Configurare AppID Early Packet Detection in Secure Firewall Threat Defense 7.4

Sommario

Introduzione

In questo documento viene descritto come configurare AppID Early Packet Detection in Cisco Secure Firewall 7.4.

Premessa - Problema (requisiti del cliente)

- Il rilevamento delle applicazioni tramite Deep Packet Inspection può richiedere più di un pacchetto per identificare il traffico.
- Talvolta, se si conosce l'indirizzo IP e/o la porta di un server applicazioni, è possibile evitare di ispezionare pacchetti aggiuntivi.

Novità

- È stata creata una nuova API LUA AppID basata su Snort che consente di mappare un indirizzo IP, una porta e un protocollo ai rispettivi:
  - protocollo applicativo (service appid),
  - Applicazione client (appid client) e
  - Applicazione Web (payload applicato).
- È possibile creare rilevatori di applicazioni personalizzati in FMC utilizzando questa API per il rilevamento delle applicazioni.
- Una volta attivato questo rilevatore, questa nuova API ci permetterebbe di identificare le applicazioni sul primo pacchetto di una sessione.

Panoramica delle funzionalità

- L'API è identificata come:
  - **addHostFirstPktApp** (protocol_appId, client_appId, payload_appId, indirizzo IP, porta, protocollo, respect)

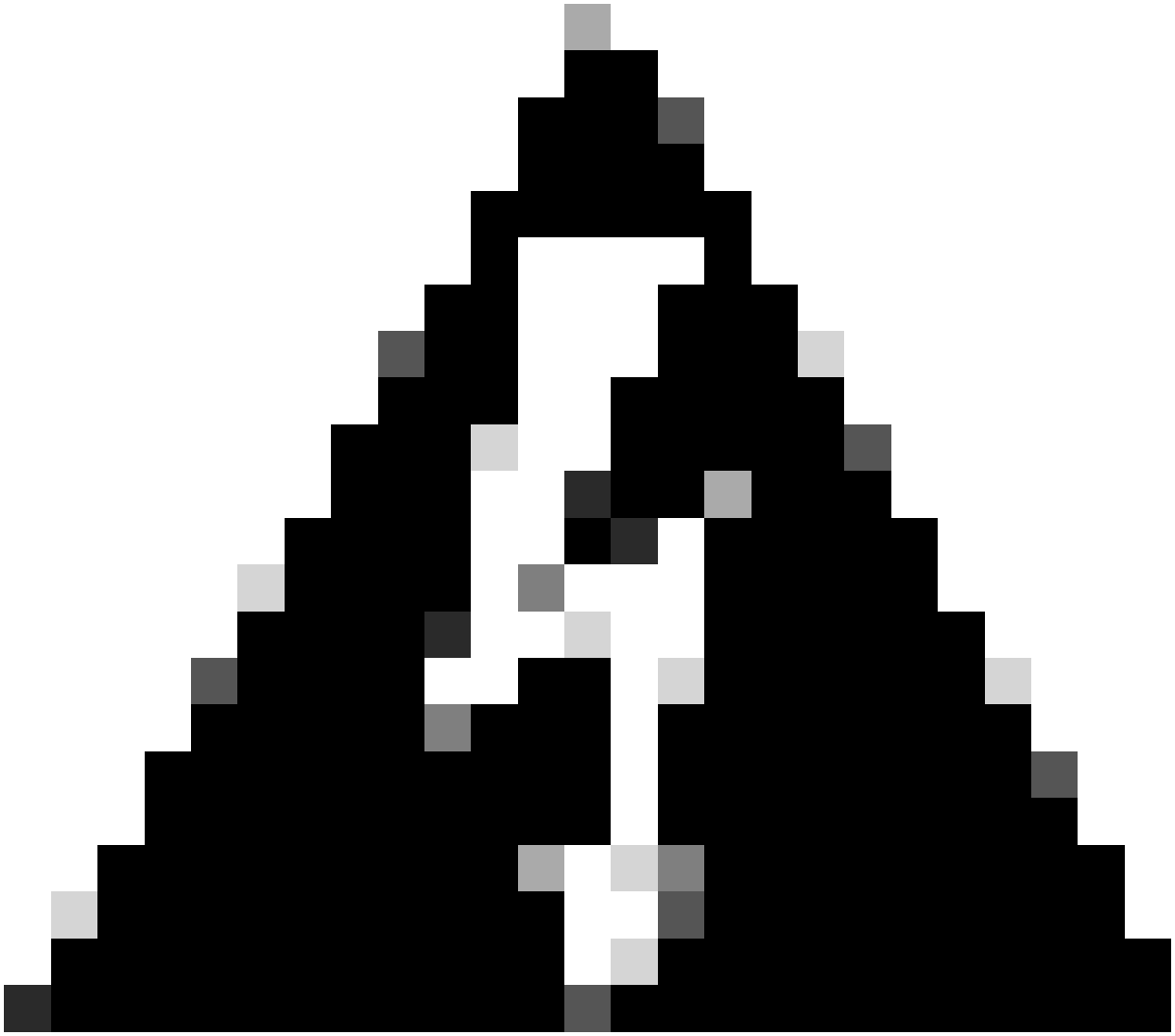
- Viene creata una voce della cache per ogni mapping creato nel rilevatore app personalizzato.
- Il primo pacchetto di tutte le sessioni in ingresso viene ispezionato per verificare se viene trovata una corrispondenza nella cache.
- Una volta trovata una corrispondenza, vengono assegnate le app corrispondenti per la sessione e il processo di individuazione delle app si arresta.
- Gli utenti hanno la possibilità di rivedere il traffico anche dopo che l'API ha trovato una corrispondenza.
- L'argomento respect è un valore booleano che indica se è necessario o meno ripetere l'analisi delle applicazioni trovate nel primo pacchetto.
- Quando la nuova ispezione è vera, l'individuazione delle app continua anche se l'API trova una corrispondenza.
- In questo caso, gli appid assegnati al primo pacchetto possono cambiare.

