Fehlerbehebung für FirePOWER Data Path 7: Richtlinie für Sicherheitsrisiken

Inhalt

Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im Übersichtsartikel.

In diesem Artikel wird die siebte Phase der Fehlerbehebung für den FirePOWER-Datenpfad (Intrusion Policy) beschrieben.

Voraussetzungen

- Dieser Artikel gilt für alle Firepower-Plattformen, auf denen eine Intrusion Policy ausgeführt wird. Die **Ablaufverfolgungsfunktion** ist nur in Version 6.2 und höher für die Firepower Threat Defense (FTD)-Plattform verfügbar.
- Kenntnisse von Open-Source-Snort sind hilfreich, aber nicht erforderlich Informationen zu Open-Source-Snort finden Sie unter https://www.snort.org/

Fehlerbehebung in der Phase der Intrusion Policy

Verwendung des "trace"-Tools zum Erkennen von Angriffsrichtlinien-Verlusten (nur FTD)

Das Trace-Tool für den Systemsupport kann über die FTD-Befehlszeilenschnittstelle (CLI) ausgeführt werden. Dies ähnelt dem **Firewall-Engine-Debug-**Tool, das im Artikel der Access Control Policy-Phase erwähnt wird, jedoch tiefer in die inneren Arbeitsabläufe von Snort eingeht. Dies kann hilfreich sein, um zu prüfen, ob Intrusion Policy-Regeln für den interessanten

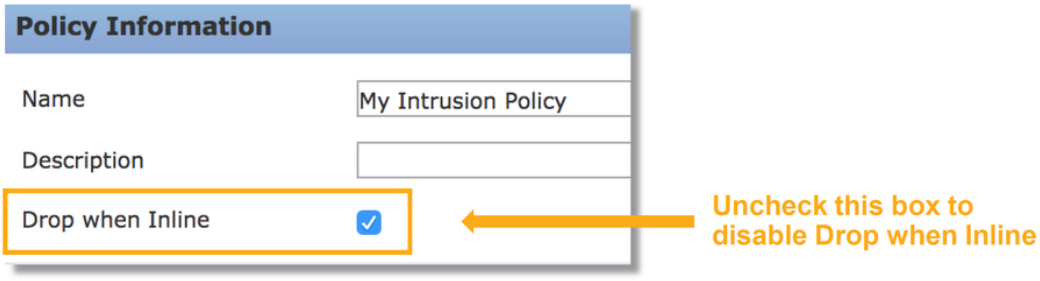
Datenverkehr ausgelöst werden.

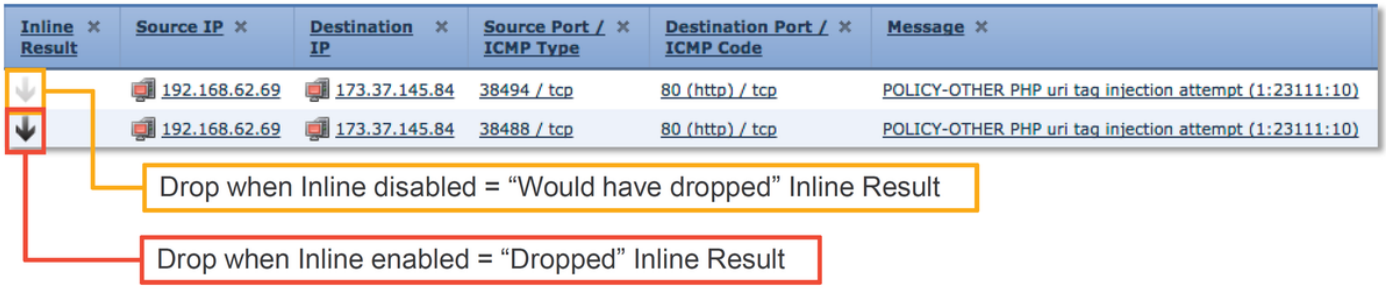
Im folgenden Beispiel wird der Datenverkehr vom Host mit der IP-Adresse 192.168.62.6 durch eine Intrusion Policy-Regel blockiert (in diesem Fall **1:23111**)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

Beachten Sie, dass die von snort angewendete Aktion **verworfen** wurde. Wenn eine Drop von snort erkannt wird, wird diese Sitzung dann auf Blacklists gesetzt, sodass alle weiteren Pakete ebenfalls verworfen werden.

