Configurer des catégories d'URL personnalisées dans Secure Web Appliance

Table des matières

Introduction

Ce document décrit la structure des catégories d'URL (Uniform Resource Locator) personnalisées dans Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fonctionnement du proxy.

- Administration sécurisée des appareils Web (SWA).

Cisco recommande que vous ayez :

- Appareil Web sécurisé physique ou virtuel (SWA) installé.
- Licence activée ou installée.
- L'Assistant de configuration est terminé.

- Accès administratif au 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.

Catégories d'URL personnalisées

Le moteur de filtrage des URL vous permet de filtrer les transactions dans les politiques d'accès, de décodage et de sécurité des données. Lorsque vous configurez des catégories d'URL pour des groupes de stratégies, vous pouvez configurer des actions pour des catégories d'URL personnalisées, le cas échéant, et des catégories d'URL prédéfinies.

Vous pouvez créer des catégories d'URL de flux en direct personnalisées et externes qui décrivent des noms d'hôte spécifiques et des adresses IP (Internet Protocol). En outre, vous pouvez modifier et supprimer des catégories d'URL.

Lorsque vous incluez ces catégories d'URL personnalisées dans le même groupe Access, Decryption ou Cisco Data Security Policy et que vous affectez des actions différentes à chaque catégorie, l'action de la catégorie d'URL personnalisée incluse la plus élevée est prioritaire.

Remarque : si le système de noms de domaine (DNS) résout plusieurs adresses IP sur un site Web et si l'une de ces adresses IP est une liste de blocage personnalisée, l'appliance de sécurité Web bloque le site Web pour toutes les adresses IP, qu'elles ne figurent pas dans la liste de blocage personnalisée.

Catégories d'URL de flux en direct

Les catégories de flux en direct externes sont utilisées pour extraire la liste des URL d'un site spécifique, par exemple pour extraire les URL Office 365 de Microsoft.

Si vous sélectionnez Catégorie de flux en direct externe pour le type de catégorie lors de la création et de la modification de catégories d'URL personnalisées et externes, vous devez sélectionner le format de flux (Format de flux Cisco ou Format de flux Office 365), puis fournir une

URL au serveur de fichiers de flux approprié.
Voici le format attendu pour chaque fichier de flux :

- Format de flux Cisco : il doit s'agir d'un fichier de valeurs séparées par des virgules (.csv), c'est-à-dire d'un fichier texte portant l'extension .csv. Chaque entrée du fichier .csv doit se trouver sur une ligne distincte, formatée comme adresse/virgule/type d'adresse (par exemple : www.cisco.com,site ou ad2.*\.com,regex). Les types d'adresse valides sont site et regex.

Voici un extrait d'un fichier .csv au format de flux Cisco :

```
www.cisco.com,site
\.xyz,regex
ad2.*\.com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Format de flux Office 365 : fichier XML situé sur un serveur Microsoft Office 365 ou sur un serveur local sur lequel vous avez enregistré le fichier. Il est fourni par le service Office 365 et ne peut pas être modifié.

Les adresses réseau dans le fichier sont entourées de balises XML, cette structure : products > product > address list > address. Dans l'implémentation actuelle, un « type de liste d'adresses » peut être IPv6, IPv4 ou URL [qui peut inclure des modèles de domaines et d'expressions régulières (regex)].

Voici un extrait d'un fichier de flux Office 365 :