Prerequisiti, Piattaforme supportate, Licenze

Piattaforme software e hardware minime

Applicazione e versione minima	Piattaforme gestite supportate e versione	Responsabile/i	Note
Secure Firewall 7.4	Tutte le piattaforme	FMC locale + FTD	Si tratta di una

Utilizzo di Snort3	che supportano FTD 7.4		funzionalità sul lato dispositivo; FTD deve essere su 7.4



Avviso: l'Snort 2 non supporta questa API.

Snort 3, istanze multiple e supporto HA/clustering

Nota: richiede che Snort 3 sia il motore di rilevamento.

FTD	
Più istanze supportate?	Sì
Supportato con dispositivi HA'd	Sì
Supportato con i dispositivi del cluster?	Sì

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
· Cisco Firepower Threat Defense con versione 7.4 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.

Dettagli funzionalità

Descrizione funzionalità funzionale

Contrasto rispetto a questa release

In Secure Firewall 7.3 e versioni precedenti	Novità di Secure Firewall 7.4
· Il rilevamento delle applicazioni per una combinazione nota di IP/porta/protocollo era disponibile solo come opzione di fallback dopo l'esaurimento di tutti gli altri meccanismi di rilevamento delle applicazioni. · In pratica, il rilevamento sul primo pacchetto di una sessione non è supportato.	· La nuova API di rilevamento lua viene valutata prima di qualsiasi altro meccanismo di rilevamento dell'applicazione, · Pertanto, nella versione 7.4, il rilevamento è supportato sul primo pacchetto di una sessione.

