Guide Produit de McAfee Client Proxy 4.1.x

Trellix

Table des matières

Présentation du produit

Présentation

Le logiciel McAfee® Client Proxy aide à protéger vos utilisateurs de terminaux contre les menaces de sécurité qui se présentent lorsqu'ils accèdent au web à partir de votre réseau ou en dehors de celui-ci.

Le logiciel client, installé sur les terminaux exécutant Microsoft Windows ou macOS, redirige les demandes web ou leur permet d'être redirigées vers un proxy pour le filtrage. Le logiciel serveur s'exécute sur l'une des trois plates-formes de gestion suivantes : McAfee ePO, McAfee ePO Cloud ou MVISION ePO.

Solution hybride Web Protection

Client Proxy est un composant essentiel de la solution hybride McAfee® Web Protection. Cette solution vous permet d'intégrer les fonctions de sécurité basées sur le réseau et sur le cloud fournies par McAfee® Web Gateway et McAfee® Web Gateway Cloud Service (McAfee® WGCS), respectivement.

Le logiciel Client Proxy autorise ou redirige le trafic web en fonction de l'emplacement du terminal :

- **Terminaux situés à l'intérieur du réseau ou connectés par VPN** : le trafic est autorisé à être redirigé vers une appliance Web Gateway installée sur le réseau pour le filtrage.
- **Terminaux situés en dehors du réseau** : le trafic est redirigé vers McAfee WGCS pour le filtrage.

Intégration avec Endpoint Security

Lors du déploiement de Client Proxy avec McAfee® Endpoint Security sur les terminaux, vous devez installer et gérer chaque produit séparément à l'aide de McAfee® ePolicy Orchestrator® (McAfee® ePO™) , McAfee ePO Cloud ou MVISION ePO.

- Administrateurs Client Proxy : configurez les stratégies et exécutez les tâches comme d'habitude.
- Administrateurs Endpoint Security : vous avez la possibilité de configurer Contrôle Web McAfee® Endpoint Security pour qu'il soit désactivé pendant l'installation de Client Proxy et qu'il redirige activement le trafic web.

Sur les terminaux exécutant Windows, vous pouvez voir si Client Proxy est installé et en cours d'exécution sur le terminal et s'il redirige activement le trafic en ouvrant la fenêtre **A propos de McAfee Client Proxy** depuis le menu **Démarrer**.

Fonctionnalités clés

Client Proxy autorise ou redirige les demandes web des utilisateurs en fonction des stratégies que vous configurez.

- **Redirection du trafic** : le logiciel redirige le trafic web vers les serveurs proxy pour le filtrage en fonction des paramètres de la stratégie Client Proxy.
- **Prise en compte de l'emplacement** : les paramètres de prise en compte de l'emplacement permettent à une stratégie de couvrir les utilisateurs travaillant à l'intérieur du réseau, en dehors du réseau, ou connectés au réseau par VPN.
- **Gestion centralisée** : le logiciel est géré avec McAfee ePO, McAfee ePO Cloud, ou MVISION ePO.

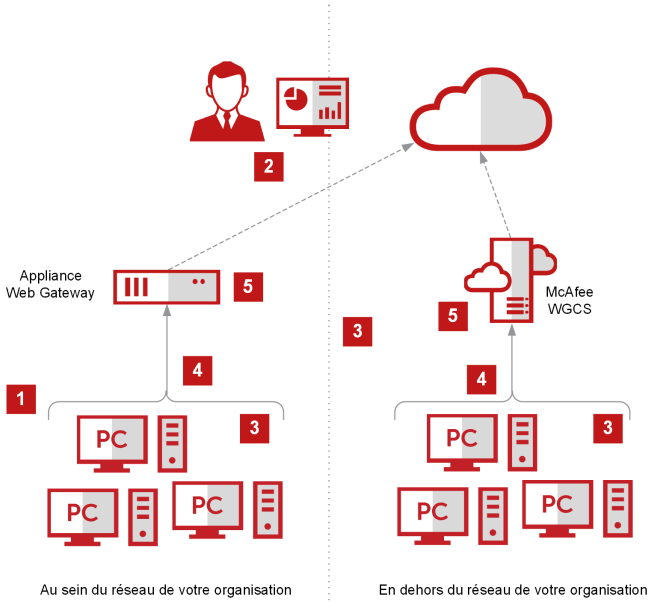
- **Indépendance du navigateur** : les paramètres du serveur proxy sont configurés dans Client Proxy plutôt que dans les navigateurs en cours d'exécution sur les terminaux.
- **Authentification transparente** : Client Proxy authentifie les utilisateurs sans demander d'informations d'identification et transmet l'appartenance aux groupes et d'autres informations dans les métadonnées qu'il ajoute aux requêtes HTTP/HTTPS.
- **Résistance à la falsification** : les utilisateurs ne sont pas autorisés à supprimer le logiciel Client Proxy à partir du terminal sans avoir demandé et reçu un code d'autorisation temporaire d'un administrateur.
- **Canal sécurisé** : le logiciel établit un canal de communication sécurisé entre Client Proxy et McAfee WGCS pour toutes les demandes HTTP/HTTPS. Cela s'applique uniquement aux proxys de cloud.

Fonctionnement

Le logiciel Client Proxy redirige, bloque ou autorise le trafic web en fonction de la stratégie Client Proxy et de l'emplacement des terminaux.

Workflow de Client Proxy

1. Le logiciel Client Proxy est installé sur les terminaux de votre organisation.
2. A l'aide de McAfee ePO, McAfee ePO Cloud, ou MVISION ePO, l'administrateur crée une stratégie Client Proxy et affecte la stratégie à tous les terminaux managés.
3. Les terminaux managés peuvent être situés à l'intérieur du réseau de votre organisation, connectés au réseau par VPN ou situés en dehors du réseau.
4. Les utilisateurs travaillant sur les terminaux demandent l'accès aux ressources web.
5. Le logiciel détermine l'emplacement de l'utilisateur, puis autorise ou redirige la demande web :
    - Dans le réseau ou connecté par VPN : permet à la demande web d'être transmise à une appliance Web Gateway installée sur le réseau, où elle est ensuite filtrée. Client Proxy est passif.
    - En dehors du réseau : redirige la demande web vers McAfee WGCS pour le filtrage. Client Proxy est actif.


2
Appliance
Web Gateway
5
3
5
McAfee
WGCS
4
4
1
3
3
PC
PC
PC
PC
PC
PC
Au sein du réseau de votre organisation
En dehors du réseau de votre organisation

Gestion des stratégies Client Proxy

Métadonnées de Client Proxy

Lorsque le logiciel Client Proxy redirige le trafic HTTP/HTTPS, il ajoute des métadonnées aux demandes.

D'autres produits, tels que Web Gateway et McAfee WGCS, utilisent les métadonnées (par exemple, l'appartenance aux groupes) lors de l'application des stratégies de protection web.

- Jetons d'authentification : jetons contenant des informations d'identité sur l'utilisateur qui effectue la demande web
- Version d'authentification : version des métadonnées partagées par Client Proxy
- Adresse IP du client : adresse IP du terminal d'où provient le trafic
- Adresse IP de la destination d'origine : adresse IP enregistrée du serveur vers lequel le trafic est dirigé
- ID du client : identifie de façon unique l'organisation du client
- ID utilisateur : identifie de façon unique l'utilisateur qui effectue la demande web
- Groupes d'utilisateurs : noms des groupes dont l'utilisateur est membre
- ID de locataire : ID partagé par les nœuds d'un cluster (McAfee ePO Cloud ou MVISION ePO)
- Nom du processus : nom du processus générant le trafic
- Chemin d'accès de l'exécutable du processus : chemin d'accès au processus qui génère le trafic
- Informations système : informations système telles que le nom du système d'exploitation de l'hôte (Windows, Mac), l'heure locale (en secondes depuis le 1/1/1970), l'adresse Mac, la durée d'activité du processus, le nom du système et le nom de la stratégie MCP

Ensembles d'autorisations (McAfee ePO)

Autorisations d'utilisateur

Vous pouvez gérer les autorisations d'utilisateur en configurant les ensembles d'autorisations dans l'interface McAfee ePO, et en attribuant un ensemble d'autorisations à chaque rôle.