```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
```

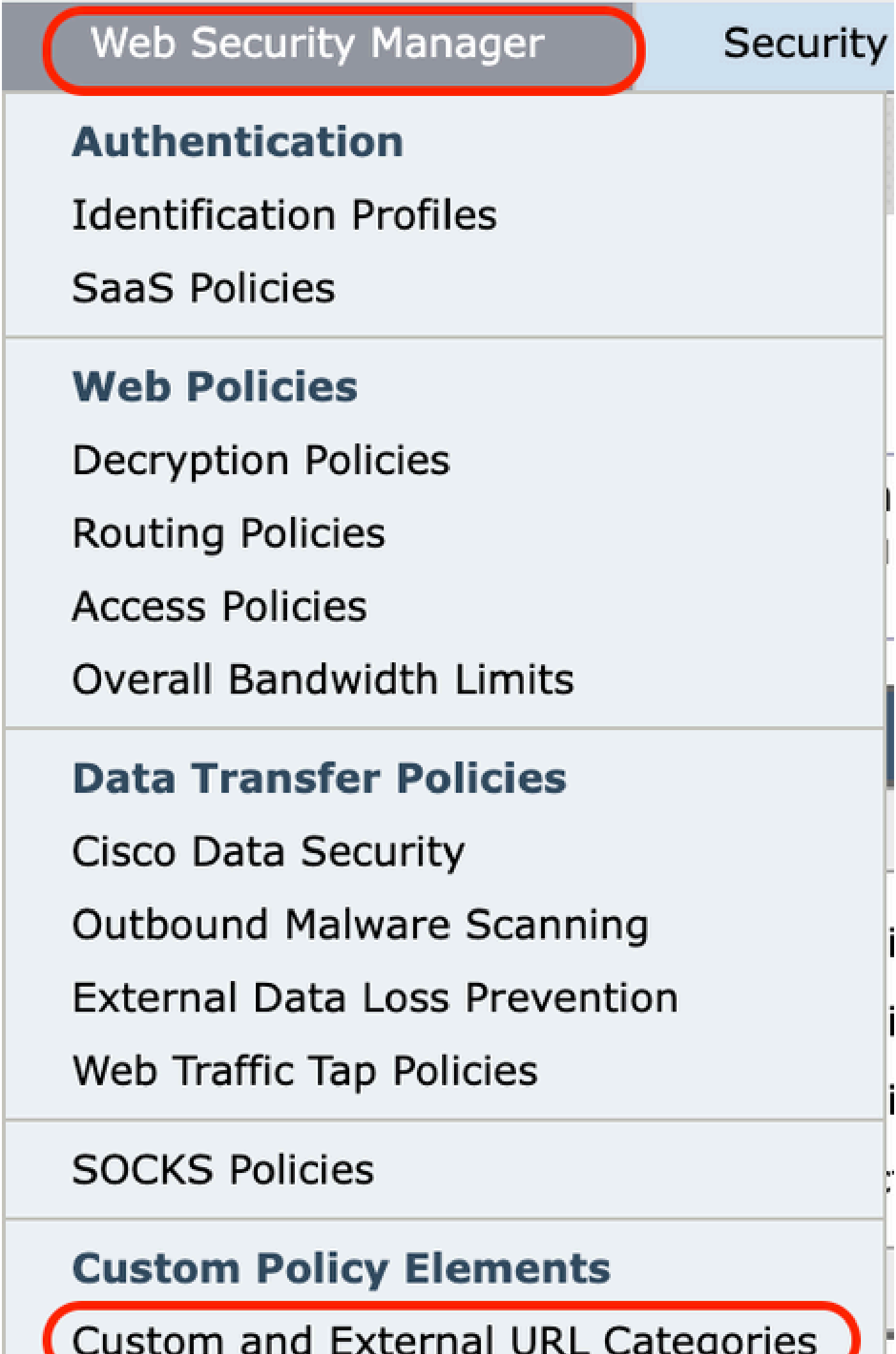
```
</product>
</products>
```

Remarque : n'incluez pas http:// ou https:// dans une entrée de site du fichier, sinon une erreur se produira. En d'autres termes, www.cisco.com est analysé correctement, tandis que http://www.cisco.com produit une erreur

---

Étapes de création de catégories d'URL personnalisées

Étape 1. Choisissez Gestionnaire de sécurité Web > Catégories d'URL personnalisées et externes.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

: saisissez un identifiant pour cette catégorie d'URL. Ce nom apparaît lorsque vous configurez le filtre d'URL pour les groupes de stratégies.

- List Order : spécifiez l'ordre de cette catégorie dans la liste des catégories d'URL personnalisées. Entrez « 1 » pour la première catégorie d'URL de la liste.
  Le moteur de filtre d'URL évalue une requête client par rapport aux catégories d'URL personnalisées dans l'ordre spécifié.

Remarque : lorsque le moteur de filtre d'URL fait correspondre une catégorie d'URL à l'URL d'une demande client, il évalue d'abord l'URL par rapport aux catégories d'URL personnalisées incluses dans le groupe de stratégies. Si l'URL de la demande ne correspond pas à une catégorie personnalisée incluse, le moteur de filtrage d'URL la compare aux catégories d'URL prédéfinies. Si l'URL ne correspond à aucune catégorie d'URL personnalisée ou prédéfinie, la demande n'est pas classée.

- Type de catégorie : choisissez Catégorie personnalisée locale ou Catégorie de flux en direct externe.
- Table de routage : choisissez Gestion ou Données. Ce choix n'est disponible que si le « routage partagé » est activé, c'est-à-dire qu'il n'est pas disponible avec les catégories personnalisées locales.

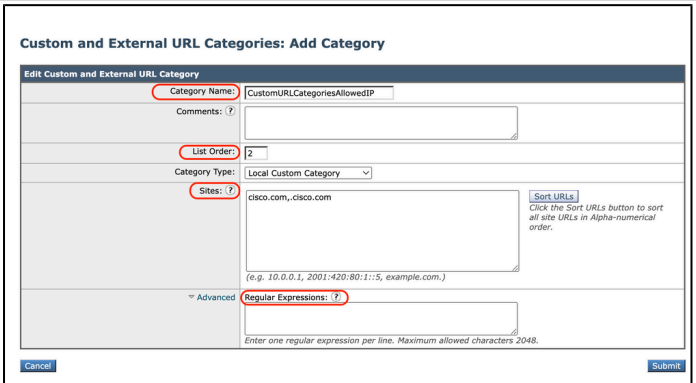
<table>
<tr>
<td> 

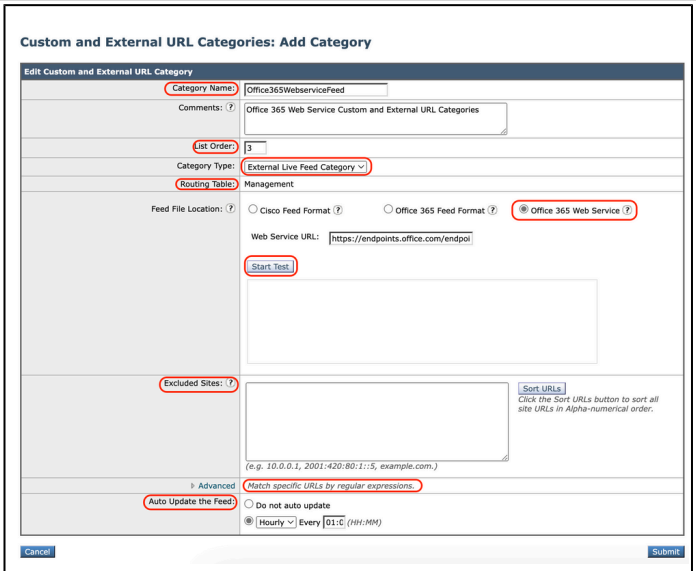
image - Catégorie d'URL personnalisée locale</td>
<td> 

Image - Catégorie d'URL personnalisée configurer les flux</td>
</tr>
<tr>
<td>Catégorie personnalisée locale</td>
<td>Catégorie de flux dynamique externe</td>
</tr>
</table>

Définir Utiliser des expressions régulières

Secure Web Appliance utilise une syntaxe d'expression régulière qui diffère légèrement de celle utilisée par d'autres implémentations de moteur de mise en correspondance de modèles Velocity.

En outre, l'appareil ne prend pas en charge de barre oblique inverse pour échapper à une barre oblique inverse. Si vous devez utiliser une barre oblique dans une expression régulière, tapez simplement la barre oblique sans barre oblique inverse.

Remarque : techniquement, AsyncOS for Web utilise l'analyseur d'expression régulière Flex

Pour tester vos expressions régulières, vous pouvez utiliser ce lien : flex lint - Regex Tester/Debugger

Attention : les expressions régulières qui renvoient plus de 63 caractères échouent et génèrent une erreur d'entrée non valide. Assurez-vous de former des expressions régulières qui ne peuvent pas renvoyer plus de 63 caractères

Attention : les expressions régulières qui effectuent des correspondances de caractères étendues consomment des ressources et peuvent affecter les performances du système. Pour cette raison, les expressions régulières peuvent être appliquées avec prudence.

Vous pouvez utiliser des expressions régulières à ces emplacements :
· Catégories d'URL personnalisées pour les politiques d'accès. Lorsque vous créez une catégorie d'URL personnalisée à utiliser avec des groupes de stratégie d'accès, vous pouvez utiliser des expressions régulières pour spécifier plusieurs serveurs Web qui correspondent au modèle que vous entrez.
· Agents utilisateurs personnalisés à bloquer. Lorsque vous modifiez les applications à bloquer pour un groupe de stratégie d'accès, vous pouvez utiliser des expressions régulières pour entrer des agents utilisateur spécifiques à bloquer.

Conseil : vous ne pouvez pas définir le contournement du proxy Web pour les expressions régulières.

Voici la liste des classes de caractères dans l'expression régulière Flex

Classes de caractères	
.	tout caractère sauf nouvelle ligne
\w \d \s	mot, chiffre, espace blanc
\W \D \S	pas mot, chiffre, espace blanc
[abc]	a, b ou c, le cas échéant
[^abc]	pas a, b ou c
[a-g]	caractère compris entre a et g
Ancres	
^abc$	début / fin de la chaîne
\b	limite de mot
Caractères échappés	
\. * \\	caractères spéciaux avec échappement
\t \n \r	tabulation, saut de ligne, retour chariot
\u00A9	échappement unicode ©

Groupes et recherche	
(abc)	groupe cible
\1	référence arrière au groupe #1
(?:abc)	groupe des Etats non producteurs
(?=abc)	anticipation positive
(?!abc)	anticipation négative
Quantificateurs et alternance	
a* a+ a ?	0 ou plus, 1 ou plus, 0 ou 1
a{5} a{2,}	exactement cinq, deux ou plus
a{1,3}	entre une et trois
a+? a{2,} ?	correspondre le moins possible
ab|cd	match ab ou cd

⚠ Attention : Méfiez-vous des points non échappés dans les motifs longs, et surtout au milieu des motifs plus longs et Méfiez-vous de ce méta-caractère (étoile *), surtout en conjonction avec le caractère de point. Tout modèle contient un point sans échappement qui renvoie plus de 63 caractères après la désactivation du point.
Toujours échapper *(étoile) et . (point) avec \ (barre oblique inverse) comme * et \.
Si nous utilisons .cisco.local dans l'expression régulière, le domaine Xcisco.local est également une correspondance.