Come funziona

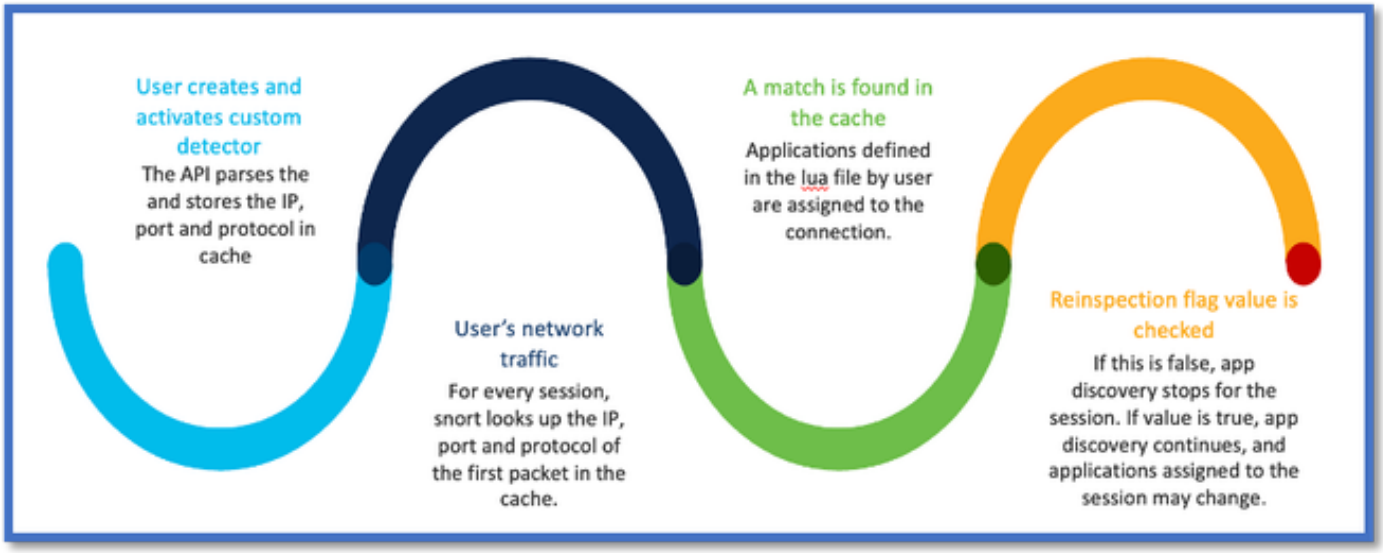
- Creare un file lua: assicurarsi che il file sia nel modello lua (nessun errore di sintassi). Verificare inoltre che gli argomenti forniti all'API nel file siano corretti.

- Creare un nuovo rilevatore personalizzato: creare un nuovo rilevatore personalizzato in FMC e caricare il file lua in esso. Attivare il rilevatore.

- Esegui traffico: invia al dispositivo il traffico che corrisponde alla combinazione IP/porta/protocollo definita nel rilevatore app personalizzato.

- Controllare gli eventi di connessione: in FMC controllare gli eventi di connessione filtrati dall'IP e dalla porta. Verrebbero identificate le applicazioni definite dall'utente.

Flusso di lavoro API rilevamento rapido pacchetti AppID



Esempio di descrizione dei campi API dal rilevatore personalizzato

gDetector:addHostFirstPktApp

(gAppIdProto, gAppIdClient, gAppId, 0, "192.0.2.1", 443, DC.ipproto.tcp);

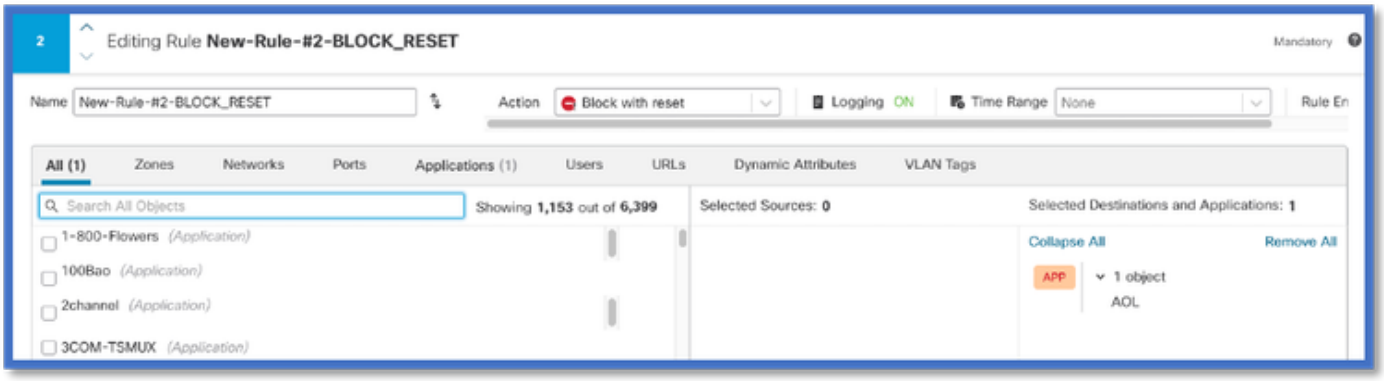
- Gli argomenti evidenziati sono i valori definiti dall'utente per il flag di ripetizione, l'indirizzo IP, la porta e il protocollo.
- 0 indica un carattere jolly.

