Interception des demandes Web

Cette rubrique contient les sections suivantes :

Survol de l'interception des demandes Web

Secure Web Appliance intercepte les demandes qui lui sont transmises par les clients ou d'autres appareils sur le réseau.

L'appliance fonctionne de pair avec d'autres appareils réseau pour intercepter le trafic. Il peut s'agir de commutateurs simples, d'appareils de redirection transparents, de dérivateurs réseau et d'autres serveurs proxy ou Secure Web Appliance.

Tâches d'interception des demandes Web

Étapes	Tâche	Liens vers des rubriques et des procédures connexes
Étape 1	Passez en revue les bonnes pratiques.	• Bonnes pratiques pour l'interception des demandes Web, on page 2

Étapes	Tâche	Liens vers des rubriques et des procédures connexes
Étape 2	(Facultatif) Effectuez les tâches de mise en réseau suivantes : • Connectez-vous et configurez les proxy en amont. • Configurez les ports d'interface réseau : • Configurez les périphériques de redirection transparents. • Configurez les voies de routage TCP/IP. • Configurez les réseaux VLAN.	• Serveurs proxy en amont • Interfaces réseau • Configuration de la redirection transparente • Configuration des routages de trafic TCP/IP • Augmentation de la capacité de l'interface à l'aide de VLAN
Étape 3	(Facultatif) Effectuez les tâches relatives au proxy Web : • Configurez le proxy Web pour qu'il fonctionne en mode transfert ou transparent. • Déterminez si des services supplémentaires sont nécessaires pour les types de protocoles que vous souhaitez intercepter • Configurez l'usurpation d'adresses IP. • Gérez le cache du proxy Web. • Utilisez des en-têtes de demande Web personnalisés. • Contournez le proxy pour certaines demandes.	• Options de proxy Web pour l'interception des demandes Web, on page 3 • Configuration des paramètres du proxy Web, on page 3 • Options de proxy Web pour l'interception des demandes Web, on page 3 • Cache du proxy Web, on page 7 • Usurpation d'adresses IP de proxy Web, on page 9 • Contournement du proxy Web, on page 12
Étape 4	Effectuez les tâches du client : • Décidez comment les clients doivent rediriger les demandes vers le proxy Web. • Configurez les clients et les ressources du client.	• Options du client pour la redirection des demandes Web, on page 18 • Utilisation de fichiers PAC avec les applications clientes, on page 19
Étape 5	(Facultatif) Activez et configurez le proxy FTP.	• Services de proxy FTP, on page 22

Bonnes pratiques pour l'interception des demandes Web

- Activez uniquement les services proxy dont vous avez besoin.
- Utilisez la même méthode de transfert et de retour (L2 ou GRE) pour tous les services WCCP définis à la section Secure Web Appliance. Cela permet le fonctionnement cohérent de la liste de contournement de proxy.

- Veillez à ce que les utilisateurs ne puissent pas accéder aux fichiers PAC depuis l'extérieur du réseau de l'entreprise. Cela permet à vos télétravailleurs d'utiliser le proxy Web lorsqu'ils se trouvent sur le réseau de l'entreprise et de se connecter directement aux serveurs Web à d'autres moments.
- Autorisez un proxy Web à accepter les en-têtes X-Forwarded-For de proxys en aval ou d'équilibreurs de charge dignes de confiance uniquement.
- Laissez le proxy Web dans le mode transparent par défaut, même si vous utilisez uniquement le transfert explicite au départ. Le mode transparent accepte également les demandes explicitement transférées.

Options de proxy Web pour l'interception des demandes Web

À lui seul, le proxy Web peut intercepter les demandes Web qui utilisent HTTP (y compris FTP sur HTTP) et HTTPS. Des modules de proxy supplémentaires sont disponibles pour améliorer la gestion des protocoles :

- **Proxy FTP.** Le proxy FTP permet l'interception du trafic FTP natif (plutôt que simplement du trafic FTP qui a été codé dans HTTP).
- **Proxy HTTPS.** Le proxy HTTPS prend en charge le déchiffrement du trafic HTTPS et permet au proxy Web de transmettre les requêtes HTTPS non chiffrées aux politiques pour l'analyse de contenu.

Note En mode transparent, le proxy Web abandonne toutes les requêtes HTTPS redirigées de manière transparente si le proxy HTTPS n'est pas activé. Aucune entrée de journal n'est créée pour les demandes HTTPS abandonnées redirigées de manière transparente.

- **Proxy SOCKS.** Le proxy SOCKS permet l'interception du trafic SOCKS.

Chacun de ces proxy supplémentaires nécessite le proxy Web pour fonctionner. Vous ne pouvez pas les activer si vous désactivez le proxy Web.

Note Le proxy Web est activé par défaut. Tous les autres proxys sont désactivés par défaut.

Thèmes connexes

- Services de proxy FTP, on page 22
- Services proxy SOCKS, on page 24

Configuration des paramètres du proxy Web

Before you begin

Activez le proxy Web.

Étape 1 Choisissez **Security Services** > **Web Proxy** (Services de sécurité > Proxy Web).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les paramètres de base du proxy Web au besoin.

Propriété	Description
HTTP Ports to Proxy (Ports HTTP vers proxy)	Ports sur lesquels le proxy Web écoute les connexions HTTP
Caching (Mise en mémoire cache)	Indique s'il faut activer ou désactiver la mise en cache du proxy Web. Le proxy Web met en cache les données pour augmenter les performances.
Proxy Mode (Mode proxy)	• **Transparent** (recommandé) : permet au proxy Web de nommer la cible Internet. Le proxy Web peut intercepter les demandes Web transparentes et explicitement transférées dans ce mode. • **Forward** (Transférer) : permet au navigateur client de nommer la cible Internet. Nécessite la configuration individuelle de chaque navigateur Web pour utiliser le proxy Web. Le proxy Web ne peut intercepter que les demandes Web explicitement transférées dans ce mode.
IP Spoofing Connection Type (Type de connexion d'usurpation d'adresses IP)	Si vous avez sélectionné le mode proxy **Transparent**, choisissez l'un des types de connexion d'usurpation d'adresses IP : • **For Transparent Connections Only** (Pour les connexions transparentes uniquement) : pour configurer l'usurpation d'adresses IP pour les connexions transparentes uniquement. • **For All Connections** (Pour toutes les connexions) : pour configurer l'usurpation d'adresses IP pour les connexions transparentes et explicites. Si vous avez sélectionné le mode proxy **Forward** (Transfert), le type de connexion d'usurpation d'adresses IP est toujours explicite. **Note** Le type de connexion d'usurpation d'adresses IP que vous choisissez est applicable à tous les protocoles : FTP natif, HTTP et HTTPS. Pour ajouter des profils d'usurpation d'adresses IP dans les politiques de routage, consultez Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage

Étape 4 Renseignez les paramètres de proxy Web avancés comme requis.

