Créer des politiques pour contrôler les demandes Internet

Cette rubrique contient les sections suivantes :

Présentation des politiques : contrôler les demandes Internet interceptées

Lorsque l'utilisateur crée une demande Web, le Secure Web Appliance configuré intercepte les demandes et gère le processus dont la demande parcourt pour arriver à son résultat final, qu'il s'agisse d'accéder à un site Web particulier, à un courriel ou même à une application en ligne. Lors de la configuration de Secure Web Appliance des politiques sont créées pour définir les critères et les actions des demandes faites par l'utilisateur.

Les politiques sont les moyens par lesquels Secure Web Appliance identifie et contrôle les demandes Web. Lorsqu'un client envoie une demande Web à un serveur, le proxy Web reçoit la demande, l'évalue et détermine à quelle politique elle appartient. Les actions définies dans la politique sont ensuite appliquées à la demande.

Secure Web Appliance utilise plusieurs types de politiques pour gérer différents aspects des demandes Web. Les types de politiques peuvent gérer entièrement les transactions par eux-mêmes ou transmettre les transactions à d'autres types de politiques pour un traitement supplémentaire. Les types de politiques peuvent être regroupés en fonction des fonctions qu'ils remplissent, comme l'accès, le routage ou la sécurité.

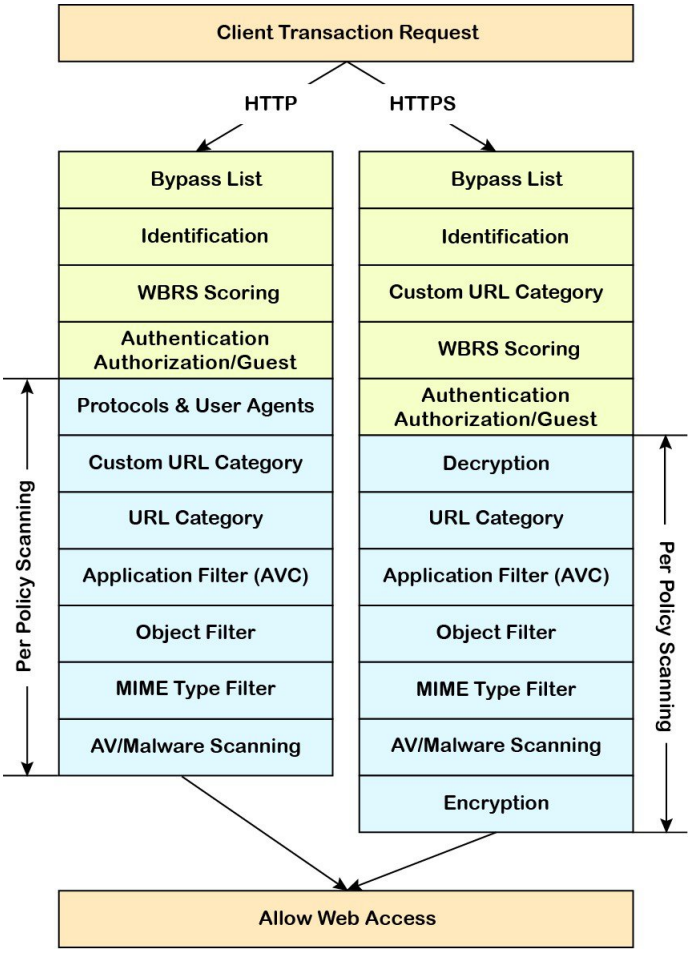
AsyncOS évalue les transactions en fonction des politiques avant d'évaluer les dépendances externes pour éviter toute communication externe inutile de l'appliance. Par exemple, si une transaction est bloquée en

fonction d'une politique qui bloque les URL non classées, la transaction n'échouera pas en fonction d'une erreur DNS.

Traitement des demandes HTTP/HTTPS interceptées

Le diagramme suivant décrit le flux d'une demande Web interceptée lors de son traitement par l'appliance.

Figure 1: Flux de transaction HTTP/HTTPS



Consultez également les diagrammes suivants qui représentent les divers flux de traitement des transactions :

- Profils d'identification et traitement d'authentification – Aucune substitution et substitutions basées sur IP
- Profils d'identification et traitement d'authentification – Substitutions basées sur des témoins
- Figure 2: Flux des transactions de groupe des politiques d'accès, on page 7
- Flux de transaction des groupes de politiques pour les politiques de déchiffrement
- Contrôle du trafic HTTPS

Présentation des tâches de gestion des demandes Web au moyen de politiques

Étape	Liste des tâches pour la gestion des demandes Web au moyen des politiques	Liens vers des rubriques et des procédures connexes
1	Configurer et séquencer les domaines d'authentification	Domaines d'authentification
2	(Pour les proxy en amont) Créez un groupe de proxy.	Création de groupes de serveurs proxy pour les serveurs proxy en amont
2	(Facultatif) Créer des applications clientes personnalisées	Applications client, on page 21
3	(Facultatif) Créer des catégories d'URL personnalisées	Création et modification de catégories d'URL personnalisées
4	Créer des profils d'identification	Classification des utilisateurs et logiciels clients
5	(Facultatif) Créer des plages de temps pour limiter l'accès en fonction de l'heure	Plages de temps et quotas, on page 23
6	Créer et trier des politiques	• Création d'une politique , on page 7 • Ordre des politiques, on page 6

Bonnes pratiques en matière de gestion des demandes Web au moyen de politiques

Si vous souhaitez utiliser les objets utilisateur Active Directory pour gérer les demandes Web, n'utilisez pas les groupes principaux comme critères. Les objets utilisateur Active Directory ne contiennent pas de groupe principal.

Politiques

- Types de politique, on page 4
- Ordre des politiques, on page 6
- Création d'une politique , on page 7

Types de politique

Type de politique	Type de requête	Description	Lien vers la tâche
Accès	• HTTP • HTTPS déchiffré • FTP	Bloquer, autoriser ou rediriger le trafic HTTP, FTP et HTTPS déchiffré entrant. Les politiques d'accès gèrent également le trafic HTTPS chiffré entrant si le proxy HTTPS est désactivé.	Création d'une politique , on page 7
SOCKS	• SOCKS	Autorisez ou bloquez les demandes de communication SOCKS.	Création d'une politique , on page 7
Authentification de l'application	• application	Autorisez ou refusez l'accès à un logiciel-service (SaaS). Utilisez la connexion unique pour authentifier les utilisateurs et renforcer la sécurité en permettant de désactiver rapidement l'accès aux applications. Pour utiliser la fonctionnalité de connexion unique des politiques, vous devez configurer Secure Web Appliance comme fournisseur d'identité et charger ou générer un certificat et une clé pour le logiciel-service.	Création de politiques d'authentification d'applications de logiciel-service (SaaS)
Gestion du protocole HTTPS chiffré	• HTTPS	Déchiffrez, transmettez ou abandonnez les connexions HTTPS. AsyncOS transmet le trafic déchiffré aux politiques d'accès pour traitement ultérieur.	Création d'une politique , on page 7
Sécurité des données	• HTTP • HTTPS déchiffré • FTP	Gérez les chargements de données sur le Web. Les politiques de sécurité des données analysent le trafic sortant pour s'assurer qu'il est conforme aux règles de l'entreprise pour les téléchargements de données, en fonction de sa destination et de son contenu. Contrairement aux politiques DLP externes, qui redirigent le trafic sortant vers des serveurs externes pour l'analyse, les politiques de sécurité des données utilisent Secure Web Appliance pour analyser et évaluer le trafic.	Création d'une politique , on page 7

Type de politique	Type de requête	Description	Lien vers la tâche
DLP (Data Loss Prevention) externe	• HTTP • HTTPS déchiffré • FTP	Envoyez le trafic sortant vers des serveurs exécutant des systèmes DLP tiers, qui l'analysent pour vérifier le respect des règles de l'entreprise pour le chargement de données. Contrairement aux politiques de sécurité des données, qui gèrent également les téléchargements de données, les politiques DLP externes déplacent le travail d'analyse loin de Secure Web Appliance, ce qui libère des ressources sur l'appliance et exploite toutes les fonctionnalités supplémentaires offertes par les logiciels tiers.	Création d'une politique , on page 7
Analyse des programmes malveillants sortants	• HTTP • HTTPS déchiffré • FTP	Bloquer, surveiller ou autoriser les demandes de téléchargement de données susceptibles de contenir des données malveillantes. Empêchez la transmission des programmes malveillants déjà présents sur votre réseau à des réseaux externes.	Création d'une politique , on page 7
Routage	• HTTP • HTTPS • FTP	Faites passer le trafic Web par des proxy en amont ou vers des serveurs de destination. Vous souhaiterez peut-être rediriger le trafic vers des proxys en amont pour préserver la conception de votre réseau existante, pour décharger le traitement de Secure Web Appliance, ou pour tirer parti des fonctionnalités supplémentaires fournies par les systèmes proxy tiers. Si plusieurs proxys en amont sont disponibles, Secure Web Appliance peut utiliser des techniques d'équilibrage de la charge pour leur distribuer des données. Conservez l'adresse IP source du client, remplacez-la par l'adresse IP du proxy Web ou une adresse IP personnalisée à l'aide du profil d'espionnage IP.	Création d'une politique , on page 7

Chaque type de politiques utilise un tableau de politiques pour stocker et gérer ses politiques. Chaque tableau de politique est accompagné d'une politique globale prédéfinie, qui conserve les actions par défaut pour un type de politique. Des politiques supplémentaires définies par l'utilisateur sont créées et ajoutées au tableau de politiques le cas échéant. Les politiques sont traitées dans l'ordre dans lequel elles sont répertoriées dans le tableau des politiques.