Argomenti	Spiegazione	Valori previsti
Flag Ripeti controllo	Se un utente preferisce ispezionare il traffico anziché adottare misure firewall basate su IP/porta/protocollo, può abilitare il valore del flag di ripetizione del controllo su 1.	0 = reinspect disabilitato o 1 = respect abilitato
Indirizzo IP	IP di destinazione (singolo	192.168.4.198 O

	o intervallo di IP in una subnet) del server. IP di destinazione del 1º pacchetto di una sessione.	192.168.4.198/24 O 2a03:2880:f103:83:face:b00c:0:25de OR 2a03:2880:f103:83:faccia:b00c:0:25de/32
Port	Porta di destinazione del primo pacchetto in una sessione.	Da 0 a 65535
Protocollo	Protocollo di rete	TCP/UDP/ICMP

Caso di utilizzo: come bloccare il traffico più rapidamente

- Visualizzazione criterio: regola di blocco per l'applicazione "AOL".



- Test del traffico con curl con: curl https://www.example.com v/s curl https://192.0.2.1/ (uno degli indirizzi IP di TEST)

<#root>

```
> curl https://www.example.com/
```

```
curl: (35) OpenSSL SSL_connect: SSL_ERROR_SYSCALL in connection to www.example.com:443
```

```
> curl https://192.0.2.1/
```

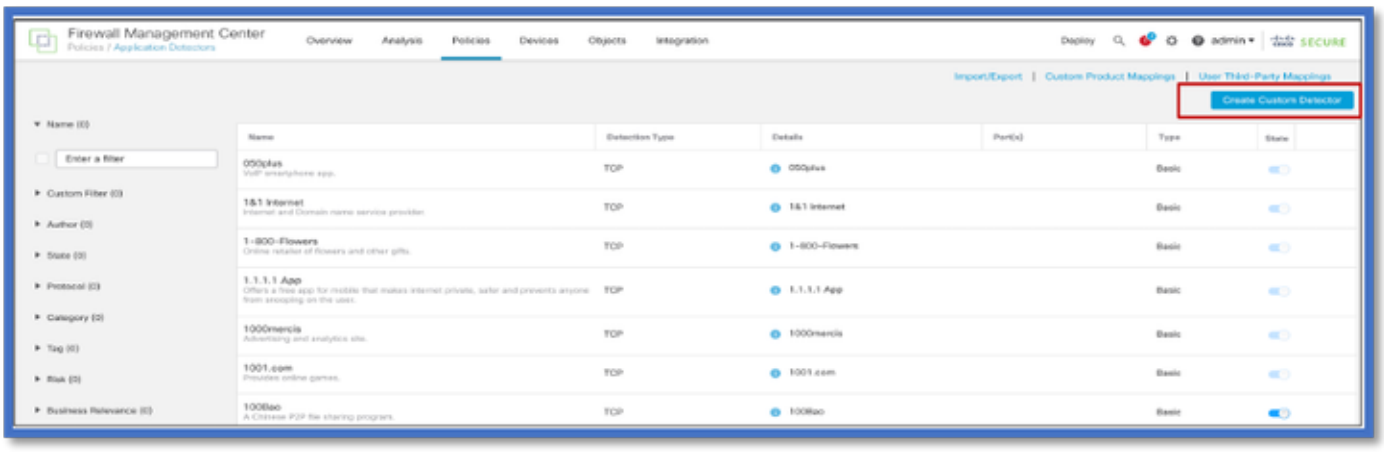
```
curl: (7) Failed to connect to 192.0.2.1 port 443: Connection refused
```

