Configurer l'intelligence de sécurité basée sur le domaine (stratégie DNS) dans le module FirePOWER avec ASDM (gestion intégrée)

Contenu

Introduction

Ce document décrit comment configurer l'intelligence de sécurité basée sur le domaine (SI) sur ASA avec le module FirePOWER à l'aide d'Adaptive Security Device Manager (ASDM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du pare-feu ASA (Adaptive Security Appliance)
- ASDM (Adaptive Security Device Manager)

- Connaissances du module FirePOWER

Note: Le filtre Security Intelligence nécessite une licence Protection.

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Modules ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) avec version logicielle 6.0.0 et ultérieure
- Module ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) avec les versions 6.0.0 et ultérieures du logiciel

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le système Firepower permet d'intercepter les requêtes de trafic DNS et recherche le nom de domaine malveillant. Si le module Firepower trouve un domaine malveillant, Firepower prend les mesures appropriées pour atténuer la demande conformément à la configuration de la stratégie DNS.

De nouvelles méthodes d'attaque conçues pour violer l'intelligence basée sur IP et utiliser à mauvais escient les fonctions d'équilibrage de charge DNS afin de masquer l'adresse IP réelle d'un serveur malveillant. Bien que les adresses IP associées à l'attaque soient fréquemment échangées entre elles et en dehors, le nom de domaine est rarement modifié.

Firepower permet de rediriger la requête malveillante vers un serveur incomplet qui peut être un serveur de miel pour détecter, dévier ou étudier les tentatives d'en savoir plus sur le trafic d'attaque.

Présentation des listes de domaines et des flux

Les listes de domaines et les flux contiennent la liste des noms de domaine malveillants qui sont ensuite classés dans les différentes catégories en fonction du type d'attaque. En règle générale, vous pouvez classer les flux en deux types.

Listes de domaines et flux fournis par Cisco TALOS

Attaques DNS : collection de noms de domaine qui recherchent continuellement des vulnérabilités ou des tentatives d'exploitation d'autres systèmes.

Bogon DNS : collection de noms de domaine qui n'allouent pas mais renvoient le trafic, également appelé Fake IPs.

Bots DNS : collection de noms de domaine qui participent activement comme faisant partie d'un botnet et sont contrôlés par un contrôleur de botnet connu.

DNS CnC : collection de noms de domaine identifiés comme serveurs de contrôle pour un Botnet connu.

Kit d'exploits DNS : Collection de noms de domaine qui tentent d'exploiter d'autres systèmes.

Malwares DNS : collection de noms de domaine qui tentent de propager des programmes malveillants ou attaquent activement quiconque les visite.

DNS Open_proxy : collection de noms de domaine qui exécutent les serveurs proxy Web ouverts et offrent des services de navigation Web anonymes.

DNS Open_relay : collection de noms de domaine qui offrent des services de relais de messagerie anonyme utilisés par les courriers indésirables et les hameçonneurs.

Phishing DNS : collection de noms de domaine qui tentent activement de tromper un utilisateur final pour qu'il saisisse ses informations confidentielles telles que les noms d'utilisateur et les mots de passe.

Réponse DNS : Collection de noms de domaine qui sont observés à plusieurs reprises et qui se livrent à des comportements suspects ou malveillants.

Courrier indésirable DNS : collection de noms de domaine identifiés comme source d'envoi de courriers indésirables.

DNS Suspicious : collection de noms de domaine affichant une activité suspecte et faisant l'objet d'une enquête active.

DNS Tor_exit_node : Collection de noms de domaine qui offrent des services de noeud de sortie pour le réseau Tor Anonymizer.

Listes de domaines et flux personnalisés

Liste de blocage globale pour DNS : Collection de la liste personnalisée des noms de domaine identifiés comme malveillants par l'administrateur.

Liste d'autorisation globale pour DNS : Collection de la liste personnalisée des noms de domaine identifiés comme authentiques par l'administrateur.

Configurer DNS Security Intelligence

Il existe plusieurs étapes pour configurer l'intelligence de sécurité basée sur les noms de domaine.

1. Configurer le flux/la liste DNS personnalisé (facultatif)
2. Configurer l'objet Sinkhole (facultatif)
3. Configurer la stratégie DNS
4. Configurer la stratégie de contrôle d'accès
5. Déployer la stratégie de contrôle d'accès

Étape 1. Configurer le flux/la liste DNS personnalisé (facultatif).

Il existe deux listes prédéfinies qui vous permettent d'y ajouter les domaines. Vous créez vos propres listes et flux pour les domaines que vous voulez bloquer.

