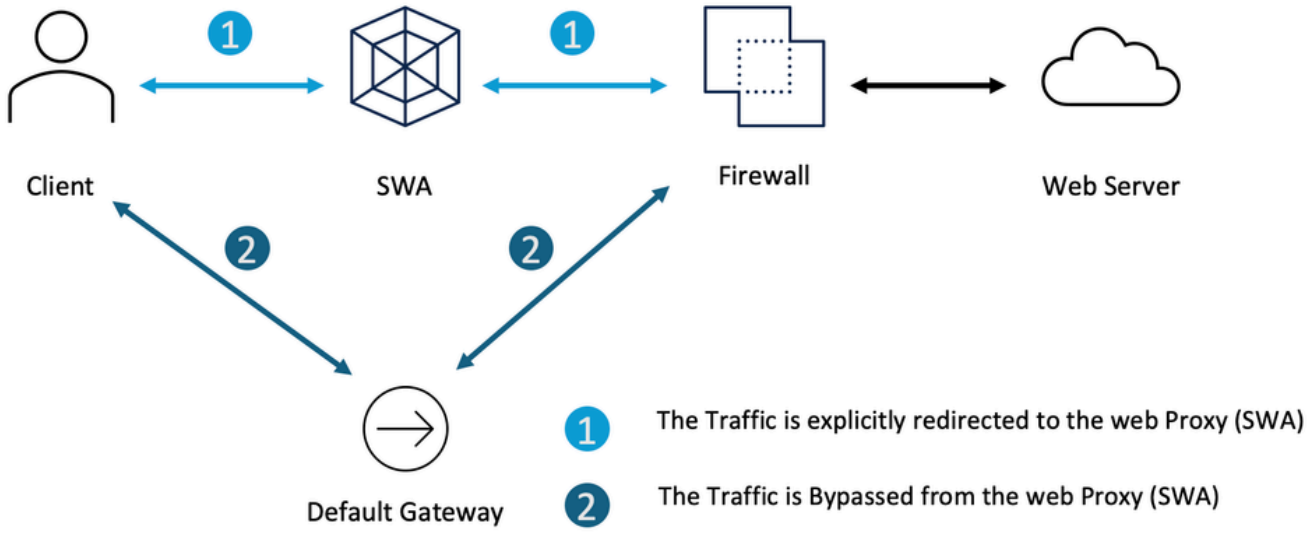


Image - Contourner le trafic dans un déploiement explicite

En fonction de votre déploiement de proxy explicite, vous pouvez exempter certaines URL d'être redirigées vers le SWA.

Configuration de proxy explicite	Étapes d'exclusion des URL de l'accès au SWA

Configuration du fichier PAC	Selon la façon dont vous avez configuré votre fichier PAC, vous pouvez définir la liste d'exceptions et définir l'action sur DIRECT.
	
	Voici quelques exemples pour contourner l'adresse IP privée afin d'atteindre le SWA :
	
	`var resolved_ip = dnsResolve(host);`
	`if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||`
	`isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||`
	`isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||`
	`isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`
	`return "DIRECT";`
	
	Ceci est un exemple de contournement du trafic vers www.cisco.com de la redirection du SWA :
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`

	Cet exemple consiste à contourner tous les sous-domaines de cisco.com pour rediriger le SWA `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` Remarque : Le fichier PAC n'étant pas un produit Cisco, les informations sont fournies à titre gracieux. Pour plus d'assistance, communiquez avec le fournisseur du logiciel.
Configuration du navigateur (Microsoft Edge, Internet Explorer, Google Chrome)	Étape 1. Dans le menu Démarrer, tapez Options Internet et appuyez sur Entrée. Étape 2. Accédez à l'onglet Connections et cliquez sur LAN Settings. Étape 3. Cliquez sur Advanced. Étape 4. Définissez les URL souhaitées dans la section Exceptions.

