Configurer la requête de plage pour le trafic Microsoft Update dans SWA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Demande de plage

Requête de plage dans l'environnement proxy

Activation de la demande de plage pour les mises à jour Microsoft

Étapes d'activation de la demande de plage uniquement pour les mises à jour Microsoft

- Étape 1 : activation de la demande de plage
- Étape 2 : création d'une catégorie d'URL personnalisée pour les URL Microsoft Updates
- Étape 3. (Facultatif) Créez un profil d'identification pour exempter le trafic des mises à jour Microsoft de l'authentification
- Étape 4. (Facultatif) Créez une stratégie de déchiffrement pour transmettre le trafic des mises à jour Microsoft
- Étape 5. Créer une stratégie d'accès pour autoriser le trafic de demandes de plage pour les mises à jour Microsoft

Modifier les journaux d'accès

Vérification

Autres informations utiles

Introduction

Ce document décrit les étapes pour permettre au trafic des mises à jour Microsoft d'utiliser la demande de plage dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA

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.

Demande de plage

Une requête de plage est une fonctionnalité d'un protocole HTTP qui permet à un client (tel qu'un navigateur Web ou un gestionnaire de téléchargement) de demander uniquement une partie spécifique d'un fichier à un serveur, plutôt que de télécharger le fichier entier en une seule fois. Cela est utile pour reprendre les téléchargements interrompus, la diffusion multimédia en continu ou l'accès efficace à des fichiers volumineux. Un client spécifie la plage d'octets souhaitée dans l'en-tête Range de la requête HTTP, et le serveur répond avec un code d'état de contenu partiel 206 s'il prend en charge les requêtes de plage, en ne remettant que le segment demandé du fichier.

Ce mécanisme améliore les performances et l'expérience utilisateur dans plusieurs scénarios. Par exemple, dans le cas de la lecture vidéo en continu, une requête de plage permet à un lecteur de n'extraire que les segments nécessaires à la lecture, ce qui réduit l'utilisation de la bande passante et améliore la réactivité. De même, les gestionnaires de téléchargement utilisent les demandes de plage pour fractionner un fichier en blocs et les télécharger en parallèle, accélérant ainsi le processus. Les requêtes de plage jouent également un rôle clé dans la mise en cache et les systèmes proxy, permettant des mises à jour partielles et réduisant les transferts de données redondants.

Requête de plage dans l'environnement proxy

Dans un environnement de proxy, les requêtes de plage jouent un rôle crucial dans l'optimisation de l'utilisation de la bande passante et l'amélioration de l'efficacité de la diffusion de contenu. Lorsque les requêtes de plage sont activées, le serveur proxy ne peut récupérer que les segments d'octets requis à partir du serveur d'origine et les mettre en cache localement. Cela permet aux clients de demander du contenu partiel, tel que des segments spécifiques d'une vidéo ou un fichier volumineux, et de le recevoir rapidement à partir du cache proxy, le cas échéant. Il permet également des téléchargements et des reprises en parallèle, ce qui est avantageux dans les environnements à bande passante limitée ou à latence élevée.

Cependant, quand les requêtes de plage sont désactivées, le proxy doit récupérer le fichier entier à partir du serveur d'origine même si le client n'a besoin que d'une petite partie. Cela entraîne un transfert de données inutile, une charge accrue sur les serveurs proxy et d'origine et des temps de réponse plus lents pour les clients. Elle empêche également les stratégies de mise en cache efficaces, car le proxy ne peut pas stocker ou servir du contenu partiel. Dans les scénarios de diffusion en continu, cela peut entraîner des délais de mise en mémoire tampon ou une dégradation de l'expérience utilisateur. La désactivation des demandes de plage peut être effectuée pour des raisons de sécurité ou de stratégie, mais elle s'effectue souvent au détriment des performances et de la flexibilité.

Prenons l'exemple d'un scénario dans lequel 10 utilisateurs tentent de télécharger 1 Mo chacun à partir d'un fichier de 100 Mo via un serveur proxy.

