Entender como as regras de Lina configuradas com recursos do Snort são tratadas

Contents

Introduction

Este documento descreve como as regras Lina são implantadas no FTD e o tratamento por Lina e Snort. Essas informações são úteis para o gerenciamento dentro da caixa (FDM) e fora da caixa (FMC).

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Firepower Device Manager (FDM)
- Defesa contra ameaças do Firepower Virtual (FTDv)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O FMC é o gerenciador de offbox para **dispositivos Threat Defense**.

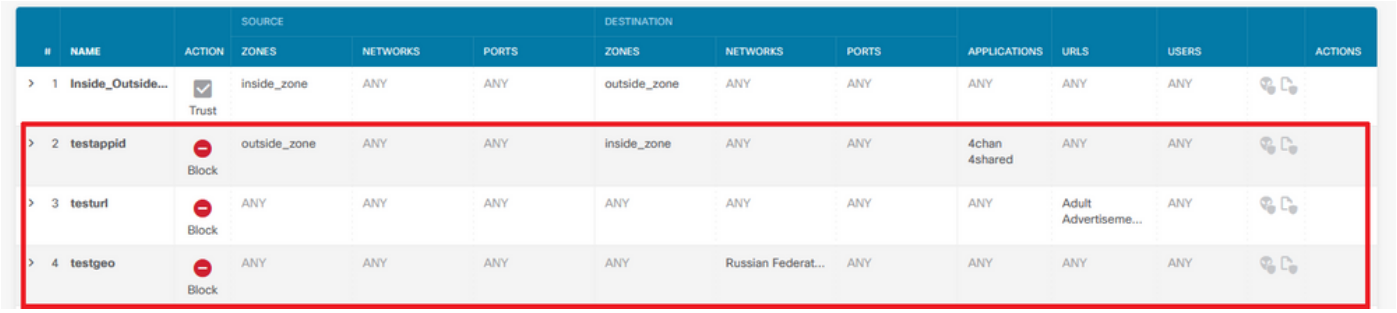
O FDM é o gerenciador da caixa de entrada para **dispositivos Threat Defense**.

As regras com recursos Snort são implantadas como Permit Any Any

Quando você cria uma regra com recursos que são executados pelo lado do Snort, como Geolocalização, filtro de URL (Universal Resource Locator), detecção de aplicativo, etc, eles são implantados no lado do Lina como uma regra permit any any.

Àprimeira vista, isso pode confundir você e fazer você pensar que o FTD permite todo o tráfego nessa regra e interrompe a verificação de correspondência da regra para as regras que se seguem.

Neste exemplo, há o Application detector, um filtro de URL e regras de bloqueio de localização geográfica:



#	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	

Aqui você pode ver a instrução de regra correta com os parâmetros configurados na GUI conforme visto no 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
```

Éassim que as regras são vistas no lado do Snort:

```
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
```

Verificar Como As Regras São Tratadas Nos Lados Lina E Snort

Como o comando packet-tracer não lida corretamente com esses tipos de regras, você precisa

testar esse tráfego ao vivo com **rastreamento de suporte do sistema** ou **suporte do sistema firewall-engine-debug**.

Este é um exemplo para atingir a regra de bloqueio de geolocalização:

```
> 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
```

Como você pode ver nessas saídas, o Snort verifica os parâmetros do pacote em relação às regras e ele corresponde à regra de bloqueio de localização geográfica, em seguida, o fluxo é

negado e a sessão é excluída para o fluxo.

No rastro de uma captura de Lina, você pode ver na fase ACCESS-LIST que você atingiu a primeira regra permit any any em vez da regra de geolocalização que você esperava atingir, no entanto, na fase SNORT, vemos no veredito que Snort atinge a regra **268435461**, que é a regra de bloqueio de geolocalização:

```
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
```

Conclusão

Como visto na configuração e nos registros de tráfego ao vivo, embora Lina mostre essas regras como Permit any any e nós atingimos essa regra no lado de Lina, o pacote é enviado para Snort para inspeção profunda.

Depois, você pode verificar se o Snort continua a passar pelas regras até que corresponda o tráfego à regra esperada.

Informações Relacionadas

Guia De Configuração Do Firepower Management Center, Regras De Controle De Acesso

Guia de configuração do Cisco Firepower Threat Defense para o gerenciador de dispositivos do Firepower, controle de acesso

ID de bug da Cisco CSCwd00446 - ENH: O Packet Tracer não mostra um acerto de regra real em vez de uma regra de Geolocalização na fase ACL

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.