Le caractère non échappé affecte les performances et il crée une lenteur pendant la navigation sur le Web. C'est parce que le moteur de correspondance de modèle doit passer par des milliers ou des millions de possibilités jusqu'à trouver une correspondance pour l'entrée correcte aussi il peut avoir quelques préoccupations de sécurité en ce qui concerne les URL similaires pour les politiques autorisées

Vous pouvez utiliser l'option de l'interface de ligne de commande (CLI) advanced proxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex, pour activer ou désactiver la conversion regex par défaut en minuscules pour les correspondances non sensibles à la casse. Utilisez cette option si vous rencontrez des problèmes de distinction majuscules/minuscules.

Limitations et problèmes de conception

- Vous ne pouvez pas utiliser plus de 30 fichiers de flux en direct externes dans ces définitions de catégorie d'URL et chaque fichier ne doit pas contenir plus de 5 000 entrées.
- Si le nombre d'entrées de flux externes augmente, cela entraîne une dégradation des performances.
- Il est possible d'utiliser la même adresse dans plusieurs catégories d'URL personnalisées, mais l'ordre dans lequel les catégories sont répertoriées est pertinent.

Si vous incluez ces catégories dans la même stratégie et définissez des actions différentes pour chacune d'elles, l'action définie pour la catégorie répertoriée en haut dans le tableau des

catégories d'URL personnalisées est appliquée.

- Lorsqu'une requête FTP (File Transfer Protocol) native est redirigée de manière transparente vers le proxy FTP, elle ne contient pas d'informations de nom d'hôte pour le serveur FTP, mais uniquement son adresse IP.

De ce fait, certaines catégories d'URL et certains filtres de réputation de sites Web prédéfinis qui ne contiennent que des informations de nom d'hôte ne correspondent pas aux requêtes FTP natives, même si les requêtes sont destinées à ces serveurs.

Si vous souhaitez bloquer l'accès à ces sites, vous devez créer des catégories d'URL personnalisées pour qu'ils puissent utiliser leurs adresses IP.

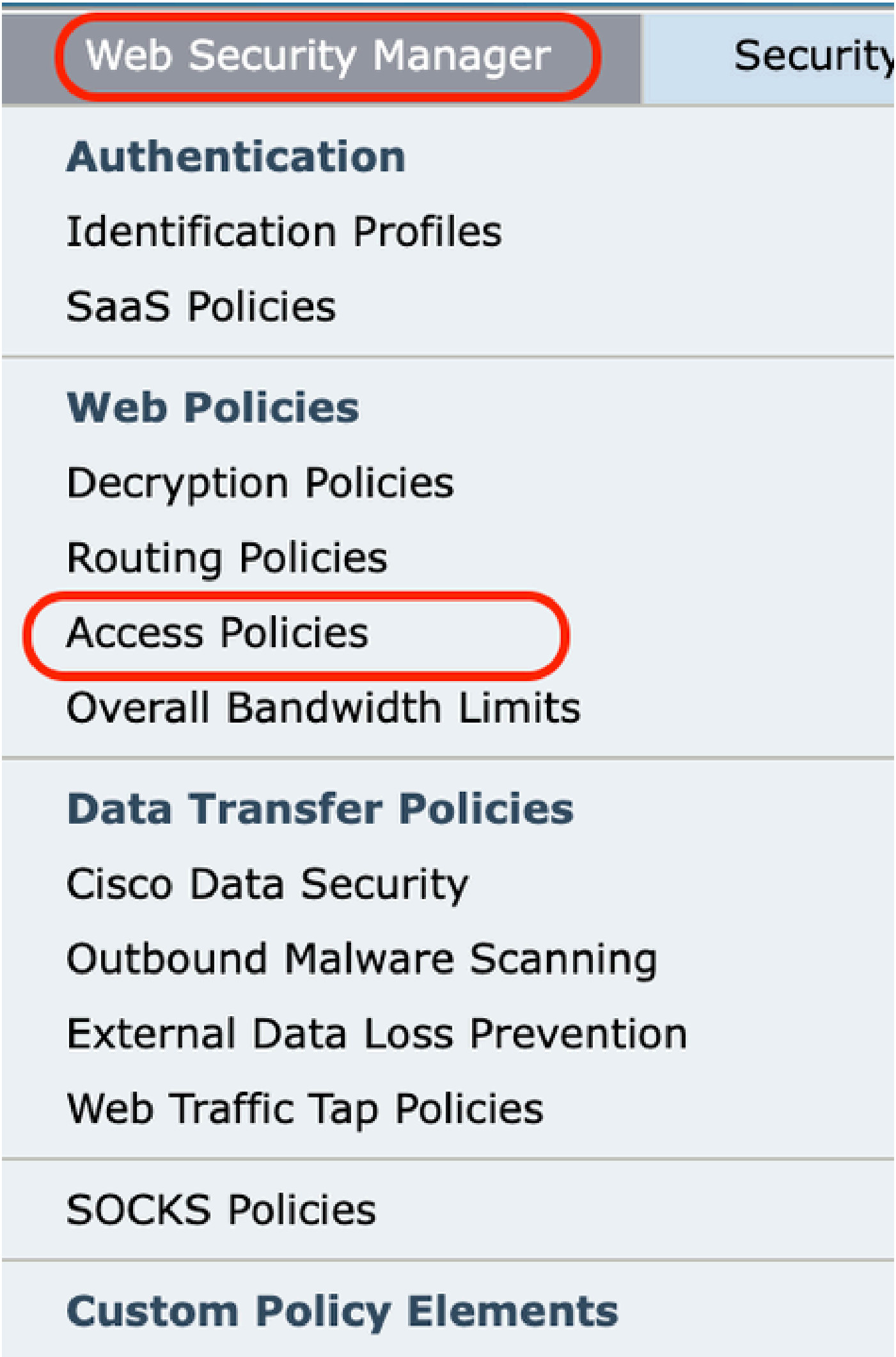
- Une URL non catégorisée est une URL qui ne correspond à aucune catégorie d'URL prédéfinie ou personnalisée incluse

Utiliser des catégories d'URL personnalisées dans les stratégies

Le moteur de filtrage des URL vous permet de filtrer les transactions dans les politiques d'accès, de décodage et de sécurité des données. Lorsque vous configurez des catégories d'URL pour des groupes de stratégies, vous pouvez configurer des actions pour des catégories d'URL personnalisées, le cas échéant, et des catégories d'URL prédéfinies.

Étapes de configuration des filtres URL pour la stratégie d'accès

Étape 1. Choisissez Gestionnaire de sécurité Web > Stratégies d'accès.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

Cliquez sur le lien dans le tableau des stratégies sous la colonne Filtre d'URL pour le groupe de stratégies que vous souhaitez modifier.

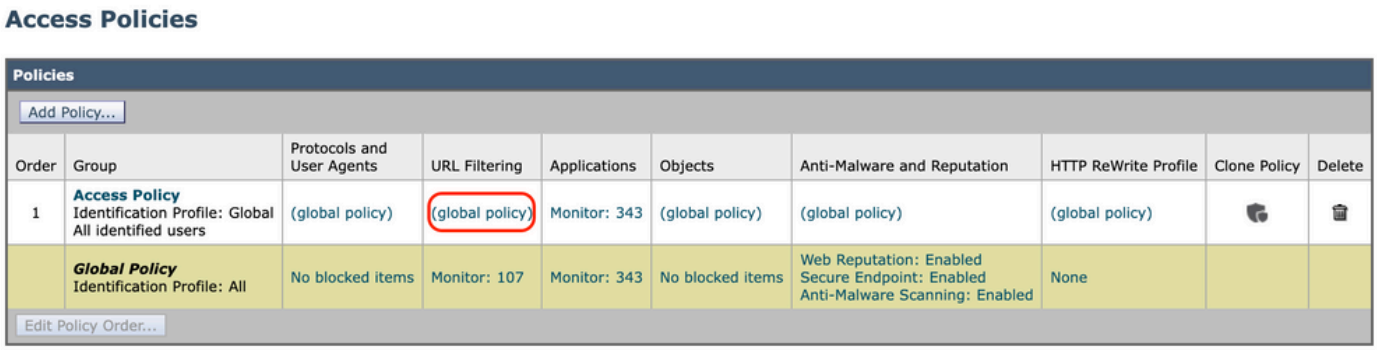


Image - Ajouter une catégorie personnalisée à la stratégie d'accès

Étape 3. (Facultatif) Dans la section Filtrage des catégories d'URL personnalisées, vous pouvez ajouter des catégories d'URL personnalisées sur lesquelles vous pouvez agir dans cette stratégie :

a) Cliquez sur Sélectionner des catégories personnalisées.

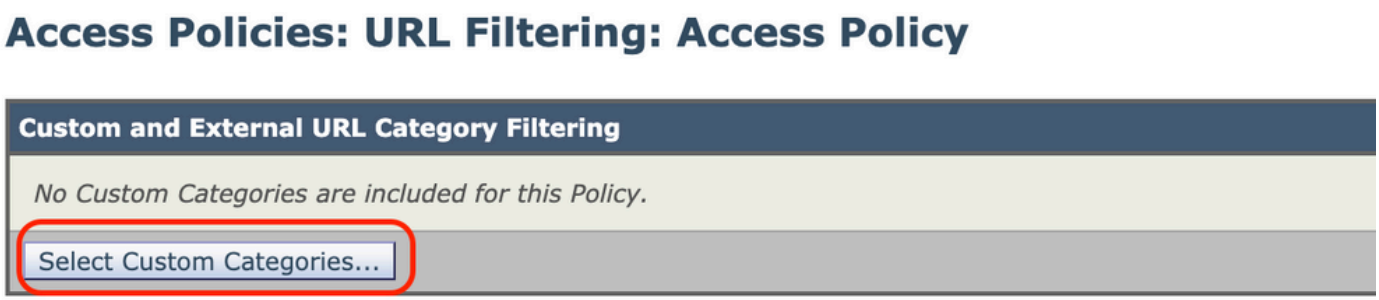


Image - Sélectionner une catégorie d'URL personnalisée

b) Choisissez les catégories d'URL personnalisées à inclure dans cette stratégie et cliquez sur Apply.

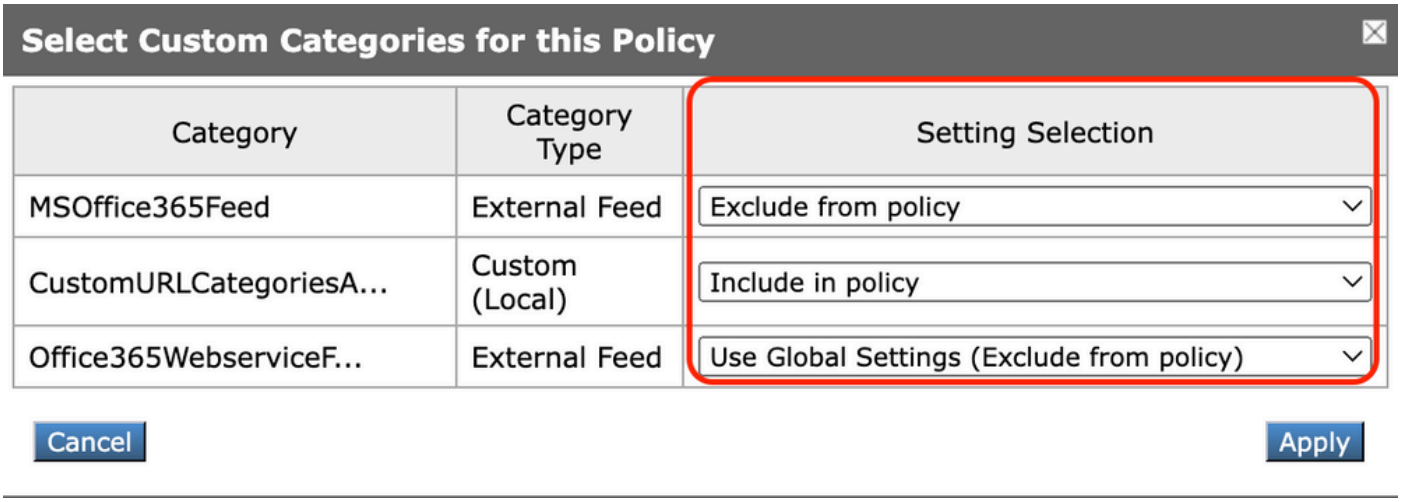


Image : sélectionnez les catégories personnalisées à inclure dans la stratégie

Choisissez les catégories d'URL personnalisées par rapport auxquelles le moteur de filtrage

d'URL doit comparer la demande du client.

Le moteur de filtre d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues.

Le moteur de filtre d'URL compare l'URL d'une requête client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la stratégie apparaissent dans la section Filtrage des catégories d'URL personnalisées.

Étape 4. Dans la section Filtrage personnalisé des catégories d'URL, sélectionnez une action pour chaque catégorie d'URL personnalisée incluse.

Image - Choisir une action pour la catégorie personnalisée

Action	Description
Utiliser les paramètres globaux	Utilise l'action pour cette catégorie dans le groupe de stratégies globales. Il s'agit de l'action par défaut pour les groupes de stratégies définis par l'utilisateur. S'applique uniquement aux groupes de stratégies définis par l'utilisateur.
Block	Le proxy Web refuse les transactions qui correspondent à ce paramètre.
Rediriger	Redirige le trafic destiné à l'origine à une URL de cette catégorie vers un emplacement que vous spécifiez. Lorsque vous choisissez cette action, le champ Rediriger vers s'affiche. Entrez une URL vers laquelle rediriger tout le trafic.
Allow	Autorise toujours les requêtes des clients pour les sites Web de cette catégorie. Les requêtes autorisées contournent tous les autres filtres et analyses de programmes malveillants. Utilisez ce paramètre uniquement pour les sites Web de confiance. Vous pouvez utiliser ce paramètre pour les sites internes.

Action	Description
Monitor	Le proxy Web n'autorise ni ne bloque la demande. Au lieu de cela, il continue à évaluer la demande du client par rapport à d'autres paramètres de contrôle de groupe de stratégies, tels que le filtre de réputation Web.
Avertir	Le proxy Web bloque initialement la demande et affiche une page d'avertissement, mais permet à l'utilisateur de continuer en cliquant sur un lien hypertexte dans la page d'avertissement.