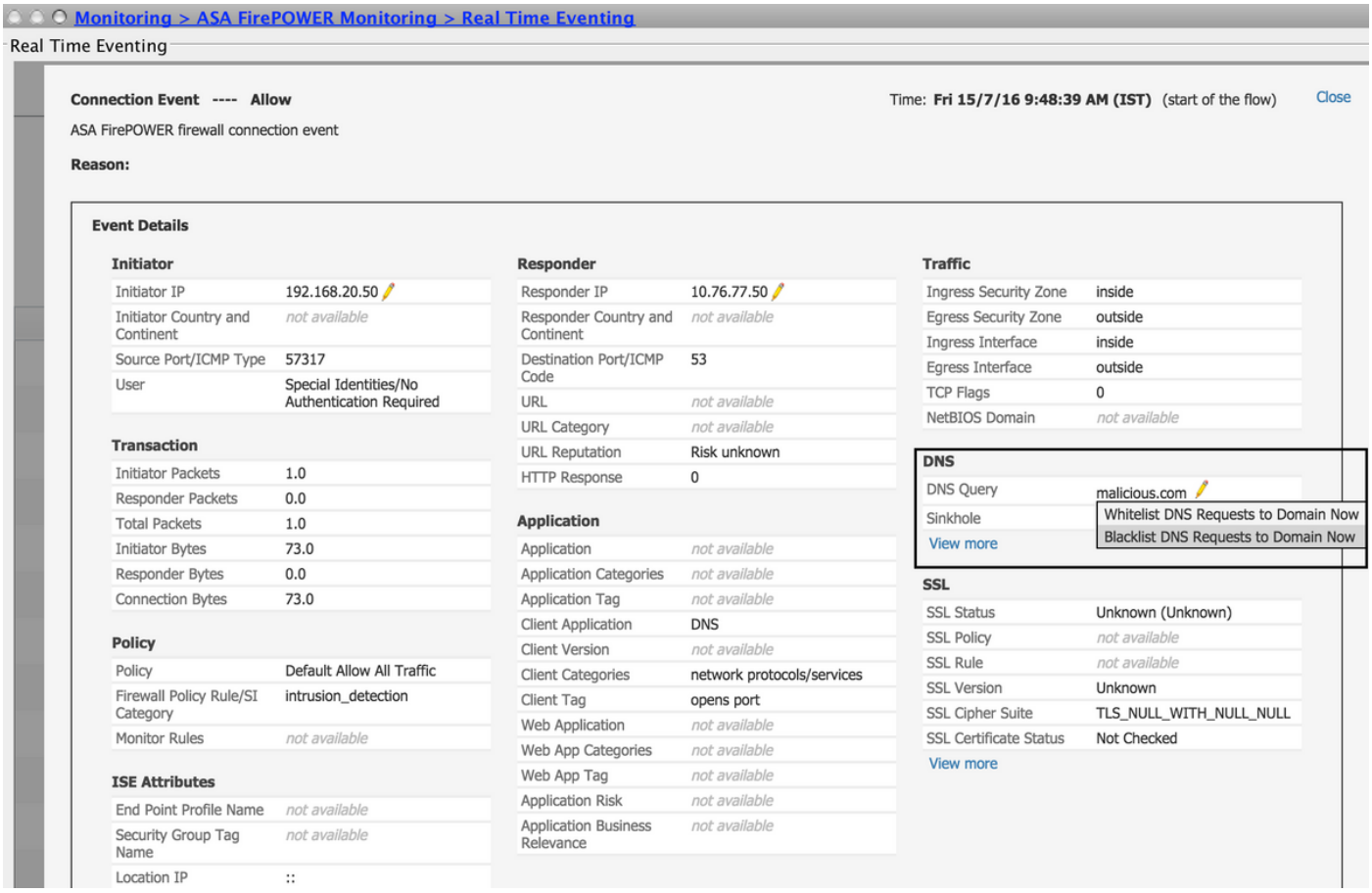
- Liste de blocage globale pour DNS
- Liste d'autorisation globale pour DNS

Ajouter manuellement des adresses IP à la liste de blocage globale et à la liste d'autorisation globale

Firepower vous permet d'ajouter certains domaines à Global-Blacklist lorsque vous savez qu'ils font partie d'une activité malveillante. Les domaines peuvent également être ajoutés à la liste blanche globale si vous voulez autoriser le trafic vers certains domaines bloqués par des domaines de liste noire. Si vous ajoutez un domaine à Global-Blacklist/Global-Whitelist, il prend effet immédiatement sans qu'il soit nécessaire d'appliquer la stratégie.

