Intégrer Umbrella à FireEye

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Aperçu

Fonctionnalité d'intégration

Configuration de votre tableau de bord Cisco Umbrella pour recevoir des informations de FireEye

Configuration de FireEye pour communiquer avec Cisco Umbrella

Garantir la connectivité : « Tester le feu » entre FireEye et Cisco Umbrella

Observation des événements ajoutés au paramètre de sécurité FireEye en mode audit

- Vérifier la liste de destinations
- Vérifier les paramètres de sécurité d'une stratégie

Application des paramètres de sécurité FireEye en « mode blocage » à une stratégie pour les clients gérés

Rapports dans Cisco Umbrella pour les événements FireEye

- Rapports sur les événements de sécurité FireEye
- Signalement du moment où les domaines ont été ajoutés à la liste de destinations FireEye

Gestion des détections indésirables ou des faux positifs

- Listes d'autorisation
- Suppression de domaines de la liste de destinations FireEye

Introduction

Ce document décrit comment intégrer Cisco Umbrella avec FireEye.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Une appliance FireEye avec accès à Internet public.
- Droits d'administration de Cisco Umbrella Dashboard.
- L'intégration FireEye doit être activée sur le tableau de bord Cisco Umbrella.

Composants utilisés

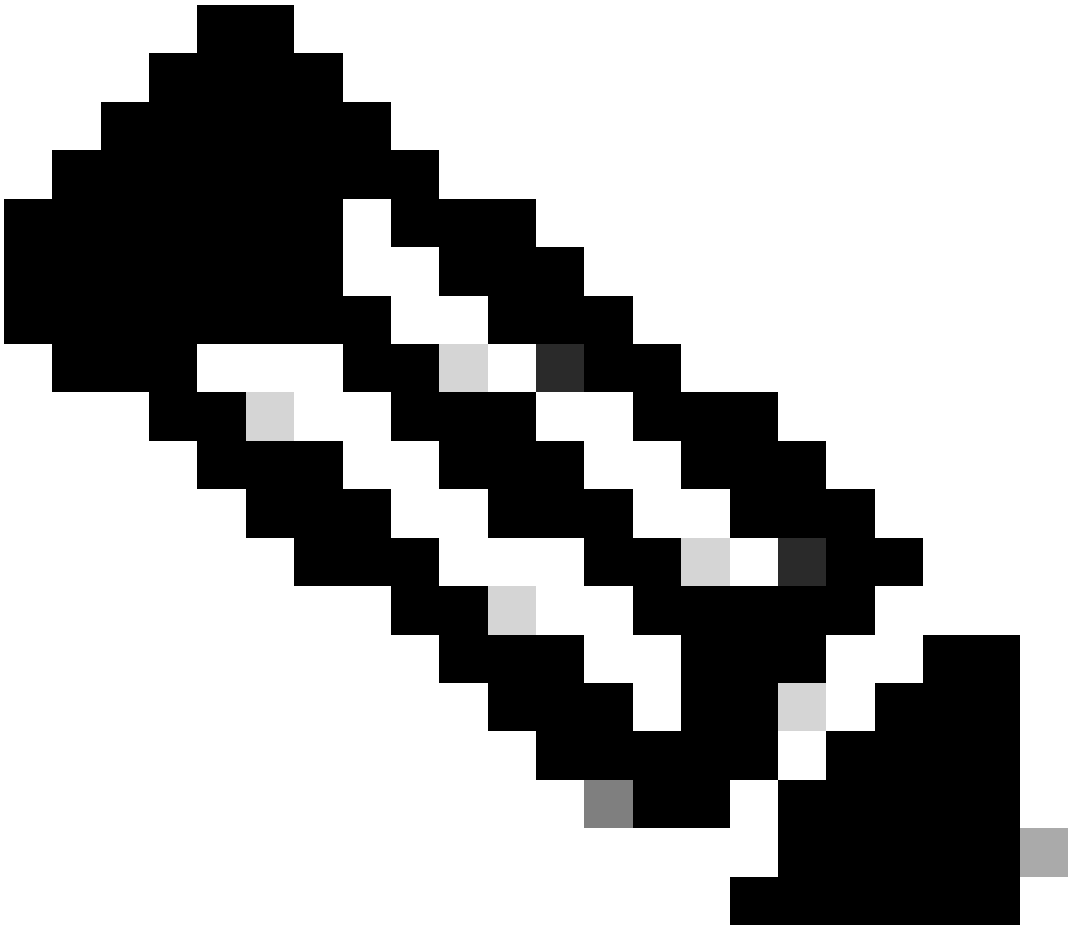
Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Grâce à l'intégration entre l'appliance de sécurité FireEye et Cisco Umbrella, les responsables de la sécurité et les administrateurs peuvent désormais étendre la protection contre les menaces avancées sur les ordinateurs portables, les tablettes ou les téléphones itinérants, tout en fournissant une autre couche d'application à un réseau d'entreprise distribué.

Ce guide explique comment configurer votre FireEye pour qu'il communique avec Cisco Umbrella afin que les événements de sécurité de FireEye soient intégrés dans des politiques qui peuvent être appliquées aux clients protégés par Cisco Umbrella.



Remarque : L'intégration FireEye est uniquement incluse dans les packages Cisco Umbrella tels que DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Si

---

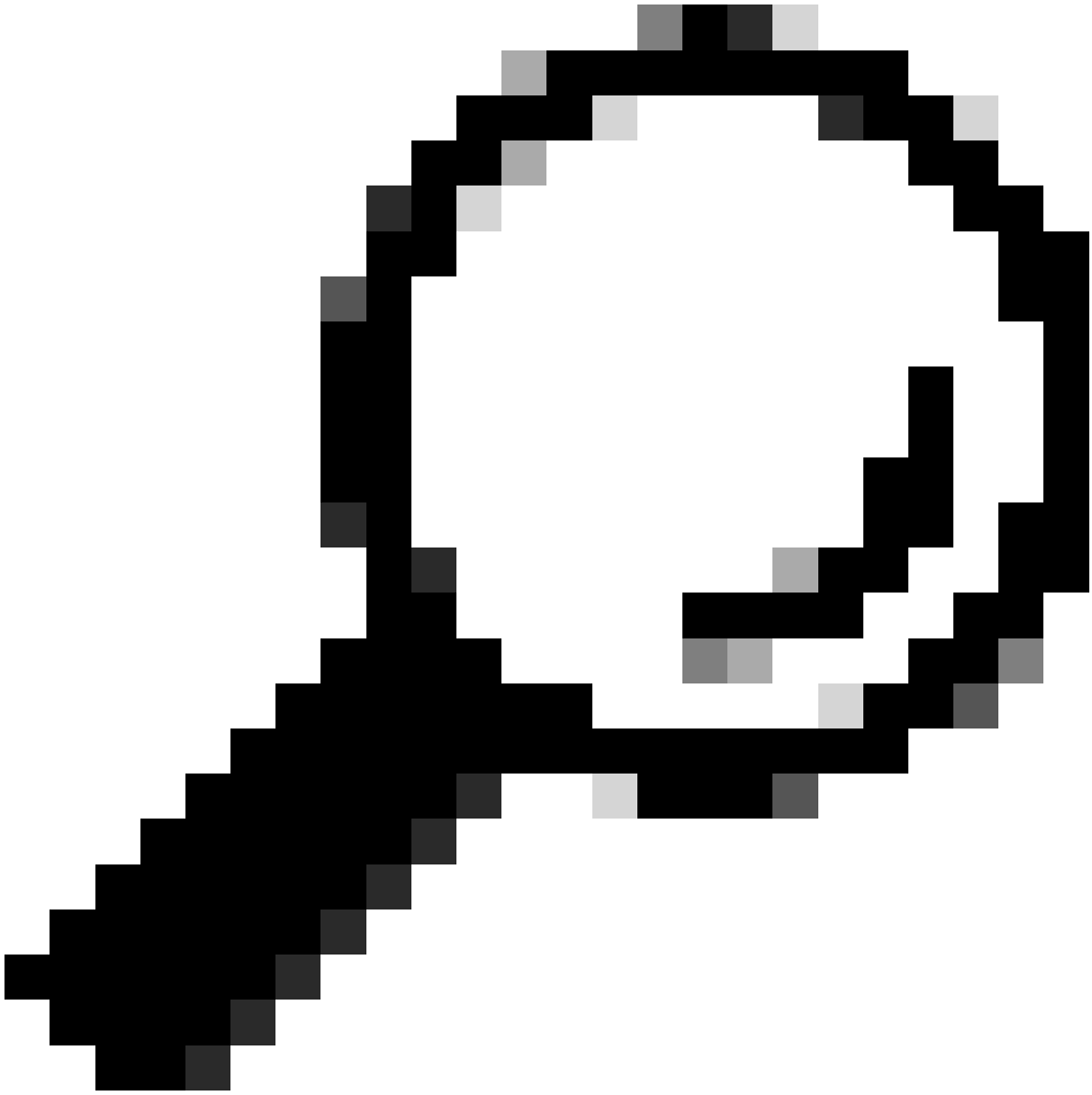
vous ne disposez pas de l'un de ces packages et souhaitez bénéficier de l'intégration FireEye, contactez votre responsable de compte Cisco Umbrella. Si vous disposez du package Cisco Umbrella approprié mais que vous ne voyez pas FireEye comme une intégration pour votre tableau de bord, contactez l'assistance Cisco Umbrella.