Demandes de plage désactivées :

- Lorsque les requêtes de plage sont désactivées, le proxy ne peut pas extraire uniquement le segment de 1 Mo dont chaque utilisateur a besoin. Au lieu de cela, il doit télécharger l'intégralité du fichier de 100 Mo à partir du serveur d'origine pour chaque requête. Cela se traduit par :
    - Trafic total de l'origine au proxy : 10 × 100 Mo = 1 000 Mo (1 Go)
    - Seuls 10 Mo de ces données sont utilisés par les clients.
    - Les 990 Mo restants sont gaspillés, ce qui entraîne une utilisation inefficace de la bande passante et une charge accrue sur les serveurs proxy et d'origine.

Demandes de plage activées :

- Lorsque les demandes de plage sont activées, le proxy récupère uniquement le 1 Mo demandé par utilisateur :
    - Trafic total de l'origine au proxy : 10 × 1 Mo = 10 Mo
    - Le proxy peut mettre en cache ces segments et les servir à d'autres utilisateurs si nécessaire.
    - Cela permet de réduire le trafic de 90 fois, d'accélérer les temps de réponse et d'améliorer considérablement l'utilisation des ressources.

Activation de la demande de plage pour les mises à jour Microsoft

Bien que les requêtes de plage améliorent les performances, elles entravent l'analyse de la sécurité et l'application des stratégies dans les environnements SWA, car ces systèmes ne peuvent pas inspecter entièrement le contenu partiel. Cet article limite l'utilisation des demandes de plage au trafic Microsoft Update uniquement.

⚠ Attention : l'activation du transfert de requête de plage peut interférer avec l'efficacité de la visibilité et du contrôle des applications (AVC) basée sur des stratégies et peut compromettre la sécurité.

Étapes d'activation de la demande de plage uniquement pour les mises à jour Microsoft

<table>
<tr>
<td>Étape 1 : activation de la demande de plage</td>
<td>Étape 1.1. Dans l’interface utilisateur graphique, cliquez sur Security Services et sélectionnez Web Proxy.

Étape 1.2. Cliquez sur Edit Settings.

Étape 1.3. Cochez la case Enable Range Request Forwarding.

Étape 1.4. Cliquez sur Submit.

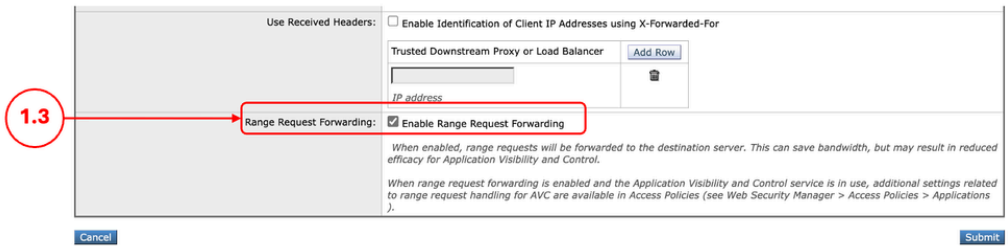


Image - Activer le transfert de requête de plage</td>
</tr>
<tr>
<td>Étape 2 : création d'une catégorie d'URL personnalisée pour les URL Microsoft Updates</td>
<td>Étape 2.1. Dans l’interface graphique, sélectionnez Web Security Manager, puis cliquez sur Custom and External URL Categories.
Étape 2.2. Cliquez sur Ajouter une catégorie pour ajouter une catégorie d'URL personnalisée.
Étape 2.3. Attribuer un nom de catégorie unique.
Étape 2.4. (Facultatif) Ajoutez une description.

Étape 2.5. Dans Ordre des listes, choisissez la première catégorie sur</td>
</tr>
</table>

laquelle vous souhaitez vous positionner.

Étape 2.6. Dans la liste déroulante Type de catégorie, sélectionnez Catégorie personnalisée locale.

Étape 2.7. Ajouter des URL de mises à jour Microsoft dans la section Sites.

Conseil : Vous pouvez consulter la liste des mises à jour Microsoft à partir de ce lien : Étape 2 - Configurez WSUS | Microsoft Learn

Mise en garde : Ne copiez/collez pas les URL telles qu'elles sont répertoriées dans les documents Microsoft ; formatez-les correctement en tant que format SWA. Pour plus d'informations, consultez Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco

Voici un exemple :

```
http://windowsupdate.microsoft.com    ===>  windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com  ===>  .windowsupdate.microsoft.com
```

Étape 2.8. Cliquez sur Submit.