Afin d'ajouter l'adresse IP à Global-Blacklist/ Global-Whitelist, naviguez jusqu'à **Monitoring > ASA FirePOWER Monitoring > Real Time Evant**, pointez la souris sur les événements de connexion et sélectionnez **View Details**.

Vous pouvez ajouter des domaines à la liste de blocage globale/liste de blocage globale. Cliquez sur **Edit** dans la section DNS et sélectionnez **Whitelist DNS Requests to Domain Now/Blacklist DNS Requests to Domain Now** pour ajouter le domaine à la liste respective, comme illustré dans l'image.



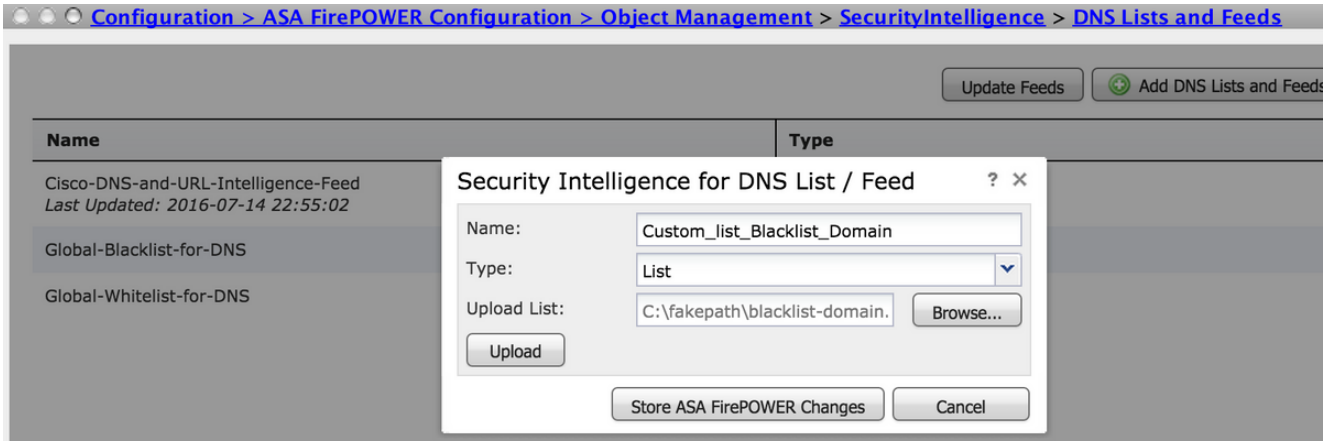
Afin de vérifier que les domaines sont ajoutés à la liste de blocage global/liste de blocage global, accédez à **Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds** et modifiez **Global-Blacklist for DNS / Global Whitelist for DNS**. Vous pouvez également utiliser le bouton Supprimer pour supprimer n'importe quel domaine de la liste.

Créer une liste personnalisée de domaines de liste noire

Firepower vous permet de créer une liste de domaines personnalisée qui peut être utilisée pour mettre en liste noire (bloquer) par deux méthodes différentes.

1. Vous pouvez écrire des noms de domaine dans un fichier texte (un domaine par ligne) et charger le fichier dans FirePOWER Module.

   Afin de télécharger le fichier, accédez à **Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds**, puis sélectionnez **Add DNS Lists and Feeds** **Name :** Spécifiez le nom de la liste Personnalisée. **type :** Sélectionnez **Liste** dans la liste déroulante. **Liste de téléchargement :** Choisissez **Parcourir** pour localiser le fichier texte dans votre système. Sélectionnez **Télécharger** pour télécharger le fichier.



Cliquez sur **Store ASA FirePOWER Changes** pour enregistrer les modifications.

2. Vous pouvez utiliser n'importe quel domaine tiers pour la liste personnalisée pour laquelle le module Firepower peut connecter le serveur tiers pour récupérer la liste de domaines.