Fonctionnalité d'intégration

L'appliance FireEye envoie d'abord à Cisco Umbrella les menaces Internet qu'elle a détectées, telles que les domaines hébergeant des programmes malveillants, la commande et le contrôle de botnets ou de sites d'hameçonnage.

Cisco Umbrella valide ensuite les informations transmises à Cisco Umbrella pour s'assurer qu'elles sont valides et qu'elles peuvent être ajoutées à une politique. Si le formatage des informations de FireEye est confirmé (par exemple, s'il ne s'agit pas d'un fichier, d'une URL complexe ou d'un domaine très populaire), l'adresse de domaine est ajoutée à la liste de destinations FireEye dans le cadre d'un paramètre de sécurité pouvant être appliqué à n'importe quelle stratégie Cisco Umbrella. Cette stratégie est immédiatement appliquée à toutes les requêtes effectuées à partir de périphériques utilisant des stratégies avec la liste de destinations FireEye.

Par la suite, Cisco Umbrella analyse automatiquement les alertes FireEye et ajoute les sites malveillants à la liste de destinations FireEye. La protection FireEye s'étend ainsi à tous les utilisateurs et périphériques distants et fournit une couche supplémentaire d'application à votre réseau d'entreprise.



Conseil : Alors que Cisco Umbrella fait de son mieux pour valider et autoriser les domaines généralement sûrs (par exemple, Google et Salesforce), pour éviter les interruptions indésirables, nous vous suggérons d'ajouter des domaines que vous ne souhaitez jamais voir bloqués à la liste verte globale ou à d'autres listes de destinations conformément à votre politique. Exemples :

- La page d'accueil de votre entreprise
- Domaines représentant des services que vous fournissez et pouvant avoir des enregistrements internes et externes. Par exemple, « mail.myservicedomain.com » et « portal.myotherservicedomain.com ».
- Les applications cloud moins connues dont vous dépendez et dont Cisco Umbrella ne tient pas compte dans la validation automatique des domaines. Par exemple, « localcloudservice.com ».

Ces domaines peuvent être ajoutés à la liste verte globale, qui se trouve sous Politiques >

Listes de destinations dans Cisco Umbrella.

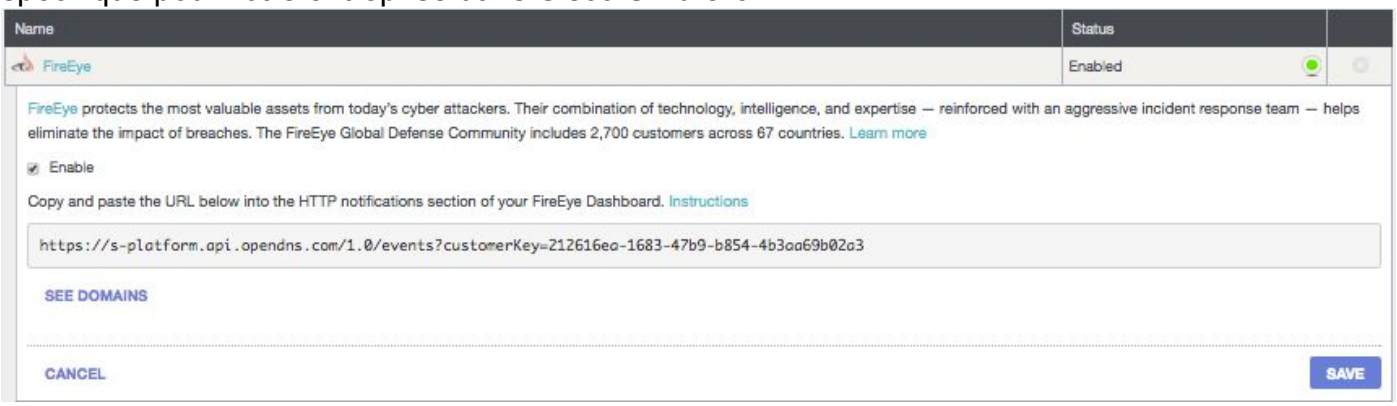
Configuration de votre tableau de bord Cisco Umbrella pour recevoir des informations de FireEye

La première étape consiste à rechercher votre URL unique dans Cisco Umbrella pour que l'appliance FireEye puisse communiquer avec vous.

1. Connectez-vous au tableau de bord Cisco Umbrella en tant qu'administrateur.

2. Accédez à Policies > Policy Components > Integrations et sélectionnez FireEye dans le tableau pour le développer.

3. Sélectionnez la zone Activer, puis sélectionnez Enregistrer. Cela génère une URL unique et spécifique pour votre entreprise dans Cisco Umbrella.

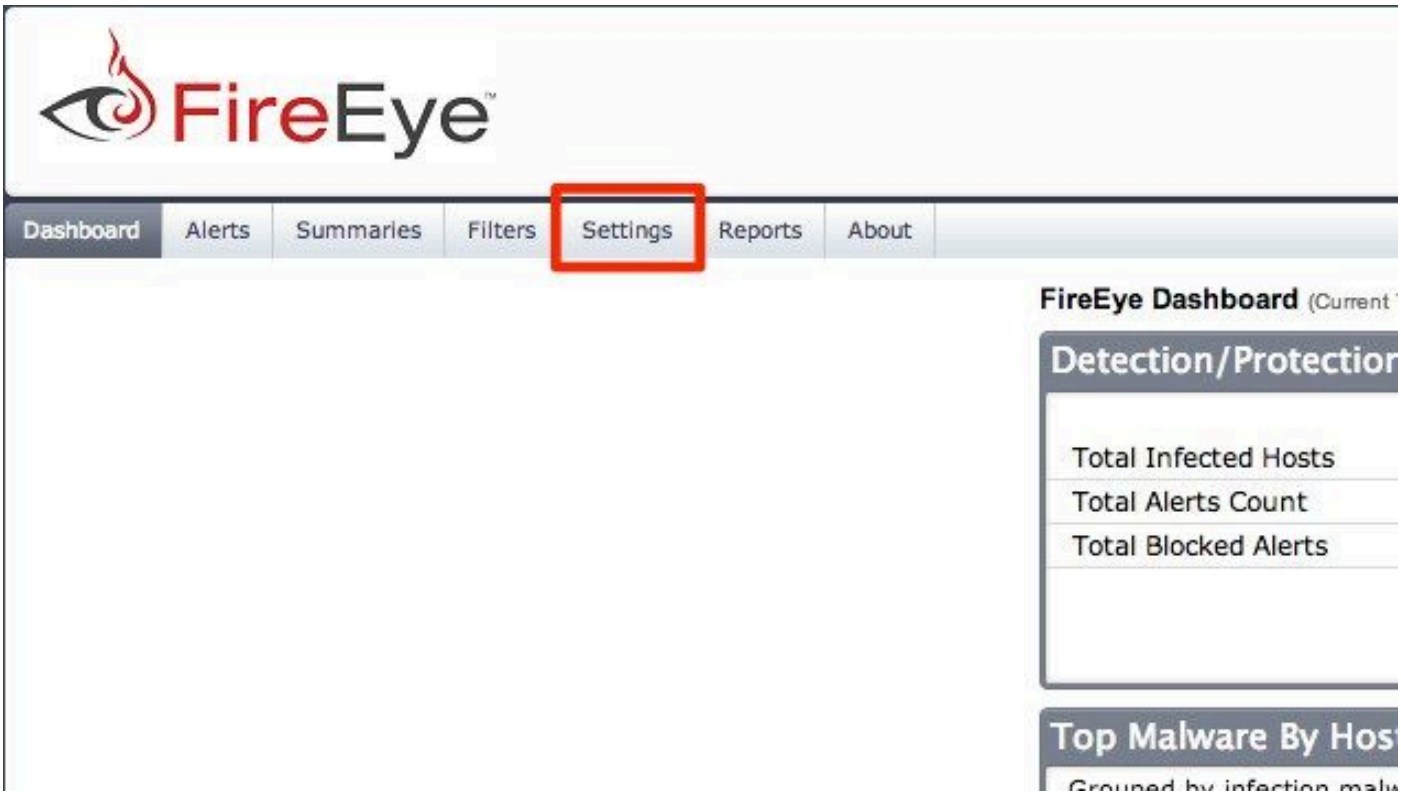


Vous pouvez utiliser cette URL ultérieurement pour configurer l'appliance FireEye afin qu'elle envoie des données à Cisco Umbrella. Veillez donc à copier l'URL.

Configuration de FireEye pour communiquer avec Cisco Umbrella

Pour commencer à envoyer du trafic de votre appliance FireEye vers Cisco Umbrella, vous devez configurer FireEye avec les informations d'URL générées dans la section précédente.