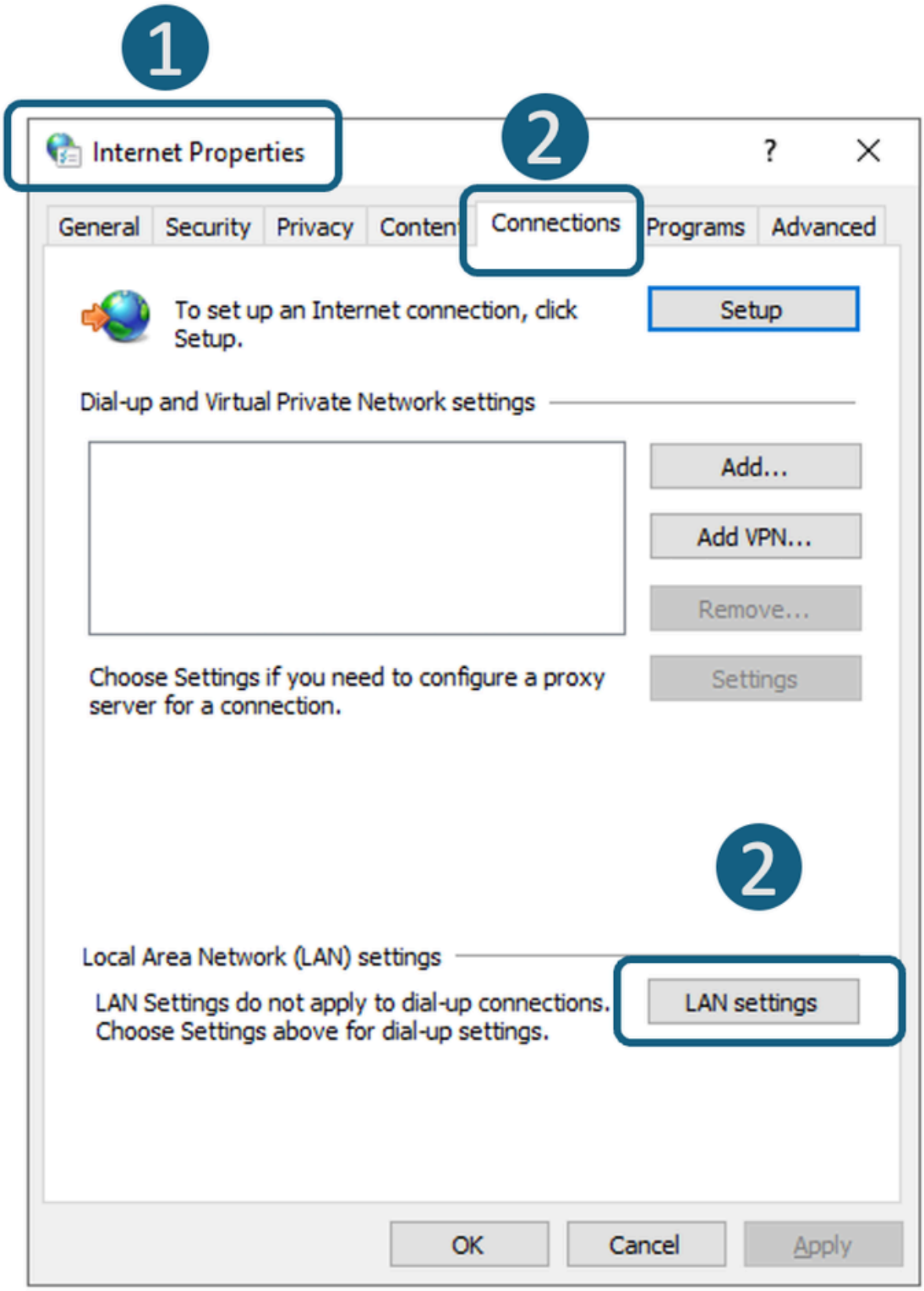


Image - Accédez aux paramètres LAN

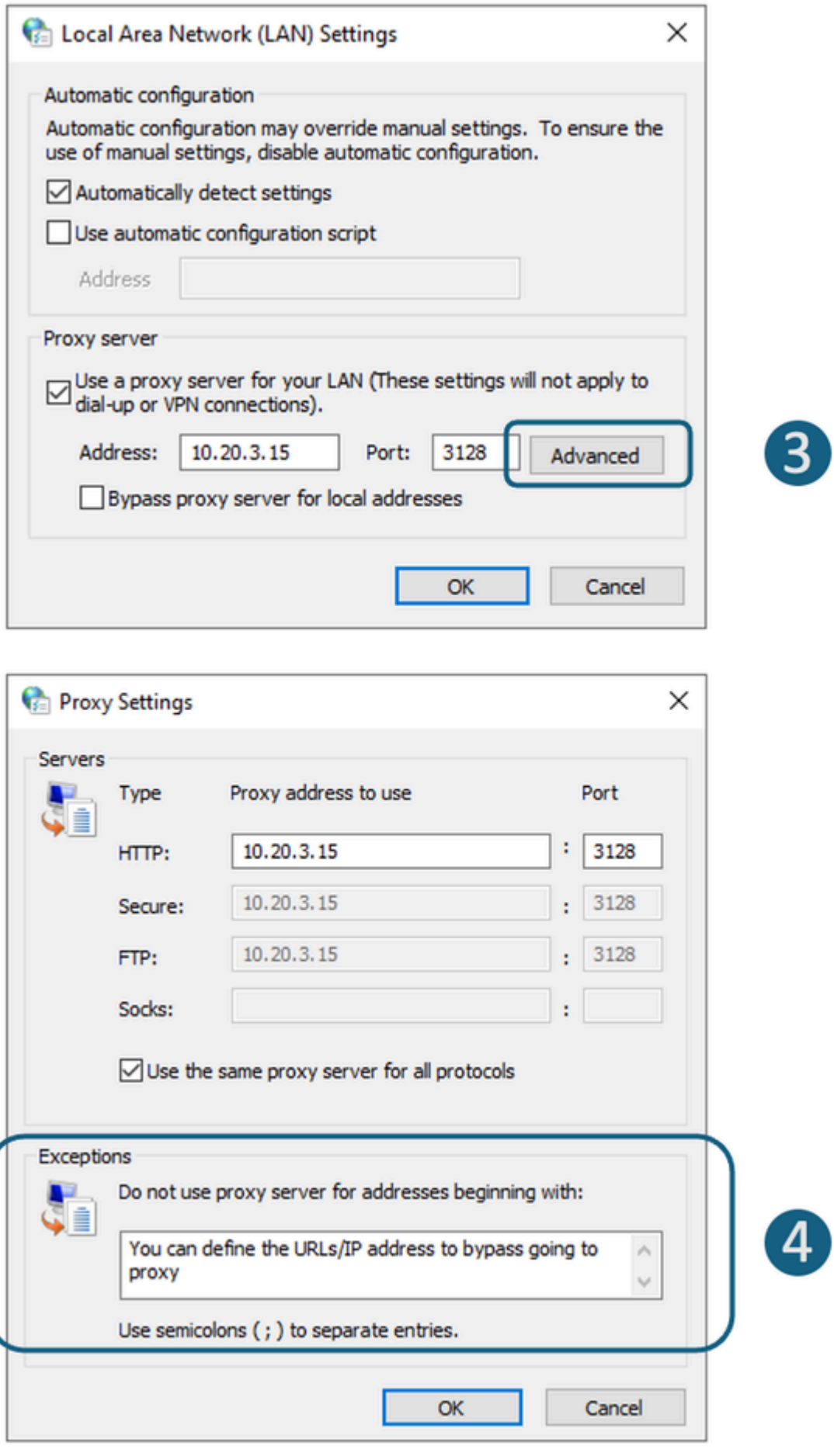