Propriété	Description
Persistent Connection Timeout (Expiration de la connexion persistante)	Durée maximale en secondes pendant laquelle le proxy Web maintient ouverte une connexion avec un client ou un serveur après qu'une transaction est terminée et qu'aucune autre activité n'est détectée. • **Client side** (Côté client). Valeur du délai d'expiration pour les connexions aux clients. • **Server side** (Côté serveur). Valeur du délai d'expiration pour les connexions aux serveurs. Si vous augmentez ces valeurs, les connexions resteront ouvertes plus longtemps et réduiront le surdébit utilisé pour ouvrir et fermer des connexions à plusieurs reprises. Cependant, vous réduisez également la capacité du proxy Web à ouvrir de nouvelles connexions si le nombre maximal de connexions persistantes simultanées a été atteint. Après avoir établi une connexion et effectué une liaison SSL, si les demandes du client ne sont pas envoyées au proxy, ce dernier attend l'expiration du délai de connexion persistante, puis met fin à la connexion avec le client. Cisco recommande de conserver les valeurs par défaut.
In-Use Connection Timeout (Délai d'expiration de la connexion en cours d'utilisation)	Durée maximale en secondes pendant laquelle le proxy Web attend davantage de données d'un client ou d'un serveur inactif lorsque la transaction en cours n'est pas encore terminée. • **Client side** (Côté client). Valeur du délai d'expiration pour les connexions aux clients. • **Server side** (Côté serveur). Valeur du délai d'expiration pour les connexions aux serveurs.
Simultaneous Persistent Connections (Server Maximum Number) [Connexions persistantes simultanées (nombre maximum de serveurs)]	Le nombre maximal de connexions (prises) que le proxy Web maintient ouvertes avec les serveurs.
Maximum Connections Per Client (Nombre maximal de connexions par client)	Limite le nombre de connexions simultanées initiées par le client à une valeur configurée. Lorsque le nombre de connexions dépasse la limite configurée, les connexions sont abandonnées et une alerte est envoyée à l'administrateur. **Note** Par défaut, le nombre maximal de connexions par client est désactivé. Pour configurer la limite, cochez la case **Maximum Connections Per Client** (Nombre maximal de connexions par client) et procédez comme suit : • **Connexions** (Connections) : saisissez le nombre de connexions simultanées admissibles. • **Exempted Downstream Proxy or Load Balancer** (Équilibre de charge ou proxy en aval dispensé) : saisissez l'adresse IP du proxy en aval, de l'équilibreur de charge ou de toute autre adresse IP client (vous ne pouvez pas configurer les sous-réseaux ou les noms d'hôte). Le proxy Web n'applique pas les restrictions des connexions simultanées aux adresses IP incluses dans cette liste de dispenses.

Propriété	Description
Generate Headers (Générer des en-têtes)	Générez et ajoutez des en-têtes qui codent les informations concernant la demande. • Les en-têtes **X-Forwarded-For** codent l'adresse IP du client d'où provient une demande HTTP. **Note** • Pour activer ou désactiver le transfert d'en-tête, utilisez l'option Miscellaneous (Divers) de la commande de l'interface de ligne de commande `advancedproxyconfig`, Do you want to pass HTTP X-Forwarded-For headers? (Voulez-vous transférer les en-têtes HTTP X-Forwarded-For?) • L'utilisation d'un proxy de transfert en amont explicite pour gérer l'authentification d'utilisateurs ou le contrôle d'accès avec authentification de proxy nécessite le transfert de ces en-têtes. • Pour les demandes HTTPS transparentes, l'appliance ne déchiffre pas l'en-tête XFF. Pour les demandes explicites, l'appliance utilise l'en-tête XFF reçu dans la demande CONNECT et ne déchiffre pas XFF à l'intérieur du tunnel SSL, de sorte que l'identification des adresses IP des clients à l'aide de X-Forwarded-For n'est pas applicable aux demandes HTTPS transparentes. • Les en-tête **Request Side VIA** (VIA côté demande) encodent les proxys par lesquels passe la demande pendant sa transmission du client au serveur. • Les en-têtes **Response Side VIA** (VIA côté réponse) encodent les proxys par lesquels passe la demande pendant sa transmission du serveur au client.
Use Received Headers (Utiliser les en-têtes reçus)	Permet à un proxy Web déployé en tant que proxy en amont d'identifier les clients à l'aide des en-têtes X-Forwarded-For envoyés par les proxys en aval. Le proxy Web n'acceptera pas l'adresse IP dans un en-tête X-Forwarded-For provenant d'une source qui n'est pas incluse dans cette liste. Si cette option est activée, elle nécessite l'adresse IP d'un proxy en aval ou d'un équilibreur de charge (vous ne pouvez pas saisir de sous-réseaux ni de noms d'hôte).
Range Request Forwarding (Transfert de demande de plage)	Cochez la case **Enable Range Request Forwarding** (Activer le transfert des demandes de plage) pour activer ou désactiver le transfert des demandes de plage. Voir Gestion de l'accès aux applications Web pour plus d'informations.

Étape 5 Envoyez et validez vos modifications.

What to do next

- Cache du proxy Web, on page 7
- Configuration de la redirection transparente

Cache du proxy Web

Le proxy Web met en cache les données pour augmenter les performances. AsyncOS comprend des modes de mise en cache définis qui vont de sécurisé à dynamique, et permet également une mise en cache personnalisée. Vous pouvez également exclure des URL spécifiques de la mise en cache en les supprimant du cache ou en configurant le cache de sorte qu'il les ignore.

Effacement du cache du proxy Web

Étape 1 Choisissez **Security Services** > **Web Proxy** (Services de sécurité > Proxy Web).

Étape 2 Cliquez sur **Clear Cache** (Effacer le cache) et confirmez votre action.

Suppression d'URL du cache du proxy Web

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `webcache > evict` pour accéder à la zone de mise en cache requise :

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

Étape 3 Entrez l'URL à supprimer du cache.

Note Si vous n'incluez pas de protocole dans l'URL, `http://` lui sera ajouté en préfixe (p. ex., `www.cisco.com` deviendra `http://www.cisco.com`)

Spécification des domaines ou des URL que le proxy Web ne met jamais en mémoire cache

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `webcache` -> `ignore` pour accéder aux sous-menu requis :

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

Étape 3 Entrez le type d'adresse que vous souhaitez gérer : `DOMAINS` ou `URLS`.

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

Étape 4 Entrez **add** (ajouter) pour ajouter de nouvelles entrées :

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

Étape 5 Entrez les domaines ou les URL, un par ligne; par exemple :

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

Vous pouvez inclure certains caractères d'expression régulière (regex) lorsque vous spécifiez un domaine ou des URL. Avec l'option `DOMAINS`, vous pouvez utiliser un point pour dispenser un domaine entier et ses sous-domaines de la mise en cache. Par exemple, vous pouvez saisir `.google.com` plutôt que simplement `google.com` pour dispenser www.google.com, docs.google.com, etc.

Avec l'option `URLS`, vous pouvez utiliser la suite complète des caractères d'expression régulière. Consultez Expressions régulières pour plus d'informations sur l'utilisation des expressions régulières.

Étape 6 Lorsque vous avez terminé de saisir les valeurs, appuyez sur Entrée jusqu'à revenir à l'interface de ligne de commande principale.

Étape 7 Validez vos modifications.