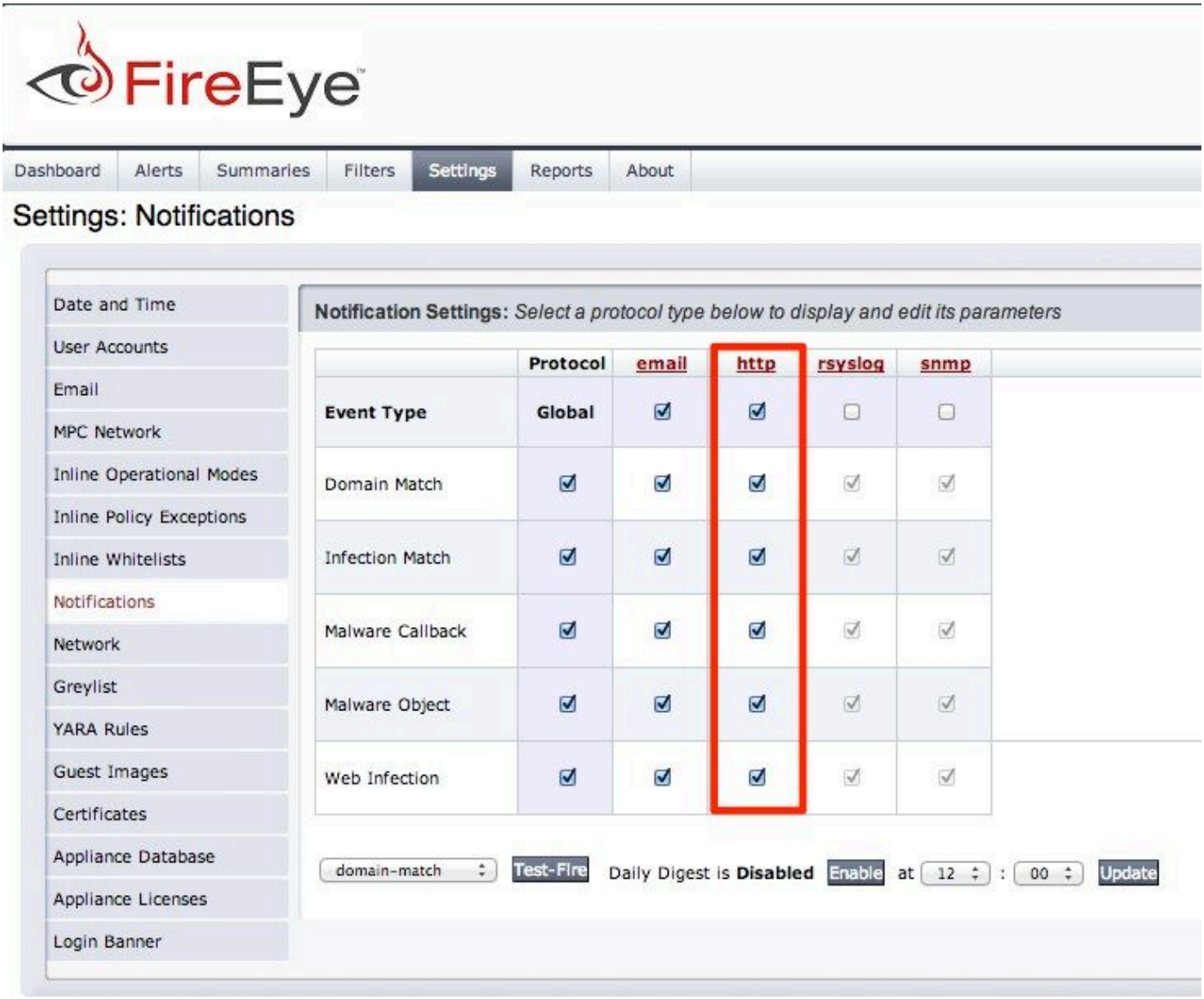
1. Connectez-vous à FireEye et sélectionnez Paramètres.



2. Sélectionnez Notifications dans la liste des paramètres :

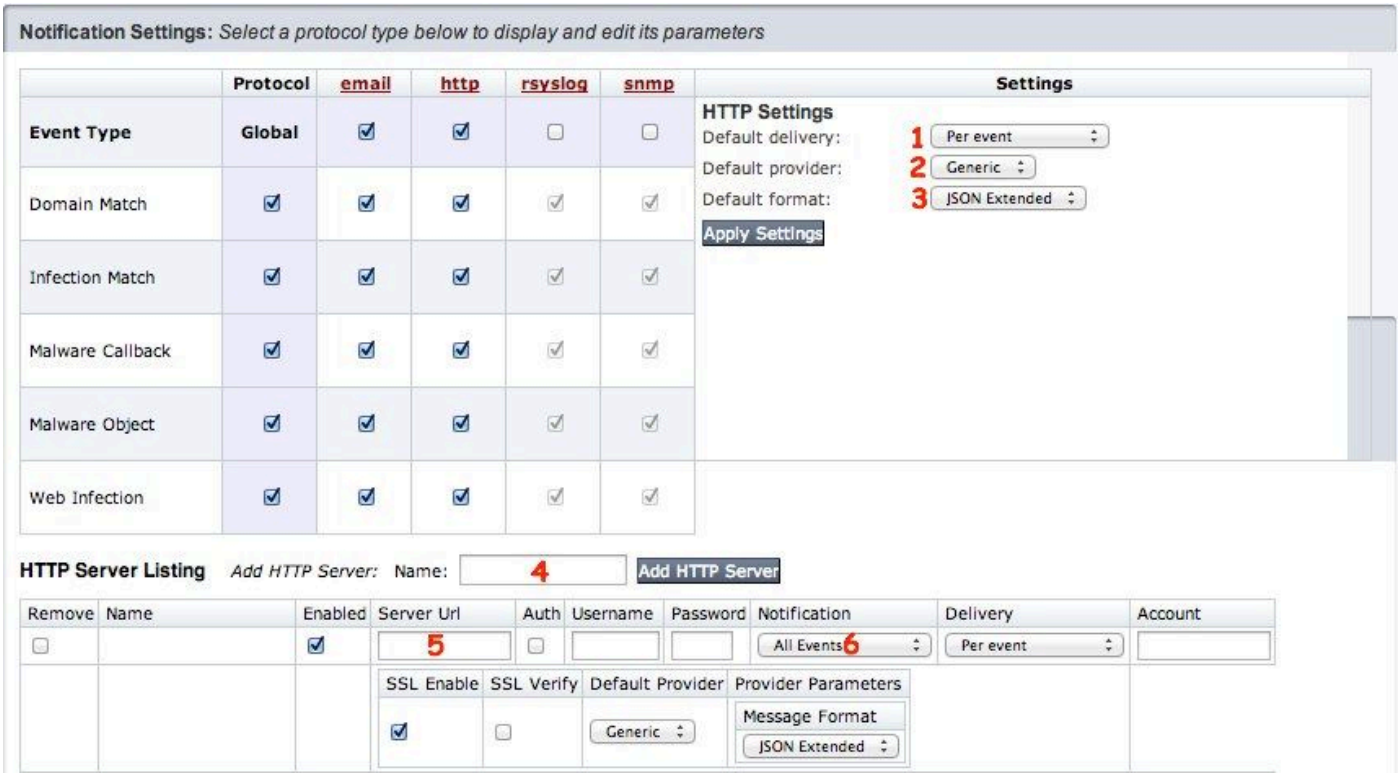
FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance Licenses
Login Banner
Date and Time Settings
Manually set the date, time, and time zone. Or, op
synchronization.
(Current Time: 11/11/13 17:29:24 UTC)
Set Manually:
November
11
2013
17
Enable NTP:
Add NTP Server:
NTP Server
Delete
Update T
pool.ntp.org
Update T
time.nist.gov
Update T
Remove Selected NTP Servers
Set Time Zone:
UTC
Set Time Zone

3. Assurez-vous que tous les types d'événements à envoyer à Cisco Umbrella sont sélectionnés (Umbrella recommande de commencer par all), puis sélectionnez le lien HTTP en haut de la colonne.



4. Lorsque le menu se développe, sélectionnez ces options pour activer la notification d'événement. Les étapes numérotées sont décrites dans la capture d'écran :

1. Livraison par défaut : Par événement
2. Fournisseur par défaut : Générique
3. Format par défaut : JSON étendu
4. Nommez le serveur HTTP « OpenDNS ».
5. Url Du Serveur : Collez ici l'URL Cisco Umbrella que vous avez générée à partir de votre tableau de bord Cisco Umbrella.
6. Liste déroulante Notification : Sélectionnez Tous les événements pour assurer une couverture maximale.