Basé Sur Les Quotas	Un avertissement s'affiche lorsqu'un utilisateur se rapproche des quotas de volume ou de temps que vous avez spécifiés. Lorsqu'un quota est atteint, une page de blocage s'affiche. .
Basé sur le temps	Le proxy Web bloque ou surveille la demande pendant les intervalles de temps que vous spécifiez.

Étape 5. Dans la section Filtre de catégorie d'URL prédéfinie, sélectionnez l'une des actions suivantes pour chaque catégorie :

- Utiliser les paramètres globaux
- Monitor
- Avertir
- Block
- Basé sur le temps
- Basé Sur Les Quotas

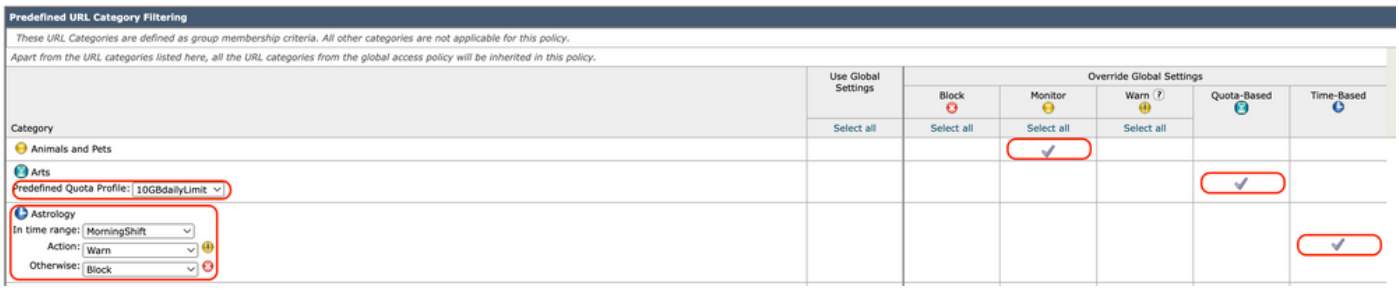


Image - Sélectionner une action pour la catégorie prédéfinie

Étape 6. Dans la section URL non classées, choisissez l'action à entreprendre pour les demandes de clients à des sites Web qui ne font pas partie d'une catégorie d'URL prédéfinie ou personnalisée. Ce paramètre détermine également l'action par défaut pour les catégories

nouvelles et fusionnées résultant des mises à jour du jeu de catégories d'URL.

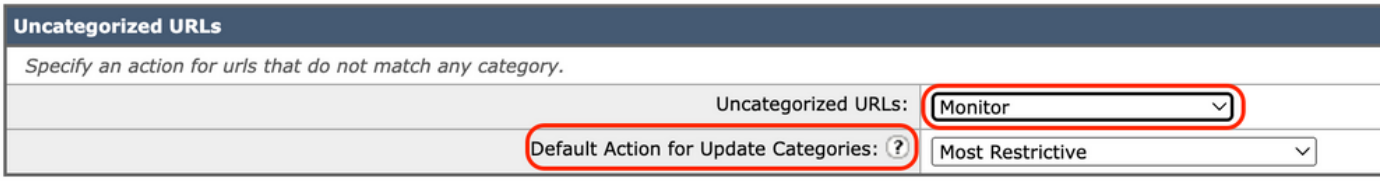
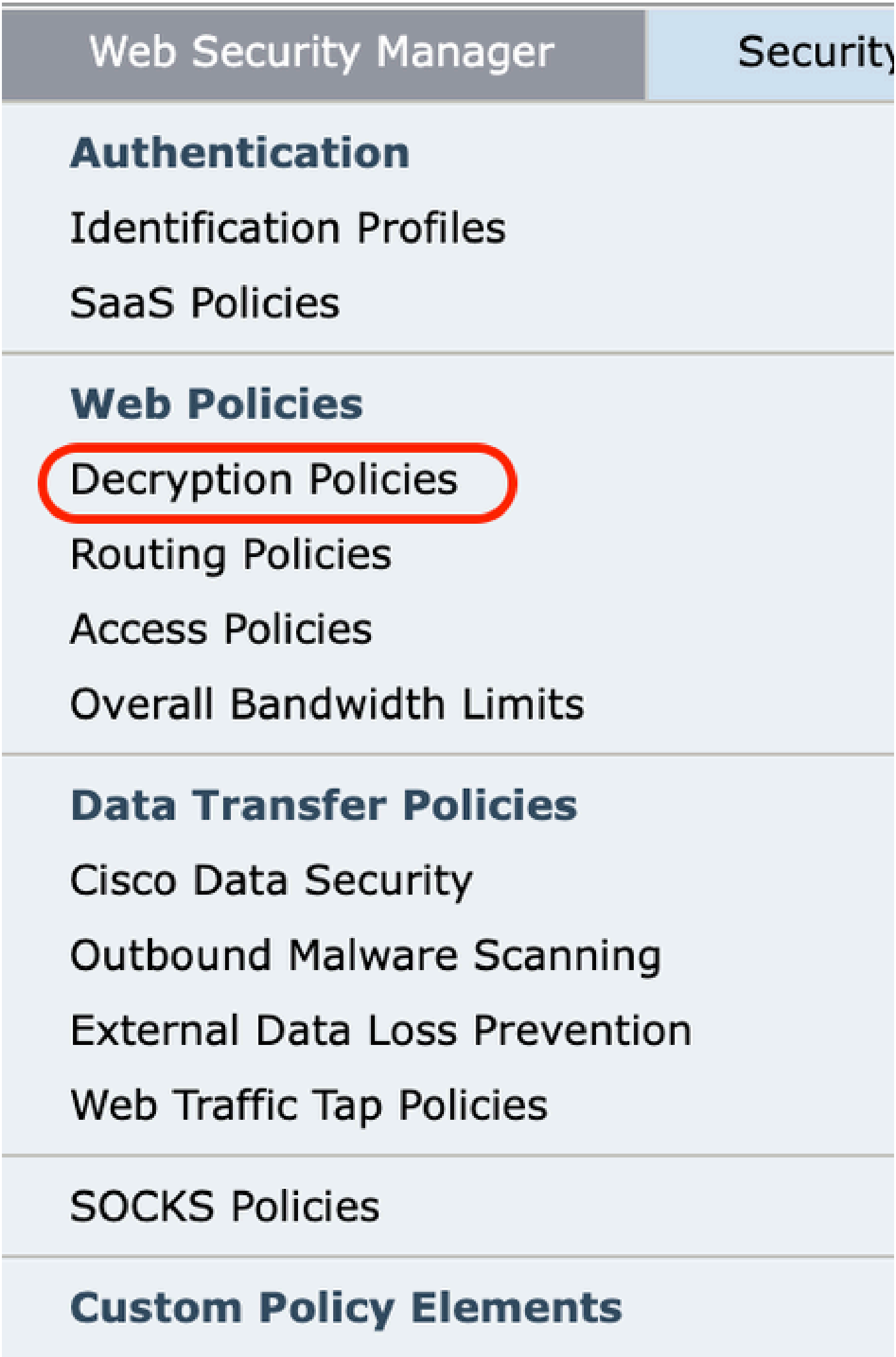


Image - Choisir une action pour l'URL non catégorisée

Étape 7. Soumettre et valider les modifications.

Étapes de configuration des filtres URL pour la stratégie de déchiffrement

Étape 1. Choisissez Web Security Manager > Decryption Policies.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

Cliquez sur le lien dans le tableau des stratégies sous la colonne Filtrage d'URL pour le groupe de stratégies que vous souhaitez modifier.

Image - Choisir un filtre d'URL

Étape 3. (Facultatif) Dans la section Filtrage des catégories d'URL personnalisées, vous pouvez ajouter des catégories d'URL personnalisées sur lesquelles vous devez agir dans cette stratégie :

a. Cliquez sur Sélectionner des catégories personnalisées.

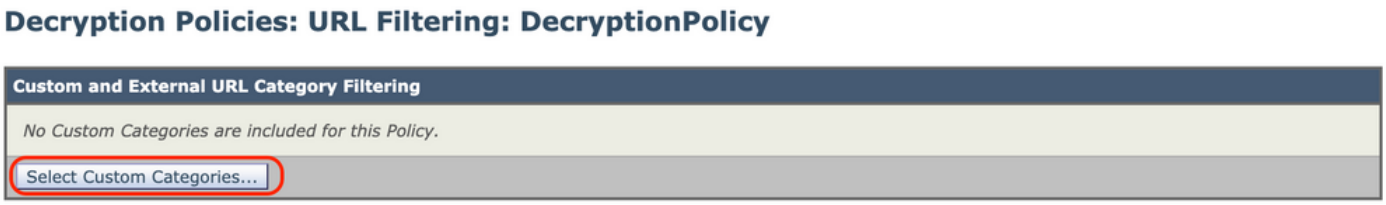


Image - Choisir des catégories personnalisées

b. Choisissez les catégories d'URL personnalisées à inclure dans cette stratégie et cliquez sur Apply.

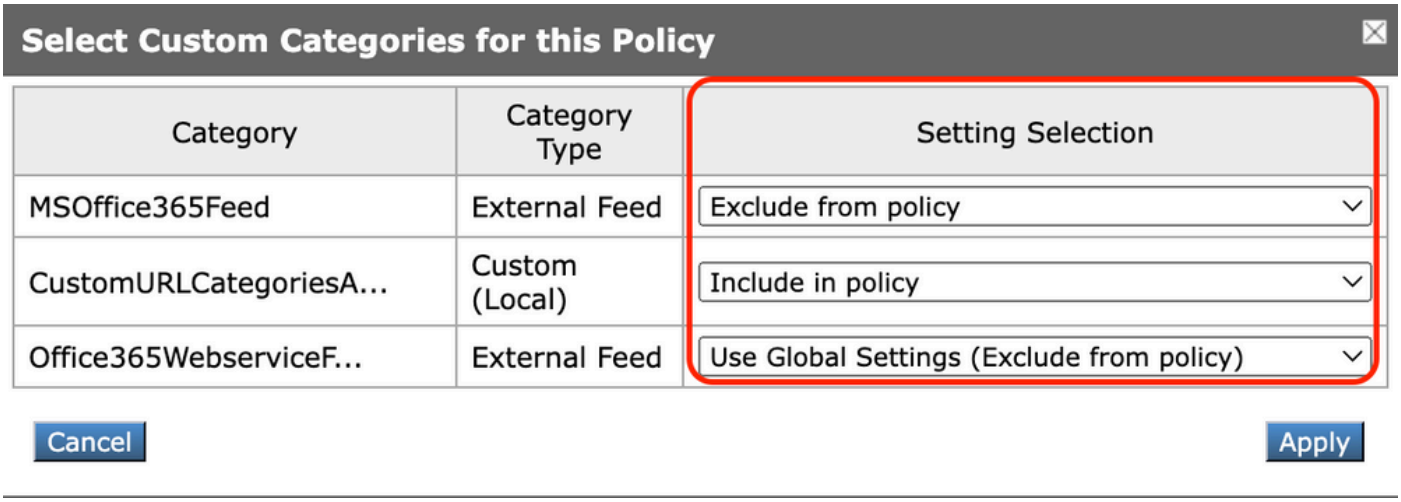


Image : sélectionnez les catégories personnalisées à inclure dans la stratégie

Choisissez les catégories d'URL personnalisées par rapport auxquelles le moteur de filtrage d'URL doit comparer la demande du client.

Le moteur de filtre d'URL compare les demandes des clients aux catégories d'URL personnalisées

incluses et ignore les catégories d'URL personnalisées exclues.

Le moteur de filtre d'URL compare l'URL d'une requête client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la stratégie apparaissent dans la section Filtrage des catégories d'URL personnalisées.

Étape 4. Choisissez une action pour chaque catégorie d'URL personnalisée et prédéfinie.

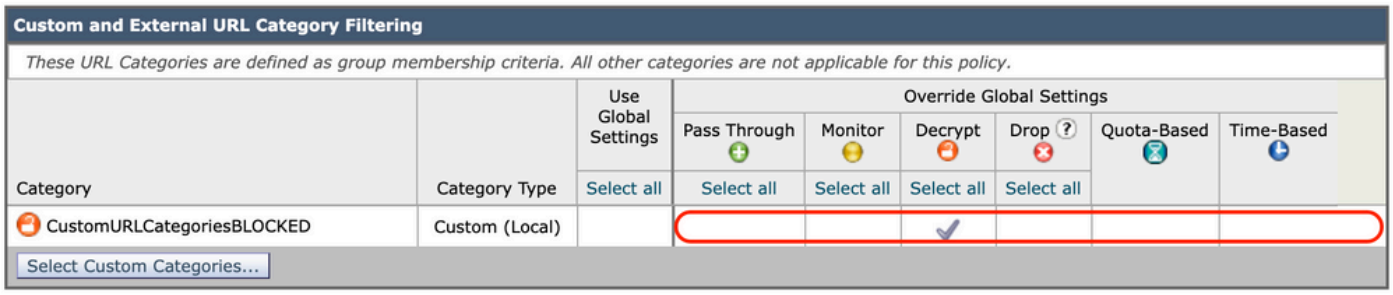


Image - Choisir une action pour la politique de déchiffrement

Action	Description
Utiliser le paramètre global	Utilise l'action pour cette catégorie dans le groupe de stratégie de décodage global. Il s'agit de l'action par défaut pour les groupes de stratégies définis par l'utilisateur. S'applique uniquement aux groupes de stratégies définis par l'utilisateur. Lorsqu'une catégorie d'URL personnalisée est exclue de la stratégie de déchiffrement globale, l'action par défaut pour les catégories d'URL personnalisées incluses dans les stratégies de déchiffrement définies par l'utilisateur est Surveillance au lieu d'Utiliser les paramètres globaux. Vous ne pouvez pas choisir Utiliser les paramètres globaux lorsqu'une catégorie d'URL personnalisée est exclue de la stratégie de décodage globale.
Passthrough	Passe par la connexion entre le client et le serveur sans examiner le contenu du trafic.
Monitor	Le proxy Web n'autorise ni ne bloque la demande. Au lieu de cela, il continue à évaluer la demande du client par rapport à d'autres paramètres de contrôle de groupe de stratégies, tels que le filtre de réputation Web.
Déchiffrer	Permet la connexion, mais inspecte le contenu du trafic. La solution matérielle-logicielle déchiffre le trafic et applique les stratégies d'accès au trafic déchiffré

Action	Description
	comme s'il s'agissait d'une connexion HTTP (Hypertext Transfer Protocol) en texte clair. Lorsque la connexion est décryptée et que les stratégies d'accès sont appliquées, vous pouvez analyser le trafic à la recherche de programmes malveillants.
Goutte	Abandonne la connexion et ne transmet pas la demande de connexion au serveur. La solution matérielle-logicielle n'avertit pas l'utilisateur qu'elle a interrompu la connexion.

Étape 5. Dans la section URL non classées, choisissez l'action à entreprendre pour les demandes de clients à des sites Web qui ne font pas partie d'une catégorie d'URL prédéfinie ou personnalisée.

Ce paramètre détermine également l'action par défaut pour les catégories nouvelles et fusionnées résultant des mises à jour du jeu de catégories d'URL.

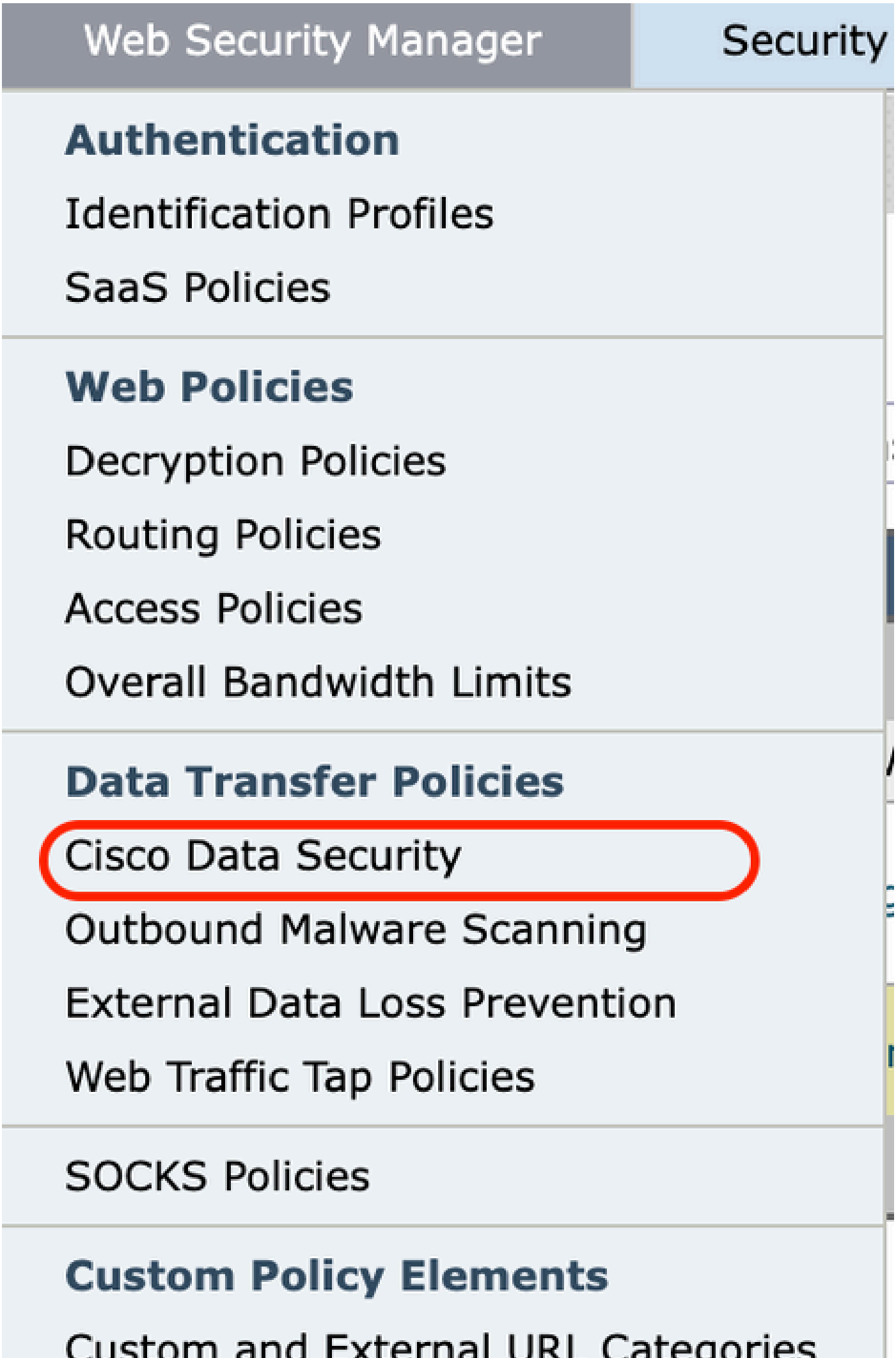
Image - Politique de déchiffrement non catégorisée

Étape 6. Soumettre et valider les modifications.

⚠ Attention : si vous souhaitez bloquer une catégorie d'URL particulière pour les demandes HTTPS (Hypertext Transfer Protocol Secure), choisissez de décrypter cette catégorie d'URL dans le groupe Stratégie de décryptage, puis choisissez de bloquer la même catégorie d'URL dans le groupe Stratégie d'accès.

Étapes De Configuration Des Filtres D'URL Pour Les Groupes De Stratégies De Sécurité Des Données

Étape 1. Choisissez Web Security Manager > Cisco Data Security.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

