Fonctionnalité de filtre d'URL HTTP ASA avec Regex

Contenu

Introduction

Ce document décrit la configuration des filtres d'URL sur un dispositif de sécurité adaptatif (ASA) avec le moteur d'inspection HTTP. Cette opération est effectuée lorsque des parties de la requête HTTP sont associées à l'utilisation d'une liste de modèles regex. Vous pouvez soit bloquer des URL spécifiques, soit bloquer toutes les URL, à l'exception d'une sélection.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

> **Note**: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configuration Steps

Voici les étapes générales de configuration :

1. Identifier une courte liste de domaines qui doivent être bloqués ou autorisés
2. Créer une carte de classe regex qui correspond à tous les domaines en question
3. Créer une carte de stratégie d'inspection HTTP qui abandonne ou autorise le trafic qui correspond à ces domaines
4. Appliquer cette carte de stratégie d'inspection HTTP à une inspection HTTP dans un cadre de stratégie modulaire

Que vous teniez ou non de bloquer certains domaines et d'autoriser tous les autres, ou de bloquer tous les domaines et d'autoriser seulement quelques-uns, les étapes sont identiques, à l'exception de la création de la carte de stratégie d'inspection HTTP.

Identifier une courte liste de domaines qui doivent être bloqués ou autorisés

Pour cet exemple de configuration, ces domaines sont bloqués ou autorisés :

- cisco1.com
- cisco2.com
- cisco3.com

Configurez les modèles regex pour ces domaines :

```
regex cisco1.com "cisco1.com"regex cisco2.com "cisco2.com"regex cisco3.com "cisco3.com"
```

Créer une carte de classe regex qui correspond à tous les domaines en question

Configurez une classe regex qui correspond aux modèles regex :

```
class-map type regex match-any domain-regex-classmatch regex cisco1.commatch regex
cisco2.commatch regex cisco3.com
```

Créer une carte de stratégie d'inspection HTTP qui abandonne ou autorise le trafic qui correspond à ces domaines

Afin de comprendre à quoi ressemblerait cette configuration, choisissez la description qui correspond le mieux à l'objectif de ce filtre d'URL. La classe regex construite ci-dessus sera soit

une liste de domaines qui doivent être autorisés, soit une liste de domaines qui doivent être bloqués.

- **Autoriser tous les domaines à l'exception de ceux répertoriés**La clé de cette configuration est qu'une carte de classe est créée lorsqu'une transaction HTTP qui correspond aux domaines répertoriés est classée comme « classe de domaine bloqué ». La transaction HTTP qui correspond à cette classe est réinitialisée et fermée. Essentiellement, seule la transaction HTTP qui correspond à ces domaines est réinitialisée.
  ```
  class-map type inspect http match-all blocked-domain-class match request header host regex class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters class blocked-domain-class  reset log
  ```
- **Bloquer tous les domaines à l'exception de ceux répertoriés**La clé de cette configuration est qu'une carte de classe est créée à l'aide du mot clé « match not ». Ceci indique au pare-feu que les domaines qui ne correspondent pas à la liste des domaines doivent correspondre à la classe intitulée « allowed-domain-class ». Les transactions HTTP correspondant à cette classe seront réinitialisées et fermées. Essentiellement, toutes les transactions HTTP seront réinitialisées à moins qu'elles ne correspondent aux domaines répertoriés.
  ```
  class-map type inspect http match-all allowed-domain-class match not request header host regex class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters class allowed-domain-class  reset log
  ```

Appliquer cette carte de stratégie d'inspection HTTP à une inspection HTTP dans un cadre de stratégie modulaire

Maintenant que la carte de stratégie d'inspection HTTP est configurée comme « regex-filter-policy », appliquez cette carte de stratégie à une inspection HTTP qui existe ou à une nouvelle inspection dans Modular Policy Framework. Par exemple, ceci ajoute l'inspection à la classe « inspection_default » configurée dans « global_policy ».

```
policy-map global_policy class inspection_default  inspect http regex-filtering-policy
```

Problèmes courants

Lorsque le mappage de stratégie d'inspection HTTP et le mappage de classe HTTP sont configurés, assurez-vous que la correspondance ou la correspondance n'est pas configurée comme elle devrait l'être pour l'objectif souhaité. Il s'agit d'un mot clé simple à ignorer et qui entraîne un comportement non intentionnel. En outre, cette forme de traitement regex, tout comme tout traitement de paquets avancé, peut entraîner une augmentation de l'utilisation du processeur ASA ainsi qu'une diminution du débit. Soyez prudent lorsque de plus en plus de motifs regex sont ajoutés.