Lina-Regeln, die mit Snort-Funktionen konfiguriert wurden, werden behandelt

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Lina-Regeln in die FTD implementiert werden und wie Lina und Snort damit umgehen. Diese Informationen sind sowohl für das Onbox- (FDM) als auch für das Offbox- (FMC) Management nützlich.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Firepower Management Center (FMC)
- FirePOWER-Gerätemanager (FDM)
- Firepower Threat Defense Virtual (FTDv)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTDv 7.0.4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

FMC ist der Offbox-Manager für **Threat Defence**-Geräte.

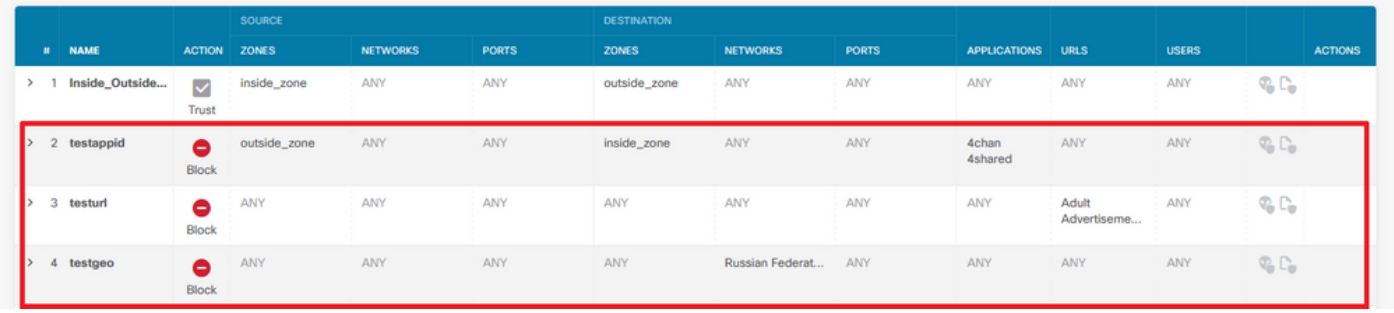
FDM ist der Onbox-Manager für **Threat Defence**-Geräte.

Regeln mit Snort-Funktionen werden so bereitgestellt, wie dies bei allen

Wenn Sie eine Regel mit Funktionen erstellen, die von der Snort-Seite ausgeführt werden, wie z. B. Geolocation, URL-Filter (Universal Resource Locator), Anwendungserkennung usw., werden sie auf der Lina-Seite bereitgestellt, um jede beliebige Regel zuzulassen.

Auf den ersten Blick kann dies Sie verwirren und Sie glauben machen, dass die FTD den gesamten Datenverkehr auf dieser Regel zulässt und die Überprüfung der Regelübereinstimmung für die folgenden Regeln stoppt.

In diesem Beispiel gibt es einen Anwendungsdetektor, einen URL-Filter und Regeln für Geolokalisierungsblöcke:



#	NAME	ACTION	SOURCE ZONES	SOURCE NETWORKS	SOURCE PORTS	DESTINATION ZONES	DESTINATION NETWORKS	DESTINATION PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Inside_Outside...	Trust	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	
2	testappid	Block	outside_zone	ANY	ANY	inside_zone	ANY	ANY	4chan 4shared	ANY	ANY	
3	testurl	Block	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Adult Advertiseme...	ANY	
4	testgeo	Block	ANY	ANY	ANY	ANY	Russian Federat...	ANY	ANY	ANY	ANY	

Hier sehen Sie die richtige Rule-Anweisung mit den auf der GUI konfigurierten Parametern (siehe Snort):

```
access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435458: L7 RULE: testappid
access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 ifc outside any ifc
inside any rule-id 268435458
access-list NGFW_ONBOX_ACL remark rule-id 268435459: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435459: L7 RULE: testurl
access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435459 any any rule-id
268435459
access-list NGFW_ONBOX_ACL remark rule-id 268435461: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435461: L5 RULE: testgeo
access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435461 any any rule-id
268435461
```

So sehen Regeln auf Snort-Seite aus:

```
268435458 deny 1 any any 2 any any any any (appid 948:5, 1079:5) (ip_protos 6)
# End rule 268435458
268435459 deny any any any any any any any any (urlcat 2027) (urlrep le 0) (urlrep_unknown 1)
268435459 deny any any any any any any any any (urlcat 2006) (urlrep le 0) (urlrep_unknown 1)
# End rule 268435459
268435461 deny 1 any any any any any any any (dstgeo 643)
# End rule 268435461
```

Überprüfen der Behandlung von Regeln auf Lina- und Snort-

Seiten

Da der Befehl "Packet-Tracer" diese Art von Regeln nicht korrekt verarbeitet, müssen Sie diesen zusammen mit Live-Datenverkehr mit der **Systemunterstützung "trace"** oder "**system support firewall-engine-debug"** testen.