L'interface utilisateur est fournie avec des rôles et des ensembles d'autorisations prédéfinis que vous pouvez modifier. Vous pouvez également ajouter un rôle et configurer un ensemble d'autorisations pour celui-ci.

Utilisateurs administrateurs

Le rôle prédéfini **Administrateur du catalogue MCP** dispose de toutes les autorisations requises pour créer, supprimer et gérer les stratégies Client Proxy. Un ensemble d'autorisations complet est nécessaire pour donner aux administrateurs Client Proxy l'autorisation de :

- Créer, supprimer et gérer des stratégies
- Envoyer les stratégies en mode Push vers les terminaux
- Afficher les requêtes

- Gérer l'extension logicielle Client Proxy
- Exécuter les fonctions du référentiel maître
- Exécuter les fonctions Help Desk

Seuls les administrateurs McAfee ePO disposent des autorisations nécessaires pour gérer l'extension logicielle, y compris :

- Installer des extensions sur un serveur McAfee ePO
- Supprimer des extensions sur un serveur McAfee ePO
- Mettre à jour des extensions sur un serveur McAfee ePO

Configuration d'un ensemble d'autorisations

Vous pouvez mettre à jour les ensembles d'autorisations pour un rôle existant ou les configurer pour un nouveau rôle.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO en tant qu'administrateur.

Procédure

1. Dans le menu de McAfee ePO, sélectionnez **Gestion des utilisateurs** → **Ensembles d'autorisations**.
2. Sous **Ensembles d'autorisations**, sélectionnez un rôle.
3. Dans le volet de configuration, cliquez sur **Modifier** pour ouvrir un ensemble d'autorisations.
4. Mettez à jour les paramètres de l'ensemble d'autorisations, puis cliquez sur **Enregistrer**.

Autorisations requises pour l'administration de Client Proxy

Des autorisations spécifiques sont requises pour l'administration de Client Proxy.

Autorisations d'administrateur pour Client Proxy

Autorisations	Paramètres	Requis pour...
Gestionnaire d'agents	Sélectionner **Afficher les gestionnaires d'agents**	• Envoyer les stratégies en mode Push vers les terminaux • Afficher les requêtes
Evénements client	Sélectionner **Afficher les événements client**	• Envoyer les stratégies en mode Push vers les terminaux • Afficher les requêtes

Autorisations	Paramètres	Requis pour...
Common Catalog	Sélectionner un **Modèle d'autorisation du catalogue**, puis sélectionner toutes les actions Common Catalog : • **Créer, renommer et dupliquer des catalogues** • **Supprimer des catalogues** • **Importer des éléments de catalogue à partir d'autres catalogues** • **Importer des éléments de catalogue à partir de fichiers** • **Exporter des éléments de catalogue vers des fichiers**	Créer, supprimer et gérer des stratégies
Actions Help Desk	Sélectionner toutes les actions de Client Proxy : • **Générer une clé de désinstallation du client** • **Générer une clé de contournement du client** • **Générer une clé de réponse maître pour les clés ci-dessus**	Exécuter les fonctions Help Desk **Note:** Les administrateurs McAfee ePO disposent de toutes les autorisations Help Desk par défaut. Avant de pouvoir accorder ces autorisations à d'autres administrateurs, vous devez d'abord installer l'extension Help Desk.
McAfee Agent	• **McAfee Agent : stratégie** : sélectionner **Afficher et modifier les paramètres** • **McAfee Agent : tâches** : sélectionner **Afficher et modifier les paramètres**	• Envoyer les stratégies en mode Push vers les terminaux • Afficher les requêtes
Stratégie MCP	Sélectionner **Afficher et modifier les paramètres de stratégie et de tâche**	Créer, supprimer et gérer des stratégies
Requêtes et rapports	Sélectionner **Modifier des groupes publics, créer et modifier des requêtes ou rapports privés, rendre publics des requêtes ou rapports privés.**	• Envoyer les stratégies en mode Push vers les terminaux • Afficher les requêtes

Autorisations	Paramètres	Requis pour...
Logiciel	**Référentiel maître** : sélectionner **Ajouter, supprimer et modifier des packages, exécuter des tâches d'extraction** **Référentiels distribués** : sélectionner **Ajouter, supprimer et modifier des référentiels, exécuter des tâches de réplication**	Exécuter les fonctions du référentiel maître : • Ajouter des packages logiciels • Supprimer des packages logiciels • Actualiser les packages archivés
Systèmes	**Arborescence des systèmes** : sélectionner **Afficher l'onglet "Arborescence des systèmes"** **Actions** : sélectionner : • **Réactiver les agents, afficher le journal d'activité de l'agent** • **Modifier les systèmes et les groupes de l'Arborescence des systèmes** • **Déployer des agents** **Utilisation des marqueurs** : sélectionner **Appliquer, exclure et effacer les marqueurs** **Catalogue de marqueurs** : sélectionner **Créer et modifier les marqueurs, les groupes de marqueurs et les critères de marquage**	• Envoyer les stratégies en mode Push vers les terminaux • Afficher les requêtes
Accès à l'Arborescence des systèmes	Sélectionner **Mon organisation**	• Envoyer les stratégies en mode Push vers les terminaux • Afficher les requêtes

Vérification et approbation des stratégies

Vous pouvez configurer la vérification et l'approbation des stratégies Client Proxy dans l'interface McAfee ePO.

Les tâches de configuration incluent la création des ensembles d'autorisations, leur affectation aux utilisateurs et la configuration des paramètres d'approbation sur la page**Paramètres serveur**.

1. Création d'ensembles d'autorisations de gestion de stratégies :
    - Ensemble d'autorisations d'utilisateur de stratégie : les utilisateurs de stratégie ont l'autorisation de créer ou de modifier des stratégies et doivent soumettre les modifications pour vérification.

- Ensemble d'autorisations d'administrateur de stratégie : les administrateurs de stratégie ont l'autorisation d'approuver et d'enregistrer les stratégies nouvelles ou modifiées ou de rejeter les modifications.

2. Création d'utilisateurs de gestion des stratégies :
   - Utilisateur de stratégie : créez cet utilisateur et affectez l'ensemble d'autorisations d'utilisateur de stratégie.
   - Administrateur de stratégie : permet de créer cet utilisateur et d'affecter l'ensemble d'autorisation d'administrateur de stratégie.
3. Configurez les paramètres d'approbation des modifications de stratégie dans le volet **Approbations** de la page **Paramètres serveur**.
   - Utilisateur de stratégie : pour obliger les utilisateurs de stratégie à soumettre des modifications de stratégie pour vérification, sélectionnez **Les utilisateurs ont besoin d'une approbation pour les modifications de stratégie**.
   - Administrateur de stratégie : pour exiger que les administrateurs de stratégies soumettent également les modifications de stratégie pour vérification, sélectionnez **Les administrateurs et les approbateurs ont besoin d'une approbation pour les modifications de stratégie**.

Pour plus d'informations, consultez le *Guide Produit de McAfee ePolicy Orchestrator*.

Méthode d'utilisation du mot de passe partagé

Le mot de passe partagé est le mot de passe qui sécurise la communication entre Client Proxy et Web Gateway ou McAfee WGCS. Le mot de passe partagé est parfois appelé secret partagé.

Si vous configurez Client Proxy lors d'un déploiement local, sur le cloud uniquement ou de manière hybride, le mot de passe partagé sécurise la communication entre les produits et les stratégies. Les détails de la configuration varient en fonction de la plate-forme de gestion.

Géré avec McAfee ePO

1. Téléchargez votre ID client et le mot de passe partagé à partir d'un serveur Web Gateway dans un fichier .xml.
2. Dans l'interface McAfee ePO, importez vos informations d'identification à partir du fichier .xml sur la page **Configuration client** lors de la configuration d'une stratégie Client Proxy.

Géré avec McAfee ePO Cloud

1. Dans l'interface McAfee ePO Cloud, configurez le secret partagé sur la page **Configuration client** lors de la configuration d'une stratégie Client Proxy.
2. Pour partager vos informations d'identification manuellement, exportez votre ID client et le mot de passe partagé dans un fichier .xml.

Géré avec MVISION ePO

1. Téléchargez votre ID client et le mot de passe partagé à partir d'un serveur Web Gateway dans un fichier .xml.
2. Dans l'interface de MVISION ePO, importez vos informations d'identification à partir du fichier .xml sur la page **Administration MCP**.