   Pour configurer ceci, accédez à **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds** puis sélectionnez **Add DNS Lists and Feeds**

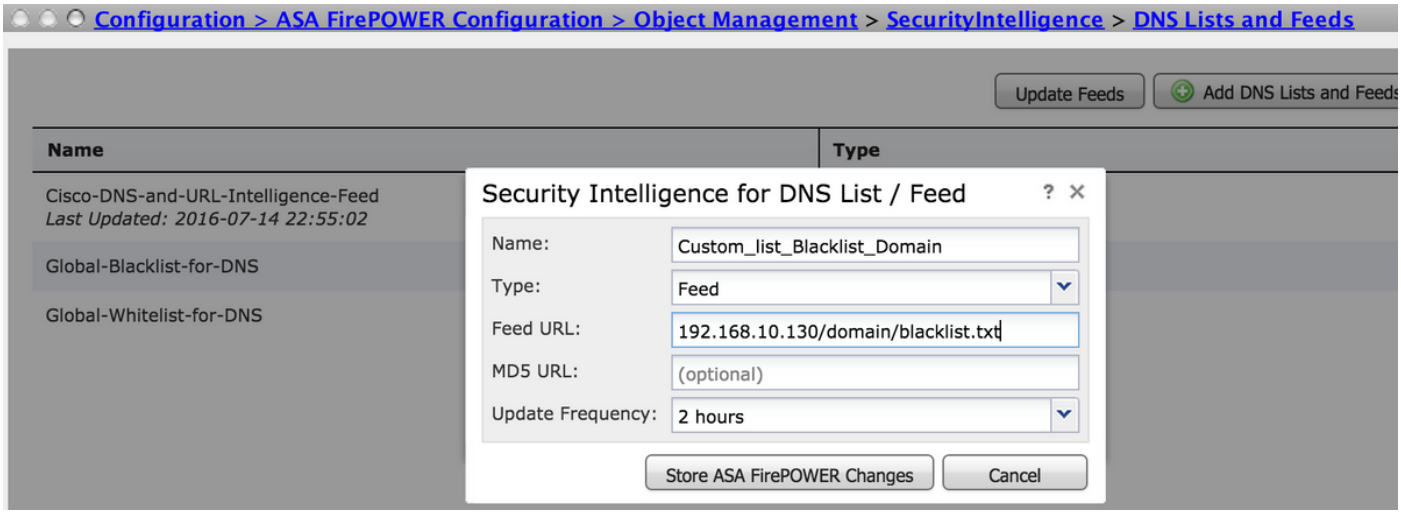
   Name : Spécifiez le nom du flux personnalisé.

   type : Sélectionnez **Feed** dans la liste déroulante.

   URL du flux : Spécifiez l'URL du serveur auquel le module FirePOWER peut se connecter et télécharger le flux.

   URL MD5 : Spécifiez la valeur de hachage pour valider le chemin d'URL du flux.

   Fréquence de mise à jour : Spécifiez l'intervalle de temps pendant lequel le module se connecte au serveur de flux d'URL.



Sélectionnez **Stocker les modifications FirePOWER ASA** pour enregistrer les modifications.

Étape 2. Configurer Un Objet Sinkhole (facultatif).

L'adresse IP incomplète peut être utilisée comme réponse à une requête DNS malveillante.

L'ordinateur client obtient l'adresse IP du serveur incomplet pour la recherche de domaine malveillant et l'ordinateur final tente de se connecter au serveur incomplet. Par conséquent, le trou d'eau peut servir de pot de miel pour enquêter sur le trafic d'attaque. Le trou d'éclat peut être configuré pour déclencher un indicateur de compromission (IOC).

Pour ajouter le serveur incomplet, **Configuration > ASA FirePOWER Configuration > Object Management > Sinkhole** & cliquez sur l'option **Add Sinkhole**.

Name : Spécifiez le nom du serveur de puits.

