Funcionalidade do filtro do URL DO HTTP ASA com Regex

Índice

Introdução

Este documento descreve a configuração de filtros URL em uma ferramenta de segurança adaptável (ASA) com o motor da inspeção HTTP. Isto é terminado quando as partes do pedido do HTTP são combinadas com o uso de uma lista de testes padrões do regex. Você pode obstruir URL específicas ou obstruir todas as URL à exceção de um seleto poucos.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

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.

Passos de configuração

Estas são as etapas da configuração geral:

1. Identifique uma pequena lista dos domínios que devem ser obstruídos ou permitido
2. Crie um mapa da classe do regex que combine todos os domínios na pergunta
3. Construa um mapa de política da inspeção HTTP que deixa cair ou permita o tráfego que combina estes domínios
4. Aplique este mapa de política da inspeção HTTP a uma inspeção HTTP na estrutura de política modular

Apesar de mesmo se você tenta obstruir alguns domínios e permitir todos os outro, ou obstrua todos os domínios e permita somente alguns, as etapas são idêntico à exceção da criação do mapa de política da inspeção HTTP.

Identifique uma pequena lista dos domínios que devem ser obstruídos ou permitido

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

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

Configurar os testes padrões do regex para estes domínios:

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

Crie um mapa da classe do regex que combine todos os domínios na pergunta

Configurar uma classe do regex que combine os testes padrões do regex:

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

Construa um mapa de política da inspeção HTTP que deixa cair ou permita o tráfego que combina estes domínios

A fim compreender o que esta configuração olharia como, escolha a descrição que esse melhor cabe o objetivo deste filtro URL. A classe do regex construída acima qualquer um será uma lista de domínios que devem ser permitidos ou uma lista de domínios que devem ser obstruídos.

- **Permita todos os domínios à exceção de esses alistados**A chave a esta configuração é que um mapa da classe está criado onde uma transação HTTP que combine os domínios alistados é classificada como a “obstruir-domínio-classe”. A transação HTTP que combina esta classe é restaurada e fechada. Essencialmente, somente a transação HTTP que combina estes domínios é restaurada.
```
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
```
- **Obstrua todos os domínios à exceção de esses alistados**A chave a esta configuração é que um mapa da classe está criado usando a palavra-chave “fósforo não”. Isto diz ao Firewall que todos os domínios que não combinarem a lista de domínios devem combinar a classe intitulada “permitir-domínio-classe”. As transações HTTP que combinam essa classe serão restauradas e fechadas. Essencialmente, todas as transações HTTP serão restauradas a menos que combinarem os domínios alistados.
```
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
```

Aplique este mapa de política da inspeção HTTP a uma inspeção HTTP na estrutura de política modular

Agora que o mapa de política da inspeção HTTP é configurado como a “regex-filtrar-política”, aplique este mapa de política a uma inspeção HTTP que exista ou a uma inspeção nova na estrutura de política modular. Por exemplo, isto adiciona a inspeção à classe do “inspection_default” configurada no “global_policy”.

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

Problemas comuns

Quando o mapa de política da inspeção HTTP e o mapa da classe HTTP são configurados, assegure-se de que o fósforo ou o fósforo não estejam configurados enquanto deve ser para o objetivo desejado. Este é uma palavra-chave simples a saltar e resultados no comportamento sem intenção. Também, este formulário do regex que processa, apenas como todo o pacote avançado que processa, pôde fazer com que a utilização CPU ASA aumente assim como taxa de transferência a deixar cair. Use o cuidado quando os testes padrões do regex são adicionados cada vez mais.