Der Grund dafür, dass snort die **Drop**-Aktion ausführen kann, ist, dass die Option "Drop when Inline" (Beim Intrusion-Policy verwerfen, wenn Inline ablegen) in der Intrusion Policy aktiviert ist. Dies kann auf der Startseite der Intrusion Policy (Intrusion Policy) überprüft werden. Navigieren Sie im FirePOWER Management Center (FMC) zu **Policies > Access Control > Intrusion (Richtlinien > Zugriffskontrolle > Zugriffskontrolle),** und klicken Sie auf das Bearbeitungssymbol neben der betreffenden Richtlinie.





Wenn "Drop When Inline" (Bei Inline verwerfen) deaktiviert ist, verwirft snort keine Pakete mehr, meldet aber trotzdem mit einem **Inline-Ergebnis** von "Hätte gefallen" in den Angriffsereignissen.

Wenn "Drop When Inline" deaktiviert ist, zeigt die Ablaufverfolgungsausgabe eine Aktion für die betreffende Datenverkehrssitzung an, die **verworfen** wird.

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

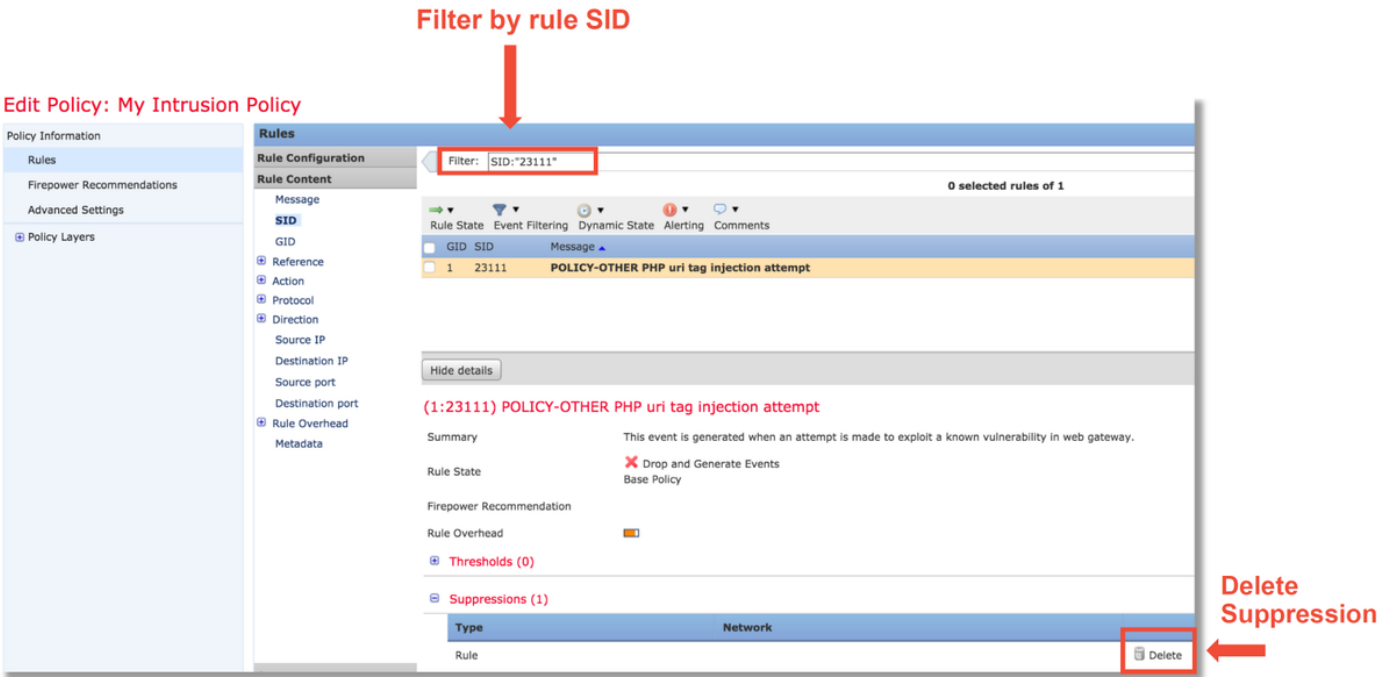
Suchen nach Unterdrückungen in den Angriffsrichtlinien