Choix du mode de mise en mémoire cache du proxy Web

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `advancedproxyconfig -> caching` pour accéder aux sous-menus requis :

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

```
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

Étape 3 Saisissez le numéro correspondant aux paramètres de cache du proxy Web dont vous avez besoin :

Entrée de gamme	Mode	Description
1	Demandes	La mise en mémoire cache la plus faible et le plus grand respect de la RFC 2616 par rapport aux autres modes.
2	Optimisé	Mise en mémoire cache modérée et respect modérée de la RFC 2616. Par rapport au mode sans échec, en mode optimisé, le proxy Web met en mémoire cache les objets si aucune heure de mise en cache n'est spécifiée quand un en-tête Last-Modified est présent. Le proxy Web met en cache les réponses négatives.
3	Dynamique	La mise en cache la plus importante et le respect de la RFC 2616 le plus faible. Par rapport au mode optimisé, le mode dynamique met en cache le contenu authentifié, les incompatibilités d'ETag et le contenu sans en-tête Last-Modified. Le proxy Web ignore le paramètre no-cache.
4	Mode personnalisé	Configurez chaque paramètre individuellement.

Étape 4 Si vous avez choisi l'option 4 (mode personnalisé), saisissez des valeurs (ou conservez les valeurs par défaut) pour chacun des paramètres personnalisés.

Étape 5 Appuyez sur **Enter** (Entrée) jusqu'à ce que vous reveniez à l'interface de commande principale.

Étape 6 Validez vos modifications.

What to do next

Thèmes connexes

- Cache du proxy Web, on page 7.

Usurpation d'adresses IP de proxy Web

Lorsque le proxy Web transfère une demande, il modifie l'adresse IP de la source de la demande pour qu'elle corresponde à la sienne par défaut. Cela augmente la sécurité, mais vous pouvez modifier ce comportement en mettant en œuvre l'usurpation d'adresses IP, de sorte que les demandes semblent provenir de l'adresse IP du client ou de toute autre adresse IP personnalisée routable plutôt que de Secure Web Appliance. Vous pouvez configurer l'usurpation d'adresses IP du proxy Web en créant des profils d'usurpation d'adresses IP pour les adresses IP personnalisées et en les ajoutant aux politiques de routage.

L'usurpation d'adresses IP fonctionne pour un trafic transparent et explicitement transféré. Lorsque le proxy Web est déployé en mode transparent, vous pouvez configurer le type de connexion d'usurpation d'adresses

IP pour les connexions redirigées de manière transparente uniquement ou pour toutes les connexions (redirigées transparentes et explicitement transférées). Si les connexions explicitement transférées utilisent l'usurpation d'adresses IP, vous devez vous assurer que vous disposez des périphériques réseau appropriés pour acheminer les paquets de retour vers Secure Web Appliance.

Lorsque l'usurpation d'identités IP est activée et que l'appliance est connectée à un routeur WCCP, vous devez configurer deux services WCCP : un basé sur les ports source et un basé sur les ports de destination.

Les profils d'usurpation d'adresses IP sont limités lorsque le trafic HTTPS est redirigé de manière transparente. Consultez Accès aux sites HTTPS à l'aide de politiques de routage avec critères de catégorie d'URL.

Thèmes connexes

- Création de profils d'usurpation d'adresses IP, on page 10
- Configuration des paramètres du proxy Web, on page 3
- Configuration des services WCCP

Création de profils d'usurpation d'adresses IP

Before you begin

Assurez-vous d'avoir sélectionné le mode proxy et le type de connexion d'usurpation d'adresses IP dans les paramètres de proxy Web. Pour en savoir plus, consultez Configuration des paramètres du proxy Web, on page 3.

Étape 1 Choisissez **Web Security Manager** > **IP Spoofing Profiles** (Web Security Manager > Profils d'usurpation d'adresses IP).

Étape 2 Cliquez sur **Add Profile** (Ajouter un profil).

Étape 3 Entrez un nom pour le profil d'usurpation d'adresses IP.

Étape 4 Entrez l'adresse IP que vous souhaitez attribuer au nom de profil d'usurpation d'identité.

Étape 5 Envoyez et validez vos modifications.

What to do next

Ajouter le profil d'usurpation d'adresses IP à une politique de routage. Pour en savoir plus, consultez Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage.

Related Topics

Modification des profils d'usurpation d'adresses IP, à la page 10
Suppression des profils d'usurpation d'adresses IP, à la page 11

Modification des profils d'usurpation d'adresses IP

Note Une fois que vous avez mis à jour un profil d'usurpation d'adresses IP, il sera mis à jour dans toutes les politiques de routage associées à ce profil.

Étape 1 Choisissez **Web Security Manager** > **IP Spoofing Profiles** (Web Security Manager > Profils d'usurpation d'adresses IP).

Étape 2 Cliquez sur le lien du nom du profil d'usurpation IP que vous souhaitez modifier.

Étape 3 Modifiez les détails du profil.

Étape 4 Envoyez et validez vos modifications.

Suppression des profils d'usurpation d'adresses IP

Étape 1 Choisissez **Web Security Manager** > **IP Spoofing Profiles** (Web Security Manager > Profils d'usurpation d'adresses IP).

Étape 2 Cliquez sur l'icône de corbeille correspondant au profil d'usurpation d'adresses IP que vous souhaitez supprimer.

Note L'appliance affiche un avertissement si le profil d'usurpation d'adresses IP que vous supprimez est affecté à une ou plusieurs politiques de routage. Dans ce cas, sélectionnez un autre profil d'usurpation d'adresses IP à affecter à toutes les politiques de routage concernées.

Étape 3 Envoyez et validez vos modifications.

En-têtes personnalisés de proxy Web

Vous pouvez ajouter des en-têtes personnalisés à des transactions sortantes spécifiques pour demander un traitement spécial aux serveurs de destination. Par exemple, si vous avez une relation avec YouTube pour les écoles, vous pouvez utiliser un en-tête personnalisé pour identifier les demandes de transaction adressées à YouTube.com comme provenant de votre réseau et comme nécessitant un traitement spécial.

Ajout d'en-têtes personnalisés aux demandes Web

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `advancedproxyconfig -> customheaders` pour accéder aux sous-menus requis :

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
```

```
- EDIT - Edit entries
[]>
```

Étape 3 Utilisez la sous-commande requise comme suit :

Option	Description
`Delete` (Supprimer)	Supprime l'en-tête personnalisé que vous identifiez. Identifiez l'en-tête à supprimer en utilisant le numéro associé à l'en-tête dans la liste renvoyée par la commande.
`New` (Nouveau)	Crée l'en-tête que vous fournissez à utiliser avec le domaine ou les domaines que vous spécifiez. Exemple d'en-tête : X-YouTube-Edu-Filter : ABCD1234567890abcdef (Dans ce cas, la valeur est une clé unique fournie par YouTube.) Exemple de domaine : youtube.com
`Edit` (Modifier)	Remplace un en-tête existant par un que vous spécifiez. Identifiez l'en-tête à supprimer en utilisant le numéro associé à l'en-tête dans la liste renvoyée par la commande.

Étape 4 Appuyez sur **Enter** (Entrée) jusqu'à ce que vous reveniez à l'interface de commande principale.

Étape 5 Validez vos modifications.

Contournement du proxy Web

Contournement du proxy Web pour les demandes Web

Vous pouvez configurer Secure Web Appliance de sorte que les demandes transparentes de clients particuliers ou vers des destinations particulières contournent le proxy Web.

En contournant le proxy Web, vous pouvez :

- Éviter les interférences avec les protocoles non conformes (ou propriétaires) qui utilisent des ports HTTP mais ne fonctionnent pas correctement lorsqu'ils se connectent à un serveur proxy.
- Veiller à ce que le trafic provenant d'une machine particulière du réseau, comme une machine de test de programmes malveillants, contourne le proxy Web et toutes ses protections de sécurité intégrées.

Le contournement ne fonctionne que pour les demandes qui sont redirigées de manière transparente vers le proxy Web. Le proxy Web traite toutes les demandes que les clients lui transmettent explicitement, que le proxy soit en mode transparent ou renvoi.

Configuration du contournement du proxy Web pour les demandes Web

Étape 1 Choisissez **Web Security Manager > Bypass Settings** (Web Security Manager > Contourner les paramètres).

Étape 2 Cliquez sur **Edit Bypass Settings** (Modifier les paramètres de contournement).

