Funcionalidade de filtro de URL do ASA HTTP com Regex

Contents

Introduction

Este documento descreve a configuração de filtros de URL em um ASA (Adaptive Security Appliance) com o mecanismo de inspeção HTTP. Isso é concluído quando partes da solicitação HTTP correspondem ao uso de uma lista de padrões regex. Você pode bloquear URLs específicos ou bloquear todos os URLs, exceto alguns selecionados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Configuration Steps

Estas são as etapas gerais de configuração:

1. Identificar uma pequena lista de domínios que devem ser bloqueados ou permitidos
2. Criar um mapa de classe regex que corresponda a todos os domínios em questão
3. Crie um mapa de política de inspeção HTTP que descarte ou permita o tráfego que corresponda a esses domínios
4. Aplicar este Mapa da Política de Inspeção HTTP a uma Inspeção HTTP na Estrutura de Política Modular

Independentemente de você tentar ou não bloquear alguns domínios e permitir todos os outros, ou bloquear todos os domínios e permitir apenas alguns, as etapas são idênticas, exceto a criação do Mapa de Políticas de Inspeção HTTP.

Identificar uma pequena lista de domínios que devem ser bloqueados ou permitidos

Para este exemplo de configuração, estes domínios são bloqueados ou permitidos:

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

Configure os padrões regex para estes domínios:

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

Criar um mapa de classe regex que corresponda a todos os domínios em questão

Configure uma classe regex que corresponda aos padrões regex:

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

Crie um mapa de política de inspeção HTTP que descarte ou permita o tráfego que corresponda a esses domínios

Para entender como seria essa configuração, escolha a descrição mais adequada ao objetivo deste filtro de URL. A classe regex criada acima será uma lista de domínios que devem ser

permitidos ou uma lista de domínios que devem ser bloqueados.

- **Permitir todos os domínios, exceto os listados**A chave dessa configuração é que um mapa de classe é criado onde uma transação HTTP que corresponda aos domínios listados é classificada como "classe de domínio bloqueado". A transação HTTP que corresponde a esta classe é redefinida e fechada. Essencialmente, somente a transação HTTP que corresponde a esses domínios é redefinida.
```
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
```
- **Bloquear todos os domínios, exceto os listados**A chave para essa configuração é que um mapa de classe é criado usando a palavra-chave "match not". Isso informa ao firewall que qualquer domínio que não corresponda à lista de domínios deve corresponder à classe denominada "classe de domínio permitido". As transações HTTP correspondentes a essa classe serão redefinidas e fechadas. Essencialmente, todas as transações HTTP serão redefinidas, a menos que correspondam aos domínios listados.
```
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
```

Aplicar este Mapa da Política de Inspeção HTTP a uma Inspeção HTTP na Estrutura de Política Modular

Agora que o Mapa da política de inspeção HTTP está configurado como "política de filtragem regex", aplique este mapa de política a uma inspeção HTTP que existe ou a uma nova inspeção na Estrutura de política modular. Por exemplo, isso adiciona a inspeção à classe "inspection_default" configurada em "global_policy".

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

Problemas comuns

Quando o mapa de política de inspeção HTTP e o mapa de classe HTTP estiverem configurados, certifique-se de que a correspondência ou não esteja configurada como deveria ser para o objetivo desejado. Essa é uma palavra-chave simples a ser ignorada e resulta em comportamento não intencional. Além disso, essa forma de processamento de regex, assim como qualquer processamento de pacote avançado, pode fazer com que a utilização da CPU ASA aumente, assim como a produtividade diminua. Tenha cuidado ao adicionar cada vez mais padrões regex.