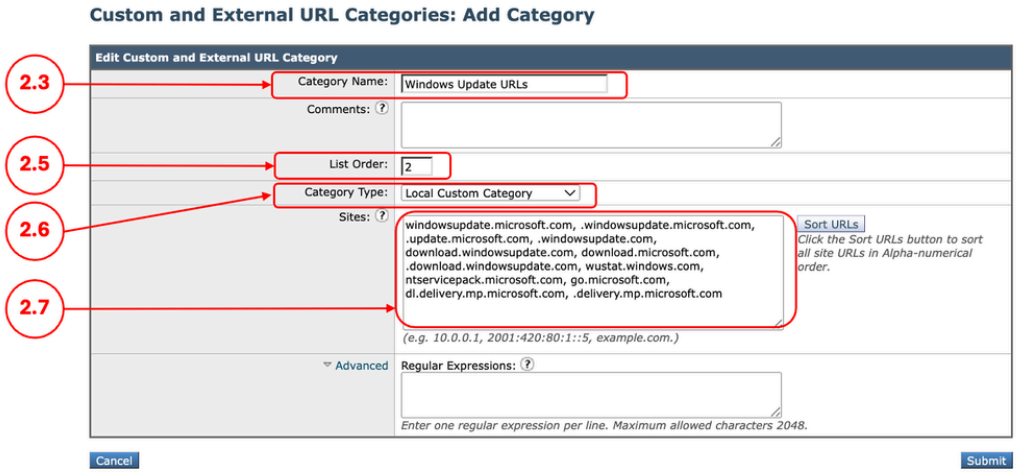


Image - Créer une catégorie d'URL personnalisée

Étape 3. (Facultatif) Créez un profil d'identification pour exempter le trafic des mises à jour Microsoft de l'authentification	Étape 3.1. Dans l’interface utilisateur graphique, sélectionnez Web Security Manager, puis cliquez sur Identification Profiles. Étape 3.2. Cliquez sur Add Profile pour ajouter un profil. Étape 3.3. Assurez-vous que la case à cocher Activer le profil d'identification est activée. Étape 3.4. Attribution d'un nom de profil unique. Étape 3.5. (Facultatif) Ajoutez une description. Étape 3.6. Dans la liste déroulante Insérer au-dessus, choisissez l'emplacement de ce profil dans le tableau.
Remarque : Cette action permet de réduire la charge d'authentification sur le SWA pour le trafic vers les mises à jour Microsoft.	Étape 3.7. Dans la section User Identification Method, choisissez Exempt from authentication/ identification. Étape 3.8. Dans le champ Define Members by Subnet (Définir les membres par sous-réseau), si vous voulez transmettre le trafic Microsoft pour des utilisateurs spécifiques, entrez les adresses IP ou les sous-réseaux qui s'appliquent, ou laissez ce champ vide pour inclure toutes les adresses IP. Étape 3.9. Dans la section Advanced, sélectionnez Custom URL Categories. Étape 3.10. Ajoutez la catégorie d'URL personnalisée créée pour les mises à jour Microsoft. Étape 3.11. Cliquez sur Terminé. Étape 3.12. Cliquez sur Submit.