Les politiques individuelles définissent les types de demandes des utilisateurs qu'elles gèrent et les actions qu'elles effectuent sur ces demandes. Chaque définition de politique comporte deux sections principales :

- **Profils d'identification et utilisateurs** : Les profils d'identification sont utilisés dans les critères d'appartenance à la politique et sont particulièrement importants car ils contiennent de nombreuses options pour identifier les transactions Web. Ils partagent également de nombreuses propriétés avec les politiques.
- **Niveau avancé** : critères utilisés pour identifier les utilisateurs auxquels la politique s'applique. Un ou plusieurs critères peuvent être précisés dans une politique, et tous doivent correspondre pour que les critères soient remplis.
    - **Protocoles** : permettent le transfert de données entre divers périphériques de réseau comme http, https, ftp, etc.
    - **Ports de proxy** : port numéroté par lequel la demande accède au proxy Web,
    - **Sous-réseaux** : le regroupement logique des périphériques réseau connectés [comme l'emplacement géographique ou le réseau local (LAN)], d'où provient la demande
    - **Plage de temps** : des plages de temps peuvent être créées pour être utilisées dans les politiques afin d'identifier ou d'appliquer des actions aux demandes Web en fonction de l'heure ou du jour où les demandes ont été effectuées. Les plages de temps sont créées en tant qu'unités individuelles.
    - **Catégories d'URL** : les catégories d'URL sont des catégories prédéfinies ou personnalisées de sites Web, tels que les actualités, les affaires, les médias sociaux, etc. Elles peuvent être utilisées pour identifier ou appliquer des actions aux demandes Web.
    - **Agents utilisateurs** : Il s'agit des applications client (comme les programmes de mise à jour et les navigateurs Web) utilisées pour formuler des demandes. Vous pouvez définir des critères de politique basés sur les agents utilisateurs et vous pouvez spécifier des paramètres de contrôle basés sur les agents utilisateurs. Vous pouvez également dispenser les agents utilisateurs de l'authentification, ce qui est utile pour les applications qui ne peuvent pas demander des informations d'authentification. Vous pouvez définir des agents utilisateurs personnalisés, mais vous ne pouvez pas réutiliser ces définitions dans d'autres politiques.

Note Lorsque vous définissez plusieurs critères d'appartenance, la demande du client doit satisfaire à tous les critères pour correspondre à la politique.

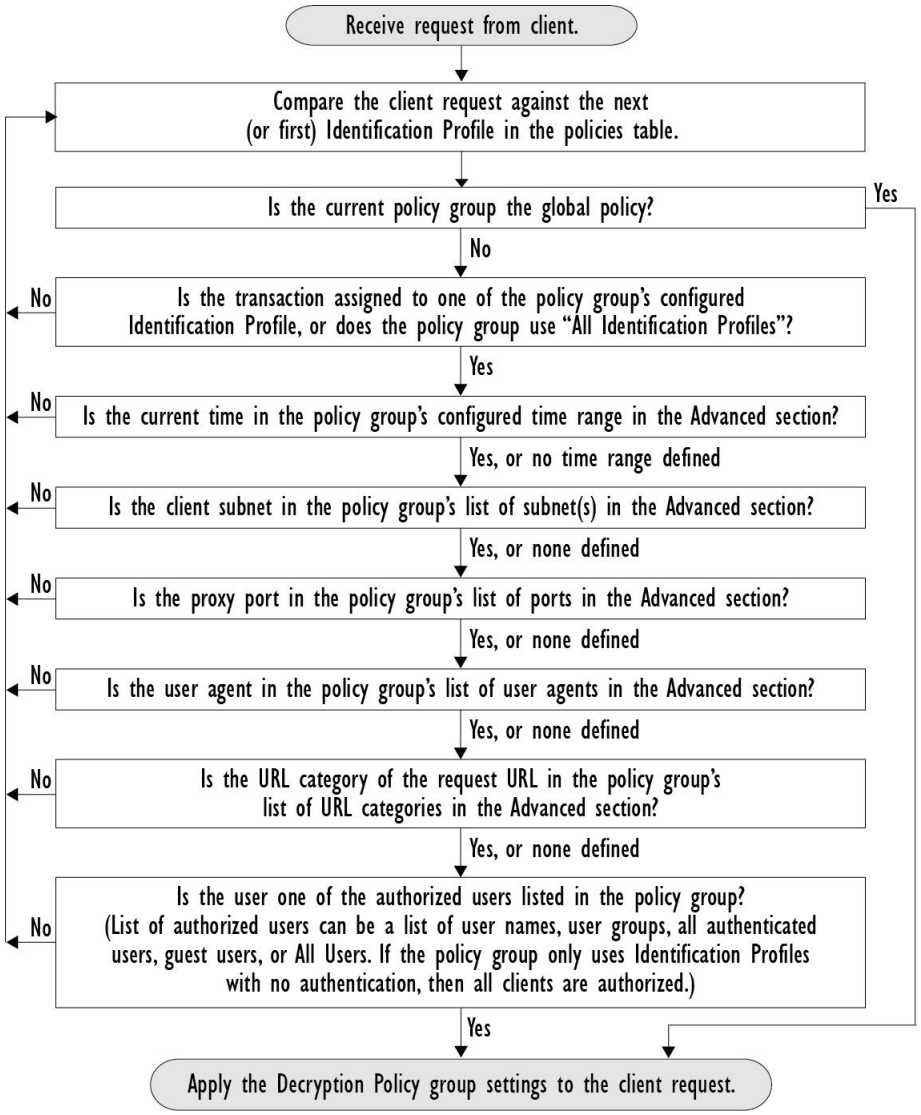
Ordre des politiques

L'ordre dans lequel les politiques sont répertoriées dans un tableau détermine la priorité avec laquelle elles sont appliquées aux demandes Web. Les demandes Web sont vérifiées par rapport aux politiques en commençant en haut du tableau jusqu'à la première politique correspondante. Toutes les politiques en dessous de ce point dans le tableau ne sont pas traitées.

Si aucune politique définie par l'utilisateur ne correspond à une demande Web, la politique globale de ce type de politique est appliquée. Les politiques globales sont toujours placées en dernier dans les tableaux et ne peuvent pas être réordonnées.

Le diagramme suivant décrit le flux d'une demande d'un client dans le tableau des politiques d'accès.

Figure 2: Flux des transactions de groupe des politiques d'accès



Création d'une politique

Before you begin

- Activez le proxy approprié :
  - Proxy Web (pour HTTP, HTTPS déchiffré et FTP)
  - Proxy HTTPS

- Proxy SOCKS

- Créez des profils d'identification associés.
- Comprenez Ordre des politiques, on page 6.
- (HTTPS chiffré uniquement) Chargez ou générez un certificat et une clé.
- (Sécurité des données uniquement) Activez les paramètres des filtres de sécurité des données Cisco.
- (DLP externe uniquement) Définissez un serveur DLP externe.
- (Routage uniquement) Définissez le proxy en amont associé sur Secure Web Appliance.
- (Facultatif) Créez des applications clientes associées.
- (Facultatif) Créez des plages de temps associées. Consultez Plages de temps et quotas, on page 23.
- (Facultatif) Créez des catégories d'URL associées. Consultez Création et modification de catégories d'URL personnalisées.

Étape 1 Dans la section **Policy Settings** (Paramètres de politique), cochez la case **Enable Identity** (Activer l'identité) pour activer cette politique ou pour la désactiver rapidement sans la supprimer.

Étape 2 Attribuez à la politique un **nom** unique.

Étape 3 La **description** est facultative.

Étape 4 Dans la liste déroulante Insert Above (Insérer au-dessus), choisissez l'emplacement de l'affichage de cette politique dans le tableau.

Note Organisez les politiques de sorte que, de haut en bas du tableau, elles aillent de la plus restrictive à la moins restrictive. Consultez Ordre des politiques, on page 6 pour obtenir de plus amples renseignements.

Étape 5 Dans la zone **Policy Expires** (Expiration de la politique), cochez la case **Set Expiration for Policy** (Définir l'expiration de la politique) pour définir le délai d'expiration de la politique. Saisissez la date et l'heure d'expiration de la politique que vous souhaitez définir. Les politiques sont automatiquement désactivées une fois qu'elles ont dépassé le délai d'expiration défini.

Note Le système vérifie les politiques toutes les minutes pour désactiver celles qui expirent dans la minute. Par exemple, si une politique est configurée pour expirer à 11 h 00, elle sera au maximum désactivée à 11 h 01.

La fonctionnalité d'expiration de politique s'applique uniquement aux politiques d'accès, de déchiffrement et de dérivation du trafic Web.

Vous recevrez un courriel trois jours avant l'expiration du contrat et un autre courriel à l'expiration de la politique.

Note Pour recevoir des alertes, vous devez activer les alertes d'expiration des politiques dans **System Administration** > **Alerts** (Administration système > Alertes). Voir la section Alertes d'expiration des politiques.

Vous pouvez également définir le délai d'expiration de la politique à l'aide des appliances Cisco Content Security Management. Les politiques expireront après le délai d'expiration défini, mais ne seront pas affichées comme désactivées dans l'interface graphique utilisateur des appliances Cisco Content Security Management.

Une fois que vous avez défini la fonction d'expiration de la politique, l'expiration se produit en fonction des paramètres d'heure locale de l'appliance.

