Funcionalidad de filtrado de URL HTTP ASA con Regex

Contenido

Introducción

Este documento describe la configuración de los filtros de URL en un dispositivo de seguridad adaptable (ASA) con el motor de inspección HTTP. Esto se completa cuando partes de la solicitud HTTP coinciden con el uso de una lista de patrones de regex. Puede bloquear direcciones URL específicas o bloquear todas las direcciones URL, excepto algunas seleccionadas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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

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

> **Nota:** Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Configuration Steps

Estos son los pasos generales de configuración:

1. Identificar una lista breve de dominios que se deben bloquear o permitir
2. Cree un mapa de clase regex que coincida con todos los dominios en cuestión
3. Cree un mapa de política de inspección HTTP que descarte o permita el tráfico que coincida con estos dominios
4. Aplicar este mapa de política de inspección HTTP a una inspección HTTP en el marco de políticas modular

Independientemente de si intenta o no bloquear algunos dominios y permitir todos los demás, o bloquear todos los dominios y permitir sólo unos pocos, los pasos son idénticos excepto para la creación del mapa de política de inspección HTTP.

Identificar una lista breve de dominios que se deben bloquear o permitir

Para este ejemplo de configuración, estos dominios están bloqueados o permitidos:

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

Configure los patrones regex para estos dominios:

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

Cree un mapa de clase regex que coincida con todos los dominios en cuestión

Configure una clase regex que coincida con los patrones regex:

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

Cree un mapa de política de inspección HTTP que descarte o permita el tráfico que coincida con estos dominios

Para entender cómo sería esta configuración, elija la descripción que mejor se adapte al objetivo de este filtro de URL. La clase regex generada arriba será una lista de dominios que se deben permitir o una lista de dominios que se deben bloquear.

- **Permitir todos los dominios excepto los enumerados**La clave de esta configuración es que se crea un mapa de clase donde una transacción HTTP que coincide con los dominios enumerados se clasifica como "clase de dominio bloqueado". La transacción HTTP que coincide con esta clase se restablece y se cierra. Básicamente, sólo se restablece la transacción HTTP que coincide con 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
  ```
- **Bloquear todos los dominios excepto los enumerados**La clave para esta configuración es que se crea un mapa de clase utilizando la palabra clave "match not". Esto indica al firewall que cualquier dominio que no coincida con la lista de dominios debe coincidir con la clase titulada "allowed-domain-class". Las transacciones HTTP que coincidan con esa clase se restablecerán y cerrarán. Básicamente, se restablecerán todas las transacciones HTTP a menos que coincidan con 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
  ```

Aplicar este mapa de política de inspección HTTP a una inspección HTTP en el marco de políticas modular

Ahora que el mapa de política de inspección HTTP está configurado como "regex-filter-policy", aplique este mapa de política a una inspección HTTP existente o a una nueva inspección en el marco de política modular. Por ejemplo, esto agrega la inspección a la clase "inspection_default" configurada en "global_policy".

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

Problemas comunes

Cuando se configuran el mapa de política de inspección HTTP y el mapa de clase HTTP, asegúrese de que la coincidencia o coincidencia no esté configurada como debería estar para el objetivo deseado. Se trata de una palabra clave sencilla que se debe saltar y que da como resultado un comportamiento no deseado. Además, esta forma de procesamiento regex, al igual que cualquier procesamiento avanzado de paquetes, podría hacer que la utilización de la CPU de ASA aumentara, así como el rendimiento bajara. Tenga cuidado cuando se agregan más y más patrones de regex.