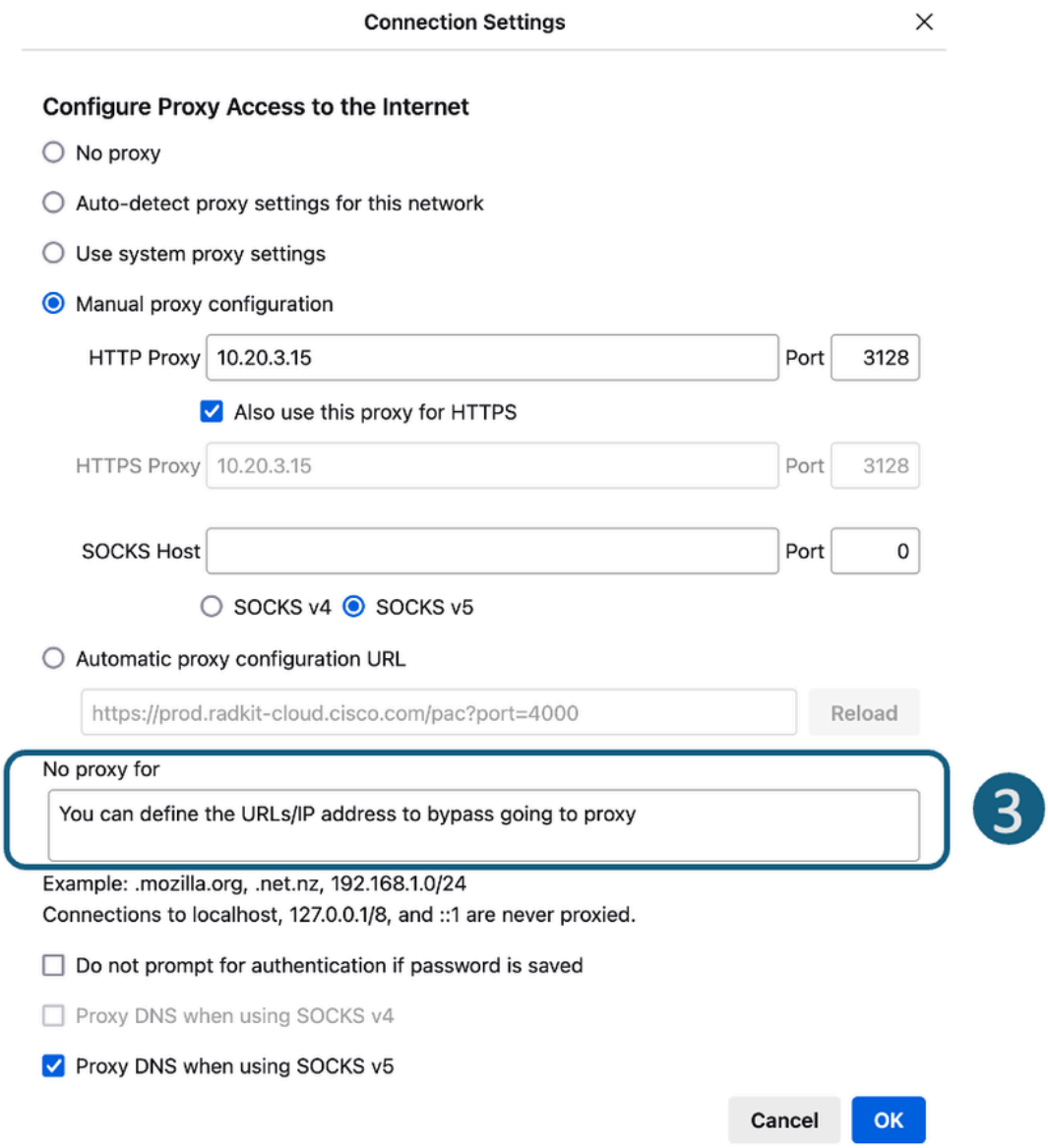
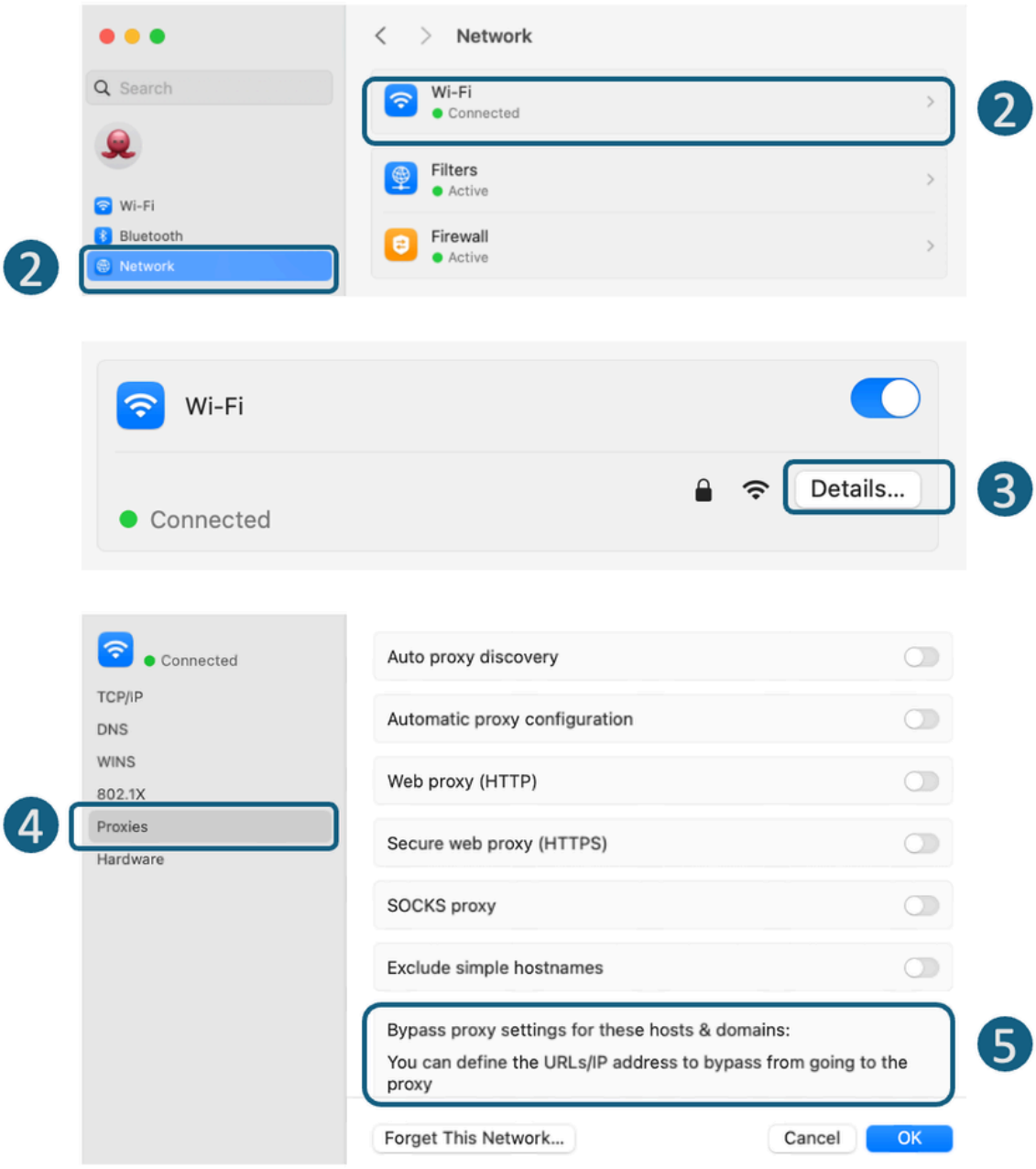


