Fonctionnalité de filtre d'URL HTTP ASA avec l'expression régulière

Contenu

Introduction

Ce document décrit la configuration des filtres URL sur une appliance de sécurité adaptable (ASA) avec l'engine d'inspection de HTTP. Ceci est terminé quand des parties de la demande de HTTP sont appariées avec l'utilisation d'une liste de modèles d'expression régulière. Vous pouvez bloquer la particularité URLs ou bloquer tout l'URLs excepté une minorité.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

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.

Configurez

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.

Étapes de configuration

Ce sont les étapes de configuration générale :

1. Identifiez une liste courte de domaines qui devraient être bloqués ou permis
2. Créez un class map d'expression régulière qui apparie tous les domaines en question
3. Construisez une carte de stratégie d'inspection de HTTP qui relâche ou les autorisations trafiquent qu'apparie ces domaines
4. Appliquez cette carte de stratégie d'inspection de HTTP à une inspection de HTTP dans le cadre de stratégie modulaire

Indépendamment de si vous essayez de bloquer quelques domaines et de laisser tous les autres, ou bloquez tous les domaines et laissez seulement quelques uns, les étapes sont identiques excepté la création de la carte de stratégie d'inspection de HTTP.

Identifiez une liste courte de domaines qui devraient être bloqués ou permis

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

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

Configurez les modèles d'expression régulière pour ces domaines :

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

Créez un class map d'expression régulière qui apparie tous les domaines en question

Configurez une classe d'expression régulière qui apparie les modèles d'expression régulière :

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

Construisez une carte de stratégie d'inspection de HTTP qui relâche ou les autorisations trafiquent qu'apparie ces domaines

Afin de comprendre ce que ressemblerait à cette configuration, choisissez la description cette des ajustements le but de ce filtre URL. La classe d'expression régulière établie ci-dessus l'un ou l'autre sera une liste de domaines qui devraient être permis ou une liste de domaines qui devraient être bloqués.

- **Permettez tous les domaines excepté ceux répertoriés**La clé à cette configuration est qu'un class map est créé où une transaction de HTTP qui apparie les domaines répertoriés est classifiée en tant que « bloquer-domaine-classe ». La transaction de HTTP qui apparie cette classe est remise à l'état initial et clôturée. Essentiellement, seulement la transaction de HTTP qui apparie ces domaines est remise à l'état initial.
```
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
```
- **Bloquez tous les domaines excepté ceux répertoriés**La clé à cette configuration est qu'un class map est créé utilisant le mot clé « match not ». Ceci indique au Pare-feu que tous les domaines qui n'apparient pas la liste de domaines devraient apparier la classe intitulée « autoriser-domaine-classe ». Transactions de HTTP qui s'assortissent que la classe sera remise à l'état initial et fermée. Essentiellement, toutes les transactions de HTTP seront remises à l'état initial à moins qu'elles apparient les 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
```

Appliquez cette carte de stratégie d'inspection de HTTP à une inspection de HTTP dans le cadre de stratégie modulaire

Maintenant que la carte de stratégie d'inspection de HTTP est configurée en tant que « expression régulière-filtrer-stratégie », appliquez cette carte de stratégie à une inspection de HTTP qui existe ou à une nouvelle inspection dans le cadre de stratégie modulaire. Par exemple, ceci ajoute l'inspection à la classe de « inspection_default » configurée dans le « global_policy ».

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

Problèmes courants

Quand la carte de stratégie d'inspection de HTTP et le class map de HTTP sont configurés, assurez-vous que la correspondance ou le match not est configurée pendant qu'il devrait être pour le but désiré. C'est un mot clé simple à ignorer et des résultats dans le comportement fortuit. En outre, cette forme d'expression régulière traitant, juste comme n'importe quel traitement de paquets avancé, pourrait faire augmenter l'utilisation du processeur ASA aussi bien que débit à relâcher. Prenez soin quand de plus en plus des modèles d'expression régulière sont ajoutés.