Étape 6 Dans la section **Policy Member Defined** (Définition des membres de la politique), indiquez la façon dont l'utilisateur et l'appartenance au groupe sont définis : dans la liste Identification Profiles and Users (Profils d'identification et utilisateurs), choisissez l'une des options suivantes :

- **All Identification Profiles** (Tous les profils d'identification) : cette politique s'appliquera à tous les profils existants. Vous devez également définir au moins une option **avancée**.
- **Select One or More Identification Profiles** (Sélectionner un ou plusieurs profils d'identification) : un tableau dans lequel vous pouvez spécifier les profils d'identification individuels s'affiche, une définition de profil d'appartenance par ligne.

Étape 7 Si vous avez choisi **All Identification Profiles** (Tous les profils d'identification) :

a) Indiquez les utilisateurs et les groupes autorisés auxquels cette politique s'applique en sélectionnant l'une des options suivantes :

- **All Authenticated Users** (Tous les utilisateurs authentifiés) : tous les utilisateurs identifiés par authentification ou identification transparente.
- **Selected Groups and Users** (Groupes et utilisateurs sélectionnés) : des utilisateurs et des groupes spécifiés sont utilisés.

  Pour ajouter ou modifier des **étiquettes Groupe sécurisé ISE** et les utilisateurs spécifiés, cliquez sur le lien suivant l'étiquette appropriée. Par exemple, cliquez sur la liste des utilisateurs actuellement spécifiés pour modifier cette liste. Consultez Ajout et modification d'étiquettes Groupe sécurisé pour une politique, on page 11 pour obtenir de plus amples renseignements.

  Si vous utilisez ISE, vous pouvez ajouter ou modifier des étiquettes Groupe sécurisé ISE. Cette fonction n'est pas prise en charge dans les déploiements ISE-PIC. Pour ajouter ou modifier des **groupes ISE** spécifiés, cliquez sur le lien suivant l'étiquette. Cette option est spécifique à ISE-PIC.
- **Guests** (Invités) : utilisateurs connectés en tant qu'invités et utilisateurs dont l'authentification a échoué.
- **All Users** (Tous les utilisateurs) : tous les clients, qu'ils soient authentifiés ou non. Si cette option est sélectionnée, au moins une option **avancée** doit également être définie.

Étape 8 Si vous avez choisi **Select One or More Identification Profiles** (Sélectionner un ou plusieurs profils d'identification), un tableau de sélection de profils s'affiche.

a) Choisissez un profil d'identification dans la liste déroulante Select Identification Profile (Sélectionner un profil d'identification) dans la colonne Identification Profiles (Profils d'identification).

b) Indiquez les utilisateurs et les groupes autorisés auxquels cette politique s'applique :

- **All Authenticated Users** (Tous les utilisateurs authentifiés) : tous les utilisateurs identifiés par authentification ou identification transparente.
- **Selected Groups and Users** (Groupes et utilisateurs sélectionnés) : des utilisateurs et des groupes spécifiés sont utilisés.

  Pour ajouter ou modifier les étiquettes Groupe sécurisé et les utilisateurs spécifiés, cliquez sur le lien suivant l'étiquette appropriée. Par exemple, cliquez sur la liste des utilisateurs actuellement spécifiés pour modifier cette liste. Consultez Ajout et modification d'étiquettes Groupe sécurisé pour une politique, on page 11 pour obtenir de plus amples renseignements.
- **Guests** (Invités) : utilisateurs connectés en tant qu'invités et utilisateurs dont l'authentification a échoué.

c) Pour ajouter une ligne au tableau de sélection de profils, cliquez sur **Add Identification Profile** (Ajouter un profil d'identification). Pour supprimer une ligne, cliquez sur l'icône de corbeille sur cette ligne.

Répétez les étapes (a) à (c) selon les besoins pour ajouter tous les profils d'identification souhaités.

Étape 9 Développez la section **Advanced** (Niveau avancé) pour définir des critères d'appartenance au groupe supplémentaires. [Cette étape peut être facultative selon la sélection dans la section **Policy Member Definition** (Définition des membres d'une politique). En outre, certaines des options suivantes ne seront pas disponibles, selon le type de politique que vous configurez.] .

Option avancée	Description
Protocols (Protocoles)	Sélectionnez les protocoles auxquels cette politique s'appliquera. **All others** (Tous les autres) désigne tout protocole non sélectionné. Si le profil d'identification associé s'applique à des protocoles spécifiques, la présente politique s'applique à ces mêmes protocoles
Proxy Ports (Ports du proxy)	Applique cette politique uniquement au trafic qui utilise des ports spécifiques pour accéder au proxy Web. Saisissez un ou plusieurs numéros de port en séparant les ports par des virgules. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. **Note** Si le profil d'identification associé s'applique uniquement à des ports proxy spécifiques, vous ne pouvez pas saisir ces ports proxy ici.
Subnets (Sous-réseaux)	Applique cette politique uniquement au trafic sur des sous-réseaux spécifiques. Sélectionnez **Define subnets** (Définir des sous-réseaux) et saisissez les sous-réseaux spécifiques, en les séparant par des virgules. Laissez l'option **Use subnets from selected Identities** (Utiliser des sous-réseaux à partir d'identités sélectionnées) si vous ne souhaitez pas de filtrage supplémentaire par sous-réseau. **Note** Si l'identité associée s'applique à des sous-réseaux spécifiques, vous pouvez restreindre davantage l'application de cette politique à un sous-ensemble d'adresses auxquelles l'identité s'applique.
Time Range (Plage de temps)	Vous pouvez appliquer des plages de temps pour l'appartenance à la politique : • Time Range (Plage de temps) : choisissez une plage de temps définie précédemment (Plages de temps et quotas, on page 23). • Match Time Range (Correspondre à la plage de temps) : utilisez cette option pour indiquer si cette plage de temps est inclusive ou exclusive. En d'autres termes, veillez à ce que les données correspondent uniquement à la plage spécifiée ou à tout intervalle hormis la plage spécifiée.
URL Categories (Catégories d'URL)	Vous pouvez restreindre l'appartenance à la politique par destinations (URL) spécifiques et par catégories d'URL. Sélectionnez toutes les catégories personnalisées et prédéfinies souhaitées. Consultez Création et modification de catégories d'URL personnalisées pour en savoir plus sur les catégories personnalisées.

Option avancée	Description

User Agents (Agents utilisateur)	Vous pouvez sélectionner des agents utilisateur spécifiques et définir des agents personnalisés à l'aide d'expressions régulières dans le cadre de la définition de l'appartenance à cette politique.
	• **Common User Agents** (Agents utilisateur communs)
	  • **Browsers** (Navigateurs) : développez cette section pour sélectionner différents navigateurs Web.
	  • **Others** (Autres) : développez cette section pour sélectionner des agents spécifiques autres que les navigateurs, tels que les programmes de mise à jour d'applications.
	• **Custom User Agents** (Agents utilisateur personnalisés) : vous pouvez entrer une ou plusieurs expressions régulières, une par ligne, pour définir des agents utilisateur personnalisés.
	• **Match User Agents** (Correspondre aux agents utilisateur) : utilisez cette option pour indiquer si ces spécifications d'agents utilisateur sont inclusives ou exclusives. Autrement dit, si la définition de l'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateur sélectionnés.

Ajout et modification d'étiquettes Groupe sécurisé pour une politique

Pour modifier la liste des étiquettes Groupe sécurisé affectées à un profil d'identification particulier dans une politique, cliquez sur le lien à côté de l'étiquettes Groupe sécurisé ISE dans la liste des groupes et des utilisateurs sélectionnés de la page Add/Edit Policy (Ajouter/modifier une politique). (Consultez Création d'une politique , on page 7.) Ce lien est soit « No tags entered » (Aucune étiquette saisie), soit une liste des étiquettes actuellement attribuées. Le lien ouvre la page Add/Edit Secure Group Tags (Ajouter/modifier des étiquettes Groupe sécurisé).

Toutes les étiquettes Groupe sécurisé actuellement affectées à cette politique sont répertoriées dans la section des étiquettes Groupe sécurisé autorisées. Toutes les balises SGT disponibles sur le serveur ISE connecté sont répertoriées dans la section de recherche des balises SGT.

Étape 1 Pour ajouter une ou plusieurs étiquettes Groupe sécurisé à la liste des étiquettes Groupe sécurisé autorisées, sélectionnez les entrées souhaitées dans la section de recherche d'étiquettes Groupe sécurisé , puis cliquez sur **Add** (Ajouter).

Note
- Les balises SGT déjà ajoutées sont surlignées en vert. Pour trouver rapidement une balise SGT spécifique dans la liste des balises disponibles, entrez une chaîne de texte dans le champ **Search** (Recherche).
- Lorsqu'un Secure Web Appliance est connecté à ISE/ISE-PIC, les balises SGT par défaut d'ISE/ISE-PIC sont également affichées. Aucun utilisateur ne sera affecté à ces balises SGT. Assurez-vous de sélectionner les balises SGT adéquates.

Étape 2 Pour supprimer une ou plusieurs étiquettes Groupe sécurisé de la liste des étiquettes Groupe sécurisé autorisées, sélectionnez ces entrées, puis cliquez sur **Delete** (Supprimer).

Étape 3 Cliquez sur Done (Terminé) pour revenir à la page Add/Edit Group (Add/Modifier un groupe).

What to do next

Thèmes connexes

- Plages de temps et quotas, on page 23
- Utilisation des applications clientes dans les politiques, on page 22

Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage

Vous pouvez configurer la manière dont le proxy Web transfère le trafic Web et les demandes à partir de l'adresse IP source en configurant la destination du routage et le profil d'usurpation d'adresses IP dans les politiques de routage.