Es ist möglich, den Datenverkehr per Snort zu verwerfen, ohne Intrusion Events an das FMC zu senden (leise Verwerfen). Dies wird durch Konfigurieren von **Unterdrückungen** erreicht**.** Um zu überprüfen, ob eine Unterdrückung in einer Intrusion Policy konfiguriert wurde, kann die Expert Shell auf dem Backend überprüft werden (siehe unten).

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name        : My Intrusion Policy
```

Beachten Sie, dass die Intrusion Policy mit dem Namen "My Intrusion Policy" (Richtlinie für Sicherheitsrisiken) eine Unterdrückung für die 1:2311-Regel enthält. Daher kann der Datenverkehr aufgrund dieser Regel ohne Ereignisse verworfen werden. Dies ist ein weiterer Grund, warum das Trace-Dienstprogramm hilfreich sein kann, da es immer noch die auftretenden Verwerfen anzeigt.

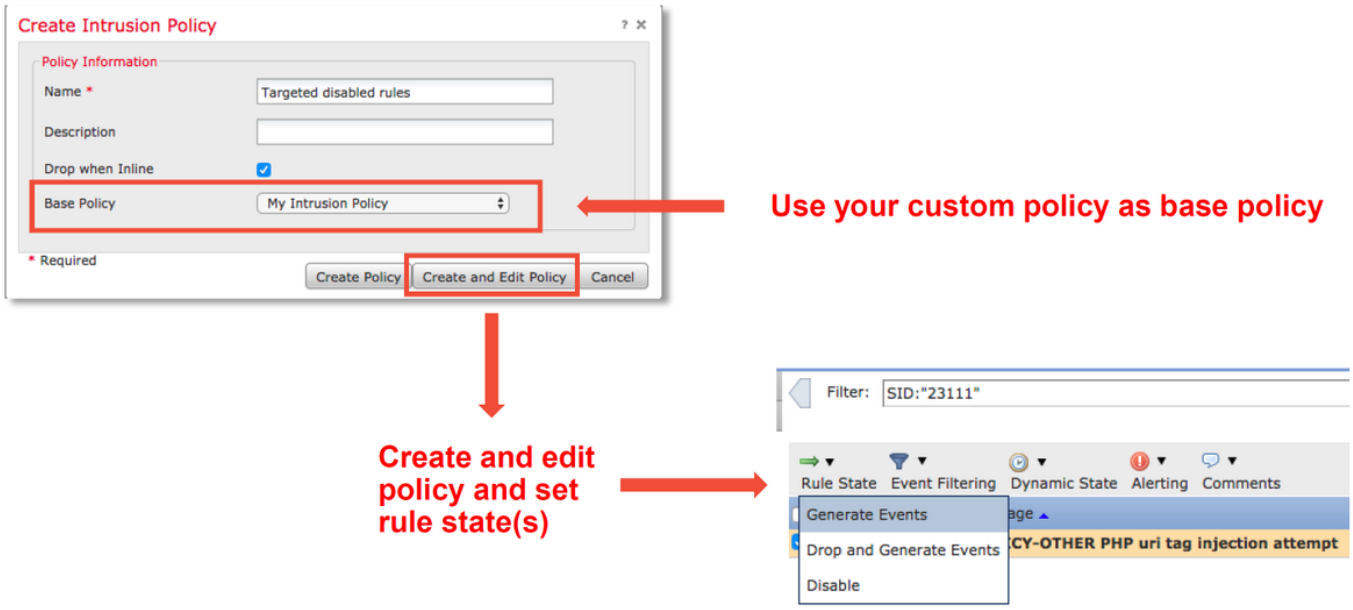
Um die Unterdrückung zu löschen, kann die betreffende Regel in der Ansicht **Intrusion Policy Rules** (Intrusionsrichtlinien) gefiltert werden. Dadurch wird eine Option zum Löschen der Unterdrückung angezeigt, wie unten gezeigt.



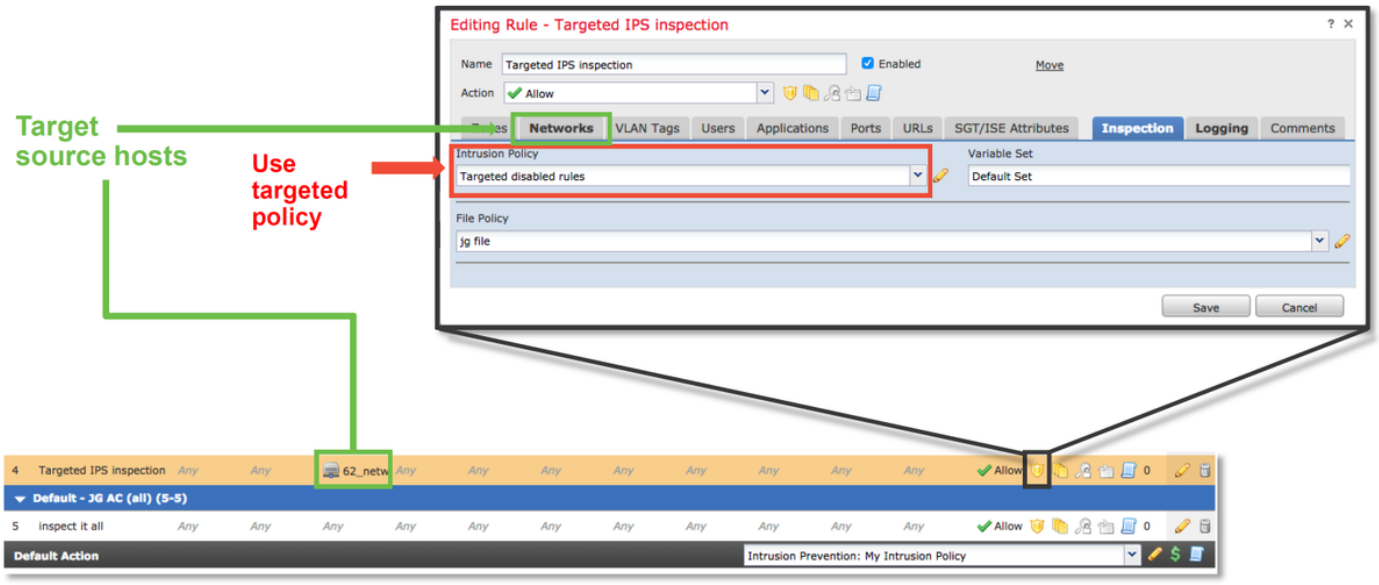
Erstellen einer Richtlinie für zielgerichtete Sicherheitsrisiken

Wenn der Datenverkehr von einer bestimmten Intrusion Policy-Regel verworfen wird, dürfen Sie nicht möchten, dass der betreffende Datenverkehr verworfen wird, Sie möchten aber möglicherweise auch nicht die Regel deaktivieren. Die Lösung besteht darin, eine neue Intrusion Policy zu erstellen, bei der die jeweilige(n) Regel(en) deaktiviert sind, und dann den Datenverkehr von den Zielhosts auswerten zu lassen.