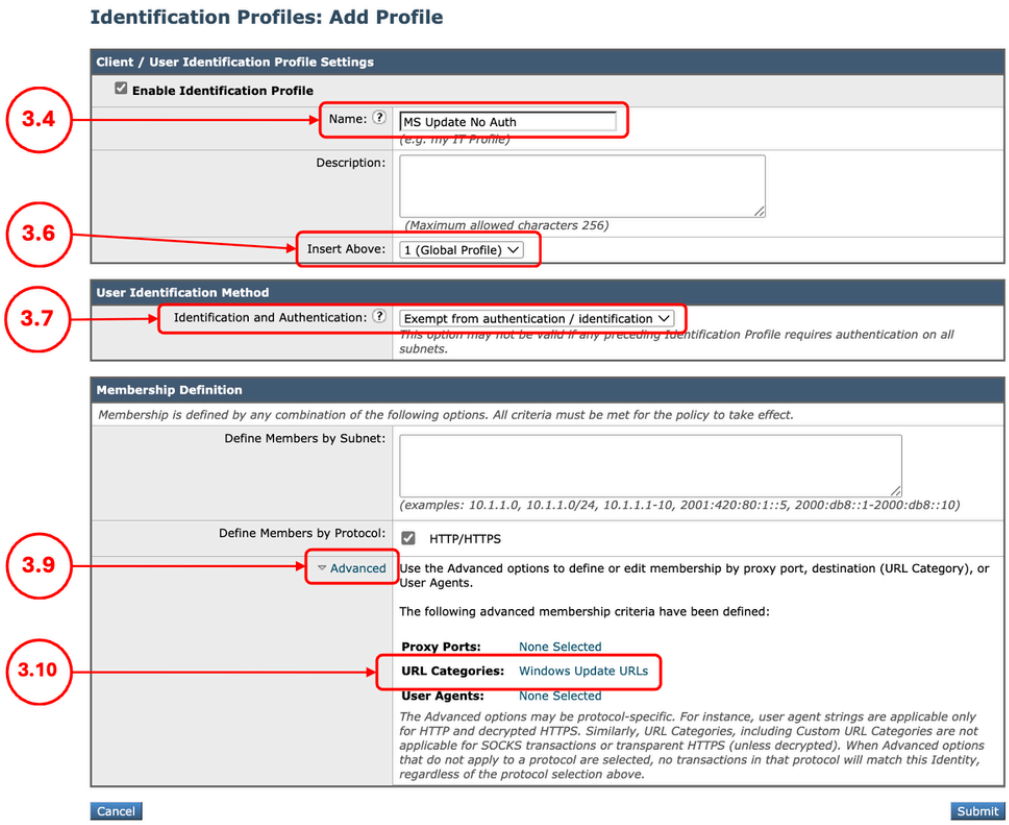


Image - Créer un profil d'identification

Étape 4. (Facultatif) Créez une stratégie de déchiffrement pour transmettre le trafic des mises à jour Microsoft

Remarque : Les mises à jour Microsoft utilisent le trafic HTTP et HTTPS pour fournir des liaisons de mise à jour. Cette action a réduit la charge de déchiffrement sur le SWA.

Étape 4.1. Dans l'interface utilisateur graphique, sélectionnez Web Security Manager, puis cliquez sur Decryption Policy.

Étape 4.2. Cliquez sur Add Policy pour ajouter une stratégie de décodage.

Étape 4.3. Attribution d'un nom de stratégie unique.
Étape 4.4. (Facultatif) Ajoutez une description.
Étape 4.5. Dans la liste déroulante Insérer au-dessus de la stratégie, sélectionnez la première stratégie.

Étape 4.6. Dans la liste Profils d'identification et utilisateurs, sélectionnez Sélectionner un ou plusieurs profils d'identification.

Étape 4.7. Sélectionnez le profil d'identification que vous avez créé à l'étape 3 et passez à l'étape 4.11.

Étape 4.8. Si vous n'avez pas créé de profil d'ID pour les mises à jour Windows, dans la section Avancé, sélectionnez Catégories d'URL personnalisées.

Étape 4.9. Ajoutez la catégorie d'URL personnalisée qui a été créée pour les mises à jour Microsoft à l'étape 2.

Étape 4.10. Cliquez sur Done (Terminé).

Étape 4.11. Cliquez sur Submit.