Procedura dettagliata di Centro gestione firewall

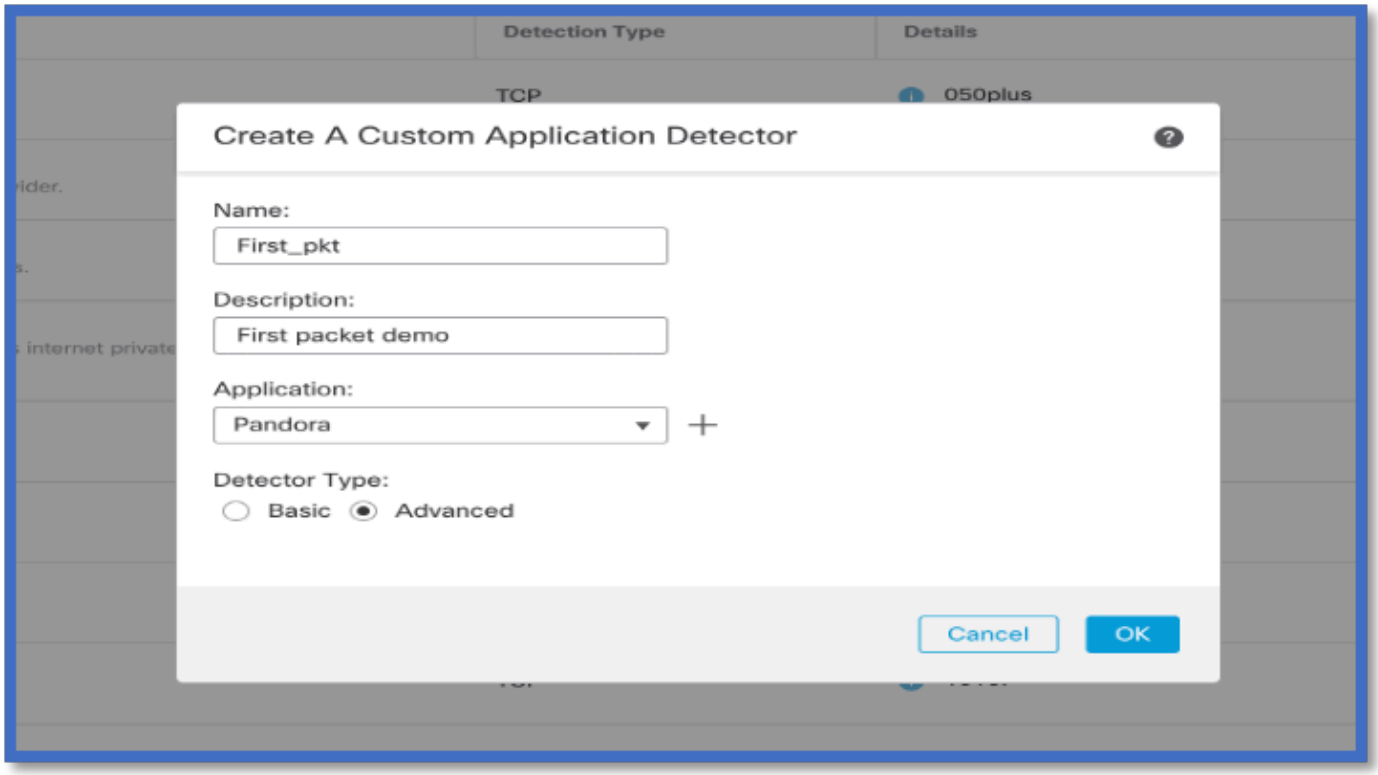
Procedura per creare un rilevatore personalizzato utilizzando l'API

Crea un nuovo rilevatore personalizzato nel CCP da:

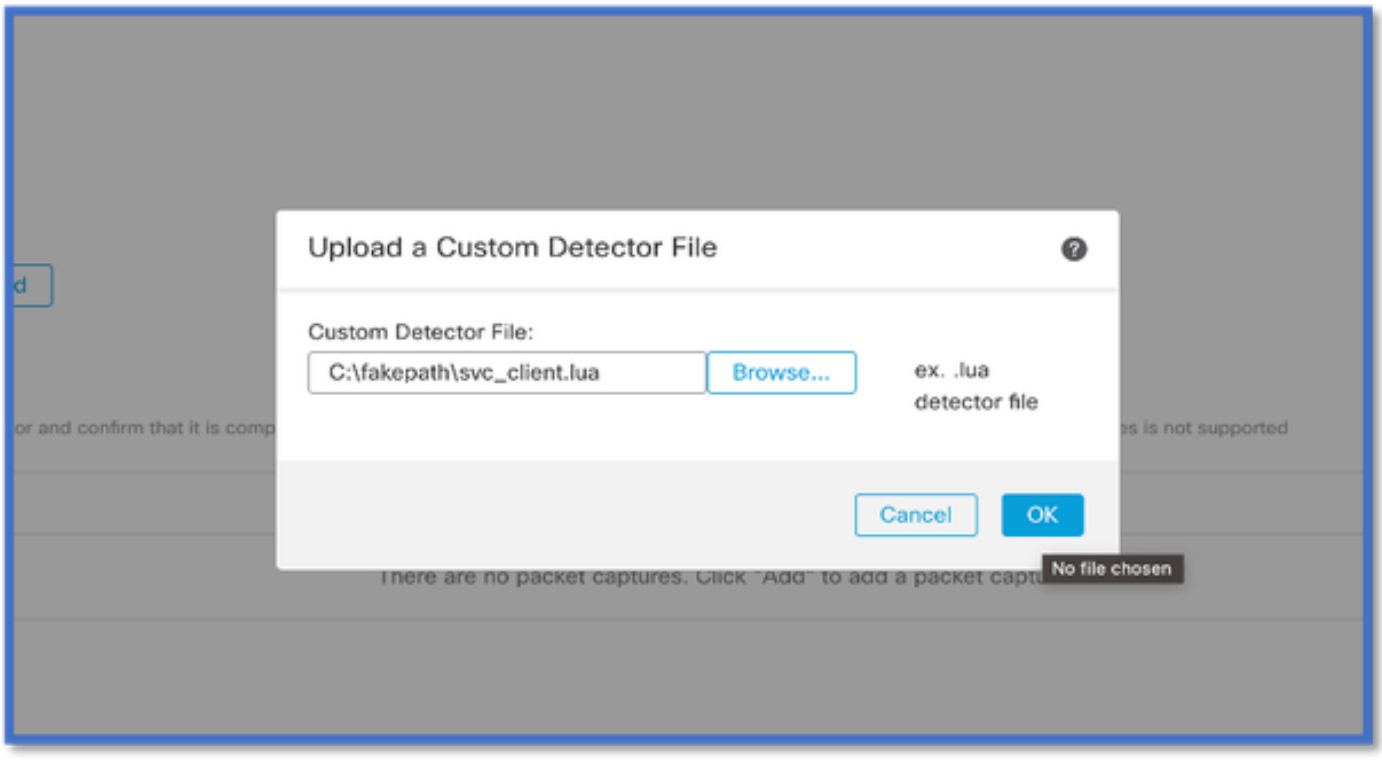
- Policies > Application Detectors > Create Custom Detector .



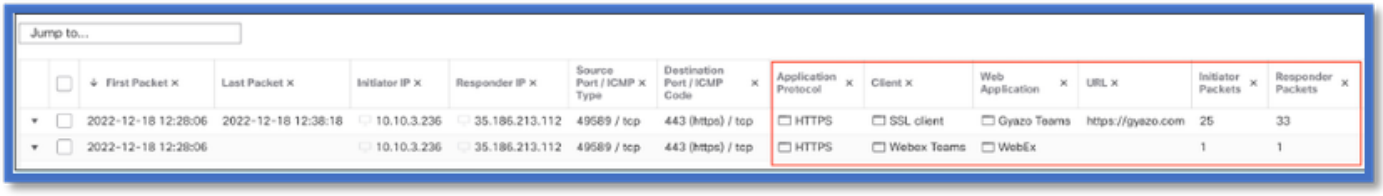
- Definire nome e descrizione.
  - Scegliere l'applicazione dal menu a discesa.
  - Selezionare Advanced Detector Type.



- Caricare il file Lua in Criteri di rilevamento. Salvare e attivare il rilevatore.