Note

- La politique de routage globale est activée par défaut même si un groupe de proxys en amont n'est pas configuré sur l'appliance.
- Les profils d'usurpation d'adresses IP ne sont pas liés à la destination de routage et peuvent être configurés indépendamment.
- La politique de routage peut être activée sans configurer un proxy en amont.

Note Pour configurer un groupe de proxy en amont pour une politique de routage dans l'appliance de gestion de la sécurité, enregistrez le fichier de configuration de Secure Web Appliance et importez-le sur l'appliance de gestion de la sécurité. Sinon, l'appliance de gestion de la sécurité affiche le proxy en amont comme «Not Found » (Introuvable) et la politique de routage sera désactivée après l'envoi de la configuration.

Étape 1 Choisissez **Web Security Manager** > **Routing Policies** (Web Security Manager > Politiques de routage).

Étape 2 Dans la page **Routing Policies** (Politiques de routage), cliquez sur le lien sous la colonne **Routing Destination** (Destination de routage) correspondant à la politique de routage que vous souhaitez configurer pour le groupe de proxy en amont.

Étape 3 Choisissez un groupe de proxy en amont approprié parmi les groupes suivants pour la politique sélectionnée :

Action	Description
Use Global Policy Settings (Utiliser les paramètres de la politique globale)	Le proxy Web utilise les paramètres définis dans la politique globale. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. Par défaut, la destination de routage pour la politique de routage globale est renseignée par **Direct Connection** (Connexion directe). S'applique uniquement aux groupes de politiques définies par l'utilisateur.
Direct Connection (Connexion directe)	Le proxy Web transfère le trafic Web directement vers son serveur Web de destination.

Action	Description
Custom upstream proxy group (Groupe de proxy en amont personnalisé)	Le proxy Web redirige le trafic Web vers un groupe de proxy externe en amont. Pour plus d'informations sur la création de groupes de proxy en amont, consultez Serveurs proxy en amont.

Étape 4 Dans la page **Routing Policies** (Politiques de routage),cliquez sur le lien sous la colonne **IP Spoofing** (Usurpation d'adresses IP) pour la politique de routage dont vous souhaitez configurer le profil d'usurpation d'adresses IP.

Étape 5 Choisissez un profil d'usurpation d'adresse IP approprié pour la politique sélectionnée parmi les suivantes :

Action	Description
Use Global Policy Settings (Utiliser les paramètres de la politique globale)	Le proxy Web utilise les paramètres définis dans la politique globale. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. Par défaut, l'usurpation d'adresses IP est désactivée pour la politique de routage globale. S'applique uniquement aux groupes de politiques définies par l'utilisateur.
Do No Use IP Spoofing (Ne pas utiliser d'usurpation d'adresses IP)	Le proxy Web modifie l'adresse IP de la source de la demande pour qu'elle corresponde à sa propre adresse afin d'augmenter la sécurité.
Use Client IP (Utiliser l'adresse IP du client)	Le proxy Web conserve l'adresse source de sorte qu'elle semble provenir du client source plutôt que de Secure Web Appliance.
Custom spoofing profile name (Nom de profil d'usurpation personnalisé)	Le proxy Web remplace l'adresse IP de la source de la demande par une adresse IP personnalisée définie dans le nom de profil d'usurpation d'adresses IP personnalisé sélectionné.

Étape 6 **Envoyez** et **validez** vos modifications.

What to do next

Thèmes connexes

- Serveurs proxy en amont
- Usurpation d'adresses IP de proxy Web

Configuration des politiques

Chaque ligne d'un tableau de politiques représente une définition de politique et chaque colonne de l'affichage actuel contient un lien vers une page de configuration pour cet élément de la politique.

Note Parmi les composants de configuration de politique suivants, vous pouvez spécifier l'option « Warn » (Avertir) uniquement avec le filtrage d'URL.

Option	Description
Protocols and User Agents (Protocoles et agents utilisateur)	Utilisé pour contrôler l'accès aux protocoles et configurer le blocage pour des applications client particulières, telles que les clients de messagerie instantanée, les navigateurs Web et les services de téléphonie sur Internet. Vous pouvez également configurer l'appliance pour tunneliser les demandes HTTP CONNECT sur des ports spécifiques. Lorsque la tunnellisation est activée, l'appliance fait passer le trafic HTTP par des ports spécifiés sans l'évaluer.
URL Filtering (Filtrage URL)	AsyncOS pour le Web vous permet de configurer la façon dont l'appliance gère une transaction en fonction de la catégorie d'URL d'une demande HTTP ou HTTPS particulière. À l'aide d'une liste de catégories prédéfinies, vous pouvez choisir de bloquer, de surveiller, d'alerter ou de définir des filtres basés sur les quotas ou le temps. Vous pouvez également créer des catégories d'URL personnalisées, puis choisir de bloquer, rediriger, autoriser, surveiller, avertir ou appliquer des filtres sur la base de quotas ou du temps pour les sites Web dans les catégories personnalisées. Voir Création et modification de catégories d'URL personnalisées pour plus d'informations sur la création de catégories d'URL personnalisées. En outre, vous pouvez ajouter des exceptions au blocage de contenu intégré ou référencé.
Applications	Le moteur de contrôle et de visibilité des applications (AVC) est un composant de la politique d'utilisation acceptable qui inspecte le trafic Web pour mieux comprendre et contrôler le trafic Web utilisé pour les applications. L'appliance autorise la configuration du proxy Web de manière à bloquer ou autoriser des applications par types d'applications et par application individuelle. Vous pouvez également appliquer des contrôles à des comportements d'applications particuliers, tels que les transferts de fichiers, au sein d'une application particulière. Voir Gestion de l'accès aux applications Web pour les informations de configuration.
Objects (Objets)	Ces options vous permettent de configurer le proxy Web pour bloquer les téléchargements de fichiers en fonction des caractéristiques du fichier, telles que la taille du fichier, le et le type MIME. Un objet est, généralement, tout élément qui peut être sélectionné, chargé, téléchargé et manipulé individuellement. Voir Politiques d'accès : blocage d'objets, on page 16 pour plus d'informations sur la définition d'objets bloqués

Option	Description
Anti-Malware and Reputation (Protection contre les programmes malveillants et réputation)	Les filtres de réputation Web permettent d'affecter un score de réputation de sites Web à une URL afin de déterminer sa probabilité de contenir des programmes malveillants basés sur l'URL. L'analyse de protection contre les programmes malveillants détecte et bloque les menaces de programmes malveillants sur le Web. Cisco Secure Endpoint identifie les programmes malveillants dans les fichiers téléchargés. La politique relative aux programmes malveillants et à la réputation hérite des paramètres globaux respectifs de chaque composant. Dans **Security Services** > **Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation), les catégories de programmes malveillants peuvent être personnalisées de manière à les surveiller ou à les bloquer en fonction des verdicts des analyses des programmes malveillants, et des seuils de score de réputation Web peuvent être personnalisés. Les catégories de programmes malveillants peuvent être personnalisées davantage dans une politique. Il existe également des paramètres globaux pour la réputation des fichiers et les services d'analyse. Pour plus de renseignements, consultez les sections Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès et Configuration des fonctionnalités d'analyse et de réputation de fichiers.
HTTP ReWrite Profile (Profil de réécriture HTTP)	Vous pouvez configurer des profils d'en-tête personnalisés pour les requêtes HTTP et créer plusieurs en-têtes dans un profil de réécriture d'en-tête. La fonction de profil de réécriture d'en-tête permet à l'appliance de transmettre les informations sur l'utilisateur et le groupe à un autre périphérique en amont une fois l'authentification réussie. Le proxy en amont considère l'utilisateur comme authentifié, contourne l'authentification supplémentaire et fournit un accès à l'utilisateur en fonction des politiques d'accès définies. Consultez En-têtes personnalisés du proxy Web par politique.
Clone Policy (Clonage de politique)	Si une politique existante comporte la plupart des paramètres que vous souhaitez dans une nouvelle politique, vous pouvez gagner du temps en clonant la politique existante, puis en la modifiant. Bien que la politique clonée partage les mêmes attributs de regroupement, elle possède sa propre identité unique, telle que le nom d'affichage, l'adresse IP, l'hôte et le nom de domaine. Les politiques suivantes avec l'option de clonage dans Cisco Secure Web Appliance peuvent également être gérées par Cisco Secure Email and Web Manager (SMA) : • Accès • Déchiffrement • Identification • Routage **Note** Vous ne pouvez copier qu'une seule politique par instance.
Clone Policy (Supprimer)	Supprime la politique créée.

Politiques d'accès : blocage d'objets

Vous pouvez utiliser les options de la page Politiques d'accès : Objets pour bloquer les téléchargements de fichiers en fonction des caractéristiques du fichier, telles que la taille du fichier, le type de fichier et le type MIME. Un objet est, généralement, tout élément qui peut être sélectionné, chargé, téléchargé et manipulé individuellement.

Vous pouvez préciser un certain nombre de types d'objets à bloquer par chaque politique d'accès et par la politique globale. Ces types d'objets comprennent les archives, les types de documents, le code exécutable, le contenu de la page Web, etc.

Étape 1 Dans la page des politiques d'accès [**Web Security Manager** > **Access Policies** (Web Security Manager > Politiques d'accès)], cliquez sur le lien dans la colonne **Objects** (Objets) de la ligne représentant la politique que vous souhaitez modifier.