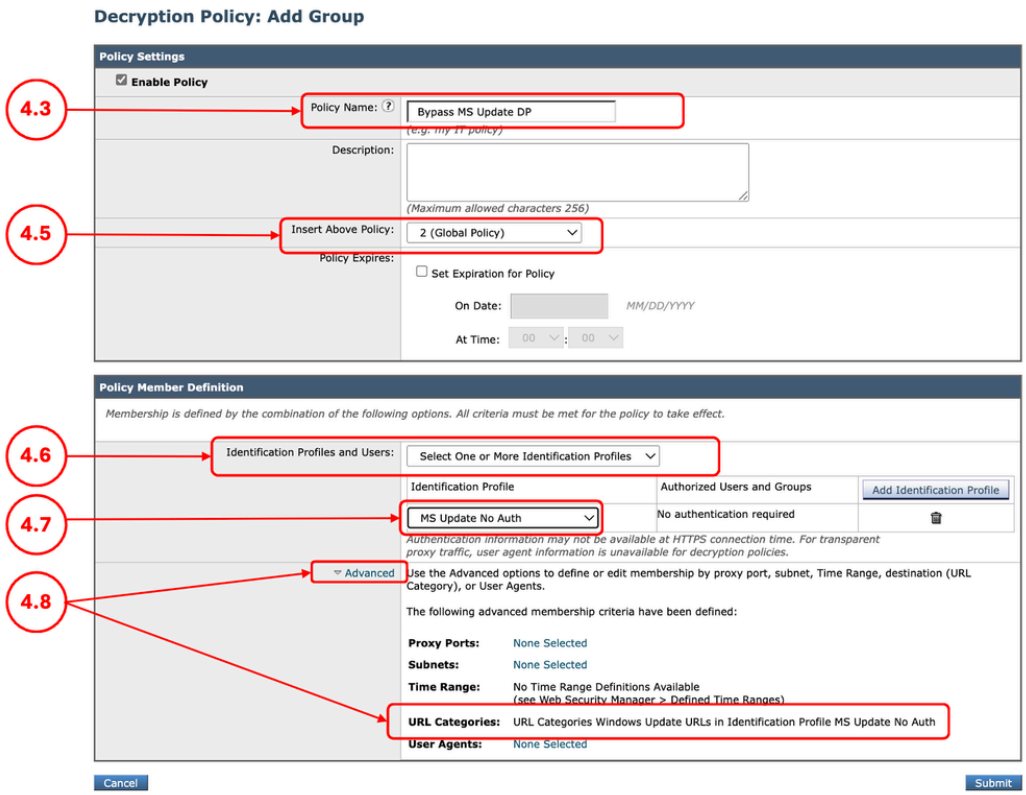


Image - Créer une stratégie de déchiffrement

Étape 4.12. Dans la page Decryption Policies sous URL Filtering, cliquez sur le lien associé à la nouvelle stratégie de décodage.

Étape 4.13. Sélectionnez Pass Through comme action pour la catégorie d'URL Mises à jour Microsoft.