Cliquez sur le lien dans le tableau des stratégies sous la colonne Filtrage d'URL pour le groupe de stratégies que vous souhaitez modifier.

Image - Sécurité des données choisir un filtre d'URL

Étape 3. (Facultatif) Dans la section Filtrage des catégories d'URL personnalisées, vous pouvez ajouter des catégories d'URL personnalisées sur lesquelles vous devez agir dans cette stratégie :

a. Cliquez sur Sélectionner des catégories personnalisées.

Image - Sélectionner un champ personnalisé

b. Choisissez les catégories d'URL personnalisées à inclure dans cette stratégie et cliquez sur Apply.

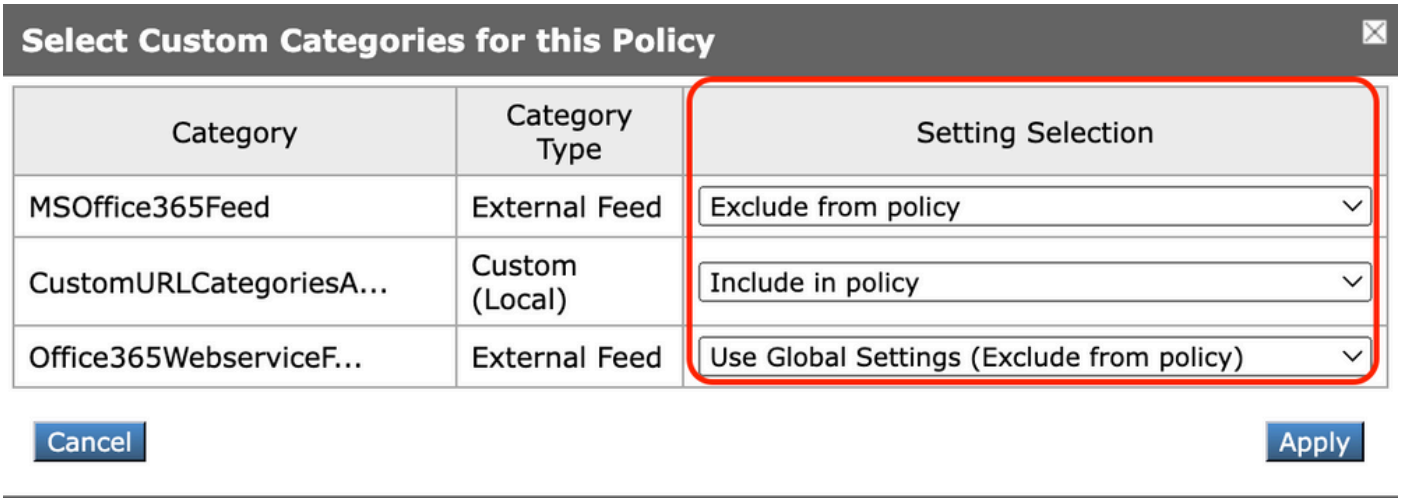


Image : sélectionnez les catégories personnalisées à inclure dans la stratégie

Choisissez les catégories d'URL personnalisées par rapport auxquelles le moteur de filtrage d'URL doit comparer la demande du client.

Le moteur de filtre d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues.

Le moteur de filtre d'URL compare l'URL d'une requête client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la stratégie apparaissent dans la section Filtrage des catégories d'URL personnalisées.

Étape 4. Dans la section Filtrage personnalisé des catégories d'URL, sélectionnez une action pour chaque catégorie d'URL personnalisée.

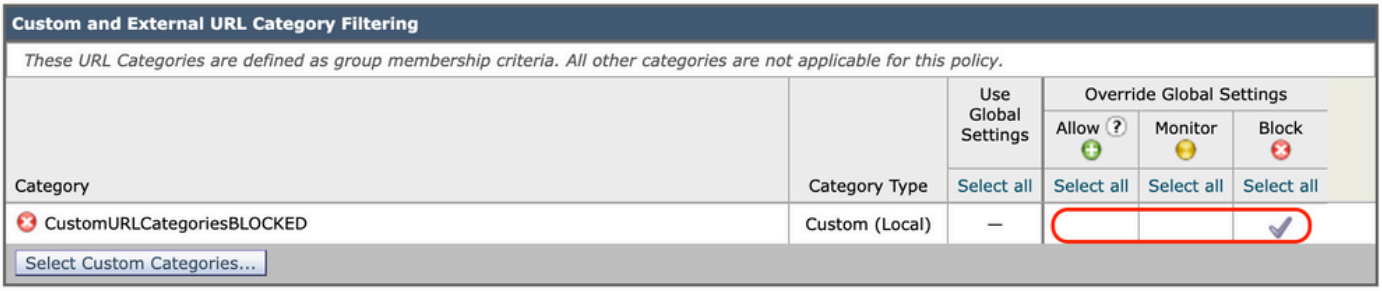


Image - Sécurité des données Choisir une action

Action	Description
Utiliser le paramètre global	Utilise l'action pour cette catégorie dans le groupe de stratégies globales. Il s'agit de l'action par défaut pour les groupes de stratégies définis par l'utilisateur. S'applique uniquement aux groupes de stratégies définis par l'utilisateur. Lorsqu'une catégorie d'URL personnalisée est exclue de la stratégie globale de sécurité des données Cisco, l'action par défaut pour les catégories d'URL personnalisées incluses dans les stratégies de sécurité des données Cisco définies par l'utilisateur est Surveiller au lieu d'Utiliser les paramètres globaux. Vous ne pouvez pas choisir Utiliser les paramètres globaux lorsqu'une catégorie d'URL personnalisée est exclue de la stratégie globale de sécurité des données Cisco.
Allow	Autorise toujours les demandes de téléchargement pour les sites Web de cette catégorie. S'applique uniquement aux catégories d'URL personnalisées. Les demandes autorisées contournent toutes les analyses de sécurité des données supplémentaires et la demande est évaluée par rapport aux stratégies d'accès. Utilisez ce paramètre uniquement pour les sites Web de confiance. Vous pouvez utiliser ce paramètre pour les sites internes.
Monitor	Le proxy Web n'autorise ni ne bloque la demande. Au lieu de cela, il continue à évaluer la demande de téléchargement par rapport à d'autres paramètres de contrôle de groupe de stratégies, tels que le filtre de réputation Web.

Action	Description
Block	Le proxy Web refuse les transactions qui correspondent à ce paramètre.

Étape 5. Dans la section Filtrage des catégories d'URL prédéfinies, sélectionnez l'une des actions suivantes pour chaque catégorie :

- Utiliser les paramètres globaux
- Monitor
- Block

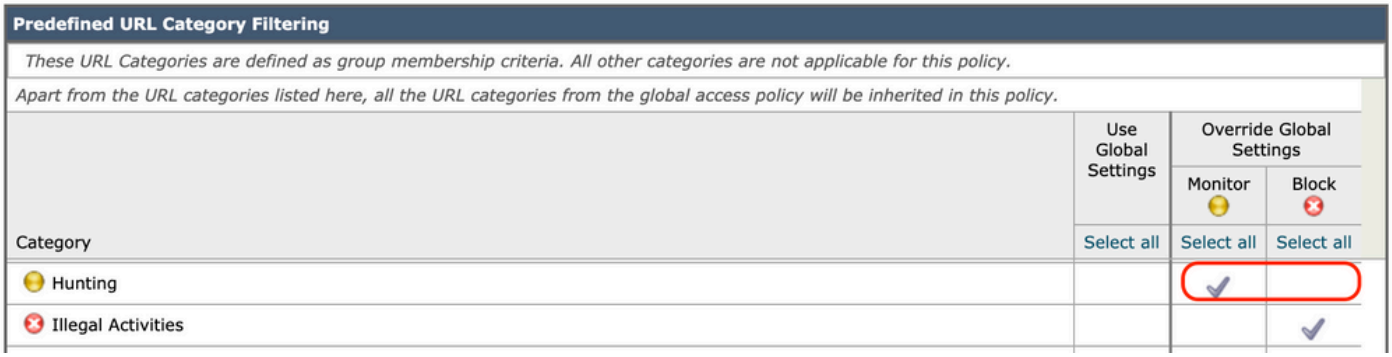


Image - Sécurité des données URL prédéfinie Choisir une action

Étape 6. Dans la section URL non classées, choisissez l'action à entreprendre pour les demandes de téléchargement vers des sites Web qui ne font pas partie d'une catégorie d'URL prédéfinie ou personnalisée.

Ce paramètre détermine également l'action par défaut pour les catégories nouvelles et fusionnées résultant des mises à jour du jeu de catégories d'URL.

Image - Sécurité des données non catégorisée

Étape 7. Soumettre et valider les modifications.

⚠ Attention : si vous ne désactivez pas la limite de taille de fichier maximale, l'appliance de sécurité Web continue à valider la taille de fichier maximale lorsque les options Autoriser ou Surveiller sont sélectionnées dans le filtrage d'URL.

Étapes De Configuration Du Contrôle Des Demandes De Téléchargement Avec Des Catégories D'URL Personnalisées

Chaque demande de téléchargement est attribuée à un groupe de stratégies « Analyse des programmes malveillants sortants » et hérite des paramètres de contrôle de ce groupe de stratégies.

Une fois que le proxy Web a reçu les en-têtes de requête de téléchargement, il dispose des informations nécessaires pour décider s'il doit analyser le corps de la requête.

Le moteur DVS analyse la demande et renvoie un verdict au proxy Web. La page de blocage apparaît à l'utilisateur final, le cas échéant.

<table>
<tr><td>Étape 1</td><td>Choisissez Web Security Manager > Outbound Malware Scanning.</td></tr>
<tr><td>Étape 2</td><td>Dans la colonne Destinations, cliquez sur le lien du groupe de stratégies que vous souhaitez configurer.</td></tr>
<tr><td>Étape 3</td><td>Dans la section Edit Destination Settings, sélectionnez "Define Destinations Scanning Custom Settings" dans le menu déroulant.</td></tr>
<tr><td>Étape 4</td><td>Dans la section Destinations à analyser, sélectionnez l'une des options suivantes :
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Ne pas analyser les téléchargements</td><td>Le moteur DVS n'analyse aucune demande de téléchargement. Toutes les demandes de téléchargement sont évaluées par rapport aux stratégies d'accès</td></tr>
<tr><td>Analyser tous les téléchargements</td><td>Le moteur DVS analyse toutes les requêtes de téléchargement. La demande de téléchargement est bloquée ou évaluée par rapport aux stratégies d'accès, en fonction du verdict d'analyse du moteur DVS</td></tr>