5. Assurez-vous que les listes déroulantes Delivery, Default Provider et Provider Parameters correspondent toutes aux paramètres par défaut, ou si plusieurs serveurs de notification sont utilisés :

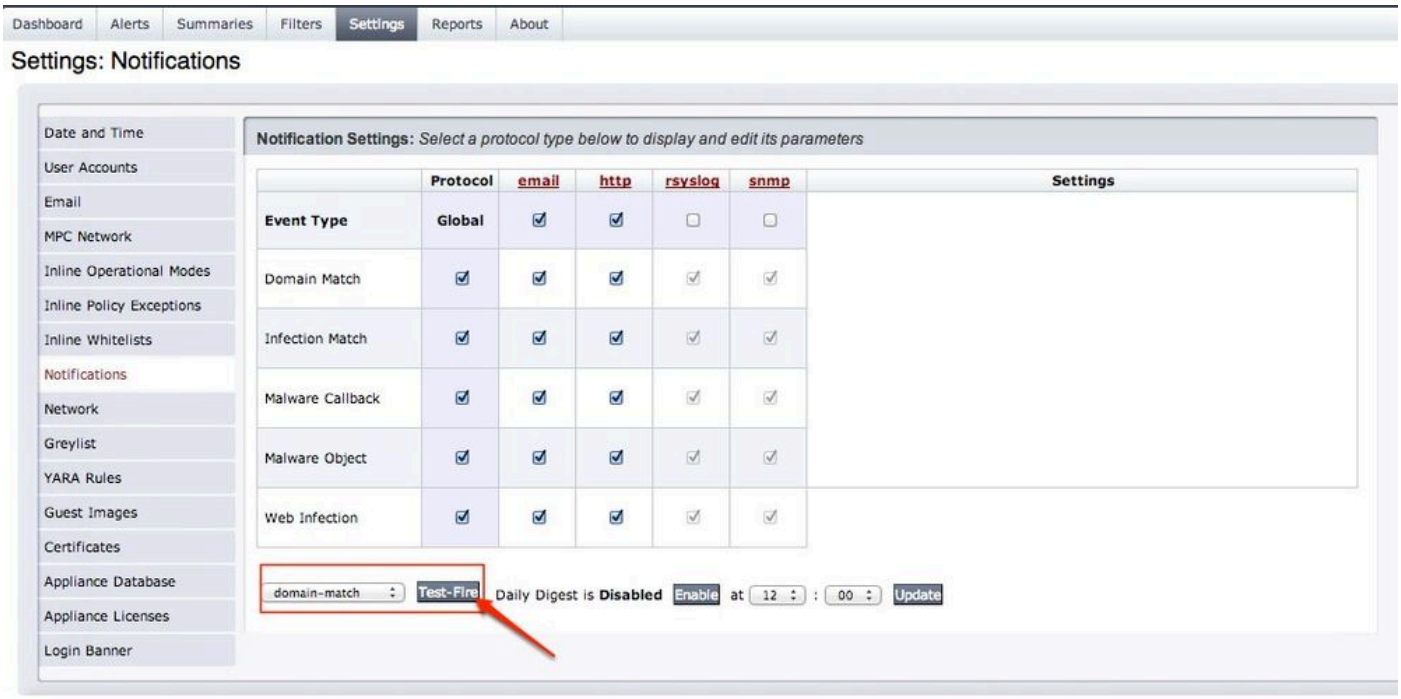
- Livraison : Base par événement
- Fournisseur par défaut : Générique
- Paramètres du fournisseur : Format de message JSON Extended
- (Facultatif) Si vous préférez envoyer le trafic via SSL, sélectionnez SSL Enable.

À ce stade, votre appliance FireEye est configurée pour envoyer les types d'événements sélectionnés à Cisco Umbrella. Apprenez ensuite à afficher ces informations dans votre tableau de bord Cisco Umbrella et à définir une politique de blocage de ce trafic.

Garantir la connectivité : « Tester le feu » entre FireEye et Cisco Umbrella

À ce stade, il est conseillé de tester votre connectivité et de vous assurer que tout est correctement configuré :

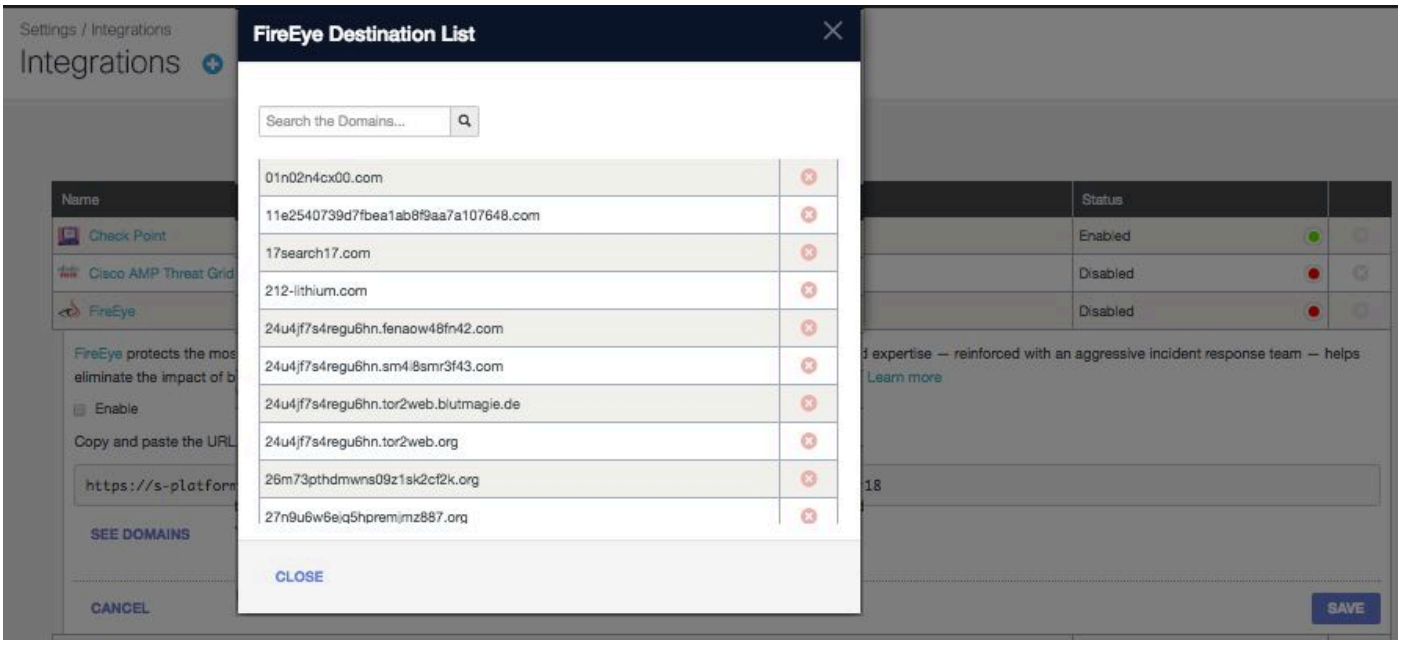
1. Dans FireEye, sélectionnez domain-match dans la liste déroulante Test Fire et sélectionnez Test Fire :



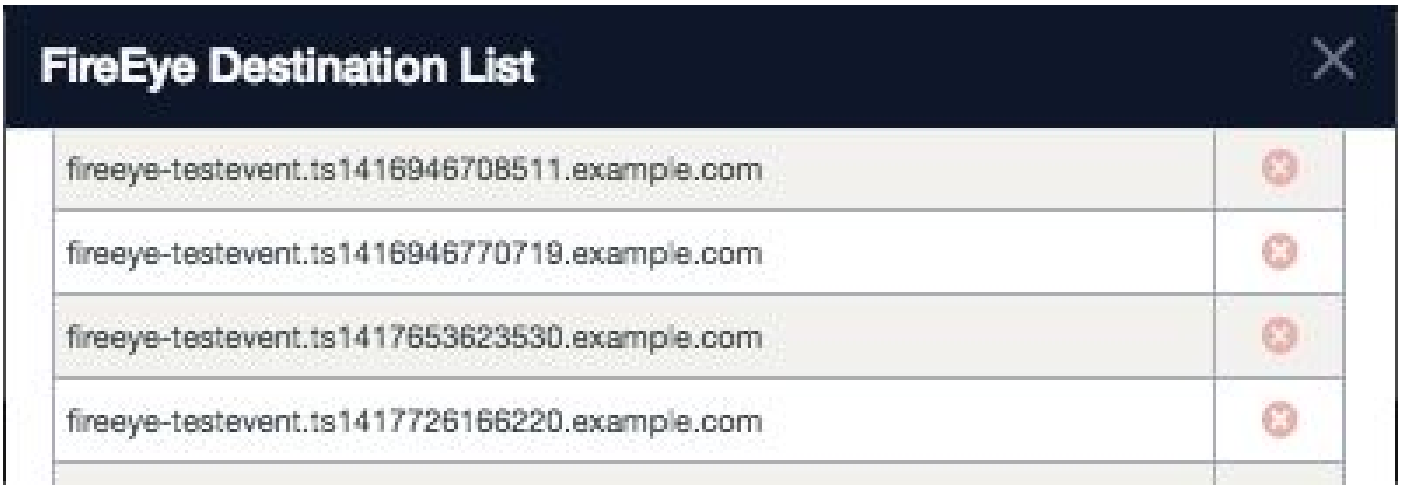
Dans Cisco Umbrella, l'intégration FireEye inclut une liste de domaines fournis par l'appliance FireEye pour voir quels domaines sont ajoutés activement.