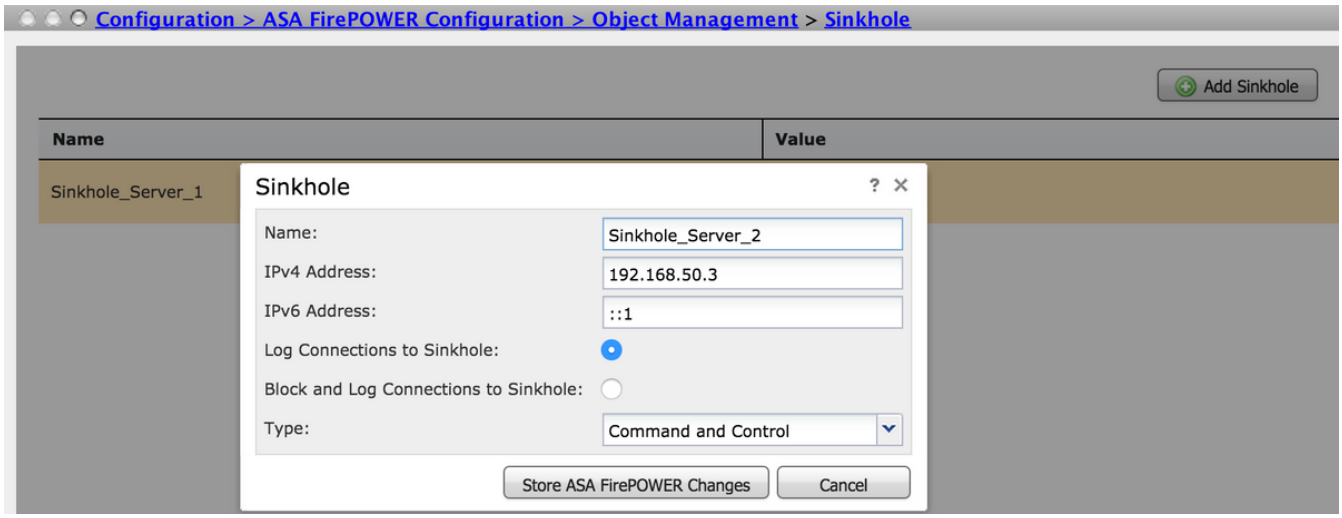
Adresse IP : Spécifiez l'adresse IP du serveur de puits.

Consigner les connexions à Sinkhole : Activez cette option pour consigner toutes les connexions entre le serveur de point d'extrémité et le serveur de puits.

Bloquer et consigner les connexions à Sinkhole : Activez cette option pour bloquer la connexion et ne vous connecter qu'au début de la connexion de flux. S'il n'y a pas de serveur physique, vous pouvez spécifier n'importe quelle adresse IP et vous pouvez voir les événements de connexion et le déclencheur IOC.

type : Spécifiez le flux dans la liste déroulante pour laquelle vous souhaitez sélectionner le type de CIO (Indication de compromission) associé aux événements de trou de disque. Il existe trois types de CIO de puits qui peuvent être étiquetés.

- Programme malveillant
- Commande et contrôle
- Hameçonner



Étape 3. Configurez la stratégie DNS.

La stratégie DNS doit être configurée pour décider de l'action pour le flux/la liste DNS. Accédez à **Configuration > ASA FirePOWER Configuration > Policies > DNS Policy.**

La stratégie DNS par défaut contient deux règles par défaut. La première règle, **Liste d'autorisation globale pour DNS**, contient la liste personnalisée du domaine autorisé (**Liste**

d'autorisation globale pour DNS). Cette règle se trouve en haut de la liste pour correspondre avant que le système ne tente de faire correspondre n'importe quel domaine de liste noire. La deuxième règle, **Liste de blocage globale pour DNS**, contient la liste personnalisée du domaine bloqué (**Liste de blocage globale pour DNS**).

Vous pouvez ajouter des règles pour définir les différentes actions pour les **listes de domaines et les flux fournis par Cisco TALOS**. Pour ajouter une nouvelle règle, sélectionnez **Ajouter une règle DNS.**

