Understand how Lina Rules Configured with Snort Features Are Handled

Contents

Introduction

This document describes how Lina rules are deployed into the FTD and the handling by Lina and Snort. This information is useful for both onbox (FDM) and offbox (FMC) management.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Firepower Management Center (FMC)
- Firepower Device Manager (FDM)
- Firepower Threat Defense Virtual (FTDv)

Components Used

The information in this document is based on these software and hardware versions:

- FTDv 7.0.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

FMC is the offbox manager for **Threat Defense** devices.

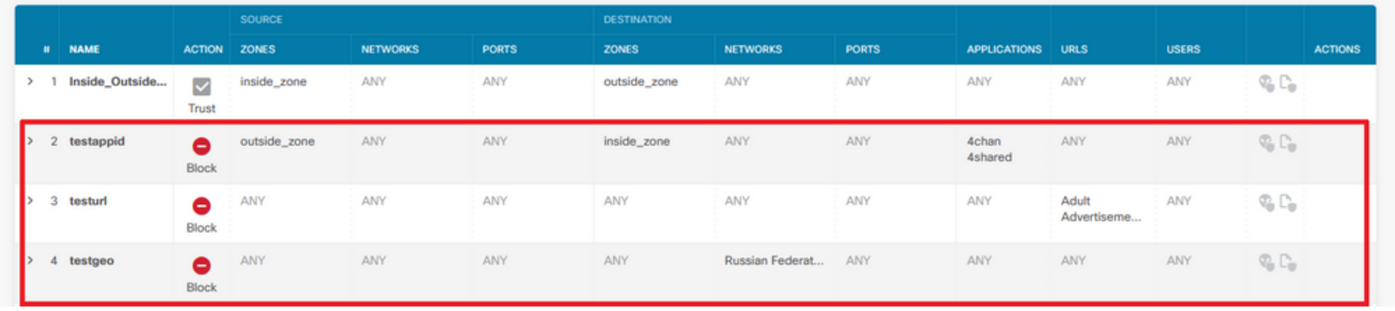
FDM is the onbox manager for **Threat Defense** devices.

Rules with Snort Features Are Deployed As Permit Any Any

When you create a rule with features that are run by Snort side, like Geolocation, URL (Universal Resource Locator) filter, Application detection, etc, they are deployed on Lina side as a permit any any rule.

At a first glance, this can confuse you and make you think that the FTD allows all the traffic on that rule and stops the rule match verification for the rules that follow.

In this example, there are Application detector, an URL Filter and Geolocation block rules:



			SOURCE			DESTINATION							
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	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		

Here you can see the correct rule statement with the parameters configured on the GUI as seen on 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
```

This is how rules are seen on Snort side:

```
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 (dstgeo 643)
# End rule 268435461
```

Verify how Rules Are Handled On Lina And Snort Sides

As packet-tracer command does not handle correctly these kind of rules, you need to test this wilth live traffic with **system support trace** or **system support firewall-engine-debug**.

This is an example to hit the geolocation block rule:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: <Geolocation block 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 -> <Geolocation block IP address> 443 6 AS=0 ID=1 GR=1-1 match rule order 4,
'testgeo', action Block
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
```

As you can see on these outputs, Snort checks the packet parameters against the rules and it matches the Geolocation block rule, then the flow is denied and session is deleted for the flow.

On the trace of a Lina capture, you can see on the ACCESS-LIST phase that you hit the first permit any any rule instead of the geolocation rule you expected to be hit, however on the SNORT phase, we see on the verdict that Snort hits rule **268435461**, which is the Geolocation block rule:

```
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
```

Conclusion

As seen with the configuration and live traffic logs, even though Lina show these rules as Permit any any and we hit said rule on Lina side, the packet is sent to Snort for deep inspection.

Afterwards, you can verify Snort continues to go through the rules until it matches the traffic to the expected rule.

Related Information

Firepower Management Center Configuration Guide, Access Control Rules

Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Access Control

Cisco bug ID CSCwd00446 - ENH: Packet-tracer does not show actual rule hit instead of a Geolocation rule on ACL phase