Hier sehen Sie eine Abbildung zum Erstellen der neuen Intrusion Policy (Intrusion Policy) (unter **Policies > Access Control > Intrusion**).



Nach dem Erstellen der neuen Intrusion Policy kann sie in einer neuen Zugriffskontrollrichtlinie verwendet werden, die auf die betreffenden Hosts abzielt, deren Datenverkehr zuvor von der ursprünglichen Intrusion Policy verworfen wurde.



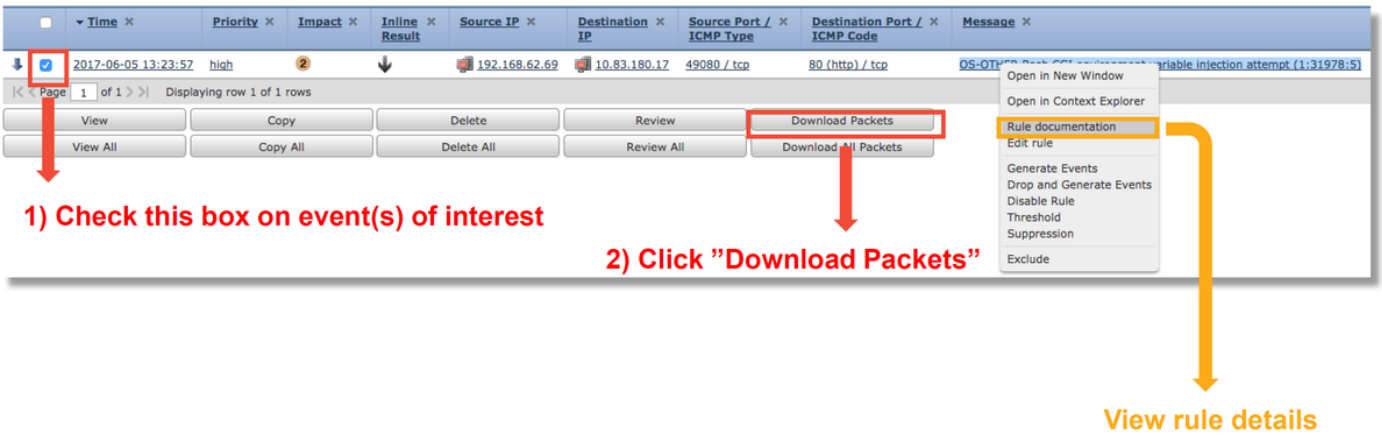
Fehlalarme Fehlerbehebung

Ein gängiges Fallbeispiel ist die falsch-positive Analyse von Angriffsereignissen. Es gibt mehrere Dinge, die überprüft werden können, bevor ein falsch positiver Fall ausgelöst wird.

1. Klicken Sie auf der Seite **Tabellenansicht von Angriffsereignissen** auf das Kontrollkästchen für das betreffende Ereignis.

2. Klicken Sie auf **Pakete herunterladen**, um die von Snort erfassten Pakete zu erhalten, wenn das Intrusion Event ausgelöst wurde.

3. Klicken Sie mit der rechten Maustaste auf den Regelnamen in der Spalte **Nachricht** und dann auf **Regeldokumentation**, um die Regelsyntax und andere relevante Informationen anzuzeigen.



Unten sehen Sie die Regelsyntax für die Regel, die das Ereignis im obigen Beispiel ausgelöst hat. Die Teile der Regel, die mit einer PCAP-Datei (Packet Capture) überprüft werden können, die vom FMC für diese Regel heruntergeladen wurde, sind fett formatiert.