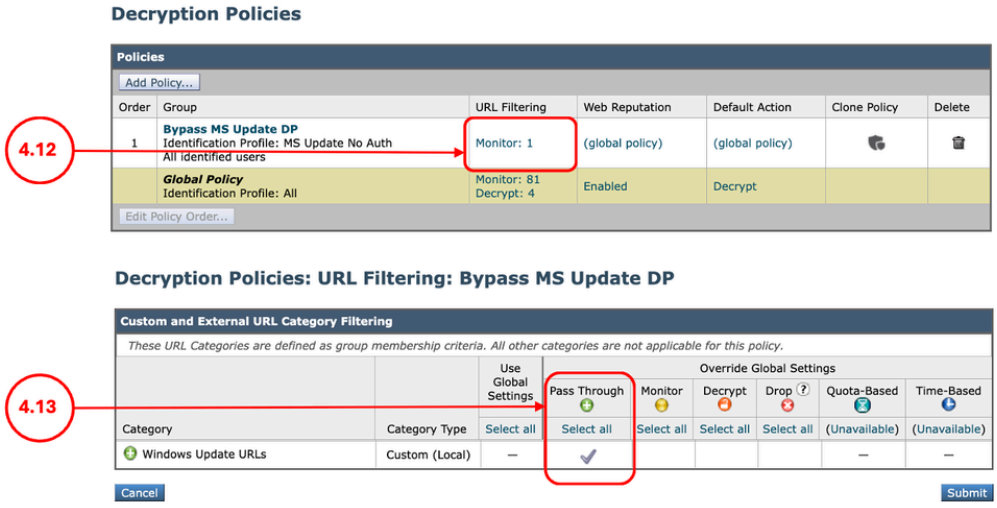


Image - Définir le Passthrough d'action pour la catégorie d'URL

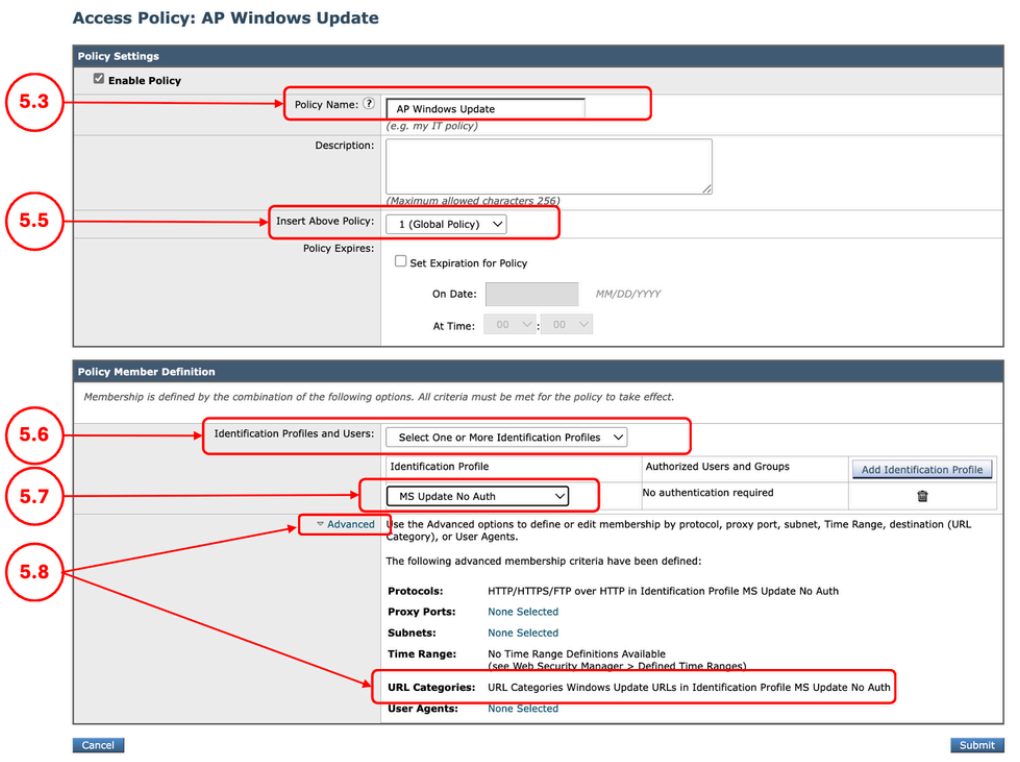
	Étape 4.14. Cliquez sur Submit.
Étape 5. Créer une stratégie d'accès pour autoriser le trafic de demandes de plage pour les mises à jour Microsoft	Étape 5.1. Dans l'interface utilisateur graphique, cliquez sur Web Security Manager et sélectionnez Access Policy. Étape 5.2. Cliquez sur Add Policy pour ajouter une stratégie d'accès. Étape 5.3. Attribution d'un nom de stratégie unique. Étape 5.4. (Facultatif) Ajoutez une description. Étape 5.5. Dans la liste déroulante Insérer au-dessus de la stratégie, sélectionnez la première stratégie. Étape 5.6. Dans la liste Profils d'identification et utilisateurs, sélectionnez Sélectionner un ou plusieurs profils d'identification. Étape 5.7. Sélectionnez le profil d'identification créé à l'étape 3, puis passez à l'étape 5.11. Étape 5.8. Si vous n'avez pas créé de profil d'ID pour Windows Update à partir de la section Avancé, choisissez Catégories d'URL personnalisées. Étape 5.9. Ajoutez la catégorie d'URL personnalisée qui a été créée pour les mises à jour Microsoft à l'étape 2. Étape 5.10. Cliquez sur Done (Terminé). Étape 5.11. Envoyer. 

Image - Créer la stratégie d'accès

Étape 5.12. Sur la page Access Policies sous URL Filtering, cliquez sur le lien associé à la nouvelle stratégie d'accès.

Étape 5.13. Sélectionnez Autoriser comme action pour la catégorie d'URL personnalisée créée pour les mises à jour Microsoft.

Étape 5.14. Cliquez sur Submit.