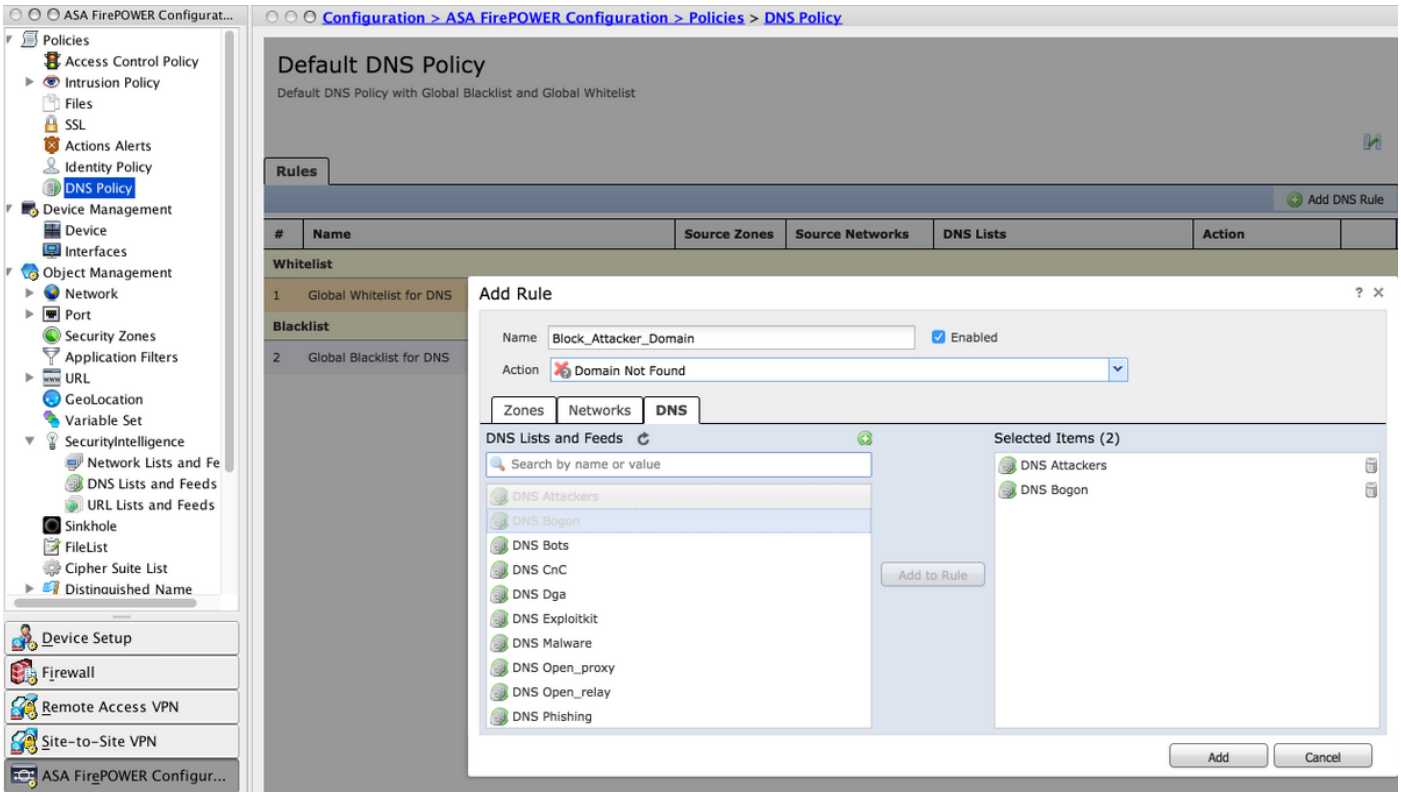
Nom : spécifiez le nom de la règle.

Action : Spécifiez l'action à déclencher lorsque cette règle correspond.

- **Liste blanche :** Ceci permet la requête DNS.
- **Monitor:** Cette action génère l'événement pour la requête DNS et le trafic continue de correspondre aux règles suivantes.
- **Domaine introuvable :** cette action envoie une réponse DNS en tant que domaine introuvable (domaine inexistant).
- **Déposer :** Cette action bloque et supprime la requête DNS en silence.
- **Encre :** Cette action envoie l'adresse IP du serveur Sinkhole comme réponse à la requête DNS.

Spécifiez les **zones/réseau** pour définir les conditions de la règle. Dans l'onglet DNS, sélectionnez les **listes et les flux DNS** et passez à l'option **Éléments sélectionnés** où vous pouvez appliquer l'action configurée.

Vous pouvez configurer plusieurs règles DNS pour différentes listes et flux DNS avec une action différente en fonction des besoins de votre organisation.