Image - Définir les exceptions

Configuration du navigateur (Mozilla Firefox)	Étape 1. Dans le coin supérieur droit, cliquez sur le menu à trois barres et sélectionnez Paramètres. Étape 2. Dans la barre de recherche, tapez proxy. Étape 3. Définissez les URL souhaitées dans la section Aucun proxy pour.  Image - Définir les exceptions dans Fire Fox
Configuration du navigateur (Apple Safari)	Étape 1. Dans le coin supérieur gauche, cliquez sur l'icône Apple et sélectionnez System Settings (Paramètres système). Étape 2. Dans le panneau de gauche, accédez à Réseau et sélectionnez l'interface réseau que vous utilisez pour accéder à Internet.

	Étape 3. Cliquez sur Détails. Étape 4. Dans le panneau de gauche, sélectionnez Proxies. Étape 5. Définissez les URL souhaitées dans la section Contourner les paramètres du proxy.  Image - Définir les exceptions dans Fire Fox
Configuration de la stratégie de groupe	Selon la façon dont vous avez configuré la stratégie de groupe pour transmettre les paramètres du proxy, vous pouvez définir la liste d'exceptions.

Contourner le trafic dans un déploiement transparent

Vous pouvez contourner le trafic dans un déploiement transparent à l'aide des paramètres de contournement WCCP ou SWA. Le contournement SWA agit au niveau de la couche 3, acheminant le trafic vers la passerelle par défaut et contournant entièrement l'appliance, ce qui empêche le traitement et la création de sessions séparées.

