ASA HTTP URL-filterfunctie met Regex

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Configureren](#)
[Configuratiestappen](#)
[Identificeer een korte lijst van domeinen die geblokkeerd of toegestaan moeten worden](#)
[Maak een regex class-kaart die overeenkomt met alle betrokken domeinen](#)
[Creëer een HTTP Inspection Policy Map die verkeer vermindert of toestaat dat deze domeinen aansluit](#)
[Pas deze HTTP Inspection Policy Map op een HTTP-inspectie toe in het modulaire beleidskader](#)
[Gemeenschappelijke kwesties](#)

Inleiding

Dit document beschrijft de configuratie van URL-filters op een adaptieve security applicatie (ASA) met de HTTP-inspectiemodule. Dit is voltooid wanneer delen van de HTTP-aanvraag zijn afgestemd op het gebruik van een lijst met regex-patronen. U kunt specifieke URL's blokkeren of alle URL's blokkeren, behalve een paar geselecteerde URL's.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

> Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Configuratiestappen

Dit zijn de algemene configuratiestappen:

1. Identificeer een korte lijst van domeinen die geblokkeerd of toegestaan moeten worden
2. Maak een regex class-kaart die overeenkomt met alle betrokken domeinen
3. Creëer een HTTP Inspection Policy Map die verkeer vermindert of toestaat dat deze domeinen aansluit
4. Pas deze HTTP Inspection Policy Map op een HTTP-inspectie toe in het modulaire beleidskader

Ongeacht of u probeert om bepaalde domeinen te blokkeren en alle andere domeinen toe te staan, of alle domeinen te blokkeren en er slechts een paar toe te staan, zijn de stappen identiek behalve de creëren van de HTTP Inspection Policy Map.

Identificeer een korte lijst van domeinen die geblokkeerd of toegestaan moeten worden

Voor dit configuratievoorbeeld zijn deze domeinen geblokkeerd of toegestaan:

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

Configureer de regex patronen voor deze domeinen:

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

Maak een regex class-kaart die overeenkomt met alle betrokken domeinen

Configuratie van een regex klasse die de regex patronen aanpast:

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

Creëer een HTTP Inspection Policy Map die verkeer vermindert of toestaat dat deze domeinen aansluit

Om te begrijpen hoe deze configuratie eruit zou zien, kiest u de beschrijving die het best past bij het doel van dit URL filter. De hierboven gebouwde regex-klasse zal een lijst van domeinen zijn

die toegestaan moeten worden of een lijst van domeinen die geblokkeerd moeten worden.

- **Laat alle domeinen behalve de genoemde toe**De sleutel tot deze configuratie is dat een class map wordt gecreëerd waarin een HTTP-transactie die overeenkomt met de genoemde domeinen wordt geclassificeerd als "geblokkeerd-domein-klasse". De HTTP-transactie die met deze klasse overeenkomt wordt opnieuw ingesteld en gesloten. In wezen wordt alleen de HTTP-transactie die met deze domeinen overeenkomt gereset.
```
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
```
- **Alle domeinen behalve de genoemde blokkeren**De sleutel tot deze configuratie is dat een class map gecreëerd wordt met het sleutelwoord "match niet". Dit vertelt de firewall dat alle domeinen die niet de lijst van domeinen beantwoorden de klasse "toegelaten-domein-klasse" zouden moeten evenaren. HTTP-transacties die overeenkomen met die klasse worden opnieuw ingesteld en gesloten. In wezen zullen alle HTTP-transacties worden gereset, tenzij ze overeenkomen met de vermelde domeinen.
```
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
```

Pas deze HTTP Inspection Policy Map op een HTTP-inspectie toe in het modulaire beleidskader

Nu de HTTP Inspection Policy Map is geconfigureerd als "regex-filtreerbeleid", moet u deze beleidskaart toepassen op een HTTP-inspectie die bestaat of een nieuwe inspectie in modulair beleidskader. Bijvoorbeeld, dit voegt de inspectie toe aan de "inspection_default" klasse gevormd in "global_policy".

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

Gemeenschappelijke kwesties

Wanneer de HTTP Inspection Policy Map en de HTTP-klassekaart zijn geconfigureerd, zorg er dan voor dat de match of match niet zo zijn geconfigureerd als dat voor het gewenste doel is. Dit is een simpel sleutelwoord om over te slaan en leidt tot onbedoeld gedrag. Ook kan deze vorm van regex-verwerking, net zoals elke geavanceerde pakketverwerking, het gebruik van ASA CPU's doen toenemen en de doorvoersnelheid naar een lagere waarde doen dalen. Gebruik voorzichtigheid wanneer er meer en meer regex patronen worden toegevoegd.