Étape 2 Choisissez le type de blocage d'objet souhaité pour cette politique d'accès :

- **Use Global Policy Objects Blocking Settings** (Utiliser les paramètres de blocage des objets de politique globale) : cette politique utilise les paramètres de blocage d'objets définis pour la politique globale; ces paramètres sont affichés en mode lecture seule. Modifiez les paramètres de la politique globale pour les modifier.
- **Define Custom Objects Blocking Settings** (Définir les paramètres de blocage d'objets personnalisés) : vous pouvez modifier tous les paramètres de blocage d'objets pour cette politique.
- **Disable Object Blocking for this Policy** (Désactiver le blocage d'objets pour cette politique) : le blocage d'objets est désactivé pour cette politique; aucune option de blocage d'objet ne s'affiche.

Étape 3 Si vous avez choisi **Define Custom Objects Blocking Settings** (Définir les paramètres de blocage des objets personnalisés) à l'étape précédente, activez et désélectionnez les options de blocage d'objets dans la page Access Policies: Objects (Politiques d'accès : Objets), selon vos besoins.

Object Size (Taille de l'objet)	Vous pouvez bloquer des objets en fonction de leur taille de téléchargement : • **Taille maximale de téléchargement HTTP/HTTPS** : indiquez la taille maximale d'objet pour le téléchargement HTTP/HTTPS (les objets plus grands que cette taille seront bloqués) ou indiquez qu'il n'y a pas de taille maximale pour le téléchargement d'objet via HTTP/HTTPS. • **Taille** maximale de téléchargement FTP : indiquez la taille d'objet maximale pour le téléchargement FTP (les objets plus grands que cette taille seront bloqués) ou indiquez qu'il n'y a pas de taille maximale pour le téléchargement d'objets par FTP.
Type d'objet de blocage	
Archives	Développez cette section pour sélectionner les types de fichiers d'archive à bloquer. Cette liste comprend les types d'archives tels que ARC, BinHex et Stuffit.

Inspectable Archives (Archives pouvant être inspectées)	Développez cette section pour choisir d'**autoriser**, de **bloquer** ou d'**inspecter** des types spécifiques de fichiers d'archive analysables. Les archives pouvant être inspectées sont des fichiers d'archives ou des fichiers compressés que Secure Web Appliance peut gonfler pour inspecter chacun des fichiers qu'il contient afin d'appliquer la politique de blocage des types de fichiers. La liste des archives pouvant être inspectées comprend des types d'archives tels que 7zip, Microsoft CAB, RAR et TAR.
	
	Les points suivants s'appliquent à l'inspection des archives :
	• Seuls les types d'archives marqués **Inspect** (Inspecter) seront gonflés et inspectés.
	• Une seule archive à la fois est inspectée. Les archives pouvant être inspectées simultanément ne peuvent pas être inspectées.
	• Si une archive inspectée contient un type de fichier auquel l'action de blocage est affectée par la politique actuelle, l'archive entière sera bloquée, quels que soient les types de fichiers autorisés qu'elle peut contenir.
	• Une archive inspectée qui contient un type d'archive non pris en charge sera marquée comme « non analysable ». Si elle contient un type d'archive bloqué, elle sera bloquée.
	• Les archives protégées par mot de passe et chiffrées ne sont pas prises en charge et seront marquées comme « non analysables ».
	• Une archive pouvant être inspectée qui est incomplète ou corrompue est marquée comme « non analysable ».
	• La valeur **DVS Engine Object Scanning Limits** (Limites d'analyse des objets du moteur DVS) spécifiées pour les paramètres globaux **Anti-Malware and Reputation** (Programmes malveillants et de réputation) s'applique également à la taille d'une archive pouvant être inspectée; un objet dépassant cette taille est marqué comme « unscannable » (non analysable). Consultez Activation des filtres contre les programmes malveillants et de réputation pour obtenir des renseignements sur cette limite de taille d'objet.
	• Une archive pouvant être inspectée marquée comme « unscannable » (non analysable) peut être entièrement bloquée ou autorisée.
	• Lorsque les politiques d'accès sont configurées pour bloquer les types MIME personnalisés et que l'inspection des archives est activée :
	  • Si l'appliance télécharge directement un fichier avec le type MIME personnalisé dans l'en-tête content-type, l'accès est bloqué.
	  • Si le même fichier fait partie d'un fichier ZIP/d'archive, l'appliance inspecte l'archive et détermine le type MIME en fonction de sa propre évaluation MIME. Si le type MIME évalué par le moteur de l'appliance ne correspond pas au type MIME personnalisé configuré, le contenu n'est pas bloqué.
	• L'appliance peut inspecter les archives configurées, mais elle est limitée par l'inspection de certaines archives telles que RAR et 7-Zip.
	
	Consultez Paramètres d'inspection des archives, à la page 18 pour obtenir des renseignements sur la configuration de l'inspection des archives.

Document Types (Types de documents)	Développez cette section pour sélectionner les types de documents texte à bloquer. Cette liste comprend les types de documents tels que FrameMaker, Microsoft Office et PDF.
Executable Code (Code exécutable)	Développez cette section pour sélectionner les types de code exécutable à bloquer. La liste comprend Java Applet, UNIX Executable et Windows Executable.
Installers (Programmes d'installation)	Les types de programmes d'installation à bloquer; la liste comprend les ensembles UNIX/LINUX.
Media (Médias)	Types de fichiers multimédias à bloquer. La liste comprend les formats de traitement d'image audio, vidéo et photo (TIFF/PSD).
P2P Metafiles (Métafichiers P2P)	Cette liste comprend les liens BitTorrent Links (`.torrent`).
Web Page Content (Contenu de page Web)	Cette liste comprend les éléments Flash et les images.
Miscellaneous (Divers)	Cette liste comprend les données de calendrier.
Custom MIME Types (Types MIME personnalisés)	Vous pouvez définir des objets/fichiers supplémentaires à bloquer en fonction du type MIME. Entrez un ou plusieurs types MIME dans le champ **Block Custom MIME Types** (Bloquer les types MIME personnalisés), un par ligne.

Étape 4 Cliquez sur **Submit** (Soumettre).

Paramètres d'inspection des archives

Vous pouvez autoriser, bloquer ou inspecter des types spécifiques d'archives pouvant être inspectées pour les politiques d'accès individuelles. Les archives pouvant être inspectées sont des fichiers d'archives ou des fichiers compressés que Secure Web Appliance peut gonfler pour inspecter chacun des fichiers qu'il contient afin d'appliquer la politique de blocage des types de fichiers. Consultez Politiques d'accès : blocage d'objets, à la page 16 pour en savoir plus sur la configuration de l'inspection des archives pour les politiques d'accès individuelles.

Remarque Lors de l'inspection des archives, les objets imbriqués sont écrits sur le disque pour examen. La quantité d'espace disque qui peut être occupée à tout moment pendant l'inspection des fichiers est de 1 Go. Tout fichier d'archive dépassant cette taille maximale d'utilisation du disque sera marqué comme non analysable.

La page Acceptable Use Controls de Secure Web Appliancefournit des paramètres d'archives pouvant être inspectées à l'échelle du système; c'est-à-dire que ces paramètres s'appliquent à l'extraction et à l'inspection des archives lorsque cela est activé dans une politique d'accès.

Étape 1 Choisissez **Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Cliquez sur le bouton **Edit Archive Settings** (Modifier les paramètres d'archives).

Étape 3 Modifiez les paramètres des archives pouvant être inspectées au besoin.

- **Maximum Encapsulated Archive Extractions** (Nombre maximal d'extractions d'archives encapsulées) : nombre maximal d'archives « encapsulées » à extraire et à inspecter. C'est-à-dire la profondeur maximale pour l'inspection d'une archive contenant d'autres archives pouvant être inspectées. Une archive encapsulée est une archive contenue dans un autre fichier d'archive. Cette valeur peut être comprise entre zéro et cinq; le décompte de profondeur commence à un avec le premier fichier imbriqué.

  L'archive externe est considérée comme le fichier zéro. Si l'archive contient des fichiers imbriqués au-delà de cette valeur imbriquée maximale, l'archive est marquée comme non analysable. Notez que cela aura une incidence sur les performances.

- **Block Uninspectable Archives** (Bloquer les archives non inspectables) : si cette case est cochée, Secure Web Appliance bloquera les archives qu'il n'a pas réussi à exploser et à inspecter.

Étape 4 **Envoyez** et **validez les modifications**.

Bloquer, autoriser ou rediriger les demandes de transactions

Le proxy Web contrôle le trafic Web en fonction des politiques que vous créez pour les groupes de demandes de transaction.

- **Allow (Autoriser).** Le proxy Web permet la connexion sans interruption. Les connexions autorisées n'ont peut-être pas été analysées par le moteur DVS.
- **Block (Bloquer).** Le proxy Web n'autorise pas la connexion et affiche plutôt une page de notification à l'utilisateur final expliquant le motif du blocage.
- **Redirect (Rediriger).** Le proxy Web n'autorise pas la connexion au serveur de destination demandé à l'origine et se connecte plutôt à une autre URL spécifiée; consultez Redirection du trafic dans les politiques d'accès.

Note Les actions précédentes sont les actions finales que le proxy Web exécute sur une demande du client. L'action Monitor (Superviser) que vous pouvez configurer pour les politiques d'accès n'est pas une action finale.

En général, différents types de politiques contrôlent le trafic en fonction du protocole de transport.