2. Après avoir sélectionné Test Fire, dans Cisco Umbrella, accédez à Settings > Integrations et sélectionnez FireEye dans le tableau pour le développer.

3. Sélectionnez Voir Domaines.



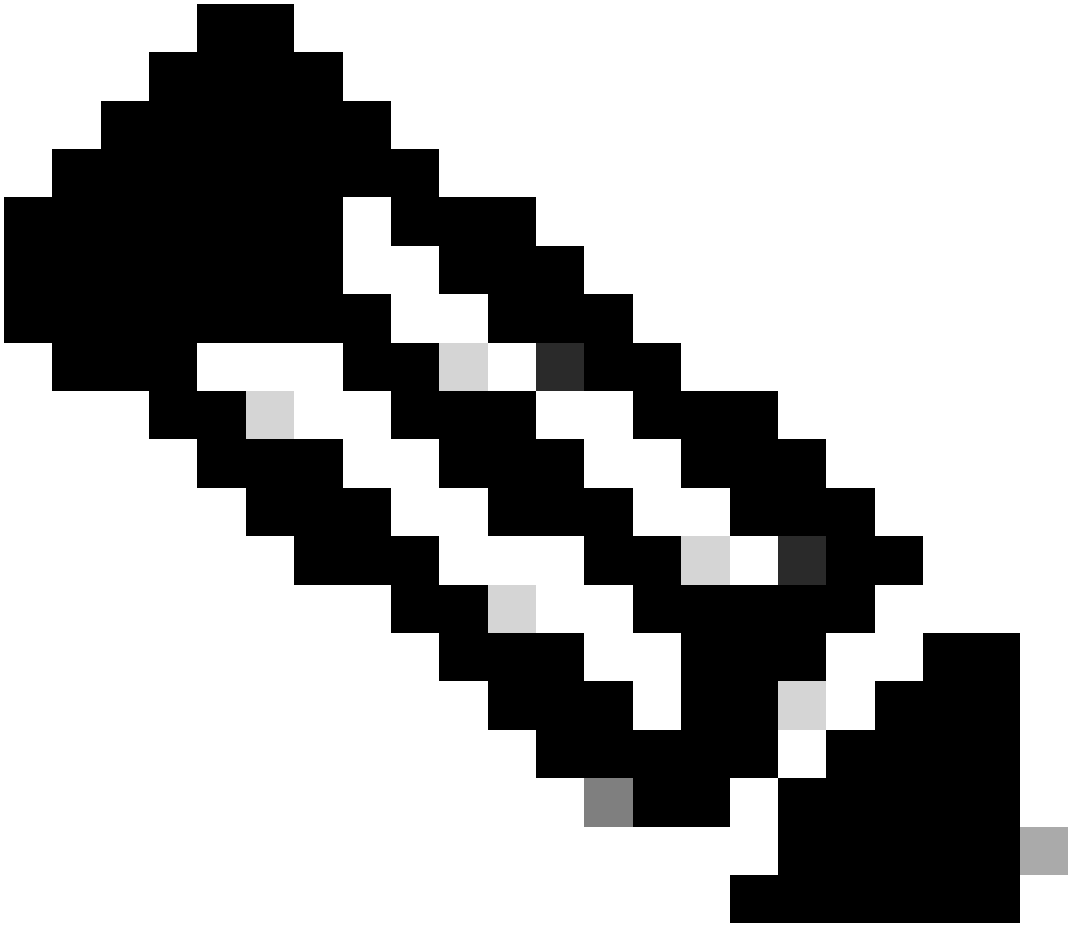
La sélection de Test Fire génère un domaine dans la liste de destinations FireEye nommé « fireeye-testevent.example.com-[date] ». Chaque fois que vous sélectionnez Test Fire dans FireEye, il crée un domaine unique avec la date de l'époque UNIX associée au test, de sorte que les futurs tests peuvent avoir un nom de domaine de test unique.



Si le test Fire réussit, d'autres événements FireEye sont envoyés à Cisco Umbrella et une liste consultable commence à être remplie et à s'allonger.

Observation des événements ajoutés au paramètre de sécurité FireEye en mode audit

Les événements de votre appliance FireEye commencent à remplir une liste de destinations spécifique qui peut être appliquée aux stratégies en tant que catégorie de sécurité FireEye. Par défaut, la liste de destinataires et la catégorie de sécurité sont en « mode audit » et ne s'appliquent à aucune stratégie. Elles ne peuvent pas entraîner de modification de vos stratégies Cisco Umbrella existantes.



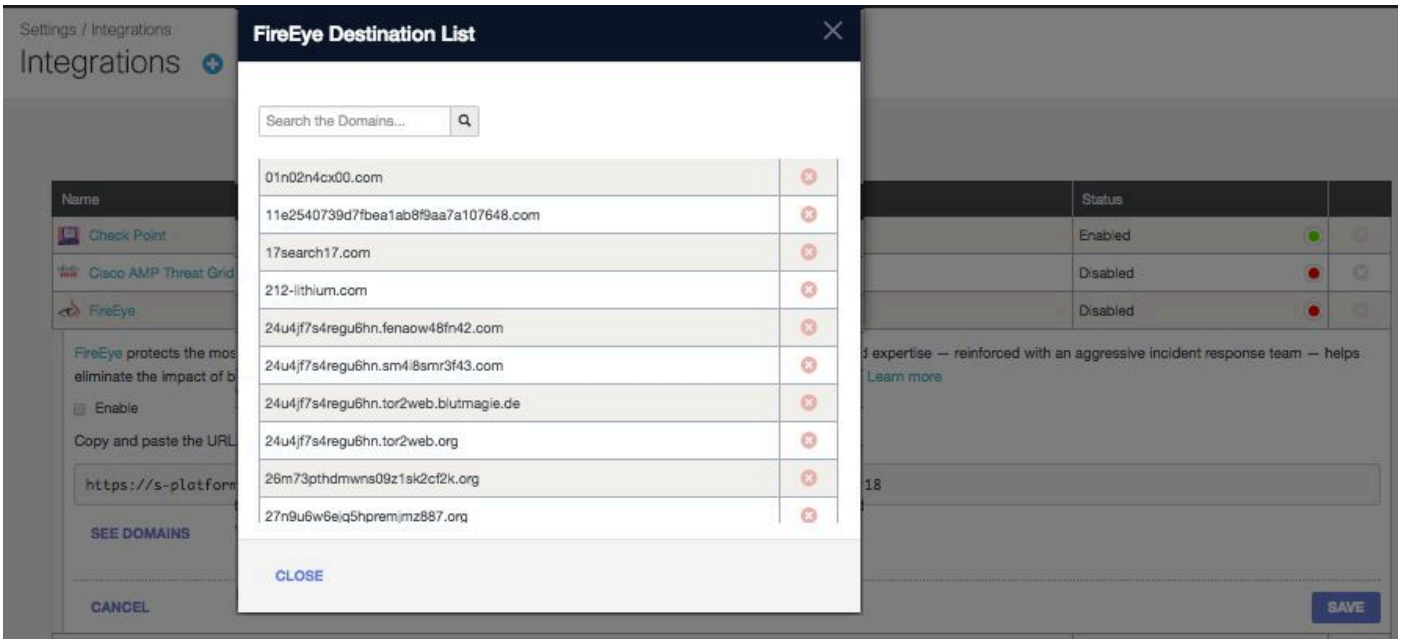
Remarque : Le « mode audit » peut être activé pendant la durée nécessaire, en fonction de votre profil de déploiement et de la configuration du réseau.