Étape 3 Entrez les adresses pour lesquelles vous souhaitez contourner le proxy Web.

Note Lorsque vous configurez /0 comme masque de sous-réseau pour une adresse IP dans 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 Choisissez les catégories d'URL personnalisées que vous souhaitez ajouter à la liste de contournement de proxy.

Note Vous ne pouvez pas définir le contournement de proxy Web pour les expressions régulières.

Note 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 5 Envoyez et validez vos modifications.

Configuration du contournement du proxy Web pour les applications

Étape 1 Choisissez **Web Security Manager > Bypass Settings** (Web Security Manager > Contourner les paramètres).

Étape 2 Cliquez sur **Edit Application Bypass Settings** (Modifier les paramètres de contournement d'application).

Étape 3 Sélectionnez les applications pour lesquelles vous souhaitez contourner l'analyse.

Étape 4 Envoyez et validez vos modifications.

Note Les paramètres de contournement de Webex ne s'appliquent qu'au trafic HTTPS. Cependant, pour le trafic HTTP, les applications peuvent être bloquées par les politiques d'accès.

En-têtes personnalisés du proxy Web par politique

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. Chaque profil peut comprendre un maximum de 12 en-têtes. Vous pouvez également modifier ou supprimer les profils d'en-tête existants. Vous pouvez ajouter le profil de réécriture d'en-tête à une politique d'accès existante pour inclure les en-têtes dans toutes les transactions auxquelles la politique d'accès particulière est appliquée.

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.

- Création de profils de réécriture d'en-têtes pour les demandes Web HTTP, à la page 14
- Modification des formats de nom d'utilisateur et d'en-tête de groupe , à la page 15 (facultatif)

• Ajout de profils d'en-tête à la politique d'accès, à la page 16

Il est recommandé de ne pas créer d'en-têtes de proxy Web personnalisés à l'aide de la commande d'interface de ligne de commande `advancedproxyconfig -> customheader` à partir d'AsynOS version 14.0.

Création de profils de réécriture d'en-têtes pour les demandes Web HTTP

Étape 1 Choisissez **Web Security Manager** -> **HTTP Rewrite Profiles** (Web Security Manager > Profils de réécriture http).

Étape 2 Cliquez sur **Add Profile** (Ajouter un profil).

Étape 3 Attribuez un nom unique au profil de réécriture d'en-tête que vous souhaitez créer.

Étape 4 Dans la zone **Headers** (En-têtes), saisissez les informations suivantes :

Remarque Vous pouvez saisir une valeur d'en-tête vide ou nulle dans Header Rewrite Profiles (Profils de réécriture d'en-tête). Lorsque vous enregistrez et validez l'en-tête ne contenant aucune valeur ou contenant une valeur nulle, l'en-tête n'est pas inclus dans les demandes sortantes. Par exemple, si vous souhaitez masquer l'en-tête `Via` sur le serveur sortant, ajoutez le nom d'en-tête `Via` aux profils de réécriture HTTP avec la valeur "".

- **Header Name** (Nom d'en-tête) : Saisissez le nom d'en-tête que vous souhaitez ajouter aux demandes HTTP. Exemple : X-Client-IP, X-Authenticated-User, X-Authenticated-Groups, etc.
- **Header Value** (Valeur d'en-tête) : Saisissez la valeur à inclure dans l'en-tête de demande correspondant au nom d'en-tête. Ajouter aux variables d'en-tête le préfixe suivant :
  - `$ReqMeta`— Pour récupérer les variables d'en-tête HTTP standard telles que l'adresse IP du client, l'utilisateur, le groupe, etc. Par exemple, pour inclure le nom d'utilisateur dans l'en-tête de la demande, le format est `($ReqMeta[X-Authenticated-User])`
  - `$ReqHeader` : Pour utiliser les valeurs des en-têtes HTTP standard ou les valeurs d'autres en-têtes définis sous le même profil de réécriture d'en-tête.

    Par exemple :

    ```
    En-tête 1 :32

    En-tête 2 : 44-($ReqHeader[Header1])-46
    ```

    La valeur de l'`en-tête 2` est `44-32-46`
- **Text Format** (Format de texte) : Choisissez le format de texte pour l'encodage. Les options disponibles sont ASCII et UTF-8.
- **Binary Encoding** (Codage binaire) : Choisissez si vous souhaitez ou non l'encodage binaire (Base64) pour les en-têtes de demande.

Remarque Selon le type de serveur, l'appliance affiche un message d'erreur si la taille du champ d'en-tête de la demande envoyée dépasse la limite maximale du serveur. Par exemple, différents types de serveurs prennent en charge différentes longueurs d'en-tête :

- Apache 2.0, 2.2 : 8k
- Nginx : 4k - 8k
- IIS (varie selon la version) : 8K - 16K
- Tomcat : (varie selon la version) 8K

Si l'identification de l'utilisateur utilise le service ISE, les paramètres globaux des en-têtes X-Authentication, c'est-à-dire X-Authenticated-User et X-Authenticated-Groups, n'appliquent pas de domaine et de mécanisme d'authentification comme préfixe.

Vous pouvez saisir UTF+8 comme valeur `($ReqMeta[HTTP_header])` même si vous sélectionnez le format de texte ASCII. Les en-têtes suivants prennent actuellement en charge `($ReqMeta[HTTP_tête])` :

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

Les en-têtes ne sont pas inclus dans les demandes sortantes si les valeurs des en-têtes sont nulles. Cela se produit lorsque vous :

- Activez l'authentification du proxy
- Définissez des groupes dans les critères d'appartenance pour la politique d'accès, la politique de déchiffrement ou la politique de routage.

Étape 5 Envoyez et validez vos modifications.

Modification des formats de nom d'utilisateur et d'en-tête de groupe

Étape 1 Choisissez **Web Security Manager** > **HTTP Rewrite Profiles** (Web Security Manager > Profils de réécriture HTTP).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Modifiez les formats.

Les formats autorisés sont les suivants :

- Nom d'utilisateur :`$authMechanism://$domainName/$userName, $authMechanism:\\$domainName\$userName, $domainName/$userName, $domainName\$userName, $userName`
- Groupe : `$authMechanism://$domainName/$groupName, $authMechanism:\\$domainName\$groupName, $domainName/$groupName, $domainName\$groupName, $groupName`

  Vous pouvez également modifier le séparateur, comme la virgule (,), les deux-points (:), le point-virgule (;), la barre oblique inverse (\), la barre verticale (|), etc.

Étape 4 Envoyez et validez vos modifications.

Ajout de profils d'en-tête à la politique d'accès

Avant de commencer

Configurez la politique d'accès. Consultez Création d'une politique.

Étape 1 Choisissez **Web Security Manager** >**Access Policies** (Web Security Manager > Politiques d'accès)

Étape 2 Dans la page Access Policies (Politiques d'accès), cliquez sur le lien HTTP Rewrite Profile (Profil de réécriture HTTP).

Vous pouvez également créer une nouvelle politique d'accès et y ajouter le profil de réécriture d'en-tête. Pour créer une stratégie d'accès, consultezCréation d'une politique

Étape 3 Sélectionnez le profil de réécriture d'en-tête que vous souhaitez ajouter à la stratégie. Après votre ajout, les en-têtes sont inclus dans la transaction HTTP à laquelle la politique d'accès particulière est appliquée.

Étape 4 Envoyez et validez vos modifications.

Vous pouvez supprimer un profil de réécriture d'en-tête lié à une politique d'accès. Avant de le supprimer, choisissez un autre profil. Le profil sélectionné sera automatiquement appliqué aux politiques d'accès.