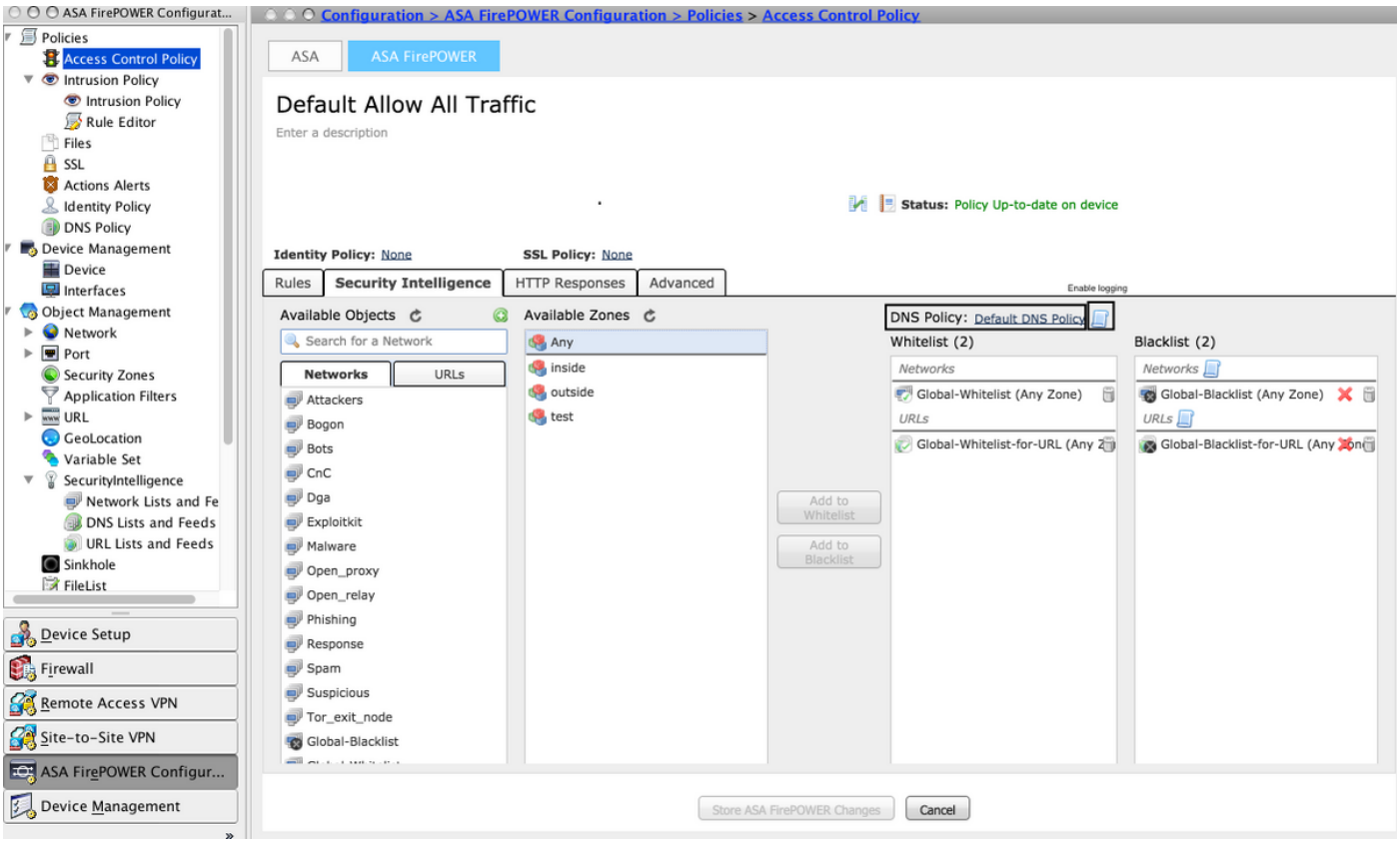


Cliquez sur l'option **Ajouter** pour ajouter la règle.

Étape 4. Configurez la stratégie de contrôle d'accès.

Afin de configurer l'intelligence de sécurité basée sur DNS, accédez à **Configuration > ASA Firepower Configuration > Policies > Access Control Policy,** sélectionnez **Security Intelligence** tab.

Assurez-vous que la stratégie DNS est configurée et, éventuellement, que vous pouvez activer les journaux lorsque vous cliquez sur l'icône des journaux comme indiqué dans l'image.



Choisissez l'option **Stocker les modifications ASA Firepower** pour enregistrer les modifications de la stratégie AC.

Étape 5. Déployer la stratégie de contrôle d'accès.

Pour que les modifications prennent effet, vous devez déployer la stratégie de contrôle d'accès. Avant d'appliquer la stratégie, vérifiez si la stratégie de contrôle d'accès est obsolète ou non sur le périphérique.

Pour déployer les modifications sur le capteur, cliquez sur **Déployer** et choisissez **Déployer les modifications FirePOWER** puis sélectionnez **Déployer** dans la fenêtre contextuelle pour déployer les modifications.