Vérifier la liste de destinations

Vous pouvez consulter la liste de destinataires FireEye à tout moment :

1. Accédez à Stratégies > Composants de stratégie > Intégrations.

2. Développez FireEye dans le tableau et sélectionnez Voir domaines.

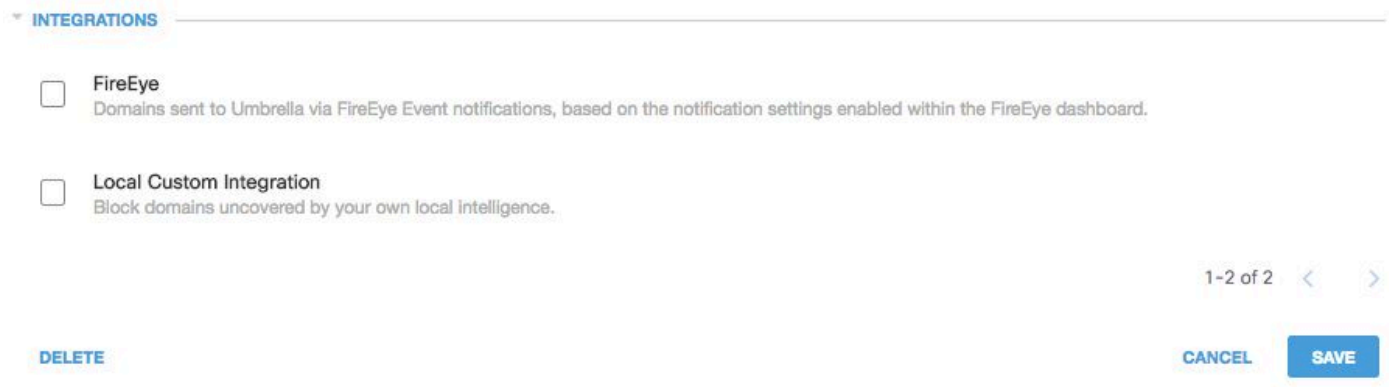


Vérifier les paramètres de sécurité d'une stratégie

Vous pouvez consulter à tout moment les paramètres de sécurité pouvant être ajoutés à une stratégie :

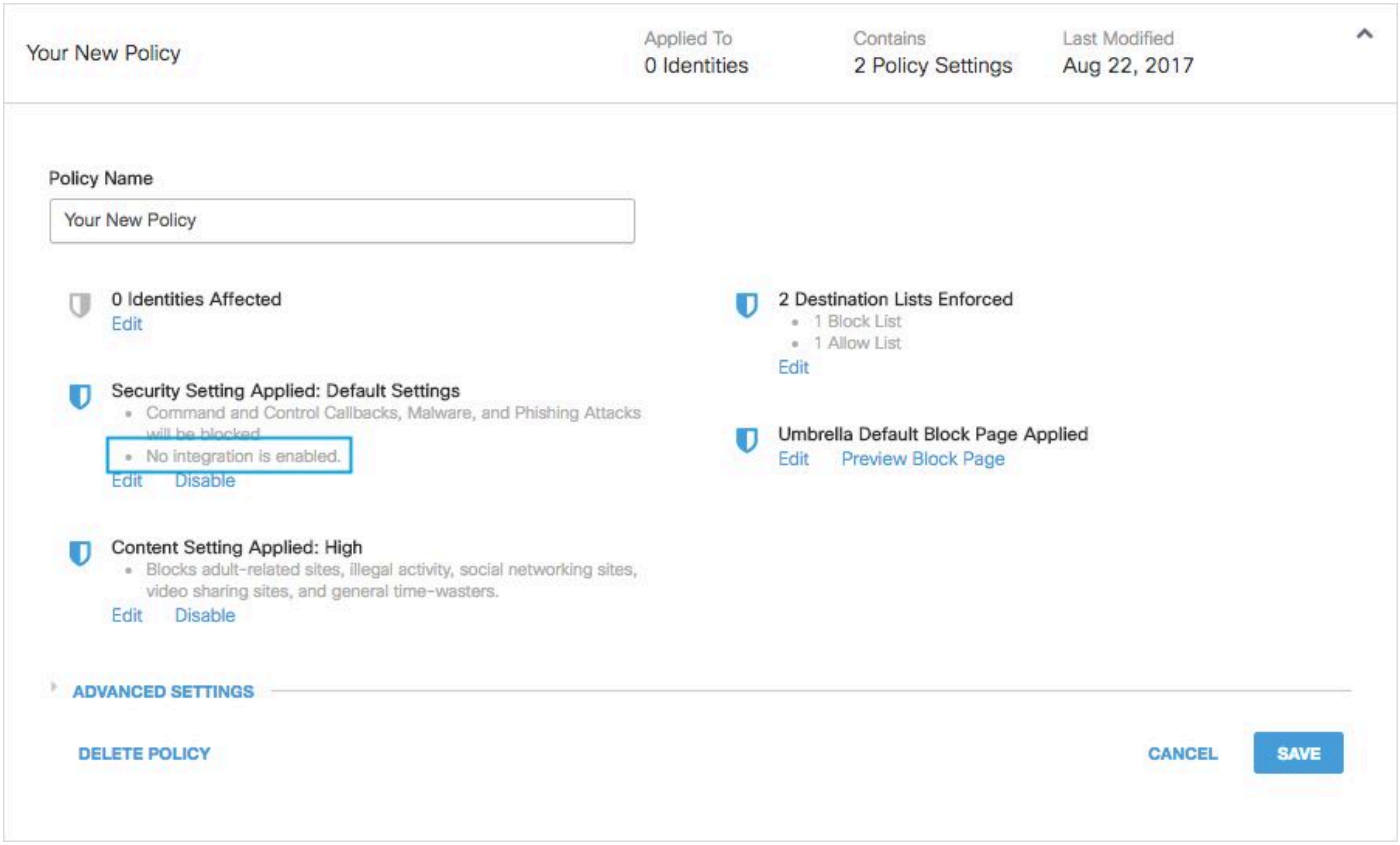
1. Accédez à Stratégies > Composants de stratégie > Paramètres de sécurité.

2. Sélectionnez un paramètre de sécurité dans le tableau pour le développer et faites défiler jusqu'à Integrations pour localiser le paramètre FireEye.



115014080803

Vous pouvez également consulter les informations d'intégration via la page Résumé des paramètres de sécurité.



115013920526

Lors de la mise en route, il est préférable de laisser ce paramètre de sécurité vide afin de s'assurer que les domaines sont correctement renseignés dans un « mode d'audit ».

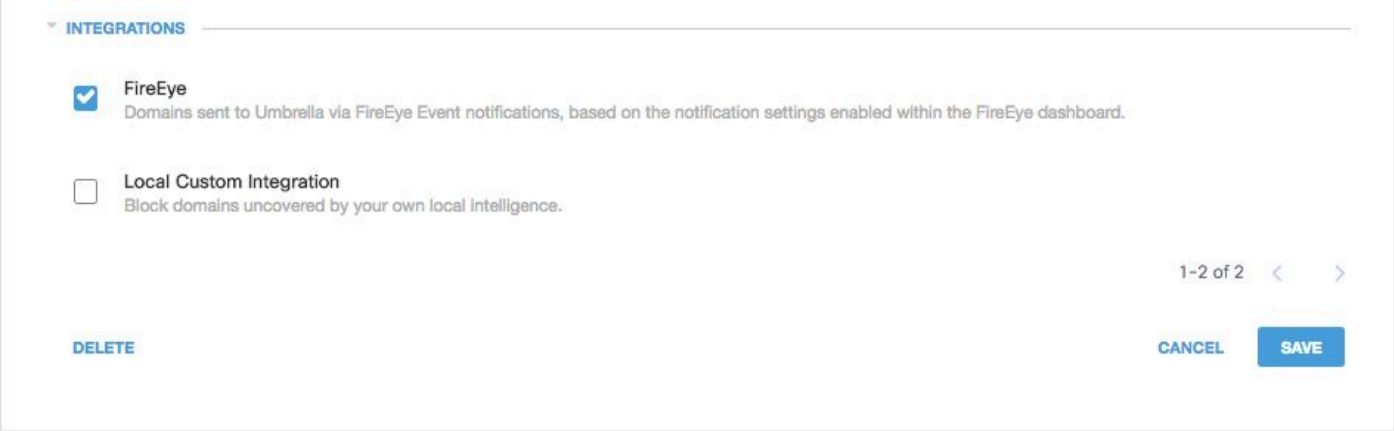
Application des paramètres de sécurité FireEye en « mode blocage » à une stratégie pour les clients gérés

Une fois que vous êtes prêt à faire appliquer ces menaces de sécurité supplémentaires par les clients gérés par Cisco Umbrella, modifiez le paramètre de sécurité sur une stratégie existante ou créez une nouvelle stratégie qui se trouve au-dessus de votre stratégie par défaut pour vous assurer qu'elle est appliquée en premier.

