了解如何处理配置了Snort功能的Lina规则

目录

简介

本文档介绍如何将Lina规则部署到FTD以及Lina和Snort的处理。此信息对机内(FDM)和机外(FMC)管理都非常有用。

先决条件

要求

建议掌握下列主题的相关知识：

- Firepower Management Center (FMC)
- Firepower设备管理器(FDM)
- Firepower威胁防御虚拟(FTDv)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FTDv 7.0.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FMC是威胁防御设备的机**下管理**器。

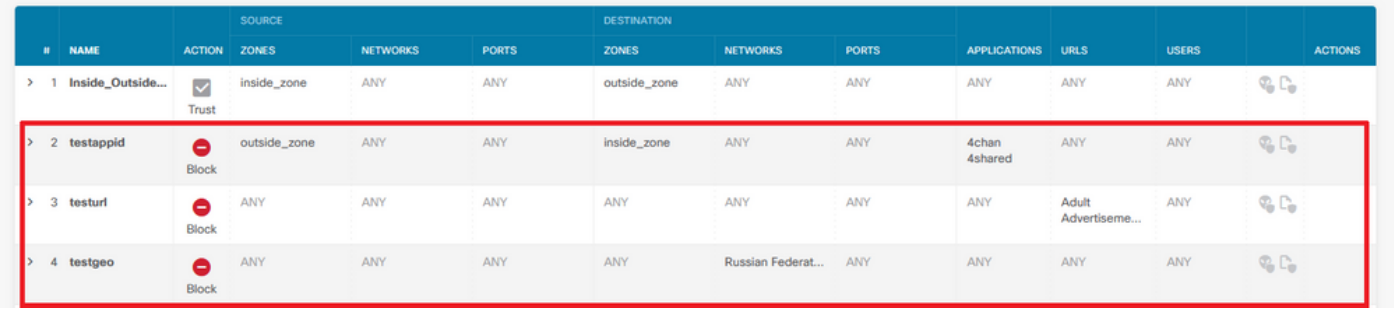
FDM是威胁防御设备的机**箱管理**器。

具有Snort功能的规则部署为permit any

当您使用由Snort端运行的功能(如Geolocation、URL(Universal Resource Locator)过滤器、应用检测等)创建规则时，它们将作为允许任何规则部署在Lina端。

乍一看，这会使您感到困惑，并让您认为FTD允许该规则上的所有流量，并停止后续规则的规则匹配验证。

在本示例中，有应用检测器、URL过滤器和地理位置阻止规则：



#	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	

在这里，您可以看到GUI上配置的参数与Snort上所示的正确规则语句：

```
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
```

在Snort端看到规则的方式如下：

```
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
```

验证在Lina和Snort端如何处理规则

由于packet-tracer命令无法正确处理此类规则，您需要使用**system support trace**或**system support firewall-engine-debug**测试此大量实时流量。

以下是一个符合地理定位阻止规则的示例：

```
> 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
```

正如您在以上输出中所看到的，Snort根据规则检查数据包参数，并且它与地理定位阻止规则匹配，然后拒绝该流并删除该流的会话。

在Lina捕获的跟踪上，您可以看到，在ACCESS-LIST阶段，您找到了第一个允许任何规则，而不是您预期要访问的地理定位规则；但在SNORT阶段，我们看到了Snort找到了规则**268435461**，这是地理定位块规则：

```
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
```

结论

如配置和实时流量日志所示，即使Lina将这些规则显示为Permit any any，并且我们在Lina端达到该规则，数据包也会发送到Snort进行深度检查。

然后，您可以验证Snort是否继续通过规则，直到其流量与预期规则相匹配。

相关信息

Firepower管理中心配置指南，访问控制规则

适用于Firepower设备管理器、访问控制的思科Firepower威胁防御配置指南

思科漏洞ID CSCwd00446 - ENH:Packet Tracer不会在ACL阶段显示实际的规则命中而不是地理定位规则

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。