Déploiement hybride

1. Dans l'interface McAfee ePO Cloud, configurez le mot de passe partagé et exportez vos informations d'identification dans un fichier .xml.
2. Dans l'interface McAfee ePO, importez vos informations d'identification à partir du fichier .xml.

Considérations à prendre en considération lors de la modification du mot de passe partagé (McAfee ePO Cloud)

Lors de la modification du mot de passe partagé dans l'interface McAfee ePO Cloud, prévoyez un temps suffisant pour sa mise à jour dans le système.

La mise à jour du mot de passe partagé implique les actions système et les estimations de temps suivantes :

1. McAfee ePO Cloud déploie la mise à jour de la stratégie Client Proxy sur les terminaux de votre organisation. La durée de cette action dépend de la valeur configurée pour le paramètre **Intervalle de mise en œuvre de stratégie** de votre stratégie McAfee Agent.
2. Le logiciel Client Proxy installé sur les terminaux partage le nouveau mot de passe avec McAfee WGCS. Cette action peut prendre jusqu'à 20 minutes.

Caution

Le mot de passe partagé doit être synchronisé dans McAfee WGCS, faute de quoi l'authentification échoue.

Importation de votre ID client et de votre mot de passe partagé (MVISION ePO)

Lors de la création de stratégies Client Proxy sur MVISION ePO ou d'une migration de stratégies Client Proxy en local vers MVISION ePO, téléchargez l'ID client et le mot de passe partagé à partir d'un serveur de passerelle web vers un fichier .xml et importez le fichier sur la page **Administration MCP**.

Note

La migration de stratégies Client Proxy en local vers MVISION ePO est prise en charge depuis Client Proxy en local 3.0.0 et versions ultérieures. Pour plus d'informations sur la migration de McAfee ePO en local vers MVISION ePO, consultez le *Guide de démarrage rapide de la migration vers MVISION ePO* sur le portail de documentation produit McAfee *(docs.mcafee.com)*.

Procédure

1. Dans le menu de MVISION ePO, sélectionnez **Configuration** → **Administration MCP**.
2. En regard de **Identifiant client**, cliquez sur **Choisir un fichier**. Accédez au dossier contenant le fichier. xml, sélectionnez-le, puis cliquez sur **Ouvrir**.

Résultats

L'ID client et le mot de passe partagé sont importés dans Client Proxy. Toutes les stratégies existantes et nouvelles sont mises à jour avec l'ID client et le mot de passe partagé importés.

Création d'une instance Common Catalog (McAfee ePO ou McAfee ePO Cloud)

Vous pouvez créer une instance Common Catalog pour Client Proxy, puis la sélectionner lors de la configuration de la liste de contournement dans une stratégie.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO ou McAfee ePO Cloud en tant qu'administrateur.

Les instances de catalogue Client Proxy sont disponibles dans le monde entier. Vous pouvez associer chaque instance à plusieurs stratégies.

Un catalogue Client Proxy comprend des listes d'éléments regroupés selon les catégories ou types suivants :

- Noms de domaine
- Adresses réseau
- Ports réseau
- Noms de processus

Sur la page Common Catalog, vous pouvez créer et configurer une instance de catalogue. Vous pouvez afficher les listes d'éléments dans chaque catégorie et ajouter, modifier ou supprimer des éléments dans les listes. Ajoutez autant de listes que nécessaire à l'instance de catalogue.

Procédure

1. Dans le menu de McAfee ePO ou McAfee ePO Cloud, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste déroulante **Actions** située sur la page **Liste des catalogues**, sélectionnez **Nouveau catalogue**.
3. Spécifiez un nom pour le nouveau catalogue et ajoutez une description facultative, puis cliquez sur **OK**.
4. Sous **Source/Destination**, dans le volet **Common Catalog**, sélectionnez une catégorie :
   - **Nom de domaine** : le trafic web envoyé aux domaines de cette liste contourne le serveur proxy. Exemple : google.com
   - **Adresse réseau (IP)** : le trafic web envoyé aux adresses IP de cette liste contourne le serveur proxy. Les adresses peuvent être configurées individuellement, sous forme de plage ou à l'aide d'un sous-réseau.
     Exemples :
     - 192.168.1.1
     - 172.31.255.10–172.31.255.20

- 10.50.0.0/255.255.128.0
- 10.50.0.0/17

- **Port réseau** : le trafic web envoyé aux ports de cette liste contourne le serveur proxy. Exemples : 40, 80, 400 – 500
- **Liste des noms de processus** : le trafic web provenant des processus de cette liste contourne le serveur proxy. Un processus s'exécute sur les terminaux. Les noms des processus Windows doivent se terminer par l'extension .exe. Les noms des processus macOS ne nécessitent pas d'extension de nom de fichier. Ajoutez McAfee et d'autres processus approuvés à cette liste.

5. Dans la liste déroulante **Actions**, sélectionnez **Nouvelle**.
6. Attribuez un nom unique à la liste ou utilisez le nom par défaut.
7. Cliquez sur **Ajouter** pour ajouter des éléments à la liste, puis cliquez sur **Enregistrer**.
   La liste est ajoutée à Common Catalog.

Résultats

L'instance Common Catalog est configurée et enregistrée.

Configuration d'une stratégie

Créer une stratégie Client Proxy

Une stratégie Client Proxy est constituée d'une liste de serveurs proxy, de paramètres de redirection, d'une liste de contournement et d'une liste de blocage qui déterminent si et où Client Proxy redirige les demandes web.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Vous pouvez créer une nouvelle stratégie à l'aide d'une stratégie existante en tant que modèle. En tant que modèle, la stratégie par défaut est en lecture seule et ne peut pas être renommée, supprimée, exportée, importée ou affectée aux terminaux.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Nouvelle stratégie**.
4. Dans la liste déroulante **Création d'une stratégie basée sur cette stratégie existante**, sélectionnez une stratégie existante à utiliser comme modèle pour la nouvelle stratégie.
5. Spécifiez le nom de la nouvelle stratégie, puis cliquez sur **OK** pour l'enregistrer.

Note

Lors de la configuration de la première stratégie sur un système Mac, sous Big Sur 11.2 et versions ultérieures, une alerte vous invite à autoriser l'adaptateur réseau McAfeeSystemExtensions. Cliquez sur **Autoriser** pour charger McAfeeSystemExtensions. Client Proxy ne redirigera pas le trafic tant que vous n'aurez pas choisi de l'autoriser. Vous devez redémarrer Client Proxy manuellement pour afficher à nouveau le volet de consentement. Pour plus d'informations, reportez-vous à l'article KB94092 de la base de connaissances McAfee.

Résultats

Vous pouvez configurer la nouvelle stratégie maintenant ou annuler la configuration, puis sélectionner et modifier la stratégie plus tard à partir du**Catalogue de stratégies**.

Gestion de la liste des serveurs proxy par Client Proxy

Le logiciel Client Proxy conserve une liste hiérachisée des serveurs proxy.

Le serveur proxy ayant le temps de réponse le plus rapide est placé en haut de la liste. Le logiciel met à jour la liste ponctuellement.

Par exemple, la liste est mise à jour lorsque l'utilisateur démarre l'ordinateur ou que la stratégie Client Proxy est modifiée. Elle est également mise à jour lorsque la connexion VPN est interrompue ou lorsqu'un serveur proxy ne répond pas. Dans ces cas-là, le logiciel teste les connexions aux serveurs proxy et réorganise la liste en fonction des temps de réponse.

Si la redirection vers le serveur proxy en tête de liste échoue, le logiciel tente une redirection vers le deuxième serveur proxy de la liste. Dans le même temps, le logiciel teste à nouveau les connexions aux serveurs proxy et met à jour la liste.

Lorsque vous configurez la façon dont le logiciel Client Proxy sélectionne le serveur proxy suivant dans la liste, vous accédez aux options suivantes :

- **Se connecter au premier serveur proxy accessible dans l'ordre de la liste ci-dessous** : le logiciel sélectionne le serveur proxy suivant dans la liste que vous avez établie.
- **Se connecter au serveur proxy avec le temps de réponse le plus rapide** : le logiciel sélectionne le serveur proxy suivant dans sa liste, en fonction du temps de réponse.