Contrat d'utilisation du proxy Web

Vous pouvez configurer Secure Web Appliance pour informer les utilisateurs qu'il filtre et surveille leur activité Web. Pour ce faire, l'appliance affiche une page de confirmation destinée à l'utilisateur final la première fois qu'un utilisateur accède à un navigateur après un certain temps. Lorsque la page de confirmation de l'utilisateur final s'affiche, les utilisateurs doivent cliquer sur un lien pour accéder au site initialement demandé ou à tout autre site Web.

Thèmes connexes

- Aviser les utilisateurs finaux des actions du proxy

Mappage de domaine

Vous pouvez configurer Secure Web Appliance de sorte que les demandes HTTPS transparentes provenant de clients particuliers ou vers des destinations particulières contournent le proxy HTTPS.

Vous pouvez utiliser l'intercommunication pour les applications qui nécessitent que le trafic passe par l'appliance, sans subir de modification, ou de vérification de certificat des serveurs de destination.

Carte de domaine pour des applications spécifiques

Avant de commencer

Assurez-vous d'avoir défini une politique d'identification pour les appareils qui nécessitent un trafic de transit vers des serveurs spécifiques. Consultez Classification des utilisateurs et logiciels clients pour obtenir de plus amples renseignements. Plus précisément, vous devez :

- Choisissez **Exempt from authentication/identification** (Dispenser de l'authentification/identification).
- Indiquer les adresses auxquelles ce profil d'identification doit s'appliquer. Vous pouvez utiliser des adresses IP, des blocs d'CIDR et des sous-réseaux.

Étape 1 Activer le proxy HTTPS. Consultez Activation du proxy HTTPS pour obtenir de plus amples renseignements.

Étape 2 Choisissez **Web Security Manager** > **Domain Map** (Web Security Manager > Carte des domaines).

a) Cliquez sur **Add Domain** (Ajouter un domaine).
b) Renseignez le champ **Domain Name** (Nom du domaine) ou indiquez le serveur de destination.
c) Choisissez l'ordre de priorité si des domaines existants sont spécifiés.
d) Entrez les adresses IP.
e) Cliquez sur **Submit** (Soumettre).

Étape 3 Choisissez **Web Security Manager** > **Custom and External URL Categories** (Web Security Manager > Catégories d'URL personnalisées et externes).

a) Cliquez sur **Add Catégorie** (Ajouter une catégorie).
b) Indiquez les renseignements suivants.

Paramètres	Description
Category Name (Nom de la catégorie)	Entrez un identifiant pour cette catégorie d'URL. Ce nom s'affiche lorsque vous configurez le filtrage d'URL pour les groupes de politiques.
List Order (Ordre de la liste)	Précisez 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 filtrage d'URL évalue une demande d'un client par rapport aux catégories d'URL personnalisées dans l'ordre spécifié.
Category Type (Type de catégorie)	Choisissez **Local Custom Category** (Catégorie personnalisée locale).
Advanced (Niveau avancé)	Vous pouvez saisir 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 schémas que vous saisissez. Consultez Expressions régulières pour plus d'informations sur l'utilisation des expressions régulières.

c) Envoyez et validez les modifications.

Étape 4 Choisissez **Web Security Manager** > **Decryption Policies** (Web Security Manager > Politiques de déchiffrement).

a) Créez une nouvelle politique de déchiffrement.
b) Choisissez le profil d'identification que vous avez créé pour contourner le trafic HTTPS pour des applications spécifiques.
c) Dans le panneau **Advanced** (Avancé), cliquez sur le lien URL Categories (Catégories d'URL).
d) Dans la colonne **Add** (Ajouter), cliquez pour ajouter la catégorie d'URL personnalisée créée à l'étape 3.
e) Cliquez sur **Done** (Terminé).
f) Dans la page des politiques de déchiffrement, cliquez sur le lien **URL Filtering** (Filtrage URL).
g) Choisissez **Pass Through** (Intercommunication).
h) Envoyez et validez les modifications.

Vous pouvez utiliser le spécificateur de format **%(** pour afficher les informations du journal d'accès. Consultez Personnalisation des journaux d'accès pour obtenir de plus amples renseignements.

Remarque

- La fonctionnalité de carte de domaine fonctionne en mode transparent HTTPS.
- Cette fonctionnalité ne fonctionne pas en mode explicite et pour le trafic HTTP.
- La catégorie personnalisée locale doit être configurée pour autoriser le trafic utilisant cette fonctionnalité.
- L'activation de cette fonctionnalité modifiera ou attribuera le nom du serveur selon le nom de serveur configuré dans la carte de domaine, même si les informations SNI sont disponibles.
- Cette fonctionnalité ne bloque pas le trafic en fonction du nom de domaine si ce trafic correspond à la mappe de domaine et si la catégorie personnalisée, la politique de déchiffrement et l'action de transmission directe correspondantes sont configurés.
- L'authentification ne fonctionne pas avec cette fonctionnalité d'intercommunication. L'authentification doit être déchiffrée, mais le trafic ne sera pas déchiffré dans ce cas.
- Le trafic UDP n'est pas surveillé. Vous devez configurer le trafic UDP pour ne pas arriver à Secure Web Appliance, mais plutôt passer directement par le pare-feu vers Internet pour des applications comme WhatsApp, Telegram, etc.
- WhatsApp, Telegram et Skype fonctionnent en mode transparent. Cependant, certaines applications comme WhatsApp ne fonctionnent pas en mode explicite en raison de restrictions appliquées à l'application.

Options du client pour la redirection des demandes Web

Si vous choisissez que les clients transfèrent explicitement les demandes au proxy Web, vous devez également décider comment configurer les clients pour le faire. Choisissez l'une des méthodes suivantes :

- **Configure Clients Using Explicit Settings** (Configurer les clients à l'aide de paramètres explicites). Configurez les clients avec le nom d'hôte et le numéro de port du proxy Web. Consultez la documentation de chaque client pour savoir comment procéder.

Note Le port du proxy Web utilise les numéros de port 80 et 3128 par défaut. Les clients peuvent utiliser l'un ou l'autre de ces ports.

- **Configure Clients Using a Proxy Auto-Config (PAC) File** [Configurer les clients à l'aide d'un fichier PAC (Proxy Auto-Config)] Les fichiers PAC fournissent aux clients des instructions sur la destination des demandes Web. Cette option vous permet de gérer de manière centralisée les modifications ultérieures apportées aux détails du proxy.

Si vous choisissez d'utiliser des fichiers PAC, vous devez également choisir l'emplacement des fichiers et la façon dont les clients les trouveront.

Thèmes connexes

- Utilisation de fichiers PAC avec les applications clientes, on page 19

Utilisation de fichiers PAC avec les applications clientes

Options de publication des fichiers de configuration automatique de proxy (PAC)

Vous devez publier les fichiers PAC là où les clients peuvent y accéder. Les emplacements valides sont les suivants :

- **Serveurs Web.**
- **Secure Web Appliance**. Vous pouvez placer les fichiers PAC sur un Secure Web Appliance, qui s'affiche pour les clients comme un navigateur Web. L'appliance propose également des options supplémentaires pour la gestion des fichiers PAC, notamment la possibilité de traiter les demandes qui utilisent des noms d'hôte, des ports et des noms de fichiers différents.
- **Ordinateurs locaux.** Vous pouvez placer le fichier PAC localement sur le disque dur d'un client. Cisco ne recommande pas cette solution comme solution générale, et elle n'est pas adaptée aux méthodes de détection automatique des fichiers PAC, mais elle peut être utile pour les tests.