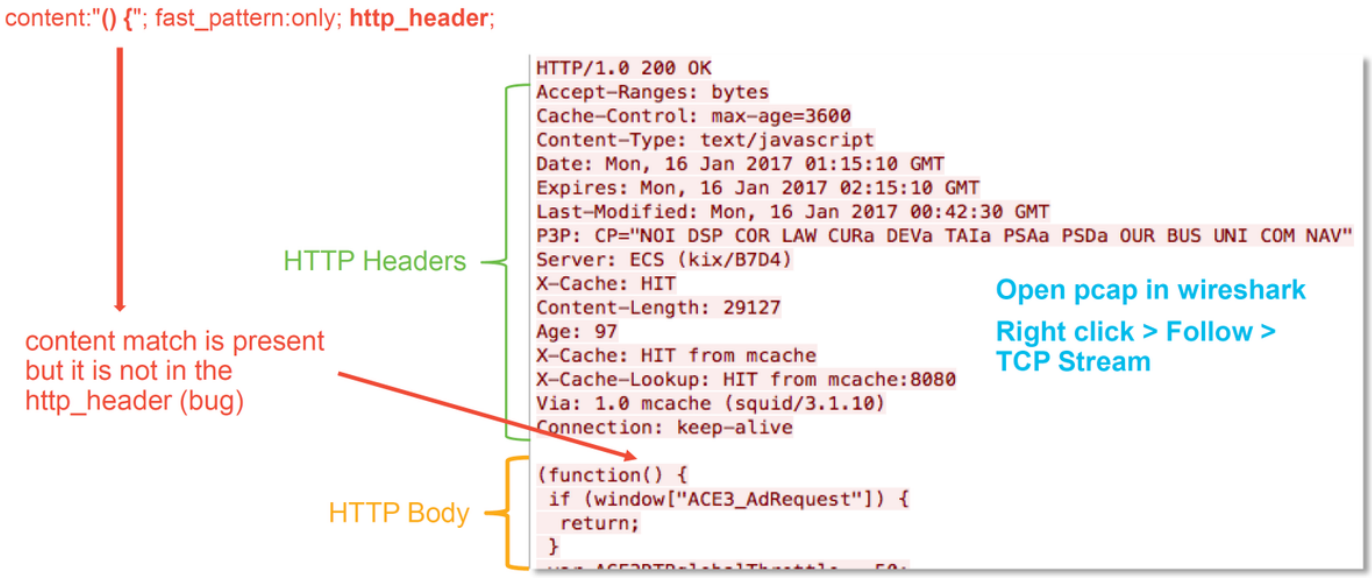
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg:"OS-OTHER Bash CGI environment variable einspritzungsversuch"; \
flow:to_server, eingerichtet; \
Content:"() {"; fast_pattern:nur; http_header; \

Metadaten:policy balance-ipsdrop, policy max-detect-ipsdrop, policy security-ipsdrop, rules-set community, **service http**; \
Referenz:cve,2014-6271; Referenz:cve,2014-6277; Referenz:cve,2014-6278; Referenz:cve,2014-7169; \
Klassentyp:versuted-admin; \
Sid: 31978; rev:5;)

Anhand dieser ersten Schritte können Sie dann den Analyseprozess durchführen, um festzustellen, ob der Datenverkehr mit der Regel übereinstimmen muss, die die Datenübertragung ausgelöst hat.

1. Überprüfen Sie die Zugriffskontrollregel, die den Datenverkehr zugeordnet hat. Diese Informationen sind Teil der Spalten auf der Registerkarte "Intrusion Events" (Angriffsereignisse).
2. Suchen Sie den in der genannten Zugriffskontrollregel verwendeten Variablensatz. Der Variablensatz kann dann unter **Objekte > Objektverwaltung > Variablensätze** überprüft werden.
3. Vergewissern Sie sich, dass die IP-Adressen in der PCAP-Datei den Variablen entsprechen (in diesem Fall ein in der **$EXTERNAL_NET-**Variable enthaltene Host, der mit einem in der Variablenkonfiguration **$HOME_NET** enthaltenen Host verbunden ist)