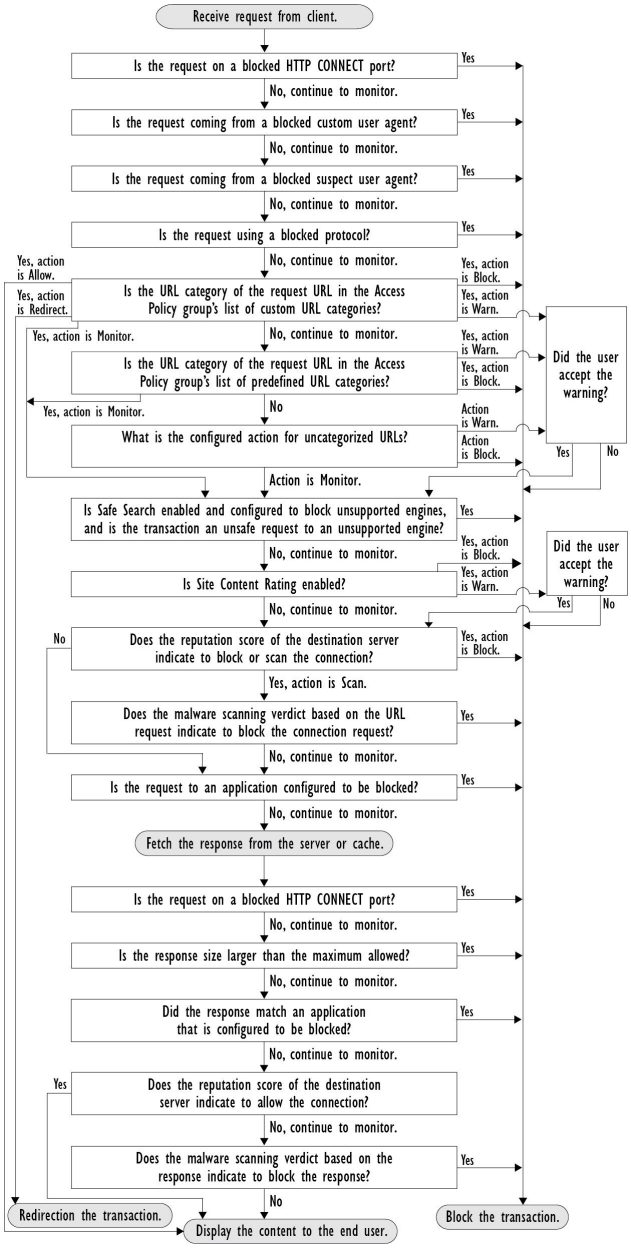
Type de politique	**Protocols (Protocoles)**				**Actions prises en charge**			
	HTTP	HTTPS	FTP	SOCKS	Block (Bloquer)	Allow (Autoriser)	Rediriger	Monitor (Superviser)
Accès	x	x	x		x	x	x	x
SOCKS				x	x	x		
SaaS	x	x						
Déchiffrement	x	x						x
Sécurité des données	x	x	x		x			x

Type de politique	Protocols (Protocoles)				Actions prises en charge			
DLP externe	x	x	x				x	
Analyse des programmes malveillants sortants	x	x	x		x			x
Routage	x	x	x				x	

Note La politique de déchiffrement prévaut sur la politique d'accès.

Le diagramme suivant montre comment le proxy Web détermine l'action à effectuer sur une demande après avoir affecté une politique d'accès particulière à la demande. Le score de réputation Web du serveur de destination est évalué une seule fois, mais le résultat est appliqué à deux étapes différentes dans le flux de décision.

Figure 3: Application des actions de politique d'accès



Applications client

À propos des applications clientes

Les applications clientes (comme un navigateur Web) sont utilisées pour formuler des demandes. Vous pouvez définir l'appartenance aux politiques en fonction des applications clientes, et vous pouvez spécifier des

paramètres de contrôle et dispenser les applications clientes de l'authentification, ce qui est utile pour les applications qui ne peuvent pas demander des informations d'authentification.

Utilisation des applications clientes dans les politiques

Définition de l'appartenance à la politique à l'aide des applications clientes

Étape 1 Choisissez un type de politique dans le menu Web Security Manager.

Étape 2 Cliquez sur un nom de politique dans le tableau des politiques.

Étape 3 Développez la section Advanced (Niveau avancé) et cliquez sur le lien dans le champ Client Applications (Applications clientes).

Étape 4 Définissez une ou plusieurs des applications clientes :

Option	Méthode
Choose a predefined client application (Choisir une application cliente prédéfinie)	Développez les sections Browser (Navigateur) et Other (Autre) et cochez les cases de l'application cliente requise. **Tip** Choisissez uniquement les options Any Version (Toute version) lorsque cela est possible, car cela offre de meilleures performances que d'avoir plusieurs sélections.
Define a custom client application (Définir une application cliente personnalisée)	Entrez une expression régulière appropriée dans le champ Custom Client Applications (Applications clientes personnalisées). Saisissez des expressions régulières supplémentaires sur les nouvelles lignes, le cas échéant. **Tip** Cliquez sur **Exemples de modèles d'applications client** pour obtenir des exemples d'expressions régulières.

Étape 5 (Facultatif) Cliquez sur le bouton d'option Match All Except The Selected **Client Applications** Definitions (Correspondre à toutes les définitions des applications clients hormis celles qui ont été sélectionnées) pour baser l'appartenance à la politique sur toutes les applications clientes, à l'**exception** de celles que vous avez définies.

Étape 6 Cliquez sur **Done** (Terminé).

Définition des paramètres de contrôle des politiques à l'aide des applications clientes

Étape 1 Choisissez un type de politique dans le menu Web Security Manager.

Étape 2 Recherchez le nom de la politique requise dans le tableau des politiques.

Étape 3 Cliquez sur le lien de la cellule dans la colonne Protocols and Client Applications (Protocoles et applications clientes) sur la même ligne.

Étape 4 Choisissez **Define Custom Settings** (Définir des paramètres personnalisés) dans la liste déroulante du volet Edit Protocols and Client Applications Settings (Modifier les protocoles et les paramètres des applications clientes) (si ce n'est pas déjà fait).

Étape 5 Entrez une expression régulière dans le champ Custom Client Applications (Applications clientes personnalisées) qui correspond à l'application cliente que vous souhaitez définir. Saisissez des expressions régulières supplémentaires sur les nouvelles lignes, le cas échéant.

Tip Cliquez sur **Example Client Application Patterns** (Exemple de modèles d'application cliente) pour obtenir des exemples d'expressions régulières.

Étape 6 Envoyez et validez vos modifications.

Dispense d'authentification pour les applications clientes

Procedure

	Command or Action	Purpose
Étape 1	Créez un profil d'identification qui ne nécessite pas d'authentification.	Classification des utilisateurs et logiciels clients
Étape 2	Définissez l'appartenance au profil d'identification comme application cliente à dispenser.	Utilisation des applications clientes dans les politiques, on page 22
Étape 3	Placez le profil d'identification au-dessus de tous les autres profils d'identification dans le tableau des politiques qui nécessitent une authentification.	Ordre des politiques, on page 6

Plages de temps et quotas

Vous pouvez appliquer des plages de temps et des quotas de temps et de volumes pour établir des politiques d'accès et de déchiffrement à restreindre quand un utilisateur a un accès, ainsi que sa durée de connexion ou son volume de données maximal (également appelé « quota de bande passante »).

- Plages de temps pour les politiques et contrôles d'utilisation acceptable, on page 23
- Quotas de temps et de volume, on page 24

Plages de temps pour les politiques et contrôles d'utilisation acceptable

Les plages de temps sont des périodes définies pendant lesquelles les politiques et les contrôles d'utilisation acceptable s'appliquent.

Note Vous ne pouvez pas utiliser des plages de temps pour définir les heures auxquelles les utilisateurs doivent s'authentifier. Les exigences d'authentification sont définies dans les profils d'identification, qui ne prennent pas en charge les plages de temps.

- Création d'une plage de temps, on page 24

Création d'une plage de temps

Étape 1 Choisissez **Web Security Manager** > **Define Time Ranges and Quotas** (Web Security Manager > Définir les plages de temps et les quotas).

Étape 2 Cliquez sur **Add Time Range** (Ajouter la plage de temps).

Étape 3 Attribuez un nom à la plage de temps.

Étape 4 Choisissez une option de **Time Zone** (Fuseau horaire) :

- **Use Time Zone Setting From Appliance** (Utiliser les paramètres de fuseau horaire de l'appliance) : utilisez le même fuseau horaire que Secure Web Appliance.
- **Specify Time Zone for this Time Range** (Indiquer le fuseau horaire pour cette plage horaire) : définissez un fuseau horaire différent, soit en tant que décalage GMT ou en tant que région, pays et un fuseau horaire spécifique dans ce pays.

Étape 5 Cochez une ou plusieurs cases **Day of Week** (Jour de la semaine).

Étape 6 Sélectionnez une option **Time of Day** (Heure de la journée) :

- **All Day** (Toute la journée) : utilisez la période complète de 24 heures.
- **From** (Du) et **To** (Au) : définissez une plage d'heures spécifique : saisissez une heure de début et une heure de fin au format HH:MM (format 24 heures).

Tip Chaque plage de temps définit une heure de début et une limite de temps de fin. Par exemple, la saisie de 8:00 à 17:00 correspond à 8:00:00 à 16:59:59, mais pas à 17:00:00. Vous devez définir minuit entre 00:00 pour l'heure de début et 24:00 pour une heure de fin.

Étape 7 Envoyez et validez vos modifications.