Basculement automatique du proxy

Lorsque cette option est activée, le logiciel vérifie la liste des serveurs proxy selon l'intervalle spécifié. Si un serveur proxy avec une priorité plus élevée est disponible, le logiciel bascule automatiquement vers celui-ci.

L'option de sélection automatique du proxy n'est disponible que lorsque **Se connecter au premier serveur proxy accessible dans l'ordre de la liste ci-dessous** est sélectionné.

Configurer la liste des serveurs proxy

Pour rediriger le trafic web vers un serveur proxy, configurez la liste et les règles du serveur proxy.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Lorsque vous configurez la liste des serveurs proxy, déterminez si Client Proxy est déployé avec McAfee ePO, McAfee ePO Cloud ou MVISION ePO.

- **En local** : configurez au moins l'une des appliances Web Gateway installées sur votre réseau en tant que serveur proxy.
- **Dans le cloud** : configurez McAfee WGCS en tant que serveur proxy et suivez le format de nom d'hôte : c<ID_client>.saasprotection.com.

  Exemple : c12345678.saasprotection.com

Note

Pour pouvoir enregistrer la stratégie, vous devez indiquer l'adresse IP ou le nom d'hôte d'au moins un serveur proxy ainsi qu'un numéro de port.

Note

Lorsque vous activez le paramètre **Canal sécurisé** d'au moins un proxy de cloud configuré dans la liste des serveurs proxy, Client Proxy ignore les serveurs proxy en local et prend uniquement en considération les serveurs proxy de cloud dans la liste. En fonction de la disponibilité du serveur proxy de cloud et du port, Client Proxy applique la fonction de redirection, de blocage ou de secours (autoriser la connexion sans canal sécurisé). Les proxies avec des domaines comme c*******.wgcs.mcafee-cloud.com et c*******.saasprotection.com sont considérés comme des proxys de cloud.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans le menu **Paramètres de Client Proxy**, sélectionnez **Serveurs proxy**.
6. Pour spécifier le mode de sélection des serveurs proxy dans la liste, sélectionnez une option :

   -

     Se connecter au premier serveur proxy accessible dans l'ordre de la liste ci-dessous : le logiciel sélectionne le serveur proxy suivant dans la liste que vous avez établie.

   -

Se connecter au serveur proxy avec le temps de réponse le plus rapide : le logiciel sélectionne le serveur proxy suivant dans sa liste, en fonction du temps de réponse.

7. Pour ajouter des serveurs proxy à la **Liste des serveurs proxy**, configurez les paramètres ci-dessous, puis cliquez sur **Ajouter**.
   - **Adresse du serveur proxy** : spécifie l'adresse IP ou le nom d'hôte du serveur proxy.
   - **Port de proxy** : spécifie le numéro de port du serveur proxy.
   - **HTTP/HTTPS** : cochez cette case pour rediriger le trafic envoyé vers les ports 80 et 443 vers un serveur proxy.
   - **Ports non HTTP/HTTPS redirigés** : spécifie les numéros de port des protocoles autres que HTTP/HTTPS dont vous souhaitez rediriger le trafic. Vérifiez que le serveur proxy prend en charge ces protocoles. Vous pouvez saisir jusqu'à 1 024 caractères dans ce champ.
8. Sélectionnez **Activer le basculement automatique de proxy**, puis spécifiez une valeur pour l'**Intervalle d'interrogation** dans cette plage : 10 – 3600 secondes. La valeur recommandée est 60 secondes.

   L'option de sélection automatique du proxy n'est disponible que lorsque **Se connecter au premier serveur proxy accessible dans l'ordre de la liste ci-dessous** est sélectionné.

   Note

   En cas d'utilisation de la fonctionnalité **Canal sécurisé**, le paramètre **Activer le basculement automatique de proxy** n'est pas applicable pour une liste de serveurs proxy.

9. Dans le champ **Spécifiez les ports supplémentaires que vous souhaitez rediriger en tant que trafic HTTP/HTTPS**, spécifiez les autres ports dont vous souhaitez rediriger le trafic comme trafic HTTP/HTTPS. Par exemple, vous pouvez rediriger le trafic envoyé vers une application. Vous pouvez saisir jusqu'à 1 024 caractères dans ce champ.
10. Sélectionnez **Bloquer le trafic sur les ports configurés si aucun des serveurs proxy n'est accessible** si vous le souhaitez.
    Si aucun des serveurs proxy configurés n'est accessible, tout le trafic vers les ports configurés et les ports 80 et 443 par défaut est bloqué.
11. Sélectionnez **Bloquer le trafic sur les ports configurés jusqu'à ce que la stratégie MCP soit prête** pour protéger le terminal lorsque Client Proxy est en cours de démarrage.
    Tout le trafic vers les ports configurés et les ports par défaut 80 et 443 est bloqué à partir du moment où l'utilisateur dispose d'un accès Internet jusqu'à ce que Client Proxy quitte le mode de contournement et commence à rediriger le trafic.
12. Sélectionnez **Bloquer le trafic IPv6 sur les ports configurés** pour exiger que les navigateurs web reviennent à IPv4.
13. Sélectionnez **Bloquer le trafic lorsque l'authentification mutuelle avec le proxy a échoué** pour garantir que Client Proxy redirige uniquement les demandes web dont il peut authentifier le serveur proxy.
14. Désélectionnez **Contourner le serveur proxy pour les adresses locales** pour rediriger tout le trafic, y compris le trafic envoyé aux adresses locales au sein du sous-réseau de votre organisation, vers un serveur proxy. Vous pouvez configurer une adresse IP, un intervalle d'adresses IP, un sous-réseau ou un CIDR. Par exemple, 192.168.1.1, 172.31.255.10-172.31.255.20, 10.50.0.0/255.255.128.0 ou 10.50.0.0/17.
15. Sélectionnez **Bloquer le trafic UDP sur les ports 80/443 pour IPv4 et IPv6** pour bloquer le trafic.
16. Cliquez sur **Enregistrer**.

Résultats

La liste des serveurs proxy est enregistrée avec la stratégie.

Configuration de la liste des serveurs proxy secondaires

Vous pouvez configurer des serveurs proxy secondaires et répartir le trafic web sélectionné sur plusieurs serveurs proxy. Lorsqu'un autre serveur proxy est en panne et que le serveur principal est disponible, Client Proxy redirige tout le trafic vers le serveur proxy principal. Lorsqu'un serveur proxy primaire est en panne, Client Proxy redirige le trafic marqué pour une autre redirection vers le serveur proxy secondaire.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Lorsque vous configurez la liste des serveurs proxy, déterminez si Client Proxy est déployé avec McAfee ePO, McAfee ePO Cloud ou MVISION ePO.

- **En local** : configurez au moins l'une des appliances Web Gateway installées sur votre réseau en tant que serveur proxy.
- **Dans le cloud** : configurez McAfee WGCS en tant que serveur proxy et suivez le format de nom d'hôte : c<ID_client>.saasprotection.com.

  Exemple : c12345678.saasprotection.com

Note

Pour pouvoir enregistrer la stratégie, vous devez indiquer l'adresse IP ou le nom d'hôte d'au moins un serveur proxy ainsi qu'un numéro de port.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans le menu **Paramètres de Client Proxy**, sélectionnez **Serveurs proxy**.
6. Cliquez sur l'onglet **Liste des serveurs proxy secondaires**.
7. Pour spécifier le mode de sélection des serveurs proxy dans la liste, sélectionnez une option :
   - **Se connecter au premier serveur proxy accessible dans l'ordre de la liste ci-dessous** : le logiciel sélectionne le serveur proxy suivant dans la liste que vous avez établie.
   -

Se connecter au serveur proxy avec le temps de réponse le plus rapide : le logiciel sélectionne le serveur proxy suivant dans sa liste, en fonction du temps de réponse.

