Détection du trafic de flux vidéo utilisant un système de FireSIGHT

Contenu

Introduction

Afin de détecter le trafic visuel de votre réseau, vous pouvez utiliser la fonctionnalité de contrôle d'accès et la caractéristique de Filtrage URL d'un système de FireSIGHT. Ce document décrit comment configurer un système de FireSIGHT à cet effet.

Conditions préalables

Conditions requises

Les instructions sur ce document exige qu'un permis de contrôle et le permis de filtre URL sont installés au centre de Gestion de FireSIGHT.

Composants utilisés

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

- Centre de Gestion de FireSIGHT
- Version de logiciel 5.2 ou plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Détecter le trafic de flux vidéo

Utilisant des filtres d'application

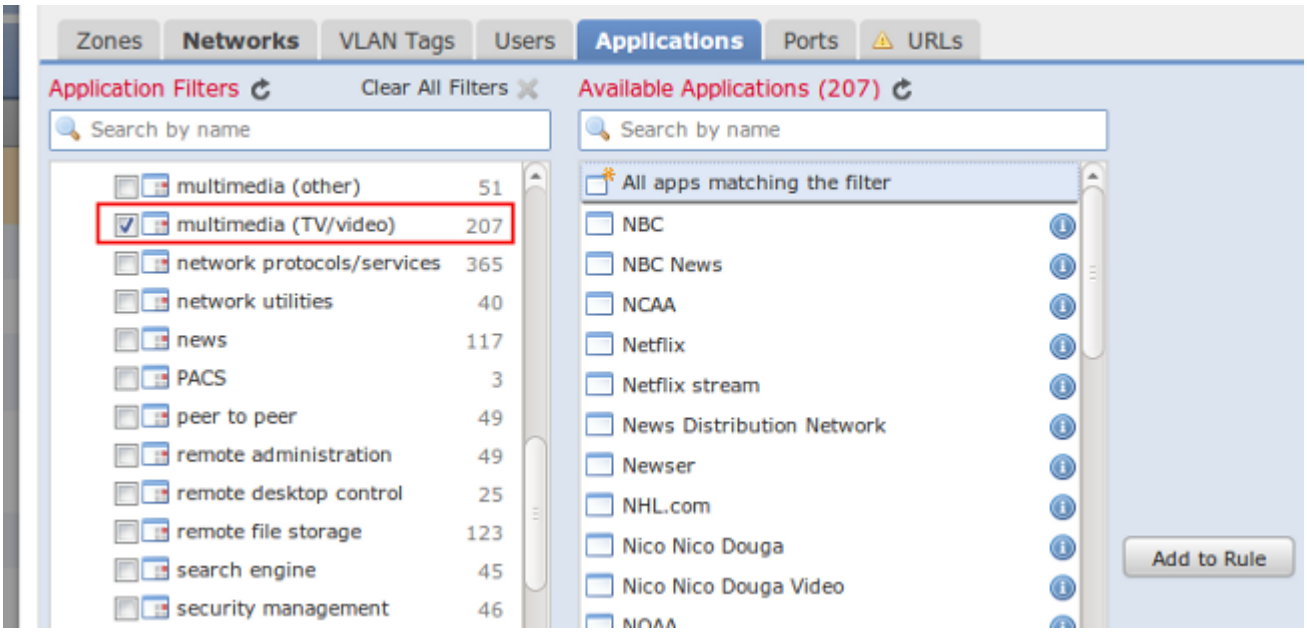
Une fonctionnalité de stratégie de contrôle d'accès te permet pour employer le type d'application comme filtre pour déterminer si le trafic est bloqué, fait confiance, ou examiné. Afin de détecter le trafic de flux vidéo utilisant des filtres d'application, suivez les étapes ci-dessous :

Étape 1 : Créez une règle de contrôle d'accès utilisant les zones, les réseaux, et l'action appropriés pour votre environnement.