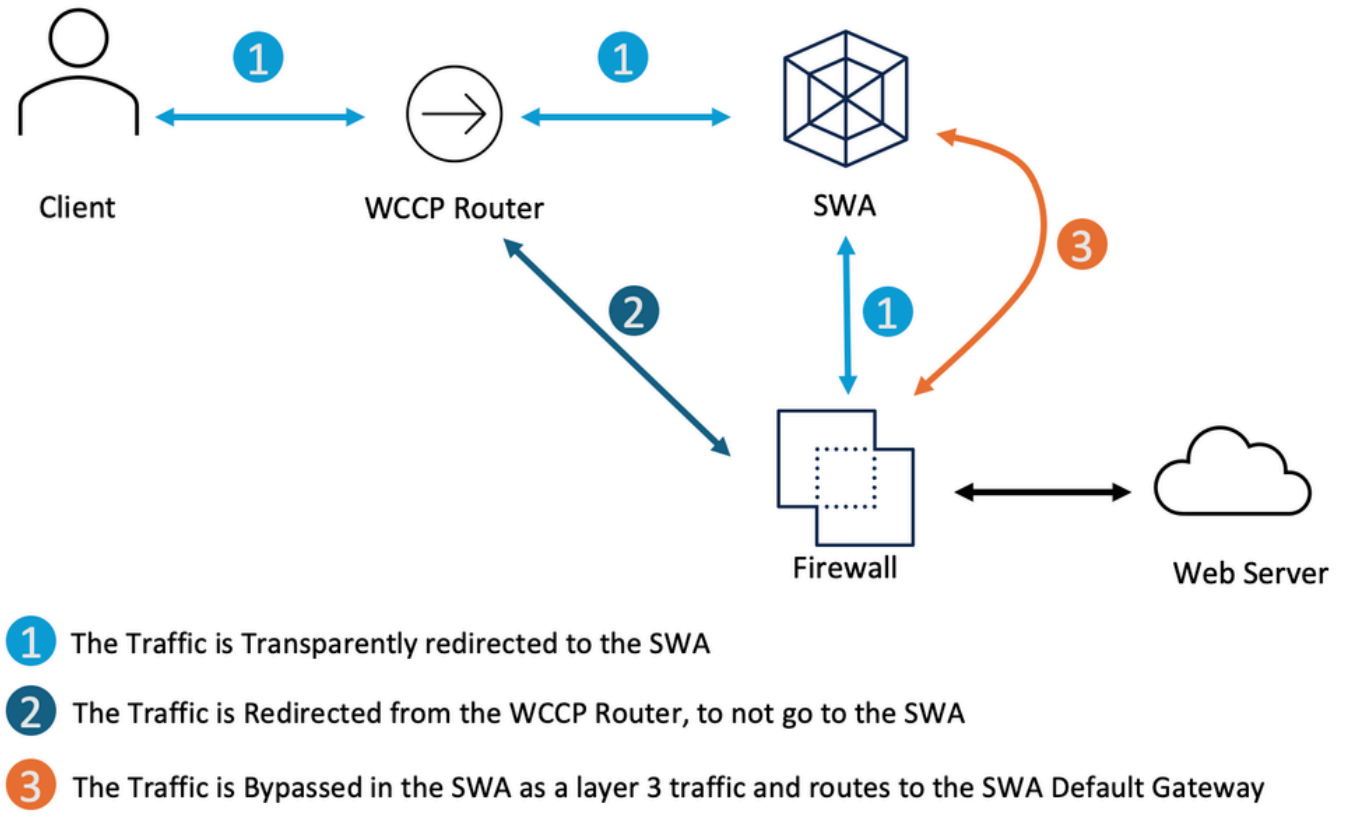
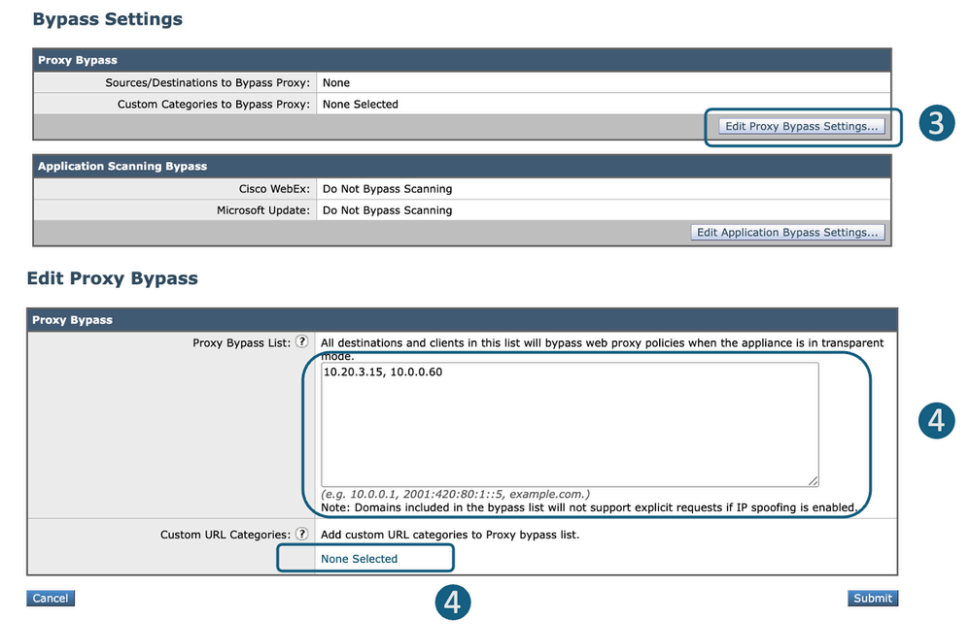