8. Pour ajouter des serveurs proxy à la **Liste des serveurs proxy**, configurez les paramètres ci-dessous, puis cliquez sur **Ajouter**.
   - **Adresse du serveur proxy** : spécifie l'adresse IP ou le nom d'hôte du serveur proxy.
   - **Port de proxy** : spécifie le numéro de port du serveur proxy.
   - **HTTP/HTTPS** : cochez cette case pour rediriger le trafic envoyé vers les ports 80 et 443 vers un serveur proxy.
   - **Ports non HTTP/HTTPS redirigés** : spécifie les numéros de port des protocoles autres que HTTP/HTTPS dont vous souhaitez rediriger le trafic. Vérifiez que le serveur proxy prend en charge ces protocoles. Vous pouvez saisir jusqu'à 1 024 caractères dans ce champ.
9. Sélectionnez **Activer le basculement automatique de proxy pour un proxy secondaire**, puis spécifiez une valeur comprise entre 10 et 3 600 pour l'option **Intervalle d'interrogation (en secondes)**. La valeur recommandée est 60 secondes.

   L'option de sélection automatique du proxy n'est disponible que lorsque **Se connecter au premier serveur proxy accessible dans l'ordre de la liste ci-dessous** est sélectionné.
10. Cliquez sur **Enregistrer**.

Résultats

La liste des serveurs proxy secondaires est enregistrée avec la stratégie.

Configuration des paramètres client

Configurez les paramètres utilisés par Client Proxy pour déterminer l'emplacement du terminal et le moment auquel il doit rediriger le trafic web. Le logiciel client teste la connectivité à l'aide d'une connexion en trois temps, puis interrompt la connexion. Le terminal peut être situé à l'intérieur du réseau, en dehors du réseau ou être connecté au réseau par VPN.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Note

Avant de pouvoir enregistrer la stratégie, vous devez fournir des valeurs pour l'ID client et le mot de passe partagé.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.

4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans la liste **Paramètres de proxy du client**, sélectionnez **Configuration client**.
6. Sélectionnez une option en fonction de votre plate-forme de gestion :
   - McAfee ePO : dans la section **Identificateur client**, cliquez sur **Parcourir** pour le localiser, puis ouvrez le fichier ID client au format .xml fourni par l'administrateur Web Gateway ou McAfee WGCS. Les valeurs de ce fichier remplissent automatiquement les champs **ID client unique** et **Mot de passe partagé**.
   - McAfee ePO Cloud : dans la section **Configurer le mot de passe partagé**, saisissez et confirmez le mot de passe partagé entre Client Proxy et McAfee WGCS. Vous pouvez également réinitialiser ou exporter le mot de passe.
   - MVISION ePO : Avant de créer des stratégies Client Proxy sur MVISION ePO ou de migrer des stratégies vers MVISION ePO, importez votre ID client et votre mot de passe partagé sur la page **Administration MCP**. Une fois les importations réussies, toutes les nouvelles stratégies Client Proxy, ainsi que celles existantes, sont mises à jour avec l'ID client et le mot de passe partagé importés.

   Note

   La migration de stratégies Client Proxy en local vers MVISION ePO est prise en charge depuis Client Proxy en local 3.0.0 et versions ultérieures. Pour plus d'informations sur la migration de McAfee ePO en local vers MVISION ePO, consultez le *Guide de démarrage rapide de la migration vers MVISION ePO* sur le portail de documentation produit McAfee *(docs.mcafee.com)*.

7. Sélectionnez un réglage de **Canal sécurisé pour les proxys de cloud** :

   Note

   Cette option s'applique uniquement à McAfee WGCS.

   - **Activer le canal sécurisé** : Cochez cette case pour établir une connexion sécurisée entre Client Proxy et McAfee WGCS. Lorsque vous cochez cette case, le logiciel valide le certificat de proxy de cloud par rapport au magasin de certificats d'équipement et établit une connexion sécurisée.

     Note

     Lorsque vous activez le **Canal sécurisé**, Client Proxy utilise le port 8081 pour vérifier la connectivité du proxy de cloud. Toutefois, vous pouvez continuer à configurer le port 8080 et le nom d'hôte du serveur proxy lors de l'ajout d'un serveur proxy de cloud.

   - **Bloquer si la validation a échoué** : Cochez cette case pour bloquer le trafic vers le serveur proxy de cloud en cas d'échec de la validation du certificat.

     Note

     Lorsque la validation de certification échoue pour un serveur proxy, le trafic vers ce serveur proxy (principal ou autre) est bloqué.

   - Si vous avez des problèmes de connectivité avec le port 8081 (port de canal sécurisé), vous pouvez décider d'autoriser ou de bloquer la connexion. Sélectionnez l'un des éléments suivants :

- **Bloquer la connexion** : Sélectionnez cette option pour bloquer la connexion.

Note

Lorsque la validation de certification échoue pour un serveur proxy, le trafic vers ce serveur proxy (principal ou autre) est bloqué.

- **Autoriser la connexion sans canal sécurisé** : Sélectionnez cette option pour autoriser la connexion via le port de proxy configuré (8080) sans établir de connexion sécurisée entre Client Proxy et McAfee WGCS.

Note

Lorsque vous sélectionnez cette option, tous les serveurs proxy configurés (en local et cloud) sont pris en considération pour le filtrage du trafic. L'ordre de sélection d'un serveur proxy dépend de l'option que vous avez sélectionnée (**Se connecter au premier serveur proxy accessible en fonction de l'ordre dans la liste ci-dessous** ou **Se connecter au serveur proxy au temps de réponse le plus rapide**) lors de la configuration de la liste de serveurs proxy.

8. Sélectionnez un paramètre de **Redirection du trafic** :
   - **Rediriger le trafic réseau lorsque l'ordinateur n'est pas connecté au réseau d'entreprise et ne fonctionne pas via le VPN** : redirige les demandes web vers un serveur proxy lorsque les utilisateurs travaillent en dehors du réseau de votre organisation et ne sont pas connectés par VPN.
   - **Toujours rediriger le trafic réseau vers les serveurs proxy** : redirige toutes les demandes web vers un serveur proxy, y compris les demandes des utilisateurs travaillant à l'intérieur du réseau, en dehors du réseau, ou connectés au réseau par VPN.
9. Sélectionnez un paramètre de **Détection d'un réseau d'entreprise** :
   - **en testant la connectivité vers l'ePO** : si le logiciel client peut se connecter au serveur McAfee ePO, le terminal se trouve à l'intérieur du réseau.
   - **en testant la connectivité à l'un des serveurs d'entreprise suivants :** si le logiciel client peut se connecter aux serveurs réseau configurés, le terminal se trouve à l'intérieur du réseau.
10. Pour configurer la **Détection d'un VPN d'entreprise**, indiquez les adresses et les numéros de port d'un ou de plusieurs serveurs VPN. Si le logiciel client peut se connecter à un réseau VPN configuré, le terminal est connecté au réseau via un VPN.
11. A l'aide d'expressions régulières, configurez le **Filtre des groupes Active Directory** pour limiter les groupes dans l'en-tête ajoutés par le logiciel client aux demandes web avant leur redirection vers le serveur proxy. Les informations d'appartenance aux groupes ne doivent pas dépasser 4096 caractères.
    Format : <nom_domaine>\\<nom_groupe>
12. (macOS) Sélectionnez un paramètre de **Fichier journal** :
    - **Consigner les messages avec une erreur et une priorité critique**
    - **Consigner les messages avec une erreur, une priorité critique, d'information et d'avertissement**
    - **Consigner tous les messages (recommandé pour la résolution des problèmes et le débogage)**
    - **Ne pas consigner les messages**

Note

Sur les terminaux exécutant Windows, les fichiers journaux sont enregistrés dans ce dossier : C:\Program Data\McAfee \MCP\Logs. Les messages d'erreurs critiques sont enregistrés dans un fichier nommé Mcp.log.

13. (Windows) Configurez les paramètres de **Protection de l'accès** :
    - **Activer la protection de l'accès** : si cette option est sélectionnée, les utilisateurs peuvent désactiver le logiciel client à l'aide du Gestionnaire des tâches de Windows, modifier ou supprimer des fichiers, et modifier les valeurs de registre.
    - **Demande de clé de publication pour la désinstallation manuelle** : si cette option est sélectionnée, les utilisateurs peuvent demander un code de libération à un administrateur et l'utiliser pour désinstaller le logiciel client. Si cette option est désélectionnée, les utilisateurs doivent utiliser la fonctionnalité de désinstallation de Windows pour désinstaller le logiciel. La meilleure pratique consiste à utiliser un code d'autorisation pour désinstaller le logiciel.
14. Cliquez sur **Enregistrer**.