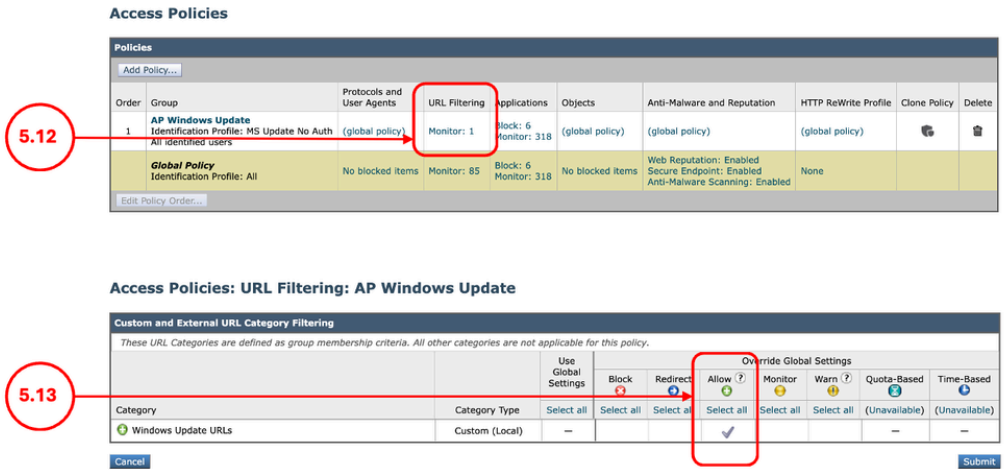


Image - Définir l'action Autoriser pour la catégorie d'URL

Étape 5.15. Sur la page Access Policies sous Applications, cliquez sur le lien associé à la nouvelle stratégie d'accès.

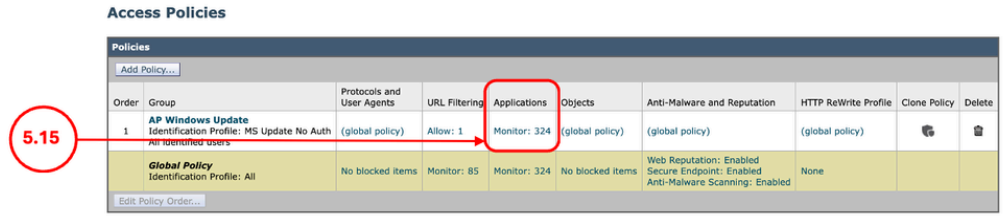


Image - Modifier la visibilité et le contrôle des applications

Étape 5.16. Dans la section Modifier les paramètres des applications, sélectionnez Définir les paramètres personnalisés des applications.

Étape 5.17. Dans la section Paramètres des applications, cliquez sur Modifier tout pour l'application Jeux, et définissez l'action sur Bloquer.

Étape 5.18. Cliquez sur Apply (appliquer).