Image - Contourner le trafic dans un déploiement transparent

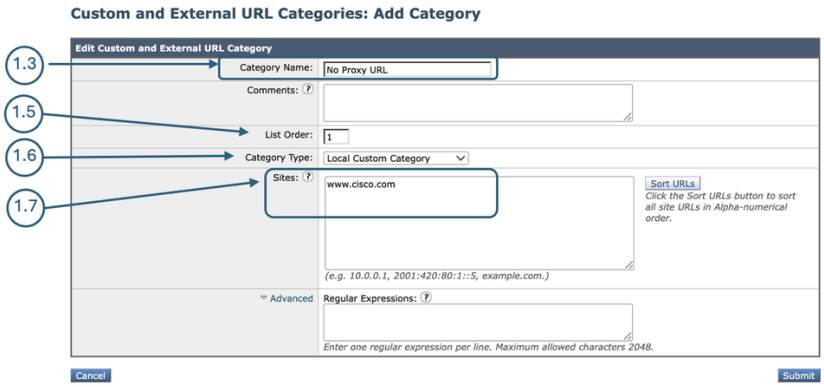
Ignorer le trafic Déploiement du proxy transparent	Étapes pour contourner le trafic avant d'atteindre le SWA
Paramètre de contournement SWA	Étape 1. Dans l'interface graphique, sélectionnez Web Security Manager. Étape 2 : sélectionnez Bypass Settings. Étape 3. Cliquez sur Edit Proxy Bypass Settings. Étape 4. Vous pouvez entrer l'URL, l'adresse IP ou ajouter une catégorie d'URL personnalisée à la liste. Étape 5. Soumettre et valider les modifications

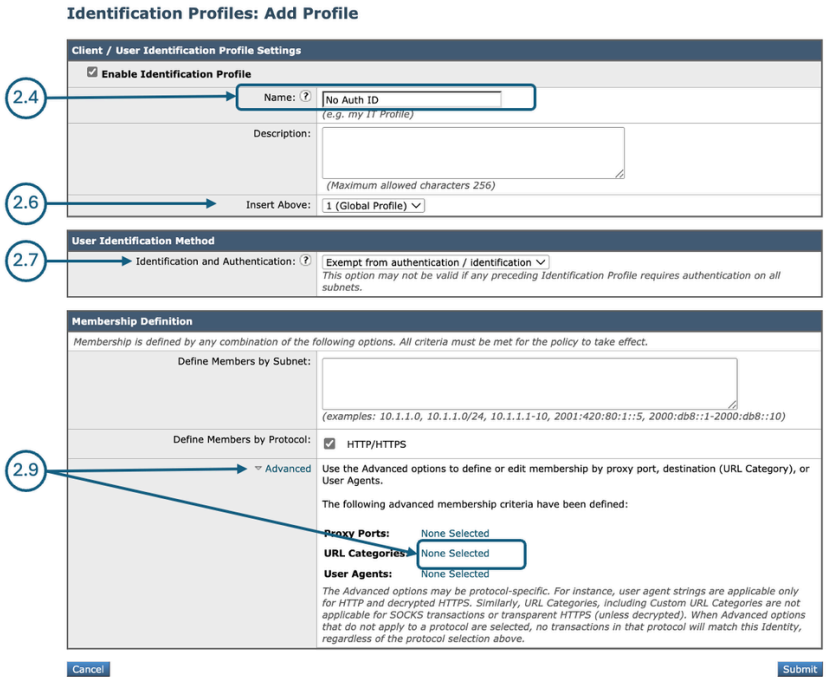
	 Image - Configuration des paramètres de contournement Conseil : Le trafic contourné avec ces paramètres n'est pas consigné dans les journaux d'accès et peut être affiché dans les journaux de contournement.
Redirection du trafic à partir du protocole WCCP (Web Cache Communication Protocol)/PBR (Policy Based Router)	Vous pouvez configurer l'adresse IP source ou de destination dans votre WCCP ou PBR pour ne pas rediriger certains trafics vers le SWA.

Configuration de l'intercommunication et autorisation du trafic dans SWA

Si le trafic atteint le SWA et afin de réduire la charge sur le SWA pour des raisons de confidentialité, vous ne voulez pas que le trafic de certaines URL soit inspecté par le SWA, utilisez ces étapes.

Étapes	Étapes
Étape 1 : création d'une catégorie d'URL personnalisée pour les URL	Étape 1.1. Dans l'interface graphique, choisissez Web Security Manager, puis cliquez sur Custom and External URL Categories.