Résultats

Les paramètres client sont enregistrés avec la stratégie Client Proxy.

Configuration de la liste de contournement (McAfee ePO ou McAfee ePO Cloud)

La stratégie Client Proxy autorise le trafic web correspondant aux éléments de la liste de contournement à contourner le serveur proxy et à accéder directement à Internet.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO ou McAfee ePO Cloud en tant qu'administrateur.

Si l'instance Common Catalog que vous souhaitez associer à cette stratégie n'existe pas, vous devez la créer avant de configurer la liste de contournement.

Procédure

1. Dans le menu de McAfee ePO ou McAfee ePO Cloud, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans le menu **Paramètres de Client Proxy**, sélectionnez **Liste de contournement**.
6. Dans la liste déroulante **Common Catalog** du volet **Liste de contournement**, sélectionnez une instance Common Catalog.
7. Ajoutez des éléments de liste du catalogue à la liste de contournement :
    a. Dans la liste déroulante **Actions**, sélectionnez **Ajouter un élément à la liste de contournement**, puis sélectionnez une catégorie.

b. Dans la boîte de dialogue **Choisir parmi les valeurs existantes**, sélectionnez les éléments de la liste que vous souhaitez ajouter à la liste de contournement.
c. (Facultatif) Modifiez un élément de liste existant ou ajoutez-en un nouveau.

Caution

Les modifications que vous apportez à cette étape s'appliquent à toutes les stratégies qui partagent cette instance de Common Catalog.

d. Cliquez sur **OK**.

La boîte de dialogue se ferme et les éléments de la liste sélectionnés sont ajoutés à la liste de contournement.

8. (Facultatif) Modifiez ou supprimez des éléments de la liste de contournement.
9. Cliquez sur **Enregistrer**.

Résultats

La liste de contournement et l'instance Common Catalog sont enregistrées avec la stratégie.

Configuration de la liste de redirection secondaire (McAfee ePO ou McAfee ePO Cloud)

Vous pouvez configurer les noms de domaine, adresses réseau, ports réseau et noms de processus figurant dans la liste de redirection secondaire pour rediriger le trafic web vers le serveur proxy de redirection secondaire. Vous pouvez afficher les listes d'éléments ajoutés à la liste de redirection secondaire et ajouter, modifier ou supprimer des éléments des listes selon vos besoins.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO ou McAfee ePO Cloud en tant qu'administrateur.

Si l'instance Common Catalog à associer à cette stratégie n'existe pas, vous devez la créer avant de configurer la liste de redirection secondaire.

Procédure

1. Dans le menu de McAfee ePO ou McAfee ePO Cloud, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans le menu **Paramètres de Client Proxy**, sélectionnez **Liste de redirection secondaire**.
6. Dans la liste déroulante **Common Catalog** du volet **Liste de redirection secondaire**, sélectionnez une instance Common Catalog.
7. Ajoutez des éléments de liste du catalogue à la liste de redirection secondaire :

a. Dans la liste déroulante **Actions**, sélectionnez **Ajouter une redirection secondaire**, puis une catégorie.
b. Dans la boîte de dialogue **Choisir parmi les valeurs existantes**, sélectionnez les éléments de la liste à ajouter à la liste de redirection secondaire.
c. (Facultatif) Modifiez un élément de liste existant ou ajoutez-en un nouveau.

Caution

Les modifications que vous apportez à cette étape s'appliquent à toutes les stratégies qui partagent cette instance de Common Catalog.

d. Cliquez sur **OK**.

La boîte de dialogue se ferme et les éléments de la liste sélectionnés sont ajoutés à la liste de redirection secondaire.

8. (Facultatif) Vous pouvez modifier ou supprimer des éléments dans la liste de redirection secondaire.
9. Cliquez sur **Enregistrer**.
   La liste de redirection secondaire et l'instance Common Catalog sont enregistrées avec la stratégie.
10. (Facultatif) Cliquez sur **Dupliquer** pour dupliquer la stratégie Client Proxy sélectionnée.

Configuration de la liste de contournement (MVISION ePO)

Vous pouvez configurer les noms de domaine, les adresses réseau, les ports réseau et les noms de processus dans la liste de contournement. Vous pouvez afficher les listes d'éléments ajoutés à la liste de contournement et ajouter, modifier ou supprimer des éléments des listes selon vos besoins.

Avant de commencer

Vous devez être connecté au serveur MVISION ePO en tant qu'administrateur.

Procédure

1. Dans le menu MVISION ePO, sélectionnez **Stratégie** → **Catalogue de stratégies** → **McAfee Client Proxy**.
2. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
3. Cliquez sur **Modifier** en regard de la stratégie à configurer.
4. Sous **Paramètres de Client Proxy**, cliquez sur **Liste de contournement**.
5. Dans le volet **Liste de contournement**, sélectionnez une catégorie :
   - **Nom de domaine** : Saisissez le nom de domaine et cliquez sur **Ajouter**. Le trafic web envoyé aux domaines de cette liste contourne le serveur proxy. Exemple : google.com
   - **Adresse réseau (IP)** : Entrez l'adresse IP du réseau, puis cliquez sur **Ajouter**. Le trafic web envoyé aux adresses IP de cette liste contourne le serveur proxy. Les adresses peuvent être configurées individuellement, sous forme de plage, à l'aide d'un sous-réseau ou de CIDR.
     Exemples :
     - 192.168.1.1
     - 172.31.255.10–172.31.255.20

- 10.50.0.0/255.255.128.0
- 10.50.0.0/17

- **Port réseau** : Saisissez le numéro de port, sa description, puis cliquez sur **Ajouter**. Le trafic web envoyé aux ports de cette liste contourne le serveur proxy. Exemples : 40, 80, 400 – 500
- **Liste des processus** : Saisissez le nom du processus, puis cliquez sur **Ajouter**. Le trafic web provenant des processus de cette liste contourne le serveur proxy. Un processus s'exécute sur les terminaux. Les noms des processus Windows doivent se terminer par l'extension .exe. Les noms des processus macOS ne nécessitent pas d'extension de nom de fichier. Ajoutez McAfee et d'autres processus approuvés à cette liste.

6. Cliquez sur **Enregistrer**.
7. Le cas échéant, cliquez sur **Dupliquer** pour dupliquer une stratégie.

Configuration de la liste de redirection secondaire (MVISION ePO)

Vous pouvez configurer les noms de domaine, adresses réseau, ports réseau et noms de processus figurant dans la liste de redirection secondaire pour rediriger le trafic web vers le serveur proxy de redirection secondaire. Vous pouvez afficher les listes d'éléments ajoutés à la liste de redirection secondaire et ajouter, modifier ou supprimer des éléments des listes selon vos besoins.

Avant de commencer

Vous devez être connecté au serveur MVISION ePO en tant qu'administrateur.

Procédure

1. Dans le menu MVISION ePO, sélectionnez **Stratégie** → **Catalogue de stratégies** → **McAfee Client Proxy**.
2. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
3. Cliquez sur **Modifier** en regard de la stratégie à configurer.
4. Sous **Paramètres de proxy du client**, cliquez sur **Liste de redirection secondaire**.
5. Dans le volet **Liste de redirection secondaire**, sélectionnez une catégorie :

   - **Nom de domaine** : saisissez le nom de domaine et cliquez sur **Ajouter**. Le trafic web envoyé aux domaines est redirigé vers le serveur proxy secondaire. Exemple : google.com
   - **Adresse réseau (IP)** : saisissez l'adresse IP du réseau, puis cliquez sur **Ajouter**. Le trafic web envoyé aux adresses IP est redirigé vers le serveur proxy secondaire. Les adresses peuvent être configurées individuellement, sous forme de plage, à l'aide d'un sous-réseau ou de CIDR.
     Exemples :

     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17

- **Port réseau** : saisissez le numéro de port et sa description, puis cliquez sur **Ajouter**. Le trafic web envoyé aux ports est redirigé vers le serveur proxy secondaire. Exemples : 40, 80, 400–500
- **Liste des processus** : saisissez le nom du processus, puis cliquez sur **Ajouter**. Le trafic web provenant des processus est redirigé vers le serveur proxy secondaire. Un processus s'exécute sur les terminaux. Les noms des processus Windows doivent se terminer par l'extension .exe. Les noms des processus macOS ne nécessitent pas d'extension de nom de fichier. Ajoutez les processus McAfee et autres processus approuvés à cette liste.