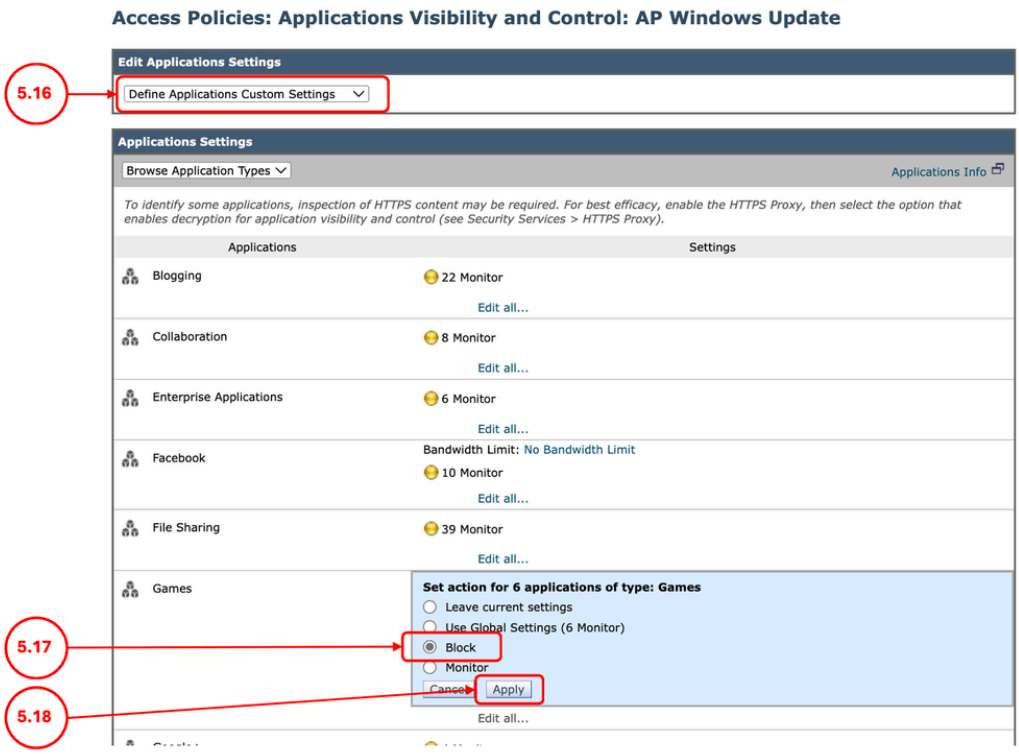


Image - Définir une action d'application à bloquer

Étape 5.19. Faites défiler jusqu'à la section Range Request Settings for Policy, assurez-vous que l'option Forward range Requests est sélectionnée.

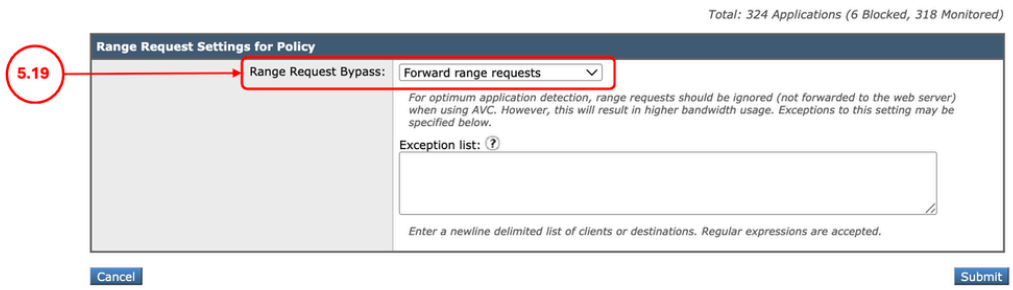


Image - Paramètres de demande de plage pour la stratégie

Étape 5.20. Cliquez sur Submit.

Étape 5.21. Sur la page Access Policies, sous Applications, cliquez sur le lien associé à la stratégie globale.

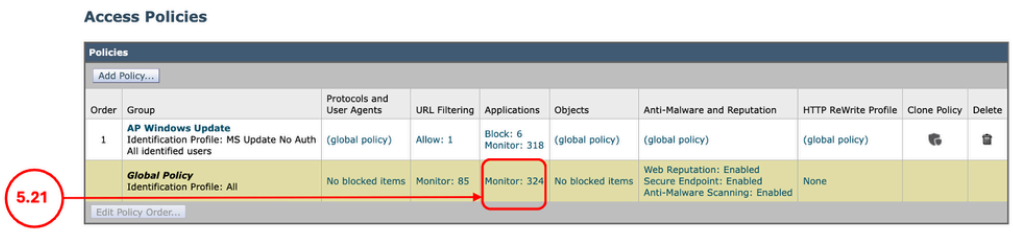


Image - Paramètres d'application de stratégie d'accès par défaut

Étape 5.22. Faites défiler jusqu'à la section Range Request Settings for Policy, assurez-vous que l'option Do Not Forward range Requests est sélectionnée,

Étape 5.23. Confirmer les modifications

Modifier les journaux d'accès

Pour plus de visibilité sur les demandes de plage des journaux d'accès, vous pouvez ajouter les champs personnalisés suivants :

[Plage du client = %<Plage :]	Affiche la plage, demandée par le client (octets)
[content= %>Longueur du contenu :]	Affiche la taille du contenu téléchargé (octets)

Pour plus d'informations sur l'ajout d'un champ personnalisé aux journaux d'accès SWA, référez-vous au guide Configurer le paramètre de performance dans les journaux d'accès.

Vérification

Exécutez cette commande CURL pour envoyer une requête de plage au SWA :

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

Dans le résultat de la CURL, vous pouvez voir la réponse HTTP est HTTP/1.1 206 :

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
```

```
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

Dans les journaux d'accès, vous pouvez voir l'action TCP_CLIENT_REFRESH_MISS/206 :

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

Autres informations utiles

- 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] - Cisco
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA) - Cisco
- Configurer le paramètre de performance dans les journaux d'accès
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco
- Contourner l'authentification dans l'appareil Web sécurisé - Cisco

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.