Commencez par créer ou mettre à jour des paramètres de sécurité :

1. Accédez à Stratégies > Composants de stratégie > Paramètres de sécurité.

2. Sous Intégrations, sélectionnez FireEye et sélectionnez Enregistrer.



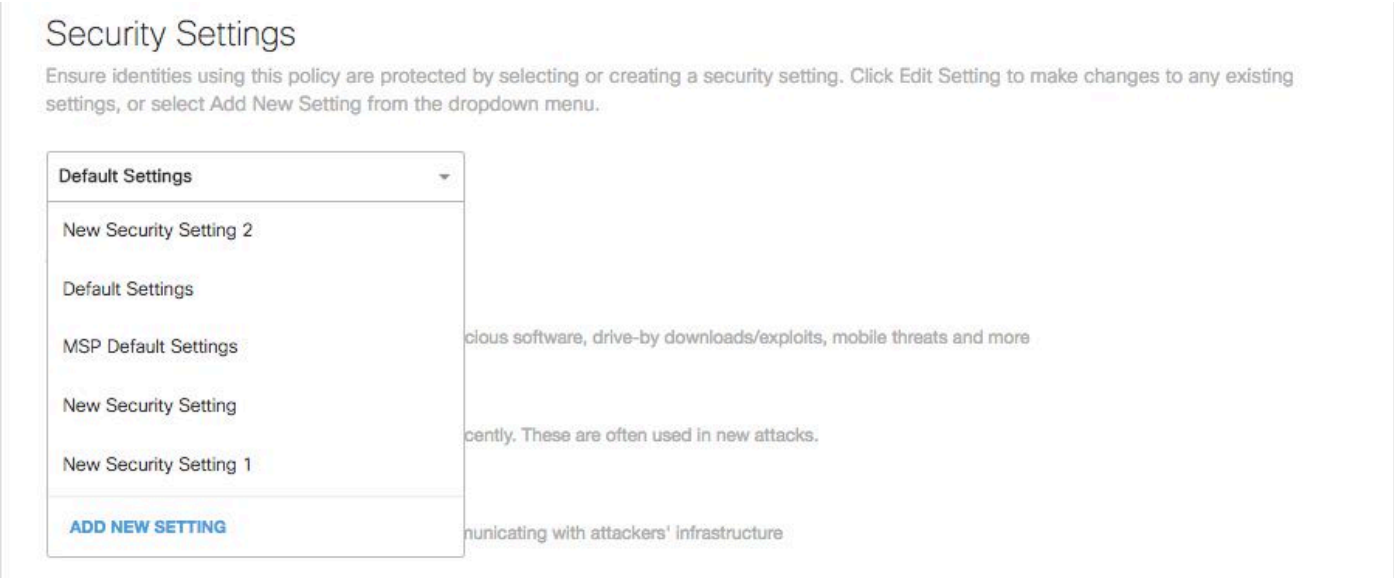
115013921406

Ensuite, dans l'Assistant Stratégie, ajoutez ce paramètre de sécurité à la stratégie que vous modifiez :

1. Accédez à Politiques > Liste des politiques.

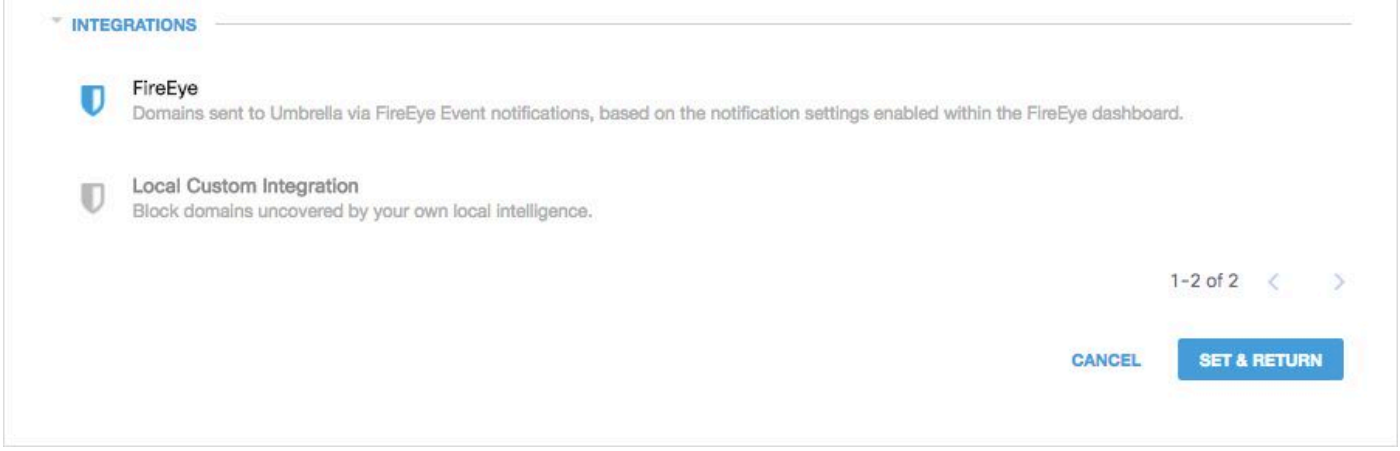
2. Développez une stratégie et sous Paramètres de sécurité appliqués, puis sélectionnez Modifier.

3. Dans la liste déroulante Paramètres de sécurité, sélectionnez un paramètre de sécurité qui inclut le paramètre FireEye.



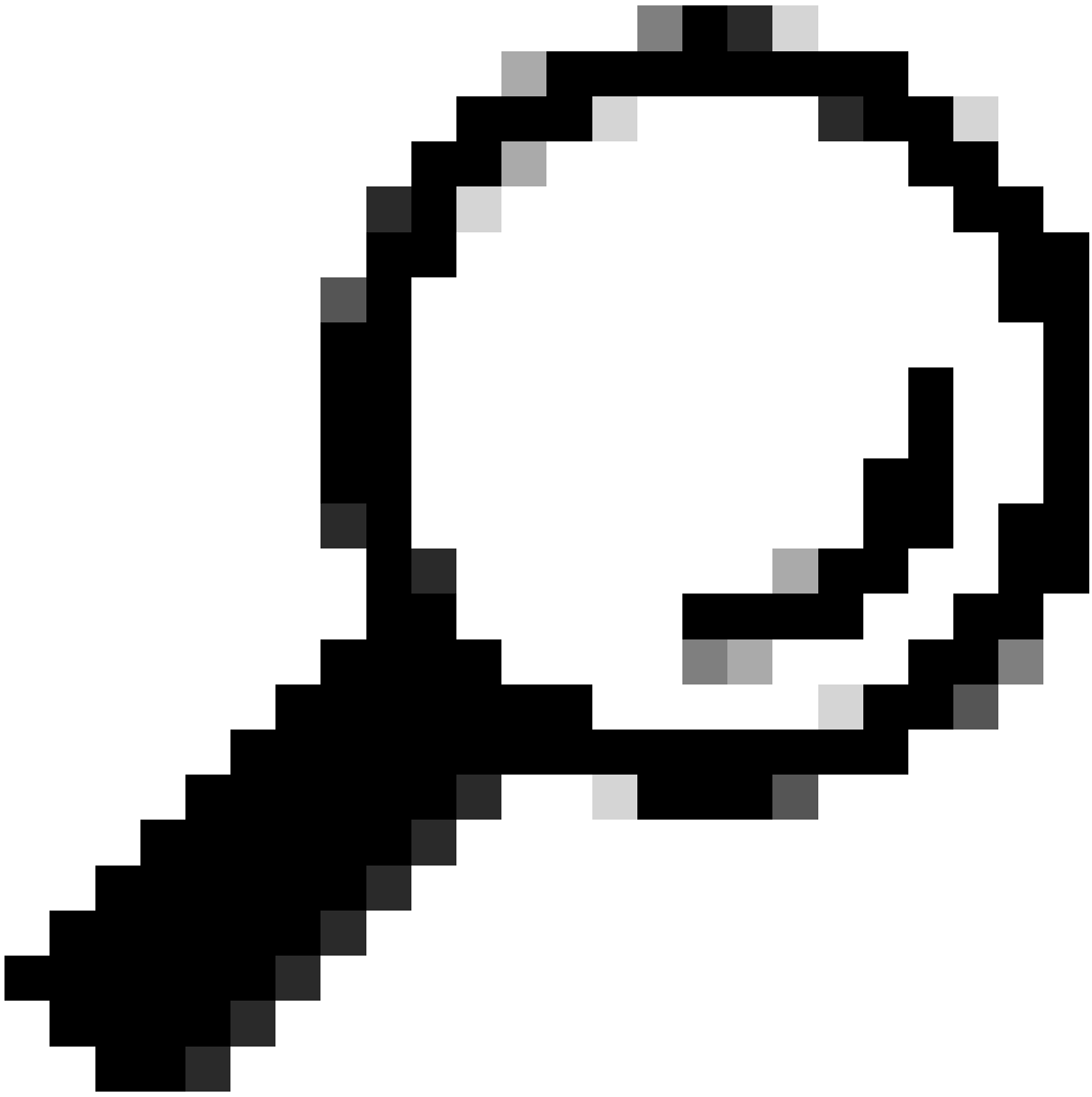
115014083083

L'icône en forme de bouclier sous Intégrations devient bleue.



115013922146

4. Sélectionnez Définir &Retour.



Conseil : Il est également possible de modifier vos paramètres de sécurité à partir de l'Assistant Stratégie.

Les domaines FireEye contenus dans le paramètre de sécurité de FireEye sont bloqués pour les identités utilisant la stratégie.