Thèmes connexes

- Hébergement des fichiers PAC sur Secure Web Appliance, on page 20
- Spécification des fichiers PAC dans les applications clientes, on page 21
- Hébergement des fichiers PAC sur Secure Web Appliance, on page 20
- Spécification des fichiers PAC dans les applications clientes, on page 21

Options du client pour la recherche des fichiers de configuration automatique de proxy (PAC)

Si vous choisissez d'utiliser des fichiers PAC pour vos clients, vous devez également décider comment les clients trouveront les fichiers PAC. Vous avez le choix entre deux options :

- **Configure client with the PAC file location** (Configurer le client avec l'emplacement du fichier PAC). Configurez le client avec une URL qui pointe spécifiquement vers le fichier PAC.
- **Configure clients to detect the PAC file location automatically** (Configurez les clients pour détecter automatiquement l'emplacement du fichier PAC). Configurez les clients pour qu'ils trouvent automatiquement les fichiers PAC à l'aide du protocole WPAD avec DHCP ou DNS.

Détection automatique des fichiers PAC

WPAD est un protocole qui permet au navigateur de déterminer l'emplacement d'un fichier PAC à l'aide de DHCP et DNS.

- **Pour utiliser WPAD avec DHCP**, vous devez configurer l'option 252 sur les serveurs DHCP avec l'URL de l'emplacement du fichier PAC. Cependant, tous les navigateurs ne prennent pas en charge DHCP.
- **Pour utiliser WPAD avec DNS**, vous devez configurer un enregistrement DNS pour qu'il pointe vers le serveur hôte du fichier PAC.

Vous pouvez configurer l'une ou l'autre des options ou les deux. WPAD essaiera d'abord de trouver les fichiers PAC à l'aide de DHCP. S'il ne peut pas, il essayera le DNS.

Thèmes connexes

- Détection automatique du fichier PAC sur les clients, on page 22

Hébergement des fichiers PAC sur Secure Web Appliance

Étape 1 Choisissez **Security Services > PAC File Hosting** (Services de sécurité > Hébergement de fichiers PAC).

Étape 2 Cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Étape 3 (Facultatif) Renseignez les paramètres de base suivants :

Option	Description
PAC Server Ports (Ports du serveur PAC)	Ports que Secure Web Appliance utilisera pour écouter les demandes de fichier PAC.
PAC File Expiration (Expiration du fichier PAC)	Autorise le fichier PAC à expirer après un nombre spécifié de minutes dans la mémoire cache du navigateur.

Étape 4 Cliquez sur **Browse** (Parcourir) dans la section PAC Files (Fichiers PAC), puis sélectionnez un fichier PAC sur votre machine locale pour le charger dans Secure Web Appliance.

Note Si le fichier que vous sélectionnez s'appelle `default.pac`, vous n'avez pas à spécifier le nom du fichier lors de la configuration de son emplacement dans un navigateur. Secure Web Appliance recherche un fichier appelé `default.pac` si aucun nom n'est spécifié.

Étape 5 Cliquez sur **Upload** (Charger) pour charger le fichier PAC sélectionné à l'étape 4 dans Secure Web Appliance.

Étape 6 (Facultatif) Dans la section Hostnames for Serving PAC Files Directly (Noms d'hôte pour la diffusion directe des fichiers PAC), configurez les noms d'hôte et les noms de fichiers associés pour les demandes de fichiers PAC qui ne comprennent pas de numéro de port :

Option	Description
Hostname (Nom d'hôte)	Nom d'hôte que la demande de fichier PAC doit inclure si Secure Web Appliance doit répondre à la demande. Comme la demande ne comprend pas de numéro de port, elle sera traitée sur les ports HTTP du proxy Web (p. ex., le port 80) et doit pouvoir être considérée comme une demande de fichier PAC par la valeur de ce nom d'hôte.
Default PAC File for "Get/" Request through Proxy Port (Fichier PAC par défaut pour la demande « Get/ » par le port de proxy)	Nom du fichier PAC qui sera associé au nom d'hôte sur la même ligne. La demande au nom d'hôte renverra le fichier PAC spécifié ici. Seuls les fichiers PAC qui ont été chargés peuvent être sélectionnés.
Add Row (Ajouter une ligne)	Ajoute une autre ligne pour spécifier des noms d'hôte et des noms de fichiers PAC supplémentaires.

Étape 7 Envoyez et validez vos modifications.

Spécification des fichiers PAC dans les applications clientes

Configuration manuelle de l'emplacement d'un fichier PAC sur les clients

Étape 1 Créez et publiez un fichier PAC.

Étape 2 Entrez une URL dans la zone de configuration du fichier PAC de votre navigateur qui pointe vers l'emplacement du fichier PAC.

Les formats d'URL suivants sont valides si Secure Web Appliance héberge le fichier PAC :

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

où *WSAHostname* correspond à la valeur du **nom d'hôte** configurée lors de l'hébergement du fichier PAC sur un Secure Web Appliance. Sinon, le format de l'URL dépendra de l'emplacement de stockage et, dans certains cas, du client.

What to do next

- Hébergement des fichiers PAC sur Secure Web Appliance, on page 20

Détection automatique du fichier PAC sur les clients

Étape 1 Créez un fichier PAC appelé wpad.dat et publiez-le sur un serveur Web ou Secure Web Appliance (le fichier doit être placé dans le dossier racine d'un serveur Web si vous souhaitez utiliser WPAD avec DNS).

Étape 2 Configurez le serveur Web pour installer les fichiers .dat avec le type MIME suivant :

```
application/x-ns-proxy-autoconfig
```

Note Un Secure Web Appliance le fait automatiquement pour vous.

Étape 3 Pour prendre en charge la recherche DNS, créez un nom DNS commençant par « `wpad` » pouvant être résolu en interne (par exemple, `wpad.exemple.com`) et associez-le à l'adresse IP du serveur qui héberge le fichier `wpad.dat`.

Étape 4 Pour prendre en charge la recherche DHCP, configurez l'option 252 de votre serveur DHCP avec l'URL de l'emplacement du fichier wpad.dat (par exemple : « `http://wpad.exemple.com/wpad.dat` »). L'URL peut utiliser n'importe quelle adresse hôte valide, notamment une adresse IP, et ne nécessite pas d'entrée DNS particulière.

What to do next

- Utilisation de fichiers PAC avec les applications clientes, on page 19
- Hébergement des fichiers PAC sur Secure Web Appliance, on page 20
- WPAD ne fonctionne pas avec Firefox

Services de proxy FTP

- Survol des services proxy FTP, on page 22
- Activation et configuration du proxy FTP, on page 23

Survol des services proxy FTP

Le proxy Web peut intercepter deux types de demandes FTP :

- **FTP natif.** Les demandes FTP natives sont générées par des clients FTP dédiés (ou par des navigateurs utilisant des clients FTP intégrés). Nécessite le proxy FTP.
- **FTP sur HTTP.** Les navigateurs encodent parfois les requêtes FTP dans des demandes HTTP, plutôt que d'utiliser le FTP natif. Ne nécessitent pas le proxy FTP.

Thèmes connexes

- Activation et configuration du proxy FTP, on page 23
- Configuration des messages de notification FTP

Activation et configuration du proxy FTP

Note Pour configurer les paramètres de proxy qui s'appliquent aux connexions FTP sur HTTP, consultez Configuration des paramètres du proxy Web, on page 3.