<tr><td>Analyser les téléchargements vers les catégories d'URL personnalisées spécifiées</td><td>Le moteur DVS analyse les demandes de téléchargement qui appartiennent à des catégories d'URL personnalisées spécifiques. La demande de téléchargement est bloquée ou évaluée par rapport aux stratégies d'accès, dépend du verdict d'analyse du moteur DVS.

Cliquez sur Modifier la liste des catégories</td></tr>
</table>
</td></tr>
</table>

	Option	Description
		personnalisées pour sélectionner les catégories d'URL à analyser
Étape 5	Envoyez vos modifications.	
Étape 6	Dans la colonne Filtrage anti-programme malveillant, cliquez sur le lien du groupe de stratégies.	
Étape 7	Dans la section Paramètres de protection contre les programmes malveillants, sélectionnez Définir les paramètres personnalisés de protection contre les programmes malveillants.	
Étape 8	Dans la section Paramètres anti-programme malveillant Cisco DVS, sélectionnez les moteurs d'analyse anti-programme malveillant à activer pour ce groupe de stratégies.	
Étape 9	Dans la section Malware Categories, choisissez de surveiller ou de bloquer les différentes catégories de programmes malveillants. Les catégories répertoriées dans cette section dépendent des moteurs d'analyse que vous activez.	
Étape 10	Soumettre et valider les modifications.	

Étapes de configuration des demandes de contrôle de téléchargement dans les stratégies DLP externes

Une fois que le proxy Web reçoit les en-têtes de demande de téléchargement, il dispose des informations nécessaires pour décider si la demande peut être envoyée au système DLP externe pour analyse.

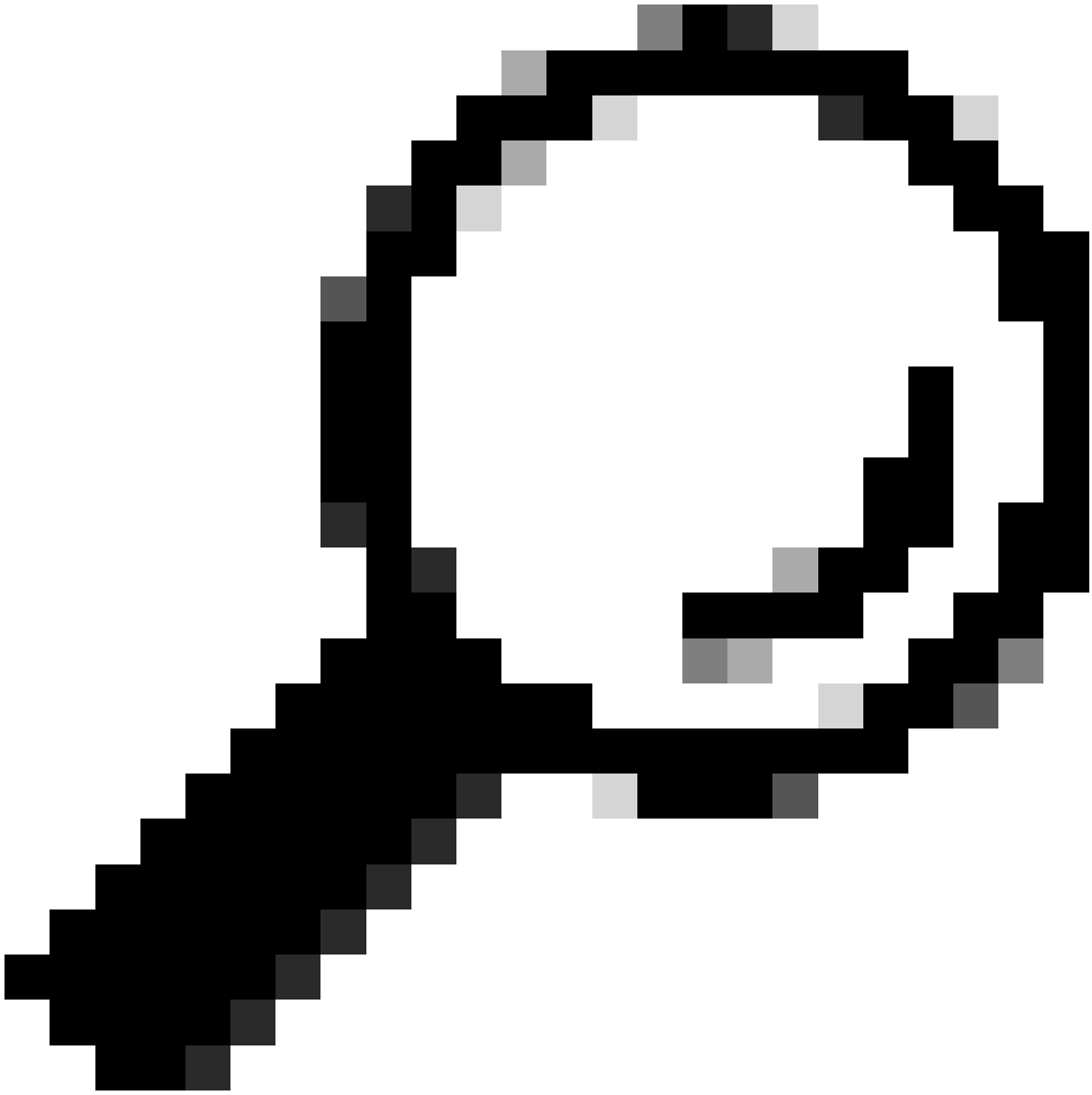
Le système DLP analyse la demande et renvoie un verdict au proxy Web, qu'il bloque ou surveille (évalue la demande par rapport aux stratégies d'accès).

Étape 1	Choisissez Web Security Manager > External Data Loss Prevention.

Étape 2	Cliquez sur le lien situé sous la colonne Destinations du groupe de stratégies que vous souhaitez configurer.
Étape 3	Dans la section Modifier les paramètres de destination, choisissez « Définir les destinations Analyse des paramètres personnalisés. »
Étape 4	Dans la section Destination à analyser, choisissez l'une des options suivantes : • N'analysez aucun téléchargement. Aucune demande de téléchargement n'est envoyée aux systèmes DLP (Data Loss Prevention) configurés pour analyse. Toutes les demandes de téléchargement sont évaluées par rapport aux stratégies d'accès. • Analyser tous les envois. Toutes les demandes de téléchargement sont envoyées au(x) système(s) DLP configuré(s) pour analyse. La demande de téléchargement est bloquée ou évaluée par rapport aux stratégies d'accès en fonction du verdict d'analyse du système DLP. • Analyser les téléchargements sauf pour les catégories d'URL personnalisées et externes spécifiées. Les demandes de téléchargement appartenant à des catégories d'URL personnalisées spécifiques sont exclues des stratégies d'analyse DLP. Cliquez sur Modifier la liste des catégories personnalisées pour sélectionner les catégories d'URL à analyser.
Étape 5	Soumettre et valider les modifications.

Contourner et passer les URL

Vous pouvez configurer l'appliance Web sécurisée dans une implémentation proxy transparente pour contourner les requêtes HTTP ou HTTPS de clients particuliers ou de destinations particulières.



Conseil : vous pouvez utiliser la fonctionnalité Passthrough pour les applications qui nécessitent le passage du trafic via l'appliance, sans avoir besoin d'aucune modification ou vérification de certificat des serveurs de destination

⚠ Attention : la fonctionnalité Domain Map fonctionne en mode HTTPS Transparent. Cette fonctionnalité ne fonctionne pas en mode explicite et pour le trafic HTTP.

- La catégorie personnalisée locale doit être configurée pour permettre au trafic d'utiliser cette fonctionnalité.
- Lorsque cette fonctionnalité est activée, elle modifie ou attribue le nom du serveur conformément au nom de serveur configuré dans le mappage de domaine, même si des informations d'indication de nom de serveur (SNI) sont disponibles.

- Cette fonctionnalité ne bloque pas le trafic basé sur le nom de domaine si ce trafic correspond au mappage de domaine et correspond à la catégorie personnalisée, à la stratégie de déchiffrement et à l'action de transfert configurés.
- L'authentification ne fonctionne pas avec cette fonction d'intercommunication. L'authentification nécessite un déchiffrement, mais le trafic n'est pas déchiffré dans ce cas.
- le trafic n'est pas surveillé. Vous devez configurer le trafic UDP pour ne pas arriver à l'appareil de sécurité Web, au lieu de cela, il doit passer directement par le pare-feu à Internet pour les applications comme WhatsApp, Telegram et ainsi de suite.
- WhatsApp, Telegram et Skype fonctionnent en mode transparent. Cependant, certaines applications comme WhatsApp ne fonctionnent pas en mode explicite en raison de restrictions sur l'application.

Assurez-vous qu'une stratégie d'identification est définie pour les périphériques qui nécessitent un trafic de transit vers des serveurs spécifiques. Plus précisément, vous devez :

- Sélectionnez Exempt de l'authentification/identification.
- Spécifiez les adresses auxquelles ce profil d'identification doit s'appliquer. Vous pouvez utiliser des adresses IP, des blocs CIDR (Classless Inter-Domain Routing) et des sous-réseaux.

Étape 1	Activez le proxy HTTPS.