4. Für den **Datenfluss** muss möglicherweise eine vollständige Sitzung/Verbindung erfasst werden. Snort wird aus Leistungsgründen nicht den gesamten Datenfluss erfassen. In den meisten Fällen kann jedoch davon ausgegangen werden, dass die Sitzung bei Auslösung der Regel eingerichtet wurde, wenn eine Regel mit dem ausgelösten Fluss:eingehend ausgelöst wurde. Daher ist eine vollständige PCAP-Datei nicht erforderlich, um diese Option in einer kurzen Regel zu überprüfen. Es mag jedoch nützlich sein, den Grund, warum sie ausgelöst wurde, besser zu verstehen.
5. Wenn Sie einen HTTP-Dienst wünschen, sehen Sie sich die PCAP-Datei in Wireshark an, um festzustellen, ob sie wie HTTP-Datenverkehr aussieht. Wenn Sie die Netzwerkerkennung für den Host aktiviert haben und die Anwendung "HTTP" zuvor gesehen hat, kann dies dazu führen, dass der Dienst in einer Sitzung übereinstimmt.

Unter Berücksichtigung dieser Informationen können die vom FMC heruntergeladenen Pakete in Wireshark weiter geprüft werden. Die PCAP-Datei kann ausgewertet werden, um festzustellen, ob das ausgelöste Ereignis eine Fehlalarme ist.



In der Abbildung oben wurde der Inhalt, für den die Regel erkennt, in der PCAP-Datei angezeigt - **"() {"**

Die Regel gibt jedoch an, dass der Inhalt im HTTP-Header des Pakets erkannt werden soll -

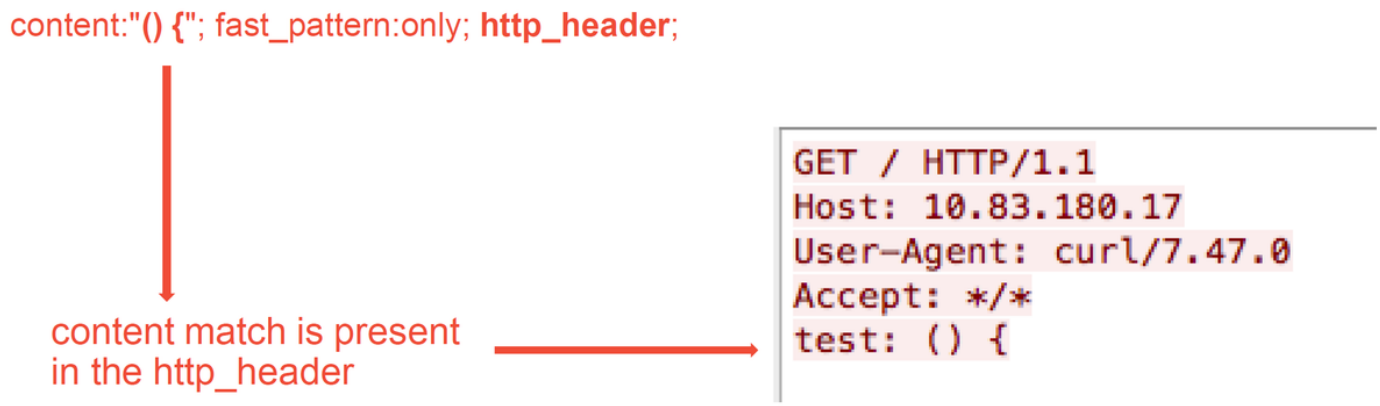
http_header

In diesem Fall wurde der Inhalt im HTTP-Text gefunden. Daher ist dies falsch positiv. Es ist jedoch nicht falsch positiv, da die Regel falsch geschrieben wurde. Die Regel ist korrekt und kann in diesem Fall nicht verbessert werden. In diesem Beispiel wird wahrscheinlich ein Snort-Fehler gefunden, der bei Snort zu Pufferverwirrung führt. Dies bedeutet, dass Snort die http_headers falsch identifiziert hat.