Étape 1 Choisissez **Security Services** > **FTP Proxy** (Services de sécurité > Proxy FTP).

Étape 2 Cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres) (si la seule option disponible est **Edit Settings** (Modifier les paramètres), le proxy FTP est déjà activé).

Étape 3 (Facultatif) Configurez les paramètres de base du proxy FTP.

Propriété	Description
Proxy Listening Port (Port d'écoute proxy)	Port sur lequel le proxy FTP sera à l'écoute pour les connexions de contrôle FTP. Les clients doivent utiliser ce port lors de la configuration d'un proxy FTP (et non comme port de connexion aux serveurs FTP, qui utilisent normalement le port 21).
Caching (Mise en mémoire cache)	Si les connexions de données d'utilisateurs anonymes sont ou non mises en cache. **Note** Les données des utilisateurs non anonymes ne sont jamais mises en cache.
Server Side IP Spoofing (Usurpation d'adresses IP côté serveur)	Permet au proxy FTP d'imiter l'adresse IP du serveur FTP. Cette option prend en charge les clients FTP qui n'autorisent pas les transactions lorsque l'adresse IP est différente pour les connexions de contrôle et de données.
Client IP Spoofing (Usurpation d'adresses IP du client)	Permet au proxy FTP d'imiter l'adresse IP source du client FTP. Lorsque cette option est activée, les demandes FTP semblent émaner du client FTP plutôt que du proxy FTP.
Authentication Format (Format d'authentification)	Offre un choix de format d'authentification que le proxy FTP peut utiliser lors de la communication avec des clients FTP.
Passive Mode Data Port Range (Plage de ports de données en mode passif)	Plage de ports TCP que les clients FTP doivent utiliser pour établir une connexion de données avec le proxy FTP pour les connexions en mode passif.
Active Mode Data Port Range (Plage du port de données en mode actif)	Plage de ports TCP que les serveurs FTP devraient utiliser pour établir une connexion de données avec le proxy FTP pour les connexions en mode actif. Ce paramètre s'applique aux connexions FTP natives et FTP sur HTTP. L'augmentation de la plage de ports permet de traiter un plus grand nombre de demandes du même serveur FTP. En raison du délai TIME-WAIT de la session TCP (généralement quelques minutes), un port ne redevient pas disponible pour le *même* serveur FTP immédiatement après avoir été utilisé. Par conséquent, un serveur FTP donné ne peut pas se connecter au proxy FTP en mode actif plus de *n* fois dans un court laps de temps, *n* étant le nombre de ports indiqué dans ce champ.

Propriété	Description
Welcome Banner (Bannière de bienvenue)	La bannière de bienvenue qui s'affiche sur les clients FTP lors de la connexion. Choisissez parmi : • **FTP server message** (Message du serveur FTP). Le message sera fourni par le serveur FTP de destination. Cette option est uniquement disponible lorsque le proxy Web est configuré pour le mode transparent et s'applique uniquement aux connexions transparentes. • **Custom message** (Message personnalisé). Lorsque cette option est sélectionnée, ce message personnalisé s'affiche pour toutes les connexions FTP natives. Lorsqu'elle n'est pas sélectionnée, elle est toujours utilisée pour les connexions FTP natives de transfert explicite.

Étape 4 (Facultatif) Configurez les paramètres avancés du proxy FTP :

Propriété	Description
Control Connection Timeouts (Délais d'expiration des connexion de données)	Nombre maximal de secondes pendant lesquelles le proxy FTP attend davantage de communications dans la connexion de contrôle de la part d'un client FTP ou d'un serveur FTP inactif lorsque la transaction en cours n'est pas terminée. • **Client side** (Côté client). Valeur de délai d'expiration pour les connexions de contrôle vers les clients FTP inactifs. • **Server side** (Côté serveur). Valeur de délai d'expiration pour les connexions de contrôle aux serveurs FTP inactifs.
Data Connection Timeouts (Délais d'expiration des connexions de données)	Temps pendant lequel le proxy FTP attend davantage de communications dans la connexion de données à partir d'un client FTP ou d'un serveur FTP inactif lorsque la transaction en cours n'est pas terminée. • **Client side** (Côté client). Valeur du délai d'expiration des connexions de données vers les clients FTP inactifs. • **Server side** (Côté serveur). Valeur du délai d'expiration des connexions de données aux serveurs FTP inactifs.

Étape 5 Envoyez et validez vos modifications.

What to do next

- Survol des services proxy FTP, on page 22

Services proxy SOCKS

Survol des services de proxy SOCKS

Le Secure Web Appliance inclut un proxy SOCKS pour traiter le trafic SOCKS. Les politiques SOCKS sont l'équivalent des politiques d'accès qui contrôlent le trafic SOCKS. Tout comme les politiques d'accès, vous pouvez utiliser les profils d'identification pour indiquer les transactions qui sont régies par chaque politique SOCKS. Une fois que les politiques SOCKS sont appliquées aux transactions, les politiques de routage peuvent régir le routage du trafic.

Notez les éléments suivants concernant le proxy SOCKS :

- Le protocole SOCKS prend uniquement en charge les connexions directes.
- Le proxy SOCKS ne prend pas en charge les proxys en amont (ne transmettra pas à ces derniers).
- Le proxy SOCKS ne prend pas en charge les services d'analyse, qui sont utilisés par Application Visibility and Control (AVC), la Prévention de la perte de données (DLP) et la détection des programmes malveillants.
- Le proxy SOCKS ne prend pas en charge le traçage des politiques.
- Le proxy SOCKS ne déchiffre pas le trafic SSL; il effectue la tunnelisation du client vers le serveur.

Activation du traitement du trafic SOCKS

Before you begin

Activez le proxy Web.

Étape 1 Choisissez **Security Services** > **SOCKS Proxy** (Services de sécurité > Proxy SOCKS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Enable SOCKS Proxy** (Activer le proxy SOCKS).

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

Configuration du serveur proxy SOCKS

Étape 1 Choisissez **Security Services** > **SOCKS Proxy** (Services de sécurité > SOCKS > Proxy).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Enable SOCKS Proxy** (Activer le proxy SOCKS).

Étape 4 Configurez les paramètres de base et avancés du proxy SOCKS.

Proxy SOCKS	Activé.
SOCKS Control Ports (Ports de contrôle SOCKS)	Ports qui acceptent les demandes SOCKS. La valeur par défaut est 1080.

UDP Request Ports (Ports de demande UDP)	Ports UDP sur lesquels le serveur SOCKS doit écouter. La valeur par défaut est 16000-16100.
Proxy Negotiation Timeout (Délai d'expiration de la négociation du proxy)	Temps d'attente (en secondes) avant d'envoyer ou de recevoir des données d'un client SOCKS dans la phase de négociation. La valeur par défaut est 60.
UDP Tunnel Timeout (Délai d'expiration du tunel UDP)	Temps d'attente (en secondes) des données d'un client ou d'un serveur UDP avant de fermer le tunnel UDP. La valeur par défaut est 60.

Création des politiques SOCKS

Étape 1 Choisissez **Web Security Manager** > **SOCKS Policies** (Web Security Manager > Politiques SOCKS).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Étape 3 Attribuez un nom dans le champ **Policy Name** (Nom de la politique).

Note Chaque nom de groupe de politiques doit être unique et contenir uniquement des caractères alphanumériques ou un espace.

Étape 4 (Facultatif) Ajoutez une description.

Étape 5 Dans le champ **Insert Above Policy** (Insérer au-dessus de la politique), choisissez l'endroit dans la table des politiques SOCKS où insérer cette politique SOCKS.

