Restrictions de contenu

Les rubriques suivantes décrivent comment configurer des politiques de contrôle d'accès pour utiliser les fonctionnalités de restriction de contenu :

À propos des restrictions de contenu

Les principaux moteurs de recherche et services de diffusion de contenu offrent des fonctionnalités qui vous permettent de restreindre les résultats de recherche et le contenu de sites Web. Par exemple, les écoles utilisent des fonctionnalités de restriction de contenu pour se conformer à la Children's Internet Protection Act (CIPA).

Lorsqu'elles sont mises en œuvre par des moteurs de recherche et des services de diffusion de contenu, vous ne pouvez appliquer des fonctionnalités de restriction de contenu que pour des navigateurs ou des utilisateurs individuels. Le système vous permet d'étendre ces fonctionnalités à l'ensemble de votre réseau.

Le système vous permet d'appliquer :

- *Recherche sécurisée* : pris en charge par de nombreux principaux moteurs de recherche, ce service filtre le contenu explicite et destiné aux adultes que les environnements des entreprises, du gouvernement et de l'éducation classent comme inacceptable. Le système ne restreint pas la capacité d'un utilisateur à accéder aux pages d'accueil des moteurs de recherche pris en charge.

Vous pouvez utiliser deux méthodes pour configurer le système afin d'appliquer ces fonctionnalités :

Méthode : règles de contrôle d'accès
: Les fonctionnalités de restriction de contenu communiquent l'état restreint d'une recherche ou d'une requête de contenu par un élément dans l'URI de la demande, un témoin associé ou un élément d'en-tête HTTP personnalisé. Vous pouvez configurer des règles de contrôle d'accès pour modifier ces éléments pendant que le système traite le trafic.

Méthode : gouffre DNS
: Pour les recherches Google, vous pouvez configurer le système pour rediriger le trafic vers l'adresse IP virtuelle (VIP) SafeSearch de Google, ce qui imposé des filtres pour la recherche sécurisée.

Le tableau ci-dessous décrit les différences entre ces méthodes d'exécution.

Tableau 1 : Comparaison des méthodes de restriction de contenu

Attribut	Méthode : règles de contrôle d'accès	Méthode : gouffre DNS
Périphériques pris en charge	N'importe lequel	Cisco Secure Firewall Threat Defense uniquement
Moteurs de recherche pris en charge	Toute `recherche SafeSearch balisée est prise en charge` dans l'onglet **Applications** de l'éditeur de règles	Google uniquement
Mode restreint YouTube pris en charge	Oui	Oui
Politique SSL requise	Oui	Non
Les hôtes doivent utiliser IPv4	Non	Oui
Journalisation des événements de connexion	Oui	Oui

Lors de la détermination de la méthode à utiliser, tenez compte des limites suivantes :

- La méthode des règles de contrôle d'accès nécessite une politique SSL, ce qui a une incidence sur les performances.
- L'adresse VIP Google SafeSearch prend en charge uniquement le trafic IPv4. Si vous configurez un gouffre DNS pour gérer les recherches Google, tous les hôtes du réseau concerné doivent utiliser IPv4.

Le système journalise différentes valeurs pour le champ **Reason** (raisons) dans les événements de connexion, selon la méthode utilisée :

- Règles de contrôle d'accès : `restriction de contenu`
- Gouffre DNS : `bloc de DNS`

Exigences et conditions préalables des restrictions de contenu

Prise en charge des modèles

Tous, ou comme indiqué dans la procédure.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès

- Administrateur de réseau

Lignes directrices et limites pour les restrictions de contenu

- La recherche sécurisée est uniquement prise en charge par Snort 2.
- YouTube et Google ne prennent pas en charge la fonctionnalité YouTubeEDU qui a été mise en œuvre dans les règles de contrôle d'accès. Veuillez supprimer toutes les règles de contrôle d'accès qui configurent YouTubeEDU, car elles ne sont pas vraiment fonctionnelles. Vous pouvez également supprimer les règles de déchiffrement associées.

