Rileva flusso elefante nei dispositivi Firepower

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati
- Premesse

Metodi

- 1. Uso del CCP
- 2. Uso della CLI
- 3. Utilizzo di NetFlow
- 4. Monitoraggio continuo e adeguamento

Informazioni correlate

Introduzione

Questo documento descrive come eseguire il rilevamento del flusso di elefante in un ambiente Cisco Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- NetFlow

Componenti usati

Le informazioni di questo documento si basano su un CCP con software versione 7.1 o successive. 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 rilevamento del flusso di elefante in Cisco Firepower è fondamentale per identificare e gestire flussi di grandi dimensioni e di lunga durata che possono consumare notevoli risorse di rete e influire sulle prestazioni. I flussi di elefante possono verificarsi in applicazioni con un elevato

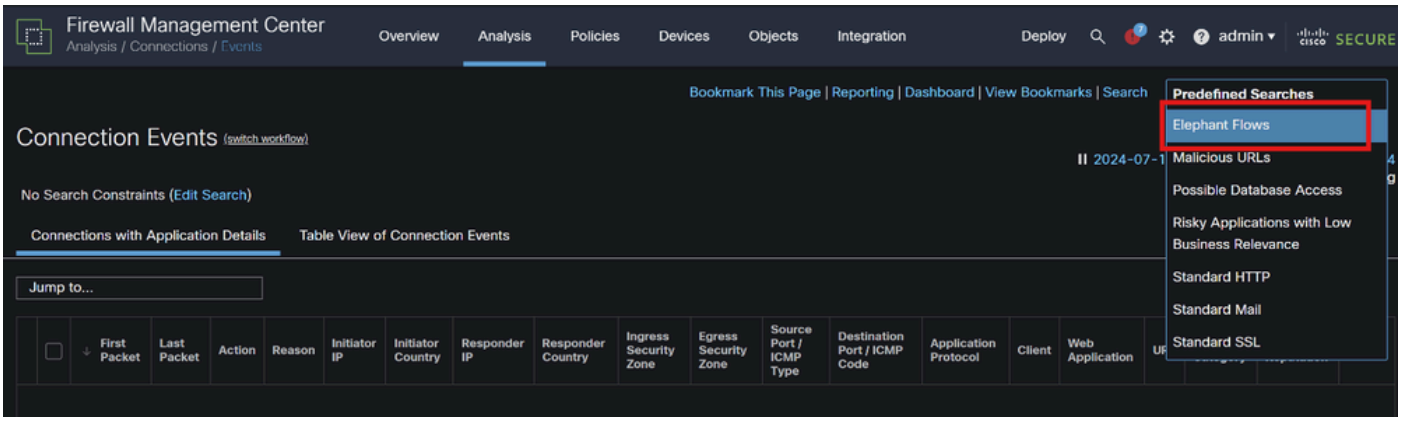
volume di dati, come lo streaming video, i trasferimenti di file di grandi dimensioni e la replica di database. È possibile identificare questa condizione tramite i metodi seguenti:

Metodi

1. Uso del CCP

Il rilevamento del flusso di elefante è stato introdotto nella versione 7.1. La versione 7.2 permette una personalizzazione più semplice e l'opzione di bypassare o anche limitare i flussi di elefante. Intelligent Application Bypass (IAB) è deprecato dalla versione 7.2.0 in poi per i dispositivi Snort 3.

Il rilevamento del flusso di elefante può essere eseguito in Analisi > Connessioni > Eventi > Ricerche predefinite > Flussi di elefante.



Eventi connessione

In questo documento viene illustrato come configurare il flusso di elefante nei criteri di controllo di accesso

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html#task_sxp_h2d_jsb

2. Uso della CLI

a. Il picking della CPU dell'istanza snort può anche indicare che la rete è in contatto con il flusso di elefante che può essere identificato usando il seguente comando:

show asp inspect-dp snort

Di seguito è riportato un esempio per l'output del comando.