Quotas de temps et de volume

Les quotas permettent à un utilisateur de continuer à accéder à une ressource Internet (ou à une classe de ressources Internet) jusqu'à ce qu'il ait épuisé le volume de données ou la limite de temps imposée. AsyncOS applique des quotas définis au trafic HTTP, HTTPS et FTP.

Lorsqu'un utilisateur approche de son quota de temps ou de volume, AsyncOS affiche d'abord un avertissement, puis une page de blocage.

Veuillez noter les points suivants concernant l'utilisation des quotas de temps et de volume :

- Si AsyncOS est déployé en mode transparent et que le proxy HTTPS est désactivé, il n'y a pas d'écoute sur le port 443 et les demandes sont abandonnées. Il s'agit d'un comportement standard. Si AsyncOS est déployé en mode explicite, vous pouvez définir des quotas dans vos politiques d'accès.

  Lorsque le proxy HTTPS est activé, les actions possibles sur une demande sont la transmission, le déchiffrement, la suppression ou la supervision. Dans l'ensemble, les quotas dans les politiques de déchiffrement ne s'appliquent qu'aux catégories d'intercommunication.

  Avec l'interconnexion, vous aurez également la possibilité de définir des quotas pour le trafic du tunnel. Avec déchiffrement, cette option n'est pas disponible, car les quotas configurés dans la politique d'accès seront appliqués au trafic déchiffré.

- Si le filtrage d'URL est désactivé ou si sa clé de fonctionnalité n'est pas disponible, AsyncOS ne peut pas identifier la catégorie d'une URL et la page **Access Policy** > **URL Filtering** (Politique d'accès > Filtrage d'URL) est désactivée. Par conséquent, la clé de fonctionnalité doit être présente et les politiques d'utilisation acceptable activées pour pouvoir configurer les quotas.
- De nombreux sites Web comme Facebook et Gmail sont mis à jour automatiquement à des intervalles réguliers. Si un site Web de ce type est laissé ouvert dans une fenêtre ou un onglet de navigateur inutilisé, il continuera de consommer le quota de temps et de volume de l'utilisateur.
- Lorsque vous redémarrez le proxy et que le mode haute performance est :
  - **Activé** : les quotas de temps et de volume ne sont pas réinitialisés. Les quotas sont automatiquement réinitialisés une fois dans la fenêtre de 24 heures en fonction de l'heure configurée.
  - **Désactivé** : les quotas de temps et de volume sont réinitialisés. L'incidence de la réinitialisation ne perdure que pour la fenêtre actuelle de 24 heures, car les quotas sont automatiquement réinitialisés une fois dans toutes les 24 heures. Le proxy peut redémarrer en raison de modifications de configuration ou d'un plantage du processus de proxy.
- Vos pages EUN (d'avertissement et de blocage) ne peuvent pas être affichées pour HTTPS même lorsque l'option decrypt-for-EUN est activée.

Note Le quota le plus restrictif s'appliquera toujours lorsque plusieurs quotas s'appliquent à un utilisateur donné.

- Calculs du quota de volume, on page 25
- Calculs des quotas de temps, on page 25
- Définition des quotas de temps, de volume et de bande passante, on page 26

Calculs du quota de volume

Le calcul des quotas de volume se fait comme suit :

- Trafic HTTP et HTTPS déchiffré : le corps de la demande et de la réponse HTTP sont pris en compte dans les limites de quota. Les en-têtes de demande et les en-têtes de réponse ne seront pas pris en compte dans le calcul des limites.
- Trafic tunnelisé (y compris HTTPS tunnelisé) : AsyncOS transfère simplement le trafic tunnelisé du client au serveur, et inversement. L'intégralité du volume de données du trafic tunnelisé est pris en compte dans les limites de quota.
- FTP : le trafic de connexion de contrôle n'est pas pris en compte. La taille du fichier chargé et téléchargé est prise en compte dans les limites de quota.

Note Seul le trafic côté client est pris en compte dans les limites de quota. Le contenu en cache est également pris en compte dans la limite, car le trafic côté client est généré même lorsqu'une réponse est fournie à partir du cache.

Calculs des quotas de temps

Le calcul des quotas de temps est le suivant :

- Trafic HTTP et HTTPS déchiffré : la durée de chaque connexion à la même catégorie d'URL, de sa formation à la déconnexion, plus une minute, est prise en compte dans la limite des quotas de temps. Si

plusieurs demandes sont adressées à la même catégorie d'URL à moins d'une minute d'intervalle, elles sont comptées comme une session continue et la minute est ajoutée uniquement à la fin de cette session (c'est-à-dire après au moins une minute de « silence »).

- Trafic de tunnel (y compris HTTPS en tunnel) : La durée réelle du tunnel, de sa formation à la déconnexion, est prise en compte dans les limites des quotas. Le calcul ci-dessus pour les demandes multiples s'applique également au trafic en tunnel.
- FTP : La durée réelle de la session de contrôle FTP, de sa création à la déconnexion, est prise en compte dans les limites des quotas. Le calcul ci-dessus pour les demandes multiples s'applique également au trafic FTP.

Définition des quotas de temps, de volume et de bande passante

Before you begin

- Accédez à **Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable) pour activer Acceptable Use Controls (Contrôles d'utilisation acceptable).
- Définissez une plage de temps, sauf si vous souhaitez que le quota s'applique comme limite quotidienne.

Étape 1 Accédez à **Web Security Manager > Define Time Ranges and Quotas** (Web Security Manager > Définir des plages de temps et des quotas).

Étape 2 Cliquez sur **Add Quota** (Ajouter un quota).

Étape 3 Entrez un **nom de quota** unique dans le champ.

Étape 4 Pour réinitialiser le quota d'heure et de volume tous les jours, sélectionnez **Reset Time and Volume quota daily at** (Réinitialiser ce quota quotidiennement à/Réinitialiser le quota de temps et de volume quotidiennement à) et entrez une heure au format 12 heures dans le champ, puis choisissez **AM** ou **PM** dans le menu. Vous pouvez également sélectionner **Select a predefined time range profile** (Sélectionner un profil de plage de temps prédéfini).

Note L'utilisation de l'option de réinitialisation du quota ne réinitialise pas la valeur configurée du quota de bande passante.

Étape 5 Pour définir un quota de temps, cochez la case **Time Quota** (Quota de temps) et choisissez le nombre d'heures dans le menu **hrs** et le nombre de minutes dans le menu **mins**, de zéro (toujours bloqué) à 23 heures et 59 minutes.

Étape 6 Pour définir un quota de volume, saisissez une valeur dans le champ et sélectionnez **KB** (Ko, kilooctets), MB (Mo, mégaoctets) ou **GB** (Go, gigaoctets) dans le menu.

Étape 7 Pour définir un quota de bande passante, saisissez une valeur dans le champ et choisissez **Kbit/s** (kilobits par seconde) ou **Mbit/s** (mégabits par seconde) dans le menu.

- Le quota de bande passante peut être configuré uniquement dans la politique d'accès. Cependant, vous ne pouvez pas configurer les deux, le quota de bande passante URL et le quota d'activité Web globale pour une même politique d'accès.
- Le quota de bande passante ne peut pas être configuré si la limite de bande passante globale ou la limite de bande passante AVC est activée, et inversement.
- Le contenu en cache est également pris en compte pour le quota de bande passante.
- Nous vous déconseillons d'ajouter un quota de bande passante à un profil de quota de temps ou de volume existant qui est mappé à la politique de déchiffrement ou à la politique CDS.

Bien que vous puissiez modifier le profil de quota, vous ne pouvez pas configurer le quota de bande passante sur une politique de déchiffrement et de CDS.

Note Supprimez tous les profils de quota dont le quota de bande passante a été configuré avant la mise à niveau vers AsyncOS version 14.5.

Étape 8 Cliquez sur **Submit** (Envoyer), puis sur **Commit Changes** (Valider les modifications) pour appliquer vos modifications. Vous pouvez également cliquer sur **Cancel** (Annuler) pour abandonner vos modifications.

What to do next

(Facultatif) Accédez à **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final) pour configurer les notifications de l'utilisateur final concernant les quotas.

Contrôle d'accès par catégorie d'URL

Vous pouvez définir et traiter les demandes Web en fonction de la catégorie de sites Web sur laquelle elles portent. Secure Web Appliance est fourni avec de nombreuses catégories d'URL prédéfinies, comme les courriels basés sur le Web et autres.

Les catégories prédéfinies, et les sites Web qui y sont associés, sont définis dans les bases de données de filtrage qui résident sur le Secure Web Appliance. Ces bases de données sont automatiquement mises à jour par Cisco. Vous pouvez également créer des catégories d'URL personnalisées pour les noms d'hôte et les adresses IP que vous spécifiez.

Les catégories d'URL peuvent être utilisées par toutes les politiques, à l'exception des politiques d'identification des demandes. Elles peuvent également être utilisées par les politiques d'accès, de gestion HTTPS chiffré et de sécurité des données pour appliquer des actions aux demandes.

Voir Création et modification de catégories d'URL personnalisées pour plus d'informations sur la création de catégories d'URL personnalisées.

Utilisation de catégories d'URL pour identifier les demandes Web

Before you begin

- Activez Acceptable Use Control, consultez Configuration du moteur de filtrage d'URL.
- (Facultatif) Créez des catégories d'URL personnalisées, consultez Création et modification de catégories d'URL personnalisées.

Étape 1 Choisissez un type de politique (sauf SaaS) dans le menu Web Security Manager.

Étape 2 Cliquez sur un nom de politique dans le tableau des politiques (ou ajoutez une nouvelle politique).

Étape 3 Développez la section **Advanced** (Niveau avancé) et cliquez sur le lien dans le champ URL Categories (Catégories d'URL).