	Étape 1.2. Cliquez sur Add Category pour ajouter une catégorie d'URL personnalisée. Étape 1.3. Attribuez un nom de catégorie unique. Étape 1.4. (Facultatif) Ajoutez une description. Étape 1.5. Dans Ordre des listes, choisissez la première catégorie sur laquelle vous souhaitez vous positionner. Étape 1.6. Dans la liste déroulante Type de catégorie, sélectionnez Catégorie personnalisée locale. Étape 1.7. Ajoutez les URL souhaitées dans la section Sites. Étape 1.8. Envoyer.  Image - Créer une catégorie d'URL personnalisée
Étape 2 : création d’un profil d’identification pour exempter le trafic de l’authentification	Étape 2.1. À partir de l'interface graphique, choisissez Web Security Manager, puis cliquez sur Identification Profiles. Étape 2.2. Cliquez sur Add Profile pour ajouter un profil. Étape 2.3. Utilisez la case à cocher Activer le profil d'identification pour activer ce profil ou le désactiver rapidement sans le supprimer. Étape 2.4. Attribuez un nom de profil unique. Étape 2.5. (Facultatif) Ajoutez une description. Étape 2.6. Dans la liste déroulante Insérer au-dessus, choisissez l'emplacement de ce profil dans le tableau. Étape 2.7. Dans la section User Identification Method, sélectionnez Exempt from authentication/ identification. Étape 2.8. Dans le champ Define Members by Subnet (Définir les membres par sous-réseau), laissez ce champ vide pour inclure toutes les adresses IP du client, sauf si vous souhaitez transmettre le trafic pour certaines adresses IP.

	Étape 2.9. Dans la section Advanced, sélectionnez Custom URL Categories.  Image - Ajouter un profil d'identification Étape 2.10. Ajoutez la catégorie d'URL personnalisée créée à l'étape 1. Étape 2.11. Cliquez sur Terminé. Étape 2.12. Envoyer.
Étape 3 : création d’une stratégie de déchiffrement pour le trafic.	Étape 3.1. Dans l'interface graphique, sélectionnez Web Security Manager, puis cliquez sur Decryption Policy. Étape 3.2. Cliquez sur Add Policy pour ajouter une stratégie de décodage. Étape 3.3. Utilisez la case à cocher Enable Policy pour activer cette stratégie. Étape 3.4. Attribuez un nom de stratégie unique. Étape 3.5. (Facultatif) Ajoutez une description. Étape 3.6. Dans la liste déroulante Insérer une stratégie ci-dessus, sélectionnez la première stratégie. Étape 3.7. Dans les profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé à l'étape 2. Étape 3.8. Envoyer.

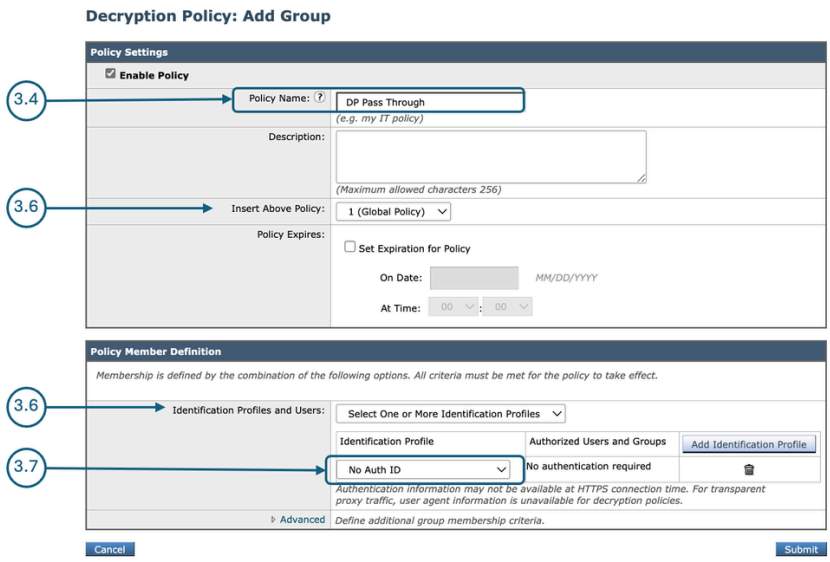
<table>
<tr>
<td></td>
<td>


Image - Créer une stratégie de déchiffrement

Étape 3.9. Sur la page Decryption Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie de décodage.

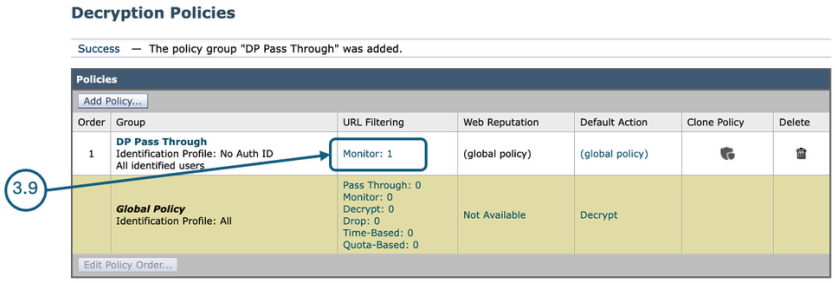


Image - Sélectionner le filtrage des URL

Étape 3.10. Sélectionnez Pass Through comme action pour la catégorie d'URL créée à l'étape 1.