Dies ist ein Beispiel, um die Geolokalisierungsregel zu treffen:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address:




Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring packet tracer and firewall debug messages

10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Packet 7: TCP
12****S*, 09/21-17:17:13.483709, seq 957225459, dsize 0
10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Session: new snort
session
10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 AppID: service:
(0), client: (0), payload: (0), misc: (0)
10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Firewall: starting
rule matching, zone 1 -> 1, geo 0(0) -> 643, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt:
0, dst sgt type: unknown, user 9999997, no url or host, no xff
10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Firewall: block
rule, 'testgeo', force_block
10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Stream: pending
block, drop
10.130.65.192 52459 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Policies: Network
0, Inspection 0, Detection 3
10.130.65.192 52459 -> <Geolocation block IP address>
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 New firewall
session
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 app event with app
id no change, url no change, tls host no change, bits 0x1
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Starting with
minimum 3, 'testurl', and SrcZone first with zones 1 -> 1, geo 0 -> 643, vlan 0, src sgt: 0, src
sgt type: unknown, dst sgt: 0, dst sgt type: unknown, svc 0, payload 0, client 0, misc 0, user
9999997
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 pending rule order
3, 'testurl', AppID for URL
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 rule order 3,
'testurl', action Block continue eval of pending deny
10.130.65.192 52460 ->




10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 MidRecovery data
sent for rule id: 268435461, rule_action:4, rev id:1095042657, rule_match flag:0x0
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 deny action
```

```
10.130.65.192 52460 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 Deleting Firewall
session
```

Wie Sie auf diesen Ausgaben sehen können, vergleicht Snort die Paketparameter mit den Regeln und stimmt mit der Geolocation-Blockregel überein. Anschließend wird der Fluss abgelehnt, und die Sitzung wird für den Fluss gelöscht.

Auf der Spur einer Lina-Erfassung können Sie in der ACCESS-LIST-Phase sehen, dass Sie die erste beliebige Regel für die Genehmigung treffen, anstatt der Geolokationsregel, die Sie erwartet haben. In der SNORT-Phase sehen wir jedoch auf dem Urteil, dass Snort die Regel 268435461 trifft, die die Geolokationsblockregel ist:

```
testftd# show cap test trace packet 1

9 packets captured

1: 17:36:52.082011 10.130.65.192.53336 > <Geolocation block IP address>.443: SWE
316839441:316839441(0) win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 10.130.65.188 using egress ifc outside(vrfid:0)

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435459 any any rule-id
268435459
access-list NGFW_ONBOX_ACL remark rule-id 268435459: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435459: L7 RULE: testurl
object-group service |acSvcg-268435459
service-object ip
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 6902, packet dispatched to next module

Phase: 10
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 11
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
00:50:56:96:D0:48 -> 00:50:56:B3:8C:E3 0800
10.130.65.192:53336 -> <Geolocation block IP address>:443 proto 6 AS=0 ID=1 GR=1-1
Packet 22: TCP 12****S*, 09/21-17:36:52.073696, seq 316839441, dsize 0
Session: new snort session
AppID: service: (0), client: (0), payload: (0), misc: (0)
Firewall: starting rule matching, zone 1 -> 1, geo 0(0) -> 643, vlan 0, src sgt: 0, src sgt
type: unknown, dst sgt: 0, dst sgt type: unknown, user 9999997, no url or host, no xff
Firewall: block rule, id 268435461, force_block
Stream: pending block, drop
Policies: Network 0, Inspection 0, Detection 3
Verdict: blacklist
Snort Verdict: (black-list) black list this flow

Result:
input-interface: outside(vrfid:0)
input-status: up
input-line-status: up
```

```
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location:
frame 0x000055b8a176d7b2 flow (NA)/NA
```

Schlussfolgerung

Wie bei der Konfiguration und den Live-Datenverkehrsprotokollen zu sehen ist, wird das Paket zur eingehenden Prüfung an Snort gesendet, obwohl Lina diese Regeln als Alle zulassen anzeigt und wir auf der Lina-Seite auf die genannte Regel treffen.

Anschließend können Sie überprüfen, ob Snort die Regeln weiterhin durchläuft, bis der Datenverkehr der erwarteten Regel entspricht.

Zugehörige Informationen

Konfigurationsleitfaden für FirePOWER Management Center, Zugriffskontrollregeln

Cisco Firepower Threat Defense - Konfigurationsleitfaden für Firepower Device Manager, Zugriffskontrolle

Cisco Bug-ID CSCwd00446 - DEU: Packet-Tracer zeigt keinen tatsächlichen Regeltrefferwert anstelle einer Geolocation-Regel in der ACL-Phase an.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.