Informazioni su Protezione DNS in Secure Firewall 7.7.0

Sommario

Introduzione

In questo documento viene descritta la funzionalità DNS Guard di Secure Firewall 7.7.0, con particolare attenzione alla funzionalità e alla risoluzione dei problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni sul protocollo DNS e sulle sessioni UDP
- Familiarità con Snort 3 e la gestione delle sessioni

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall Threat Defense (FTD) versione 7.7.0
- Firepower Management Center (FMC) versione 7.7.0

- Snort versione 3

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.

Premesse

Il DNS è un protocollo basato su richiesta-risposta UDP con sessioni di breve durata. A differenza di Lina, le sessioni DNS in Snort 3 non vengono cancellate immediatamente dopo la risposta DNS. Le sessioni DNS vengono invece eliminate in base a un timeout di flusso di 120 secondi o più. Ciò comporta un accumulo di sessioni non necessario, che potrebbe altrimenti essere utilizzato per altre connessioni TCP o UDP.

Confronto con la release precedente

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		• DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

Nuova funzionalità in 7.7

Nuove caratteristiche

- Questa funzionalità "Protezione DNS" cancella il flusso UDP immediatamente dopo la ricezione e l'ispezione del pacchetto di risposta DNS.
- Si tratta di un miglioramento specifico del protocollo rispetto alla progettazione e all'architettura correnti di Snort 3.

Nozioni di base: Piattaforme supportate, Licenze

Piattaforme e manager FTD

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

Piattaforme supportate

Altri aspetti del supporto

FTD	
Licenses Required	Essentials, URL, Threat, Malware
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

Licenze e compatibilità

Problema

Nelle versioni precedenti, in particolare Secure Firewall 7.6 e versioni successive, la sessione DNS rimane un flusso Snort 3 non aggiornato fino a quando non viene eliminato dal timeout UDP. Ciò causa problemi di gestione delle sessioni e potrebbe portare a un utilizzo inefficiente delle risorse, poiché le sessioni DNS si accumulano inutilmente.

Passi per ricreare il problema

Per osservare il problema, eseguire il comando Lina per controllare le connessioni DNS attive dal lato Lina:

```
show conn detail
```

In Secure Firewall 7.6 e versioni successive, le sessioni DNS rimangono attive fino al timeout UDP, con conseguente inefficienza delle risorse.

Soluzione

La funzionalità Protezione DNS di Secure Firewall 7.7.0 risolve questo problema cancellando immediatamente il flusso UDP dopo la ricezione e l'ispezione del pacchetto di risposta DNS. Questo miglioramento specifico del protocollo garantisce che le sessioni DNS in Snort 3 vengano rilasciate immediatamente, impedendo l'accumulo di sessioni non necessarie e migliorando l'efficienza delle risorse.

Panoramica delle funzionalità

La funzionalità Protezione DNS cancella il flusso UDP immediatamente dopo la ricezione e l'ispezione del pacchetto di risposta DNS. Non è necessario attendere il timeout di UDP per il flusso dello snort.

- Quando il traffico DNS sulla scatola è sufficiente, questa funzione riduce il numero di flussi attivi a causa della tempestiva pulizia dei flussi Snort corrispondenti.
- È possibile gestire un numero maggiore di connessioni TCP/UDP senza eliminare le connessioni attive, il che migliora l'efficacia complessiva della confezione.

Risoluzione dei problemi

Per verificare la funzionalità della funzionalità Protezione DNS, utilizzare il comando Lina per assicurarsi che le sessioni UDP vengano rilasciate alla ricezione di una risposta DNS:

<#root>

>

show snort counters | begin stream_udp

Output di esempio senza la funzione di protezione DNS:

```
stream_udp sessions: 755
 max: 12
created: 755
released: 0
total_bytes: 124821
```

<#root>

>

```
show snort counters | begin stream_udp
```

Output di esempio con la funzione di protezione DNS:

```
stream_udp sessions: 899
max: 14
created: 899
released: 899
total_bytes: 135671
```

Gli output indicano che tutte le sessioni create vengono rilasciate in tempo utile, a conferma del corretto funzionamento della funzionalità Protezione DNS.

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).