Étape 2 : Sélectionnez l'onglet d'**applications**. Vous trouverez beaucoup de sélections possibles dans la section de **filtres d'application**.

Étape 3 : Faites descendre l'écran aux **filtres** section d'**application**, vous trouvera un filtre nommé les **multimédia (TV/video)**, avec plus de 200 applications disponibles. Vous pouvez sélectionner une application à la fois, ou toutes les applications. Afin de sélectionner toutes les applications dans ce filtre, sélectionnez **tous les app appariant le filtre** et cliquez sur Add **pour ordonner le** bouton.

> **Conseil** : Afin de vous aider à comprendre les applications, cliquez sur en fonction l'icône de l'*information* qui est juste de chaque application. Il décrit l'application et te fournit les risques, les types, la pertinence d'affaires, etc. de chaque application.



Étape 4 : Vous pouvez également souhaiter visualiser la catégorie de **balises** qui est sous la section de **filtres d'application**. Vous trouverez de diverses balises telles que le **vidéo de partage**, **coulant le flux**, la **vidéoconférence**, le **protocole UDP**, et le **webcam** pour toutes les autres applications que vous voudriez ajouter qui n'ont pas été répertoriés dans la catégorie des **multimédia (TV/video)**.

Étape 5 : Sauvegardez et réappliquez la stratégie de contrôle d'accès à vos périphériques gérés.

Conseil : De nouveaux types d'application sont ajoutés dans des mises à jour de la base de données de vulnérabilité (VDB). La conservation de votre courant de version VDB te permet pour détecter les ajouts les plus récents aux catégories aussi bien qu'aux applications plus anciennes.

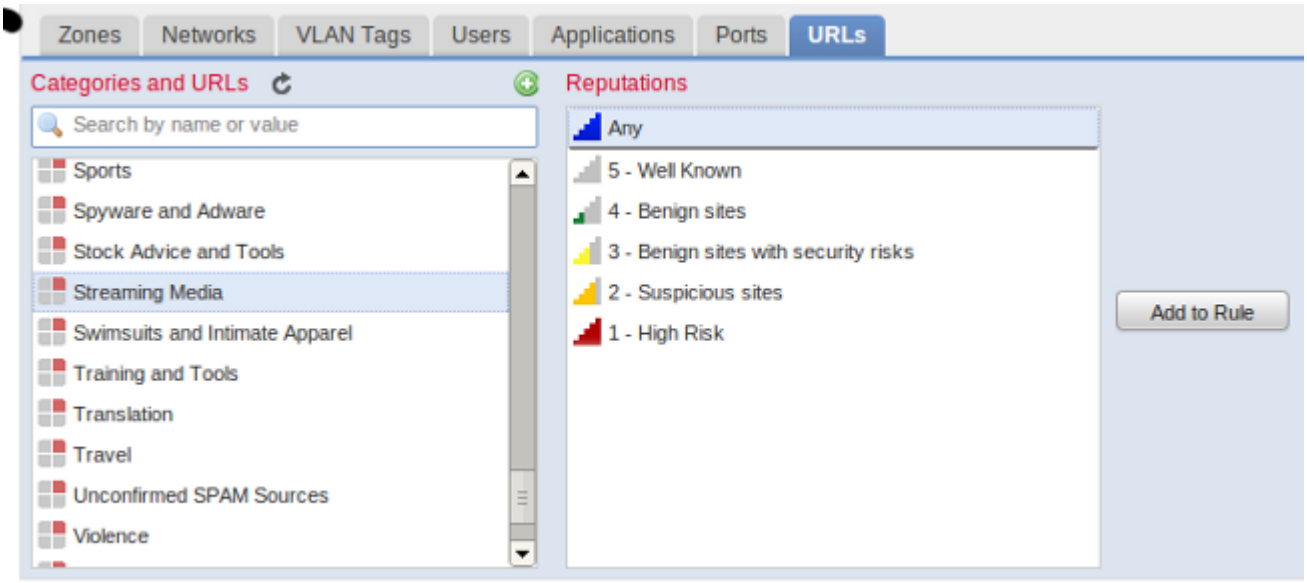
Utilisant le Filtrage URL

Vous pouvez également détecter le trafic de flux vidéo à l'aide du Filtrage URL. Pour faire cela, terminez-vous les étapes suivantes quand vous ajoutez une règle de contrôle d'accès :

Étape 1 : Sélectionnez l'onglet **URLs**.