6. Cliquez sur **Enregistrer**.
7. Le cas échéant, cliquez sur **Dupliquer** pour dupliquer une stratégie.

Importation ou exportation de la liste de contournement (MVISION ePO)

Vous pouvez utiliser les options d'importation et d'exportation pour copier les listes de contournement. Une fois que vous avez importé ou exporté la liste de contournement, vous pouvez ajouter, modifier et supprimer les éléments qu'elle contient. Il est conseillé d'exporter la liste de contournement existante, de la modifier et d'importer à nouveau le fichier. L'importation d'une liste de contournement remplace toutes les entrées de contournement existantes. Seul le format de fichier .txt est pris en charge pour les options d'importation ou d'exportation.

Voici un exemple de liste d'éléments de la liste de contournement :

```
type = DOMAIN google.com
type intel.com = NETWORKADDRESS 192.168.1.1
172.31.255.10 - 172.31.255.20
10.50.0.0/255.255.128.0
10.50.0.0/17 type = Description du numéro de port NETWORKPORT
Port 80,443 Http/Https 21-47 avec plage
22
31,78,100-500 type = PROCESSNAME chrome.exe
firefox. exe
Xcode
```

Note

Vous pouvez ajouter des numéros de port sans aucune description, et le nom du processus est le nom du processus Windows ou macOS.

Procédure

1. Dans le menu MVISION ePO, sélectionnez **Stratégie** → **Catalogue de stratégies** → **McAfee Client Proxy**.
2. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
3. Cliquez **Modifier** sur la même ligne que la stratégie pour laquelle vous souhaitez importer ou exporter la liste de contournement.
4. Sous **Paramètres de Client Proxy**, cliquez sur **Liste de contournement**.
5. Dans le volet **Liste de contournement**, procédez comme suit :

- Pour exporter une liste de contournement, cliquez sur **Exporter la liste de contournement**. Le navigateur télécharge la liste de contournement sous la forme d'un fichier .txt.
- Pour importer une liste de contournement, cliquez sur **Importer la liste de contournement**.
  - Dans la boîte de dialogue, cliquez sur **Choisir un fichier** pour accéder au dossier contenant le fichier de liste de contournement. Sélectionnez le fichier, puis cliquez sur **Ouvrir**. Un message de confirmation s'affiche après l'importation de la liste de contournement.

    Note

    Vérifiez que la liste d'éléments de la liste de contournement est au bon format. En cas d'échec de l'importation, la boîte de dialogue **Importer la liste de contournement** revient au numéro de ligne auquel l'erreur s'est produite. Une fois les erreurs corrigées, vous pouvez à nouveau importer le fichier.

6. Cliquez sur **Enregistrer**.

Importation ou exportation de la liste de redirection secondaire (MVISION ePO)

Vous pouvez utiliser les options d'importation et d'exportation pour copier les listes de redirection secondaire. Une fois l'importation ou l'exportation de la liste de redirection secondaire terminée, vous pouvez ajouter, modifier et supprimer les noms de domaine qu'elle contient. Il est conseillé d'exporter la liste de redirection secondaire existante, de la modifier, puis de l'importer à nouveau. L'importation d'une liste de redirection secondaire remplace toutes les entrées de redirection secondaire existantes. Seul le format de fichier .txt est pris en charge pour les options d'importation ou d'exportation.

Voici un exemple de liste de redirection secondaire :

```
type = DOMAIN google.com
intel.com
```

Procédure

1. Dans le menu MVISION ePO, sélectionnez **Stratégie** → **Catalogue de stratégies** → **McAfee Client Proxy**.
2. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
3. Cliquez sur **Modifier** en regard de la stratégie pour laquelle la liste de redirection secondaire doit être importée ou exportée.
4. Sous **Paramètres de Client Proxy**, cliquez sur **Liste de redirection secondaire**.
5. Dans le volet **Liste de redirection secondaire**, procédez comme suit :
   - Pour exporter la liste de redirection secondaire, cliquez sur **Exporter la liste de redirection secondaire**. Le navigateur télécharge la liste de redirection secondaire sous forme de fichier .txt.
   - Pour importer la liste de redirection secondaire, cliquez sur **Importer la liste de redirection secondaire**.

- Dans la boîte de dialogue, cliquez sur **Choisir un fichier** pour accéder au dossier contenant le fichier de liste de redirection secondaire. Sélectionnez le fichier, puis cliquez sur **Ouvrir**. Un message de confirmation s'affiche après l'importation de la liste de redirection secondaire.

Note

Vérifiez que le format de la liste des noms de domaine figurant dans la liste de redirection secondaire est corect. En cas d'échec de l'importation, la boîte de dialogue **Importer la liste de redirection secondaire** revient au numéro de la ligne dans laquelle l'erreur s'est produite. Une fois les erreurs corrigées, vous pouvez à nouveau importer le fichier.

6. Cliquez sur **Enregistrer**.

Configurer la liste de blocage

Chaque stratégie Client Proxy est associée à une liste de processus bloqués.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Une liste de processus est une liste des processus qui s'exécutent sur les terminaux. Les noms des processus Windows doivent se terminer par l'extension .exe. Les noms des processus macOS ne nécessitent pas d'extension de nom de fichier.

Pour réduire la quantité de trafic redirigé vers le serveur proxy pour être filtré, configurez la liste des processus de terminal dont l'accès au réseau est bloqué.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans le menu **Paramètres de Client Proxy**, sélectionnez **Liste de blocage**.
6. Sélectionnez une option :
   - **Autoriser le trafic à accéder directement à la destination** : tous les processus sont autorisés à accéder à Internet sans passer par un serveur proxy.
   - **Bloquer le trafic pour tous les processus (à l'exception des processus de contournement listés)** : l'accès à Internet est bloqué pour tous les processus, à l'exception des processus sur la liste de contournement.
   - **Bloquer le trafic uniquement pour les processus suivants** : tous les processus sont autorisés à accéder à Internet sans passer par un serveur proxy, à l'exception de ceux présents sur cette liste. Configurez la liste à l'aide des fonctions **Ajouter**, **Modifier** et **Supprimer**.
7. Cliquez sur **Enregistrer**.

Résultats

La liste de blocage est enregistrée avec la stratégie Client Proxy.

Affectation d'une stratégie aux terminaux

Vous pouvez affecter une stratégie Client Proxy à vos terminaux à l'aide de McAfee ePO, McAfee ePO Cloud ou MVISION ePO.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Sélectionnez le niveau organisationnel auquel vous souhaitez affecter la stratégie.

   Pour sélectionner tous les terminaux gérés par votre plate-forme, sélectionnez **Mon organisation**.

3. Cliquez sur **Stratégies affectées**.
4. Dans la liste déroulante **Produit**, sélectionnez la version actuelle de McAfee Client Proxy.
5. Dans la colonne **Actions**, cliquez sur **Modifier l'affectation** en regard de la stratégie que vous souhaitez affecter.
6. Dans **Hériter de**, sélectionnez **Bloquer l'héritage et affecter la stratégie et les paramètres ci-dessous**.
7. Dans la liste déroulante **Stratégie affectée**, sélectionnez la stratégie.
8. Sélectionnez une option pour **Verrouiller l'héritage de stratégie** :
   - **Déverrouillé** : une autre stratégie peut être affectée à un ou plusieurs sous-groupes.
   - **Verrouillé** : cette stratégie doit être affectée à tous les sous-groupes.
9. Cliquez sur **Enregistrer**.

Résultats

La stratégie est affectée à vos terminaux.

Exporter une stratégie vers un fichier .xml ou .opg

Exportez une stratégie Client Proxy à partir de McAfee ePO, McAfee ePO Cloud ou MVISION ePO vers un fichier .xml ou .opg.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO, McAfee ePO Cloud ou MVISION ePO en tant qu'administrateur.

Pour les ordinateurs autonomes qui ne sont pas gérés avec McAfee ePO ou McAfee ePO Cloud, vous devez exporter la stratégie vers un fichier .opg et enregistrer le fichier localement sur vos ordinateurs.

