

Funciones del filtro ASA HTTP URL con Regex

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Pasos de configuración](#)

[Identifique una breve lista de dominios que deban ser bloqueados o ser permitidos](#)

[Cree una correspondencia de la clase del regex que haga juego todos los dominios en la pregunta](#)

[Construya una correspondencia de políticas del examen HTTP que caiga o permite el tráfico que hace juego estos dominios](#)

[Aplique esta correspondencia de políticas del examen HTTP a un examen HTTP en el Marco de políticas modular](#)

[Problemas comunes](#)

Introducción

Este documento describe la configuración de los filtros URL en un dispositivo de seguridad adaptante (ASA) con el motor del examen HTTP. Se completa esto cuando corresponden con a las partes del pedido de HTTP con el uso de una lista de modelos del regex. Usted puede bloquear los URL específicos o bloquear todos los URL a excepción una minoría.

Prerrequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Utilice la herramienta [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos utilizados en esta sección.

Pasos de configuración

Éstos son los pasos de la Configuración general:

1. Identifique una breve lista de dominios que deban ser bloqueados o ser permitidos
2. Cree una correspondencia de la clase del regex que haga juego todos los dominios en la pregunta
3. Construya una correspondencia de políticas del examen HTTP que caiga o permite el tráfico que hace juego estos dominios
4. Aplique esta correspondencia de políticas del examen HTTP a un examen HTTP en el Marco de políticas modular

Sin importar independientemente de si usted intenta bloquear algunos dominios y permitir todos los demás, o bloquee todos los dominios y permita solamente algunos, los pasos son idéntico a excepción de la creación de la correspondencia de políticas del examen HTTP.

Identifique una breve lista de dominios que deban ser bloqueados o ser permitidos

Para este ejemplo de configuración, se bloquean o se permiten estos dominios:

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

Configure los modelos del regex para estos dominios:

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

Cree una correspondencia de la clase del regex que haga juego todos los dominios en la pregunta

Configure una clase del regex que haga juego los modelos del regex:

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

Construya una correspondencia de políticas del examen HTTP que caiga o permite el tráfico que hace juego estos dominios

Para entender lo que parecería esta configuración, elija la descripción esa los mejores ajustes la meta de este filtro URL. La clase del regex construida arriba cualquiera será una lista de dominios que deban ser permitidos o una lista de dominios que deban ser bloqueados.

- **Permita todos los dominios a excepción de los que está enumerados**La clave a esta configuración es que una correspondencia de la clase está creada donde una transacción HTTP que hace juego los dominios enumerados se clasifica como “bloquear-dominio-clase”. Se reajusta y se cierra la transacción HTTP que hace juego esta clase. Esencialmente, solamente se reajusta la transacción HTTP que hace juego estos dominios.

```
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
```

- **Bloquee todos los dominios a excepción de los que está enumerados**La clave a esta configuración es que una correspondencia de la clase está creada usando la palabra clave “coincidencia no”. Esto dice a Firewall que cualquier dominio que no haga juego la lista de dominios debe hacer juego la clase titulada “permitir-dominio-clase”. Las transacciones HTTP que hacen juego esa clase serán reajustadas y cerradas. Esencialmente, todas las transacciones HTTP serán reajustadas a menos que hagan juego los dominios enumerados.

```
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 esta correspondencia de políticas del examen HTTP a un examen HTTP en el Marco de políticas modular

Ahora que la correspondencia de políticas del examen HTTP se configura como “regex-filtrar-directiva”, aplique esta correspondencia de políticas a un examen HTTP que exista o a un nuevo examen en el Marco de políticas modular. Por ejemplo, esto agrega el examen a la clase del “inspection_default” configurada en el “global_policy”.

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

Problemas comunes

Cuando se configuran la correspondencia de políticas del examen HTTP y la correspondencia de la clase HTTP, asegúrese que esa coincidencia o coincidencia no esté configurado mientras que debe estar para la meta deseada. Éste es una palabra clave simple a saltar y resultados en el comportamiento involuntario. También, esta forma de regex que procesaba, apenas como cualquier paquete avanzado que procesaba, pudo hacer la utilización de la CPU ASA aumentar así como producción a caer. Cuide cuando los modelos del regex se agregan cada vez más.