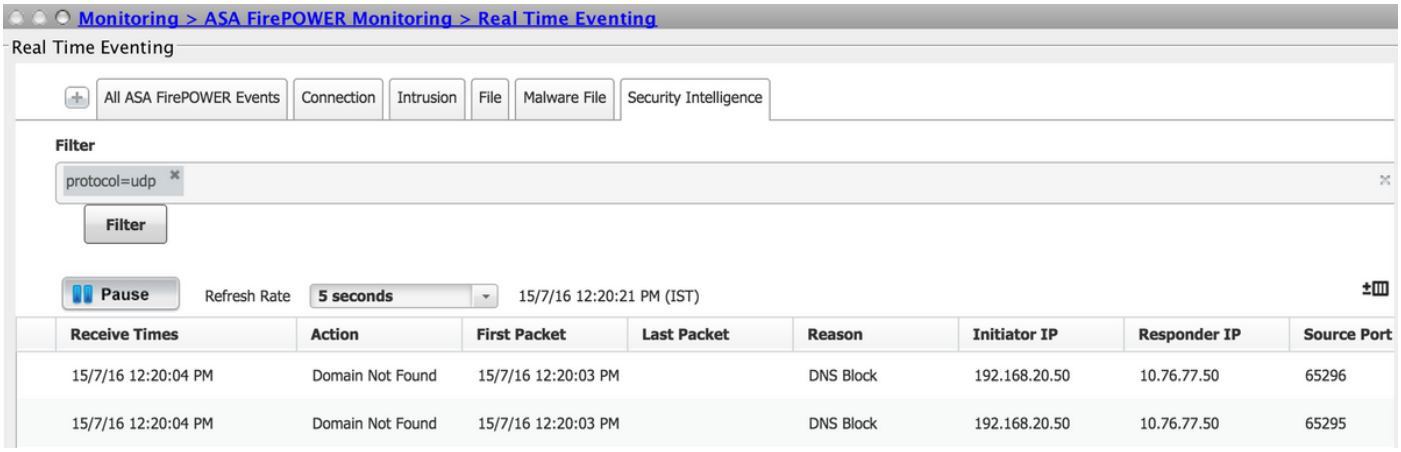
> **Note**: Dans la version 5.4.x, pour appliquer la stratégie Access au capteur, cliquez sur **Appliquer les modifications ASA FirePOWER.**

Note: Accédez à Monitoring > ASA Firepower Monitoring > Task Status. Assurez-vous que la tâche est terminée pour confirmer les modifications de configuration. **Vérification**La configuration ne peut être vérifiée que si un événement est déclenché. Pour cela, vous pouvez

forcer une requête DNS sur une machine. Cependant, soyez prudent quant aux répercussions lorsqu'un serveur malveillant connu est ciblé. Après avoir généré cette requête, vous pouvez voir l'événement dans la section Évolution en temps réel.

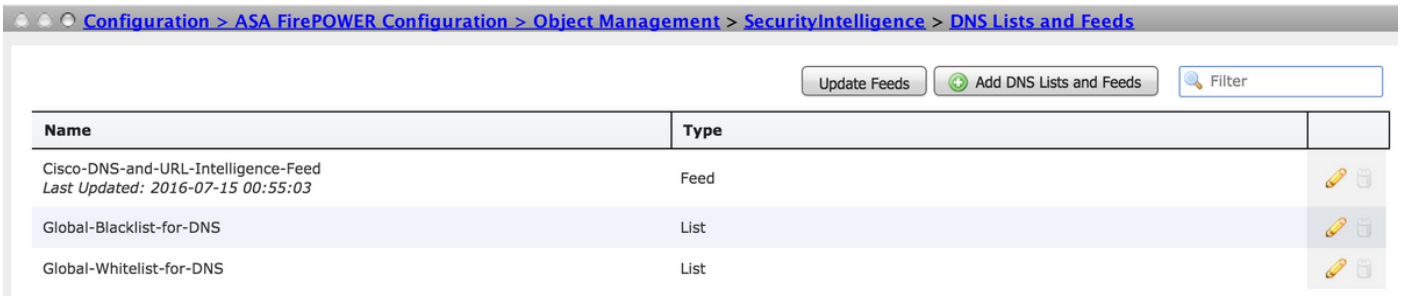
Surveillance des événements DNS Security Intelligence

Afin de voir l'intelligence de sécurité par le module Firepower, accédez à Monitoring > ASA Firepower Monitoring > Real Time Evant. Sélectionnez l'onglet Security Intelligence. Ceci affiche les événements comme le montre l'image :



Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.Afin de vous assurer que les flux Security Intelligence sont à jour, accédez à Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds et vérifiez l'heure de la dernière mise à jour du flux. Vous pouvez choisir Modifier pour définir la fréquence de mise à jour du flux.



Assurez-vous que le déploiement de la stratégie de contrôle d'accès s'est terminé correctement. Surveillez l'onglet Événement en temps réel de Security Intelligence pour voir si le trafic est bloqué ou non.

Informations connexes

- Guide de démarrage rapide du module Cisco ASA FirePOWER
- Support et documentation techniques - Cisco Systems