Procédure

1. Dans le menu principal, sélectionnez **Stratégie** → **Catalogue de stratégies**.
2. Dans la liste **Produits**, sélectionnez la version actuelle de Client Proxy.
3. Cliquez sur **Stratégie MCP** pour afficher la liste des stratégies.
4. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez configurer.
5. Dans la liste déroulante **Actions**, sélectionnez **Exporter la stratégie vers un fichier**.
6. Cliquez avec le bouton droit sur le fichier de stratégie que vous souhaitez télécharger, puis cliquez sur **Enregistrer** → **OK**.
   - **Fichier serveur de stratégie McAfee Client Proxy** : exporte la stratégie Client Proxy vers un fichier .xml que vous pouvez utiliser pour la résolution des problèmes.
   - **Fichier du client de stratégies McAfee Client Proxy** : exporte la stratégie Client Proxy vers un fichier .opg que vous pouvez enregistrer sur vos ordinateurs autonomes ou terminaux.
7. Renommez le fichier .opg en StratégieMCP.opg, puis copiez-le à cet emplacement sur les ordinateurs clients :
   - Ordinateurs Windows : C:\ProgramData\McAfee\MCP\Policy\Temp
   - Ordinateurs macOS : /usr/local/mcafee/mcp/policy

Résultats

Lorsque Client Proxy est exécuté sur les ordinateurs autonomes ou terminaux, il charge la stratégie et commence à rediriger le trafic.

Suspendre la mise en œuvre de stratégie sur un ordinateur exécutant Windows ou macOS

Si un utilisateur doit accéder ou transférer des informations confidentielles pour une raison commerciale approuvée, vous pouvez suspendre la mise en œuvre de stratégie sur un ordinateur autonome ou terminal exécutant Windows ou macOS.

Pour suspendre la mise en œuvre de stratégie, suivez le protocole authentification-réponse fourni par le logiciel Help Desk.

Procédure

1. **Utilisateur** : ouvre la boîte de dialogue **Saisir le code d'autorisation** :
   - Windows : dans le menu **Démarrer**, cliquez sur **McAfee** → **Contourner McAfee Client Proxy**.
   - macOS : depuis l'icône McAfee dans la barre d'état, sélectionnez **Console**, puis **Client Proxy**.

Caution

L'utilisateur doit laisser la boîte de dialogue ouverte en attendant de recevoir le code d'autorisation. En cas de fermeture, la procédure doit être recommencée.

2. **Utilisateur** : vous envoie un e-mail qui inclut :
   - Le nom et l'adresse e-mail de l'utilisateur
   - Le numéro de **Nom de stratégie et Révision de stratégie** (copié à partir de la boîte de dialogue **Saisir le code d'autorisation**)
   - Le code d'**identification** (copié à partir de la boîte de dialogue **Saisir le code d'autorisation**)
3. **Administrateur** : à l'aide du logiciel Help Desk et des valeurs fournies par l'utilisateur, il génère le code de publication et l'envoie à l'utilisateur. Dans MVISION ePO, vous pouvez générer un code d'autorisation sur la page **Administration MCP**.
4. **Utilisateur** : saisit le code d'autorisation dans le champ **Autorisation**, puis clique sur **OK** (Windows) ou **Autorisation** (macOS).

Résultats

La mise en œuvre de stratégie est suspendue pour la période que vous avez spécifiée lors de la génération du code d'autorisation.

Requêtes et rapports

Création et exécution d'une requête de base de données (McAfee ePO)

Créez et exécutez une requête de base de données pour renvoyer des informations sur les stratégies et les tâches client.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO en tant qu'administrateur.

Note

Un administrateur McAfee ePO Cloud peut exécuter des requêtes, mais pas les créer.

Procédure

1. Dans le menu de McAfee ePO, sélectionnez **Rapports** → **Requêtes et rapports**.
2. Dans le menu **Groupes**, sélectionnez **Groupes McAfee** → **McAfee Client Proxy**, puis cliquez sur **Nouvelle requête**.
3. Dans le **Générateur de requêtes** : dans la liste **Groupe de fonctionnalités**, sélectionnez **Gestion des stratégies**.
4. Sélectionnez un **Type de résultat**, puis cliquez sur **Suivant** :
   - **Tâches client appliquées** : renvoie les noms des tâches client et les niveaux organisationnels sur lesquels elles ont été appliquées.
   - **Stratégies appliquées** : renvoie les noms des stratégies et les niveaux organisationnels sur lesquels elles ont été appliquées.
   - **Héritage bloqué de l'affectation de tâche client** : renvoie les noms des tâches client et les niveaux organisationnels où les affectations de tâche ont été bloquées.
   - **Héritage bloqué d'affectation de stratégie** : renvoie les noms des stratégies et les niveaux organisationnels où l'affectation de stratégie a été bloquée.

   La page **Graphique** s'ouvre.
5. Configurez la façon dont vous souhaitez afficher les résultats de la requête au format graphique :
   a. Sélectionnez un type de graphique.
   b. Spécifiez les étiquettes, les unités, les ordres de tri et les autres valeurs selon les besoins.
   c. Cliquez sur **Suivant**.

   La page **Colonnes** s'ouvre.
6. Configurez la façon dont vous souhaitez afficher les résultats de la requête sous forme de tableau, puis cliquez sur **Suivant** :
   - Dans le menu **Colonnes disponibles**, cliquez sur les noms des colonnes pour les sélectionner.
   - Dans le volet **Colonnes sélectionnées**, fermez les colonnes pour les supprimer.
   - Pour réorganiser les colonnes sélectionnées, faites-les glisser, puis déposez-les ou utilisez les touches fléchées.

La page **Filtre** s'ouvre.

7. Configurez la façon dont vous souhaitez filtrer les résultats de la requête :
   a. Dans le menu **Propriétés disponibles**, cliquez sur les noms des propriétés pour les sélectionner.
   b. Dans la liste déroulante **Comparaison**, sélectionnez un opérateur pour chaque propriété.
   c. Pour chaque opérateur, sélectionnez une valeur.
8. Cliquez sur **Exécuter** pour afficher les résultats de la requête, puis cliquez sur **Modifier la requête** pour apporter des modifications selon les besoins.
9. Cliquez sur **Enregistrer**, puis sur la page **Enregistrer la requête** :
   a. Spécifiez un nom et une description facultative pour la requête.
   b. Sélectionnez un groupe existant ou spécifiez un nouveau groupe.
   c. Cliquez sur **Enregistrer**.

Résultats

La requête de base de données est enregistrée pour une utilisation ultérieure.

Création d'un rapport Client Proxy (McAfee ePO ou MVISION ePO)

Document au format .pdf répertoriant le nombre de terminaux pour lesquels l'installation de Client Proxy a réussi ou échoué au cours du dernier mois.

Avant de commencer

Vous devez être connecté au serveur McAfee ePO ou MVISION ePO en tant qu'administrateur.

Procédure

1. Dans le menu de McAfee ePO ou MVISION ePO, sélectionnez **Rapports** → **Requêtes et rapports**.
2. Dans la liste **Groupes**, sélectionnez **Groupes McAfee** → **McAfee Client Proxy**.
3. Cliquez sur l'onglet **Rapports**, puis sur **Nouveau rapport**.
4. Depuis la **Boîte à outils**, faites glisser un ou plusieurs modèles vers la zone **Disposition du rapport**, puis configurez-les et positionnez-les :
   - **Image**
   - **Saut de page**
   - **Graphique de requête**
   - **Tableau de requête**
   - **Texte**

Note

Lors de l'ajout d'un graphique ou d'un tableau de requêtes, sélectionnez **MCP : événements de réussite/échec des installations sur les terminaux au cours du dernier mois** dans la liste déroulante **Requête**.

5. Pour personnaliser le rapport, cliquez sur les options suivantes :
   - **En-tête et pied de page**
   - **Configuration de la page**
   - **Paramètres d'exécution**
6. Cliquez sur **Exécuter** pour afficher le rapport au format .pdf.
7. Cliquez sur **Enregistrer**, puis dans la boîte de dialogue **Nom, description et groupe** :
   a. Spécifiez un nom et une description facultative pour le rapport.
   b. Sélectionnez un groupe existant ou spécifiez un nouveau groupe.
   c. Cliquez sur **OK**.

Résultats

Le rapport Client Proxy est enregistré et peut être exécuté à nouveau.

COPYRIGHT

Trellix