Étape 2	Choisissez Web Security Manager > Domain Map. a. Sélectionnez Ajouter un domaine. b. Saisissez le nom de domaine ou le serveur de destination. c. Choisissez l'ordre de priorité si certains domaines sont spécifiés. d. Saisissez les adresses IP. e. Cliquez sur Submit.
Étape 3	Choisissez Web Security Manager > Custom and External URL Categories. a. Sélectionnez Ajouter une catégorie. b. Fournissez ces informations.

<table>
<tr><td></td><td>
<table>
<tr><th>Paramètres</th><th>Description</th></tr>
<tr><td>Nom de catégorie</td><td>Entrez un identificateur pour cette catégorie d'URL. Ce nom apparaît lorsque vous configurez le filtre d'URL pour les groupes de stratégies.</td></tr>
<tr><td>Ordre des listes</td><td>Spécifiez l'ordre de cette catégorie dans la liste des catégories d'URL personnalisées. Entrez « 1 » pour la première catégorie d'URL de la liste.

Le moteur de filtre d'URL évalue une requête client par rapport aux catégories d'URL personnalisées dans l'ordre spécifié.</td></tr>
<tr><td>Type de catégorie</td><td>Sélectionnez Catégorie personnalisée locale.</td></tr>
<tr><td>Avancé</td><td>Vous pouvez entrer des expressions régulières dans cette section pour spécifier des ensembles d'adresses supplémentaires.

Vous pouvez utiliser des expressions régulières pour spécifier plusieurs adresses qui correspondent aux modèles que vous entrez.</td></tr>
</table>
c. Envoyez et validez les modifications.
</td></tr>
<tr><td>Étape 4</td><td>Choisissez Web Security Manager > Decryption Policies.

a. Créez une nouvelle stratégie de déchiffrement.

b. Sélectionnez le profil d'identification que vous avez créé pour contourner le trafic HTTPS pour des applications spécifiques.

c. Dans le panneau Avancé, cliquez sur le lien Catégories d'URL.

d. Dans la colonne Add, cliquez sur pour ajouter la catégorie d'URL personnalisée créée à l'étape 3.

e. Sélectionnez Terminé.

f. Dans la page Stratégies de décodage, cliquez sur le lien Filtrage des URL.</td></tr>
</table>

	g. Sélectionnez Passthrough. h. Envoyez et validez les modifications. (Facultatif) Vous pouvez utiliser le spécificateur de format %(pour afficher les informations du journal d'accès.

Configurer Le Contournement Du Proxy Web Pour Les Requêtes Web

Une fois que vous avez ajouté les catégories d'URL personnalisées à la liste de contournement de proxy, toutes les adresses IP et les noms de domaine des catégories d'URL personnalisées sont contournés pour la source et la destination.

Étape 1	Choisissez Gestionnaire de sécurité Web > Ignorer les paramètres.
Étape 2	Cliquez sur Edit Bypass Settings.
Étape 3	Saisissez les adresses pour lesquelles vous souhaitez contourner le proxy Web. Remarque : lorsque vous configurez /0 comme masque de sous-réseau pour toute adresse IP de la liste de contournement, l'appliance contourne tout le trafic Web. Dans ce cas, l'appliance interprète la configuration comme 0.0.0.0/0.
Étape 4	Sélectionnez les catégories d'URL personnalisées que vous souhaitez ajouter à la liste de contournement de proxy.
Étape 5	Envoyez et validez vos modifications.

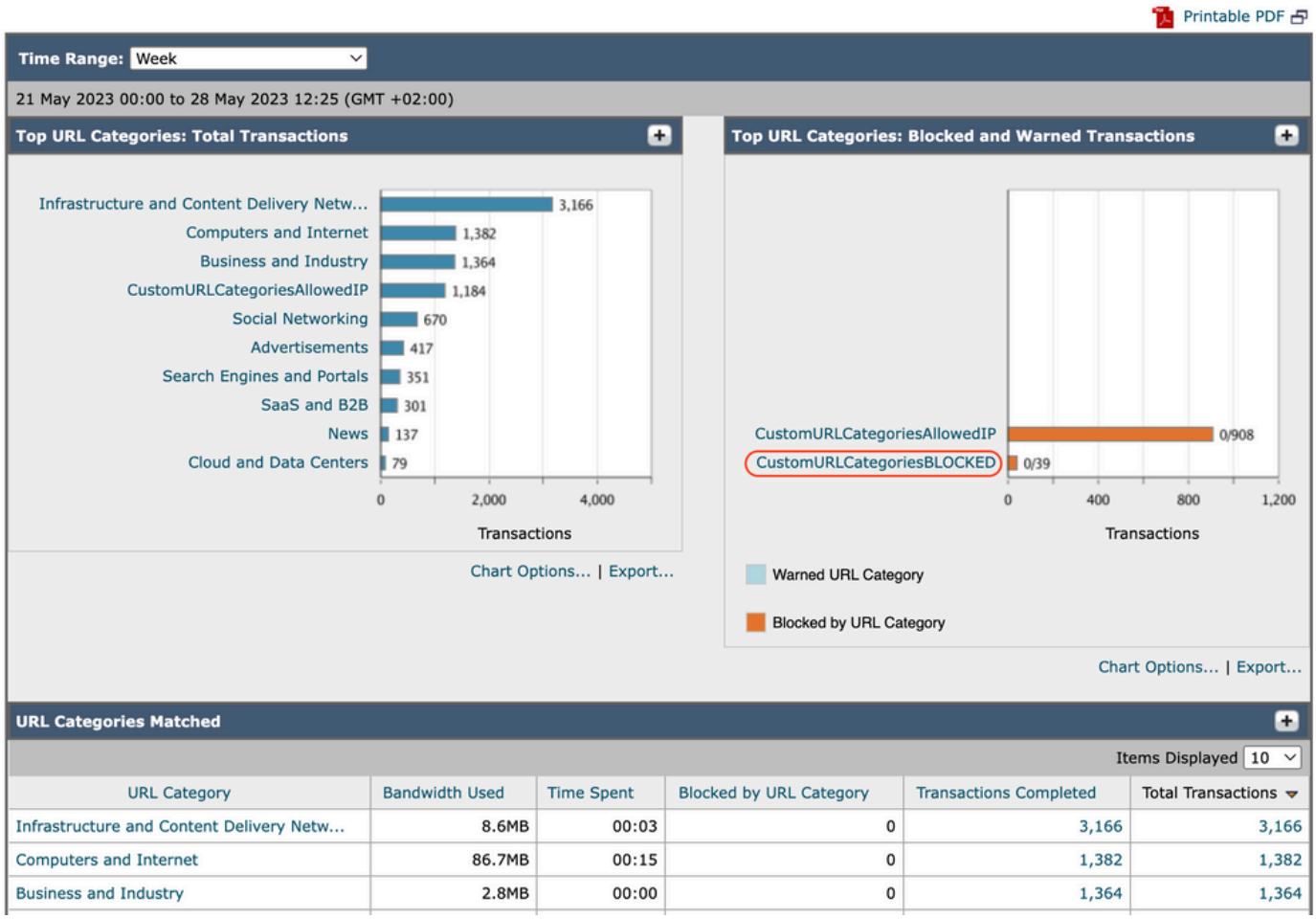
Attention : vous ne pouvez pas définir le contournement du proxy Web pour les expressions régulières.

Rapports

La page "Création de rapports" >> Catégories d'URL fournit un affichage collectif des statistiques d'URL qui inclut des informations sur les principales catégories d'URL correspondantes et les principales catégories d'URL bloquées.

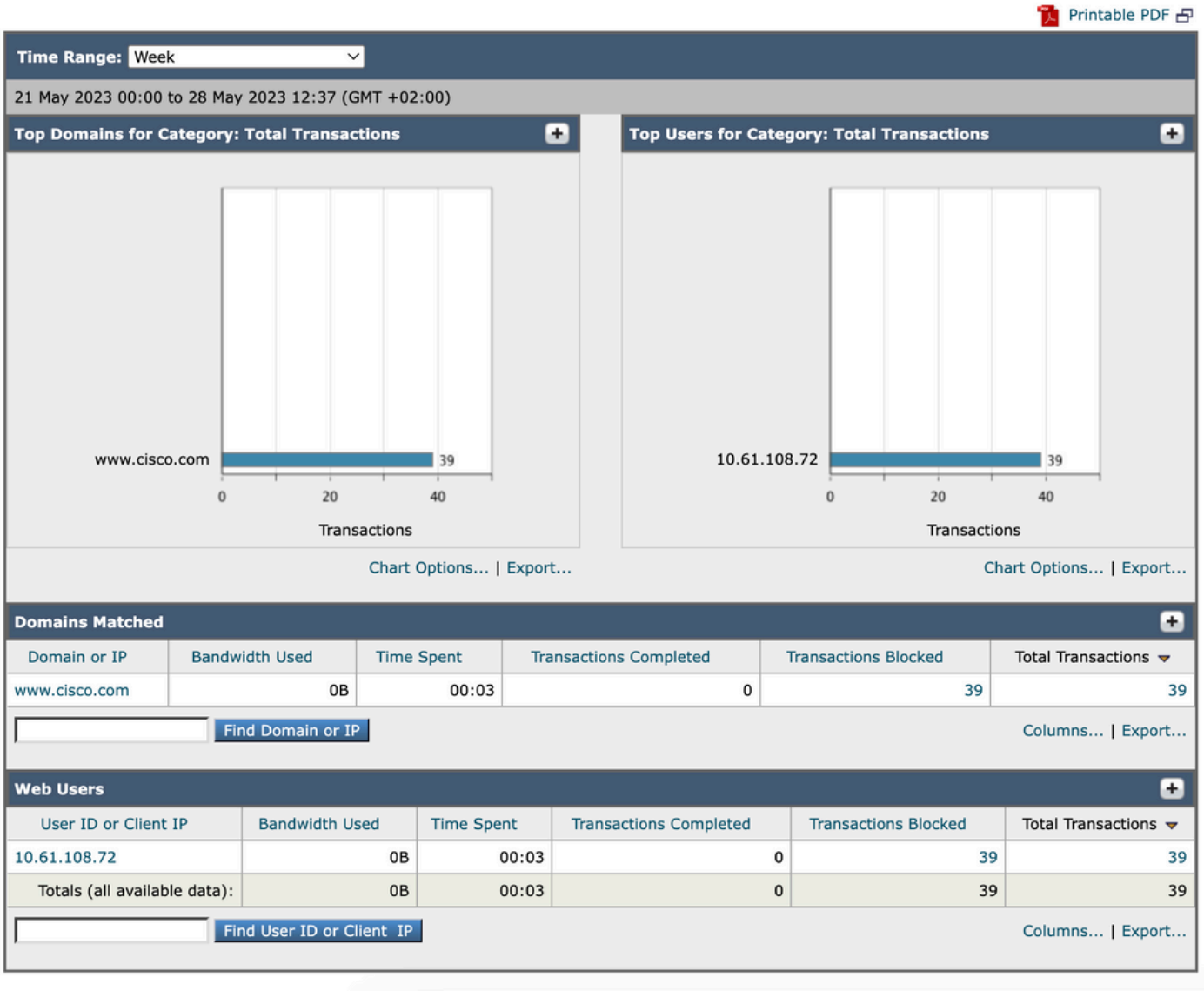
Cette page affiche des données spécifiques à chaque catégorie pour les économies de bande passante et les transactions Web.

Profilé	Description
Intervalle de temps (liste déroulante)	Choisissez la plage de temps pour votre rapport.
Premières catégories d'URL par nombre total de transactions	Cette section répertorie les principales catégories d'URL visitées sur le site sous forme de graphique.
Premières catégories d'URL par transactions bloquées et averties	Répertorie l'URL principale qui a déclenché une action de blocage ou d'avertissement par transaction dans un format graphique.
Catégories d'URL correspondantes	Affiche la répartition des transactions par catégorie d'URL au cours de la période spécifiée, ainsi que la bande passante utilisée et le temps passé dans chaque catégorie. Si le pourcentage d'URL non classées est supérieur à 15-20 %, envisagez les options suivantes : • Pour des URL localisées spécifiques, vous pouvez créer des catégories d'URL personnalisées et les appliquer à des utilisateurs ou des stratégies de groupe spécifiques. • Vous pouvez signaler des URL non classées et mal classées à Cisco pour évaluation et mise à jour de la base de données. • Vérifiez que les filtres de réputation Web et anti-programme malveillant sont activés.



Rapport de catégorie Image-URL

Vous pouvez cliquer sur un nom de catégorie pour afficher plus de détails liés à cette catégorie, tels que Domaines correspondants ou Liste des utilisateurs.



Page Image - Rapport détaillé

L'ensemble des catégories d'URL prédéfinies peut être mis à jour régulièrement et automatiquement sur votre appareil de sécurité Web .

Lorsque ces mises à jour se produisent, les anciens noms de catégorie continuent à apparaître dans les rapports jusqu'à ce que les données associées aux anciennes catégories soient trop anciennes pour être incluses dans les rapports.

Les données de rapport générées après la mise à jour d'un jeu de catégories d'URL utilisent les nouvelles catégories, de sorte que vous pouvez voir les anciennes et les nouvelles catégories dans le même rapport.

