Funzionalità del filtro URL HTTP ASA con Regex

Sommario

Introduzione

In questo documento viene descritta la configurazione dei filtri URL su un'appliance ASA (Adaptive Security Appliance) con il motore di ispezione HTTP. Questa operazione viene completata quando parti della richiesta HTTP vengono associate all'utilizzo di una lista di modelli regex. È possibile bloccare URL specifici o bloccare tutti gli URL ad eccezione di alcuni.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Procedura di configurazione

Di seguito vengono riportati i passi della configurazione generale:

1. Identificare un breve elenco di domini da bloccare o consentire
2. Creare una mappa della classe regex che corrisponda a tutti i domini in questione
3. Crea una mappa dei criteri di ispezione HTTP che consente di eliminare o autorizzare il traffico corrispondente a questi domini
4. Applica questa mappa dei criteri di ispezione HTTP a un'ispezione HTTP in Modular Policy Framework

Indipendentemente dal fatto che si tenti o meno di bloccare alcuni domini e di autorizzare tutti gli altri o di bloccare tutti i domini e consentirne solo alcuni, i passaggi sono identici tranne che per la creazione della mappa dei criteri di ispezione HTTP.

Identificare un breve elenco di domini da bloccare o consentire

Per questo esempio di configurazione, questi domini sono bloccati o consentiti:

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

Configurare i modelli regex per questi domini:

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

Creare una mappa della classe regex che corrisponda a tutti i domini in questione

Configurare una classe regex che corrisponda ai modelli regex:

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

Crea una mappa dei criteri di ispezione HTTP che consente di eliminare o autorizzare il traffico corrispondente a questi domini

Per comprendere l'aspetto della configurazione, scegliere la descrizione che meglio si adatta all'obiettivo del filtro URL. La classe regex generata in precedenza sarà un elenco di domini da

consentire o un elenco di domini da bloccare.

- **Consenti tutti i domini tranne quelli elencati**La chiave di questa configurazione è la creazione di una mappa di classe in cui una transazione HTTP corrispondente ai domini elencati viene classificata come "block-domain-class". La transazione HTTP corrispondente a questa classe viene reimpostata e chiusa. In pratica, viene reimpostata solo la transazione HTTP corrispondente a questi domini.
```
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
```
- **Blocca tutti i domini ad eccezione di quelli elencati**La chiave di questa configurazione è che una mappa di classe viene creata usando la parola chiave "match not". Ciò indica al firewall che i domini che non corrispondono all'elenco di domini devono corrispondere alla classe denominata "allowed-domain-class". Le transazioni HTTP corrispondenti a tale classe verranno reimpostate e chiuse. In pratica, tutte le transazioni HTTP verranno reimpostate a meno che non corrispondano ai domini elencati.
```
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
```

Applica questa mappa dei criteri di ispezione HTTP a un'ispezione HTTP in Modular Policy Framework

Ora che la mappa dei criteri di ispezione HTTP è configurata come "regex-filtro-policy", applicare questa mappa dei criteri a un'ispezione HTTP esistente o a una nuova ispezione in Modular Policy Framework. Ad esempio, l'ispezione viene aggiunta alla classe "selection_default" configurata in "global_policy".

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

Problemi comuni

Quando la mappa dei criteri di ispezione HTTP e la mappa delle classi HTTP sono configurate, assicurarsi che non sia configurato alcun abbinamento o abbinamento come dovrebbe essere per l'obiettivo desiderato. Si tratta di una semplice parola chiave da ignorare che determina un comportamento non previsto. Inoltre, questa forma di elaborazione regex, come qualsiasi elaborazione avanzata dei pacchetti, potrebbe causare un aumento dell'utilizzo della CPU dell'ASA e una riduzione della velocità di trasmissione. Fate attenzione quando aggiungete sempre più modelli regex.