> show asp inspect-dp snort

ID ID ID informazioni stato istanza SNORT Inspect

Sintassi Cpu Conns Segs/Pkts Status Tot (utente) | sys

— — — —

0 16450 8% (7%| 0%) 2,2 K 0 PRONTO

1 16453 9% (8%| 0%) 2,2 K 0 PRONTO

2 16451 6% (5%| 1%) 2,3 K 0 READY

3 16454 5% (5%| 0%) 2,2 K 1 PRONTO

4 16456 6% (6%| 0%) 2,3 K 0 PRONTO

5 16457 6% (6%| 0%) 2,3 K 0 PRONTO

6 16458 6% (5%| 0%) 2,2 K 1 PRONTO

7 16459 4% (4%| 0%) 2,3 K 0 PRONTO

8 16452 9% (8%| 1%) 2,2 K 0 READY

9 16455 100% (100%| 0%) 2,2 K 5 READY <<<< Utilizzo elevato della CPU

10 16460 7% (6%| 0%) 2,2 K 0 PRONTO

— — — —

Riepilogo 15% (14%| 0%) 24,6 K 7

b. Inoltre, l'output del comando "top" dalla modalità root può anche aiutare a controllare qualsiasi istanza Snort che diventa alta.

c. Esportare i dettagli della connessione utilizzando questo comando per verificare la presenza di traffico superiore che attraversa il firewall.

show asp inspect-dp snort

mostra dettagli conn | reindirizzare il disco0:/con-detail.txt

Il file si trova in "/mnt/disk0" dalla modalità Linux. Copiare lo stesso in **/ngfw/var/common** per scaricarlo da FMC.

cp

/mnt/disk0/<nome file> /ngfw/var/common/

Di seguito è riportato un esempio per l'output dei dettagli di connessione.

UDP inside: 10.x.x.x/137 inside: 10.x.x.43/137, flag - N1, idle 0s, **uptime 6D2h**, timeout 2m0s, **byte 123131166926** <<<< **123 GB e uptime sembra essere di 6 giorni 2 ore**

ID chiave di ricerca connessione: 2255619827

UDP inside: 10.x.x.255/137 inside: 10.x.x.42/137, flag - N1, idle 0s, uptime 7D5h, timeout 2m0s, byte 11633898274

ID chiave di ricerca connessione: 1522768243

UDP inside: 10.x.x.255/137 inside: 10.x.x.39/137, flag - N1, idle 0s, uptime 8D1h, timeout 2m0s, byte 60930791876

ID chiave di ricerca connessione: 1208773687

UDP inside: 10.x.x.255/137 inside: 10.x.x0.34/137, flag - N1, idle 0s, uptime 9D5h, timeout 2m0s, byte 59310023420

ID chiave di ricerca connessione: 597774515

3. Utilizzo di NetFlow

I flussi di elefante sono flussi di traffico con elevati volumi che possono influire sulle prestazioni della rete. Il rilevamento di questi flussi implica il monitoraggio del traffico di rete per identificare modelli che indicano flussi persistenti di grandi dimensioni. Cisco Firepower fornisce strumenti e funzionalità per rilevare e analizzare il traffico di rete, inclusi i flussi di elefanti. Lo strumento NetFlow aiuta a raccogliere le informazioni sul traffico IP per il monitoraggio.

In questo documento viene illustrato il processo dettagliato per la configurazione dei criteri NetFlow in FMC

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221612-htz-01-2024-configure-netflow-in-fmc.html

Utilizzare un raccoglitore e un analizzatore NetFlow (ad esempio, Cisco Stealthwatch, SolarWinds o qualsiasi altro strumento di analisi NetFlow) per analizzare i dati raccolti. Una volta identificati i flussi di elefanti, è possibile adottare delle misure per mitigarne l'impatto:

- Traffic Shaping e QoS: implementare policy QoS (Quality of Service) per assegnare le priorità al traffico e limitare la larghezza di banda dei flussi di elefanti.
- Criteri di controllo di accesso: creare criteri di controllo di accesso per gestire e limitare i flussi di elefante.
- Segmentazione: utilizzare la segmentazione della rete per isolare i flussi di grandi volumi e ridurre al minimo l'impatto sul resto della rete.
- Bilanciamento del carico: implementare il bilanciamento del carico per distribuire il traffico in modo più uniforme tra le risorse di rete.

4. Monitoraggio continuo e adeguamento

Monitoraggio regolare del traffico di rete per rilevare nuovi flussi di elefante e modificare le policy e le configurazioni in base alle esigenze.

Questo processo consente di rilevare e gestire in modo efficace i flussi di elefante nell'implementazione di Cisco Firepower, garantendo migliori prestazioni di rete e un migliore utilizzo delle risorse.

Informazioni correlate

Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.2

Configurare NetFlow in FMC

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).