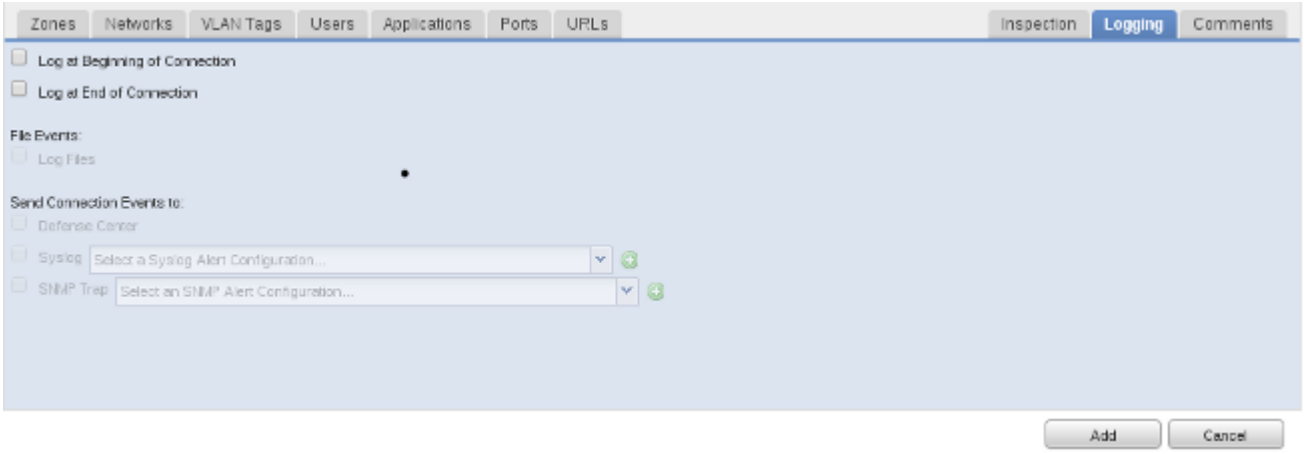
Étape 2 : Choisissez la catégorie de **streaming media**. Vous pouvez alors sélectionner le niveau de **réputation des** medias que vous êtes concerné par, de **réputé au risque fort**. Ceci te permet pour détecter le nouveau trafic de flux vidéo pendant que le nouvel URLs sont ajoutés à la base de données de Filtrage URL que vous devriez mettre à jour régulièrement.

Étape 3 : Après avoir ajouté les règles, sauvegardez la stratégie de contrôle d'accès et réappliquez-la à vos périphériques gérés.



Se connecter le trafic de flux vidéo

Une fois que vous avez configuré l'application ou des filtres URL, vous pouvez activer se connecter pour dépister ces connexions. Pour faire cela, sélectionnez l'onglet **se connectant**.



Si vous configurez une règle de contrôle d'accès de bloquer le trafic de flux vidéo, **log** choisi au **début de la connexion** pour se connecter les connexions. Si vous voulez la règle de générer les informations sur le type de flux vidéo en service sur votre réseau et la durée des connexions, **log** choisi à l'**extrémité de la connexion**.

> **Note**: Les applications d'UDP sont non connectées, ainsi les sessions d'UDP ne sont pas considérées complètes jusqu'à ce qu'une heure passe sans davantage de trafic UDP entre la source et la destination.