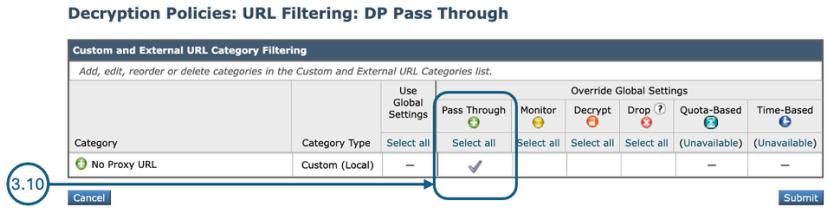


Image - Définir l'action sur Passthrough

Étape 3.11. Envoyer.</td>
</tr>
<tr>
<td>Étape 4. Créez une stratégie d’accès pour autoriser le trafic des mises à jour Microsoft.</td>
<td>Étape 4.1. Dans l'interface graphique, sélectionnez Web Security Manager, puis cliquez sur Access Policy.</td>
</tr>
</table>

Étape 4.2. Cliquez sur Add Policy pour ajouter une stratégie d'accès.

Étape 4.3. Utilisez la case à cocher Enable Policy pour activer cette stratégie.
Étape 4.4. Attribuez un nom de stratégie unique.
Étape 4.5. (Facultatif) Ajoutez une description.
Étape 4.6. Dans la liste déroulante Insérer une stratégie ci-dessus, sélectionnez la première stratégie.

Étape 4.7. Dans les profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé à l'étape 2.

Étape 4.8. Envoyer.

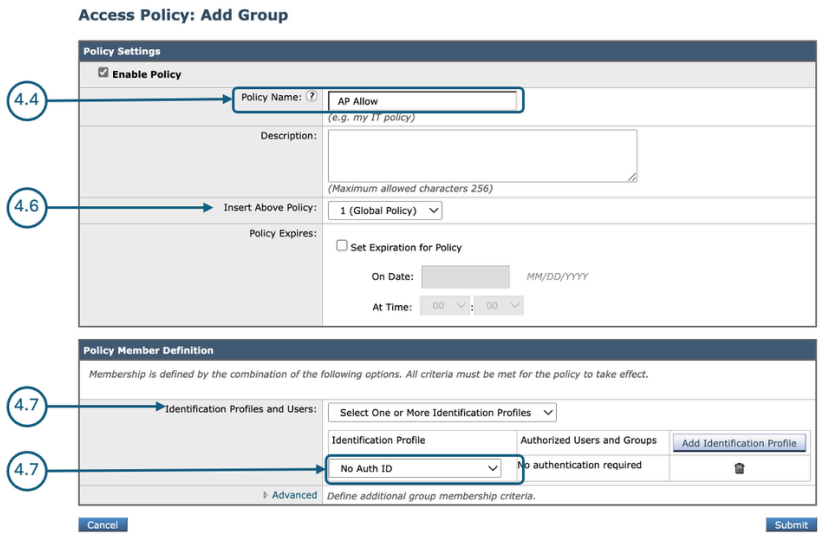


Image - Créer une stratégie d'accès

Étape 4.9. Sur la page Access Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie d'accès.

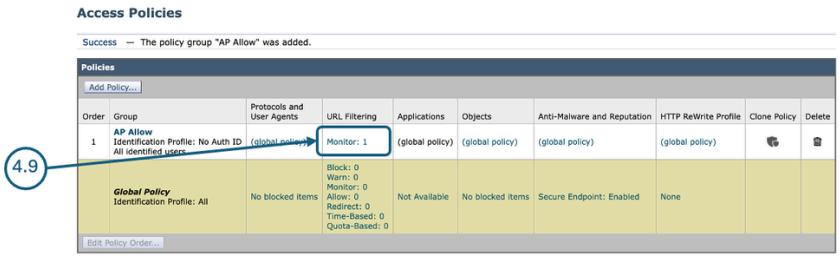


Image - Sélectionner le filtrage des URL

Étape 4.10. Sélectionnez Autoriser comme action pour la catégorie d'URL personnalisée créée pour la catégorie d'URL créée à l'étape 1.

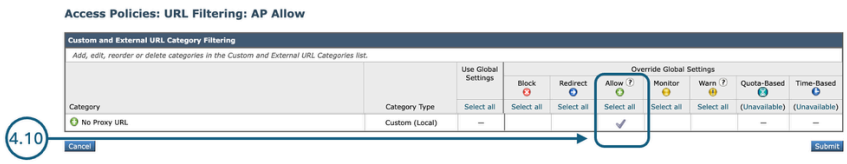


Image - Définir l'action sur Autoriser

Étape 4.11. Envoyer.

Étape 4.12. Valider les modifications

Autres informations utiles

- Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée
- Contourner l'authentification dans l'appliance Web sécurisée
- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - GD(General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance]
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance
- Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA)
- Utilisation des meilleures pratiques de sécurisation des appliances Web
- Bloquer le trafic dans l'appliance Web sécurisée
- Bloquer le trafic de téléchargement dans l'appliance Web sécurisée
- Bloquer le téléchargement de fichiers exécutables dans SWA

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.