Utilisation de règles de contrôle d'accès pour appliquer une restriction de contenu

La procédure suivante explique comment configurer les règles de contrôle d'accès pour restreindre le contenu.

Remarque Lorsque la recherche sécurisée est activée dans une règle de contrôle d'accès, la normalisation en ligne est activée automatiquement.

Procédure

Étape 1 Créez une politique de déchiffrement.

Étape 2 Ajoutez des règles pour le traitement du trafic de recherche sécurisée :

- Choisissez **Déchiffrer - Resigner** comme **action** pour les règles.
- Dans **Applications**, ajoutez des sélections à la liste **Applications et filtres** sélectionnés :
  - Recherche sécurisée : ajoutez l filtre `catégorie : moteur de recherche`.

Étape 3 Définissez les positions de règles pour les règles que vous avez ajoutées. Cliquez dessus et faites-les glisser ou utilisez le menu contextuel pour la couper et la coller.

Étape 4 Créez ou modifiez une politique de contrôle d'accès et associez la politique de déchiffrement à la politique de contrôle d'accès.

Pour en savoir plus, consultez Association d'autres politiques au contrôle d'accès.

Étape 5 Dans la politique de contrôle d'accès, ajoutez des règles pour le traitement du trafic de la recherche sécurisée :

- Choisissez **Allow** (autoriser) comme **action** pour les règles.
- Dans **Applications**, cliquez sur l'icône **Recherche sécurisée** ( ) et définissez les options connexes.
  - Options de recherche sécurisée pour les règles de contrôle d'accès, à la page 4

- Dans la **zone Applications**, affinez les sélections d'applications dans la liste **Applications et filtres** sélectionnés .

  Dans la plupart des cas, l'activation de la recherche sécurisée remplit la liste des **applications et des filtres** sélectionnés avec les valeurs appropriées. Le système ne remplit pas automatiquement la liste si une application de recherche sécurisée est déjà présente lorsque vous activez la fonctionnalité. Si les applications ne se remplissent pas comme prévu, ajoutez-les manuellement comme suit :

  - Recherche sécurisée : ajoutez l filtre `catégorie : moteur de recherche`.

Pour en savoir plus, consultez Configuration des conditions d'application et des filtres.

Étape 6 Définissez les emplacements des règles de contrôle d'accès que vous avez ajoutées. Cliquez dessus et faites-les glisser ou utilisez le menu contextuel pour la couper et la coller.

Étape 7 configurer la page de réponse HTTP que le système affiche lorsqu'il bloque le contenu restreint; voir Choix des pages de réponse HTTP.

Étape 8 Déployer les changements de configuration.

Options de recherche sécurisée pour les règles de contrôle d'accès

Le système Firepower prend en charge le filtrage de recherche sécurisée pour certains moteurs de recherche uniquement. Pour obtenir la liste des moteurs de recherche pris en charge, consultez les applications marquées `Safesearch prise en charge` dans l'onglet **Applications** de l'éditeur de règles de contrôle d'accès. Pour obtenir la liste des moteurs de recherche non pris en charge, consultez les applications marquées `Safesearch non prise en charge`.

Lorsque vous activez la recherche sécurisée pour une règle de contrôle d'accès, définissez les paramètres suivants :

Activer la recherche sécurisée
Active le filtrage de recherche sécurisée pour le trafic qui correspond à cette règle.

Trafic de recherche non pris en charge
Spécifie l'action que vous souhaitez que le système effectue lorsqu'il traite le trafic provenant de moteurs de recherche non pris en charge. Si vous choisissez **Block** (Bloquer) ou **Block with reset** (Bloquer avec réinitialisation), vous devez également configurer la page de réponse HTTP que le système affiche lorsqu'il bloque le contenu restreint. voir Choix des pages de réponse HTTP.

