فهم كيفية معالجة قواعد LINA التي تم تكوينها باستخدام ميزات SNORT

المحتويات

المقدمة

يوضح هذا المستند كيفية نشر قواعد Lina في FTD وكيفية التعامل معها بواسطة Lina و snort. تكون هذه المعلومات مفيدة لكل من إدارة المربع (FDM) والإزاحة (FMC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- مركز إدارة Firepower (FMC)
- مدير جهاز Firepower (FDM)
- الدفاع الظاهري ضد تهديد Firepower (FTDv)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- FTDv 7.0.4

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

إن FMC هو مدير صندوق البريد لأجهزة **الدفاع عن التهديد**.

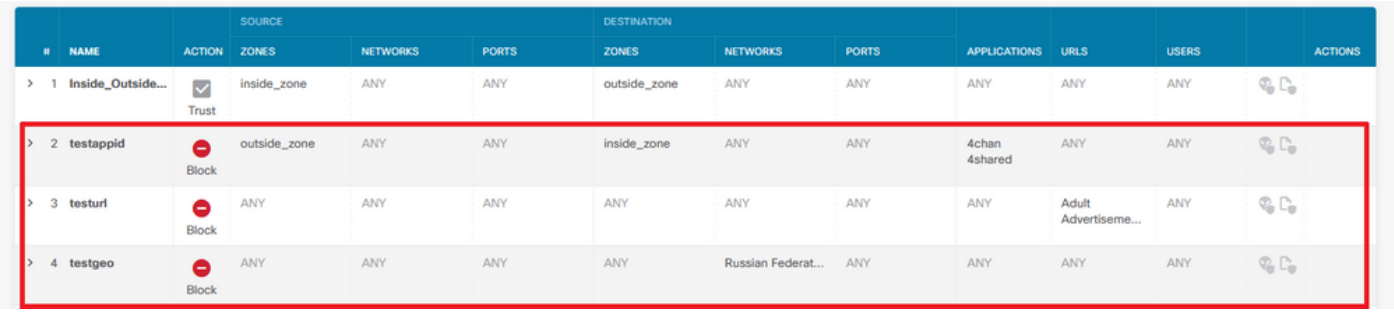
FDM هو مدير المربع لأجهزة **الدفاع عن التهديد**.

يتم نشر القواعد التي تحتوي على ميزات الشم للسماح بأي

عندما تقوم بإنشاء قاعدة باستخدام ميزات يتم تشغيلها بواسطة جانب Snort، مثل الموقع الجغرافي، وعامل تصفية URL (محدد موقع الموارد العالمي)، واكتشاف التطبيقات، وما إلى ذلك، يتم نشرها على جانب Lina للسماح بأي قاعدة.

للوهلة الأولى، قد يؤدي ذلك إلى إرباكك ويجعلك تعتقد أن FTD يسمح بكل حركة مرور البيانات على تلك القاعدة ويوقف التحقق من مطابقة القاعدة للقواعد التي تليها.

في هذا المثال، يوجد كاشف التطبيق، وعامل تصفية URL وقواعد كتل تحديد الموقع الجغرافي:



#	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	

يمكنك هنا رؤية بيان القاعدة الصحيح مع المعلمات التي تم تكوينها على واجهة المستخدم الرسومية (GUI) كما هو موضح في 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
```

وهذه هي الطريقة التي ترى بها القواعد على جانب الشخير:

```
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
```

تحقق من كيفية التعامل مع القواعد على جوانب Lina و snort

بما أن أمر packet-tracer لا يعالج هذا النوع من القواعد بشكل صحيح، فأنت تحتاج إلى إختبار حركة المرور المباشرة هذه باستخدام **تتبع دعم النظام** أو **دعم النظام جدار الحماية-المحرك-debug**.

اذه مثال للضغط على قاعدة كتلة الموقع الجغرافي:

```
> 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
```

كما يمكنك أن ترى في هذه المخرجات، يتحقق snort من معلمات الحزمة مقابل القواعد ويطابق قاعدة كتلة الموقع الجغرافي، ثم يتم رفض التدفق ويتم حذف جلسة العمل للتدفق.

على تتبع التقاط Lina، يمكنك أن ترى في مرحلة قائمة الوصول أن توقع بالوصول إلى أول، ومع تصريح بأي قاعدة بدل من قاعدة الموقع الجغرافي التي كنت تتوقع الوصول إليها،

ذلك في مرحلة الشيخ، نرى على الحكم أن Snort تضرب القاعدة **268435461**، وهي قاعدة كتلة الموقع الجغرافي:

```
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
```

الرارق

كما هو الحال مع التكوين وسجل حركة المرور الحية، على الرغم من أن ليانا تظهر هذه القواعد على أنها تسمح بأي شيء ونحن نضرب القاعدة المذكورة على جانب ليانا، يتم إرسال الحزمة إلى الشورت للتفتيش العميق.

بعد ذلك، يمكنك التحقق من إستمرار Snort في المرور خلال القواعد حتى يطابق حركة المرور بالقاعدة المتوقعة.

معلومات ذات صلة

دليل تكوين مركز إدارة Firepower وقواعد التحكم في الوصول

دليل تكوين الدفاع عن تهديد FirePOWER ل FirePOWER Device Manager، التحكم في الوصول من Cisco

معرف تصحيح الأخطاء من Cisco CSCwd00446 - ENH: الأمر Packet-tracer قيمة القاعدة الفعلية التي تم الوصول إليها بدلا من قاعدة تحديد الموقع الجغرافي على مرحلة قائمة التحكم في الوصول (ACL)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).