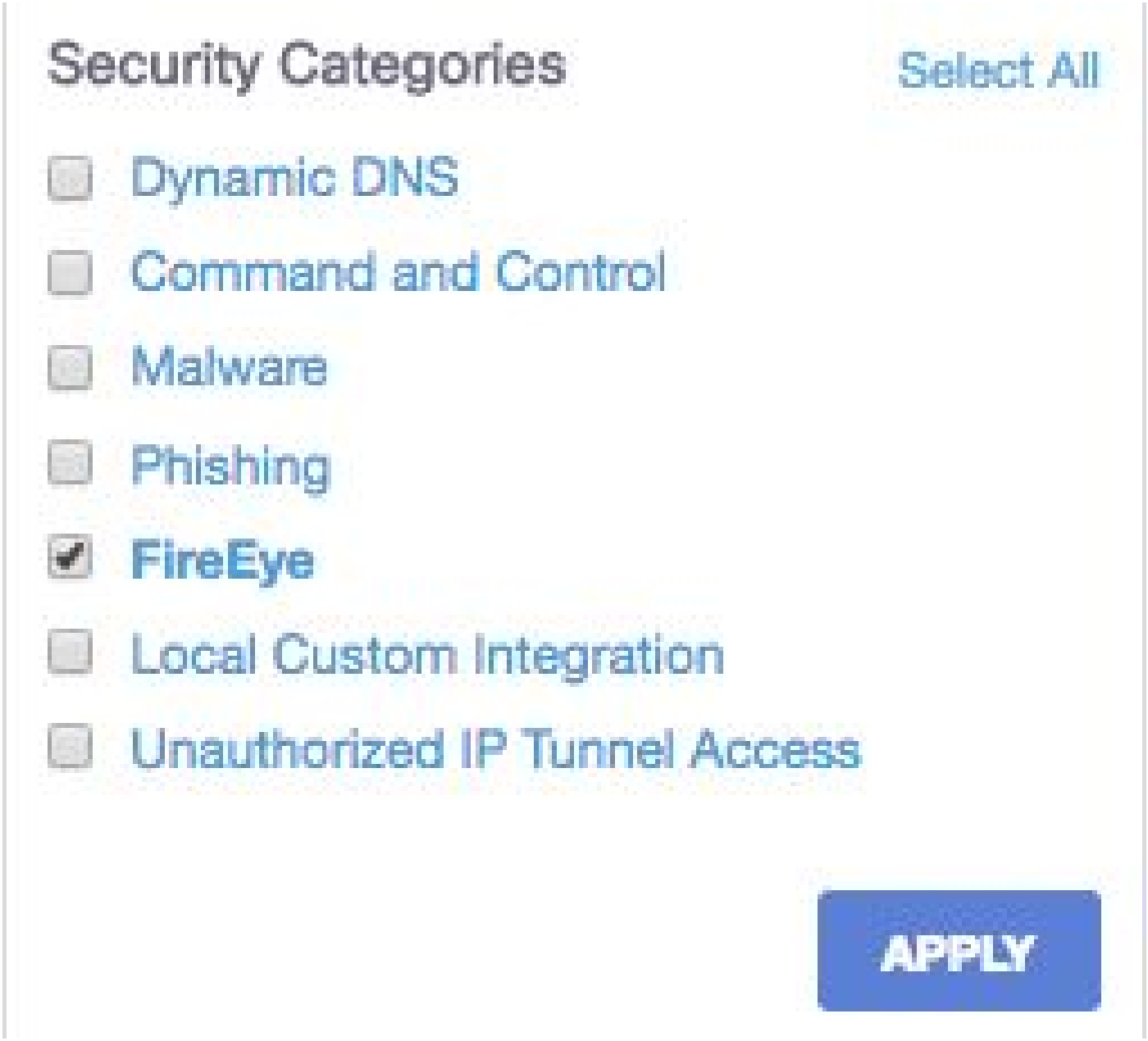
Rapports dans Cisco Umbrella pour les événements FireEye

Rapports sur les événements de sécurité FireEye

La liste de destinataires FireEye est l'une des catégories de sécurité disponibles pour les rapports. La plupart ou la totalité des rapports utilisent les catégories de sécurité comme filtre. Par exemple, vous pouvez filtrer les catégories de sécurité pour afficher uniquement les activités liées à FireEye :

1. Accédez à Reporting > Activity Search.

2. Sous Catégories de sécurité, sélectionnez FireEye pour filtrer le rapport et afficher uniquement la catégorie de sécurité pour FireEye.



115013924986

3. Sélectionnez Appliquer pour afficher l'activité liée à FireEye pour la période sélectionnée dans l'état.

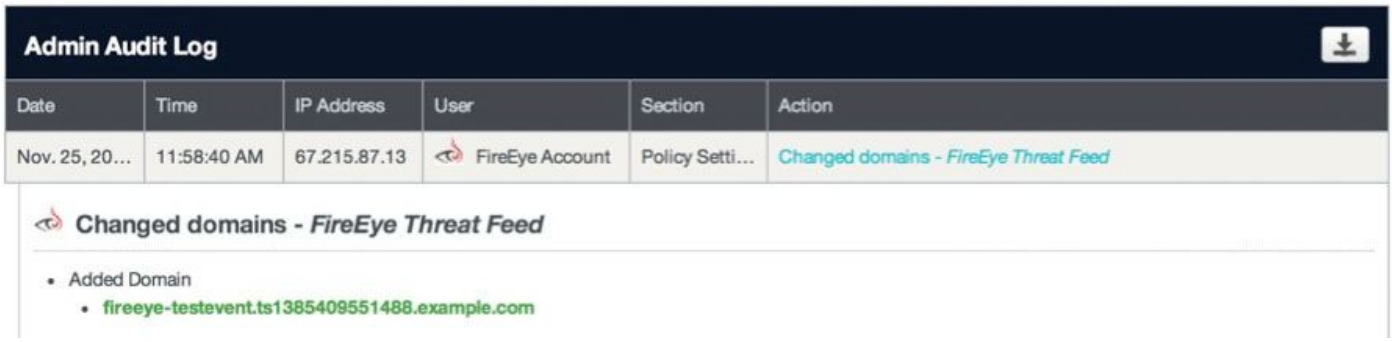
Signalement du moment où les domaines ont été ajoutés à la liste de destinations FireEye

Le journal d'audit d'administration inclut les événements de l'appliance FireEye lorsqu'il ajoute des domaines à la liste de destination. Un utilisateur nommé « Compte FireEye », également marqué du logo FireEye, génère les événements. Ces événements incluent le domaine qui a été ajouté et l'heure à laquelle il a été ajouté.

Vous pouvez filtrer pour inclure uniquement les modifications FireEye en appliquant un filtre pour l'utilisateur « Compte FireEye ».

Si l'étape « Test Fire » précédente a été effectuée, l'ajout du domaine de test FireEye peut

apparaître dans le journal d'audit.



Gestion des détections indésirables ou des faux positifs

Listes d’autorisation

Bien que peu probable, il est possible que les domaines ajoutés automatiquement par votre appliance FireEye déclenchent une détection indésirable qui empêche vos utilisateurs d'accéder à des sites Web particuliers. Dans une telle situation, Umbrella recommande d'ajouter le ou les domaines à une liste d'autorisation (Politiques > Listes de destination), qui a priorité sur tous les autres types de listes de blocage, y compris les paramètres de sécurité.

Cette approche est préférable pour deux raisons.

- Tout d'abord, si l'appliance FireEye devait ajouter à nouveau le domaine après sa suppression, la liste d'autorisation protège contre ce risque, ce qui entraînerait d'autres problèmes.
- Ensuite, la liste verte affiche un historique des domaines problématiques pouvant être utilisés pour des analyses ou des rapports d'audit.

Par défaut, une liste verte globale est appliquée à toutes les stratégies. L'ajout d'un domaine à la liste verte globale entraîne l'autorisation du domaine dans toutes les stratégies.

Si le paramètre de sécurité FireEye en mode bloc est appliqué uniquement à un sous-ensemble de vos identités Cisco Umbrella gérées (par exemple, il est appliqué uniquement aux ordinateurs et périphériques mobiles itinérants), vous pouvez créer une liste d'autorisation spécifique pour ces identités ou stratégies.

Pour créer une liste verte :

1. Accédez à Politiques > Listes de destinations et sélectionnez l'icône Ajouter.

2. Sélectionnez Autoriser et ajoutez votre domaine à la liste.

3. Sélectionnez Enregistrer.

Une fois la liste de destinations enregistrée, vous pouvez l'ajouter à une stratégie existante couvrant les clients qui ont été affectés par le blocage indésirable.

Suppression de domaines de la liste de destinations FireEye

À côté de chaque nom de domaine dans la liste de destination FireEye se trouve une icône Delete. La suppression de domaines vous permet de nettoyer la liste de destinations FireEye en cas de détection indésirable.

Toutefois, la suppression n'est pas permanente si l'appliance FireEye renvoie le domaine à Cisco Umbrella.

Pour supprimer un domaine :

1. Accédez à Paramètres > Intégrations, puis sélectionnez "FireEye" pour le développer.

2. Sélectionnez Voir Domaines.

3. Recherchez le nom de domaine que vous souhaitez supprimer.

4. Cliquez sur l'icône Supprimer.

5. Sélectionnez Fermer.

6. Sélectionnez Enregistrer.

Dans le cas d'une détection indésirable ou d'un faux positif, Umbrella recommande de créer immédiatement une liste d'autorisation dans Cisco Umbrella, puis de corriger le faux positif dans l'appliance FireEye. Vous pourrez ensuite supprimer le domaine de la liste de destinations FireEye.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.