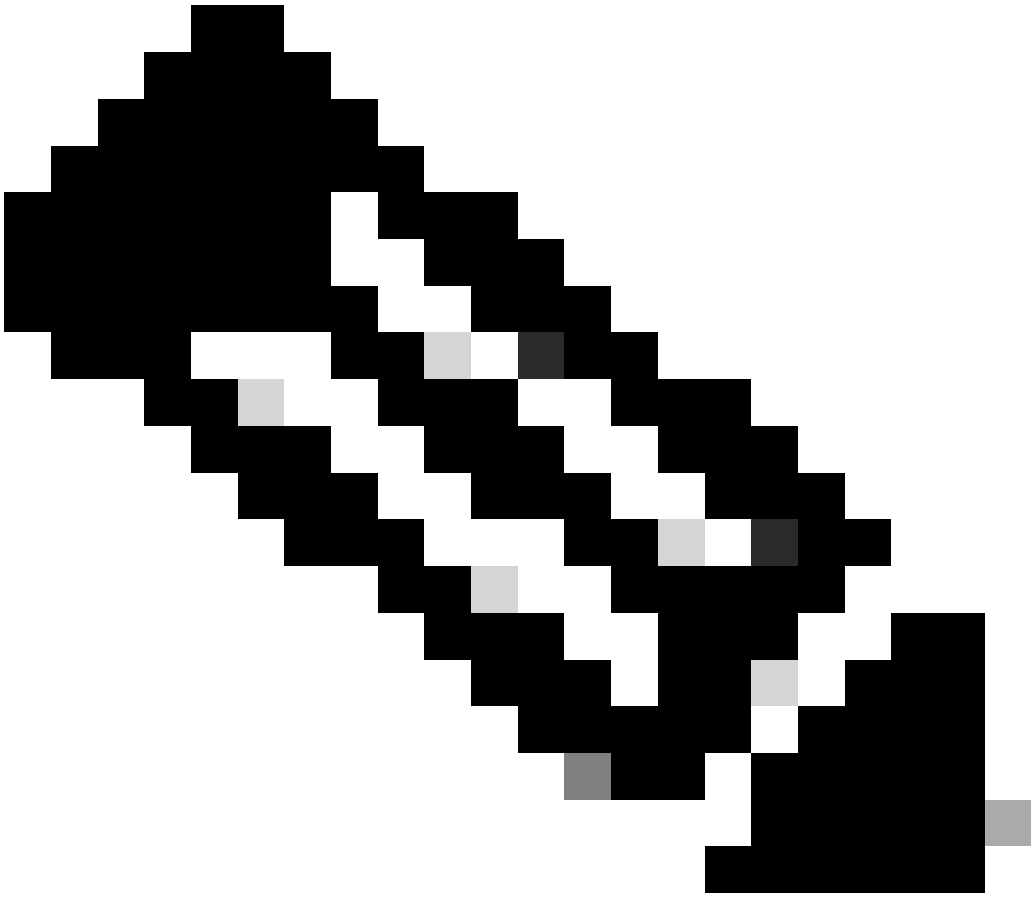
Reinspect abilitato v/s disabilitato



Jump to...

First Packet	Last Packet	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	Initiator Packets	Responder Packets
2022-12-18 12:28:06	2022-12-18 12:38:18	10.10.3.236	35.186.213.112	49589 / tcp	443 (https) / tcp	HTTPS	SSL client	Gyazo Teams	https://gyazo.com	25	33
2022-12-18 12:28:06		10.10.3.236	35.186.213.112	49589 / tcp	443 (https) / tcp	HTTPS	Webex Teams	WebEx		1	1

- I due eventi mostrano l'inizio della connessione rispetto alla fine della connessione quando è abilitata la ripetizione del controllo.



Nota:

1. I "HTTPS, Webex e Webex Teams" sono identificati dall'API all'inizio della connessione. Poiché la nuova ispezione è vera, l'individuazione delle app continua e gli ID delle app vengono aggiornati a 'HTTPS, client SSL e team Gyazo'.

2. Si noti il numero di pacchetti dell'iniziatore e del risponditore. I metodi di rilevamento dell'app standard richiedono un numero di pacchetti molto maggiore rispetto all'API.