In diesem Fall können Sie nach vorhandenen Bugs für die snort/IPS-Engine in der Version, in der Ihr Gerät ausgeführt wird, suchen. Wenn keine Bugs vorhanden sind, kann ein Ticket beim Cisco Technical Assistance Center (TAC) geöffnet werden. Um ein solches Problem zu untersuchen, sind vollständige Sitzungsaufzeichnungen erforderlich, da das Cisco Team prüfen muss, wie Snort diesen Zustand erreicht hat, der nicht mit einem einzigen Paket durchgeführt werden kann.

Wahrhaft positives Beispiel

Die folgende Abbildung zeigt die Paketanalyse für dasselbe Intrusion Event. Dieses Mal ist das Ereignis ein echtes positives Ereignis, da der Inhalt im HTTP-Header angezeigt wird.



Daten für TAC

Daten	Anweisungen
Fehlerbehebungsdatei vom FirePOWER-Gerät, die den Datenverkehr prüft	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117
Paketerfassungen, die vom FMC heruntergeladen wurden	Anweisungen hierzu finden Sie in diesem Artikel.
Alle relevanten erfassten CLI-Ausgaben, z. B. **Trace**-Ausgabe	Anweisungen hierzu finden Sie in diesem Artikel.

Nächste Schritte

Wenn festgestellt wurde, dass die Intrusion Policy-Komponente nicht die Ursache des Problems ist, besteht der nächste Schritt in der Fehlerbehebung für die Network Analysis Policy-Funktion.

Klicken Sie hier, um zum letzten Artikel zu gelangen.