Note Lorsque vous configurez plusieurs politiques SOCKS, déterminez un ordre logique pour chaque politique. Ordonnez vos politiques pour vous assurer que la correspondance est correcte.

Étape 6 Dans la section **Identity and Users** (Identités et utilisateurs), choisissez une ou plusieurs identités à appliquer à ce groupe de politiques.

Étape 7 (Facultatif) Développez la section « Advanced » (Avancé) pour définir les exigences d'appartenance supplémentaires.

Proxy Ports (Ports du proxy)	Le port configuré dans le navigateur. (Facultatif) Définissez l'appartenance au groupe de politiques par le port de proxy utilisé pour accéder au proxy Web. Entrez un ou plusieurs numéros de port dans le champ Proxy Ports (Ports du proxy). Séparez les valeurs de ports multiples par des virgules. Vous pouvez définir l'appartenance à un groupe de politiques sur le port du proxy, si un ensemble de clients est configuré pour transférer explicitement les demandes sur un port et un autre ensemble de clients est configuré pour transférer explicitement les demandes sur un port différent. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques SOCKS.

Subnets (Sous-réseaux)	(Facultatif) Définissez l'appartenance au groupe de politiques par sous-réseau ou autres adresses. Vous pouvez choisir d'utiliser les **adresses** qui peuvent être **définies** avec l'**identité** associée ou vous pouvez entrer des **adresses spécifiques** ici. **Note** Si l'identité associée à ce groupe de politiques définit ses membres par des adresses, dans ce groupe de politiques, vous devez saisir des adresses qui constituent un sous-ensemble des adresses de l'identité. L'ajout d'adresses dans le groupe de politiques réduit davantage la liste des transactions qui correspondent à ce groupe de politiques.
Time Range (Plage de temps)	(Facultatif) Définir l'appartenance au groupe de politiques par plage de temps : **a.** Sélectionnez une plage de temps dans le champ **Time Range** (Plage de temps). **b.** Indiquez si ce groupe de politiques doit s'appliquer aux heures à l'intérieur ou à l'extérieur de la plage de temps sélectionnée.

Étape 8 Envoyez et validez les modifications.

What to do next

- (Facultatif) Ajoutez une identité à utiliser avec les politiques SOCKS.
- Ajoutez une ou plusieurs politiques SOCKS pour gérer le trafic SOCKS.

Cisco Umbrella Seamless ID

La fonctionnalité Cisco Umbrella Seamless ID permet à l'appliance de transmettre les informations d'identification de l'utilisateur à Cisco Umbrella Secure Web Gateway (SWG) après une authentification réussie. Cisco Umbrella SWG vérifie les informations de l'utilisateur dans Active Directory en fonction des informations d'identification authentifiées reçues de Secure Web Appliance. Cisco Umbrella SWG considère l'utilisateur comme authentifié et lui fournit un accès en fonction des politiques de sécurité définies.

Secure Web Appliance transmet les informations d'identification de l'utilisateur à Cisco Umbrella SWG à l'aide des en-têtes HTTP; X-USWG-PKH, X-USWG-SK et X-USWG-Data.

Remarque

- Les en-têtes Cisco Umbrella Seamless ID remplacent les en-têtes avec le même nom sur Secure Web Appliance, le cas échéant.
- La fonctionnalité Cisco Umbrella Seamless ID prend en charge le schéma d'authentification auprès d'Active Directory uniquement. Cette fonctionnalité ne prend pas en charge LDAP, Cisco Identity Services Engine (ISE) et l'agent Cisco Context Directory (CDA).
- Cisco Umbrella SWG ne prend pas en charge le trafic FTP et SOCKS.

Tableau 1 : Comportement du trafic HTTPs

Mode de déploiement	Méthode de substitution	Decrypt for Authentication (Déchiffrer pour authentification)	Authentification Secure Web Appliance	Partage Cisco Umbrella Seamless ID
Explicite	Substitution d'IP	Oui/Non	Oui	Oui
Transparent	Substitution d'IP	Oui	Oui	Oui
Transparent	Substitution d'IP	Non	Ignore l'authentification	Non
Explicite	Témoin, sans chiffrement des identifiants	Oui/Non	Oui	Oui
Explicite	Témoin, avec chiffrement des identifiants	Oui/Non	Oui	Non
Transparent	Témoin avec/sans chiffrement des identifiants	Oui/Non	Ignore l'authentification	Non

Remarque Secure Web Appliance récupère la valeur UPN pour l'utilisateur authentifié à partir d'Active Directory et permet à Cisco Umbrella Seamless ID d'appliquer les politiques Web correctes pour les utilisateurs. Pour que cette fonctionnalité soit opérante, vous devez affecter à tous les utilisateurs Active Directory des valeurs UPN par défaut ou personnalisées.

Cette section aborde les points suivants :

- Configuration de Cisco Umbrella Seamless ID
- Configuration de la destination de routage pour Cisco Umbrella SWG

Configuration de Cisco Umbrella Seamless ID

Avant de commencer

- Chargez manuellement le certificat racine ou Cisco Umbrella personnalisé sur l'appliance en sélectionnant **Network** > **Certificate Management** > **Manage Trusted Root Certificates**(Réseau > Gestion des certificats > Gérer les certificats racine approuvés). Voir Gestion des certificats.
- Assurez-vous d'avoir configuré les profils d'identification pour l'authentification.
- Définissez des politiques de routage avec des profils d'identification configurés.

Étape 1 Choisissez **Web Security Manager** > **Cisco Umbrella Seamless ID** .

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Saisissez l'adresse IP ou le nom d'hôte Cisco Umbrella SWG.

Étape 4 Entrez les numéros de port du SWG pour le trafic HTTP et HTTPS.

Vous pouvez saisir au maximum six numéros de port.

Étape 5 (Facultatif) Cliquez sur **Connectivity Test** (Test de connectivité) pour vérifier la connectivité de Cisco Umbrella SWG sur les ports et la validation des certificats.

Étape 6 Entrez l'ID unique d'organisation du client de Cisco Umbrella SWG.

Étape 7 Envoyez et validez.

Configuration de la destination de routage pour Cisco Umbrella SWG

Pour créer une nouvelle politique de routage, consultez Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage.

.

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 dans la colonne **Routing Destination** (Destination de routage) correspondant à la politique de routage dont vous souhaitez configurer le Cisco Umbrella Seamless ID avec le port requis.

Étape 3 Sélectionnez le Cisco Umbrella Seamless ID approprié avec port comme groupe de proxys en amont pour la politique. La liste déroulante Upstream Proxy Group (Groupe de proxys en amont) affiche tous les Cisco Umbrella Seamless ID avec ports que vous avez configurés dans la page **Cisco Umbrella Seamless ID** (**Web Security Manager** > **Cisco Umbrella Seamless ID**).

Remarque Si vous supprimez un **Cisco Umbrella Seamless ID** avec un numéro de port (**Web Security Manager** > **Cisco Umbrella Seamless ID**) déjà associé à une politique de routage, la destination du routage est automatiquement remplacée par « Direct Connection » (Connexion directe).

Étape 4 Envoyez et validez vos modifications.

Résolution de problèmes de demandes d'interception

- Les catégories d'URL ne bloquent pas certains sites FTP
- Déconnexion des transferts FTP volumineux
- Le fichier de zéro octet apparaît sur les serveurs FTP après le chargement du fichier
- Unable to Route FTP Requests Via an Upstream Proxy (Impossible d'acheminer les requêtes FTP de la voie de routage par le biais d'un proxy en amont)
- 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

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.