Risoluzione dei problemi/Diagnostica

Panoramica sulla diagnostica

- Nuovi log vengono aggiunti nel debug di identificazione dell'applicazione di supporto al sistema per indicare se sono presenti applicazioni individuate dalla prima API di rilevamento pacchetti.
- I log mostrano anche se l'utente ha scelto di eseguire nuovamente l'ispezione del traffico.
- Il contenuto del file di rilevamento lua caricato dall'utente è disponibile sul FTD sotto /var/sf/appid/custom/lua/<UUID> .
- Eventuali errori nel file lua vengono scaricati sull'FTD nel file /var/log/messages al momento dell'attivazione del rilevatore.

CLI: supporto del sistema, identificazione applicazione-debug

<#root>

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 New AppId session

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service: HTTPS(1

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 New firewall session

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Src
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
```

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_RESET', action Re

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 MidRecovery data sent for rule id: 268437504, rule_acti
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Generating an SOF event with rule_id = 268437504 ruleAc
```

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 reset action

192.0.2.1 443 > 192.168.1.16 51251 6 AS-4 ID=0 New AppId session
192.0.2.1 443 > 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service:
HTTPS (1122), client: AOL(1419), payload: AOL (1419), reinspect: False
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload changed, referred no change, miss no change, Mad no change, fas host no change, bits 0x1D 192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 New firewall session
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Saclone first with zones 1 →> 1, geo 0(xff0) →> 0, yan 0, sae, sgt; 0, sag sat, type: unknown, det sat: 0, det sat type: unknown, sve 1122, payload 1419, client 1419, mise 0, user 9999997, no Mad or host, no xff
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_
_RESET', action
Reset
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID=0 MidRecovery, data sent for rule id: 268437504, rule_action:5, rev id:3558448739, Eule_match flag:0x1
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID-0 Generating an SOF event with zuleid - 268437504
ruleAction = 5 ruleReason = 0

Posizione del contenuto di AppID Lua Detectors

Per verificare se l'agente di rilevamento Lua con questa nuova API esiste sul dispositivo/FTD, è possibile verificare se l'API addHostFirstPktApp è in uso nelle 2 cartelle di rilevamento dell'applicazione:

1. Rilevatori AppID VDB -/var/sf/appid/odp/lua

2. Rilevatori personalizzati -/var/sf/appid/custom/lua

Ad esempio:grep addHostFirstPktApp * in ciascuna cartella.

Problemi di esempio:

- Problema: rilevatore Lua personalizzato non attivato sul CCP.

Percorso da controllare: /var/sf/appid/custom/lua/

Risultato previsto: in questo punto deve essere presente un file per ogni rilevatore di app personalizzato attivato nel FMC. Verificare che il contenuto corrisponda al file lua caricato.

- Problema: il file di rilevamento lua caricato contiene errori.

File da controllare: /var/log/messages on FTD

Registro errori:

<#root>

Dec 18 14:17:49 intel-x86-64 SF-IMS[15741]:

Error - appid: can not set env of Lua detector /ngfw/var/sf/appid/custom/lua/6698fbd6-7ede-11ed-972c-d12

Procedura di risoluzione dei problemi

Problema: applicazioni non identificate correttamente per il traffico diretto all'indirizzo IP e alla porta definiti dall'utente.

Passaggi per la risoluzione dei problemi:

- Verificare che il rilevatore lua sia correttamente definito e attivato sull'FTD.
    - Verificare il contenuto del file lua sull'FTD e controllare che non siano rilevati errori durante l'attivazione.
- Controllare l'IP, la porta e il protocollo di destinazione del primo pacchetto nella sessione di traffico.
    - Può corrispondere ai valori definiti nel rilevatore lua.
- Controllare system-support-application-identification-debug.
    - Cercare la riga Host cache match found on first packet. Se mancante, indica che non è stata trovata alcuna corrispondenza dall'API.

Dettagli su limitazioni, problemi comuni e soluzioni

Nella versione 7.4 non è disponibile un'interfaccia utente per l'utilizzo dell'API. Il supporto dell'interfaccia utente verrà aggiunto nelle versioni future.

Cronologia delle revisioni

Revisione	Data di pubblicazione	Commenti

1.0	18 luglio 2024	Release iniziale

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).