Utilisation d'un gouffre DNS pour appliquer une restriction de contenu

En règle générale, un gouffre DNS oriente le trafic loin d'une cible particulière. Cette procédure décrit comment configurer un gouffre DNS pour rediriger le trafic vers l'adresse IP virtuelle (VIP) SafeSearch de Google, ce qui imposé des filtres de contenu dans les résultats de recherche Google et YouTube.

Étant donné que Google SafeSearch utilise une adresse IPv4 unique pour l'adresse VIP, les hôtes doivent utiliser des adresses IPv4.

Mise en garde Si votre réseau comprend des serveurs proxy, cette méthode de restriction de contenu n'est pas efficace, sauf si vous positionnez vos défense contre les menaces périphériques entre les serveurs mandataires et Internet.

Cette procédure décrit l'application des restrictions de contenu pour les recherches Google uniquement. Pour appliquer une restriction de contenu pour d'autres moteurs de recherche, consultez Utilisation de règles de contrôle d'accès pour appliquer une restriction de contenu, à la page 3.

Avant de commencer

Cette procédure s'applique uniquement à défense contre les menaces et nécessite la licence IPS .

Procédure

Étape 1 Obtenez une liste des domaines Google pris en charge en cliquant sur l'URL suivante : https://www.google.com/supported_domains.

Étape 2 Créez une liste DNS personnalisée sur votre ordinateur local et ajoutez les entrées suivantes :

- Pour appliquer Google SafeSearch, ajoutez une entrée pour chaque domaine Google pris en charge.
- Pour appliquer le mode restreint de YouTube, ajoutez une entrée « YouTub.com ».

La liste DNS personnalisée doit être au format de fichier texte (.txt). Chaque ligne du fichier texte doit spécifier un nom de domaine individuel, dépourvu de points de début. Par exemple, le domaine pris en charge « .Google.com » doit apparaître sous le nom « Google.com ».

Étape 3 Téléversez la liste DNS personnalisée dans centre de gestion; voir Téléversement de nouvelles listes de renseignements sur la sécurité vers Cisco Secure Firewall Management Center.

Étape 4 Déterminez l'adresse IPv4 pour l'adresse VIP Google SafeSearch. Par exemple, exécutez `nslookup` sur forcesecuresearch.Google.com.

Étape 5 Créer un objet gouffre pour l'adresse VIP SafeSearch; voir Création d'objets de gouffre.

Utilisez les valeurs suivantes pour cet objet :

- IPv4 Address (adresse IPv4) : Saisissez l'adresse VIP SafeSearch.
- IPv6 Address (adresse IPv6) : Saisissez l'adresse IPv6 de boucle avec retour (`::1`).
- Journaliser les connexions au gouffre : cliquez sur Journaliser les connexions.
- Type : Choisissez **Aucun**.

Étape 6 Créer une politique DNS de base; voir Création de politiques DNS de base.

Étape 7 Ajoutez une règle DNS pour le gouffre; voir Création et modification des règles DNS.

Pour cette règle :

- Cochez la case **Enabled** (activer).
- Choisissez `Sinkhole` (gouffre) dans la liste déroulante **Action**.
- Choisissez l'objet gouffre que vous avez créé dans la liste déroulante **Sinkhole** (gouffre).
- Ajoutez la liste DNS personnalisée que vous avez créée à la liste des **éléments sélectionnés** sur **DNS**.

- (Facultatif) Choisissez un réseau dans **Networks** (réseaux) pour limiter la restriction de contenu à des utilisateurs spécifiques. Par exemple, si vous souhaitez limiter la restriction de contenu aux utilisateurs étudiants, affectez les étudiants à un sous-réseau différent de celui du corps professoral et spécifiez ce sous-réseau dans cette règle.

Étape 8 Associer la politique DNS à une politique de contrôle d'accès; voir Association d'autres politiques au contrôle d'accès.

Étape 9 Déployer les changements de configuration.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.