Dans les statistiques d'URL de la page Catégories d'URL des rapports, il est important de comprendre comment interpréter ces données :

Type de données	Description
Filtrage des URL contourné	Représente la stratégie, le port et l'agent utilisateur admin bloqués qui se produisent

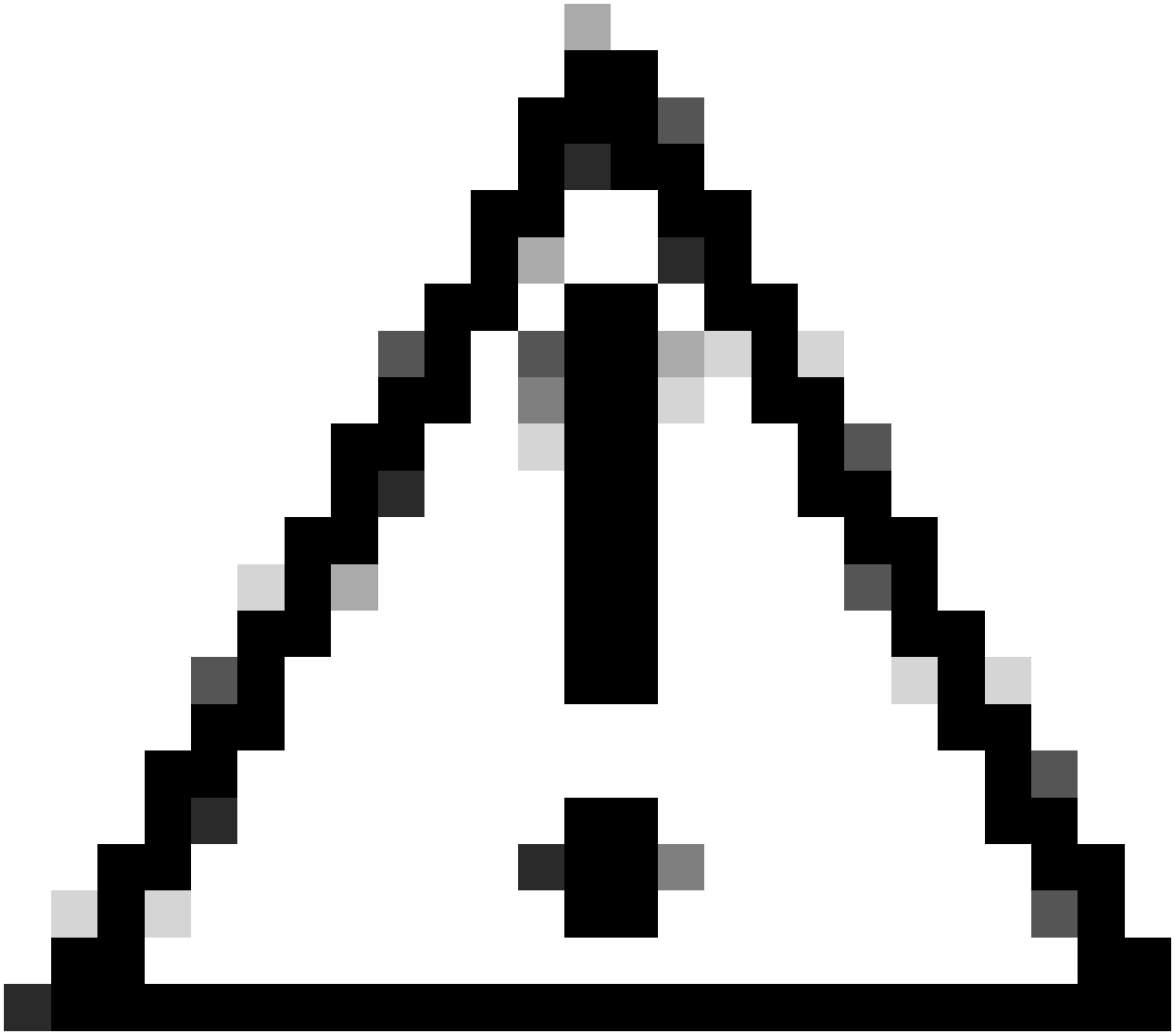
	avant le filtrage d'URL.
URL non catégorisée	Représente toutes les transactions pour lesquelles le moteur de filtrage d'URL est interrogé, mais aucune catégorie ne correspond.

Afficher Les Catégories D'URL Personnalisées Dans Le Journal D'Accès

L'appliance Web sécurisée utilise les quatre premiers caractères des noms de catégorie d'URL personnalisés précédés de « c_ » dans les journaux d'accès.

Dans cet exemple, le nom de la catégorie est CustomURLCategoriesBLOCKED et dans les journaux d'accès, vous pouvez voir C_Cust :

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



Attention : considérez le nom de catégorie d'URL personnalisé si vous utilisez Sawmill pour analyser les journaux d'accès. Si les quatre premiers caractères de la catégorie d'URL personnalisée comprennent un espace, Sawmill ne peut pas analyser correctement l'entrée du journal d'accès. Utilisez uniquement les caractères pris en charge dans les quatre premiers caractères.

Conseil : si vous souhaitez inclure le nom complet d'une catégorie d'URL personnalisée dans les journaux d'accès, ajoutez le spécificateur de format %XF aux journaux d'accès.

Lorsqu'un groupe de stratégies d'accès Web a une catégorie d'URL personnalisée définie sur Monitor et qu'un autre composant (tel que les filtres de réputation Web ou le moteur d'analyse des différents verdicts (DVS)) prend la décision finale d'autoriser ou de bloquer une demande d'URL dans la catégorie d'URL personnalisée, l'entrée du journal d'accès pour la demande affiche la catégorie d'URL prédéfinie au lieu de la catégorie d'URL personnalisée.

Pour plus d'informations sur la configuration des champs personnalisés dans les journaux d'accès,

consultez : Configurer le paramètre de performance dans les journaux d'accès - Cisco

Dépannage

Catégorie non concordante

Dans les journaux d'accès, vous pouvez voir à quelle catégorie d'URL personnalisée appartient la demande, si la sélection n'est pas comme prévu :

- Si la demande est classée dans d'autres catégories d'URL personnalisées, recherchez une URL dupliquée ou une expression régulière correspondante dans d'autres catégories ou déplacez la catégorie d'URL personnalisée vers le haut et testez à nouveau. Il est préférable d'examiner attentivement la catégorie d'URL personnalisée correspondante.

- Si la demande est classée en catégories prédéfinies, vérifiez les conditions dans la catégorie d'URL personnalisée existante, si toutes correspondent, essayez d'ajouter l'adresse IP et de tester ou assurez-vous que la faute de frappe et l'expression régulière correcte sont utilisées, le cas échéant.

Les catégories prédéfinies ne sont pas à jour

Si les catégories prédéfinies ne sont pas à jour ou si « err » apparaît dans les journaux d'accès de la section de catégorie d'URL, assurez-vous que TLSv1.2 est activé pour Updater.

Pour modifier la configuration SSL de Updater, procédez comme suit depuis l'interface utilisateur graphique :

Étape 1. Dans Administration système, sélectionnez Configuration SSL

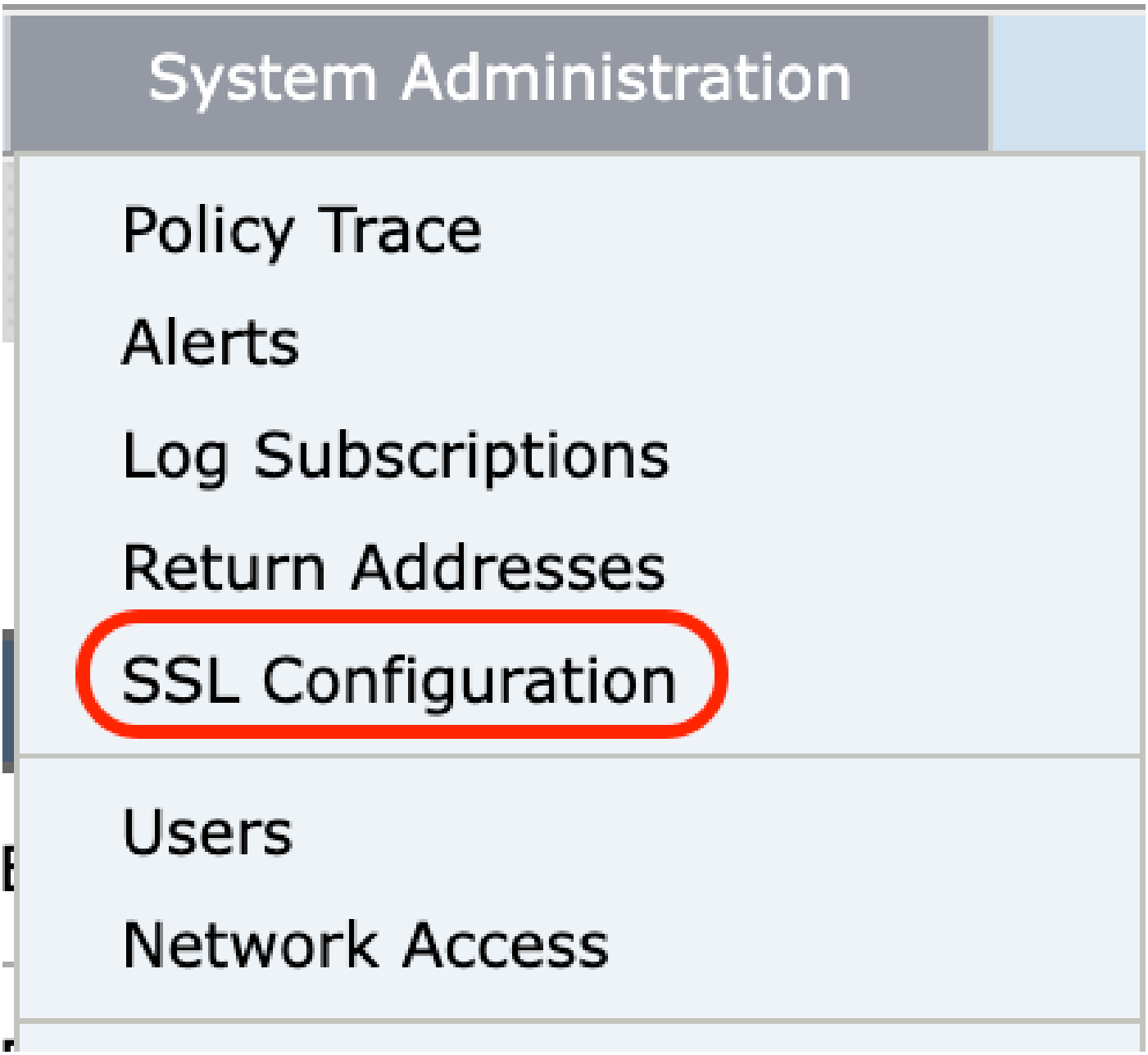


Image - configuration ssl

Étape 2. Sélectionnez Modifier les paramètres.

Étape 3. Dans la section Update service, sélectionnez TLSv1.2

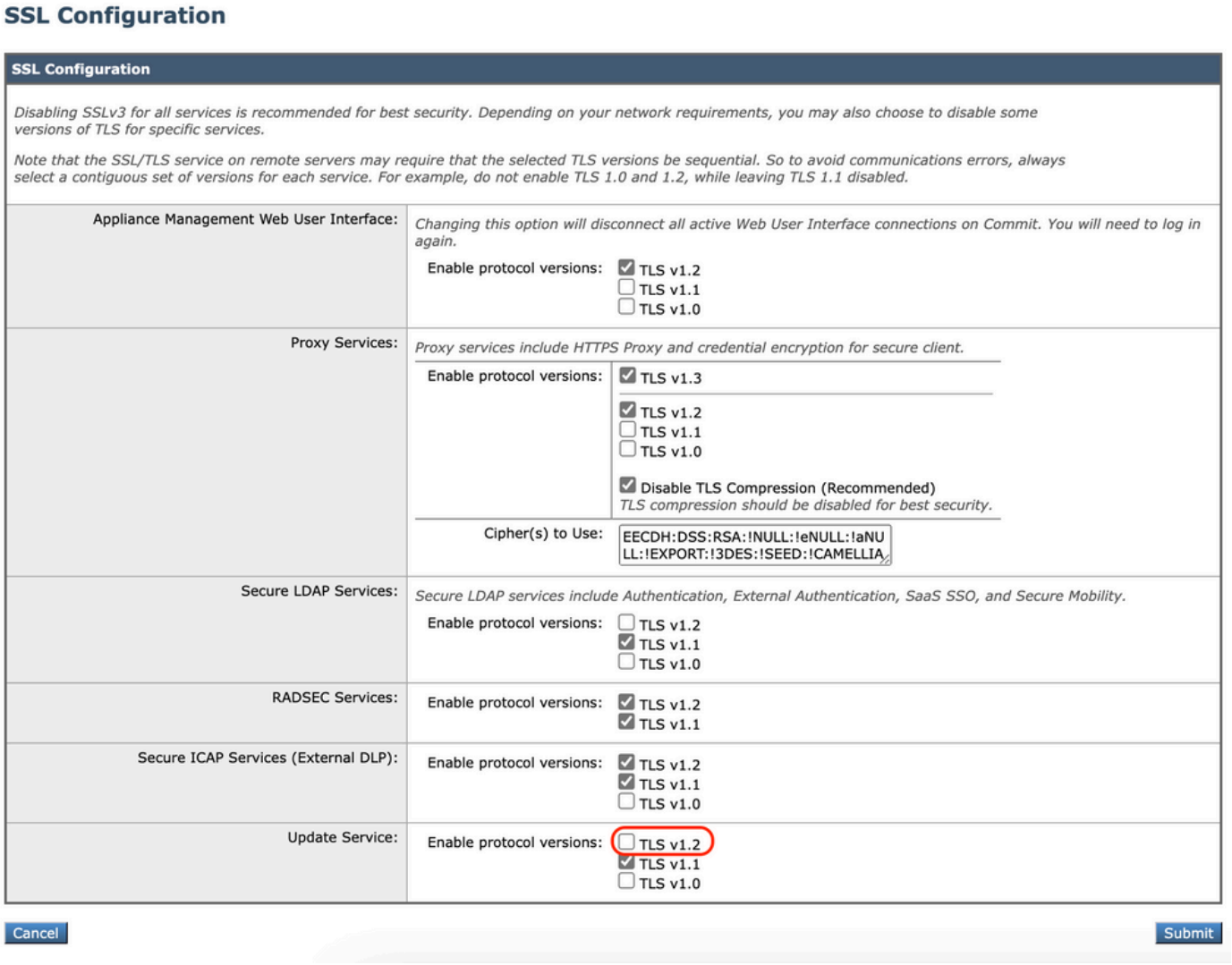


Image - Mettre à jour le service TLSv1.2

Étape 4. Envoyer et valider les modifications

Pour modifier la configuration SSL de Updater, procédez comme suit à partir de l'interface de ligne de commande :

Étape 1. À partir de CLI, exécutez sslcofig

Étape 2. Tapez version et appuyez sur Entrée

Étape 3. Choisir Updater

Étape 4. Choisissez TLSv1.2

Étape 5. Appuyez sur Entrée pour quitter l'assistant

Étape 6 : validation des modifications

```
SWA_CLI> sslconfig
```

```
Disabling SSLv3 is recommended for best security.

Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequentia
1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.
[]> versions

SSL/TLS versions may be enabled or disabled for the following services:

        LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secu
        Updater - Update Service
        WebUI - Appliance Management Web User Interface
        RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
        SICAP - Secure ICAP Service
        Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

         LDAPS  Updater  WebUI   RADSEC  SICAP   Proxy
TLSv1.0    N       N       N      N/A      N       N
TLSv1.1    Y       Y       N       Y       Y       N
TLSv1.2    N       N       Y       Y       Y       Y
TLSv1.3   N/A     N/A     N/A     N/A     N/A      Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services
[]> 2


Currently enabled protocol(s) for Updater are TLSv1.1.


To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
[]> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y


Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.
```

Référence

Recommandations relatives aux meilleures pratiques pour les appareils de sécurité Web Cisco - Cisco

BRKSEC-3303 (ciscolive)

Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance - GD (General Deployment) - Connect, Install, and Configure [Cisco Secure Web Appliance] - 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.