Étape 4 Cliquez sur les cellules de colonne Add (Ajouter) correspondant aux catégories d'URL selon lesquelles vous souhaitez identifier les demandes Web. Effectuez cette opération pour les listes de catégories d'URL personnalisées et de catégories d'URL prédéfinies, le cas échéant.

Étape 5 Cliquez sur **Done** (Terminé).

Étape 6 Envoyez et validez vos modifications.

Utilisation de catégories d'URL pour traiter une demande Web

Before you begin

- Activez Acceptable Use Control, consultez Configuration du moteur de filtrage d'URL.
- (Facultatif) Créez des catégories d'URL personnalisées, consultez Création et modification de catégories d'URL personnalisées.

Note Si vous avez utilisé des catégories d'URL comme critères dans une politique, ces catégories seules sont disponibles pour spécifier des actions au sein de la même politique. Certaines des options décrites ci-dessous peuvent être différentes ou ne pas être disponibles pour cette raison.

Étape 1 Choisissez entre **Access Policies** (Politiques d'accès), **Cisco Data Security Policies** (Politiques de sécurité des données Cisco) ou **Encrypted HTTPS Management** (Gestion HTTPS chiffrée) dans le menu Web Security Manager.

Étape 2 Recherchez le nom de la politique requise dans le tableau des politiques.

Étape 3 Cliquez sur le lien de la cellule dans la colonne URL Filtering (Filtrage d'URL) sur la même ligne.

Étape 4 (Facultatif) Ajoutez des catégories d'URL personnalisées :

a) Cliquez sur **Select Custom Categories** (Sélectionner des catégories personnalisées).

b) Choisissez les catégories d'URL personnalisées à inclure dans cette politique et cliquez sur **Apply** (Appliquer).

Choisissez les catégories d'URL personnalisées auxquelles le moteur de filtrage d'URL doit comparer la demande du client. Le moteur de filtrage d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues. Le moteur de filtrage d'URL compare l'URL dans une demande d'un client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la politique apparaissent dans la section Custom URL Category Filtering (Filtrage de catégories d'URL personnalisées).

Étape 5 Choisissez une action pour chaque catégorie d'URL personnalisée et prédéfinie.

Note Les actions disponibles varient selon les catégories personnalisées et prédéfinies, et selon les types de politiques.

Étape 6 Dans la section Uncategorized URLs (URL non classées), choisissez l'action à entreprendre pour les demandes des clients adressées aux sites Web qui n'entrent pas dans une catégorie d'URL prédéfinie ou personnalisée.

Étape 7 Envoyez et validez vos modifications.

Utilisateurs à distance

• À propos des utilisateurs à distance, on page 29

À propos des utilisateurs à distance

Cisco AnyConnect Secure Mobility étend le périmètre du réseau aux terminaux distants, ce qui permet l'intégration des services de filtrage Web offerts par Secure Web Appliance.

Les utilisateurs mobiles et distants utilisent le client Cisco AnyConnect Secure VPN (réseau privé virtuel) pour établir des sessions VPN avec Adaptive Security Appliance (ASA). L'ASA envoie le trafic Web à Secure Web Appliance avec des informations identifiant l'utilisateur par adresse IP et par nom d'utilisateur. Secure Web Appliance analyse le trafic, applique les politiques d'utilisation acceptable et protège l'utilisateur contre les menaces à la sécurité. L'appliance de sécurité renvoie tout le trafic jugé sûr et acceptable à l'utilisateur.

Lorsque Secure Mobility est activé, vous pouvez configurer les identités et les politiques à appliquer aux utilisateurs en fonction de leur emplacement :

- **Utilisateurs à distance.** Ces utilisateurs sont connectés au réseau à partir d'un emplacement distant à l'aide du VPN. Secure Web Appliance identifie automatiquement les utilisateurs à distance lorsque Cisco ASA et le client Cisco AnyConnect sont utilisés pour l'accès VPN. Sinon, l'administrateur Secure Web Appliance doit indiquer les utilisateurs à distance en configurant une plage d'adresses IP.
- **Utilisateurs locaux.** Ces utilisateurs sont connectés au réseau physiquement ou sans fil.

Quand Secure Web Appliance est intégré à Cisco ASA, vous pouvez le configurer pour identifier les utilisateurs par un nom d'utilisateur authentifié de manière transparente afin de permettre la connexion unique pour les utilisateurs à distance.

Comment configurer l'identification des utilisateurs à distance

Tâche	Informations complémentaires
1. Configurez l'identification des utilisateurs à distance.	Configuration de l'identification des utilisateurs à distance, on page 30
2. Créez une identité pour les utilisateurs à distance.	Classification des utilisateurs et logiciels clients 1. Dans la section « Define Member by User Location » (Définir les membres par emplacement utilisateur), sélectionnez Remote Users Only (Utilisateurs à distance uniquement). 2. Dans la section « Define Member by Authentication » (Définir les membres par l'authentification), sélectionnez « Identify Users Clearly using Cisco ASA integration » (Identifier les utilisateurs de manière transparente par l'intégration Cisco ASA).
3. Créez une politique pour les utilisateurs à distance.	Création d'une politique , on page 7

Configuration de l'identification des utilisateurs à distance

Étape 1 Services de sécurité > AnyConnect Secure Mobility, puis cliquez sur **Enable** (Activer).

Étape 2 Lisez les conditions du contrat de licence d'AnyConnect Secure Mobility, puis cliquez sur **Accept** (Accepter).

Étape 3 Configurez l'identification des utilisateurs à distance.

Option	Description	Étapes supplémentaires
IP Address (Adresse IP)	Indiquez une plage d'adresses IP que l'appliance doit considérer comme attribuées aux périphériques distants.	**a.** Entrez une plage d'adresses IP dans le champ IP Range (Plage d'adresses IP). **b.** Passez à l'étape 4.
Cisco ASA Integration (Intégration Cisco ASA)	Indiquez un ou plusieurs systèmes Cisco ASA avec lesquels Secure Web Appliance communique. Le système Cisco ASA gère un mappage entre l'adresse IP et l'utilisateur et communique cette information à Secure Web Appliance. Lorsque le proxy Web reçoit une transaction, il obtient l'adresse IP et détermine l'utilisateur en vérifiant le mappage entre l'adresse IP et l'utilisateur. Lorsque les utilisateurs sont déterminés par l'intégration avec un système Cisco ASA, vous pouvez activer la connexion unique pour les utilisateurs à distance.	**a.** Saisissez le nom d'hôte ou l'adresse IP du système Cisco ASA. **b.** Saisissez le numéro de port utilisé pour accéder au système ASA. Le numéro de port par défaut du système Cisco ASA est 11999. **c.** Si plusieurs système Cisco ASA sont configurés dans une grappe, cliquez sur **Add Line** (Ajouter une ligne) et configurez chaque système ASA de la grappe. **Note** Si deux systèmes Cisco ASA sont configurés pour la haute disponibilité, saisissez un seul nom d'hôte ou une seule adresse IP pour le système Cisco ASA *actif*. **d.** Saisissez la phrase secrète d'accès pour Cisco ASA. **Note** La phrase secrète que vous entrez ici doit correspondre à la phrase secrète d'accès configurée pour le système Cisco ASA indiqué. **e.** Facultatif, cliquez sur **Start Test** (Commencer le test) pour vérifier que Secure Web Appliance peut se connecter au système Cisco ASA configuré.

Étape 4 Envoyez et validez les modifications.

Note Activez AnyConnect Security Mobility (**Security Services** > **AnyConnect Security Mobility**) (AnyConnect Security Mobility > Services de sécurité > AnyConnect Security Mobility) pour rendre l'option Define Members by User Location (Définir les membres par emplacement utilisateur) disponible sur Secure Web Appliance. Par défaut, cette option est disponible sur l'appliance Cisco de gestion de la sécurité de contenu [**Web** > **Configuration Master** > **Identification Profiles** (Web > Fichier de configuration principal > Profils d'identification)]. Lorsque vous utilisez l'option Define Member by User Location (Définir les membres par emplacement utilisateur) pour configurer un profil d'identification dans l'appliance de gestion de la sécurité et publiez cette configuration sur Secure Web Appliance, où AnyConnect Security Mobility n'est pas activé, le profil d'identification est désactivé.

Affichage de l'état et des statistiques de l'utilisateur distant pour les ASA

Utilisez cette commande pour afficher les informations relatives à Secure Mobility quand Secure Web Appliance est intégré à un ASA.

Commande	Description
`musstatus`	Cette commande affiche les informations suivantes : • L'état de la connexion Secure Web Appliance avec chaque ASA. • La durée de la connexion Secure Web Appliance avec chaque ASA en minutes. • Le nombre de clients distants de chaque ASA. • Le nombre de clients distants desservis, qui est défini comme le nombre de clients distants qui ont transmis du trafic par l'intermédiaire de Secure Web Appliance. • Le nombre total de clients distants.

Résolution de problèmes de politiques

- Politique d'accès non configurable pour HTTPS
- Certains fichiers Microsoft Office ne sont pas bloqués
- Le blocage des types d'objets exécutables DOS bloque les mises à jour pour Windows OneCare
- Disparition du profil d'identification de la politique
- La politique n'est jamais appliquée
- Les demandes HTTPS et FTP via HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification
- Politique globale de correspondances des utilisateurs pour les demandes HTTPS et FTP via HTTP
- Politique d'accès incorrecte attribuée à l'utilisateur
- Outil de résolution de problèmes liés aux politiques : Suivi des politiques

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.